



Hub Reference Guide

Untethered Labs, Inc.
support@gkaccess.com

Contents

WHAT IS THE GATEKEEPER HUB?	3
ACCESSING THE HUB DASHBOARD.....	3
ADDING THE LICENSE	5
1 DASHBOARD	8
1.1 PERSISTENT BUTTONS	8
1.2 MY PROFILE	11
2 ADMINISTRATION	13
2.1 HUB ADMINISTRATION	13
<i>Active Hub Accounts</i>	13
<i>Inactive Hub Accounts</i>	15
<i>Hub Account Roles</i>	16
<i>Licenses</i>	18
<i>Audit Information</i>	19
<i>Hub Logos</i>	19
<i>Database Information</i>	20
2.2 CLIENT ADMINISTRATION.....	20
<i>Computer Lock Screen Logo</i>	20
<i>GateKeeper Client Admin Access</i>	20
<i>Off-site Hub Access Administration</i>	22
2.3 NOTIFICATIONS (BELL ICON).....	22
3 GROUPS SETTINGS	23
3.1 ORGANIZATION.....	25
3.2 CREATING GROUPS.....	25
3.3 ADD OR REMOVE COMPUTERS IN GROUPS	29
3.4 ADDING AND REMOVING USERS IN GROUPS	29
<i>Sync Users for Organization Group</i>	29
<i>Add or Remove Users from Groups</i>	30
3.5 MANAGE GROUP SETTINGS.....	31
<i>Lock Settings</i>	31
<i>Unlock Settings</i>	33
<i>Advanced Settings</i>	36
<i>Global Settings</i>	37
4 COMPUTERS.....	38
4.1 COMPUTERS VIEW	39
4.2 GROUPS VIEW	43
4.3 DEACTIVATE COMPUTERS	44
5 USERS	46
5.1 ADD NEW USERS	47
5.2 UPDATE AD ACCOUNTS	55
6 ALERTS	57

	<i>User Alerts</i>	58
	<i>System Alerts</i>	66
7	REPORTS	68
8	LOGS	72
	<i>Client Logs</i>	72
	<i>Server Logs</i>	73
	<i>Alert Logs</i>	73
9	SCANS	74
10	APPLICATIONS	75
11	FREQUENTLY ASKED QUESTIONS (FAQS)	75
11.1	SERVER SETUP	75
	<i>How can I check if the GateKeeper server is installed on my local machine?</i>	75
	<i>How can I obtain the IP address of the computer with the GateKeeper server installed?</i>	76
11.2	ACCOUNT MANAGEMENT	76
	<i>Why do I need a license?</i>	76
	<i>Where can I find my licenses?</i>	76
	<i>How do I upload a license?</i>	77
	<i>How can I grant another user permission to access the dashboard?</i>	78
11.3	USER MANAGEMENT	79
	<i>What to do if a user loses their GateKeeper token?</i>	79
	<i>What if a user comes in to work without their GateKeeper token?</i>	80
11.4	LOGS	80
	<i>What happens to the logs if a computer is not connected to the server?</i>	80
12	ABOUT	80

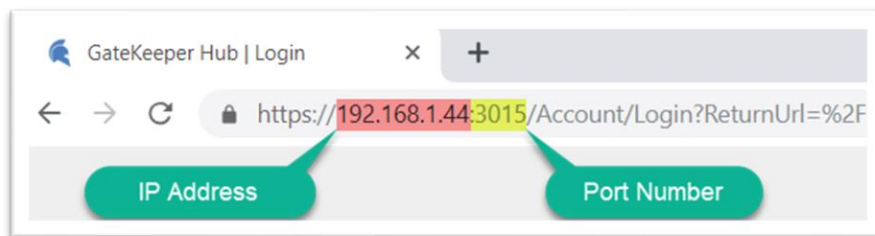
What is the GateKeeper Hub?

The GateKeeper Hub is your personal command center that allows you, as a GateKeeper administrator, to implement policies on the GateKeeper network. Once installed, the GateKeeper Hub dashboard can be accessed from any computer on your network. It gives admins the ability to

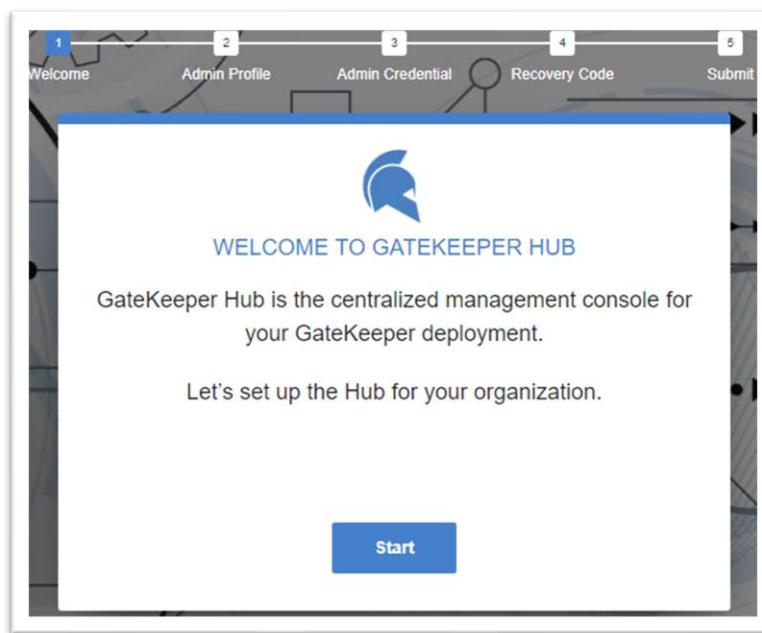
- Push global settings on all client computers
- Create high-security or convenience zones for users
- Generate detailed audit reports for compliance regulations
- Manage access control on all client computers
- Real-time tracking of all GateKeeper users

Accessing the Hub Dashboard

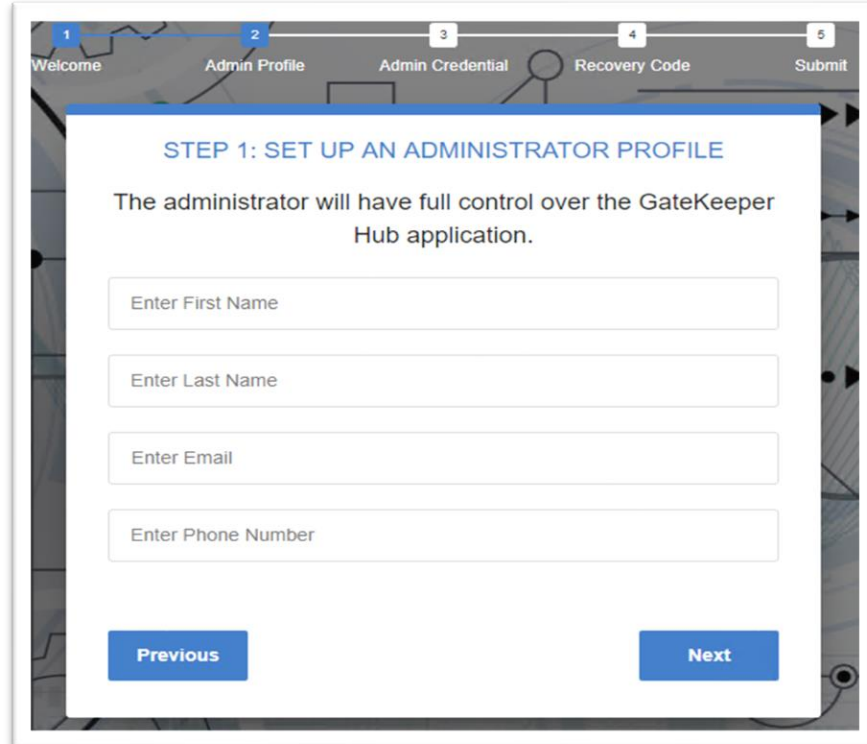
Open Google Chrome web browser (which is our recommended browser) and on the address bar, type “https://<IP Address of the GateKeeper Server>:<Port Number>”. Example for the IP Address and Port Number are provided in screenshot below. If it is the same machine:



As the **Dashboard** is starting up, you will be prompted to view a few introductory steps to get things going. When the dashboard loads for the first time, click **Start** to begin the registration process.

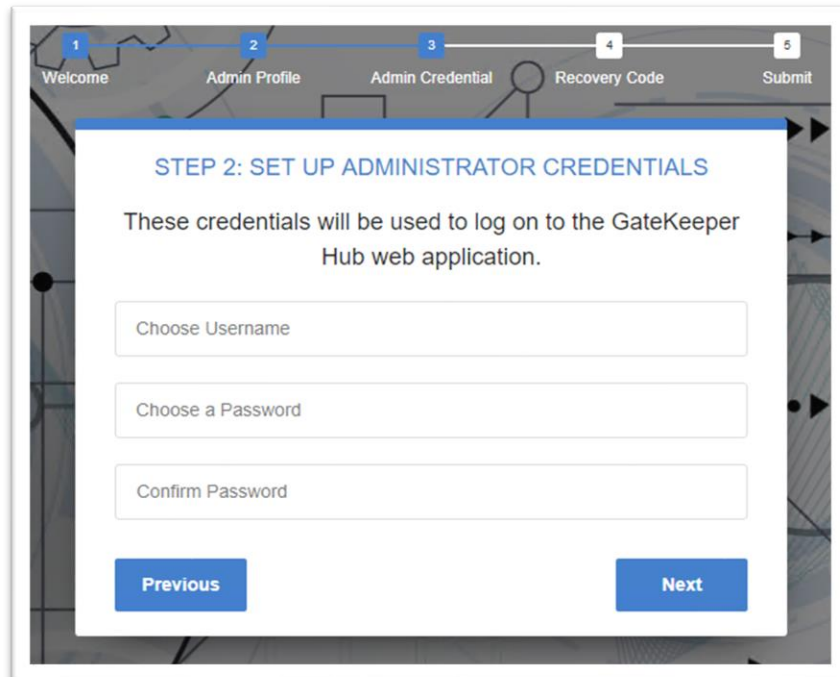


In **Step 1**, enter first name, last name, email, phone number, then click **Next**.



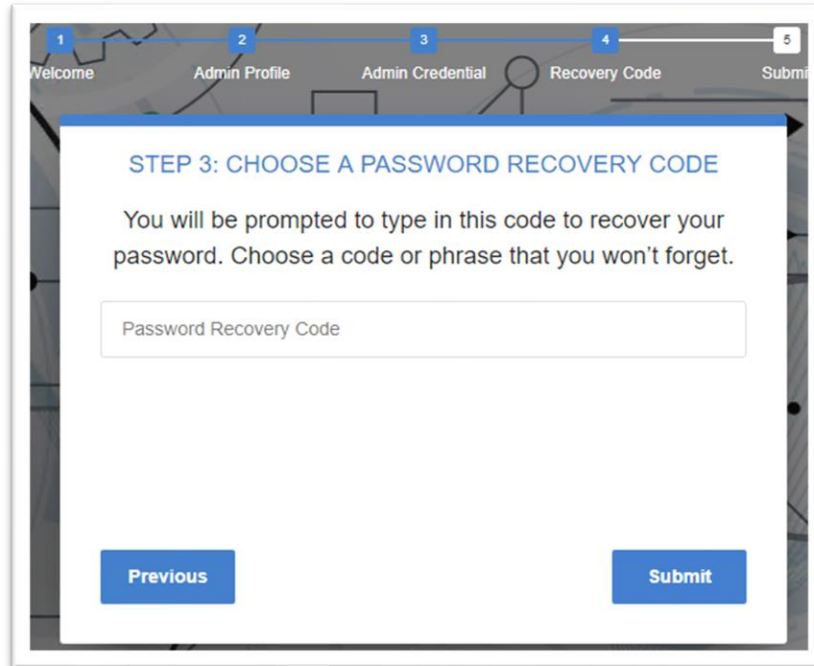
The screenshot shows a web interface for setting up an administrator profile. At the top, a progress bar indicates five steps: 1 (Welcome), 2 (Admin Profile), 3 (Admin Credential), 4 (Recovery Code), and 5 (Submit). Step 2 is currently active. The main heading is "STEP 1: SET UP AN ADMINISTRATOR PROFILE". Below it, a subheading states: "The administrator will have full control over the GateKeeper Hub application." There are four text input fields: "Enter First Name", "Enter Last Name", "Enter Email", and "Enter Phone Number". At the bottom, there are two blue buttons: "Previous" on the left and "Next" on the right.

In **Step 2**, create a username and password to log in as the GateKeeper administrator.



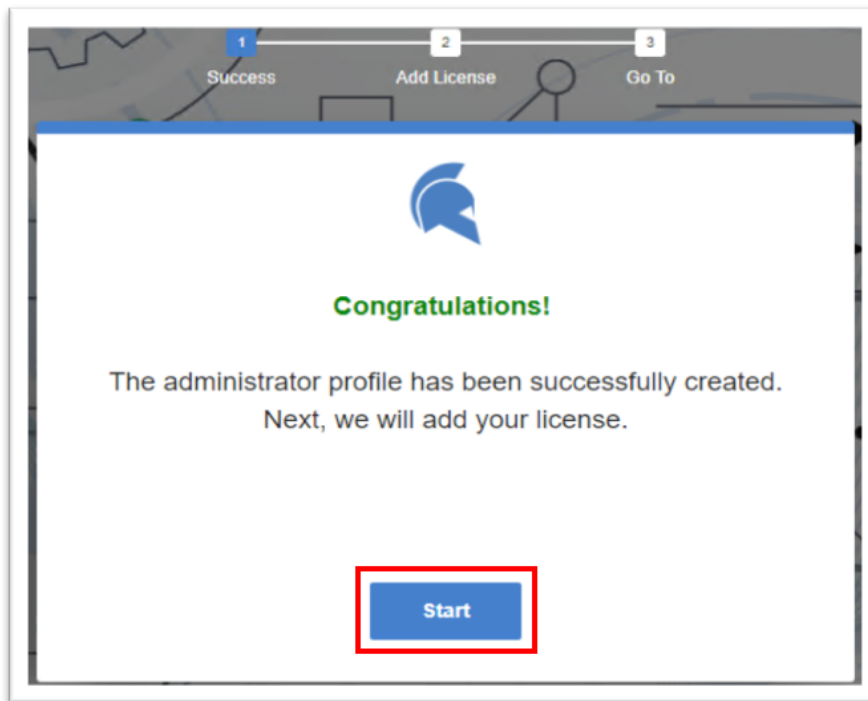
The screenshot shows a web interface for setting up administrator credentials. At the top, a progress bar indicates five steps: 1 (Welcome), 2 (Admin Profile), 3 (Admin Credential), 4 (Recovery Code), and 5 (Submit). Step 3 is currently active. The main heading is "STEP 2: SET UP ADMINISTRATOR CREDENTIALS". Below it, a subheading states: "These credentials will be used to log on to the GateKeeper Hub web application." There are three text input fields: "Choose Username", "Choose a Password", and "Confirm Password". At the bottom, there are two blue buttons: "Previous" on the left and "Next" on the right.

In **Step 3**, choose a **Password Recovery Code** to retrieve your forgotten password. Click **Submit**.

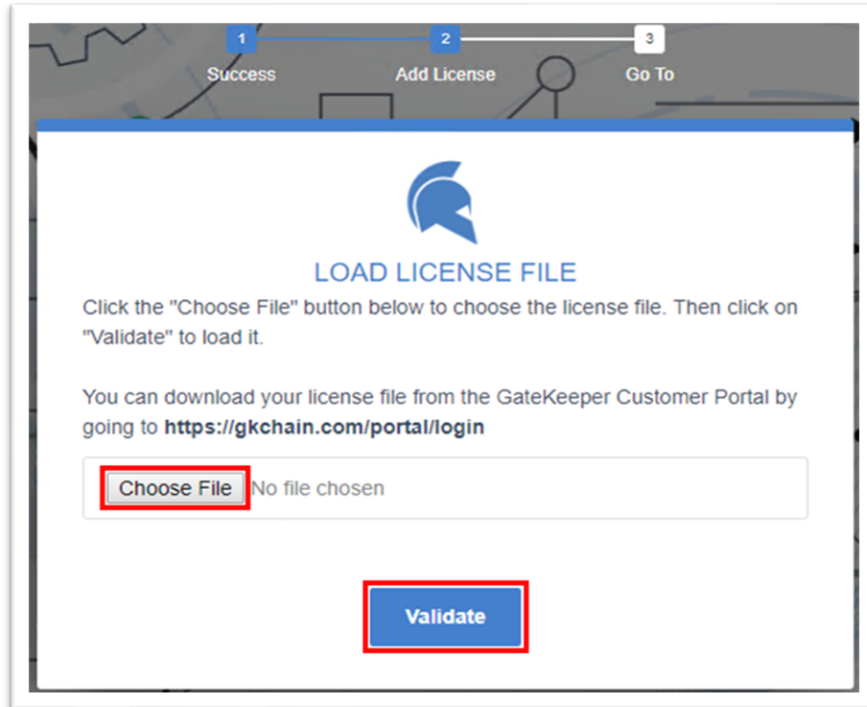


Adding the License


Congratulations! You have successfully created your administrator profile. In order to activate GateKeeper Hub, a user must upload their purchased license. Click **Start**.



Click **Choose File** and select the license file that you downloaded after purchase. Click **Validate**.



1 Success 2 Add License 3 Go To



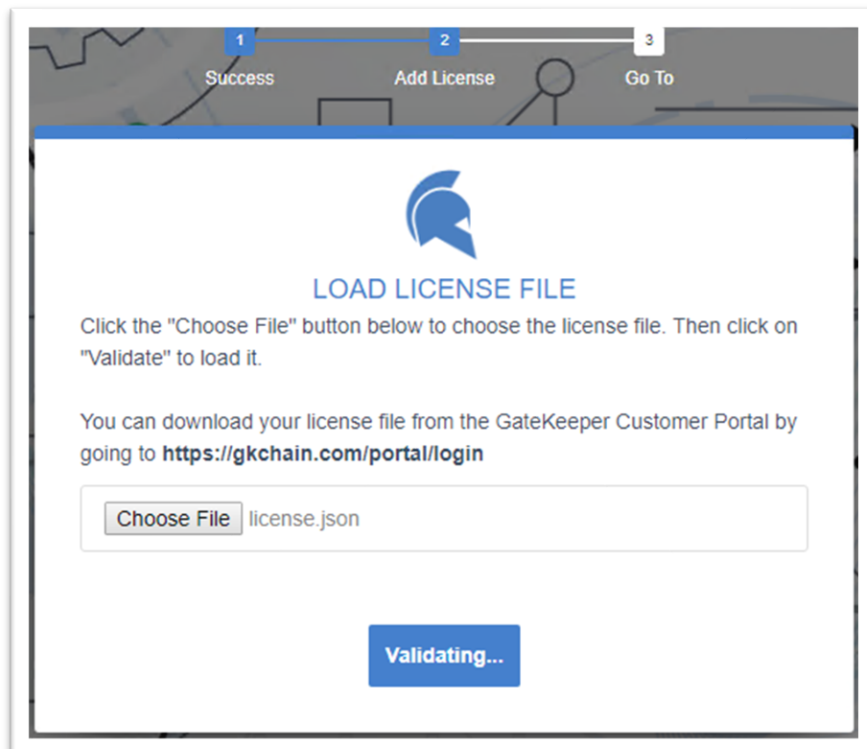
LOAD LICENSE FILE

Click the "Choose File" button below to choose the license file. Then click on "Validate" to load it.


You can download your license file from the GateKeeper Customer Portal by going to <https://gkchain.com/portal/login>

Choose File No file chosen

Validate



1 Success 2 Add License 3 Go To



LOAD LICENSE FILE

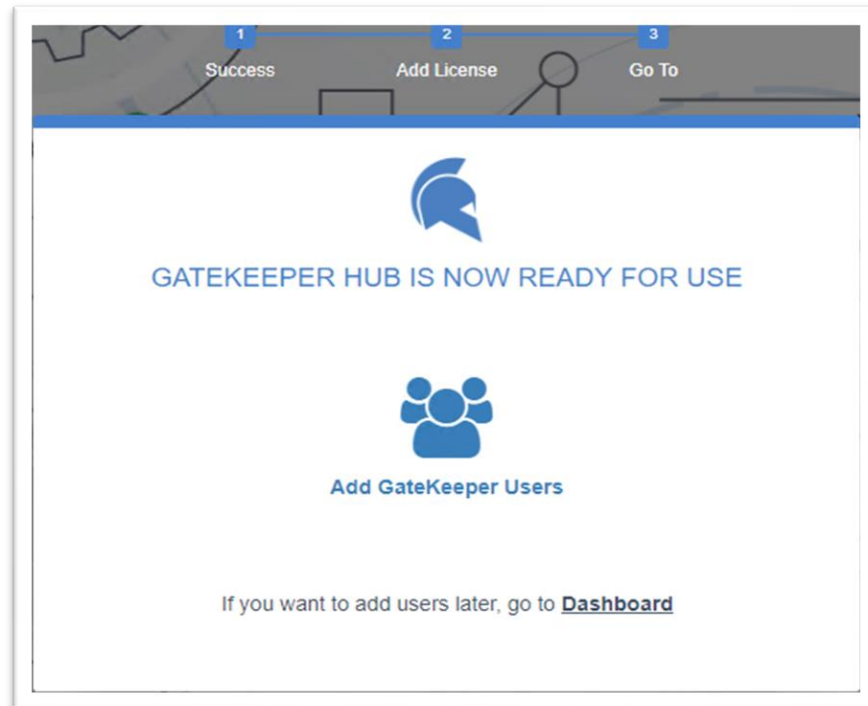
Click the "Choose File" button below to choose the license file. Then click on "Validate" to load it.

You can download your license file from the GateKeeper Customer Portal by going to <https://gkchain.com/portal/login>

Choose File license.json

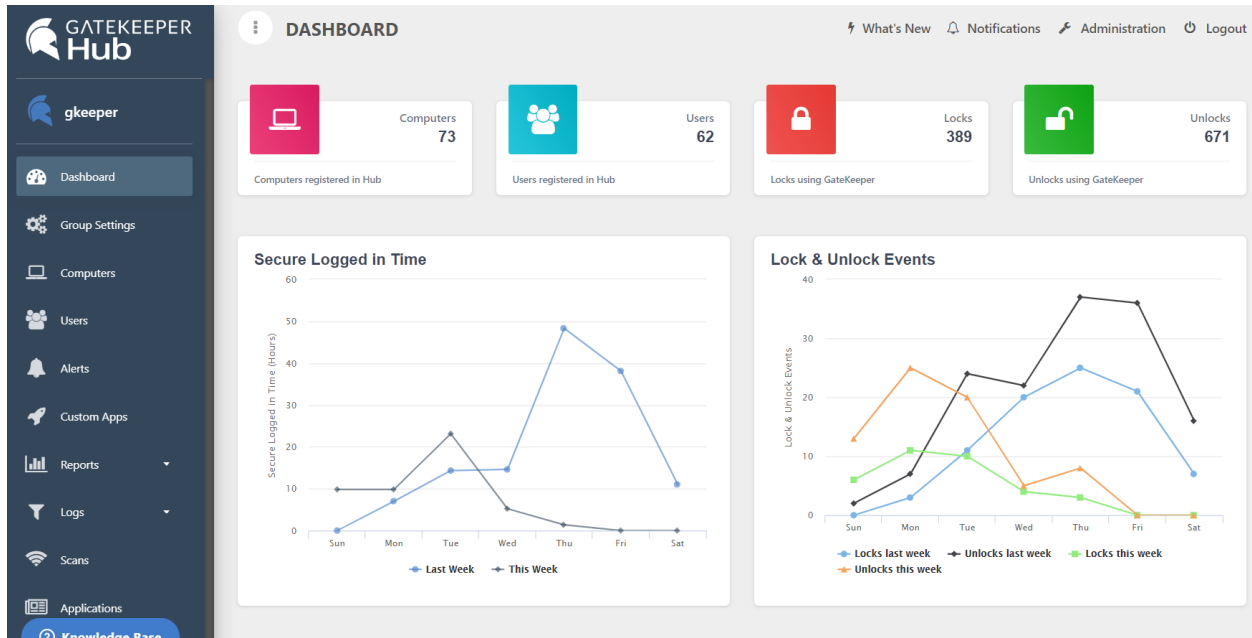
Validating...

Once the license is validated, GateKeeper Hub will be available for use.



1 Dashboard

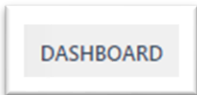
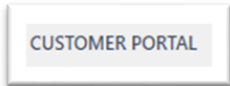

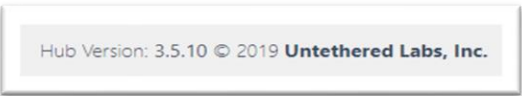
The **Dashboard** page provides an overview of GateKeeper activity on your network. Provided below is a breakdown of all components and screenshot of the **Dashboard** page.









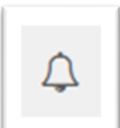


1.1 Persistent Buttons

There are clickable elements and links that exist on every page view in the Hub.

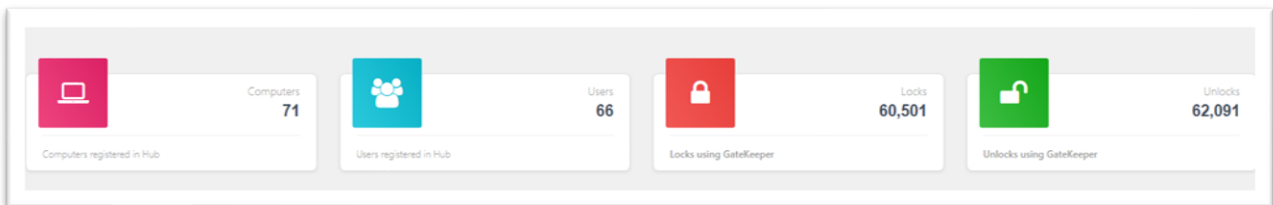


	The link redirects the user to the Dashboard page.
	The link sends the user to the GateKeeper Customer Portal website.
	The Support link opens the user's default email program to contact the GateKeeper support team.
	The Untethered Labs, Inc. link sends the user to the GateKeeper homepage.

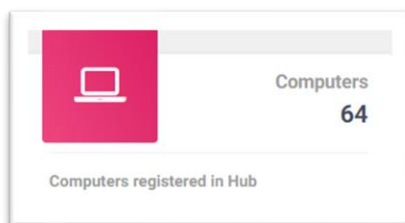
At the top of most pages are the following buttons.

 DASHBOARD	 What's New  Notifications  Administration  Logout
	What's New: The lightning icon shows the latest updates to the GateKeeper solution.
	Notifications: The bell icon - view and manage all notifications. From the dropdown menu, users can click any notification to go to the related page. This will be elaborated more in the Bell icon section of this document.
	Administration: The wrench icon. This page includes other sections such as Hub Administration and Client Administration . These sections are explained in the Administration section of this document.
	Logout: Clicking the power button icon will log the user out of the GateKeeper Hub.

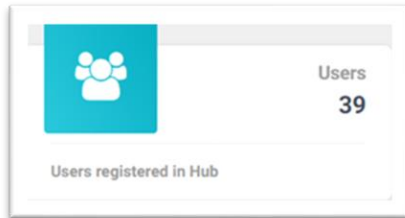
The status bar is located on top of the **Dashboard** page.



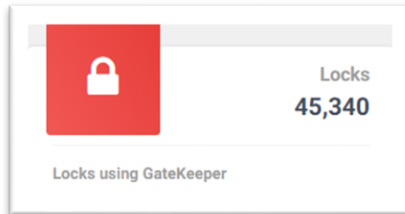
These four views provide real-time information on how many **Computers** are currently registered to Hub, **Users** currently registered to Hub, **Locks** and **Unlocks** being performed using GateKeeper Hub. The numbers change according to the usage of the application.



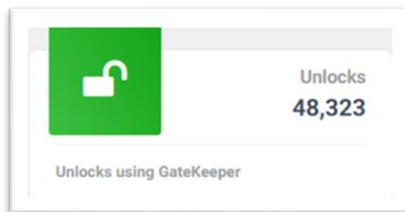
'**Computers**' shows how many computers are registered on the hub. Click to navigate to the **Computers** page.



'Users' shows how many users are registered on the Hub. Click to navigate to the **Users** page.



'Locks' shows how many auto-locks have been performed using GateKeeper.



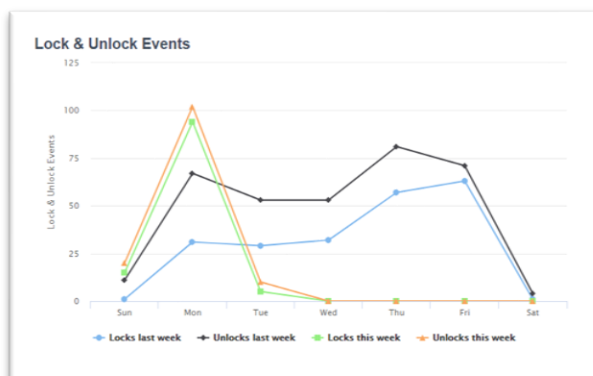
The **Unlocks** status view shows how many unlocks have been performed using GateKeeper.

Dashboard page also shows a summary of your weekly and monthly GateKeeper activity analytics.



Secure Logged in Time

This display shows the organization's GateKeeper activity of secured sessions each day of the week. When the user hovers their mouse over the data points, information will be displayed in hours.



Lock & Unlock Events

Shows the organization's GateKeeper lock and unlock activity for the past and current week.

Computers Activity: This section keeps track of how actively users are using their GateKeeper tokens to log in and log out of each computer. The list displays each computer's name with **Total Sessions**, **Total Time**, **Sessions Today**, and **Time Today**. Users can view past data with the calendar option.

Users Activity: This section keeps track of how actively users are using their GateKeeper tokens to lock and unlock computers. The list displays each users name with **Total Sessions**, **Total Time**, **Sessions Today**, and **Time Today**. Users can view past data with the calendar option.

Computers Activity 2019-12

Computer	Total Sessions	Total Time (hrs)	Sessions Today	Total Time Today (hrs)
SVP-DESKTOP	19	69.50	0	0.00
UL-LAPTOP-06	9	76.63	0	0.00
SVP-LAPTOP-02	7	160.64	1	0.28
99	0	0.00	0	0.00
999	0	0.00	0	0.00

1-5 of 73 items < 1 2 3 4 5 ... 15 > 5 / page

Users Activity 2019-12

User	Total Sessions	Total Time (hrs)	Sessions Today	Total Time Today (hrs)
Siddharth Potbhare	27	234.92	1	0.28
Sai Vaddi	9	76.75	0	0.00
Abe Kim	0	0.00	0	0.00
Abhinav	0	0.00	0	0.00
Abhinav Jain	0	0.00	0	0.00

1-5 of 50 items < 1 2 3 4 5 ... 10 > 5 / page



Clicking the GateKeeper Hub icon will redirect to the [Dashboard](#).

Clicking your username will open 'Your Account' page.

1.2 My Profile


On the **Profile** tab, users can change profile picture, username, name, email address, and number, and option to receive monthly GateKeeper activity email reports.

GATEKEEPER Hub


gkeeper

- Dashboard
- Group Settings
- Computers
- Users
- Alerts
- Custom Apps
- Reports
- Logs
- Scans
- Applications


YOUR ACCOUNT



PROFILE




PASSWORD



ROLES

Username
gkeeper



First Name
GateKeeper

Last Name
Hub

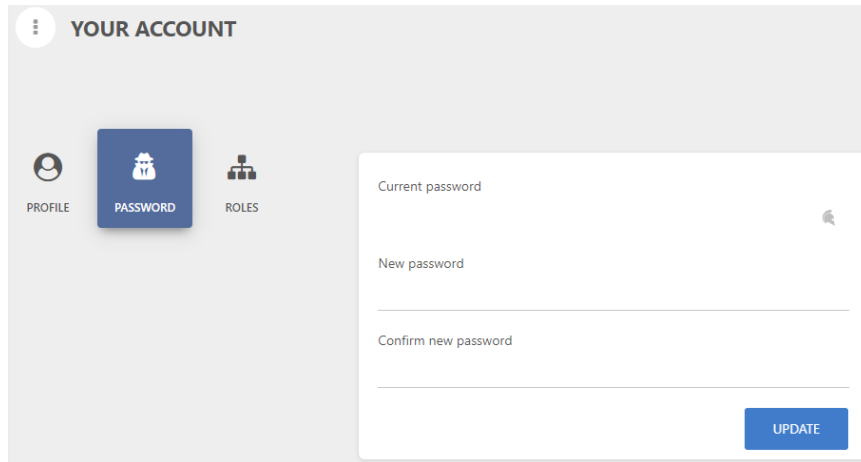
Email
siddharth@ulabs.io

Phone number
2026766486

☒ Email me my Monthly Report

SAVE

On the **Password** tab, update current password and choose a code to recover their password.



YOUR ACCOUNT

PROFILE **PASSWORD** ROLES

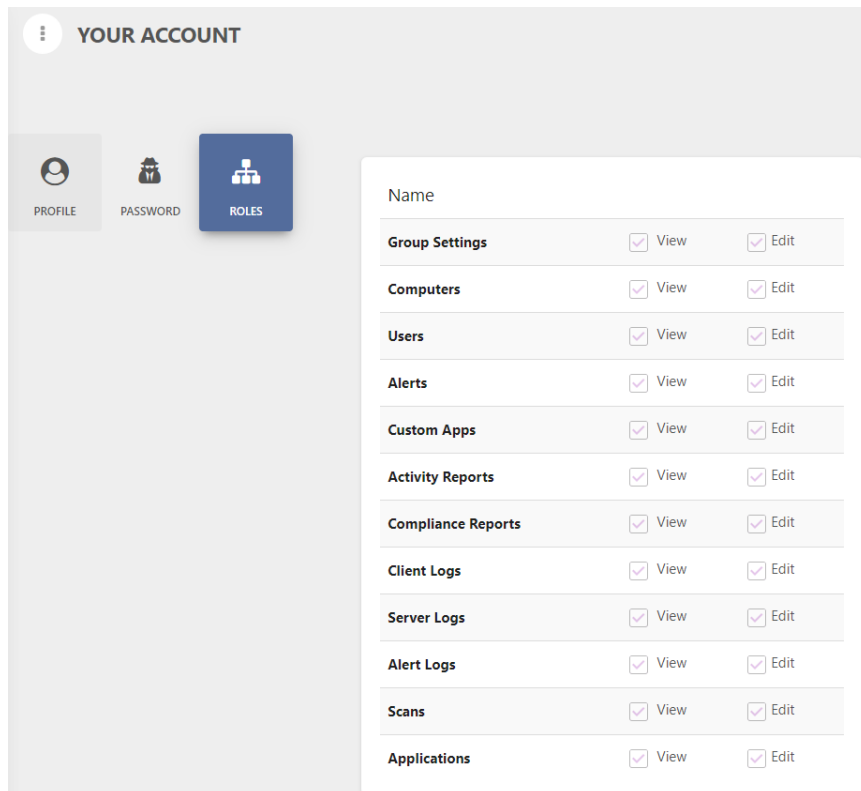
Current password

New password

Confirm new password

UPDATE

The **Roles** tab shows what settings and features the current user can manage within the Hub.



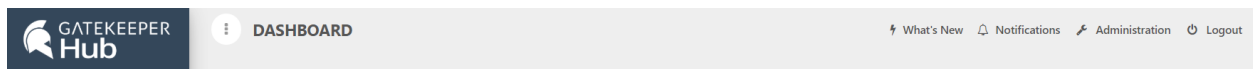
YOUR ACCOUNT

PROFILE PASSWORD **ROLES**

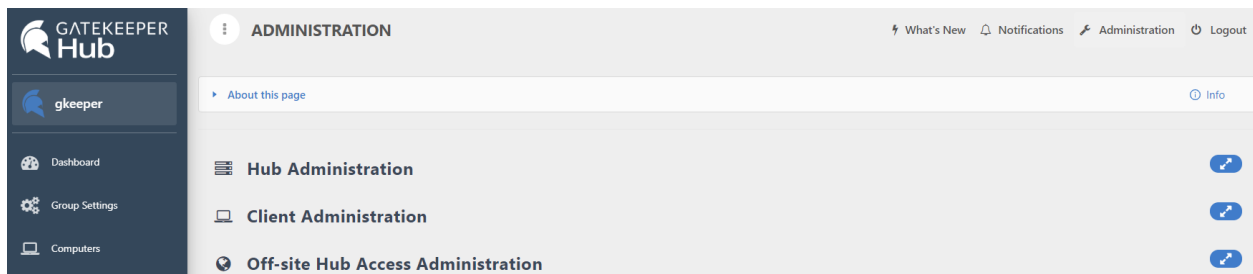
Name		
Group Settings	<input checked="" type="checkbox"/> View	<input checked="" type="checkbox"/> Edit
Computers	<input checked="" type="checkbox"/> View	<input checked="" type="checkbox"/> Edit
Users	<input checked="" type="checkbox"/> View	<input checked="" type="checkbox"/> Edit
Alerts	<input checked="" type="checkbox"/> View	<input checked="" type="checkbox"/> Edit
Custom Apps	<input checked="" type="checkbox"/> View	<input checked="" type="checkbox"/> Edit
Activity Reports	<input checked="" type="checkbox"/> View	<input checked="" type="checkbox"/> Edit
Compliance Reports	<input checked="" type="checkbox"/> View	<input checked="" type="checkbox"/> Edit
Client Logs	<input checked="" type="checkbox"/> View	<input checked="" type="checkbox"/> Edit
Server Logs	<input checked="" type="checkbox"/> View	<input checked="" type="checkbox"/> Edit
Alert Logs	<input checked="" type="checkbox"/> View	<input checked="" type="checkbox"/> Edit
Scans	<input checked="" type="checkbox"/> View	<input checked="" type="checkbox"/> Edit
Applications	<input checked="" type="checkbox"/> View	<input checked="" type="checkbox"/> Edit

2 Administration

To access, click **Administration** (wrench icon) in the upper-right corner of the Hub Dashboard.



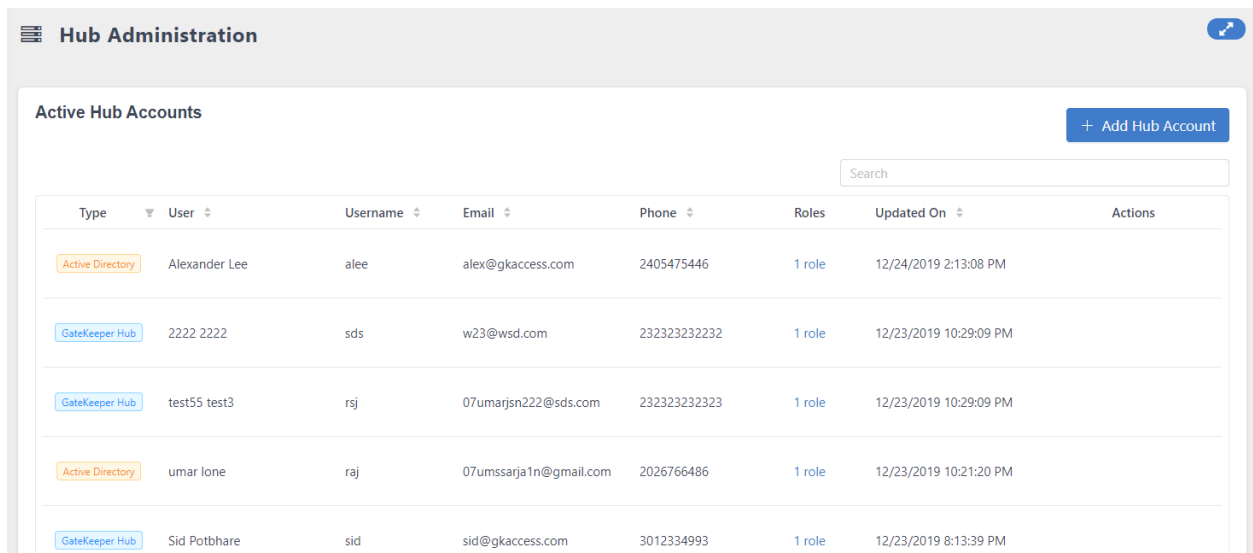
Administration page: admins can manage other Hub users, upload licenses and logos, define admin roles, stop/start data collection, change Lock Screen logo, and control Client Admin Access.



2.1 Hub Administration



Active Hub Accounts



Administrators can add new Hub admin users by clicking **+ Add Hub Account**.

This will bring up the **'Add Hub Accounts'** page. Enter the user's information.

Add Hub Accounts Info X

Profile Credentials Summary

Add from Active Directory

First Name	Last Name	Email	Phone Number	Roles	Actions
<input type="text" value="James"/>	<input type="text" value="Holden"/>	<input type="text" value="james.holden@gkaccess.o"/>	<input type="text" value="2405475446"/>	Select	Remove

+ Add Row

Enter user's credentials.

Add Hub Accounts Info X

Profile Credentials Summary

Account Type	Username	Password	Confirm Password	Actions
GateKeeper Hub	<input type="text" value="jholden"/>	<input type="password" value="....."/>	<input type="password" value="....."/>	Remove

Add Hub Accounts Info X

Profile Credentials Summary

Verify and Save Hub Accounts

First Name	Last Name	Username	Email	Phone Number	Account Type
James	Holden	jholden	james.holden@gkaccess.com	2405475446	GateKeeper Hub

Save Hub Accounts

Click **Save Hub Accounts**.

Administrators can also manage other existing Hub accounts.

Email	Phone	Roles	Updated On	Actions
abrahak@g.clemson.edu	4437833034	1 roles	11/1/2019 12:37:24 PM	Manage Deactivate

The 'Update Hub Account' window will appear. The administrator can edit roles, change their Password Recovery Code, change their password, and schedule a monthly email report.

Manage Hub Account: Alexander Lee

Info X

Username: alee

Type: Active Directory

Password: Password

Confirm Password: Confirm Password

Roles: 1 role selected

Monthly Report: ☒ Subscribed


Click **Update Account** when done editing.

Inactive Hub Accounts

From the 'Active Hub Accounts' section, administrators can **Deactivate** Hub accounts.

User	Username	Email	Phone	Roles	Updated On	Actions
Test Test	Test	abrahak@g.clemson.edu	4437833034	1 roles	11/1/2019 12:37:24 PM	Manage Deactivate

A prompt will pop up to confirm the action.


Do you want to deactivate Hub Account for Test Test?

GateKeeper Hub access for the user will be removed.

The account will then appear in the 'Inactive Hub Accounts' section.

Inactive Hub Accounts							
							<input type="text" value="Search"/>
Type	User	Username	Email	Phone	Roles	Added On	Actions
GateKeeper Hub	xasdasd asdasdas	dfgfdgdfgdf8			1 role	11/13/2019 5:42:54 PM	
GateKeeper Hub	User Test	harris	harris@gman.com	3213213221	1 role	8/19/2019 5:58:32 PM	
GateKeeper Hub	Kyle Sullivan	kyle	kyle@gkaccess.com	2405475446	1 role	8/5/2019 11:57:47 AM	

To reactivate the Hub account, hover over the desired account, and then click **Activate**.

GateKeeper Hub	Kyle Sullivan	kyle	kyle@gkaccess.com	2405475446	1 role	8/5/2019 11:57:47 AM	Activate
----------------	---------------	------	-------------------	------------	--------	----------------------	----------

Hub Account Roles

The different roles for your Hub server will be located here.

Hub Account Roles			
			<input type="text" value="Search"/>
Name	Description	Actions	
Administrator	Complete read and write access to all aspects of GateKeeper Hub		
Limited-User	Read access to all aspects of GateKeeper Hub		
Test	test		

To add new roles, click **Add Role**.

Hub Account Roles

Add Role

Enter in a name and description for the role. Once you have finished, click **Next**.

Create a Role

Information

Permissions

Summary

Name:

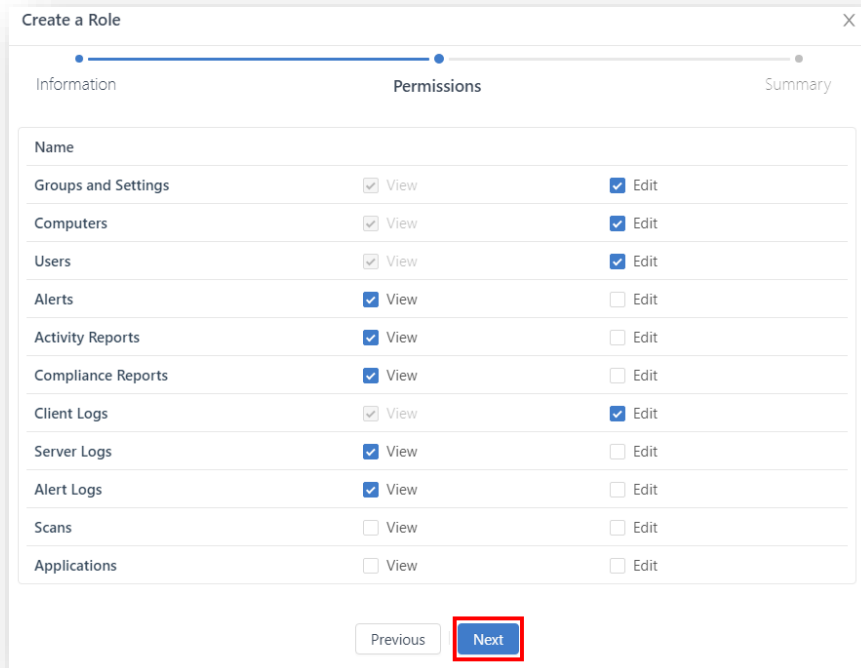
Test Guide

Description:

Example Role for Hub Guide

Next

Assign the permissions and type of access that the role is permissioned to have.

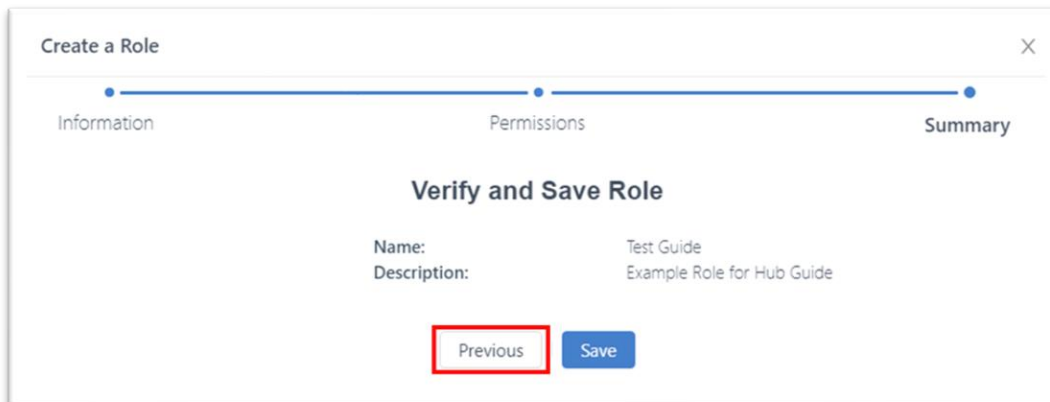


The 'Create a Role' dialog box is shown with the 'Permissions' tab selected. It features a table with various system components and their associated 'View' and 'Edit' permissions. The 'Next' button is highlighted with a red box.

Name	View	Edit
Groups and Settings	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Computers	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Users	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Alerts	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Activity Reports	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Compliance Reports	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Client Logs	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Server Logs	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Alert Logs	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Scans	<input type="checkbox"/>	<input type="checkbox"/>
Applications	<input type="checkbox"/>	<input type="checkbox"/>

Previous **Next**

If there are any changes you would like to make, click **Previous**.



The 'Create a Role' dialog box is shown with the 'Summary' tab selected. It displays the role's name and description, and the 'Previous' button is highlighted with a red box.

Verify and Save Role

Name: Test Guide
Description: Example Role for Hub Guide

Previous Save

Click **Save** to finish the process.

Create a Role

Information

Permissions

Summary

Verify and Save Role

Name:

Test Guide

Description:

Example Role for Hub Guide

Previous

Save

Licenses

The user licenses for the GateKeeper Hub server can be updated/changed here.

Valid Until	Users	Name	Email	Phone	Days Left	Status	Off-site Access	Actions
8/31/2019 8:00:00 P M	5	Sid	sid@gkaccess.com	3012334993	Expired	Active		

Click Browse to select new License file

BROWSE

UPLOAD

Valid Until	Users	Name	Email	Phone	Days Left	Status	Off-site Access	Actions
12/30/2019 7:00:00 PM	5	Abe Kim - QA1	abe@gkaccess.com		56	Active		


Click Browse to select new License file

BROWSE

UPLOAD

Click **Browse**, locate the license file you downloaded from the [Customer Portal](#) after purchase.

Licenses


Valid Until	Users	Name	Email	Phone	Days Left	Status	Off-site Access	Actions
12/30/2019 7:00:00 PM	5	Abe Kim - QA1	abe@gkaccess.com		56	Active		

Click Browse to select new License file

BROWSE **UPLOAD**

Once you have selected the file, click **Upload** to change the license.

Licenses


Valid Until	Users	Name	Email	Phone	Days Left	Status	Off-site Access	Actions
12/30/2019 7:00:00 PM	5	Abe Kim - QA1	abe@gkaccess.com		56	Active		

Click Browse to select new License file

BROWSE **UPLOAD**

Alternatively, under the **Actions** category you can [Deactivate](#) or [Delete](#) the license.

Licenses

Valid Until	Users	Name	Email	Phone	Days Left	Status	Off-site Access	Actions
12/30/2019 7:00:00 PM	5	Abe Kim - QA1	abe@gkaccess.com		56	Active		Deactivate Delete

Audit Information

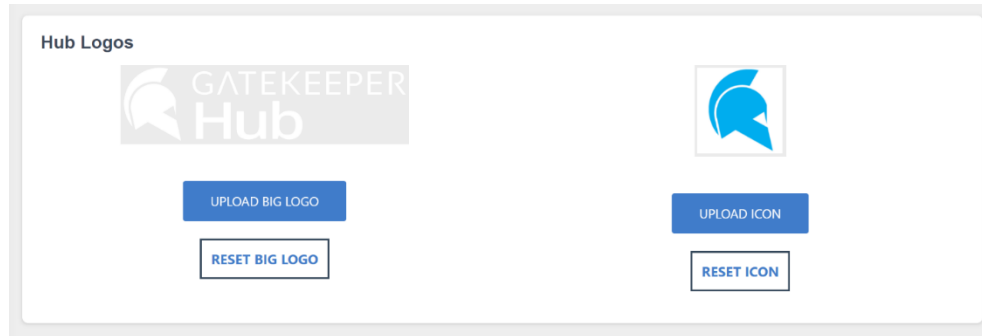
Administrators can choose to gather Real-Time Scans, Client Audit Logs, and Server Logs.

Audit Information

Collect Real-Time Scans ⓘ	Yes No
Collect Client Audit Logs ⓘ	Yes No
Collect Server Logs ⓘ	Yes No

Hub Logos

The logos displayed on the Hub can be customized (e.g. your corporate logo/icon). If you would like to revert the logo back to the default GateKeeper icons, click the corresponding **Reset** button.



Database Information

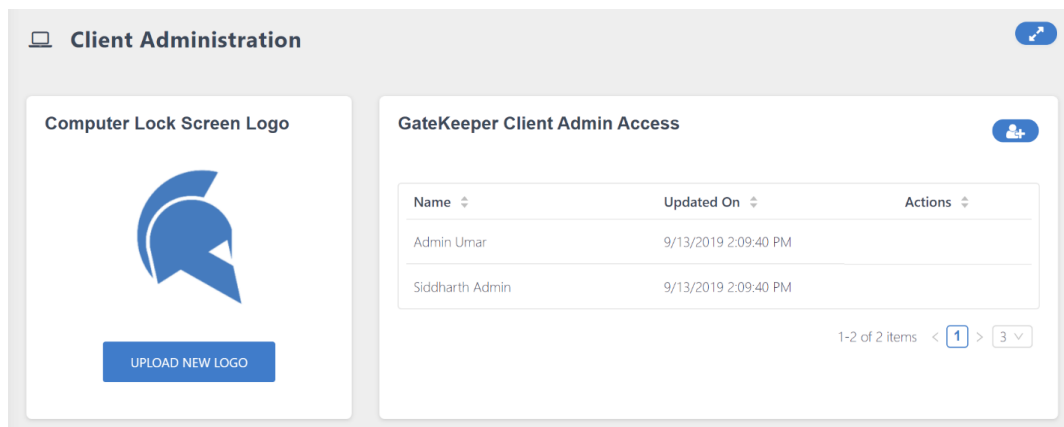
Admins can view how much data in the SQL database has been allocated and in use by GateKeeper.

Database Information			
Server Type: Express Edition (64-bit)		Database Name: GateKeeper-3	Database allocated space: 1,680 MB
Schema	Table	Row Count	Size
GateKeeper	Scans	6,465,608	628.88 MB
GateKeeper	EventLogs	777,184	251.76 MB
GateKeeper	Credentials	2,156	0.82 MB
GateKeeper	Devices	1,019	0.45 MB
GateKeeper	Computers	94	0.13 MB

2.2 Client Administration

Computer Lock Screen Logo

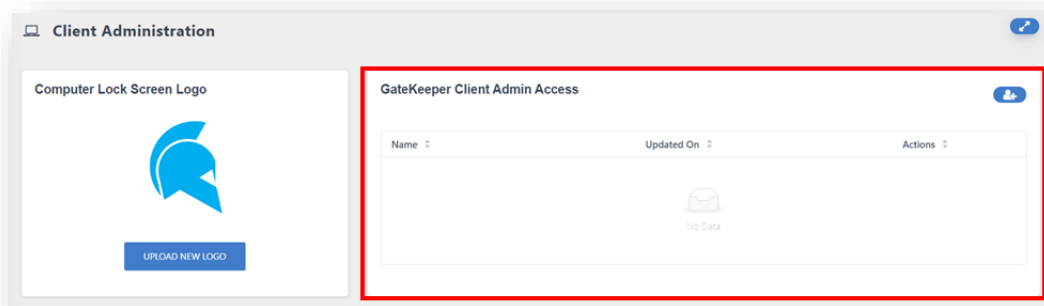
The logo that appears on the lock screen for the Client application can be changed under the **Computer Lock Screen Logo** section by clicking **Upload New Logo**.



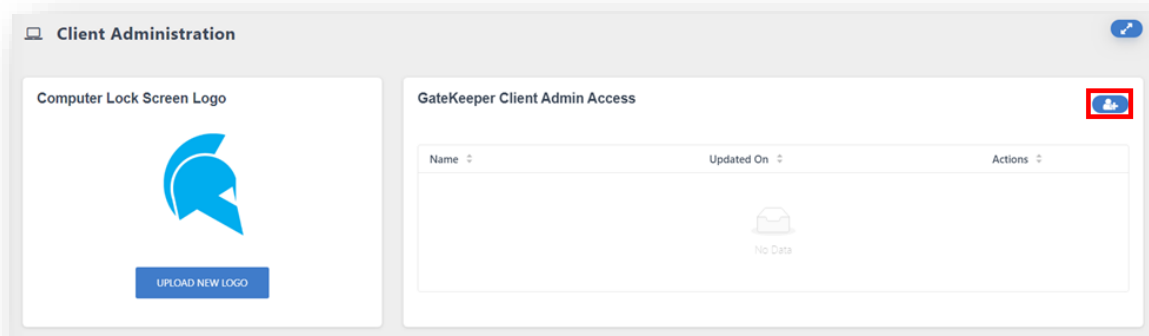
GateKeeper Client Admin Access

Here, an admin can create a GateKeeper Client admin name and password. These credentials are used to temporarily enable the Windows Credential Provider after it has been disabled on a computer. After

unlocking the Windows Credential Provider, the admin can log in using their domain or local username and password.





To add a new GateKeeper Client Admin Access, click the  icon.




A small popup window will appear. Fill out all the information and then click **Save**.

Add GateKeeper Client Admin Access


Name (required)


Admin Access Password (required)


Confirm Admin Access Password (required)


Off-site Hub Access Administration

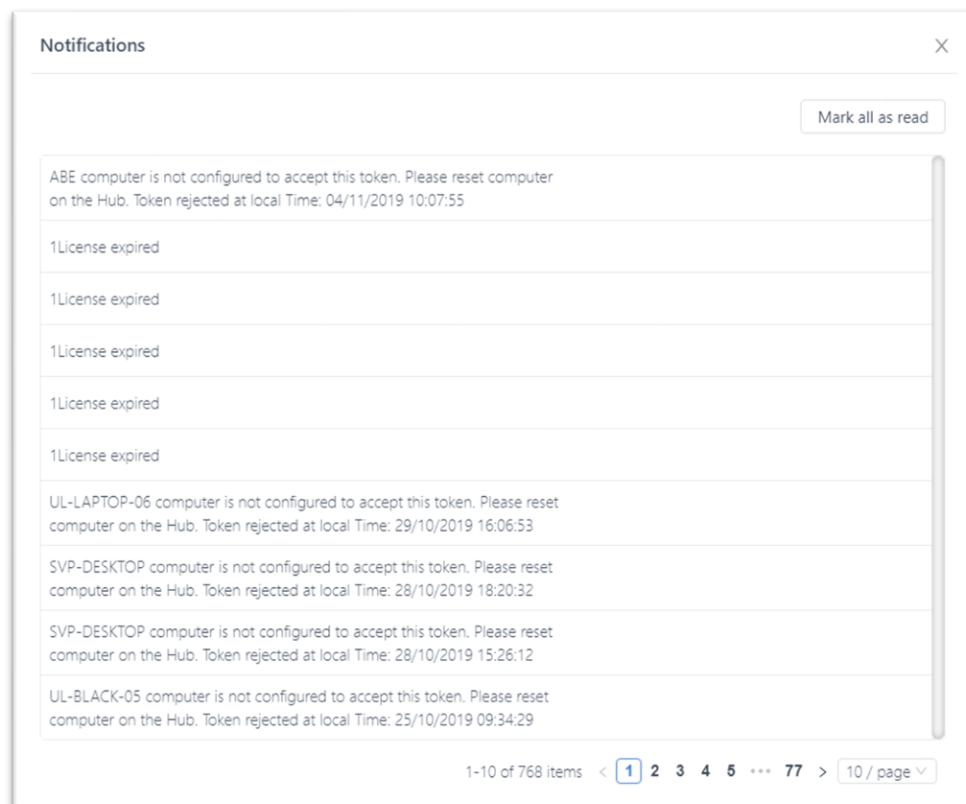
GateKeeper Hub website runs on this computer and is accessible only on the local network. This means that when a computer is not on the network, the GateKeeper Client application is unable to communicate with the Hub, unless there is a VPN connection. Furthermore, Hub administrators cannot access the website over the Internet, unless they are using a VPN connection. However, it is possible to set up off-network access to the GateKeeper Hub website using a reverse tunneling service managed through the GateKeeper Hub Manager. If you want the GateKeeper Hub website accessible through the Internet, you can set a unique URL for the Hub and set up the tunneling service using this setting on the manager.

You must obtain an offsite access license from the GateKeeper support team in order to enable this feature. If you do not have an offsite access license, then you will not be able to set up the tunneling service. Please contact support@gkaccess.com if you would like to obtain the offsite access license.

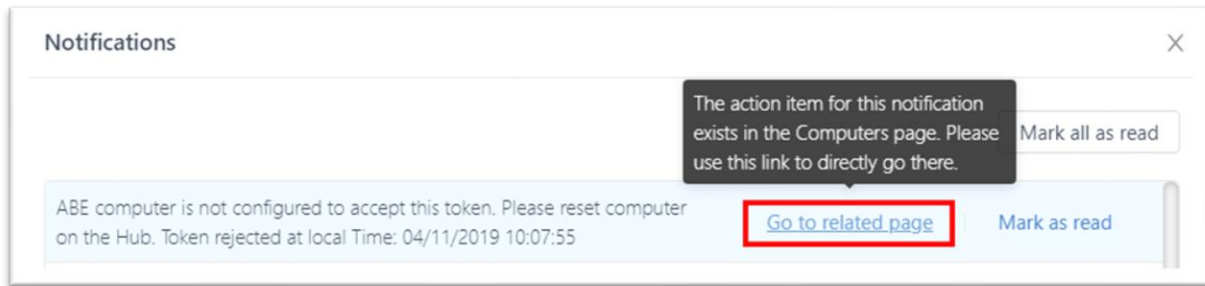
2.3 Notifications (Bell Icon)

The bell icon brings up the **Notifications** side panel. This shows all the recent events that have been logged in the GateKeeper system.

 Notifications



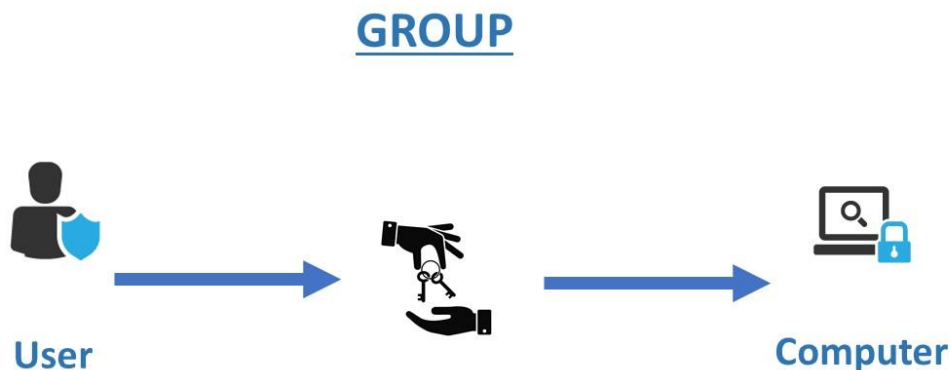
Hover over any notification and two options will appear. [Go to related page](#) will redirect to where the action item originated from. [Mark as read](#) will clear the notice from the **Notifications** panel.



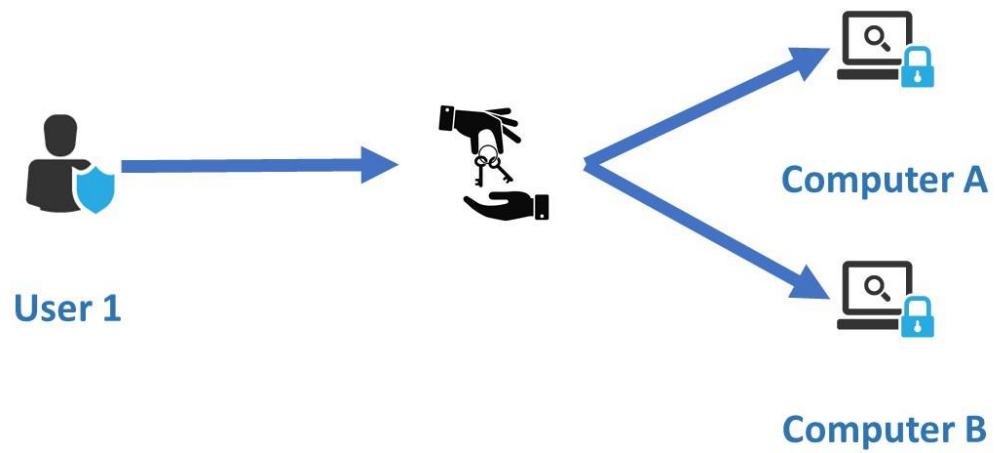
3 Groups Settings

Groups: settings for all computers connected to the GateKeeper Hub. **Group** section allows users to modify settings per individual Group. Prior to using this page, the administrator must ensure all users are assigned a GateKeeper token and the GateKeeper Client application is installed on all computers.

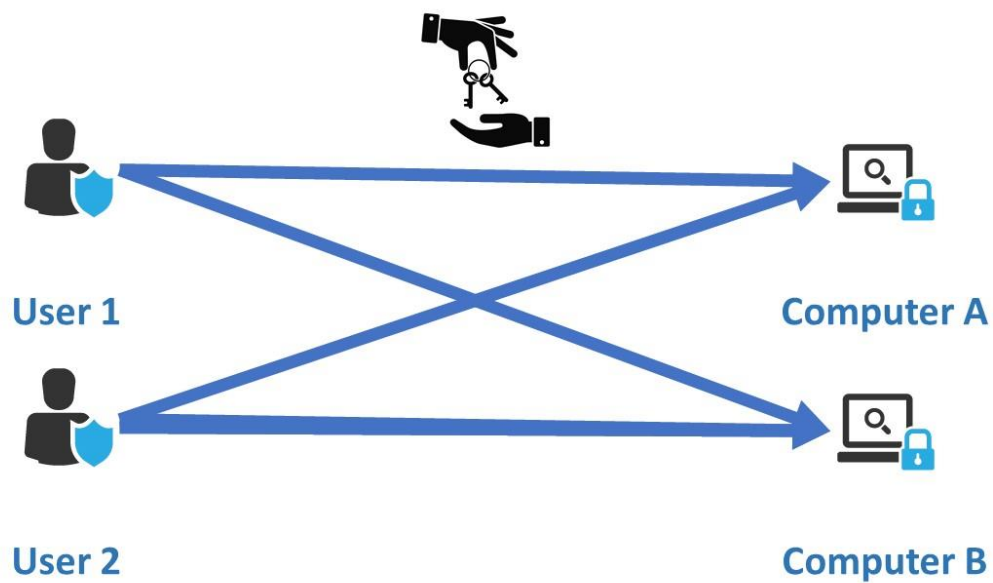
*A computer can only be assigned to one Group at a time. A user can be assigned to many Groups.

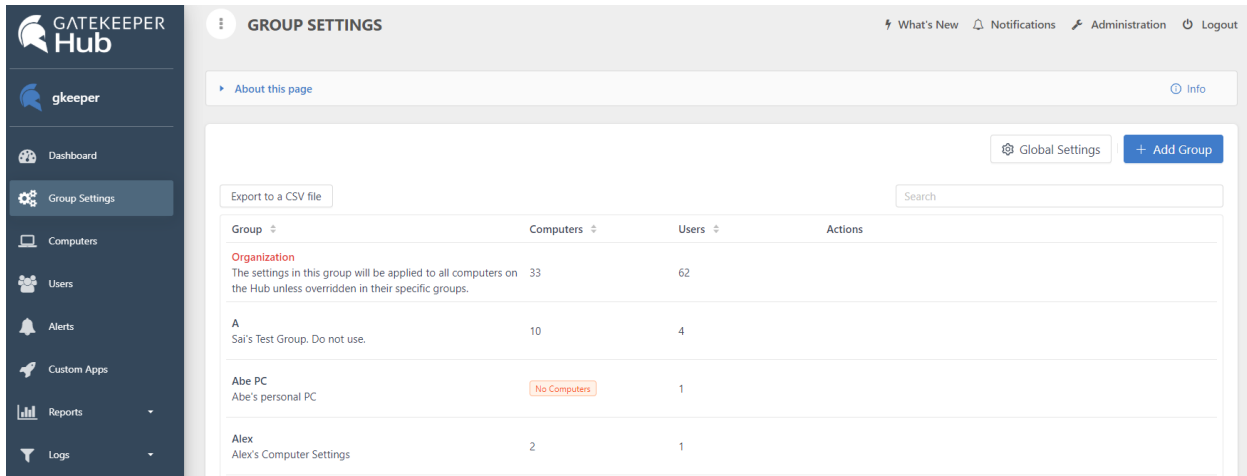


GROUP



GROUP





GROUP SETTINGS

What's New Notifications Administration Logout

About this page Info

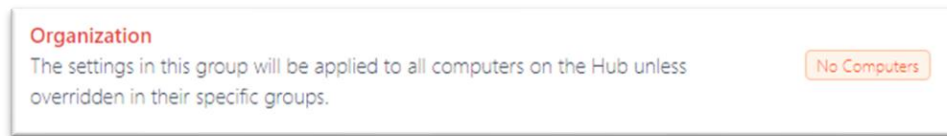
Global Settings + Add Group

Export to a CSV file Search

Group	Computers	Users	Actions
Organization The settings in this group will be applied to all computers on the Hub unless overridden in their specific groups.	33	62	
A Sai's Test Group. Do not use.	10	4	
Abe PC Abe's personal PC	No Computers	1	
Alex Alex's Computer Settings	2	1	

3.1 Organization

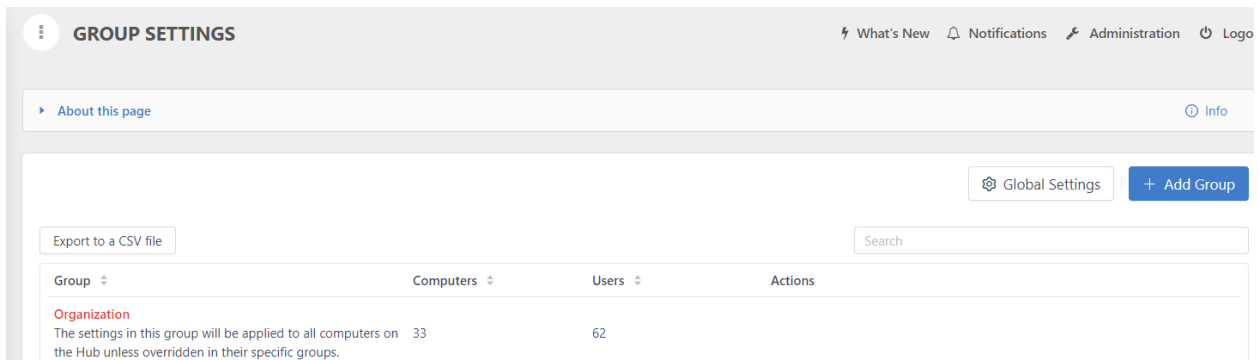
The **Organization** group cannot be deleted - it is the default **Group** that any computer that is not in another **Group** is automatically assigned to.



Organization

The settings in this group will be applied to all computers on the Hub unless overridden in their specific groups.

No Computers



GROUP SETTINGS

What's New Notifications Administration Logout

About this page Info

Global Settings + Add Group

Export to a CSV file Search

Group	Computers	Users	Actions
Organization The settings in this group will be applied to all computers on the Hub unless overridden in their specific groups.	33	62	

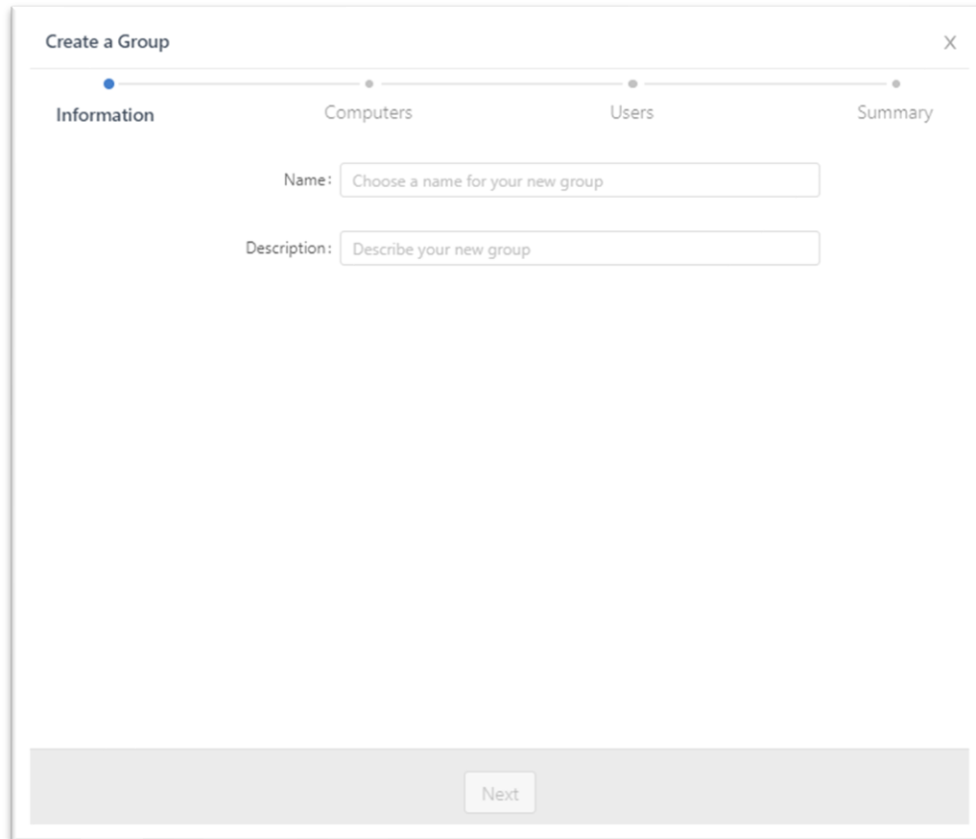
3.2 Creating Groups

Administrators can add new **Groups**, each with their own unique settings. Click **+ Add Group**.

+ Add Group

INFORMATION

The **'Create a Group'** side panel window will appear. Enter the Group's name and a description.



The "Create a Group" dialog box features a progress bar at the top with four steps: Information, Computers, Users, and Summary. The "Information" step is currently active, indicated by a blue dot. Below the progress bar, there are two text input fields: "Name:" with a placeholder "Choose a name for your new group" and "Description:" with a placeholder "Describe your new group". At the bottom right of the dialog, there is a "Next" button.

COMPUTERS

Assign computer(s) to the **Group** (at least one computer). Click **Next**.

Create a Group

Information

Computers

Users

Summary

<input checked="" type="checkbox"/> Computer	Group	Department
<input type="checkbox"/> UL-BENCH-ALEX	Organization	General
<input checked="" type="checkbox"/> UL-LAPTOP-03	Alex Lee	General
<input checked="" type="checkbox"/> UL-LAPTOP-04	Organization	General
<input checked="" type="checkbox"/> UL-LAPTOP-05	Organization	General
<input type="checkbox"/> UL-LAPTOP-06	Sai	General
<input type="checkbox"/> UL-LAPTOP-07	Alex	General
<input type="checkbox"/> UL-LAPTOP-10	Alex	General
<input type="checkbox"/> Untethereds-Air.fios-router.home	Organization	General
<input type="checkbox"/> Untethereds-iMac	Area_51	General
<input type="checkbox"/> Untethereds-iMac.local	Area_51	General
<input type="checkbox"/> Untethereds-MacBook-Air	Organization	General
<input type="checkbox"/> Untethereds-MacBook-Air.local	Area_51	General
<input type="checkbox"/> Untethereds-Mac-mini.local	Area_51	General
<input type="checkbox"/> VADDI	Sai	General

Previous

Next

USERS

Assign users to the **Group**. Click **Next**.

*Only users assigned to this **Group** can unlock the computers in the same **Group**.

Create a Group

Information

Computers

Users

Summary

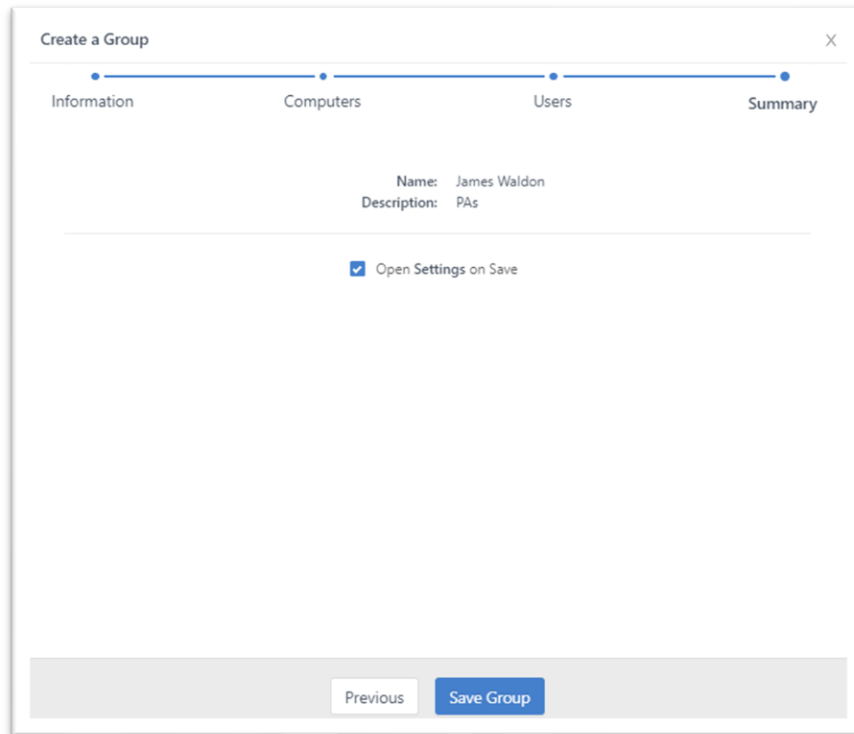
<input type="checkbox"/> User	Department
<input type="checkbox"/> Scott Simpson	General
<input type="checkbox"/> Serge Henry	IT
<input type="checkbox"/> Siddharth Potbhare	Engineering
<input type="checkbox"/> SP	General
<input type="checkbox"/> Test11	General
<input type="checkbox"/> Test2 User	TestDepartment
<input type="checkbox"/> Testing SAM User	General
<input type="checkbox"/> Timothy Barksdale	tech support
<input type="checkbox"/> Tom Watson	Engineering
<input type="checkbox"/> ULabs	General
<input type="checkbox"/> Umar	Engineering
<input type="checkbox"/> Ummer Dar	QA
<input type="checkbox"/> User A	General
<input type="checkbox"/> User B	General

Previous

Next

SUMMARY

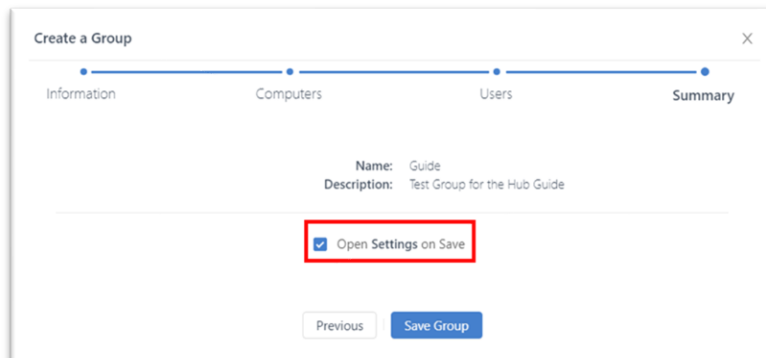
If there are any changes you would like to make, click **Previous**.



The screenshot shows the 'Create a Group' dialog box with the 'Summary' tab selected. The progress bar at the top indicates the steps: Information, Computers, Users, and Summary. The 'Name' field is filled with 'James Waldon' and the 'Description' field is filled with 'PAs'. Below these fields, the checkbox 'Open Settings on Save' is checked. At the bottom of the dialog, there are two buttons: 'Previous' and 'Save Group'.

Click **Save Group** to finish.

Select the checkbox for “**Open Settings on Save**” checkbox to change settings after.



This screenshot is similar to the previous one, but the 'Open Settings on Save' checkbox is highlighted with a red rectangle. The 'Name' field is filled with 'Guide' and the 'Description' field is filled with 'Test Group for the Hub Guide'. The 'Previous' and 'Save Group' buttons are still visible at the bottom.

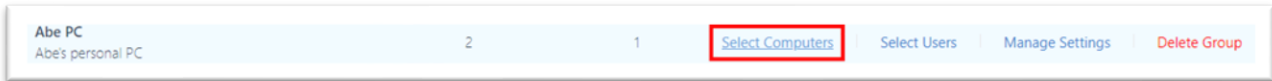
“**Manage settings in Group [Group’s name]**” side panel will appear.

Manage settings in Group: Lisa computer

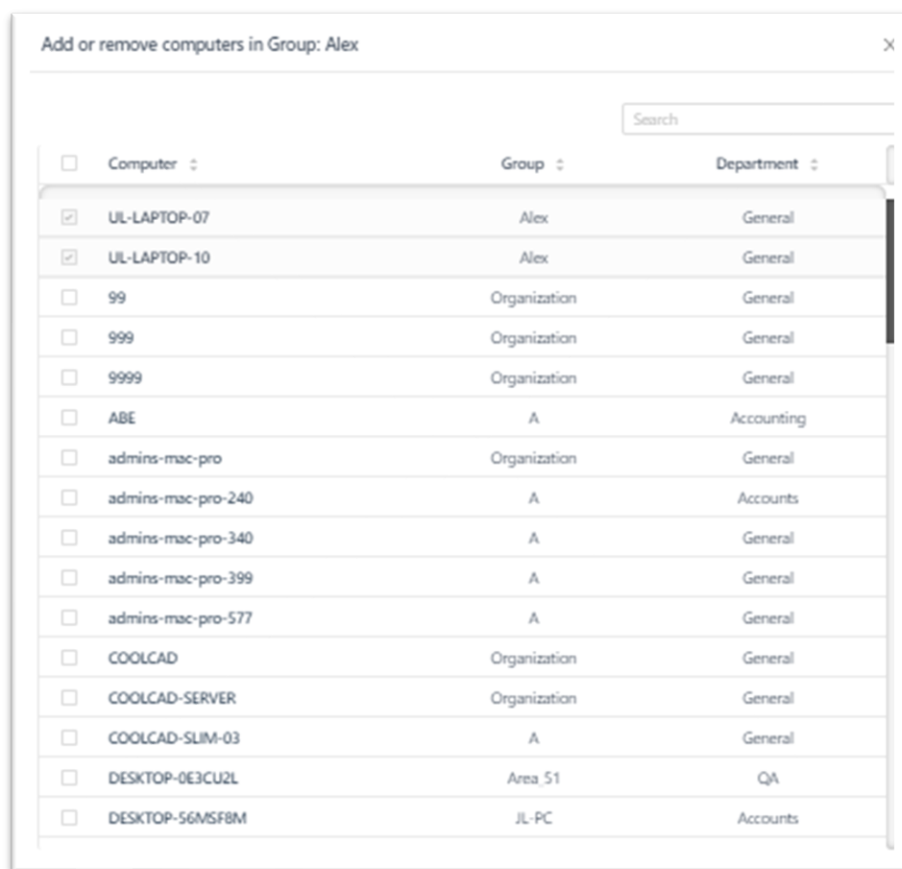
LOCK SETTINGS UNLOCK SETTINGS ADVANCED SETTINGS

3.3 Add or remove Computers in Groups

To change (add or remove) computers in a **Group**, hover over the desired **Group** and click [Select Computers](#).



The “Add or remove computers in Group: [Group’s name]” side panel will appear. Select your computers.



Once you have selected the computers you would like to put into the **Group**, click **Save Computers**.

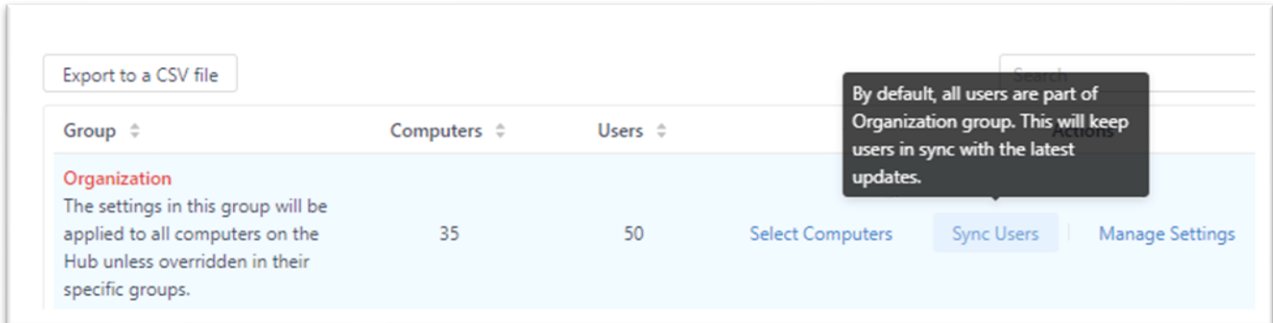
3.4 Adding and removing Users in Groups

Sync Users for Organization Group

The **Sync Users** button will ensure that any new users added to the GateKeeper Hub are made part of the **Organization** group. While the Hub server automatically adds every new user to the **Organization**

group, the **Sync User** button refreshes groups to ensure that every GateKeeper user is part of the **Organization** group, just in case for whatever reason, the auto-sync did not complete.

Hover over the **Organization Group** and click [Sync Users](#).



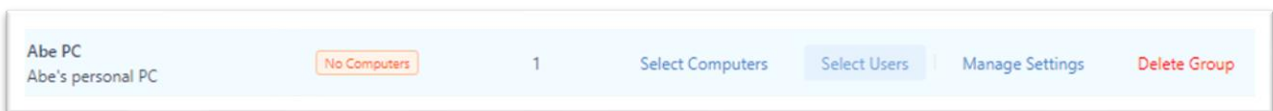
Export to a CSV file

Group	Computers	Users	Actions
Organization The settings in this group will be applied to all computers on the Hub unless overridden in their specific groups.	35	50	Select Computers Sync Users Manage Settings

By default, all users are part of Organization group. This will keep users in sync with the latest updates.

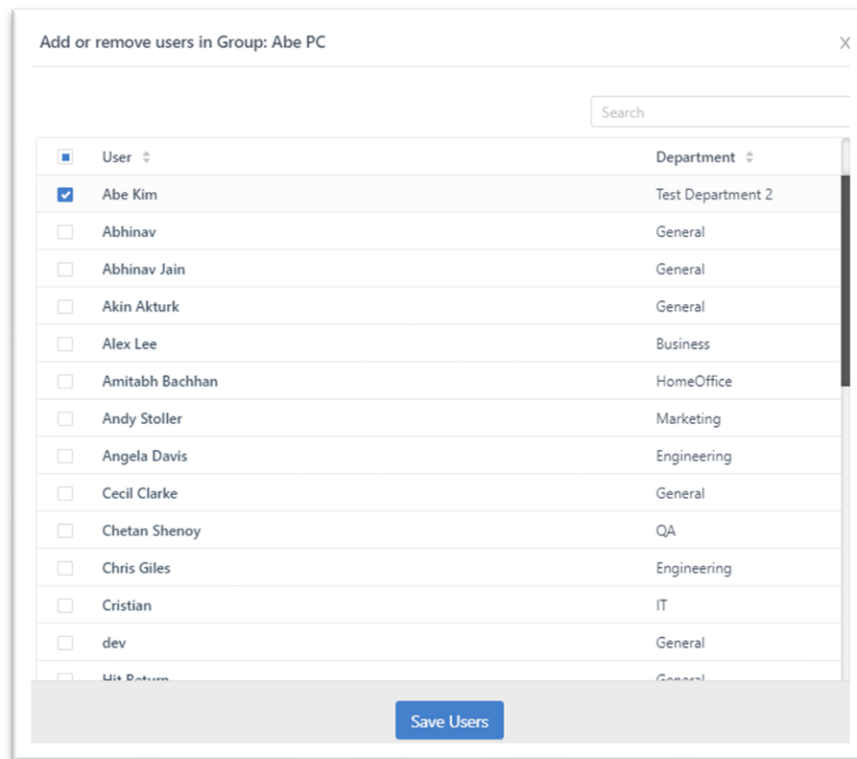
Add or Remove Users from Groups

To add or remove users in a **Group**, click [Select Users](#) next to the Group's name.



Group	Computers	Users	Actions
Abe PC Abe's personal PC	No Computers	1	Select Computers Select Users Manage Settings Delete Group

Add new users or remove existing ones by selecting or unselecting names for the **Group**. Click **Save**.



Add or remove users in Group: Abe PC

Search

User	Department
<input checked="" type="checkbox"/> Abe Kim	Test Department 2
<input type="checkbox"/> Abhinav	General
<input type="checkbox"/> Abhinav Jain	General
<input type="checkbox"/> Akin Akturk	General
<input type="checkbox"/> Alex Lee	Business
<input type="checkbox"/> Amitabh Bachhan	HomeOffice
<input type="checkbox"/> Andy Stoller	Marketing
<input type="checkbox"/> Angela Davis	Engineering
<input type="checkbox"/> Cecil Clarke	General
<input type="checkbox"/> Chetan Shenoy	QA
<input type="checkbox"/> Chris Giles	Engineering
<input type="checkbox"/> Cristian	IT
<input type="checkbox"/> dev	General
<input type="checkbox"/> Mit Bhatnagar	General

Save Users

3.5 Manage Group Settings

To change the settings for a **Group**, hover over the desired **Group** and click [Manage Settings](#).



This will bring up the “Manage settings in Group: [Group’s name]” side panel window.

Manage settings in Group: Lisa computer

LOCK SETTINGS

UNLOCK SETTINGS

ADVANCED SETTINGS

Lock Settings

Below are the options for each setting along their explanations.

Manage settings in Group: Alex
Info
X

LOCK SETTINGS
UNLOCK SETTINGS
ADVANCED SETTINGS

Proximity Lock Method
Set on Client computer

Proximity Lock Method defines how GateKeeper automatically secures your computer when you walk away. Use **Lock Workstation** if you are the only user, and, **Disconnect Session** if multiple people use this computer.

Button Lock Method
Set on Client computer

Button Lock Method defines how GateKeeper secures your computer when you press the action button on your token or phone app. Use **Lock Workstation** if you are the only user, and, **Disconnect Session** if multiple people use this computer.

Inactivity Lock Method
15
Sec
Disable

Inactivity Lock Method will lock the computer if the user is inactive for the specified time. Use **Lock Workstation** if you are the only user, and, **Disconnect Session** if multiple people use this computer.

Disconnect Remote Session
Set on Client computer

Enable or **Disable** disconnecting the remote session when the local computer is locked. This method is only applicable when the remote computer is running the GateKeeper Remote application for access management.

Token Visibility Timeout
45 Sec

The computer will lock if no data packets are received from the token within this **Token Visibility Timeout** period. This typically happens when the token is very far away from the computer. 30s is the default setting.

Lock Delay Timeout
Set on Client computer

GateKeeper will delay locking the computer after a lock decision has been made for this **Lock Delay Timeout** period. Choose a value for this delay if you want to prevent the computer from locking immediately when you walk away. **Important:** This lock delay will only apply when the computer is locked due to proximity.

Operating System Timeout

Set on Client computer

GateKeeper can disable your screen saver from starting when your computer times out. Choose the appropriate option to keep your timeout policy enabled or to disabled.

Motion Detection Sensitivity

Set on Client computer

Choose a level of sensitivity to motion to force the computer to lock faster. High motion sensitivity will allow the computer to lock quicker. If the system is locking too much while you are sitting at your desk, reduce the motion sensitivity to the Low level.

Lock Sensitivity

Medium

Lock Sensitivity changes the lock/unlock distance for your computer. The higher the sensitivity, the shorter the distance to lock. We recommend Medium sensitivity for the best lock/unlock experience.

Note: Applies to Client App version 3.6.9 or lower.

Save Changes

Proximity Lock Method

Proximity Lock Method defines how GateKeeper automatically secures your computer when you walk away. Use **Lock Workstation** if you are the only user, and, **Disconnect Session** if multiple people use this computer.

Set on Client computer:	Allows end-users to choose the settings on the Client application.
Disable:	Turns off the feature.
Lock Workstation:	Auto-locks the computer. Leaves the current session active and available for any user to login.
Disconnect Session (Switch User):	Locks the computer and enables switching between local or AD user accounts on Windows 7 and Mac (OS 10.13 and 10.14) computers.
Logout:	Logs the user out from the computer.

Button Lock Method

Button Lock Method defines how GateKeeper secures your computer when you press the action button on your token or phone app. Use **Lock Workstation** if you are the only user, and, **Disconnect Session** if multiple people use this computer.

Inactivity Lock Method

Inactivity Lock Method will lock the computer if the user is inactive for the specified time. Use Lock Workstation if you are the only user, and, Disconnect Session if multiple people use this computer.

Disconnect Remote Session

Enable or **Disable** disconnecting the remote session when the local computer is locked. This method is only applicable when the remote computer is running the GateKeeper Remote application for access management.

Token Visibility Timeout

Set a timer for how long the computer will remain unlocked if suddenly the software receives no data from the token. Sudden signal loss can happen if a user places their hand over the token or buries it in their pocket. This feature is set in 15-second increments (15, 30, 45, 60).

Lock Delay Timeout

GateKeeper will delay locking the computer after a lock decision has been made for this Lock Delay Timeout period. Choose a value for this delay if you want to prevent the computer from locking immediately when you walk away. Important: This lock delay will only apply when the computer is locked due to proximity.

Operating System Timeout

Disable your screen saver from starting when your computer times out. Choose the appropriate option to keep your timeout policy enabled or to disabled. If your timeout policy is set by your network administrator, this setting will not override the network policy.

Motion Detection Sensitivity

Choose a level of sensitivity to motion to force the computer to lock faster. High motion sensitivity will allow the computer to lock quicker. If the system is locking too much while you are sitting at your desk, reduce the motion sensitivity to the Low level.

Set on Client computer:	Allows end-users to choose the settings on the Client application.
Low:	Slow lock speed.
Medium:	Intermediate lock speed.
High:	Fast lock speed.

Lock Sensitivity

Changes the lock/unlock distance for your computer. The higher the sensitivity, the shorter the distance needed to lock. We recommend **Medium** sensitivity for the best lock/unlock experience for most environments.

Set on Client computer:	Allows end-users to choose the settings on the Client application.
High:	Short range lock.
Medium:	Medium range lock.
Low:	Long range lock.
Minimum:	Longest range lock.

Unlock Settings

Below are the different setting options for unlocking functions.

Manage settings in Group: Lisa computer

[Info](#) [X](#)

LOCK SETTINGS

UNLOCK SETTINGS

ADVANCED SETTINGS

Unlock Method

Set on Client computer ▼

Unlock Method defines how GateKeeper will unlock your computer. We recommend the **GateKeeper with PIN Login** option for secure 2-factor authentication.

Quick Return Timeout

60 Sec ▼

Set on Hub ▼

GateKeeper can be set to automatically unlock the computer if the user comes back to the same computer within this **Quick Return Timeout** period. Only applicable when the **Unlock Method** is set to **GateKeeper with PIN Login**.

Force PIN Login Timeout

1 hrs

Set on Hub ▼
☒ Never

GateKeeper can force users to type in their PIN to login irrespective of their chosen **Unlock Method** if the user comes back to the the computer AFTER this PIN Login Timeout period. Use this to force users to type in their PINs occasionally.

Require user to enter Windows/macOS password

Set on Client computer ▼

You can choose to enter your username and password IN ADDITION to GateKeeper authentication. Users can be forced to type in their username/password at every unlock, or only when logging on to the computer. We recommend setting this option to **NEVER**.

Windows/macOS standard login

Set on Client computer ▼

GateKeeper can disable the standard login methods (username/password) for your computer. If you choose to **Disable** the default login method, then you can only access your computer with your GateKeeper. If you forget your PIN or lose your GateKeeper, you will NOT be able to access your computer.

Save Changes

Unlock Method

Unlock Method defines how GateKeeper will unlock your computer. We recommend the **GateKeeper with PIN Login** option for secure 2-factor authentication.

Set on Client computer:	Allows end-users to choose the settings on the Client application.
Automatic Login:	Proximity login - once the user is in the range of the computer, the user will be authenticated.
Press Enter to Login:	When the token is in range of the computer, pressing the Enter key will authenticate the user.
Touch to Login:	Touch the token to the USB proximity sensor to authenticate – just like an NFC card.

GateKeeper with PIN Login:	Requires the presence of a GateKeeper token and typing of a secret PIN to authenticate.
----------------------------	---

Quick Return Timeout

GateKeeper can be set to automatically unlock the computer if the user comes back to the same computer within this **Quick Return Timeout** period. Only applicable when the **Unlock Method** is set to **GateKeeper with PIN Login**.

Set on Client computer:	Allows end-users to choose the settings on the Client application.
Set on Hub:	Allows Hub admins to set the time for the Group's Quick Return Timeout option.

Force PIN Login Timeout

GateKeeper can force users to type their PIN to log in irrespective of their chosen **Unlock Method** if the user comes back to the computer AFTER this PIN Login Timeout period. Use this to force users to confirm their identity at required intervals. If the timer is set to 1 hour with the **Automatic Login** mode, then the users will be required to log in with their PIN after every 1 hour.

Set on Client computer:	Allows end-users to choose the settings on the Client application.
Set on Hub:	Allows Hub admins to set the time for the Group's Force PIN Login Timeout option.

Require user to enter Windows/macOS password

You can choose to enter your username and password IN ADDITION to GateKeeper authentication. Users can be forced to type in their username/password at every unlock, or only when logging on to the computer. We recommend setting this option to **NEVER**.

Set on Client computer:	Allows end-users to choose the settings on the Client application.
Never:	GateKeeper will never ask for your Windows or Mac username and password to authenticate.
At Login:	GateKeeper will ask for Windows or Mac username and password only when you log into your account using their token.
Always:	Any time a user unlocks their computer with their token, they will be asked for their Windows or Mac username and password.

Windows/macOS standard login

Option to disable the standard login methods (username/password) for your computer. If you choose to **Disable** the default login method, then you can only access your computer with your GateKeeper. If you forget your PIN or lose your GateKeeper, you will NOT be able to access your computer.

Set on Client computer:	Allows end-users to control this feature from their own computers.
Enable:	Any time a user unlocks their computer with their token, they will be asked for their Windows or Mac username and password.
Disable:	This will disable the Windows/macOS login option. If the user does not have their token, they will not be able to access the computer.

Advanced Settings

Manage settings in Group: Lisa computer
Info X

LOCK SETTINGS
UNLOCK SETTINGS
ADVANCED SETTINGS

GateKeeper Application Launcher
Set on Client computer

GateKeeper Application Launcher is a tool that allows GateKeeper users to launch custom applications with their GateKeeper credentials on any computer. Hub administrators can set up these applications on the Hub via the **Custom Apps** tab. Use this setting to enable or disable the GateKeeper Application Launcher on the client computers.

Notifications
Set on Client computer

Enable or disable receiving notifications from GateKeeper client application.

Add new user through client application
☒

Allow or prevent GateKeeper users from adding new users through the client application. We recommend preventing users from adding new users for security purposes.

Add credentials through client application
☒

Allow or prevent GateKeeper users to add more credentials to their profile. These can be domain, local or web credentials. We recommend keeping this option enabled for your users.

Add tokens through client application
☒

Allow or prevent GateKeeper users to add new tokens to their profile. We recommend disabling this option if you want administrators to manage tokens for your users.

Set range through client application
☒

Allow or prevent GateKeeper users from changing the range settings on the client application. Once the range is set, we recommend disabling this option to prevent inappropriately training the GateKeeper software. Note: Applies to Client App version 3.6.9 or lower.

Change server address through client application
☒

Allow or prevent GateKeeper users on the client application from changing the connection to the Hub server. This option should be disabled so that users cannot disconnect the computer from the GateKeeper Hub network.

ase
Save Changes

GateKeeper Application Launcher

GateKeeper Application Launcher is a tool that allows GateKeeper users to launch custom

applications with their GateKeeper credentials on any computer. Hub administrators can set up these applications on the Hub via the Custom Apps tab. Use this setting to enable or disable the GateKeeper Application Launcher on the client computers.

Notifications

Enables or disables desktop GateKeeper notifications on the local PC.

Add new user through client application

Allow or prevent GateKeeper users from adding new users through the client application. We recommend preventing users from adding new users for security purposes.

Add credentials through client application

Allow or prevent GateKeeper users to add more credentials to their profile. These can be domain, local or web credentials. We recommend keeping this option enabled for your users.

Add tokens through client application

Allow or prevent GateKeeper users to add new tokens to their profile. We recommend disabling this option if you want administrators to manage tokens for your users.

Set range through client application

Allow or prevent GateKeeper users from changing the range settings on the client application. Once the range is set, we recommend disabling this option to prevent inappropriately training the GateKeeper software.

Change server address through client application

Allow or prevent GateKeeper users on the client application from changing the connection to the Hub server. This option should be disabled so that users cannot disconnect the computer from the GateKeeper Hub network.

Global Settings



Authenticators: Choose what authentication device will use to access computers on your network.

- **GateKeeper Bluetooth Tokens:** GateKeeper Halberd or Trident App soft token for smartphones.

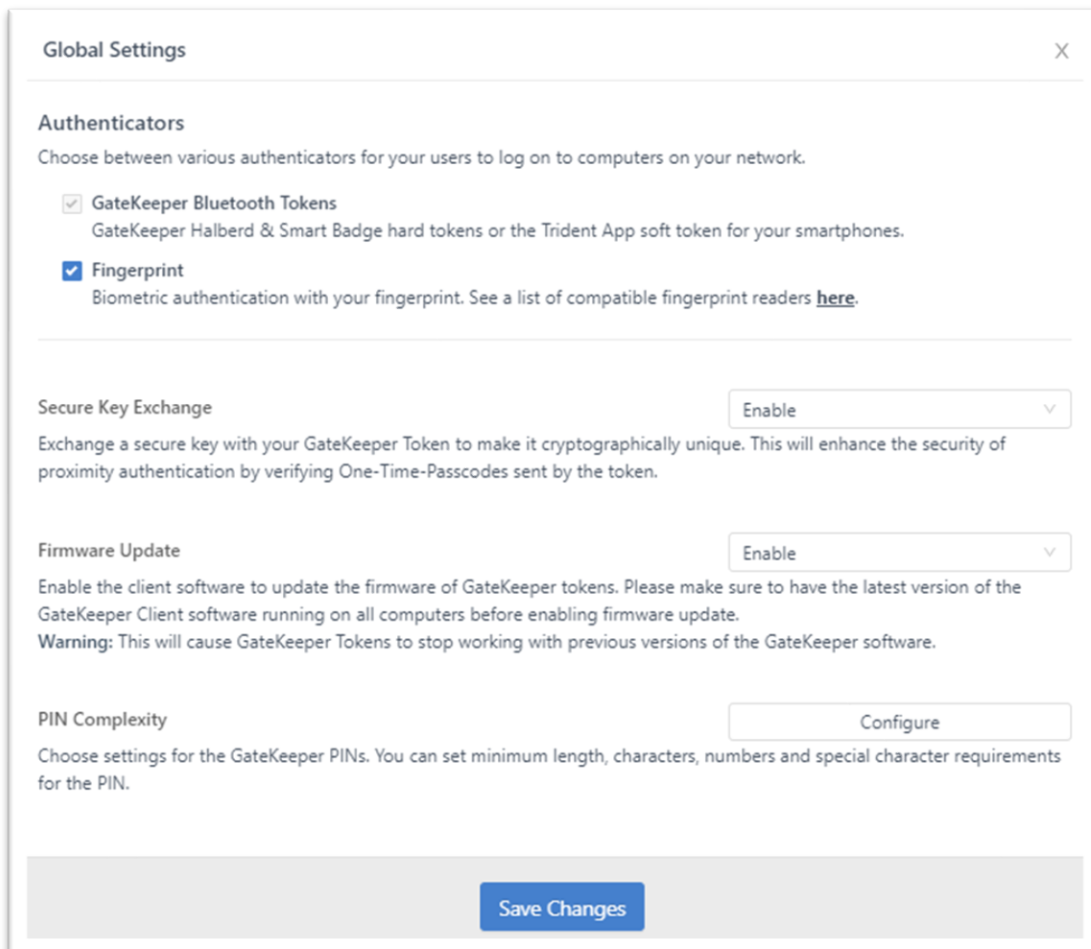
- **Fingerprint:** Biometric authentication with your fingerprint. See a list of compatible fingerprint readers [here](#).

Secure Key Exchange: Exchange a secure key with your GateKeeper Token to make it cryptographically unique. This will enhance the security of proximity authentication by auto-verifying One-Time-Passcodes sent by the token.

Firmware Update: Enable the Client software to update the firmware of GateKeeper tokens. Please make sure to have the latest version of the GateKeeper Client software running on all computers before enabling firmware update.

Warning: This will cause GateKeeper tokens to stop working with version 3.6.9 and prior.

PIN Complexity: Choose strength requirements for the GateKeeper PINs. You can set minimum length, characters, numbers, and special character requirements for the PIN.



Global Settings [X]

Authenticators
Choose between various authenticators for your users to log on to computers on your network.

- ☒ **GateKeeper Bluetooth Tokens**
GateKeeper Halberd & Smart Badge hard tokens or the Trident App soft token for your smartphones.
- ☒ **Fingerprint**
Biometric authentication with your fingerprint. See a list of compatible fingerprint readers [here](#).

Secure Key Exchange [Enable ▾]
Exchange a secure key with your GateKeeper Token to make it cryptographically unique. This will enhance the security of proximity authentication by verifying One-Time-Passcodes sent by the token.

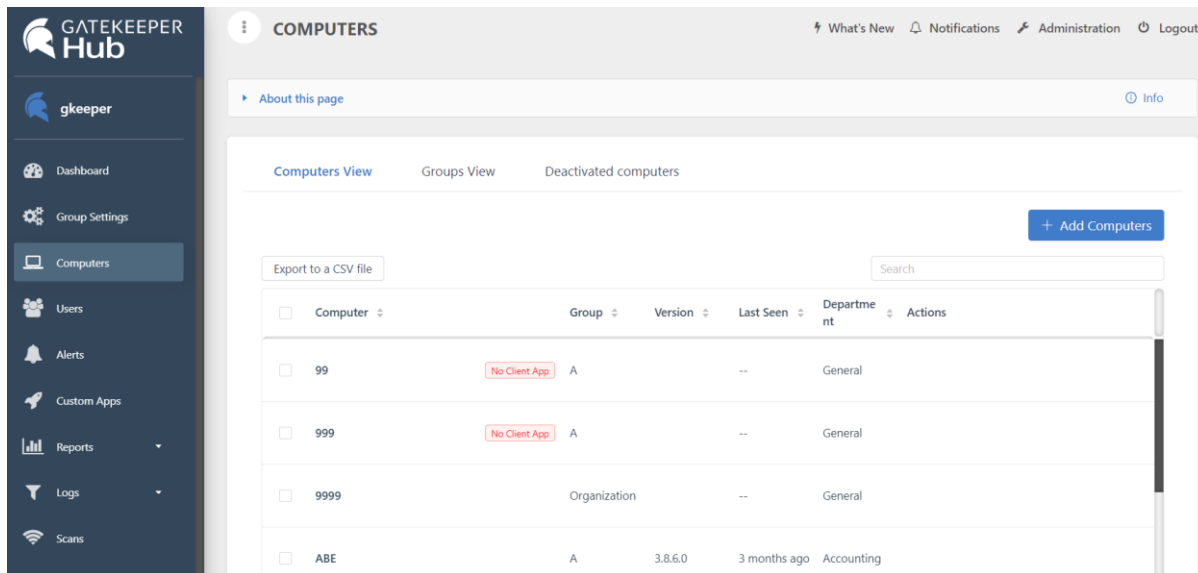
Firmware Update [Enable ▾]
Enable the client software to update the firmware of GateKeeper tokens. Please make sure to have the latest version of the GateKeeper Client software running on all computers before enabling firmware update.
Warning: This will cause GateKeeper Tokens to stop working with previous versions of the GateKeeper software.

PIN Complexity [Configure]
Choose settings for the GateKeeper PINs. You can set minimum length, characters, numbers and special character requirements for the PIN.

Save Changes

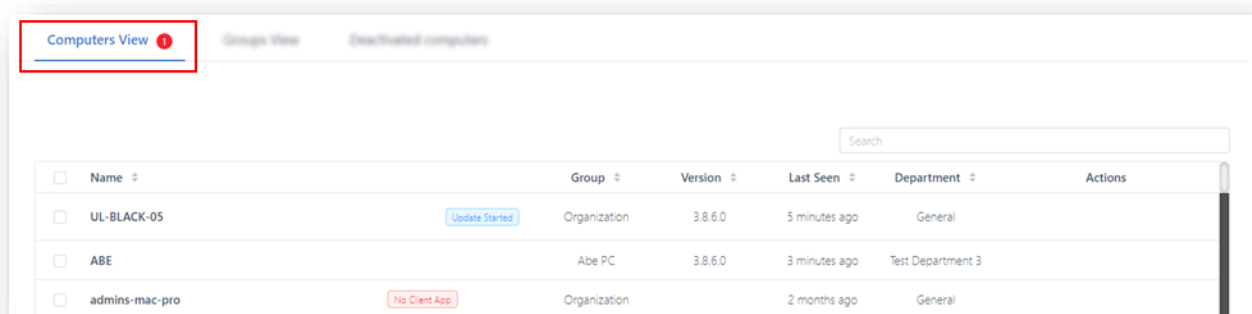
4 Computers

Lists all computers with GateKeeper Client installed and are connected to the GateKeeper Hub server.



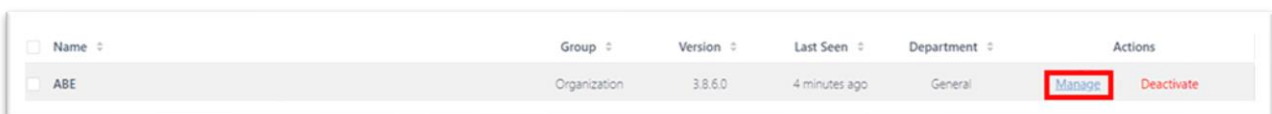
4.1 Computers View

Listed under the **Computers View** section are names of all the computers, the **Group** the **Computer** is assigned to, the application version installed, the last recorded activity time on the computer, and the department the computer belongs to.



4.1.1.1 Add User to Computers

Hover over the desired computer, under the **Actions** category you will see the [Manage](#) option.



The “**Manage computer: [Computer’s name]**” side panel will appear. This will open the **Profile** tab. Here, you can set the **Location** of the computer as well as the **Department** that the computer belongs to. You can also view information such as the IP Address, Client version installed on the computer, MAC Address, and the OS the computer is running. Click **Save Profile**.

Manage computer: SACHARLAP1 Info X

Profile Groups Computer-Specific Credential Update Client Software

Name: SACHARLAP1

IP Address: 192.168.1.64

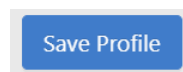
Client Version: 3.5.6.0

MAC Address: 68A3C4A0Aafb

OS: Microsoft Windows NT 6.2.9200.0

Department: General

Click the **Save Profile** button to proceed.



On the “**Groups**” tab, you can assign users to a new **Group** of computers by clicking the drop-down menu.

Manage computer: SACHARLAP1 Info X

Profile **Groups** Computer-Specific Credential Update Client Software

Important
Access to a computer for a user is defined based on which Group the computer and user belong to. For more control over access, check the [Group Settings](#) page.

Computer	Group	Actions
SACHARLAP1	<div>Organization</div> <div>Organization</div> <div>A</div> <div>Abe PC</div> <div>Alex</div>	

Click **Save**. On the **Computer-Specific Credential** tab, see what login credentials are on the computer.

To add a new credential, hover over the computer, under the **Actions** category, click [Edit](#).

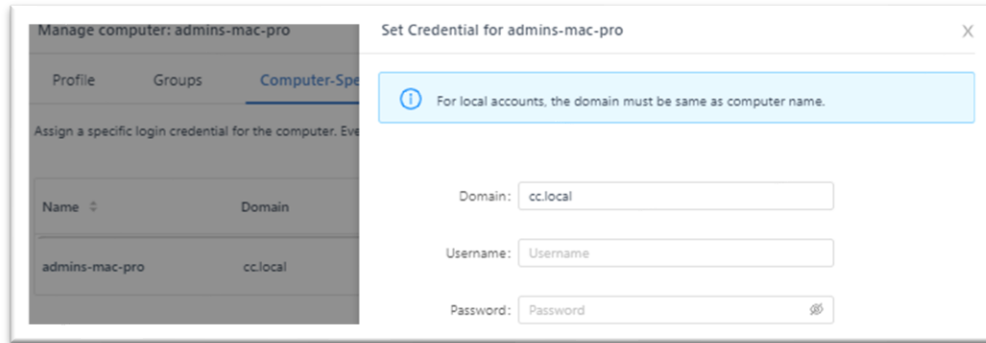
manage computer: admin-mac-pro

Profile Groups **Computer-Specific Credential** Update Client Software

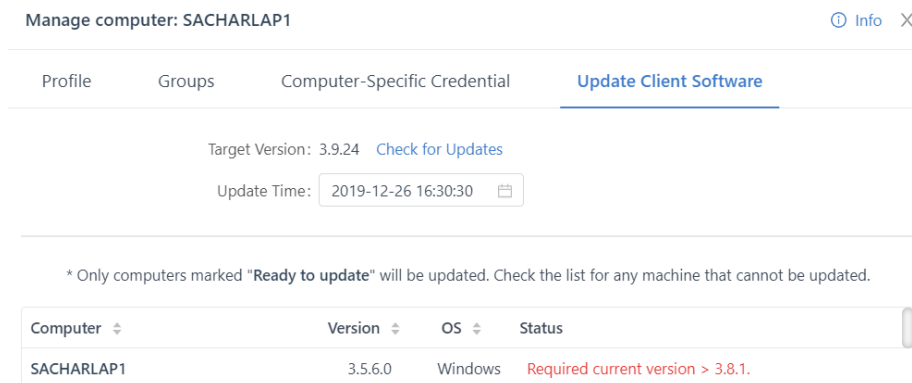
Assign a specific login credential for the computer. Every GateKeeper user will log on to the computer using this credential.

Name	Domain	Username	Password	Actions
admins-mac-pro	cc.local	--	--	Edit Delete

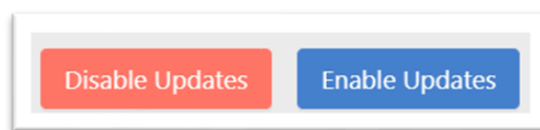
This brings up the “**Set Credential for [Computer’s name]**” side panel. Here, you can input the Domain, Username, and Password for the computer. Click **Save** to keep the login credential. Once the computer-specific credential is set, any user accessing this computer with a GateKeeper token will log in with these credentials by default. Click the **Save** when done.



The **Update Client Software** tab allows you to check if there are any new updates. It also allows you to set the date and time to auto-update the Client application software on the computers.



Computer	Version	OS	Status
SACHARLAP1	3.5.6.0	Windows	Required current version > 3.8.1.



4.1.1.2 Add or Remove Computers from Groups

If there are multiple computers you want to add or remove, select them all, then click **Manage Computers**.

Computers View Groups View Deactivated computers

[Export to a CSV file](#) [Manage Computers](#) [Deactivate Computers](#) Selected 5 of 73 computers.

Select all computers in the table

<input type="checkbox"/>	Computer	Group	Version	Last Seen	Department	Actions
<input checked="" type="checkbox"/>	COOLCAD-SLIM-03	A	3.2.3.0	4 months ago	General	
<input checked="" type="checkbox"/>	DESKTOP-0E3CU2L	Area_51	3.9.20.0	21 days ago	QA	
<input checked="" type="checkbox"/>	DESKTOP-56MSF8M	JL-PC	3.9.24.0	2 hours ago	Accounts	
<input type="checkbox"/>	DESKTOP-C3PEVEC	Sid	9.0.0.0	3 months ago	Engineering	
<input type="checkbox"/>	DESKTOP-D3B27R5	Organization	3.0.15.0	2 years ago	General	

If you want to put all the selected computers in one **Group**, you can use the [Use same group for all](#) option to assign the current **Group** that the computer is into all selected PCs. All users in that **Group** will have access to all the computers in that group.

Name	Group
UL-BLACK-05	A
ABE	A
admins-mac-pro	A

This computer's group will be filled automatically in all dropdowns.

[Use same group for all](#)

If you don't want to use the same **Group**, then click the drop-down box for each computer and select the **Group**. Click **Save** to proceed.

Computer	Group	Actions
99	A	Use same group for all
COOLCAD-SERVER	Organization	
COOLCAD-SLIM-03	A	
DESKTOP-0E3CU2L	Abe PC	
DESKTOP-56MSF8M	Alex	
	Alex Lee	
	Area_51	
	Business Team's Test Group	

The **Update Client Software** tab allows you to check for and schedule any new software updates.

Manage Computers Info X

Profile Groups Computer-Specific Credential **Update Client Software**

Target Version: 3.9.24 [Check for Updates](#)

Update Time: 2019-12-26 16:34:10

* Only computers marked "Ready to update" will be updated. Check the list for any machine that cannot be updated.

Computer	Version	OS	Status
99		macOS	Only Windows machines can be updated.
COOLCAD-SERVER	3.8.6.0	Windows	Last seen 3 months ago. Make sure it is active.
COOLCAD-SLIM-03	3.2.3.0	Windows	Required current version > 3.8.1.
DESKTOP-0E3CU2L	3.9.20.0	Windows	Last seen 21 days ago. Make sure it is active.
DESKTOP-56MSF8M	3.9.24.0	Windows	Latest Version already installed.

[Disable Updates](#) [Enable Updates](#)

4.2 Groups View

Groups View shows computers by assigned **Group**. Click a **Group** to see all computers assigned to it.

Computers View **Groups View** Deactivated computers

Search

Group	Computers
Organization	33 Computers
A	10 Computers
Alex	2 Computers

Manage Computers Deactivate Computers Selected 0 of 2 computers. [Select all computers in the table](#)

Computer	Version	Last Seen	Department	Actions
UL-LAPTOP-07	3.4.3.0	7 months ago	General	
UL-LAPTOP-10	3.3.4.0	7 months ago	General	

Alex Lee 1 Computers

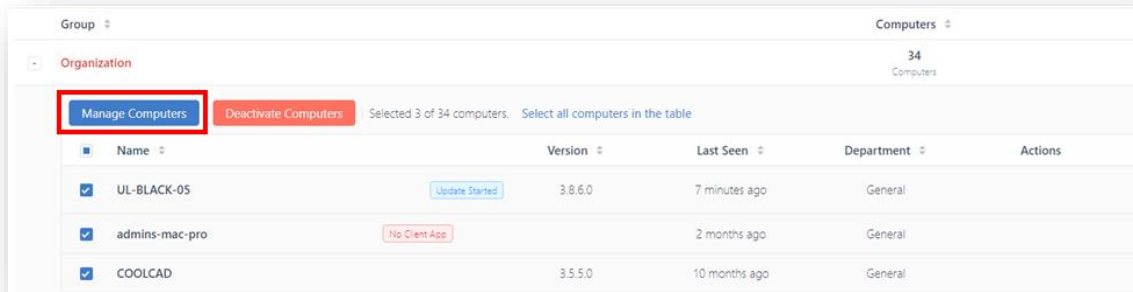
Area_51 9 Computers

Business Team's Test Group 3 Computers

To move a computer to another **Group** (gives another user permission to use that computer), hover over the desired computer, click [Manage](#).

Name	Version	Last Seen	Department	Actions
UL-BLACK-05	3.8.6.0	4 minutes ago	General	Clear Status Update Started Manage Deactivate

To move multiple computers, select all the desired computers and click **Manage Computers**.

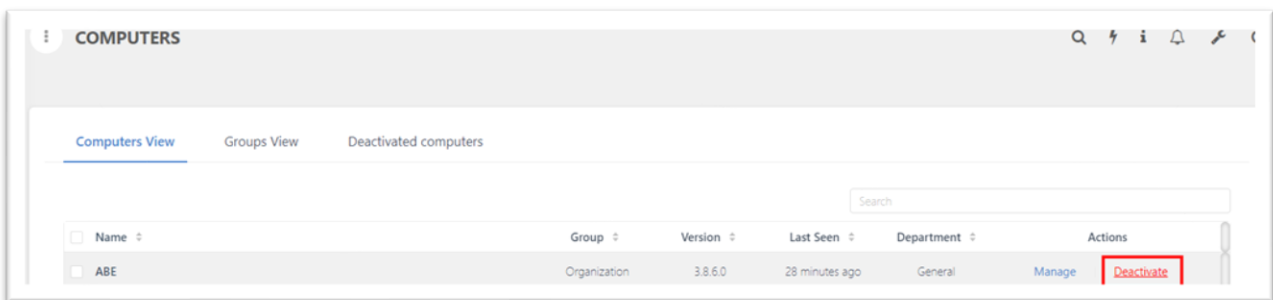


4.3 Deactivate Computers

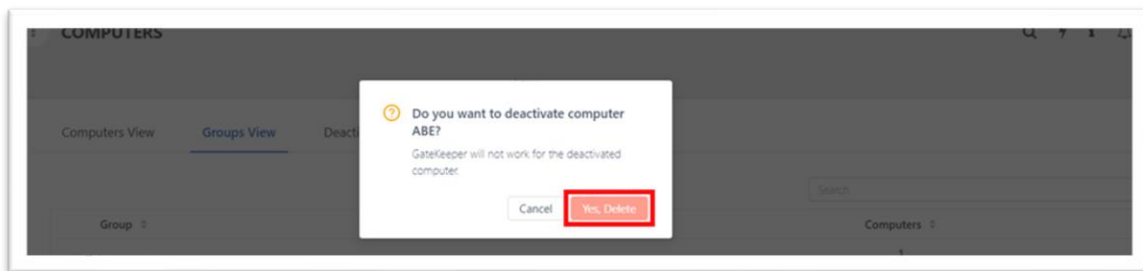
Deactivated computers can't be interacted with through the Hub or Client applications.

4.3.1.1 Deactivating a Single Computer

To deactivate a computer, hover over the desired computer. Below **Actions**, click [Deactivate](#).

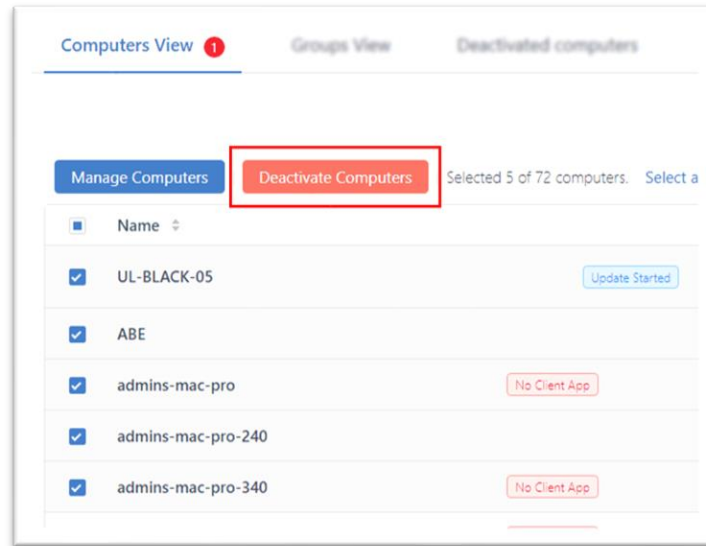


Confirm that the computer you clicked [Deactivate](#) on is correct. Click **"Yes, Delete"** to confirm.

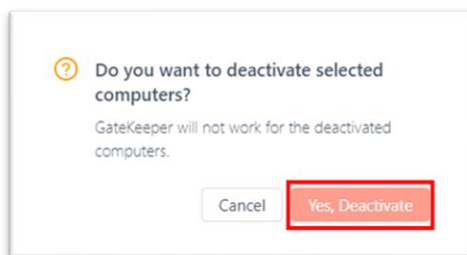


4.3.1.2 Deactivating Multiple Computers

To deactivate multiple computers, select all the desired computers. Click **Deactivate Computers**.

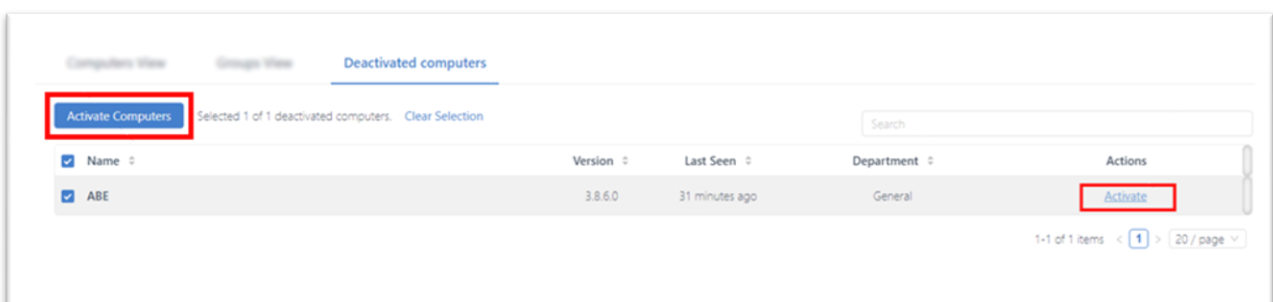


A small prompt window will ask you to confirm the action. Click **“Yes, Deactivate”** to finish.

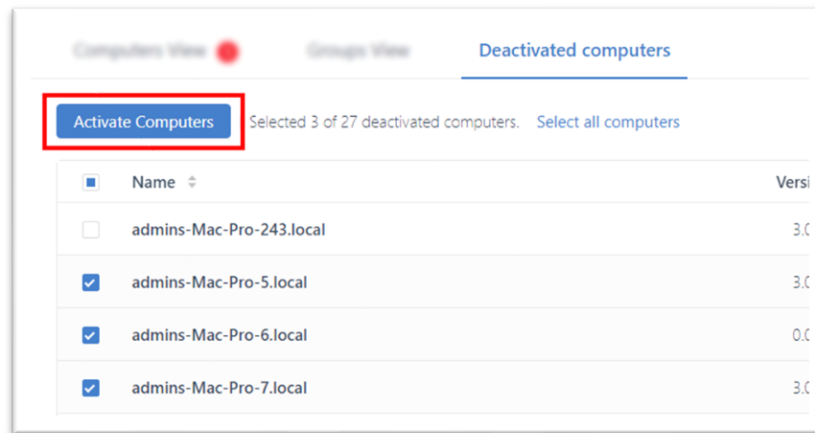


4.3.1.3 Activating Deactivated Computers

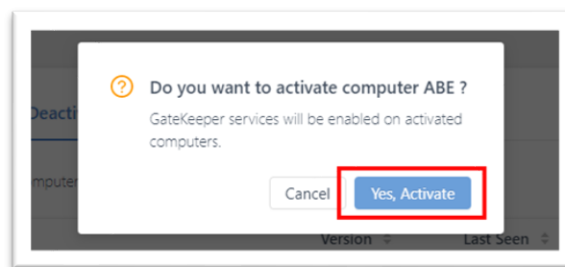
Select the [Activate](#) option under the **Actions** tab for a single computer.



For multiple computers, click **“Activate Computers”** in the top left corner.

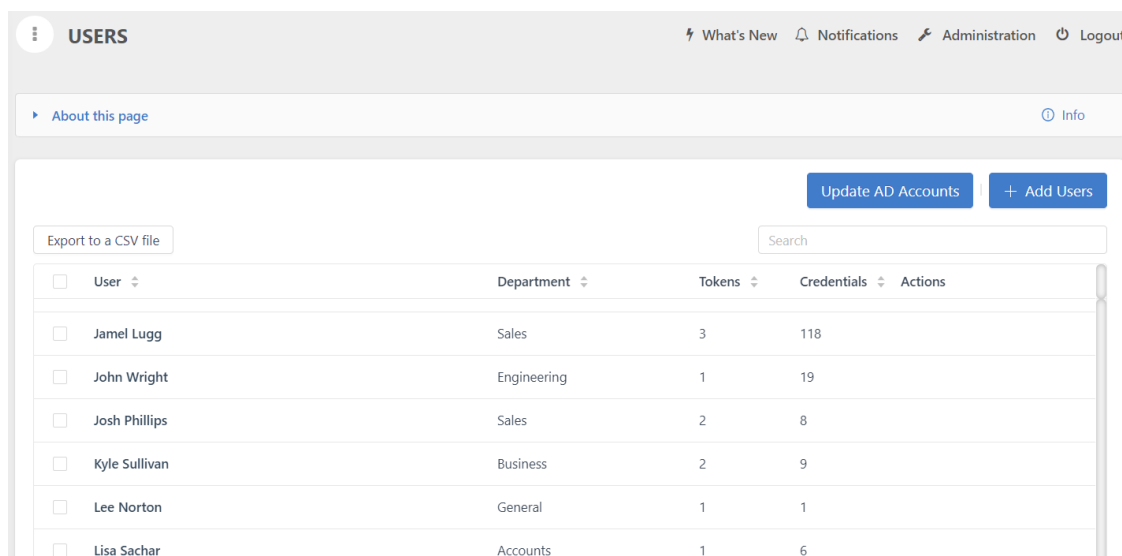


Click “Yes, Activate”.



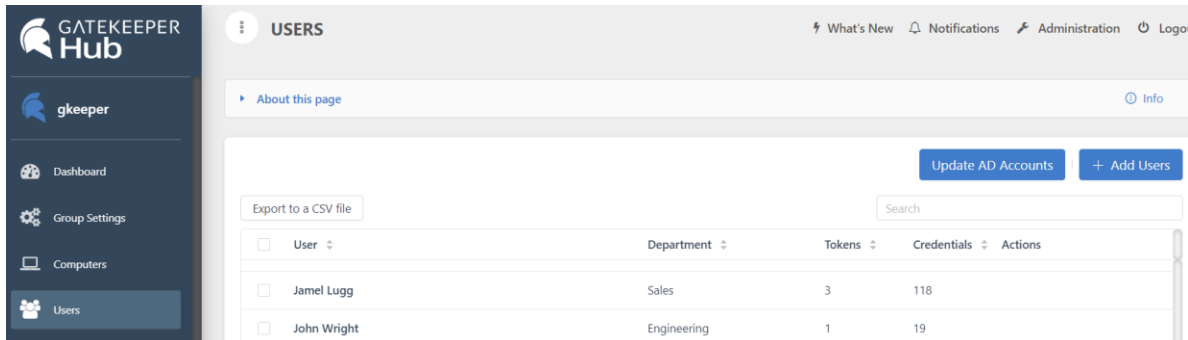
5 Users

Add new users to the GateKeeper Hub. Also displays all user accounts registered on the GateKeeper network with their names, email, phone number, department, tokens, Groups, and credentials.



5.1 Add New Users

Users can be added to the GateKeeper Hub either from the Client desktop application or the **Users** tab in the Hub.

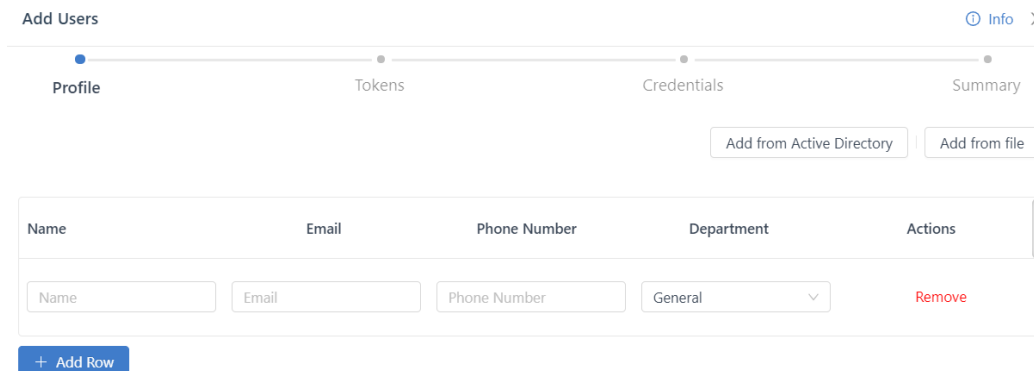


5.1.1.1 Add a Single User

Click **Add Users**.

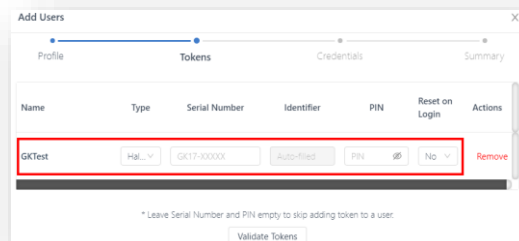
+ Add Users

Enter the name, email, phone number, and department for the user, and click **Next**.



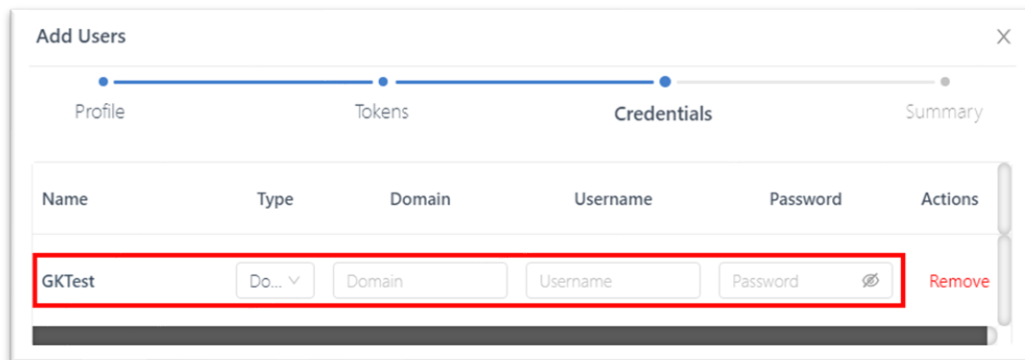
Enter the information to be added to the account. You can click **Validate Tokens** now to check if the token's serial number has been filled in correctly, or GateKeeper will confirm automatically, later.

Alternatively, you can leave the fields empty and skip this step.



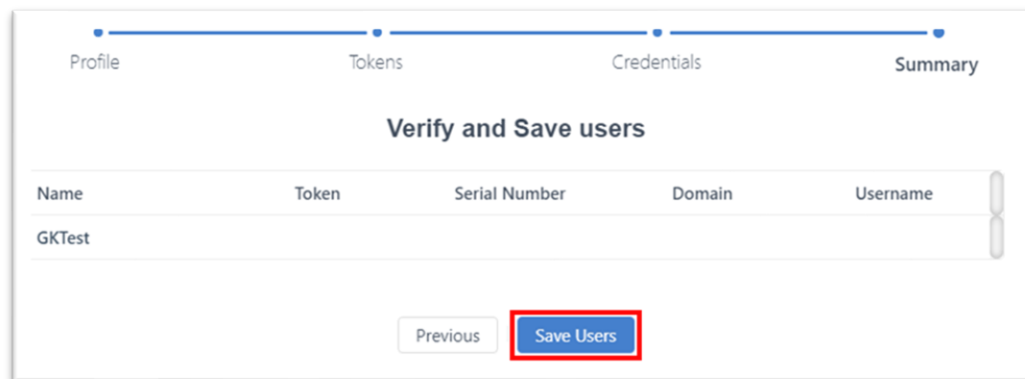
You can then add the different credentials you want the account to have.

Alternatively, you can leave the fields empty and skip this step.



Name	Type	Domain	Username	Password	Actions
GKTest	Do...				Remove

Verify the information is correct, then click **Save User** to add the user to the database.



Name	Token	Serial Number	Domain	Username
GKTest				

Previous **Save Users**

5.1.1.2 Add Multiple Users

On the **Users** page, click **Add Users**.



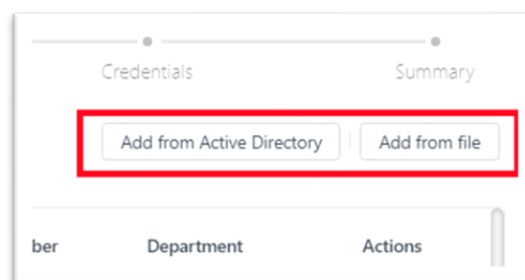
USERS

What's New Notifications Administration Logout

About this page Info

Update AD Accounts + Add Users

Select either **Add from Active Directory** or **Add from file** to upload multiple users via CSV file.



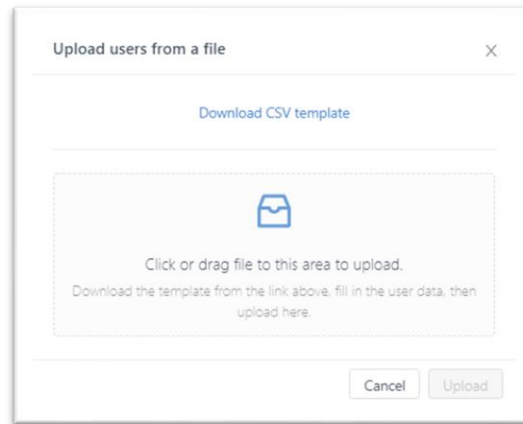
Credentials Summary

Add from Active Directory Add from file

ber Department Actions

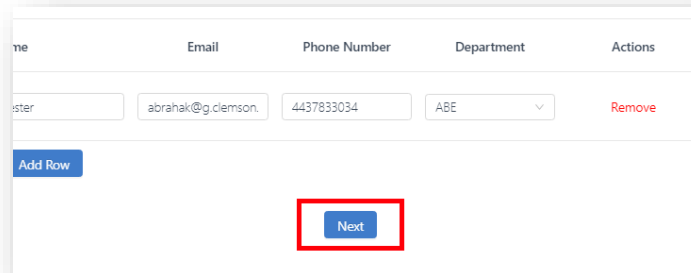
Selecting **Add from file** brings up this pop-up window.

Click [Download the CSV template](#) and input all the desired users into the file.

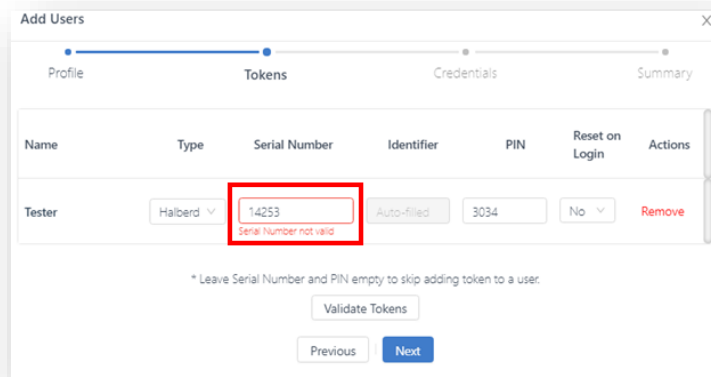


Click or drag the file into the designated area on the screen to upload the users to the Hub.

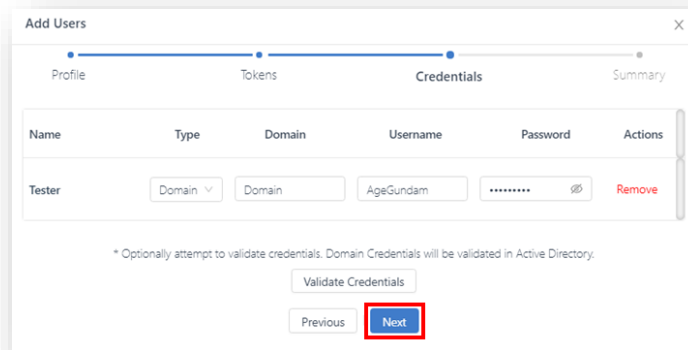
Once you have uploaded the file, click **Next**.



Once the file is uploaded, look for any incorrect information regarding the tokens. Click **Next**.



The next page will be where you can upload credentials for each user. Click **Next**.



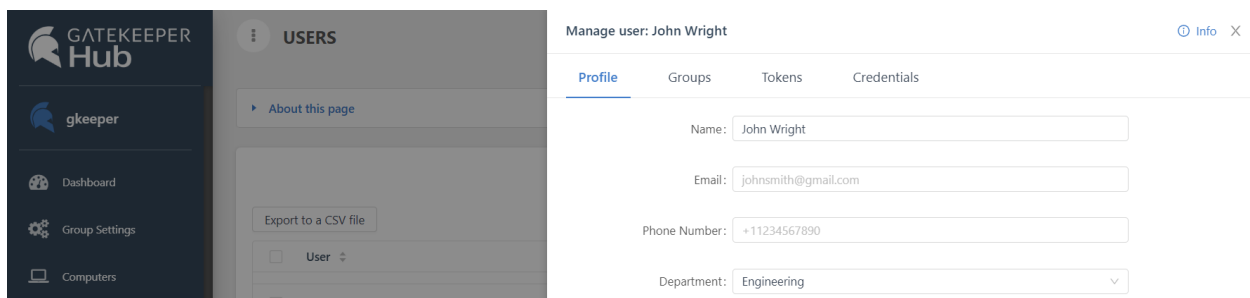
Look over the information and click **Save Users** to finish uploading users.

5.1.1.3 User Management Page

To view a user's details or to add a new token and/or credential, go to the **Users** page. In the **Actions** column, click [Manage](#) next to the desired user.

<input type="checkbox"/>	Name	Department	Tokens	Credentials	Actions
<input type="checkbox"/>	Abe Kim	Test Department 2	1	15	Manage Delete

A side panel window will appear from the right side of the screen.



At the **User Management Page**, you can view the profile of the user, what **Group** they are in, their tokens, and their credentials.

Profile	Groups	Tokens	Credentials
----------------	--------	--------	-------------

5.1.1.4 Profile

The user's name, email address, phone number, and department is displayed here.

Manage user: John Wright Info X

[Profile](#)
[Groups](#)
[Tokens](#)
[Credentials](#)

Name:

Email:

Phone Number:

Department:

5.1.1.5 Groups

Shows the **Group(s)** that the **User** is assigned and which **Group(s)** the user does NOT have access to. If a user needs access to a computer, they need to be added to the **Group** that the computer is in.

Manage user: Angela Davis X

[Profile](#)
[Groups](#)
[Tokens](#)
[Credentials](#)

Selected users currently **HAVE** access to computers in these groups.

Group	Actions
Macs	
Organization	

Selected users currently **DO NOT HAVE** access to computers in these groups.

Group	Actions
A	
Abe PC	
Alex	
Alex Lee	
Area_51	
Business Team's Test Group	

To add or revoke access to a **Group** for a user, go to the **Actions** column.

Manage user: Angela Davis

[Profile](#)
[Groups](#)
[Tokens](#)
[Credentials](#)

Selected users currently **HAVE** access to computers in these groups.

Group	Actions
Macs	Revoke

Click [Revoke](#) for the **Group** that the user that is already a member of or [Add](#) for the **Group** that the user does not have access to.

Manage user: John Wright

Profile **Groups** Tokens Credentials

Selected users currently **HAVE** access to computers in these groups.

Group	Actions
Macs	Revoke
Organization	

Selected users currently **DO NOT HAVE** access to computers in these groups.

Group	Actions
-------	---------

5.1.1.6 Add or Delete GateKeeper Tokens

All the tokens associated with a user (phone with Trident app or Halberd) will be displayed here with their Type, Serial, MAC Address, and Battery status last recorded on the token.

Manage user: Angela Davis

Profile Groups **Tokens** Credentials

[+ Add Token](#)

Search

Type	Serial	Mac Address	Battery	Actions
Halberd	GK17-13001	E5:61:BD:84:75:DC	--	

If you misplace your token, please inform your admin and ask them to delete the token from your user account to avoid anyone else from potentially using the token. Click [here](#) for instructions.

If you forgot the PIN associated with your GateKeeper token, you can reset it by going to the **Actions** column and clicking [Change PIN](#) next to the desired token.

Type	Serial	Mac Address	Battery	Actions
Halberd	GK17-13001	E5:61:BD:84:75:DC	--	Change PIN Delete

Enter your new PIN, retype new PIN, and click **Save**. Now you can access your credentials with the new PIN. If you want to create a new PIN after you log in, you can select the **Reset PIN at next login** option.

Change PIN for Token: GK17-13001

* indicates a required field.

New PIN *:

Confirm PIN *:

☐ Reset PIN at next login

To register a new token, click **Add Token**.

Profile	Groups	Tokens	Credentials
			+ Add Token

Select the type of token (Halberd, Android, iPhone, Smart Badge) and then enter the serial number printed on the inside the battery cover. If you are using your phone as your GateKeeper, please open your Trident app to find your soft token serial number.

Add Token

* indicates a required field.

Token Type:

Serial Number *:

Mac Address *:

Halberd

Android

iPhone

GKBadge

Click **Validate**.

✓

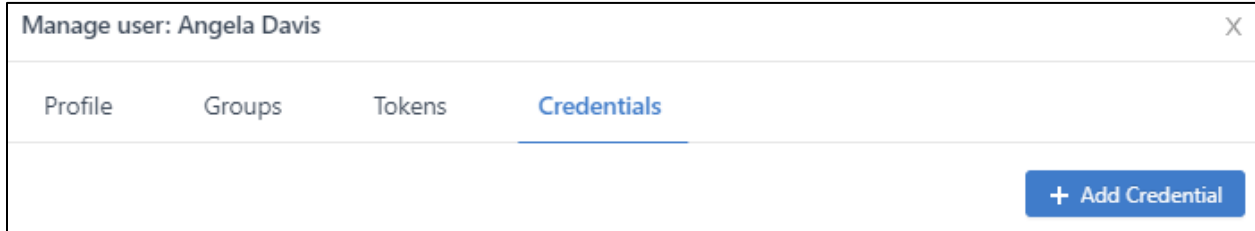
Serial Number *:

Validate

The MAC address will get updated automatically, choose a PIN for the token, retype PIN to confirm. If you're registering a token for a different user (e.g. admin onboarding a new employee), check '**Reset PIN at next login**'. This will allow the end-user to change their token's PIN at their next login. Click **Save** to add this token to the user. Now all the credentials are associated to this token as well.

5.1.1.7 Passwords

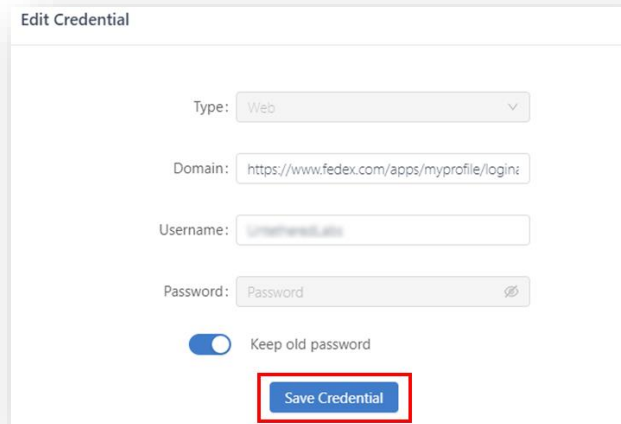
All credentials (Web, OTP, Mac Local, Windows Local) associated with a user will be displayed here. If you've added the user using the GateKeeper client application, then the credential (domain, local) the user's token was registered with will be displayed here.



To update an existing credential, such as changing a username or password, under the **Actions** column, click [Edit](#) next to the desired credential.

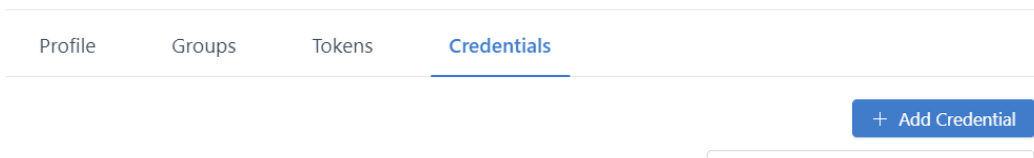
Type	Domain	Username	Actions
WEB	https://www.fedex.com/apps/myprofile/loginandcontact/	untetheredlabs	Edit Delete

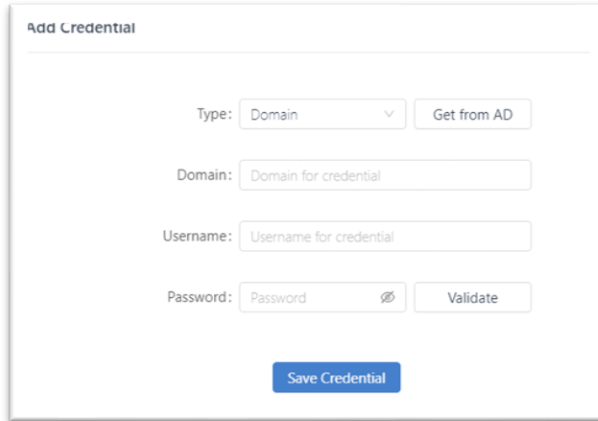
After making the changes, click **Save Credential**.



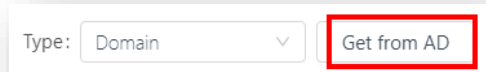
To add a new credential to an existing user, click **Add Credential**.

** You can also add credentials using the GateKeeper Client desktop application or GateKeeper Chrome extension (websites only).*



A screenshot of the 'Add Credential' form in the GateKeeper Hub. The form has a title 'Add Credential' at the top. Below the title, there are four rows of input fields. The first row is 'Type:' with a dropdown menu showing 'Domain' and a 'Get from AD' button. The second row is 'Domain:' with a text input field containing 'Domain for credential'. The third row is 'Username:' with a text input field containing 'Username for credential'. The fourth row is 'Password:' with a text input field containing 'Password', a small eye icon, and a 'Validate' button. At the bottom of the form is a blue 'Save Credential' button.

Select the type of credential (Web, OTP, Mac Local or Windows Local), enter the domain, and username manually or get it from the Active Directory by clicking 'Get from AD'.

A close-up screenshot of the 'Type:' dropdown menu and the 'Get from AD' button. The 'Get from AD' button is highlighted with a red rectangular border.

Leave the password field blank to update it later from the lock screen on any computer your credential has access to.

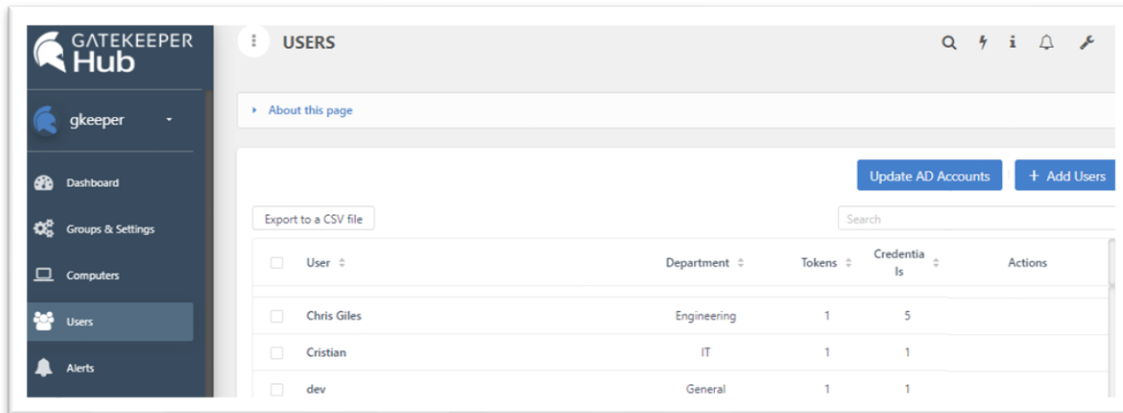
Click **Save Credential**. Now all the tokens the user has can be used to log in using this credential.

NOTE - To add login credentials for a local account, enter the computer name as the **Domain**.

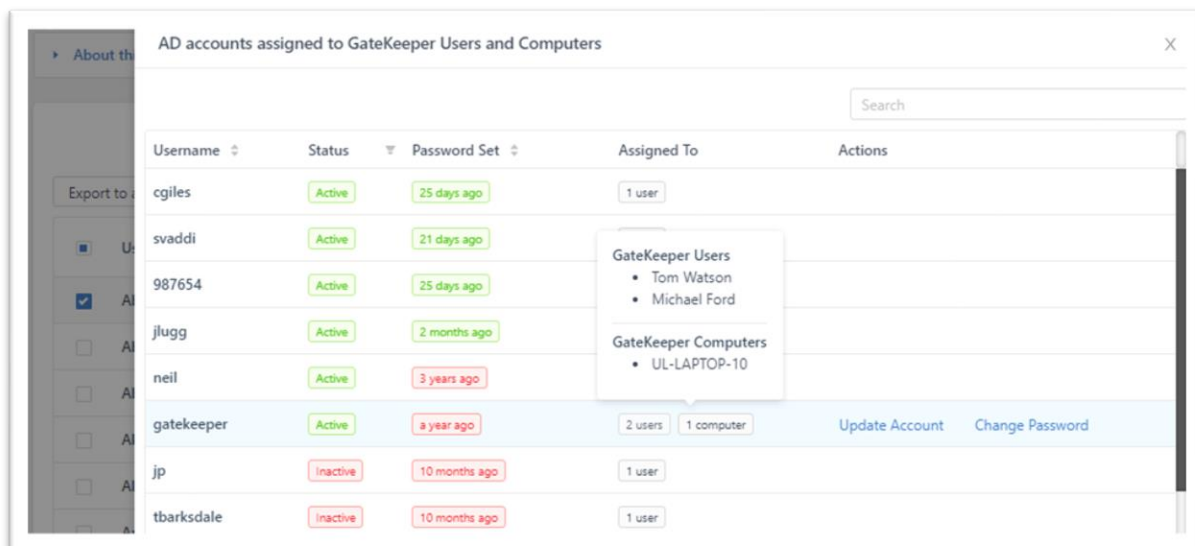
5.2 Update AD Accounts

IT admins can change each users' Active Directory (AD) passwords and accounts directly from the GateKeeper Hub to save a tremendous amount of time and effort.

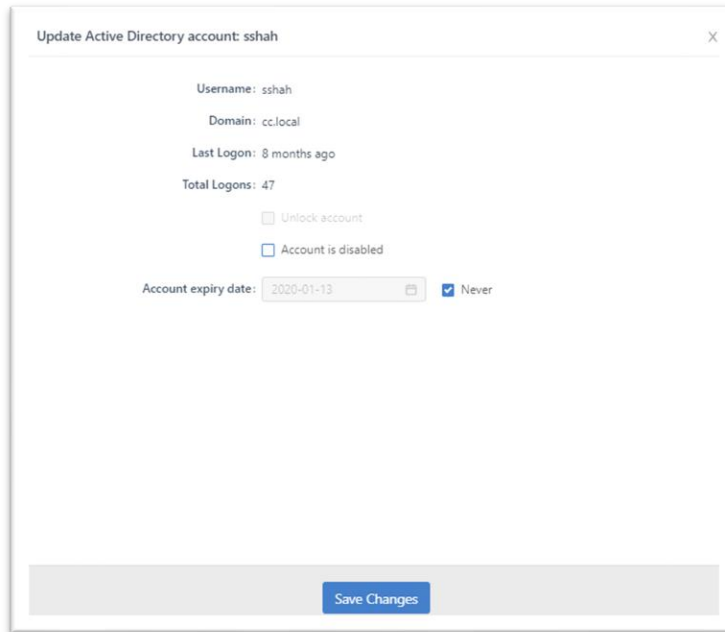
1. Log in to your **GateKeeper Hub**.
2. Go to the "**Users**" tab on the left side.
3. Click the blue button for "**Update AD Accounts**" in the upper-right.



4. Hover over a username and click "Update Account" or "Change Password" under the Actions column on the right side.



Update Active Directory Account:



Update Active Directory account: sshah

Username: sshah

Domain: cc.local

Last Logon: 8 months ago

Total Logons: 47

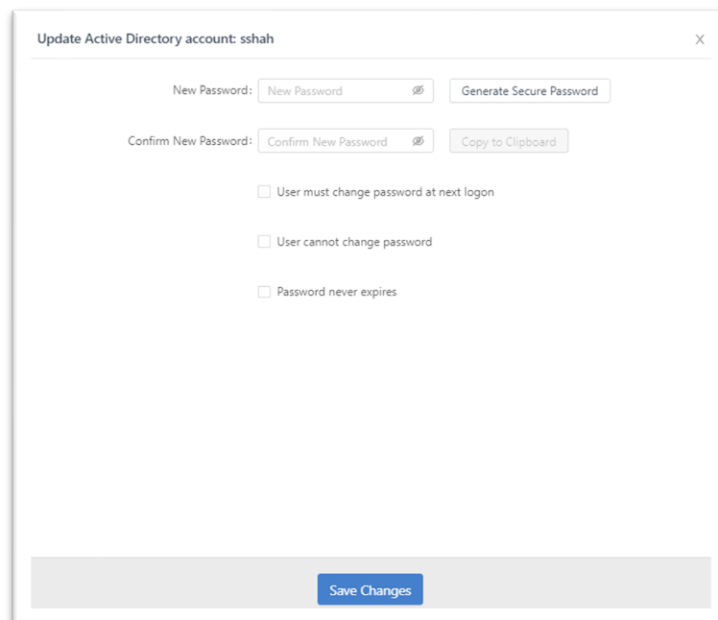
☐ Unlock account

☐ Account is disabled

Account expiry date: 2020-01-13 ☒ Never

Save Changes

Change AD Password:



Update Active Directory account: sshah

New Password:

Confirm New Password:

☐ User must change password at next logon

☐ User cannot change password

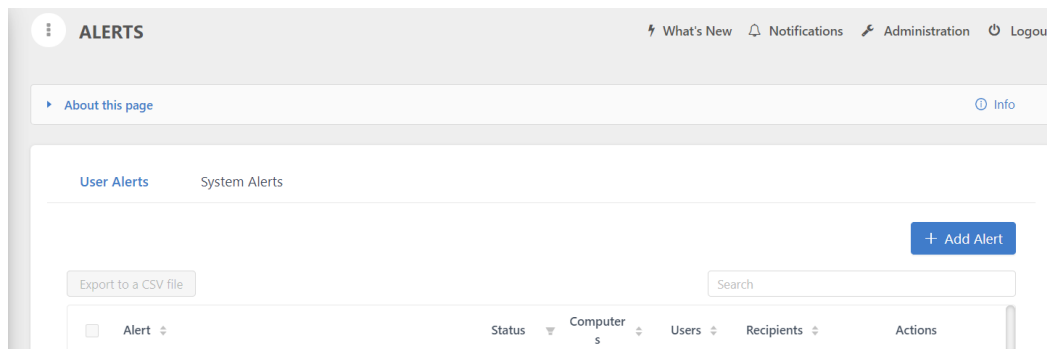
☐ Password never expires

Save Changes

6 Alerts

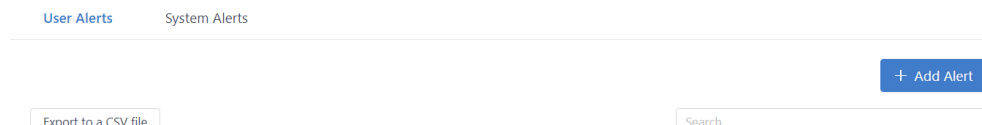
There are two types of alerts: **User Alerts** and **System Alerts**. Never miss critical alerts.

User Alerts

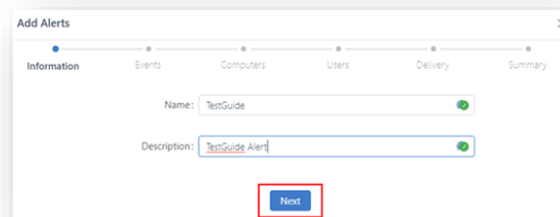


6.1.1.1 Add Alert

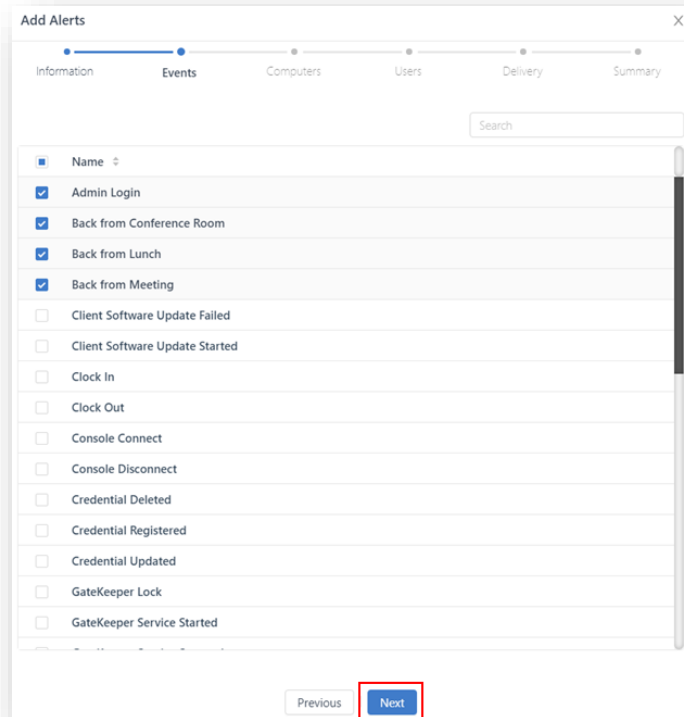
To add your own custom alerts, click **Add Alert**.



Enter the **Name** and **Description** for your **Alert**. Then click **Next** to proceed.



Then you can select the events to assign to the **Alert**. Click **Next**.



Add Alerts

Information Events Computers Users Delivery Summary

Search

Name	Selected
Admin Login	<input checked="" type="checkbox"/>
Back from Conference Room	<input checked="" type="checkbox"/>
Back from Lunch	<input checked="" type="checkbox"/>
Back from Meeting	<input checked="" type="checkbox"/>
Client Software Update Failed	<input type="checkbox"/>
Client Software Update Started	<input type="checkbox"/>
Clock In	<input type="checkbox"/>
Clock Out	<input type="checkbox"/>
Console Connect	<input type="checkbox"/>
Console Disconnect	<input type="checkbox"/>
Credential Deleted	<input type="checkbox"/>
Credential Registered	<input type="checkbox"/>
Credential Updated	<input type="checkbox"/>
GateKeeper Lock	<input type="checkbox"/>
GateKeeper Service Started	<input type="checkbox"/>

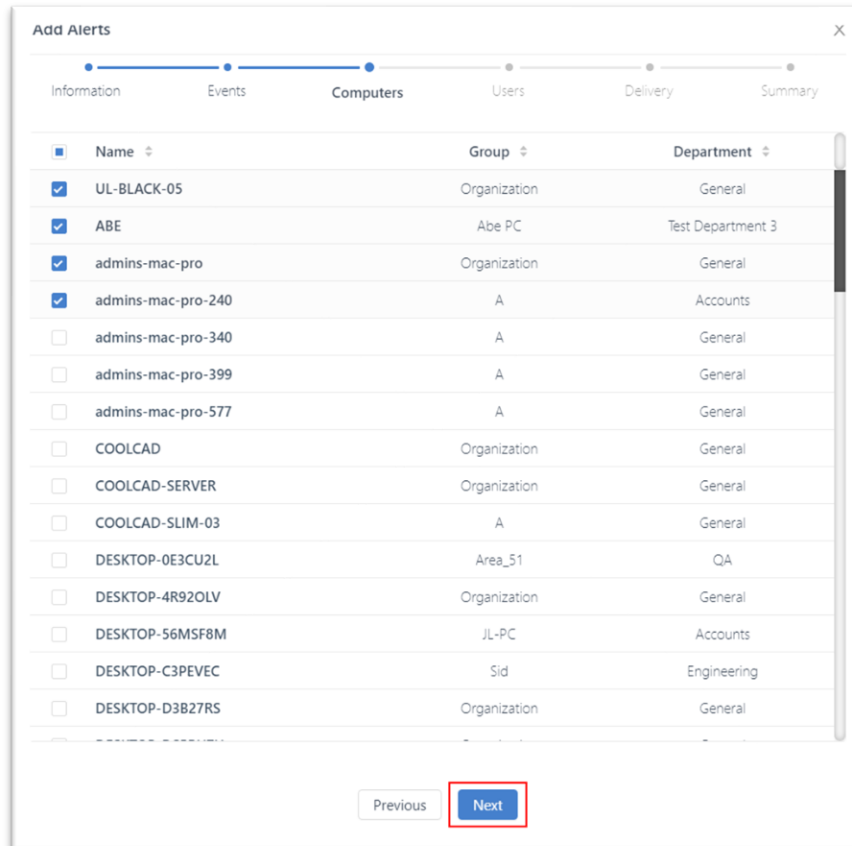
Previous **Next**

Below is a list of all the “Events” options available:

- Admin Login
- Back from Conference Room
- Back from Lunch
- Back from Meeting
- Client Software Update Failed
- Client Software Update Started
- Clock In
- Clock Out
- Console Connect
- Console Disconnect
- Credential Deleted
- Credential Registered
- Credential Updated
- GateKeeper Lock
- GateKeeper Service Started
- GateKeeper Service Stopped
- GateKeeper Unlock
- In Conference Room
- Login Failed

Non-GateKeeper Lock
 Non-GateKeeper Unlock
 Out for Lunch
 Out for Meeting
 Remote Disconnect
 Session Locked
 Session Logoff
 Session Logon
 Session Unlocked
 Token Deleted
 Token PIN has been Reset
 Token Registered
 Update Successful
 User Connected
 User Disconnected
 User Registered
 Web Credential Used

Then you can select the **Computers** to be a part of the **Alerts**. Click **Next**.



Add Alerts

Information Events **Computers** Users Delivery Summary

<input type="checkbox"/>	Name	Group	Department
<input checked="" type="checkbox"/>	UL-BLACK-05	Organization	General
<input checked="" type="checkbox"/>	ABE	Abe PC	Test Department 3
<input checked="" type="checkbox"/>	admins-mac-pro	Organization	General
<input checked="" type="checkbox"/>	admins-mac-pro-240	A	Accounts
<input type="checkbox"/>	admins-mac-pro-340	A	General
<input type="checkbox"/>	admins-mac-pro-399	A	General
<input type="checkbox"/>	admins-mac-pro-577	A	General
<input type="checkbox"/>	COOLCAD	Organization	General
<input type="checkbox"/>	COOLCAD-SERVER	Organization	General
<input type="checkbox"/>	COOLCAD-SLIM-03	A	General
<input type="checkbox"/>	DESKTOP-0E3CU2L	Area_51	QA
<input type="checkbox"/>	DESKTOP-4R92OLV	Organization	General
<input type="checkbox"/>	DESKTOP-56MSF8M	JL-PC	Accounts
<input type="checkbox"/>	DESKTOP-C3PEVEC	Sid	Engineering
<input type="checkbox"/>	DESKTOP-D3B27RS	Organization	General

Previous **Next**

Then you can assign users to be a part of the **Alerts**. Click **Next**.

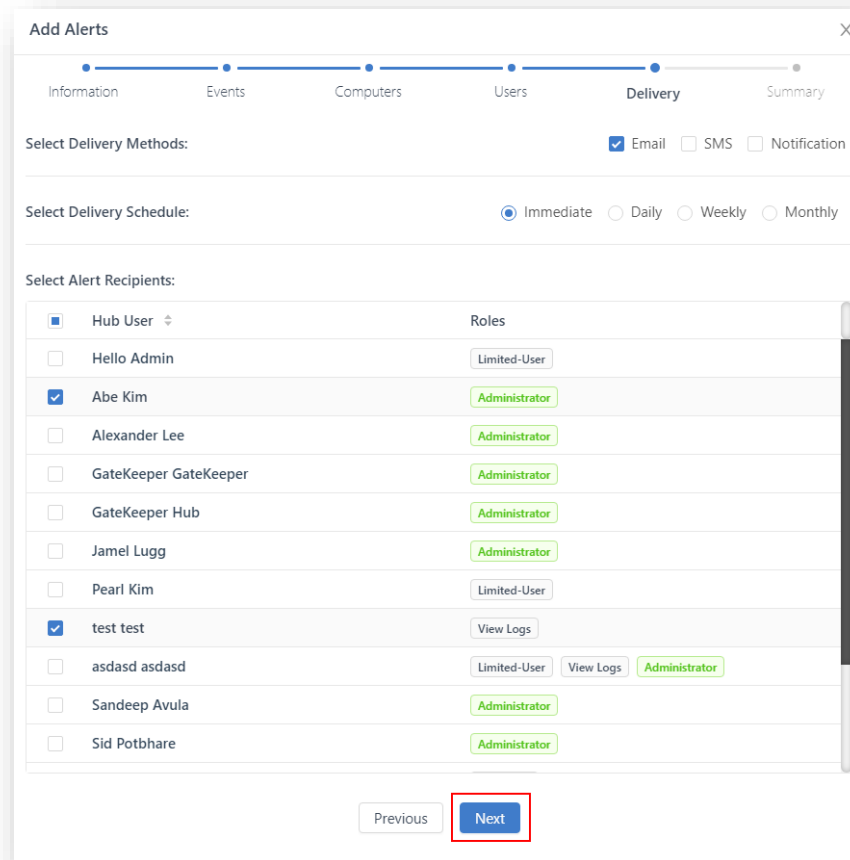
Add Alerts
×

Information
Events
Computers
Users
Delivery
Summary

<input type="checkbox"/> Name	Department
<input checked="" type="checkbox"/> Abe Kim	Test Department 2
<input checked="" type="checkbox"/> Abhinav	General
<input checked="" type="checkbox"/> Abhinav Jain	General
<input type="checkbox"/> AJ	IT
<input type="checkbox"/> Ajay Chandhok	General
<input type="checkbox"/> Akin Akturk	General
<input type="checkbox"/> Alex Lee	Business
<input type="checkbox"/> Amitabh Bachhan	HomeOffice
<input type="checkbox"/> Andy Stoller	Marketing
<input type="checkbox"/> Angela Davis	Engineering
<input type="checkbox"/> Cecil Clarke	General
<input type="checkbox"/> Chetan Shenoy	QA
<input type="checkbox"/> Chris Giles	Engineering
<input type="checkbox"/> Cristian	IT
<input type="checkbox"/> CSV User 1	Accounts

Previous
Next

Then you can select the **Delivery Method**, Delivery Schedule, and **Alert** recipients. Click **Next**.



Add Alerts

Information Events Computers Users **Delivery** Summary

Select Delivery Methods: ☒ Email ☐ SMS ☐ Notification

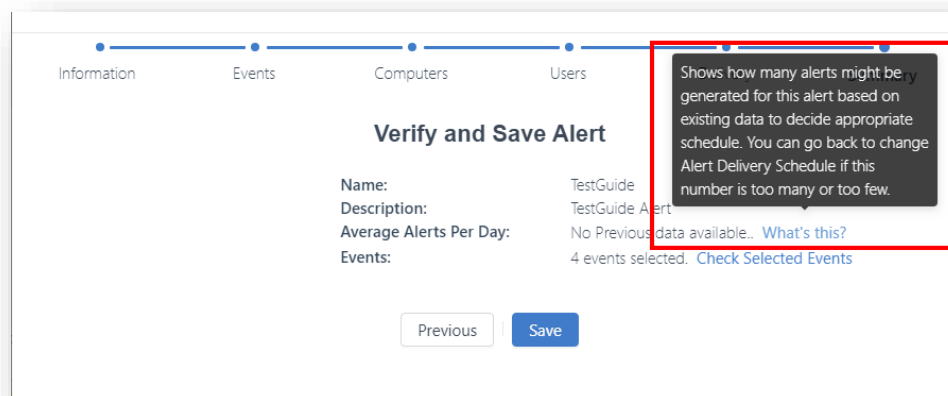
Select Delivery Schedule: ☒ Immediate ☐ Daily ☐ Weekly ☐ Monthly

Select Alert Recipients:

Hub User	Roles
<input type="checkbox"/> Hello Admin	Limited-User
<input checked="" type="checkbox"/> Abe Kim	Administrator
<input type="checkbox"/> Alexander Lee	Administrator
<input type="checkbox"/> GateKeeper GateKeeper	Administrator
<input type="checkbox"/> GateKeeper Hub	Administrator
<input type="checkbox"/> Jamel Lugg	Administrator
<input type="checkbox"/> Pearl Kim	Limited-User
<input checked="" type="checkbox"/> test test	View Logs
<input type="checkbox"/> asdasd asdasd	Limited-User View Logs Administrator
<input type="checkbox"/> Sandeep Avula	Administrator
<input type="checkbox"/> Sid Potbhare	Administrator

Previous **Next**

If you hover over the [What's this?](#) option, it will explain what is meant by **Average Alerts Per Day**.



Information Events Computers Users

Verify and Save Alert

Name: TestGuide

Description: TestGuide Alert

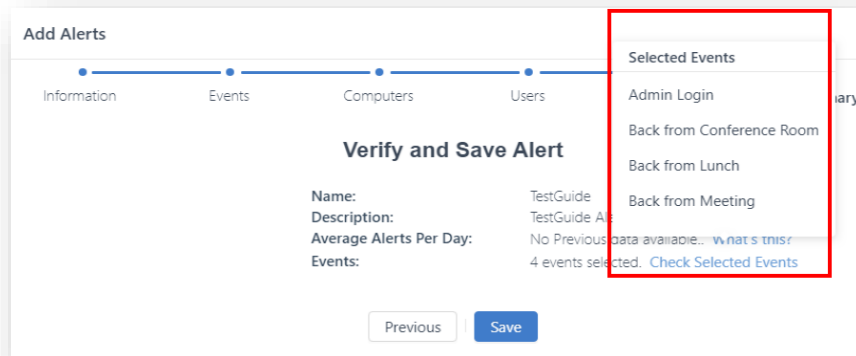
Average Alerts Per Day: No Previous data available.. [What's this?](#)

Events: 4 events selected. [Check Selected Events](#)

Previous **Save**

Shows how many alerts might be generated for this alert based on existing data to decide appropriate schedule. You can go back to change Alert Delivery Schedule if this number is too many or too few.

To see the Events you have selected to be alerted on, click [Check Selected Events](#).



Add Alerts

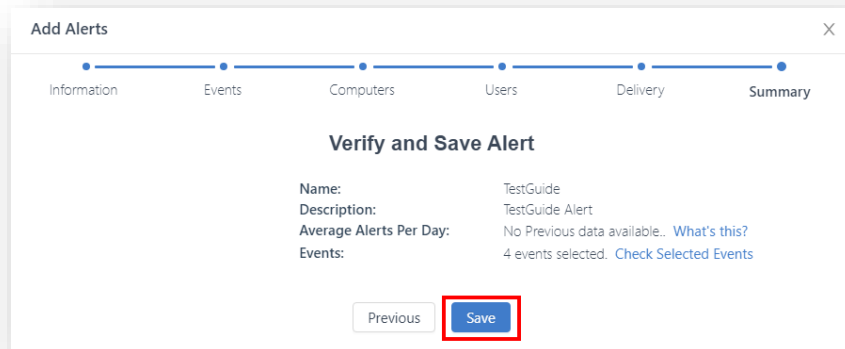
Information Events Computers Users

Verify and Save Alert

Name: TestGuide
Description: TestGuide Alert
Average Alerts Per Day: No Previous data available.. [What's this?](#)
Events: 4 events selected. [Check Selected Events](#)

Previous Save

If everything looks correct, click **Save** to add and activate your new **Alert**.



Add Alerts

Information Events Computers Users Delivery Summary

Verify and Save Alert

Name: TestGuide
Description: TestGuide Alert
Average Alerts Per Day: No Previous data available.. [What's this?](#)
Events: 4 events selected. [Check Selected Events](#)

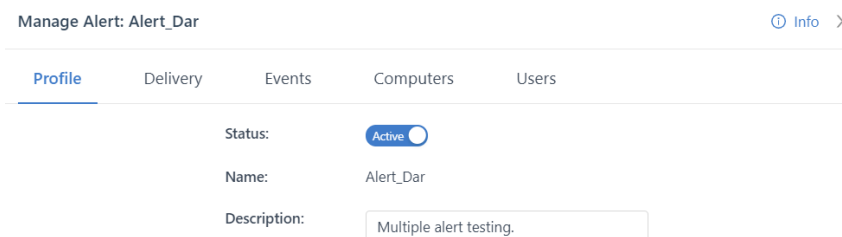
Previous **Save**

6.1.1.2 Manage Alerts

If you need to make any changes to an **Alert**, hover over the alert and click **Manage**.

<input type="checkbox"/>	Name ▾	Status ▾	Computers ▾	Users ▾	Recipients ▾	Actions
<input type="checkbox"/>	Alert_Dar Multiple alert testing.	Active	1	1	1	Manage Delete

This will bring up the “**Manage Alert: [Alert’s name]**” side panel window that opens up to the **Profile** tab. Here, you can change the description of the alert. Click **Save Profile**.



Manage Alert: Alert_Dar ⓘ Info X

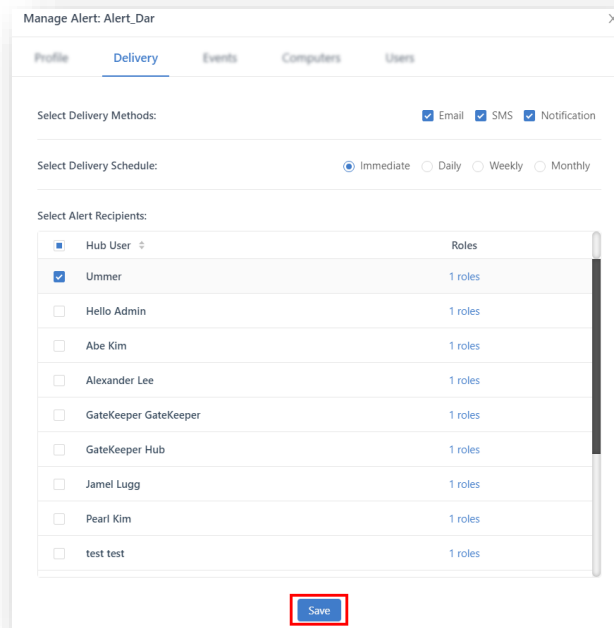
Profile Delivery Events Computers Users

Status: **Active**

Name: Alert_Dar

Description:

On the **Delivery** tab you can change the delivery method, delivery schedule, and **Alert** recipients.



Manage Alert: Alert_Dar

Profile Delivery Events Computers Users

Select Delivery Methods: ☒ Email ☒ SMS ☒ Notification

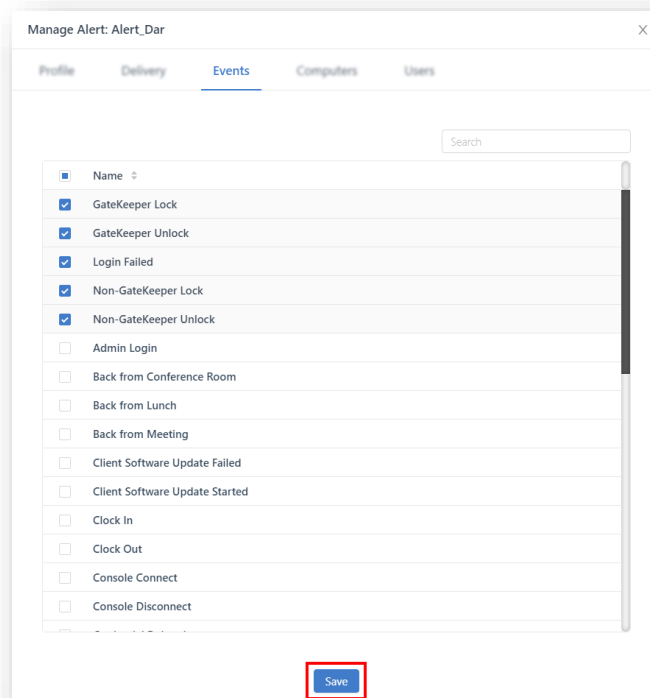
Select Delivery Schedule: ☒ Immediate ☐ Daily ☐ Weekly ☐ Monthly

Select Alert Recipients:

Hub User	Roles
<input checked="" type="checkbox"/> Ummer	1 roles
<input type="checkbox"/> Hello Admin	1 roles
<input type="checkbox"/> Abe Kim	1 roles
<input type="checkbox"/> Alexander Lee	1 roles
<input type="checkbox"/> GateKeeper GateKeeper	1 roles
<input type="checkbox"/> GateKeeper Hub	1 roles
<input type="checkbox"/> Jamel Lugg	1 roles
<input type="checkbox"/> Pearl Kim	1 roles
<input type="checkbox"/> test test	1 roles

Save

On the **Events** tab, you can change the selected **Events** for the Alert. Click **Save**.



Manage Alert: Alert_Dar

Profile Delivery Events Computers Users

Search

Name
<input checked="" type="checkbox"/> GateKeeper Lock
<input checked="" type="checkbox"/> GateKeeper Unlock
<input checked="" type="checkbox"/> Login Failed
<input checked="" type="checkbox"/> Non-GateKeeper Lock
<input checked="" type="checkbox"/> Non-GateKeeper Unlock
<input type="checkbox"/> Admin Login
<input type="checkbox"/> Back from Conference Room
<input type="checkbox"/> Back from Lunch
<input type="checkbox"/> Back from Meeting
<input type="checkbox"/> Client Software Update Failed
<input type="checkbox"/> Client Software Update Started
<input type="checkbox"/> Clock In
<input type="checkbox"/> Clock Out
<input type="checkbox"/> Console Connect
<input type="checkbox"/> Console Disconnect

Save

On the **Computers** tab, you can change which computers to receive alerts on. Click **Save**.

Manage Alert: Alert_Dar

Profile
Delivery
Events
Computers
Users

<input checked="" type="checkbox"/>	Name	Group	Department
<input checked="" type="checkbox"/>	DESKTOP-0E3CU2L	Area_51	QA
<input checked="" type="checkbox"/>	UL-BLACK-05	Organization	General
<input checked="" type="checkbox"/>	ABE	Abe PC	Test Department 3
<input type="checkbox"/>	admins-mac-pro	Organization	General
<input type="checkbox"/>	admins-mac-pro-240	A	Accounts
<input type="checkbox"/>	admins-mac-pro-340	A	General
<input type="checkbox"/>	admins-mac-pro-399	A	General
<input type="checkbox"/>	admins-mac-pro-577	A	General
<input type="checkbox"/>	COOLCAD	Organization	General
<input type="checkbox"/>	COOLCAD-SERVER	Organization	General
<input type="checkbox"/>	COOLCAD-SLIM-03	A	General
<input type="checkbox"/>	DESKTOP-4R92OLV	Organization	General
<input type="checkbox"/>	DESKTOP-56MSF8M	JL-PC	Accounts
<input type="checkbox"/>	DESKTOP-C3PEVEC	Sid	Engineering
<input type="checkbox"/>	DESKTOP-D3B27RS	Organization	General

Save

On the **Users** tab, you can change which users receive alerts on. Click **Save**.

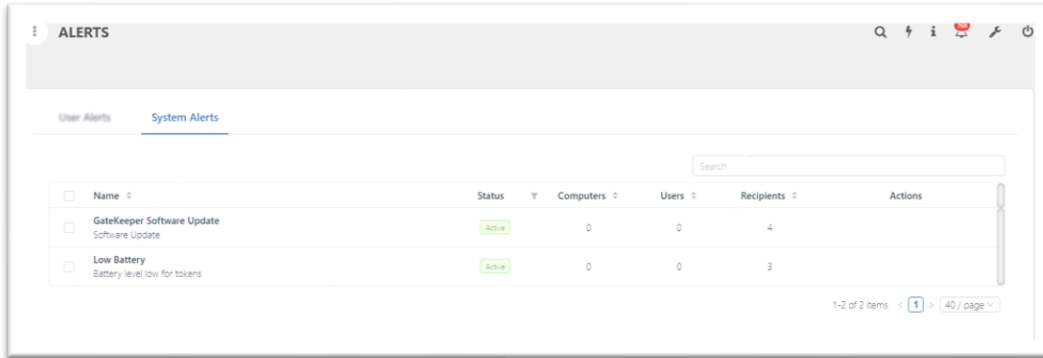
Manage Alert: Alert_Dar

Profile
Delivery
Events
Computers
Users

<input checked="" type="checkbox"/>	Name	Department
<input checked="" type="checkbox"/>	Ummer Dar	QA
<input checked="" type="checkbox"/>	Abe Kim	Test Department 2
<input checked="" type="checkbox"/>	Abhinav	General
<input type="checkbox"/>	Abhinav Jain	General
<input type="checkbox"/>	AJ	IT
<input type="checkbox"/>	Ajay Chandhok	General
<input type="checkbox"/>	Akin Akturk	General
<input type="checkbox"/>	Alex Lee	Business
<input type="checkbox"/>	Amitabh Bachhan	HomeOffice
<input type="checkbox"/>	Andy Stoller	Marketing
<input type="checkbox"/>	Angela Davis	Engineering
<input type="checkbox"/>	Cecil Clarke	General
<input type="checkbox"/>	Chetan Shenoy	QA
<input type="checkbox"/>	Chris Giles	Engineering
<input type="checkbox"/>	Cristian	IT

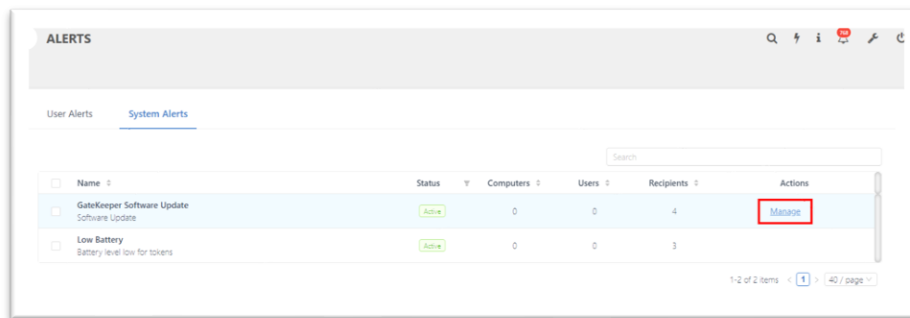
Save

System Alerts

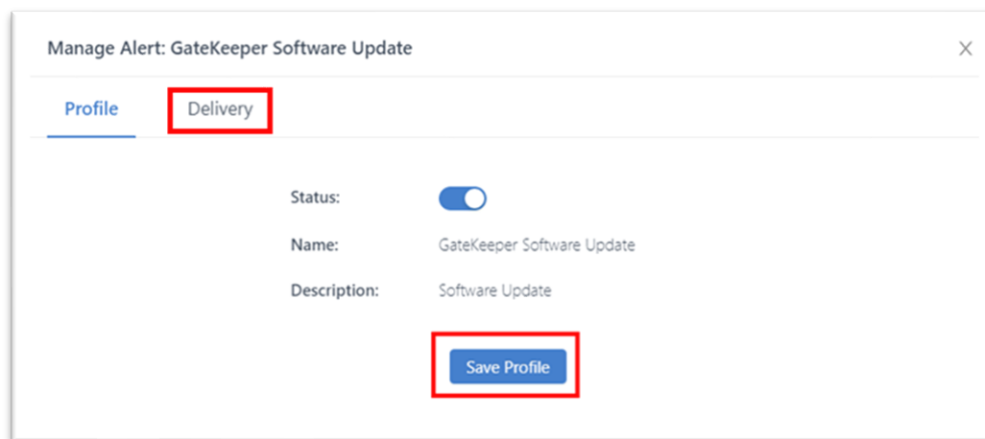


6.1.1.3 Manage System Alerts

Hover over either the **GateKeeper Software Update** or **Low Battery** alert. Click [Manage](#).



Toggle the **Alert** on or off. Click **Save Profile**. Then, click the **Delivery** tab.



On the **Delivery** tab, you select **Delivery Method**, **Delivery Schedule**, alert recipient. Click **Save**.

Manage Alert: GateKeeper Software Update

Profile
Delivery

Select Delivery Methods:
☒ Email
☐ SMS
☒ Notification

Select Delivery Schedule:
☐ Immediate
☒ Daily
☐ Weekly
☐ Monthly

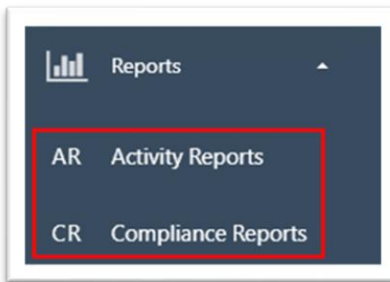
Select Alert Recipients:

<input checked="" type="checkbox"/> Hub User	Roles
<input checked="" type="checkbox"/> Siddharth Potbhare	1 roles
<input checked="" type="checkbox"/> Sai Vaddi	1 roles
<input checked="" type="checkbox"/> UMAR FAROOQ	1 roles
<input checked="" type="checkbox"/> Ummer	1 roles
<input type="checkbox"/> Hello Admin	1 roles
<input type="checkbox"/> Abe Kim	1 roles
<input type="checkbox"/> Alexander Lee	1 roles
<input type="checkbox"/> GateKeeper GateKeeper	1 roles
<input type="checkbox"/> GateKeeper Hub	1 roles

Save

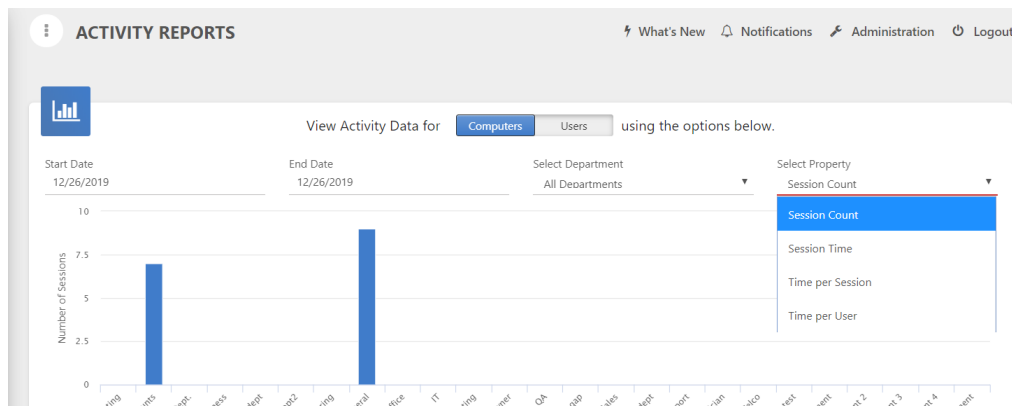
7 Reports

This page has two reports: **Activity Reports** and **Compliance Reports** pages.

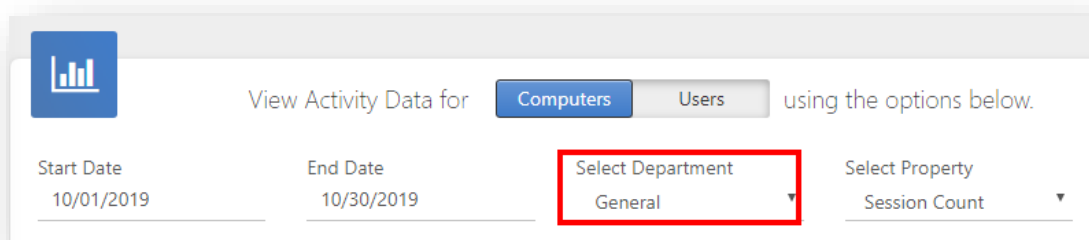


7.1.1.1 Activity Reports

This page shows records of sessions on all Client computers and **Users**. Set filters to display **Session Count**, **Session Time**, **Time per Session**, and **Time per User** for each department's computers or users.



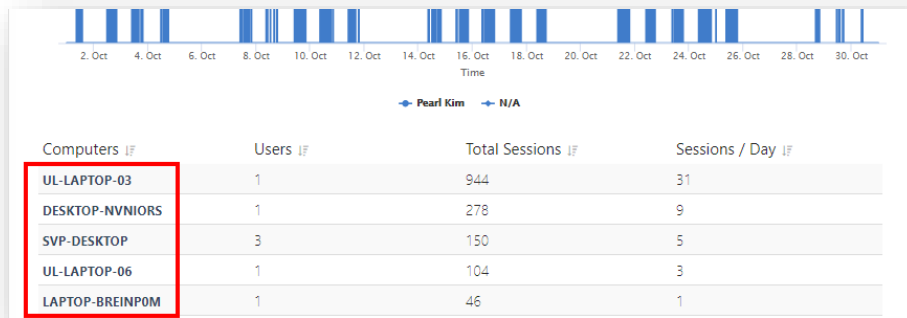
To view **Time Charts** for individual computers, select the department that the computer is in.



View Activity Data for **Computers** **Users** using the options below.

Start Date: 10/01/2019 End Date: 10/30/2019 Select Department: **General** Select Property: Session Count

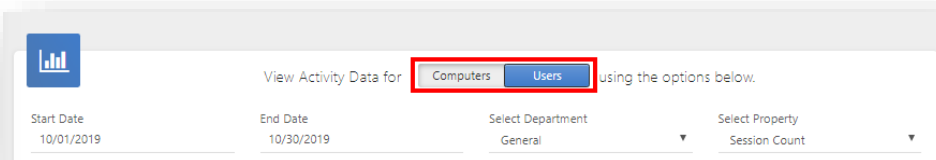
Click the computer's name.



Displays the number of active users, total sessions, and sessions per day by computer.

Computers	Users	Total Sessions	Sessions / Day
UL-LAPTOP-03	1	944	31
DESKTOP-NVNIORS	1	278	9
SVP-DESKTOP	3	150	5
UL-LAPTOP-06	1	104	3
LAPTOP-BREINPOM	1	46	1

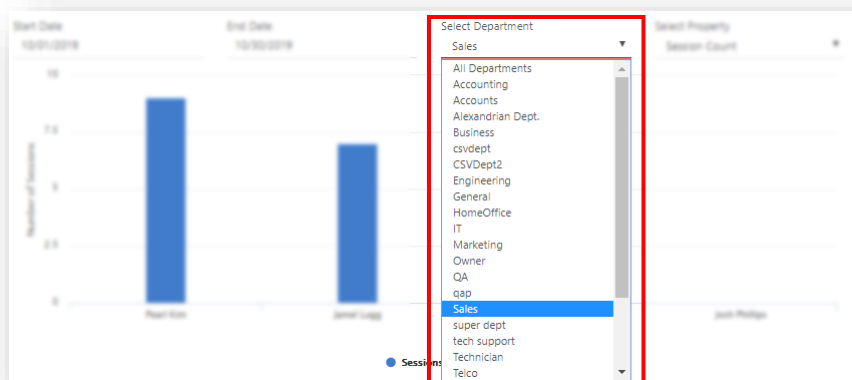
To view the session details for individual users, toggle the view mode from **Computer** to **Users**.



View Activity Data for **Computers** **Users** using the options below.

Start Date: 10/01/2019 End Date: 10/30/2019 Select Department: General Select Property: Session Count





Select the user's department.



Select Department: Sales

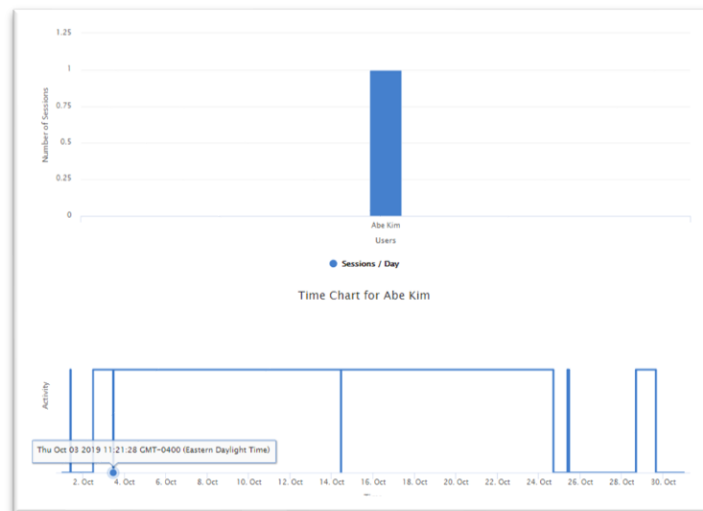
Select Property: Session Count

Scroll down and click the desired user to view their time charts.

Users 	Computers 	Total Sessions 	Sessions / Day 
Abe Kim	1	31	1

Showing 1 to 1 of 1 entries


This chart displays the session logs for all the computers the user logged into on the selected dates.



7.1.1.2 Compliance Reports

Generates reports on login time, logout time, and session duration.

COMPLIANCE REPORTS
What's New
Notifications
Administration
Logout


Generate Compliance Reports for **Computers** **Users** using the filter options below.

COMPUTERS

USERS

Start Date

End Date


☒ Email me after generation

GENERATE

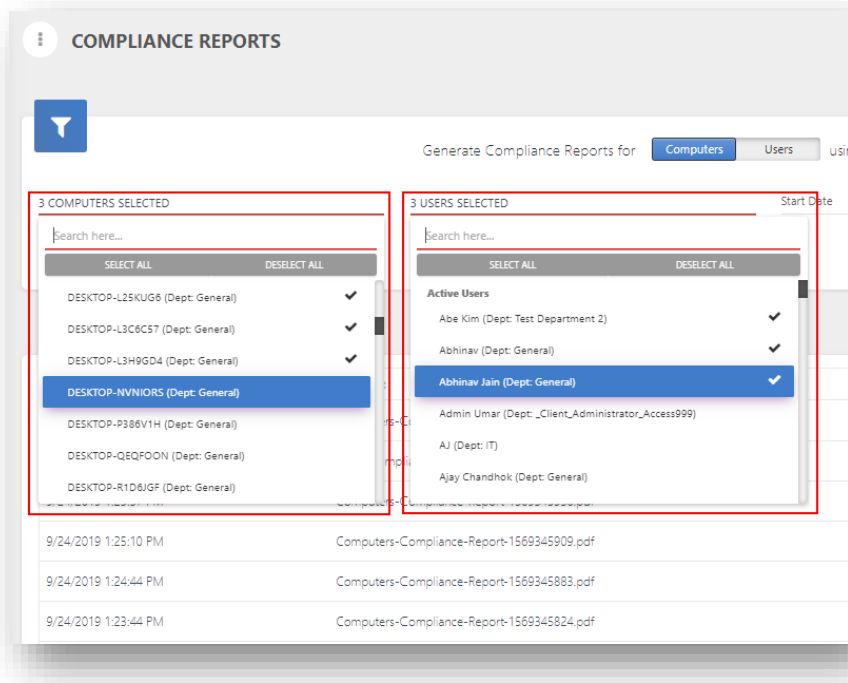
CLEAR

Date	Name	Created By	Size	Actions
12/16/2019 11:21:00 AM	Computers-Compliance-Report-1576513259.pdf	GateKeeper Hub	0.1 MB	Download Delete

Select either **Computers** or **Users** to generate a report on.


Generate Compliance Reports for **Computers** **Users** using the filter options below.

Then select the desired computers and users to include in the report.



The screenshot shows the 'COMPLIANCE REPORTS' section with tabs for 'Computers' and 'Users'. Under '3 COMPUTERS SELECTED', the following computers are listed with checkboxes:

Computer Name	Dept	Selected
DESKTOP-L25KUG6	General	<input checked="" type="checkbox"/>
DESKTOP-L3C6C57	General	<input checked="" type="checkbox"/>
DESKTOP-L3H9GD4	General	<input checked="" type="checkbox"/>
DESKTOP-NVNIORS	General	<input checked="" type="checkbox"/>
DESKTOP-P386V1H	General	<input type="checkbox"/>
DESKTOP-QEQFOON	General	<input type="checkbox"/>
DESKTOP-R1D6JGF	General	<input type="checkbox"/>

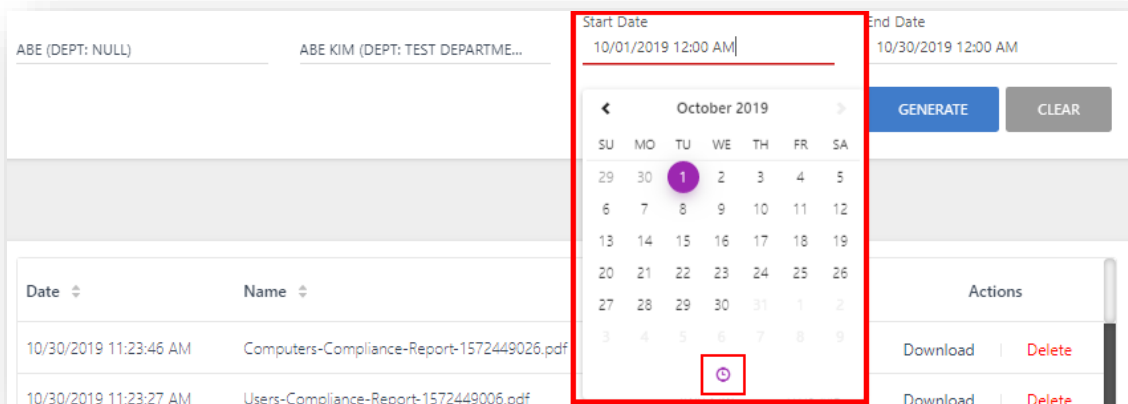
Under '3 USERS SELECTED', the following users are listed with checkboxes:

User Name	Dept	Selected
Abe Kim	Test Department 2	<input checked="" type="checkbox"/>
Abhinav	General	<input checked="" type="checkbox"/>
Abhinav Jain	General	<input checked="" type="checkbox"/>
Admin Umar	_Client_Administrator_Access999	<input type="checkbox"/>
AJ	IT	<input type="checkbox"/>
Ajay Chandhok	General	<input type="checkbox"/>

Below the selection lists, a table shows generated reports:

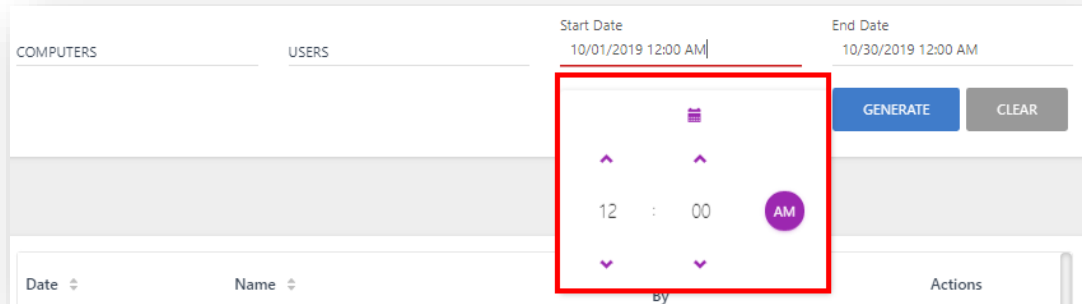
Date	Report Name
9/24/2019 1:25:10 PM	Computers-Compliance-Report-1569345909.pdf
9/24/2019 1:24:44 PM	Computers-Compliance-Report-1569345883.pdf
9/24/2019 1:23:44 PM	Computers-Compliance-Report-1569345824.pdf

Select the **Start Date** and **End Date** by clicking the **clock icon** below the calendar.

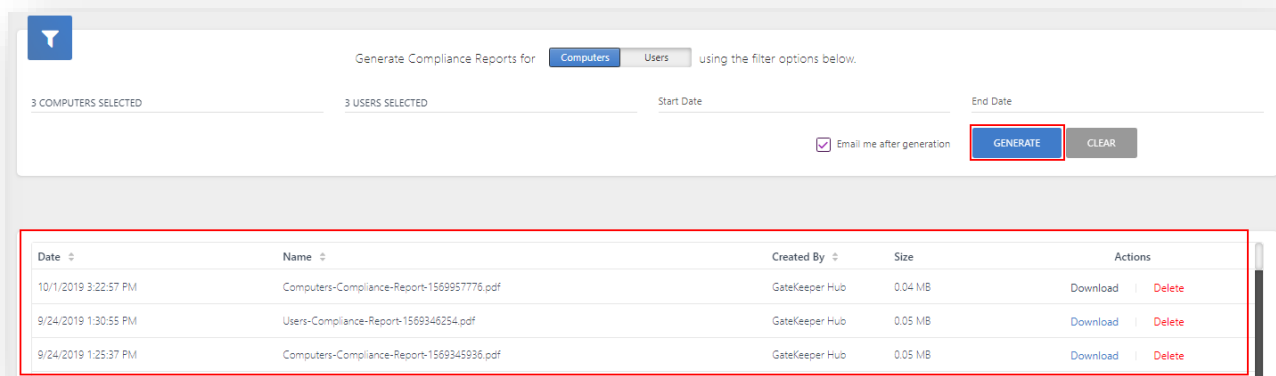


The screenshot shows the 'Start Date' and 'End Date' fields. The 'Start Date' is set to '10/01/2019 12:00 AM' and the 'End Date' is set to '10/30/2019 12:00 AM'. A calendar for October 2019 is displayed, with the 1st highlighted. Below the calendar, a table shows generated reports:

Date	Name	Actions
10/30/2019 11:23:46 AM	Computers-Compliance-Report-1572449026.pdf	Download Delete
10/30/2019 11:23:27 AM	Users-Compliance-Report-1572449006.pdf	Download Delete



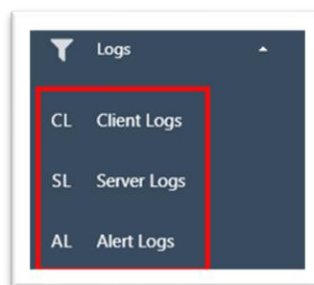
Click **Generate**.



Date	Name	Created By	Size	Actions
10/1/2019 3:22:57 PM	Computers-Compliance-Report-1569957776.pdf	GateKeeper Hub	0.04 MB	Download Delete
9/24/2019 1:30:55 PM	Users-Compliance-Report-1569346254.pdf	GateKeeper Hub	0.05 MB	Download Delete
9/24/2019 1:25:37 PM	Computers-Compliance-Report-1569345936.pdf	GateKeeper Hub	0.05 MB	Download Delete

8 Logs

There are three different types of logs under the **Logs** tab for GateKeeper.



Client Logs

This page maintains user activity on the GateKeeper Client computers.

CLIENT LOGS

⚡ What's New

🔔 Notifications

🔧 Administration

👤 Logout

▶ About this page

📘 Info

COMPUTERS

INCLUDE USERS

EXCLUDE USERS

EVENTS

START DATE

END DATE

100 Records

SEARCH

CLEAR

Export to a CSV file

Date	Computer	User	Domain	Token	Event
12/26/2019 4:50:13 PM	DESKTOP-C3PEVEC	--	--	--	Remote Connect
12/26/2019 4:46:37 PM	SVP-LAPTOP-02	Siddharth Potbhare	cc.local	299E1WJ3Q8CGN	User Connected
12/26/2019 4:46:11 PM	SVP-LAPTOP-02	--	--	--	GateKeeper Service Started
12/26/2019 4:37:53 PM	UL-LAPTOP-06	Sai Vaddi	cc.local	GK17-11525	Session Unlocked
12/26/2019 4:37:53 PM	UL-LAPTOP-06	Sai Vaddi	cc.local	GK17-11525	GateKeeper Unlock

Server Logs

This page maintains records of all activities and setting changes on the Hub server. Useful for audit purposes and investigating incidents.

SERVER LOGS				
About this page Info				
INCLUDE USERS	EXCLUDE USERS	ACTIONS		
START DATE	END DATE	100 Records	SEARCH	CLEAR
Export to a CSV file				
Date	Server User	Role	Action	Description
12/26/2019 5:02:23 PM	GateKeeper Hub	Limited-User	Logged In	Logged in with username gkeeper
12/26/2019 4:44:56 PM	GateKeeper Hub	Limited-User	Updated	Group: Sai settings were updated
12/26/2019 4:41:26 PM	GateKeeper Hub	Limited-User	Logged In	Logged in with username gkeeper
12/26/2019 4:20:52 PM	GateKeeper Hub	Limited-User	Logged In	Logged in with username gkeeper

Alert Logs

Displays the delivery status of messages pertaining to GateKeeper events, whether these messages have been **“Delivered”** or **“Not Delivered.”**

ALERT LOGS

[What's New](#)
[Notifications](#)
[Administration](#)
[Logout](#)

[About this page](#)
[Info](#)

ALERTS

COMPUTERS

INCLUDE USERS

EXCLUDE USERS

EVENTS

START DATE

END DATE

100 Records

SEARCH

CLEAR

Export to a CSV file

Date	Alert	Computer	User	Event	Delivery Status
12/26/2019 2:45:17 PM	JamelComputerUnlock	DESKTOP-56MSF8M	Jamel Lugg	GateKeeper Unlock	Not Delivered
12/26/2019 2:37:16 PM	JamelComputerUnlock	DESKTOP-56MSF8M	Jamel Lugg	GateKeeper Unlock	Not Delivered
12/26/2019 2:14:28 PM	Alex Alert	UL-LAPTOP-03	Alex Lee	User Disconnected	Delivered
12/26/2019 2:14:28 PM	Alex Alert	UL-LAPTOP-03	Alex Lee	GateKeeper Lock	Delivered
12/26/2019 2:08:28 PM	JamelComputerUnlock	DESKTOP-56MSF8M	Jamel Lugg	GateKeeper Unlock	Not Delivered

9 Scans

The **Scans** page maintains records about how far/near a GateKeeper token was to a client computer, displays the username associated with the token, and the time when it sensed the token.

Each GateKeeper USB proximity sensor (receiver) scans for GateKeeper tokens present around it and reports its findings. The records can be filtered based on computer name, users, range, and dates.

This is an excellent tool for security and incident investigations.

SCANS

[What's New](#)
[Notifications](#)
[Administration](#)
[Logout](#)

[About this page](#)
[Info](#)

COMPUTERS

INCLUDE USERS

EXCLUDE USERS

ALL RANGES

Start Date

End Date

100 Records

SEARCH

CLEAR

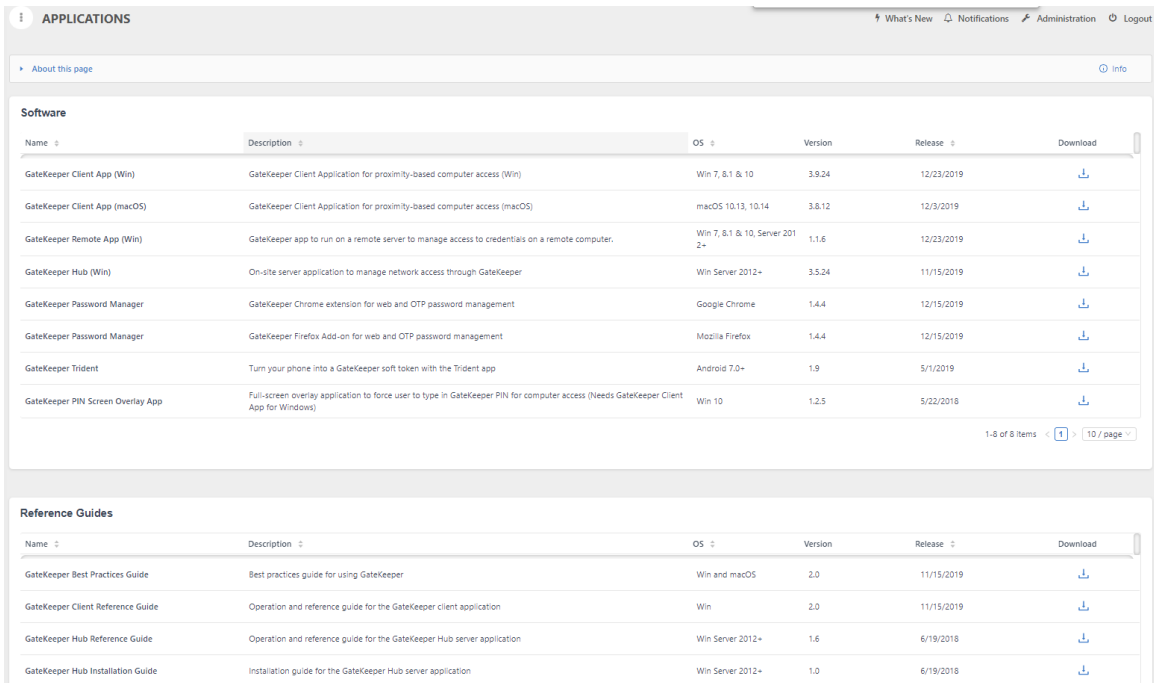
Export to a CSV file

Date	Computer	User	Decision
12/26/2019 5:13:54 PM	SVP-DESKTOP	Pearl Kim	Far
12/26/2019 5:13:34 PM	SVP-DESKTOP	Pearl Kim	Near
12/26/2019 5:12:38 PM	SVP-DESKTOP	Pearl Kim	Far
12/26/2019 5:12:00 PM	SVP-DESKTOP	Michael Ford	Near

10 Applications

This page contains the links to download all the latest GateKeeper applications. Check the version number of the current application installed on your system and if it's not the latest one, under the **Download** category click the download icon to update it.

GateKeeper also has scripts for easy, silent install to all the Client computers to ensure no downtime.



The screenshot shows the 'APPLICATIONS' section of the GateKeeper Hub interface. It features a table of software applications and a section for reference guides.

Name	Description	OS	Version	Release	Download
GateKeeper Client App (Win)	GateKeeper Client Application for proximity-based computer access (Win)	Win 7, 8.1 & 10	3.9.24	12/23/2019	Download
GateKeeper Client App (macOS)	GateKeeper Client Application for proximity-based computer access (macOS)	macOS 10.13, 10.14	3.8.12	12/3/2019	Download
GateKeeper Remote App (Win)	GateKeeper app to run on a remote server to manage access to credentials on a remote computer.	Win 7, 8.1 & 10, Server 2012+	1.1.6	12/23/2019	Download
GateKeeper Hub (Win)	On-site server application to manage network access through GateKeeper	Win Server 2012+	3.5.24	11/15/2019	Download
GateKeeper Password Manager	GateKeeper Chrome extension for web and OTP password management	Google Chrome	1.4.4	12/15/2019	Download
GateKeeper Password Manager	GateKeeper Firefox Add-on for web and OTP password management	Mozilla Firefox	1.4.4	12/15/2019	Download
GateKeeper Trident	Turn your phone into a GateKeeper soft token with the Trident app	Android 7.0+	1.9	5/1/2019	Download
GateKeeper PIN Screen Overlay App	Full-screen overlay application to force user to type in GateKeeper PIN for computer access (Needs GateKeeper Client App for Windows)	Win 10	1.2.5	5/22/2018	Download

1-8 of 8 items | 10 / page

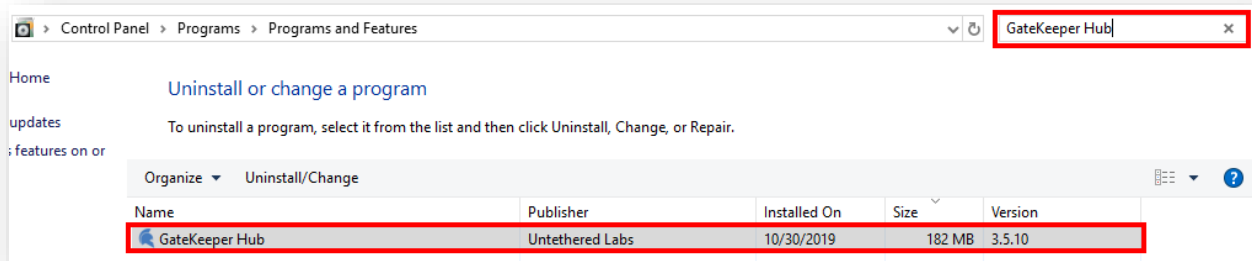
Name	Description	OS	Version	Release	Download
GateKeeper Best Practices Guide	Best practices guide for using GateKeeper	Win and macOS	2.0	11/15/2019	Download
GateKeeper Client Reference Guide	Operation and reference guide for the GateKeeper client application	Win	2.0	11/15/2019	Download
GateKeeper Hub Reference Guide	Operation and reference guide for the GateKeeper Hub server application	Win Server 2012+	1.6	6/19/2018	Download
GateKeeper Hub Installation Guide	Installation guide for the GateKeeper Hub server application	Win Server 2012+	1.0	6/19/2018	Download

11 Frequently Asked Questions (FAQs)

11.1 Server setup

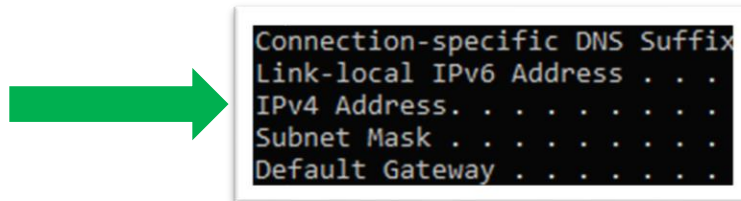
How can I check if the GateKeeper soft server is installed on my local machine?

Open Control Panel > Programs > Programs and Features, search for **GateKeeper Hub**.



How can I obtain the IP address of the computer with the GateKeeper server installed?

Log in to the computer where the GateKeeper server is installed and open the **Command Prompt** from the **Start Menu**, type '**ipconfig**' and hit Enter. The computer's IP address is the one corresponding to the **IPv4 Address**.



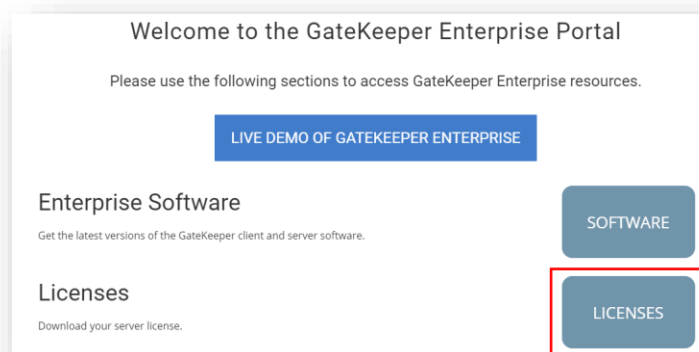
11.2 Account Management

Why do I need a license?



The GateKeeper Enterprise license is used to activate the server dashboard which allows you to manage permissions to access computers on the network and enforce global settings on all the Client computers connected to the GateKeeper server. Each end user requires 1 user license.


Where can I find my licenses?


After purchase, log in to your online GateKeeper account on the [Customer Portal](#). Click **Licenses**.



You will be directed to the **License Files for GateKeeper Hub Server Application**.


License Files for GateKeeper Hub Server Application					
Download your license file(s) from the links below. The license file needs to be uploaded into the server application to enable full functionality.					
Assigned To	Nodes	Type	Valid From	Valid To	Download
Abraham Kim	5	N/A	2017-05-17	2017-05-31	
Abe Kim - QA	15	N/A	2019-08-29	2019-12-31	

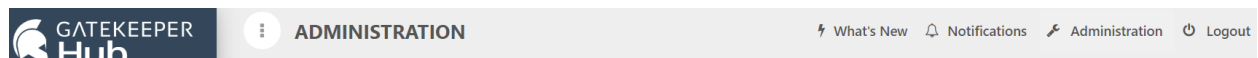
Click the  icon under **Download**.

Abraham Kim	5	N/A	2017-05-17	2017-05-31	
-------------	---	-----	------------	------------	---

How do I upload a license?

Make sure to have your server license purchased and [downloaded](#).

Open the Hub in your browser. Click Administration (the  icon) on the top right of the screen.



On the **Administration** page, click **Hub Administration**. This will expand and show more fields.



Scroll down to the **Licenses** field.

GATEKEEPER Hub									
Licenses									
Valid From	Valid Until	Us er	Assigned To	Email	Phone	Days Left	Statu s	Off-site Access	Actions
12/03/2019	12/03/2119	50	Sai Sandeep Vaddi	saisandeepvaddi@gmail.com	6824722966	36,513	Inactive	✖	
12/05/2019	12/05/2020	58	Sai Sandeep Vaddi	saisandeepvaddi@gmail.com	6824722966	357	Inactive	✖	
12/03/2019	12/03/2020	5	Sai Sandeep Vaddi	saisandeepvaddi@gmail.com	6824722966	355	Active	✖	

Click **BROWSE**, find the license file downloaded from the [GateKeeper Customer Portal](#) after purchase.

Licenses

Valid Until	Users	Name	Email	Phone	Days Left	Status	Off-site Access	Actions
12/30/2019 7:00:00 PM	400	ULabs/Main/MSPTest	sid@ulabs.io		61	Active	✓	
10/30/2019 8:00:00 PM	10	Sai Test 22Oct2	sai@gkaccess.com		Expired	Active	✓	

Click Browse to select new License file

[BROWSE](#) [UPLOAD](#)

Select the license and click **UPLOAD** to finish updating your license.

Licenses

Valid Until	Users	Name	Email	Phone	Days Left	Status	Off-site Access	Actions
12/30/2019 7:00:00 PM	400	ULabs/Main/MSPTest	sid@ulabs.io		61	Active	✓	
10/30/2019 8:00:00 PM	10	Sai Test 22Oct2	sai@gkaccess.com		Expired	Active	✓	

Click Browse to select new License file

[BROWSE](#) [UPLOAD](#)

How can I grant another user permission to access the dashboard?
On the **Users** page, click “Add Users”.

GATEKEEPER Hub **USERS**

[Add Users](#)

Name	Department	Tokens	Credentials	Actions
<input type="checkbox"/> Abe Kim	Test Department 2	1	15	
<input type="checkbox"/> Abhinav	General	1	1	
<input type="checkbox"/> Abhinav Jain	General	1	1	

Fill in the profile details (**Tokens** and **Credentials** are optional).

Add Users

Profile Tokens Credentials Summary

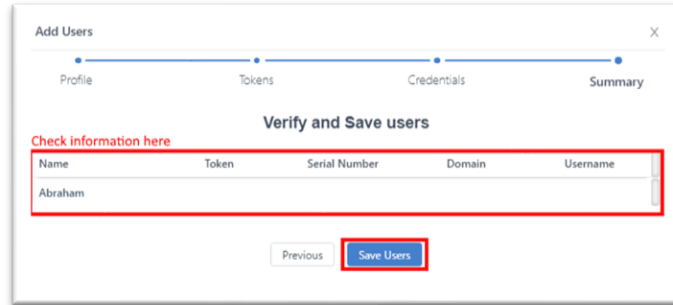
[Add from Active Directory](#) [Add from file](#)

Name	Email	Phone Number	Department	Actions
<input type="text" value="Name"/>	<input type="text" value="Email"/>	<input type="text" value="Phone Number"/>	<input type="text" value="General"/>	Remove

[+ Add Row](#)

[Next](#)

Click **Save Users**.



Add Users [X]

Profile Tokens Credentials Summary

Verify and Save users

Check information here

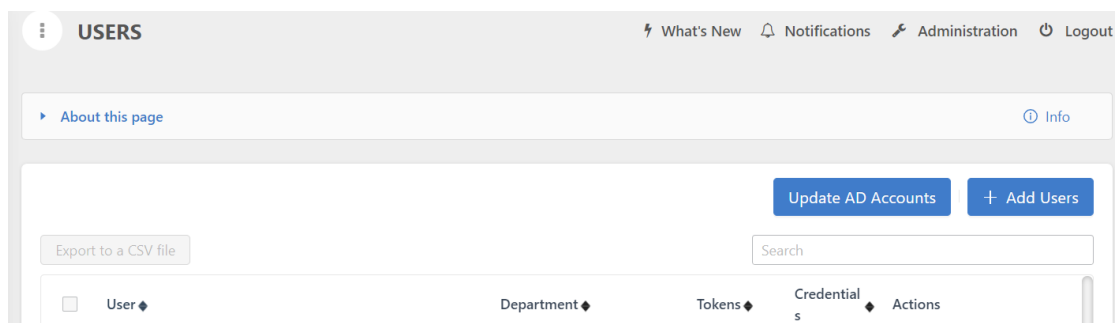
Name	Token	Serial Number	Domain	Username
Abraham				

Previous **Save Users**

11.3 User Management

What to do if a user loses their GateKeeper token?

In case a user loses their token, search for their name on the **Users** page using the search filter.



USERS [What's New] [Notifications] [Administration] [Logout]

About this page [Info]

Export to a CSV file [Search]

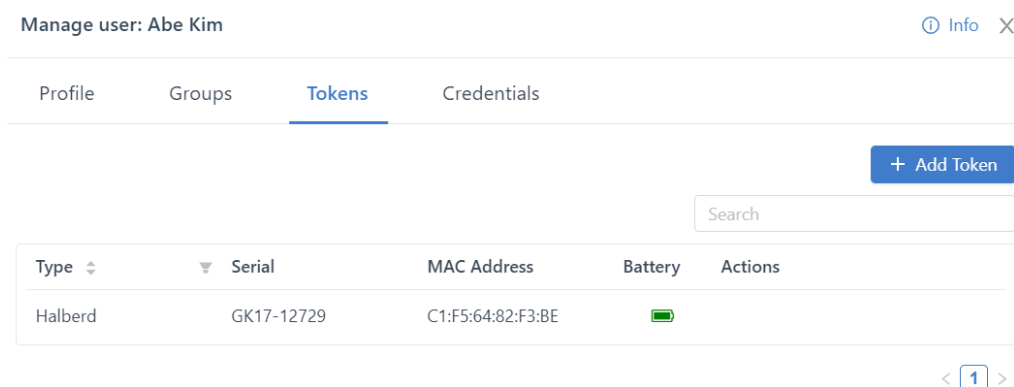
[Update AD Accounts] [+ Add Users]

Name	Department	Tokens	Credentials	Actions
Abe Kim	Test Department 2	1	15	Manage Delete

Under the **Actions** column, click [Manage](#). The “Manage user: [User’s name]” side panel will appear.

Name	Department	Tokens	Credentials	Actions
Abe Kim	Test Department 2	1	15	Manage Delete

Click the **Tokens** Tab.




Manage user: Abe Kim [Info] [X]

Profile Groups **Tokens** Credentials


[+ Add Token]

[Search]

Type	Serial	MAC Address	Battery	Actions
Halberd	GK17-12729	C1:F5:64:82:F3:BE		Delete

< **1** >

Under the **Actions** column, click [Delete](#). This will remove their token from their account.

Type ▾	Serial ▾	Mac Address	Battery	Actions
Halberd	GK17-12729	C1:F5:64:82:F3:BE		Edit Delete

Add a new token to the user's account from the desktop application or the server dashboard.

What if a user comes in to work without their GateKeeper token?

Users can always log in using their Windows or Mac username and password as the GateKeeper does not mask the Windows or Mac method of logging in. But, to ensure best practices, a new GateKeeper token must be added to the user's account. When the user brings back their original token, delete the backup token from their account.

11.4 Logs

What happens to the logs if a computer is not connected to the server?

The computers also keep track of logs locally. When they connect back to the GateKeeper Hub, the logs are synchronized with the server logs. No records are missed if the computer is connected back to the server within two days.

12 About

Untethered Labs, Inc.

www.gkaccess.com

5000 College Avenue, College Park, MD 20742 USA

Email: support@gkaccess.com

Phone: 240-547-5446