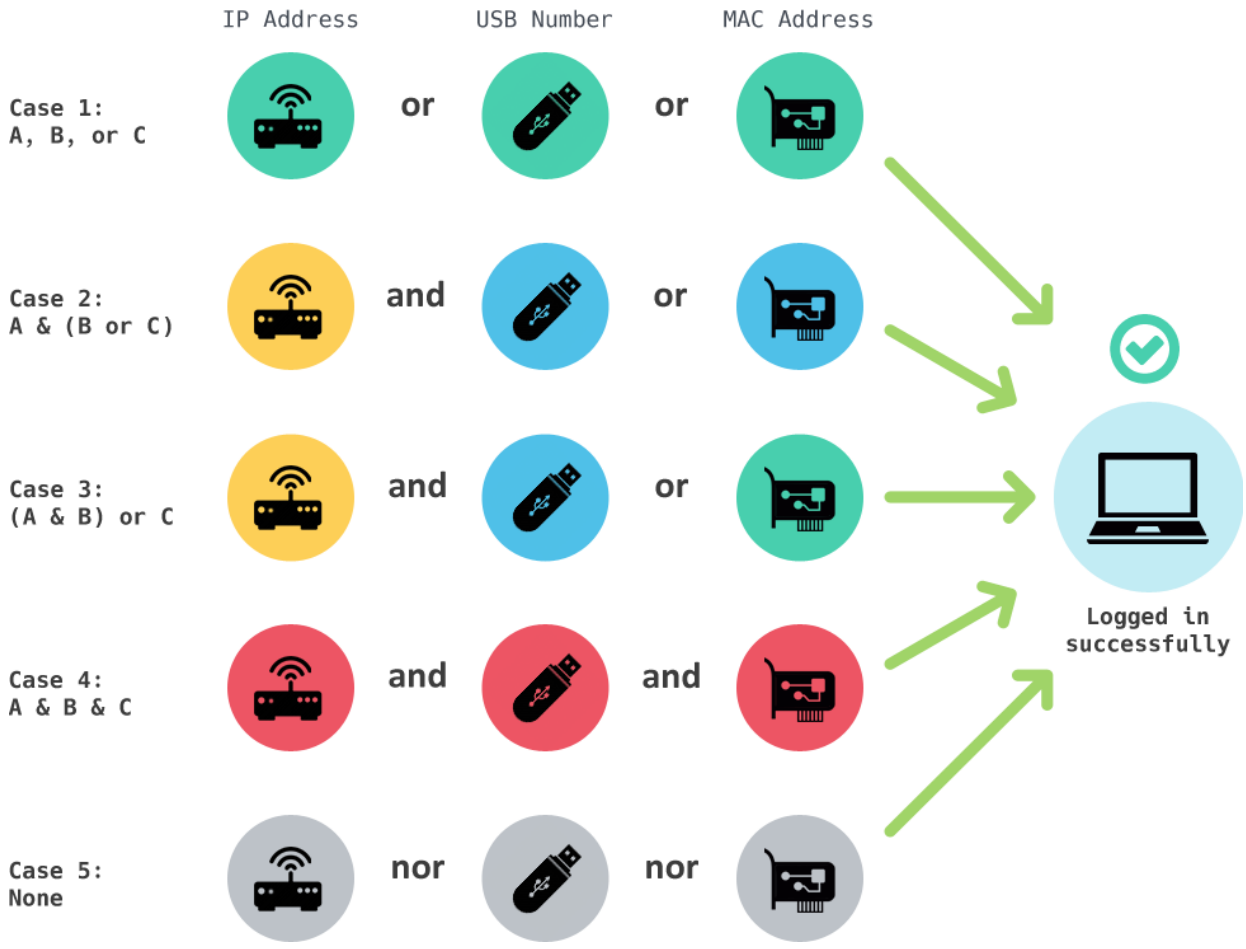
MofficeSuite – Controlling Login Access

Introduction

Corporate data security is one of the greatest concerns for businesses. How do we keep proprietary knowledge away from prying eyes in today's Cloud-based environment? MofficeSuite adds valuable security features to prevent login through various access conditions. Administrators can decide whether users must log into MofficeSuite through specific IP addresses, registered USB numbers, and/or computer MAC addresses. In addition, administrators may allow or reject logging in from all, or unregistered mobile devices. In this guide, we'll go over the duties that first administrators, then users must perform in order for the login limit system to work smoothly.

When settings up login access limitations, there are various options available for selection. Admins can include no or all conditions and from there, choose selected conditions as well as appropriate substitutions if desired. We'll get into how to set these up in the next page. In the figure below, view different cases available for login control.



Through MofficeSuite login access limitations, strengthen your company's IT security while preventing unwanted logins from outsiders.

Administrator Guide

As an administrator, you decide which login methods and options you want to enact for employees in your company. Let's go over this process step-by-step.

First, log into the **postmaster** administrator account.

From there, head to the main menu marked 🔒 **Security**.

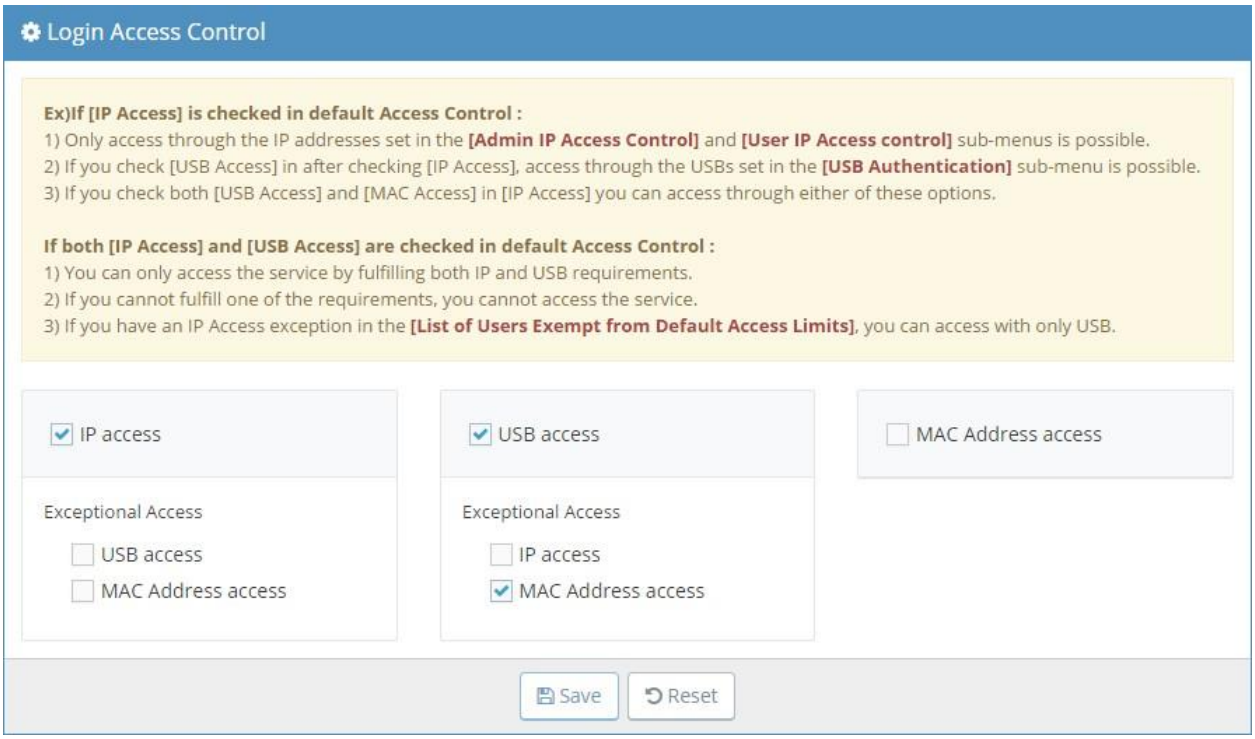
Administrator Part I. Login Access Control Sub-Menu

The first sub-menu you will be redirected to is called **Login Access Control** and this is where the administrator can decide the conditions by which access is granted to users.

In topmost module marked Login Access Control, check ☑ any of the boxes labeled IP access, USB access, or MAC Address access to respectively add that condition as a requirement to log in. When one of the main boxes is checked as a necessary requirement, the other conditions are listed as possibilities for **Exceptional Access**. Exceptional access means that the method selected at the bottom can be used as a substitute for the main condition.

In the example below, IP access and USB access are selected as required conditions. However, USB access has MAC Address access checked as a possible substitute in Exceptional Access. This means that users can use either 1) a registered IP address and USB number or 2) a registered IP address and MAC address to access MofficeSuite.

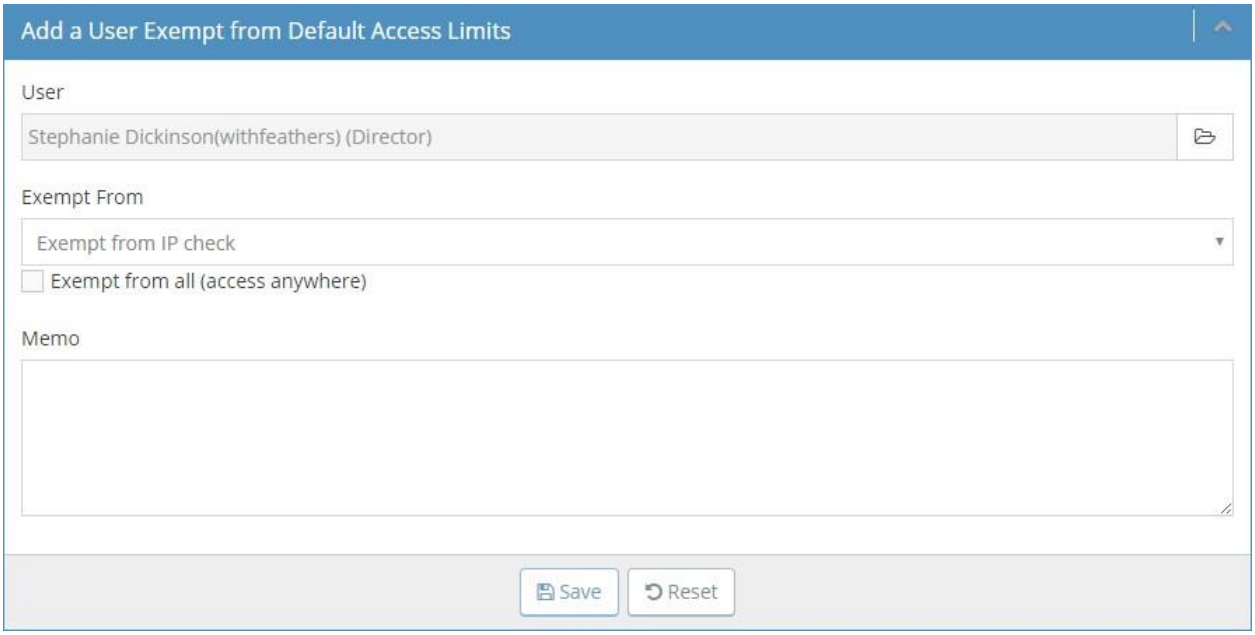
Save changes.



The bottom two modules relate to special users who are exempt from one or all restraints of login access conditions. The middle module will allow you to add a new user exception or edit an existing exempt user.

First, select a user from the Organization Chart. Then in the second field, choose to exempt them from a specific condition (IP check, USB check, or MAC address check) or check ☑ to exempt them from all conditions and allow access to MofficeSuite from anywhere.

Save changes.



In the bottommost module, view a list of exempt users and brief details about their status. Check the box ☑ next to user(s) to delete them or enable/disable their usage. To edit the exemption for the user, click the edit icon ✎ farthest to the right and their information will appear for editing in the above **Add a User Exempt from Default Access Limits** module.

Administrator Part II. Admin IP Access Control

Through the **Admin IP Access Control** sub-menu, specify IP addresses that are allowed to access the postmaster administrator account. Note that this is separate from the next sub-menu, **User IP Access Control** because the postmaster account is a separate, strictly managerial account for the software while normal users view standard collaboration menus.

By default, the postmaster administrator account can be accessed from anywhere. To limit access by IP address, simply enter the desired addresses into the field (the field automatically fills with the IP address your PC is detected to be using) and click the plus button ✚ to add it. The address will appear in the list below and access from other IPs will be rejected. To restore access from anywhere, delete all the below-listed IP addresses with the trash can 🗑 icon. Saving will occur automatically.

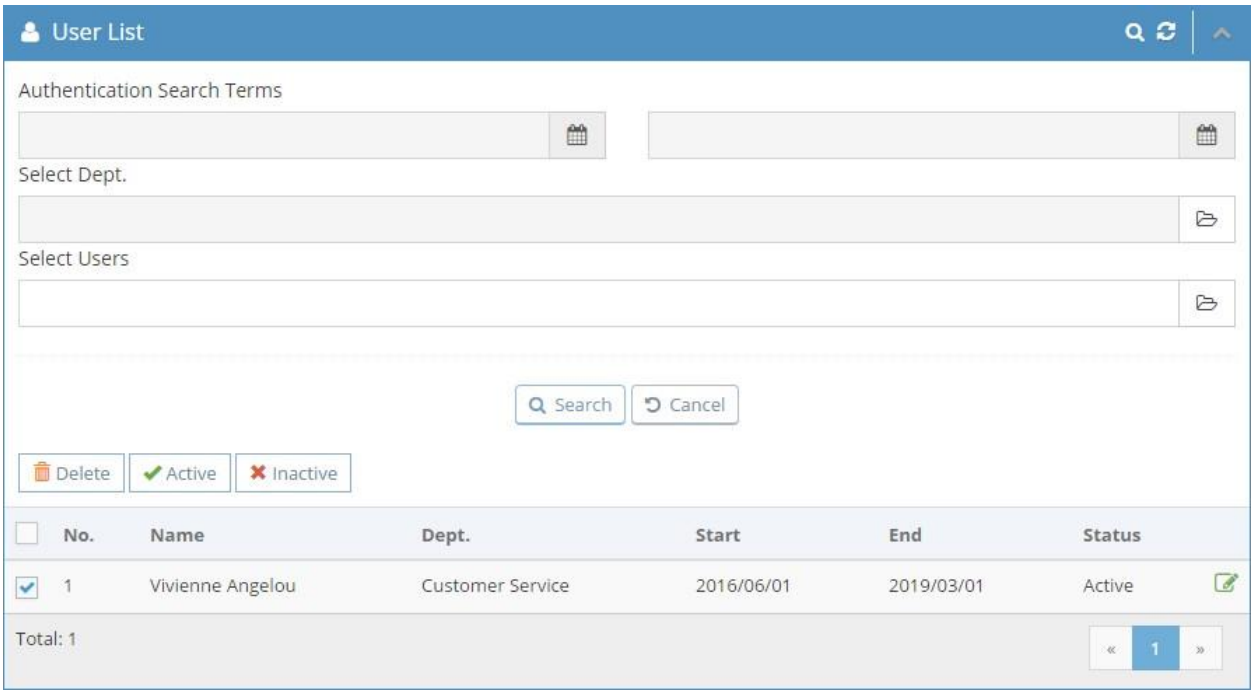
Administrator Part III. User IP Access Control

Is IP Address selected as one of your login access conditions or substitutes? Register IP Addresses for company employees using the **User IP Access Control** sub-menu.

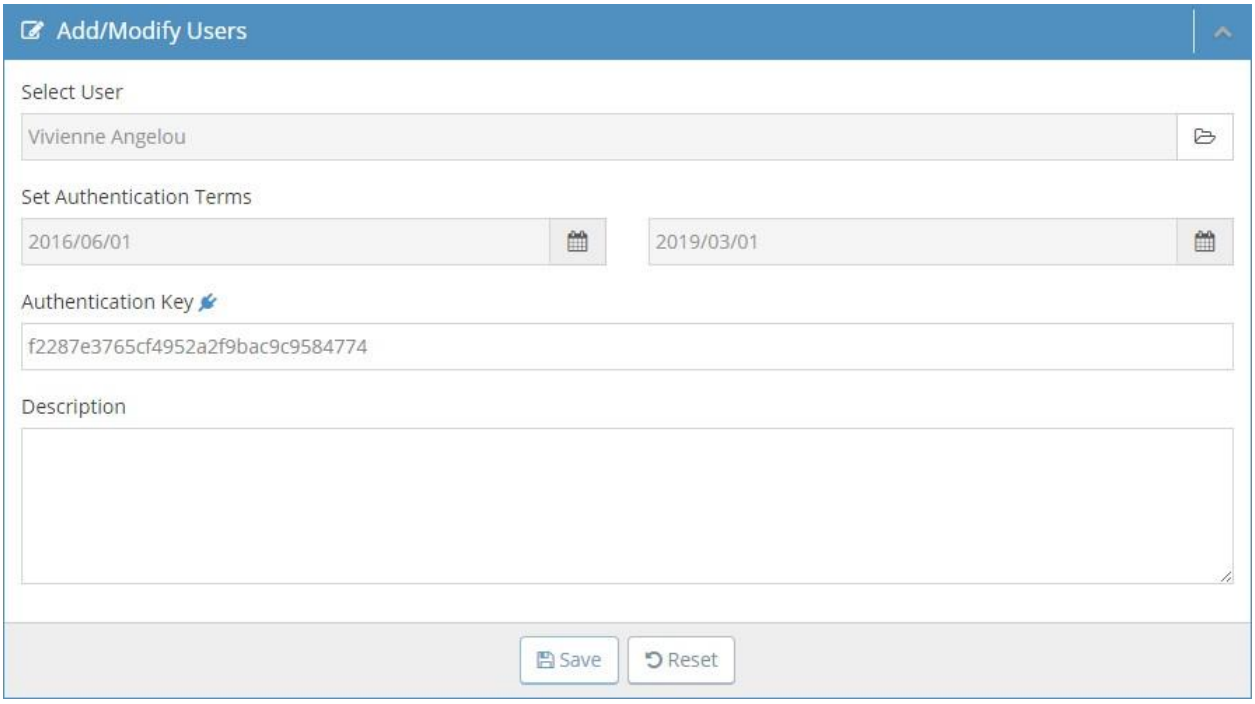
In similar fashion to the previous Admin IP Access Control sub-menu, the administrator will add approved IP Addresses in the field and add it to the list using the plus icon ✚ one at a time. Removing an address from the list can likewise be done by clicking the trash can 🗑 icon next to the IP that needs to be deleted.

Administrator Part IV. USB Authentication

Utilizing the **USB Authentication** sub-menu, administrators can approve for USB number registration requests from users. By checking the box ☑ next to a user in the upper **User List** module, delete the entry or enable/disable usage of the USB number. Click the magnifying glass 🔍 icon at the top right-hand corner to toggle fields that can be used to search for specific entries in the USB list. Fill in conditions for the USB authentication term, user's department, or user's name to start a search.

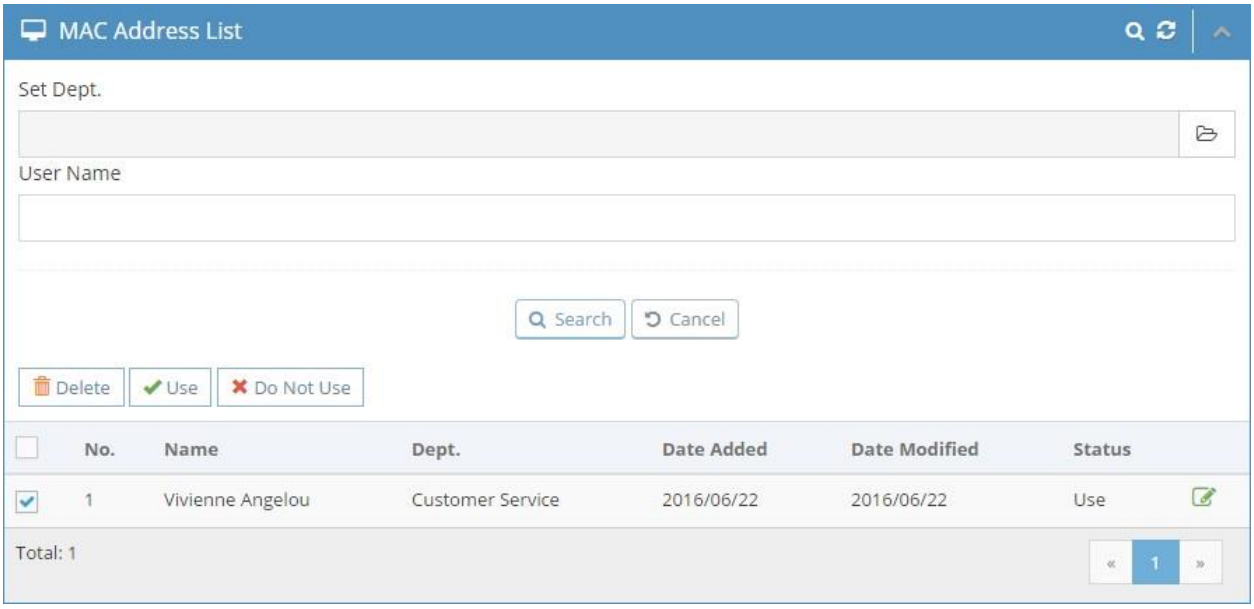


At the bottom/right module, administrators can add USB numbers manually or edit ✎ existing USB number entries. Select the user from the Organization Chart and the validity period of the USB number (authentication terms). If the user made the request, their requested USB key will appear in the field. If adding USBs manually, the unique number of the currently connected USB drive will appear as the authentication key. Make sure to save changes.

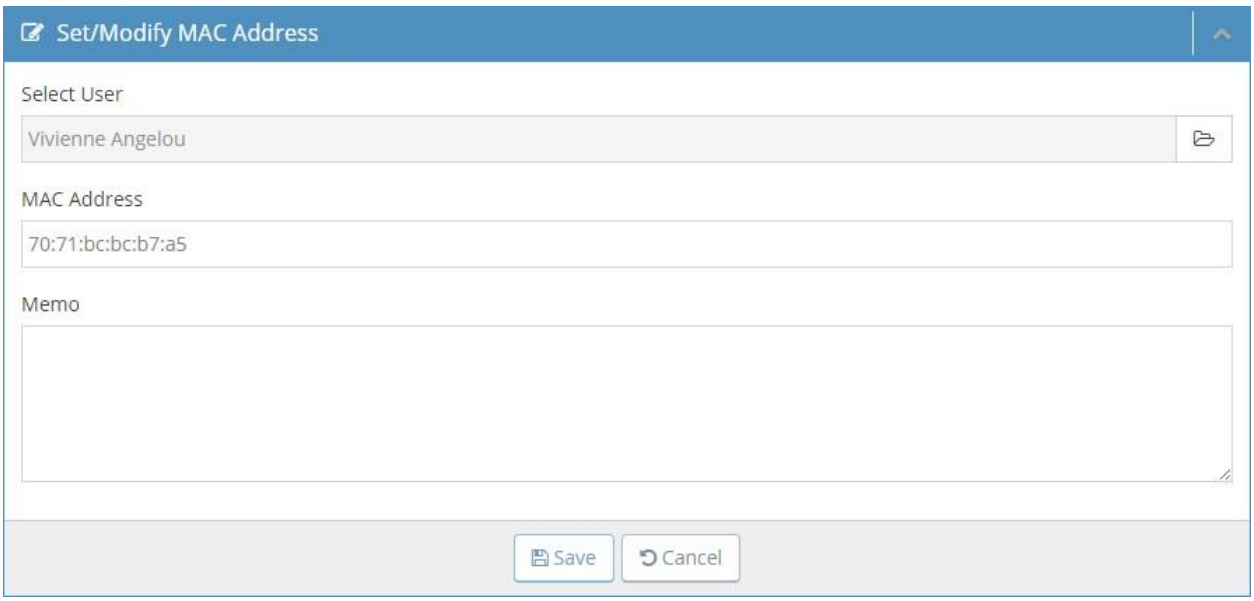


Administrator Part V. MAC Address Authentication

Similar to the previous USB Authentication sub-menu, the **MAC Address Authentication** sub-menu allows the administrator to approve and manage MAC addresses for users. In the module entitled **MAC Address List**, view a list of users who have registered or requested to register a MAC address to their account. To enable/disable a number or delete it from the list, check the box ☑ next to the name of the individual and select the desired option. The administrator can likewise look up users by department name or name by toggling the magnifying glass 🔍 icon button and entering the search fields.

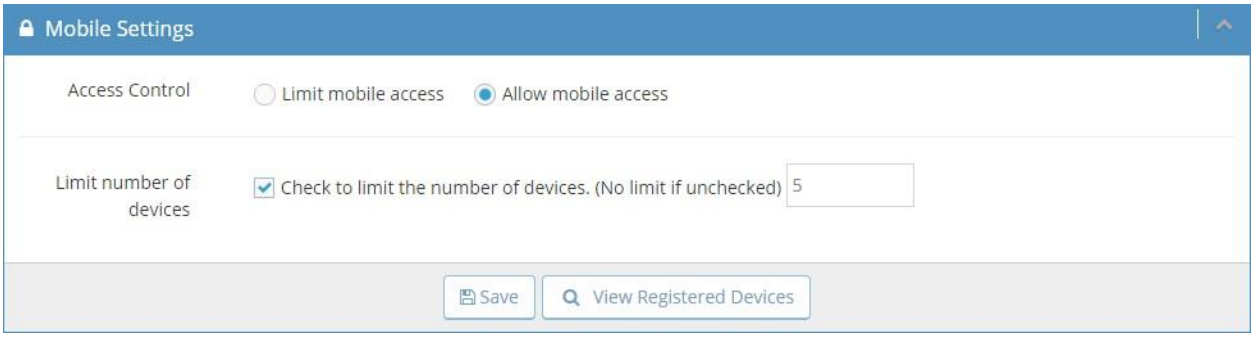


In the subsequent Set/Modify MAC Address module, either create a new MAC address or edit previous ones that were selected using the edit ✎ icon to the very right of the list entry. Herein, select users through the Organization Chart and write in the MAC address manually or view the user-requested MAC address. Remember to save changes.



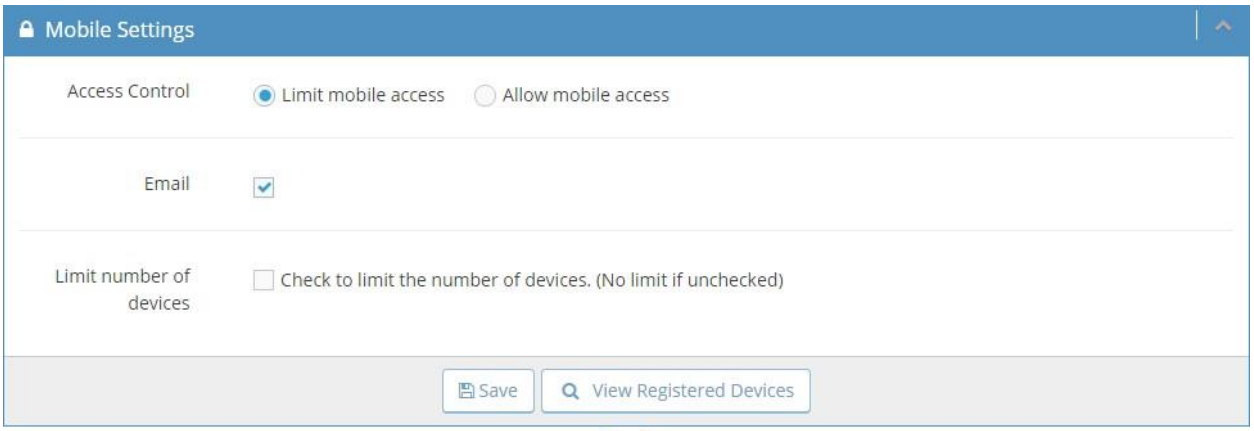
Administrator Part VI. Mobile Authentication

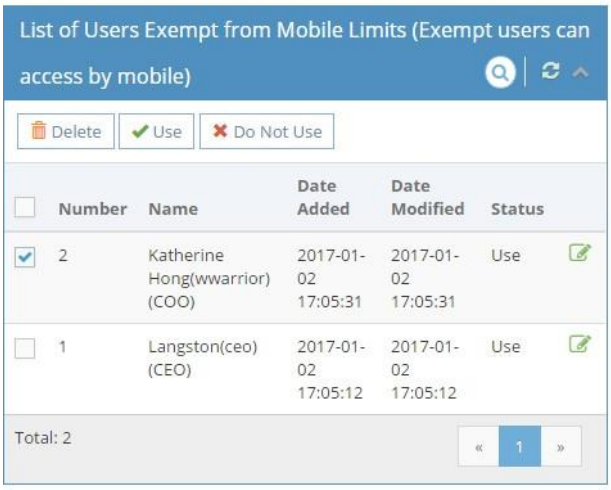
Aside from desktop login access, administrators can limit access via mobile apps through the **Mobile Authentication** sub-menu. There are two main control options that an administrator can exercise—"Access Control" to limit mobile access to devices that the user has marked as "In Use" in their respective personal settings page and "Limit number of devices" to set the maximum number of devices that a user is allowed to use. Choosing "Allow mobile access" will let users use any mobile device to log into MofficeSuite applications, the only limit being the number of devices.



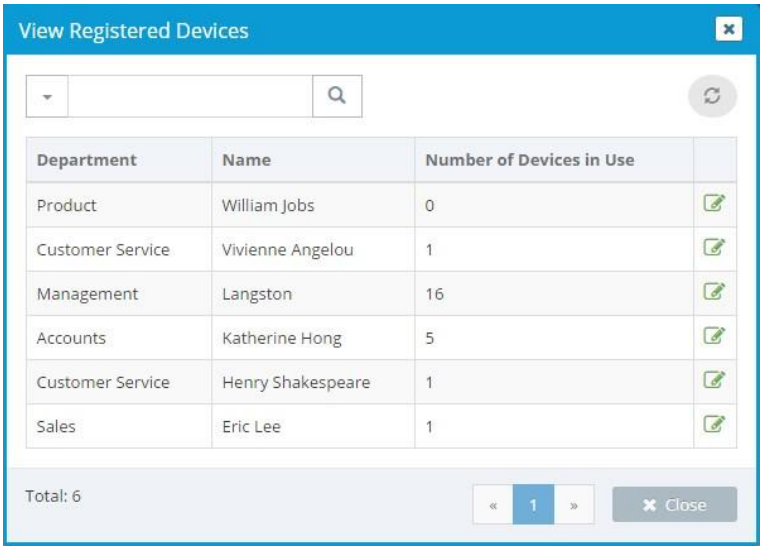
If the "Limit mobile access" option is selected, administrators can set up another option—exception users who will not be affected by mobile login limitations. To add users to the list, select a name from the Organization Chart through the **Add users who are exempt from mobile access limits** module and add the user to the list. From the list, enable/disable the user's status or delete their entry.

Note that checking ☑ the **Email** option in the **Mobile Settings** module will send an email to all company employees alerting them of the activation of limited mobile access.

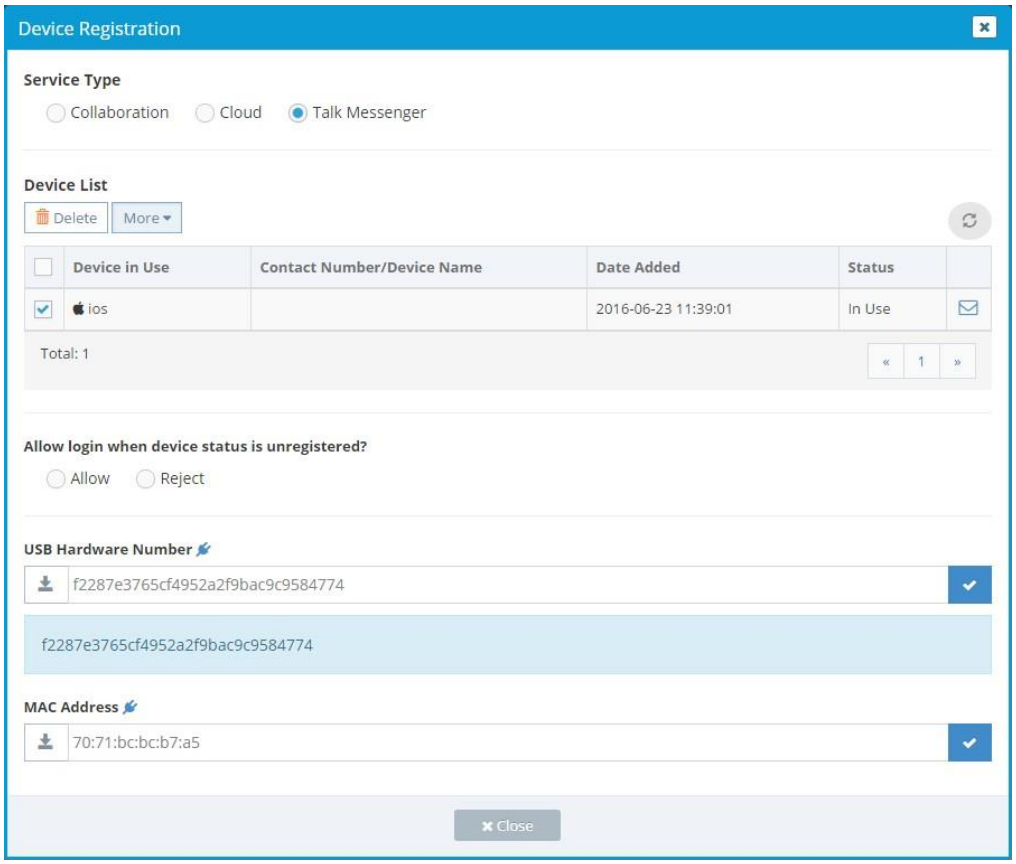




In addition to mobile limiting abilities, administrators can also confirm the mobile devices each user has added through the **View Registered Devices** button. A list of users will appear who have had at least 1 mobile login and their current number of devices in use will also be displayed.



Click on the edit icon next to a user to view more information about the user and their mobile device usage. Select a mobile application in "Service Type" to view its login history and the device status. Below that, administrators can specifically allow login/reject login for unregistered devices and check the user's USB number and MAC address.



User Guide

As a user, you are responsible for various tasks to assist administrators in login control. These actions will take place in the settings menu.

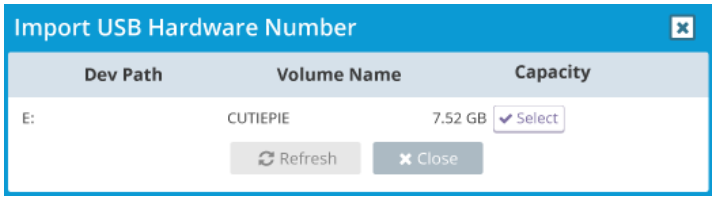
First, log into your user account. Click the down caret ▾ next to your name at the top right-hand corner. From the menu that appears, click ⚙ **Settings**. From here, we can request a USB number/MAC address to register depending on the administrator login limitations or approve mobile devices for access if mobile access is limited.

User Part I. Import USB Number & MAC Address

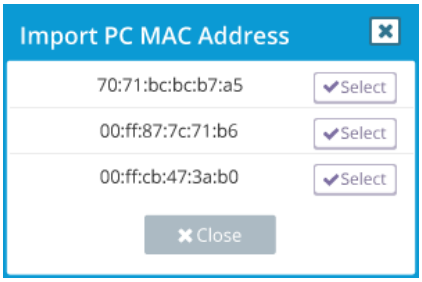
Head to the menu entitled **Groupware Setting** and scroll down to the very bottom of the page. Before you start the importing process, you'll need to install the plug-in. Press the download button next to the plug icon above the "USB Hardware Number" section. You will need to restart your browser after installing the plug-in.

After returning to the page, you're ready for import.

To select a USB number, click the **Import USB Hardware Number** button. Select a USB drive connected to your computer and hit "Select".



To get the PC MAC Address, click the **Import PC MAC Address** button. "Select" the MAC address you would like to use.



After finishing the number import process, click save. The number requests for USB and MAC address will be sent to the administrator.

User Part II. Mobile Settings

The heart of mobile limitations culminates in the **Mobile Settings** sub-menu. Herein Mobile Access, users can view which devices has connected to their account via MofficeSoft mobile applications (MofficeSuite, CloudDisk, and Talk messenger).

If an administrator set the “Limit mobile access” option, users must use the drop-down menu under the **Status** column to change the desired devices from “Unregistered” (default) to “In Use”. If not, the user will receive an error upon attempting to log into the aforementioned device and MofficeSuite will be blocked from access.

Users can thus control login access for mobile through this settings page.