MITRATECH

TeamConnect® Enterprise 5.0

© 2017 Mitratech

Administrator Guide

TeamConnect® Enterprise 5.0 Administration Guide

Document ID: tce_5_0_admin_1, published on 10/11/2017

Copyright © 2017, Mitratech Holdings, Inc. All rights reserved.

Disclaimer of Warranty

Mitratech Holdings, Inc. (Mitratech) makes no representations or warranties, either expressed or implied, by or with respect to anything in this document, and shall not be liable for any implied warranties of merchantability or fitness for a particular purpose or for any indirect, special or consequential damages.

Mitratech reserves the right to not support non-standard or non-default functionality and extended functionality available in third-party software, unless specifically documented as supported or certified in the Mitratech product documentation. For further information regarding third-party non-standard or non-default functionality, please contact Mitratech Support.

This document, along with the software that it describes, is furnished under license and may be used or copied only in accordance with the terms of such license. The content of this document is furnished for informational use only, is subject to change without notice, and should not be construed as commitment by Mitratech.

The following document is for the TeamConnect™ Enterprise 5.0 release only. Though every effort was made to ensure that the information in this document is correct and reliable, Mitratech does not assume any liability for any errors encountered in this document.

If you need support for TeamConnect™ Enterprise 5.0, please contact the Mitratech support team by sending an email to: support@mitratech.com. For more information about Mitratech, visit our web site: http://www.mitratech.com.

"Mitratech", TeamConnect™ Enterprise, TeamConnect™ Legal, TeamConnect™ Legal Matter Management, Collaborati®, TeamConnect™ Collaborati Spend Management®, TeamConnect™ Deadlines, TeamConnect™ AP Link, TeamConnect™ Office Suite, TeamConnect™ Legal Reports, TeamConnect™ SOP Manager, TeamConnect™ Financial Management, TeamConnect™ Screen Designer, and TeamConnect™ Upgrade Toolkit are trademarks and products of Mitratech Holdings, Inc. All other products or services mentioned in this book are the trademarks or service marks of their respective companies or organizations.

GOVERNMENT RIGHTS LEGEND:
Use, duplication or disclosure by the U.S. Government is subject to restrictions set forth in the applicable Mitratech license agreement and as provided in DFARS 227.7202-1(a) and 227.7202-3(a) (1995), DFARS 252.227-7013 (Feb 2012)FAR 12.212(a) (1995), FAR 52.227-19 (Dec 2007), or FAR 52.227-14, as applicable.

CONTACT US:
Mitratech Holdings, Inc.
5001 Plaza on the Lake Suite 111, Austin, TX 78746
Phone: (512) 382-7322

NOTE: Throughout Mitratech product publications, in addition to using full product names where necessary, we also use familiar and shorter terms to increase your ease of reading. You may find the following aliases for our product names:

TeamConnect for TeamConnect Enterprise
Matter Management for TeamConnect Legal Matter Management
TeamConnect Legal for TeamConnect Legal Matter Management
CSM for TeamConnect Collaborati Spend Management
Collaborati Spend Management for TeamConnect Collaborati Spend Management
SOP or SOP Manager for TeamConnect SOP Manager
Legal Hold for TeamConnect Legal Hold
Legal Reports for TeamConnect Legal Reports
Deadlines for TeamConnect Deadlines
AP Link for TeamConnect AP Link
Office Suite for TeamConnect Office Suite
Financial Management for TeamConnect Financial Management
Screen Designer for TeamConnect Screen Designer
Upgrade Toolkit for TeamConnect Upgrade Toolkit

Acknowledgements

This product includes software developed by the following organizations:

Apache Software Foundation (http://www.apache.org/)

OpenSymphony Group (http://www.opensymphony.com/).

The license agreements for these and other supplemental software packages can be found in your installation media in subfolder Supplemental_Software_Licenses. That subfolder also contains Open Source Components.pdf, which lists the locations, license types, and specific versions of components that are available on the web.

Table of Contents

Part I Enterprise Administrator Help 9

1 Getting Started 9

Admin Area User Interface 9
Group Rights Pages 9
Admin Settings General Page 10
Save Options 11
Terminology 12

2 Account Administration 12

Planning and Best Practices 13
Understanding Rights 14
Rights for End-Users 15
Rights for Administrators 16
Rights for Solution Developers 16
Rights for System Record Types 19
Prerequisites for Rights to System Record Types 21
Rights Impacts on Related Records 21
Rights for Categories and Custom Fields 22
Prerequisites for Rights to All Categories and Custom Fields 24
Prerequisites for Rights to Single Categories and Custom Fields 25
Rights for Custom Record Types 27
Rights for TeamConnect Features or Areas 28
Groups 28
Working with Groups 32
Searching for Groups 32
Viewing Groups 33
Creating or Editing Groups 33
Creating a Group Using a Template 35
Changing Group Members 35
Assigning or Viewing Group System Rights 36
Assigning or Viewing Global User Rights for a Group 38
Results from Assigning Global User Rights 40
Assigning Global Admin Rights to a Group 46
Results from Assigning Global Admin Rights 47
Assigning Global Setup Rights to a Group 48
Results from Assigning Global Setup Rights 49
Example for Assigning Rights to View Contacts 53
Example for Assigning Rights to Create Contacts 54
Example for Assigning Rights to Edit Contacts 54
Example for Assigning Rights to Delete Contacts 55
Example for Assigning All Rights to Contacts Pages and Fields 55
Examples for Assigning Projects Rights 56
Assigning All Rights to Dispute Pages and Fields 57
Assigning Group Category and Custom Field Rights 58
Example for Assigning Rights to Contact Categories and Fields 60
Hierarchy Overview of Group Rights 62
Assigning Group Tool Rights 64
Changing Group Default Object Views 65

Viewing or Creating Group History ... 66
Deleting a Group ... 66
Users ... 67
Working with Users ... 68
Searching for Users ... 69
Viewing Users ... 69
Creating or Editing Users ... 71
Creating a User Using a Template ... 75
Example for Creating a Limited-Privilege User ... 75
Activating and Inactivating a User ... 76
Prompting Users to Change Their Passwords ... 76
Editing or Viewing a User's Preferences ... 76
Unlocking User Accounts ... 77
Changing a User's Group Membership ... 77
Assigning or Viewing User System Rights ... 78
Assigning or Viewing Global User Rights for a User ... 82
Assigning or Viewing Global Admin Rights for a User ... 83
Assigning or Viewing Global Setup Rights for a User ... 84
Assigning or Viewing User Category Rights ... 85
Assigning or Viewing User Tool Rights ... 87
Viewing or Creating User History ... 88
Deleting a User ... 88
Using the User General Page ... 89
3 System Administration ... 89
Working with Admin Settings ... 90
General Admin Settings ... 91
Record Locking ... 91
BusinessObjects Web Intelligence Single Sign-on ... 92
Setting Up General Settings ... 93
User Interface Settings ... 96
Custom Logo ... 96
Color Profile Administration ... 96
Moving Action Buttons ... 102
Setting User Selection Options ... 102
Item Selection ... 103
Setting up the User Interface ... 103
Regions and Localization ... 106
Region Settings ... 106
Setting Regional Settings ... 106
Working with Locales ... 109
Localizing Data in TeamConnect ... 114
Exporting Data for Translation ... 114
Importing Translated Data ... 117
Calendar Settings ... 118
Documents Settings ... 118
Document Version Control ... 119
Network File Systems for Documents (WebDAV) ... 119
Managing Documents ... 120
Search Results Settings ... 122
Maximum Search Results ... 123
Setting Up Search Results ... 124
Reporting Settings ... 127
Defining Reporting Settings ... 127
Security Settings ... 128

Defining the User Password Policy ... 128
Configuring User Authentication ... 133
Email Settings ... 135
Email Notification ... 136
TeamConnect IMAP Server ... 137
Setting Up SSL for the IMAP Server ... 138
Configuring the IMAP Server ... 139
Starting and Stopping the IMAP Server ... 140
Email Rights ... 141
Email Clients ... 141
Setting Up Email ... 141
Notification Settings ... 143
Customizing System Notifications ... 146
Invoices Settings ... 147
Setting Decimal Places for Invoice Line Items ... 149
Approval Settings ... 149
Maintenance Settings ... 151
Connections Settings ... 152
Setting Up Connections ... 153
Admin Settings History ... 154
Recording a History for Admin Settings ... 154
About TeamConnect ... 155
Viewing TeamConnect Versions and License Information ... 155
Viewing Information About Available Updates ... 156
Choosing Your Support Options ... 157
Viewing Information About Your Product License ... 157
Licensing Schemes ... 157
License Style ... 158
Uploading a License File ... 158
TeamConnect Logs ... 159
Default Logs ... 159
Working with Logs ... 160
Viewing Logs ... 160
Things to Remember ... 161
Clearing Logs ... 162
Changing System Logging Levels ... 162
Turning Audit Loggers On or Off ... 164
TeamConnect Administrator Tools ... 165
Scheduled Actions Monitor ... 166
Accessing the Scheduled Actions Monitor ... 166
Tasks Available from the Scheduled Actions Monitor ... 167
Create a New Scheduled Action ... 167
Actions Against the Table ... 168
Deactivate Scheduled Actions ... 169
Activate Scheduled Actions ... 169
Delete Scheduled Actions ... 170
Run a Scheduled Action ... 170
Things to Remember ... 170
4 Authentication ... 170
Login URLs ... 170
NTLM Authentication Plug-in ... 171
NTLM Prerequisites ... 172
Configuring Internet Information Services ... 173
Disabling Anonymous Access ... 173

Editing the NTLM Configuration File ... 174
Installing the NTLM Configuration File ... 174
Enabling NTLM Authentication for TeamConnect Users ... 175
LDAP Authentication Plug-in ... 176
LDAP Authentication Prerequisites ... 176
Creating Custom LDAP Authentication Error Pages ... 177
Defining LDAP Parameters ... 177
Installing LDAP Plug-in Files ... 181
LDAP Authentication Sample Files ... 182
Sample Custom Log-in Page ... 182
Sample Custom Error Page ... 184
Sample Restore Session Page ... 184
Sample LDAP Configuration File ... 185
Custom Authentication Plug-ins ... 186
Customizing Message Screens ... 187
Enabling a Default Authentication Method ... 187
Overriding Authentication for Individual Users ... 187
5 Troubleshooting and Frequently Asked Questions ... 188
Frequently Asked Questions ... 189
Users and Groups ... 189
Address Books ... 191
Budgets ... 192
Admin Settings ... 192
Licensed Seats ... 192
Troubleshooting ... 192
6 Rights for End-users ... 194
System Record Rights ... 196
Account Rights ... 196
Basic Account Rights ... 196
Additional Account Rights ... 197
Appointment Rights ... 199
Basic Appointment Rights ... 199
Additional Appointment Rights ... 201
Contact and Address Book Rights ... 203
Basic Contact and Address Book Rights ... 203
Additional Contact Rights ... 205
Document Rights ... 208
Basic Document Rights ... 208
Additional Document Rights ... 209
Expense Rights ... 215
Basic Expense Rights ... 215
Additional Expense Rights ... 216
History Rights ... 218
Basic History Rights ... 218
Additional History Rights ... 219
Invoice Rights ... 221
Basic Invoice Rights ... 221
Additional Invoice Rights ... 222
Report Rights ... 226
Task Rights ... 227
Basic Task Rights ... 227
Additional Task Rights ... 228
TeamConnect Features and Areas ... 230
Preferences Rights ... 231

Release Edit Locks Right ... 231
Scheduled Actions Rights ... 231
Custom Record Rights ... 232
Project/Matter Rights ... 232
Basic Project/Matter Rights ... 232
Additional Project/Matter Rights ... 233
Project/Matter Involved Rights ... 236
Basic Involved Rights ... 237
Additional Involved Rights ... 238
Project/Matter Milestones Rights ... 240
Basic Project/Matter Milestone Rights ... 241
Additional Milestones Rights ... 241
7 Rights for Administrators ... 243
Rights for Group Records ... 243
Basic Group Rights ... 244
Additional Group Rights ... 244
Rights for User Records ... 245
Basic User Rights ... 246
Additional User Rights ... 246
Rights for Admin Settings and Logs ... 247
8 Rights for Solution Developers ... 248
Administer Custom Tools Rights ... 249
Global Navigation Toolbar Rights ... 250
Customize Home Pages Rights ... 250
Lookup Tables Rights ... 251
Custom Lookup Tables Rights ... 252
Multi-currency Lookup Table Rights ... 252
Miscellaneous Settings Rights ... 253
Object Definitions Rights ... 255
Customize Portal Panes Rights ... 263
Routes Rights ... 263
System Settings and Appenders Rights ... 265
9 Documents and Folders ... 266
Directory Structure ... 266
Top Level Folder ... 267
Attachments Folder ... 268
HTTPRoot Folder ... 268
System Folder ... 269
Users Folder ... 273
Automatically Created Folders ... 273
10 Glossary ... 275
Index 288

1 Enterprise Administrator Help

Welcome to the *TeamConnect® Enterprise Administrator Help*.

Groups	Users
Admin Settings	Logging
End-user Rights	Administrator Rights
Solution Developer Rights	Documents and Folders

1.1 Getting Started

This chapter provides an overview of common page elements and terminology that are unique to the TeamConnect Admin area. See Records for general descriptions of application pages.

1.1.1 Admin Area User Interface

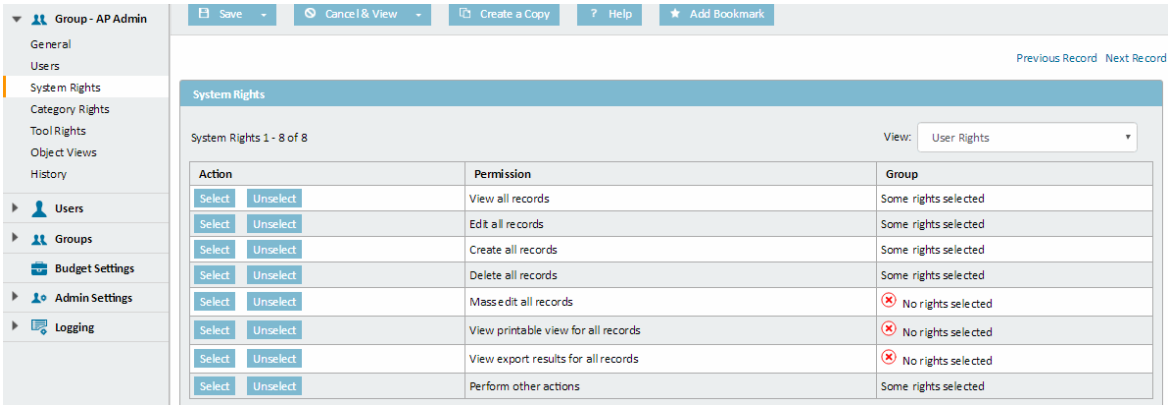
This section describes the common elements that are found on application pages under the **Admin** tab.

The Account Administration section includes descriptions of how to manage user and group accounts. From the **Admin** tab, open the Users list page by clicking the **Users** link, or open the Groups list page by clicking the **Groups** link.

The System Administration section includes descriptions of how to manage system settings and how to manage system and audit logs. From the **Admin** tab, open the Admin Settings **General** page by clicking the **Admin Settings** link. Open the Logging area by clicking the **Logging** link.

1.1.1.1 Group Rights Pages

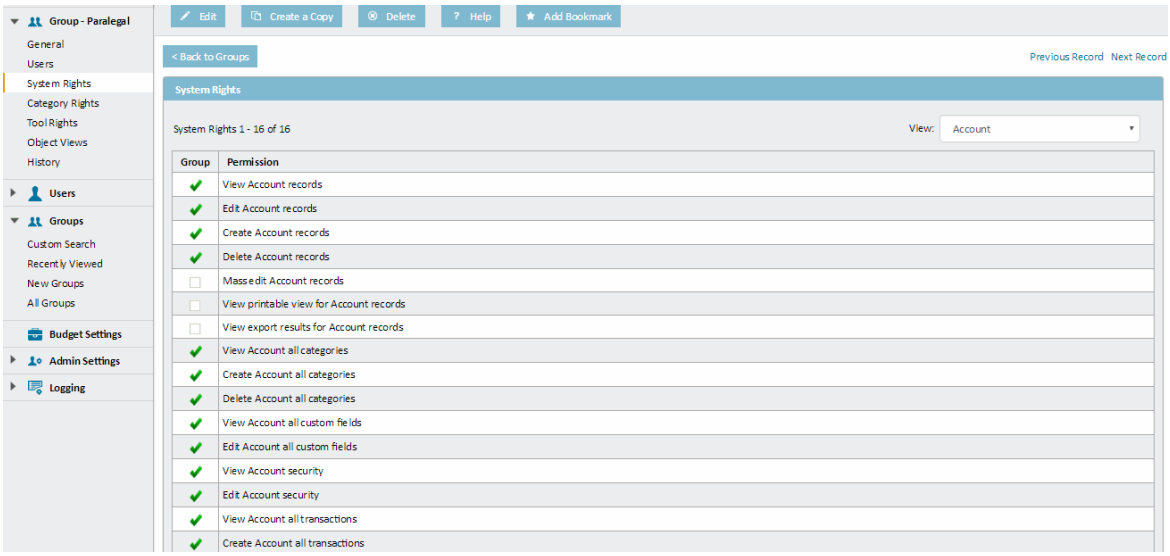
From a group record, the **System Rights** and **Category Rights** pages use a **View** drop-down list to filter the Permissions you will see on the page's body. Details on Group Rights functionality can be found on the Hierarchy Overview of Group Rights.



Group Record - System Rights Page, All User Rights View

For example, if you select the **User Rights** option from the **View** drop-down list, the resulting list of rights will apply globally to records and areas that are typically accessed by end users.

Otherwise, if you select Account from the View drop-down list, the Permission list will refresh with a list of rights specific to account records.

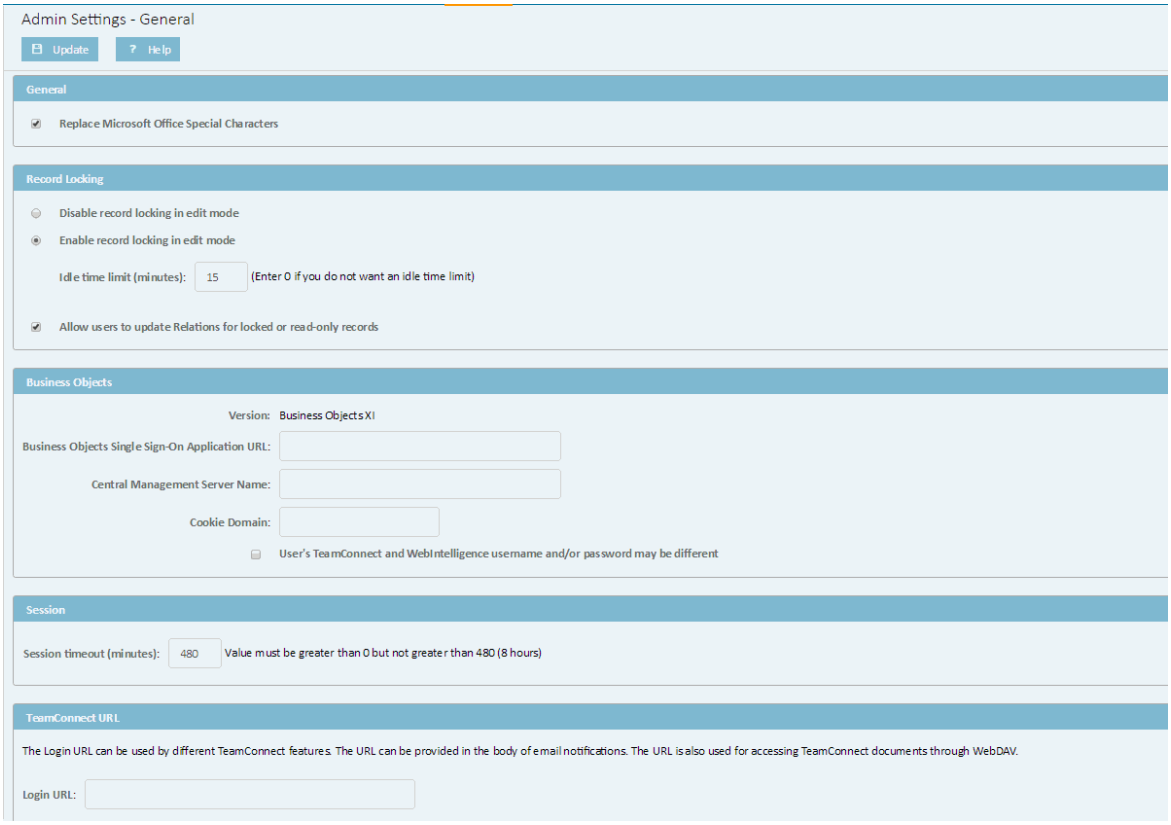


Group Record - System Rights Page for Accounts

For more information, see Understanding Rights and Assigning or Viewing Group System Rights.

1.1.1.2 Admin Settings General Page

From the **Admin** tab, **Admin Settings** link, you can configure certain system settings. There are multiple pages from the Admin Settings area that are labeled by function. For example, you can configure general settings, email-related settings, search results settings, etc. In addition, you can view the application version number (**About** page) and record notes about changes you make to Admin Settings (**History** page).



Admin Settings - General Page

1.1.1.3 Save Options

When working with user or group records, the **Save** button on the upper left area of the page has a drop-down option that allows selection among four save options. The default setting for this option can be determined by administrators as outlined in Setting up the User Interface.

If you click or hover over the drop-down arrow, as shown at the right, the following choices for saving will appear:

- **Save & Close** will save the record, then close the record's page and return you to the previous page you were working on.
- **Save** will save the record but leave the record in edit mode.
- **Save & View** will save the record, then present the record in view-only mode.
- **Save & New** will save the record, then open a new record.

If the label on the Save button is already the choice you want, simply click the button. If not, click the drop-down arrow on the right edge of the button and make your choice from the list that is shown there.

1.1.2 Terminology

Between TeamConnect 2.5 and the current TeamConnect version there has been significant redesign of the user's application look and feel. Accordingly, there have been changes to the terms used to refer to application pages and elements on each page. Although the user-facing application area and User Help use the TeamConnect 3.x terminology, there are some remaining TeamConnect 2.5 screen elements in the Designer application area and Customization Help. The Administration Help uses a combination of terminology.

The following table includes common terms used to reference pages or screens and the elements within. Please be aware that the terms may be used interchangeably.

Synonymous Terms in TeamConnect Guides

User Help Term	Customization Help Term
Page	**Screen or Tab**
Section	**Block**
Collection	**Search View, with criteria**
Record type	**Object**

1.2 Account Administration

This chapter describes how to plan and set up users and groups of users for TeamConnect. A major consideration for organizing groups is determining which rights should be assigned. This chapter is organized by concepts you should understand before you can start the tasks of creating and configuring users and groups.

Note: *Account administration in this chapter refers to setting up users and user groups. Account records related to finances are different.*

Support staff might use some procedures under the Users section. For example, Activating and Inactivating a User.

Before You Begin

The **TeamConnectAdmin** user account is provided for you. Log into TeamConnect as this user for initial system and accounts setup. The TeamConnectAdmin user can create and administer contacts, users, groups, and system settings. For example, create contacts and user accounts for yourself and the solution developer who is going to customize TeamConnect for your organization.

The TeamConnectAdmin user has predefined rights that cannot be changed. The associated contact records do not represent real people, and cannot be changed or deleted. You cannot delete the TeamConnectAdmin user account.

1.2.1 Planning and Best Practices

The following are recommendations for planning your accounts setup.

Many of the tasks below will have already been handled by your TeamConnect Certified Professional. For example, all tasks pertaining to assigning rights to groups are handled by the TeamConnect Certified Professional only. Your role as a System Administrator is to create user accounts and assign those users to the appropriate groups. You may also create new groups that have no rights, and use those groups as routes in workflows, such as the flow that approves invoices.

Information about assigning rights to groups is provided here to help you better understand the nature of security in TeamConnect.

Recommended Practice

You can choose different ways to set up group and user accounts. The following is suggested to save time.

1. Gather business requirements for different groups you need to support. For example, which rights or records access each group will require and which users belong to which group(s).
2. Plan group accounts.

   Organize each group's rights to records, categories/custom fields, and tools.
3. Create group accounts and assign rights to groups.
4. Create user accounts.
5. From each group account, add users to groups.

Information to Gather

Before assigning rights to a group of users, obtain answers to the following questions:

- Which record types should the group access?
- For each record type, decide the following:
  - Which access rights should be assigned?

    For example, view records, edit records, create records, or delete records.

    For a record type you'll usually also need to assign access rights to sections or pages that are associated with the record type. For example, view record security or edit record security.
  - Which categories should be accessible to the group? Which access rights should be assigned? For example, view record category, add record category, or remove record category.
  - Which custom fields should be available to the group? Which access rights should be assigned? For example, view category custom fields, or edit category custom fields.
- For TeamConnect features or areas, such as User Preferences, Admin Settings, Designer System Settings, object definitions, etc., decide on the following:

- Which access rights should be assigned? For example, view object definition records, edit object definition records, create object definition records, or delete object definition records.

  For a TeamConnect feature or area you may also need to assign access rights to sections or pages that are associated with the record type. For example, view object definition rules, edit object definition rules, create object definition rules, or delete object definition rules.

- Which tools should the group be able to use?

Before creating users, gather the following information:

- Basic information about your users. See Creating or Editing Users for additional details.
- Required authentication mechanisms

Tips

- If an individual requires custom rights, create a separate group, assign required rights, and add the user to that group.
- During group account planning, consider your users' job roles and organize group rights accordingly. For example, users that share job titles can be grouped with the same rights requirements.

1.2.2 Understanding Rights

There are three general ways to provide access to information and functionality in TeamConnect:

- Assigning rights
- Setting user type
- Assigning object views

This section includes conceptual information for understanding common traits of TeamConnect rights.

Using this Section

- Read Understanding Rights to get an overview of how rights work in TeamConnect. Review the examples provided to apply the concepts to scenarios you might use.
- Use specific procedures to navigate to application pages for assigning rights. For example:
  - Assigning or Viewing Group System Rights
  - Assigning Group Category and Custom Field Rights
  - Assigning Group Tool Rights
- Refer to the appendixes for detailed descriptions of available rights. For example:
  - Rights for End-users
  - Rights for Administrators
  - Rights for Solution Developers

- For more information, see Creating or Editing Users, Changing Group Default Object Views.

Types of Rights

Rights are used to assign access to view and work with:

- Records

  Categories, custom fields, custom blocks, forms

- TeamConnect features or areas
- Tools

Rights are also divided into three groups:

- **Rights for End-users**—Majority of these rights affect viewing and working with records, categories, and custom fields. This group also includes rights to areas, such as Preferences.
- **Rights for Administrators**—These rights affect viewing and working with user and group accounts, the Admin Settings area, and logs.
- **Rights for Solution Developers**—These rights affect customizing and managing Custom Tools, Global Navigation toolbar, Home Pages, Lookup Tables, Miscellaneous Settings, Object Definitions, Portal Panes, Routes, and viewing and working with System Settings (from the Designer area of the application).

1.2.2.1 Rights for End-Users

The rights grouped under the User Rights list view (from a user record's **System Rights** page) refer to rights that are expected to be assigned to a group of end-users.

- Records:
  - Account
  - Appointment
  - Contact
  - Document
  - Expense
  - History
  - Invoice
  - Task
  - Project
- Categories, custom fields, custom blocks, or forms for the record types listed above
- TeamConnect features or areas:
  - User Preferences
  - Scheduled Actions

- Tools (for more information, see Assigning Group Tool Rights)

Note: *Users can also set access rights for individual records.*

TeamConnect Legal Matter Management Records

- Advice & Counsel
- Cost Center
- Dispute
- Transaction

1.2.2.2 Rights for Administrators

- Records:
  - Groups
  - Users
- TeamConnect features or areas:
  - **Admin Settings**—System settings that are available from the **Admin** tab.
  - **Logs**—The Logging area includes system loggers, system appenders, audit loggers, and audit appenders.

1.2.2.3 Rights for Solution Developers

When assigning rights to a group of solution developers, you will typically assign rights to view or work with TeamConnect features or areas:

- **Administer Custom Tools**—Allows management of custom tools.
- **Global Navigation**—Allows customization of the global navigation toolbar and links that display under the toolbar.
- **Home Pages**—Allows management and customization of home pages in TeamConnect after logging in.
- **Lookup Tables**—Allows management and customization of system lookup tables, custom lookup tables, and multi-currency lookup tables in TeamConnect.
- **Miscellaneous Settings**—Allows management of custom fields that should be considered part of a user's system preferences. Custom fields added to the Designer application, **Miscellaneous Settings** page correspond to fields that display on a user's **Preferences** area, **Other Settings** page. Also includes rights to override record edit locks and to override system search results limits.
- **Object Definitions**—Allows management of system and custom object definitions (record types).
- **Portal Panes**—Allows management and customization of applets that are available for user home pages. Portal Panes can be information-driven, for example, containing TeamConnect

search views or RSS feeds. In addition, Portal Panes can be functionality-driven, for example, containing links to frequently used areas, such as workflow approval or record creation wizards.

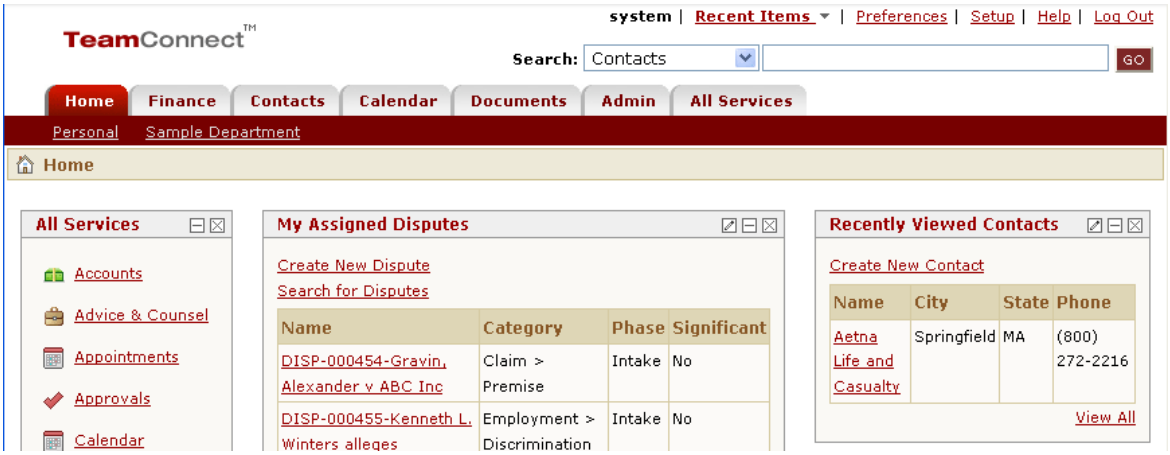
- **Routes**—Allows management and customization of the part of a workflow approval rule where approvers, reviewers, process managers, and email notifications are defined.
- **System Settings**—From the Designer application, these are TeamConnect system settings that apply to all users, including Rule Execution, Default Object Views, Authentication Plug-In (default and custom plug-ins), and Clear Cache Properties. These rights also allow access to manage system appenders and audit appenders.

Access Rights to TeamConnect Designer

If you assign any of the following rights to a group (from a group record's **System Rights** page), its members will be able to access the Designer area of TeamConnect by clicking a **Setup** link from the upper right corner of TeamConnect:

- Any rights resulting from the Setup Rights view.
- Any rights resulting from the Administer Custom Tools view.
- Any rights resulting from the Global Navigation view.
- Any rights resulting from the Home Pages view.
- Any rights resulting from the Lookup Tables view.
- Any rights resulting from the Custom Lookup Tables view.
- Any rights resulting from the Multi-Currency view.
- Any rights resulting from the Miscellaneous Settings view.
- Any rights resulting from the Object Definitions view.
- Any rights resulting from the Portal Panes view.
- Any rights resulting from the Routes view.
- Any rights resulting from the Global Navigation view.
- Any rights resulting from the System Settings view (under the Setup rights list).

A second browser window will open with the Designer area of the application. The initial browser for the User area of the application will remain open.



Home Page with Setup Link to Designer Application Area

Rights related to Solution Developers are described in the appendix, Rights for Solution Developers.

Tips

- If a user is a member of multiple groups, the rights that the user inherits are cumulative. The user inherits all rights assigned to all groups.
- Categories only apply to rights for record types that end-users work with, but not to rights for administrators. For example, when assigning rights to work with user records, you do not need to assign rights to associated categories.
- There are additional rights dependencies that may result in users not able to view expected data. Such data may display as "SECURED". See each record type's rights in the appendix, Rights for End-users, for more information.
    - For example, if you do not give the user or group at least the Read right to Contact, the user or group is unable to add or see appointment attendees, vendors in invoices, contacts associated with tasks and expenses, task and project assignees, and so on, even if the group or user has all the appropriate rights to Appointment, Task, Invoice, and project records.
    - Similarly, if you do not give at least the Read right to a custom object, the user or group is unable to see or select the records of this custom object as parents in other custom object records, as posting criteria in accounts, or see custom fields of type Custom Object with this object, and so on.
- Pre-population rules do not check the current user's rights when they trigger the creation or update of object records. For example, a user without rights to create an account could create a project and automatically trigger a pre-population rule that creates an associated account. You should test and review your templates and pre-population rules to make sure that they comply with your organization's security policies.

1.2.2.4 Rights for System Record Types

This section describes commonalities among rights to view and work with system record types (records that are provided standard with TeamConnect).

From a group's **System Rights** page, if you select a record type from the **View** drop-down list, the page will be updated with a list of rights for that record type.

Each record type's rights can be broken down into two groups:

- Basic rights—Include the minimal rights required to view or work with a group of records. These rights include:
  - **View records**—Allows searching, viewing, and printing records.

    Allows access to the list page for a record type, advanced search page for a record type. Allows access to **General** and **Workflow** pages for contact records.

    For example, if you assign the **View Contact Records** right to a group, group members can view the **Contact List** page, **Advanced Contact Search** page. In addition, group members can open contact records and view the records' **General** and **Workflow** pages. For example, see Example for Assigning Rights to View Contacts.
  - **Edit records**—Allows editing, searching, viewing, and printing records.

    Allows access to the list page for a record type, advanced search page for a record type. Allows access to **General** and **Workflow** pages for expense records. For example, see Example for Assigning Rights to Edit Contacts.
  - **Create records**—Allows creating and printing records.

    Allows access to the list page for a record type, advanced search page for a record type. Allows access to **General** and **Workflow** pages for expense records. For example, see Example for Assigning Rights to Create Contacts.
  - **Delete records**—Allows deleting, searching, viewing, and printing records.

    Allows access to the list page for a record type, advanced search page for a record type. Allows access to **General** and **Workflow** pages for expense records. For example, see Example for Assigning Rights to Delete Contacts.

    For Edit, Create, and Delete record rights, a group must also have View record rights. The corresponding ability to search, view, and print records results.
- Additional rights—Allow access to view or work with additional pages that belong to the record type, for example, the **Security** page. These rights typically vary per record type. In addition, these rights require that the View records and/or Edit records rights for the record type have also been assigned.

  For example, if the **Expense Post** right is assigned to a group, group members can post expenses. This right applies to certain record types but not all.

Note: *There may be exceptions for each record type's rights to* ***General*** *pages or other page. Refer to the appendix, Rights for End-users, for details.*

Records Linked From Other Records

Certain records, such as Documents and Histories, appear as pages that belong globally to other records. For example, if a group has rights to work with Documents, then from any system object record (Contact, Expense, Account, Appointment, etc.), a group member will see a page link for **Documents** associated with that record.

Certain records appear as pages that belong to specific other records. For example, the following list displays records that appear as page links for other records:

- **Document**—If rights are assigned for Document records, a **Documents** page link will be available from all system object records.
- **History**—If rights are assigned for History records, a **History** page link will be available from all system object records.
- **Account**—If rights are assigned for Account records, an **Accounts** page link will be available from Project (custom object) records.
- **Expense**—If rights are assigned for Expense records, an **Expenses** page link will be available from Project (custom object) records.
- **Task**—If rights are assigned for Task records, a **Tasks** page link will be available from Project (custom object) records.
- **Attendee**—If rights are assigned for User, Groups, or Contact records, an **Attendees** page link will be available from Appointment records.
- **Appointment**—If rights are assigned for Appointment records, an **Appointments** page link will be available from Project (custom object) records.

Tips and Warnings

- Administrator rights, such as rights to view or work with User Accounts, are assigned at the record type level but do not have associated categories and custom fields.
- Assigning rights to the Documents record type affects user access to the Documents sub-page of all records. Also note that assigning the **Create Document records** right (to upload documents to a record) requires assigning the **View Document records** right. For additional information on operations that are available with the Create Document records right, see Document Rights.
- If rights are assigned for a group, including Create and Edit record rights, it is likely that Create, Edit, and Delete rights to sub-pages and sections that are part of that record type will also be assigned.
- Certain records, such as invoices, tasks, and expenses, require additional operations such as:
  - Post
  - Void
  - Assign Task
- You can also set rights for individual records.

1.2.2.4.1 Prerequisites for Rights to System Record Types

There are commonly repeating prerequisites to assigning rights. Descriptions follow for basic record rights and well as rights to sections or pages associated with a record type.

Requirements for Basic Record Rights

The following list describes the dependencies between basic rights for records. Rights like **View Contact records** and **Create Contact records** do not have any prerequisite rights.

- **View records**—No additional rights required.
- **Edit records**—Requires **View records**.

  For example, if **Edit Contact records** rights are assigned, **View Contact records** rights must also be assigned.
- **Create records**—Requires **View records**.
- **Delete records**—Requires **View records**.

  For example, if **Delete Contact records** rights are assigned, **View Contact records** rights must also be assigned.

Requirements for Additional Rights to Records

The following list describes the dependencies between rights for additional record pages, such as the **Security** page. Generally rights for additional record pages require the corresponding View record right. For example, to assign **View Expense Security**, **View Expense records** must also be assigned.

- **View** *Record section/page*—Requires the corresponding View records right.

  For example, if **View Contact security** rights are assigned, **View Contact records** rights must also be assigned.
- **Edit** *Record section/page*—Requires the corresponding View records right, Edit records right, and View Record section/page right.

  For example, if **Edit Contact security** rights are assigned, **View Contact records**, **Edit Contact records**, and **View Contact security** rights must also be assigned..
- **Create** *Record section/page*—Requires the corresponding View records right, Edit records right, and View Record section/page right.
- **Delete** *Record section/page*—Requires the corresponding View records right, Edit records right, and View Record section/page right.

1.2.2.4.2 Rights Impacts on Related Records

For system record types, user access to certain record pages (such as Documents, History) depends on rights set at the Document record rights and History record rights level.

For custom objects (projects/matters), user access to record pages (such as Involved) depend on rights set within the custom object record rights.

1.2.2.5 Rights for Categories and Custom Fields

Generally rights are assigned to a category as a prerequisite to assigning rights to its associated custom fields, sections, and forms. Access to categories and custom fields also require access to the related record type. Users looking to set or configure Group Rights should view the following pages for further detail: Hierarchy Overview of Group Rights, Assigning Group Category and Custom Field Rights, Example for Assigning Rights to Contact Categories and Fields.

Types of Category Rights

By default, each record type has two categories, the base category and a Default category. Typically, a TeamConnect Certified Professional will add additional categories for your company. These custom categories will have corresponding rights.

Each category for a record type has the corresponding rights:

View Category

- For the base category, allows viewing the Categories page or section of the record.
- For the Default category or custom categories, allows viewing the selected category from the **Categories** page or section.

Add Category—Allows adding the category for the record.

For tasks, expenses: allows selecting a default category. This requires both add and remove rights.

Remove Category—Allows Removing the category for the record.

For tasks, expenses—allows changing a default category. This requires both add and remove rights.

View All Custom Fields

Allows user complete view rights for all subfields on the category. If this is not checked, users will not be able to add **Edit All Custom Fields,** as View rights are a precursor to editing.

Edit All Custom Fields

Allows user complete edit rights for all subfields on the category.

Individual Fields

For example, for contacts, the corresponding base category rights are View Contact category, Add Contact category, and Remove Contact category.

If a custom category, Contractor, were added for contacts, the corresponding category rights would be: View Contractor category, Add Contractor category, and Remove Contractor category. See Example for Assigning All Rights to Contacts Pages and Fields and Example for Assigning Rights to Contact Categories and Fields for examples on assigning rights to categories and custom fields.

Tips

- For accounts, contacts, invoices, projects, appointments, documents, involved's, and histories—the base View Category right allows viewing the selected category from the **Categories** page or section.

- For tasks, expenses—the base View Category right allows viewing the selected category from the Category drop-down list on the **General** page.
- The list of categories in the **Categories** drop-down list in the **Categories** block displays only those categories to which the user has the Create rights.

Types of Custom Field Rights

Each custom field that is associated with a record type's category has the corresponding right:

- View Custom Field—Allows viewing the custom field, form, or section.
- Edit Custom Field—Allows entering, changing, deleting field values in the custom field, form, or section.

For example, for expenses, the corresponding base category's custom field rights are View Contact custom fields and Edit Contact custom fields.

If a custom category, Contractor, was added for contacts, and a custom field, Private Investigator, was added, then the corresponding custom field rights could be: View Contractor custom fields and Edit Contractor custom fields.

Differences in Category Functionality

There are several groups of objects that have different functionality on their record screens in the user interface. These groups of objects are:

- **Account**, **Contact**, **Invoice**, **Project** (custom object)—Record screens of these objects have a **Categories** system block where the user, depending on his or her rights, can work with the appropriate categories.

  In the **Categories** drop-down list of the **Categories** block, the user can see all categories for which he or she has Create rights; these are the categories that the user can add. Below the data entry fields, the user can see all the existing categories that are added to each record. Depending on his or her rights, the user might be able to delete these categories.

- **Task** and **Expense**—Record screens of these objects do not have a separate **Categories** block. Instead, they have a **Default Category** field in the **General** block where the user, depending on his or her rights, can work with the appropriate categories.

  By selecting a category in this field, the user does the following:

  a. Adds this category to the record.

  b. Deletes the previously selected category.

  Important: *If users lack Delete rights for a category, they cannot select a new one--even if they have Create rights for the category.*

- **Appointment**, **Document**, **History**, and **Involved**—The record screens of these four objects do have a separate **Categories** block like most system objects. Yet they also have the **Default Category** field in the General block, which results in the following functionality:

  - Depending on their rights, users can add the appropriate category and set it as the default by selecting it in the **Default Category** field.

- However, by selecting a new default category, the user does not delete the previous default category from the record. It can be deleted only by using the **Categories** block.

Tips

- Rights for adding categories allow users to select or activate a category for the specified record type. Generally the active categories act like filters to provide or restrict access to related custom fields. Categories are created by solution developers with the exception of the primary and default categories, which are provided for every record type.
- Rights for removing categories allow users the ability to deactivate a category for the specified record type. Afterward, the result for the user is that any related custom fields for that category will be hidden from the **Details** page or **Details** section. Categories can only be deleted from the system by solution developers.
- Solution Developer Rights to work with Categories and Custom Fields only apply to rights for records (except users and group).

1.2.2.5.1 Prerequisites for Rights to All Categories and Custom Fields

There are commonly repeating prerequisites to assigning rights. Descriptions follow for rights to all categories and well as rights to custom fields for a record type.

Requirements for Rights to All Categories

The following table describes the dependencies between rights to access all categories for a record type.

Dependencies for Rights to all Categories for a Record Type

Rights	Also Requires ___ Right	Example
View Record all categories	**View** *Records*	For example, if the **View Contact all categories** right is assigned, the **View Contact Records** right must also be assigned.
Add Record all categories	**View** *Records* **Edit** *Records* **View** *Record* **all categories**	For example, if the **Create Contact all categories** right is assigned, the following must also be assigned: • **View Contact Records** right • **Edit Contact Records** right • **View Contact all categories** right
Remove Record all categories	**View** *Records* **Edit** *Records* **View** *Record* **all categories**	

Requirements for Rights to All Custom Fields

The following table describes the dependencies between rights to access all custom fields for a record type.

Dependencies for Rights to all Custom Fields for a Record Type

Rights	Also Requires ___ Right	Example
View Record all custom fields	**View** *Records* **View** *Record* **all categories**	For example, if the **View Contact all custom fields** right is assigned, the following must also be assigned: • **View Contact Records** right • **View Contact all categories** right
Edit Record all categories	**View** *Records* **Edit** *Records* **View** *Record* **all categories**	

1.2.2.5.2 Prerequisites for Rights to Single Categories and Custom Fields

There are commonly repeating prerequisites to assigning rights. Descriptions follow for basic record rights and well as rights to sections or pages associated with a record type.

Requirements for Rights to Individual Categories and Custom Fields

The following generally apply to all record types that are standard with TeamConnect:

- When assigning view or edit rights to a custom field, the corresponding rights to the related category are also required.
- Update rights to custom field requires view rights to custom field and view rights to related category.

The following table describes the dependencies between rights to access an individual category for Account, Contact, Invoice, Project (custom object).

Dependencies for Rights to a Category for a Record Type

Rights	Also Requires ___ Right	Example
View Record category	**View** *Records*	For example, if the **View Contact Employee category** right is assigned, the **View Contact Records** right must also be assigned.

Add Record category	**View** *Records* **Edit** *Records* **View** *Record category*	For example, if the **Create Contact Employee category** right is assigned, the following must also be assigned: • **View Contact Records** right • **Edit Contact Records** right • **View Contact Employee category** right
Remove Record category	**View** *Records* **Edit** *Records* **View** *Record category*	

The following table describes the dependencies between rights to access a custom field for a record type.

Dependencies for Rights to a Custom Field for a Record Type

Rights	Also Requires ___ Right	Example
View Record custom field	**View** *Records* **View** *Record category*	For example, if the **View Contact Full-time custom field** right is assigned (associated with the **Employee** category), the following must also be assigned: • **View Contact Records** right • **View Contact Employee category** right
Edit Record custom field	**View** *Records* **Edit** *Records* **View** *Record category*	

Categories can be created with parent-child hierarchies.

The following table describes the dependencies between rights for categories with parent-child relationships for a record type. For the example column, assume that categories have been added to the Contact object definition.

Dependencies for Rights to Categories with parent-child relationships for a Record Type

Rights	Also Requires ___ Right	Example

View Record category (child)	**View** *Records* **View** *Record category* (parent) **Add** *Record category* (parent) **Remove** *Record category* (parent)	For example, if the **View Contact all categories** right is assigned, the **View Contact Records** right must also be assigned.
Add Record category (child)	**View** *Records* **Edit** *Records* **View** *Record category* (child) **View** *Record category* (parent) **Add** *Record category* (parent) **Remove** *Record category* (parent)	For example, assume that a solution developer has created a parent category, External, for Contacts. Also assume that a child category, External Court, was created for Contacts. Assigning the **Add External > Court category** right requires assigning the **View External > Court category**, **Add External category**, and **View External category** rights.
Remove Record category (child)	**View** *Records* **Edit** *Records* **View** *Record category* (child) **View** *Record category* (parent) **Add** *Record category* (parent) **Remove** *Record category* (parent)	

1.2.2.6 Rights for Custom Record Types

Individual records of custom objects are collectively called Projects in the standard TeamConnect documentation. Depending on the number of custom objects defined for your organization, there are several sets of these rights, each group listed under the object's name in the **View** drop-down list on the **Rights** and **Category Rights** pages in user and group accounts, for example Claim, Policy, and Matter. Every time a new custom object, and embedded custom object, is created, a new set of rights are automatically added to the list.

Each set of rights for custom object records includes the following object-level and category-level rights:

- To the custom object itself—Refer to Project/Matter Rights.
- To the custom object's Involved object—Refer to Project/Matter Involved Rights.

Note: *Even though embedded objects can be accessed only from within custom objects, all rights to them must be set separately like to a regular custom object.*

1.2.2.7 Rights for TeamConnect Features or Areas

TeamConnect areas include Admin Settings and System Settings. Rights to areas generally include view rights to the related pages and edit rights to change values from related pages. The table below provides a summary of rights to TeamConnect areas that can be assigned and the resulting user features.

Rights to TeamConnect Areas

Rights	Related Functionality
View	Viewing related pages
Edit	Entering, changing, or deleting values from related pages

For example, if the **View Admin Settings records** right is assigned to a group, group members can view the **Admin Settings** pages and configured values. In addition, group members can view the **Logging** pages for system logs and audit logs.

For example, if the **Edit Admin Settings records** right is assigned, group members can edit the **Admin Settings** pages. In addition, group members can edit system logger levels, clear system and audit logs.

1.2.3 Groups

Group accounts are used to organize users who need similar security rights. In this version of TeamConnect, rights are configured for groups and not for users.

Group Record Pages

There are six group-specific pages:

- The **General** page lets you enter information about the group, such as Description and ID.
- The **Users** page lets you add users to a group or remove users from a group.
- The **System Rights** page lets you view rights to work with records, application areas, and application features
- The **Category Rights** page lets you view rights to categories and custom fields by record type.
- The **Tool Rights** page lets you view rights to system tools and custom tools.
- The **Object Views** page lets you view the default object views for a group.

Additional pages associated with a group include:

- The **History** page lets you add notes about changes to the group or review previous history notes.

Collaborati Spend Management (CSM) Default Group

CSM comes with a default CSM Admin group:

User group	Rights
CSM Admin	Members of the **CSM Admin** group have no Admin (access to the Admin tab), User, category, or Setup (access to the Designer area) rights. They have rights only to the following: • **CSM Settings** object and its embedded objects • **Activity Code Authorization** object • **Expense Code Authorization** object • **Invoice Payment** object • **Payment Field Mapping** object • **Synchronization History** object • **Task Code Authorization** object • **Timekeeper** object • **Vendor** object and its embedded objects • **Vendor Timekeeper Classification Contact Mgmt** object • **Invoice Validation Rule Setting** tool • **Xml Worksheet** tool

TeamConnect Legal Matter Management Default Groups

Matter Management comes with five user groups with the following sets of pre-configured rights based on their job responsibilities within a legal department:

User group	Rights
Dispute Attorney	Members of the **Dispute Attorney** group have no Admin rights (access to the Admin tab) or Setup rights (access to the Designer area). They have rights only to the following: • All User Rights ***Caution:*** *"All User Rights" includes the Account object.* • **Dispute** object, and its embedded objects

	• **Advice & Counsel** object • **Cost Center** object and its embedded object • Category rights to some Line Item categories • **Time Entry Tool** tool ***Note:*** *The contact's default* ***Category*** *needs to be set to Internal (or the current Time Entry Setting,* ***General*** *tab,* ***Timekeeper Category*** *value).*
Legal Administrator	Members of the **Legal Administrator** group have no Admin rights (access to the Admin tab) or Setup rights (access to the Designer area). They have rights only to the Dispute object, its related and embedded objects, and to the following: • **All User Rights** ***Caution****: "All User Rights" includes the Account object.* • **Advice & Counsel** object • **Cost Center** object and its embedded object • **Dispute** object and its embedded objects • **Time Entry Setting** object and its embedded objects • **Time Period** object • **Transaction** object and its embedded objects • Category rights to some Line Item categories • **DeleteAllRecords** tool • **Import Design** tool • **Legal Preferences** tool • **Reassign Work** tool • **Time Entry Tool** tool ***Note:*** *The contact's default Category needs to be set to Internal (or the current Time Entry Setting, General tab, Timekeeper Category value).* • **Xml Worksheet** tool
Paralegal	Members of the **Paralegal** group have no Admin rights (access to the Admin tab) or Setup rights (access to the Designer area). They have rights only to the following:

	• **All User Rights** ***Caution:*** *"All User Rights" includes the Account object.* • **Dispute** object and its embedded objects • **Advice & Counsel** object • **Cost Center** object and its embedded object • **Transaction** object, and its embedded objects • Category rights to some Line Item categories • **Time Entry Tool** tool ***Note:*** *The contact's default* ***Category*** *needs to be set to Internal (or the current Time Entry Setting,* ***General*** *tab,* ***Timekeeper Category*** *value).*
Reporting	Members of this group can view the **Reports** home page. This user group has no Admin, User, Category, Tool, or Setup rights.
Transaction Attorney	Members of the **Transaction Attorney** group have no Admin rights (access to the Admin tab) or Setup rights (access to the Designer area). They have rights only to the following: • **All User Rights** ***Caution:*** *"All User Rights" includes the Account object.* • **Advice & Counsel** object • **Cost Center** object and its embedded object • **Transaction** object, and its embedded objects • Category rights to some Line Item categories • **Time Entry Tool** tool ***Note:*** *The contact's default* ***Category*** *needs to be set to Internal (or the current Time Entry Setting,* ***General*** *tab,* ***Timekeeper Category*** *value).*

For more information about configuring group accounts, see Creating or Editing Groups.

Because users should not alter TeamConnect's automated financial accounts, you should restrict user access to the Account object. Many rules and wizards depend on the standard configuration.

1.2.3.1 Working with Groups

You can perform the following tasks when you are working with groups.

Groups List

- Searching for Groups—Search for a group to view or edit.
- Viewing Groups—View a list of groups or open an individual group.
- Creating or Editing Groups—Add or update a group.
- Deleting a Group—Delete a group.

Group General Page

- Creating or Editing Groups—Add or update a group.

Group Users Page

- Changing Group Members—Add users to a group or remove users from a group.

Group System Rights Page

- Assigning or Viewing Group System Rights—Assign or view rights to work with records, application areas, and application features.

Group Category Rights Page

- Assigning Group Category and Custom Field Rights—Assign category and custom field rights to a group.

Group Tool Rights Page

- Assigning Group Tool Rights—Assign rights to work with system and custom tools.

Group Object Views Page

- Changing Group Default Object Views—Set a group's default object views.

Group History Page

- Viewing or Creating Group History—Create or view notes about changes to a group.

1.2.3.2 Searching for Groups

You can search groups using the Advanced Group Search page. Search using multiple field values as criteria. For example, you can search for expenses by Name, Description, and creation date.

To perform an advanced search for a group

1. Select the **Admin** tab.
2. Click the **Groups** link under the tab bar.
3. Click the **Advanced Search** link.
4. (optional) To search for a group within a specific collection, in the **Search Within** drop-down list, select the collection name.
5. (optional) To limit the fields used to search, in the **Filter** drop-down list, select an appropriate option.
6. Enter search criteria in the resulting fields. See Group General Page for descriptions of search criteria fields.
7. Click **Search**.
8. To open a group account, from the right pane, click a group name link.

1.2.3.3 Viewing Groups

You can view groups by browsing group collections. Alternatively, you can search for a group.

To view groups

1. Click the **Admin** tab.
2. Click the **Groups** link under the tab bar.
3. (optional) From the left navigation pane, click a Group collection link. For example, **Recently Viewed**, **New Groups**, or **All Groups**.
4. To open a group, from the right pane, click a group name link.

1.2.3.4 Creating or Editing Groups

Before creating a group, it is recommended to search existing groups to make sure you will not create a duplicate.

Each group of users requires:

- Configuration of rights for record types
- Configuration of rights for categories and related custom fields
- Configuration of rights for tools
- Addition of group members

The following steps describe the general results from assigning rights but each record type might have specific exceptions or rights dependencies. See Rights for End-users, Rights for Administrators, and Rights for Solution Developers for more information.

Tip: *You can create a group by making a copy of an existing group and updating its properties, such as Name, members, and rights. See Creating a Group Using a Template.*

To create or edit a group account

1. Select the **Admin** tab.
2. Click the **Groups** link under the tab bar.
3. Select one of the following options:
   - To create a group, click **New**.
   - To edit a group, click the **Edit Record** icon to the left of a group.
4. From the **General** page, complete the following fields:
   - (required) **Group Name**—-Enter the name of this group. Maximum length: 50 characters.
   - (required) **Unique Name**—Enter a unique name to identify this group. Enter letters and numbers in default English only.
   - (optional) **Description**—Enter a description of this group. Maximum length: 250 characters.
5. To set up record rights, click **System Rights** from the left navigation pane.

   For more information, see Assigning or Viewing Group System Rights, Rights for End-users, Rights for Administrators, and Rights for Solution Developers.

   For an overview on rights, see Understanding Rights.
6. To set up rights for categories and custom fields, click **Category Rights** from the left navigation pane.

   For more information, see Assigning Group Category and Custom Field Rights.

   For an overview on rights, see Understanding Rights.
7. To enable tools, click **Tool Rights** from the left navigation pane.

   Check the tools to enable.

   For more information, see Assigning Group Tool Rights.
8. To add users to the group, click **Users** from the left navigation pane. Do the following for each user to add:
   - Click **Add New** Item.
   - From the **Users** drop-down list, select a user to add to the group.

     Set a user's primary group from the user's account.

     For more information, see Changing Group Members.
9. Click a save option.

1.2.3.4.1 Creating a Group Using a Template

You can use an existing group like a template. You can create a copy of a group and then edit some fields to create a new group.

Field values from the following original group's pages are copied to the new record:

- **General** page
- **Users** page
- **System Rights** page
- **Category Rights** page
- **Tool Rights** page

To create a group using a template

1. Search for a group to copy and open it.
2. Click **Create a Copy**.
3. Edit the group as required. For example, change the **Group Name**.
4. Click a save option.

Field values from the original group's **History** page are not copied to the new group.

1.2.3.5 Changing Group Members

From a group's **Users** page, you can add or remove users from a group. Afterward, the group members will inherit any additional rights assigned to the group.

To change members of a group

1. Search for a group and open it.
2. Click **Edit**.
3. From the left navigation pane, click **Users**.
4. To add a user to the group:
   a. Click **Add New Item**.
   b. From the **Users** drop-down list, select a user to add to the group.

      Set a user's primary group from the user's account.
5. To remove a user from the group:
   a. Select the check-box to the left of the user to remove membership.
   b. Click **Remove**.
6. Click a save option.

1.2.3.6 Assigning or Viewing Group System Rights

From a group's **System Rights** page, you can assign or view rights to work with records, application areas, and application features.

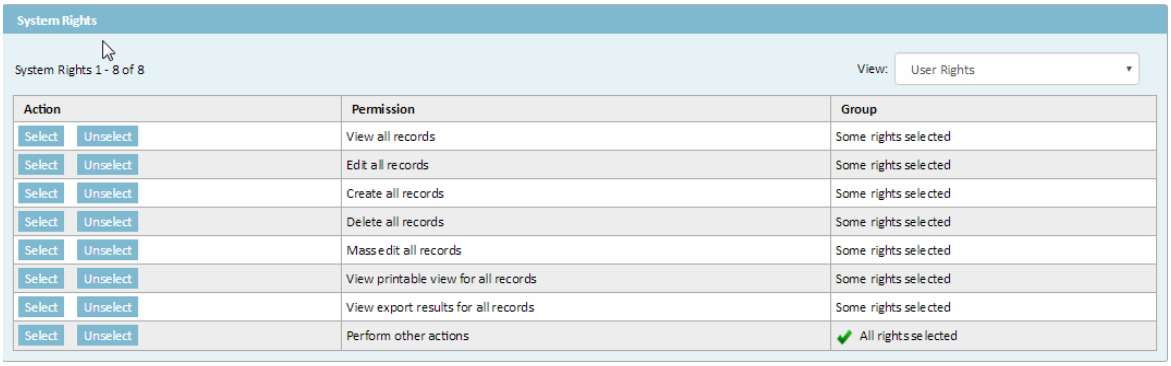
You can assign or view rights that apply:

- Globally—If you expect to enable rights across multiple record types or multiple application areas, work with these types of rights to save time. Global rights are organized into three groups: User rights, Admin rights, and Setup rights.

  For example, if you select the **View** drop-down list, **User Rights** option then the resulting page you can assign rights to view all contact records, view all document records, view all project records, etc., with one button click.

- Individually—If you expect to enable rights for a limited number of record types (for example, allow restricted access to a couple record types), work with these types of rights.

  For example, if you select the **View** drop-down list, **Contacts** option then from the resulting page you can assign more granular level rights such as View Contact records, Edit Contact records, Create Contact records.



Sample Screen for Assigning Contact (Individual) Record Rights to a Group

Additional information about groups:

- New groups do not have any rights (record rights, category or custom fields rights, or tool rights) assigned by default.
- Rights are cumulative. If a user is a member of multiple groups then the user inherits all rights assigned to all groups.
- If you assign global rights to a group and later add a custom object (record type), category, or custom fields, it is recommended to manually grant access rights to the new object, category, or custom fields.

To assign or view individual record rights

1. Search for a group and open it.
2. To change record rights, from the left navigation pane, click **System Rights**.

   From the **View** drop-down list, select a record type (for example, Contacts).

   - To assign a specific record or area right, select the check-box for the permission under the **Group** column.

- To unassign a specific record or area right, clear the check-box for the permission under the **Group** column.

3. Click a save option.

Group System Rights Page Field Descriptions

Field descriptions for specific records or areas are described in:

- Rights for End-users
- Rights for Administrators
- Rights for Solution Developers

Group System Rights Page Fields

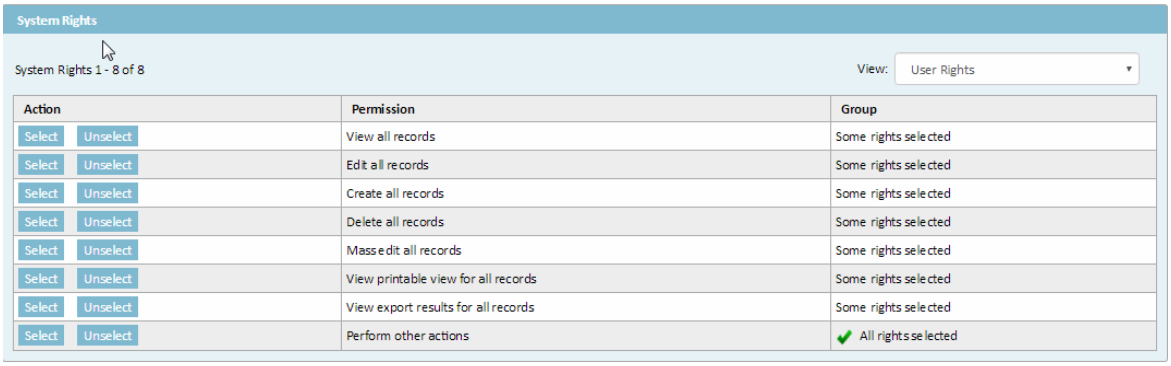
Label	Description
View drop-down list	A list of record types and application areas to which you can assign access rights, for example, system settings, object definitions, etc. After selecting a list option, the workspace is updated with a list of rights specific to that option. For example, if you select Contacts, the rights list displays only rights for working with contact records.
Action	(Available only in Edit view when a global rights option is selected from the **View** menu, such as **User Rights**, **Admin Rights**, or **Setup Rights**) Displays both of the following per permission: • **Select**—Enables all permissions for all child records under this rights group. • **Unselect**—Disables all permissions for all child records under this rights group.
Permission	The available Permissions list items depends on the type of option selected from the **View** drop-down list. • If a global rights option is selected from the **View** drop-down list (for example, **User Rights**, **Admin Rights**, **Setup Rights**), permissions include the following: **View all record types**—To grant search and read rights for records of this type, select the **View all record types** check-box. **Edit all record types**—To grant rights to edit records of this type, select the **Edit all record types** check-box. **Create all record types**—To grant rights to create records of this type, select the **Create all record types** check-box.

	Delete all record types—To grant rights to delete records of this type, select the **Delete all record types** check-box. **Perform all other actions** ***Note:*** *See Understanding Rights, Rights for End-users, Rights for Administrators, and Rights for Solution Developers.* • If an individual rights option is selected from the **View** drop-down list (for example, Contacts, Documents, etc.), permissions like the following are available: View *Contact* records Edit *Contact* records Create *Contact* records Delete *Contact* records View *Contact* all categories Create *Contact* all categories Delete *Contact* all categories View *Contact* all custom fields Edit *Contact* all custom fields ***Note:*** *The list above provides examples of permissions related to individual record types but is not all-inclusive.*
Group	(Available only when a global rights option is selected from the **View** menu, such as **User Rights**, **Admin Rights**, or **Setup Rights**) Displays one of the following per permission: • **All rights selected**—Indicates the permission was enabled globally. • **Some rights selected**—Indicates that permissions for the child record types were enabled individually, resulting in some permissions being disabled. • **No rights selected**—Indicates that no permissions for the child record types were enabled.

1.2.3.6.1 Assigning or Viewing Global User Rights for a Group

From a group's **System Rights** page, you can assign or view rights typically associated with end-user functions using a global User Rights view. This option allows for quick assignment of access rights to multiple record types or application areas that end-users typically use.

Note: *In this topic, global User Rights refers to Permissions available when you select the* ***User Rights*** *option from the* ***View*** *drop-down list of a group account's* ***System Rights*** *page.*



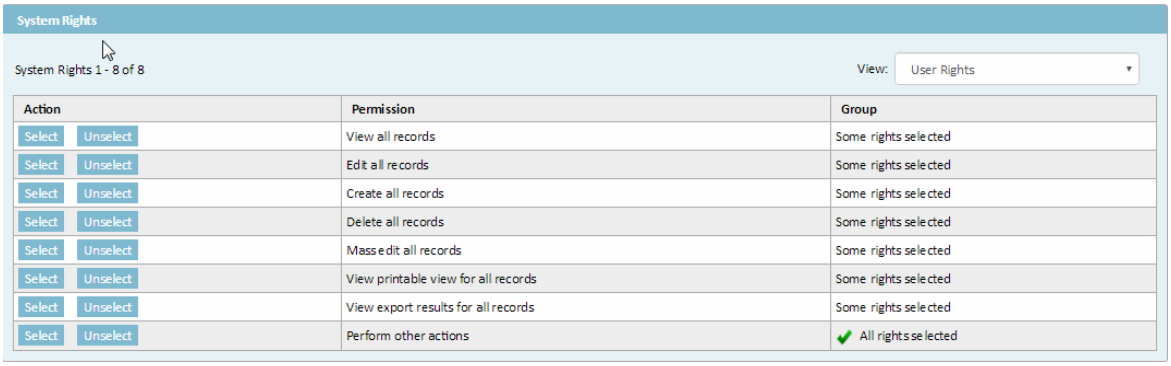
Group - System Rights Page for Global User Rights (Edit View)

To assign or view global User Rights for a group

1. Search for a group and open it.
2. From the left navigation pane, click **System Rights**.
3. From the **View** drop-down list, select **User Rights**. To assign rights, do one of more of the following:
   - To assign view rights to all records from the User application area, associated categories and custom fields, associated pages for the records (such as Security), click **Select** next to the **View All Records Permission**.
   - To assign edit rights to all records from the User application area, associated categories and custom fields, associated pages for the records (such as Security), click **Select** next to the **Edit All Records Permission**.
   - To assign create rights to all records from the User application area, associated categories and custom fields, associated pages for the records (such as Security), click **Select** next to the **Create All Records Permission**.
   - To assign delete rights to all records from the User application area, associated categories and custom fields, associated pages for the records (such as Security), click **Select** next to the **Delete All Records Permission**.
   - To assign mass edit rights to all records from the User application area, associated categories and custom fields, associated pages for the records (such as Security), click **Select** next to the **Mass Edit All Records Permission**.
   - To assign any remaining rights to all records from the User application area, associated categories and custom fields, associated pages for the records (such as Security), click **Select** next to the **Perform other actions Permission**.
4. If you are viewing currently assigned rights, the status displays under the Group column. For more information, see Group System Rights Page Field Descriptions.
5. Click a save option.

1.2.3.6.2 Results from Assigning Global User Rights

The following tables list the granular level rights that are automatically assigned when you assign one or more global User Rights. In this topic, global User Rights refers to Permissions available when you select the **User Rights** option from the **View** drop-down list of a group account's **System Rights** page.



Group - System Rights Page with User Rights View (Edit View)

The following table displays rights assigned from the group **System Rights** page when the **View** drop-down list **User Rights** option is selected and the **View All Records** permission displays the status **All Rights Selected**.

Rights Assigned with View all records Permission (for global User Rights)

Record Type	Individual Right
Account	• View Account records • View Account all categories • View Account all custom fields • View Account security • View Account all transactions
Appointment	• View Appointment records • View Appointment all categories • View Appointment all custom fields • View Appointment security • View Appointment Resources
Contact	• View Contact records • View Contact all categories • View Contact all custom fields • View Contact involvement • View Contact rates

	• View Contact relations • View Contact security • View Contact skills • View Contact territories
Documents	• View Document records • View Document all categories • View Document all custom fields • View Document security
Expenses	• View Expense records • View Expense all categories • View Expense all custom fields • View Expense security
History	• View History records • View History all categories • View History all custom fields • View History security
Invoice	• View Invoice records • View Invoice all categories • View Invoice all custom fields • View Line Item records • View Line Item all categories • View Line Item all custom fields • View Invoice security
Preferences	• View Preferences
Report	• View Report records
Task	• View Task records • View Task assignees • View Task all categories

	• View Task all custom fields • View Task security
Scheduled Actions	• View Scheduled Actions records

The following table displays rights assigned from the group System Rights page when the View drop-down list User Rights option is selected and the Edit All Records permission displays the status All Rights Selected.

Rights Assigned with Edit all records Permission (from global User Rights)

Record Type	Individual Right
Account	• Edit Account records • Edit Account all custom fields • Edit Account security
Appointment	• Edit Appointment records • Edit Appointment all custom fields • Edit Appointment security • Edit Appointment Attendees • Edit Appointment Resources
Contact	• Edit Contact records • Edit Contact all custom fields • Edit Contact rates • Edit Contact security • Edit Contact skills
Documents	• Edit Document records • Edit Document all custom fields • Edit Document security
Expenses	• Edit Expense records • Edit Expense all custom fields • Edit Expense security
History	• Edit History records

	• Edit History all custom fields • Edit History security
Invoice	• Edit Invoice records • Edit Invoice all custom fields • Edit Line Item records • Edit Line Item all custom fields • Edit Invoice security
Preferences	• Edit Preferences
Report	• Edit Report records • Edit Report security
Task	• Edit Task records • Edit Task assignees • Edit Task all categories • Edit Task all custom fields • Edit Task security

The following table displays rights assigned from the group System Rights page when the View drop-down list User Rights option is selected and the Create All Records permission displays the status All Rights Selected.

Rights Assigned with Create all records Permission (from global User Rights)

Record Type	Individual Right
Account	• Create Account records • Create Account all categories • Create Account all transactions
Appointment	• Create Appointment records • Create Appointment all categories • Create Appointment Attendees • Create Appointment Resources
Contact	• Create Contact records

	• Create Contact all categories • Create Contact rates • Create Contact relations • Create Contact skills • Create Contact territories
Documents	• Create Document records • Create Document all categories
Expenses	• Create Expense records • Create Expense all categories
History	• Create History records • Create History all categories
Invoice	• Create Invoice records • Create Invoice all categories • Create Line Item records • Create Line Item all categories
Task	• Create Task records • Create Task all categories

The following table displays rights assigned from the group System Rights page when the View drop-down list User Rights option is selected and the Delete All Records permission displays the status All Rights Selected.

Rights Assigned with Delete all records Permission (from global User Rights)

Record Type	Individual Right
Account	• Delete Account records • Delete Account all categories
Appointment	• Delete Appointment records • Delete Appointment all categories • Delete Appointment Attendees • Delete Appointment Resources

Contact	• Delete Contact records • Delete Contact all categories • Delete Contact rates • Delete Contact relations • Delete Contact skills • Delete Contact territories
Documents	• Delete Document records • Delete Document all categories
Expenses	• Delete Expense records • Delete Expense all categories
History	• Delete History records • Delete History all categories
Invoice	• Delete Invoice records • Delete Invoice all categories • Delete Line Item records • Delete Line Item all categories
Task	• Delete Task records • Delete Task all categories
Scheduled Actions	• Delete Scheduled Actions records

The following table displays rights assigned from the group System Rights page when the View drop-down list User Rights option is selected and the Perform other actions permission displays the status All Rights Selected.

Rights Assigned with Perform other actions Permission (from global User Rights)

Record Type	Individual Right
Appointment	• Scheduler Tool
Documents	• View letter generation • View XML generation • View template data mapping

	• View version • Revert version
Expenses	• Post Expense • Void Expense
Invoice	• Post Invoice • Void Invoice
Task	• Post Task • Void Task • Assign Task

1.2.3.6.3 Assigning Global Admin Rights to a Group

From a group's **System Rights** page, you can assign rights typically associated with system administrator functions using a global Admin Rights view. This option allows for quick assignment of access rights to multiple record types or application areas that system or business administrators typically use.

*Note: In this topic, global Admin Rights refers to Permissions available when you select the **Admin Rights** option from the **View** drop-down list of a group account's **System Rights** page.*

To assign global Admin Rights

1. Search for a group and open it.
2. From the left navigation pane, click **System Rights**.

   From the **View** drop-down list, select **Admin Rights**.

   - To assign view rights to all records from the Admin application area, associated pages for the records (such as Security), click **Select** next to the **All Admin View Rights Permission**.
   - To assign edit rights to all records from the Admin application area, associated pages for the records (such as Security), click **Select** next to the **All Admin Edit Rights Permission**.
   - To assign create rights to all records from the Admin application area, associated pages for the records (such as Security), click **Select** next to the **All Admin Create Rights Permission**.
   - To assign delete rights to all records from the Admin application area, associated pages for the records (such as Security), click **Select** next to the **All Admin Delete Rights Permission**.

See Assigning or Viewing Group System Rights for information about assigning groups of rights to end-users, solution developers, or administrators.

3. Click a save option.

1.2.3.6.4 Results from Assigning Global Admin Rights

The following tables list the granular level rights that are automatically assigned when you assign one ore more global Admin Rights. In this topic, global Admin Rights refers to Permissions available when you select the **Admin Rights** option from the **View** drop-down list of a group account's **System Rights** page.

The following table displays rights assigned from the group **System Rights** page when the **View** drop-down list **Admin Rights** option is selected and the **All admin view rights** permission displays the status All Rights Enabled.

Rights Assigned with All admin view rights Permission (from global Admin Rights)

Record Type	Individual Right
Group	• View Group records • View Group members
User	• View User records • View User group memberships
Admin Settings	• View Admin Settings records

The following table displays rights assigned from the group **System Rights** page when the **View** drop-down list **Admin Rights** option is selected and the **All admin edit rights** permission displays the status **All Rights Enabled**.

Rights Assigned with All admin edit rights Permission (from global Admin Rights)

Record Type	Individual Right
Group	• Edit Group records
User	• Edit User records
Admin Settings	• Edit Admin Settings records

The following table displays rights assigned from the group **System Rights** page when the **View** drop-down list **Admin Rights** option is selected and the **All admin create rights** permission displays the status **All Rights Enabled**.

Rights Assigned with All admin create rights Permission (from global Admin Rights)

Record Type	Individual Right
Group	• Create Group records • Create Group members
User	• Create User records • Create User group memberships

The following table displays rights assigned from the group **System Rights** page when the **View** drop-down list **Admin Rights** option is selected and the **All admin delete rights** permission displays the status **All Rights Enabled**.

Rights Assigned with All admin delete rights Permission (from global Admin Rights)

Record Type	Individual Right
Group	• Delete Group records • Delete Group members
User	• Delete User records • Delete User group memberships

1.2.3.6.5 Assigning Global Setup Rights to a Group

From a group's **System Rights** page, you can assign rights typically associated with solution developer functions using a global Setup Rights view. This option allows for quick assignment of access rights to multiple record types or application areas that solution developers typically use.

Note: *In this topic, global Setup Rights refers to Permissions available when you select the* ***Setup Rights*** *option from the* ***View*** *drop-down list of a group account's* ***System Rights*** *page.*

To assign global Setup Rights

1. Search for a group and open it.
2. From the left navigation pane, click **System Rights**.

   From the **View** drop-down list, select **Setup Rights**.

   - To assign view rights to all records from the Designer (Setup) application area, associated pages for the records (such as Security), click **Select** next to the **All setup view rights Permission**.

- To assign edit rights to all records from the Designer (Setup) application area, associated pages for the records (such as Security), click **Select** next to the **All setup edit rights Permission**.
- To assign create rights to all records from the Designer (Setup) application area, associated pages for the records (such as Security), click **Select** next to the **All setup create rights Permission**.
- To assign delete rights to all records from the Designer (Setup) application area, associated pages for the records (such as Security), click **Select** next to the **All setup delete rights Permission**.

  See Assigning or Viewing Group System Rights for information about assigning groups of rights to end-users, solution developers, or administrators,.

3. Click a save option.

1.2.3.6.6 Results from Assigning Global Setup Rights

The following tables list the granular level rights that are automatically assigned when you assign one ore more global Setup Rights. In this topic, global Setup Rights refers to Permissions available when you select the **Setup Rights** option from the **View** drop-down list of a group account's **System Rights** page.

The following table displays rights assigned from the group **System Rights** page when the **View** drop-down list **Setup Rights** option is selected and the **All setup view rights** permission displays the status **All Rights Enabled**.

Rights Assigned with All setup view rights Permission (from global Setup Rights)

Record Type	Individual Right
Administer Custom Tools	• View Administer Custom Tools records
Global Navigation	• View Global Navigation records
Home Pages	• View Home Pages records
Lookup Tables (System)	• View Lookup Tables records
Custom Lookup Tables	• View Custom Lookup Tables records
Multi-currency	• View Multi-currency records
Miscellaneous Settings	• View Miscellaneous Settings records
Object Definitions	• View Object Definitions records • View Object Definitions custom fields

	• View Object Definitions forms • View Object Definitions object views • View Object Definitions blocks • View Object Definitions rules • View Object Definitions rule qualifiers • View Object Definitions search views • View Object Definitions templates • View Object Definitions wizards
Portal Panes	• View Portal Panes records
Record Locks	• Release Edit Locks
Routes	• View Routes records
Route Stops	• View Route Stops records
Search Results	• Bypass Search Limits
System Settings	• View System Settings records

The following table displays rights assigned from the group **System Rights** page when the **View** drop-down list **Setup Rights** option is selected and the **All setup edit rights** permission displays the status **All Rights Enabled**.

Rights Assigned with All setup edit rights Permission (from global Setup Rights)

Record Type	Individual Right
Administer Custom Tools	• Edit Administer Custom Tools records
Global Navigation	• Edit Global Navigation records
Home Pages	• Edit Home Pages records
Lookup Tables (System)	• Edit Lookup Tables records
Custom Lookup Tables	• View Custom Lookup Tables records
Multi-currency	• Edit Multi-currency records

Miscellaneous Settings	• Edit Miscellaneous Settings records
Object Definitions	• Edit Object Definitions records • Edit Object Definitions custom fields • Edit Object Definitions forms • Edit Object Definitions object views • Edit Object Definitions blocks • Edit Object Definitions rules • Edit Object Definitions rule qualifiers • Edit Object Definitions search views • Edit Object Definitions templates • Edit Object Definitions wizards
Portal Panes	• Edit Portal Panes records
Routes	• Edit Routes records
Route Stops	• Edit Route Stops records
System Settings	• Edit System Settings records

The following table displays rights assigned from the group **System Rights** page when the **View** drop-down list **Setup Rights** option is selected and the **All setup create rights** permission displays the status **All Rights Enabled**.

Rights Assigned with All setup create rights Permission (from global Setup Rights)

Record Type	Individual Right
Administer Custom Tools	• Create Administer Custom Tools records
Global Navigation	• Create Global Navigation records
Home Pages	• Create Home Pages records
Lookup Tables (System)	• Create Lookup Tables records
Custom Lookup Tables	• Create Custom Lookup Tables records
Multi-currency	• Create Multi-currency records

Miscellaneous Settings	• Create Miscellaneous Settings records
Object Definitions	• Edit Object Definitions records • Edit Object Definitions custom fields • Edit Object Definitions forms • Edit Object Definitions object views • Edit Object Definitions blocks • Edit Object Definitions rules • Edit Object Definitions rule qualifiers • Edit Object Definitions search views • Edit Object Definitions templates • Edit Object Definitions wizards
Portal Panes	• Edit Portal Panes records
Routes	• Edit Routes records
Route Stops	• Edit Route Stops records
System Settings	• Edit System Settings records

The following table displays rights assigned from the group **System Rights** page when the **View** drop-down list **Setup Rights** option is selected and the **All setup delete rights** permission displays the status **All Rights Enabled**.

Rights Assigned with All setup delete rights Permission (from global Setup Rights)

Record Type	Individual Right
Administer Custom Tools	• Delete Administer Custom Tools records
Global Navigation	• Delete Global Navigation records
Home Pages	• Delete Home Pages records
Lookup Tables (System)	• Delete Lookup Tables records
Custom Lookup Tables	• Delete Custom Lookup Tables records
Multi-currency	• Delete Multi-currency records

Miscellaneous Settings	• Delete Miscellaneous Settings records
Object Definitions	• Delete Object Definitions records • Delete Object Definitions custom fields • Delete Object Definitions object views • Delete Object Definitions blocks • Delete Object Definitions rules • Delete Object Definitions rule qualifiers • Delete Object Definitions search views • Delete Object Definitions templates • Delete Object Definitions wizards
Portal Panes	• Delete Portal Panes records
Routes	• Delete Routes records
Route Stops	• Delete Route Stops records

1.2.3.6.7 Example for Assigning Rights to View Contacts

In order for a group member to access contacts, you must assign minimal view rights. Afterward, the group member will be able to view the Contact list page, the **General** page for contact records, the **Workflow** page for contact records. In addition, the group member will be able to search contacts from the **Advanced Contact Search** page.

To assign rights to view contacts

1. Search for a group and open it.
2. Click **System Rights** from the left pane.
3. Select **Contact** from the **View** drop-down list (right side).
4. Select the **View Contact records** check-box.
5. Click a save option.

The View Contact records right results in the display of the **Contacts** tab, **Contacts List** page, **Manage Contact Collections** page, **Contact Collections Subscription** page, **Advanced Contact Search** page. From a contact record, the View Contact records right results in the display of the **General** page and **Workflow** page, including read-access to sections and fields on those pages.

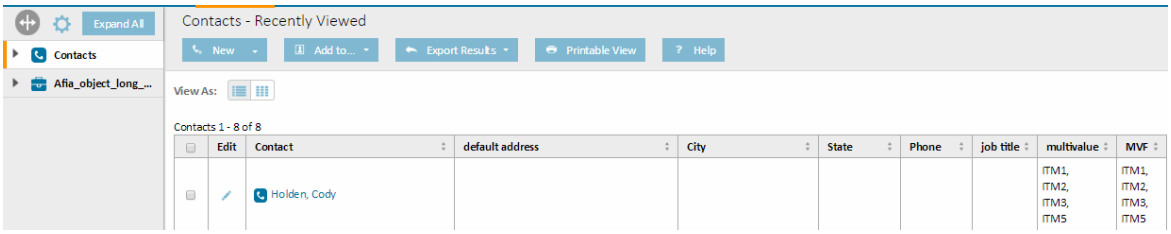
1.2.3.6.8 Example for Assigning Rights to Create Contacts

In order for a group member to create contacts, you must assign the basic right, Create Contact records. In addition, this right requires the assignment of View Contact records.

To assign rights to create contacts

1. Search for a group and open it.
2. Click **System Rights** from the left pane.
3. Select **Contact** from the **View** drop-down list (right side).
4. Select the **Create Contact records** check-box.
5. Also select the **View Contact records** check-box.
6. Click a save option.

The Create Contact records right requires the assignment of the View Contact records right. As a result, a group member with Create Contact records right will have access to all pages that result from the View Contact record right. In addition, the Create Contact record right will result in a **New** button that is available on the Contact List page.



Contacts List Page (New Button)

1.2.3.6.9 Example for Assigning Rights to Edit Contacts

To assign rights to edit contacts

1. Search for a group and open it.
2. Click **System Rights** from the left pane.
3. Select **Contact** from the **View** drop-down list (right side).
4. Select the **Edit Contact records** check-box.
5. Also select the **View Contact records** check-box.
6. Click a save option.

The Edit Contact records right requires the assignment of the View Contact records right. As a result, a group member with Edit Contact records right will have access to all pages that result from the View Contact record right. In addition, the Edit Contact record right will result in an Edit Record icon that is available on the Contact List page. From contact records, an **Edit** button will be available.

1.2.3.6.10 Example for Assigning Rights to Delete Contacts

To assign rights to delete contacts

1. Search for a group and open it.
2. Click **System Rights** from the left pane.
3. Select **Contact** from the **View** drop-down list (right side).
4. Select the **Delete Contact records** check-box.
5. Also select the **View Contact records** check-box.
6. Click a save option.

The Delete Contact records right requires the assignment of the View Contact records right. As a result, a group member with Delete Contact records right will have access to all pages that result from the View Contact record right. In addition, the Delete Contact record right will result in a **Delete** button from an open contact's pages.

1.2.3.6.11 Example for Assigning All Rights to Contacts Pages and Fields

For records that contain information that should be commonly shared, you may choose to assign access to all related pages, categories, custom fields, sections, and forms. If you assign rights to work with all categories and all custom fields from the **System Rights** page, those rights will propagate to categories and custom fields that are created in the future.

To assign rights to all pages and fields of contacts

1. Search for a group and open it.
2. Click **System Rights** from the left pane.

   The **System Rights** page will open.
3. Select **Contact** from the **View** drop-down list (right side).
4. Select the check-box to the left of Permission (table heading). Afterward, all rights related to contact records should be selected.

Note: *The following rights are selected and give global access to the current Contact categories and custom fields:*

- **View Contact all categories**
- **Create Contact all categories**

- **Delete Contact all categories**

If you assign the **View all categories**, **Create all categories**, or **Delete all categories** rights, the group will automatically have rights to access and work with categories that are created in the future for the record type.

- **View Contact all custom fields**
- **Edit Contact all custom fields**

If you assign the **View all custom fields** or **Edit all custom fields rights**, the group will automatically have rights to access and work with custom fields that are created in the future for the record type.

5. Click a save option.

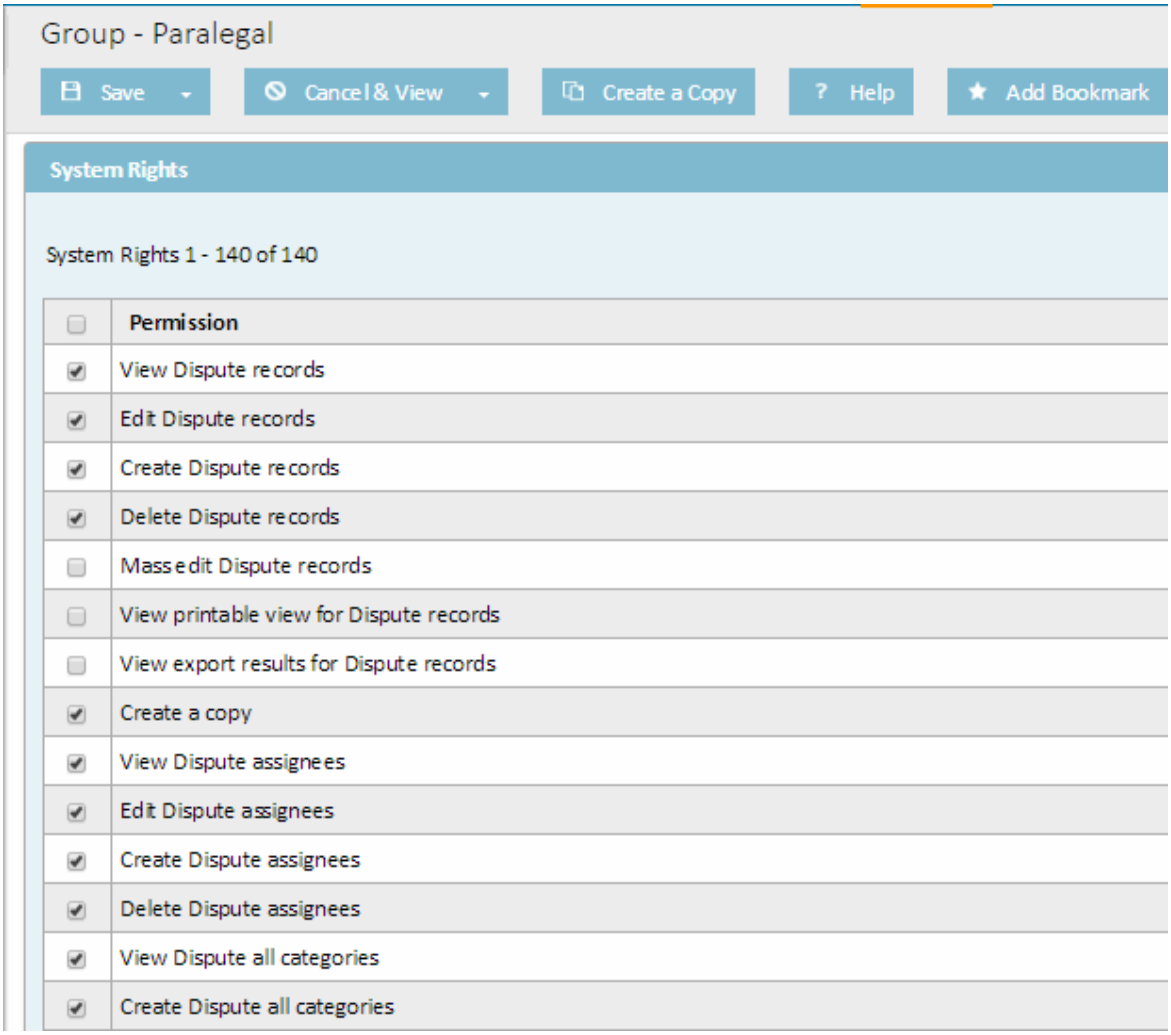
After assigning rights above, the following screen views are available to group members:

Note: *All basic contact pages are available (**General**, **Workflow**). All additional contact pages are available (**Details**, **Categories**, **Rates**, **Relations**, **Skills**, **Territories**, **Security**).*

1.2.3.6.12 Examples for Assigning Projects Rights

The custom object, Dispute, will be used to show how rights appear for custom objects (projects). The following screens display rights for Dispute records. An Involved child object was added to the Dispute object.

Note: *Dispute is used as an example and it is automatically included with TeamConnect Legal Matter Management but the Dispute object is not included with TeamConnect Enterprise.*



Group System Rights for Dispute (Custom Object)

Note: *Rights for the child Involved object include Permission list items, View Involved Party Records through Edit Involved Party Security.*

The **Create a Copy** right is unique to custom objects. If it is assigned the resulting application page will display the **Copy** button from an open dispute record.

1.2.3.6.12.1 Assigning All Rights to Dispute Pages and Fields

The following section describes how to assign access to all dispute record related pages, categories, custom fields, sections, and forms.

Note: *Dispute is used as an example and it is automatically included with TeamConnect Legal Matter Management but the dispute object is not included with TeamConnect.*

To assign all rights to dispute record pages and fields

1. Search for a group and open it.
2. Click **System Rights** from the left pane.

   The **System Rights** page will open.
3. Select **Dispute** from the **View** drop-down list (right side).
4. Select the check-box to the left of Permission (table heading). Afterward, all rights related to dispute records should be selected.
5. Click a save option.

After assigning rights above, the respective screen views are available to group members.

Note: *The links in the left pane above represent record pages that the group member can access.*

1.2.3.7 Assigning Group Category and Custom Field Rights

From a group's **Category Rights** page, you can assign rights to specific categories and custom fields per record type. Additionally, you can assign high level rights to all categories and custom fields across all record types. For more details on how field-level security works for TeamConnect 4.2 +, see Rights for Categories and Custom Fields.

Note: *Custom searches have the following option: Custom search will respect Custom Field Rights. When enabled, users who do not have rights to a custom field cannot search on those fields. This setting will default to 'on' for new implementations and will default to 'off' for upgraded TeamConnect instances.*

To assign category and custom field rights

1. Search for a group and open it.
2. To change rights for categories and custom fields, from the left navigation pane, click **Category Rights**. See the appendix, Rights for End-users for additional information about general rights for categories and custom fields for each record type.
3. To assign global category or custom field rights for all record types, do the following:
   - From the **View** drop-down list, select **User Rights**.
   - From the resulting rights list, click the **Select** button for the following permission rows:
     - **View all categories**—Allows access to the **Categories** pages of all records.
     - **Add all categories**—Allows addition or selection of all available categories from the **Categories** pages of all records.
     - **Remove all categories**—Allows removal or clearing of all categories from the **Categories** pages of all records.
     - **View all custom fields**—Allows access to custom fields associated with any categories from the **Details** pages of all records.

- **Edit all custom fields**—Allows data entry or changes for custom fields values associated with any categories from the **Details** pages of all records.

  Afterward, all rights for categories and custom fields of all record types will be assigned to the group.

4. To assign specific category or custom field rights for a specific record type, do the following:
   - From the **View** drop-down list, select a record type. For example, Contacts.
   - To assign the following base category rights, select the check-box next to each right:
     - **View Contact category**—Allows access to the **Categories** page of the contact record.
     - **Add Contact category**—Allows addition or selection of all available categories from the **Categories** page of the contact record.
     - **Remove Contact category**—Allows removal or clearing of all categories from the **Categories** page of the contact record.
     - **View Contact custom fields**—Allows access to custom fields associated with any contact categories from the **Details** page of the contact record.
     - **Edit Contact custom fields**—Allows data entry or changes for custom fields values associated with any contact categories from the **Details** page of the contact record.
   - To assign additional category or custom field rights, select the respective check-box.
   - ***Note:*** *Further detail on this functionality is highlighted in Hierarchy Overview of Group Rights.*
5. Click a save option.

Group Category Rights Page Field Descriptions

Label	Description
View drop-down list	A list of record types for which you can assign rights to work with associated categories and custom fields. After selecting a list option, the workspace is updated with a list of rights specific to categories and custom fields for that option. For example, if you select Contacts, the rights list displays only rights for working with contact categories and custom fields.
Permission	A general list of rights follows. For more information, see Understanding Rights and Rights for Categories and Custom Fields. • **View category**—To grant rights to view categories for the selected record type and rights to set a category as default, select the **View category** check-box. • **Add category**—To grant rights to add a category to the selected record type, select the **Add category** check-box.

- **Remove category**—To grant rights to remove a category from the selected record type, select the **Remove category** check-box.
- **View all custom fields**—To grant rights to see custom fields associated with the selected record type, select the **View all custom fields** check-box. Additional requirements include: Rights to read the associated category and its parent categories; and rights to read associated custom objects.
- **Edit all custom fields**—To grant rights to edit custom field values associated with the selected record type and categories, select the **Edit all custom fields** check-box. Additional requirements include: Rights to view the custom fields on that category.
- **Individual Fields**—To manage view and edit rights for custom fields on a given object. Click the dropdown arrow on the respective row ( ) to open the view and edit options.

Important: Adjustments made to the category rights at-large will affect custom field rights. For example, if the **View all custom fields** check-box is selected, all custom field **View** check-boxes will become read-only. If the individual fields were not selected prior to clicking the parent category **View All** button, they will appear to be read-only and unchecked. Despite this, view rights will be on for all custom fields in the category. Likewise, the same conditions apply for the **Edit all custom fields** check-boxes and the respective custom fields on a category. Similar to how the category rights function, **Edit** rights will not be available for any custom field that does not have **View** rights enabled.

1.2.3.7.1 Example for Assigning Rights to Contact Categories and Fields

There may be a group that you'd like to assign access to work with some custom fields but not all custom fields of a record type. It is recommended to assign rights to view and add the related category. Afterward, you can assign rights to one or more custom fields associated with that category.

The following example will serve to demonstrate how to add **View** rights to all of the custom fields under the External->Attorney category. **Edit** rights will also be activated for two of the three custom fields ("Minority" and "Overall Performance").

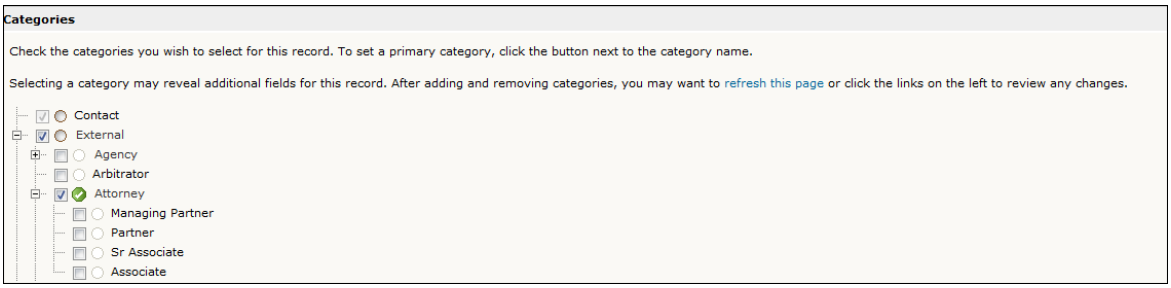
For more details on how field-level security works for TeamConnect 4.2+, see Hierarchy Overview of Group Rights.

To assign group rights to specific custom fields

1. Search for a group and open it.
2. Click **System Rights** from the left pane.

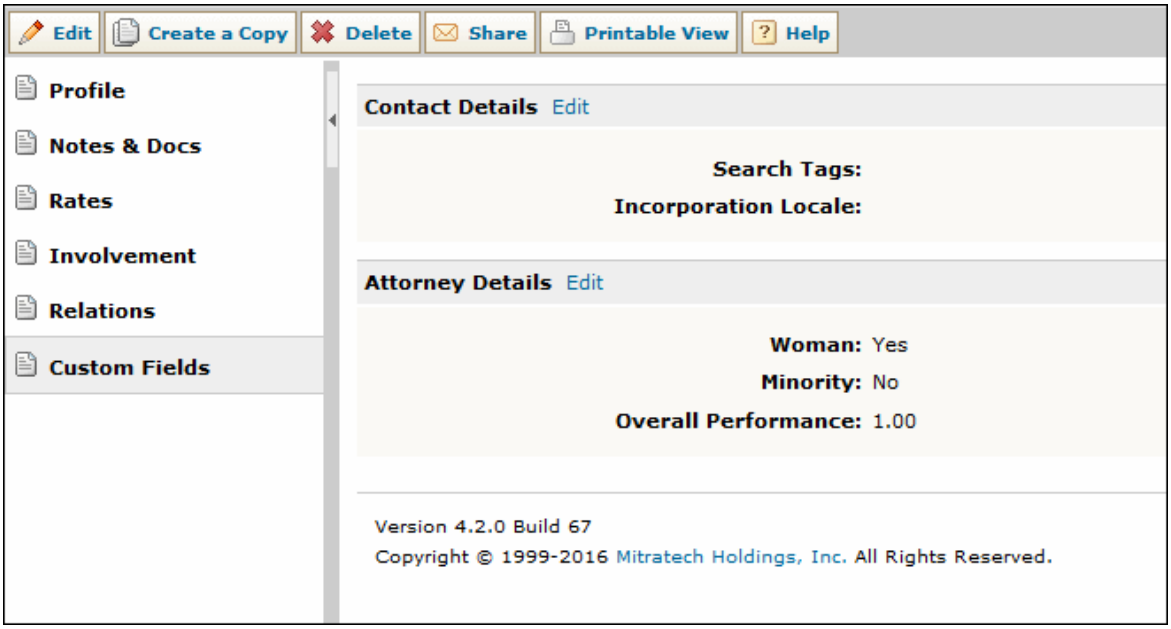
3. Select **Contact** from the **View** drop-down list (right side).
4. Select the **View Contact records** check-box.
5. Select the **Edit Contact records** check-box.
6. Save.
7. Click **Category Rights** from the left pane.
8. Select **Contact** from the **View** drop-down list (right side).
9. Click the **Edit** button.
10. Enable **View Category** for External > Attorney.
11. Click the **Individual Fields** drop-down arrow ( ) for External > Attorney.
12. Click the parent **View** check-box for the **Fields** under External->Attorney.
13. Click the Minority and Overall Performance check-boxes underneath **Edit** for **Fields**.
14. Click a save option.

After assigning rights above to a group, the following screen views can be selected under the **Categories** subsection of the **Contact** profile. Make sure to **Save** after making changes to the contact record.



Assigning Category to Contact

After assigning the following category, the following custom fields are visible via the **Custom Fields** link on the sidebar navigation:



Note: *If rights are turned off on system blocks, those blocks will not be visible. Rights turned off on custom blocks will appear as SECURED.*

1.2.3.8 Hierarchy Overview of Group Rights

Improved granular group rights (as of TeamConnect 4.2) allows for more robust control over user privileges. In setting up these rights, it is important to understand which settings take precedence. Some sections, as detailed below, will change the read-only/read-write status of others. An example of setting up rights can be found on the Example for Assigning Rights to Contact Categories and Fields.

Hierarchy Overview of Rights

The following sections describe how group rights can be configured in TeamConnect 4.2+.

It should be noted that the far left checkbox on the top row will give all view and edit rights on all object categories and fields. When this box is checked, all subsidiary custom fields will be unable to be checked, but will retain view and edit permissions.

Chart Number	Section Type	Details
1	Full Parent-level rights management	These checkboxes will enable or disable all items within the column. Users should note that:

Chart Number	Section Type	Details
		1. Edit rights cannot be enabled for any category lacking the respective View rights. 2. Category rights take precedence over custom field-level rights.
2	Individual Category Item Rights	Each of these checkboxes enables or disables the respective right for that category and column (e.g., selected example provides **View** rights for **External** category on Contact object). Selecting the **View all custom fields** or **Edit all custom fields** box will "gray-out" the boxes for custom fields (see Section 4). If you have not individually checked the custom field-level boxes prior to the View/Edit all custom fields box, they will be grayed out as empty boxes. **However, you will still have View or Edit rights if the Section 2 View all custom fields/Edit all custom fields boxes are checked, regardless of whether the Section 4 boxes have check-marks.** For more detail, see Section 4 of this table, or the Addendum at the end of this document.
3	Full Category-level rights management	Clicking any box in this column will apply full rights on the category to the group. As this will enable the **View all custom fields/Edit all custom fields** boxes, the Section 4 custom field-level rights boxes will be grayed out. If you have not individually checked the custom field-level boxes prior to the View/Edit all custom fields box, they will be grayed out as empty boxes. **However, you will still have View or Edit rights if the Section 2 View all custom fields/Edit all custom fields boxes are checked, regardless of whether the Section 4 boxes have check-marks.**
4	Custom Field-level rights management	Click the green caret symbol to view the custom fields for the respective category. If the **View all custom fields/Edit all custom fields** boxes are checked for the row, these custom field-level boxes will be grayed out. In this case, even if they are grayed out without checks present.

1.2.3.9 Assigning Group Tool Rights

From a group's **Tool Rights** page, you can assign rights to tools. Afterward, the group members will be able to view and work with the tools.

Note: *Some tools are available from the User application area and other tools are available from the Designer application area.*

To assign group tool rights

1. Search for a group and open it.
2. To make tools available, from the left navigation pane, click **Tool Rights**.
   - To enable a tool for the group, select the tool's check-box.
   - To disable a tool, clear the tool's check-box.

     For more information, see the Groups Tool Rights fields table.
3. Click a save option.

Groups Tool Rights Field Descriptions

Label	Description
Permission	Select the check-box for each tool to enable: • **Contact Sweeper**—Administrator's tool to perform a duplicate contacts check across the system. Recommend restricting access to this tool to system administrators. • **Design Snapshot Tool**—Solution developer's tool to capture your latest design snapshot, provide a summary of archived design snapshots, generate design upgrade files. After the right is assigned, access this tool from the Designer area. • **Design Import Tool**—Solution developer's tool to apply a design upgrade file to upgrade a QA or production TeamConnect instance from an older design version to a newer design version. After the right is assigned, access this tool from the Designer area. • **Reassignment Tool**—Reassigns multiple appointments, projects, and tasks. • **Exchange Rates**—Administrator's tool to update current exchange rates. For details see Updating Exchange Rates. • **Invoice Validation Rule Setting**—Solution developer's tool to activate or deactivate invoice validation rules. After the right is

assigned, access this tool from the Designer area. Members of the CSM Admin group have default access rights to the Invoice Validation Rule Setting tool.

- **Global Search Index Tool**—The Global Search Index Tool is utilized to update Global Search after objects have been enabled or disabled and clear search server information.
- **Map Line Item Codes**—Solution developer's tool to map invoice line item codes (fee/task codes, expense codes, or activity codes). This tool only appears on the Tool Rights page if it has been loaded in TeamConnect.
- **Expense Unit Prices**—Administrator's tool. For details, see Updating Expense Unit Prices.
- **Data Import Wizard**—Administrator's tool to import data from an Excel spreadsheet into TeamConnect fields. For details, see Importing Data to Create Records.
- **Screen Designer**—Solution developer's tool to build a screen block from a WYSIWYG layout. For details, see Using Screen Designer.
- **Locale Manager**—Solution developer's tool to control which locales are available to use as system default, or to choose as an end user's preference.
- (TeamConnect Legal Matter Management and TeamConnect® Express) **Create Next Fiscal Budget**—Business manager's tool to define the fiscal year for matter budgets.
- (TeamConnect Legal Matter Management and TeamConnect® Express) **Legal Preferences Tool**—Business manager's tool to set preferences for budget definition. For example, defining the budget year start, setting up budget detail levels.
- (TeamConnect Legal Matter Management only) **Time Entry Tool**—Business manager's tool to manage timekeepers' entries.

Note: *Additional tools may be available depending on whether custom tools have been added to your system.*

1.2.3.10 Changing Group Default Object Views

From a group's **Object Views** page, you can change the default set of object views for the group. If a solution developer has designed custom object views (created custom pages, sections, fields, and/or forms for an object), you can select a custom object view.

Object views can also be assigned at the system level and this is performed from the Designer area of TeamConnect. Object views assigned at the group level override system level object views.

Users that belong to multiple groups will see the object views assigned to their default group as specified in their user account. Assigning different views of an object to different groups of users is one way of controlling access to object record information. No matter which categories or custom

fields individual members of a user group can access, they cannot see them if these categories or custom fields are not included in the object view assigned to their default group.

To change default object views for a group

1. Search for a group and open it.
2. Click **Object Views** from the left pane.
3. (optional) For an object (record type) click the corresponding **Object View** drop-down list and select a different object view.
4. Click a save option.

Note: *The selected settings take effect immediately, and users who do not have a default group set in their user accounts see the object views assigned to the system.*

1.2.3.11 Viewing or Creating Group History

From a group's **History** page, you can create a history (containing notes about changes to the group), view a list of related history records, or perform an advanced search for a history.

To create a history for a group

1. Search for a group and open it.
2. Click **History** from the left pane.

   The group's History list page will open. You can click a history **Description** to view its details.
3. Click **New History**.
4. Enter a change **Description**.
5. Click a save option.

1.2.3.12 Deleting a Group

When you delete a group, the users that are group members will not be deleted but they will lose security rights that were granted through the group.

Scenarios that Prevent Deletion

When you try to delete a group, the following scenarios prevent the deletion:

- If any record's **Security** page grants rights to the group (record-level security).
- If any User accounts specify the group as their Primary group.
- If the group is assigned to the Process Manager role of any active workflow rule.

- If the group is linked to any active workflow request (even if the group is not assigned to a Process Manager role).

To delete a group

1. Select the **Admin** tab.
2. Click the **Groups** sub-tab link.
3. (optional) From the left navigation pane, select a Group view.
4. Click the name of the group to delete.

   The group record opens.
5. Click **Delete**.

What is Deleted

When you delete a group, the following associated data gets deleted:

- All rights assigned in the **System Rights**, **Category Rights**, and **Tool Rights** pages of the group account.
- Member list (not the user accounts).
- Default object view selections.
- Approval route stop members where this group was selected.
- Home Page copies created for the members of this group.
- Associated History records.

1.2.4 Users

You need to create a user account for anyone who needs to log into TeamConnect. Each user account also requires an associated contact record. Some contacts, such as external vendors, will be created in TeamConnect but will not have corresponding user accounts.

Generally, user accounts will not be used to assign security rights unless the user was migrated from TeamConnect 2.x. For new user accounts, you can view

For more information on setting up rights, see Assigning or Viewing Group System Rights.

User Record Pages

The following are user-specific pages:

- The **General** page lets you enter information about the user, such as User Name and Password. You can also manage a user's account from the **General** page, for example, activate or inactive an account and set an account expiration date.
- The **Group Memberships** page lets you add a user to a group or remove a user from a group.

- The **System Rights** page lets you assign or view rights to work with records, application areas, and application features.
- The **Category Rights** page lets you assign or view rights to categories and custom fields by record type.
- The **Tool Rights** page lets you assign or view rights to system tools and custom tools.
- The **History** page is also associated with a user. The **History** page lets you add notes about changes to the user or review previous history notes.

1.2.4.1 Working with Users

You can perform the following tasks when you are working with users.

Users List

- Searching for Users—Search for a user to view or edit.
- Viewing Users—View a list of users or open an individual user.
- Creating or Editing Users—Add a user or edit a user's information.
- Deleting a User—Delete a user.

User General Page

- Creating or Editing Users—Add a user or edit a user's information.
- Activating and Inactivating a User—Activate or inactivate a user.
- Prompting Users to Change Their Passwords—Set a prompt for a users to change their password on application login.
- Editing or Viewing a User's Preferences—Edit or view a user's preferences.
- Unlocking User Accounts—Unlock user accounts that have been locked due to unauthorized access attempts or incorrect passwords.

User Group Memberships Page

- Changing a User's Group Membership—Add a user to a group or remove a user from a group.

User System Rights Page

- Assigning or Viewing User System Rights—Assign or view rights to work with records, application areas, and application features.

User Category Rights Page

- Assigning or Viewing User Category Rights—Assign category and custom field rights to a user.

User Tool Rights Page

- Assigning or Viewing User Tool Rights—Assign rights to work with system and custom tools.

User History Page

- Viewing or Creating User History—Create or view notes about changes to a user.

1.2.4.2 Searching for Users

From the **Users - Search** page, search for users using multiple field values as criteria. For example, you can search for users by **Name**, **User Type**, and associated **Contact**.

To perform an advanced search for a user

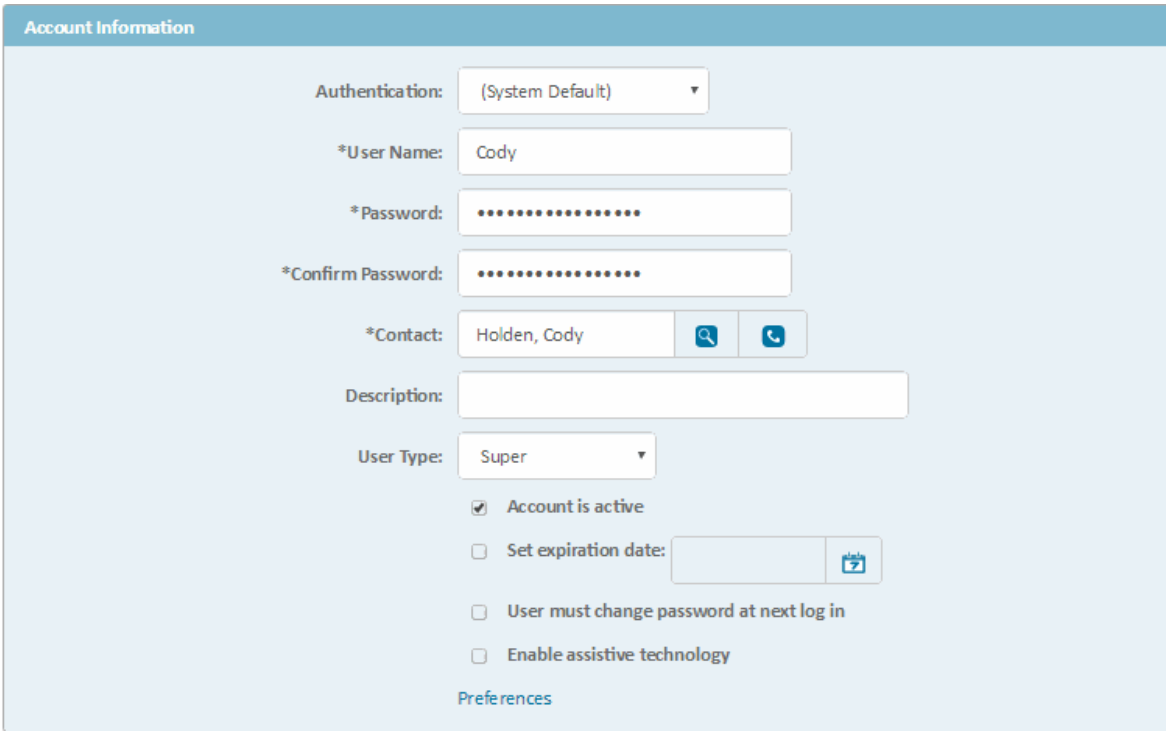
1. Click the **Admin** tab.
2. Click the **Users** link under the tab bar.
3. Click the **Custom Search** link.

   The **Users - Search** page opens.
4. (optional) To limit the fields used to search, in the **Field** drop-down list of the **Filter Criteria** section, select an appropriate option.
5. Enter search criteria in the resulting fields. See User General Page Field Descriptions table for descriptions of search criteria fields.
6. Click **Search**.
7. To open a user account, from the right pane, click a user's associated contact name link.

1.2.4.3 Viewing Users

You can view users by browsing user collections. Alternatively, you can search for a user (see Searching for Users).

From a user record's **General** page, you must search for a contact to associate with the user. Afterward in edit-mode, a contact icon will display, allowing you to click through to the associated contact record.



User Record - General Page

To browse a list of users by view

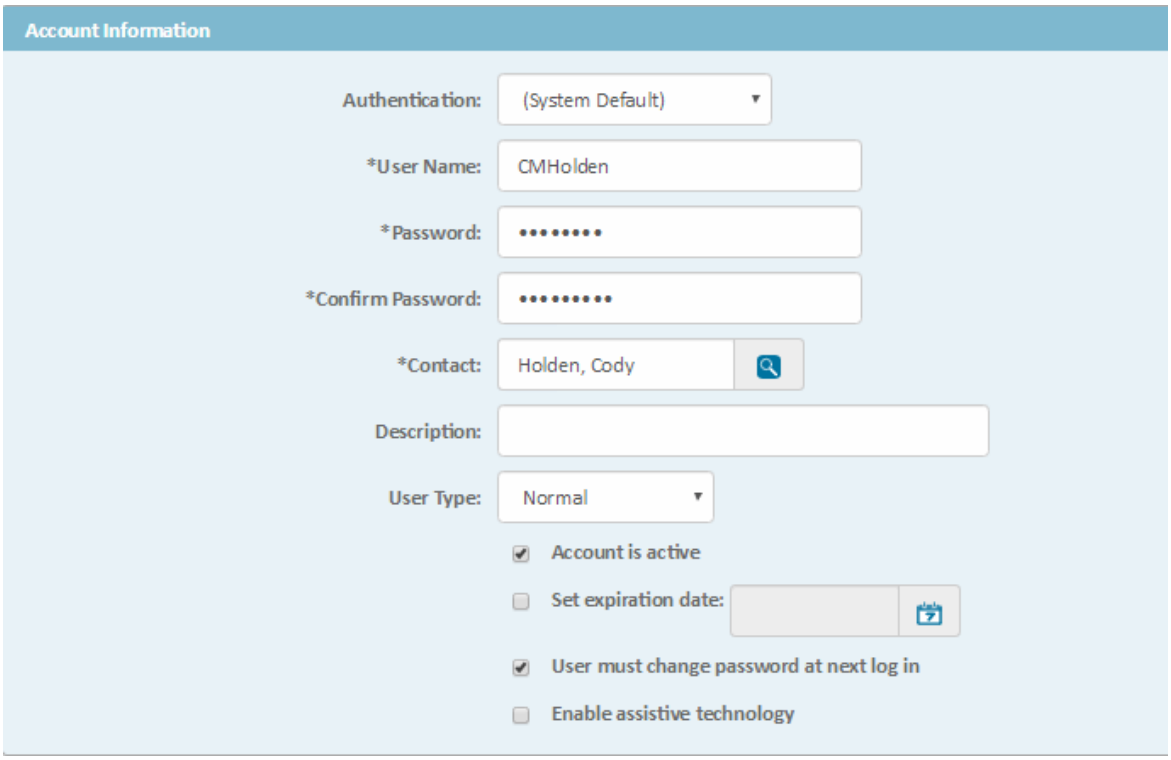
1. Click the **Admin** tab.
2. Click the **Users** link under the tab bar.
3. (optional) From the left pane, select a User collection:
   - **Recently Viewed**—Displays the last 50 users that you opened. You cannot delete this collection link, change its order. It is always the first collection listed in the left pane.
   - **Super Users**—Displays users whose **User Type** is **Super**, which typically means they have more security rights than Normal users.
   - **Limited-Privilege Users**—Displays users whose **User Type** is **Limited-Privilege**.
   - All Users
   - **Normal Users**—Displays users whose **User Type** is **Normal**.
   - **Inactive Users**—Displays users with inactive accounts.
   - **Active Users**—Displays users with active accounts.
   - **New Users**—Displays users that have been created within the current session. The results of this collection are sorted alphabetically.
4. To open a user account, from the right pane, click a user's associated contact name link.

1.2.4.4 Creating or Editing Users

Before creating a user, search existing users to make sure you do not create a duplicate. Users intending to create user accounts must have **View** and **Edit** rights for the Contact, User, and Preferences object to successfully complete the task.

Note: *If you are editing an existing user in a way that affects their access rights to records or other features, and that user is presently logged in, some of your changes might not take effect until that user ends their session and then logs back in.*

To create a new user, you enter information similar to the following image.



Creating a New User

To create or edit a user

1. Click the **Admin** tab.
2. Click the **Users** link under the tab bar.
3. Click the **New** button.
4. Select an **Authentication Type**.
5. Enter a **User Name**. Maximum length: 50 characters. User names cannot contain spaces or more than one @ character.
6. Enter the user's **Password**. Maximum length: 250 characters. Restrictions are based on the **Password Parameters** on the **Security** page of **Admin Settings**.

7. Retype or copy the password into the **Confirm Password** field.
8. Click the **Search Contacts** icon and search for a contact to associate with the user. Create a contact record for the user if one does not exist.
9. Select a **User Type** from the drop-down list.
   - **Super**—Can access all public and private records, as long as the user has group rights to those records.
   - **Normal**—Can access all public records. Can access private records only if record-level security is granted to the user.
   - **Limited-privilege**—Can access only records created by the user and records to which they have been granted explicit access by another user. Limited-privilege users will only see records to which they are assigned unless they are specifically assigned rights at the record level.

     If you need to allow limited-privilege users to perform tasks not normally available to them, such as the ability to approve an invoice, there must be a rule written that gives them record level rights to the invoice so that they can see and approve it.
10. Select the **Account is active** check-box.
11. Click a save option.

Note: *If your licensing scheme specifies a limit on the number of named active users, and the user you are saving is active and would exceed the limit, you will see an error message. You can retain the user's information by clearing the* ***Account is Active*** *check-box, then trying the save again. For details about licensing schemes, see Viewing Information About Your Product License.*

Note: *Newly added users will be temporarily unable to see data on reports that are run from the Reports tab. This is because Data Warehouse does not yet have the new user's information and cannot determine their security rights. This situation will resolve itself when the next Data Warehouse refresh job runs.*

User General Page Field Descriptions

Label	Description
User Name	(required) Type a name. Maximum length: 50 characters.
Password	(required) Type the password. Maximum length: 250 characters.
Confirm Password	(required) Retype or copy the password.
Contact	(required) Search for the contact (person or company) for which you are creating the account. If the contact does not yet exist, you can add a new

	contact from the **Contacts Search** window of the Search Module.
Description	Enter a brief description for the user, if necessary. Maximum length: 250 characters.
User Type	Select one of the following: • **Super**—Can access all public and private records. This setting overrides access restrictions based on record-level security settings. Recommended for system administrators and solution developers. • **Normal**—Can access all public records. Can access private records only if created by the user or if record-level security is granted to the user. Recommended for internal staff. • **Limited-Privilege**—Can access only records created by the user and records where record-level security has been explicitly granted to the user. Recommended for Outside Counsel. If you need to allow limited-privilege users to perform tasks not normally available to them, such as the ability to approve an invoice, there must be a rule written that gives them record level rights to the invoice so that they can see and approve it. ***Note:*** *Access to a record automatically grants access to its embedded records but not to its related records. For example, if a limited-privilege user has the right to access a dispute record, they cannot automatically access the dispute's related involved parties, tasks, histories, or expenses, but they can access its allegation (embedded object) records.*
Authentication Type	Select the authentication mechanism from the drop-down list to use when authenticating a user during login. This setting determines which TeamConnect login URL to give a user. Select one of the following: • **System Default**—This option maps to the default authentication mechanism selected in the Admin Settings. See Authentication for more information. • **Standard Authenticator**—If this user does not require custom authentication, select this option. • *Additional options*—Authentication options for installed plug-ins can also be selected. See Authentication for more information. If you installed a 3rd party user authentication plug-in (for example, LDAP), this option will display. If this user should use custom authentication, select the plug-in option. See Authentication for more information.

	Note: *For the TeamConnectAdmin and System user accounts, the only option is Standard TeamConnect and cannot be changed.* ***Note:*** *If a custom authentication type, such as NTLM authentication, is selected in the Authentication drop-down list, the* ***Password*** *field will not display. In addition, if the system's default authentication is set to a custom authentication type, such as NTLM, and the user's Authentication is set to (System Default), the* ***Password*** *field will not display.*
Account is active	Selecting this check-box enables the account. If you remove the checkmark to disable a user account, the record remains in the system. Recommended for staff on vacation or on leave of absence. Users with disabled user accounts: • Cannot log into TeamConnect. • Do not display in the list of available users in drop-down list and Search Module fields (for example, for assignees, attendees). • Do not receive any approval requests if they are stop members in other routes.
Set expiration date	To disable the account on a specific date, select this check-box and enter a date. Recommended for temporary employees, as they are not be able to log into TeamConnect after the expiration date.
User must change password at next log in	Select this check-box to prompt the user to change his or her password on the next application login. ***Note:*** *Make sure that the date range between the current date and date set in this field is larger than the* ***System Settings***, ***Password Policy*** *page's* ***Maximum Age*** *field value. Otherwise the user will not be able to change his/her password.* See Defining the User Password Policy.
Enable assistive technology	Select this check-box to enable Accessible Mode for the vision impaired. This setting currently applies to the Designer application that is available if the user has rights to any rights for solution developers. Changes take effect the next time the user logs into the system. For more information on Accessibility in TeamConnect, see the User Guide.

1.2.4.4.1 Creating a User Using a Template

You can use an existing user like a template. You can create a copy of a user record and then edit some fields to create a new user.

Field values from the following original user's pages are copied to the new record:

- **General** page
- **Group Memberships** page
- **System Rights** page
- **Category Rights** page
- **Tool Rights** page

To create a user using a template

1. Search for a user to copy, and open it.
2. Click **Create a Copy**.
3. Edit the user as required. For example, change the **User Name** and **Password**.
4. Click a save option.

Field values from the original user's **History** page are not copied to the new user.

1.2.4.4.2 Example for Creating a Limited-Privilege User

There may be individuals for whom you want to create user accounts but only with restricted access to a select number or type of records. For example, if your company has external vendors, you may want to provide the vendors with access to the specific project records with which they are involved.

Rights to work with either specific record types or all record types are set at the group level. At the user level, there is an additional setting (User type) that determines whether the user has access to all public records or limited access to records.

Note: *If you need to allow limited-privilege users to perform tasks not normally available to them, such as the ability to approve an invoice, there must be a rule written that gives them record level rights to the invoice so that they can see it and approve it.*

To create a limited-privilege user

1. Create users. See Creating or Editing Users.
2. For each user, from the **General** page, **User** type drop-down list, select **Limited-Privilege**.
3. Open the project record to grant access rights to (for this group).
4. Click **Security** from the left pane of the project.
5. To assign the user rights to search, view, or open the project, from the **User Rights** section, click **Edit**.

6. Click **Add User Rights**.
7. From the **Allow** drop-down list, select **Allow**.
8. From the **Users** drop-down list, select the user.
9. Click a save option.

1.2.4.5 Activating and Inactivating a User

From a user's **General** page, you can activate or inactivate the user's account.

To activate or inactivate a user

1. Search for a user and open it.
2. To activate a user, select the **Account is active** check-box.
3. To inactivate a user, clear the **Account is active** check-box.
4. To set a future date when the user's account will be disabled, select the **Set expiration date** check-box. Click the Calendar icon to select a date.
5. Click a save option.

1.2.4.6 Prompting Users to Change Their Passwords

From a user's **General** page, you can enable a prompt that requires the user to change their password to enforce security standards, for example, if you assign a generic password to new users.

To prompt users to change their passwords

1. Search for a user and open the user's account.
2. Select the **User must change password at next log in** check-box to prompt the user to change his or her password on the next TeamConnect login.

   Make sure that the time span between the current date and date set in this field is larger than the **Maximum Age** field value on the **Security** page of the **Admin Settings**. Otherwise the user will not be able to change his/her password. See Defining the User Password Policy.
3. Click a save option.

1.2.4.7 Editing or Viewing a User's Preferences

A user can set individual application preferences. In addition, an administrator with appropriate rights to user records can view or edit a user's preferences from the user record's **General** page.

To edit or view a user's Preferences

1. Search for a user and open the user's account.
2. From the **General** page, click **Preferences**.

   The user's **Preferences** page opens.

   For information about field descriptions, from the User Guide or help, search for Personalizing Your Settings.

1.2.4.8 Unlocking User Accounts

To guard against unauthorized access, you can limit the number of failed login attempts on the **Password Policy** page of the Admin Settings area. For details, see Security Settings.

When the **Enable User Lockout** check-box is selected, users have a specific number of attempts within a time interval to successfully enter a password for their user name. If users exhaust their number of attempts, TeamConnect locks the user account, preventing login attempts.

Whether user accounts are locked due to unauthorized individuals attempting to access the system or legitimate users who enter incorrect passwords, you can unlock user accounts if you have Update rights to user accounts.

To unlock a user account

1. Search for a user and open the user's account.
2. Clear the **Account is Locked** check-box.

   This check-box only appears on the **General** tab when a user account is locked.
3. Click a save option.

The user account is unlocked and user access is restored. The **Account is Locked** check-box is removed from the **General** tab of the user account.

When an account is locked, TeamConnect does not attempt to assign a new password. If desired, you can assign one (for example, if a user cannot remember the current password) or prompt the user to change the password on his or her next login. See Creating or Editing Users.

1.2.4.9 Changing a User's Group Membership

From the **Group Membership** page, add users to groups or remove users from groups.

To change a user's group membership

1. Search for a user and open the user's account.
2. Click the **Group Memberships** link from the left pane.
3. To add the user to a group:

   a. (optional) Click **Add New Item**.

b. From the corresponding **Group** drop-down list, select the group to add membership.

c. (optional) To apply the group's object views as this user's default, select the corresponding **Primary** button.

4. To remove the user from a group:

a. Select the check-box to the left of the group to remove membership.

b. Click **Remove**.

5. Click a save option.

Users Group Membership Page Field Descriptions

Label	Description
Group Membership Row	For each group, the following fields apply: • **Line**—Read-only. Displays row number. • **Group**—Select a group from the drop-down list to add or remove the current user to/from the member list. • **Primary**—Select one group's Primary button for the user. The user's default object view is determined by the primary group assigned. If the user belongs to multiple groups, the first group will be selected as Primary by default. • **Action**—Click the icon to edit an existing user's account.
Remove	To remove a user from the current group, select the check-box to the left of the user's row and click the **Remove** button.
Add Another Item	To add a blank Group Membership row, click the **Add Another Item** button and then select a group (see the **Group Membership row** description above).

1.2.4.10 Assigning or Viewing User System Rights

From a user account's **System Rights** page, you can do the following:

- (For users created in TeamConnect version 2.x or earlier) Assign and view rights to records, application areas, and application features at the user account level.

  In addition, view rights to records, application areas, and application features inherited from the users' member group(s).

- (For users created in TeamConnect 3.x) View rights to records, application areas, and application features inherited from the users' member group(s). For these users, you cannot assign or manage record rights at the user level. You must edit a member group's record rights. For more information, see Assigning or Viewing Group System Rights.

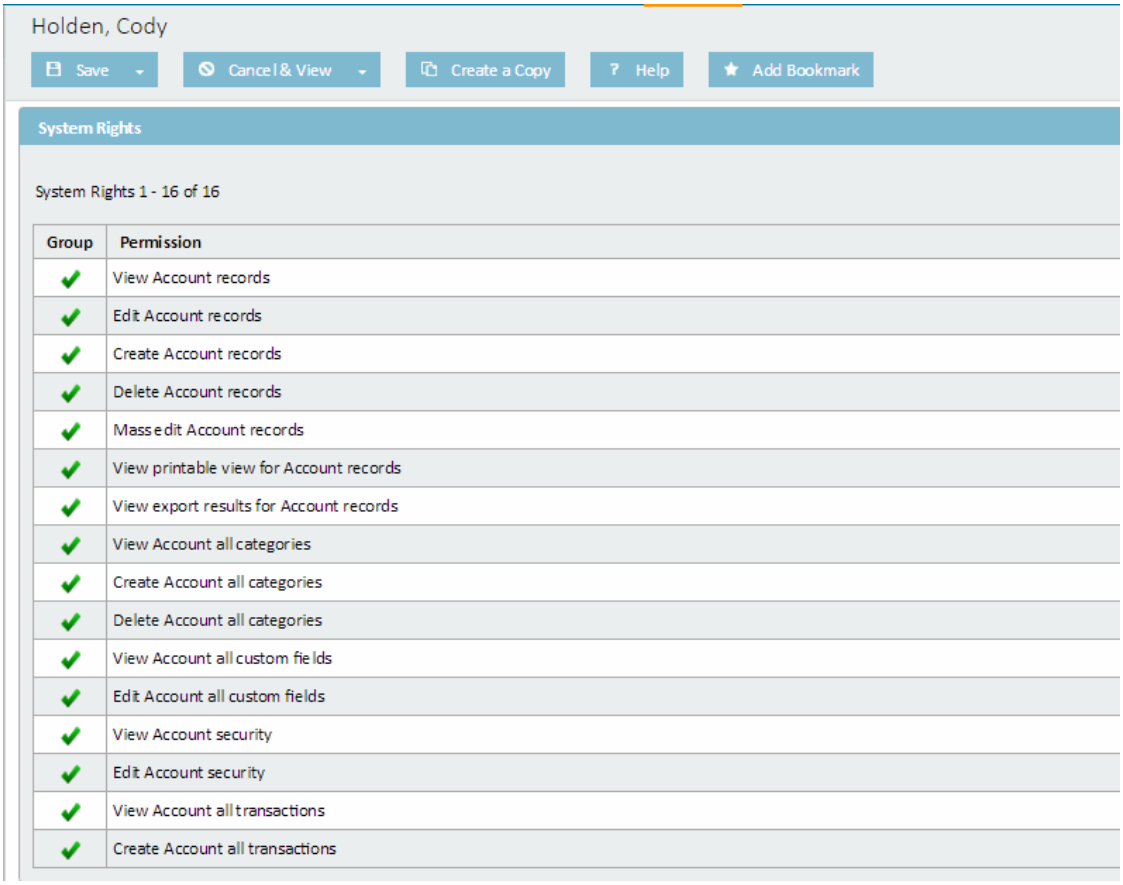
(For users created in TeamConnect 2.5 SP4 or earlier) You can assign rights that apply:

- Globally—If you expect to enable rights across multiple record types or multiple application areas, work with these types of rights to save time. Global rights are organized into three groups: User rights, Admin rights, and Setup rights.

  For example, if you select the View drop-down list, User Rights option then the resulting page you can assign rights to view all contact records, view all document records, view all project records, etc., with one button click.

- Individually—If you expect to enable rights for a limited number of record types (for example, allow access to a couple record types), work with these types of rights.

  For example, if you select the View drop-down list, Contacts option then from the resulting page you can assign more granular level rights such as View Contact records, Edit Contact records, Create Contact records.



User Record - System Rights Page for Contact Rights (Edit Mode for Users Created in TeamConnect 2.5 SP4 or Earlier)

Note: *In the screenshot above, the check-boxes under the* ***Group*** *column are read-only.*

Rights are cumulative. If a user has rights assigned at the user-account level and rights inherited from member groups, the user's rights are the sum of user rights and member group rights. If a user is a member of multiple groups then the user inherits all rights assigned to all groups.

If you assign global rights to a user and later add a custom object (record type), category, or custom fields, it is recommended to manually grant access rights to the new object, category, or custom fields.

To assign or view individual record rights

1. Search for a user account and open it.
2. To change record rights, from the left navigation pane, click **System Rights**.
3. From the **View** drop-down list, select an option (for example, Contacts).
4. (For users created in TeamConnect 2.5 SP4 or earlier only) You can do one or more of the following:
   - To assign a specific record or area right, select the check-box for the permission under the **User** column.
   - To unassign a specific record or area right, clear the check-box for the permission under the **User** column.
   - If you are viewing existing rights, the **User** column displays rights assigned at the user account level. The **Group** column displays rights inherited from member groups.
5. (For users created in TeamConnect 3.x) The **Group** column displays rights currently inherited from member groups.

   The **System Rights** page for a user created in TeamConnect 3.x does not display a **User** column.
6. Click a save option.

User System Rights Page Field Descriptions

Field descriptions for specific records or areas are described in:

- Rights for End-users
- Rights for Administrators
- Rights for Solution Developers

User System Right Page Fields

Label	Description
View drop-down list	A list of record types and application areas to which you can assign access rights, for example, system settings, object definitions, etc. After selecting a list option, the workspace is updated with a list of rights specific to that option. For example, if you select Contacts, the rights list displays only rights for working with contact records.

Action	(Available only for users migrated from TeamConnect 2.5 SP4 or earlier. Also only available in Edit view when a global rights option is selected from the **View** menu, such as **User Rights**, **Admin Rights**, or **Setup Rights**) Displays both of the following per permission: • **Select**—Enables all permissions for all child records under this rights group. The corresponding rights will be applied at the user account level. • **Unselect**—Disables all permissions for all child records under this rights group. The corresponding rights will be applied at the user account level.
Permission	The available Permissions list items depends on the type of option selected from the **View** drop-down list. • If a global rights option is selected from the **View** drop-down list (for example, User Rights, Admin Rights, Setup Rights), permissions include the following: **View all record types**—To grant search and read rights for records of this type, select the **View all record types** check-box. **Edit all record types**—To grant rights to edit records of this type, select the **Edit all record types** check-box. **Create all record types**—To grant rights to create records of this type, select the **Create all record types** check-box. **Delete all record types**—To grant rights to delete records of this type, select the **Delete all record types** check-box. **Perform all other actions** ***Note:*** *See Understanding Rights, Rights for End-users, Rights for Administrators, and Rights for Solution Developers.* • If an individual rights option is selected from the **View** drop-down list (for example, Contacts, Documents, etc.), permissions like the following are available: **View** *Contact* **records** **Edit** *Contact* **records** **Create** *Contact* **records** **Delete** *Contact* **records** **View** *Contact* **all categories** **Create** *Contact* **all categories** **Delete** *Contact* **all categories** **View** *Contact* **all custom fields** **Edit** *Contact* **all custom fields**

	Note: *The list above provides examples of permissions related to individual record types but is not all-inclusive. For comprehensive lists of permissions according to record type, see System Record Rights.*
Group	Display values indicate which rights are currently assigned from member group(s). The available Permissions list items depends on the type of option selected from the **View** drop-down list. • If a global rights option is selected from the **View** drop-down list (for example, User Rights, Admin Rights, Setup Rights), one of the following may display: ○ **All rights selected**—Indicates the permission was enabled globally. ○ **Some rights selected**—Indicates that permissions for the child record types were enabled individually, resulting in some permissions being disabled. ○ **No rights selected**—Indicates that no permissions for the child record types were enabled. • If an individual rights option is selected from the **View** drop-down list (for example, Contacts, Documents, etc.), one of the following displays: ○ A read-only green check-box for individual record rights that are currently assigned to a member group. ○ A read-only empty check-box for individual record rights that are currently unassigned to all member groups.

1.2.4.10.1 Assigning or Viewing Global User Rights for a User

From a user's **System Rights** page, you can assign or view rights typically associated with end-user functions using a global User Rights view. This option allows for quick assignment of access rights to multiple record types or application areas that end-users typically use.

Note: *In this topic, global User Rights refers to Permissions available when you select the **User Rights** option from the **View** drop-down list of a user account's **System Rights** page.*

Note: *Assigning global User rights is only supported for users migrated from TeamConnect 2.5 SP4 or earlier.*

To assign or view global User Rights for a user

1. Search for a user account and open it.
2. From the left navigation pane, click **System Rights**.

3. From the **View** drop-down list, select **User Rights**. To assign rights, do one or more of the following:
   - To assign view rights to all records from the User application area, associated categories and custom fields, associated pages for the records (such as Security), click **Select** next to the **View All Records Permission**.
   - To assign edit rights to all records from the User application area, associated categories and custom fields, associated pages for the records (such as Security), click **Select** next to the **Edit All Records Permission**.
   - To assign create rights to all records from the User application area, associated categories and custom fields, associated pages for the records (such as Security), click **Select** next to the **Create All Records Permission**.
   - To assign delete rights to all records from the User application area, associated categories and custom fields, associated pages for the records (such as Security), click **Select** next to the **Delete All Records Permission**.
   - To assign any remaining rights to all records from the User application area, associated categories and custom fields, associated pages for the records (such as Security), click **Select** next to the **Perform other actions Permission**.
4. If you are viewing currently assigned rights, the status of enabled rights per permission displays under a column:
   - **User**—Displays status of rights assigned at the user account level.
   - **Group**—Displays status of rights assigned at the member groups level.

   For more information, see User System Rights Page Field Descriptions.
5. Click a save option.

   For more information about the granular record-level rights bundled under a global User Rights permission, see Results from Assigning Global User Rights. Information presented in the data tables apply to users and groups.

1.2.4.10.2 Assigning or Viewing Global Admin Rights for a User

From a user's **System Rights** page, you can assign rights typically associated with system administrator functions using a global Admin Rights view. This option allows for quick assignment of access rights to multiple record types or application areas that system or business administrators typically use.

Note: *In this topic, global Admin Rights refers to Permissions available when you select the* ***Admin Rights*** *option from the* ***View*** *drop-down list of a user account's* ***System Rights*** *page.*

Note: *Assigning global Admin rights is only supported for users migrated from TeamConnect 2.5 SP4 or earlier.*

To assign or view global Admin Rights for a user

1. Search for a user account and open it.
2. From the left navigation pane, click **System Rights**.

   From the **View** drop-down list, select **Admin Rights**.

   - To assign view rights to all records from the Admin application area, associated pages for the records (such as Security), click **Select** next to the **All Admin View Rights Permission**.
   - To assign edit rights to all records from the Admin application area, associated pages for the records (such as Security), click **Select** next to the **All Admin Edit Rights Permission**.
   - To assign create rights to all records from the Admin application area, associated pages for the records (such as Security), click **Select** next to the **All Admin Create Rights Permission**.
   - To assign delete rights to all records from the Admin application area, associated pages for the records (such as Security), click **Select** next to the **All Admin Delete Rights Permission**.

     See Assigning or Viewing Group System Rights for information about assigning groups of rights to end-users, administrators, or solution developers.
3. If you are viewing currently assigned rights, the status of enabled rights per permission displays under a column:
   - **User**—Displays status of rights assigned at the user account level.
   - **Group**—Displays status of rights assigned at the member groups level.

     For more information, see User System Rights Page Field Descriptions.
4. Click a save option.

   For more information about the granular record-level rights bundled under a global Admin Rights permission, see Results from Assigning Global Admin Rights. Information presented in the data tables apply to users and groups.

1.2.4.10.3 Assigning or Viewing Global Setup Rights for a User

From a user's **System Rights** page, you can assign rights typically associated with solution developer functions using a global Setup Rights view. This option allows for quick assignment of access rights to multiple record types or application areas that solution developers typically use.

Note: *In this topic, global Setup Rights refers to Permissions available when you select the* ***Setup Rights*** *option from the* ***View*** *drop-down list of a group account's* ***System Rights*** *page.*

Note: *Assigning global Setup rights is only supported for users migrated from TeamConnect 2.5 SP4 or earlier.*

To assign or view global Setup Rights for a user

1. Search for a user account and open it.
2. From the left navigation pane, click **System Rights**.

   From the **View** drop-down list, select **Setup Rights**.

   - To assign view rights to all records from the Designer (Setup) application area, associated pages for the records (such as Security), click **Select** next to the **All setup view rights Permission**.
   - To assign edit rights to all records from the Designer (Setup) application area, associated pages for the records (such as Security), click **Select** next to the **All setup edit rights Permission**.
   - To assign create rights to all records from the Designer (Setup) application area, associated pages for the records (such as Security), click **Select** next to the **All setup create rights Permission**.
   - To assign delete rights to all records from the Designer (Setup) application area, associated pages for the records (such as Security), click **Select** next to the **All setup delete rights Permission**.

     See Assigning or Viewing Group System Rights for information about assigning groups of rights to end-users, solution developers, or administrators.
3. If you are viewing currently assigned rights, the status of enabled rights per permission displays under a column:

   - **User**—Displays status of rights assigned at the user account level.
   - **Group**—Displays status of rights assigned at the member groups level.

     For more information, see User System Rights Page Field Descriptions.
4. Click a save option.

   For more information about the granular record-level rights bundled under a global Setup Rights permission, see Results from Assigning Global Setup Rights. Information presented in the data tables apply to users and groups.

1.2.4.11 Assigning or Viewing User Category Rights

From a user account's **Category Rights** page, you can do the following:

- (For users created in TeamConnect 2.5 SP4 or earlier) You can assign or view rights to categories and custom fields.

  Afterward, the user will be able to view and work with the categories (for example, add and remove categories from a record type) and custom fields (for example, populate or edit the field value).
- (For users created in TeamConnect 3.x) You can view rights to categories and custom fields inherited from the users' member group(s). For these users, you cannot assign or manage category or custom field rights at the user account level. You must edit a member group's category or custom field rights. For more information, see Assigning Group Category and Custom Field Rights.

(For users created in TeamConnect 2.5 SP4 or earlier) You can assign rights that apply:

- Globally—If you expect to enable rights to work with most categories and custom fields across multiple record types, work with these types of rights to save time.

  For example, if you select the **View** drop-down list, **User Rights** option then on the resulting page you can assign rights to view all categories (for all contact records, all document records, all project records, etc.) with one button click.

  Note: *In the screenshot above, the permission status messages under the* ***Group*** *column are read-only and indicate which permissions are inherited from a member group.*

- Individually—If you expect to enable more restricted access to categories and custom fields, you can set more granular level access per record type and per specific category/custom field.

  Note: *In the screenshot above, the check-boxes under the* ***Group*** *column are read-only and indicate which permissions are inherited from a member group.*

To assign or view category and custom field rights

1. Search for a user account and open it.
2. To change rights for categories and custom fields, from the left navigation pane, click **Category Rights**. See the appendix, Rights for End-users for additional information about general rights for categories and custom fields for each record type.
3. (For users created in TeamConnect 2.5 SP4 or earlier only) To assign global category or custom field rights for all record types, do the following:
   - From the View drop-down list, select **User Rights**.
   - From the resulting rights list, click the **Select** button for the following permission rows:
     - **View all categories**—Allows access to all records', **Categories** pages.
     - **Add all categories**—Allows addition or selection of all available categories from all records', **Categories** pages.
     - **Remove all categories**—Allows removal or clearing of all categories from all records', **Categories** pages.
     - **View all custom fields**—Allows access to custom fields associated with any categories from all records', **Details** pages.
     - **Edit all custom fields**—Allows data entry or changes for custom fields values associated with any categories from all records', **Details** pages.

       Afterward, all rights for categories and custom fields of all record types will be assigned to the user.
4. (For users created in TeamConnect 2.5 SP4 or earlier only) To assign specific category or custom field rights for a specific record type, do the following:
   - From the **View** drop-down list, select a record type. For example, Contacts.

- To assign the following base category rights, select the check-box next to each right:
  - **View** *Contact* **category**—Allows access to contact record, **Categories** page.
  - **Add** *Contact* **category**—Allows addition or selection of all available categories from the contact record, **Categories** page.
  - **Remove** *Contact* **category**—Allows removal or clearing of all categories from the contact record, **Categories** page.
  - **View** *Contact* **custom fields**—Allows access to custom fields associated with any contact categories from the contact record, **Details** page.
  - **Edit** *Contact* **custom fields**—Allows data entry or changes for custom fields values associated with any contact categories from the contact record, **Details** page.

    To assign additional category or custom field rights, select the check-box next to the right.

5. If you are viewing currently assigned rights, the status of enabled rights per permission displays under a column:
   - **User** column—Displays status of rights assigned at the user account level.
   - **Group** column—Displays status of rights assigned at the member groups level.

     For more information, see User System Rights Page Field Descriptions.
6. Click a save option.

1.2.4.12 Assigning or Viewing User Tool Rights

From a user account's **Tool Rights** page, you can do the following:

- (For users created in TeamConnect 2.5 SP4 or earlier) Assign rights to tools. Afterward, the user will be able to view and work with the tools.
- (For users created in TeamConnect 3.x) View tool rights inherited from member group(s). For these users, you cannot assign or manage tool rights at the user account level. You must edit a member group's tool rights. For more information, see Assigning Group Tool Rights.

Note: *In the screenshot above, the check-boxes under the* ***Group*** *column are read-only and indicate which permissions are inherited from a member group.*

Some tools are available from the User application area and other tools are available from the Designer application area.

To assign user tool rights

1. Search for a user and open it.
2. To make tools available, from the left navigation pane, click **Tool Rights**.
3. (For users created in TeamConnect 2.5 SP4 or earlier) You can do the following:

To enable a tool for the user, select the tool's check-box.

To disable a tool, clear the tool's check-box.

4. View tool rights currently inherited from member groups under the **Group** column. A green check-box indicates the permission is enabled.
5. Click a save option.

1.2.4.13 Viewing or Creating User History

From a user's **History** page, you can create a history (containing notes about changes to the user), view a list of related history records, or perform an advanced search for a history.

To create a history for a user

1. Search for a user and open the user's account.
2. Click **History** from the left pane.

   The user's History list page will open. You can click a history **Description** to view its details.
3. Click **New History**.
4. Enter a change **Description**.
5. Click a save option.

1.2.4.14 Deleting a User

When you delete a user, the groups that the user belongs to will not be deleted.

Scenarios that Prevent Deletion

When you try to delete a user, the following scenarios prevent the deletion:

- You are deleting your own user account.
- The user is a Process Manager in a route or an approval process in any status (pending, completed, and so on).
- The user is an approver in an approval process in any status (pending, completed, and so on).
- The user is the last member of a group that has a Process Manager role in an approval rule.

To delete a user account

1. Select the **Admin** tab.
2. Click the **Users** sub-tab link.
3. (optional) From the left navigation pane, select a User list view.

4. Click the link with the user's name.
5. Click **Delete**.

What is Deleted

When you delete a user, the following associated data gets deleted:

- All rights assigned in the Rights, Categories, and Tools tabs of the account.
- Group Membership information.
- Record-level Security tab settings for the user.
- Project assignment entries where this user was selected.
- Password history.
- Home Page copies created for this user.
- History records.

1.2.4.15 Using the User General Page

For a list of pages that belong to a user, see Working with Users.

From the General page, you can perform the following:

- Creating or Editing Users
- Example for Creating a Limited-Privilege User
- Activating and Inactivating a User
- Prompting Users to Change Their Passwords
- Editing or Viewing a User's Preferences

1.3 System Administration

TeamConnect system administration includes the initial configuration of Admin Settings and management of TeamConnect logs.

Admin Settings refers to TeamConnect system settings that are configured by Administrators. Additional system settings are located in the TeamConnect Designer area under System Settings. Both Admin Settings and System Settings are global and apply to all users by default. Certain settings can be customized by users for their individual application sessions.

Managing TeamConnect logs includes viewing TeamConnect log files, changing logging levels (which types of events are logged), and clearing log files. See Appenders for more information about creating appenders and additional log management tasks.

1.3.1 Working with Admin Settings

The Admin Settings area allows you to define or enable global settings according to the business needs of your organization. Admin Settings generally define system behavior for all users.

Admin settings include the following:

- General Admin Settings
- User Interface Settings
- Region Settings
- Calendar Settings
- Documents Settings
- Search Results Settings
- Reporting Settings
- Security Settings
- Email Settings
- Notification Settings
- Invoices Settings
- Maintenance Settings
- Connections Settings
- Admin Settings History
- About TeamConnect

Admin Settings vs. User Preferences

Users can override the following Admin Settings from their Preferences pages:

- Date and time formats on the Admin Settings **General** page:
  - Date and Time formats in Read-only mode
  - Date and Time formats in Edit mode
  - Time zone
- Search result settings on the Admin Settings **General** page:
  - Number of results per page
  - Number of columns of contact results per page
  - What to do when there is only one record returned by a search
- **User Interface** page:

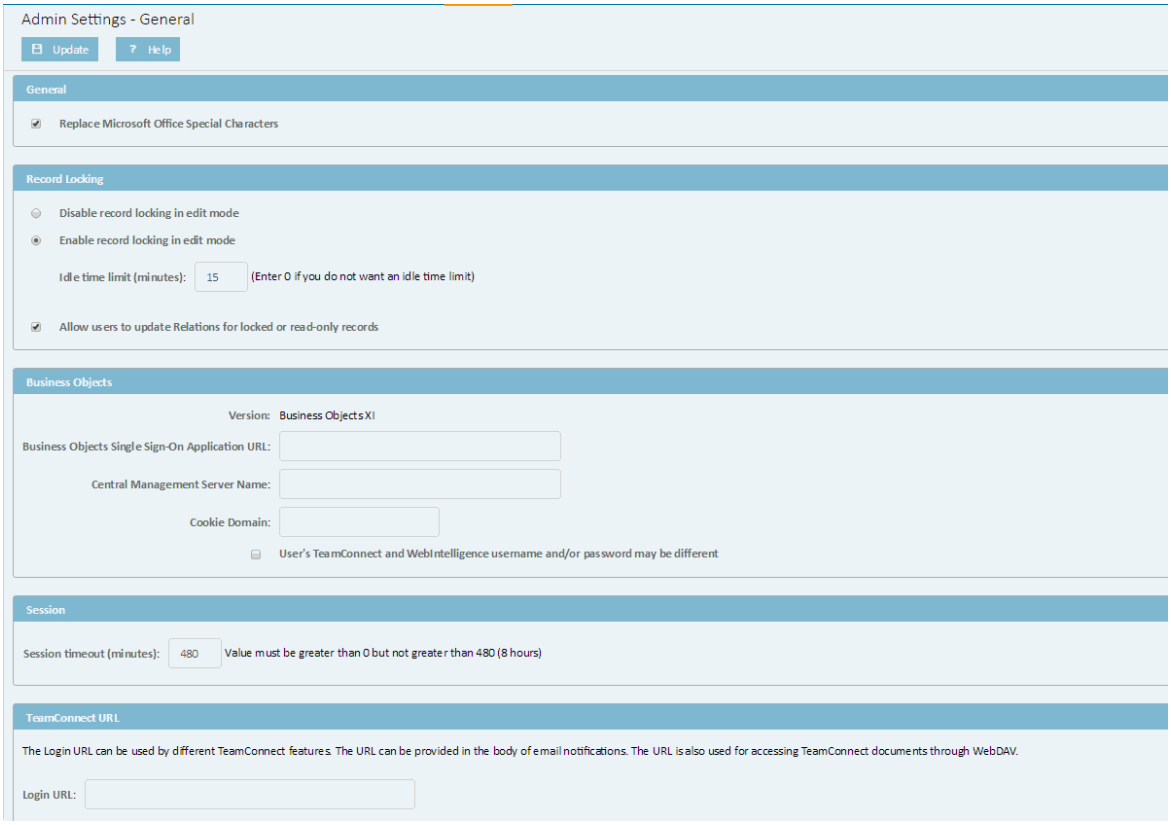
  All appearance settings can be set by each user. For example, screen colors and fonts.

1.3.1.1 General Admin Settings

You can configure the following Admin Settings from the General page:

- (For the TeamConnect Designer area only) Working with documents using applets.
- Record locking—Configure the record locking behavior for scenarios where multiple users may try to update the same TeamConnect file.
- WebIntelligence Single sign-on—Allows TeamConnect users to click reports views from TeamConnect without having to enter Business Objects WebIntelligence login information.

A conceptual overview of the settings follows. If you prefer to skip to the procedure for configuring the settings, see Setting Up General Settings.



Admin Settings - General Page

1.3.1.1.1 Record Locking

The Record Locking settings determine how an open record can be updated. Options include:

- **Not locking records—**Allows multiple users to view a record that is already open, but only the first user who saves the record will have record changes saved.
- **Locking records—**Prevents other users from updating an open record. Record locking only applies to system objects and custom objects for end-users (see Release Edit Locks Right). record locking does not apply to user or group records.

  Setting a lock time-out—Prevents other users from updating an open record. After the current record owner has been idle for a specified time duration, the record will be unlocked.

In addition, you can enable or disable rights to update the **Relations** tab of a locked contact or project record.

Optionally, you can assign rights to unlock records from Group rights.

1.3.1.1.2 BusinessObjects Web Intelligence Single Sign-on

If your company uses BusinessObjects Web Intelligence to generate reports based on TeamConnect data, you can enable BusinessObjects Web Intelligence single sign-on (BOSS) from TeamConnect. Afterward, when a user tries to view a report from TeamConnect, they do not need to type their WebIntelligence username and password.

Currently, the single sign-on capability can be configured for BusinessObjects Web Intelligence XI.

When TeamConnect and Web Intelligence User Names and Passwords Differ

By default, TeamConnect passwords and user names are sent to WebIntelligence for authentication purposes. If the username and password combinations do not match, when the user attempts to run a report, an error page is displayed with several options, one of which is the option to log in to Business Objects manually.

To avoid the manual Web Intelligence login, from Admin Settings, for the General page, select the **User's TeamConnect and WebIntelligence username and/or password may be different** check-box. Also let the users know they must enter their Web Intelligence login information from the **Preferences** area, **Other Settings** page.

Setting up Business Objects WebIntelligence Support

The following is an overview of steps to set up Business Objects WebIntelligence support:

1. Deploy and configure the Business Objects Single Sign-on (BOSS) web application. See the BusinessObjects documentation and Business Objects Single Sign-on in the Installation Help for more information.

   Note: *The BusinessObjects Web Intelligence administrator should configure the single sign-on capability.*

2. A solution developer must enable user access to Business Objects reports from TeamConnect home pages.
3. Configure BusinessObjects Web Intelligence settings from TeamConnect Admin Settings.
4. If any user's TeamConnect user and password combination is different from their BusinessObjects Web Intelligence user and password combination, notify users that they need to update their User **Preferences**, **Other Settings** page.

Points to Remember

- If you upgrade from Business Objects 5.x or 6.x to Business Objects XI, make sure all WebIntelligence URLs in portal panes are updated accordingly.
- Sessions on the WebIntelligence server are created only when users click the WebIntelligence URLs in their home pages, not during the TeamConnect login.

1.3.1.1.3 Setting Up General Settings

The following steps describe how to configure the **General** page from Admin Settings. Field descriptions are provided in a table below.

After you update and save the **General** settings page, the changes take effect for users automatically.

To set up General settings

1. Select the **Admin** tab.
2. Click the **Admin Settings** link under the tab bar.
3. The **General** page should display. Otherwise click the **General** link in the left pane.
4. Edit the fields based on descriptions in the Admin Settings - General Page fields table.
5. Click **Update**.

Admin Settings - General Page Field Descriptions

Section	Field Names and Descriptions	Default Value
General	**Replace Microsoft Office Special Characters** To enable pasting special characters from Microsoft Office documents, select the check-box. If the check-box is cleared, field values containing Microsoft office special characters may not display properly in the user interface but the value stored in the database will be accurate. ***Note:*** *For existing records containing Microsoft Office special characters in field values, you need to create a script to update values manually.*	**Replace Microsoft Office Special Characters—**Disabled (check-box cleared)
Record Locking	Select one of the following: • **Disable record locking in edit mode**—Allows multiple users to edit the same record simultaneously. The first changes checked in by a user will be saved. Subsequent attempts to check in record changes will trigger warnings that the Document has changed.	The following are enabled: • Enable record locking in edit mode • The **Idle time limit (minutes)** is active and set to **15**. • Allow users to update Relations for

	• **Enable record locking in edit mode**—Prevents multiple users from editing the same Document simultaneously. If you selected **Enable record locking in edit mode**, you can type the **Idle time limit (minutes)**, which is the maximum time length after which a record that is locked without any changes saved will become unlocked. To allow users to update the Relations tab for locked records, check **Allow users to update Relations for locked or read-only records**. For more information, see Record Locking.	locked or read-only records
Business Objects WebIntelligence Settings for version XI	The following descriptions apply if you are using Business Objects XI: • **Business Objects Single Sign-on Application URL**—The fully qualified URL of the Business Objects Single Sign-on web application that was deployed and configured as part of the TeamConnect installation. The URL must include the domain name. • **Central Management Server Name**—The name of the central management server. You must provide the name, not the IP address. • **Cookie Domain**—If BOSS is deployed on a different server node than the WebIntelligence node, you must provide the name of the cookie domain. • **User's TeamConnect and WebIntelligence username and/or password may be different**—See BusinessObjects Web Intelligence Single Sign-on. • **Version**—Select Business Objects XI For more information, see BusinessObjects Web Intelligence Single Sign-on.	
Session	Enter a numeric value (minutes) after which an inactive user's session will time out. Afterward, the user will need to log in to TeamConnect	60 minutes

	again. If a negative value is entered, user sessions will not time out. ***Note:*** *If your application server has an application session timeout configuration, the TeamConnect* ***Session Timeout*** *value will override the application server timeout setting.* If a user is running both a User application area browser and a Designer application area browser, the Designer browser session starts when the browser is opened. As a result, it is possible for the User browser session to time out before the Designer browser session.	
TeamConnect URL	**Login URL**—Enter the TeamConnect login URL. For example: *http://host_name:8001/teamconnect3/*login (where you need to replace host_name with the IP address or application server name; replace 8001 with the port running the TeamConnect application; replace teamconnect3 with the TeamConnect application name) ***Important:*** *If you use the WebDAV feature to associate Document folders with email messages, you must put a valid URL in the* ***Login URL*** *field.* For email notifications, this URL is sent in the body of the email. This field is also required if your company uses HTTPS for the login URL, if you use a proxy server with TeamConnect, or if you use a different application server to log in to TeamConnect. ***Note:*** *You must include* ***/login*** *at the end of the URL. It is also recommended to type the public IP address, not the local IP address of the host server.*	Configure the TeamConnect URL in the TeamConnect system settings

1.3.1.2 User Interface Settings

You can configure the following Admin Settings from the **User Interface** page:

- Company Settings—Enable custom logos and alternate texts and select color profiles for company-wide UI customization. ***Note:*** *The Color Profile option will determine the* ***Use System Color*** *preference for all users.*
- Button Defaults—Set the default Save Button and default Cancel button options (e.g., Save vs. Save & View).
- Custom Color Profile—Select a designed custom color profile.
- Batch Display Settings—Move the **Action** column and its buttons from the right of the display to the left of the display.
- User selection—For certain fields that are populated by user or contact names, you can choose the selection format (drop-down list or search).
- Login screen Message—Text that displays on the login page. For example, a welcome message.

A conceptual overview of the settings follows. If you prefer to skip to the procedure for configuring the settings, see Setting up the User Interface.

1.3.1.2.1 Custom Logo

If you choose to replace the default company logo with a custom logo, the graphic in the upper left of application pages (after login) will be changed.

Note: *For best appearance, use custom logos that are 50 pixels or less in height.*

1.3.1.2.2 Color Profile Administration

Beginning with TeamConnect 5.0, team administrators are able to further customize TeamConnect for their company through color profile administration.

Custom profile color schemes can be designed by an administrator and made available to all users. While regular TeamConnect user preferences on color profiles will trump color profiles set by administrators, administrators retain control over what selections are made available.

Developing a Custom Color Profile

The full process for developing custom profiles is as follows:

1. Right-click the LESS Template File Example provided on step 2 and click **Save Link As..** or **Save Target As...**
2. Save the file locally with your desired template name. Ensure that it maintains the ".less" extension.

Note: *You may need to select 'All Files' from the Save as Type dropdown and manually enter the '.less' extension after the file name in the File name entry field before saving.*

LESS Template Link	TCE Version Introduced	Additions from Initial Template
Initial LESS Template File Example	TeamConnect 5.0	N/A
LESS Template File Example - 5.0.1	TeamConnect 5.0.1	Now supports custom colors for top navigation bar, block titles, and left navigation bar.

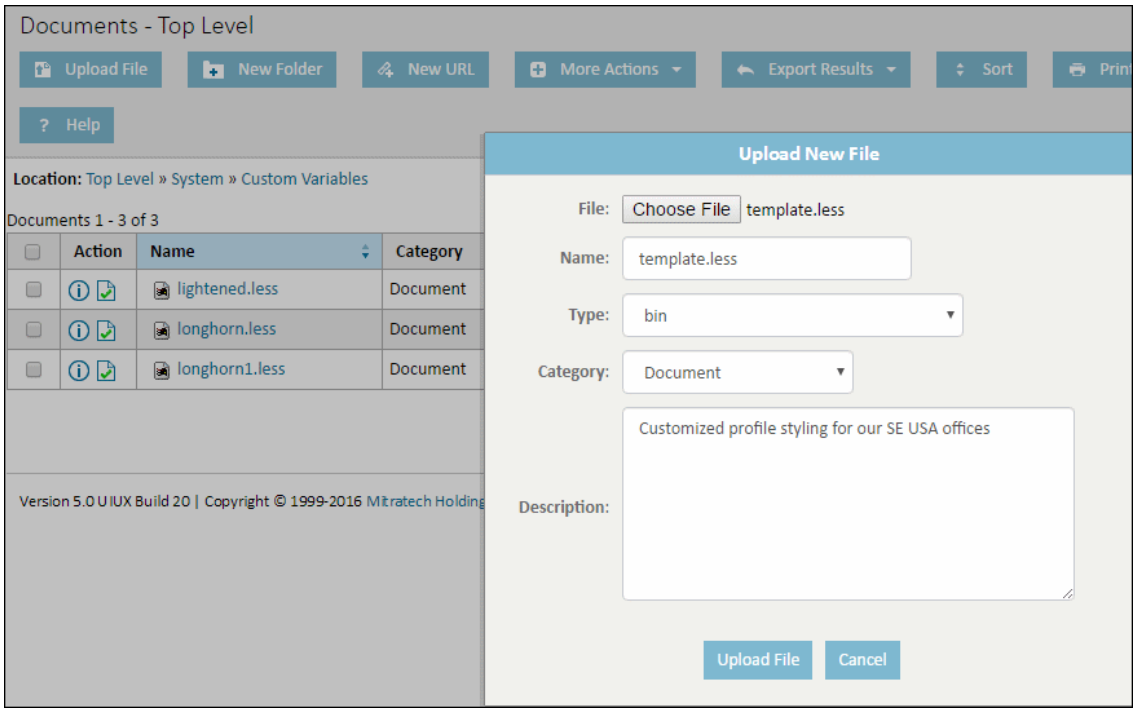
3. Edit the LESS file to your desired color specifications with your favorite text editor (e.g. Notepad++, Sublime, etc.). Colors are determined via hex codes. Hex codes color pickers can be found on several web sites, including the w3schools color picker. ***Important:*** *Please review the Best Practices for Custom Color Profile Editing below to ensure compatibility with TeamConnect.*
4. Save the new LESS file, making sure that you do not have any spaces or special characters in the name.

Uploading a LESS file

Administrators can upload a new LESS file two ways. One method is using the **Upload a new Color Profile** button on the **Company Settings** block of **Admin Settings>User Interface.**

Alternatively, users can upload LESS files by following these steps:

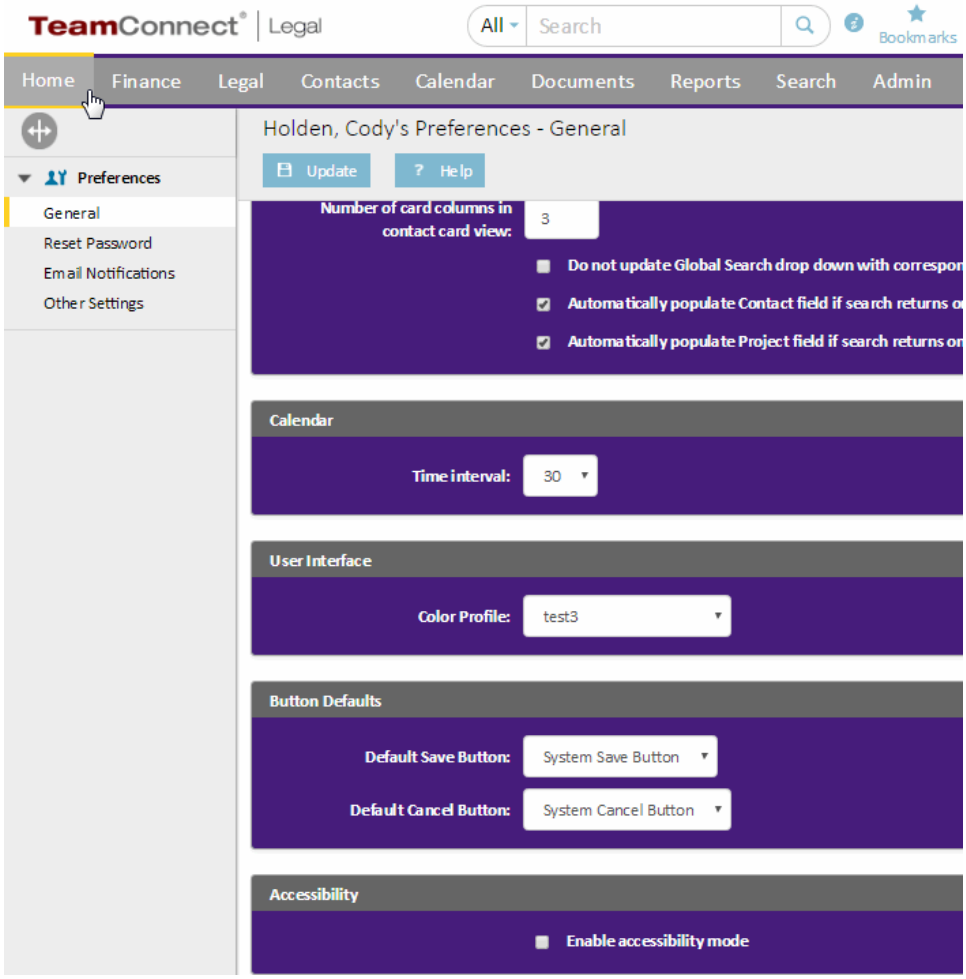
1. Select the **Documents** tab from the top navigation bar.
2. Click **Top Level** from the sidebar to view document folder structure.
3. Click **System**.
4. Click **Custom Variables.** This Custom Variables folder is only for uploading LESS files. ***Note:*** *The Custom Styles folder is also new as of TeamConnect 5.0. For more information on the Custom Styles folder, see step 10 of this procedural.*
5. Once inside the **Custom Variables** folder, click the **Upload File** button. Select your LESS file. The type field can be set to **bin**. See the image below for more detail.



Uploading a LESS file to Custom Variables

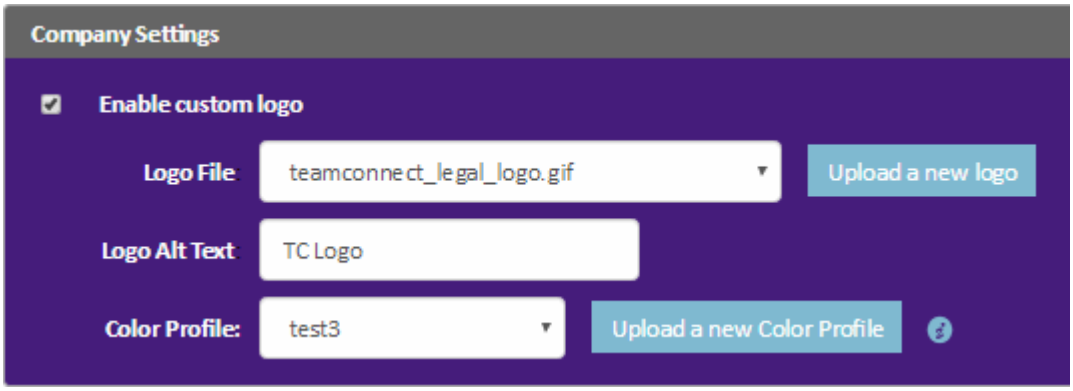
Implementing a new Custom Profile

1. To implement a new color profile, go to the **General** tab of your Preferences. The Preferences link is located under the user icon with your name in the upper-right corner of the application.
2. From the **User Interface** section of the General preferences page, select the **Color Profile** you uploaded.
3. Click the **Update** button to apply these changes.



New LESS File Implementation

Users are able to click the **Use System Color** option within their **Preferences** as a color profile. The choice selected from the **Color Profile** field on the **Company Settings** block of **Admin Settings>User Interface** determines which file is used as this option.



Setting the Use System Color option

Removing Color Profiles

To remove a color profile as a choice for their users, administrators must follow these steps in order for best results:

1. From the **Custom Variables** folder in your **Documents**, select the check-box for the LESS file you would like to remove. **Note:** See the steps for **Uploading a LESS file** for help locating this folder, if necessary.
2. Click the icon to go to the respective page for that file.
3. Click the **Delete** button to remove the LESS file. ***Note:*** *After deleting the LESS file, users will no longer see that option as a choice in their Color Profile selection. However,* ***users who already had this option selected will still see their same profile design.***
4. To entirely remove the color profile, go to the **Custom Styles** folder within the **System** document directory and repeat the same delete process as outlined in steps 2 and 3 of this section. Users with this style in use will be moved to the default color scheme.

If the CSS (**Custom Styles**) file is deleted and the LESS file (**Custom Variables**) remains, the option will persist for users, and the stylesheet will be re-created upon selection.

Best Practices for Custom Color Profile Editing

Color profile designers are encouraged to make edits to their profile, test it, and return to make further edits in lieu of completing it all at once without viewing it in the application. ***Important:*** *If you intend on using the same file name for these revisions and edits, you will need to delete the pre-existing CSS and LESS files for these changes to be reflected. For more information, see Removing Color Profiles within this Color Profile Administration section.*

- @field-text should have good contrast with:
  - @block-header
  - @block-body
  - @table-highlight
  - @button-background
  - @button-background-hover
- @label-color should have good contrast with:
  - @block-body
  - @block-header
  - @table-highlight
- @selected-border should have good contrast with:
  - the white (#FFFFFF) background
- @hover-border should have good contrast with:

- the white (#FFFFFF) background
- the gray (#949494) main navigation bar background

- @main-border should have good contrast with:
  - the white (#FFFFFF) background & text in Calendar
  - the gray (#949494) main navigation bar background
  - the gray (#EDEDED) on a contact card
- @anchor-hover should have good contrast with:
  - the white (#FFFFFF) background
- @anchor-text should have good contrast with:
  - the white (#FFFFFF) background
- @block-body should have good contrast with:
  - @field-text
  - @label-color
  - the white (#FFFFFF) background
- @block-edit-icon should have good contrast with:
  - @block-header
- @table-highlight should have good contrast with:
  - @field-text
  - @table-border
- @button-background should have good contrast with:
  - the gray (#EDEDED) on the left navigation & button bar
  - the white (#FFFFFF) background
- @button-background-hover should have good contrast with:
  - the gray (#EDEDED) on the left navigation & button bar
  - the white (#FFFFFF) background
- @block-border
  - determines the color of the box shadow, so consider the color against the white (#FFFFFF) background
- @table-border should have good contrast with:
  - @table-highlight
  - @block-body

- the white (#FFFFFF) background

- @left-nav-icon should have good contrast with:
  - the gray (#EDEDED) on the left navigation
  - the white (#FFFFFF) background
- @block-header should have good contrast with:
  - the white (#FFFFFF) background & text

Sample values for a High Contrast Theme

- @selected-border #AAA
- @hover-border #6C6C6C
- @mani-border #333
- @anchor-text #333
- @anchor-hover #666
- @block-header #666
- @block-body #EEE
- @block-edit-icon #000
- @table-highlight #BCBCBC
- @button-background #666
- @button-background-hover #333
- @field-text #333
- @block-border #ADADAD
- @table-border #ADADAD
- @label-color #6C6C6C
- @left-nav-icon #333

1.3.1.2.3 Moving Action Buttons

The Action column and buttons appear in areas where you want to copy or edit information. By default, this column appears as the last column on the right of a display and contains action icons, such as edit or copy.

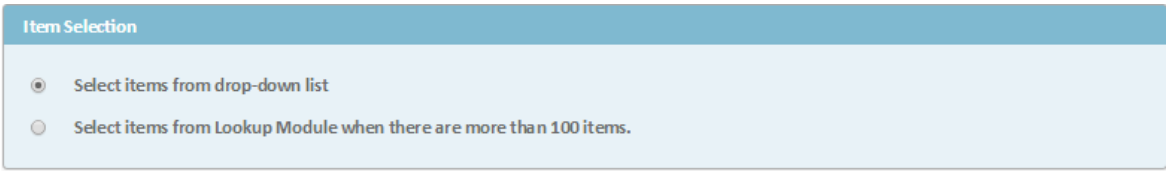
If you prefer, you can move this column and icons to the far right of the display for all users.

1.3.1.2.4 Setting User Selection Options

For certain TeamConnect records, a field may require selection of a TeamConnect user (to populate the field). For example, when adding an assignee to a project or when adding a user to a group account. The **User Selection** block of Admin Settings>User Interface determines whether user records are selected from a drop-down list or from a search module.

- **Select users from drop-down list**—Select this option if your organization does not have too many user names to display in a drop-down list. If your organization has a large number of users, performance can be affected if the drop-down list setting is selected. It may also be inefficient for users to sift through the list of names to find the appropriate user or users to select.

- **Select users from User Search Module**—This option is recommended if there are too many users to effectively display in a drop-down list.



User Selection Options

1.3.1.2.5 Item Selection

This setting determines whether lookup table records are selected from a drop-down list or from a search module.

- **Select items from a drop-down list**—Select this option if your organization always wants to display lookup table items using a drop-down list, no matter how many items there are.
- **Select items from Lookup Module when there are more than 100 items**—This option is recommended if there may be 100 or more items to display. If there are fewer than 100 items to display, the items will show in a drop-down list. If there are 100 or more, a search module with auto-suggest capability is displayed instead.

Note: *The setting that you choose is the default selection for lookup items. The default item selection could still be overridden by developers for specific fields in the design.*

1.3.1.2.6 Setting up the User Interface

The following steps describe how to configure the **User Interface** page from Admin Settings. Field descriptions are provided in a table below.

After you update and save **Admin Settings** from the **User Interface** page, the changes take effect for users automatically.

To set up the User Interface

1. Select the **Admin Settings** link from the **All** button..
2. Click the **User Interface** link in the left pane.
3. Edit the fields based on descriptions in the Admin Settings - User Interface Page fields table.
4. Click **Update**.

Admin Settings - User Interface Page Field Descriptions

Section	Field Names and Descriptions	Default Value

Company Settings	• **Enable custom logo**—Select this check-box to change the logo that appears on the upper left of application pages. If this check-box is cleared, skip the remaining fields under the Company Settings section. • **Logo File**—To upload a logo file, click the **Upload a new logo** link. Browse for the local file and select it. Click OK. ***Note:*** *It is recommended to upload logo files with a maximum height of 50 pixels.* If you have already uploaded a new logo file, you can select it from the Logo File drop-down list. • **Logo Alt Text**—Enter text to display while the browser is loading the image, or if the browser has images turned off. For example, "Company logo". For more information, see Custom Logo. • **Color Profile Administration**—Upload and manage user color profiles. For more information, it is strongly recommended that you view Color Profile Administration.	• Disabled (**Enable custom logo** check-box cleared) • **Logo File—Default** (Mitratech logo)
Button Defaults	Select the default Save and default Cancel buttons from the following options: • Save Changes • Save & Close • Save & View • Save & New • Cancel & Close • Cancel & View	**Save Changes** **Cancel & Close**
Batch Display Settings	• **Position action buttons on the left**—Place a checkmark in this checkbox for the **Action** column in a table of batch entries to display on the left side of the table. Remove the checkmark for the **Action** column to display on right side of the table.	Disabled

User Selection	Select one of the following: • **Select users from drop-down list**—Displays TeamConnect users in a drop-down list on pages requiring user name input. Recommended when the number of user accounts is not large. • **Select users from User Search Module**—Displays a search module on pages requiring user name input. Recommended when the number of user accounts is large. For more information, see Setting User Selection Options.	**Select users from drop-down list**
Item Selection	Select one of the following: • **Select items from a drop-down list**—Displays lookup table items using a drop-down list, no matter how many items there are. • **Select items from Lookup Module when there are more than 100 items**—Displays a drop-down list if there are fewer than 100 items to display. If there are 100 or more, a search module with auto-suggest capability is displayed instead.	**Select users from drop-down list**
All Services Menu Settings	• **Disable Documents in All Services Menu**—Select this check-box to remove the **Documents** link from the All Services Menu and the All Services Portal Pane. You must log back in to TeamConnect after changing this setting for it to take effect. • As of TeamConnect 5.0.1, enabling this checkbox will remove the Documents search view from the left navigation panel. • **Disable History in All Services Menu**—Select this check-box to remove the **History** link from the All Services Menu and the All Services Portal Pane. You must log back in to TeamConnect after changing this setting for it to take effect.	• Disabled (**Disable Documents in All Services Menu** check-box cleared) • Disabled (**Disable History in All Services Menu** check-box cleared)
Login Settings	**Message**—Type a message to display on the login screen. For example, "Welcome to TeamConnect".	

1.3.1.3 Regions and Localization

TeamConnect provides options that let you customize system and custom data for multiple languages and regions. Localized areas include the user interface, and features such as the time and date display. You can localize one or more languages and character sets. Localization key values have been updated in TeamConnect 5.0. Detail on these updates can be found in the online help on the Localization Key Changes page.

Note: *Numbers are not localized and are displayed as Western Arabic numerals, such as 0, 1, 2, 3, 4.*

TeamConnect provides the following options to help you localize data:

- **The Admin Settings Region page**—Lets you select a default locale, and select the way that you want to display the system date, time zone, and year. You can also select your local currency type on this page.
- **Locale Manager tool**—Lets you select, change, and delete one or more locales. Additionally, you can export TeamConnect messages and user interface fields to an Excel spreadsheet, enter translations, and then upload the translated date back into TeamConnect. This process allows international users to view information in their preferred language.

1.3.1.3.1 Region Settings

You can configure the following from the **Region** page:

- Default locale information—The system default locale and how it is applied to individual end users.
- System date format—Choose the default date format for users.
- System time zone and format—Choose the default time zone and time format for users.
- Two-digit year threshold—Choose a Year marker that differentiates when two-digit dates are considered 20th century versus 21st century.
- Default currency—Choose a system currency.

1.3.1.3.1.1 Setting Regional Settings

Use the Admin Settings **Region** page to set your default locale, date and time formats, year threshold, and default currency.

Once you update and save settings on the **Region** page, the changes are visible to users immediately.

To set regional settings

1. Click the **All** button.

2. Click **Admin Settings** under the dropdown bar.
3. In the left pane, click the **Region** link.
4. Select or edit the fields based on descriptions in the Admin Settings - Region Page field table.
5. Click **Update**.

Admin Settings - Region Page Field Descriptions

Section	Field Names and Descriptions
Locale	• **Default Locale**—Select the default locale that controls the language used in the TeamConnect session, as well as the country format options for dates, times and numbers. You can add or remove locale choices for this drop-down list by running the Locale Manager tool. See Working with Locales. Default Locale: English - United States ***Note:*** *A change in default locale will force a page refresh, and will change the values of Date Format and Time Format to values consistent with the new locale.* • **Default users to their browser locale if user locale not set**—Set how the system default locale is applied. ○ If the end user has set a locale in their own Preferences page, that locale will be used during their TeamConnect session. ○ If the end user has not set a locale preference, and this check-box is selected, the locale associated with the user's web browser will be used during their TeamConnect session. ○ If the end user has not set a locale preference, and this check-box is not selected, the system default locale will be used during their TeamConnect session. ○ Default to browser locale: unselected
Date Formats	• **Edit mode date format**—Selecting one of the following (where mm is month, dd is day, and yyyy is year): ○ **mm/dd/yyyy**—For example, 12/25/2000 is December 25, 2000 (default); or ○ **yyyy-mm-dd**—For example, 2000-12-25 • **Read-only mode date format**--Select one of the following (where mm is month, dd is day, and yyyy is year): ***Note:*** *Year values are always displayed in 4 digits.* ○ **mm/dd/yy** (default)—For example, 12/25/05 is December 25, 2000; or

	Note: *In edit-mode, this date will display with the year in 4-digit format (mm/dd/yyyy)* ○ **Month dd, yyyy** (abbreviated)—For example, Dec. 25, 2000; or ○ **Month dd, yyyy**—For example, December 25, 2000; or ○ **Day, Month dd, yyyy**—For example, Sunday, December 25, 2000; or ○ **yyyy-mm-dd**—For example, 2000-12-25 ***Note:*** *These values are based on the default locale, and may be overridden at runtime if the end user has selected a different locale in their Preferences.*
Time Formats	• **Edit mode time format**—Select one of the following: ○ **HH:MM AM/PM** (default)—Where HH is hour, MM is minutes. For example, 05:10 PM; or ○ **Military time**—For example, 17:10. • **Read-only mode time format**—Select one of the following: ○ **HH:MM AM/PM** (default)—Where HH is hour, MM is minutes. For example, 05:10 PM; or ○ **Military time**—For example, 17:10. ○ **Time Zone**—Click the drop-down list to change the system Time Zone. Default is Greenwich Mean Time. These values are based on the default locale, and may be overridden at runtime if the end user has selected a different locale in their Preferences.
Year Threshold	**Two-digit Year Threshold**—Type a two-digit year value for the system to interpret which two-digit year values fall in the 20th century or 21st century. Default is 25. For example, a threshold of 25 would mean that values from 00 to 25 are interpreted as 21st century dates (2000 to 2025). Consequently, values from 26 to 99 are interpreted as 20th century dates (1926 to 1999).
Multi-currency	**Default Currency**—Select the local currency. Default is United States, Dollars. The options within the list are set through the Designer application area.

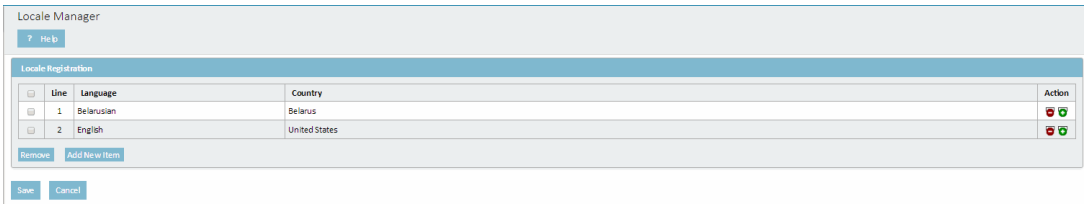
1.3.1.3.2 Working with Locales

Use the **Locale Manager** tool to add, change, or delete locales. Only locales that you add in this tool can be selected by administrators or end users.

To access the Locale Manager tool

1. Click the **All** tab.
2. In the **Tools** section, select **Locale Manager**.

   The Locale Manager tool page opens.



Locale Manager Tool

To add a locale

1. Click **Add New Item**.

   A new row appears in the table of locales.
2. (optional) Click the **Language** drop-down list, and then select a language.
3. Click the **Country** drop-down list, and then select a country.
4. Repeat steps 1 through 3 for as many locales as you need to add.
5. Click **Save**.

   TeamConnect checks for duplicate additions and displays error messages if any are found. If there are no errors, your locales are saved.

To remove a locale

1. Select the check-box next to the locale that you want to remove.
2. Click **Remove**.

   That locale's row disappears from the table of locales.
3. Click **Save**.

If you attempt to remove the locale that is the current Default Locale for the system, you will see an error message.

The table below contains the supported locale languages and the associated country.

Supported Locales/Languages

Language	Country
Albanian	Albania
Belarusian	Belarus
Bulgarian	Bulgaria
Catalan	Spain
Chinese (Simplified)	China
Chinese (Simplified)	Singapore
Chinese (Traditional)	Hong Kong
Chinese (Traditional)	Taiwan
Croatian	Croatia
Czech	Czech Republic
Danish	Denmark
Dutch	Belgium
Dutch	Netherlands
English	Australia
English	Canada
English	India
English	Ireland
English	Malta
English	New Zealand
English	Philippines

English	Singapore
English	South Africa
English	United Kingdom
English	United States
Estonian	Estonia
Finnish	Finland
French	Belgium
French	Canada
French	France
French	Luxembourg
French	Switzerland
German	Austria
German	Germany
German	Luxembourg
German	Switzerland
Greek	Cyprus
Greek	Greece
Hebrew	Israel
Hindi	India
Hungarian	Hungary
Icelandic	Iceland

Indonesian	Indonesia
Irish	Ireland
Italian	Italy
Italian	Switzerland
Japanese (Gregorian calendar)	Japan
Korean	South Korea
Latvian	Latvia
Lithuanian	Lithuania
Macedonian	Macedonia
Malay	Malaysia
Maltese	Malta
Norwegian (Bokmål)	Norway
Polish	Poland
Portuguese	Brazil
Portuguese	Portugal
Romanian	Romania
Russian	Russia
Serbian (Cyrillic)	Bosnia and Herzegovina
Serbian (Cyrillic)	Montenegro
Serbian (Cyrillic)	Serbia
Slovak	Slovakia

Slovenian	Slovenia
Spanish	Argentina
Spanish	Bolivia
Spanish	Chile
Spanish	Colombia
Spanish	Costa Rica
Spanish	Dominican Republic
Spanish	Ecuador
Spanish	El Salvador
Spanish	Guatemala
Spanish	Honduras
Spanish	Mexico
Spanish	Nicaragua
Spanish	Panama
Spanish	Paraguay
Spanish	Peru
Spanish	Puerto Rico
Spanish	Spain
Spanish	United States
Spanish	Uruguay
Spanish	Venezuela

Swedish	Sweden
Thai (Western digits)	Thailand
Turkish	Turkey
Ukrainian	Ukraine
Vietnamese	Vietnam

1.3.1.3.3 Localizing Data in TeamConnect

By default, all of the information that is visible in the TeamConnect user interface and all error/ information messages appear in English. If you wish to view this information in a different language, you can export the English data to an Excel spreadsheet, enter the translated data into corresponding fields on the spreadsheet, and then import the translated data back into TeamConnect.

Once the translated data is imported back into TeamConnect, the translated elements appear in your preferred language. For more information about setting your locale languages, see Working with Locales.

1.3.1.3.3.1 Exporting Data for Translation

TeamConnect lets you export localization data so that you can translate it into your preferred locale language. Exported localization data is saved to an Excel workbook named *TeamConnect_MessageResources.xls*.

To export data for translation

1. Click the **All** tab.
2. In the **Tools** section, select **Locale Manager**.

   The Locale Manager opens.
3. In the left pane, click the **Export** link.
4. Click the **Export to file** button.

   A dialog box opens.
5. In the dialog box, select one of the following options:
   - To immediately open the spreadsheet, click **Open with**, and then click **OK**.
   - To save the spreadsheet without opening it, click **Save File**, select the appropriate location, and then click **OK**.

Using the Exported Worksheets

TeamConnect_MessageResources.xls contains all of the TeamConnect data that is available to translate.

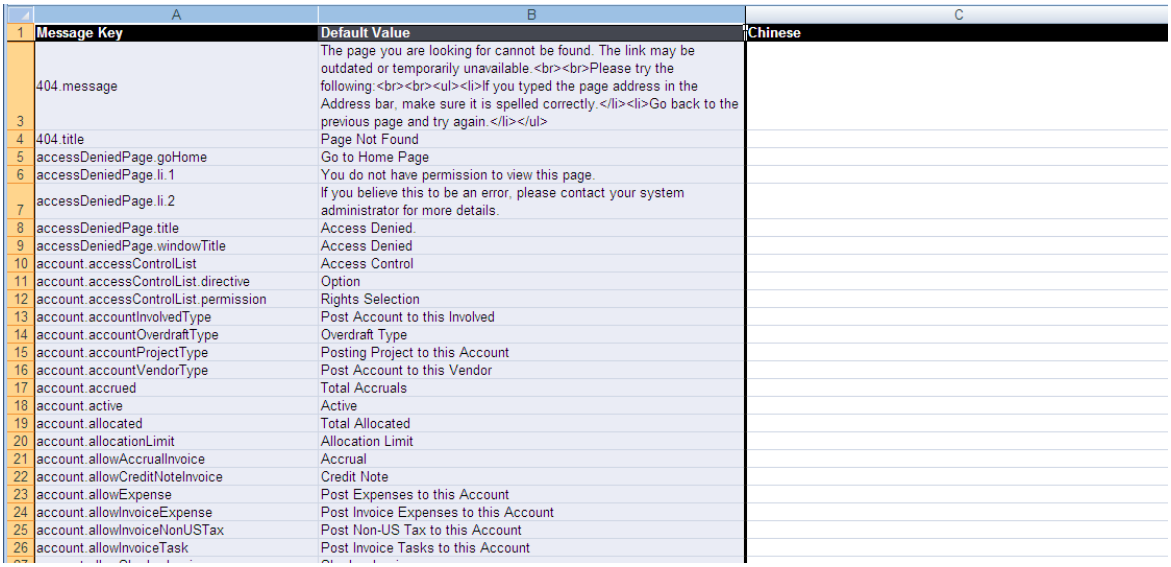
The workbook contains the following spreadsheets:

- **Static Resources**—Contains all of the system error messages and default user interface fields and labels.
- **Design Resources**—Contains fields and labels for all of the following :
    - Object definitions
    - Related objects
    - System lookup tables
    - Custom lookup tables
    - Home pages
    - Portal panes
    - Routes
    - Wizards

  This page also contains the text for the following:
    - The custom logo
    - The welcome message on the login page
    - The maintenance notification message
    - Additionally, this page may also contain fields and labels for other designs, such as CSM and TeamConnect Legal if installed.
- **Custom Resources**—Contains custom message keys and values. May also contain custom message keys and values for other designs, such as CSM and TeamConnect Legal if installed.

The first two columns of each spreadsheet are in default English and cannot be modified or deleted:

- **Message Key** column—Contains the identification keys for corresponding default values.
- **Default Value** column—Contains the actual text for the default data. For example, for error or informational messages, the **Default Value** is the actual text of the message.



	A	B	C
1	Message Key	Default Value	Chinese
3	404.message	The page you are looking for cannot be found. The link may be outdated or temporarily unavailable. Please try the following: - If you typed the page address in the Address bar, make sure it is spelled correctly. - Go back to the previous page and try again.	
4	404.title	Page Not Found	
5	accessDeniedPage.goHome	Go to Home Page	
6	accessDeniedPage.li.1	You do not have permission to view this page.	
7	accessDeniedPage.li.2	If you believe this to be an error, please contact your system administrator for more details.	
8	accessDeniedPage.title	Access Denied.	
9	accessDeniedPage.windowTitle	Access Denied	
10	account.accessControlList	Access Control	
11	account.accessControlList.directive	Option	
12	account.accessControlList.permission	Rights Selection	
13	account.accountInvolvedType	Post Account to this Involved	
14	account.accountOverdraftType	Overdraft Type	
15	account.accountProjectType	Posting Project to this Account	
16	account.accountVendorType	Post Account to this Vendor	
17	account.accrued	Total Accruals	
18	account.active	Active	
19	account.allocated	Total Allocated	
20	account.allocationLimit	Allocation Limit	
21	account.allowAccruallnvoice	Accrual	
22	account.allowCreditNoteInvoice	Credit Note	
23	account.allowExpense	Post Expenses to this Account	
24	account.allowInvoiceExpense	Post Invoice Expenses to this Account	
25	account.allowInvoiceNonUSTax	Post Non-US Tax to this Account	
26	account.allowInvoiceTask	Post Invoice Tasks to this Account	

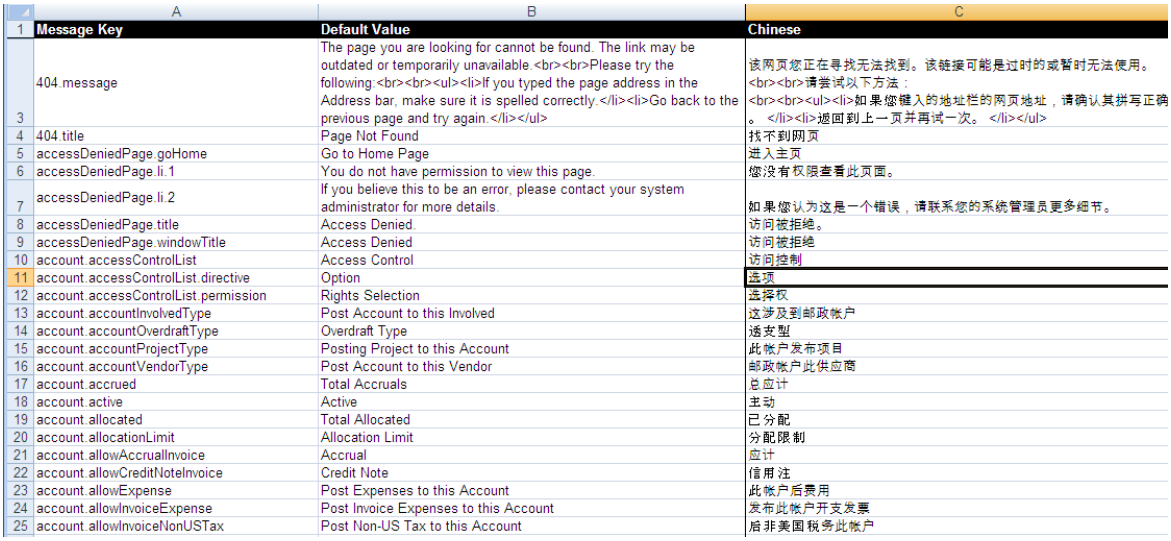
Exported Excel Spreadsheet with Message Keys and Default Value Text

Additional columns correspond to the locales that you registered in TeamConnect using the Locale Manage tool. See Working with Locales for more information.

You cannot add or remove any columns in this workbook.

Entering or Changing Localized Data

You can enter or change translated data in the columns that correspond to the locales that you registered n TeamConnect.



	A	B	C
1	Message Key	Default Value	Chinese
3	404.message	The page you are looking for cannot be found. The link may be outdated or temporarily unavailable. Please try the following: - If you typed the page address in the Address bar, make sure it is spelled correctly. - Go back to the previous page and try again.	该网页您正在寻找无法找到。该链接可能是过时的或暂时无法使用。 请尝试以下方法： - 如果您键入的地址栏的网页地址，请确认其拼写正确。 - 返回到上一页并再试一次。
4	404.title	Page Not Found	找不到网页
5	accessDeniedPage.goHome	Go to Home Page	进入主页
6	accessDeniedPage.li.1	You do not have permission to view this page.	您没有权限查看此页面。
7	accessDeniedPage.li.2	If you believe this to be an error, please contact your system administrator for more details.	如果您认为这是一个错误，请联系您的系统管理员更多细节。
8	accessDeniedPage.title	Access Denied.	访问被拒绝。
9	accessDeniedPage.windowTitle	Access Denied	访问被拒绝
10	account.accessControlList	Access Control	访问控制
11	account.accessControlList.directive	Option	选项
12	account.accessControlList.permission	Rights Selection	选择权
13	account.accountInvolvedType	Post Account to this Involved	这涉及到邮政帐户
14	account.accountOverdraftType	Overdraft Type	透支型
15	account.accountProjectType	Posting Project to this Account	此帐户发布项目
16	account.accountVendorType	Post Account to this Vendor	邮政帐户此供应商
17	account.accrued	Total Accruals	总应计
18	account.active	Active	主动
19	account.allocated	Total Allocated	已分配
20	account.allocationLimit	Allocation Limit	分配限制
21	account.allowAccruallnvoice	Accrual	应计
22	account.allowCreditNoteInvoice	Credit Note	信用注
23	account.allowExpense	Post Expenses to this Account	此帐户后费用
24	account.allowInvoiceExpense	Post Invoice Expenses to this Account	发布此帐户开支发票
25	account.allowInvoiceNonUSTax	Post Non-US Tax to this Account	后非美国税务此帐户

Excel Spreadsheet with Localized Data

To enter or change localized data

Enter or change translated data in the appropriate columns and corresponding fields on the spreadsheet.

To make changes to localized data after the file is imported, see Changing Localized Data After Import.

Once you enter the localized data, you can upload the translations. See Importing Translated Data for more information.

Note: *If you copy and paste translated data from third-party translation software, such as Google Translate, you may have difficulty deleting or making changes to the text once you paste it in the spreadsheet. To avoid this, after you copy the text, go to the appropriate cell on the spreadsheet, right-click, select* ***Paste Special****, and then select* ***Text****. This removes any hidden characters and allows you to make changes to the pasted text when necessary.*

Tags, Punctuation, and Symbols

If the information in the **Default Value** column contains html tags, such as <li> or %20, or symbols, punctuation marks, and/or numbers, such as {0} or "{1}", the corresponding translation must also include this information.

For example, if you are translating the following into German:

```
<b>Results Display</b>
{1}: Multiple matches were found for "{0}".
(ANY)
```

The translated text must appear as follows:

```
<b>Ergebnisse anzeigne </b>
{1}: Mehrere Spiele wurden fur "{0}" gefuden.
(Beliebig)
```

Important: *If you are translating into a language that may have very long words, to improve readability, it is recommended that you use recognized abbreviations in place of the long version of words whenever possible.*

Adding new locales

You cannot add new locales to the spreadsheet. You must first register the new locale in TeamConnect, and then export the *TeamConnect_MessageResources.xls* file again. A new blank column appears on the spreadsheet, along with the previously localized data. See To add a locale for more information.

1.3.1.3.3.2 Importing Translated Data

After you export and then translate the data, you can import the spreadsheets into TeamConnect. The default data is replaced and you can view TeamConnect in your preferred language.

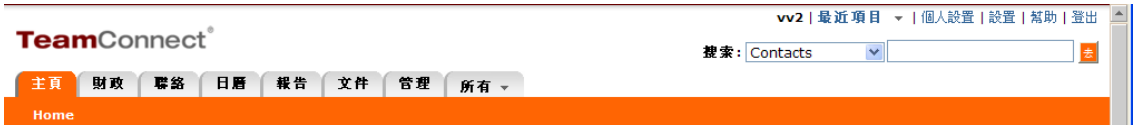
For information about exporting, see Exporting Data for Translation.

Important: *You can only import Excel files that end in .xls or .xlsx.*

To import translated localized data

1. Click the **All** tab.
2. In the **Tools** section, select **Locale Manager**.
3. In the left pane, click the **Import** link.
4. Click **Browse** to locate and select the appropriate .xls or .xlsx file.
5. Click **Upload**.

The file is added to TeamConnect and the data is displayed in your preferred language.



TeamConnect Tabs and Global Menu Translated to Chinese

Changing Localized Data After Import

To change localized data after you import the spreadsheet, you must export the *TeamConnect_MessageResources.xls* file again, make changes, and then import the spreadsheet back to TeamConnect. Your changes appear once the spreadsheet is imported.

1.3.1.4 Calendar Settings

Note: *For TeamConnect, always choose the option* ***Use standard appointment records****. Use of other calendaring applications is not presently supported in TeamConnect.*

1.3.1.5 Documents Settings

You can configure the following Admin Settings from the **Documents** page:

- **Enable document version control**—Enable management of files uploaded to TeamConnect. For example, when one user checks out a file, other users can view that file but cannot upload changes to that file.
- **Enable WebDAV**—Allows users to manage TeamConnect Documents area files using Internet Explorer.
- **Maximum size of uploaded file (megabytes)**—Defines the maximum document size that can be uploaded to TeamConnect. The default is 50 MB and the minimum value allowed is 1 MB.

A conceptual overview of the settings follows. If you prefer to skip to the procedure for configuring the settings, see Managing Documents.

1.3.1.5.1 Document Version Control

Enabling Document Version Control provides document version management in TeamConnect. When a document has been updated, a user can check out the existing document, and check in the latest document, resulting in an additional document version.

If you enable Document Version Control, users who need rights to view different document versions will also need the Document Read rights and Document Version Read rights. Users who need rights to revert to previous document versions will also need the Document Update rights and Document Version Revert rights. For more information, see the Documents section of the appendix, Rights for End-users.

Important: *When Document Version Control is enabled, the TeamConnect database stores all versions of all documents, requiring additional storage space.*

For detail on document versioning and how versions interact with search results, please see Global Search and Version Control .

1.3.1.5.2 Network File Systems for Documents (WebDAV)

The WebDAV feature allows users to perform the following from Internet Explorer:

- Upload local files to TeamConnect
- Download TeamConnect files locally
- Copy files to other TeamConnect folders
- Move files to other TeamConnect folders

Important: *The TeamConnect WebDAV feature is certified for Internet Explorer versions 6 and 7.*

Important: *If you use the WebDAV feature, you must put a valid URL in the Login URL field of Email Settings. See the Admin Settings, Email Page Field Descriptions table for details.*

If the Enable WebDAV setting is enabled, TeamConnect Documents pages will display a Open In Explorer link in the upper right. Clicking this hyperlink opens the current TeamConnect Documents folder in Internet Explorer. You can also refer to 3rd party documentation for using Internet Explorer 6 as a WebDAV client.

The following overview includes prerequisites and steps to use WebDAV for Documents folders:

1. Enable WebDAV from TeamConnect Admin Settings.
2. Send users instructions for setting up Internet Explorer to automatically link to TeamConnect Documents folders. In addition, you must provide the following URLs to users:
    - User's Documents folder URL:

      http://*Hostname:PortNumber/application_name/davroot/Users/user_name*

      For example,

      http://10.7.7.3:8005/teamconnect/davroot/Users/John

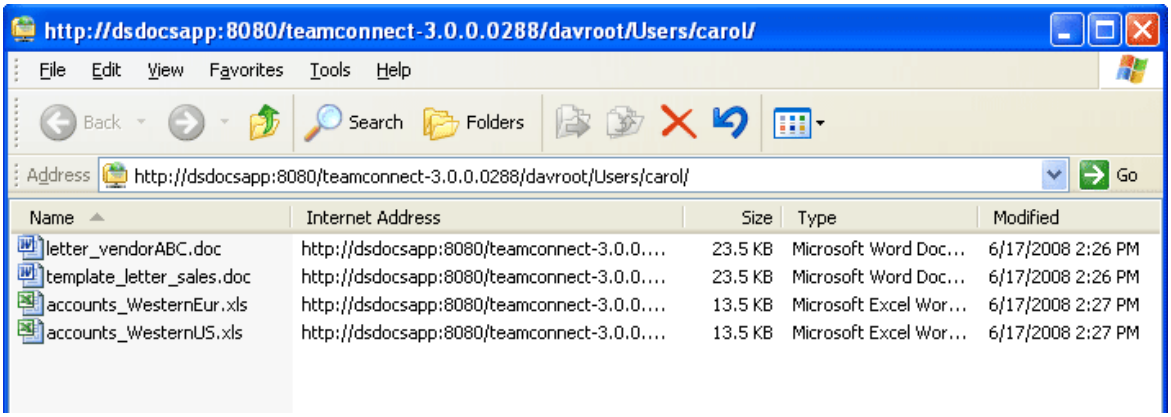
- TeamConnect Root Documents folder URL:

  http://*Hostname:PortNumber/application_name/davroot/*

  For example,

  http://10.7.7.3:8005/teamconnect/davroot/

After WebDAV is enabled from TeamConnect and configured from Internet Explorer, a screen like the following becomes available:



Explorer Screen Networked to TeamConnect User's Documents Folder (WebDAV)

Points to Remember

- Internet Explorer only supports WebDAV URLs that are less than 100 characters long. See the following Microsoft Knowledge Base note for more information:

  http://support.microsoft.com/kb/325355

- TeamConnect includes a WebDAV level 2 server capability.
- TeamConnect supports the WebDAV functionality specified in RFC 2518.
- The WebDAV server uses the same authentication set up for the user in TeamConnect. If single sign-on is not set up, the server requests a username and password; this is the username and password of the TeamConnect user.
- TeamConnect will automatically check out and check in a file when it receives a put (copy) request if the file is not locked by the user or checked out to another user.
- Checking out a file in TeamConnect will not lock the file in Internet Explorer.
- Microsoft refers to WebDAV as "Web Folders".

1.3.1.5.3 Managing Documents

Use the Admin Settings, **Documents** page to perform the following tasks:

- Enable document versioning
- Enable WebDAV
- Set the maximum size of documents that can be added to TeamConnect

To set up Documents

1. Select the **Admin** tab.
2. Click **Admin Settings** under the tab bar.
3. Click the **Documents** link in the left pane.
4. Edit the fields based on descriptions in the Admin Settings - Documents Page field table.
5. Click **Update**.

Admin Settings - Documents Page Field Descriptions

Section	Field Names and Descriptions
Document Security Default Settings	• **Replace rights on subfolders**—The default setting for the **Replace rights on subfolders** setting on the **Security** page of a record. If this setting has a checkmark, if you change the rights of a folder, its subfolders and files also receive the same rights. Without a checkmark, if you change the rights of a folder, the rights of its subfolders and files do not change. If you add a folder or file to a folder with this setting, the folder or file does not update with the folder's rights. To receive security updates, the folder or file must be in the folder when the rights change. • **Replace rights on existing files**—The default setting for the **Replace rights on existing files** setting on the **Security** page of a record. If this setting has a checkmark, if you change the rights of a folder, its files also receive the same rights. Without a checkmark, if you change the rights of a folder, the rights of its files do not change. If you add a file to a folder with this setting, the file does not update with those rights. To receive security updates, the file must be in the folder when the rights change.
Document Settings	• **Enable Document Version Control**—To enable access to previous Document versions, select the check-box. For more information, see Document Version Control. • **Enable WebDAV**—To enable use of the WebDAV protocol to view the TeamConnect Documents area folders from Internet Explorer, select the check-box. To restrict the TeamConnect Documents area folders viewing to the TeamConnect web application, clear the check-box. For more information, see Network File Systems for Documents (WebDAV). • **Maximum size of uploaded file (megabytes)**—Defines the maximum size of documents that can be uploaded to TeamConnect. The default is 50 MB and the minimum value allowed is 1 MB.

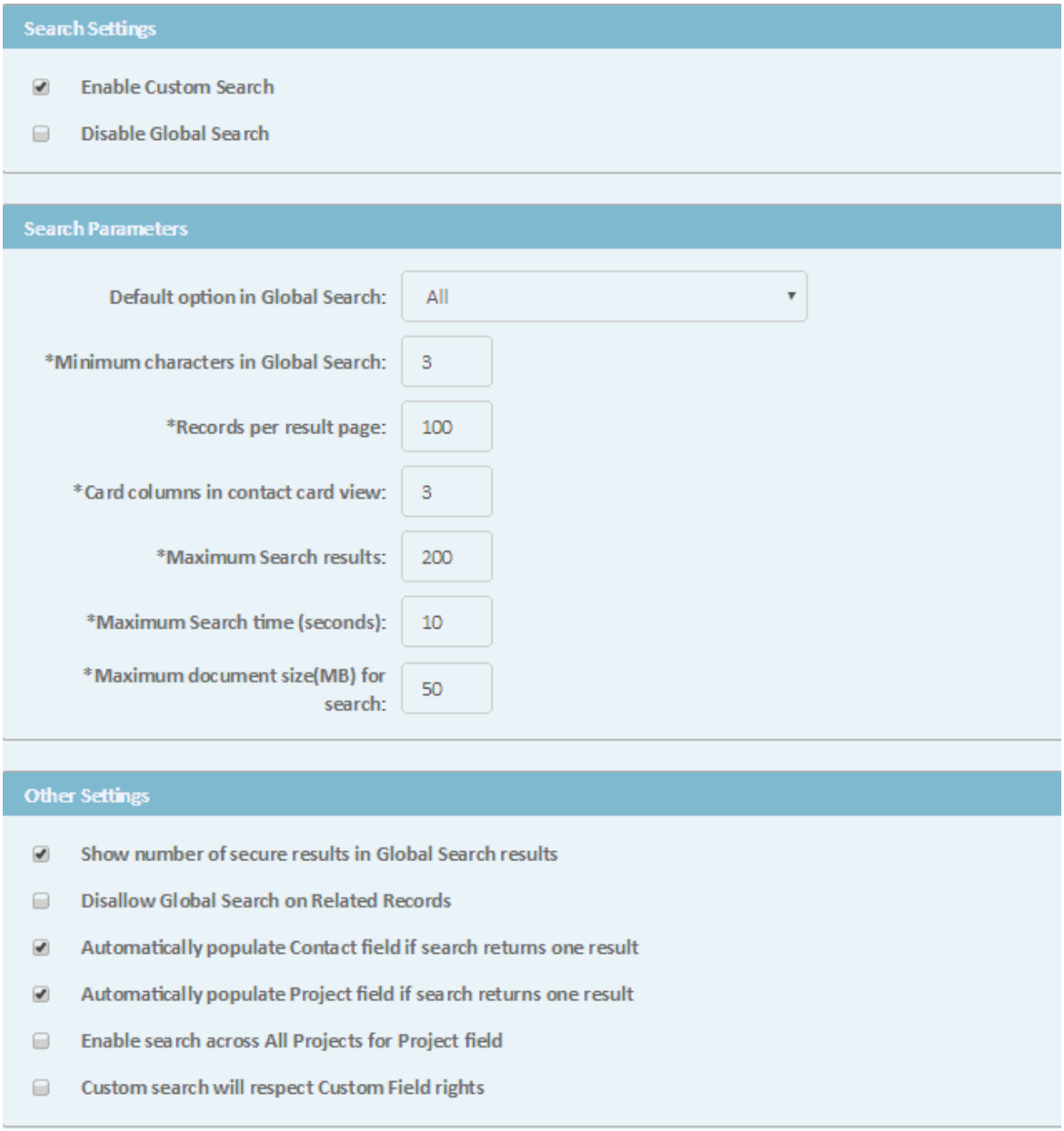
	Note: *The size of the documents that users can add also depends on the amount of memory that is currently allocated to the application server. Users may have difficulty adding documents if your allocated memory is low.*

1.3.1.6 Search Results Settings

You can configure the following Admin Settings from the **Search Results** page:

- Default Global Search object and Global Search parameters—For global searches, select the default record type to search. Set global search term requirements.
- Default Search results display and parameters—Set the number of search results that display per application page. Set the maximum search results that display.
- Search timeout threshold—Set a maximum time (seconds) that the system performs a search.
- Search across Projects—For certain search fields, you can set searches to find results across different projects (or all custom objects).
- Enable Custom Search—Turn the Custom Search feature on or off.
- Disable Global Search—Turn off Global Search and remove the Global Search bar.
- Custom search will respect Custom Field Rights—Users who do not have rights to a custom field cannot search on those fields. This setting will default to 'on' for new implementations and will default to 'off' for upgraded TeamConnect instances.

A conceptual overview of the settings follows. If you prefer to skip to the procedure for configuring the settings, see Setting Up Search Results.



Admin Settings - Search Results Page

1.3.1.6.1 Maximum Search Results

When TeamConnect contains many records it is recommended that you limit the number of search results that display and set a search timeout. This will ensure reasonable system performance times for users.

To limit the number of search results that display, you can decrease the **Maximum Search results** field value (default 1000).

To limit the time allowed to perform a search, you can decrease the **Maximum Search time (seconds)** field value (minimum value, and default, is 10 seconds). If you are using TeamConnect's built-in reporting feature, put a higher value in this field.

Records Not Displayed

In addition to the search criteria that the user specifies on the search screen, other criteria also determines which records are retrieved and displayed. The following records are NOT displayed:

- Records that do not match invisible qualifiers that may be defined in the search view.
- Records that are filtered out by the system because of where the user is accessing the search screen. For example, when a user searches for child projects from within a parent project, only the projects of the appropriate child object are displayed. Similar filtering applies for other types of related records.
- Records to which the current user lacks access due to the security settings on the record's Security tab. In certain cases, these records can be retrieved but cannot be accessed from a search screen because the hyperlink to the record is replaced with the word "secured."
- Records that are not retrieved before the Maximum number of search results is reached, which discontinues any further searching.
- Records that are not retrieved before the Maximum search time is reached, which discontinues any further searching.

1.3.1.6.2 Setting Up Search Results

The following steps describe how to configure the **Search Results** page from Admin Settings. Field descriptions are provided in a table below.

To set up Search Results settings

1. Select the **Admin** tab.
2. Click **Admin Settings** under the tab bar.
3. Click the **Search Results** link in the left pane.
4. Edit the fields based on descriptions in the Admin Settings - Search Results Page fields table.
5. Click **Update**.

Admin Settings - Search Results Page Field Descriptions

Section	Field Names and Descriptions (*=required)	Default Value
Search Parameters	• ***Card columns in contact card view**—(Only for contacts search views where the Results Display Type is set to Card) For contacts search results, enter the number of columns to display. The default is 3.	• ***Card columns in contact card view**—3 • **Default option in Global Search**—Contacts

	Contact the solution developer for more information about contacts search view configuration. • **Default option in Global Search**—To specify a default Global Search type, select an option from this drop-down list. The options include system objects and custom objects. • ***Maximum Search results**--Enter the number of records to retrieve when users perform a search (Global or from a search view defined for an object type) in the **Maximum Search results** field. For more information, see Maximum Search Results. • ***Maximum Search time (seconds)**—Enter the search timeout threshold. The default and minimum value is 10. If you are using the built-in reporting feature, you may wish to use a larger value. For more information, see Maximum Search Results. • ***Minimum characters in Global Search**—Type the minimum number of characters required for Global searching across **All** (records) or **All Projects** in the **Minimum characters in Global Search** field. This value does not apply to Global searches for an individual system object or custom object. ***Important:** The minimum value is 1; however, values less than 3 may lead to large search result sets and slow response times.* • ***Records per result page**—Enter the number of records to display per page of search results. The default is 10.	• ***Maximum Search results**—1000 • ***Maximum Search time (seconds)**—10 • ***Minimum characters in Global Search**—1 • ***Records per result page**—-10
Other Settings	• **Enable search across all projects for Project field**—Do one of the following: To make searches across all custom objects (projects) available to users, select the **Enable search across all projects for Project field** check-box.	• **Enable search across all projects for Project field**—Disabled (not selected) • **Show approximate total**

	To restrict searches to a custom object type, clear the **Enable search across all projects for Project field** check-box. • **Show approximate total number of Global Search results (including records users have no rights to)**—Do one of the following: To display the approximate numeric count of Global Search results, select the **Show approximate total number of Global Search results (including records users have no rights to)** check-box. To display the numeric count of Global Search results that the current user has rights to view, clear the **Show approximate total number of Global Search results (including records users have no rights to)** check-box. • **Automatically populate Contact field if search returns one result**—Do one of the following: To automatically populate a Contact field when the related Contact Search Module returns one record result, select the **Automatically populate Contact field if search returns one result** check-box. To display a link to a record if a search returns one record result, clear the **Automatically populate Contact field if search returns one result** check-box. • **Automatically populate Project field if search returns one result**—Do one of the following: To automatically populate a Project field when the related Project Search Module returns one record result, select the **Automatically populate Project field if search returns one result** check-box. To display a link to a record if a search returns one record result, clear the **Automatically populate Project field if search returns one result** check-box.	**number of Global Search results (including records users have no rights to)**—Disabled (not selected) • **Automatically populate Contact field if search returns one result**—Enabled (selected) • **Automatically populate Project field if search returns one result**—Enabled (selected)
Custom Search	• **Enable Custom Search**—Select this check-box to put a New Search link on each record type's list page. Clicking New Search brings	Selected

	up a set of search criteria and result fields that can be customized by the end user.	
Global Search	• **Disable Global Search**—Select this check-box to remove the Global Search drop-down list and text input box from all pages.	Disabled (**Disable Global Search** check-box cleared)

1.3.1.7 Reporting Settings

Use the Reporting page to define the maximum number of search results when exporting and printing reports and the maximum number of data points allowed on a chart.

To define reporting settings

- For a Tabular View, in the **Maximum search results in Export and Printable View** box, enter the maximum number of search results that you can export to Excel and print in Printable View.
- For a Chart View, in the **Maximum number of data points allowed in chart display**, enter the maximum number of data points allowed when executing a chart.

1.3.1.7.1 Defining Reporting Settings

Use the **Reporting** page to view information about your connection to Data Warehouse and to set search and data point values for the tabular view and chart view.

You can also set the parameters that will be used when generating the .pdf version of the report.

To view Data Warehouse connection information

- If you are successfully connected to the Data Warehouse, **Data Warehouse was last refreshed on <date> <time> appears**. **<date>** and **<time>** are displayed in your current preferred format.
- If you are not connected to the Data Warehouse, **Cannot connect to the data warehouse** appears.

To define report search settings

- For a Tabular View, in the **Maximum search results in Export and Printable View** box, enter the maximum number of search results that you can export to Excel and print in Printable View.
- For a Chart View, In the **Maximum number of data points allowed in chart display**, enter the maximum number of data points allowed when executing a chart.

To set .pdf parameters for reports

The **Default Page Settings** section lets you define the parameters that you want to use when generating a PDF version of the report:

- In the **Orientation** section, click the appropriate position for the report. Options are Portrait (default) or Landscape.
- In the **Margins** section, select the appropriate margin settings. You can use inches or centimeters by selecting an option in the Unit field. The default setting is 0.5.

Each **Header** and **Footer** area of the .pdf is divided into three sections. In each section, you can add one of the following options:

- Report Title
- Page #
- Page # of #
- Run Date
- Run Date/Time
- Logo

You can make a selection in one or more sections or leave all sections empty. Long lines of text will span across empty sections. For example, it you type a long string of text in section one of a header, and nothing in sections two and three, the text in section one will span across all three sections.

Note: *These settings apply to graphic and tabular reports that are exported as .pdf files and reports that are set up to run as .pdf's on an automatic schedule.*

1.3.1.8 Security Settings

You can perform the following tasks on the Admin Settings **Security** page:

- Defining the User Password Policy
- Configuring User Authentication

1.3.1.8.1 Defining the User Password Policy

Use the **Security** page to define your company's password policy as follows:

- **Password Parameters**—Set the guidelines that users must follow when creating log in passwords and how frequently users must change their passwords.
- **Account Lockout**—Set whether or not users are locked out of the system after multiple unsuccessful login attempts.
- **Display Password Policy**—Choose to display your company's complete password policy on the change password page when a user is prompted to change a password.
- **Account Expiration**—Set whether or not user accounts expire after a specified period of inactivity.

- **Password Reset**—Set whether or not users can reset their own password from the login screen. This reset will be accomplished by an automated single-use reset email. For more information on how a user would reset in this method, see Logging In.

Note: *If you are an existing user, your current password is not affected by password policy changes. If you attempt to change your password, you must then adhere to the new policies when creating a password. When you change an existing user's password on the* ***General*** *tab of the user account, all of the password policy settings apply to the new password, except for the* ***Minimum Age*** *setting. This allows you to change a user's password immediately when necessary.*

To define the user password policy

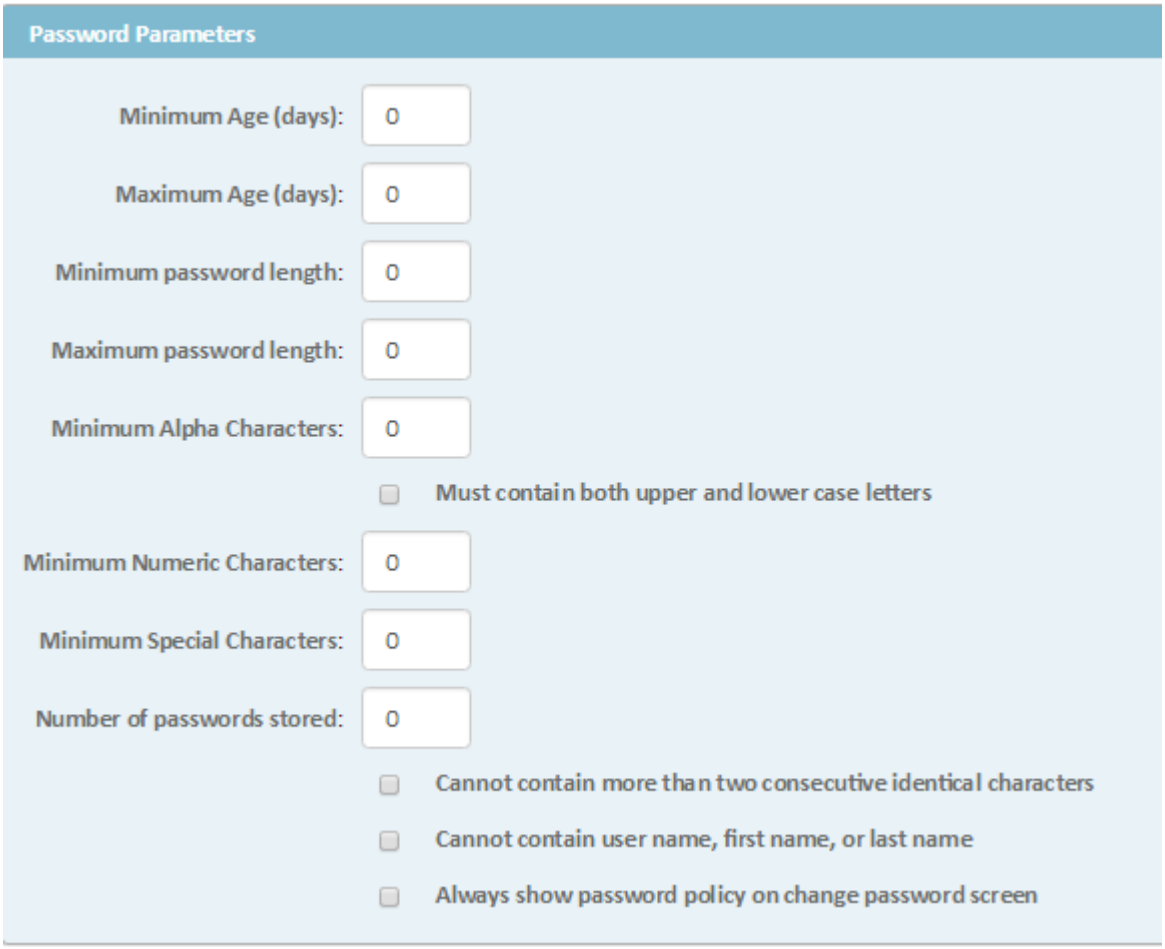
1. Click the **Admin** tab.
2. Click **Admin Settings** under the tab bar.
3. In the left pane, click the **Security** link.

   The **Security** page opens.

   See the Security Page - Password Account Settings fields table for specific field information.

Setting Password Parameters

(Optional) In the **Password Parameters** section, edit the appropriate fields. Leaving the default "0" in a field means that you do not want to set criteria for that option. See the Security Page - Password Account Settings fields table for specific field information. ***Note:*** *Passwords with more than 50 characters can result in a user being locked out of the system.*



Admin Settings Security Page - Password Parameters Section

Displaying the Password Policy

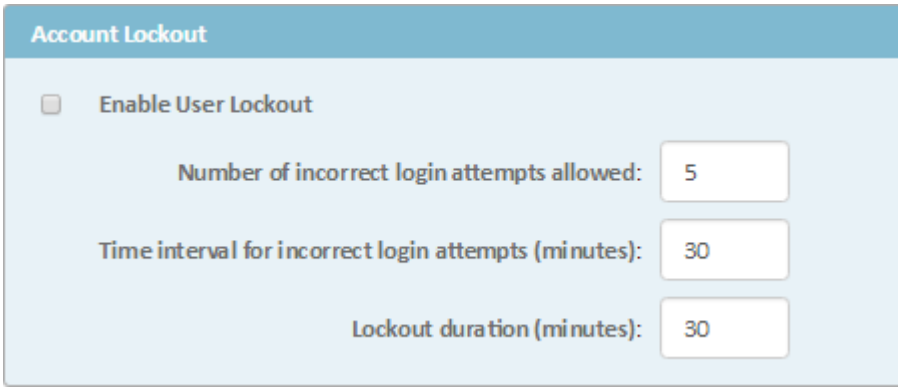
(optional) Click the **Always show password policy on change password screen** check-box to display the password policy details that you selected on the Password Parameters screen whenever a user is prompted to change a password.

This also allows the password policy to appear on the **Reset Password** page in user preferences. See Changing Password for more information.

The graphic below displays the text that users may see on the change password screen and the **Reset Password** page if this check-box is selected:

Setting Account Lockout

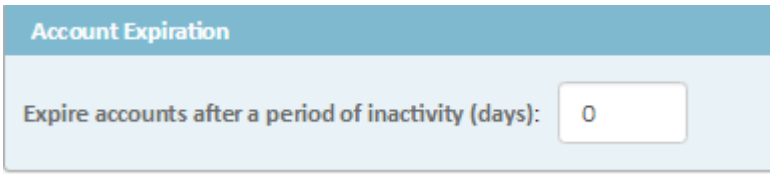
(Optional) In the **Account Lockout** section, check **Enable User Lockout**, and then enter the appropriate information. See the Security Page - Password Account Settings fields table for specific field information. If you clear this check-box, users are never locked out of their accounts for too many login attempts or time interval/duration violations.



Admin Settings Security Page - Account Lockout Section

Setting Account Expiration

(optional) In the **Account Expiration** section, enter the number of days of inactivity that cause the account to expire. The default value for this field is zero. If the value is set to zero, the inactivity expiration will never occur.



Admin Settings Security Page - Account Expiration Section

To set account expiration, click **Update**.

TeamConnect enforces the password policy the next time users try to log in. Users are prompted to change their password if it does not meet the specified criteria.

Enabling AutoComplete for User Name on the Log In Page

(optional) If you leave the **AutoComplete Settings** check-box selected, when you begin to enter a **User Name** on the TeamConnect log in page, a pop-up suggests names that you can choose from based on names that you previously entered on the log in page. If you unselect this check-box, the auto complete feature is disabled.

Security Page - Password Account Settings Field Descriptions

Section	Field Name and Description
Password Parameters	• **Minimum Age (days)—**Enter the minimum number of days that a user must keep an existing password before it can be changed. This setting is based on the date that the password is set or changed. This setting only applies to an end user's ability to change their password on the Password Settings screen or from the login screen. Administrators can change user passwords from user accounts' General tab.

	• **Maximum Age (days)—**Enter the maximum number of days before a user has to change an existing password. This setting is based on the date that the password is set or changed. • **Minimum password length—**Enter the minimum number of characters, alpha and numeric) required for a password. • **Maximum password length—**Enter the maximum number of characters (alpha and numeric) required for a password. • **Minimum Alpha Characters—**Enter the minimum number of letters (A - Z and/or a - z) that must be included in the password. • **Must contain both upper and lower case letters—**If selected, the password must contain lower and upper case letters, such as WeDnesDay. • **Minimum Numeric Characters—**Enter the minimum number of numbers that must be included in the password. • **Minimum Special Characters—**Enter the minimum number of special characters that must be included in the password. For example *, &, #, @ are all special characters. • **Number of passwords stored—**Enter the number of previously used passwords that TeamConnect should not allow users to reuse. ***Note:*** *For the options above, leaving the default "0" in a field means that you do not want to set criteria for that option.* • **Cannot contain more than two consecutive identical characters—**If selected, the password may not contain more than two consecutive letters or numbers. • **Cannot contain user name, first name or last name—**If selected, the password cannot contain the user's first or last name. • **Always show password policy on change password screen—**If selected, in the user interface, the complete password policy displays on the change password page when a user is prompted to change a password. This also allows the password policy to appear on the Reset Password page in user preferences.
Account Lockout	• **Enable User Lockout—**Select this check-box to lock a user's account after a specified number of consecutive, unsuccessful login attempts. Once this number is reached, the user can no longer log in and must contact an administrator. By default, this feature is disabled, which means that users can make an unlimited number of unsuccessful login attempts without getting locked out.

	Note: *The following fields are only available if the* ***Enable User Lockout*** *check-box is selected.* • **Number of login attempts allowed—**Enter the maximum number of failed login attempts before a user's account is locked. 5 is the default. • **Time interval (minutes)—**Enter the number of minutes TeamConnect observes and counts failed login attempts. 30 minutes is the default. • **Lockout duration (minutes)—**The length of time that a locked out user must wait before trying to log in again.
Account Expiration	**Expire accounts after a period of inactivity (days)—**Enter the number of days after which the account expires due to a lack of activity. The default value is zero, which means that accounts never expire.
AutoComplete Settings	**Allow AutoComplete for User Name—**If you select this option, when you begin to enter the first few characters of a **User Name** on the TeamConnect log in page, a pop-up suggests names that you can choose from based on names that you previously used on the log in page.

1.3.1.8.2 Configuring User Authentication

Use the **Authentication Plug-in** section of the Admin Settings **Security** page to choose the default authentication method used by TeamConnect. Authentication is the process of comparing the username and password entered in the TeamConnect login screen to those stored in the database. If the information matches, the user is allowed access to TeamConnect.

The Standard Authentication plug-in is the default authentication method and logs the user into TeamConnect only. This is a secure method, but your organization might choose to integrate the TeamConnect authentication process with a network-wide method. The selected default method applies to all users except those that you specifically override.

Plug-ins are categorized based on their effect on the login process. The two main types of authentication plug-ins are:

- **Standard Authentication**—Allows users to bypass the login screen. If you load an authentication plug-in that has standard sign-on support, users do not see the login screen or enter a username and password because they are authenticated at the network level. If standard authentication is enabled, no other standard sign-on mechanism can be used.
- **Non-standard Authentication**—Allows the identity verification to be handled by an external mechanism used in your environment. This type of plug-in allows authentication to be performed by your local network method, but still requires users to log in to TeamConnect by entering a username and password. You can install various non-standard sign-in plug-ins, and then select which one is used on a per user basis.

Note: *In order to have a choice of authentication methods, the appropriate configuration files must be edited and plug-ins must be installed as described in Authentication.*

Regardless of the plug-in that you select, only Standard authentication is used for the TeamConnect Admin and System user accounts and you cannot change it.

Single Sign-on

If you plan to use a single sign-on method such as NTLM or LDAP, it must be the default authentication method. It is not possible to have Standard Authenticator as the default while overriding a few individual users with NTLM or LDAP.

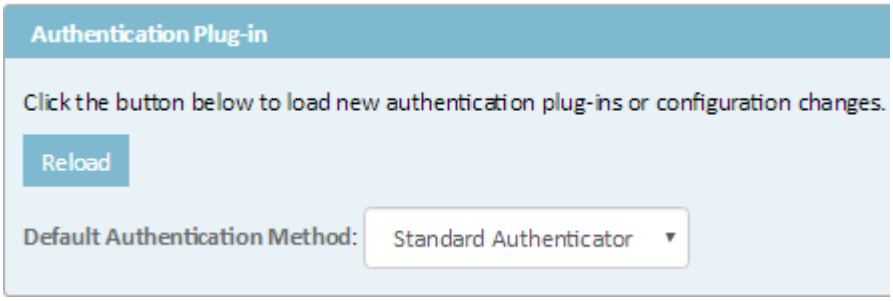
When single sign-on is the default authentication method, you cannot override a few individual users with standard authentication. Instead, for those users, you must ensure that they use the regular login URL, then append **standardLogin** to the end of the URL, to force the use of standard authentication.

For information about how to override authentication for individual users, see Creating or Editing Users.

To configure user authentication

1. Select the **Admin** tab.
2. Click **Admin Settings** under the tab bar.
3. In the left pane, click the **Security** link.

   The **Security** page opens.
4. In the Authentication Plug-in section, click the **Reload** button to refresh any recently changed or added authentication methods.



Admin Settings Security Page - Authentication Plug-in Section

5. In the **Default Authentication Method** drop-down list, select the method that you want to use as the default.

   The method that is currently the default has **(System default)** at the end of its name.
6. If additional fields appear as a result of the method you select, complete the appropriate fields, such as the URL where all user login information is stored for LDAP.
7. Click **Upload**.

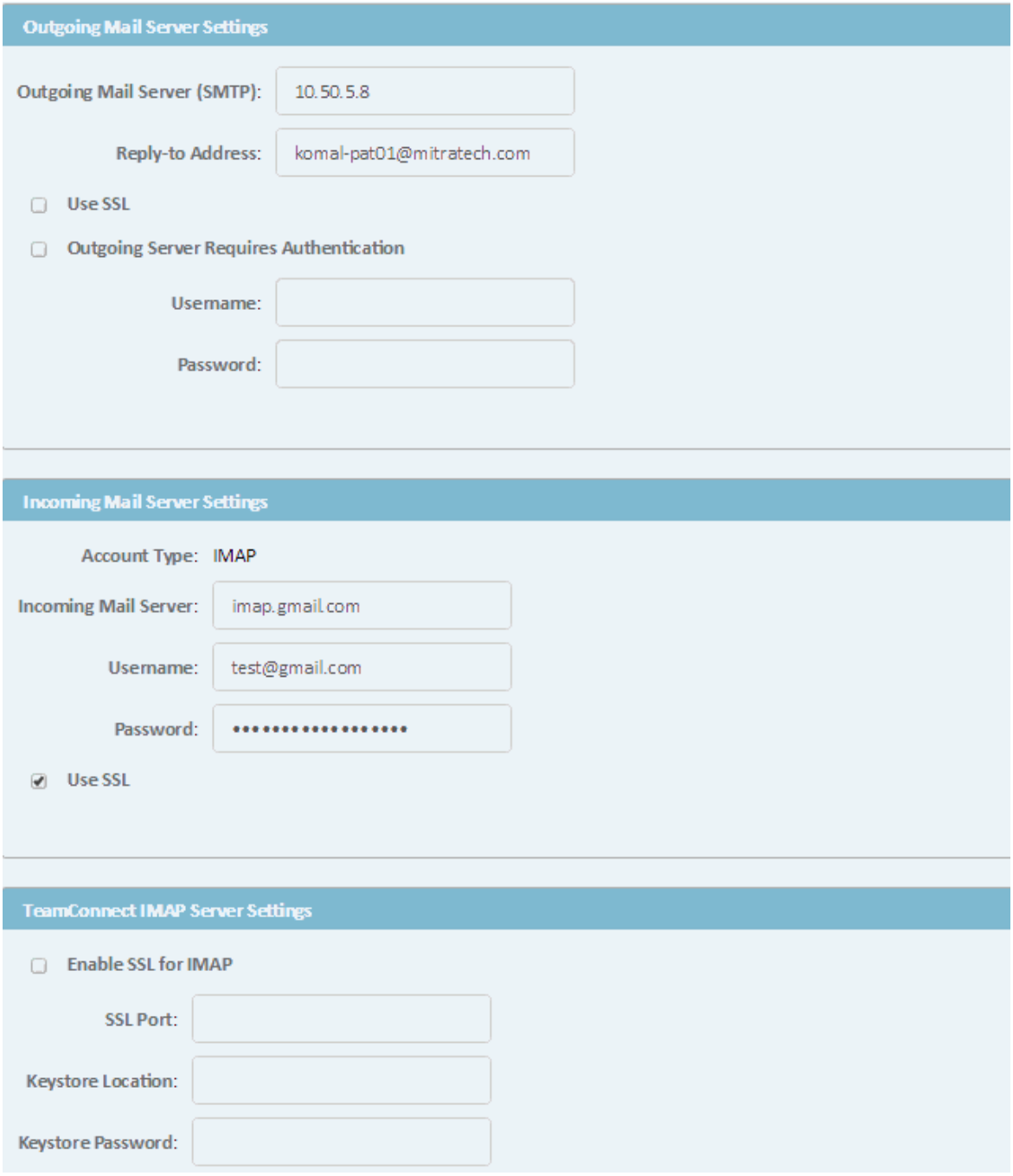
   All users who are configured in their user accounts to be authenticated by the selected mechanism are now authenticated using that method.

1.3.1.9 Email Settings

You can configure the following from Email Settings:

- SMTP server information for outgoing email notifications
- IMAP server information for incoming email notifications
- TeamConnect IMAP server name and port
- TeamConnect login URL (for email notifications, HTTPS)

A conceptual overview of the settings follows. If you prefer to skip to the procedure for configuring the settings, see Setting Up Email.



Email Settings Page

1.3.1.9.1 Email Notification

There are four sources of email notifications from TeamConnect:

- Default system notifications
- SMTP appender (sends email notifications for Error events from the TeamConnect system log)
- Scheduled action and custom action rules email notifications

- Approval routes email notifications

The following is an overview of steps to set up email notification support:

Note: *Depending on which type of email notification you are setting up, some of the prerequisites may differ.*

1. Set up the email recipients list (for Approval Routes and SMTP Appender).
2. Set up the SMTP Server information from the Admin Settings, Email page, Email Properties section. This is required for system email notifications.
3. Restart the TeamConnect application server.
4. Remind users to enable email notifications from their **Preferences** area.

Prerequisites

- If your email system requires authentication each time an email is sent:
  - TeamConnect's application server must have JDK version 1.5 or above.
  - The SMTP server must have an email account set up for TeamConnect.
  - The SMTP server must allow the username with which TeamConnect authenticates to be different from the username used as the From address of the message. (The From address of the message is set to the contact email address for the user who made the assignment or appointment. The SMTP appender uses the value of the Reply-To Address field in the Email Properties). Check with your email administrator to correct this limitation if it exists.
- If you are using the SMTP appender or if authentication is required for sending email, you MUST specify the username and password for TeamConnect's email account in the Email Properties section of the Email tab in Admin Settings.

Points to Remember

- Some email notifications are provided by default with TeamConnect and other email notifications are created for Approval routes.
- The SMTP appender also uses the SMTP hostname and Reply-To address from the **Email Properties** section.
- When a user is the only recipient of an email, it is sent in the user's selected language. When there are multiple recipients, the email is sent in the selected system locale. See Setting Regional Settings for more information.

1.3.1.9.2 TeamConnect IMAP Server

Note: *IMAP settings pages are not visible to users who are running TeamConnect® Express.*

The TeamConnect IMAP Server allows users to synchronize folders and email (from an email client) with Project records in TeamConnect (such as, Disputes, Matters, or Transactions).

Perform the following to set up and start the TeamConnect IMAP Server:

1. (optional) If you will require encrypted connections (SSL) to the TeamConnect IMAP Server, set up SSL for the IMAP Server.
2. Enable IMAP search views for custom objects (from TeamConnect; for example, Disputes). For more information, see Enabling IMAP Search for Custom Object Search Views.
3. Configure the IMAP Server (from TeamConnect).
4. Start the IMAP Server (from TeamConnect).
5. Verify user/group rights for email messages and folders (from TeamConnect).
6. Configure users' email clients.

1.3.1.9.2.1 Setting Up SSL for the IMAP Server

The TeamConnect IMAP Server supports encrypted connections (SSL). If you will require encrypted IMAP connections (SSL) from IMAP Clients, the following are required:

Important: *The JDK installation used for running the Keytool should be the same JDK installation used by the TeamConnect application server. For additional information about keystores, see your JDK vendor documentation.*

1. Get the Keytool security tool (provided in a JDK).

   Note: *For remaining SSL setup requirements, high level descriptions are provided but you must refer to your JDK vendor's documentation for details.*

2. Using Keytool, do the following on the TeamConnect server:
   - Create a keystore (including a public/private key pair). Use the RSA algorithm.

     Note: *You will need the keystore file location, keystore password, and key password to set up the TeamConnect IMAP Server.*

   - Generate a Certificate Signing Request (CSR). Send a request for a signed certificate to a Certification Authority (CA), using the information in the CSR.
   - After you receive the resulting certificates from the CA, use Keytool to import the certificates to the keystore.

     Note: *If you had generated a self-signed certificate above, you need to replace it by importing a signed certificate from the CA.*

Important: *The keystore used for IMAP over SSL must be generated by a Keytool from a JDK. Also it is recommended to generate a new CSR from the Keytool and order a new SSL certificate for the IMAP server.*

1.3.1.9.2.2 Configuring the IMAP Server

You can change the IMAP Port number and set up the IMAP Server to start automatically when TeamConnect is restarted.

Tips and Warnings

- If you have already started the IMAP Server, and you update the IMAP Port, you need to stop and start the IMAP Server before the new port number will take effect.
- If you have already started the IMAP Server and you update the auto-start behavior of the IMAP Server, the changes take effect the next time you restart TeamConnect.
- If you are unable to start the IMAP Server, there might be a port usage conflict. Another IMAP Server may be running on the application server. There may be permissions restrictions where the default port is reserved for system processes or use by privileged users. You may need to change the port number (for example, 49152 or greater).
- If you have already started the IMAP Server, and you update settings related to SSL for IMAP Server, you need to stop and start the IMAP Server before changes will take effect.
- The TeamConnect IMAP Server supports encrypted connections (SSL) and unencrypted connections simultaneously. If SSL is enabled from IMAP Server system settings, IMAP Clients can still use unencrypted connections using the IMAP Port number

To configure the IMAP Server

1. Select the **Admin** tab.
2. Click **Admin Settings** under the tab bar.
3. Click the **Email** link in the left pane.
4. Edit the fields based on descriptions in the TeamConnect IMAP Server Email Settings table.
5. Click **Update**.
6. Restart TeamConnect on the application server.

TeamConnect IMAP Server Email Settings

Field	Description
Enable SSL	Indicates whether an encrypted IMAP connection is supported.
SSL Port	Enter the port number where you want IMAP server to listen for SSL connections. If you require IMAP Clients to connect to the IMAP Server using SSL, this value must match the IMAP Port specified on users' email client IMAP account. Also see the description for IMAP Port in this table.
KeyStore Location	The path to the keystore file (including the keystore file name). This location should be in the same machine that hosts TeamConnect. For example, /certs/

	ImapKeystore/imapkeystore.jks
KeyStore Password	The keystore password.
Key Password	Password for the generated private key, which you used to obtain the certificate.
IMAP Port	Enter the IMAP port number (for non-SSL connections). This port must match the IMAP Port specified on users' email client IMAP account. The default value is 143. ***Note:*** *Even if you select the Enable SSL check-box, you can still set the IMAP Port and IMAP clients can connect to the IMAP Server using non-SSL connections. Also see the description for SSL Port in this table.*
Status	(Read-only) Indicates whether the TeamConnect IMAP Server is **Started** or **Stopped**.
Run on Startup	Indicates whether the TeamConnect IMAP Server will be automatically started when TeamConnect is started (or restarted). If this check-box is cleared, you would need to manually start the TeamConnect IMAP Server after TeamConnect is started.

1.3.1.9.2.3 Starting and Stopping the IMAP Server

By default, the IMAP Server is disabled. You must manually start the IMAP Server the first time.

Tips and Warnings

- If you restart the IMAP Server while users have IMAP Clients open, the users will need to close and reopen their IMAP Clients.
- You can start the IMAP Server from the Admin Settings without restarting the TeamConnect server.
- The **Start** button is available only if the IMAP Server status is **Stopped**.
- The **Stop** button is available only if the IMAP Server status is **Started**.

To start and stop the IMAP Server

1. Select the **Admin** tab.
2. Click **Admin Settings** under the tab bar.
3. Click the **Email** link in the left pane.

4. Do one of the following:
   - To start the IMAP Server, click **Start**.
   - To stop the IMAP Server, click **Stop**.
5. Click **Update**.

1.3.1.9.2.4 Email Rights

Some prerequisite rights for working with email and email folders need to be set up from the Admin area of TeamConnect in user or group rights. There are additional email record and email folder-level rights that can be managed from the user area of TeamConnect.

For details, see Rights for End-users.

1.3.1.9.2.5 Email Clients

See the *Release Notes* for specific client versions supported.

1.3.1.9.3 Setting Up Email

The following steps describe how to configure the Email page from Admin Settings. You can use the **Email** page to configure the connection to an SMTP Server (for system email notifications), configure the connection to an IMAP Server, and configure the TeamConnect URL for email notifications or HTTPS connections. Field descriptions are provided in a table below.

To set up Email

1. Select the Admin tab.
2. Click Admin Settings under the tab bar.
3. Click the Email link in the left pane.
4. Edit the fields based on descriptions in the TeamConnect IMAP Server Email Settings table.
5. Click Update.
6. Restart TeamConnect on the application server.

   Afterward, users must do the following:
   - Verify that the default email address in their contact record is the email address to which notifications should be sent.
   - From the Preferences area, select the Email Notifications that they want to receive.

Important: *Each user who assigns other users to tasks and projects, or adds them as appointment attendees, should have a default email address in their contact*

record. If the Email Properties are not defined properly, email notifications will not be sent from TeamConnect.

Admin Settings, Email Page Field Descriptions

Section	Field Names and Descriptions (*=required)	Default Value
Outgoing Mail Server Settings	• **Outgoing mail server (SMTP)**—The host name or IP address of your Simple Mail Transfer Protocol (SMTP) email server. ***Note:*** *TeamConnect routes SMTP connections through port 25 (the default SMTP port).* For more information, see Email Notification. • **Reply-To Address**—A default email address that will be used as system email notification Reply-to address and email From address. A reply-to address is required in order for TeamConnect to automatically send email. If a user performs an action that triggers a system email notification, that user's contact record primary email address will override the **Reply-To Address** value as the resulting email message's From and Reply-to email address. Otherwise, if the contact record has no email address populated, the **Reply-To Address** value will be used as the email message's From and Reply-to email address. If the **Reply-To Address** is empty and the triggering user/contact's email address is empty, then a system email notification will not be sent. ***Note:*** *The SMTP appender also uses the **Reply-To Address** as the **From** address for Error log email messages.* • **Use SSL**—The check-box you select if the SMTP server uses SSL (secure socket layer) to send email. ***Note:*** *TeamConnect uses port 465 as the default SSL port.* • **Outgoing server requires authentication**—Select this check-box if the SMTP server requires	empty

	authentication for sending email. When selected, you must enter a username and password. • **Username**—TeamConnect's user name for authenticating with the SMTP server. • **Password**—TeamConnect's password for authenticating with the SMTP server.	
Incoming Mail Server Settings	• **Account Type**—Indicates that the email account that sends users incoming mail from TeamConnect has to have IMAP enabled. • **Incoming mail server**—The name of the server for the email account, for example, imap.gmail.com. • **Username**—The email address that TeamConnect uses to send emails. TeamConnect only pays attention to unread emails. As a result, you should create an email account specifically for the use of incoming mail. • **Password**—The password of the email account. • **Use SSL**—The check-box you select if the IMAP server uses SSL (secure socket layer) to send email. ***Note:*** *TeamConnect uses port 993 as the default SSL port and port 143 as the default non-SSL port.*	empty
TeamConnect IMAP Server Settings	These settings are described in detail in the TeamConnect IMAP Server Email Settings table.	empty

1.3.1.10 Notification Settings

Rules can be designed to send email notifications after certain actions have been triggered. To customize the templates used for these emails, you can update the notification system settings. Notifications can be defined for all objects, all custom objects, or a specific system or custom object.

See Specifying Actions for Custom Action Rules and Defining Settings for Scheduled Action Rules for more information about creating and editing rules to send notifications, as well as defining recipients of notifications.

Users must be given the appropriate rights to view, edit, create, and delete notification templates. For details, see the Rights for End-users appendix.

For notification templates that will be defined only for a custom object, the custom object must be created before creating the templates.

To view notification templates

1. Click the **Admin** tab.
2. Click **Admin Settings** under the tab bar.
3. Click **Notifications** in the left pane.

   The page of notification templates opens. Click the following table column headers to sort the list of notification templates: **Name**, **Active**, **Description**, **Defined for**.
4. To open a notification template, click its link in the **Name** column.

To create or edit notification templates

1. Click the **Admin** tab.
2. Click **Admin Settings** under the tab bar.
3. Click **Notifications** in the left pane.
4. Select one of the following options:
   - To create a new notification template, click the **New** button.
   - To edit a notification template, click the **Edit** icon next to the record that you want to edit.

     The notification template opens to its **General** page.
5. On the **General** page, enter or edit the appropriate information. See the Admin Settings - General Page fields table for more information.

   Fields with an asterisk are required and must be completed before you can save this record.
6. Click the **Email Definition** link in the left pane.
7. On the **Email Definition** page, enter or edit the appropriate information. See the Email Definition Page fields table for more information.

   Fields with an asterisk are required and must be completed before you can save this record.
8. Select a save option.

General Page Field Descriptions

Field (* = required)	Description
***Name**	The name of the notification template.

***Key**	Uniquely identifies a template. Notification templates cannot have the same unique key. This key can be used to retrieve the template in a custom action rule through the notification API. It can also be used to identify the template in a custom design for use at the global level and at the object definition level. After you save the notification template, the unique key appears as read-only text and you cannot change it.
Is active?	The active status of the notification template. An inactive template will not show up as a selection option anywhere, such as in Admin Settings, object definitions, rules, etc. If a template that is associated with a rule or action is deactivated, the template notification will continue to use the deactivated template.
Description	A description of the notification template. Limited to 250 characters.
***Defined for**	The object type the notification template is defined for. Available selections in the drop-down menu are **All Objects**, **All Projects**, and individual system or custom object types.

Email Definition Page Field Descriptions

Field (* = required)	Description
***Subject line**	The subject line of the notification template. Limited to 250 characters. Supports Object Navigator variables.
***Body**	The body text of the notification template. Limited to 250,000 characters. Supports Object Navigator variables. You can use the editor buttons in this field to format the email body text as you desire. Click the **Select Field** link under the **Body** field to show the **Object Navigator** button. The **Object Navigator** button opens a pop-up menu that displays the objects whose fields can be inserted into either the **Subject line** or **Body** of notification templates. This is determined by which field the text cursor was last active in when the **Insert** button is clicked. The objects available in Object Navigator are determined by which objects the template is defined for. In the Admin Settings pages, the object fields will be depicted in the text as variables, such as ${currentUser}.

Important: *The Object Link > Share URL value in Object Navigator will not display properly in notification emails if the* ***Login URL*** *setting in the* ***General*** *page of* ***Admin Settings*** *is not defined properly.*

To make a copy of a notification template

1. Click the **Admin** tab.
2. Click **Admin Settings** under the tab bar.
3. Click **Notifications** in the left pane.
4. Click the link in the **Name** column of the desired notification template.
5. Click the **Copy** button.

   The notification template editor opens with the contents of the copied notification template. The exceptions are the Name field, which is set to "Copy of [original template name]", and the Unique Key field, which is set to blank.
6. Edit the appropriate information on the **General** and **Email Definition** pages.
7. Select a save option.

To print a notification template

1. Click the **Admin** tab.
2. Click **Admin Settings** under the tab bar.
3. Click **Notifications** in the left pane.
4. Click the link in the **Name** column of the notification template you want to print.
5. Click the **Printable View** button.

1.3.1.10.1 Customizing System Notifications

In the **System Notifications** section, you can specify which notification templates are sent in place of the default system notifications. This section lists general actions performed by objects that send system notifications. Beside each action is a drop-down list of available notification templates for that action.

Templates that are customized at this level will be used by all objects that perform the relevant action unless another notification template is selected in an object definition, which supersedes these settings.

To customize a system notification for an action

1. Click the **Admin** tab.
2. Click **Admin Settings** under the tab bar.

3. Click **Notifications** in the left pane.
4. In the **System Notifications** section, select the notification template from the drop-down menu next to the desired action. To set a system notification back to its default, select **Default** from the drop-down menu.
5. Click the **Update** button.

System Notifications Actions

The following list contains the types of email notifications. Updated the field in the **System Notifications** section to send a custom notification template instead of the default system notification.

- **Set as an assignee**—The notification that users receive when assigned to a record.
- **Workflow approval request**—The notification that users receive when assigned as the approver of a request.
- **Workflow approval notice**—The notification that users who complete an action that created an approval request receive when another user approves the request.
- **Workflow rejection notice**—The notification that users who complete an action that created an approval request receive when another user rejects the request.
- **Workflow review request**—The notification that users receive when assigned as a reviewer of a request.
- **Workflow expiration notice**—The notification that approvers receive to remind them that an approval request is about to expire.
- **Workflow review completion notice**—The notification that users receive when a review they requested is complete.

1.3.1.11 Invoices Settings

Invoices in TeamConnect represent bills that outside counsel and other vendors send to your organization. To customize how users work with invoices, you can update the invoice system settings.

To update Invoices settings

1. Click the **Admin** tab.
2. Click **Admin Settings** under the tab bar.
3. Click **Invoices** in the left pane.
4. Edit the fields based on descriptions in the the Admin Settings, Invoice Page fields table.
5. Click **Update**.

Admin Settings, Invoice Page Field Descriptions

Section	Field Names and Descriptions	Default Value
Invoice Settings	• **Reason for rejection is required**—Select the check-box if you want to require users to select a reason for rejection on the **My Approvals** page before they reject invoice approval requests. • **Comment to requestor is required**—Select the check-box if you want to require users to enter comments in the **Comment to Requestor** field on the **My Approvals** page before they reject invoice approval requests. • **Require In House Comments upon adjustment**—Select the check-box if you want to require the user to enter comments in the **In House Comments** field when adjusting an invoice line item. • **Allow users not part of workflow to edit line items**—Place a checkmark in the checkbox if you want to allow users who are not part of the invoice approval group to edit line items when an invoice is in the approval workflow. In addition to selecting this checkbox, users must have system rights to edit line items. • **Enable International Line Item Tax Details**—Place a checkmark in the checkbox to enable invoices to specify non-US taxes for individual line items.	Check-boxes are empty
Invoice Line Item Filter Criteria	**Maximum number of items in list**—Enter the maximum number of items that can appear in multi-select lists when selecting values for a search of the **Line Items** fields on the **General** page of an invoice. If the number of items in a multi-select list is higher than the number you enter, a search box appears instead of a list. The search box allows the user to search across all databases.	100
Invoice Line Items Display	The following fields apply to the **Line Items** section on the **General** page of an invoice. • **Line Item Rate**—Specify up to how many numbers users can enter after the decimal in the **Rate** field. • **Line Item Units/Hours**—Specify up to how many numbers users can enter after the decimal in the **Unit** field.	2 for both options

	These settings apply immediately to all new invoices. Existing data does not change. For more information about setting decimal places, see Setting Decimal Places for Invoice Line Items.	

1.3.1.11.1 Setting Decimal Places for Invoice Line Items

In the **Invoice Line Items Display** section, you can specify how many numbers users can enter after the decimal for the **Rate** or **Unit** line item fields on the **General** page of an invoice. Setting the number of decimal places for invoice line items is useful for rates or units that use fractions, such as photocopying at $0.055 per page.

The system saves values in one of the following ways:

- If users enter values with more decimal places than the system setting, the system rounds the value. See examples 1 and 2 in the Examples of Setting Decimal Places table.
- Values an equal distance from the decimal place round down if the value before the 5 is even and up if the value before the 5 is odd. See examples 3 and 4 in the Examples of Setting Decimal Places table.
- If users enter values with less decimal places than the system setting, the system adds zeros to the value. See example 5 in the Examples of Setting Decimal Places table.

The following table provides examples of how the system formats values in the **Rate** and **Unit** fields.

Examples of Setting Decimal Places

Example Number	Number of Digits after Decimal	Value User Enters	Format of Value
1	2	0.0345	0.03
2	2	0.0379	0.04
3	3	1.1245	1.124 (because 4 is even)
4	3	1.1235	1.124 (because 3 is odd)
5	4	0.03	0.0300

1.3.1.12 Approval Settings

Use the **Approvals** page to control the settings for approval requests and the **My Approvals** pages.

To update Approval settings

1. Click the **Admin** tab.
2. Click **Admin Settings** under the tab bar.
3. Click **Approvals** in the left pane.
4. Edit the fields based on descriptions in the Admin Settings, Invoice Page fields table.
5. Click **Update**.

Admin Settings, Approval Page Field Descriptions

Section	Field Names and Descriptions	Default Value
Approval Settings	• **Allow batch approval**—Select this field to allow approvers to approve multiple requests at the same time by clicking the **Approve Selected** button below the table on the **Requests to Approve** page. Remove the checkmark to remove the **Approve Selected** button below the table so that approvers can only approve requests individually. • **Allow batch rejection**—Select this field to allow approvers to reject multiple requests at the same time by clicking the **Reject Selected** button below the table on the **Requests to Approve** page. Remove the checkmark to remove the **Reject Selected** button below the table so that approvers can only reject requests individually. • **Show days remaining before approval expires instead of date of expiration**—Select this field to include the **Days Pending Action** column in the **Requests to Approve** table. This column lists the number of days before the request expires. Without a checkmark, the table includes a **Due Date** column with the date of expiration. • **Require Internal Comments upon rejection**—Select this field to require the approver to enter comments in the **Internal Comments** field of the **Confirm Rejection** popup to reject the record(s). • **Allow this group to batch reassign approval requests**—Select a group from the drop-down field to allow the members of that group to use the **Reassignment** page of **My Workflow Processes**.	The first check-box has a checkmark, and the other three have no checkmarks.
Expiration Reminders	**Enable reminder x day(s) prior to expiration**—Select this field to enable the ability for approvers to receive email reminders before requests expire. After you place a checkmark in the check-box, enter a number of days in the text field.	The first check-box has a checkmark and the text field has a 1.

	You can set up to three reminders. To receive the email reminders, the user must enable those reminders under **Email Preferences**.	

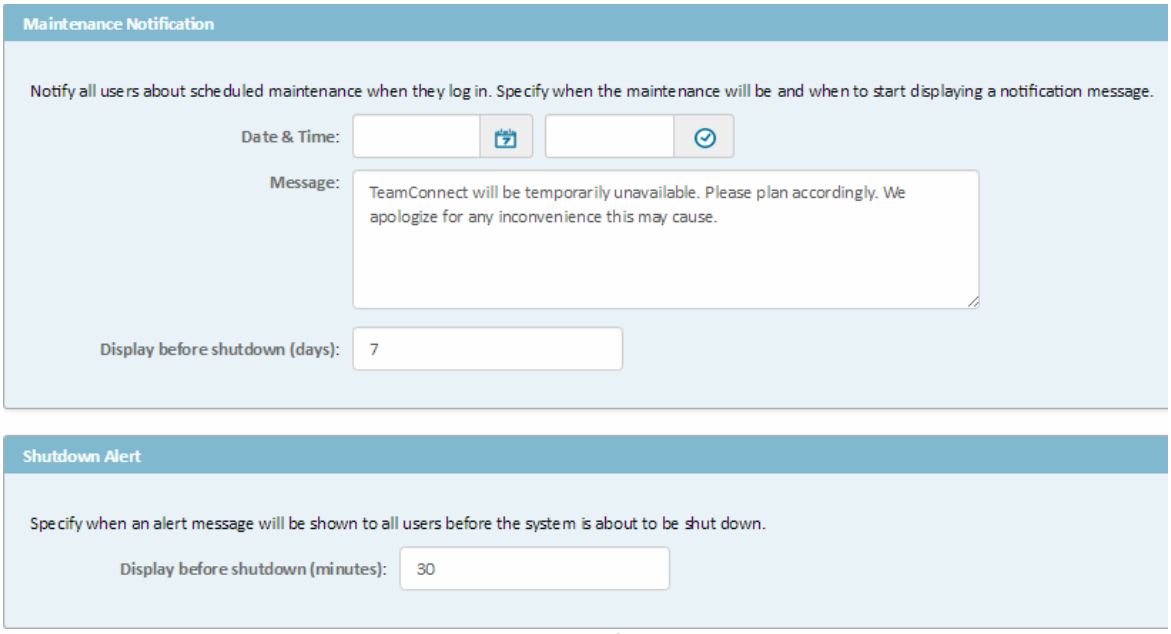
1.3.1.13 Maintenance Settings

The **Maintenance** link in Admin Settings displays a page that you can use to set up advisory messages warning of upcoming periods of system maintenance, during which TeamConnect will not be available to end users.

There might be no values in the fields on this page. You need to enter values only when a maintenance shutdown is approaching. There are two kinds of advisory messages:

Maintenance Notification messages appear when a user starts a session. These are intended for longer-term advisories when a shutdown is not imminent.

Shutdown Alert messages appear, brightly highlighted, at the top of every page of a user's session. These are intended to warn the user that shutdown is imminent and they should save their work and log out immediately.



Maintenance Settings

Maintenance Settings

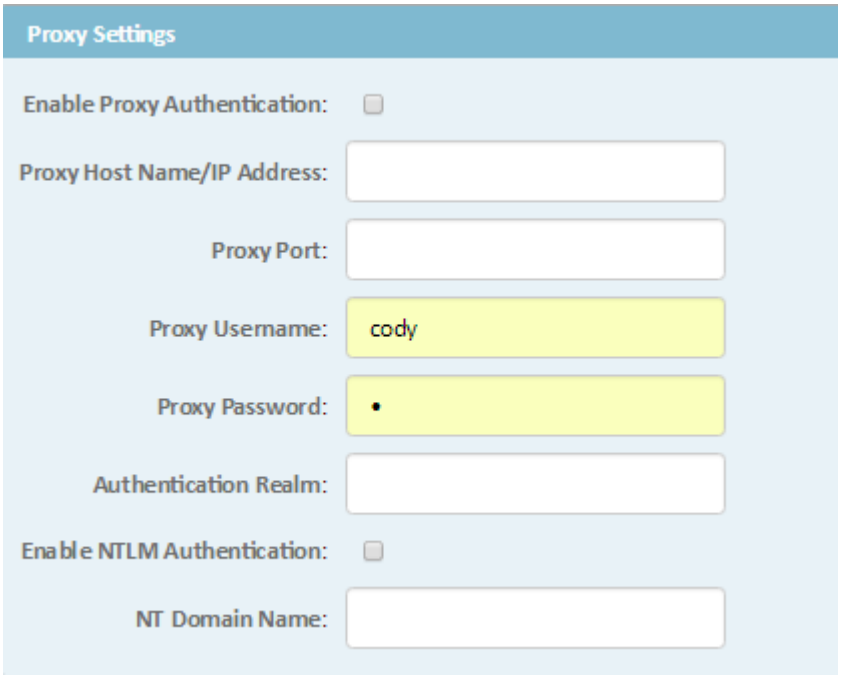
Field	Description
Date	Enter the date at which the maintenance shutdown will occur. You can type the date, or you can click on the calendar icon to select a date.
Time	Enter the time at which the shutdown will occur. Select a time from the drop-down list.

Message	Enter the text of the advisory message to be displayed to users.
Display before shutdown (days)	Enter the number of days before the actual shutdown. During these days each user who logs in will see the advisory message in a separate window when their session begins. Default is 7 days.
Display before shutdown (minutes)	Enter the number of minutes before shutdown. During this period the advisory message will appear, highlighted, at the top of every page in a user's session. Default is 30 minutes.

Once the date and time have passed, TeamConnect will stop issuing advisory messages. However, the values in these fields will persist until they are manually erased or changed in the future.

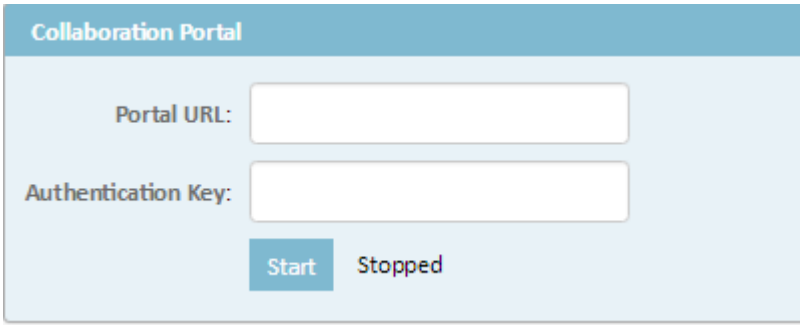
1.3.1.14 Connections Settings

You can configure proxy authentication settings from the Connections page. Depending on your network configurations, proxy authentication may be required for your application to connect to Mitratech's server when viewing the Available Updates (see Viewing Information About Available Updates).



Admin Settings - Connections Page

Proxy authentication information on this page is used when connecting to Mitratech's Available Updates server, and when the Collaborati Spend Management feature connects to Collaborati.



Collaboration Portal

The Collaboration Portal is designed to allow secure access to your TeamConnect instance from outside of your firewall. For more information on this feature, contact Mitratech Support.

1.3.1.14.1 Setting Up Connections

The following steps describe how to configure the Connections page from Admin Settings. Field descriptions are provided in a table below.

To set up Connections

1. Select the **Admin** tab.
2. Click **Admin Settings** under the tab bar.
3. Click the **Connections** link in the left pane.
4. Edit the fields based on descriptions in the Admin Settings - Connections Page fields table.
5. Click **Update**.

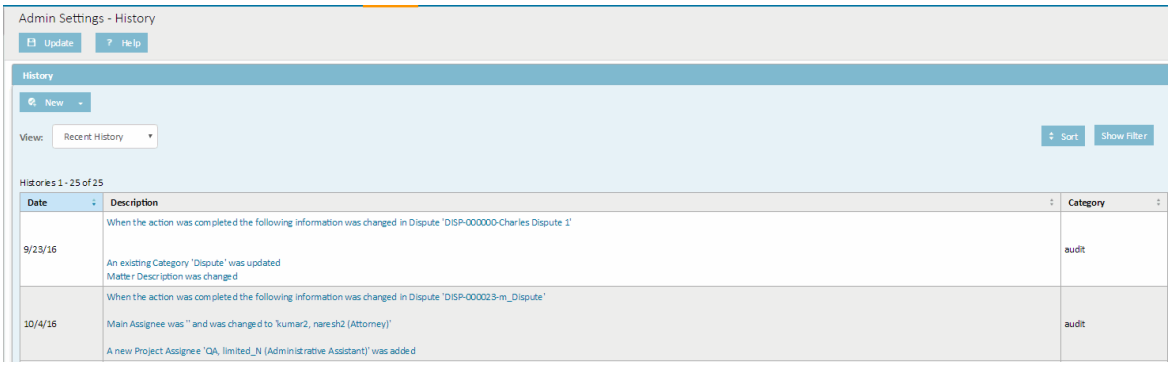
Admin Settings - Connections Page Field Descriptions

Field Names and Descriptions	Default Value
Enable Proxy Authentication—To require TeamConnect to perform certain connections through a proxy server, select the check-box.	Disabled (check-box cleared)
Proxy Host Name / IP Address—Enter the node name, or IP address, by which your proxy server is known on your network.	None
Proxy Port Number—Enter the port number on which your proxy server listens for requests.	None
Proxy Username—Enter the user name which authorizes your requests to the proxy server.	None

Proxy Password—Enter the password which authorizes your requests to the proxy server. Enter plain text. (The password is stored in a secure format in the database.)	None
Proxy Realm—Enter the name of the realm that is associated with the protected area, for example, yourcompanyname.com. The realm name should be ASCII characters, with no spaces or punctuation except a hyphen (allowed only in the middle of the realm name) or a period.	None
Enable NTLM Authentication—If you check this setting, all requests to the proxy server will use the username and password that you use to log in to your operating system domain. Any values in "Proxy Username" and "Proxy Password" will be ignored when NTLM is enabled.	Disabled (check-box cleared)
NT Domain—If NTLM Authentication is selected, enter the name of the NT domain against which your client should be authenticated.	None

1.3.1.15 Admin Settings History

For any changes made to Admin Settings, you can record notes on the **History** page.



Admin Settings - History Page

1.3.1.15.1 Recording a History for Admin Settings

The following steps describe how to use the **History** page from Admin Settings. Field descriptions are provided in a table below.

To record a history for Admin Settings

1. Select the **Admin** tab.
2. Click the **Admin Settings** link under the tab bar.
3. Click **History** from the left pane.
4. Click **New History**.

5. Enter a change **Description**.
6. Click **Update**.

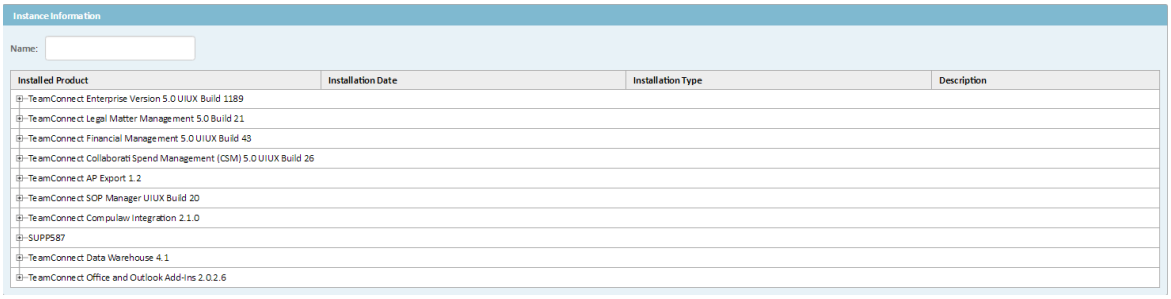
Admin Settings - History Page Field Descriptions

Field (*-required)	Description
***Date**	This field is automatically populated with the current date.
Time	This field is automatically populated with the time that the new history was opened.
***Description**	Enter a change description.

1.3.1.16 About TeamConnect

You can find the TeamConnect version, latest run database scripts, CSM version, and SOP version (if applicable) from the **About** page in Admin Settings.

In addition, you can view the details of the license file. See Viewing Information About Your Product License for explanations of licensing concepts.



Admin Settings - About Page for Version and License Key Information

1.3.1.16.1 Viewing TeamConnect Versions and License Information

The following steps describe how to use the **About** page from Admin Settings. Field descriptions are provided in a table below.

To view TeamConnect versions and license information

1. Select the **Admin** tab.
2. Click the **Admin Settings** link under the tab bar.
3. Click **About** from the left pane. All fields on the resulting page are read-only.

4. Click the **+** sign next to TeamConnect to view a history of database scripts that have been run for the instance.
5. Click the **+** sign next to CSM to view a history of CSM versions that have been installed.
6. (only if SOP is installed) Click the + sign next to SOP to view a history of SOP versions that have been installed.

Admin Settings, About Page Field Descriptions

Field	Description
Installed Product	Displays the product name and version. For database scripts, a TeamConnect version displays as a parent to related scripts.
Installation Date	Displays the date the product was installed.
Installation Type	For database scripts, displays SQL Script.
Description	For database scripts, displays the script name.

1.3.1.16.2 Viewing Information About Available Updates

On the **About** page, the block titled **Available Updates** displays product updates that you can install, download, or request, based on the product versions that you presently have licensed. In addition, this block may display information about products that you do not presently have licensed, but which relate to your licensed products.

Note: *To take advantage of the Available Updates feature, you must allow your application server to make HTTP requests to Mitratech's server. Connection parameters are built into TeamConnect, but if you cannot connect, you may need to configure your firewall to allow connection. Contact Mitratech Support to get specific connection information.*

The fields and links in this block are described below.

Admin Settings, About page, Available Updates block

Field	Description
Product	Displays the product name of the update. Updates are grouped by product.
Version	Displays the specific version of the update.
File Size	For updates that can be downloaded immediately, the file size of the download is shown. For updates that must be requested from Mitratech, **N/A** is displayed.

Instructions	Displays a **Read Me First** link which, when clicked, opens a new window showing release notes and other detailed information about the update. If an update does not have detailed information available from this page, the text **Available Upon Request** is displayed, indicating that you should contact your Mitratech support representative for more information.
Install or Download	Some updates can be applied to your application immediately, while it is being used. Such updates show an **Install Now** link in this field. When you click the link, and answer a confirmation window, the update is downloaded and is immediately applied to your application. The update will affect logged-in users immediately. You should perform the Install action at times when other users are not using the application. (Collaborati Spend Management can be updated through Install Now, but it will not take effect until you stop and restart TeamConnect.) Some updates are more complex and cannot be installed while users are logged in. These updates can be downloaded now and applied at a time when the application has been stopped. Such updates show a **Download Now** link in this field. When you click the link, the update is saved to a file location that you specify. Updates for products that you have not licensed will have a blank entry in this field. Updates which do not have downloads will have an **Available Upon Request** entry in this field.

1.3.1.16.3 Choosing Your Support Options

TeamConnect can send minimal information about your application to Mitratech. In addition, it can send more detailed information about your application's environment, which can aid Mitratech Support in resolving problems more quickly. Check-boxes allow you to grant permission to send:

- Basic product information
- More detailed environmental information

1.3.1.16.4 Viewing Information About Your Product License

On the **About** page, the block titled **License** displays the terms and status of your TeamConnect product license. Your license determines how many users can use TeamConnect.

1.3.1.16.4.1 Licensing Schemes

The types of licensing schemes include the following:

- **Total Users**—In this scheme, both normal users and limited-privilege users are counted together when determining the license limit.
- **Normal Users and Limited-Privilege Users**—In this scheme, there are separate limits stored for normal users and limited-privilege users.

A value of **Site** in any limit field causes that portion of the license to be treated as unlimited.

For specific information about user types, see User General Page Field Descriptions or Creating or Editing Users.

1.3.1.16.4.2 License Style

The **License Style** field indicates how these limits are enforced. If its value is **NAMED**, then you are restricted in how many active users you can enter into the database, even if they do not all use the application simultaneously. You may create more users than the license limit specifies, but the additional users cannot be active.

If the License Style value is **CONCURRENT**, then you may enter more active users than the license limit specifies, but your license restricts how many of them can log in to the application concurrently.

Note: *The count of concurrent sessions is affected by the application server's handling of expired sessions. For example, in BEA WebLogic, the default setting for checking for expired sessions is every 60 seconds. So if you had the maximum number of concurrent users logged in, and one user's session timed out, another user wouldn't be able to log in until WebLogic cleaned up the expired session, which might be up to 60 seconds from the logout time. See WebLogic documentation for information about changing this setting (invalidation-interval-secs).*

If you use the licensing scheme "Normal Users and Limited-Privilege Users", then there will be two limit fields visible and you must specify a License Style value for each limit. The two styles do not have to be the same. For example, you may wish to enforce a NAMED style for the normal user limit and a CONCURRENT style for the limited-privilege user limit.

1.3.1.16.4.3 Uploading a License File

Note: *The following procedure assumes that you obtained the license file from Mitratech Support and saved it to an accessible location.*

To upload and activate the license file

1. Log in to TeamConnect.
2. Click the **Admin** tab, and the click the **Admin Settings** sub-tab link.
3. In the left pane, click the **About** link.
4. In the **License** section, click the **Upload License** button.
5. In the **Upload a new license file** window, browse to the location of the license file and select it.
6. Click **Upload**.

   The license file is now activated and users can log in to TeamConnect.

If you see error messages indicating that you exceeded or are about to exceed the maximum number of active users, contact Mitratech Support for an upgraded license. See License Style for specific information about types of licenses.

1.3.2 TeamConnect Logs

Loggers and Appenders

Use the following terminology for this section. In the logging process, loggers perform the logging operation and capture event message data. Different types of appenders can be defined to physically store the event message data. File appenders or log files are the most common appenders. In addition, appenders are organized in two different ways, by data content and by data format or distribution.

In the area of log data content, there are two types of logs in TeamConnect:

- **System appenders**—Record what TeamConnect is doing in the background by capturing messages generated by the system. This can be useful for debugging or when customizing the application.
- **Audit appenders**—Track user activity, which may be necessary to meet certain policies or compliance regulations regarding user activity.

Division of Logging Functionality

TeamConnect logging features are divided between the Admin and Designer areas.

In the Admin area, you can:

- View file appenders (log files)
- Clear or delete file appenders (log files)
- Change logging severity levels (for loggers). For example, change from Error message tracking level to Debug message tracking level if you need additional details for troubleshooting a TeamConnect component.

In the Designer area, you can define new log appenders (log files or email notifications), edit existing appenders, or toggle audit loggers on/off.

Note: *TeamConnect logging uses the log4j® API.*

1.3.2.1 Default Logs

By default, TeamConnect has several active file appenders (log files in text format). These files are stored in the location specified for log folders at the time when TeamConnect was installed. There are three default logging appenders:

- **Default** (for system logging)—Logs all of the messages that are generated by all of the system loggers and writes them to the **system.log** file.
- **XML Appender**—Logs messages regarding XML requests, according to the level selected for the **XML** logger, and writes them to the **xml.log** file.

- **Default** (for audit logging)—Logs messages from all active audit loggers and writes them to the **audit.log** file.

Note: *If Collaborati Spend Management is installed on your system, the* ***CSM Appender*** *is installed by default.*

For information about how to view the default logs, see Viewing Logs.

1.3.2.2 Working with Logs

From the Admin Logging area, you can perform the following:

- Viewing Logs
- Clearing Logs
- Changing System Logging Levels
- Turning Audit Loggers On or Off

See Appenders for additional information about creating and editing appenders.

1.3.2.2.1 Viewing Logs

The system and audit logs generated by file appenders are stored on the TeamConnect server. You can view logs by:

- Clicking a **View Log** link from TeamConnect.
- Opening the file on the TeamConnect server.

To view a log file

1. Click the **Admin** tab.
2. Click the **Logging** link under the tab bar.
3. To view a system log file
   - Click the **System** link from the left pane.

     The System Logging page displays.
   - From the **System Appenders** section, locate the name of the log you want to view and click the corresponding **View Log** link.
4. To view an audit log file
   - Click the **Audit** link from the left pane.

     The **Audit Logging** page displays.
   - From the **Audit Appenders** section, locate the name of the log you want to view and click the corresponding **View Log** link.

5. The current log file for the log you selected is displayed in a new browser window. The most recent log events are listed at the bottom of the log file.

1.3.2.2.1.1 Things to Remember

- If a log file is very large, clicking the **View Log** link might cause a lockup in your browser session as it tries to transfer the large amount of data from the server. If this is a concern, right-click the **View Log** link, then choose context menu item **Save Link As**, then save the log to a file on a local disk drive. Open that local file with your browser.
- To view the latest log messages, press F5 or click your browser's **Refresh** button.
- For both System Appenders and Audit Appenders, if TeamConnect is running on a cluster of application servers, a drop-down list to the left of the **View Log** link allows you to choose the specific node whose log you wish to view. Node names consist of a machine name, followed by a numeric process ID.
- The log location is specified using the app.logFolder parameter in the Web Application Deployment Descriptor when TeamConnect is installed.

Default TeamConnect Log Folders

If you did not update the Log Folder field (app.logFolder parameter) when updating the teamconnect.properties file using the TeamConnect Installer, you can find TeamConnect logs in the following locations:

- For Apache Tomcat (Linux)—/<*Apache_HOME*>/bin/logs

  For example:

  /opt/tomcat/apache-tomcat-6.0.16/bin/logs

- For Apache Tomcat (Windows)—C:\<*Apache_HOME*>\logs

  For example:

  C:\Program Files\Apache Software Foundation\Tomcat 6.0\logs

- For WebLogic (Linux)—<*WebLogic_Home*>/user_projects/domains/<*domain_name*>/logs

  For example:

  /opt/bea/user_projects/domains/Mitratech/logs

- For WebSphere—<*WebSphere_Home*>/AppServer/profiles/<*profileName*>/logs

  For example, on Windows:

  C:\WAS61\WebSphere\AppServer\profiles\AppSrv02\logs\

1.3.2.2.2 Clearing Logs

For troubleshooting or maintenance purposes, you can manually clear the contents of a log. Clearing a log is different from rolling over a log in that the existing contents of the log will be deleted and not archived to a back-up file.

For example, one scenario in which clearing a log is useful is when you are trying to isolate the log messages related to a specific functional issue. You might clear a log, change the related logger's logging severity level to DEBUG, and then try to reproduce the issue. Afterward, the log would most likely isolate the event messages that can help troubleshoot the issue.

To clear a log file

1. Click the **Admin** tab.
2. Click the **Logging** link under the tab bar.
3. To clear a system log file
   - Click the **System** link from the left pane.

     The **System Logging** page opens.
   - From the **System Appenders** section, locate the name of the log you want to clear and click the corresponding **Clear Log** link.
4. To clear an audit log file
   - Click the **Audit** link from the left pane.

     The **Audit Logging** page opens.
   - From the **Audit Appenders** section, locate the name of the log you want to clear and click the corresponding **Clear Log** link.
5. To view any new log messages, click the corresponding **View Log** hyperlink.

1.3.2.2.3 Changing System Logging Levels

Each message that can be written to a log has an associated log level that indicates the severity of the issue that caused the message to be written to the log. You can specify what severity of messages you want logged for each logger (or TeamConnect component).

Note: *This is a system-wide setting. When you set a logger to a specific log level, you are specifying the most verbose severity level of messages that you want written to appenders defined for that logger. Although there is an analogous setting in the appender definition for log threshold, the logger's logging level overrides the log threshold.*

To set the system logging level

1. Click the **Admin** tab.
2. Click the **Logging** link under the tab bar.

3. To change a system logger's logging level
   - Click the **System** link from the left pane.
   - From the **System Loggers** or **Detailed System Loggers** section, scroll to a logger. From the corresponding Level drop-down list, select a logging level:
     - **Debug**—Minor, frequent events in TeamConnect.
     - **Info**—Significant, frequent events in TeamConnect.
     - **Warn**—Minor issues external to TeamConnect.
     - **Error**—Serious issues that are usually associated with a Java exception.
     - **Fatal**—Rarely used in TeamConnect.

       By default, system logger levels are set to **Error**, but you can adjust the severity based on the type of information you need to be captured in your logs.

       See System Loggers and Detailed System Loggers for a description of the system loggers that come with standard TeamConnect.
4. Click **Update**.

   Your changes take effect immediately. All appenders defined for these loggers are now logging messages according to the log level that you have specified, and according to each appender's threshold.

System Loggers

Logger	Description
Request	Logs HTTP request information including headers, cookies, and parameters. This logger can automatically be set to the Debug level each time TeamConnect application is restarted. This depends on the value of the syslog.basic.request parameter in the Web Application Deployment Descriptor.
Response	Logs HTTP response header information.
Rule	Logs messages generated by rules that have been defined for your implementation of TeamConnect.
SQL	Logs TopLink-generated SQL statements. This logger can automatically be set to the Debug level each time TeamConnect application is restarted. This depends on the value of the syslog.basic.sql parameter in the Web Application Deployment Descriptor.

XML	Logs messages regarding XML requests.

Detailed System Loggers

Logger	Description
Authentication	Logs all messages regarding user authentication.
Batch Display Component	Logs all messages regarding the batch display component.
Custom Blocks	Logs all messages regarding custom blocks.
Deletion	Logs all messages regarding record deletion.
IMAP	Logs events related to the TeamConnect IMAP Server and Email Viewer.
Portal	Logs all messages regarding portal panes, including custom content.
Reflection	Logs all messages generated by TeamConnect's reflection factory.
Search	Logs all messages regarding search views and searching for records.
Stores	Logs all messages regarding TeamConnect stores.
Sync Server	Logs all messages regarding cache synchronization.
Tools	Logs all messages regarding both system and custom tools.
UI Components	Logs all messages regarding rendering of TeamConnect screens.
WebDAV	Logs all messages related to WebDAV document management.

1.3.2.2.4 Turning Audit Loggers On or Off

Audit loggers send their messages to logs defined by audit appenders. Audit loggers are turned on or off system-wide. You do not have to set levels for audit loggers.

You can turn audit loggers on or off as needed. When turned on, the logger's messages immediately start getting logged for all defined audit appenders.

To turn audit loggers on or off

1. Click the **Admin** tab.
2. Click the **Logging** link under the tab bar.
3. Click the **Audit** link from the left pane.

   The **Audit Logging** page opens.
4. From the **Audit Loggers** section, locate the name of the log you want to turn on and select **On** from the drop-down list.
5. Locate the name of the log you want to turn off and select **Off** from the drop-down list.
6. For descriptions of available audit loggers, see the following table.

Audit Loggers

Logger	Description
API Read	Turn on this logger to log read calls to the API.
API Update	Turn on this logger to log update calls to the API.
Page Open	Turn on this logger to log the opening of a page by a user.
Login/Sign Off	Turn on this logger to log user sign on/off events.
Export/Download	Turn on this logger to log PDF exports or downloads from users.

Example Results for Users

For example, if **Internal Time** is selected in the **Budget for** section and **Annual+Month** is selected in the **Extend budget level** by section, the following corresponding accounts are created for each dispute or transaction record:

- Internal Fees
- Internal Fees : Annual (one for each fiscal year)
- Internal Fees : Monthly (twelve for each fiscal year)

1.3.3 TeamConnect Administrator Tools

Several administration functions are performed by starting the related tool from the Tools page (accessed from **All Services**, **Tools**.)

1.3.3.1 Scheduled Actions Monitor

Use this tool to observe and control actions that are scheduled to execute at specific times in the future.

Note: *The right to this tool must be assigned before the tool is visible to a user. The right is found under System Rights, User Rights, Scheduled Action.*

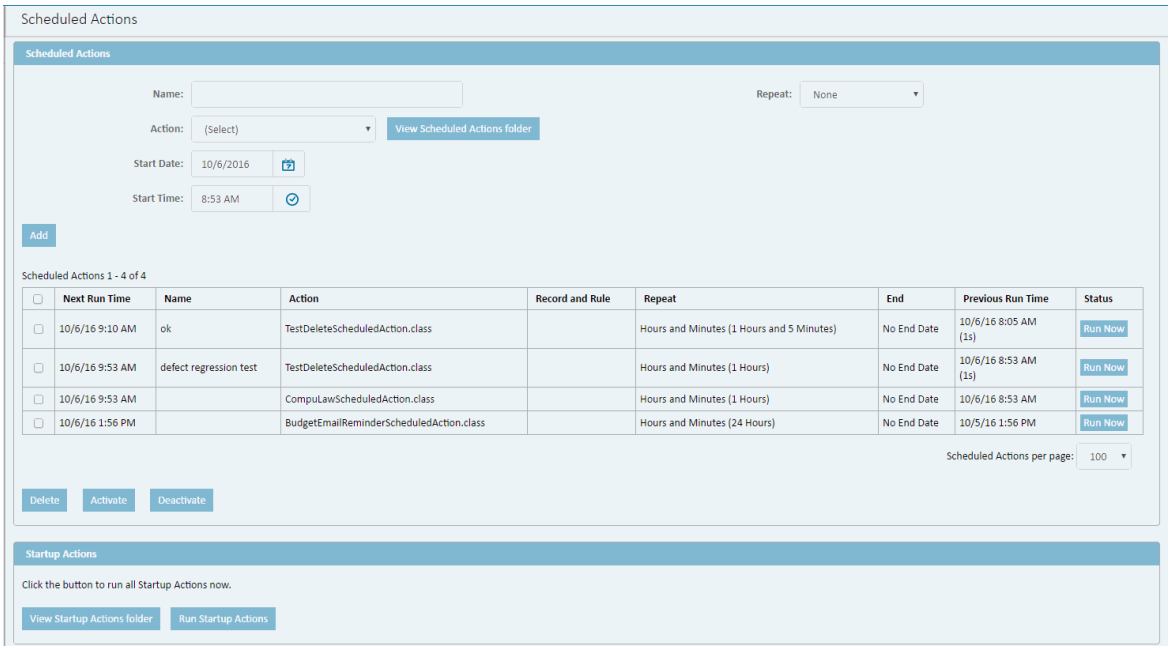
All actions pending execution that have been scheduled by Scheduled Action rules, or by Custom Action rules that utilize the Scheduled Actions API, automatically get listed in the Scheduled Actions Monitor. You can use this page to view and delete pending actions when necessary.

For example, the system's Scheduled Action rules may be set to automatically create tasks for a user, but those tasks might no longer need to be created because of other circumstances. As the Administrator, you can delete the scheduled actions that are going to eventually create these tasks on the scheduled dates.

You can also create entirely new scheduled actions on an as-needed basis.

1.3.3.1.1 Accessing the Scheduled Actions Monitor

To access the Scheduled Actions Monitor, select **Scheduled Actions** from the **Tools** link. The Scheduled Actions Monitor opens, as shown in the following image. You must have the appropriate rights to access and view the Scheduled Actions Monitor.



Scheduled Actions Monitor Screen

You can refresh the information on this screen at any time by using your browser's **Refresh** button.

1.3.3.1.2 Tasks Available from the Scheduled Actions Monitor

From this page you can do any of the following tasks:

- Create a New Scheduled Action
- Actions Against the Table
- Activate Scheduled Actions
- Delete Scheduled Actions
- Run a Scheduled Action

1.3.3.1.2.1 Create a New Scheduled Action

Create a new scheduled action by entering values in the fields at the top of the page, then clicking **Add**. The new scheduled action is in active status and will run at the time you specified.

The following table describes these fields.

Scheduled Actions Monitor - Creating a New Scheduled Action

Field or column	Description
Name	Enter a name that describes the action.
Repeat	If this action will execute only once, keep the default value of **None** in this drop-down list. If this action will be executed repeatedly, choose the time interval from the list of choices. Specify the period of time between rule action repetitions after the initial execution after the rule has been triggered. Additional options will appear depending on the selection in the **Repeat** drop-down list. • **Hours and Minutes—**The scheduled action will repeat after the specified number of **Hours** and **Minutes** have passed. • **Daily—**The scheduled action will repeat every day. Select the **Weekdays only** check-box to set the rule action to be repeated only from Monday through Friday. • **Weekly—**The scheduled action will repeat every week. Use the **Day** drop-down list to select on which day of the week the action will be repeated. • **Monthly—**The scheduled action will repeat every month. Use the **Day of the Month** drop-down list to select on which day of the month the action will be repeated, from **1** to **31**, or **Last** for the last day of the month. • **Yearly—**The scheduled action will repeat every year. Use the **Day and Month** drop-down lists to select on which month and day of the year the action will be repeated.

End	Specify when the scheduled action repetitions will stop. • **No End Date—**The scheduled action will repeat indefinitely until the rule is deleted or inactivated. This is the default option. • **After—**The scheduled action will execute for the specified number of repetitions. • **Until—**The scheduled action will repeat until the specified date.
Action	This drop-down list contains all the executable actions that have been uploaded to the **Top Level / System / Scheduled Actions** folder in Documents. Choose which action (usually a Java class file) should be associated with the new scheduled action that you are creating. The link **View Scheduled Actions Folder** opens this folder in Documents so that you can work with its contents, if necessary.
Start Date and Start Time	These two fields specify the first time that the new scheduled action should be run. For actions that are repeated, this time becomes the basis for all the future repetition intervals. If you enter a date and time that are in the past, and this is not a repeating action, an error message is shown.

Important: *Actions that are scheduled to repeat monthly on the 29th, 30th, or 31st day of the month will not occur in months that do not have those dates. To avoid this issue, use the **Last** option for the last day of the month.*

1.3.3.1.2.2 Actions Against the Table

The table in the lower portion of the Monitor shows which scheduled actions have run and which are pending. You can take several actions by using this table and its adjacent buttons. Here are the elements of the table:

Scheduled Actions Monitor Screen

Field or column	Description
Next Run Time	All actions have a next run time, except startup actions and actions that have been deactivated. If something prevents an action from running at the scheduled time - for example, if TeamConnect itself has an outage - this time will remain unchanged.
Name	This is an optional, user-friendly name that describes the action.
Action	This is the actual file that will be run when the action runs.

Record and Rule	Many scheduled actions are the result of a scheduled-action rule running against a specific record. In this case, the name of the record appears here as a hyperlink. Clicking the name will open the record. The name of the scheduled-action rule also appears here.
Repeat	Indicates the time interval in which the action is scheduled to repeat. If it is a one-time action, this field contains **none**.
End	For repeating actions, describes the condition under which the repetitions will end. See "Repeat" in the Scheduled Actions Monitor table for details.
Previous Run Time	Shows the last date/time this action was run, and duration of the run. If an action failed during its last run, a failure message is shown here. For one-time actions, this field will always be empty.
Status	**Inactive** for actions that have been deactivated. **Running** for actions that are currently running. Otherwise, the **Run Now** button appears. Clicking the **Run Now** button causes the action to run immediately. Such a run does not count towards the number of repetitions before the end, if a number had been configured for this action.

1.3.3.1.2.3 Deactivate Scheduled Actions

If you deactivate a scheduled action, it remains pending but does not execute.

To deactivate a scheduled action

1. Select the check-box next to the scheduled action that you want to deactivate. You may select more than one check-box at once.
2. Click **Deactivate**.

The selected scheduled action(s) is deactivated and the Monitor refreshes to reflect this. The value in field **Status** now says "Inactive".

1.3.3.1.2.4 Activate Scheduled Actions

If you activate a scheduled action that had been inactive, it will run at its next scheduled date and time. If that date and time are already past, it will run immediately.

To activate a scheduled action

1. Select the check-box next to the scheduled action that you want to activate. You may select more than one check-box at once.

2. Click **Activate**.

The selected scheduled action(s) is activated and the Monitor refreshes to reflect this.

1.3.3.1.2.5 Delete Scheduled Actions

If you have the appropriate rights, you can delete scheduled actions to prevent them from being executed.

To delete a scheduled action

1. Select the check-box next to the scheduled action that you want to delete. You may select more than one check-box at once.
2. Click **Delete** and confirm that you want to delete the selected scheduled action.

The selected scheduled action(s) is deleted and the Monitor refreshes to reflect this.

1.3.3.1.2.6 Run a Scheduled Action

The **Run Now** button, if visible in the Status field for a scheduled action, can be clicked to cause the action to run immediately, notwithstanding its next scheduled run date. This button is not visible if the action has been deactivated.

1.3.3.1.3 Things to Remember

If a scheduled action is configured to end after a certain number of repetitions, that number is decremented each time the action is run. Even if the action fails due to an internal error or some external reason (e.g., database server is down), the number is decremented. However, running the action via the **Run Now** button does not decrement the number of repetitions remaining.

If an action is scheduled to run at a certain time interval, but then is deactivated, and is not re-activated until after that next scheduled run time, the action will run immediately. It will then revert to its regularly scheduled time interval.

1.4 Authentication

Authentication is the process of securely identifying a user who is requesting a connection to TeamConnect. TeamConnect contains a facility for standard authentication, in which the user name and password are stored within TeamConnect itself. In addition, TeamConnect provides two plug-ins to accommodate two other popular means of custom authentication: NTLM and LDAP.

1.4.1 Login URLs

TeamConnect has two types of login URLs.

Login URL	Description

System Default	Give users the System Default login URL if you have selected **System Default** authentication in their **User Account** screen settings. This is the default login URL.
	If you have not installed any custom authentication mechanisms into TeamConnect, give this login URL to your users.
	The URL takes the form:
	`http://[host]/[context path]/login`
	For example:
	`http://tcserver/tc240/login`

Standard TeamConnect	Give users the Standard TeamConnect login URL if you have selected **Standard TeamConnect** authentication in their **User Account** screen settings. If you have installed custom authentication mechanisms into TeamConnect, give this login URL only to users who are not authenticated by those custom mechanisms.
	The URL takes the form:
	`http://[host][:port]/[context path]/standardLogin`
	For example:
	`http://10.0.1.72:5001/tc240/standardLogin`

The **TeamConnectAdmin** account always uses the standard login URL.

The user who administers the Data Warehouse feature must log in with standard authentication.

For details on authentication and its effect on logging in to TeamConnect, see Authenticating Yourself.

1.4.2 NTLM Authentication Plug-in

If you use TeamConnect with a Software as a Service (SaaS) license, you do not need to perform any of the tasks described in this section, except for Enabling NTLM Authentication for TeamConnect Users.

This document provides the instructions to install and configure TeamConnect to use the NTLM Authentication plug-in to enable single sign-on and user authentication. For other general information about the plug-in, including the software prerequisites for running it, read the release notes.

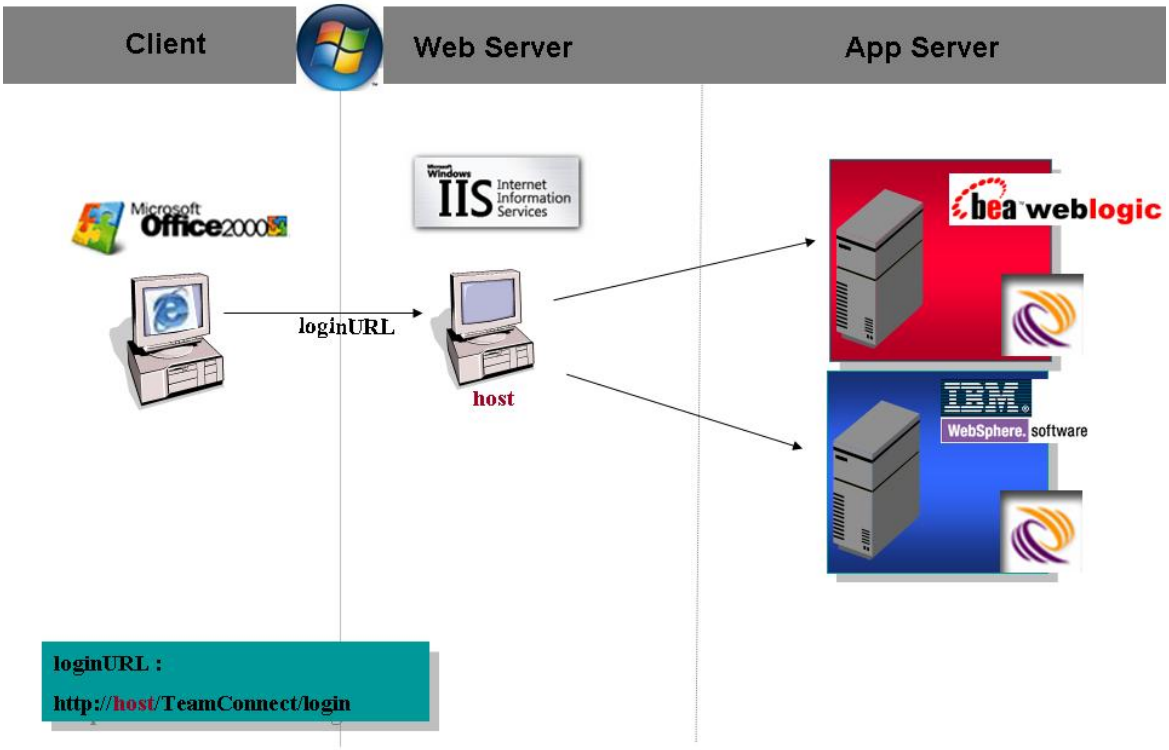
The NTLM authentication plug-in allows TeamConnect to authenticate a user through a challenge/response system in conjunction with Microsoft® Internet Information Services (IIS). When authenticated through NTLM, the user no longer has to submit separate authentication credentials, such as username and password, to access TeamConnect.

When the NTLM authentication plug-in is enabled, users who are successfully authenticated bypass the TeamConnect login page and go directly to their TeamConnect home page. Aside from the lack of a login page, there is no change to the user interface.

If the user account fails authentication through NTLM a denial page is displayed. When troubleshooting denials, verify that the login user ID corresponds to a valid user account name within

TeamConnect and that the appropriate domain is specified in the System Settings page in the Admin section of TeamConnect.

Shown below is a diagram of the general concept of NTLM authentication as it affects the application server and web server in TeamConnect:



Conceptual View of NTLM Authentication

1.4.2.1 NTLM Prerequisites

The following requirements must be met in order to use the NTLM authentication plug-in for TeamConnect:

- Your TeamConnect environment must be a pure Microsoft solutions environment using Internet Information Services (IIS). The environment must include an application server that is compatible with IIS. For specific versions of IIS and application servers that are supported, refer to Application and Web Servers.
- Within TeamConnect, you must specify a list of one or more domains in which to authenticate all users. NTLM automatically authenticates users based on their Windows login name and domain. You can, however, change the behavior of the default plug-in.
- Each user that is authenticated through NTLM must have a corresponding user name defined in TeamConnect.
- The application servers supported are the same for your Enterprise instance. For more detail, please see Application and Web Servers.

1.4.2.2 Configuring Internet Information Services

The process below describes the sequence of configuration requirement tasks:

- Configure Microsoft IIS plug-in to disable anonymous access.
- Customize Message Screens.
- Upload the NTLM authentication configuration class files to the Documents area of TeamConnect.
- Enable NTLM authentication through the **Admin Settings/Security** page of TeamConnect.
- Configure TeamConnect user accounts for using NTLM authentication.

It also provides two URLs that can be used for logging in and explains the difference between them.

The following sections explain each task in the order in which you should perform them.

1.4.2.2.1 Disabling Anonymous Access

In order to use NTLM authentication you must disable anonymous access in IIS. When anonymous access has been disabled, IIS looks for other means of authentication and finds NTLM authentication.

Note: *The following steps are for Windows XP Professional. If you are using another version of Windows, these steps might differ.*

To disable anonymous access to IIS

1. On the computer running your web server, click **Start > Programs > Administrative Tools > Internet Services Manager**.
2. In the left pane, open **Web Sites**, click **Default Web Site**, and then be certain that the web site is stopped. Click the **Stop** button in the toolbar, if necessary.
3. Right-click **Default Web Site**, and then click **Properties**.
4. Click the **Directory Security** tab.
5. In the **Anonymous Access and Authentication Control** section, click **Edit**.
6. Clear the **Anonymous Access** check box. If a checkbox named **Integrated Windows authentication** is present, be sure that it is presently checked. Then click **OK**.
7. Click **OK**.
8. With **Default Web Site** highlighted, click the **Start** button in the toolbar to start the web site.
9. Close the Internet Information Services console.

Important: *You must also configure the proxy plug-in for IIS. For general information about doing this, see Web Proxy Settings.*

Stop and restart IIS when these steps are completed.

1.4.2.3 Editing the NTLM Configuration File

The configuration file, **authenticationDescriptor.properties**, needs to be edited to match your particular network environment. Shown below is the default text of this file.

```
## This is a sample properties file for NTLM authentication. You can
tailor it to your specific
## situation to work with the NTLM authentication mechanism included
within TeamConnect. All
## un-commented properties in this file are required, though their
values can be changed.
# Identification properties for this authentication component
tc.displayName=NTLM based Single Sign On
tc.uniqueId=SNTLM
tc.isSSO=true
# Custom page mappings (omit any that do not apply)
#page.badCredentials=tryagain.html
#page.lockedAccount=giveup.html
#page.maximumLogins=sorry.html
#page.logout=goodbye.html
#page.sessionTimeout=missedyou.html
# NTLM configuation properties
#
# The NT domain against which clients should be authenticated.
ntlm.tcDomain=TCDOMAIN
ntlm.remoteUserHeader=
```

The value of **ntlm.tcDomain** can be a single domain name or it can be a list of domain names, delimited by semicolons. The domain portion of a user's login name (such as "terry@mycompany.com") is matched against this property value and, if a matching domain is not found, authentication fails.

If you expect to override the default error message pages, modify the "page mappings" section to supply your own HTML file names.

Property **ntlm.remoteUserHeader** must exist in the configuration file, but it does not always need to have a value associated with it. You may find that for WebLogic application servers, a value of `Proxy-Remote-User` works best and, for WebSphere application servers, a value of $WSRU works best.

Note that even if you do not use properties **page.logout** and **page.sessionTimeout**, TeamConnect will construct a logout page on the fly to use in these situations, to avoid redisplaying the login page, which would cause an automatic re-login with NTLM.

1.4.2.4 Installing the NTLM Configuration File

NTLM authentication plug-in installation consists of a configuration file that must be uploaded to a specific directory within the **Documents** area of TeamConnect: authenticationDescriptor.properties

You must edit the **authenticationDescriptor.properties** file, as described in Editing the NTLM Configuration File.

To install the NTLM Authentication configuration file

1. In the TeamConnect tab bar, select **Documents**.
2. Navigate to **Top Level**, then **System**.
3. Create a folder named **Authentication**.
4. In the **Authentication** folder that you just created, create a sub-folder named **NTLM**.
5. In the **NTLM** folder that you just created, create the following sub-folders:

   Caution: *The folder names must be entered exactly as they appear below.*

   - **classes**
   - **pages**

6. In the **classes** folder that you just created, upload this file: authenticationDescriptor.properties
7. The **pages** folder does not require any file uploads, unless you choose to override the default error message pages, using the page.xxx properties in the configuration file. If so, you would upload your matching custom error message pages to this folder.

The NTLM Authentication plug-in is now installed.

1.4.2.5 Enabling NTLM Authentication for TeamConnect Users

Before assigning authentication methods to individual users, be sure that NTLM has been chosen as the default authentication mechanism. To do so, refer to Enabling a Default Authentication Method.

To enable other users to log in to TeamConnect using NTLM authentication, each user account must be properly configured except for **TeamConnectAdmin**. However, if you followed the directions in Enabling a Default Authentication Method, NTLM is now the system default authentication mechanism, and users who are already set to use the default need no editing. You need to perform overrides only:

- For users who may have previously been overridden with a different authentication method and are now using NTLM. In this case you can set their method to **(System Default)**.
- For users who are not using NTLM.

For details on performing an override, see Overriding Authentication for Individual Users.

Important: *For user "TeamConnectAdmin", do not attempt to use NTLM authentication. Force this user to go through standard authentication by appending* ***/standardLogin*** *to the end of the URL that launches TeamConnect.*

Important: *When using Web Services and NTLM to connect to TeamConnect, be sure that the URL in your NTLM configuration points to the TeamConnect application server, not the Internet Information Server.*

For information about which login URL to give your users based on the authentication mechanism, see Login URLs.

1.4.3 LDAP Authentication Plug-in

By default, TeamConnect authenticates each user by comparing a username and password entered in the login screen with information stored in the TeamConnect database. This is a safe and secure method of authentication, but your organization might choose to integrate the TeamConnect authentication process with a network-wide authentication mechanism, such as an LDAP (**L**ightweight **D**irectory **A**ccess **P**rotocol) server.

You can integrate any version of TeamConnect 3.0 and higher with LDAP by uploading a configuration file to TeamConnect's **Documents** area. Once this is done correctly, the LDAP authentication plug-in is available on the **Authentication Plug-In** block of the **Admin Settings/ Security** page.

TeamConnect also provides the ability for you to enable LDAP authentication per user through a setting on the user's account.

Note: *TeamConnect's integration with LDAP for authentication does not provide single-sign-on (SSO) functionality to TeamConnect. Each user must sign on to TeamConnect, and then sign on to other applications.*

For additional assistance, such as customization for your LDAP directory structure or authentication using password comparison, contact Mitratech Client Services. In addition, if your server is using password encryption or an SSL connection, certain changes might be required in the plug-in. These modifications can be made by Mitratech.

This guide does not cover managing access rights in TeamConnect. You must define group rights to TeamConnect objects and tools directly in TeamConnect. TeamConnect is not compatible with LDAP Access Control Lists (ACL).

As with other applications to which users gain access through your LDAP server, users can log in to TeamConnect only when the LDAP server is available.

1.4.3.1 LDAP Authentication Prerequisites

The process of configuring TeamConnect for LDAP integration includes the following basic steps:

1. Creating Custom LDAP Authentication Error Pages—(optional) Create custom HTML pages for use with LDAP authentication.
2. Defining LDAP Parameters—Enter information in TeamConnect's LDAP properties file.
3. Installing LDAP Plug-in Files—Upload a TeamConnect LDAP properties file to the TeamConnect Documents area. You can also upload customized authentication error messages.
4. Enabling a Default Authentication Method—Enable the LDAP plug-in from TeamConnect Admin Settings.
5. Overriding Authentication for Individual Users—Allows you to enable LDAP authentication for individual user accounts. This step is only required if you do not select LDAP as the default authentication mechanism in the previous step.

1.4.3.2 Creating Custom LDAP Authentication Error Pages

You have the option to create customized screens for logging into TeamConnect using LDAP authentication and related error messages. To enable custom error pages, you must do the following:

1. Create custom error pages.
2. Update the LDAP **authenticationDescriptor.properties** file properties for the new pages.
3. Upload the custom pages to the TeamConnect Documents area folder:

   \Top Level\System\Authentication\LDAP\pages

   See Installing LDAP Plug-in Files for more information.

Note: *If you choose not to create customized error and login pages then you should comment out related lines from the LDAP authenticationConfiguration.properties file.*

Requirements

The custom pages should be in HTML format. The custom page file extensions should be .html

If any custom pages require images, those images should be uploaded to the TeamConnect Documents area

Custom Error Pages List

A list of pages that can be customized follows. Each page has a corresponding property in the LDAP **authenticationDescriptor.properties** file whose value should match the file name you create per page. The corresponding properties are described in Defining LDAP Parameters.

- Authentication Failed page
- Normal Logout page
- Session Timeout page
- Restore Session page
- Bad Credentials page
- Account Locked page

1.4.3.3 Defining LDAP Parameters

To enable TeamConnect to use your LDAP plug-in, you must provide certain parameters which represent your environment and save them in a properties file. You must modify the **authenticationDescriptor.properties** file for LDAP authentication and enter the appropriate information in these parameters according to the descriptions in the table below.

Note: *To comment out a property, type* **#** *at the beginning of the line to comment it out.*

LDAP Parameters and Definitions

Parameter	Description	Example

tc.displayName	Required field. Do not change this value.	
tc.uniqueId	Required field. Do not change this value.	
tc.isSSO	Required field. Do not change this value.	
ldap.host	LDAP server host name. This value is combined with ldap.port and ldap.root to form the ldap-server URL.	`10.0.0.1` ***Note:*** *When combined with ldap.port and ldap.root values, an ldap-server URL like* `ldap://10.0.0.1:389/dc=myserver,dc=org` would result
ldap.port	LDAP server port. This value is combined with ldap.host and ldap.root to form the ldap-server URL.	`389` ***Note:*** *When combined with ldap.host and ldap.root values, an ldap-server URL like* `ldap://10.0.0.1:389/dc=myserver,dc=org` would result
ldap.root	Enter the top-level DN (distinguished name) under which the TeamConnect users can be found in the LDAP directory structure. This value is combined with ldap.host and ldap.port to form the ldap-server URL.	`dc=springframework,dc=org` ***Note:*** *When combined with ldap.host and ldap.port values, an ldap-server URL like* `ldap://10.0.0.1:389/dc=myserver,dc=org` would result
ldap.userDn	Enter the name of the attribute that stores the username on the LDAP server. TeamConnect will log into the LDAP server with this username.	`directory.username=uid`

	Note: *Do not confuse the attribute name with the actual value of the username that it stores.*	
ldap.password	Enter the name of the attribute that stores the password on the LDAP server. TeamConnect will log into the LDAP server with this password. ***Note:*** *Do not confuse the attribute name with the actual value of the password that it stores.*	`directory.password=userPassword`
ldap.userDnPatterns	The elements of the user's Distinguished Name that, when assembled, will form the complete DN to authenticate the user's identity to the LDAP Directory Service (if authentication is required).	`uid={0},ou=people` ***Note:*** *This example would obtain the DN for the user by substituting the user login name in the supplied pattern and attempting to bind as that user with the login password. This would work if all your users are stored under a single node in the directory.*
ldap.groupDnPattern	The group's Distinguished Name. For authentication, users will need to belong to this group. You must create and configure this group on the LDAP server. Then add users to this group.	teamconnect
ldap.groupRoleAttribute	The attribute which contains the name of the authority defined by the group entry. This parameter is used to load authorities from groups in the LDAP directory.	The default value is cn
page.badCredentials	Page to display if the password does not match the password stored for the TeamConnect user account.	`/login.html?error=bc`

	Note: *If you do not create a custom file, then comment out this line.*	
page.lockedAccount	Page to display if the TeamConnect user account is locked and User Locking is enabled in TeamConnect settings. ***Note:*** *If you do not create a custom file, then comment out this line.*	`/login.html?error=1`
page.maximumLogins	Page to display if the LDAP account has already exceeded their maximum allowed sessions. ***Note:*** *If you do not create a custom file, then comment out this line.*	`/login.html?error=1`
page.logout	This page is shown when a user logs out normally. ***Note:*** *If you do not create a custom file, then comment out this line.*	`/login.html`
page.sessionTimeout	This page is shown when a user's session times out. ***Note:*** *If you do not create a custom file, then comment out this line.*	`login.html?error=2`

To define LDAP parameters in the properties file

1. Copy the LDAP **authenticationDescriptor.properties** file from the TeamConnect Installer installation path (subfolder utilities\config\ldap) to your local hard disk.

   Tip: *When editing a properties file, use a text-only editor to ensure no formatting codes get inserted by the application.*

2. Edit the **authenticationDescriptor.properties** file according to your environment. For details about each parameter, see the LDAP Parameters and Definitions table.
3. Save and close this file.
4. Make note of the location of this modified file so that you can use it in the next procedure.

Now that you have configured your LDAP plug-in, you must upload a file into TeamConnect, as described in Installing LDAP Plug-in Files.

1.4.3.4 Installing LDAP Plug-in Files

This section describes:

1. Creation of TeamConnect Documents area folders for LDAP files
2. Uploading LDAP configuration files for TeamConnect
3. Uploading custom LDAP screens

LDAP authentication plug-in installation consists of a configuration file, **authenticationDescriptor.properties**, that must be uploaded to a specific directory within the **Documents** area of TeamConnect:

You *must* edit the **authenticationDescriptor.properties** file, as described in Defining LDAP Parameters.

To install the LDAP Authentication configuration file

1. In the TeamConnect tab bar, select **Documents**.
2. Navigate to **Top Level**, then **System**.
3. Create a folder named **Authentication**.
4. In the **Authentication** folder that you just created, create a sub-folder named **LDAP**.
5. In the **LDAP** folder that you just created, create the following sub-folders:

   Caution: *The folder names must be entered exactly as they appear below.*

   - **classes**
   - **pages**

6. In the **classes** folder that you just created, upload this file: **authenticationDescriptor.properties**
7. The **pages** folder does not require any file uploads, unless you choose to override the default error message pages. using the page.xxx properties in the configuration file. If so, you would upload your matching custom error message pages to this folder.

The LDAP Authentication plug-in is now installed.

To complete the implementation of LDAP, make sure that you are using the correct default authentication method, as described in Enabling a Default Authentication Method. If LDAP is not your default authentication method, override individual users who need LDAP, as described in Overriding Authentication for Individual Users. If LDAP is your default authentication method, you need to perform overrides only:

- For users who may have previously been overridden with a different authentication method and are now using LDAP. In this case you can set their method to **(System Default)**.
- For users who are not using LDAP.

Also, user **TeamConnectAdmin** should always use the Standard Authentication method. You can force this behavior by appending **/standardLogin** to the end of the URL that launches TeamConnect for that user.

1.4.3.5 LDAP Authentication Sample Files

This section provides sample files described in this guide.

- Sample Custom Log-in Page
- Sample Custom Error Page
- Sample Restore Session Page
- Sample LDAP Configuration File

1.4.3.5.1 Sample Custom Log-in Page

Note: *You do not need to customize the TeamConnect login page for LDAP Authentication. If you customize the login page, however, you must reference the j_spring_security_check servlet, the user field input value should correspond to the j_username variable, the password field input value should correspond to the j_password variable as shown in the example below.*

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://
www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
<title>Log In - TeamConnect 3.0</title>
</head>
<body scroll="no">
    <div id="horizon" style="margin-top:150px">
        <div id="content">
            <div id="contentText">
                <center>
                <table class="logincontent" border="0" width="600" cellpadding="0"
                cellspacing="0">
                <tr>
                <td style="background-image: url(images/bg_login.jpg); background-
                repeat: no-repeat;">
                <!-- LOGIN TABLE [BEGIN] -->
                    <table border="0" width="600" cellpadding="0" cellspacing="0">
                    <tr>
                        <td colspan="2" style="line-height: 1.5em;" align="center">
                        </td>
```

```
                    </tr>
                    <tr>
                        <td height="150" align="center">
                            <form method="post" id="loginForm" name="loginForm"
                            action="j_spring_security_check">
                            <table border="0" cellpadding="5" cellspacing="0"
                            style="margin: 10px;">
                            <tr valign="middle">
                                <td width="90" align="right" nowrap><b>User Name:</b></
                                td>
                                <td align="left"><input type="text" name="j_username"
                                id="j_username" size="18" maxLength=50 tabindex="1"/></
                                td>
                            </tr>
                            <tr valign="middle">
                                <td align="right" nowrap><b>Password:</b></td>
                                <td align="left"><input autocomplete="off"
                                type="password" name="j_password" id="j_password"
                                size="18" maxLength=50 tabindex="2"/></td>
                            </tr>
                            <tr valign="middle">
                                <td align="right" nowrap> </td>
                                <td colspan="2" align="left" class="texthdr"
                                nowrap><input type="submit" name="submit" value="Log
                                In" class="mainSearchBtn"></td>
                            </tr>
                            </table>
                            </form>
                        </td>
                    </tr>
                </table>
                </td>
                </tr>
                </table>
                </center>
            </div>
        </div>
    </div>
</body>
<script>
$("j_username").focus();
</script>
</html>
```

1.4.3.5.2 Sample Custom Error Page

Note: *You do not have to customize error pages. If you create custom error pages, they must be in HTML format (with file extension .HTML). You can use existing TeamConnect error message JSP files but cannot upload custom JSP files.*

```
<html>
    <head>
    </head>
    <body>
    Authentication error.
    </body>
</html>
```

1.4.3.5.3 Sample Restore Session Page

Note: *The following is a sample HTML page content you may choose to redirect to for the LDAP parameter, ldap.restoreSessionUrl*

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://
www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
<title>You have another session open</title>
</head>
<body>
    <div id="horizon" style="margin-top:150px">
        <div id="content">
            <div id="contentText">
                <center>
                    <table border="0" width="500" cellpadding="0" cellspacing="0"
                    style="margin: 20px;">
                        <tr valign="top">
                            <td class="bgcolor16" align="left" style="padding: 20px;
                            border-bottom: 1px solid #CCCCCC; line-height: 1.7em;">
                            <table border="0" cellpadding="3" cellspacing="0">
                            <tr valign="top">
                                <td style="padding: 8px 0px 0px 15px;">
                                    <span class="titlehdr5">You have another session
                                    open</span>
                                </td>
                            </tr>
                            <tr>
                                <td style="padding: 8px 0px 8px 15px;"><span
                                style="padding:200px 0px 20px 0px;">You are either
                                logged in at another location or did not log out of
```

```
                        your previous session.<p>Do you want to recover the
                        previous session and return to what you were working
                        on, or start a new session (losing all previous work)?
                        </span></td>
                    </tr>
                    <tr>
                        <td align="center" class="texthdr">
                        <form name="mainForm" action="restoreSession.htm"
                        method="post">
                        <input type="button" name="recover" value="Recover
                        Session" class="mainSearchBtn"
                        onclick="document.getElementById('restoreSession').valu
                        e=true;document.mainForm.submit();" /> 
                        <input type="button" name="new" value="New Session"
                        class="mainSearchBtn"
                        onclick="document.getElementById('restoreSession').valu
                        e=false;document.mainForm.submit();" /> 
                        <input type="hidden" id="restoreSession"
                        name="restoreSession" value="true" />
                        </form>
                        </td>
                    </tr>
                    </table>
                    </td>
                </tr>
            </table>
        </center>
    </div>
</div>
</div>
</body>
</html>
```

1.4.3.5.4 Sample LDAP Configuration File

```
## This is a sample properties file for LDAP authentication. You can
tailor it to your specific
## situation to work with the LDAP authentication mechanism included
within TeamConnect. All
## un-commented properties in this file are required, though their values
can be changed.
# Identification properties for this authentication component
tc.displayName=LDAP Team Connect Authenticator
tc.uniqueId=LDAP
tc.isSSO=false
# Custom page mappings (omit any that do not apply)
#page.badCredentials=tryagain.html
#page.lockedAccount=giveup.html
```

```
#page.maximumLogins=sorry.html
#page.logout=goodbye.html
#page.sessionTimeout=missedyou.html
# LDAP configuration properties
#
# The URL of the LDAP server to be used
ldap.host=10.1.2.48
ldap.port=389
ldap.root=dc=domain,dc=com
# DN of the user/administrator allowed to connect to the LDAP server
ldap.userDn=cn=Manager,dc=domain,dc=com
# Password of the user/administrator
ldap.password=secret
#
ldap.userDnPatterns=uid={0},ou=Department
#
ldap.groupDnPattern=ou=Department
#
ldap.groupRoleAttribute=cn
```

1.4.4 Custom Authentication Plug-ins

You can write your own authentication plug-in and integrate it with TeamConnect security. The details of the plug-in code are beyond the scope of this document, but here are the general principles:

Write your own Java class, implementing one of these two interfaces:

- CustomSSOAuthenticator
- CustomUserPwdAuthenticator

Write an **authenticationDescriptor.properties** file. The file needs to have at least the following lines (sample data shown in italics):

- tc.displayName=*My Authenticator*
- tc.uniqueId=*MYAUTH*
- tc.isSSO=*true*
- tc.authenticatorClassName=*com.mitratech.teamconnect.authentication.provider.TestMySSOAuthenticator*

It's a good idea to override some default error-message HTML files, too:

- page.badCredentials=*loginFailed.html*
- page.logout=*logout.html*
- page.sessionExpired=*timeout.html*

Put your new class in Document folder **System/Authentication/MYAUTH/classes** (the folder path must incorporate the value of tc.uniqueId). Put the properties file in there too.

As a sibling of folder **classes**, create folder **pages**. Put in HTML files to be used for overriding the default error-condition pages. This is especially important if you're writing an SSO authenticator.

1.4.4.1 Customizing Message Screens

If you enable an authentication plug-in mechanism in TeamConnect, you can customize the screens that you encounter while accessing and logging out of TeamConnect. You must write, test, and deploy your own Java class to display the customized screens. You should do this step only if you plan to provide extra information for users during their sessions.

Your custom Java class must implement interface **javax.servlet.Filter**. It should be deployed in the same Documents folder as the configuration files.

1.4.5 Enabling a Default Authentication Method

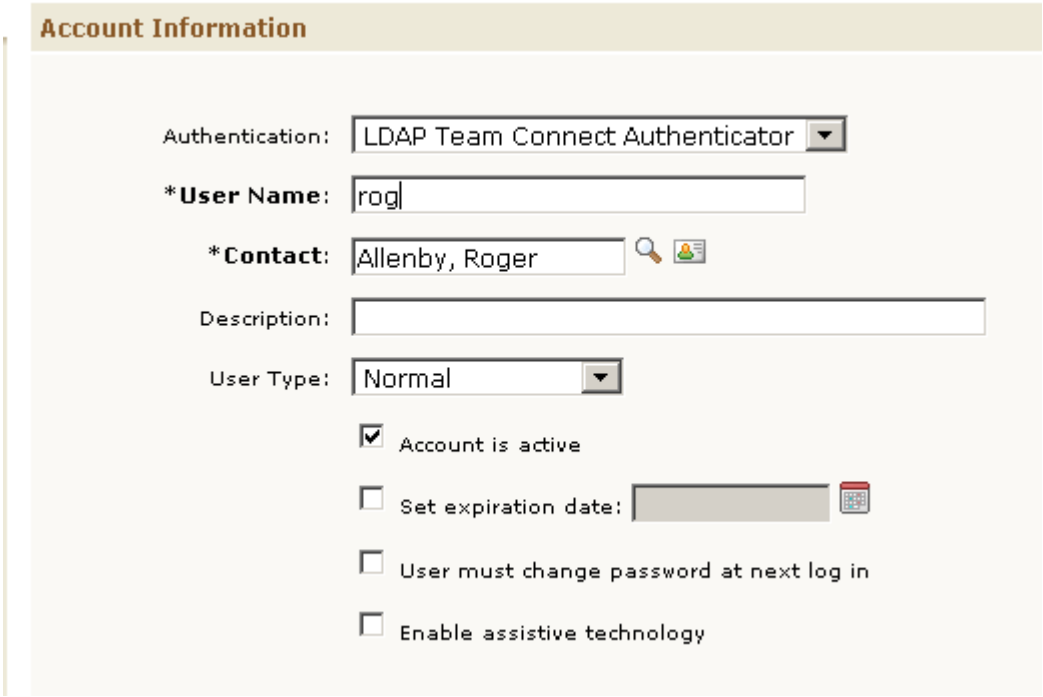
Enabling a Default Authentication Method

Choose a default method as described in Configuring User Authentication. The names used in the default authentication drop-down correspond to the value of **tc.displayName** in the **authenticationDescriptor.properties** file that is associated with each authentication method.

1.4.6 Overriding Authentication for Individual Users

Now that a default plug-in has been configured, you must override the authentication method for each user account that requires a non-default method. (Users whose authentication matches the default method do not require any overrides.) For details on settings on the user account screen, see Creating or Editing Users.

The example below presumes that your default authentication method is not LDAP, but some individual users do need to authenticate through LDAP. The steps described are similar no matter which method you are using to override.



Example: User Record - General Page

To configure an individual user account to use LDAP authentication

1. Click the **Admin** tab.
2. Click the **Users** link under the tab bar.
3. Open the desired user account.
4. From the **Authentication** drop-down list on the **General** page, select **LDAP** TeamConnect **Authenticator**.

   The screen refreshes and all fields regarding TeamConnect passwords are removed since a user who is authenticated through LDAP does not need a TeamConnect password.
5. Click **Save**.

   LDAP authentication configuration is completed.

The next time the user logs in to TeamConnect, even though the TeamConnect login screen is presented, he or she is actually authenticated through LDAP.

1.5 Troubleshooting and Frequently Asked Questions

This section provides additional frequently asked questions and troubleshooting information about users, groups, and the IMAP Server.

1.5.1 Frequently Asked Questions

This section includes additional information about application features, such as tips or helpful facts under the following topics.

- Users and Groups
- Address Books
- Budgets
- Admin Settings
- Licensed Seats

1.5.1.1 Users and Groups

Q: I created an object view and assigned it to a user group, but the members of this group don't see the new object view.

Make sure that you set the appropriate **Default Group** for the user. A user without a default group assigned uses the object views defined on the **Object Views** tab of the Designer application area **System Settings**.

If a default group is selected, the user uses the object views selected on the **Object Views** page of the group account. You can select the default group for a user on the **Group Memberships** page of the user account.

Q: What happens if I deactivate or delete user accounts?

When you deactivate a user account, the user's name is removed from the lists of Task and Project assignees, Appointment attendees, and Approval routes. However, it still appears on the **History** tab of records where they have entered History records, and other areas where that user is referenced as the **Created By**, **Modified By**, and so on.

If you delete a user account, all references to the user are removed from all records. In the records, the **Created By** and **Modified By** fields point to the TeamConnectAdmin user account instead.

Q: If I enable the User Lockout feature, will a user that gets locked out be deactivated in TeamConnect?

While a user is locked out of TeamConnect, only his or her ability to log in is disabled. The user account in TeamConnect remains active. This means that the user appears on all active lists, such as Appointment attendees, and can still be assigned to tasks or projects.

To unlock the user, clear the **Account is Locked** check box on the user account's **General** page. After doing this, the user is able to log into TeamConnect, and everything in his or her account is unaffected.

Q: Why don't I see the authentication plug-in that I uploaded to TeamConnect in the list of available plug-ins on the system settings screen?

After you upload a plug-in, in order for it to be visible from the **Plug-in** drop-down list for first time use, you must refresh the list. To do this, click **Load Plug-in**. Afterwards, the **Plug-in** drop-down list will contain the name of the plug-in that you uploaded.

Q: Why don't I see custom objects' embedded objects on the Security tab's Other Restrictions section of custom object definitions?

The additional record-level security restrictions of a custom object on its related objects does not include embedded objects.

Q: What is the difference between cascading record-level security in the Related Object Security block and the Other Restrictions block on the Security tab of custom object definitions?

In the **Related Object Security** block, you can set custom objects' record-level security to cascade to their related objects automatically. When read-only rights are cascaded from parent records to their related object records, users can still create related objects. For situations when parent projects have read-only access, due to security or workflow reasons, you can use the **Other Restrictions** block to deny users the ability to update, delete, or create related object records, even if they are the creators.

Q: Why can't I create a record? (User with Create record rights or Create all record rights)

You must assign both Create record rights and View record rights for a group member to be able to create records. For example:

- From global record rights for end-users, you must assign both **View all records** and **Create all records** to a group. Afterward, group members will be able to create all record types described in Rights for End-users.
- For a specific record type (for example, contacts), you must assign both **View Contact records** and **Create Contact records** rights.

Q: Why don't I see a new user in the New Users collection?

Users in the **New Users** collection are sorted alphabetically. If a collection contains many records you may not see the expected record near the top of the list. Users in the **Recently Viewed** collection are sorted with the topic record as the most recently viewed record.

Q: Why don't I see rights for the Involved object for a new custom object (project)?

After you create a custom object (project), you need to create a corresponding **Involved**. Afterward, from the **User Rights** list (of the group's **Record Rights** page), you can select the

custom object and assign rights for the related **Involved** records.

Q: Why was someone able to edit a user or group record while I was editing the record? Record locking was enabled.

Record locking only applies to system objects and custom objects for end users (see Rights for End-users). Record locking does not apply to user or group records.

Q: (TeamConnect®Enterprise Legal only) Why are some group members (users) unable to view the Legal tab?

If group members do not have rights to view any record types that belong under the **Legal** tab, then the Legal tab does not display. For example, Advice and Counsel, Cost Centers, Disputes, Time Entry Settings, and Transactions are record types that can display under the **Legal** tab so if a user belongs to groups that do not have rights to any of those record types, then the **Legal** tab does not display.

Q: I got a "Session Timeout" warning, tried to log back in, and got a "Recover Session" page?

The actual expiration of a session might be significantly later than the session timeout warning. That's because of the application server's handling of expired sessions. For example, in BEA WebLogic, the default setting for checking for expired sessions is every 60 seconds. So if a session timed out, it would actually still be valid until WebLogic cleaned up the expired session, which might be up to 60 seconds from the timeout message. If you tried to log in again during this period, the still-valid session would cause a Recover Session page to appear. In this WebLogic example, if you wanted to alter the application server's behavior, you could consult WebLogic documentation for information about changing the applicable setting (invalidation-interval-secs).

Q: I have a license for a number of concurrent users, but I can't use the entire number?

This situation is also caused by application servers, as described in the question above. If you had the maximum number of concurrent users logged in simultaneously, and one user's session timed out, another user wouldn't be able to log in until the application server cleaned up the expired session.

1.5.1.2 Address Books

Q: Where do I assign rights for Address Books?

Address Book access rights are bundled with contact records access rights. If you assign the right, **View Contact records**, to a group then group members will also be able to view address books, create address books, edit address books (name and public vs. private status), and delete address books. If you assign the right, **Edit Contact records**, to a group then group members will also be able to add and remove contacts from address books.

1.5.1.3 Budgets

Q: I can't see a Budget page from disputes or transactions. Why?

Based on settings in the Legal Preferences tool, users may or may not be able to adjust budgets from dispute and transaction records. From the Legal Preferences tool, if the **Extend budget level by field** is set to **Do not budget by fiscal period**, budgets will not display within dispute and transaction records.

1.5.1.4 Admin Settings

Q: From Admin Settings, I set the Read-only mode date format to mm/dd/yy but records display dates with the year in the format yyyy (4-digits). Why?

When records are in edit-mode, the year must display with 4 digits.

1.5.1.5 Licensed Seats

Q: How can I tell how many licensed user seats are remaining (unused)?

You cannot view this number directly, but you can check your license limits, then view your current active users to determine how many have been used. To check license limits, click the **Admin** tab. Click the **Admin Settings** link under the tab bar. Click the **About** link from the left pane. From the resulting page, the **License** section displays the details of the license key, including limits. To count active users, click the **Users** link beneath the **Admin** tab, and view the count of users in the **Active** collection.

1.5.2 Troubleshooting

IMAP

Issue: Troubleshooting the TeamConnect IMAP Server

Resolution: There are two ways to view IMAP Server events from a log.

You can view the system default log. See Viewing Logs.

You can also create an IMAP Appender.

License File

Issue: A "License file is missing" error message displays

Resolution: If you have not uploaded a license file for your application, an error message will display throughout the application ("License file is missing. Please check that it exists under Top Level

\System"). The license file should be uploaded to the **Documents** area \Top Level\System folder in TeamConnect.

Issue: A "User account cannot be created because the number of active user accounts has exceeded the limit specified in the license key" error message displays

Resolution: If you have reached the maximum number of users allowed in your current license file, this error displays when you attempt to create a new user. To add seats to the license file, contact Mitratech support. For more information, see How can I tell how many licensed user seats are remaining (unused)?.

Issue: A "User account cannot be updated because the number of active user accounts has exceeded the limit specified in the license key." error message displays

Resolution: If you have reached the maximum number of users allowed in your current license file, this error displays when you attempt to activate an inactive user. For more information, see How can I tell how many licensed user seats are remaining (unused)?.

Issue: A "License file is invalid. Please check that it is correctly formatted." error message displays

Resolution: If the license file you uploaded cannot be validated, this error message will display throughout the application. Contact Mitratech support for assistance.

WebDAV

Issue: When a user uploads files in batch loads using the WebDAV feature, the TeamConnect Documents displays all files as having the type, Data Mapping Files, instead of the actual file type (for example .DOC). The files that were uploaded in batch do not appear in full-text search results.

Resolution: You may need to update a TeamConnect configuration file with information about document extensions and MIME types that you expect to upload in batch.

Email Notifications

Issue: TeamConnect system email notifications include links to TeamConnect that do not work.

Resolution: Verify that you have set up the **Login URL** field in Admin Settings. For more information, see the topic Setting Up Email and description of the **Login URL** field.

Clustered Environment

Issue: In a clustered environment, data does not appear identically in each workstation session and/or the database server issues optimistic locking error messages.

Resolution: Cache synchronization between nodes in the cluster may not be working properly.

Searching

Issue: When performing a global search using "All as the qualifier, an error message appears.

Resolution: You may need to enable full-text search as follows:

1. On the SQLServer host, open **Services** and look for **SQL Full-text Filter Daemon Launcher (MSSQLSERVER)**.
2. Ensure that this service is running and is started by the same user who started the SQLServer (MSSQLSERVER) service.
3. Once the service is running, log-in to Microsoft SQL Server Management Studio as 'sa' user.
4. Open the master database and execute the following command:

```
sp_fulltext_service 'restart_all_fdhosts'
```

Localization Spreadsheet

Issue: I cut and pasted translated text into the Excel localization spreadsheet and now I cannot delete it or make any changes.

Resolution: If you plan to copy and paste translated data from third-party translation software, such as Google Translate, you may have difficulty deleting or making changes to the text that you paste into Excel.

To avoid this, after you copy your text and are in the Excel spreadsheet, go to the appropriate cell, right-click, select **Paste Special**, and then select **Text**. This removes any hidden characters and allows you to make changes to your pasted text if necessary.

1.6 Rights for End-users

This appendix provides reference tables with information on how to assign rights to groups of end users. These rights involve access to a given TeamConnect record type, along with the appropriate pages and features associated with this type. You may access these features using the **View** menu in the **Record Rights** list page.

You can only assign rights at the group level and not specifically to users. Any user who is a member of a given group inherits all the rights assigned to that group.

How To Use This Reference:

Each table contains the following information:

- Name of the right you may assign to a group
- Description of the operations this right allows a group to do
- Prerequisite rights a group needs in order to have this right (if applicable)
- TeamConnect pages that these rights enable a group to view

For information about rights that apply to administrator-type users, see Rights for Administrators.

For information about rights that apply to solution developer-type users, see Rights for Solution Developers.

Rights to System Records

You may assign rights to the following system record types, listed in the **View** menu, to do primary operations in TeamConnect:

- Account
- Appointment
- Contact
- Document
- Expense
- History
- Invoice
- Task

Rights to Custom Records

TeamConnect allows system designers to create custom records. For TeamConnect, custom records are referred to in this guide as Projects. For Matter Management, custom records are referred to in this guide as Matters. After a project or matter has been created, its name will appear in a group record's **Record Rights** page, **View** drop-down list.

TeamConnect Legal Records

A few custom record (matter) types are included with TeamConnect Legal.

- Advice and Counsel
- Cost Center
- Dispute
- Transaction

Note: *Record rights associated with Advice and Counsel, Cost Center, Dispute, Transaction records can be found in the Project/Matter Rights and Project/Matter Involved Rights.*

Rights to TeamConnect Areas or Features

Utility operations allow group members to do specific operations with TeamConnect record types. You may assign rights to do these operations, using the following options listed in the **View** menu:

- Preferences
- Record Locking

- Scheduled Actions
- Search Settings

1.6.1 System Record Rights

This section lists and explains the rights you can assign to system record types in TeamConnect. Some of these rights also apply to TeamConnect Projects (custom record types).

Note: *For more information on Projects, see Custom Record Rights.*

1.6.1.1 Account Rights

You must assign the appropriate rights for viewing and working with financial Account records, as explained in the following tables:

- The Basic Rights to Account table explains basic rights you can assign, allowing access to financial accounts, for example, **View Account records** and **Edit Account records**.
- The Additional Rights to Account table explains rights you can assign, allowing access to additional pages that are part of a financial account, for example, **View Account security** and **Create Account security**.

1.6.1.1.1 Basic Account Rights

One or more basic account rights is required to view or work with financial accounts.

Basic Rights to Account

Right	Description	Prerequisite Rights	Pages
View Account records	Allows groups to search for, print, and see existing Accounts.	None	Accounts list **Advanced Account Search** Account record > • **General** • **Posting Criteria** • **Workflow** • **Child Accounts**
Edit Account records	Allows groups to change existing Accounts.	**View Account records**	Same as for **View Account records**
Create Account	Allows groups to create and print new Accounts. These groups can	**View Account records**	Same as for **View Account records**

records	also create a copy of the current record. ***Note:*** *To select a parent Account or create child Accounts, groups must be able to view the appropriate Accounts.* To set any Account's posting criteria, groups must be able to view the appropriate: • Contacts • Projects and their categories • Expenses, Tasks, and their categories		
Delete Account records	Allows groups to delete existing Accounts.	**View Account records**	Same as for **View Account records**
Mass edit Account records	Allows groups to mass edit existing Accounts.	**View Account records** **Edit Account records**	**Mass Edit** page

1.6.1.1.2 Additional Account Rights

After you give groups one or more of the basic rights, additional rights and operations may become available to them, which were not accessible before. They also need to view pages where the operations are available. These Account rights enable a group to view the following additional TeamConnect pages:

- **Account** record > **Security**
- **Account** record > **Transactions**

The following table explains these additional group rights to Account:

Additional Rights to Account

Right	Description	Prerequisite Rights			Pages
		View Account Records	Edit Account Records	Additional	

View Account all categories	Allows groups to see existing Account categories and set one category as the default.	**X**		None	**Account** record > **Categories**
Add Account all categories	Allows groups to add categories to Accounts.			None	
Delete Account all categories	Allows groups to delete categories from Accounts.	**X**	**X**	**View Account all categories**	
View Account all custom fields	Allows groups to see all the custom fields of Accounts. ***Note:*** *To work with any custom field, groups must be able to view the field's category and its parents.* To see custom fields in a Project, groups must be able to view the Project.	**X**		**View Account all categories**	As customized by design
Edit Account all custom fields	Allows groups to change custom fields in Accounts.	**X**	**X**	**View Account all custom fields**	
View Account security	Allows groups to see security access information for Accounts.	**X**		None	**Account** record > **Security**
Edit Account security	Allows groups to change security settings for individual accounts. ***Note:*** *Before you can enable security editing for a group and its users, the group must be able to view the*	**X**	**X**	**View Account security**	

	appropriate Contacts.				
View Account all transactions	Allows groups to see the transactions already posted to any Account. ***Note:*** *To see transactions, groups must be able to view the appropriate Invoice Line Items, Expenses, and Tasks. Otherwise, these elements are displayed as "SECURED."*	**X**		None	**Account** record > **Transactions**
Create Account all transactions	Allows groups to create and post transactions to an Account.	**X**		None	

1.6.1.2 Appointment Rights

You must assign the appropriate rights for viewing and working with appointments, as explained in the following tables:

- The Basic Appointment Rights table explains basic rights you can assign to work with calendar Appointments, for example, **View Appointment records** and **Edit Appointment records**.
- The Additional Appointment Rights table explains rights you can assign to work with additional pages that are part of a calendar appointment, for example, **View Appointment security** and **Edit Appointment security**.

1.6.1.2.1 Basic Appointment Rights

One or more basic appointment rights is required to view or work with appointments.

The following table explains the basic rights to Appointment:

Basic Rights to Appointment

Right	Description	Prerequisite Rights	Pages

View Appointment records	Allows groups to search for, print, and see existing Appointments. ***Note:*** *To view Appointments associated with Projects, groups must be able to see the appropriate Projects.* Viewing rights also provide access to the Calendar view, which is one of the Appointment search views. To create Appointments with the Calendar view, groups need the **Create Appointment records** right to the appropriate Appointments.	None	Appointments list **Advanced Appointment Search** Appointment record > • **General** • **Attendees** • **Workflow**
Edit Appointment records	Allows groups to change existing Appointments.	**View Appointment records**	Same as for **View Appointment records**
Create Appointment records	Allows groups to create and print Appointments. These groups can also create a copy of the current record. ***Note:*** *To create appointments associated with Project records, groups must be able to view the appropriate Projects.*	**View Appointment records**	Same as for **View Appointment records**
Delete Appointment records	Allows groups to delete existing Appointments.	**View Appointment records**	Same as for **View Appointment records**
Mass edit Appointment records	Allows groups to mass edit existing Appointments.	**View Appointment records** **Edit Appointment records**	**Mass Edit** page

1.6.1.2.2 Additional Appointment Rights

There are additional appointment record pages that are available. Generally, access to these additional pages requires the assignment of the **View Appointment records** and/or **Edit Appointment records** rights.

- **Appointment** record > **Attendees**
- **Appointment** record > **Resources**
- **Appointments** list > **Scheduler**
- **Appointment** record > **Security**

The following table explains these rights to additional appointment pages:

Additional Rights to Appointment

Right	Description	Prerequisite Rights			Pages
		View Appointment records	Edit Appointment records	Additional	
Add Appointment attendees	Allows groups to add attendees to Appointments. ***Note:*** *To view and add attendees, groups must be able to view the appropriate Contacts.*	**X**	**X**	None	**Appointment** record > **Attendees**
Edit Appointment attendees	Allows groups to change an attendee's information.	**X**	**X**	None	
Delete Appointment attendees	Allows groups to remove attendees from Appointments.	**X**	**X**	None	
View Appointment all categories	Allows groups to see existing Appointment categories and set one of them as the default.	**X**		None	**Appointment** record > **Categories**
Create Appointment all categories	Allows groups to add categories to Appointments.	**X**	**X**	**View Appointment all**	

				categories	
Delete Appointment all categories	Allows groups to remove categories from Appointments.	**X**	**X**	**View Appointment all categories**	
View Appointment all custom fields	Allows groups to see custom fields of Appointments. ***Note:*** *To work with a custom field, groups must be able to view its associated category and the category's parents.* To see custom fields in Project, groups must have be able to view the appropriate Projects.	**X**		None	As customized by design
Edit Appointment all custom fields	Allows groups to change custom fields of Appointments.	**X**	**X**	**View Appointment all custom fields**	
View Appointment resources	Allows groups to see existing resources for Appointments.	**X**		None	**Appointment** record > **Resources**
Edit Appointment resources	Allows groups to change resource information.	**X**	**X**	**View Appointment resources**	
Create Appointment resources	Allows groups to add resources to Appointments.	**X**	**X**	**View Appointment resources**	

Delete Appointment resources	Allows groups to remove resources from Appointments.	**X**	**X**	**View Appointment resources**	
Scheduler Tool	Allows groups to create Appointments with the Scheduler Tool.	**X**	**X**	None	**Appointments** list > **Scheduler**
View Appointment security	Allows groups to see the security access for Appointments.	**X**		None	**Appointment** record > **Security**
Edit Appointment security	Allows groups to change the security for Appointments. ***Note:*** *To set security for groups and users, the group must be able to view the appropriate Contacts.*	**X**	**X**	**View Appointment security**	

1.6.1.3 Contact and Address Book Rights

You must assign the appropriate rights for viewing and working with contacts, as explained in the following tables:

- The Basic Rights for Contacts table explains basic rights you can assign to work with contacts, for example, **View Contact records** and **Edit Contact records**.
- The Additional Rights to Contacts table explains rights you can assign to work with additional pages that are part of a contact, for example, **View Contact security** and **Edit Contact security**.

1.6.1.3.1 Basic Contact and Address Book Rights

One or more basic contact rights is required to view or work with contacts and address books.

The following table explains the basic rights for working with contacts:

Basic Rights for Contacts

Right	Description	Prerequisite Rights	Pages
View Contact	Allows users to search for and view existing Contacts.	None	Contacts list page

records	Also allows users to view, edit (name and change public vs. private status), create, and delete address books.		**Advanced Contact Search** page
			Contact record >
			• **General** page >
			  ○ **Address** section
			  ○ **Phone** section
			  ○ **Fax** section
			  ○ **Email** section
			  ○ **Internet Address** section
			• **Workflow** page

Edit Contact records	Allows users to change existing Contacts. Also allows users to add or remove contacts from address books.	**View Contact records**	Same as for **View Contact records**
Create Contact records	Allows users to create new Contacts. To specify a company, users must also have the Read right to Contact. This right also determines whether users can add contacts in the Search Module window.	**View Contact records**	Same as for **View Contact records**
Delete Contact records	Allows users to delete existing Contacts.	**View Contact records**	Same as for **View Contact records**
Mass edit Contact records	Allows groups to mass edit existing Contacts.	**View Contact records** **Edit Contact records**	**Mass Edit** page

1.6.1.3.2 Additional Contact Rights

There are additional contact record pages that are available. Generally, access to these additional pages requires the assignment of the View Contact records and Edit Contact records rights.

- **Contact** record > **Categories**
- **Contact** record > **Rates**
- **Contact** record > **Relations**
- **Contact** record > **Security**
- **Contact** record > **Skills**
- **Contact** record > **Territories**

The following table explains these rights to additional contact pages:

Additional Rights to Contacts

Right	Description	Prerequisite Rights			Pages
		View Contact records	Edit Contact records	Additional	
View Contact all categories	Allows users to view existing contact categories and set one of them as default.	**x**			**Contact** record > **Categories**
Add Contact all categories	Allows users to add categories to contacts.	**x**	**x**	**View Contact all categories**	
Remove Contact all categories	Allows users to delete categories from contacts.	**x**	**x**	**View Contact all categories**	
View Contact all custom fields	Allows users to view custom fields of contacts. To work with custom fields, users must have at least the Read right to the associated category and its parents. To see custom fields of type Custom Object, users must	**x**			As customized by design

	have at least the Read right to the custom object.				
Edit Contact all custom fields	Allows users to change custom fields of contacts.	**x**	**x**	**View Contact all custom fields**	
View Contact involved	Allows users to view a contact's involvement in various custom objects. To view a contact's involvement, users must have at least the Read right to custom objects. To view a contact's involved roles, users must have at least the Read right to the Involved object and its categories.	**X**		None	**Contact** record > **Involved** page
View Contact rates	Allows users to view assigned contact rates. ***Note:*** *To see tasks for which rates are set, users must have at least the Read right to Task.*	**x**		**View Task Records**	**Contact** record > **Rates**
Edit Contact rates	Allows users to update existing rate information for contacts.	**x**	**x**	**View Contact rates**	
Create Contact rates	Allows users to add rates to contacts. ***Note:*** *To add rates, the users must have at least the Read right to Task.*	**x**	**x**	**View Contact rates** **View Task Records**	
Delete Contact	Allows users to delete rates from contacts.	**x**	**x**	**View Contac**	

rates				**t rates**	
View Contact relations	Allows users to view existing contact relations.	**x**			**Contact** record > **Relations**
Create Contact relations	Allows users to add relations to contacts.	**x**	**x**	**View Contact relations**	
Delete Contact relations	Allows users to delete relations from contacts.	**x**	**x**	**View Contact relations**	
View Contact security	Allows users to view security access for contacts.	**x**			**Contact** record > **Security** page
Edit Contact security	Allows users to change security for contacts.	**x**	**x**	**View Contact security**	
View Contact skills	Allows users to view existing contact skills.	**x**			**Contact** record > **Skills** page
Edit Contact skills	Allows users to update existing skill information for contacts.	**x**	**x**	**View Contact skills**	
Create Contact skills	Allows users to add skills to contacts.	**x**	**x**	**View Contact skills**	
Delete Contact skills	Allows users to delete skills from contacts.	**x**	**x**	**View Contact skills**	
View Contact	Allows users to view existing contact territories.	**x**			**Contact** record > **Territories** page

territories					
Create Contact territories	Allows users to add territories to contacts.	**x**	**x**	**View Contact territories**	
Delete Contact territories	Allows users to delete territories from contacts.	**x**	**x**	**View Contact territories**	

1.6.1.4 Document Rights

Documents in TeamConnect are unique record types. A document uploaded to TeamConnect is a record and can be accessed from the Documents tab. In addition, documents can be associated with other record types from a different record's Documents page. For example, if you assign rights to Create Contact records and Create Document records, then group members can upload documents from a contact's Documents page.

You must assign the appropriate rights to work with documents, as explained in the following tables:

- The Basic Rights to Document table explains basic rights you can assign to work with documents, for example, **View Document records** and **Edit Document records**.
- The Additional Rights to Document table explains rights you can assign to work with additional pages related to documents, for example, **View Document security** and **Edit Document security**.

1.6.1.4.1 Basic Document Rights

One or more basic document rights is required to view or work with documents.

Note: *Whereas other record types have multiple pages associated with each record, documents behave differently. From the Documents List page, when a document's Properties icon is clicked, a list of property pages associated with that document opens. Document property pages associated with basic document rights include General, and Workflow pages.*

The following table explains the basic rights to Document:

Basic Rights to Document

Right	Description	Prerequisite Rights	Pages
View Document records	Allows groups to search for, view, print, and share existing	None	Documents list

	Documents, as well as search for and view folders. ***Note:*** *For a group member to be able to access its own Document folder or other contact folders, the group member must be able to view the appropriate Contacts.*		**Advanced Document Search** Document Properties > • **General** • **Workflow**
Edit Document records	Allows groups to check out and check in Documents.	**View Document records**	Same as for **View Document records**
Create Document records	Allows groups to upload new Documents, as well as to create folders, links, and shortcuts to Documents. ***Note:*** *To specify the author of a Document, groups must be able to view the appropriate Contact.*	**View Document records**	Same as for **View Document records**
Delete Document records	Allows groups to delete existing Documents or move them to another location in the Documents area. ***Note:*** *To move Documents, a group must also have the Create Document records right.*	**View Document records**	Same as for **View Document records**
Mass edit Document records	Allows groups to mass edit existing Documents.	**View Document records** **Edit Document records**	**Mass Edit** page

1.6.1.4.2 Additional Document Rights

There are additional Document Property pages that are available. Generally, access to these additional pages requires the assignment of the **View Document records** and **Edit Document records** rights. These Document rights enable a group to view the following additional property pages, email folders, and email messages:

- **Document** Properties > **Categories**
- **Document** Properties > **Security**
- **Document** Properties > **Versions**
- **Email Folder**
- **Email** record

Note: *E-mail features and rights are only available with TeamConnect Projects. For more information on Projects, see Custom Record Rights. If the TeamConnect IMAP Server is set up and active, you must enable appropriate rights to groups to work with e-mail (treated as documents in TeamConnect).*

The following table explains these additional group rights to documents:

Additional Rights to Document

Right	Description	Prerequisite Rights			Pages
		View Document records	Edit Document records	Additional	
View Document all categories	Allows groups to view existing Document categories and set one of them as the default.	**X**		None	**Document** Properties > **Categories**
Create Document all categories	Allows groups to add categories to Documents.	**X**	**X**	**View Document all categories**	
Delete Document all categories	Allows groups to remove categories from Documents.	**X**	**X**	**View Document all categories**	
View Document all custom fields	Allows groups to view custom fields of Documents. ***Note:*** *To work with any custom field, groups must be able to view the*	**X**		None	As customized by design

	field's category and its parents. To see custom fields in a Project, groups must be able to view the Project.				
Edit Document all custom fields	Allows groups to change custom fields of Documents.	**X**	**X**	**View Document all custom fields**	
Generate New XML Based Document	Allows groups to create a new XML Document from an existing template. ***Note:*** *To generate a Document, a group needs to be able to view the appropriate Documents list. However, to save a generated Document, the group also needs the ability to create Documents in that list.*	**X**		None	
View Document security	Allows groups to view security access for Documents.	**X**		None	**Document** Properties > **Security**
Edit Document security	Allows groups to change security for Documents. ***Note:*** *Before you can enable security editing for a group and its users, the group must be able to view the appropriate Contacts.*	**X**	**X**	**View Document security**	

View Document versions	Allows groups to view the version history of Documents. ***Note:*** *To generate a version history of Documents, a group must enable the Version Control feature, using the system settings.*	**X**		None	**Document** Properties > **Versions**
Revert Document versions	Allows groups to remove the current most recent version of a Document and save the previous version as most recent.	**X**	**X**	**View Document versions**	
View email	Allows groups to search for and view email in TeamConnect.	**X**		**View Project records**	**Documents** list > **Email Folder**
Move email from non TeamConnect- IMAP folder to TeamConnect- IMAP folder	Allows groups to move e-mail messages from an email client's non TeamConnect-IMAP folder to a TeamConnect-IMAP folder.		**X**	**Create Document records** **View Project records** **Edit Project records**	**Documents** list > **Email Folder**
Move email between TeamConnect- IMAP folders	Allows groups to move email messages between an email client's TeamConnect-IMAP folders.	**X**	**X**	**Create Document records** **Delete Document**	**Documents** list > **Email Folder**

				records **View Project records** **Edit Project records**	
Delete email	Allows groups to delete IMAP email messages (for email clients and TeamConnect).	**X**		**Delete Document records** **View Project records** **Edit Project records**	**Email** record
Change email attributes (priority, read/ unread)	Allows groups to change email message attributes (for email clients).			**Create Document records** **View Project records** **Edit Project records**	**Email** record
Add TeamConnect- IMAP subfolder	Allows groups to create TeamConnect-IMAP subfolders (for email clients).			**Create Document records**	**Documents** list

				View Project records **Edit Project records**	
Rename / Delete TeamConnect- IMAP subfolder	Allows groups to delete TeamConnect-IMAP subfolders (for email clients and TeamConnect).	**X**	**X**	**Delete Document records** **View Project records** **Edit Project records**	**Documents** list
Add TeamConnect- IMAP subfolder	Allows groups to create TeamConnect-IMAP subfolders (for e-mail clients).			**Create Document records** **View Project records** **Edit Project records**	**Documents** list
Rename / Delete TeamConnect- IMAP subfolder	Allows groups to delete TeamConnect-IMAP subfolders (for e-mail clients and TeamConnect).	**X**	**X**	**Delete Document records** **View Project records**	**Documents** list

				Edit Project records	

`

1.6.1.5 Expense Rights

You must assign the appropriate rights for viewing and working with expense records, as explained in the following tables:

- The Basic Rights to Expense table explains basic rights to work with budget Expenses, for example, **View Expense records** and **Edit Expense records**.
- The Additional Rights to Expense table explains rights to work with additional pages that are part of an expense, for example, **View Expense security** and **Edit Expense security**.

1.6.1.5.1 Basic Expense Rights

One or more basic expense rights is required to view or work with expenses.

The following table explains the basic rights to expenses:

Basic Rights to Expense

Right	Description	Prerequisite Rights	Pages
View Expense records	Allows groups to search for and view existing Expenses.	None	Expenses list **Advanced Expense Search** Expense record > • **General** • **Transactions** • **Workflow**
Edit Expense records	Allows groups to change existing Expenses.	**View Expense records**	Same as for **View Expense records**
Create Expense records	Allows groups to create and print expenses. These groups can also create a copy of the current record. Also allows usage of the Expense Entry Tool. To be able to associate expenses with a specific Project and	**View Expense records**	Same as for **View Expense records**

	Contacts, groups must be able to view the Project and appropriate Contacts.		
Delete Expense records	Allows groups to delete existing Expenses.	**View Expense records**	Same as for **View Expense records**
Mass edit Expense records	Allows groups to mass edit existing Expenses.	**View Expense records** **Edit Expense records**	**Mass Edit** page

1.6.1.5.2 Additional Expense Rights

There are additional expense record pages that are available. Generally, access to these additional pages requires the assignment of the View Expense records and Edit Expense records rights. These Expense rights enable a group to view the following additional expense pages:

- **Expense** record > **Categories**
- **Expense** record > **Security**

The following table explains these additional group rights to expenses:

Additional Rights to Expense

Right	Description	Prerequisite Rights			Pages
		View Expense records	Edit Expense records	Additional	
Post	Allows groups to post Expenses to accounts. From any page of an open expense, a Post button becomes available unless the expense has posted.	**X**	**X**	None	
Void	Allows groups to void Expenses from accounts. From any page of an open expense, a Void button becomes available unless the expense has not posted.	**X**	**X**	None	

View Expense all categories	Allows groups to view existing Expense categories and set one of them as the default.	**X**		None	**Expense** record > **Categories**
Create Expense all categories	Allows groups to add categories to Expenses.	**X**	**X**	**View Expense all categories**	
Delete Expense all categories	Allows groups to remove categories from Expenses.	**X**	**X**	**View Expense all categories**	
View Expense all custom fields	Allows groups to view custom fields of Expenses. ***Note:*** *To work with any custom field, groups must be able to view the field's category and its parents.* To see custom fields in a Project, groups must be able to view the Project.	**X**		None	As customized by design
Edit Expense all custom fields	Allows groups to change custom fields of Expenses.	**X**	**X**	**View Expense all custom fields**	
View Expense security	Allows groups to view security access for Expenses.	**X**		None	**Expense** record > **Security**
Edit Expense security	Allows groups to change security for expenses. ***Note:*** *Before you can enable security editing for a group and its users, the group must be*	**X**	**X**	**View Expense security**	

	able to view the appropriate Contacts.				
Expense Entry Tool	Tool to add, post, and delete multiple expenses in batch.	**X**	**X**	**Create Expense records** **Post** (Expenses) **Delete Expense records**	**Expense Entry Tool**

1.6.1.6 History Rights

History records in TeamConnect are unique record types. A history in TeamConnect is a record and can be accessed from the All Services tab, History link. In addition, histories can be associated with other record types from a different record's History page. For example, if you assign rights to Create Contact records and Create History records, then group members can create a history from a contact's History page.

You must assign appropriate rights to enable viewing or working with History records, as explained in the following tables:

- The Basic Rights to History table explains basic rights you can assign to work with History records, for example, **View History records** and **Edit History records**.
- The Additional Rights to History table explains rights you can assign to work with additional pages that are part of a history record, for example, **View History security** and **Edit History security**.

1.6.1.6.1 Basic History Rights

One or more basic history rights is required to view or work with history records.

The following table explains the basic rights to history records:

Basic Rights to History

Right	Description	Prerequisite Rights	Pages
View History records	Allows groups to search for, print, and see existing History entries.	None	Histories list **Advanced History Search**

	Note: *Because History entries can be created only from within records, groups must be able to view the appropriate records. Also, it is possible for users to search and view history records that are associated with another record type the user does not have access rights for. For example, if a user does not have rights to expense records, they can still search and view history records associated with expenses.*		History record > • **General** • **Workflow**
Edit History records	Allows groups to change existing History entries.	**View History records**	Same as for **View History records**
Create History records	Allows groups to create and print new History entries. These groups can also create a copy of the current record. ***Note:*** *Because History entries can be created only from within records, groups must be able to view the appropriate records.*	**View History records**	Same as for **View History records**
Delete History records	Allows groups to remove existing History entries.	**View History records**	Same as for **View History records**
Mass edit History records	Allows groups to mass edit existing History entries.	**View History records** **Edit History records**	**Mass Edit** page

1.6.1.6.2 Additional History Rights

There are additional history record pages that are available. Generally, access to these additional pages requires the assignment of the View History records and Edit History records rights. These History rights enable a group to view the following additional expense pages:

- History record > Categories

- History record > Security

The following table explains these additional group rights to History:

Additional Rights to History

Right	Description	Prerequisite Rights			Pages
		View History records	Edit History records	Additional	
View History all categories	Allows groups to view the existing History categories and set one of them as the default.	**X**		None	**Histories** record > **Categories**
Create History all categories	Allows groups to add categories to History entries.	**X**	**X**	**View History all categories**	
Delete History all categories	Allows groups to delete categories from History entries.	**X**	**X**	**View History all categories**	
View History all custom fields	Allows groups to view custom fields of History entries. ***Note:*** *To work with a custom field, groups must be able to view its category and the category's parents.*	**X**		None	As customized by design
Edit History all custom fields	Allows groups to change custom fields of History entries.	**X**	**X**	**View History all custom fields**	
View History security	Allows groups to view security access for History entries.	**X**		None	**History** record > **Security**

Edit History security	Allows groups to change security for History entries. ***Note:*** *Before you can enable security editing for a group and its users, the group must be able to view the appropriate Contacts.*	**X**	**X**	**View History security**	

1.6.1.7 Invoice Rights

You must assign the appropriate rights to enable viewing and working with invoices, as explained in the following tables:

- The Basic Rights to Invoice table explains basic rights to work with invoices, for example, **View Invoice records** and **Edit Invoice records**.
- The Additional Rights to Invoice explains rights you can assign to work with additional pages that are part of a invoice, for example, **View Invoice security** and **Edit Invoice security**.

Invoice rights include rights to Invoice line items.

1.6.1.7.1 Basic Invoice Rights

One or more basic invoice rights is required to view or work with invoices.

The following table explains the basic rights to Invoice:

Basic Rights to Invoice

Right	Description	Prerequisite Rights	Pages
View Invoice records	Allows groups to search for, print, and view existing Invoices. ***Note:*** *To be able to view a specific vendor, groups must be able to view the appropriate Contacts.*	None	Invoices list **Advanced Invoice Search** Invoice record > • **General** • **Transactions** • **Workflow** • **Versions**
Edit Invoice records	Allows groups to change existing Invoices.	**View Invoice records**	Same as for **View Invoice records**

Create Invoice records	Allows groups to create and print new Invoices. These groups can also create a copy of the current record. ***Note:*** *To be able to select a specific vendor, groups must be able to view the Contact.*	**View Invoice records**	Same as for **View Invoice records**
Delete Invoice records	Allows groups to delete existing Invoices.	**View Invoice records**	Same as for **View Invoice records**
Mass edit Invoice records	Allows groups to mass edit existing Invoices.	**View Invoice records** **Edit Invoice records**	**Mass Edit** page

1.6.1.7.2 Additional Invoice Rights

After you give groups one or more of the basic rights, additional rights and operations may become available to them, which were not accessible before. They also need to view pages where the operations are available. These Invoice rights enable a group to view the following additional TeamConnect pages:

- **Invoices** record > **Categories** page
- **Invoice** record > **General** page > **Line Items** section
- **Invoice** record > **Security** page

The following table explains these additional rights to invoices:

Additional Rights to Invoice

Right	Description	Prerequisite Rights			Pages
		View Invoice records	Edit Invoice records	Additional	
Post	Allows groups to post Invoices to accounts. From any page of an open invoice, a Post button becomes available unless the invoice has posted.	**X**	**X**	None	

Void	Allows groups to void Invoices from accounts. From any page of an open invoice, a Void button becomes available unless the invoice has not posted.	**X**	**X**	None	
View Invoice all categories	Allows groups to view the existing Invoice categories and set one of them as the default.	**X**		None	**Invoices** record > **Categories**
Create Invoice all categories	Allows groups to add categories to Invoices.	**X**	**X**	**View Invoice all categories**	
Delete Invoice all categories	Allows groups to remove categories from Invoices.	**X**	**X**	**View Invoice all categories**	
View Invoice all custom fields	Allows groups to view custom fields of Invoices. ***Note:*** *To work with a custom field, groups must be able to view its category and the category's parents.* To see the custom fields in a Project, groups must be able to view the Project.	**X**		None	As customized by design
Edit Invoice all custom fields	Allows groups to change custom fields of Invoices.	**X**	**X**	**View Invoice all custom fields**	
View Line Item Records	Allows groups to view Invoice line items.	**X**		None	**Invoice** record > **General** page >

Edit Line Item Records	Allows groups to change Invoice line items. ***Note:*** *Because Invoice Line Items are associated with Projects, Task Categories, Expense Categories and Contacts, groups must be able to view these four items.*	**X**	**X**	**View Line Item Records**	**Line Items** section
Create Line Item Records	Allows groups to add line items to Invoices. ***Note:*** *Because Invoice Line Items are associated with Projects, Task Categories, Expense Categories and Contacts, groups must be able to view these four items.*	**X**	**X**	**View Line Item Records**	
Delete Line Item Records	Allows groups to remove line items from Invoices.	**X**	**X**	**View Line Item Records**	
View Line Item all categories	Allows groups to view the existing Invoice line item categories and set one of them as the default.	**X**		None	**Line Item** record > **Categories**
Create Line Item all categories	Allows groups to add categories to Invoice line items.	**X**	**X**	**View Line Item records** **View Line Item all categories**	

Delete Line Item all categories	Allows groups to remove categories from Invoice line items.	**X**	**X**	**View Line Item records** **View Line Item all categories**	
View Line Item all custom fields	Allows groups to view custom fields of Invoice line items. ***Note:*** *To work with a custom field, groups must be able to view its category and the category's parents.* To see the custom fields in a Project, groups must be able to view the Project.	**X**		None	As customized by design
Edit Line Item all custom fields	Allows groups to change custom fields of Invoice line items.	**X**	**X**	**View Line Item records** **View Line Item all categories** **View Line Item all custom fields**	
View Invoice security	Allows groups to view security access for Invoices.	**X**		None	**Invoice** record > **Security**

Edit Invoice security	Allows groups to change security for Invoices. ***Note:*** *Before you can enable security editing for individual invoices, the group must be able to view the appropriate Contacts.*	**X**	**X**	**View Invoice security**	

1.6.1.8 Report Rights

You must assign the appropriate rights to enable viewing and working with Reports, as explained in the following table:

Report Rights

Right	Description	Prerequisite Rights	Pages
View Report records	Allows groups to view Report lists, Report folders, view the results of Report execution, and view Report properties.	None	• Reports list • Reports Chart View • Reports Tabular View **Report** record > • **General** • **Data** • **Chart**
Edit Report records	Allows groups to save changes to a Report and Report folders.	**View Reports records**	Same as for **View Report records**
Create Report records	Allows groups to create a new Report or Report folder.	**View Reports records** **Edit Report records**	Same as for **View Report records**
Delete Report Records	Allows groups to delete Reports and Report folders.	**View Reports records** **Edit Report records**	Same as for **View Report records**

		Create Report records	
View Report security	Allows groups to view security access for Reports	**View Reports records**	**Reports** record > **Security** page
Edit Report security	Allows groups to change security for Reports.	**View Reports records**	**Reports** record > **Security** page

1.6.1.9 Task Rights

You must assign groups the appropriate rights to enable them to work with Task records, as explained in the following tables:

- The Basic Rights to Task table explains basic rights you may assign a group to allow its members to work with Tasks, for example, **View Task records** and **Edit Task records**.
- The Additional Rights to Task explains rights you must assign a group to allow its members to work with additional features that are part of a Task, for example, **View Task security** and **Edit Task security**.

1.6.1.9.1 Basic Task Rights

One or more basic task rights is required to view or work with tasks.

The following table explains the basic rights to Task:

Basic Rights to Task

Right	Description	Prerequisite Rights	Pages
View Task records	Allows groups to search for, print, and see existing Tasks. ***Note:*** *To view the projects and Contacts associated with tasks, groups must be able to see Contacts and Projects.*	None	Tasks list **Advanced Task Search** Task record > • **General** • **Transactions** • **Workflow**
Edit Task records	Allows groups to change existing Tasks.	**View Task records**	Same as for **View Task records**
Create Task records	Allows groups to create and print tasks. Also allows the usage of the Task Entry Tool.	**View Task records**	Same as for **View Task records**

	Note: *To be able to use the Task Entry tool, groups must be able to view and edit rights to the appropriate Task categories*. To be able to associate Tasks with specific Projects and Contacts, groups must be able to see Contacts and the appropriate Projects.		
Delete Task records	Allows groups to delete existing Tasks.	**View Task records**	Same as for **View Task records**
Mass edit Task records	Allows groups to mass edit existing Tasks.	**View Task records** **Edit Task records**	**Mass Edit** page

1.6.1.9.2 Additional Task Rights

After you give groups one or more of the basic rights, additional rights and operations may become available to them, which were not accessible before. They also need to view pages where the operations are available. These Task rights enable a group to view the following additional TeamConnect pages:

- **Task** record > **Assignees**
- **Task** record > **Security**

The following table explains these additional group rights to Task:

Additional Rights to Task

Right	Description	Prerequisite Rights			Pages
		View Task records	Edit Task records	Additional	
Post	Allows groups to post Tasks to accounts. From any page of an open task, a Post button becomes available unless the task has posted.	**X**	**X**	None	

Void	Allows groups to void Tasks from accounts. From any page of an open task, a Void button becomes available unless the task has not posted.	**X**	**X**	None	
View Task Assignees	Allows groups to view the list of past and current Task assignees. ***Note:*** *To view Task assignees, groups must be able to see Contacts.*	**X**		None	**Task** record > **General** page > **Assignment History** section
Assign Task	Allows groups to reassign Tasks to another group. ***Note:*** *To view Task assignees, groups must be able to see Contacts.*	**X**	**X**	**View Task Assignees**	
View Task all categories	Allows groups to view the current default Task category.	**X**		None	**Task** record > **Categories**
Create Task all categories	Allows groups to add categories to Tasks.	**X**	**X**	**View Task all categories**	
Delete Task all categories	Allows groups to delete categories from Tasks.	**X**	**X**	**View Task all categories**	
View Task all custom fields	Allows groups to see custom fields of Tasks. ***Note:*** *To work with a custom field, groups must be*	**X**		None	As customized by design

	able to view its category and the category's parents. To see the custom fields in a Project, groups must be able to view the Project.				
Edit Task all custom fields	Allows groups to change custom fields of Tasks.	**X**	**X**	**View Task all custom fields**	
View Task security	Allows groups to view security access for Tasks.	**X**		None	**Task** record > **Security** page
Edit Task security	Allows groups to change security for Tasks. ***Note:*** *Before you can enable security editing for a group and its users, the group must be able to view the appropriate Contacts.*	**X**	**X**	**View Task security**	
Task Entry Tool	Tool to add, post, and delete multiple tasks in batch.	**X**	**X**	**Create Task records** **Delete Task records** **Post** (Tasks)	Task Entry Tool

1.6.2 TeamConnect Features and Areas

This section explains rights related to TeamConnect features and areas, such as User Preferences.

1.6.2.1 Preferences Rights

You must assign the appropriate rights to view and edit User Preferences. Afterward, each group member can edit their individual preferences that apply to their personal TeamConnect experience.

The following table explains the rights to Preferences:

Rights to Preferences

Right	Description	Prerequisite Rights	Page
View Preferences	Allows groups to view their Preferences.	None	**Preferences**
Edit Preferences	Allows groups to change their Preferences.	**View Preferences**	

1.6.2.2 Release Edit Locks Right

This right only has an effect if the **Enable record locking in edit mode** Admin Setting is enabled. For more information about this system setting, see Setting Up General Settings.

The following table explains the right for releasing record locks:

Rights to Record Locking

Right	Description	Prerequisite Rights	Page
Release edit locks	Allows group members to release the lock on a record when it is open for editing by another user. A Release Lock button becomes available after this right is assigned and the conditions above are met. For more information, see Record Locking and releasing the lock and Setting Up General Settings.	None	N/A

1.6.2.3 Scheduled Actions Rights

You must assign the appropriate rights to view or delete Scheduled Actions. See Scheduled Actions Monitor for more information about Scheduled Actions.

The following table explains the rights to Scheduled Actions:

Scheduled Actions Rights

Right	Description	Prerequisite Rights	Page

View Scheduled Actions records	Allows groups to access the Scheduled Actions Monitor and view the pending actions listed.	None	**All** page > **Tools** page > **Scheduled Actions**
Delete Scheduled Actions records	Allows groups to delete scheduled actions in the Scheduled Actions Monitor so that they are not executed.	**View Scheduled Actions records**	

1.6.3 Custom Record Rights

Record types that solution developers can create and customize for your company are custom records. This section describes standard rights that would be assigned to a generic custom record, called a project (for TeamConnect) or matter (for TeamConnect Legal and TeamConnect® Express).

1.6.3.1 Project/Matter Rights

For TeamConnect, custom records are referred to in this guide as Projects. For TeamConnect Legal and TeamConnect® Express, custom records are referred to in this guide as Matters. In this guide, the terms project and matter can be considered as the same.

You must assign the appropriate rights to view or work with Projects/Matters, as explained in the following tables:

- The Basic Rights to Project/Matter table explains basic rights to work with a Project/Matter, for example, **View Project records** and **Edit Project records**.
- The Additional Project/Matter Rights explains rights you can assign to work with additional pages that are part of that Project, for example, **View Project security** and **Edit Project security**.

1.6.3.1.1 Basic Project/Matter Rights

One or more basic project rights is required to view or work with projects.

The following table explains the basic rights to a Project/Matter:

Basic Rights to Project/Matter

Right	Description	Prerequisite Rights	Pages
View Project records	Allows groups to search for, print, and view existing Project records.	None	**Projects** list **Advanced Project Search** Project record > • **General**

			• **Workflow**
Edit Project records	Allows groups to change existing Project records.	**View Project records**	Same as for **View Project records**
Create Project records	Allows groups to create new Project records. ***Note:*** *If the Project is centered around Contacts, groups must be able to view the appropriate Contacts.* If the Project requires a parent or is embedded in another Project, groups must be able to view the parent Project.	**View Project records**	Same as for **View Project records**
Delete Project records	Allows groups to delete existing Project records.	**View Project records**	Same as for **View Project records**
Mass edit Project records	Allows groups to mass edit existing Project records.	**View Project records** **Edit Project records**	**Mass Edit** page

1.6.3.1.2 Additional Project/Matter Rights

After you give groups one or more of the basic rights, additional rights and operations may become available to them, which were not accessible before. They also need to view pages where the operations are available. These Project/Matter rights enable a group to view the following additional TeamConnect pages:

- **Project/Matter** record > **Assignees**
- **Project/Matter** record > **Phases**
- **Project/Matter** record > **Involved**
- **Project/Matter** record > **Relations**
- **Project/Matter** record > **Security**

The following table explains these additional group rights to a Project/Matter:

Additional Project/Matter Rights

Right	Description	Prerequisite Rights	Pages

		View Project records	Edit Project records	Additional	
Create a copy	Allows groups to create a copy of the current Project. ***Note:*** *Giving this right causes the Create a copy button to appear on the Project record page.*	**X**	**X**	None	**Project** record
View Project Assignees	Allows groups to see existing Project assignees. ***Note:*** *To view assignees, groups must be able to see Contacts.*	**X**		None	**Project** record > **Assignees**
Edit Project Assignees	Allows groups to unassign or reassign Project assignees. ***Note:*** *To change assignees, groups must be able to see Contacts.*	**X**	**X**	**View Project Assignees**	
Create Project Assignees	Allows groups to add assignees to Projects. ***Note:*** *To add assignees, groups must be able to see Contacts.*	**X**	**X**	**View Project Assignees**	
Delete Project Assignees	Allows groups to remove assignees from Projects.	**X**	**X**	**View Project Assignees**	
View Project all categories	Allows groups to see the existing Project categories and set one of them as the default.	**X**		None	**Project** record > **Categories**

Create Project all categories	Allows groups to add categories to Project records.	**X**	**X**	**View Project all categories**	
Delete Project all categories	Allows groups to delete categories from Project records.	**X**	**X**	**View Project all categories**	
View Project all custom fields	Allows groups to view custom fields in Project records. ***Note:*** *To work with any custom field, groups must be able to view the field's category and its parents.* To see custom fields in a Project, groups must be able to view the Project.	**X**		None	As customized by design
Edit Project all custom fields	Allows groups to change custom fields in Project records.	**X**	**X**	**View Project all custom fields**	
Involved parties rights	For details about rights to Involved parties, see Project/ Matter Involved Rights. ***Note:*** *All of these rights appear in this segment of the menu.*				**Project** record
View Project phases	Allows groups to view Project phases.	**X**		None	**Project** record > **Phases**
Edit Project phases	Allows groups to change Project phases.	**X**	**X**	None	

View Project relations	Allows groups to view existing relationships between Projects.	**X**		None	**Project** record > **Relations**
Create Project relations	Allows groups to add relations between Projects.	**X**	**X**	**View Project relations**	
Delete Project relations	Allows groups to delete relations between Projects.	**X**	**X**	**View Project relations**	
View Project security	Allows groups to view security access for Project records.	**X**		None	**Project** record > **Security**
Edit Project security	Allows groups to change security for Project records. ***Note:*** *Before you can enable security editing for a group and its users, the group must be able to view the appropriate Contacts.*	**X**	**X**	**View Project security**	

1.6.3.2 Project/Matter Involved Rights

For TeamConnect, custom records are referred to in this guide as Projects. For TeamConnect Legal and TeamConnect® Express, custom records are referred to in this guide as Matters. In this guide, the terms project and matter can be considered as the same.

Involved Parties (Involved) are contacts associated with the Project/Matter, but not assigned to the Project/Matter. You must assign the appropriate rights to enable specific Involved-related operations, as explained in the following tables:

- The Basic Rights to Involved Contact table explains basic rights you may assign a group to allow its members to work with Involved Parties, for example, **View Project involved** and **Edit Project involved**.
- The Additional Involved Rights explains rights you must assign a group to allow its members to work with additional features that are part of an Involved Contact, for example, **View Project involved security** and **Edit Project involved security**.

See the *User Guide* for more information on projects and involved records.

Note: *After creating a custom object (project), you must create an associated Involved object. Afterward you can assign rights for that Involved object.*

1.6.3.2.1 Basic Involved Rights

One or more basic Involved rights is required to view or work with involved contacts.

The following table explains the basic rights to Involved:

Basic Rights to Involved Contact

Right	Description	Prerequisite Rights	Pages
View Project involved	Allows users to print and view existing Contacts who are Involved Parties in Projects. ***Note:*** *Before a group can view Involved Contact information, its members must be able to view the Involved Parties. The group must also be able to view and create the Involved Contact roles and categories before it can view Contact information.*	**View Project records**	**Project** record > **Involved** page Involved record > • **General** • **Relations** • **Workflow**
Edit Project involved	Allows users to change existing Involved Contact records.	**View Project records** **View Project involved**	Same as for **View Project involved**
Create Project involved	Allows users to create new Involved Parties. ***Note:*** *Before a group can create a new Involved Contact, its members must be able to view the Involved Parties. The group must also be able to view and create the Involved Contact roles and categories before it can view Contact information.*	**View Project records** **View Project involved**	Same as for **View Project involved**

Delete Project involved	Allows users to delete existing Involved Parties.	**View Project records** **View Project involved**	Same as for **View Project involved**

1.6.3.2.2 Additional Involved Rights

After you give groups one or more of the basic rights, additional rights and operations may become available to them, which were not accessible before. They also need to view pages where the operations are available. These Involved rights enable a group to view the following additional TeamConnect pages:

- **Involved** record > **Categories**
- **Involved** record > **Relations**
- **Involved** record > **Security**

The following table explains these additional group rights to Involved:

Additional Involved Rights

Right	Description	Prerequisite Rights			Pages
		View Project involved	**Edit Project involved**	**Additional**	
View Project involved all categories	Allows groups to view the existing Involved categories and set one of them as the default.	**X**	**X**	**View Project records**	**Involved** record > **Categories**
Create Project involved all categories	Allows groups to add categories to Involved Parties.	**X**	**X**	**View Project records** **View Project involved all categories**	
Delete Project involved all categories	Allows groups to delete categories from Involved Parties.	**X**	**X**	**View Project records** **View Project**	

				involved all categories	
View Project involved all custom fields	Allows groups to view custom fields of Involved Parties. ***Note:*** *To work with any custom field, groups must be able to view the field's category and its parents.* To see custom fields in a Project, groups must be able to view the Project.	**X**	**X**	**View Project records**	As customized by design
Edit Project involved all custom fields	Allows groups to change custom fields of Involved Parties.	**X**	**X**	**View Project records** **View Project involved all custom fields**	
View Project involved relations	Allows groups to view existing relationships between Involved Parties.	**X**	**X**	**View Project records**	**Involved** record > **Relations**
Create Project involved relations	Allows groups to create relationships between Involved Parties.	**X**	**X**	**View Project records** **View Project involved relations**	
Delete Project involved relations	Allows groups to delete relationships between Involved Parties.	**X**	**X**	**View Project records**	

				View Project involved relations	
View Project involved security	Allows groups to view security access for Involved Parties.	**X**	**X**	**View Project records**	**Involved** record > **Security**
Edit Project involved security	Allows groups to change security for Involved Parties. ***Note:*** *Before you can enable security editing for a group and its users, the group must be able to view the appropriate Contacts.*	**X**	**X**	**View Project records** **View Project involved security**	

1.6.3.3 Project/Matter Milestones Rights

For TeamConnect, custom records are referred to in this guide as Projects. For TeamConnect Legal and TeamConnect® Express, custom records are referred to in this guide as Matters. In this guide, the terms project and matter can be considered as the same.

Milestones are measurable activities within a project that help bring the project to conclusion. You must assign the appropriate rights to view or work with milestones, as explained in the following tables:

- The Basic Rights for Milestones table explains basic rights you may assign to a group to allow its members to work with Milestones, for example, **View Project Milestones** and **Edit Project Milestones**.
- The Additional Milestone Rights table explains rights you can assign to work with additional pages that are part of that Project, for example, **View Project security** and **Edit Project security**.

See the User Guide for more information on projects and milestones.

Note: *After creating a custom object (project), you must create an associated Involved object. Afterward you can assign rights for that Involved object.*

1.6.3.3.1 Basic Project/Matter Milestone Rights

One or more basic milestone rights is required to view or work with milestones.

The following table explains the basic rights to a milestone:

Basic Rights for Milestones

Right	Description	Prerequisite Rights	Pages
View Milestone records	Allows groups to search for, print, and view existing Milestone records.	None	**Project** record > **Milestones** page **Milestones** record > • **General** • **Security** • **Workflow**
Edit Milestone records	Allows groups to change existing Milestone records.	**View Project records** **View Project milestones**	Same as for **View Project milestones**
Create Milestone records	Allows groups to create new Milestone records.	**View Project records** **View Project milestones**	Same as for **View Project milestones**
Delete Milestone records	Allows groups to delete existing Milestone records	**View Project records** **View Project milestones**	Same as for **View Project milestones**

1.6.3.3.2 Additional Milestones Rights

After you give groups one or more of the basic rights, additional rights and operations may become available to them, which were not accessible before. They also need to view pages where the operations are available. These Milestones rights enable a group to view the following additional TeamConnect pages:

- **Milestones** record > **Categories**
- **Milestones** record > **Security**

The following table explains these additional group rights to a milestone:

Additional Milestone Rights

Right	Description	Prerequisite Rights	Pages

		View Project milestones	Edit Project milestones	Additional	
View Project milestones all categories	Allows groups to view the existing Milestones categories and set one of them as the default.	**X**	**X**	**View Project records**	**Milestones** record > **Categories**
Create Project milestones all categories	Allows groups to add categories to Milestones.	**X**	**X**	**View Project records** **View Project milestones all categories**	
Delete Project milestones all categories	Allows groups to delete categories from Milestones.	**X**	**X**	**View Project records** **View Project milestones all categories**	
View Project milestones custom fields	Allows groups to view custom fields of Milestones. ***Note:*** *To work with any custom field, groups must be able to view the field's category and its parents.* To see custom fields in a Project, groups must be able to view the Project.	**X**	**X**	**View Project records**	As customized by design
Edit Project milestone	Allows groups to change custom fields of milestones.	**X**	**X**	**View Project records**	

all custom fields				**View Project milestone all custom fields**	
View Project milestone security	Allows groups to view security access for Milestones.	**X**	**X**	**View Project records**	**Milestone** record > **Security**
Edit Project milestone security	Allows groups to change security for Milestones.	**X**	**X**	**View Project records** **View Project milestone security**	

1.7 Rights for Administrators

This appendix provides reference tables for assigning rights to TeamConnect record types and areas that should be accessed by administrator-type users. From a group record's **Record Rights** page, the rights described in this appendix are a subset of options from the **View** drop-down list.

Record types for administrators include:

- **Groups**—Group accounts in TeamConnect.
- **Users**—User accounts in TeamConnect.

TeamConnect areas for administrators include:

- **Admin Settings**—From the **Admin** tab, these are TeamConnect system settings that apply to all users.

1.7.1 Rights for Group Records

You must assign the appropriate rights for viewing and working with group records. This section contains the following tables that explain these rights and their associated operations:

- The Basic Rights for Group Records table explains basic rights you can assign, allowing access to group accounts, for example, **View Group records** and **Edit Group records**.
- The Additional Rights for Groups table explains rights you can assign, allowing access to additional pages that are part of a group account, for example, **View Group Users** and **Create Group Users**.

1.7.1.1 Basic Group Rights

One or more basic group rights is required to view or work with group records.

Basic Rights for Group Records

Right	Description	Prerequisite Rights	Page

View Group records	Allows searching, viewing, and printing existing group accounts.	None	• **Groups List** page
			• **Group Advanced Search** page
			• **Group** record
			  ○ **General** page
			  ○ **Object Views** page
			  ○ **Tool Rights** page

Edit Group records	Allows editing existing group accounts.	**View Group records**	See the **View Group records** right.

Create Group records	Allows creating group accounts.	None	• **Groups List** page
			• **Group** record
			  ○ **General** page
			  ○ **Object Views** page
			  ○ **Tool Rights** page

Delete Group records	Allows deleting existing group accounts.	**View Group records**	See the **View Group records** right.

1.7.1.2 Additional Group Rights

There are additional group record pages that are available. Generally, access to these additional pages requires the assignment of the View Group Records and/or Edit Group Records rights.

- **Group** record > **Users** page
- **Group** record > **Record Rights** page

- **Group** record > **Category Rights** page

The following table explains rights to additional group pages.

Additional Rights for Groups

Right	Description	Prerequisite Rights			Page
		View Group Records	Edit Group Records	Additional	
View Group Users	Allows users to view existing group members. ***Note:*** *To view existing group members, users must have the Read rights to user account.*	**x**			**Group** record > **Users** page
Create Group Users	Allows users to add members to groups. ***Note:*** *To view existing group members, users must have the Read rights to user account.*	**x**	**x**	**View Group Users**	
Delete Group Users	Allows users to delete members from groups.	**x**	**x**	**View Group Users**	
View Group Rights	Allows users to view existing group rights.	**x**			**Group** record: • **Record Rights** page • **Category Rights** page
Edit Group Rights	Allows users to set and change group rights.	**x**	**x**	**View Group Rights**	

1.7.2 Rights for User Records

You must assign the appropriate rights for viewing and working with user records. This section contains the following tables that explain these rights and their associated operations:

- The Basic Rights for User records table explains basic rights you can assign, allowing access to user accounts, for example, **View User records** and **Edit User records**.

- The Additional Rights for Users table explains rights you can assign, allowing access to additional pages that are part of a group account, for example, **View User Group Memberships** and **Create User Group Memberships**.

1.7.2.1 Basic User Rights

One or more basic user rights is required to view or work with user records.

Basic Rights for User records

Right	Description	Prerequisite Rights	Page

View User records	Allows searching, viewing, and printing existing user accounts.
	
	Note: *To be able to view a user account, users must at least have Read rights to the Contact object.*
		None	• **Users List** page
			• **User Advanced Search** page
			• **User** record >
			  ○ **General** page
			  ○ **Tool Rights** page

Edit User records	Allows editing existing user accounts.	**View User records**	See the **View User records** right.

Create User records	Allows creating and printing user accounts.
	
	Note: *To be able to create a user account, users must at least have Read rights to the Contact object.*
		None	• **Users List** page
			• **User** record >
			  ○ **General** page
			  ○ **Tool Rights** page

Delete User records	Allows deleting existing user accounts.	**View User records**	See the **View User records** right.

1.7.2.2 Additional User Rights

There are additional user record pages that are available. Generally, access to these additional pages requires the assignment of the basic **View User Records** and/or **Edit User Records** rights.

- **User** record > **Group Memberships** page
- **User** record > **Record Rights** page
- **User** record > **Category Rights** page

The following table explains rights to additional user pages.

Additional Rights for Users

Right	Description	Prerequisite Rights			Page
		View Group Records	Edit Group Records	Additional	
View Group Memberships	Allows viewing and printing the groups the user belongs to. ***Note:*** *To view groups, users must have the View Group records right.*	**x**			**User** record > **Group Memberships** page
Create Group Memberships	Allows adding the current user to groups. ***Note:*** *To view groups, users must have View Group records right.*	**x**	**x**	**View Group Memberships**	
Delete Group Memberships	Allows removing the current user from groups.	**x**	**x**	**View Group Memberships**	
View User Rights	Allows viewing the user's record rights and category rights.	**x**			**User** record > **Record Rights** page **Category Rights** page
Edit User Rights	Allows editing the user's record rights and category rights.	**x**	**x**	**View User Rights**	

1.7.3 Rights for Admin Settings and Logs

From the **Admin** tab, there are two areas that can be accessed, **Admin Settings** and **Logging**. You can assign rights to both areas from the Admin Settings-related rights.

You must assign the appropriate rights for viewing and working with Admin Settings and logs. This section contains the following table that explains rights you can assign, for example, **View Admin Settings** and **Edit Admin Settings**.

Rights for Admin Settings and Logs

Right	Description	Prerequisite Rights
View Admin Settings	Allows viewing Admin Settings. Also allows viewing system logs and audit logs, and clearing existing system logs.	None
Edit Admin Settings	Allows editing Admin Settings. Also allows editing default system logging levels.	**View Admin Settings**

1.8 Rights for Solution Developers

This appendix provides reference tables for assigning rights to TeamConnect areas that solution developers need to access. From a group record's **Record Rights** page, the rights described in this appendix are a subset of options from the **View** drop-down list.

TeamConnect areas or features for solution developers include:

- **Administer Custom Tools**—Page that allows management of custom tools.
- **Global Navigation**—Page that allows customization of the global navigation toolbar and subnavigation links (displayed under a toolbar tab).
- **Home Pages**—Page that allows management and customization of home pages or the initial page in TeamConnect after logging in.
- **Lookup Tables**—Page that allows management and customization of system lookup tables in TeamConnect.
- **Custom Lookup Tables**—Page that allows management and customization of custom lookup tables in TeamConnect.
- **Multi-currency Lookup Table**—Page that allows management and customization of the multi-currency lookup table in TeamConnect.
- **Miscellaneous Settings**—Page that allows management of custom fields that should be considered part of a user's system preferences. Custom fields added to the Designer application, **Miscellaneous Settings** page correspond to fields that display on a user's **Preferences** area, **Other Settings** page.
- **Object Definitions**—Area that allows management of system and custom object definitions (record types).
- **Portal Panes**—Area that allows management and customization of applets that are available for user home pages. Portal Panes can be information-driven, for example, containing TeamConnect search views or RSS feeds. In addition, Portal Panes can be functionality-driven, for example, containing links to frequently used areas, such as workflow approval or record creation wizards.
- **Routes**—Area that allows management and customization of the part of a workflow approval rule where approvers, reviewers, process managers, and email notifications are defined.
- **Route Stops**—Page that allows management of route stops (required approvers)

- **System Settings**—From the Designer application, these are TeamConnect system settings that apply to all users. These rights also allow access to manage system appenders and audit appenders.

See Access Rights to TeamConnect Designer for information about minimal required rights to work with the TeamConnect Designer area.

1.8.1 Administer Custom Tools Rights

There are multiple steps to managing custom tools in TeamConnect.

1. Solution Developers must do the following:
   a. Create custom tool source files and upload them to TeamConnect.
   b. Afterward, from the **Administer Custom Tools** page, the developer must add the custom tool to the TeamConnect list of available custom tools.
2. Administrators or developers must enable rights to the custom tool from the Tool Rights page of appropriate group records.
3. Afterward, users will be able to view and work with custom tools.

Rights described in this section refer to step 1b, above.

After you assign any of the Administer Custom Tools rights (**View Administer Custom Tools records**, **Edit Administer Custom Tools records**, **Create Administer Custom Tools records**, or **Delete Administer Custom Tools records**), the following page will be available:

- (from the **Tools** menu) **Administer Custom Tools** page

Administer Custom Tools Rights

Right	Description	Prerequisite Rights
View Administer Custom Tools records	Allows users to view the existing tools by the **Tools** drop-down on the **Admin** menu bar.	None
Edit Administer Custom Tools records	Allows users to change the information regarding existing tools.	**View Administer Custom Tools records**
Create Administer Custom Tools records	Allows users to add new (custom) tools.	**View Administer Custom Tools records**
Delete Administer Custom Tools records	Allows users to delete existing custom tools.	**View Administer Custom Tools records**

1.8.2 Global Navigation Toolbar Rights

The **Global Navigation** page allows solution developers to customize the Global Navigation toolbar (tabs, related links, and page content per tab) that displays when users log into TeamConnect. You must assign the appropriate rights for viewing and working with the **Global Navigation** page. This section contains a table that explains these rights and their associated operations

After you assign any of the Global Navigation rights (**View Global Navigation records**, **Edit Global Navigation records**, **Create Global Navigation records**, or **Delete Global Navigation records**), the following page will be available:

- (from the **Go To** menu) **Global Navigation** page

Rights to Customize the Global Navigation Toolbar

Right	Description	Prerequisite Rights
View Global Navigation records	Allows users to view the Global Navigation area.	
Edit Global Navigation records	Allows users to edit the tab names, tab display order, and subnavigation links that display on the global navigation toolbar.	**View Global Navigation records**
Create Global Navigation records	Allows users to create tabs and links that display on the global navigation toolbar.	**View Global Navigation records**
Delete Global Navigation records	Allows users to delete tabs and links that display on the global navigation toolbar.	**View Global Navigation records**

1.8.3 Customize Home Pages Rights

The **Home Pages** page allows solution developers to customize the high level content that displays on the initial page after users log into TeamConnect. You must assign the appropriate rights for viewing and working with the **Home Pages** page. This section contains a table that explains these rights and their associated operations

After you assign any of the Home Pages rights (**View Home Pages**, **Edit Home Pages**, **Create Home Pages**, or **Delete Home Pages**), the following page will be available:

- (from the **Go To** menu) **Home Pages** page

Rights to Customize Home Pages

Right	Description	Prerequisite Rights
View Home Pages	Allows users to search for and view existing Home Pages.	**View Portal Panes**

	Note: *Because Portal Panes are a major component of Home Pages, users must have at least the Read right to Portal Panes.*	
Edit Home Pages	Allows users to change existing Home Pages.	**View Home Pages**
Create Home Pages	Allows users to create new Home Pages. ***Note:*** *Because Portal Panes are a major component of Home Pages, users must have at least the Read right to Portal Panes.*	**View Portal Panes**
Delete Home Pages	Allows users to delete existing Home Pages.	**View Home Pages**

1.8.4 Lookup Tables Rights

Lookup Tables Rights refers to rights for solution developers to customize certain system lookup tables. The rights described below affect access to the Lookup Tables area > **System** tab. To a user, the result affects the list options that display from certain drop-down lists in the TeamConnect UI.

Rights for System Lookup Tables

Right	Description	Prerequisite Rights	Page
View System Tables	Allows users to view existing system lookup tables and lookup table items.	**x**	**System** tab
Edit System Tables	Allows users to change existing lookup table items.	**View System Tables**	
Create System Tables	Allows users to add new system lookup table items.	**View System Tables**	
Delete System Tables	Allows users to delete existing system lookup table items.	**View System Tables**	

1.8.5 Custom Lookup Tables Rights

Custom Lookup Tables Rights refers to rights for solution developers to create and manage custom lookup tables. The rights described below affect access to the Lookup Tables area > **Custom** tab. To a user, the result affects the list options that display from certain drop-down lists in the TeamConnect UI.

Rights for Custom Lookup Tables

Right	Description	Prerequisite Rights	Page
View Custom Lookup Table records	Allows users to view existing custom lookup tables and lookup table items.		**Custom** tab
Create Custom Lookup Table records	Allows users to create new custom lookup tables.	**View User Tables**	
Delete Custom Lookup Table records	Allows users to delete existing custom lookup tables.	**View User Tables**	
Create Custom Lookup Table Items	Allows users to add new custom lookup tables items.	**View User Tables**	
Delete Custom Lookup Table Items	Allows users to delete existing custom lookup tables items.	**View User Tables**	
Edit Custom Lookup Table Items	Allows users to change existing custom lookup tables items.	**View User Tables**	

1.8.6 Multi-currency Lookup Table Rights

Multi-currency Lookup Table Rights refers to rights for solution developers to manage the multi-currency lookup table. The rights described below affect access to the Lookup Tables area > Multi-currency tab. To a user, the result affects the list options that display from certain drop-down lists in the TeamConnect UI.

Rights for the Multi-currency Lookup Table

Right	Description	Prerequisite Rights	Page
View Multi-currency Table	Allows users to view the multi-currency lookup table and lookup table items.		**Multi-currency** tab
Create Multi-currency Table	Allows users to add new multi-currency lookup table items.	**View Multi-currency Table**	
Edit Multi-currency Table	Allows users to edit existing multi-currency lookup table items.	**View Multi-currency Table**	
Delete Multi-currency Table	Allows users to delete existing multi-currency lookup table items	**View Multi-currency Table**	

1.8.7 Miscellaneous Settings Rights

The **Miscellaneous Settings** page from the Designer application allows solution developers to manage custom fields that affect individual users' Preferences. After making changes to the **Miscellaneous Settings** page, those custom fields should be available from a user's **Preferences** area. You must assign the appropriate rights for viewing and working with the **Miscellaneous Settings** page. This section contains a table that explains these rights and their associated operations. In addition, rights to release edit locks and bypass search limits are located on the **Miscellaneous Settings** page.

After you assign any of the Miscellaneous Settings rights (**View Miscellaneous Settings**, **Edit Miscellaneous Settings**, **Create Miscellaneous Settings**, or **Delete Miscellaneous Settings**), the following page will be available:

- (from the **Tools** menu) **Misc. Settings**

Rights for Miscellaneous Settings

Right	Description	Prerequisite Rights	Page
Release edit locks	Allows group members to release the lock on a record when it is open for editing by another user. A Release Lock button becomes available after this right is assigned and the conditions above are met. See addition information about Record Locking and releasing the lock and Setting Up General Settings.	None ***Note:*** *This right only has an effect if the* ***Enable***	

		record locking in edit mode *Admin Setting is enabled. For more information about this system setting, see Setting Up General Settings.*	
Bypass search limits	Allows groups to bypass the Admin Settings for the Maximum Search results and **Maximum Search time (seconds)**. ***Note:*** *If a search exceeds the limits, the group's users can click a **Return All Results** link to bypass the limit. TeamConnect then returns all records the group has access rights to, which may take more time.* If a user does NOT have bypass rights and their search exceeds the maximum number of records or seconds, TeamConnect displays the records that were retrieved before the limit or time out was reached.	None	
View Miscellaneous Settings	From the Designer application, allows access to the **Tools** drop-down list, **Misc. Settings** option. Also allows users to view existing custom fields that have been added to the **Misc. Settings** page.	**x**	**Miscellaneous Settings**
Edit Miscellaneous Settings	Allows users to change existing custom fields from the **Misc. Settings** page.	**View Miscellaneous Settings**	

Create Miscellaneous Settings	Allows users to create new custom fields to be used for **Misc. Settings** page.	**View Miscellaneous Settings**	
Delete Miscellaneous Settings	Allows users to delete existing custom fields from **Misc. Settings** page.	**View Miscellaneous Settings**	

1.8.8 Object Definitions Rights

The **Object Definitions** area from the Designer application allows solution developers to manage system and custom objects. After making changes to the **Object Definitions** area, those objects should have corresponding rights from a group's **Record Rights** page, **View** drop-down list. You must assign the appropriate rights for viewing and working with the **Object Definitions** area. This section contains a table that explains these rights and their associated operations.

After you assign any of the basic Object Definitions rights (**View Home Pages**, **Edit Home Pages**, **Create Home Pages**, or **Delete Home Pages**), the following pages will be available:

- (from the **Go To** menu) **Object Definitions** list
- Object Definition record for each of the following system objects:
  - **Account**
  - **Appointment**
  - **Contact**
  - **Document**
  - **Expense**
  - **Group**
  - **History**
  - **Invoice**
  - **Task**
  - **User**
- Object Definition record for any custom objects

Within each system object's Object Definition view, the following system blocks are represented by tabs:

- **Custom Fields**
- **Forms**
- **Object Views**
- **(Custom) Blocks**

- **Rules**
- **Templates**
- **Wizards**

There are corresponding rights to work with the system blocks (tabs), for example, **View Object Definition Custom Fields**. If you deny rights to a system block, a user will not be able to perform operations on the corresponding tab, but all system block tabs will still display. For details, see Rights for System Record Types, Rights for Custom Record Types, and Requirements for Basic Record Rights, Requirements for Additional Rights to Records.

Object Definition Rights

Right	Description	Prerequisite Rights			Page
		View Object Definitions	Edit Object Definitions	Additional	
View Object Definitions	Allows users to access and view existing object definitions.				• **Object Definitions List** page • **Object Definition** for: ○ **Account** ○ **Appointment** ○ **Contact** ○ **Contact Group** ○ **Document** ○ **Expense** ○ **History** ○ **Invoice** ○ **Task**
Edit Object Definitions	Allows users to change existing object definitions.	**x**			
Create Object Definitions	Allows users to create new custom object definitions and set the auto numbering, auto naming, add phases and add phase transitions.				
Delete Object Definitions	Allows users to delete existing custom object definitions.	**x**	**x**		
View Object Definition	Allows users to view existing user rights.	**x**			**Custom Fields** tab

Custom Fields					
Edit Object Definition Custom Fields	Allows users to change existing custom fields.	**x**	**x**	**View Object Definition Custom Fields**	
Create Object Definition Custom Rights	Allows users to set and change user rights.	**x**	**x**	**View Object Definition Custom Fields**	
Delete Object Definition Custom Fields	Allows users to delete existing custom fields.	**x**	**x**	**View Object Definition Custom Fields**	
View Object Definition Forms	Allows users to view existing forms.				**Forms** tab
Edit Object Definition Forms	Allows users to change existing forms.	**x**	**x**	**View Object Definition Forms**	
View Object Definition Object Views	Allows users to access and view existing object views.	**x**			**Object Views** tab
Edit Object Definition Object Views	Allows users to change existing object views.	**x**	**x**	**View Object Definition Object Views**	

Create Object Definition Object Views	Allows users to create new customized object views. ***Note:*** *To add custom blocks to the new object view, users must at least have Read rights to blocks.*	**x**	**x**	**View Object Definition Object Views**	
Delete Object Definition Object Views	Allows users to delete existing object views.	**x**	**x**	**View Object Definition Object Views**	
View Object Definition (Custom) Blocks	Allows users to view existing custom blocks.	**x**			**Blocks** tab
Edit Object Definition (Custom) Blocks	Allows users to change existing custom blocks.	**x**	**x**	**View Object Definition (Custom) Blocks**	
Create Object Definition (Custom) Blocks	Allows users to add new custom blocks.	**x**	**x**	**View Object Definition (Custom) Blocks**	
Delete Object Definition (Custom) Blocks	Allows users to delete existing custom blocks.	**x**	**x**	**View Object Definition (Custom) Blocks**	

View Object Definition Rules	Allows users to view existing rules	**x**			**Rule** screen > **General** tab **Action** tab
Edit Object Definition Rules	Allow users to change rules	**x**	**x**	**View Object Definition Rules**	
Create Object Definition Rules	Allow users to create new rules. To create valid rules with qualifiers, users must save the general rule data and then set the qualifiers. So, users must have Update rights to rules and the Read and Update rights to qualifiers. To set actions for approval rules, users must have the Read right to the route.	**x**	**x**	**View Object Definition Rules**	
Delete Object Definition Rules	Allow users to delete rules	**x**	**x**	**View Object Definition Rules**	
View Object Definition Rule Qualifiers	Allow users to view rule qualifiers			**View Object Definition Rules**	**Rule** screen > **Qualifier** tab
Edit Object Definition Rule Qualifiers	Allow users to change rule qualifiers			**View Object Definition Rules** **Edit Object Definition Rules**	

				View Object Definition Rule Qualifiers	
Create Object Definition Rule Qualifiers	Allow users to add rule qualifiers.			**View Object Definition Rules** **Edit Object Definition Rules** **View Object Definition Rule Qualifiers**	
Delete Object Definition Rule Qualifiers	Allow users to delete rule qualifiers			**View Object Definition Rules** **Edit Object Definition Rules** **View Object Definition Rule Qualifiers**	
View Object	Allow users to view existing conditions	**x**			**Conditions** tab

Definition Conditions					
Edit Object Definition Conditions	Allow users to change conditions	**x**	**x**	**View Object Definition conditions**	
Create Object Definition Conditions	Allows users to create new conditions	**x**	**x**	**View Object Definition conditions**	
Delete Object Definition Conditions	Allow users to delete existing conditions	**x**	**x**	**View Object Definition conditions**	
View Object Definition Search Views	Allow users to view search views.	**x**			**Search Views** tab
Edit Object Definition Search Views	Allow users to change existing search views ***Note:*** *With this right, users can add, change, and delete search qualifiers and display columns.*	**x**	**x**	**View Object Definition Search Views**	
Create Object Definition Search Views	Allow users to create new search views including qualifiers and display columns.	**x**	**x**	**View Object Definition Search Views**	

Delete Object Definition Search Views	Allow users to delete search views	**x**	**x**	**View Object Definition Search Views**	
View Object Definition Templates	Allow users to view Templates	**x**			**Templates** tab
Create Object Definition Templates	Allow users to create new Templates	**x**	**x**	**View Object Definition Templates**	
Edit Object Definition Templates	Allow users to change Templates	**x**	**x**	**View Object Definition Templates**	
Delete Object Definition Templates	Allow users to delete Templates	**x**	**x**	**View Object Definition Templates**	
View Object Definition Wizards	Allow users to view existing wizards	**x**			**Wizards** tab
Edit Object Definition Wizards	Allow users to change wizards	**x**	**x**	**View Object Definition Wizards**	
Create Object	Allows users to create new wizards.	**x**	**x**	**View Object Definiti**	

Definition Wizards	***Note:*** *To associate templates with wizards, users must at least have Read rights to Templates.*			**on Wizards**	
Delete Object Definition Wizards	Allow users to delete existing wizards	**x**	**x**	**View Object Definition Wizards**	

1.8.9 Customize Portal Panes Rights

The Portal Panes area allows solution developers to customize the content within individual panes (portal panes) that display on the initial page (home page) that opens after users log into TeamConnect. You must assign the appropriate rights for viewing and working with the Portal Panes area. This section contains a table that explains these rights and their associated operations

After you assign any of the Portal Pane rights (View Portal Panes, Edit Portal Panes, Create Portal Panes, or Delete Portal Panes), the following page will be available:

- (from the Go To menu) Portal Panes page

Rights to Customize Portal Panes

Right	Description	Prerequisite Rights
View Portal Panes	Allows users to search for and view existing Portal Panes.	
Edit Portal Panes	Allows users to change existing Portal Panes.	**View Portal Pane**
Create Portal Panes	Allows users to create new Portal Panes.	
Delete Portal Panes	Allows users to delete existing Portal Panes.	**View Portal Pane**

1.8.10 Routes Rights

The **Routes** area allows solution developers to manage routes (approvers, reviewers, process managers, and email notifications associated with workflow approvals). You must assign the appropriate rights for viewing and working with the **Routes** area. This section contains a table that explains these rights and their associated operations.

After you assign any of the basic Routes rights (**View Routes**, **Edit Routes**, **Create Routes**, or **Delete Routes**), the following pages will be available:

- (from the **Go To** menu) **Routes** List page
- Existing routes

  For each route, the following tabs are available: **General**, **Stops**, and **Email Notifications**.

Before users/groups can view or work with the **Stops** tab, you must assign one of the corresponding rights (**View Route Stops**, **Edit Route Stops**, **Create Route Stops**, or **Delete Route Stops**); otherwise the tab will not display content. From the Routes area, the **Stop** tab defines required check points during an approval process.

Routes Rights

Right	Description	Prerequisite Rights			Page
		View Routes	Edit Routes	Additional	
View Routes	Allow users to view routes				• **Route** > **General** tab • **Route** > **Email Notification** tab ***Note:*** *The **Stop** tab is available but doesn't display content or allow stop management until Route Stop rights are assigned.*
Edit Routes	Allow users to change routes	**x**			
Create Routes	Allow users to create new routes. ***Note:*** *To create routes with stops, users must first save the general route information and then create the desired stops. Thus, users must have the Update right to Routes and the Read and Update rights to Stops.*				
Delete Routes	Allow users to delete routes	**x**			
View Route Stops	Allow users to view existing stops.	**x**			**Route** > **Stop** tab

Edit Route Stops	Allow users to add new stops to routes.	**x**	**x**	**View Route Stops**	
Create Route Stops	Allow users to change stops of routes.	**x**	**x**	**View Route Stops**	
Delete Route Stops	Allow users to delete stops from routes.	**x**	**x**	**View Route Stops**	

1.8.11 System Settings and Appenders Rights

From the Designer application, **System Settings** drop-down list, there are two areas that can be accessed, **System Settings** and **Appenders**. You can assign rights to both areas from the System Settings rights.

You must assign the appropriate rights for viewing and working with System Settings and appenders. This section contains the following table that explain these rights and their associated operations:

- The Rights for System Settings and Appenders table explains rights you can assign, for example, **View System Settings** and **Edit System Settings**.

After you assign any of the System Settings rights (**View System Settings** or **Edit System Settings**), the following pages will be available:

- From the Designer application, System Settings area:
  - **Rule Execution** page
  - **Custom Messages** page
  - **Clear Cache: 2.x UI Settings** page
  - **Default Object Views** (system-level) page
  - **Authentication Plug-In** page
  - **Backward Compatibility Settings** page
  - **History**
- From the Designer application, Appenders area:
  - **System Appenders** page
  - **Audit Appenders** page

Rights for System Settings and Appenders

Right	Description	Prerequisite Rights

View System Settings	Allows users to access and view the system settings.	None
Edit System Settings	Allows users to change the system settings.	**View System Settings**

1.9 Documents and Folders

The TeamConnect Documents area contains files that are related to your customized system design and documents that users attach to records. This appendix provides a reference to the default directory structure.

1.9.1 Directory Structure

The following directory structure of the **Documents** area includes not only files for TeamConnect records, but also all files that control the customized design of your application. <*CustomObjects*> and <*UserNames*> are placeholders for your system's custom objects and user names.

Note: *Depending on the specific TeamConnect product that you are using, your username may be denied access to folders* ***System****,* ***Users****,* ***Attachments****, object definition folders, and subfolders* ***Rules*** *and* ***Screens*** *beneath each object definition folder.*

```
Top Level
  |
  |-- /Attachments
  |       |-- /Accounts
  |       |-- /Appointments
  |       |-- /Contacts
  |       |-- /Expenses
  |       |-- /Histories
  |       |-- /Invoices
  |       |-- /Line Items
  |       |-- /Tasks
  |       |-- /<CustomObjects> ...
  |
  |-- /System
  |       |-- /Custom Rules
  |       |-- /HTTPRoot
  |       |-- /Icons
  |       |-- /Legacy Rules
  |       |-- /Libraries
  |       |-- /Logging
  |       |-- /Object Definitions
  |       |         |-- /Accounts
```

```
|       |         |-- /Appointment
|       |         |-- /Contact
|       |         |-- /Document
|       |         |-- /Expense
|       |         |-- /History
|       |         |-- /Invoice
|       |         |-- /Involved
|       |         |-- /Line Item
|       |         |-- /Task
|       |         |-- /<CustomObjects> ...
|       |-- /Portal
|       |-- /Screens
|       |-- /StartUp
|       |-- /Tools
|
|-- /Users
|       |-- /<UserNames> ...
```

Caution: *To avoid causing problems with your system, do not alter the system folders. The only folders that you should delete, move, or rename are subfolders that you created or the folders of custom object definitions.*

This section describes the directory structure so that you can properly manage the files and folders related to records and to your system design. It includes the following topics:

- Top Level Folder
  - Attachments Folder
  - HTTPRoot Folder
  - System Folder
  - Users Folder
- Automatically Created Folders

For specific details about using the **Documents** area pages, see the *User Guide*.

1.9.1.1 Top Level Folder

At the top level of the TeamConnect document directory structure, there is a folder called **Top Level**. The **Top Level** folder contains the following folders:

Subfolders under the Documents Top Level Folder

Folder	Description
Attachments	Contains folders that store attached documents for each record in TeamConnect. Attachments to a specific record can also be accessed through the **Documents** page of the record.

	Note: *These folders are automatically created when a user accesses the* ***Documents*** *tab of a record for the first time. The folder is created whether or not a user uploads a document to the corresponding record.* For more details about the **Attachments** folder, see Attachments Folder.
HTTPRoot	May contain scripts, custom style sheets, or images to be referenced by custom blocks via HTTP. You can create subfolders under this folder to better organize your items. For more details about the **HTTPRoot** folder, see HTTPRoot Folder.
System	Contains several folders that store all of the design information for your application including blocks (sections), Document Generator templates, class files for rules, and so on. For more details about these folders, see System Folder.
Users	Contains a folder for each TeamConnect user where personal files may be stored. When a user clicks the **Documents** tab, the user's individual Documents folder is automatically displayed. For more details, see Users Folder.

1.9.1.1.1 Attachments Folder

The **Top Level/Attachments** folder contains automatically-created folders for all system and custom objects in TeamConnect (except for embedded objects, because their records cannot have attached documents).

Each object's folder contains subfolders for every record created for that specific object. The subfolders are named after the records whose attachments they contain, according to these patterns:

- Folders for system object records, such as Accounts, Contacts, and Expenses, are named using the name of the record and its primary key. For example: David_Hendrikson(44).
- Folders for custom object records, such as claims, litigations, and so on, are named using the Unique ID of the record, according to the Unique ID settings in the object definition. For example, if claims are set to auto-numbering, then the folder is named using the number of the claim record.

You can use the **Attachments** folder to navigate to the specific attachments of a record; however, you may find it easier to open the record and click its **Documents** tab.

1.9.1.1.2 HTTPRoot Folder

The **Top Level/HTTPRoot** folder stores scripts, style sheets, and image files that a custom block or block template can reference through HTTP. You can also create subfolders under this folder to organize your files better.

1.9.1.1.3 System Folder

By default, the Top Level/System folder contains the following folders:

- Authentication (requires manual creation)
- Custom Rules
- Icons
- Legacy Rules
- Libraries
- Logging
- Object Definitions
- Portal
- Screens
- StartUp
- Tools

Authentication

If you use an authentication plug-in with TeamConnect, you must manually create the **Top Level/System/Authentication** folder.

Afterward, for each authentication plug-in you plan to use, you must manually create the following sub-folders:

Top Level/System/Authentication/<*Plug-in_Name*>

Top Level/System/Authentication/<*Plug-in_Name*>/classes

Top Level/System/Authentication/<*Plug-in_Name*>/pages

The folder specified by <*Plug-in_Name*> should be the unique four-letter code specified in the plug-in's class file. Upload the authentication plug-in file to the corresponding authentication plug-in subfolder (for example, **Top Level/System/Authentication/NTLM**).

Use an authentication plug-in's subfolders as follows:

- **classes**—Stores necessary Java class files
- **pages**—Stores necessary XML files

For more information about installing plug-ins and a full description of the **Authentication** folder's contents, see the specific document for your authentication mechanism, which is provided by Mitratech.

Important: *Make sure to replace the folder name examples, AuthMechanism1 or AuthMechanism2, with the unique four letter code specified by the plug-in class file used in your environment.*

Custom Rules

The **Top Level/System/Custom Rules** folder is a common folder used for storing Java files that are shared by multiple object definitions. Files in this folder can be referenced by:

- Custom action rules
- Scheduled action rules
- Wizard page actions
- Wizard page transition rules

For example, if three different custom objects require the same Java files for their custom action rules, then you can use this folder to upload the necessary Java files for all three custom objects.

Files in the **Custom Rules** folder do not become available on the **Qualifiers** or **Action** tab of rules. The **Custom Rules** folder can store only supporting files that may be referenced by custom qualifiers or actions for specific object definitions.

Icons

The **Top Level/System/Icons** folder contains images used by various objects in TeamConnect. You can upload images to this folder to be used as icons that appear in the corner of object records and in the button for the record on the TeamConnect task bar.

The images in this folder that are in web-friendly formats (JPG, GIF, and so on) are listed in the **Icon Image File** drop-down list on the **General** page of all object definitions.

If no image files are stored in this folder, each object will use its default image.

Legacy Rules

The **Top Level/System/Legacy Rules** folder is used for storing any Java class files for rules that were written for TeamConnect version 1.6.x. Previously, each object definition had its own **Legacy Rules** folder for storing these files. This centralized folder allows the files to be shared by multiple objects, instead of being uploaded to each individual object definition. This folder is not applicable if you do not have any TeamConnect version 1.6.x rules.

Libraries

The **Top Level/System/Libraries** folder allows developers to deploy JAR files outside of the **TeamConnect.war** file or the **WEB-INF/lib** folder to implement a custom solution. The class loader that loads classes from this folder is the parent of the following types of custom Java code:

- Custom appenders
- Custom Java blocks
- Custom portlets
- Custom tools
- Rules
    - Automated qualifiers
    - Automated actions

  - Scheduled actions
- Wizard initializers
- Wizard page transitions

The JAR files uploaded to this folder do not override the ones included in the TeamConnect WAR file or those that are present in the application server's classpath.

It is not necessary to restart TeamConnect if new JAR files are uploaded to the **Libraries** folder because they are automatically added to the class path. However, if JAR files are updated, you must restart TeamConnect in order for the changes to be applied.

Logging

The **Top Level/System/Logging** folder contains any Java class files used for modifying the log level that triggers a log message to be sent via email.

By default, the log defined by an SMTP appender is emailed when an event with the level of **Error** is generated. However, you can set the appender to email the log at a different log level.

Object Definitions

The **Top Level/System/Object Definitions** folder contains subfolders for each object definitions, including system object and custom object definitions. Each subfolder contains all of the files needed for the corresponding object's design, such as blocks, Document Generator templates, rule class files, and so on. The subfolders for each object are automatically created when the object is saved.

The following folders are found in each system object's folder—**Document Templates**, **Rules**, **Screens**, and **Template Folders**.

Two additional folders, named after the **Involved** object, are also found in the folder of any custom object that has these objects defined for it.

Object Definition Subfolders

Folder	Description
Document Templates	Contains the document templates that have been created and uploaded for use with the Document Generator.
Rules	Contains three subfolders: • **Automated Actions**—Contains Java or JavaScript files for the corresponding object definition. These files define an action that will be executed or a method that will be called wherever automated actions are used. For example, the custom actions or scheduled actions for rules are stored in this folder. Also, the files for wizard page actions and wizard page transition rules are stored in this folder.

	• **Automated Qualifiers—**Contains files that define custom qualifiers for the corresponding object definition. Rules that use these files for their qualifiers can be of any rule type. • **Legacy Rules—**Contains any Java class files for rules that were written for the corresponding object definition in TeamConnect version 1.6.x. This folder is not applicable if you do not have any TeamConnect version 1.6.x rules.
Screens	Contains all uploaded XML files that can be used for blocks for the corresponding object. They are available on the object definition's **Custom Blocks** tab.
Template Folders	Contains the directory structures, including all necessary documents, that have been created for use with object templates. When a record is created using a template or wizard, the directory structure for the template that is stored in **Template Folders** is automatically added to the **Attachments** folder of the record.
Involved	(Custom objects only) Contains the folders **Document Templates**, **Rules**, **Screens**, and **Template Folders** for the Involved Object.

Portal

The **Top Level/System/Portal** folder allows you to add custom content to portal panes on your users' home pages. Files placed in this folder can be used to obtain external data to be displayed in a portal pane.

Screens

The **Top Level/System/Screens** folder stores the following files that apply a common look and feel to system and custom blocks:

- **template.xml**--An XML template that defines the layout of block headers and footers
- **global.css**--A global cascading style sheet that contains definitions used by **template.xml** and custom blocks

StartUp

The **Top Level/System/StartUp** folder allows developers to deploy class files that should be executed when TeamConnect starts. This can be useful for installation scripts, to initialize TeamConnect using custom code, and to check consistency in the application for the session.

Important: *You should limit access to the* ***StartUp*** *folder to prevent the addition of malicious code.*

To enable the execution of custom code in the **StartUp** folder, you must set the app.runStartUp application parameter to YES in the **web.xml** file.

If you want to stop the execution of all class files in the **StartUp** folder in the event of any runtime errors or exceptions, you can set the app.runStartUp.failOnError parameter to YES.

TeamConnect finishes its standard initialization before it executes the class files in the **StartUp** folder. Your custom code can affect TeamConnect's initialization after the standard initialization and before TeamConnect becomes available via a web browser.

This start up functionality only supports Java class files. TeamConnect ignores non-Java class files and any sub-folders to the **StartUp** folder. However, you can include JAR files and reference to them from your class files. You can also upload Java classes that may be referenced from the executing class.

If multiple class files are present in the **StartUp** folder, TeamConnect executes them according to the alphabetical order of the file names.

Tools

The **Top Level/System/Tools** folder contains a subfolder for each custom tool that has been uploaded to TeamConnect. Each custom tool's folder contains two subfolders:

- **classes**—Stores necessary Java class files
- **resource**—Stores necessary XML files

You must manually create these folders when you create a custom tool.

1.9.1.1.4 Users Folder

The Top Level/Users folder contains a <username> subfolder for each user where their personal files may be stored. When a user selects Documents from the Go to menu, their personal Top Level/ Users/<UserName> folder opens by default. Each user can create subfolders in their personal folder, provided that they have been given the rights to do so.

1.9.2 Automatically Created Folders

The following table summarizes the folders that are automatically created when you create items in TeamConnect.

Certain folders are created automatically, the first time a user accesses the folder, rather than when the item itself is first created by a user. This helps keep the database clear of unnecessary folders.

Automatically Created Document Folders

New item created in TeamConnect	When folder is created	Path of automatically created folder	How folder is named	Folder contents
User	When users first access their personal folder by selecting	Top Level/ Users/ UserName For example:	Username (login name) specified in user account	Folder is empty upon creation. After the folder is created, it may

	Documents from the **Go to** list	Top Level/ Users/Jack		contain documents uploaded by and subfolders created by the user.
Custom object (including Embedded objects)	Upon creation of the custom object	Top Level/ System/Object Definitions/ ObjectName For example: Top Level/ System/Object Definitions/Case	Name of custom object as defined in the object definition	Folders for files needed for the object's design, including: • **Document Templates** • **Rules** • **Screens** • **Template Folders** For custom objects, the folders for Involved are stored here, if they are defined for the object. ***Note:*** *Embedded object folders do not contain any of the subfolders listed above except for Screens.*
Involved Object	Upon creation of the Involved Object	Top Level/ System/Object Definitions/ CustomObjectName/ InvolvedName	Name of Involved object as defined in the object definition	Folders for files needed for the Involved object's design, including the following: • **Document Templates** • **Rules** • **Screens** • **Template Folders**

Record created without Template files or folders	When a user first opens the record's **Attachments** folder by opening the record's **Documents** tab	Top Level/ Attachments/ ObjectName/ RecordName For example: Top Level/ Attachments/ Account/ Jones_Account _0402	• **System object records**—named using the record's name and its primary key • **Custom object records**—named using the Unique ID of the record, according to the settings in the object definition	• Folder is empty upon creation. • After the folder is created, it may contain any documents uploaded, or folders created, that are attached to the record by being added through its **Documents** block.
Record created with Template files or folders	Upon creation of the record.	Top Level/ Attachments/ ObjectName/ RecordName/ FolderName (or FileName) For example: Top Level/ Attachments/ Account/ Settlements_Ac count_0402/ TaxForms		• Upon creation, the folder includes files or folders that are automatically attached to the record because they are included in the Template. • After creation, the folder may contain any documents uploaded or folders created through the record's **Documents** block.

1.10 Glossary

A

accounts

Entities used for tracking financial accounts or budgets electronically. Accounts are typically defined for transactions related to a project. In addition, posting criteria are typically defined per account (which financial transactions can post to the account).

Admin Rights

These are access rights to features available from the **Admin** tab in the user interface. These include user records, group records, Admin Settings area, and logger rights.

Administrator (TeamConnectAdmin user)

A user (such as TeamConnectAdmin) whose job responsibilities include creating or maintaining user and group accounts, specifying the appropriate admin settings for the organization, and managing logs.

appender

A definition of a system or audit log. Appenders can be of various types, including SMTP, socket and file. File appenders are the most commonly used, as the logging statements are simply captured in a file. A log can be a general TeamConnect log, or it can be associated with a specific *logger*, so that it captures messages only from a certain TeamConnect area, such as portal panes or custom blocks.

applet

A small utility written in Java. In TeamConnect, applets can be used for the document screen interface and the hierarchical item selector. If applets are enabled on the system, users can enable them for their own use on the **Preferences** tab of the **Preferences** screen.

Application Programming Interface (API)

A set of object classes that expose public methods the TeamConnect system.

A language and message format used by a program to communicate with an operating system, database management system, communications protocol, or some other control program. For TeamConnect, the Web Services API provides services equivalent to end-user functionality in the application user interface (UI).

application server

In a TeamConnect environment, the application server hosts the TeamConnect .WAR or .EAR file. In TeamConnect properties files, the application server might also be called the host.

Appointment

A *System Object* that allows users to track their scheduled events, engagements, or meetings. Appointments are automatically available for custom objects.

Approval

In TeamConnect workflow process, an approval is an authorization action performed by a approver. After all required approvers perform approval actions on workflow requests, the original TeamConnect operation completes.

Approvers

In TeamConnect workflow process, an approver is a user with the authority to approve or reject certain actions attempted by requestors. There can be several approvers at each level of an *Approval* process.

During an approval process, approvers may be able to send the approval request to reviewers for review before they make their decision. Approvers can view their approval requests on the **My Approvals screen.**

Assignees

TeamConnect *Users* who are assigned to one or more Projects or Tasks. There can be one or several users assigned to a project. In projects each assignee can have a different role, such as attorney, agent, appraiser, paralegal, and so on. Typically, the main assignee is in charge of the whole project, whereas the rest of the assigned users are responsible for certain parts of the project. Tasks can have only one current assignee.

Attendees

TeamConnect Users and members of Contact Groups who are expected to take part in an event, such as a meeting or conference call, for which there is an Appointment scheduled.

authorization

Permission to access a resource controlled by a server. Authorization typically occurs after a server evaluates the access control list (ACL) associated with a resource. The types of events that require authorization to TeamConnect include user login, running TeamConnect rules, and running Web Service requests.

B

Block

A group of system and/or custom fields included into a single file, XML (for custom blocks) or JSP (for system blocks). In the end-user interface, each block is typically displayed as a separate tab or a section on the record screen.

TeamConnect *Object Views* provided by Mitratech consist of system blocks, such as **General**, **Categories**, **Workflow**, **Assignees**, **Attendees**, and so on. You can also create your own Custom Blocks using *Custom Fields*.

C

Category

Lookup items that allow you to organize custom fields into blocks or sections on the screen for the **Main** user interface. By adding or deleting categories in a record, users display or hide respectively the associated blocks of details in that record. Categories also help users to organize their records by certain types, for example, employee contact records vs. non-employee contact records, domestic vs. international accounts, and so on.

Category Rights

See *Category Security*.

Category Security

The *Rights* to the object's categories and their custom fields. This is the second level of security, after the object level. All rights assigned at this level take effect only if the access to the object itself is granted.

Category-level rights add more granularity to the object-level rights. A user might have access to the object, but you can still control access to the organization-specific information stored in the custom fields and displayed in forms or custom blocks.

CLASSPATH

An environment variable or argument set on the command-line that tells the Java Virtual Machine where to look for user-defined classes and packages in Java programs.

COD

Custom Object Definition

Contact

A *System Object* definition used to create a TeamConnect record for an individual, organization or group within a organization (such as department). Contacts can be organized into groups by creating *Address books*.

CSM

Collaborati Spend Management

Custom Fields

Custom fields can be created per system or custom object. These fields allow you to meet the individual needs of your organization.

Custom Object

Business Objects created for your organization by a TeamConnect Solution Developer TeamConnect Certified Professional. Custom Objects can have names used within your industry for files, such as matters, claims, litigation, or policies.

The individual instances of Custom Objects are sometimes referred to as Projects or Matters within this documentation.

Custom View

See *Object View*.

D

DataSource

An object that provides the means by which connection pooling may be neatly hidden and performed. A DataSource object is a factory for Connection objects. An object that implements the DataSource interface will typically be registered with a JNDI service provider. A JDBC driver that is accessed via the DataSource API does not automatically register itself with the DriverManager. This is the preferred way of communicating with a data source (for example, a database) and provides a good alternative to using a DriverManager.

Debug Settings

Refers to a scenario when an administrator changes a logger's logging level to Debug. This results in the highest possible detail level of output to the log file. Setting a logger's logging level to Debug is useful to help troubleshoot an issue but afterward you should change the logging level to Warning (or a less verbose setting) to maintain optimal system performance.

Document

A *System Object* definition used to manage files, folders, shortcuts, or hyperlinks in the TeamConnect Documents area. Documents are usually "attached to" other TeamConnect Records by uploading a file from the Documents page of a TeamConnect record.

Additional files necessary for customization of TeamConnect are also uploaded as Documents. These include XML files for *Custom Blocks*, *Custom Actions* for Java *Rules*, files included in *Templates*, and other files related to your customized system design.

E

end-user

A person who uses TeamConnect in a non-administrator or non-Solution developer capacity. This user type would typically not have rights to the **Admin** tab or the Designer application area.

For example, an end-user would typically have rights to work with system objects such as Documents, Contacts, and may have rights to work with custom objects such as legal Disputes. An end-user would typically have rights to create, edit, view, search, and delete contacts in TeamConnect.

Embedded Objects

Simple Custom Objects created as children of other *Custom Objects (parent objects)*. An Embedded Object can only exist within the context of a parent Custom Object. Within *Wizards* and *Templates*, embedded objects are considered *Related Objects*.

Expense

A *System Object* definition that is intended to allow *Users* to track internal costs of doing business in their organization. Expenses are automatically available as a system *Block* in *Object Views* for *Custom Objects*.

F

Full-Text Search

Allows you to search for items in the database according to their content. TeamConnect provides the feature of content searching in uploaded documents, and certain fields in *Records*, if Microsoft® SQL Server Full-Text Search or Oracle® Text (interMedia) is available on your database server. For

example, using content searching, you could search the content of uploaded documents to find a file in which a certain person's name is mentioned. This feature is available in search screens if the appropriate fields are included in the corresponding *Search View*.

G

Group

Typically refers to Group accounts (used in TeamConnect account administration to group multiple users with similar access rights or day-to-day business responsibilities). A group could also refer to a *Contact Group*.

Group Rights

Access *rights* to features and application areas that can be accessed in the user interface. These primarily include the rights to all *System Object* and *Custom Object* records, and certain *Tools*, such as Scheduler, Batch Task and Expense Entry. Rights are assigned by group account.

H

History

A *System Object* definition used to create notes associated with a specific Record. History records can only be created in relation to an already existing record. You can search for a history record from a global History search page.

Home Page

The first screen that users see after logging in to TeamConnect. Home Pages function as a starting point for all TeamConnect users and can be personalized to fit their individual needs. Users can access various types of information or do different actions from *Portal Panes* that are available on the Home Page.

host

A computer that hosts (is the source of) information or services used by other devices.

hostname

The logical name of a computer, such as machine.domain.domain, which is translated into an IP address.

HTTPS

A secure version of HTTP, implemented using the Secure Sockets Layer (SSL).

HyperText Transfer Protocol (HTTP)

The method for exchanging information between HTTP servers and clients.

I

internationalization

See *Localization*.

Internet Message Access Protocol (IMAP)

A standard mail server used on the Internet. It provides a message store that holds incoming email until users log in and download it.

Invoice

A *System Object* definition used to electronically track invoices or bills sent by *Vendors*. Invoices are typically billing records for goods or services provided by 3rd party vendors to TeamConnect customers.

Involved

A *System Object* definition used to keep track of various involved parties associated with a *Project*. An Involved object is always related to a *Custom Object*.

J

JAR

(Java Archive file) A file type packaged with the ZIP file format, for data compression. Libraries shipped with TeamConnect are typically distributed in .JAR format.

JDBC

Java database connectivity

JRE

Java runtime environment is a software bundle from Sun Microsystems that allows a computer system to run a Java application. The bundle includes the JVM and API. The API provides a set of standard class libraries. You can download the current JRE version by testing their JVM at the Java.com test page.

Java Virtual Machine (JVM)

A virtual machine is a simulated computer; it runs on a host computer but behaves as if it is a separate computer. The Java Virtual Machine works as a self-contained operating environment to run Java applets, with the advantage that Java applets can be run independently from the host operating system.

L

Lightweight Directory Access Protocol (LDAP)

A protocol used to access a directory listing. LDAP support is implemented in browsers and email programs, which can query an LDAP-compliant directory. In a TeamConnect environment, if you already have a 3rd party LDAP Server set up, you can configure TeamConnect user authentication to occur through your LDAP Server.

Localization

The process of customizing system and custom data for multiple languages and regions. In TeamConnect, you can localize the user interface and features, such as the time and data display. To localize in TeamConnect, you export the English data to an Excel spreadsheet, enter the translated data into corresponding fields, and import the translated data back into TeamConnect. After you import the data, the translated elements appear in your preferred language.

The term *localization* can be confused with *internationalization*, which involves selecting a language at runtime.

Line Item

A *System Object* definition used to list the goods or services specified in an *Invoice*. The details of each line item, such as the type (fee or expense), price, quantity, and dates must be entered in the Line Items screen of the corresponding invoice. Line items must be created from an existing invoice.

Logger

A component for a specific area of TeamConnect for which a system or audit log can be defined. For example, TeamConnect has loggers for portal panes, custom blocks, the XML layer, and user login/ sign off. When you define a log (or *appender*), you select which logger's messages it captures.

Lookup Table

Tables that organize, store and quickly access multiple items, such as contacts' roles, types of address, phone, fax and other contact information, and so on. In addition to adding, renaming, inactivating, and deleting items in system lookup tables, you can define new custom lookup tables and their contents. In the end-user interface, lookup tables are represented by either drop-down lists (most commonly) or radio buttons, where the user can look up the necessary information and make the appropriate selection.

Users have the option of displaying item hierarchies in a regular drop-down list or in a Java applet called a hierarchical item selector.

N

NTLM

NT LAN Manager. Former name for Windows Integrated Security. In a TeamConnect environment, you can configure TeamConnect user authentication to occur through a Microsoft Internet Information Services Server.

O

Object Definition

A specification of all properties of a *System Object* or *Custom Object*. A TeamConnect Solution Developer TeamConnect Certified Professional may edit a System Object Definition to create custom rules, create additional search views, customize additional object views, create wizards, or create custom blocks, among other operations. A TeamConnect Solution Developer TeamConnect Certified Professional would create a new object definition for a custom object.

Properties that are part of an Object Definition include its name, icon, categories and custom fields, look and feel of corresponding records, search views, wizard contents for creating its *Records*, and associated rules, among other properties.

Object View

A layout definition of tabs, sections/blocks, and other user interface elements per object definition. For an object definition, you can create multiple object views as an alternate method of customizing the available system and custom blocks for an object's records. For each group account, you can set each object definition's default Object View as an alternate method of setting record rights.

P

Portal Pane

A component of a *Home Page*, which represents a specialized menu that allows users to access different information or do specific tasks directly from the Home Page.

Preferences

System preferences that a user can set for his individual TeamConnect session. Preferences include color scheme and time zone, among other settings. Preferences settings are available from the **Preferences** link in the upper right corner of the user interface.

Process Manager

In TeamConnect workflow process, a TeamConnect group whose members are responsible for monitoring approval processes that are sent to approvers. Process Managers receive notifications of approval requests when there is an error. They may also be notified when a request is rejected or

expired. They can restart an approval process to resolve errors, rejections, or expirations, or reassign the task of approving a request to other users when necessary. They can also reject approval requests.

Project

Refers to a Record or instance of a *Custom Object*.

R

record

An instance of a *System Object* or *Custom Object* in TeamConnect, created and accessed in the user interface.

Record Security

Access protection set at the level of individual object records. For example, you can make a *Record* Private or Public or you can grant or deny the rights to read, update, and delete a record to other *Users* or *Groups*. This level of security can be set only on the **Security** tabs of individual records in the end-user interface. This is the lowest level of access rights. All rights assigned at this level take effect only if the appropriate rights are assigned at the object level.

request

In TeamConnect workflow process, an attempted operation by a user that is initially pending approval before the original operation can complete.

requestor

In a TeamConnect workflow process, a user who performs an action that triggers an approval process, such as posting an *invoice*. The *request* is sent to *approvers* according to the approval route that is defined for that workflow process.

reviewer

In TeamConnect workflow process, a user who reviews an approval request. An approver designates the reviewer for a request.

rights

Access permissions to records (categories, custom fields) and functional areas in TeamConnect. In TeamConnect, access rights are applied to enforce record or system security, preventing users from viewing or changing records/settings they should not be able to access. Rights are assigned to *Group accounts*.

Route

In TeamConnect workflow process, a defined hierarchy of groups whose members' *Approval* is required to authorize a requested operation. It is an approval path that can consist of one or more nodes, called Stops, that can contain one or more *Members* who can approve or reject the operation. Routes are used for the Workflow purposes, to control the actions that take place in your business processes.

Rules

TeamConnect allows you to create rules that control whether the operations attempted by users are in accordance with your business processes. A rule is triggered when the operation is attempted, and the *Qualifiers* are checked to determine what should occur. For example, rules can ensure that certain *Custom Fields* are filled out if a particular *Category* is selected.

Approval rules postpone the operation until all members in the approval process, or *Route*, have approved the operation.

Rules written using Java class files or JavaScript can also perform *Automated Actions* when they are triggered.

S

Search Module

A special utility that allows the user to quickly search for a specific record and link it to the record with which you are currently working without leaving its screen. The Search Module is represented by a field with two icons, **Find** and **Open**, next to it.

Secure Sockets Layer (SSL)

An industry standard protocol developed by Netscape for securing communications. It works by using public-key cryptography and certificates.

Service Of Process (SOP)

The procedure employed to give legal notice to a person (defendant etc.) of a court or administrative body's exercise of its jurisdiction over that person so as to enable that person to respond to the proceeding before the court, body or other tribunal. Usually, notice is furnished by delivering a set of court documents to the person to be served.

SQL*Plus

A command line SQL and PL/SQL language interface and reporting tool that ships with the Oracle Database Client and Server. It can be used interactively or driven from scripts.

Structured Query Language (SQL)

A computer language used to create, modify, retrieve and manipulate data from relational database management systems and object-relational database management systems. It is an ANSI/ISO standard.

System Object

Default *Business Objects* provided by Mitratech to your organization. They represent business objects that are common to most business models regardless of the specific industry.

TeamConnect System Objects include: *Account*, *Contact*, *Appointment*, *Expense*, *Invoice*, *Line Item*, *Task*, *History*, *Document*, *Involved*, *User* account, and *Group* account.

T

Task

A *System Object* definition used to track *internal* assignments, usually related to *Projects*. For example, preparing reports, following up on cases, reviewing documentation, and so on.

Template

This term can refer to the following:

- Document templates
- Templates used with Wizards
- Templates used with rules
- Templates used with wizards and rules

A document template is a template designed for use with the Document Generator. You can use this capability to generate documents from Records using certain fields, such as the name of the contact associated with the record.

Templates used with wizards or rules define default values that should be automatically filled in for certain fields, *Sub-objects*, and *Related Objects*. For more details on templates, see Creating Custom Pages.

tool

There are system tools that come by default with TeamConnect; however, it is also possible to create custom tools.

transaction

Events or happenings in your business that change its financial position, such as buying supplies, paying bills, withdrawing money, or buying equipment. For example *Expenses*, *Tasks*, and *Invoices* and regular money withdrawals from and transfers between *Accounts* incur transactions against accounts.

U

User

An account created for a person who logs into TeamConnect. Users must be members of *Groups*.

User Interface (UI)

The graphical representation of TeamConnect on the computer screen, where the user can click buttons and hyperlinks, make selections from drop-down lists, enter text into fields, and so on.

V

Version Control

A method of tracking the edits made to a document that is uploaded to TeamConnect. Version control allows users to access previous versions of a document, and even revert the current version back to a previous version if needed. Version control must be activated by the TeamConnect *Administrator*.

W

Workflow

In TeamConnect, workflow is defined through Approval Rules at the Object Definition level.

For example, in a financial setting, a financial officer may trigger an approval rule by attempting to delete an account. A corresponding approval request would be sent to an accounting manager (approver) who would approve or reject the request.

X

XML (extensible markup language)

In TeamConnect environments, XML is commonly used as the file format for properties files. When creating custom blocks in the TeamConnect Designer application area, you upload .XML files to designated screens folders (under TeamConnect Documents) that define a custom block.

Index

- . -

.css 96
.lss 96

- 4 -

4.2 62

- A -

account rights 196
  additional 197
  basic 196
accounts
  best practices 13
  rights 14
Action buttons 102
address book rights 203
  basic 203
admin setting rights 247
Admin Settings 90, 96
  About page 155
  Approval page 149
  Calendar page 118
  Connections page 153
  Documents page 120
  Email page 141
  general 10
  General page 93
  general settings 91
  History page 154
  Invoices page 147
  localization 106
  Maintenance page 151
  Notifications page 143
  regions 106
  Regions page 106
  Reporting page 127
  Search Results page 124
  Security page 128
  User Interface page 103
administrator tools 165
  Scheduled Actions Monitor 166
administrators 9
  accounts 12
  system 89
appender rights 265
appointment rights 199
  additional 201
  basic 199
approval admin settings 149
Audit Logging page 160
  clearing 162
  turning off 164
  turning on 164
authentication 170
  custom plug-in 186
  LDAP plug-in 176
  login URLs 170
  NTLM plug-in 171
automatically created structure 273

- B -

BusinessObjects 92

- C -

category rights 22
  prerequisites for all 24
  prerequisites for individuals 25
color profile 96, 96
color profile css 96
connections admin settings 152
contact rights 203
  additional 205
  basic 203
custom authentication plug-in 186
  default method 187
  message screens 187
  overriding authentication 187
Custom field 62
custom field and groups 62
custom field rights 22
  prerequisites for all 24
  prerequisites for individuals 25
custom logo 96
custom lookup table rights 252

custom record rights 232
involved parties 236
matters 232
milestones 240
projects 232
custom tool rights 249

- D -

design documents 266
automatically created folders 273
directory structure 266
document admin settings 118
file systems 119
version control 119
WebDAV 119
document directory structure 266
Attachments folder 268
HTTPRoot folder 268
System folder 269
top level folder 267
Users folder 273
document rights 208
additional 209
basic 208

- E -

email admin settings 135
email notifications 136
IMAP server 137
expense rights 215
additional 216
basic 215

- F -

frequently asked questions
address books for administrators 191
Admin Settings 192
budgets 192
from administrators 189
groups 189
licenses 192
users 189

- G -

general admin settings 91
getting started
administrators 9
global navigation toolbar rights 250
glossary
for administrators 275
group category rights 58
group custom field rights 58
group history 66
group object views 65
group record rights 243
additional 244
basic 244
Group Rights 62
group system rights 36
assigning disputes 57
assigning global admin 46
assigning global setup 48
assigning global users 38
assigning projects example 56
contact categories 60
contact fields 60
contacts example 55
creating contacts example 54
deleting contacts example 55
editing contacts example 54
global admin rights 47
global setup rights 49
global user results 40
viewing contacts example 53
group tool rights 64
groups 62
accounts 28
category rights 58
creating 33
custom field rights 58
deleting 66
editing 33
history 66
members 35
object views 65
pages 9
rights 28
searching 32

groups 62
system rights 36
templates 35
tool rights 64
viewing 33
working with 32

- H -

Hierarchy 62
Hierarchy Rights 62
history admin settings 154
recording 154
history rights 218
additional 219
basic 218
home page rights 250

- I -

IMAP email settings 137
configuring 139
email clients 141
email rights 141
SSL 138
starting 140
stopping 140
inolved party rights
basic 237
inserting new color profile 96
invoice admin settings 147
decimal places 149
invoice rights 221
additional 222
basic 221
involved party rights 236
additional 238
item selections 103

- L -

LDAP authentication plug-in 176
error pages 177
installing files 181
parameters 177
prerequisites 176
sample configuration file 185
sample error file 184
sample files 182
sample login file 182
sample restore file 184
less file 96
license information 157
schemes 157
style 158
uploading file 158
Locale Manager Tool 109
localization 114
exporting data 114
importing data 117
log rights 247
logging 159
appenders 159
default folders 161
login URLs 170
lookup table rights 251

- M -

maintenance admin settings 151
matter rights 232
additional 233
basic 232
involved parties 236
milestones 240
milestone rights 240
additional 241
basic 241
miscellaneous setting rights 253
multi-currency lookup table rights 252

- N -

notification admin settings 143
system notifications 146
NTLM authentication configuration file
editing 174
installing 174
NTLM authentication plug-in 171
anonymous access 173
enabling 175
Internet information services 173
prerequisites 172

- O -

object definition rights 255

- P -

portal pane rights 263
project rights 232
  additional 233
  basic 232
  involved parties 236
  milestones 240

- R -

record locking 91
region settings 106
report rights 226
reporting admin settings 127
rights 14, 62
  accounts 196
  address books 203
  admin settings 247
  administer custom tools 249
  administrator types 16
  administrators 243
  appenders 265
  appointments 199
  categories 22
  contacts 203
  custom fields 22
  custom lookup tables 252
  custom record types 27
  custom records 232
  documents 208
  end-user types 15
  end-users 194
  expenses 215
  global navigation toolbar 250
  group records 243
  history 218
  home pages 250
  invoice 221
  involved parties 236
  logs 247
  lookup tables 251
  matters 232
  milestones 240
  miscellaneous settings 253
  multi-currency lookup tables 252
  object definitions 255
  portal panes 263
  projects 232
  report 226
  routes 263
  solution developers 248
  solution developers types 16
  system record types 19
  system records 196
  system settings 265
  task 227
  TeamConnect areas 28
  TeamConnect features 28
  user records 245
route rights 263

- S -

saving 11
Scheduled Actions Monitor 166
  actions 168
  activating 169
  creating 167
  deactivating 169
  deleting 170
  finding 166
  Run Now button 170
  running 170
  tasks 167
search results admin settings 122
  maximum search results 123
security admin settings 128
  user authentication 133
System Logging page 160
  clearing 162
system record rights 196
  accounts 196
  address books 203
  appointments 199
  contacts 203
  documents 208
  expenses 215
  history 218
  invoice 221

system record rights 196
prerequisites 21
related records 21
report 226
task 227
system setting rights 265

- T -

task rights 227
additional 228
basic 227
TeamConnect area rights 230
preferences 231
release edit locks 231
scheduled actions 231
TeamConnect Enterprise
administrators 9
TeamConnect feature rights 230
preferences 231
release edit locks 231
scheduled actions 231
TeamConnect logs 159
clearing 162
system logging levels 162
TeamConnect summary 155
available updates 156
license information 157
support options 157
versions 155
terminology
administrators 12
top level folder
Attachments 268
HTTPRoot 268
System 269
Users 273
troubleshooting
for administrators 192

- U -

understanding 14
user category rights 85
user history 88
user interface admin settings 96
Action buttons 102
custom logo 96
item selections 103
user selections options 102
user record rights 245
additional 246
basic 246
user selection options 102
user system rights 78
assigning global admin 83
assigning global setup 84
assigning global users 82
user tool rights 87
users
accounts 67
activating 76
category rights 85
creating 71
deleting 88
editing 71
General page 89
history 88
inactivating 76
limited-privilege 75
membership 77
passwords 76
preferences 76
rights 67
searching 69
system rights 78
templates 75
tool rights 87
unlocking accounts 77
viewing 69
working with 68