COMODO
Creating Trust Online®

Comodo Two Factor

Software Version 2.8

Administration Guide

Guide Version 2.8.071813

Comodo Group Inc.
1255 Broad Street
STE 100
Clifton, NJ 07013

Table of Contents

1.Introduction to Comodo Two Factor

Comodo Two Factor (ComodoTF) service is a two factor authentication solution for secure access to confidential services. An authentication factor is a piece of information and process used to authenticate or verify a person's identity or other entity requesting access under security constraints. Two-factor authentication is a system wherein two different factors are used in conjunction to authenticate.

1.1 Overview of Solution & Outline of Processes

Digital Client Certificates are an easy to deploy, affordable and effective PKI solution to enabling the enhanced user identification and access controls needed to protect sensitive online information. Client certificates are delivered electronically, and can be automatically installed on just about any computer or mobile device. They can also be stored and transported on smart cards or USB tokens for use when traveling. PKI client certificates are an essential element of Comodo's Two-Factor Authentication solution that provides strong user access authentication, protects the privacy of online data, and offers a transparent log-on method that won't inconvenience users.

Each certificate, in addition to traditional login credentials, establishes a user's unique identity to a remote server application – in this case the Comodo Two Factor proxy server. Each certificate can only be used to authenticate one particular user because only that user's computer has the corresponding and unique private key needed to complete the authentication process. Self-enrollment for and installation of a client certificate onto an end users' machine requires no expertise and will not inconvenience users like other two factor solutions that rely upon expensive physical devices.

A PKI based client certificate assures an enterprise that the person logging into a secure service is indeed one of their users by validating not only their User ID and Password, but their certificate as well. This type of solution can only be delivered by a Certification Authority such as Comodo because only a Certification Authority has the experience, expertise and security infrastructure to manage the full life-cycle of public digital certificates - including issuance, renewal and revocation.

The remainder of this section includes a brief overview of the authentication methodologies that are implemented by the Comodo TF solution in order to provision true, Two Factor Authentication of end users, namely:

- **First Factor Authentication - Existing User Credentials**
- **Second Factor Authentication - Digital Client Certificates**
- **Auxiliary, Out of Band, Second Factor Authentication**

1.1.1 First Factor Authentication - Existing User Credentials

The first factor includes:

- The login page hosted on the Two Factor Server is an exact copy of the enterprise's existing login page (This makes the Two Factor Server transparent to the end user).
- Once the account holder enters their username and password, the Two Factor Server hands the request off via a secure SSL connection to the enterprise's server.
- The enterprise server then processes the login request and responds to the Two Factor proxy server.

Note: The Two Factor server does not keep a record of any user details such as passwords or account information - nor does it require such information in order to deploy the Two Factor Client Certificates to the end user. The Comodo Two Factor Server will only proceed to the provisioning and/or authentication of the client certificate after the enterprise's web server has validated the account holders username and password.

1.1.2 Second Factor Authentication - Digital Client Certificates

The provisioning of an X.509 client certificate onto the end users machine. This certificate, once installed into the certificate store of the user's Internet browser (e.g. Internet Explorer, FireFox, Opera) will be requested and verified every time the user logs into the Two Factor server and will authenticate them as the genuine account holder. The presence of this certificate on the end users machine is needed to complete the authentication process. This means that even if a hacker obtained an account holders username and password, they would still be denied access to the account because the Two Factor server would not detect the client certificate on the machine the hacker is connecting from.

1.1.3 Auxiliary, Out of Band, Second Factor Authentication

In order to validate themselves to the Two Factor servers, a user must connect from a machine that they have installed a certificate on. If this is not the case, and no certificate is detected, then the primary Two-Factor process cannot be completed. Example scenarios include:

1. The user chose not to install an authentication certificate during the New User Enrollment Process. In this instance, the user will have to go through the activation procedure every time they log on or until such time as they decide to install a certificate.
2. The user is attempting to access his account from a different machine to the one they installed the certificate on. For example, they are using their work computer or laptop for the first time to access their account but installed the certificate on their home PC; they are trying to access from a 'public' computer such as those in Internet cafes or libraries; they are trying to access from a mobile device for the first time; they are trying to access from a recently purchased computer.

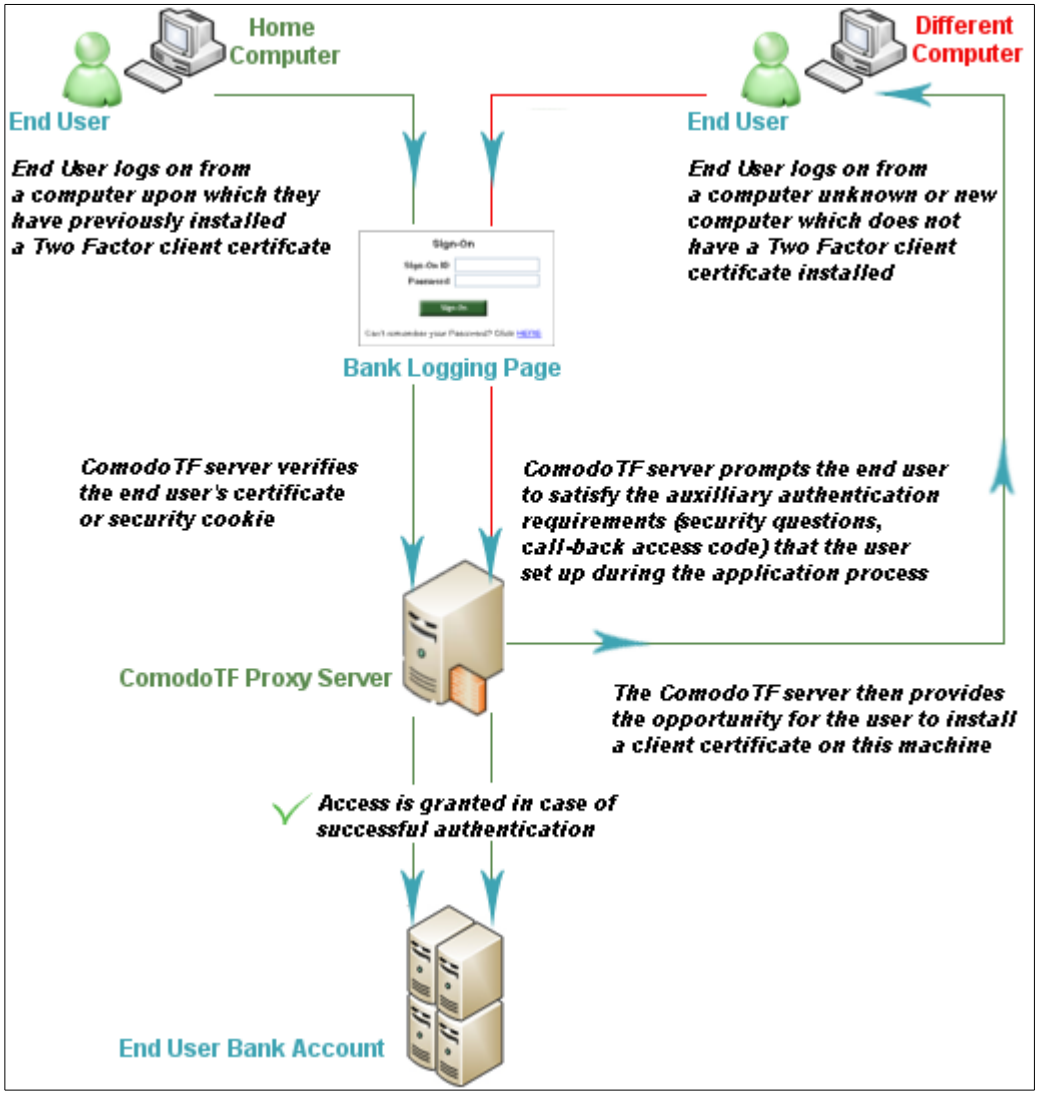
To ensure the highest levels of validation are used at all times, Comodo Two Factor also incorporates an out-of-band second factor authentication process via telephone or SMS.

During enrollment the user is required to supply a minimum of one and a maximum of four contact telephone numbers. They are also required to enter a contact email address. In the event that a certificate is not detected on the user's machine during a subsequent connection attempt, then user will be presented with a pre-populated list of these contact details and asked to choose one. The Two Factor server will then send a randomly generated, one-time activation password to the chosen location. (If they selected a telephone number, they will receive an automated voice message. They also have the option to receive the password as an SMS text message or email). The Administrator can view the one time activation password generated for the user and how the password was sent to the user from the Admin Console. For more details see the section **View Activation Code Sent to the User**.

The user must then enter this activation password at the website. If it is verified as correct by the Two Factor server, then the user is allowed to connect to their account. They are also provided with the opportunity to install a client certificate on the machine they are currently attempting to connect from. For computers and devices that the user wishes to be trusted (computers they own or use at work) then a certificate should be installed. For computers that the user does not wish to be trusted (computers in public places such as Internet cafes or computers they do not plan to use regularly), then the user should use the activation password mechanism.

The diagram below shows a basic outline of the authentication process that an *existing* Comodo Two Factor end user will experience when they:

- Log onto to the secure service from a computer which already has a client certificate installed.
- Log onto the secure service from an unknown or new computer which does not yet have a client certificate installed.



1.2 Comodo Two Factor Authentication Benefits

1. Highly flexible and configurable proxy-based authentication solution that can be virtually deployed in hours.
2. Seamless front-end for most user-access web pages, as well as for Microsoft Outlook Web Access and SharePoint.
3. Leverages Comodo's Public Key Certificate Authority Infrastructure. PKI is widely recognized as supplying the strongest form of authentication and encryption service available.
4. Low cost – automates the digital certificate issuance and management keeping administrative overhead to a minimum. No modification to existing applications.
5. Easy to Use – simple client account setup conveniently allows continued use of existing user-names and passwords. Certificates are automatically installed.

1.3 Guide Structure

This guide is intended to take you through the step-by-step process of organization, configuration and use of Comodo Two Factor service.

- Section 1, **Introduction to Comodo Two Factor** is a high level overview of the solution and serves as an introduction to the main themes and concepts that are discussed in more detail later in the guide.
- Section 2, **The 'User' tab** covers the creation and management of End Users.

- Section 3, **The 'Admin' tab** covers the creation and management of Administrators and Operators.
- Section 4, **The 'Settings' tab** contains information on how to change ComodoTF access password and clear History Records.
- Section 5, **The 'Roles' Tab** contains explanations on creating and editing new roles that can be assigned to Administrators and Operators.
- Section 6, **The 'Blacklist' tab** contains information on how to deny access requests that come from IP addresses from specific countries.
- Section 7, **The 'Reports' tab** contains an overview of the area, descriptions of each report type and guidance on how to access the required report type.
- Section 8, **The 'License' tab** explains the process for viewing and changing of the license.
- Section 9, **Logging out of Comodo Two Factor** explains the process for logging out.
- Section 10, **FAQ** contains FAQ that cover certain aspects of the service.
- Section 11, **About Comodo** contains company and contact information.

1.3.1 Definition of Terms

Access, management and executional privileges in Comodo Two Factor are spread across three default classes of user – Administrator, Operator and User. Administrators and Operators are types of 'Role' - each with a distinct set of pre-configured permissions and capabilities (see **1.5.4.Roles** for more details). The default privileges available to each of these role types is outlined in the following table and the table in **section 1.3.2.**

Definition of Terms	
Role Type	**Definition**
Administrator	Administrators are the top level administrator and can access all areas and functionality of the ComodoTF administrative console. • Administrators have full visibility and control over Client Certificates of users • Administrators are listed in and can be managed and created from the 'Admin' area of the ComodoTF administrative console. Furthermore, only Administrators are allowed access to the 'Admin' area • New Administrators can only be created and managed by an existing Administrator • Administrators are able to create and manage 'Administrators', 'Operators' and can manage all Users • Administrators can change the product license
Operator	Operators have privileges to access administrative console, monitor and manage users activity. • Operators have full visibility and control over Client Certificates of users • Operators have no access to 'Admin' area of the interface • Operators cannot create other Operators or Administrators • Operators cannot change product license • Operators cannot clear History Records
User	A 'User' is a person that has authenticated themselves to the Two Factor interface by logging into their secure web service account and, in doing so, have requested or been provisioned with an authentication certificate or secure cookie.

Definition of Terms	
	• 'Users' have no access rights whatsoever to the administrative console of Comodo TF. They exist in Comodo TF as a function of their request/ownership of a second factor authentication credential such as security cookie or digital certificate • A new End-User can be created in Comodo Two Factor: a) via **Manual creation by an Administrator or an Operator in the 'User' tab** b) Automatically via Self-enrollment procedure (when logging to the secure website / service account e.g. his/her bank account for the first time) • All Users are listed in the 'User' tab of ComodoTF interface

1.3.2 Administrator's and Operator's Roles – Comparative Table

Note: The table below lists the default permissions for the Role types of 'Administrator' and 'Operator'. These are the default Roles that ship with Comodo Two Factor and their configuration of permissions cannot be modified. If an administrator with a different permutation of permissions is required then you must create a new Role type (click the 'Add Role' button in the 'Roles' area). Once created, the new Role type can be assigned to users as required.

Roles - Comparison of Default Permissions			
Actions	**Definition**	**Role = Administrator**	**Role = Operator**
Manage Administrators	View, Add, Edit, Change Password	✓	✓
Manage Operators	View, Add, Edit, Change Password	✓	✗
Manage Users	Multiple view and Action settings. See **The Roles tab** for full list.	✓	✓
View Reports	All type of reports available	✓	✓
View License	View	✓	✓
Update License	Update	✓	✗
View Roles	Add, Edit Delete	✓	✗
Applications	View, Edit	✓	✗
Manage Users' Certs	Add, Delete, Edit	✓	✓

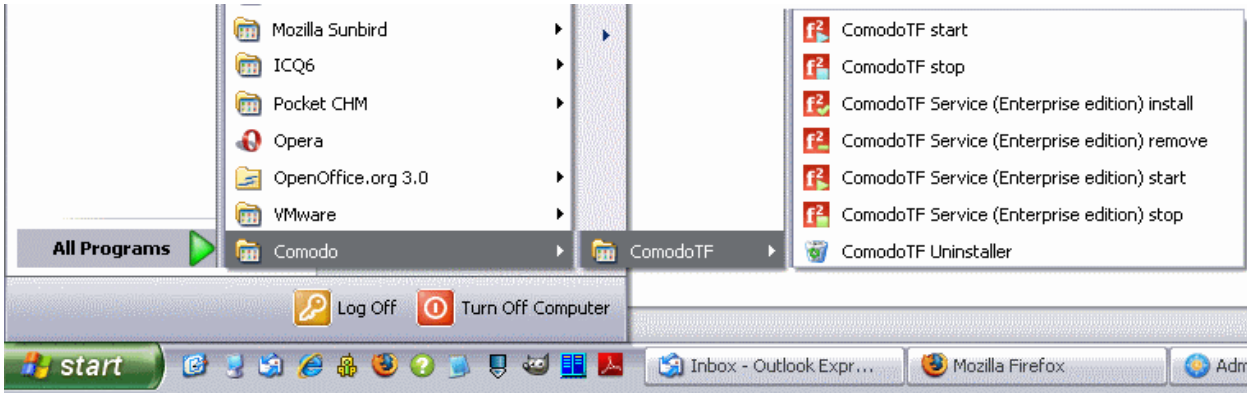
Roles - Comparison of Default Permissions			
Change Settings	Change Password	✓	✗
	Clear History Records	✓	✗
Restricted Countries	View, Change	✓	✓

1.4 Logging into Comodo Two Factor Admin Interface

To access Comodo Two Factor (ComodoTF)

For Windows users click:

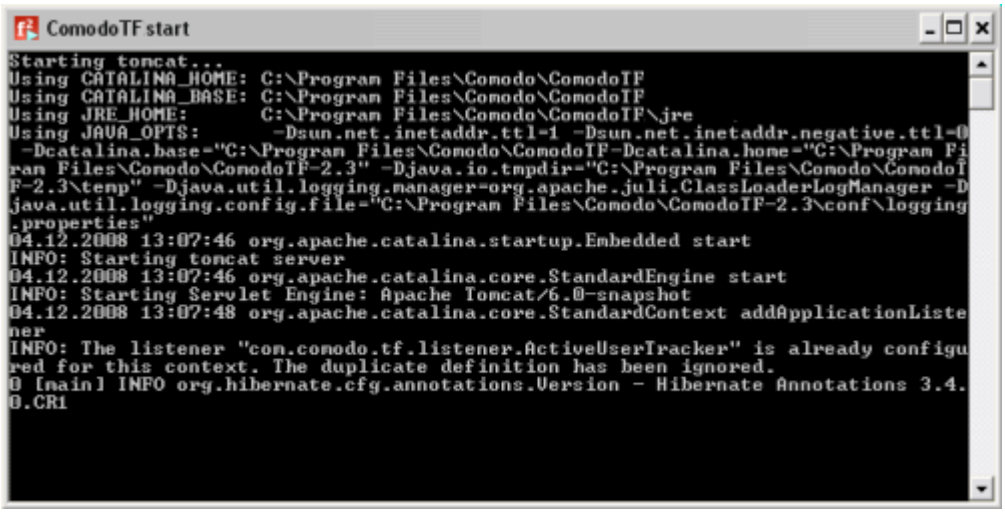
- **Start > All Programs > Comodo > ComodoTF > ComodoTF start.**



For Unix users:

go
cd ComodoTF-xx/bin
execute $ ./startup.sh

This will launch ComodoTF application:



Alternatively, once your account has been setup, your account manager will provide the login URL for the Comodo Two Factor interface. By default, the format of this URL is: https://YOURSERVER/comodotf/. Enter your login and password, and click the 'Login' button.

If you have not been supplied with your login details, please contact your account manager.

After logging in, the password for your administrators account can be changed at any time via the '**Settings**' tab.

1.5 The Main Interface – Summary of Areas

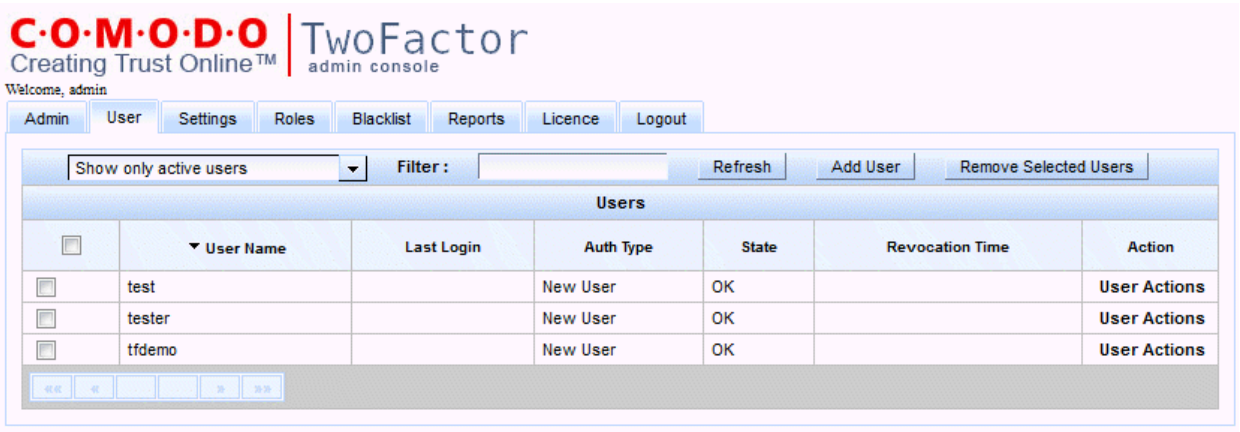
Comodo Two Factor interface has a tab structure that facilitates access to all major settings.

- There are (a maximum of) nine tabs that cover each of the main functional areas of the solution. These are '**Admin**', '**User**', '**Settings**', '**Roles**', '**Blacklist**', '**Reports**', '**License**' and '**Logout**'.
- The remainder of this introductory section contains a brief introduction to each tabbed area. Full details of the actual usage and functionality of the tabbed areas listed above are in sections 'The User tab', 'The Admin tab', Settings, Roles, Blacklist, License and Reports.

Tip: Pointing the mouse cursor over the main console elements will show helpful tool tips which contain a short explanation of the element's functionality.

1.5.1 User

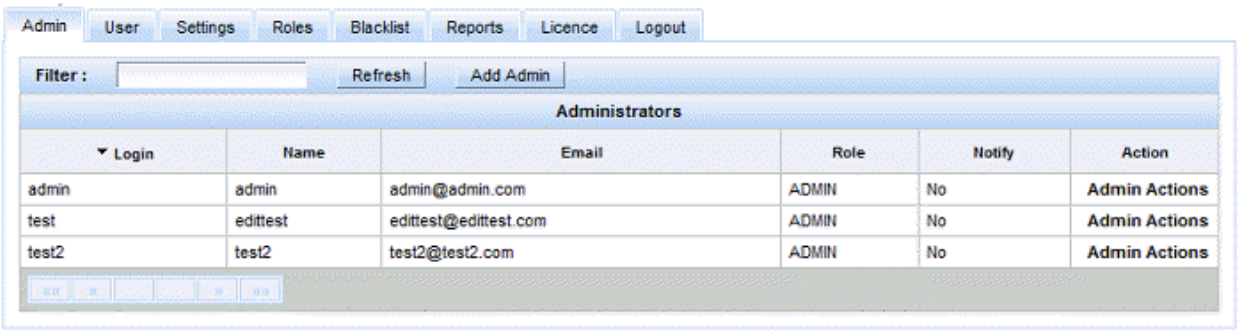
List of ComodoTF service end-users. Allows appropriately privileged personnel to add new users and edit existing users.



Click here for more information about the 'User' section.

1.5.2 Admin

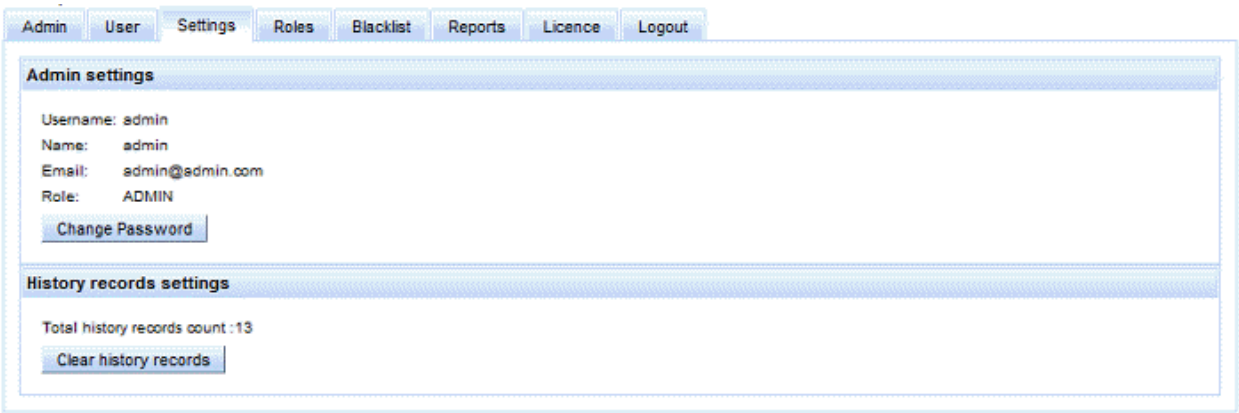
Displays a list of personnel with administrative roles, including 'Administrators', 'Operators' and custom roles that have been created using the **'Roles'** area. This area also facilitates the addition, editing and removal of administrators/operators/personnel with custom roles.



Click here for more information about 'Admin' section.

1.5.3 Settings

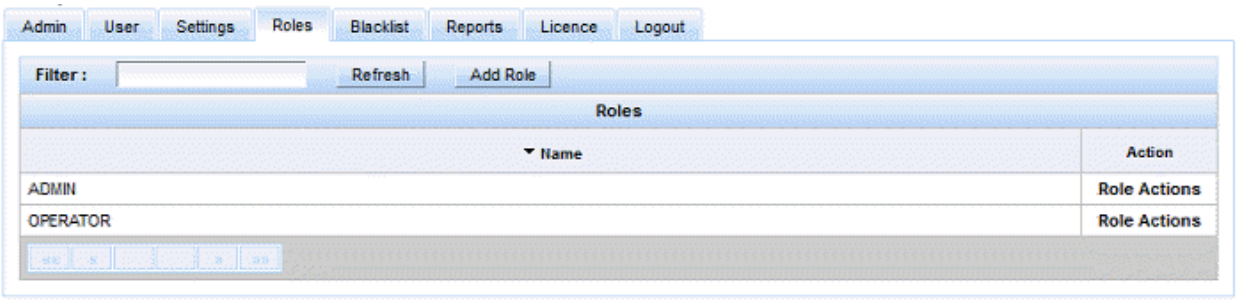
Allows the person that is currently logged in to modify their password and clear history records.



Click here for more information about the 'Settings' area.

1.5.4 Roles

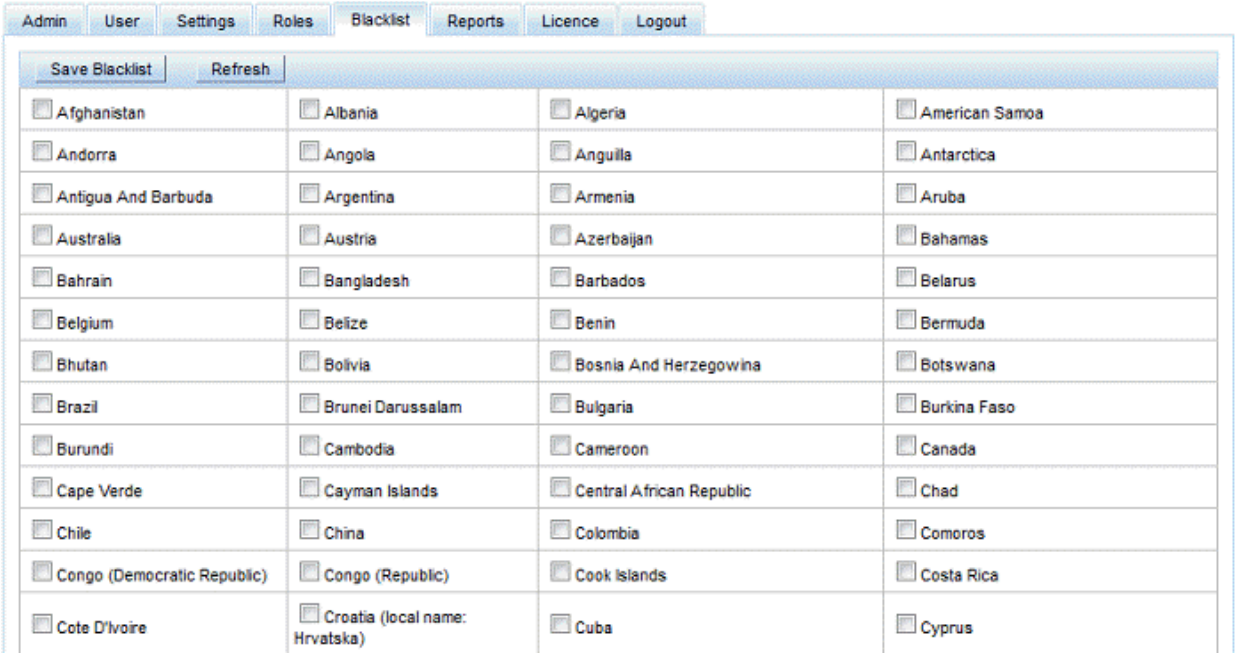
Allows the administrator to create new roles and edit permissions for the created roles.



Click here for more information about the 'Roles' area.

1.5.5 Blacklist

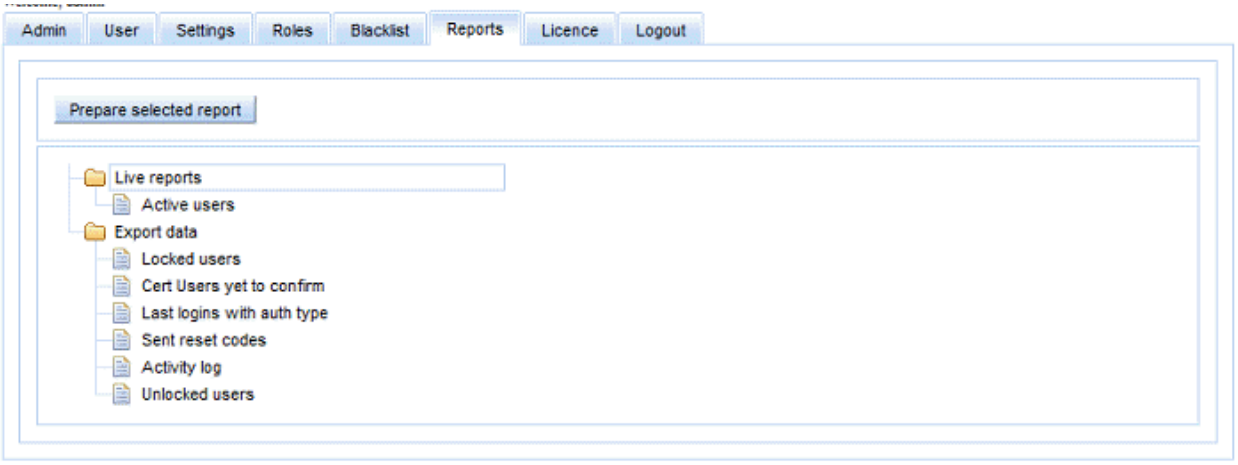
Provides full management of ComodoTF service administrators.



Click here for more information about the 'Blacklist' area.

1.5.6 Reports

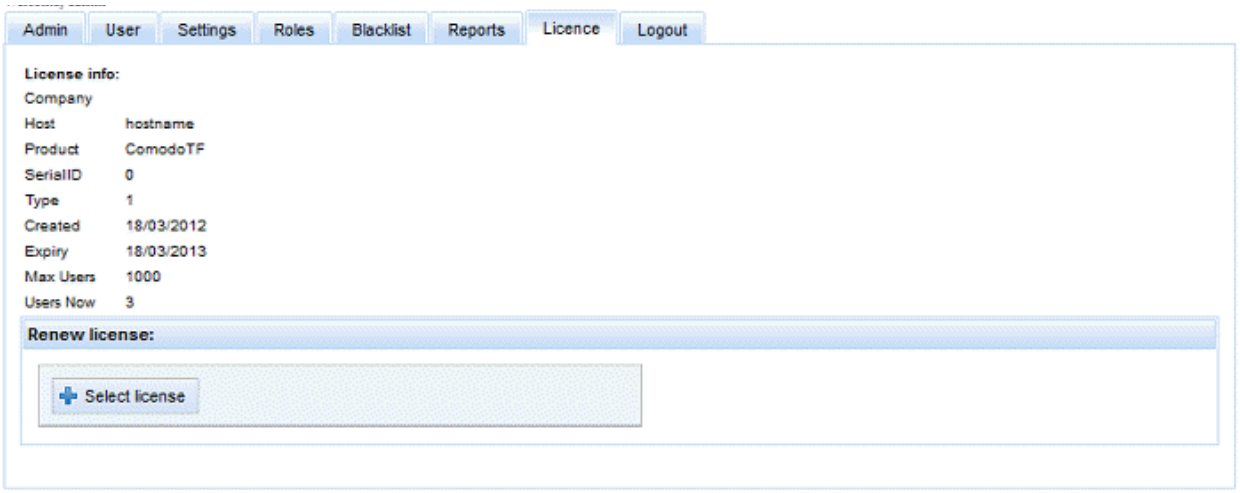
Enables the administrator to create various activity and user related reports.



Click here for more information about 'Reports' section.

1.5.7 License

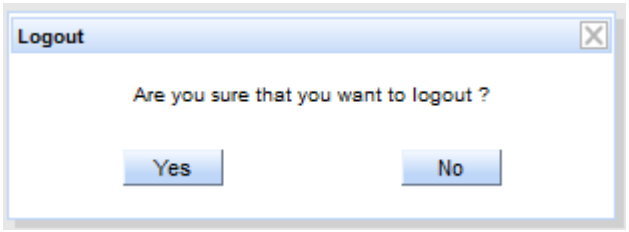
Displays the current license information and enables the Administrator to renew the license upon expiry.



Click here for more information about 'License' section.

1.5.8 Logout

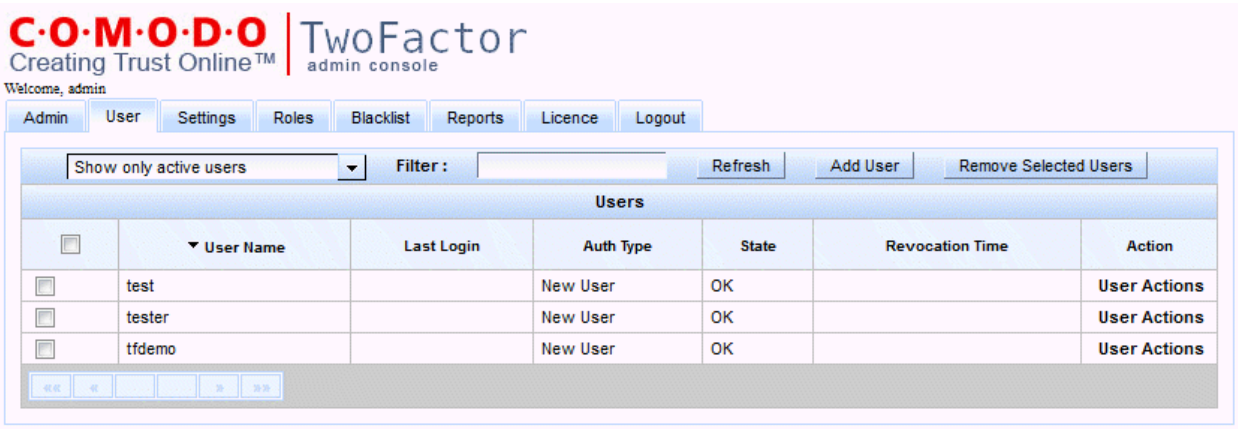
Logs the current user out of the ComodoTF service.



2 The 'Users' Tab

2.1 Overview

Once you login, you will see the list of users (if any), that were already authenticated via Comodo Two Factor.



2.1.1 'User' – Table of Parameters

User – Table of Parameters		
Field Name	**Value**	**Description**
User name	User name	User name as entered in login box.
Last Login	Date, or blank	Date of the last login, or blank if user never logged in.
Auth Type	New User	User is new, and no security questions/answers, nor certificate installations were done for this user.
	Question Challenge	User authenticates with security question.
	Callback	User authenticates with callback.
	Cert Installed	The user entered questions/answers challenge and installed a client certificate at least once. This shows that the user tried to install certificate someday, but user still can reject certificate during installation process, delete it or login from the other browser without certificate via security questions or callback.
	No Auth	User doesn't need to provide certificate, or to answer security question. He will be logged into the system right after entering correct login/password.
	Cookie	User can install secure cookie and authenticate with it.
State	OK	User can access the site.
	LOCKED	User locked and will not be able to access the site.

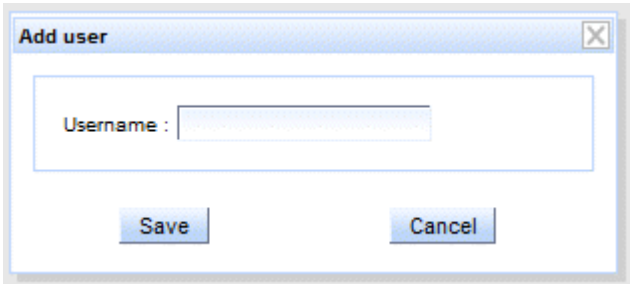
User – Table of Parameters		
	LOCKED DUE TO WRONG ANSWER	User is locked because the wrong answer was entered.
	RESET	User's questions were reset, and reset code was generated, but wasn't entered.
Revocation Time	Date, or blank	Date and time when the certificate was revoked. All certificates issued prior to that date will not work.
Action	Control	Enables administrator manage that user settings.
Add User	Control	Enables administrator to add a new user.
Refresh	Control	Updates the list of displayed users to reflect changes such as newly added user; changes in state or authentication type, etc.

2.2 User Management

The 'User' area provides administrators with the ability to create new users, grant or deny access to ComodoTF end-user interface.

2.2.1 Adding a New User

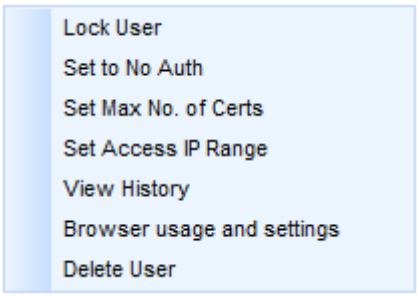
1. Switch to the 'User ' tab;
2. Click the ‘Add’ button to open the ‘Add User’ form.
3. Enter a new user name.



4. Click 'Save' to add the end-user to the ComodoTF.

2.2.2 User Actions

Point the mouse cursor over the 'User Actions' control alongside the end-user's name to view 'actions' menu:

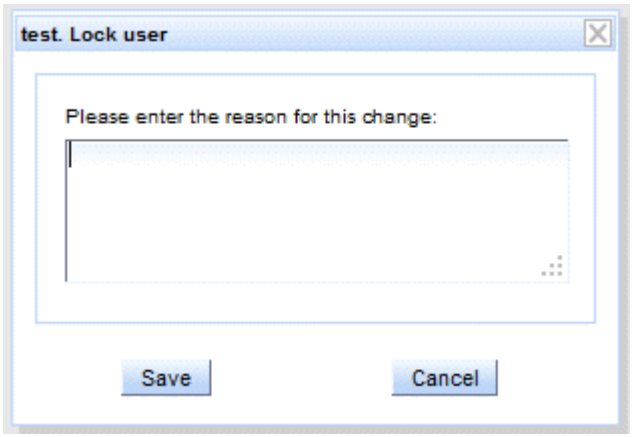


Note: The options in the Actions dialog depend on the permissions defined in the Role, assigned to the Administrator/Operator currently logged-in. For a full list of default permissions granted to Administrators and Operators, see **Administrator's and Operator's Roles – Comparative Table** and for more details on Roles and creating a new role, see **The Roles tab**.

Action Dialog – Table of Parameters	
Action	**Description**
Lock User	Enables administrator to lock the user account, preventing user from logging in.
Unlock User	Enables administrator to unlock a previously locked user account, enabling user to log - in.
Set to No Auth	Enables administrator to set the user state to **No Auth** (available only if state is not **No Auth**). A user can log in entering only login/password and don't use certificate or cookies, do not answer on security questions and not to enter an activation code if he need it before. User's Auth Type becomes 'No Auth'. To enable this action in rules.xml should be entered: challenge type="NO_AUTH" **Note**: Setting a User to No Authorization state completely resets the user. The user will be treated as new user and all the credentials like security questions and answers are to be reset on re-authorizing the user.
Set to 'Auth'	Enables administrator to set normal authentication for the user. User state will be set as **New User.** (available only if state is **No Auth)**
Reset User	Sets user state to 'New User' clearing out existing security questions, answers or phone numbers, cookies and email addresses. (in case if FULL_RESET is enabled in user's configuration). Otherwise, admin needs to select options for user to change during next login into the secure website.
Set Max. No of Certs	Sets certificates' quantity available for the user. Possible values: default, unlimited, custom. **Click here for more information**.
Set Access IP Range	Enables the administrator to manage IP ranges for user. **Click here for more information**.
Language	Enables the administrator to set the interface language for the user. **Click here for more information**
View History	Enables administrator to view the list of events that occurred to the user.

Action Dialog – Table of Parameters	
Browser Usage and settings	Enables administrator to view the list of browsers (locations) through which the user has logged-in to the secure website. If required, the administrator can also change the authentication modes (Client Certificate/Security Cookie/Callback(or questions)) for every registered browser used by the user. **Click here for more information**.
Revoke Certificates	Enables administrator to revoke all certificates issued before current time. (available only if a digital certificate is installed). To enable possibility to install certs for users rules.xml should contain: challenge type="CLIENT_CERT" (should be above 'COOKIE' challenge type)
Delete User	Enables the administrator to delete the selected user and revoke that user's client certificate or security cookie. Although all user data will remain in the database, Comodo Two Factor will treat this user as though they were a NEW user upon subsequent attempts to log in to the secure service (banking website etc). Upon deletion: • Any authentication cookies associated with this user will be invalidated. • Any client certificates issued to the user will be revoked • The next time this user attempts to login they will need to go through the initial set up process again and enter their email address, set up their call back data / security questions and be offered the opportunity to obtain a new client certificate or security cookie.

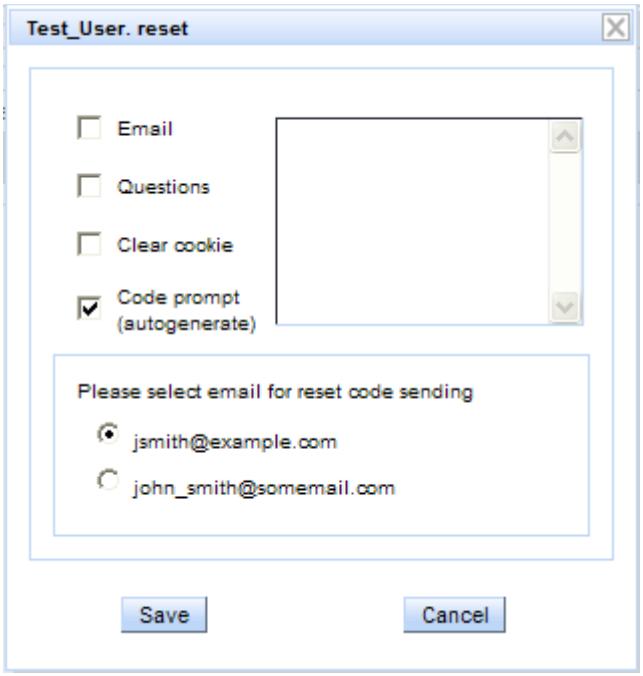
For all options listed above (except **Reset User**, **'Max Set Max. No of Certs'**, **'Set Access IP Range'**, **'View History'**, View History, Browsing usage and settings, delete User and **'Locations'**) the following dialog appears:



This enables administrator to comment the action. The descriptions of the exceptions' dialogs follow below.

2.2.2.1 Reset User

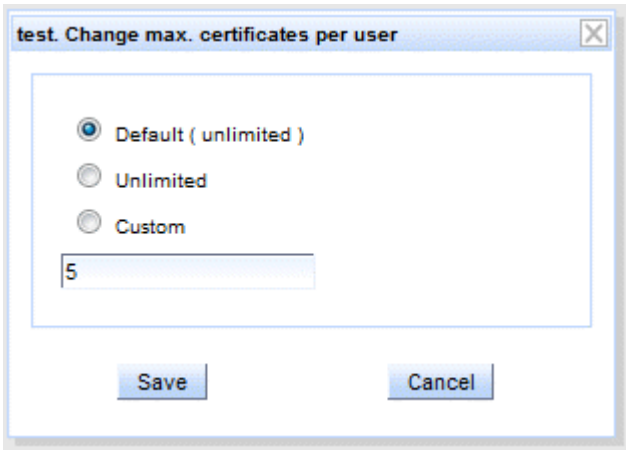
The 'Reset User' option enables administrators to manually reset all or some of the user's security settings.



Reset User – Table of Parameters	
Reset Type	**Description**
Email	Resets user's email. User will have to set email at next login once more.
Questions	Resets user's security questions / answers. User will have to set them at next login once more.
Clear cookie	Resets user's security cookie. User will have to get it at next login once more.
Code prompt (autogenerate)	Sends one-time password (reset code / activation code) to user.
Callback	Resets user's callback settings. User will have to set them at next login once more.
Select email	Visible only if 'Code prompt' is checked. Enables administrator to send automatically generated one-time access password to the user's email address.

2.2.2.2 Set Max No. of Certs

'Set Max. no of certs' enables the administrator to assign the number of certificates that can be allotted to the user.



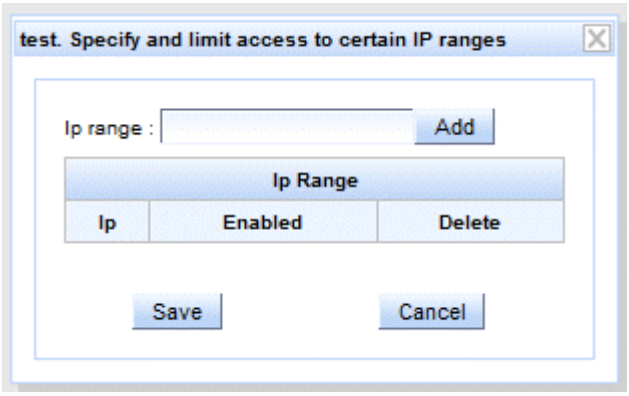
Select any one of the following options by selecting the corresponding radio button: Default, Unlimited or Custom and enter the number that denotes the number of certificates for the selected option.

2.2.2.3 Set Access IP Range

'Set Access IP range' enables the administrator to manage IP ranges for user. Depending on the configuration of Comodo Two Factor service administrator can set the followings types of authentication:

- By default, if users come from known IP addresses (specified in the IP range) – access is granted without any security checks. If users come from unknown IP addresses (not specified in the IP range) – users must identify themselves via their designated authentication procedure (Security Questions or Call Back);
- If users come from known IP addresses (specified in the IP range) – access is granted without any security checks. If users come from unknown IP addresses (not specified in the IP range) – access denied and no security checks take place.
- If users come from known IP addresses (specified in the IP range) they must identify themselves via their designated authentication procedure (Security Questions or Call Back). If users come from unknown IP addresses (not specified in the IP range) – access is denied and no security checks take place.

Note: This will work if enabled in rules.xml (see 'Installation&Configuration Guide: *Comodo Two Factor Integration – Challenges'* section).

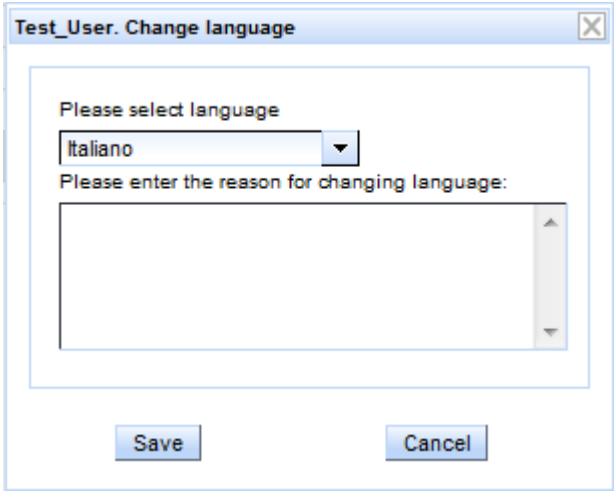


IP Range – Table of Parameters		
Form Element	**Type**	**Description**
IP range	Text Field	Administrator should specify IP range for the user. It should be IP address followed by netmask, e.g. 123.456.78.91/16.

IP Range – Table of Parameters		
Add	Control	Enables administrator to add desirable IP range to the list of IP ranges.
IP	Text Field	Shows the defined IP range.
Enabled	Check-box	If checked the rule of defined range for that user is active.
Delete	Control	Deletes the IP range from the list.
Save	Control	Saves the changes.

2.2.2.4 Set Language

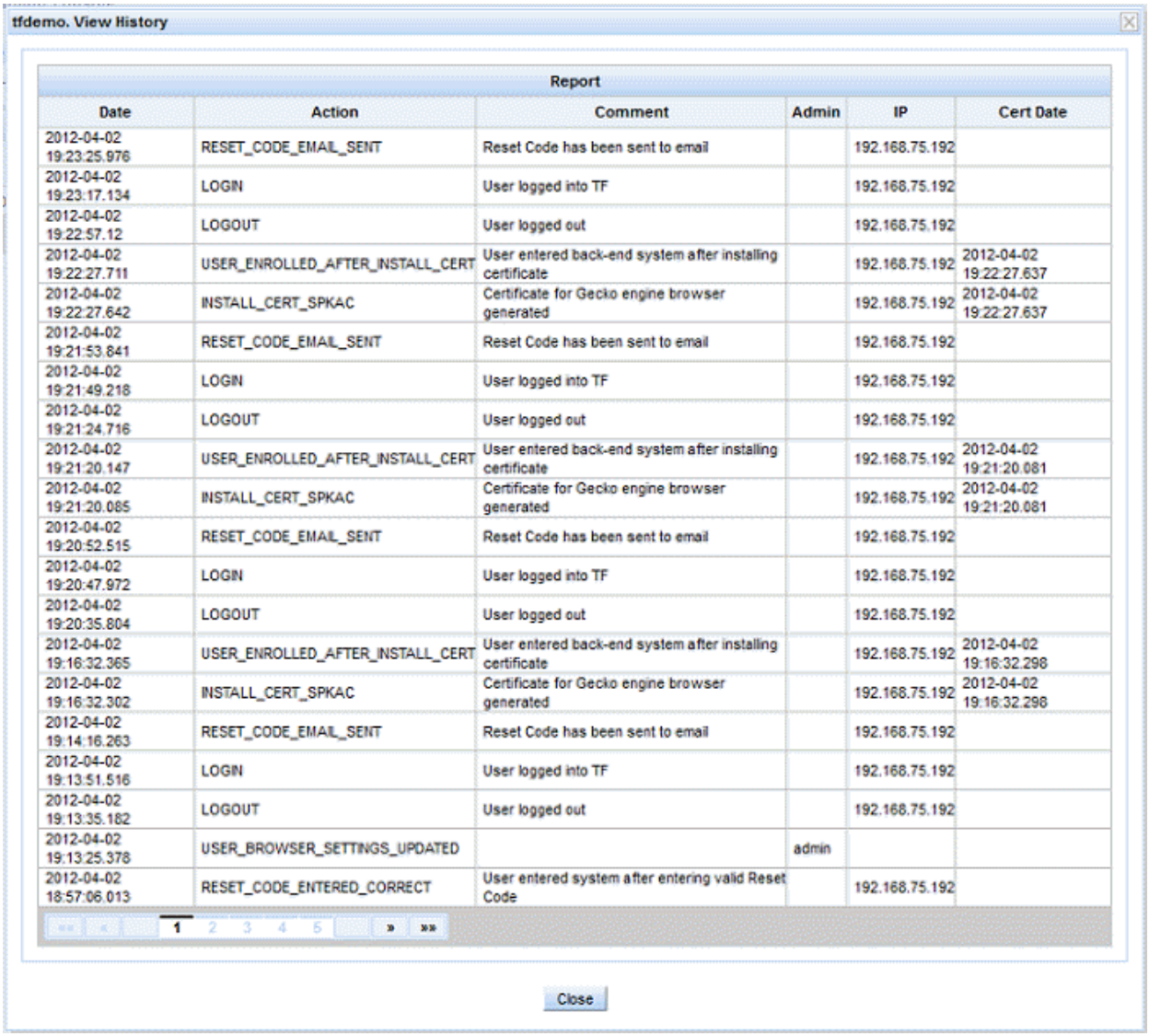
The 'Set Language' option enables the administrator to set the interface language for the user corresponding to the locality of the user.



Select Locale – Table of Parameters		
Form Element	**Type**	**Description**
Please select the language	Drop-down menu	Administrator should select the interface language for the user from the drop-down menu.
Please enter the reason for changing the language	Text Field	Administrator should enter a reason for setting or changing the interface language.
Save	Control	Saves the changes.
Cancel	Control	The 'Cancel' button annuls the changes.

2.2.2.5 View History

Selecting the 'View History' action will open a log of all events relating to the chosen user during their interaction with the Comodo Two Factor service.



History Dialog – Table of Parameters		
Form Element	**Type**	**Description**
Title	Text Field	Title shows the user's name.
Date	Text Field	Date/Time of the last action;
Action	Text Field	Operation, that was performed.
Comment	Text Field	The comment entered in the **Please enter reason** dialog while performing the respective user action.

History Dialog – Table of Parameters		
Admin	Text Field	Username of the administrator, that performed the action. Filled out only for actions, which Administrator performed for the given user.
IP	Text Field	User's IP address. Filled out only for actions, which were performed by the given user.
Cert Date	Text Field	Date/Time of the certificate's generation (the certificate, that was used during last login to the secure account). This information is additional monitoring factor and is saved in database of ComodoTF server.
Close	Control	Closes the 'History' dialog.

The following table lists the various Actions Values in the History dialog and their description:

Table of Actions – Value of History Dialog	
Action Value	**Description**
CREATE	The Administrator's account was created
ANSWER_FAILED	Entered invalid answer to security question
LOGIN	User logged into the account via ComodoTF
LOGIN_FIRST	User logged into the account via ComodoTF for the first time
LOGIN_FAILED	User entered invalid login or password
LOGOUT	User logged out.
ADMIN_LOGIN_FAILED	Administrator entered invalid login or password
LOCK	User was locked by administrator
LOCK_COMPLETE	User was locked due too many failed unlock attempts
INCORRECT_UNLOCK_CODE	User entered wrong unlock code
INCORRECT_ONETIME_PASSWORD	User entered wrong one-time password
LOCK_MAX_FAILED_ATTEMPTS	User was locked due too many failed attempts
LOCK_ADMIN_MAX_FAILED_ATTEM	Administrator was locked due too many failed attempts

Table of Actions – Value of History Dialog	
PTS	
LOCK_RESET_CODE	User was locked due too many failed reset attempts
USER_UNLOCK_BY_ADMIN	User was unlocked by administrator
USER_SELF_UNLOCK	User unlocked himself (using reset code (One-Time Password))
USER_UNLOCK_BY_TIMEOUT	User was unlocked after timeout
USER_RESET_BY_ADMIN	User settings were reset by administrator
USER_UPDATED_PHONES	User updated phones by Admin prompt
USER_BROWSER_SETTINGS_UPDATED	Browser settings updated by administrator
FULL_RESET	After full reset user status is changed to New User
USER_RESET_BY_ADMIN_WITH_CODE	User settings were reset with code prompt by administrator
RESET_CODE_SMS_SENT	Reset Code has been sent via SMS
RESET_CODE_SMS_SENDING_FAILED	Sending Reset Code via SMS failed
RESET_CODE_CALLBACK_SENT	Reset Code has been sent via callback
RESET_CODE_CALLBACK_SENDING_FAILED	Sending Reset Code via callback failed
RESET_CODE_EMAIL_SENT	Reset Code has been sent to email
RESET_CODE_EMAIL_SENDING_FAILED	Sending Reset Code via email failed
RESET_CODE_GENERATED	Reset Code (One-Time Password) was generated
RESET_CODE_ENTERED_INVALID	User entered Invalid Reset Code
RESET_CODE_ENTERED_CORRECT	User entered valid Reset Code
RESET_CODE_POSSIBLE_HACK	User tried to bypass Reset Code, possible Hack attempt. If user was reset by

Table of Actions – Value of History Dialog	
	admin he can try to load reset code page from his old store and submit it. In this case system does not allow him to check old reset code and locks this attempt.
USER_ENROLLED_CERT	User authenticated with previously installed certificate
USER_ENROLLED_AFTER_INSTALL_CERT	User authenticated after installing the certificate
USER_ENROLLED_AFTER_INSTALL_CERT_ERROR	User logged into the account after a certificate installation error
USER_ENROLLED_AFTER_CERT_INSTALL_CANCEL	User logged into the account after canceling certificate installation
USER_ENROLLED_AFTER_CRT_AGR_DECLINED	User logged into the account after declining certificate agreement
USER_ENROLLED_WITH_NO_AUTH	User logged into the account without TF authentication
USER_ENROLLED_WITH_KNOWN_IP	User logged into the account from a known IP address
USER_ENROLLED_WITHOUT_QUESTION_SET	User logged into the account without defining security questions (using 'Continue' button)
USER_ENROLLED_QUESTION	User authenticated with security questions
USER_ENROLLED_WITHOUT_CALLBACK_SET	User logged into the account without defining callback settings (using 'Continue' button)
USER_ENROLLED_CALLBACK	User authenticated with callback info
USER_ENROLLED_AFTER_INSTALL_COOKIE	User logged into the account after installing the security cookie
USER_ENROLLED_COOKIE	User authenticated with previously installed cookie
PROXY_DENIED_BLACKLISTED	User access is denied: the location is in Black list
PROXY_DENIED_UNKNOWN_IP	User access is denied: user IP is unknown
CERT_INSTALL_SKIPPED	User had problem installing certificate on IE and skipped the installation. He authenticated using proxy.
ERROR_INSTALL_CERT	Certificate installation was failed

Table of Actions – Value of History Dialog	
INSTALL_CERT_SPKAC	Certificate for Gecko engine browser was generated
ERROR_INSTALL_CERT_SPKAC	Certificate for Gecko engine browser generation was failed
INSTALL_CERT_CRMF	Certificate for Gecko engine browser was generated
ERROR_INSTALL_CERT_CRMF	Certificate for Gecko engine browser generation was failed
INSTALL_CERT_PKCS10	Certificate for MS Internet Explorer was generated
ERROR_INSTALL_CERT_PKCS10	Certificate for MS Internet Explorer generation was failed
INSTALL_CERT_PKCS12	Certificate for other browsers was generated
ERROR_INSTALL_CERT_PKCS12	Certificate for other browsers generation was failed
CERT_AGREEMENT_ACCEPTED	User accepted install certificate agreement
CERT_AGREEMENT_DECLINED	User declined install certificate agreement
CLEAR_COOKIES	Cookies were cleared by admin
NO_AUTH	Admin set authorization type as 'no auth'
ENABLE_AUTH	Admin set authorization type as 'auth'
ADMIN_UPDATE	Administrators account was updated (admin password was changed)
LOCALE_CHANGED	The interface language was changed for the user by the administrator.
REVOKE	All certificates installed before revoke date are disabled
SET_MAX_CERTS	Max amount of certificates was changed to this user
UPDATE_RESTRICTED_COUNTRIES	Restricted countries list was updated by administrator
USER_IP_RANGES_UPDATED	IP ranges were updated
USER_UPDATED_EMAIL	User updated email by Admin prompt
ENABLE_MASTER_STATUS	User account was set as Master

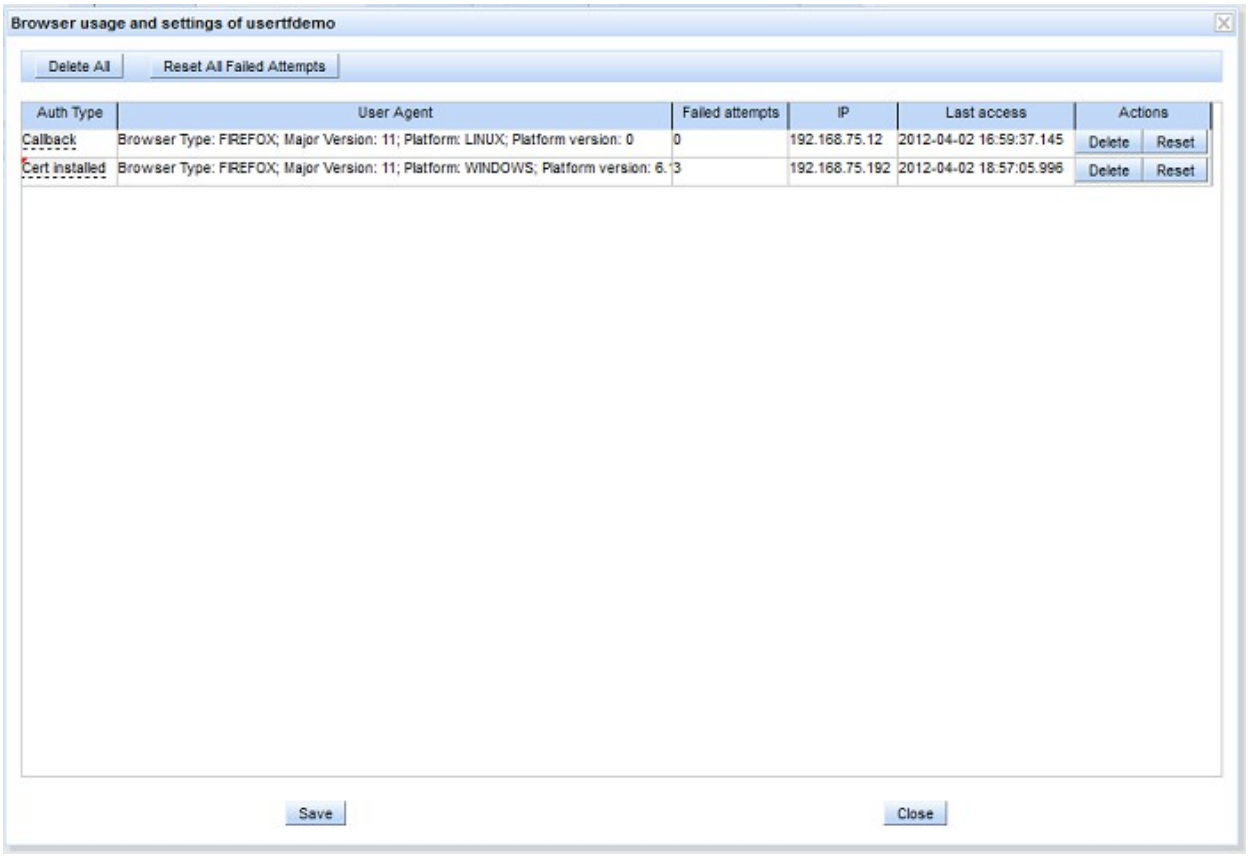
Table of Actions – Value of History Dialog	
DISABLE_MASTER_STATUS	Master status was removed from user account
DISABLE_COOKIE_MODE	Cookie mode was disabled
ENABLE_COOKIE_MODE	Cookie mode was enabled
ENABLE_COOKIE_MODE_BY_USER	User installed authentication cookie
ANSWER_POSSIBLE_HACK	User tried to submit different answers by-passing our forms, possible Hack attempt. This can be caused when he entered incorrect answers 3 times (or more then configured). In case if he saved (or loaded from cache) "enter answer" page and submitted it from browser more than 3 times, his answers then were not checked, system does not allow him to login to his account and locks this attempt.
URL_PARAMS_POSSIBLE_HACK	User tried to submit different answers by-passing our forms, possible Hack attempt. User tries to manually enter hack parameters into URL. If user was locked by admin, he can try to enter url parameters to reach reset page. System prevents it and locks his attempt.
USER_UPDATED_QA	User updated security Questions and Answers by Admin prompt
CHANGE_QUESTION_ANSWER	User changed security question
CHANGE_SECURITY_SETTINGS	User changed security settings
CREATE_QUESTION_ANSWER	User created security questions/answers for the first time
CALLBACK_DATA_CREATED	User set callback data.
CALLBACK_DATA_UPDATED	Callback data of the user were updated by user
CALLBACK_DATA_RESET	Callback data of the user were reset by user
USER_ADDED	User was added by an administrator or operator.
USER_DELETED	User was deleted by an administrator or operator.
MULTIPLE_USERS_DELETED	Multiple users were deleted by administrator.

2.2.2.6 Browser Usage and Settings

The 'Browser Usage and Settings' dialog displays the list of browsers (locations) through which the user has logged-in to the secure account in the previous login attempts with their authentication types. It also allows the you to change the authentication type (Client certificate/Security/Callback or (or Security Questions) set for each type of the browser for the specific user based

on compatibility of the Browser for Certificate and Cookies installation. **Click here for details on compatibility of browsers with certificate and cookies installation**.

For example, if the certificate installation has failed for a specific browser in any of the previous attempts - meaning the browser did not support certificate installation, you can change the authentication type to cookie mode or callback mode for that browser to enable trouble free login for the user using the browser he/she wants.

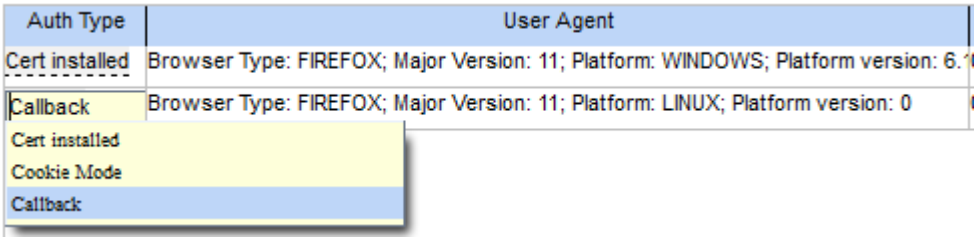


Browser usage.... – Table of Parameters		
Form Element	**Type**	**Description**
Title	Text Field	Title shows the user's name.
Auth type	Text Field	The current authentication type set for the browser indicated in the next column. This can be changed for future logins for the same user by clicking on the text. **Click here for more details.**
User Agent	Text Field	The type of the browser, its version and the Operating System on which the browser is installed. This enables the administrator to identify the browser precisely.
Failed Attempts	Text Field	Indicates the previous attempts in which the certificate installation has failed. This information assists the administrator to make a decision of switching this browser to cookie mode or callback mode for the selected user.
IP	Text Field	The IP address from which the user has logged-in through this browser.
Last Access	Text Field	The date and time of last access through this browser.

Browser usage.... – Table of Parameters		
Save	Control	Saves all changes made on the user "Browser Usage and Settings" records.
Close	Control	Closes the 'Location' dialog.
Delete	Control	Delete concrete "Browser Usage and Settings" record.
Delete all	Control	Delete all "Browser Usage and Settings" records.
Reset	Control	Reset failed attempts for concrete "Browser Usage and Settings" record.
Reset All Failed Attempts	Control	Reset failed attempts for all "Browser Usage and Settings" records.

Changing the Authentication Type for Selected Browser

1. Click on the authentication type beside the selected browser.
2. From the drop-down menu, select the authentication type you want to set for the browser.



3. Click 'Save'.

The change in the authentication mode settings will be saved and the 'Location' dialog will be closed. On the next login attempt by the user through the same browser, the user will be prompted to install a certificate (if you have set the authentication made as Cert installed mode), delivered a Security Cookie (if you have set the authentication made as Cookie mode) or asked to answer one of the security questions set beforehand (if you have set the authentication made as Callback mode).

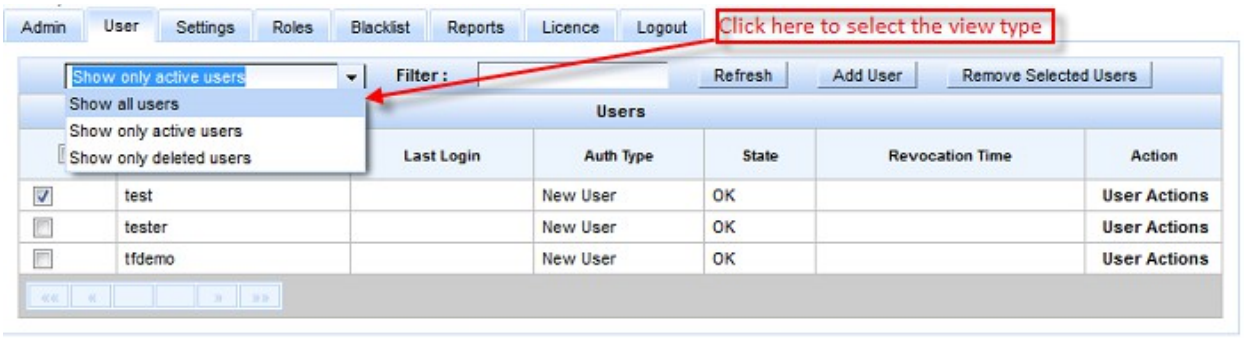
Compatibility of Browsers for Client Certificate Installation and Cookie Installation

Browser	Client Certificates	Secure Cookies
Internet Explorer 8		
Internet Explorer 9		
Internet Explorer 7		
Firefox		

Browser	Client Certificates	Secure Cookies
Opera 9.63 and below, Opera 11.61 and above	✓	✓
Opera 9.64 and above	Certificate installation unsupported Certificate enrollment on certificates installed before update to 9.63 is supported.	✓
Safari on OS without RFC5746 support	✗	✓
Safari on OS with RFC5746 support	✓	✓
Blackberry	✗	✓
Chrome 3.0 and above on Windows, Mac OS and Linux	✓	✓
Chrome 2.0 and below	✗	✓
MS IE Mobile 6 and above	✗	✓
MS IE Mobile 5	Not tested	✓
Konqueror 4.x	✗	✓
Konqueror 3.x	✓	✓
Netscape	✓	✓
Other browsers based on IE, Safari or Firefox (AOL, OmniWeb etc.)	✓	✓
Android	✗	✓

2.2.3 View Options

You can set the view type of the list of users under the Users tab by selecting the view type from the drop-down combo box near the upper left corner of the interface.

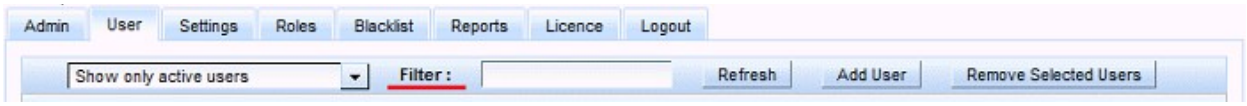


The options available are:

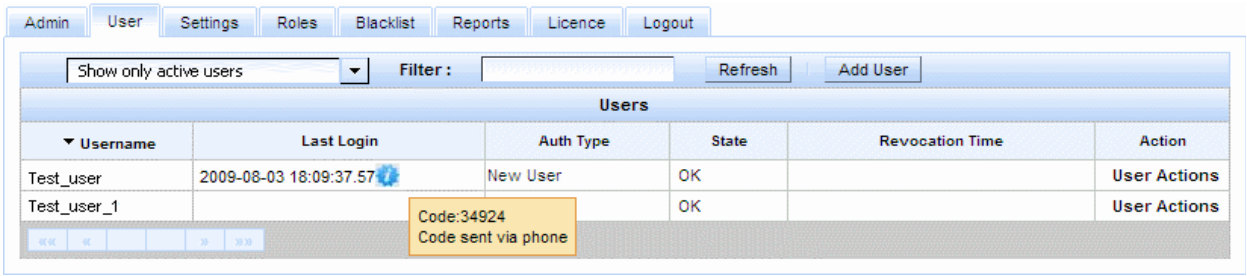
- **Show all users** – Selecting this will display all the users who were already authenticated via Comodo Two Factor.
- **Show only active users** – Selecting this option will display only the users whose credentials are active (current users).
- **Show only deleted users** – Selecting this option will display a list of only the users deleted by the administrator.

2.2.4 Filtering Options

You can search for particular user name by entering part of the user name into *Filter* field.



2.2.5 View Activation Code Sent to the User



In the event a user is connecting to the website from a machine different from that in which the security cookie or the certificate is installed, the Two Factor server will send a randomly generated, one-time activation password to the user through the user's telephone, email or as SMS as chosen by the user. The user must then enter this activation password at the website. See the section **Auxiliary, Out of Band, Second Factor Authentication** for more details.

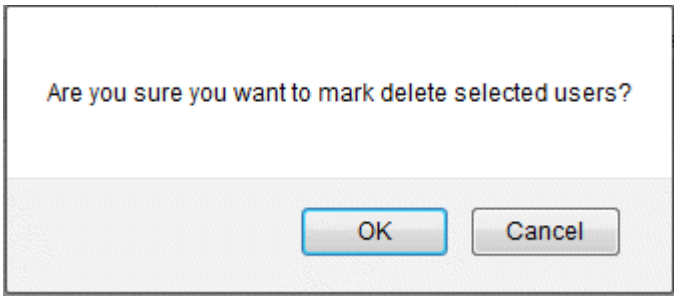
Administrators will be able to view the one-time activation password generated for the user during the user's last login attempt from an 'out of band' machine and the mode of sending the OTP to the user (phone, SMS or email).

A star icon is displayed beside 'Last Login' detail of the users, whose last login was from an 'out of the band' machine. Placing the mouse cursor over the star icon will display the last OTP generated and sent to the user and the medium (phone, SMS or email) through which the OTP was sent.

2.2.6. Remove Selected Users

1. Switch to the 'User' tab;
2. Using Filter functionality load required set of users;

3. Mark users for removal by clicking appropriate checkbox in the leftmost column;
4. Click the "Remove Selected Users" button to remove users;
5. Confirm removal.

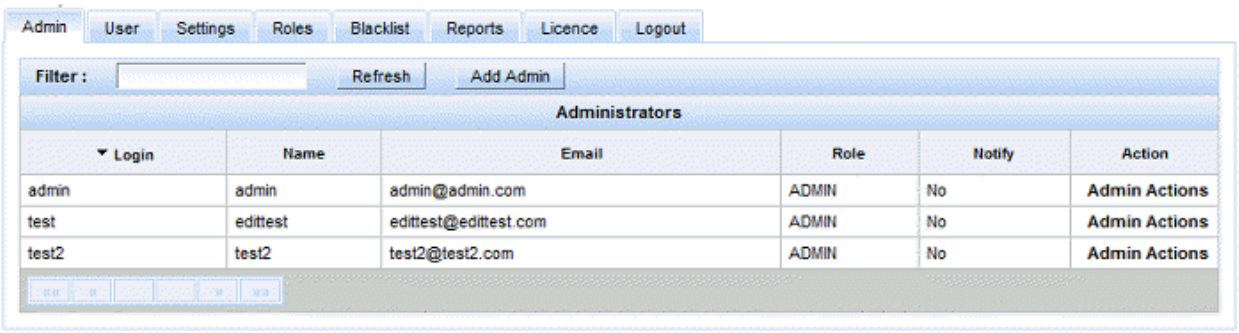


3 The 'Admin' Tab

3.1 Overview

The 'Admin' tab is a useful tool for administrators, which helps them define, manage, create administrators and operators.

Note: Admin tab is visible only for administrators. (**More...**)



The Admin tab – Table of Parameters	
Filed Name	**Description**
Login	Administrator's or operator's name as entered in login box.
Name	Administrator's or operator's full name as entered when creating.
Email	A person's email address which was set when adding.
Role	A person can have ADMIN's or OPERATOR's privileges.
Notify	If enabled a person will receive notifications about all important events.
Action	Actions available for a person's account (Edit or Change Password)

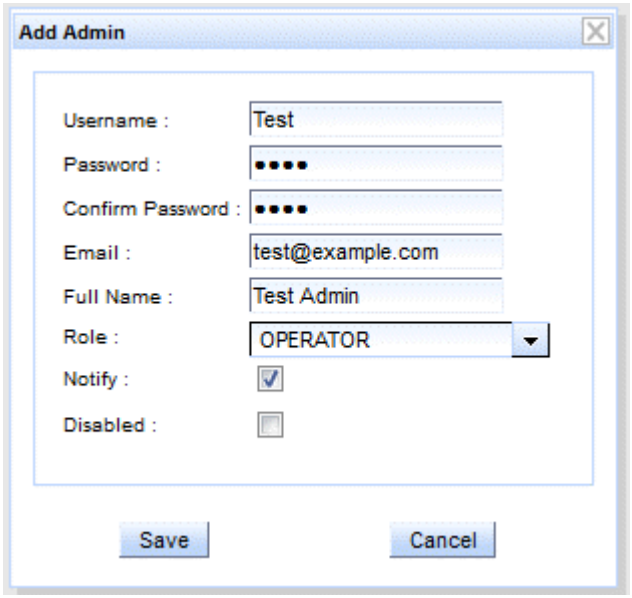
The Admin tab – Table of Parameters	
Add Admin	Enables administrator to add a new administrator or operator.
Refresh	Updates the list of displayed administrators to reflect changes such as newly added administrator or operator; changed person's role, etc.

3.2 Admin Management

Using 'Admin' tab an administrator can create new administrator or operator, change their passwords and edit details.

3.2.1 Adding New Administrators and Operators

1. Switch to the 'Admin' tab of ComodoTF console.
2. Click on 'Add Admin' button.
3. Complete the 'Add Admin' form.



4. Click 'Save' to add the administrator or operator to the ComodoTF interface.

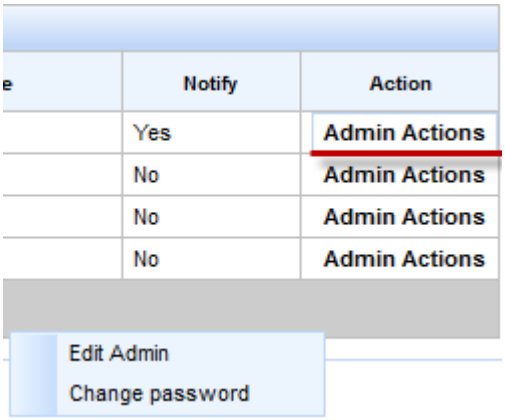
Note: An administrator's (or operator's) details can be modified at any time by clicking the 'Edit' button next to their name in the 'Action' section.

Add Admin form – Table of Parameters		
Form Element	**Type**	**Description**
Username	Text Field	Administrator should enter login for the new administrator.
Password ***(required)***	Text Field	Password to access the Certificate Manager interface. **Note**: If 'strong' passwords are enabled then the following criteria apply:

Add Admin form – Table of Parameters		
		• The password must be of 8-15 characters length • Must be alphanumeric • Must include at least one special character or uppercase letter. Strong passwords can be enabled by setting the '**ADMIN_PASSWORD_STRONG**' parameter to 'true' by modifying the 'conf/localhost.properties' file. See the TF installation and Configuration guide for more details.
Confirm ***(required)***	Text Field	Confirmation of the above.
Email	Text Field	Administrator should enter full email address.
Full Name	Text Field	Administrator should enter full name of administrator or operator.
Role	Drop-down	Enables to assign the role with a set of administrative privileges for the new Administrator. The default roles are 'Administrator' and 'Operator' (See the table **Roles – Comparison of default permissions** for more details). The Administrator can also create new roles with custom list of privileges and assign the role to the new Administrator. See **The Roles tab** for more details on creating new roles. **Note:** Only one role may be assigned to TF administrator. If an Administrator needs to be given a set of permissions, which is a combination of permissions pertaining to different roles, then a new role has to be created with the required permissions and assigned to the new administrator.
Notify	Check-box	Checking this box instructs Comodo Two Factor to notify about all important events.
Disabled	Check-box	Checking this box disables the new Administrator. Disabled administrators are highlighted with gray background.

3.2.2 Editing an Administrator or Operator

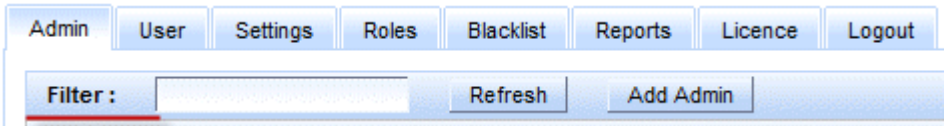
To edit settings for Administrator, switch to 'Admin' tab, and point mouse cursor over the 'Admin Actions' alongside the person's name.



Control	Description
Edit Admin	Enables administrator to edit all person's details except username. The interface is similar to 'New Admin' interface. See the previous section **Adding New Administrators and Operators** for more details.
Change Password	Enables administrator to change Administrator's/Operator's access password.

3.2.3 Filtering Options

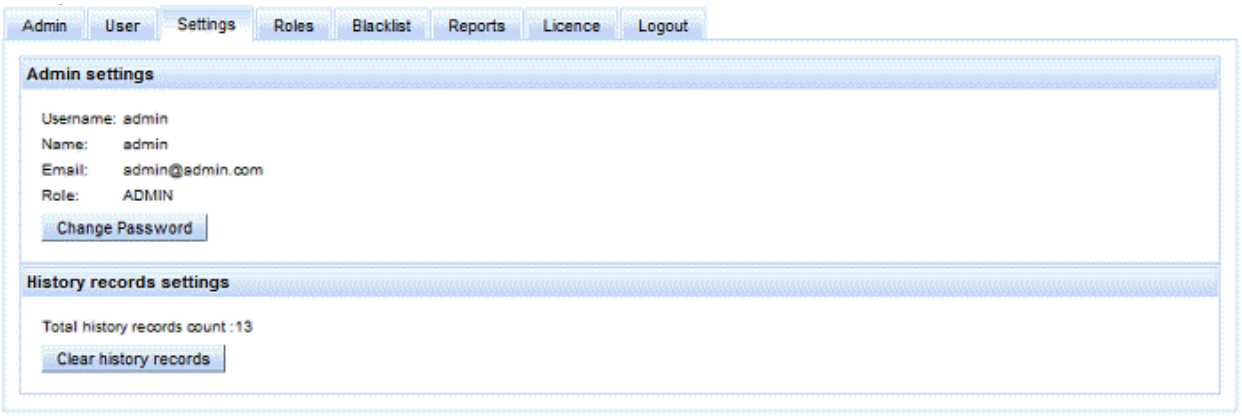
You can search for particular Administrator by entering part of the administrator's login name into *Filter* field.



4 The 'Settings' Tab

4.1 Overview

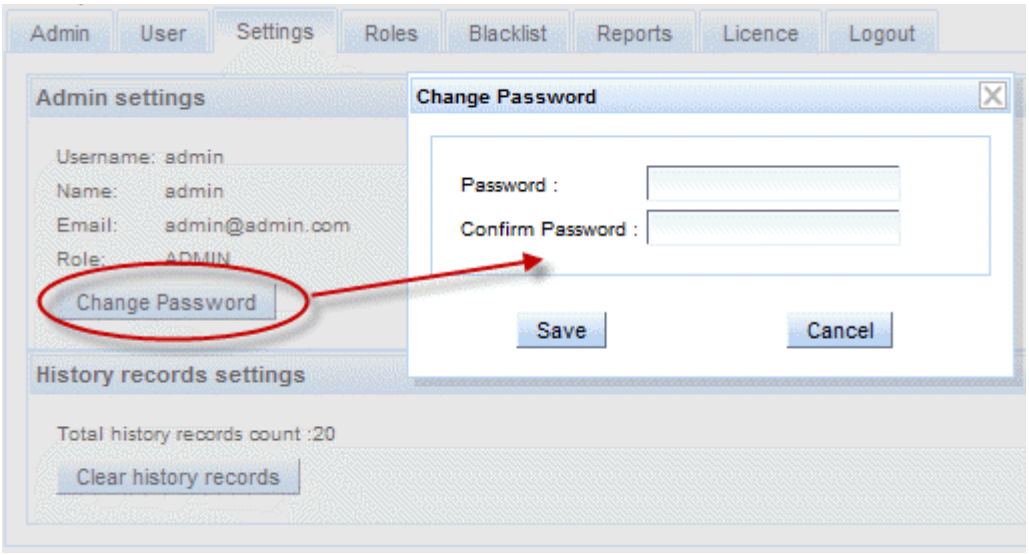
The 'Settings' tab enables administrator to view their current settings, such as user name, email and role.



It also enables the administrator to **change the login password** and to configure for **clearing the history records** for smoother operation.

4.2 Change Password

Administrators can change their passwords by switching to 'Settings' tab, and clicking **'Change Password'** button.



4.3 Clear History Records

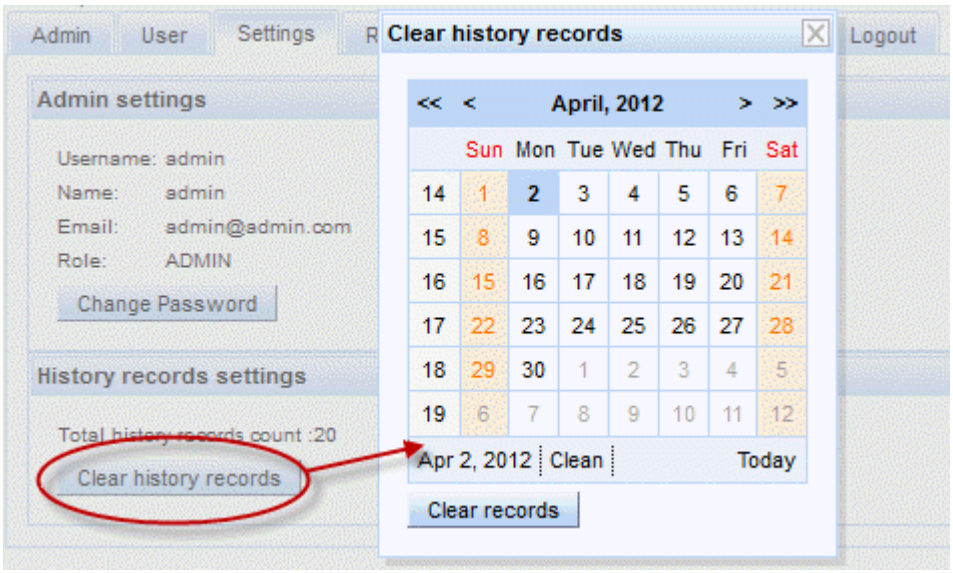
The log of all events relating to each user during their interaction with the Comodo Two Factor service is maintained as history records in a history table. The number of records currently in the history table is displayed in the 'History records settings' area of the 'Settings' interface.

Eventually, the number of records increase to an extent that it may impact on the performance while reading the the history table or while upgrading Comodo TF to a newer version. The administrators can clear the old and unwanted history records periodically to ensure smooth operation and easy upgrading to a newer version.

To clear the history records

1. Switch to the 'Settings' tab of ComodoTF console.
2. Click 'Clear history records' button from the 'Settings' interface.

A calendar window will be opened.

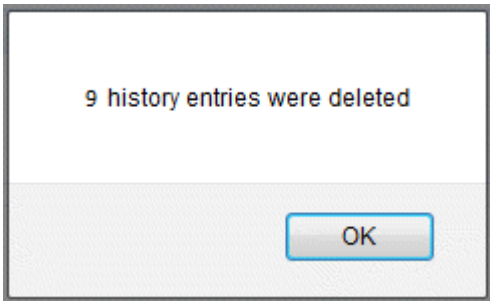


3. Select the date to clear all the history records logged before it.

The selected date will appear at the bottom left of the calendar window. If you want to reselect the date (in case you have chosen the date wrongly), click the 'Clean' link and select the date again.

4. Click the 'Clear records' button.

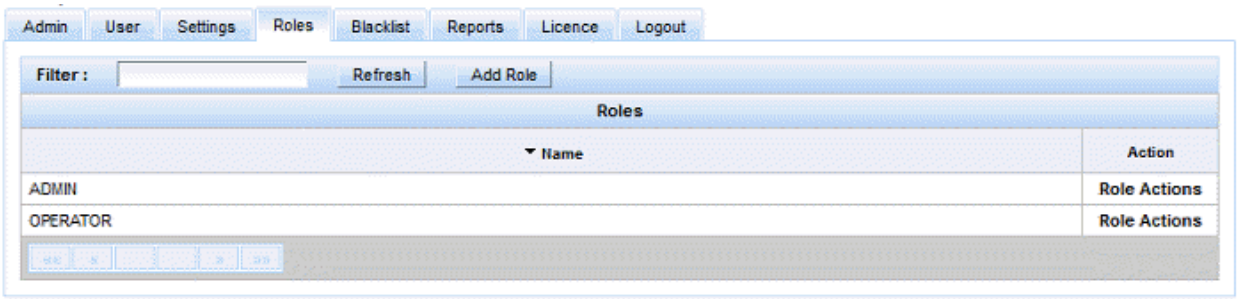
All the history records stored prior to the selected date will be removed from the history table and a conformation dialog will be displayed.



5 The 'Roles' Tab

5.1 Overview

The Roles tab allows the administrator to create a new role and edit permissions for the created roles.



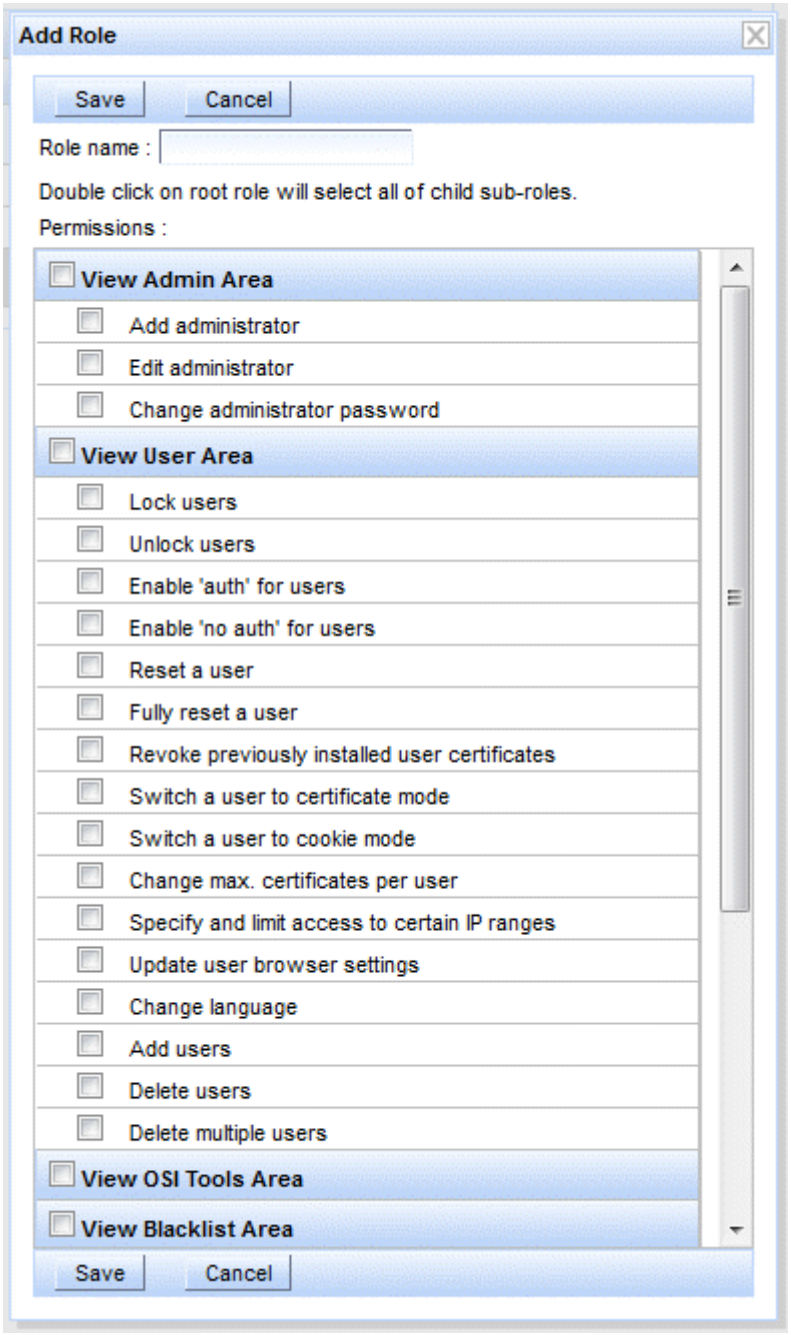
The Roles tab – Table of Parameters	
Filed Name	**Description**
Name	The name of the new Role
Action	Actions available for a person's account (Edit Permissions).
Add Role	Enables administrator to add a new role and define permissions for that role.
Refresh	Updates the list of displayed roles to reflect changes such as newly added role, or permissions edited for a role, etc.

5.2 Roles Management

Using the Roles tab the administrator can add a new role for a person, set permissions for that role and delete multiple users.

5.2.1 Adding a New Role

1. Switch to the 'Role' tab of ComodoTF console.
2. Click on 'Add Role' button. The following screen will be displayed:



3. Enter a name in the 'Role Name' field.
4. Select the required checkboxes to assign the permissions for the role being created (See the table below).
5. Click the 'Save' button.

Add Role form – Table of Parameters	
Option	**Description**
Permissions Related to 'Admin' Area	
View Admin Area	Enables personnel with this role to view the 'Admin' area of Comodo TF. (See The '**Admin' tab** for more details). The admin related settings are valid only if

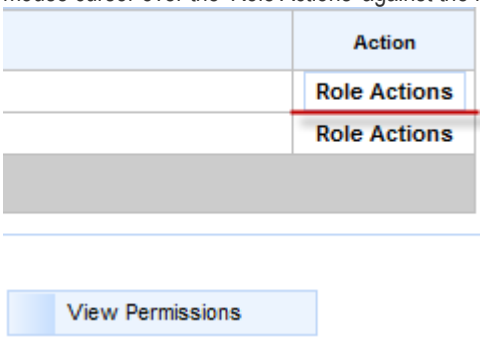
Add Role form – Table of Parameters	
Option	**Description**
	this option is checked.
Add administrator	Enables personnel with this role to add new administrators/operators.
Edit administrator	Enables personnel with this role to edit existing administrators/operators.
Change administrator password	Enables personnel with this role to change administrators passwords.
Permissions Related to 'User' Area	
View User Area	Enables personnel with this role to view the 'User' area of Comodo TF. (See **The 'Users' tab** for more details) The user related settings are valid only if this option is checked.
Lock Users	Enables personnel with this role to lock users if required.
Unlock Users	Enables personnel with this role to unlock users.
Enable 'Auth' for users	Enables personnel with this role to set authorization type for a user as 'Auth' (the end-user will need a client certificate or to answer security questions/receive a call-back in order to log in to their account)
Enable 'No Auth' for users	Enables personnel with this role to set authorization type for a user as 'No Auth' (the end-user will not need a client certificate or to answer security questions/receive a call-back in order to log in to their account)
Reset a user	Enables personnel with this role to reset a user if required. See **Reset User** for more details.
Fully reset a user	Enables personnel with this role to perform full reset of a user status. A full reset will change user status to 'New User', remove any existing security questions/call back details and force the user to re-register.
Revoke previously installed user certificates	Enables personnel with this role to disable all certificates that belong to the user in question.
Change max. certificates per user	Enables personnel with this role to set the maximum number of certificates for a user. See **Max Certs** for more details.
Update user browser settings	Enables personnel with this role to change user browser usage details and settings.
Specify and limit access to certain IP ranges	Enables personnel with this role to limit the IP range for a user access. See **IP Range** for more details.

Add Role form – Table of Parameters	
Option	**Description**
Change language	Enables personnel with this role to change the interface for a user. See **Languages** for more details.
Add users	Enables personnel with this role to create new users. See **Adding a New User** for more details.
Delete users	Enables personnel with this role to delete existing users.
Permissions Related to 'Blacklist' Area	
View Blacklist Area	Enables personnel with this role to view the 'Blacklist' area of Comodo TF (See **The 'Blacklist' tab** for more details). The options related to Blacklist are valid only if this is checked.
Edit black-listed countries	Enables personnel with this role to modify black-listed countries.
Permissions Related to 'License' Area	
View License Area	Enables personnel with this role to view 'License' area of Comodo TF (See **The 'License' tab** for more details). The options related to license are valid only if this is checked.
Update license	Enables personnel with this role to update Comodo TF license.
Permissions Related to 'Reports' Area	
View Reports	Enables personnel with this role to view 'Reports' area of Comodo TF (See **The 'Reports' tab** for more details).
Permissions Related to 'Applications' Area	
View Applications Area	Enables personnel with this role to view applications.
Edit Application	Enables personnel with this role to edit applications.
Permissions Related to 'Roles' Area	
View Roles Area	Enables personnel with this role to view the 'Roles' area of Comodo TF (See **The 'Roles' tab** for more details). The options related to 'Roles' are valid only if this is checked.
Add new role	Enables personnel with this role to add a new 'Role'.
Edit Role	Enables personnel with this role to edit an existing 'Role'.

Add Role form – Table of Parameters	
Option	**Description**
Delete role	Enables personnel with this role to delete an existing 'Role'.
Permissions Related to 'Settings' Area	
View Settings Area	Enables personnel with this role to view the 'Settings' area of Comodo TF (See **The 'Settings' tab** for more details). The options related to 'Roles' are valid only if this is checked.
Clear History	Enables personnel with this clear history records of user related events.
Permissions Related to 'OSI Tools' Area	
View OSI Tools Area	Enables personnel with this role to view OSI Tools area of Comodo TF. **Tip:** The OSI Tools Area enables administrator to view and import reports of the IP addresses which had access to the secure website e.g. bank system.

5.2.2 Editing the Permissions Granted to a Role

To edit the permissions of a Role, point mouse cursor over the 'Role Actions' against the required Role's name.

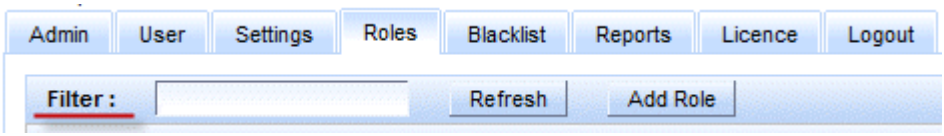


Control	Description
Edit Permissions	Enables administrator to edit the permissions granted for the Role. The interface is similar to 'Add a new role' interface. See the previous section **Adding a New Role** for more details.

Note: The default Roles 'Admin' and 'Operator' cannot be edited or deleted. For a full list of permissions granted to the default roles, see **Administrator's and Operator's roles – Comparative Table**.

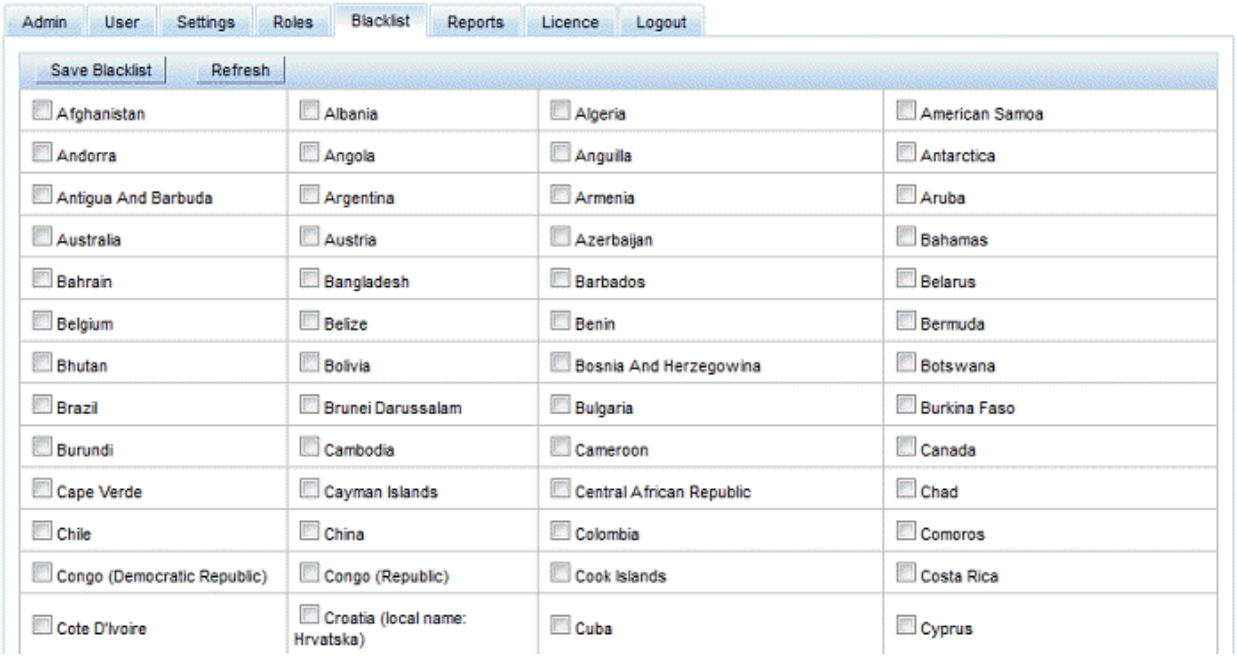
5.2.3 Filtering Options

You can search for particular Role by entering the name of the role in the *Filter* field.



6 The 'Blacklist' Tab

The 'Blacklist' tab enables administrator to deny access for customers, who come from IP addresses from specific countries. Such customers will see the message that access to the application is denied.



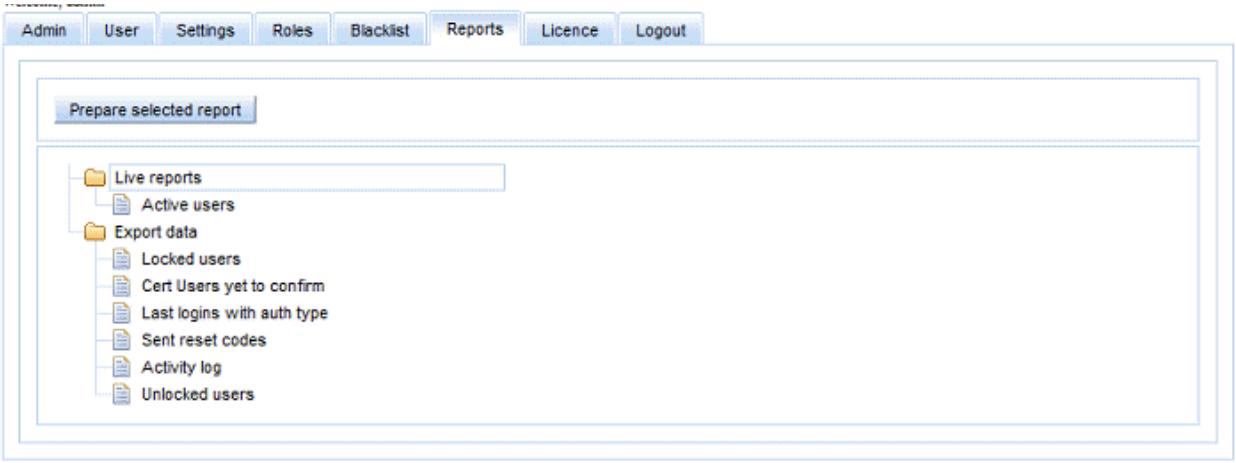
To do that, switch to 'Blacklist' tab, and check the box(es) alongside country(ies) that you would like to block.

Click '**Save Blacklist**' button when done to preserve changes. Clicking 'Refresh' button updates the list of countries displayed in the section.

7 The 'Reports' tab

7.1 Overview

The 'Reports' tab allows Administrators, Operators and other personnel with the appropriate security role to view and export multiple report types.

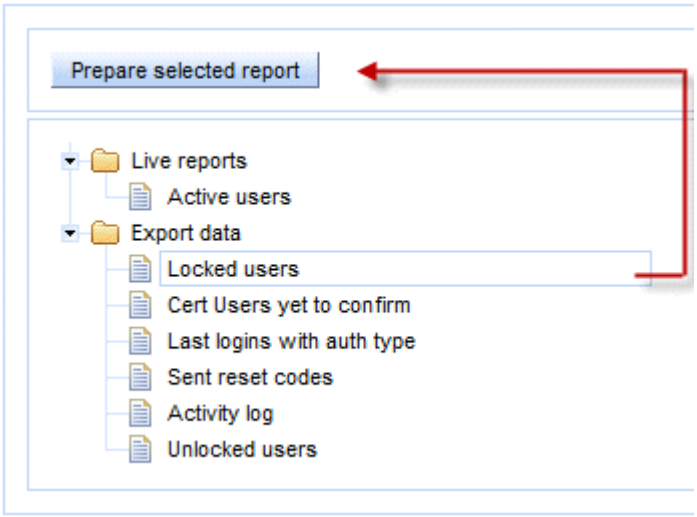


Reports tab – Table of Parameters		
Report Type		**Description**
Live reports	***Active Users***	Displays a log of all users currently logged into the secure website/service e.g. The bank system.
Export data	***Locked users***	Displays a log of all users who were locked for some reason for selected period of time.
	Cert Users Yet to confirm	Displays a log of all users who installed a certificate, but never used it for logging into the system for selected period of time.
	Last logins with auth type	Displays a log of all users and their authentication types for selected period of time.
	Sent reset codes	Displays a log of detailed information about all one-time passwords sent to users for selected time period (time, send method, IP to which the resent code was sent, etc., but without the actual reset code sent).
	Activity log	Displays a log of all actions for selected period of time.
	Unlocked users	Displays a log of all unlocked users for selected period of time.

7.2 View Report

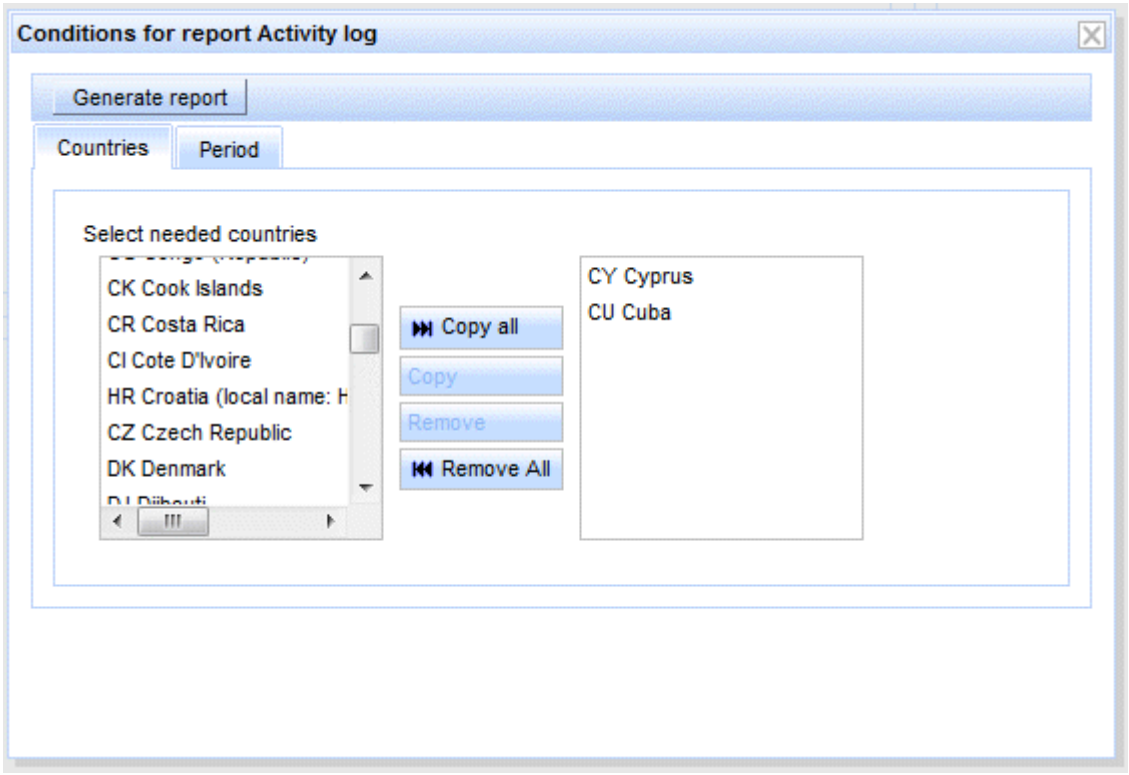
To view reports of a particular type:

1. Select the desired type of report from the drop-down list.
2. Click the 'Prepare selected report' button.

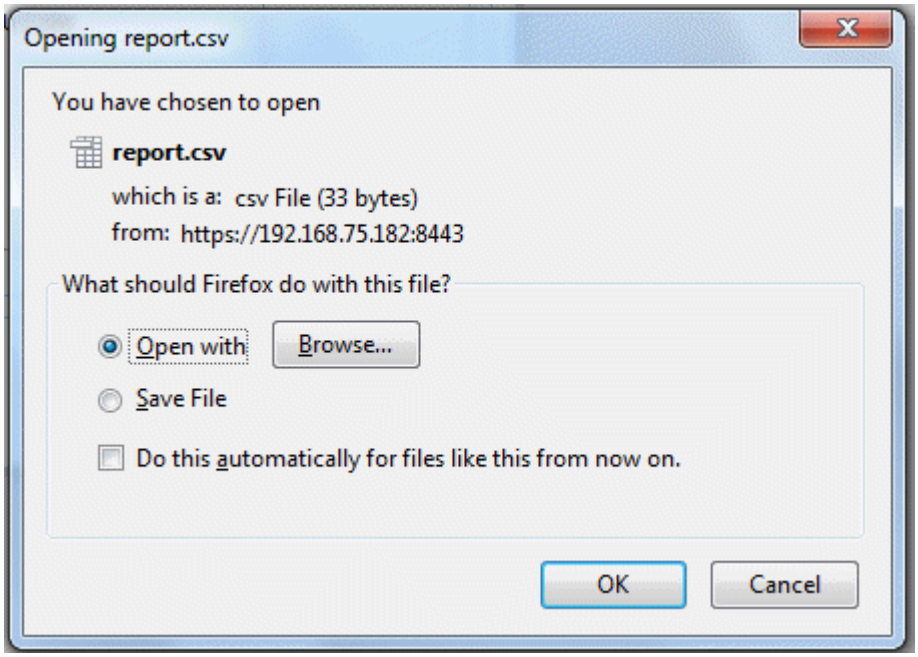


3. In the dialog that appears select, the time period for the statistics:

4. For 'Activity log' report you must also select a country (see screen shot below)

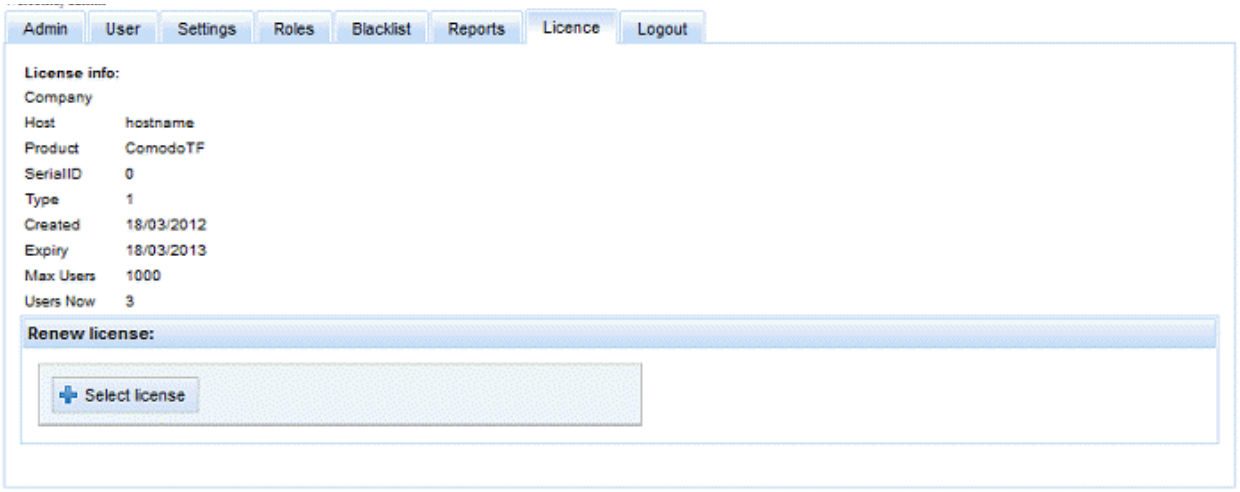


5. Click 'Generate report' button in the upper left corner of the dialog.
6. Download and save generated report (.csv format).



8 The 'License' Tab

The 'License' tab displays the current Comodo Two Factor license information.



License tab – Table of Parameters	
Fields	**Description**
Company	Displays the company's name.
Host	Displays the host name of ComodoTF server location.
Product	Displays product's name.
SerialID	Displays the unique serial ID of the product.
Type	Displays a type of the license.
Created	Displays the date of license creation.
Expired	Displays the expiration date of the license.
Max Users	Displays the maximum number of users allowed by the license.
Users Now	Displays the number of users registered in the system.

8.1 License Update

To update your Comodo TF license, please contact **sales@comodo.com**. Then you need to:

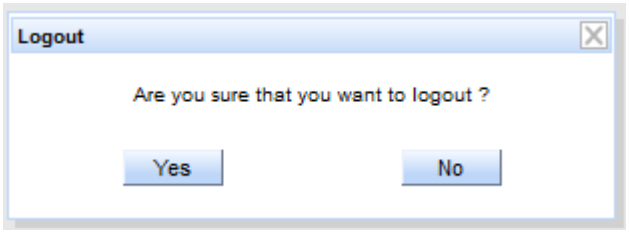
1. Save the license file to your computer;
2. In the 'license' section of the Comodo TF interface, press 'Select license' button;
3. Browse to and select the license file you saved previously.

Alternatively you can:

1. Save your license file to ComodoTFx.x/conf/. (license should have name license.<HOSTNAME>.xml. Where <HOSTNAME> = hostname in tomcat-cfg.xml (for example <tf hostname="localhost"...))
2. Restart the Comodo TF server for the changes to take effect.

9 Logging out of Comodo Two Factor

Administrator can log out from admin interface by clicking the 'Logout' tab.



10 FAQ

1. **Can't use AOL browser to install certificate.**

   After logging in to AOL ask the user to minimize AOL and open Internet Explorer (IE) to set up Certificate. After they set this up in IE they will be able to use AOL to access on-line banking.

2. **Can't use Secure website in Quicken to install certificate.**

   Perform the certificate installation in Internet Explorer first, then use Quicken to access on-line banking.

   Locked out of security questions - users are sure they are entering the correct answer to the challenge question.

   Reset Comodo security for customer and have customer set up the security questions again.

3. **Customers with MAC's having trouble with Safari.**

   Recommend upgrade to Mozilla Firefox as this is a preferred browser for MAC. Download Mozilla Firefox from www.getfirefox.com and install it. It has the capability of managing certificates on it's own, OR customers should review the online FAQ where we have added additional instructions for Safari users.

4. **Mozilla Firefox asks for Master Password when installing certificate.**

   Firefox is actually asking to set the Master Password and the user can use whatever they want as a password. If they want to disable the Master Password following the install they must go to Firefox→Preferences→Security and clear the Master Password check-box.

5. **MAC users with Internet Explorer having problems.**

   Internet Explorer on MAC does not work. Recommend upgrade to Mozilla Firefox as this is the preferred browser for MAC. Download Mozilla Firefox from www.getfirefox.com and install it. OR, use Safari.

6. **Customer has Safari Browser with multiple login ID's. With one login ID they can login using the certificate but can not find the certificate for the other login ID.**

   The Safari appears to work for one login ID. Customers with multiple login ID's can either use a different browser (Firefox) or they can use the certificate for one login ID and answer the security questions for the other login ID's.

7. **After time out when setting up challenge questions, user can not go back to beginning of system.** Instruct customer to close the browser and go back in to set up questions again.

About Comodo

The Comodo companies are leading global providers of Security, Identity and Trust Assurance services on the Internet. Comodo CA offers a comprehensive array of PKI Digital Certificates and Management Services, Identity and Content Authentication (Two-Factor - Multi-Factor) software, and Network Vulnerability Scanning and PCI compliance solutions. In addition, with over 10,000,000 installations of its threat prevention products, Comodo Security Solutions maintains an extensive suite of endpoint security software and services for businesses and consumers.

Continual innovation, a core competence in PKI and a commitment to reversing the growth of Internet-crime distinguish the Comodo companies as vital players in the Internet's ongoing development. Comodo, with offices in the US, UK, China, India, Romania and the Ukraine, secures and authenticates the online transactions and communications for over 200,000 business customers and millions of consumers, providing the intelligent security, authentication and assurance services necessary for trust in on-line transactions.

Comodo Group Inc.

1255 Broad Street

STE 100

Clifton, NJ 07013

United States

Tel : +1.877.712.1309

Tel: +1.703.637.9361

Email: **EnterpriseSolutions@Comodo.com**

Comodo CA Limited

3rd Floor, 26 Office Village, Exchange Quay, Trafford Road, Salford, Greater Manchester M5 3EQ,

United Kingdom.

Tel : +44 (0) 161 874 7070

Fax : +44 (0) 161 877 1767

For additional information on Comodo - visit **http://www.comodo.com**.