Lenovo

ThinkShield

ThinkShield Key Vault Portal Web Application User Guide

December 2019

Table of Contents

Table of Contents 2
ThinkShield Key Vault Portal Overview 4
Roles vs Capabilities 5
Role Descriptions 6
- Has a Lenovo ID 6
- Base User 6
- Edge User 6
- Maintenance User 6
- Org Admin 6

Capabilities 7
- First Launch 8
- Claiming a Device 11
- Unclaiming a Device 17
- Transfer 19
  - Send 19
  - Receive 21
  - Cancel all Transfers 22
- Export Devices 24
- Import Devices 25
- Automatic Activation 27
- Manual Activation 29
- Re-sync 35
- Create a Group 36
- Group Devices 38
- Remove Devices from Group 40
- Delete a Group 41
- Create an Organization 43
  - Lenovo ID Authentication 44
  - Active Directory Authentication 47
- Edit My Profile 50
- Logout 52

Edit Device Name 53
Update Device Key 55
Invite a User 57
Remove a User 59
Import Users 62
Export Users 67
Bulk Invite Users 69
Help/ Contact Support 73

ThinkShield Key Vault Portal Overview

Lenovo ThinkSystem SE350 Edge server (hereinafter Device) is supplied to customers in locked state for security reasons.
One-time code (Secure Activation Code) is generated and shipped to the customer admin separately from the Device. This code will be used for secure device claiming within the ThinkShield Key Vault Portal (hereinafter Portal).

The Device can be unlocked in three different ways:

1. Automatically
2. Manually
3. Via the Mobile App – *Action is done NOT on Portal side.*

The web application is available **worldwide**.

Supported languages:

- English
- Simplified Chinese
- Traditional Chinese
- French
- German
- Italian
- Spanish

Lenovo

Roles vs Capabilities

Roles → / Function ⋁	Has a Lenovo ID	Base User	Edge User	Maintenance User	Org Admin
Can Login to ThinkShield Key Vault Portal		x	x	x	x
Edit My Profile		x	x	x	x
Logout		x	x	x	x
Access to an Organization		x	x	x	x
Create an Organization	x				
Devices Tab			**x**	**x**	**x**
Claiming a Device			x	x	x
Unclaiming a Device			x	x	x
Automatic Activation			x	x	x
Manual Activation			x	x	x
Re-sync			x	x	x
Edit Device Name			x	x	x
Update Device Key				x	
Transfer					x
Import / Export Devices					x
Bulk Claim				x	x
Users Tab					**x**
Invite a User					x
Remove a User					x
Import / Export Users					x
Bulk Invite Users					x
Groups Tab				**x**	**x**
Create a Group				x	x
Delete a Group				x	x
Group Devices / Remove Devices from Group				x	x

Role Descriptions

Has a Lenovo ID

This user has a Lenovo ID account but does not have role permissions to any portal organizations.

Base User

This user can login to organizations but has no access to any capabilities. This user can also login to the ThinkShield Edge Mobile Management Application within the same organizations. This user is primarily used to onboard users from an external authentication service (e.g. Active Directory Federated Services, ADFS).

Edge User

This user can login to organizations. This user can also login to the ThinkShield Edge Mobile Management Application within the same organizations. This user is primarily used to give permissions to users who will activate the SE350 which physical presence to the device (at the “edge”). This user does not have the ability to conduct user or grouping functions.

Maintenance User

This user can login to organizations. This user can also login to the ThinkShield Edge Mobile Management Application within the same organizations. This user is primarily used to for maintenance users who will perform device actions (e.g. claim and activate) as well as device grouping. This user role is the only role who can update the device key in the event of motherboard failure which requires device key exchange.

Org Admin

This user can login to organizations. This user can also login to the ThinkShield Edge Mobile Management Application within the same organizations. This user has top level permissions within an organization. However, this user role cannot update the device key in the event of motherboard failure which requires device key exchange.

Capabilities

The following features are available based on Role vs Capabilities:

1. Claim Device (add a Device to the Organization)
2. Unclaim Device (remove a Device from the Organization)
3. Transfer (send a Device to other Organization)
4. Import Devices
5. Export Devices
6. Automatic activation
7. Manual activation
8. Re-sync
9. Create a Group
10. Group Devices
11. Remove Devices from Group
12. Delete a Group
13. Create an Organization
14. Edit My Profile
15. Logout
16. Edit Device Name
17. Update Device Key
18. Invite a User
19. Remove a User
20. Import Users
21. Export Users
22. Bulk Invite Users
23. Help/Contact Support

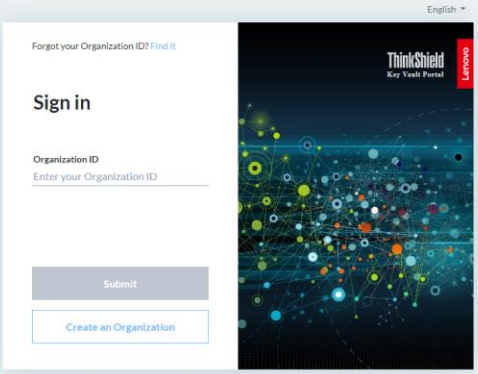
First Launch

Visit https://portal.thinkshield.lenovo.com as the starting location to:

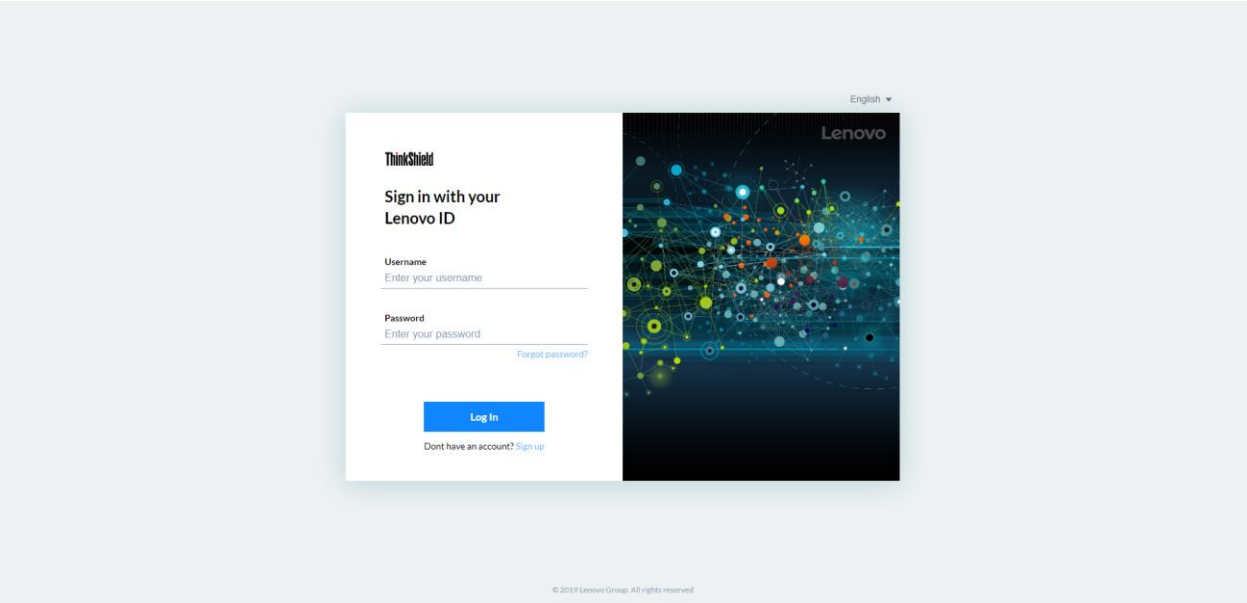
1) Login to an organization
2) Create new organizations
3) Find your organization ID

When logging into an organization, an organization ID is required. The organization ID is what uniquely identifies your organizations from other organizations. At anytime users can utilize the “Forgot your Organization ID? Find it” for their relevant information.

Note: You can also change language on this page.

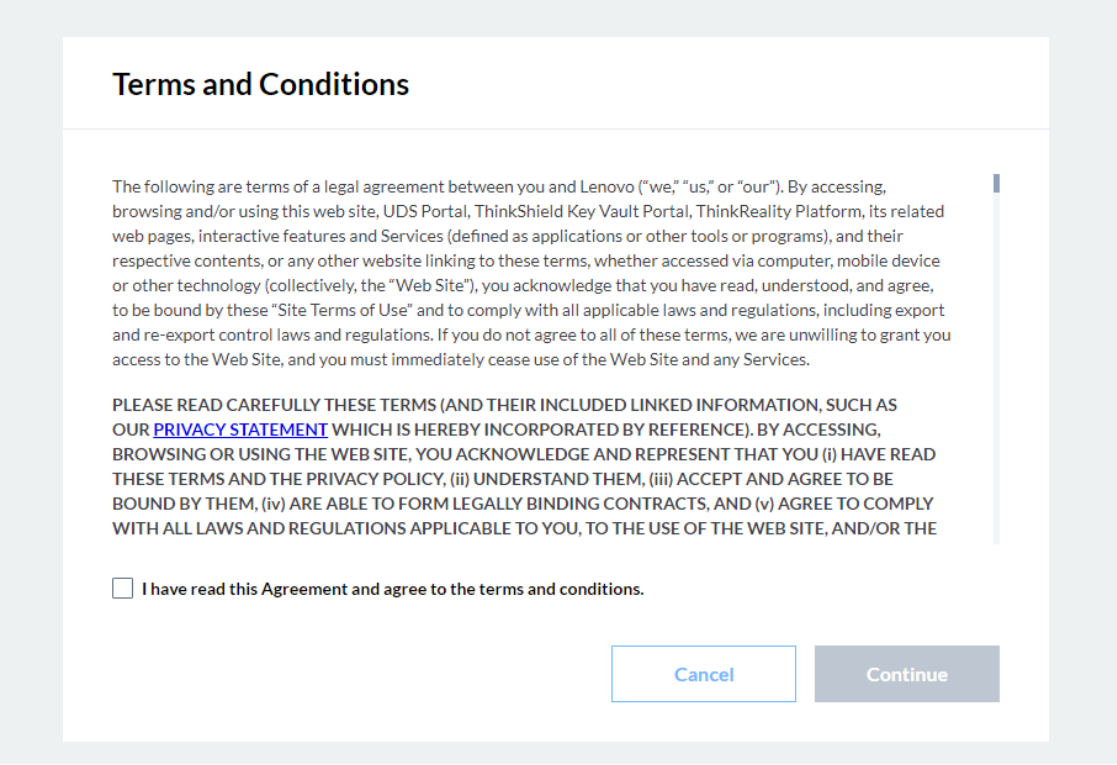


Log in using your Lenovo ID and password in ‘Username’ and ‘Password’ fields and click ‘Log In’ button. If you don’t have Lenovo ID click ‘Sign up’ next to ‘Don’t have an account’ and follow the instructions to create Lenovo account.

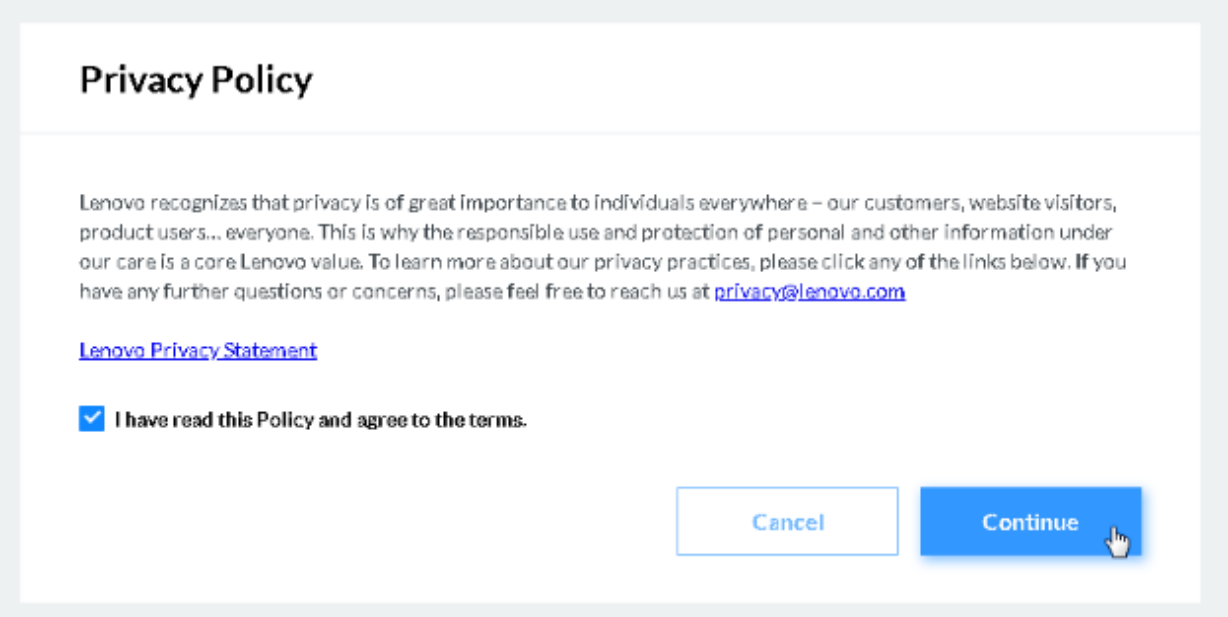


In order to use web application, you need to accept Terms and Conditions. Read and click ‘Continue’ button.

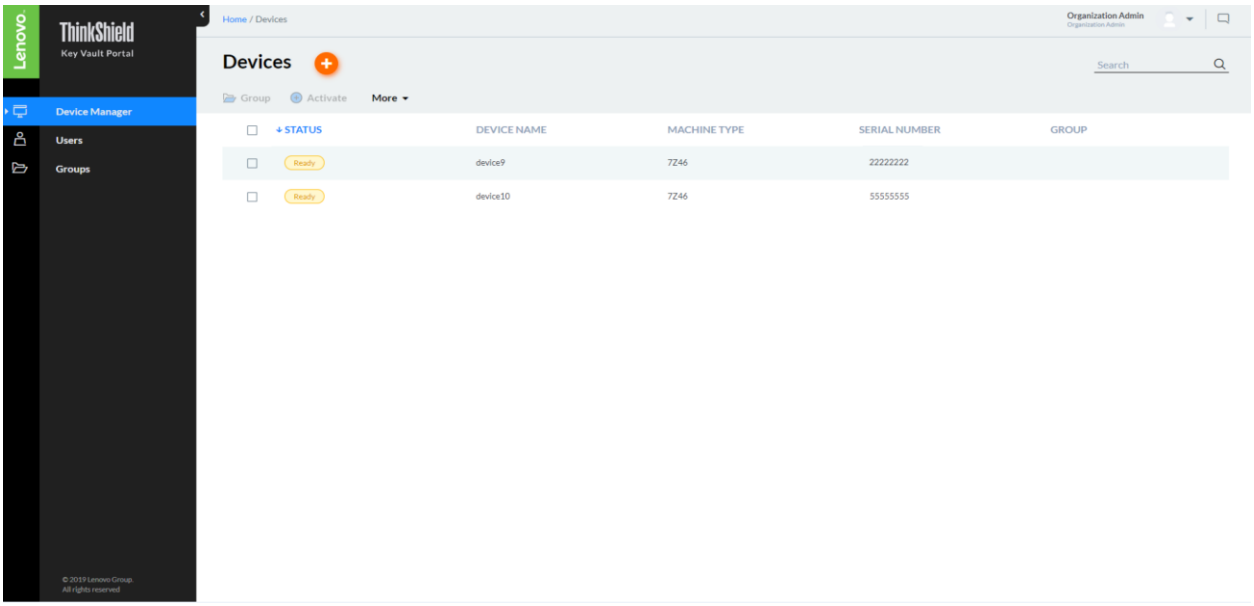
Note: Terms and Conditions are displayed only after user logs into the Portal for the first time.



In order to use web application, you need to accept Privacy Policy. Read and click ‘Continue’ button.
Note: Privacy Policy is displayed only after user logs into the Portal for the first time.

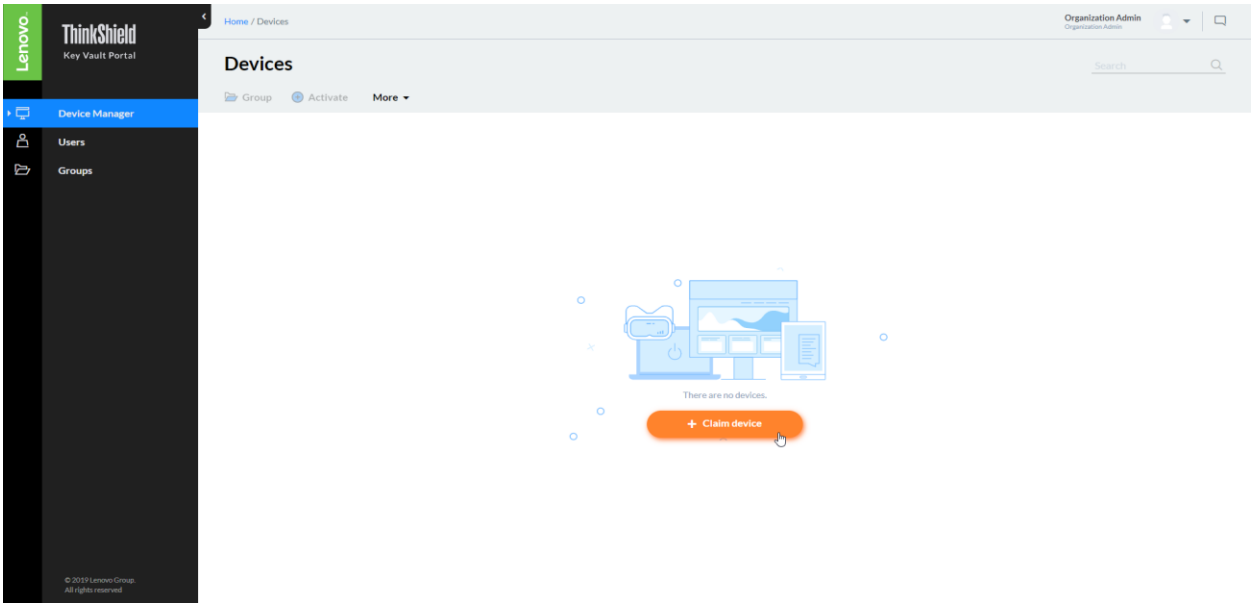


User is redirected to ‘Devices’ page after successful login.

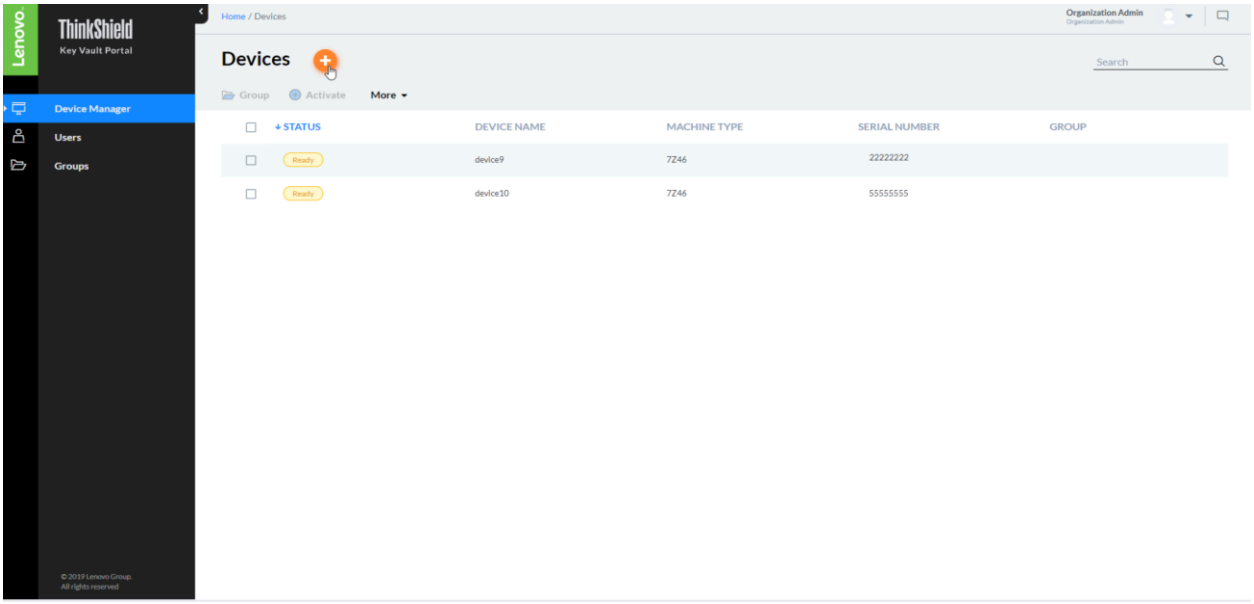


Claiming a Device

If there are no Devices in the Organization, click ‘Claim device’ in order to claim a Device.



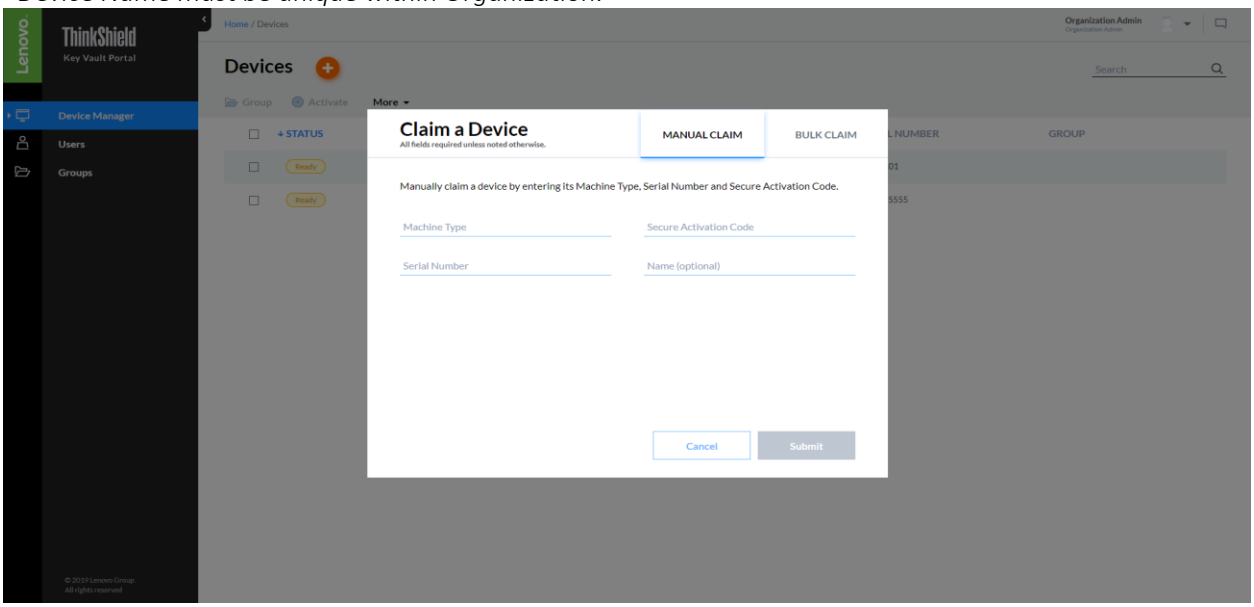
If there are any Devices in the Organization, click ‘+’ icon at the top of the page in order to claim a Device.



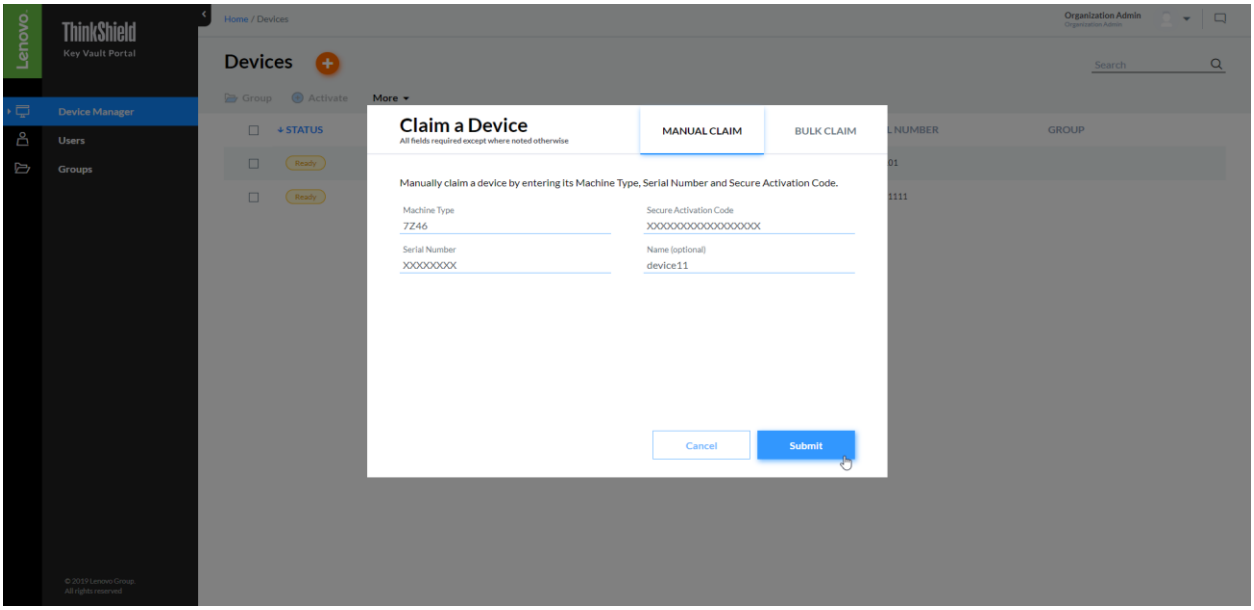
'Manual Claim' allows to claim one Device at a time. To claim a Device provide Machine Type, Serial Number and Activation Code, all these fields are required.
'Name*' field is optional, if you do not provide it, the system will generate a unique Device name.

Note: There are two Activations Codes that can be used to claim a Device. The first Activation Code is provided with the Activation Flyer (Secure Activation Guide). Another Activation Code can be read from a Device (for example, using Mobile App). Both codes are valid and can be used for Device claiming.

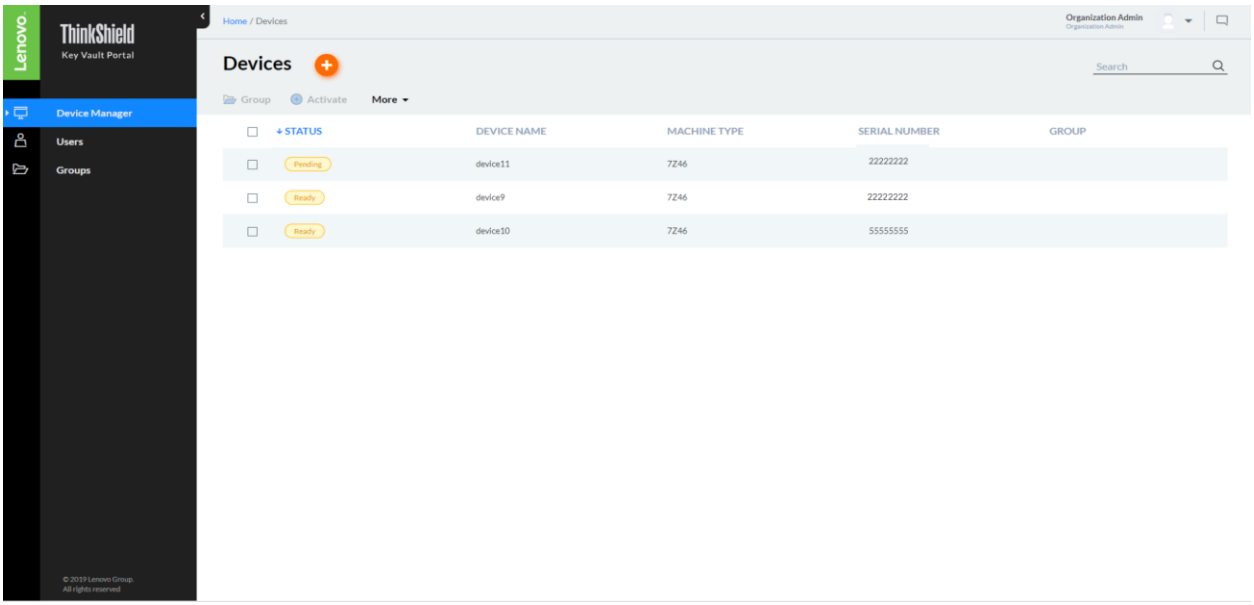
**Device Name must be unique within Organization.*



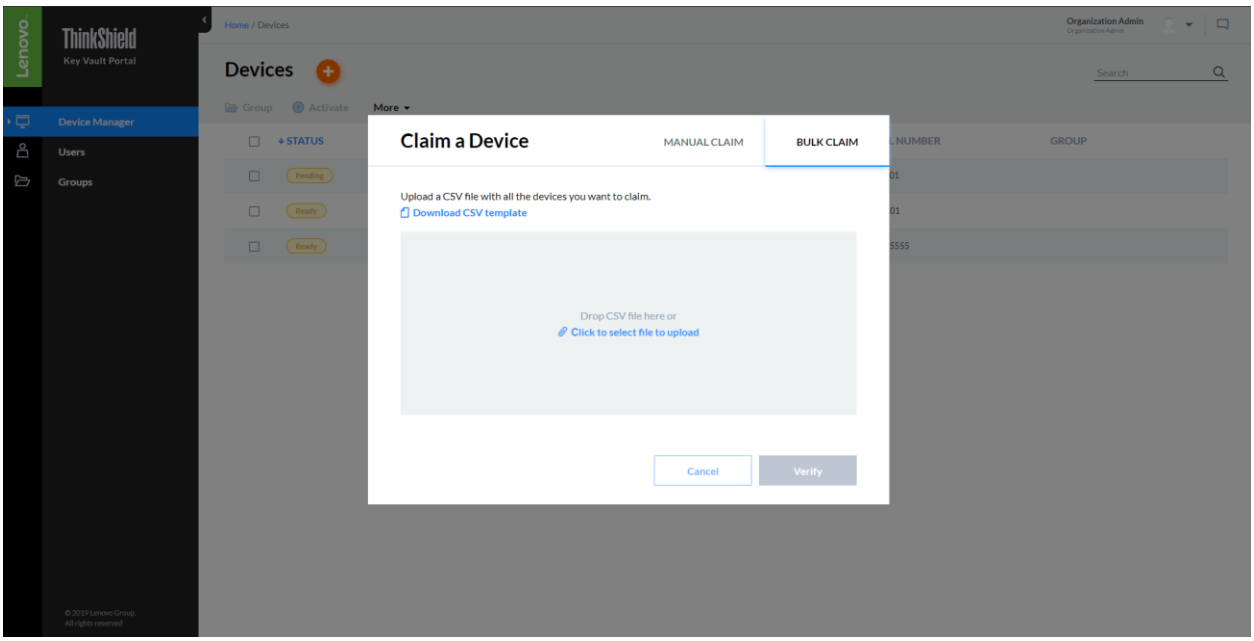
Click 'Claim' when all the data is provided.



The Device starts displaying in the Devices list. The status of the Device is Pending.

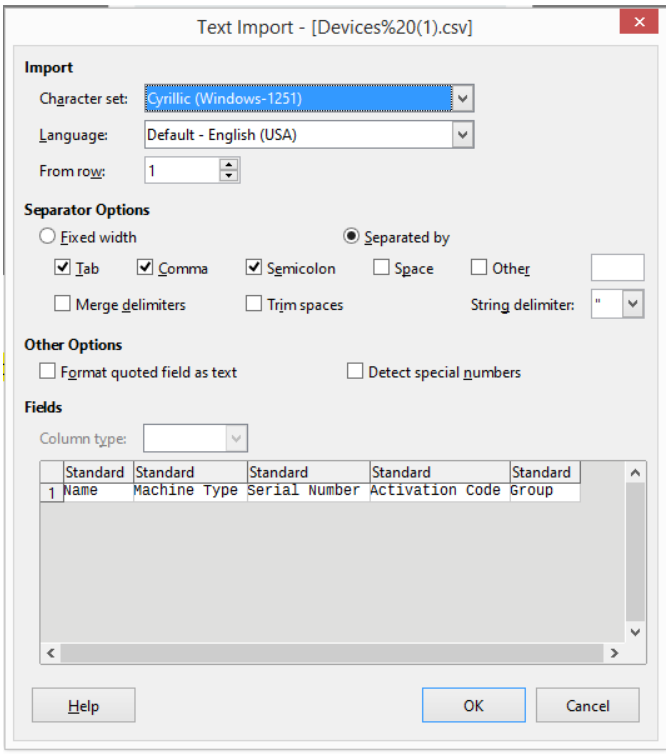


'Bulk Claim' allows to claim up to 1000 Devices at a time.



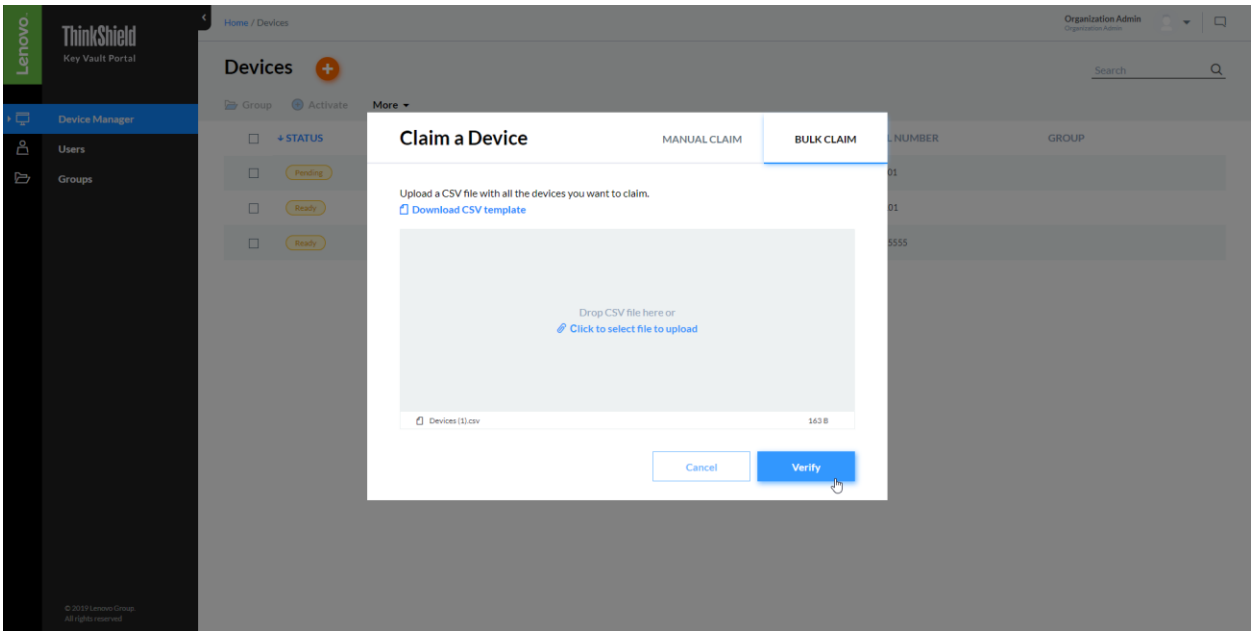
Download CSV template and fill in all the required data. The required fields are: Machine Type, Serial Number and Activation Code. All other fields are optional.

'Name' field will be generated by the system if you do not provide it.

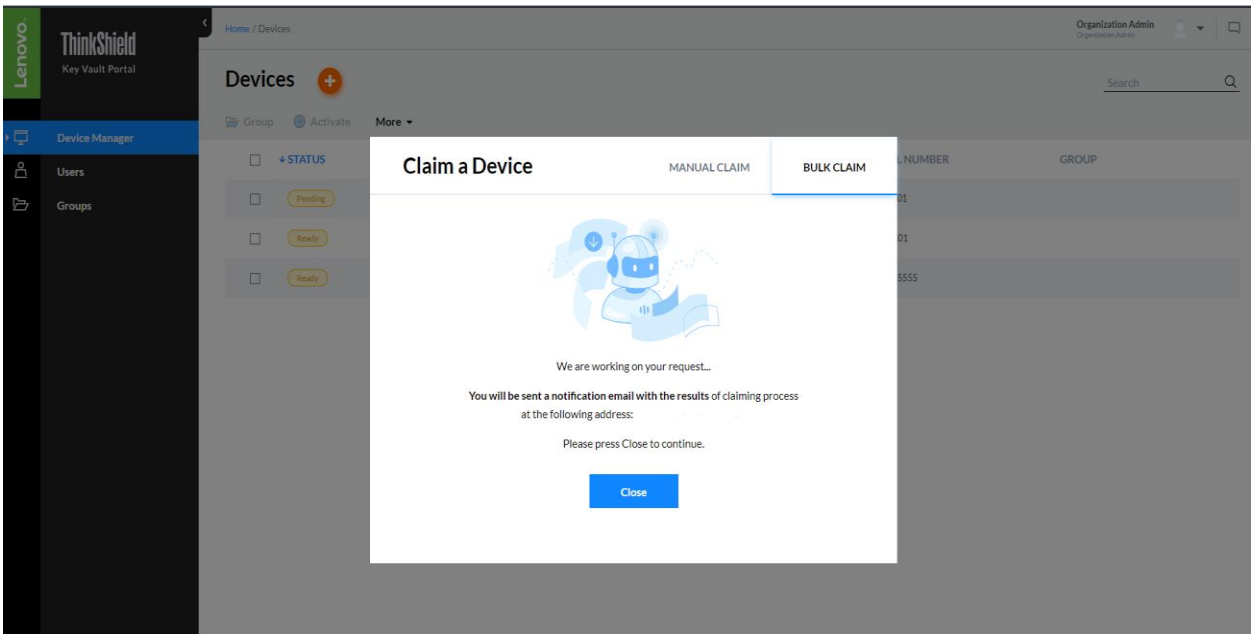


	A	B	C	D	E
1	Name	Machine Type	Serial Number	Activation Code	Group
2		7Z46	11111111	XXXXXXXXXXXXXXX	
3		7Z46	22222222	XXXXXXXXXXXXXXX	
4		7Z46	33333333	XXXXXXXXXXXXXXX	
5					
6					

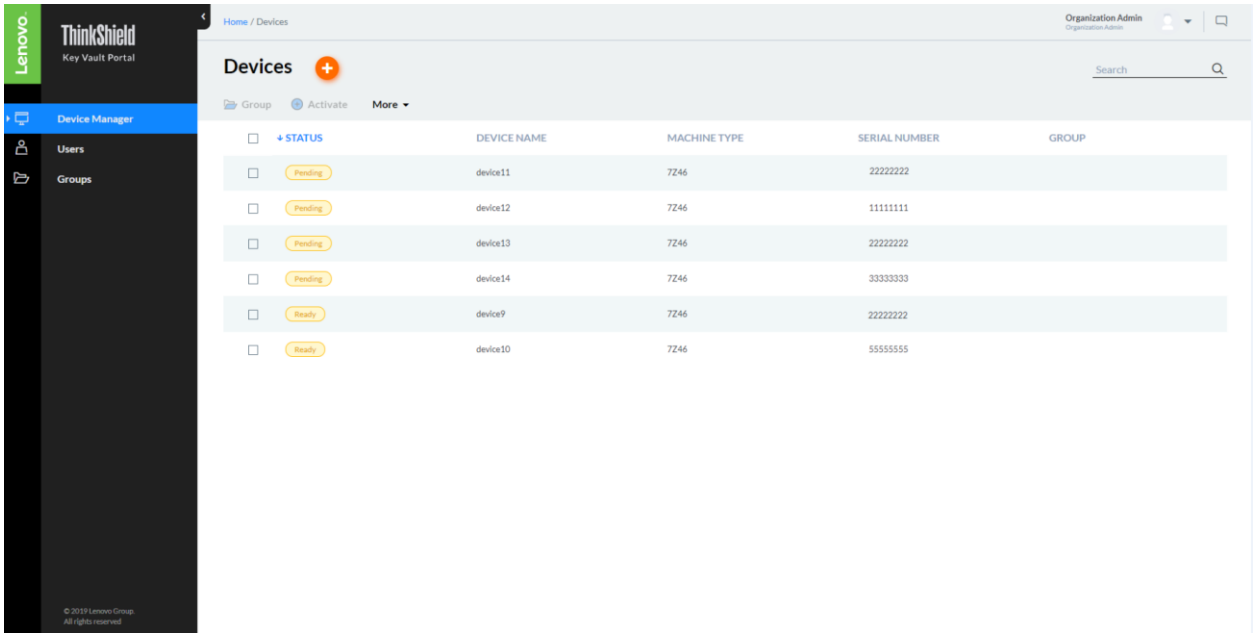
Upload a CSV file to the Portal. Click ‘Verify‘ after the file has been uploaded.



As soon as the verification process is over you will get a confirmation email to the email address associated with your profile.

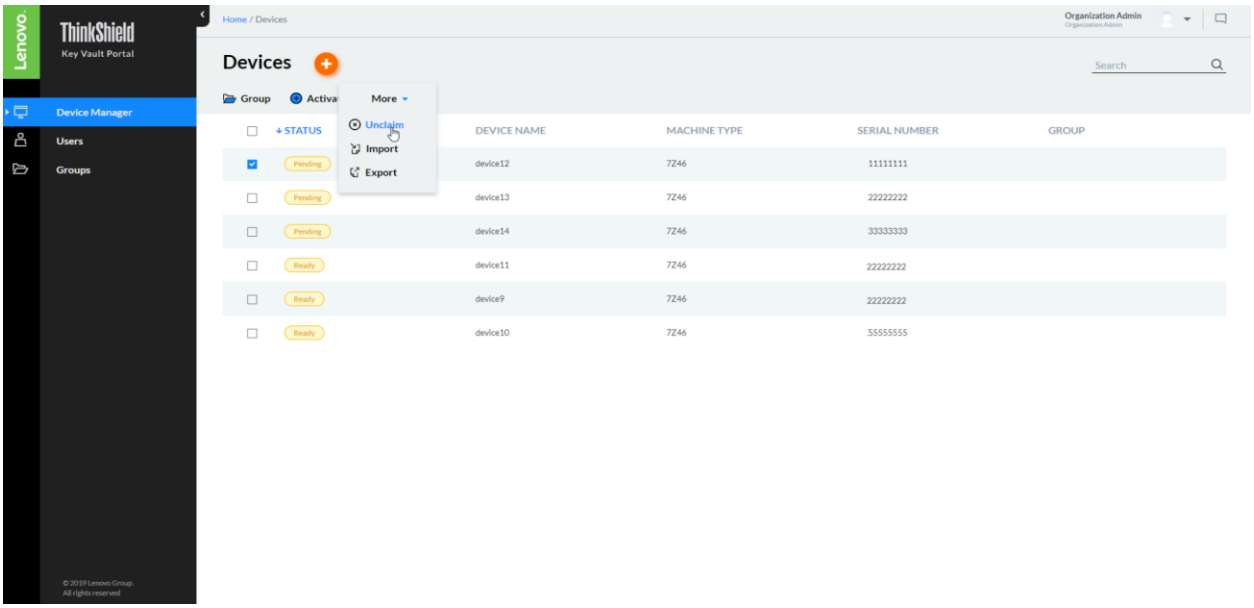


In case of successful upload, the Device(s) starts displaying in the Devices list. The status of the Device(s) is Pending.

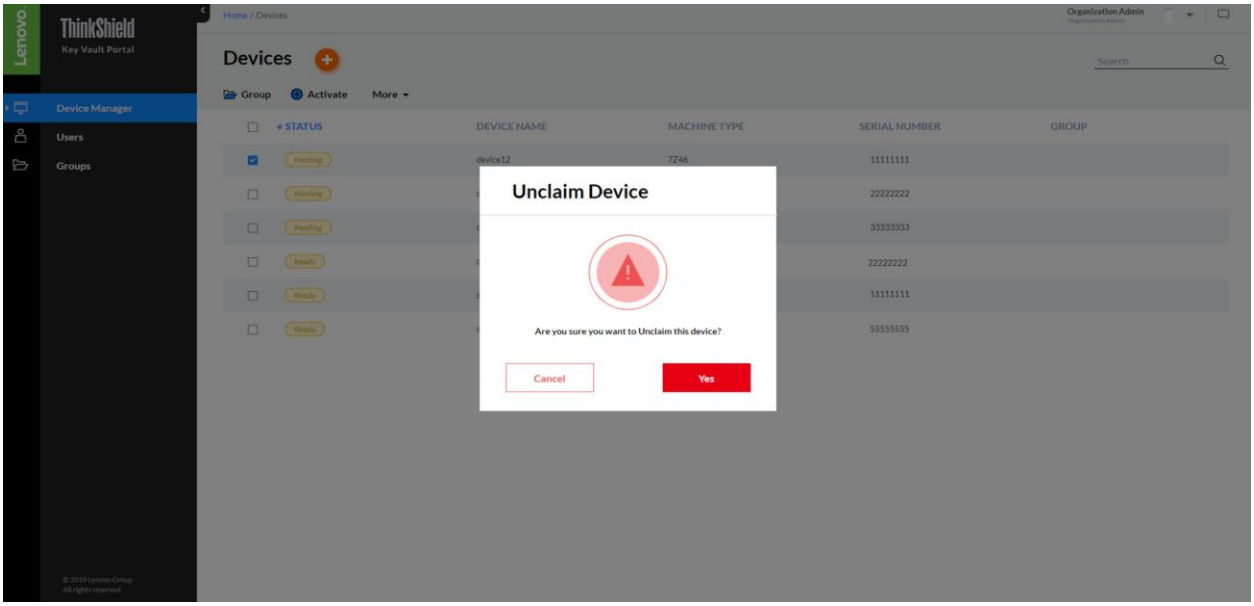


Unclaiming a Device

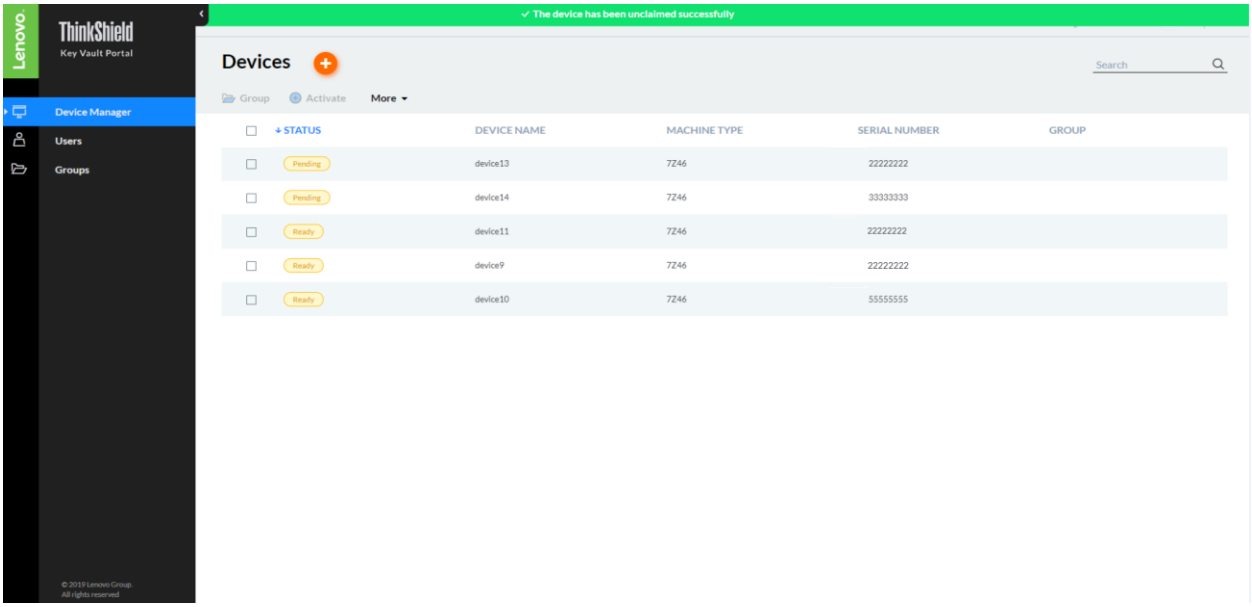
Check the Device(s) you want to unassign from the Organization and click ‘Unclaim’ in ‘More’ drop-down at the top of the page in order to unclaim a Device.



Confirm the action by clicking ‘Yes’ on ‘Are you sure…’ pop-up.



The selected Device(s) are removed from the Organization list.

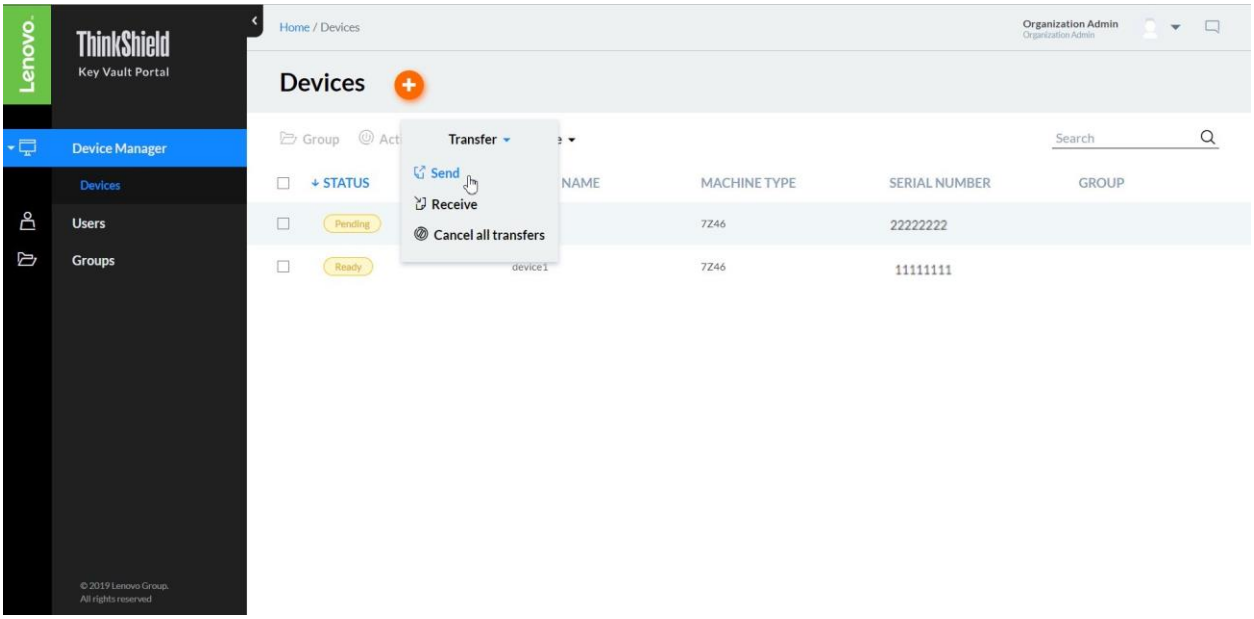


Transfer

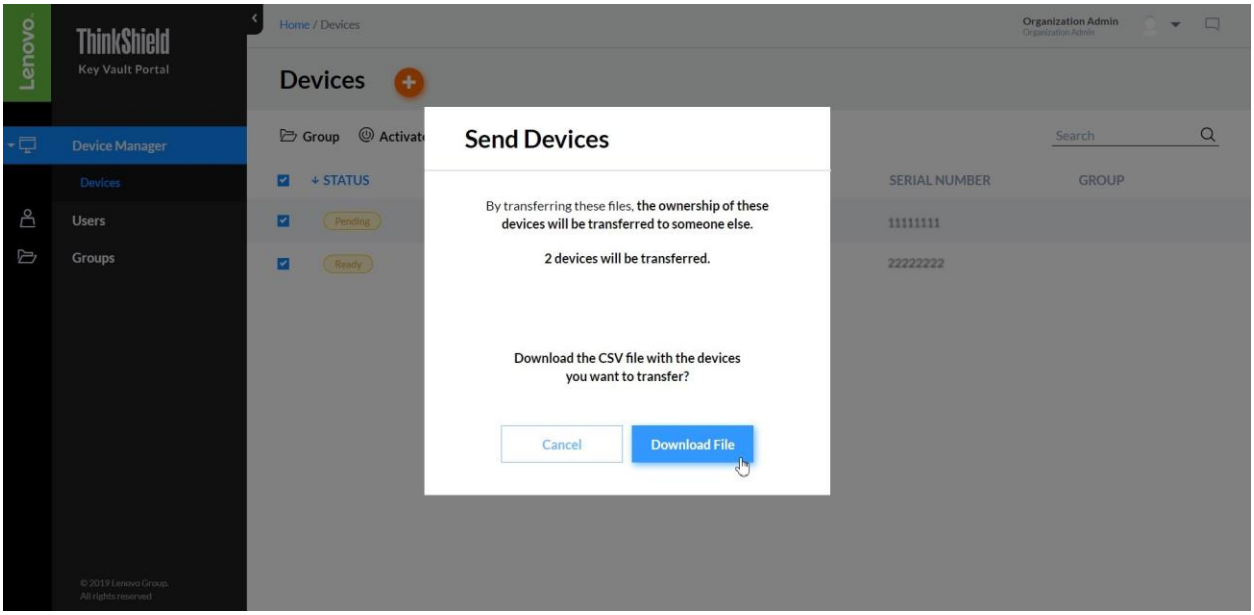
‘Transfer' option allows to send one Device or several Devices to other organization.

Send

To send the Devices to other organization check the Device(s) you want to transfer and click 'Send' in 'Transfer' drop-down at the top of the page.

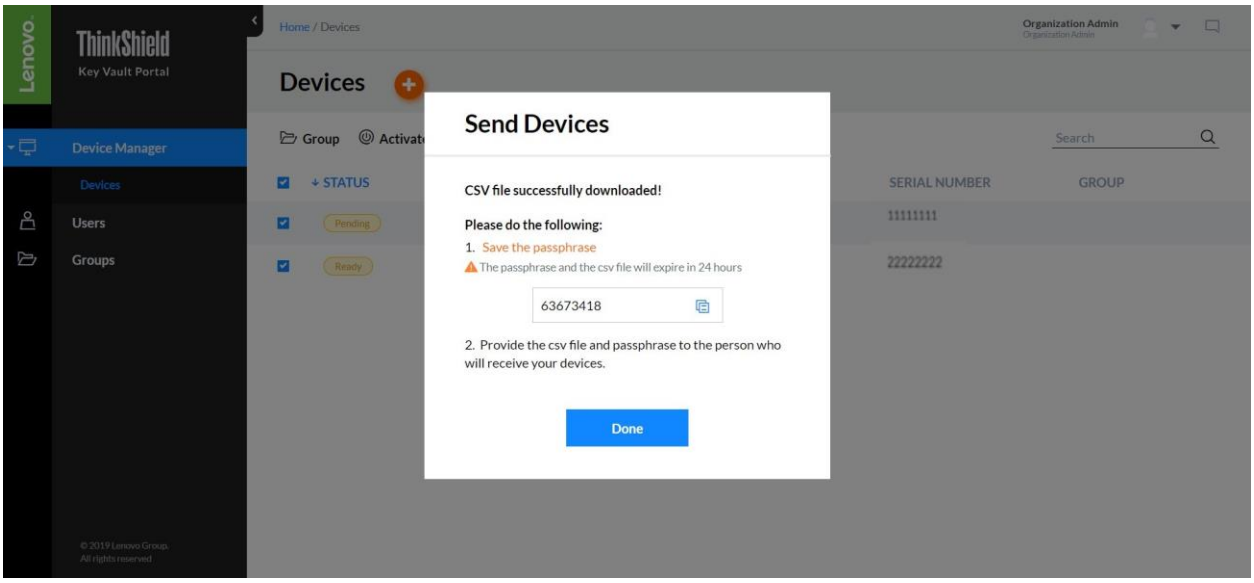


Click 'Download file' on the pop-up window 'Send Devices'. A .CSV file with the Device(s) you want to transfer will be downloaded to your computer.



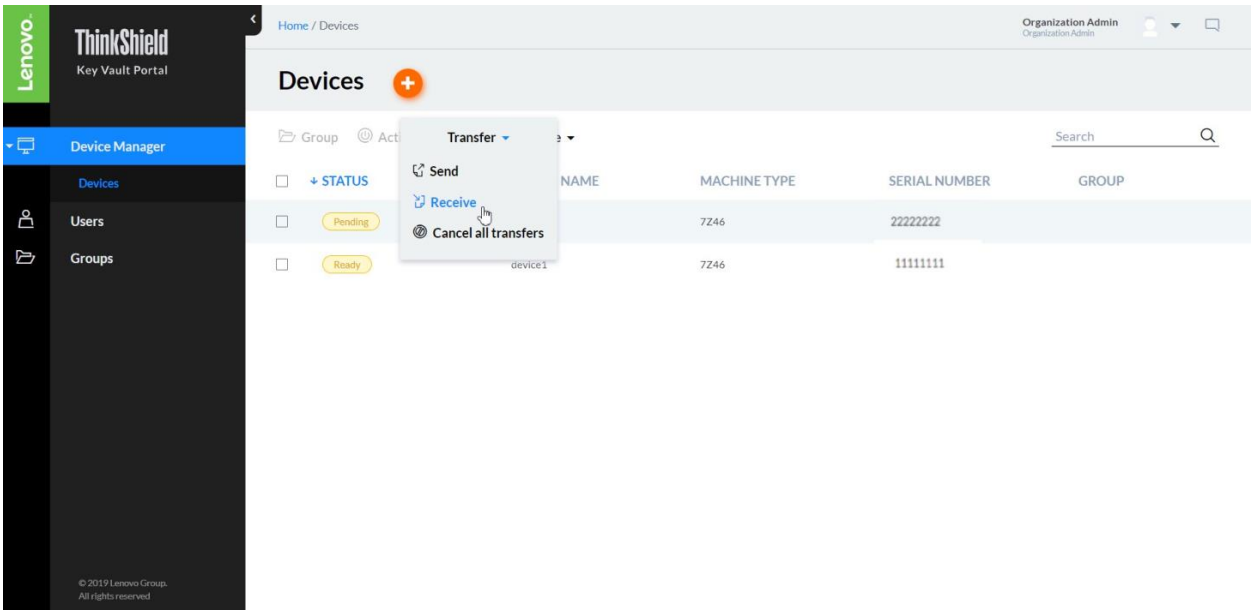
After a .CSV file has been downloaded, the passphrase will be shown on 'Send Devices' pop-window. Copy and save the passphrase and click 'Done'. Provide the downloaded .CSV file and the passphrase to a person who will receive your Devices.

Note: The passphrase and a .CSV file expire after 24 hours. Please make sure you have sent them to a receiver within 24 hours after they were generated.

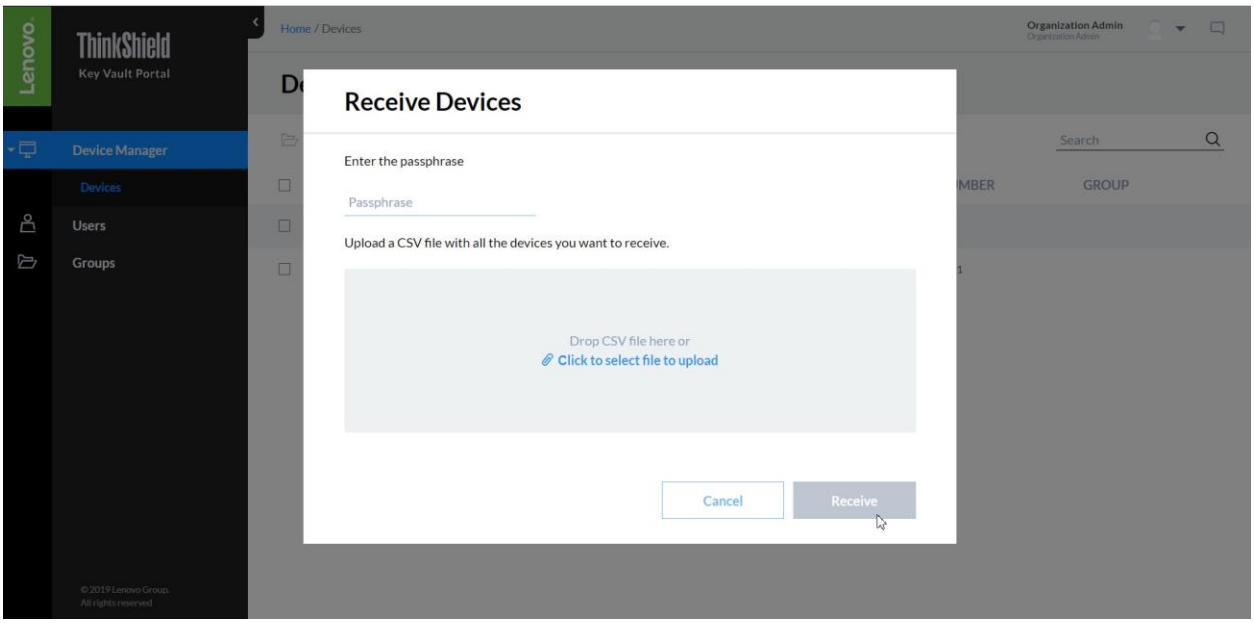


Receive

To receive the Device(s) from other organization click 'Receive' in 'Transfer' drop-down.

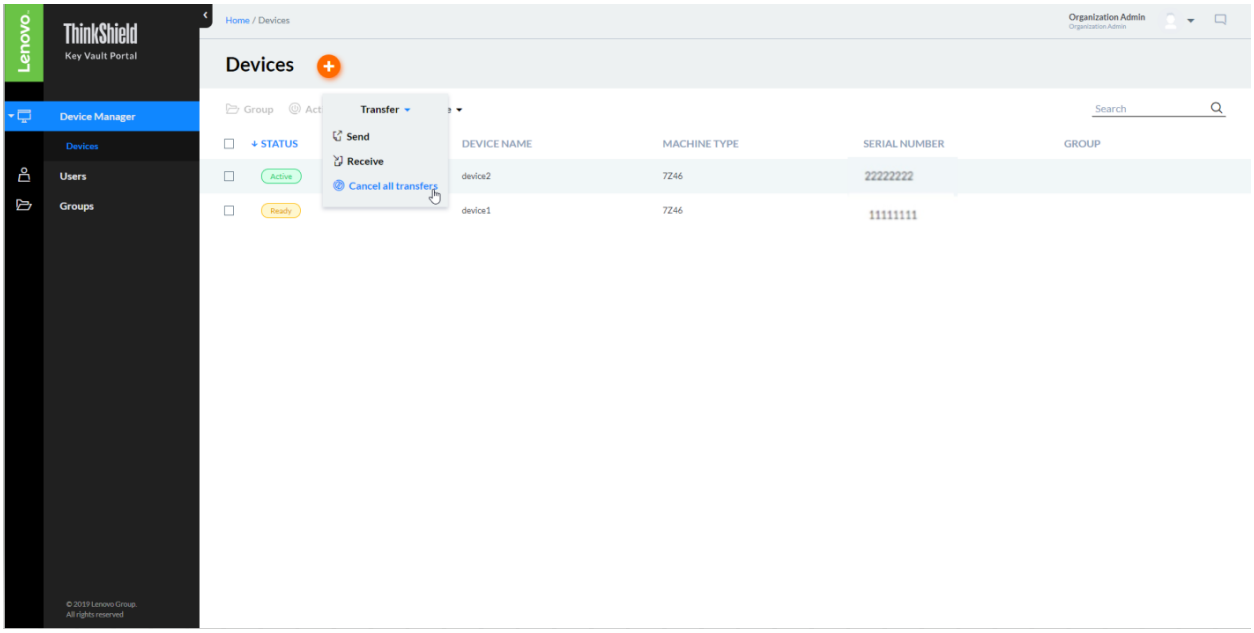


Provide a passphrase and upload a .CSV file with a list of Devices you received from other organization. Click 'Receive' after all the information has been provided. The Devices will be transferred to your organization.

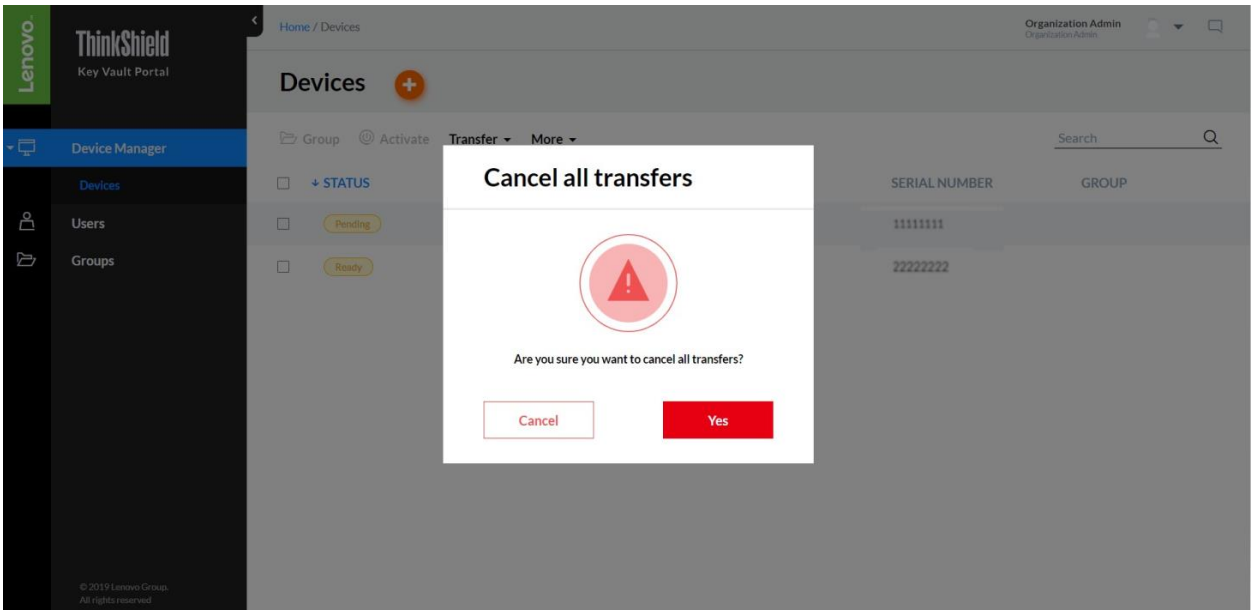


Cancel all Transfers

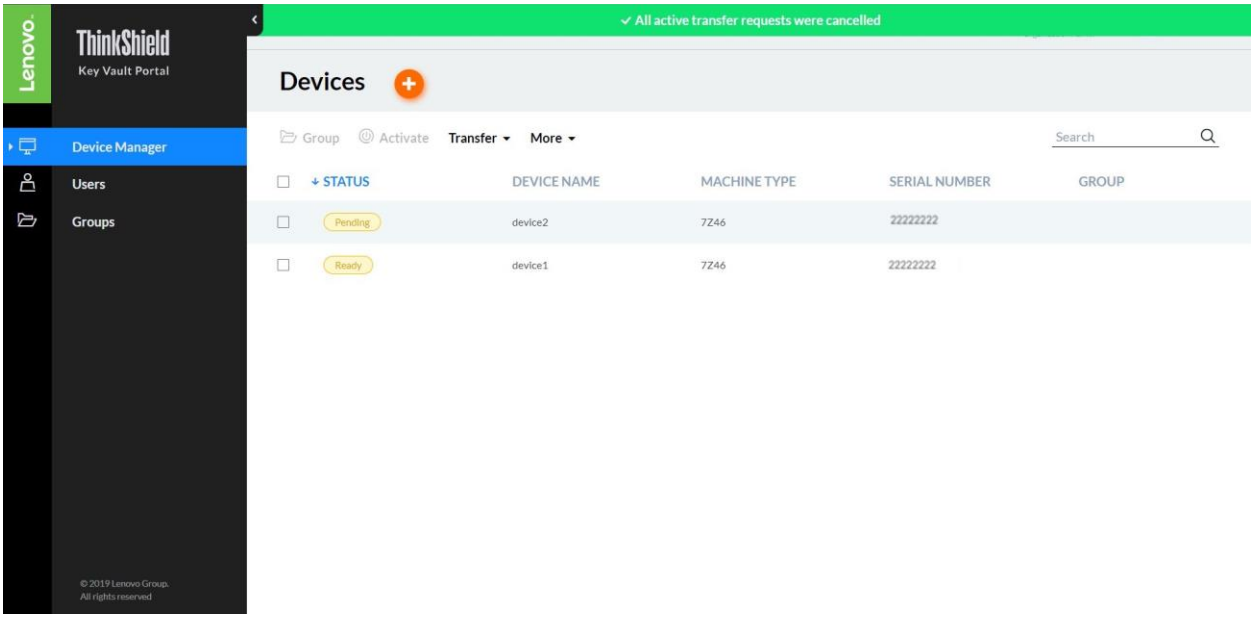
To cancel the transfer(s) click 'Cancel all transfers' in 'Transfer' drop-down at the top of the page. This will stop all your current transfers and a receiver will be unable to transfer the Device(s) to their organization.



Confirm the action by clicking 'Yes' on 'Cancel all transfers' pop-up.

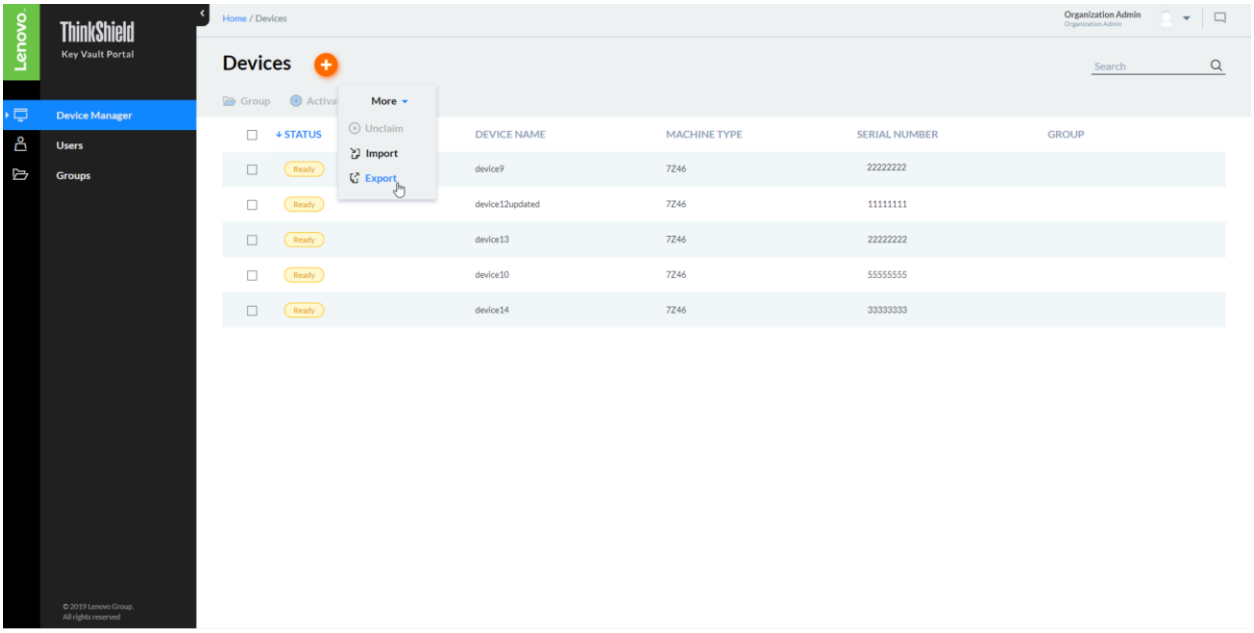


All current transfers are canceled.

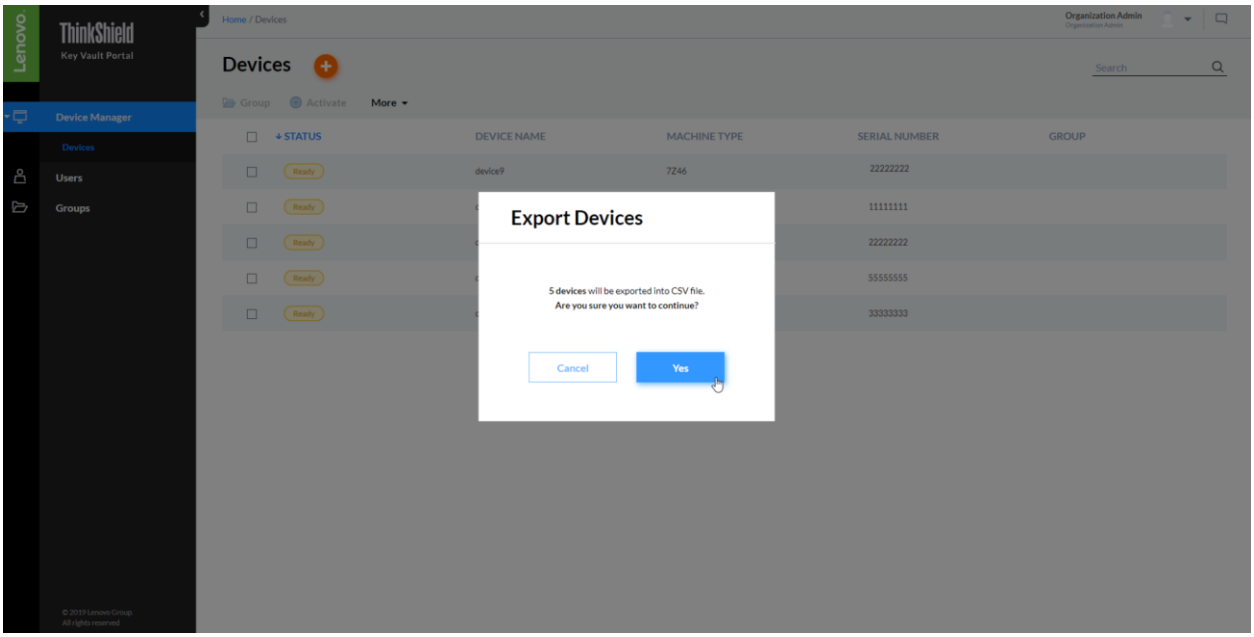


Export Devices

'Export' option allows to download a file with the list of all the Devices and their associated attributes. To export a list of Devices, click 'Export' in 'More' drop-down at the top of the page.

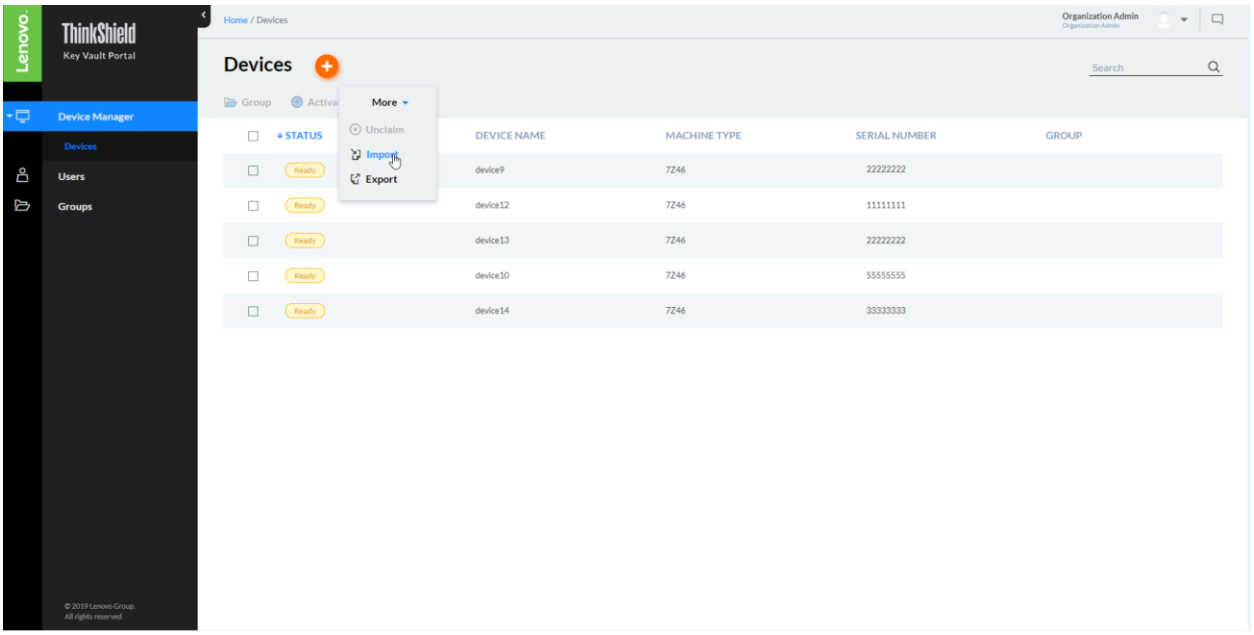


Click 'Yes' on 'Export Devices' pop-up to initiate downloading process.

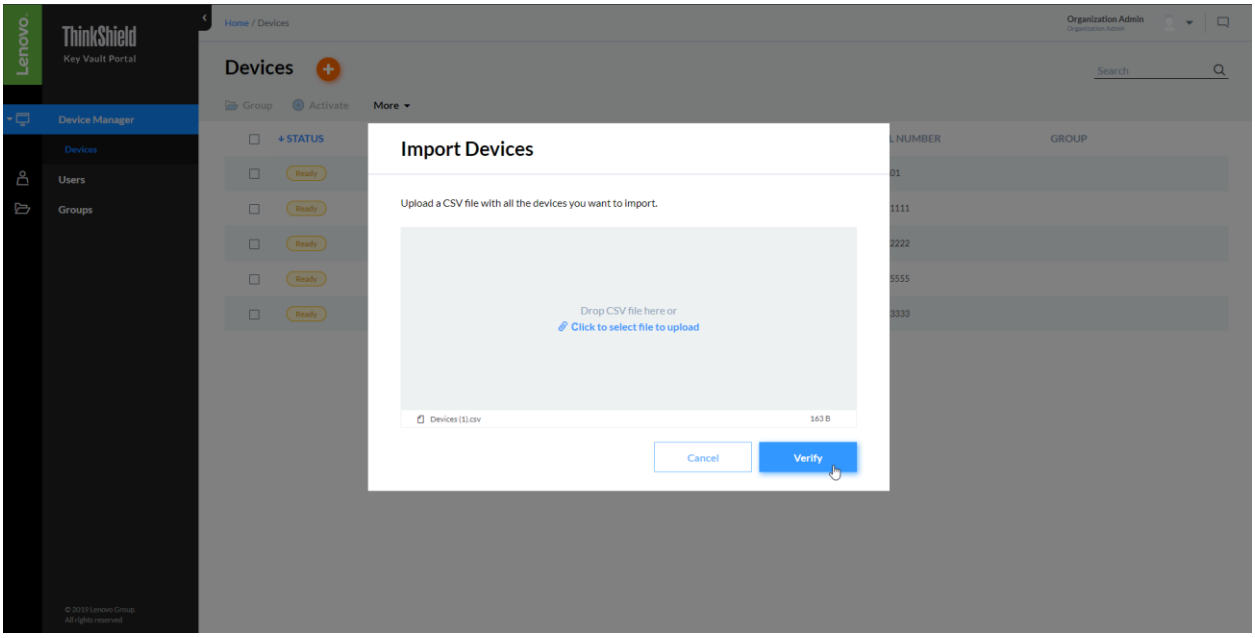


Import Devices

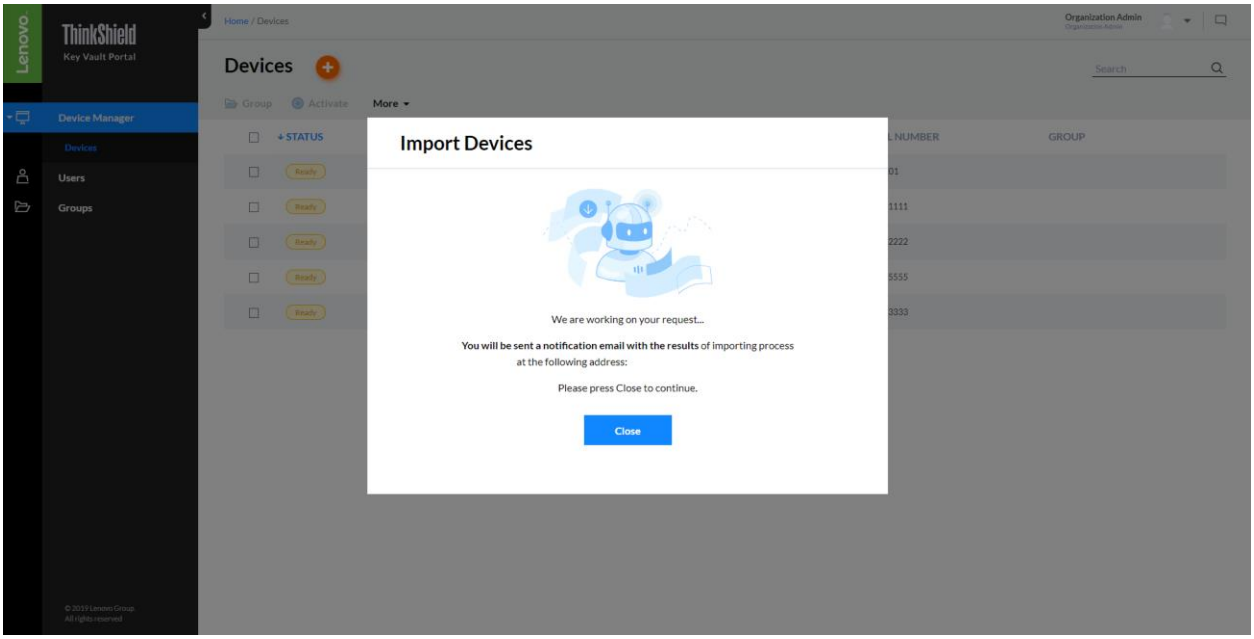
'Import' option allows to upload updated Devices information. To start importing process click 'Import' in 'More' drop-down at the top of the page.



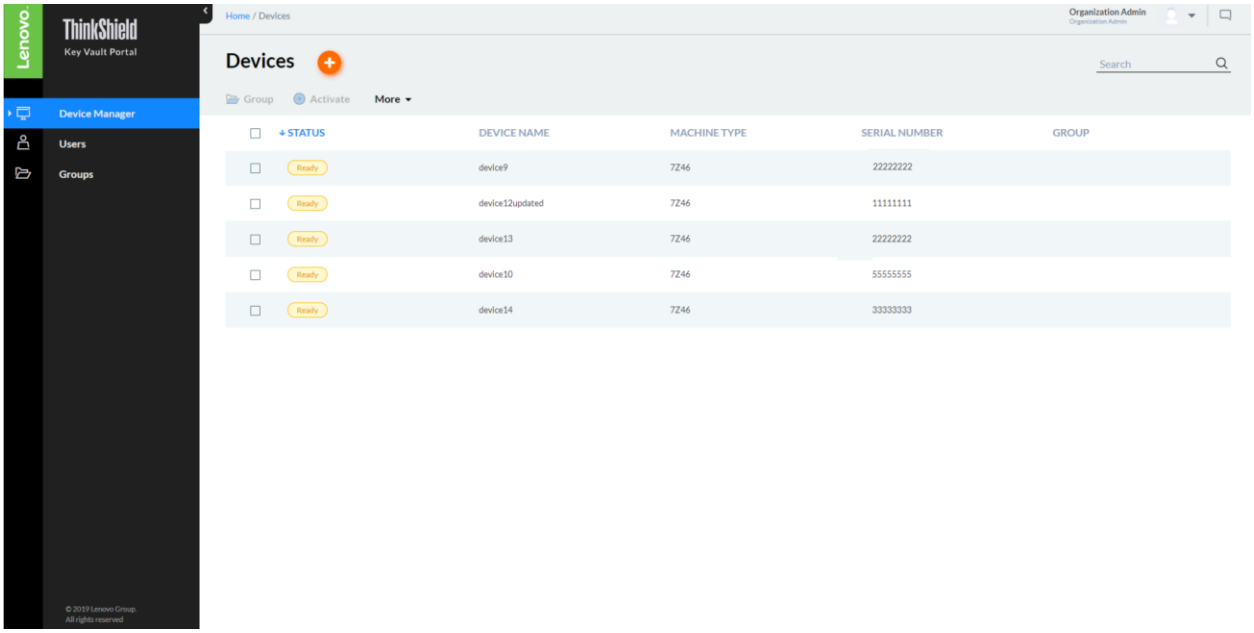
Upload a CSV file with all the devices you want to update and click 'Verify'.



As soon as the updating process is over you will get a confirmation email to the email address associated with your profile.

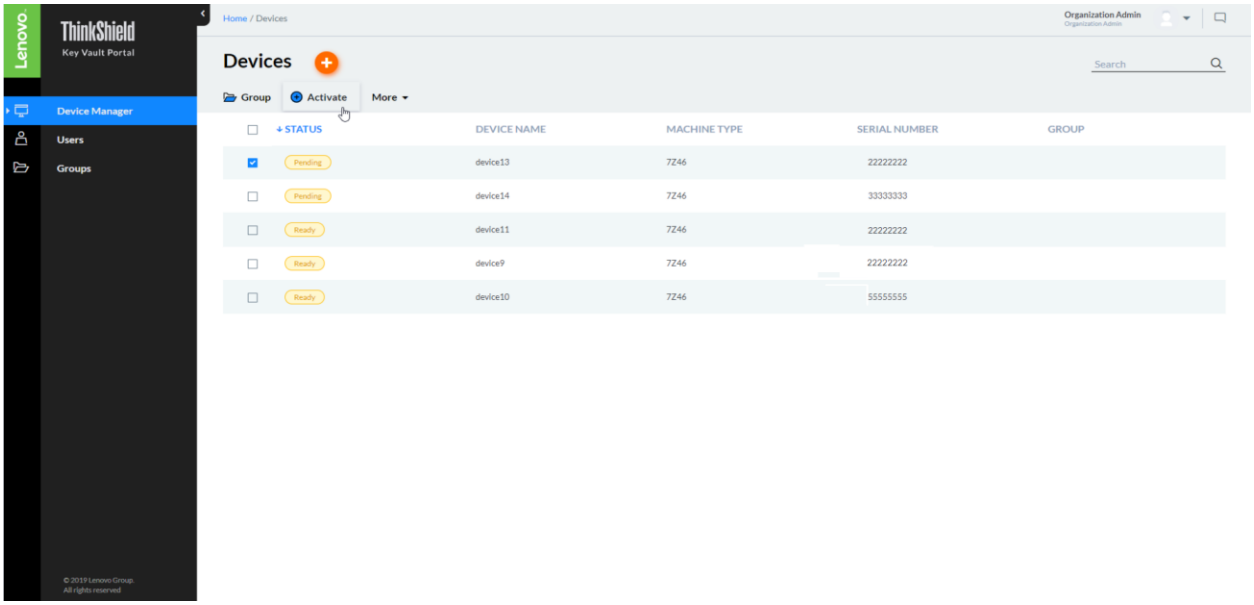


In case of successful import, the updates will be reflected in the Devices list.

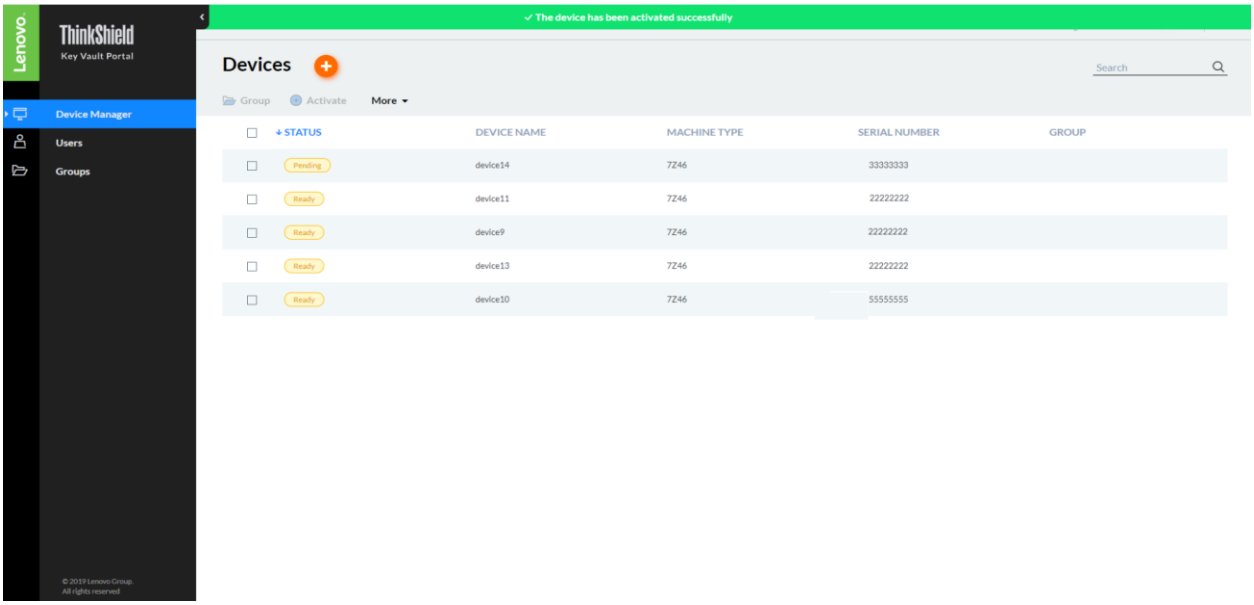


Automatic Activation

Check the Device(s) that need to be activated automatically and click ‘Activate’.



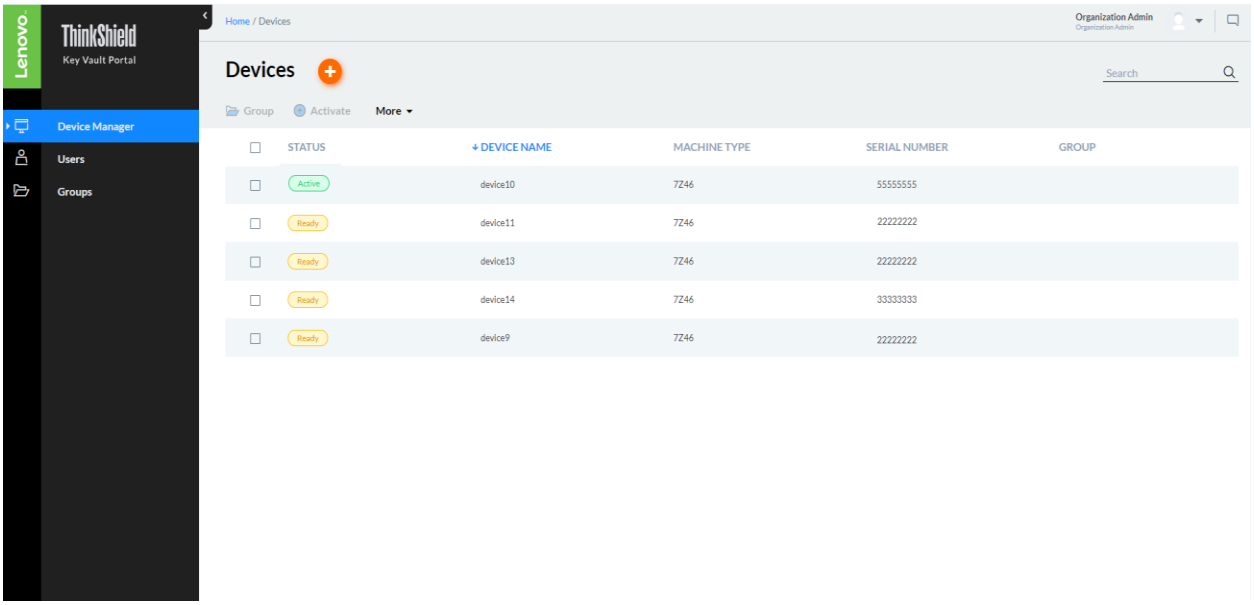
The status of such Devices will change to ‘Ready’.



Connect XClarity Controller management port to Internet. The Device will connect with the Portal and finish activation process automatically. After successful activation, the Device will become unlocked. – Action is done NOT on Portal side.*

** From device plug in the first call to the Portal happens after 10 minutes, thereafter the call happens every 5 minutes for 2 hours and 20 minutes. After that time the device requires a Device restart (or power cycle) to reinitialize this process.*

Device status changes to Active on the Portal.

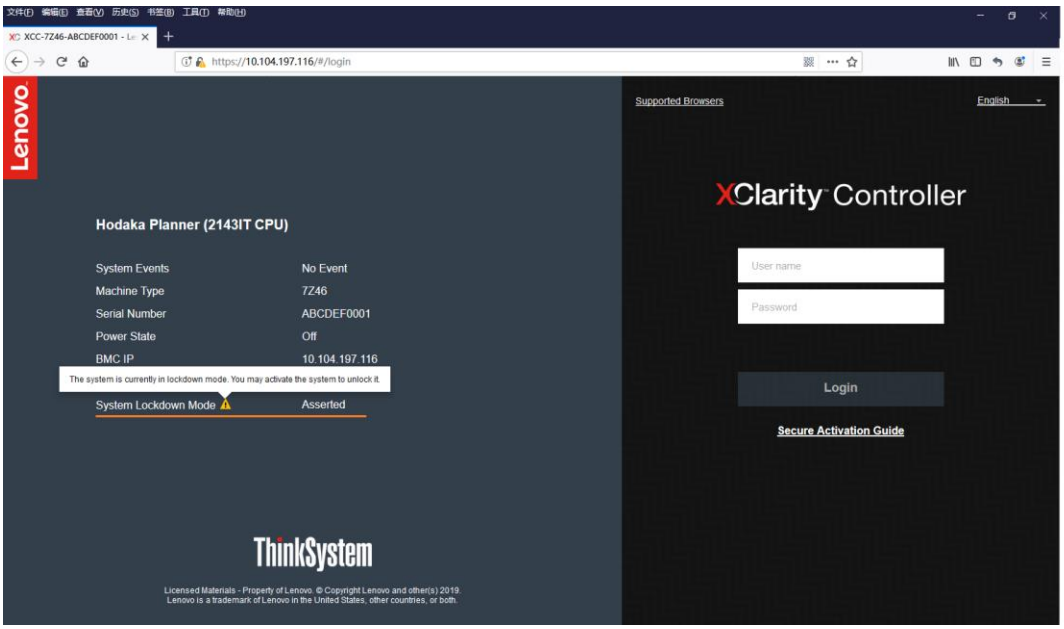


Manual Activation

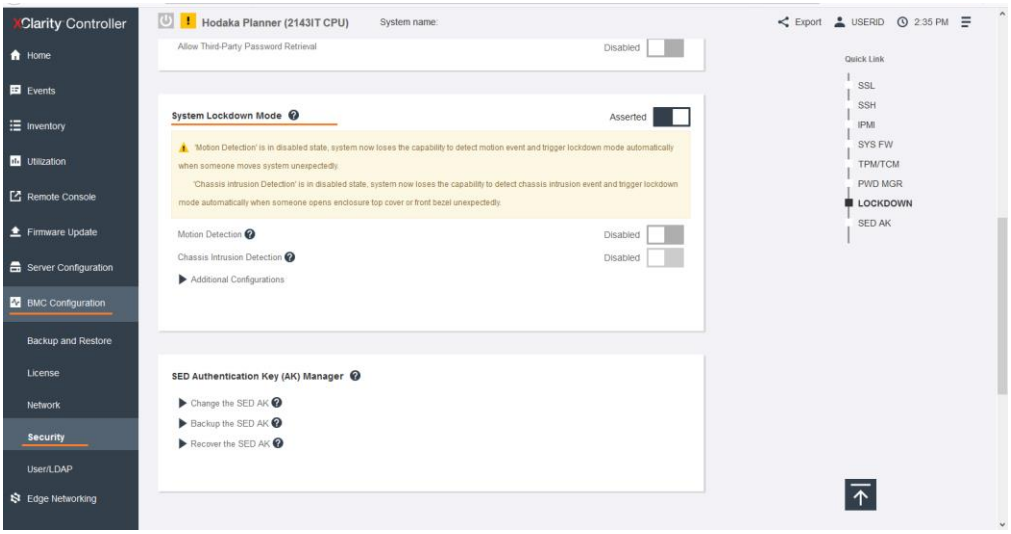
NOTE: to activate device manually actions should be performed on Portal (highlighted in green) and BMC web console (highlighted in blue).

Open BMC web console and check if system is in lockdown mode. Login with BMC credentials.

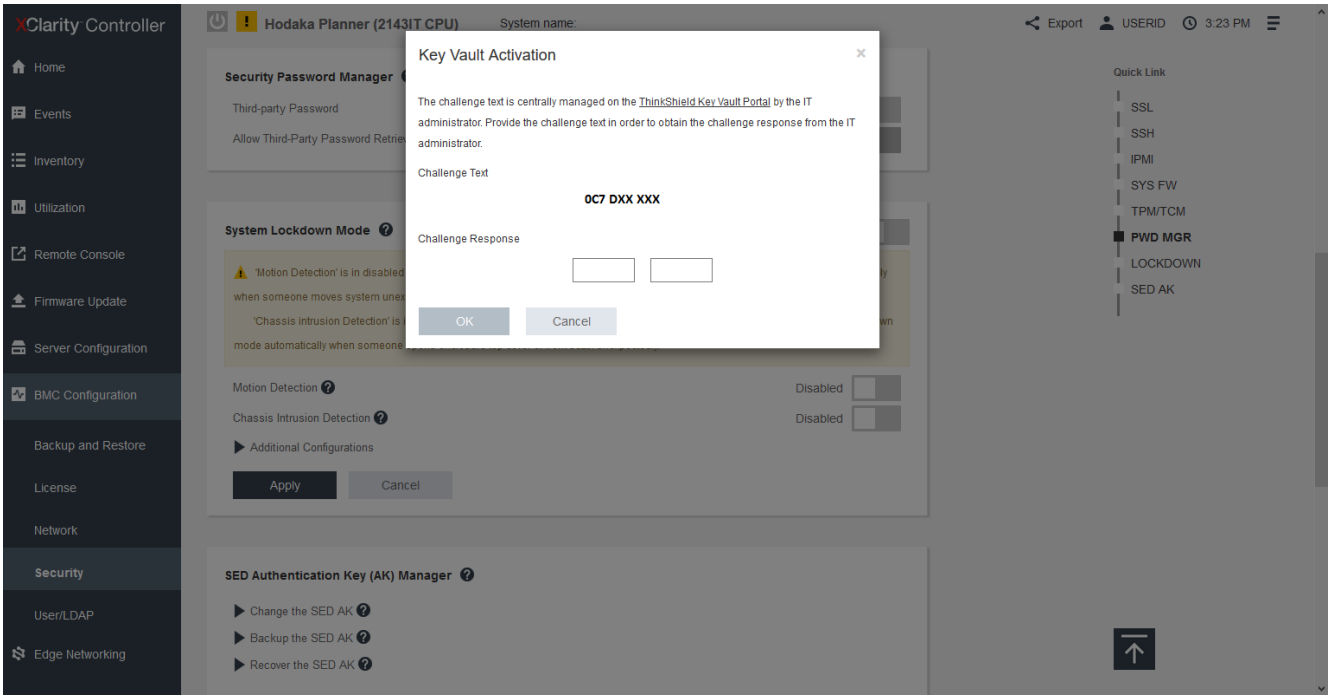
Note: If "System Lockdown Mode" is asserted state, system is currently in lockdown mode and needs to be activated. If "System Lockdown Mode" is de-asserted state, it means that system has been activated.



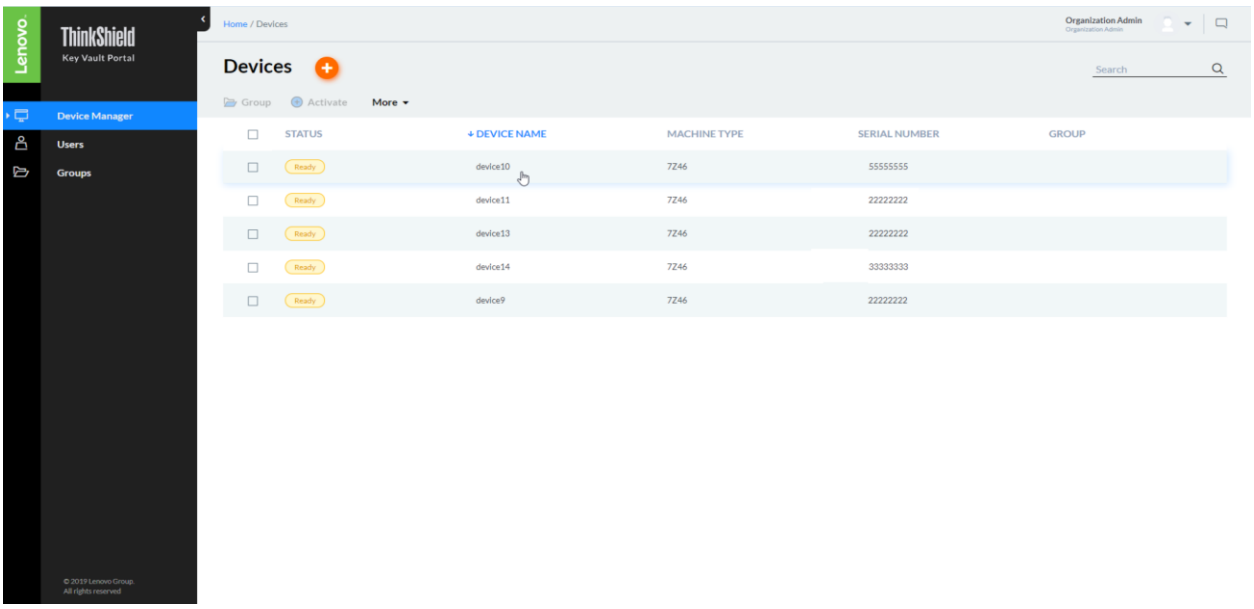
Go to "System Lockdown Mode" page.



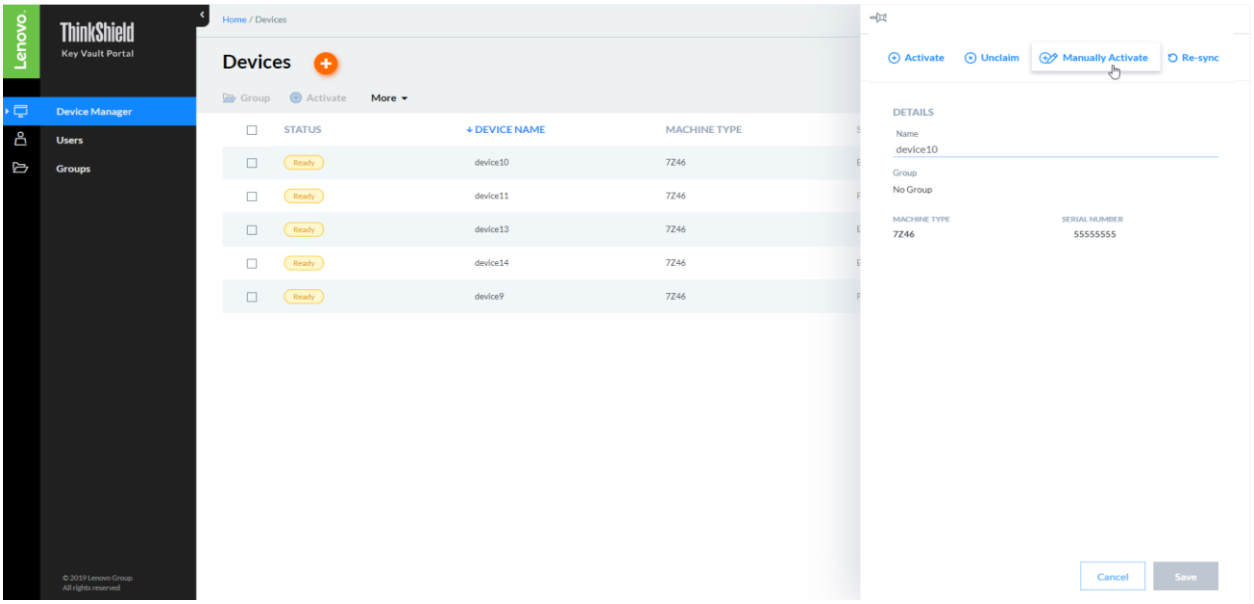
Scroll “System Lockdown Mode” toggle button to De-asserted state. Write down the **Challenge Text** from ‘**Key Vault Activation**’ pop-up.



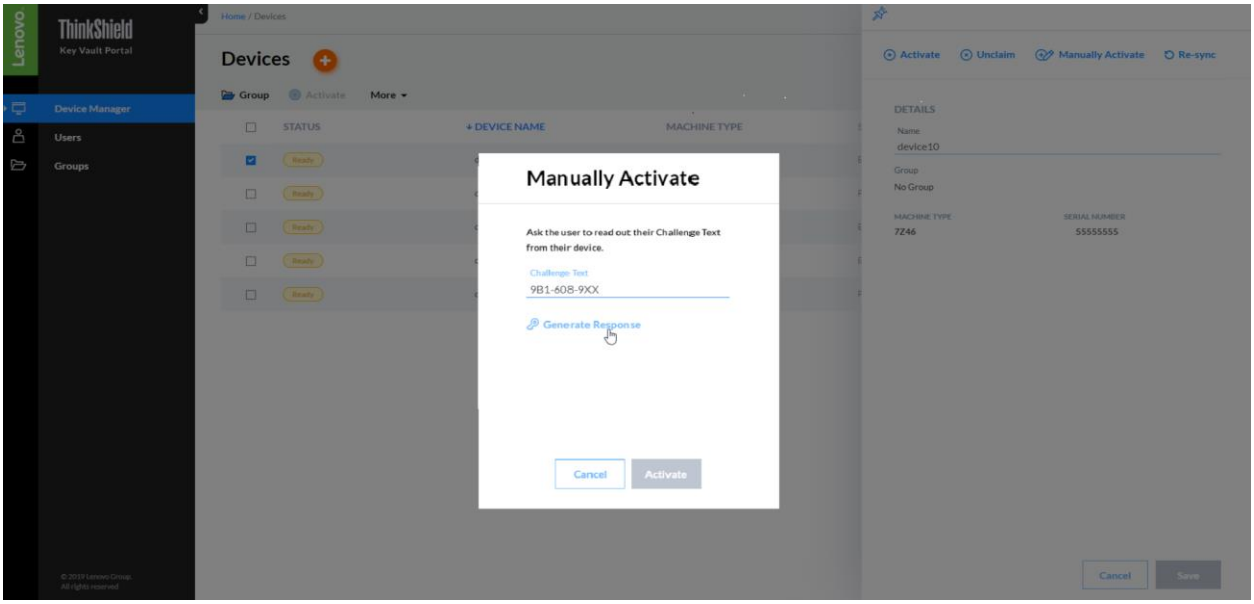
Log into Portal as Organization Admin and click on the Device that needs to be activated manually.



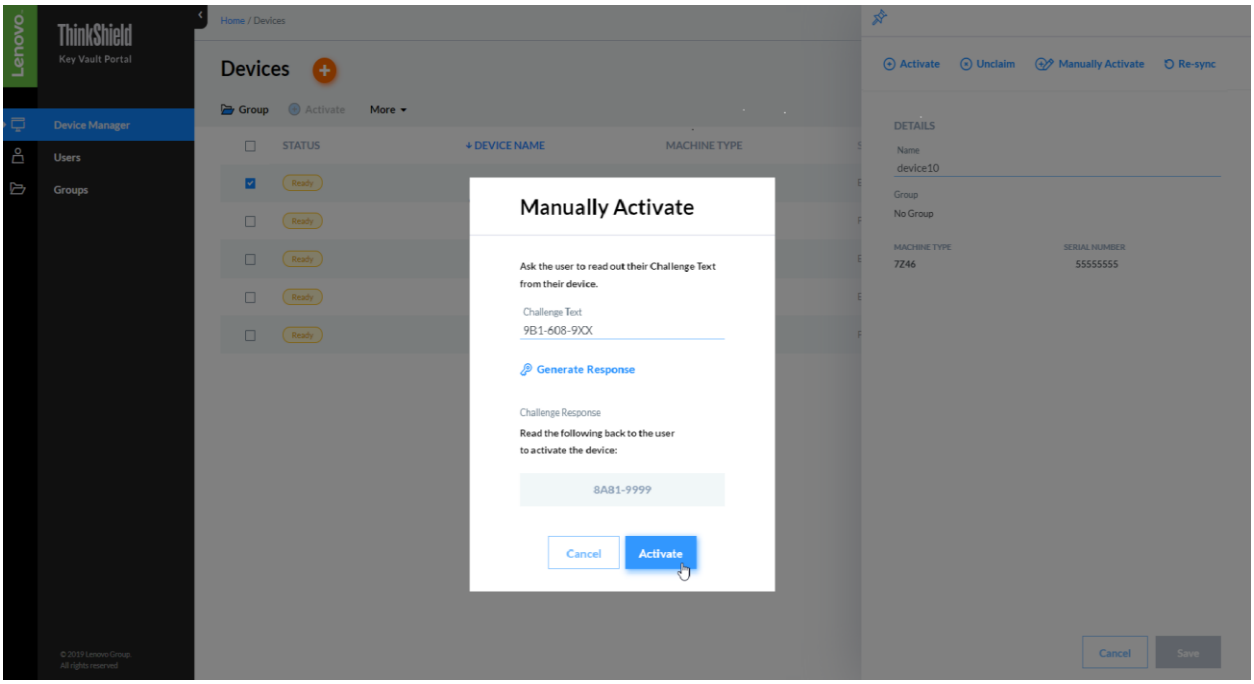
Click ‘Manually Activate’ button on the Device tray (Device top navigation panel).



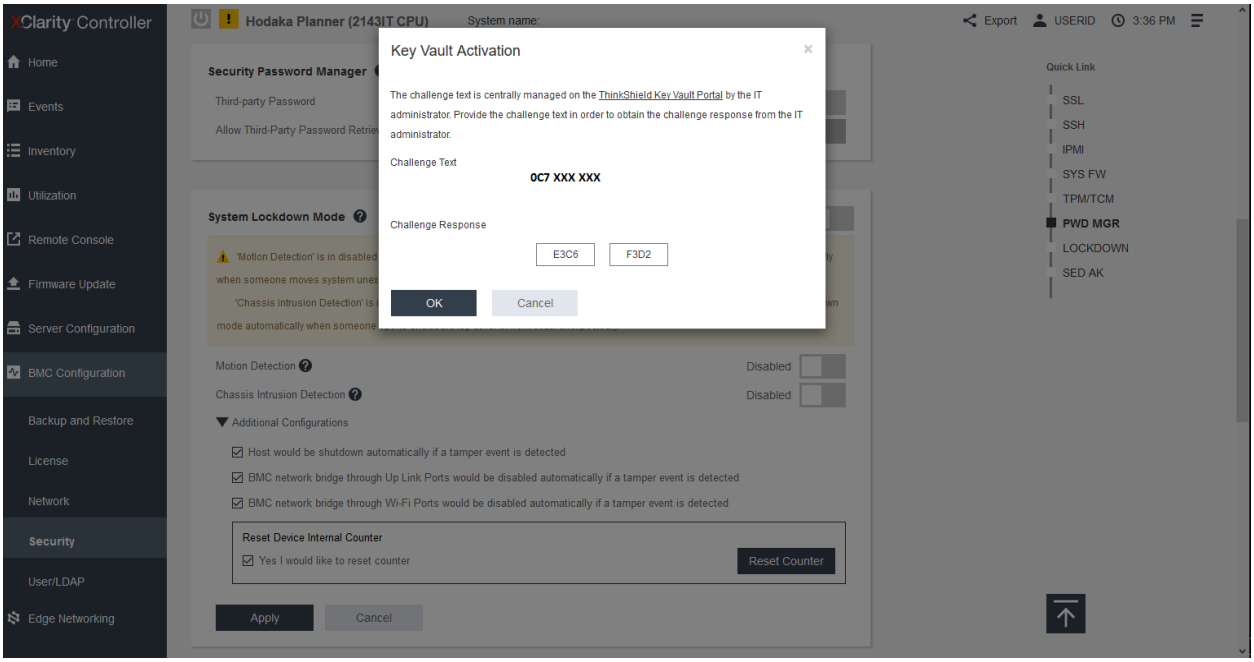
Provide Challenge Text from ‘Key Vault Activation’ pop-up into ‘Manually Activate’ pop-up and click ‘Generate Response’. If Challenge Text is valid, the Challenge Response will be displayed on the screen.



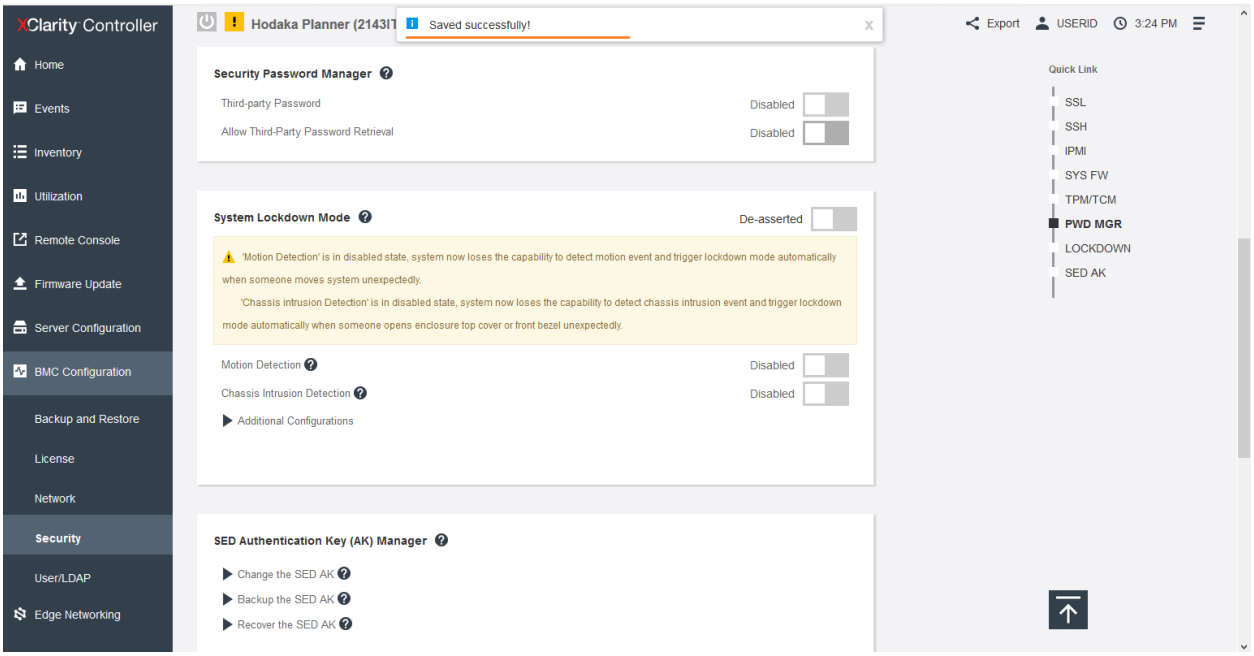
Write down ‘Challenge Response’.



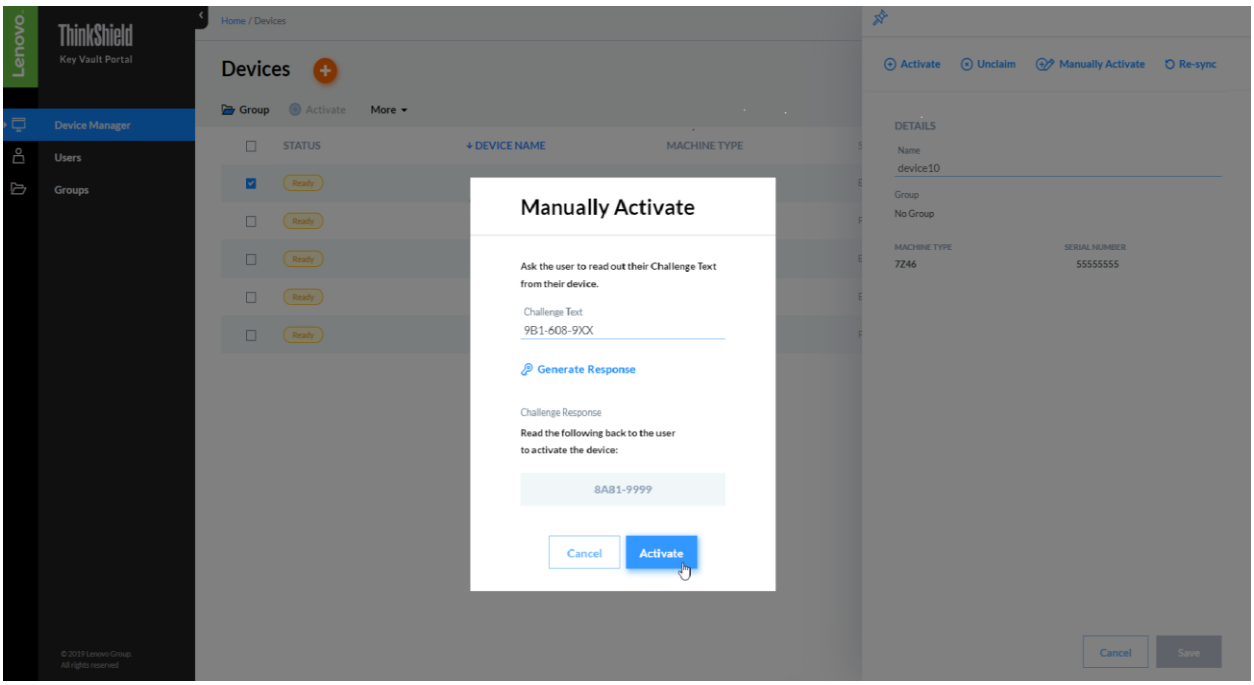
Provide ‘Challenge Response’ into ‘Key Vault Activation’ pop-up (BMC web console) and click ‘OK’.



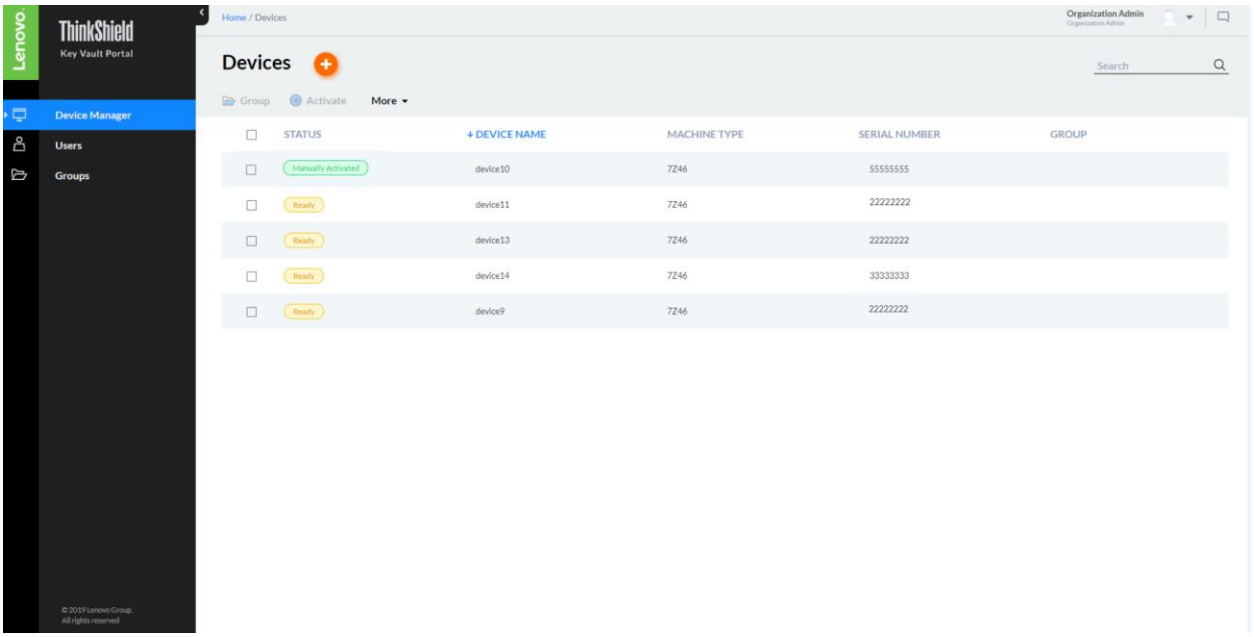
Click ‘Apply’. System Lockdown Mode changes to De-asserted state. The Device gets activated.



Click ‘Activate’ button on ‘Manually Activate’ pop-up (Portal).

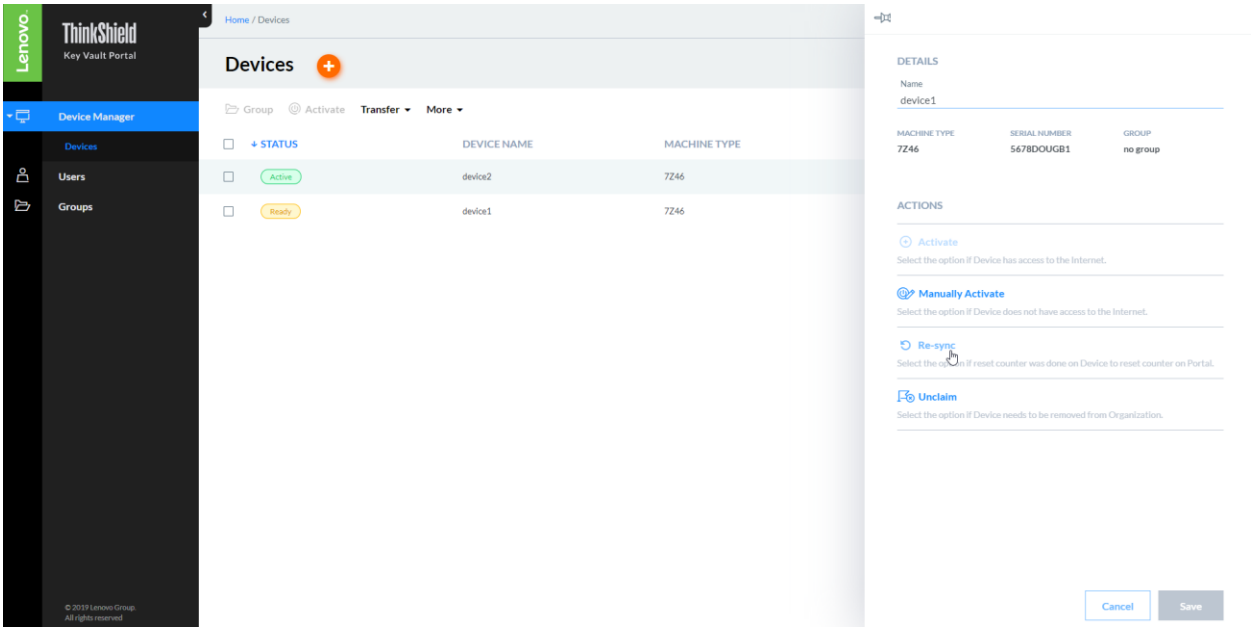


The Device changes its status to ‘Manually Activated’.

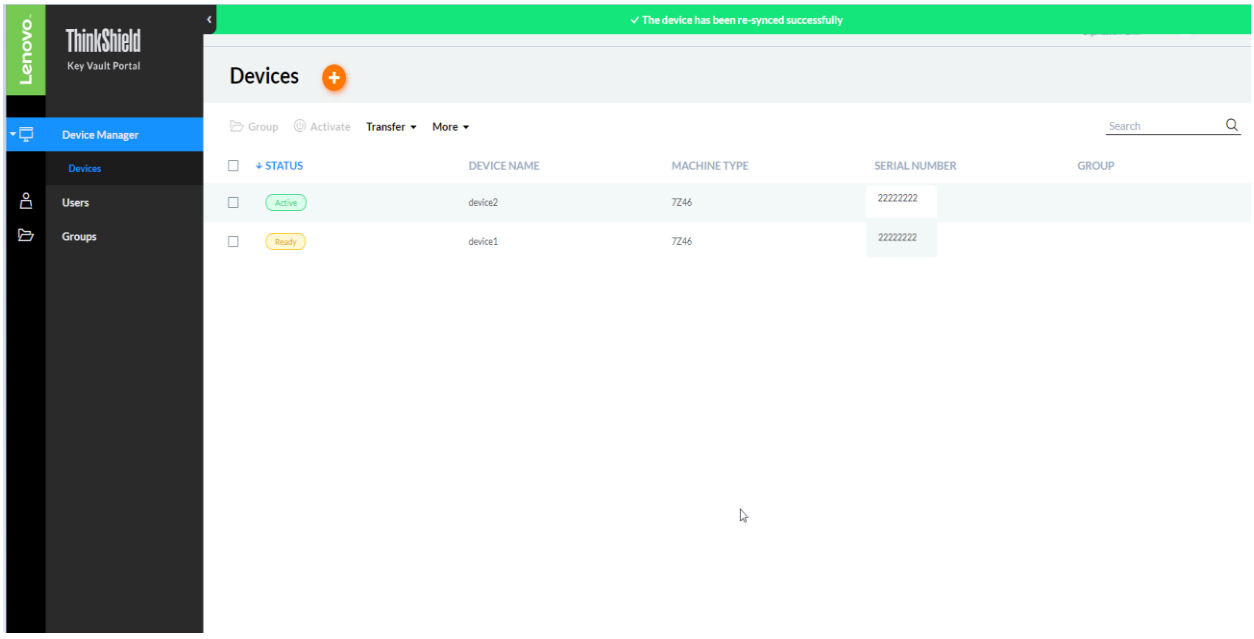


Re-sync

'Re-sync' counters option allows a user to reset the counters on the ThinkShield Key Vault Portal and a Device. To re-sync counters click 'Re-sync' on the Device tray.

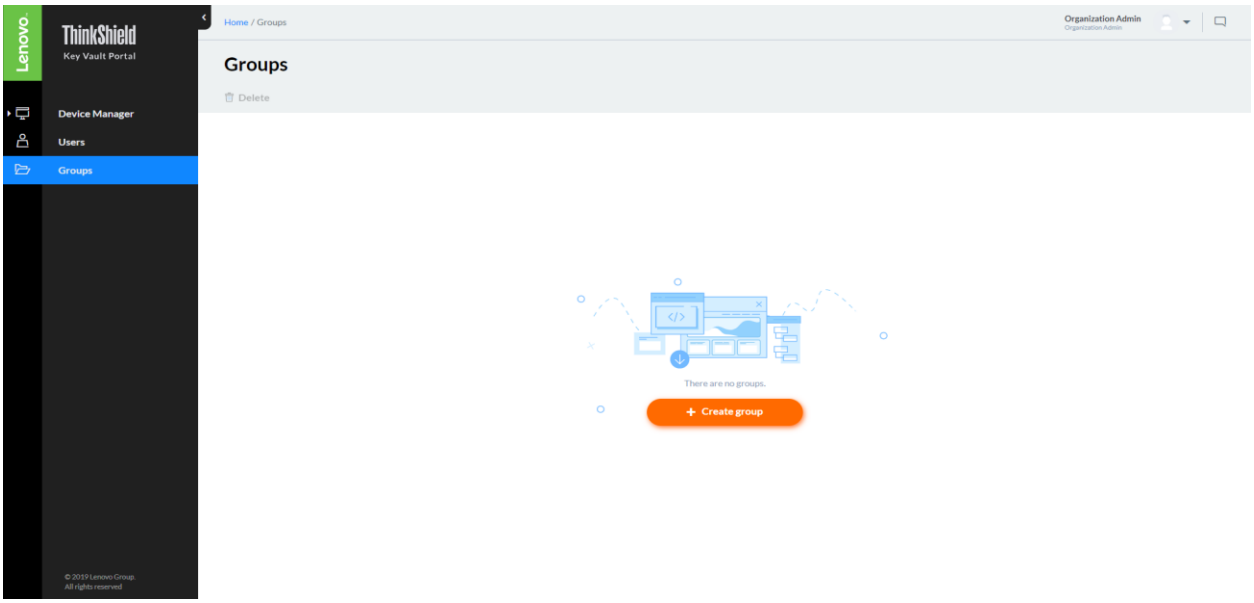


The counters are re-synced.

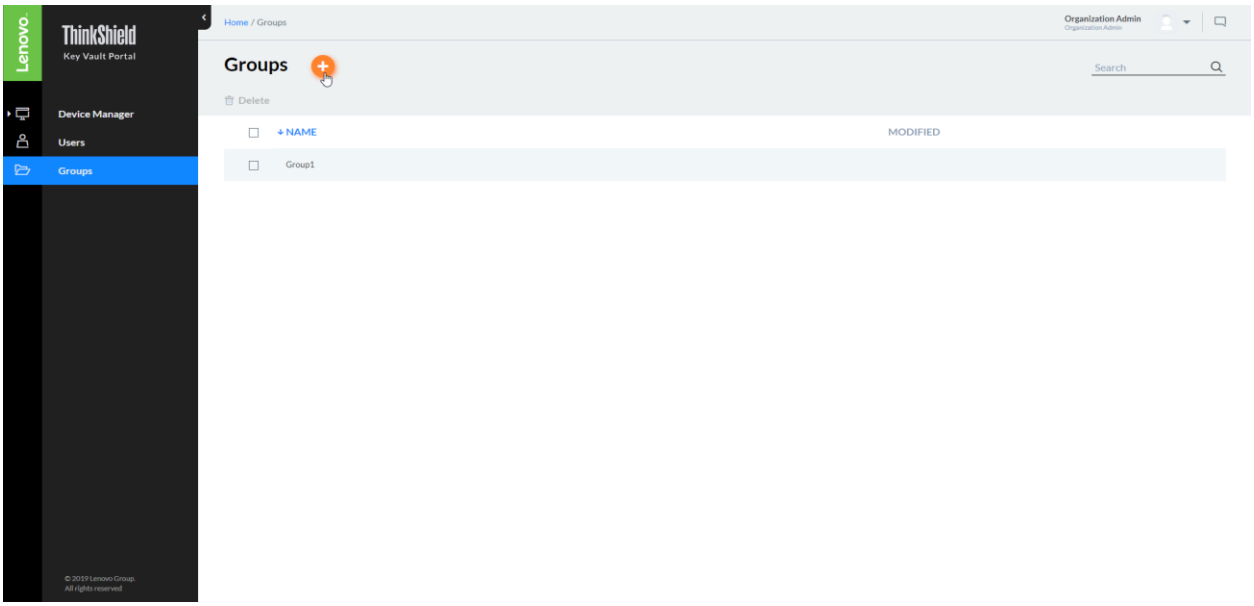


Create a Group

In order to add a new Group go to ‘Groups’ page and click ‘Create Group’.

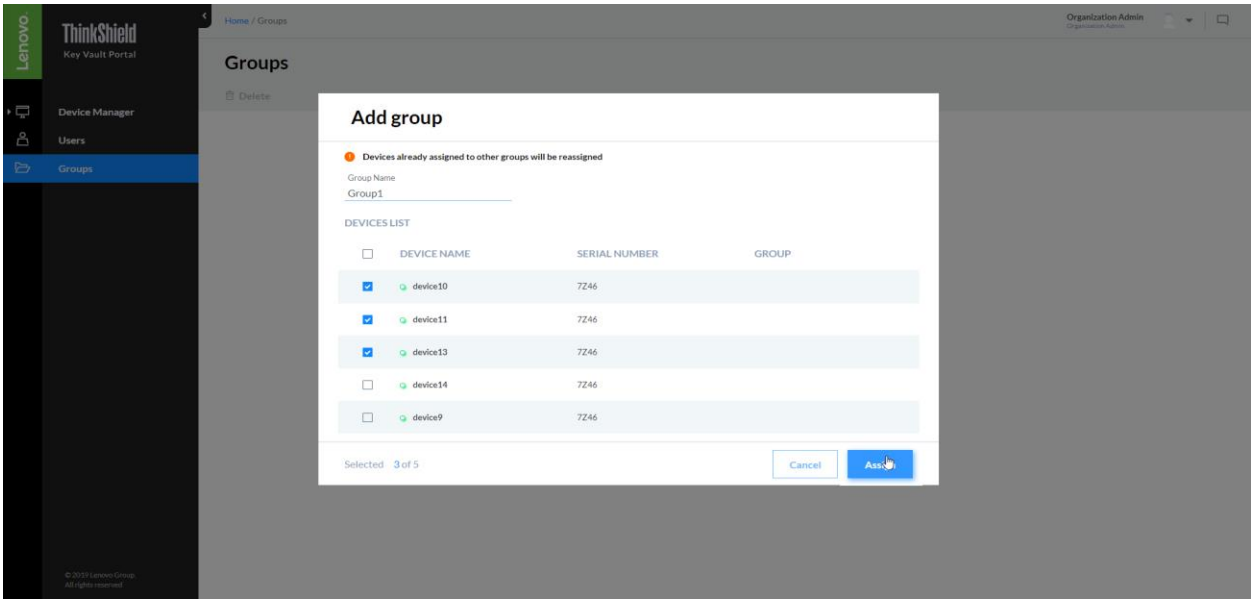


If there are Groups in the Organization, click ‘+’ icon at the top of the page in order to add a new Group.



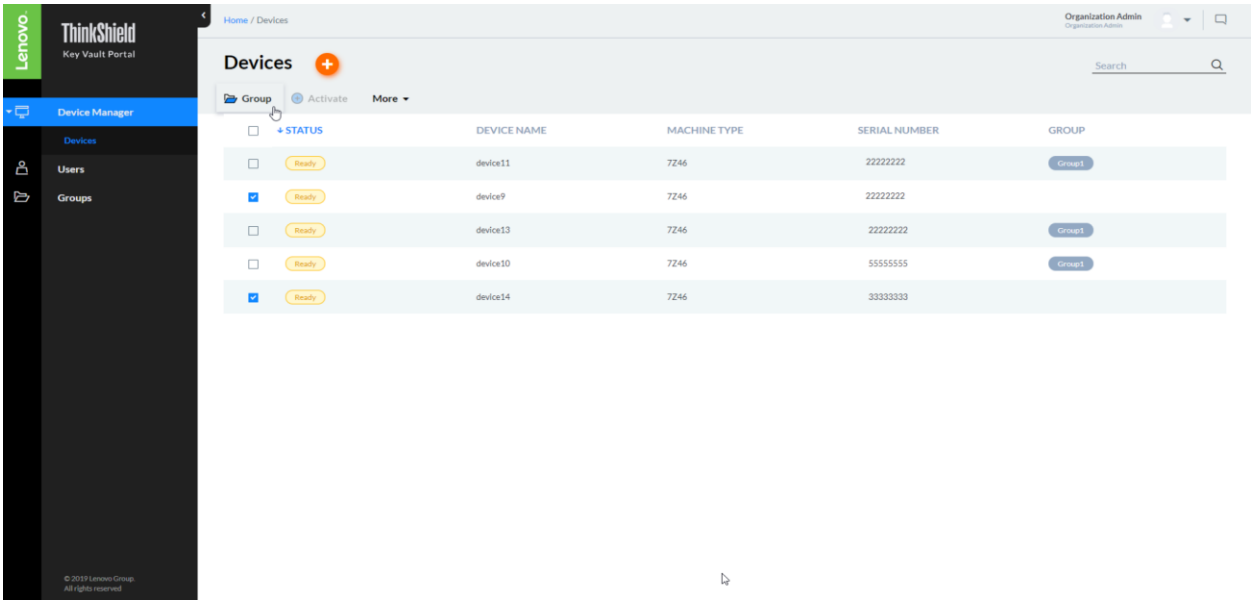
Fill in a required field ‘Group Name’ and check the Device(s) you want to assign to the Group. Click ‘Assign‘.

Please note that all the Devices that are already assigned to other groups will be reassigned.

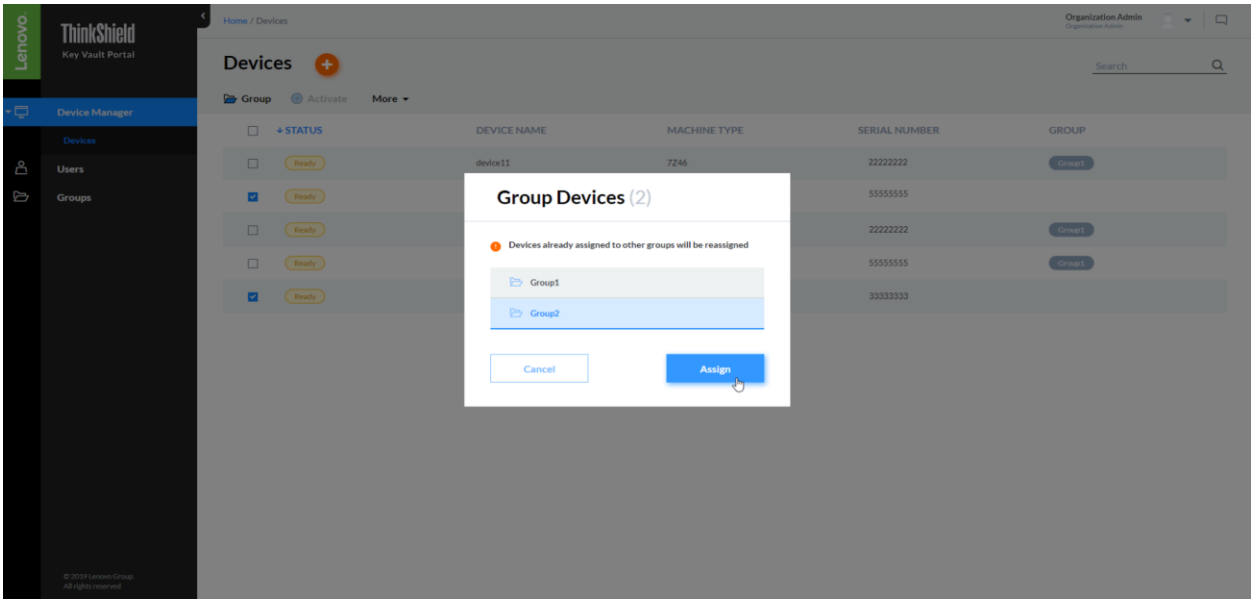


Group Devices

In order to assign a Device to the Group, go to the list of your Devices on ‘Devices’ page and check the Device(s) you want to assign to the Group. Click ‘Group’ at the top of the page.

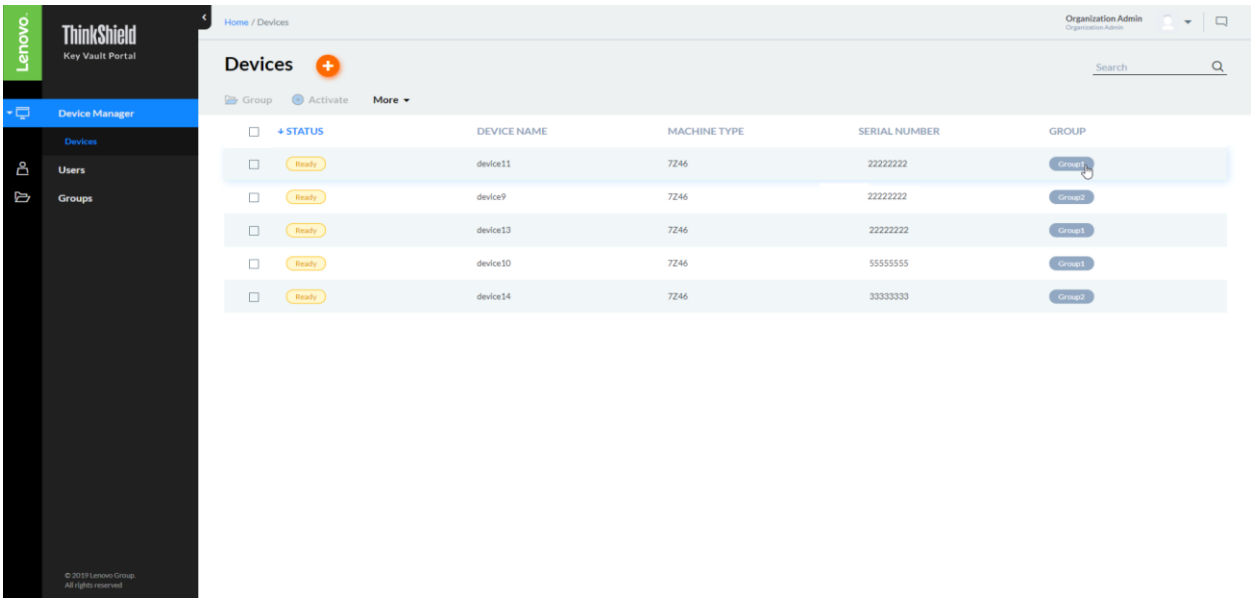


Choose the Group you want to assign the Device(s) to and click ‘Assign’.



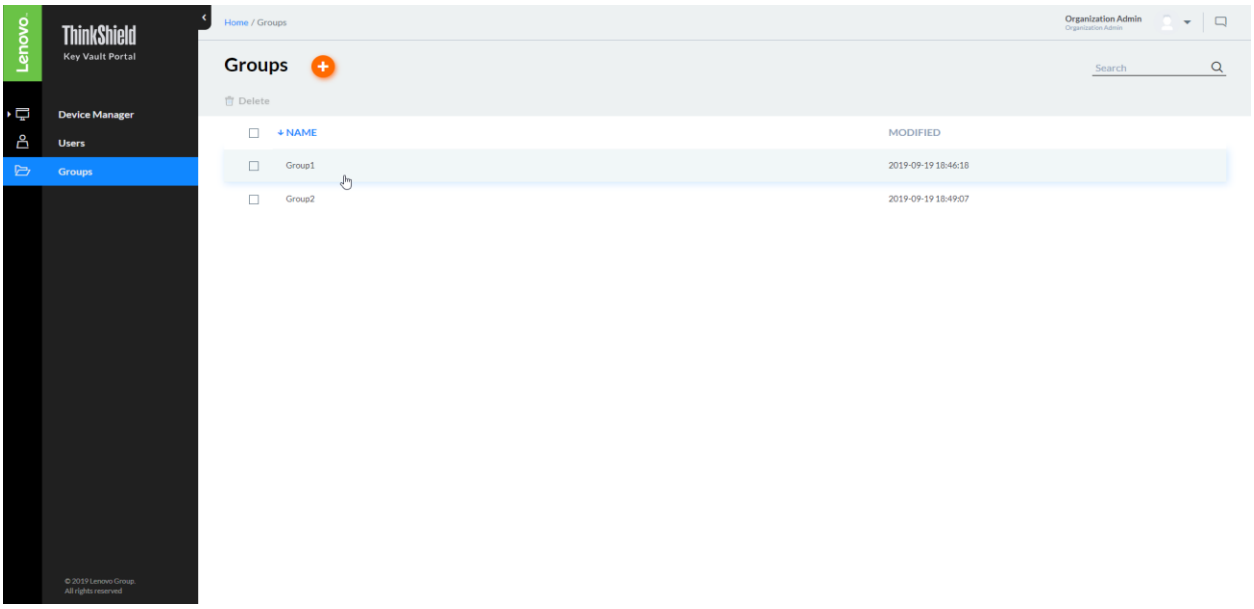
The Device is assigned to the Group.

Note: You can see the name of the Group next to each assigned Device.

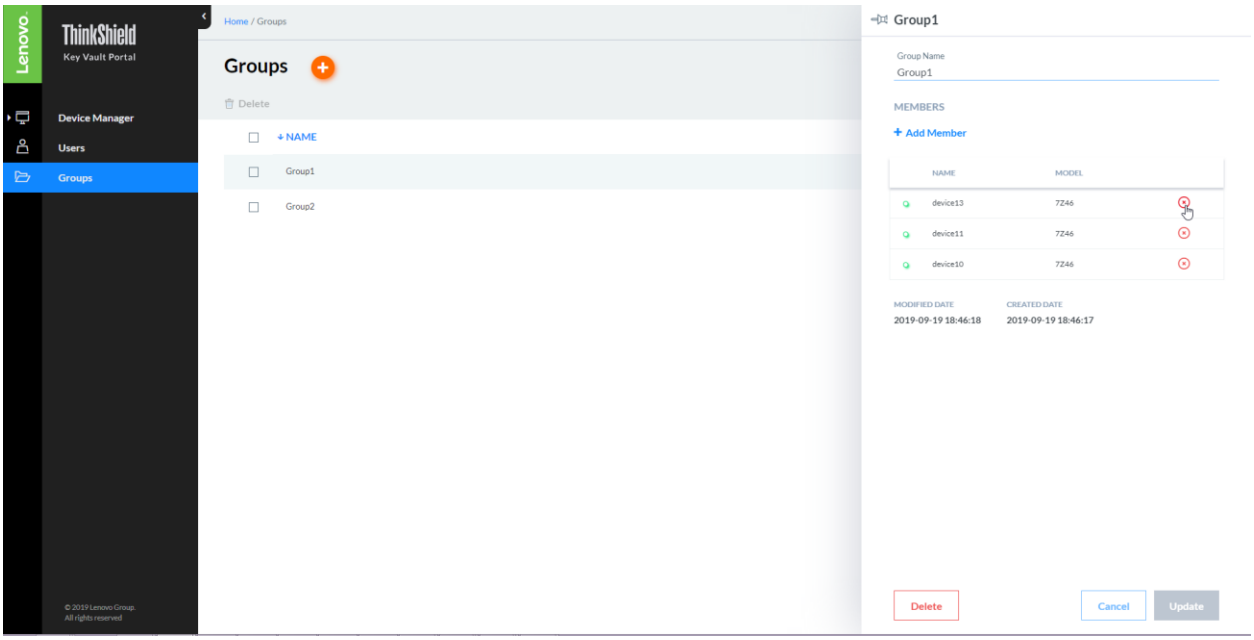


Remove Devices from Group

Select the Group by clicking on it.

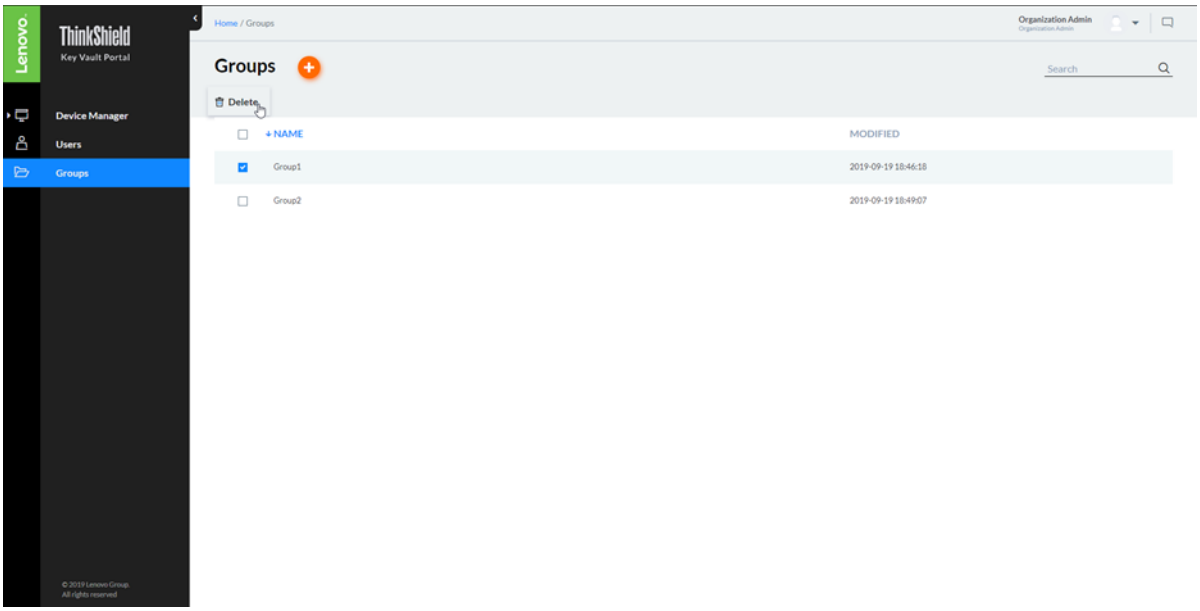


Click ‘X’ next to the Device that needs to be removed from the Group.

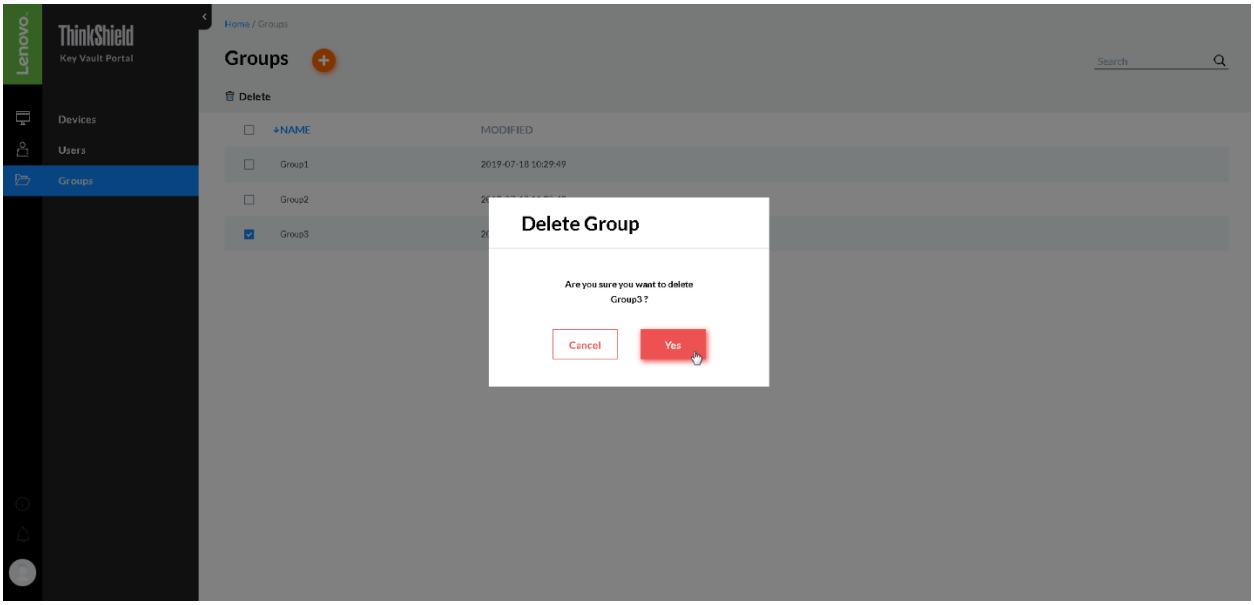


Delete a Group

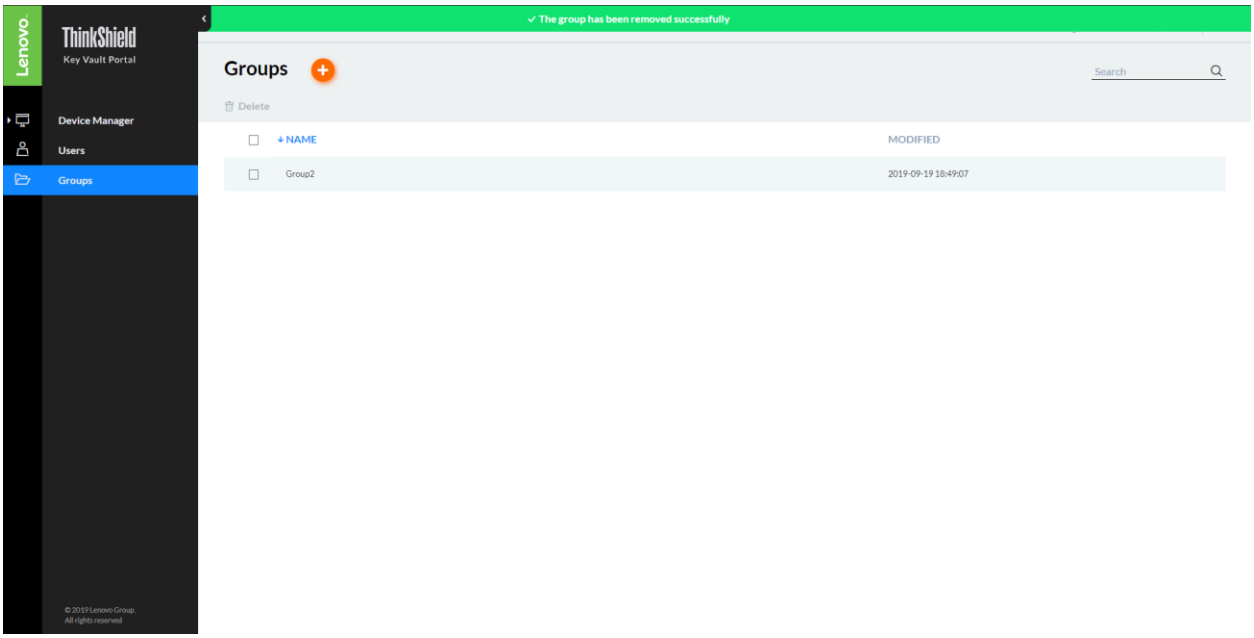
Check the Group(s) you want to delete from the Organization and click ‘Delete’.



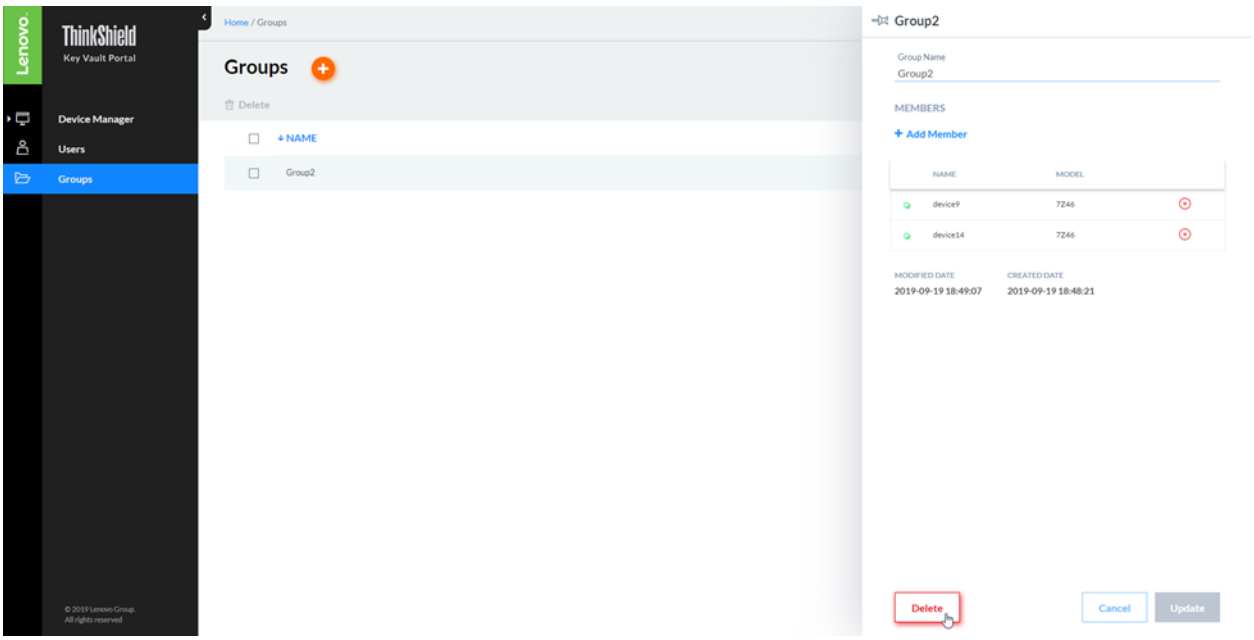
Click ‘Yes’ on ‘Are you sure…’ pop-up.



The Group is removed from the Organization

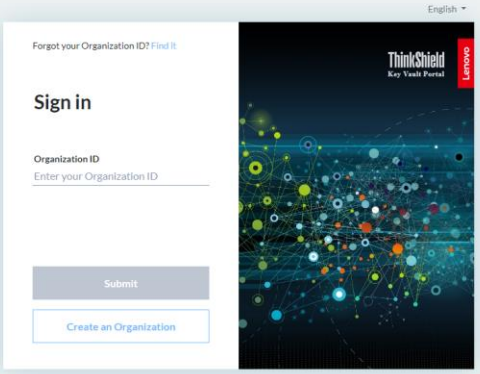


An alternative way to delete a group is to click ‘Delete‘ button on the Group Tray.

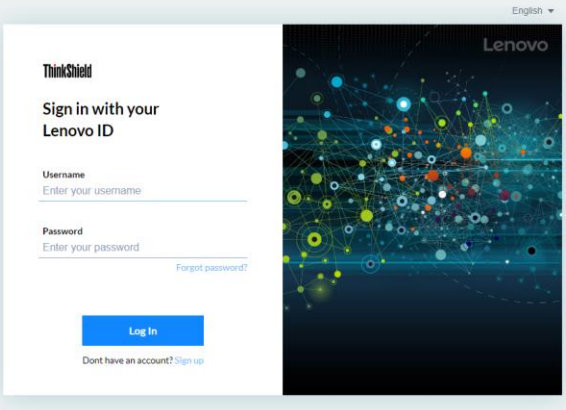


Create an Organization

To create a new organization go to https://portal.thinkshield.lenovo.com/ and select the “Create Organization”.



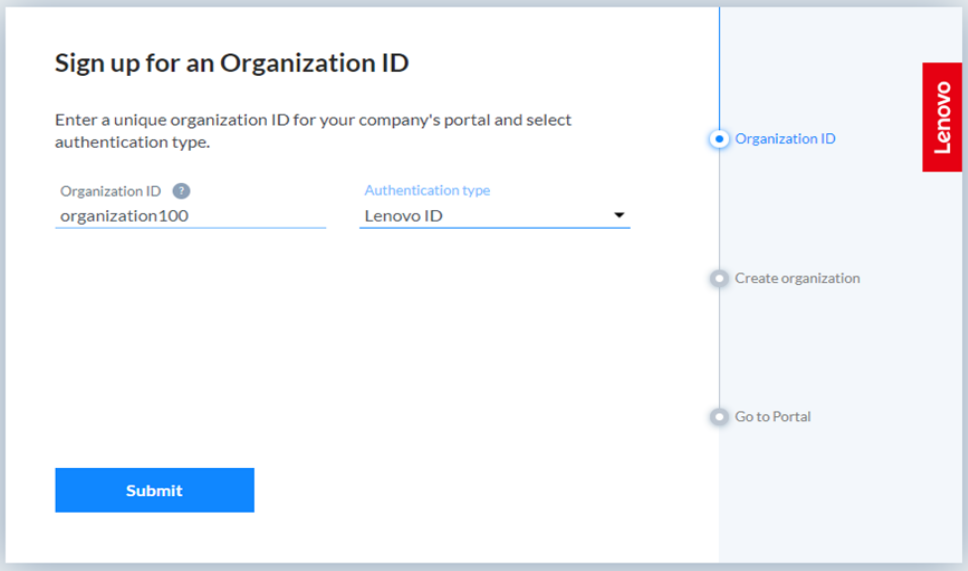
Log in using your Lenovo ID and password in ‘Username’ and ‘Password’ fields and click ‘Log In’ button. If you don’t have Lenovo ID click ‘Sign up’ next to ‘Don’t have an account’ and follow the instructions to create Lenovo account.



Lenovo ID Authentication

Provide a unique Organization ID and select the Lenovo ID authentication type.

Note: The Organization ID will be required for logging in.

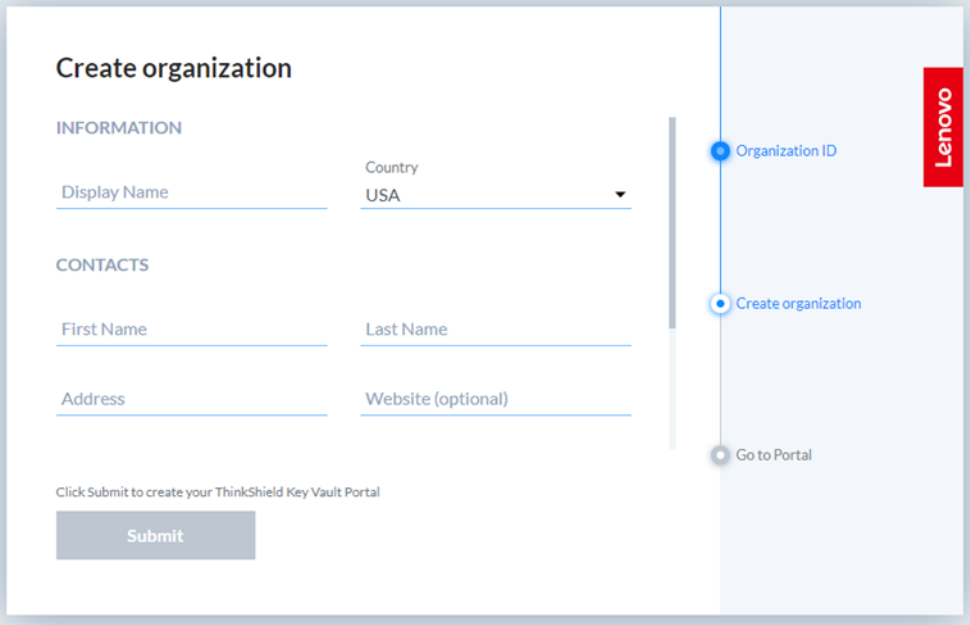


For ‘Lenovo ID’ authorization type provide the required information about your Organization. Required fields are:

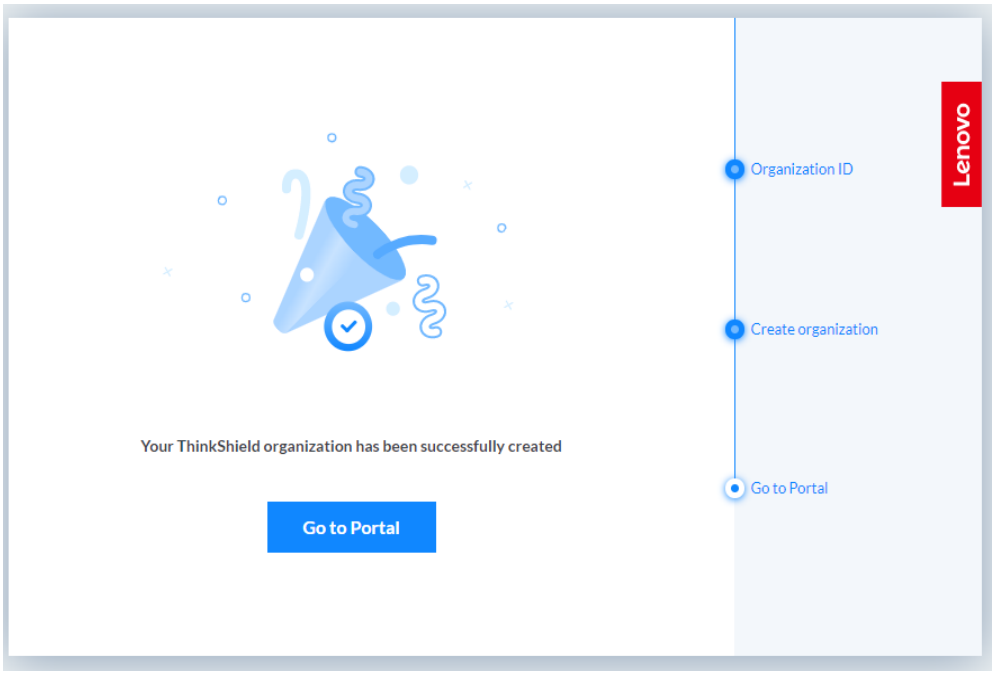
- Display Name
- Country
- First Name
- Last Name
- Address

Note: All other fields are optional.

Click ‘Submit’ after all the information is provided. The system will process your request and notify you as soon as the organization has been created.



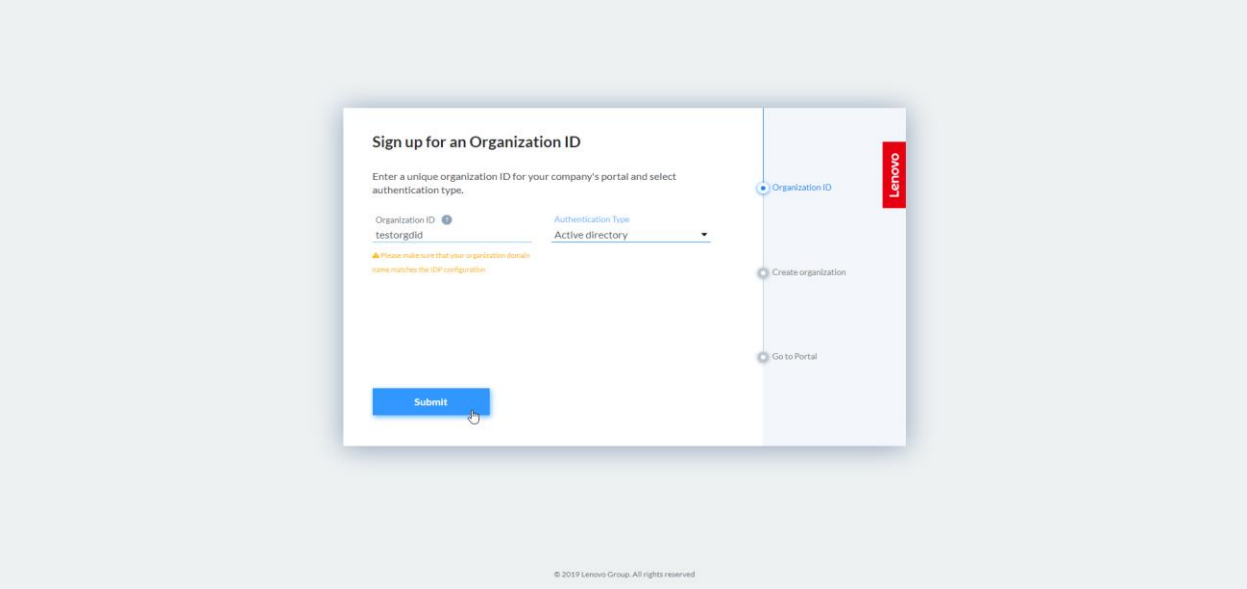
Click ‘Go to Portal’ to log in to your Organization. Provide your Organization ID, enter your Lenovo ID credentials and click ‘Log in’ to enter your organization.



Active Directory Authentication

Provide a unique Organization ID and select the Active Directory authentication type.

Note: Make sure that your Organization ID name matches the IDP configuration.



For ‘Active Directory’ authorization type provide the required information about your Organization. Required fields are:

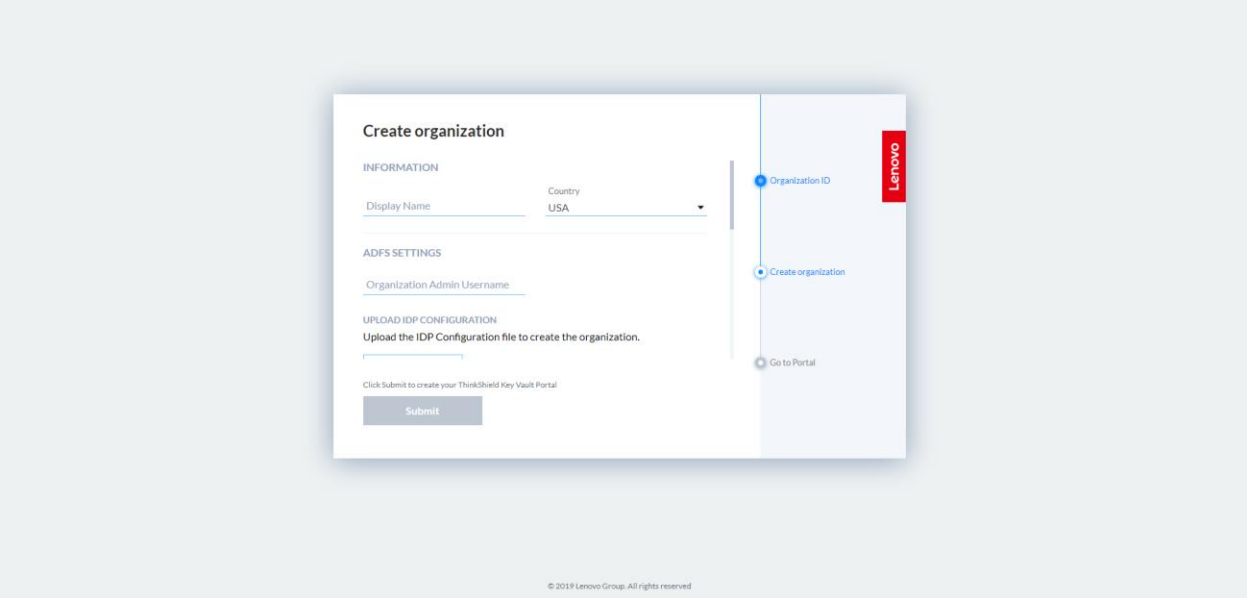
- Display Name
- Country
- First Name
- Last Name
- Address
- Organization Admin Username (Make sure your admin email matches the IDP configuration)

Note: All other fields are optional.

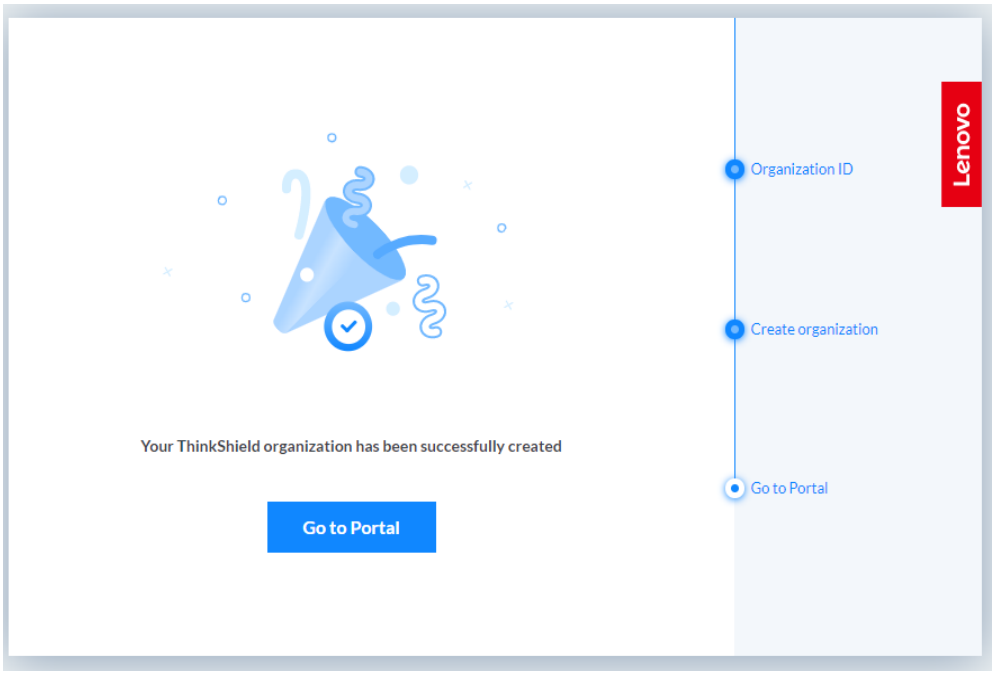
Required actions are:

- Upload IDP Configuration File (Obtain your IDP metadata from your service provider, ensure the metadata is in XML format).
- Download SAML Metadata (for upload to SAML server).

Click ‘Submit’ after all the information is provided. The system will process your request and send the Organization Admin Username specified an email verification to complete the organization creation.

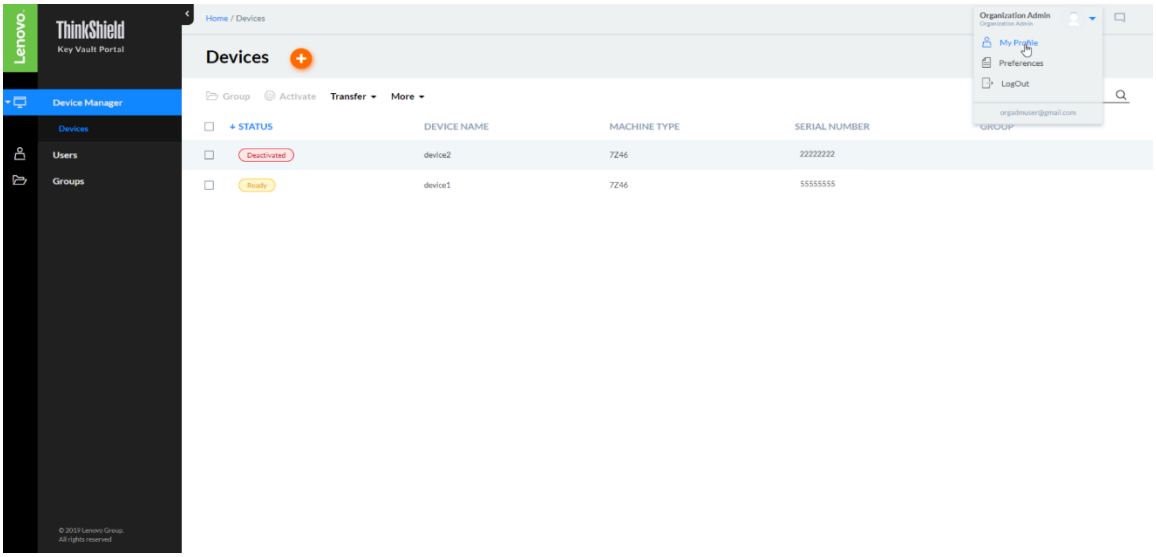


Click ‘Go to Portal’ to log in to your Organization. Provide your Organization ID, enter your Active Directory credentials and click ‘Log in’ to enter your organization.



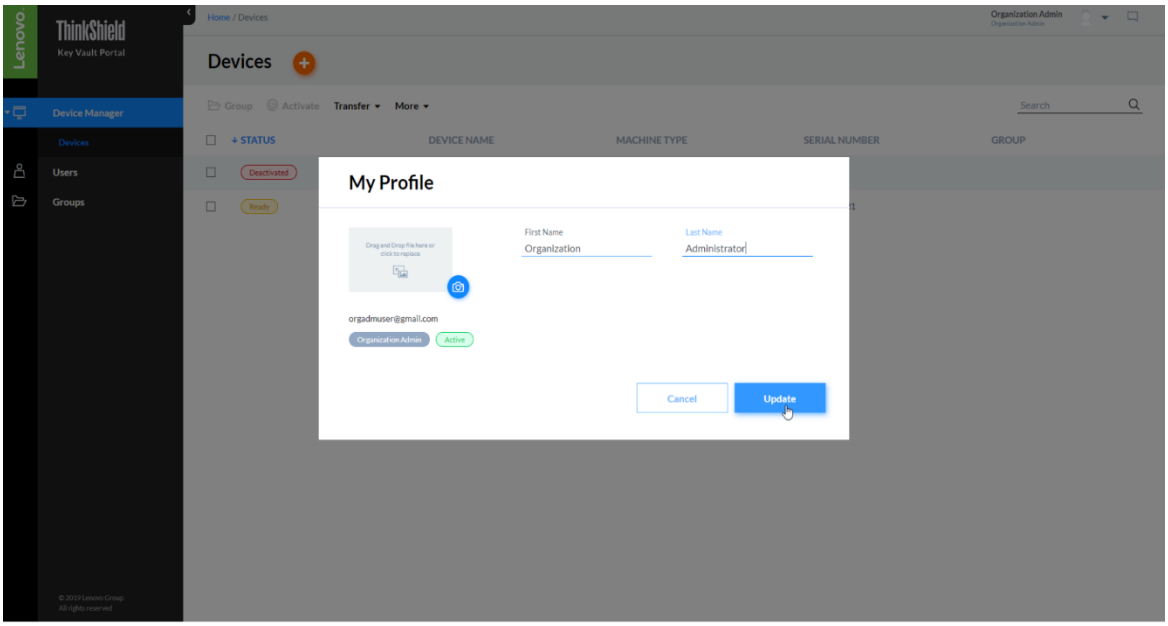
Edit My Profile

To edit profile information, click the ‘User’ icon in the right upper corner and select ‘My Profile’ from the drop-down.



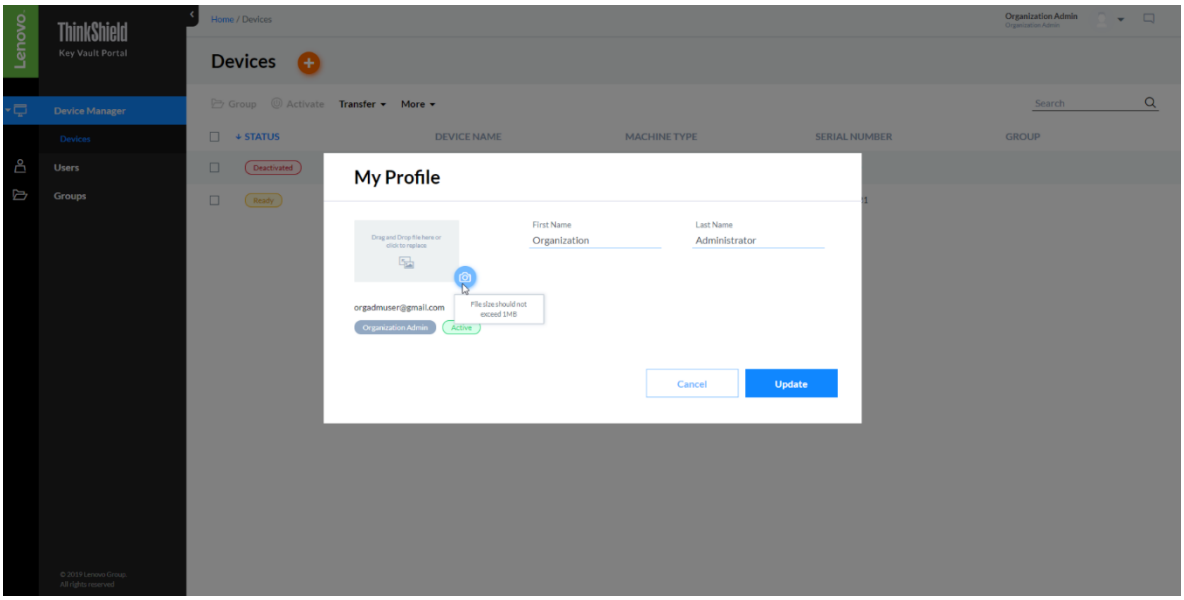
In ‘My Profile’ pop-up window, edit/update your profile information and click ‘Update’.

Note: The editable fields are ‘First Name’ and ‘Last Name’.



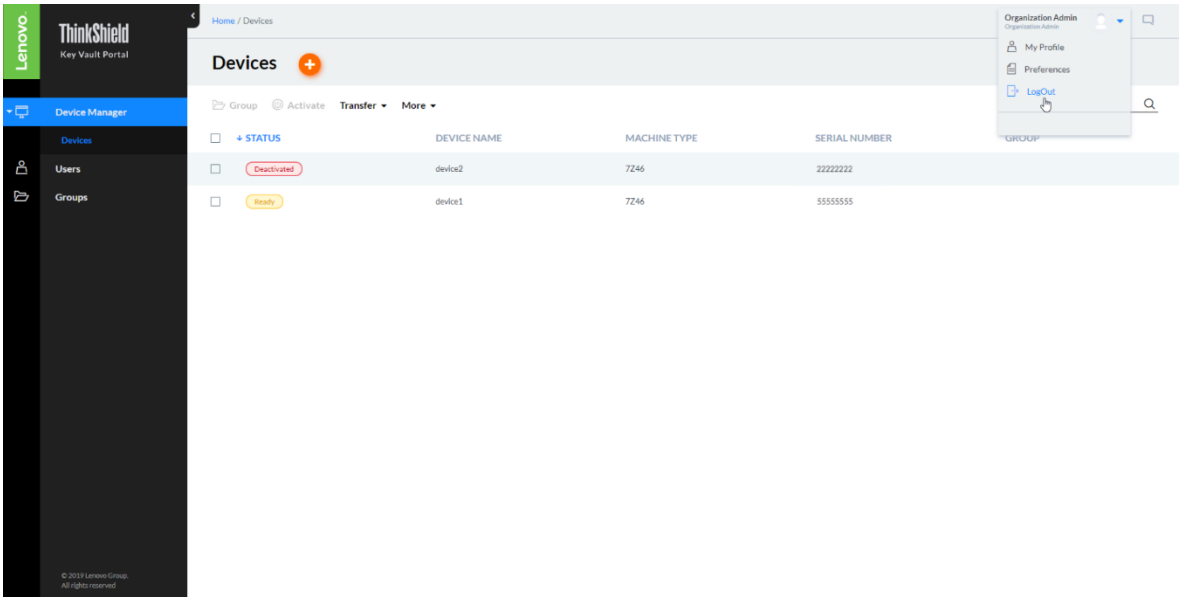
In order to upload/update a profile picture, click the ‘Photo’ icon, upload an image from your computer and click ‘Update’.

Note: An image size should not exceed 1 Mb.

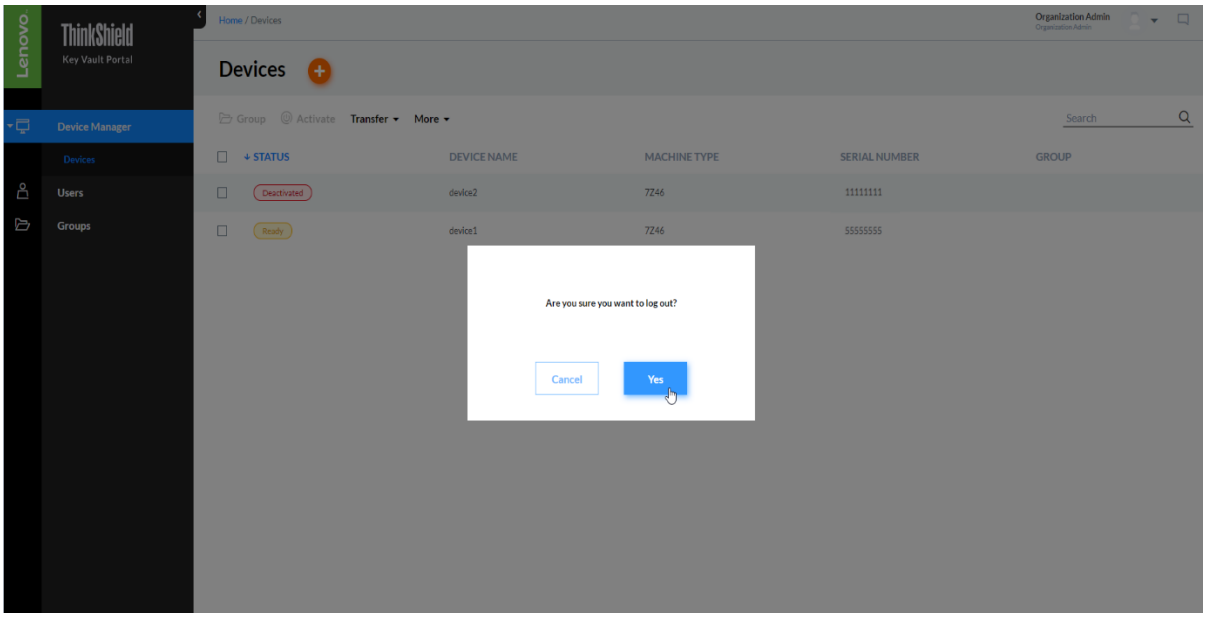


Logout

In order to log out from the profile, click the ‘User’ icon in the right upper corner and select ‘Log Out’ in the drop-down.

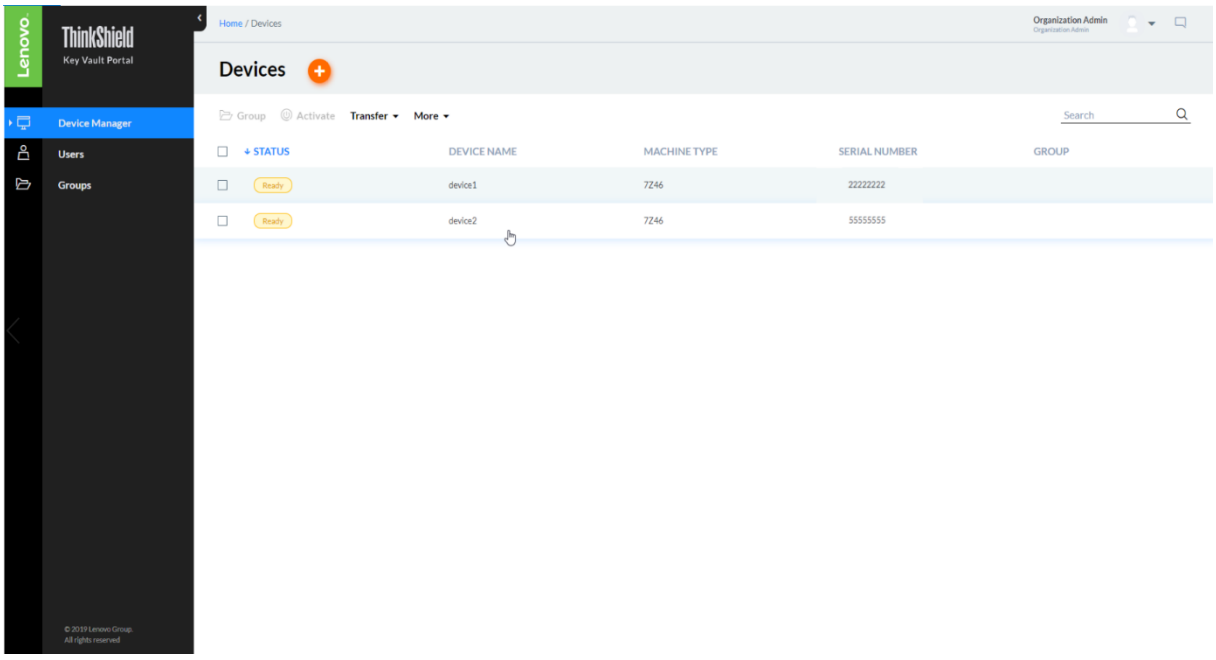


Confirm the action by clicking ‘Yes’ in the pop-up window.

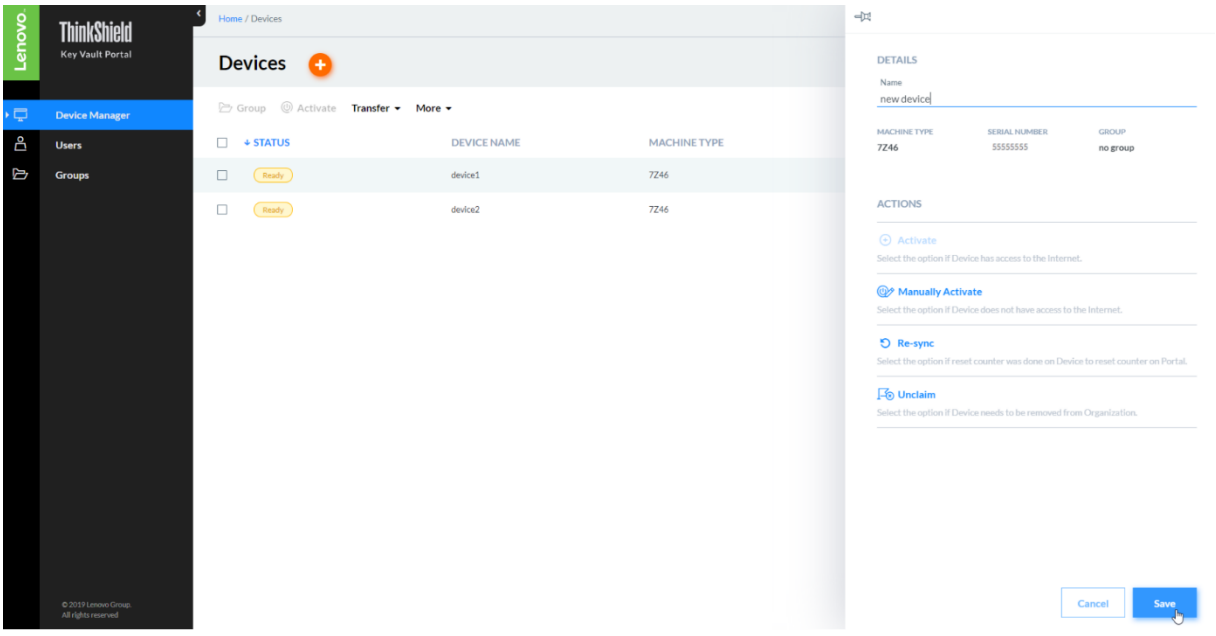


Edit Device Name

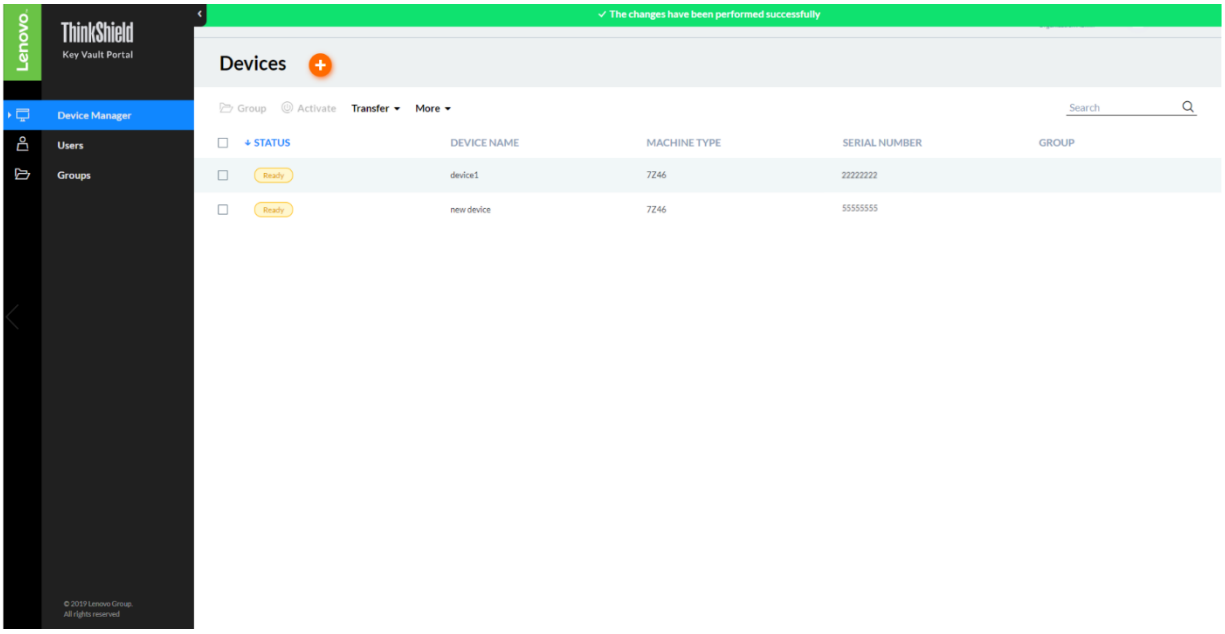
Select the Device you want to edit by clicking on it.



Update/edit a Device name on the device tray and click ‘Save’.



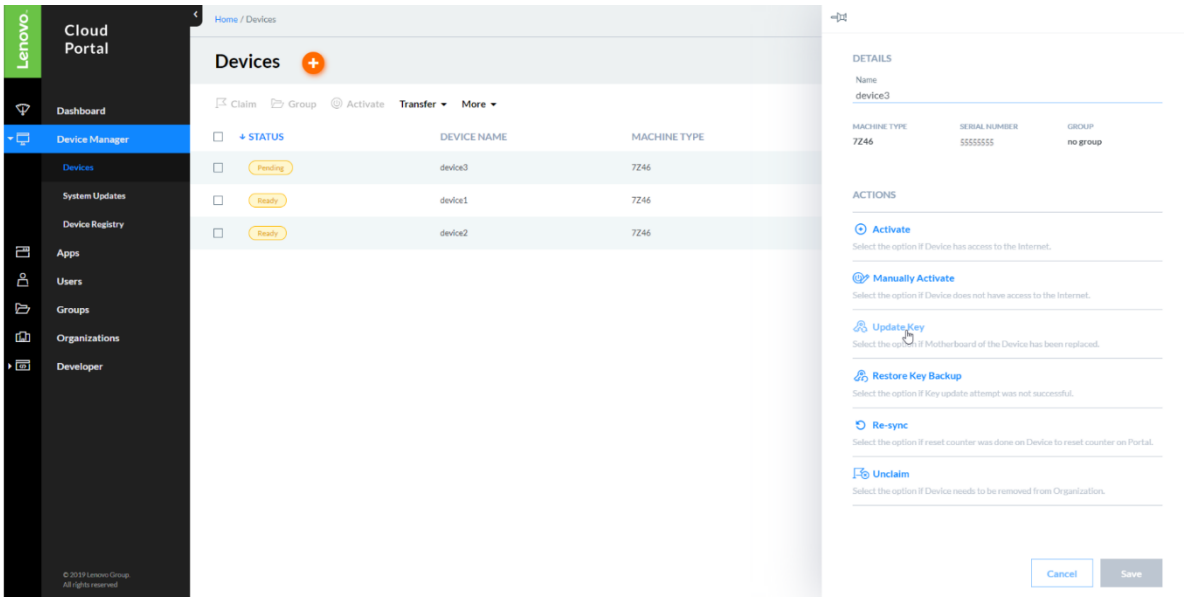
A Device name is successfully updated.



Update Device Key

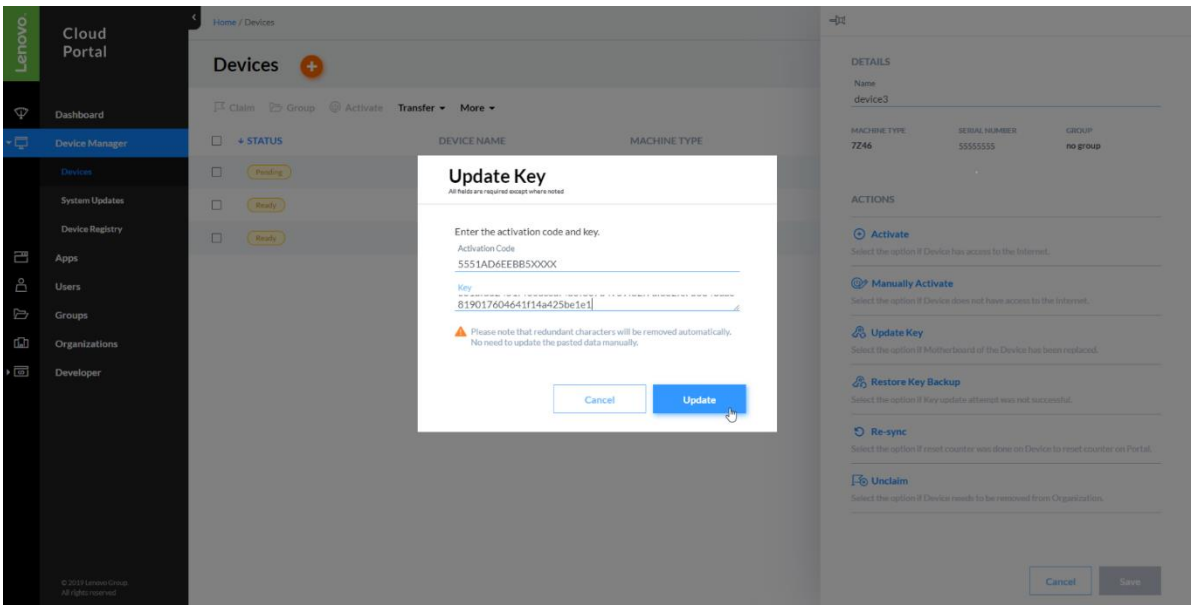
Update public key option is to facilitate exchange of a motherboard on failure when a new public / private key information is needed for an existing Machine Type and Serial Number.

Click the Device you want to update a key for to open a device tray. Select ‘Update Key’ on the device tray.

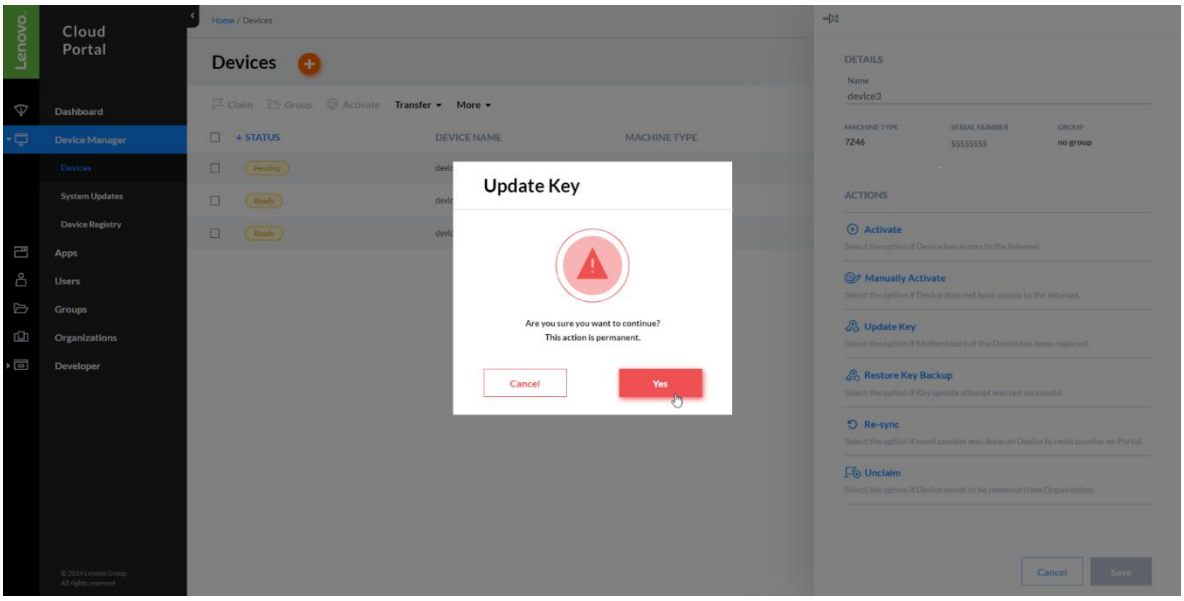


Provide Activation Code and old Public Key and click ‘Update’.

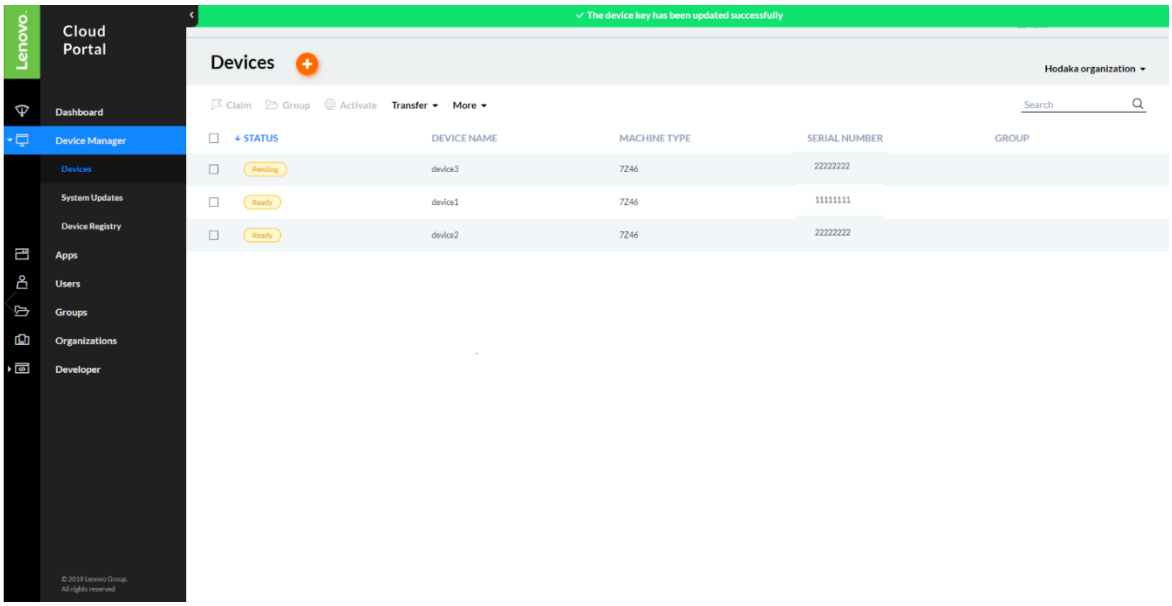
Note: Old Public Key is displayed in the ThinkShield Mobile Application. (This option is available for Maintenance User)



Confirm action by clicking ‘Yes’ in ‘Update Key’ pop-up window.

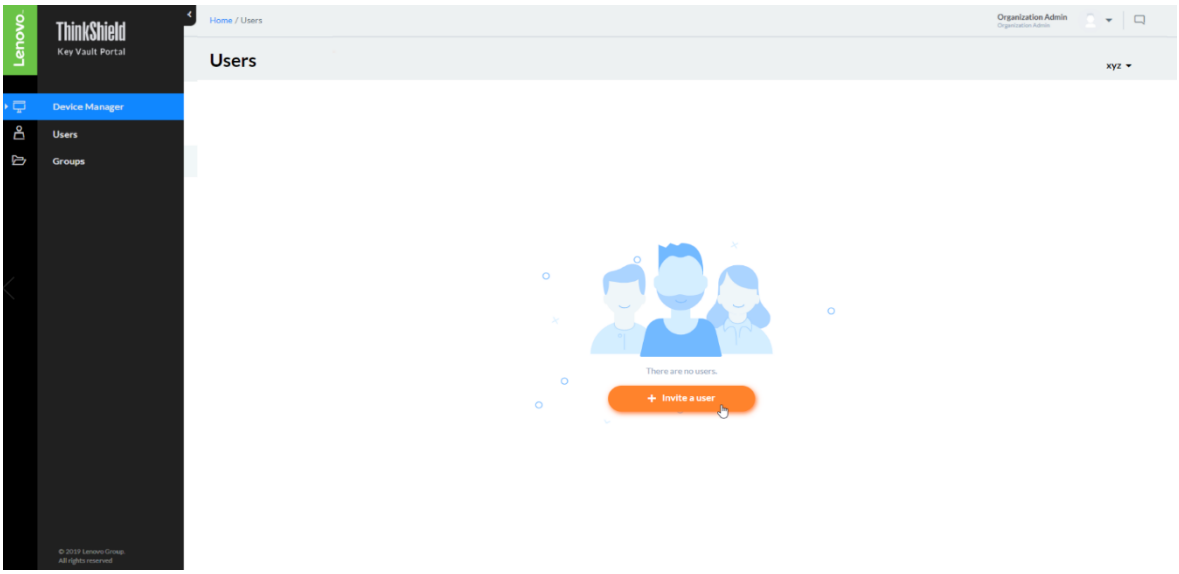


A public key is successfully updated.

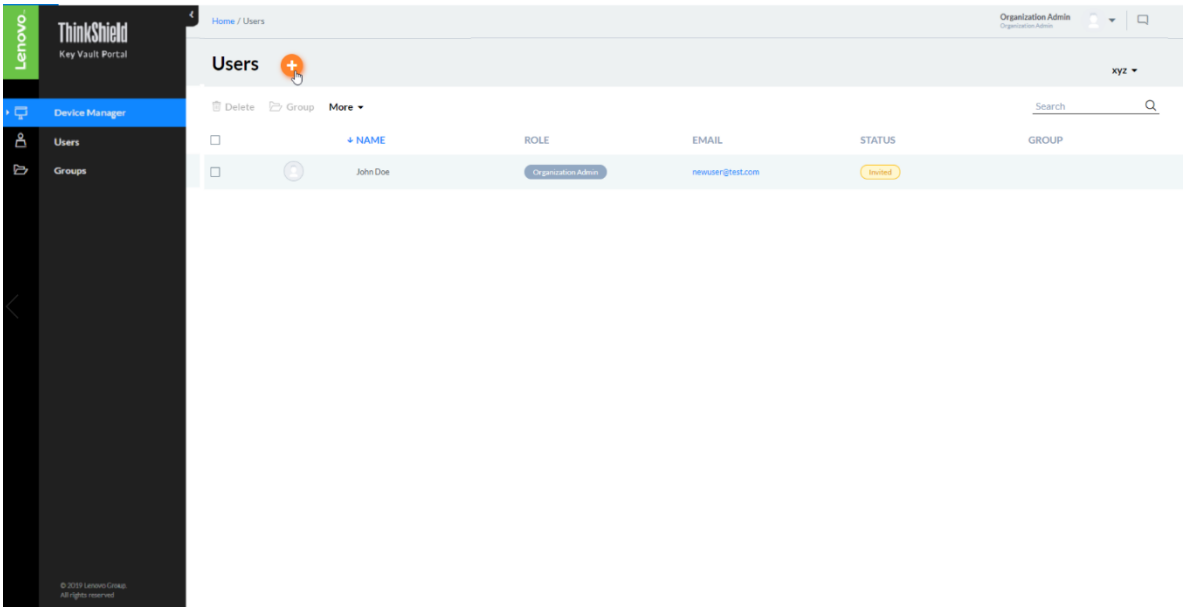


Invite a User

In order to invite a User to the Organization go to ‘Users’ page and click ‘Invite a User’.

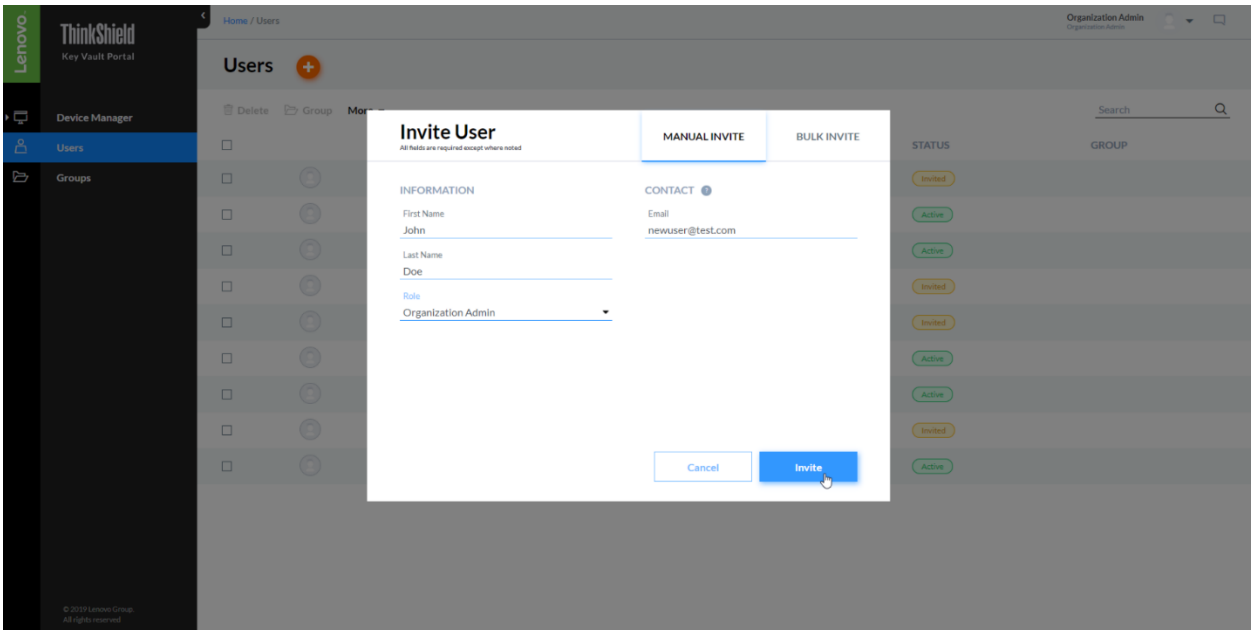


If there are users in the Organization click ‘+’ icon at the top of the page in order to invite a new User.



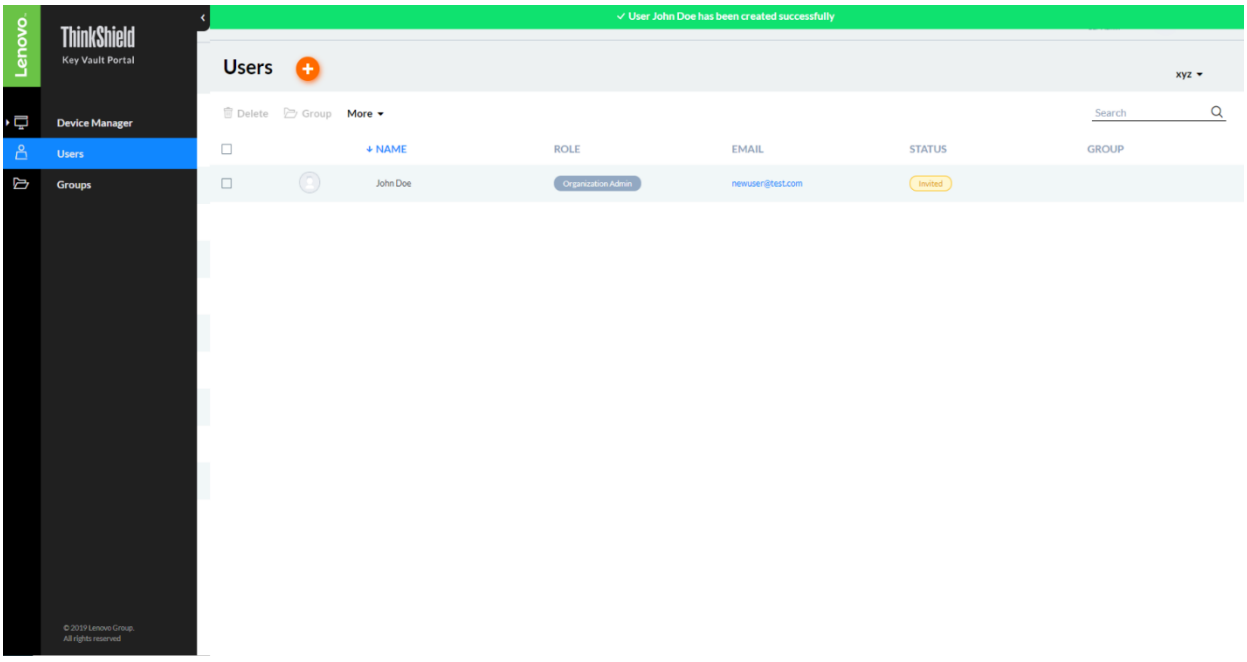
Select ‘Manual Invite’ tab on ‘Invite User’ pop-up window. Provide First Name, Last Name, Email Address, select a user role and click ‘Invite’.

Note: Please make sure that the email address provided is correct. An email with an invitation will be sent to the email address provided.



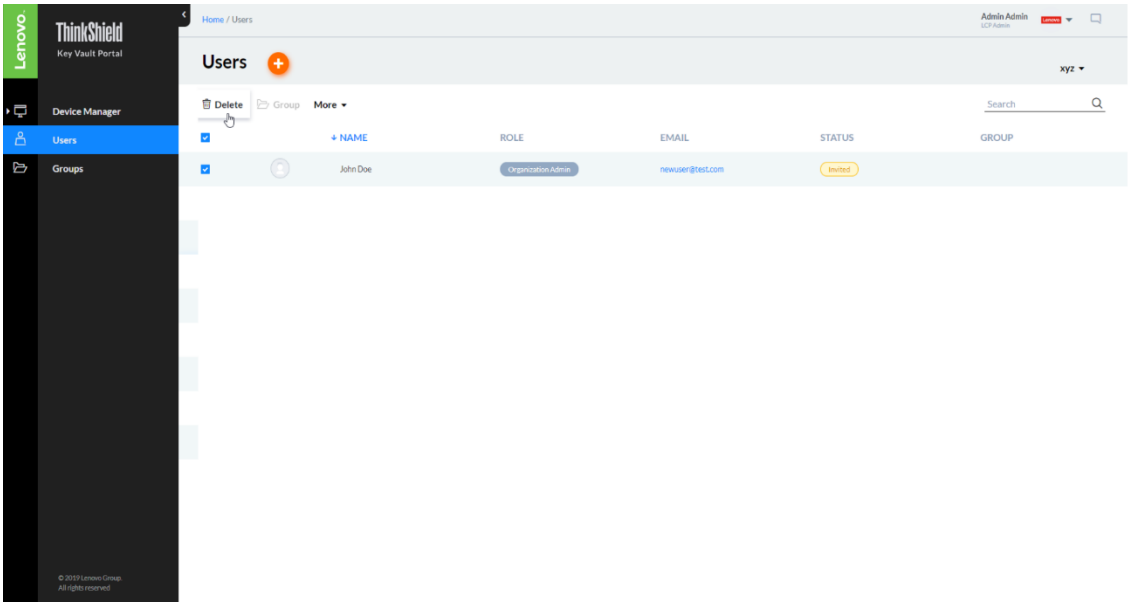
A user is successfully invited to the Organization.

Note: All the invited users have ‘Invited’ status. As soon as a user accepts an invitation sent to their email address their status will change to ‘Active’.

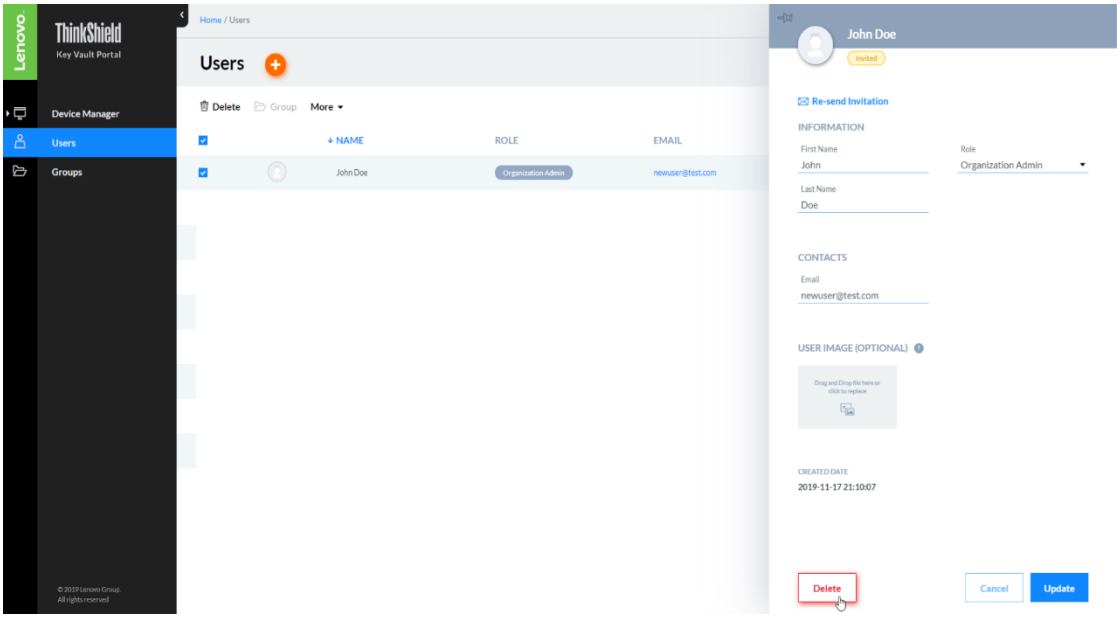


Remove a User

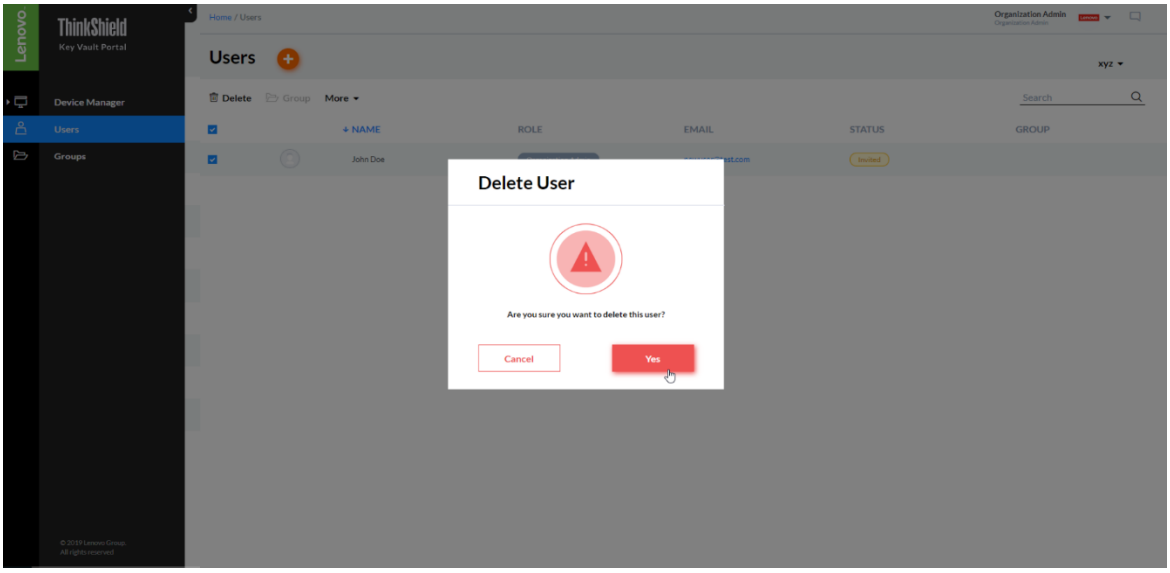
Check a User you want to remove from the Organization and click ‘Delete’ at the top of the page.

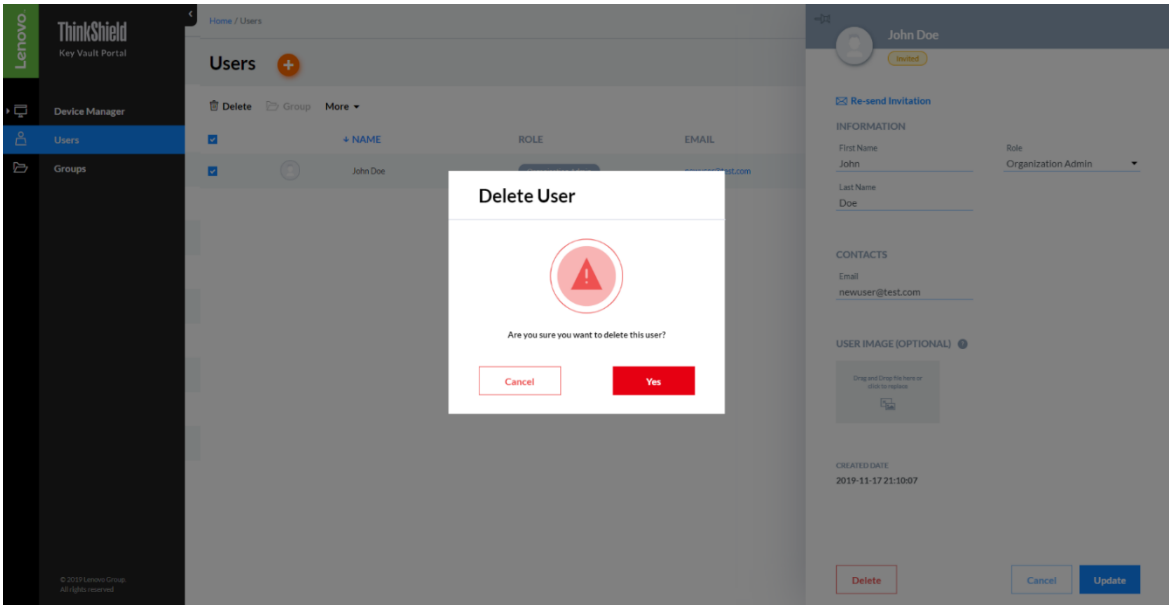


An alternative way to remove a User is to open a User tray by clicking on a User you want to remove and click ‘Delete’ at the bottom of the tray.

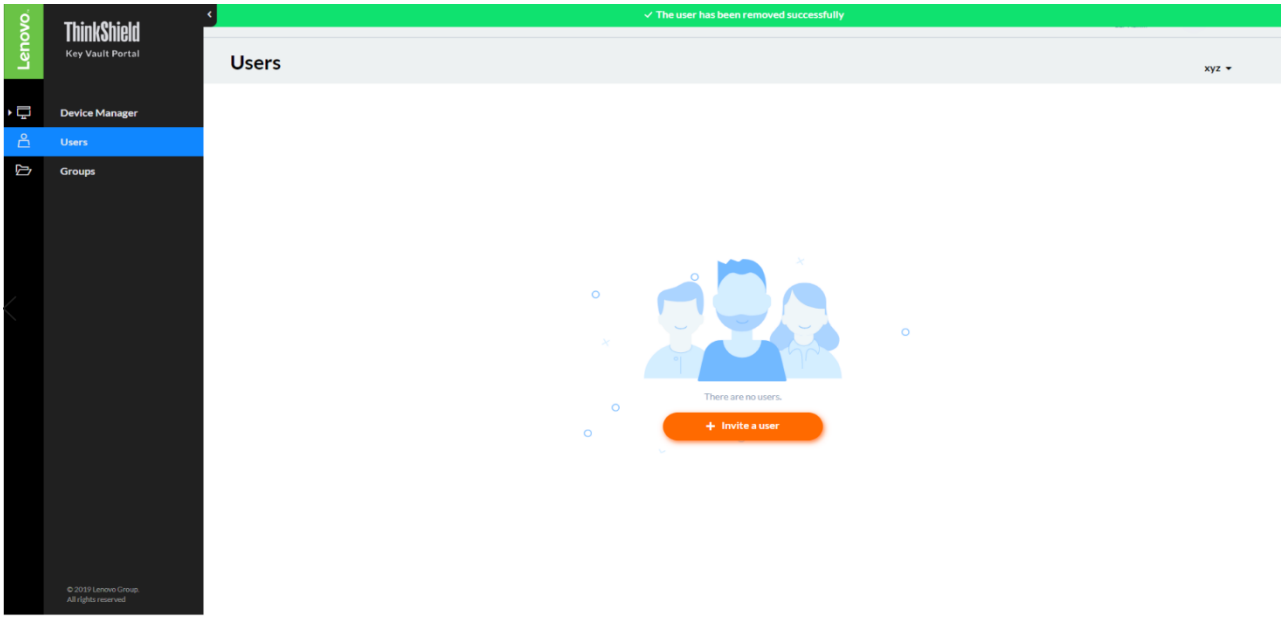


Confirm the action by clicking ‘Yes’ on the pop-up window.





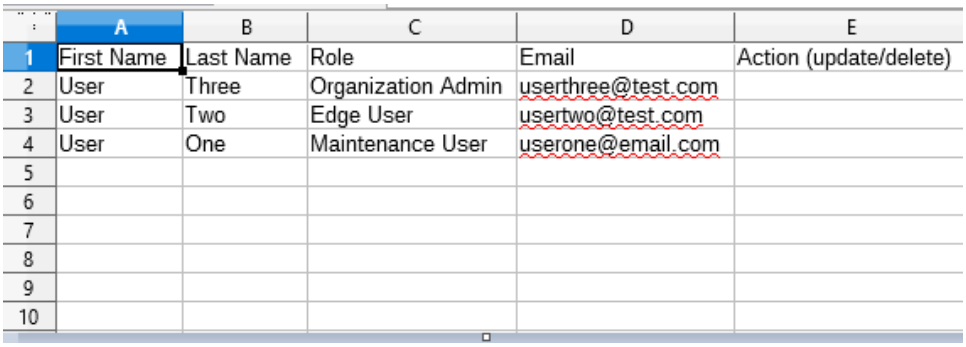
A User is successfully removed from the Organization.



Import Users

'Import' option allows to upload updated/edited Users information.

To edit a user list open a .CSV file downloaded while exporting.



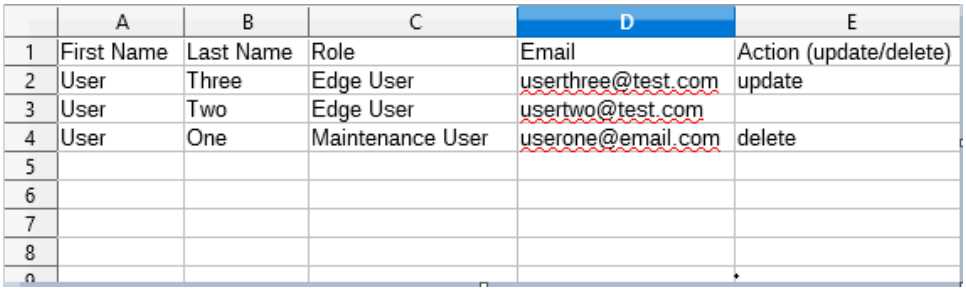
	A	B	C	D	E
1	First Name	Last Name	Role	Email	Action (update/delete)
2	User	Three	Organization Admin	userthree@test.com	
3	User	Two	Edge User	usertwo@test.com	
4	User	One	Maintenance User	userone@email.com	
5					
6					
7					
8					
9					
10					

Make necessary changes to the list and save the file.

Note: Available actions are update user's information or delete a user from the list.

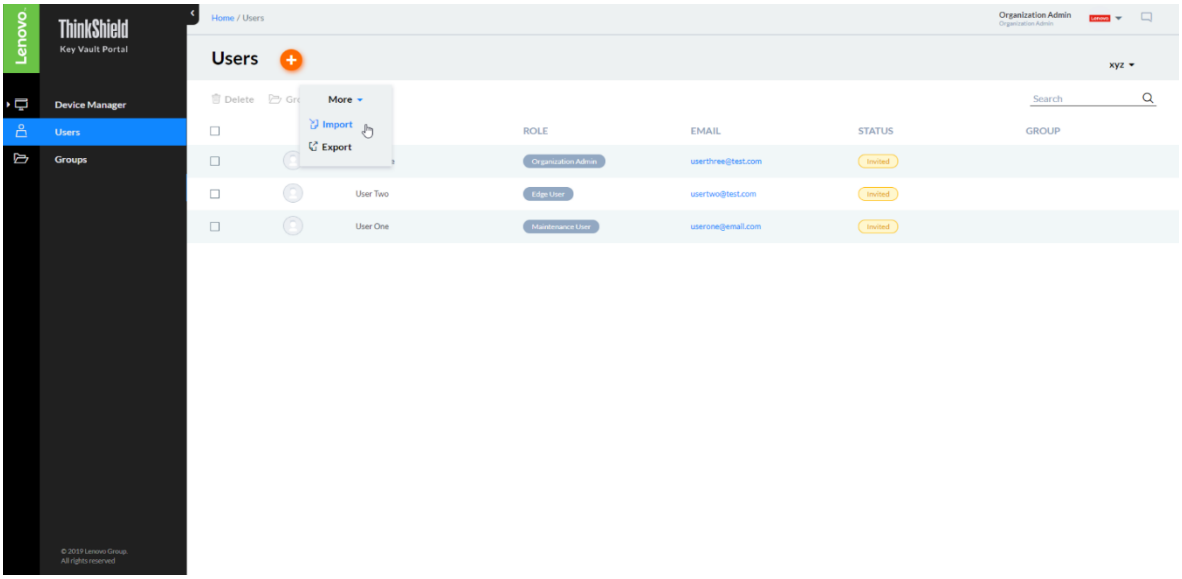
Put 'update' next to a User whose information you want to update. Editable fields are First Name, Last Name and Role.

Put 'delete' next to a User you want to remove from the Organization.

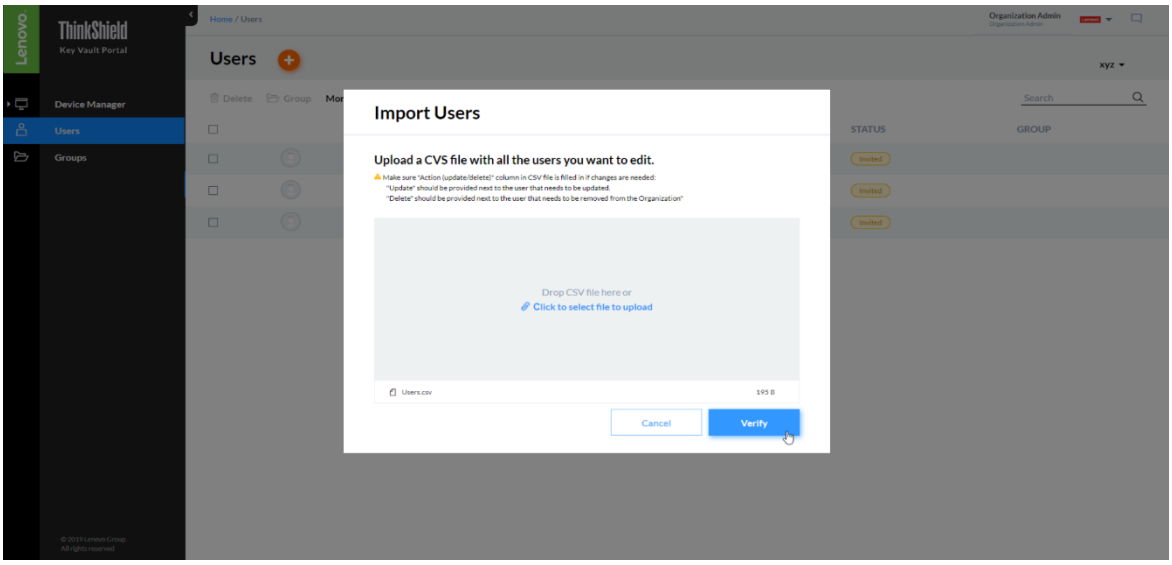


	A	B	C	D	E
1	First Name	Last Name	Role	Email	Action (update/delete)
2	User	Three	Edge User	userthree@test.com	update
3	User	Two	Edge User	usertwo@test.com	
4	User	One	Maintenance User	userone@email.com	delete
5					
6					
7					
8					

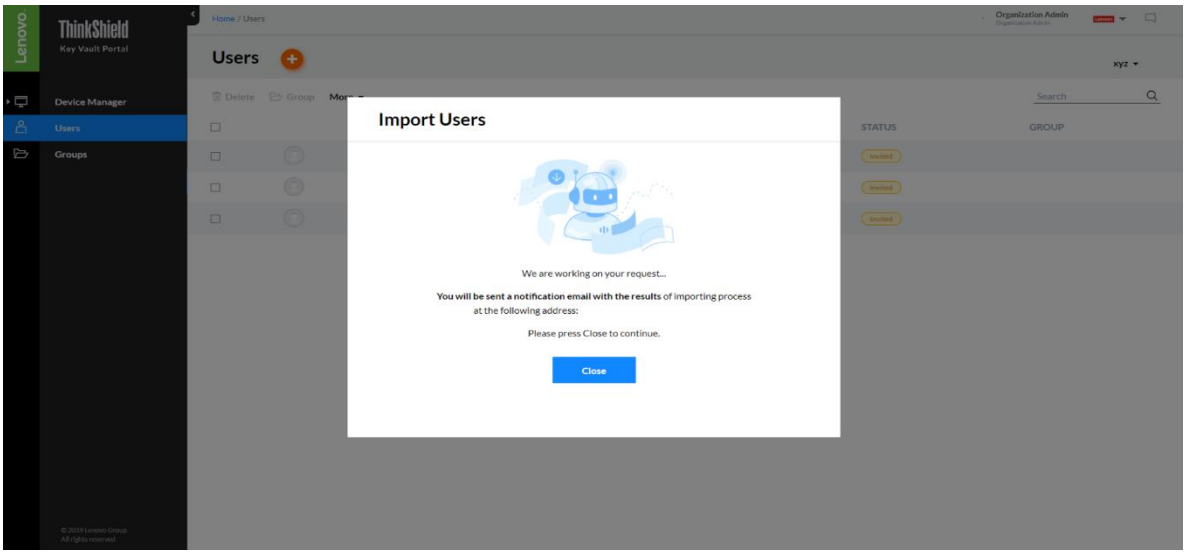
To start importing process click ‘Import’ in ‘More’ drop-down at the top of the page.



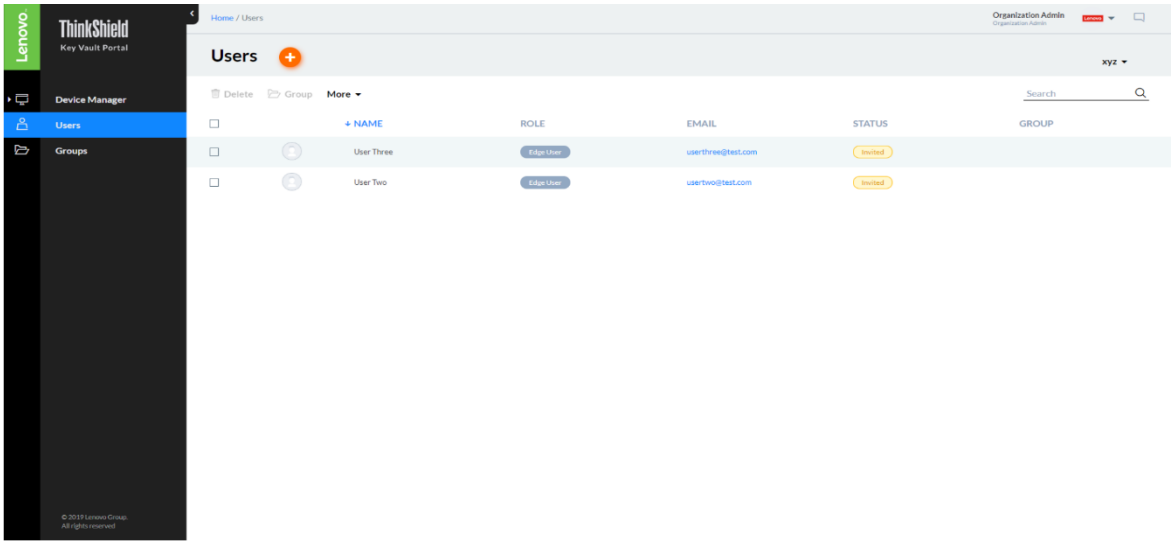
Upload a .CSV file to the Portal. Click ‘Verify‘ after the file has been uploaded.



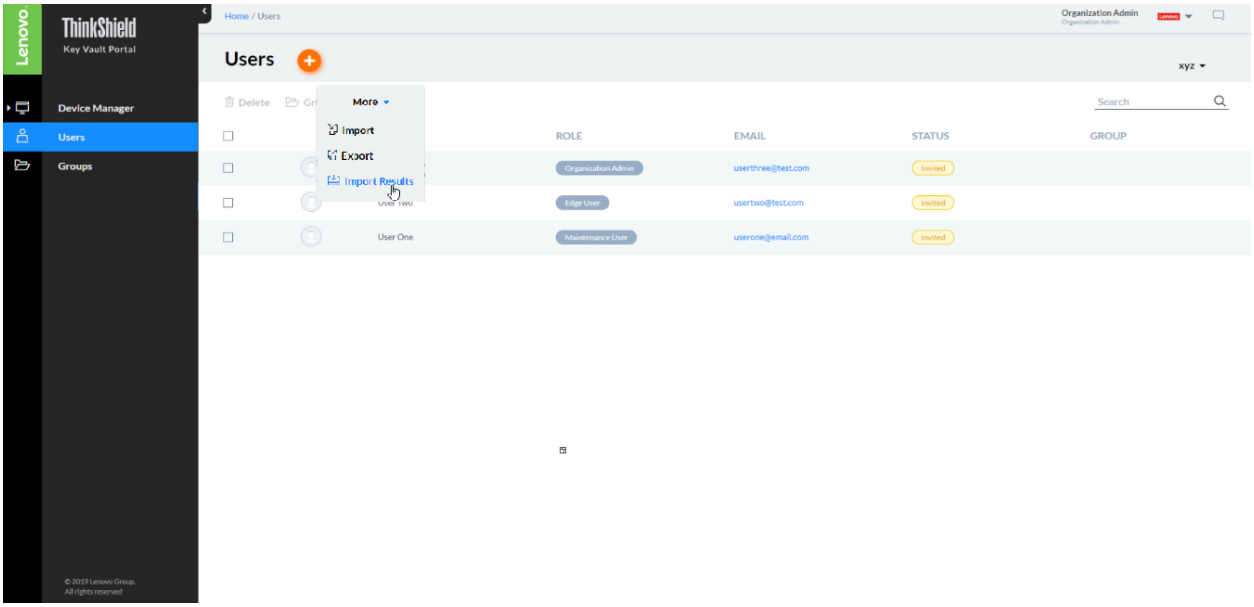
As soon as the verification process is over you will get a confirmation email to the email address associated with your profile.



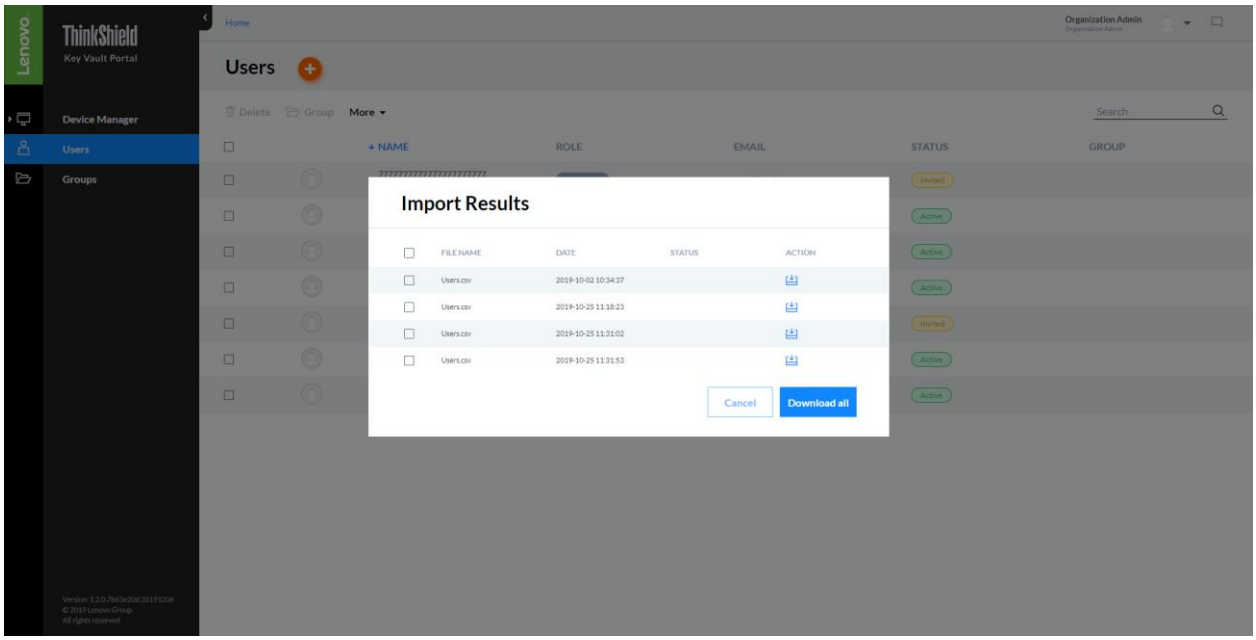
The User list is updated.



To see the detailed import results, click ‘Import Results in ‘More’ drop-down.

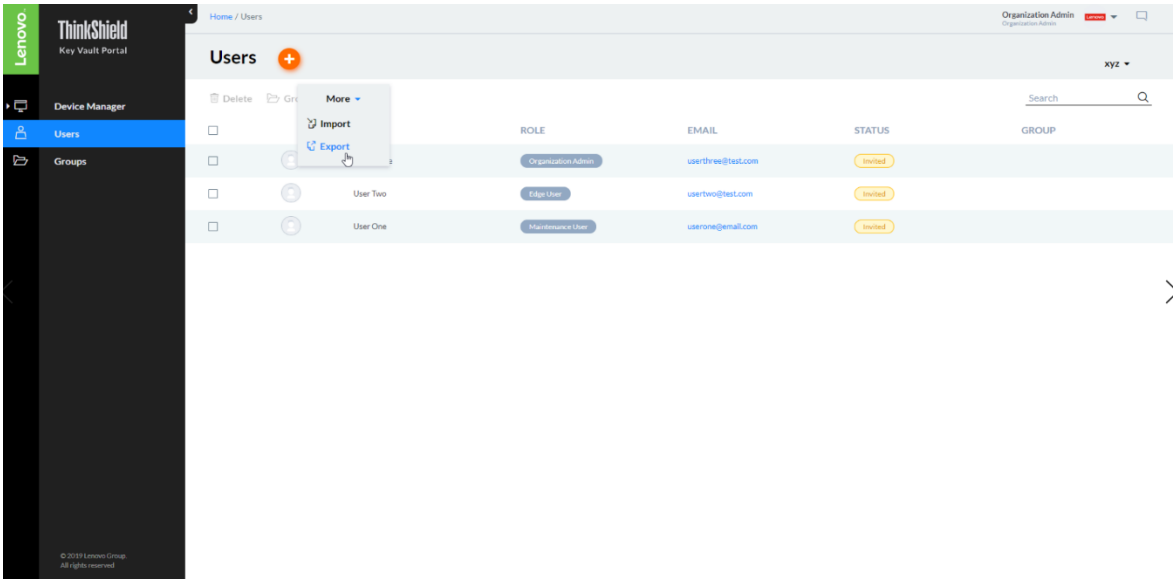


Select the file you want to view and click ‘Download’ icon in ‘Action’ section next to that file.

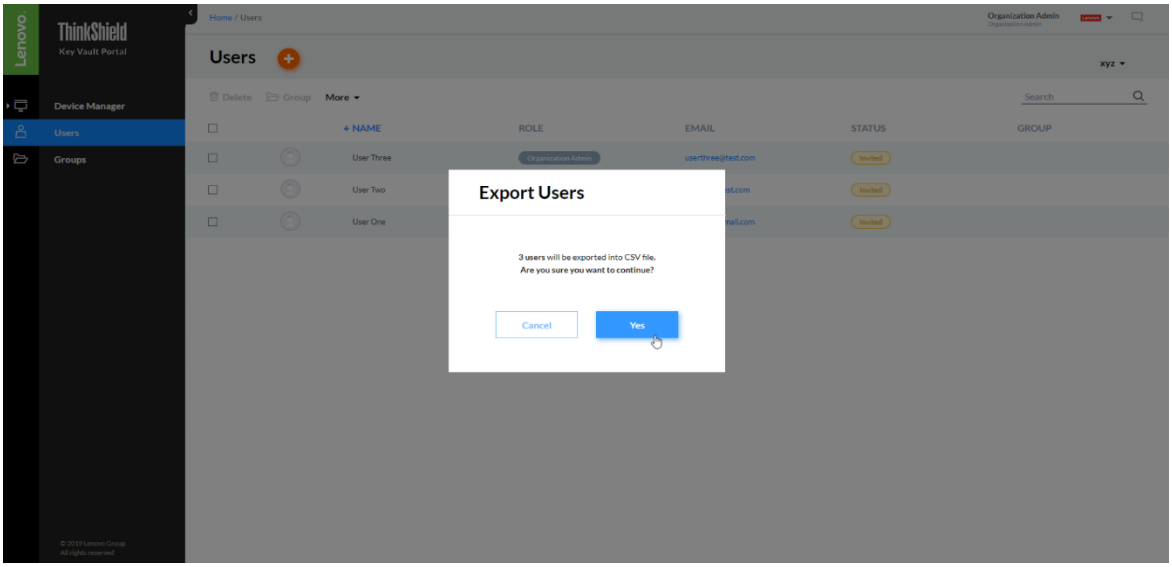


Export Users

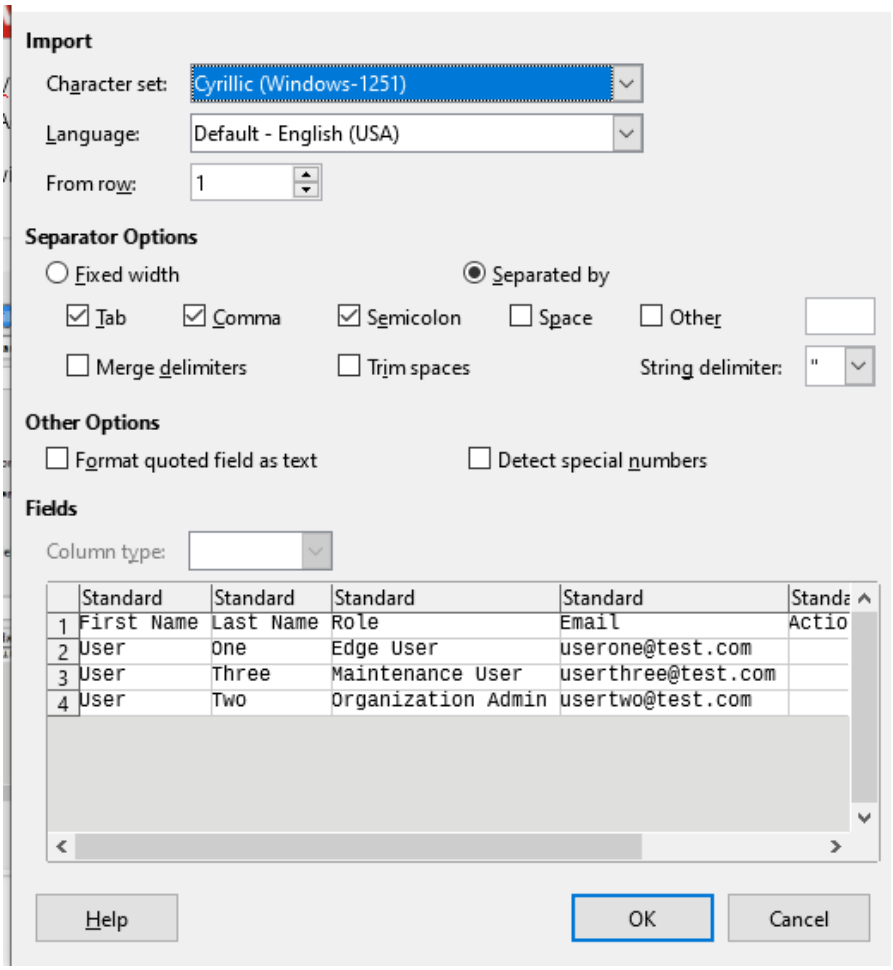
'Export' option allows to download a file with the list of all the Users and their profile information. To export a list of Users, click 'Export' in 'More' drop-down at the top of the 'Users' page.



Confirm the action by clicking 'Yes' on 'Export Users' pop-up window.



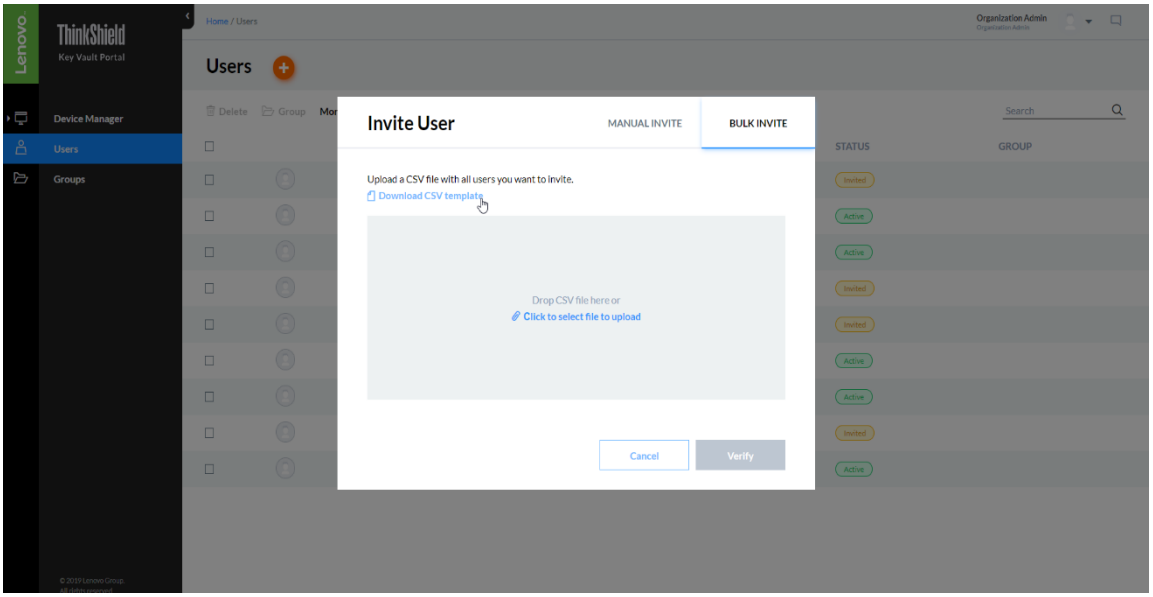
A .CSV file with a list of Users is downloaded to your computer.



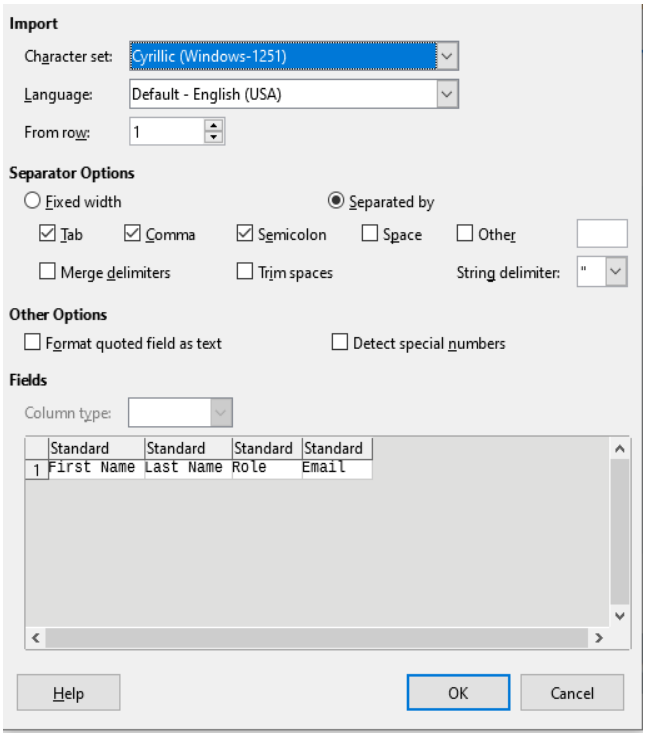
Bulk Invite Users

'Bulk Invite' allows to invite up to 1000 Users at a time.

Select 'Bulk Invite' tab on 'Invite User' pop-up window and download .CSV template.

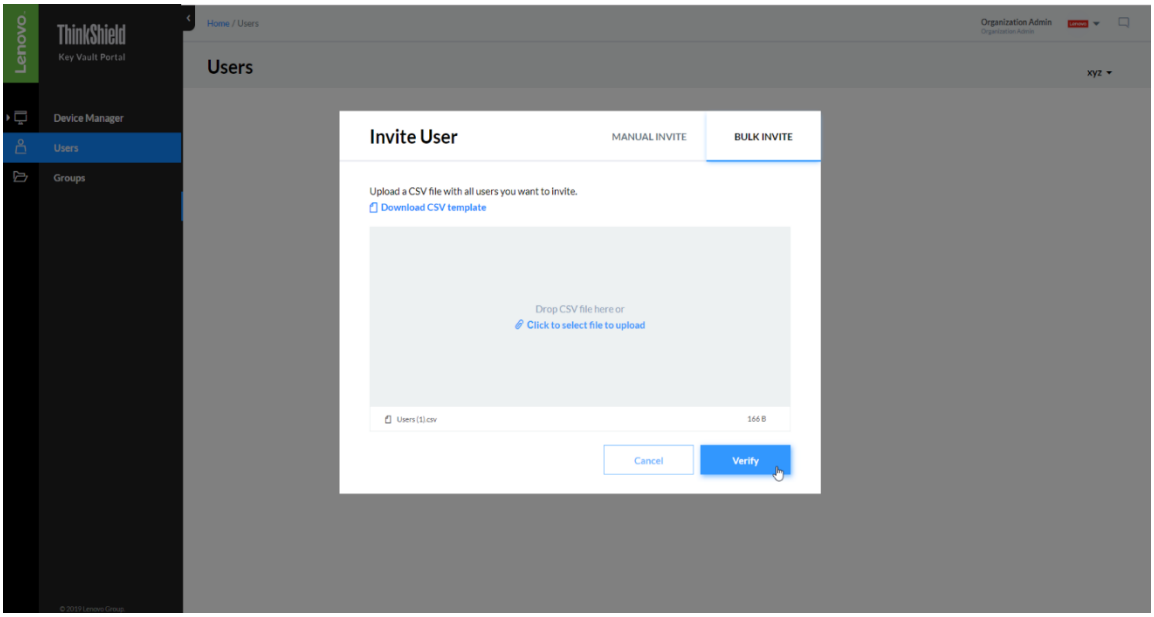


Fill in all the required data and save the file. The required fields are: First Name, Last Name, Role and Email Address.

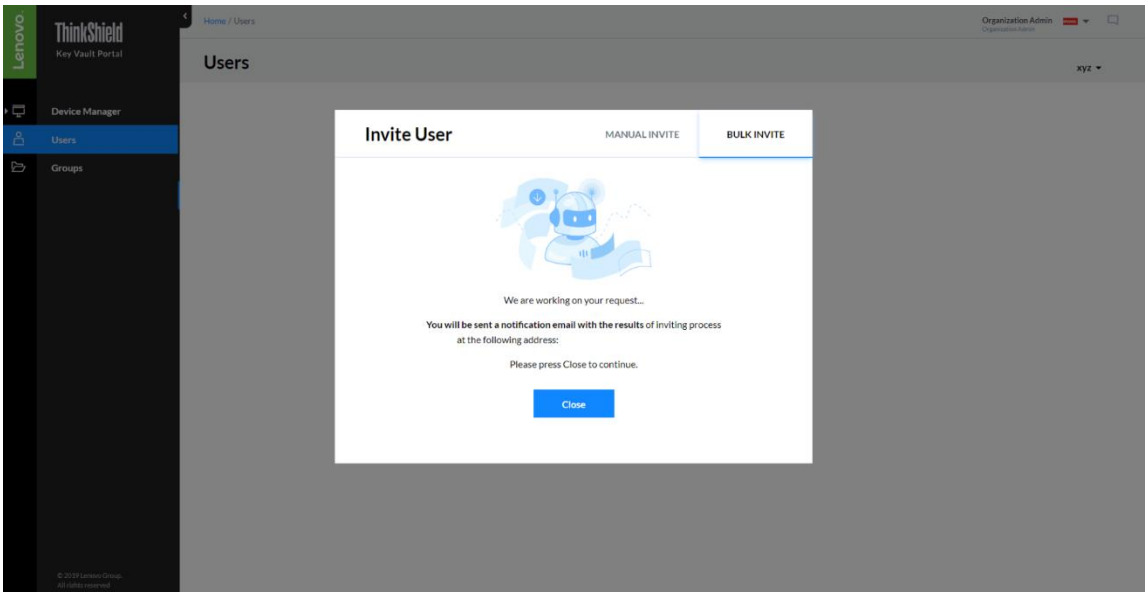


	A	B	C	D
1	First Name	Last Name	Role	Email
2	User	One	Edge User	userone@test.com
3	User	Two	Organization Admin	usertwo@test.com
4	User	Three	Maintenance User	userthree@test.com
5				
6				
7				
8				
9				

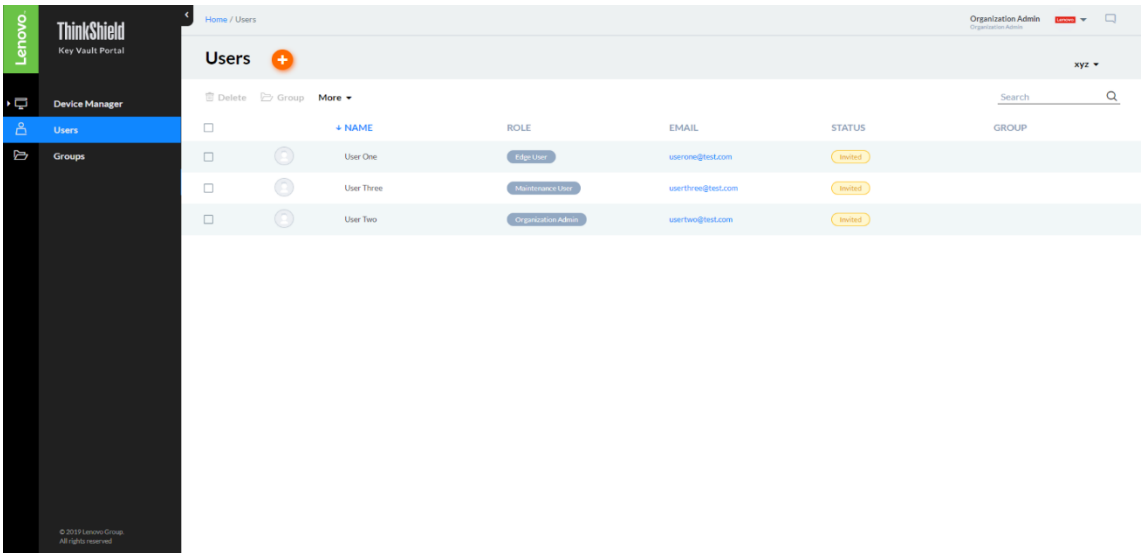
Upload a CSV file to the Portal. Click ‘Verify‘ after the file has been uploaded.



As soon as the verification process is over you will get a confirmation email to the email address associated with your profile.



In case of successful upload, the Users start displaying in the User list. The status of the Users is ‘Invited’.

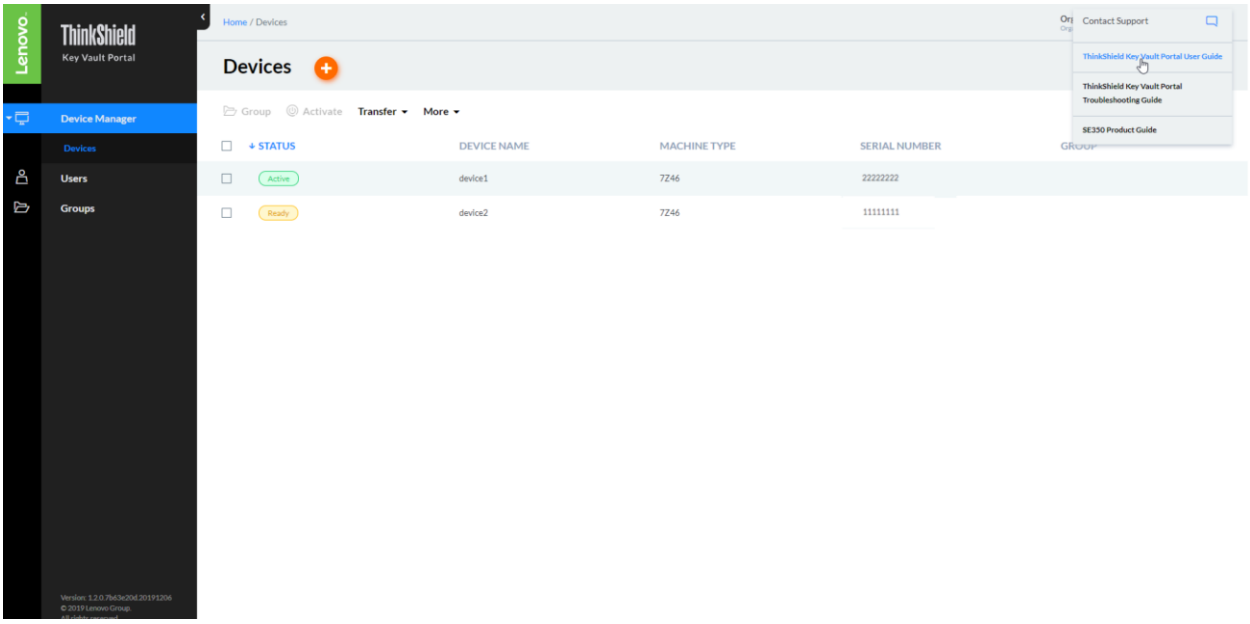
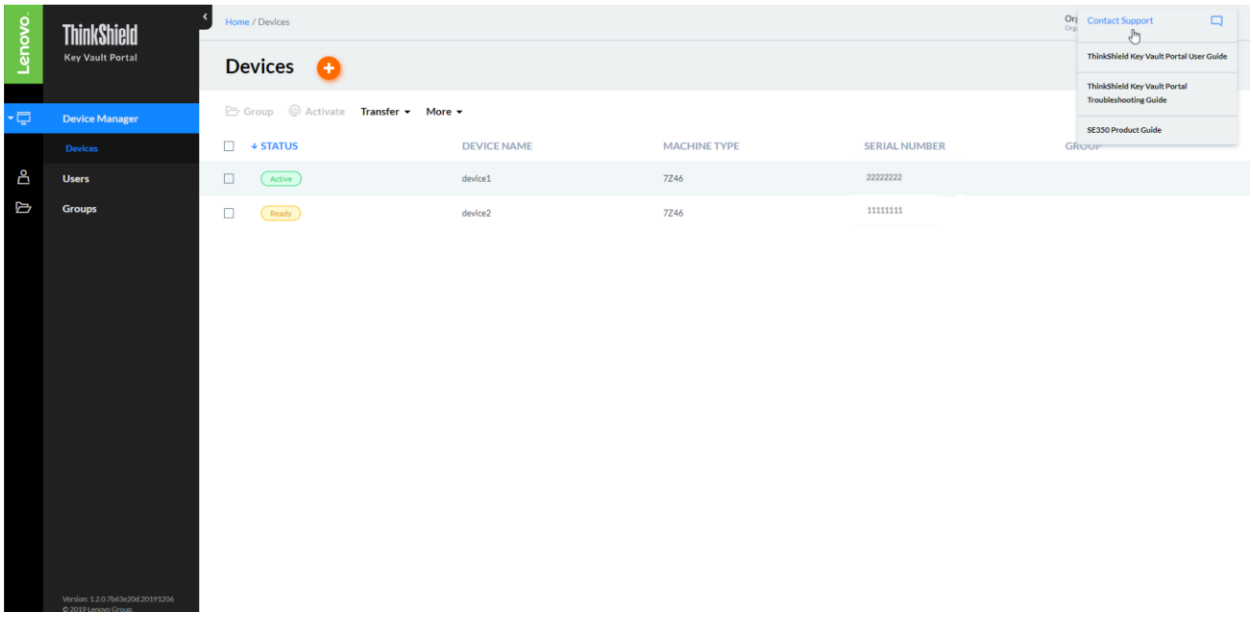


Help/ Contact Support

Click ‘Help’ button at the top right corner of the screen. Select the document from the drop-down window and click on it. The document selected will be opened in a new tab.

The documents available are:

- ThinkShield Key Vault User Guide
- ThinkShield Key Vault Portal Troubleshooting Guide
- SE350 Product Guide



To contact our Customer Support click ‘Contact Support’ in ‘Help’ drop-down or contact us directly at thinkshield@lenovo.com.