ADMIN GUIDE

WWPass wwSafe Management Utility

September 2014

TABLE OF CONTENTS

CHAPTER 1 — GET STARTED

This chapter provides information on what is covered in this documentation, smart start for set up, how to preserve content in wwSafe and what to do if you need assistance.

Welcome

This documentation covers managing wwSafe™, a client/server application from WWPass®. It is written for administrative users (see below).

wwSafe is managed from the wwSafe Management Utility (MU) and the wwSafe client.

The MU is a web utility that is run via a web browser and connects to a certain wwSafe server.

More about administrative users

Domain Administrators are administrative users for wwSafe.

Domain Administrators are responsible for managing the domains they administrate and the users of these domains.

When a Domain Administrator is logged in, the users of the domain (or domains) managed are shown.

Your hardware PassKey™ or Mobile PassKey tells wwSafe which role or roles you have. A PassKey is a cryptographic and anonymous authentication device from WWPass.

Before you run the wwSafe MU or client, connect your hardware PassKey or Mobile PassKey to your personal computer. If you have all three roles, you can use the same PassKey for all of them.

More about wwSafe

wwSafe allows enterprise users to securely store and share confidential files in the cloud. The files might be contracts, patents, legal documents, or intellectual property. They can be shared with individual users and with groups.

Employees of many different enterprises can work in wwSafe using different domains.

Files are safely stored in wwSafe Cabinets that are designed to prevent data breaches.

Files can only be accessed by and shared with authorized users. To prove that they are authorized, each user must authenticate their identity with a PassKey when they log into wwSafe.

Authorized users can include internal users such as enterprise employees and external users such as clients who need to safely share information with an enterprise.

The only way users can reconstruct file metadata and access stored files is by authenticating with hardware PassKey or Mobile PassKey. An enterprise can choose whether to use two-factor authentication (PassKey plus access code) or single-factor authentication (PassKey only).

wwSafe integrates with Microsoft Windows Azure and Amazon S3 for cloud storage and local OpenLDAP/Active Directory for the user account repository.

Note: All data stored in wwSafe is transported using the Transport Layer Security (TLS) protocol, a cryptographic protocol that provides communication security over the Internet.

Smart Start for Set Up

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

These steps can be performed after:

- The wwSafe client is deployed to the personal computers of all users (administrative and non-administrative).
- Hardware PassKeys or PassKeys for Mobile for all users (administrative and non-administrative) have been activated and registered with the wwSafe server.

Domain Administrator steps are performed from both, the wwSafe client and the wwSafe Management Utility (MU).

Smart Start

Steps for wwSafe Domain Administrators

1. **View users of a Domain**
2. **Create a new user in the Dashboard**
3. **Assign cabinet a user**
4. **View user cabinets**
5. **View statistics**

Preserving Content in wwSafe

This topic provides best practices for ensuring that files stored in wwSafe Cabinets can be recovered when users leave your enterprise or are removed from wwSafe.

The files stored in Cabinets can only be recovered if they are available in shared folders or also stored in your file system.

Best practices

Ask each wwSafe user to:

- Store files in folders in their Cabinets.
- Share each folder they create with their department manager. (They can share their folders with other wwSafe users as needed.)
- Give the manager Share permissions for each folder. This is the highest permissions level.

- Assign ownership of the folder to the manager immediately before they leave your enterprise or are removed from wwSafe (if circumstances allow).

Note: To share a file in wwSafe, a user shares its folder. Individual files and Cabinets cannot be shared. Files must be stored in a folder before they can be shared.

Need assistance?

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

Phone	1-888-WWPASS0 (+1-888-997-2770)
Email	support@wwpass.com

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.

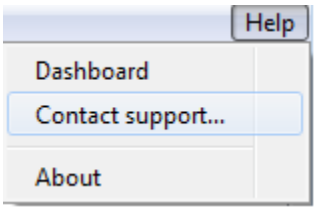
All WWPass logs available on the wwSafe client computer are automatically attached to the email.

Logs contain information that can help Product Support troubleshoot problems. They are located:

- On Windows: C:\Users\<username>\AppData\Local\WWPass\wwpass.log
- On Mac: ~/Library/Logs/wwpass/wwpass.log
- On Ubuntu: ~/.cache/wwpass/wwpass.log

To report a problem from Dashboard:

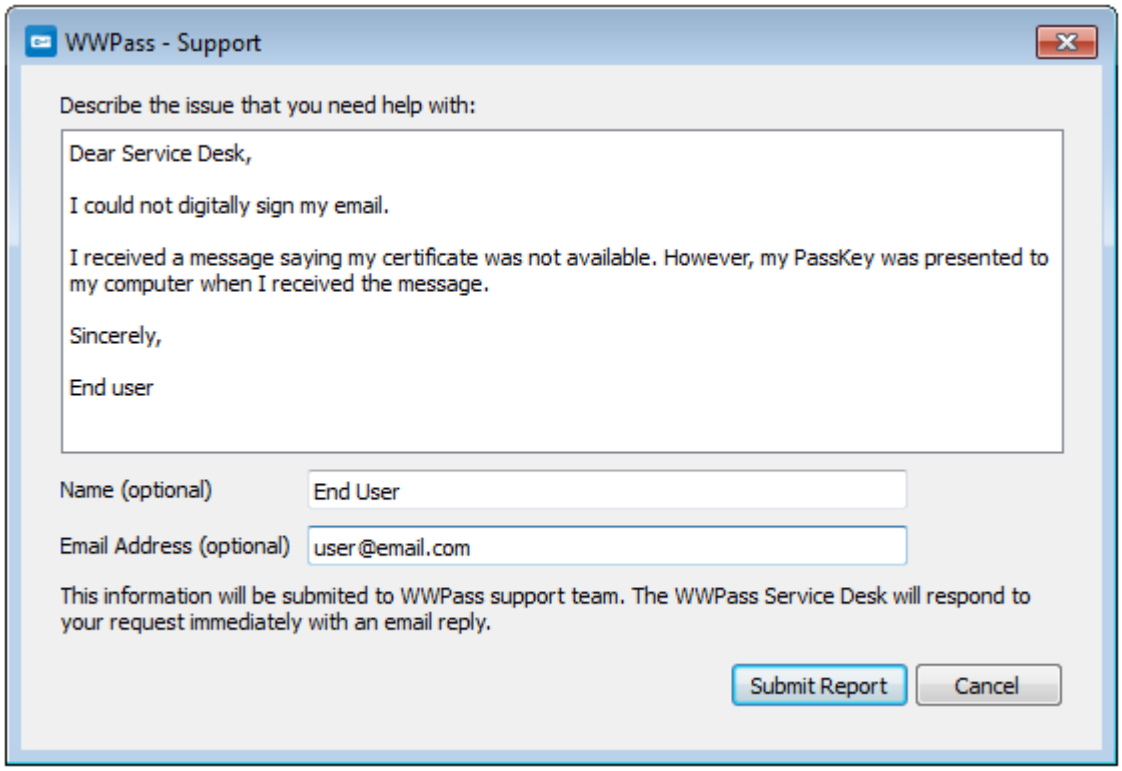
1. Click the **Help** in the upper-right corner of Dashboard and then **Contact support** as shown below:



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. You can also enter your name.

4. Click Submit Report to email your report along with logs on the wwSafe client computer.



CHAPTER 2 — COMPONENTS AND REQUIREMENTS

This chapter covers basic information about wwSafe components, requirements for wwSafe server and Management Utility, for the wwSafe Client and wwSafe users.

wwSafe Components

wwSafe includes the following components:

- **wwSafe Client**—This is a cross-platform application that provides users with an easy-to-use intuitive interface for storing and sharing files. The wwSafe client is installed on your personal computer of each wwSafe user. Each user's PassKey from WWPass ensures that only they can access their files. The client is installed with a setup wizard. See Install the wwSafe client.

- **wwSafe Cloud Server**—This runs on an Ubuntu computer or virtual machine (12.04 Precise Pangolin is required). The wwSafe server communicates with WWPass, Azure or Amazon cloud storage, and local OpenLDAP/Active Directory. wwSafe clients connect to the wwSafe Cloud Server to authenticate users, run commands for storing and sharing files, and access file data in the Cloud back-end.

- **wwSafe Management Utility (MU)**—This resides on the wwSafe server host and is run via a web browser. The MU provides administrative users with a centralized tool for managing wwSafe users and storage:

    - wwSafe Domain Administrators can use the MU to manage domains they administrate, add new users and delete existing ones from their domains.

  wwSafe Domain Administrator can use the MU to audit the administrative operations and to view statistics of the domains they manage.

  Each administrative user's PassKey is used for secure access to the MU.

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. For detailed information, see requirements for the server, client, and users.

The components you need from WWPass are covered in the checklist for What You Need from WWPass.

Needed for wwSafe client

✔ Computer with Microsoft Windows 7 or 8.1

✔ Microsoft .NET 4.5

✔ Web browser to authenticate with a hardware 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 privileges

✔ Ubuntu user with root privileges

Requirements for the wwSafe Client

Requirement	Details
Microsoft Windows/Linux Ubuntu/Mac	Computer with one of the following 32-bit or 64-bit operating systems: • Microsoft Windows 7 • Microsoft Windows 8 • Mac OS X 10.8 or 10.9 • Ubuntu 14.04 LTS (Trusty Tahr) • Ubuntu 12.04 LTS (Precise Pangolin) Minimum storage requirements for wwSafe are as follows: • Windows – 50 MB • Mac – 80 MB • Ubuntu – 14 MB
Web browser	A browser is needed on the Windows computer to authenticate into wwSafe with a PassKey or a Mobile PassKey and activate the PassKey. Supported browsers are: • Microsoft Internet Explorer 9 and 10 (32-bit and 64-bit) • Mozilla Firefox 14 to current version • Google Chrome 20 to current version
WWPass products	WWPass Security Pack and wwSafe client. 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.

Requirements for wwSafe Users

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

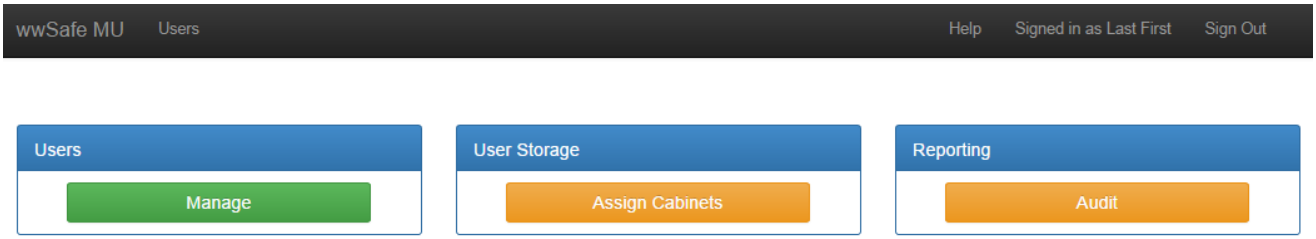
Requirement	Details
User account and credentials	Account in local OpenLDAP/Microsoft Active Directory (AD). This is used as a user's wwSafe account. Their Active Directory user name is shown in wwSafe. The first time a user logs into wwSafe, they associate their PassKey or Mobile PassKey with their account and register it with the wwSafe server by entering their Active Directory username and password. These might be the same as the username and password for Windows login (corporate installation). **Note:** 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 case with cloud installation Security Admin while creating a user emails him/her login and activation code.
WWPass products	A KeySet or a Mobile PassKey from WWPass. A KeySet is needed for each wwSafe user (administrative and non-administrative). • In case with a hardware KeySet, it includes the PassKey used for authenticating into wwSafe during login from the wwSafe client or Management Utility. • In case with a mobile application, it includes only a Mobile PassKey used for authenticating into wwSafe during login from the wwSafe client or Management Utility.

CHAPTER 3 — DOMAIN ADMIN FEATURES

Overview for Domain Administrator features

Users with the wwSafe Domain Administrator role can manage Domains they administrate and users of these Domains.

Functions for managing Domains and members of these Domains are available on the Domain Administrator menu of the wwSafe Management Utility (MU). This menu is displayed when a Domain Administrator is logged in.



Features for Domains

- View statistics of Domains administrated

Features for Users of the Domains administrated

- View users of a Domain
- Create new Domain users
- Assign cabinets to a user
- View user cabinets
- Delete users

Domain Administrator Creation

A Security Administrator creates a Domain Administrator using both wwSafe MU and wwSafe Client.

1. Using a browser, login to wwSafe Cloud MU
2. From the Users Menu select **Create User** and enter Surname (last name), given name (first name), login, activation code, choose user's domain from the pull down menu and hit **Save**.
3. Email the Domain Administrator registration email.
4. Using the wwSafe Client, the Domain Admin has to login to wwsafecloud.wwpass.com on port 443 using the on-time ticket.
5. The WWPass Security Administrator invites Domain Administrator to a domain group using the wwSafe Client:
    a. From the Organize Menu

b. Select the desired group

c. Select **Add member**

d. Select a person from the pull down menu

e. Select access rights from the pull down menu

Invitation will be sent to target user via the wwSafe Client.

6. Using the wwSafe Client, the Domain Administrator has to login to wwsafecloud.wwpass.com on port 443 and accept the invitation.

Note: domain administrator should test folder creation and file upload using the wwSafe client and signing into the wwSafe MU at https://wwsafecloudmu.wwpass.com/

Run wwSafe MU

This topic covers running the wwSafe Management Utility (MU) and logging into the wwSafe server.

In order to log in, you need to connect your PassKey to your personal computer you are using to access the MU. The wwSafe server uses your PassKey or Passkey for Mobile to determine which role or roles you have and authenticate your identity.

Once you log into the wwSafe MU, you remain logged in until you explicitly log out or turn off the personal computer used to access the server. If you close your browser after logging in, you do not need to log in and authenticate the next time you run the wwSafe MU.

Note: If the wwSafe server does not recognize you as an administrative user, the following message appears when you try to log into the wwSafe MU: "You do not have administrative permissions to use the wwSafe MU". This can happen if your PassKey has not been registered with the wwSafe server or you have not joined an administrative group. Check the Notification pane of your wwSafe client to see if an invitation to join the Administrators group is waiting for your acceptance. Then accept the invitation. You are added to the administrative group.

To run the wwSafe MU:

1. Connect the hardware PassKey or the Mobile PassKey of a wwSafe IT Manager, a wwSafe Security Administrator, a Domain Administrator or of all three roles to your personal computer.

2. Run the wwSafe Management Utility from a web browser by entering the URL for the wwSafe server, for example: wwsafe.mycompany.net

3. Click 

from the **Sign In** Screen to log into the wwSafe server. (If you are currently logged in, the wwSafe Management Utility appears instead of the **Sign In** Screen. You can skip the remaining steps.)

Note: If your hardware PassKey or Mobile PassKey is not connected to your computer, a message prompts you to connect your Key (pair – in case with a PassKey for Mobile). Connect your PassKey. The message is cleared. You do not need to click **Cancel**.

Click 

in the WWPass Authentication Request to authenticate your identity with the wwSafe server. You are logged into the wwSafe MU.

Domains

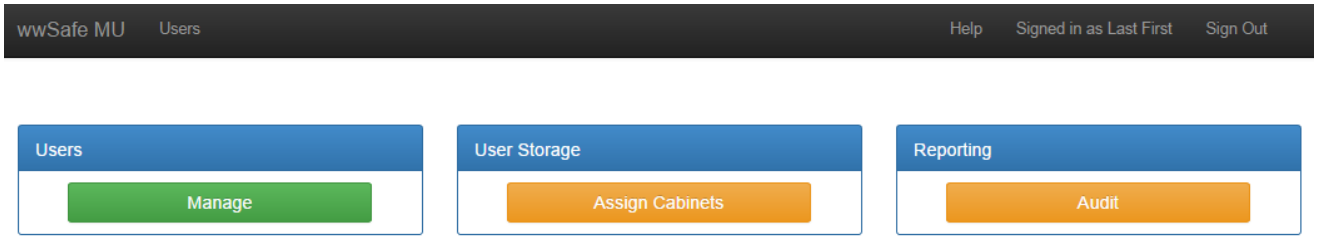
This topic covers Domain management.

View the Statistics of the Domain administrated

Domain Admins can view statistics of the domains administrated.

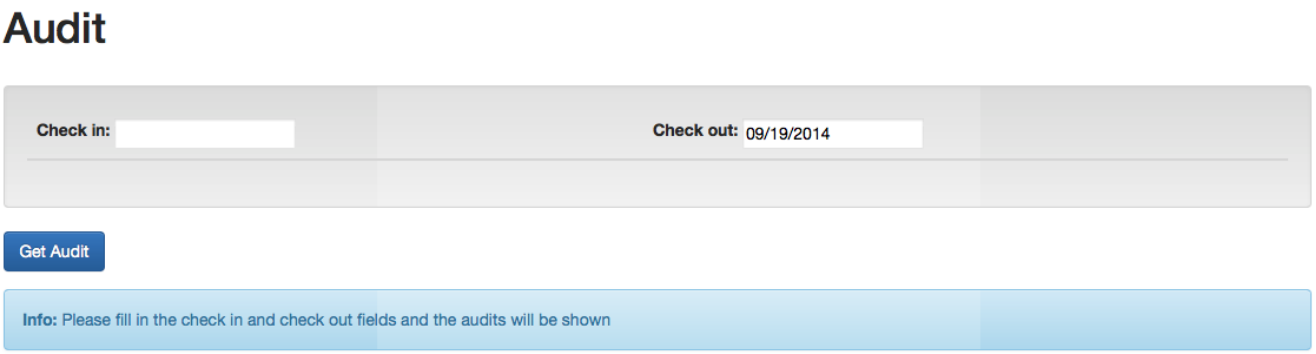
To view the Domain audit

1. Connect the hardware PassKey or Mobile PassKey to your personal computer and log in wwSafeMU as a Domain Administrator.
2. Click the **Audit** button.

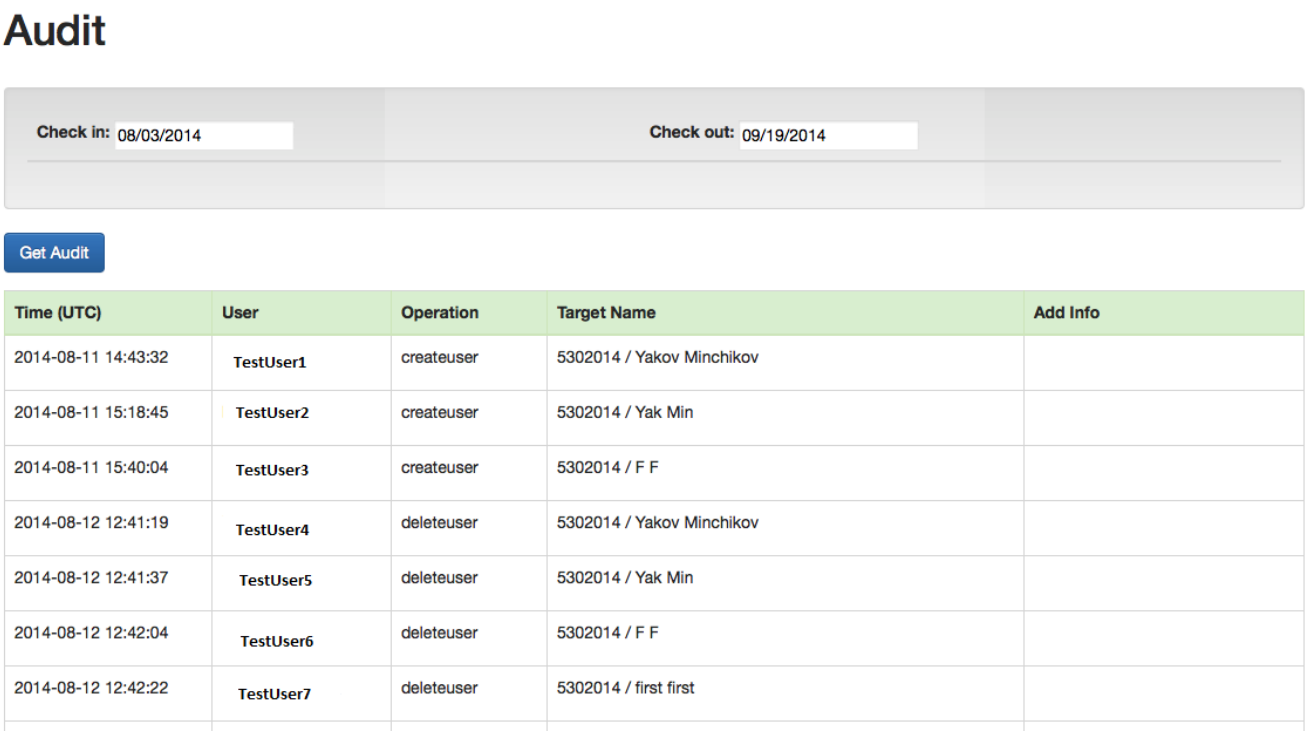


3. The Audit page will appear. Fill in the dates needed and click the 

button.



4. You will get audit history for the date range specified. Operations are shown from oldest to newest, with oldest at the top.



5. Scan audit history in the Audit page to see all operations performed from the wwSafe MU in the date range specified. The operations shown are described below.

Columns in Audit History

Time UTC	User	Operation	Target Name	Add Info
The local UTC time an operation was performed. (UTC stands for Coordinated Universal Time.)	Name of the IT Manager, Security Administrator or Domain Administrator who performed an operation.	Type of operation that was performed. The following operations can be shown:	The target of an operation. The following can be shown:	Additional information about an operation. The following can be shown:
		• assignvault—Shown when a Cabinet type is assigned to a user. This creates a Cabinet with that type.	• Identification number for the Cabinet that is created.	• None shown.
		• chowngroup—Shown when the owner of a group is changed.	• The group name or unique identifier (GID) for the group.	• Name or unique identifier (PUID) for the new owner.
		• deleteuser—Shown when a user is removed from wwSafe.	• User name or unique identifier (PUID) for the	• None shown.

			deleted user.	
		• delstorageacc—Shown when a storage account is deleted from wwSafe.	• Name of the deleted storage account.	• None shown.
		• delvault—Shown when a Cabinet is deleted from wwSafe.	• Identification number for the deleted Cabinet.	• None shown.
		• delvaulttype—Shown when a Cabinet type is deleted from wwSafe.	• Identification number for the deleted Cabinet type.	• Identification number for the Cabinet type selected to replace the deleted type. When a Cabinet type is deleted, it must be replaced by another Cabinet type. Cabinets that were created from the deleted type then use the properties if the replacement type.
		• login—Shown when a wwSafe IT Manager or Security Administrator logs into the wwSafe server from the wwSafe MU.	• None shown.	• None shown.
		• modstorageacc—Shown when the Azure primary access key for a wwSafe storage account is changed.	• Name of the storage account.	• None shown.
		• modvaulttype—Shown when the storage limit for a Cabinet type is	• The Cabinet type's identification	• The Cabinet type's new storage limit.

		changed.	number.	
		• newstorageacc—Shown when a new wwSafe storage account is created.	• Name of the new storage account.	• Type of storage used for the new storage account. This is always Azure as Windows Azure clouds storage is supported for wwSafe.
		• newvaulttype—Shown when a Cabinet type is created.	• The new Cabinet type's identification number.	• The name used by default for Cabinets created from the Cabinet type. Users can change the name in their wwSafe clients.
		• renamegroup—Shown when a wwSafe group is renamed.	• The old group name or unique identifier (GID) for the group.	• The new group name.
		• setvaulttype—Shown when a Cabinet's type is changed.	• The identification number of the Cabinet.	• The identification number of the Cabinet's new Cabinet type.
		• updateconfig—Shown when a wwSafe storage account is created or changed.	• None shown.	• None shown.

Users of the Domains administrated

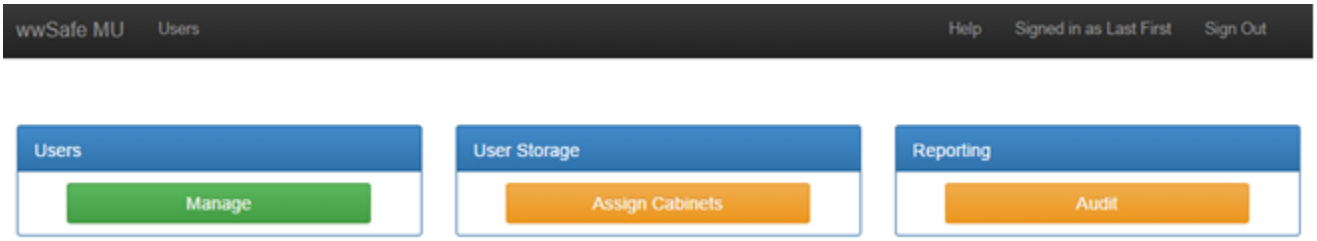
This topic covers user management of the domains administrated.

View users of a Domain

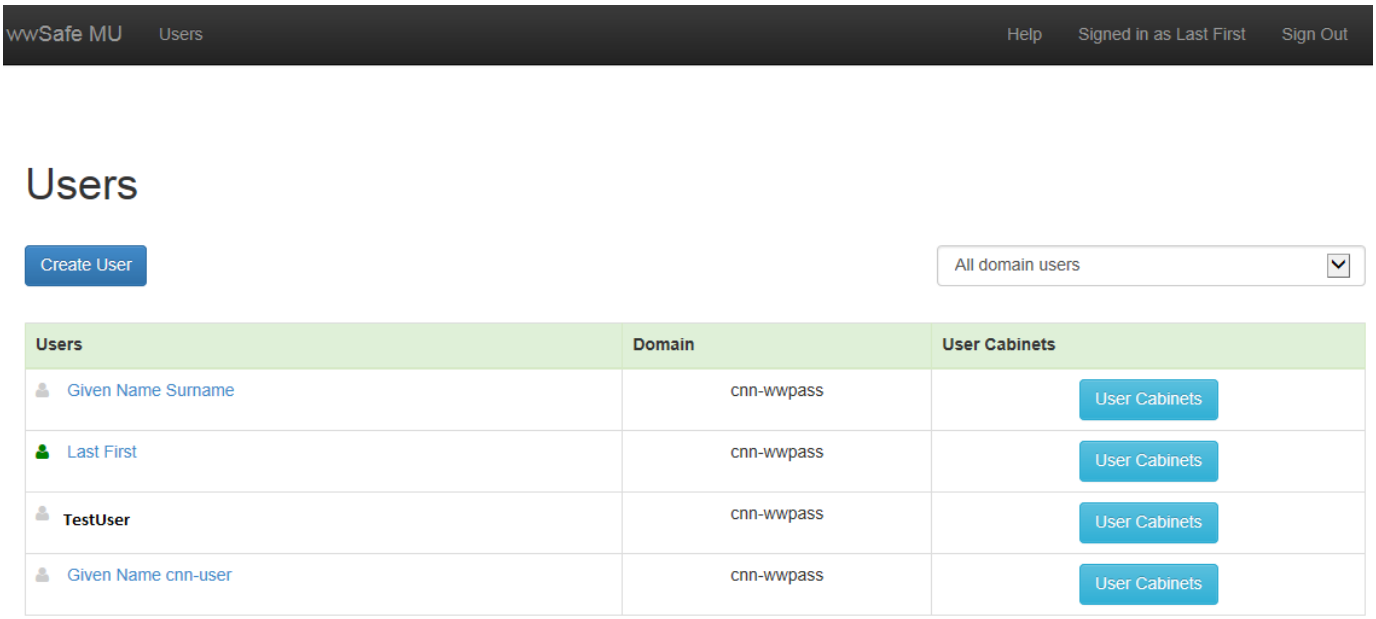
Domain Administrators can view the list of users of the Domain.

To view users of a Domain

1. Connect the hardware PassKey or Mobile PassKey to your personal computer and log in wwSafeMU as a Domain Administrator.



2. Click the **Manage** button or the **Users** tab.



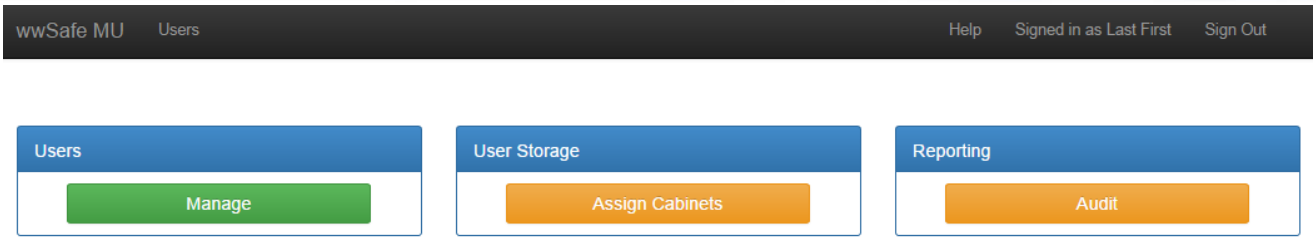
3. You will see list of users of your Domain. If you administrate more than one Domain, you can filter users by a domain in the upper-right corner.

Create a new user in the Domain administrated

A Domain Administrator can add new users to the Domain administrated.

To create new Domain users

1. Connect the hardware Passkey or Mobile Passkey and log in wwSafeMU as a Domain Administrator.

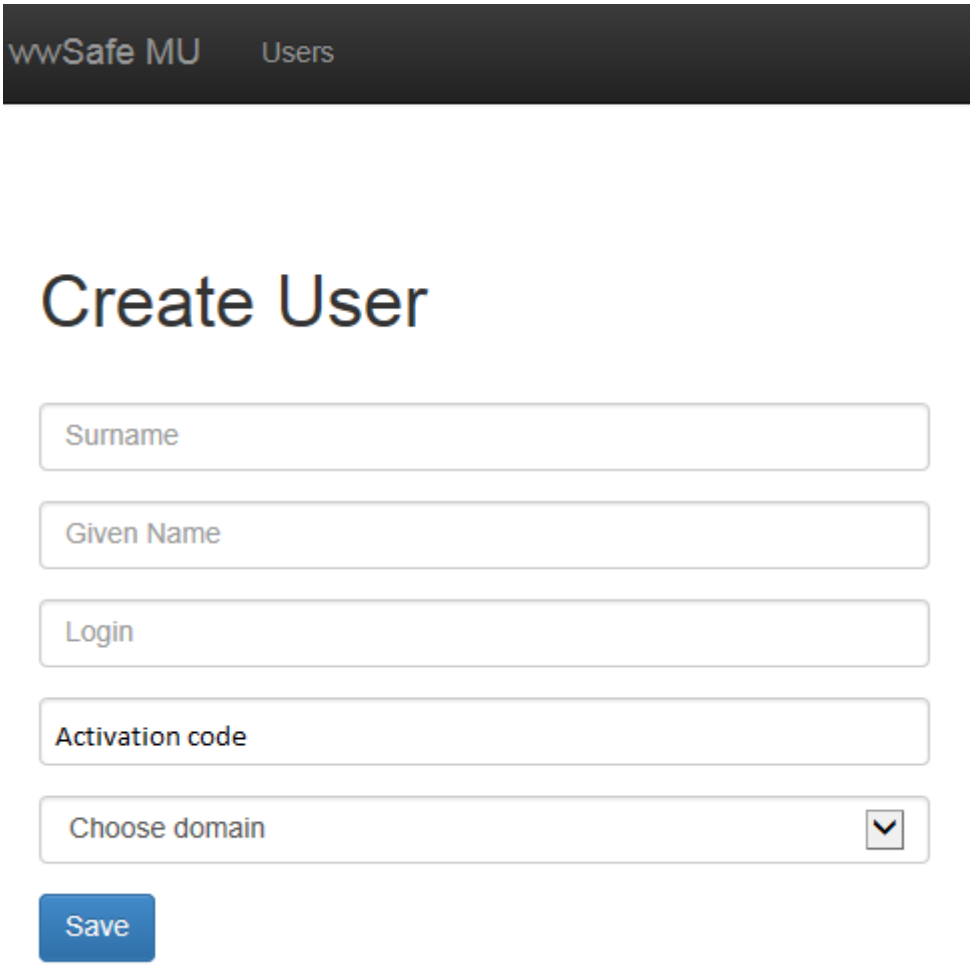


2. Click the **Manage** button or the **Users** tab.

3. A Users page will appear, click the 

button.

4. Fill in information about a new user, choose a Domain and click **Save**.



5. The new domain user has been successfully created. Send the ticket indicated to the new user to initialize the account. You can also see users' domain, login and activation code.

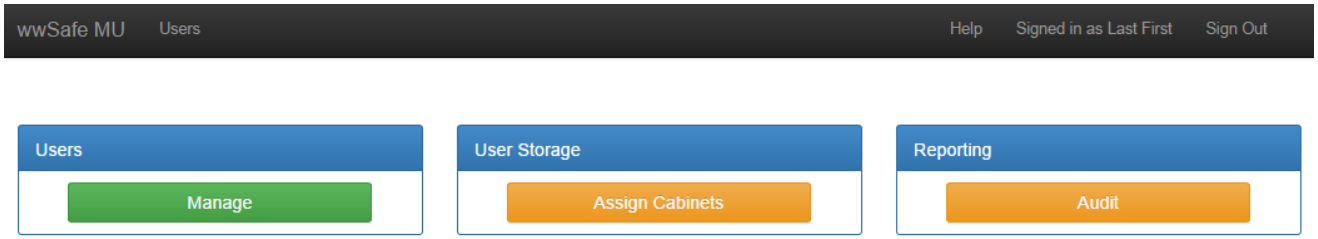
6. Click the **User profile** to view information about the newly created user.

Rename a user

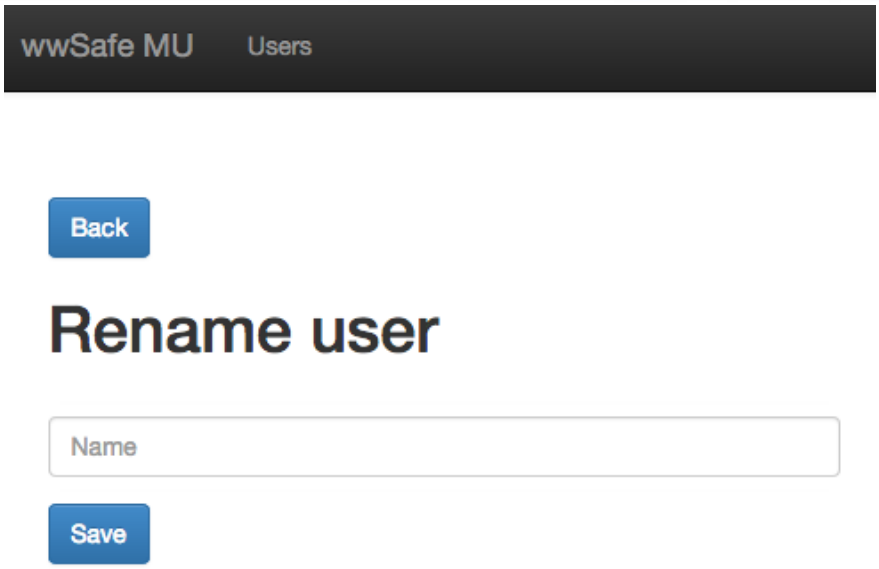
A Domain Administrator can rename users of the Domain administrated.

To rename a user

1. Connect the hardware PassKey or Mobile PassKey and log in wwSafe MU as a Domain Administrator.



2. The Users page will appear. Click a user name you want to rename.
3. The **Rename User** page will appear.



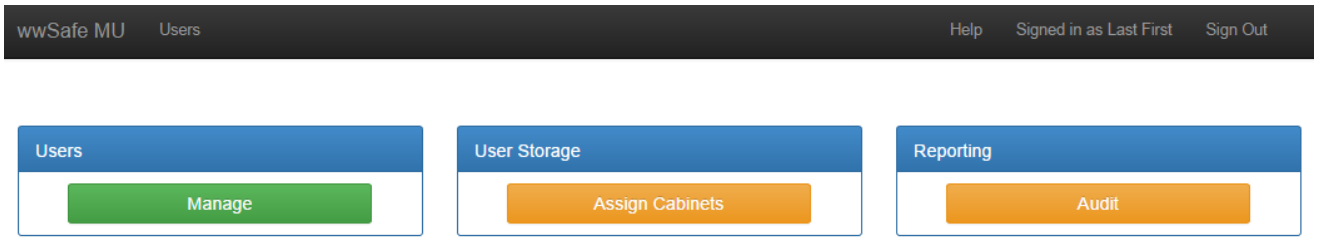
4. Enter a new user name and click the **Save** button.
5. The user has been successfully renamed.

Assign cabinet to a user

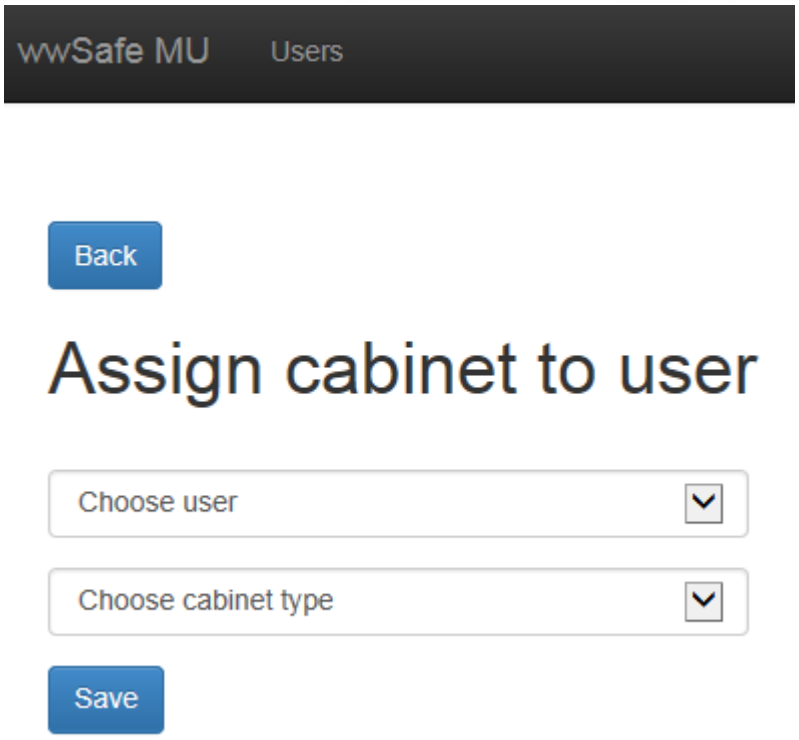
A Domain Administrator can assign a cabinet to any user of the domain administrated.

To assign cabinet to a user

1. Connect the hardware PassKey or Mobile PassKey and log in wwSafeMU as a Domain Administrator.



2. Click the **Assign Cabinets** button. The Assign cabinet to user page will appear.



3. Choose a user from the Domain administrated and a cabinet type.
4. Click the Save button.

Note: You can also assign a cabinet to a user from the Users tab. Click the **Users** tab – the **User Cabinets** button (in a row of the user you want to assign a cabinet to) – the **Assign cabinet to user** button (you will be prompted to the Assign cabinet to user page). Next follow the instructions above starting from paragraph 2.

View user cabinets

A Domain Administrator can view cabinets of users of the domains administrated.

To view user cabinets

1. Connect the hardware PassKey or Mobile PassKey and log in wwSafeMU as a Domain Administrator.
2. Click the Users tab and the Users page will appear.
3. Click the User Cabinets to view a list of cabinets.

Delete a user

A Domain Administrator can delete users from the domains administrated.

To delete a user

1. Connect the hardware PassKey or Mobile PassKey and log in wwSafe MU as a Domain Administrator.
2. Click the Users tab and the Users page will appear.
3. Click the user name you want to delete.
4. Click the **Remove** button to delete a user.

5. Click the **Remove** button to confirm.

6. The user has been successfully deleted.

Copyright © 2014 WWPass Corp. All rights reserved.
WWPass | 1155 Elm Street, Manchester, NH 03110 | Tel: +1.603.836.4932 or +1.888.997.2771 | www.wwpass.com