boolebox

Configuration guide

Last update - 17 June, 2021

Table of contents

1 Introduction

Welcome to the CONFIGURATION section of the BooleBox administrator guide. In this area you will discover the steps needed for the activation of the license and for the correct configuration of the platform according to the standard methods tested and certified by the technical support team. In addition, you will find useful information about the CONTROL PANEL, which you will use to configure and monitor the service status of the platform components.

Within this section, in the form of a note in bold, you will find some indications to obtain the Common Criteria EAL2+ certified version.

Note: within this section, you will find some useful notes in order to configure correctly the mobile app. The mobile application is not subject to Common Criteria EAL2+ evaluation.

2 ASP.NET service configuration

Before proceeding with the activation of the license, it is necessary to verify that the Windows ASP.NET service is active and that it is configured to start automatically. To configure the ASP.NET service:

- In the SERVICES section of the control panel, double click on the ASP.NET STATE SERVICE item.
- If the service is not active, click on the START button located in the SERVICE STATUS area.
- From the dropdown menu next to the STARTUP TYPE item, select AUTOMATIC.
- Click on APPLY.
- Click on OK.

3 License activation

After completing the installation procedure, in order to correctly configure the BooleBox platform and access the control panel, it is necessary to proceed with the activation of the license. **In order to configure the Common Criteria EAL2+ certified version of BooleBox On-Premises, you must have a 2048-bit RSA key certificate available. In the case of a standard installation, the certificate automatically generated by the server during the IIS installation phase (installed during the installation phase of BooleBox On-Premises application) will be used. Otherwise, in the event of an explicit request from the customer, BooleBox On-Premises will use the certificate generated and provided by the customer, that need to be installed by inserting it in the Windows certificate store.**

If the available machine has direct access to the internet, you can proceed with the activation of the online license; if instead the BooleBox public server or the available machine does not have any type of internet access, you can take advantage of the manual activation of the offline license.

3.1 Online license activation

To proceed with the activation of the online license:

- Open the BooleBox On-Premises application.
- In the window that is going to appear on your screen, enter the code license (20 characters) provided by the sales team while purchasing the solution.
- Click on the three dots next to the field below.
- In the window that is going to appear on your screen, select the certificate containing the public and private encryption keys of BooleBox On-Premises configuration file. This file contains the Master Key, i.e. the key used to encrypt data in the storage.

- Click CONFIRM to complete the activation of the online license.

Note: by installing the application on multiple nodes, you can install a specific instance of BooleBox On-Premises for each indicated node. The same Master Key encryption certificate must be imported on each node in .pfx format.

If you entered a certificate not containing the private key, an error message will appear, informing that the certificate entered must contain the private key.

3.2 Offline license activation

To proceed with the activation of the offline license:

- In the window that is going to appear on your screen, click on YES.
- In the LICENSE WITHOUT INTERNET CONNECTION window, click on COPY to copy the code generated for the external server.
- Open a browser window on a PC that has an internet connection available.
- Type this URL.
- In the browser page reached through the link provided, paste the code previously copied in the appropriate field.
- Click on GET CODE.
- Select the entire code obtained and copy it by clicking CTRL + A.
- Paste the code collected in the above step in the appropriate field of the LICENSE WITHOUT INTERNET CONNECTION panel.
- Click on CONFIRM.
- In the window that is going to appear on your screen, click OK.

Note: by installing the application on multiple nodes, you can install a specific instance of BooleBox On-Premises for each indicated node. The same Master Key encryption certificate must be imported on each node in .pfx format. The license must instead be activated only on the first node. For the following nodes:

- Copy the following files inside the first node: C:Program FilesBooleBox on-premisesBooleBox.dat and C:Program FilesBooleBox on-premisesWebAppBooleBoxcert.dat.
- Paste the files above on the remaining nodes.
- Launch the application.
- Select LICENSE INFO.
- Select LICENSE UPDATE to upgrade the license and follow the steps above to activate the offline license.

4 Control panel

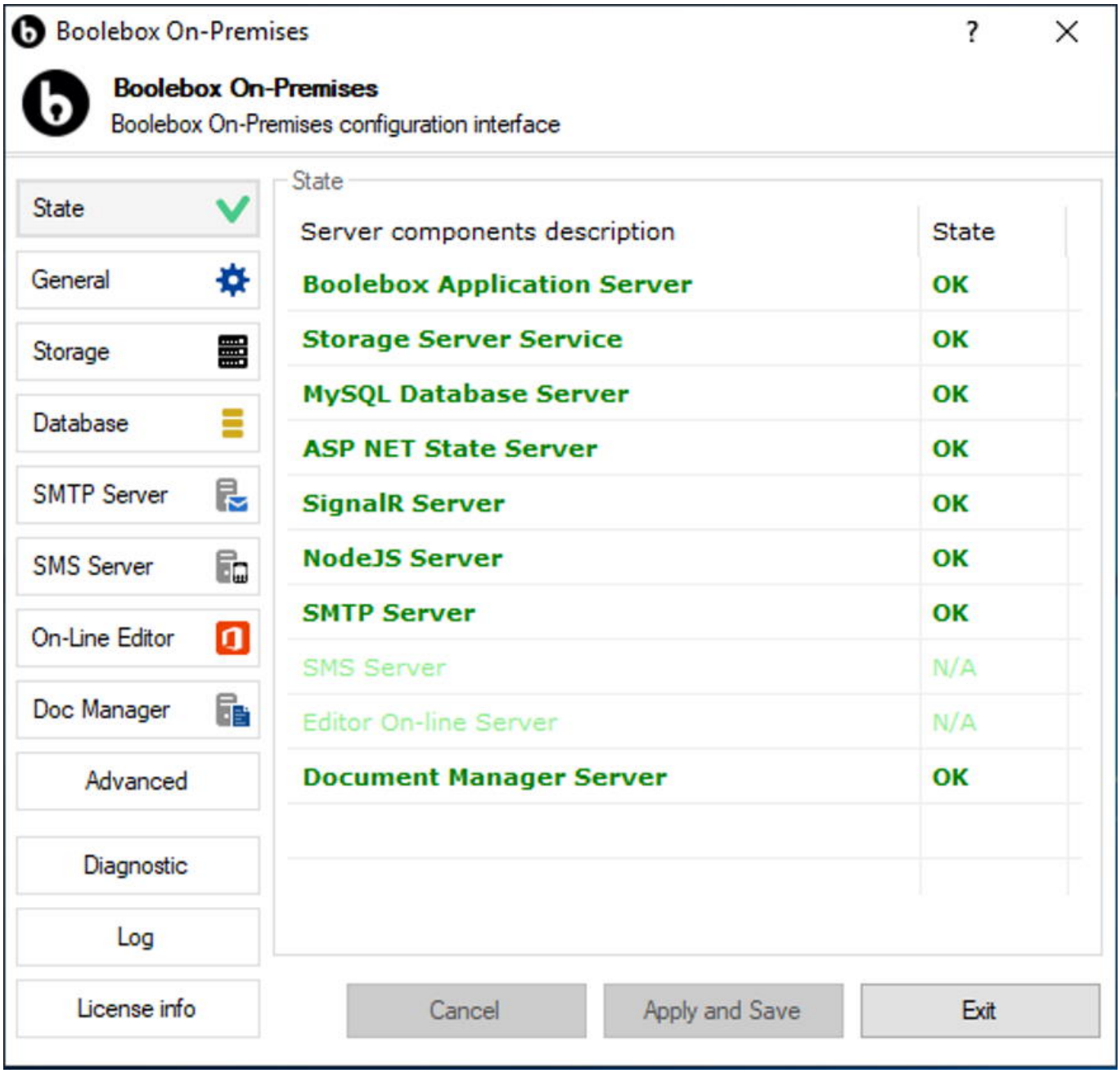
In order to use the platform correctly, it is necessary to proceed with the configuration of all BooleBox components by using the control panel, automatically appeared after the activation of the license. You can use the control panel to obtain license information, to perform the related updates and to consult the BooleBox On-Premises application log.

4.1 State

Within the STATE tab of the control panel, you can monitor the status of BooleBox On-Premises services, to get a general overview of the platform and correct any malfunctions.
Each of the BooleBox services can take one of the following statuses:

- **OK (green) –** the service is active.
- **KO (red) –** the service is not active or is not correctly installed/configured.
- **N/A (gray) –** the service is not installed.
- **UPDATE (yellow) –** the service requires an update.

Note: if the status from the service is different from OK, click on the corresponding tab to check the configuration and possibly correct it.


Boolebox On-Premises
Boolebox On-Premises
Boolebox On-Premises configuration interface
State
General
Storage
Database
SMTP Server
SMS Server
On-Line Editor
Doc Manager
Advanced
Diagnostic
Log
License info
State
Server components description
State
Boolebox Application Server
OK
Storage Server Service
OK
MySQL Database Server
OK
ASP NET State Server
OK
SignalR Server
OK
NodeJS Server
OK
SMTP Server
OK
SMS Server
N/A
Editor On-line Server
N/A
Document Manager Server
OK
Cancel
Apply and Save
Exit

4.2 General

Within the GENERAL tab, you need to configure the following fields:

- **IP SERVER ADDRESS OF THE ASP NET STATE SESSION –** address relative to BooleBox servers Cache.For configurations with only one node, enter the IP address in the format **serverip: 42424 (127.0.0.1:42424)** and click on CONNECT and APPLY AND SAVE. In the case of multiple nodes, instead, specify the server on which ASP.Net State Service and BooleBox Server Service are installed and click on CONNECT and APPLY AND SAVE.
- **PUBLIC URL OF BOOLEBOX SERVER –** URL address used by users to access the BooleBox platform, exploited as a link within the platform itself (e.g. e-mail notifications).To configure the URL, enter the IP address or the FQDN (Fully Qualified Domain Name) name of the server on which BooleBox On-Premises was installed preceded by “https” and click on CONNECT and APPLY AND SAVE.

  Note: if the CONNECT operation fails, please verify that the IIS related to this service is active.

  Note: in case of use of HTTPS protocol with TLS certificate supplied by the customer, it is necessary to configure the IIS bindings so that port 443 can be used. For the IIS configuration relating to port 443, please refer to this link.

- **URL SERVER ADDRESS OF SIGNAL R –** the URL address or the FQDN name of the server where SignalR is installed.To configure the URL, enter the IP address or the FQDN name of the server where SignalR was installed preceded by “https” and click on CONNECT and APPLY AND SAVE. **Note: if the CONNECT operation fails, verify that the IIS related to this service is active.**
- **URL SERVER ADDRESS OF NODE.JS –** URL address or the FQDN name of the server where Node.JS is installed.To configure the URL, enter the IP address or the FQDN name of the server where Node.JS is installed followed by the related port and click on CONNECT and APPLY AND SAVE.

Note: the port to be indicated is 3000 for http connections and 3500 for https connections.

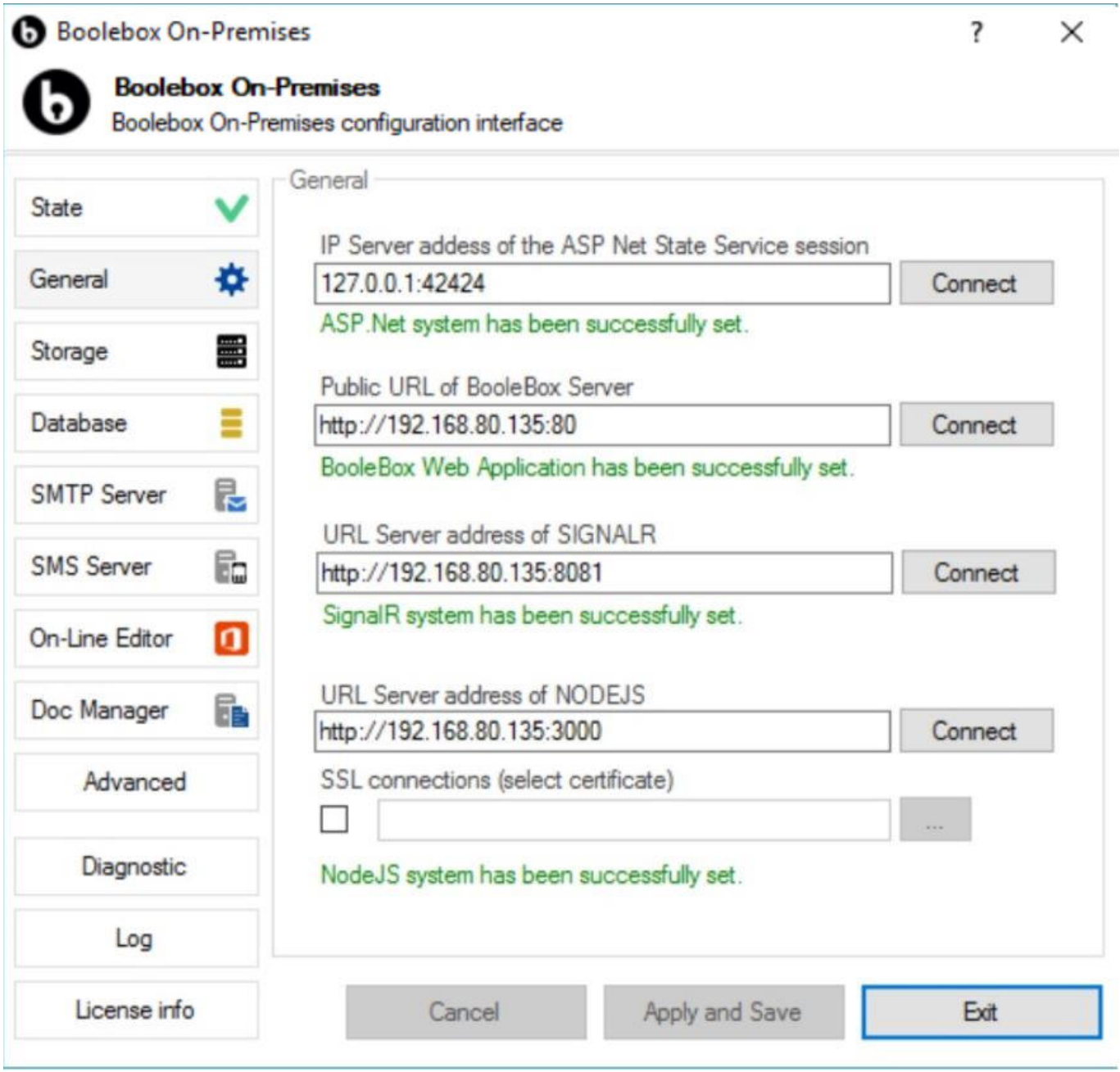
- In case of use of 1.2 TLS certificate (recommended), click on the relative checkbox and select the 1.2 TLS certificate, which must be in **.pfx** format.**Note: this certificate is mandatory for BooleBox On-Premises instances that are configured according to Common Criteria EAL2+ specifications and want to grant the access from web browser through HTTPS protocol.**

General note: if the CONNECT operation is not successful, it is necessary to verify the correct resolution of the DNS name for each URL entered.

In order to install the Common Criteria EAL2+ version of BooleBox On-Premises, you must configure the storage provided by BooleBox, named BOOLEBOX STORAGE in this section.

Note: this section shows the configuration of all the components that can be integrated into the platform, but only the components installed must be configured. In particular, to configure the Common Criteria EAL2+ certified version of BooleBox On-Premises, it is necessary to install only the components required by the certification and in compliance with the indications provided in this guide for the certification itself.

Note: to proceed with the configuration of BooleBox On-Premises in accordance with the criteria imposed by the Common Criteria EAL2 + certification, it is necessary to configure the BooleBox On Premise site to listen only via the HTTPS protocol, by deactivating the HTTP port activated by default or by automatically upgrading the connection from HTTP to HTTPS.


Boolebox On-Premises
Boolebox On-Premises
Boolebox On-Premises configuration interface
State
General
Storage
Database
SMTP Server
SMS Server
On-Line Editor
Doc Manager
Advanced
Diagnostic
Log
License info
General
IP Server addess of the ASP Net State Service session
127.0.0.1:42424
Connect
ASP.Net system has been successfully set.
Public URL of BooleBox Server
http://192.168.80.135:80
Connect
BooleBox Web Application has been successfully set.
URL Server address of SIGNALR
http://192.168.80.135:8081
Connect
SignalR system has been successfully set.
URL Server address of NODEJS
http://192.168.80.135:3000
Connect
SSL connections (select certificate)
...
NodeJS system has been successfully set.
Cancel
Apply and Save
Exit

4.3 Storage

Within the STORAGE tab, all the information related to the BooleBox Storage server is listed.

If you want to configure the STORAGE offered by BooleBox:

- Click on BOOLEBOX STORAGE.
- In the SERVER STORAGE SERVICE URL field, enter the URL (IP address and corresponding port) for the server on which you installed the BooleBox Storage Service component in HTTPS format.
- In the STORAGE ACCESS KEY area, enter an alphanumeric password to protect the saved items.**Note: the password entered must not contain any special characters.**
- Click on CONNECT.
- Click on APPLY AND SAVE.

If you want to configure Amazon cloud storage as a BooleBox storage, select the AMAZONS3 REMOTE STORAGE entry.

- In the fields below, enter the parameters related to the desired Amazon remote storage.

If you want to configure Microsoft Azure storage, select MICROSOFT AZURE BLOB STORAGE:

- In the fields below, enter the parameters related to the desired Microsoft Azure remote storage.

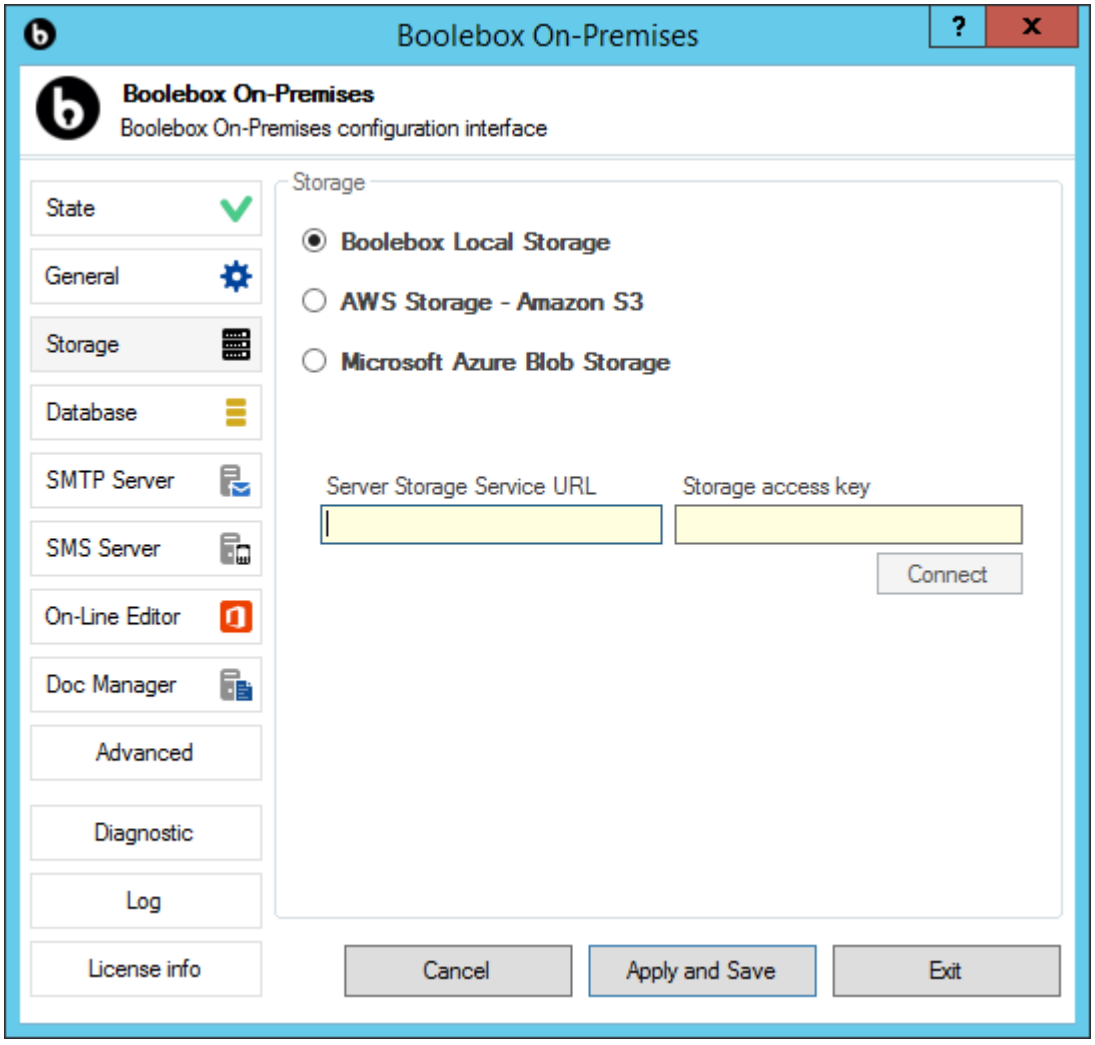
Note: the default location for storing data uploaded on the BooleBox platform is contained in the path c:\Program Files\BooleBox Storage Service\BooleBox Storage Service\App_Data\Storage. If the default path has been changed during installation, the data storage path will be the one indicated during the installation procedure. To change the storage path, open the SETTINGS.CONFIG file contained in c:\Program Files\BooleBox Storage Service\BooleBox Storage Service\ and change the line < add key=”Path” value=”” / > to < add key=”Path”value=\\storagepath / >

In order to install the Common Criteria EAL2+ certified version, you must configure

the BOOLEBOX STORAGE.

Note: in case of use of HTTPS protocol with TLS certificate supplied by the customer, it is necessary to configure the IIS bindings so that port 443 can be used. For the IIS configuration relating to port 443, please refer to this link.

Note: to proceed with the configuration of BooleBox On-Premises in accordance with the criteria imposed by the Common Criteria EAL2 + certification, it is necessary to configure the Server Storage Service site to listen only via the HTTPS protocol, by deactivating the HTTP port activated by default or by automatically upgrading the connection from HTTP to HTTPS.



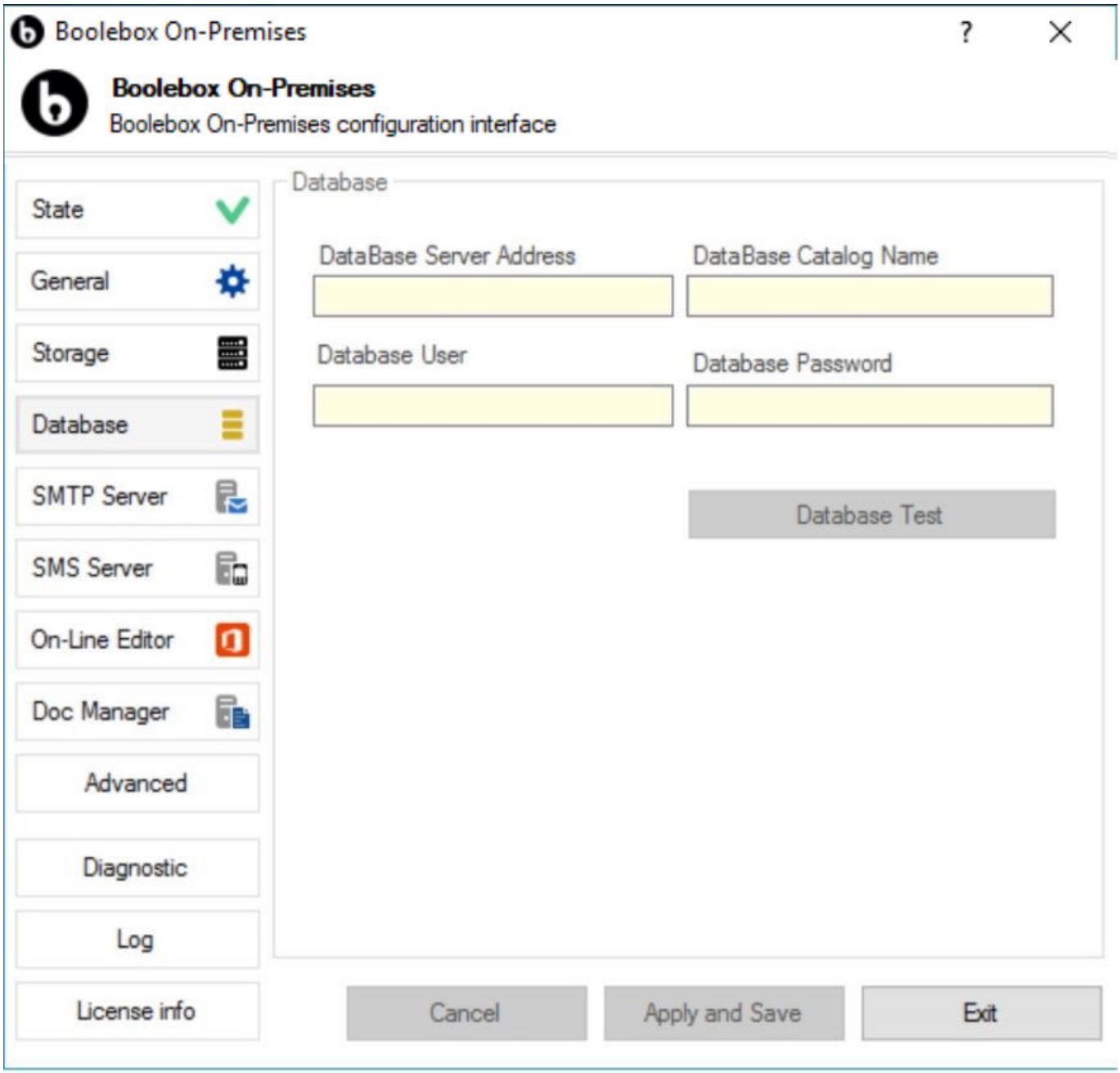
4.4 Database

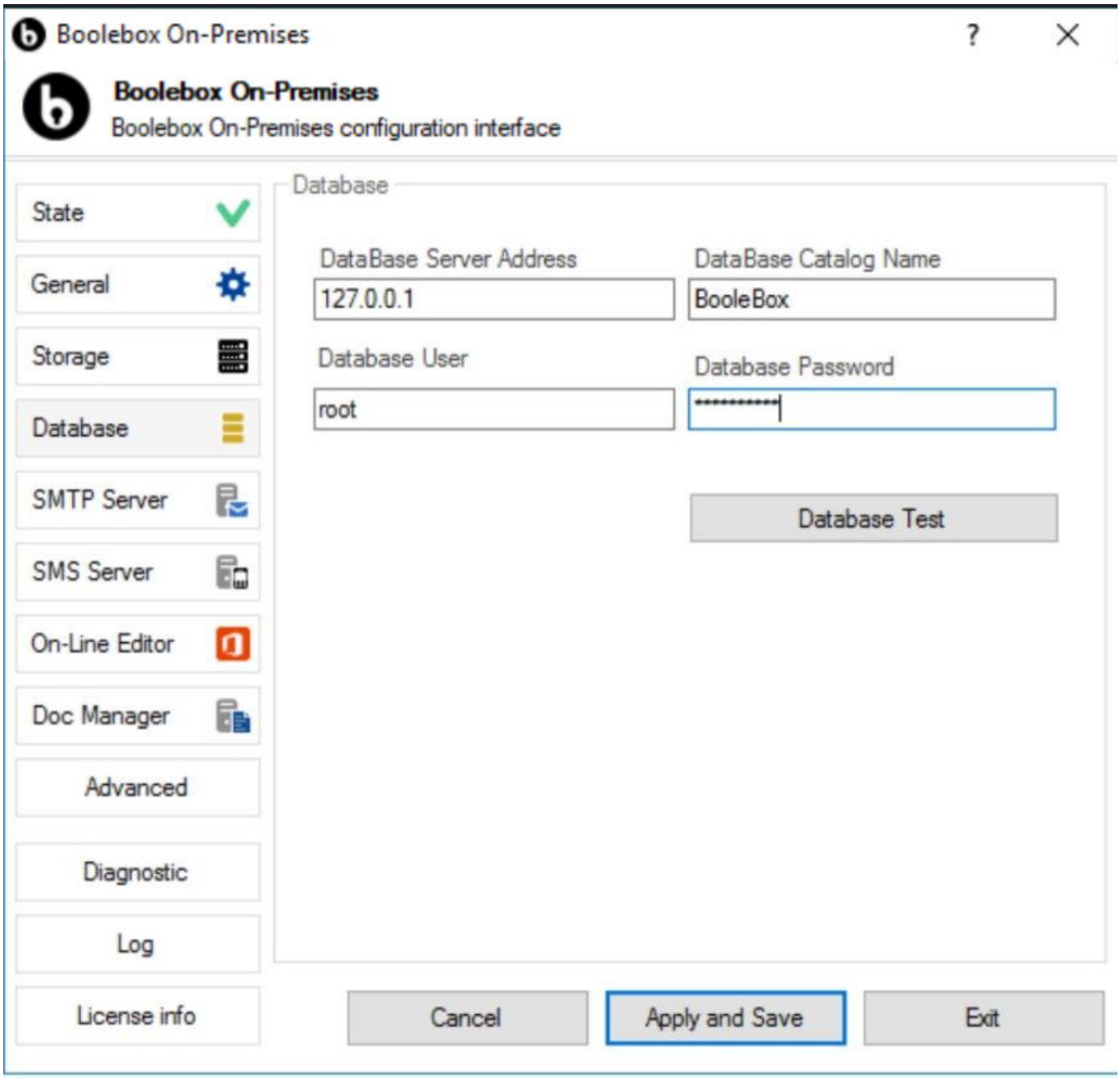
The DATABASE tab displays all the information about the database used by BooleBox On-Premises. To configure correctly this section, you must complete the following fields:

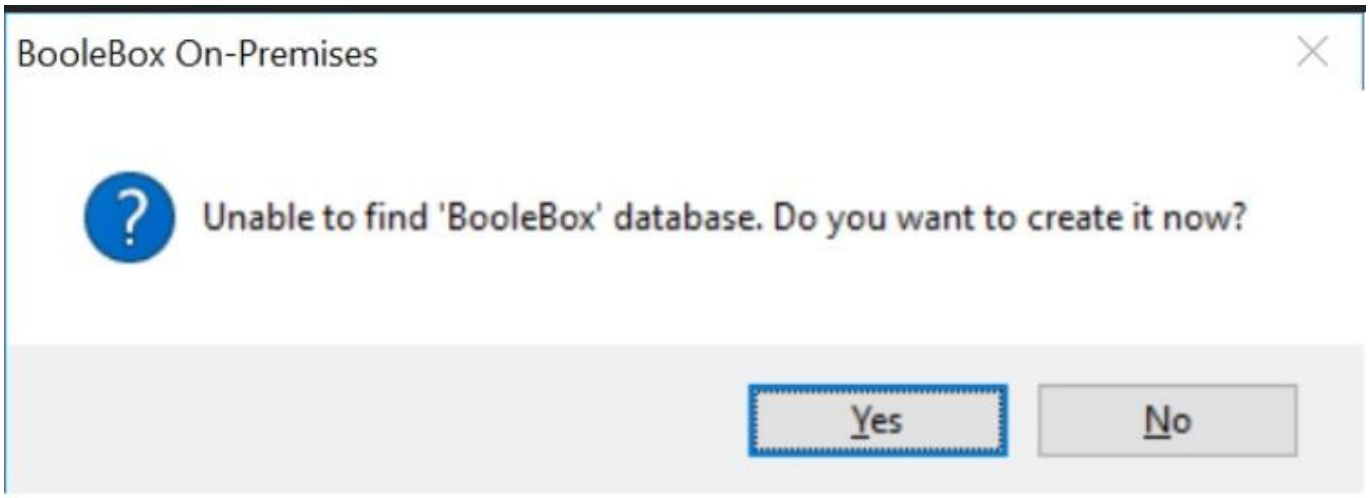
- **DATABASE SERVER ADDRESS –** the IP address of the server on which MySQL was installed.
- **DATABASE CATALOG NAME –** the database name that will be used by BooleBox to store all configuration, logs and data encryption keys files.
- **DATABASE USER –** the name of the user who will have access to the database.
- **DATABASE PASSWORD –** the password for the user indicated in the DATABASE USER field.
- Click on DATABASE TEST to create the database specified above.
- In the window that is going to appear on your screen, click on YES.
- On the next two screens, click on OK.
- Click on APPLY AND SAVE.

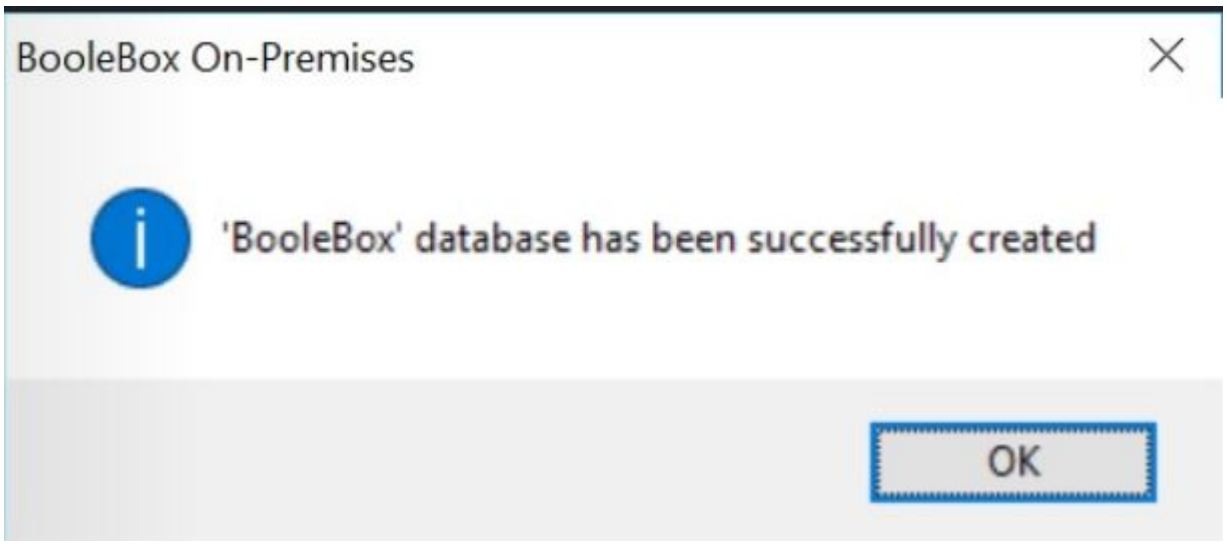
Note: the DATABASE TEST command, in case of an already existing database, performs two other operations:
– Checking the connection status with the database server.
– Database update in case of platform upgrades.

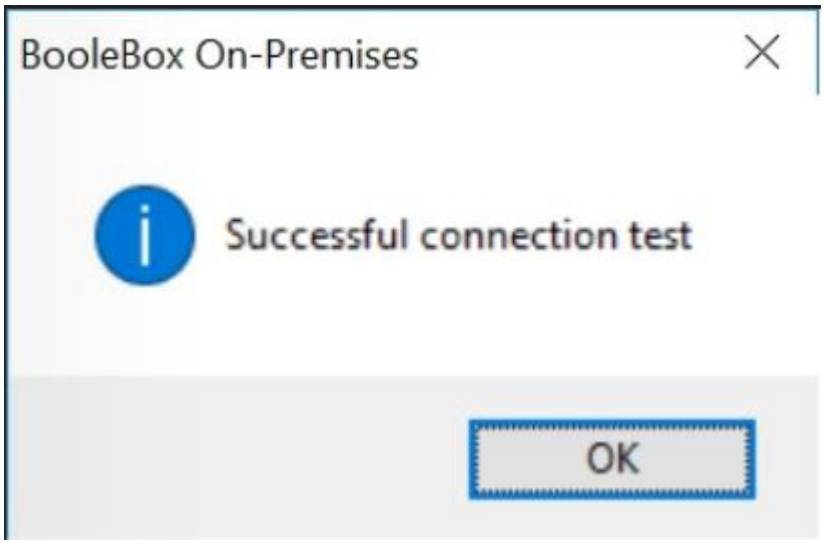
Note: if the database is not installed on the same server of BooleBox On-Premises, you must execute the following command from MySQL command prompt: GRANT ALL PRIVILEGES ON *.* TO 'USERNAME'@'%' IDENTIFIED BY 'PASSWORD' WITH GRANT OPTION;


Boolebox On-Premises
Boolebox On-Premises
Boolebox On-Premises configuration interface
State
General
Storage
Database
SMTP Server
SMS Server
On-Line Editor
Doc Manager
Advanced
Diagnostic
Log
License info
Database
DataBase Server Address
DataBase Catalog Name
Database User
Database Password
Database Test
Cancel
Apply and Save
Exit


Boolebox On-Premises
Boolebox On-Premises
Boolebox On-Premises configuration interface
State
General
Storage
Database
SMTP Server
SMS Server
On-Line Editor
Doc Manager
Advanced
Diagnostic
Log
License info
Database
DataBase Server Address
127.0.0.1
DataBase Catalog Name
BooleBox
Database User
root
Database Password
Database Test
Cancel
Apply and Save
Exit


BooleBox On-Premises
Unable to find 'BooleBox' database. Do you want to create it now?
Yes
No


BooleBox On-Premises
'BooleBox' database has been successfully created
OK

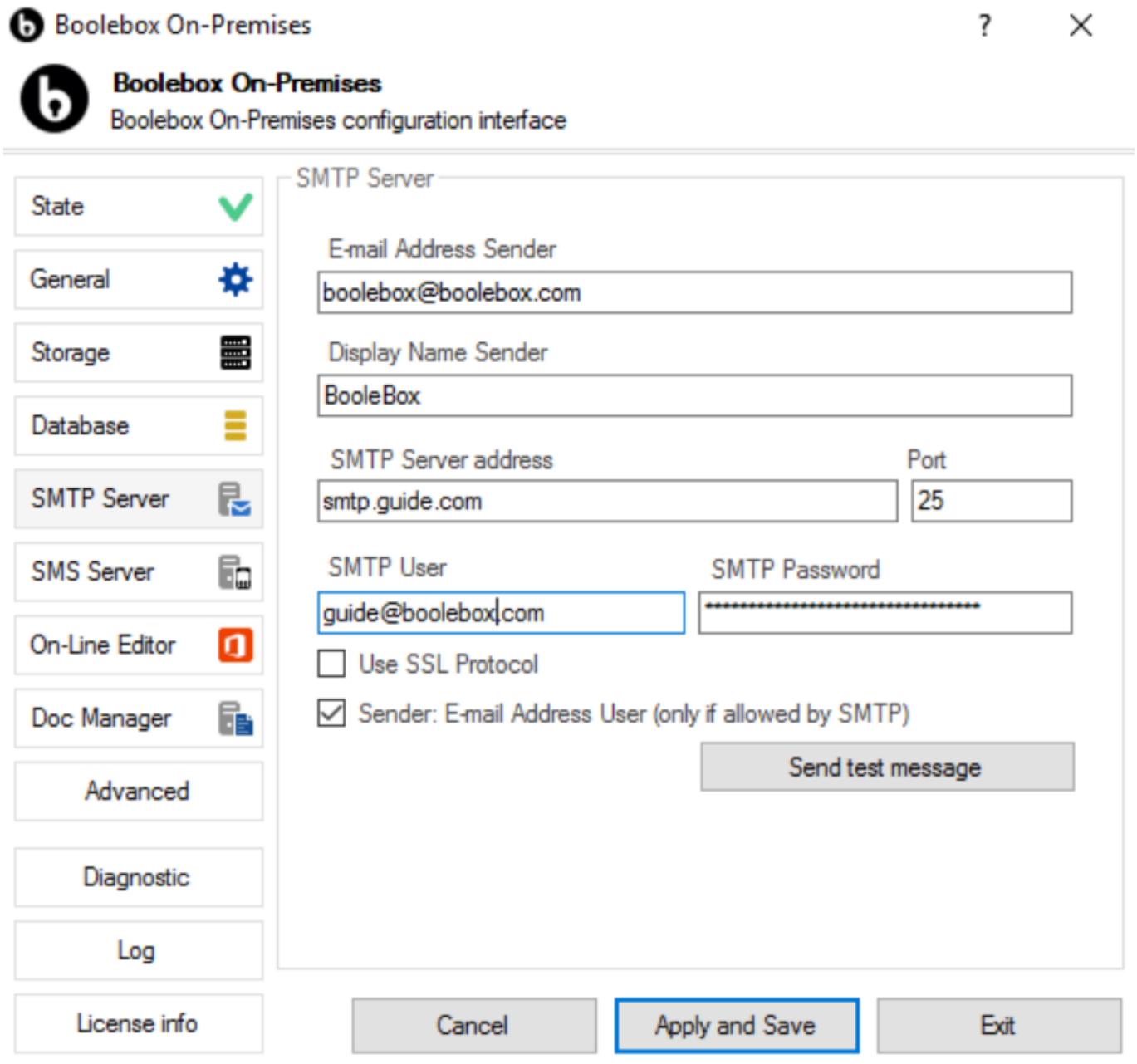

BooleBox On-Premises
Successful connection test
OK

4.5 SMTP server

The SMTP SERVER tab displays information about the mail server used by BooleBox On-Premises. To complete the configuration of this section, these fields must be completed:

- **E-MAIL ADDRESS SENDER –** the e-mail address that will be used to send file sharing notifications on the BooleBox platform.
- **DISPLAY NAME SENDER –** the name associated with the specified e-mail address, which is the name that will be displayed as the sender of the notification message.
- **SMTP SERVER ADDRESS –** the IP address or the FQDN name of the mail server.
- **PORT –** the communication port used by the e-mail server: 25 in case of standard connection or 587 in case of secure connection.
- **USER SMTP –** the username for the e-mail address specified in the E-MAIL ADDRESS SENDER field.
- **SMTP PASSWORD –** the password for the user just mentioned.
- If you want to use a secure connection, click on the SSL/TLS PROTOCOL checkbox.
- If you want to replace the address **noreply@boolebox.com** displayed in the notification e-mails with the BooleBox account e-mail, click on the SENDER E-MAIL ADDRESS USER checkbox. Warning: this feature is available only for SMTP servers that support it.
- Click on APPLY AND SAVE.

Note: in order to install the Common Criteria EAL2+ certified version of BooleBox On-Premises, you must set a secure connection by clicking on the SSL/TLS PROTOCOL checkbox. More precisely, the type of certificate inserted must be TLS 1.2 and the server mail port to be indicated must be 587.


Boolebox On-Premises
Boolebox On-Premises
Boolebox On-Premises configuration interface
State
General
Storage
Database
SMTP Server
SMS Server
On-Line Editor
Doc Manager
Advanced
Diagnostic
Log
License info
SMTP Server
E-mail Address Sender
booleboxx@boolebox.com
Display Name Sender
BooleBox
SMTP Server address
smtp.guide.com
Port
25
SMTP User
guide@boolebox.com
SMTP Password
Use SSL Protocol
Sender: E-mail Address User (only if allowed by SMTP)
Send test message
Cancel
Apply and Save
Exit

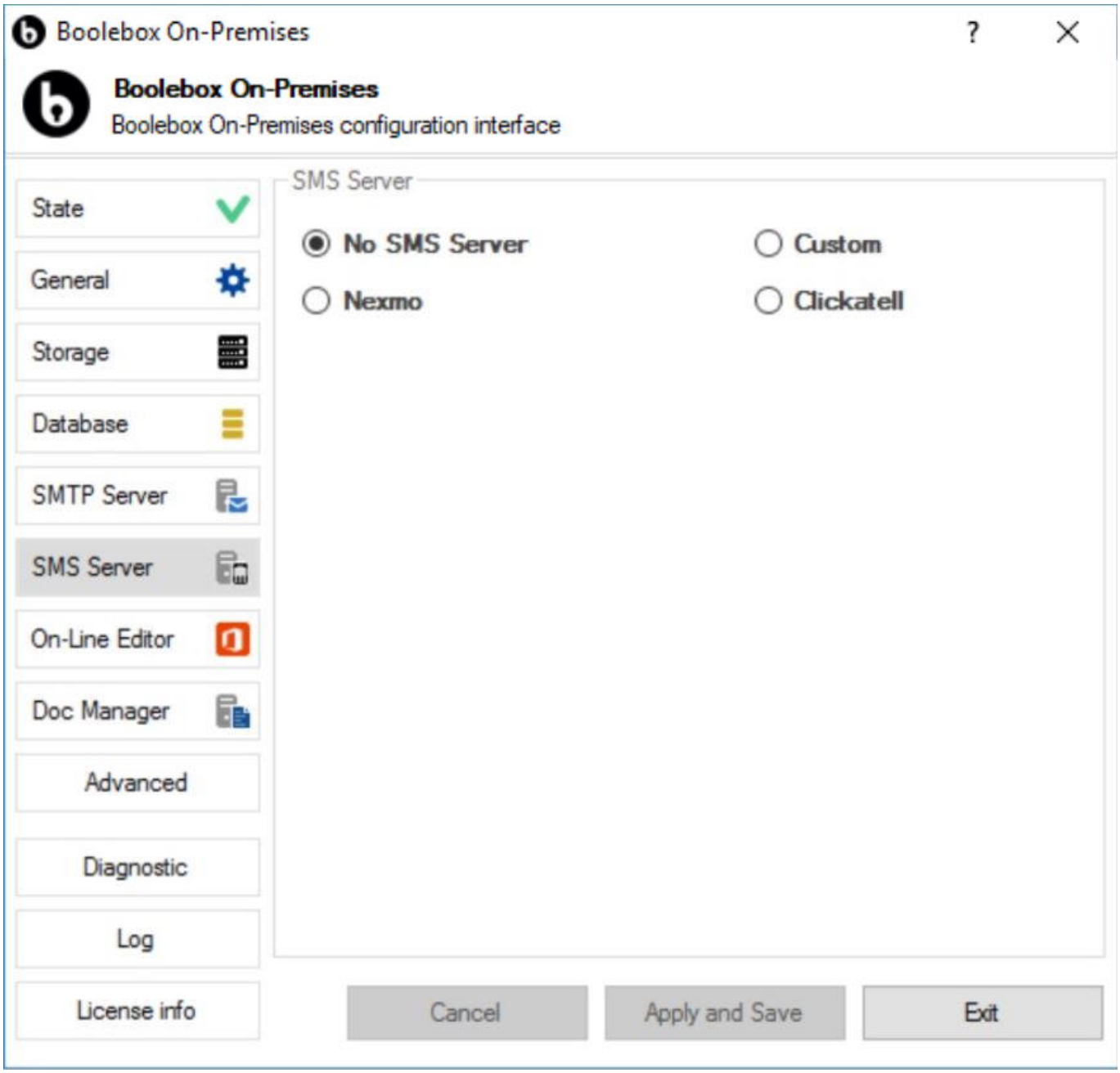
4.6 SMS server

Within the SMS SERVER tab, the SMS gateway service providers are displayed. Configuring an SMS gateway service provider is a prerequisite for using the two-step verification process with OTP (One Time Password) via SMS. You can select one of the following options, each of which must be confirmed by clicking APPLY AND SAVE:

- **NO SMS SERVER –** the OTP is sent via e-mail.
- **CUSTOM –** the OTP is sent via the internal SMS gateway to the corporate network. To configure the corporate gateway service:- In the SERVER URL field, enter the URL address for the company internal SMS gateway.
  – In the PARAMETERS area, specify the parameters for the SMS gateway provider to be sent to the URL indicated above. The TO and TEXT parameters, corresponding to the recipient's number and message text, are mandatory. You can also change the default name parameters by double clicking on the parameter of interest, adding new ones by selecting them and clicking on the '+' button or removing them by selecting them and clicking on the "-" button.
- **NEXMO –** the OTP is sent through the online service of NEXMO. To configure the NEXMO gateway service:- In the URL SERVER field, specify the URL address for the SMS NEXMO gateway.
  – In the SENDER NAME field, enter the name that will appear as the sender of the message.
  – In the KEY API field, enter the key to allow the integration of NEXMO with BooleBox On-Premises.
  – In the SECRET API KEY field, enter the secret key released by NEXMO to allow integration with BooleBox On-Premises.
- **CLICKATELL –** the OTP is sent via the CLICKATELL online service. To configure the CLICKATELL gateway service:- In the CLICKATELL SERVER URL field, specify the URL for the CLICKATELL gateway.
  – In the CLICKATELL API ID field, enter the key to allow CLICKATELL integration with BooleBox On- Premises.

– In the CLICKATELL USER field, enter the username issued by Clickatell to access the service.
– In the CLICKATELL PASSWORD field, enter the password issued by Clickatell to access the service.

Note: in order to obtain the Common Criteria EAL2+ certified version, you must configure NEXMO or CLICKATELL as a SMS gateway service provider. More precisely, the NO SMS SERVER option must not be enabled.

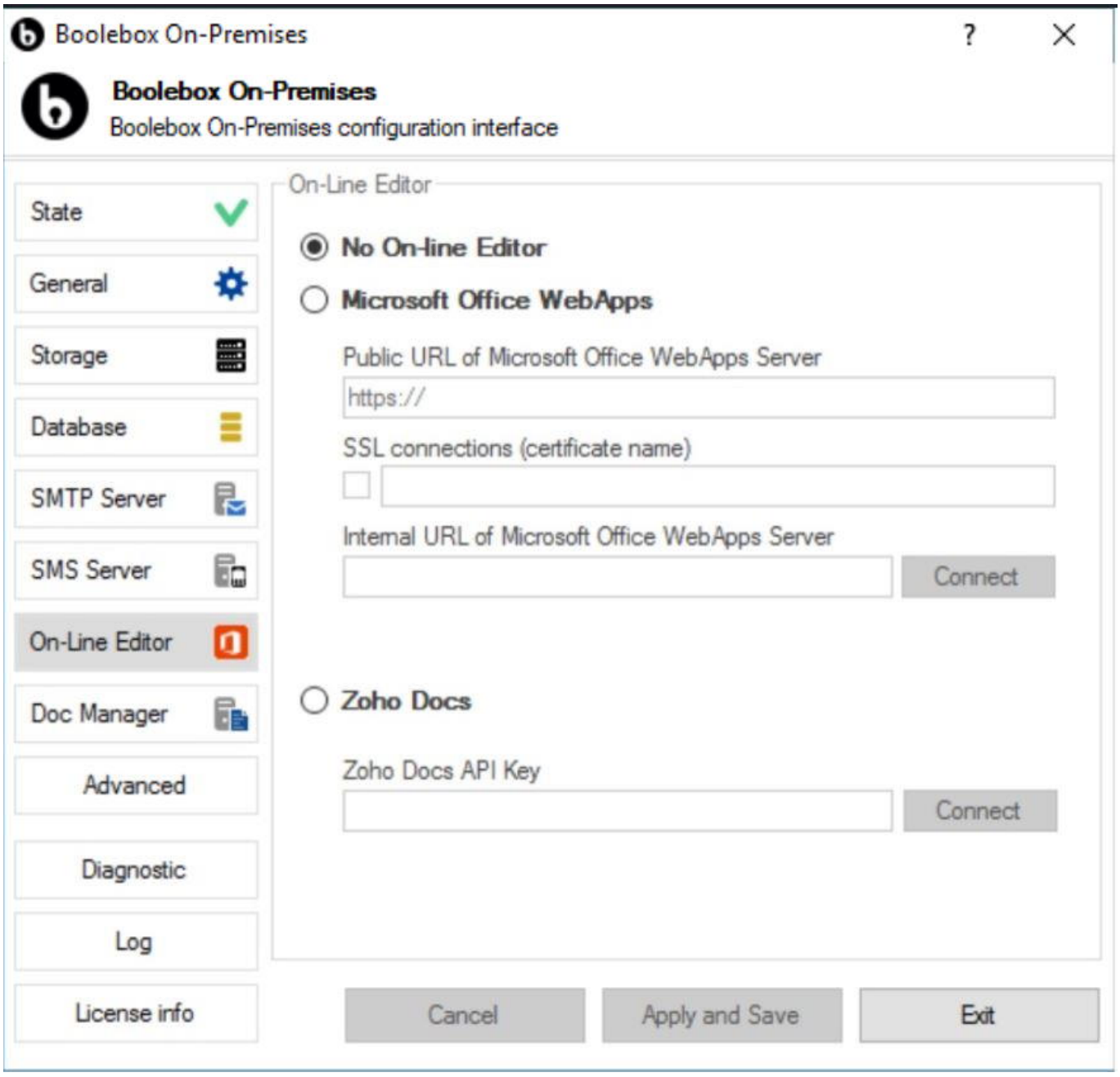

Boolebox On-Premises
Boolebox On-Premises
Boolebox On-Premises configuration interface
State
General
Storage
Database
SMTP Server
SMS Server
On-Line Editor
Doc Manager
Advanced
Diagnostic
Log
License info
SMS Server
No SMS Server
Custom
Nexmo
Clickatell
Cancel
Apply and Save
Exit

4.7 On-line editor

Within the ON-LINE EDITOR tab, it is possible to manage the settings related to the online editing tool, which can be used to edit documents directly on the platform, without having to download them. You can select one of the following options, each of which must be confirmed by clicking APPLY AND SAVE:

- **NO ON-LINE EDITOR –** when enabled, this option doesn't allow you to edit documents online.
- **MICROSOFT OFFICE WEB APPS –** when enabled, this option allows you to use Microsoft Office as an online editing platform.To use Microsoft Office:
  – in the PUBLIC URL OF MICROSOFT OFFICE WEBAPPS SERVER field, enter the public URL of the Microsoft Office Web Apps server used for online editing inside the platform.
  If you want to use a secure connection to the server webapps, click on the SSL CONNECTIONS checkbox and indicate in the next field the friendly name related to the SSL certificate used.
  – in the INTERNAL URL OF MICROSOFT OFFICE WEB APPS field, enter the internal URL of the Microsoft Office Web Apps server used for the online editing within the platform.
  – Click on CONNECT to automatically start the Office Web Apps server configuration based on the parameters shown in the previous fields.
- **ZOHO DOCS –** when enabled, this option allows BooleBox to use Zoho as an online editor. To select this option, you need a Zoho license, whose API Key must be entered in the appropriate field.

Note: in order to install the Common Criteria EAL2+ version of BooleBox On-Premises, you must enable the NO ON-LINE EDITOR option.


Boolebox On-Premises
Boolebox On-Premises
Boolebox On-Premises configuration interface
State
General
Storage
Database
SMTP Server
SMS Server
On-Line Editor
Doc Manager
Advanced
Diagnostic
Log
License info
On-Line Editor
No On-line Editor
Microsoft Office WebApps
Public URL of Microsoft Office WebApps Server
https://
SSL connections (certificate name)
Internal URL of Microsoft Office WebApps Server
Connect
Zoho Docs
Zoho Docs API Key
Connect
Cancel
Apply and Save
Exit

4.8 Doc manager

Within the DOC MANAGER tab, it is possible to configure all the parameters related to the Document Manager used for the BooleBox instance in use. To correctly configure this section, you must indicate all the IP addresses for the Document Manager servers.

To add a new IP address:

- Click on ADD.
- Enter the IP address.
- Click on OK.

To remove an IP address:

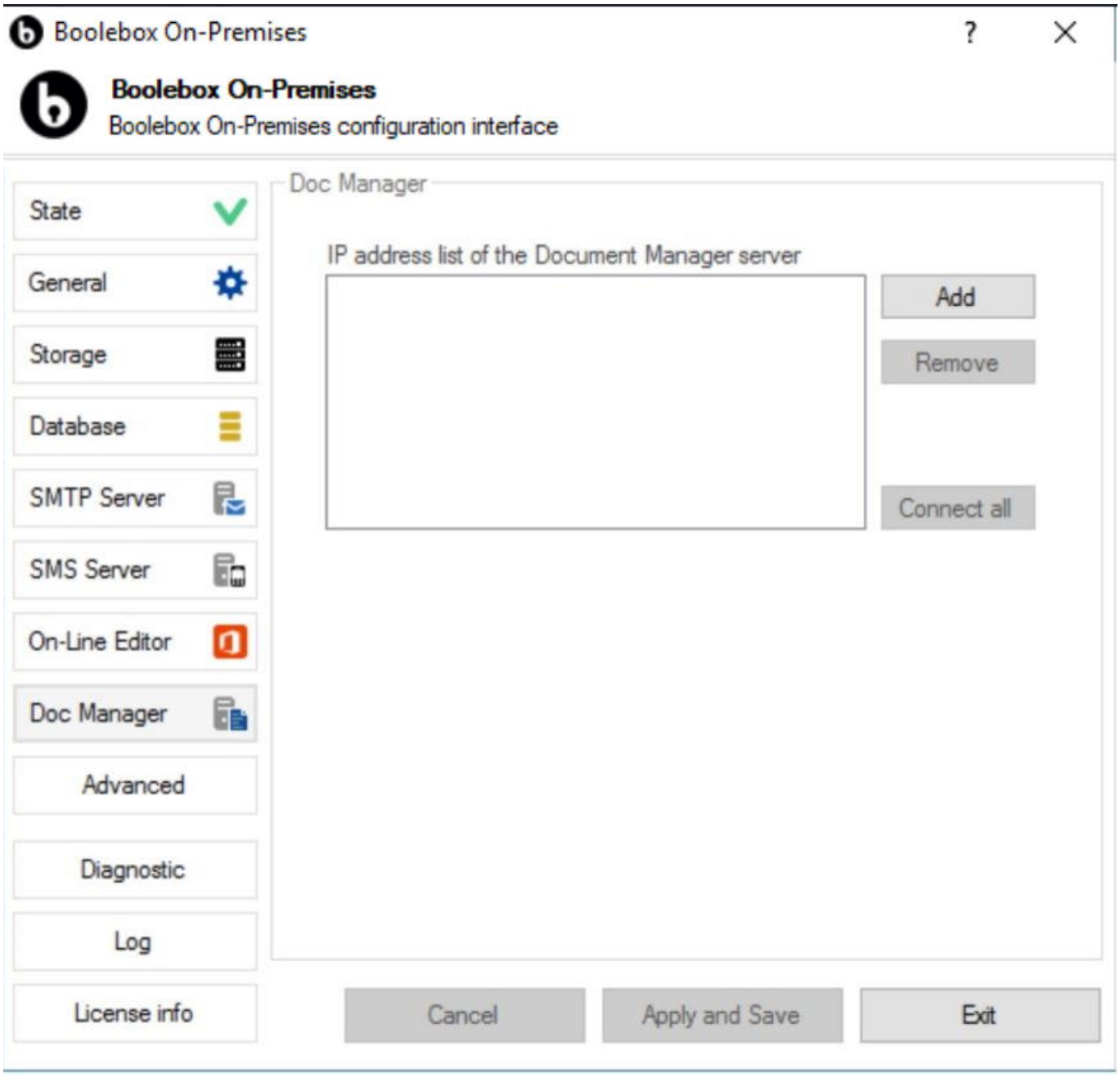
- Click on the IP address.
- Click on REMOVE.

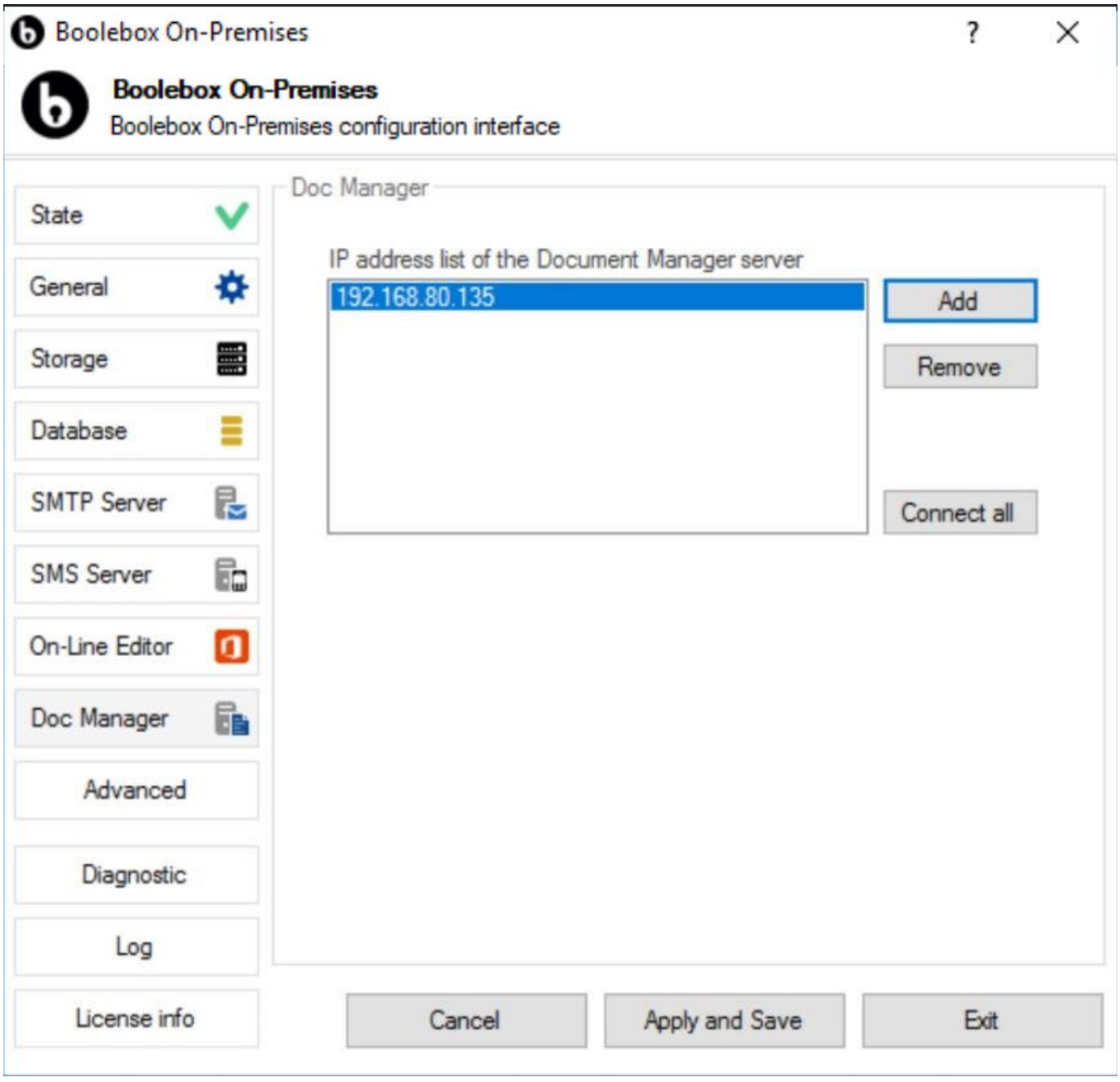
After indicating the IP addresses of the Document Manager servers:

- Click on CONNECT ALL to perform a connection test with all the Document Manager servers listed.
- Click on APPLY AND SAVE to confirm.

Note: before connecting to the server(s) by clicking on CONNECT ALL, it is necessary to have the BooleBox Document Manager Service application installed on each of the specified machines.

Note 2: if using separate servers, the same activation license certificate must be used.


Boolebox On-Premises
Boolebox On-Premises
Boolebox On-Premises configuration interface
State
General
Storage
Database
SMTP Server
SMS Server
On-Line Editor
Doc Manager
Advanced
Diagnostic
Log
License info
Doc Manager
IP address list of the Document Manager server
Add
Remove
Connect all
Cancel
Apply and Save
Exit


Boolebox On-Premises
Boolebox On-Premises
Boolebox On-Premises configuration interface
State
General
Storage
Database
SMTP Server
SMS Server
On-Line Editor
Doc Manager
Advanced
Diagnostic
Log
License info
Doc Manager
IP address list of the Document Manager server
192.168.80.135
Add
Remove
Connect all
Cancel
Apply and Save
Exit

4.9 Advanced

Within the ADVANCED tab, you can enable the WINDOWS AUTHENTICATION and STRONG AUTHENTICATION options. To activate the WINDOWS AUTHENTICATION option:

- Click on the WINDOWS AUTHENTICATION checkbox.
- Accessing the BooleBox platform, thanks to Kerberos and NTLM integrations, will now be possible also inserting the same credentials used to access the company domain.

To enable the use of STRONG AUTHENTICATION certified systems (SiteMinder and DataPower):

- Select the desired STRONG AUTHENTICATION system from the drop-down menu.**Note: if the DATAPOWER item is selected, the SHARED KEY field will appear, in which the key generated by the DataPower system and used to decrypt session cookies must be entered.**

Note: to enable the WINDOWS AUTHENTICATION option successfully:

- **The BooleBox WebApps servers must be added to the corporate domain.**
- **The WINDOWS AUTHENTICATION option must be enabled in the IIS of the BooleBox and RestApi sites.**

To configure the integration between BooleBox and Splunk:

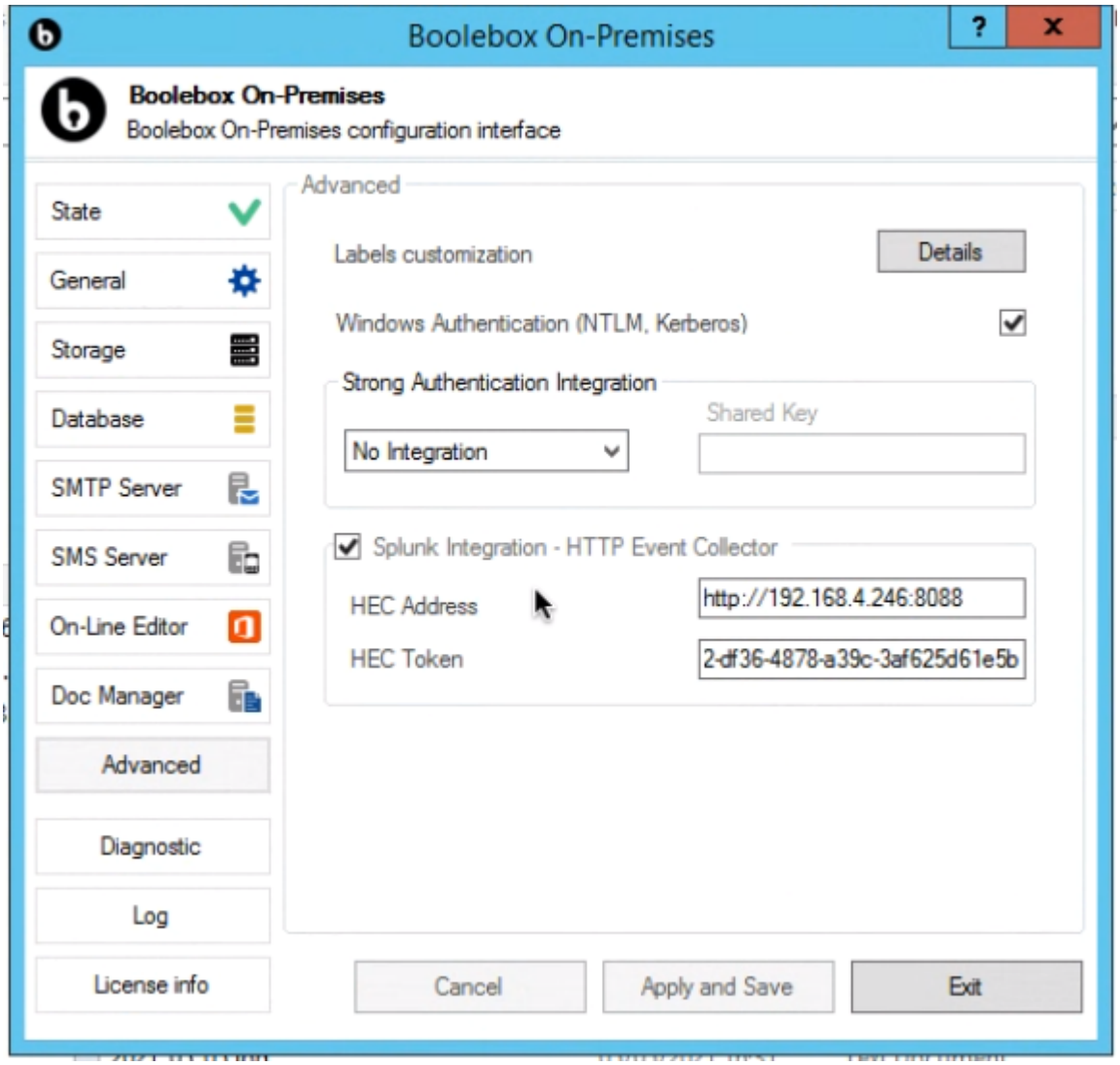
- Click on the checkbox SPLUNK INTEGRATION – HTTP EVENT COLLECTOR.
- Insert the HEC ADDRESS.
- Insert the HEC TOKEN.

Note: for details concerning Splunk configuration, please visit this link.

Note: By clicking on the WINDOWS AUTHENTICATION checkbox, the login page will show the link to access the BooleBox platform using the Windows credentials, that will be validated by IIS.

If the SSO option (Single Sign On) is not enabled, you will have to click on the WINDOWS AUTHENTICATION link also for logins subsequent to the first one; otherwise, credentials won't be asked again and the Windows credentials shown will be automatically used to access the platform.

Note: in order to configure the Common Criteria EAL2+ certified version of BooleBox On-Premises, you must not use any of the STRONG AUTHENTICATION systems listed above and you must deactivate the flag associated to the WINDOWS AUTHENTICATION checkbox.



4.10 Diagnostic

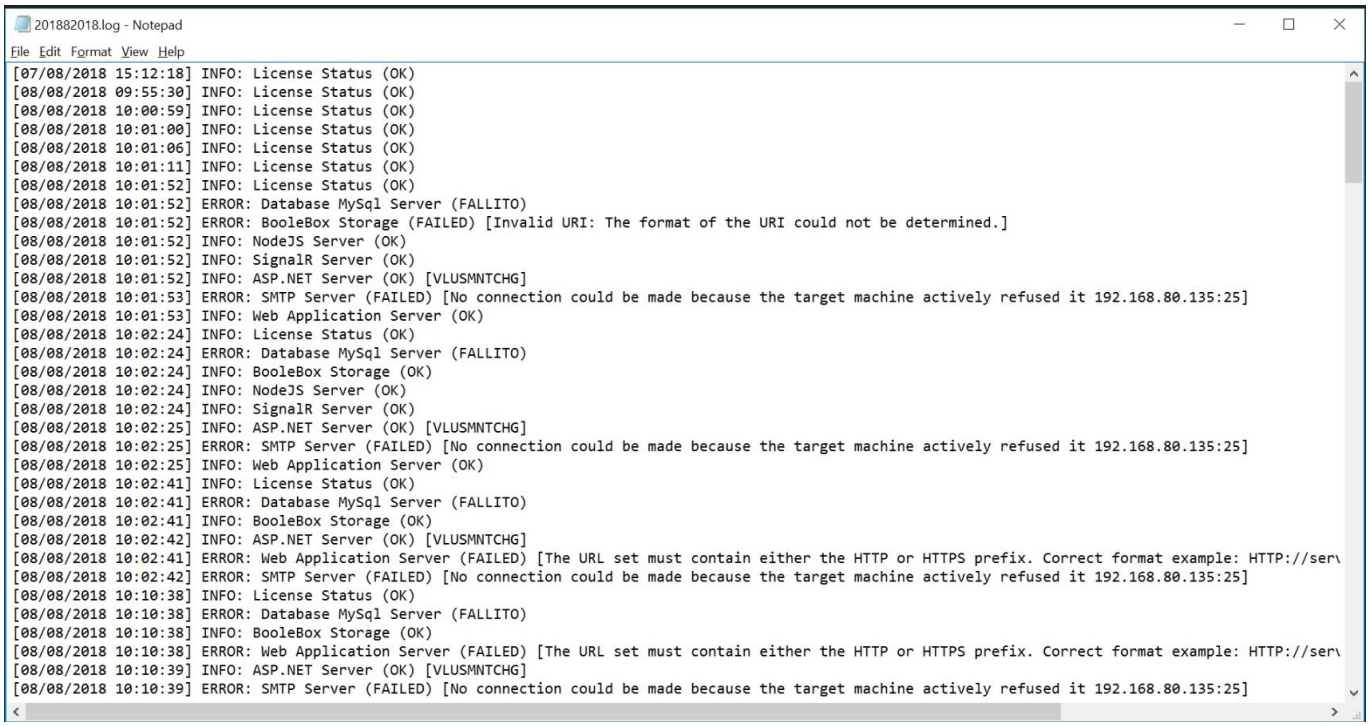
By clicking on the DIAGNOSTIC button, you can perform a test to check the operating status of all BooleBox On-Premises services. Each service, at the end of the verification test, can appear in the following states:

- **OK –** the service works correctly.
- **KO –** the service has not been properly installed or configured.
- **N/A (Not Available) –** The service has not been configured yet.

4.11 Log

By clicking on the LOG button, it is possible to obtain a .txt file showing the logs relating to the BooleBox On-Premises application, to view in detail any errors related to the platform services, shown in red with the wording KO inside the STATE tab.

Note: log files are stored in the C:Program FilesBooleBox on-premisesLogs.



4.12 License info

Within the LICENSE INFO tab, all the information related to the BooleBox On-Premises license is displayed:

- **LICENSE INFO –** the version number of the application in use.
- **LICENSE KEY –** the alphanumeric characters of the BooleBox On-Premises license in use.
- **ACTIVATION DATE –** the activation date of the BooleBox On-Premises license in use.
- **EXPIRATION DATE –** the expiration date of the BooleBox On-Premises license in use.
- **TYPE OF LICENSE –** the type of BooleBox On-Premises license in use (PRIMARY SERVER or SECONDARY SERVER).
- **USER LICENSED –** the number of users covered by the BooleBox On-Premises license in use.
- **USERS CREATED –** the number of users employing the BooleBox On-Premises license in use.
- **APPS AVAILABLE –** the list of functions enabled for the BooleBox On-Premises license in use.**Note: the number of enabled features varies depending on the type of BooleBox On-Premises license purchased.**
- **ENCRYPTION ALGORITHM –** the type of algorithm used by the system.
- A list of information regarding the certificate used during the license activation.

Within the LICENSE INFO tab, it is also possible to change the certificate and update the license.

To change the activation license certificate:

- Click on CHANGE CERTIFICATE.
- In the window that is going to appear on your screen, select the desired certificate.
- Click on OK.

To upgrade the license in use:

- Click on UPDATE LICENSE.

- BooleBox On-Premises server, connecting to the BooleServer internet portal dedicated to licenses activations, will update all the details related to the BooleBox On-Premises license in use.

5 Additional components configuration

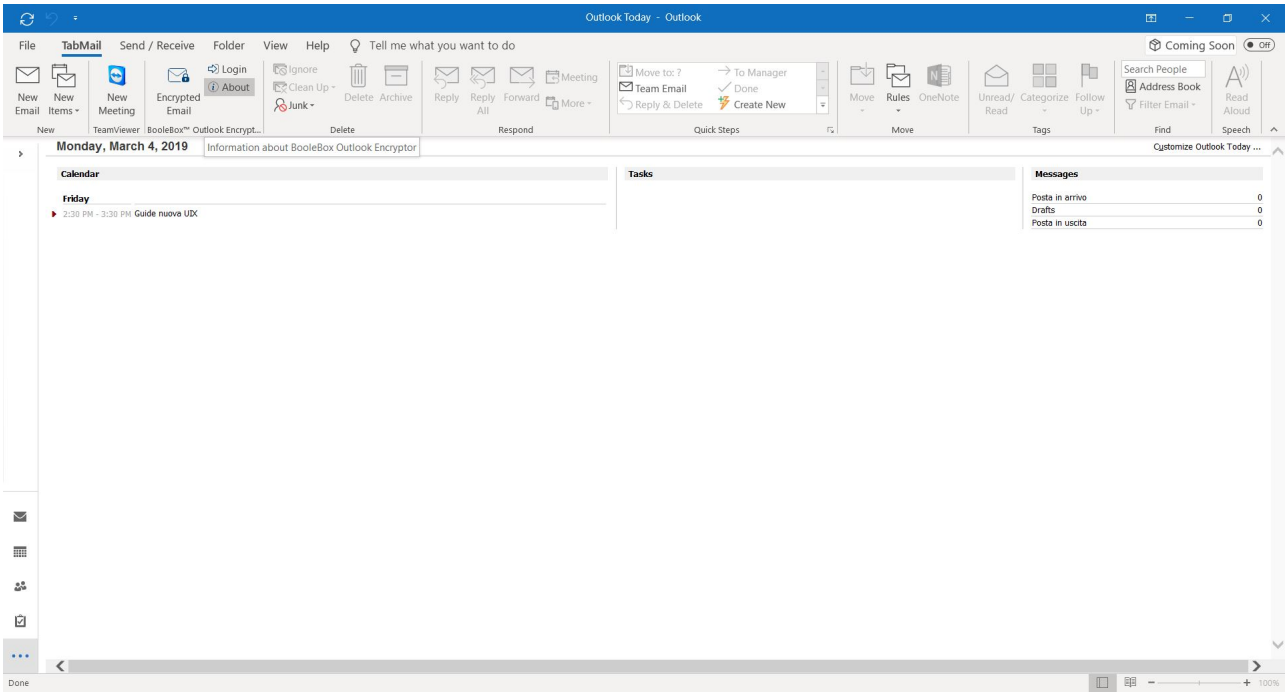
Procedure for configuring Outlook Encryptor, File Encryptor Client, File Encryptor Server and AD Sync.

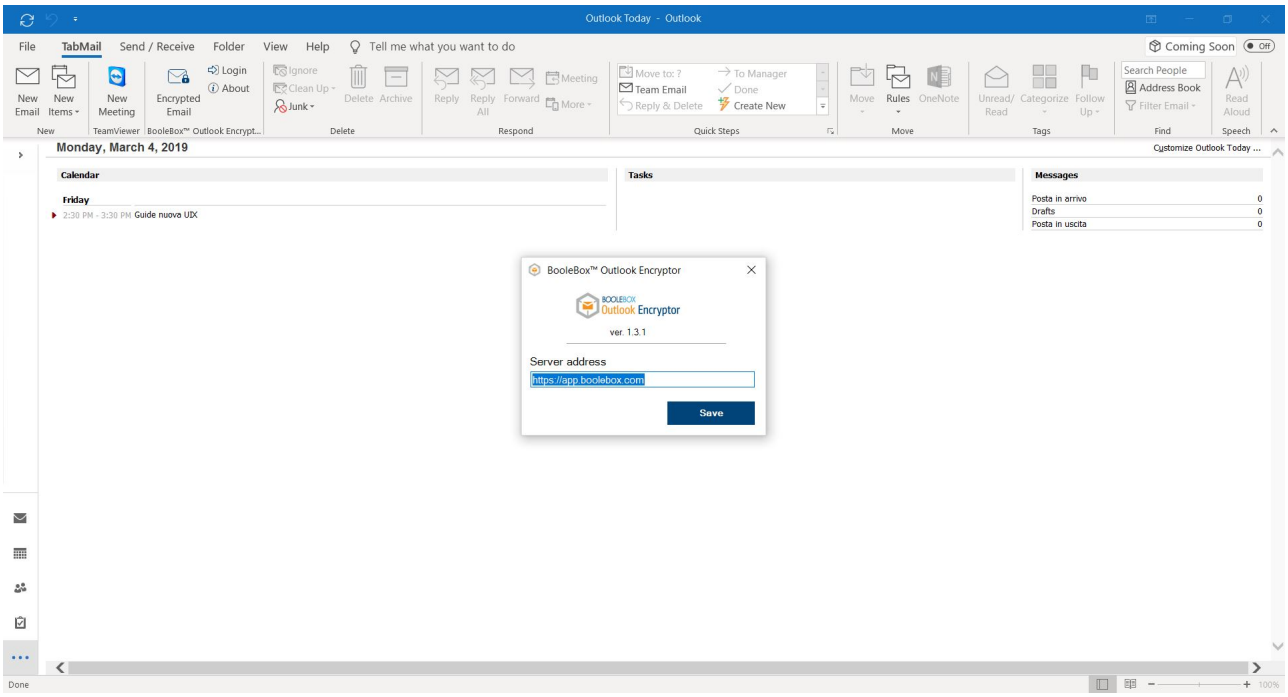
Note: the following chapter deals with the configuration of components that must not be installed for the Common Criteria EAL2+ certified version of BooleBox On-Premises. For this reason, the entire chapter does not apply to the configuration of the platform in the Common Criteria EAL2+ certified version.

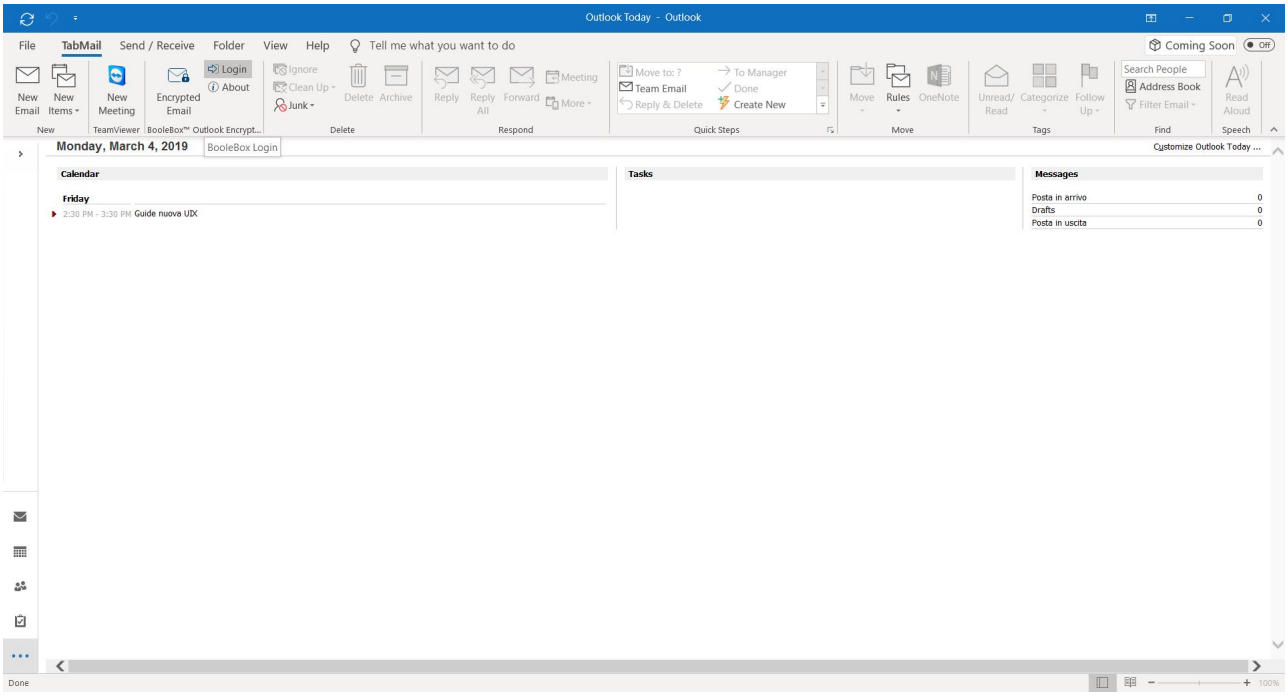
5.1 Outlook encryptor

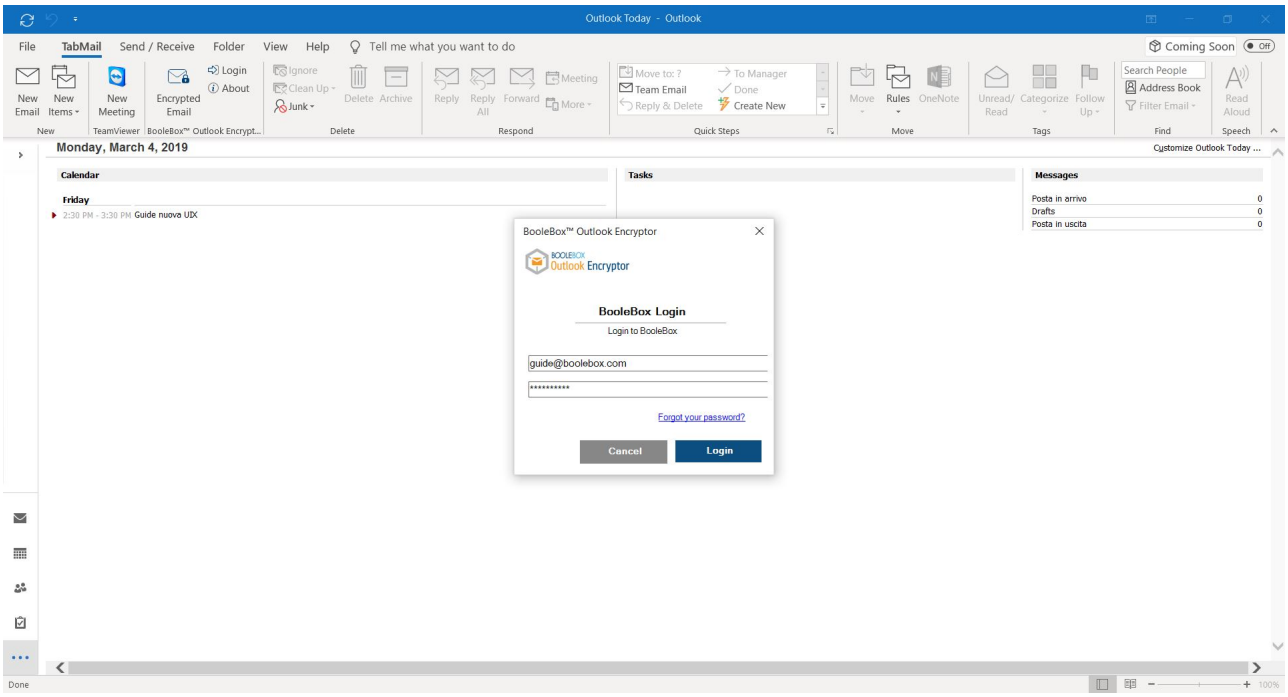
To correctly configure the Outlook Encryptor component:

- Open the Outlook® mail client.
- Click on the ABOUT command in the BOOLEBOX ™ OUTLOOK ENCRYPTOR section of the ribbon to change the URL of the server.
- In the window that is going to appear on your screen, enter the URL of the server that manages BOOLEBOX ON-PREMISES.
- Click on SAVE.
- Click on the LOGIN command in the BOOLEBOX ™ OUTLOOK ENCRYPTOR section of the ribbon to access the server that manages BOOLEBOX ON-PREMISES.
- In the window that is going to appear on your screen, enter your BooleBox account username and password and click on LOGIN.
- Once this operation is completed, the LOGIN button will disappear and a welcome message will be displayed for the configured user.


Outlook Today - Outlook
File
TabMail
Send / Receive
Folder
View
Help
Tell me what you want to do
Coming Soon
Off
New Email
New Items
New Meeting
Encrypted Email
Login
About
Ignore
Clean Up
Junk
Delete
Archive
Reply
Reply All
Forward
Meeting
More
Move to: ?
Team Email
Reply & Delete
To Manager
Done
Create New
Move
Rules
OneNote
Unread/ Read
Categorize
Follow Up
Search People
Address Book
Filter Email
Read Aloud
New
TeamViewer
BooleBox™ Outlook Encrypt...
Delete
Respond
Quick Steps
Move
Tags
Find
Speech
Monday, March 4, 2019
Information about BooleBox Outlook Encryptor
Customize Outlook Today ...
Calendar
Friday
2:30 PM - 3:30 PM Guide nuova UIX
Tasks
Messages
Posta in arrivo 0
Drafts 0
Posta in uscita 0
Done
100%


Outlook Today - Outlook
File
TabMail
Send / Receive
Folder
View
Help
Tell me what you want to do
Coming Soon
Off
New Email
New Items
New Meeting
Encrypted Email
Login
About
Ignore
Clean Up
Junk
Delete
Archive
Reply
Reply All
Forward
Meeting
More
Move to: ?
Team Email
Reply & Delete
To Manager
Done
Create New
Move
Rules
OneNote
Unread/ Read
Categorize
Follow Up
Search People
Address Book
Filter Email
Read Aloud
New
TeamViewer
BooleBox™ Outlook Encrypt...
Delete
Respond
Quick Steps
Move
Tags
Find
Speech
Monday, March 4, 2019
Customize Outlook Today ...
Calendar
Friday
2:30 PM - 3:30 PM Guide nuova UIX
Tasks
Messages
Posta in arrivo 0
Drafts 0
Posta in uscita 0
BooleBox™ Outlook Encryptor
BOOLEBOX Outlook Encryptor
ver. 1.3.1
Server address
https://app.boolebox.com
Save
Done
100%


Outlook Today - Outlook
File
TabMail
Send / Receive
Folder
View
Help
Tell me what you want to do
Coming Soon
Monday, March 4, 2019
BooleBox Login
Calendar
Friday
2:30 PM - 3:30 PM Guide nuova UIX
Tasks
Messages
Posta in arrivo 0
Drafts 0
Posta in uscita 0
Done


Outlook Today - Outlook
File
TabMail
Send / Receive
Folder
View
Help
Tell me what you want to do
Coming Soon
Monday, March 4, 2019
Calendar
Friday
2:30 PM - 3:30 PM Guide nuova UIX
Tasks
Messages
Posta in arrivo 0
Drafts 0
Posta in uscita 0
BooleBox™ Outlook Encryptor
BooleBox Login
Login to BooleBox
guide@boolebox.com
Forgot your password?
Cancel
Login
Done

5.2 File Encryptor Server

To configure the server component of File Encryptor, click on the BOOLEBOX FILE ENCRYPTOR icon – which automatically appears on the desktop with the installation of the server component – and grant the required permissions. In the window that is going to appear on your screen, these fields must be completed:

- **BOOLEBOX SERVER ADDRESS –** l'URL attraverso cui raggiungere il server BooleBox di riferimento (for example https://app.boolebox.com).
- **API KEY –** key that allows API calls to a configured company,available among the company's features within the Dashboard.
- **MULTI-PROCS –** the maximum number of simultaneous encryption processes.**Note: the recommended value is 5, but it can be increased according to the characteristics (RAM and CPU) of the server on which the File Encryptor component was installed.**
- **DEVICE ID –** the name to identify the device on which the File Encryptor Server has been installed, used when the configured rule must be valid only for a specific device.
- Click on SAVE to complete the operation.

If the corporate network is configured with a proxy, the File Encryptor Server requires configuration of the related proxy. To configure the proxy server:

- Click on the File Encryptor Server icon that appears on your desktop at the end of the installation.
- Select the USE PROXY item.
- Enter the reference address of the proxy you want to configure in the appropriate field.
- If you want to bypass the newly configured proxy server, select the SET BYPASS PROXY item.
- If you need to enter the credentials to access the proxy, select USE NETWORK CREDENTIALS and enter the username and password of the relevant network.
- Click on SAVE to complete the operation.

To find out further information about File Encryptor usage and configuration, please refer to this link.

5.3 File Encryptor Client

If the corporate network is configured with a proxy, the File Encryptor Client requires the configuration of the relevant proxy. To configure a proxy server:

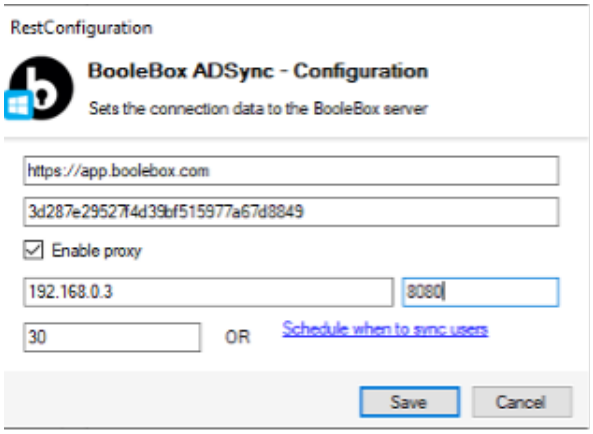
- Double-click on the FILE ENCRYPTOR (CLIENT) shortcut and select the item SET PROXY.
- Select the USE PROXY item, enter the IP or URL address of the proxy to be configured and, if necessary, the NETWORK CREDENTIALS.

To find out further information about File Encryptor usage and configuration, please refer to this link.

5.4 AD Sync

To correctly configure the AD SYNC component, after opening the application for the first time, the following fields must be completed:

- **SERVER ADDRESS –** the address of the BooleBox server, reachable via http and https connections.
- **KEY API –** The company KEY API generated in the BooleBox Dashboard.
- **PROXY USERNAME –** username to access the proxy server.
- **PROXY PASSWORD –** password to access the proxy server.
- **TIMER –** the time interval in minutes that the system will request from the AD SYNC application.
- Click on SAVE to save the configured settings.

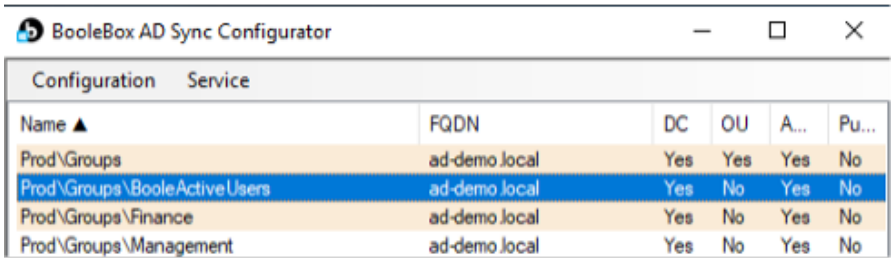


The main screen shows the groups and the OU (Organizational Units) that are synchronized. For each group/OU, the following information will be displayed:

- **NAME –** the group name.
- **FQDN –** Fully Qualified Domain Name.
- **DC –** Domain Controller.
- **OU –** Organizational Unit.
- **AD AUTH –** information that indicates whether the group uses the BooleBox password or

AD users.

- **PUBLIC –** information that indicates whether a BooleBox group is public or private.



5.5 BooleBox AD Service

In order to correctly configure the BooleBox AD Service component, you will have to indicate in the SETTINGS.CONFIG file a DC (Domain Controller) and a FQDN (Fully Qualified Domain Name) modifying the following lines with the required specifications:

- <add key=”AddressDomainController” value=”” />” in <add key=”AddressDomainController” value=”DC ADDRESS OR DNS” />
- <add key=”FQDN” value=””/> in <add key=”FQDN” value=”FQDNNAME”. />

If not presents add the following lines, modifying the required value for LDAPS key:

- <add key=”Authentication” value=”LDAP” />
- <add key=”LDAPS” value=”false” />

Note: if not changed during installation, the path SETTINGS.CONFIG file path will be: C:Program FilesBooleBox AD Service

6 Mobile app configuration

If you purchased BooleBox On-Premises and you want to configure the mobile application through MDM (Mobile Device Management) to change the server to which the application will connect, perform the following actions:

- Create a **config** file by setting the file extension as **.json.**
- Enter the company server URL in the file.
- Copy the created file in the root directory of all the devices that will have access to the mobile application.

Note: BooleBox mobile application is not part of Common Criteria EAL2+ certified TOE (Target Of Evaluation).

7 Activities monitoring

Windows services to be verified in case of failures or checks of BooleBox platform activities.

7.1 Actvities monitoring

To monitor the operating status of the platform, it is necessary to use BooleBox On-Premises control panel. In case some problems that cannot be resolved with the tool in the control panel (CONNECT) occur, you must check the status of the following Windows services (when installed):

- ASP.NET State Service.
- BooleBox Document Service.
- BooleBox Server Service.
- World Wide Web Publishing Service.
- NodeJS.
- The name of the MySQL service.

  Note: the default name of the service is MySQL57. If changed during installation, check that the name matches the one assigned.

8 Backup & restore

Cautions necessary before embarking on a backup & restore procedure.

8.1 Backup & restore

Should you wish to undertake a backup and restore procedure for the components of the platform, it is necessary to provide for the saving of:

- **STORAGE** – containing all the encrypted data.
- **DATABASE** – containing all the references to the files on the storage, as well as all the configuration parameters made through the Dashboard and the activity logs.
- **FILE BOOLEBOX.DAT** – containing part of the encryption key used by the system (localized, if the path was not changed during installation, in C: Program Files BooleBox On-Premises).
- **MASTER KEY ENCRYPTION CERTIFICATE** – selected during license activation to encrypt all configuration files and to protect the license in use.

For storage and database, the backup frequency should be scheduled according to usage; a weekly frequency is anyway recommended.

The BooleBox.dat file must be saved every time the system configuration is changed.

We recommend to perform backup/restore procedures out of the platform usage hours. Before proceeding with the backup/restore procedure it is advisable to stop the IIS service on the WebApp server.

9 Common Criteria EAL2+ certification

In order to configure BooleBox in the certified Common Criteria EAL2+ version, it is necessary to verify that the safety objectives defined for the operating environment are satisfied.

OPERATIONAL ENVIRONMENT OBJECTIVE	DESCRIPTION	SECURITY PRECAUTIONS TO BE TAKEN
OE.IDENTIFY	The Operational Environment supports the TOE in identifying and authenticating the authorized Operating System Administrators, authorized DBMS Administrator and authorized Storage Administrator.	Configure the Operating System, the DBMS and the Storage in such a way that they identify the administrators of the TOE through credentials of adequate robustness. Set a password for the administrator of the DBMS and the Operating System that respects the complexity criteria defined for the TOE.
OE.AUDIT PROTECT	The operational environment shall provide the capability to protect the integrity of audit log files generated by the TOE.	Perform an incremental and continuous backup of the database managed by the TOE. Configure the area of the DB where the log files reside in such a way that it is accessible only to authorized DB administrators.
OE.PHYSICAL ACCESS	The physical access to the area where the TOE is hosted will be granted to TOE authorized administrators only.	Install the TOE in a controlled access area, which can only be accessed by authorized administrators.

OE.DB	Those responsible for the TOE configuration and administration must ensure that access to the database via mechanisms outside the TOE boundary is restricted to TOE authorized administrators only, that will be configured in the DBMS as database administrators. The DB is considered by the TOE as a trusted IT Product.	Make sure that the administrators of the DBMS are all and only the administrators of the TOE. Make the Database reachable only from the TOE machine.
OE.SO	Those responsible for the TOE configuration and administration must ensure that access to the Operating System via mechanisms outside the TOE boundary is restricted to TOE authorized administrators only, that will be configured in the Operating System as OS System Administrators. Only TOE authorized administrators can launch and execute TOE components and review the log files stored by the OS. The OS is considered by the TOE as trusted IT product.	Make sure that the users of the Operating System are all and only the administrators of the TOE.
OE.STORAGE	Those responsible for the TOE configuration and administration must ensure that physical and logical access to the storage in TOE environment via mechanisms outside the TOE boundary is restricted to TOE authorized administrative users only. The STORAGE is considered by the TOE as trusted IT product.	If the Storage is implemented on NAS, SAN or File Server instead of on the local File System of the TOE, the Storage must: • Be installed in the same room where the TOE was installed. • Be accessible only by TOE administrators.

OE.STAFF	Staff working as TOE authorized administrator shall be faithfully selected, skilled and trained for proper operation without compromising the TOE and proper TOE configuration at installation phase.	Make sure that the personnel appointed by the TOE administrator have followed the training courses provided by the BooleBox technical support team and have been selected in accordance with the company’s selection policies and procedures.
OE.TIME	The operational environment shall provide a reliable time reference.	Configure the Operating System with a reliable clock timing.
OE.CRYPTO	The Operational Environment shall provide FIPS 140-2 validated cryptographic functionalities (RSA 2048 bit key generation, AES 256 bit key generation, Random Number Generation for OTP generation, Random alphanumeric string generation for key generation, RSA encryption/decryption, SHA256 hashing, AES 256 encryption/decryption using .NET 4.5.1 libraries) and protocols (HTTPS based on AES 256 and RSA 2048) to properly support the TOE for audit log file protections and secure transfer of information between End User side and Server Side and between the TOE and other non-TOE component required in the TOE environment.	Configure the security policies of the Operating System in order to be able to use the FIPS 140-2 validated cryptographic features. Also make sure that secure communication protocols are active (HTTPS based on AES 256 and RSA 2048) to correctly support the TOE for the protection of log files, control and secure transfer of information both between the end user and server side, and between the TOE and another component not required in the TOE environment.

OE.ALIGNEDBACKUP	The operational environment should provide a secure back-up of the DBMS data, of the Storage, of the BooleBox.dat configuration file and of the certificate used to encrypt the Master Key.	It is advisable to perform incremental backups with intervals adapted to the operating needs of the company in question.
OE.CONTINUITY	The operational environment shall provide a system to ensure operational continuity in the event of a power failure.	Provide support units in the operating environment appropriate to the needs of the company in question (UPS, generator set, alternative electrical supply system, etc.) for managing the lack of electricity for prolonged periods that could cause data loss.
OE.AUDIT	The Operational Environment shall support the TOE in the generation of audit records, correlating them to the proper user when applicable, as a result of specific TOE activities and operations performed by TOE users. In addition, the Operational Environment shall guarantee that only OS System Administrators (the only System Administrators configured at OS level are TOE authorized administrators) can accede and visualize the aforementioned audit information.	Activate the audit functions of the operating system and of the DBMS to record the actions performed by the respective administrators.

OE.LOG STORE	The operating environment shall grant that there is enough space dedicated to log management.	Implement a procedure to periodically check the remaining space for log management or alternatively install a software that informs the administrative user when the storage space dedicated to logs is about to end.
OE.INTEGRITY	The Operational environment shall provide the capability to protect the integrity of executable files of the TOE using .NET framework technology.	Use software that preserves hashes of the executable files used and alarms the user in case of file manipulation.
OE.CERTIFICATE	The Operational environment shall support the TOE generating and securely storing the certificate containing the Kpriv and the Kpub used for BBOP MASTER KEY encryption/decryption.	Use secure systems for generating and storing the digital certificate. It is advised to use Common Criteria certified HSM systems.
OE.PERSONALKEY	The Operation environment shall grant a secure distribution of a personal key correlate to a classification project and users are responsible for the secure management of their personal keys.	It is recommended to save the Personal Key used on a file uploaded on BooleBox and protected with Personal Key.

OE.DOC	Those responsible for the TOE configuration and administration must ensure that access to the Document Manager Server via mechanisms outside the TOE boundary is restricted to TOE authorized administrators only, that will be configured in the Document Manager Server as Document Manager Server Administrators. The Document Manager Server is considered by the TOE as a trusted IT Product.	Make sure that the users of the Document Manager Server are all and only the administrators of the TOE.

10 Configuration – troubleshooting

Welcome to the CONFIGURATION – TROUBLESHOOTING section of BooleBox guide. In this section you will find useful indications aimed at solving typical problems that may arise during the BooleBox On-Premises configuration phases. The section puts at your disposal both a paragraph in which the typical error situations related to the control panel functions are grouped, and some specific paragraphs relating to all the other components connected to the base platform.

10.1 Control panel

BooleBox On-Premises control panel allows the administrator user to check the operating status of the services connected to the platform through the available tabs. In this paragraph the typical error situations that may occur in relation to control panel functionalities are grouped.

10.1.1 General TAB

IP Server address of the ASP.net State Service session

If the connection check performed through the CONNECT button doesn’t work, you must verify:

- **ASP.NET SERVICE STATUS –** in order to guarantee the correct functioning of the platform, the ASP.NET service must be running; in addition, the settings relating to the service must impose automatic execution when the server is started: in the event of restarting it the service must indeed restart automatically. You can check the status of the service through the Windows services panel and, if it is not started, restart it manually.
- **SERVER IP ADDRESS AND CONNECTION PORT –** in order to guarantee the correct

functioning of the platform, the server must be reachable on the network at the IP address specified through the indicated port. If the indicated server is protected by a specific firewall, it is necessary to open the TCP/IP ports according to the firewall rules, in order to allow in any case to reach the server. To make sure that all the prerequisites listed above are respected, check that in the GENERAL tab, in correspondence with the IP SERVER ADDRESS OF THE ASP.NET STATE SERVICE SESSION field, the IP address of the server and its port have been correctly indicated. Please note that the server to be specified corresponds to the one where the service was installed: more precisely, the format of the address to be indicated is serveripaddress:42424.

Public URL of BooleBox Server

If the connection check performed through the CONNECT button doesn't work, you must verify:

- **SERVER IP ADDRESS AND CONNECTION PORT –** in order to guarantee the correct functioning of the platform, the server must be reachable on the network at the IP address specified through the indicated port. If the indicated server is protected by a specific firewall, it is necessary to open the TCP/IP ports according to the firewall rules in order to allow in any case to reach the server. To make sure that all the prerequisites listed above are respected, check that in the GENERAL tab, in correspondence to the PUBLIC URL OF BOOLEBOX SERVER field, the indicated IP address corresponds to that of the server on which the BooleBox Web App has been installed. The format of the IP address must be http://serveripaddress:80 if the HTTP connection protocol is used and https://serveripaddress:443 if the HTTPS connection protocol is used.
- **IIS SERVER STATUS –** in order to guarantee the correct functioning of the platform, it is necessary that the IIS server where the application was published is active. Then verify that the IIS server is activated, that the publication port is the correct one (80 for the http protocol, 443 for the https protocol) and that the website is online and running through the IIS management console in Windows Server.

URL SERVER ADDRESS OF SIGNAL R

If the connection check performed through the CONNECT button doesn't work, you must verify:

- **SERVER IP ADDRESS AND CONNECTION PORT –** in order to guarantee the correct

functioning of the platform, it is necessary to verify that, in correspondence with the URL SERVER ADDRESS OF SIGNALR field inside the GENERAL tab, the IP address and the relative port have been correctly indicated to allow the server to be reached at the IP address specified through the indicated port. In particular, the IP address must correspond to that of the server on which the component was installed; the IP address has to be specified in the format http://serveripaddress:80 if you are using HTTP protocol or http://serveripaddress:443 if you are using HTTPS protocol. Furthermore, if the server in question is protected by a specific firewall, it is necessary to open the TCP/IP ports in accordance with the rules of the same firewall to ensure in any case that the server is reached.

- **IIS SERVER STATE –** in order to guarantee the correct functioning of the platform, it is necessary that the IIS server where the application was published is active. Then verify that the IIS server is activated, that the publication port is the correct one and that the website is online and running through the IIS management console in Windows Server.

ADDRESS SERVER URL OF NODEJS

If the connection check performed through the CONNECT button doesn’t work, you must verify:

- **SERVER IP ADDRESS AND CONNECTION PORT –** in order to guarantee the correct functioning of the platform, the server must be reachable on the network at the IP address specified through the indicated port. If the indicated server is protected by a specific firewall, it is necessary to open the TCP/IP ports according to the firewall rules in order to reach the server in any case. To ensure that all the prerequisites listed above are met, check that in the GENERAL tab, in correspondence with the URL SERVER ADDRESS OF NODEJS field, the IP address indicated corresponds to that of the server on which the component was installed. The IP address format must be http://serveripaddress:3000 if the HTTP connection protocol is used and https://serveripaddress:3500 if the HTTPS connection protocol is used.

Note: in some cases, such as the failure of internal platform notifications, a reset of the NodeJS component may be necessary. In order to do this, perform the following actions:

- Access the server where the NodeJS component was installed.
- Open the task manager.
- End the process “Node.js: Server-side JavaScript”.
- Restart the BOOLEBOXSERVERSERVICE.EXE service from the Windows control panel.
- Click on the related CONNECT button in the GENERAL tab of the control panel of BooleBox to check the status of the component.

Note: in case of use of HTTPS protocol with TLS certificate supplied by the customer, it is necessary to configure the IIS bindings so that port 443 can be used. For the IIS configuration relating to port 443, please refer to this link.

Note: to proceed with the configuration of BooleBox On-Premises in accordance with the criteria imposed by the Common Criteria EAL2 + certification, it is necessary to configure the BooleBox On Premise site to listen only via the HTTPS protocol, by deactivating the HTTP port activated by default or by automatically upgrading the connection from HTTP to HTTPS.

10.1.2 Storage TAB

BooleBox storage

If the connection check performed through the CONNECT button doesn’t work, you must verify:

- **SERVER IP ADDRESS AND CONNECTION PORT –** in order to guarantee the correct functioning of the platform, it is necessary to verify that, in correspondence with the SERVER STORAGE SERVICE URL item in the GENERAL tab, the IP address and the relative port have been indicated correctly to allow the server to be reached at the specified IP address through the indicated port. In particular, the IP address must correspond to that of the server on which the component was installed; the IP address has to be specified in the format http://serveripaddress:80. Furthermore, if the server in question is protected by a specific firewall, it is necessary to open the TCP/IP ports in accordance with the rules of the same firewall to ensure in any case that the server is reached.
- **IIS SERVER STATE: –** in order to guarantee the correct functioning of the platform, it is necessary that the IIS server where the application is published is active. Then verify that

the IIS server is activated, that the publication port is the correct one and that the website is online and running through the IIS management console in Windows Server.

Amazon S3 Key

Should problems arise regarding the configuration or use of Amazon S3 Remote Storage, you must verify:

- **STORAGE PARAMETERS –** the storage manager, when signing the contract, releases parameters to be introduced in order to use Amazon S3 storage as support storage. It is therefore necessary to verify that the parameters entered in the STORAGE tab are correct and in particular coincide with those released by the service provider.
- **STORAGE CONNECTIVITY –** to allow a correct use of the platform, it is necessary that the latter can connect to the chosen storage. It is therefore necessary to verify through the CONNECT key that the connection with the storage takes place correctly. If the server hosting the storage is protected by a firewall, it is necessary to open the TCP/IP ports in accordance with the firewall rules, to allow the server to be reached in any case.

Note: in case of use of HTTPS protocol with TLS certificate supplied by the customer, it is necessary to configure the IIS bindings so that port 443 can be used. For the IIS configuration relating to port 443, please refer to this link.

Note: to proceed with the configuration of BooleBox On-Premises in accordance with the criteria imposed by the Common Criteria EAL2 + certification, it is necessary to configure the Server Storage Service site to listen only via the HTTPS protocol, by deactivating the HTTP port activated by default or by automatically upgrading the connection from HTTP to HTTPS.

10.1.3 Database TAB

If problems related to MySQL Database arise, it is necessary to verify:

- **SERVER IP ADDRESS AND CONNECTION PORT –** the IP address of the server in which it is present the database must be reachable on the network using the TCP/IP protocol

and accompanied by the relevant port. If the server in question is protected by a specific firewall, it is necessary to open the TCP/IP ports in accordance with the firewall rules, to allow the server to be reached in any case. In particular, the IP address to be entered in the DATABASE SERVER ADDRESS field must be in the serveripaddress:3306 format. If the connection port differs from the standard port (3306), it is necessary to indicate the port used in the IP address.

- **DATABASE NAME –** BooleBox On-Premises requires to insert in the DATABASE CATALOG NAME field the name of the database of the platform, which will be used for storing all the configuration data, the logs and the file encryption keys. For a correct functioning of the platform itself, it is therefore necessary to verify that the name of the database entered is correct and corresponds to that of the DB created in the configuration phase, as indicated in the CONTROL PANEL > DATABASE section of this guide.
- **NAME AND PASSWORD OF DATABASE USER –** for the connection to the database to take place correctly, it is necessary to indicate in the DATABASE USER and DATABASE PASSWORD fields the username and password of the user who will have access to the database. It is therefore necessary to check that the previous parameters have been entered correctly.
- **MYSQL SERVICE STATUS –** check on the server where the DB has been installed that the MySQL service is active and running.
- **SERVER RESOURCES –** in order to allow the database to work correctly, the server on which the DB has been installed must have the necessary resources (RAM and disk space). In the event that problems regarding the MySQL DB arise, using the tools made available by the operating system installed on the server itself (Windows Server or Linux), verify that the available resources are sufficient and in particular corresponding to the ones listed in the INSTALLATION > INSTALLATION PREREQUISITES section.

10.1.4 Smtp Server TAB

SMTP SERVER

Should problems regarding the SMTP service arise, it is necessary to verify:

- **SMTP PARAMETERS –** parameters introduced in the SMTP SERVER ADDRESS, PORT, SMTP USER, SMTP PASSWORD fields must be correct and in particular coincide with those released by the service provider.
- **SMTP SERVER STATUS –** the SMTP server, through the TCP/IP communication protocols, must be reachable on the network at the IP address and port indicated. Therefore, check that the parameters entered during configuration in the SMTP SERVER tab are correct and in particular coincide with those released by the service provider. If the server in question is protected by a specific firewall, it is necessary to open the TCP/IP ports in accordance with the firewall rules to allow the server to be reached in any case.
- **SMTP SERVICE STATUS –** verify that the SMTP service is online and running.

10.1.5 Sms Server TAB

Custom – Nexmo – Clickatell

In the event that problems regarding the SMS server arise, it is necessary to verify:

- **SMS SERVER PARAMETERS –** the server connection parameters provided by the service provider and entered in the SMS SERVER tab fields must be correct and in particular correspond to those provided by the operator.
- **CONNECTIVITY –** check the connectivity and reachability of the provider in use. If necessary, contact the support provider of the services used for sending SMS.
- **SUBSCRIPTION –** verify that the subscription to the SMS gateway service provider is active and not expired.

10.1.6 Online editor TAB

Microsoft Office WebApps

If problems regarding the online Office editor arise, check:

- **IP ADDRESSES –** the IP addresses entered in the PUBLIC URL OF MICROSOFT OFFICE WEBAPPS SERVER and INTERNAL URL OF MICROSOFT OFFICE WEBAPPS SERVER fields must be correct and in particular coincide with those provided by the service manager.
- **CONNECTION CERTIFICATE –** in case of connection via HTTPS protocol, verify that the certificate indicated in the SSL CONNECTION field (CERTIFICATE NAME) is the correct and valid one.
- **EDITOR ONLINE SERVER –** the server on which the online editor has been installed must be reachable via the TCP/IP communication protocols. Check that the server where the online editor is installed is reachable and that the service in question is active and running on the server. If the server is protected by a specific firewall, it is necessary to open the TCP/IP ports in accordance with the firewall rules to allow the server to be reached in any case.

ZOHO DOCS

If problems concerning the ZOHO DOCS service arise, it is necessary to check:

- **PARAMETERS –** in order to use ZOHO DOCS as an online editor, you need to enter the api key for the service provided by the same manager. Verify that the API key inserted in the ZOHO DOCS API KEY field is correct and in particular corresponding with that provided by the service provider.
- **CONNECTIVITY –** check connectivity and reachability of the provider in use. If necessary, contact the service provider support.
- **SUBSCRIPTION –** verify that the service provider subscription is active and not expired.

10.1.7 Doc manager TAB

DOC MANAGER

If the connection check through the CONNECT ALL button does not work, it is necessary to check:

- **IP ADDRESS AND DOC MANAGER SERVER PORT –** in order to guarantee the correct

functioning of the platform, the server on which the Document Manager component has been installed must be reachable on the network using the specified IP address and the port 2451. If the server in question is protected by a specific firewall, it is necessary to open the TCP/IP ports in accordance with the firewall rules, to ensure that the server is reached in any case.

- **SERVICE STATUS –** in order to guarantee the correct functioning of the platform, the BOOLEBOX DOCUMENT SERVICE APPLICATION service must be active and running on the server where it was installed.
- **SERVER RESOURCES –** the server hosting the DOCUMENT MANAGER service must have the necessary resources (RAM and disk space) for the proper functioning of the same. It is therefore necessary to check with the service manager that the prerequisites for operating the DOCUMENT MANAGER service are respected for the server used as listed in the INSTALLATION > INSTALLATION PREREQUISITES section of this guide.

10.1.8 Advanced TAB

Windows authentication (NTLM, Kerberos)

If problems concerning authentication through the Windows Authentication system arise, it is necessary to verify:

- **CREDENTIAL FAULTS –** the user credentials entered to log in must be correct and in particular coincide with the credentials of your Windows account.
- **CREDENTIAL VALIDITY –** the credentials used to perform the Windows Authentication must be valid: it is therefore advisable to check that they have not expired and that the user has not been blocked or disabled in the ACTIVE DIRECTORY company domain.
- **WEB SERVER APP –** the servers on which the BooleBox Web App has been installed must be entered in the corporate Active Directory Domain; in addition, the Windows Authentication option must be enabled in the IIS configuration of the BooleBox and RestApi sites (a necessary condition to use Windows Authentication).

Strong authentication

Should problems regarding the Strong Authentication option arise, according to the Strong Authentication system used, it is necessary to check:

- **SITEMINDER SERVER –** the server provided by the service provider must be functional and reachable online. In case of problems, please contact the service manager for further changes.
- **DATAPOWER SHARED KEY –** the SHARED KEY generated by the DATAPOWER system must be corrected to ensure that the session cookies are decrypted.

10.1.9 License info TAB

Change certificate

Within the LICENSE INFO tab it is possible to replace the certificate used by BooleBox On-Premises to encrypt the master key. In order to be able to carry out the symmetrical block cipher operated by BooleBox, it is necessary to use a certificate containing the private key. The certificate must also be valid. If problems regarding the practice of changing the certificate arise, verify that the latter reflects the characteristics listed above.

License update

The license update procedure, thank you to a connection between the BooleBox On-Premises server and the BooleServer internet portal dedicated to the activation of platform licenses, allows you to update all the details relating to the BooleBox On-Premises license in use. Should problems arise regarding the license update procedure, it is necessary to check:

- **SERVER INTERNET CONNECTION –** BooleBox On-Premises server must have an internet connection available in order to guarantee the achievement of the validation site. If you don’t have an internet connection available, please follow the procedure explained in the LICENSE ACTIVATION > OFFLINE LICENSE ACTIVATION section of this guide.
- **LICENSE VALIDITY –** BooleBox On-Premises license referred to in the license update procedure must be valid: it is therefore recommended to check the validity of the license in use and contact BooleBox technical support at support@boolebox.com in case of

problems.

10.2 Standard server components

Standard server components are the applications strictly necessary for the correct functioning of the platform. This section lists the checks to be carried out in the event that problems regarding these components arise.

10.2.1 MySQL

If problems concerning the MySQL database arise, it is necessary to check:

- that the MySQL database service is active on the machine hosting the DB;
- that the database is reachable on the port indicated during installation, which can be checked in the DATABASE tab of BooleBox On-Premises control panel;
- that the user entered in the BooleBox On-Premises application control panel as the user designated to access the DB has the necessary permissions to perform the operations requested by the platform;
- that there is sufficient free disk space on the server where the DB is installed, as indicated in the INSTALLATION PREREQUISITES section of this guide.

10.2.2 BooleBox On-Premises

If the web application of BooleBox On-Premises is not accessible, it is necessary to verify that:

- the URL address entered in the web page is correct and in particular corresponding to that of the Wep Application;
- the ASP.NET service is up & running on the server that hosts the WebApp;
- the Microsoft Windows IIS service is active and running and the site of the application is up & running from the IIS control panel (in case of further problems concerning IIS also check the Microsoft Windows Server log);
- any balancer used for configurations with multiple WebApp access servers is functioning and able to reach the WebApp reference server through the correct TCP/IP ports;

- the license of the purchased instance is valid: otherwise, the “Site in maintenance” page will appear in the browser;
- the certificate entered in Windows in the configuration part of Microsoft IIS is correct and valid: otherwise connection problems to the WebApp through the HTTPS protocol could occur. If you find that the certificate in question has expired, proceed with its replacement and restart the publication in IIS;

10.2.3 BooleBox Server Service

If problems concerning the Server Service component arise, it is necessary to verify:

- that the service is active on the server that hosts the component;
- that the server is reachable via the TCP/IP port used by the service (2450).

10.2.4 BooleBox Document Service

If problems concerning the Document Service component arise, it is necessary to check:

- from the DOC MANAGER tab of BooleBox On-Premises control panel that the parameters entered to use the service are correct. In order to do this, perform a connection test using the CONNECT button. If the connection check fails, verify that the server’s IP address is correct and that the server hosting the Document Service is reachable via the specified TCP/IP port (2451);
- that BooleBox Document Service is up & running on the server where the component is installed;
- that the certificate installed and used to encrypt the Master Key on the server hosting the BooleBox web app has also been installed on the server which hosts the BooleBox Document Service: otherwise it will not be possible to keep the service up & running, making previews unavailable.

10.2.5 BooleBox Storage Service

If problems arise regarding the Storage Service component, it is necessary to check:

- from the STORAGE tab of BooleBox On-Premises control panel that the parameters entered to use the service are correct. To do this, perform a connection test using the CONNECT button. If the connection test fails, check that the IP address of the server and the port entered in control panel fields are correct and that the server hosting the BooleBox Storage Service is reachable through the specified TCP/IP port;
- from the IIS control panel, that the Microsoft Windows IIS service is up and running and that the application site is up & running. In case of problems concerning IIS, also check the Microsoft Windows Server log;
- that the user indicated as IDENTITY in the application pool of BooleBox Storage Service site has the rights for reading and writing in the destination where BooleBox files are saved. In order to do this, verify that in the path indicated in the SETTINGS.CONFIG file of the same component the permissions listed above are allowed;
- that there is free space to be used for saving data on the disk/storage used: for storage settings, check the path in the component’s SETTINGS.CONFIG file.

10.3 Optional server components

Optional server components are the applications that allow you to expand BooleBox functionalities on server side. This section lists the checks to be carried out in the event that problems arise regarding these components.

10.3.1 BooleBox AD Service

If problems arise regarding the BooleBox AD Service component, it is necessary to check:

- from the IIS control panel, that the Microsoft Windows IIS service is up and running and that the site of the application is up & running. If problems regarding the IIS service arise, also check the Microsoft Windows Server log;
- that the IP address and port related to the machine on which the BooleBox AD Service component has been installed are correct and coinciding with those set in the company's customizations. The insertion of these parameters is described in the COMPANY > VIEWING AND CUSTOMIZING COMPANY PROPERTIES > ACTIVE DIRECTORY;
- that the Microsoft Active Directory service can be reached via the network TCP/IP ports used by the server on which the AD Service component has been installed;
- that the configuration parameters inserted in the SETTINGS.CONFIG file (IP address or FQDN of the domain controller and the type of authentication protocol – SAML or AD standards) are correct;

10.3.2 SignalR

If problems concerning the SignalR component arise, it is necessary to check:

- from the GENERAL tab of the BooleBox On-Premises control panel that the IP address and port of the server on which SignalR was installed have been indicated correctly. After doing this, perform a connection test using the CONNECT button. If the connection test fails, verify that the server hosting the SignalR service is reachable on the network using

the specified TCP/IP port;
- from the IIS control panel that the Microsoft Windows IIS service is active and running and that the application site is up & running. If problems regarding the IIS service arise, also check the Microsoft Windows Server log.

Note: if the controls listed in the previous points are not sufficient to solve the problems concerning the SignalR component, it could be useful to check the service status of the same component through the following links: http://serveripaddress:80/check or https://serveripadress:443/check if the SSL/TLS certificate is used. On the displayed page, if the service is working correctly, the "OK" sentence will appear; if the certificate has expired, a warning message indicating that the SSL/TLS certificate is not valid will be displayed. In the case of a blank page, the causes of the fall of the service are to be found in the Windows event viewer.

10.3.3 AD Sync

If problems concerning the AD Sync component arise, it is necessary to check:

- that the parameters required by the application have been entered correctly, as indicated in the ADDITIONAL COMPONENTS CONFIGURATION > AD SYNC section of this guide. In particular, check that the server indicated in the SERVER ADDRESS field is reachable via TCP/IP through the correct ports.

10.3.4 Node.JS

If problems concerning the Node.JS component arise, it is necessary to verify:

- from the GENERAL tab of BooleBox On-Premises control panel that the IP address or FQDN with the relative port of the server on which the component was installed has been inserted correctly. To do this, carry out a connection test using the CONNECT button. If the connection test fails, make also sure that the server hosting the Node.JS service is reachable via the specified TCP/IP port;

- in case of SSL connection, that the certificate is installed correctly and still valid;
- that the Node.Js: Server-side Java Script process is active and present in the Microsoft Windows Server Task Manager where the component is installed. If not, restart the BOOLEBOX SERVER SERVICE service on the machine hosting the component.

Note: if the controls listed in the previous points are not sufficient to solve the problems concerning the Node.JS component, it could be useful to check the service status of the same component through the following links: http://serveripaddress:3000/getpush or https://serveripadress:3500/getpush if the SSL/TLS certificate is used. On the displayed page, if the service is working correctly, a string containing all the parameters of the connected user will appear; if the certificate has expired, a warning message indicating that the SSL/TLS certificate is not valid will be displayed. In the case of a blank page, the causes of the fall of the service are to be found in the Windows event viewer.

10.3.5 File Encryptor Server

If problems concerning File Encryptor Server component arise, it is necessary to verify:

- that the service concerning the File Encryptor Server component is up & running on the server hosting the component.
- that the API KEY inserted when configuring the component is correct and in particular corresponding to the one generated for the company. The generation of the API KEY is described in the COMPANY > VIEWING AND EDITING COMPANY PROPERTIES > API KEY section of this guide.
- that the user with whom the service is running has the necessary permissions to access the repository where the data to be encrypted are stored, configured in the File Encryptor rules.
- that the parameters related to the eventual proxy server are correct.

10.3.6 Office online

For problems concerning the Office Online Server platform, refer to the official installation page of Microsoft site.

10.4 Optional client components

Optional client components are the applications that allow you to expand BooleBox functionalities on client side. This section lists the checks to be carried out in the event that problems regarding these components arise.

10.4.1 File Encryptor Client

If problems concerning the File Encryptor Client component arise, it is necessary to verify that the parameters indicated to configure the possible use of a proxy server have been entered correctly.

10.4.2 Outlook Encryptor

If problems arise regarding the Outlook Encryptor plugin, it is necessary to verify:

- that the BooleBox server address has been entered correctly in the plugin information menu;
- that the username and the password entered correspond to those of your BooleBox account.
- that the Microsoft Office version installed is one of those supported by the plugin, as indicated in the INSTALLATION PREREQUISITES section of this guide.