



Comodo **Two Factor** **Share Point & Outlook Web** **Access**

Software Version 2.4

Administration Guide

Guide Version 2.4.011811

Table of Contents

1.Introduction to Comodo TF for SharePoint and OWA	3
1.1.Overview of Solution & Outline of Processes.....	4
1.1.1.First Factor Authentication - Existing User Credentials.....	4
1.1.2.Second Factor Authentication - Digital Client Certificates or Security Cookie.....	4
1.1.3.Auxiliary, Out of Band, Second Factor Authentication.....	5
1.2.Comodo TF for SharePoint and OWA Authentication Benefits.....	6
1.3.Guide Structure.....	6
1.3.1.Definition of Terms.....	7
1.3.2.Administrator's and Operator's Roles - Comparative Table.....	8
1.4.Logging into Comodo TF for SharePoint and OWA Admin Interface.....	9
1.5.The Main Interface - Summary of Areas.....	10
1.5.1.User	10
1.5.2.Admin.....	10
1.5.3.Settings.....	11
1.5.4.Roles.....	11
1.5.5.Blacklist	11
1.5.6.Reports.....	12
1.5.7.License.....	12
1.5.8.Logout	13
2.The 'Users' Tab.....	13
2.1.Overview.....	13
2.1.1.'User' - Table of Parameters.....	13
2.2.User Management.....	14
2.2.1.Adding a New User.....	14
2.2.2.User Actions.....	15
2.2.2.1.Reset User.....	16
2.2.2.2.Set Max No. of certs.....	17
2.2.2.3.Set Access IP range.....	18
2.2.2.4.Set Language.....	19
2.2.2.5.View History.....	20
2.2.2.6.Browser Usage and Settings.....	25
2.2.3.View Options.....	27
2.2.4.Filtering Options.....	28
2.2.5.View Activation Code Sent to the User.....	28
3.The 'Admin' Tab.....	28
3.1.Overview.....	28
3.2.Admin Management.....	29
3.2.1.Adding New Administrators and Operators.....	29
3.2.2.Editing an Administrator or Operator.....	30
3.2.3.Filtering Options.....	31
4.The 'Settings' Tab.....	31
4.1.Overview.....	31
4.2.Change Password.....	31
5.The 'Roles' Tab.....	32
5.1.Overview.....	32
5.2.Roles Management.....	33
5.2.1.Adding a New Role.....	33

5.2.2.Editing the Permissions Granted to a Role.....	36
5.2.3.Filtering Options.....	36
6.The 'Blacklist' Tab.....	36
7.The 'Reports' Tab.....	37
7.1.Overview.....	37
7.2.View Report.....	38
8.The 'License' Tab.....	40
8.1.License Update.....	41
9.Logging out of Comodo TF for SharePoint and OWA.....	41
10.FAQ.....	41
About Comodo.....	43

1. Introduction to Comodo TF for SharePoint and OWA

Comodo TF for SharePoint and OWA (Comodo TF SOWA) 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

Security Cookies and the Digital Client Certificates are easy to deploy, affordable and effective solutions to enable the enhanced user identification and access controls needed to protect sensitive online information. The cookies (or the X.509 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. The cookies (or the client certificates) are the essential elements of Comodo's Two-Factor Authentication solution that provide strong user access authentication, protect the privacy of online data, and offer a transparent log-on method that won't inconvenience users.

Each security cookie (or the certificate), in addition to traditional login credentials, establishes a user's unique identity to a remote server application - in this case the Comodo TF for SharePoint and OWA proxy server. Comodo offers both the forms of second factor authentication - Security Cookies or Client Certificates - but Comodo TF SOWA trial users are restricted to the use of security cookies. Each cookie (or the 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 cookie (or the client certificate) onto an end user's machine requires no expertise and will not inconvenience users like other two factor solutions that rely upon expensive physical devices.

The second factor authentication 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 security cookie or the 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 SOWA 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 or Security Cookie**
- **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 user-name 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 TF for

SharePoint and OWA 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 user-name and password.

1.1.2. Second Factor Authentication - Digital Client Certificates or Security Cookie

The provisioning of a security cookie (or, if the vendor prefers, an X.509 client certificate) onto the end users machine. Once installed into the user's Internet browser (e.g., Internet Explorer, Firefox, Opera), this security cookie (or the certificate) will be requested and verified every time the user logs into the Two Factor Office server and will authenticate them as the genuine account holder. The presence of this security cookie (or the 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 Office server would not detect the security cookie (or the client certificate) on the machine the hacker is connecting from.

Note: By default, in Comodo TF SOWA is available only security cookie installation, but administrator is able to order and install digital certificate.

1.1.3. Auxiliary, Out of Band, Second Factor Authentication

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

1. The user chose not to install a security cookie (or 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 security cookie (or a certificate).
2. The user is attempting to access his account from a different machine to the one they installed the security cookie (or the certificate) on. For example, they are using their work computer or laptop for the first time to access their account but installed the security cookie (or 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.

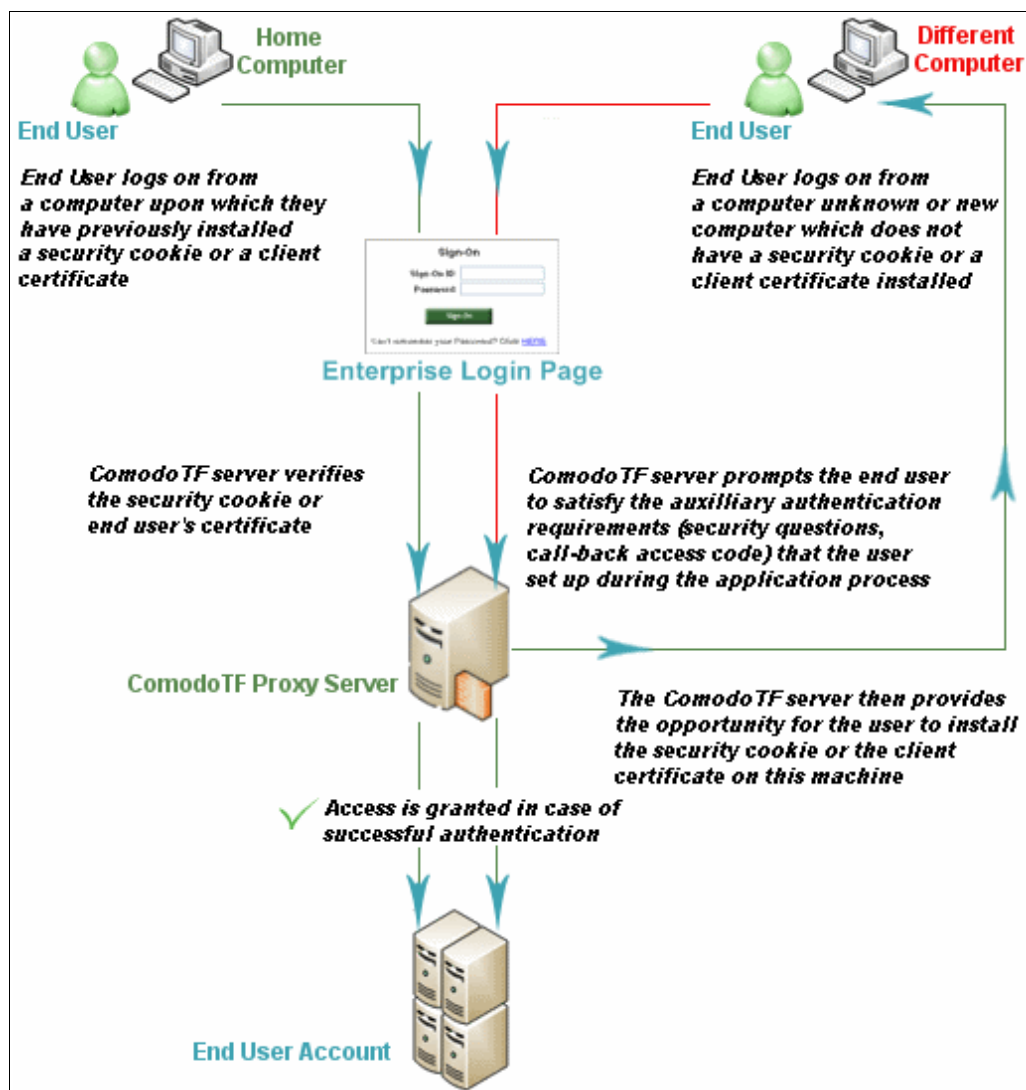
To ensure the highest levels of validation are used at all times, Comodo TF for SharePoint and OWA also incorporates an out-of-band second factor authentication process via telephone or SMS.

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 security cookie (or the 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 Office server, then the user is allowed to connect to their account. They are also provided with the opportunity to install a security cookie (or 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 security cookie or 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 TF for SharePoint and OWA end user will experience when they:

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



1.2. Comodo TF for SharePoint and OWA 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 experience in 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/secure cookie 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. Security cookies (or digital 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 TF for SharePoint and OWA service.

- Section 1, **Introduction to Comodo TF for SharePoint and OWA**, 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 Comodo TF SOWA access password.
- 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 to 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 TF for SharePoint and OWA**, 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 preconfigured permissions and capabilities (see [1.5.4.Role](#) 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	Description
<i>Administrator</i>	<p>Administrators are the top level administrator and can access all areas and functionality of the Comodo TF SOWA administrative console.</p> <ul style="list-style-type: none"> • Administrators have full visibility and control over Client Certificates/Cookies of users. • Administrators are listed in and can be managed and created from the 'Admin' area of the Comodo TF SOWA 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.
<i>Operator</i>	<p>Operators have privileges to access administrative console, monitor and manage users activity.</p> <ul style="list-style-type: none"> • 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.
<i>User</i>	<p>A 'User' is a person that has authenticated themselves to the Two Factor interface by logging into their OWA or SharePoint account and, in doing so, have requested or been provisioned with an authentication certificate or secure cookie.</p> <ul style="list-style-type: none"> • 'Users' have no access rights whatsoever to the administrative console of Comodo TF SOWA. They exist in Comodo TF SOWA 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 TF for SharePoint and OWA:

Definition of Terms	
	<ul style="list-style-type: none"> via Manual creation by an Administrator or an Operator in the 'User' tab; Automatically via Self-enrollment procedure (when logging to their back end account for the first time). All Users are listed in the 'User' tab of Comodo TF SOWA 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.

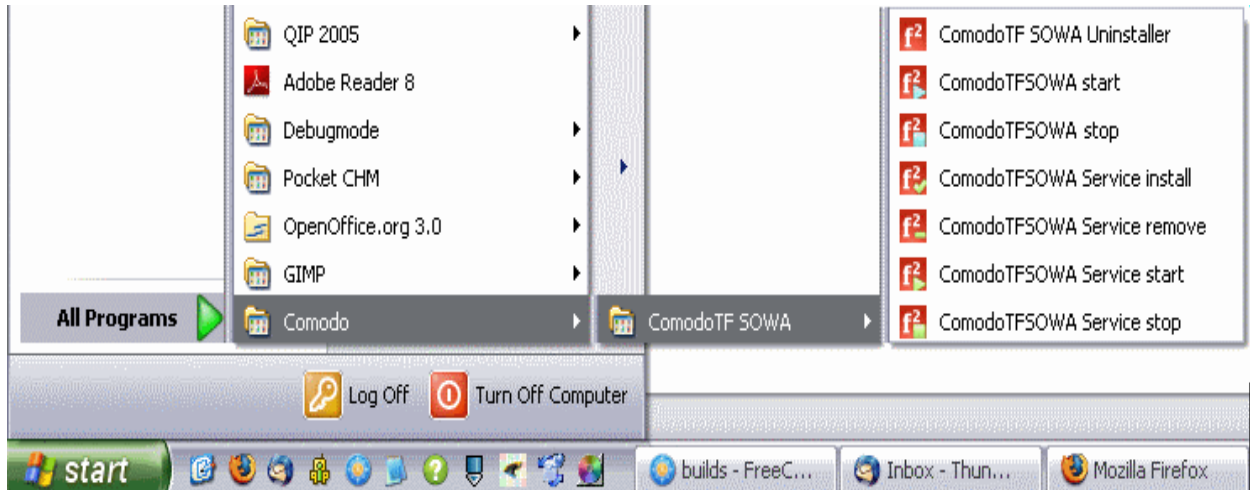
Roles - Comparison of Default Permissions			
Actions	Definition	Role = Administrator	Role = Operator
Manage Administrators	View, Add, Edit, Change Password	✓	✓
Manage Operators	View, Add, Edit, Change Password	✓	✗
Manage Users	Multiple view and Action settings. See The Roles tab for full list.	✓	✓
View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

1.4. Logging into Comodo TF for SharePoint and OWA Admin Interface

Comodo TF SOWA is intended for automatic integration with MS SharePoint and / or Outlook Web Access.

To access Comodo TF for SharePoint and OWA (Comodo TF SOWA)

For Windows users click: Start > All Programs > Comodo > Comodo TF SOWA > Comodo TF SOWA start



For Unix users:

```
go  
cd ComodoTFSOWA-x.x/bin  
execute $ ./startup.sh
```

This will launch Comodo TF SOWA application:

```

C:\ComodoTFO\Office start
INFO: Starting Servlet Engine: Apache Tomcat/6.0.14
Jan 31, 2008 5:28:06 PM org.apache.catalina.startup.ContextConfig defaultWebConf
ig
INFO: No default web.xml
Jan 31, 2008 5:28:12 PM org.apache.catalina.startup.ContextConfig defaultWebConf
ig
INFO: No default web.xml
AbandonedObjectPool is used (org.apache.tomcat.dbcp.dbcp.AbandonedObjectPool@b4b
e3d)
  LogAbandoned: true
  RemoveAbandoned: true
  RemoveAbandonedTimeout: 12600
Jan 31, 2008 5:28:20 PM org.apache.catalina.startup.ContextConfig defaultWebConf
ig
INFO: No default web.xml
AbandonedObjectPool is used (org.apache.tomcat.dbcp.dbcp.AbandonedObjectPool@1f4
88f1)
  LogAbandoned: true
  RemoveAbandoned: true
  RemoveAbandonedTimeout: 12600
Jan 31, 2008 5:28:31 PM org.apache.coyote.http11.Http11Protocol init
INFO: Initializing Coyote HTTP/1.1 on http-443
Jan 31, 2008 5:28:31 PM org.apache.coyote.http11.Http11Protocol start
INFO: Starting Coyote HTTP/1.1 on http-443

```

Now you can now login to Comodo Two Factor via your web browser by visiting: https://your_comodotfsowa_domain.com:1234/comodotf. (replace 'your_comodotfsowa_domain.com' with the actual name of your domain). Enter your login and password, and click on 'Login' button.



Login

Login :
Password :

Login Reset

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 TF for SharePoint and OWA interface has a tab structure that facilitates access to all major settings.



- There are (a maximum of) eight tabs that cover each of the main functional areas of the solution. These are **'Admin'**, **'User'**, **'Settings'**, **'Roles'**, **'Blacklist'**, **'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'**, **The 'Settings' tab**, **The 'Roles' tab**, **The 'Blacklist' tab**, **The 'License' tab** and **The 'Reports' tab**.

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

1.5.1. User

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

Admin	User	Settings	Roles	Blacklist	Reports	Licence	Logout
<div> Show all users Filter : Refresh Add User </div>							
Users							
▼ Username	Last Login	Auth Type	State	Revocation Time	Action		
New_User2		New User	OK		User Actions		
Test_User		New User	OK		User Actions		
Test_User1		New User	OK		User Actions		

[Click here for more information about the 'User' section.](#)

1.5.2. Admin

Displays a list of personell 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/personell with custom roles.

▼ Login	Name	Email	Role	Notify	Action
admin	admin	admin@admin.com	ADMIN	No	Admin Actions

[Click here for more information about 'Admin' section.](#)

1.5.3. Settings

Allows the person that is currently logged in to modify their password.

Username: admin
Name: admin
Email: admin@admin.com
Role: ADMIN
[Change Password](#)

[Click here for more information about the 'Settings' area.](#)

1.5.4. Roles

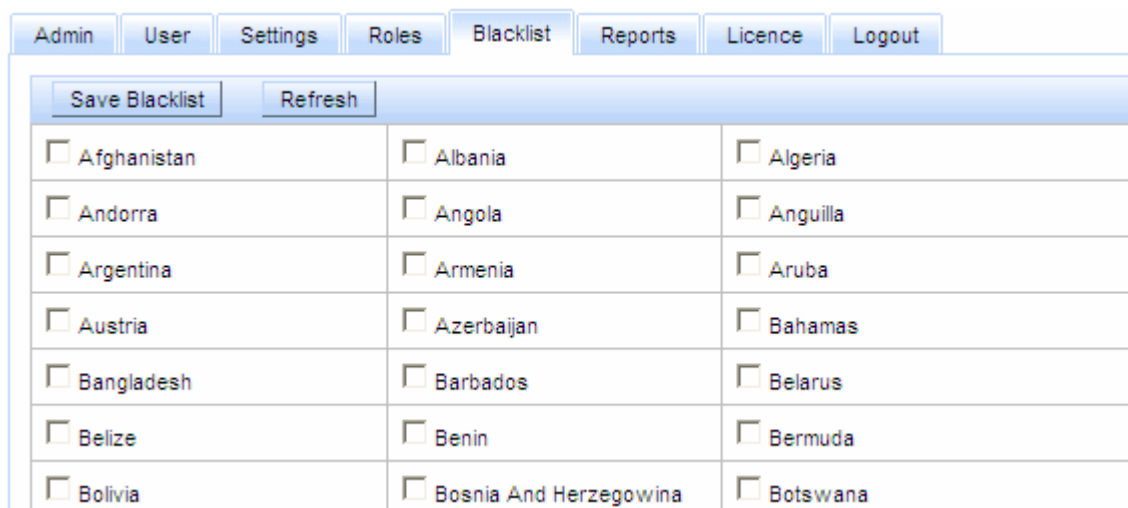
Allows the administrator to create new roles and edit permissions for the created roles.

▼ Name	Action
ADMIN	Role Actions
OPERATOR	Role Actions

[Click here for more information about the 'Roles' area.](#)

1.5.5. Blacklist

Provides full management of Comodo TF SOWA service administrators.

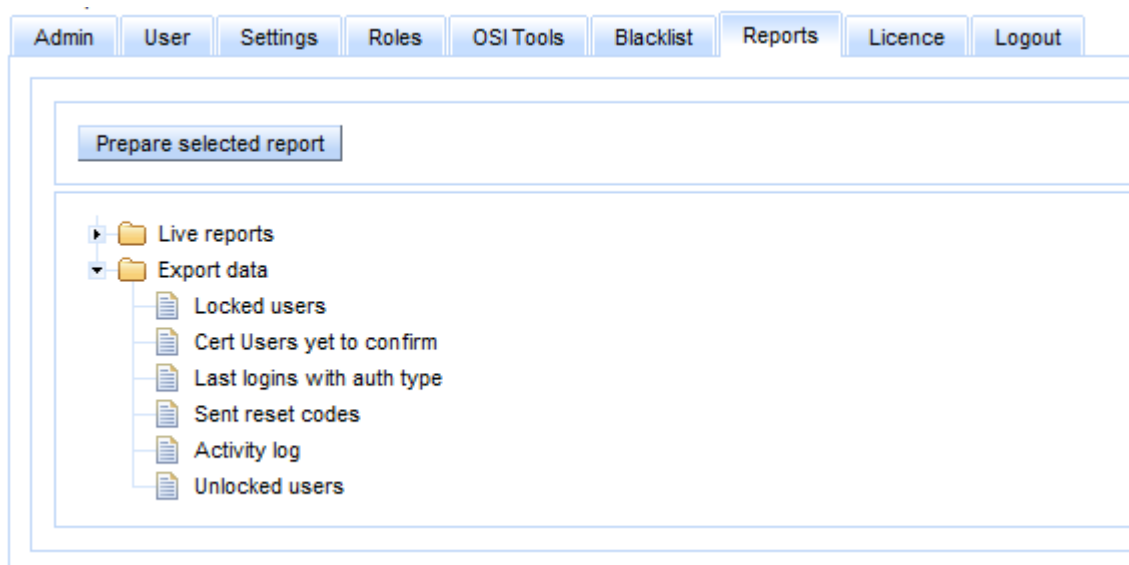


<input type="button" value="Save Blacklist"/> <input type="button" value="Refresh"/>		
<input type="checkbox"/> Afghanistan	<input type="checkbox"/> Albania	<input type="checkbox"/> Algeria
<input type="checkbox"/> Andorra	<input type="checkbox"/> Angola	<input type="checkbox"/> Anguilla
<input type="checkbox"/> Argentina	<input type="checkbox"/> Armenia	<input type="checkbox"/> Aruba
<input type="checkbox"/> Austria	<input type="checkbox"/> Azerbaijan	<input type="checkbox"/> Bahamas
<input type="checkbox"/> Bangladesh	<input type="checkbox"/> Barbados	<input type="checkbox"/> Belarus
<input type="checkbox"/> Belize	<input type="checkbox"/> Benin	<input type="checkbox"/> Bermuda
<input type="checkbox"/> Bolivia	<input type="checkbox"/> Bosnia And Herzegowina	<input type="checkbox"/> Botswana

[Click here for more information about the 'Blacklist' area.](#)

1.5.6. Reports

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



- Live reports
- Export data
 - Locked users
 - Cert Users yet to confirm
 - Last logins with auth type
 - Sent reset codes
 - Activity log
 - Unlocked users

[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 Comodo TF SOWA 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 TF for SharePoint and OWA.

Users					
▼ Username	Last Login	Auth Type	State	Revocation Time	Action
New_User2		New User	OK		User Actions
Test_User		New User	OK		User Actions
Test_User1		New User	OK		User Actions

2.1.1. 'User' - Table of Parameters

User - Table of Parameters		
Field Name	Values	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.

User - Table of Parameters		
Auth Type	New User	User is new, and no security questions/answers, nor cookie/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.
	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 to manage the 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 Comodo TF SOWA end-user interface.

2.2.1. Adding a New User

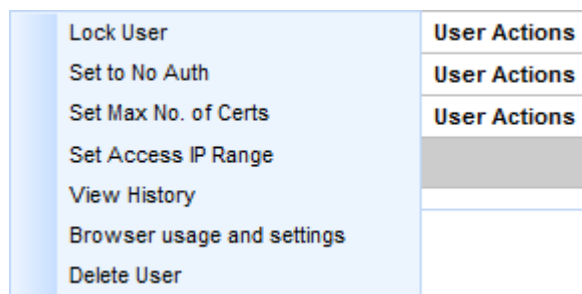
1. Switch to the 'User' tab;
2. Click the 'Add' button to open the 'Add User' form.

3. Enter a new user name.

4. Click 'Save' to add the end-user to the Comodo TF SOWA.

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](#).

Actions 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 the user account (available only if Auth Type is LOCKED)
Set to No Auth	Enables administrator to set the user state to No Auth (available only if state is not 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 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.

Actions Dialog Table of Parameters	
Set Max. No of Certs	Sets certificates' quantity available for the user. Possible values: default, unlimited, custom.
Set Access IP Range	Enables administrator to manage IP ranges for user. Click here for more information.
Set 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. Click here for more information.
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).
Delete User	<p>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).</p> <p>Upon deletion:</p> <ul style="list-style-type: none"> 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**, '**Set Max. No of Certs**', '**Set Access IP Range**', and '**View History**') the following dialog appears:

The dialog box has a title bar that says "Please enter reason." with a close button (X) on the right. Inside the dialog, there is a large rectangular text input field. At the bottom of the dialog, there are two buttons: "Save" on the left and "Cancel" on the right.

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.

Test_User. reset

☐ Email

☐ Questions

☐ Clear cookie

☒ Code prompt (autogenerate)

Please select email for reset code sending

☒ jsmith@example.com

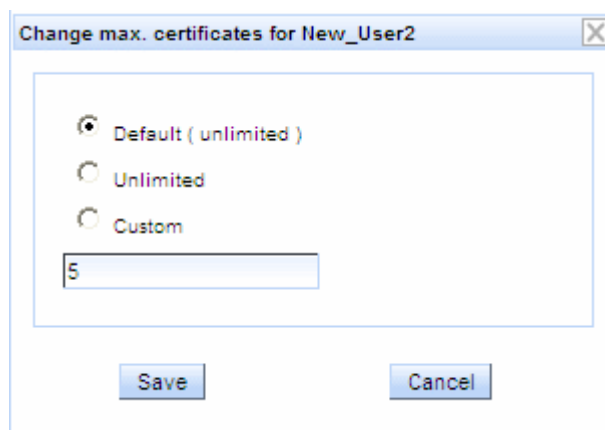
☐ john_smith@somemail.com

Save Cancel

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.



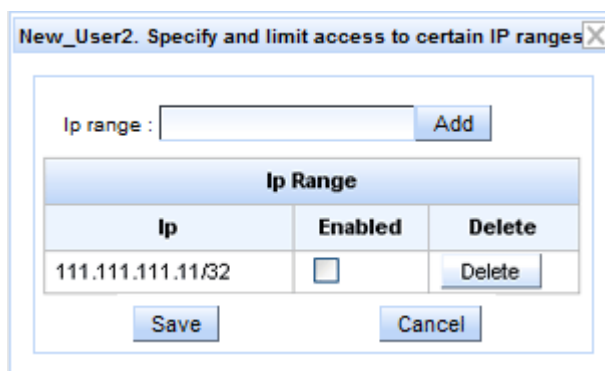
Select any one of the following options by selecting the corresponding radio button: Default, Unlimited or Custom and enter the number that denotes the number of certificates for the selected option.

2.2.2.3. Set Access IP range

'Set Access IP range' enables the administrator to manage IP ranges for user. Depending the on configuration of Comodo TFSOWA , the administrator can set the following types of authentication:

- By default, if users come from known IP addresses (specified in the IP range) - access granted is without any security checks. If users come from unknown IP addresses (not specified in the IP range) - users must identify themselves via their designated 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 prompted authentication procedure (SQ or CB). If users come from unknown IP addresses (not specified in the IP range) - access **is denied and no security checks take place**.

Note / Tip: This will work if enabled in rules.xml (see 'Installation&Configuration Guide: *Comodo TF for SharePoint and OWA Integration - Challenges*' section).



IP Range for User - 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.
Add	Control	Enables administrator to add desirable IP range to the list of IP ranges.

IP Range for User - Table of Parameters		
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.
Cancel	Control	The 'Cancel' button annuls 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.

The screenshot shows a Windows-style dialog box titled "Test_User. Change language". Inside the dialog, there is a label "Please select language" above a dropdown menu currently showing "Italiano". Below this is a label "Please enter the reason for changing language:" followed by a large empty text area. At the bottom of the dialog are two buttons: "Save" and "Cancel".

Select Language 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.

Note: The end user can set the interface language on his/her first login to the secure account. The language set by the user will be displayed in the 'Language' column of the Admin console. However, the Administrator can change from the

Admin Console, overriding the language setting made by the user, if required.

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.

Report					
Date	Action	Comment	Admin	IP	Cert Date
2009-05-21 12:09:29.62	USER_DELETED	User was deleted by administrator	admin		
2009-05-21 11:56:01.275	NO_AUTH	Testing	admin		
2009-05-21 11:50:15.203	USER_UNLOCK_BY_ADMIN	Testing	admin		
2009-05-21 11:44:38.277	LOCK	Test	admin		
2009-05-21 11:30:50.636	USER_ADDED	User was added by administrator	admin		

Close

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.
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 back end account). This information is additional monitoring factor and is saved in database of Comodo TF SOWA server.
Close	Control	Closes the 'History' dialog.

Table of Actions - Values of History Dialog	
Action Value	Description

Table of Actions - Values of History Dialog

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_ATTEMPTS	Administrator was locked due too many failed attempts
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
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

Table of Actions - Values of History Dialog

ILED	
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 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_CERT_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

Table of Actions - Values of History Dialog

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
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)

Table of Actions - Values of History Dialog

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
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

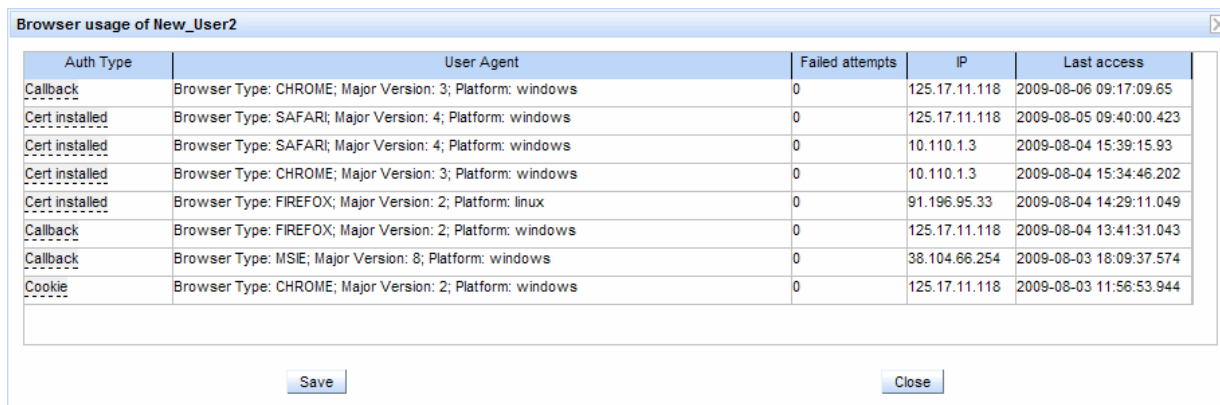
Table of Actions - Values of History Dialog

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.

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.



Auth Type	User Agent	Failed attempts	IP	Last access
Callback	Browser Type: CHROME; Major Version: 3; Platform: windows	0	125.17.11.118	2009-08-06 09:17:09.65
Cert installed	Browser Type: SAFARI; Major Version: 4; Platform: windows	0	125.17.11.118	2009-08-05 09:40:00.423
Cert installed	Browser Type: SAFARI; Major Version: 4; Platform: windows	0	10.110.1.3	2009-08-04 15:39:15.93
Cert installed	Browser Type: CHROME; Major Version: 3; Platform: windows	0	10.110.1.3	2009-08-04 15:34:46.202
Cert installed	Browser Type: FIREFOX; Major Version: 2; Platform: linux	0	91.196.95.33	2009-08-04 14:29:11.049
Callback	Browser Type: FIREFOX; Major Version: 2; Platform: windows	0	125.17.11.118	2009-08-04 13:41:31.043
Callback	Browser Type: MSIE; Major Version: 8; Platform: windows	0	38.104.66.254	2009-08-03 18:09:37.574
Cookie	Browser Type: CHROME; Major Version: 2; Platform: windows	0	125.17.11.118	2009-08-03 11:56:53.944

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 the changes made on the authentication type for the selected browser for this user.
Close	Control	Closes the 'Location' dialog.

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.

Auth Type	User Agent
Cert installed	Browser Type: CHROME; Major Version: 3; Platform: windows
Cert installed	Browser Type: SAFARI; Major Version: 4; Platform: windows
Cert installed ▼	Browser Type: SAFARI; Major Version: 4; Platform: windows
Cert installed	Browser Type: CHROME; Major Version: 3; Platform: windows
Cookie	Browser Type: FIREFOX; Major Version: 2; Platform: linux
Callback	Browser Type: FIREFOX; Major Version: 2; Platform: windows
Callback	Browser Type: MSIE; Major Version: 8; Platform: windows
Cookie	Browser Type: CHROME; Major Version: 2; Platform: windows

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 mode as Cert installed mode), delivered a Security Cookie (if you have set the authentication mode as Cookie mode) or asked to answer one of the security questions set beforehand (if you have set the authentication mode as Callback mode).

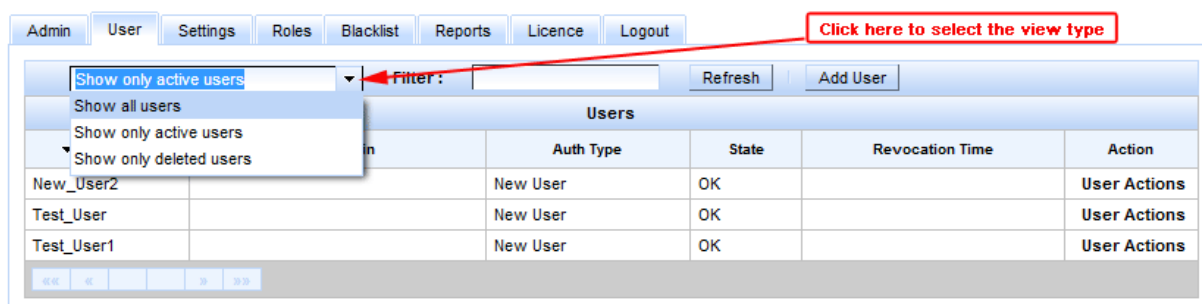
Compatibility of Browsers for Client Certificate Installation and Cookie Installation

Browser	Client Certificates	Secure Cookies
Internet Explorer 8	✓	✓
Internet Explorer 7	✓	✓
Internet Explorer 6	✓	✓
Firefox 3.x	✓	✓
Firefox 2.0	✓	✓
Opera 9.63 and below	✓	✓
Opera 9.64 and above	Certificate installation unsupported Certificate enrollment on certificates installed before	✓

Browser	Client Certificates	Secure Cookies
	update to 9.63 is supported.	
Safari 4.0	✓	✓
Safari 3.0	✓	✓
Blackberry	✗	✓
Chrome 3.0	✓	✓
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.)	✓	✓

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.

The screenshot shows the 'User' tab selected in the top navigation bar. Below the navigation bar, there is a dropdown menu set to 'Show all users' and a text input field labeled 'Filter :'. To the right of the 'Filter' field is a 'Refresh' button.

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.

The screenshot shows the 'Users' table with columns: Username, Last Login, Auth Type, State, Revocation Time, and Action. The user 'Test_user_1' is highlighted, and a tooltip is displayed over the star icon in the 'Last Login' column.

Username	Last Login	Auth Type	State	Revocation Time	Action
Test_user	2009-08-03 18:09:37.57	New User	OK		User Actions
Test_user_1			OK		User Actions

Code:34924
Code sent via phone

3. The 'Admin' Tab

3.1. Overview

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

Note: Admin tab is visible only for administrators. ([More...](#))

The screenshot shows the 'Admin' tab selected in the top navigation bar. Below the navigation bar, there is a 'Filter' field and an 'Add Admin' button. The 'Administrators' table is displayed with columns: Login, Name, Email, Role, Notify, and Action.

Login	Name	Email	Role	Notify	Action
admin	admin	admin@admin.com	ADMIN	No	Admin Actions

The Admin tab - Table of Parameters	
Field 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 which took place.
Action	Actions available for a person's account (Edit or Change Password)
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 Comodo TF SOWA console
2. Click on 'Add Admin' button
3. Complete the 'Add Admin' form

The 'Add Admin' dialog box is shown with the following fields and values:

- Username : Test
- Password : [masked]
- Confirm Password : [masked]
- Email : test@example.com
- Full Name : Test Admin
- Role : OPERATOR
- Notify : ☒
- Disabled : ☐

Buttons: Save, Cancel

4. Click 'Save' to add the administrator or operator to the Comodo TF SOWA 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	<p>Password to access the Certificate Manager interface.</p> <p>Note. If 'strong' passwords are enabled then the following criteria apply:</p> <ol style="list-style-type: none"> The password must be of 8-15 characters length Must be alphanumeric Must include at least one special character or uppercase letter. <p>Strong passwords can be enabled by setting the 'ADMIN_PASSWORD_STRONG' parameter to 'true' by modifying the 'conf/localhost.properties' file. See the TF SOWA installation guide for more details.</p>
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	<p>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.</p> <p>Note: Only one role may be assigned to TF administrator. If an Administrator</p>

Add Admin form - Table of Parameters		
		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.

Role	Notify	Action
	Yes	<u>Admin Actions</u>
Edit Admin		Admin Actions
Change password		Admin Actions

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 person'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.

Admin	User	Settings	Roles	Blacklist	Reports	Licence	Logout
Filter : <input type="text"/> <input type="button" value="Refresh"/> <input type="button" value="Add Admin"/>							

4. The 'Settings' Tab

4.1. Overview

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

Admin User **Settings** Roles Blacklist Reports Licence Logout

Username: admin
 Name: admin
 Email: admin@admin.com
 Role: ADMIN

Change Password

4.2. Change Password

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

Admin User Settings **Roles** Blacklist Reports Licence Logout

Username: admin
 Name: admin
 Email: admin@admin.com
 Role: ADMIN

Change Password

Change Password

Password :
 Confirm Password :

Save Cancel

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.

Admin User Settings **Roles** Blacklist Reports Licence Logout

Filter : Refresh Add Role

Roles	
Name	Action
ADMIN	Role Actions
OPERATOR	Role Actions

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

The Roles tab Table of Parameters

permissions edited for a role, etc.

5.2. Roles Management

Add Role

Save Cancel

Role name :

<input type="checkbox"/>	Fully reset a user
<input type="checkbox"/>	Revoke previously installed user certificates
<input type="checkbox"/>	Switch a user to certificate mode
<input type="checkbox"/>	Switch a user to cookie mode
<input type="checkbox"/>	Change max. certificates per user
<input type="checkbox"/>	Assign 'Master Account' status to a user account
<input type="checkbox"/>	Remove 'Master Account' status from user account
<input type="checkbox"/>	Specify and limit access to certain IP ranges
<input type="checkbox"/>	Change language
<input type="checkbox"/>	Add users
<input type="checkbox"/>	Delete users
<input type="checkbox"/>	View OSI Tools Area
<input type="checkbox"/>	View Blacklist Area
<input type="checkbox"/>	Edit black-listed Countries
<input type="checkbox"/>	View License Area
<input type="checkbox"/>	Update licence
<input type="checkbox"/>	View Reports
<input type="checkbox"/>	View Roles Area
<input type="checkbox"/>	Add new role
<input type="checkbox"/>	Edit role
<input type="checkbox"/>	Delete role

Save Cancel

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

5.2.1. Adding a New Role

1. Switch to the 'Role' tab of ComodoTF SOWA Admin 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.

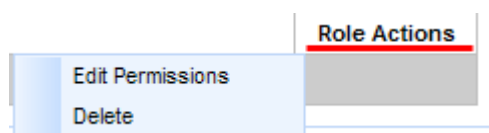
Add Role form - Table of Parameters	
Option	Description
Permissions Related to 'Admin' Area	
View Admin Area	Enables personnel with this role to view the 'Admin' area of Comodo TF SOWA. (See The 'Admin' tab for more details). The admin related settings are valid only if this option is checked.
Add administrator	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 SOWA. (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 the users if required.
Unlock Users	Enables personnel with this role to unlock the locked 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 security cookie 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 need a security cookie 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.
Switch a user to cookie mode	Enables personnel with this role to switch a user to certificate authentication mode. See Changing the Authentication type for Selected Browser for more details.
Switch a user to certificate mode	Enables personnel with this role to switch a user to cookie authentication mode. See Changing the Authentication type for Selected Browser for more details.

Add Role form - Table of Parameters	
Option	Description
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.
Assign 'Master Account' status to a user account	Enables personnel with this role to set a user account as master account
Remove 'Master Account' status from user account	Enables personnel with this role to remove the Master account status from a master account and to set it as normal account
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.
Change language	Enables personnel with this role to change the interface language was changed for a user. See Language for more details.
Add users	Enables personnel with this role to add new users. See Adding a New User for more details.
Delete user	Enables personnel with this role to delete existing users.
Permissions Related to 'Blacklist' Area	
View Blacklist Area	Enables personnel with this role to view 'Blacklist' area of Comodo TF SOWA. (See The 'Blacklist' tab for more details). The options related to Blacklist are valid only if this is checked.
Edit black-listed countries	Enables the administrator to modify which countries are black-listed
View License Area	Enables to view 'License' area of Comodo TF SOWA (See The 'License' tab for more details). The options related to license are valid only if this is checked.
Update license	Enables personell with this role to update Comodo TF license.
Permissions Related to 'Reports' Area	
View Report	Enables to personell with this role view the 'Reports' area of Comodo TF SOWA (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.

Add Role form - Table of Parameters	
Option	Description
Permissions Related to 'Roles' Area	
View Roles Area	Enables personnel with this role to view the 'Roles' area of Comodo TF SOWA (See The 'Roles' tab for more details). The options related to 'Roles' are valid only if this is checked.
Add new role, Edit role, Delete role	Enables personnel with this role to add a new 'Role'.
Edit Role	Enables personnel with this role to edit an existing 'Role'.
Delete role	Enables personnel with this role to delete an existing 'Role'.

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.

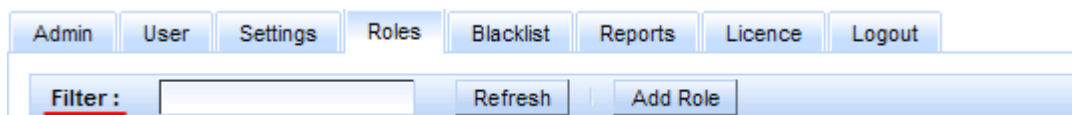


Control	Description
Edit Permissions	Enables administrator to edit the permissions granted for the Role. The interface is similar to 'Add a new role' interface. See the previous section Adding a New Role for more details.
Delete	Enables administrator to delete the Role.

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.

<input type="button" value="Save Blacklist"/> <input type="button" value="Refresh"/>		
<input type="checkbox"/> Afghanistan	<input type="checkbox"/> Albania	<input type="checkbox"/> Algeria
<input type="checkbox"/> Andorra	<input type="checkbox"/> Angola	<input type="checkbox"/> Anguilla
<input type="checkbox"/> Argentina	<input type="checkbox"/> Armenia	<input type="checkbox"/> Aruba
<input type="checkbox"/> Austria	<input type="checkbox"/> Azerbaijan	<input type="checkbox"/> Bahamas
<input type="checkbox"/> Bangladesh	<input type="checkbox"/> Barbados	<input type="checkbox"/> Belarus
<input type="checkbox"/> Belize	<input type="checkbox"/> Benin	<input type="checkbox"/> Bermuda
<input type="checkbox"/> Bolivia	<input type="checkbox"/> Bosnia And Herzegovina	<input type="checkbox"/> Botswana

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

Click '**Save counties**' 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

- Live reports
 - Active users
- Export data
 - Locked users
 - Cert Users yet to confirm
 - Last logins with auth type
 - Sent reset codes
 - Activity log
 - Unlocked users

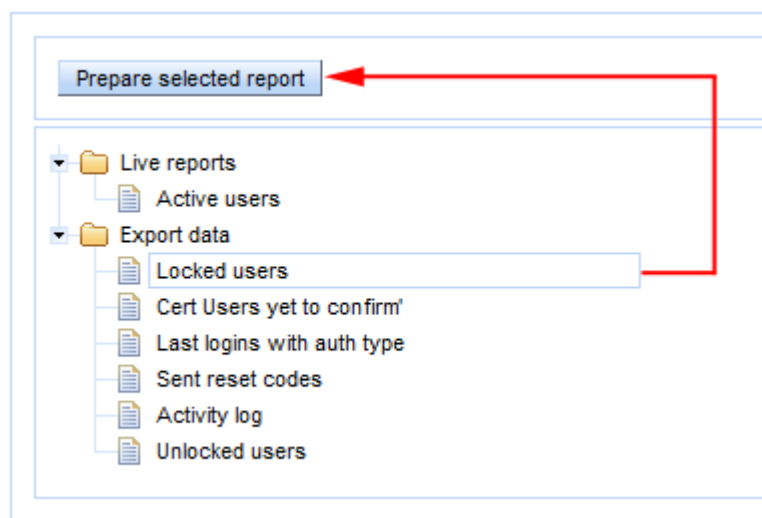
The 'Reports' tab allows Administrators, Operators and other personnel with the appropriate security role to view and export multiple report types.

Reports tab - Table of Parameters		
Report Type		Description
Live reports	<i>Active Users</i>	Displays a log of all currently logged into the system users.
Export data	<i>Locked users</i>	Displays a log of all users who were locked for some reason for selected period of time.
	<i>Cert users yet to confirm</i>	Displays a log of all users who installed a certificate, but never used it for logging into the system for selected period of time.
	<i>Last logins with auth type</i>	Displays a log of all users and their authentication types for selected period of time.
	<i>Sent reset codes</i>	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 reset code was sent, etc., but without the actual reset code sent).
	<i>Activity log</i>	Displays a log of all actions for selected period of time.
	<i>Unlocked users</i>	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:

Conditions for report Locked users

Generate report

Period

Select date from

May, 2009						
<<	<				>	>>
Sun	Mon	Tue	Wed	Thu	Fri	Sat
18	26	27	28	29	30	1
19	3	4	5	6	7	8
20	10	11	12	13	14	15
21	17	18	19	20	21	22
22	24	25	26	27	28	29
23	31	1	2	3	4	5
May 21, 2009			Clean		Today	

Select date to

May, 2009						
<<	<				>	>>
Sun	Mon	Tue	Wed	Thu	Fri	Sat
18	26	27	28	29	30	1
19	3	4	5	6	7	8
20	10	11	12	13	14	15
21	17	18	19	20	21	22
22	24	25	26	27	28	29
23	31	1	2	3	4	5
May 21, 2009			Clean		Today	

Note: For 'Activity log' report you must also select a country (see screenshot below).

Conditions for report Activity log

Generate report

Countries Period

Select needed countries

IL Israel
IT Italy
JM Jamaica
JP Japan
JO Jordan
KZ Kazakhstan
KI Kiribati

Copy all

Copy

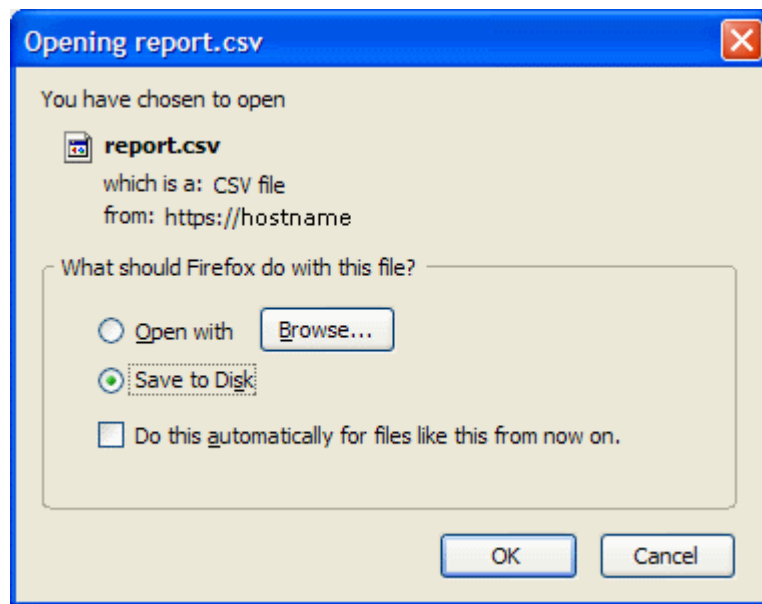
Remove

Remove All

ZW Zimbabwe
KE Kenya

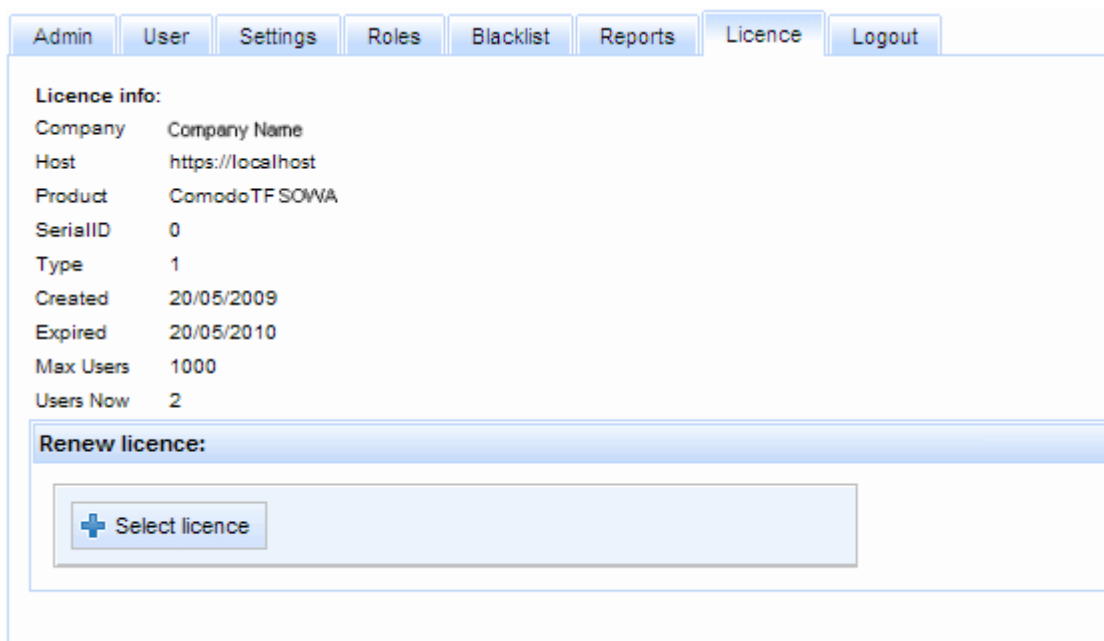
- Click the 'Generate report' button in the upper left corner of the dialog.

5. Download and save the generated report (.csv format).



8. The 'License' Tab

The 'License' tab displays the current Comodo TFSOWA license information.



Admin User Settings Roles Blacklist Reports Licence Logout

Licence info:

Company Company Name

Host https://localhost

Product ComodoTF SOWA

SerialID 0

Type 1

Created 20/05/2009

Expired 20/05/2010

Max Users 1000

Users Now 2

Renew licence:

+ Select licence

License tab - Table of Parameters	
Field	Description
Company	Displays the company's name.
Host	Displays the host name of Comodo TF SOWA 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:

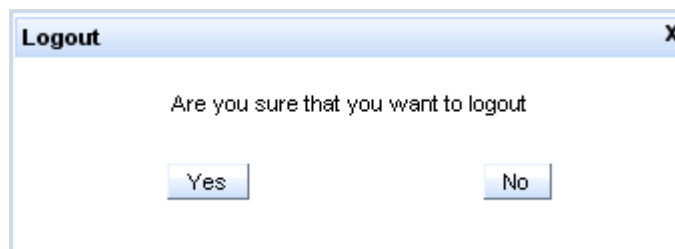
1. Save the license file to your computer;
2. In the 'License' section of Comodo TF SOWA interface press 'Select License' button;
3. Browse to and select the license file you saved previously.

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 SOWA server for the changes to take effect.

9. Logging out of Comodo TF for SharePoint and OWA

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



10. FAQ

1. **Can't use AOL browser to install security cookie or the certificate.**

After logging in to AOL ask the customer to minimize AOL and open Internet Explorer (IE) to set up the Security Cookie or the Certificate. After they set this up in IE they will be able to use AOL to access system.

2. **Can't use the back end website in Quicken to install security cookie or the certificate.**

Perform the cookie or certificate installation in Internet Explorer first, then use Quicken to access on-line back end system.

3. **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.

4. **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 cookies/certificates on it's own, OR customers should review the online FAQ where we have added additional instructions for Safari users.

5. **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 checkbox.

6. **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.

7. **Customer has Safari Browser with multiple login ID's. With one login ID they can login using the cookie/certificate but cannot find the cookie/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.

8. **After time out when setting up challenge questions, user cannot 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.

525 Washington Blvd. Jersey City,
NJ 07310

United States

Tel: +1.888.256.2608

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>.

