
Technical Document

Title: TEA Security and Administration
Category: The Exceptional Assistant - Administration
Author: TEA Support Team

Last Revision Date: February 13, 2004
Revision #: 1.0
Reference ID: n/a

TEA Security and Administration

You might think that it's just common sense that any business that collects personal information from customers would also have a security plan in place to protect the confidentiality and integrity of the information. Actually, it's far more than just common sense these days - it's the law in both Canada and the US and in many other countries around the globe. Aside from any legal issues, it's also just plain good for business. When you show your customers that you care about the security of their personal information, you increase their level of confidence in your institution.

Organizations using The Exceptional Assistant (TEA) range from government-funded initiatives to private lending institutions, each one undoubtedly having implemented an information security plan to some degree. Although computer systems aren't the only responsibility related to information security, they are an important one. The personal and financial information stored in TEA must also be considered.

In too many cases, organizations do not adopt any security protocol within TEA and as such allow employees far more access to functionality than is actually required to perform the tasks within their position. The reality is that if organizations allow users to have full access (administrator privileges) to TEA, and therefore access to functionality beyond what is required to perform their job, the data and the privacy of personal client information may be at risk.

User Profiles

User Profiles are the basis of defining an individual's access to specific functions and areas of TEA. It is imperative that they be assigned specifically based on the roles and responsibilities of the individual staff members within the organization.

When TEA is shipped to customers, it comes with five predefined User Profiles. They are numbered from one to five and the higher the number the more access privileges the user has. These profiles were created to assist customers in creating/modifying profiles. Although these profiles may closely represent the various positions in your organization, we strongly advise that you create your own User Profiles for each core position in your organization. This will ensure that users only have access to the functionality required for their role in the TEA database.

It is best for TEA users to only be assigned the specific permissions to perform their required tasks. The more features that are accessible, the more confusing it is for an individual to complete their tasks as the additional 'screen noise' can make TEA seem less intuitive. Also, if permissions are not assigned based on user capacity in the system, critical features are made available to users who have no

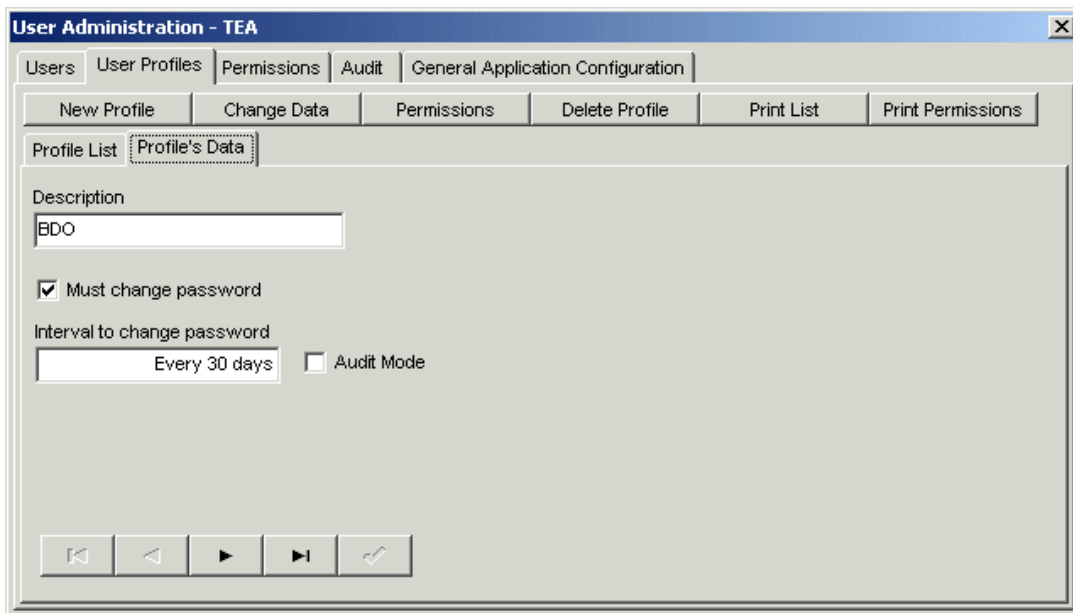
training or knowledge on how to use them. This is one of the major causes of data corruption and data inaccuracies.

Within TEA, there are several configuration options that allow you to enforce your desired protocol including:

- Ability to define User Profiles based on key positions in your organization.
- Ability to force users to change passwords based on a user-defined interval.
- Ability to time-out users after a user-defined period of inactivity.
- Keep track of password histories for users in the database.
- User accounts can expire if they are only temporary staff members.
- Audit log of when users login and out of the database.
- Ability to disable users after a specific period of inactivity.
- Ability to disable Users after a user-defined number of unsuccessful login attempts.
- Ability to assign varying levels of access to TEA features and functionality (permissions).

Customizing the User Profiles

- 1 Log into the **TEA Administration Module** using your assigned username and password and select **User Management**.
- 2 In the list of available applications, select **TEA** and click **Open**.
- 3 Select the **User Profiles** tab.
- 4 Select the **Profile's Data** tab to see the settings for the selected profile.






Key options that provide enhanced data security and should be activated during the configuration of User Profiles include:

Option	Description
Must change password / Interval to change password	Forces the users to change their password on a regular interval (monthly, weekly etc.) as specified by the interval. It is critical that users create unique passwords using a combination of lower case and uppercase letters combined with numbers. This makes the password very difficult to deduce and provides a safeguard against security vulnerabilities.
Audit Mode	Tracks all of the users who login/out of the database including the time they logged in/out and the computer from which they did so.
Permissions	Allows the administrator to control the level of access a user or group of users has to the different functions and areas in TEA.

Permissions

Once you have defined the basic User Profiles that you will use in TEA, you can begin to setup the permissions for each profile. The assigning of permissions is one of the most important aspects of User Administration and User Profiles. You must first identify the specific roles and responsibilities of each core position in your organization and then assign the appropriate permission to each task listed as required. There are three levels of permission that can be assigned to a task or function in TEA

Index of Permissions

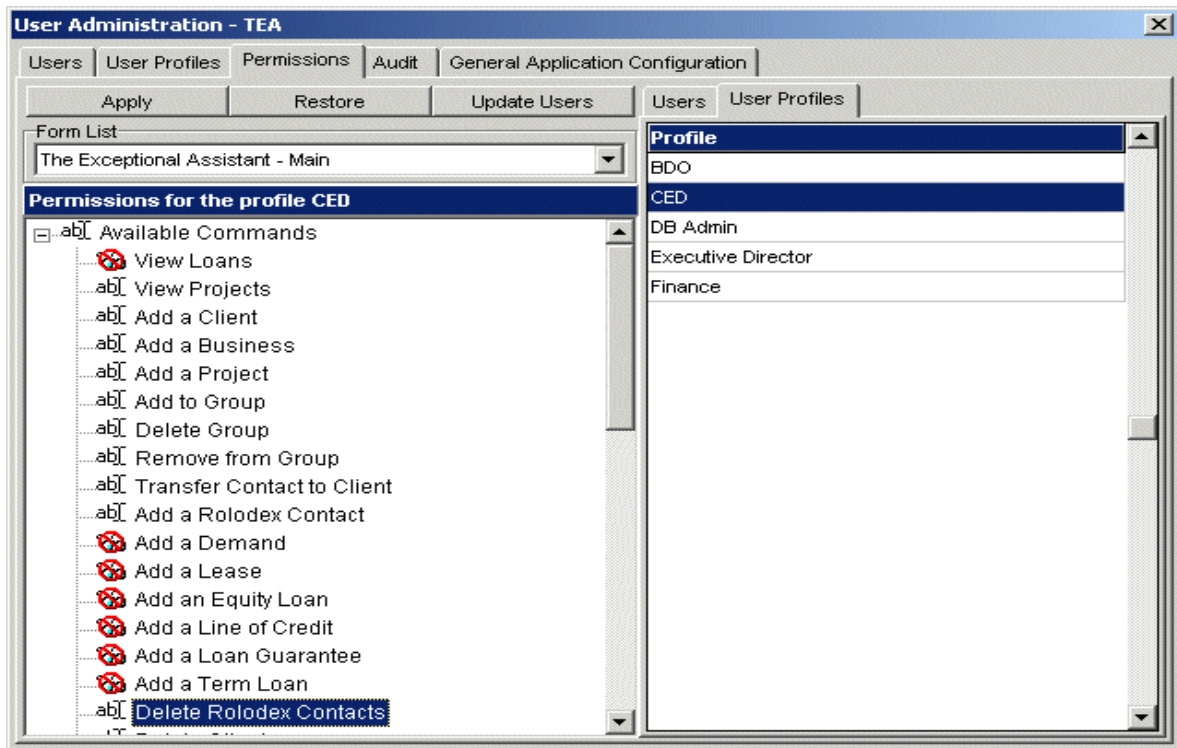
	feature is not available to profile or user
	feature is available to profile or user
	profile or user can see the feature but cannot access it

Viewing and Assigning Permissions

The following instructions take you through the process of assigning the desired permissions for a single profile. In all likelihood, you will have more than one profile so this procedure will have to be repeated for each user profile defined in your system. In addition, the commands or functions available in TEA have been grouped by Form. Each form contains a list of available commands that are specific to that area of TEA. A section of the following procedure will need repeating for each form.

- 1 Log into the **TEA Administration Module** using your assigned username and password and select **User Management**.
- 2 In the list of available applications, select **TEA** and click **Open**.

- 3 Select the **Permissions** tab.
- 4 From the tab control to the right, select the **User Profiles** tab.



- 5 Select a profile.
- 6 In the Forms List drop-down, select the first form listed.
Note: You will have to follow the next 3 steps procedure for each form listed.
- 7 Expand the list of **Available Commands** if required.
- 8 For each command (or function) listed, set the permission level by clicking on command name until the desired permission symbol is displayed (see index above).



We have developed some sample User Profile Worksheets to assist you in the development of user profiles and permissions for your organization which is located at the end of this document.

- 9 When done, click **Apply** to apply the changes you've made to the profile's permissions
- 10 Click the **Update Users** button. This updates all users that currently belong to the selected profile with the updated permissions.
- 11 Repeat Steps 6-10, selected a different form from the Forms List drop-down until you have updated all forms.
- 12 Close the **User Management** window and then close the **TEA Administration Module**.

General Application Configuration

There are various settings that globally control the database related to user access and data security. These settings can be found in the User Administration module under General Application Configuration. The key settings are defined below:

Setting	Description
Time Out	Users are automatically logged out when inactivity has exceeded the specified value (calculated in minutes). This is an excellent safeguard and a policy that should be adopted by all organizations. If a user forgets to logout at the end of the day or before a break, the database will logout automatically providing the 'Time Out' setting is configured properly.
Maximum unsuccessful login attempts and Disable User	Users are disabled (login privileges revoked) after the specified number of consecutive, unsuccessful login attempts.
Maximum Inactive Days	Users are disabled (login privileges revoked) if the number of days since their last successful login to TEA or TEA Admin has surpassed the maximum days specified.
Maximum Password History	When a user is forced to make regular password changes, the previous specified number of passwords are kept on file. The new password entered cannot be in this previous list, and each new password bumps the earliest password off the history list. This forces the user to actually change their password, and not to re-use old passwords.

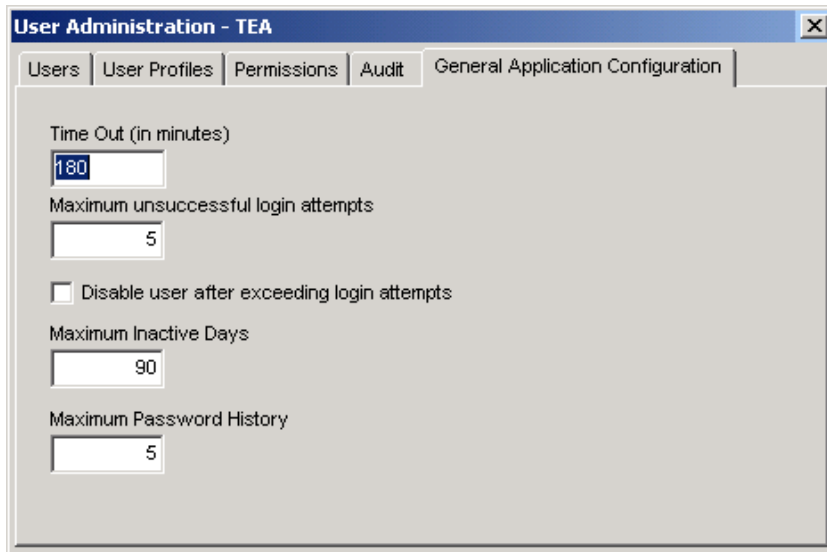


Once a user has been disabled, an Administrator is required to re-enable the user before they will be allowed to login again.

To modify the General Application Configuration

- 1 Log into the **TEA Administration Module** using your assigned username and password and select **User Management**.
- 2 In the list of available applications, select **TEA** and click **Open**.

- 3 Select the **General Application Configuration** tab and make modifications as desired.



The screenshot shows a window titled "User Administration - TEA" with a close button in the top right corner. The window has a tabbed interface with five tabs: "Users", "User Profiles", "Permissions", "Audit", and "General Application Configuration". The "General Application Configuration" tab is selected. The configuration area contains the following settings:

- Time Out (in minutes):** A text input field containing the value "180".
- Maximum unsuccessful login attempts:** A text input field containing the value "5".
- Disable user after exceeding login attempts:** An unchecked checkbox.
- Maximum Inactive Days:** A text input field containing the value "90".
- Maximum Password History:** A text input field containing the value "5".

The User Administration is not difficult to configure. By taking the time to give due consideration to the specific roles and responsibilities of each user in the system and setting the General Application Configuration options appropriately, you can significantly decrease any security and personal information vulnerabilities in your system.

In addition to the sample profiles included as appendices in this document, we have designed User Profile and Permissions Worksheets to assist you in creating and defining your own user profiles. We strongly recommend that you complete the User Profile and Permissions Worksheets before attempting to modify the user profiles in TEA Admin. These worksheets can be downloaded from the Resource Centre on the TEA website (<http://www.commongoals.com/tix>).

Appendix A - Sample Profiles

Five sample profiles are defined below. You can use these as guidelines for positions and profiles within your organization. List staff in your office that fits the profile so that you can assign each staff/TEA user to the correct user profile in the TEA Administration Module.

Profile #	Profile Name	Responsibilities	Staff
1	BDO	To solicit and attract new financing deals that fall within the mandate of our organization. This includes the completion of all loan underwriting and legal responsibilities for deal completion. All related parameters must be entered in the TEA database up to the completion of the lending terms and amortization schedule.	Ian Getdadeals
2	Finance	To ensure that all financial matters involving the corporation are in accordance with GAAP. To provide the final audit and approval of all loans entered in system. To perform all banking duties including PAP's and reconciliation.	John Moneyman
3	DB Admin	To administer the TEA database and all of its components. To ensure the database is always up-to-date with all current patches. To create new reports using the CRB and to download any new reports from the web site as needed. To assign and maintain access privileges in the database for all users using organizational user access and security protocol.	Scott Technowiz
4	CED	To create strategic partnerships within the community to foster economic development and healthy communities. This includes always looking for new opportunities within the community for employment creation and socio-economic gain.	Krista Coordinator
5	Exec. Director	To ensure the vision, mission and operating values of the organization is always in the forefront of all decisions. To oversee the entire portfolio and lending operations in addition to solicitation and acquisition of capitalization sources for our Loan Funds.	Shannon Bigshot

Appendix B - Sample Permissions

Sample Permissions for form Main

The following chart provides suggested permissions for the available commands on form Main for the sample user profiles discussed earlier. Your profiles and the permissions assigned to them may differ.

Profile #	1	2	3	4	5
Profile Name	BDO	Finance	DB Admin	CED	Exec. Director
Main - Available Commands					
View Loans	Y	Y	Y	N	Y
View Projects	N	N	Y	Y	Y
Add a Client	Y	N	Y	Y	Y
Add a Business	Y	N	Y	N	Y
Add a Project	N	N	Y	Y	Y
Add to Group	Y	N	Y	Y	Y
Delete Group	Y	N	Y	Y	Y
Remove from Group	Y	N	Y	Y	Y
Transfer Contact to Client	Y	N	Y	Y	Y
Add a Rolodex Contact	Y	Y	Y	Y	Y
Add a Demand	Y	N	Y	N	Y
Add a Lease	Y	N	Y	N	Y
Add an Equity Loan	Y	N	Y	N	Y
Add a Line of Credit	Y	N	Y	N	Y
Add a Loan Guarantee	Y	N	Y	N	Y
Add a Term Loan	Y	N	Y	N	Y
Delete Rolodex Contacts	Y	Y	Y	Y	Y
Delete Clients	Y	N	Y	Y	Y
Delete Projects	N	N	Y	Y	Y
Delete Businesses	Y	N	Y	N	Y
Delete Loans	N	N	Y	N	N
Print Report: Rolodex List	Y	Y	Y	Y	Y
Print Report: Business Information	Y	Y	Y	Y	Y
Print Report: Business List	Y	Y	Y	Y	Y
Print Report: Client Information	Y	Y	Y	Y	Y
Print Report: Client List	Y	Y	Y	Y	Y
Miscellaneous Contacts	Y	Y	Y	Y	Y
Batch Manager	N	Y	Y	N	N
Simulate Amortization Schedules	Y	Y	Y	Y	Y
Report Explorer	N	Y	Y	N	N
Advance Session Date	N	Y	Y	N	N
View Business	Y	Y	Y	N	Y
Global Interest Update	N	Y	Y	N	N
Floating Rate Tables	N	Y	Y	N	N
View Investment	N	Y	Y	N	Y
Delete Investment	N	N	Y	N	N
Add Investment	N	N	Y	N	Y
ACH Manager	N	Y	Y	N	N
Loan Transaction Processing	N	Y	Y	N	N
Global Interest Update for	N	Y	Y	N	N
Investment Transaction	N	Y	Y	N	N
Add Investor	N	N	Y	N	Y
View Investor	N	Y	Y	N	Y
Delete Investor	N	N	Y	N	Y

Sample Permissions for form Loans

The following chart provides suggested permissions for the available commands on form Loans for the sample user profiles discussed earlier. Your profiles and the permissions assigned to them may differ.

Profile #	1	2	3	4	5
Profile Name	BDO	Finance	DB Admin	CED	Exec. Director
Loans					
Loan Conversion Wizard	N	Y	Y	N	N
Add Task	Y	Y	Y	N	Y
Add Note	Y	Y	Y	N	Y
Add Attachment	Y	Y	Y	N	Y
Add Collateral	Y	Y	Y	N	Y
Edit Collateral	Y	Y	Y	N	Y
Delete Collateral	Y	Y	Y	N	Y
Edit Transaction	N	Y	Y	N	N
View Journal Entry	N	Y	Y	N	N
Reverse Transaction	N	Y	Y	N	N
Add Leverage	Y	N	Y	N	Y
Add Employment Statistic	Y	N	Y	N	Y
Add Bank Contact	Y	N	Y	N	Y
Delete Bank Contact	Y	N	Y	N	Y
Transfer To Approved	N	Y	Y	N	N
Add Insurance	N	Y	Y	N	N
Edit Insurance	N	Y	Y	N	N
Calculate Insurance	N	Y	Y	N	N
Deleted Transactions List	N	Y	Y	N	Y
Calculate Ownership	Y	Y	Y	N	Y
View Share Transactions	Y	Y	Y	N	Y
View Dividend Schedule	Y	Y	Y	N	Y
Add Lease Item	Y	Y	Y	N	Y
Edit Lease Item	Y	Y	Y	N	Y
Delete Lease Item	Y	Y	Y	N	Y
View All Terms	Y	Y	Y	N	Y
View All Rates	Y	Y	Y	N	Y
Delete Attachment	Y	Y	Y	N	Y
Delete Employment Statistic	Y	N	Y	N	N
Delete Leverage	Y	N	Y	N	N
Delete Note	Y	Y	Y	N	Y
Delete Task	Y	Y	Y	N	Y
Delete Transaction	N	Y	Y	N	N
Edit Note	Y	Y	Y	N	Y
Edit Employment Statistic	Y	N	Y	N	N
Edit Attachment	Y	Y	Y	N	Y
Edit Leverage	Y	N	Y	N	N
Edit Task	Y	Y	Y	N	Y
Change Loan Type	Y	Y	Y	N	Y
Add Transaction	N	Y	Y	N	N
Delinquency Journal	M	Y	Y	N	N
Amortization Workshop	Y	Y	Y	N	Y
Delete Insurance	N	Y	Y	N	N
Loan Options	N	Y	Y	N	N
Add Participation	Y	Y	Y	N	Y
Edit Participation	Y	Y	Y	N	Y
Add Required Report	Y	Y	Y	N	Y
Edit Required Report	Y	Y	Y	N	Y
Delete Required Report	Y	Y	Y	N	Y
Add Escrow Invoice	N	Y	Y	N	N
Edit Escrow Invoice	N	Y	Y	N	N

Profile #	1	2	3	4	5
Profile Name	BDO	Finance	DB Admin	CED	Exec. Director
Delete Escrow Invoice	N	Y	Y	N	N
Add Financial Statement	Y	Y	Y	N	Y
Edit Financial Statement	Y	Y	Y	N	Y
Delete Financial Statement	Y	Y	Y	N	Y

Sample Permissions for form Investment

The following chart provides suggested permissions for the available commands on form Investment for the sample user profiles discussed earlier. Your profiles and the permissions assigned to them may differ.

Profile #	1	2	3	4	5
Profile Name	BDO	Finance	DB Admin	CED	Exec. Director
Investment					
Add Task	Y	Y	Y	N	Y
Add Note	Y	Y	Y	N	Y
Add Attachment	Y	Y	Y	N	Y
Edit Transaction	N	Y	Y	N	N
View Journal Entry	N	Y	Y	N	N
Reverse Transaction	N	Y	Y	N	N
Add Bank Contact	Y	Y	Y	N	Y
Remove Bank Contact	Y	Y	Y	N	Y
View Deleted Transactions List	N	Y	Y	N	Y
Remove Investor	Y	N	Y	N	N
Add Loan	Y	N	Y	N	Y
Remove Loan	Y	N	Y	N	Y
Add Required Report	Y	Y	Y	N	Y
Edit Note	Y	Y	Y	N	Y
Delete Note	Y	Y	Y	N	Y
Edit Attachment	Y	Y	Y	N	Y
Delete Attachment	Y	Y	Y	N	Y
Edit Task	Y	Y	Y	N	Y
Delete Task	Y	Y	Y	N	Y
Delete Transaction	N	Y	Y	N	N
View All Terms	Y	Y	Y	N	Y
View All Rates	Y	Y	Y	N	Y
Delete Required Report	Y	Y	Y	N	Y
Edit Required Report	Y	Y	Y	N	Y
Add Transaction	N	Y	Y	N	N
Delinquency Journal	N	Y	Y	N	N
Change Investment Type	Y	Y	Y	N	Y
Amortization Workshop	Y	Y	Y	N	Y
View/Change Status Dates	Y	Y	Y	N	Y
View Options	N	Y	Y	N	N

Appendix C - Useful Resources and Links

Title	Link	
Privacy Commissioner of Canada (Website)	http://www.privcom.gc.ca/index_e.asp	CDN
Industry Canada - PIPEDA and Privacy for Business (Website)	http://privacyforbusiness.ic.gc.ca/epic/internet/inpfb-cee.nsf/vwGeneratedInterE/Home	CDN
Federal Trade Commission - Privacy Initiatives (Website)	http://www.ftc.gov/privacy/index.html	US
Financial Privacy - The Gramm-Leach Bliley Act (Website)	http://www.ftc.gov/privacy/glbact/index.html	US
Blank Profiles and Permissions Worksheets for TEA (MS-Excel spreadsheet)	http://www.commongoals.com/tix/en/support/support.cfm	n/a