



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

Software Version 2.4

Installation and Configuration Guide

Guide Version 2.4.011811

Table of Contents

1.Introduction to Comodo TF for SharePoint and OWA.....	4
1.1.Guide Structure.....	4
2.Installation.....	4
2.1.System Requirements.....	4
2.2.Windows.....	4
2.3.Linux/Unix/BSD.....	9
2.3.1.Console Installation.....	15
3.Upgrade.....	15
3.1.From 2.x to 2.4.....	15
3.2.From 1.x to 2.4.....	16
4.Configuration.....	17
4.1.Overview.....	17
4.2.Modifying Tomcat-cfg.xml file.....	17
4.2.1.Comodo Two Factor Container.....	17
4.2.1.1.Binding to Particular IP.....	17
4.2.1.2.Setting up HTTPS.....	17
4.2.1.3.Truststore.....	18
4.2.2.Admin Interface.....	18
4.2.2.1.Restricting Access.....	18
4.2.3.Clustering.....	18
4.2.4.Database Connection.....	20
4.2.4.1.Embedded (Derby).....	20
4.2.4.2.MS SQL 2000 & 2005.....	20
4.2.4.3.MySQL 4.x & 5.x.....	22
4.2.4.4.Oracle 8.x - 10.x.....	23
4.2.4.5.PostgreSQL 7.x & 8.x.....	25
4.3.Creating and Modifying \$hostnames.properties File.....	27
4.3.1.Certificate Authority Login Information.....	27
4.3.2.SMTP Server Configuration.....	27
4.3.3.Product Configuration.....	27
4.3.4.Configuration Options.....	28
4.4.Configure Standard Questions.....	35
4.5.Logs.....	35
4.5.1.Access.....	35
4.5.2.Comodo Two Factor SOWA.....	35
4.6.Starting/Stopping Comodo Two Factor SOWA.....	35
4.6.1.Windows.....	35
4.6.2.Linux/Unix/BSD.....	35
5.Integration.....	36
5.1.Intercept Rules.....	36
5.1.1.General Intercept Rules.....	36
5.1.2.Request Intercept Rules.....	37
5.1.3.Response Intercept Rules.....	37
5.1.4.Challenge rules.....	38
5.1.5.Request conditions summary.....	39
5.1.6.Response conditions summary.....	40
5.1.7.Settings summary.....	41

5.2.Examples.....	41
5.2.1.HTTP Authentication.....	42
5.2.2.URL_HASH (MacKeys).....	43
5.2.3.Proxy All Mode.....	43
6.Customization.....	44
6.1.Work Area.....	44
6.2.Styles.....	45
6.3.New User Screen.....	48
6.4.Text Changes.....	49
6.5.Using BackEnd headers and footers under inside BackEnd links.....	49
7.Getting Support.....	50
About Comodo.....	51

1. Introduction to Comodo TF for SharePoint and OWA

The Comodo TF for SharePoint and OWA (Comodo TF SOWA) service is a Multi Factor Authentication solution for secure access to confidential services. This document is intended for administrators wishing to install and host the Comodo TF SOWA solution on in-house servers.

1.1. Guide Structure

This guide is intended to take you through the step-by-step process of organization, configuration and use of Comodo TF SOWA for SharePoint and Outlook Web Access service.

- Section 1 - **Introduction**, 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 - **Installation**, contains detailed explanations on how to install Comodo TF SOWA service on **Windows** and **Linux/Unix** Operating Systems.
- Section 3 - **Upgrade**, covers the procedure for upgrading Comodo TF SOWA from previous versions.
- Section 4 - **Configuration** - contains detailed explanations on how to configure Comodo TF SOWA service. This section forms the main body of the guide and covers elements such as initial post-install configuration, instructions for connecting to database types, SMTP configuration, starting and shutting down Comodo TF SOWA and many other items relating to the configuration and customization of the installation.
- Section 5 - **Integration**, contains information and examples on how to integrate Comodo TF SOWA with web based applications in order to provide additional authentication layer(s).
- Section 6 - **Customization**, contains detailed explanations on how to configure and customize the end user interface. This includes information about how to modify the text and style of the default Comodo TF SOWA template in order to create custom login and setup pages for end users.
- Section 7 - **Getting Support**, contains information and links for getting product support
- Section 8 - **About Comodo** contains company and contact information.

2. Installation

2.1. System Requirements

Before you install Comodo TF SOWA service, please ensure that your server meets the system requirements listed in this section and you have read the installation instructions.

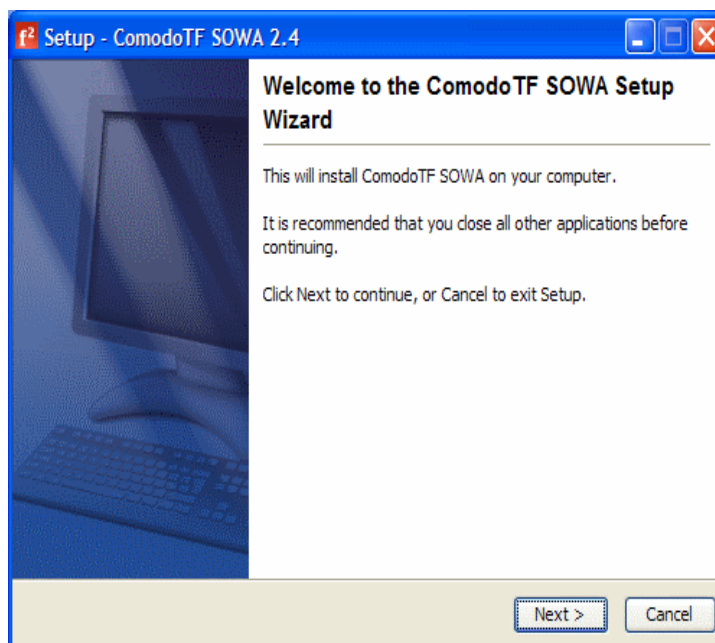
- Windows (XP to Windows 7), FreeBSD, Linux or Solaris Operating Systems.
- Sun Java Runtime environment (JRE) 1.6.11 or above

Note: For Unix and Solaris, you will need to install the JRE **before** Comodo TF SOWA is to be installed where as Windows and Linux will have the JRE installed during the installation of Comodo TF SOWA .

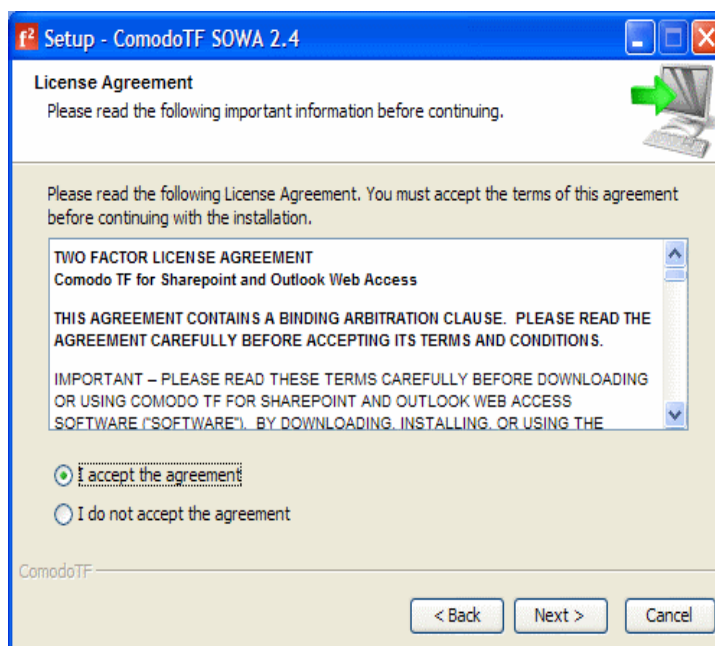
- 512MB of RAM
- 2 GB disk space
- Internet connection

2.2. Windows

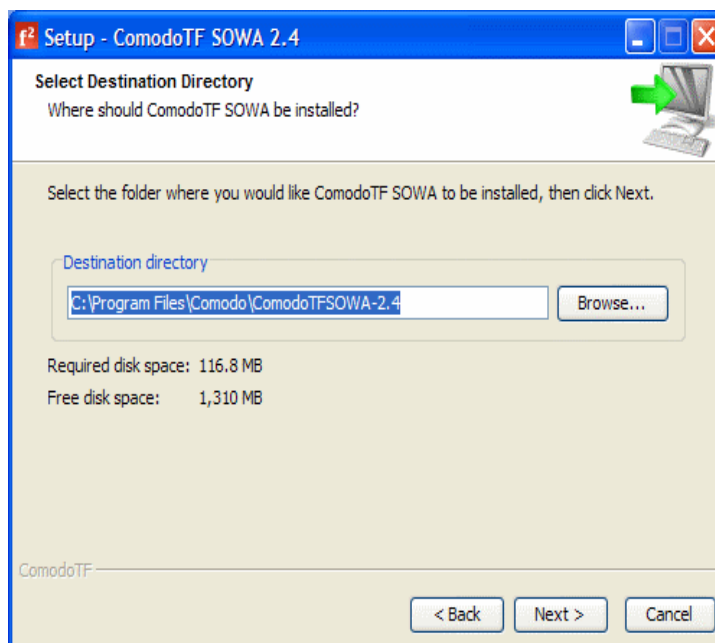
1. Run the installation file for Comodo TF SOWA and follow the instructions in the Comodo TF SOWA Setup Wizard.



2. Next you must complete the initialization phase by reading and accepting the license agreement. After you read the End-User License Agreement, tick off the 'I accept the agreement' radio button and click 'Next' to continue installation. If you decline, you cannot continue with the installation.

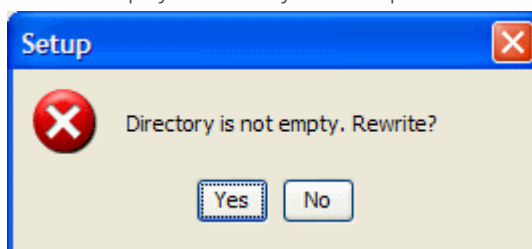


3. On the Destination Directory Selection screen, confirm the location of where to install Comodo TF SOWA. The default destination directory is the *C:\Program Files\Comodo\ComodoTFSOWA-x.x* (where *x.x* is the version number of Comodo TF SOWA to be installed).



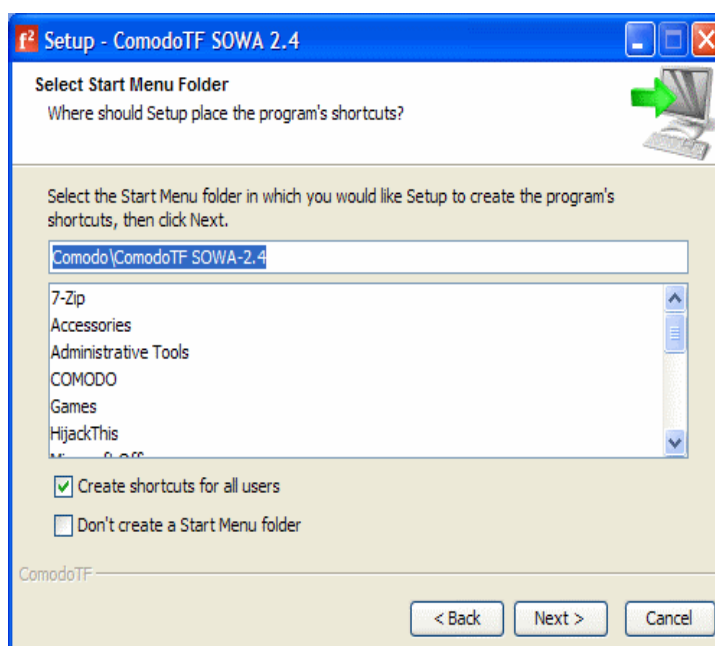
If you do not wish to install the Comodo TF SOWA files in the default location and want to select a different folder, click **Browse**, and choose another folder.

Note: Comodo TF SOWA Setup Wizard will display an error if you have specified a folder that is not presently empty.

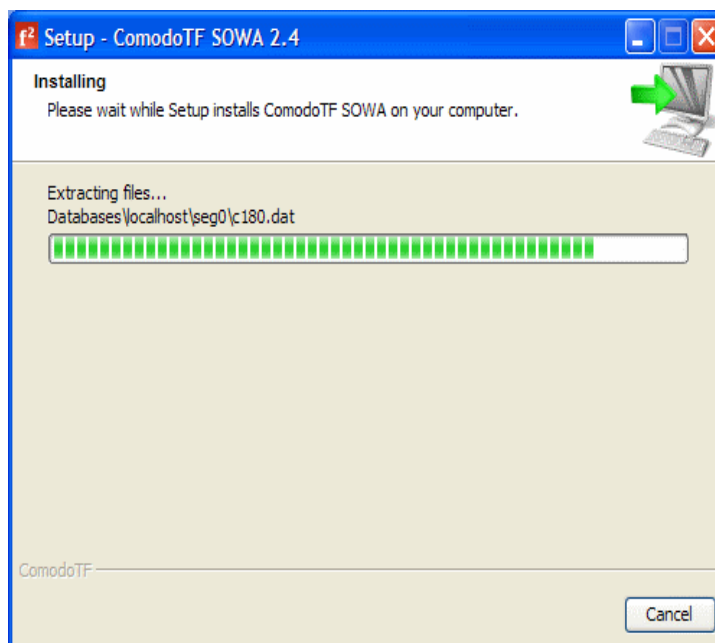


To select another destination folder click **No**. To use the selected folder click **Yes**. If Yes then Comodo TF SOWA files will overwrite **all files** in the folder.

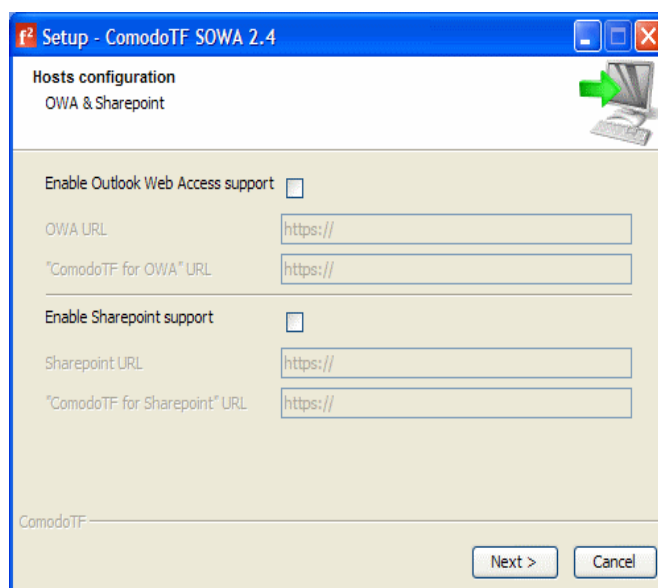
4. Next, select the Start Menu folder. Check the box against the needed option:



5. A setup status dialog box is displayed. You will see a progress bar indicating that files are being installed.



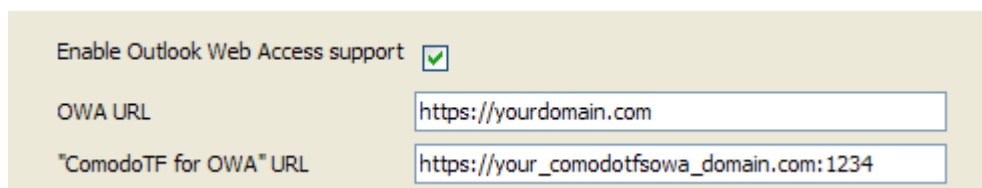
6. Next, check the boxes against the needed options:



Check the box against **Enable Outlook Web Access Support** if you wish to enable this service (you can use both OWA and MS SharePoint services):

OWA URL - Set host-name (or IP address) of your Outlook Web Access host

"Comodo TF for OWA" URL - Set host-name (or IP address) of your Comodo TF SOWA host



Check the box against **Enable SharePoint Support** if you wish to enable this service (you can use both OWA and MS SharePoint services):

SharePoint URL - Set host-name (or IP address) of your SharePoint host

"Comodo TF for SharePoint" URL - Set host-name (or IP address) of your Comodo TF SOWA host

Enable Sharepoint support	<input checked="" type="checkbox"/>
Sharepoint URL	<input type="text" value="https://yourdomain.com"/>
"ComodoTF for Sharepoint" URL	<input type="text" value="https://your_comodotfsowa_domain.com:1234"/>

Note: You can use both HTTP and HTTPS protocols. But we strongly recommend to use HTTPS to secure your information.

Click 'Next' to continue installation process.

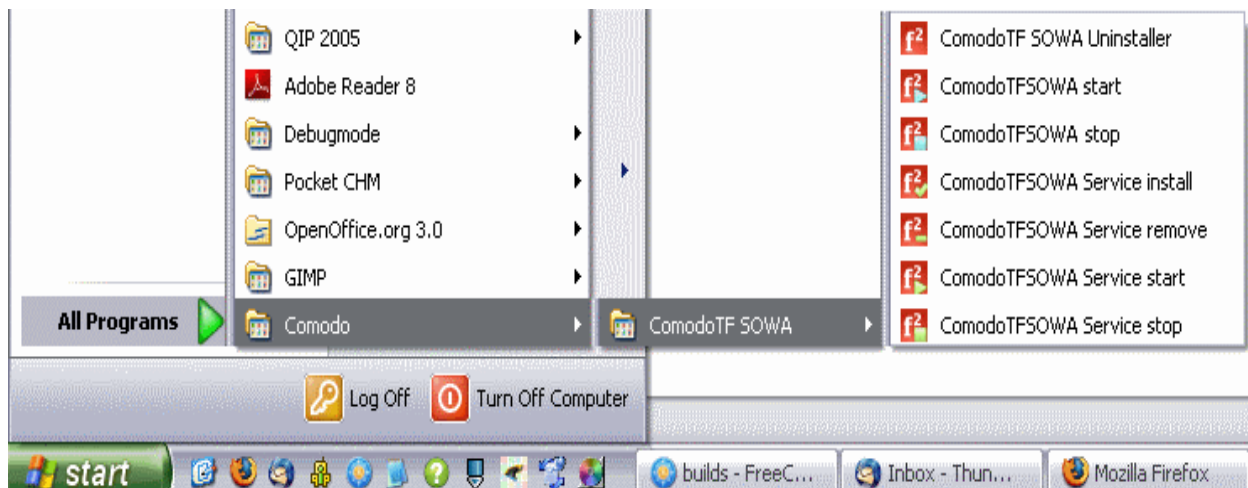
- Set email settings, these settings will be used in Comodo TF SOWA authentication procedure.

- If you want to run Comodo TF SOWA as Windows service, select the check box **Install service** 'ComodoTFSOWA2.4'.

9. Click 'Finish' to complete installation process and initial configuration.



Now you can start Comodo TF SOWA service from Windows Start menu.



Note: If you want to run Comodo TF SOWA service manually from the **Start Menu**, you should have full administrative rights on the server.

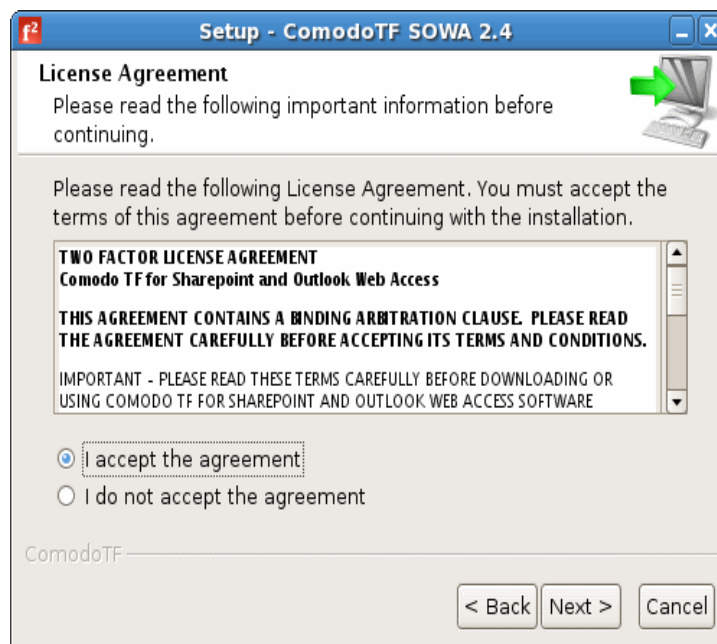
2.3. Linux/Unix/BSD

This section shows you installation of Comodo TF SOWA server for Linux/Unix//Unix-like Operating Systems using a Graphical User Interface (GUI).

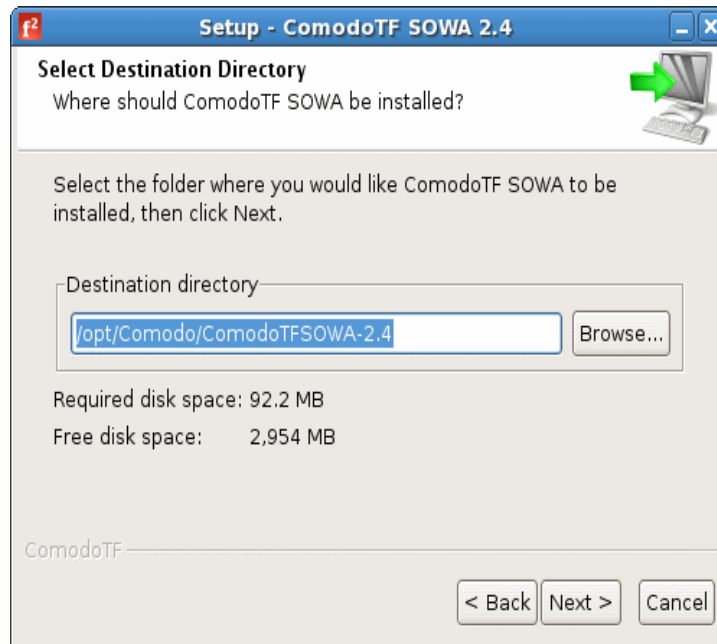
1. Run the installation file for Comodo TF SOWA and follow the instructions in the Comodo TF SOWA Setup Wizard.



2. Next you must complete the initialization phase by reading and accepting the license agreement. After you read the End-User License Agreement, tick off the 'I accept the agreement' radio button and click 'Next' to continue installation. If you decline, you cannot continue with the installation.



3. On the Destination Wizard page, confirm the location of the Comodo TF SOWA installation files.



To install the program in the default destination location, click 'Next'.

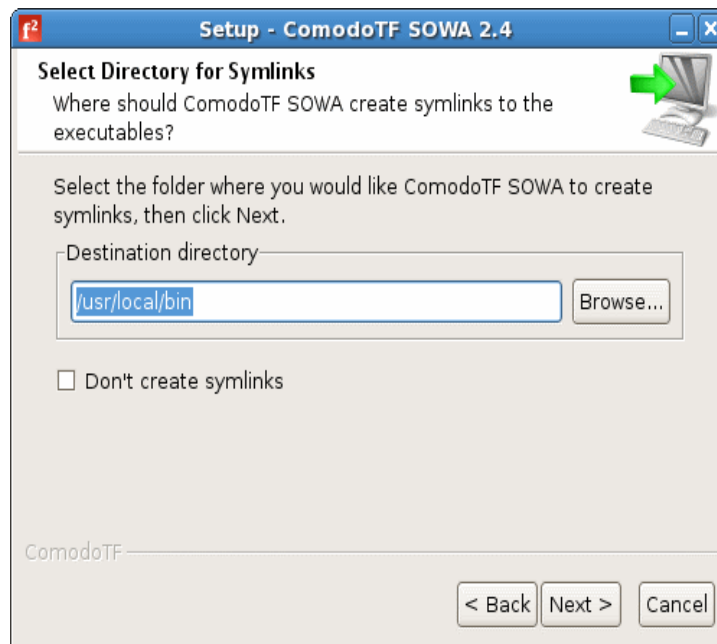
If you do not wish to install the Comodo TF SOWA files in the default location and want to select a different folder, click 'Browse', and choose another folder. Click 'Next' to continue with the installation process.

Note: Comodo TF SOWA Setup Wizard will inform you, if you have specified the existing folder information.

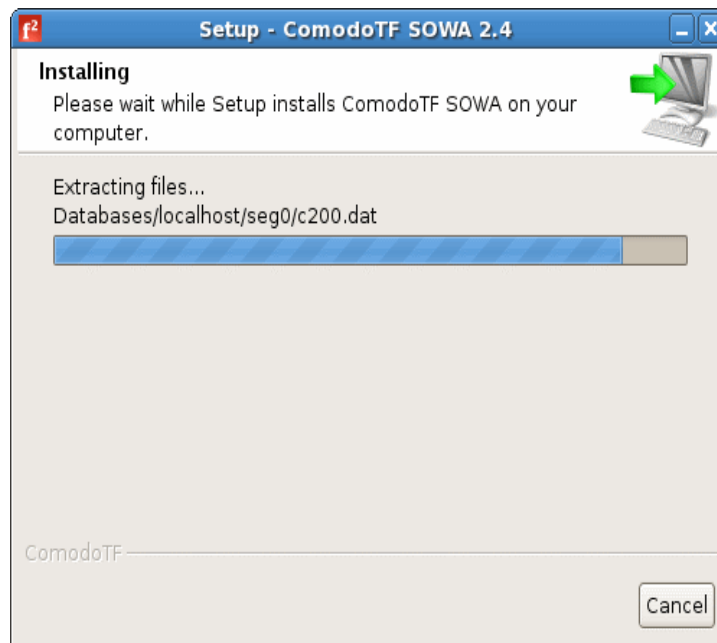


To select another destination folder click 'No'. To use the selected folder click 'Yes'. In this case all the files in the folder will be re-written.

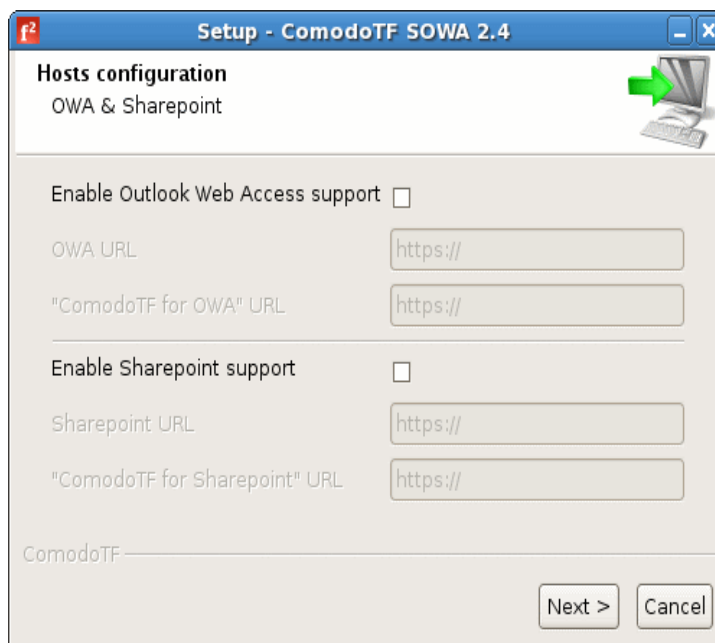
4. Next, select a folder to create the symlinks.



5. A setup status dialog box is displayed. You will see a progress bar indicating that files are being installed.



6. Next, check the boxes against the required options:



Check the box against **Enable Outlook Web Access Support** if you wish to enable this service (you can use both OWA and MS SharePoint services):

OWA URL - Set host-name (or IP address) of your Outlook Web Access host

'ComodoTF for OWA' URL - Set host-name (or IP address) of your Comodo TF SOWA host

Enable Outlook Web Access support ☒

OWA URL

"ComodoTF for OWA" URL

- Check the box against **Enable SharePoint Support** if you wish to enable this service (you can use both OWA and MS SharePoint services):

SharePoint URL - Set host-name (or IP address) of your SharePoint host

"ComodoTF for SharePoint" URL - Set host-name (or IP address) of your Comodo TF SOWA host

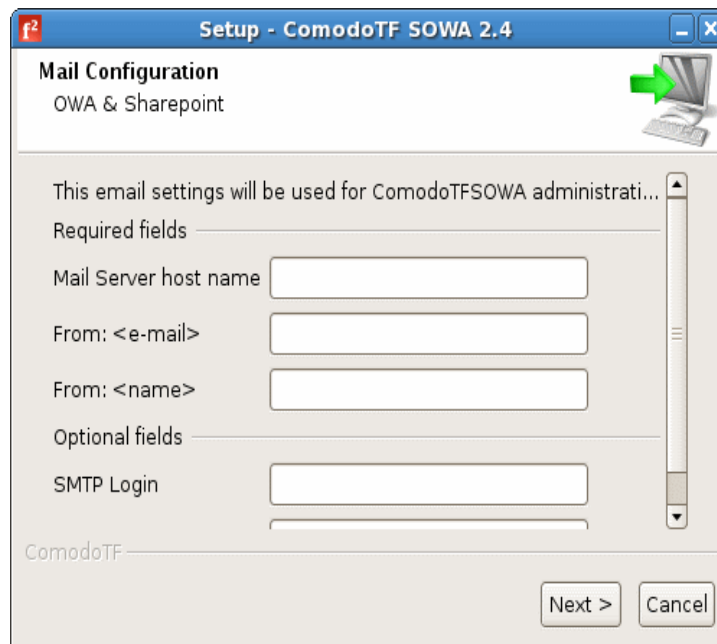
Enable Sharepoint support ☒

Sharepoint URL

"ComodoTF for Sharepoint" URL

Note: You can use both HTTP and HTTPS protocols. But we strongly recommend to use HTTPS to secure your information.

7. Configure email settings, these settings will be used in Comodo TF SOWA authentication procedure.



8. A dialog indicating the creation of daemons for setting Comodo TF SOWA as a start/stop service will be displayed.



Click 'Next'.

Note / Tip: To configure Comodo TF SOWA as a start-up service, you have to manually add it in autostart using start/stop scripts from **\$(ComodoTFSOWA.)/bin** folder.

9. Click 'Finish' to complete installation.



2.3.1. Console Installation

In order to launch installation of ComodoTF SOWA on Linux/Unix/Unix-like Operating Systems without GUI execute:

Linux: `./ComodoTFSOWA-x.x-Linux.sh -c` or `sh ComodoTFSOWA-x.x-Linux.sh`

Unix: `./ComodoTFSOWA-x.x-Unix.sh -c` or `sh ComodoTFSOWA-x.x-Unix.sh`

Note: x.x is the version of Comodo TF SOWA that is to be installed.

3. Upgrade

If you already have a previous version of ComodoTF SOWA, you can upgrade it to Comodo TF SOWA version 2.4 by following the instructions given below. Before upgrade, please make sure the target machine meets the hardware and software prerequisites. Full details regarding system requirements can be found in the section, **System Requirements**.

Click the following links for detailed explanations on upgrading to 2.4 from versions 2.x, and 1.x.

- [Upgrading ComodoTF SOWA version 2.x to ComodoTF SOWA version 2.4](#)
- [Upgrading ComodoTF SOWA version 1.x to ComodoTF SOWA version 2.4](#)

3.1. From 2.x to 2.4

If you are presently using ComodoTF SOWA 2.x, then upgrading is easy. ComodoTF SOWA's Installation Wizard will upgrade a current installation to 2.4, but to safeguard against data loss and to provide for testing both instances side-by-side, we recommend upgrading in the following manner.

1. Stop ComodoTF SOWA.
2. Copy the following files from /conf/ folder on current ComodoTF SOWA 2.x installation:
 - tomcat-cfg.xml
 - **\$hostname**.properties
 - rules.**\$hostname**.xml

Note: **\$hostname** is the value given in **tomcat-cfg.xml** for the hostname attribute of the <tf> tag. Example: <tf hostname="hostname">; hostname.properties

Note: If your *config.properties* define LANG key then you have to update it.

For example in case of 'LANG=lang.en;lang.callback_en;lang.customfile' you should:

1. Update this key with new value:
 - remove '.en' and '_en' from the end of all subvalues
 - add lang.certenroll subvalue

you should have now "LANG=lang.;lang.callback;lang.customfile;lang.certenroll"

2. Rename physical file *ComodoTF/lang/customfile.properties* to *customfile_en.properties*

3.2. From 1.x to 2.4

1. Stop ComodoTF SOWA
2. Run Comodo TF SOWA version 2.4 installation file and install into a new directory.

Note for Linux/Unix Users: If you don't have GUI access, remember to run the installation file with the - c option.

3. Make a duplicate/backup of **tomcat-cfg.xml**.
4. Open and modify **tomcat-cfg.xml**
 - a) Fill <tf hostname='localhost' appBase='webapps' sslPort='8443'> with values from 1.x's */conf/server.xml* <Connector> tag.

Note: You can customize the hostname attribute of the <tf> tag. For more information please see the section **Configuration**.

b) If you are not using embedded database uncomment and fill <database> tag with values from 1.x's */conf/Catalina/localhost/comodotf.xml* <Resource> tag. For More Information on how to configure the <database> tag please see the section **Configuration**.

Important Note: Remember to backup your existing Database **before** upgrading! Failure to do so may result in data loss!!!

5. Copy the following files from the old version:
 - a) **Database** - If using Derby, the embedded Java database, then copy the Database directory (folder and all) from the 1.x folder to the 2.x main directory.
 - b) **Config*.properties** - Copy from */shared/classes/config*.properties* to */conf/\$hostname.properties*.
 - c) **Header and Footer** - Copy from 1.x's */etc/*.header* and */*.footer* into 2.x's */etc/* folder as *\$hostname.header* and *\$hostname.footer*

Note: If your **config.properties** file defines LANG key, then you MUST update it for use on ComodoTF SOWA 2.x.

Example: LANG=lang.en;lang.callback_en;

1. Update this key with new value:
 - remove '.en' and '_en' from the end of all subvalues
 - add lang.certenroll subvalue

you should now have: LANG=lang.;lang.callback;lang.certenroll

2. Rename physical file *ComodoTF/conf/lang/customfile.properties* to *customfile_en.properties*

6. Create new rules.*\$hostname.xml* using instructions found later in the guide (See **Section 5 Integration**) or please **contact the Comodo TF support team**. Don't use old rules.xml from ComodoTF 1.x as this format is incompatible with ComodoTF SOWA 2.x

Note: *\$hostname* is the value given in **Step 4a** for the hostname attribute of the <tf> tag. Example: <tf hostname='hostname'>; hostname.properties.

4. Configuration

4.1. Overview

By default, Comodo TF for SharePoint and Outlook Web Access is shipped pre-configured. You will need to alter following to finish the configuration.

Edit file:

ComodoTFSOWA-xx/conf/localhost.properties

Set NEW_HOST - URL through which your BackEnd site will be available through Comodo TF SOWA during testing phase

Set SUB - the substitution rules that will substitute OLD_HOST with NEW_HOST

Set MULTI_HOST_MODE - this provides ability to work with back-end systems deployed on more than one host. Possible values(yes/no). Default: No

The header & footer files are located in:

- ComodoTFSOWA-xx/etc/sql/empty.header;
- ComodoTFSOWA-xx/etc/sql/empty.footer.

You can change them to improve the look & feel of injected pages.

For further customization, edit the files *ComodoTFSOWA-xx/conf/tomcat-cfg.xml* and *ComodoTFSOWA-xx/conf/localhost.properties*. as explained below.

4.2. Modifying Tomcat-cfg.xml file

If you want to install SSL certificate, configure the IP restrictions, HTTPS connection ports, access restriction to the Admin interface, Database connections etc, you need to edit the file *ComodoTFSOWA-xx/conf/tomcat-cfg.xml*.

4.2.1. Comodo Two Factor Container

4.2.1.1. Binding to Particular IP

By default ComodoTF SOWA binds to all IPs on ports 80 and 443. If you want to change it so that Comodo TF SOWA binds to particular IP only, add address attribute to <tf> tag in *ComodoTFSOWA-xx/conf/tomcat-cfg.xml*. Like:

```
<tf hostname='localhost' address='192.168.1.1'
...
>
```

Important Note: Remember to rename:

license.\$hostname.xml,\$hostname.properties,\$hostname.truststore,\$hostname.keystore, to the hostname defined within the <tf> tag in 'ComodoTFSOWA-xx/conf/tomcat-cfg.xml'.

4.2.1.2. Setting up HTTPS

By default Comodo TF SOWA uses port 443 for HTTPS. If you need to change this port at any time, edit file: *ComodoTFSOWA-xx/conf/tomcat-cfg.xml*.

You will need to modify line:

```
<tf
```

```
sslPort='443' >
```

4.2.1.3. Truststore

Comodo TF SOWA defines 'truststore' which allows us to specify the trusted range of certificates, so that only certificates issued by a specifies Root Authority would be accepted.

The truststore is located in *ComodoTFSOWA-xx/conf/\$hostname.truststore* and comes pre-configured.

4.2.2. Admin Interface

To access admin interface for Comodo TF SOWA, enter in your browser: *https://SERVER/comodotf*
Default login/password: *admin/admin*.

4.2.2.1. Restricting Access

You can restrict access to admin interface by editing *ComodoTFSOWA-xx/conf/tomcat-cfg.xml* file.
Uncomment

```
< admin> <allow> ip </allow>
<allow> ip </allow>
<deny> ip </deny>
</admin >
```

The valve will allow access by all IPs specified in allow attribute, but those specified in deny attribute.

4.2.3. Clustering

By installing two instances of Comodo TF SOWA pointed to the same database, you can achieve clustered setup. The system will be setup in active/active mode. You can add as many servers as you want to the cluster.

Important:

- i. Note that all Comodo TF SOWA nodes MUST have their own application copy on the same relative path!
- ii. Make sure that all Comodo TF SOWA nodes have the same version number!

To configure cluster

1. Install and configure load balancer. Note that load balancer is not included in ComodoTF SOWA package. You can use any hardware, apache with mod_jk or other load balancer;
2. Open tomcat-cfg.xml file;
3. uncomment <cluster> and <databaseCacheCluster> tags;
4. Configure <cluster> and <databaseCacheCluster> tags to match your network and load balancer configuration.

The configuration details and examples are given below.

1. <cluster> tag - Session clustering.

Examples:

```
<cluster jvmRoute='tomcat1'
    receiverPort='4002'
    protocol='ajp'
    ajpPort='6789'>
    <multicast />
</cluster>

<cluster jvmRoute='tomcat1'
    protocol='https'
    receiverPort='4002'>
    <staticMember address='192.168.75.31' port='4002' />
    <staticMember address='10.85.1.' port='5555' />
</cluster>
```

Attributes :

jvmRoute - In case of 'ajp' protocol attribute should match corresponding worker name in workers.properties in mod_jk (Apache). In other cases it is used just for node identification (Can be any unique name in cluster group).

receiverPort - TCP port that listens for replication messages. Use any available port.

Note:

- The port should be unique among other tomcat nodes in case of vertical clustering.
- In case of static cluster members, make sure that receiverPort is the same as port attribute for <staticMember> tag representing current node.

protocol - cluster protocol type - either 'ajp', 'memory', 'https'.

ajpPort - port for ajp connector (load balancer requests) to listen. Use only with 'ajp' protocol. In case of 'https' protocol, <tf sslPort> will be used automatically for load balancer requests.

Child tags: <multicast> OR <staticMember>

<multicast> - Used for one-to-many server communication to broadcast the availability of services via IP multicast. Can be specified once, does not work together with <staticMember>.

Example:

```
<multicast multicastAddress="228.1.1.5" multicastPort="33567" />
```

Attributes:

multicastAddress - (Optional) The multicast address that the membership will broadcast its presence and listen for other heartbeats on. The default value is 228.0.0.4 Make sure your network is enabled for multicast traffic.

multicastPort : (Optional) The multicast port, the default value is 45564

<staticMember> - Used for many-to-many servers communication to broadcast the availability of services via TCP. Can be specified many times, does not work together with <multicast>

Note: <staticMember> list should include current node where port = <cluster receiverPort...> and address = node IP

Example:

```
<staticMember address='228.1.1.5' port='33567' aliveTime='500' uniqueId='{0,1,2,3,4,5,6,7,8,9}'
domain='tomcat-cluster' />
```

Attributes:

address - The host (or network interface) that this static member listens for cluster messages.

port - The port that this static member listens to for cluster messages.

aliveTime - (Optional) The number of milliseconds since this members was created, is kept track of using the start time

uniqueId - (Optional) A universally unique id for this static member. The values must be 16 bytes.

domain - (Optional) The logical cluster domain for this this static member listens for cluster messages.

I. <databaseCacheCluster> tag - Database Cache Clustering.

Examples:

```
<databaseCacheCluster
  receiverPort='4005'>
  <multicast multicastAddress='231.12.21.132' multicastPort='45566' />
</databaseCacheCluster>
```

```
<databaseCacheCluster
  receiverPort='4005'>
  <staticMember address='192.168.75.31' port='4444' />
  <staticMember address='10.85.1.2' port='5555' />
</databaseCacheCluster>
```

Attributes:

receiverPort - TCP port listening for replication messages.

Note: The port should be unique among other tomcat nodes in case of vertical clustering.

Child tags: <multicast> OR <staticMember>

<multicast> - Used for one-to-many server communication to broadcast the availability of services via IP multicast
. Can be specified once, does not work together with <staticMember>.

Example:

```
<multicast multicastAddress="228.1.1.5" multicastPort="33567" />
```

Attributes:

multicastAddress - (Optional) The multicast address that the membership will broadcast its presence and listen for other heartbeats on. The default value is 231.12.21.132 Make sure your network is enabled for multicast traffic.

multicastPort : (Optional) The multicast port, the default value is 45566

bindAddress : (Optional) The bind address which should be used by this transport

bindPort : (Optional) The port to which the transport binds.

bindInterface : (Optional) The interface (NIC) which should be used by this transport

<staticMember> - Used for many-to-many servers communication to broadcast the availability of services via TCP.
Can be specified many times, but does not work together with <multicast>.

Example:

```
<staticMember address="228.1.1.5" port="33567"/>
```

Attributes:

address - The host (or network interface) that this static member listens for cluster messages.

port - The port that this static member listens to for cluster messages.

4.2.4. Database Connection

4.2.4.1. Embedded (Derby)

If you are using embedded database and need to connect to it, you will have to stop Comodo TF SOWA first.
Then use the next commands:

1. \$ cd ComodoTFSOWA-xx/Databases
2. \$ java -cp ../lib/derby.jar:../lib/derbytools.jar org.apache.derby.tools.ij
3. ij> connect 'jdbc:derby:default';

Note: Make sure you have stopped Comodo TF SOWA prior your attempt to connect to database.

When you want to disconnect, execute:

```
ij> exit;
```

4.2.4.2. MS SQL 2000 & 2005

1. Create database for Comodo TF SOWA.
2. Load schema: *ComodoTFSOWA-xx/etc/sql/schema_mssql.sql*
3. Download JDBC driver for MS SQL and copy it to *ComodoTFSOWA-xx/lib* (you need *msbase.jar*, *mssqlserver.jar*, *msutil.jar* files). You can download them from: <http://www.microsoft.com/downloads/details.aspx?familyid=4f8f2f01-1ed7-4c4d-8f7b-3d47969e66ae&displaylang=en>
4. Edit file *ComodoTFSOWA-xx/conf/tomcat-cfg.xml*.

5. Comment out <database type='embedded' />
6. Uncomment and change <database driverClassName="" url="" username="" password=""/>
Change username to MS SQL username
Change password to MS SQL password
Change driverClassName to: com.microsoft.sqlserver.jdbc.SQLServerDriver
Change url to: jdbc:sqlserver://HOST:PORT;databaseName=DATABASE_NAME

Definition of Terms	
HOST	hostname of MS SQL db
PORT	MS SQL port (usually 1433)
DATABASE_NAME	database name for Comodo TF SOWA

Set the values for the parameters:

- logAbandoned;
- removeAbandoned;
- removeAbandonedTimeout;
- maxActive;
- maxIdle;
- maxWait;
- poolSize;
- validationQuery;
- testOnBorrow.

as given in the table below.

Parameter	Possible Values	Description
logAbandoned	Boolean (true/false)	If set to false, the information on abandoned database connections will not be logged. Default = True
removeAbandoned	Boolean	If set to false, the abandoned database connections will not be removed. Default = True
removeAbandonedTimeout	Numeric	Specifies the timeout period (in milliseconds) for removing abandoned database connection. Default = 12600 Note: This setting will be active only if removeAbandoned is set to True.
maxActive	Numeric	Specifies the number of allowed active connections. Default = 10
maxIdle	Numeric	Specifies the number of allowed idle connections. Default = 5
maxWait	Numeric	Specifies the maximum waiting time (in milliseconds) for database connection. Default = -1 (unlimited)
poolSize	Numeric	Specifies the number of pooled connections. Default = 10

Parameter	Possible Values	Description
validationQuery	<i>String</i>	Query used to determine if connection to database server is stalled or broken before executing any SQL query. Default = null
testOnBorrow.	<i>Boolean</i>	If 'true' validation query is executed (if set). Default value = true

Example:

```
<database driverClassName='com.microsoft.sqlserver.jdbc.SQLServerDriver'
url='jdbc:sqlserver://<HOST>:<PORT>;databaseName=<DATABASE_NAME>'
username='<MS SQL username>' password='<MS SQL password>'
logAbandoned='true'
removeAbandoned='true'
removeAbandonedTimeout='30'
maxActive='100'
maxIdle='30'
maxWait='10000'
validationQuery='null'
testOnBorrow='false'
/>
```

4.2.4.3. MySQL 4.x & 5.x

1. Create database for Comodo TF SOWA.
2. Load schema: *ComodoTFSOWA-xx/etc/sql/schema_mysql.sql*
3. Download JDBC driver for MS SQL and copy it to *ComodoTFSOWA-xx/lib*. You can download it from:
<http://www.mysql.com/products/connector/j/>
* MySQL licensing fees might apply
4. Edit file *ComodoTFSOWA-xx/conf/tomcat-cfg.xml*.
5. Comment out `<database type='embedded' />`
6. Uncomment and change `<database driverClassName="" url="" username="" password="" />`
Change username to MySQL username
Change password to MySQL password
Change driverClassName to: `com.mysql.jdbc.Driver`
Change url to: `jdbc:mysql://HOST:PORT/DATABASE_NAME?autoReconnect=true`

Definition of Terms	
HOST	hostname of MySQL db
PORT	MySQL port (usually 3306)
DATABASE_NAME	database name for Comodo TF SOWA

Set the values for the parameters:

- logAbandoned;
- removeAbandoned;
- removeAbandonedTimeout;
- maxActive;
- maxIdle;
- maxWait;

- poolSize;
- clustered;
- validationQuery;
- testOnBorrow.

as given in the table below.

Parameter	Possible Values	Description
logAbandoned	Boolean (true/false)	If set to false, the information on abandoned database connections will not be logged. Default = True
removeAbandoned	Boolean	If set to false, the abandoned database connections will not be removed. Default = True
removeAbandonedTimeout	Numeric	Specifies the timeout period (in milliseconds) for removing abandoned database connection. Default = 12600 Note: This setting will be active only if removeAbandoned is set to True.
maxActive	Numeric	Specifies the number of allowed active connections. Default = 10
maxIdle	Numeric	Specifies the number of allowed idle connections. Default = 5
maxWait	Numeric	Specifies the maximum waiting time (in milliseconds) for database connection. Default = -1 (unlimited)
poolSize	Numeric	Specifies the number of pooled connections. Default = 10
clustered	Boolean	If set to true, the use of database cluster replication will be allowed. Default = False
validationQuery	String	Query used to determine if connection to database server is stalled or broken before executing any SQL query. Default = null
testOnBorrow.	Boolean	If 'true' validation query is executed (if set). Default value = true

Example:

```
<database driverClassName='com.mysql.jdbc.Driver'
url=' jdbc:mysql://<HOST>:<PORT>/<DATABASE_NAME>?autoReconnect=true'
username='<MySQL username>' password='<MySQL password>'
logAbandoned='true'
removeAbandoned='true'
removeAbandonedTimeout='30'
maxActive='100'
maxIdle='30'
maxWait='10000'
clustered='true'
validationQuery='null'
testOnBorrow='false'
/>
```

4.2.4.4. Oracle 8.x - 10.x

1. Create database for Comodo TF SOWA.

2. Load schema: *ComodoTFSOWA-xx/etc/sql/schema_oracle.sql*
3. Download Oracle Thin JDBC driver and copy it to *ComodoTFSOWA-xx/lib*. You can download it from:
http://www.oracle.com/technology/software/tech/java/sqlj_jdbc/index.html
4. Edit file *ComodoTFSOWA-xx/conf/tomcat-cfg.xml*
5. Comment out <database type='embedded' />
6. Uncomment and change <database driverClassName="" url="" username="" password="" />
Change username to Oracle username
Change password to Oracle password
Change driverClassName to: oracle.jdbc.driver.OracleDriver
Change url to: jdbc:oracle:thin:@HOST:PORT:SID

Definition of Terms	
HOST	hostname of Oracle db
PORT	Oracle port (usually 1521)
SID	The Oracle System Identifier that uniquely identifies Oracle instance

Set the values for the parameters:

- logAbandoned;
- removeAbandoned;
- removeAbandonedTimeout;
- maxActive;
- maxIdle;
- maxWait;
- poolSize;
- clustered;
- validationQuery;
- testOnBorrow.

as given in the table below.

Parameter	Possible Values	Description
logAbandoned	Boolean (true/false)	If set to false, the information on abandoned database connections will not be logged. Default = True
removeAbandoned	Boolean	If set to false, the abandoned database connections will not be removed. Default = True
removeAbandonedTimeout	Numeric	Specifies the timeout period (in milliseconds) for removing abandoned database connection. Default = 12600 Note: This setting will be active only if removeAbandoned is set to True.
maxActive	Numeric	Specifies the number of allowed active connections. Default = 10
maxIdle	Numeric	Specifies the number of allowed idle connections. Default = 5

Parameter	Possible Values	Description
maxWait	Numeric	Specifies the maximum waiting time (in milliseconds) for database connection. Default = -1 (unlimited)
poolSize	Numeric	Specifies the number of pooled connections. Default = 10
clustered	Boolean	If set to true, the use of database cluster replication will be allowed. Default = False
validationQuery	String	Query used to determine if connection to database server is stalled or broken before executing any SQL query. Default = null
testOnBorrow.	Boolean	If "true" validation query is executed (if set). Default value = true

Example:

```

<database driverClassName='oracle.jdbc.driver.OracleDriver'
url=' jdbc:oracle:thin:@<HOST>:<PORT>:<SID>'
username='<Oracle username>' password='<Oracle password>'
logAbandoned="true"
removeAbandoned="true"
removeAbandonedTimeout="30"
maxActive='100'
maxIdle='30'
maxWait='10000'
clustered='true'
validationQuery='null'
testOnBorrow='false'
/>

```

4.2.4.5. PostgreSQL 7.x & 8.x

- Create database for Comodo TF SOWA.
*You might have to enable postgresql to listen on TCP/IP port.
See <http://www.postgresql.org/docs/8.1/static/runtime-config-connection.html> for more information.
Download JDBC driver for PostgreSQL and copy it to *ComodoTFSOWA-xx/lib*. It can be downloaded at <http://jdbc.postgresql.org/download.html>
- Load schema: *ComodoTFSOWA-xx/etc/sql/schema_postgresql.sql*
- Edit file *ComodoTFSOWA-xx/tomcat-cfg.xml*.
- Comment out <database type="embedded" />
- Uncomment and change <database driverClassName="" url="" username="" password="" />
Change username to PostgreSQL username
Change password to PostgreSQL password
Change driverClassName to: org.postgresql.Driver
Change url to: jdbc:postgresql://HOST:PORT/DATABASE_NAME

Definition of Terms	
HOST	hostname of PostgreSQL db
PORT	MS SQL port (usually 5432)
DATABASE_NAME	database name for Comodo TF SOWA

Set the values for the parameters:

- logAbandoned;
- removeAbandoned;
- removeAbandonedTimeout;
- maxActive;
- maxIdle;
- maxWait;
- poolSize;
- clustered;
- validationQuery;
- testOnBorrow.

as given in the table below.

Parameter	Possible Values	Description
logAbandoned	Boolean (true/false)	If set to false, the information on abandoned database connections will not be logged. Default = True
removeAbandoned	Boolean	If set to false, the abandoned database connections will not be removed. Default = True
removeAbandonedTimeout	Numeric	Specifies the timeout period (in milliseconds) for removing abandoned database connection. Default = 12600 Note: This setting will be active only if removeAbandoned is set to True.
maxActive	Numeric	Specifies the number of allowed active connections. Default = 10
maxIdle	Numeric	Specifies the number of allowed idle connections. Default = 5
maxWait	Numeric	Specifies the maximum waiting time (in milliseconds) for database connection. Default = -1 (unlimited)
poolSize	Numeric	Specifies the number of pooled connections. Default = 10
clustered	Boolean	If set to true, the use of database cluster replication will be allowed. Default = False
validationQuery	String	Query used to determine if connection to database server is stalled or broken before executing any SQL query. Default = null
testOnBorrow.	Boolean	If "true" validation query is executed (if set). Default value = true

Example:

```
<database driverClassName="org.postgresql.Driver"
url=" jdbc:postgresql://<HOST>:<PORT>/<DATABASE_NAME>"
username="<PostgreSQL username>" password="< PostgreSQL password>"
logAbandoned="true"
removeAbandoned="true"
removeAbandonedTimeout="30"
maxActive="100"
maxIdle="30"
```

```
maxWait="10000"  
clustered="true"  
validationQuery="null"  
testOnBorrow="false"  
</>
```

4.3. Creating and Modifying \$hostnames.properties File

If you want to configure the login options, mail server options etc., you need to edit the file *ComodoTFSOWA-xx/conf/localhost.properties*.

4.3.1. Certificate Authority Login Information

Your certificate authority login information will be provided to you by your Sales representative. To change your Comodo CA password, go to: <http://www.comodo.com> and login using your existing UN/PW combination. Once inside your secure account you can change your password.

4.3.2. SMTP Server Configuration

If you want Comodo TF SOWA to allow your customers to re-set security questions/answers, you will need to point Comodo TF SOWA to a working mail server.

Edit file *ComodoTFSOWA-xx/conf/localhost.properties*:

1. Set USE_CLIENTS_EMAIL=yes; (no - means no email reset; default = yes).
2. Set FROM_NAME to name to appear in customer's mail client as FROM field.
3. Set FROM_ADDRESS to email address from which emails will be sent.
4. Set ONETIME_PASSWORD_MESSAGE_SUBJECT to subject of the reset email.
5. Set SMTP_HOST to mail server host name
6. If your server requires SMTP AUTH in order to send email, set fields SMTP_LOGIN and SMTP_PASSWORD. Otherwise these fields can be omitted.

SSL/TLS Settings

If your server makes use of SSL or TLS, then use a set of the following parameters:

SSL

1. Set SMTP_USE_SSL = true, if you want to use secure SSL protocol to send your mails (false - means SSL protocol will not be used).
2. Set SMTP_SSL_PORT to the port number of your SMTP server when using SSL connections (usually 465).

TLS

1. Set SMTP_USE_TLS = true if you want to use TLS protocol to send your mails (false - means TLS protocol will not be used)
2. Set SMTP_TLS_PORT to the port number of your SMTP server when using TLS connections (usually 587).

Note: You can configure either SSL or TLS protocol for sending emails - but not both at the same time.

4.3.3. Product Configuration

If you want to use the same domain name for your back-end system as prior to Comodo TF SOWA install:

1. Setup hosts file on your server to point your back-end site domain name to real (old) back-end site IP.

Note: You might also need to setup the hosts file on the old back-end site itself, if the server needs to communicate with itself using domain name.

2. Change DNS to point domain to Comodo TF SOWA server.
3. Change NEW_HOST/SUB to match OLD_HOST.

If you want to use a new domain name for back-end system:

4. Change DNS to point that domain to Comodo TF SOWA server.
5. Change NEW_HOST/SUB to match new domain.

4.3.4. Configuration Options

The runtime configuration of Comodo TF SOWA can be altered by editing 'ComodoTFSOWA-xx/conf/\$hostname.properties', where \$hostname is defined within the <tf> tag in *ComodoTFSOWA-xx/conf/tomcat-cfg.xml*.

This configuration file controls functionality of the software. For any changes to take affect, software Comodo TF SOWA has to be restarted after the change is made.

Configuration Options		
Option Name	Possible Values	Description
Host Configuration		
OLD_HOST	String	IP address or Fully Qualified Domain Name (FQDN) of the secure website server, for use in request substitutions.
NEW_HOST	String	IP address or FQDN of the Comodo TF server, for use in request substitutions.
SEPARATOR	Character	Character used for separating values in the SUB key (explained below). Example: To use 'I' as the separator, the key should be SEPARATOR=I
SUB	String	Substitute pairs of hosts delimited by the separator character defined in the SEPARATOR key, for use in response substitutions. Example: SUB=https://domainname.comIhttps://mytfhost:8443Isecure-domainname.comImytfhost:8443)
MULTI_HOST_MODE	Logical (yes or no)	If set to yes, enables working with secure web service having different host names. All the hosts must be added in SUB key. Example: host1=aaa.com host2=bbb.com Keys in configuration properties: MULTI_HOST_MODE=Yes SUB=aaa.comImytfhost/aaalbbb.comImytfhost/bbb
DEFAULT_DOMAIN	String	If this key is set, all usernames will be converted to standard form username@default_domain_value. Use it when you want user 'test', 'domain/test', 'domain\test' and 'test@domain' be treated

Configuration Options		
Option Name	Possible Values	Description
		as one user. Default = no conversion
Security Questions and Answers		
QUESTION_TYPE	Standard_Multi	Standard set of questions, as defined in questions table
	Custom_Multi	Custom question entered by client
	Mixed_Multi	Allows both, custom and pre-defined (Standard_Multi) questions
NUMBER_OF_QUESTIONS	Numeric	Number of questions/answers for customer to enter. Default = 3
MAX_FATTEMPTS	Numeric	The number of re-tries for customer to enter security answer. Once the number is reached, customer will be locked out. Default = 3
NO_STICKY_QUESTION	Boolean	If true, asking questions are always chosen randomly, even if user gave invalid answer. Default = false
MIN_QUESTION_SIZE	Numeric	Minimum size of custom question. Default = 10
MIN_ANSWER_SIZE	Numeric	Minimum size of answer. Default = 6
CONFIRM_QA	Boolean	If true, new user will be prompted to confirm his security questions and answers. Default = false
CASE_SENSITIVE_ANSWER	Boolean	If true, answer matching will be case sensitive. Default = false
ASTERISKS_ANSWERS	Boolean	If true, answers will be masked with asterisks when user provides an answer to security question. Default = false
E-Mail Settings		
USE_CLIENTS_EMAIL	Yes/No	Client must enter his/her email address at the same time with q/a. The address will be used to send reset code, in case customer forgot security answers
SMTP_HOST	String	Mail Server host name
SMTP_PORT	Numeric	Port number of SMTP server. Default = 25
SMTP_USE_SSL	Boolean	Specifies whether or not to send emails using SSL protocol. Default = false
SMTP_SSL_PORT	Numeric	Port number of SMTP server when using SSL secure connection.

Configuration Options		
Option Name	Possible Values	Description
		Default: 465
SMTP_USE_TLS	Boolean	Specifies whether or not to send emails using TLS protocol. Default = false
SMTP_LOGIN	String (optional)	Login for authorization when sending email. This key can be bypassed or left empty if no authorization required.
SMTP_PASSWORD	String	Password for authorization when sending email if authorization is required..
FROM_ADDRESS	String	From: email address to use when sending customer email with reset code
FROM_NAME	String	From: name to use when sending customer email with reset code
ONETIME_PASSWORD_MESSAGE_SUBJECT	String	Subject for the email with reset code. Default = ComodoTFSOWA Reset code.
NUMBER_OF_EMAILS	Numeric	Number of user emails (default value 1, max number 5).
Certificate Common Name (CN) Settings		
CN_PREFIX	String	Certificate common name prefix. The last '#' will be stripped out if present (It is used to terminate 'space' characters)
CN_SUFFIX	String	Certificate common name suffix
CN_MASK_SIZE	Numeric	Number of characters at the end of user name to show. All other characters will be replaced with *. If set to 0 no part of user name will be masked. Default = 0
CN_PADDING	Numeric	Pads the user name in CN with * characters up to the length specified. This is done before applying CN_PREFIX & CN_SUFFIX. If set to 0 no padding will be done. Default = 0
PKCS12_PASSWORD	String	Password used to protect PKCS12 encapsulated certificate for Safari/Opera and other browsers that don't support automatic certificate installation. Default = secure
Certificate Authority Login Information		
CA_LOGIN	String	Your ComodoCA login

Configuration Options		
Option Name	Possible Values	Description
CA_PASSWORD	String	Your ComodoCA password
CA_CERTIFICATE_ID	Numeric	Intermediate certificate Id
CA_CERTIFICATE_ID_IE	Numeric	Intermediate certificate Id for certificates issued for IE (usually UTN cross-signed)
CRL_NAME	String (optional)	The name of the CRL used for certificate revocation.
Certificate Related Settings		
SIMPLE_AUTH_MODE	Boolean	If set to false, separate authentication types can be used for every user browser/system pair (for example if the user is logged in from IE and installed certificate, the user may still install cookies in Firefox and then can authenticate with certificates on IE and with security cookie on Firefox). Default = False .
SHARED_KEY	String	This Key is used for connection with Certificate Enroller for certificate installation. Useful when Certenroll and TF application are hosted on different servers. Default = TEST
MAX_CERTIFICATES	Numeric	Specifies number of certificates customer may install. Revoking certificates will reset the counter. If set to -1, unlimited certificates can be installed by customer. Default = -1 (unlimited)
CERT_EXPIRE_DAYS	Numeric	Expiration term of the client certificate in days. Default = 365
TS_MAX_CERT_REQ	Numeric	Specifies the number of attempts the user will be prompted to install cookie instead of certificate in case of certificate installation problems on some XP computers. Default = 2
NO_AGREEMENT	Boolean	Specifies whether or not to show Certificate Subscriber Agreement for user certificate installation. Default = false
IE_KEY_USER_PROTECTED	Boolean	If set to true, additional dialog box will pop-up in IE, prompting user to select certificate protection level (and optionally protect it with password). Default = false
IE_KEY_EXPORTABLE	Boolean	If set to false, it will be impossible to export private key for client certificates installed through IE. Default = true
IE_ADVANCED	Boolean	If set to true, IE users will see additional advanced link that would allow them to change IE_KEY_USER_PROTECTED and IE_KEY_EXPORTABLE parameters. Default = false
Cookies Related Setting		

Configuration Options		
Option Name	Possible Values	Description
COOKIE_EXPIRE_D	Numeric	Expiration term of the client cookie in days. Default = 365
Callback		
CALLBACK_PHONE	Boolean	Use phone number for send reset code by voice. Default = yes
CALLBACK_SMS	Boolean	Use phone number for send reset code by sms. Default = yes
CALLBACK_ALLOW_EXTENSION	Boolean	Use extension (additional number). Default = no
CALLBACK_INTERNATIONAL_NUMBERS	Boolean	Use country code. If no, value '1' (code of USA) will be used. Default = no
DEFAULT_COUNTRY_PHONE_CODE	String	This phone country code will be displayed on CALLBACK new user page by default. Default = 1 (USA)
CALLBACK_AUTH_ID	String	Callback Authentication ID. Option is required for Callback by phone or SMS.
CALLBACK_CUSTOMER_ID	String	Callback Customer ID. Option is required for Callback by phone or SMS.
UNLOCK_AFTER_LOCK_TYPES	String	Unlock types in 'unlock after lock' screen. Possible values are EMAIL and CALLBACK. Default = EMAIL
Misc		
LANG	String (optional)	Allows to specify different language files for text modifications. It can load many files conf/lang/NAME1_LOCALE.properties;conf/lang/NAME2_LOCALE.properties, split with standard separator symbols(,;) or SEPARATOR symbol. You can see default files in conf/lang/directory. Also note that files should be created for every locale defined in LOCALE key (explained below) Default: lang.;lang.certenroll
LOCALE	string	Allows to specify the interface languages for the user pages. The available options are: <ul style="list-style-type: none"> en - English it - Italian ru - Russian

Configuration Options		
Option Name	Possible Values	Description
		<p>Example:</p> <p>To set English, Italian and Russian Locales, the key should be <code>LOCALE=en;it;ru</code></p> <p>Default = en</p>
ALLOW_CONTINUE_UNTIL	Date (mm/dd/yyyy)	If specified, displays the count down of days until 'Continue' link will work for end customer, allowing end customer to by-pass setup of security questions.
HTTP_REMOVE_IP_HEADER	String	Populates particular HTTP header with customer's remote IP address, when querying back end server. Default = HTTP_X_FORWARDED_FOR
REMOTE_IP_HEADER	String	HTTP header to use to retrieve Remote IP. If missing, standard tools to retrieve remote IP will be used.
LOCK_TIMEOUT	Boolean	If true, the accounts that were locked out due to invalid answers, will be unlocked 30 minutes (then 1 hour, 4 hours, 24 hours, and locked permanently) after they were locked. Default = true
DB_AUTO_UPDATE	Boolean	If set to true, ComodoTFSOWA will try to upgrade database with latest DB scheme for given ComodoTFSOWA version. Database user record must have privileges to CREATE/ALTER tables. Default = true.
OPEN_PROXY_RBLs	String	Semi-colon separated list of RBLs to use to check incoming IPs for open proxy.
RESET_CODE_EXP_TIME	Numeric	Sets expiration time of One-Time password in hours. Default = 24.
Additional Options		
SERVICE_PROVIDER	String	The service provider name, to appear in Client Certificate Subscriber Agreement
FULL_RESET	Boolean	If True, show Full Reset dialog box instead of standard reset window. Default = False
IP_DB_PATH	String	Path to Geographic IP database (IP -> Country)
IP_DB_UPDATE_PERIOD	Numeric	Period of automatic update of Geographic IP database (IP -> Country) in days. 0 = no automatic updates. Default = 30
IP_DB_ADDRESS	String	<p>Address to download IP database from.</p> <p>Default = <code>http://tfdownloads.comodo.com/ip2country/ip.dat</code></p>

Configuration Options		
Option Name	Possible Values	Description
DEFAULT_IP_RANGE	String	Default IP subnet to use with IP Range rules. Allows all users from specified IP range to pass without standard ComodoTFSOWA verification.
RULES	String	'Rules' files that define how requests will be intercepted and which additional authentication factors will be used.
ADMIN_CHANGE_PASSWORD	Boolean	If 'Yes' - when new admin user logs in for the first time - prompt him to change his password. Default = false.
ADMIN_PASSWORD_STRONG	Boolean	If 'True' - new password must match the following restrictions: <ul style="list-style-type: none"> • 8-15 characters; • must be alphanumeric; • must include at least one special character or uppercase letter. Default: false.
ADMIN_PASSWORD_EXPIRE	Numeric	Number of days for password to expire. 0 means that password will never expire. Default = 0.
ADMIN_PASSWORD_DISALLOW_OLD	Numeric	Number of previous admin's passwords that are not allowed to be reused when admin is changing his password. Default = 0.
CACHE	String	NONE - no caching being done. MEMORY - in memory caching only. DISK - in memory and on disk caching. Default = NONE.
CACHE_MEMORY_SIZE	Numeric	Number of items to hold in memory. Default = 50.
CACHE_DISK_SIZE	Numeric	Number of items to hold on disk. Default = 1000.
CACHE_DIR	String	Cached files' directory location. *Default = \$ {CATALINA.HOME}/cache/*
CACHE_REFRESH	Numeric	Number of seconds since item was cached after which item will be removed from cache. Default = 0 , which means that the item never expires.
MAX_OUTGOING_HTTP_CONNECTIONS	Numeric	Number of max outgoing concurrent connections from ComodoTF to server (parameter is used by connection pool). Default = 100
USE_MULTITHREADED_HTTP	Boolean	If set to false, the Servlet will create new connection to backend server for every request. This will increase number of open connections and decrease a chance to mix connections between users. Default = true

4.4. Configure Standard Questions

To setup standard security questions that user can select from drop down list connect to database via your favorite database client software. Insert into table 'questions' questions in the order you would like customer to see them. Like:

```
insert into questions (id, question) values (1, 'What was your favorite pet name');
insert into questions (id, question) values (2, 'What is your mother maiden name');
...
```

Note: Make sure you set QUESTION_TYPE to Standard_Multi, Mixed_Multi, or Custom_Multi in \$hostname.properties, where \$hostname is defined within the <tf> tag in 'ComodoTFSOWA-xx/conf/tomcat-cfg.xml'.

4.5. Logs

4.5.1. Access

To enable access logging, edit file *ComodoTFSOWA-xx/conf/tomcat-cfg.xml*. Find and uncomment < Access logging> tag.

Comodo Two Factor SOWA supports only the 'pattern' attribute for <accessLog pattern="combined" /> tag. You can find more information on log patterns here:

<http://tomcat.apache.org/tomcat-6.0-doc/config/valve.html#Access%20Log%20Valve>

Example:

```
<accessLog pattern='combined' />
```

This will produce... 'ComodoTFSOWA-xx/logs/\$hostname_access.log', where \$hostname defined within the <tf> tag in *ComodoTFSOWA-xx/conf/tomcat-cfg.xml*.

4.5.2. Comodo Two Factor SOWA

You can alter Comodo TF SOWA logging by editing *ComodoTFSOWA-xx/conf/log4j.properties* file. The log files are saved in *ComodoTFSOWA-xx/logs* directory.

4.6. Starting/Stopping Comodo Two Factor SOWA

4.6.1. Windows

To start Comodo Two Factor SOWA use the following commands

```
cd ComodoTFSOWA-xx/bin
c:\startup.bat
```

Note: By default ComodoTF SOWA is configured to listen on port 443. As a result, you have to execute ./startup.sh as privileged user (root) or change port to any value above 1024.

To shutdown Comodo Two Factor SOWA use the following commands

```
cd ComodoTFSOWA-xx/bin
c:\shutdown.bat
```

4.6.2. Linux/Unix/BSD

To start Comodo Two Factor SOWA use the following commands

```
cd ComodoTFSOWA-xx/bin
$ ./startup.sh
```

Note: By default ComodoTF SOWA is configured to listen on port 443. As a result, you have to execute `./startup.sh` as privileged user (root) or change port to any value above 1024.

To shutdown Comodo Two Factor SOWA use the following commands

```
cd ComodoTFSOWA-xx/bin
$ ./shutdown.sh
```

5. Integration

Comodo TF for SharePoint and Outlook Web Access can be integrated with most web based application to provide additional authentication layer. ComodoTFSOWA acts as reverse proxy, subjecting each request and response to a series of rules. Once specific rule is triggered, ComodoTFSOWA can perform extra authentication steps, inject pages, or deny customer the access to the web application.

The configuration for ComodoTFSOWA rules can be set in the file *ComodoTFSOWA-xx/conf/rules.example.xml*.

Note: This can be changed by setting the RULES variable in *ComodoTFSOWA-xx/conf/\$hostname.properties* file.

5.1. Intercept Rules

5.1.1. General Intercept Rules

Substitute Rule - specifies mime types that will be proceeded with body substitute. As shown in sample 1.1 below - any response that have text/html MIME-TYPE or contains in MIME-TYPE word 'JavaScript' will be substituted . There are can be any number of <substitute> tags in rules XML file. If no <substitute> section is found - only default type (text/html) will be substituted. If <substitute> section is empty (no <conditionsResponse> tags) - no substitutes will be made.

Sample 1.1:

```
<substitute>
  <conditionsResponse>
    <condition_mimetype value="text/html" match="EQUALS"/>
  </conditionsResponse>
</substitute>
<substitute>
  <conditionsResponse>
    <condition_mimetype value="JavaScript" match="CONTAINS"/>
  </conditionsResponse>
</substitute>
```

External Link Rule - Used to inform user by displaying warning if he/she is going to leave BackEnd site by clicking link that goes off. (Leaving site disclaimer) .In sample 1.2 - on all link pointing on URL's different than '**www.trust.com**' - warning disclaimer will be shown.

Sample 1.2

```
<ext_link>
  <settings>
    <setting name="trustedHost" value="www.trust.com"/>
  </settings>
  <conditionsResponse>
    <condition_mimetype value="text/html" match="EQUALS"/>
  </conditionsResponse>
</ext_link>
```

Cookies Rule - specifies cookie intercepting. Cookie interception needed when session cookie is used by backend website software, and login state is changed within session, without altering cookie. Does not require any additional parameters or inner tags.

Sample 1.3

```
<cookie_intercept/>
```

HTTP Authorization Rule - specifies HTTP header 'Authorization' intercepting. Header interception needed when 'Authorization' header is used by backend website software. Does not require any additional parameters or inner tags.

Sample 1.4

```
<httpauth_intercept/>
```

Conditions for **General Intercept Rules** are :

Request conditions:

Request header exists, request header value, web parameter exists, web parameter value, Http method, URI.

Response conditions:

Request header exists, request header value, web parameter exists, web parameter value, Http method, text, URI.

5.1.2. Request Intercept Rules

Local Page Rule - used to display local page **instead** of remote. From sample 1.5 we can see that , when user requests /webapp/index.html page he/she will receive local page , by path /usr/local/comodotf/wrapper.html, instead of BackEnd page.

Sample 1.5

```
<local_page>
  <conditionsRequest>
    <condition_uri value=" /webapp/index.html" match="EQUALS"/>
  </conditionsRequest>
  <settings>
    <setting_filename
value="/usr/local/comodotf/wrapper.html"/>
  </settings>
</local_page>
```

URL Hash rule - used to enable OSI Non-Integrated Third-Party Authentication Support, and set values of Secret Key and Secret Data obtained from OSI.

Sample 1.6

```
<url_hash>
  <conditionsRequest>
    <condition_uri value="/Common/SignOn/Start.asp"
match="CONTAINS"/>
    <condition_webparam_exists name="SignOnID" exists="true"/>
    <condition_webparam_exists name="Password" exists="true"/>
  </conditionsRequest>
  <settings>
    <setting name="secretKey" value="xxx"/>
    <setting name="secretData" value="xxx"/>
    <setting name="login" value="SignOnID"/>
    <setting name="password" value="Password"/>
  </settings>
</url_hash>
```

Conditions for this **Request Intercept Rules** are equals and following:

Request conditions:

Request header exists, request header value, web parameter exists, web parameter value, Http method, URI.

5.1.3. Response Intercept Rules

Login Rule - rule responsible for processing user login action (successful or failed), in addition it contains declaration of Challenge Rules (described below).

<challenges> tag specifies steps that TF will pass during user authorization. Steps will be passed in the same order as specified in rules file (**Challenge rules** described below).

<condition_success> tag specifying request that should be checked for success of login. Should be used only when success condition and intercept conditions does not match. **<condition_failed>** tag specifying request that should be checked for failure of login.

<settings> tag specifying login variable and login method. Login name is defined by attribute loginVar. Login method is defined by loginreader. The loginreader supports next values: 'param', 'httpauth' and 'multipart'.

Sample 1.7

```
<login>
  <conditionsResponse>
    <condition_uri value="/Common/SignOn/enter.asp"
    match="EQUALS"/>
    <condition_response_header_value name="referer"
    value="/Common/SignOn/ExpiredPassword.asp"
    match="NOT_EQUALS"/>
  </conditionsResponse>
  <conditions_success>
    <condition_uri value="/Common/SignOn/enter.asp"
    match="CONTAINS"/>
    <condition_text value="/Common/SignOn/CheckAccess.asp"
    match="CONTAINS"/>
  </conditions_success>
  <conditions_failed>
    <condition_uri value="/Common/SignOn/enter.asp"
    match="CONTAINS"/>
    <condition_text value="/Common/SignOn/SignOnError.asp"
    match="CONTAINS"/>
  </conditions_failed>
  <challenges>
    <challenge type="LOCKED_USER"/>
    <challenge type="INBANK_CHANGEES"/>
    <challenge type="ADMIN_RESET"/>
    <challenge type="IPRANGE"/>
    <challenge type="NO_AUTH"/>
    <challenge type="BLACK_LIST"/>
    <challenge type="CLIENT_CERT"/>
    <challenge type="COOKIE"/>
    <challenge type="SECURITY_QUESTION"/>
  </challenges>
  <settings>
    <setting name="loginVar" value="SignOnID"/>
    <setting name="loginreader" value="param"/>
  </settings>
</login>
```

Logout Rule - specifies request that identifies user's log out. If section is empty of missed logout will not detecting and user session will be closed only by time out. Multiple logout rules are allowed. As shown below, TF will change user state to LOGGED_OUT, if in the processing response, URI will be equals to '/Common/SignOn/Start.asp'.

Sample 1.8

```
<logout>
  <conditionsResponse>
    <condition_uri value="/Common/SignOn/Start.asp"
    match="EQUALS"/>
  </conditionsResponse>
</logout>
```

Conditions for this **Response Intercept Rules** are equals and following:

Response Conditions:

Request header exists, request header value, response header exists, response header value, web parameter exists, web parameter value, Http method, Text, URI.

5.1.4. Challenge rules

Challenge Rules - Table of Definitions	
Parameter	Description

Challenge Rules - Table of Definitions	
NO_AUTH	Doesn't perform any extra authentication on user, so user authenticates only with BackEnd login/password.
BLACK_LIST	Denies access for users from restricted countries or open proxies. This rule does not work for NO_AUTH users.
SECURITY_QUESTION	Allows user to authenticate via security question/answer. Don't use simultaneously with CALLBACK rule! Important: If you replace SECURITY_QUESTION rule with CALLBACK rule, don't forget to reset all existing users' security settings.
CLIENT_CERT	This rule must work before SECURITY_QUESTION or CALLBACK. If it is set before COOKIE, then certificate authentication will be default authentication, otherwise the default will be cookie authentication.
MASTER_CERT	Allows BackEnd Insider to login as any BackEnd client using his master certificate. <param name="allowedReferrer" value=""/> should be always defined.
IPRANGE_ONLY	Allows access for all users from specified IP range, for other users access will be denied (no ssl, question or certificate checks works). Priority of the rule depends from order in rules.xml
IPRANGE_REQUIRED	Denies access for all users from specified IP range, other users will pass standard verification. Priority of the rule depends from order in rules.xml
IPRANGE	Allows access for all users from specified IP range, other users will pass standard verification. Priority of the rule depends from order in rules.xml
INBANK_CHANGES	Allows to change security settings (email address) and to change security questions after the user has finished authentication process.
INBANK_CHANGECS	Allows to change callback settings (phones/email address) after user has finished authentication process.
ADMIN_RESET	Allows user to enter reset code provided by admin once the user was locked out due to wrong security answers. This rule works only for users, which have been locked due to wrong answer and doesn't work for users, which are locked by admin.
COOKIE	Allow user to authenticate with cookie as second factor. If it is set before CLIENT_CERT, this authentication will be default authentication, otherwise certificate installation will be default.
CALLBACK	Allows user to authenticate via sending him reset code by phone, sms or email. Don't use simultaneously with SECURITY_QUESTION rule! Important: If you replace CALLBACK rule with SECURITY_QUESTION rule, don't forget to reset all existing users' security settings.

5.1.5. Request conditions summary

Request Conditions Summary		
Name	Tag Syntax	Description

Request Conditions Summary		
Request header exist	<condition_request_header_exists name="" exists="" />	Checks if the header name exists in request headers.
Request header value	<condition_request_header name="" value="" match="" />	Checks for specified header name and it's value in request.
Request web parameter exist	<condition_webparam_exists name="" exists="" />	Checks if the given parameter name presents in the POST or GET request query.
Request web parameter value	<condition_webparam_value match="" name="" value="" />	Check for specified parameter name and it's value in the request query.
Request http method	<condition_httpmethod value="" />	Checks if the request having the same method as specified one (GET,POST, HEAD, etc).
Request uri	<condition_uri match="" value="" />	Assessment for specified URL in request.

5.1.6. Response conditions summary

Response Conditions Summary		
Name	Tag Syntax	Description
Response header exists	<condition_response_header_exists name="" exists="" />	Checks if the header name exists in response headers.
Response header value	<condition_response_header name="" value="" match="" />	Checks if response contains specified header name and it's value.
Response web parameter exists	<condition_webparam_exists name="" exists="" />	Checks if the given parameter name present in the POST or GET response query.
Response web parameter value	<condition_webparam_value match="" name="" value="" />	Checks if the specified parameter name and it's value is present in the response query.
Response http method	<condition_httpmethod value="" />	Checks if the response having the same method as specified one (GET,POST, HEAD, etc).
Response text	<condition_text match="" value="" />	Checks for specified text in response body.
Response uri	<condition_uri match="" value="" />	Assessment for specified URL in response.

Response Conditions Summary		
Response mimetype	<condition_mimetype match="" value="" />	Assessment for specified mimetype in response.

5.1.7. Settings summary

Settings Summary		
Name	Tag Syntax	Description
Setting	<setting name="name" value="value"/>	Simple setting pair, consisting of name and value.
Setting parameter alias	<setting_param_alias name="name" alias="alias" value="value" />	Setting pair (name, value) with additional parameter 'alias' - alias for name.
Setting filename	<setting_filename value="" />	Setting defining filename.
Setting text	<setting_text value="" />	Setting defining some text value.

5.2. Examples

This section contains examples of the rules.xml file, for different authentication modes.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
```

```
<rules>
```

```
  <version version="2.0"/>
```

```
  <interceptGeneral>
```

```
    <substitute>
```

```
      <conditionsResponse>
```

```
        <condition_mimetype value="javascript" match="CONTAINS"/>
```

```
      </conditionsResponse>
```

```
    </substitute>
```

```
    <substitute>
```

```
      <conditionsResponse>
```

```
        <condition_mimetype value="text/html" match="EQUALS"/>
```

```
      </conditionsResponse>
```

```
    </substitute>
```

```
    <ext_link>
```

```
      <settings>
```

```
        <setting name="trustedHost" value="www.fnbi.com"/>
```

```
      </settings>
```

```
      <conditionsResponse>
```

```
        <condition_mimetype value="text/html" match="EQUALS"/>
```

```
      </conditionsResponse>
```

```
    </ext_link>
```

```
    <cookie_intercept/>
```

```
    <httpauth_intercept/>
```

```
  </interceptGeneral>
```

```
  <interceptRequest>
```

```
</interceptRequest>
```

```

<interceptResponse>
  <login>
    <conditionsResponse>
      <condition_uri value="/Common/SignIn/enter.asp" match="EQUALS"/>
      <condition_response_header_value name="referer"
value="/Common/SignIn/ExpiredPassword.asp"
match="NOT_EQUALS"/>
    </conditionsResponse>
    <conditions_success>
      <condition_uri value="/Common/SignIn/enter.asp" match="CONTAINS"/>
      <condition_text value="/Common/SignIn/CheckAccess.asp"
match="CONTAINS"/>
    </conditions_success>
    <conditions_failed>
      <condition_uri
value="/Common/SignIn/enter.asp" match="CONTAINS"/>
      <condition_text
value="/Common/SignIn/SignInError.asp" match="CONTAINS"/>
    </conditions_failed>
    <challenges>
      <challenge type="LOCKED_USER"/>
      <challenge type="INBANK_CHANGESS"/>
      <challenge type="ADMIN_RESET"/>
      <challenge type="IPRANGE"/>
      <challenge type="NO_AUTH"/>
      <challenge type="BLACK_LIST"/>
      <challenge type="CLIENT_CERT"/>
      <challenge type="COOKIE"/>
      <challenge type="SECURITY_QUESTION"/>
    </challenges>
    <settings>
      <setting name="loginVar" value="SignInID"/>
      <setting name="loginreader" value="param"/>
    </settings>
  </login>
  <logout>
    <conditionsResponse>
      <condition_uri value="/Common/SignIn/Start.asp" match="EQUALS"/>
    </conditionsResponse>
  </logout>
  <logout>
    <conditionsResponse>
      <condition_uri value="/Common/Signoff/SignOff.asp" match="EQUALS"/>
    </conditionsResponse>
  </logout>
  <osi/>
</interceptResponse>
</rules>

```

5.2.1. HTTP Authentication

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<rules>
  <version version="2.0"/>

  <interceptGeneral>
    <substitute>
      <conditionsResponse>
        <condition_mimetype value="text/html" match="EQUALS"/>
      </conditionsResponse>
    </substitute>
    <cookie_intercept/>
    <httpauth_intercept/>

  </interceptGeneral>

  <interceptRequest>

```

```

</interceptRequest>

<interceptResult>
  <login>
    <conditionsResponse>
      <condition_request_header_exists name="Authorization" exists="false"/>
      <condition_response_header name="Status" value="401" match="CONTAINS"/>
      <condition_response_header_exists name="WWW-Authenticate" exists="true"/>
    </conditionsResponse>
    <conditions_success>
      <condition_request_header_exists name="Authorization" exists="true"/>
      <condition_response_header name="Status" value="200" match="CONTAINS"/>
    </conditions_success>
    <conditions_failed>
      <condition_request_header_exists name="Authorization" exists="true"/>
      <condition_response_header name="Status" value="401" match="CONTAINS"/>
      <condition_response_header_exists name="WWW-Authenticate" exists="true"/>
    </conditions_failed>
    <challenges>
      <challenge type="LOCKED_USER"/>
      <challenge type="INBANK_CHANGECS"/>
      <challenge type="INBANK_CHANGECS"/>
      <challenge type="ADMIN_RESET"/>
      <challenge type="NO_AUTH"/>
      <challenge type="BLACK_LIST"/>
      <challenge type="COOKIE"/>
      <challenge type="CALLBACK"/>
    </challenges>
    <settings>
      <setting name="loginreader" value="httpauth"/>
    </settings>
  </login>
</interceptResult>
</rules>

```

5.2.2. URL_HASH (MacKeys)

```

<url_hash>
  <conditionsRequest>
    <condition_uri value="/Common/SignOn/Start.asp" match="CONTAINS"/>
    <condition_webparam_exists name="SignOnID" exists="true"/>
    <condition_webparam_exists name="Password" exists="true"/>
  </conditionsRequest>
  <settings>
    <setting name="secretKey" value="xxx"/>
    <setting name="secretData" value="xxx"/>
    <setting name="login" value="SignOnID"/>
    <setting name="password" value="Password"/>
  </settings>
</url_hash>

```

5.2.3. Proxy All Mode

This mode can be set by commenting out all rules in *rules.xml* except `<substitute>`. In this case Comodo TF SOWA will pass all requests directly to Backend application, without trying to inject Comodo TF SOWA authentication layer. In this mode Comodo TF SOWA will not connect to database, nor challenge user with extra security questions or certificates. **THIS MODE SHOULD BE USED ONLY IN EMERGENCY SITUATIONS, AS IT REMOVES ALL THE SECURITY LAYERS PROVIDED BY Comodo TF SOWA.**

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<rules>
  <version version="2.0"/>
  <interceptGeneral>
    <substitute>
      <conditionsResponse>
        <condition_mimetype value="text/html" match="EQUALS"/>
      </conditionsResponse>
    </substitute>
  </interceptGeneral>

```

```
</interceptGeneral>  
<interceptRequest />  
<interceptResponse />  
</rules>
```

6. Customization

Comodo TF for SharePoint and Outlook Web Access templates varied much since the previous version - now it is far more easy to configure templates, and conveniently to use them.

6.1. Work Area

The main idea is that the work place is divided into 3 sections specified by:

```
<div class='comodoLeft'>  
<div class='comodoMiddle'>  
<div class='comodoRight'>
```

The screenshot shows a security verification interface. It is divided into three main sections:

- comodoLeft area:** Contains informational text on the left side, including sections like "Why should I do this?", "Should I register this computer?", and "When will you ask me a security question?".
- comodoMiddle area:** The central area containing the main security question and answer input. It includes a message: "We were unable to verify your computer. For your added security, please answer the following security question that you previously set up." Below this is a form for "Question: question 3" with an "Answer:" input field. Further down, there is a checkbox option: "Enable this computer with my security cookie for future secure and convenient online banking." and buttons for "Continue" and "Change Security Questions".
- comodoRight area:** Contains additional informational text on the right side, including sections like "Why do I have to answer a security question?", "Should I register this computer?", and "When will you ask me a security question?".

The middle section usually contains the main interface area, for example:

We were unable to verify your computer. For your added security, please answer the following security question that you previously set up.

Question: question 3

Answer:

If you are currently using a computer that you plan to normally use for online banking, you can enable it for secure and convenient online banking with a security cookie. Your security cookie will authenticate you and eliminate the need to answer a security question each time you access your account. We strongly recommend that you only enable computers that you plan to normally use for online banking.

☐ Enable this computer with my security cookie for future secure and convenient online banking.

[Continue](#)

[Change Security Questions](#)

Why do security

We were comput
number
Therefo
your acc
answer
question

Should I

Register
comput
some h
comput
access
should
that you
account
register
used co

When u

Help information is located in the right section:

Change security questions and answers

Answer security question.

Help Information →

To make changes, you must first answer the following security question.

Question: question 3

Answer:

When will you ask me a security question?

When logging in from an unregistered computer (such as a public or infrequently used computer) or when you login from a computer that you have not yet registered.

Left section is reserved, and stay invisible (CSS style ='display:none').

Left / Right can be made visible/invisible via CSS content.

Content for them can be specified via left_side_comment / right_side_comment (generic comment label), right_side_comment_TEMPLATE_NAME (like right_side_comment_requestcert.vm) for particular page or right_side_comment_TEMPLATE_NAME_AUTHTYPE (like right_side_comment_requestcert.vm_4 for requestcert.vm in cookie mode). Generic template for all pages of particular AUTHTYPE can be specified using right_side_comment_AUTHTYPE label. It can be right_side_comment or left_side_comment.

AUTHTYPES (Authentication Types) are:

- 0 - new user
- 1 - no authentication
- 2 - certificate based authentication
- 3 - security question based authentication
- 4 - cookie based authentication
- 5 - callback based authentication

6.2. Styles

For <div> are used next additional styles:

- comodotfInput: Used to create input fields for important questions;

security question that you previously set up.

Question: question 3

Answer:

If you are currently using a computer that you plan to normally use for online banking

- comodotfText: Used to edit/format text;

We were unable to verify your computer. For your added security, please answer the following security question that you previously set up.


Question: question 3

Answer:

If you are currently using a computer that you plan to normally use for online banking, you can enable it for secure and convenient online banking with a security cookie. Your security cookie will authenticate you and eliminate the need to answer a security question each time you access your account. We strongly recommend that you only enable computers that you plan to normally use for online banking.

☐ Enable this computer with my security cookie for future secure and convenient online banking.


- comodotfNote: Used for different NOTES;



Important Note!

You have to have cookies enabled in your browser to use this feature

- comodotfError: Used for error messages;



You have entered invalid answer.

Attempt 1 out of 3

Besides for some HTML elements you can use next styles:

- comodotflabel: Used to name some html tags;

Question: question 3

Answer:

- comodotfForm: It is tag form itself;

Question: question 3

Answer:

If you are currently using a computer that you plan to normally use for online banking, you can enable it for secure and convenient online banking with a security cookie. Your security cookie will authenticate you and eliminate the need to answer a security question each time you access your account. We strongly recommend that you only enable computers that you plan to normally use for online banking.

☐ Enable this computer with my security cookie for future secure and convenient online banking.

[Continue](#)

- comodotfTable: Used to format table style;

Setup new security questions and answers

Enter new security questions and answers

1 Question

(min. 10 characters)

Answer

(min. 6 characters)

2 Question

(min. 10 characters)

Answer

(min. 6 characters)

3 Question

(min. 10 characters)

Answer

(min. 6 characters)

[Submit](#)

[Go Back](#)

- comodotfIndex: Used to format index style;

1 Question

Answer

2 Question

Answer

3 Question

Answer

- comodotfAnswer/comodotfQuestion: Used to format question/answer's styles;

1 Question	<input type="text"/>
Answer	<input type="text"/>
2 Question	<input type="text"/>
Answer	<input type="text"/>
3 Question	<input type="text"/>
Answer	<input type="text"/>

All code is XHTML (meaning XML compatible, like input tag should have /> not just >, like <input type='text' name='abc'/>, same with
 and any other tag that doesn't have matching close tag).

6.3. New User Screen

By default 'new user' screen looks like the following:

To strengthen online banking security, an additional authentication layer has been added. In the next few steps we ask that you please setup a new security question and answer.


1 Question (min. 10 characters)
Answer (min. 6 characters)

2 Question (min. 10 characters)
Answer (min. 6 characters)

3 Question (min. 10 characters)
Answer (min. 6 characters)

If you are currently using a computer that you plan to normally use for online banking, you can enable it for secure and convenient online banking with a security cookie. Your security cookie will authenticate you and eliminate the need to answer a security question each time you access your account. We strongly recommend that you only enable computers that you plan to normally use for online banking.

☒ Enable this computer with my security cookie for future secure and convenient online banking.

 **Important Note!**
 You have to have cookies enabled in your browser to use this feature

[Continue without it](#)

The following customizations are available:

1. Captions '1 Question', '2 Question', '3 Question' can be changed to 'Question 1', 'Question 2', 'Question 3'. To do this you should uncomment the following constant in lang file:
 label_security_question_cust=Question {0}
2. Link 'Continue without it' can be changed to button and moved from under the button 'Continue' to the right side of it.
 Also the button 'Continue without it' can be located twice: before the questions and under them. To do this you should uncomment the following constant in lang file:
 continue_button=<input type="button" value="{2}" onClick="window.location='{0}?{1}&STEP=continue';">

After both these customizations 'new user' screen will look like the following:

To strengthen online banking security, an additional authentication layer has been added. In the next few steps we ask that you please setup a new security question and answer.

1 Question (min. 10 characters)
Answer (min. 6 characters)

2 Question (min. 10 characters)
Answer (min. 6 characters)

3 Question (min. 10 characters)
Answer (min. 6 characters)

Please provide the e-mail address that you would like to use in the event that you would like to reset your security questions and answers.
E-Mail Address

If you are currently using a computer that you plan to normally use for online banking, you can enable it for secure and convenient online banking with a security cookie. Your security cookie will authenticate you and eliminate the need to answer a security question each time you access your account. We strongly recommend that you only enable computers that you plan to normally use for online banking.

☐ Enable this computer with my security cookie for future secure and convenient online banking.

[Continue without it](#)

6.4. Text Changes

To customize text as it appears in Comodo TF SOWA, copy file *ComodoTFSOWA-XX/conf/en.properties.example* to *ComodoTFSOWA-xx/conf/lang/ANYNAME.properties*.

Modify content of this file to use wording that you would prefer.

Add parameter **LANG=lang.ANYNAME** to *ComodoTFSOWA-xx/conf/localhost.properties*.

Note: Customization files should be added for every locale defined in LOCALE key and file should be called: *ComodoTFSOWA-xx/conf/lang/ANYNAME_LOCALE.properties*.

You can change visual appearance of email: you can add .html tags into proper parameters at *lang.properties*, ex. *mail_reset_code*.

Restart Comodo TF SOWA.

6.5. Using BackEnd headers and footers under inside BackEnd links

By default, after pressing inside BackEnd links you go to different pages, in which BackEnd headers and footers are displayed.

If you don't want, that headers and footers will be shown, add parameters `tf_showheader=0` and `tf_showfooter=0` into BackEnd Link.

Then after pressing BackEnd Link you will see the screen like below:

Change security questions and answers

Answer security question.
To make changes, you must first answer the following security question.

Question: question 3

Answer:

Setup new security questions and answers
Enter new security questions and answers

1 Question (min. 10 characters)

Answer (min. 6 characters)

2 Question (min. 10 characters)

Answer (min. 6 characters)

3 Question (min. 10 characters)

Answer (min. 6 characters)

Note: You can use this feature with tf_showheader and tf_showfooter for all Comodo TF SOWA Screens, not only for BackEnd Links and following pages.

7. Getting Support

Comodo is committed to provide the best support to its products. It offers the support in following forms:

- **Phone Support**
- **Email Support**
- **Support Ticketing System**

Phone Support

The administrators can contact the support team using the following numbers. The phone support is available 24/7.

US : +1-888-256-2608

International : +1-703-637-9361

Email Support

The Administrators can also contact the support team by sending an email to EnterpriseSolutions@comodo.com

Support Ticketing System

The Comodo's support portal is hosted at <http://support.comodo.com>. After registering for a free account, administrators can submit support tickets that will be handled by our professional and experienced product experts. The support portal also contains a product knowledge base and other useful links that can help to solve some of the most common queries about the product.

- Administrators are also encouraged to register at the Comodo community messageboards (Sign up at : <http://forums.comodo.com>).Introduction to Comodo TF for SharePoint and OWA.

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>.