

POLITECNICO DI MILANO



DIPARTIMENTO DI ELETTRONICA, INFORMAZIONE E BIOINGEGNERIA

Master of Science in Electronics System Engineering

*Highest level of data security and secure sharing of data in a constant controlled manner, with continuous encryption, absolute protection and always accessible of data by using **BOOLE SERVER***

Supervisor: FRANCO ZAPPA

Master's thesis of:

Muhammad Irfan

Matriculation Number: 804984

Academic Year: 2013 - 2014

Acknowledgement

This thesis has been carried out during the year 2014 as a Student of Master of Science in Electronics System Engineering at Politecnico di Milano, Italy.

I offer my sincere gratitude to my Supervisor Professor **Franco Zappa and my Company “Boole Server”** (<http://www.booleserver.com>) staff who have supported me throughout my thesis with their patience and knowledge. I attribute the level of my master’s degree to his encouragement and dedication to advise me.

Then thanks to all the dear friends for their support and morale in the course of this thesis, helping and encouraging me during my stay.

Finally I am grateful to my family and unforgettable my parents emotional strength, support and prayers to me all the time.

Abstract

In my thesis I write about my internship work in an IT data security software solution company” Boole Server “s.r.l Milan, Italy. Boole Server has developed a system capable of protecting the content of confidential documents against all intrusions, coming from both outside and inside the user company.

Presentations, documents, images or spreadsheets: no matter what type of information is to be secured, Boole Server protects company data by making them available in a controlled manner, choosing selectively those who can access them, how, when, and for how long. The Boole Server system is user-friendly and allows to work on files even by connecting from outside the company and through a variety of devices (tablets, laptops, smartphones), in total security.

In this company I was work as software testing and provide technical support to customers and following are my major key working points

- Testing of Boole Box (Cloud base product) software on Windows operating system as well as on IOS and android devices and report to the programmers on daily basis of founded bugs.
- Provide technical support of Boole Server product to the entire intentional customer's around the world.
- Installation and maintain Boole server product's on physical and virtual machines (VMware Server)
- Working on different Microsoft servers, SQL server, active directory, IIS (internet information services), Network load balancer\fail over configurations, SMTP server etc.

List of Figures

Figure 1: Boole Server	8
Figure 2: Data Security	8
Figure 3: Multi-Level Architecture	9
Figure 4: Boole Server Absolute Protection	10
Figure 5: Boole Server Continuous Encryption	10
Figure 6: Boole Server Always Accessible Data	11
Figure 7: Boole Server Constant Control	11
Figure 8: Boole Server Secure Sharing	12
Figure 9: Server Side	13
Figure 10: Welcome Message	16
Figure 11: Install/Restore	17
Figure 12: License	18
Figure 13: Registration Data	19
Figure 14: General Administration	20
Figure 15: SMTP Server Address	21
Figure 16: SMTP Properties	22
Figure 17: Archive Unit	23
Figure 18: Boole Server Group	24
Figure 19: Log File	25
Figure 20: Installation Process	26
Figure 21: General Administrator	27
Figure 22: Boole Server Configuration	29
Figure 23: Configuration Topology	30
Figure 24: Configuration Topology	31
Figure 25: Configuration Topology	33
Figure 26: Web Client	39
Figure 27: Sharing	40
Figure 28: Sharing Case - 1	41
Figure 29: Sharing Limited	42
Figure 30: Sharing With Boole Server Profile	42
Figure 31: Sharing Customized	43
Figure 32: Sharing Case - 2	43
Figure 33: Sharing Case - 3	44
Figure 34: Sharing Limitations	45
Figure 35: Sharing Warning Message	45
Figure 36: Customized Watermark	47
Figure 37: Sharing With Boole Server Profiles	48
Figure 38: Sharing With Boole Server Profiles e-mail	49
Figure 39: Sharing With Boole Server Profiles e-mail to all	49
Figure 40: Sharing Summery	50
Figure 41: Sharing Successful Warring Box	51
Figure 42: Sharing Message	52
Figure 43: Get Link	53
Figure 44: Get Link Dialog Box	53
Figure 45: External User File Viewer	54

Figure 46: Encrypt Text	55
Figure 47: Encrypt Message	56
Figure 48: Group Share	56
Figure 49: Sharing Limitations	57
Figure 50: Encrypted Text	58
Figure 51: Boole Server Agent	59
Figure 52: Opening File in Offline Mode	60
Figure 53: Boole Server Agent - Offline Mode	60
Figure 54: Encrypted World File	61
Figure 55: Encryption Invoice.....	61
Figure 56: Encrypted World & Excel File.....	61
Figure 57: Encryption Certificate	62
Figure 58: Offline Certificate Password	62
Figure 59: Encrypted World & Excel File.....	62
Figure 60: Encryption Certificate	63
Figure 61: Offline Certificate Password	63
Figure 62: Mail Encryptor.....	64
Figure 63: Boole Server App.....	64
Figure 64: Sharing Folder	68
Figure 65: Mail Encryptor Warning Box.....	69
Figure 66: Mail Encryptor Custom Setting	69
Figure 67: Protection Template Properties	70
Figure 68: Custom Protect & Sharing Options	71
Figure 69: Mail Encryptor Setting Options.....	72
Figure 70: Protection Template Properties	73
Figure 71: Boole Box	77
Figure 72: Boole Box Panel	78
Figure 73: Boole Box New Share	78
Figure 74: Boole Box Custom Templates	79
Figure 75: Boole Box Activity Log.....	79
Figure 76: Boole Box Your Account.....	80
Figure 77: Boole Box Login.....	81
Figure 78: Boole Box Comparison with Others	82

Table of Contents

Acknowledgement	2
Abstract.....	3
List of Figures	4
CHAPTER 1: INTRODUCTION	8
1.1 Boole Server:.....	8
1.2 Key Benefits of Boole Server:.....	10
1.2.1 Absolute Protection:	10
1.2.2 Continuous Encryption:.....	10
1.2.3 Always Accessible Data:	11
1.2.4 Constant Control:	11
1.2.5 Secure Sharing:	12
CHAPTER 2: BOOLE SERVER	13
2.1 Server Side:	13
2.2 Installation & Configuration of Boole Server:.....	14
2.2.1 BOOLE SERVER SETUP:.....	14
2.2.2 Boole Server 3.2 application:	14
2.2.3 Web Client Internet site:.....	14
2.2.4 SQL Server Express 2012:.....	15
2.2.5 Boole Server Wizard (New installation):.....	15
2.3 General Administrator:	27
2.3.1 Show Log:	27
2.3.2 Protect Red Key:.....	28
2.3.3 Edit Red Key:	28
2.4 BOOLE SERVER INTERFACE:	28
2.4.1 Control Panel:.....	28
2.4.2 System Monitor:	28
2.4.3 System Bar:	28
2.4.4 Status Bar:	29
2.5 Different Types of Configurations:.....	30
2.5.1 Boole Server Simplest Infrastructure:.....	30
2.5.2 Boole Server Advanced Infrastructure in High Availability (HA):.....	30
2.5.2.1 Boole Server Advanced Infrastructure in HA Type - 1:	31
2.5.2.2 Boole Server Advanced Infrastructure in HA Type - 2:	33
2.5.3 Balancer Configuration:	36
CHAPTER 3: BOOLE SERVER CLIENT SIDE	39

3.1 Web client:	39
3.2 Most Important features of Boole Web client:.....	39
3.2.1 Sharing In Boole Server:.....	39
3.2.2 Custom Sharing Options:	46
3.2.3 External Users (SHARING FILES AND/OR FOLDERS WITH EXTERNAL USERS):	52
3.3 Other Boole Web Client Functionalities:	52
3.3.1 Get Link:	52
3.3.2 Remote Drive:	54
3.3.3 Encrypt Text:	55
CHAPTER 4: BOOLE SERVER AGENT	59
4.1 Introduction:	59
4.2 Offline Use of Local Protected File:.....	59
4.2.1 CASE 1:	61
4.2.2 CASE 2:	61
4.2.3 CASE 3:	62
4.3 Top Secret Protection:	63
4.4 Mail Encryptor:.....	64
4.5 Boole Server App:	64
CHAPTER 5: CUSTOMER QUERIES.....	66
CHAPTER 6: BOOLE BOX.....	77
6.1 Private Keys:.....	77
6.2 Secure Mail:	77
6.3 Secure Sync:	77
6.4 Synchronize:.....	77
6.5 Most Important Features of Boole Box:	78
6.5.1 File Manager:	78
6.5.2 Default Sharing Security Limitation:	78
6.5.3 Custom Sharing Security Limitation:	79
6.5.4 Activity Logs:	79
6.5.5 Account Management Setting:	80
6.5.6 Access from Non-Trusted Devices:	80
6.6 Comparison between Different Cloud Based Services:	81
6.7 Boole Box Software Testing Bugs:.....	82
Reference	85
ABBREVATIONS	86

CHAPTER 1: INTRODUCTION

- 1) Boole Server (Data-centric protection software)
- 2) Boole Box (Cloud based secure data protection & shearing)

1.1 Boole Server:

Comprehensive and unique software the Boole Server data loss prevention software protects the confidentiality of information. It is a comprehensive system which prevents improper use of confidential files by unauthorized cooperators, suppliers, and users.



Figure 1: Boole Server

Nowadays, it is easier than ever to lose control of confidential documents which, without protection, can be printed, copied or forwarded to competitors or press agencies. Do not forget that employees can keep and use the documents they own, even when they no longer work with their former employers. Thanks to Boole Server all documents and data will be always protected and under control through the highest-level data loss prevention system.



Figure 2: Data Security

The system developed by Boole Server offers:

- Protection of confidential company files
- Immediate and controlled data sharing with work groups, cooperators or customers, even via e-mail
- Absolute integrality with the most widely used applications (e.g. Office, SharePoint)
- Constant monitoring of all accesses and uses on encrypted files
- Flexibility to suit the needs of both professional firms and multinationals with complex structure. Boole Server can be applied to countless fields of use, and meets the needs of multinationals, as well as SMBs, professional firms, and the Public Administration. This is confirmed by the direct experience of organizations and companies which have already implemented and used our data protection software with satisfaction.
- Compatibility with all devices (tablets, smartphones, laptops), so that every user can manage the secure sharing of company files even when connecting from outside the company.

The Boole Server data-centric protection software is based on a multi-level



Figure 3: Multi-Level Architecture

architecture for streamlined security management by those in charge of the company data.

At an operational level, much functionality is offered to users who need to work on protected files:

- Data Encryption, to protect confidential information
- Private Cloud, to create secured company cloud computing
- File Sharing, to share company data in a secure way
- Watermark, to avoid the unauthorized disclosure of confidential data
- Secure Messenger, to exchange encrypted messages of any kind (texts, e-mails, Skype, Gmail, Msn messenger) and avoid the leak of confidential information

1.2 Key Benefits of Boole Server:

One can take advantage with 5 Key benefits by using Boole server

1.2.1 Absolute Protection:

Boole Server is the strongest data protection software available for your company's data. Boole Server goes beyond the traditional perimeter security systems which are often



Figure 4: Boole Server Absolute Protection

complex and not entirely efficient.

Boole Server secures confidential information in an innovative way: files are protected everywhere and at any time, both inside and outside the company. Boole Server architecture offers an additional guarantee of confidentiality: system administrators are not authorized to access the content of Boole Server protected files; only data managers can access them and set access and sharing rights.

1.2.2 Continuous Encryption:

Boole Server protects files, e-mails and texts through 2048 bit encryption based on a



Figure 5: Boole Server Continuous Encryption

military symmetric algorithm.

Boole Server file encryption system is continuous even while using the encrypted file: unlike all the other encryption systems, whose protection disappears the very moment the file is open and viewable on the PC screen, Boole Server offers persistent protection even while editing previously encrypted files. To avoid jeopardizing the confidentiality of the information contained in the encrypted resources, Boole Server stores the encryption and decryption keys centrally, rather than on the device used for accessing the file: one can be sure that the file cannot be decrypted without being authorized by Boole Server.

1.2.3 Always Accessible Data:

Boole Server users can access protected information everywhere and at any time,



Figure 6: Boole Server Always Accessible Data

without jeopardizing its security level.

With a robust Web interface, Boole Server is compatible with all types of devices (tablets, smartphones, laptops), and allows users to access their file everywhere. Storing files in total security is no longer a problem: you can manage data accessibility and maintain complete protection.

Boole Server ensure immediate accessibility to information by creating a secure private Cloud: it applies the same technology on which the management of protected files is based, and uses the SSL communication protocol - the same used by banks.

1.2.4 Constant Control:

Boole Server makes it possible to centrally manage and monitor all company files.



Figure 7: Boole Server Constant Control

Data managers can check at any time which activities have been performed on files or data, or which operations have been performed by a given user. A state-of-the-art auditing system and the graphic representation of the gathered data allow for true control on everything that happens with the data protected by, by Boole Server.

1.2.5 Secure Sharing:

Boole Server's protection provides a revolutionary approach to company file sharing: it is not only possible to decide which resources are to be shared, with whom and for how long, but also to assign to a single file differentiated access rights according to the selected profile: one single document can be only viewed by one user, and edited and updated by another user.



Figure 8: Boole Server Secure Sharing

Granularity, selectivity, and editing control: sharing properties assigned to a user on a given file can be edited or even revoked at any time. Security is always maintained on confidential information, even when encrypted files are shared outside the company.

CHAPTER 2: BOOLE SERVER

Boole Server can be divided into two parts for easy understanding

- 1) Server side (The core of the whole data protection system)
- 2) Client Side (The tool to use Boole Server functionalities)

2.1 Server Side:

The core of the whole data protection system the Boole Server system protects the confidentiality of company data against any interception attempt, by blocking all channels



Figure 9: Server Side

through which confidential information may be improperly viewed, disclosed or corrupted.

The Server where Boole Server is installed on is the core of the whole system for company file protection.

Just like the mind which governs and controls a sophisticated system, within the Boole Server architecture the server is responsible for all operations ensuring the protection and encryption of data, information related to profiles and relevant authorizations to access and use every single file.

Processing such data allows Boole Server-based solutions to focus on:

- control of data confidentiality
- protection of the intellectual property
- granular access to information according to hierarchical functional and customizable rights
- traceability of the operations users perform on files
- protection against thefts of company data

Different Configurations and their installation Methods:

When I am talking about installation of Boole server the procedure of installation is the same on different kind of configuration and topologies

Here is the unique installation procedure of Boole server which I used for installation on different kind of configurations

2.2 Installation & Configuration of Boole Server:

PREREQUISITES FOR BOOLE SERVER INSTALLATION

Boole Server can be installed only on machines with O.S. Microsoft Windows Server 2008R2 or 2012.

Prerequisites for server installation:

- SQL Server 2008R2 o 2012 (in test environments even Express versions)
- NET Framework 4.0
- IIS (Internet Information Server) 7.4

2.2.1 BOOLE SERVER SETUP:

To start Boole Server installation, it is necessary to launch the Setup.exe file represented by the Boole Server icon.

- As a first operation, the Setup will check the minimum operating requirements (see above list); if they are not present, they will be automatically installed.
- Automatic installation is not active for IIS prerequisite.
- After prerequisites installation, it will be possible to choose whether to perform either complete or customized installation.

It is possible to choose whether to install the following components or not:

1. Boole Server 3.2 application
2. Web Client Internet site
3. SQL Server Express 2012

2.2.2 Boole Server 3.2 application:

Boole Server application is the core of the solution. Users' access and rights to access protected data are managed centrally by this application. Moreover, the application control panel allows setting all system configurations related to the infrastructure where Boole Server is located.

2.2.3 Web Client Internet site:

Boole Server Internet site is the main entrance to the platform as well as the access front-end to use all information contained and managed by the application. The Internet site is automatically installed on

IIS during setup, and can be used on the same machine where Boole Server is installed, or on separate network segments (DMZ).

2.2.4 SQL Server Express 2012:

All references to users and files managed with Boole Server are contained in the encrypted Data Base based on SQL Server. Even 2048-bit keys randomly generated during information protection are generated and saved within the same Database. The Database can be automatically installed during setup on the same machine where Boole Server is installed; it is also possible to set another Database on a server located in a different network segment.

Note: Given its limitations, it is advisable to use SQL Server Express version only for Test or Proof of Concept installations, and NOT for production environments. Since the database is a critical element for the correct functioning of the system, it is highly advisable to arrange a highly reliable environment and frequently scheduled differential Backups. Besides minimizing information loss, this type of backup significantly reduces operation times since the amount of data to be sent is progressively lower.

2.2.5 Boole Server Wizard (New installation):

When Boole Server is first started, the Wizard process is automatically accessed. It allows configuring the solution and making it function:

Proposed Wizard steps are as follows:

Welcome:

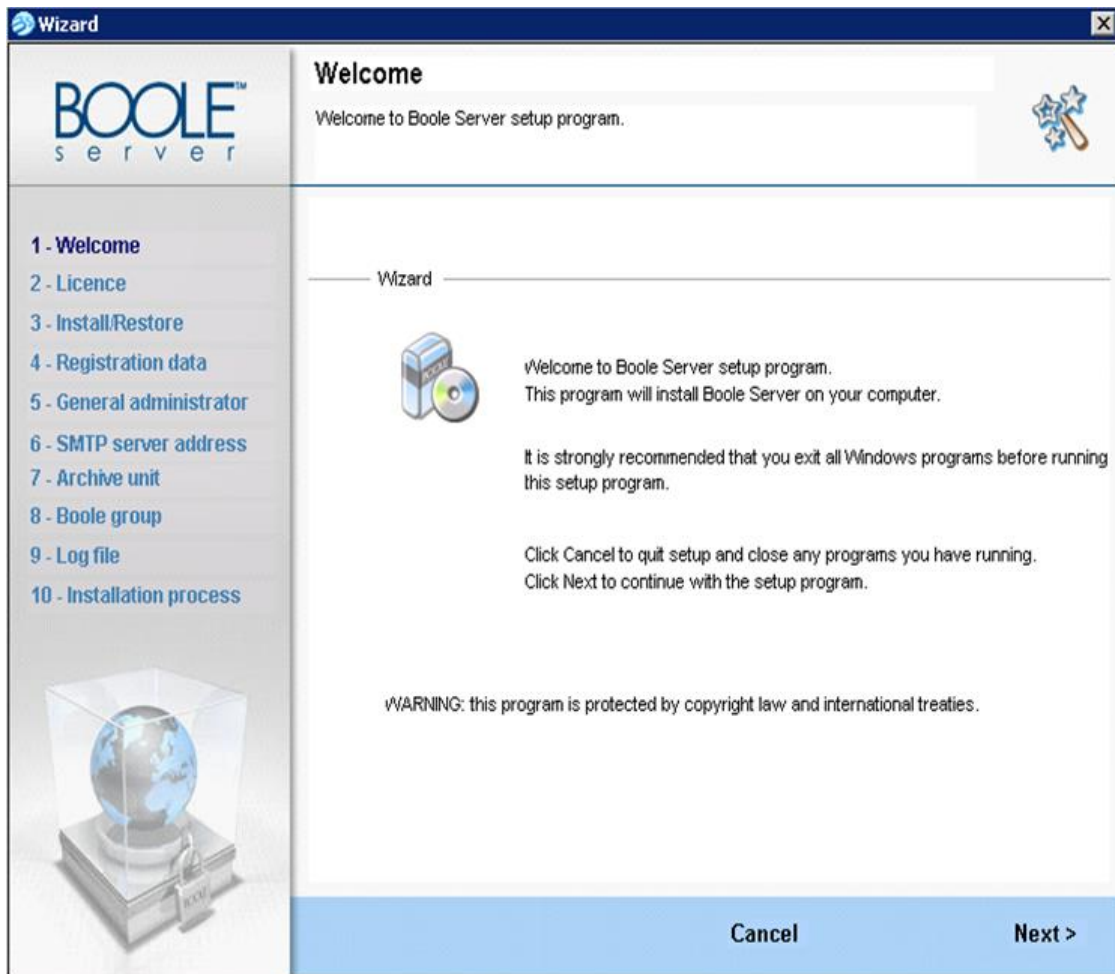


Figure 10: Welcome Message

Install/Restore:

This step allows to define the Boole Server installation:

- Install Boole Server (first Boole Server installation)
- Install Secondary node... (installation of a secondary for highly reliable infrastructures)
- Restore a previous installation... (in case of data recovery)

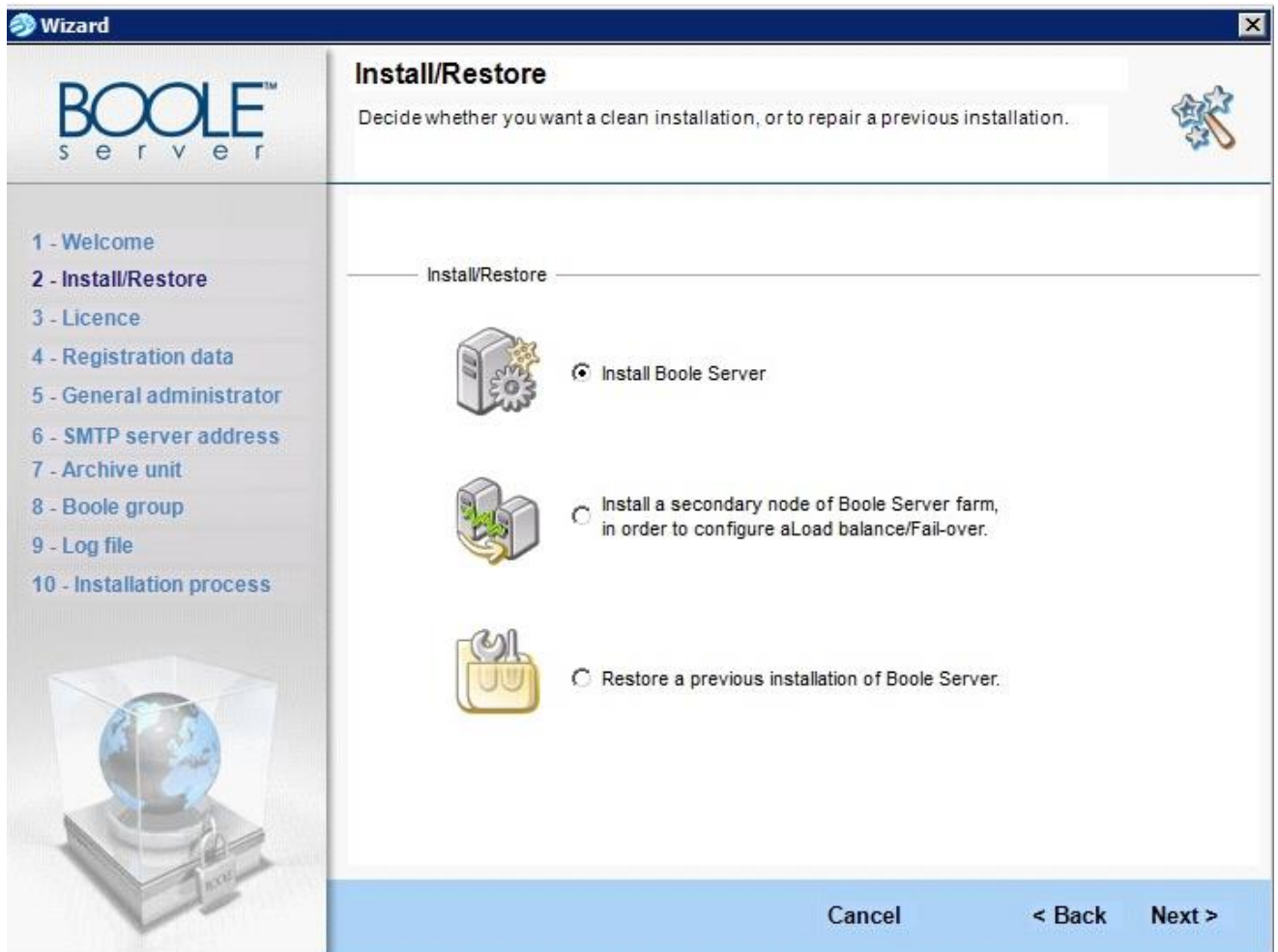


Figure 11: Install/Restore

NOTE: In the event of a system crash you can restore to a previous set-up. In this way you can restore not only your data but also system structure settings and configuration.

License:

- a. In this section, the purchased license number has to be entered. It is necessary to set the key to symmetrically encrypt the Database content (it is possible to edit the key at any moment).
- b. Using the key (also called Red Key) is moreover essential to recover Boole Server installation in case of system fault.
- c. In case of loss of the red key, it will no longer possible to recover the data protected by Boole Server.
- d. It is optionally possible to protect the set Red Key by selecting a digital certificate through which to protect it. In case of system recovery, such certificate will be required to recover the Red Key; in absence of such certificate, it is alternatively possible to directly use the Red Key.

- e. Since the red key also allows decrypting data, it is common practice that the red key is written and kept by Notaries, Lawyers, CEOs, Chairmen or any other impartial officer in the company which the license belongs to.
- f. License activation process is performed only after having entered the red key. The application automatically generates a code which allows Boole Server service center to check the authenticity of the license entered.
- g. License activation can be performed:
 - Either online, automatically through the relevant “Activate” button; or
 - In OFFLINE mode, by copying the code in the clipboard and pasting it in the relevant text field available at the <https://license.booleserver.com> Website; the code generated by the Internet site has to be copied and pasted in the “Activation code” text field.
- h. If the purchased license is to be activated for the second time, it will be necessary to contact Boole Server service center.

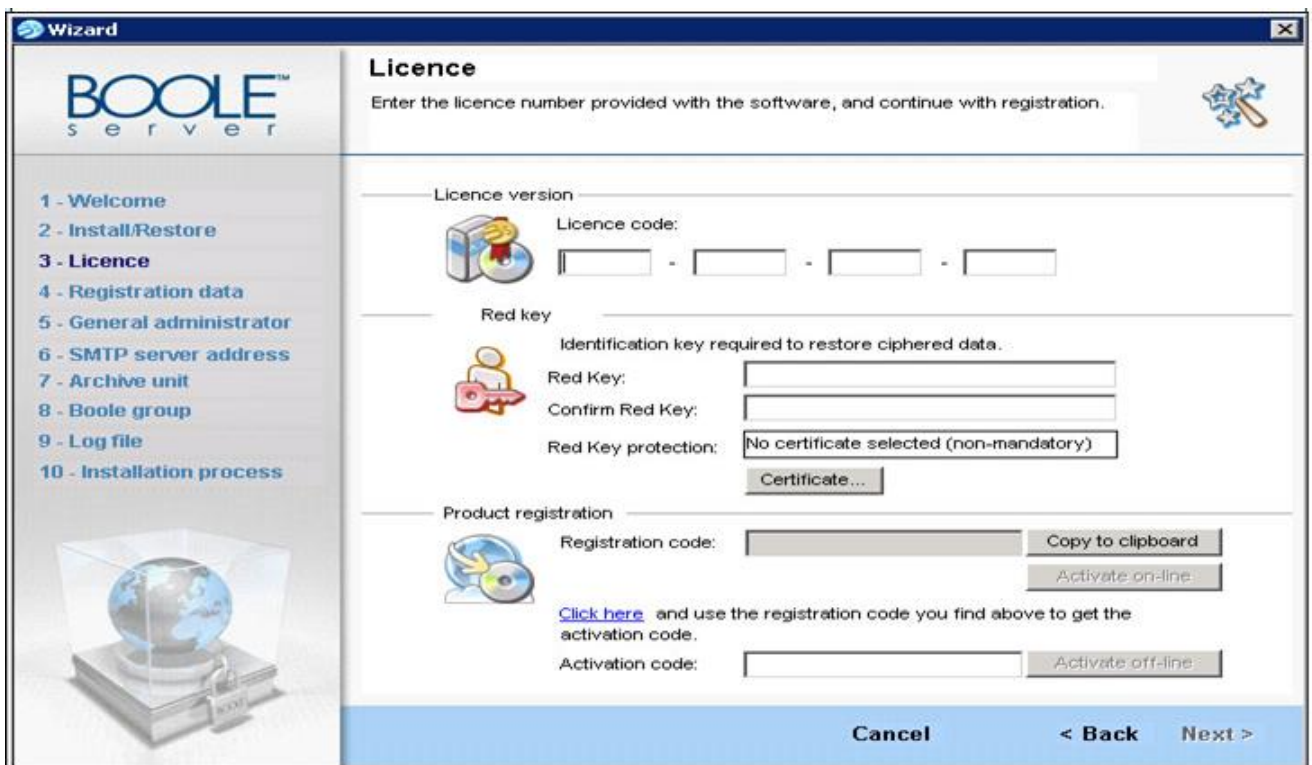


Figure 12: License

Registration Data:

Company’s data entered in this window will be used as default values for signatures in notification e-mails sent by the server and in files signed by Boole Server during encryption process.



Figure 13: Registration Data

General Administrator:

- a. Boole Server allows to set several system administrators; it is compulsory to set the main administrator in this step.
- b. Since it has full access rights to Boole Server functionalities, this administrator is also called "Super Administrator".
- c. This Administrator's access credentials (together with the red key) are also useful to recover data in case of disaster or restore of a previous Boole Server installation.
- d. If this Administrator's credentials are lost, it will be no longer possible to correctly recover data through the relevant Restore function

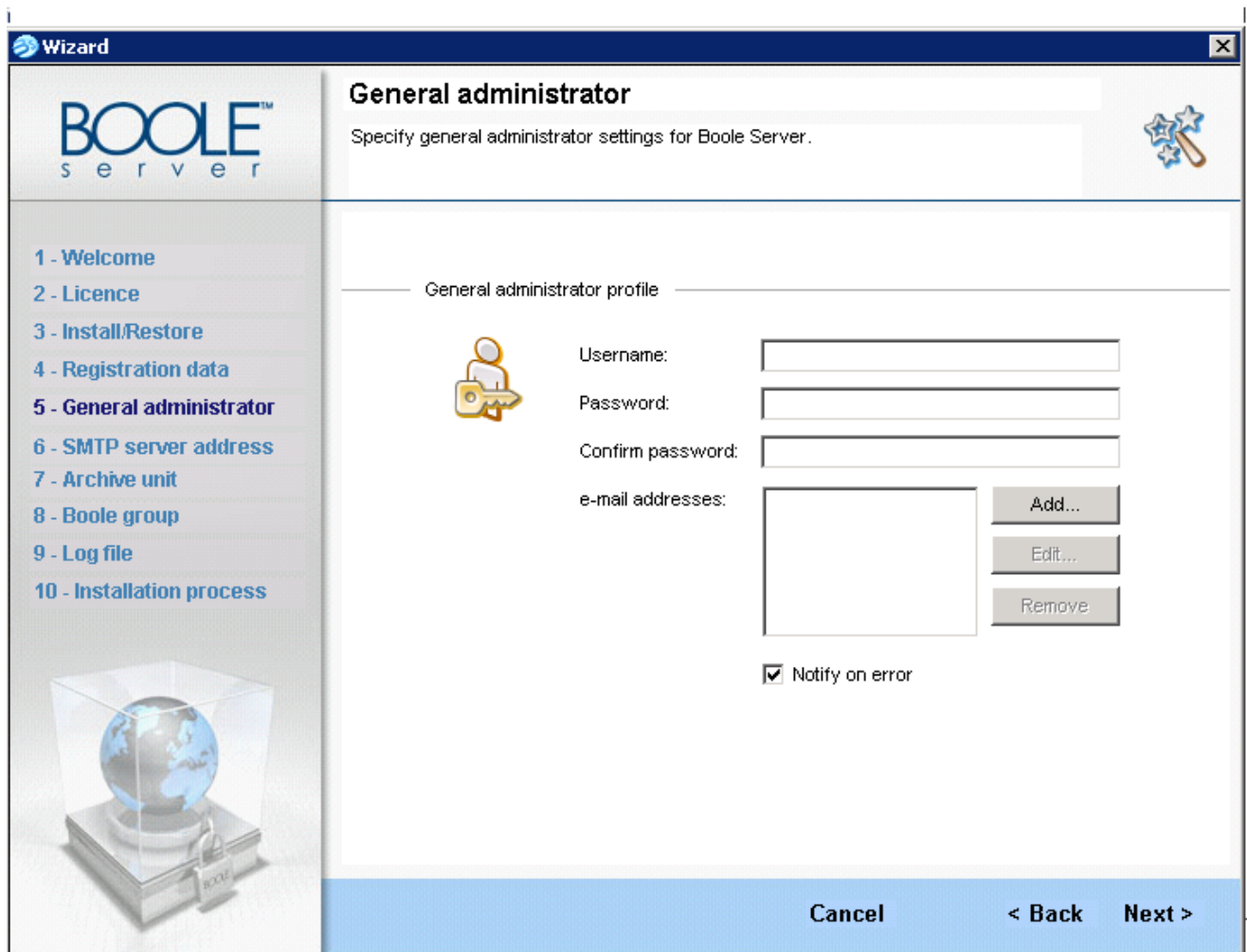


Figure 14: General Administration

NOTE: the data entered for the General Administrator created during installation cannot be edited. After installation it is possible to create other General Administrator profiles, enabled to monitor how the server application works according to specific privileges.

NOTE: If no valid e-mail address is specified, the created profile will not receive any e-mail notifications about the system status, the license expiring date and other important information on how Boole Server works.

SMTP server address:

- a. To be notified by Boole Server via e-mail in case of application malfunctions, it is needed to set the data related to one or more SMTP servers. Currently this setting is not compulsory, but it is highly inadvisable to neglect its configuration.
- b. SMTP Server is also used to send notifications about operations performed client-side (e.g. sharing notifications, invitations to new users, etc.).
- c. During SMTP server configuration, it will be also necessary to set the e-mail address from which notifications will be sent. It is important to notice that this e-mail

address will be used ONLY to send system notifications (e.g. Boole Server malfunctions or Notifications related to purchase licenses).

- d. As for notifications about client-side operations (as described above), SMTP server will send them by using, as the origin e-mail address, the e-mail address related to the user who is performing the operation. This is the reason why it is ALWAYS advisable to set an e-mail address for each created user.



Figure 15: SMTP Server Address

- Click on Add
- A dialog box appears, in which you need to enter a valid e-mail address which will be used as sender for any system notification sent via e-mail by Boole Server.
- Insert the server address and the relative communication port used.

NOTE: The specified e-mail address will be used for the system notification only.

- Enable The server requires a secure connection (SSL) option if the SMTP server requires a protected connection.
- If the SMTP server requires credential, enable the Authentication required checkbox: the fields below will automatically be activated.
- Enter in the corresponding fields Username, Password, associated with the SMTP server you are setting.
- Confirm with OK.



Figure 16: SMTP Properties

NOTE: If the SMTP server indicated is not available, a warning message will ask whether you wish to save the settings anyway.

- The SMTP address added will appear in the list in the main window; if you wish to add another address repeat the steps described above.

NOTE: At the end of the installation, all properties associated with the Boole Server SMTP address configuration may be edited by authorized profiles by using the server application.

- If you do not want to add an SMTP server, just move on to the next step. A warning message will inform you that without a valid SMTP server, Boole Server will not be able to send any e-mail.
- To proceed click next

Archive unit:

- a. Boole Server allows to protect data in two clearly defined modes:
 - Encryption of files contained in any storage unit, which maintain the same save path and can be exchanged through all channels known so far (e.g. e-mails, network share, Skype, etc.)
 - File centralization through Boole Server configured storages, where to upload and share files through the relevant Web Client, the application whose features can be compared to online storage services, such as DropBox, Microsoft SkyDrive, or other types of Cloud Storage. A fundamental difference between usual Cloud services and Boole Server lays in the fact that, thanks to Boole Server, data are stored in storage units located within the company, and not at external ISPs: this is the reason why, during configuration, Boole Server requires to set a storage unit.
- b. All files archived in Boole Server storage are encrypted with symmetric 2048-bit keys. Besides encrypting their content, the system encrypts their structure, as well: this implies that system administrators are not able to know what kind of information is exchanged by Boole Server users.
- c. More than one storage unit can be set in Boole Server

ATTENTION!

For paths with remote locations, it is very important to make sure you do not specify target paths that are included or include other entered paths; otherwise the system will not be able to accurately calculate the total free space for each archive unit.

ATTENTION!

To allow the configuration of a Boole Server farm, the Archive unit must be set in shared network storage.

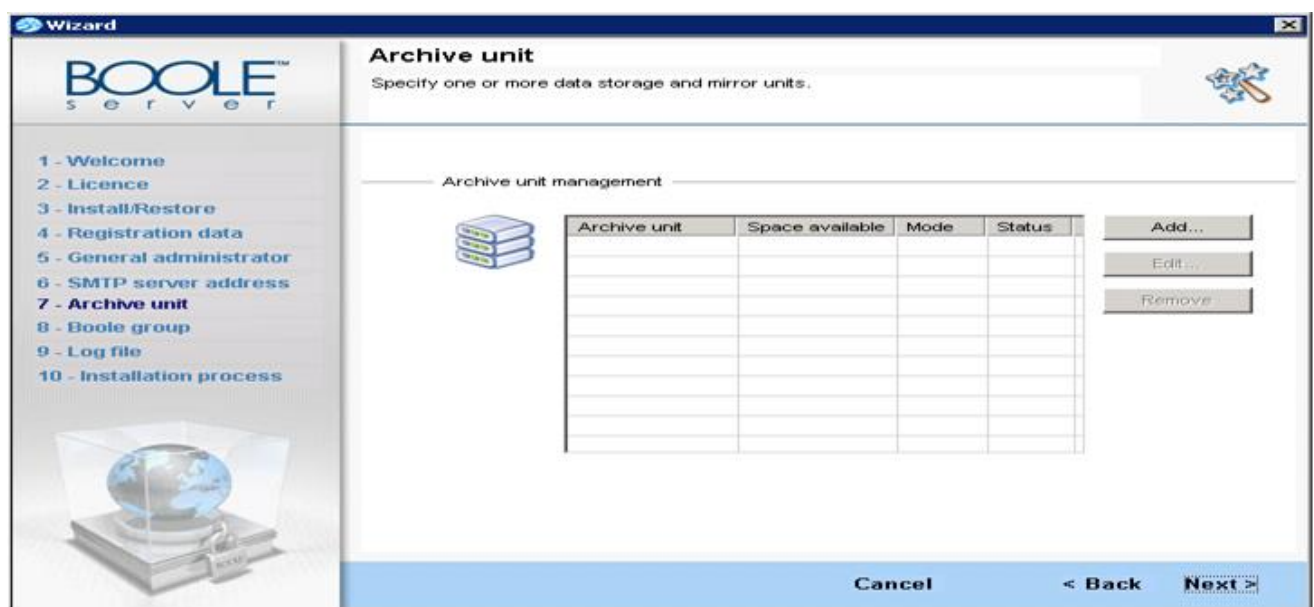


Figure 17: Archive Unit

NOTE: At the end of the installation, all properties associated with the storage unit configuration may be edited by authorized profiles by using the server application.

Boole Server Group:

a. This step allows to configure the database and the first Boole Server group.

b. Database:

- If the database was not present on the machine and you decided to use the SQL Server Express installed during Setup process, the status of Database functioning would be already positive (“SUCCESS”). During SQL Server installation, the Setup has already set some configuration data, such as:
 1. Database Name: Boole Server (automatically created)
 2. Database Address: .\BooleServer (name of local instance of the DB assigned during installation)
 3. Username: sa (default administrator user)
 4. Password: BooleServerdb32 (default password)
- If another existing database is used, the status will be surely “FAILED”. It will be therefore necessary to enter, in the relevant “Set Database” section, the settings of the remote server to be reached.

ATTENTION: Boole Server will overwrite the database if another with the same name already exists.

c. First Boole Server Group:

- To allow the functioning of Boole Server, it is necessary to create at least one group. In this step, only group administrator is usually set, while users are created after installation has been successful performed.



Figure 18: Boole Server Group

Log File:

Log files are necessary to track all operations performed on the server. If you do not wish to track this information, you need to uncheck the options presented in this step.

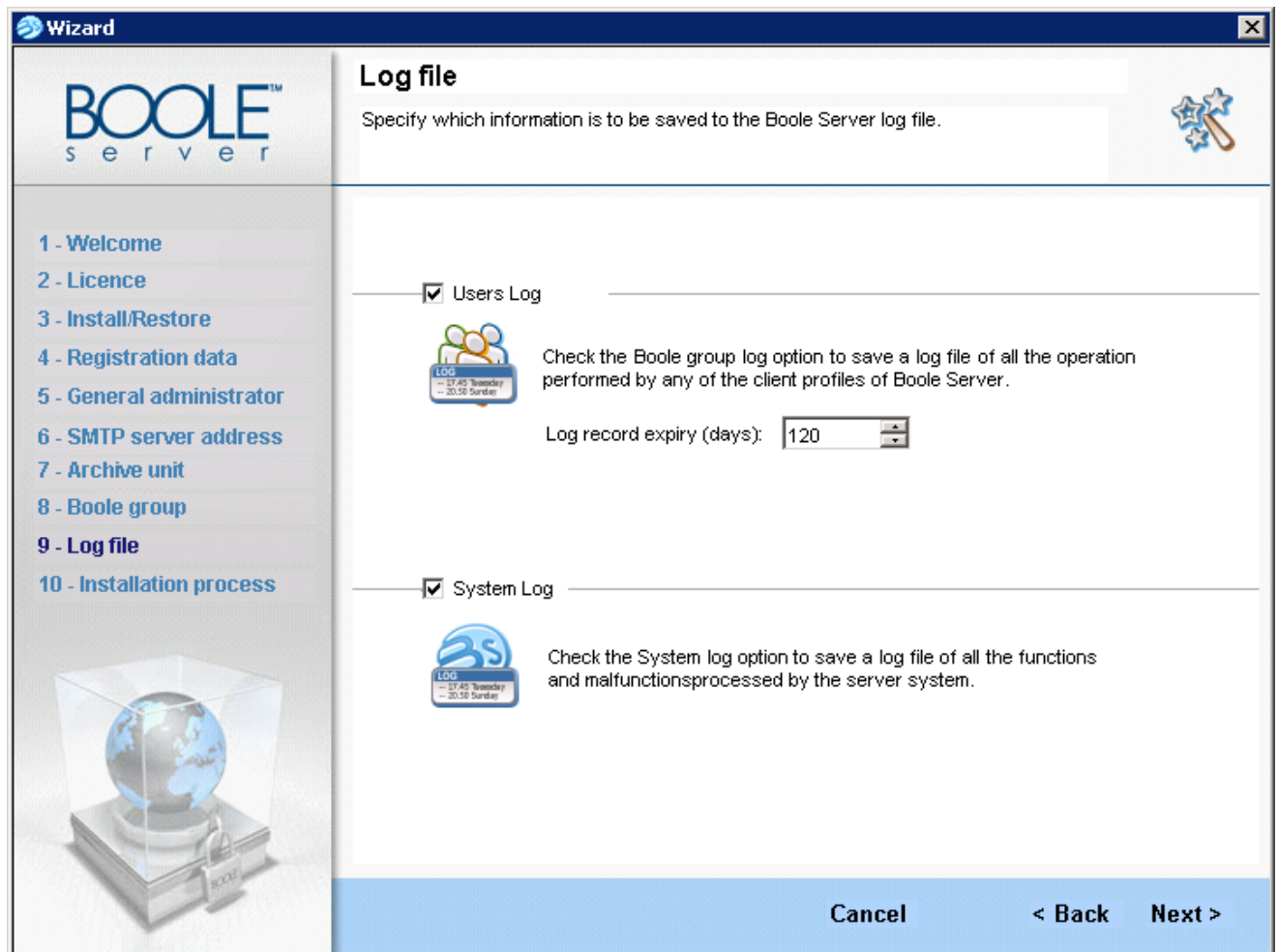


Figure 19: Log File

NOTE: After the installation has finished, all the properties associated with the configuration of Boole Server log files can be edited by authorized profiles using the application server.

ATTENTION!

Activation of the Boole group log option is required if you wish to use Auditing.

Installation Process:

- a. In the last step of the Wizard, Boole Server checks again all set configurations. Green ticks prove that installation has been successful.
- b. After Setup has finished, a link to Boole Server 3.2 will be created on the Desktop, on the taskbar, and in Windows Control Panel.

- c. To make sure that the WebClient has been correctly installed in IIS, after closing the Wizard interface, it is
- d. necessary to start Internet Explorer and type the following address: http://localhost
- e. If the Boole Server Web Client Log-In window appears, the Website installation has been successfully
- f. performed.
- g. If an error message appears, check in IIS Management Console that Boole Server Website is correctly
- h. started and does not conflict with other Internet sites previously installed.

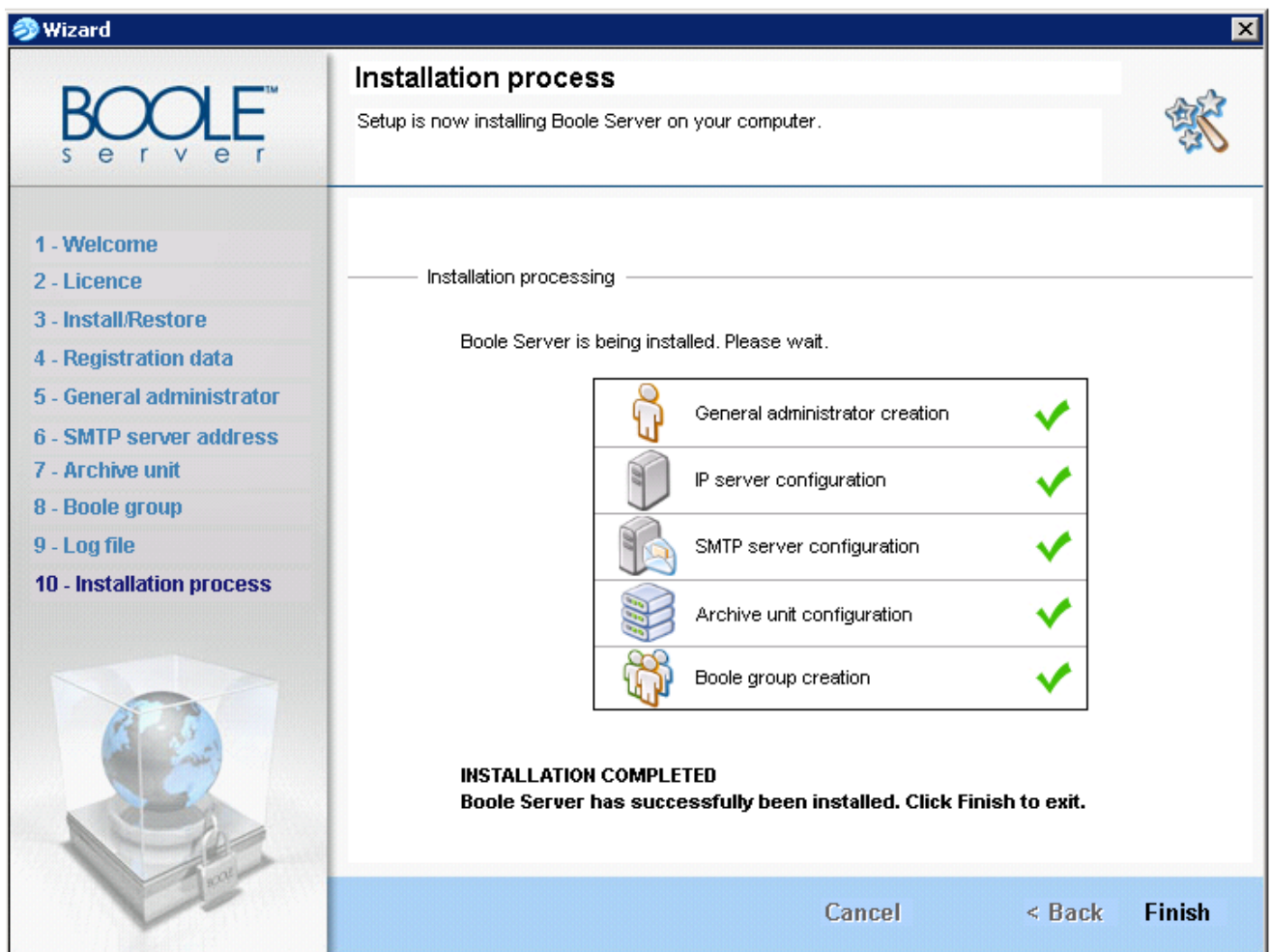


Figure 20: Installation Process

When installation is complete click Finish to close the installation Wizard. The login window to access Boole Server automatically appears; enter the username and password you configured during the installation and press OK to confirm.

2.3 General Administrator:

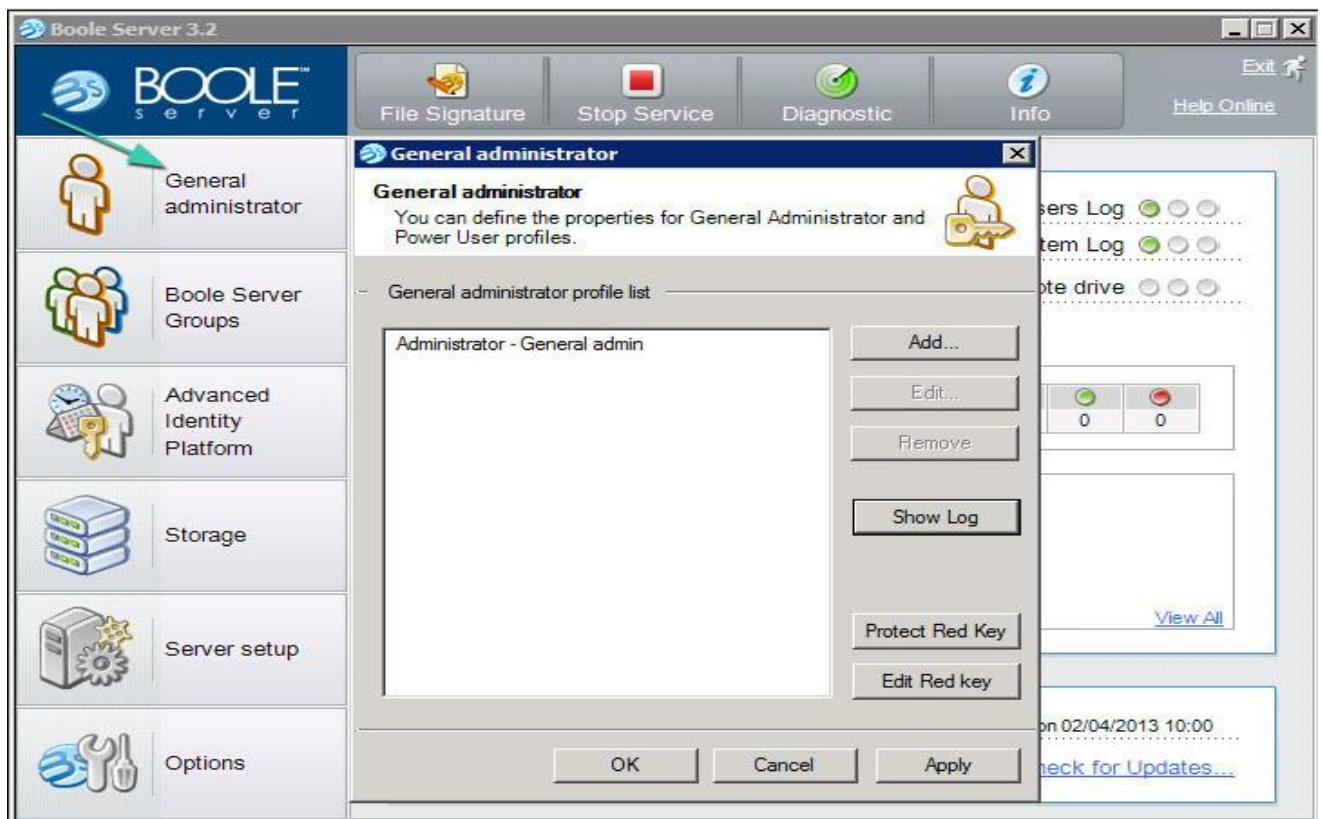


Figure 21: General Administrator

One of the main Boole Server features is the possibility to prevent system administrators to access data stored by users. For this reason, it is possible to create Administrators with limited access to the Boole

Server interface and critical functionalities (e.g.: password change, user's removal). It is moreover possible

To set the maximum number of operations which Administrators are authorized to perform within the areas where they are authorized to operate?

In the General Administrator section, it is also possible to access the following functionalities:

2.3.1 Show Log:

Thanks to this feature, the company can control the operations performed by Boole Server administrators. For security reasons, Administrators are not authorized to access this functionality.

Therefore, to view the operations performed by Boole Server administrators, it is necessary to enter the red key (see Chapter 2.2, paragraph 2.b): it is usually used to check

the conformity of the operations performed within the system or in case of judicial inspections.

2.3.2 Protect Red Key:

If no digital certificate through which to protect the Red Key has been specified during installation, this section allows to select a certificate.

2.3.3 Edit Red Key:

This section allows editing the red key, if it is needed for security reasons. This operation, which can be performed only when services are turned off, may take a few minutes given the amount of data managed by Boole Server.

2.4 BOOLE SERVER INTERFACE:

Once installation has finished, by using username and password configured during installation, it will be Possible to access the interface for managing server functionalities. Boole Server interface is divided into four areas:

2.4.1 Control Panel:

The control panel allows configuring various aspects of the Server (administrators, users and groups,

2.4.2 System Monitor:

This area allows viewing, through colored leds, the status of active services on server (connection to Server, storage status, SMTP server status, etc.)

2.4.3 System Bar:

This bar allows to operate on Boole Server (it is possible to stop and restart the

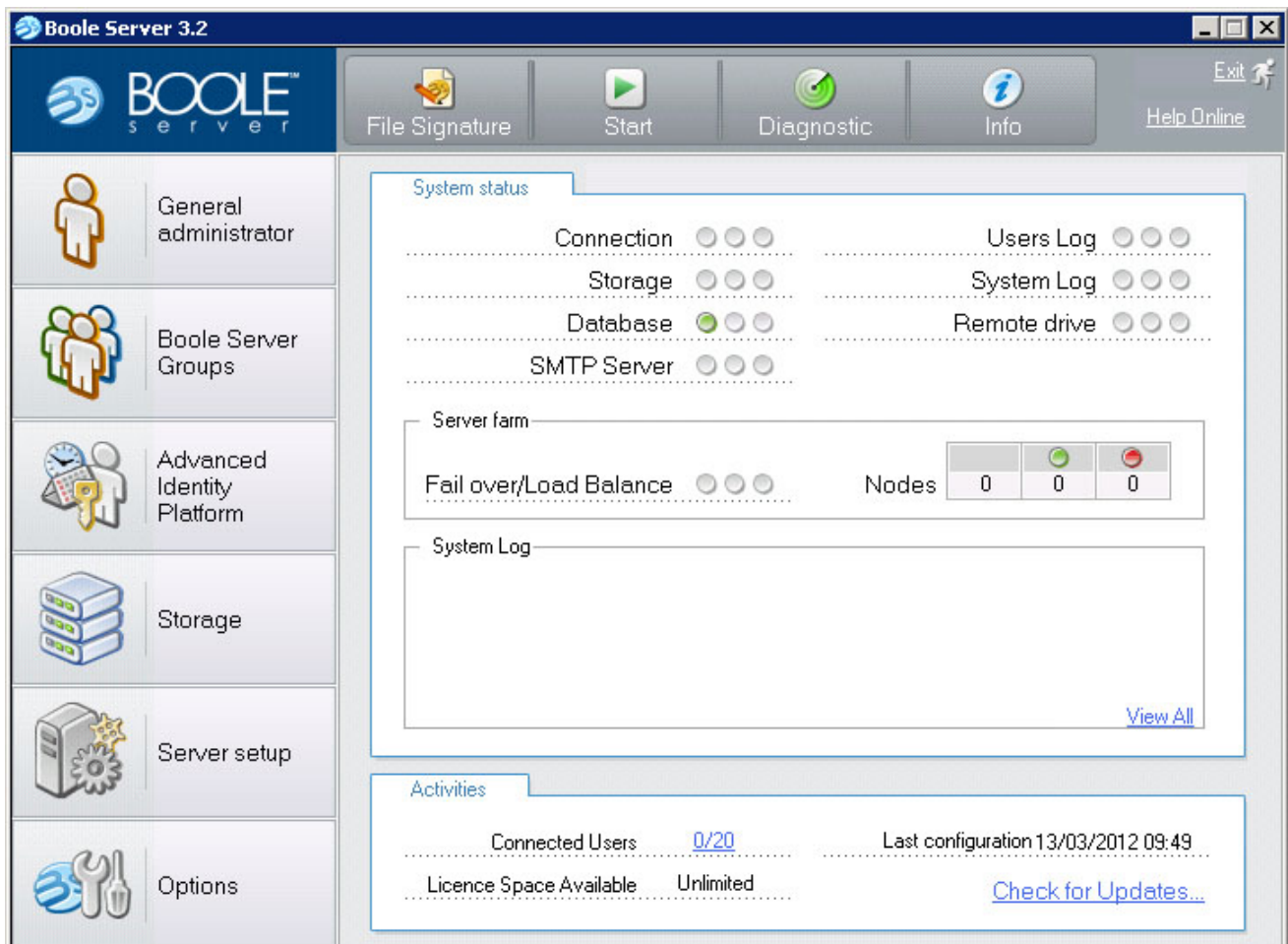


Figure 22: Boole Server Configuration

server, read the online guide and information about the license, etc.)

2.4.4 Status Bar:

It offers hints on how to use server functionalities. The elements contained in Boole Server control panel allow configuring the whole solution according to one's own needs.

2.5 Different Types of Configurations:

Boole Server architecture is designed to encrypt digital documents, while allowing their secured and controlled sharing with work groups, staff, and external customers.

2.5.1 Boole Server Simplest Infrastructure:

Simplest configuration without any backend /failover case

Explanation:

In this simplest model the installation method is same as I mentioned above in details

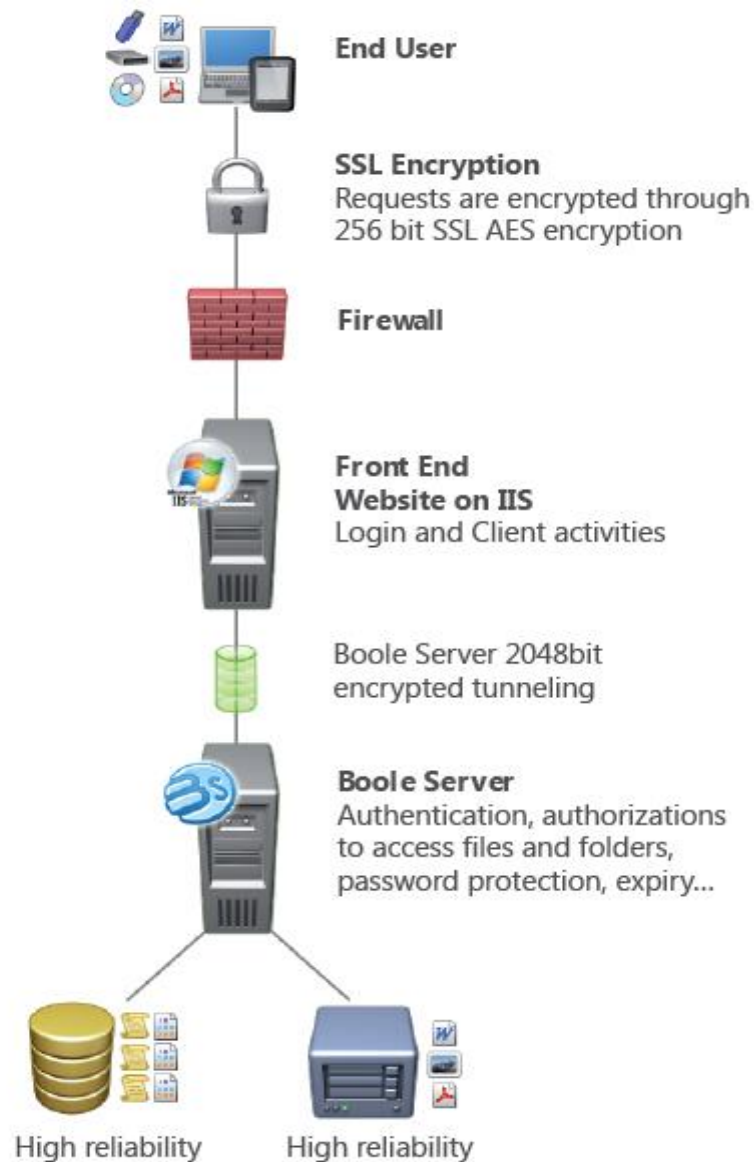


Figure 23: Configuration Topology

2.5.2 Boole Server Advanced Infrastructure in High Availability (HA):

Here are more advance configurations which is mostly used at customer end and I configure these configurations on physical machines as well as on virtual machines and these are currently used configurations

For each described infrastructure, a reference diagram is provided together with the relevant sequence of Operations to be performed to ensure the correct configuration and subsequent functioning of Boole Server.

NOTES: The IP addresses used are examples.

Described infrastructures include only 2 redundancy nodes, both for Boole Server and for IIS. They can be however configured in case of a higher number of nodes.

2.5.2.1 Boole Server Advanced Infrastructure in HA Type - 1:

Boole Server configuration for High availability (HA) environment in which two Boole sever in farm configuration is installed on a same network for more availability and redundancy by using network load balancer/failover.

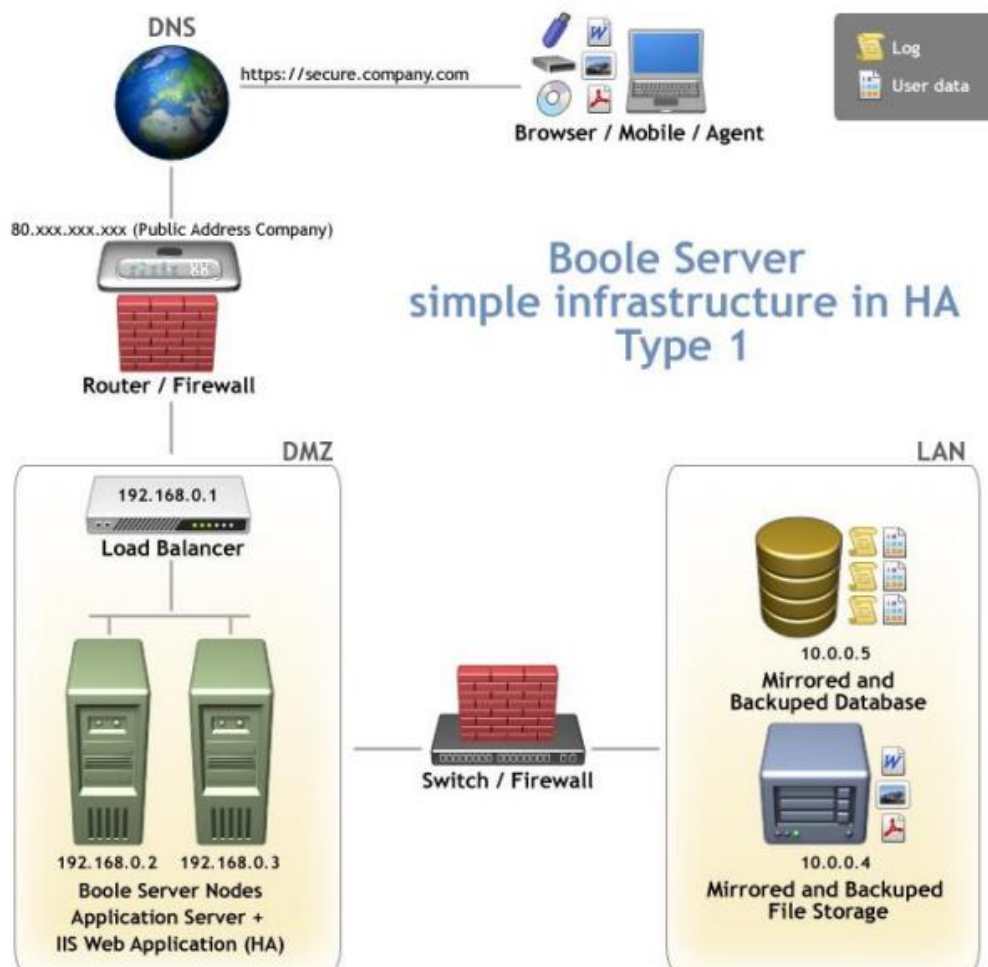


Figure 24: Configuration Topology

Set LAN 1:

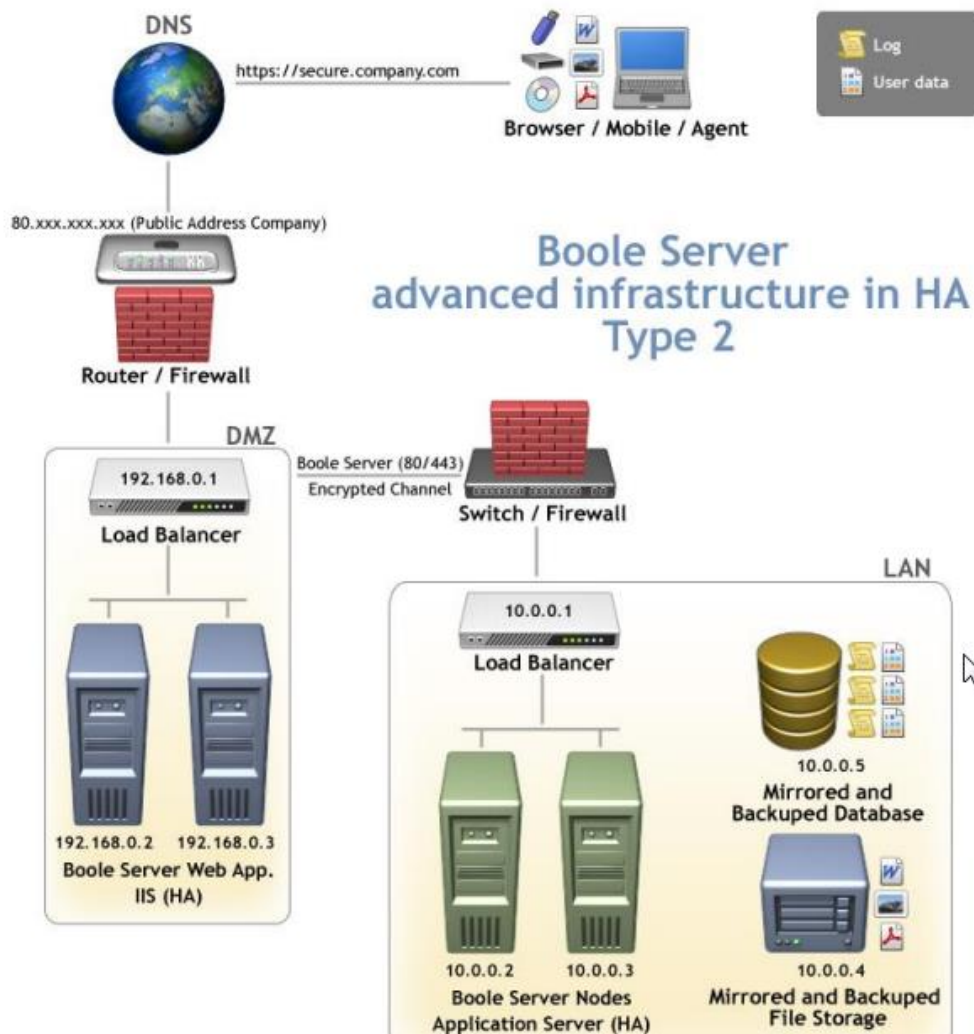
- 1) Install SQL Server 2008R2 database on 10.0.0.5 server (in HA environment, if possible), reachable by both Servers (192.168.0.2 and 192.168.0.3);
- 2) Set a file server on 10.0.0.4 (in HA environment, if possible), reachable by both Servers (192.168.0.2 and 192.168.0.3);
- 3) Set a Balancer in DMZ which points to the two IP addresses 192.168.0.2 and 192.168.0.3 (Windows Network Load Balance is enough)
- 4) From the Firewall which divides the two zones (DMZ and LAN), open the ports to access the Database and storage;
- 5) Perform Boole Server Setup with Web Application on the two servers (192.168.0.2 and 192.168.0.3);
- 6) Perform Boole Server Installation Wizard as Primary Server on machine 192.168.0.2;
- 7) In Primary Server, from Boole Server Panel, in Server Setup -> IP Server section, add the following listening IP addresses: a. 192.168.0.2; b. Remove address 127.0.0.1;
- 8) Set File Signature to correctly start the service: enter company's data.
- 9) Enter Network Credentials on both nodes (credentials authorized to read and write in the network storage previously set).
- 10) In Server Setup -> Boole Farm section, set primary and secondary server.
- 11) Start the service.
- 12) Execute Boole Server Installation Wizard as Secondary Node on machine 192.168.0.3.
- 13) In Secondary Node, from Boole Server Panel, in Server Setup -> IP Server section, add the following listening IP addresses: a. 192.168.0.3; b. Remove address 127.0.0.1;
- 14) Start the service.
- 15) Access "Web Client" folder available in Boole Server installation path and edit the following parameters contained in the SETTINGS.CONFIG file:
 - A. For the file contained in Primary Server (192.168.0.2):
 1. <add key="LocalWebSiteAddress" value=" "/>
 2. <add key="BooleAddress" value="192.168.0.2"/>
 3. <add key="BoolePort" value="2450"/>
 - B. For the file contained in Secondary Node (192.168.0.3):
 1. <add key="LocalWebSiteAddress" value=" "/>
 2. <add key="BooleAddress" value="192.168.0.3"/>
 3. <add key="BoolePort" value="2450"/>

NOTE: Before performing the following steps, check on both nodes, through Boole Server panel, that the farm is in active status and that no problems are detected in the general status (check there are no red lights).

- 16) Perform the following tests:
 - a. On both Boole Server nodes, run Internet Browser and type the private IP address of the machine in the address bar. Example for Primary Server: http://192.168.0.2
- 17) If the Web application has been successfully installed, the Boole Server login window will appear in a few seconds.

- a. In the relevant fields, enter the access credentials to access the profile set in the first group created during Wizard installation. If access does not return the "Connection Failed" message, the application is correctly running. This test has to be performed on both nodes.
- 18) On both IIS servers, install a CA certificate, valid if possible, to recognize the Web address through which the browser is connecting, and to ensure that data are always transferred in encrypted mode.
 - 19) In IIS binding, do not disable the HTTP private connection to the Website. It is important that it stays enabled to allow the Website to connect to itself through the private IP set in the LocalWebSiteAddress variable of the Settings.config in the two IIS servers.
 - 20) Associate router IP public address (80.xxx.xxx.xxx) with DNS record of company's address (e.g. <https://secure.company.com>).
 - 21) Perform routing of IP public number (80.xxx.xxx.xxx) towards the IP private address of the Balancer in DMZ.
 - 22) Connect externally.

2.5.2.2 Boole Server Advanced Infrastructure in HA Type - 2:



Boole Server advance architecture which divides our configuration in front end and back end for more security so that user can't directly connect with that server which is directly contacted to DB and storage but the configuration and installation method is same as in simple configuration and in this configuration users are not directly contact with back end server.

Set LAN 2:

- 1) Install SQL Server 2008R2 database on 10.0.0.5 server (in HA environment, if possible), reachable by both Servers (10.0.0.2 and 10.0.0.3);
- 2) Set a file server on 10.0.0.4 (in HA environment, if possible), reachable by both Servers (10.0.0.2 and 10.0.0.3);
- 3) Set a Balancer in LAN which points to the two IP addresses 10.0.0.2 and 10.0.0.3 (Windows Network Load Balance is enough);
- 4) Perform Boole Server Setup with Web Application on the two servers 10.0.0.2 and 10.0.0.3;
- 5) Execute Boole Server Installation Wizard as Primary Server on machine 10.0.0.2;

- 6) In Primary Server, from Boole Server Panel, in Server Setup -> IP Server section, add the following listening IP addresses: a. 10.0.0.2; b. Remove address 127.0.0.1;
- 7) Set File Signature to correctly start the service: enter company's data.
- 8) Enter Network Credentials on both nodes (credentials authorized to read and write in the network storage previously set).
- 9) In Server Setup -> Boole Farm section, set primary and secondary server.
- 10) Start the service.
- 11) Execute Boole Server Installation Wizard as Secondary Node on machine 10.0.0.3;
- 12) In Secondary Node, from Boole Server Panel, in Server Setup -> IP Server section, add the following listening IP addresses: a. 10.0.0.3; b. Remove address 127.0.0.1;
- 13) Start the service.
- 14) Access "WebClient" folder available in Boole Server installation path and edit the following parameters contained in the SETTINGS.CONFIG file:
 - A. For the file contained in Primary Server (10.0.0.2):
 - a. `<add key="LocalWebSiteAddress" value=""/>`
 - b. `<add key="BooleAddress" value="10.0.0.2"/>`
 - c. `<add key="BoolePort" value="2450"/>`
 - B. For the file contained in Secondary Node (10.0.0.3):
 - a. `<add key="LocalWebSiteAddress" value=""/>`
 - b. `<add key="BooleAddress" value="10.0.0.3"/>`
 - c. `<add key="BoolePort" value="2450"/>`

NOTE: Before performing the following steps, check on both nodes, through Boole Server panel,

- 15) That the farm is in active status and that no problems are detected in the general status (check there are no red lights).
- 16) Perform the following tests:
 - a. On both Boole Server nodes, run Internet Browser and type the private IP address of the Machine in the address bar. Example for Primary Server: `http://10.0.0.2`
- 17) If the Web application has been successfully installed, the Boole Server login window will appear in a few seconds.
 - b. In the relevant fields, enter the access credentials to access the profile set in the first group created during Wizard installation. If access does not return the "Connection Failed "message, the application is correctly running this test has to be performed on both nodes

Set DMZ:

- 1) Set a Balancer in DMZ which points to the two IP addresses 192.168.0.2 and 192.168.0.3 (Windows Network Load Balance is enough);

- 2) Perform Boole Server Setup by installing only the Web Application on the two servers 192.168.0.2 and 192.168.0.3;
- 3) Access “WebClient” folder available in Boole Server installation path and edit the following parameters contained in the SETTINGS.CONFIG file:
 - A. For the file contained in Primary Server (192.168.0.2):
 - a. <add key="LocalWebSiteAddress" value="http:// 10.0.0.1"/>
 - b. <add key="BooleAddress" value=""/>
 - c. <add key="BoolePort" value=""/>
 - B. For the file contained in Secondary Node (192.168.0.3):
 - a. <add key="LocalWebSiteAddress" value="http:// 10.0.0.1"/>
 - b. <add key="BooleAddress" value=""/>
 - c. <add key="BoolePort" value=""/>
- 4) From the Firewall which divides the two zones (DMZ and LAN) open port 80;
- 5) Perform the following tests:
 - a. On both IIS servers, run Internet Browser and type the private IP address of the machine in the address bar. Example for the first server: http://192.168.1.2
- 6) If the Web application has been successfully installed, the Boole Server login window will appear in a few seconds.
 - a. In the relevant fields, enter the access credentials to access the profile set in the first group created during Wizard installation. If access does not return the “Connection Failed “message, the application is correctly running this test has to be performed on both IIS servers
- 7) On both IIS servers, install a CA certificate, valid if possible, to recognize the Web address through which the browser is connecting, and to ensure that data are always transferred in encrypted mode.
- 8) In IIS binding, do not disable the HTTP private connection to the Website. It is important that it stays enabled to allow the Website to connect to itself through the private IP set in the LocalWebSiteAddress variable of the Settings.config in the two IIS servers
- 9) Associate router IP public address (80.xxx.xxx.xxx) with DNS record of company’s address (e.g. https://secure.company.com).
- 10) Perform routing of IP public number (80.xxx.xxx.xxx) towards the IP private address of the Balancer in DMZ.
- 11) Connect externally.

2.5.3 Balancer Configuration:

The configuration of load balancer is same in farm configuration network and I also used this configuration method

To configure a balancer, all of the following are needed:

1. Server which serves as a balancer
2. Servers which are added to the balancer cluster

Fundamental prerequisite is that all NICs of the Servers you wish to add to the cluster are configured with a static IP address and not with DHCP. The Network Load Balancing feature is to be installed on the three servers.

To install the feature, follow these steps:

1. Launch Manager Server.
2. Select Features.
3. Select add Features.
4. Select Network Load balancing from the list of available features.
5. Click on "Next" to perform installation.

After installing the service on all servers, it is necessary to create the cluster:

On the server which serves as a balancer:

1. Launch Network Load Balancing Manager.
2. From the "Cluster" menu, select "New".
3. Enter host address in the configuration window.
4. In the "Host Parameters" window, set the priorities to assign to the host (1 for primary node, 2 for Secondary node and so on)
5. In the "Cluster IP Addresses" window, enter the IP address to assign to the cluster.
6. In the "Cluster Parameters" window, enter an Internet Name to assign to the cluster, and select the Multicast option in the "cluster operation mode" box
7. In the "Port Rules" window, edit the TCP or UDP port to be used.
8. Click on Finish and wait for the first cluster node to be added.
9. Repeat the operation for the second node.

To allow the Web Client to maintain the session among several IIS instances in the presence of a balancer, the following configuration is necessary:

- 1) Edit Web.config of all nodes, by replacing:

```
<sessionState timeout="60" mode="InProc"></sessionState>
```

With

```
<sessionState timeout="60" mode="StateServer"
stateConnectionString="tcpip=server:port"></sessionState>
```

Where server:port is the port of the machine authorized to maintain the session.

After </sessionState> add

```
<machineKey
```

```
ValidationKey='5DE7C67E937E863DD39258E7B3F01645C77EB8AB4065A6FE26533C
8E7D19BB4B2
```

```
74394524012A0ABDA53D09E3D4BB7CFE6608D8F5A2E11562C7A998B725F94C9'
```

```
decryptionKey='95F3B7B4A71DAA3B86651A609F437F31A20AA99E404CCA9C'
```

```
Validation='SHA1'/>
```

Configure ASP.Net State Service on the machine chosen to maintain the session33

- 2) Edit the register by entering 1 in the key:

```
HKLM\SYSTEM\CurrentControlSet\Services\aspnet_state\Parameters\AllowRemote  
Connections
```

- 3) Open port 42424 (default port) set in:

```
HKLM\SYSTEM\CurrentControlSet\Services\aspnet_state\Parameters\Port
```

- 4) Start the service

CHAPTER 3: BOOLE SERVER CLIENT SIDE

3.1 Web client:

The tool to use Boole Server functionalities the Boole Server Web Client is the tool through which users can exploit the functionalities the system provides. They only need to connect from any Internet browser, either Windows or Mac.



Figure 26: Web Client

The Web Client control panel allows:

- protected centralization of files and folders
- sharing of company files in a selective, granular and temporary manner
- creation and control of access profiles
- monitoring the activities performed by users on protected files
- sharing messages in encrypted mode
- viewing files in protected mode
- encryption of company texts and files
- sending via e-mail direct links to centralized encrypted resources

3.2 Most Important features of Boole Web client:

3.2.1 Sharing In Boole Server:

- Boole Server profiles - (Sharing files and/or folders with other profiles) to share files and/or folders with other Boole Server profiles.
- External users - (Sharing files and/or folders with external users)

To share files and/or folders via e-mail, with external users who are not registered in Boole Server

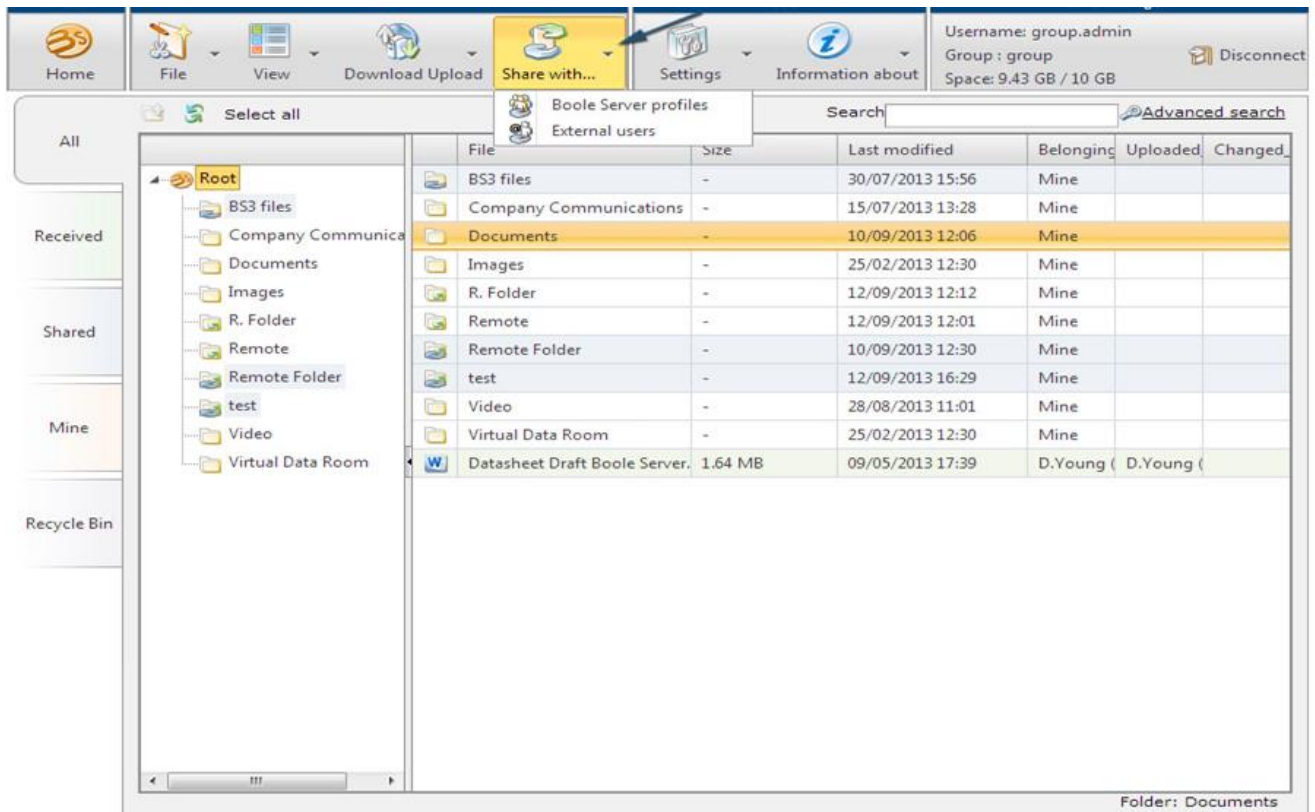


Figure 27: Sharing

A window will appear through which you can configure Share properties

ATTENTION!

You can even share entire folders: every time a file is saved in the shared folder, it will automatically inherit all the sharing properties previously set for the folder containing it.

According to the authorizations granted to the profile, after clicking on Share, the following cases may occur:

- Case 1: Boole Server default Templates are displayed
- Case 2: only the assigned Templates are displayed
- Case 3: it is possible to set protection and sharing properties.

NOTES: Protection Templates can define both the protection level to be applied and the sharing recipients; it is also possible to define only the protection level, granting the profile the possibility to select the sharing recipients

It is also possible to use Nested Templates to gather together several Protection Templates with different protection and sharing levels.

Nested Templates can be configured only by the System Administrator (Server side)

CASE 1:

The window with the default Templates will appear: the profile has been assigned the authorizations to use the protection Templates available in Boole Server.

By default, the following Templates are assigned to Boole Server profiles:

- Customized: customized protection
- Not Classified
- Limited
- Reserved
- Secret
- Top Secret



Figure 28: Sharing Case - 1

- To view the protection properties of a Template, select the desired item and click on the corresponding I icon



Figure 29: Sharing Limited

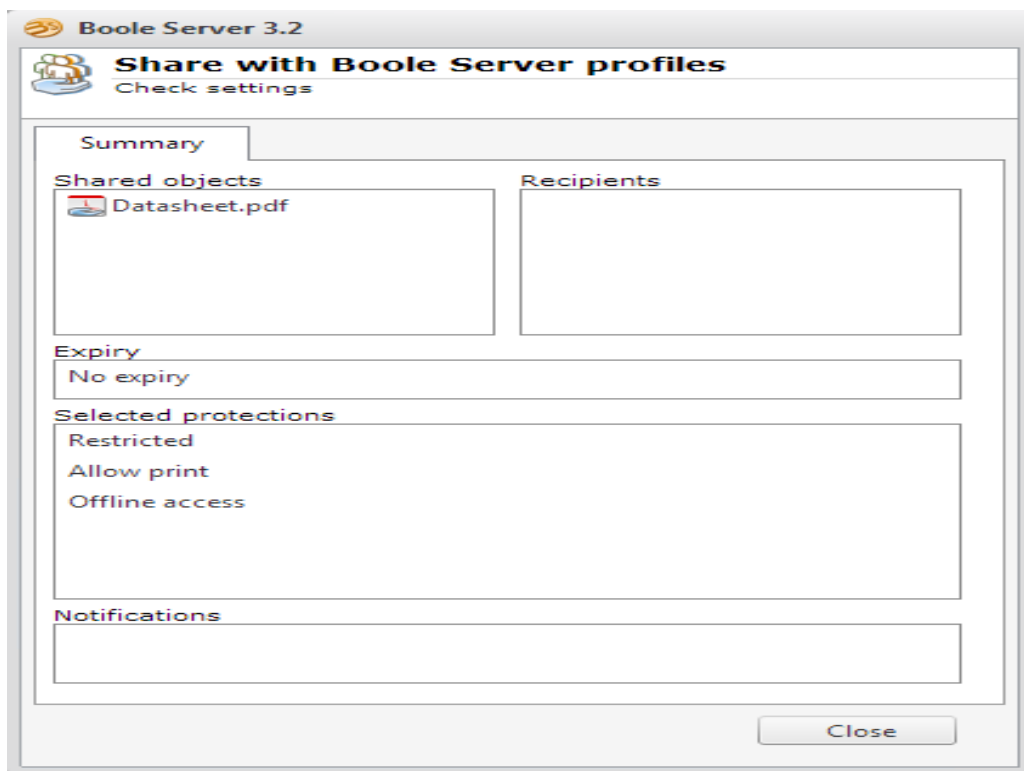


Figure 30: Sharing With Boole Server Profile

NOTE: The default Template corresponding to Customized allows to access the window for customized configuration of the protection and sharing properties.

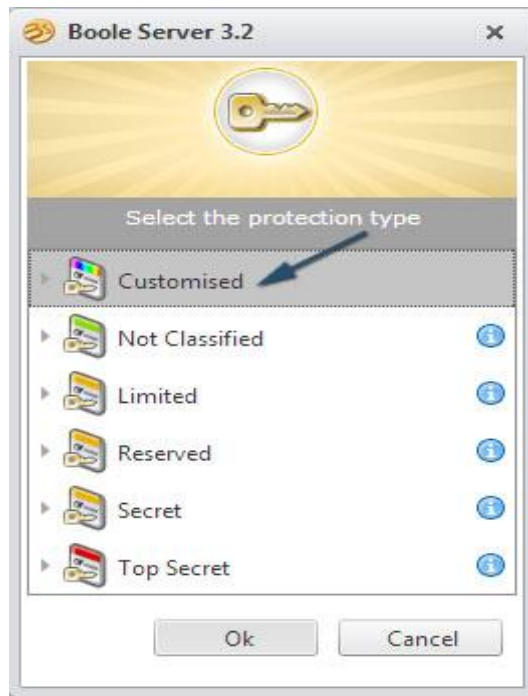


Figure 31: Sharing Customized

CASE 2:

A message will show to confirm that sharing has been successfully completed: the profile has been assigned the authorizations to share his own resources through one single protection Template.

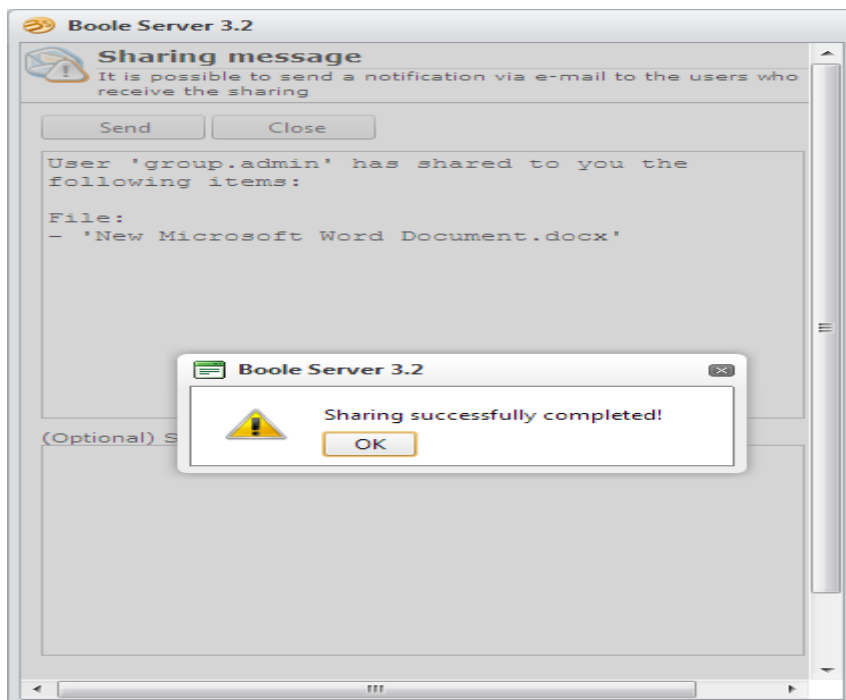


Figure 32: Sharing Case - 2

CASE 3:

The window for the configuration of sharing properties will appear: the profile is authorized to set protection and sharing properties.

- The Users screen appears in the foreground by default: you need to select the profiles you want to share the selected files with.
- From the dropdown menu in the Group list field select the group where the profile you want to share files with is included; the name of the group the user belongs to will show by default.
- According to the selected group, in the field below the list of profiles associated with the selected group will appear: select the profile you wish to share files with.
- Click on Share with the whole group or Share with the selected users: the selected users will be displayed in the list below together with the other sharing recipients.
- To selectively remove certain profiles or groups from the sharing recipients previously selected, select the desired entry and click on Remove.

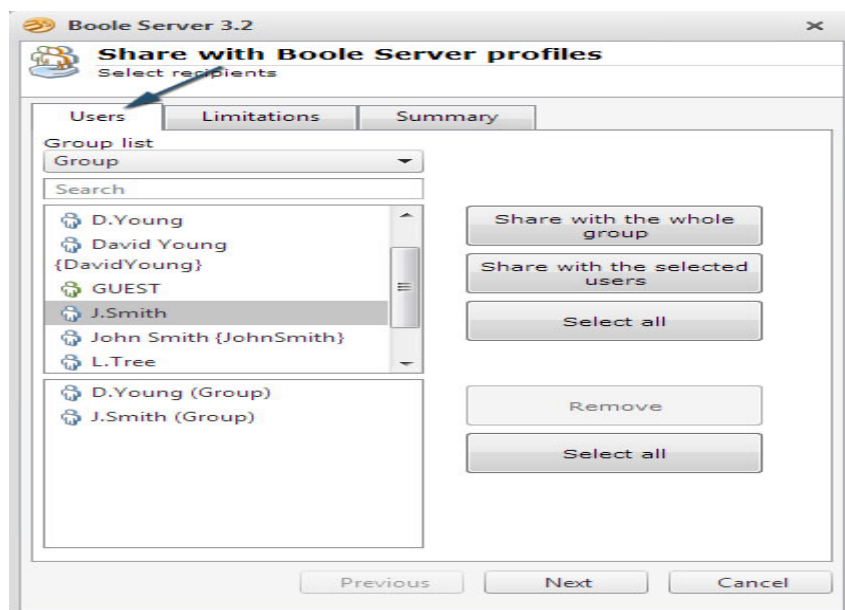


Figure 33: Sharing Case - 3

- Click on Next at the bottom of the window or bring the Limitations screen in the foreground.
- The Limitations tab allows to set security properties to be applied to the file you wish to share.

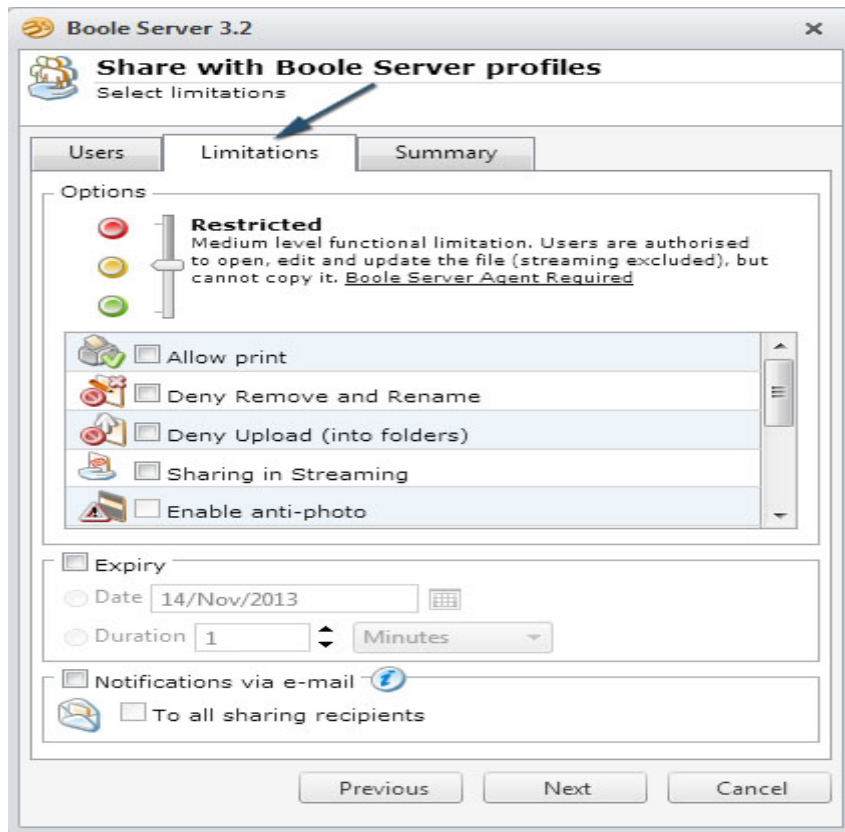


Figure 34: Sharing Limitations

- In the Options area, it is possible to set the protection level to be applied to the file you wish to share, by vertically moving the mouse pointer:
- Read-only - High level functional limitation - Red led: Users are authorized to view the file, but cannot edit it.
- Restricted - Medium level functional limitation - Yellow led: Users are authorized to open, edit and update files, but cannot copy them.
- Unlimited - Low level functional limitation - Green led: Users are authorized to perform any operation on files.
- By clicking on *Boole Server Agent Required*, a window shows containing the following message: *in order to view the protected file in the selected mode, the sharing recipient must have the Boole Server Agent application installed on his*

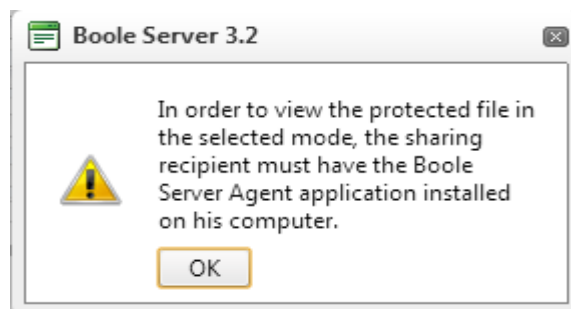


Figure 35: Sharing Warning Message

computer

- Click Ok to close the window

According to the selected protection level, the area below displays additional options which are applied to sharing recipient.

3.2.2 Custom Sharing Options:

- Allow Print: allows the recipient to print the shared file.
- Deny Remove and Rename: allows blocking the relevant operations.
- Deny Upload (into folders): allows blocking the upload of files into a shared folder
- Sharing in Streaming: to share the selected resources in protected streaming, i.e. a special protected format which is not editable.
- Enable anti-photo: makes the file in protected streaming available in a particular mode through which it is possible to view only one of its part at a time, as if a light were pointed on the area you wish to view. To move the Adjustable reflector you need to move the mouse pointer.
- Enable download in PDF: allows the recipient to download the file in non-editable PDF format.
- Apply Watermark: allows applying watermarks to the secured file. By enabling this option, the next field will be automatically enabled: clicking on the setting icon, the Customized watermark window shows through which it is possible to edit the characteristics of the watermark set by default. The available parameters are:
 - Position: to choose the appropriate position where the watermark will appear.
 - Font size: to select the type size for the text of the watermark.
 - Text opacity: to choose the degree of opacity for the text.
 - Background opacity: to choose the degree of opacity for the background against which the text will be displayed.
 - Text color: to select the text color. To view the colors available, click on the color swatch near the words.
 - Background color: to select the background color against which the watermark text will be displayed. To view the colors available, click on the color swatch near the words.
 - Parameters: to set the text you wish to appear in the watermark; to select dynamic values, click on the question mark (?) to learn the syntax through which the desired parameter can be correctly set (e.g., by typing %ip, the watermark will contain the IP address number from which the sharing recipients will view the file).
- Offline access: allows downloading received sharing's and makes it available in offline mode
- On any computer: allows using the offline file on any computer and not only on the computer from which the certificate has been generated.
- Allow re sharing: allows the sharing recipient to share the received resources with other users

- Only if authorized: allows forwarding sharing only if authorized by the original sender. When the recipient of the current sharing tries to share the received file, the sender will be notified and can choose whether to authorize the sharing or not.
- Deny file opening with Office macros and/or plug-ins: deny file opening if Microsoft macros or plug-ins are detected.
- By clicking on Preview, it is possible to preview the watermark set.
- Click Ok to confirm.

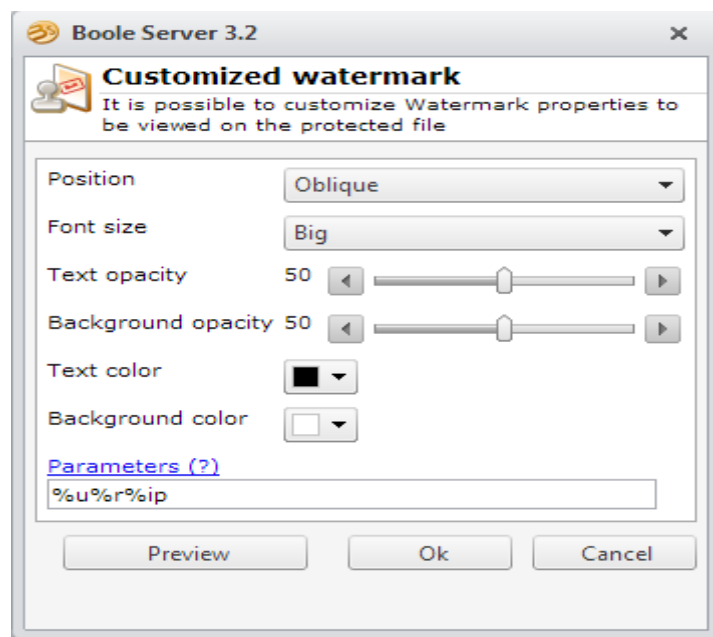


Figure 36: Customized Watermark

According to the type of authorization to grant to sharing recipients, it is possible to set different combinations of protection and sharing to be applied to centralized resources.

Some practical examples follow:

- Example 1: if you wish to share a file with no encryption protection, in order for the recipient to download it in local, edit and copy it, you need to select the unlimited protection level, without enabling any additional option.
- Example 2: if you wish to share a file in protected and encrypted mode, in order for the recipient to access it in read-only mode with no editing possibility, you need to select the Read Only protection level, without enabling any additional option.
- Example 3: if you wish to share a file in streaming and protected viewing mode, in order for the recipient to access it only through Web browser, with no possibility of editing, updating and copying it, you need to select the restricted protection level and enable the Sharing in Streaming additional option.
- In the Expiry area of the Limitations tab, it is possible to set an expiry time after which the sharing will no longer be available.

- If the Expiry checkbox is not enabled, sharing is authorized without time limit
- By enabling the Expiry checkbox and the Date option, it is possible to set a date beyond which sharing will not be available: click on the calendar icon to select a date.
- By enabling the Duration option, it is possible to enter in the relevant field the time length the sharing will be available: the countdown will start when the recipient accesses sharing.

ATTENTION!

The Expiry option will not be applied in case of offline use of the item you are about to share.

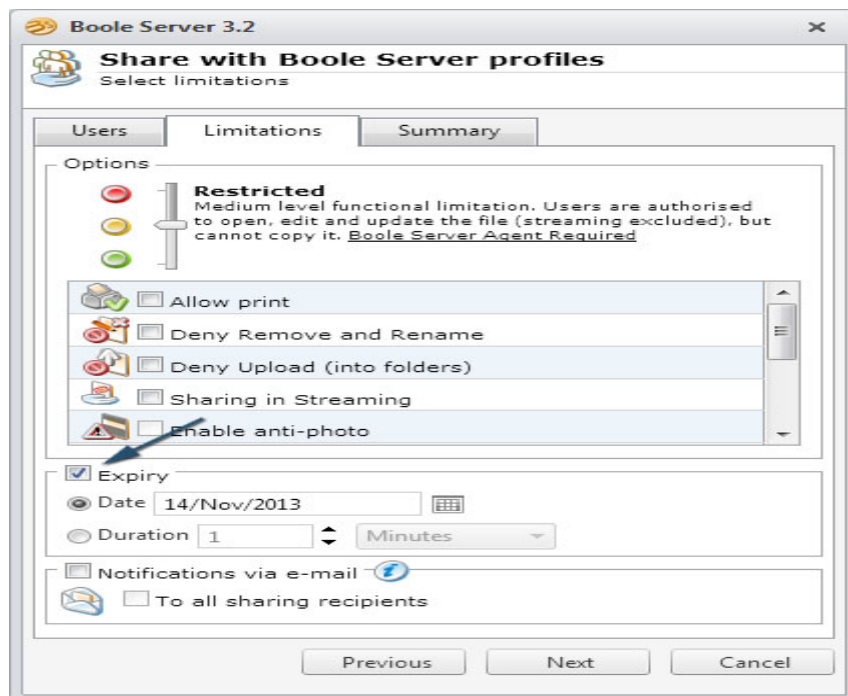


Figure 37: Sharing With Boole Server Profiles

- By enabling the Notifications via e-mail option, Boole Server will send, to the selected profile's e-mail address, notifications about the activities performed on protected and shared files.
- By enabling them to all sharing recipients' option, Boole Server will send, to the e-mail address of the sharing recipient or recipients, notifications about the activities performed on protected and shared files.

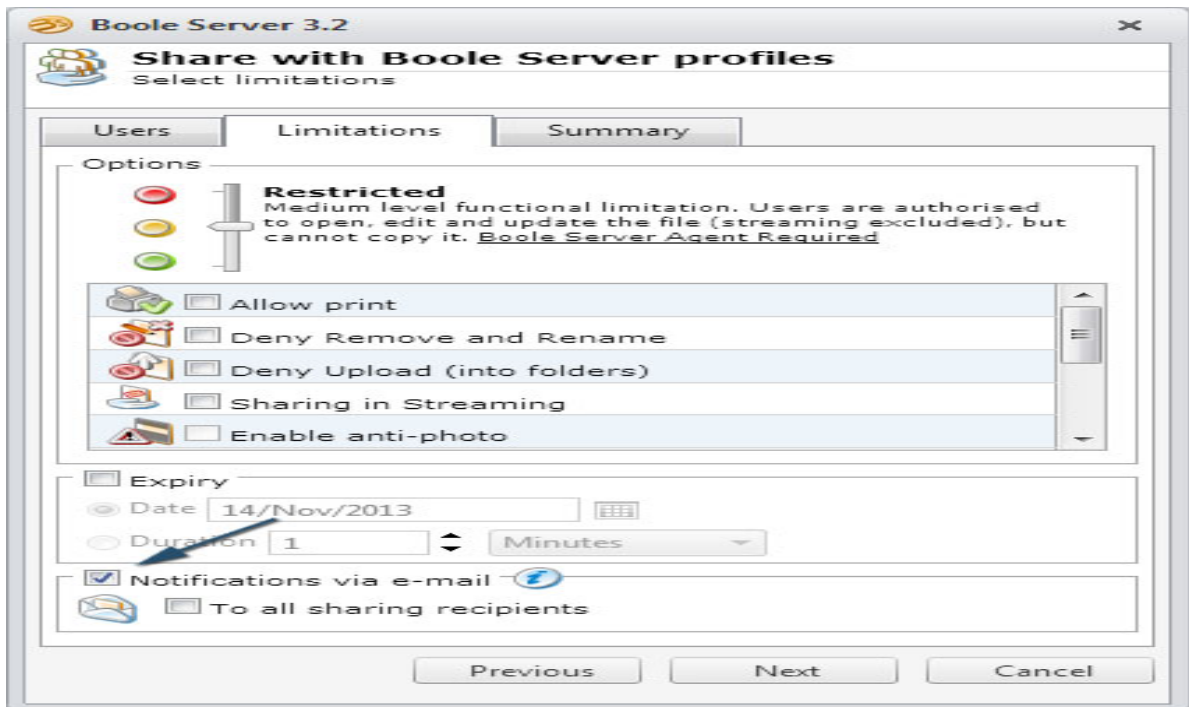


Figure 38: Sharing With Boole Server Profiles e-mail

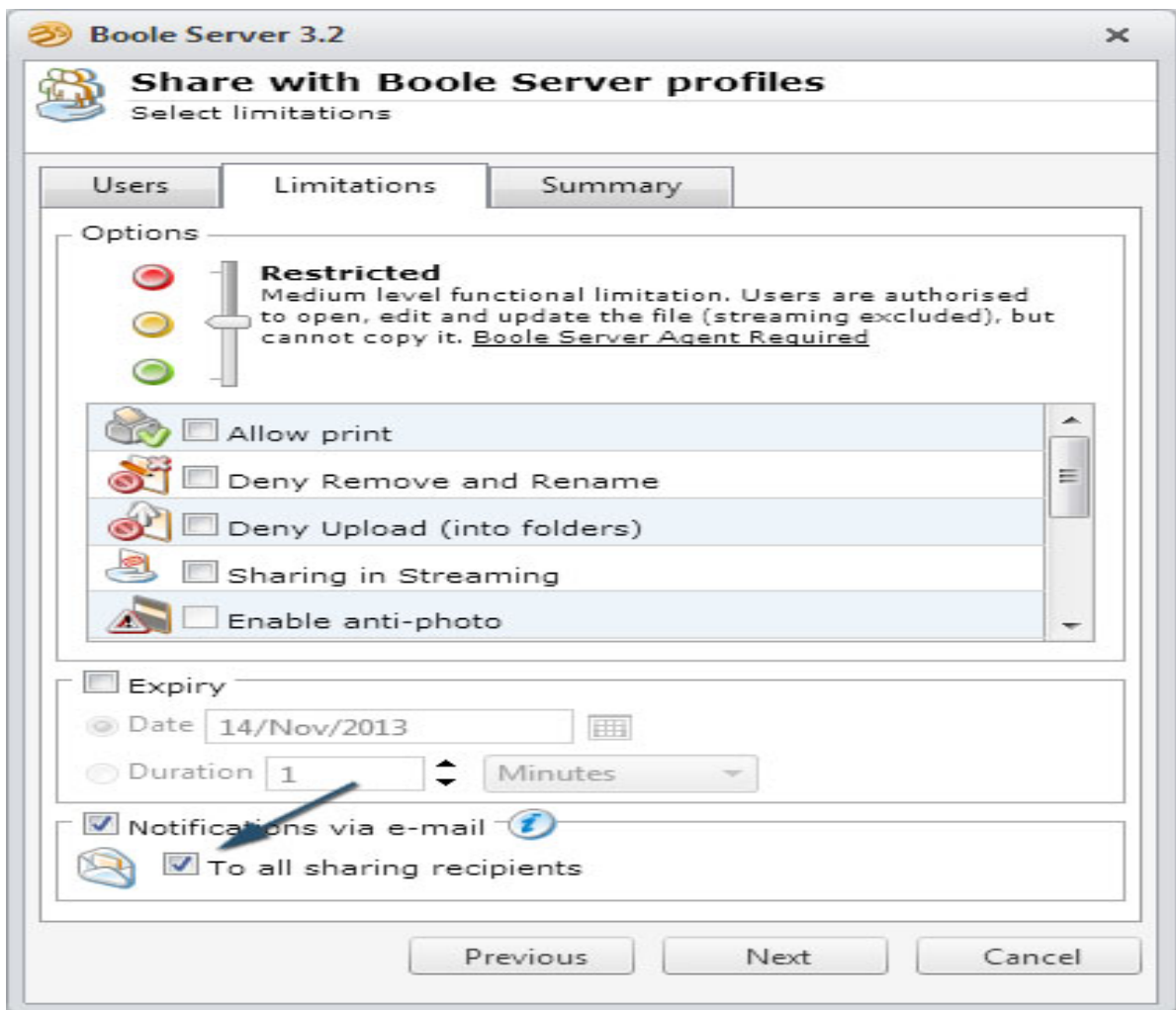


Figure 39: Sharing With Boole Server Profiles e-mail to all

NOTE: You can change the e-mail address specified in the field related to the Notifications via e-mail option accessing the Security Notifications tab available in the Setting-Options window.

- Click on Next in the lower part of the window or bring the Summary screen in the foreground: all the characteristics of the current sharing are summarized here:
- Shared objects
- Recipients
- Expiry
- Selected Protections
- Notifications

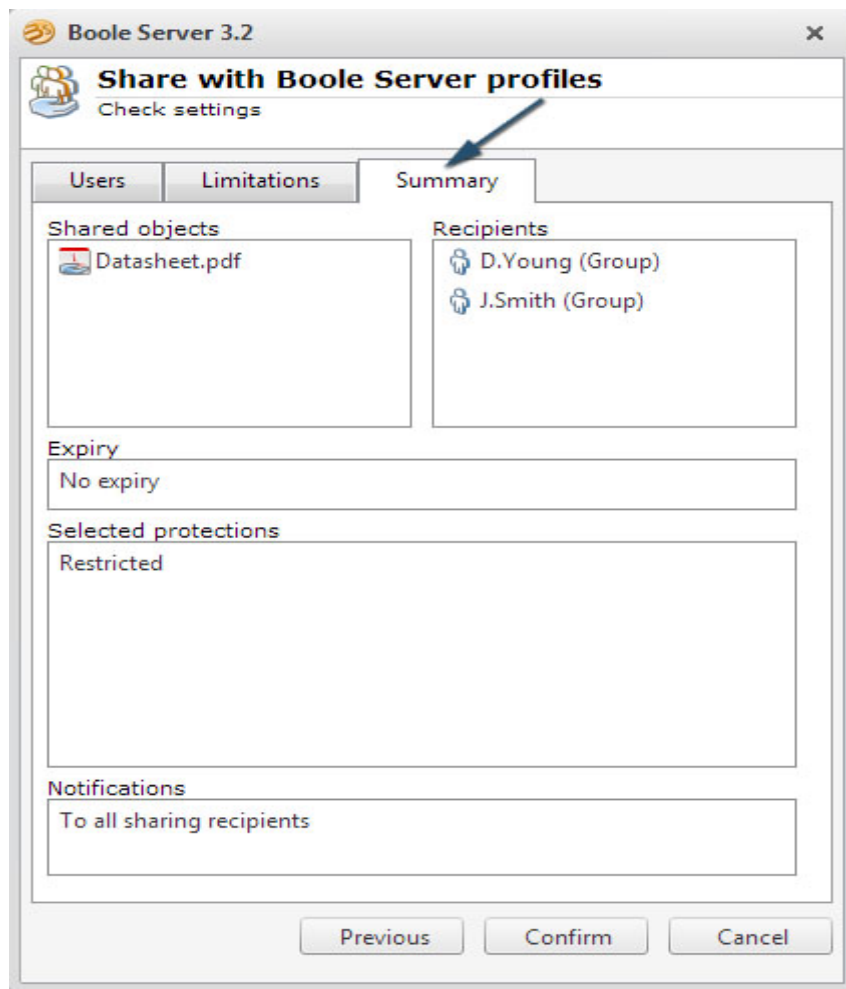


Figure 40: Sharing Summary

- Click on Confirm to enable the configured settings.
- A message will confirm the sharing operation has been carried out successfully.

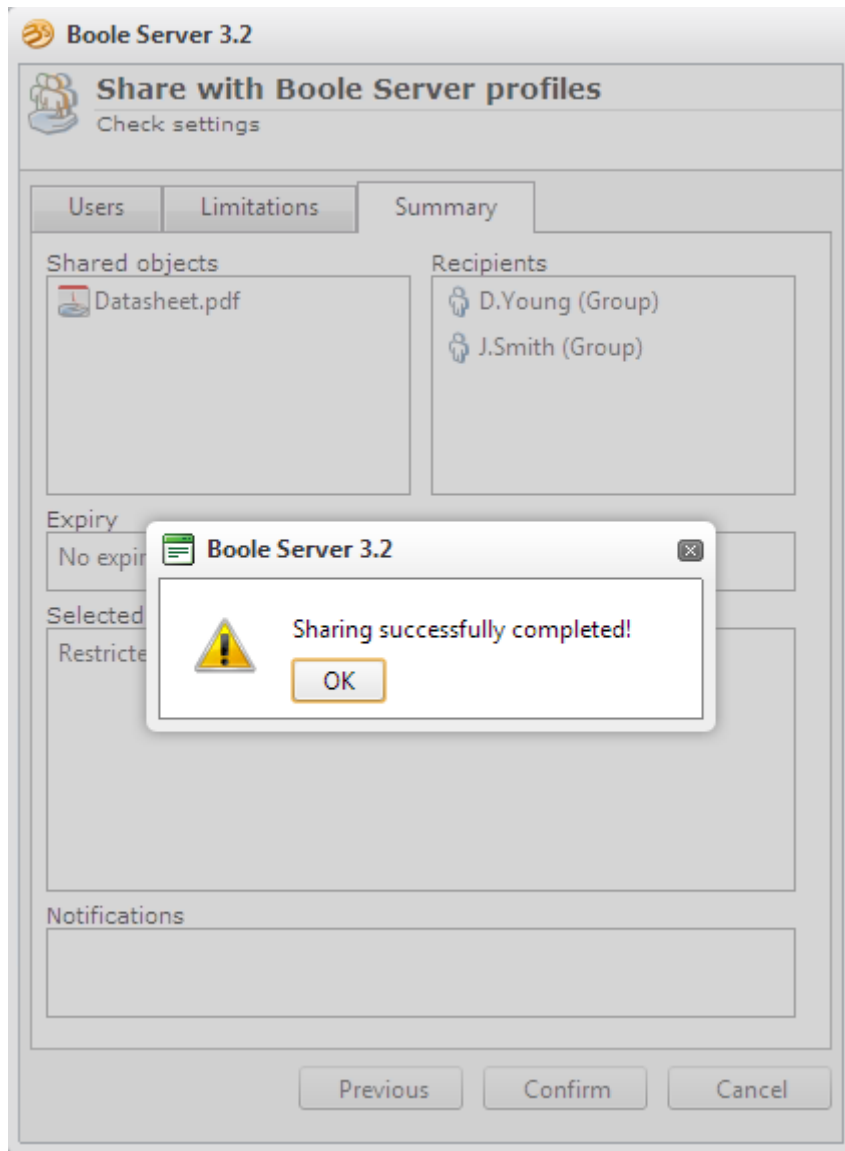


Figure 41: Sharing Successful Warning Box

- Once the sharing is completed, a new window divided into two areas will appear. The upper area is set by default, and shows information related to the profile and direct link to the file you are sharing; the lower area allows to enter an e-mail message, to inform the sharing recipients about the new resources available in Boole Server.

NOTE: It is possible to send a notification e-mail only if an e-mail address is associated to the Boole Server profile who receives the sharing, and if a valid SMTP server has been configured during Boole Server installation.

- If you wish, edit the e-mail text set by default.
- Press Send to send the message.
- Press Close if you do not wish to notify the sharing recipient.



Figure 42: Sharing Message

NOTE: If a folder has been shared, at the end of the configuration process it will be marked by a little hand.

3.2.3 External Users (SHARING FILES AND/OR FOLDERS WITH EXTERNAL USERS):

It is possible to share via e-mail the resources contained in Boole Server centralized space with external users, who are not registered among the System profiles (multiple selection of files or folders is also possible). The System allows entering the sharing recipient e-mail address and making Boole Server protected resources accessible.

3.3 Other Boole Web Client Functionalities:

Following are the more Boole web client features:

3.3.1 Get Link:

Thanks to the Get link functionality, it is possible to directly connect to a file or folder contained in Boole Server centralized resources.

To directly connect:

- Select the desired file or folder
- Right click: a contextual menu will appear
- Click on Get link

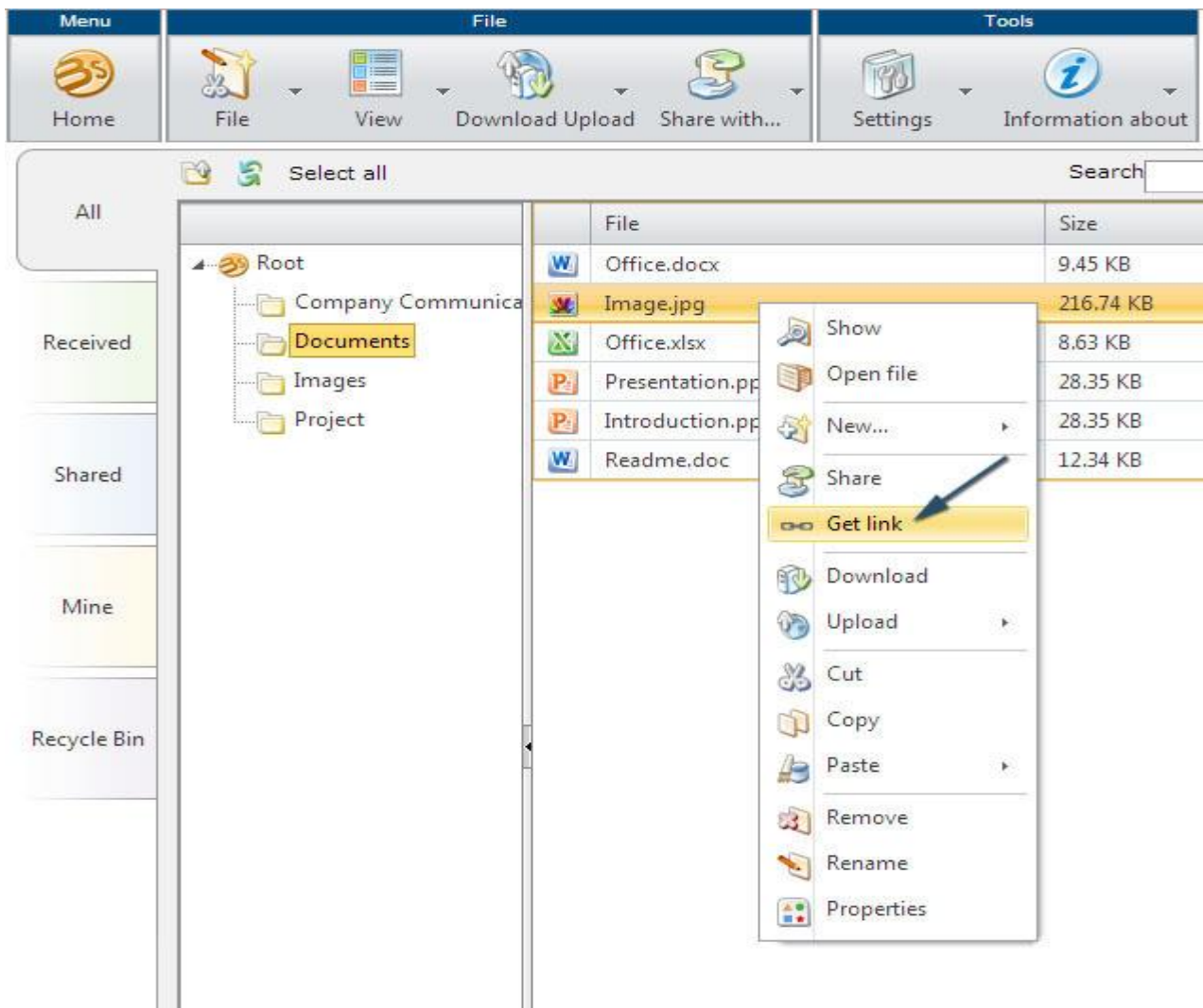


Figure 43: Get Link

- A new window will appear which contains the link to the selected item: since the link corresponds to a Web page with direct connection to the previously selected file or folder, it can be copied, sent or stored for subsequent use.
- To close the window, click on Ok.

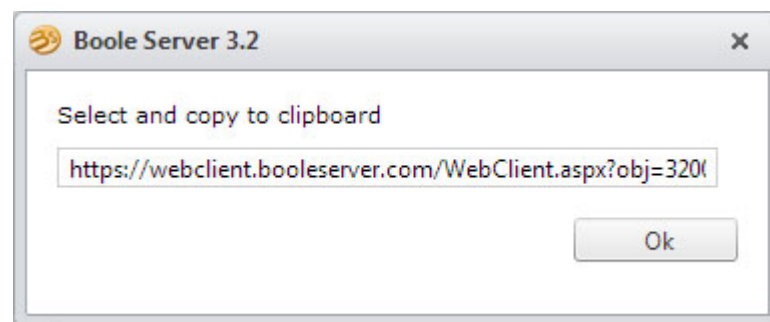


Figure 44: Get Link Dialog Box

To use the link associated to one of Boole Server resources:

- Copy the link in the address bar of the Web browser and start the connection
- A new page will appear. It contains the image associated to the file to which the link is connected
- Click on the relevant file icon within the central area, if you wish to perform download.

NOTE: As for folders, you will get a direct connection link which allows to view only the content associated to it, through the usual Boole Server Web Client screen.

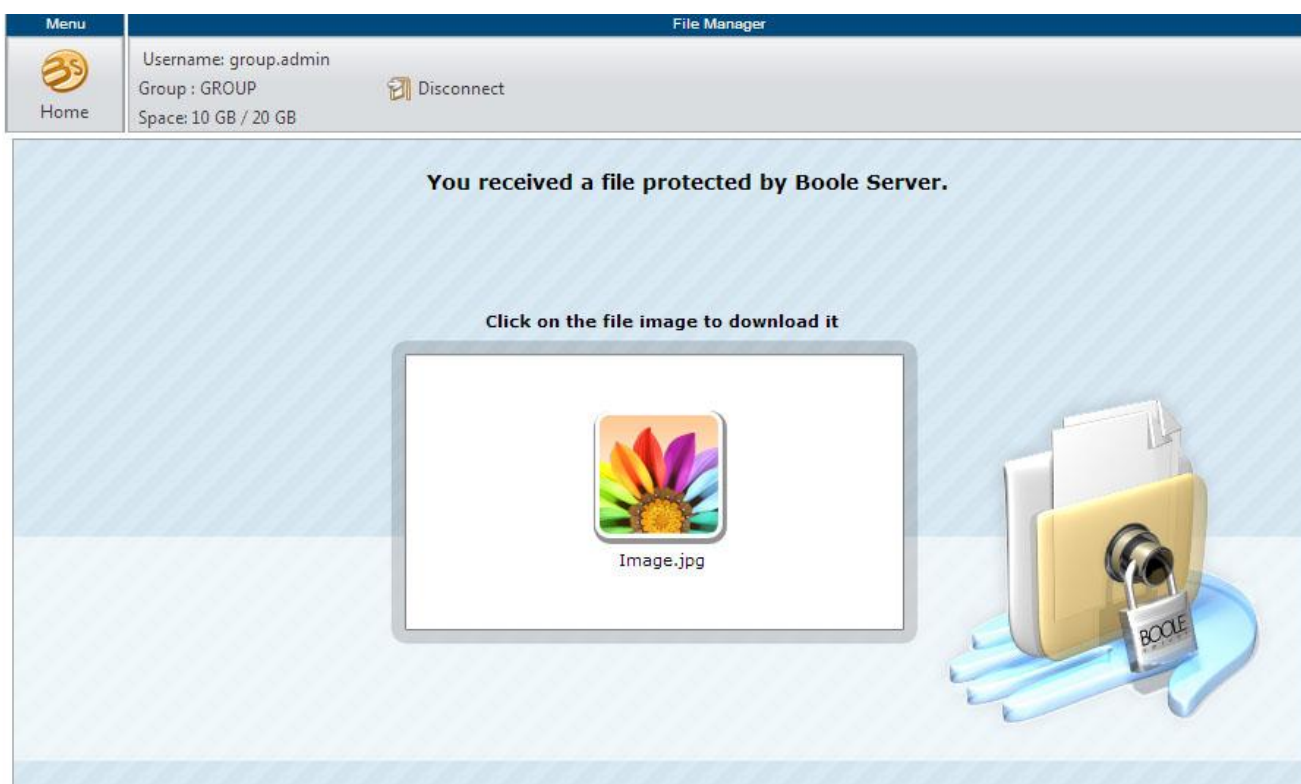


Figure 45: External User File Viewer

NOTE: The link you will get for the direct connection to a file or folder corresponds to the link received via [sharing notifications](#)

3.3.2 Remote Drive:

Thanks to the Remote Drive functionality activated by the Administrator, the Boole Server system allows the access in protected mode of the local shared disks through Microsoft Active Directory: the system is able to synchronize the resources belonging to a specific profile through Boole Server Web Client with the content of local shared disks, and vice versa.

When connecting to Boole Desktop Client, the Boole Server profile synchronized with the local disk will have access to all the resources contained in the configured local folder.

Every time a user add, remove, edit or rename a file in the local folder, the same operation will be automatically mirrored in the centralized resources; similarly when a Boole Server profile associated to Remote Drive add, remove, edit or rename a file in the centralized resources, the same operation will be automatically mirrored in the local folder.

Users to which the Remote Drive functionality has been associated server-side will notice no difference in the normal use of the Web Client.

3.3.3 Encrypt Text:

Boole Server allows encrypting the textual content and exchanging it in a safe way: only selected recipients will be authorized to access it.

To encrypt a text:

- Click on Text encryptor menu.
- Select Encrypt text.

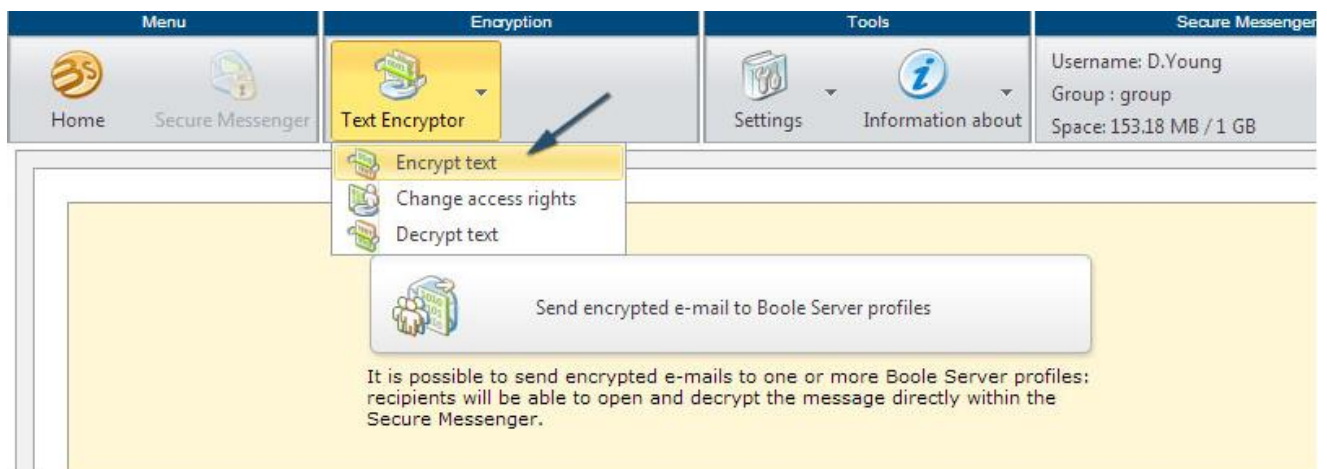


Figure 46: Encrypt Text

- A new page shows where you can write the message you wish to encrypt.
- In the relevant area, write the message you wish to encrypt.

- Click on Encrypt message button.

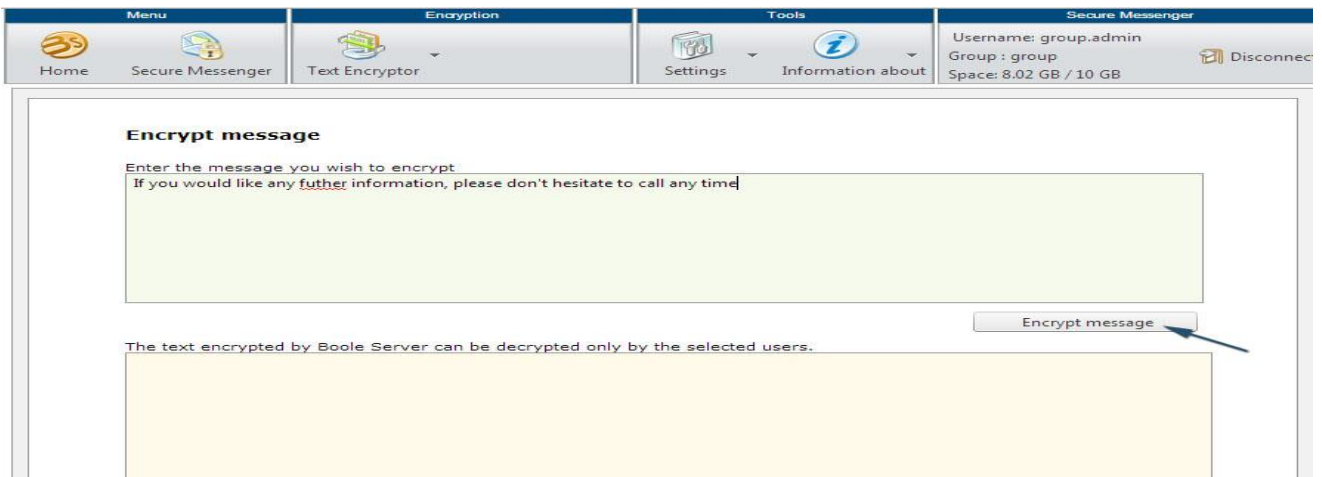


Figure 47: Encrypt Message

- The window shows where it is possible to set the security properties to be applied to the text you wish to encrypt.
- The Users tab appears in the foreground by default where it is possible to choose whether and with whom to share the encrypted text.
- From the dropdown menu in the Group list field select the group where the profile you want to share the encrypted text with is included; the name of the group the user belongs to will show by default.
- According to the selected group, in the field below the list of profiles associated with the selected group will appear: select the profile you wish to share the encrypted text with.
- Click on Share with the whole group or Share with the selected users: the selected users will be displayed in the list below together with the other sharing recipients.

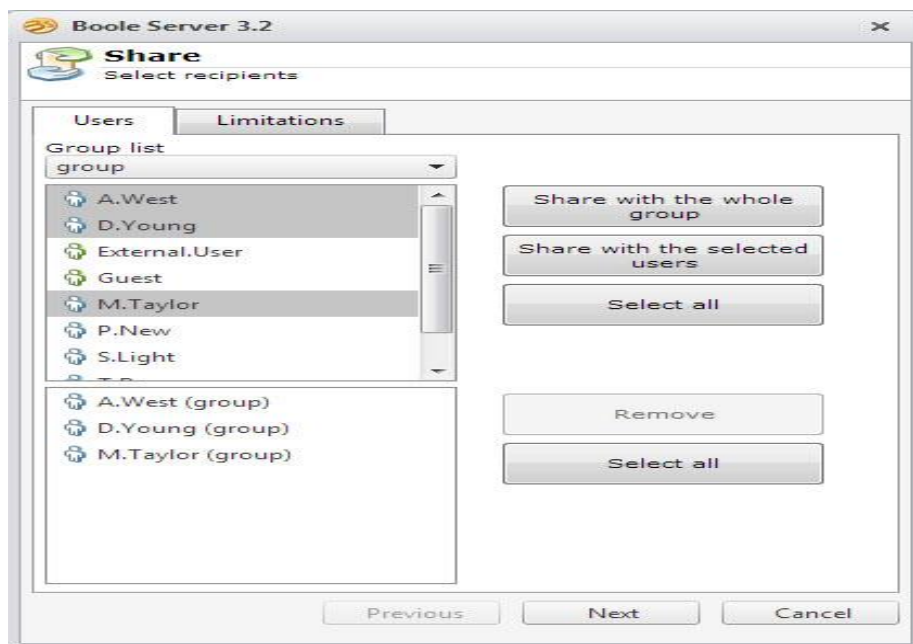


Figure 48: Group Share

- Click on Next or bring the Limitations tab in the foreground.
- Enable the Expiry option if you wish to set a validity period beyond which the encrypted text will not be available:
- Select the Date option and click on the dropdown menu to view the calendar and select a date.
- Select the Duration option and enter the validity period of the sharing, which will be consumed only while the text will be in use.
- Enabling the Notifications via e-mail option, Boole Server will send to the specified e-mail address the notifications related to the activities performed on the protected file.

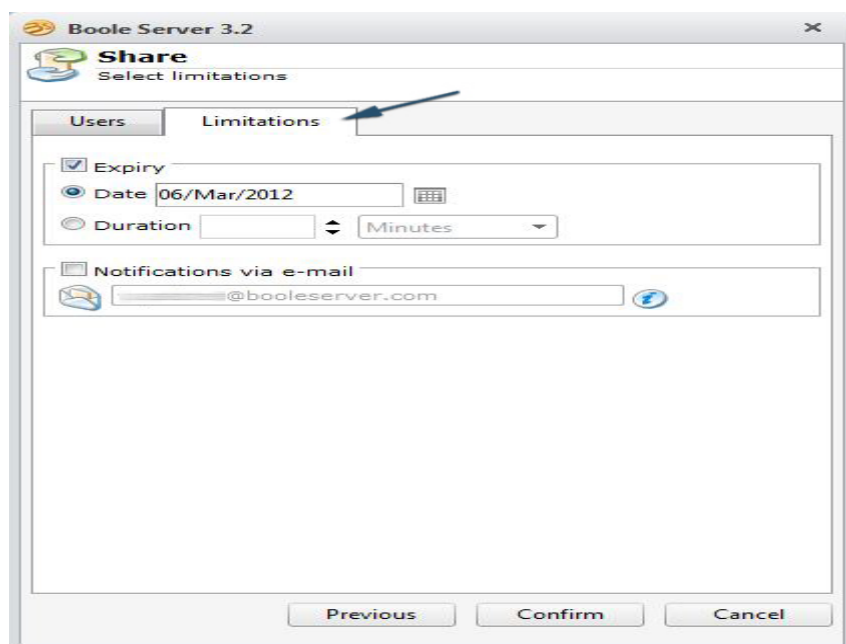


Figure 49: Sharing Limitations

- Click on Confirm to apply the settings.
- The selected text appears as encrypted in the area below: the encrypted text is preceded and followed by a string informing the user that the text is encrypted (e.g. <START SELECT - BOOLE SERVER ENCRYPTION> C433260AEC6CECCEBD <BOOLE SERVER ENCRYPTION - END SELECT>).

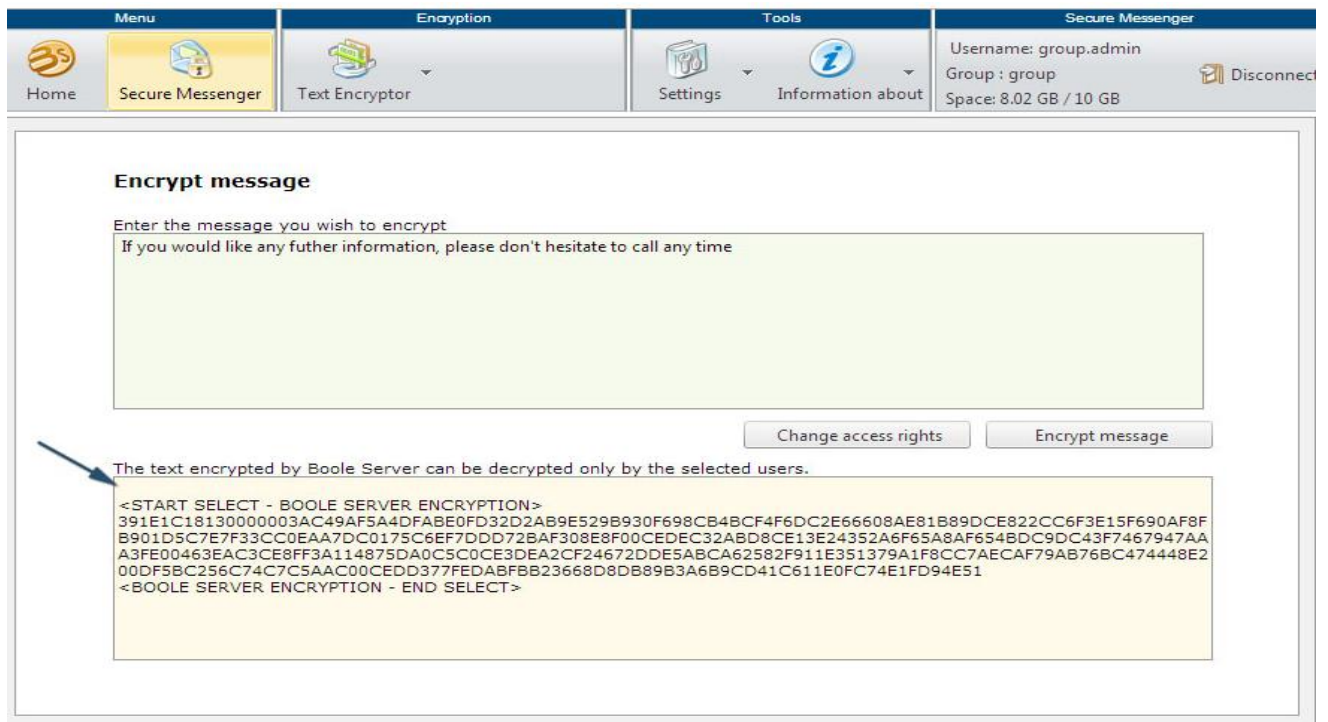


Figure 50: Encrypted Text

- The encrypted text can be deciphered by the profiles belonging to the same group of the profile who has performed the protection.
- The encrypted text can be copied and pasted in any kind of files: wherever it is, only the authorized profiles will be allowed to decrypt it using Boole Server Web Client or Boole Server Agent.

CHAPTER 4: BOOLE SERVER AGENT

4.1 Introduction:

Highest protection for company data the Boole Server Agent has been conceived to meet the needs for highest data protection, while ensuring further control and protection



Figure 51: Boole Server Agent

operations on company files to be added to those included in the Web Application.

Through the Agent, Boole Server users can:

- benefit from the Top Secret functionalities to block unauthorized screen capture activities
- work on files in protected mode
- encrypt files and folders in local
- share encrypted resources in local in a selective, granular and temporary manner
- create encrypted local disks
- synchronize a local disk with centralized resources accessible via Web Client

4.2 Offline Use of Local Protected File:

Boole Server Agent allows to access and use protected files or archives, without requiring an active connection to the server, by using an offline certificate previously generated.

In order to use a local protected file without connection to Boole Server:

- Right click on the protected file you wish to use in offline mode
- Click on Boole Server
- Select Open in offline mode

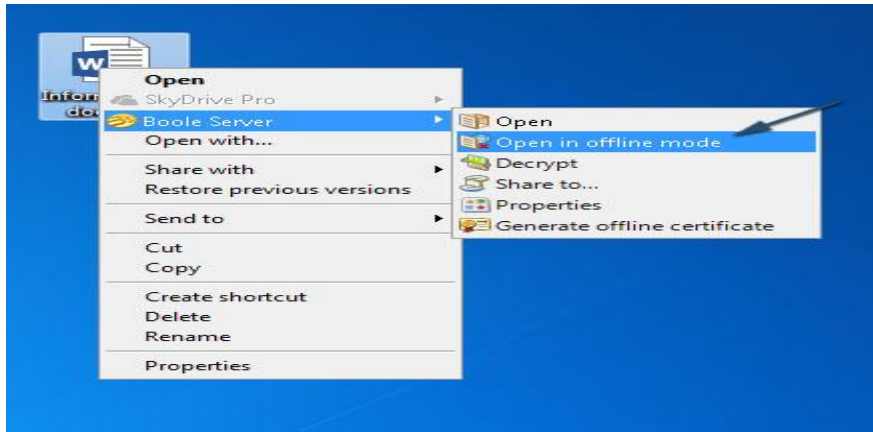


Figure 52: Opening File in Offline Mode

It is also possible to use a local file protected in offline mode, according to the following procedure:

- Double click on the protected file you want to use in offline mode.
- The login window appears.
- Enable the Open in offline mode option.
- Click on Login



Figure 53: Boole Server Agent - Offline Mode

According to the configured type of offline certificate, the following cases may occur:

- Case 1: access the protected file or archive through a unique and non-transferable offline certificate
- Case 2: access one or more protected files or archives through multiple offline certificate with password
- Case 3: access one or more protected files or archives through multiple offline certificate with password and recognition of one or more authorized PCs

4.2.1 CASE 1:

After logging in in offline mode:

- The Windows Browse window shows
- Select the previously generated offline certificate associated to the file you wish to use.
- If the offline certificate is correct, the file will open.

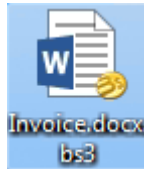


Figure 54: Encrypted World File



Figure 55: Encryption Invoice

ATTENTION!

The generated offline certificate can be used only if it is stored into the disk memory where saving has occurred: if the certificate is copied or moved into another disk, it will be impossible to use the certificate, even if the authorizations to use the protected file in offline mode on any PC are granted.

NOTE: Profiles can use the protected files in offline mode according to the received authorizations.

4.2.2 CASE 2:

After logging in in offline mode:

- The Windows Browse window shows
- Select the previously generated offline certificate associated to one or more files you wish to use.

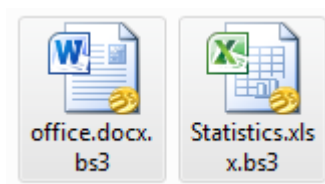


Figure 56: Encrypted World & Excel File

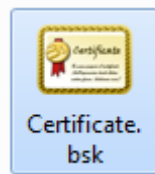


Figure 57: Encryption Certificate

- If the offline certificate is correct, the Offline Certificate Password window shows
- Enter the password associated to the file of the selected offline certificate
- Click Ok to confirm



Figure 58: Offline Certificate Password

- If the combination between offline certificate and password is correct, the file will open.

4.2.3 CASE 3:

After logging in in offline mode:

- The Windows Browse window shows
- Select the previously generated offline certificate associated to one or more files you wish to use

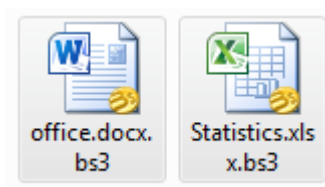


Figure 59: Encrypted Word & Excel File



Figure 60: Encryption Certificate

- If the offline certificate is correct, the Offline Certificate Password window shows
- Enter the password associated to the file of the selected offline certificate
- Click Ok to confirm

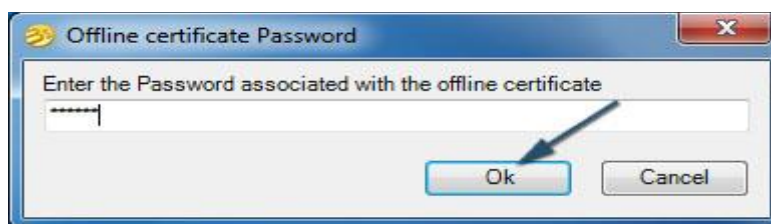


Figure 61: Offline Certificate Password

- If the combination between offline certificate and password is correct, and the PC from which the profile is accessing is listed among the authorized ones, the file will open.

4.3 Top Secret Protection:

Boole Server Agent does not only allow protecting and sharing files in local, encrypt texts and manage protected Archives, but it also allows using Top Secret protection on centralized files accessible through Web Client.

When sharing centralized file, it is possible to set, via Web Client, some protection options requiring Boole Server Agent installed on the computer of the profile to whom the files are made available.

If Boole Server Agent is not installed on the machine from which the profile who received the sharing is accessing the centralized files, the system will not authorize the access.

For instance:

- The profile A shares a centralized file in streaming mode.
- He enables the Anti-Capture protection.
- When the sharing recipient tries to access the file, a message will inform him that he is authorized to open the shared file only if he has Boole Server Agent.
- The profile will be able to download or confirm that he already has Boole Server Agent.

- If the profile does not have Boole Server Agent and decides not to download it from the link provided, the shared file cannot be accessed.

Boole Server Agent also allows automatically opening, editing or updated centralized files through Web Client.

Instead of downloading, editing and uploading a file again in Boole Server, if you have Boole Server Agent, you can open the file through the application associated to the file format, edit and save it: after saving it, Boole Server Agent will automatically upload the updated file and replace the previous version.

According to this procedure, the temporary file which has been downloaded to allow opening in local is a .bslink file: this format can be only opened through Boole Server Agent.

4.4 Mail Encryptor:

Dedicated plug-in integrated in Microsoft Outlook thanks to the dedicated plug-in, it is possible to integrate Boole Server protection mechanisms within Microsoft Outlook for a complete fusion with the most widely used e-mail client included in the Microsoft Office

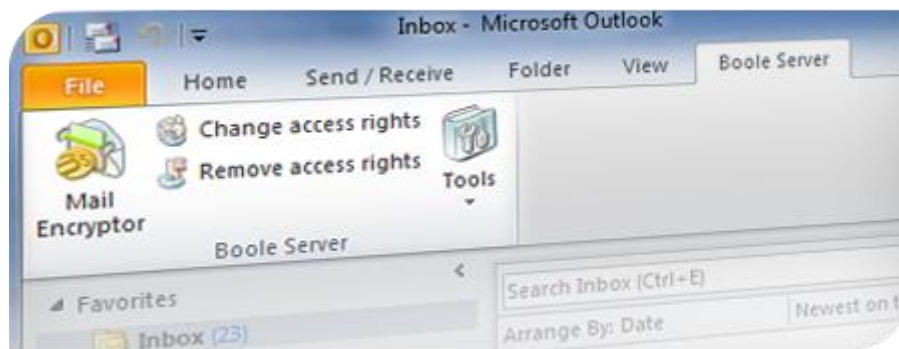


Figure 62: Mail Encryptor

suite.

Without leaving the Office application, it is possible to encrypt, send, and receive e-mails in the most secured and easy way. The possibility to set automatic protection rules also allows that e-mail messages are automatically encrypted every time the system detects a given word or information previously marked as "sensitive".

4.5 Boole Server App:

The free apps for iOS and Android the applications for iOS (iPad and iPhone) and Android are available for free in Apple App Store and Google Play Store. They allow to

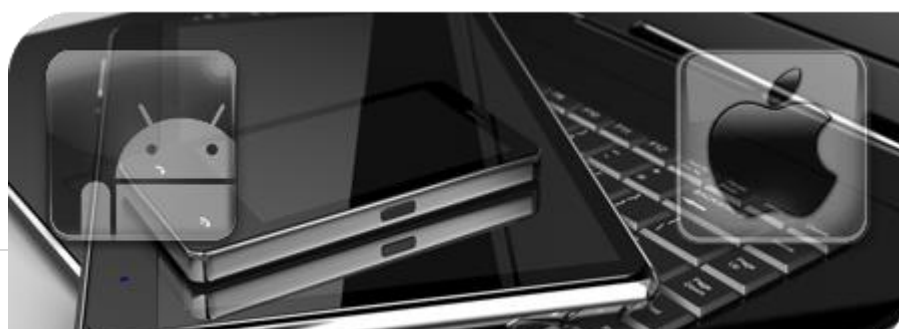


Figure 63: Boole Server App

access Boole Server protected files in total security and seamless mobility.

The Apps ensure highest protection to company files, wherever you are, without jeopardizing the security level: the innovating data-centric software guarantees total protection everywhere and on a great variety of file formats (Office, pdf, jpg, tif, png, mp3).

By using Boole server apps the user can take advantage with following functionalities:

- Accessing protected files
- Encrypting company data
- Sharing encrypted and protected files
- Monitoring activities performed on company files

And much more.

CHAPTER 5: CUSTOMER QUERIES

During my internship I provide the technical support to all the international customers. Following are some of the customer queries with my supported answers.

Question: 1)

Please see below customer queries.

Can we integrate Boole Server with PKI System?
Can Boole server support and verify Computer Certificate.
Can Boole Server support Smart Card.?

Answer: 1)

With the reference of your below email you can use the use the certificate with Boole server for the SSO(Single sign on)through any digital certificate and by using these certificate you can protect your red key as well.

Question: 2)

Boole Server does support multi-tenant structure?

Answer: 2)

Yes, but the DB (data base) is only one.

Question: 3)

After a while, the use of Boole Server to be canceled if desired (if it is uninstall) are experiencing problems related to data access does? (Data over Mail and file server).

Answer: 3)

If you decide to uninstall Boole server first of all you need to decrypt all the data otherwise you will not be able to access them.

Question: 4)

Offline data without internet access can be run from one place to do? (Mail protection and file protection).

Answer: 4)

Offline mode is available in Boole Server. The user can generate offline certificate in order to access the protected files when not connected to internet

Question: 5)

Boole supposed to be the domain of the server?

Answer: 5)

Boole Server can be joined to a domain or not. It depends if you need to integrate AD users or not.

Question: 6)

I believe Arabic Language is supported, so how do we go about it in order to install the language pack?

Answer: 6)

Actually no, The Arabic language is not currently supported by Boole Server. However, we can think of implementing this language against deal which justifies this implementation.

Question: 7)

Problem to set Expiry option for Offline Files

Answer: 7)

It is useless to set expiration on offline certificate because offline certificate work with Boole server time

Question: 8)

Can we migrate the current share folders to Boole Secure Vault with the similar permissions?

Answer: 8)

Suppose sheared network folder ([\\surname\sheared folder\](#)) you can transfer it by using remote protection rule or folder synchronization with the same permission

Question: 9)

How can we create templates for logs?

Answers: 9)

There is no possibility to create templates for logs.

Question: 10)

I've created the "Bank of Greece" folder but the option to share is not active. Hence, how can I share an entire folder?

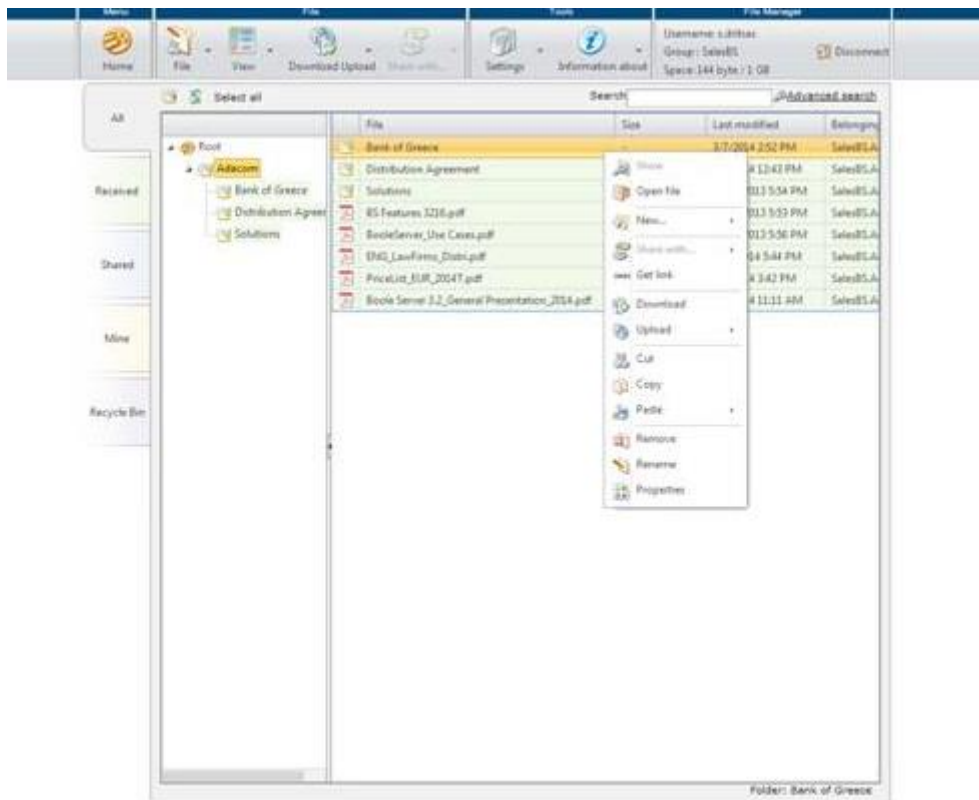


Figure 64: Sharing Folder

Answer: 10)

Because that user creates a folder inside a sheared folder to solve this issue you should have to create a folder outside the sheared folder or you need the permission of re-sharing from the owner of sheared folder.

Question: 11)

I'm testing MailEncryptor and when I try disable incoming mail protection, by Outlook, the message below is displayed when I click in **Tools/Options**:

- I changed the Registry with **CheckIncomingMail=0** and the message is the same.
- Can you help me? The people of the Monte Cristalina do not need crypt all received emails.

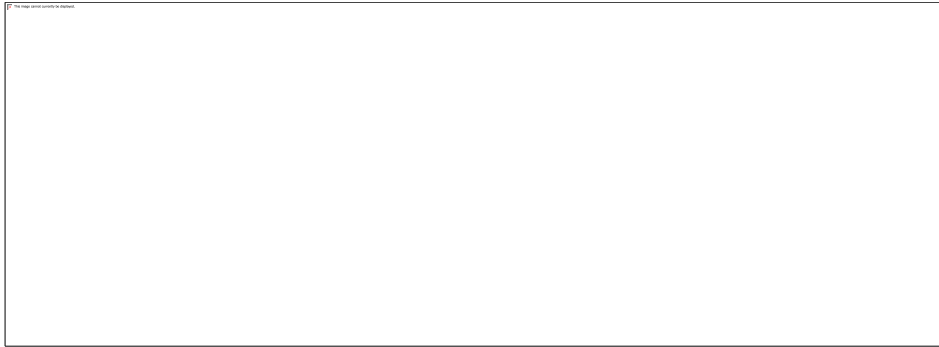
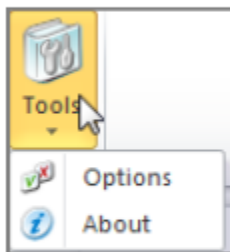


Figure 65: Mail Encryptor Warning Box

The steps below are not displayed:

Note: profiles with administrator privileges are necessary to use the advanced functionalities of the **Mail Encryptor** plug-in.



By selecting **Options**, a new window shows, through which it is possible to:

- block sending e-mails when the connection to Boole Server is not available
- disable protection for incoming e-mails

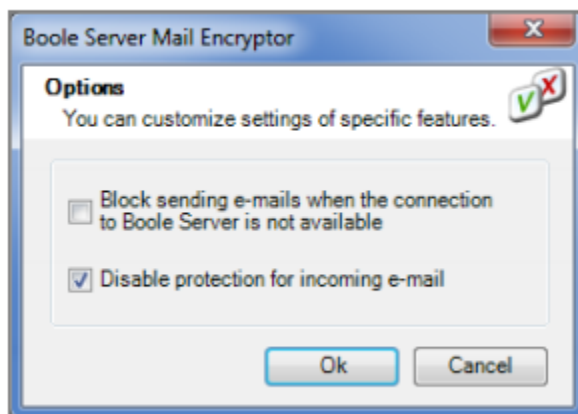


Figure 66: Mail Encryptor Custom Setting

About Sharing in Streaming, this feature do not appears when I try share a file and in the AIP settings is disabled;

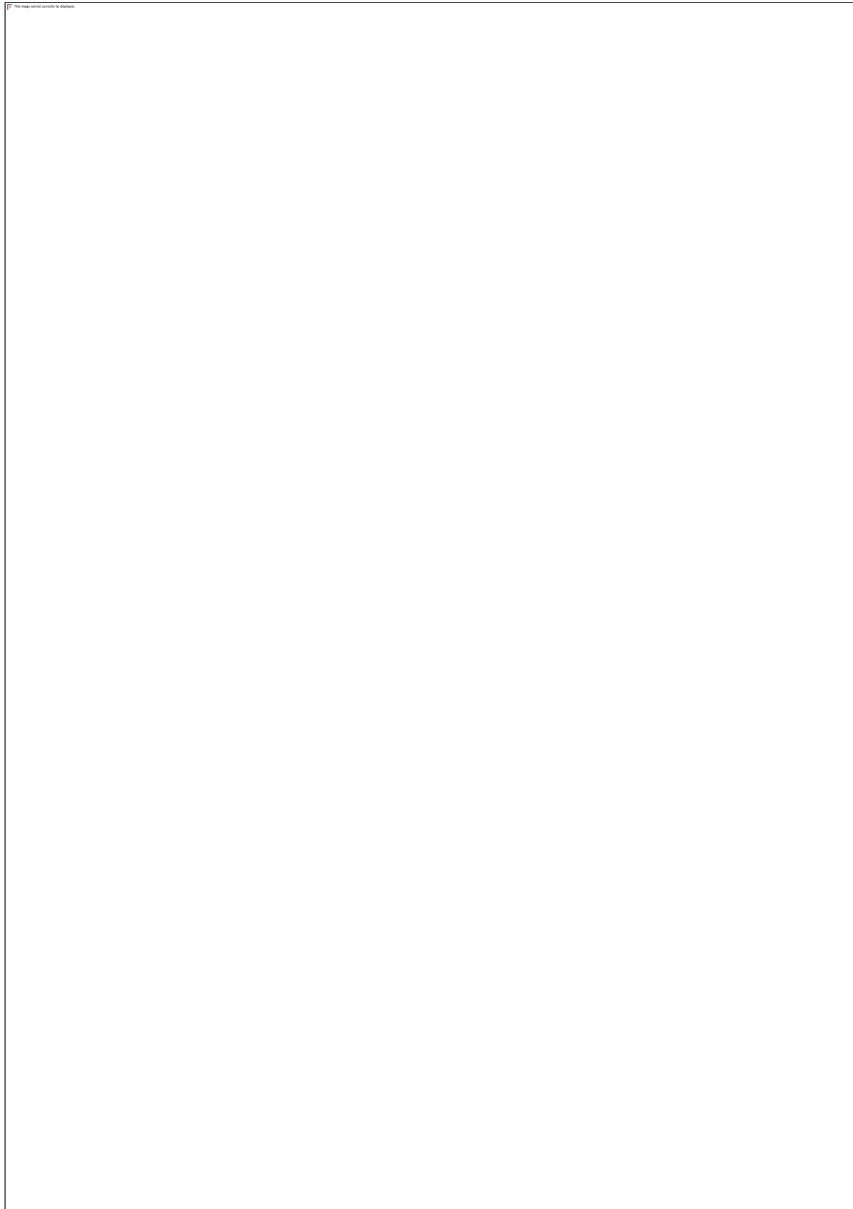


Figure 67: Protection Template Properties

With customized option



Figure 68: Custom Protect & Sharing Options

Answer: 11)

The answer of your 1st problem is that you should open your outlook as an administrator

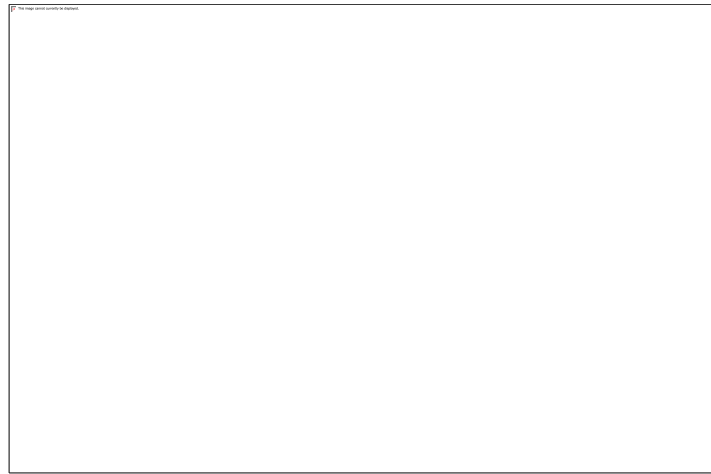


Figure 69: Mail Encryptor Setting Options

And related to 2nd problem I suggest you ,the streaming features is only for web client not for agent(local) so for visibility of this option you must have to choose only **web client** when you set the properties of protection templates on server side and please see the below figure for reference.

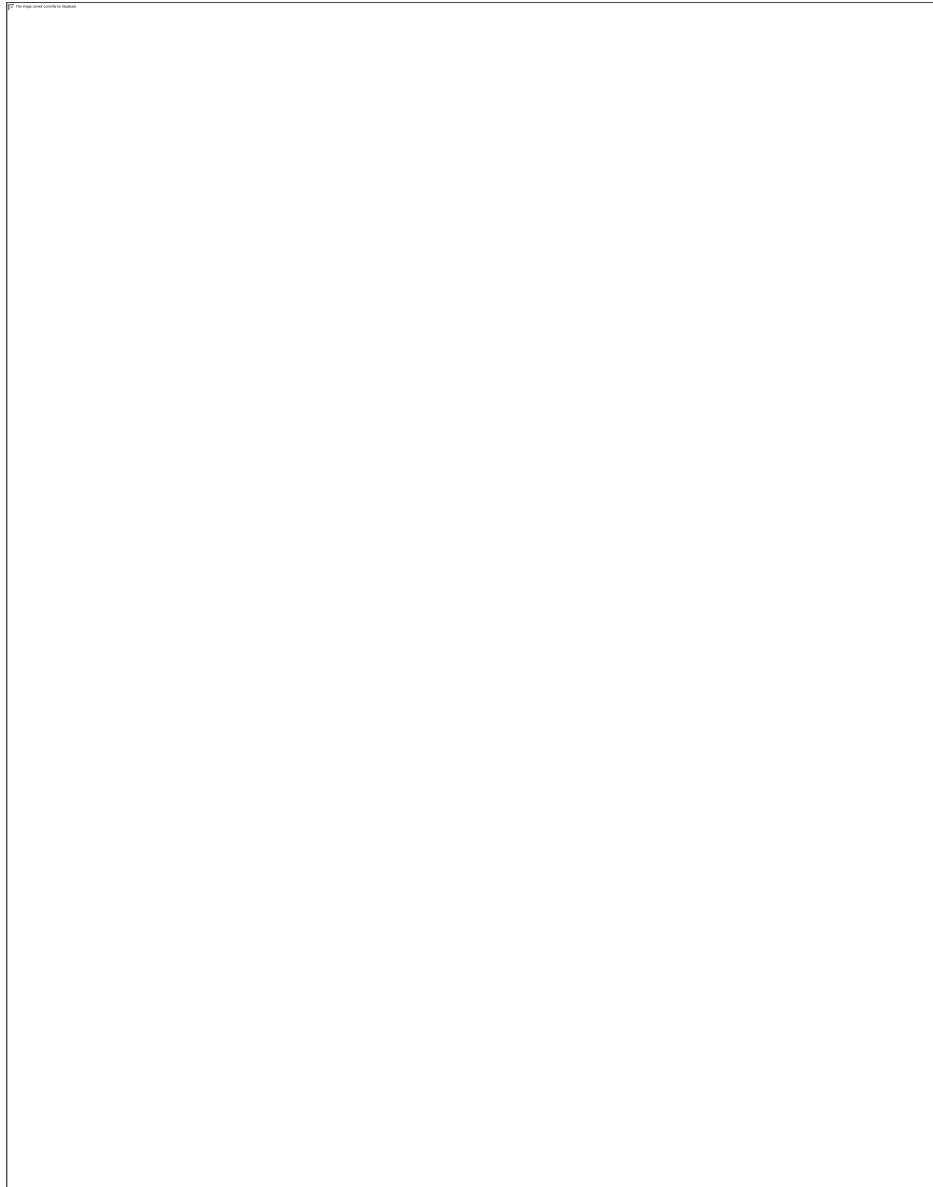


Figure 70: Protection Template Properties

Question: 12)

Customer wants that a specific group (AI) should be able to view the contents of the all Boole Server encrypted files being exchanged in and out of Company network (Be it on Local or via Web client. In short, everything encrypted by Boole Server).

Well said that, below I tried to find out how to achieve this stated requirement.

In Local Protection (For Shared Path or Folder on Users Machine): if this specific group (or group member) is made the admin of every Boole Server group then as per option available in local protection rule, we can assign the file ownership to the Group Admin and hence we achieve the requirement. Please let me know, if there is a better way to achieve this.

For manual method of encryption using Boole Agent or via Web client, we can have the specific group (AI) be the default sharing recipient (with file ownership privileges or unlimited protection) and then allow the end user to select the sharing recipients with which they actually intended to share the files with.

Can you confirm that in this way, we can achieve the requirement?

Answer: 12)

Related to 1st option it did not possible because every group admin has a different group name and it is not possible to create two or more Boole groups with same name and also one thing more the local and the remote protection rules valid only specified monitoring folders.

---- **Enabling the option Assign file ownership to the group administrator, the file on which** the rule will be applied will become property of the administrator of the group belonging to the profile to which the rule is being applied: in this way only the administrator will be authorized to change the protections automatically applied by the rule.

Yes we can do manually by using 2nd option but for this every groups and users should be complete group visibility of that specific group (AI) also every groups and users should be an availability of customize template or unlimited protection template.

Question: 13)

Is it possible customizing 'Boole Web Page' to add the concerned company's logo and remove all Boole Server logo/information?

Answer: 13)

Yes! Customization of the Web Client interface is possible. We can customize the interface with customer's logo and colors, and this usually goes at a cost depending on the size of this project.

Question: 14)

I'm a bit confused about the 'External Sharing Basket' Concept? (For e.g. if the customer has say 50 sharing's, so is it 50 active sharing's (concurrent) or once you share file/files with the external users then it is considered as 1 sharing consumed and so once 50 sharing's is fully consumed, the user cannot share anymore files/emails with the external users. So the user has to purchase the additional external sharing basket?) , please correct me if I'm wrong here.

Answer: 14)

It is actually right. Please find below further hints:

- If I share a file with 3 External Users, the counter of my basket goes down by 3: e.g. if my basket is 50, then it goes down to 47.
- if I share a file with an External Users and he opens it a given number of times, the counter of my basket goes down by 1, only the first time he opens the file.
- If I share a file with External User A and then with External User B, my counter goes down by 2.
- if I share a file with External User in yellow mode, then I edit protection level to red, my counter goes down by 1 at the moment of first sharing
- if I share a file with External User A with one week expiry, then – after expiry – I edit and extend expiry date, my counter goes down by 1 at the moment of first sharing

Question: 15)

Information about Boole Server and TITUS integration (If a document has been classified as Top Secret by the TITUS, then Boole Server can automatically encrypt this file with Top Secret Limitation or how does it work?) , could you please share the documents about the integration?

Answer: 15)

Thanks to the integration with Titus classification system, it is possible to apply the Boole Server protection and sharing levels, or to set automatic encryption rules to files according to Meta-tag classification by Titus in a nutshell, Boole Server detects Titus classified documents and applies the template having the same name. Documents about Boole Server and Titus are currently under drafting.

Question: 16)

Our current Boole server is installed on SATA disk in our VM Cluster, We are planning to move that to SAS Disk through Storage Vmotion. During this the VM Host won't be getting changed only the storage getting migrated to SAS storage pool.

Would like to know is this move will impact anything on license, is there any specific steps we need to know before moving the storage please confirm.

Answer: 16)

Please let me inform you that Boole Server detects all such movements as malicious operations (e.g. consider the case of hard-disk thefts).

Therefore, after moving Boole Server into another machine, you will be warned that the license will block in 30 days – as a consequence of the possibly “malicious” operation detected.

For this reason, before proceeding with the movement, please let me ask you to provide us with license number (first four digits are enough), in order for us to authorize centrally such movement.

As soon as your license will be authorized, please feel free to proceed with the movement. Bear in mind that, after the movement has been performed, you will need to refresh the license.

CHAPTER 6: BOOLE BOX

The only truly secure, sync and share solution.



Figure 71: Boole Box

Boole Box allows exchanging files containing sensitive information, in a simple and secure way on a cloud. A useful tool for those who need to consult balance sheets, financial data, strategies, confidential documents or any other information required to be kept confidential: not only does Boole Box allow to access information in a secure way, but it also allows to constantly monitoring all activities performed on the files which have been protected.

With Boole Box the data in the cloud is always accessible everywhere and always synched by the also protected with Boole Box you can be shared or protected. What is you need with Boole Box that makes more secure?

6.1 Private Keys:

Boole Box protected data with the highest military grade encryption 2048 bits when someone looking for an extra security, can use the private keys to encrypt and protect data with the private key only known to you. Unlike other cloud services whether is the single key known to the cloud provider.

6.2 Secure Mail:

Boole Box beyond protecting the files to protect the communication with Boole Box one can send emails in complete security, the only recipient can read it. one can do this feature still most popular email client like Gmail, Yahoo etc. As someone usually do.

6.3 Secure Sync:

Thanks to the cloud the files are updated and accessible everywhere from any device but with Boole Box they are also protected even if your PC or smart phone get stolen or damage or lost with Boole Box the documents stay safe and available the files on the device are encrypted and can't be read. And by using Boole secure sync one can set any one of these options

6.4 Synchronize:

- Synchronize and protect
- Protect with local encryption
- Easy And Secure Collaboration

Boole Box helps you and your colleagues to work together securely, you decide who has access what documents, you can should be able to write, edit, and leave notes & comments, the documents you collaboration are stay encrypted and secure.

6.5 Most Important Features of Boole Box:

6.5.1 File Manager:

Here is general picture of home page of Boole Box

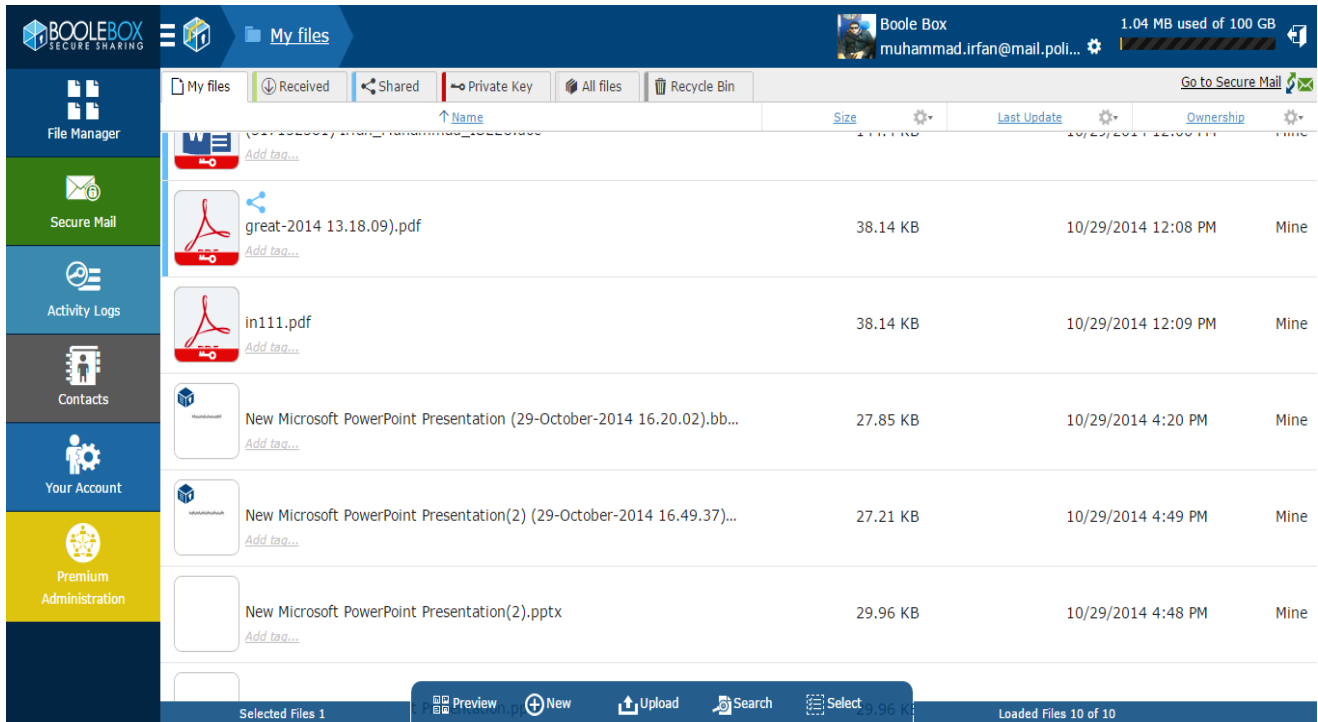


Figure 72: Boole Box Panel

6.5.2 Default Sharing Security Limitation:

Sharing files or folders by using default level of security limitation options

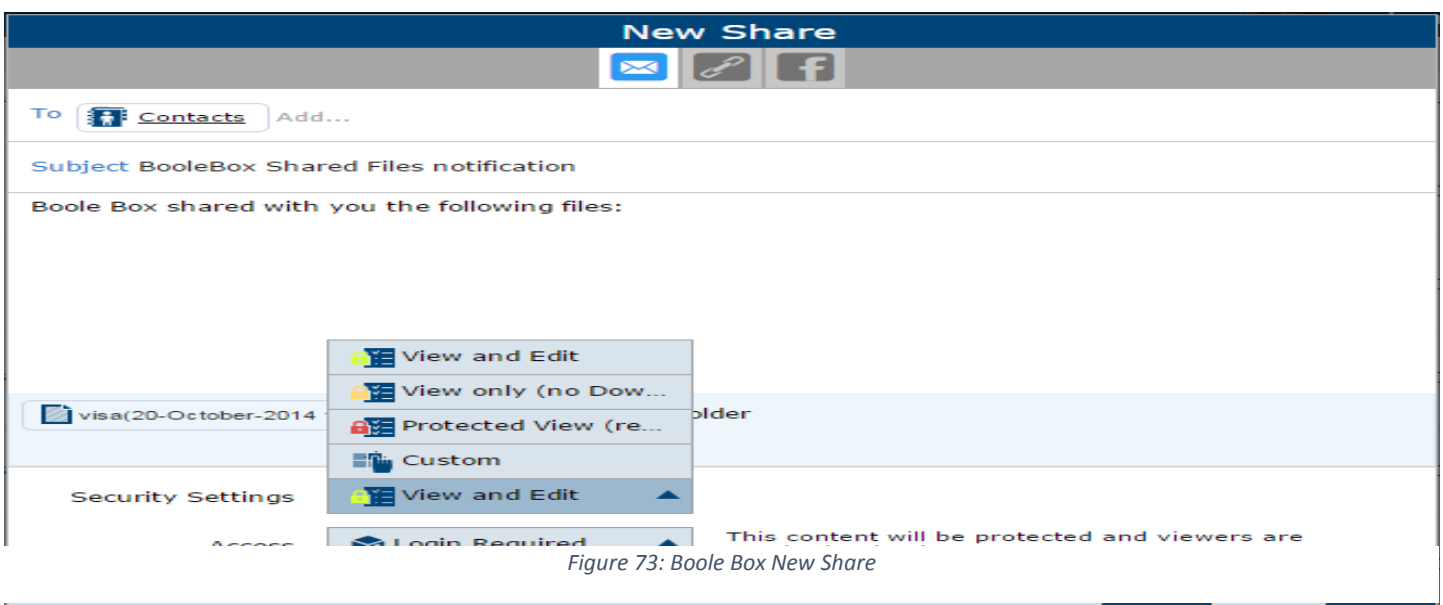
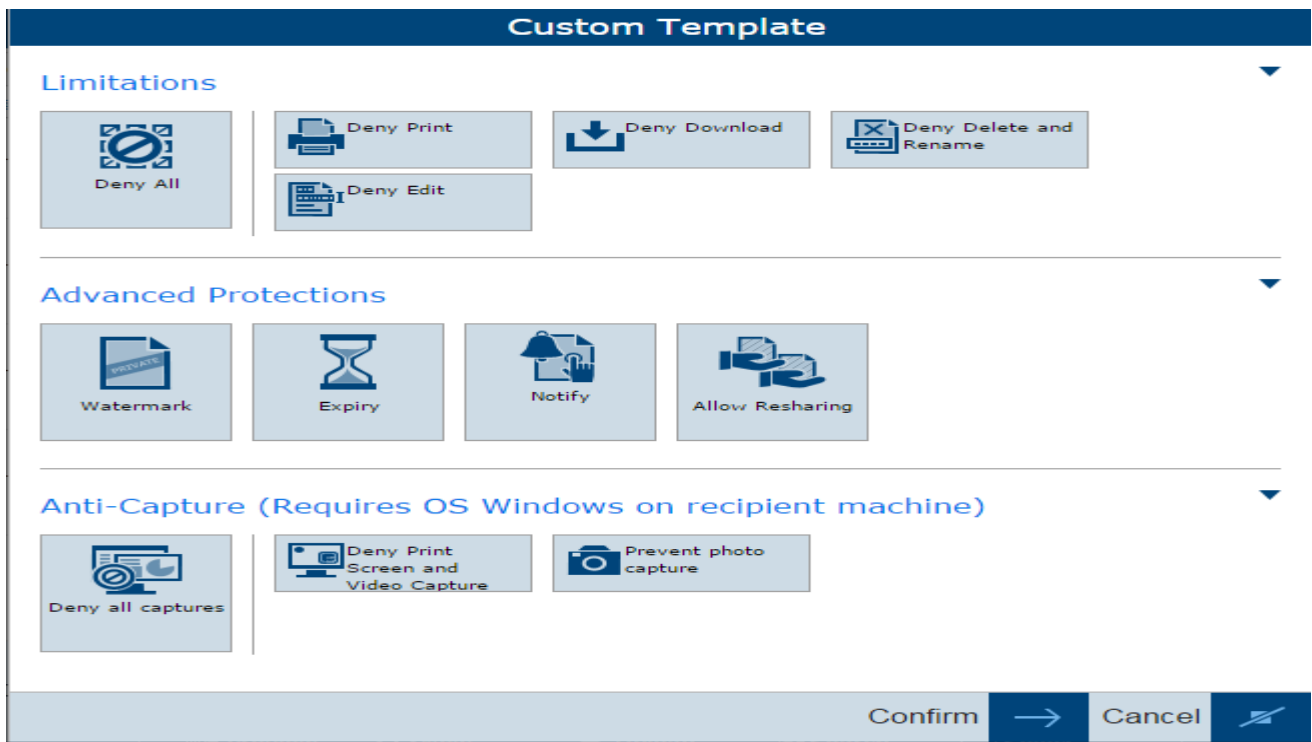


Figure 73: Boole Box New Share

6.5.3 Custom Sharing Security Limitation:



Sharing files or folder by using customize security setting options

6.5.4 Activity Logs:

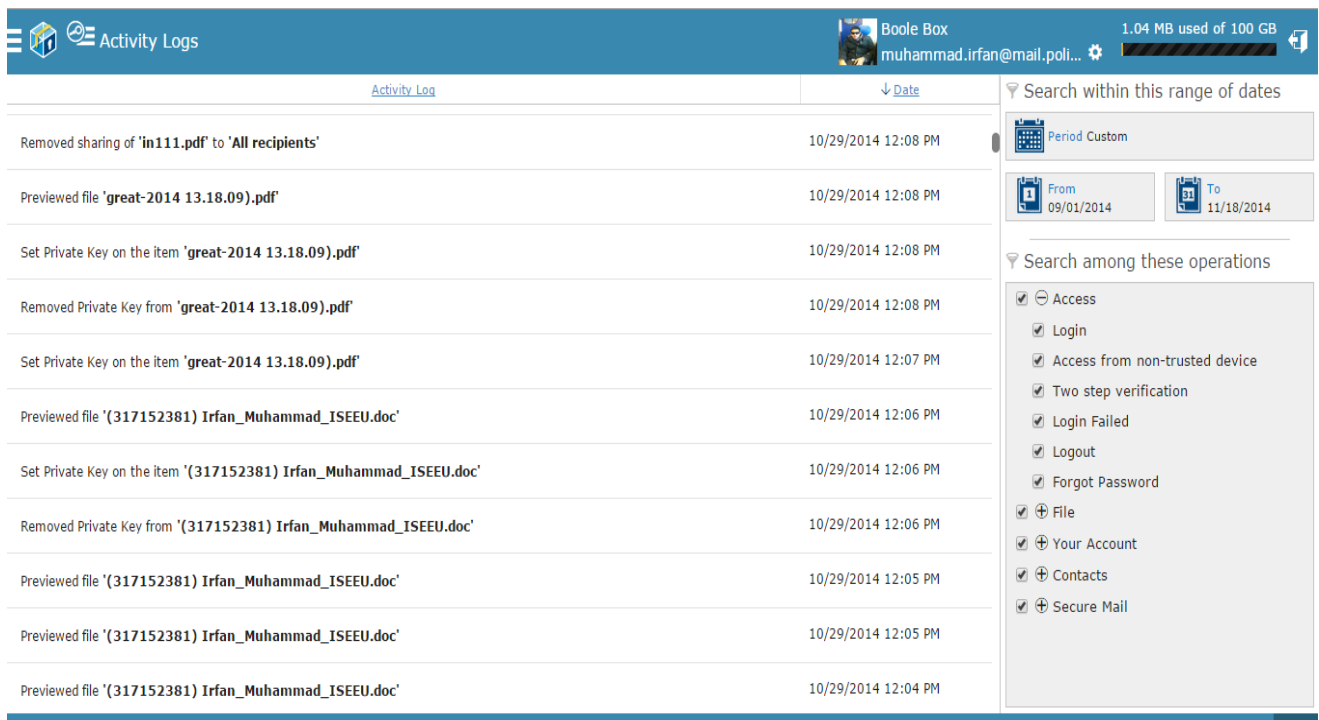


Figure 75: Boole Box Activity Log

Figure 74: Boole Box Custom Templates

Activity Log of type operation performed with Boole Box

6.5.5 Account Management Setting:

In the account management area one can take advantage of the following features also

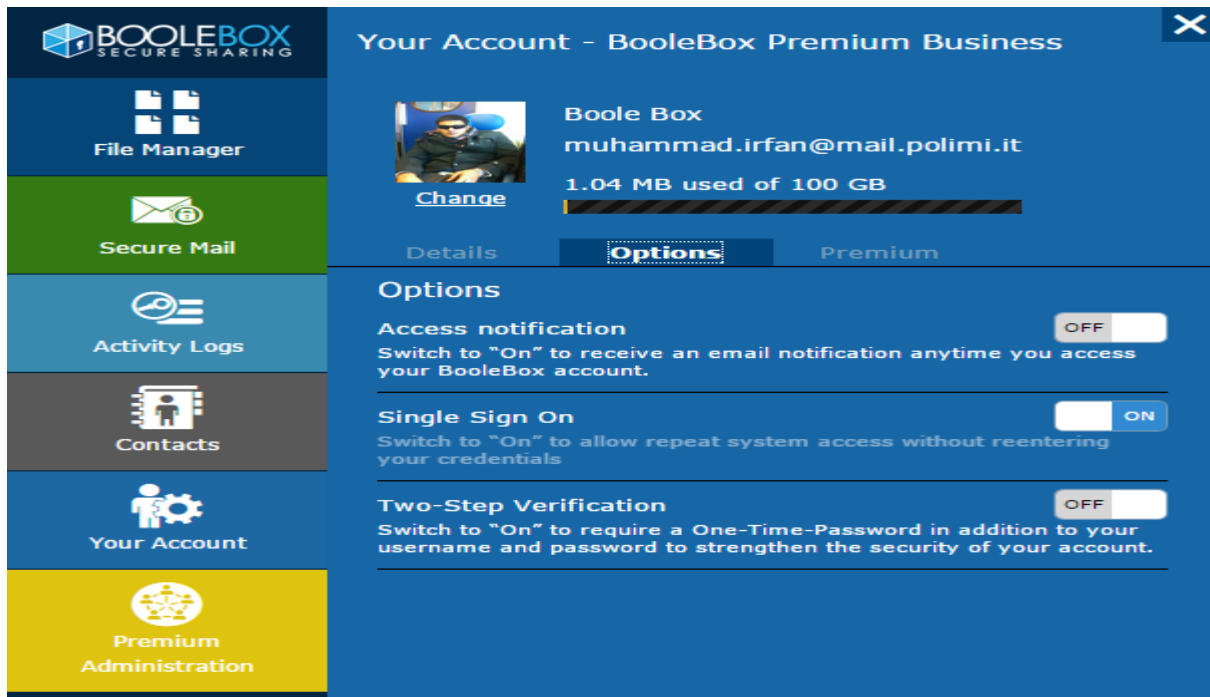


Figure 76: Boole Box Your Account

6.5.6 Access from Non-Trusted Devices:

Access from non-trusted devices for more security

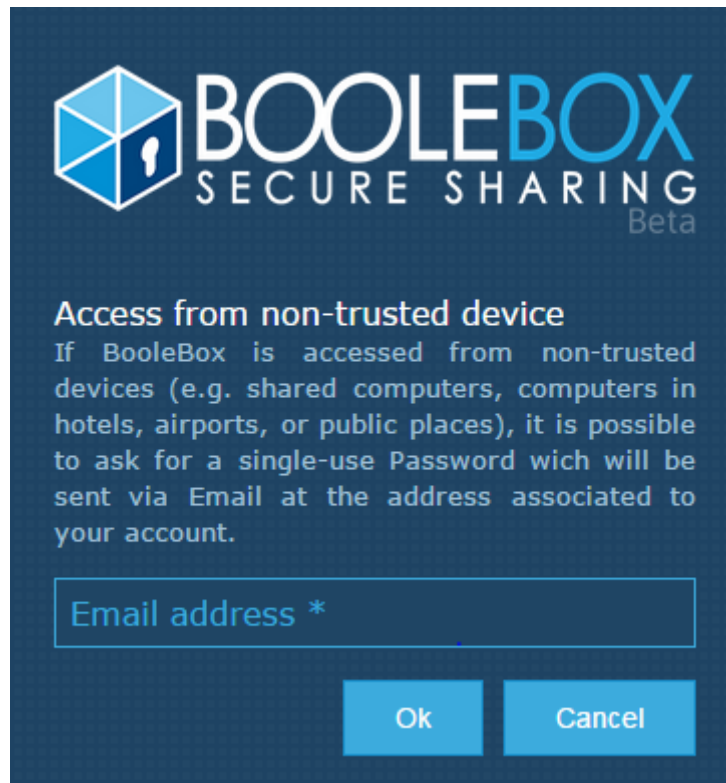


Figure 77: Boole Box Login

6.6 Comparison between Different Cloud Based Services:

Here is the brief picture between Boole box and other cloud based services just like drop box, Google drive, and one drive

					
Security					
Secure Sockets Layer (SSL) and AES-256 bit encryption	✓	✓	✓	✓	✓
Private Key to protect documents and folders	✓	✗	✗	✗	✗
Local File encryption during sync	✓	✗	✗	✗	✗
Automatic Saving of edited file even if encrypted	✓	✗	✗	✗	✗
Native Email Encryption (Secure Mail)	✓	✗	✗	✗	✗
Native Email Encryption (Secure Mail)	✓	✗	✗	✗	✗
Access notification on every login	✓	✗	✗	✗	✗
Screen capture block	✓	✗	✗	✗	✗
Encryption of Emails stored and sent by Gmail Account	✓	✗	✗	✗	✗
Sharing					
Share File and Folder with permissions	✓	✓	✗	✓	✓
Share File and Folder encrypted with Private Key	✓	✗	✗	✗	✗
Share Documents with Dynamic Watermark (Recipient data)	✓	✗	✗	✗	✗
Deny or Allow resharing of folders	✓	✓	✓	✗	✓
Share with short time frames(Minutes, Hours...)	✓	✗	✗	✗	✗
Realtime activities notification to all the recipient of a shared file	✓	✗	✗	✗	✗
Managing Files					
Preview File Microsoft Projects and Microsoft Visio in Browser	✓	✗	✗	✗	✗
File and Folder classification	✓	✓	✗	✗	✓
Previous versions of file can be viewed and restored	✓	✓	✓	✓	✓
Activity logs on single file or folder	✓	✓	✓	✗	✓
Collaboration					
Create and edit documents in program	✓	✓	✗	✓	✓
Create and share Annotations in document	✓	✗	✗	✗	✓
Simultaneous collaboration	✓	✓	✗	✓	✓
Plug-In					
Microsoft Outlook for Windows Plugin	✓	✗	✗	✗	✓

Figure 78: Boole Box Comparison with Others

6.7 Boole Box Software Testing Bugs:

List of founded bugs during testing of BOOLE BOX on windows operating system, android devices and IOS devices

- When shear files with expiry and anti-capture option's then the expiry not works.
- One time password request is not working properly.
- Empty bin messenger is not recorded in activity log area.
- Opening and download Of PK protected files is problematic on android devices the system gives an error the PK is not correct.

- When I apply PK from PC and iPhone I see a continuously processing until I refresh the page.
- I am not able to open .bbx local protected file's
- Synchronization problem when I am trying to working on bigger size of files
- Renaming issue when I rename from web client the system gives a warning "access denied" and on the other hand when I rename from local sync folder the web client file\folder is not updated according to new name.
- When I edit any PK protected file from local sync folder then after editing the PK automatically removed.
- Full water mark is not working.
- when I using protected view template during sharing and the recipient can't open or preview it on iPhone and the recipient also facing problem to open it on pc and when he trying to open it on pc he receive this type of message{"content": "Access to the path'C:\\inetpub\\wwwroot\\App_Data\\4278782742329448314' is denied.

 at System.IO.__Error.WinIOError(Int32 errorCode, String maybeFullPath)\u00d\u00a at System.IO.Directory.InternalCreateDirectory(String fullPath, String path, Object dirSecurityObj, Boolean checkHost)\u00d\u00a at System.IO.Directory.InternalCreateDirectoryHelper(String path, Boolean checkHost)\u00d\u00a at WebClient.FileManager.DownloadProtectedDocument(Params _oParam, CacheData _oData, IDSettingsData _oSettings, Int64 _iTokenID, String _szUrl) in p:\\Boole.WebCommunicator\\Boole4\\BS\\FileManager.aspx.cs:line 3602\u00d\u00a at WebClient.FileManager.Page_Load(Object sender, EventArgs e) in p:\\Boole.WebCommunicator\\Boole4\\BS\\FileManager.aspx.cs:line 10327\u00d\u00a at System.Web.UI.Control.LoadRecursive()\u00d\u00a at System.Web.UI.Page.ProcessRequestMain(Boolean includeStagesBeforeAsyncPoint, Boolean includeStagesAfterAsyncPoint)","type":3}"
- Facing problem to delete multiple files from recycle bin from iPhone.
- Facing problem to restore of multiple files from recycle bin from iPhone.
- During sharing from iPhone and when I use custom template then here I am facing problem to select deny print, deny download, deny delete and rename, deny edit and anti-capture option.
- PK protected files are not download both from sender and receiver side on IOS and Android devices.
- When I shear files with expiry and anti-capture option's then the expiry don't works.
- To upload very bigger size of file just like 4GB multimedia files on Boole box web client then I am facing problem to upload and when upload reaches to 4% then It automatically goes back to 1% and it repeat again and again I make this test on different browser and on different profiles from PC but at the end I get the same result.

- When I try to open received files (with anti-capture protection options) then the system gives an error "the exe is not completely downloaded and could be dangerous" I am facing this problem in chrome browser.
- When I try to open get link or FB sharing on mobile devices I can open it but the open page is blank.
- I am facing problem to upload from iPhone (sometime it works and other time it's not work).
- I am not able to open PK protected files on both sender and receiver side with IOS and Android.
- I am not able to download RK protected files on both sender and receiver side with IOS and android.
- I always see the print option after applying deny print function on PK protected files and without PK protected files both on IOS and Android devices.
- Facing problem to open PDF from PC as well as from mobile devices in case of FB Sharing but and facing problem of re-sharing from PC and mobile devices
- I don't see any option to select all the files or folders in secure messenger in case of Android.
- In android facing problem to set date expiry because OK button is not working.

Reference

- Boole Server
via Rutilia 10/8
20141 Milan - ITALY
Phone: +39 02 8738 3213
E-mail: info@booleserver.com
Skype: booleserver
Web: <http://www.booleserver.com/>

ABBREVIAZIONI

IT	Information Technology
SQL	Structured Query Language
IIS	Internet Information Services
AD	Active Directory
SMTP	Simple Mail Transfer Protocol
HA	High Availability
SMBs	Service Message Box
Gmail	Google Mail
PC	Personal Computer
DMZ	Decentralized Machine Zone
SSL	Secure Sockets Layer
IP	Internet Protocol
LAN	Local Area Network
CA	Certificate Authority
HTTP	Hyper Text Transfer Protocol
NICs	Network Interface Cards
DHCP	Dynamic Host Configuration Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
iOS	Iphone Operating System
PKI	Public Key Infrastructure
SSO	Single Sign On
DB	Data Base
AIP	Advance Identity Platform
SATA	Serial Advanced Technology Attachment
SAS	Single Attach Station
VM	Virtual Machine
PK	Private Key
FB	Facebook