

Overview

Productive Access, Inc. (PAI) understands that security is important to our customer, which is why it's our top priority. When you use the SaaS (software as a service) version of mTAB™ (mTABWeb), you'll enjoy the piece of mind that only our security infrastructure can provide.

We recognize the importance of the security of your data and have put into place controls to ensure your confidential and proprietary information will only be able to be accessed by individuals who are explicitly authorized to view the information.

Security Measures

Among other security measures, mTABWeb provides:

- Experienced, professional engineers dedicated to data and systems protection
- Continuous deployment of proven and up-to-date security technologies, including proprietary solutions developed by PAI.
- Total commitment to a secure, stable and private, co-located system managed by PAI.

Security Details

mTABWeb is as secure as any leading online application service provider. Configured by experts and rigorously tested before going into production, our security infrastructure includes proven, up-to-date firewall protection, intrusion detection systems and other security technologies, including proprietary products developed by PAI.

Information Access Control

To provide both centralized administration and management, the mTABWeb Data Server allows an administrator to establish access control via groups that govern access to studies made available through mTABWeb. After a user is authenticated, the mTABWeb Server can limit access to only those resources that have been made available to that user.

The key design components include:

- Users: individual accounts by username.
- Groups: Named by the client administrator to aggregate users. By assigning individual users to specific groups and authorizing groups to access studies, administrators can greatly reduce administrative overhead.
- Administrators: mTABWeb enables administrators to create accounts, groups and assign study permissions per group. An administrator can fully administrate all groups and studies.

User Access Control

Secure Socket Layer, or "encrypted" web traffic transmission is automatically deployed throughout the system. This includes encrypted username/passwords during authentication and all data transfers between the server and the client. There are no administrative consequences to this additional security level.

A user can only be created using mTABWeb. The administrator creates users and assigns users to groups. mTABWeb identifies first time users and, if the users selects the "remember me" check box, will create a machine identification tag or "cookie" for the machine. The "cookie" is associated with only one user. This enables mTABWeb to pre-fill the username and password fields during the login process.

Once a user is authenticated by mTABWeb, a session identifier is created and associated with the user. This session identifier contains information regarding the user and their permissions. The session mechanism has a timeout property, if a user logs in and is then inactive for 3 hours, the session will timeout. Only users with valid session identifiers can access data in the mTABWeb system. For added security, the session id is automatically scrambled and re-established in the background at regular intervals.

Unauthorized access attempts are logged and reported in real-time to the mTABWeb administrators via email notifications. After a customer definable amount of unsuccessful attempts to gain access, mTABWeb will disable a user account automatically. mTABWeb will automatically deny access to any computer associated with unauthorized access. The administrator must intervene and either allow access for this user and machine or permanently disable the account and computer.

mTAB Databases

As served on mTABWeb, the databases are not directly accessible as a file or files by the user and therefore cannot be downloaded and examined by the user.

Moreover, the mTAB database format is a copyrighted and proprietary design of Productive Access Incorporated. PGP does not license this technology to third parties, and therefore there is no other manner in which to examine an mTAB database other than by use of the mTAB software product.

The mTAB database format is highly compressed and configured in a manner that is, for all practical purposes, impossible to interpret without direct assistance from PGP. This interpretation would include extension to any possible means of interception and capture of the Internet communication between a user and the server.

mTAB database files can be optionally configured for download only in combination of permission to a user and separate permission to each individual database eligible for downloading. This configuration requires concurrent approval by both PGP and the client administrator. The benefit of the optional mTAB database downloading is the ability for client to maintain an additional backup of the database on the client site.

Tradeoffs: Administrative time in maintaining the additional backup, additional client responsibility required for backing up and securing the downloaded files.

Perimeter Defense

The network perimeter is protected by firewalls and monitored by intrusion detection systems. In addition PAI continuously monitors and analyzes security logs to proactively identify security threats.

Data Security

Precautions have been taken to minimize physical access to the data associated with mTABWeb. Access to data is controlled at the operating system level.

Internal Systems Security

Inside the perimeter firewalls, systems are safeguarded by network address translation, port redirection, Network Address Translation (NAT), non-routable IP address schemes and more. The specific details of these features are proprietary.

Operating System Security

PAI enforces tight operating system-level security by using a minimal number of access points to all production servers. We protect all operating system accounts with strong passwords. All servers are maintained at the vendor's recommended patch levels and recommendations for security. The servers are further secured by disabling or removing all unnecessary users, protocols, and processes.

Reliability and Backup

All data is backed up on a nightly basis. Disaster recovery plans are in place and tested on a consistent basis. Daily incident status and audit reports allow our engineers to proactively respond to problems.

Base Security Model

Role of the Client Administrator

A Client Administrator exists for each mTABWeb customer account and the administrator represents a key aspect of the mTABWeb security model. The administrator is typically a client employee familiar with the mTABWeb service, or the administrator can optionally be a PAI / Gamma (hereafter: PGP) employee, if required by the client.

Administrator Responsibilities

- Maintain the user listing
The administrator is responsible for the addition, deletion and disabling of client users up to the maximum number of licensed users. The web-based tools provided to the administrator will prohibit adding users beyond the maximum number licensed.
- Create user groups as required
Users can be organized into groups, which can enable limiting the exposure of specific studies to individual users. Users can be placed into one or more groups, thereby increasing the administrator's flexibility in exposing studies to selected individuals (e.g. all users can see studies A - F, group 2 users can incrementally see studies E, G, etc.)
- Maintain study permissions and "Available Studies Menu" folder housekeeping
The Administrator is notified by e-mail when a new study is available to the client. The Administrator will then:
 - o Permission the studies to the appropriate client group. (Initially ONLY the administrator has permission to view the study)
 - o Place the studies in the appropriate "Available Studies Menu" folders. This is a housekeeping step that makes it more convenient for users to find studies in the Available Studies Menu.

The following sections will provide descriptions and screen shots of mTABWeb's security features. After logging in to www.mtabweb.com, the administrator will be presented with the mTABWeb homepage.

How to Maintain the User Listing

To add a user, select User Admin from the Admin menu and you will be presented with the screen below. If your total number of users has not yet exceeded the maximum number of licenses, you will be permitted to add users. Enter the required fields: Email Address and Full Name and then select the optional fields that you desire. A randomly generated password is automatically created once the Insert button is selected. The optional fields consist of:

- Language – available options include English, French, German or Japanese. At present, only English and French languages are fully implemented; contact your PGP representative regarding your language requirements.
- Admin Privileges – a client can have one or more administrators, please see Page 3 of this document for a detailed list of capabilities and responsibilities this option allows.
- Study Privileges – allows the user to permission studies to other users within the client.
- Import Recodes – This allows the user to import recodes created in mTAB for Windows.
- Allow Slice – available options include No Slice and Database Controlled. Selecting the No Slice option prevents the user from exporting record level data. The Database Controlled option controls record level access based on how the database was constructed.
- Allow Resource Management – allows the user to publish saved tabs, recodes and User Defined Question (UDQs) to other users within the client outside of their group.
- Disabled – This allows the administrator to prohibit this user from accessing mTABWeb without altogether deleting the user.

The screenshot displays the mTABWeb User Administration interface. At the top, there is a navigation bar with links for Home, About, and Logout. Below this is a header section with the PAI logo and the text 'mTABWeb Demo'. A secondary navigation bar includes links for Support, Manage Resources, Tools, and Admin. The main content area is titled 'User Manager' and features a form for adding or editing users. The form includes fields for Email Address, Full Name, Password (labeled 'Randomly Generated'), Language (set to English), Admin Privileges, Study Privileges, Import Recodes, Allow Slice (set to Database Controlled), and Allow Resource Management. An 'INSERT' button is located below the form. Below the form is a 'User List' table with the following data:

	Email	Full Name	Group	Disabled
[edit]	webtrial	Guest Account	All Users	N
[edit]	Admin	Admin	All Users	N
[edit]	Fiona.dryburgh@poferries.com	Fiona Dryburgh	All Users	N
[edit]	cliff.hudson@poferries.com	Cliff Hudson	All Users	N

The footer of the page includes the text 'Making Molehills Out of Mountains...' and a copyright notice: '© 2002-2003 Productive Access, Incorporated'. There are also links for Terms Of Use, Contact Us, Global Home, and mTABWeb Overview.

Client Specific Security

To delete a user, disable a user or change the password or options of a user, scroll down to the bottom of the User Manager web page, and click the [edit] link preceding the user's name. The user information will be filled in and the New, Update and Delete buttons will appear.

To change the password or options of a user, click the appropriate item, make the change and then click on the Update button.

To disable a user, click on the Disabled checkbox and click on the Update button. This will prevent this user from logging in to mTABWeb but will not remove the user from the Users table.

To delete a user, click on the Delete button. You will be prompted with a message asking if you are sure, Select Yes and this will remove the user from the Users table.

The screenshot displays the mTABWeb User Administration interface. At the top, there is a navigation bar with the PAI logo, the text 'mTABWeb Demo', and links for 'Home | About | Logout'. Below this is a secondary navigation bar with 'Support', 'Manage Resources', 'Tools', and 'Admin'. The main content area is titled 'User Manager' and includes a dropdown menu for 'mTABWeb Demo' and 'All Users'. A form for editing a user is shown with the following fields:

- Email Address: webtrial@paiwhq.com
- Full Name: Guest Account
- Password: trial
- Language: English
- Admin Privileges:
- Study Privileges:
- Import Recodes:
- Allow Slice - 1: Database Controlled
- Allow Resource Management:
- Disabled?:

Buttons for 'NEW', 'UPDATE', and 'DELETE' are visible, along with a link for '[Expired DB Download Relationships]'. Below the form is a 'User List' table:

	Email	Full Name	Group	Disabled
[edit]	webtrial@paiwhq.com	Guest Account	All Users	N
[edit]	Admin	Admin	All Users	N
[edit]	Fiona.dryburgh@poferries.com	Fiona Dryburgh	All Users	N
[edit]	cliff.hudson@poferries.com	Cliff Hudson	All Users	N

The footer features the slogan 'Making Molehills Out of Mountains...' and the following text: 'mTABWeb.com Terms Of Use | Contact Us | Global Home | mTABWeb Overview. This site is protected by copyright and trade mark laws under U.S. and International Law. Review our privacy policy. All rights reserved. © 2002-2003 Productive Access, Incorporated.'

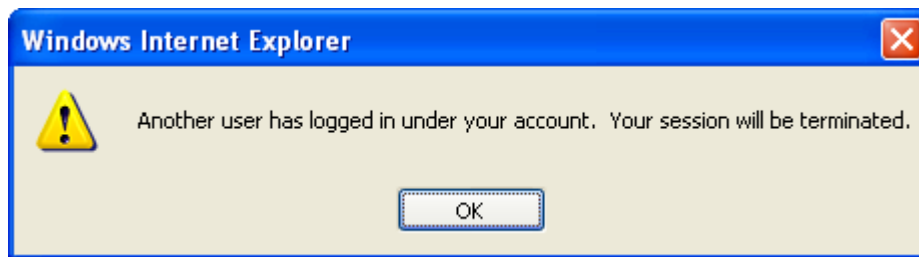
Client Specific Security

New User Notification E-mail

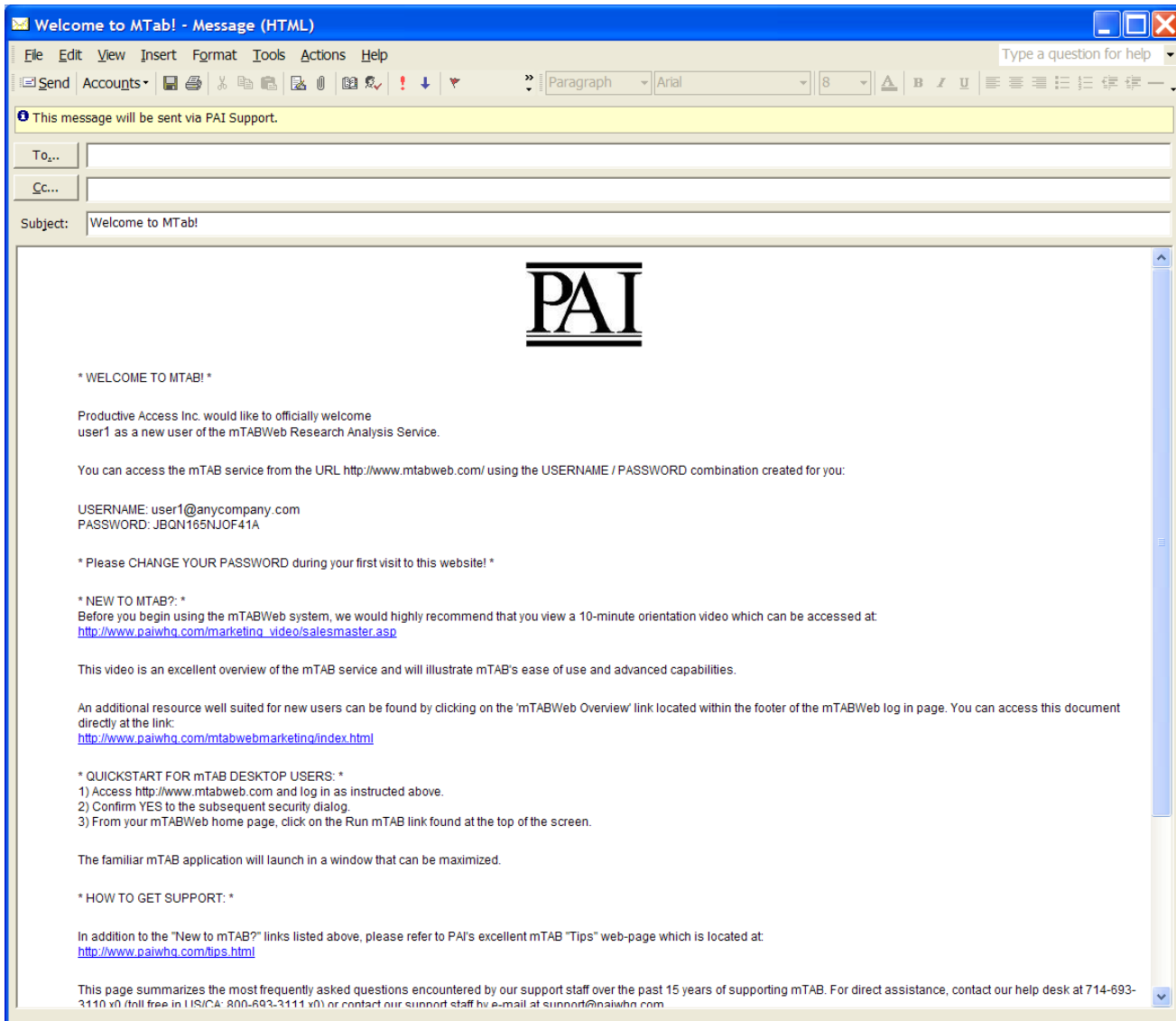
mTABWeb incorporates the e-mail address of the user as mTABWeb's "username" for login purposes. New users are issued an automated "Welcome to mTAB" e-mail after the creation of the user account. This email contains a temporary, randomly generated password and a web link that the user must access in order to set their personal password. This step is required before their first use of the mTABWeb software and it validates the user by confirming their receipt of email at their "username" account. In this manner, mTABWeb's security is linked to the client's security as a user's ability to receive e-mail is linked to the client policies (example: user unable to receive e-mail after termination, or only via a VPN connection).

Concurrent usage of a User Account

The mTABWeb software prohibits users from concurrently using the same account. If an incremental mTABWeb session is attempted with a username/password that is already in use, a message appears on the screen of the machine that initially logged in, indicating what has occurred. If you feel that your account is being abused or you have received this message in error, you should email your administrator for assistance.



“Welcome to mTAB” e-mail example



How to Maintain Groups

To add a group, select Group Admin from the Admin menu and you will be presented with the screen below.

The screenshot shows the 'Group Manager' section of the mTABWeb application. It includes a form for creating or editing a group with the following fields:

- Group Name: [Text Input]
- Group Webpage Name: [Text Input]
- Logo File (Max W: 120px x H: 90px): [Text Input] [Browse...]
- Max Users: [Dropdown Menu: 1]
- Disabled: [Checkbox]
- Restricted Ip Range Set 1-5: Each with Low and High IP address input fields.

Below the form is an 'INSERT' button and a 'Group List' table:

	Name	Max. Users	Members	Permissions	Last Updated	Disabled
[Edit]	All Users	1	[Edit]	[Edit]	9/27/2003 2:30:09 PM	N
[Edit]	Customer Demonstration	1	[Edit]	[Edit]	6/16/2006 5:04:59 PM	N
[Edit]	NML Demo	2	[Edit]	[Edit]	4/13/2005 2:06:50 PM	N

The only required field is the Group Name. This text will be visible to any user of the group in the Studies Menu folder structure in the mTABWeb application. The optional fields consist of:

- Group Webpage Name - This is the title displayed to the users of this group. In the screen above, it would appear in place of the "mTABWeb Demo" title. If this optional text is not provided, then the Group Name will be used as the title.
- Logo File - This is the larger logo on the left-hand side. Please note the maximum size should be Width:120px x Height:90px.
- Max Users - This sets the maximum number of users that can be assigned to this group.
- Disabled - This allows the administrator to prohibit all of the users, assigned to the group, from accessing mTABWeb without altogether deleting the users.
- Restricted IP Range Set 1-5 - This filter would preclude logging into mTABWeb from a machine that was not in the specified IP filter range. There are 5 total IP ranges available at the Group level. This allows the administrator to limit the ability of all users assigned to this group to access mTABWeb conveniently from a home office or other specific locations without explicitly connecting to their client network via VPN.

Client Specific Security

To delete a group, or change the options of a group, scroll down to the bottom of the Group Manager web page, and click the [edit] link preceding the group's name. The group information will be filled in and the New, Update and Delete buttons will appear.

To change the options of a group, click the appropriate item, make the change and then click on the Update button.

To delete a group, click on the Delete button. You will be prompted with a message asking if you are sure. Select Yes and this will remove the group from the Groups table.

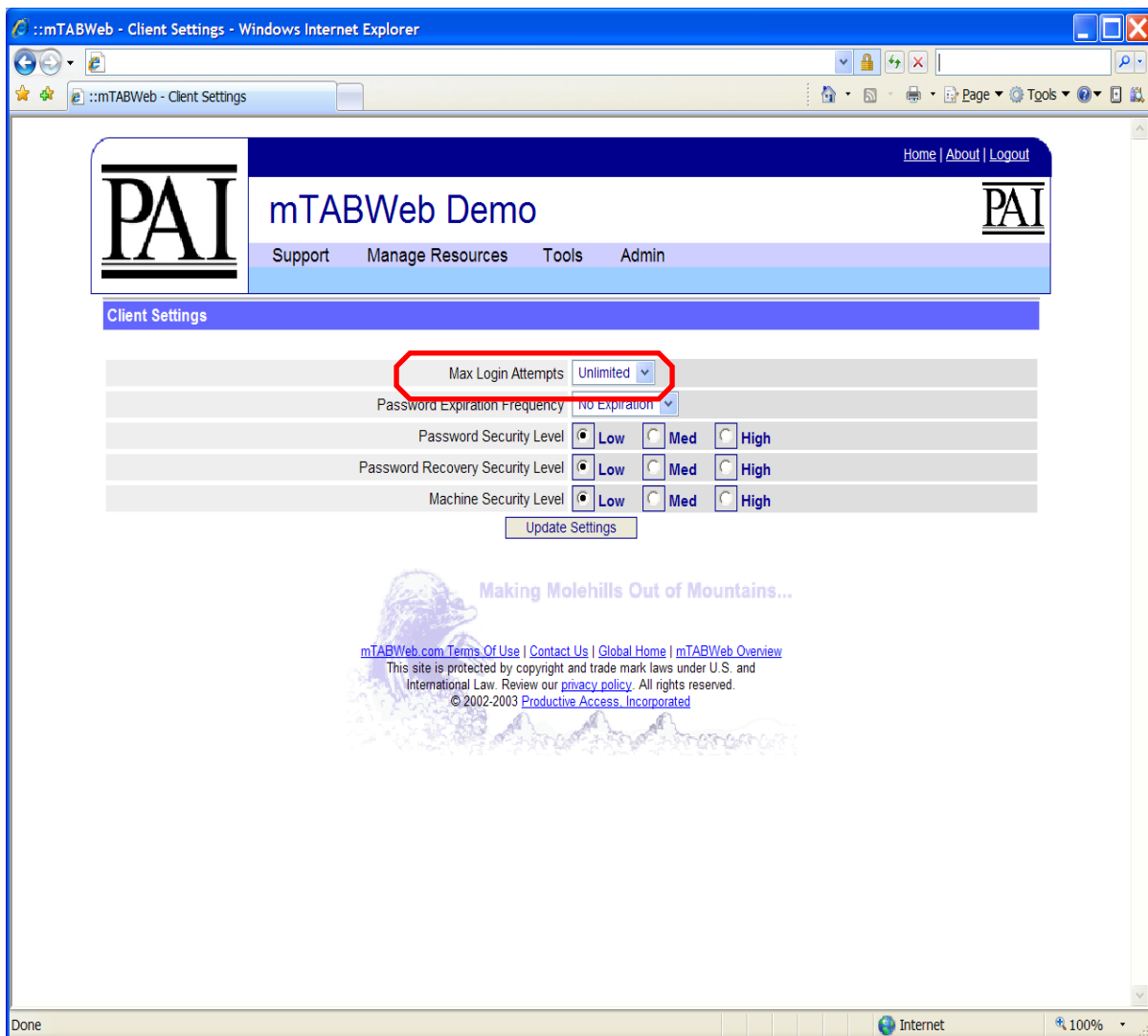
Client Specific Security Model enhancements

There are a number of security level options available that are configurable at the customer level. In this way, individual customers can decide on the relative tradeoffs between additional security vs. additional administrative burden and user performance penalties.

The customer specific configurable options are listed below, along with screen shots and considerations in terms of tradeoffs in performance and additional administration.

Maximum incorrect password attempts prior to "lock down"

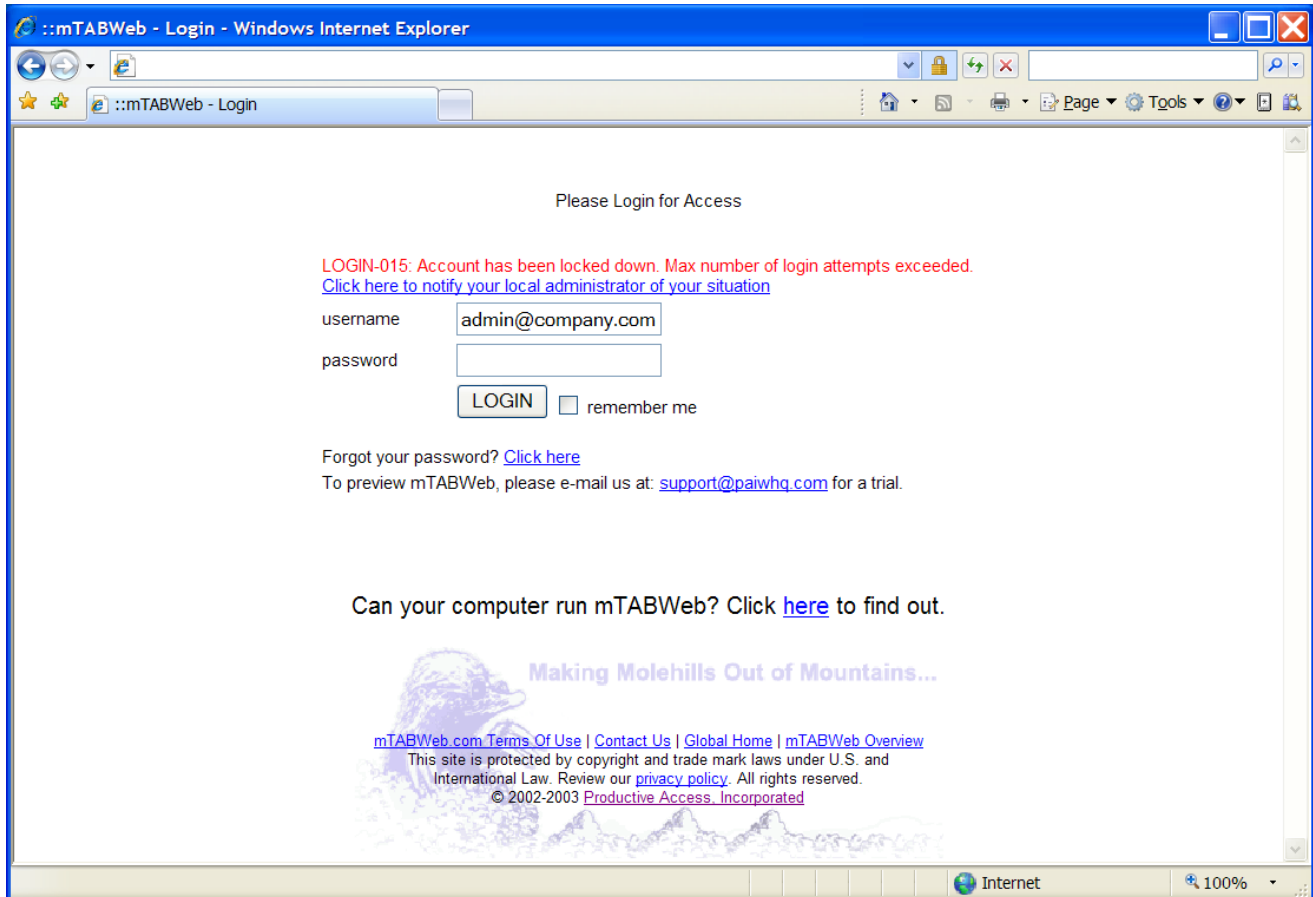
The client administrator can specify the number of username/password attempts that would be allowed by a user on an account prior to locking down the account. Please see red circled-option in screen shot below.



Client Specific Security

A "locked down" account must be re-enabled by the administrator. The user would receive a notice from the mTABWeb login page that the account was locked as a result of exceeding the allowable incorrect username/password attempts.

The error message contains a link that would allow the user to send an email to the administrator to re-enable the account. The administrator would re-enable the account via the provided web-interface, which would issue the "Welcome to mTAB" e-mail to the username e-mail address. The default password authentication setting is unlimited attempts.



Client specific password requirements

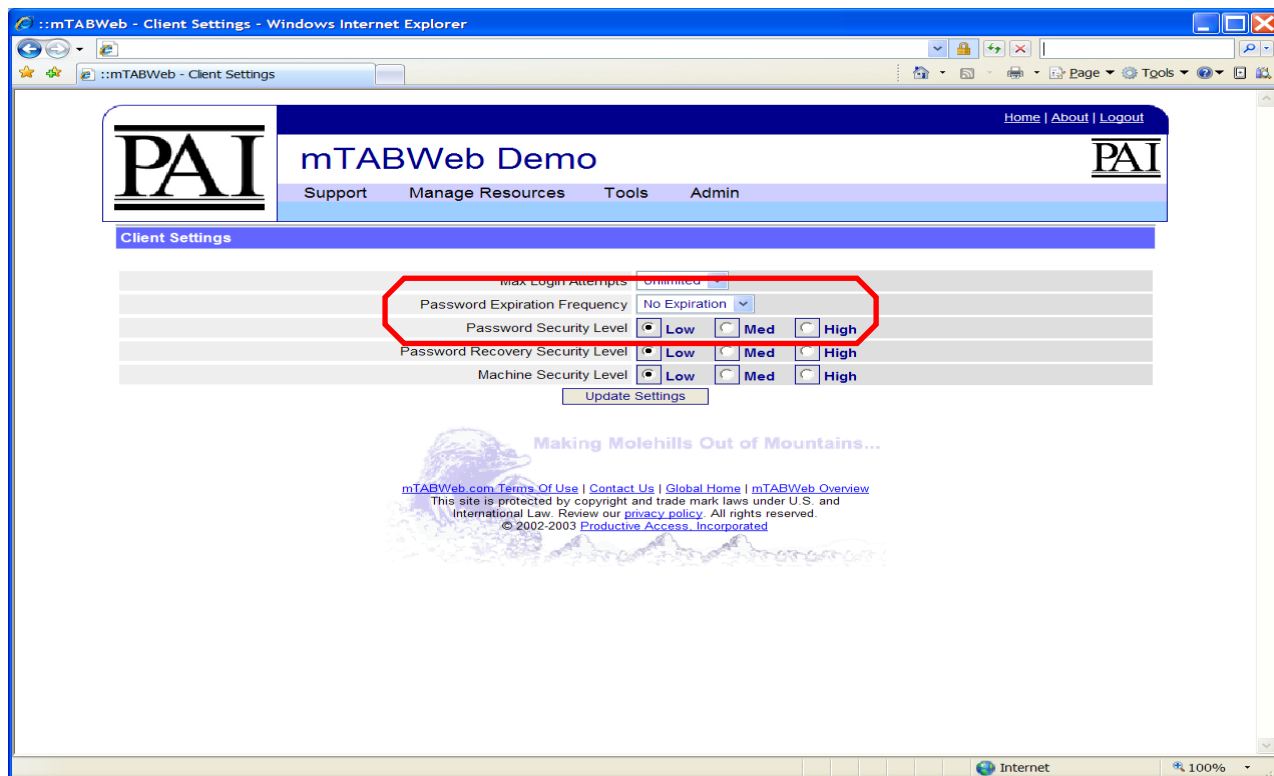
- a) Low - Any password other than no password.
- b) Medium – password must exceed 6 characters.
- c) High - password must exceed 6 characters and must include a combination of alpha and numerical characters.

Password Expiration Frequency

User passwords expire at a frequency determined by the client administrator. The administrator is sent an e-mail containing a web link that lists all client user accounts and their associated usage (tab runs). All accounts are considered “cancelled” in this e-mail and the administrator is required to re-enable each account by checkbox interface (“check all” option provided). The administrator receives up to three e-mail reminders if this process is not completed within 10 days.

Once the administrator completes the audit process, users are issued “Welcome to mTAB” e-mails requiring the users to re-establish their personal password prior to their next login. This step re-validates the user by confirming their receipt of email at their “username”.

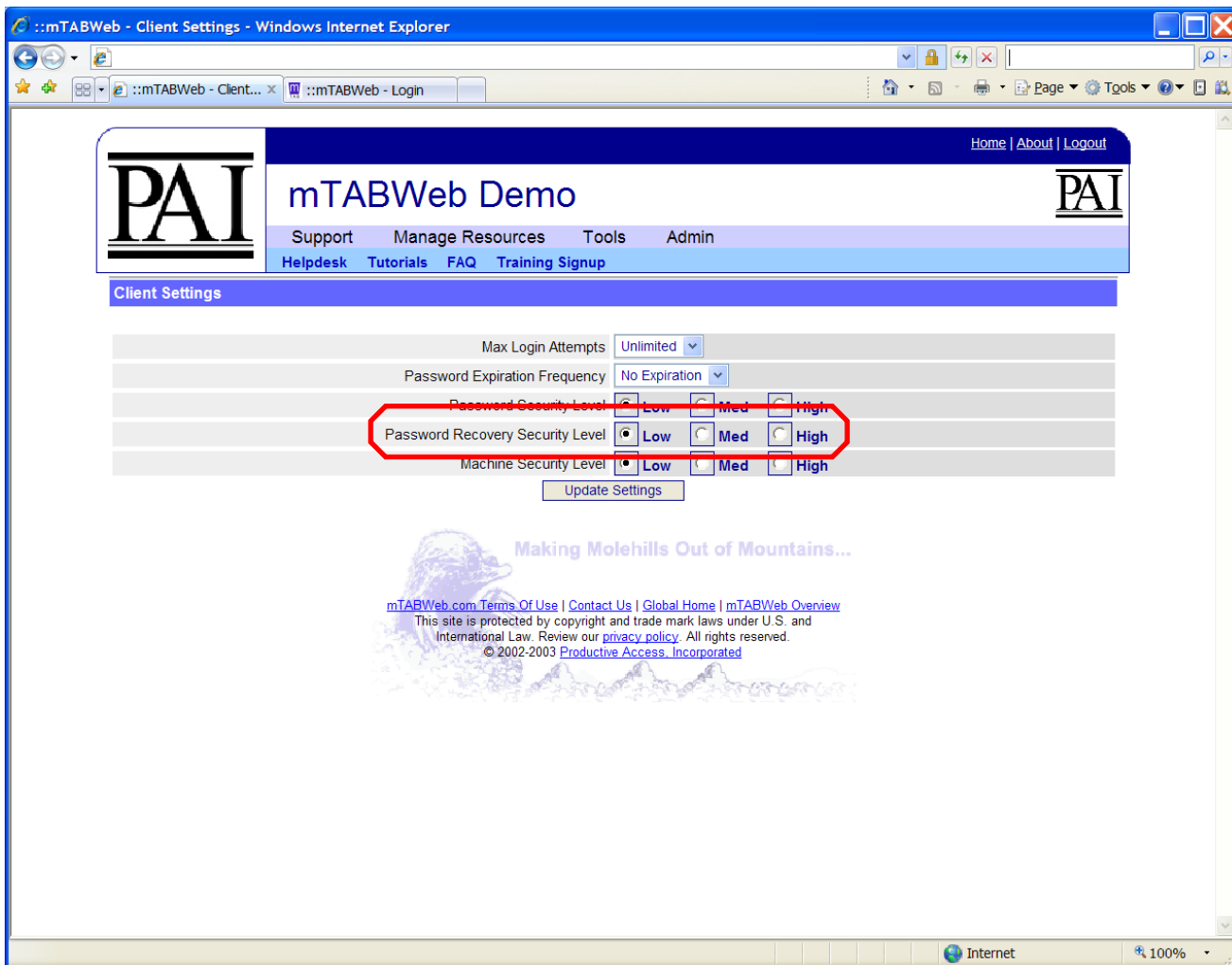
Tradeoffs: additional administrative burden and potential inconvenience for both the users and administrators.



Password Recovery Security Level

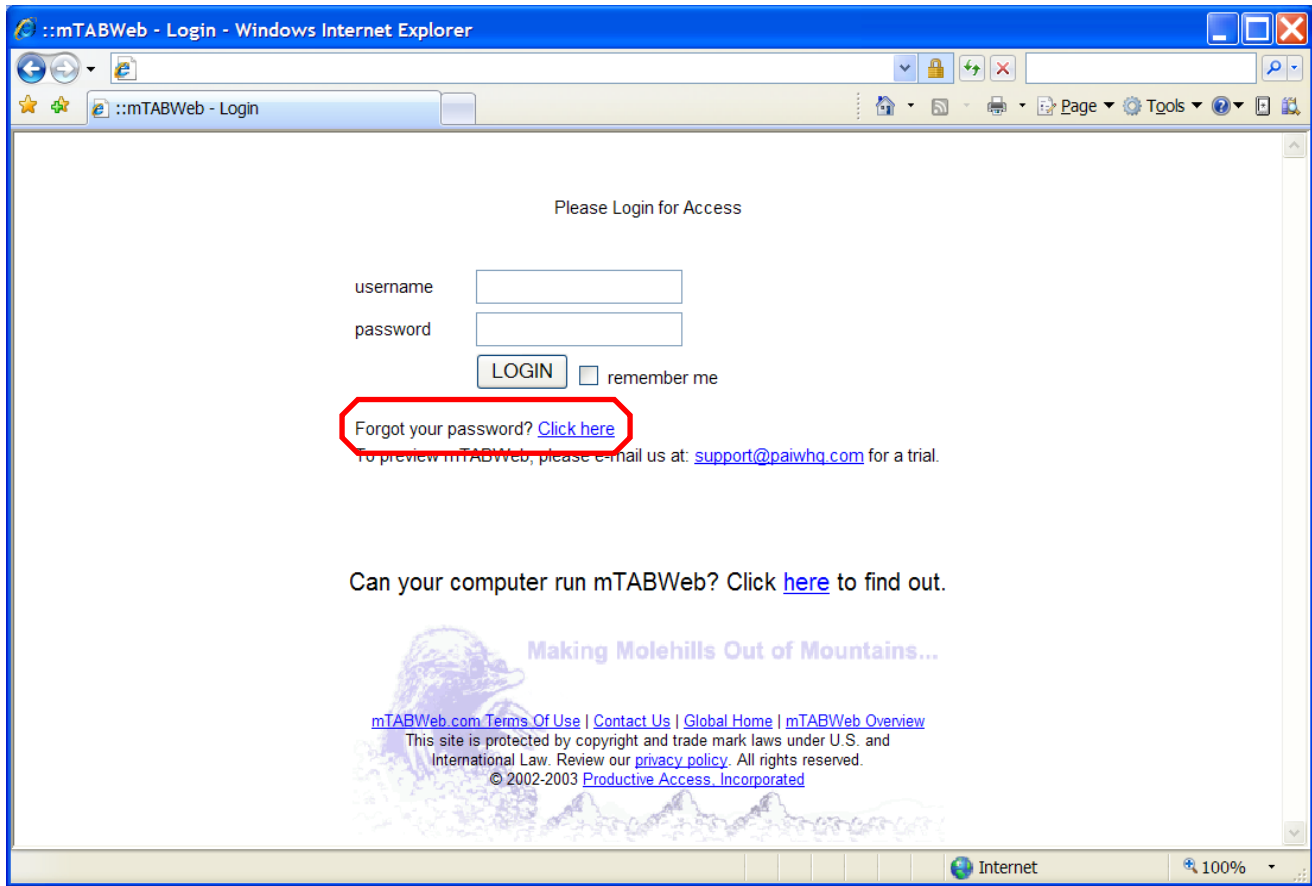
- a) Low - User can request password recovery by email and begin using the account immediately.
- b) Medium - User can request password recovery by email. User is forced to change password via the "Welcome to mTAB" e-mail process and the administrator is CC-ed.
- c) High - password recovery can come only from the administrator (i.e. user can not receive an automated recovery) and user is forced to change the password via the "Welcome to mTAB" e-mail process. User can optionally be prohibited from using the same personal password.

Tradeoffs: additional administrative burden and potential inconvenience for both the users and administrators.

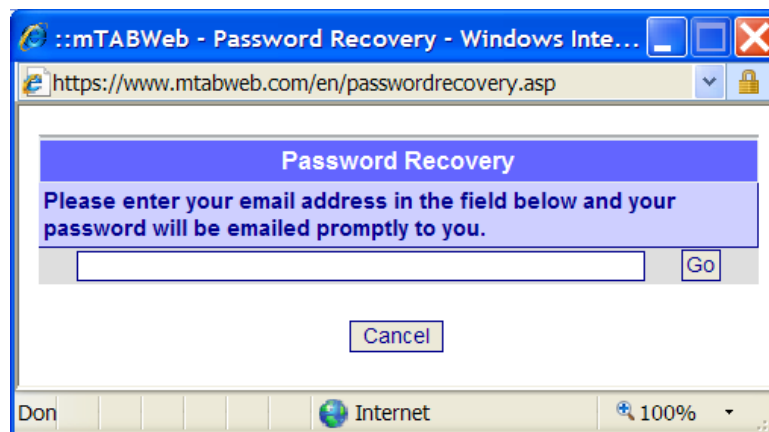


Client Specific Security

If a user cannot remember their password, they can click the red circled Click here link, in the screen shot below.



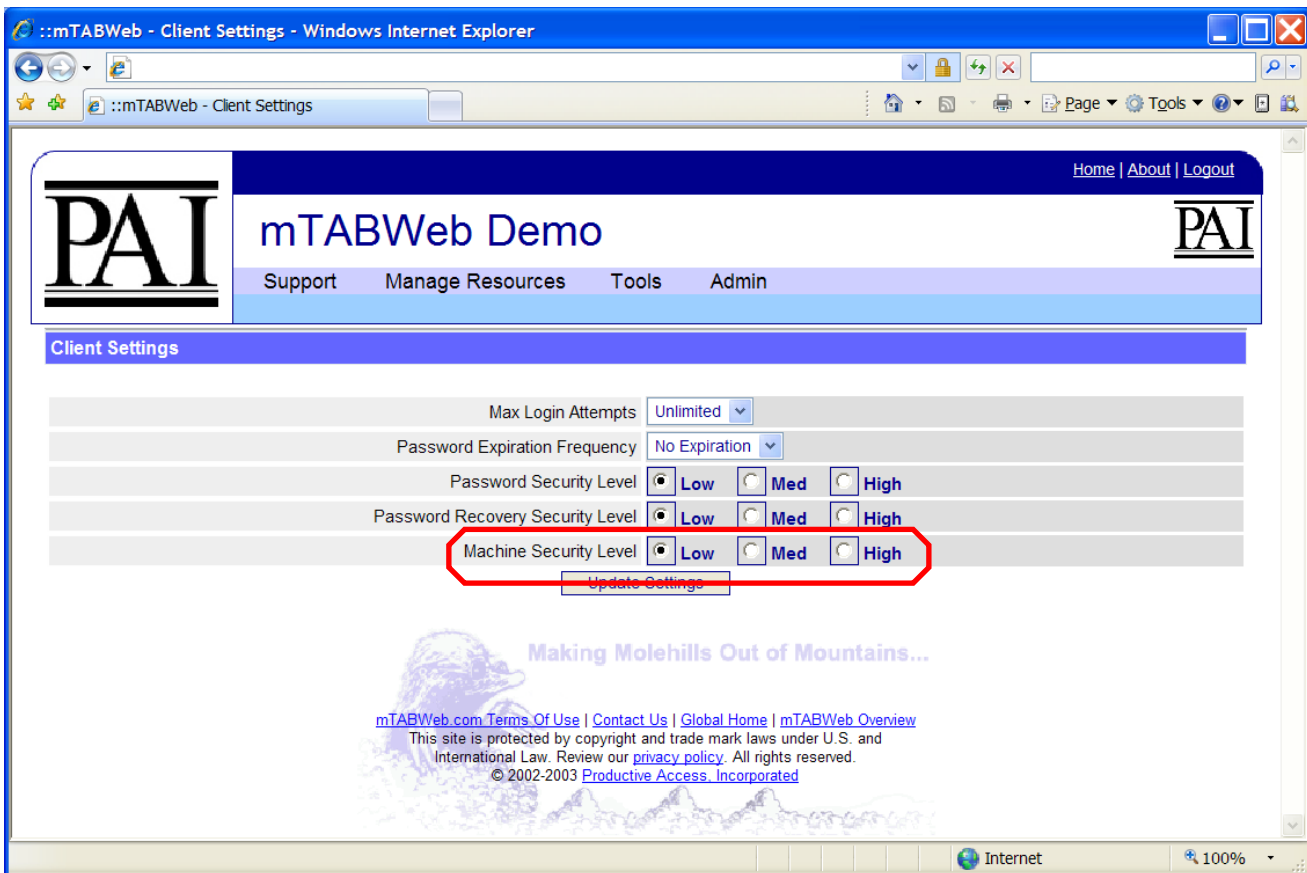
After selecting that link, a popup box will be presented. The user is required to fill in a valid email address.



Machine Specific security measure

- a) Low – none.
- b) Medium – cookie is written to the machine linking the user account to the machine. If the account is used on another machine, user will be required to receive an automated e-mail on that machine confirming authorization (i.e. "Welcome to mTAB" e-mail). Administrator is CC-ed on this email.
- c) High – cookie is written to user machine linking user account to that machine. If the user account is used on a new machine, the Administrator must specifically authorize this machine. (i.e. user cannot receive an automated authorization). A "Welcome to mTAB" e-mail will be generated by the administrator to the e-mail address of the user for subsequent authorization.

Tradeoffs: additional administrative burden and potential inconvenience for both the users and administrators.



Client Administration Documentation

This document has touched on a few areas regarding Client Administration. Please refer to the more detailed, step-by-step instructions on Client Administration for mTABWeb. Please click on the link below

www.paiwhq.com/docs/mTABWeb_Administration_Guide.pps