



# **INSTALLATION GUIDE**

**for wwSafe™ from WWPass®**

**Version 2.0**

September 2014

# TABLE OF CONTENTS

Chapter 1 — Welcome .....	4
Documentation for wwSafe .....	4
Need Assistance? .....	5
Report a Problem from Dashboard .....	5
Chapter 2 — wwSafe Components.....	6
Chapter 3 — wwSafe Requirements .....	7
Checklist: What you need in your system .....	8
Checklist: What you need from WWPass .....	9
Requirements for the wwSafe Server and Management Utility .....	11
Requirements for the wwSafe Client.....	13
Requirements for wwSafe Users .....	14
Chapter 4 — Smart Start for Installation .....	15
Chapter 5 — Set Up to Use Active Directory .....	17
1. Download file for wwSafe schema .....	18
2. Apply wwSafe schema to Active Directory.....	18
3. Obtain SSL certificate .....	18
4. Create an account for the wwSafe service user .....	18
5. Create an account for the first Security Administrator .....	18
Chapter 6 — Prepare for Server Installation.....	19
1. Perform setup for the first wwSafe Security Administrator .....	20
2. Download server installation and configuration scripts .....	20
3. Obtain a service provider certificate signed by WWPass .....	21
4. Configuration backup and recovery .....	21
Chapter 7 — Install the Server.....	23
Install the wwSafe server automatically .....	24
Install the wwSafe server manually.....	25
Chapter 8 — Configure the Server .....	27
1. Run the configuration script .....	28
Restart the configuration script .....	28
2. Begin or continue a configuration .....	29
3. Configure service provider parameters.....	29
4. Configure Active Directory parameters .....	31
5. Configure network and TLS parameters .....	32
6. Create the server encryption key .....	35
7. Set up debug logging .....	36
8. Save the configuration and start the server .....	36
Chapter 9 — Create Administrative Groups .....	37

Overview .....	38
Register Security Administrator and create groups from Ubuntu .....	38
Register Security Administrator and create groups from the client.....	38
Register the PassKey of the first Security Administrator .....	38
Create administrative groups from the client .....	40
Chapter 10 — Install the Client .....	44
Overview .....	45
Install the Client on Individual Computers.....	45
Chapter 11 — Set Up for PassKey Login .....	46
Overview .....	47
When can users log into wwSafe? .....	47
How to set up for PassKey login .....	47
How to connect a PassKey and log in .....	48
Chapter 12 — Assign Administrative Roles .....	49
Overview .....	50
How to assign administrative roles .....	50
Chapter 13 — Set up Storage and Groups .....	53

## CHAPTER 1 — WELCOME

This documentation covers how to install and configure wwSafe™, a client/server application from WWPass® that lets users securely store and share files in the cloud.

It also provides a Smart Start for setting up storage and creating groups for sharing files in wwSafe. Complete information on setting up and managing wwSafe is available in Management Utility online [help](#).

Installation and configuration information is provided for the system administrators and IT managers who install and configure the wwSafe server, Management Utility, and client.

Setup information for storage and groups is provided for wwSafe Security Administrators, IT Managers and Domain Administrators. Users with these roles are created at the end of the configuration process.

### Documentation for wwSafe

Documentation	What It Covers	Who It's For	Where to Find It
Installation guide	Installation, configuration and setup overview for wwSafe.	<ul style="list-style-type: none"><li>• IT managers</li><li>• System administrators</li><li>• wwSafe Security Administrators</li><li>• wwSafe IT Managers</li></ul>	Sales at WWPass. (+1-888-997-2770)
Help for wwSafe Management Utility	Setting up and managing wwSafe with the wwSafe Management utility.	<ul style="list-style-type: none"><li>• wwSafe Security Administrators</li><li>• wwSafe IT Managers</li><li>• Domain Administrators</li></ul>	Click Help <a href="#">link</a> at top of Management Utility interface.
Help for wwSafe client	Using the wwSafe client and setup performed from the client.	<ul style="list-style-type: none"><li>• wwSafe end users</li><li>• wwSafe Security Administrators</li><li>• wwSafe IT Managers</li><li>• Domain Administrators</li></ul>	Click User Guide <a href="#">link</a> at top of client interface.

## Need Assistance?

If you encounter a problem with wwSafe or have a question, you can contact WWPass Product Support:

Phone 1-888-WWPASS0 (+1-888-997-2770)

Email [support@wwpass.com](mailto:support@wwpass.com)

Online [Support form](#)


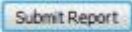
## Report a Problem from Dashboard

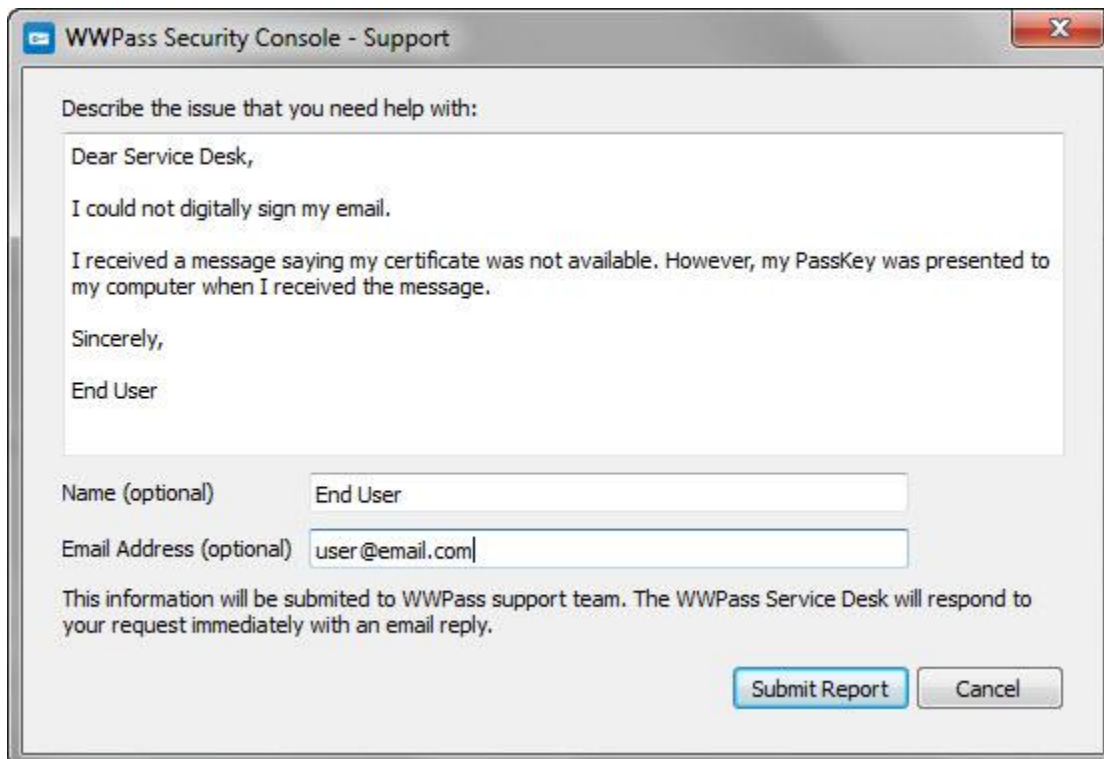
An easy way to report a problem is to email Product Support directly from the WWPass Dashboard. This is installed on wwSafe client computers as part of the WWPass Security Pack, the software pack needed to activate and authenticate with a PassKey™ or PassKey for Mobile from WWPass.

All WWPass logs available on the wwSafe client computer are automatically attached to the email. Logs contain information that can help Product Support troubleshoot problems.

Logs are located in Users\username and ProgramData. They should not be changed before they are sent to Product Support.

## To report a problem from Dashboard

1. Click the mail button  in the upper-right corner of the Dashboard.
2. In the Support window that opens, type a description of the problem you need help with. You can also type a question.
3. Enter the email address Product Support should reply to. Also enter your name.
4. Click  to email your report along with logs on the wwSafe client computer.



**WWPass Security Console - Support**

Describe the issue that you need help with:

Dear Service Desk,

I could not digitally sign my email.

I received a message saying my certificate was not available. However, my PassKey was presented to my computer when I received the message.

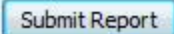
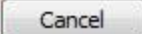
Sincerely,

End User

Name (optional)

Email Address (optional)

This information will be submitted to WWPass support team. The WWPass Service Desk will respond to your request immediately with an email reply.

## CHAPTER 2 — WWSAFE COMPONENTS

---

wwSafe includes the following components:

- **wwSafe Client**—This is a Windows-based application that provides users with an easy-to-use intuitive interface for storing and sharing files. Each user's PassKey/PassKey for Mobile from WWPass ensures that only they can access their files. The client is installed with a setup wizard. See [Install the wwSafe client](#).
- **wwSafe Server**—This runs on an Ubuntu computer or virtual machine (12.04 Precise Pangolin is required). The wwSafe server communicates with WWPass, Azure/Amazon cloud storage, and Active Directory. wwSafe clients connect to the server to authenticate users, run commands for storing and sharing files, and access file data in Azure or Amazon.
- **wwSafe Management Utility**—This resides on the wwSafe server host and is run via a web browser. The Management Utility provides administrative users with a centralized tool for managing wwSafe users and storage:
  - wwSafe IT Managers can use the Management Utility to create Cabinets for storing files and allocate Azure/Amazon storage space to Cabinets.
  - wwSafe Security Administrators can use the Management Utility to view lists of users and their Cabinets, check users' online status, delete users, and create groups for sharing files and assigning administrative roles.
  - wwSafe Domain Administrators can use the MU to manage domains they administrate, add new users and delete existing ones from their domains.

Both types of users can use the Management Utility to audit administrative operations and view statistics that indicate current usage and load for a wwSafe server. Each administrative user's PassKey or Passkey for Mobile is used for secure access to the Management Utility.

The Management Utility is installed along with the wwSafe server.

## CHAPTER 3 — WWSAFE REQUIREMENTS

---

This chapter covers what's needed to run the wwSafe client, server, and Management Utility. Checklists provide quick overviews of all components needed. Requirements tables provide detailed information on each component.

### Topics In This Chapter

---

- [Checklist: What you need in your system](#)
- [Checklist: What you need from WWPass](#)
- [Requirements for the wwSafe Server and Management Utility](#)
- [Requirements for the wwSafe Client](#)
- [Requirements for wwSafe Users](#)



## Checklist: What you need in your system

This checklist lets you see at a glance what you need in your system to run the wwSafe client, server, and Management Utility. The components you need from WWPass are covered in the next checklist.

For detailed information, see requirements for the [server](#), [client](#), and [users](#).

### Needed for wwSafe server and Management Utility

- ✓ Computer with Linux Ubuntu Server 12.04.3 LTS (Precise Pangolin)
- ✓ Microsoft Azure cloud storage (information on integrating Azure with wwSafe is covered under [Create Storage Accounts](#) in Management Utility help) or Amazon S3 Cloud.
- ✓ Microsoft Active Directory 2000, 2003 or 2008 for user account repository (**This requirement is additional if wwSafe is installed with local user directory**).
- ✓ Web browser to run Management Utility and authenticate with PassKey or Passkey for Mobile
- ✓ TLS server certificate for the wwSafe service name, for example, wwsafe.mycompany.com (can be created by wwSafe configuration script)

### Needed for wwSafe client

- ✓ Computer with Microsoft Windows 7 or 8.1
- ✓ Microsoft .NET 4.5
- ✓ Web browser to authenticate with PassKey or a Mobile Passkey

### Needed for wwSafe users (administrative and non-administrative)

- ✓ Account in Active Directory

If someone outside your enterprise will connect to your wwSafe server, add an account for that user to Active Directory.

You might want to include -companyname in their user name to identify them as an external user in the wwSafe client and Management Utility.

### Users needed for wwSafe server installation and configuration

- ✓ Active directory user with administrator permissions
- ✓ Ubuntu user with root privileges



## Checklist: What you need from WWPass

This checklist lets you see at a glance what you need from WWPass to run wwSafe. For detailed information, see requirements for the [server](#), [client](#), and [users](#).

WWPass components can be obtained from Sales at WWPass: 1-888-997-2771

### Needed from WWPass

- ✓ Credentials for downloading software from WWPass  
These are needed to download and install wwSafe software
- ✓ WWPass KeySet or Mobile PassKey for authentication into wwSafe  
Required for each administrative and non-administrative user
- ✓ WWPass Security Pack  
Required on each Windows computer where the client and Management Utility will run (provides software needed to activate a KeySet or a Mobile PassKey and use the PassKey with wwSafe)
- ✓ wwSafe Client  
Installed on Windows computer of each administrative and non-administrative user with setup wizard from WWPass
- ✓ wwSafe server and Management Utility  
Installed and configured on an Ubuntu computer with the following from WWPass:
  - Installation script—wwsafe-bootstrap.sh or wwSafe virtual appliance
  - Configuration script—wwsafe\_configure.py (installed by installation script)
- ✓ File to apply wwSafe schema to Active Directory  
The wwsafe.ldif file is installed on the Windows server for Active Directory
- ✓ Service provider certificate signed by WWPass  
Stored on Ubuntu server host to authenticate the wwSafe server with WWPass. Basic steps to obtain are:
  1. Contact Sales at WWPass and ask for a service provider name and ID
  2. Generate Private Key without a password on the server
  3. Use the service provider name and ID obtained to generate a certificate signing request (CSR)
  4. Send certificate signing request to WWPass
  5. When WWPass returns the signed certificate and WWPass CA certificate, store both on the server host

For detailed steps, see [Obtain a service provider key and certificate.](#)

## Requirements for the wwSafe Server and Management Utility

Requirement	Details
Ubuntu operating system	<p>Computer or virtual machine with Linux Ubuntu Server 12.04.3 LTS (Precise Pangolin). Needed as server host for wwSafe server and Management Utility. A user with root privileges for Ubuntu is needed to install and configure the server.</p> <p>Minimum requirements for the computer:</p> <ul style="list-style-type: none"> <li>• Storage—10 MB (for software and logs)</li> <li>• Memory—2 GB RAM</li> <li>• CPU—One 32-bit or 64-bit Intel or AMD processor</li> <li>• Outbound Internet access</li> <li>• Configured network adapter and known IP address or hostname for the both external (Internet) and internal (enterprise) networks</li> </ul> <p><b>Note:</b> A web server is installed on Ubuntu by the wwSafe installation script.</p>
Cloud storage	<p>Microsoft Windows Azure/Amazon S3 Cloud storage.</p> <p>Required for storing the file data users add to wwSafe. One Azure/Amazon account is used for all wwSafe users. Microsoft Windows Azure/Amazon S3 SDK for Python is installed by the wwSafe server installation script. Click <a href="#">here</a> to see Azure documentation. <b>Note:</b> How much storage is needed depends on how many users store files in wwSafe and the size of the files they store.</p>
Directory service	<p>Microsoft Windows Server 2000, 2000 3 or 2008 with Active Directory (<b>This requirement is additional if wwSafe is installed with local user directory</b>).</p> <p>Required for user account provisioning. User accounts are mapped from Active Directory to wwSafe. Each user has a unique identifier (PUID) that is associated with their Active Directory account and the PassKey they use to authenticate with wwSafe.</p> <p>A fully qualified domain name (“DN=mydomain,DN=com”) and Active Directory administrator are needed for installation and configuration of the wwSafe server.</p> <p><b>Note:</b> If you want to restrict wwSafe access to an Organizational Unit in Active Directory, you can do this during configuration by specifying the name of that unit along with the Active Directory domain name (“CN=Users,DN=mydomain,DN=com”).</p>
Service provider key and certificate	<p>A service provider key and certificate from WWPASS.</p> <p>The certificate is needed to authenticate the wwSafe server with WWPASS. See <a href="#">Obtain a service provider key and certificate</a>.</p>
TLS Certificate	<p>An TLS (Transport Layer Security) server certificate and key pair TLS for the wwSafe service name, for example, wwsafe.mycompany.com.</p> <p>Required to secure incoming connections for the wwSafe server and Management Utility web server. If you do not have a TLS certificate, the server configuration script can create a self-signed certificate. See <a href="#">Configure network and TLS parameters</a>.</p>

Requirement	Details
<b>Web browser</b>	<p>A browser is needed to run the wwSafe Management Utility, authenticate into wwSafe with a PassKey or a Mobile PassKey, and activate the PassKey.</p> <p>Supported browsers are:</p> <ul style="list-style-type: none"><li>• Microsoft Internet Explorer 9, 10 and 11 (32-bit and 64-bit)</li><li>• Mozilla Firefox 14 to current version</li><li>• Google Chrome 20 through 34</li></ul>
<b>WWPass products</b>	<p>WWPass Security Pack</p> <p>The Security Pack includes software needed to activate and use a PassKey or a Mobile Passkey with wwSafe. The pack must be installed on each Windows computer from which the wwSafe Management Utility will be run.</p>

## Requirements for the wwSafe Client

Requirement	Details
<b>Operating System</b>	<p>Computer with one of the following 32-bit or 64-bit operating systems:</p> <ul style="list-style-type: none"> <li>• Microsoft Windows 7</li> <li>• Microsoft Windows 8</li> <li>• Mac OS X 10.8 or 10.9</li> <li>• Ubuntu 14.04 LTS (Trusty Tahr)</li> <li>• Ubuntu 12.04 LTS (Precise Pangolin)</li> </ul> <p>Minimum storage requirements for wwSafe are as follows:</p> <ul style="list-style-type: none"> <li>• Windows – 50 MB</li> <li>• Mac – 80 MB</li> <li>• Ubuntu – 14 MB</li> </ul>
<b>Web browser</b>	<p>A browser is needed on the Windows computer to authenticate into wwSafe with a PassKey or a Mobile PassKey and activate the PassKey.</p> <p>Supported browsers are:</p> <ul style="list-style-type: none"> <li>• Microsoft Internet Explorer 9 and 10 (32-bit and 64-bit)</li> <li>• Mozilla Firefox 14 to current version</li> <li>• Google Chrome 20 to current version</li> </ul>
<b>WWPass products</b>	<p>WWPass Security Pack and wwSafe client.</p> <p>The Security Pack includes software needed to activate and use a PassKey or a Mobile PassKey with wwSafe. The pack and client must be installed on the Windows computer of each user who will run the client.</p>

## Requirements for wwSafe Users

These requirements must be met for each wwSafe user—administrative and non-administrative.

Requirement	Details
<b>User account and credentials</b>	<p>Account in Microsoft Active Directory (AD). This is used as a user's wwSafe account. Their Active Directory user name is their user name in wwSafe.</p> <p>(When using local user directory, AD is not required).</p> <p>The first time a user logs into wwSafe, they associate their PassKey/Passkey for Mobile with their account and register it with the wwSafe server by entering their Active Directory username and password. These might be the same as the username and password for Windows login.</p> <p><b>Note:</b> A user can be an internal user such as an employee or an external user such as a client. If someone outside your enterprise will connect to your wwSafe server, add an account for that user to Active Directory. You might want to include -companyname in their user name to identify them as an external user in the wwSafe client and Management Utility.</p>
<b>WWPass products</b>	<p>A KeySet from WWPass.</p> <p>A KeySet is needed for each wwSafe user (administrative and non-administrative). It includes the PassKey/PassKey for Mobile used for authenticating into wwSafe during login from the wwSafe client or Management Utility.</p>

## CHAPTER 4 — SMART START FOR INSTALLATION

---

This Smart Start provides an overview of the major steps involved in installing and configuring the wwSafe client, server, and Management Utility. It serves as a road map to installation process.

### Smart Start

1. Set up to use Active Directory with wwSafe
  - a) Download wwsafe.ldif file for wwSafe schema ([steps](#))
  - b) Apply wwSafe schema to Active Directory ([steps](#))
  - c) Obtain SSL certificate for secure communication with Active Directory ([steps](#))
  - d) Create account for wwSafe service user ([steps](#))
  - e) Create account for first Security Administrator ([steps](#))
2. Prepare for wwSafe Server Installation
  - a) Perform setup for first wwSafe Security Administrator ([steps](#))
  - b) Download installation script, wwsafe-bootstrap.sh (this installs the configuration script, wwsafe\_configure.py) ([steps](#))
  - c) Obtain service provider key and certificate ([steps](#))
3. Install wwSafe Server and Management Utility
  - a) Install wwSafe server automatically ([steps](#)) or manually ([steps](#))
4. Configure wwSafe Server and Management Utility
  - a) Run configuration script (wwsafe\_configure.py) ([steps](#))
  - b) Configure service provider parameters ([steps](#))
  - c) Configure Active Directory parameters ([steps](#))
  - d) Configure network and TLS parameters ([steps](#))
  - e) Create server encryption key ([steps](#))
  - f) Set up debug logging ([steps](#))
  - g) Save configuration and start the server ([steps](#))
5. Create administrative groups and register first Security Administrator ([steps](#))
6. Install wwSafe Client ([steps](#))



7. Set up to use PassKey/PassKey for Mobile login for wwSafe ([steps](#))
  - a) Give each user a KeySet (includes PassKey) or make sure each user installed WWPass PassKey for Mobile application on their smartphones, Active Directory credentials (needed to register PassKey/Mobile PassKey with wwSafe), and address and port for wwSafe server (needed to log in from client)
  - b) Install the WWPass Security Pack on each Windows computer from which the client and Management Utility will be run
  - c) Ask each wwSafe user to activate their KeySet or Mobile PassKey from their Windows computer and register their PassKey with wwSafe by logging in for first time from client
8. Assign administrative roles ([steps](#))
9. Set up storage and groups for wwSafe ([steps](#))



**Note:** Information on integrating Azure/Amazon cloud storage with wwSafe is covered under [Create Storage Accounts](#) in Management Utility help.

## CHAPTER 5 — SET UP TO USE ACTIVE DIRECTORY

---

This chapter covers setting up to use Active Directory with wwSafe. User accounts are mapped from Active Directory to wwSafe. Each user's Active Directory account is their wwSafe account. Note that when using local user directory, setting up and using AD is not required.

The first time a user logs into wwSafe, they associate their PassKey with their account and register it with the wwSafe server by entering their Active Directory username and password. (These might be the same as their username and password for Windows login.)

### Topics In This Chapter

---

1. [Download file for wwSafe schema](#)
2. [Apply wwSafe schema to Active Directory](#)
3. [Obtain SSL certificate for secure communication](#)
4. [Create account for wwSafe service user](#)
5. [Create account for first Security Administrator](#)

## 1. Download file for wwSafe schema

Follow these steps to download the wwsafe.ldif file; this applies the wwSafe schema to Active Directory:

- a) Download wwsafe.ldif to your Windows server for Active Directory from:

<https://server-packages.wwpass.net/wwsafe/wwsafe.ldif>

- b) When prompted, enter the login and password provided by WWPASS.

## 2. Apply wwSafe schema to Active Directory

Follow these steps to apply the wwSafe schema to Active Directory using the wwsafe.ldif file:

- a) Run Active Directory as an administrator.
- b) Run the wwsafe.ldif file exactly as shown:

```
C:\>ldifde -i -f wwsafe.ldif -c "<SchemaContainerDN>" "#schemaNamingContext"
```

## 3. Obtain SSL certificate

If you want to use the SSL (secure sockets layer) protocol for secure communication between the wwSafe server and Active Directory, obtain an SSL certificate and store it on the Ubuntu computer that will host the server. The server configuration script will prompt for the location of the certificate. You can obtain an SSL certificate from an internal domain-based Certificate Authority (CA) or an external CA such as DigiCert or Symantec.

## 4. Create an account for the wwSafe service user

Create an Active Directory account for a service user that the wwSafe server can use to connect to Active Directory. The server is bound to Active Directory under this user's account. The user should have permissions to modify user accounts in Active Directory.

The recommended login name for the service user is "wwsafeuser". (A typical user name should not be used.) The server configuration script will prompt for the service user's Active Directory login name and password.

## 5. Create an account for the first Security Administrator

Create an Active Directory account for the first wwSafe Security Administrator. This user creates administrative groups and assigns administrative roles by inviting users to the groups. The Security Administrator's Active Directory credentials are needed to register their PassKey with the wwSafe server. They are the first user to register, which establishes them as the first Security Administrator.



**Note:** If someone outside your enterprise will connect to your wwSafe server, add an account for that user to Active Directory. You might want to include -companyname in their user name to identify them as an external user in the wwSafe client and Management Utility.

## CHAPTER 6 — PREPARE FOR SERVER INSTALLATION

---

This chapter covers how to prepare for installing and configuring the wwSafe server and Management Utility.

It is recommended that you perform all preparation before you run installation and configuration scripts. This allows you to run the scripts without interruption.

### Topics In This Chapter

---

1. [Perform setup for the first wwSafe Security Administrator](#)
2. [Download installation and configuration scripts](#)
3. [Obtain a service provider certificate signed by WWPass](#)

## 1. Perform setup for the first wwSafe Security Administrator

Follow these steps to perform setup for the first wwSafe Security Administrator. This user creates administrative groups and assigns administrative roles by inviting users to join the groups. Setup ensures that the first Security Administrator is ready to do this at the end of the configuration process.

- a) Install the WWPass Security Pack on the Windows computer of the first Security Administrator. This software pack is needed to activate their KeySet or Mobile PassKey.
- b) Activate the KeySet or Mobile PassKey of the first Security Administrator by accessing WWPass [Key Services](#) from their Windows computer.
- c) Install the wwSafe client on the Windows computer of the first Security Administrator. They will use the client to invite users to administrative groups. They can also use it to create groups.



**Note:** Information on creating an Active Directory account for the first Security Administrator is covered under [Set Up to Use Active Directory](#). The account and the KeySet/Mobile Passkey for the first wwSafe Security Administrator should only be used for that role.

## 2. Download server installation and configuration scripts

- a. Follow these steps to download the wwSafe server installation script, `wwsafe-bootstrap.sh`. This script can be used to automatically install the wwSafe server, wwSafe Management Utility, and server configuration script, `wwsafe_configure.py`. When installation is complete, the installation script automatically starts the server configuration script.

Run the following command from the Ubuntu computer that will host the wwSafe server:

```
$ wget --no-check-certificate https://server-packages.wwpass.net/wwsafe/wwsafe-bootstrap.sh  
--user=<login> --password=<password>
```

Replace text in angle brackets with the login and password provided by WWPass.

**Tip:** If you use the PuTTY SSH and telnet client to run commands on Ubuntu, you can copy and paste the download command from this document.

- b. Download and configure the ready wwSafe virtual appliance image.

### 3. Obtain a service provider certificate signed by WWPass

Follow these steps to obtain a service provider certificate signed by WWPass. This is needed to authenticate your wwSafe server with WWPass.

Although the configuration script can perform step b) for you, you will need to pause the script at that point, then run it again to perform remaining steps.

- a) Obtain a service provider name and ID (SPID) by contacting Sales at WWPass (1-888-997-2771).
- b) Generate a service provider Private Key and certificate signing request (CSR) by running the OpenSSL command below from the Ubuntu computer that will host the wwSafe server. Substitute your service provider name and ID from WWPass for text in angle brackets:

```
openssl req -new -newkey rsa:4096 -nodes -subj \
"/O=<Your service provider name>/CN=<Your service provider ID>" \
-keyout <Your service provider name>.key \
-out <Your service provider name>.req
```

- c) Store the Private Key in a directory on Ubuntu, for example:  
  
    /etc/ssl/private/wwsafe-sp.key
- d) Email the certificate signing request to your Sales representative at WWPass.
- e) When WWPass returns a signed certificate and WWPass CA certificate, store both in a directory on the Ubuntu server host, for example:

    /etc/ssl/certs/

### 4. Configuration backup and recovery

wwSafe 2.0 architecture provides high level of server reliability due to these factors:

1. All meta-data are stored in the WWPass DDS, the reliability is guaranteed by the core WWPass technology.
2. All file data are stored in cloud storages with the appropriate level of reliability.
3. The server appliance (either virtual or hardware) contains only the code, the basic configuration files and the server logs. This allows to easily reinstall the server without losing the actual data and configuration.

Let's consider the third case in details: rebuilding wwSafe server if the appliance was crashed for any reason.

During wwSafe installation and initial configuration these parts will appear:

1. wwSafe server and MU code. This code is installed using Ubuntu package system. The software can be reinstalled at any time following the wwSafe installation documentation.
2. wwSafe configuration files. The files are located in the /etc/wwpass folder. It is recommended to archive this folder in a safe place to get rid of passing the initial configuration procedure once again.

3. WWPass Server Provider certificate and secret key. These files are required to use WWPass technology. It is strongly recommended to backup these files in the safe and secure place. Otherwise the new key should be generated and the new certificate should be issued by the WWPass Support.
4. wwSafe server encryption key. Default location is: `/etc/ssl/private/wwsafe-enc.key`. It is strongly required to backup this key in a safe and secure place. If you lose this key the wwSafe server data and meta-data will be lost without possibility to recover.
5. wwSafe log files. Located in the folder `/var/log/wwpass/wwsafe`. You need to backup these files only for information/debugging reasons.

Please follow the recommendations above to make recovery process simpler.

The recover process consists of these steps:

1. Prepare clean operating system according to the requirements and install wwSafe software according to the instructions (or just install the wwSafe appliance image).
2. Use the SP certificate and key from backup or issue the new pair from WWPass
3. Use the backed up configuration files or recreate them by running `wwsafe_cofigure` script and answering the questions.
4. Use the backed up server encryption key.

In this case all the previous data, meta-data and MU configuration will be recovered and ready to use.



## CHAPTER 7 — INSTALL THE SERVER

---

This chapter covers how to install the wwSafe Server and Management Utility. They can be installed automatically with the `wwsafe-bootstrap.sh` script or manually using Ubuntu commands.

### Topics In This Chapter

---

- [Install the wwSafe server automatically](#)
- [Install the wwSafe server manually](#)

## Install the wwSafe server automatically

- a. Follow these steps to automatically install the wwSafe server and Management Utility on the Ubuntu computer that will host the server. Installation is performed using the wwsafe-bootstrap.sh script obtained during [preparation](#) for installation. (To install the server manually, go to step 3.)
  1. Run the wwsafe-bootstrap.sh script from Ubuntu as a user with root privileges using these commands:  
  

```
$ chmod a+x wwsafe-bootstrap.sh
```

```
$ sudo ./wwsafe-bootstrap.sh
```

  
When prompted, enter your password for Ubuntu.
  2. When prompted for a password and user name, enter the login and password provided by WWPass.
  3. When installation is complete, the script pauses at the first configuration step and “Running wwSafe configuration script” is displayed. Go to [Configure the Server](#).

### b. Virtual Appliance installation guide

This document describes the first steps required for the wwSafe 2.0 installation and initial configuration using the Virtual Appliance image.

The image is supported by the VMWare ESX infrastructure. Please see the VMWare ESX documentation for the image import instructions.

The server contains Ubuntu 12.04 LTS distribution with the additional software installed. The operating system components and the wwSafe server software can be updated using Ubuntu package management system (apt).

The user account with sudo permissions is available for configuration.

Login: wwsafeuser

Password: ags1owvAcu

Please follow these steps to configure wwSafe:

It is strongly recommended to change the password at the first login.

Configure the network parameters.

Run wwSafe configuration script `/opt/wwpass/wwsafe/wwsafe_configure.py` and follow the wwSafe installation documentation.

## Install the wwSafe server manually

Follow these steps to manually install the wwSafe server and Management Utility on the Ubuntu computer that will host the server. All steps must be performed by a user with root privileges.

1. Install the following Ubuntu packages and their dependencies using the command(s) shown:

Package	Command to use
nginx python-tornado	\$ sudo apt-get install nginx python-tornado
python-ldap	\$ sudo apt-get install python-ldap
Pcsd	\$ sudo apt-get install pcsd
python-support python-enum	\$ sudo apt-get install python-support python-enum \$ sudo apt-get install python-software-properties

2. Add the wwSafe repository with these commands (use the login and password provided by WWPass):

```
$ sudo apt-add-repository \
'deb https://login:password@server-packages.wwpass.net/ wwsafe/'
```

3. Add the WWPass public key using this command:

```
$ wget -q http://packages.wwpass.com/wwpass.asc -O- | sudo apt-key add -
```

1. Update the package list using this command:

```
$ sudo apt-get update
```

2. Install the following wwSafe software and third-party software from the wwSafe repository using the commands shown:

Package	Command to use
azure-sdk-for-python	\$ sudo apt-get install azure-sdk-for-python
asn1py	\$ sudo apt-get install asn1py
corenetwork-common	\$ sudo apt-get install corenetwork-common
python-gnutls-old	\$ sudo apt-get install python-gnutls-old
python-tlslite	\$ sudo apt-get install python-tlslite
asynctdispatcher	\$ sudo apt-get install asynctdispatcher
sev-mu-library	\$ sudo apt-get install sev-mu-library
sev-server	\$ sudo apt-get install sev-server
sevmu-server	\$ sudo apt-get install sevmu-server

3. Install the following client packages and their dependencies using the commands shown:

Package	Command to use
python-sev-library	\$ sudo apt-get install python-sev-library
libwwtoken-test	\$ sudo apt-get install libwwtoken-test

4. Go to [Configure the Server](#).

## CHAPTER 8 — CONFIGURE THE SERVER

---

This chapter covers configuring the wwSafe Server and Management Utility using the configuration script. This is called `wwsafe_configure.py` and is included with the installation script, `wwsafe-bootstrap.sh`.

### Topics In This Chapter

---

1. [Run the configuration script](#)
2. [Begin or continue a configuration](#)
3. [Configure service provider parameters](#)
4. [Configure Active Directory parameters](#)
5. [Configure network and TLS parameters](#)
6. [Create the server encryption key](#)
7. [Set up debug logging](#)
8. [Save the configuration and start the server](#)

## 1. Run the configuration script

How you run the configuration script (wwsafe\_configure.py) for the wwSafe server depends on how you installed the server:

- a) If you installed the server automatically with the installation script (wwsafe-bootstrap.sh), the configuration script starts automatically and pauses at the first question. Go to step 2.
- b) If you installed the server manually, run the configuration script using the command below:

```
$ sudo /opt/wwpass/wwsafe/wwsafe_configure.py
```

When prompted, enter your password for Ubuntu.

### Answering script questions

Here are tips to follow when you answer script questions:

- Use the Enter key to record values:
  - To use your own value, type the value and press Enter.
  - To use a default value, just press Enter. Default values are shown in brackets [default value]. If the default is Yes, it is shown like this: [Y/n]. If the default is No, it is shown like this: [y/N].Using default values is recommended.
- Use the Tab key to automatically complete system paths.
- Use the Up or Down key to navigate backward or forward through input history. You can change input, if needed. However, you will need to re-enter all input that follows a change.

### Restart the configuration script

If the configuration script is interrupted for any reason, you can restart the script using the following command (this is the command for running the script manually):

```
$ sudo /opt/wwpass/wwsafe/wwsafe_configure.py
```

When the script asks if you want to restart from a recent step, type **Y** and press enter. Script execution resumes at the command that follows the last command executed.

## 2. Begin or continue a configuration

When the configuration script is started, it detects whether you are beginning or continuing configuration for a wwSafe server and asks one of the questions below.

Script Questions	What to Input
Do you want to create a new instance of wwSafe service	<p>The script asks this question the first time it is run or if it completed the last time it was run. Answer as follows:</p> <ul style="list-style-type: none"> <li>Press Enter to use the default (<b>Y</b>) if you want to configure a new wwSafe server.</li> <li>Type <b>n</b> and press Enter if you do not want to configure a new wwSafe server. Script execution is ended.</li> </ul>
Previous wwSafe configuration was not completed. Do you want to continue from the recent step?	<p>The script asks this question if it did not complete the last time it was run. Answer as follows:</p> <ul style="list-style-type: none"> <li>Press Enter to use the default (<b>Y</b>) if you want to continue the script. Execution resumes at the command that follows the last command executed.</li> <li>Type <b>n</b> and press Enter if you do not want to continue the script. The script then asks if you want to create a new instance of the wwSafe service. Answer as described for the “new instance” question above.</li> </ul>

## 3. Configure service provider parameters

Service provider parameters specify the location of your service provider certificate signed by WWPass. This is needed to authenticate your wwSafe server with WWPass.

How you answer service provider questions depends on whether you have a signed certificate from WWPass. Follow [Path 1](#) if you obtained certificate during [preparation](#) for installation. Follow [Path 2](#) if you do not have a signed certificate from WWPass.

### Path 1

Follow this path if you have a service provider key and certificate from WWPass.

Script Questions	What to Input
Do you already have WWPass SP ID for wwSafe service?	Press Enter to use the default ( <b>Y</b> ).
Please input SP private key (PEM format) path	<p>Enter the path to your service provider Private Key on the Ubuntu computer that hosts the wwSafe server, for example:</p> <p><code>/etc/ssl/private/wwsafe-sp.key</code></p>
Please input SP certificate path	<p>Enter the path to your service provider certificate from WWPass on the Ubuntu computer, for example:</p> <p><code>/etc/ssl/certs/wwsafe-sp.crt</code></p> <p>If the certificate is valid, the script displays the following message, “Valid certificate found” and identifies your service provider name.</p>



## Path 2

Follow this path if you do not have a service provider key and certificate from WWPass.

First, obtain a service provider name and ID from WWPass (call Sales at 1-888-997-2771). The configuration script needs these to generate a certificate signing request.

Script Questions	What to Input
Do you already have WWPass SP ID for wwSafe service?	Type <b>n</b> and press Enter.
Do you want to generate new WWPass SP ID key and certificate request?	Press Enter to use the default ( <b>Y</b> ).
Please input the preferred wwSafe SP name	Enter the service provider name obtained from WWPass.
Please input the SP ID received from WWPass (hex string)	Enter the service provider ID obtained from WWPass.  The script generates a 4096-bit RSA Private Key and certificate signing request (CSR), and identifies the paths to both on Ubuntu, for example:  <code>/etc/ssl/private/wwsafe-sp.key</code>
Please send this certificate request to WWPass and obtain the SP certificate	Pause the script and email the certificate signing request generated by the script to your Sales representative at WWPass: <a href="mailto:sales@wwpass.com">sales@wwpass.com</a>
	When WWPass returns the signed certificate and WWPass CA certificate, store both in a directory on Ubuntu, for example:  <code>/etc/ssl/certs/</code>  Then restart the configuration script and specify the locations of the Private Key and certificate following the steps in <a href="#">Path 1</a> .

## 4. Configure user directory parameters

Do you want to configure local OpenLDAP server to store user information (RECOMMENDED)?

- If you respond No, you need to fill in the AD parameters (4a)
- If you answer Yes, you need to use local user directory (4b)

**4a.** This subsection covers Active Directory configuration.

Active Directory parameters specify information the wwSafe server needs to communicate with Active Directory. User accounts are mapped from Active Directory to wwSafe.

Script Questions	What to Input
Please input AD hostname/IP address	Type the Active Directory server hostname or IP address, for example: 10.10.10.10
Do you want to use SSL connection to AD?	Specify whether to use the SSL (secure sockets layer) cryptographic protocol for secure communication between the wwSafe server and Active Directory: <ul style="list-style-type: none"> <li>• Type <b>y</b> if you want to use the SSL protocol.</li> <li>• Press Enter to use the default (<b>N</b>) if you do not want to use the SSL protocol.</li> </ul>
Please input the file path of the certificate authority for AD connection	If you responded <b>y</b> to using an SSL connection, enter the path to your <a href="#">SSL certificate</a> on the Ubuntu computer that hosts the wwSafe server.
Please input AD full domain name (e.g. domain.com)	Type the fully qualified domain name for Active Directory using the subdomain.domain.com format, for example: myservername.mycompany.com
Please input AD service user login (e.g. domain\wwsafeuser)	Type the login name of the <a href="#">service user</a> the wwSafe server will use to connect to Active Directory using the domain name\login name format, for example: mycompany\wwsafeuser
Please input AD service user password	Type the password of the service user the wwSafe server will use to connect to Active Directory.
Please input AD DN for users	If you want to restrict wwSafe access to users in a certain Organizational Unit in Active Directory, enter the domain name with the name of the unit, for example: users.myservername.mycompany.com Press Enter to use the default name shown by the script.

**4b.** This subsection covers local user directory. In this case local OpenLDAP server is set and configured for user management via wwSafe MU.

Please input OpenLDAP hostname/IP address (127.0.0.1 – by default, not recommended to change)	Input the information required.
OpenLDAP server was configured with the root login and password: root login and password are indicated.	These login and password are used to log into the local OpenLDAP from an external client.
<p>Now you have to create the Security Administrator wwSafe user:</p> <ul style="list-style-type: none"> <li>• Please input the first name of initial wwSafe Security Administrator</li> <li>• Please input the last name of initial wwSafe Security Administrator</li> <li>• Please input login for the wwSafe Security Administrator Please</li> <li>• Input one-time password for the wwSafe Security Administrator</li> </ul>	<p>Input the information required.</p> <p><b>Note:</b> you cannot use the login and password configured earlier, you have to think about new login and password.</p>

Next, go to wwSafe Client to create a new user and two groups. Follow the instructions described in wwSafe Client and wwSafe MU Help documents.

## 5. Configure network and TLS parameters

Network and TLS parameters specify the hosts and ports to use for daemons that handle service requests for the wwSafe server and wwSafe Management Utility.

These parameters also specify the Internet protocol to use for incoming connections, the redirect port for the HTTPS protocol, and location of the TLS (Transport Layer Security) server certificate needed to secure connections for the wwSafe server and the wwSafe Management Utility web server. If you do not have a TLS certificate, the configuration script can create a self-signed certificate for you.

Script Questions	What to Input
Please input IP address for wwSafe server (to listen clients connections—external or internal)	<p>Type the IP address of the Ubuntu computer that hosts the wwSafe server, for example:</p> <p>10.10.10.10</p> <p>Press Enter to use the default: 0.0.0.0 (for all addresses)</p>
Please input wwSafe listen port	<p>Type the number of the port on which the wwSafe server should listen for incoming client connections.</p> <p>Press Enter to use the default: 443</p>
Do you have TLS certificate for your wwSafe and wwSafe Management Utility servers (e.g. wws.domain.com)	<p>A TLS (Transport Layer Security) server certificate from a Certificate Authority (CA) is needed on the wwSafe server host for the wwSafe service name, for example, wwsafe.mycompany.com. It ensures secure connections between the server and the wwSafe Management Utility.</p> <p>Respond to TLS certificate questions as follows:</p> <ul style="list-style-type: none"> <li>Press Enter to use the default (Y) if you have a TLS key and certificate pair.</li> </ul> <p>When prompted, enter the paths to your TLS Private Key and certificate on the wwSafe server host.</p> <p>If the certificate is valid, the script displays the hostname of the wwSafe server host.</p> <ul style="list-style-type: none"> <li>Type n and press Enter if you do not have a TLS certificate and key pair. Then go to the next question.</li> </ul>
Do you want to create self-signed TLS certificate for your wwSafe/Management Utility server (e.g. wwsafe.domain.com)?	<p>Press Enter to use the default (Y) and ask the script to create a self-signed TLS certificate.</p> <p>When prompted, enter the hostname of the wwSafe server host, for example:</p> <p>wwsafe.domain.com</p>
Please input wwSafe Management Utility listen host/address (for administrators, external or internal)	<p>Type the hostname or IP address of the host on which the wwSafe web interface will listen for connections from the wwSafe Management Utility, for example:</p> <p>10.10.10.10</p> <p>Press Enter to use the default: 0.0.0.0 (for all addresses)</p>

Script Questions	What to Input
Do you want to use secure web connection (HTTPS) for wwSafe Management Utility interface	<p>Specify whether you want to use HTTPS (hypertext transfer protocol secure) for secure communication via the wwSafe Management Utility web interface:</p> <ul style="list-style-type: none"> <li>Press Enter to use the default (Y) if you want to use the HTTPS protocol. The TLS certificate used for secure connections between the server and the wwSafe Management Utility will also be used for the Management Utility web interface.</li> <li>Type n and press Enter if you do not want to use the HTTPS protocol. The HTTP protocol will be used.</li> </ul>
Please input wwSafe Management Utility listen port (SSL-enabled)	<p>Type the number of the SSL-enabled external port on which the wwSafe Management Utility should listen for incoming HTTPS connections:</p> <p>Press Enter to use the default: 8001</p>
Please input wwSafe Management Utility HTTP-to-HTTPS redirect port	<p>Type the number of the external port to use for automatic redirect from HTTP to HTTPS. Users will be forwarded to the secure wwSafe Management Utility address when they use "http" instead of "https" in the address.</p> <p>Press Enter to use the default: 80</p>
Please input wwSafe Management Utility web host	<p>Type address of the web host for the wwSafe Management Utility. Administrative users will use this address to access and run the Management Utility.</p> <p>Press Enter to use the default.</p>
Please input wwSafe service listen host	<p>Type the hostname or IP address of the host on which the wwSafe server will listen for requests from the wwSafe Management Utility.</p> <p>Press Enter to use the default: 127.0.0.1</p>
Please input wwSafe service listen port	<p>Type the number of the port on which the wwSafe server will listen for requests from the wwSafe Management Utility.</p> <p>Press Enter to use the default: 8002</p>
Please input wwSafe Management Utility service listen host	<p>Type the hostname or IP address of the host on which the wwSafe Management Utility web server will listen.</p> <p>Press Enter to use the default: 127.0.0.1</p>
Please input wwSafe Management Utility service listen port	<p>Type the number of the port on which the wwSafe Management Utility web server will listen.</p> <p>Press enter to use the default: 8003</p>

## 5. Create the server encryption key

The server encryption key is used to encrypt the metadata of files in wwSafe. Encrypted metadata is fragmented and dispersed in WWPass data centers around the globe. File data is stored in Windows Azure/Amazon S3. Metadata includes file attributes such as date of creation and size plus authentication information needed for file access.

The configuration script creates a server encryption key the first time the script is run for a new wwSafe server. The script also prompts you to create a backup of the key.



**Important:** It is extremely important to make a backup copy of the server encryption key. If the main key is lost and a backup is not available, files can no longer be accessed in wwSafe. All the data stored there will be lost.

Script Questions	What to Input
Please input wwSafe server key file name	Type the name of your server encryption key file. If a key file is not available, press enter to create one with the default file name and path:  /etc/ssl/private/wwsafe-enc.key
Do you want to back up your server key file	Press Enter to use the default (Y) and create a backup copy of the server encryption key.
Please input wwSafe backup server key file name	Type a file name and path for the backup copy of the key, for example:  /etc/ssl/private/wwsafe-enc-backup.key  <b>Important:</b> It is recommended that you copy the backup key to a safe storage location that is separate from the server host, for example a flash drive or other device.

## 6. Set up debug logging

If you want to use debug logging to troubleshoot any problems with your installation of wwSafe, use debug logging parameters to create a debug log.

Script Questions	What to Input
Do you want to use debug logging?	<p>Specify whether you want to use debug logging:</p> <ul style="list-style-type: none"> <li>Press Enter to use the default (Y) if you want to implement debug logging. The script creates a debug log in: /var/log/wwpass/wwsafe</li> <li>Type <b>n</b> and press Enter if you do not want to use debug logging.</li> </ul>

## 7. Save the configuration and start the server

When configuration is complete, the configuration script does the following:

- Automatically creates containers in WWPass storage for server audit information, server preferences, and lists of wwSafe Cabinets, groups, and authentication tickets.
- Saves the wwSafe server and Management Utility configuration in the following files:
  - /etc/wwpass/wwsafe.conf
  - /etc/wwpass/wwsafemu.conf
  - /etc/nginx/sites-available/wwsafe
- Starts services for the wwSafe server and Management Utility. (If the Nginx default site is enabled, the script asks if you want to disable it. Disabling the site is recommended.)

After the server is started, you are prompted to [connect](#) a PassKey or PassKey for Mobile to the server host in order to register the first Security Administrator with wwSafe and use their account to create groups for assigning administrative roles:

- If you can connect a PassKey/PassKey for Mobile to Ubuntu, click [here](#) for the steps to follow.
- If you cannot connect a PassKey/PassKey for Mobile to Ubuntu, click [here](#) for the steps to follow.

For more information, see [Create Administrative Groups](#).



## CHAPTER 9 — CREATE ADMINISTRATIVE GROUPS

---

This chapter covers how to register the PassKey/PassKey for Mobile of the first wwSafe Security Administrator and create groups for wwSafe Security Administrators and IT Managers.

### Topics In This Chapter

---

- [Overview](#)
- [Register Security Administrator and create groups from Ubuntu](#)
- [Register Security Administrator and create groups from client](#)

## Overview

Administrative groups are used to assign administrative roles for wwSafe.

The first wwSafe Security Administrator creates the groups and assigns administrative roles by inviting users to join the groups. There is one group for wwSafe Security Administrators and one for IT Managers.

How is the first Security Administrator established? They are the first user to log into the wwSafe server and register their PassKey/PassKey for Mobile. Other users should not log in until the first Security Administrator logs in.

Use one of the procedures that follow to register the first Security Administrator and create administrative groups. The first is performed from Ubuntu. The second is performed from the wwSafe client.

Later, the first Security Administrator [assigns](#) administrative roles. This happens after the wwSafe client is [deployed](#) and [setup](#) for PassKey login is performed for all users.

### Register Security Administrator and create groups from Ubuntu

This procedure is performed from Ubuntu at the end of the server configuration script. It can be followed if you can [connect](#) a PassKey or Mobile PassKey to the Ubuntu computer that hosts the wwSafe server:

1. When the configuration script prompts for a Passkey/PassKey for Mobile, connect the PassKey reserved for the first Security Administrator to the computer.
2. Log into wwSafe with the user name and password for the Active Directory account created for the first Security Administrator. The Security Administrator's PassKey is registered with the wwSafe server and the script creates administrative groups called Security Administrators and IT Managers.

### Register Security Administrator and create groups from the client

This procedure is performed from the wwSafe client. The first three steps depend on setup performed during [preparation](#) for installation.

#### Register the PassKey of the first Security Administrator

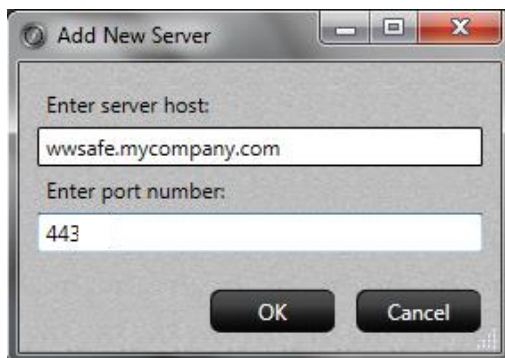
1. Go to the personal computer of the first Security Administrator and connect their PassKey/PassKey for Mobile to the computer.
2. Start the wwSafe client from the Windows Start Menu. The login window opens.

3. Enter wwSafe server connection information as follows:

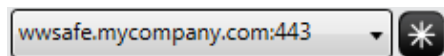
- a) Click the Add New Server button  to open the Add New Server dialog.



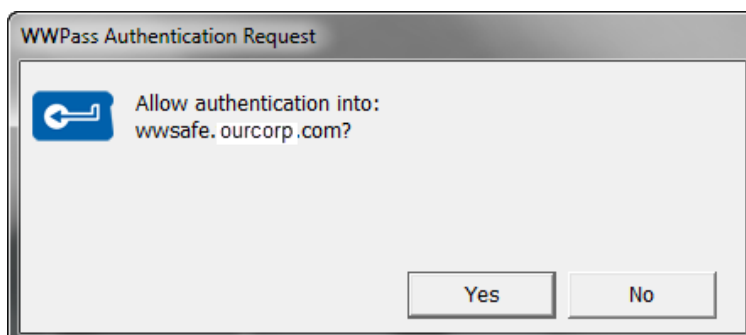
- b) Enter the address for your wwSafe server, for example: `wwsafe.mycompany.com`.
- c) Enter the number of the port used for wwSafe on the server host. The default is 443.



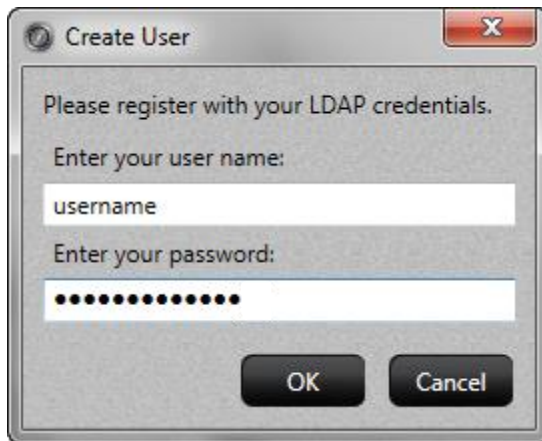
- d) Click **OK** to save your settings. The login window appears with your wwSafe server shown in the server list.




4. Open wwSafe by clicking **Enter** from the login window.
5. Click **Yes** in the WWPass Authentication Request that asks if you want to allow authentication into your wwSafe server.

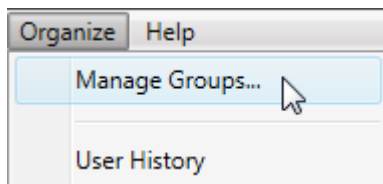


6. Enter the access code for the Security Administrator's PassKey or PassKey for Mobile in the WWPass Access Code Request dialog and click **OK**.
7. When the Create User dialog opens, enter the user name and password for the first Security Administrator's Active Directory account. Then click **OK**. The Security Administrator's PassKey/PassKey for Mobile is registered with your wwSafe server and the main wwSafe window opens.



### Create administrative groups from the client

1. Leave the Security Administrator's PassKey in place and the main client window open.
2. Select **Manage Groups...** from the Organize menu or click .



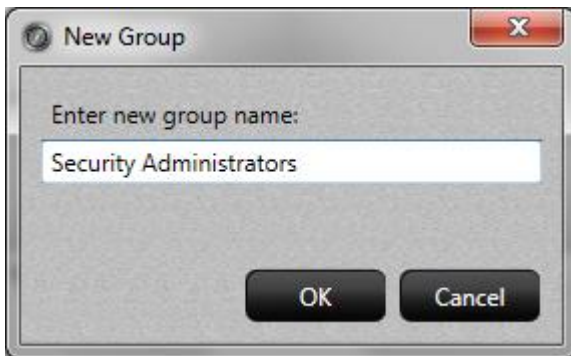
The Groups window opens.



3. From the Groups window, click **New**. The New Group dialog opens.



4. Enter the name to use for the Security Administrators group in the New Group dialog and click **OK**. Using the name "Security Administrators" is recommended but not required. **The Security Administrators group must be created first.**



The group is created and added to the Groups window.





- From the Groups window, click **New**. The New Group dialog opens.

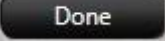


- Enter the name to use for the IT Managers group in the New Group dialog and click **OK**. Using the name "IT Managers" is recommended but not required. **The IT Managers group must be created second.**



The group is created and added to the Groups window.



- Click  to close the Groups window.



## CHAPTER 10 — INSTALL THE CLIENT

---

This chapter covers installing the wwSafe client. This is needed on the Windows computer of each wwSafe user—administrative and non-administrative.

### Topics In This Chapter

---

- [Overview](#)
- [Install the Client on Individual Computers](#)

## Overview



The wwSafe client can be installed individually on each user's computer as described below or deployed on an enterprise basis from a network distribution point with the deployment method you normally use.

## Install the Client on Individual Computers

Follow the steps below to install the client on individual Windows computers using the setup wizard provided by WWPass. The wizard should be available in a computer's Downloads list, on a local or network drive, or on the desktop.

### To install the wwSafe client

---

1. Run the Setup Wizard for the wwSafe client from a user's Windows computer under the user's Windows account. The user needs administrator rights for their computer.
2. From the Welcome screen, click  to begin installing or updating the client. A progress bar shows how far installation has progressed.
3. When installation has successfully completed, the Completed screen appears. Click  to close the setup wizard.

## CHAPTER 11 — SET UP FOR PASSKEY LOGIN

---

This chapter covers setting up for PassKey login for wwSafe. Setup must be performed for each wwSafe user—administrative and non-administrative. It includes registering their PassKey or PassKey for Mobile with the wwSafe server.

### Topics In This Chapter

---

- [Overview](#)
- [How to set up for PassKey login](#)
- [How to connect a PassKey and log in](#)

## Overview

To log into wwSafe from the client or Management Utility, users [connect](#) a PassKey or Mobile PassKey and enter its Access code.

Users do not need a user name and password except for the first time they try to connect to the wwSafe server. At this point, they are prompted to enter their Active Directory credentials in order to register their PassKey/Passkey for Mobile with the wwSafe server.

## When can users log into wwSafe?

- Users can log in and run the wwSafe client after they register their PassKey or Passkey for Mobile with the wwSafe server.
- Users can log in and run the wwSafe Management Utility after they register their PassKey or PassKey for Mobile with the wwSafe server and are assigned the Security Administrator role, the IT Manager role, or both. See [Assign Administrative Roles](#).

## How to set up for PassKey login

Follow the steps below to set up for PassKey/PassKey for Mobile login. Steps link to online help for the wwSafe client and KeySets/Key Services.

### To set up for PassKey login

---

1. Give the following to each wwSafe user (administrative and non-administrative):
  - KeySet from WWPass (this includes the PassKey needed for authentication into wwSafe) or PassKey for Mobile application installed on your smartphone.
  - Username and password for their Active Directory account. These are needed to register their PassKey/PassKey for Mobile with the wwSafe server.
  - Address of the wwSafe server, for example: wwsafe.mycompany.com
  - Port used for communication with the wwSafe server. The default is 443.
2. Install the WWPass Security Pack on each Windows computer from which the wwSafe client and Management Utility will be run. This software pack is needed to activate and use a PassKey or PassKey for Mobile with wwSafe. Click [here](#) for installation steps in Key Services help.
3. Ask each user to activate their KeySet from their Windows computer (click [here](#) for activation steps in Key Services help) or activate their Mobile Passkey (click [here](#) for activation steps in PassKey for Mobile help) by going to [Key Services](#) .
4. Ask each user to register their PassKey/PassKey for Mobile with the wwSafe server by running the client and logging into the server with their Active Directory credentials. Click [here](#) for first-time login steps in client help.

## How to connect a PassKey and log in

To log into wwSafe with a PassKey, you "connect" it to your computer and enter your access code for the PassKey.

How you "connect" a PassKey or Mobile PassKey to your computer depends on your PassKey version. You can either:

- Place it on an NFC reader (Version 2 and higher)  
or
- Insert it into a USB port (Version 1 and higher)  
or
- Pair it with your computer (Passkey for Mobile)

Enter your access code using exactly the same characters and cases (upper and/or lower) you specified when you activated your PassKey/PassKey for Mobile.

You are given three chances to enter the correct code. If you enter the wrong access code three times in a row, your PassKey/PassKey for Mobile is locked for 15 minutes and cannot be used.

## CHAPTER 12 — ASSIGN ADMINISTRATIVE ROLES

---

This chapter covers assigning administrative roles. The wwSafe Security Administrator and IT Manager roles are assigned by the first Security Administrator after administrative groups are [created](#) and users register PassKeys/PassKeys for Mobile with the wwSafe server.

### Topics In This Chapter

---

- [Overview](#)
- [How to assign administrative roles](#)

## Overview

The first wwSafe Security Administrator assigns administrative roles by inviting users to join the Security Administrators group, the IT Managers group, or both.

Invitations are sent to the Notification pane of a user's wwSafe client.

A user becomes a wwSafe Security Administrator or IT Manager when they accept an invitation to the group for that role:

- Security Administrators manage users and groups from the Management Utility and client.
- IT Managers manage storage from the wwSafe Management Utility. At least one IT Manager is needed to set up storage for wwSafe.

After a user accepts an invitation, give them the URL for the wwSafe Management Utility.



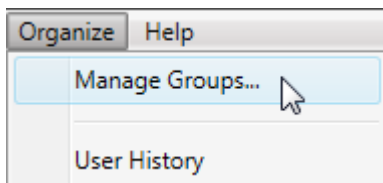
**Important:** It is a best practice to have at least two wwSafe Security Administrators so that a backup administrator is available. If you have no Security Administrator access, you might need to reinstall the wwSafe Server in order to restore access.

## How to assign administrative roles

Follow the steps below to assign administrative roles using the account and PassKey/PassKey for Mobile of the first wwSafe Security Administrator.

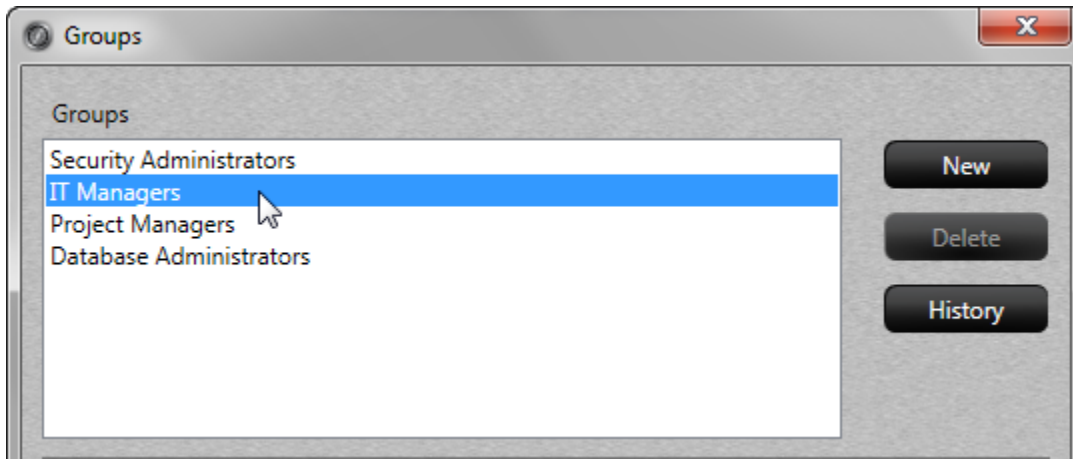
### To assign administrative roles

1. Go to the Windows computer of the first Security Administrator and [connect](#) the PassKey to the computer.
2. Start the wwSafe client from the Windows Start Menu and enter the access code for their PassKey/PassKey for Mobile to log in. The main wwSafe window opens.
3. Select **Manage Groups...** from the Organize menu or click **Groups** to open the Groups window.

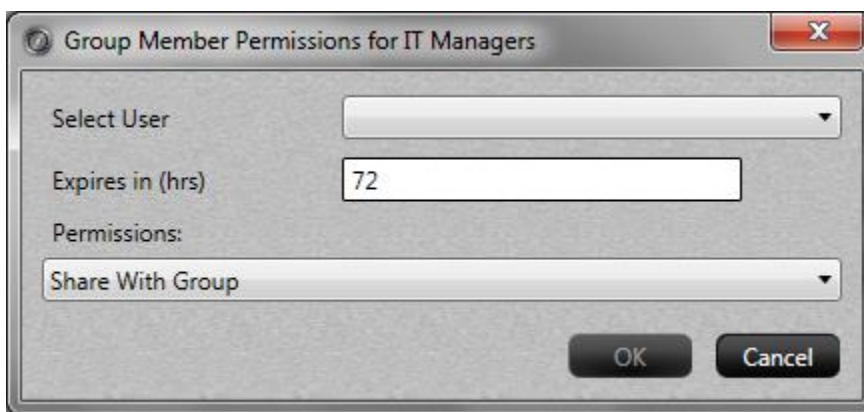




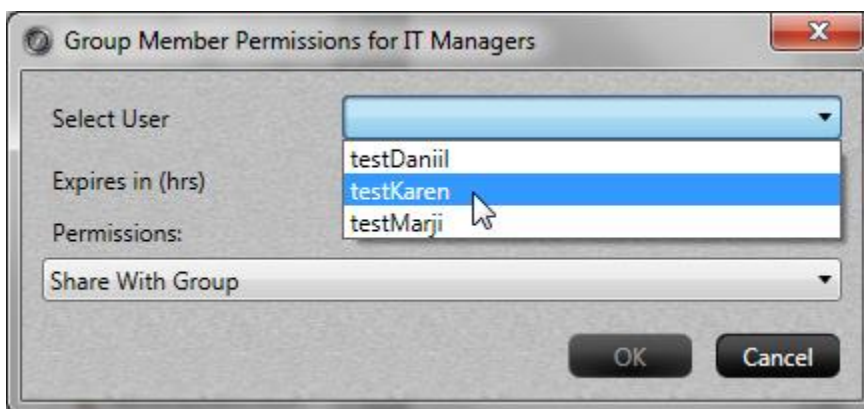
4. Click on the name of the IT Managers group or Security Administrators Group to select the group.



5. Click **Invite**. The Group Member Permissions window opens.



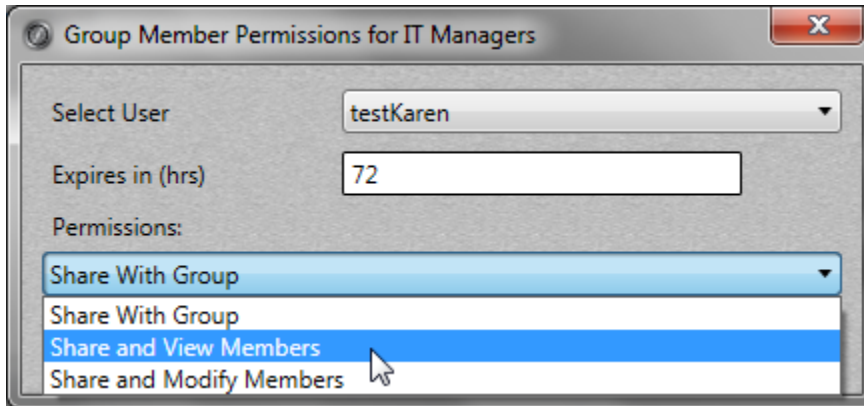
6. Click in the **Select User** list and select the name of a wwSafe user. The list shows the names of all users whose PassKeys/PassKeys for Mobile are registered with the wwSafe server.



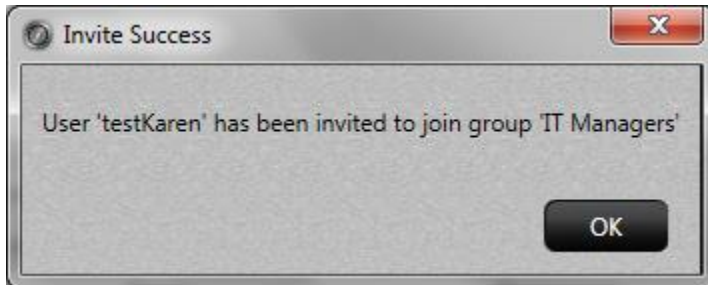
7. Enter an expiration time for the group invitation in the **Expires in (hrs)** box. The value must be a whole number. The default is 72 hours. To be added to the group, the user must accept the invitation before the expiration time passes.


Expires in (hrs)

8. Assign group permissions to the user by clicking in the **Permissions** list and selecting a permissions level. The lowest permissions level (Share With Group) is selected by default. Click [here](#) to see a permissions chart in Management Utility help.



9. Click **OK** to send an invitation to the selected user. Then click **OK** to clear the message that confirms the invitation was sent.



10. Click  to close the Groups window.

11. After a user accepts an invitation to an administrative role, give them the URL for the wwSafe Management Utility. (When a user accepts an invitation, their name is shown in the list for the Security Administrators or IT Managers group.)

## CHAPTER 13 — SET UP STORAGE AND GROUPS

This chapter provides a Smart Start with an overview of the major steps involved in setting up to use wwSafe. Steps include setting up storage and creating groups for folder sharing.

Complete information on setting up and managing wwSafe is available in Management Utility [help](#). The information includes how to integrate Azure/Amazon storage with wwSafe.

Setup steps can be performed after:

- The wwSafe server and Management Utility are [installed](#) and configured.
- The wwSafe client is [deployed](#) to the Windows computers of all users.
- PassKeys/Mobile PassKeys for all users have been [activated](#) and registered with the wwSafe server.
- Users with the wwSafe IT Manager, Security Administrator and Domain Administrator [roles](#) are available.

Steps are performed by a wwSafe IT Manager and a wwSafe Security Administrator. IT Manager steps are performed from the Management Utility. Security Administrator and Domain Administrator steps are performed from the wwSafe Client and wwSafe MU.

### Smart Start for wwSafe Setup

#### Steps for wwSafe IT Managers

##### 1 Create Storage Accounts

Create one or more storage accounts for wwSafe Cabinets. You select a storage account when you create Cabinet types in the next step. The account points to your Azure cloud storage, which is used for storing the file data users add to wwSafe Cabinets.

To create storage accounts, present the PassKey of any IT Manager to a Windows computer where the WWPASS Security Pack is installed, run the wwSafe Management Utility, and follow the steps under [Create Storage Accounts](#) in Management Utility help. The steps tell you how to integrate Azure storage with wwSafe.

##### 2 Create Cabinet Types

Create Cabinet types for Cabinets. You select a Cabinet type when you assign a Cabinet to users. Each Cabinet has the properties of its Cabinet type.

The properties that can be set for a Cabinet type are:

- The wwSafe storage account it uses.
- Its storage capacity.
- Whether it has the default setting. When a Cabinet type has the default setting, Cabinets with this type are automatically assigned to all wwSafe users.

Different Cabinet types can be defined to meet different storage needs.

To create Cabinet types, present the PassKey of any IT Manager to a

Windows computer where the WWPass Security Pack is installed, run the wwSafe Management Utility, and follow the steps under [Create Cabinet Types](#) in Management Utility help.

### 3 Assign Cabinets to Users

Assign one or more Cabinets to users. This creates Cabinets in their wwSafe clients.

To assign Cabinets, present the PassKey of any IT Manager to a Windows computer where the WWPass Security Pack is installed, run the wwSafe Management Utility, and follow the steps under [Assign Cabinets to Users](#) in Management Utility help.

**Note:** Some Cabinets are automatically assigned to all wwSafe users. This happens when a Cabinet type with the Use by Default setting is created.

## Steps for wwSafe Security Administrators

### 4 Create groups for sharing folders

Create Groups that can be used for sharing folders and their files in wwSafe.

Before you begin, ask users to provide information about the groups they need. Ask about the purpose of each group, what its name should be, and who should be invited to join.

To create folder-sharing groups, present the PassKey of any Security Administrator to a Windows computer with the wwSafe client, run the client, and follow the steps under [Create Groups for Folder Sharing](#) in Management Utility help.

### 5 Invite users to join groups for sharing folders

Invite users to join each group created for folder sharing. As you invite users to a group, you give them permissions for the group (click [here](#) to see a permissions chart in Management Utility help):

- If one or more users have Share and Modify permissions for the group, they can invite other users to join.
- If no users have Share and Modify permissions, you need to issue all invitations to the group. You might issue invitations based on the list provided by the user who requested the group.

To invite users to groups for folder sharing, present the PassKey of any Security Administrator to a Windows computer with the wwSafe client, run the client, and follow the steps under [Create Groups for Folder Sharing](#) in Management Utility help.

**Important:** Before users can be invited to join groups, they need to run the wwSafe client and register their PassKeys with the wwSafe server.

## 6 Create users

Create wwSafe users in wwSafe MU.

To create wwSafe users, present the PassKey or PassKey for Mobile of any Security Administrator to your personal computer where the WWPass Security Pack is installed, run the wwSafe Management Utility, and follow the steps under [Create users](#).

## 7 Create domains

Create Domains in wwSafe to be able securely store files and data of different enterprises and give access to their employees.

To create wwSafe users, present the PassKey or PassKey for Mobile of any Security Administrator to your personal computer where the WWPass Security Pack is installed, run the wwSafe Management Utility, and follow the steps under Create domains.