Reseller Portal Administrator Guide

CTERA Portal

November 2015
Version 5.0

Tip

For legal information and for the end user license agreement, refer to Legal Information in this guide.

Contents

1

About the CTERA Portal

CTERA Portal is a scalable cloud service delivery platform that you use to create, deliver and manage cloud storage applications, including file sharing and sync, backup, and mobile collaboration. CTERA Portal is hosted by CTERA in the cloud, and enables you to offer managed cloud services with no upfront investment in infrastructure and without requiring installation.

CTERA Portal enables you to extend cloud services to remote sites and mobile users, via CTERA Cloud Gateways, CTERA Agents, and CTERA Mobile app. The portal ensures data consistency, maintains version history and facilitates file sharing amongst users, regardless of their access method.

CTERA employs both global source-based de-duplication and data compression. This ensures that only incremental data changes are transferred for storage in the cloud, and that data blocks are stored only once, which dramatically reduces storage capacity needs and overall network traffic.

CTERA cloud gateways and end-point agents are remotely managed with CTERA Portal using a single web-based console. Template-based management, centralized monitoring, customized alerting and remote software and firmware upgrade capabilities make it easy to manage cloud gateways of various types and sizes as well as individual end-point agents – up to hundreds of thousands of connected devices – with no need for on-site IT presence in remote locations.

In This Chapter

Management Features

With the CTERA Portal, you control all aspects of Cloud Attached Storage, including:

- **Service Provisioning**

  Create user subscription plans that include cloud storage volume, services, number of devices per account, and snapshot retention policy.

- **User Management**

Manage anywhere from tens to hundreds of thousands of team members. Control user access, subscription plans, and view real-time storage usage and account status.

- **Remote Device Management and Monitoring**

  Manage CTERA cloud gateways and agents remotely. This enables you to view the device status in detail, including logged events, network status, storage volumes, and recent backups, as well as to set firmware upgrades, associated backup folders, and more.

- **Real-Time Event Monitoring**

  Centrally monitor and audit all events pertaining to the cloud service.

- **Reporting**

  Run and export detailed reports on a variety of usage parameters, including storage usage, bad files, snapshot status, and more. Generate user reports that are automatically emailed as PDF attachments.

- **Private Branding**

  Brand all aspects of the end-user experience, customizing it to your own corporate identity. This includes the CTERA Portal user interface and all automated email notifications.

Storage Clients

As part of the CTERA Cloud Attached Storage architecture, CTERA Portal can deliver cloud services to desktop, server, and mobile endpoints and to on-premises storage hardware. CTERA Portal connects to the following storage clients:

- ***CTERA Cloud Gateways*** (on page 9)
- ***CTERA Agents*** (on page 9)
- ***CTERA Mobile*** (on page 9)

Throughout this guide, the term "device" refers generically to CTERA Cloud Gateways and CTERA Agents.

CTERA Cloud Gateways

CTERA's cloud gateways are hybrid appliances that seamlessly combine local storage, cloud storage, data protection functionality and collaboration capabilities in a single, cost-effective package. Ideal for SMBs as well as enterprise branches and remote offices, CTERA's cloud gateways can replace legacy file servers and tape backup in a single solution with significant cost savings.

The cloud gateways feature a full set of Network Attached Storage (NAS) capabilities and comprehensive backup functionality, utilizing on-premises storage capabilities for speed and local sharing, while taking advantage of cloud storage for off-site backup, universal access, file sharing, and folder synchronization.

CTERA cloud gateways are managed remotely by CTERA Portal. Template-based management and remote firmware upgrades make it possible to manage numerous cloud gateways while maintaining minimal on-site IT and reducing total cost of ownership.

CTERA Agents

CTERA Agents are small-footprint software agents that perform both cloud backup and enterprise file sync and share (EFSS) functions. CTERA Agents can connect either directly to the cloud or to a CTERA cloud gateway.

CTERA Agents are available for Windows, Linux and Mac platforms, and are licensed for either laptop/desktop use or for servers. In all cases they provide file sync and backup capabilities. When connected to a CTERA cloud gateway, the CTERA Agent for Windows also supports backup of Microsoft server applications, and disk-level ("bare metal") backup.

CTERA Agents can be managed remotely by CTERA Portal, where all aspects of backup, sync and agent setup can be monitored and configured from a single console, including software upgrades.

CTERA Mobile

CTERA Mobile for iOS, Android, and Windows Phone enables business users to access their files securely, view them, edit them, and store them in the cloud where they can be shared with colleagues, partners and customers.

Users can also easily upload files, such as photos and documents, from their mobile device to their cloud drives.

CTERA Mobile works in tandem with CTERA Portal to provide access to private folders and team project workspaces, as well as the ability to view and download backup files.

CTERA Provisioning

User accounts need to be provisioned in order for end users to obtain services. This is done by setting the subscription plan, or adding add-ons to the user account.

If a subscription plan or add-on is modified, all user accounts assigned to the plan or add-on is automatically updated with the changes.

The following provisioning methods are available for end-user provisioning:

- **Subscription plans**

  In order to obtain services, end users can be subscribed to a *subscription plan*. The subscription plan includes the list of services provided to the user and the quota for each service.

  The subscription plan also specifies a snapshot retention policy for the user's folders (see ***Understanding Snapshot Retention Policies*** (see "***Snapshot Retention Policies***" on page 134)).

- **Add-ons**

  End users can subscribe to more services in addition to their subscription plan, by adding add-ons to the account. Each *add-on* defines a set of services that subscribed users will receive in addition to the services specified in the subscription plan. For example, an add-on may include an additional 10 GB of storage space for the number of devices specified in the subscription plan.

  Add-ons can be stacked as desired. For example, a user may have a subscription plan for 100 GB of storage, as well as two add-ons for 10GB of storage and one add-on for 5GB of storage. While the add-ons are valid, the user will be entitled to 125GB of cloud storage.

- **Vouchers**

  Vouchers are prepaid coupons that encapsulate specific add-ons and plans. When a device owner redeems a voucher encoding an add-on, the add-on is added to the user's account. When a device owner redeems a voucher encoding a plan, they are assigned to the subscription plan.

Tip

Vouchers can also contain a hidden plan that is not exposed to end users.

CTERA Portal allows you to mix and match these provisioning methods in order to obtain the combination that best suits your company's business model and your customer's needs.

2

Getting Started

In This Chapter

Browser Requirements

In order to use the CTERA Portal, you will need one of the following internet browsers:

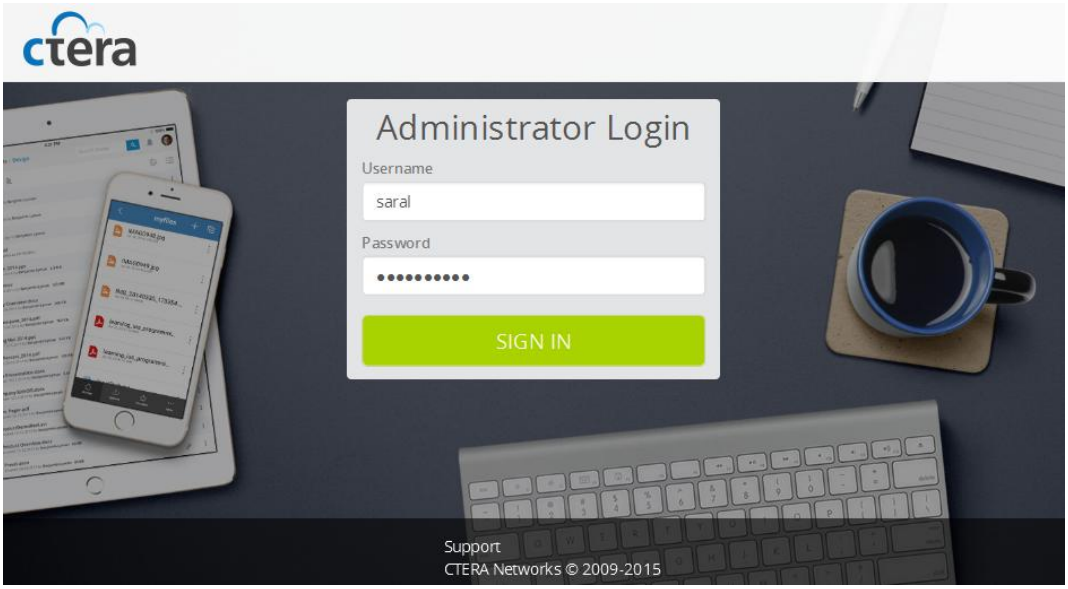
- Microsoft Internet Explorer 9.0 or later
- Mozilla Firefox
- Apple Safari
- Google Chrome
- Microsoft Edge (certain functions, such as "drag and drop," are not available due to browser limitations.)

Logging into the Administration Interface

1. Using a Web browser, open `http://<PortalDNS>/staff`.

   Where `<PortalDNS>` is your CTERA Portal's DNS name. For example, if your portal's DNS name is "myportal.acme.com", you must open `http://myportal.acme.com/staff`.

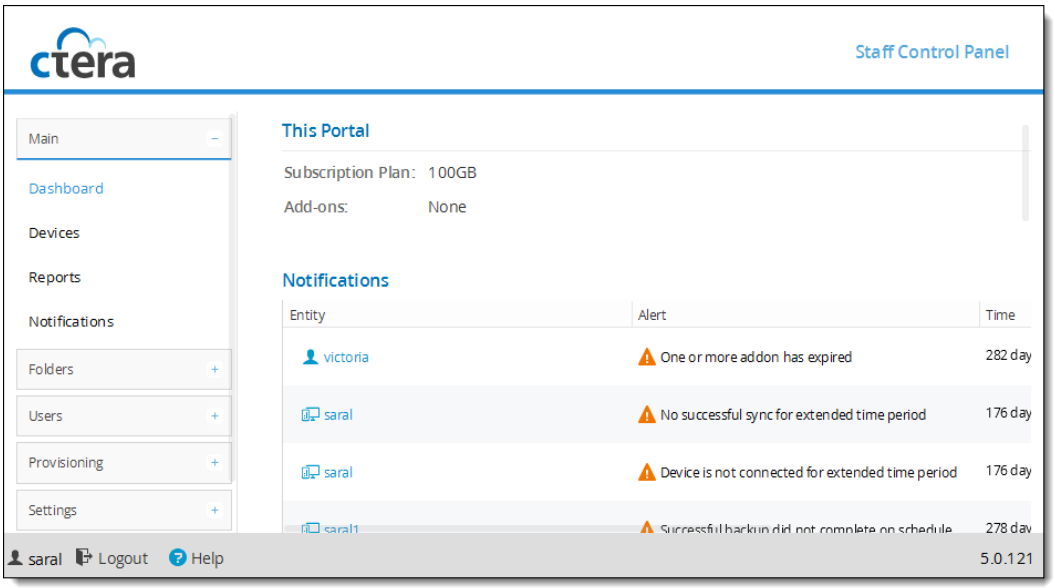
The CTERA Portal opens displaying the **Administrator Login** page.



2 In the fields provided, type your user name and password.

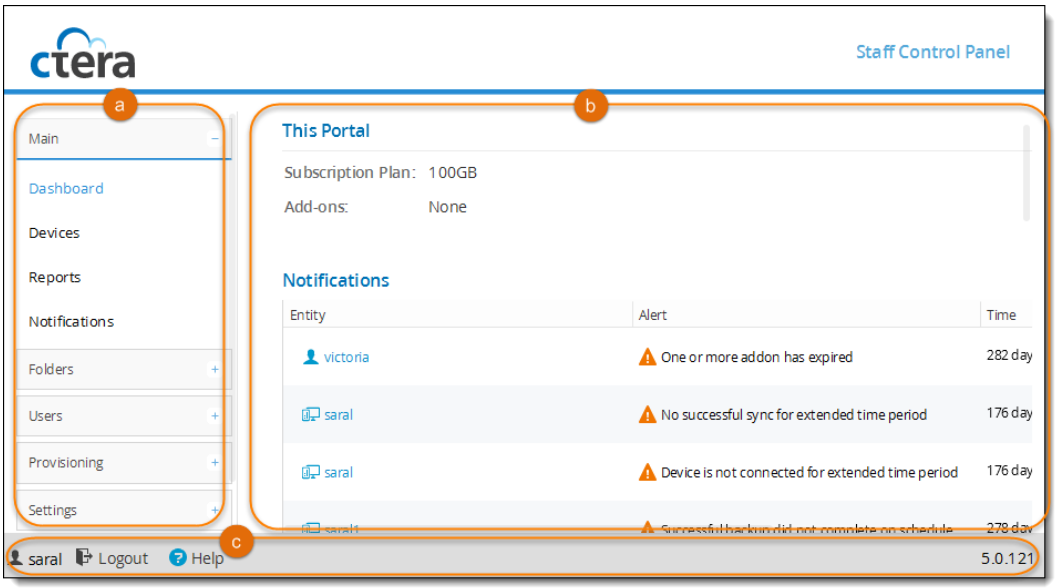
3 Click **Log In**.

The Staff Control Panel opens displaying your portal's **Main > Dashboard** page.



Using the Staff Control Panel

The **Staff Control Panel** consists of the following elements:



a **Menu**. Used for navigating between pages in the CTERA Portal. Click to expand a menu section and then click a menu item to display it in the main frame.

b **Main frame**. Displays the CTERA Portal pages, each of which contains controls and information.

c **Status bar**. Displays general and session-specific controls and information.

The Status Bar

The status bar includes the following elements:

- Your user name
- A button for logging out of the CTERA Portal

  See ***Logging Out*** (on page 14).

- A button for accessing online help
- The firmware version

Accessing Online Help

To access online help

- In the status bar, click **Help**.

Logging Out

To log out of the CTERA Portal

1. In the status bar, click **Logout**.

   You are logged out of the CTERA Portal.

Tip

You will be automatically logged out after a period of inactivity.

3

Managing Devices

The word *device* refers to both CTERA cloud gateways and CTERA Agents that are connected to the CTERA Portal. Devices are automatically added to the CTERA Portal, when their owners connect their CTERA cloud gateways or CTERA Agents to the CTERA Portal.

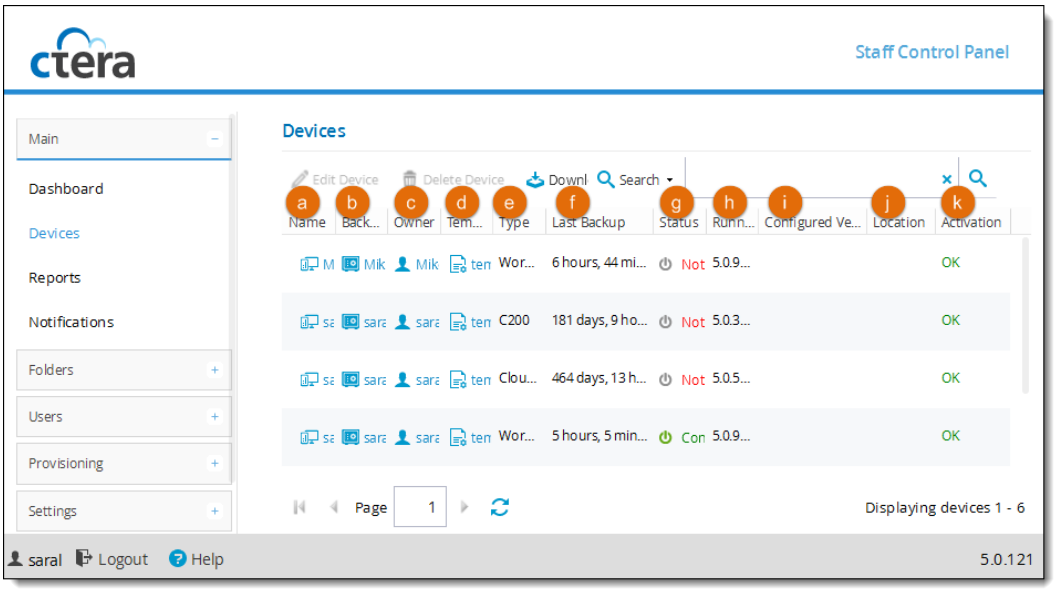
In This Chapter

Viewing All Devices

To view all devices connected to the portal

Select **Main > Devices** from the menu.

The **Main > Devices** page displays all devices connected to the portal.



a **Name**. The device's name.

To edit the device or view its details, click the device name. For further details, see ***Editing Device Settings*** (on page 24) and ***Viewing Individual Devices*** (see "***Viewing Individual Devices' Statuses***" on page 17).

b **Backup Folder**. The device's backup folder.

To edit the folder, click the folder name. For further details, see ***Adding and Editing Folders*** (see "***Creating New Cloud Drive Folders***" on page 44).

c **Owner**. The user account name of the device's owner.

To edit the user account, click the user account name. For further details, see Adding and Editing User Accounts.

Note: When viewing devices in the User Account Manager, this column does not appear.

d **Template**. The configuration template assigned to the device.

e **Type**. The device type.

f **Last Backup**. The amount of time that has elapsed since the device's last backup operation, in hours and minutes.

g **Status**. The device's connection status. This can be either of the following:

- Connected
- Not Connected

h **Running Version**. The firmware version currently installed on the device.

i **Configured Version**. The firmware version that the device is configured to download and install.

Note: Once the device has downloaded and installed the configured firmware successfully, the running firmware will be the same as the configured firmware.

j **Location**. The device's location.

k **Activation**. The device's activation status. This can be either of the following:

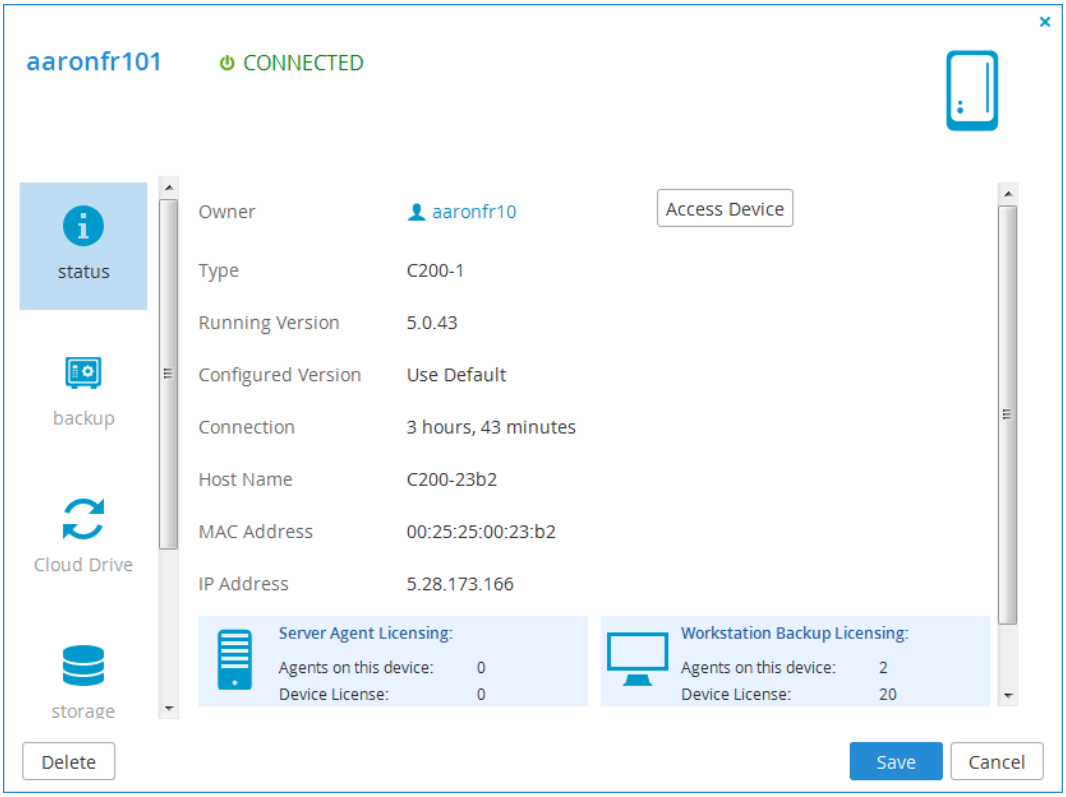
- **OK**. The device has been activated.
- **Pending**. The device is pending activation.

Viewing Individual Devices' Statuses

To view an individual device's status

1. Click the device name in the **Main > Devices** page.

The device's connection status is displayed at the top of the screen (**Connected** / **Not Connected**).



The following information is displayed:

Table 1: Status Tab Fields

This field...	Displays...
Owner	The full name of the device's owner. When editing an existing device, you can click on the owner's name to open the User Account Manager and manage the owner's user account. For information on managing user accounts, see ***Managing User Accounts*** (on page 77).
Type	The device type.
Running Version	The firmware version currently installed on the device.
Configured Version	The firmware version that the device is configured to download and install. **Note**: Once the device has downloaded and installed the configured firmware successfully, the running firmware will be the same as the configured firmware.
Connection	The connection duration in hours and minutes.
Host Name	The device's host name.
MAC Address	The device's MAC address.
IP Address	The device's IP address.
Operating System	The operating system on which the device is installed. This field is only relevant if the device is a CTERA Agent.
Licensing Status	The device's licensing status (**Ok** or **Unlicensed**). This field is only relevant if the device is a CTERA Agent.
Server Agent Licensing	This area displays information about CTERA Server Agent licensing for the device. It only appears if the device is a CTERA cloud gateway.
Agents on this device	The number of server agents installed for the device.
Device License	The number of server agent licenses taken from the licenses included with the device.
From Portal	The number of server agent licenses taken from the quota allocated to the device owner's CTERA Portal account.
Workstation Backup Licensing	This area displays information about CTERA Workstation Backup licensing for the device. It only appears if the device is a CTERA cloud gateway.
Agents on this device	The number of workstation agents installed for the device.

This field...	Displays...
Device License	The number of workstation agent licenses taken from the licenses included with the device.
From Portal	The number of workstation agent licenses taken from the quota allocated to the device owner's CTERA Portal account.

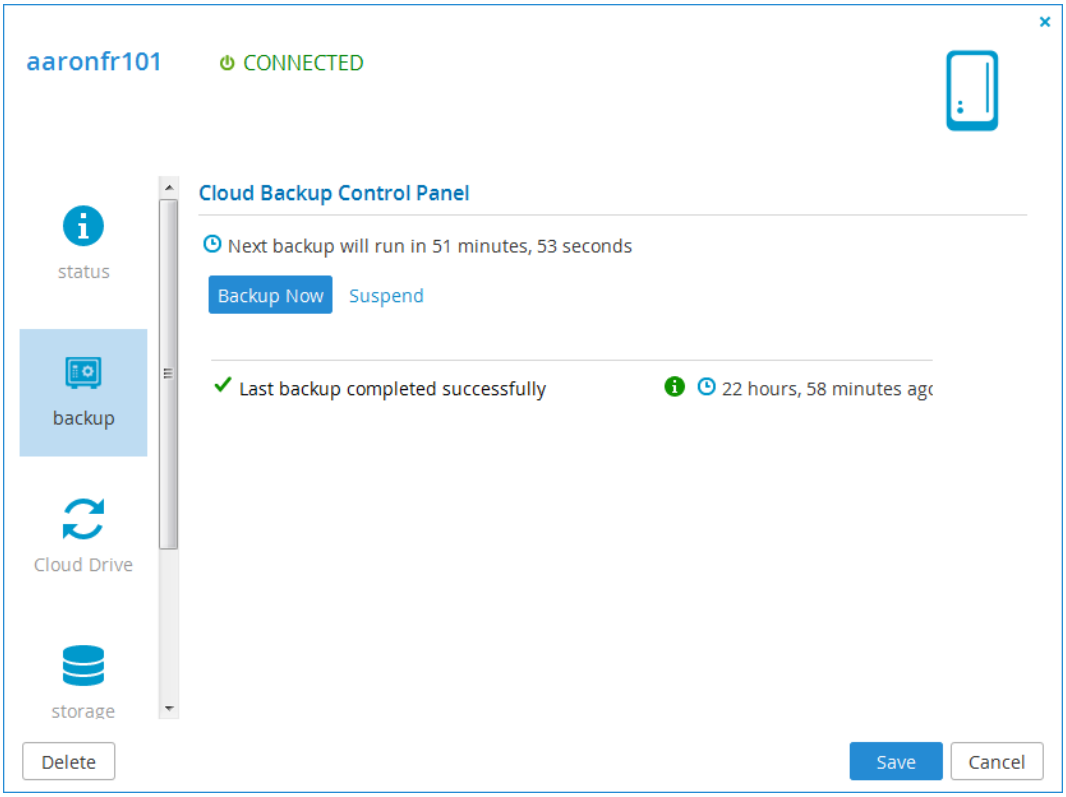
Viewing Individual Devices' Backup Status

Tip

Backup status can only be viewed if the device is connected.

To view an individual device's backup status

1. Click the Device name in the **Main > Devices** page.
2. Select the **backup** tab.



The following information is displayed:

Table 2: Backup Tab Fields

This field...	Displays...
Next backup will run in	The amount of time until the next scheduled automatic backup.
The last backup result	The status of the last backup: • **Completed successfully** • **Backup in Progress** • **The last backup has failed**, followed by the reason it failed If an error occurred during backup, refer to the backup logs for details. See ***Viewing Cloud Backup Logs*** (on page 231).
	Mouse-over this icon to view the following information about the last backup: • The total size of the files that you selected for backup • The total number of files that you selected for backup • The amount of time the backup took
	The amount of time since the last backup ended.

Viewing Individual Cloud Gateway's Storage Status

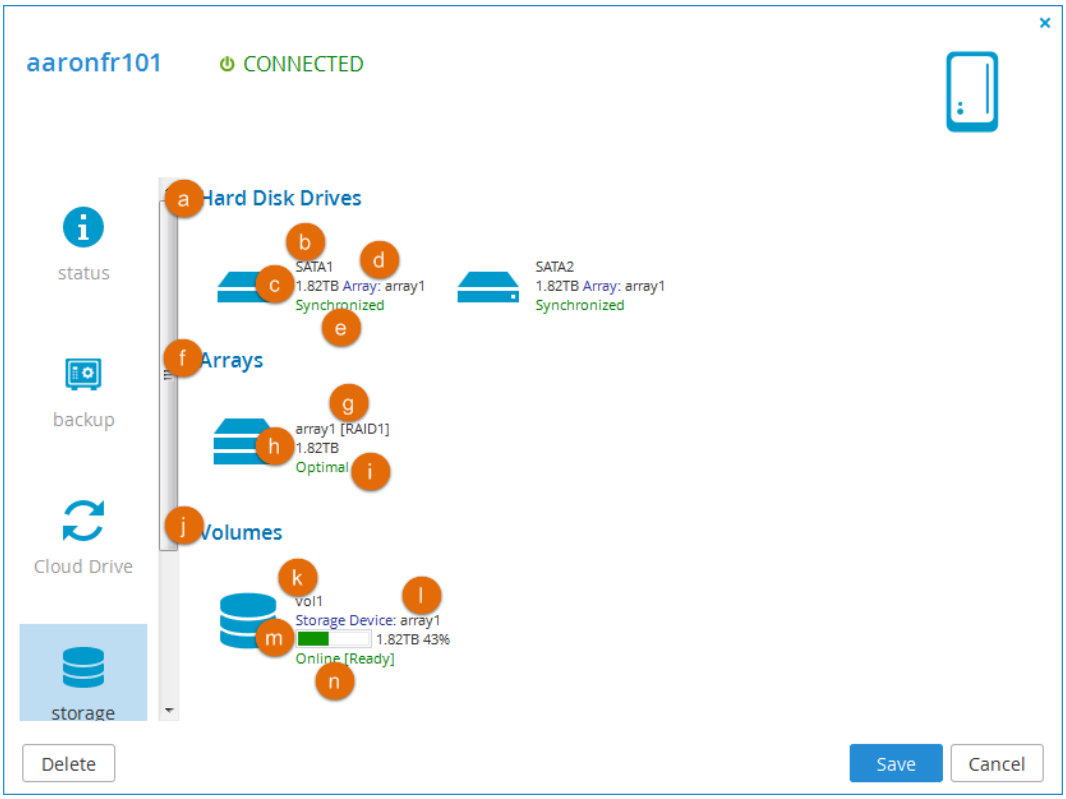
Tip

Storage status only appears if the device is a CTERA cloud gateway and connected. It does not appear if the device is an agent.

To view an individual cloud gateway's storage status

1 Click the Device name in the **Main > Devices** page.

2 Select the **storage** tab.



The following information is displayed:

a All disk drives installed on the CTERA Portal.

For each drive:

b The disk type.

c The disk size in GB. Note that you may notice a discrepancy between the disk capacity stated on the disk's packaging and the disk capacity displayed in the CTERA Portal Dashboard. This difference is due to the fact that vendors define 1 GB as 1 billion (109) bytes, while computers define 1 GB as 230 bytes.

d The array to which the disk is assigned.

e The disk status:

- **Synchronized**. This drive is in a RAID array and is in optimal condition.
- **OK**. The drive is not in a RAID array and is in optimal condition.
- **FAIL**. The hard drive has failed.
- **Unrecognized**. The hard drive contains unrecognized data. You must format the hard drive before it can be used.
- **Inactive**. This drive is in a RAID array, but is currently not in use.
- **Rebuilding**. This drive is in a RAID array that is currently being rebuilt.

- **In Use**. The drive is currently in use.

f All arrays defined on the CTERA Portal.

For each array:

g The array name and RAID type.

h The array size in GB.

i The array status:

- **Optimal**. The array is in optimal condition.
- **Degraded**. The array is accessible and there is no data loss; however, the array type is RAID1 (Mirroring), and a disk is failed or missing. Performance and reliability may be reduced. Replace the failed drive as soon as possible.
- **Fail**. The array is not accessible.
- **Recovering**. A degraded array is being repaired. The CTERA Portal is currently synchronizing out-of-sync members of the array, and performance of the CTERA Portal may be reduced. Once the recovery is finished, the array will return to optimal state.
- **Scrubbing**. Data scrubbing is in progress.

j All volumes defined on the CTERA Portal.

For each volume:

k The volume name.

l The storage device on which the volume is located.

m A bar representing of the percentage of the volume currently in use, followed by the volume size in GB, followed by the percentage of the volume currently in use.

n The volume's status in the format: Mode [Status]. The mode can be **Online** or **Offline**. The status can be:

- **Key required**. The volume is encrypted and requires a key.
- **Contains errors**. The file system needs to be repaired.
- **Read only**. The file system is incompatible with current firmware.
- **Corrupted**. Failed to read the file system status.
- **Unknown**. No file system was found in the volume.
- **Ready**. The volume is ready for use.
- **Recovering**. The file system is being recovered after a non-clean shutdown.
- **Mounting**. Routine cleanup is being performed after a non-clean shutdown.

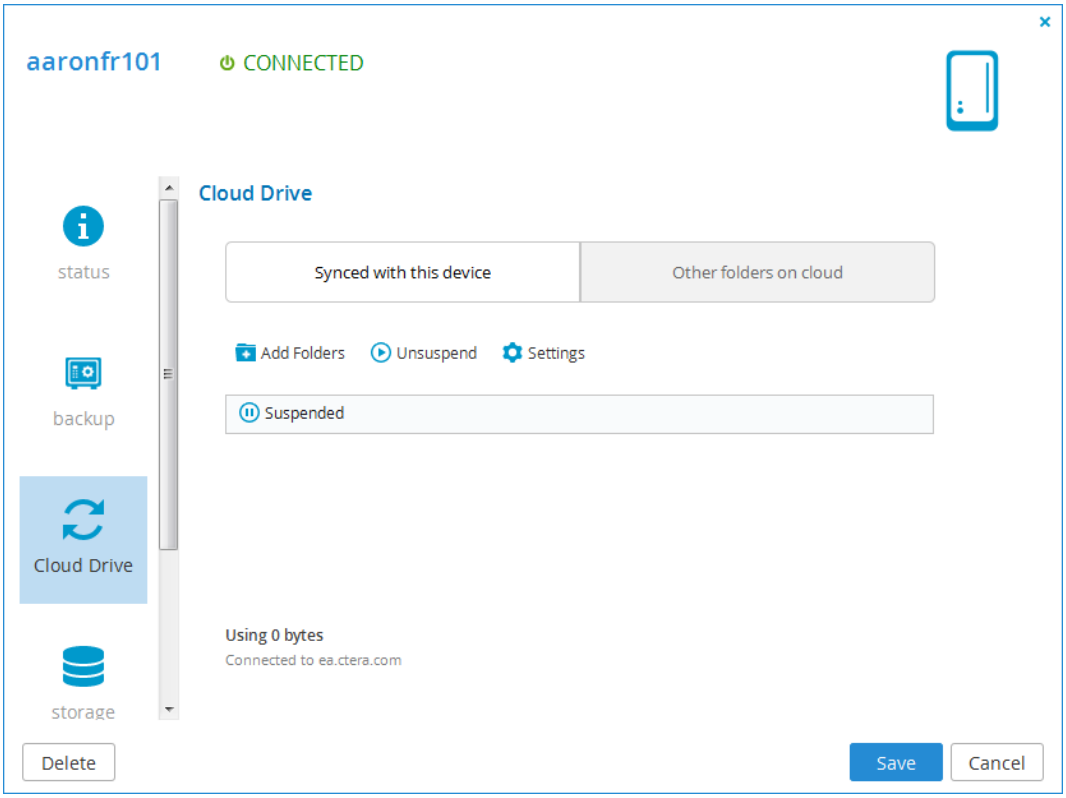
- **Formatting**. The volume is being formatted.
- **Converting**. The volume is being converted (from EXT3 to NEXT3, or the opposite).
- **Resizing**. The volume is being resized.
- **Repairing**. The volume is being repaired.
- **Checking**. The volume is being scanned for errors.
- **Checking Quota**. The volume's storage quotas are being recalculated.

Managing Cloud Drive Synchronization

Through the devices page, you can view and manage the cloud drive synchronization of a device.

To manage the cloud drive synchronization of a device

1. Click the device name in the **Main > Devices** page.
2. Select the **Cloud Drive** tab.



You can make the following changes:

- Change the Cloud Drive operation mode: either **Classic** or **Sync Gateway**. (Relevant only for cloud gateways.)
- Suspend/Unsuspend syncing between the cloud drive and the device.

- Add/remove folders to/from the Cloud Drive synchronization.
- Change which folders in the Cloud Drive sync to which folders on the device

Refer to the device's user guide for complete information about managing the Cloud Drive.

Editing Device Settings

You can edit the following device settings:

- **Device name**

  When a CTERA device is first connected to the CTERA Portal, it is assigned a name based on the owner's user name, by default. For example, if John Smith's user name is JohnS, and he adds two devices, the first device will be named JohnS, and the second will be named JohnS1. If desired, you can edit a device's name.

- **Template**

  You can specify whether the device should inherit its settings from a device configuration template. For information on device configuration templates, see ***Managing Device Configuration Templates*** (on page 183).

- **Backup folder**

  If desired, you can change the folder used for the device's backups. This is useful, for example, if an old device has failed, and you want to restore the old device's backup to a new device. To do so, delete the old device, then assign the old device's backup folder to the new device.

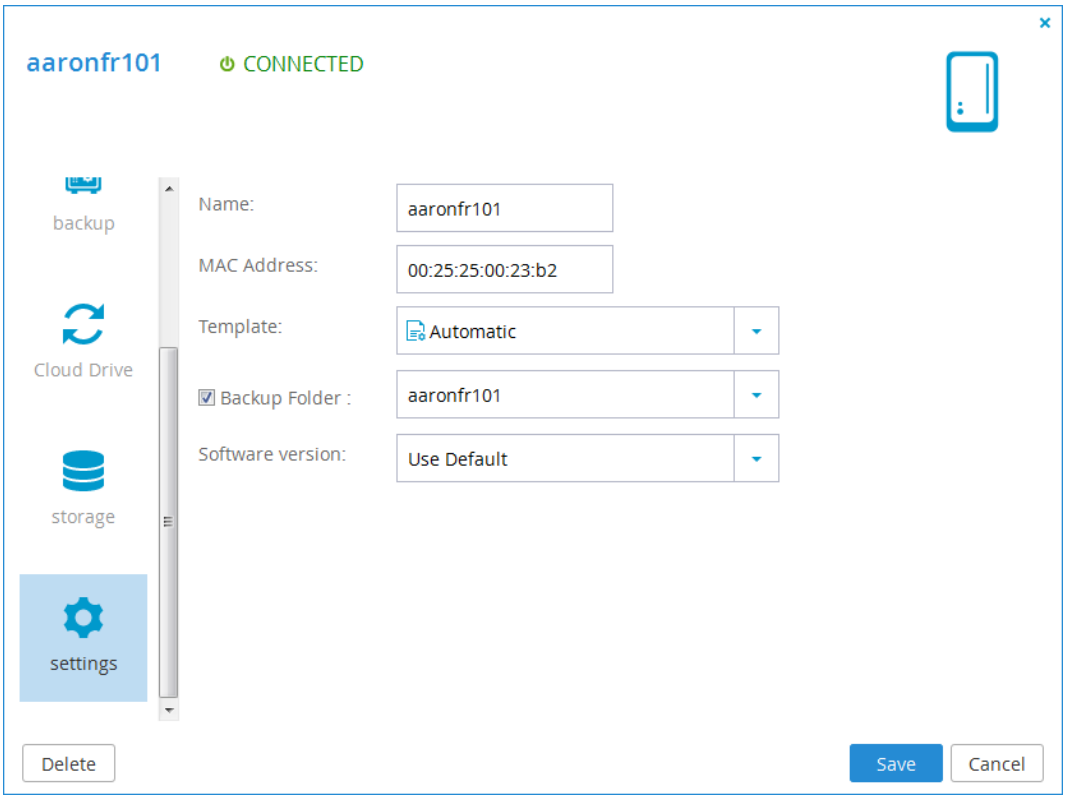
- **Software version**

  You can install a specific firmware on the device.

To edit a device

1. Click the device name to open the device manager.

2 Select the **Settings** tab.



3 Complete the fields using the information in the following table.

4 Click **Save**.

Table 3: Device Manager Settings Fields

In this field...	Do this...
Name	Type a new name for the device.
Template	Specify which template to use for the device, by selecting one of the following: • A specific template • **No Template**. Do not use a template for this device. • **Automatic**. Automatically assign a template to this device, based on the configured automatic template assignment policy. See ***Configuring Automatic Template Assignment*** (see "***Configuring the Automatic Template Assignment Policy***" on page 212). The default value is **Automatic**.
Backup Folder	Check/uncheck the box to enable or disable backup operations for the device. In the dropdown list, select a specific folder in which all of the device's backups should be stored.
Software version	Specify which firmware to use for this device, by selecting one of the following: • A specific firmware • **Use Default**. Use the default firmware for this device type.

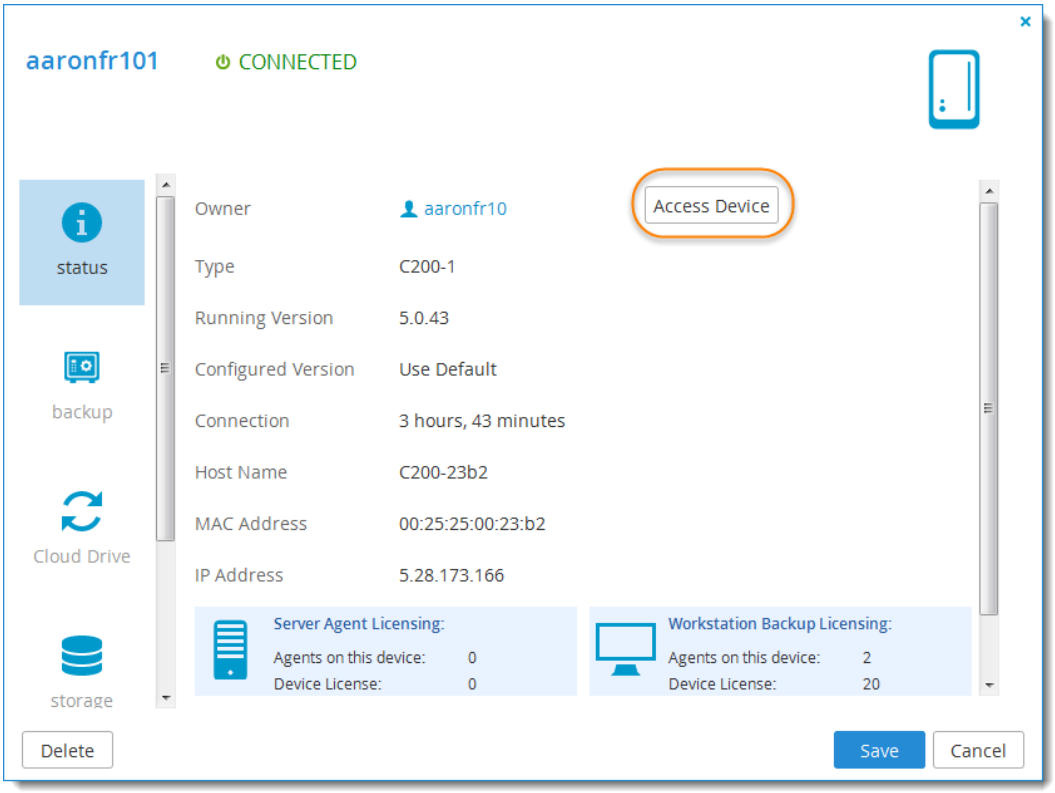
Remotely Managing Devices

You can remotely access a device and the files on it, when the following conditions are met:

- A device administrator has enabled remote administration for the device.
- A device administrator has assigned you a user name and password for accessing the device.

To remotely manage a device

1. Click the Device name in the **Main > Devices** page.
2. In the **status** tab, click **Access Device**.



The following things happen:

- If Single Sign On is disabled, the **Log In** window appears.

  In the fields provided, type your user name and password for accessing this device, then click **Log In**.

- The device's management Web interface appears displaying the **Configuration** tab.

Tip

To use Single Sign On from the Portal to the device, your administrator role must include **Allow SSO** permissions (see***Customizing Administrator Roles*** (on page 109)), and **Allow single sign on from CTERA Portal** must be enabled in the device's **Remote Access** settings.

In this tab, you can manage device settings. For information, refer to the device's User Guide.

1. To manage the files on the device, click the **Files** tab.

   The File Manager appears. For information using on this tab, refer to the device's User Guide.

2. To manage CTERA Agents associated with the device, click the **My Computers** tab.

   The **My Computers** tab appears. For information using on this tab, refer to the device's User Guide.

Remotely Performing Cloud Backup Operations on Devices

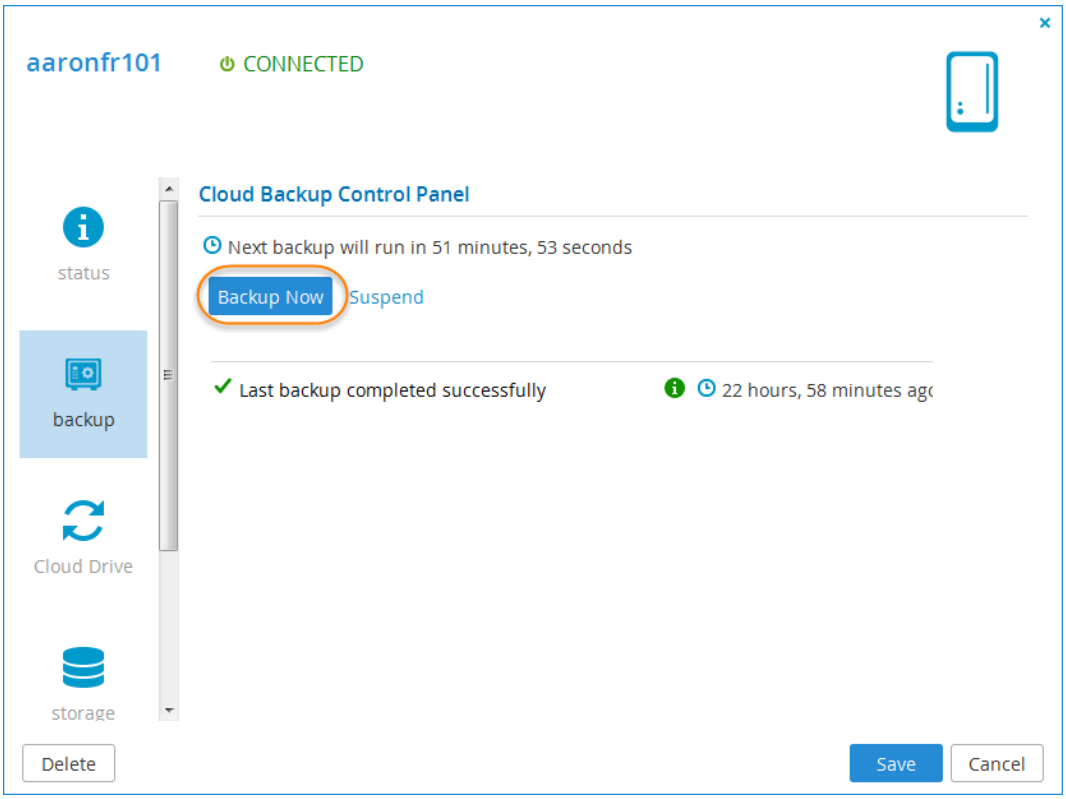
You can start, stop, suspend, or resume cloud backup directly from the Device Manager, without logging into the remote device.

Manually Starting Cloud Backup

You can manually start cloud backup at any time.

To manually start cloud backup

1. Click the Device name in the **Main > Devices** page.
2. In the **backup** tab, click **Backup Now**.



A progress bar appears, and the files are backed up to cloud storage.

A success message appears.

Canceling the Current Cloud Backup

You can cancel a running cloud backup.

Tip

Only the current backup will be cancelled. The next automatic backup will occur as scheduled.

To cancel the current cloud backup

1. Click the Device name in the **Main > Devices** page.
2. In the **backup** tab, click **Cancel**.

The current backup is canceled.

Suspending the Cloud Backup Service

You can suspend the CTERA Cloud Backup service, including:

- The currently running backup
- All scheduled automatic backup

To suspend the CTERA Cloud Backup service

1. Click the Device name in the **Main > Devices** page.
2. In the **backup** tab, click **Suspend**.

   If a backup is currently running, it is paused. All future automatic backups are suspended.

   A message appears, indicating that backup has been suspended.

Resuming the Cloud Backup Service

If the CTERA Cloud Backup service is suspended, you can unsuspend it.

To resume the CTERA Cloud Backup service

1. Click the Device name in the **Main > Devices** page.
2. In the **backup** tab, click **Unsuspend**.

   If a backup was running at the time when backups were suspended, that backup is resumed.

   Otherwise, cloud backup will occur at the next scheduled time.

Exporting Devices to Excel

You can export a list of devices and their details to a Microsoft Excel (*.xls) file on your computer.

To export devices to Excel

1. Select **Main > Devices** from the menu.
2. Click **Export to Excel**.

   The devices are exported.

Remote Wiping Mobile Devices

Remote wipe causes a device running CTERA Mobile to log out and to erase all locally synced files. In addition, the wiped device's key is invalidated. Once remote wipe has been activated through the CTERA Portal, wiping commences as soon as the device comes online. An email notification is sent to the administrator who initiated the wipe procedure, once remote wipe has completed.

Remote wipe can be performed only by administrators whose roles include the *Allow remote wipe for devices* permission.

To wipe a mobile device

1. In the **Main > Devices** page, click the name of the mobile device you want to wipe.
2. In the **Status** tab, click **Remote Wipe**.
3. Click **Remote Wipe**. A confirmation message appears.
4. Select **I understand that this action cannot be undone or canceled**.
5. Click **Erase All Data**. The CTERA data is wiped from the mobile device.

Deleting Devices

To delete a device

1. In the **Main > Devices** page, select the desired device's row, then click **Delete Device**.

   A confirmation message appears.

2. Do one of the following:

   - To delete the device including its backup folders, click **Delete device including associated folders**.
   - To delete the device only, click **Delete device only**.

   The device is deleted and disconnected from the CTERA Portal.

   If you chose to delete backup folders, the folders are deleted from the CTERA Portal, as well.

4

Viewing Reports

The CTERA Portal provides reports about the following:

- Folders
- Folder Groups
- Devices
- Plans
- Add-ons

In This Chapter

Viewing the Folders Report

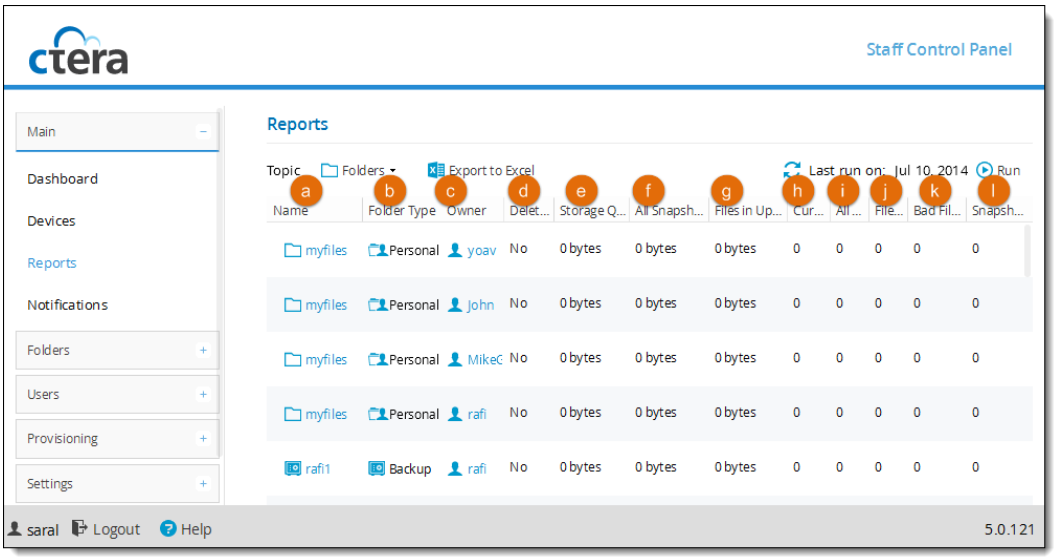
You can view detailed information about all folders, including deleted ones.

To view the Folders Report

1. Select **Main > Reports** from the menu.
2. Select **Folders** from the **Topic** drop-down list.

   If a CTERA Portal administrator already ran the Folders Report, the report is displayed, and the report date appears in the **Last run on** field.
3. If the **Last run on** field displays "Never", or if you would like to update the displayed report, click **Run**.

A new report is generated.



a **Name**. The folder's name.

b **Folder Type**. The type of folder (Personal Folder/Project/Backup Folder)

c **Owner**. The folder's owner.

d **Deleted**. Indicates whether the folder has been deleted (true/false).

e **Storage Quota Usage**. The percentage of storage quota used.

f **All Snapshots Size**. The size of all snapshots of this folder.

g **Files in Upload Size**. The size of files that are currently being uploaded to this folder.

h **Current Snapshot Files**. The number of files in the current snapshot (that is, not including previous versions that are stored for this folder).

i **All Snapshots Files**. The total number of files in all snapshots (that is, including previous versions that are stored for this folder).

j **Files in Upload**. The number of files that are currently being uploaded to this folder.

k **Bad Files**. The number of corrupted files in the folder.

l **Snapshots Number**. The number of previous versions currently stored for this folder.

Viewing the Folder Groups Report

You can view detailed information about all folder groups, including deleted ones.

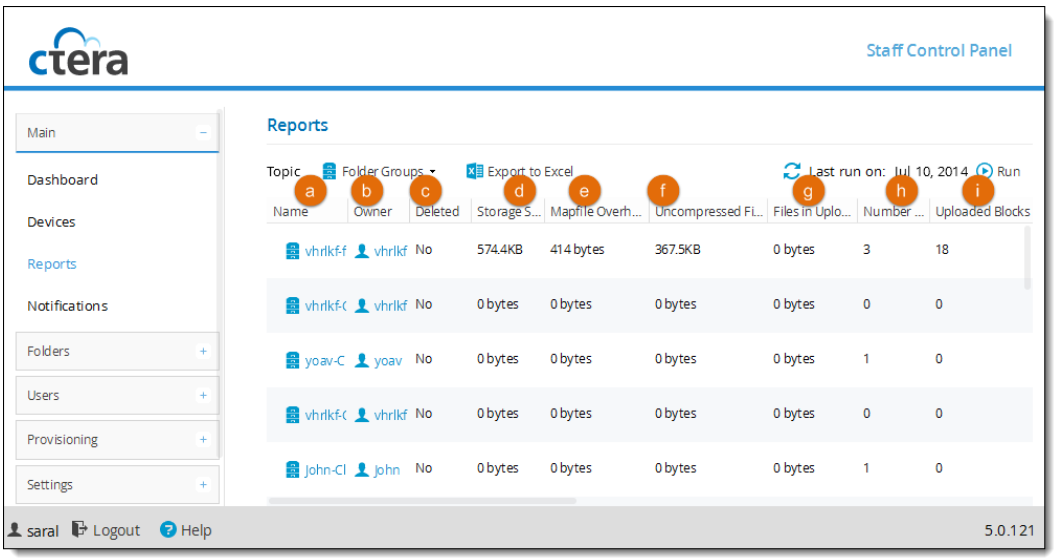
To view the Folder Groups Report

1. Select **Main > Reports** from the menu.
2. Select **Folder Groups** from the **Topic** drop-down list.

If a CTERA Portal administrator already ran the Folder Groups Report, the report is displayed, and the report date appears in the **Last run on** field.

3 If the **Last run on** field displays "Never", or if you would like to update the displayed report, click **Run**.

4 A new report is generated.



a **Name**. The folder group's name.

b **Owner**. The folder group's owner.

c **Deleted**. Indicates whether the folder group has been deleted (true/false).

d **Storage Space**. The amount of storage space consumed by this folder group.

e **Mapfile Overhead**. The amount of space consumed by the mapfiles for this folder group.

f **Uncompressed Files Size**. The uncompressed size of the files in folders belonging to this folder group.

g **Files in Upload Size**. The size of files that are currently being uploaded to folders belonging to this folder group.

h **Number of Folders**. The number of folders belonging to this folder group.

i **Uploaded Blocks**. The number of uploaded blocks in folders belonging to this folder group.

j **In Upload Blocks**. The number of blocks currently being uploaded to folders belonging to this folder group.

k **In Upload Mapfiles**. The number of mapfiles currently being uploaded to folders belonging to this folder group.

l **Missing Blocks**. The number of missing blocks in folders belonging to this folder group.

m **Total Mapfiles**. The total number of mapfiles in folders belonging to this folder group.

n **Missing Mapfiles**. The number of missing mapfiles in folders belonging to this folder group.

o **Total Files**. The total number of files in folders belonging to this folder group.

p **Files in Upload**. The number of files that are currently being uploaded to folders belonging to this folder group.

q **Bad Files**. The number of corrupted files in folders belonging to this folder group.

Viewing the Devices Report

You can view detailed information about all devices.

To view the Devices Report

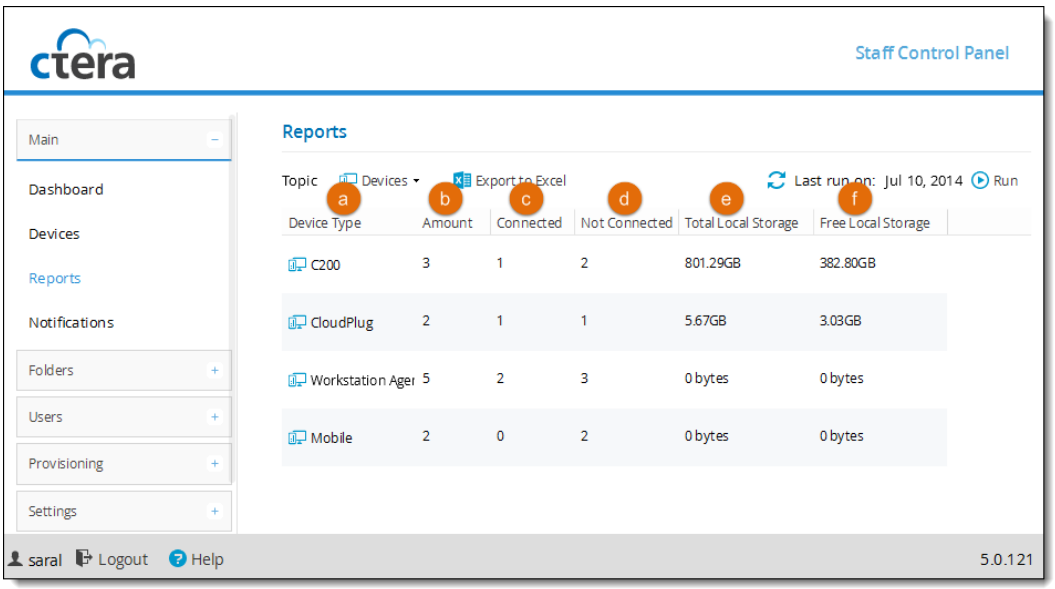
1 Select **Main > Reports** from the menu.

2 Select **Devices** from the **Topic** drop-down list.

If a CTERA Portal administrator already ran the Devices Report, the report is displayed, and the report date appears in the **Last run on** field.

3 If the **Last run on** field displays "Never", or if you would like to update the displayed report, click **Run**.

A new report is generated.



a **Device Type**. The device type.

b **Amount**. The number of devices of this type.

c **Connected**. The number of devices of this type that are currently connected to the CTERA Portal.

d **Not Connected**. The number of devices of this type that are currently not connected to the CTERA Portal.

e **Total Local Storage**. The total amount of local storage space reported by devices of this type.

f **Free Local Storage**. The amount of local storage space that is currently reported as unused by devices of this type.

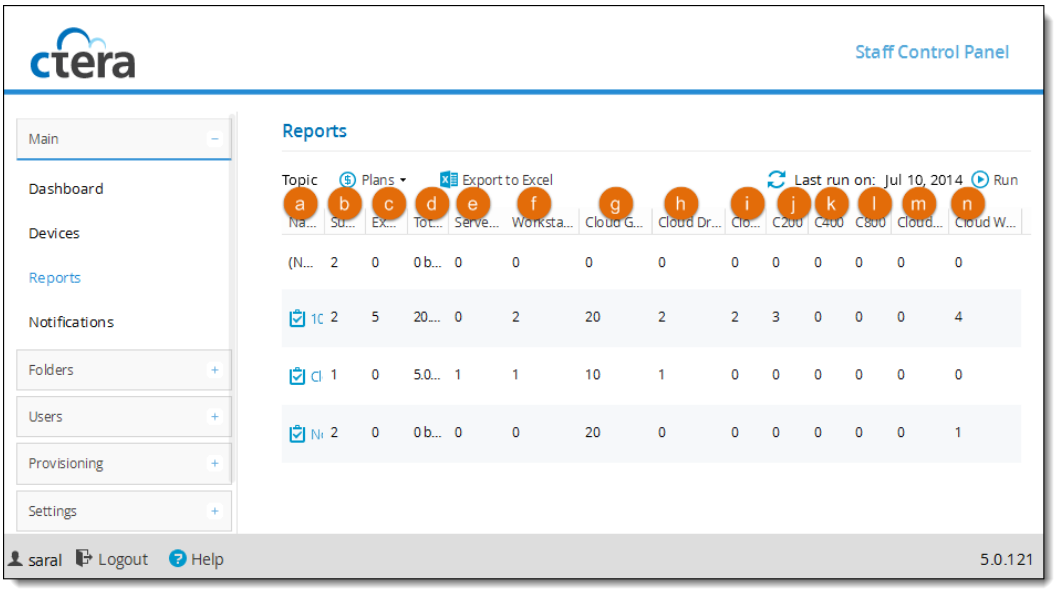
Viewing the Plans Report

To view the Plans Report

1. Select **Main > Reports** from the menu.
2. Select **Plans** from the **Topic** drop-down list.

   If a CTERA Portal administrator already ran the Plans Report, the report is displayed, and the report date appears in the **Last run on** field.
3. If the **Last run on** field displays "Never", or if you would like to update the displayed report, click **Run**.

   A new report is generated.



a **Name**. The plan's name.

b **Subscriptions**. The number of subscriptions to the plan.

c **Expired**. The number of expired subscriptions to the plan.

d **Total Storage Space**. The total amount of cloud storage space quota included in all instances of this plan, in GB.

e For example, if 10 users are subscribed to a plan with 10GB storage space, this field will display 100GB.

f **Server Agent Licenses**. The total number of server agent licenses included in all instances of this plan. For example, if 10 users are subscribed to a plan with 5 server agent licenses, this field will display 50.

g **Workstation Backup Licenses**. The total number of workstation backup licenses included in all instances of this plan. For example, if 10 users are subscribed to a plan with 10 workstation backups, this field will display 100.

h **Cloud Gateway Licenses**. The total number of appliance licenses included in all instances of this plan. For example, if 10 users are subscribed to a plan with 10 appliance licenses, this field will display 100.

i **Cloud Drive Licenses**. The total number of Cloud Drive licenses included in all instances of this plan. For example, if 10 users are subscribed to a plan with 10 Cloud Drive licenses, this field will display 100.

j **CloudPlug**. The number of CloudPlug cloud gateways owned by users who are subscribed to the plan.

k **C200**. The number of C200 cloud gateways owned by users who are subscribed to the plan.

l **C400**. The number of C400 cloud gateways owned by users who are subscribed to the plan.

m **C800**. The number of C800 cloud gateways owned by users who are subscribed to the plan.

n **Cloud Server Agent**. The number of server agents in Cloud Agent mode owned by users who are subscribed to the plan.

o **Cloud Workstation Backup**. The number of workstation agents in Cloud Agent mode owned by users who are subscribed to the plan.

Viewing the Add-Ons Report

To view the Add-Ons Report

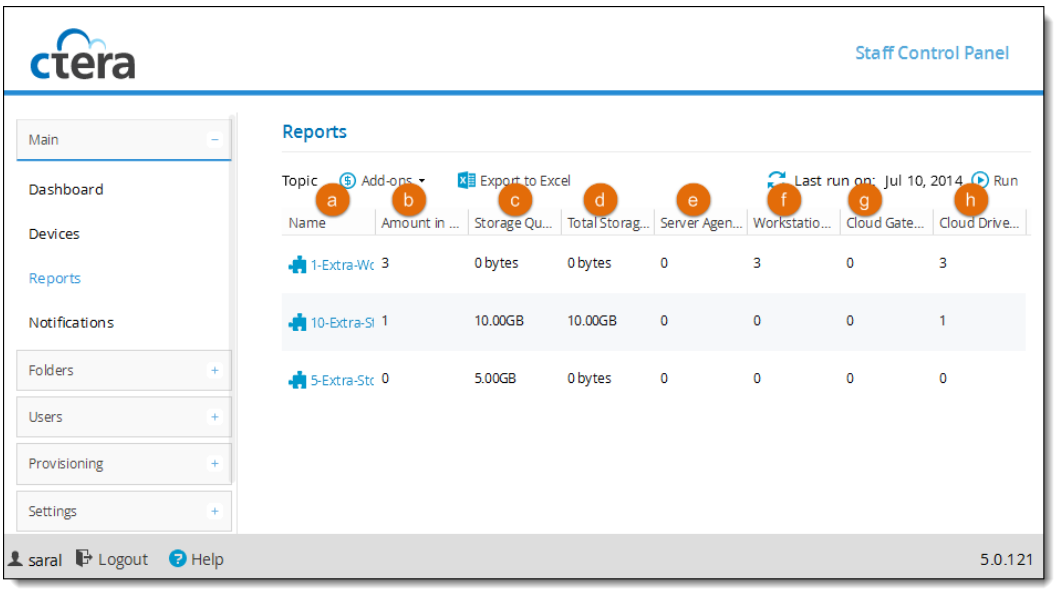
1 Select **Main > Reports** from the menu.

Select **Add-ons** from the **Topic** drop-down list.

If a CTERA Portal administrator already ran the Add-ons Report, the report is displayed, and the report date appears in the **Last run on** field.

2 If the **Last run on** field displays "Never", or if you would like to update the displayed report, click **Run**.

A new report is generated.



a **Name**. The add-on's name.

b **Amount in use**. The number of add-ons that are currently in use.

c **Storage Quota**. The amount of storage space included in a single instance of this add-on.

d **Total Storage Space**. The total amount of storage space included in all instances of this add-on.

For example, if the storage quota of a single instance of this add-on is 10GB, and the add-on is used 15 times, then the total storage space is 150GB.

e **Server Agent Licenses**. The total number of server agent licenses included in all instances of this add-on.

f **Workstation Backup Licenses**. The total number of workstation backup licenses included in all instances of this add-on.

g **Cloud Gateway Licenses**. The total number of cloud gateway licenses included in all instances of this add-on.

h **Cloud Drive Licenses**. The total number of Cloud Drive licenses included in all instances of this add-on.

Exporting Reports to Excel

You can export reports to a CSV file that can be opened in Microsoft Excel.

To export a report

1 View the desired report.

2 Click **Export to Excel**.

The report is exported to a CSV file.

5

Managing Folders

In This Chapter

Overview

CTERA Portal has two types of cloud folders: backup folders, and Cloud Drive folders.

Backup folders are part of the Cloud Backup service. When a user backs up a device, a backup folder is automatically created in the CTERA Portal, to contain the device's backups.

Cloud Drive folders. are folders created by the Cloud Drive service for personal and shared use. The portal automatically creates a personal folder for each user account's private files when the user account is created in the CTERA Portal. The folder appears to the user as "`My Files`" and is the user's home folder, and it contains files that can only be viewed and edited by the user. The home folder name and the automatic creation of the home folder can be changed in the General Settings of the Virtual Portal Settings (**Settings > Virtual Portal Settings**).

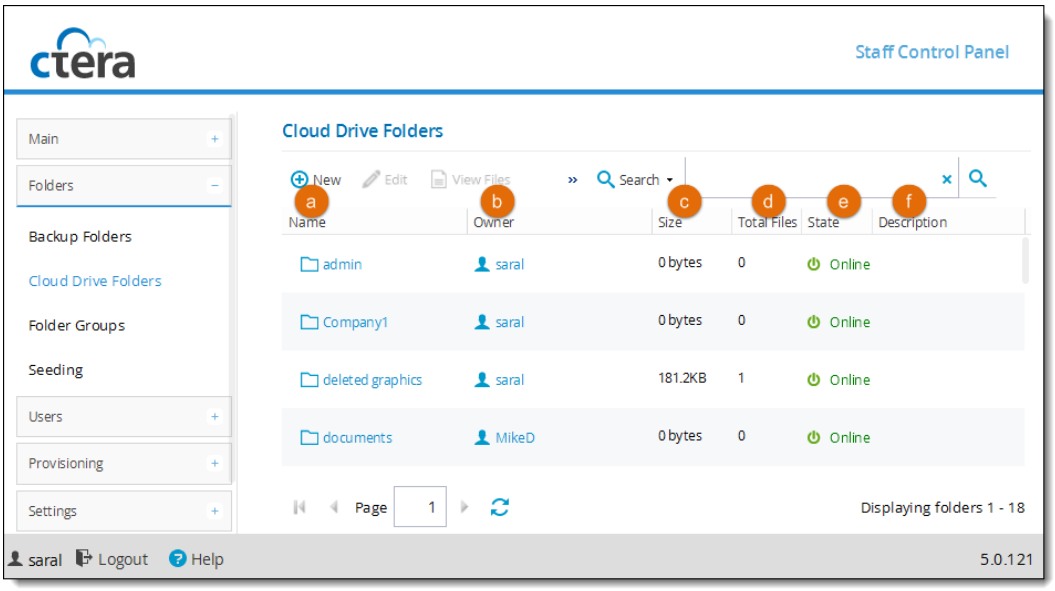
By default, when folders are created in the CTERA Portal, they are assigned a name based on the device's name. For example, if a device is named JohnS, then this device's files will be backed up to a folder called JohnS, and its cloud files will be stored in a folder called JohnS-CloudFiles followed by a number. If desired, you can add new folders manually, and you can edit their properties.

Viewing Cloud Drive Folders

To view all cloud drive folders in the portal

1. In the navigation pane, click **Folders > Cloud Drive Folders**.

   The **Folders > Cloud Drive Folders** page appears, displaying all cloud drive folders.



   a **Name**. The folder's name.

   To view the folder's contents, click the folder name. For further details, see ***Adding and Editing Folders*** (see "***Creating New Cloud Drive Folders***" on page 44).

   b **Owner**. The user account name of the folder's owner.

   To edit the user account, click the user account name. For further details, see ***Managing User Accounts*** (on page 77).

   c **Size**. The current size of the folder in MB.

   d **Total Files**. The total number of files in the folder.

   e **State**. The folder's state. This can have the following values:

   - **Online**. The folder is online, and it is possible to view, modify, and back up files to it.
   - **Offline**. The folder is offline, and it is not possible to view, modify, and back up files to it. Folders may be taken offline during some maintenance operations, such as when repairing a folder using the CTERA Cloud FSCK utility.

   Folders inherit their state from the folder group.

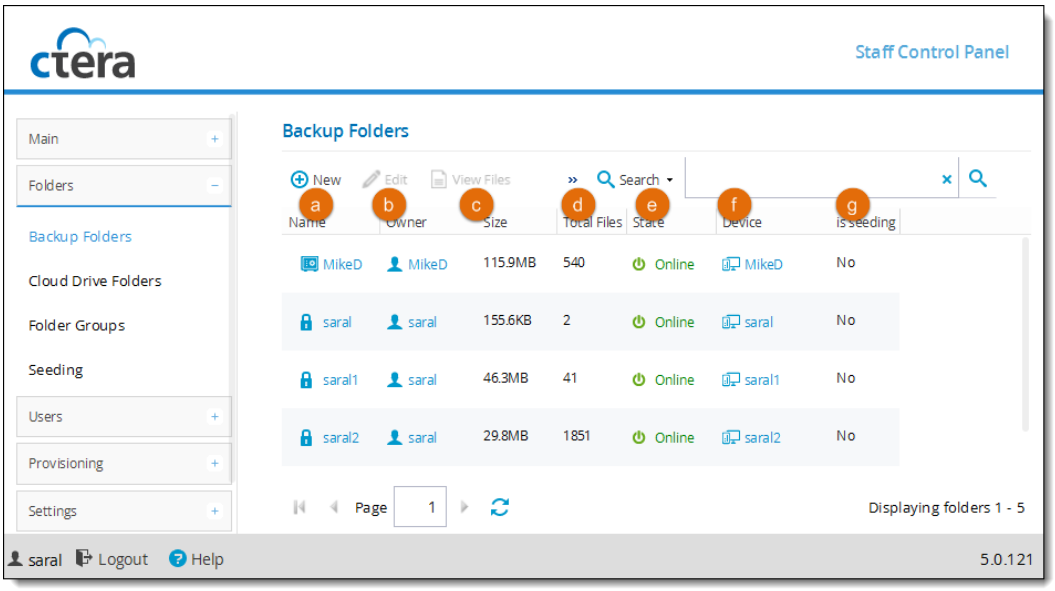
   f **Description**. A description of the folder.

Viewing Backup Folders

To view all backup folders in the portal

1. In the navigation pane, click **Folders > Backup Folders**.

   The **Folders > Backup Folders** page appears, displaying all backup folders.



a **Name**. The folder's name.

To view the folder's contents, click the folder name. For further details, see ***Adding and Editing Folders*** (see "***Creating New Cloud Drive Folders***" on page 44).

b **Owner**. The user account name of the folder's owner.

To edit the user account, click the user account name. For further details, see ***Managing User Accounts*** (on page 77).

c **Size**. The current size of the folder in MB.

d **Total Files**. The total number of files in the folder.

e **State**. The folder's state. This can have the following values:

- **Online**. The folder is online, and it is possible to view, modify, and back up files to it.
- **Offline**. The folder is offline, and it is not possible to view, modify, and back up files to it. Folders may be taken offline during some maintenance operations, such as when repairing a folder using the CTERA Cloud FSCK utility.

Folders inherit their state from the folder group.

f **Device**. The device's name.

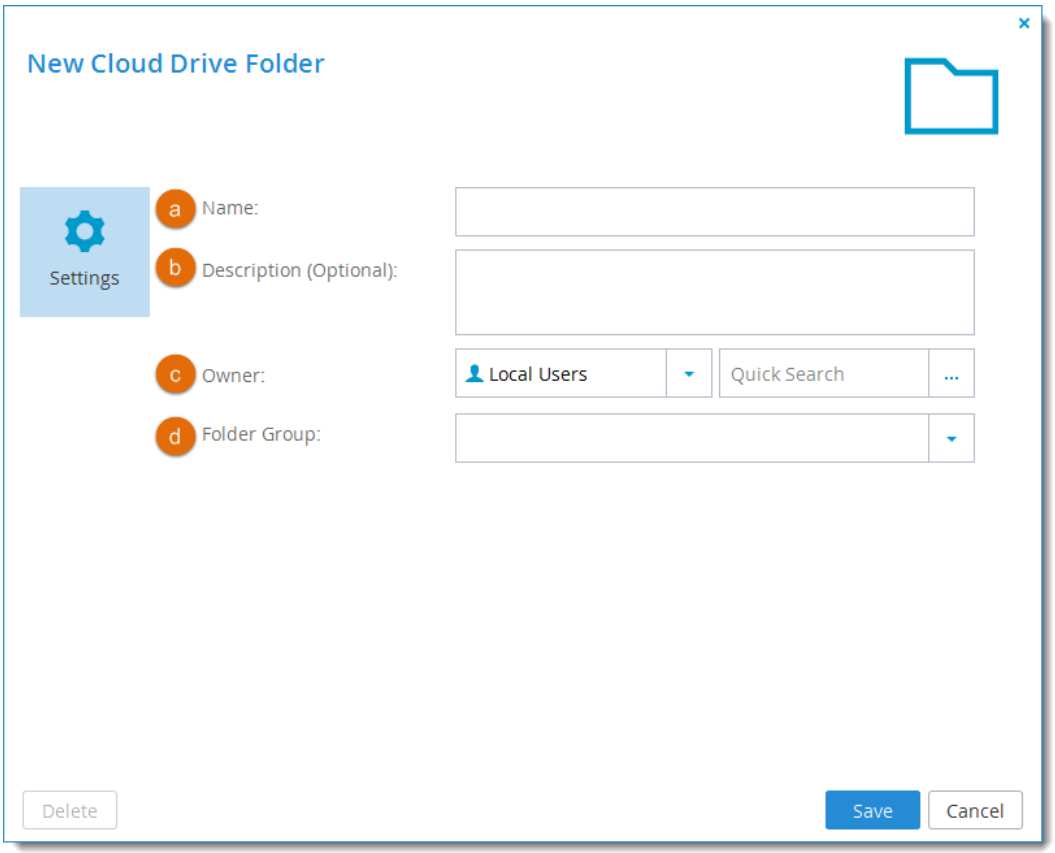
To edit the device, click the device name. For further details, see ***Editing Device Settings*** (on page 24).

g **Is seeding**. Indicates whether the folder is currently in the process of loading a seeding file (Yes/No). While seeding is in progress, backups to this folder are temporarily suspended.

Creating New Cloud Drive Folders

To create a new folder

1 In the **Folders > Cloud Drive Folders** page, click **New**.



2 Complete the fields:

a **Name**. Type a name for the folder.

b **Description**. Optionally type a description for the folder.

c **Owner**. Select the user who should be the owner of the folder. The owner will be able to control access to the folder.

d **Folder Group**. Select a folder group for the folder. For information about folder groups, see ***Managing Folder Groups*** (on page 65).

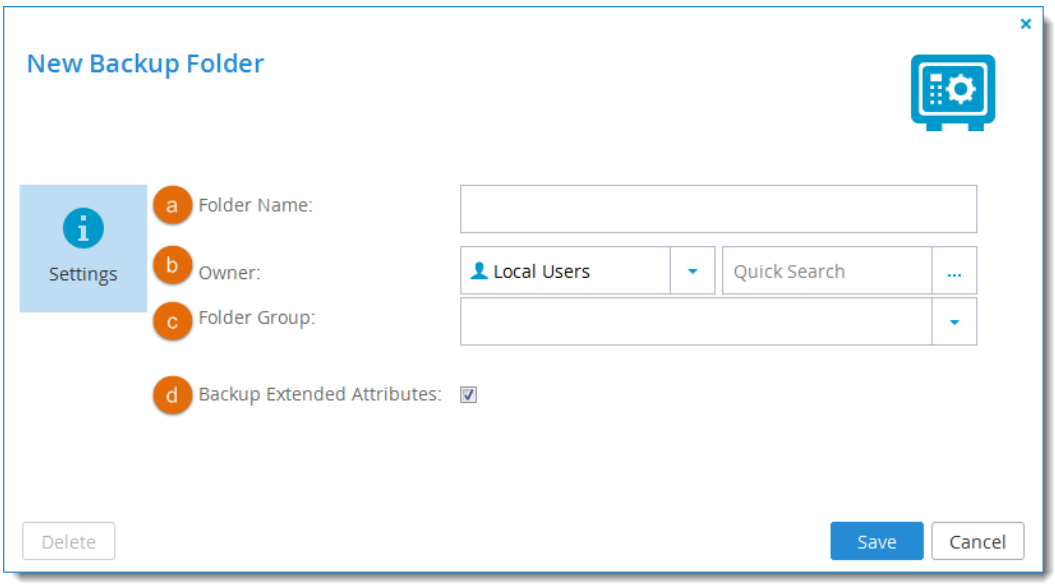
3 Click **Save**.

The new folder is added to the Cloud Drive folders.

Creating New Backup Folders

To create a new folder

1. In the **Folders > Backup Folders** page, click **New**.



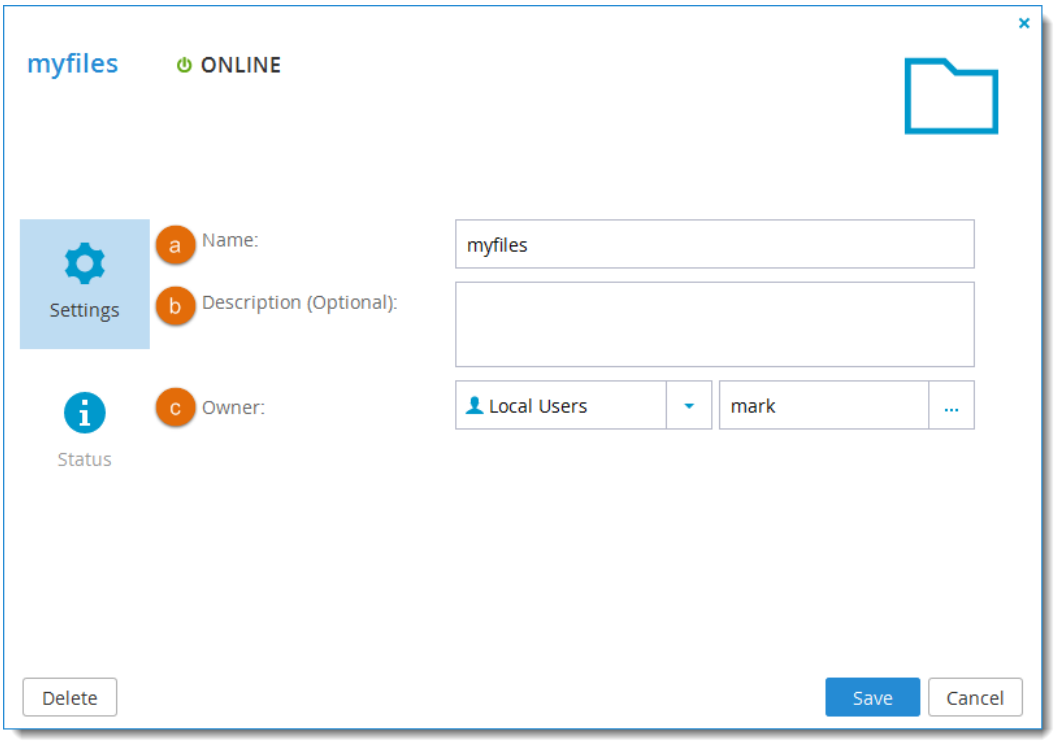
2. Complete the fields:
   - **a** **Folder Name**. Type a name for the folder.
   - **b** **Owner**. Select the user who should be the owner of the folder. The owner will be able to control access to the folder.
   - **c** **Folder Group**. Select a folder group for the folder. For information about folder groups, see ***Managing Folder Groups*** (on page 65).
   - **d** **Backup Extended Attributes**. Select this option to back up special file permissions and metadata.
3. Click **Save**.

   The new folder is added to the Backup folders.

Editing Cloud Drive Folders

To edit a Cloud Drive folder

1 Select the folder in the **Folders > Cloud Drive Folders** page and click **Edit**.



2 Edit the fields as needed:

- **a** **Name**. The name of the folder.
- **b** **Description** (optional). A description for the folder.
- **c** **Owner**. The user who owns the folder. The owner controls access to the folder. Click to select a new user.

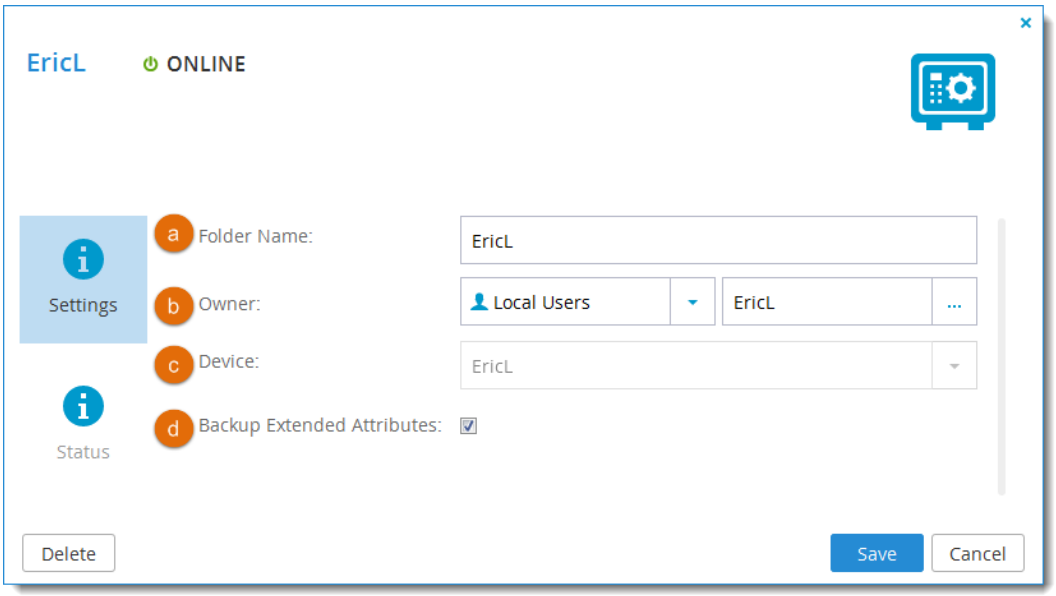
3 Click **Save**.

The changes are saved.

Editing Backup Folders

To edit a backup folder

1 Select the folder in the **Folders > Backup Folders** page and click **Edit**.



2 Edit the fields as needed:

a **Folder Name**.

b **Owner**. you can click on the owner's name to open the User Account Manager and manage the owner's user account. For information on managing user accounts, see ***Managing User Accounts*** (on page 77).

c **Device**. The device with which this folder is associated.

This field is read-only.

d **Backup Extended Attributes**.

3 Click **Save**.

The changes are saved.

Viewing Folder Contents

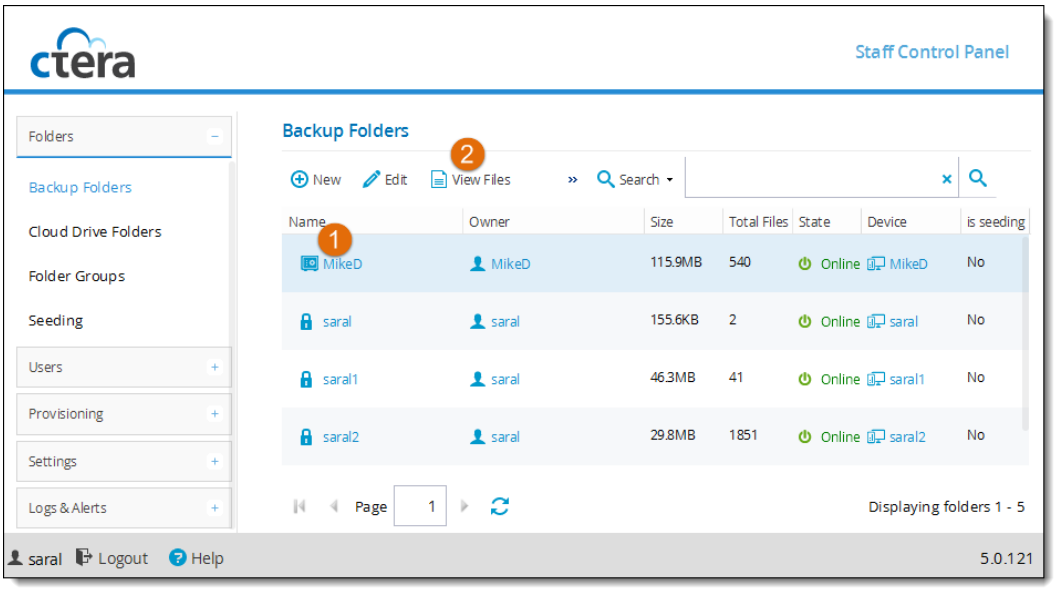
Viewing Backup Folder Contents

Tip

Viewing folder content can be restricted through the *Access End User Folders* attribute in the **Edit Role** dialog. See ***Customizing Administrator Roles*** (on page 109) for details.

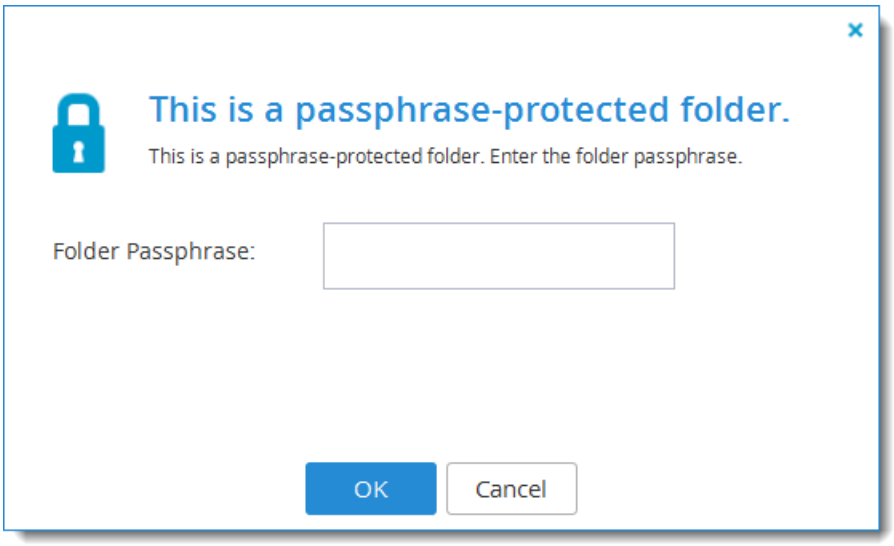
To view a backup folder's content

1. Select the folder in the Backup Folders page.
2. Click **View Files**.



3. If the folder is passphrase-protected, enter the passphrase for accessing for the folder and click **OK**.

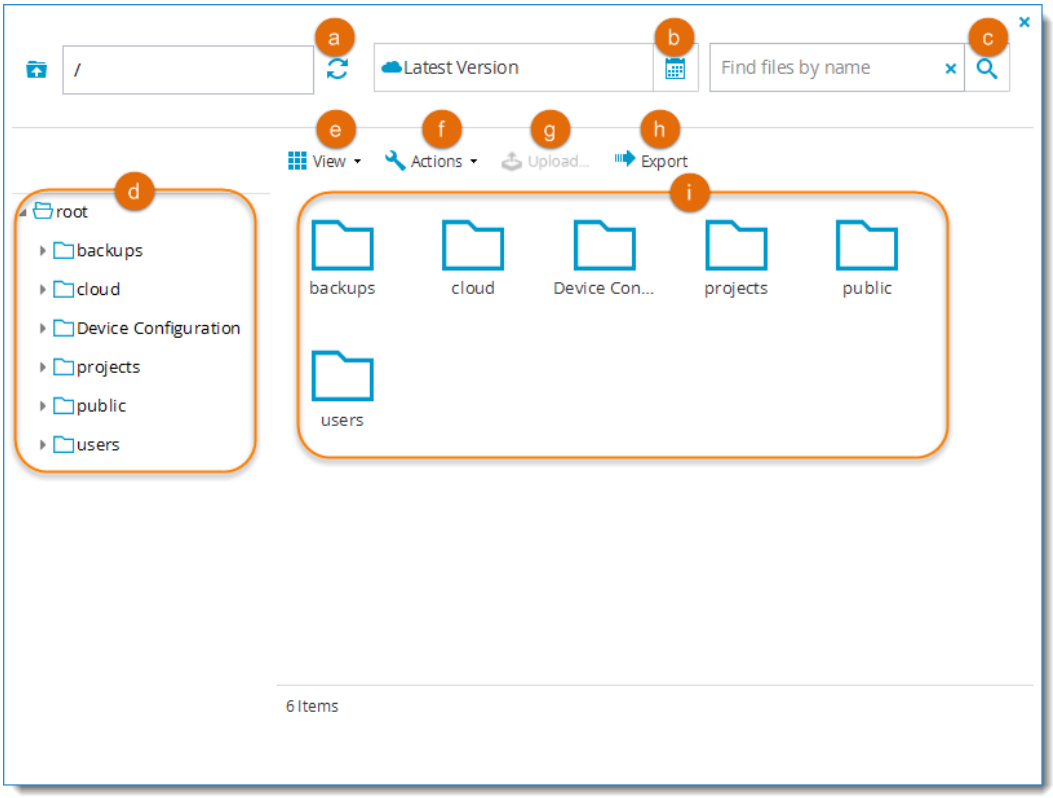
If the folder is passphrase-protected, the **Passphrase Protected Folder** window appears.



Do the following:

1. In the **Folder Passphrase** field, type the passphrase for accessing the folder.
2. Click **OK**.

The **File Manager** window opens displaying files from the last backup operation or snapshot.



a The refresh button. Click to refresh the view.

b Click to navigate to previous versions of up folders.

c Enter a file name to search for a file.

d A tree of the folder content.

e Changes the way folders are displayed in the right pane (i). You can select either icons view or table view.

f Actions menu, providing actions you can do with a selected folder. You must select the folder in the right pane (i) and then the actions become available in the menu.

g Click to upload a file to a folder.

h Click to export the files and folders to a seeding station. To export, you need an empty portable drive connected to a defined export seeding station. Seeding stations are added to the system by global CTERA portal administrators.

i The right pane. Select folders in this pane to perform actions on the folders.

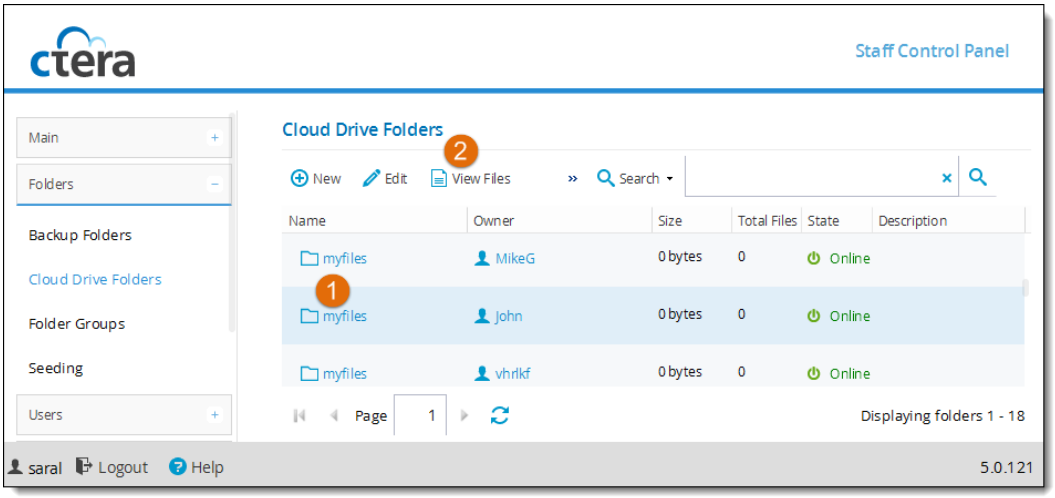
Viewing Cloud Drive Folder Contents

Tip

Viewing folder content can be restricted through the *Access End User Folders* attribute in the **Edit Role** dialog. See ***Customizing Administrator Roles*** (on page 109) for details.

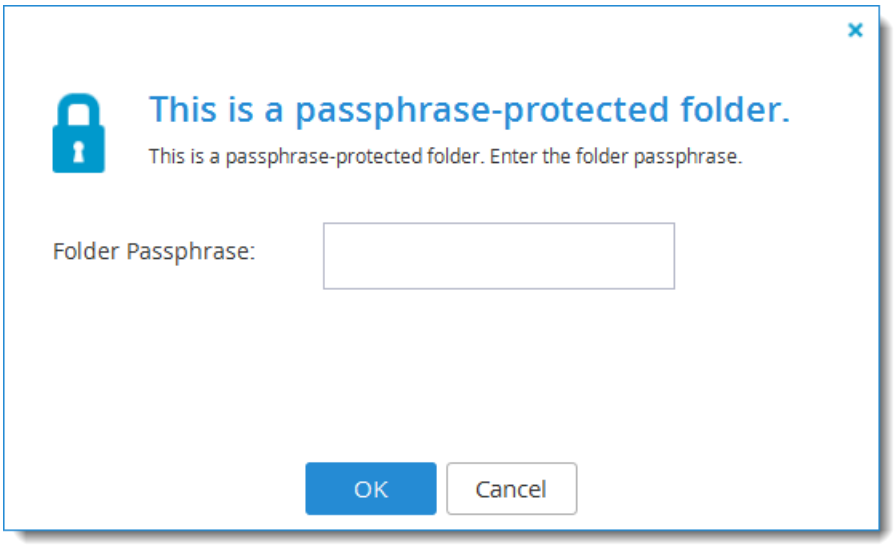
To view a folder's content

1. Select the folder in the Cloud Drive Folders page.
2. Click **View Files**.



3. If the folder is passphrase-protected, enter the passphrase for accessing for the folder and click **OK**.

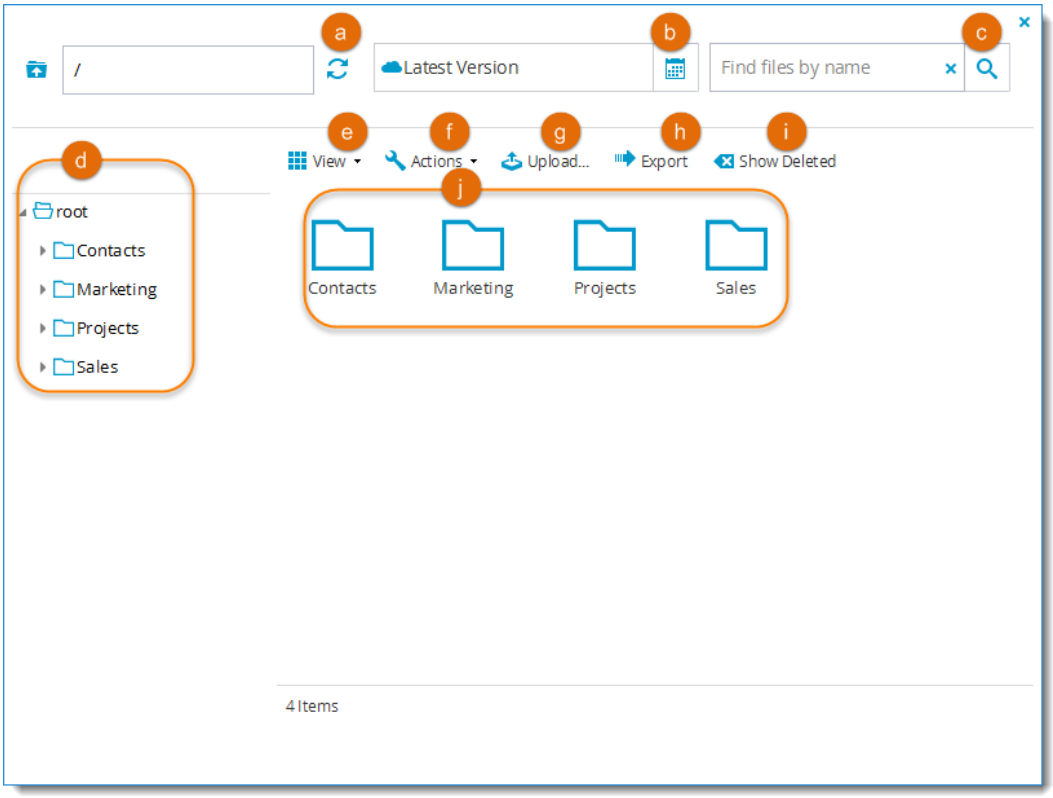
If the folder is passphrase-protected, the **Passphrase Protected Folder** window appears.



Do the following:

1. In the **Folder Passphrase** field, type the passphrase for accessing the folder.
2. Click **OK**.

The **File Manager** window opens displaying files from the last backup operation or snapshot.



a The refresh button. Click to refresh the view.

b Click to navigate to previous versions of up folders.

c Enter a file name to search for a file.

d A tree of the folder content.

e Changes the way folders are displayed in the right pane (j). You can select either icons view or table view.

f Actions menu, providing actions you can do with a selected folder. You must select the folder in the right pane (j) and then the actions become available in the menu.

g Click to upload a file to a folder.

h Click to export the files and folders to a seeding station. To export, you need an empty portable drive connected to a defined export seeding station. Seeding stations are added to the system by global CTERA portal administrators.

i Click to show deleted files.

j The right pane. Select folders in this pane to perform actions on the folders.

Navigating Between Folders

To navigate between folders

Do any of the following:

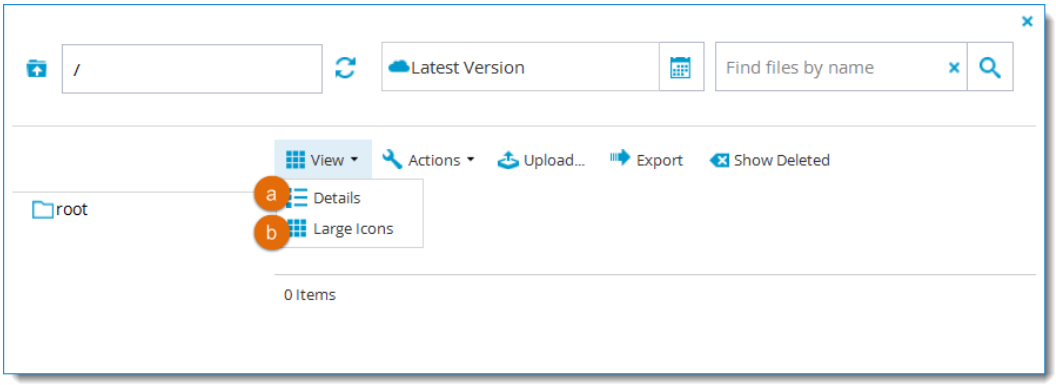
- In the tree pane, expand the nodes and click on the desired folders.
- In the upper bar, type the desired file or folder path.
- To navigate to the parent folder of the currently displayed folder, in the upper bar, click .

The folder's contents appear in the right pane.

Changing the Right Pane View

To change the right pane view

In the right pane, click **View** and then select the desired view.



a **Details**. Displays the items in the right pane in a table. To sort the tables according to the data in one column, click the column's header. To change sort direction, click the column header again.

b **Large Icons**. Displays the items in the right pane as large icons.

Refreshing the View

To refresh the view

- In the upper bar, click  .

  The view is refreshed.

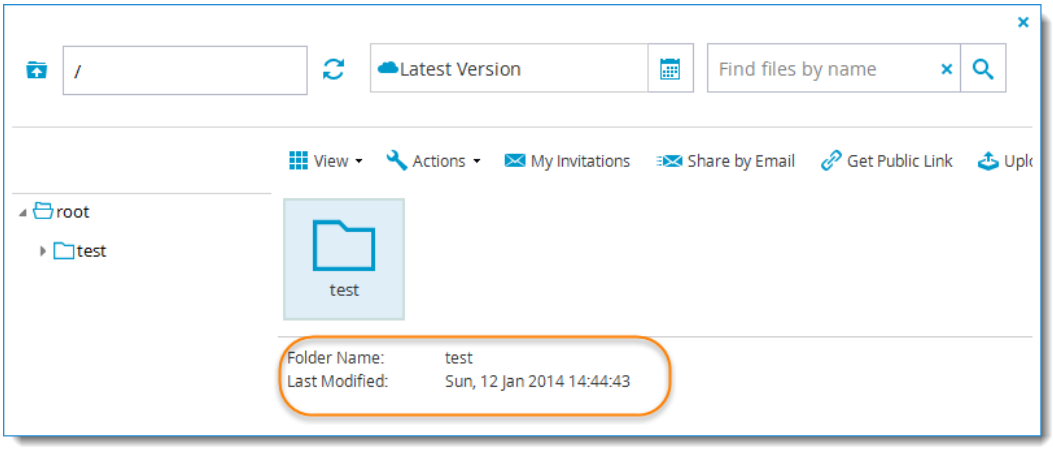
Selecting Files and Folders

- To select a single file/folder, click on the file/folder's row.
- To select multiple files, press and hold the CTRL key, while clicking on the desired files or folders.
- To select all items in the current folder, click **Actions** and then click **Select All**, or press CTRL+A.
- To select a range of files, press and hold the Shift key, click the file at the start of the range, and then click on the file at the end of the range.

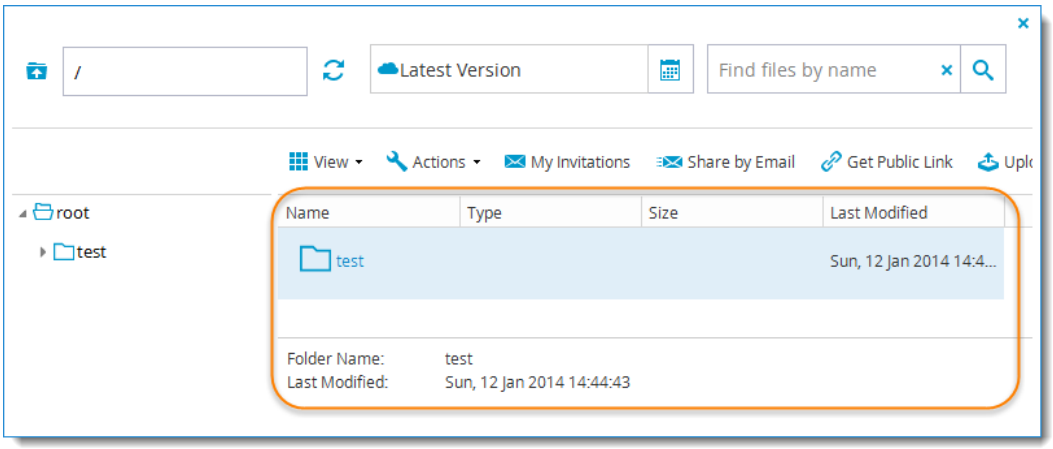
Viewing File or Folder Details

- ***Navigate to the file/folder*** (see "***Navigating Between Folders***" on page 52) and select the file/folder in the right pane.

  In ***Large Icons view*** (see "***Changing the Right Pane View***" on page 52), the file/folder's details appear at the bottom of the right pane.



In ***Details view*** (see "***Changing the Right Pane View***" on page 52), the file/folder's details are displayed in the table as well.



Downloading Files and Folders

- In ***Large Icons view*** (see "***Changing the Right Pane View***" on page 52), double-click the file.
- In ***Details view*** (see "***Changing the Right Pane View***" on page 52), click the file name once.

The file is downloaded to your computer.

Downloading Multiple Files or Entire Folders

1. ***Select the files or folder(s)*** (see "***Selecting Files and Folders***" on page 53).
2. Click **Actions**, and then click **Download**.

The selected files/folders are downloaded to your computer in a .zip file.

Uploading Files

This procedure is relevant for cloud drive folders only.

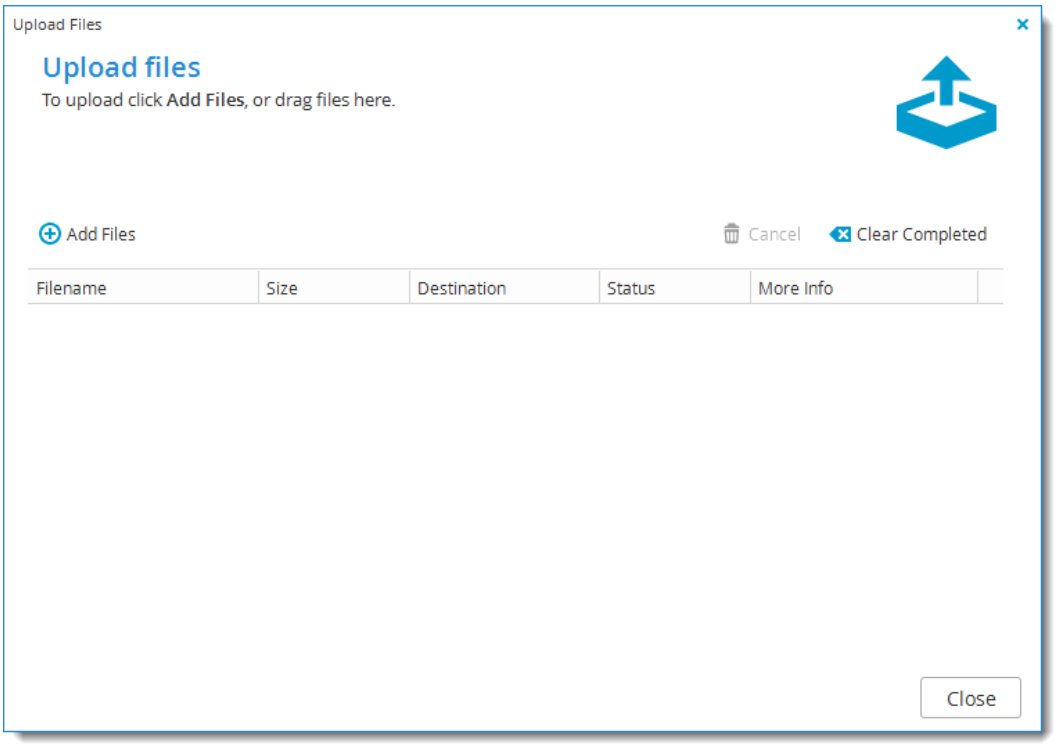
To upload files

1. In the File Manager, navigate to the desired folder.

   See ***Navigating Between Folders*** (on page 52).

2. In the right pane, click **Upload**.

The **Upload files** window appears.

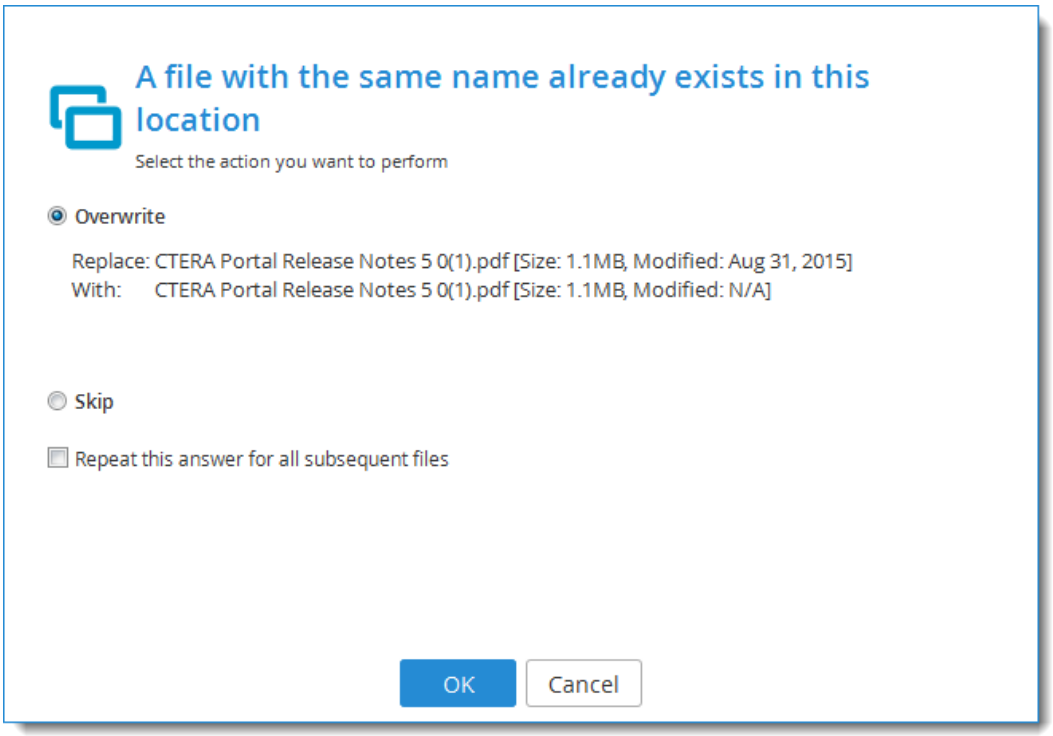


3 For each file you want to upload, do one of the following:

- Click **Add files** and browse to the desired file.
- If using Google Chrome or Mozilla FireFox, drag and drop a file from your computer to the **Upload files** window.

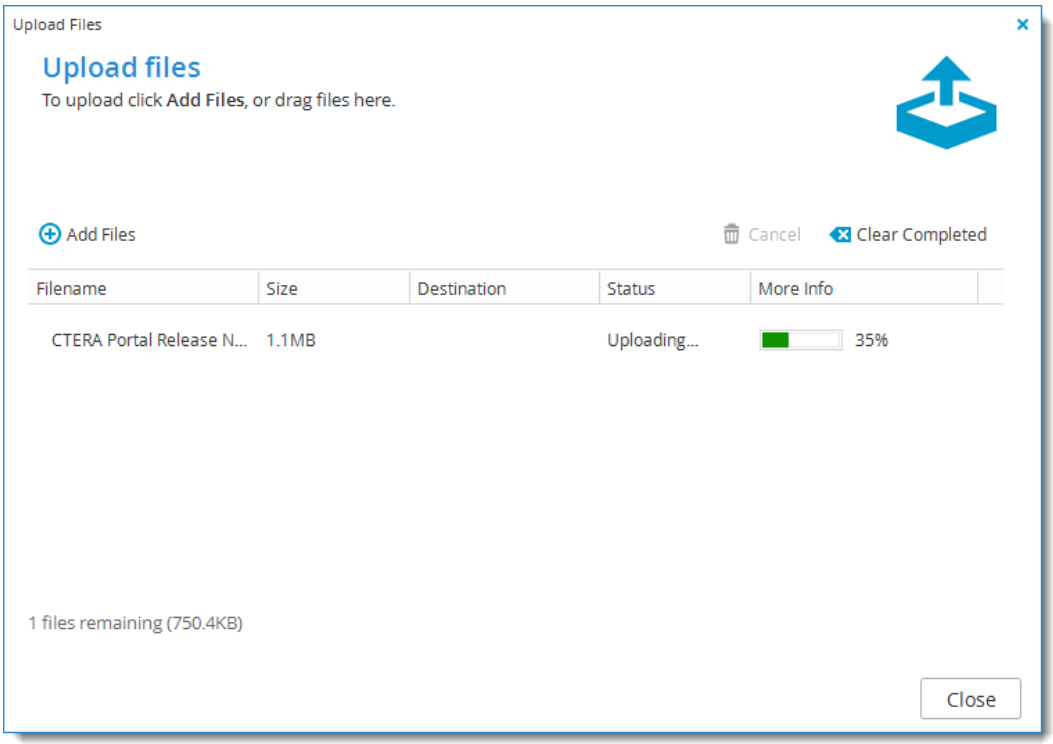
The following things happen:

- If the file already exists, the following window appears.



To overwrite the file in cloud storage with the file on your computer, choose **Overwrite** and click **Ok**. Otherwise, upload of this file will be canceled.

- The file is uploaded, and a progress bar displays the upload progress.



- To cancel an upload, select the file whose upload you want to cancel, and then click **Cancel**.
- To clear the list of completed uploads, click **Clear Completed**.

4. When done uploading all desired files, click **Close**.

Creating New Folders

This procedure is relevant for cloud folders only.

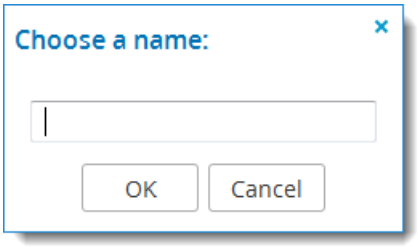
To create a new folder

1. Navigate to the desired parent folder.

   See ***Navigating Between Folders*** (on page 52).

2. Click **Actions** and then click **New Folder**.

   The **Choose a name** dialog box appears.



3. In the field provided, type a name for the new folder.
4. Click **OK**.

Renaming Files and Folders

This procedure is relevant for cloud folders only.

To rename a file or folder

1. Navigate to the desired file/folder.

   See ***Navigating Between Folders*** (on page 52).

2. In the right pane, click on the file/folder's row.
3. Click **Actions** and then click **Rename**.

   The **Choose a name** dialog box appears.

4. In the field provided, type a new name for the file/folder.
5. Click **OK**.

Deleting Files and Folders

Deleting files and folders is supported for cloud folders only. Deleting files and folders is not supported for backup folders.

1. Select the desired file or folder.

   See ***Selecting Files and Folders*** (on page 53).

2. Click **Actions** and then click **Delete**.
3. Click **Yes** to confirm.

   The selected items are deleted.

Copying/Moving Files and Folders

This procedure can be used for a backup folder, only if the backup folder belongs to the same folder group as the user account's cloud folders.

To copy or move files or folders

1. ***Select the files or folder(s).*** (see "***Selecting Files and Folders***" on page 53)
2. Do one of the following:
   - To copy the selected items, click **Actions** and then click **Copy**, or press CTRL+C.
   - To move the selected items, click **Actions** and then click **Cut**, or press CTRL+X.
3. ***Navigate to the target folder.*** (see "***Navigating Between Folders***" on page 52)
4. Click **Actions** and then click **Paste**, or press CTRL+V.

   The selected items are copied/moved to the target folder.

Restoring Files and Folders to Devices

This procedure is relevant for backup folders only.

To restore files or folders to a device

1. In the File Manager, navigate to the desired files/folders.

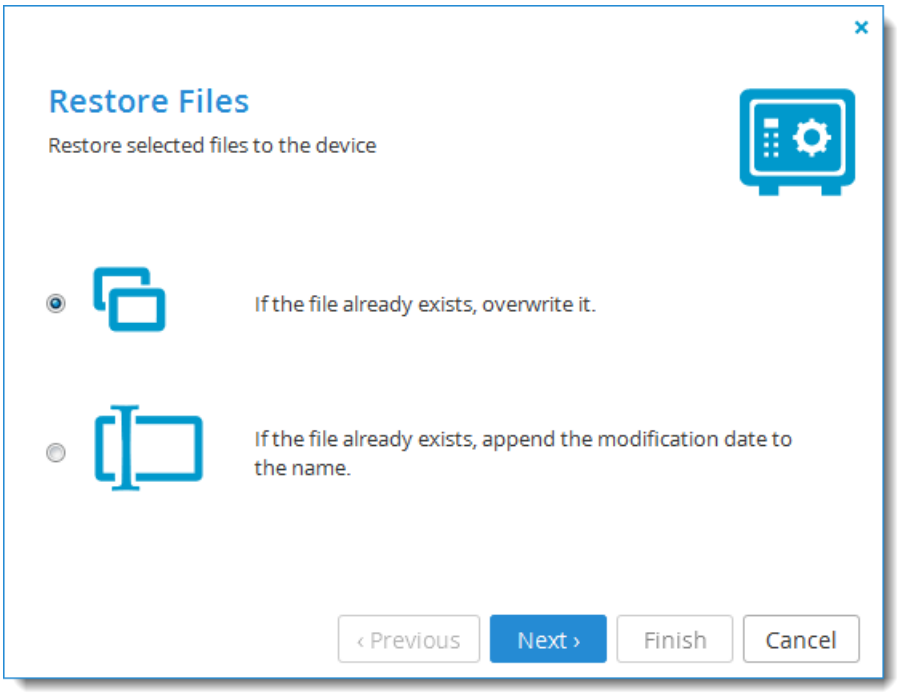
   See ***Navigating Between Folders*** (on page 52).

2. Select the desired file or folder.

   See ***Selecting Files and Folders*** (on page 53).

3. Click **Actions** and then click **Restore to Device**.

The **Restore Files** dialog box appears.

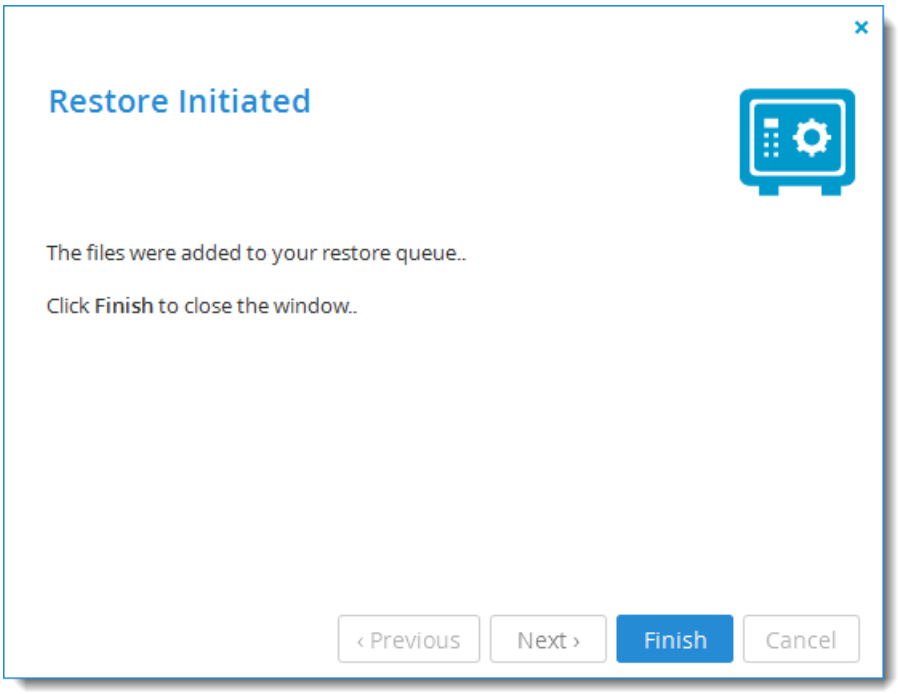


4 Specify how to handle files that already exist on the device, by doing one of the following:

- To specify that the files on the device should be overwritten by the files in the portal, choose **If the file already exists, overwrite it**.
- To specify that the files on the device should have the modification date appended to their name, choose **If the file already exists, append the modification date to the name**.

5 Click **Next**.

The **Restore Initiated** screen appears.



6 Click **Finish**.

A progress bar appears, and the files are restored to the device.

Searching for Files

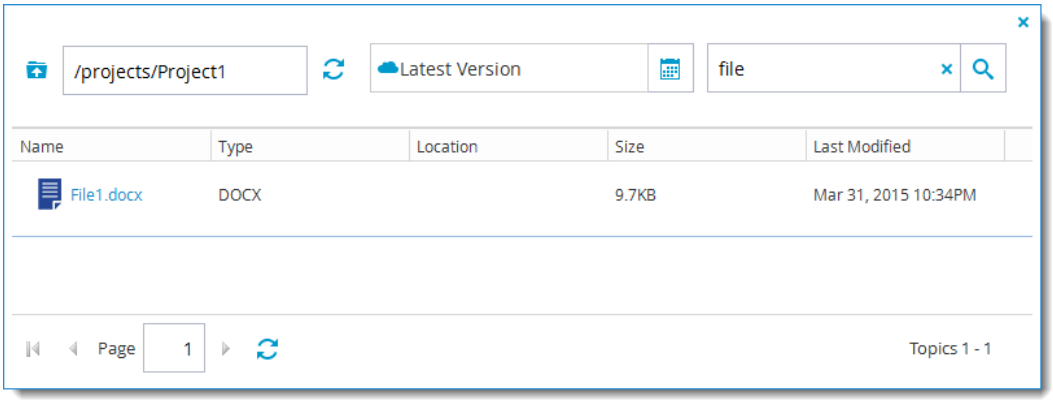
If full text search is enabled on the device, you can search for files containing specific text, located anywhere in the document's file name.

To search for files

1 In the File Manager's upper bar, in the **Find files by name** field, type the text you want to search for.

2 Click .

The search results appear.



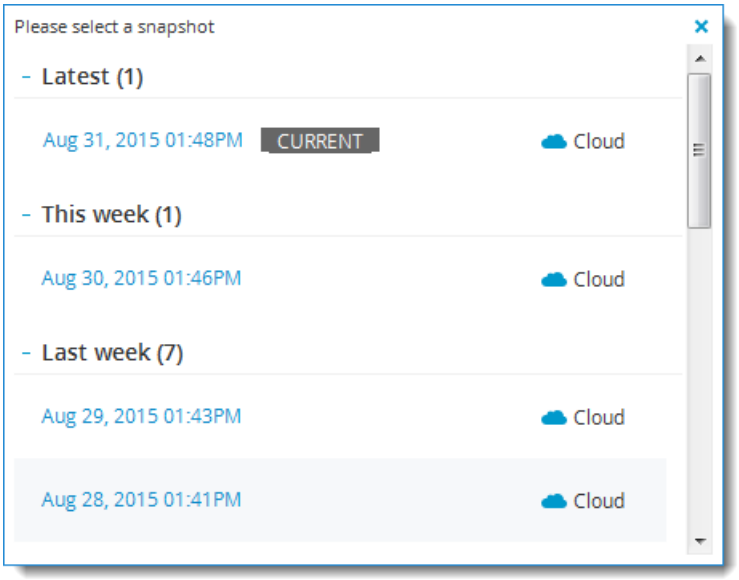
3. To download a file appearing in the search results, click on its name.
4. To clear the search results, click ×.

Viewing Previous Versions of Files and Folders

To view previous versions of files and folders

1. In the File Manager's upper bar, click .

   The **Please select snapshot** window opens.



2. Click on the snapshot containing the file/folder versions you want to view.

   Latest Version contains the current version of files and folder in cloud backup. The snapshots are marked according to their type: NEXT3 ( ) or cloud ( ).

   The snapshot contents appear, and you can view and download them. You can also copy and paste them to the Latest Version.

Changing Passphrases for Accessing Backup Folder Contents

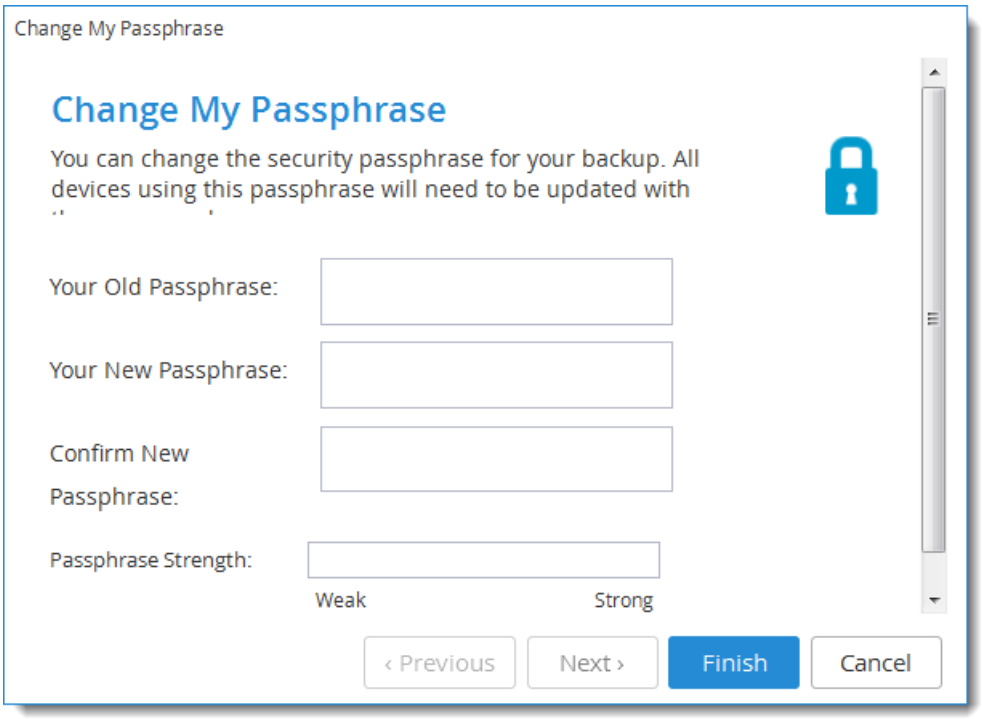
To change a passphrase

1. Do one of the following:

   - In the **Folders > Backup Folders** page, select the desired folder's row, and then click **Change Passphrase**.
   - In the File Manager, click **Actions**, and then click **Change Passphrase**.

   See ***Viewing Folder Contents*** (on page 48).

The **Change My Passphrase** dialog box appears.



2. In the **Your Old Passphrase** field, type the folder's old passphrase.
3. In the **Your New Passphrase** and **Confirm New Passphrase** fields, type a new passphrase.

   The **Passphrase Strength** area displays the passphrase's strength.
4. Click **Finish**.
5. Do one of the following:
   - If cooperative de-duplication is disabled, you will need to update the passphrase on the device associated with this folder, to enable the device to access the folder.
   - If cooperative de-duplication is enabled (which is the default), you will need to update the passphrase on all devices using this folder group.

Exporting Folders to Excel

You can export a list of folders and their details to a Comma Separated Values (*.csv) file on your computer, which you can open in Microsoft Excel.

To export folders to Excel

- Do one of the following:
  - To export cloud drive folders, in the **Folders > Cloud Drive Folders** page, click **Export to Excel**.
  - To export backup folders, in the **Folders > Backup Folders** page, click **Export to Excel**.

The folders are exported.

Deleting Folders

To delete a folder

1. Do one of the following:
   - To delete a cloud drive folder, in the **Folders > Cloud Drive Folders** page, select the desired folder's row, then click **Delete Folder**.
   - To delete a backup folder, in the **Folders > Backup Folders** page, select the desired folder's row, then click **Delete Folder**.
2. Click **Yes** to confirm.

   The folder is deleted.

6

Managing Folder Groups

In This Chapter

Overview

CTERA Portal organizes cloud folders in *folder groups.* Each folder group acts as a de-duplication realm. De-duplication means that when files are written to a folder in a folder group, the files' content is compared to data already stored in *other* folders in the same folder group. Only the data that *differs* from existing data in the other folders is stored in the folder group. In other words, similar data is only stored once. This accelerates the file transfer, and saves storage space.

Folder groups are organized according to each user's de-duplication level for backup folders and for Cloud Drive folders.

For backup folders and for Cloud Drive folders, you can set the de-duplication level to any of the following:

- **User**

  A single folder group is created for each user account, containing all of the user account's backup/cloud folders. De-duplication is performed for the user account's folder group. Therefore, if a user owns multiple devices, and the devices back up similar data, the similar data will only be stored once.

- **Folder**

A folder group is created for each of a user account's devices, containing all of the device's backup/cloud folders. De-duplication is performed separately for each of the user account's folder groups.

Portal

A single folder group is shared by *all* user accounts in the portal. The folder group acts as a de-duplication realm that spans the entire portal. In other words, if different users' devices back up similar data, the similar data will only be stored once.

You can change the default deduplication levels for any user created in the portal, and you can change any user's deduplication levels. You can choose a different level for backup folders and for Cloud Drive folders.

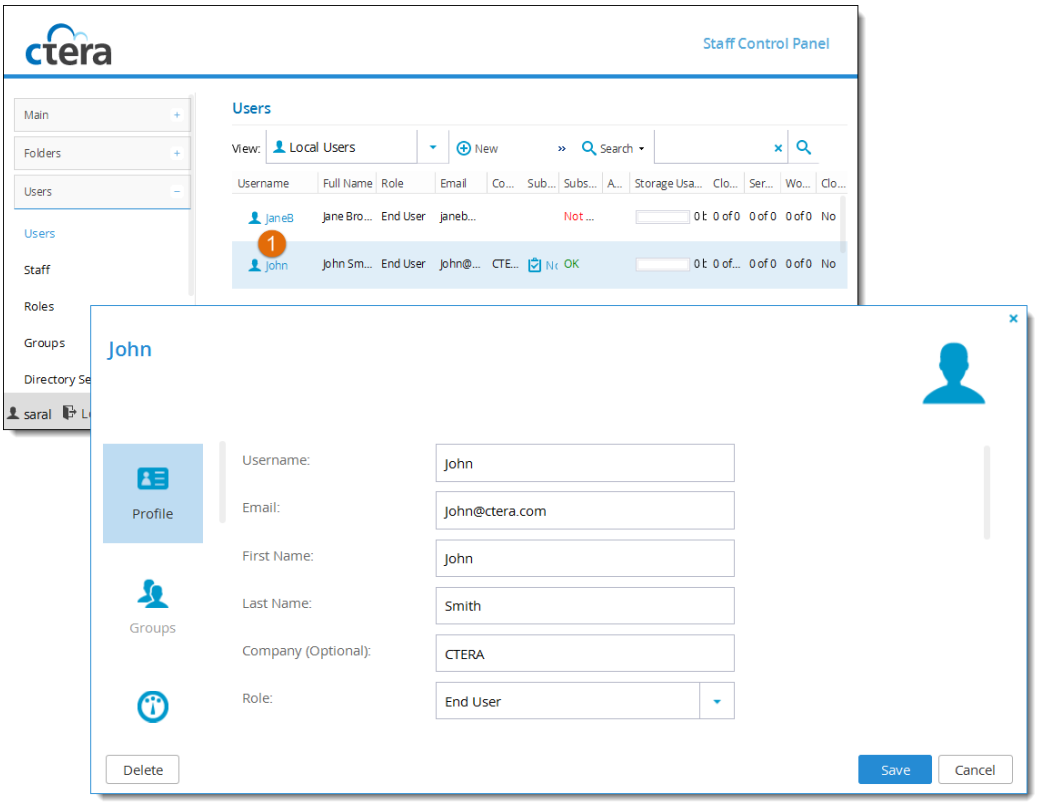
Tip

All folders in a folder group must use the same encryption key and passphrase.

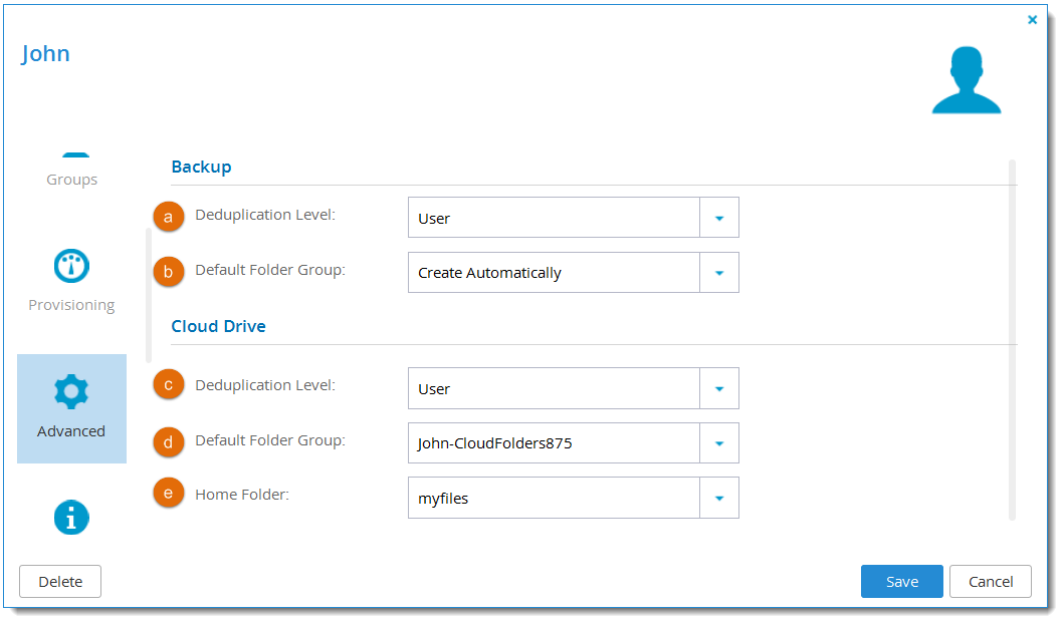
Changing a User's Deduplication Level

To change deduplication levels for a user's folders

1 Select **Users > Users** from the menu, and click the user's username.



2 Select the **Advanced** tab and change the deduplication levels for Backup and Cloud Drive folders:



Backup

a **Deduplication Level**. Specify the default de-duplication level to use for new backup folders. Select one of the following:

- **User** (default). Create a single folder group for the user account, containing all of the user account's backup folders. De-duplication is performed for the user account's folder group.
- **Folder**. Create a folder group for each of the user account's devices, containing all of the device's backup folders. De-duplication is performed separately for each of the user account's folder groups.

b **Default Folder Group**. Appears only if **User** is selected as the *Deduplication Level*. Select the default folder group to use for all of the user account's backup folders. This can be either of the following:

- An existing folder group
- **Create Automatically** (default). Automatically create a new folder group.

Cloud Drive

c **Deduplication Level**. Specify the default de-duplication level to use for new cloud folders. Select one of the following:

- **User** (default). Create a single folder group for the user account, containing all of the user account's cloud folders. De-duplication is performed for the user account's folder group.

- **Folder**. Create a folder group for each of the user account's devices, containing all of the device's cloud folders. De-duplication is performed separately for each of the user account's folder groups.

d **Default Folder Group**. Appears only if **User** is selected as the *Deduplication Level*. Select the default folder group to use for all of the user account's cloud folders. This can be either of the following:

- An existing folder group
- **Create Automatically** (default). Automatically create a new folder group.

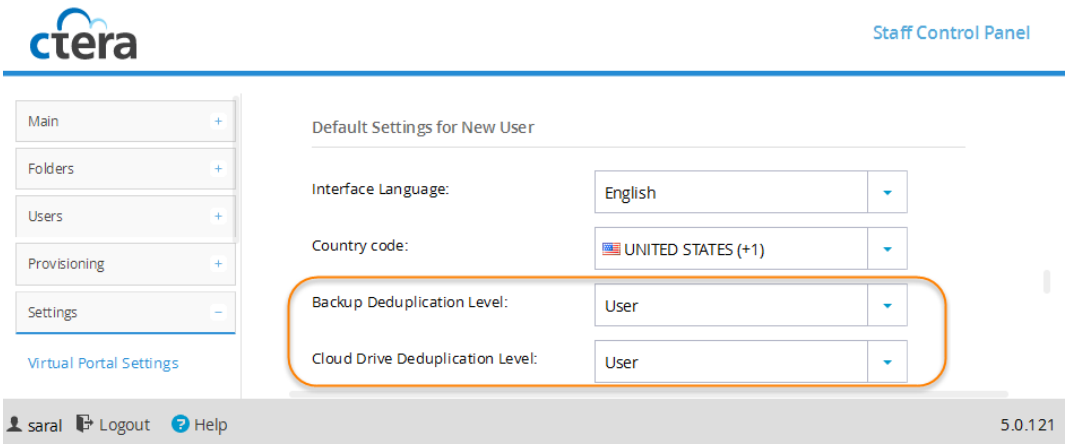
e **Home Folder**. Select one of the user's personal folders to act as the user's home folder. The home folder is a personal folder that is linked to the user account and cannot be deleted.

Changing the Default Deduplication Level

To change the default deduplication levels for users in the portal

1 Select **Settings > Virtual Portal Settings** from the menu.

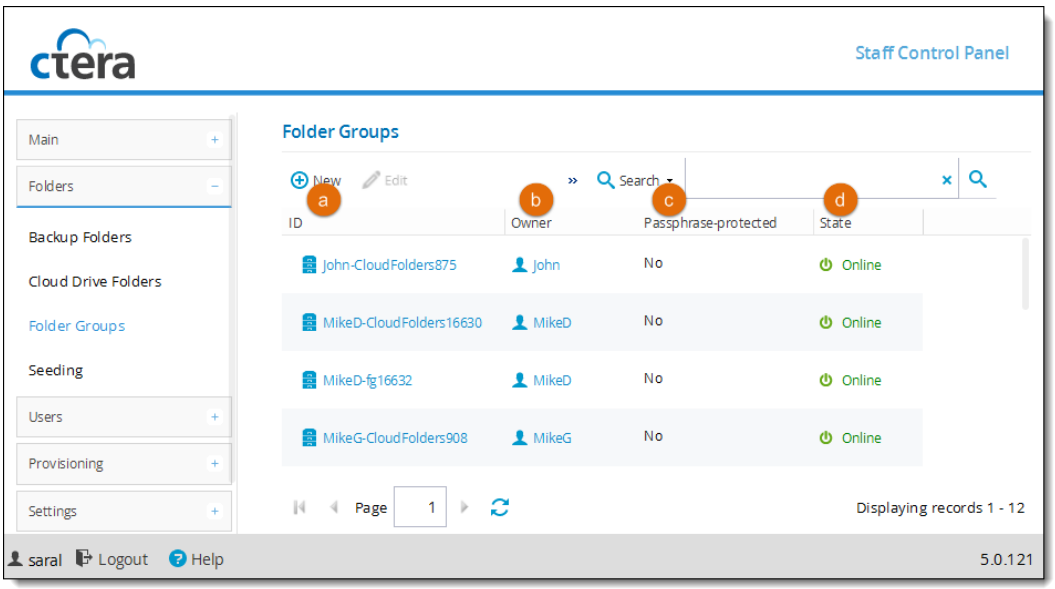
2 Scroll down to **Default Settings for New User**. and you can change the **Backup Deduplication Level** and the **Cloud Drive Deduplication Level**. These are the default settings used for all new users.



Viewing Folder Groups

To view all folders groups in the portal

Select **Folders > Folder Groups** from the menu.



a **ID**. The folder group's name.

To edit the folder group's name, click the folder group name. For further details, see ***Adding and Editing Folder Groups*** (on page 70).

b **Owner**. The user account name of the folder group's owner.

To edit the user account, click the user account name. For further details, see ***Editing User Profiles*** (on page 83).

c **Passphrase-protected**. Indicates whether the folder group is passphrase-protected or not (Yes / No).

d **State**. The folder group's state (Online / Offline).

Adding and Editing Folder Groups

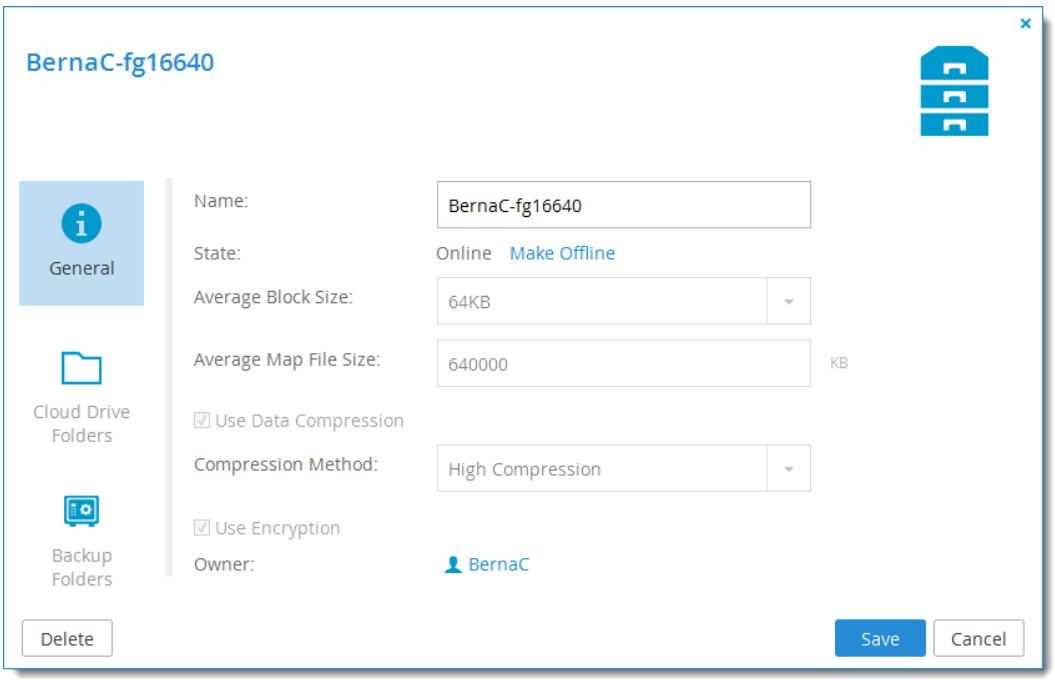
When a device first backs up files to the CTERA Portal, and cooperative de-duplication is enabled for the device's owner, a folder group is automatically created. By default, the folder group is assigned a name based on the device's name. If desired, you can add new folder groups manually, and you can edit their properties.

To add or edit a folder group

1. Do one of the following:

   - To add a new folder group, browse to the **Folders > Folder Groups** page, and click **New**.
   - To edit an existing folder group, .
   - Select the desired folder group's row and click **Edit**.
   - Click on the folder group's name.

   The Folder Group Manager opens displaying the **General** tab.



   The Folder Group Manager opens displaying the **General** tab.

2. Complete the fields using the information in the following table.
3. Click **Save**.

Table 4: Folder Group Manager General Fields

In this field...	Do this...
Name	Type a name for the folder group.
State	Select the folder group's state. This can have the following values: **Online**. The folder group is online, and it is possible to view, modify, and back up files to its member folders. **Offline**. The folder group is offline, and it is not possible to view, modify, and back up files to its member folders. Folder groups may be taken offline during some maintenance operations, such as when repairing a folder using the CTERA Cloud FSCK utility. All member folders will inherit the folder group's state.
Average Block Size	The average block size used by the folder group. This field is editable, when manually creating a new folder group. Otherwise, it is read-only, and its value is inherited from the definition of the selected Cloud FS version in the virtual portal's settings. See ***Configuring Virtual-Portal Settings*** (see "***Configuring Virtual Portal Settings***" on page 163). Changing this value for an existing folder group does not affect blocks already existing in the folder group.
Average Map File Size	The average map file size used by the folder group. This field is editable, when manually creating a new folder group. Otherwise, it is read-only, and its value is inherited from the definition of the selected Cloud FS version in the virtual portal's settings. See ***Configuring Virtual-Portal Settings*** (see "***Configuring Virtual Portal Settings***" on page 163).
Use Data Compression	This field indicates whether data in this folder group will be stored in compressed format. This field is editable, when manually creating a new folder group. Otherwise, it is read-only, and its value is inherited from the definition of the selected Cloud FS version in the virtual portal's settings. See ***Configuring Virtual-Portal Settings*** (see "***Configuring Virtual Portal Settings***" on page 163).

Compression Method	If the **Use Data Compression** setting is enabled, specify the default compression method to use for file storage. Select one of the following: **High Compression** **High Speed** The default value is **High Speed**. This field is editable, when manually creating a new folder group. Otherwise, it is read-only, and its value is inherited from the virtual portal's settings. See ***Configuring Virtual-Portal Settings*** (see "***Configuring Virtual Portal Settings***" on page 163).
Use Encryption	This field indicates whether data in this folder group will be stored in encrypted format. This field is editable, when manually creating a new folder group. Otherwise, it is read-only, and its value is inherited from the virtual portal's settings. See ***Configuring Virtual-Portal Settings*** (see "***Configuring Virtual Portal Settings***" on page 163).
Owner	When adding a new folder group, select an owner for the folder group. When editing an existing folder group, you can click on the owner's name to open the User Account Manager and manage the owner's user account. For information on managing user accounts, see ***Managing User Accounts*** (on page 77).

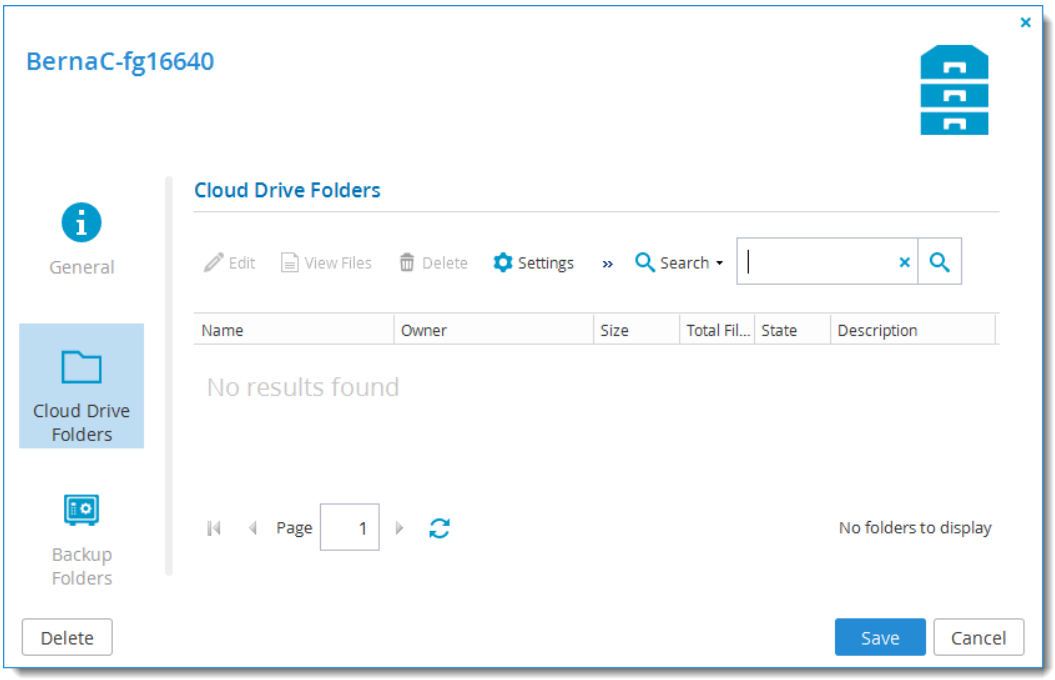
Managing Cloud Drive Folders for Folder Groups

You can manage the cloud drive folders in a folder group.

To manage cloud drive folders in a folder group

1. Click the folder group's name to open the Folder Group Manager for the folder.
2. Click the **Cloud Drive Folders** tab.

The **Cloud Drive Folders** tab appears with a table of cloud drive folders in the folder group.



3 Perform any of the folder management tasks described in Managing Folder Contents, as if you were working in the **Folders > Cloud Drive Folders** page.

Managing Backup Folders for Folder Groups

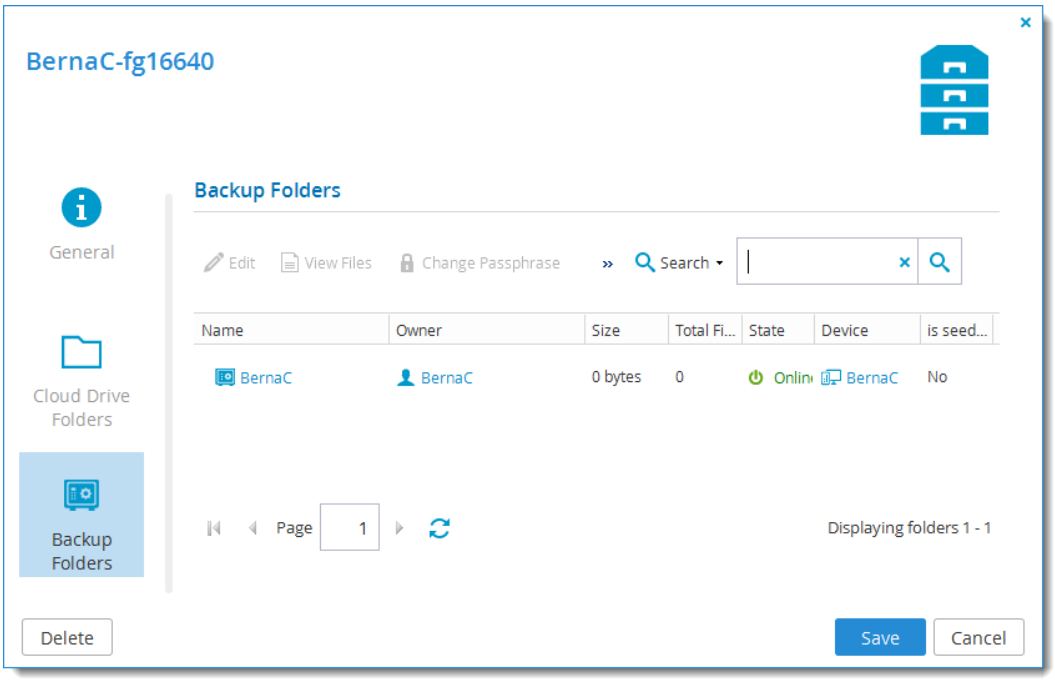
You can manage the backup folders in a folder group.

To manage backup folders in a folder group

1 Click the folder group's name to open the Folder Group Manager for the folder.

2 Click the **Backups** tab.

The **Backups** tab appears with a table of backup folders in the folder group.



3 Perform any of the backup folder management tasks described in ***Managing Folders*** (on page 41), as if you were working in the **Folders > Backup Folders** page.

Changing Passphrases for Accessing Folder Group Contents

Warning

Changing the passphrase for a folder group will cause all devices using folders in the folder group to be unable to backup files, until the backup service has been re-configured with the new passphrase in the devices' administration interfaces.

To change a passphrase

1 Select **Folders > Folder Groups** from the menu.

The **Folders > Folder Groups** page appears, displaying all folder groups.

2 Select the desired folder group's row.

3 Click **Change Passphrase**.

The **Change My Passphrase** dialog box appears.

4 In the **Your Old Passphrase** field, type the folder group's old passphrase.

5 In the **Your New Passphrase** and **Confirm New Passphrase** fields, type a new passphrase.

The **Passphrase Strength** area displays the passphrase's strength.

6 Click **Finish**.

7 For each device using a folder in this folder group, do the following:

a Log in to the device's administration interface.

See ***Remotely Managing Devices*** (on page 27).

b Run the **Backup Setup Wizard** and enter the new passphrase.

Exporting Folder Groups to Excel

You can export a list of folder groups and their details to a Microsoft Excel (*.xls) file on your computer.

To export folder groups to Excel

1 In the navigation pane, click **Folders > Folder Groups**.

The **Folders > Folder Groups** page appears, displaying all folder groups.

2 Click **Export to Excel**.

The folder groups are exported.

Deleting Folder Groups

To delete a folder group

1 Do one of the following:

- In the **Folders > Folder Groups** page, select the desired folder group's row, then click **Delete**.
- Click the folder group name to open the folder group's manager, and then click **Delete**.

2 Click **Yes** to confirm.

The folder group is deleted.

7

Managing User Accounts

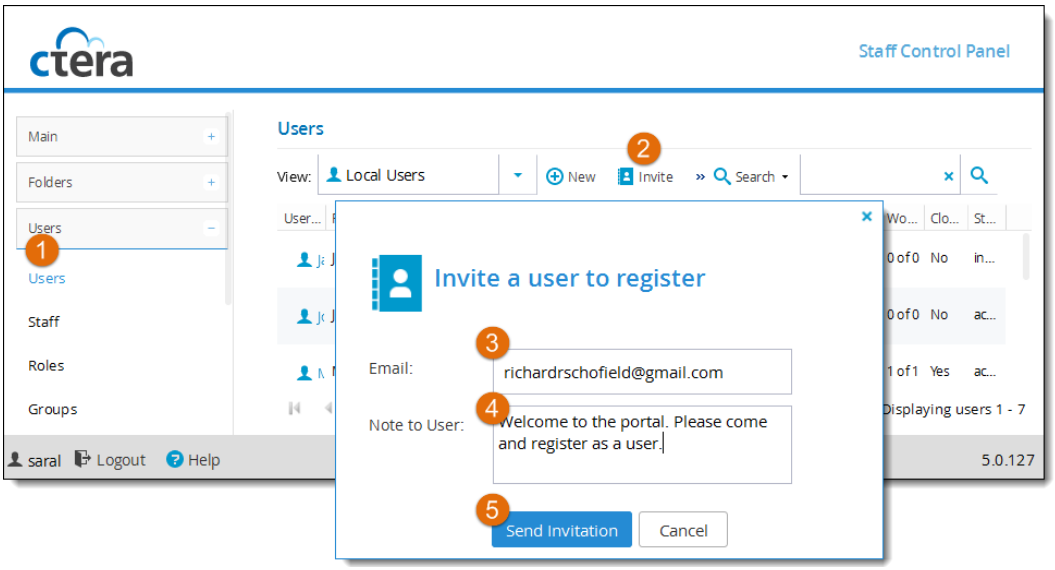
End users are registered with the CTERA Portal and have access to the End User Portal. Each user is represented in the CTERA Portal by a *user account*.

In This Chapter

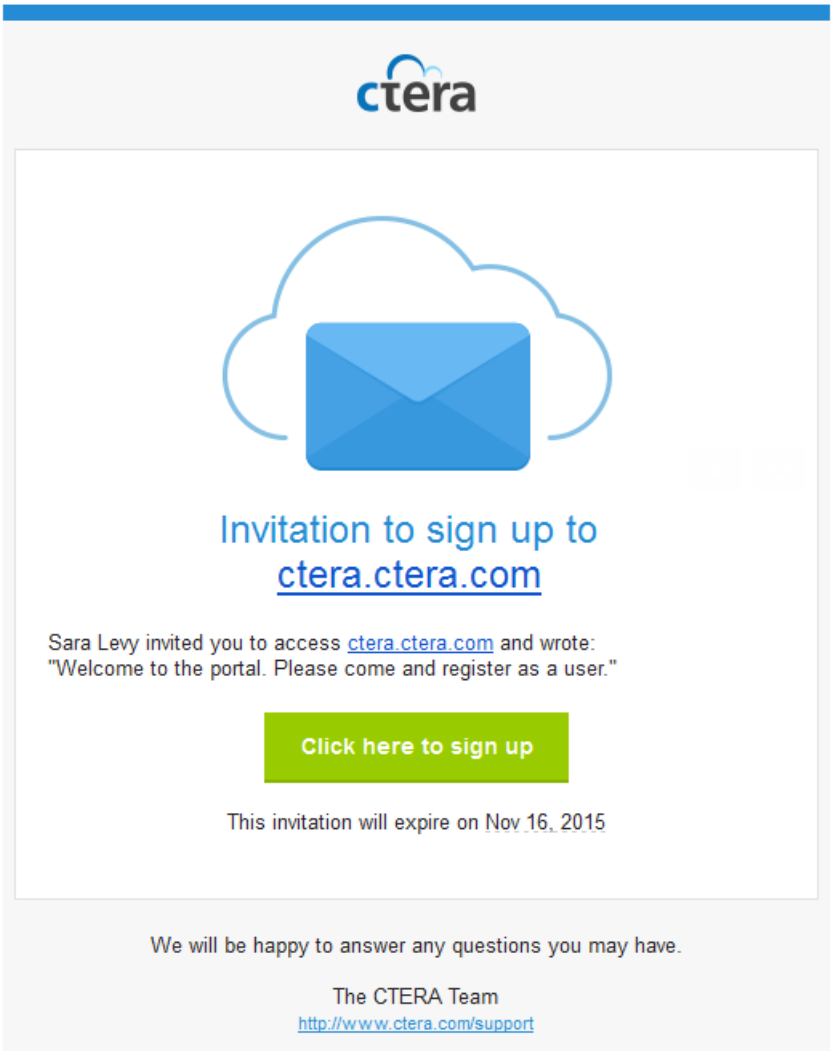
Inviting Users to Register

1. Browse to **Users > Users**.
2. Click **Invite**.
3. In the **Email** field, enter the email address of the person you want to invite to register.
4. In the **Note to User** field, enter any message you want to send to the user.

5 Click **Send Invitation**.



The person you invited receives an invitation by email with a link to complete the registration.



The user clicks the link to the portal, registers account details and then receives an email to activate their account. Portal administrators receive email notifications that the user has registered.

- To control the expiration period of registration invitations, go to **Settings > Virtual Portal Settings** and scroll down to User Registration.
- To change the relevant email templates, see ***Configuring Email Templates*** (on page 221).

Viewing User Accounts

To view all user accounts in the portal

1 Browse to **Users > Users**.

a **Username**. The user account's user name.

To edit the user, click the user name.

b **Full Name**. The user's full name.

c **Role**. The user's role.

d **Email**. The user's email address.

e **Company**. The name of the user's company.

f **Subscription Plan**. The user account's assigned subscription plan.

To modify the subscription plan, click the plan's name. For further details, see ***Adding and Editing Subscription Plans*** (see "***Adding and Editing Plans***" on page 140).

g **Subscription Status**. The user account's subscription status. This can be any of the following:

- **Expired on date**. The subscription plan expired on the specified date.

- **Expires in days**. The subscription plan will expire in the specified number of days. This status is only relevant when the plan will expire within 30 days.
- **Expiration date**. The subscription plan will expire on the specified date. This status is relevant when the plan will expire in more than 30 days.
- **Not Subscribed**. The user is not subscribed to a plan.
- **OK**. The subscription will not expire within 30 days.

h **Add Ons**. The number of add-ons for the user account.

To modify the list of add-ons, click on the number. For further details, see ***Adding and Editing Add-ons*** (on page 151).

i **Storage Usage**. A bar graph indicating the amount of storage the user has consumed out of the total amount provisioned.

j **Cloud Gateway Licenses**. The number of cloud gateways associated with the user account out of the total amount provisioned.

k **Server Agent Licenses**. The number of CTERA Server Agents installed out of the total amount provisioned.

l **Workstation Backup Licenses**. The number of CTERA Workstation Agents installed and using the Cloud Backup service out of the total amount provisioned.

m **Cloud Drive**. Whether or not the user has the Cloud Drive service.

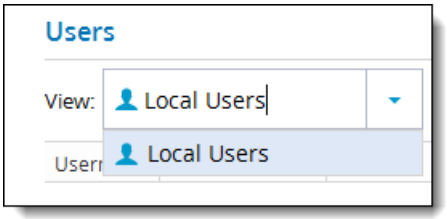
n **Status**. The user's account status. This can be either of the following:

- **active**. The account is active, and the user can access the CTERA Portal.
- **inactive**. The account is inactive, and the user cannot access the CTERA Portal.

Filtering the View

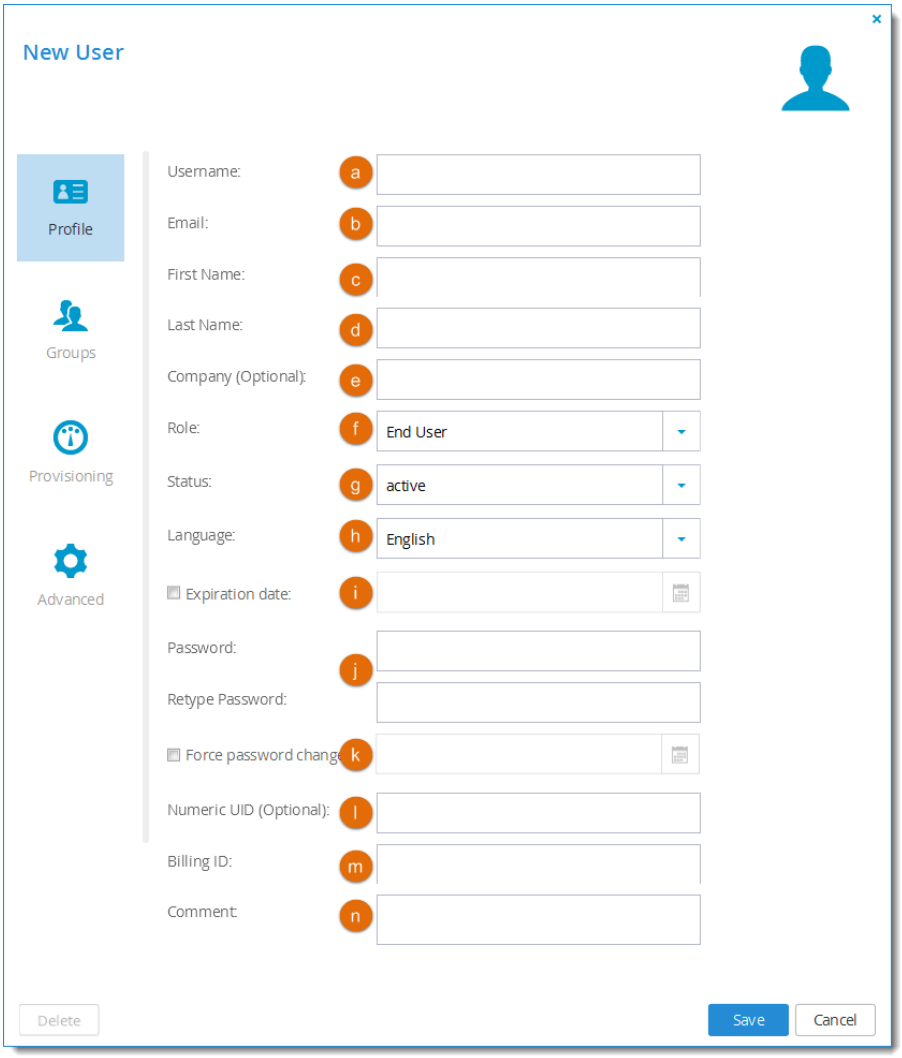
To view only a specific type of users, in the **View** drop-down list, select:

- A domain name, to view only users of a specific domain.
- **Local Users**, to view users defined in the local user database.



Adding New Users

1 Browse to **Users > Users**, and click **New**.



2 Complete the fields in the **Profile** tab:

a **Username**. Type a user name for the user's CTERA Portal account.

b **Email**. Type the user's email address.

c **First Name**. Type the user's first name.

d **Last Name**. Type the user's last name.

e **Company** (optional). Type the name of the user's company.

f **Role**. Select the user's role. This can be either of the following:

- **Read/Write Administrator**. The user can access the End User Portal, and can access the Staff Control Panel with read-write permissions.

- **Read Only Administrator**. The user can access the End User Portal, and can access the Staff Control Panel with read-only permissions.
- **End User** (default). The user can access the End User Portal.
- **Disabled**. The user account is disabled. The user cannot access the End User Portal.

Tip

In order to access the End User Portal, the user must have a role other than Disabled, and their status must be active.

g **Status**. Select the account status. This can be either of the following:

- **active**. The account is active, and the user can access the CTERA Portal.
- **inactive**. The account is inactive, and the user cannot access the CTERA Portal.

The default value for new users created by an administrator is *active*.

The default value for invited users is *inactive*. The status changes to *active* when the invited user activates the account.

h **Language**. The user's interface language.

i **Expiration date**. The expiration date of the user account.

j **Password / Retype Password**. Type a password for the user's CTERA Portal account. Password requirements depend on the password policy, which can be overridden and modified in the **Virtual Portal Settings** (Browse to **Settings > Virtual Portal Settings** and scroll down to **Password Policy**).

k **Force password change**. Check the box to specify an expiration date for the user's password, then click  to select the date. When the password has expired, the user will be required to configure a new password upon their next login.

l Numeric UID (Optional). Type a numeric user ID to assign the user's CTERA Portal account.

m **Billing ID**. Type the user's billing ID.

n **Comment**. Type a free-text description of the user account.

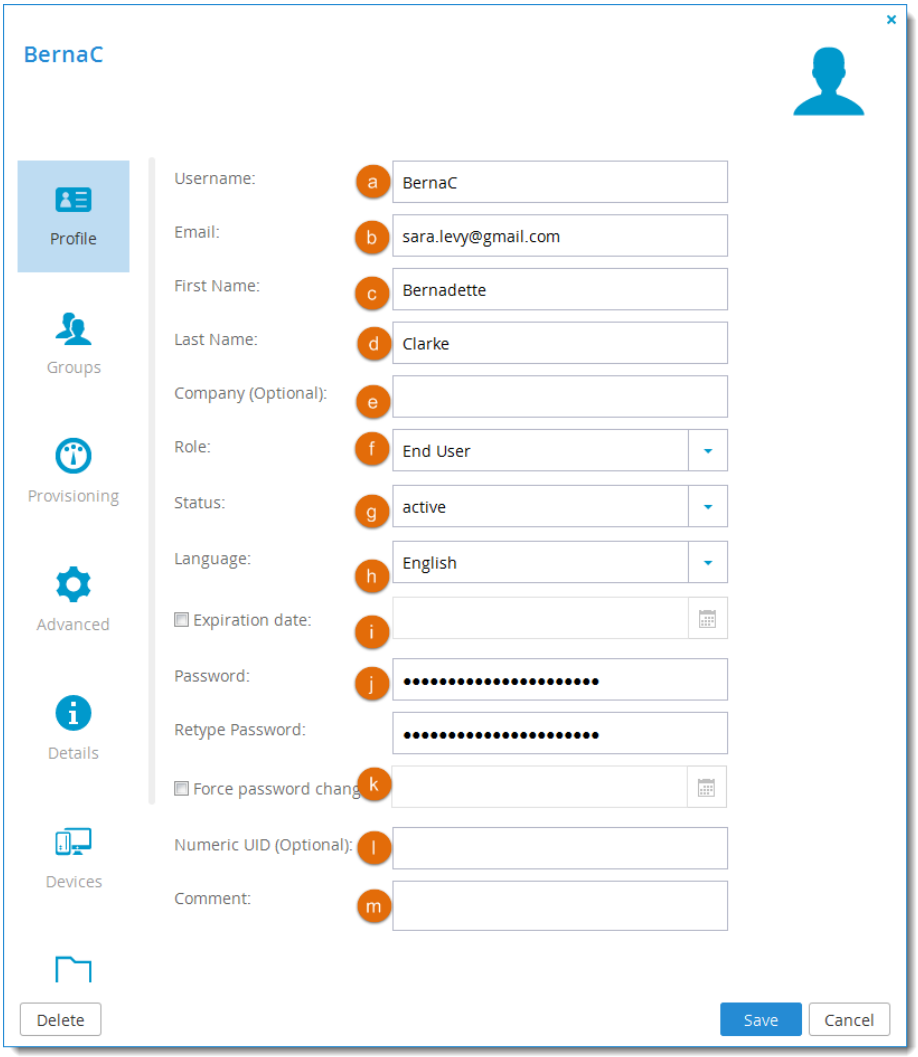
3 Click **Save**.

The user is added.

Editing User Profiles

1 Browse to **Users > Users** and click the username of the account you want to edit, or select the account's row and click **Edit**.

The User Account Manager opens displaying the **Profile** tab.



2 Change the fields as needed:

a **Username**. Type a user name for the user's CTERA Portal account.

b **Email**. Type the user's email address.

c **First Name**. Type the user's first name.

d **Last Name**. Type the user's last name.

e **Company** (optional). Type the name of the user's company.

f **Role**. Select the user's role. This can be either of the following:

- **Read/Write Administrator**. The user can access the End User Portal, and can access the Staff Control Panel with read-write permissions.
- **Read Only Administrator**. The user can access the End User Portal, and can access the Staff Control Panel with read-only permissions.
- **End User** (default). The user can access the End User Portal.
- **Disabled**. The user account is disabled. The user cannot access the End User Portal.

Tip

In order to access the End User Portal, the user must have a role other than Disabled, and their status must be active.

g **Status**. Select the account status. This can be either of the following:

- **active**. The account is active, and the user can access the CTERA Portal.
- **inactive**. The account is inactive, and the user cannot access the CTERA Portal.

The default value for new users created by an administrator is active.

The default value for invited users is *inactive*. The status changes to *active* when the invited user activates the account.

h **Language**. The user's interface language.

i **Expiration date**. The expiration date of the user account.

j **Password / Retype Password**. Type a password for the user's CTERA Portal account. Password requirements depend on the password policy, which can be overridden and modified in the **Virtual Portal Settings** (Browser to **Settings > Virtual Portal Settings** and scroll down to **Password Policy**).

k **Force password change**. Select this option to specify an expiration date for the user account password, and then click _ to select the date. When the password has expired, the user will be required to configure a new password upon their next login.

l **Numeric UID** (optional). Type a numeric user ID to assign the user's CTERA Portal account.

m **Billing ID**. Type the user's billing ID.

n **Comment**. Type a description of the user account.

3 Click **Save** to save your changes.

Enabling/Disabling User Accounts

If a user signed up for a CTERA Portal account via self-registration, and **Require Email Confirmation** is enabled (see ***User Registration Settings*** (on page 167)), the user will receive an email from the CTERA Portal containing an activation link. The new user account will remain disabled until the user confirms the registration by clicking the link. If for some reason the user does not click the link, you can enable the user account as described in the following procedure.

In addition, you can temporarily disable a user account, and then re-enable it as desired.

To enable a user account

1. In the **Users > Users** page, click the username of the account you want to edit, or select the account's row and click **Edit**.

   The User Account Manager opens displaying the **Profile** tab.

2. In the **Status** field, select **active**.
3. Click **Save**.

To disable a user account

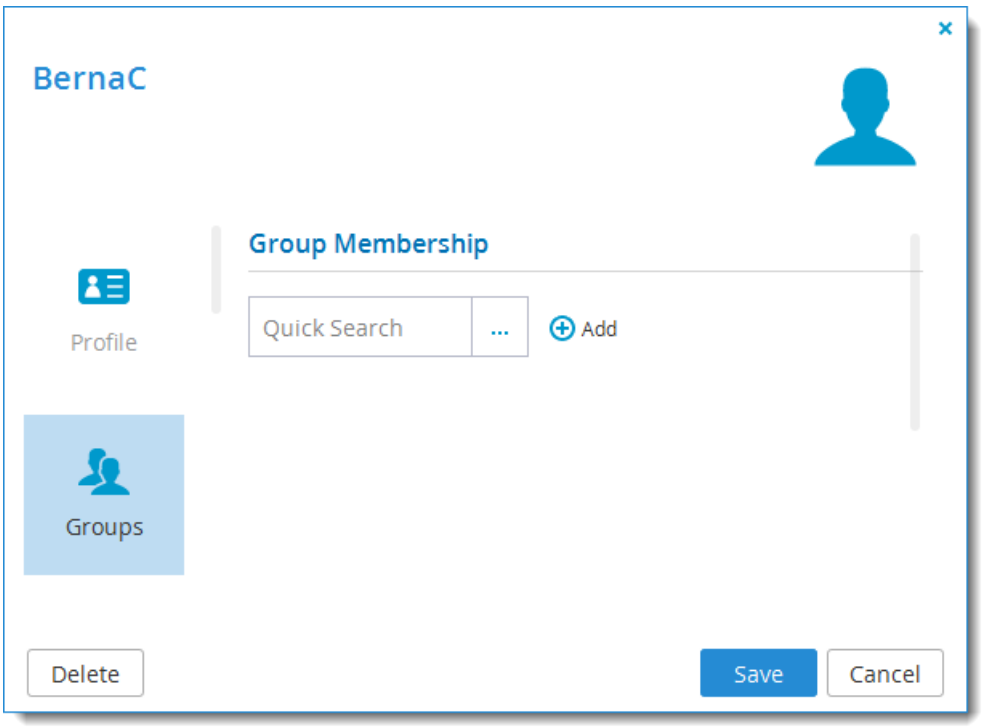
1. Browse to **Users > Users** and click the username of the account you want to edit, or select the account's row and click **Edit**.

   The User Account Manager opens displaying the **Profile** tab.

2. In the **Status** field, select **inactive**.
3. Click **Save**.

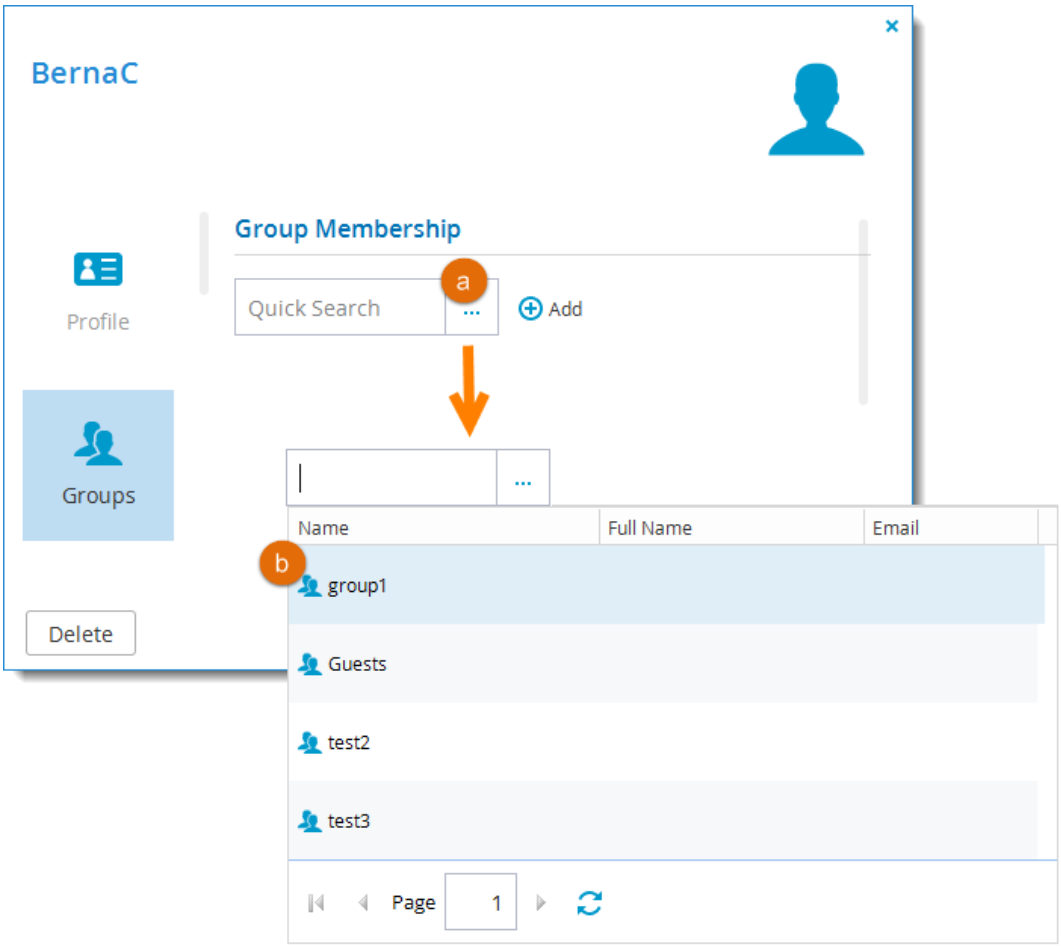
Adding Users to Groups

1. Click the user's name in the **Users > Users** page (or select the user's row and click **Edit**.)
2. When the user's editor opens, select the **Groups** tab.



3. To add the user account to a user group, do the following:
   a. In the **Quick Search** field, type a string that appears anywhere within the name of the desired user group, then click ... .

A table of user groups matching the search string appears.

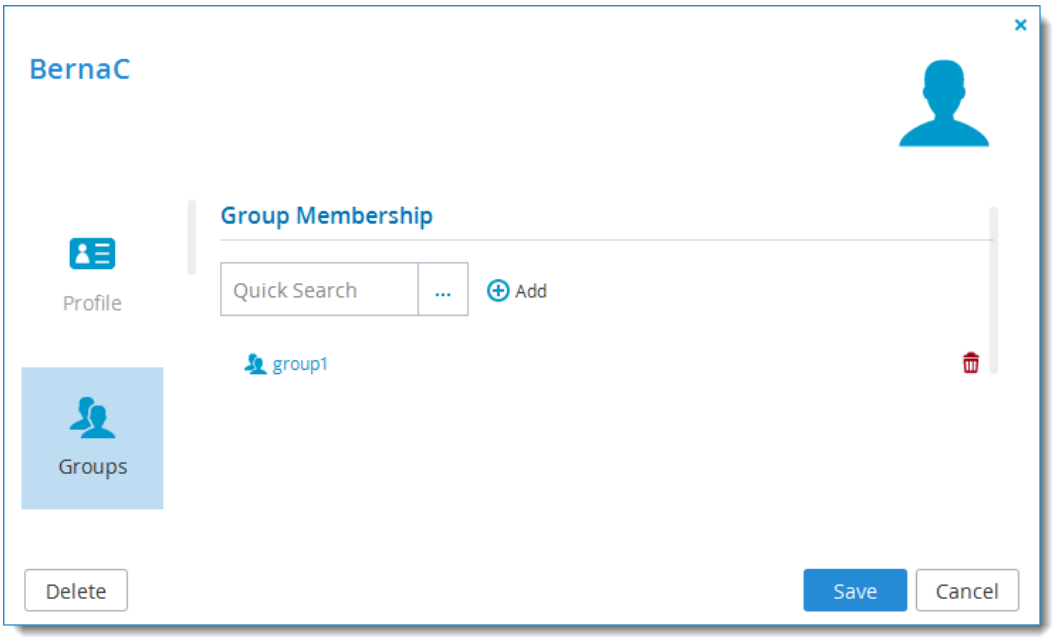


b Select the desired user group in the table.

The user group appears in the **Quick Search** field.

c Click **Add**.

The user group is added to the list of user groups to which the user account belongs.



You can edit any listed user group, by clicking on its name. See ***Adding and Editing User Groups*** (on page 114).

4 To remove the user account from a user group, in the user group's row, click .

The user group is removed from the list.

5 Click **Save**.

Provisioning User Accounts

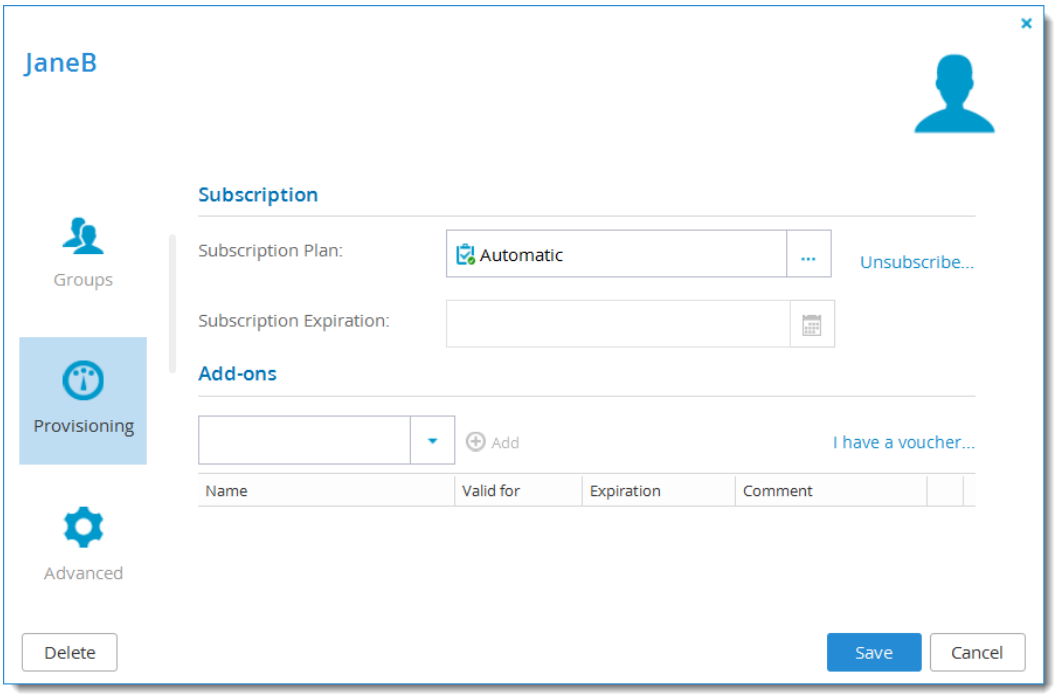
Users may be assigned to a default subscription plan or assigned automatically to another plan based on automatic template assignment settings (see ***Provisioning*** (on page 133)). If desired, you can subscribe an individual user to a different subscription plan. You can also unsubscribe the user account, which deletes all files stored in the account and terminates the account.

Assigning User Accounts to Subscription Plans

To assign a user account to a subscription plan

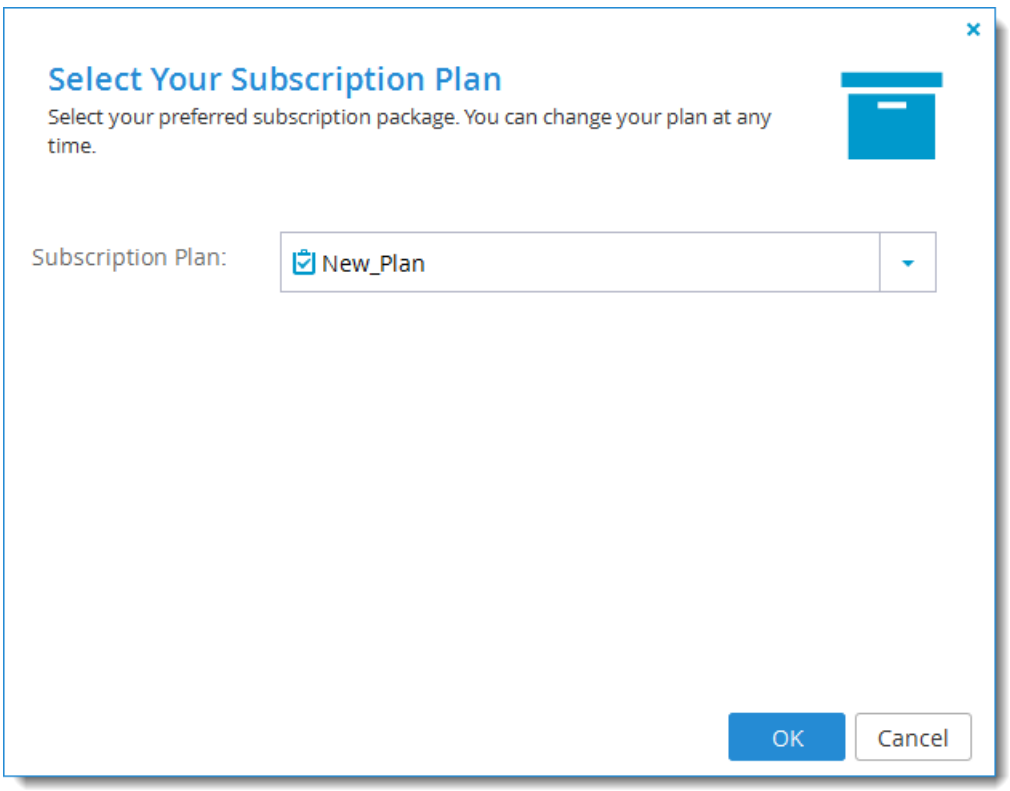
1 Click the user's name in the **Users > Users** page (or select the user's row and click **Edit**.)

2 When the user's editor opens, select the **Provisioning** tab.



3 In the **Subscription Plan** field, click  .

The **Select Your Subscription Plan** dialog box opens.



4 In the **Subscription Plan** drop-down list, select the subscription plan to assign the user account.

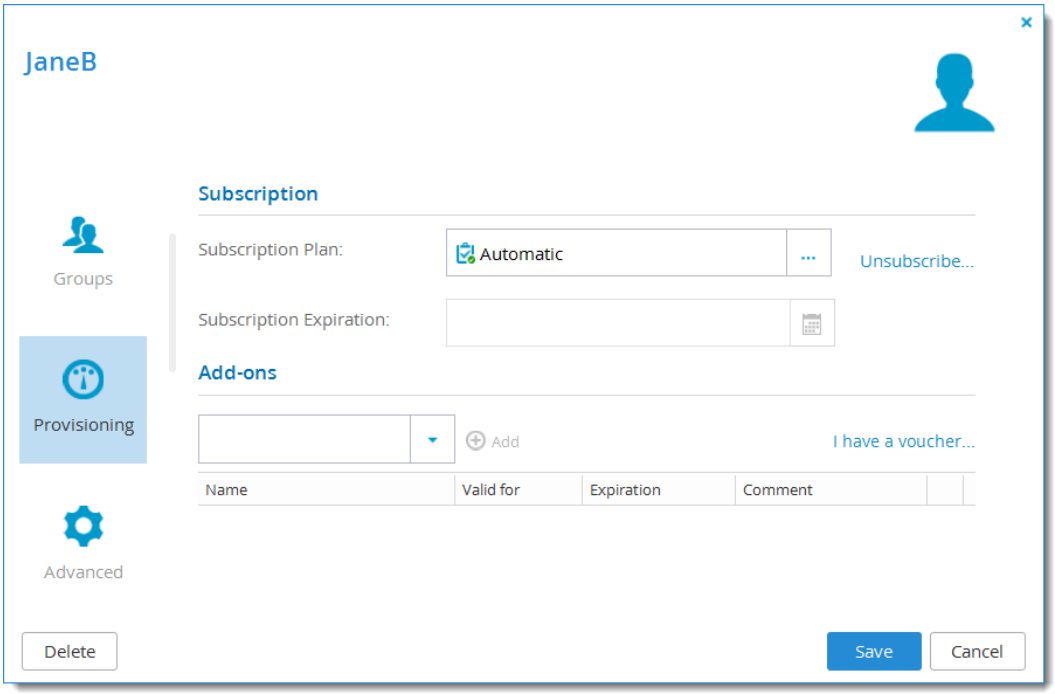
5 Click **OK**.

Adding Add-ons to User Accounts

To add an add-on to a user account

1 Click the user's name in the **Users > Users** page (or select the user's row and click **Edit**.)

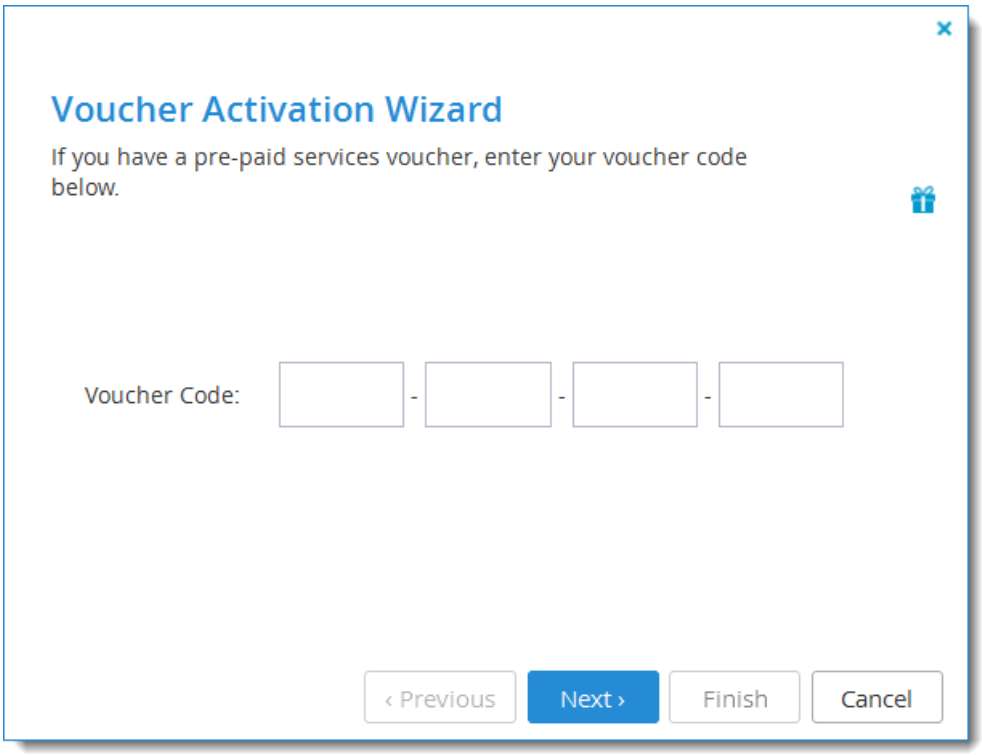
2 When the user's editor opens, select the **Provisioning** tab.



3 To use a voucher for an add-on:

a Click **I have a voucher**.

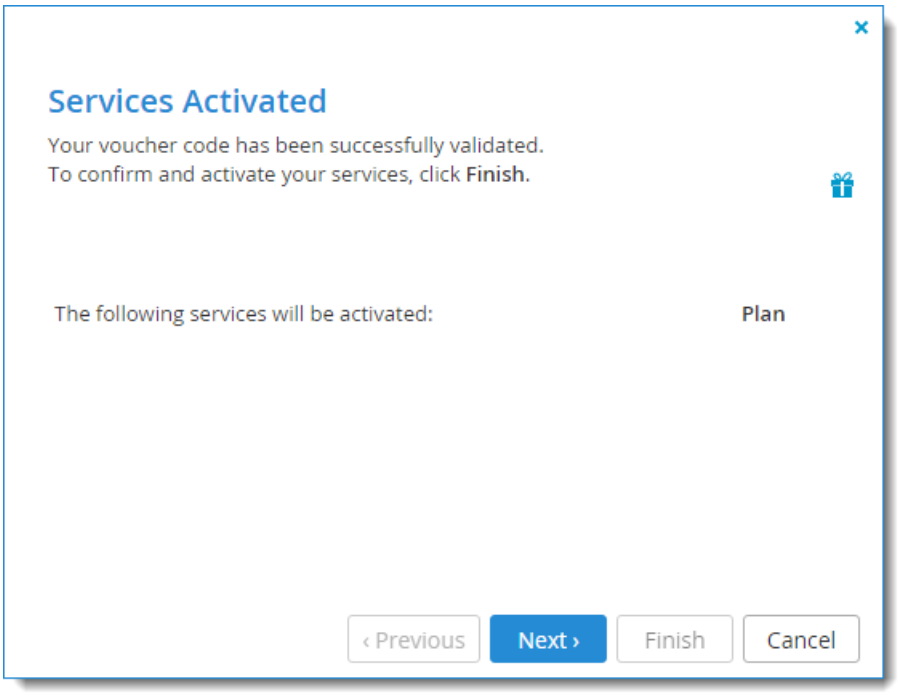
The **Voucher Activation Wizard** opens.



b Type the voucher code in the fields provided.

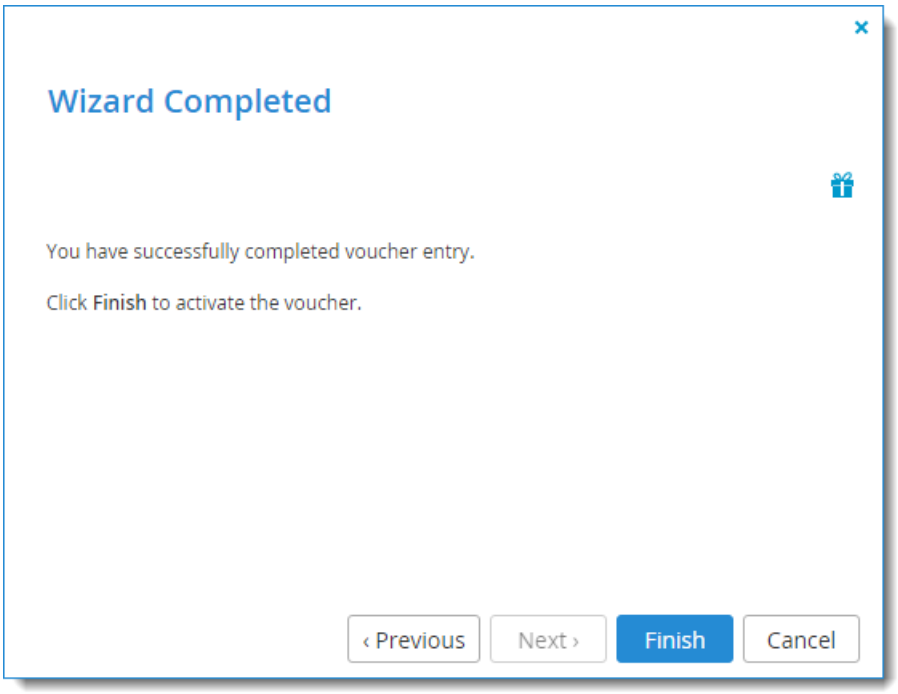
c Click **Next**.

The **Services Activated** screen appears with the voucher details.



d Click **Next**.

The **Wizard Completed** screen appears.



e Click **Finish**.

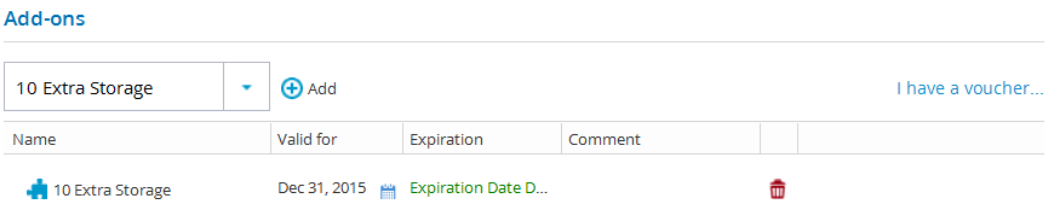
The **Manage Add-ons** dialog box reappears with the add-on listed.

4 To add an add-on for the user account, do the following:

a In the drop-down list, select the desired add-on.

b Click **Add**.

The add-on appears in the list box.



c In the add-on's row in the list box, click in the **Valid For** column, and then click .

A calendar appears.

d Select the date on which the add-on subscription should end.

The **Expiration** column is updated accordingly.

5 To remove an add-on from the user account, in the add-on's row in the list box, click .

The add-on is removed.

6 Click **Save**.

The add-on is added to the user account.

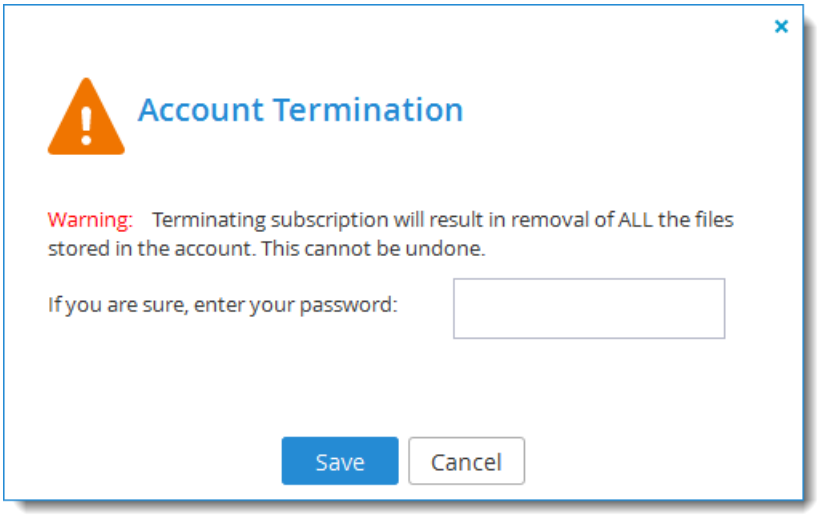
Terminating User Accounts

Unsubscribing a user account from a subscription plan terminates the user account and removes all the files stored in the account.

To terminate a user account:

1. Click the user's name in the **Users > Users** page (or select the user's row and click **Edit**.)
2. When the user's editor opens, select the **Provisioning** tab.
3. Click **Unsubscribe**.

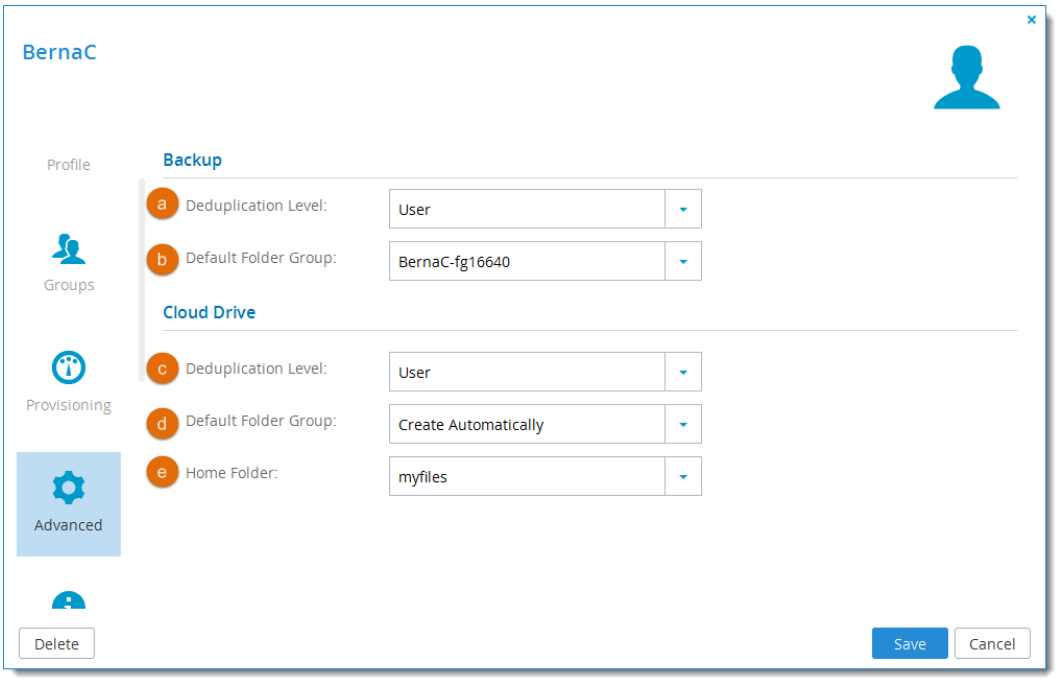
   The **Account Termination** dialog appears.



4. If you are sure you want to proceed, enter your password in the field provided.
5. Click **Save**.

Configuring a User's Deduplication Settings

1. Click the user's name in the **Users > Users** page (or select the user's row and click **Edit**.)
2. When the user's editor opens, select the **Advanced** tab and change the deduplication settings as needed:



Backup

a **Deduplication Level**. Specify the default de-duplication level to use for new backup folders. Select one of the following:

- **User** (default). Create a single folder group for the user account, containing all of the user account's backup folders. De-duplication is performed for the user account's folder group.
- **Folder**. Create a folder group for each of the user account's devices, containing all of the device's backup folders. De-duplication is performed separately for each of the user account's folder groups.

b **Default Folder Group**. Appears only if **User** is selected as the *Deduplication Level*. Select the default folder group to use for all of the user account's backup folders. This can be either of the following:

- An existing folder group
- **Create Automatically** (default). Automatically create a new folder group.

Cloud Drive

c **Deduplication Level**. Specify the default de-duplication level to use for new cloud folders. Select one of the following:

- **User** (default). Create a single folder group for the user account, containing all of the user account's cloud folders. De-duplication is performed for the user account's folder group.
- **Folder**. Create a folder group for each of the user account's devices, containing all of the device's cloud folders. De-duplication is performed separately for each of the user account's folder groups.

d **Default Folder Group**. Appears only if **User** is selected as the *Deduplication Level*. Select the default folder group to use for all of the user account's cloud folders. This can be either of the following:

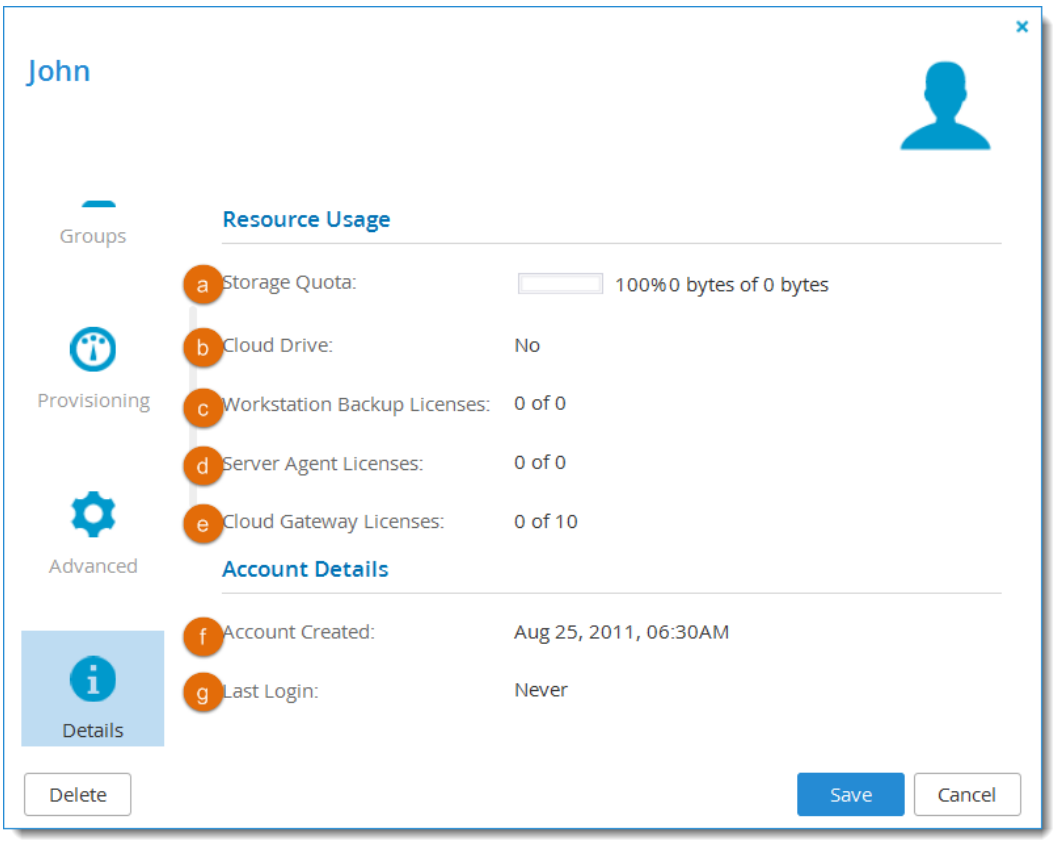
- An existing folder group
- **Create Automatically** (default). Automatically create a new folder group.

e **Home Folder**. Select one of the user's personal folders to act as the user's home folder. The home folder is a personal folder that is linked to the user account and cannot be deleted.

3 Click **Save**.

Viewing User Account Details

1. Click the user's name in the **Users > Users** page (or select the user's row and click **Edit**.)
2. When the user's editor opens, select the **Details** tab.



a **Storage Quota**. The amount of storage the user has consumed out of the total amount available in their subscription plan.

b **Cloud Drive**. Whether the user is provisioned to have the Cloud Drive service.

c **Workstation Backup Licenses**. The number of CTERA Workstation Agents installed and using the cloud backup service out of the total number available in the user account's subscription plan.

d **Server Agent Licenses**. The number of CTERA Server Agents installed out of the total number available in the user account's subscription plan.

e **Cloud Gateway Licenses**. The number of cloud gateways associated with the user account out of the total number available in the user account's subscription plan.

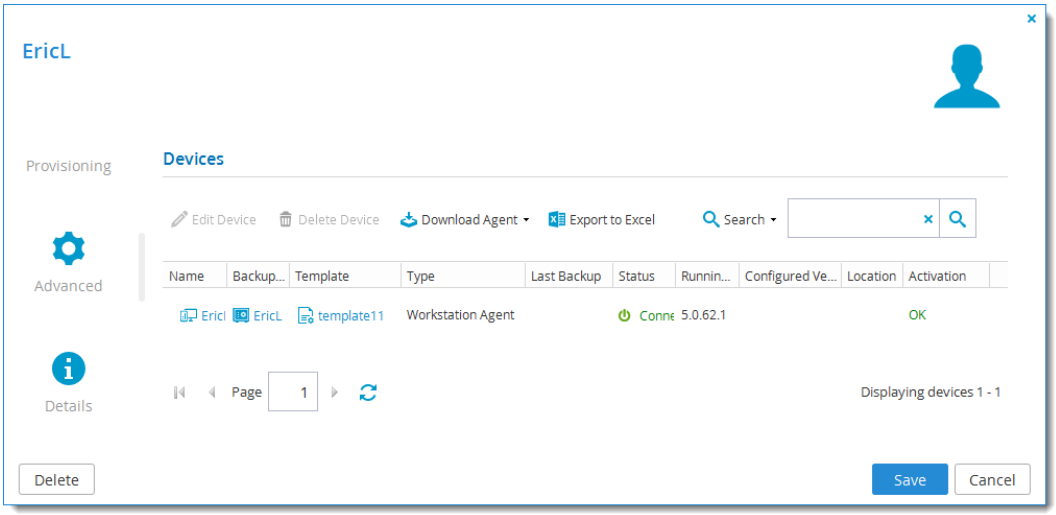
f **Account Created**. The date and time when the user account was created.

g **Last Login**. The date and time when the user last logged in to the CTERA Portal.

Managing a User's Devices

1. Click the user's name in the **Users > Users** page (or select the user's row and click **Edit**.)
2. When the user's editor opens, select the **Devices** tab.

   The **Devices** tab appears with a table of devices associated with the user account.

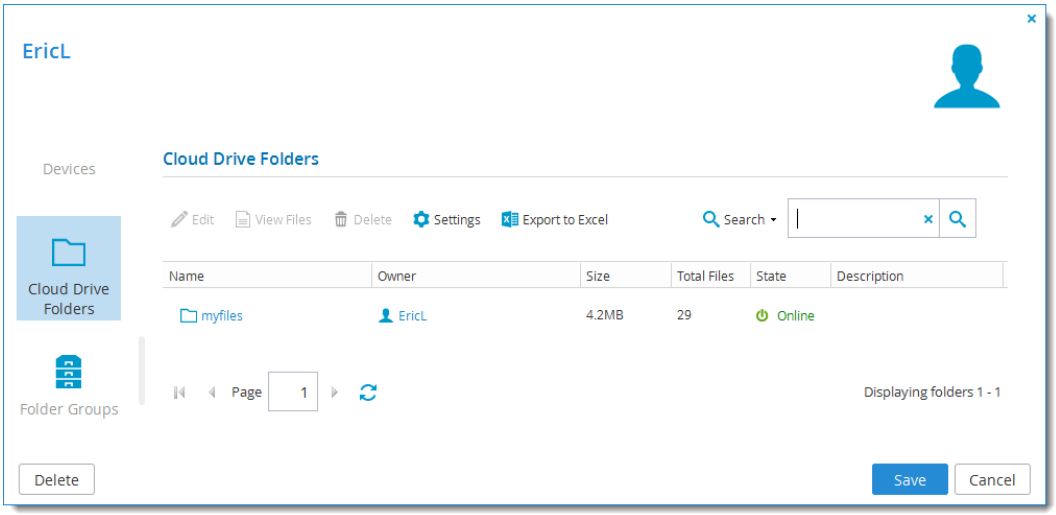


3. Perform any of the device management tasks described in Managing Devices, as if you were working in the **Main > Devices** page.

Managing a User's Cloud Drive Folders

1. Click the user's name in the **Users > Users** page (or select the user's row and click **Edit**.)
2. When the user's editor opens, select the **Cloud Drive Folders** tab.

   The **Cloud Drive Folders** tab displays all cloud drive folders owned by the user.

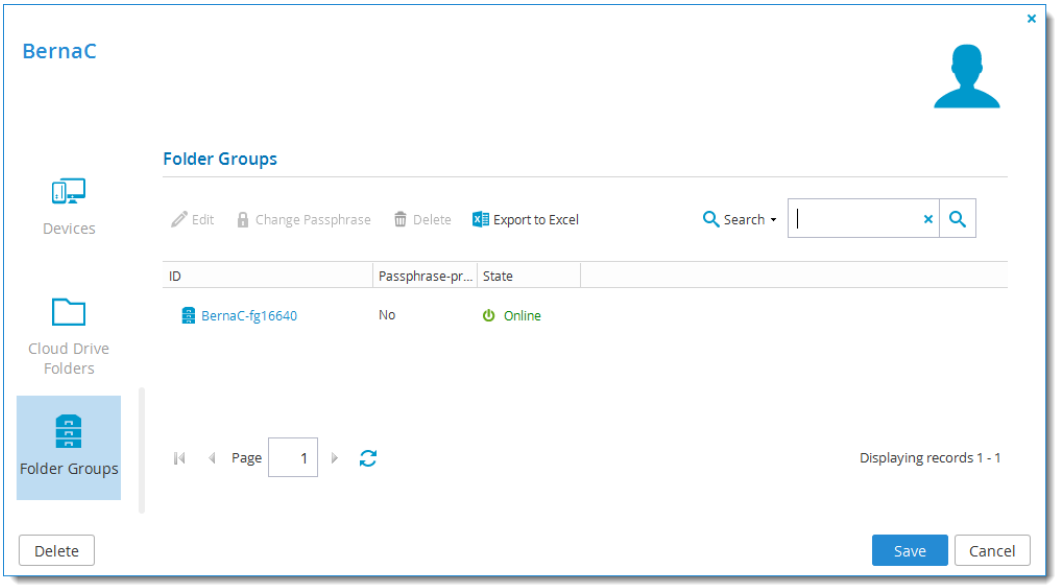


3 Perform any of the project management tasks described in ***Managing Folders*** (on page 41), as if you were working in the **Folders > Cloud Drive Folders** page.

Managing a User's Folder Groups

1 Click the user's name in the **Users > Users** page (or select the user's row and click **Edit**.)

2 When the user's editor opens, select the **Folder Groups** tab. The **Folder Groups** tab displays all folder groups associated with the user.



3 Perform any of the folder group management tasks described in ***Managing Folder Groups*** (on page 65), as if you were working in the **Folders > Folder Groups** page.

Exporting User Accounts to Excel

You can export a list of user accounts and their details to a Microsoft Excel (*.xls) file on your computer.

To export user accounts to Excel

1 Select **Users > Users** from the menu.

The **Users > Users** page appears, displaying all user accounts.

2 Click **Export to Excel**.

The user accounts are exported.

Applying Provisioning Changes

CTERA Portal applies changed plan and add-on settings to all users every day at midnight. If desired, you can use the following procedure to apply all changes immediately.

Tip

If CTERA Portal is integrated with a directory service, applying provisioning changes will also cause CTERA Portal to synchronize all the users with the directory.

To apply provisioning changes to all users

1. Select **Users > Users** from the menu.

   The **Users > Users** page appears, displaying all user accounts.

2. Click **Apply Provisioning Changes**.

   While provisioning changes are applied, progress is indicated by a progress bar.

   You can click **Stop** at any time if you want to stop the operation.

   When the operation is complete, the **Completed** screen appears.

3. Click **Close**.

Deleting User Accounts

Deleting a user account from the CTERA Portal cancels the user's subscriptions to plans and add-ons, and deletes all of the user's folders and folder groups.

To delete a user account

1. Click the user's name in the **Users > Users** page to edit the user and click the **Delete** button inside the user editor.

2. Click **Yes** to confirm.

   The user account is deleted.

8

Managing Staff Administrators

Staff administrators manage CTERA Portal settings and contents through the Staff Control Panel of the reseller portal.

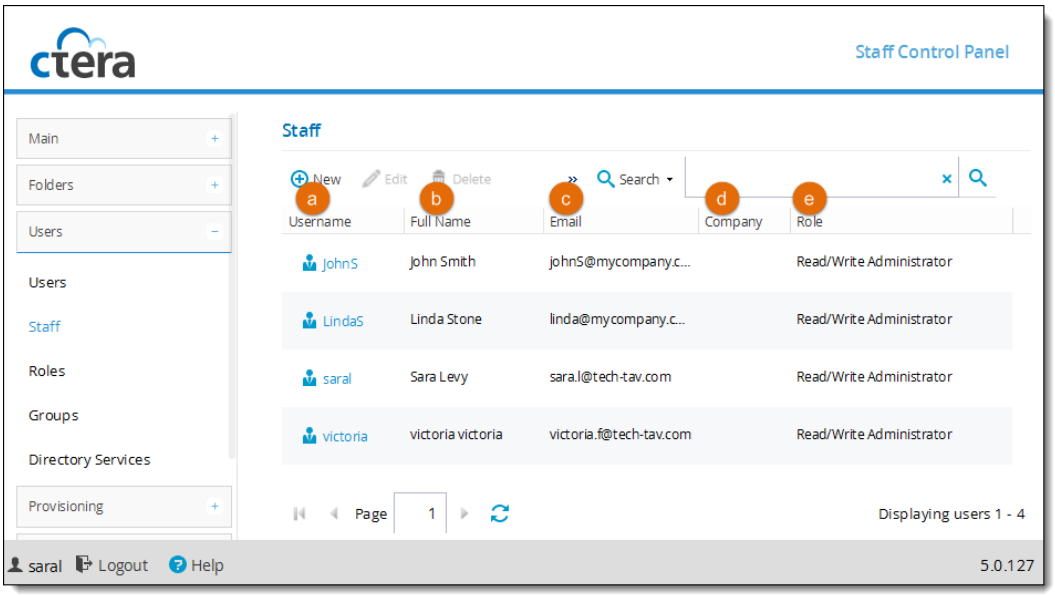
In This Chapter

Viewing Staff Administrators

To view all staff administrators in the portal

1 Select **Users > Staff** from the menu.

The **Users > Staff** page displays all CTERA Portal staff administrators in the portal.



a **Username**. The administrator's user name.

To edit the administrator, click the user name. For further details, see ***Adding and Editing Staff Administrators*** (on page 102).

b **Full Name**. The administrator's full name.

c **Email**. The administrator's email address.

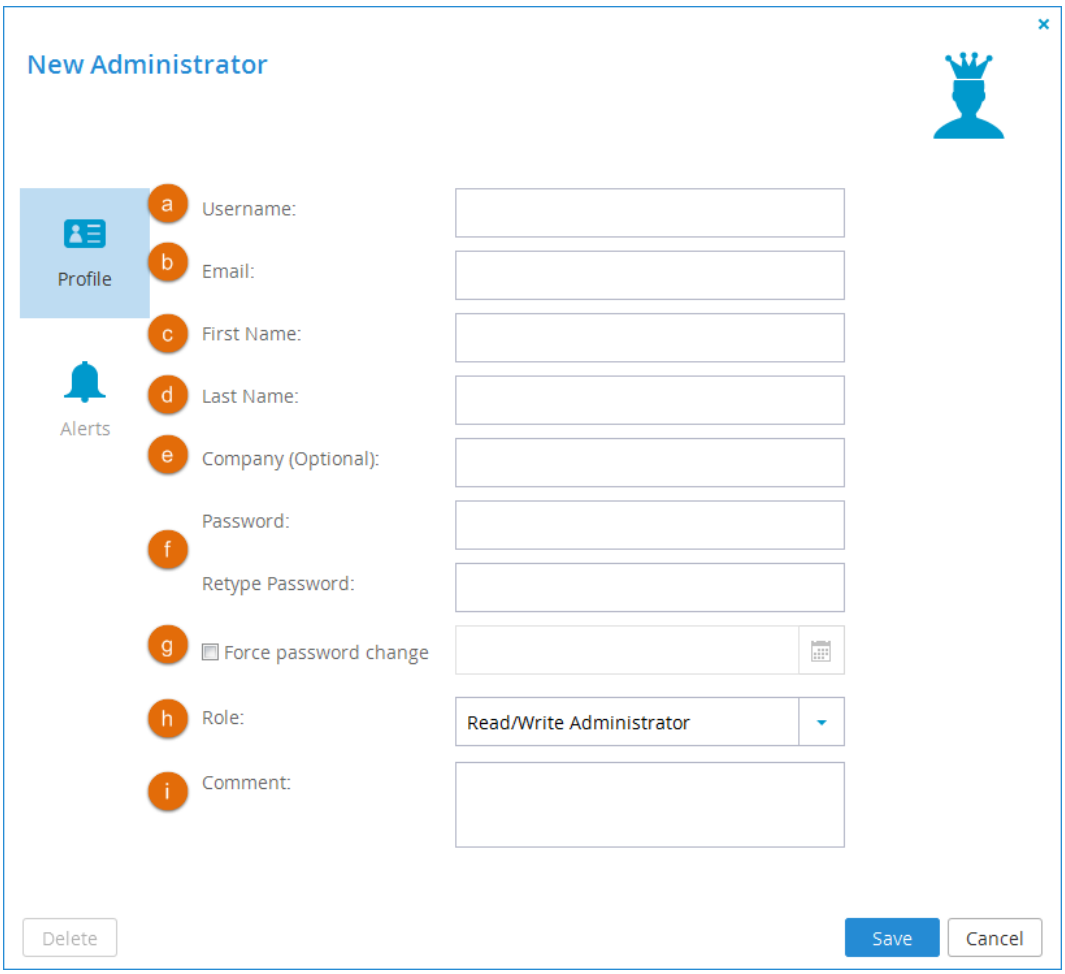
d **Company**. The name of the administrator's company.

e **Role**. The administrator's role. See ***Customizing Administrator Roles*** (on page 109).

Adding and Editing Staff Administrators

To add or edit a staff administrator

1. Do one of the following:
   - To add a new administrator, in the **Users > Staff** page, click **New**.
   - To edit an existing administrator, click the administrator's name on the **Users > Staff** page.
2. Edit the administrator's details as needed:



a **Username**. Type a user name for the administrator's CTERA Portal account.

b **Email**. Type the administrator's email address.

c **First Name**. Type the administrator's first name.

d **Last Name**. Type the administrator's last name.

e **Company**. Type the name of the administrator's company.

This field is optional.

f **Password / Retype Password**. Type a password for the administrator's CTERA Portal account.

The password must be at least 5 characters long.

g **Force password change**. Select this option to specify an expiration date for the administrator account's password, then click  to select the date.

When the password has expired, the administrator will be required to configure a new password upon their next login.

h **Role**. Specify the administrator's role.

For information on the available roles, see ***Customizing Administrator Roles*** (on page 109).

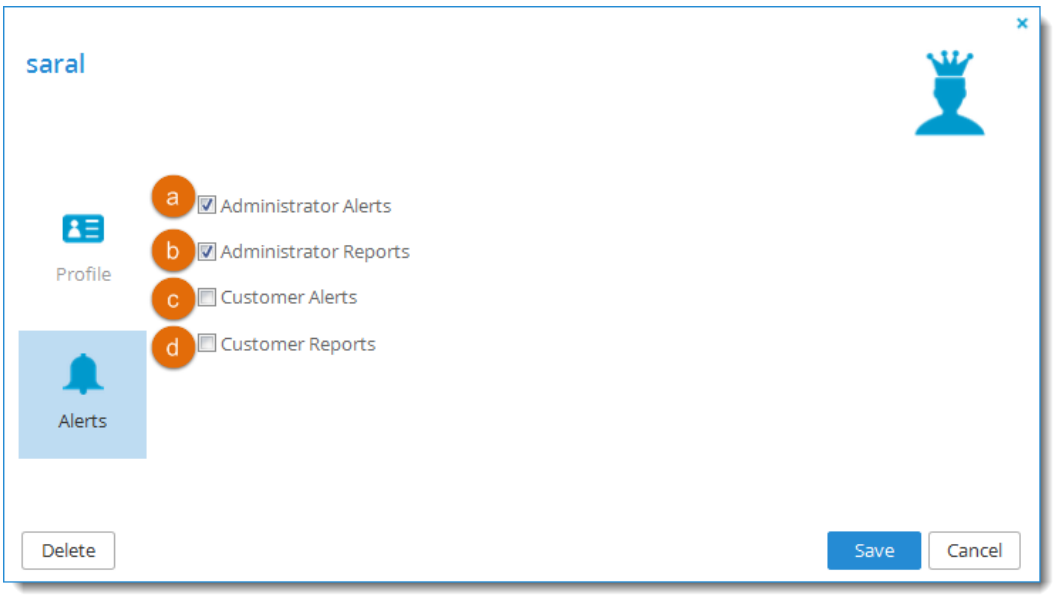
i **Comment**. Type a description of the administrator's CTERA Portal account.

3 Click **Save**.

Configuring Staff Administrator Alerts

To configure a staff administrator's alerts

1. On the **Users > Staff** page, click the administrator's name to open the administrator's profile.
2. Select the **Alerts** tab.



3. Check the types of alerts the administrator should receive:
   a. **Administrator Alerts**. Notifications about portal-level problems.
   b. **Administrator Reports**. Notifications reporting portal-level activity.
   c. **Customer Alerts**. Notifications about device-level problems.
   d. **Customer Reports**. Notifications about customer activity.
4. Click **Save**.

Deleting Staff Administrators

To delete a staff administrator

1. In the **Users > Staff** page, select the desired administrator's row, then click **Delete**.
2. Click **Yes** to confirm.

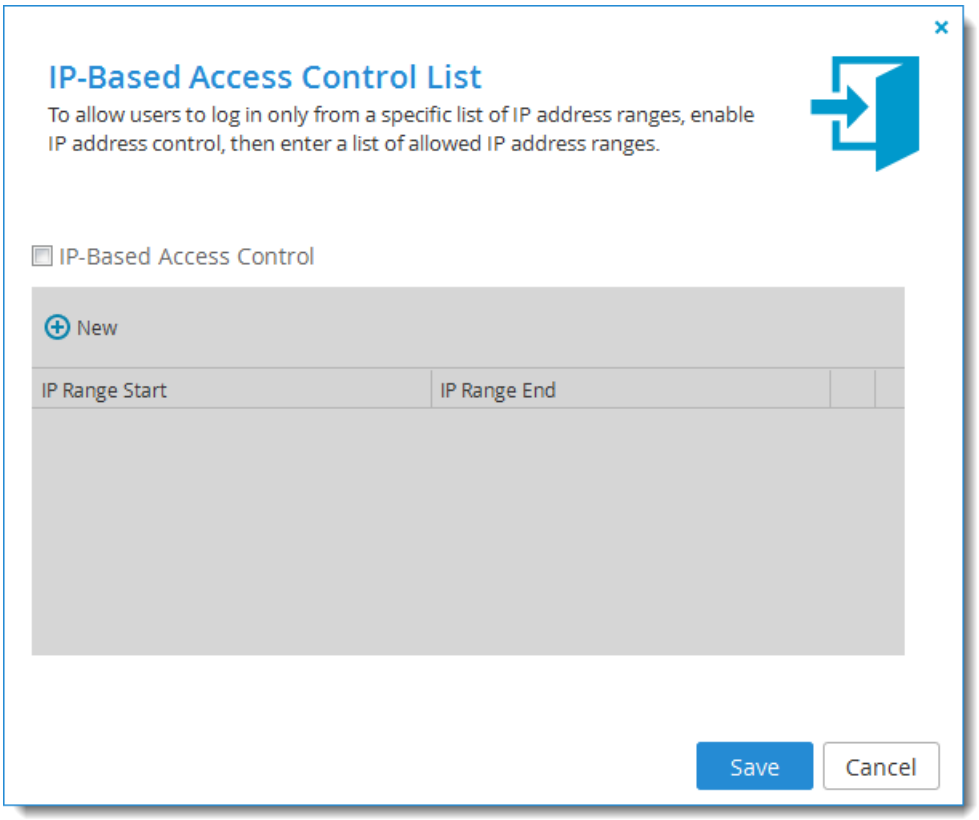
   The administrator is deleted.

Configuring an IP-Based Access Control List

You can configure an IP-based access control list, specifying the IP address ranges from which administrators can access the CTERA Portal interface.

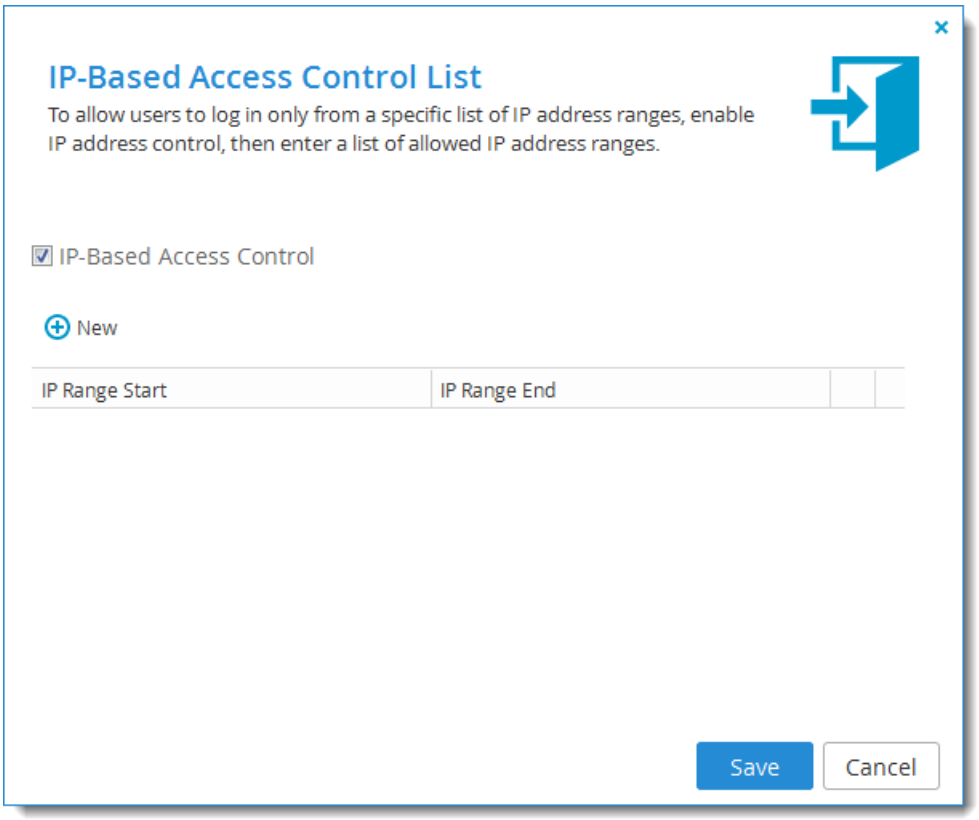
To configure an IP-based access control list

1. In the **Users > Staff** page, click **Access Control**.



2. Select the **IP-Based Access Control** check box.

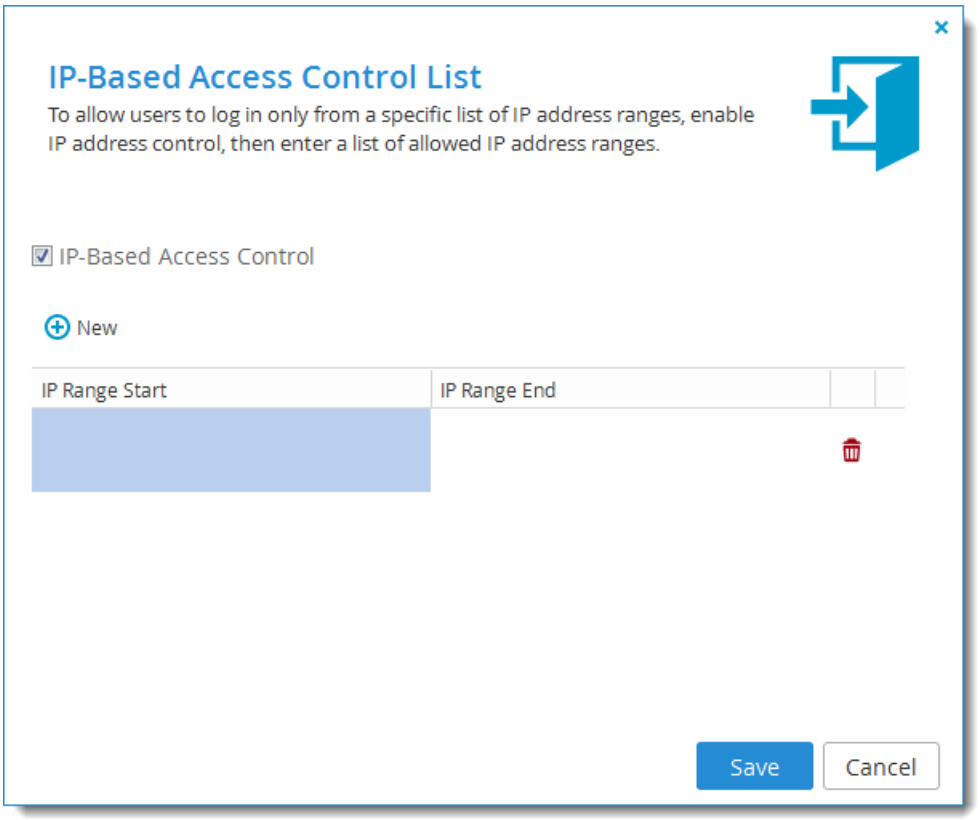
The list box is enabled.



3 To add an IP address range from which access to the CTERA Portal interface is allowed, do the following:

a Click **New**.

A new row is added to the list box.



b Click in the **IP Range Start** field, and type the starting IP address.

c Click in the **IP Range End** field, and type the ending IP address.

4 To remove an IP address range, in the IP address range's row, click .

The IP address range is removed.

5 Click **Save**.

Importing Staff Administrators from a File

You can import a list of staff administrators and their details from a comma separated values (*.csv) file.

The *.csv file's columns must be in the following order:

1 Username

2 First name

3 Last name

4 Email address

5 Company (Optional)

6 Password

7 Role

8 Plan (Optional)

9 Numeric UID (Optional)

10 External Account ID (Optional)

11 Comment (Optional)

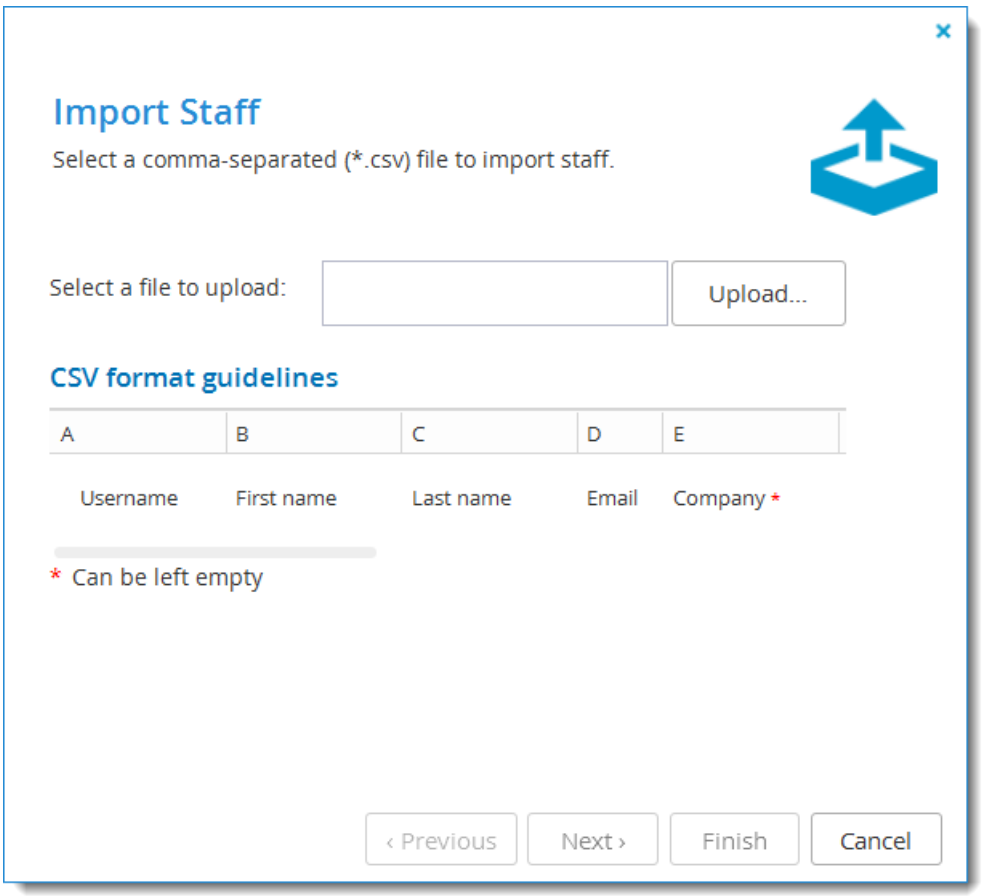
Optional fields can be left blank.

To import staff administrators from a *.csv file

1 In the navigation pane, click **Users > Staff**.

2 Click **Import**.

The **Import Staff** wizard appears.



3 Click **Upload**. The file is uploaded and the **Import Completed** screen appears.

4 Click **Finish**.

Customizing Administrator Roles

By default, CTERA Portal includes three built-in administrator roles for administrators:

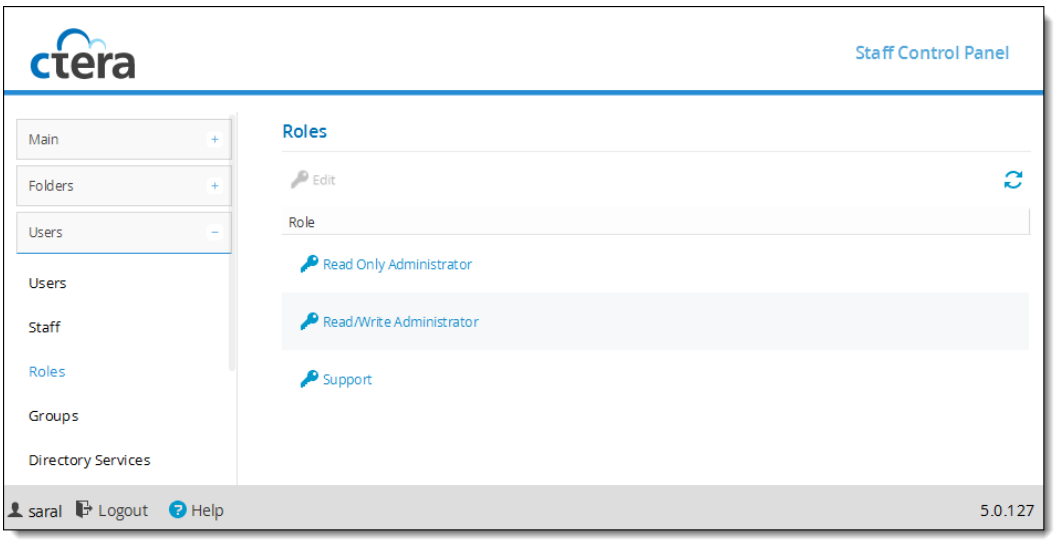
- **Read/Write Administrator**. The administrator has read-write permissions throughout the CTERA Portal.
- **Read Only Administrator**. The administrator has read-only permissions throughout the CTERA Portal.
- **Support**. The administrator has read/write access to devices, user accounts, folders, and folder groups, and read-only access to all other settings in the CTERA Portal.

You can customize these roles, adding or removing permissions as desired.

To customize an administrator role

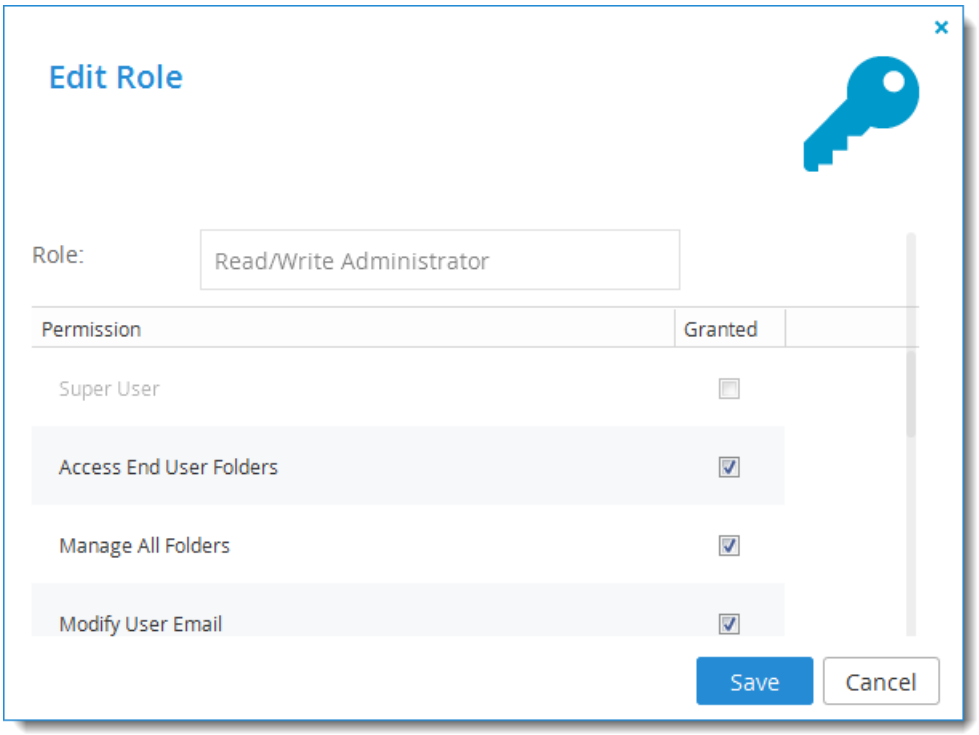
1. Select **Users > Roles** from the menu.

   The **Users > Roles** page appears, displaying all CTERA Portal administrator roles.



2. Either click a role or select a role's row and then click **Edit**.

The **Edit Role** window opens.



3 Check the permissions you want to include in the role, and uncheck those that you don't want to include:

- **Access End User Folders**. Select this option to allow administrators with this role to access end users' folders. If this option is not selected, and an administrator with this role attempts to access an end user's folder, the administrator will be prompted to enter the folder owner’s password.
- **Manage All Folders**. Select this option to allow administrators with this role to manage all folders. Without this permission, an administrator has only read-only access to the projects, backup folders and personal folder objects unless the administrator is the folder owner and the administator or a user group the administrator belongs to has collaboration permissions for the folder (defined in the folder's settings).
- **Modify User Email**. Select this option to allow administrators with this role to modify the email addresses associated with user accounts.
- **Modify User Password**. Select this option to allow administrators with this role to modify the passwords associated with user accounts.
- **Modify Virtual Portal Settings**. Select this option to allow administrators with this role to modify virtual portal settings.
- **Modify Roles**. Select this option to allow administrators with this role to modify administrator roles.

- **Allow Single Sign On to Devices**. Select this option to allow administrators with this role to remotely manage devices for which Remote Access with single sign on (SSO) is enabled, without entering the username and password for accessing the device. For information on remotely managing devices, see ***Remotely Managing Devices*** (on page 27).
- **Allow Remote Wipe for Devices**. Select this option to allow administrators with this role to perform remote wipe of CTERA Mobile devices.
- **Allow Seeding Export**. Select this option to allow administrators with this role to perform seeding export.
- **Allow Seeding Import**. Select this option to allow administrators with this role to perform seeding import.

4 Click **Save**.

Table 5: Default Permissions per Administrator Role

Permission	Read/Write Administrator	Read Only Administrator	Support
Access End User Folders	Yes	Yes	No
Manage All Folders	Yes	No	Yes
Modify User Email	Yes	No	Yes
Modify User Password	Yes	No	Yes
Modify Portal Settings	Yes	No	No
Modify Roles	Yes	No	No
Allow Single Sign On to Devices	No	No	No
Allow remote wipe for devices	Yes	No	Yes
Allow Seeding Export	Yes	No	Yes
Allow Seeding Import	Yes	No	Yes

9

Managing User Groups

In This Chapter

Overview

User groups are groups of users that you can define and then use when configuring the ***automatic template assignment policy*** (see "***Configuring the Automatic Template Assignment Policy***" on page 212) or setting permissions for accessing ***folders*** (see "***Managing Folders***" on page 41).

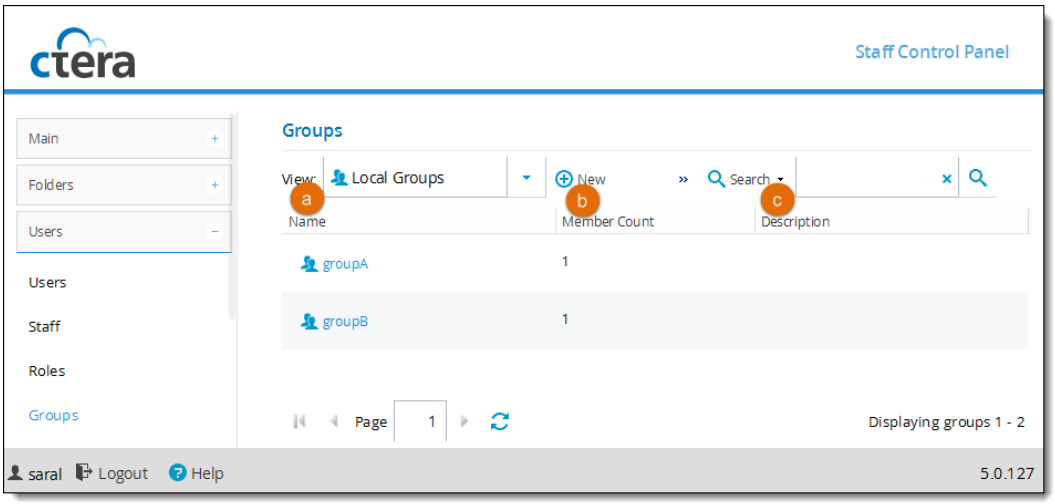
Tip

Directory service groups are supported.

Viewing User Groups

To view all user groups in the portal

1 Browse to the **Users > Groups** page.



a **Name**. The user group's name.

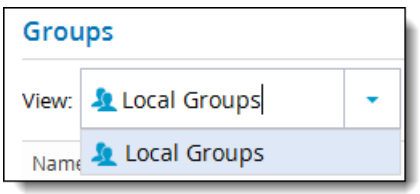
b **Member Count**. The number of user accounts that are members of the user group.

c **Description**. A description of the user group.

Filtering the User Groups Page

To view only a specific type of user groups, in the **View** drop-down list:

- To view only users from the directory service, select the Active Directory or LDAP directory name.
- To view groups defined in the local user database, select **Local Groups**.



Adding and Editing User Groups

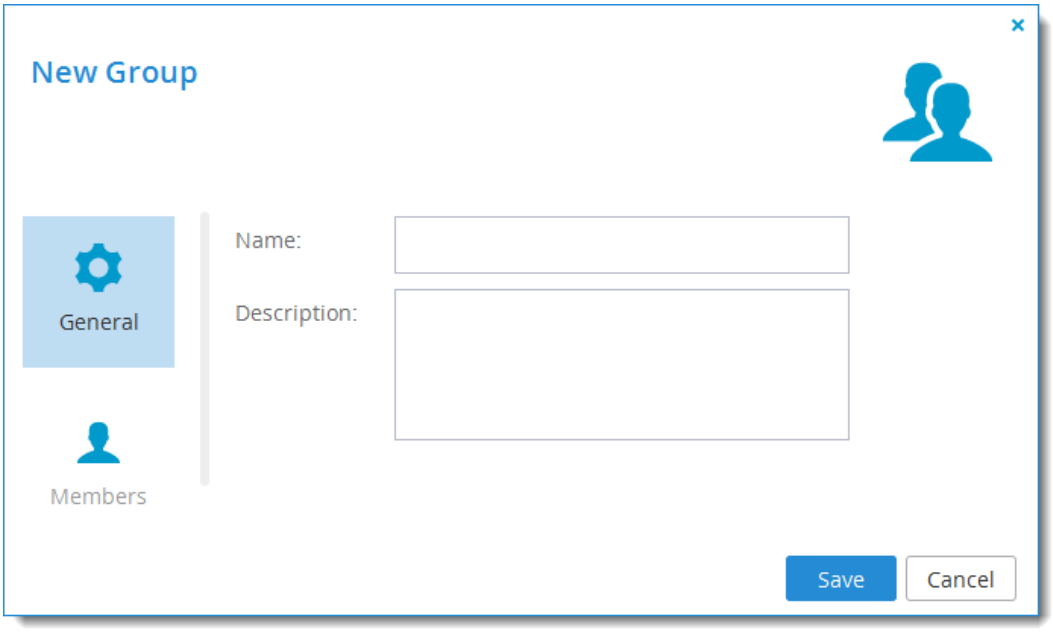
To add or edit a user group

1 Browse to the **Users > Groups** page.

The **Users > Groups** page displays all user groups.

2 Click **New** to add a new user group or Do one of the following:

- To add a new user group, click **New** in the **Users > Groups** page.
- To edit an existing user group, either click the user group's name or select the user group's row and click **Edit**.



3 In the **Name** field, type a name for the group.

4 In the **Description** field, type a description of the group.

5 Click **Save**.

Configuring User Group Members

Tip

User accounts can belong to multiple user groups.

Tip

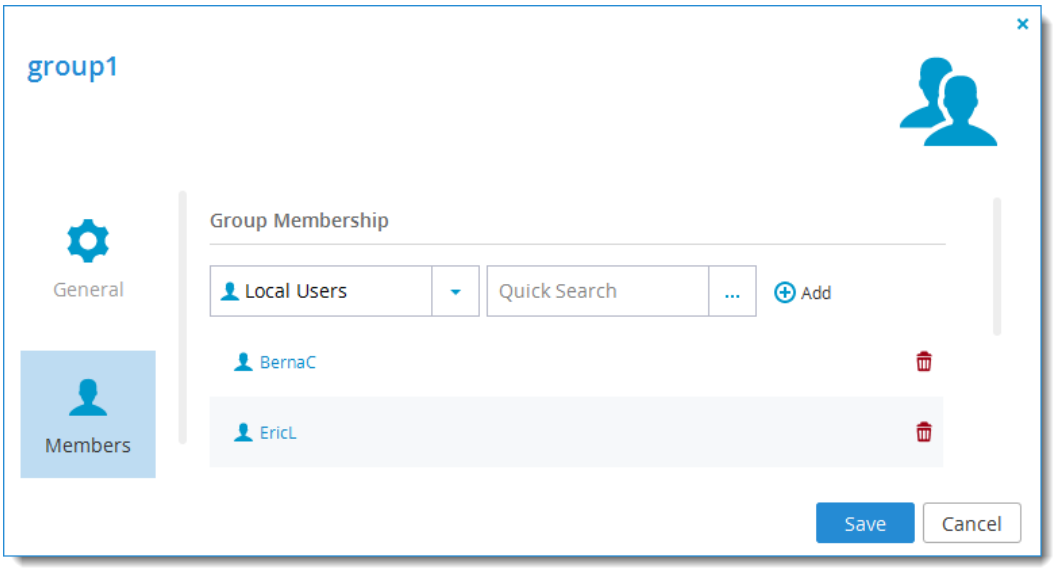
User accounts can be added to user groups as described in the following procedure or as described in ***Configuring Group Membership for User Accounts*** (see "***Adding Users to Groups***" on page 86).

To configure a user group's members

1 In the **Users > Groups** page, click the user group's name to open the user group manager.

2 Select the **Members** tab.

The **Members** tab appears with a list of group members.



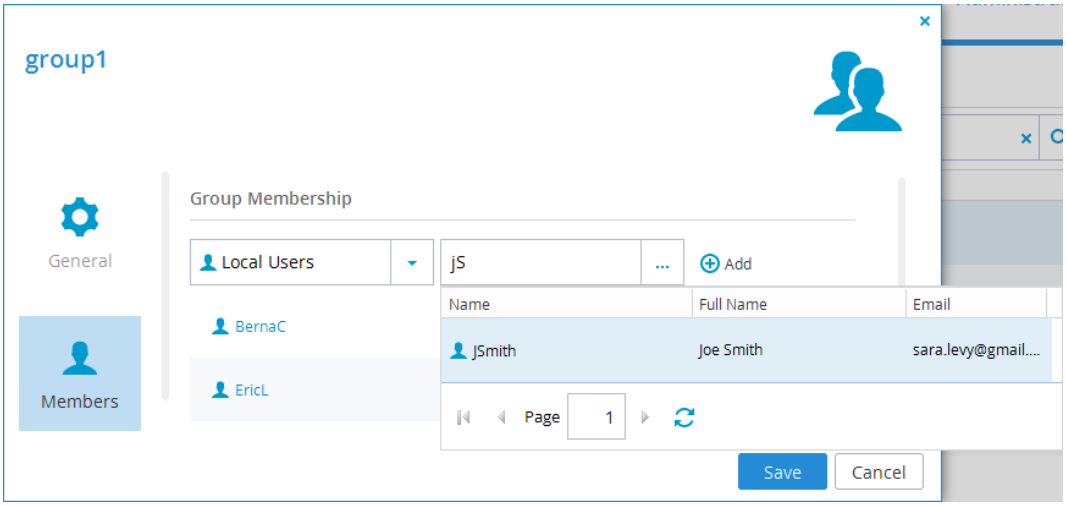
3 (Optional) To view only a specific type of users, in the **Show** drop-down list, do one of the following:

- To view only users from the directory service, select the Active Directory or LDAP directory name.
- To view users defined in the local user database, select **Local Users**.

4 To add a user account to the user group, do the following:

a In the **Quick Search** field, type a string that appears anywhere within the name of the desired user account, then click ... .

A table of user accounts matching the search string appears.



b Select the desired user account in the table.

The user account appears in the **Quick Search** field.

c Click **Add**.

The user account is added to the list of group members.

You can edit any listed user account, by clicking on its name.

5 To remove a user account from the user group, in the user account's row, click .

The user account is removed from the list.

6 Click **Save**.

Deleting User Groups

Tip

Deleting a user group does not delete the group members.

To delete a user group

1 Either:

- Select the user group's row in the **Users > Groups** page, and then click **Delete**.
- Click the user group's name to open the user group manager and then click **Delete**.

2 Click **Yes** to confirm.

The user group is deleted.

10

Using Directory Services

In This Chapter

Overview

The CTERA Portal can be integrated with the following directory services:

- Microsoft Active Directory
- LDAP directory services:
  - OpenDS
  - Oracle Unified Directory
  - Oracle Directory Server Enterprise Edition
  - Sun Java System Directory Server

User accounts will be automatically fetched and refreshed from the directory, and user authentication will be performed using the directory.

CTERA Portal administrators can define an access control list specifying which directory service groups and individual users are permitted to access the CTERA Portal, and which user roles they should be assigned in CTERA Portal.

Tip

Users must have an email address, as well as a first and last name, defined in the directory service. Users without one of those attributes in the directory service cannot log in to the CTERA Portal and will cause synchronization to fail.

Tip

Nested groups are not supported.

How Directory Service Synchronization Works

When integrated with a directory service, CTERA Portal fetches user data from the directory upon the following events:

- An administrator can manually fetch specific users from the directory. See ***Manually Fetching User Data*** (on page 130).
- If a user attempts to log in, but does not yet have a local CTERA Portal account, their user account is automatically fetched from the directory.
- CTERA Portal automatically re-fetches all previously fetched directory users, every day at midnight, as part of the daily "Apply provisioning changes" task.
- An administrator can force a re-synchronization of all previously fetched directory users, by running the **Apply Provisioning Changes Wizard**. See ***Applying Provisioning Changes*** (on page 99).

CTERA Portal handles special cases as follows:

- If during the fetch it is determined that a user exists in the local user database but not in the directory, then the user is assumed to have been deleted, and CTERA Portal deletes the user from the local user database. The user's folders are not deleted.
- If the access control list specifies that the user is no longer allowed to access CTERA Portal, then CTERA Portal changes the user account's role to "Disabled". The user account is not deleted.

Tip

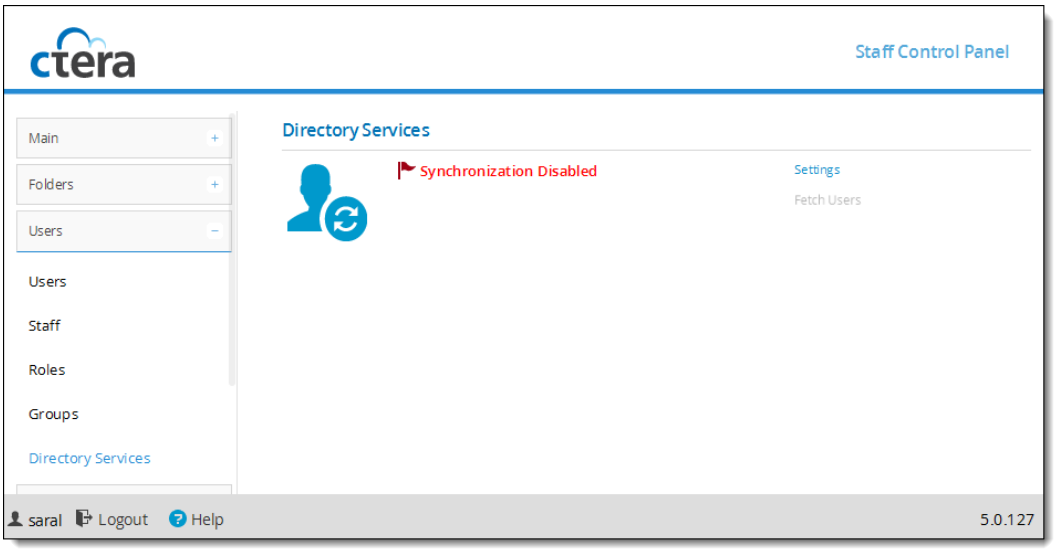
Each virtual portal can optionally be integrated with a different Active Directory or LDAP directory.

Integrating CTERA Portal with an Active Directory Domain, Tree, or Forest

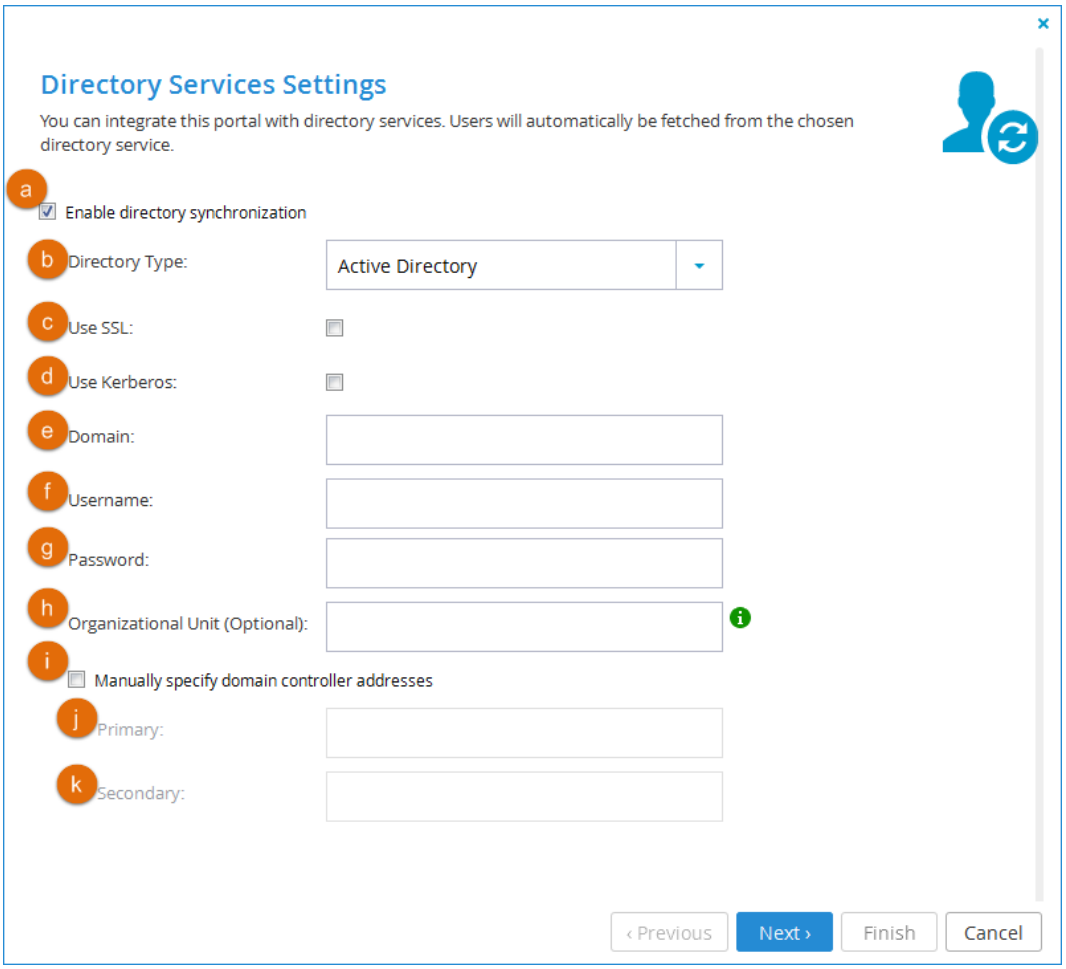
To integrate a virtual portal with an Active Directory domain, tree, or forest

1. In the navigation pane, click **Users > Directory Services**.

   The **Users > Directory Services** page appears.



2 Click **Settings**. and set the Directory Services settings:



a **Enable Directory Synchronization**. Select this option to enable integration with an Active Directory domain.

b **Directory Type**. Select **Active Directory** as the type of directory with which to integrate CTERA Portal.

c **Use SSL**. Select this option to connect to the Active Directory domain using SSL.

d **Use Kerberos**. Select this option to use the Kerberos protocol for authentication when communicating with the Active Directory domain. This is useful for achieving Single Sign On (SSO) with Windows computers. If unchecked, LDAP is used.

Tip

Only one virtual portal, per system, can use Kerberos.

e **Domain**. Type the name of Active Directory domain with which you want to synchronize users.

f **Username**. Type the username that CTERA Portal should use for authenticating to Active Directory.

g **Password**. Type the password that CTERA Portal should use for authenticating to Active Directory.

h **Organizational Unit** (optional). Type the name of the organizational unit (OU) within the Active Directory domain.

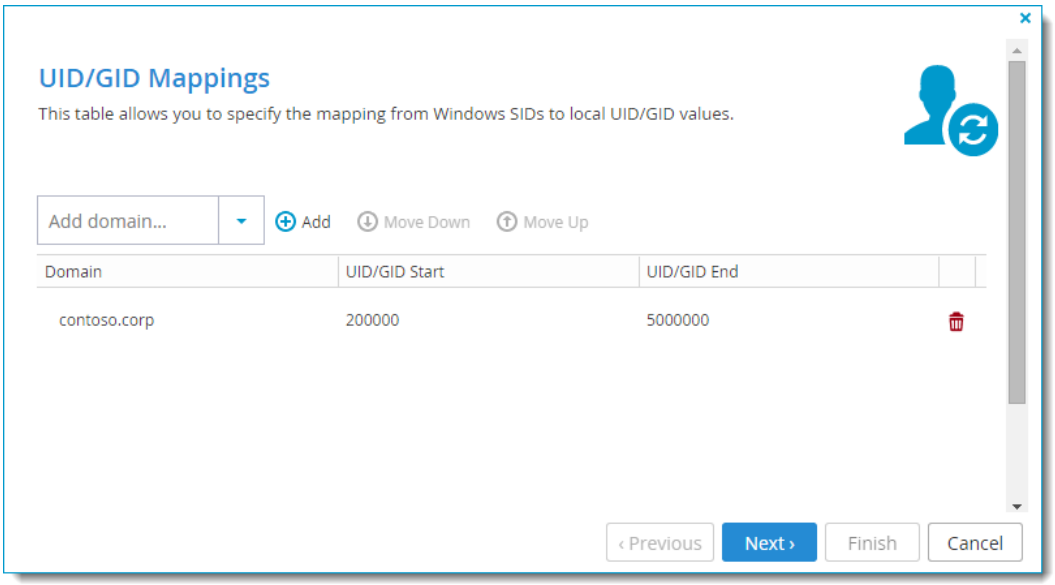
i **Manually specify domain controller addresses**. Select this option to manually specify the IP address of the Active Directory domain controller(s). If unchecked, DNS is used to automatically find the Active Directory domain controller(s).

j **Primary**. If you selected Manually specify domain controller addresses, type the address of the primary Active Directory domain controller.

k **Secondary**. If you selected Manually specify domain controller addresses, type the address of the secondary Active Directory domain controller.

3 Click **Next**.

The UID/GID Mappings dialog box appears.



4 To add the other domains in the tree/forest, do the following for each one:

a In the **Add domain** field, either type the desired domain's name, or select it from the drop-down list.

b Click **Add**.

The domain appears in the table.

c Click in the **UID/GID Start** field, and type the starting number in the range of CTERA Portal user and group IDs (UID/GID) that should be assigned to users and user groups from this domain.

d Click in the **UID/GID End** field, and type the ending number in the range of CTERA Portal user and group IDs (UID/GID) that should be assigned to users and user groups from this domain.

5 To re-order the domains, do any of the following:

- To move a domain up in the table, click on the desired domain, then click **Move Up**.
- To move a domain down in the table, click on the desired domain, then click **Move Down**.

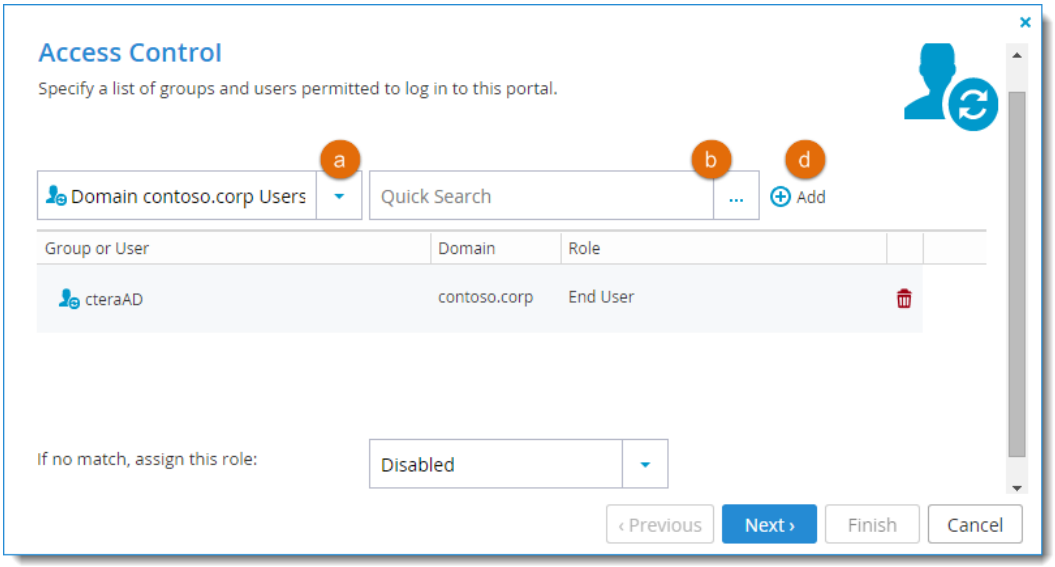
The order in which domains appear in the table represents the order in which the domains will appear in drop-down lists throughout the CTERA Portal interface.

6 To remove a domain, in their row, click .

The domain is removed from the table.

Click **Next**.

The **Access Control** dialog box appears.



7 Add each Active Directory user and user group that should be allowed to access the virtual portal, by doing the following:

a In the drop-down list, select one of the following:

- **Users**. Search the users defined in Active Directory.
- **Groups**. Search the user groups defined in Active Directory.

b In the **Quick Search** field, type a string that appears anywhere within the name of the user or user group you want to add, then click ...

A table of users or user groups matching the search string appears.

c Select the desired user or user group in the table.

The user or user group appears in the **Quick Search** field.

d Click **Add**.

The user or user group is added to the list of users and user groups who should have access to the virtual portal.

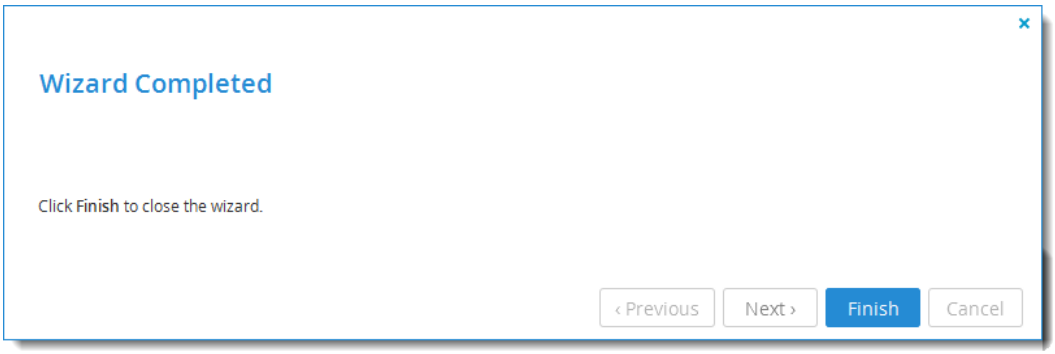
8 To remove a user or user group, in their row, click .

The user or user group is removed from the list.

9 In each user and user group's row, click in the **Role** column, then select the desired user role from the drop-down list:

- **Read/Write Administrator**. The user can access the End User Portal, and can access the Staff Control Panel with read-write permissions.
- **Read Only Administrator**. The user can access the End User Portal, and can access the Staff Control Panel with read-only permissions.
- **End User** (default). The user can access the End User Portal.
- **Disabled**. The user account is disabled. The user cannot access the End User Portal.

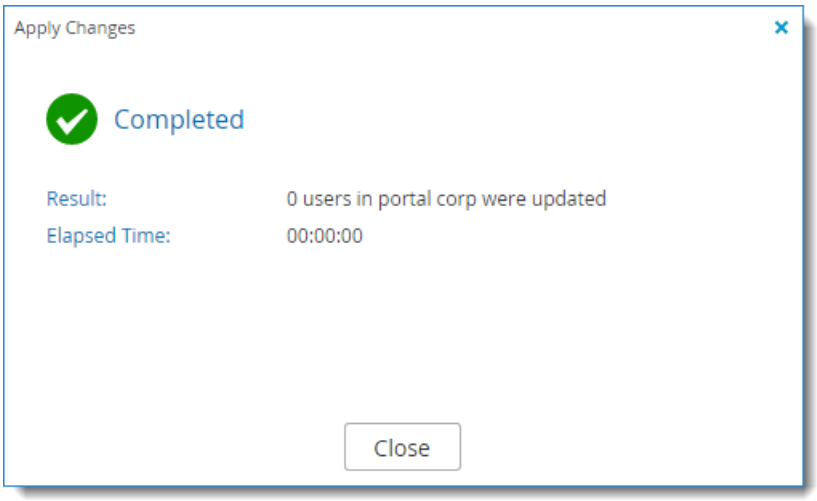
The **Wizard Completed** screen appears.



10 Click **Finish**. The User data is fetched from Active Directory, and the **Apply Changes** window opens displaying **Running** screen with a progress bar that tracks the operation's progress.

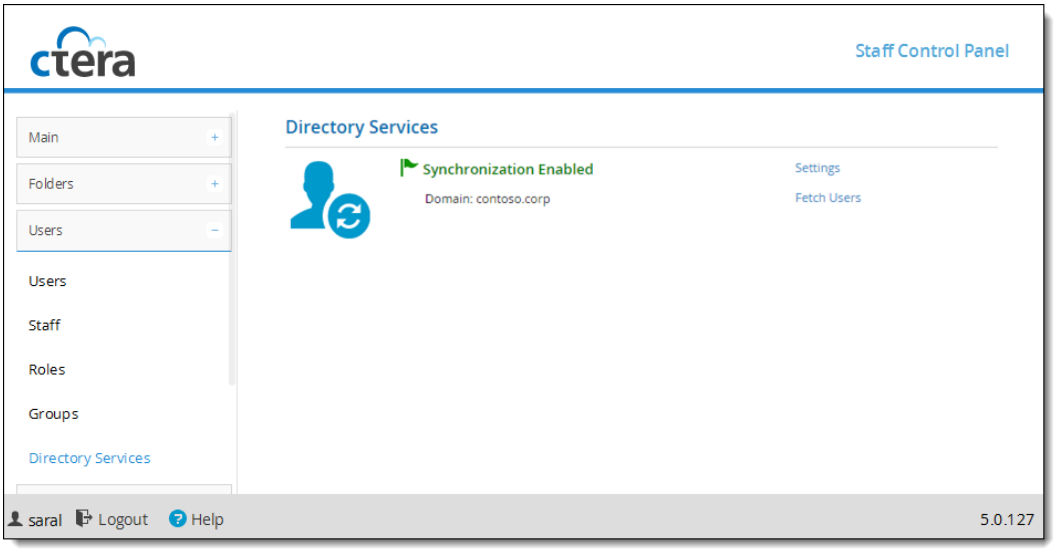
To stop the process, click **Stop**. To close the progress bar, while the process continues in the background, click **Continue in Background**.

When the operation is complete, the **Completed** screen appears.



11 Click **Close**.

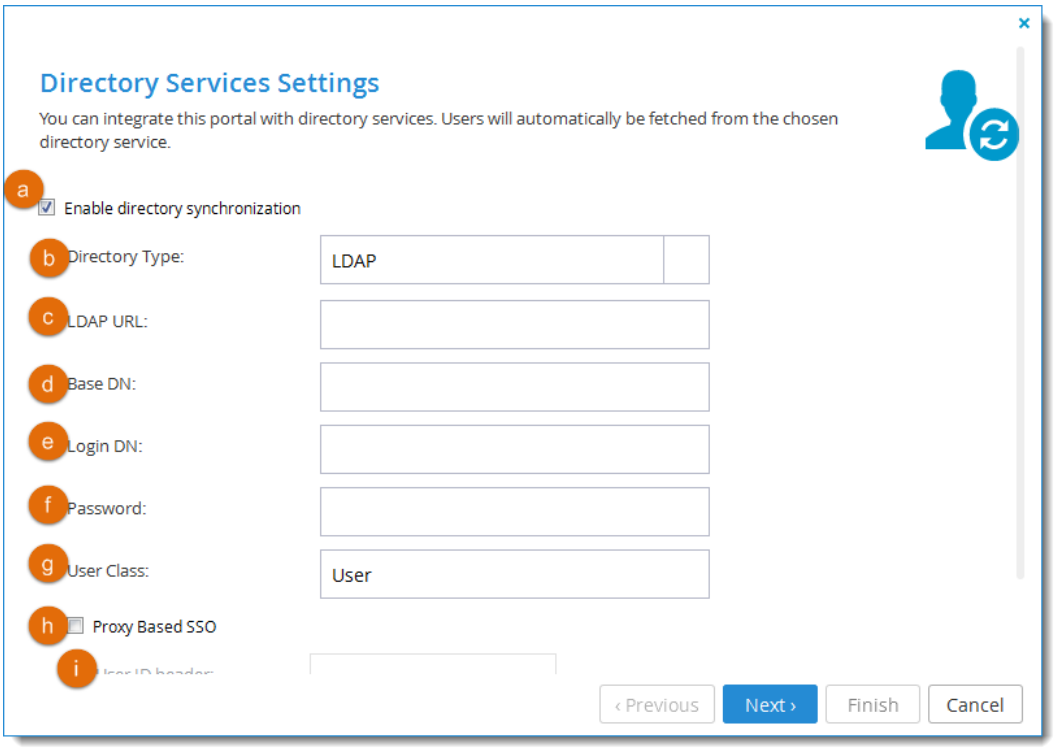
Synchronization with Active Directory is enabled.



Integrating CTERA Portal with an LDAP Directory Server

To integrate a virtual portal with an LDAP directory

1 In the **Users > Directory Services** page, click **Settings**.



2 Complete the fields:

a **Enable Directory Synchronization**. Select this option to enable integration with an LDAP directory service.

b **Directory Type**. Select LDAP as the type of directory service with which to integrate CTERA Portal.

c **LDAP URL**. Type the URL for connecting to the LDAP server.

d **Base DN** (Optional). Type the base DN of the LDAP server.

e **Login DN**. Type the distinguished name of a user with full user read rights, used for binding (authenticating) to the LDAP server (also known as bind DN).

f **Password**. Type the password to use for binding (authenticating) to the LDAP server.

g **User Class**. Type the LDAP object class for user objects in the LDAP directory.

h **Proxy Based SSO**. Check this option to configure an access manager that supports proxy-based SSO (also known as reverse proxy-based SSO). To enable this feature, you also need to enter the User ID Header.

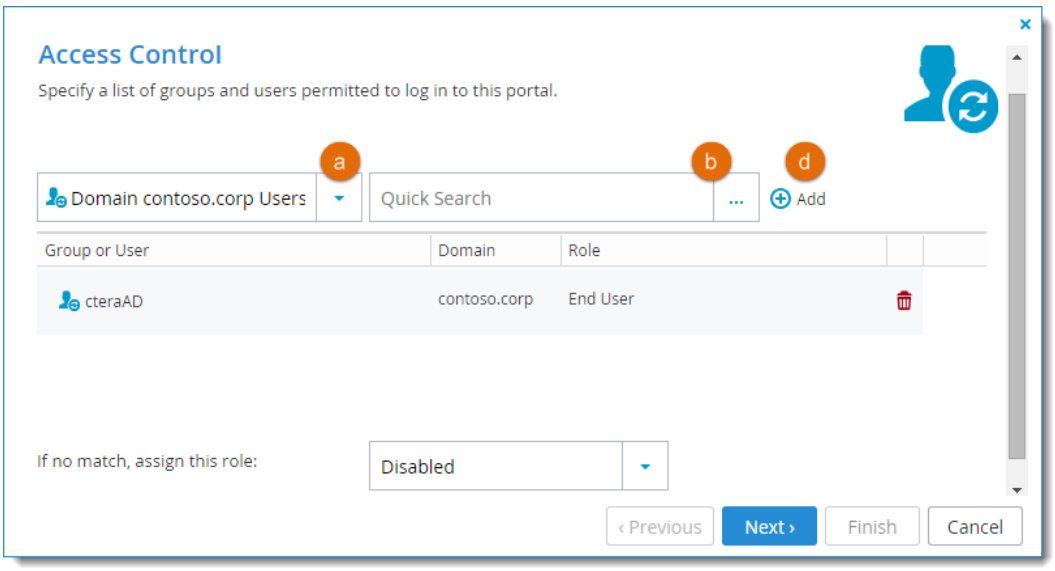
i **User ID Header**. If you checked proxy-based SSO, enter the attribute that your access manager adds to each incoming HTTP request.

3 Click **Next**.

The Advanced LDAP Mappings dialog box appears.

4 To configure the portal to match a custom LDAP schema, edit the LDAP mappings by clicking the LDAP attributes to enter the attributes that map to the corresponding user properties.

5 Click **Next** and add each LDAP directory user and user group that should be allowed to access the virtual portal:



a In the **Users** drop-down list, select one of the following:

- **Users**. Search the users defined in the LDAP directory.
- **Groups**. Search the user groups defined in the LDAP directory.

b In the **Quick Search** field, type a string that appears anywhere within the name of the user or user group you want to add, then click ... .

A table of users or user groups matching the search string appears.

c Select the desired user or user group in the table.

The user or user group appears in the **Quick Search** field.

d Click **Add**.

The user or user group is added to the list of users and user groups who should have access to the virtual portal.

6 To remove a user or user group, in their row, click .

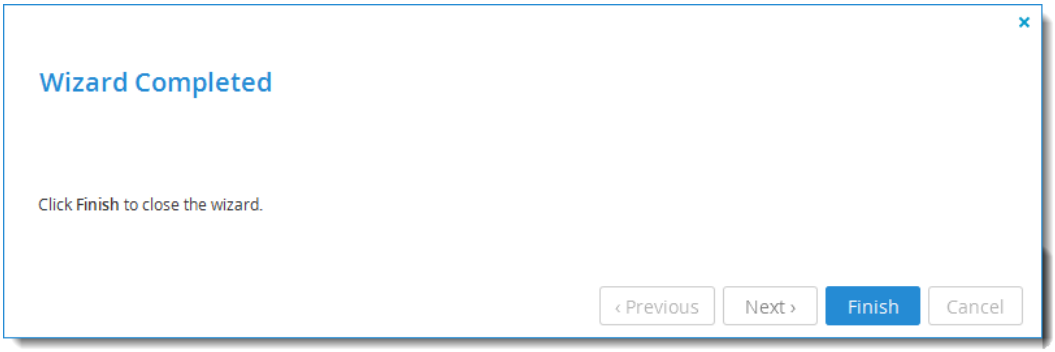
The user or user group is removed from the list.

In each user and user group's row, click in the **Role** column, then select the desired user role from the drop-down list:

- **Read/Write Administrator**. The user can access the End User Portal, and can access the Staff Control Panel with read-write permissions.
- **Read Only Administrator**. The user can access the End User Portal, and can access the Staff Control Panel with read-only permissions.
- **End User** (default). The user can access the End User Portal.
- **Disabled**. The user account is disabled. The user cannot access the End User Portal.

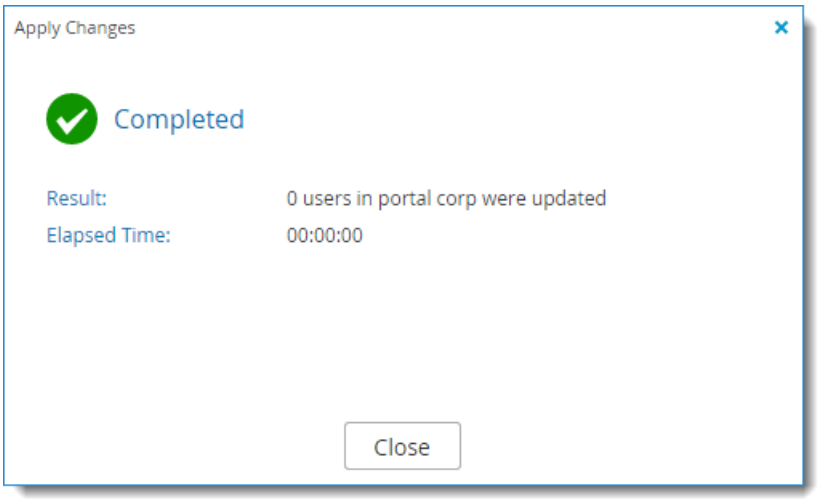
7 Click **Next**.

The **Wizard Completed** screen appears.



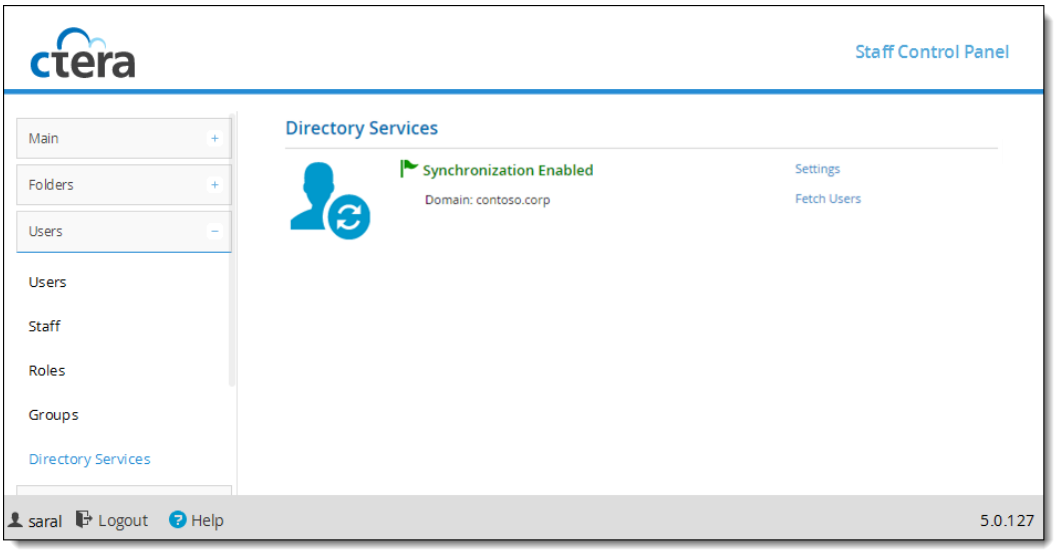
Click **Finish**. User data is fetched from the LDAP directory.

When the operation is complete, the **Completed** screen appears.



Click **Close**.

Synchronization with the LDAP directory is enabled.



Manually Fetching User Data

If desired, you can manually fetch user data from an integrated Active Directory, LDAP directory, or Apple Open Directory. This is useful in the following situations:

- If you would like to immediately update data in the local user database, instead of waiting for CTERA Portal to automatically fetch data at midnight.
- If you would like to create an account for a user that does not yet exist in the local user database, before their first login.

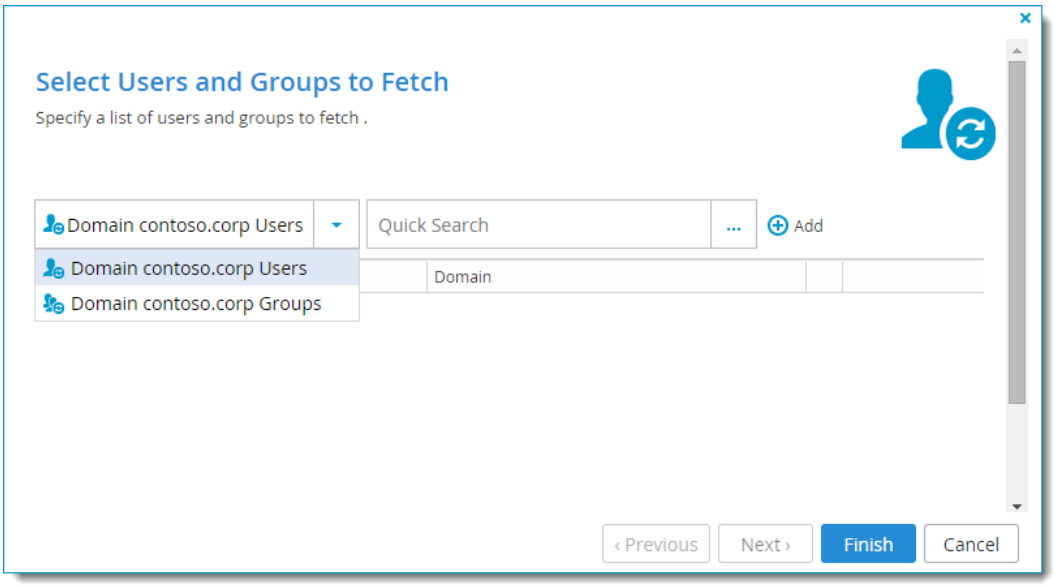
To manually fetch user data

1. Select **Users > Directory Services** from the menu.

   The **Users > Directory Services** page appears.

2. Click **Fetch Users**.

The **Fetch Users Wizard** appears, displaying the **Select Users and Groups to Fetch** dialog box.



3 Add each user and user group from the directory service for which you would like to fetch data, by doing the following:

a In the **Users** drop-down list, select one of the following:

- **Users**. Search the users defined in the integrated directory service.
- **Groups**. Search the user groups defined in the integrated directory service.

b In the **Quick Search** field, type a string that appears anywhere within the name of the user or user group you want to add, then click ... .

A table of users or user groups matching the search string appears.

c Select the desired user or user group in the table.

The user or user group appears in the **Quick Search** field.

d Click **Add**.

The user or user group is added to the list of users and user groups for which data should be fetched.

4 To remove a user or user group, in their row, click .

The user or user group is removed from the list.

5 Click **Finish**.

The following things happen:

- User data is fetched from the directory service, and the **Apply Changes** window opens displaying **Running** screen with a progress bar that tracks the operation's progress.

To stop the process, click **Stop**. To close the progress bar, while the process continues in the background, click **Continue in Background**.

- When the operation is complete, the **Completed** screen appears.

6. Click **Close**.

11

Provisioning

In This Chapter

Overview

Plans, Add-ons, and Vouchers

User accounts need to be provisioned in order for end users to obtain services. This is done by setting the subscription plan, or adding add-ons to the user account.

If a subscription plan or add-on is modified, all user accounts assigned to the plan or add-on is automatically updated with the changes.

The following provisioning methods are available for end-user provisioning:

- **Subscription plans**

In order to obtain services, end users can be subscribed to a *subscription plan*. The subscription plan includes the list of services provided to the user and the quota for each service.

The subscription plan also specifies a snapshot retention policy for the user's folders.

- **Add-ons**

  End users can subscribe to more services in addition to their subscription plan, by adding add-ons to the account. Each *add-on* defines a set of services that subscribed users will receive in addition to the services specified in the subscription plan, for a specified period of time. For example, an add-on may include an additional 10 GB of storage space for the number of devices specified in the subscription plan.

  Add-ons can be stacked as desired. For example, a user may have a subscription plan for 100 GB of storage, as well as two add-ons for 10GB of storage and one add-on for 5GB of storage. While the add-ons are valid, the user will be entitled to 125GB of cloud storage.

- **Vouchers**

  Vouchers are prepaid coupons that encapsulate specific add-ons and plans. When a device owner redeems a voucher encoding an add-on, the add-on is added to the user's account. When a device owner redeems a voucher encoding a plan, they are assigned to the subscription plan.

Tip

Vouchers can also contain a hidden plan that is not exposed to end users.

Tip

In order to use vouchers, vouchers support must be enabled in the CTERA Portal general settings. See ***General Settings*** (on page 166).

- CTERA Portal allows you to mix and match these provisioning methods in order to obtain the combination that best suits your company's business model and your customer's needs.

Snapshot Retention Policies

The CTERA Portal retains previous file versions for each user, by using snapshots. *Snapshots* are read-only copies of files as they were at a particular point in time.

The CTERA Portal creates snapshots automatically and retains them according to a configurable *snapshot retention policy* that is provisioned via subscription plans. So long as a snapshot is retained by CTERA Portal, the relevant version of the user data can be retrieved.

What Does a Snapshot Retention Policy Specify?

A retention policy specifies the following:

- **The number of hours to retain all snapshots**

  Every snapshot is retained for this amount of time. After this time has passed for any given snapshot, the snapshot may be retained or deleted depending on the other settings.

- **The number of hourly snapshots to retain**

  For example, if hourly snapshots are set to 10, then the last 10 hourly snapshots will be retained. If daily snapshots are set to 0, then the hourly snapshot will be deleted when the next hour starts.

- **The number of daily snapshots to retain**

  For example, if daily snapshots are set to 10, then the last 10 daily snapshots will be retained. If daily snapshots are set to 0, then the daily snapshot will be deleted when the next day starts.

  Tip

  A day is defined as starting at 00:00:00 and ending at 23:59:59.

- **The number of weekly snapshots to retain**

  A weekly snapshot is the latest snapshot taken during the week.

  Tip

  A week is defined as starting on Monday and ending on Sunday.

  Example 1:

  Let's say snapshots were successfully taken every day until the current day, which is Sunday. The weekly snapshot is the one taken on Sunday, as it is the latest snapshot taken this week.

  Example 2:

  Snapshots were successfully taken every day until the current day, except the Saturday and Sunday snapshots, which were not taken because the device was turned off. The weekly snapshot is the one taken on Friday, as it is the latest snapshot taken this week.

- **The number of monthly snapshots to retain**

  A monthly snapshot is the latest snapshot taken during the month.

  Example 1:

Let's say snapshots were successfully taken every day until the current date, which is April 30th. The monthly snapshot is the one taken on the 30th, as it is the latest snapshot taken this month.

Example 2:

Snapshots were successfully taken every day until the current date, except snapshots for the 25th through the 30th, which were not taken because the device was turned off. The monthly snapshot is the one taken on the 24th, as it is the latest snapshot taken this month.

The number of quarterly snapshots to retain

A quarterly snapshot is the latest snapshot taken during the quarter.

Example 1:

Let's say snapshots were successfully taken every day until the current date, which is the March 31. The quarterly snapshot is the one taken on March 31st, as it is the latest snapshot taken this quarter.

Example 2:

Snapshots were successfully taken every day until the current date, except snapshots for March 25 through 31 were not taken because the device was turned off. The quarterly snapshot is the one taken on March 24th, as it is the latest snapshot taken this quarter.

The number of yearly snapshots to retain

A yearly snapshot is the latest snapshot taken during the year.

Example 1:

Let's say snapshots were successfully taken every day until the current date, which is the December 31st. The yearly snapshot is the one taken on the 31st, as it is the latest snapshot taken this year.

Example 2:

Snapshots were successfully taken every day until the current date, except snapshots for the 25nd through the 31st were not taken because the device was turned off. The yearly snapshot is the one taken on the 24th, as it is the latest snapshot taken this year.

The numbers of days to keep deleted files

The default retention period for deleted files is 30 days.

When portal users delete a file or a folder either via the Web interface, or via the local synchronization folder, the deleted data is moved to a recycle bin. It is then retained in the recycle bin for a period of time (in days) defined in the retention policy of the user's assigned subscription plan. As long as files are retained, users can recover their deleted data from their Cloud Drive using a Recycle Bin feature in the end user portal interface.

CTERA Portal Snapshot Retention for the Cloud Drive Service

Each user account that uses the Cloud Drive service is assigned a home folder in the CTERA Portal, upon creation of the user account. The home folder (Cloud Drive) serves as the block destination for CTERA Cloud Gateway and CTERA Cloud Agent sync operations. Snapshots of Cloud Drive folders are taken for each folder once every five minutes, if there were any changes in the folder during that five minutes.

CTERA Portal Snapshot Retention for the Cloud Backup Service

Each CTERA C Series cloud gateway and CTERA Cloud Agent that uses the Cloud Backup service is assigned a dedicated backup folder in the CTERA Portal, which serves as the block destination for the cloud gateway or Cloud Agent.

When a CTERA cloud gateway or CTERA Cloud Agent initiates a Cloud Backup job, the CTERA Portal automatically creates a snapshot of the cloud gateway's or Cloud Agent's backup folder. The snapshot's timestamp is the time at which the Cloud Backup job was initiated by the client.

Snapshot Consolidation

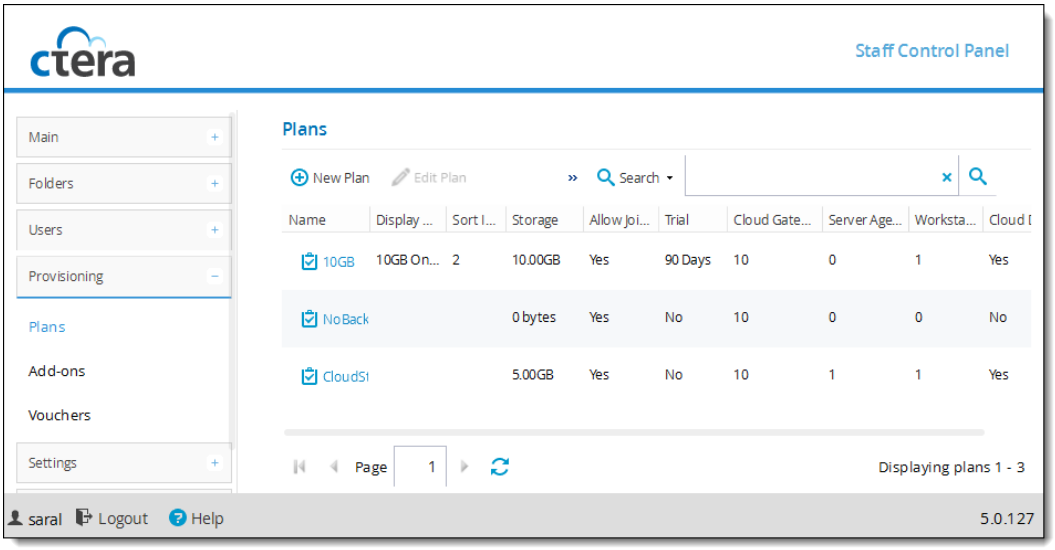
The snapshot consolidator is a scheduled job that runs once a day at midnight. It is responsible for deleting all the snapshots that should not be retained, according to the retention policy.

Viewing Plans

To view all subscription plans in the portal

1. In the navigation pane, click **Provisioning > Plans**.

   The **Provisioning > Plans** page appears, displaying all subscription plans.



   If a default subscription plan is defined, it is marked with the icon.

   The table includes the following columns.

Table 6: Plans Fields

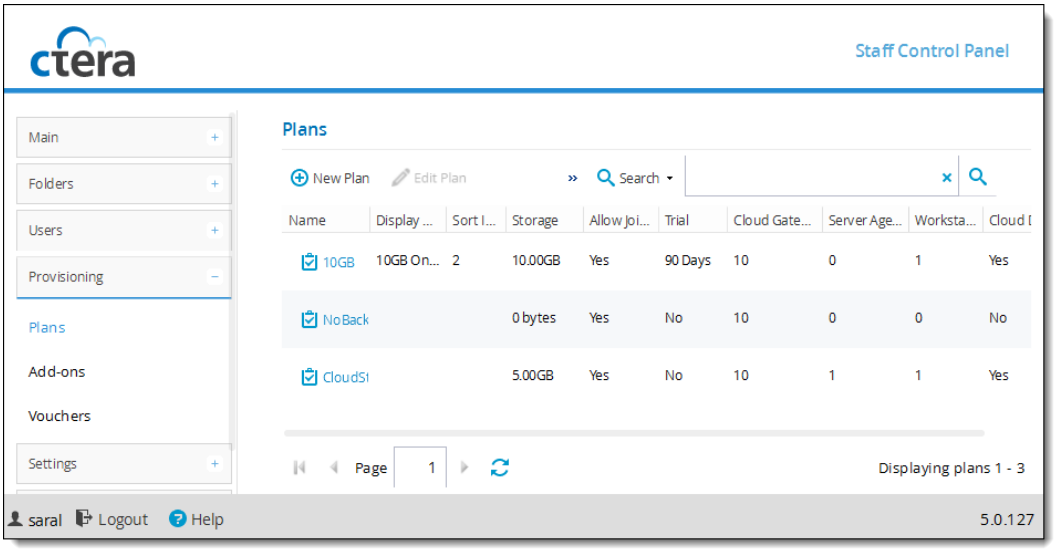
This field...	Displays...
Name	The subscription plan's name. To edit the subscription plan, click the subscription plan name. For further details, see ***Adding and Editing Subscription Plans*** (see "***Adding and Editing Plans***" on page 140).
Display Name	The subscription plan's name, as displayed in the End User Portal and notifications.
Sort Index	An index number assigned to the subscription plan, in order to enable custom sorting of the subscription plans displayed to end users in the **Subscribe to Plan** wizard.
Storage	The amount of storage space included in the plan.
Allow Joining	Indicates whether users can subscribe to this plan from the End User Portal (**Yes**/**No**). **Note**: If set to **No**, an administrator can still assign users to this plan.
Trial	If the plan includes a free trial period, this column displays the number of days included in the free trial period. If the plan does not include a free trial period, this column displays **No**.
Cloud Gateway Licenses	The number of CTERA cloud gateway licenses included in the plan. A CTERA cloud gateway license is consumed by a CTERA cloud gateway connected to a CTERA Portal user account.
Server Agent Licenses	The number of CTERA Server Agent licenses included in the plan. A Server Agent license is consumed by a Server Agent in Cloud Agent mode using the CTERA Cloud Backup service.
Workstation Backup Licenses	The number of CTERA Workstation Backup licenses included in the plan. A workstation backup license is consumed by a CTERA Workstation Agent in Cloud Agent mode using the CTERA Cloud Backup service.
Cloud Drive Licenses	Whether a CTERA Cloud Drive license is included in the plan. A Cloud Drive license enables the user to connect and sync data to the CTERA Portal for up to five devices associated with the user account, including: CTERA Agents (Server or Workstation Backup) and mobile devices (iPhone, iPad, and so on).

Adding and Editing Plans

To add or edit a subscription plan

1 In the navigation pane, click **Provisioning > Plans**.

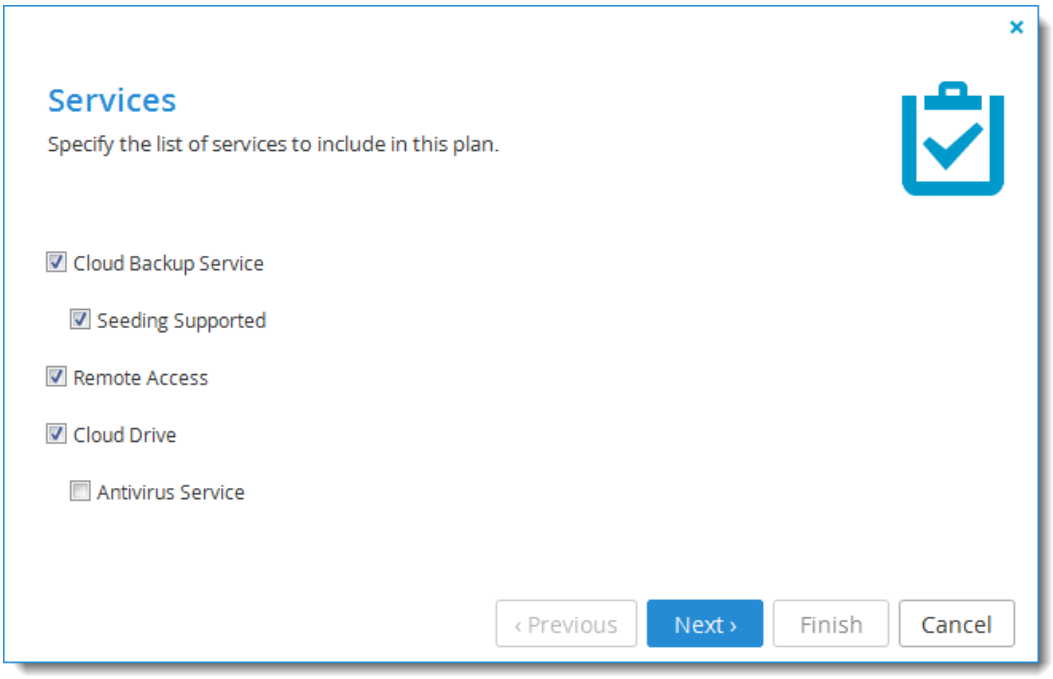
The **Provisioning > Plans** page appears, displaying all subscription plans.



2 Do one of the following:

- To add a new subscription plan, click **New Plan**.
- To edit an existing subscription plan, select the desired subscription plan's row and then click **Edit Plan.**

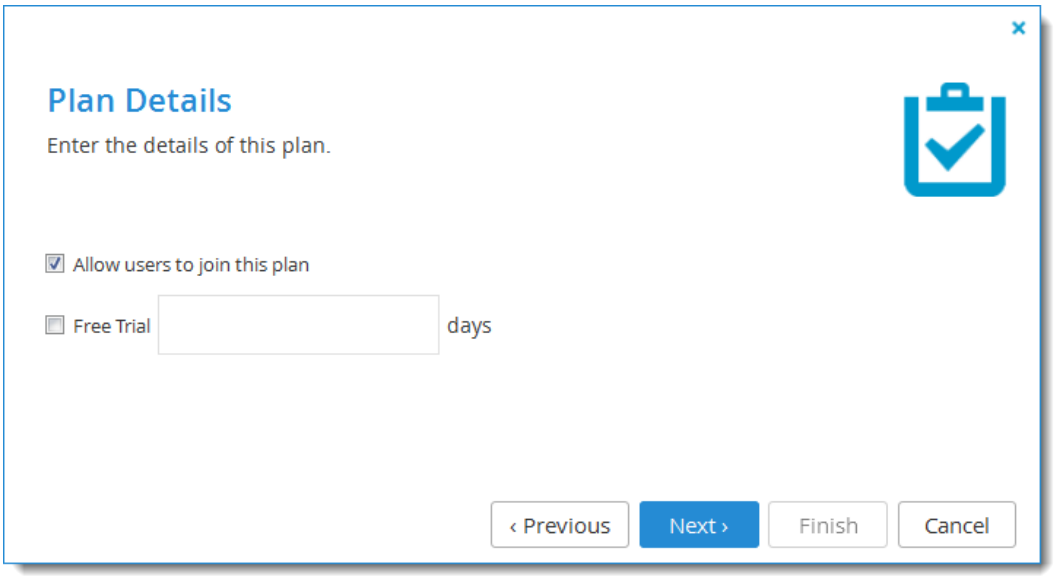
The **Plan Details Wizard** opens displaying the **Services** dialog box.



3 Choose which services to include in the plan:

- **Cloud Backup Service**. Indicates that the Cloud Backup Service is included in the subscription plan.
- **Seeding Supported**. Select this option to include backup seeding in the subscription plan.
- **Remote Access**. Select this option to include remote access in the subscription plan. Remote access includes both access to the device's management interface via the CTERA Portal and a dedicated URL, access to the user's files via the CTERA Portal and a dedicated URL.
- **Note:** Device owners can disable remote access via the device's management interface.
- **Cloud Drive**. Select this option to include private cloud drives in the subscription plan. In a team portal, users will be able to access the private cloud drive in addition to the team cloud drive. Users will be able to access their cloud drives via the End User Portal's Files tab, for the purpose of viewing, uploading, and downloading files.
- **Antivirus Service**. Select this option to include the Cloud Drive antivirus service in the plan. When antivirus is activated, files are scanned for malware automatically and transparently, before they are downloaded for the first time. The Cloud Drive antivirus service requires an additional license.

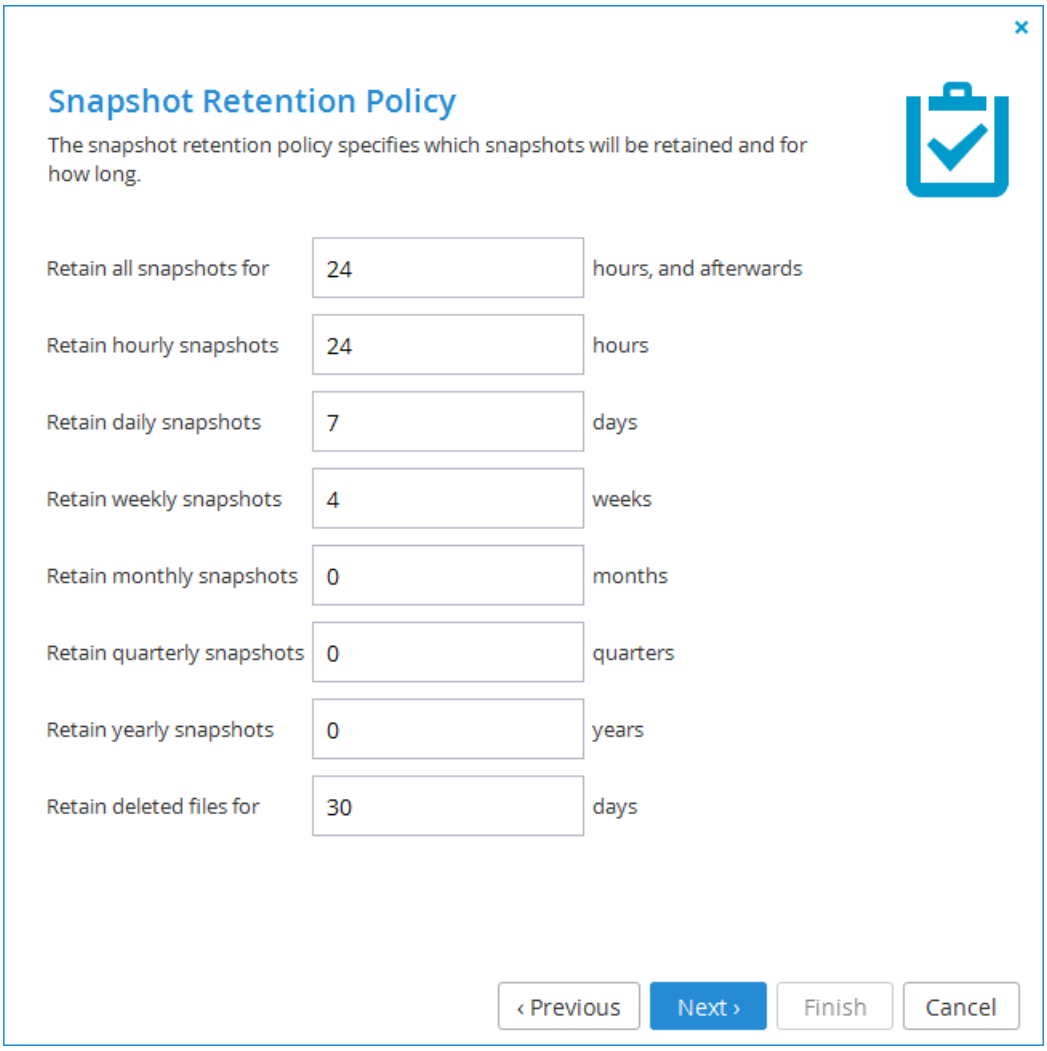
4 Click **Next**.



5 Select **Allow users to join this plan** to allow users to subscribe to this subscription plan. If this option is not selected, the subscription plan is invisible to end users, and only administrators can assign users to this plan.

6 Select **Free Trial** to include a free trial period in the subscription plan. Then type the desired number of days that subscribers should receive the subscription plan for free.

7 Click **Next**.



8 Set the snapshot retention policy:

- **Retain all snapshots for**. Type the number of hours after creation that all snapshots should be retained for.
- **Retain hourly snapshots**. Type the number of hourly snapshots that should be retained.
- **Retain daily snapshots**. Type the number of daily snapshots that should be retained.
- **Retain weekly snapshots**. Type the number of weekly snapshots that should be retained.
- **Retain monthly snapshots**. Type the number of monthly snapshots that should be retained.
- **Retain quarterly snapshots**. Type the number of quarterly snapshots that should be retained.

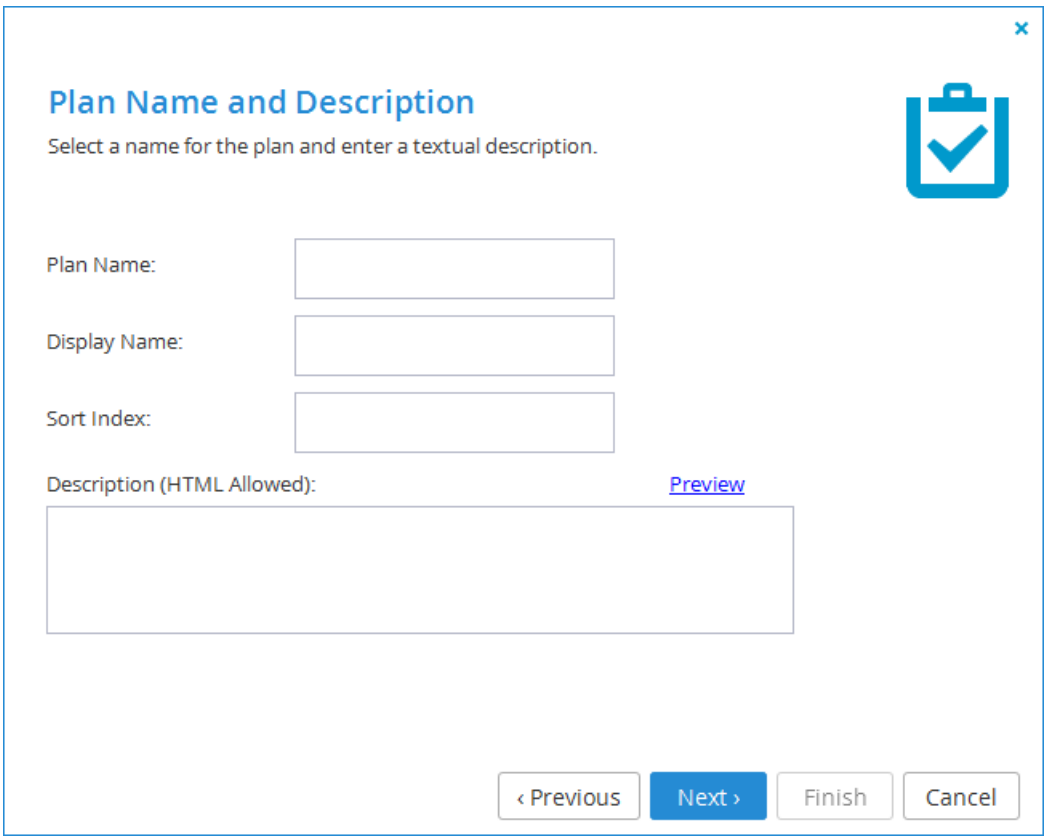
- **Retain yearly snapshots**. Type the number of yearly snapshots that should be retained.
- **Retain deleted files for**. Type the number of days to retain deleted files.

Tip

For an explanation of each policy, see ***Understanding Snapshot Retention Policies*** (see "***Snapshot Retention Policies***" on page 134).

9 Click **Next**.

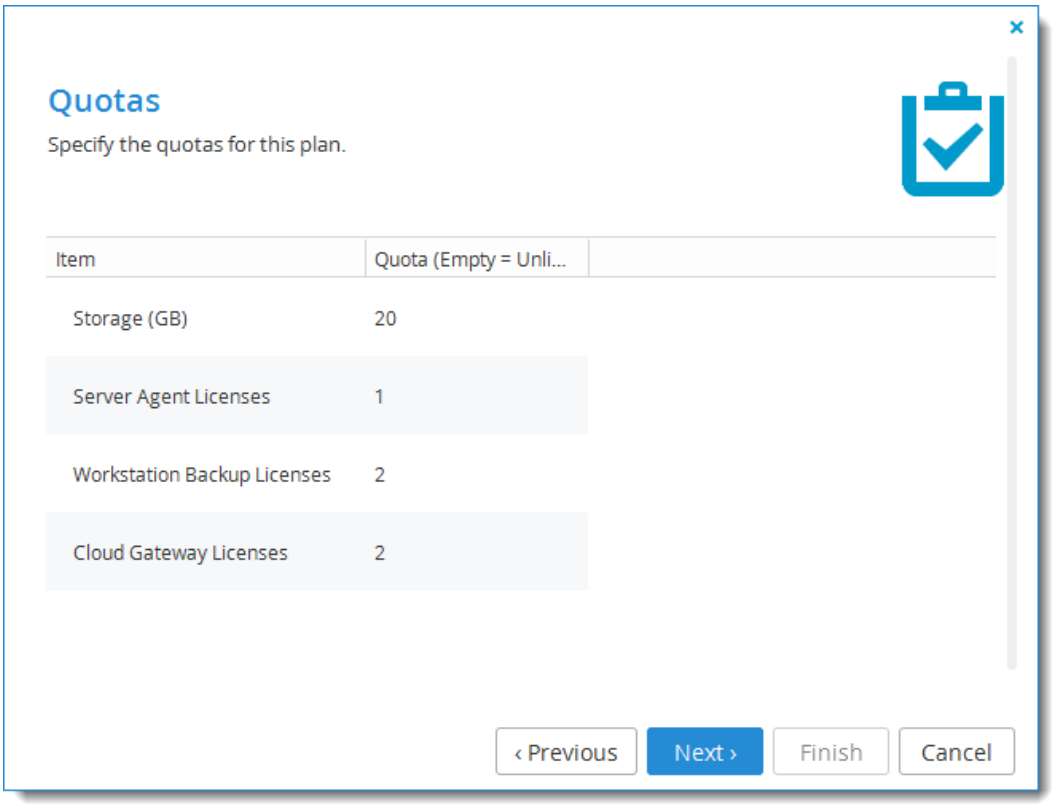
The **Plan Name and Description** dialog box appears.



10 Fill in the name and description for the plan:

- **Plan Name**. Type a name for the subscription plan.
- **Display Name**. Type the name to use when displaying this subscription plan in the End User Portal and notifications.
- **Sort Index**. Type an index number to assign the subscription plan, in order to enable custom sorting of the subscription plans displayed to end users in the Subscribe to Plan wizard. This field is optional.
- **Description**. Type a description of the subscription plan. HTML is supported.
- **Preview**. Click this button to view a preview of the subscription plan description in a new window.

11 Click **Next**.



12 For each item, click in the **Quota** field, and then type the number of item units to include in the subscription plan.

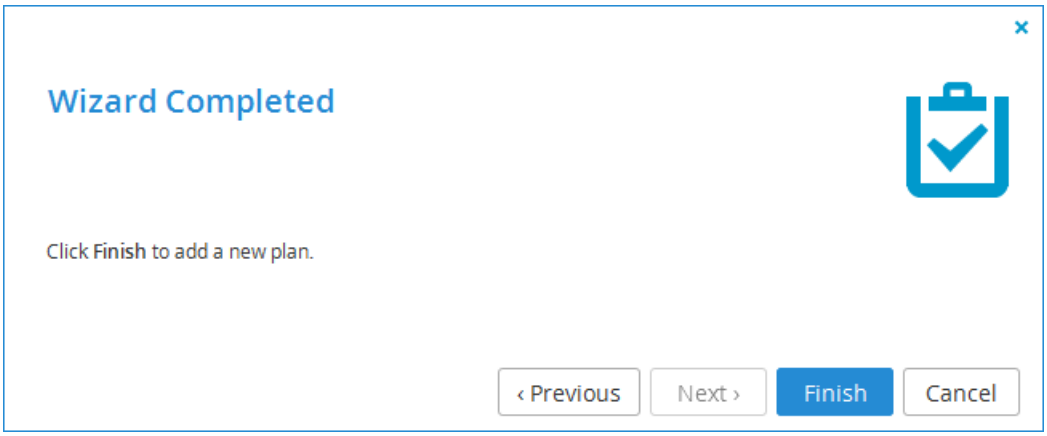
For example, to include 5GB of storage space, click in the Storage Quota (GB) item's **Quota** field and type 5.

Tip

The specified license quotas must not exceed the number specified in the license. Otherwise, an error message will appear when you attempt to assign a user to this plan.

13 Click **Next**.

The **Wizard Completed** screen appears.



14 Click **Finish**.

If you edited an existing plan, the following things happen:

- Provisioning changes are applied to all users, and the **Apply Provisioning Changes** window opens displaying **Running** screen with a progress bar that tracks the operation's progress.

  To stop the process, click **Stop**. To close the progress bar, while the process continues in the background, click **Continue in Background**.

- When the operation is complete, the **Completed** screen appears.

15 Click **Close**.

Setting/Removing the Default Plan

The default subscription plan is automatically assigned to all new user accounts.

To set a subscription plan as the default

1 Select **Provisioning > Plans** from the menu.

The **Provisioning > Plans** page appears, displaying all subscription plans.

2 Select the desired subscription plan's row.

3 Click **Set Default.**

The selected subscription plan becomes the default subscription plan and is marked with the icon.

To remove a subscription plan from being the default

1 Select **Provisioning > Plans** from the menu.

The **Provisioning > Plans** page appears, displaying all subscription plans.

2 Select the default subscription plan's row.

3 Click **Remove Default.**

The subscription plan is no longer the default, and the icon is removed.

Automatically Assigning Plans

Automatic Plan Assignment allows you to define a policy that determines which subscription plan will be assigned to which users.

You can automatically assign subscription plans based on the following user attributes:

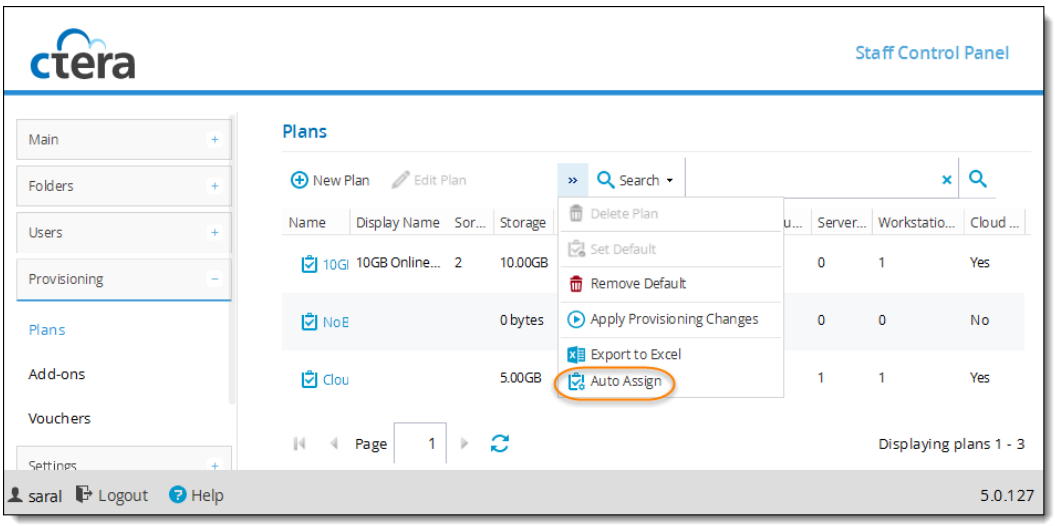
- Username
- User Groups
- Role
- First Name
- Last Name
- Company
- Billing ID
- Comment

The policy rules are processed in ascending order. The first rule that matches applies. You can change the rules' order by using the Move Down/Move Up buttons. You can also choose to apply a default plan in the event that no rule applies.

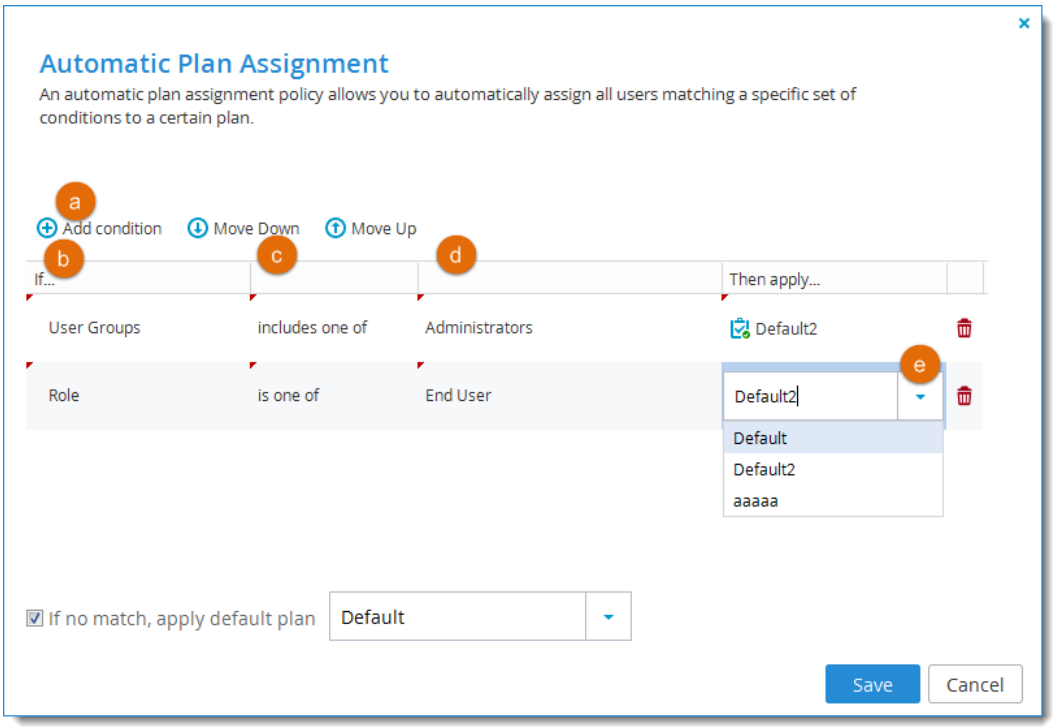
This feature is particularly useful if the portal is integrated with a ***Directory Service*** (see "***Using Directory Services***" on page 119). It allows you to define a policy even before users have joined the service, so that when users join, they will be automatically assigned the appropriate quota and licenses.

To configure automatic plan assignment

1 On the **Provisioning > Plans** page, select **Auto Assign**.



2 Add conditions for auto assignment:



a. Click **Add condition**.

b. Select a user attribute.

c. Select an operator, such as "includes one of".

d. Select a value for the operator.

e. Select the subscription plan to apply if a user satisfies the condition.

3. To delete any conditions that you added, click  in the row for the condition.

4. When you're done adding conditions, click **Save**.

Exporting Subscription Plans to Excel

You can export plans to a CSV file that can be opened with Microsoft Excel.

To export plans

1. Select **Provisioning > Plans** from the menu.

   The **Provisioning > Plans** page appears, displaying all subscription plans.

2. Click **Export to Excel**.

   All subscription plans are exported to a CSV file.

Applying Provisioning Changes

CTERA Portal applies changed plan and add-on settings to all users every day at midnight. If desired, you can use the following procedure to apply all changes immediately.

To apply provisioning changes

1. Select **Provisioning > Plans** from the menu.

   The **Provisioning > Plans** page appears, displaying all subscription plans.

2. Click **Apply Provisioning Changes**.

   The following things happen:

   - Provisioning changes are applied to all users, and the **Apply Provisioning Changes** window opens displaying **Running** screen with a progress bar that tracks the operation's progress.

     To stop the process, click **Stop**. To close the progress bar, while the process continues in the background, click **Continue in Background**.

   - When the operation is complete, the **Completed** screen appears.

3. Click **Close**.

Deleting Subscription Plans

To delete a plan

1. Select the plan's row.
2. Click **Delete Plan.**
3. Click **Yes** to confirm.

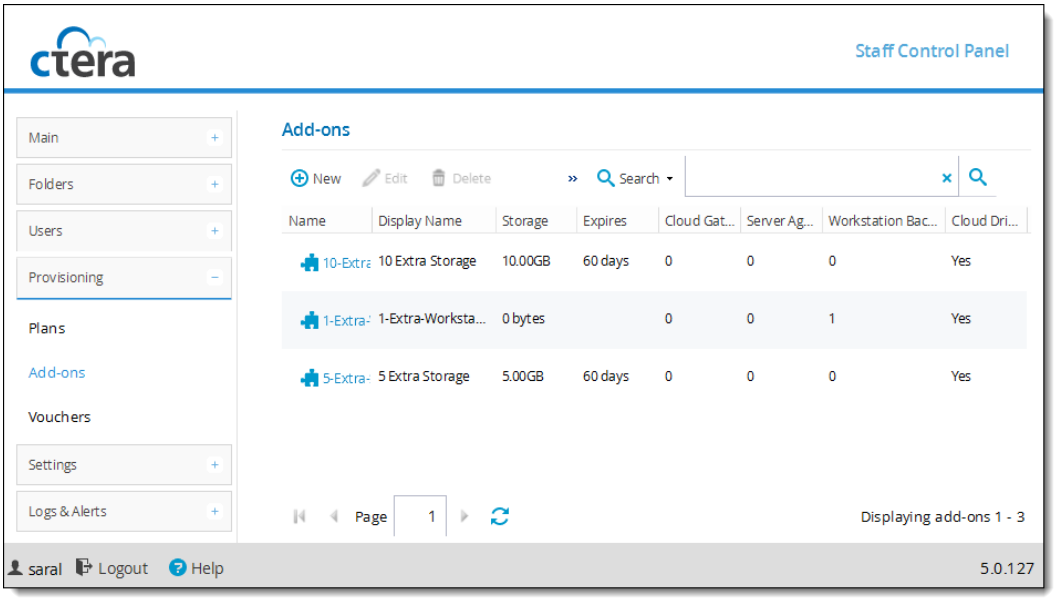
   The subscription plan is deleted.

Viewing Add-ons

To view all add-ons in the portal

In the navigation pane, click **Provisioning > Add-ons**.

The **Provisioning > Add-ons** page appears, displaying all add-ons.



The table includes the following columns.

Table 7: Add-ons Fields

This field...	Displays...
Name	The add-on's name. To edit the add-on, click the add-on name. For further details, see ***Adding and Editing Add-ons*** (on page 151).
Display Name	The add-on's name, as displayed in the End User Portal and notifications.
Storage	The amount of storage space included in the add-on.
Expires	The number of days after adding this add-on, that the add-on will expire.
Cloud Gateway Licenses	The number of CTERA cloud gateway licenses included in the add-on.
Server Agent Licenses	The number of CTERA Server Agents included in the add-on.
Workstation Backup Licenses	The number of CTERA Workstation Backup licenses included in the add-on.
Cloud Drive Licenses	The number of CTERA Cloud Drive licenses included in the add-on.

Adding and Editing Add-ons

Once you have added an add-on to the portal, you can then add the add-on directly to user accounts, as described in ***Adding Add-ons to User Accounts*** (on page 90). Alternatively, for a "pre-paid" business model, you can create vouchers for the add-on, as described in ***Adding Vouchers*** (on page 158). End users can then redeem the vouchers in order to add the add-on to their user accounts.

To add or edit an add-on

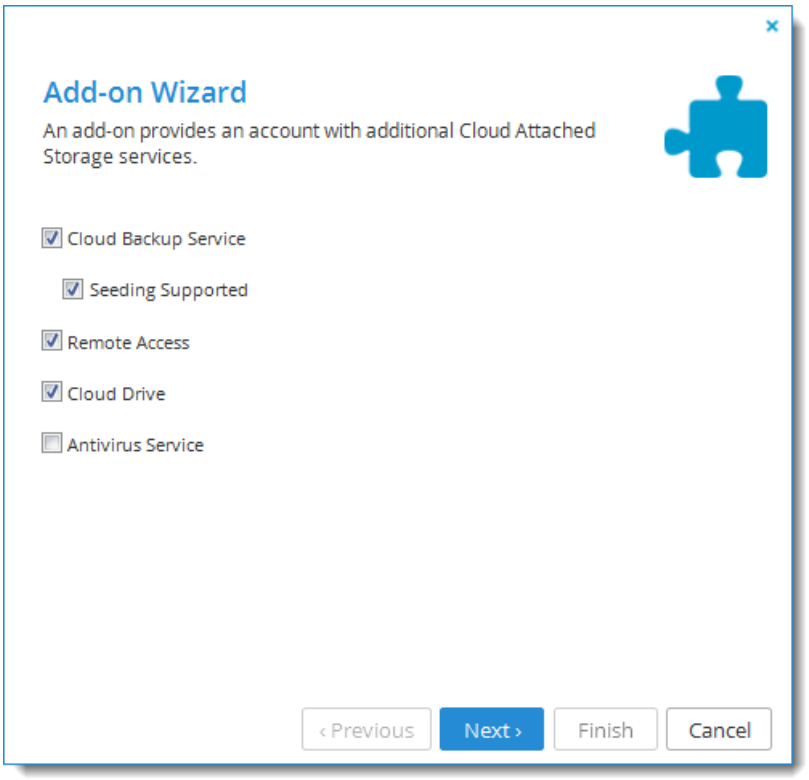
1. In the navigation pane, click **Provisioning > Add-ons**.

   The **Provisioning > Add-ons** page appears, displaying all add-ons.

2. Do one of the following:

   - To add a new add-on, click **New**.
   - To edit an existing add-on, select the desired add-on's row and then click **Edit.**

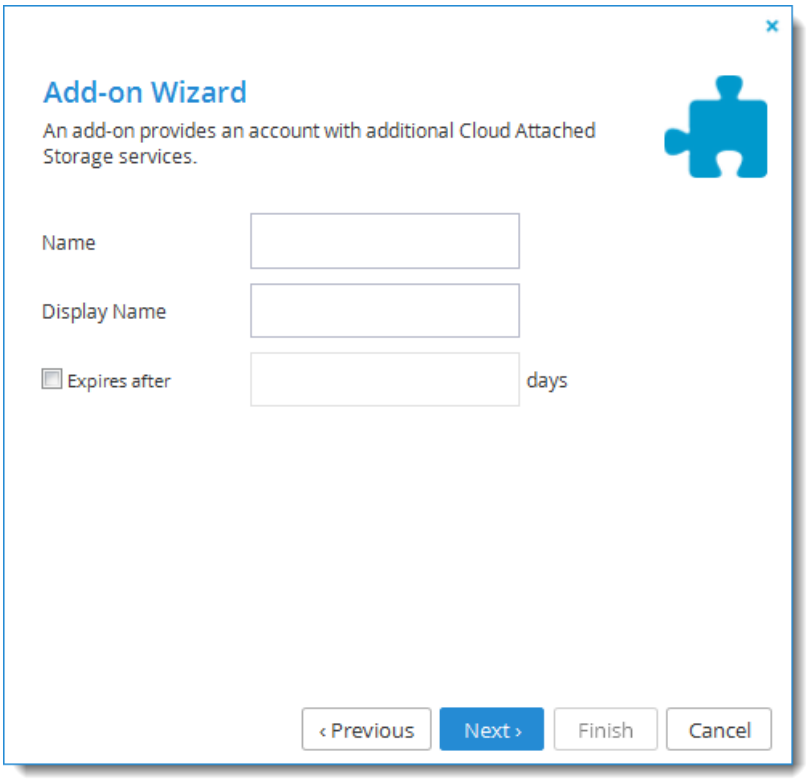
The **Add-on Wizard** opens displaying the **Add-on Wizard** dialog box.



3 Complete the fields using the information in ***Add-on Services Fields*** (page 156).

4 Click **Next**.

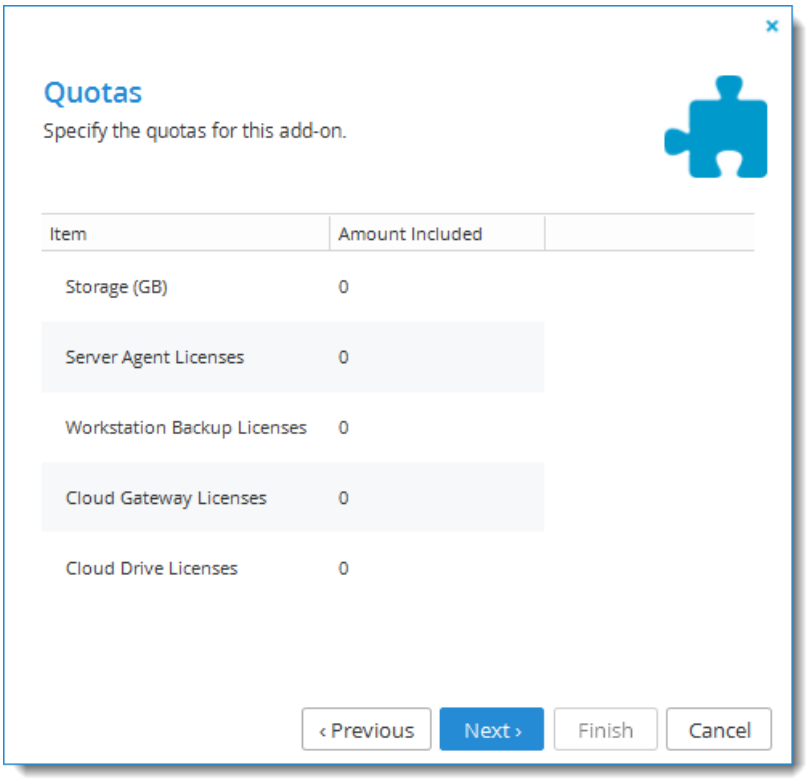
A second **Add-on Wizard** dialog box appears.



5 Complete the fields using the information in ***Add-on Details Fields*** (page 156).

6 Click **Next**.

The **Quotas** dialog box appears.

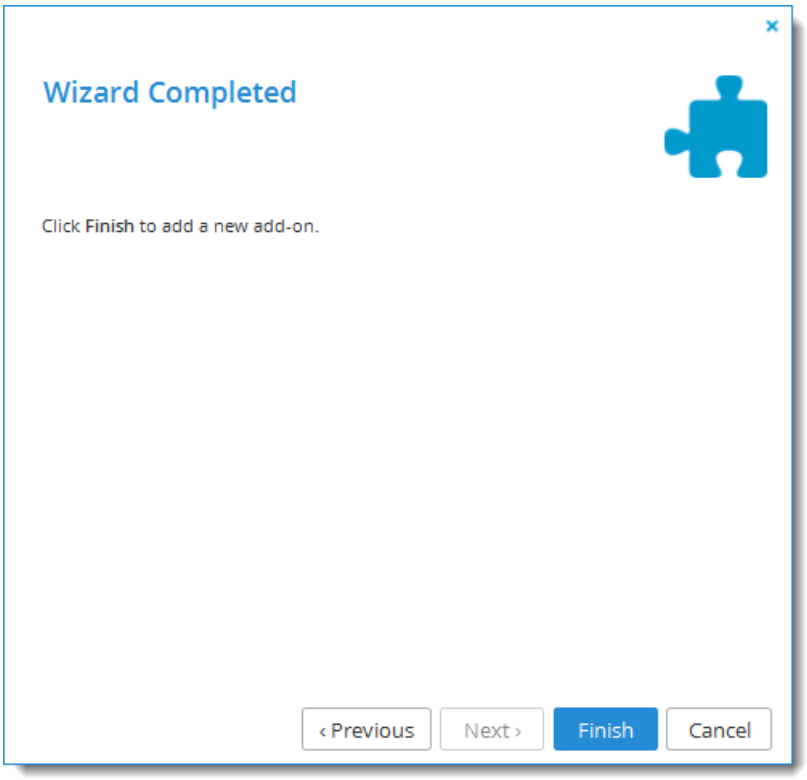


7 For each item, click in the **Amount Included** field, and then type the number of item units to include in the subscription plan.

For example, to include 5GB of storage space, click in the **Storage Quota (GB)** item's **Amount Included** field and type 5.

8 Click **Next**.

The **Wizard Complete** screen appears.



9 Click **Finish**.

If you edited an existing add-on, the following things happen:

- Provisioning changes are applied to all users, and the **Apply Provisioning Changes** window opens displaying **Running** screen with a progress bar that tracks the operation's progress.

  To stop the process, click **Stop**. To close the progress bar, while the process continues in the background, click **Continue in Background**.

- When the operation is complete, the **Completed** screen appears.

10 Click **Close**.

Table 8: Add-on Services Fields

In this field...	Do this...
Cloud Backup Service	Indicates that the Cloud Backup Service is included in the add-on. This field is read-only.
Seeding Supported	Select this option to include backup seeding in the add-on.
Remote Access	Select this option to include remote access in the add-on. Remote access includes both access to the device's management interface via the CTERA Portal and a dedicated URL, access to the user's files via the CTERA Portal and a dedicated URL. **Note**: Device owners can disable remote access via the device's management interface.
Cloud Drive	Select this option to include private cloud drives in the add-on. In a team portal, users will be able to access the private cloud drive in addition to the team cloud drive. Users will be able to access their cloud drives via the End User Portal's **Files** tab, for the purpose of viewing, uploading, and downloading files.
Antivirus Service	Select this option to include the Cloud Drive Antivirus service in the add-on. When antivirus is activated, files are scanned for malware automatically and transparently, before they are downloaded for the first time. The Cloud Drive antivirus service requires an additional license.

Table 9: Add-on Details Fields

In this field...	Do this...
Name	Type a name for the add-on.
Display Name	Type the name to use when displaying this add-on in the End User Portal and notifications.
Expires after	Select this option to define an expiration date for the add-on, then type the number of days after the add-on has been added to the user account that the add-on should expire.

Exporting Add-ons to Excel

You can export add-ons to a CSV file that can be opened with Microsoft Excel.

To export add-ons

1. In the navigation pane, click **Provisioning > Add-ons**.

   The **Provisioning > Add-ons** page appears, displaying all add-ons.

2. Click **Export to Excel**.

   All add-ons are exported to a CSV file.

Applying Provisioning Changes

CTERA Portal applies changed plan and add-on settings to all users every day at midnight. If desired, you can use the following procedure to apply all changes immediately.

To apply provisioning changes

1. In the navigation pane, click **Provisioning > Add-ons**.

   The **Provisioning > Add-ons** page appears, displaying all add-ons.

2. Click **Apply Provisioning Changes**.

   The following things happen:

   - Provisioning changes are applied to all users, and the **Apply Provisioning Changes** window opens displaying **Running** screen with a progress bar that tracks the operation's progress.

     To stop the process, click **Stop**. To close the progress bar, while the process continues in the background, click **Continue in Background**.

   - When the operation is complete, the **Completed** screen appears.

3. Click **Close**.

Deleting Add-ons

To delete an add-on

1. In the **Provisioning > Add-ons** page, select the add-on's row.
2. Click **Delete.**
3. Click **Yes** to confirm.

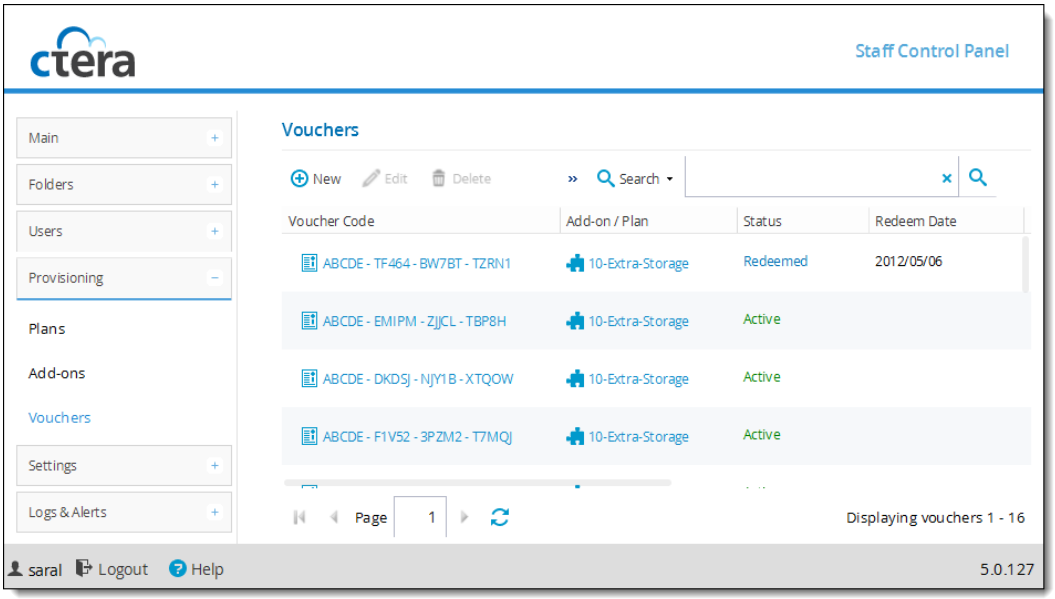
   The add-on is deleted.

Adding Vouchers

To add a voucher

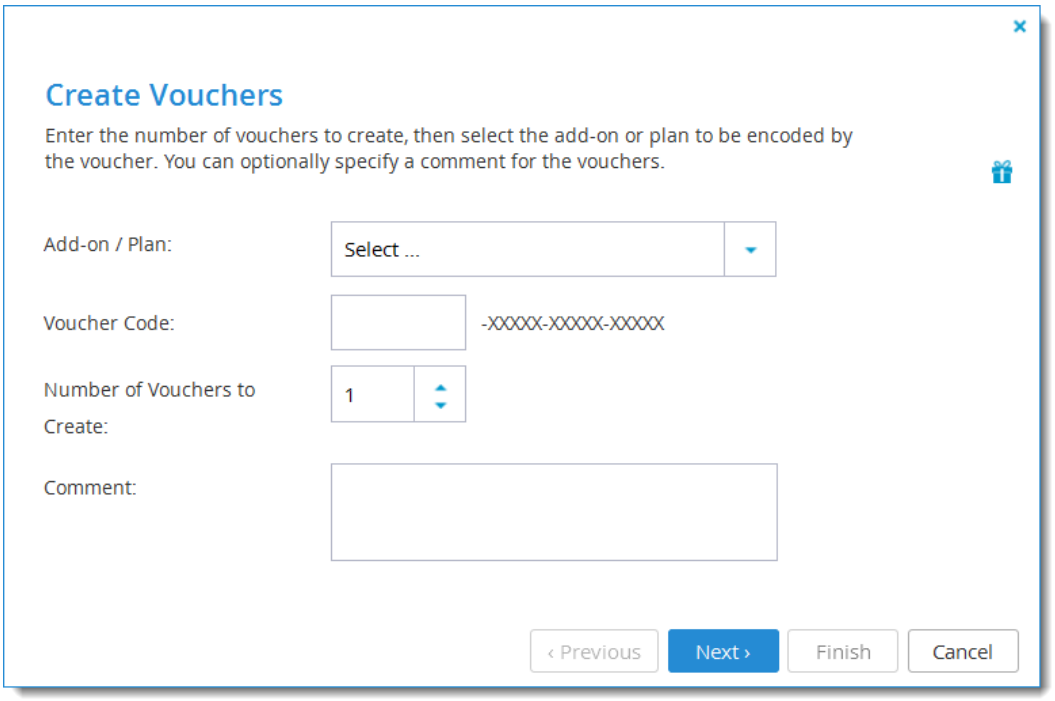
1 In the navigation pane, click **Provisioning > Vouchers**.

The **Provisioning > Vouchers** page appears, displaying all vouchers.



2 Click **New**.

The **Create Vouchers** opens displaying the **Create Vouchers** dialog box.



3 Complete the fields using the information in the following table.

4 Click **Next**.

The **Wizard Complete** screen appears.

5 Click **Finish**.

Table 10: Voucher Wizard Fields

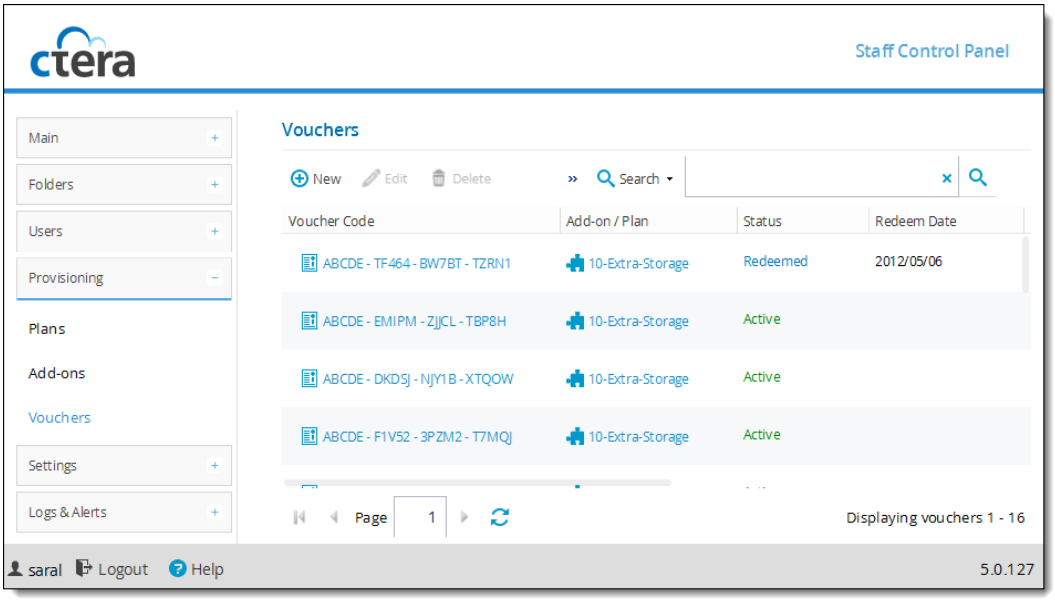
In this field...	Do this...
Add-on / Plan	Select the add-on or subscription plan to which this voucher applies.
Voucher Code	Type the voucher code prefix to use for all vouchers of this type. This can be any sequence of five alphanumeric characters. For example: PKG1Y.
Number of Vouchers to Create	Click the arrows or type in the field, to specify the number of vouchers of this type to create. For example: 10.
Comment	Type a description of this voucher. For example: “This voucher can be redeemed for 1 year of 10GB online backup service”.

Viewing Vouchers

To view all vouchers in the portal

1. In the navigation pane, click **Provisioning > Vouchers**.

   The **Provisioning > Vouchers** page appears, displaying all vouchers.



   The table includes the following columns.

Table 11: Vouchers Fields

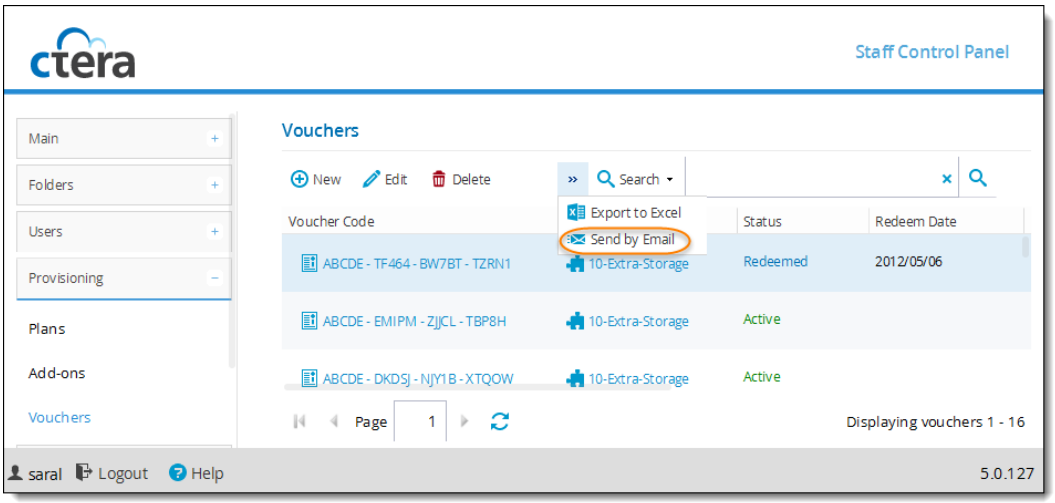
This field...	Displays...
Voucher Code	The voucher's code.
Add-on / Plan	The add-on or subscription plan to which this voucher applies.
Status	The voucher's status. **Active**. The voucher has not yet been redeemed. **Redeemed**. The voucher has been redeemed by a user, and is no longer available to be redeemed by other users.
Redeem Date	The date on which the voucher was redeemed.
Redeemed By	The name of the user account that redeemed the voucher.
Issue Date	The date on which the voucher was created.
Comment	A description of the voucher.

Sending Vouchers by Email

You can send an email message to end users, notifying them that a voucher has been issued to them.

To send a voucher by email

1. In the **Provisioning > Vouchers** page, select the voucher's row.
2. Click **Send by Email**.



An email message opens in your email client. The message's content can be edited as desired.

For information on customizing the message's default content, see ***Customizing Email Notification Templates*** (on page 221).

3. In the **To** field, type the end user's email address.
4. Click **Send**.

Exporting Vouchers to Excel

You can export vouchers to a CSV file that can be opened in Microsoft Excel.

To export vouchers

- In the **Provisioning > Vouchers** page, click **Export to Excel**.

All vouchers are exported to a CSV file.

Deleting Vouchers

To delete a voucher

1. In the **Provisioning > Vouchers** page, select the voucher's row.
2. Click **Delete.**
3. Click **Yes** to confirm.

   The voucher is deleted.

12

Configuring Virtual Portal Settings

In This Chapter

Overview

Virtual portal settings include:

- Password policy
- Customer Support contact details
- How long registration invitations to users are valid for
- Whether the folders of users who have no quota should be automatically deleted after a period of time

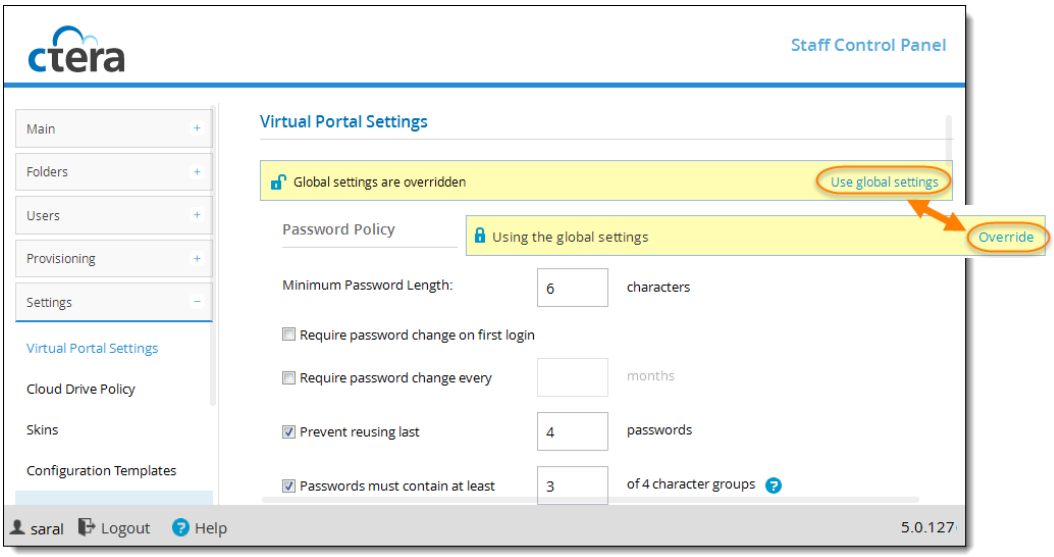
By default, the portal inherits its settings from global virtual portal settings, which are set for multiple virtual portals by a global portal administrator. If desired, you can override the global settings for the portal and modify the settings as needed.

Changing the Settings

To change virtual portal settings

1. Select **Settings > Virtual Portal Settings** from the menu**.**
2. Override the global settings, by clicking **Override**.

   To revert to global settings, click **Use global settings**.



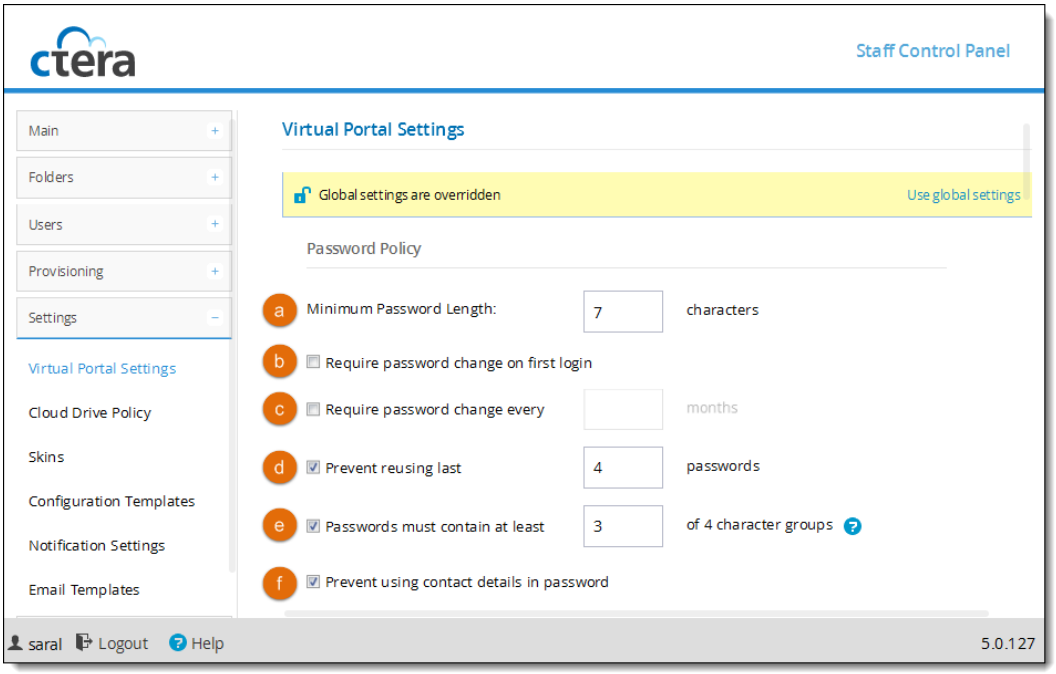
3. Change settings as required in the **Settings > Virtual Portal Settings** page.
4. Scroll down to the end of the page and click **Save** to save your changes.

Password Policy

CTERA Portal features a password strength policy to comply with security standards. You can:

- Configure a password rotation cycle (in months)
- Prevent the re-use of the last X passwords
- Determine the number of character groups required in a user's password. The available character group values are:
  - Lowercase characters
  - Uppercase characters
  - Numerical characters
  - Special characters such as "!@#$"

- Prevent users from using their personal details in their password, including first name, last name, email, username, and company name.



a **Minimum Password Length**. Type the minimum number of characters that must be used in a CTERA Portal account password. The default value is 7 characters.

b **Require password change on first login**. Select this option to require users to change their password on their first login.

c **Require password change every**. Select this option to require users to change their password after a certain number of months, then specify the desired number of months in the field provided. When the specified number of months has elapsed, the user's password will expire, and they will be required to configure a new password upon their next login.

d **Prevent reusing last... passwords**. Select this option to prevent users from reusing a specified number of their previous passwords when they change their password. Specify the number of previous passwords you want this to apply to.

e **Passwords must contain at least.... of 4 character groups**. Select this option to require users to choose passwords that contain at least a specified number of the following character groups:

f Lowercase characters

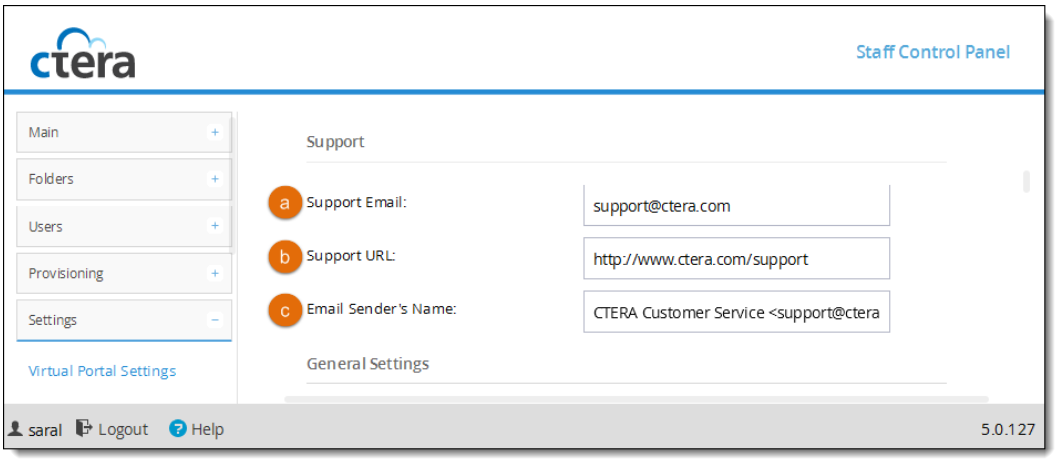
g Uppercase characters

h Numerical characters

i Special characters such as “!@#$”

j **Prevent using contact details in password**. Select this option to prevent users from using their personal details in their password, including first name, last name, email, username, and company name.

Support Settings

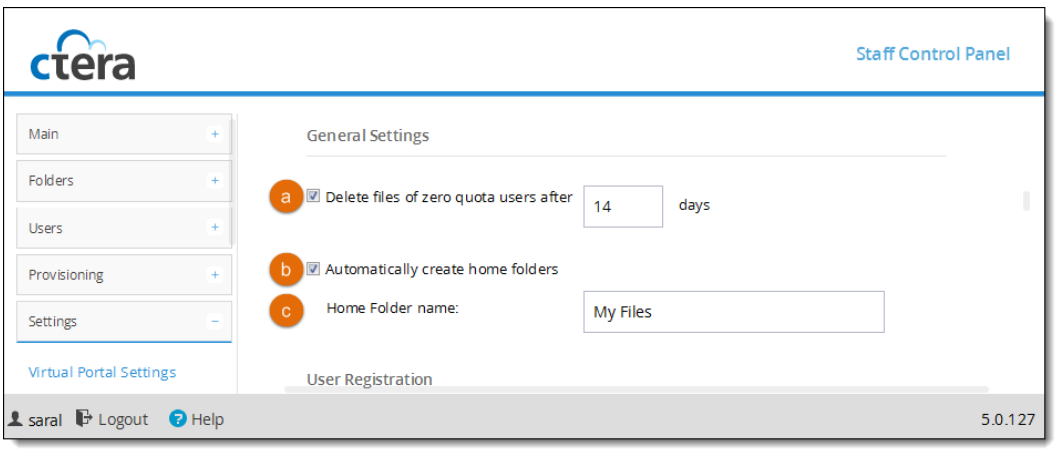


a **Support Email**. Type the email address to which support requests should be sent. This email address will appear in the From field of all email notifications sent by the CTERA Portal system.

b **Support URL**. Type the URL to which CTERA Portal users should browse for customer support. This URL will appear at the bottom screen in the End User Portal interface, as well as in all email notification templates.

c **Email Sender's Name**. Type the email address that should appear in the From field of notifications sent to end users and staff by the virtual portals. For example: "CTERA Customer Service <support@ctera.com>"

General Settings

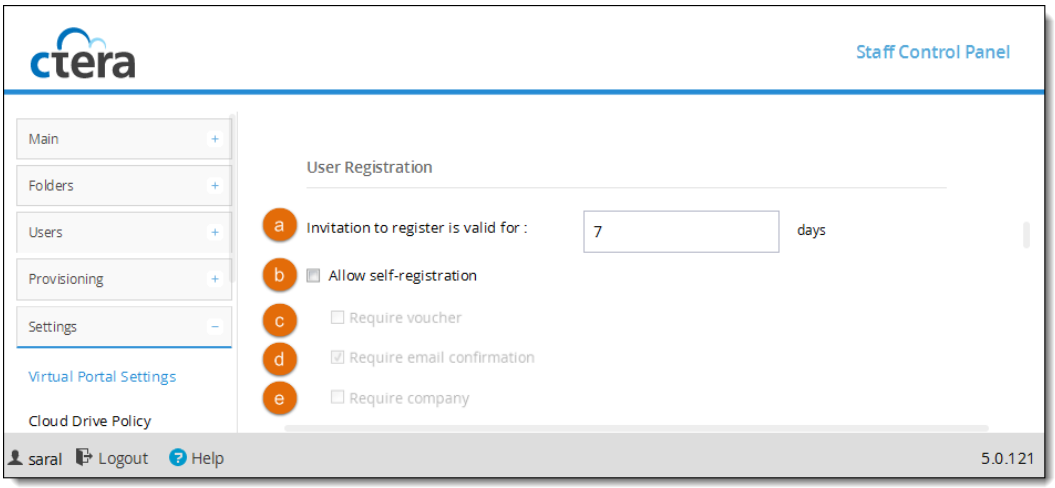


a **Delete files of zero quota users after**. Select this option to specify that the storage folders of customers who have no quota (for example, customers with expired trial accounts) should be deleted automatically after a certain number of days, then specify the desired number of days in the field provided. Enabling this option helps free storage space. A notification is sent to the customer prior to deletion, prompting the customer to purchase cloud storage in order to avoid the scheduled deletion of their files. Storage folders of over-quota users with a non-zero quota will not be deleted. The default value is 14 days.

b **Automatically create home folders**. Select this option to specify that one personal folder is automatically created for each new user account. This folder is given the home folder name entered in the Home Folder name field.

c **Home Folder name**. The name of the personal folder created for each new user account. Relevant only if Automatically create home folders is enabled.

User Registration Settings



a **Invitation to register is valid for:... days**. Enter the validity period, in days, for registration invitations sent to users by team portal administrators. If a user has not registered for the service after the number of days specified in this field, the invitation will expire.

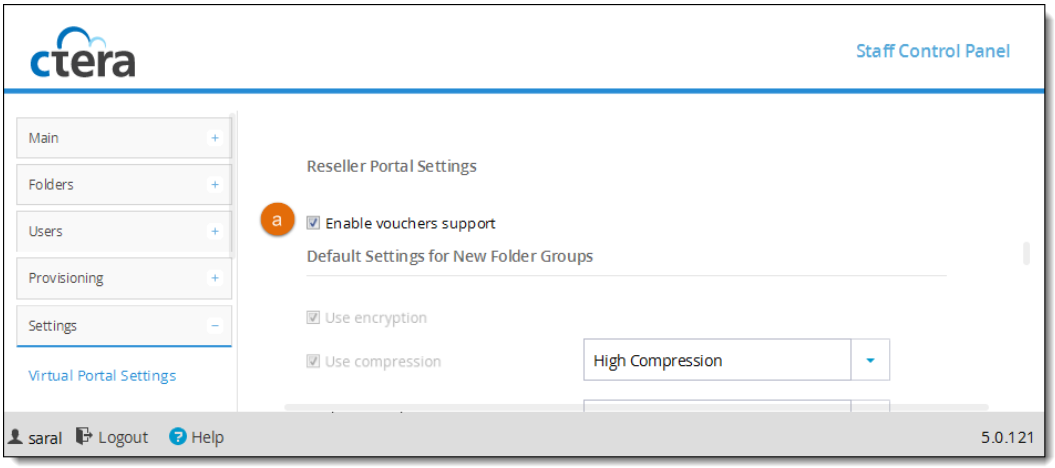
b **Allow self-registration**. Select this option to allow end users to sign up for a CTERA Portal account, by surfing to the CTERA Portal and filling in a form. If this check box is cleared, the registration form will not appear in the CTERA Portal, and users will be defined only by an administrator. If selected, the **Require voucher**, **Require email confirmation**, and **Require company** fields are enabled.

c **Require voucher**. Select this option to require end users to supply a valid voucher code when registering a new CTERA Portal account.

d **Require email confirmation**. Select this option to require end users to confirm their registration by email, in order for their CTERA Portal account to be activated. This is recommended, since it ensures that the user has entered a valid email address.

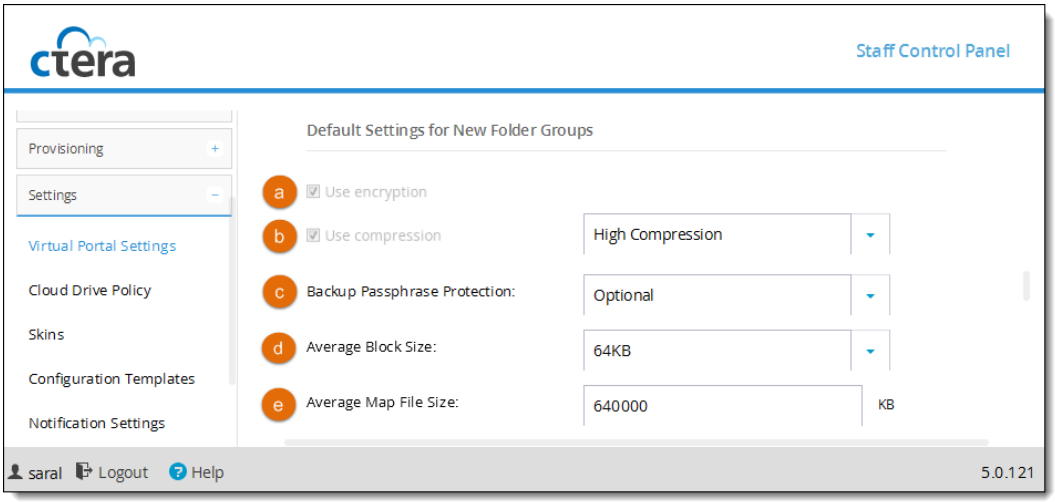
e **Require company**. Select this option to require end users to specify their company, when registering a new CTERA Portal account.

Reseller Portal Settings



a **Enable vouchers support**. Select this option to enable the use of vouchers in the CTERA Portal. If this option is cleared, the **Provisioning > Vouchers** menu item will not appear in the portal's menu.

Default Settings for New Folder Groups



a **Use encryption**. Select this option to specify that the Encryption check box should be selected by default in all new folder groups' settings; that is, data in newly created folder groups will be stored in encrypted format by default.

If encryption is not needed, and you want to improve performance, you can disable this option.

Note: This value applies to new folder groups only and cannot be changed for existing folder groups.

Note: Passphrase protection is only available in encrypted folders.

b **Use compression**. Select this option to specify that data in newly created folder groups will be stored in encrypted format by default. The Compression check box will be selected by default in all new folder groups' settings.

Clearing this option results in higher performance; moreover, additional storage space will be used.

Specify the default compression method used by new folder groups by selecting one of the following from the dropdown list:

- High Compression
- High Speed (default)

Note: This value applies to new folder groups only and cannot be changed for existing folder groups.

c **Backup Passphrase Protection**. The policy regarding whether using passphrase protection for backups is optional for users.

- **Optional** (default). Users may choose whether to protect backups with a passphrase.
- **Required**. Users must use a passphrase to protect backups.
- **Disabled**. Users cannot protect backups with a passphrase.

Tip

Data protected with a user-defined passphrase cannot be retrieved if the passphrase is lost.

d **Average Block Size**. Select the average block size used by new folder groups.

The CTERA de-duplication engine splits each stored file into blocks. Increasing the Average Block Size causes the files to be split into larger chunks before storage, and results in increased read/write throughput at the cost of a reduced de-duplication ratio. Increased block size is useful for workloads that require high performance, as well as for those that do not gain greatly from de-duplication (for example, where the stored files consist mostly of videos, images, and music files that are not frequently modified).

Decreasing the average block size results in better de-duplication, since the portal can better identify finer-grained duplicate data.

Note: Changing this value does not affect existing folder groups. The new value applies to new folder groups only.

The default value is 512KB.

e **Average Map File Size**. Type the average map file size used by new folder groups.

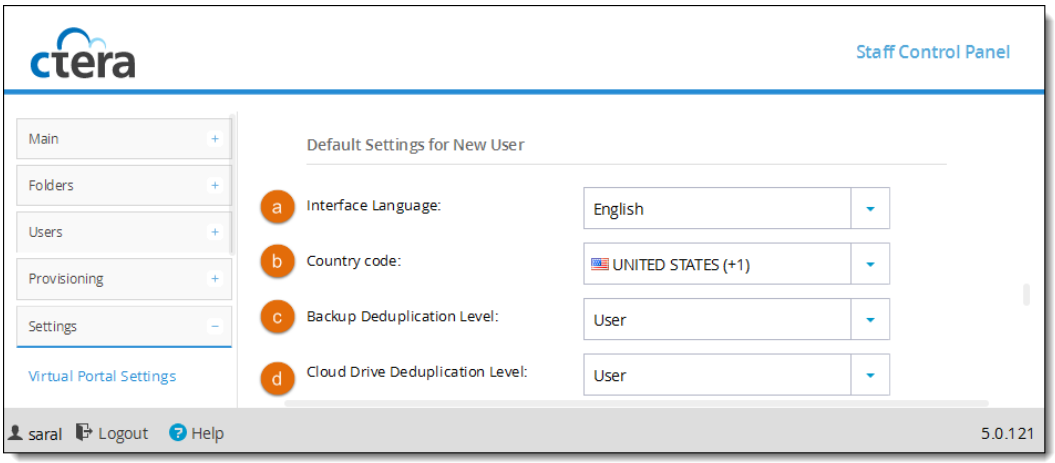
CTERA Portal uses file maps to keep track of the blocks each file is made of. The Average Map File Size represents the maximum size of file that will be represented using a single file map object. For example, if the average map file size is set to 100MB, files of up to approximately 100 MB will have one file map, files of up to approximately 200MB will have two file maps, and so on.

Reducing the average map file size causes more file maps to be created per file. This may result in smoother and less bursty streaming of files; however, it will also result in some extra overhead for creating, indexing, and fetching the additional file maps.

Note: This value applies to new folder groups only and cannot be changed for existing folder groups.

The default value is 640,000 KB.

Default Settings for New User



a **Interface Language**. Select the default language for new users. This language can be overridden by end users in the End User Portal.

The following languages are supported: English, French, German, Hebrew, Italian, Polish, Spanish, and Portuguese.

b **Country Code**. The user's country code for text messages. This is relevant for two factor authentication when content is shared with the user and a passphrase is sent to the user via text message.

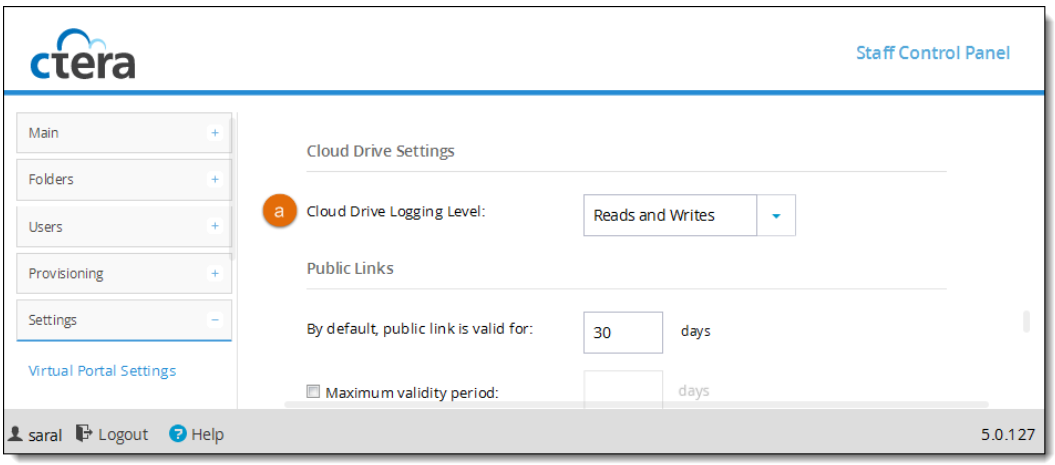
c **Backup Deduplication Level**. Specify the default de-duplication level to use for backup folders, for all new users. Select one of the following:

- **User** (default). Create a single folder group for each user account, containing all of the user account's backup folders. De-duplication is performed for the user account's folder group.
- **Folder**. Create a folder group for each of a user account's devices, containing all of the device's backup folders. De-duplication is performed separately for each of the user account's folder groups.

d **Cloud Drive Deduplication Level**. Specify the default de-duplication level to use for cloud folders, for all new users. Select one of the following:

- **User** (default). Create a single folder group for each user account, containing all of the user account's cloud folders. De-duplication is performed for the user account's folder group.
- **Folder**. Create a folder group for each of a user account's devices, containing all of the device's cloud folders. De-duplication is performed separately for each of the user account's folder groups.

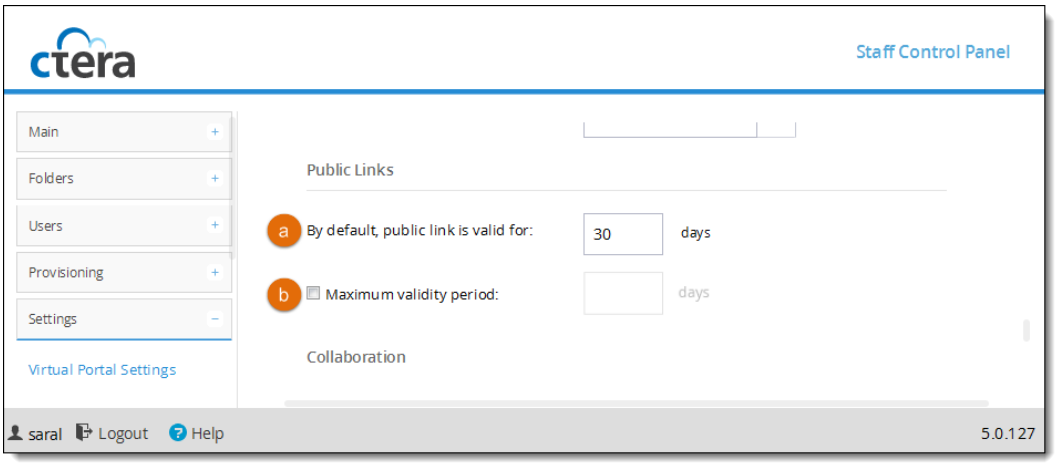
Cloud Drive Settings



a **Cloud Drive Logging Level**. Set the logging level for the Cloud Drive to one of the following:

- **None**
- **Writes Only**
- **Reads and Writes**

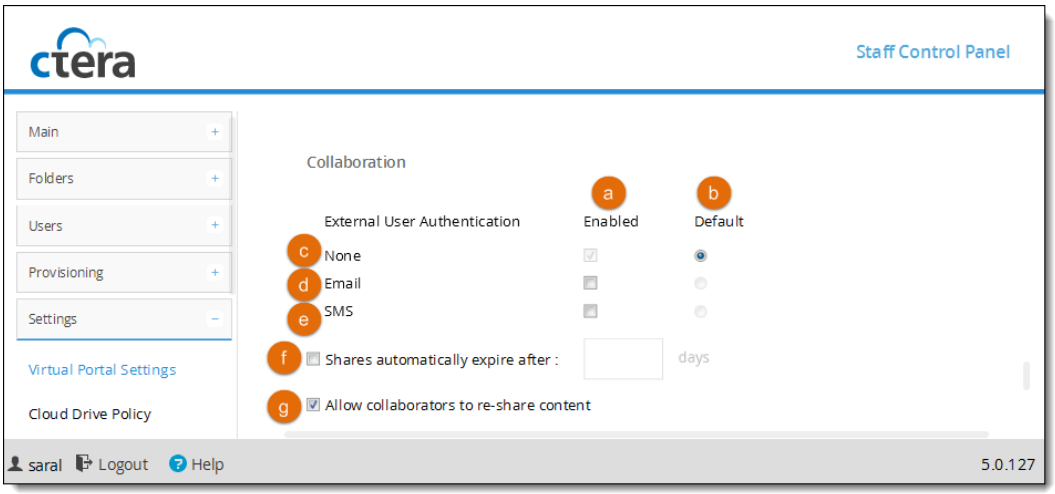
Public Links



a **By default, public link is valid for**. The default number of days for which public link to a folder is valid.

b **Maximum validity period**. The maximum validity period a user can choose for a public link when sharing a folder by public link.

Collaboration



a **Enabled**. This method of external user authentication is available for end users to choose when they send invitations to external users to collaborate on files.

b **Default**. This method of external user authentication is the default method used to authenticate external users who are invited by end users to collaborate on files.

c **None**. No user authentication is applied.

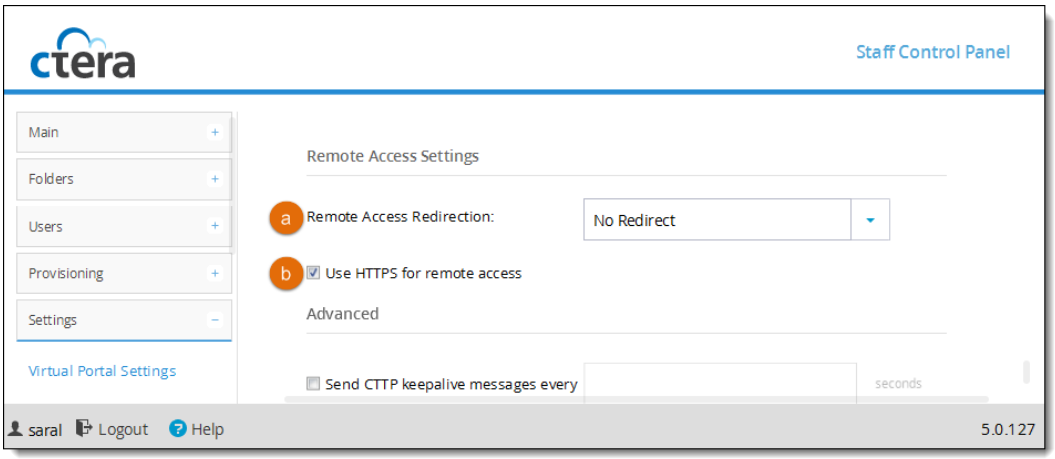
d **Email**. The invitation recipient receives a time limited authenticated link to the file or folder. On every access, a new 6 digit passcode challenge is sent to the recipient by email. The recipient must enter the passcode before accessing the file or folder. This ensures that the invitation is not usable in case the invitation link is accidentally forwarded to another person, or posted on a public website.

e **SMS**. The invitation recipient receives a time limited authenticated link to the file or folder. On every access, a new 6 digit passcode challenge is sent to the recipient by text message. The recipient must enter the passcode before accessing the file or folder. This ensures that the invitation is not usable in case the invitation link is accidentally forwarded to another person, or posted on a public website.

f **Shares automatically expire after**. The time period after which invitations to share files with external users expire.

g **Allow collaborators to re-share content**. If checked, end users are allowed to allow collaborators to re-share content with other users.

Remote Access Settings



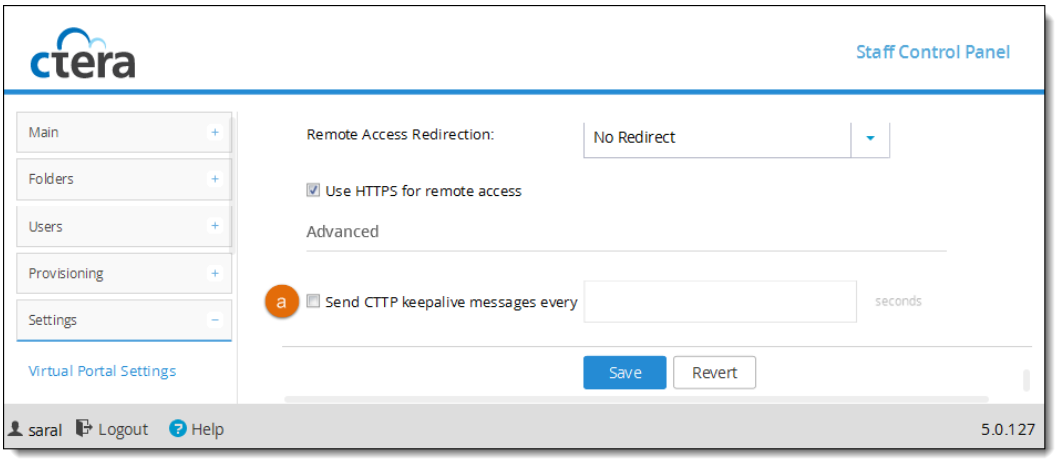
a **Remote Access Redirection**. Specify whether Web clients attempting to remotely access a device should be redirected to communicate directly with the device, instead of relaying communications through the CTERA Portal. Select one of the following:

- Public IP Redirect. Redirect Web clients to the device's public IP address.
- Private IP Redirect (default). Redirect Web clients to the device's private IP address.
- No Redirect. Do not redirect communications between Web clients and the device. Relay all communications through the CTERA Portal.

b **Use HTTPS for remote access**. Select this option to use HTTPS for remotely accessing devices, using the remote access service.

For example, if a device is named "dev1" and the portal is names "portal.mycompany.com", then enabling this option will cause the client's browser to be automatically redirected from the HTTP URL http://dev1.portal.mycompany.com to the HTTPS-secured URL https://portal.mycompany.com/devices/dev1.

Advanced Settings



a **Send CTTP keepalive messages every**. Select this option to prevent proxy or load balancer servers from preemptively terminating connection between a CTERA Agent and the CTERA Portal. This may be relevant if the CTERA Agent is configured to use a proxy server and there are connectivity problems during Cloud Backup or Cloud Sync. This is because some proxy servers and load balancers are configured to close open connections that are not transferring any data after a certain amount of time, thereby causing connectivity problems.

In the field provided, specify an interval, in seconds, smaller than the timeout value configured on the proxy or load balancer server.

13

Cloud Drive Policy

Cloud Drive policy determines the type of data that can be synchronized through the CTERA Cloud Agent, Cloud Gateways and CTERA Mobile app, or uploaded to CTERA Portal via the Web interface.

To set Cloud Drive policy, you create DENY and ALLOW rules based on the following attributes:

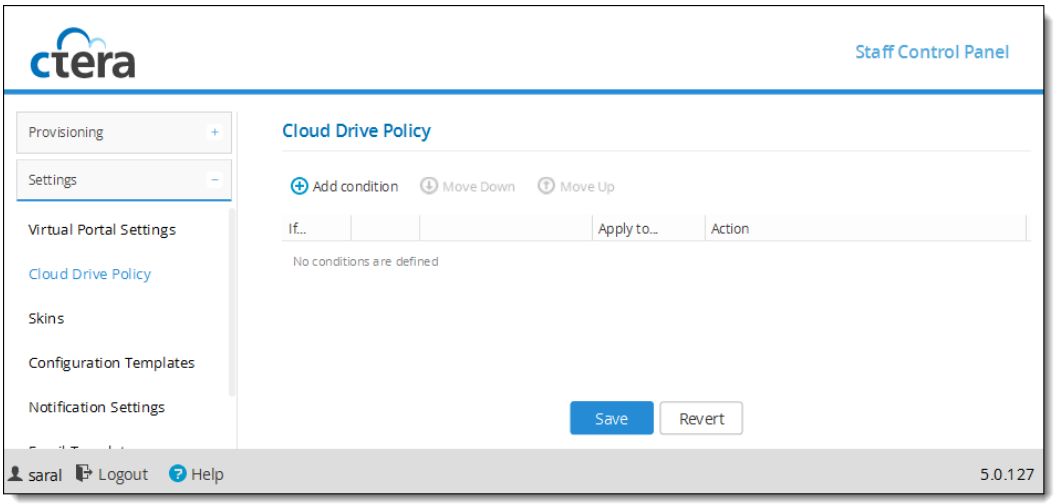
- File Size
- File Name
- File Type

Each rule can be applied to everyone or to a specific user or group, whether they are users and groups from an integrated directory service or local users and groups defined in the portal.

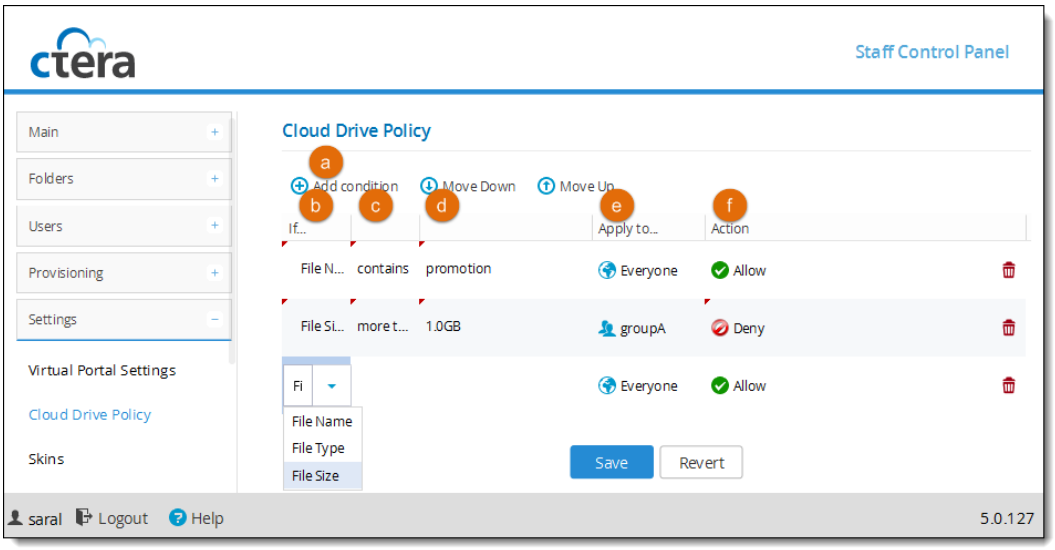
In addition, it is possible to apply Cloud Drive policy rules to external users (that is, users who were invited to collaborate by email address or by means of a public link), by using a special group called "External Users".

To configure Cloud Drive policy

1. Browse to the **Settings > Cloud Drive Policy** page.



2 Add conditions to the policy:



a Click **Add condition**.

b Select a file attribute.

c Select an operator, such as "is one of".

d Select a value for the operator.

e If necessary, change who it applies to.

f Select Deny or Allow to deny or allow the specified file attribute.

3 To delete any conditions that you added, click in the row for the condition.

4 When you're done adding conditions, click **Save**.

14

Overriding Global Branding Settings

In This Chapter

Overview

By default, the portal inherits its branding settings from the global settings. If desired, you can override the global branding settings for the portal, and brand your CTERA Portal by applying the following:

- A skin with your company logo and color scheme
- A custom **Login** page

Creating Skins

To create a skin

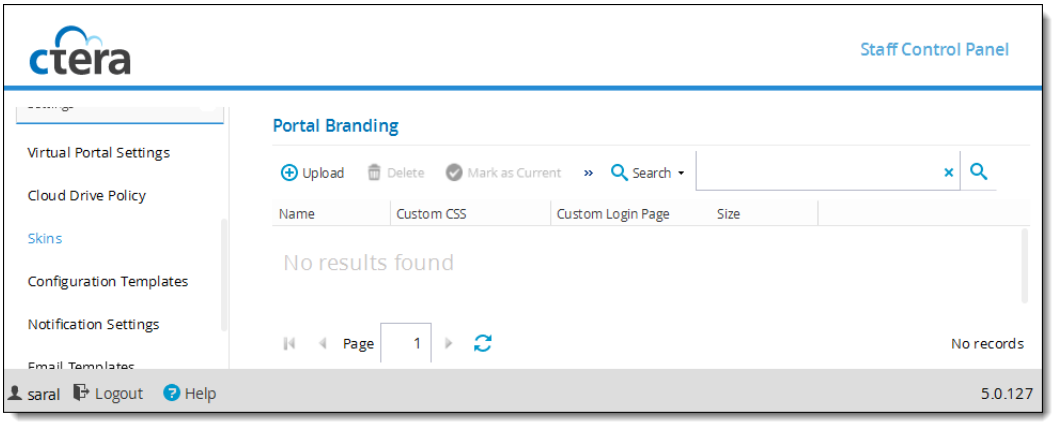
1. Request a basic skin from CTERA support.
2. Extract the ZIP file that you received.
3. Edit the HTML and CSS files as desired.
4. Replace the graphic files as desired.
5. Put the changed files back in the ZIP file.
6. Change the ZIP file's extension to ".skin".

Uploading Skins

To upload a skin

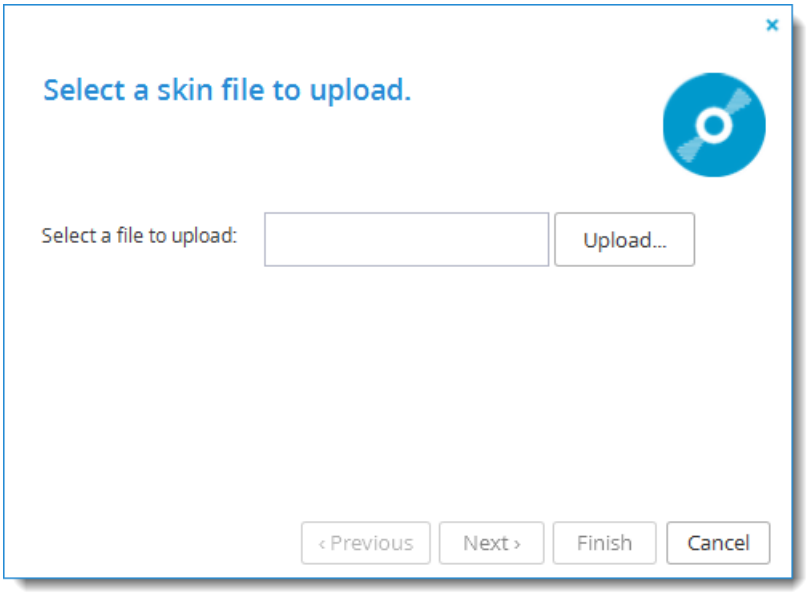
1. Browse to **Settings > Skins**.

   The **Settings > Skins** page appears.



2. Click **Upload**.

   The **Skin Upload Wizard** appears displaying the **Select a file to upload** dialog box.



3. Click **Upload** and browse to the desired *.skin file.

   The skin is uploaded.

   At the end of the process, the **Completing the Skin Upload Wizard** screen appears.

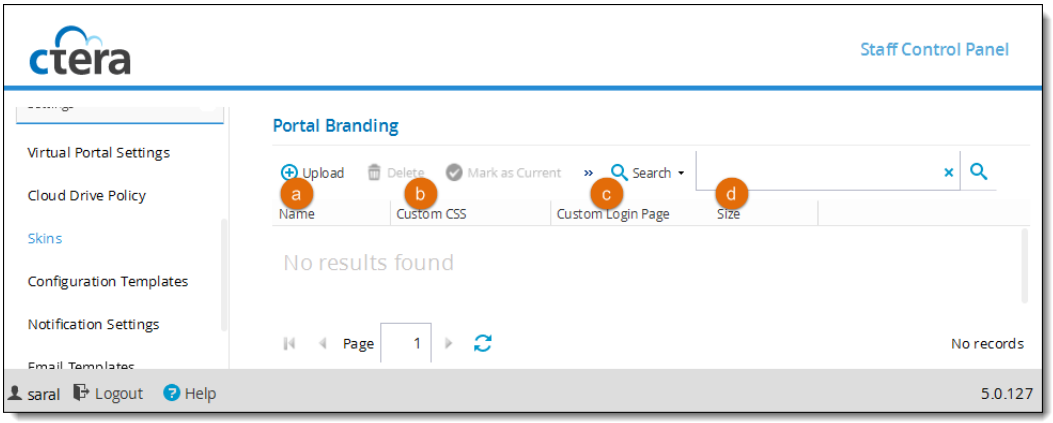
4. Click **Finish**.

Viewing Skins

To view all skins in the portal

1 Browse to **Settings > Skins**.

The **Settings > Skins** page appears displaying all skins.



a **Name**. The skin's name.

b **Custom CSS**. Indicates whether the skin includes a custom CSS (Yes/No).

c **Custom Login Page**. Indicates whether the skin includes a custom Login page (Yes/No).

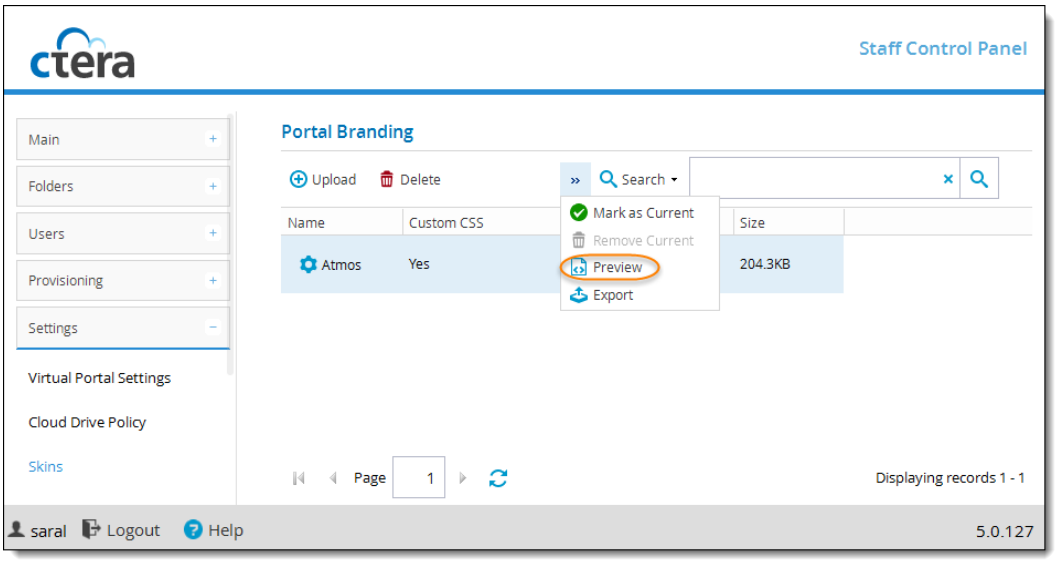
d **Size**. The *.skin file's size.

Previewing Skins

To preview a specific skin

1 In the **Settings > Skins** page, select the skin's row.

2 Click **Preview**.



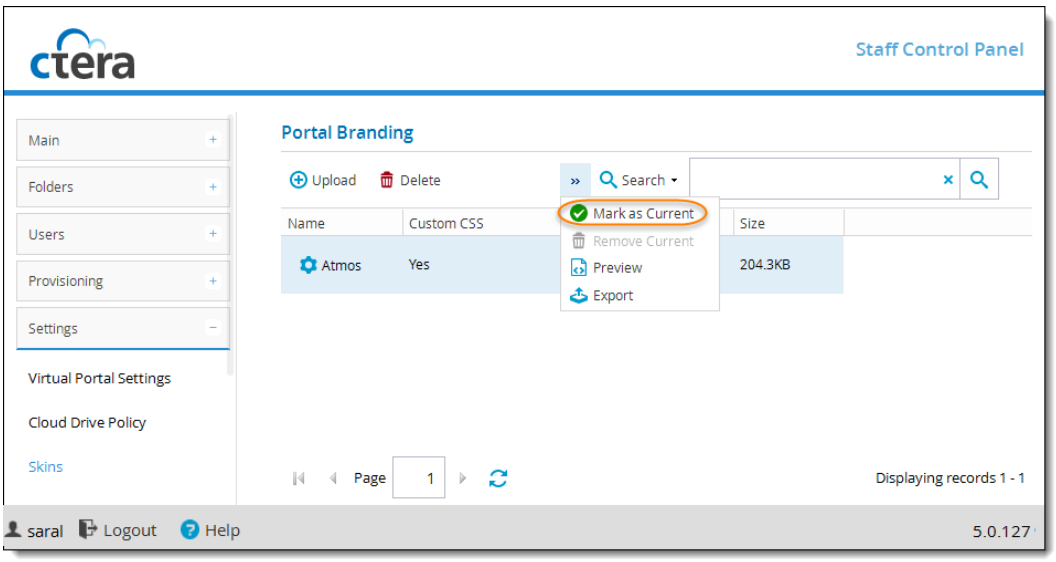
A preview opens in a new window.

Applying Skins

To apply a skin to the CTERA Portal

1 In the **Settings > Skins** page, select the skin's row.

2 Click **Mark as Current.**



The selected skin is applied to the CTERA Portal and marked with the icon.

Applying the Default Skin

When you remove the currently applied skin, the default CTERA Portal skin is used.

Tip

The removed skin is *not* deleted from the system.

To remove the currently applied skin

1. In the **Settings > Skins** page, click **Remove Current.**

   The default CTERA Portal skin is applied.

Deleting Skins

To delete a skin

1. In the **Settings > Skins** page , select the skin's row and click **Delete.**
2. Click **Yes** to confirm.

   The skin is deleted.

15

Managing Device Configuration Templates

In This Chapter

Overview

CTERA Portal enables you to centrally manage device settings, by assign devices to *device configuration templates*: When a device is assigned to a template, it inherits the following settings from that template:

- Backup sets and exclude sets
- Backup applications (relevant for CTERA Server Agents only)
- Backup schedule
- Backup throughput control
- Installed software and firmware versions
- Automatic firmware updates

Tip

Settings inherited from a template can be overridden from the device's Web interface.

Devices can be assigned to templates in the following ways:

- Manually, by editing the device settings.

  See ***Editing Device Settings*** (on page 24).

- Automatic template assignment.

  Devices can be assigned to templates based on the *automatic template assignment policy*, which specifies a set of criteria for assigning a template (such as device type, installed operating system, and so on), as well as an optional default template that is assigned when none of the criteria are met.

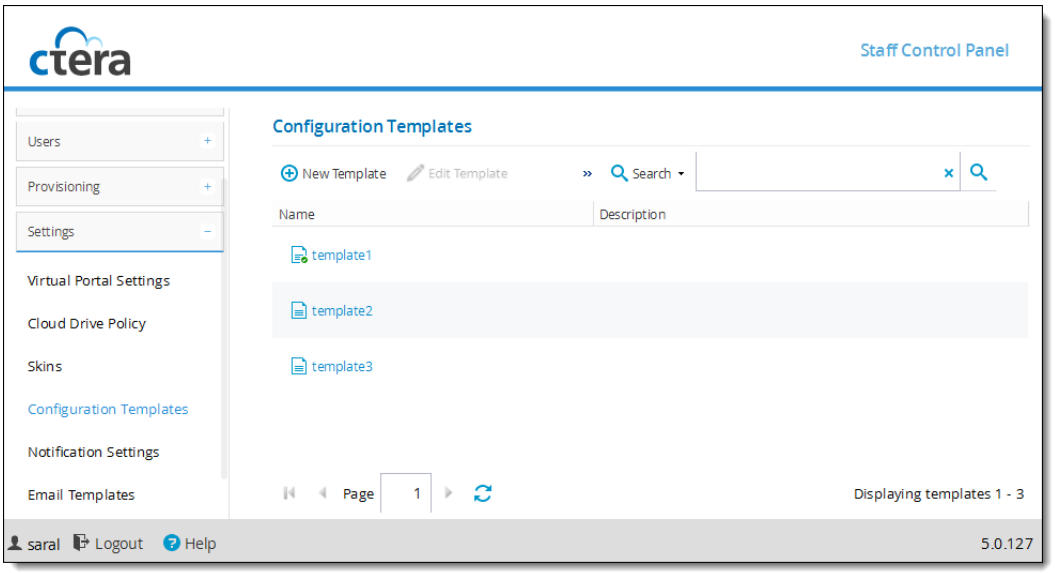
  See ***Configuring the Automatic Template Assignment Policy*** (on page 212).

Viewing Device Configuration Templates

To view all device configuration templates in the portal

- Browse to **Settings > Configuration Templates**.

  The page displays all templates, including each template's name and description.

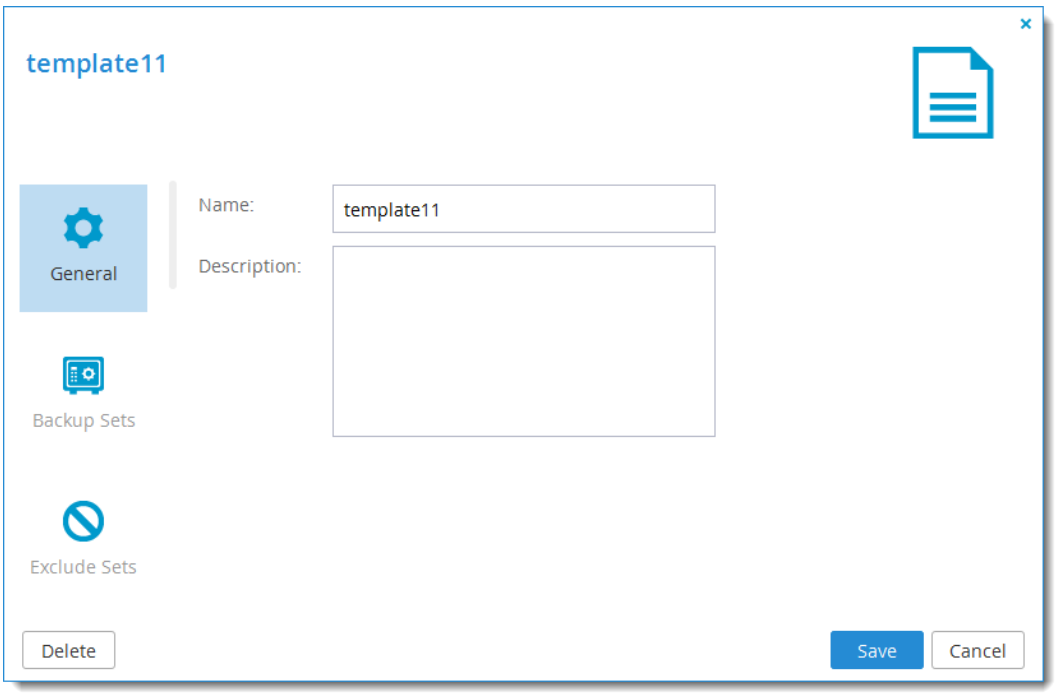


Adding and Editing Device Configuration Templates

To add or edit a device configuration template

1. Select **Settings > Configuration Templates** from the menu.
2. Click **New Template** to create a new template, or select a template's row and click **Edit Template** to edit.

   The Configuration Template Manager opens displaying the **General** tab.



3. In the **Name** field, type a name for the template.
4. In the **Description** field, type a description of the template.
5. Either click **Save** and open the template again any time to add configuration, or select other tabs to add configuration to the template and then click **Save** when you're done.

Backup and Exclude Sets

Backup sets are filters that you can define which select files to include in the backup based on criteria of your choice, such as file type, location, modification date, and so on.

Exclude sets are filters that you can define which select files to exclude from the backup based on criteria of your choice. The CTERA Portal determines the final set of files to include in a backup operation, by performing the following checks for each file:

1. Checks whether the file is contained in an Exclude Set. If so, the file is skipped.
2. Checks whether the file is contained in a Backup Set. If so, the file is backed up.
3. Checks whether the file is contained in a folder that was selected specifically for backup in the device interface. If so, the file is backed up.

When you create backup sets, you can specify files by extension type, name, location, size and/or modification date. For example, you could create a set called "My Music" and include all files with the extensions *.wav and *.mp3 that are located in the folder **My Documents > Music**.

If a file is included in a backup set and the backup set is enabled, it will be included in the backup even if it is not selected as a *Backup File*.

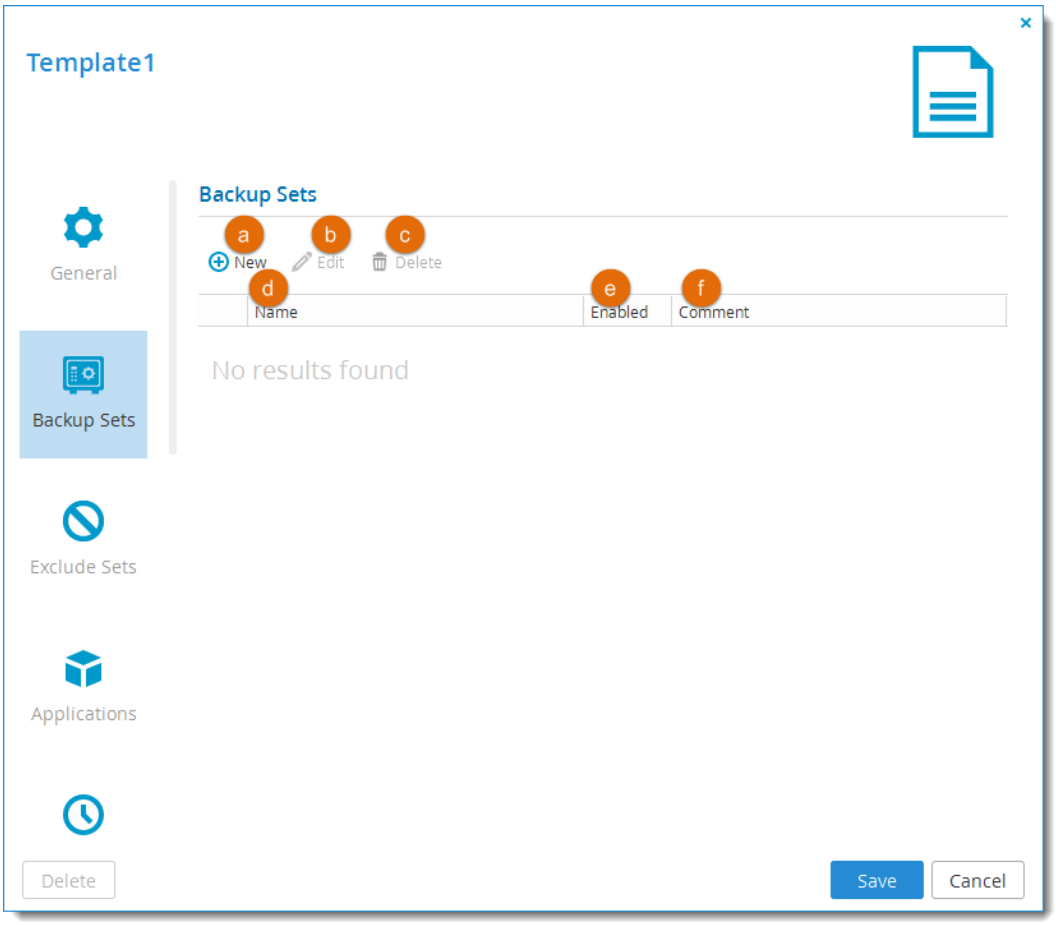
If a file is included in an enabled backup set but also included in an Exclude set, the file will be excluded from the backup.

When you create a backup set, it is automatically enabled. Backup sets can be enabled or disabled.

Creating Backup and Exclude Sets

To add a Backup Set or an Exclude Set

1 Go to the **Backup Sets** or **Exclude Sets** tab and click **New.**



a **New**. Create a new backup or exclude set.

b **Edit**. Edit a backup or exclude set (select the set and then click.)

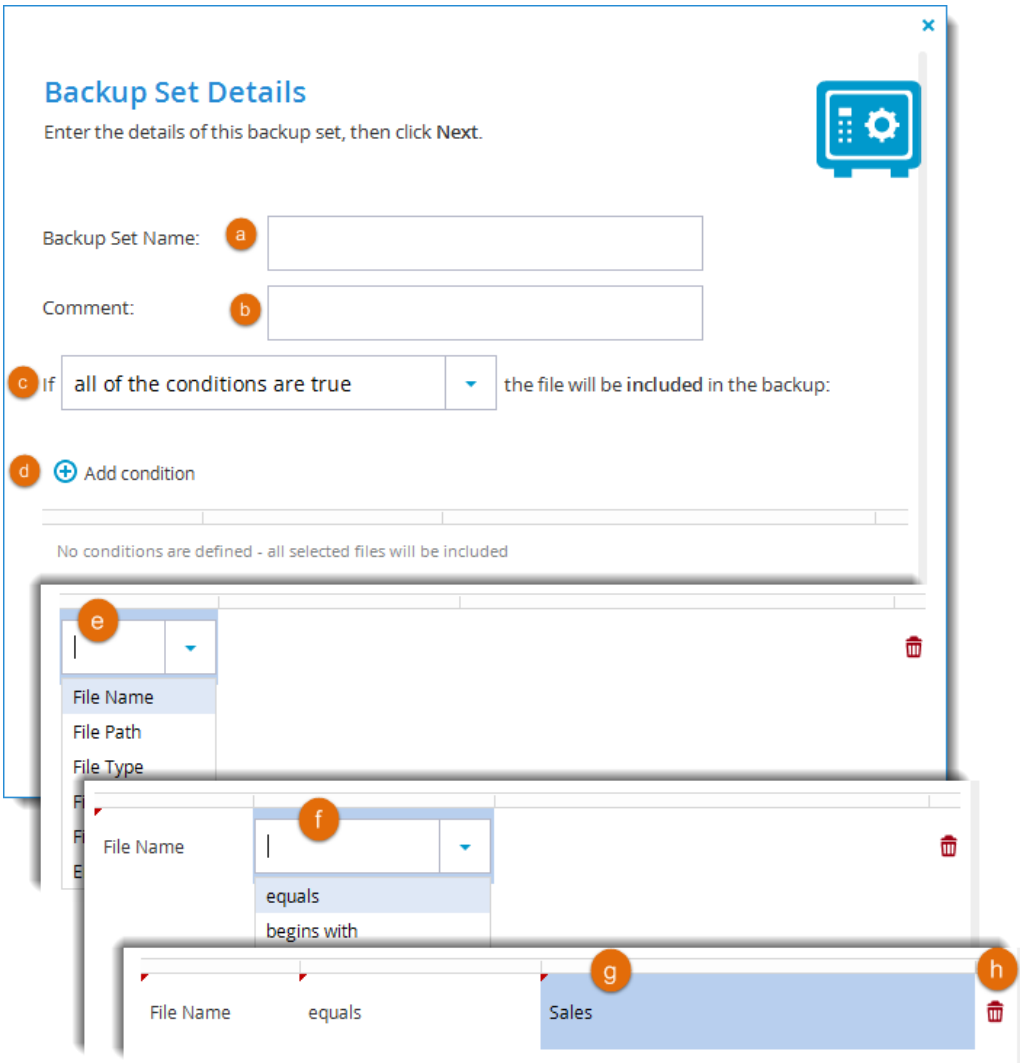
c **Delete**. Delete a backup or exclude set (select the set and then click)

d **Name**. The name of each backup or exclude set.

e **Enabled**. If checked, the backup or exclude set is enabled. Click the checkbox to disable/enable a backup or exclude set.

f **Comment**. A description of the backup or exclude set.

2 Click **New** to create a new backup set and set the details and conditions for the backup or exclude set:



a In the **Backup Set Name** field, enter a name for the backup set.

b In the **Comment** field, type a description of the backup set.

c In the **If** field:

- To specify that all of the conditions (that you are about to define) must be met in order for a file to be included in the backup set, select **all of the conditions are true**.
- To specify that one or more of the conditions must be met in order for a file to be included in the backup set, select **at least one of the conditions is true**.

Define conditions for a file to be included in the backup set, by doing the following for each condition:

d Click **Add condition**.

e Click **Select**, then select the desired condition parameter from the drop-down list.

f In the second column, click **Select**, then select the desired condition operator from the drop-down list. See ***Backup Set Condition Operators*** (page 193) for details.

g Click in the third column, and complete the condition:

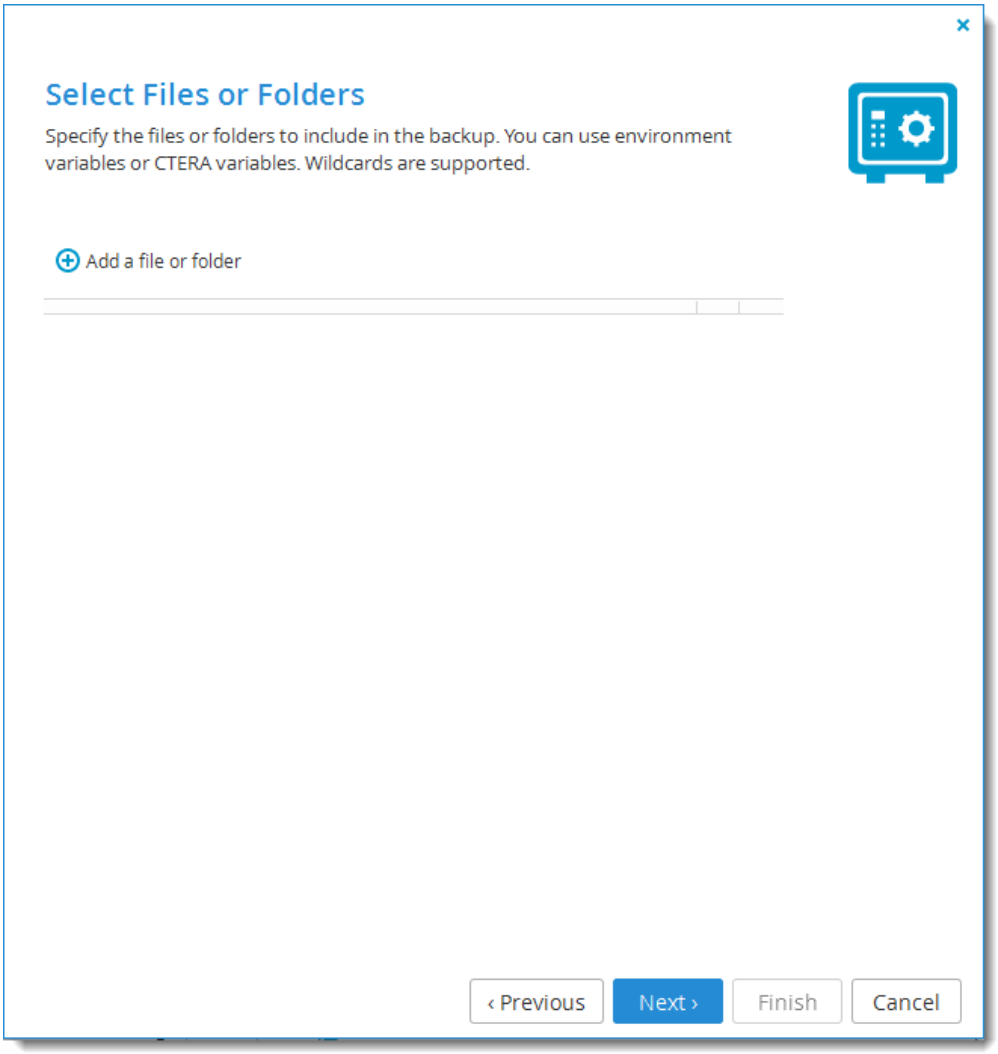
- If the parameter is **File Size**, type the desired file size and unit.
- If the parameter is **File Modified**, click  and choose the desired date.
- For all other parameters, type the desired free-text value.

For example, if you select **File Name** as the condition parameter in the first column, select **begins** with as the condition operator in the second column, and type "Work-123-" in the third column, then the backup set will include all files whose names begin with "Work-123-".

Likewise, if you select **File Type** as the condition parameter in the first column, select **is one of** with as the condition operator in the second column, and type "avi, mov, mpg" in the third column (without the quotation marks), then the backup set will include all files with the extension *.avi, *.mov, and *.mpg.

h If you need to delete a condition, click  in its row.

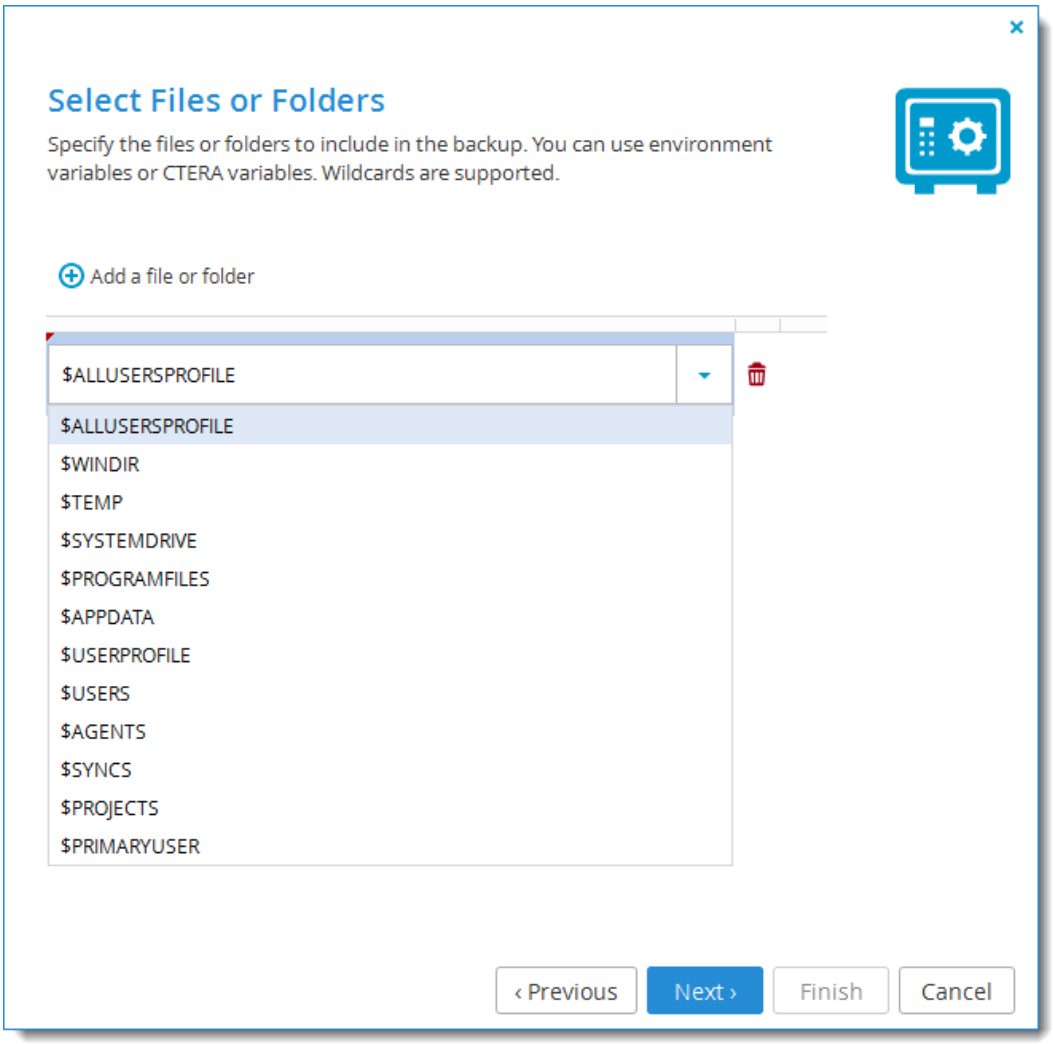
3 Click **Next**, and select which folders to which you want to apply the conditions for the backup or exclude set:



4 Specify the files and folders to which this backup set applies, by doing the following for each file/folder:

a Click **Add a file or folder**.

A row is added to the table.



b Click in the row, and do one of the following:

- Type a variable's name in the field.
- Select a variable from the drop-down list.

You can use any operating system environment variable defined on the Windows or Linux machine, for the user account on which the CTERA service is running. If the specified environment variable is not defined on the machine, this row in the policy is ignored. In addition, a set of CTERA-specific environment variables can be used. For a description of supported variables of all types, see ***Backup Set Environment Variables*** (page 194).

Wildcards are supported. For example, you can type "$USERS/*/MyFolder" to back up the `MyFolder` folder under all users' home directories.

For UNIX/Windows interoperability, backup sets support the use of both slashes and backslashes. Any slashes or backslashes will be automatically converted to the type supported by the machine's OS.

When you specify a folder name, all of the files and subfolders in it are automatically included, and there is therefore no need to add “*” at the end of the folder name.

5 Click **Next** and then **Finish**.

The new backup set is created and automatically enabled.

Table 12: Backup Set Condition Operators

Use this operator...	To do this...
equals	Include all files for which the parameter in the first column matches the string in the third column. This operator is relevant for the **File Name**, **File Path**, and **File Type** parameters only.
begins with	Include all files for which the parameter in the first column begins with the string in the third column. This operator is relevant for the **File Name**, **File Path**, and **File Type** parameters only.
ends with	Include all files for which the parameter in the first column ends with the string in the third column. This operator is relevant for the **File Name**, **File Path**, and **File Type** parameters only.
contains	Include all files for which the parameter in the first column contains the string in the third column. This operator is relevant for the **File Name**, **File Path**, and **File Type** parameters only.
is one of	Include all files for which the parameter in the first column is included in the set specified in the third column. This operator is relevant for the **File Name**, **File Path**, and **File Type** parameters only.
less than	Include all files whose size is less than the amount specified in the third column. This operator is relevant for the **File Size** parameter only.
more than	Include all files whose size is more than the amount specified in the third column. This operator is relevant for the **File Size** parameter only.
before	Include all files whose last modification date is before the date specified in the third column. This operator is relevant for the **File Modified** parameter only.
after	Include all files whose last modification date is after the date specified in the third column. This operator is relevant for the **File Modified** parameter only.

Table 13: Backup Set Environment Variables

Use this variable...	To specify this...
Common OS Variables	Common operating system variables.
$ALLUSERSPROFILE	The Windows "All Users" profile directory.
$WINDIR	The Windows directory.
$TEMP	The Windows temporary files directory.
$SYSTEMDRIVE	The Windows system drive.
$PROGRAMFILES	The Windows Program Files directory.
User-specific Windows Environment Variables	Variables that are executed separately for each user in the system.
$APPDATA	The path to the application data directory. For example: `C:\Documents and Settings\`*username*`\Application Data`, where *username* is the user's username.
$USERPROFILE	The path to the user profile directory. For example: `C:\Documents and Settings\`*username*, where *username* is the user's username.
CTERA Appliance Template Variables	Variables that are defined for CTERA cloud gateways.
$USERS	The home directories folder on the CTERA cloud gateway.
$AGENTS	The CTERA Agents folder on the CTERA cloud gateway.
$SYNCS	The "Clientless Backup" destination folder on the CTERA cloud gateway.
$PROJECTS	The projects folder on the CTERA cloud gateway.
$PRIMARYUSER	The profile folder of the local user who connected the CTERA Agent to the CTERA Portal or cloud gateway. For example, if the local user who connected the agent to the portal is "JohnSmith", then $PRIMARYUSER will refer to C:\Users\JohnSmith. This variable is relevant for the CTERA Windows Agent only.

Modifying Backup and Exclude Sets

To modify a backup or exclude set, click the name of the backup set in the **Backup Sets** or **Exclude Sets** tab and proceed as for creating.

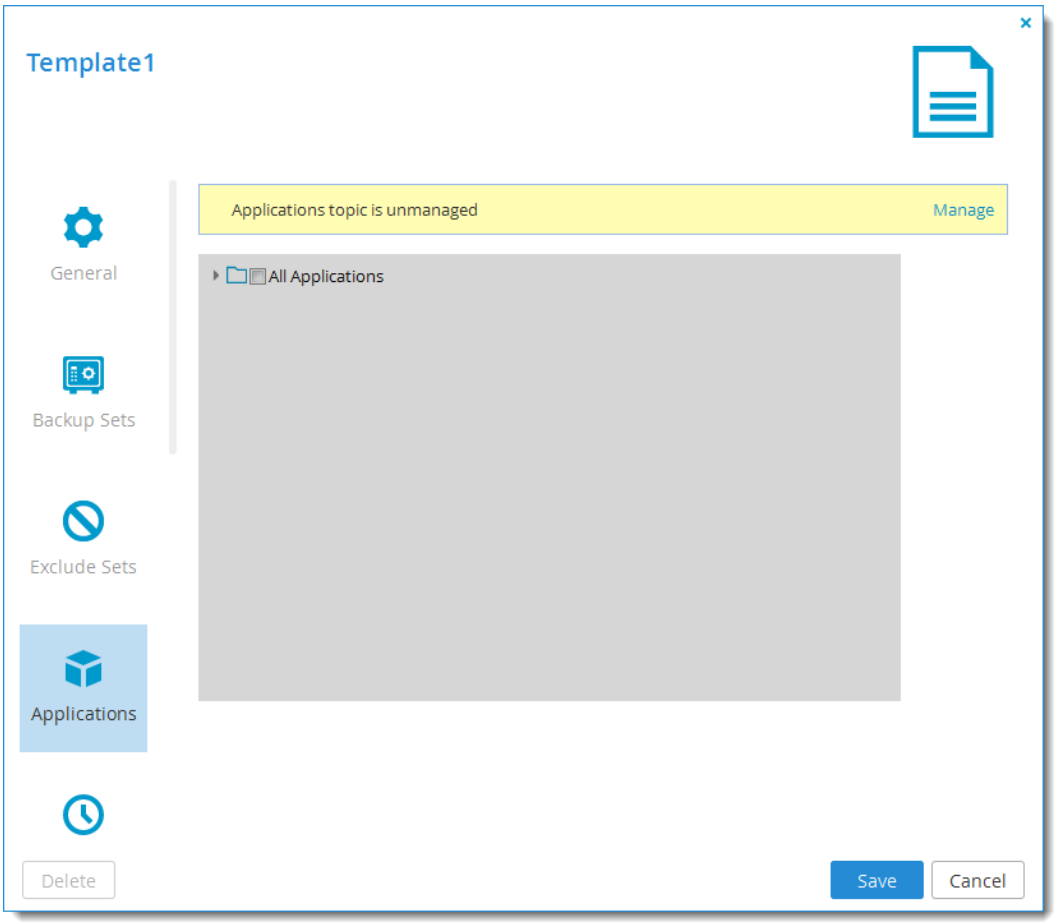
Selecting Applications for Backup

Tip

If a selected application is not installed on the target device, it will be ignored.

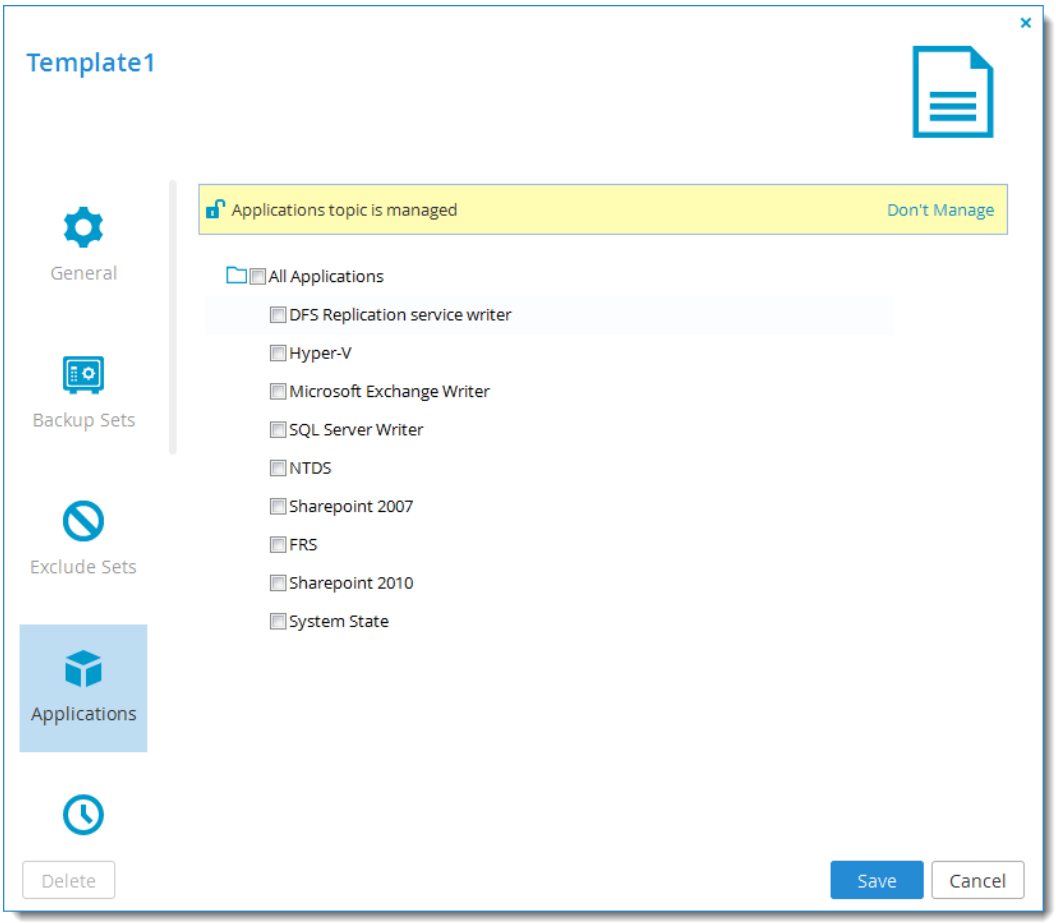
To select applications for backup

1 Select the **Applications** tab.



2 If the applications topic is currently unmanaged, click **Manage**. The device template will now manage which applications are backed up in any devices using this template. Management of application backup will be disabled in the devices' local administration interfaces.

If you prefer that application backup is managed from each device's administration interface, you can revert by clicking **Don't Manage**.

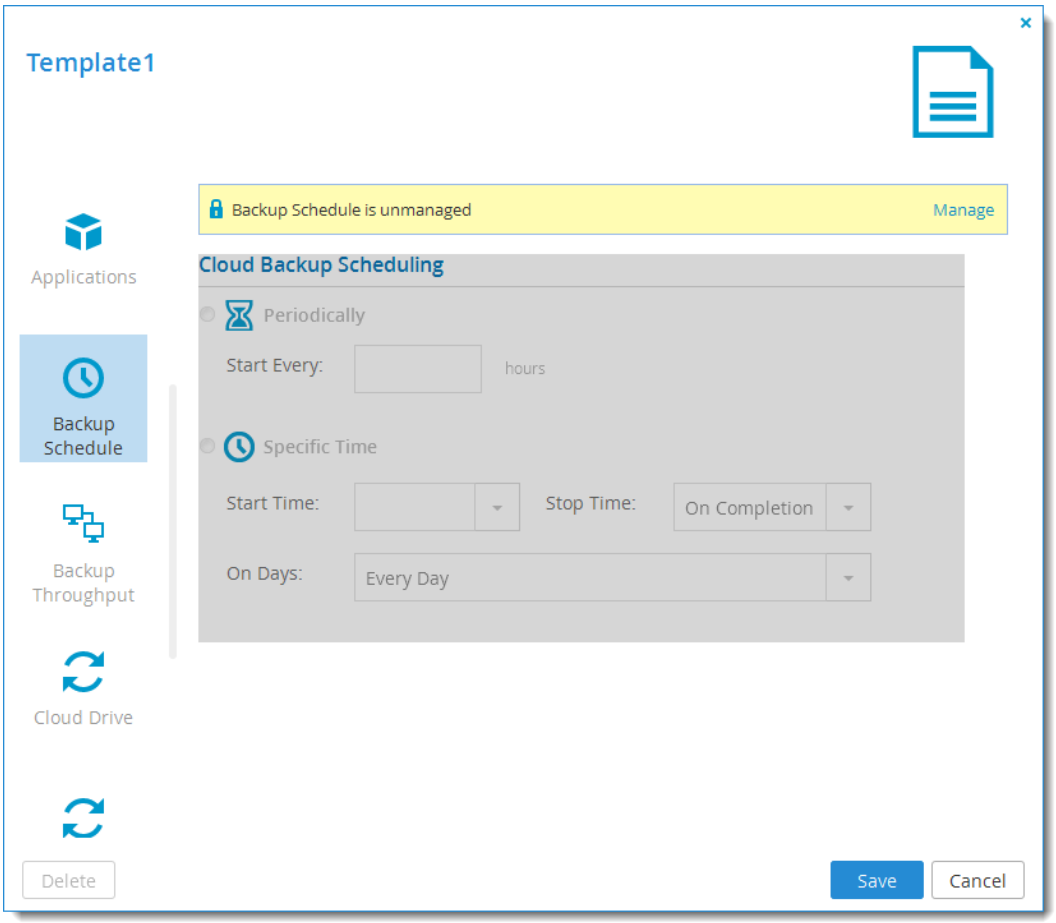


3. Expand the tree nodes and select the check boxes next to the applications you want to back up.
4. Click **Save**.

Cloud Backup Schedule

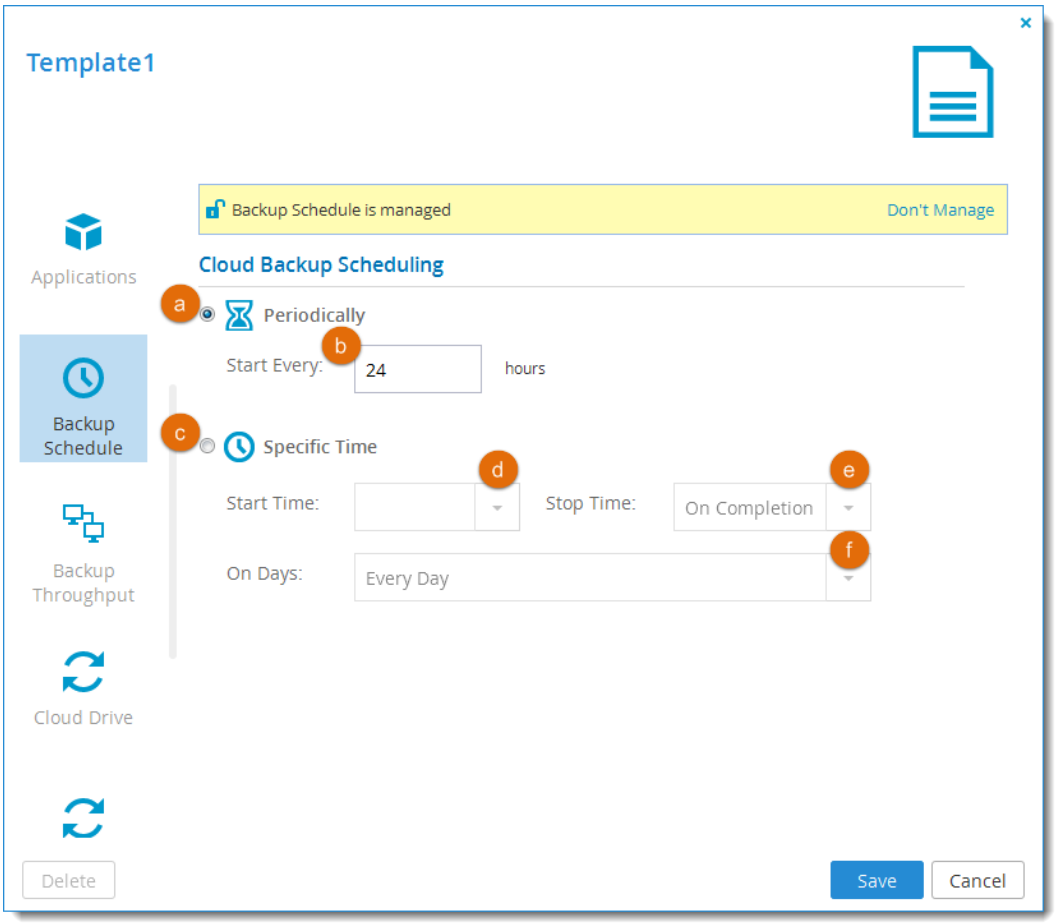
To manage the cloud backup schedule

1 Select the **Backup Schedule** tab.



2 If the backup schedule is currently unmanaged, click **Manage**. The device template will now manage the backup schedule for any devices using this template. Management of backup schedule will be disabled in the devices' local administration interfaces.

If you prefer that backup schedule is managed from each device's administration interface, you can revert by clicking **Don't Manage**.



3 Configure the backup schedule:

a **Periodically**. Choose this option to automatically back up files every specified number of hours.

b **Start Every**. Type the amount of time between automatic cloud backups, in hours. (The default is 24 hours.)

c **Specific Time**. Choose this option to automatically back up files according to a specified daily schedule.

d **Start Time**. Select the time at which cloud backup should start.

Tip

If a given backup extends past the scheduled time for the next automatic backup, the next automatic backup will commence immediately upon completion of the prior backup.

e **Stop Time**. Select the time at which cloud backup must end. This can be any of the following:

- A specific hour
- **On Completion** (default). The backup operation will only end when cloud backup is complete.

Tip

If the amount of changed data to back up is large, the backup process can take several hours or days. Therefore, if a stop time is configured, the backup process may not be completed within the time frame. For example, if you specify that data should be backed up between 12 AM - 2 AM, and the backup requires 3 hours, the backup will not be completed.

f **On Days**. Select the days on which cloud backup should be performed. This can be any of the following:

- One or more specific days
- **Every Day** (default). Cloud backup will occur every day.

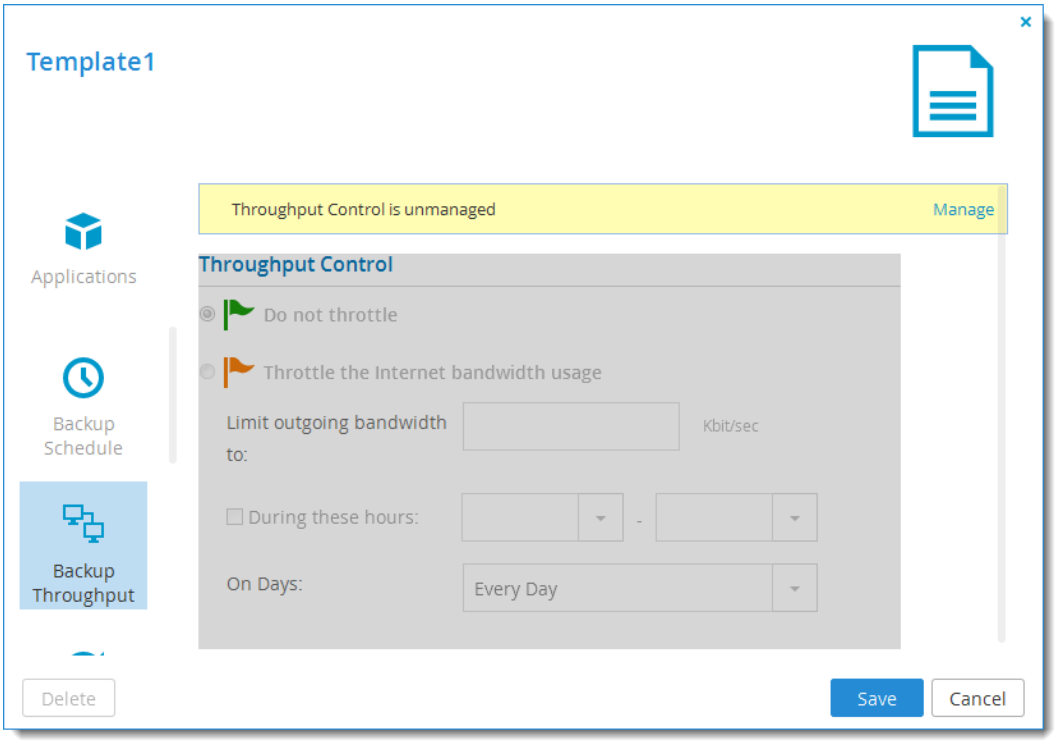
4 Click **Save**.

Backup Throughput

If desired, you can restrict the amount of bandwidth used for backing up files online.

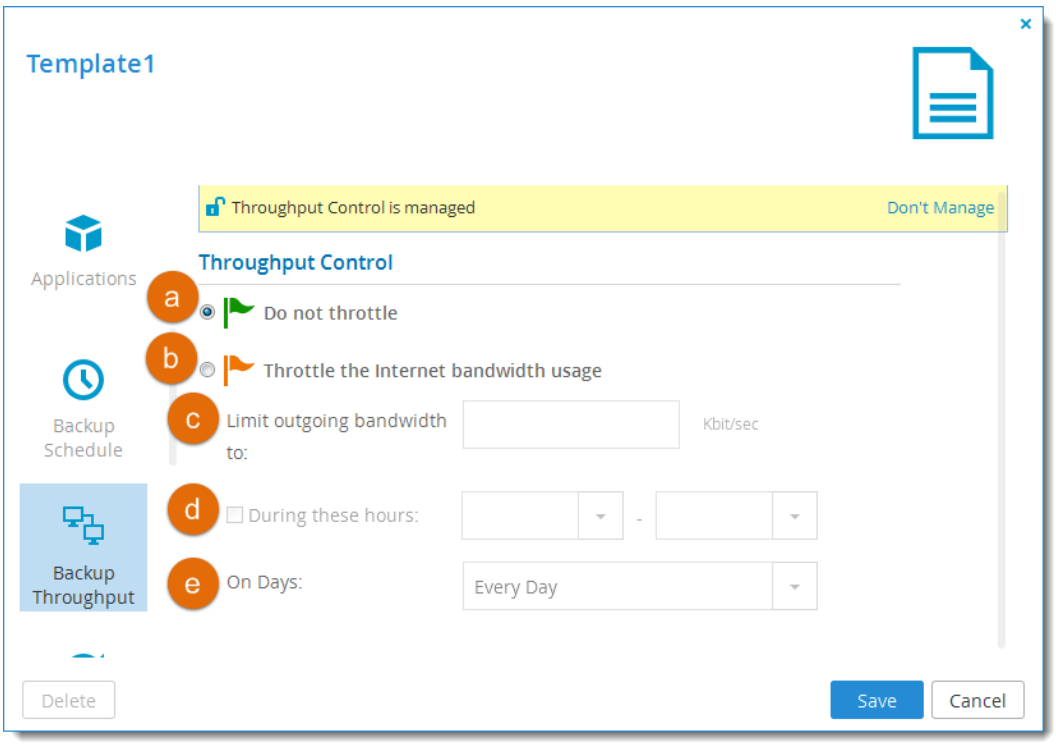
To restrict throughput

1 Select the **Backup Throughput** tab.



2 If backup throughput is currently unmanaged, click **Manage**. The device template will now manage backup throughput for any devices using this template. Management of backup throughput will be disabled in the devices' local administration interfaces.

If you prefer that backup throughput is managed from each device's administration interface, you can revert by clicking **Don't Manage**.



3 Configure the backup throughput settings:

a **Do not throttle**. Choose this option to specify that throughput should not be restricted.

b **Throttle the Internet bandwidth usage**. Choose this option to restrict the bandwidth used for cloud backups.

c **Limit outgoing bandwidth to**. Type the maximum bandwidth to use for cloud backups in kilobytes per second.

d **During these hours**. Select this option to specify that the bandwidth used for cloud backups should be restricted only at specific times of the day. Then use the drop-down lists to specify the time range during which the bandwidth should be restricted.

e **On Days**. Select to specify that the bandwidth used for cloud backups should be restricted only on specific days. This can be any of the following:

- One or more specific days
- **Every Day** (default). Bandwidth used for cloud backup will be restricted every day.

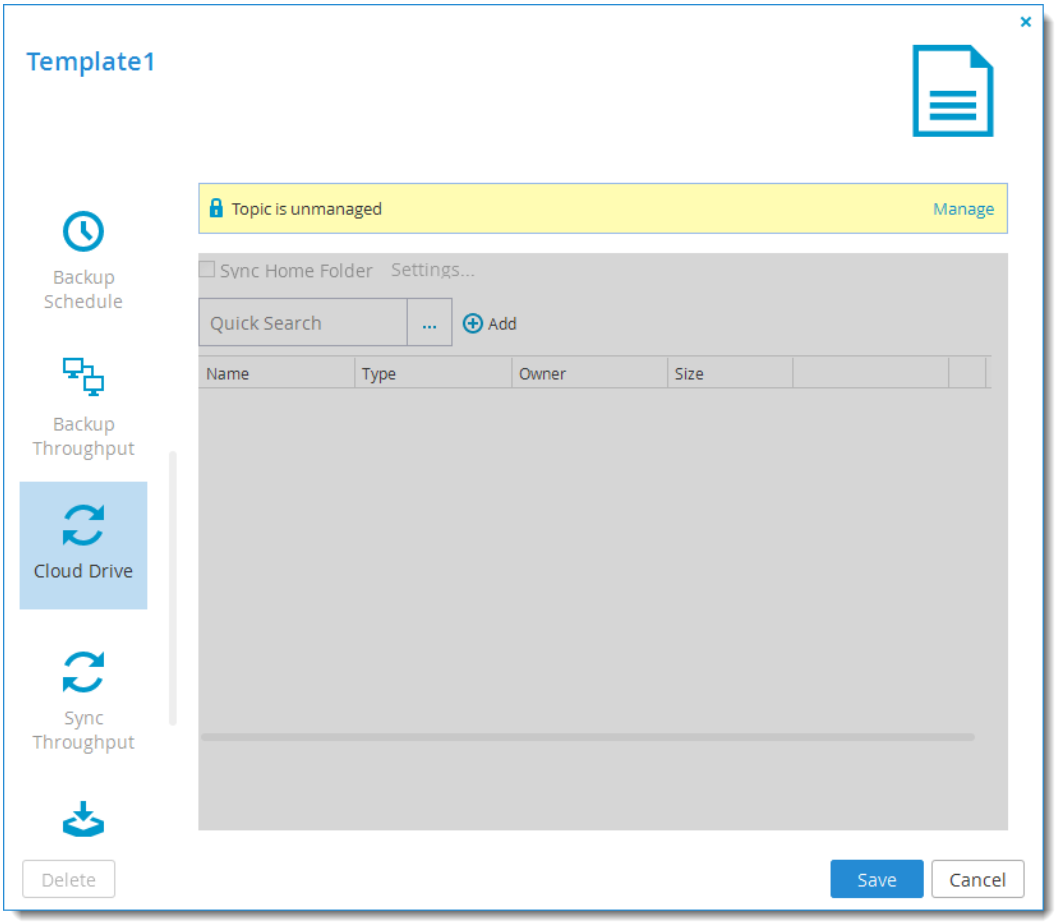
4 Click **Save**.

Cloud Drive Synchronization

You can specify which portal cloud folders should be synchronized with the device, and with which folder each cloud drive folder should be synced.

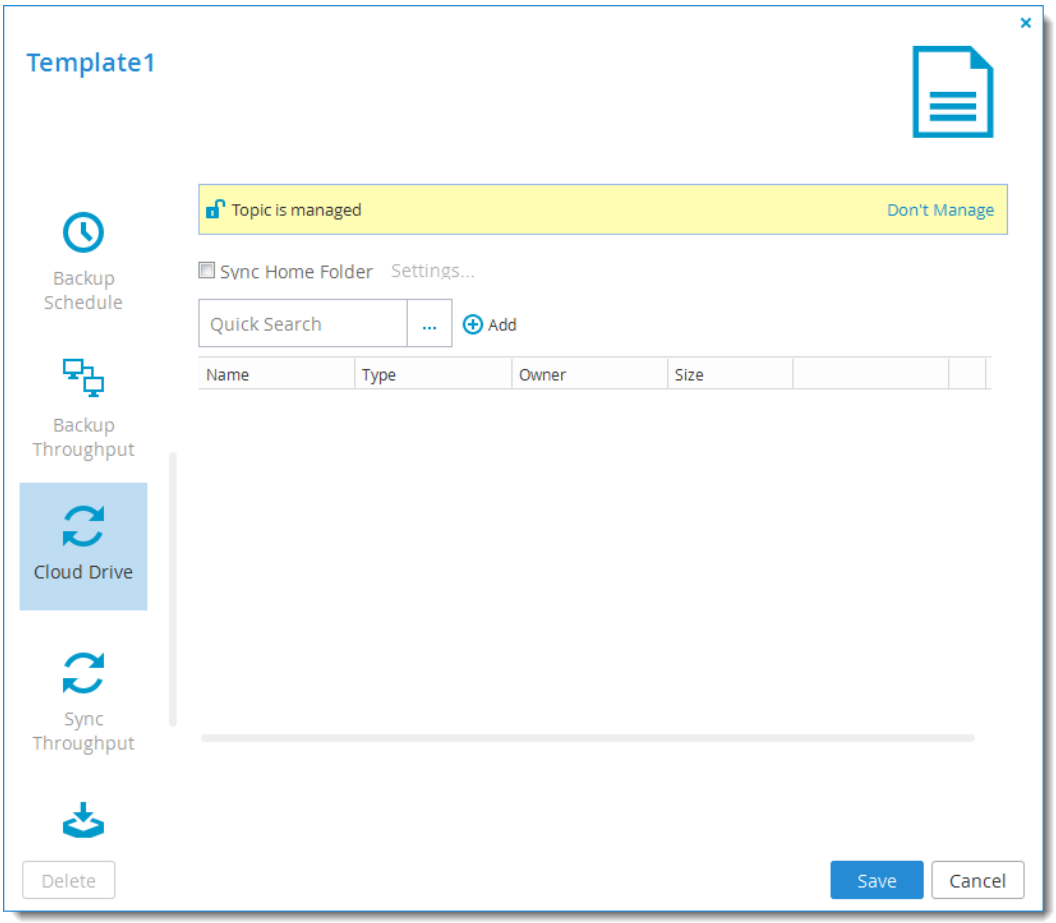
To manage cloud drive sync in the device template

1 Select the **Cloud Drive** tab.

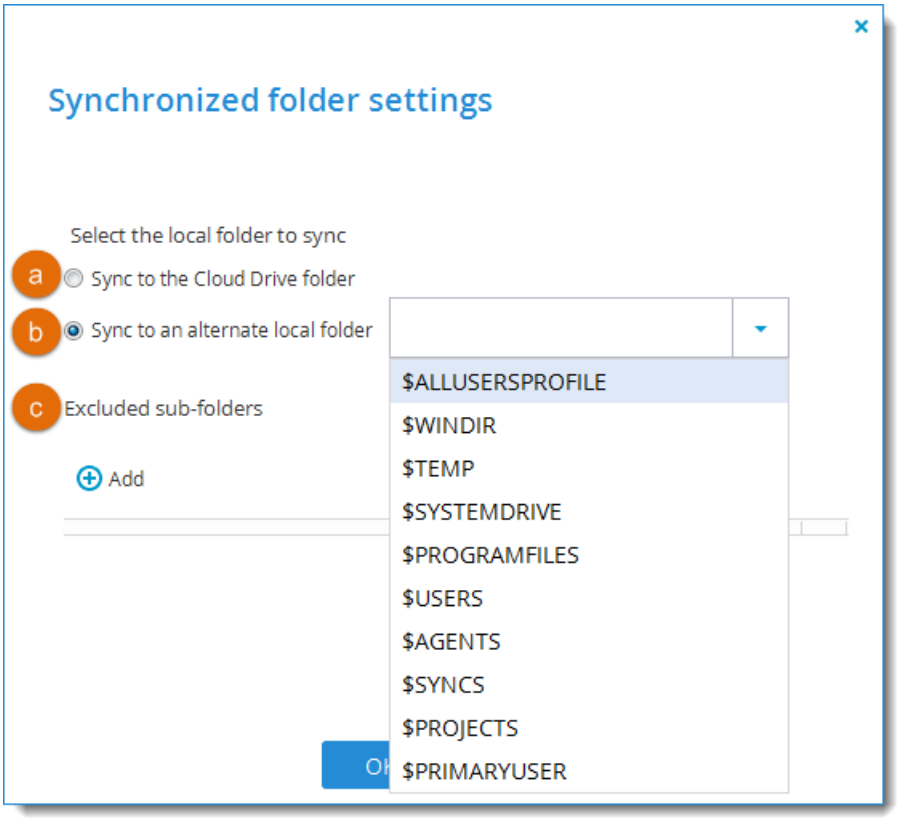


2 If the topic is currently unmanaged, click **Manage**. The device template will now manage cloud drive folder sync in any devices using this template. Management of cloud drive sync will be disabled in the devices' local administration interfaces.

If you prefer that cloud drive sync should be managed from each device's administration interface, you can revert by clicking **Don't Manage**.



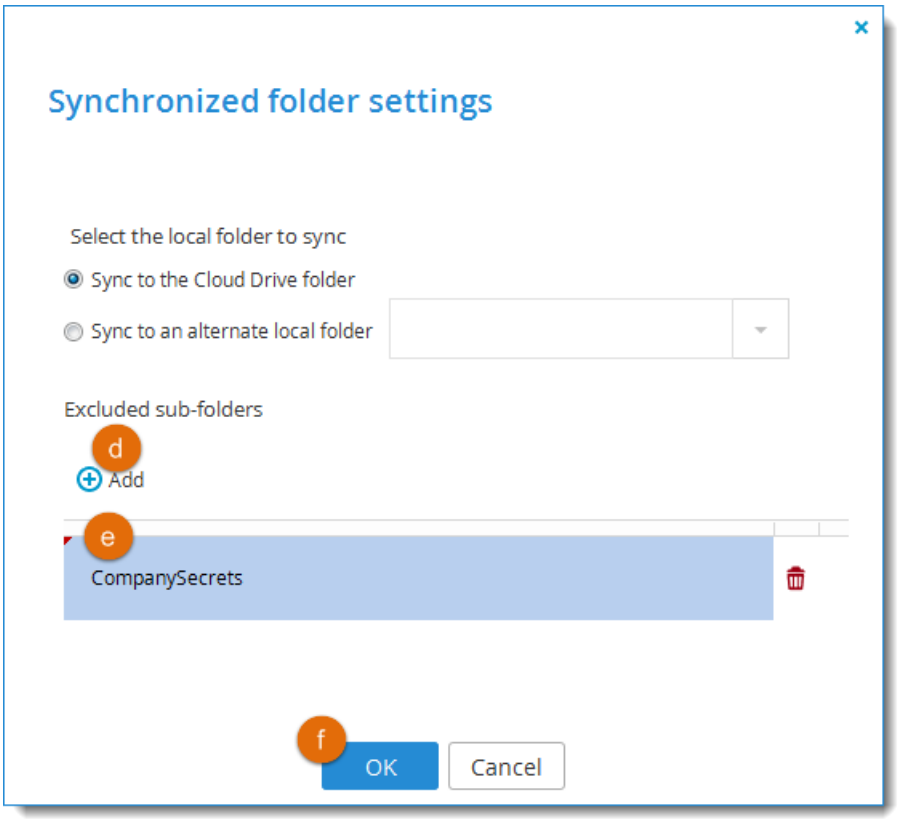
3 To sync the home folder, select **Sync Home Folder** and set which local folder on the device the cloud drive home folder should be synced:



a Sync the folder to a subfolder of the **cloud** folder on the gateway.

b Sync the folder to any folder on the gateway you select, using one of the ***supported variables*** (page 194).

c Exclude sub-folders:



d Click **Add** in the **Excluded sub-folders** section.

A row is added to the **Excluded sub-folders** list.

e Click in the row and type the name of a sub-folder you want to exclude from syncing.

Repeat the previous steps to add more sub-folders as necessary until all the folders you want to exclude are listed.

f Click **OK** to apply your changes.

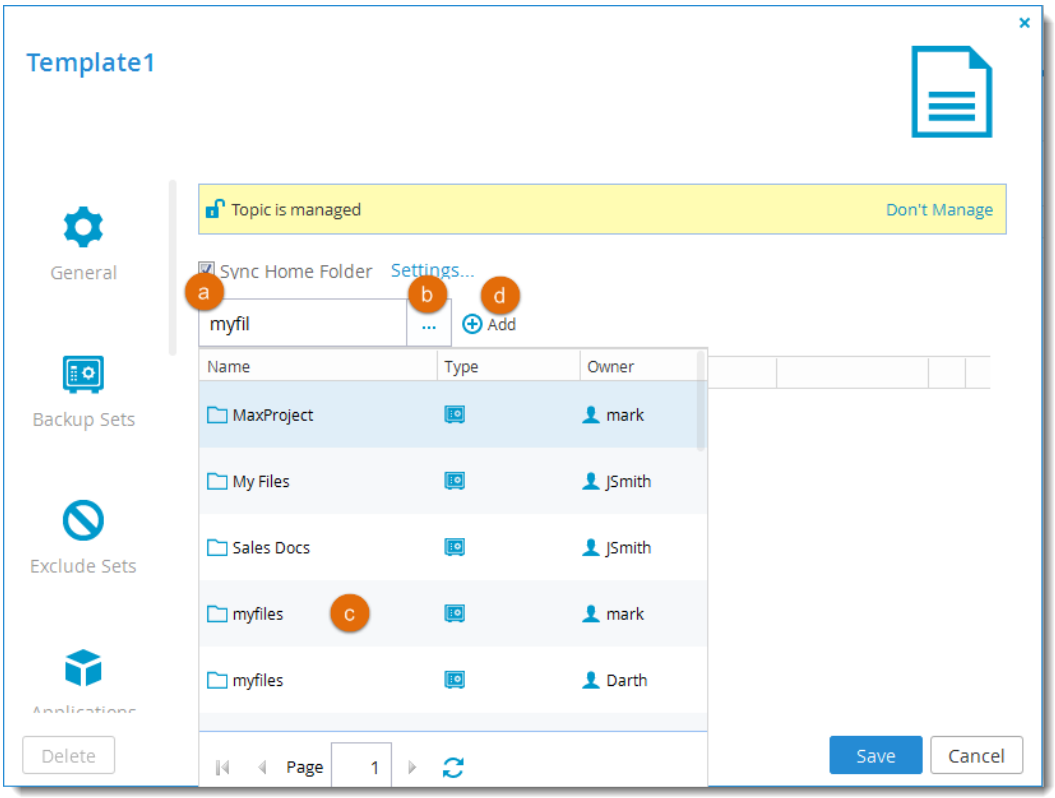
4 To add more cloud drive folders to sync with the device:

a Click in the **Quick Search** field and type a search string to search for the name of a cloud drive folder you want to add.

b Click 

.

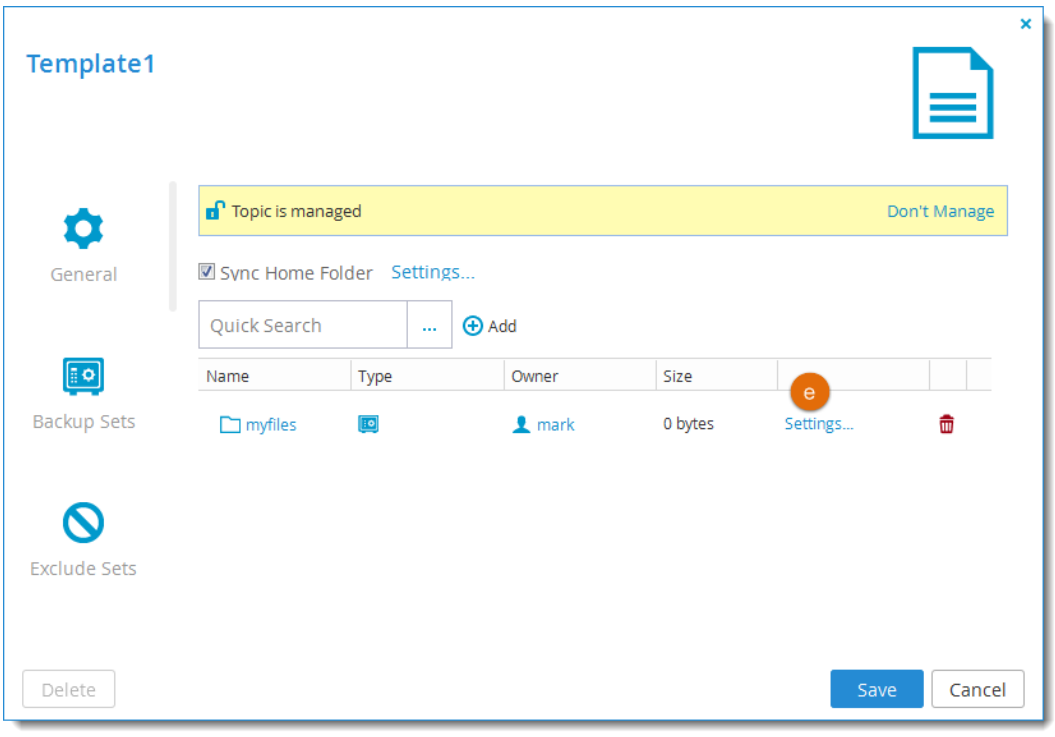
All the folders including the search string in their names appear.



c Select the folder you want to add.

d Click **Add**.

The folder is added to the list.



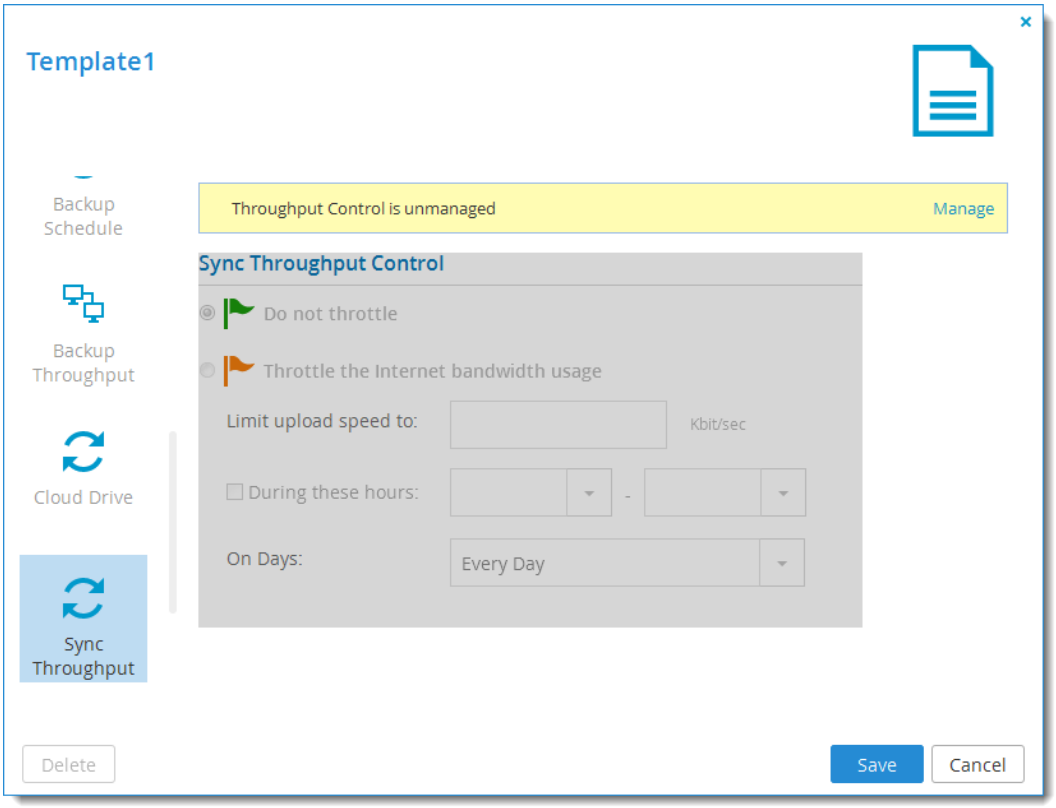
e To set which folder on the device the folder should sync with, click the **Settings** button in the folder's row, and set the folder as described above.

5 Click **Save**.

Managing Sync Throughput

To control whether the cloud sync upload speed is limited, and how and when it is limited:

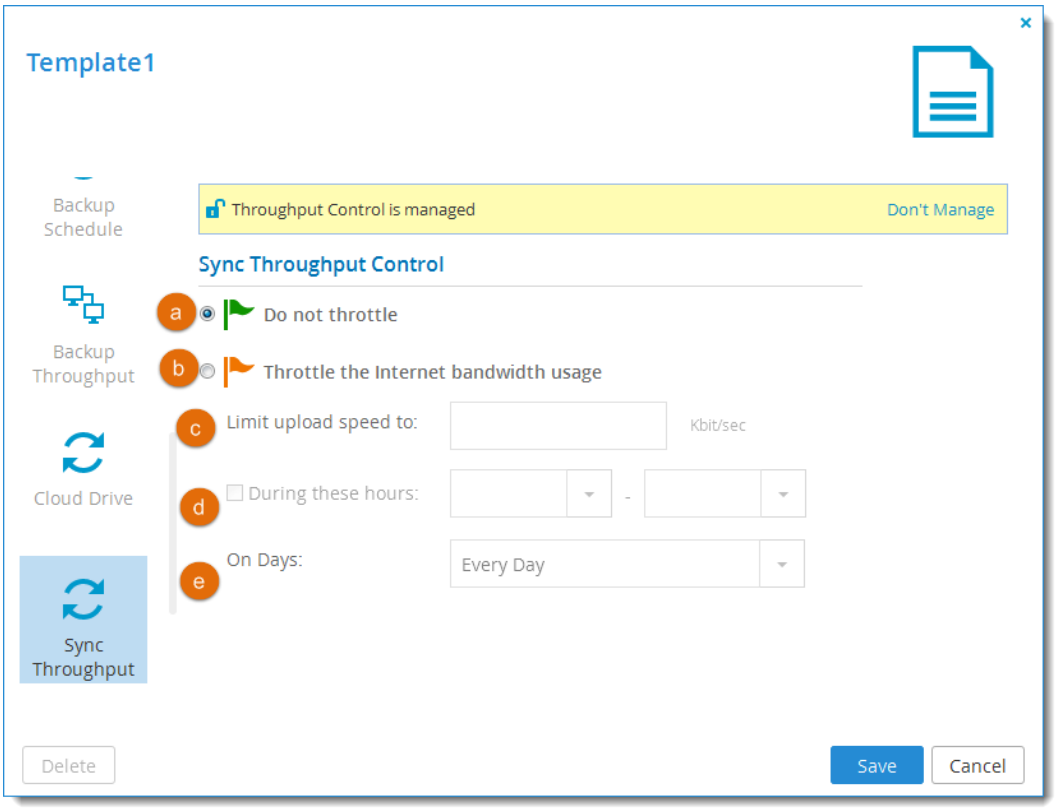
1 Select the **Sync Throughput** tab.



2 If sync throughput is currently unmanaged, click **Manage**. The device template will now manage sync throughput for any devices using this template. Management of sync throughput will be disabled in the devices' local administration interfaces.

If you prefer that sync throughput is managed from each device's administration interface, you can revert by clicking **Don't Manage**.

3 Set the controls for sync throughput:



a **Do not throttle**. Unlimited speed for uploading files to the Cloud Drive for syncing.

b **Throttle the Internet bandwidth usage**. Limited speed of uploading files to the Cloud Drive for syncing. Enables (c), (d), and (e).

c **Limit upload speed to**. Type the maximum speed to use for cloud drive sync upload in Kbits per second.

d **During these hours**. Select this option to specify that the bandwidth used for cloud drive sync upload should be restricted only at specific times of the day. Then use the drop-down lists to specify the time range during which the bandwidth should be restricted.

e **On Days**. Select to specify that the bandwidth used for cloud drive sync upload should be restricted every day (default) or only on specified days.

4 Click **Save**.

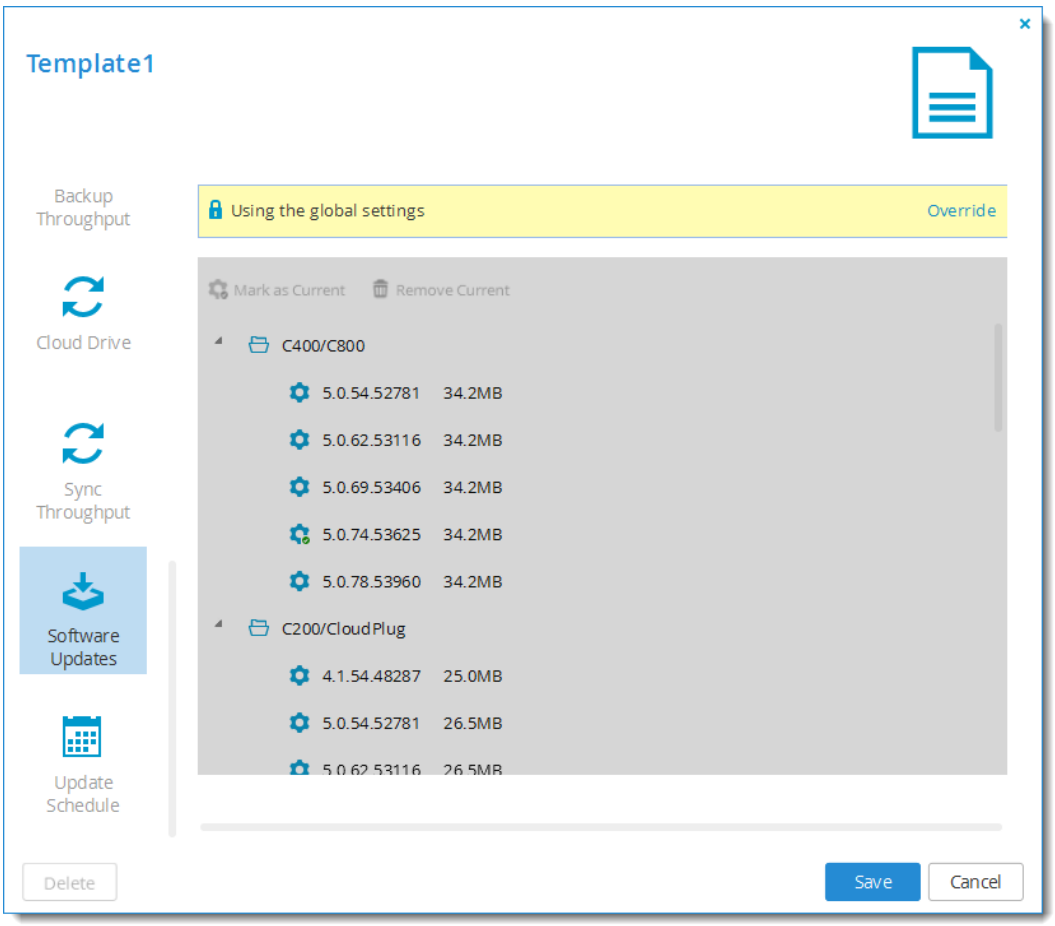
Marking a Firmware Image as the Current Firmware Image

When you mark a firmware image as the current firmware image, all devices that are of the relevant device platform, assigned to this template, and set to automatically download firmware images will download this firmware image.

There can only be one current firmware image per device platform.

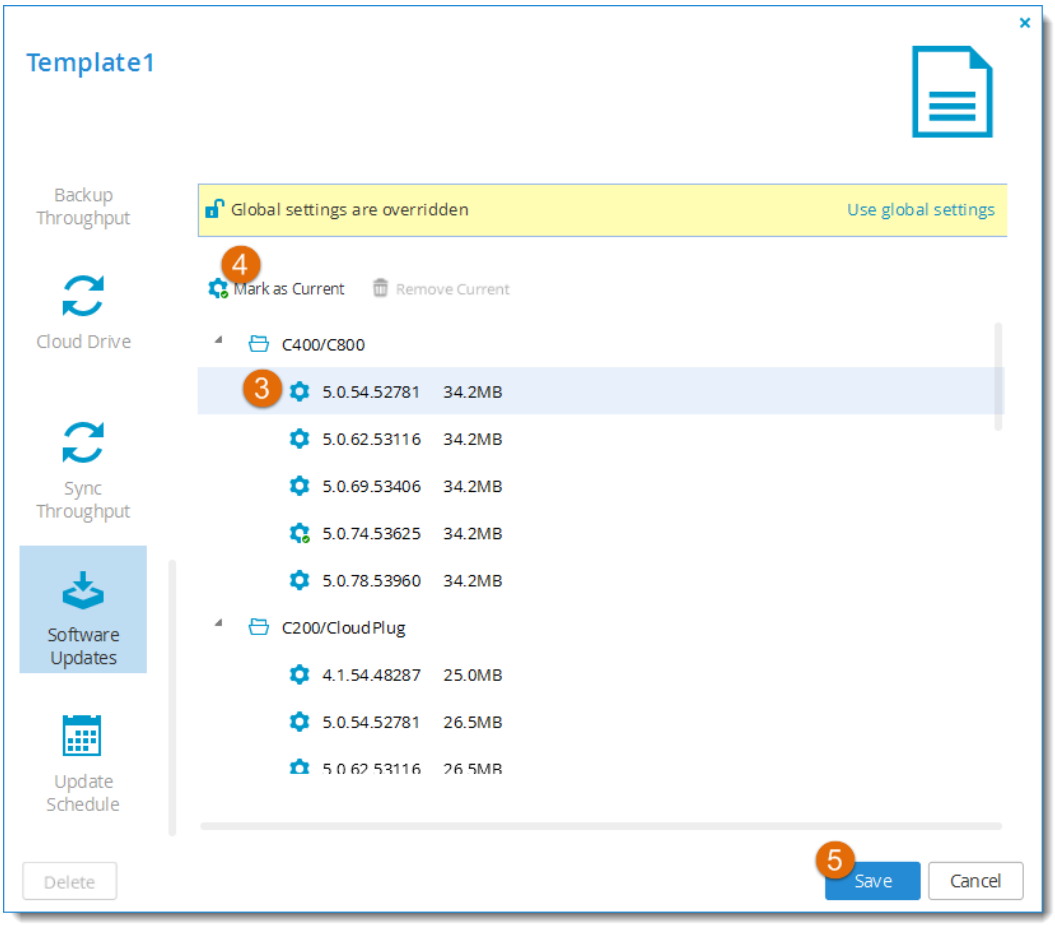
To mark a firmware image as the current firmware image

1 Select the **Software Updates** tab.



2 Click **Override** if you want to override global settings.

When global settings are overridden, you can revert to global settings, by clicking **Use global settings**.



3 Select the desired firmware image's row.

4 Click **Mark as Current**.

The selected firmware image becomes the current firmware image and is marked with the icon.

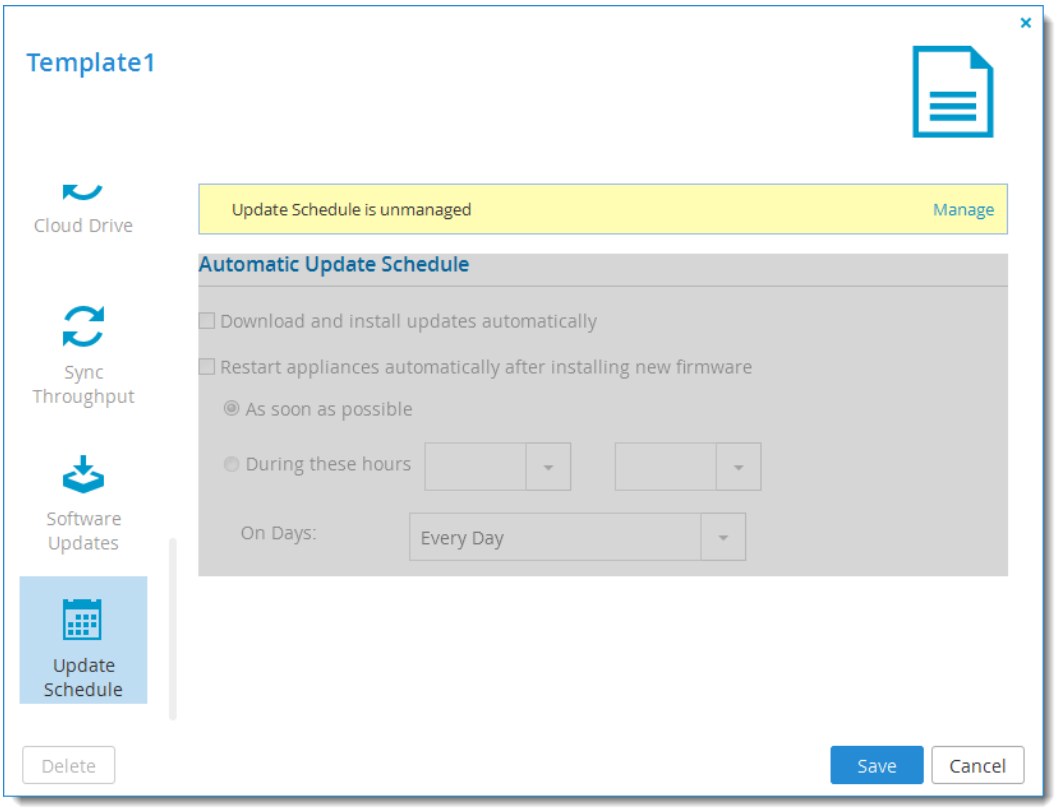
5 Click **Save**.

Configuring Automatic Firmware Updates

If desired, you can configure your devices to automatically download and install firmware updates.

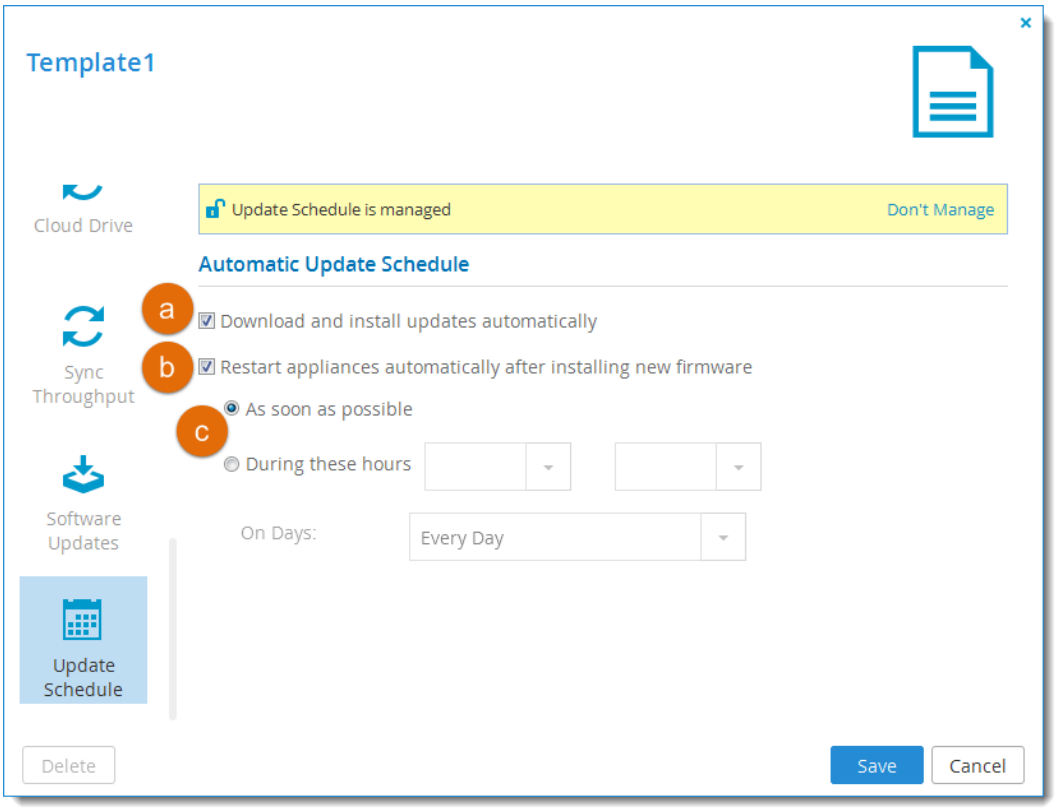
To configure automatic firmware updates

1. Select the **Update Schedule** tab.



2. If the update schedule is currently unmanaged, click **Manage**. The device template will now manage the firmware update schedule for any devices using this template. Managing the firmware update schedule will be disabled in the devices' local administration interfaces.

If you prefer that the firmware update schedule should be managed from each device's administration interface, you can revert by clicking **Don't Manage**.



3 Configure the firmware update schedule:

a To specify that the CTERA Portal should download and install firmware updates automatically, click **Download and install updates automatically**. If you do not select this option, device owners must perform firmware updates manually.

To specify that the CTERA Portal should automatically reboot after installing new firmware updates, do the following:

b Click **Restart automatically after installing new firmware**.

c Specify when automatic rebooting should occur, by doing one of the following:

- To reboot as soon as possible after a firmware update, choose **As soon as possible**.

  In this case, the CTERA Portal will reboot as soon as it is recommended to do so. For example, the automatic reboot might be deferred, if the CTERA Portal is undergoing system maintenance that should not be interrupted.

- To reboot only during specific hours, choose **During these hours**, then use the drop-down down lists to specify the desired time range.

- To reboot on automatically specified days, choose **On Days** and select one or more specific days or **Every Day** to automatically reboot every day (default).

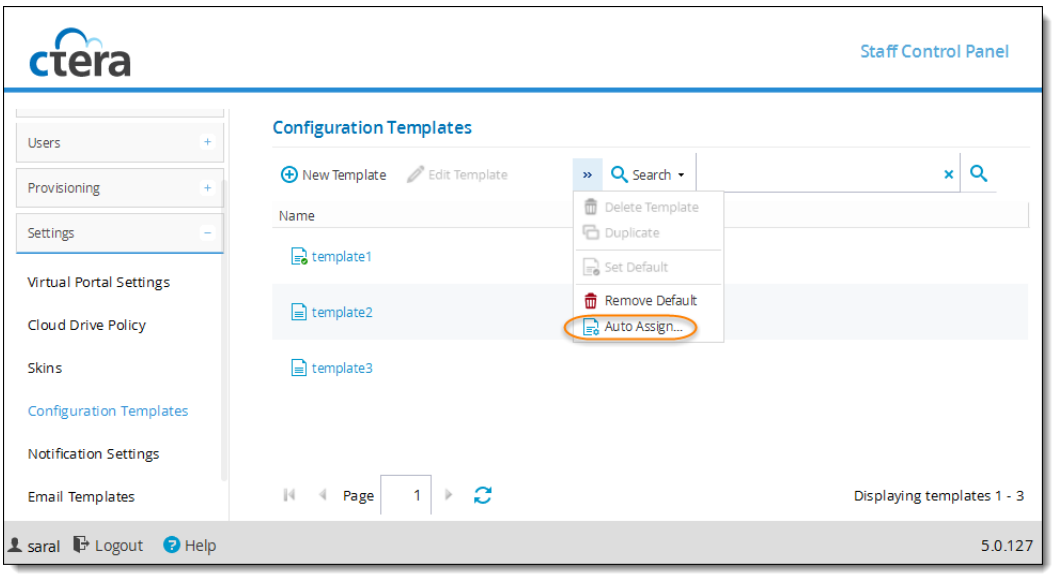
4 Click **Save**.

Configuring the Automatic Template Assignment Policy

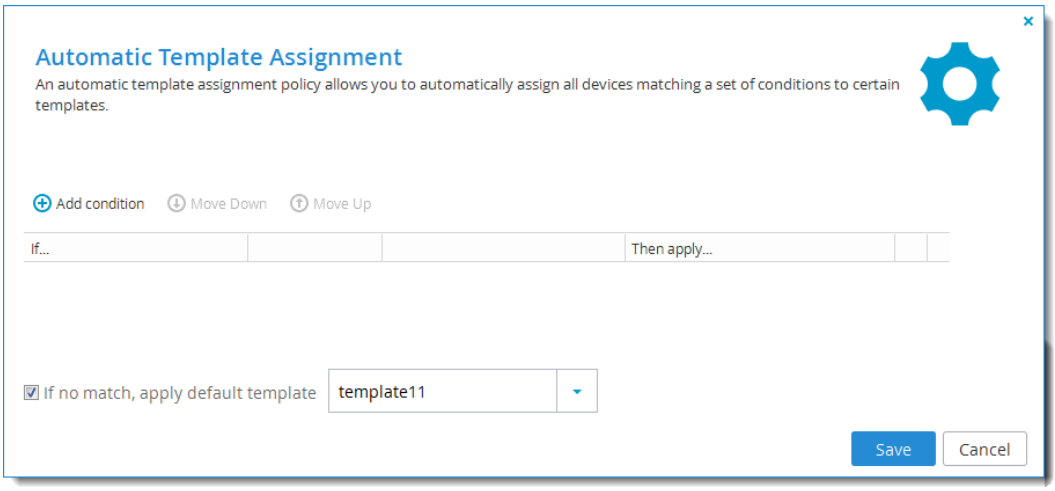
To configure the automatic template assignment policy

1 Browse to **Settings > Configuration Templates**.

2 Click **Auto Assign**.



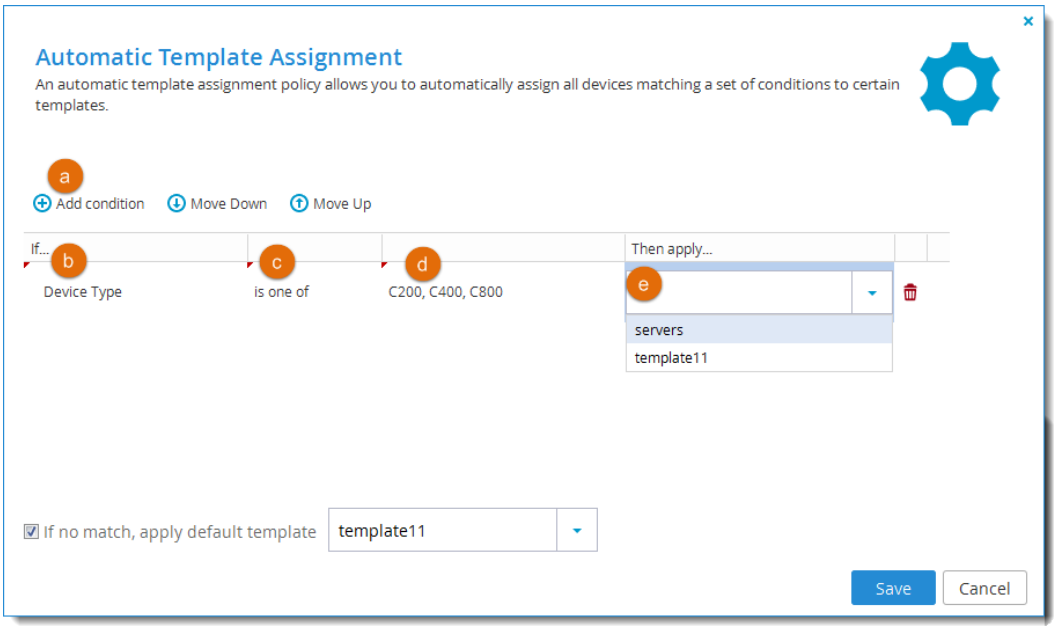
The Automatic Template Assignment dialog box appears.



3 Define the desired conditions for a device to be assigned to a template, by doing the following for each condition:

a Click **Add condition**.

A row appears in the table.



b Click the cell in the first column, then select the desired condition parameter from the drop-down list.

c Click in the second column, then select the desired condition operator from the drop-down list.

d Click in the third column, and complete the condition, by selecting values or typing the desired free-text value.

Multiple values must be separated by commas.

For example, if you select **Installed Version** as the condition parameter in the first column, select **equals** with as the condition operator in the second column, and type "3.0" in the third column, then the condition will be met when the device's installed firmware version is 3.0.

Another example: If you select **Owner Groups** as the condition parameter in the first column, select **includes one of** as the condition operator in the second column, and type "groupA, groupB" in the third column, then the condition will be met when the device owner's user account belongs to user group "groupA" or user group "groupB".

e Click in the **Then apply** column, and select the template that should be assigned when the condition is met.

4 To delete a condition, click in its row.

5 To specify that the policy should include a default device configuration template, do the following:

a Select the **If no match, apply default template** check box.

b In the **If no match, apply default template** drop-down list, select the template to apply when none of the conditions are met.

6 Click **Save**.

Setting the Default Device Configuration Template

Tip

You can also set the default device configuration template as part of an automatic template assignment policy.

To set a device configuration template as the default

1 Select the desired template's row.

2 Click **Set Default**.

The selected template is marked with the icon.

To set no default device configuration template

1 Click **Remove Default**.

No default template is configured.

Duplicating Configuration Templates

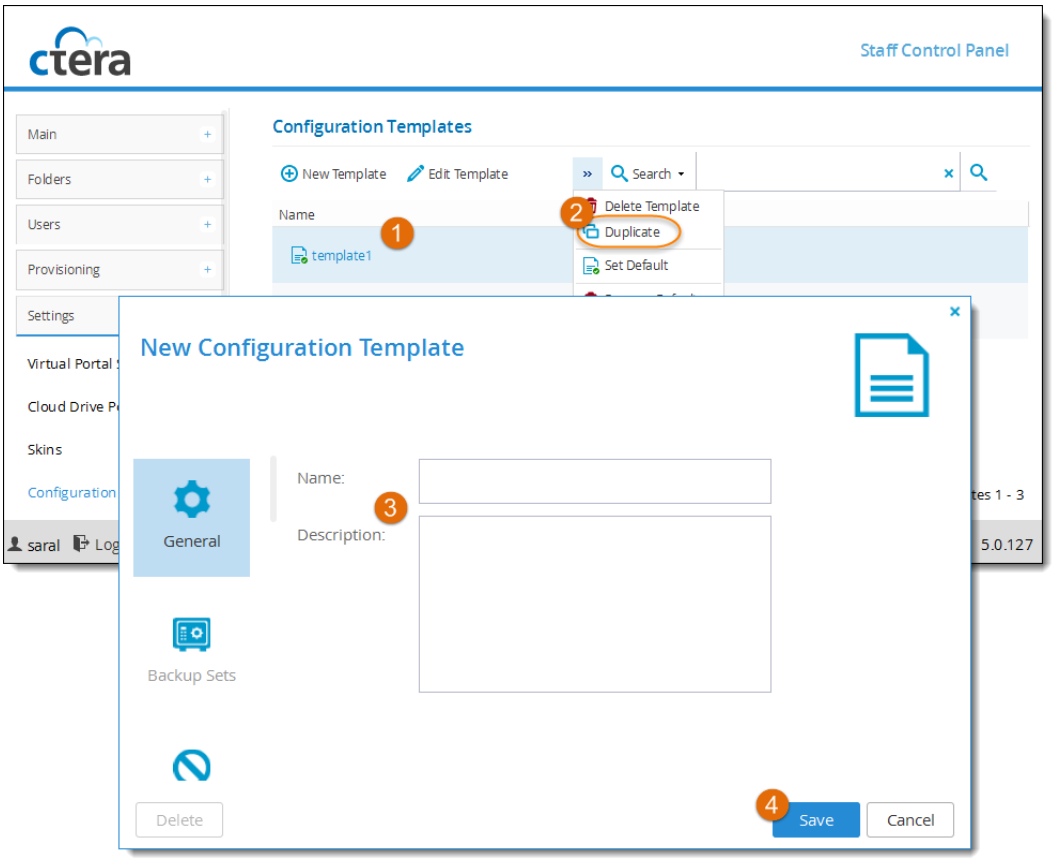
You can create a duplicate of an existing configuration template, then edit it as desired. All settings, except for the template name and description, are copied from the original template.

To duplicate a configuration template

1 Select the template's row.

2 Click **Duplicate**.

A New Configuration Template dialog box opens.



3 Type the **Name** and **Description** of the new template.

4 Click **Save**.

Deleting Device Configuration Templates

When a device configuration template is deleted from the CTERA Portal, the automatic template assignment policy rules that specify that template are automatically deleted. The policy is then reapplied to all devices that specify automatic template assignment.

Tip

When deleting device configuration templates, the following restrictions apply:

- You may not delete a template that is manually assigned to a device.
- You may not delete the default template.

To delete a device configuration template

1 Do one of the following:

- Select the template's row, then click **Delete Template**.
- Select the template and click **Edit Template** to open the template's manager, and then click **Delete**.

2 Click **Yes** to confirm.

The template is deleted.

16

Notifications

In This Chapter

Overview

You can receive and view notifications about the portal users and their devices:

- On the **Notifications** dashboard **(Main > Notifications**). Here, you receive all types of notifications that are enabled on the Notification Settings page (**Settings > Notification Settings**).
- In the main Dashboard (**Main > Dashboard**) This page displays a summary of the ten highest priority notifications.
- By email. Notifications are sent to administrators by email.

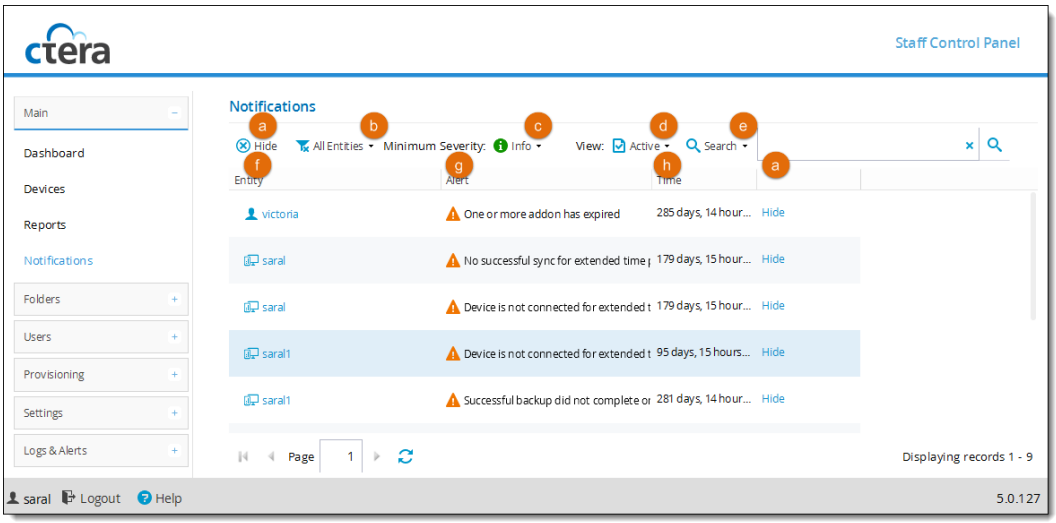
Notifications enable you to track error and warning conditions. For instance, one can use the notification dashboard to track failed backup jobs.

The notification dashboard displays error and warning conditions that are currently in effect. It is possible to mark specific notifications as hidden, if you do not feel that they require immediate attention. Those notifications can always be unhidden later if desired.

The Notifications Dashboard

To see the notifications dashboard

Select **Main > Dashboard** from the menu.



a **Hide**. Select a notification's row and click **Hide** to hide the notification. You might want to do hide a notification if you don't feel it requires immediate attention. You can unhide it again any time by displaying hidden notifications (see (d)) and then clicking the **Unhide** button that appears here instead of **Hide**. .

b Filter by entity. Click the arrow to select which types of entities you want to display notifications for.

c Filter by severity. Click the arrow to select the minimum severity level you want to display.

d View active/hidden notifications. Click the arrow to toggle between viewing only active notifications or active and hidden notifications.

e **Search**. Search by entity and/or alert text. Click the arrow to select **Entity** and/or **Alert**, enter search text and click .

f **Entity**. The entity that the notification concerns. Click the entity name to open it's editor. For example, if the entity is a device click the device name to open the device's editor window.

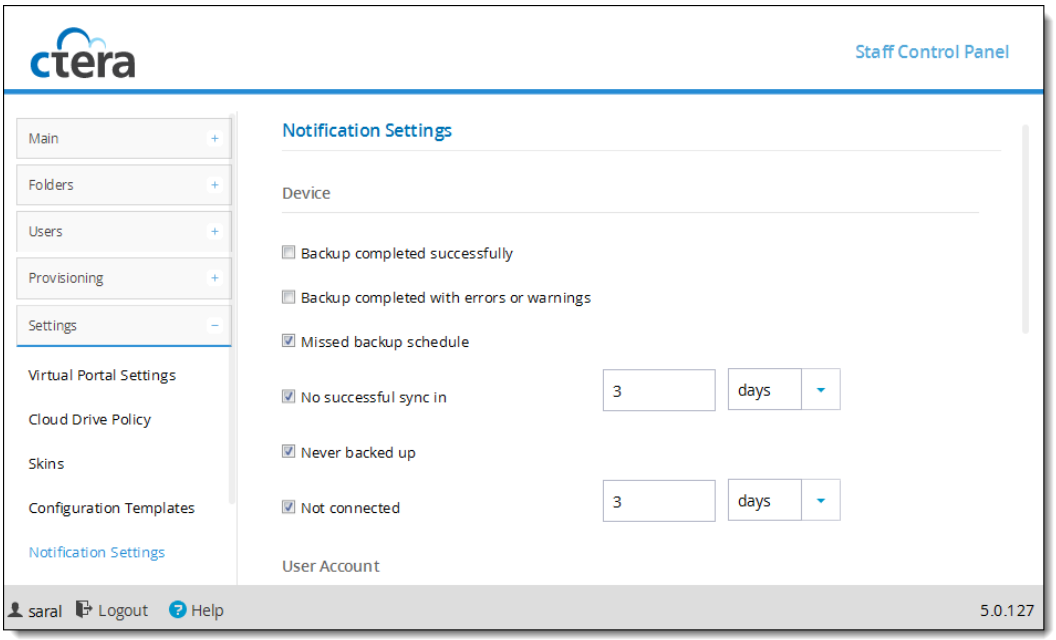
g **Alert**. The alert message.

h **Time**. The time at which the alert was triggered.

Configuring Notification Settings

To configure notifications

1 Browse to **Settings > Notification Settings**.



2 Select notifications to enable them. Deselect notifications to disable them.

3 Click **Save** to save your changes.

Any notifications of the types that are enabled appear on the notifications dashboard. (**Main > Notifications**). The top ten highest priority notifications also appear on the main dashboard (**Main > Dashboard**).

17

Configuring Email Templates

In This Chapter

Overview

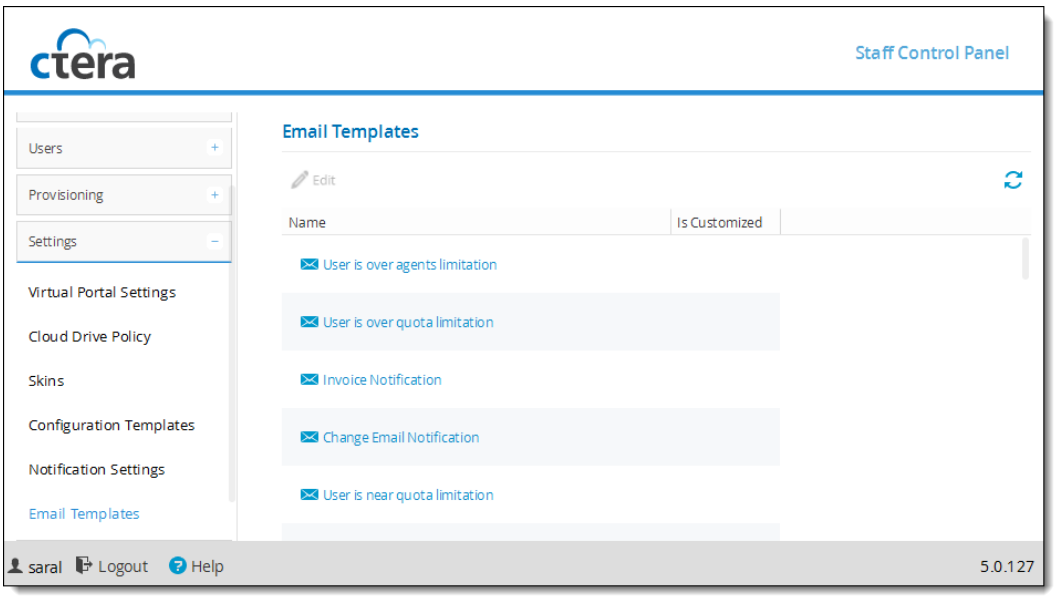
You can configure email notification templates for notifications sent to users from the portal. The email notifications are in HTML format.

Customizing Email Notification Templates

To customize email notification templates

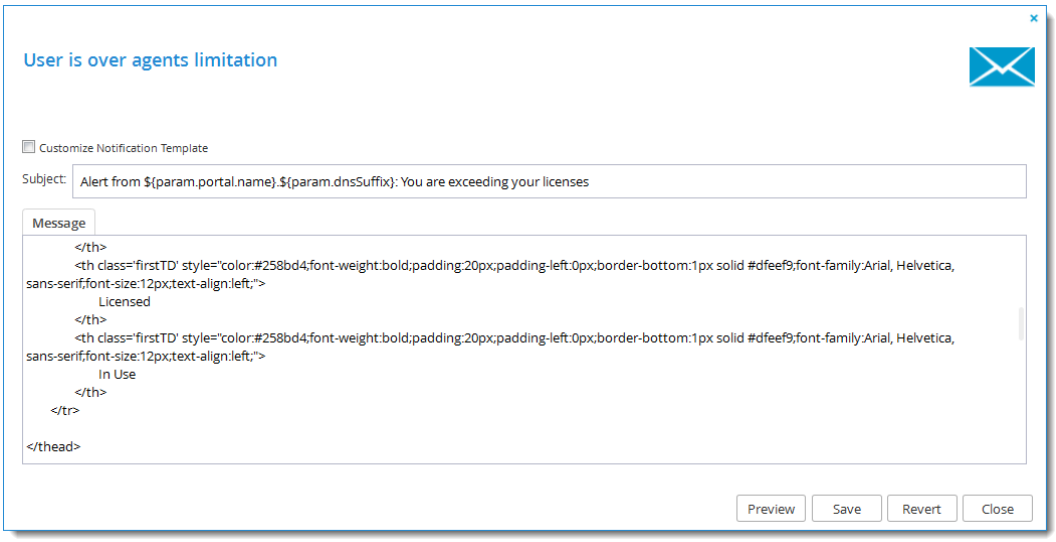
1 Browse to **Settings > Email Templates**.

The **Settings > Email Templates** page appears with a list of email templates. For a description of each template, see ***Email Notification Templates*** (on page 224).



2 Select the desired email template's row and then click **Edit**.

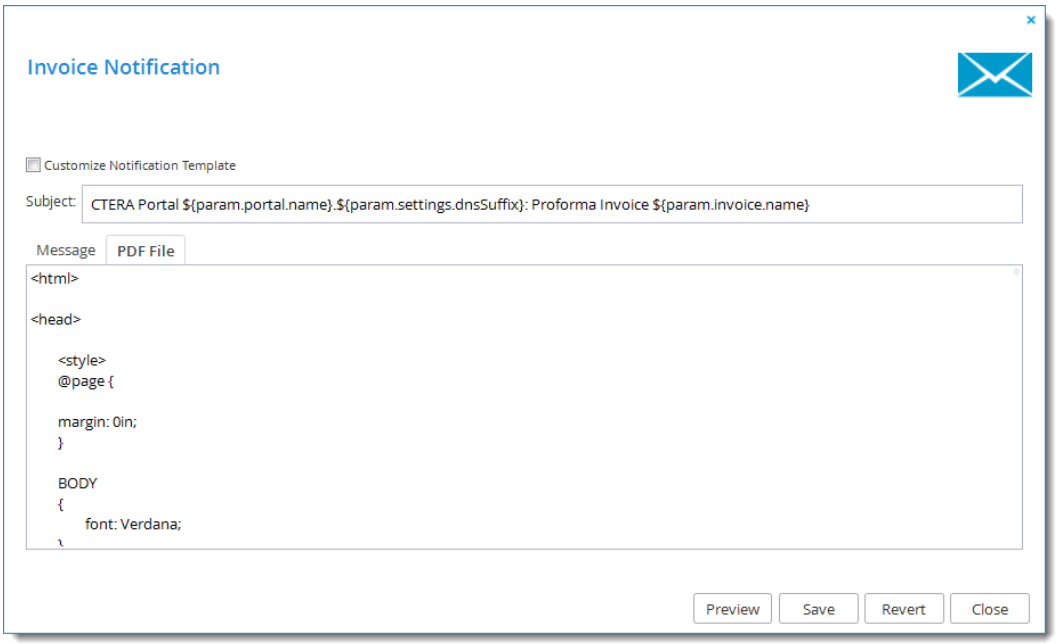
The **Notification Template Editor** opens displaying the **Message** tab.



If the notification includes a PDF attachment, the **Notification Template Editor** will include a **PDF** tab, as well.

3. Select the **Customize Notification Template** check box.
4. In the **Subject** field, type the text that should appear in the notification email's Subject line.
5. In the **Message** box, modify the template as desired.
6. To preview your changes, click **Preview**.
7. To edit a PDF attachment, do the following:
   a. Click the **PDF File** tab.

The **PDF File** tab appears.



b In the **PDF** box, modify the template as desired.

c To preview your changes, click **Preview**.

The PDF is downloaded to your computer.

8 To undo your unsaved changes, click **Revert**.

9 Click **Save**.

Email Notification Templates

Template Name	Description
User is over agents limitation	A notification sent to end users when they have exceeded the licensed number of CTERA Agents.
User is over quota limitation	A notification sent to end users when their cloud storage space is full.
Invoice Notification	A notification sent to end users with an invoice PDF attached. This template allows customizing both the email message and the PDF.
Change Email Notification	A notification sent to end users when a request is made to change their email address.
User is near quota limitation	A notification sent to end users when the amount of cloud backup storage space used reaches or exceeds a certain percentage. The percentage is configured locally.
Password Recovery Notification	A notification sent to end users when a request is made to reset their password.
Device Not Connected	A notification sent to end users when their device has not connected to the CTERA Portal for a certain number of days. The number of days is configured locally.
User Report	A monthly report sent to end users, which includes the following information: Account information Storage statistics Usage report Details of all the user's devices Information on the status of the user's cloud backups
Trial is about to expire	A notification to end users when their trial subscription will expire.
Registration Confirmation	A notification sent to end users after registering with the CTERA Portal, but before activating their account.
header	The HTML header that appears at the top of all notifications.
footer	The HTML footer that appears at the bottom of all notifications.

Template Name	Description
New User Notification	A notification sent to end users when an account has been created for them by an administrator, inviting them to use the portal. The email message contains the portal address, as well as the username and password.
Device activated	A notification sent to end users when their device has been activated.
SMS Verification Code	A notification of a pass code sent to guest invitation recipients by SMS. The recipient must enter the passcode before accessing the file or folder that they are invited to share.
Email Verification Code	A notification of a pass code sent to guest invitation recipients by email. The recipient must enter the passcode before accessing the file or folder that they are invited to share.
Device Wipe completed	A notification sent to the portal administrator who initiated a device wipe when all data and settings have been deleted from the mobile device.
Backup Completed with Errors or Warnings	A notification sent to end users when workstation or server cloud backup has completed with errors or warnings.
Backup Completed Successfully	A notification sent to end users when cloud backup of their workstation or server has completed successfully.
Alert Notification	An alert sent to portal administrators when a log is generated, if an applicable email alert is configured. To configure email alerts, see ***Using Email Alerts*** (on page 241).
No Cloud Drive Sync For Extended Time Period	A notification sent to end users if no cloud sync has occurred between their cloud drive and their workstation or server for a specified time period.
User Account Activated	A notification sent to end users to inform the user that the user's account is now active.
Successful User Registration	A notification sent to a end users informing them that a user they invited has successfully completed the registration process to
Invitation to Register	An invitation to register sent to an external user from an administrator.
Expired Invitation to Register	A notification sent to an external user informing them that an invitation for the user to register has expired.

Template Name	Description
Invitation to Collaborate	A guest invitation to access shared files or folders.
One or more addon has expired	A notification to end users when one or more add-on(s) to which they are subscribed has expired.
Malware blocked	A notification to end users to tell them that malware was detected and blocked in a file they recently uploaded.
One or more addon is about to expire	A notification to end users when one or more add-on(s) to which they are subscribed will expire soon.
Reshare as public link	A notification sent to end users telling them that another user with whom they shared a folder has just created a public link to reshare that folder.
Device Never Backed Up	A notification sent to end users telling them that their device has never backed up.
Backup did not complete on schedule	A notification sent to end users telling them that their device missed its scheduled backup.
Reshare by adding collaborators	A notification sent to end users telling them that another user with whom they shared a folder has resshared your folder with other people, listing the new collaborators.

18

Viewing Logs

The CTERA Portal **Log Viewer** includes the following log categories:

Table 14: Log Categories

This log category...	Displays...
System	All events that do not belong in other log categories.
Local Backup	Events related to synchronization operations.
Cloud Backup	Events related to backup or restore operations.
Cloud Sync	Events related to cloud drive synchronization operations.
Access	Events related to user access to the CTERA Portal.
Audit	Changes to the CTERA Portal configuration.
Agents	Events related to CTERA Agents.

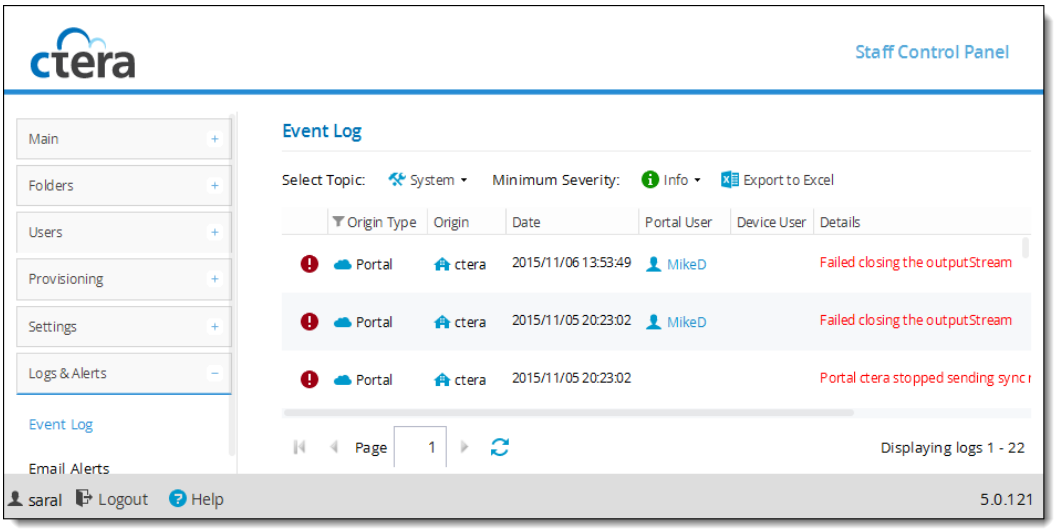
In This Chapter

Viewing System Logs

To view System logs

1 Browse to **Logs & Alerts > Event Log**.

2 From the **Select Topic** dropdown box, select **System**.



The following information is displayed:

Table 15: System Log Fields

This field...	Displays...
Type	An icon indicating the log level. See ***Log Levels*** (page 228).
Origin Type	The type of entity that sent the event log (the portal or a device).
Origin	The entity that sent the event log. To edit or view details about the entity, click the entity name.
Date	The date and time at which the event occurred.
Portal User	The portal administrator or user who triggered the event. To edit the administrator or user, click their user name.
Device User	The user who triggered the event on the device. This field is relevant only for events where the origin is a device.
Details	A description of the event.
More Info	Causes may be listed here.

Table 16: Log Levels

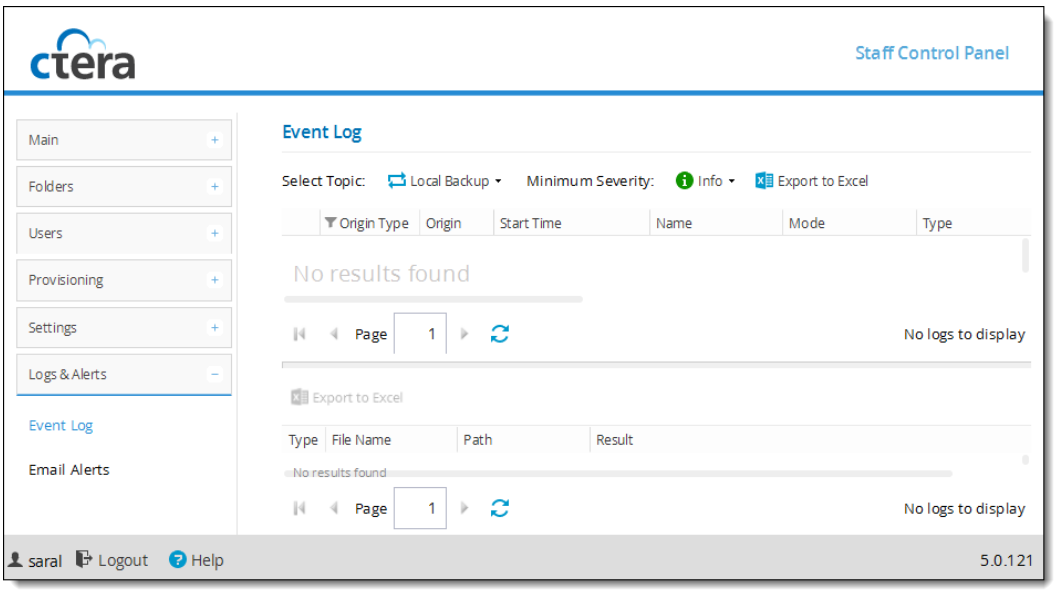
Icon	Log Level
	Error
	Warning
	Info

Icon	Log Level
	Debug

Viewing Local Backup Logs

To view Local Backup logs

1. Browse to **Logs & Alerts > Event Log**.
2. In the **Select Topic** drop-down list, select **Local Backup**.



3. To view files for which errors occurred during a synchronization operation, click on the desired operation in the upper pane.

   Information about files for which errors occurred appears in the lower pane.

The following information is displayed.

Table 17: Local Backup Log Upper Pane Fields

This field...	Displays...
Type	An icon indicating the log level. See ***Log Levels*** (page 228).
Origin Type	The type of entity sent the event log (a virtual portal or a device).
Origin	The entity that sent the event log. To edit or view details about the entity, click the entity name.
Start Time	The date and time at which the synchronization operation started.
Name	The name of the sync rule.
Mode	The operation mode, **Backup** or **Restore**.
Type	The type of synchronization, **manual** or **scheduled**.
Level	The synchronization level, **Files** or **Sync**.
Duration	The amount of time the synchronization operation took.
Result	The result of the synchronization operation.
Files	The number of files to be backed up.
Size	The total size of the files to be backed up.
Transferred Files	The number of files transferred to cloud storage during the backup operation.
Transferred Size	The size of the files transferred to cloud storage during the backup operation.
Changed Files	The number of files that changed since the last backup operation.
Changed Size	The total size of the files that changed since the last backup operation.
More Info	Additional information about the event.

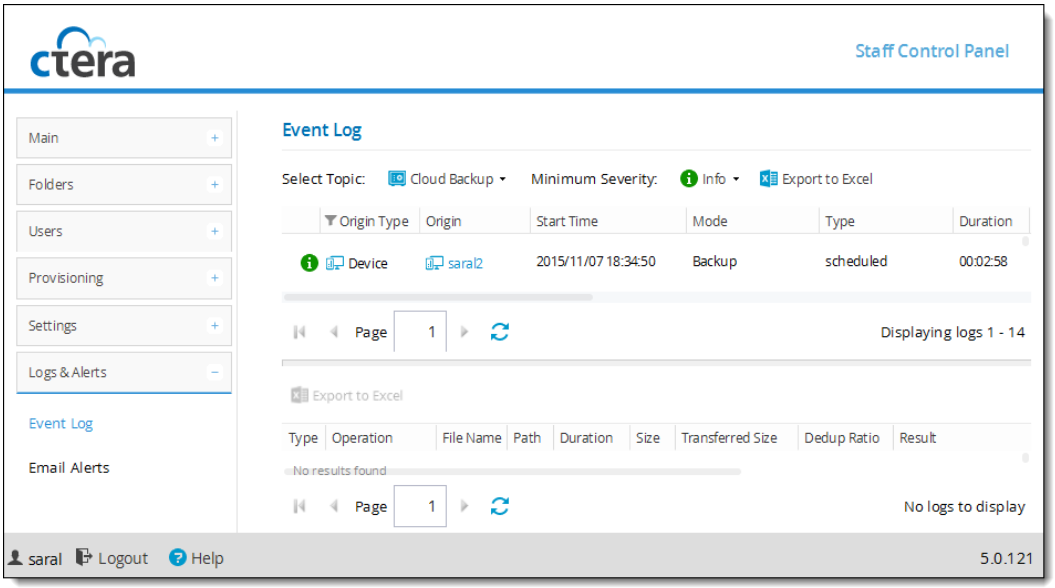
Table 18: Local Backup Log Lower Pane Fields

This field...	Displays...
Type	An icon indicating that an error occurred during synchronization.
File Name	The name of the file for which an error occurred.
Path	The path to the file.
Result	The result of the synchronization operation.

Viewing Cloud Backup Logs

To View Cloud Backup logs

1. Browse to **Logs & Alerts > Event Log**.
2. In the **Select Topic** drop-down list, select **Cloud Backup**.



3. To view additional logging information for a backup operation, click on the desired operation in the upper pane.

   Information about files included in the backup operation appears in the lower pane.

The following information is displayed.

Table 19: Cloud Backup Log Upper Pane Fields

This field...	Displays...
Type	An icon indicating the log level. See ***Log Levels*** (page 228).
Origin Type	The type of entity that sent the event log (a virtual portal or a device).
Origin	The entity that sent the event log. To edit or view details about the entity, click the entity name.
Start Time	The date and time at which the backup operation started.
Mode	The operation mode, **Backup** or **Restore**.
Type	The type of backup, **manual** or **scheduled**.
Duration	The amount of time the backup operation took.
Result	The result of the backup operation.
Files	The number of files to be backed up.
Size	The total size of the files to be backed up.
Transferred Files	The number of files transferred to cloud storage during the backup operation.
Transferred Size	The size of the files transferred to cloud storage during the backup operation.
Changed Files	The number of files that changed since the last backup operation.
Changed Size	The total size of the files that changed since the last backup operation.
More Info	Additional information about the event.

Table 20: Cloud Backup Log Lower Pane Fields

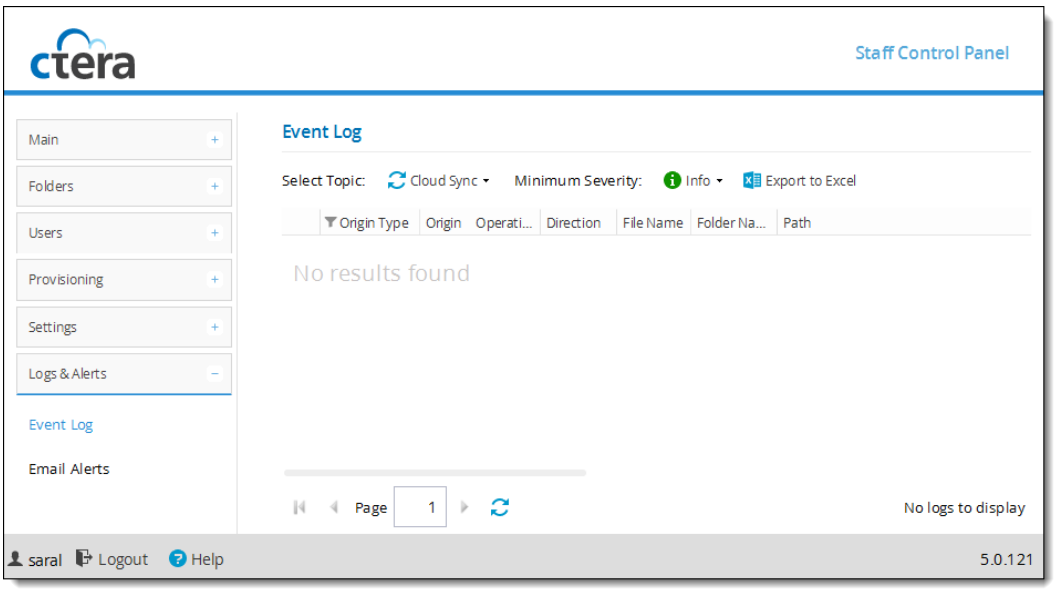
This field...	Displays...
Type	An icon indicating whether backup was successful or not.
Operation	The operation performed (**create**, **delete**, **modify**, or **rename**).
File Name	The name of the backed up file.
Path	The path to the backed up file.
Duration	The amount of time backup took for the file.
Size	The size of the file.
Transferred Size	The size of the file transferred to cloud storage.

This field...	Displays...
Dedup Ratio	The de-duplication ratio for the file.
Result	The result of the backup operation.

Viewing Cloud Sync Logs

To view Cloud Sync logs

1. Browser to **Logs & Alerts > Event Log**.
2. In the **Select Topic** drop-down list, select **Cloud Sync**.



The following information is displayed.

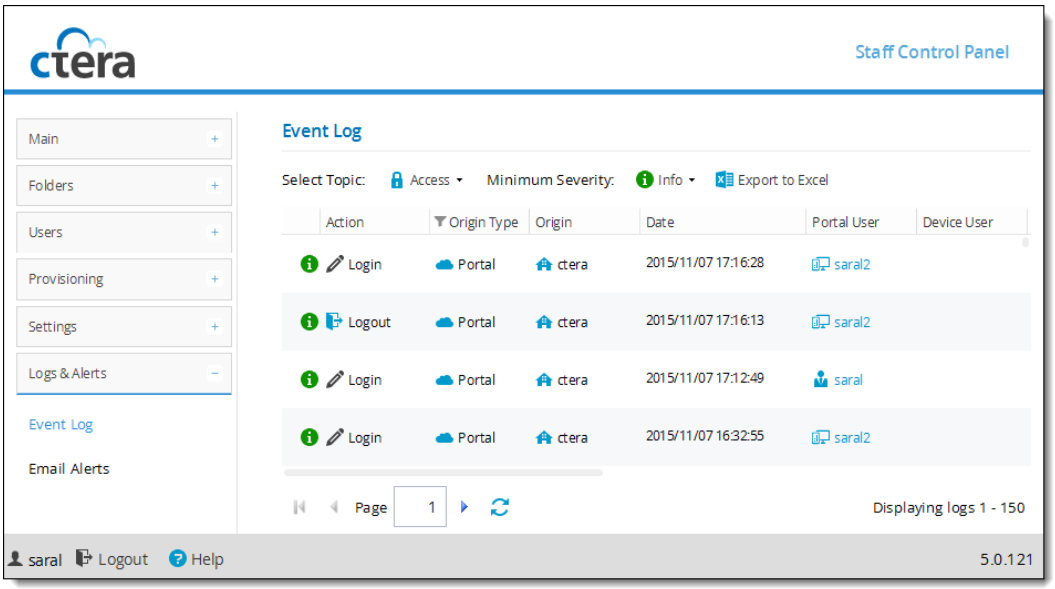
Table 21: Cloud Sync Log Fields

This field...	Displays...
Type	An icon indicating the log level. See ***Log Levels*** (page 228).
Origin Type	The type of entity sent the event log (a virtual portal or a device).
Origin	The entity that sent the event log. To edit or view details about the entity, click the entity name.
Operation	The synchronization operation performed: **New**. A new file or directory was created. **Updated**. A file or directory was updated.
Direction	The synchronization operation's direction: **In**. From the cloud drive to the local drive. **Out**. From the local drive to the cloud drive.
File Name	The name of the file transferred during the synchronization operation.
Folder Name	The name of a folder containing the file transferred during the synchronization operation.
Path	The path to the file transferred during the synchronization operation.
Start Time	The date and time at which the synchronization operation started.
Duration	The amount of time the synchronization operation took.
Size	The size of the synchronized file.
Transferred Size	The actual amount of data transferred.
Dedup Ratio	The de-duplication ratio for the file transferred during the synchronization operation.
Result	The result of the synchronization operation.

Viewing Access Logs

To view Access logs

1. Browse to **Logs & Alerts > Event Log**.
2. In the **Select Topic** drop-down list, select **Access**.



The following information is displayed:

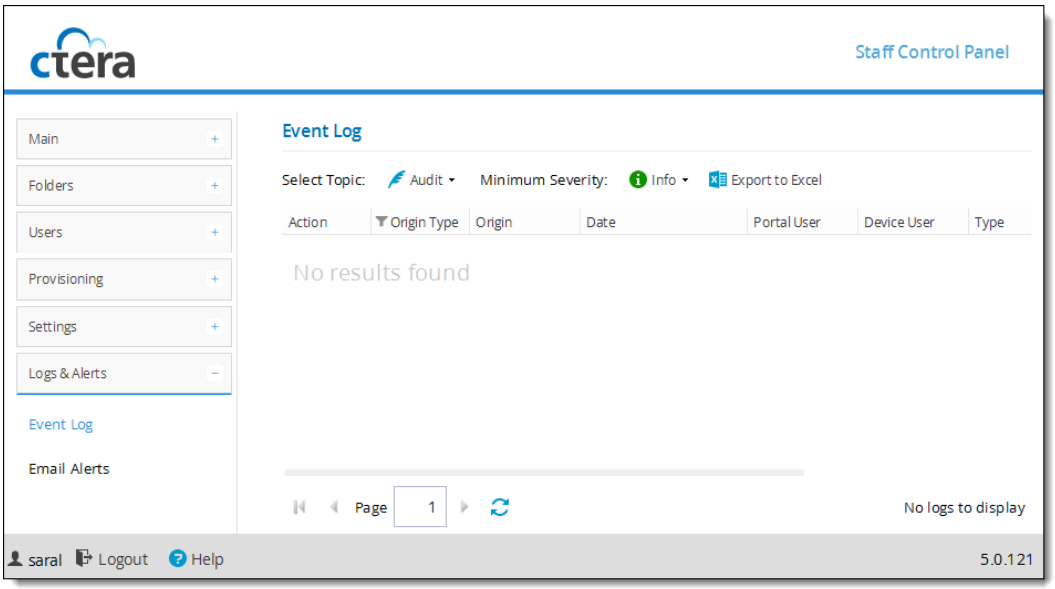
Table 22: Access Log Fields

This field...	Displays...
Type	An icon indicating the log level. See ***Log Levels*** (page 228).
Action	The action type (**login**, **logout**, **rename** ...)
Origin Type	The type of entity sent the event log (the portal or a device).
Origin	The entity that sent the event log. To edit or view details about the entity, click the entity name.
Date	The date and time at which the event occurred.
Portal User	The portal administrator or user who triggered the event. To edit the administrator or user, click their user name.
Device User	The user who triggered the event on the device. This field is relevant only for events where the origin is a device.
Protocol	The protocol used when triggering the event: GUI CIFS (Windows File Sharing) AFP FTP NFS RSync CTERA Agent WebDAV
Details	A description of the event.
Client IP	The IP address from which the user triggered the event.
Target	The entity on which the action was performed.
More Info	Additional information about the event.

Viewing Audit Logs

To view Audit logs

1. Browse to **Logs & Alerts > Event Log**.
2. In the **Select Topic** drop-down list, select **Audit**.



The following information is displayed:

Table 23: Audit Log Fields

This field...	Displays...
Action	The action type. See ***Action Types*** (page 238).
Origin Type	The type of entity sent the event log (a virtual portal or a device).
Origin	The entity that sent the event log. To edit or view details about the entity, click the entity name.
Date	The date and time at which the event occurred.
Portal User	The portal administrator or user who triggered the event. To edit the administrator or user, click their user name.
Device User	The user who triggered the event on the device. This field is relevant only for events where the origin is a device.
Type	The type of setting that was affected by the action. For example, if CTERA Portal administrator JohnS was deleted, this column displays "PortalAdmin".
Target	The object that was affected by the action. For example, if user JohnS was deleted, this column displays "JohnS".
More Info	Additional information about the event.

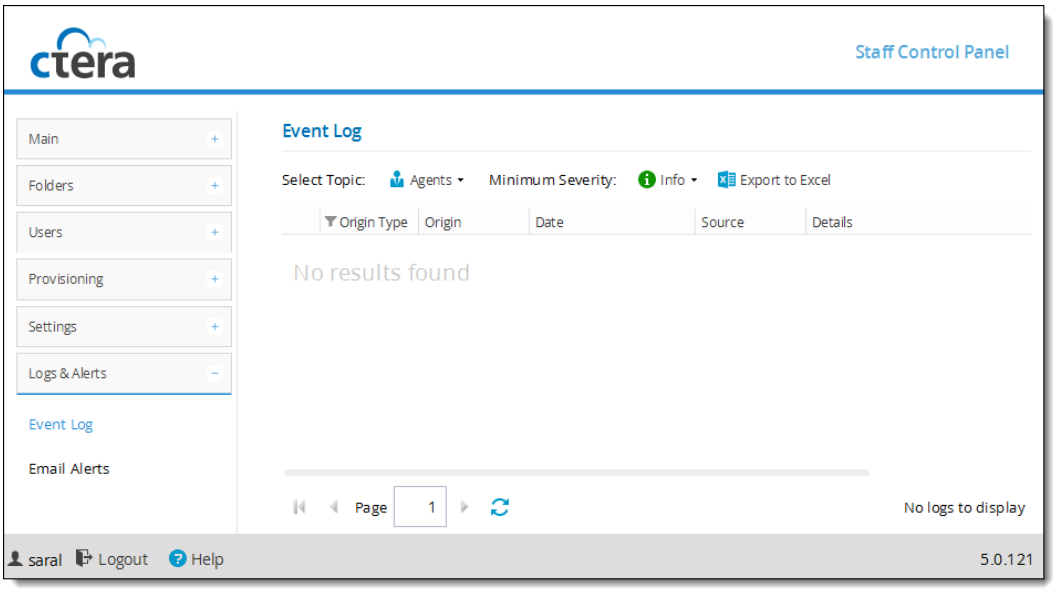
Table 24: Action Types

Icon	Label	Description
	Added	An object was added to the CTERA Portal.
	Deleted	An object was deleted from the CTERA Portal.
	Modified	An object was modified.
	Formatted	A disk was formatted.
	Disabled	A setting was disabled.
	Enabled	A setting was enabled.

Viewing Agent Logs

To view Agents logs

1. Browse to **Logs & Alerts > Event Log**.
2. In the **Select Topic** drop-down list, select **Agents**.



The following information is displayed:

Table 25: CTERA Agents Log Fields

This field...	Displays...
Type	An icon indicating the log level. See ***Log Levels*** (page 228).
Origin Type	The type of entity sent the event log (a virtual portal or a device).
Origin	The entity that sent the event log. To edit or view details about the entity, click the entity name.
Date	The date and time at which the event occurred.
Source	The name of the CTERA Agent-installed computer that triggered the event.
Details	A description of the event.
More Info	Additional information about the event.

Exporting Logs to Excel

You can export logs to a CSV file that can be opened in Microsoft Excel.

To export logs

1. View the desired log category.
2. Click **Export to Excel**.

   The logs in the current log category are exported to a CSV file.

19

Using Email Alerts

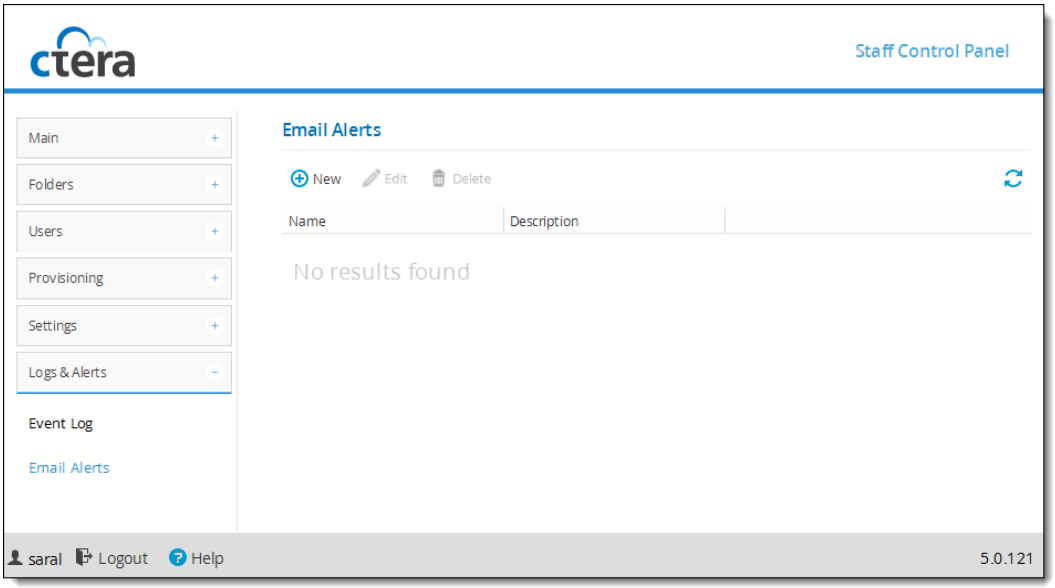
You can configure the CTERA Portal to automatically send email alerts to end users and administrators upon certain CTERA Portal log messages.

In This Chapter

Adding and Editing Email Alerts

To add or edit an email alert

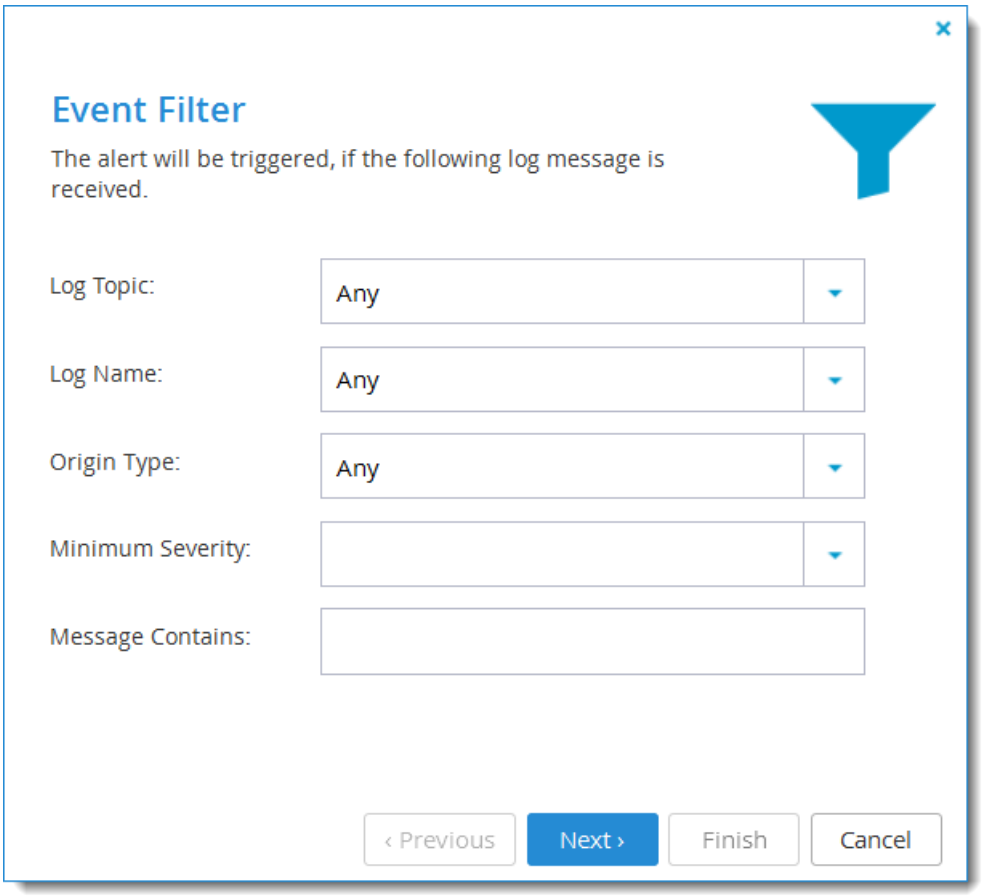
1. Browse to **Logs & Alerts > Email Alerts**.



2. Do one of the following:

   - To add a new email alert, click **New**.
   - To edit an existing email alert, select the email alert's row and click **Edit**.

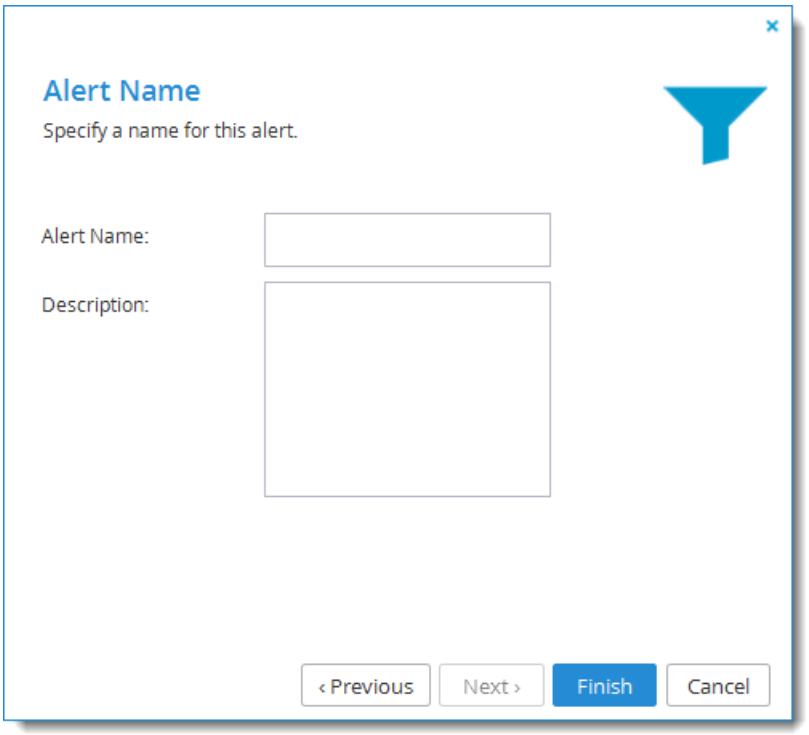
The **Alert Rule Wizard** opens displaying the **Event Filter** dialog box.



3 Complete the fields using the information in the following table.

4 Click **Next**.

The **Alert Name** dialog box appears.



5 In the **Alert Name** field, type a name for the email alert.

6 In the **Description** field, type a description of the email alert.

7 Click **Finish**.

Table 26: Alert Rule Event Filter Fields

In this field...	Do this...
Log Topic	Select the category of logs that should trigger the email alert. For an explanation of the log categories, see ***Viewing Logs*** (on page 227). Alternatively, select **Any** to specify that any log category can trigger the email alert.
Log Name	Select the name of the log that should trigger the email alert. Alternatively, select **Any** to specify that any log can trigger the email alert.
Origin Type	Select the entity from which a log must originate in order to trigger the email alert. Alternatively, select **Any** to specify that any log can originate from any entity in order to trigger the email alert.
Minimum Severity	Select the minimum severity a log must have in order to trigger the email alert. For an explanation of the log severities, see ***Log Levels*** (page 228).
Message Contains	Type the text that the log message must contain in order to trigger the email alert.

Viewing Email Alerts

To view all email alerts

Select **Logs & Alerts > Email Alerts** from the menu.

The **Logs & Alerts > Email Alerts** page displays all email alerts.

The table includes the following columns.

Table 27: Email Alert Fields

This field...	Displays...
Name	The email alert's name. To edit the email alert, click the alert's name.
Description	A description of the email alert.

Deleting Email Alerts

To delete an email alert

1. Select the email alert's row.
2. Click **Delete.**
3. Click **Yes** to confirm.

   The email alert is deleted.

Index

D

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V

W