your files.
your cloud.

ADMINISTRATOR GUIDE

Team Portal

October 2016

Version 5.5

Copyright © 2009-2016 CTERA Networks Ltd.

All rights reserved. No part of this document may be reproduced in any form or by any means without written permission from CTERA Networks Ltd.

Information in this document is subject to change without notice and does not represent a commitment on the part of CTERA Networks Ltd.

CTERA, C200, C400, C800, C800+, Virtual Gateway, P1200, CloudPlug, NEXT3, Cloud Attached Storage, and Virtual Cloud Drive are trademarks, service marks, or registered trademarks of CTERA Networks Ltd.

All other product names mentioned herein are trademarks or registered trademarks of their respective owners.

The products described in this document are protected by U.S. patents, foreign patents, or pending applications.

Note: For legal information and for the end user license agreement, refer to Legal Information at the end of this guide.

CONTENTS

About CTERA Portal 8
Management Features 8
Storage Devices 9
CTERA Cloud Storage Gateways 9
CTERA Agents 9
CTERA Mobile 10
Getting Started 11
Browser Requirements 11
Logging In To the Global Administration Interface 11
Managing Devices 13
Viewing All Devices 13
Viewing Individual Devices' Statuses 14
Viewing Individual Devices' Backup Status 16
Viewing Individual Cloud Storage Gateway's Storage Status 18
Managing Cloud Drive Synchronization 20
Editing Device Settings 21
Remotely Managing Devices 23
Remotely Performing Cloud Backup Operations on Devices 25
Manually Starting Cloud Backup 25
Canceling the Current Cloud Backup 25
Suspending the Cloud Backup Service 26
Resuming the Cloud Backup Service 26
Exporting Devices to Excel 26
Remote Wiping Mobile Devices 26
Deleting Devices 27
Viewing Reports 28
Viewing the Folders Report 28
Viewing the Folder Groups Report 29
Viewing the Devices Report 31
Viewing the Plans Report 32
Exporting Reports to Excel 33

Managing Folders **34**
Viewing Cloud Drive Folders 34
Viewing Backup Folders 35
Creating New Cloud Drive Folders 37
Creating New Backup Folders 38
Editing Cloud Drive Folders 39
Editing Backup Folders 40
Viewing Folder Contents 40
Changing Passphrases for Accessing Backup Folder Contents 41
Exporting Folders to Excel 43
Deleting Folders 43
Managing Folder Groups **44**
Changing a User's Deduplication Level 45
Changing the Default Deduplication Level 47
Viewing Folder Groups 48
Adding and Editing Folder Groups 48
Managing Cloud Drive Folders for Folder Groups 51
Managing Backup Folders for Folder Groups 52
Changing Passphrases for Accessing Folder Group Contents 53
Exporting Folder Groups to Excel 54
Deleting Folder Groups 54
Managing User Accounts **55**
Inviting Users to Register 55
Viewing User Accounts 57
Filtering the Users Page 58
Adding New Users 58
Editing User Profiles 60
Enabling/Disabling User Accounts 61
Adding Users to Groups 62
Provisioning User Accounts in Team Portals 64
Assigning User Accounts to Subscription Plans 64
Terminating User Accounts 66
Configuring a User's Deduplication Settings 66
Viewing User Account Details 68
Generating Monthly Reports 69
Managing a User's Devices 69

Managing a User's Cloud Drive Folders 70
Managing a User's Folder Groups 70
Configuring User Alerts (Administrators Only) 71
Exporting User Accounts to Excel 71
Applying Provisioning Changes 72
Deleting User Accounts 72
Customizing Administrator Roles 72

Configuring Single Sign On 76

Managing User Groups 79

Viewing User Groups 79
Filtering the User Groups Page 80
Adding and Editing User Groups 80
Configuring User Group Members 81
Deleting User Groups 83

Using Directory Services 84

How Directory Service Synchronization Works 84
Integrating CTERA Portal with an Active Directory Domain, Tree, or Forest 85
Integrating CTERA Portal with an LDAP Directory Server 91
Integrating CTERA Portal with an Apple Open Directory Server 94
Manually Fetching User Data 96

Provisioning 98

Overview 98
Plans 98
Snapshot Retention Policies 98
Viewing Plans 101
Adding and Editing Plans 102
Setting/Removing the Default Plan 106
Automatically Assigning Plans 107
Exporting Subscription Plans to Excel 109
Applying Provisioning Changes 109
Deleting Subscription Plans 109

Content Protection **110**
Cloud Drive Policy 110
Collaboration Policy 112
Collaboration Policy Example 115
Collaboration Permissions 115
Collaboration Permissions Example 117
Configuring Virtual Portal Settings **118**
Changing the Settings 119
Password Policy 119
Support Settings 121
App Stores URL Settings 121
General Settings 122
User Registration Settings 122
Team Portal Settings 123
Default Settings for New Folder Groups 123
Default Settings for New User 125
Cloud Drive Settings 126
Public Links 126
Collaboration 127
Remote Access Settings 128
Advanced 128
Managing Device Configuration Templates **130**
Viewing Device Configuration Templates 131
Adding and Editing Device Configuration Templates 131
Backup and Exclude Sets 132
Adding Backup and Exclude Sets 133
Modifying Backup and Exclude Sets 139
Selecting Applications for Backup 140
Cloud Backup Schedule 142
Backup Throughput 144
CTERA Agent Scripts 146
Cloud Drive Synchronization 148
Managing Sync Throughput 153
Marking a Firmware Image as the Current Firmware Image 155

Configuring Automatic Firmware Updates 157
Configuring the Automatic Template Assignment Policy 159
Setting the Default Device Configuration Template 161
Duplicating Configuration Templates 161
Deleting Device Configuration Templates 162

Notifications 164

The Notifications Dashboard 164
Configuring Notification Settings 165

Configuring Email Templates 166

Customizing Email Notification Templates 166
Email Notification Templates 169

Viewing Logs 172

Viewing System Logs 172
Viewing Local Backup Logs 174
Viewing Cloud Backup Logs 175
Viewing Cloud Sync Logs 177
Viewing Access Logs 179
Viewing Audit Logs 180
Viewing Agent Logs 182
Exporting Logs to Excel 183

Using Email Alerts 184

Viewing Email Alerts 184
Adding and Editing Email Alerts 185
Deleting Email Alerts 188

Legal Information 189

1

ABOUT 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 Storage Gateways, CTERA Agents, and CTERA Mobile. 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 deduplication 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 storage gateways and endpoint 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 storage gateways of various types and sizes as well as individual endpoint 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
- Storage Devices

MANAGEMENT FEATURES

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

- **Service Provisioning**
  Create customer subscription plans that include cloud storage volume, number of devices per account, snapshot retention policy, and time limits.
- **User Management**
  Manage anywhere from tens to hundreds of thousands of subscribers. Control user access, subscription plans, and view real-time storage usage and account status.
- **Remote Device Management and Monitoring**
  Manage CTERA cloud storage 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.
  Branding is not described in this user guide. Contact CTERA to find out how to rebrand.

STORAGE DEVICES

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 devices:

- CTERA Cloud Storage Gateways
- CTERA Agents
- CTERA Mobile

Throughout this guide, the term *device* refers generically to a CTERA Cloud Storage Gateway, CTERA Agent, or CTERA Mobile.

CTERA Cloud Storage Gateways

CTERA's cloud storage 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 enterprise branches, SMBs and remote offices, CTERA's cloud storage gateways can replace legacy file servers and tape backup in a single solution with significant cost savings.

The cloud storage gateways feature a full set of Network Attached Storage (NAS) capabilities and comprehensive backup and sync and share functionalities, 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 Storage Gateways are managed remotely by CTERA Portal. Template-based management and remote firmware upgrades make it possible to manage numerous cloud storage gateways while maintaining minimal on-site IT and reducing total cost of ownership.

CTERA Cloud Storage Gateways comprise the CTERA C200, C400, C800, and C800+ physical appliances and the Virtual Cloud Storage Gateway (Virtual Gateway).

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 storage gateway.

CTERA Agents are available for Windows, Mac and Linux 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 storage 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 is an Enterprise File Sync and Share (EFSS) app that 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 create and/or update MS Office files online, upload files, such as photos and documents, all directly from their mobile device to their cloud drive.

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 and synced content.

2

GETTING STARTED

This chapter contains all the information you need in order to get started using the CTERA Portal.

In this chapter

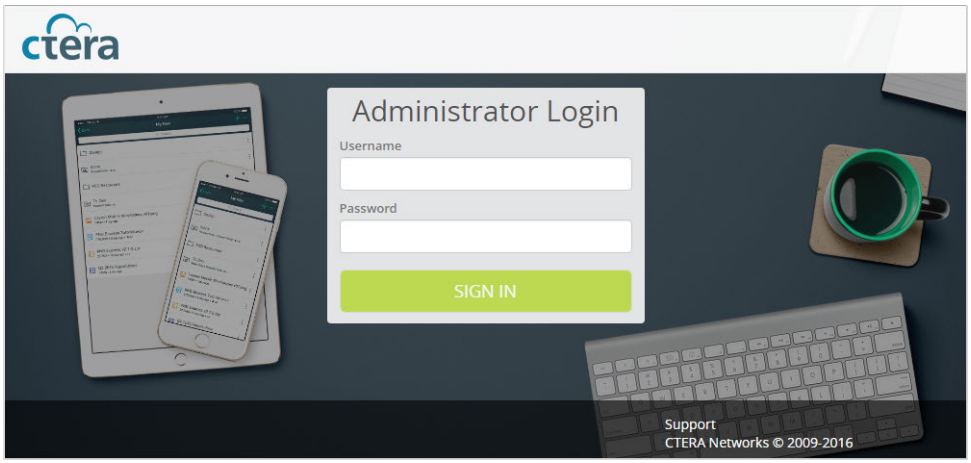
- Browser Requirements
- Logging In To the Global Administration Interface

BROWSER REQUIREMENTS

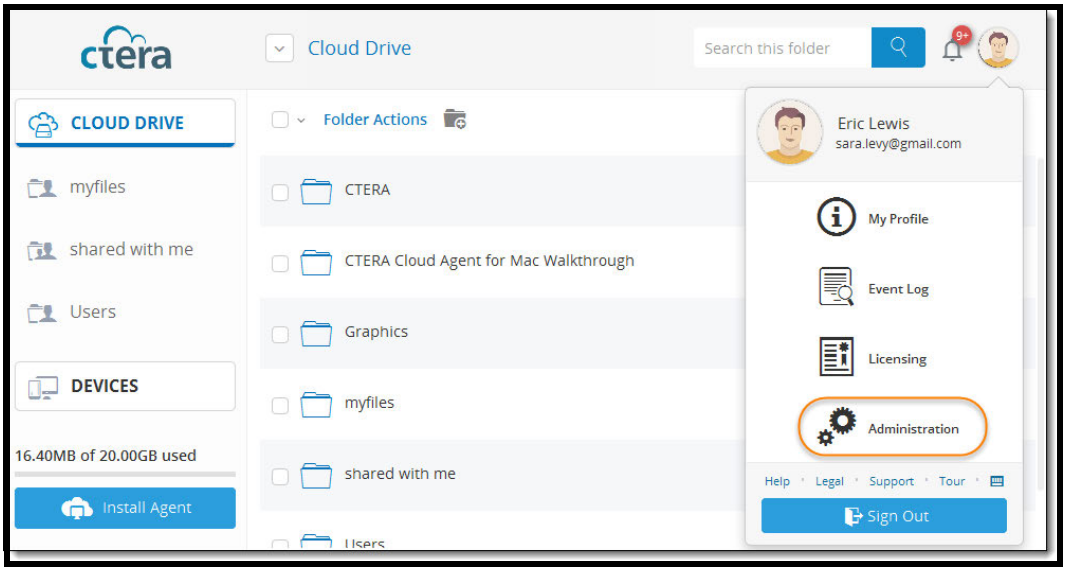
In order to use the CTERA Portal, you will need one of the following internet browsers:

- Microsoft Internet Explorer 11.0 or later
- Mozilla Firefox. The two latest versions are supported.
- Apple Safari. The two latest versions are supported.
- Google Chrome. The two latest versions are supported.
- Microsoft Edge. Certain functions are not available due to browser limitations.

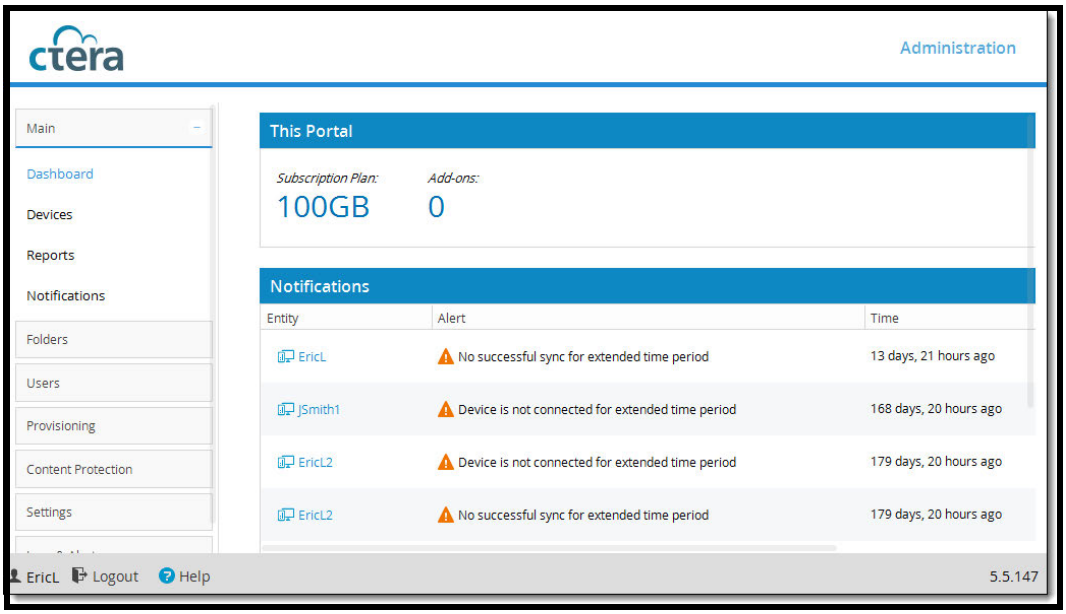
LOGGING IN TO THE GLOBAL ADMINISTRATION INTERFACE



1 From your team portal admin account, click your avatar at the top right (or your initials, if you have not yet configured an avatar) and select **Administration**.



2 The Team Portal Administration interface is displayed.



3

MANAGING DEVICES

The word *device* refers to a CTERA Cloud Storage Gateway, CTERA Agent, or CTERA Mobile connected to the CTERA Portal. Devices are automatically added to the CTERA Portal, when their owners connect their CTERA Cloud Storage Gateways, CTERA Agents, or CTERA Mobiles to the CTERA Portal.

In this chapter

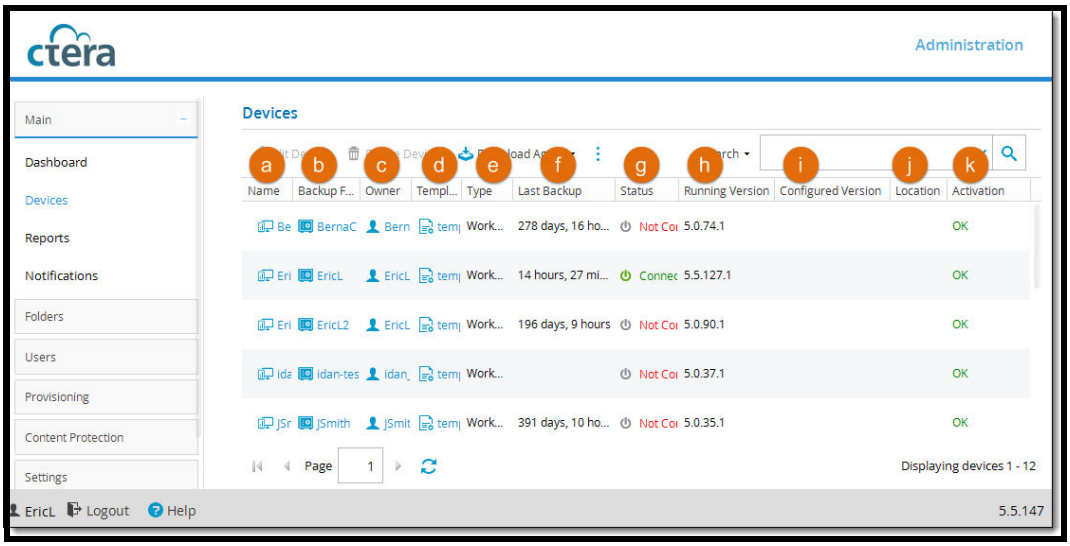
- Viewing All Devices
- Viewing Individual Devices' Statuses
- Viewing Individual Devices' Backup Status
- Viewing Individual Cloud Storage Gateway's Storage Status
- Managing Cloud Drive Synchronization
- Editing Device Settings
- Remotely Managing Devices
- Remotely Performing Cloud Backup Operations on Devices
- Exporting Devices to Excel
- Remote Wiping Mobile Devices
- Deleting Devices

VIEWING ALL DEVICES

To view all devices connected to :

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

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



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 and Viewing Individual Devices' Statuses.

b **Backup Folder**. The device's backup folder.
To edit the folder, click the folder name. For further details, see Creating New Cloud Drive Folders.

c **Owner**. The user account name of the device's owner.
To edit the user account, click the user account name.Adding New Users
Note: When viewing devices in the User Account Manager, this column does not appear.

d **Template**. The 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 **Portal**. The virtual portal in which the device is defined.

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

j **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.

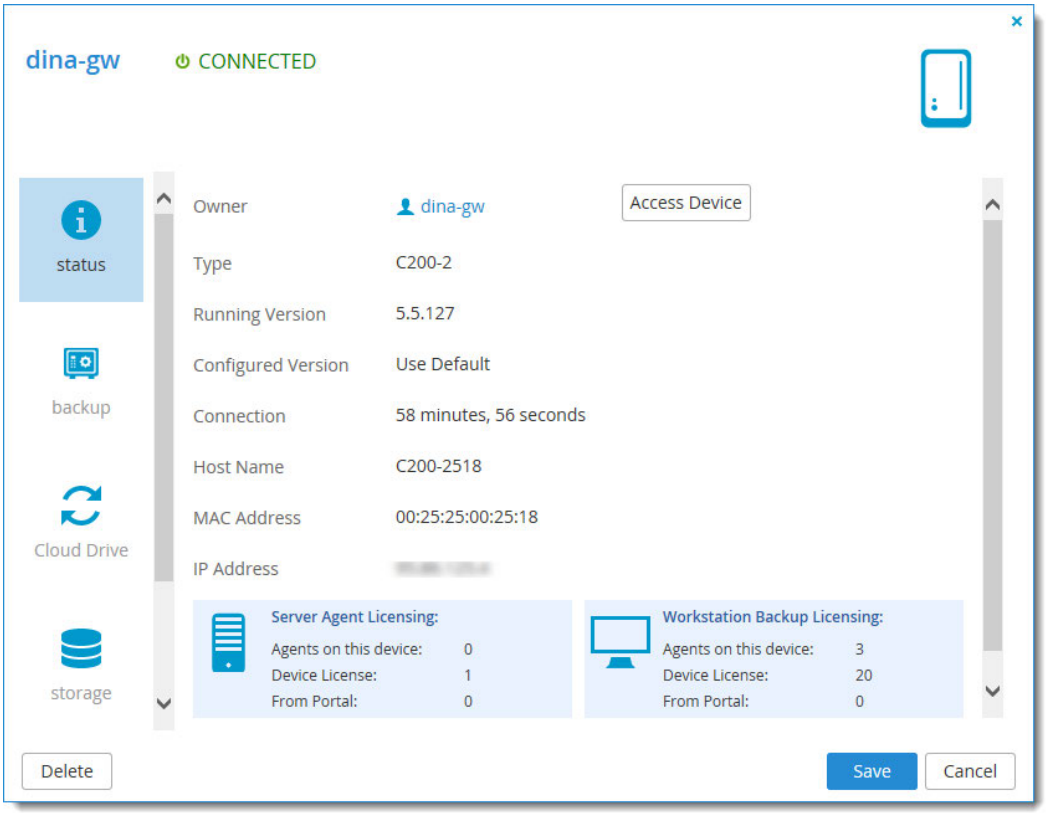
k **Location**. The device's location.

l **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:

- 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:

This field...	Displays...
Cloud backup service licensing status	Shows whether the cloud backup service is licensed. This status is displayed only if the device is a CTERA Agent.
Disable Cloud Backup (button)	Click to disable the cloud backup service for this agent. Disabling the cloud backup service on a device frees up the cloud backup license for another device.
Access Device	This button is displayed if the device is a CTERA Cloud Storage Gateway. It opens the configuration interface for the device.
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.
Type	The device type.
Running Version	The firmware version currently installed on the device.

This field...	Displays...
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.
Server Agent Licensing	This area displays information about CTERA Server Agent licensing for the device. It is only displayed if the device is a CTERA Cloud Storage 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 is only displayed if the device is a CTERA Cloud Storage Gateway.
Agents on this device	The number of workstation agents installed for the device.
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.

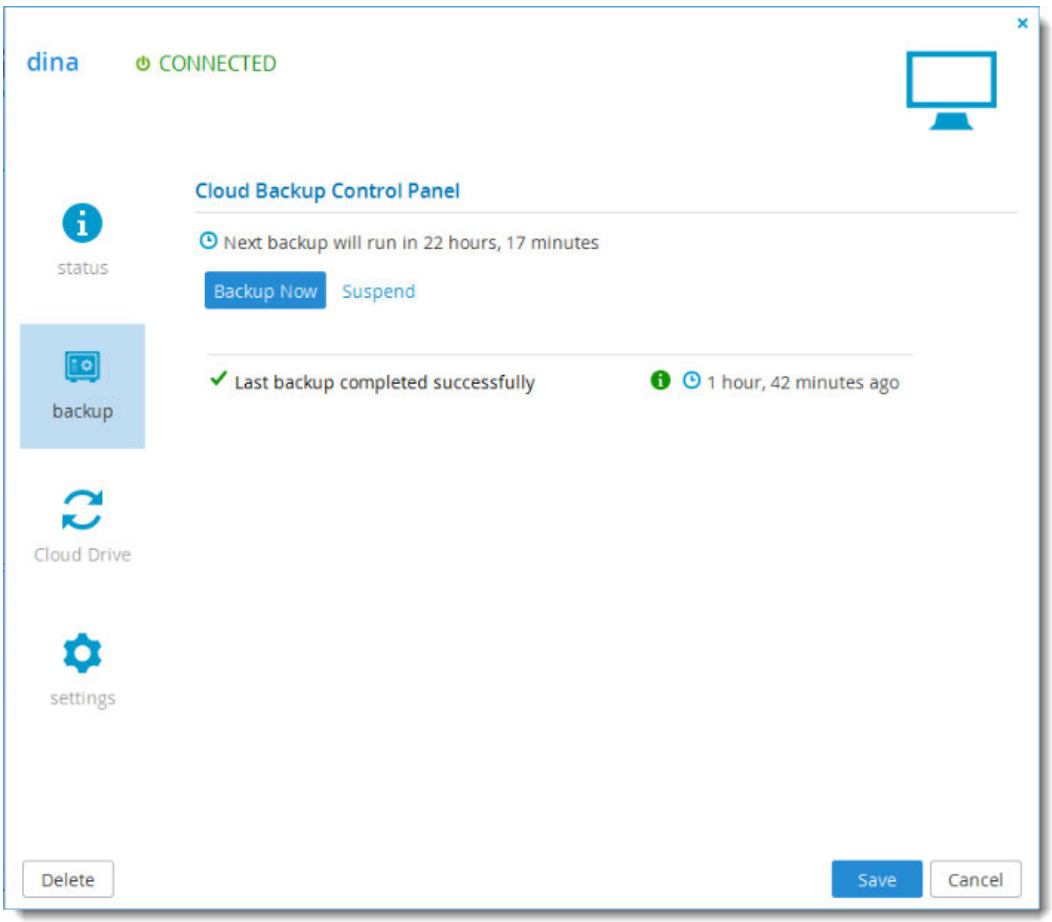
VIEWING INDIVIDUAL DEVICES' BACKUP STATUS

Note: Backup status can only be viewed if the device is connected and the Cloud Backup service is enabled on the device.

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:

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 Local Backup Logs.

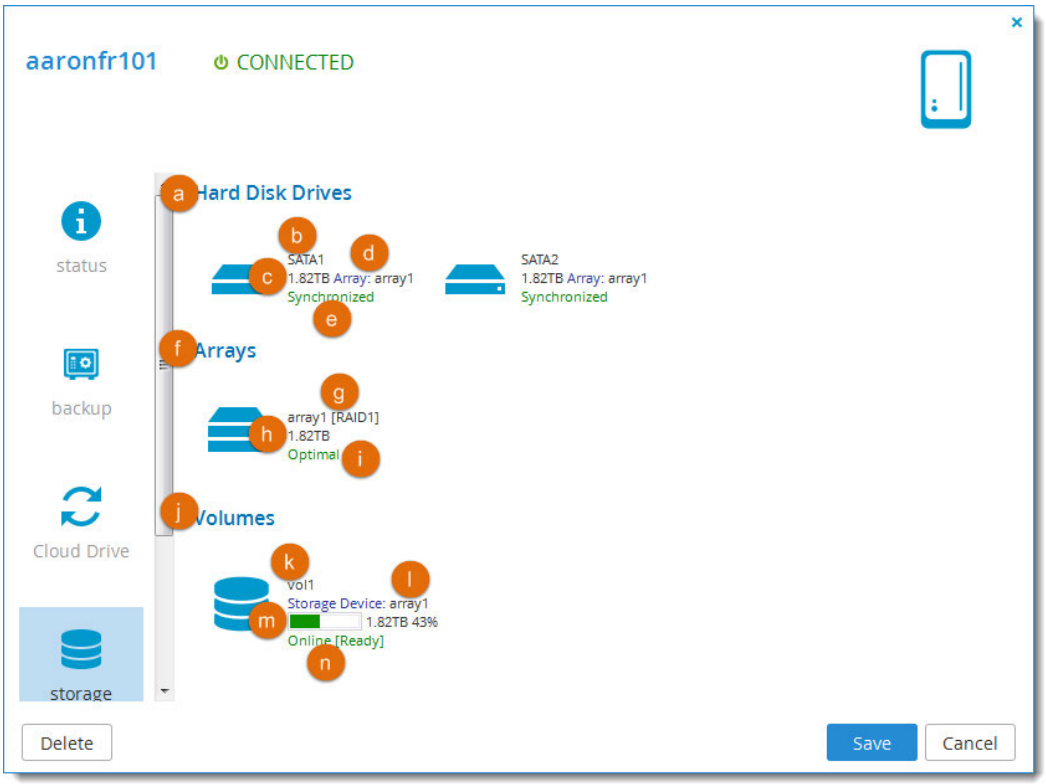
This field...	Displays...
	Mouse-over this icon to view the following information about the last backup: • The total size of the files that you selected for backup • The total number of files that you selected for backup • The amount of time the backup took
	The amount of time since the last backup ended.

VIEWING INDIVIDUAL CLOUD STORAGE GATEWAY'S STORAGE STATUS

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

To view an individual cloud storage 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.

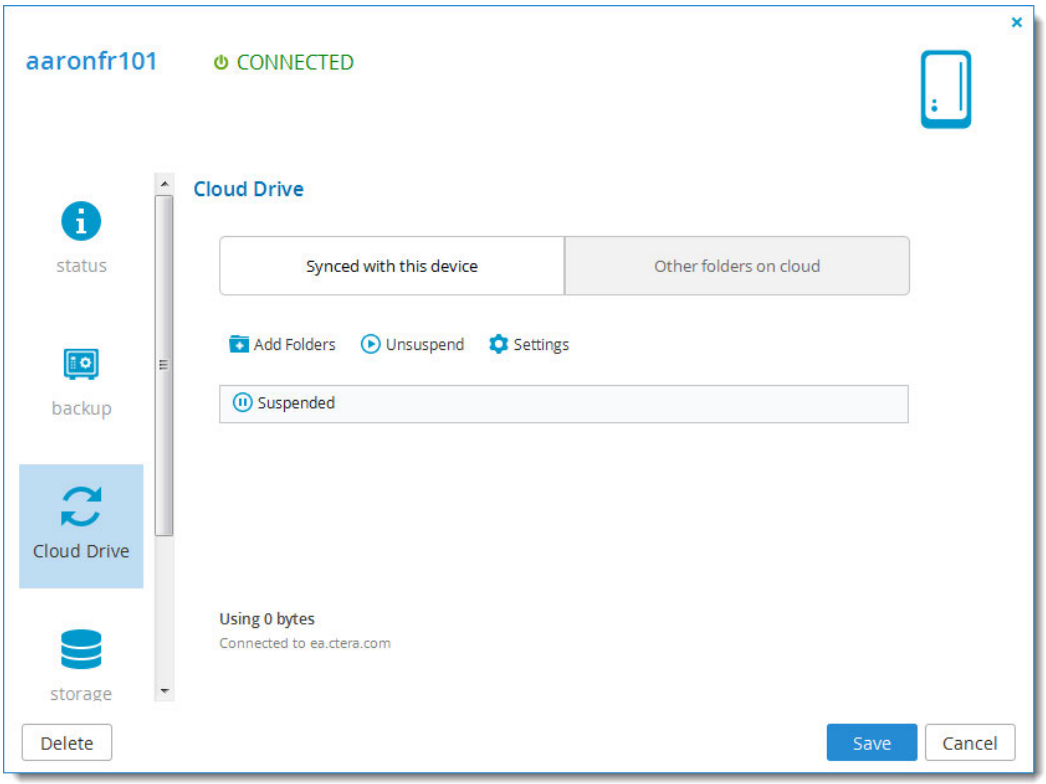
- **Mounting**. Routine cleanup is being performed after a non-clean shutdown.
- **Formatting**. The volume is being formatted.
- **Converting**. The volume is being converted (from EXT3 to NEXT3, or the opposite).
- **Resizing**. The volume is being resized.
- **Repairing**. The volume is being repaired.
- **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. This is relevant if the Cloud Drive service is enabled for the 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:

- 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
- Change the Cloud Drive operation mode: either **Classic** or **Sync Gateway**. (Relevant only for cloud storage gateways.)

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

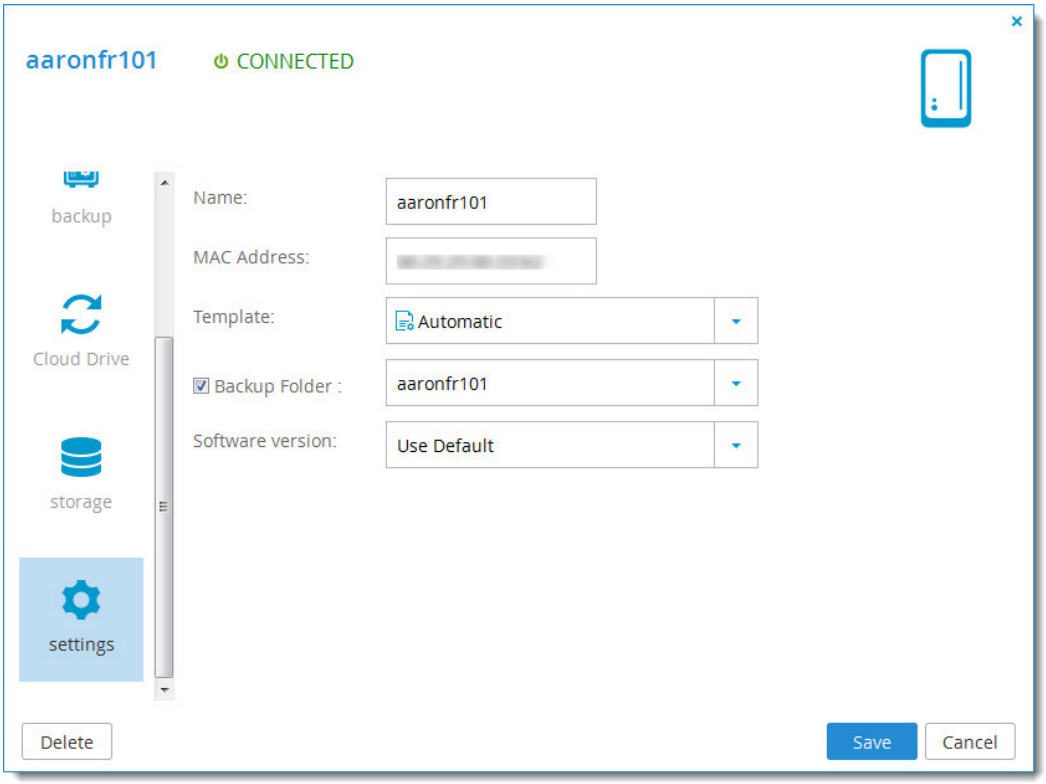
EDITING DEVICE SETTINGS

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 host name of the device. If the device has the same hostname as another portal device, a number is appended to the host name.
- **Template**
  You can specify whether the device should inherit its settings from a device configuration template. Device configuration templates are per virtual portal. To manage device configuration templates, switch to the specific virtual portal's view and go to the **Settings > Templates** page. For information on device configuration templates, see Managing Device Configuration Templates.
- **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.

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 automatic template assignment policy configured in the virtual portal. See Configuring the Automatic Template Assignment Policy. The default value is **Automatic**.

In this field...	Do this...
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.

4 Click **Save**.

REMOTELY MANAGING DEVICES

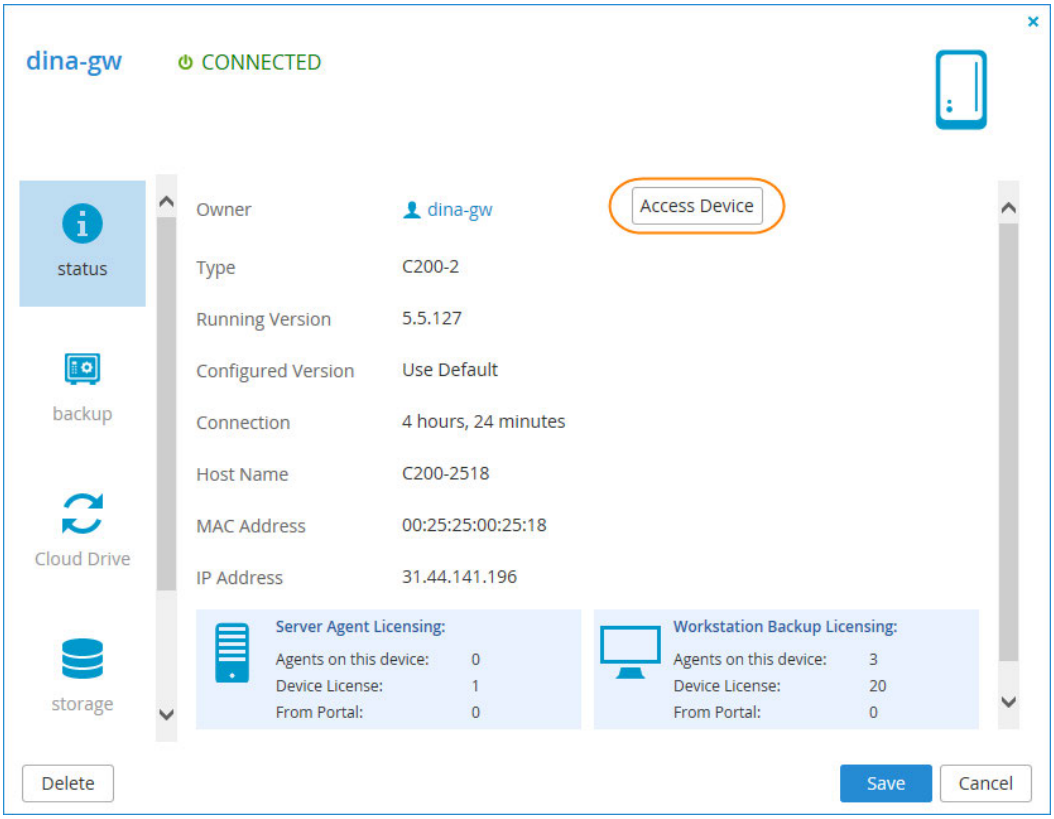
You can remotely access a device and the files on it, when the following conditions are met:

- 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.
- The device is a CTERA Cloud Storage Gateway or a CTERA Agent.

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 is displayed.
  In the fields provided, type your user name and password for accessing this device, then click **Log In**.
- The device's management Web interface is displayed. For information about managing a device, refer to the device's user guide.

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

REMOTELY PERFORMING CLOUD BACKUP OPERATIONS ON DEVICES

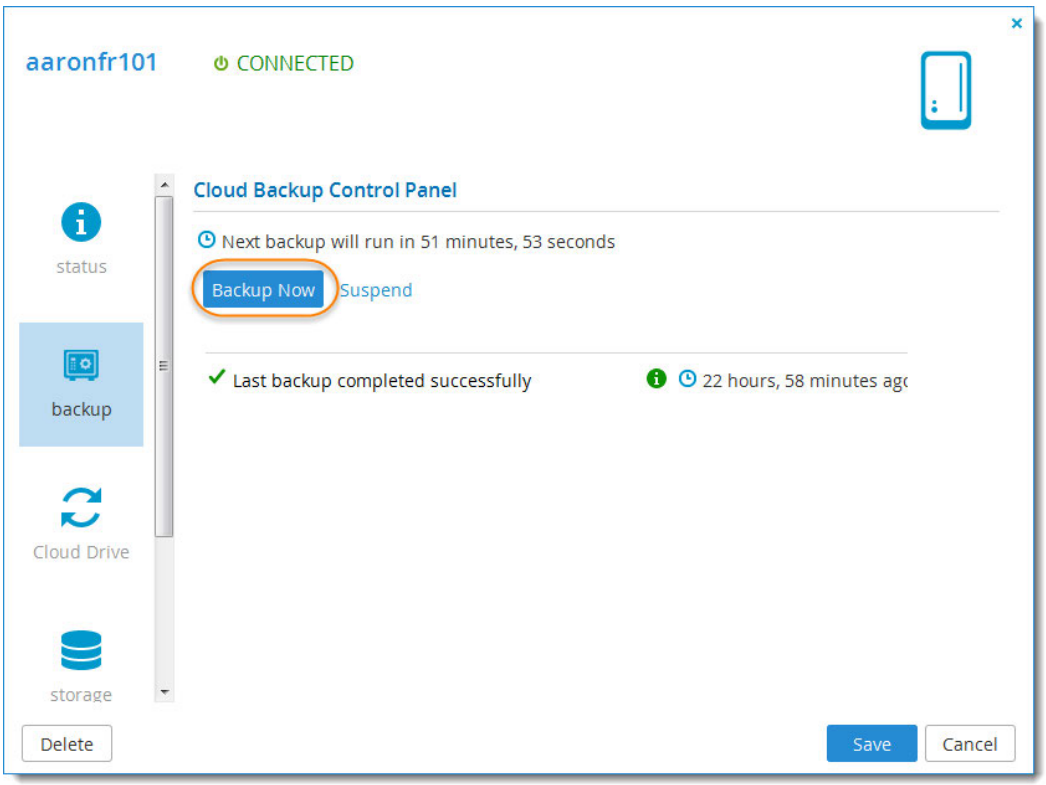
You can start, stop, suspend, or resume cloud backup directly from the Device Manager, without logging into the remote device. This is relevant for CTERA Cloud Storage Gateways and CTERA Agents and can be done if the Cloud Backup service is enabled.

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 is displayed, and the files are backed up to cloud storage.
A success message is displayed.

Canceling the Current Cloud Backup

You can cancel a running cloud backup.

Note: Only the current backup will be canceled. 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 is displayed, 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 is displayed.
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 is displayed.
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 the following global administration reports:

- Folders
- Folder Groups
- Devices
- Plans

In this chapter

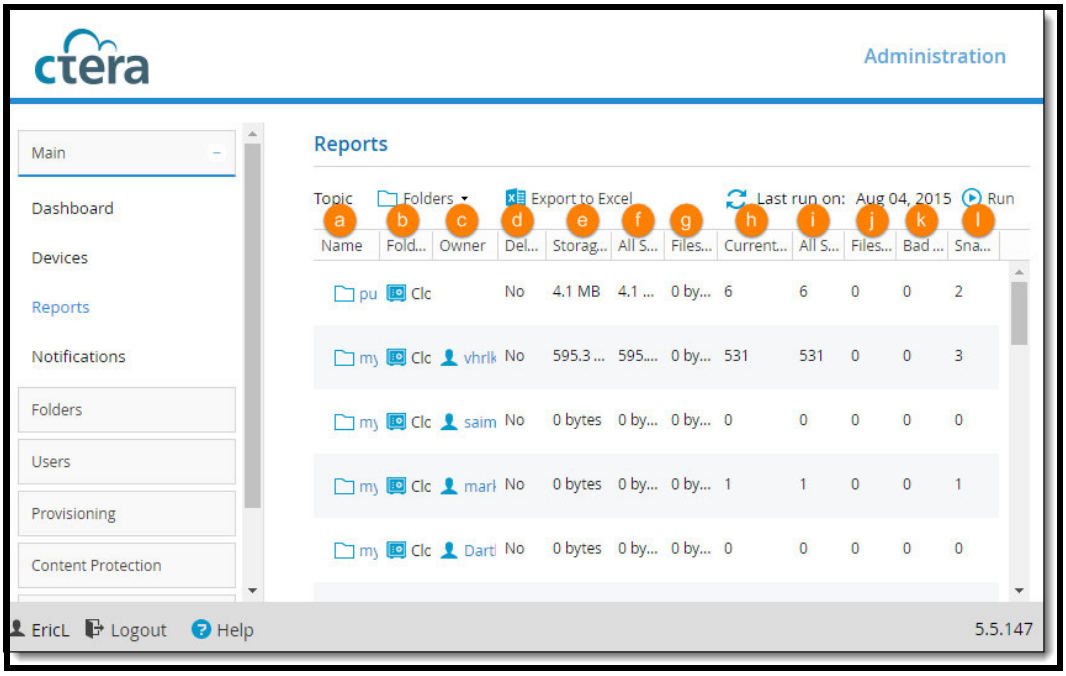
- Viewing the Folders Report
- Viewing the Folder Groups Report
- Viewing the Devices Report
- Viewing the Plans Report
- Exporting Reports to Excel

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 is displayed 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.

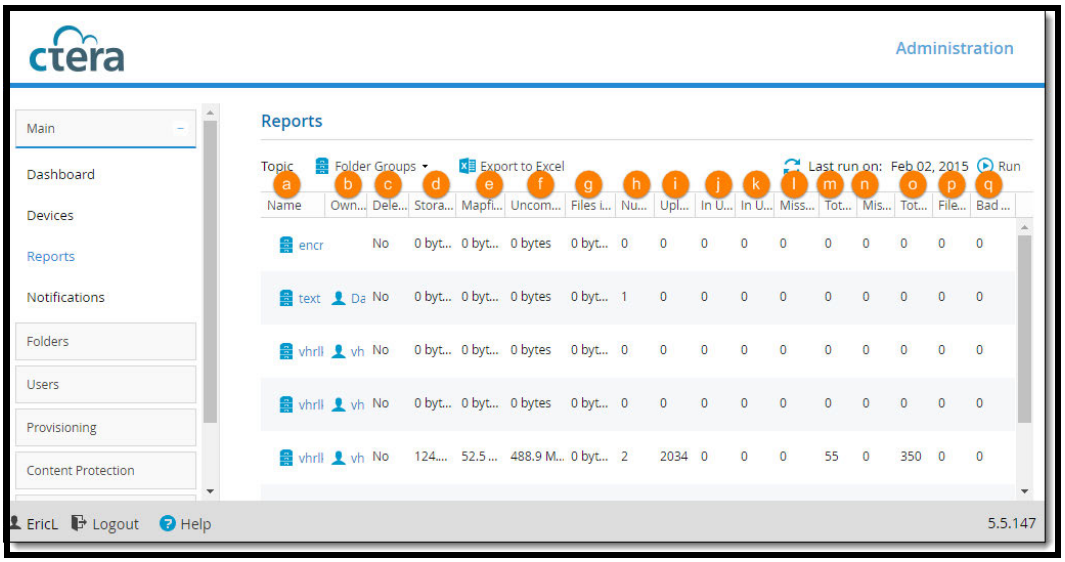
VIEWING THE FOLDER GROUPS REPORT

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 is displayed 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 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.

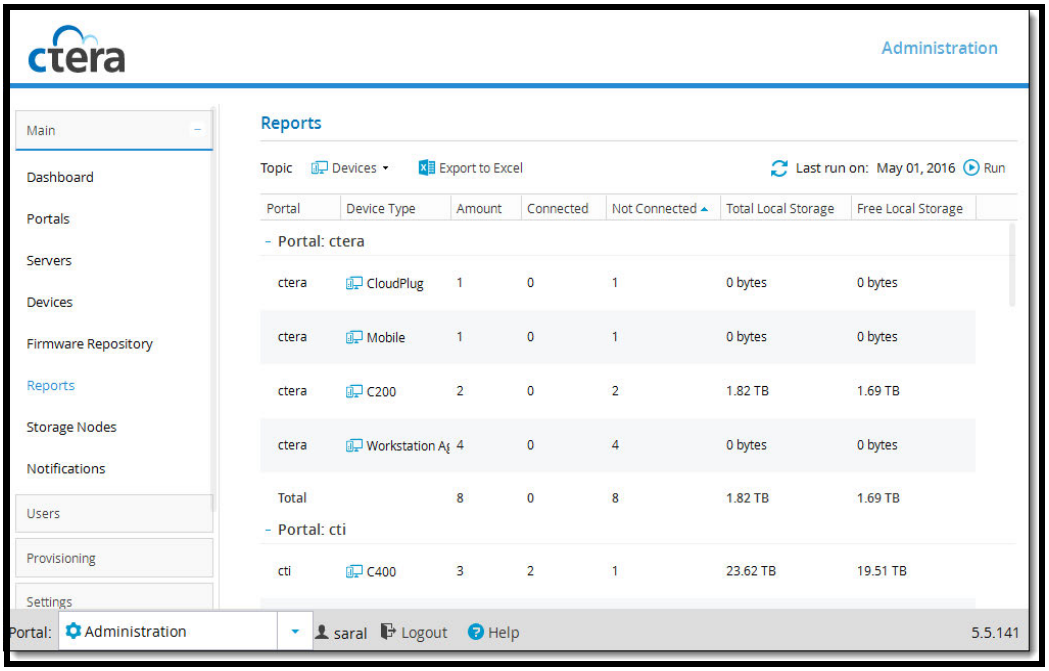
q **Bad Files**. The number of corrupted files in folders belonging to this folder group.

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 is displayed 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.



r **Device Type**. The device type.

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

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

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

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

w **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.
3. If a CTERA Portal administrator already ran the Plans Report, the report is displayed, and the report date is displayed in the **Last run on** field.
4. 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. For example, if 10 users are subscribed to a plan with 10GB storage space, this field will display 100GB.

e **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.

f **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.

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

h **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.

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

j **C200**. The number of C200 Cloud Storage Gateways owned by users who are subscribed to the

plan.

k **C400**. The number of C400 Cloud Storage Gateways owned by users who are subscribed to the plan.

l **C800**. The number of C800 Cloud Storage Gateways owned by users who are subscribed to the plan.

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

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

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

- Viewing Cloud Drive Folders
- Viewing Backup Folders
- Creating New Cloud Drive Folders
- Creating New Backup Folders
- Editing Cloud Drive Folders
- Editing Backup Folders
- Viewing Folder Contents
- Changing Passphrases for Accessing Backup Folder Contents
- Exporting Folders to Excel
- Deleting Folders

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.

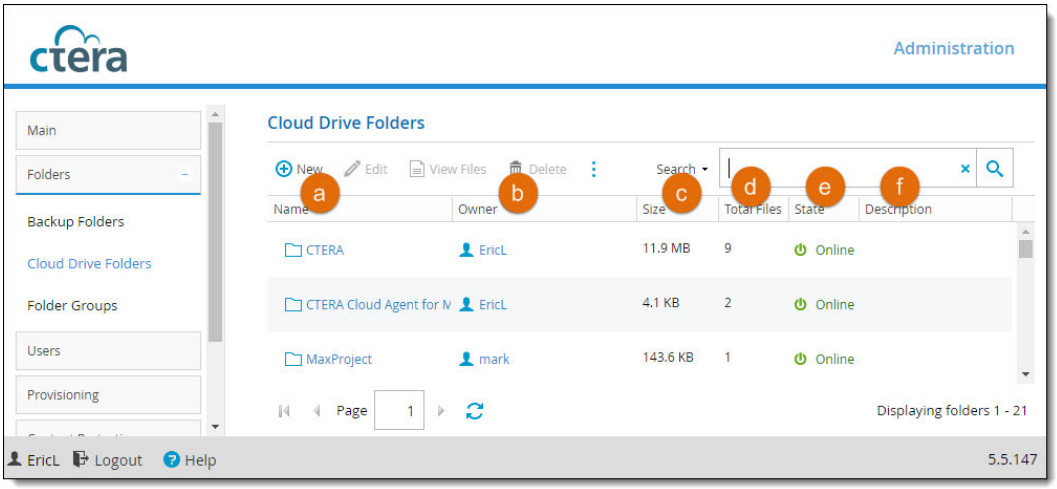
Cloud Drive folders. are folders created by the Cloud Drive service for personal and shared use. The portal automatically creates a personal folder for each user account's private files when the user account is created in the CTERA Portal. The folder is displayed to the user as `My Files` and is the 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, accessed via **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

- Select **Folders > Cloud Drive Folders** from the menu.
  The **Folders > Cloud Drive Folders** page opens, 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 Creating New Cloud Drive Folders.

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 Adding and Editing User Accounts.

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.

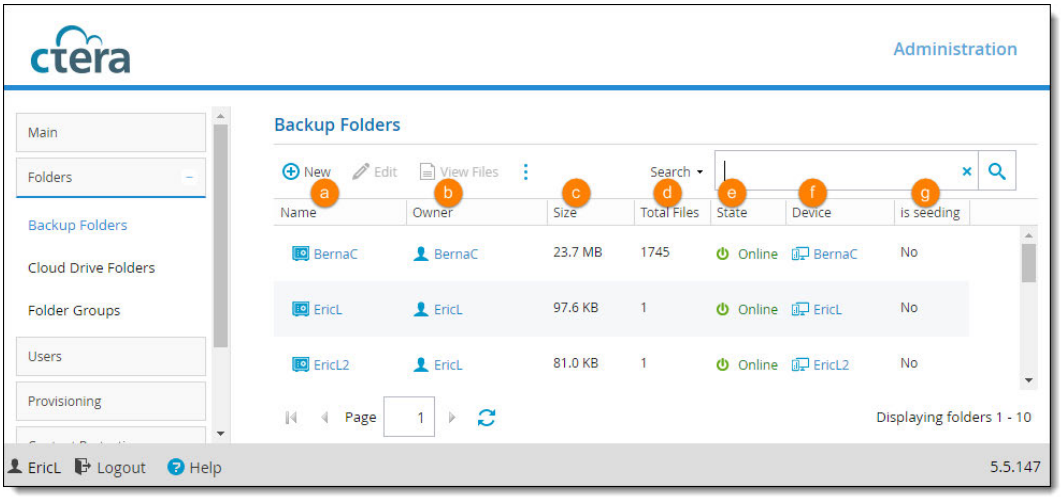
Folders inherit their state from the folder group.

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

VIEWING BACKUP FOLDERS

To view all backup folders in the portal

- Select **Folders > Backup Folders** from the menu.
  The **Folders > Backup Folders** page opens, displaying all backup folders.



a **Name**. The folder's name.
To view the folder's contents, click the folder name. For further details, see Creating New Cloud Drive Folders.

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 Adding and Editing User Accounts.

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.

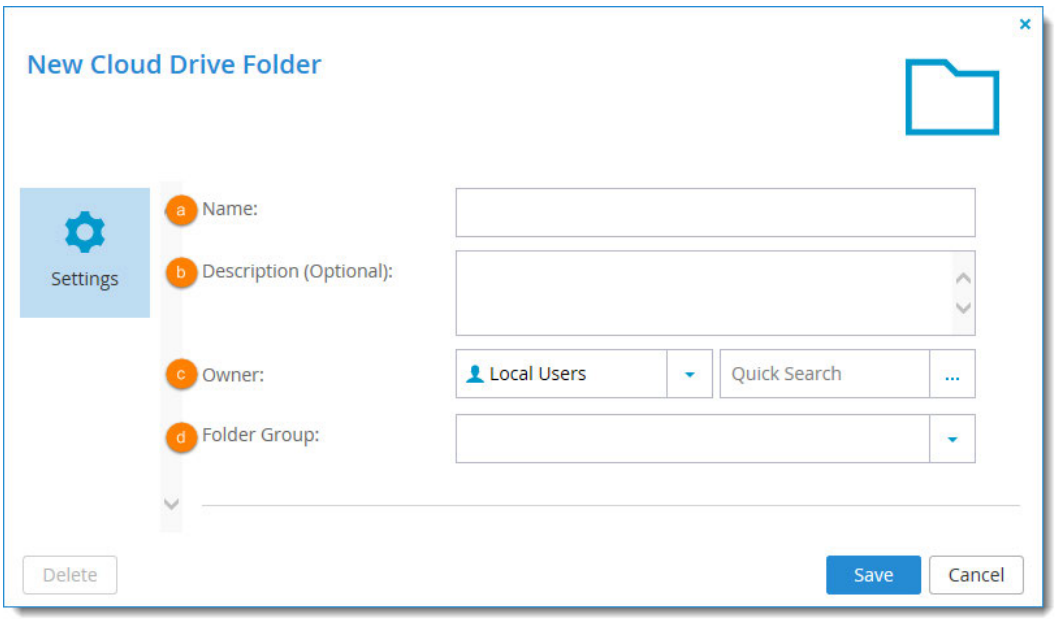
f **Device**. The device's name.
To edit the device, click the device name. For further details, see Editing Device Settings.

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.

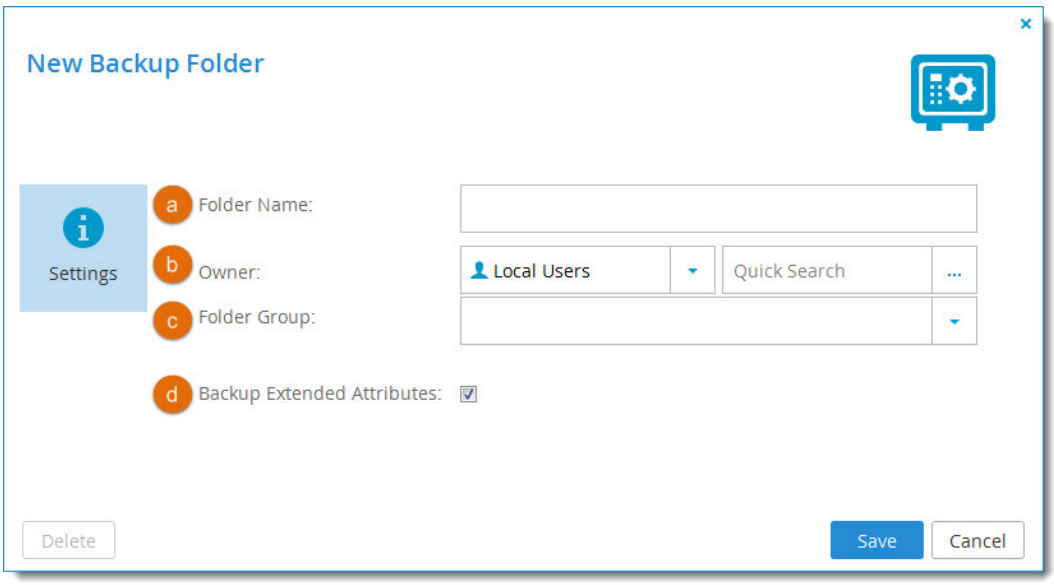
   d **Folder Group**. Select a folder group for the folder. For information about folder groups, see Managing Folder Groups.

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.

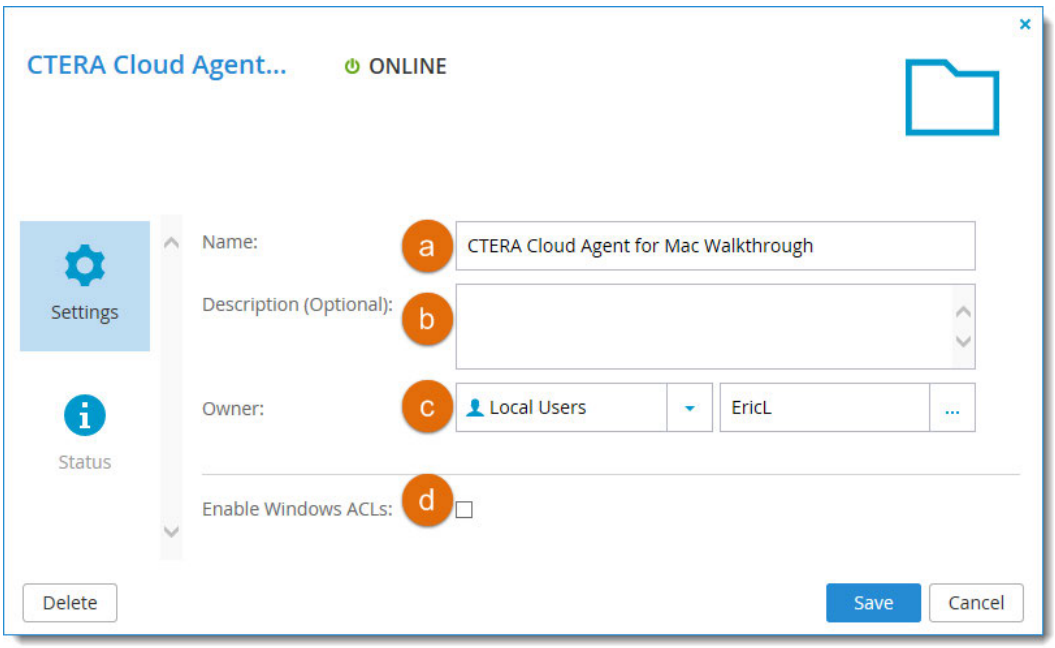
d **Backup Extended Attributes**. Select this option to back up special file permissions and metadata.

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:

- e **Name**. The name of the folder.
- f **Description** (optional). A description for the folder.
- g **Owner**. The user who owns the folder. The owner controls access to the folder. Click to select a new user.
- h **Enable Windows ACLs.** Select this option if you are backing up a cloud storage gateway share to this folder and the share supports NT ACLs and extended attributes on the gateway.

  Note: The files are saved in the portal using the NT ACL settings defined on the files. In this case, restoring the files from the portal to a cloud storage gateway maintains the NT ACL settings. However, all access to the files directly on the portal is blocked. Also, you can only restore the files from the portal via a cloud storage gateway. Thus, if the cloud storage gateway is not available for any reason, the files on the portal are also not available. This applies to all folders that are synced from the cloud storage gateway, including the **My Files** root folder and any other privately defined folder.

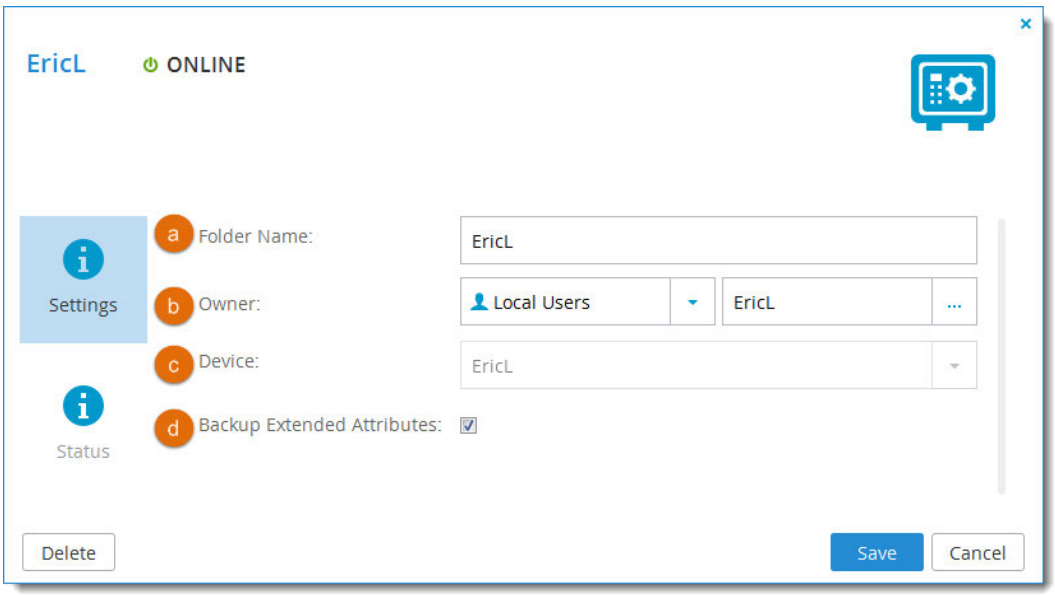
3 Click **Save**.

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.

   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.

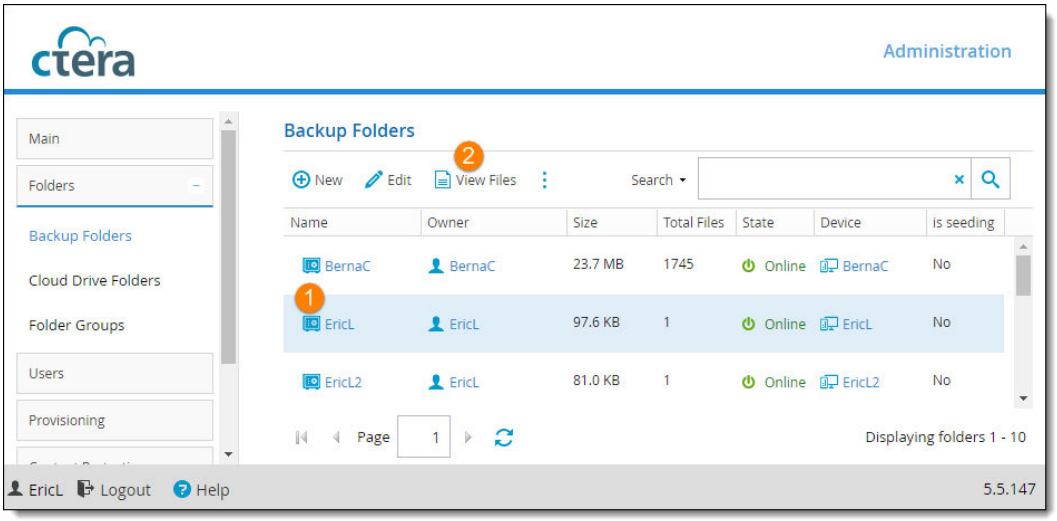
VIEWING FOLDER CONTENTS

Note: Viewing folder content can be restricted through the *Access End User Folders* attribute in the **Edit Role** dialog. See Customizing Administrator Roles for details.

To view a folder's content:

1 Select the folder in the **Backup Folders** page or the **Cloud Drive Folders** page.

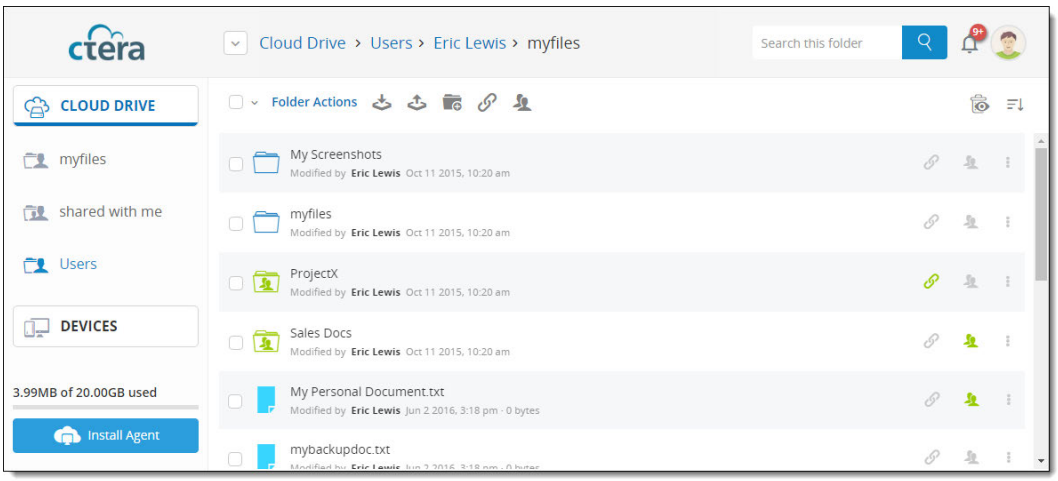
2 Click **View Files**.



3 If the folder is passphrase-protected, enter the passphrase for accessing for the folder and click **OK**. (Relevant only for backup folders.)

Similarly, if you don't have permission to access the folder, you are prompted for the folder owner's password. Enter the password and click **OK**.

The end user portal view opens, showing the folder you selected under **Users**.



For help managing files in this view, see the *CTERA End User Portal Quick Start Guide*. You can access this guide by clicking your avatar at the top right and then clicking **Help**.

CHANGING PASSPHRASES FOR ACCESSING BACKUP FOLDER CONTENTS

To change a passphrase:

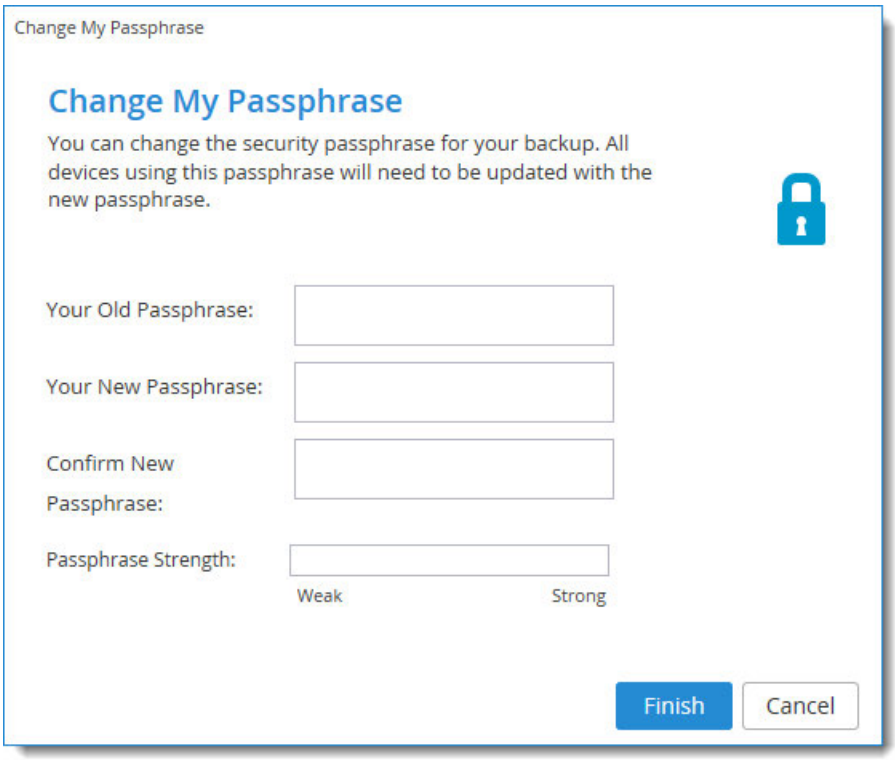
1 Do one of the following:

- 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.

The **Change My Passphrase** dialog box is displayed.



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 deduplication 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 deduplication 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

- Changing a User's Deduplication Level
- Changing the Default Deduplication Level
- Viewing Folder Groups
- Adding and Editing Folder Groups
- Managing Cloud Drive Folders for Folder Groups
- Managing Backup Folders for Folder Groups
- Changing Passphrases for Accessing Folder Group Contents
- Exporting Folder Groups to Excel
- Deleting Folder Groups

CTERA Portal organizes cloud folders in *folder groups.* Each folder group acts as a deduplication realm. Deduplication 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 deduplication level for backup folders and for Cloud Drive folders.

For backup folders and for Cloud Drive folders, you can set the deduplication 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 deduplication 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.

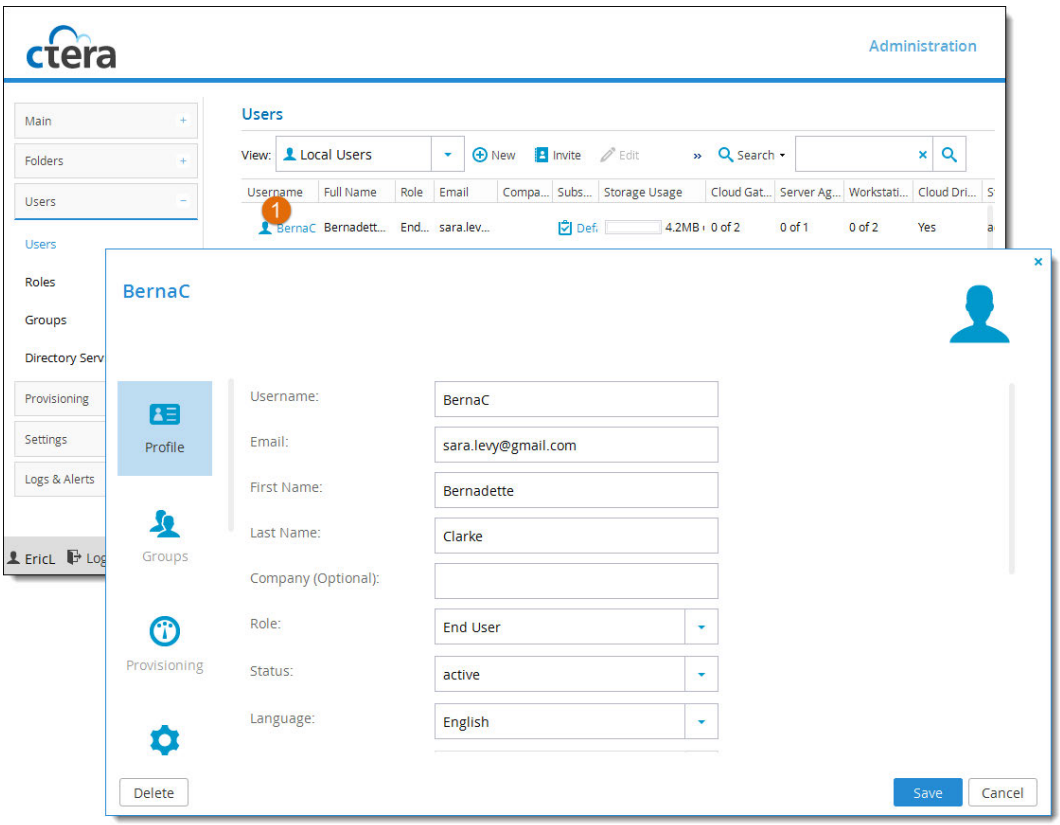
You can change the default deduplication levels for any user created in the portal, and you can change any user's deduplication levels. You can choose a different level for backup folders and for Cloud Drive folders.

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

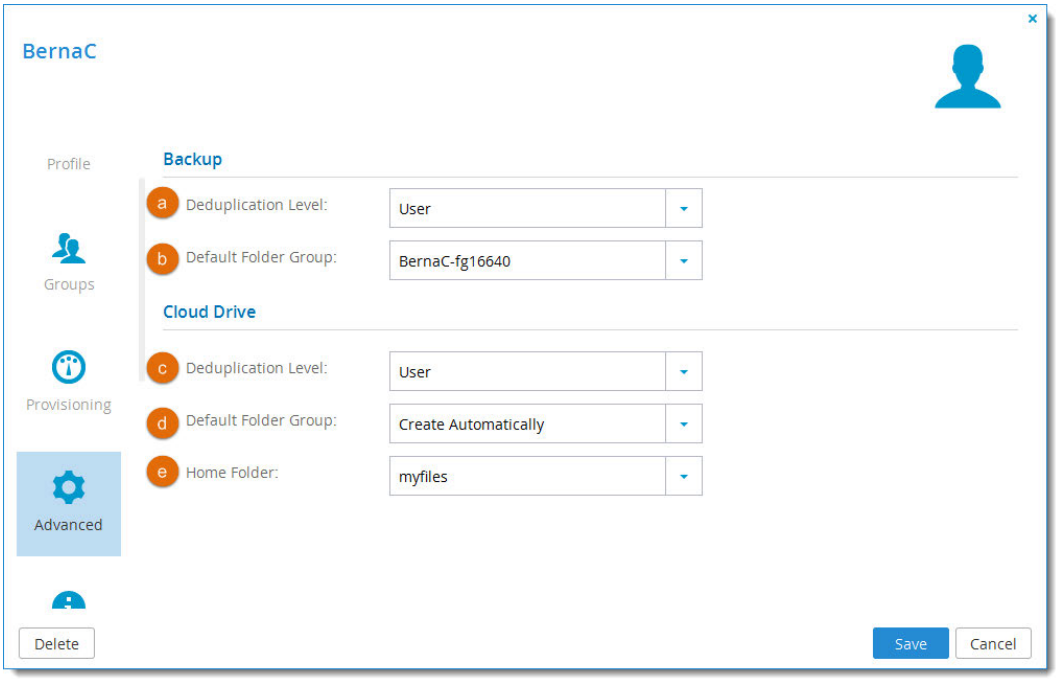
CHANGING A USER'S DEDUPLICATION LEVEL

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 deduplication level to use for new backup folders. Select one of the following:

- **User**. Create a single folder group for the user account, containing all of the user account's backup folders. Deduplication is performed for the user account's folder group.
- **Portal** (default). Use a single folder group that is shared by the entire virtual portal, containing all of the backup folders in the portal.
- **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**. Displayed 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 deduplication level to use for new cloud folders. Select one of the following:

- **User**. 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.
- **Portal** (default). Use a single folder group that is shared by the entire virtual portal, containing all of the cloud folders in the portal.
- **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**. Displayed 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.

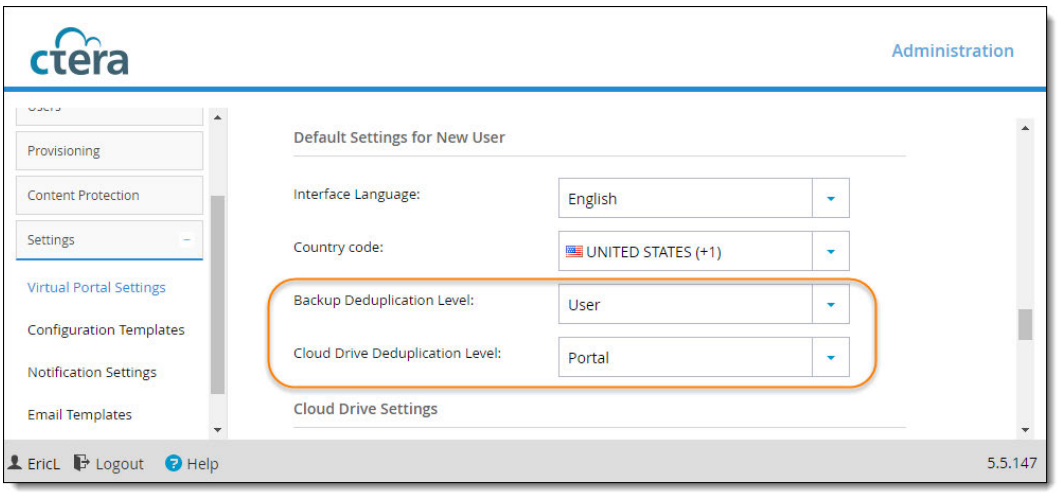
e **Home Folder**. Select one of the user's personal folders to act as the user's home folder. The home folder is a personal folder that is linked to the user account and cannot be deleted.

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.

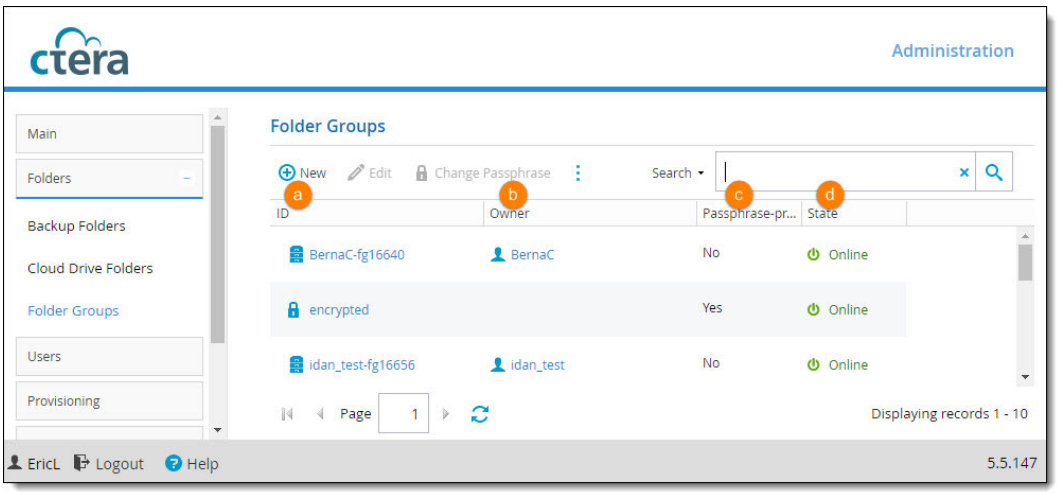
2 Scroll down to **Default Settings for New User**. and you can change the **Backup Deduplication Level** and the **Cloud Drive Deduplication Level**. These are the default settings used for all new users.



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.

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.

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

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

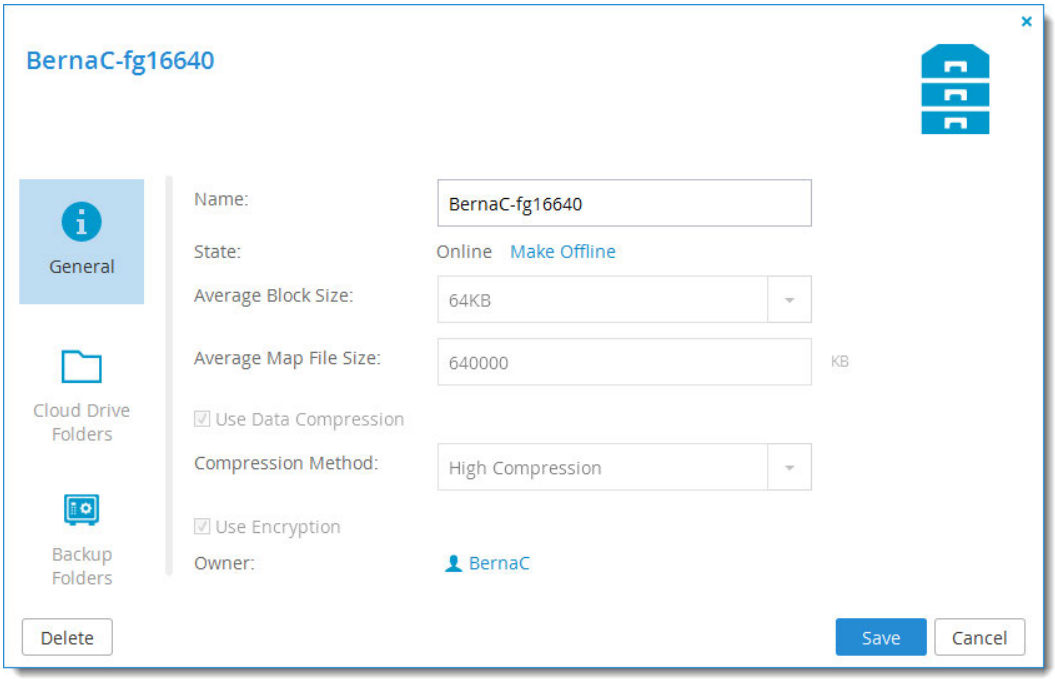
ADDING AND EDITING FOLDER GROUPS

When a device first backs up files to the CTERA Portal, and cooperative deduplication 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 following information.

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.

In this field...	Do this...
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. 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.
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.
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.

In this field...	Do this...
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.
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.

3 Click **Save**.

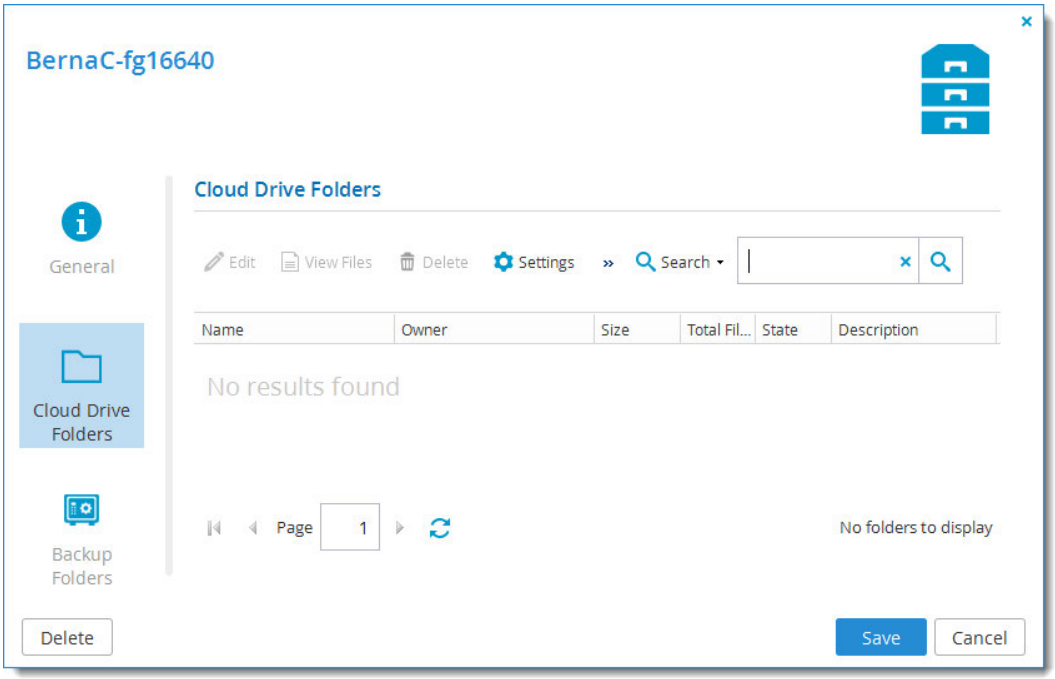
MANAGING CLOUD DRIVE FOLDERS FOR FOLDER GROUPS

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 is displayed 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.

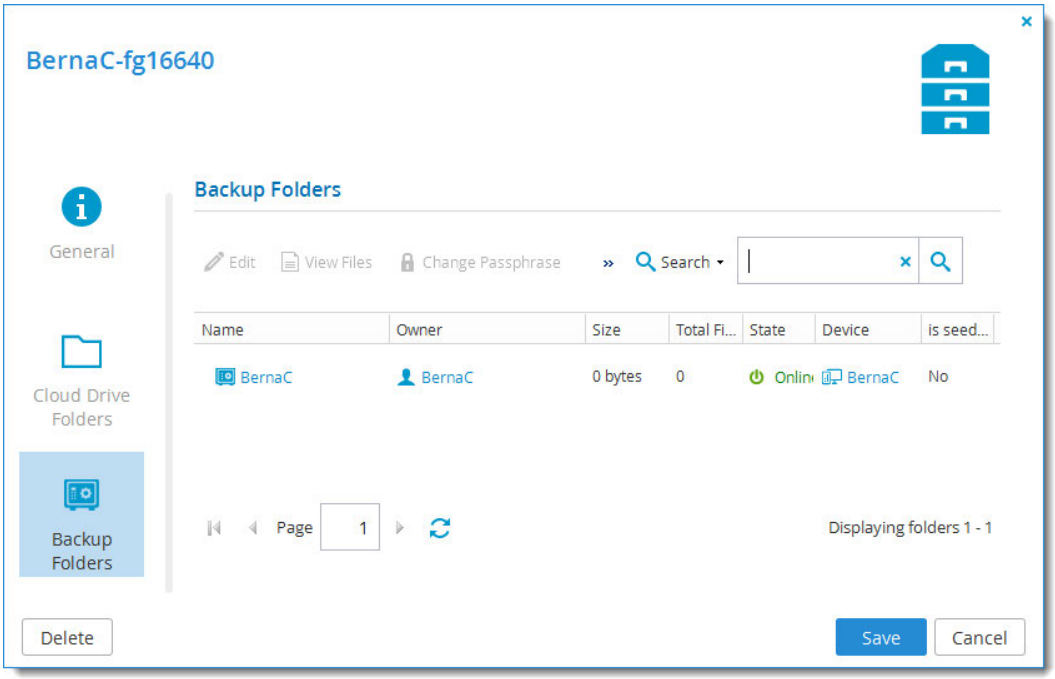
MANAGING BACKUP FOLDERS FOR FOLDER GROUPS

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 is displayed with a table of backup folders in the folder group.



3 Perform any of the backup folder management tasks described in Managing Folders, 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 opens, displaying all folder groups.

2 Select the desired folder group's row.

3 Click **Change Passphrase**.
The **Change My Passphrase** dialog box is displayed.

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.

   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 opens, 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

In this chapter

- Inviting Users to Register
- Viewing User Accounts
- Filtering the Users Page
- Adding New Users
- Editing User Profiles
- Enabling/Disabling User Accounts
- Adding Users to Groups
- Provisioning User Accounts in Team Portals
- Configuring a User's Deduplication Settings
- Viewing User Account Details
- Generating Monthly Reports
- Managing a User's Devices
- Managing a User's Cloud Drive Folders
- Managing a User's Folder Groups
- Configuring User Alerts (Administrators Only)
- Exporting User Accounts to Excel
- Applying Provisioning Changes
- Deleting User Accounts
- Customizing Administrator Roles

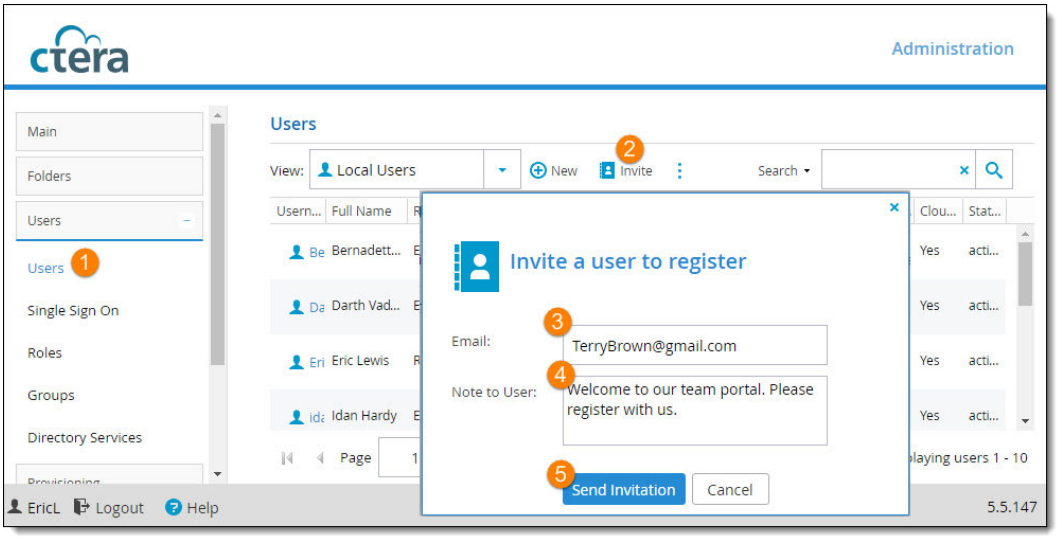
End users are registered with the CTERA Portal and have access to the End User Portal. Each user is represented in the CTERA Portal by a *user account*.

Users can be added manually in the **Users** page, as described below. **Groups** can be added manually in the **Groups** page, as described in Managing User Groups.

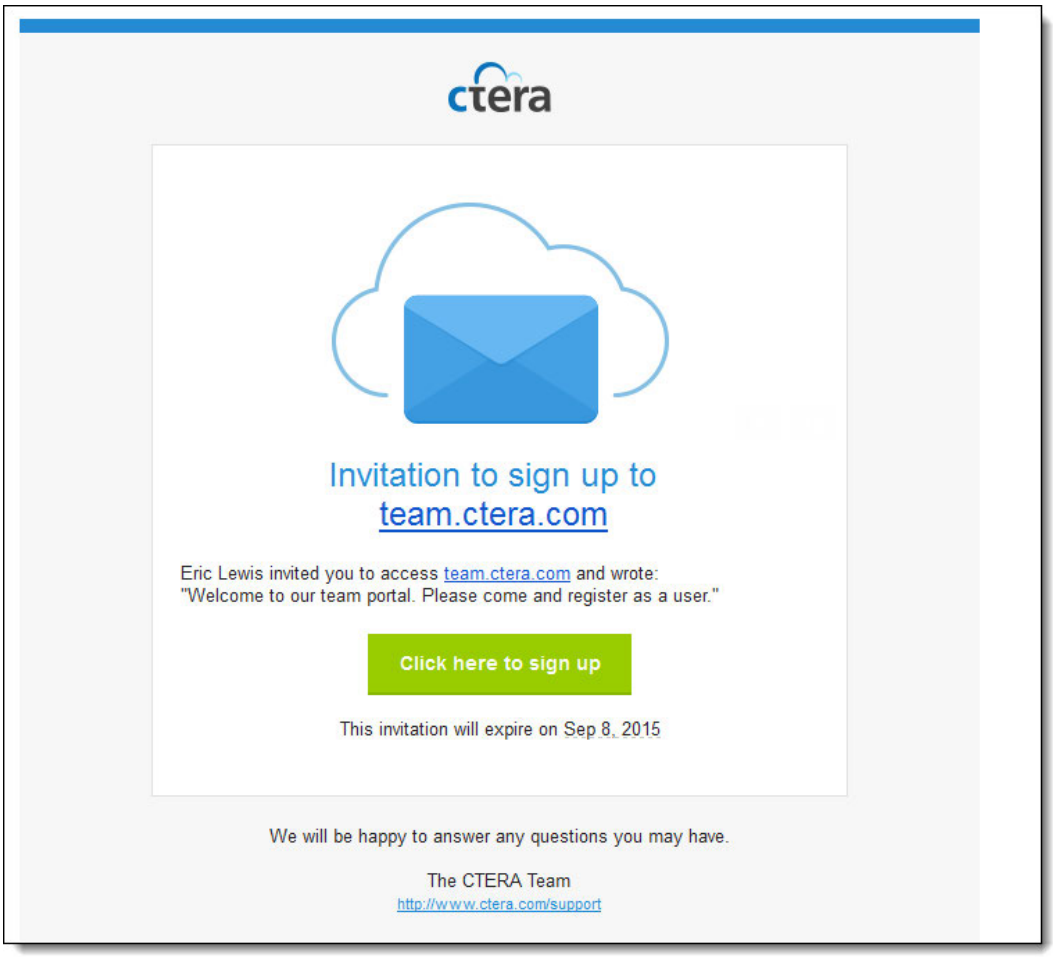
Alternatively, CTERA Portal supports directory services, such as Active Directory. You can attach a directory service and fetch users and groups from the directory service. For information about using a directory service, see Using Directory Services.

INVITING USERS TO REGISTER

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



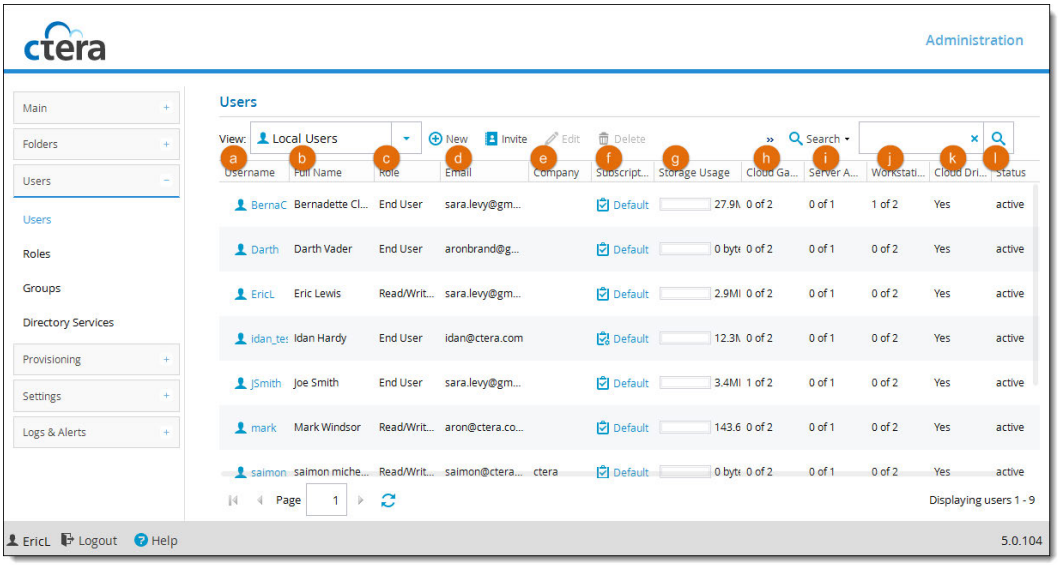
The user clicks the link to the portal, registers account details and then receives an email to activate their account. Portal administrators receive email notifications that the user has registered.

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

VIEWING USER ACCOUNTS

To view all user accounts in the portal:

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



a **Username**. The user account's user name.
To edit the user, click the user name. For further details, see Adding and Editing User Accounts.

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.

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

h **vGateway Licenses**. The number of CTERA Virtual Gateway licenses used by the user account out of the total number provisioned.

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

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

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

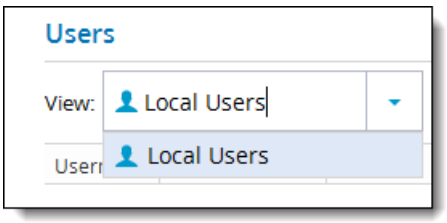
l **Status**. The user's account status. This can be either of the following:

- 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 USERS PAGE

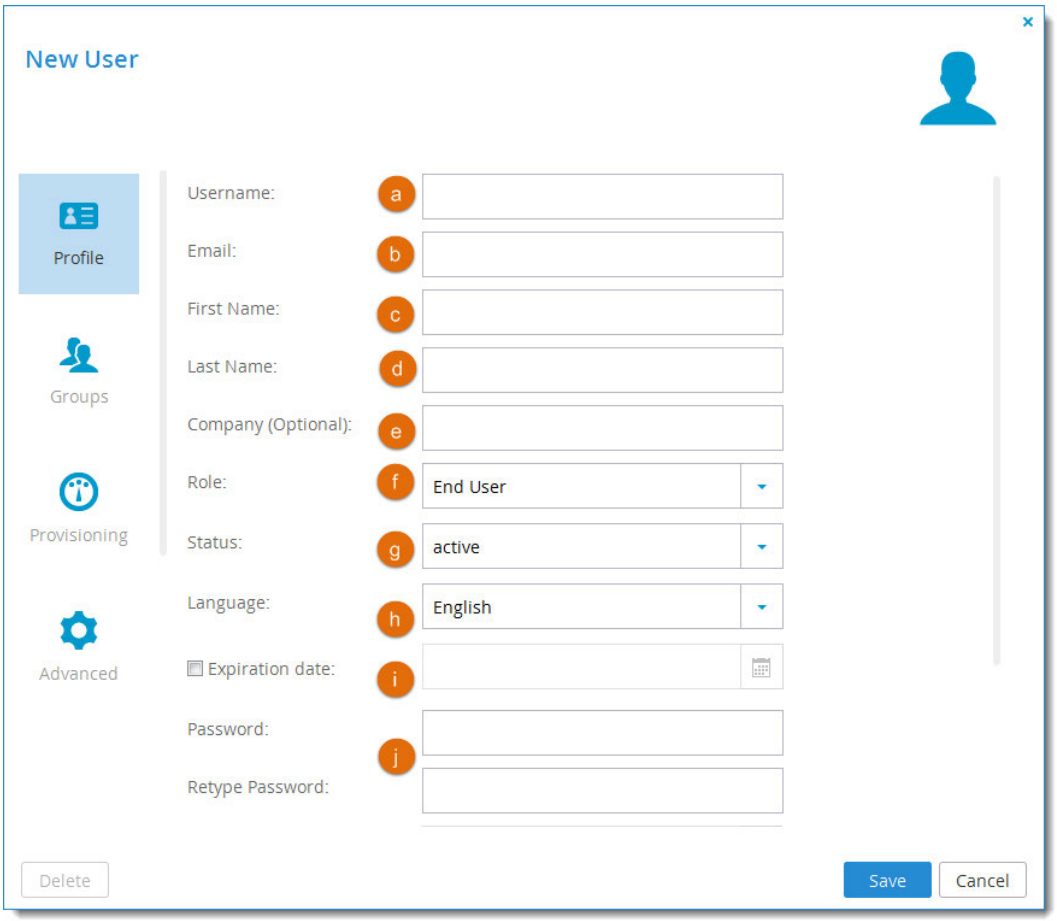
To view only a specific type of users, in the **View** drop-down list, select:

- 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 Select **Users > Users** from the menu, 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 Administration tab of the End User Portal with read-write permissions. For information about this tab, see CTERA Portal Interfaces and Users. This role is relevant for team portals only.
      - **Read Only Administrator**. The user can access the End User Portal, and can access the Administration tab of the End User Portal with read-only permissions. For information about this tab, see CTERA Portal Interfaces and Users. This role is relevant for team portals only.
      - **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.

      Note: 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.

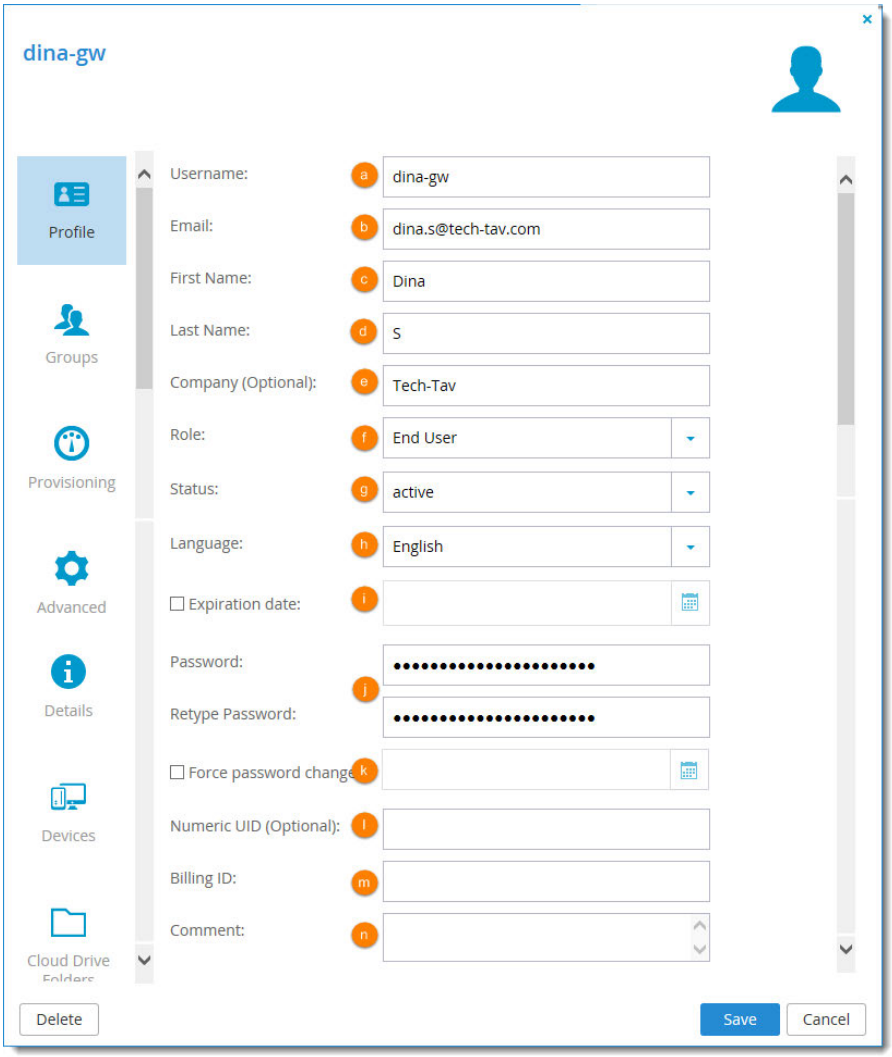
      The default value for new users created by an administrator is *active*.

      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 the calendar icon 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. **Comment**. Type a description of the user account.
3. Click **Save**.

   The user is added.

EDITING USER PROFILES

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 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 Administration tab of the End User Portal with read-write permissions. For information about this tab, see CTERA Portal Interfaces and Users.
- **Read Only Administrator**. The user can access the End User Portal, and can access the

Administration tab of the End User Portal with read-only permissions. For information about this tab, see CTERA Portal Interfaces and Users.

- **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.

Note: 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**. Select this option to specify an expiration date for the user account password, and then click the calendar icon 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 **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), 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**.

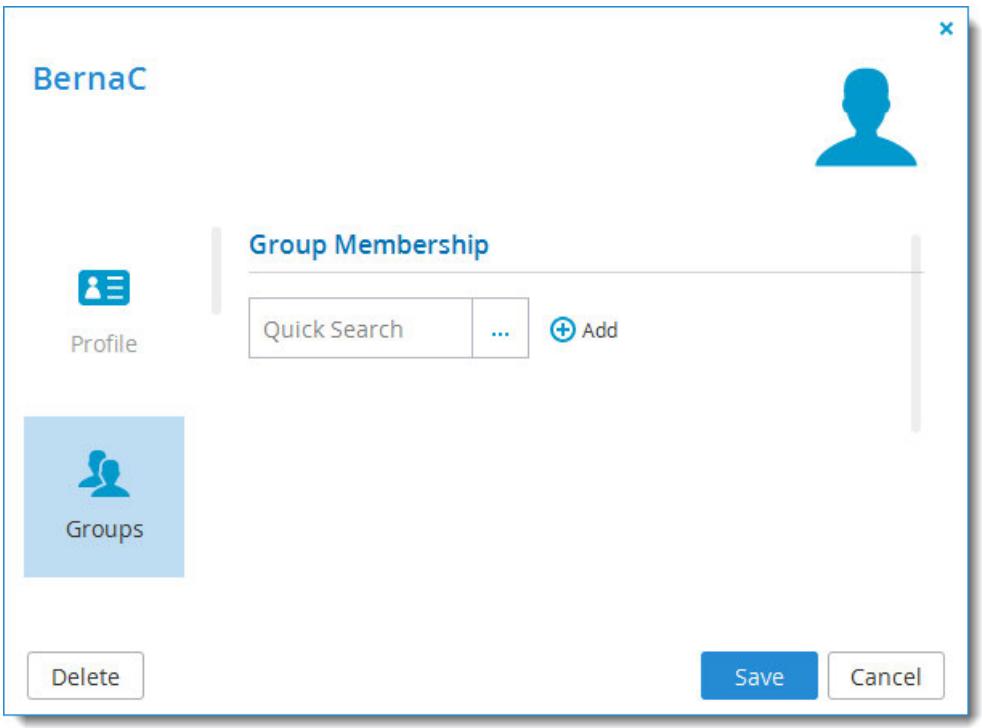
3 Click **Save**.

To disable a user account:

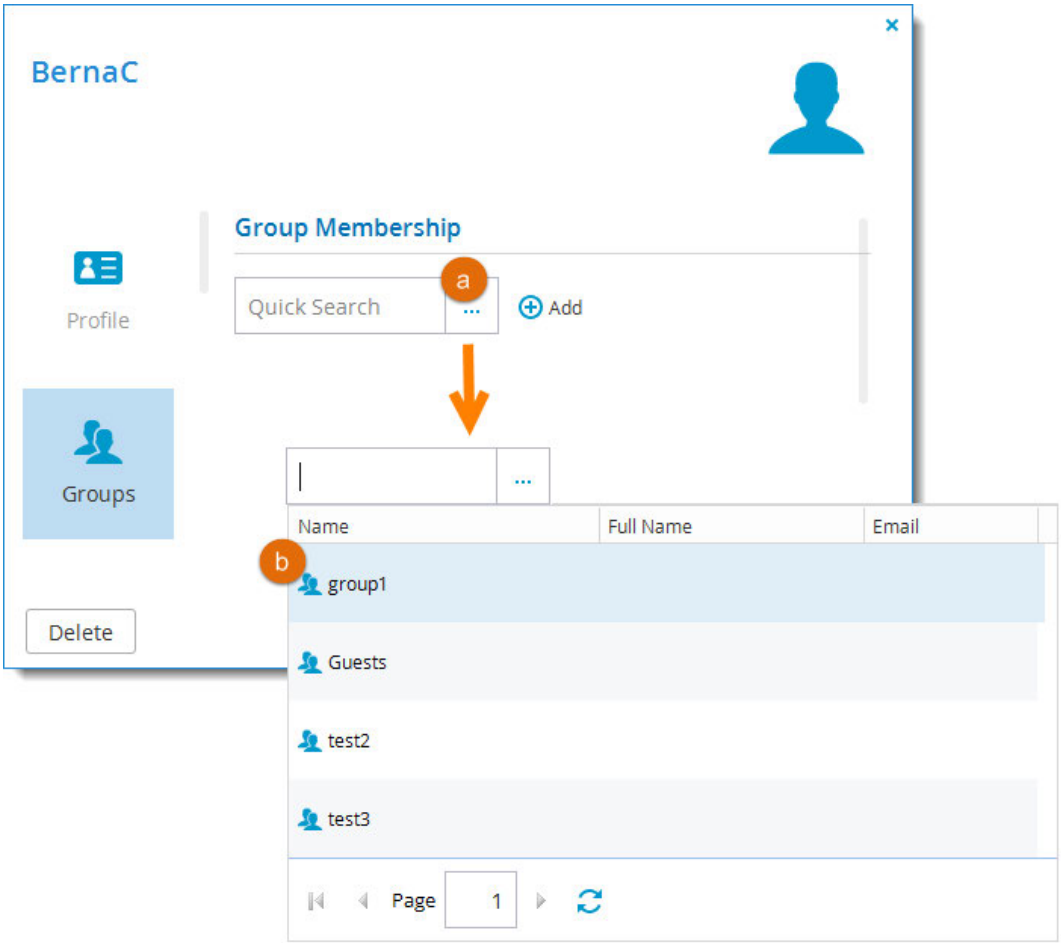
1. Browse to **Users > Users** and click the username of the account you want to edit, or select the account's row and click **Edit**.
   The User Account Manager opens displaying the **Profile** tab.
2. In the **Status** field, select **inactive**.
3. Click **Save**.

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.

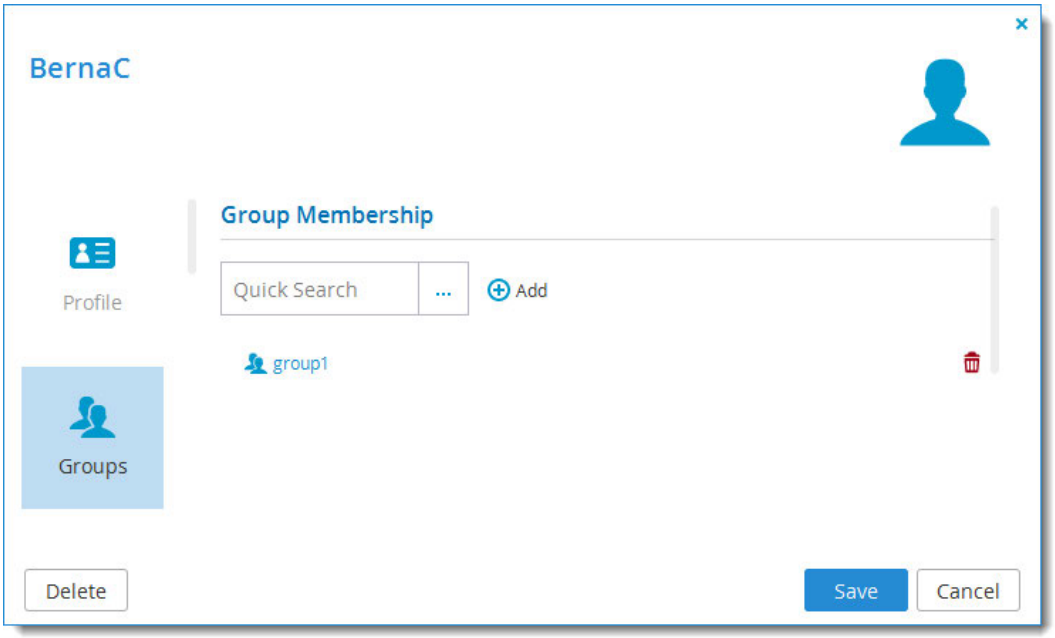


3. To add the user account to a user group, do the following:
   a. In the **Quick Search** field, type a string that is displayed anywhere within the name of the desired user group, then click ...
   A table of user groups matching the search string is displayed.



b Select the desired user group in the table.
The user group is displayed 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.

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 IN TEAM PORTALS

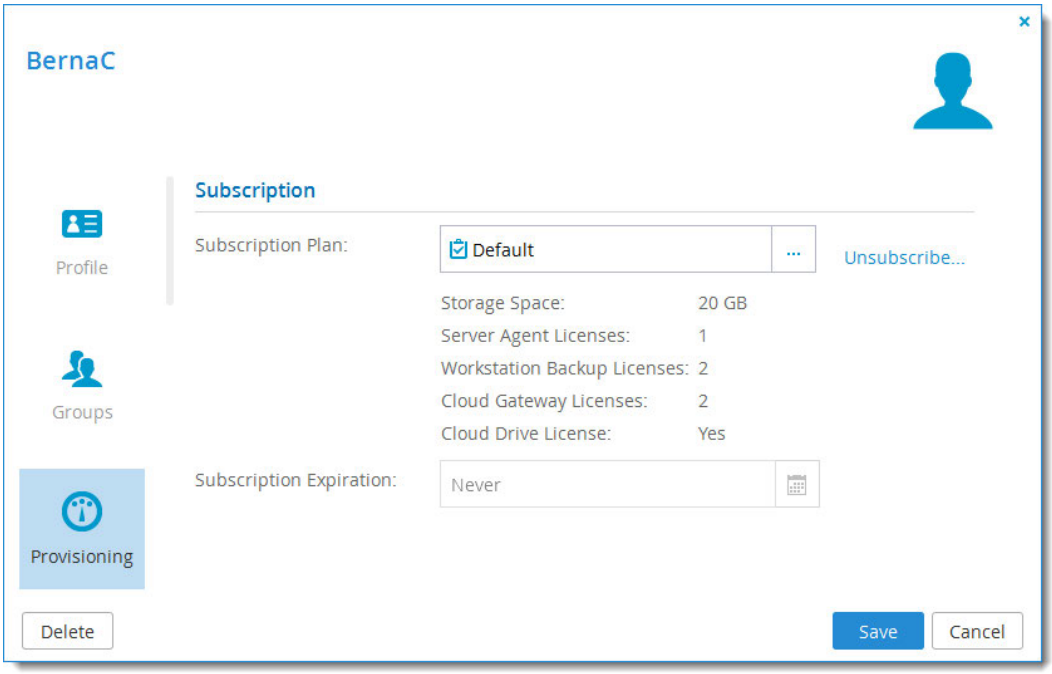
Team members may be assigned to a default subscription plan or assigned automatically to another plan based on automatic template assignment settings (see Provisioning). If desired, you can subscribe an individual user to a different subscription plan. You can also unsubscribe the user account, which 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:

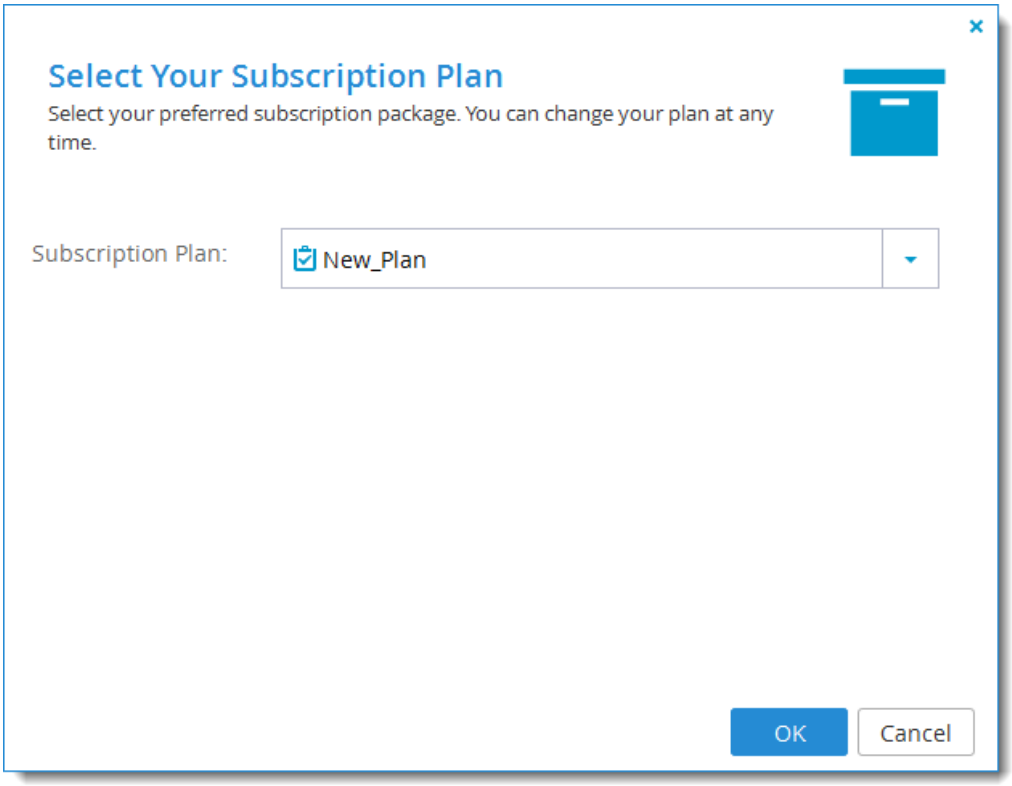
1 Click the user's name in the **Users > Users** page or select the user's row and click **Edit**.

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**.

Terminating User Accounts

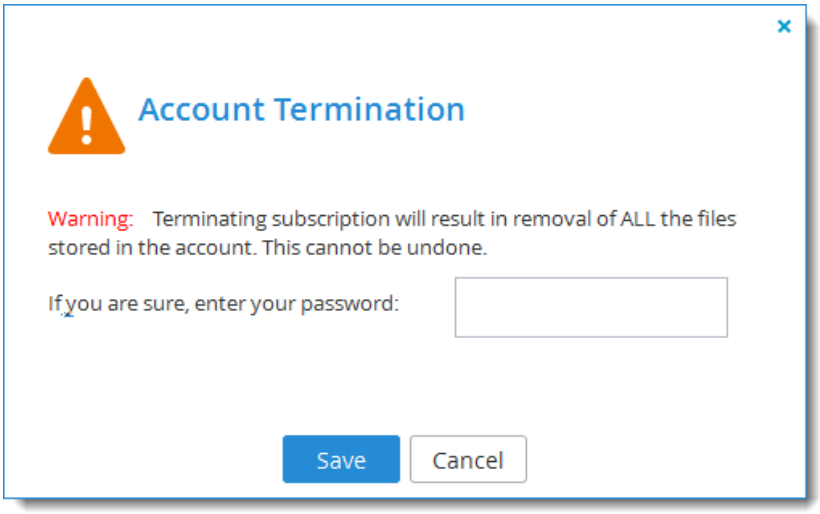
Unsubscribing a user account from a subscription plan terminates the user account and removes all the files stored in the account.

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 is displayed.



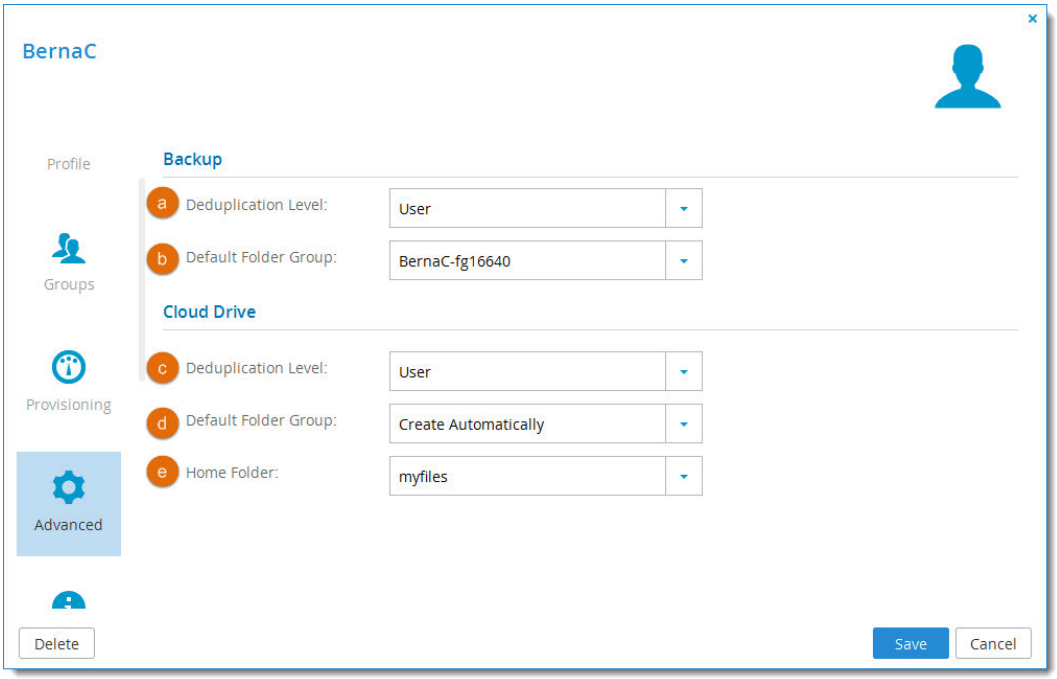
4 If you are sure you want to proceed, enter your password in the field provided.

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 deduplication level to use for new backup folders. Select one of the following:

- **User**. 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.
- **Portal** (default). Use a single folder group that is shared by the entire virtual portal, containing all of the backup folders in the portal.
- **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**. Displayed 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 deduplication level to use for new cloud folders. Select one of the following:

- **User**. 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.
- **Portal** (default). Use a single folder group that is shared by the entire virtual portal, containing all of the cloud folders in the portal.
- **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**. Displayed 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.

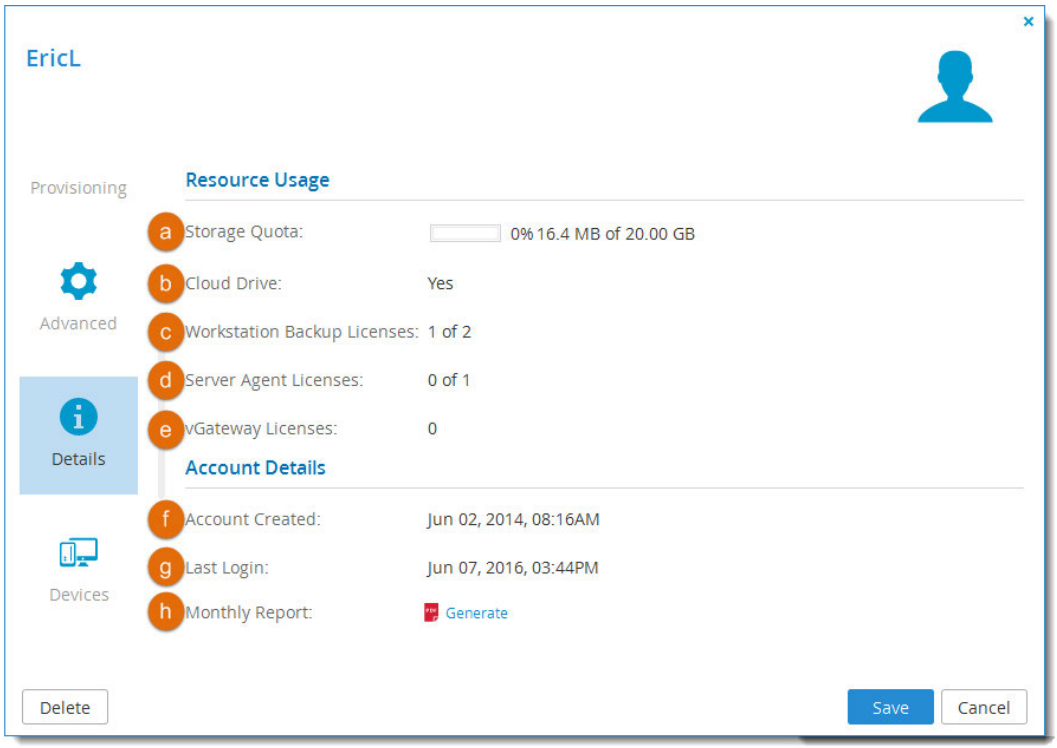
e **Home Folder**. Select one of the user's personal folders to act as the user's home folder. The home folder is a personal folder that is linked to the user account and cannot be deleted.

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 **vGateway Licenses**. The number of CTERA Virtual gateways associated with the user account. If the user's subscription plan includes Virtual Gateways, this number is expressed as a number

of the total number of Virtual Gateways 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.

h **Monthly Report**. A link for generating and downloading a monthly report of events in the user account in PDF format.

GENERATING MONTHLY REPORTS

You can trigger the immediate generation and sending of the monthly report for a specific user account.

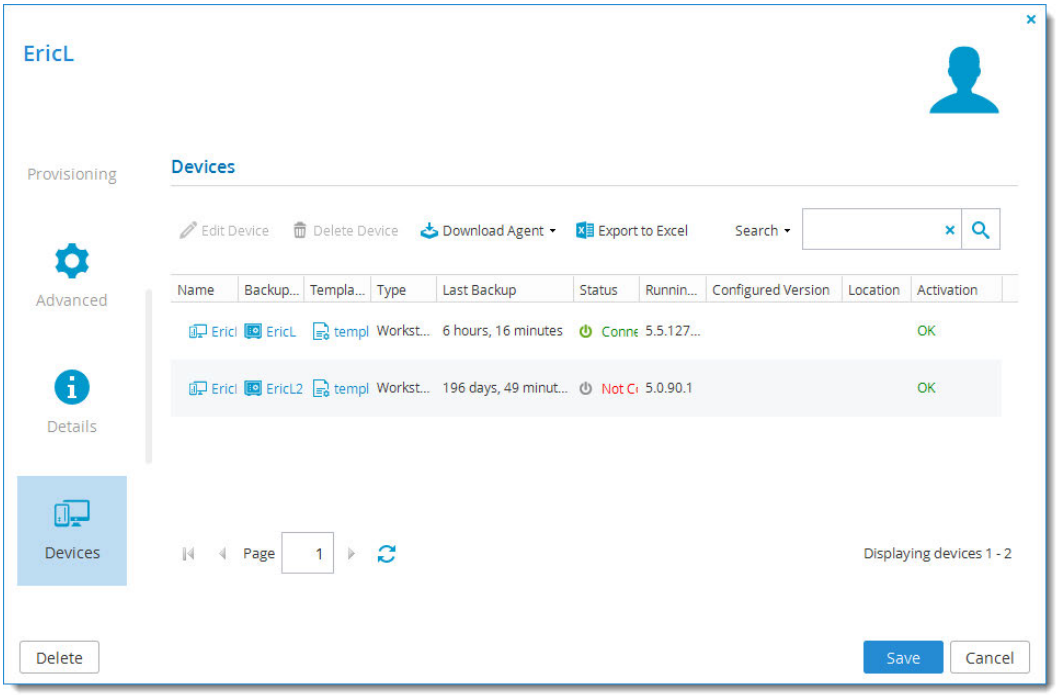
To generate a monthly report for the user account

- On the **Details** tab, click **Generate**.
  A report is generated and sent to the user by email.

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 is displayed with a table of devices associated with the user account.

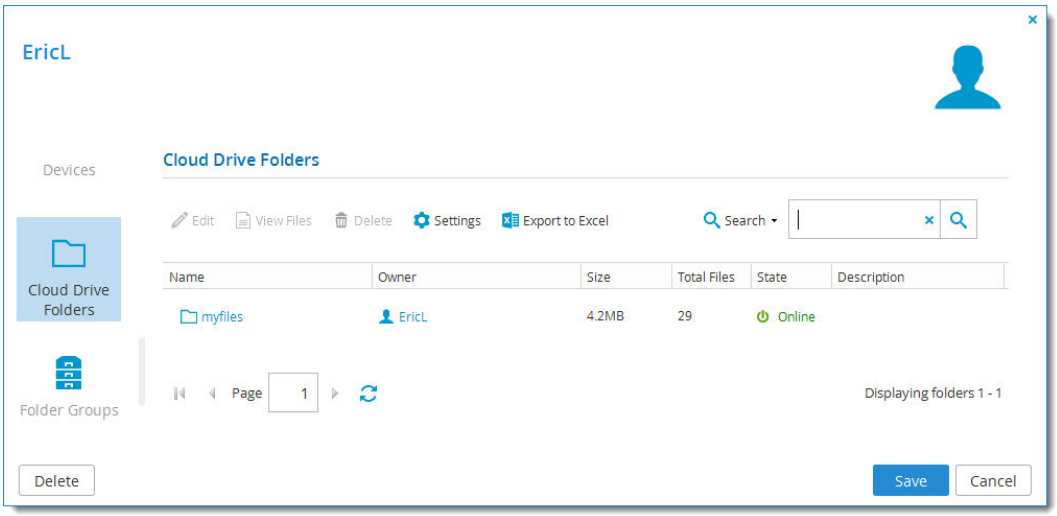


3 Perform any of the device management tasks described in Managing Devices, as if you were working in the **Main > Devices** page.

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.

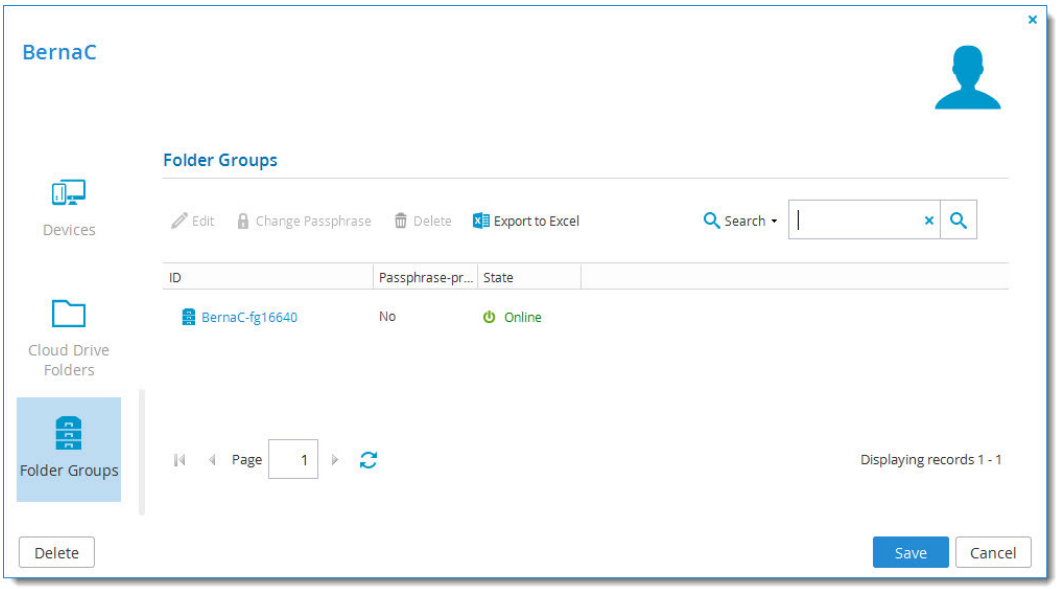


3 Perform any of the project management tasks described in Managing Folders, as if you were working in the **Folders > Cloud Drive Folders** page.

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.



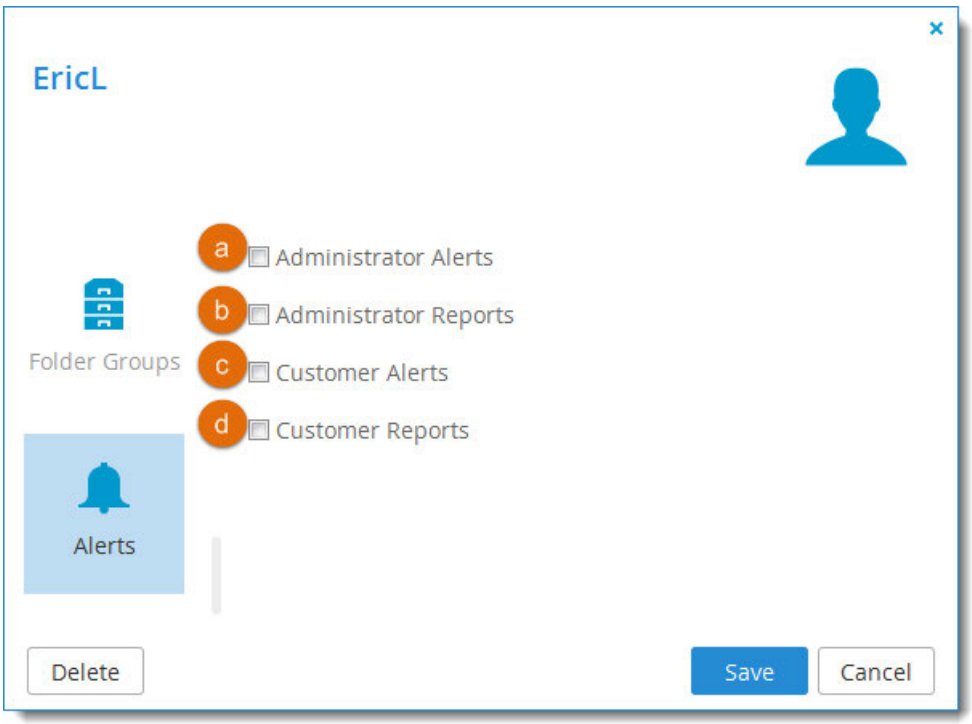
3 Perform any of the folder group management tasks described in Managing Folder Groups, as if you

were working in the **Folders > Folder Groups** page.

CONFIGURING USER ALERTS (ADMINISTRATORS ONLY)

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 **Alerts** tab.



3 Check the types of alerts the user 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**.

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 opens, 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.

Note: 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 opens, 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 is displayed.
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.

CUSTOMIZING ADMINISTRATOR ROLES

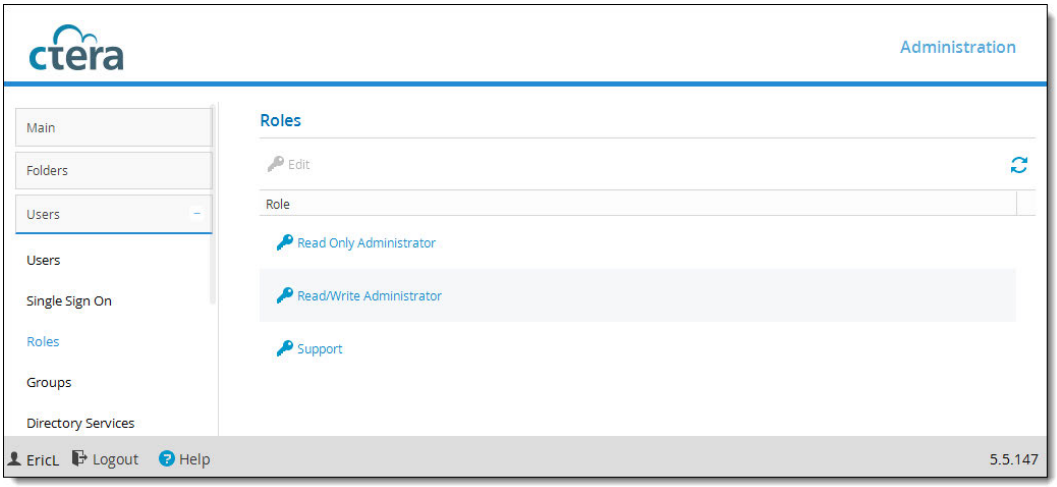
By default, CTERA Portal includes three built-in administrator roles for administrators:

- **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.

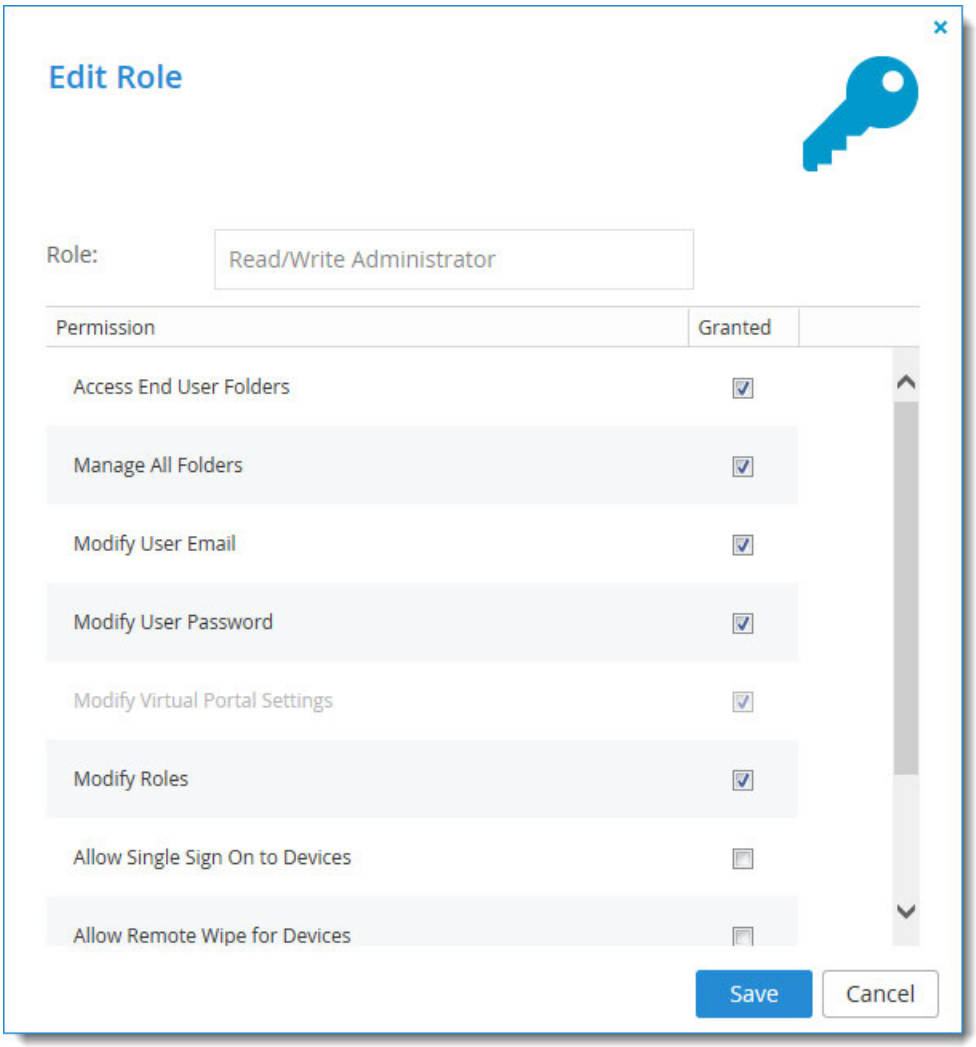
You can customize these roles, adding or removing permissions as desired.

To customize an administrator role:

1. Select **Users > Roles** from the menu.
   The **Users > Roles** page opens, 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 administrator 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.
   - **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**.

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

Permission	Read/Write Administrator	Read Only Administrator	Support
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

8

CONFIGURING SINGLE SIGN ON

CTERA Portal supports user identity federation over SAML 2.0. SAML enables you to centralize your corporate user identities and provide Single Sign-On (SSO) capabilities to all of your enterprise applications. When SSO is enabled on the portal, users' passwords are not stored on CTERA Portal. Instead, user authentication is performed through the identity provider’s login page.

To configure SAML SSO, you will need an SAML identity provider. SAML Single Sign On has been tested with the following identity providers:

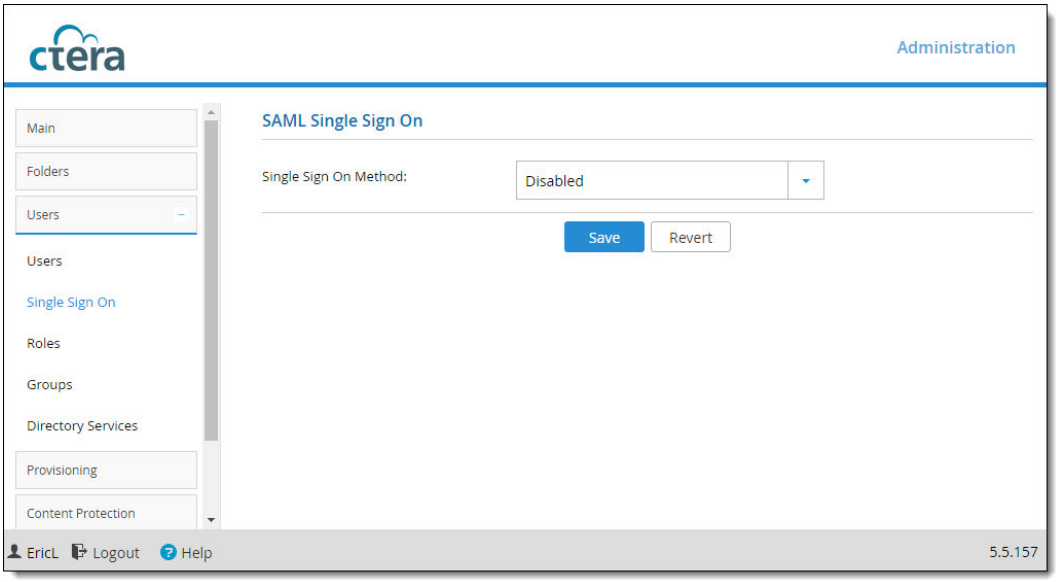
- Okta
- OneLogin
- Microsoft Active Directory Federation Services 2.0 on Windows 2008 and Windows 2012

If you would like to use a different identity provider, contact CTERA to validate the provider.

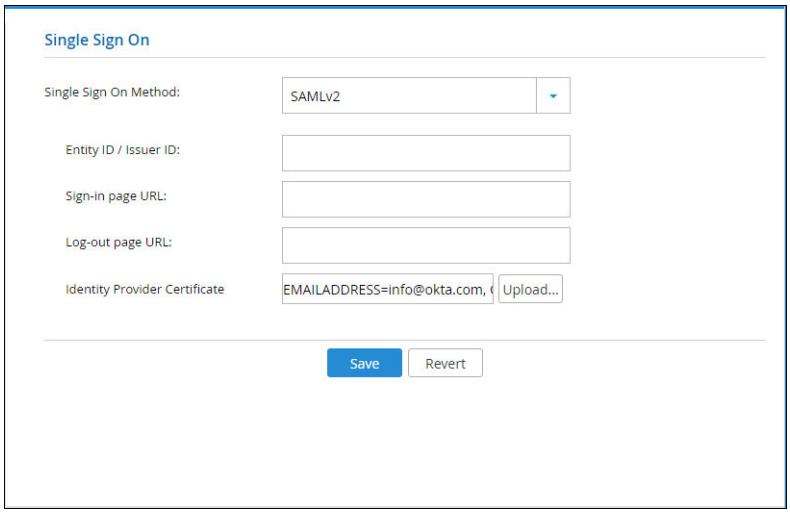
You need to enable SSO on the portal and specify the identity provider's parameters. Once configured, the provider will handle the sign-in process for the portal users, including providing authentication credentials for the users.

To configure SAML single sign on

1 Select **Users > Single Sign On** from the menu.



2 Select **SAMLv2** from the dropdown box.



3 Enter the details of the SAML identity provider:

Field Name	Description	Okta field	OneLogin field
Entity ID/Issuer ID	A free text string that uniquely identifies your SAML identity provider. This must match the entity ID that you choose when signing up for the identity provider's SSO service.	The IdP ID (Identity Provider).	The IdP ID (Identity Provider).
Sign-in page URL	The URL that CTERA Portal should redirect global administrators to when they sign in. You need to get this from the provider. The URL has the following format: `https://cterawalla.idProvider.com/home/genericSaml/string_x/string_y`	The IDP Login URL: the ACSurl endpoint.	IdP login URL.

Field Name	Description	Okta field	OneLogin field
Log-out page URL	The URL that CTERA Portal should redirect your global administrators to when they log out of the global administrator interface. Without this URL configured, a logout will redirect to the sign-in page URL and log the user back into the portal. You need to get this from the provider.	The single logout URL and set **Enable Single Logout** to True in Okta.	IdP logout URL. This is optional.
Identity Provider Certificate	The authentication certificate issued by the provider. You need to get this from the provider, usually by download from the provider's site. Click the **Upload** button here to upload your provider's certificate.	Export the certificate from Okta Single Sign-On and upload it to the CTERA Portal.	Copy the entire X.509 Certificate string.

4 Click **Save**.

9

MANAGING USER GROUPS

In this chapter

- Viewing User Groups
- Filtering the User Groups Page
- Adding and Editing User Groups
- Configuring User Group Members
- Deleting User Groups

User groups are groups of users that you can define and then use to simplify assigning user permissions. Groups are useful when setting several types of policies and permissions, such as:

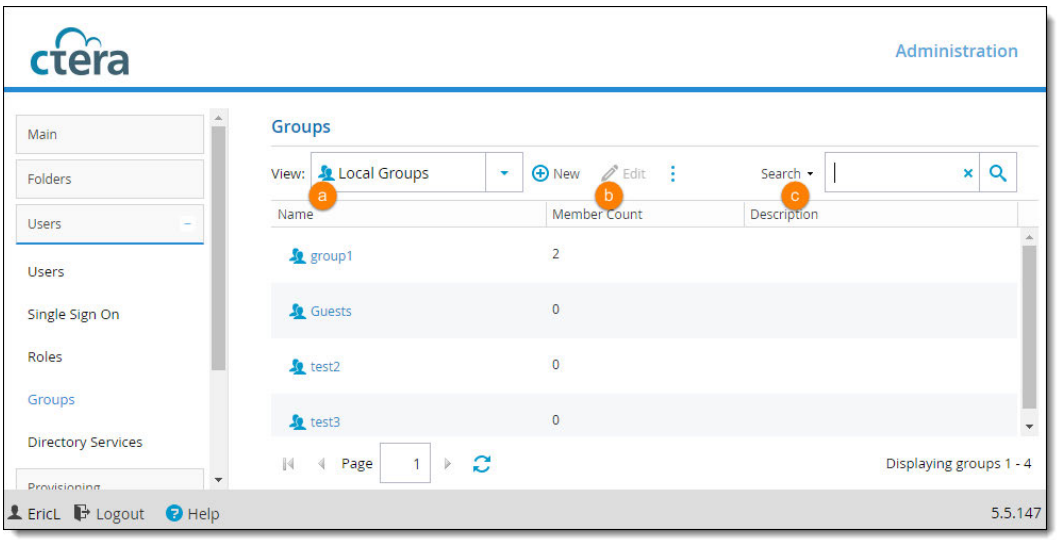
- Automatic template assignment policy. See Configuring the Automatic Template Assignment Policy.
- Setting permissions for accessing folders. See Managing Folders.
- Setting Collaboration Permissions.

Note: You can create groups manually, as described below, or you can fetch groups from a directory service, as described in Using Directory Services.

VIEWING USER GROUPS

To view all user groups in the portal:

- Select **Users > Groups** from the menu.



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

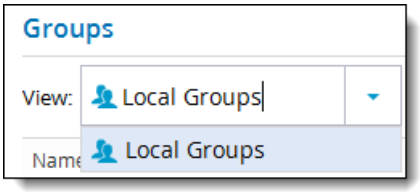
b **Member Count**. The number of user accounts that are members of the user group.

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:

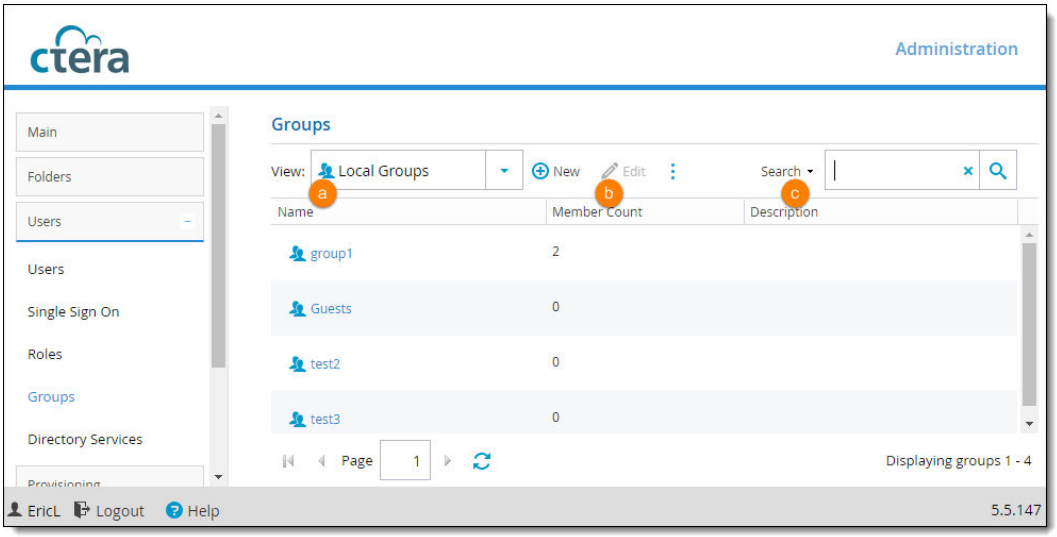
- To view only users from the directory service, select the Active Directory or LDAP directory name.
- To view groups defined in the local user database, select **Local Groups**.



ADDING AND EDITING USER GROUPS

To add or edit a user group:

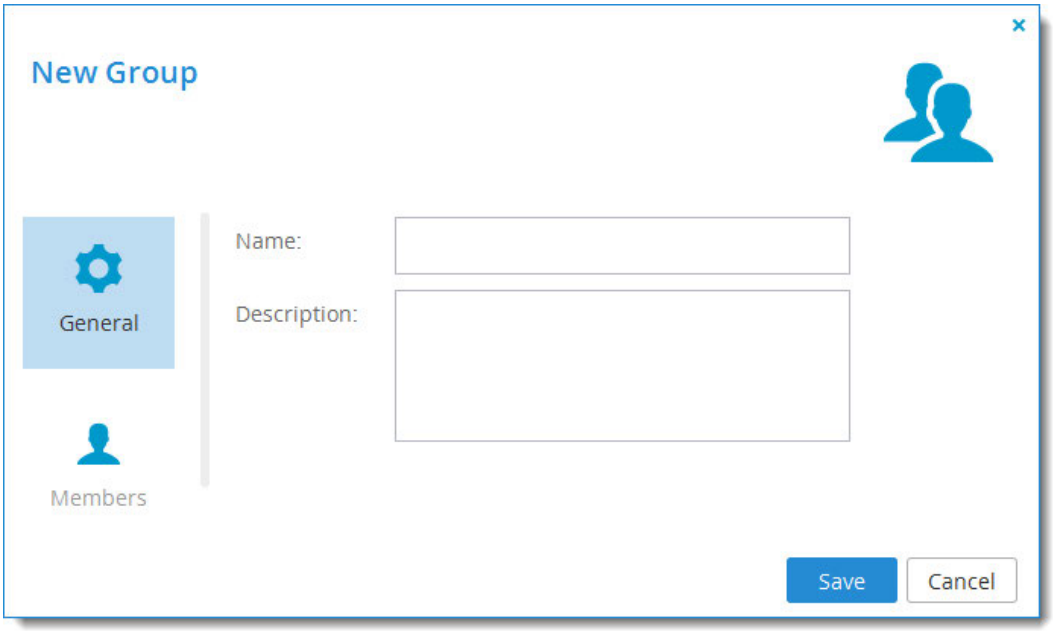
1 Select **Users > Groups** from the menu.
The **Users > Groups** page displays all user groups.



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**.

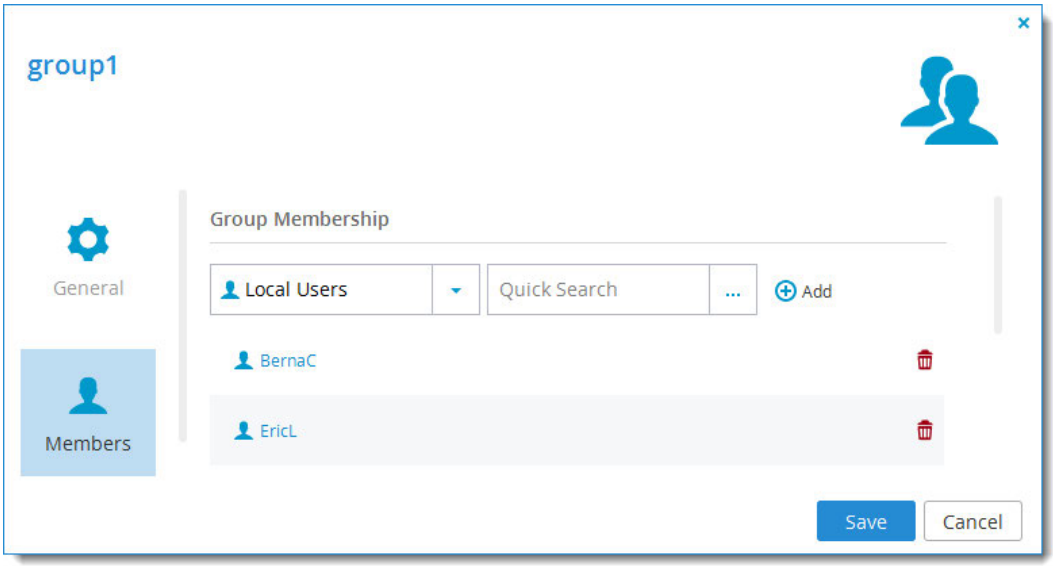
CONFIGURING USER GROUP MEMBERS

Note: User accounts can belong to multiple user groups.

Note: User accounts can be added to user groups as described in the following procedure or as described in Adding Users to Groups.

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 is displayed with a list of group members.

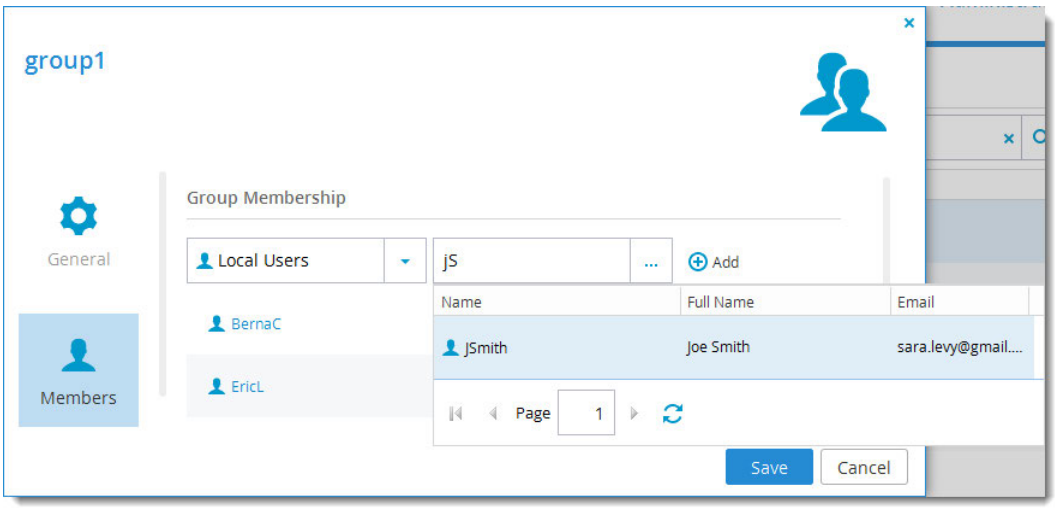


3 (Optional) To view only a specific type of users, in the **Show** drop-down list, do one of the following:

- 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 is displayed anywhere within the name of the desired user account, then click ...
A table of user accounts matching the search string is displayed.



b Select the desired user account in the table.
The user account is displayed 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

Note: 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

- How Directory Service Synchronization Works
- Integrating CTERA Portal with an Active Directory Domain, Tree, or Forest
- Integrating CTERA Portal with an LDAP Directory Server
- Integrating CTERA Portal with an Apple Open Directory Server
- Manually Fetching User Data

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
- Apple Open Directory

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.

Note: 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.

Note: 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.
- 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.

CTERA Portal handles special cases as follows:

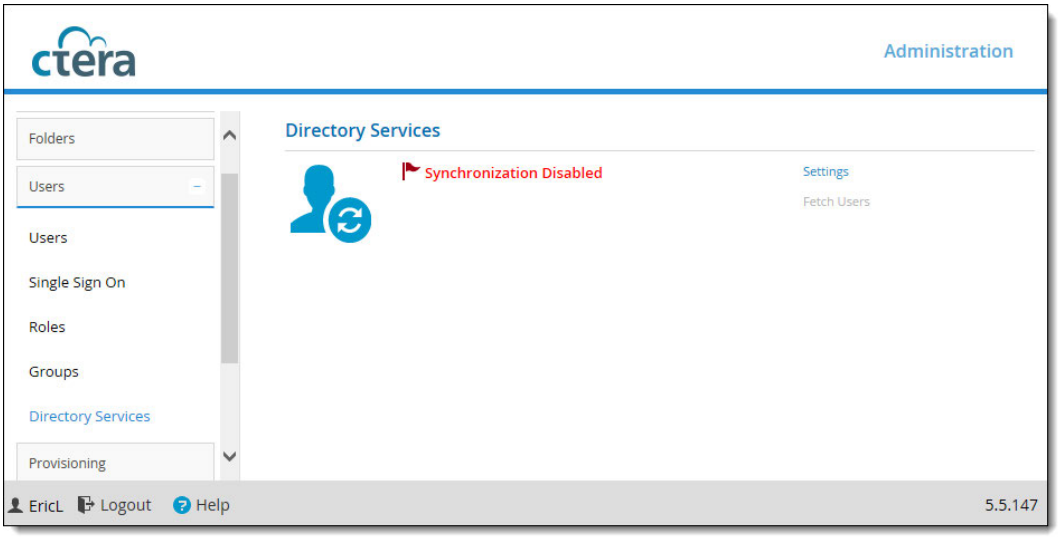
- If during the fetch it is determined that a user exists in the local user database but not in the directory, then the user is assumed to have been deleted, and CTERA Portal deletes the user from the local user database. The user's folders are not deleted.
- If the access control list specifies that 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.

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

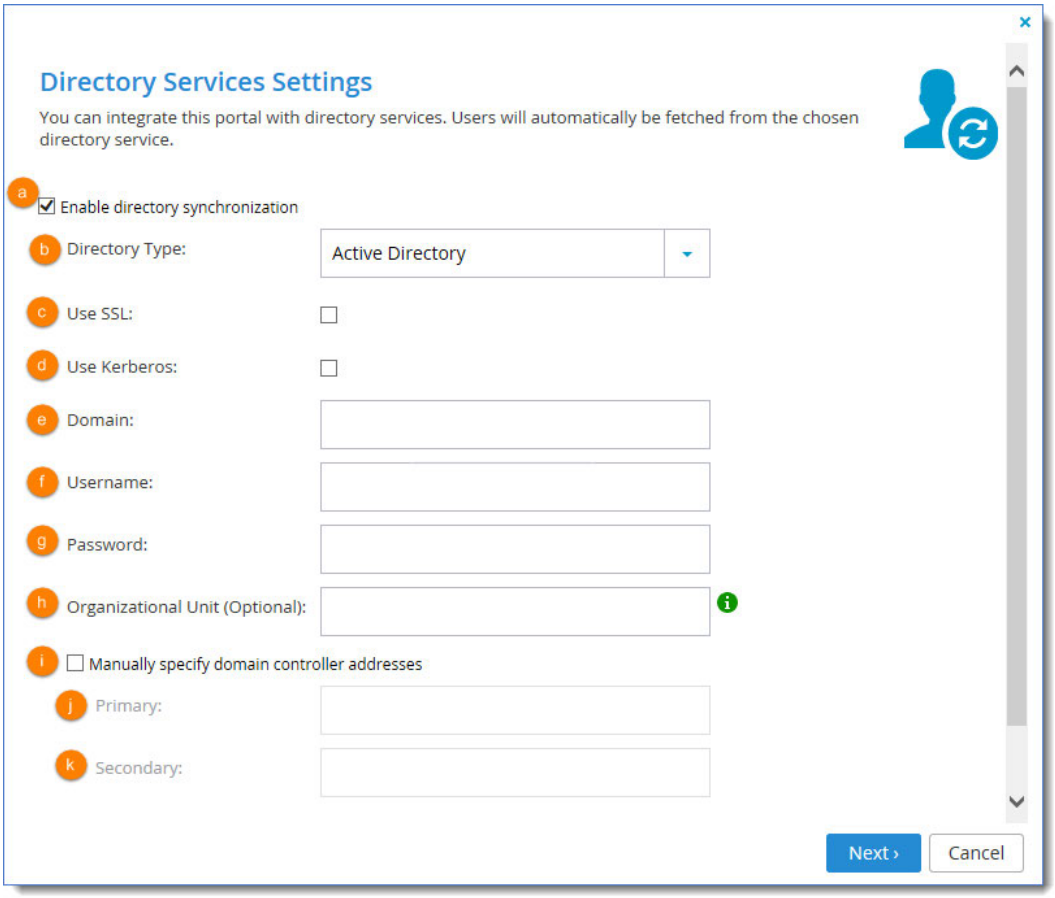
INTEGRATING CTERA PORTAL WITH AN ACTIVE DIRECTORY DOMAIN, TREE, OR FOREST

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

1 Select **Users > Directory Services** from the menu.
The **Users > Directory Services** page is displayed.



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.

Note: 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.

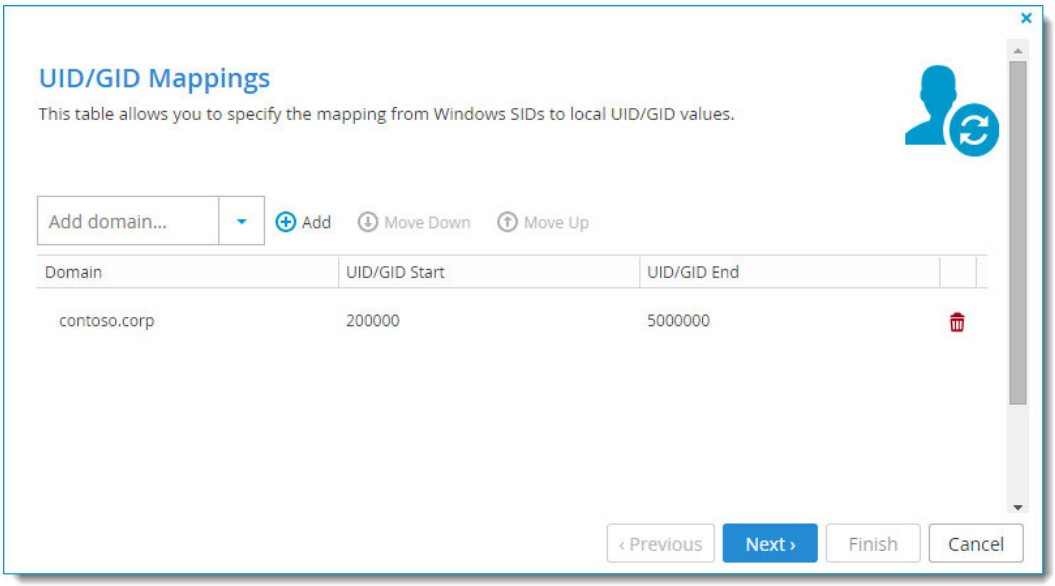
h **Organizational Unit** (optional). Type the name of the organizational unit (OU) within the Active Directory domain.

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 is displayed.



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 is displayed 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.

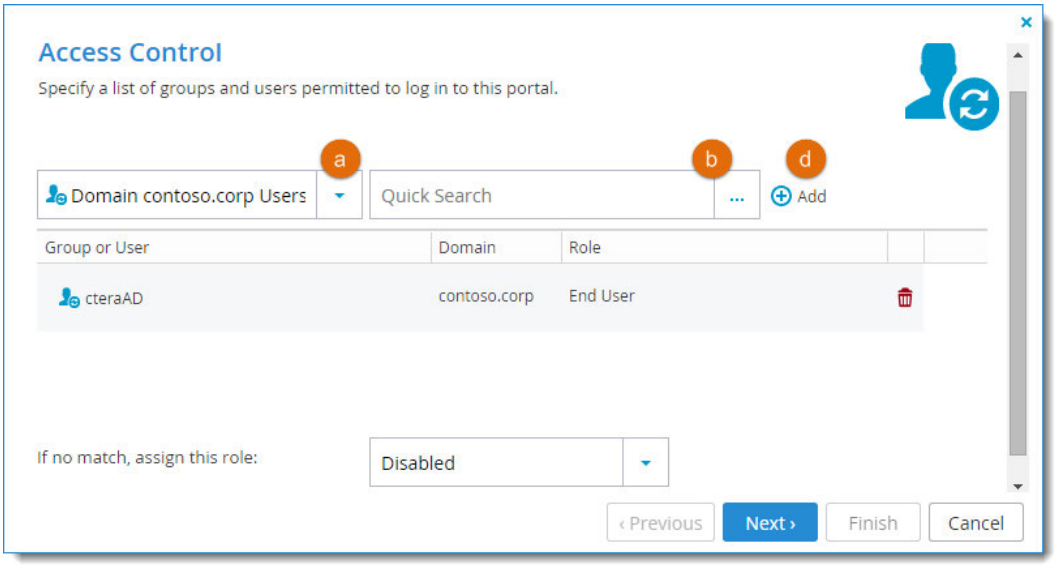
d Click in the **UID/GID End** field, and type the ending number in the range of CTERA Portal user and group IDs (UID/GID) that should be assigned to users and user groups from this domain.

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 is displayed.



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.

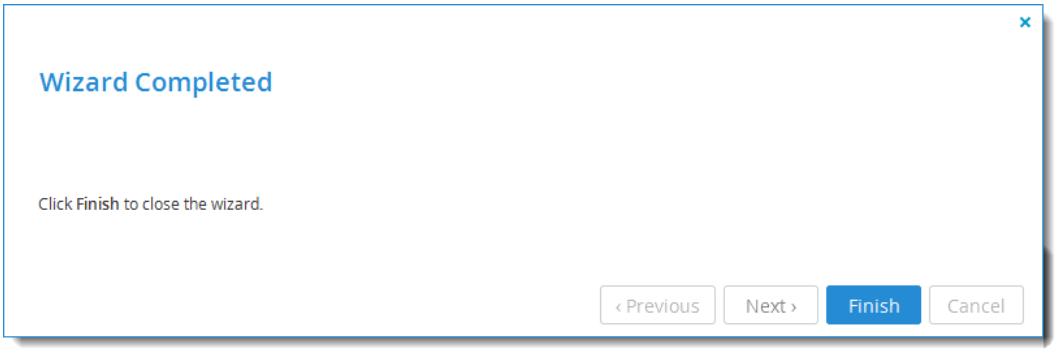
b In the **Quick Search** field, type a string that is displayed anywhere within the name of the user or user group you want to add, then click ...
A table of users or user groups matching the search string is displayed.

c Select the desired user or user group in the table.
The user or user group is displayed in the **Quick Search** field.

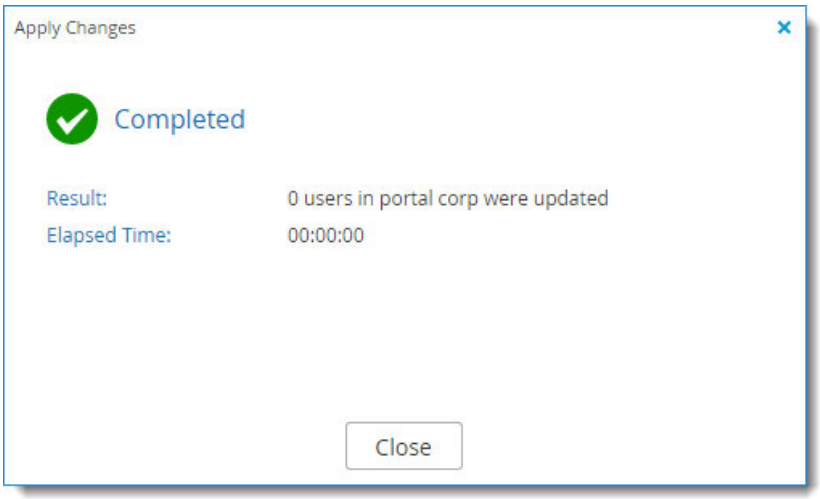
d Click **Add**.
The user or user group is added to the list of users and user groups who should have access to the virtual portal.

8 To remove a user or user group, in their row, click 🗑.
The user or user group is removed from the list.

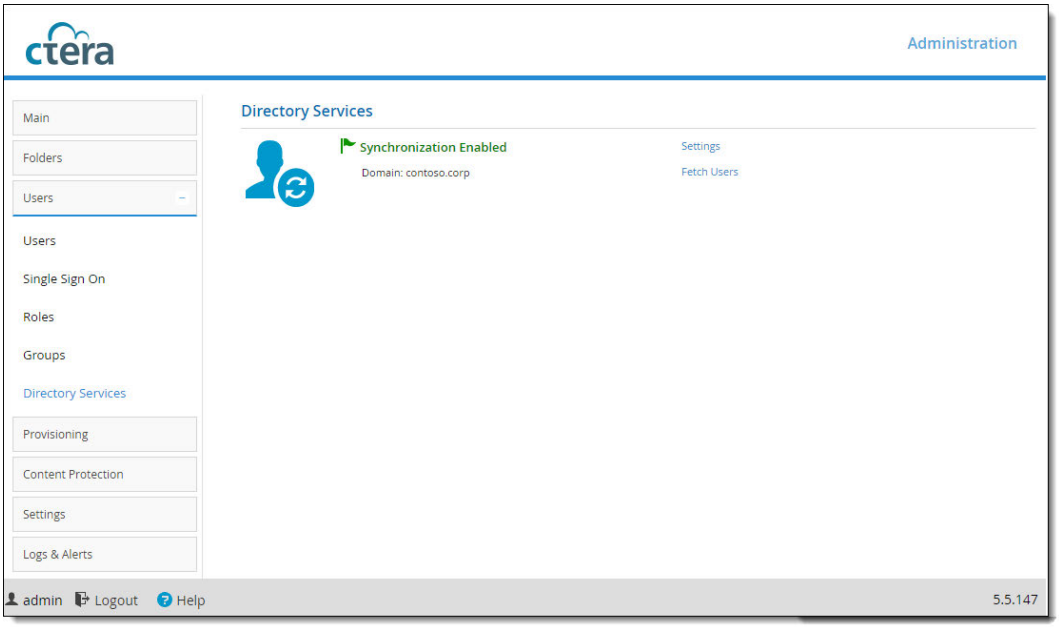
9 In each user and user group's row, click in the **Role** column, then select the desired user role from the drop-down list.
Options include **Disabled**, **End User**, **Read Only Administrator**, and **Read/Write Administrator**.
For information on these roles, see User Manager Profile Fields.
The **Wizard Completed** screen is displayed.



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 is displayed.



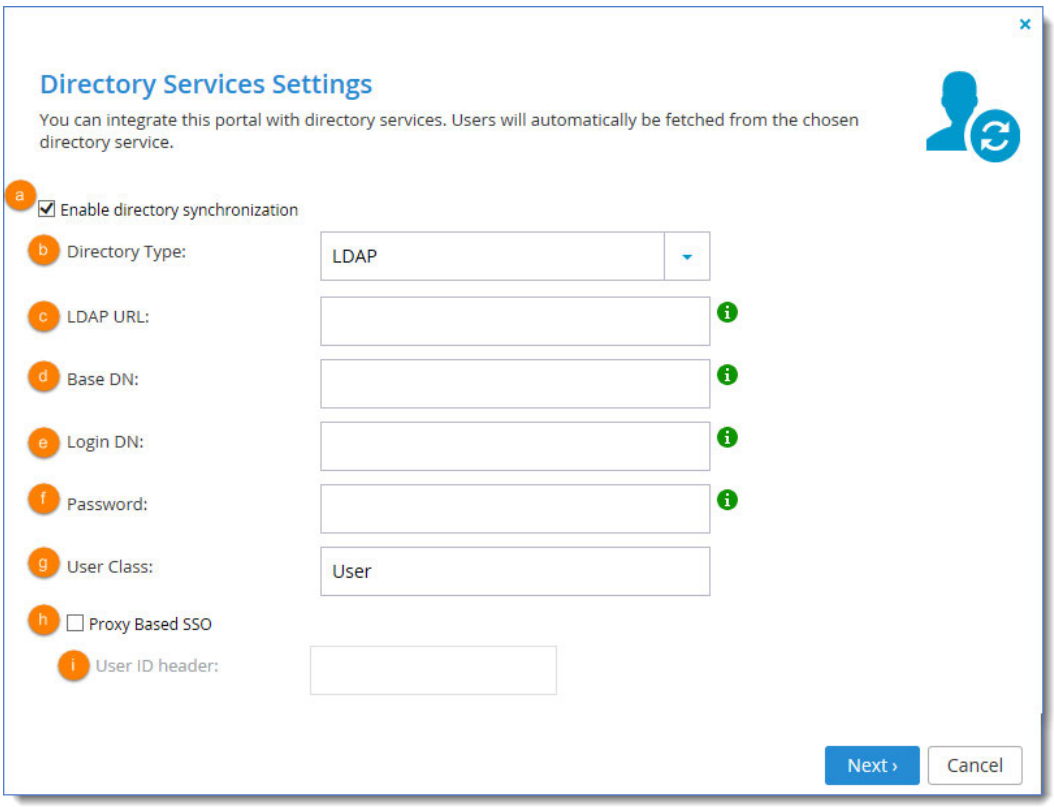
11 Click **Close**.
Synchronization with Active Directory is enabled.


ctera
Administration
Main
Folders
Users
Users
Single Sign On
Roles
Groups
Directory Services
Provisioning
Content Protection
Settings
Logs & Alerts
Directory Services
Synchronization Enabled
Domain: contoso.corp
Settings
Fetch Users
admin
Logout
Help
5.5.147

INTEGRATING CTERA PORTAL WITH AN LDAP DIRECTORY SERVER

To integrate a virtual portal with an LDAP directory:

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



2 Complete the fields:

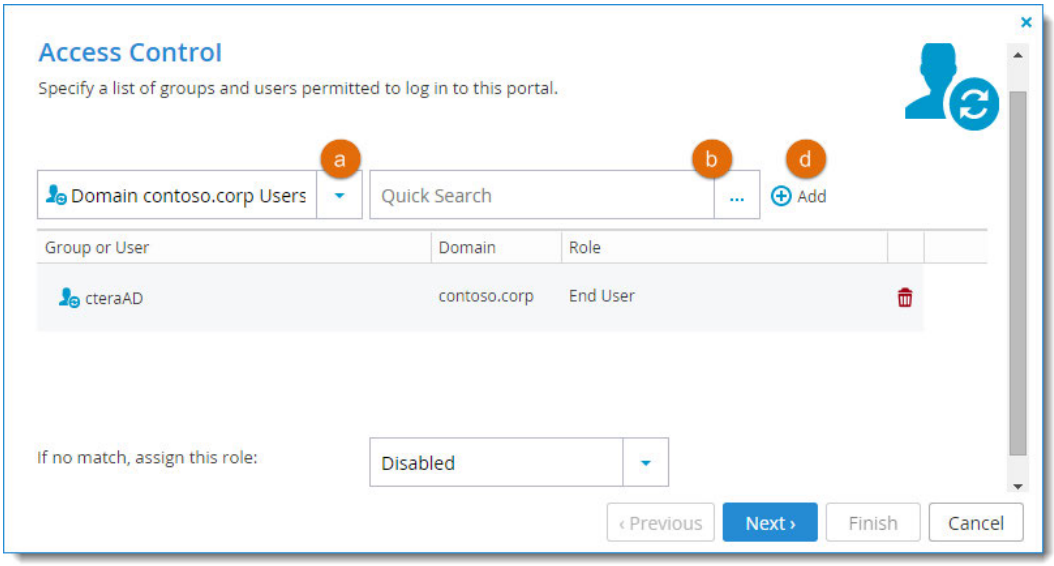
- a **Enable Directory Synchronization**. Select this option to enable integration with an LDAP directory service.
- b **Directory Type**. Select LDAP as the type of directory service with which to integrate CTERA Portal.
- c **LDAP URL**. Type the URL for connecting to the LDAP server.
- d **Base DN** (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 is displayed.

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 is displayed 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 is displayed.

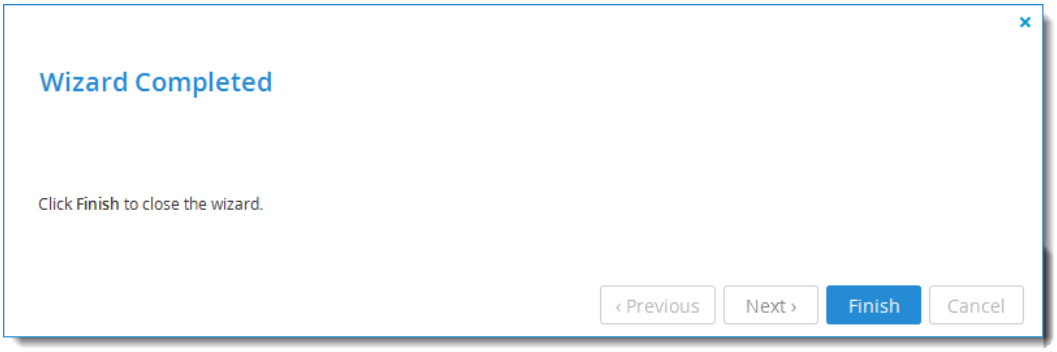
c Select the desired user or user group in the table.
The user or user group is displayed in the **Quick Search** field.

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.

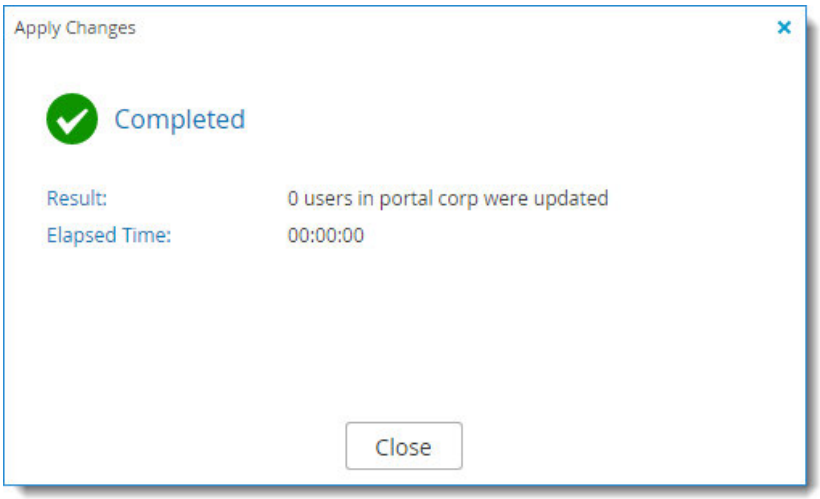
6 To remove a user or user group, in their row, click 🗑.
The user or user group is removed from the list.

7 In each user and user group's row, click in the **Role** column, then select the desired user role from the drop-down list.
Options include **Disabled**, **End User**, **Read Only Administrator**, and **Read/Write Administrator**. For information on these roles, see User Manager Profile Fields.

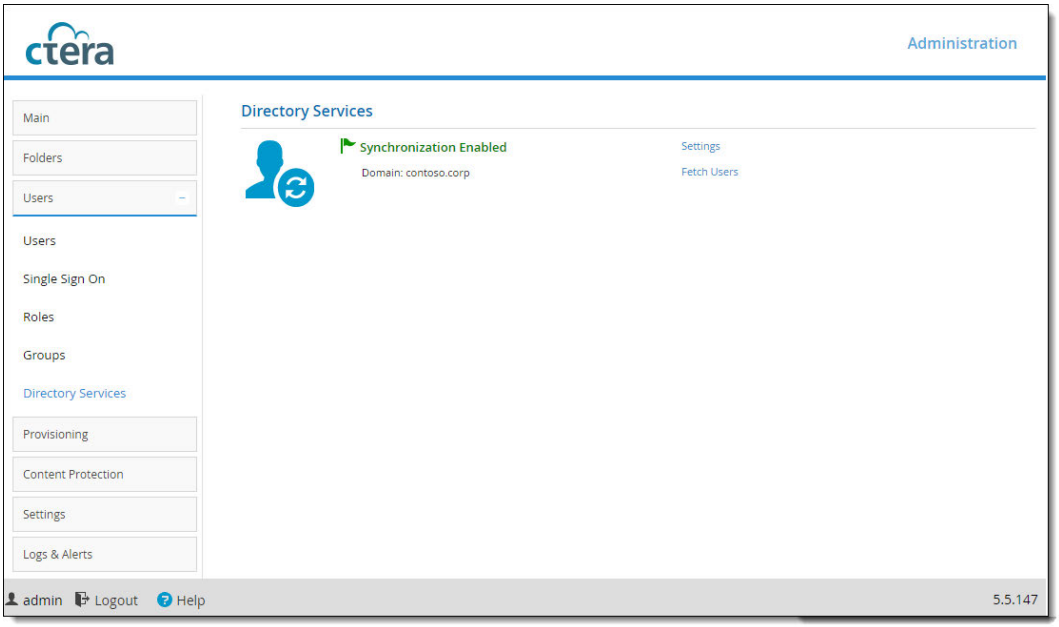
8 Click **Next**.
The **Wizard Completed** screen is displayed.



9 Click **Finish**. User data is fetched from the LDAP directory.
When the operation is complete, the **Completed** screen is displayed.



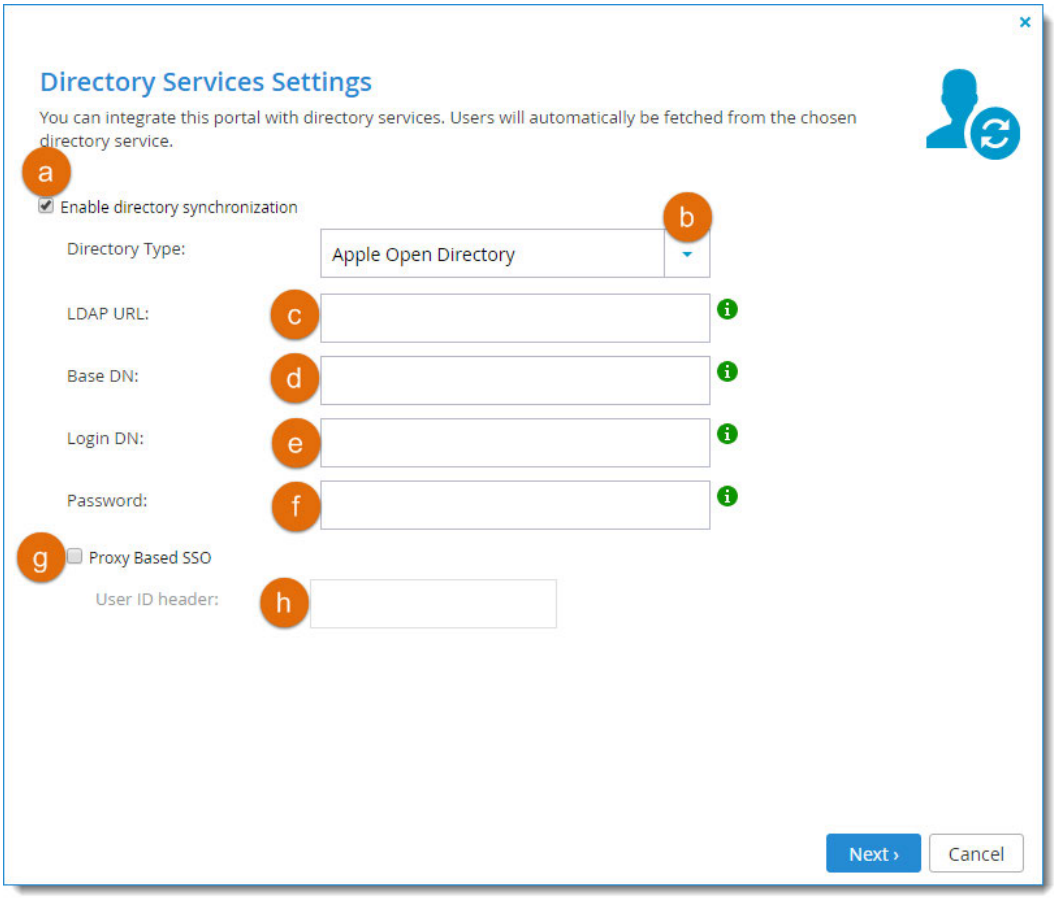
10 Click **Close**.
Synchronization with the LDAP directory is enabled.



INTEGRATING CTERA PORTAL WITH AN APPLE OPEN DIRECTORY SERVER

To integrate a virtual portal with an Apple Open Directory server:

1. In the navigation pane, click **Users > Directory Services**.
   The **Users > Directory Services** page is displayed.
2. Click **Settings**.
   The **Directory Services Wizard** opens, displaying the **Synchronization Settings** dialog box.



3 Complete the fields:

- a **Enable Directory Synchronization**. Select this option to enable integration with an Apple Open Directory server.
- b **Directory Type**. Select Apple Open Directory as the type of directory service with which to integrate CTERA Portal.
- c **LDAP URL**. Type the URL for connecting to the Apple Open Directory server.
- d **Base DN**. Type the base DN of the Apple Open Directory server. (Optional.)
- e **Login DN**.Type the distinguished name of a user with full user read rights, used for binding (authenticating) to the Apple Open Directory server (also known as bind DN).
- f **Password**. Type the password to use for binding (authenticating) to the Apple Open Directory server.
- g **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**. The proxy server passes the user's identifier in an HTTP header.
- h **User ID Header**. If you checked proxy-based SSO, enter the attribute that your access manager adds to each incoming HTTP request.

4 Click **Next** and continue through the wizard.

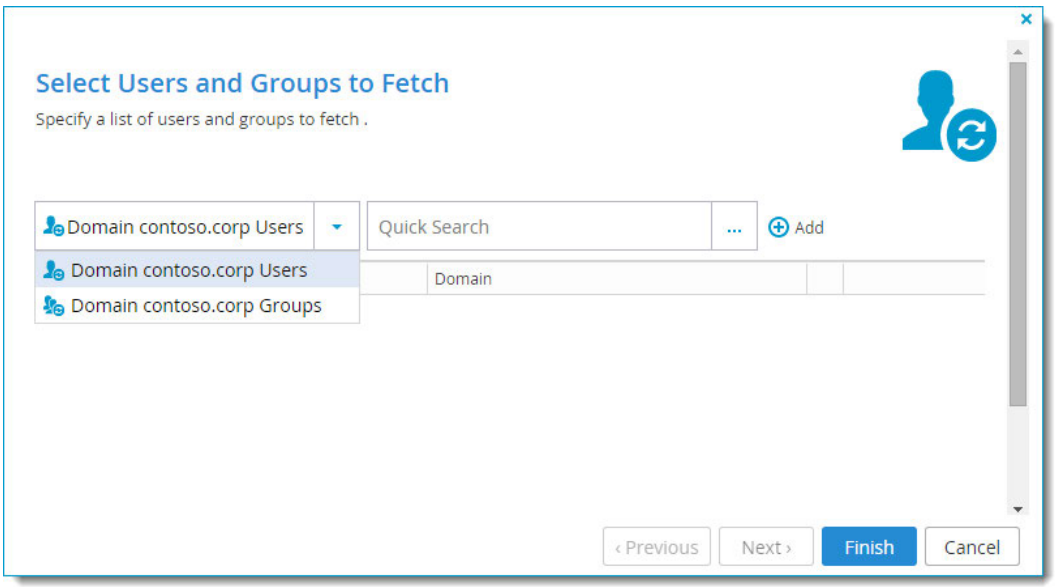
MANUALLY FETCHING USER DATA

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 is displayed.
2. Click **Fetch Users**.
   The **Fetch Users Wizard** opens, 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 is displayed 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 is displayed.
   c. Select the desired user or user group in the table.
      The user or user group is displayed 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 is displayed. 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 is displayed.
6. Click **Close**.

11

PROVISIONING

In this chapter

- Overview
- Viewing Plans
- Adding and Editing Plans
- Setting/Removing the Default Plan
- Automatically Assigning Plans
- Exporting Subscription Plans to Excel
- Applying Provisioning Changes
- Deleting Subscription Plans

OVERVIEW

Plans

Users in the team portal obtain services through subscription plans for an open-ended period of time without payment.

A team portal is subscribed to a global plan that determines the maximum licenses and snapshot retention policies for the whole portal. A default user subscription plan is created automatically and contains the licenses specified in the global plan. All user accounts are assigned to this default plan.

You can create alternate subscription plans and assign those to individual user accounts. You can change the default plan that is assigned to users. You can also define conditions for automatically assigning plans to users based on user attributes.

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.

  Note: 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.

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

  Example 1:
  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:
  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:
  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:
  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 Storage 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 Cloud Storage 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 Storage Gateway or Cloud Agent.

When a CTERA Cloud Storage Gateway or CTERA Cloud Agent initiates a Cloud Backup job, the CTERA Portal automatically creates a snapshot of the cloud storage 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.

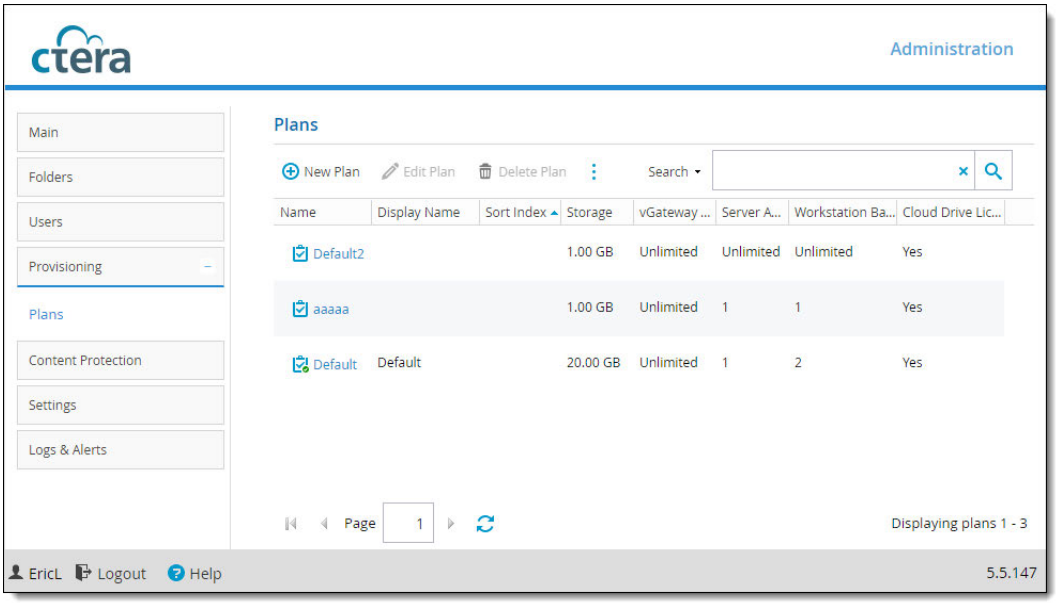
Snapshot Consolidation

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:

- Select **Provisioning > Plans** from the menu.
  The **Provisioning > Plans** page opens, displaying all subscription plans.



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

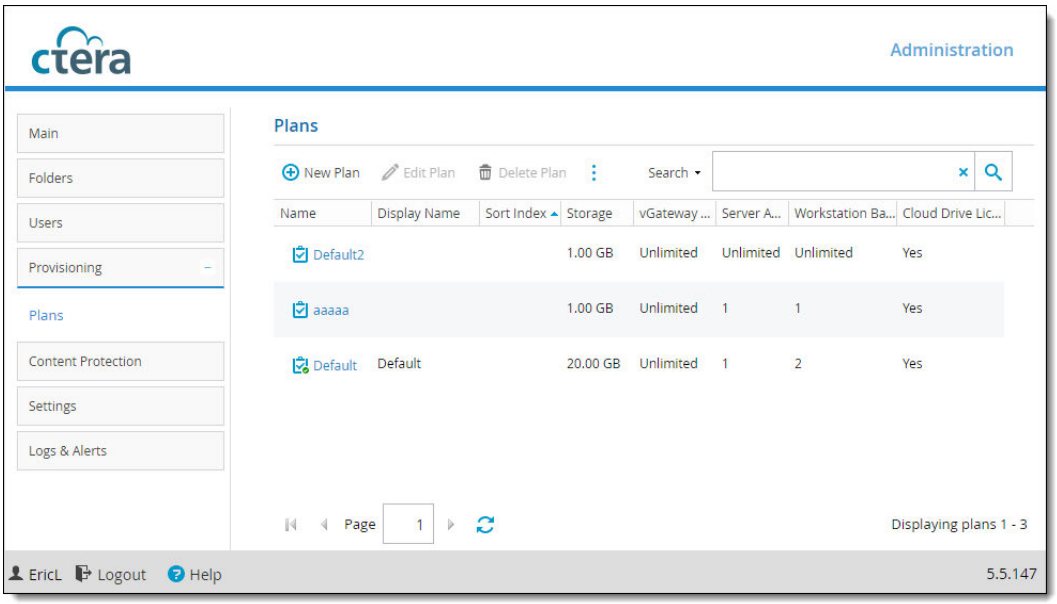
This field...	Displays...
Name	The subscription plan's name. To edit the subscription plan, click the subscription plan name. For further details, see Adding and Editing Plans.
Display Name	The subscription plan's name, as displayed in the End User Portal and notifications.
Sort Index	An index number 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.
vGateway Licenses	The number of CTERA virtual gateway licenses included in the plan. A CTERA Virtual Gateway license is consumed by a CTERA Virtual 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.

This field...	Displays...
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:

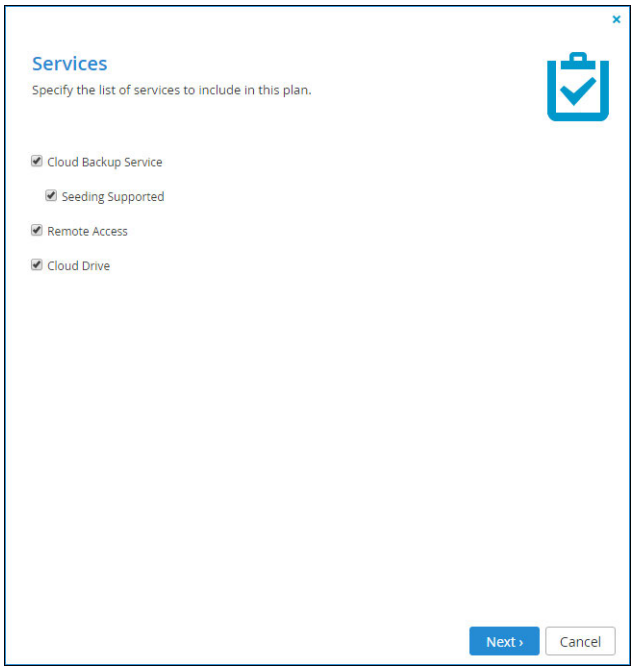
1 Select **Provisioning > Plans** from the navigation pane.
The **Provisioning > Plans** page opens, displaying all subscription plans.



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.

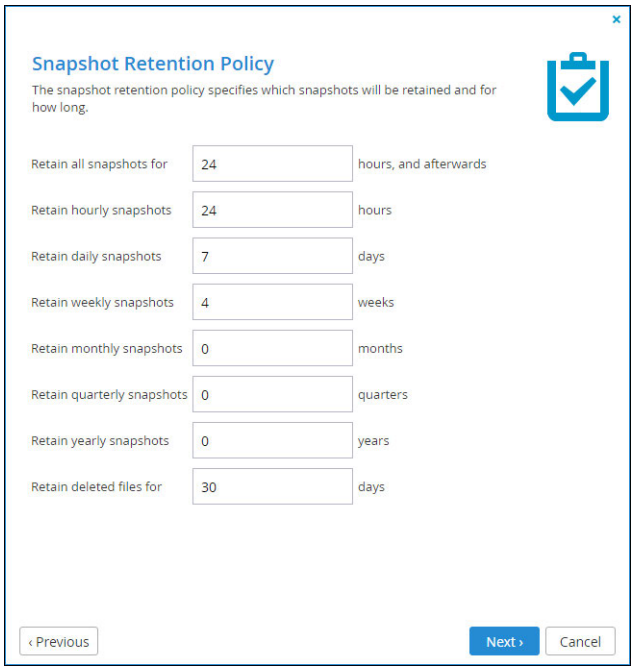
Seeding Supported – Select this option to include backup seeding in the subscription plan.

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.

4 Click **Next**.



5 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.

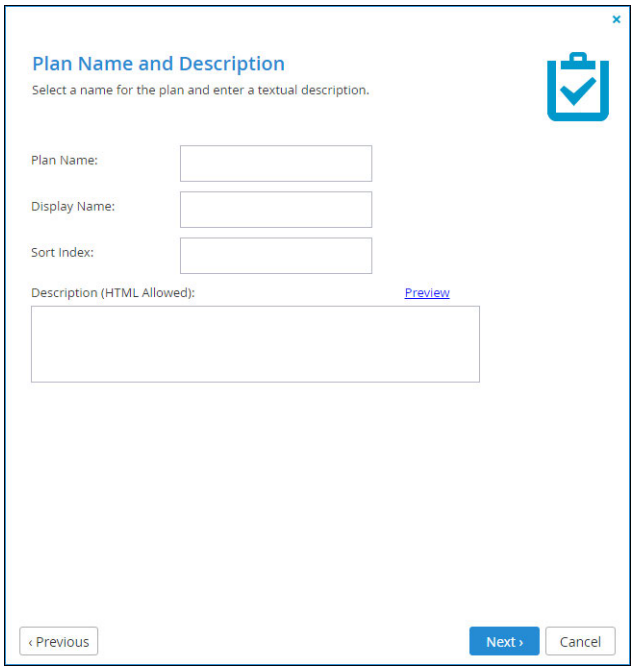
Retain yearly snapshots. Type the number of yearly snapshots that should be retained.

Retain deleted files for – Type the number of days to retain deleted files.

Note: For an explanation of each policy, see Snapshot Retention Policies.

6 Click **Next**.

The **Plan Name and Description** dialog box is displayed.



7 Fill in the name and description for the plan:

Plan Name – Type a name for the subscription plan.

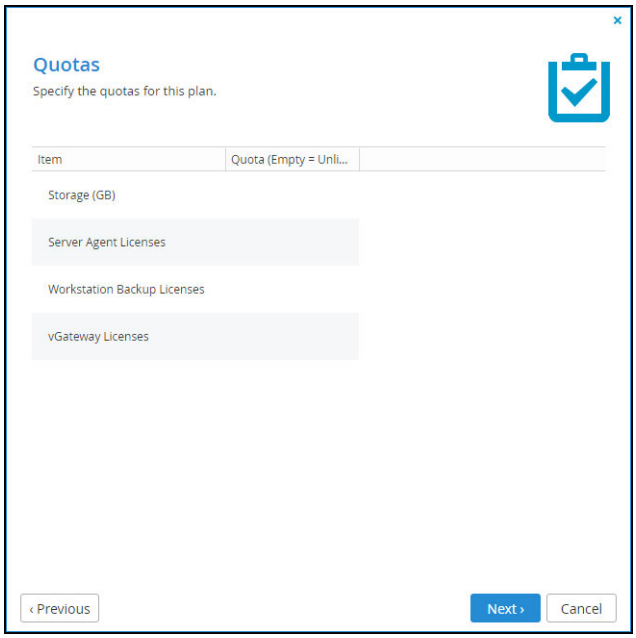
Display Name – Type the name to use when displaying this subscription plan in the End User Portal and notifications.

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.

8 Click **Next**.



9 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 100GB of storage space, click in the Storage Quota (GB) item's **Quota** field and type 100.

Note: The specified license quotas must not exceed the number specified in the license. An error message is displayed when you attempt to assign a user to a plan with a quota that exceeds the number specified in the license.

10 Click **Next**.
The **Wizard Completed** screen is displayed.

11 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 is displayed.

12 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 opens, 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 opens, 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 plans will be assigned to which users.

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

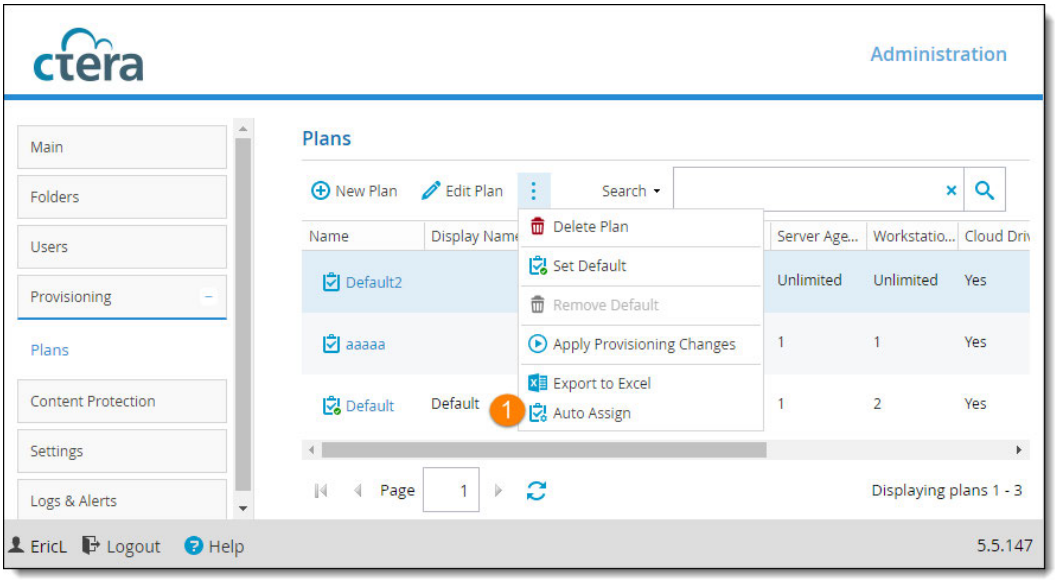
- Username
- User Groups
- Role
- First Name
- Last Name
- Company
- Billing ID
- Comment

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.

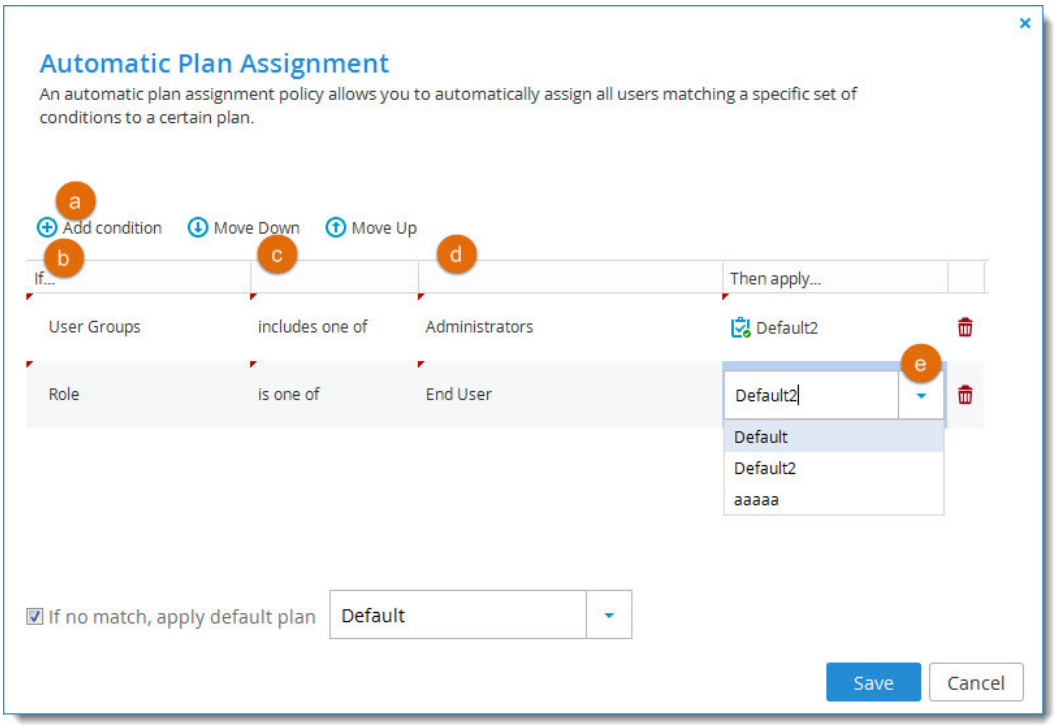
This feature is particularly useful if the portal is integrated with a Directory Service (Using Directory Services. It allows you to define a policy even before users have joined the service, so that when users join, they will be automatically assigned the appropriate quota and licenses.

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 opens, 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 opens, 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 is displayed.

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.

12

CONTENT PROTECTION

In this chapter

- Cloud Drive Policy
- Collaboration Policy
- Collaboration Permissions

CLOUD DRIVE POLICY

Cloud Drive policy determines the type of data that can be synchronized through CTERA Cloud Agents, Cloud Storage Gateways and CTERA Mobile apps, 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:

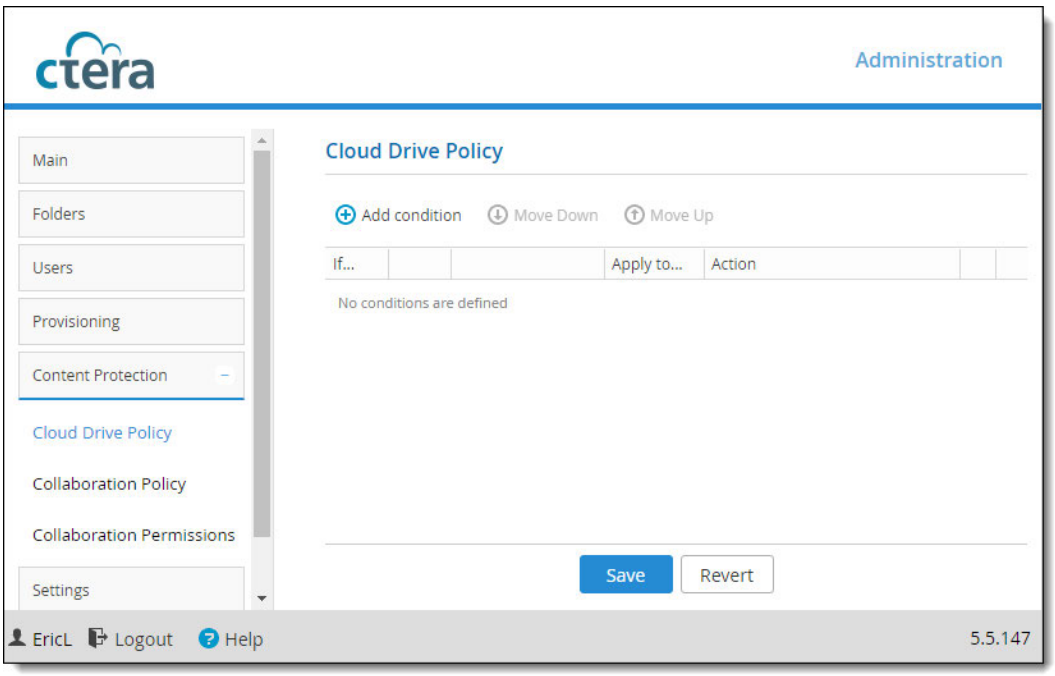
- File Size
- File Name
- File Type

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.

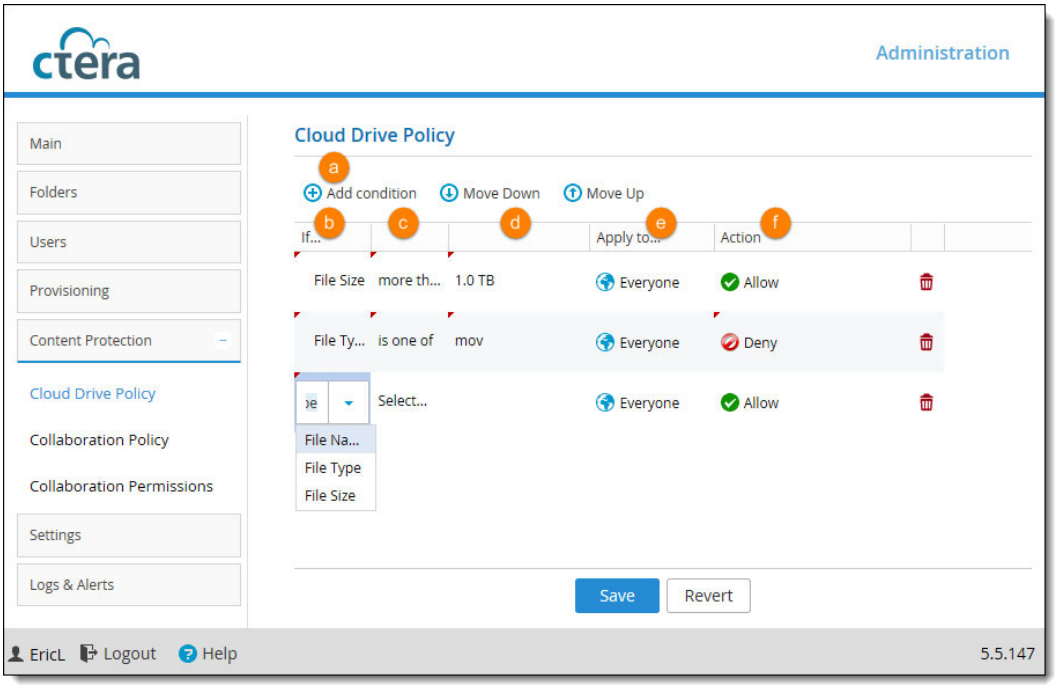
In addition, it is possible to apply Cloud Drive policy rules to external users (that is, users who were invited to collaborate by email address or by means of a public link), by using a special group called *External Users*.

To configure Cloud Drive policy:

1 Select **Content Protection > Cloud Drive Policy** from the menu.



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**.

COLLABORATION POLICY

CTERA Portal enables you to implement a corporate data sharing policy for collaboration with external users. Using the **Content Protection > Collaboration Policy** page, you can define a policy to restrict external collaboration by specific users or groups and define the sanctioned collaboration domains.

Note: Actions performed on data shared with users outside of your corporate domain are logged in the access log, **Logs & Alerts > Event Log**, (Viewing Access Logs) and visible to the content owner, collaborators, and portal administrators.

Collaboration policy rules control:

- Which portal members can enable which external users to collaborate on data stored on the portal.
- What minimum type of authentication those external users will need to use if your portal users share data with them.
- The highest level of access permission the external users can be allowed by the specified portal members.

Optionally, each policy rule can apply to a subset of your portal members, allowing different collaboration rules for different portal users.

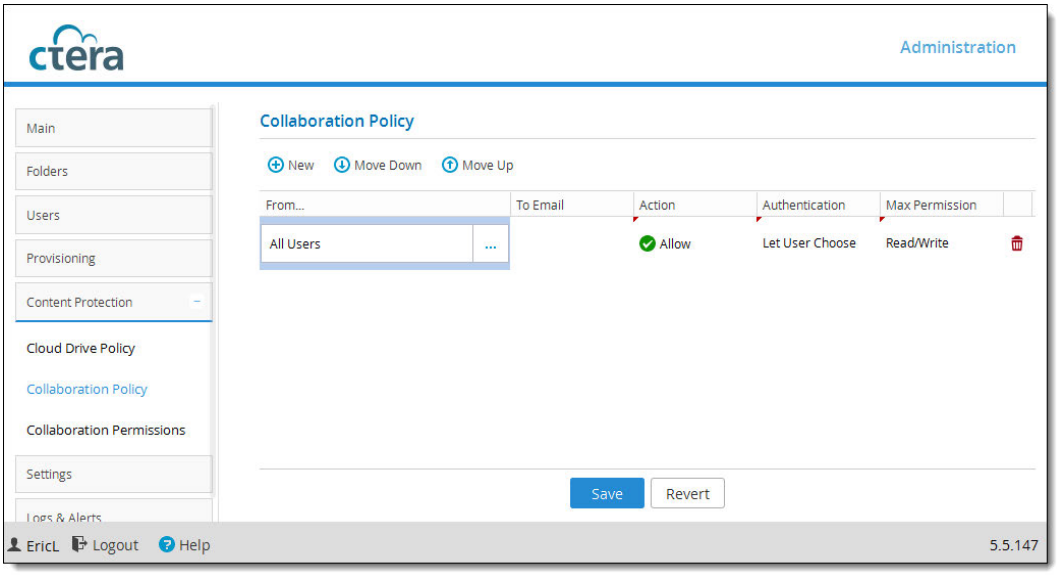
You can move rules up and down the list on the policy page. When a user invites an external user to collaborate, the first rule on the list, from the top downwards, that matches the external users' email address applies.

Note: Any external user email address which is not specifically denied by any collaboration policy rule will be allowed to collaborate.

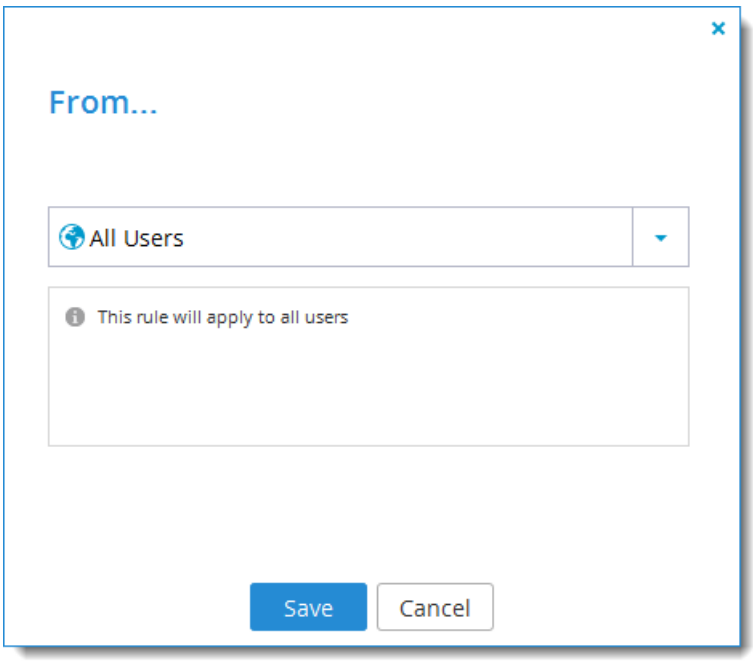
Note: The policy is not applicable to files and folders shared via public links or collaboration with internal users. Collaboration limits for internal users can be set via the Collaboration Permissions page.

To add a collaboration policy rule:

1 In the **Content Protection > Collaboration Policy** page, click **New**.
A rule's row is added to the list.



2 Click in the newly added row in the **From** column and then click ...



3 Use the and the search box to specify which user(s) or user group the rule will apply to. Click **Save** when you're done.

Note: To create user groups, go to the **Users > Groups** page.

4 In the **To Email** column, specify which external recipient email address(es) the rule will apply to. You can enter an email address or you can specify an entire domain, by using wildcards. For example, to specify all gmail addresses, enter `*@gmail.com` or `@gmail.com`.

5 In the **Action** column, choose one of:
   - **Allow**. To allow the specified user or user group to collaborate on files and folders with external users at the specified email addresses.
   - **Deny**. To deny the specified user or user group to collaborate on files and folders with external users at the specified email addresses.

6 In the **Authentication** column, set which authentication methods the external users will have to use in order to access the shared files or folders:
   - **Let User Choose**. Let the portal end user choose which authentication method to use to authenticate the external user for access to the shared file or folder.
   - **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.
   - **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.

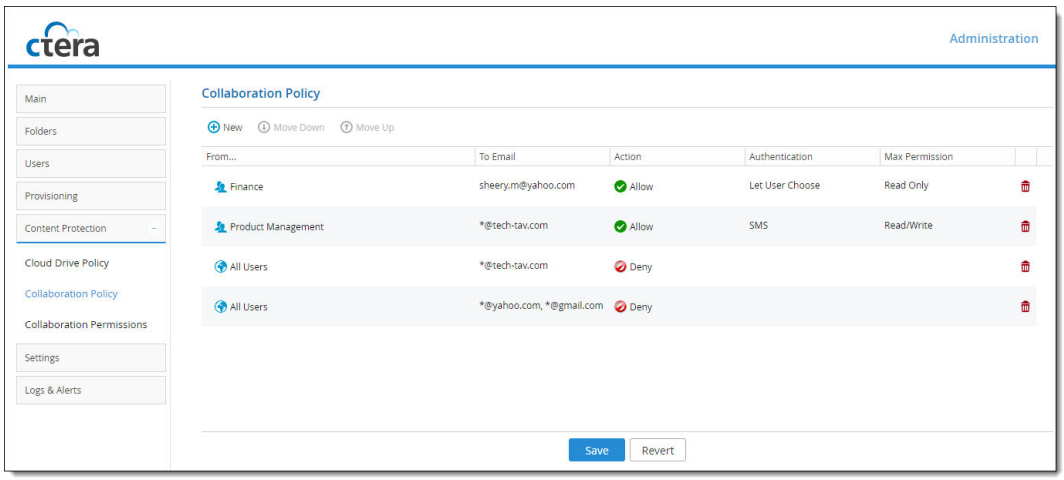
7 In the **Max permission** column, set the highest permission level that the user can grant the external collaborator on any shared files:
   - **Read/Write**
   - **Read Only**
   - **Preview Only**

   Note: *Preview Only* share recipients are able to view the file using the portal's integrated document preview server. The file is protected with a watermark that includes the recipient's email or IP address. Users with *Preview Only* permission are unable to download, copy, or print the file. In addition, content shared in *Preview Only* mode cannot be synchronized for offline access by CTERA Agents, Cloud Storage Gateways, or CTERA Mobile.

8 Click **Save**.

Collaboration Policy Example

Consider this example:



If a member of the *Finance* group invites *sheery.m@yahoo.com* to collaborate on a file or folder, the collaboration will be allowed, the *Finance* group member will be able to choose any authentication method, and *sheery.m@yahoo.com* will have read only access to the file or folder.

If any user who does not belong to the *Finance* group tries to invite *sheery.m@yahoo.com* to collaborate, the collaboration will be denied. If the first rule were moved down to below the fourth rule, then even *sheery.m@yahoo.com* would be denied all collaboration access even if the invitation is sent by a member of the *Finance* group. Likewise if a *Finance* group member tries to invite a different *yahoo.com* email address.

COLLABORATION PERMISSIONS

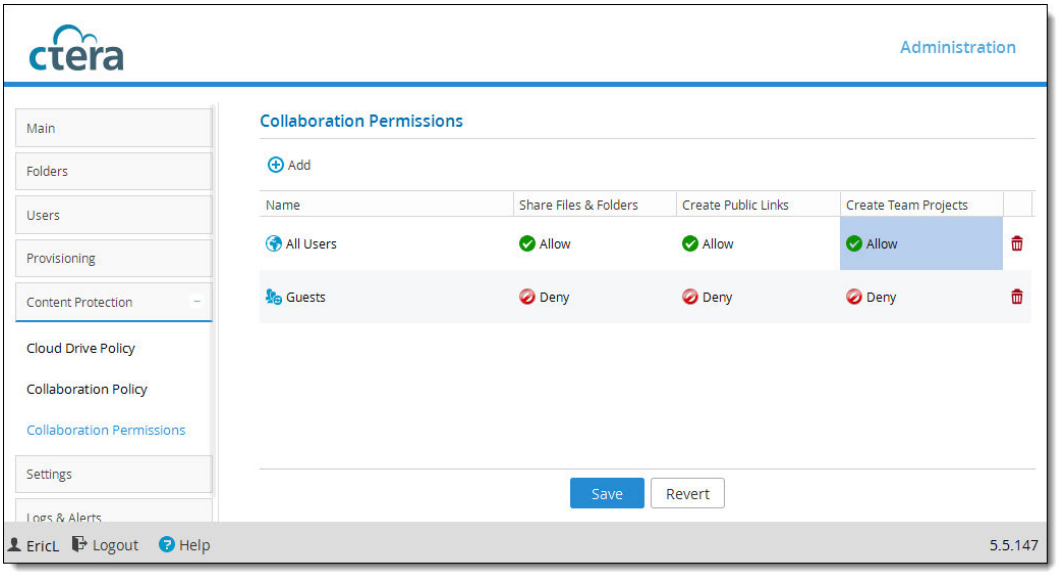
Users and groups can share files and folders through the end user portal, create public links for access to files and folders, and they can create team projects (these are shared folders without individual owners).The **Collaboration Permissions** page enables you to restrict users' permissions to collaborate. You do this by defining rules that give the desired permissions to specified users or user groups.

Rules defined in Collaboration Permissions are processed as follows:

- User rules get precedence over group rules.
- *Deny* rules have higher priority than *Allow* rules.

To add a collaboration permissions rule:

1. In the **Content Protection > Collaboration Permissions** page, click **Add**.
   A row is added.



2 Click the new row in the **Name** column and select a user or user group or *All Users*. This specifies which users the rule will apply to.

3 Click in the other columns and select **Allow**/**Deny** for each action. The actions you can allow or deny are:

   a **Share files and folders**. Users can share files or folders with specified users, groups, or external email addresses, and specify the type of access each collaborator can have. The access types that the user can choose from for their collaborators (for example, preview only, read only, etc.) may be limited by the Collaboration Policy.

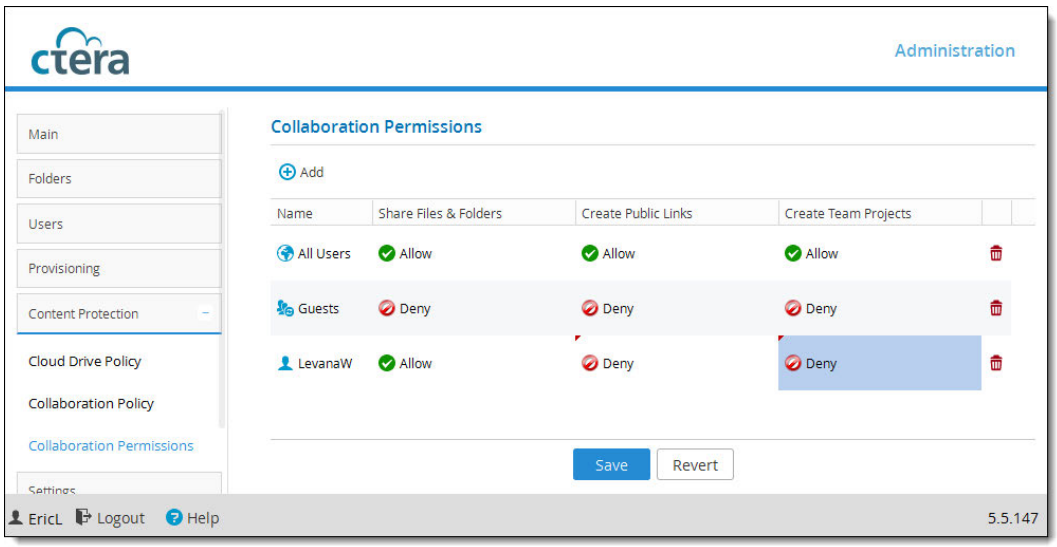
   b **Create public links**. Users can create a public link to any folder or file and then send the link to anyone else they choose. The user can set an expiration date.

   c **Create Team Projects**. These are shared folders which, once created, no longer appear to users as shared by an owner because they are intended for team collaboration.

4 Click **Save**.

Collaboration Permissions Example

Consider this example:



Suppose Dan Blue and Levana White both belong to the *Guests* group. Vered Pink is another user who does not belong to the *Guests* group.

According to the rules shown in the example:

- Vered has permission to share files and folders, create public links, and create team projects, since she is one of *all users* who are allowed all of those permissions and there is no rule denying her any collaboration permissions.
- Dan has no collaboration permissions at all, since he is a member of the *Guests* group which is denied collaboration permissions, and the group rule takes precedence over the *all users* rule, and there is no user rule allowing him any collaboration permissions.
- Levana has permission to share files and folders, but not to create public links or create team projects. This is because there is a specific rule for her as a user that allows her to share files and folders. That rule takes precedence over the *Guests* group rule, which would deny her all collaboration permissions, since user rules take precedence over group rules.

13

CONFIGURING VIRTUAL PORTAL SETTINGS

In this chapter

- Changing the Settings
- Password Policy
- Support Settings
- App Stores URL Settings
- General Settings
- User Registration Settings
- Team Portal Settings
- Default Settings for New Folder Groups
- Default Settings for New User
- Cloud Drive Settings
- Public Links
- Collaboration
- Remote Access Settings
- Advanced

Virtual portal settings include:

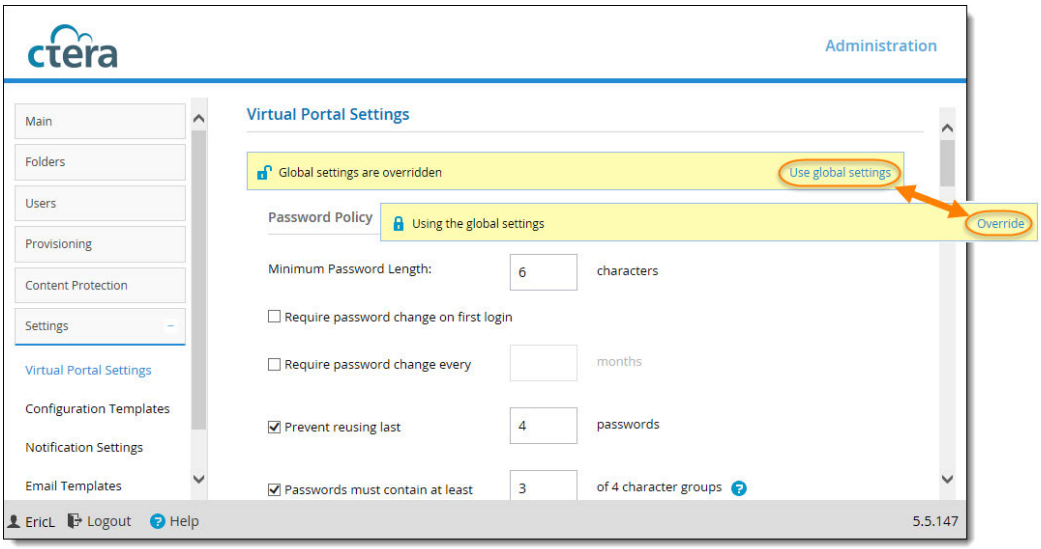
- Password policy
- Customer Support contact details
- App store URLs
- How long registration invitations to users are valid for
- Whether the folders of users who have no quota should be automatically deleted after a period of time
- Collaboration restrictions
- Remote access settings
- and many more

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**.

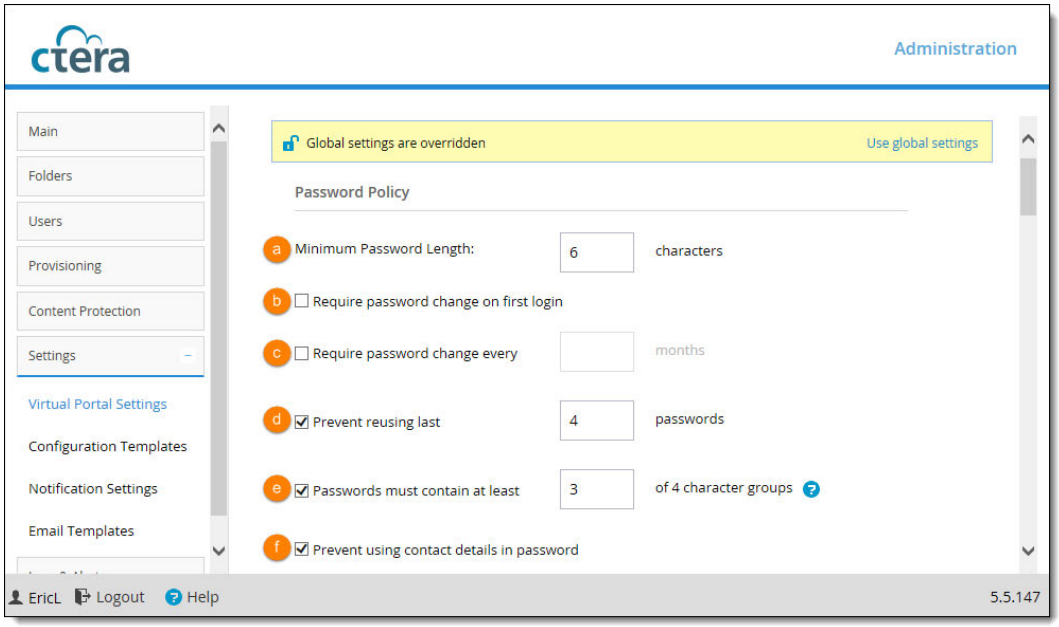


3. Change settings as required in the **Settings > Virtual Portal Settings** page.
4. Scroll down to the end of the page and click **Save** to save your changes.

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.

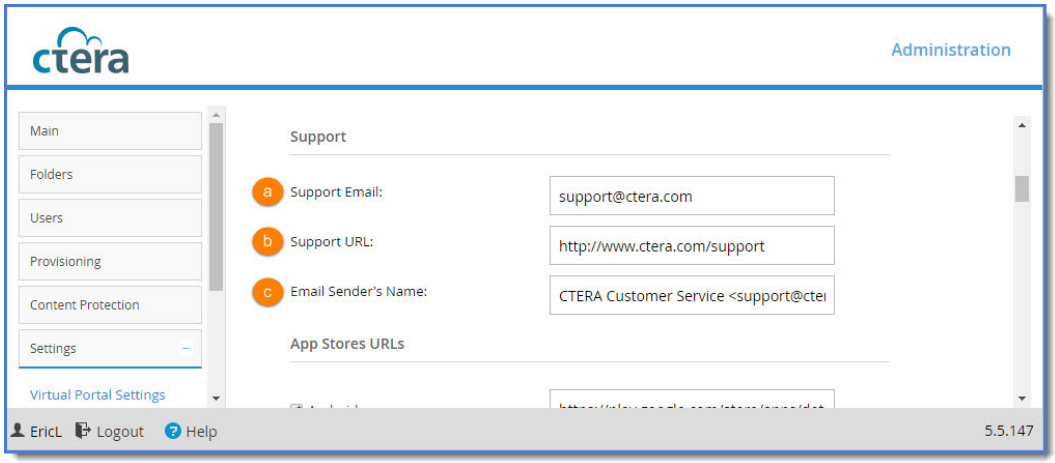
d **Prevent reusing last... passwords**. Select this option to prevent users from reusing a specified number of their previous passwords when they change their password. Specify the number of previous passwords you want this to apply to.

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:

- Lowercase characters
- Uppercase characters
- Numerical characters
- Special characters such as “!@#$”

f **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

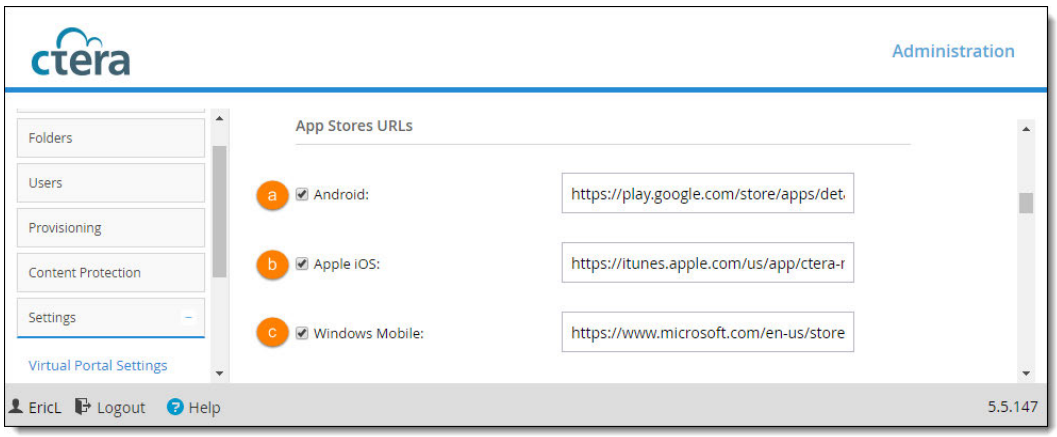


a **Support Email**. Type the email address to which support requests should be sent. This email address will appear in the From field of all email notifications sent by the CTERA Portal system.

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>`.

APP STORES URL SETTINGS

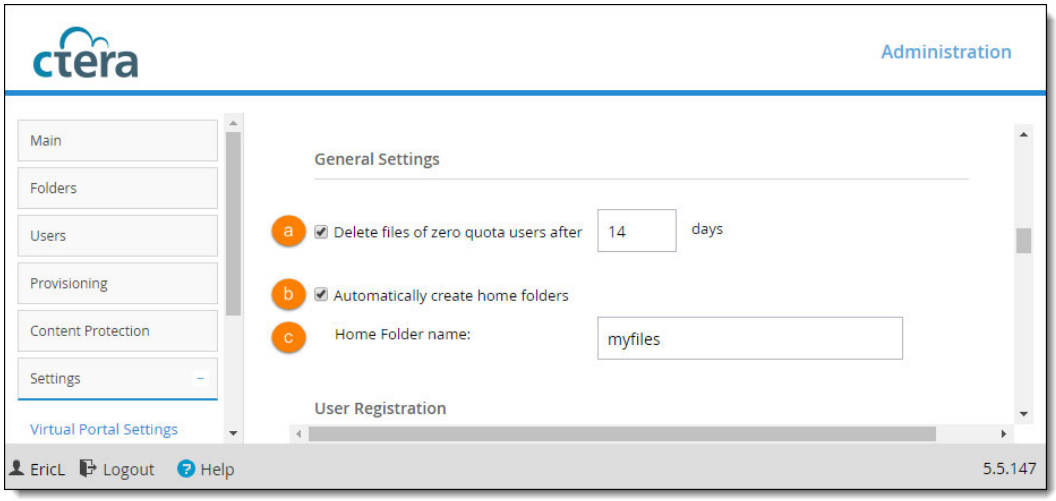


a **Android**. The URL of the Android app store.

b **Apple iOS**. The URL of the Apple app store.

c **Windows Mobile**. The URL of the Windows Mobile app store.

GENERAL SETTINGS

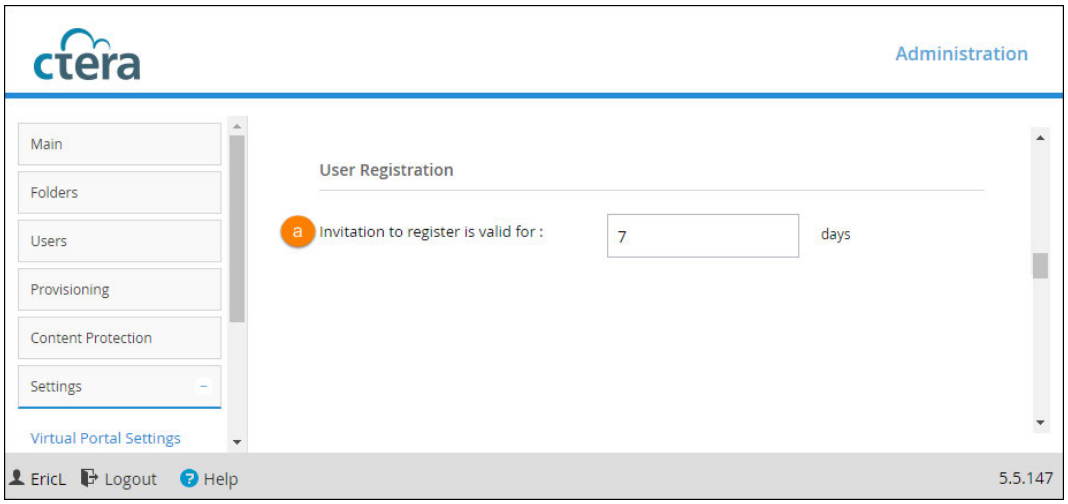


a **Delete files of zero quota users after**. Select this option to specify that the storage folders of customers who have no quota (for example, customers with expired trial accounts) should be deleted automatically after a certain number of days, then specify the desired number of days in the field 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.

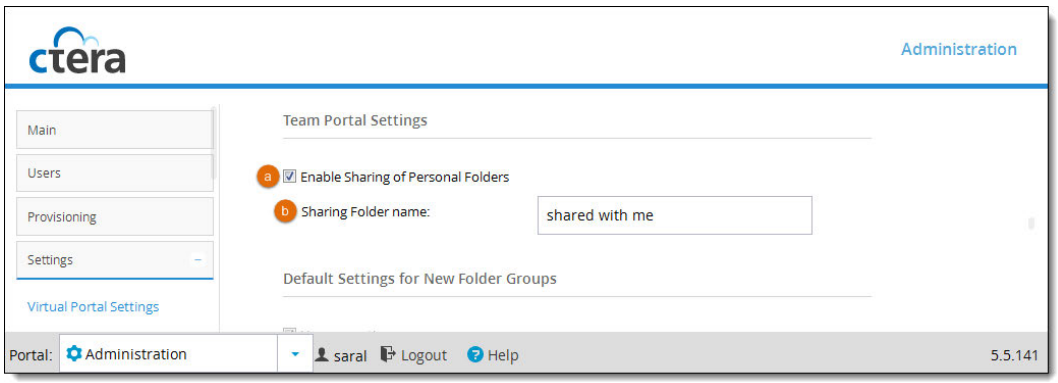
c **Home Folder name**. The name of the personal folder created for each new user account. Relevant only if Automatically create home folders is enabled.

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.

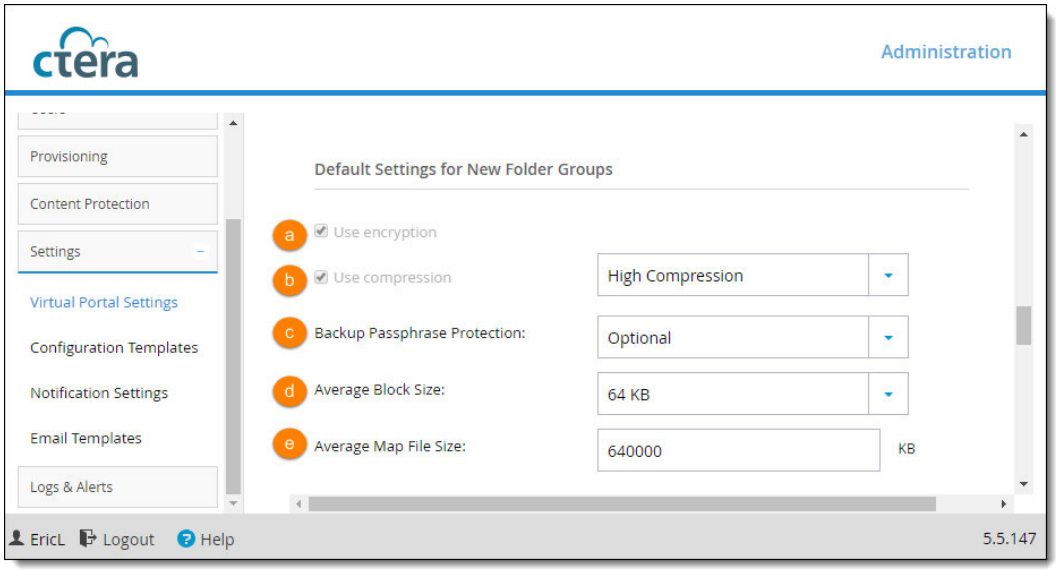
TEAM PORTAL SETTINGS



a **Enable Sharing of Personal Folders**. Select this option to enable team portal members to share personal folders with other team portal members.

b **Sharing Folder name**. The name of the folder in each user's cloud drive folder hierarchy in which other users' personal folders that were shared with the user appear. Relevant only if **Enable Sharing of Personal Folders** is selected.

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.

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 which data compression method will be selected by default for newly created folder groups:

- 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.

Note: 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 deduplication 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 deduplication ratio. Increased block size is useful for workloads that require high performance, as well as for those that do not gain greatly from deduplication (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 deduplication, 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.

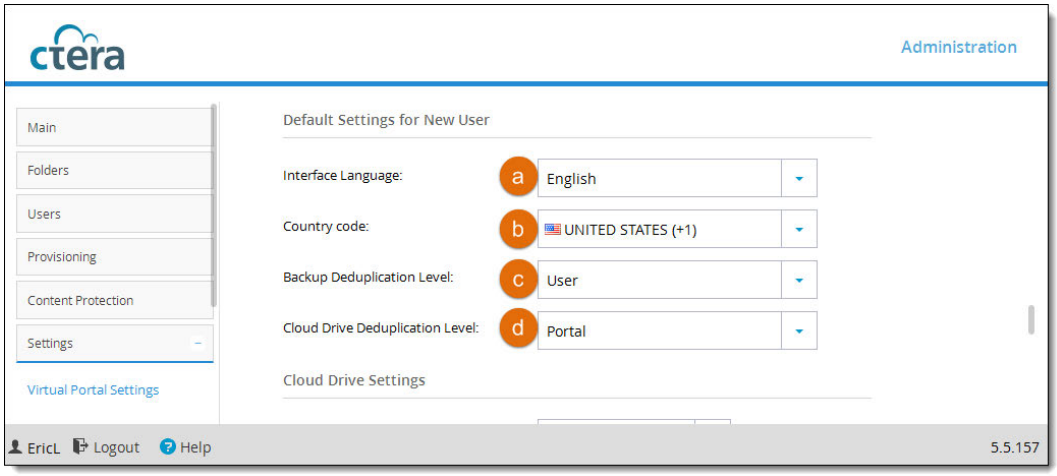
CTERA Portal uses file maps to keep track of the blocks each file is made of. The Average Map File Size represents the maximum size of file that will be represented using a single file map object. For example, if the average map file size is set to 100MB, files of up to approximately 100 MB will have 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.

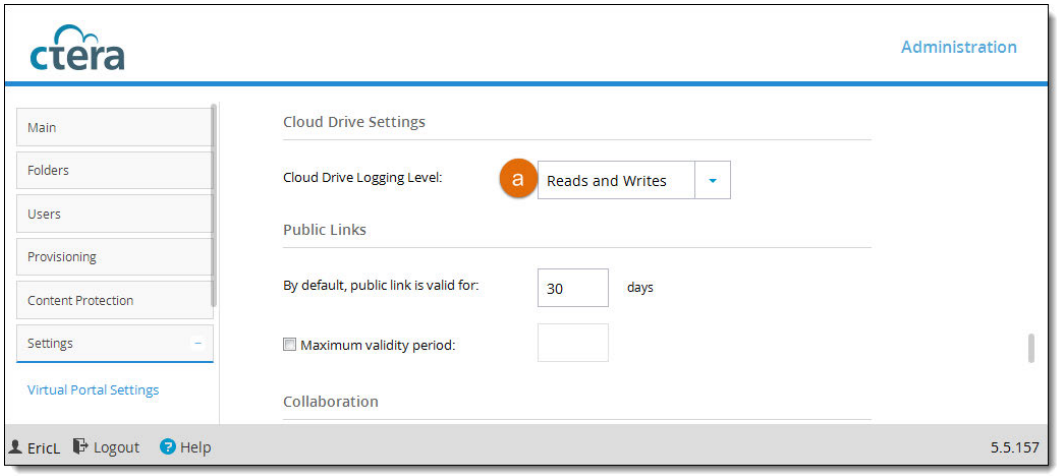
c **Backup Deduplication Level**. Specify the default deduplication level to use for backup folders, for all new users in team portals. Select one of the following:

- **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.
- **Portal**. Create a single folder group for each virtual portal, containing all of the backup folders in the portal.
- **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 deduplication level to use for cloud folders, for all new users in team portals. Select one of the following:

- **User**. 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.
- **Portal** (default). Create a single folder group for each virtual portal, containing all of the cloud folders in the portal.
- **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.

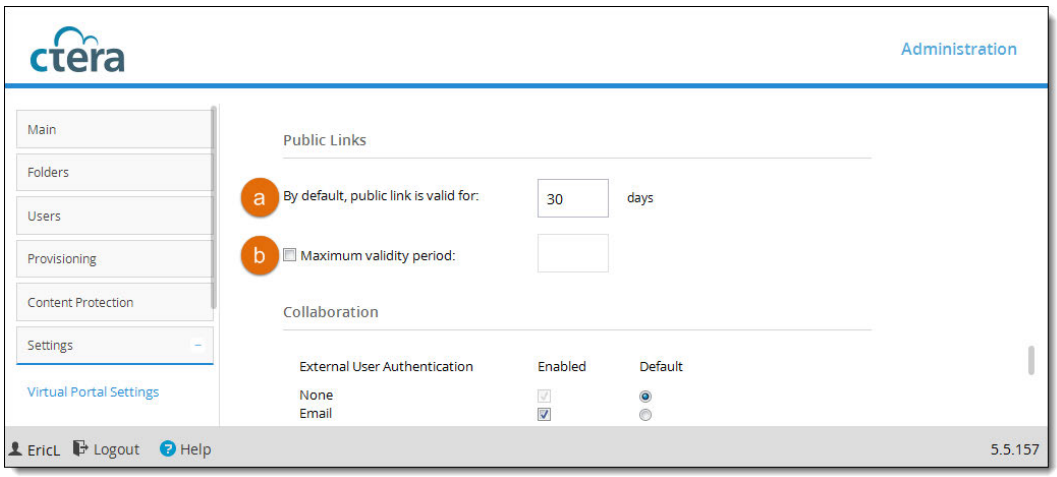
CLOUD DRIVE SETTINGS



a **Cloud Drive Logging Level**. Set the logging level for the Cloud Drive to one of the following:

- **None**
- **Writes Only**
- **Reads and Writes**

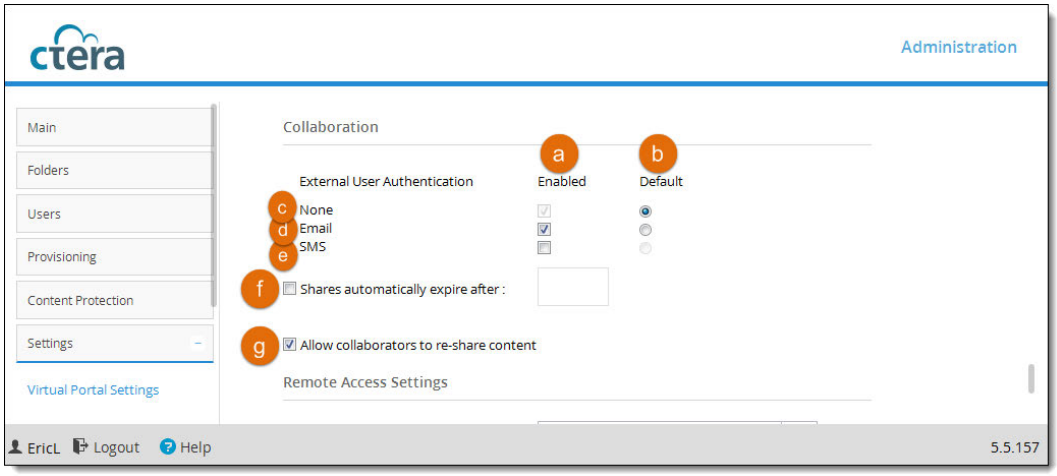
PUBLIC LINKS



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.

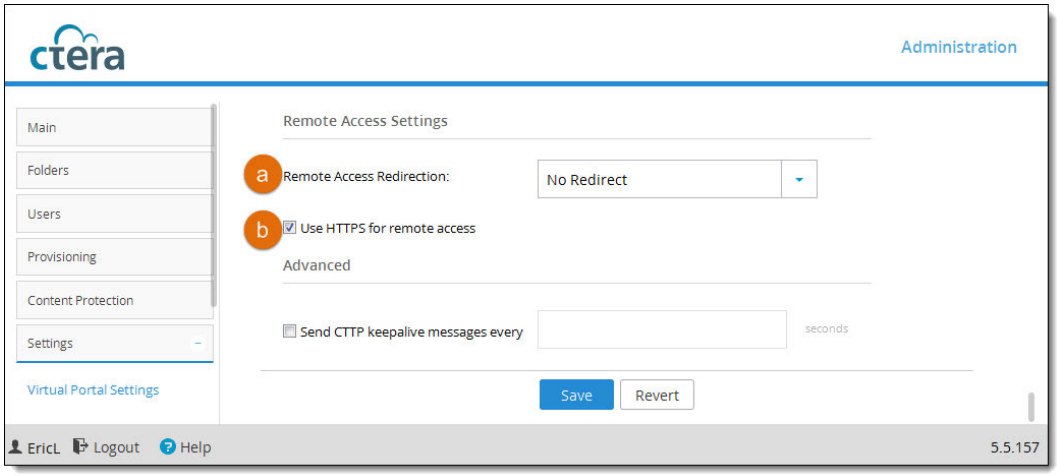
d **Email**. The invitation recipient receives a time limited authenticated link to the file or folder. On every access, a new 6 digit passcode challenge is sent to the recipient by email. The recipient must enter the passcode before accessing the file or folder. This ensures that the invitation is not 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

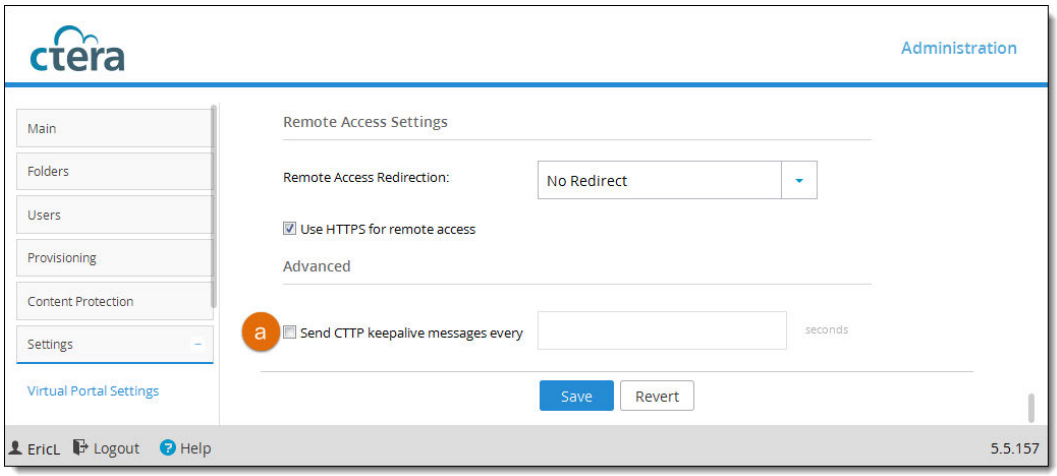


a **Remote Access Redirection**. Specify whether Web clients attempting to remotely access a device should be redirected to communicate directly with the device, instead of relaying communications through the CTERA Portal. Select one of the following:

- 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 p*ortal.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



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.

14

MANAGING DEVICE CONFIGURATION TEMPLATES

In this chapter

- Viewing Device Configuration Templates
- Adding and Editing Device Configuration Templates
- Backup and Exclude Sets
- Selecting Applications for Backup
- Cloud Backup Schedule
- Backup Throughput
- CTERA Agent Scripts
- Cloud Drive Synchronization
- Managing Sync Throughput
- Marking a Firmware Image as the Current Firmware Image
- Configuring Automatic Firmware Updates
- Configuring the Automatic Template Assignment Policy
- Setting the Default Device Configuration Template
- Duplicating Configuration Templates
- Deleting Device Configuration Templates

CTERA Portal enables you to centrally manage device settings, by assigning 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
- Scripts that run on CTERA Agents (relevant for CTERA Agent devices only)
- Installed software and firmware versions
- Automatic firmware updates

Note: Settings inherited from a template can be overridden from the device's Web interface.

Devices can be assigned to templates in the following ways:

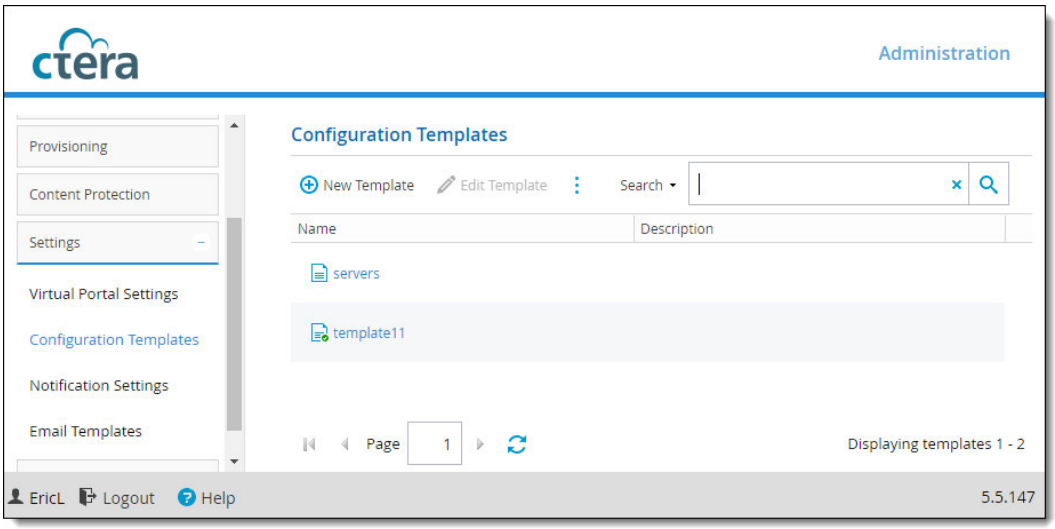
- Manually, by editing the device settings.
  See Editing Device Settings.
- Automatic template assignment.
  Devices can be assigned to templates based on the *automatic template assignment policy*, which specifies a set of criteria for assigning a template (such as device type, installed operating 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.

VIEWING DEVICE CONFIGURATION TEMPLATES

To view all device configuration templates in the portal:

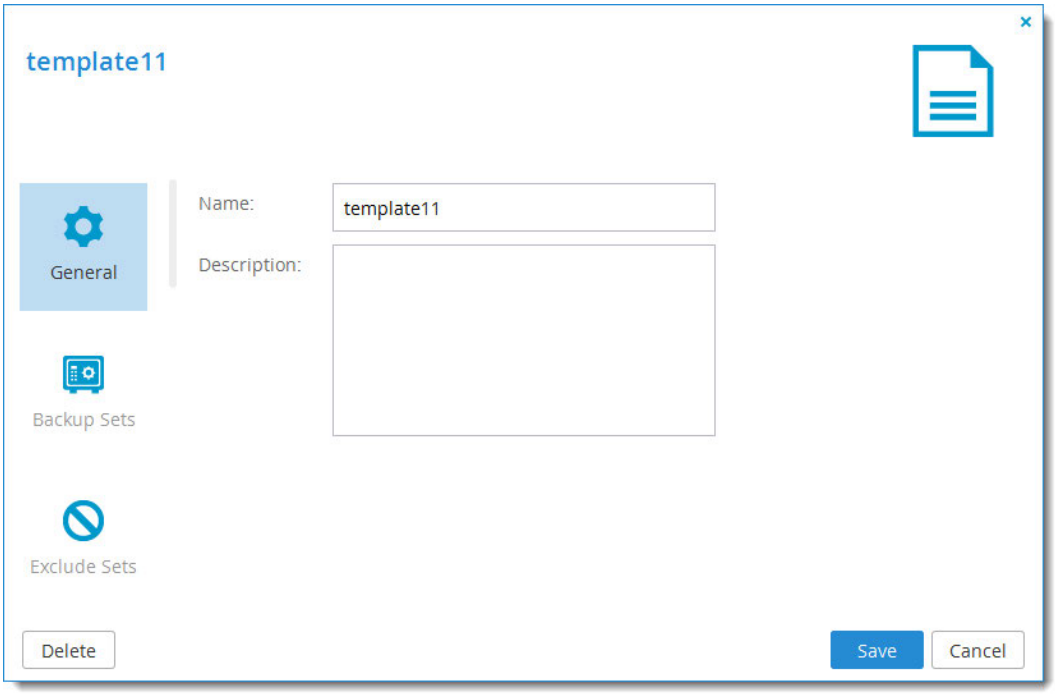
- Select **Settings > Configuration Templates** from the menu.
  The page displays all templates, including each template's name and description.



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:

- Checks whether the file is contained in an Exclude Set. If so, the file is skipped.
- Checks whether the file is contained in a Backup Set. If so, the file is backed up.
- 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*.

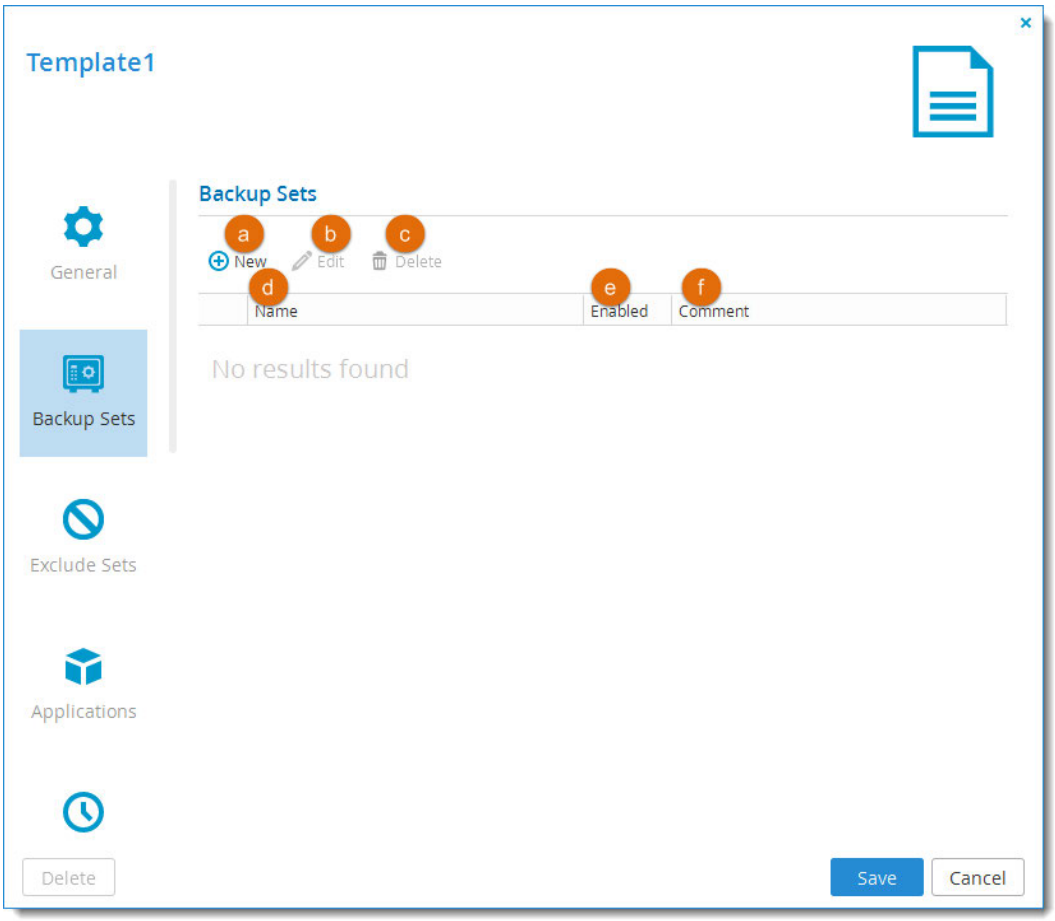
If a file is included in an enabled backup set but also included in an Exclude set, the file will be excluded from the backup.

When you create a backup set, it is automatically enabled. Backup sets can be enabled or disabled.

Adding 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.)

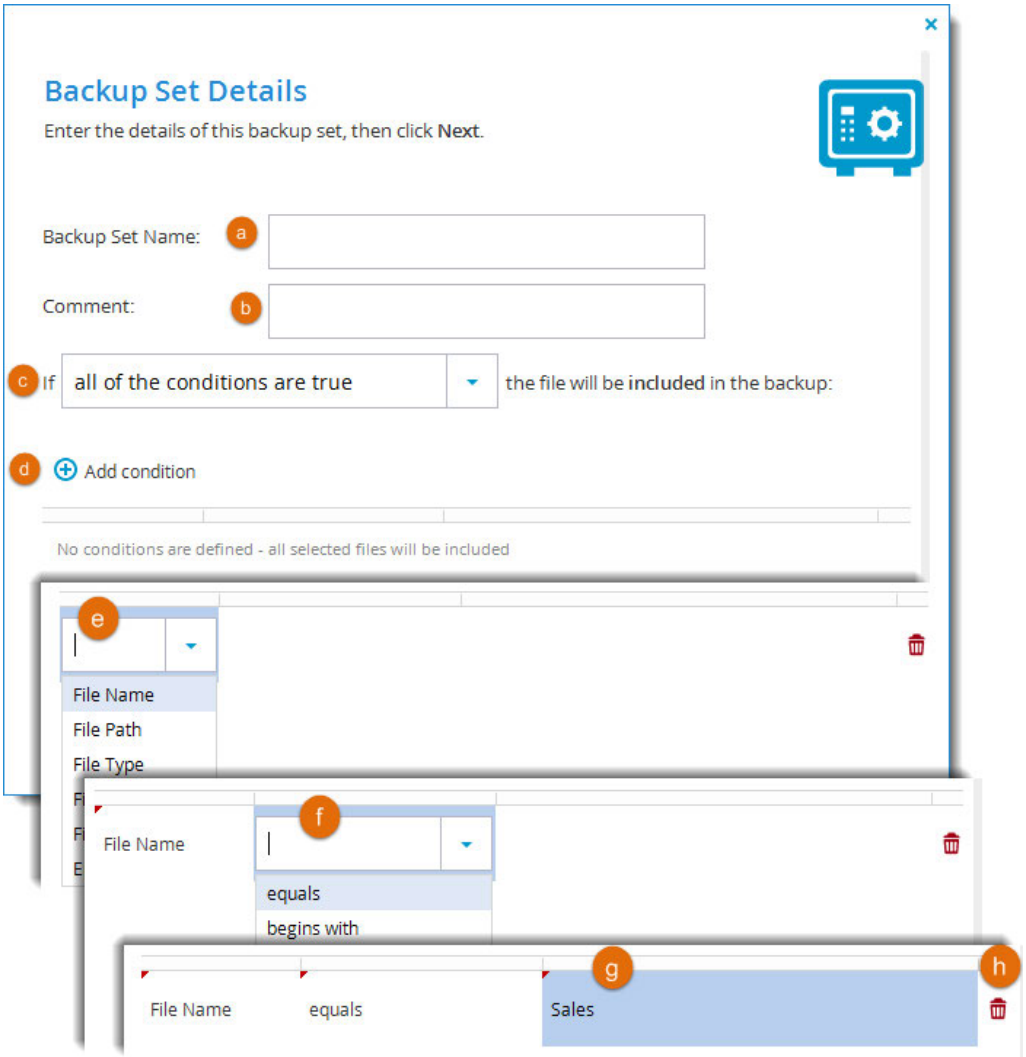
c **Delete**. Delete a backup or exclude set (select the set and then click)

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.

g Click in the third column, and complete the condition:

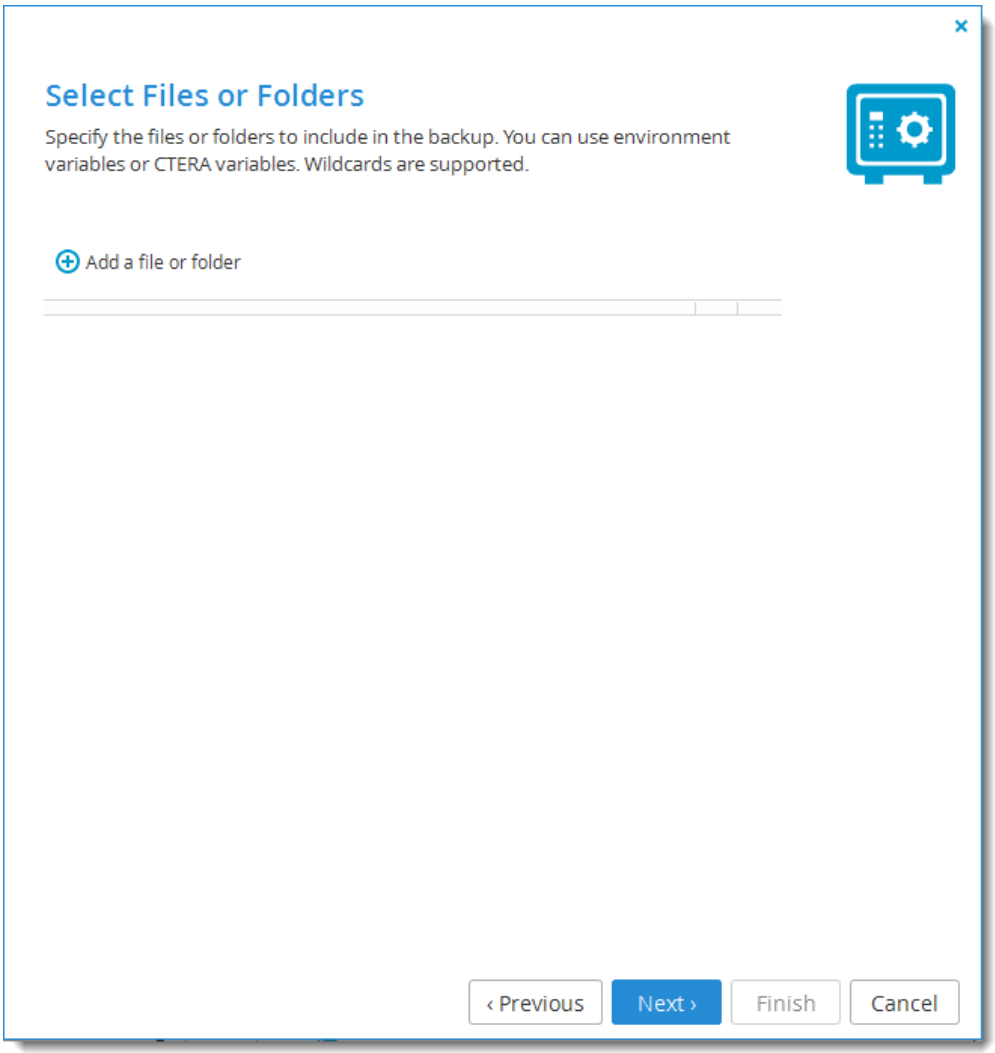
- If the parameter is **File Size**, type the desired file size and unit.

- 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.

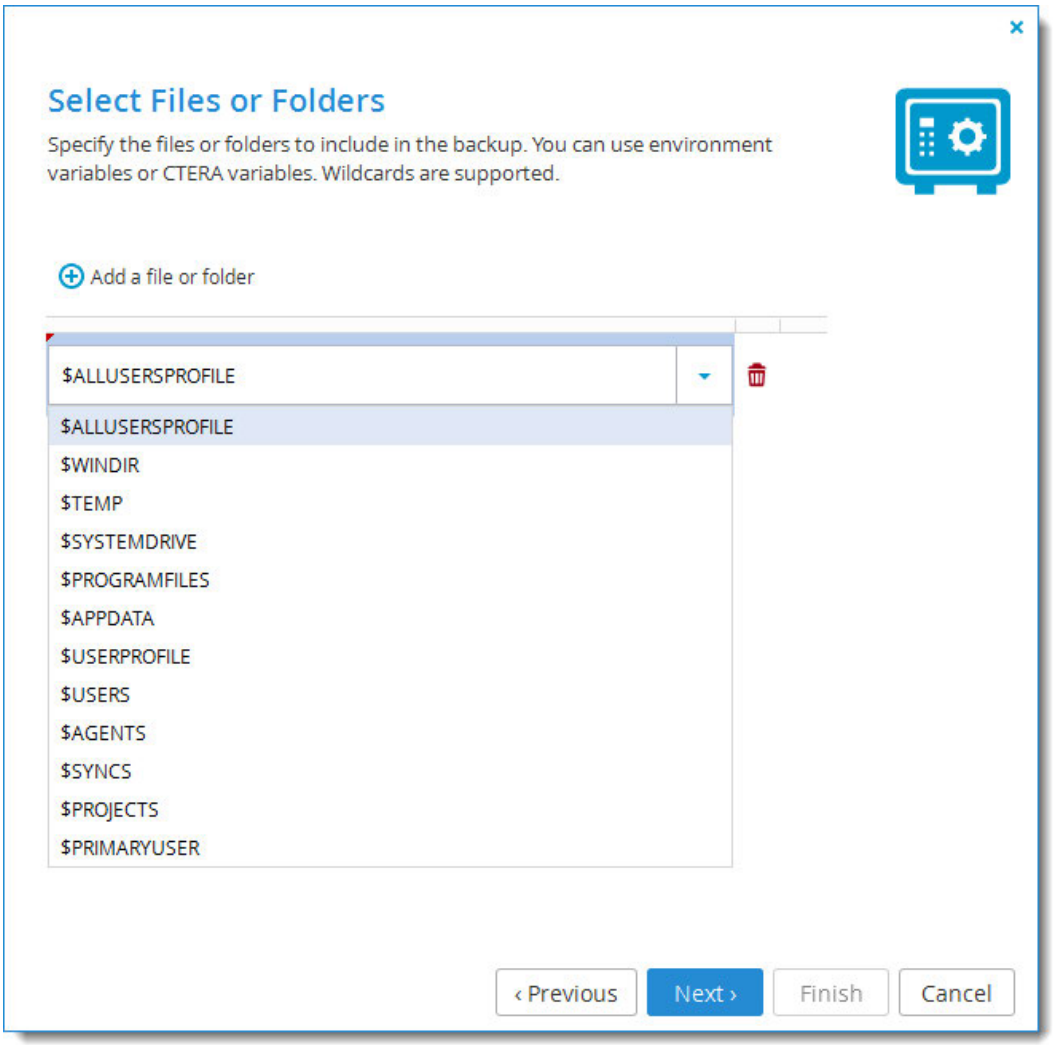
h If you need to delete a condition, click in its row.

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.
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.

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.

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 Storage Gateways.
$USERS	The home directories folder on the CTERA Cloud Storage Gateway.
$AGENTS	The CTERA Agents folder on the CTERA Cloud Storage Gateway.
$SYNCS	The Clientless Backup destination folder on the CTERA Cloud Storage Gateway.
$PROJECTS	The projects folder on the CTERA Cloud Storage Gateway.
$PRIMARYUSER	The profile folder of the local user who connected the CTERA Agent to the CTERA Portal or CTERA Cloud Storage 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

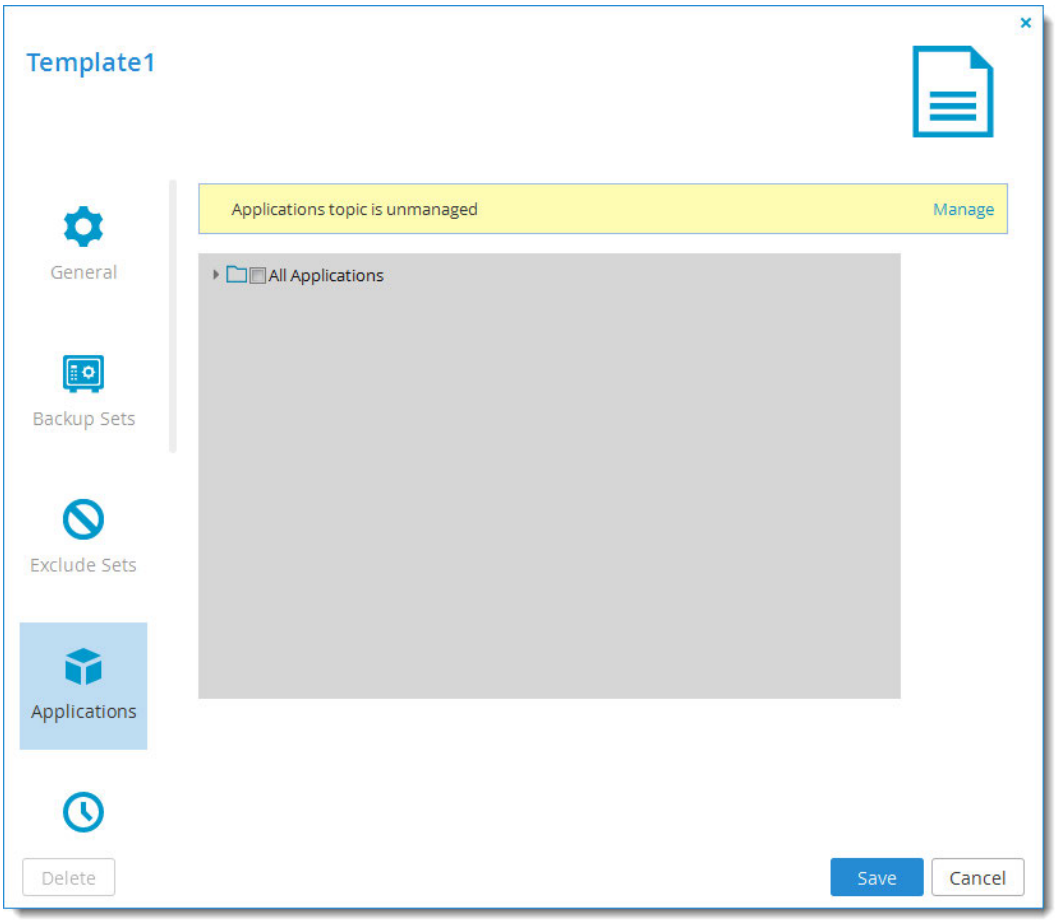
To modify a backup or exclude set, click the name of the backup set in the **Backup Sets** or **Exclude Sets** tab and proceed as for creating.

SELECTING APPLICATIONS FOR BACKUP

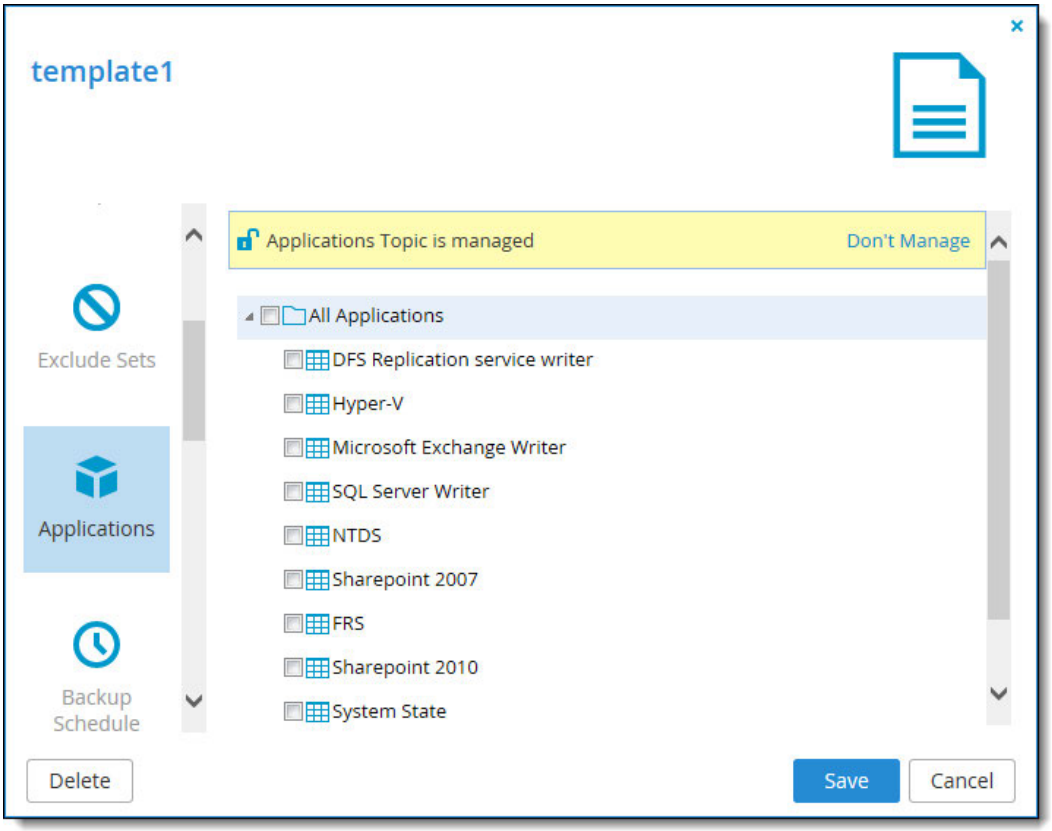
Note: If a selected application is not installed on the target device, it will be ignored.

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**.



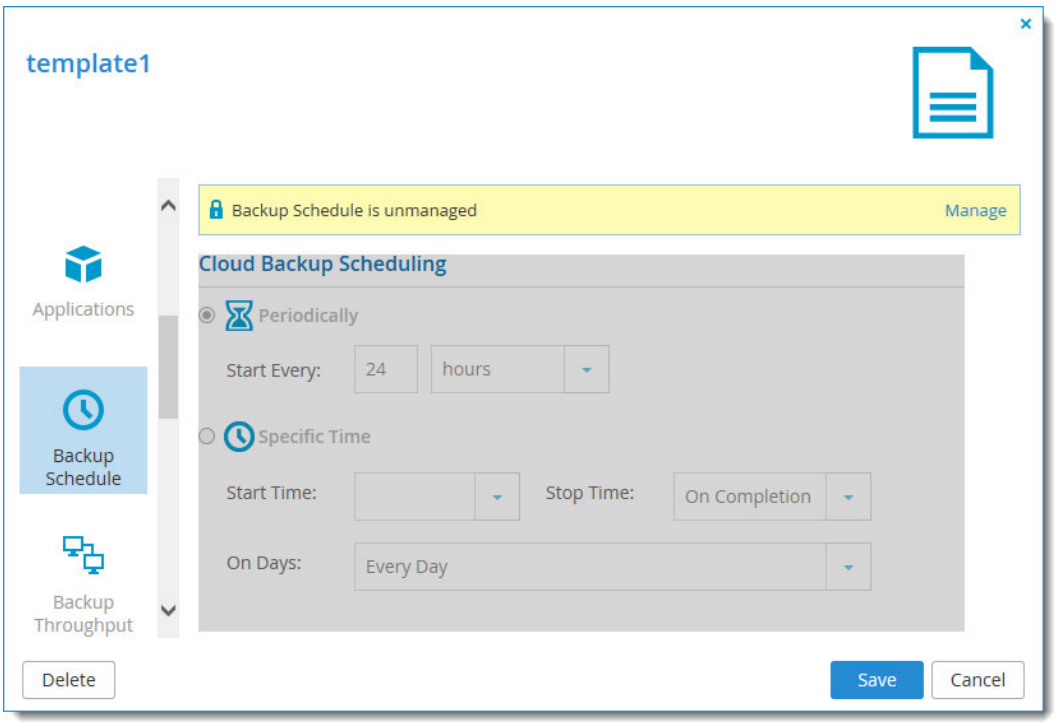
3 Expand the tree nodes and select the check boxes next to the applications you want to back up.

4 Click **Save**.

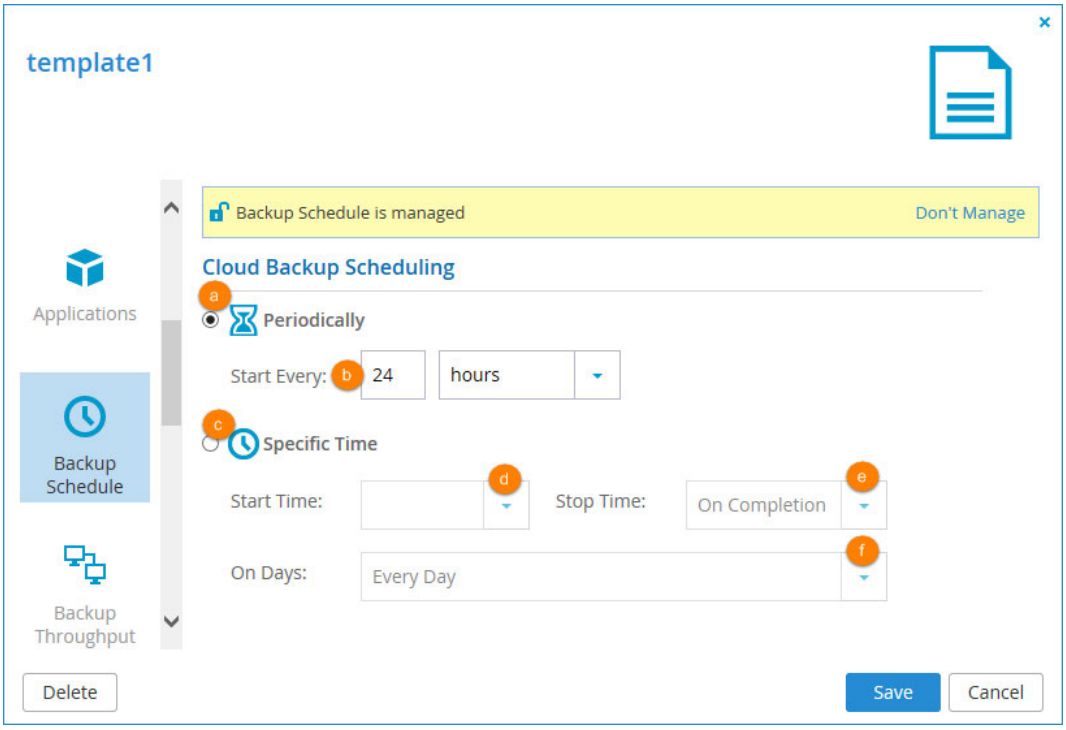
CLOUD BACKUP SCHEDULE

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.

Note: 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.

Note: 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.

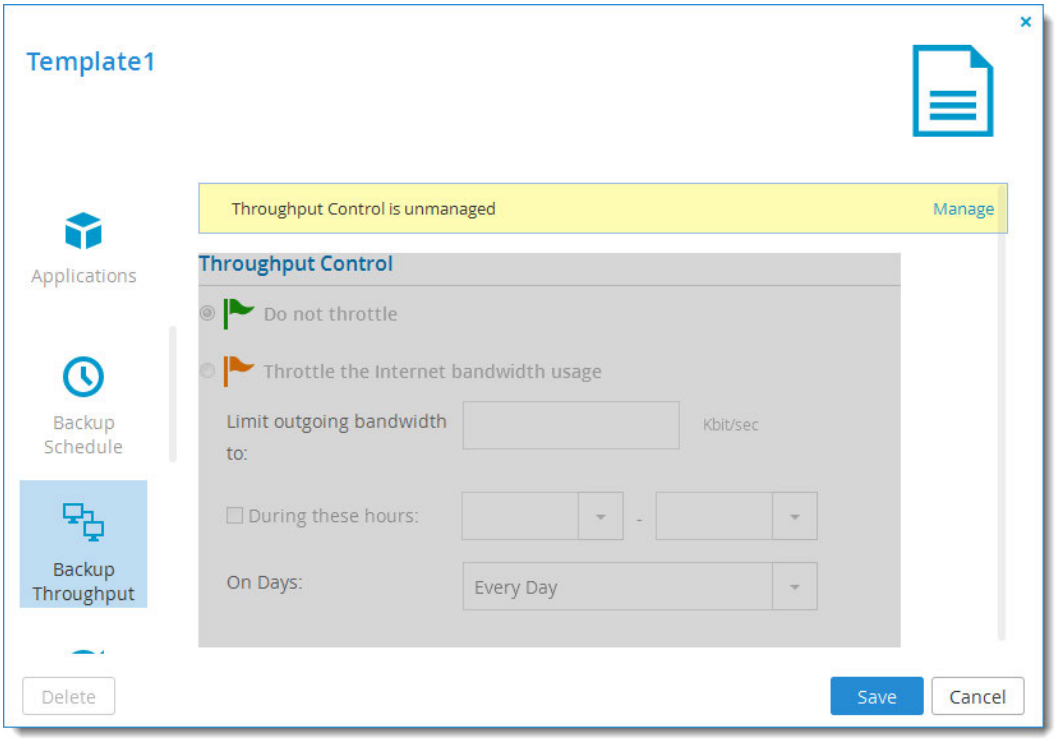
4 Click **Save**.

BACKUP THROUGHPUT

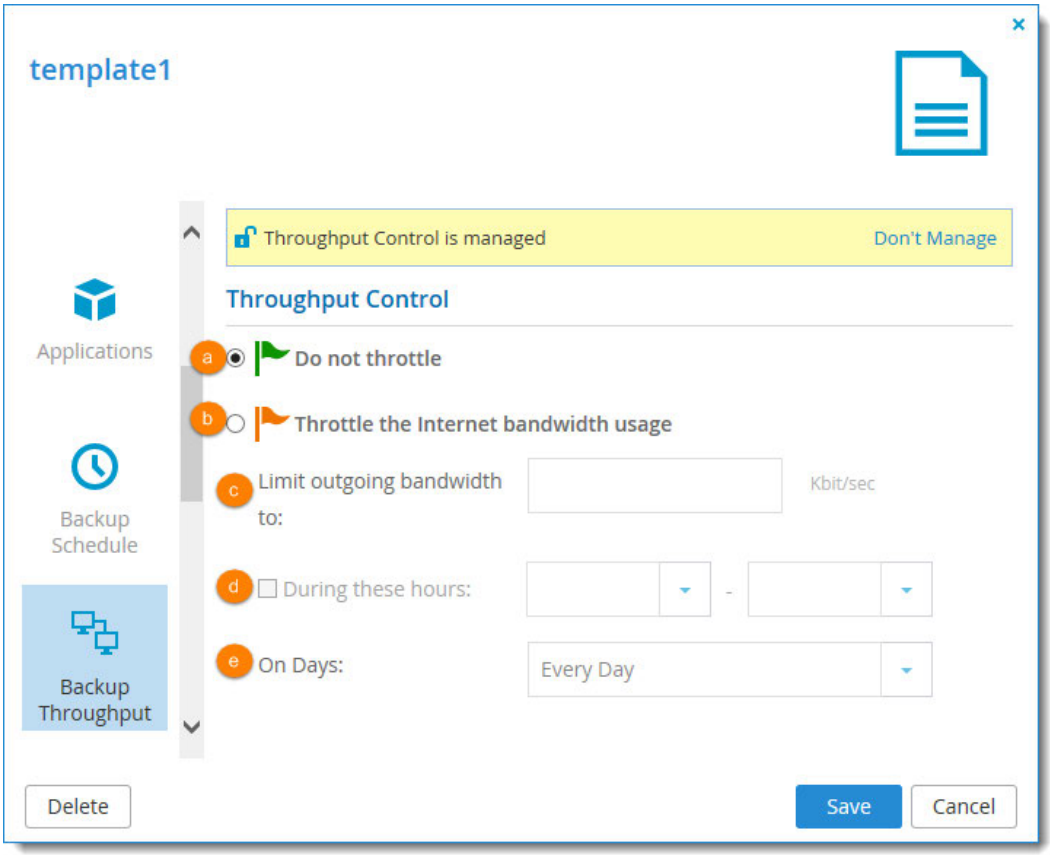
If desired, you can restrict the amount of bandwidth used for backing up files online.

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**.

CTERA AGENT SCRIPTS

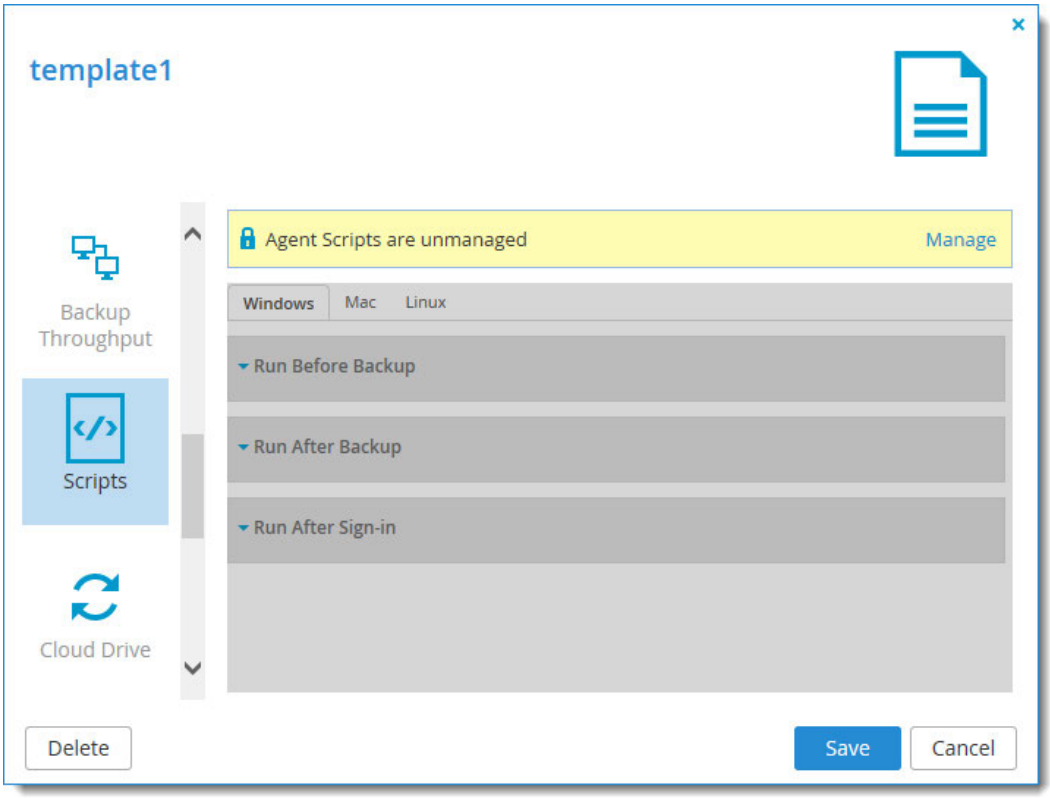
You can create and manage CTERA Agent scripts within device templates. The scripts are updated and pushed to agents connected to the portal and run on the Mac OS X-, Windows-, and Linux-based environments on which the agents run.

You can configure scripts to run at any of the following stages of agent processes:

- Run before backup
- Run before restore
- Run after sign in

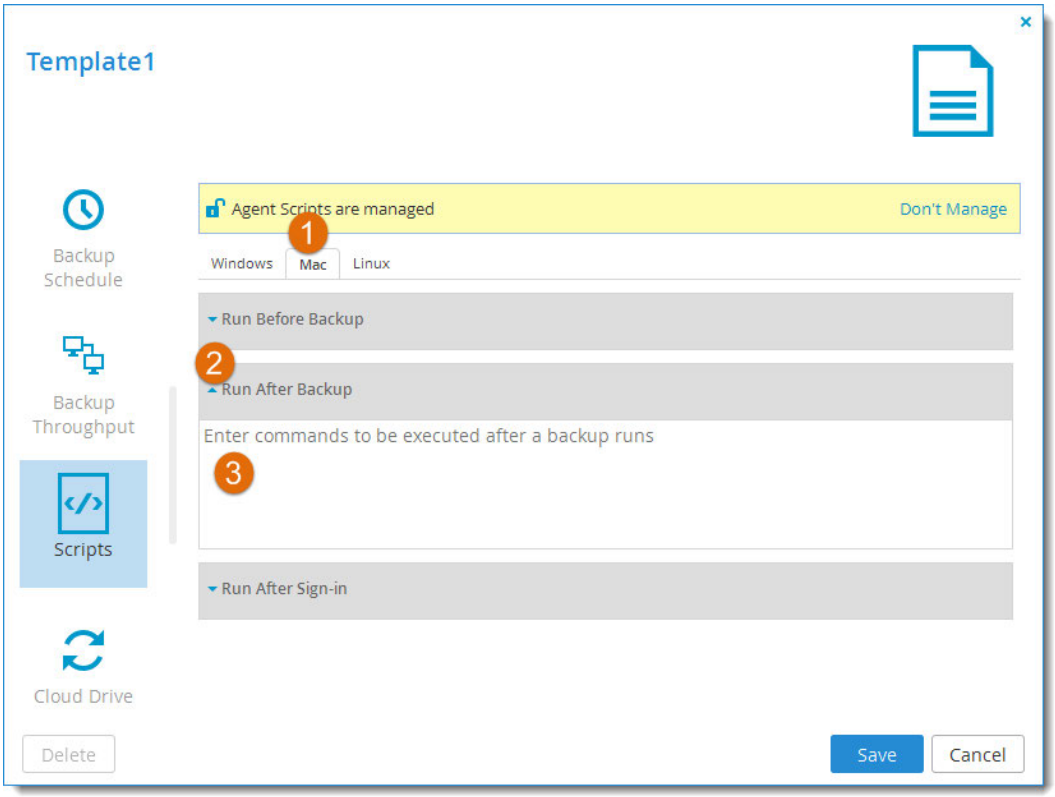
To configure scripts in a device configuration template:

1 Select the **Scripts** tab.



2 Click **Manage** to enable the templates.

3 Add all the scripts you want to include in the template.



To add a script:

a Select the tab for the relevant agent platform.

b Click the stage at which you want the script to run. For example, **Run After Backup**.

c Enter the script, using supported commands.

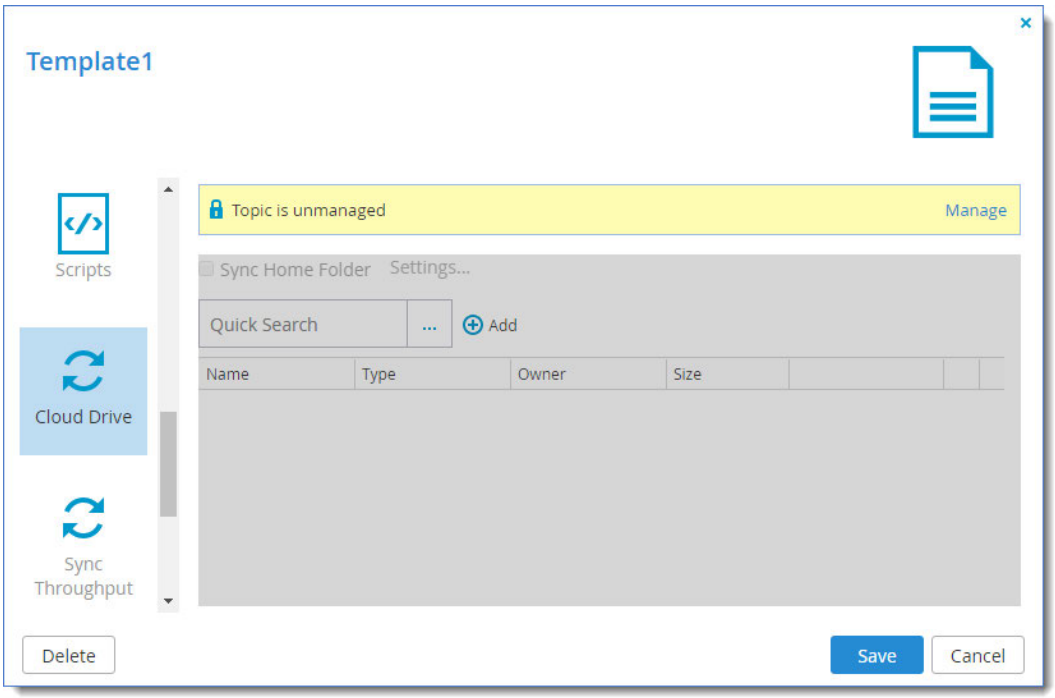
4 Click **Save**.

CLOUD DRIVE SYNCHRONIZATION

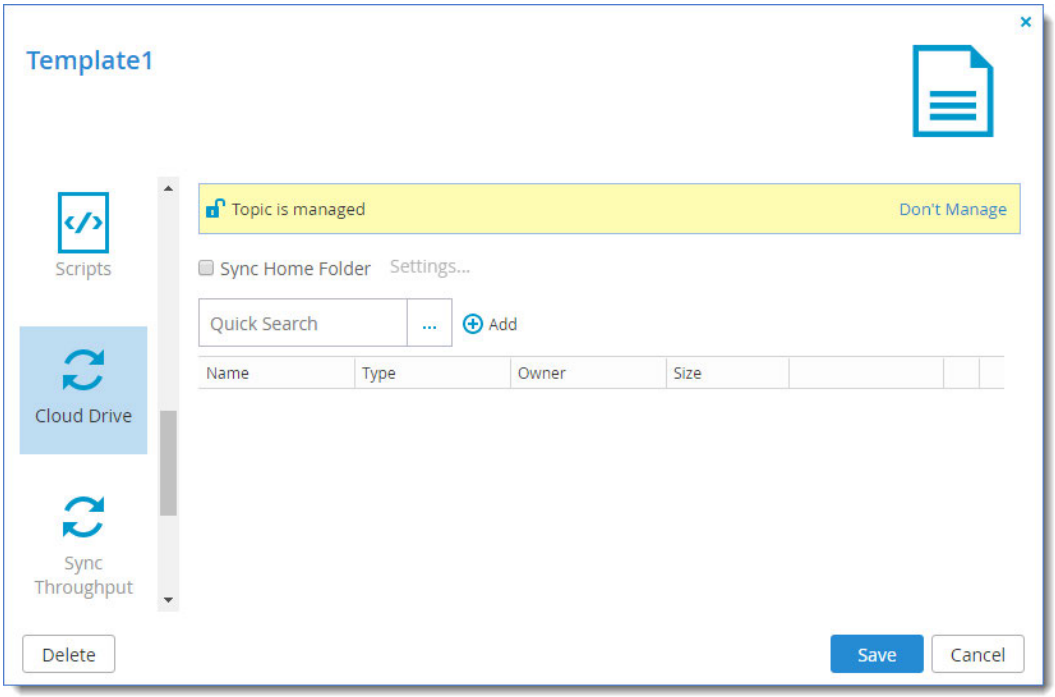
You can specify which portal cloud folders should be synchronized with the device, and with which folder each cloud drive folder should be synced.

To manage cloud drive sync in the device template:

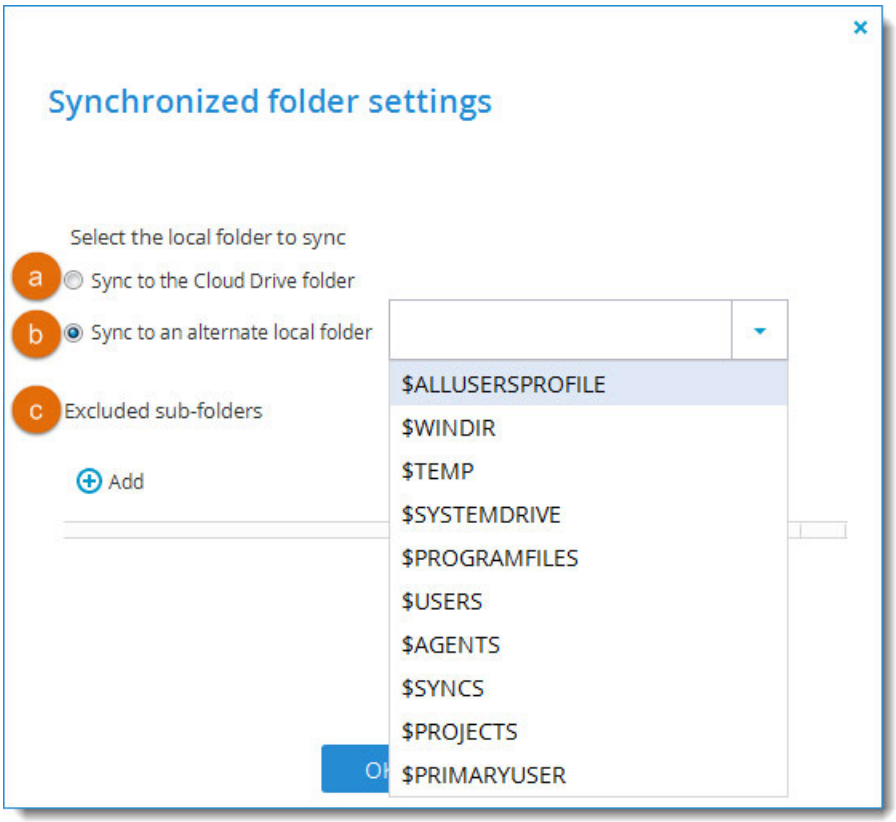
1 Select the **Cloud Drive** tab.



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**.



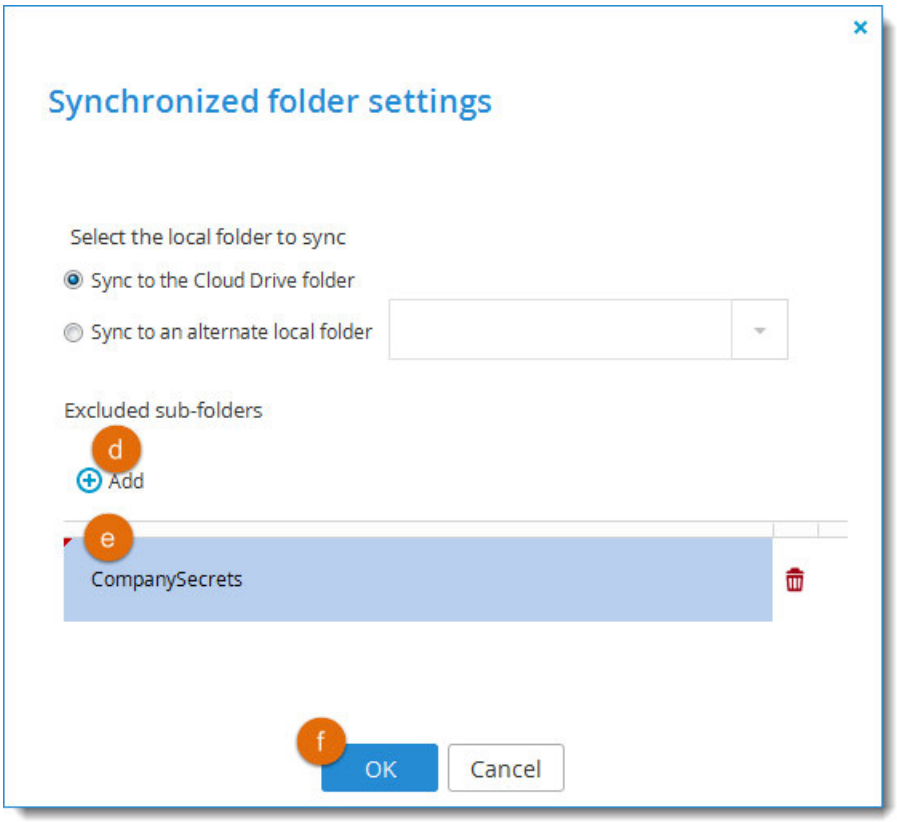
3 To sync the home folder, select **Sync Home Folder** and set which local folder on the device the cloud drive home folder should be synced:



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 Backup Set Environment Variables.

c Exclude sub-folders:



d Click **Add** in the **Excluded sub-folders** section.
A row is added to the **Excluded sub-folders** list.

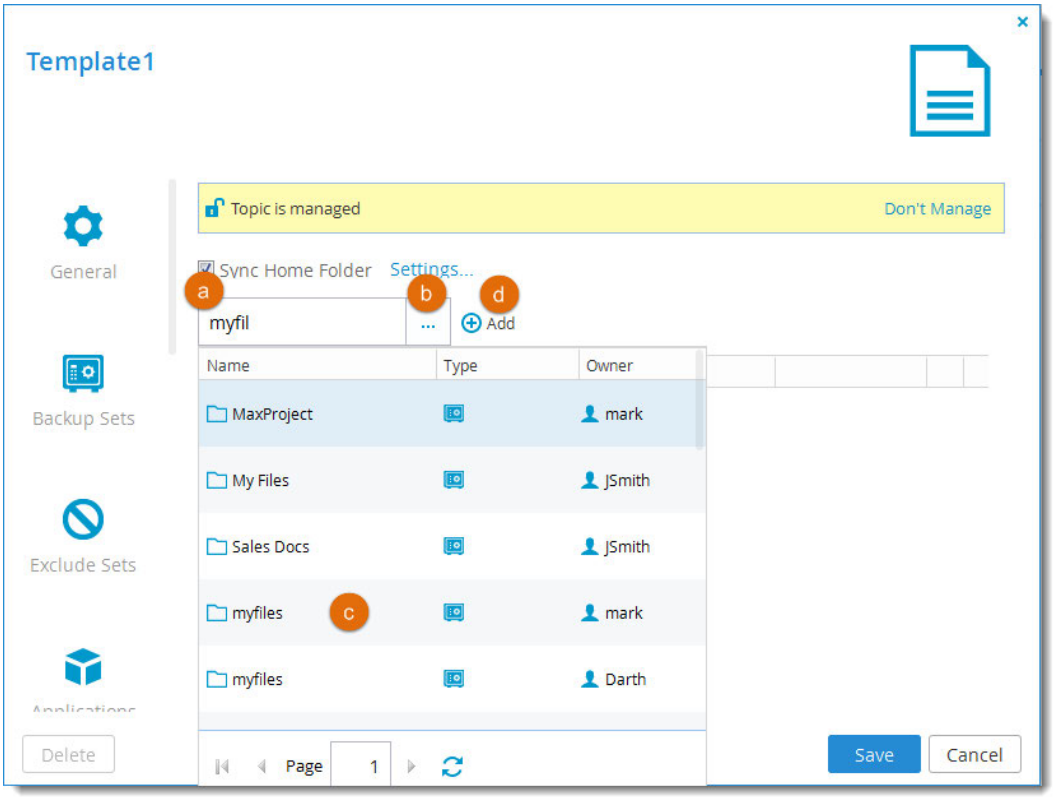
e Click in the row and type the name of a sub-folder you want to exclude from syncing.
Repeat the previous steps to add more sub-folders as necessary until all the folders you want to exclude are listed.

f Click **OK** to apply your changes.

4 To add more cloud drive folders to sync with the device:

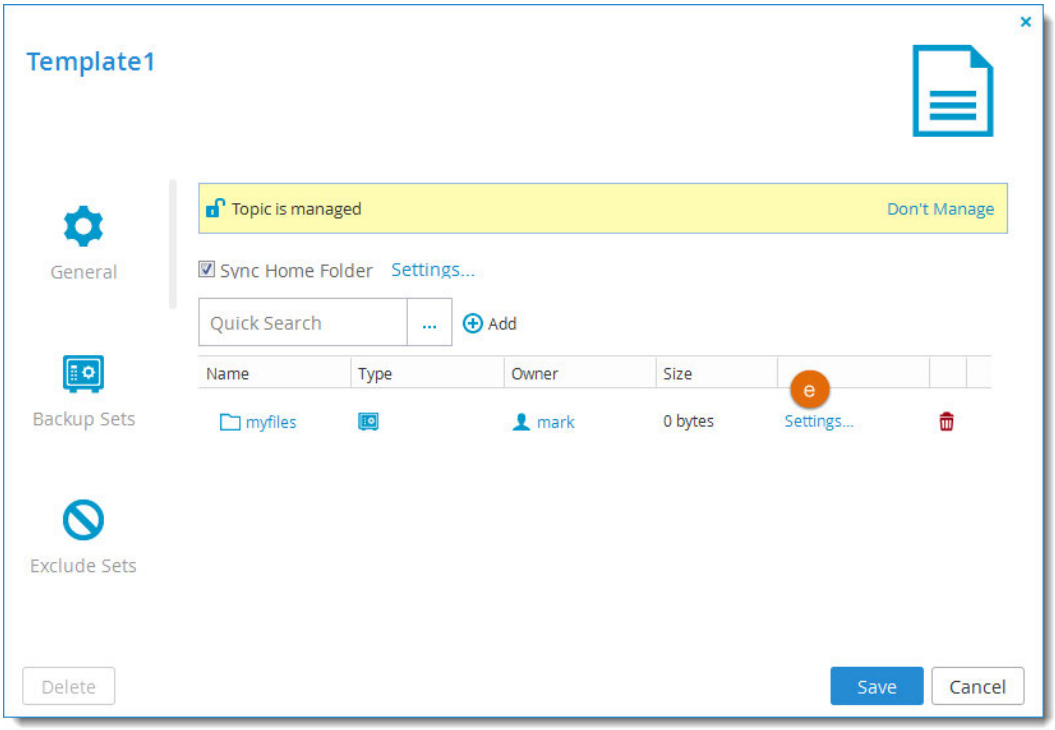
a Click in the **Quick Search** field and type a search string to search for the name of a cloud drive folder you want to add.

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.



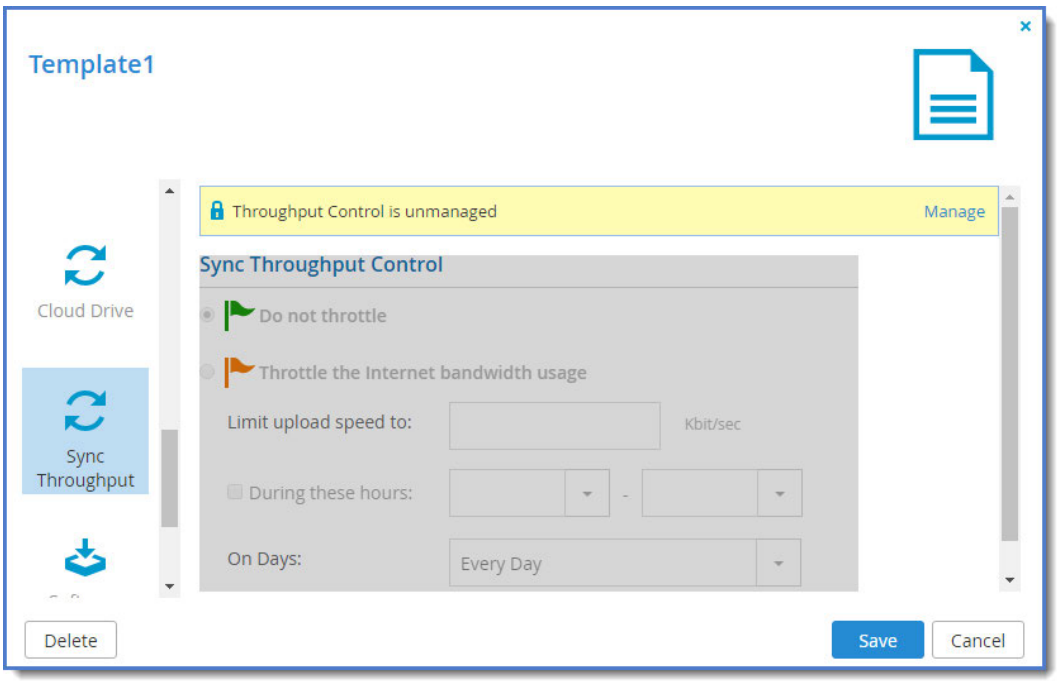
e To set which folder on the device the folder should sync with, click the **Settings** button in the folder's row, and set the folder as described above.

5 Click **Save**.

MANAGING SYNC THROUGHPUT

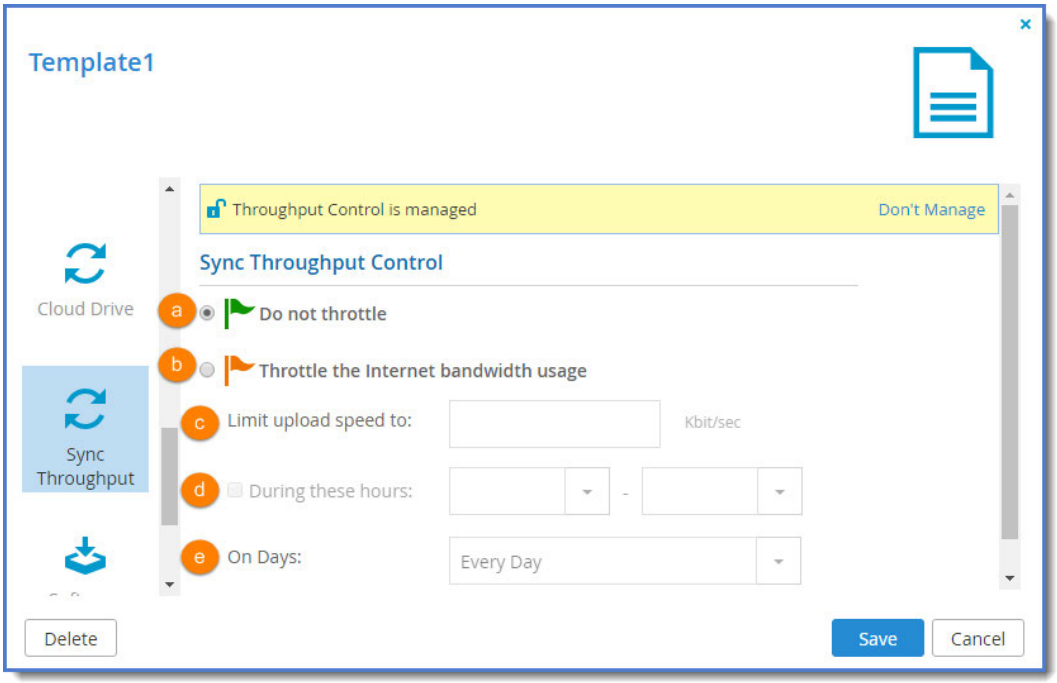
To control whether the cloud sync upload speed is limited, and how and when it is limited:

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**.

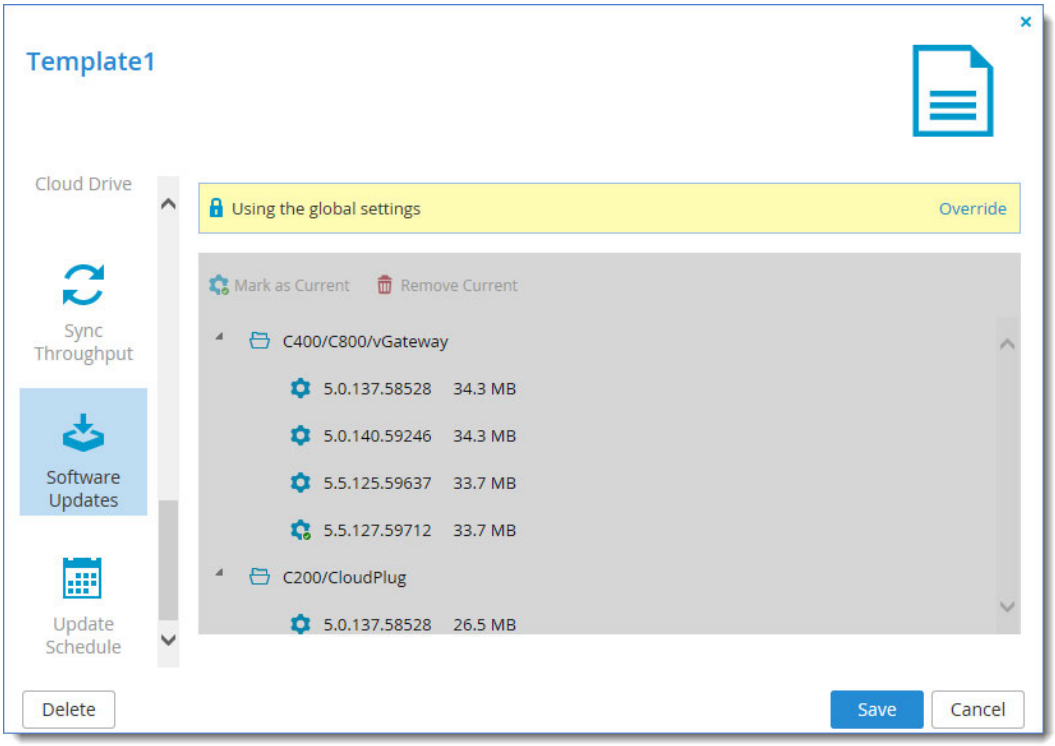
MARKING A FIRMWARE IMAGE AS THE CURRENT FIRMWARE IMAGE

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.

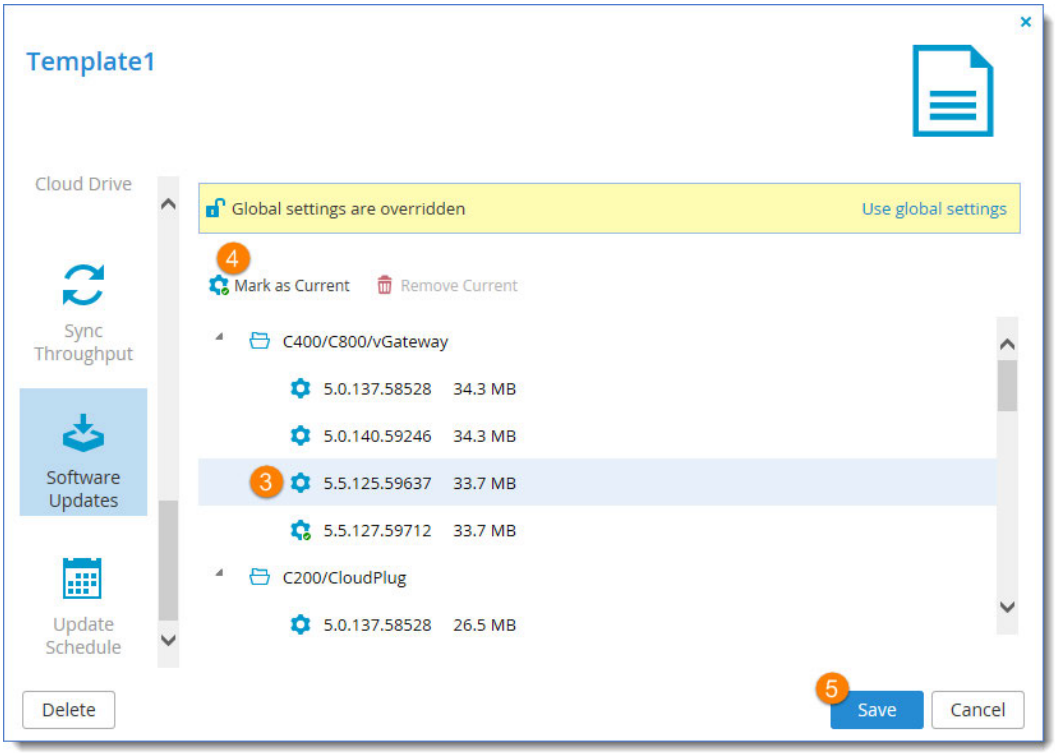
There can only be one current firmware image per device platform.

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.

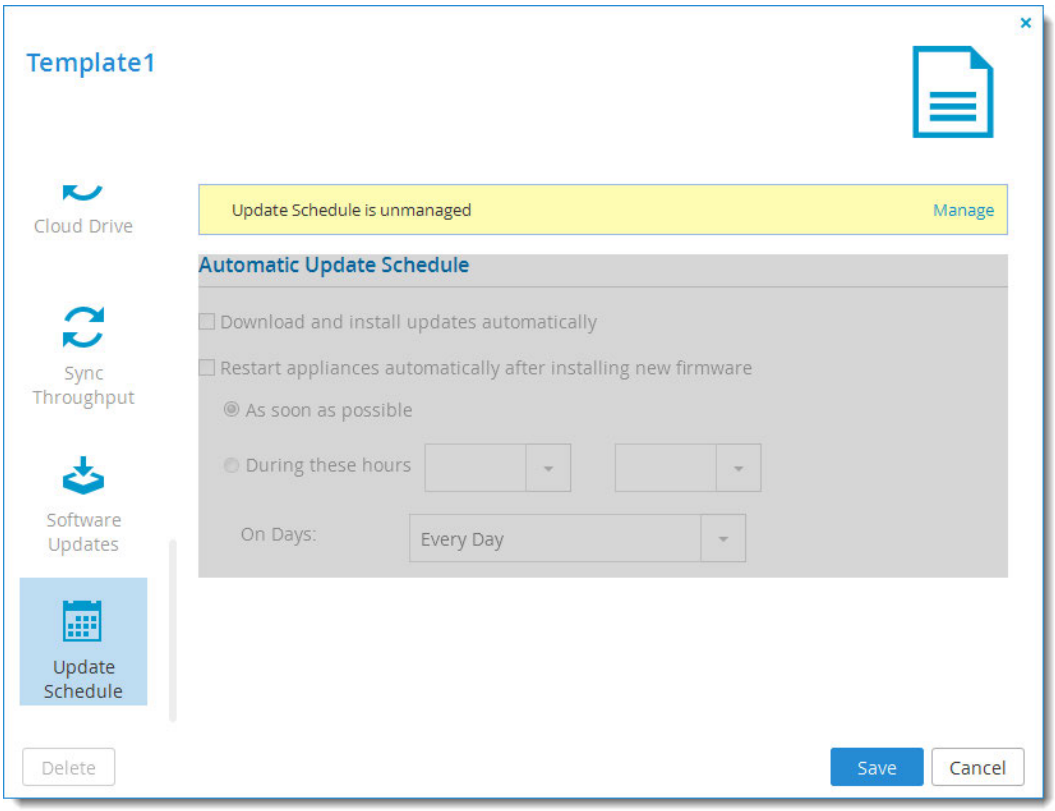
5 Click **Save**.

CONFIGURING AUTOMATIC FIRMWARE UPDATES

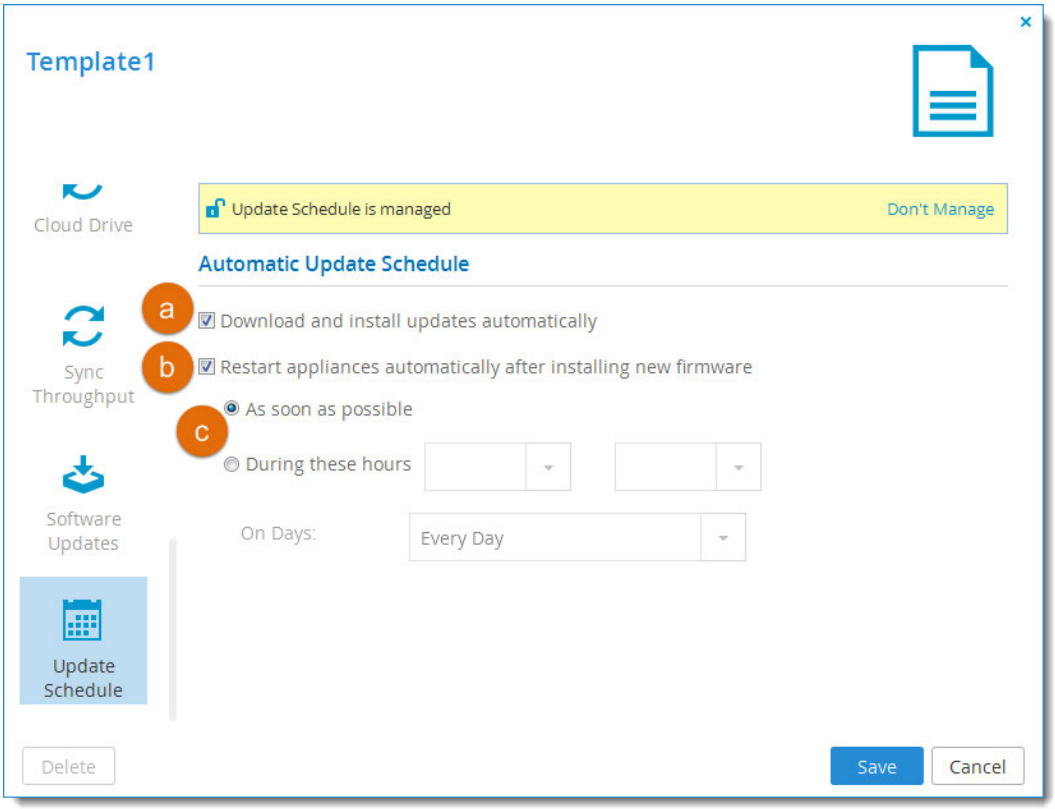
If desired, you can configure your devices to automatically download and install firmware updates.

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 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).

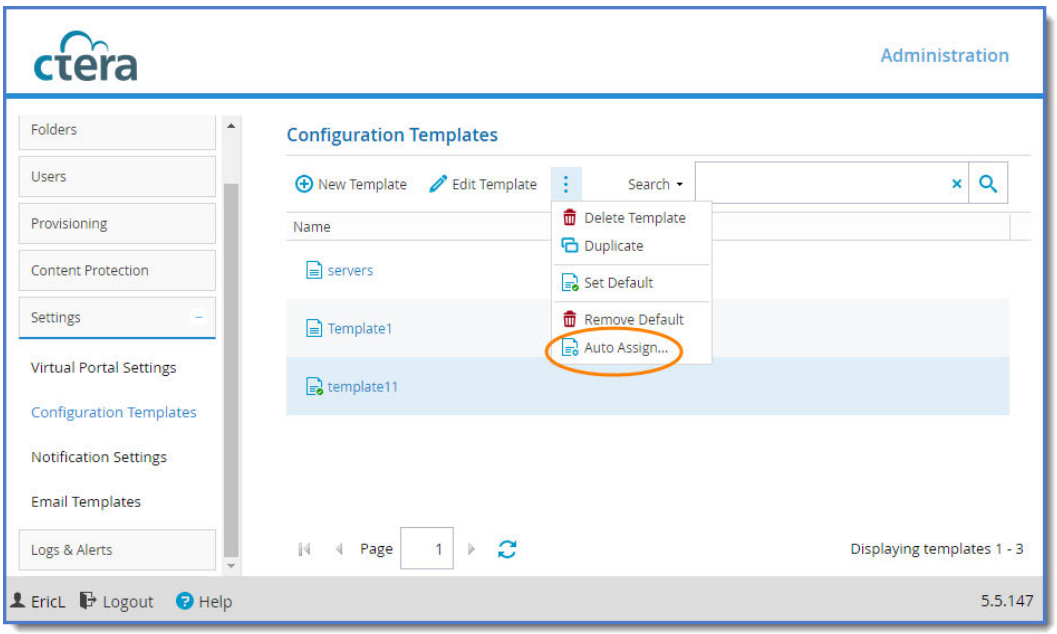
4 Click **Save**.

CONFIGURING THE AUTOMATIC TEMPLATE ASSIGNMENT POLICY

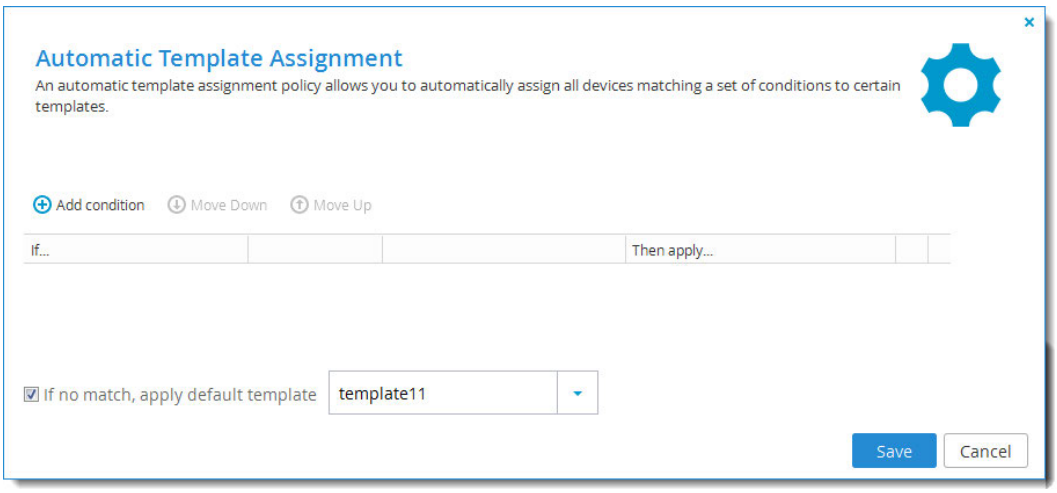
To configure the automatic template assignment policy:

1 Select **Settings > Configuration Templates** from the menu.

2 Click **Auto Assign**.

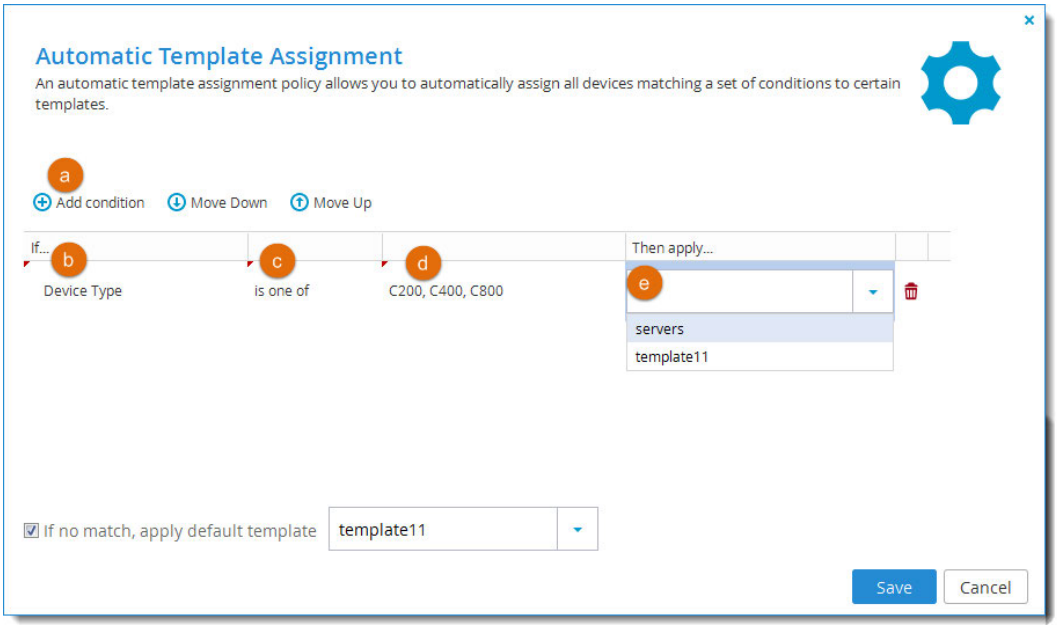


The Automatic Template Assignment dialog box is displayed.



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 is displayed 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 `5.0` in the third column, then the condition will be met when the device's installed firmware version is 5.0.

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

Note: 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:

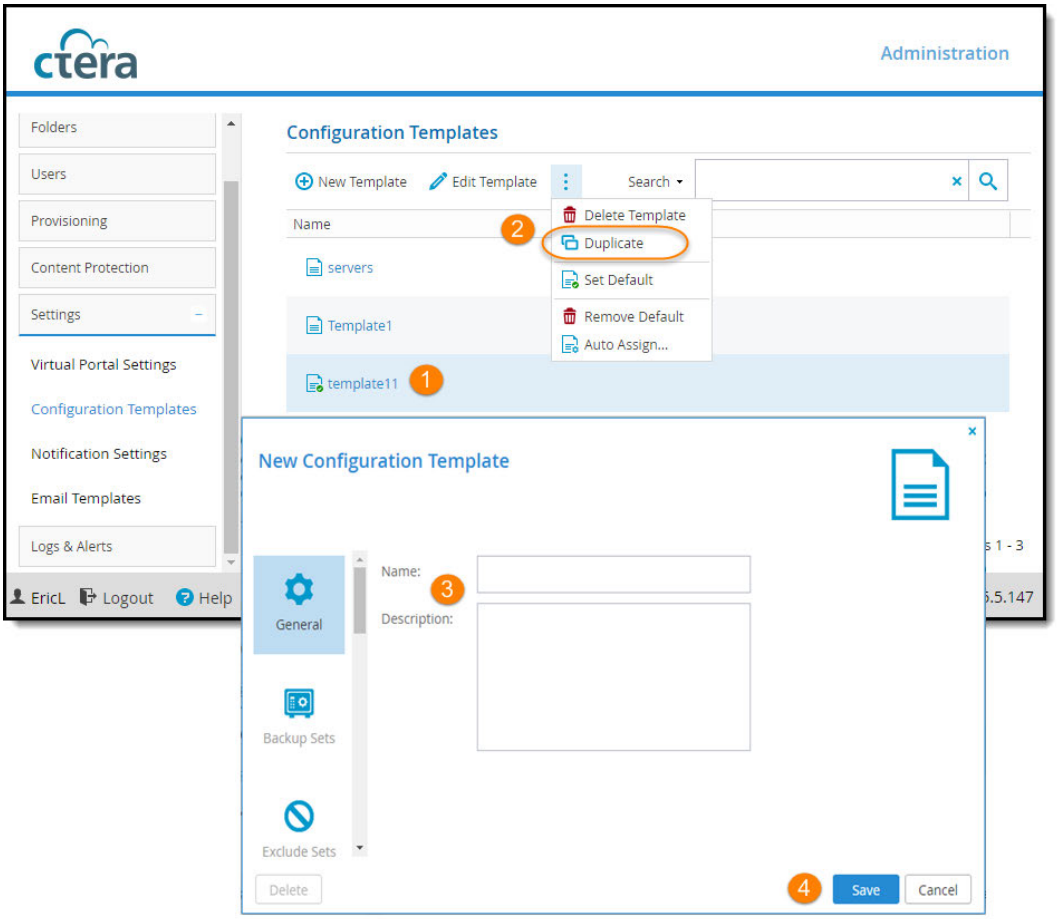
- Click **Remove Default**.
  No default template is configured.

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 is displayed.



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.

Note: 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.

15

NOTIFICATIONS

In this chapter

- The Notifications Dashboard
- Configuring Notification Settings

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.

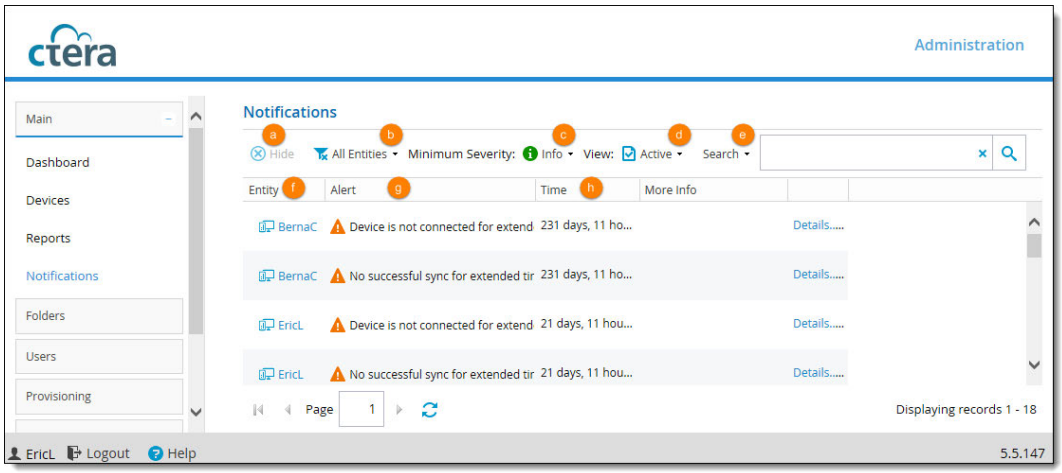
Notifications enable you to track error and warning conditions. For instance, one can use the notification dashboard to track failed backup jobs.

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 selecting the notification and clicking the **Unhide** button that is displayed 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 them.

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.

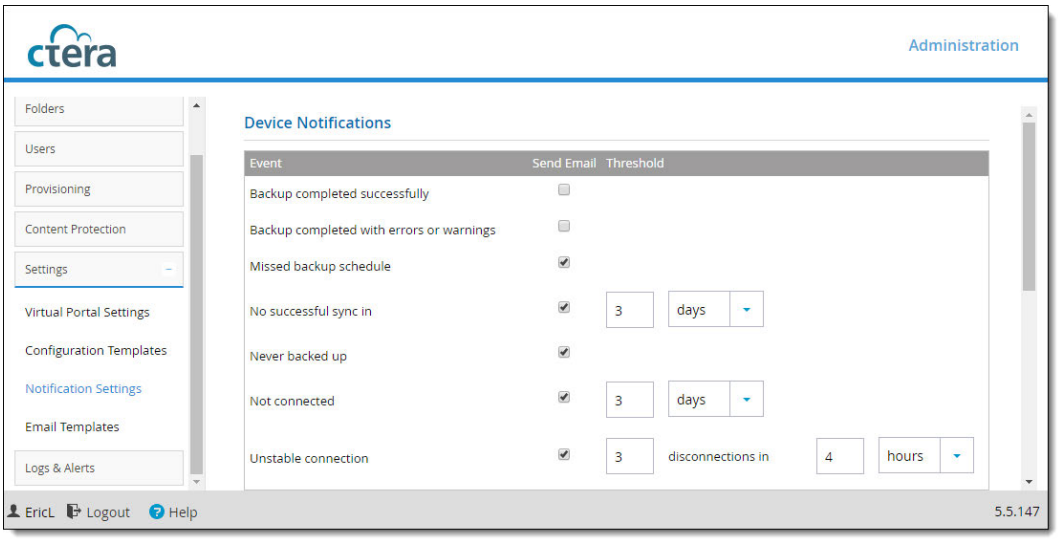
g **Alert**. The alert message.

h **Time**. The time at which the alert was triggered.

CONFIGURING NOTIFICATION SETTINGS

To configure notifications:

1 Select **Settings > Notification Settings** from the menu.



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**).

16

CONFIGURING EMAIL TEMPLATES

In this chapter

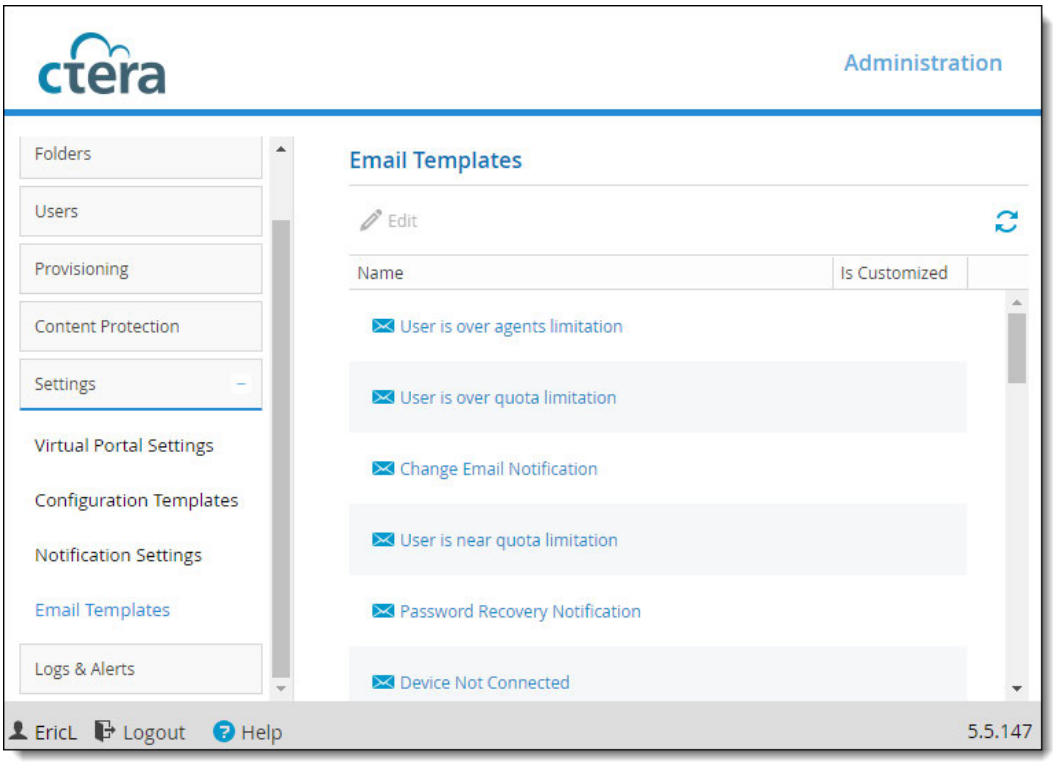
- Customizing Email Notification Templates
- Email Notification Templates

You can configure email notification templates for notifications sent to users from the portal. The email notifications are in HTML format.

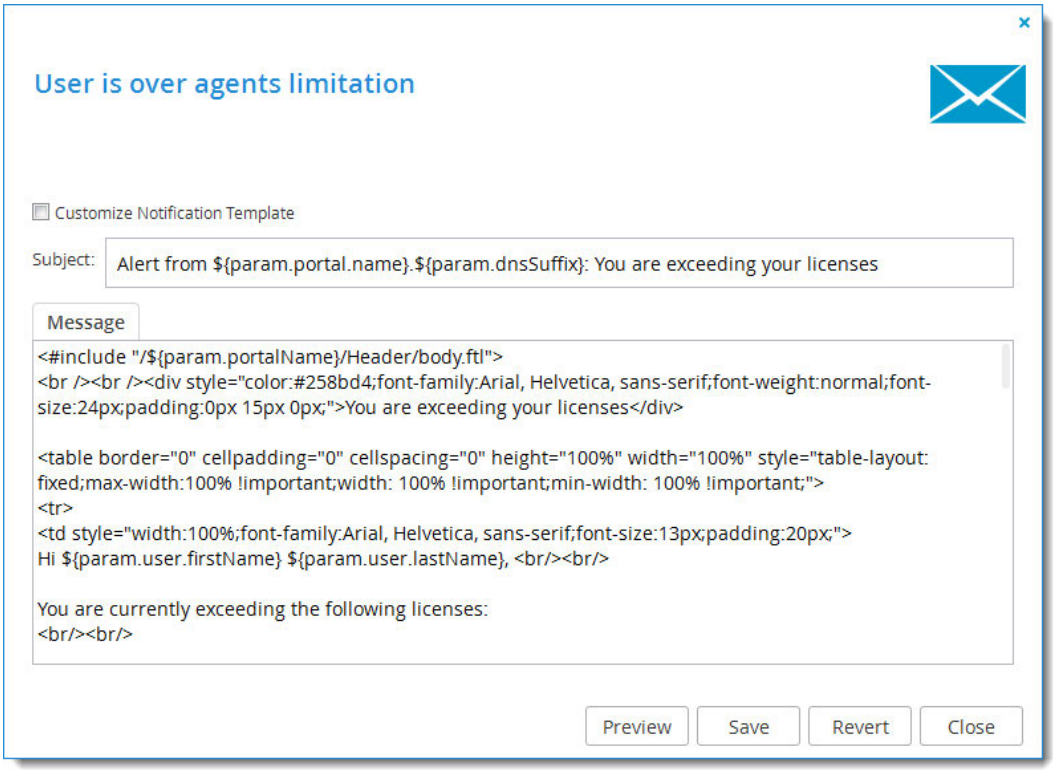
CUSTOMIZING EMAIL NOTIFICATION TEMPLATES

To customize email notification templates:

1 Select **Settings > Email Templates** from the menu.
The **Settings > Email Templates** page is displayed with a list of email templates. For a description of each template, see Email Notification Templates.

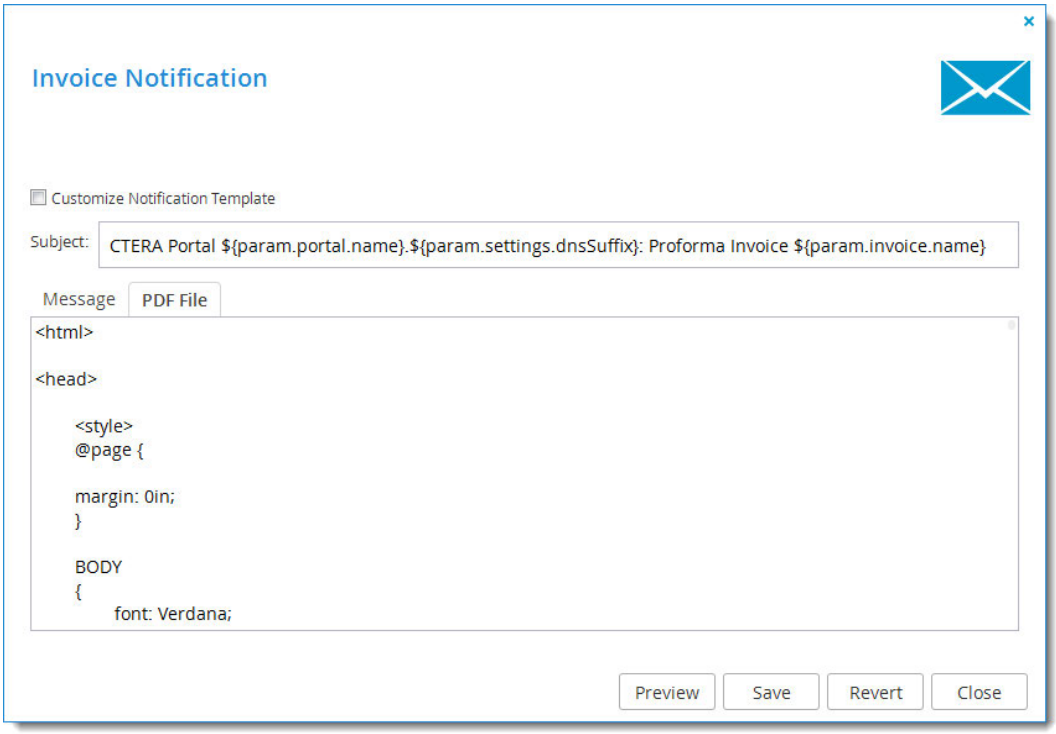


2 Select the desired email template's row and then click **Edit**.
The **Notification Template Editor** opens, displaying the **Message** tab.



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 is displayed.



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.
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. See Configuring Notification Settings.
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. See Configuring Notification Settings.
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
header	The HTML header that is displayed at the top of all notifications.
footer	The HTML footer that is displayed at the bottom of all notifications.
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.

Template Name	Description
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 Adding and Editing Email Alerts.
No Cloud 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.
Invitation to Collaborate	A guest invitation to access shared files or folders.
Malware blocked	A notification to end users to tell them that malware was detected and blocked in a file they recently uploaded.

Template Name	Description
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 reshared your folder with other people, listing the new collaborators.

17

VIEWING LOGS

The CTERA Portal **Log Viewer** includes the following 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.

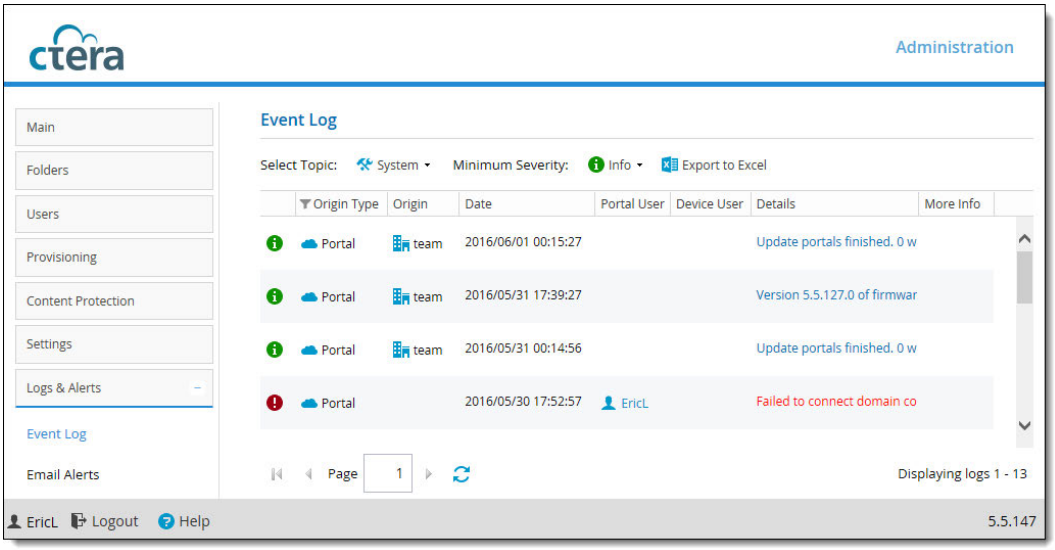
In this chapter

- Viewing System Logs
- Viewing Local Backup Logs
- Viewing Cloud Backup Logs
- Viewing Cloud Sync Logs
- Viewing Access Logs
- Viewing Audit Logs
- Viewing Agent Logs
- Exporting Logs to Excel

VIEWING SYSTEM LOGS

To view System logs:

1. Select **Logs & Alerts > Event Log** from the menu.
2. From the **Select Topic** dropdown box, select **System**.



The following information is displayed:

This field...	Displays...
Type	An icon indicating the log level. See Log Levels (page 175).
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.

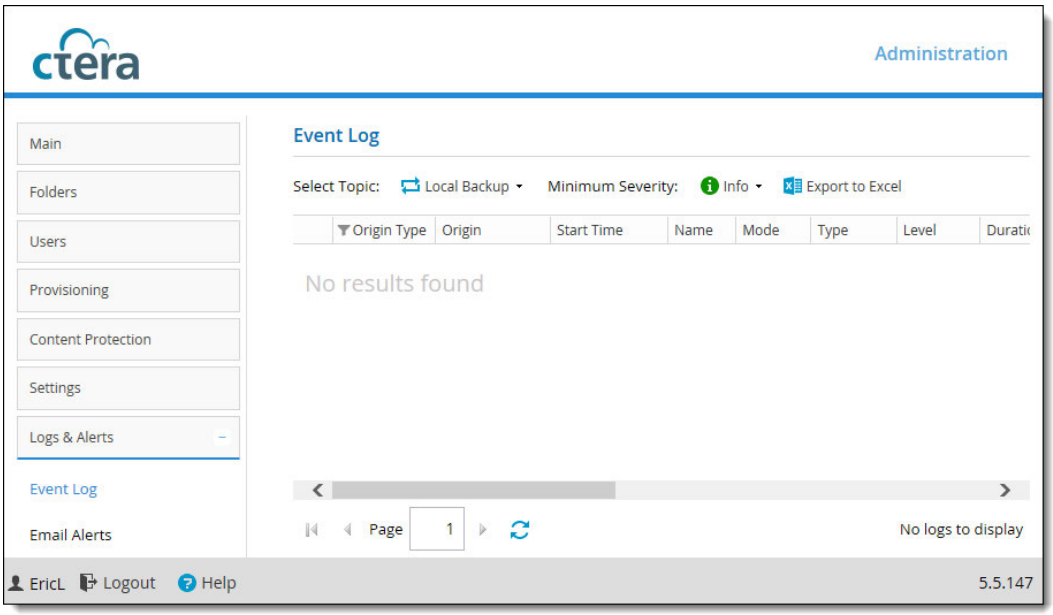
Log Levels

Icon	Log Level
	Error
	Warning
	Info
	Debug

VIEWING LOCAL BACKUP LOGS

To view Local Backup logs:

1. Select **Logs & Alerts > Event Log** from the menu.
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.

This field...	Displays...
Type	An icon indicating the log level. See Log Levels.
Origin Type	The type of entity sent the event log (a virtual portal or a device).

This field...	Displays...
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.

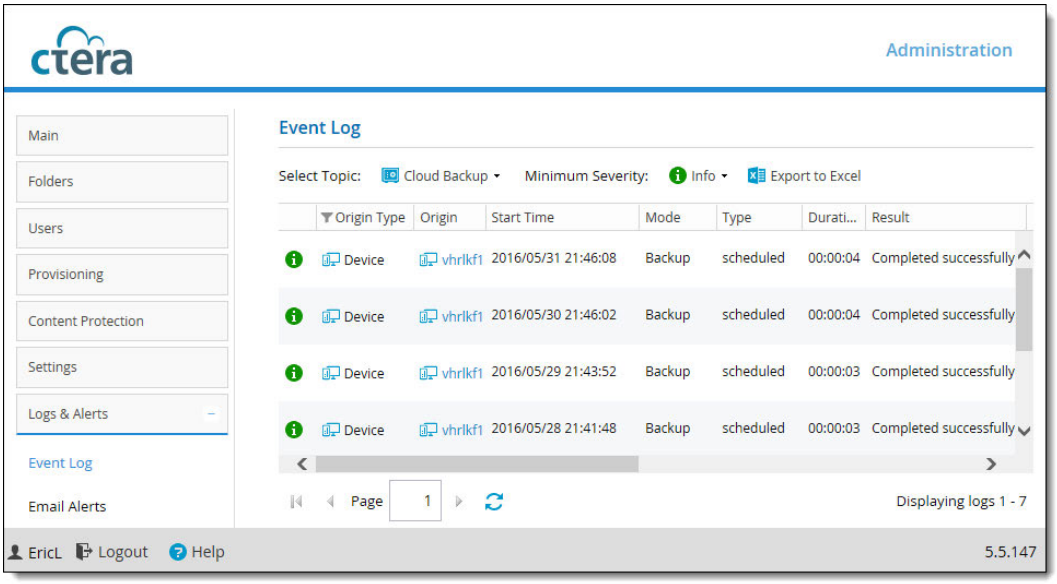
Information about files for which errors occurred is displayed in the lower pane.

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. Select **Logs & Alerts > Event Log** from the menu.
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.

This field...	Displays...
Type	An icon indicating the log level. See Log Levels (page 175).
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.

This field...	Displays...
Changed Size	The total size of the files that changed since the last backup operation.
More Info	Additional information about the event.

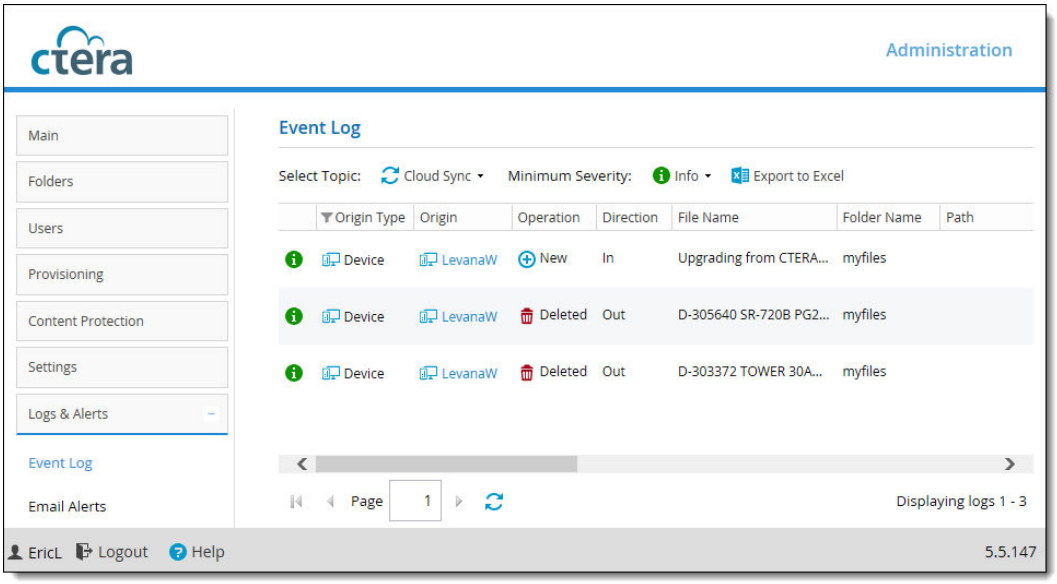
Information about files included in the backup operation is displayed in the lower pane.

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.
Dedup Ratio	The deduplication ratio for the file.
Result	The result of the backup operation.

VIEWING CLOUD SYNC LOGS

To view Cloud Sync logs:

1. Select **Logs & Alerts > Event Log** from the menu.
2. In the **Select Topic** drop-down list, select **Cloud Sync**.



The following information is displayed.

This field...	Displays...
Type	An icon indicating the log level. See Log Levels.
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.

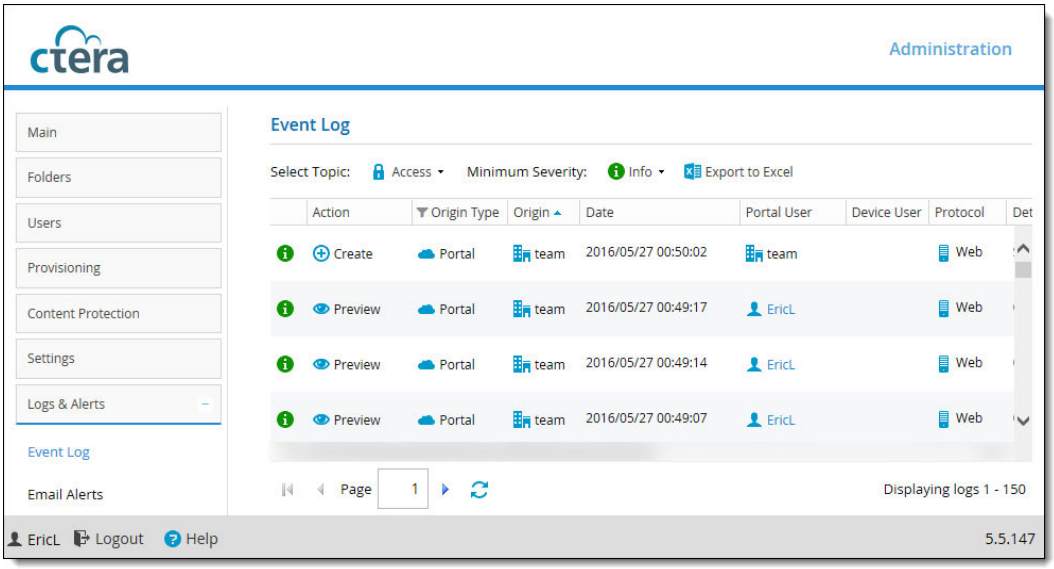
This field...	Displays...
Transferred Size	The actual amount of data transferred.
Dedup Ratio	The deduplication ratio for the file transferred during the synchronization operation.
Result	The result of the synchronization operation.

VIEWING ACCESS LOGS

To view Access logs:

1 Select **Logs & Alerts > Event Log** from the menu.

2 In the **Select Topic** drop-down list, select **Access**.



The following information is displayed:

This field...	Displays...
Type	An icon indicating the log level. See Log Levels (page 175).
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.

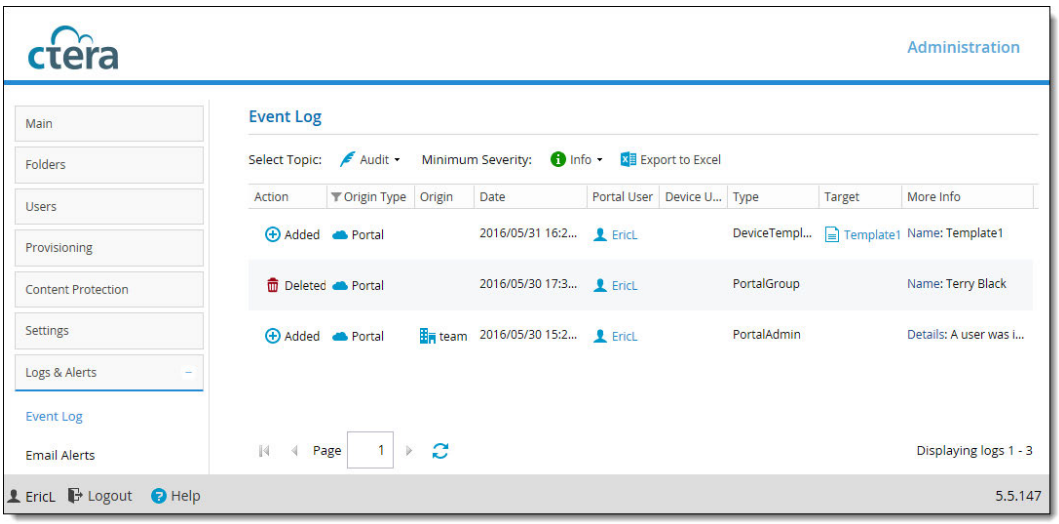
This field...	Displays...
Device User	The user who triggered the event on the device. This field is relevant only for events where the origin is a device.
Protocol	The protocol used when triggering the event: • GUI • CIFS (Windows File Sharing) • AFP • FTP • NFS • RSync • CTERA Agent • WebDAV
Details	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 Select **Logs & Alerts > Event Log** from the menu.

2 In the **Select Topic** drop-down list, select **Audit**.



The following information is displayed:

This field...	Displays...
Action	The action type. See Action Types.
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.

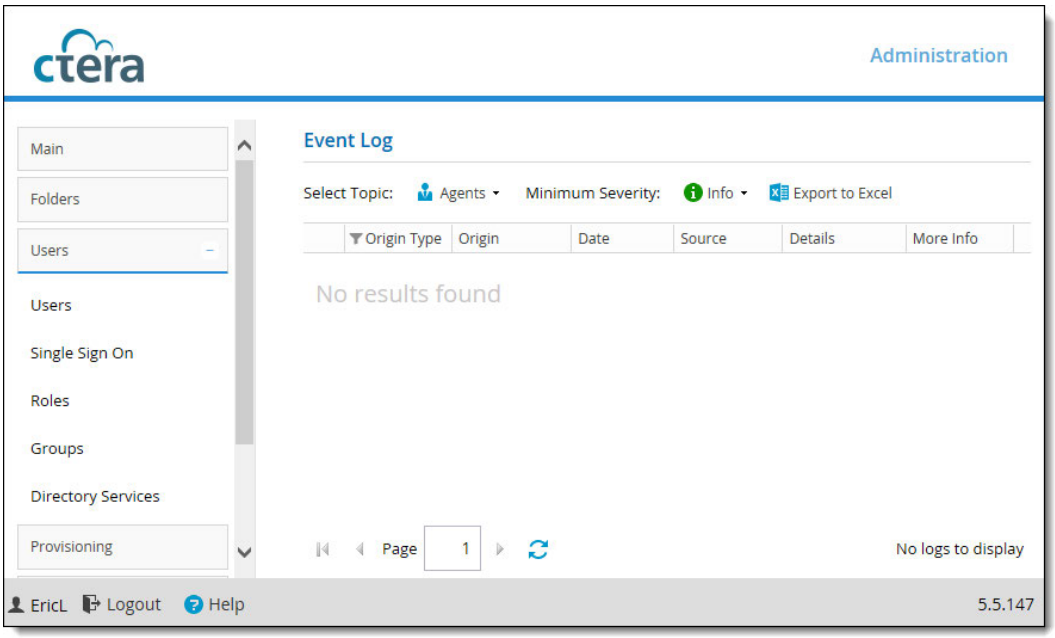
Action Types

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. Select **Logs & Alerts > Event Log** from the menu.
2. In the **Select Topic** drop-down list, select **Agents**.



The following information is displayed:

This field...	Displays...
Type	An icon indicating the log level. See Log Levels (page 175).
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.

18

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

- Viewing Email Alerts
- Adding and Editing Email Alerts
- Deleting Email Alerts

VIEWING EMAIL ALERTS

To view all email alerts:

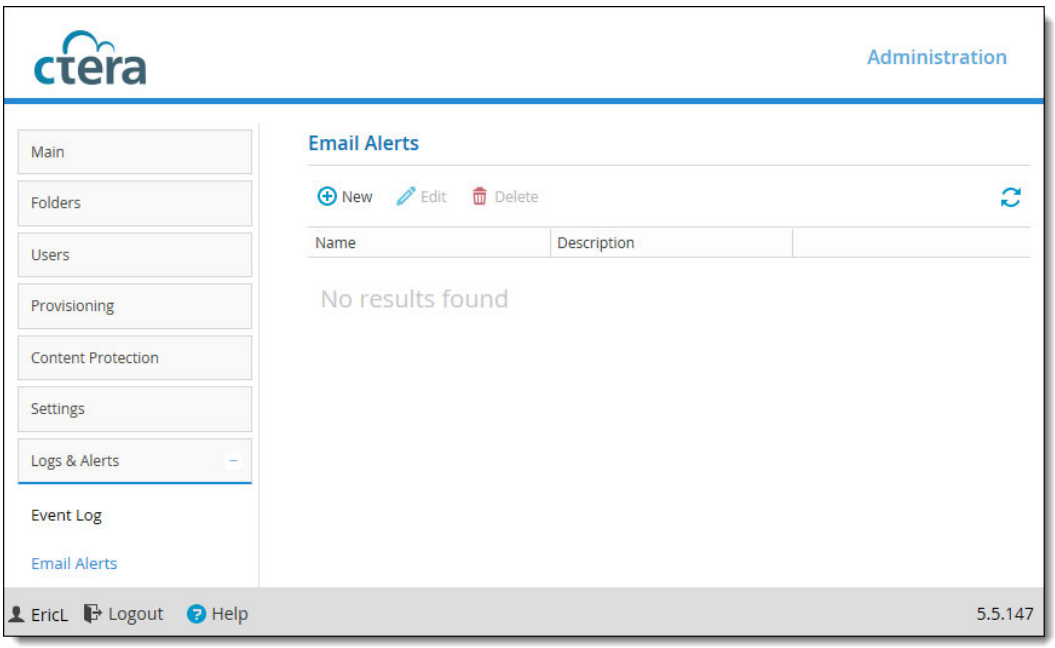
- Select **Logs & Alerts > Email Alerts** from the menu.
  The **Logs & Alerts > Email Alerts** page displays all email alerts.

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.

ADDING AND EDITING EMAIL ALERTS

To add or edit an email alert:

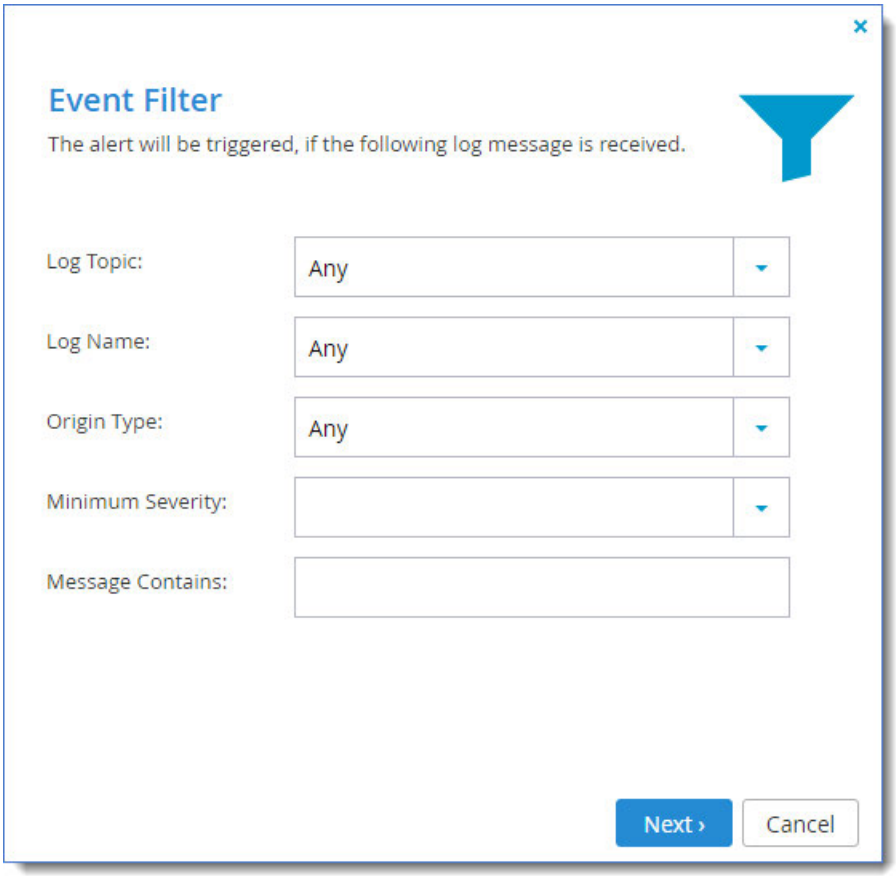
1 Select **Logs & Alerts > Email Alerts** from the menu.



2 Do one of the following:

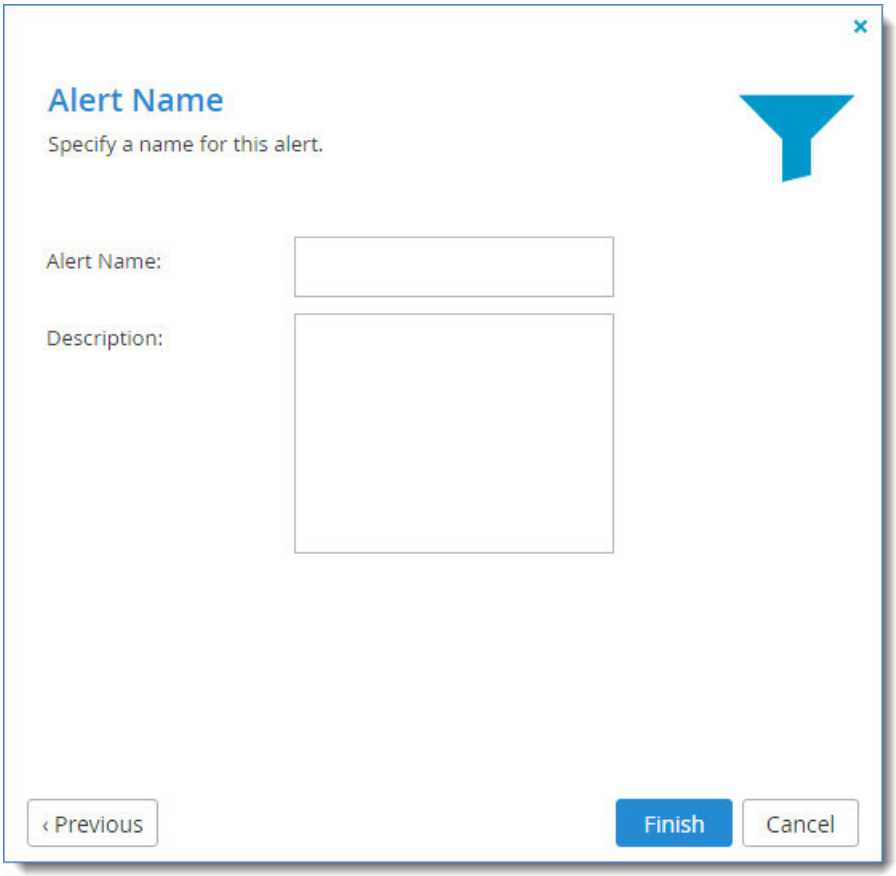
- To add a new email alert, click **New**.
- To edit an existing email alert, select the email alert's row and click **Edit**.

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 is displayed.



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**.

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. 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.
Message Contains	Type the text that the log message must contain in order to trigger 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.

19

LEGAL INFORMATION

This chapter contains important legal information about your CTERA products.

CTERA END USER LICENSE AGREEMENT

This End User License Agreement (the "**Agreement**") by and between the individual installing and/or using the Software (as such term is defined below) and any legal entity on whose behalf such individual is acting (collectively, "**You**" or "**you**") and CTERA Networks Ltd. ("**CTERA**"), governs Your use of the object code format of (i) any software or firmware program embedded or included in any hardware product supplied by CTERA or its authorized partners, and (ii) any software program supplied by CTERA or its authorized partners; and (iii) all accompanying manuals and other documentation, and all enhancements, upgrades, and extensions thereto that may be provided by CTERA or its authorized partners to You from time to time, unless otherwise indicated by CTERA (the "**Software**").

PLEASE NOTE: BY DOWNLOADING, INSTALLING, COPYING, ACCESSING, OR USING THE SOFTWARE, OR BY CHOOSING THE “I ACCEPT" OPTION LOCATED ON OR ADJACENT TO THE SCREEN WHERE THIS AGREEMENT MAY BE DISPLAYED, YOU INDICATE YOUR ACKNOWLEDGMENT THAT YOU HAVE READ THIS AGREEMENT AND AGREE TO BE BOUND BY AND COMPLY WITH ITS TERMS. YOUR WRITTEN APPROVAL IS NOT REQUIRED FOR THE VALIDITY OR ENFORCEABILITY OF THIS AGREEMENT. IF YOU ARE ACCEPTING THESE TERMS ON BEHALF OF ANOTHER PERSON OR A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT AND WARRANT THAT YOU HAVE FULL AUTHORITY TO BIND THAT PERSON, COMPANY, OR LEGAL ENTITY TO THESE SOFTWARE LICENSE TERMS. IF YOU DO NOT AGREE TO THESE SOFTWARE LICENSE TERMS, DO NOT DOWNLOAD, INSTALL, COPY, ACCESS, OR USE THE SOFTWARE AND PROMPTLY RETURN THE SOFTWARE, INCLUDING ALL PACKAGING, MEDIA, DOCUMENTATION, AND PROOF OF PAYMENT, TO THE PARTY FROM WHOM IT WAS OBTAINED FOR A REFUND OF THE AMOUNT PAID, PROVIDED THAT THE RETURN IS MADE WITHIN TEN (10) DAYS OF THE DATE OF PURCHASE.

1. License to Use Software

1.1 Subject to proper payment to CTERA and Your compliance with the terms and conditions of this Agreement, CTERA hereby grants You a non-exclusive, non-sublicensable, non-transferable license to install and use the Software, solely for Your internal business needs, in accordance with the terms set forth in this Agreement and subject to any further restrictions in CTERA documentation, and solely on the CTERA appliance on which CTERA installed the Software, or, for stand-alone Software, solely on a single computer running a validly licensed copy of the operating system for which the Software was designed. You agree that, except for the limited, specific license rights granted in this section 1, You receive no license rights to the Software.

1.2 Unless otherwise authorized in writing by CTERA and to the extent otherwise provided in the applicable license for Free Programs (as defined below), You undertake not to (and not to allow third parties to) (1) sublicense, lease, rent, loan, or otherwise transfer the Software to any third party, (2) decompile, disassemble, decrypt, extract or otherwise reverse engineer or attempt to reconstruct or discover any source code of, or any underlying ideas in, the Software ("**Reverse Engineering**"), (3) modify, enhance, supplement, adapt, or prepare derivative works from the Software, (4) allow others to use the Software and use the Software for the benefit of third parties, (5) develop any other product containing any of the concepts and ideas contained in the Software, (6) remove, obscure, or alter CTERA's or any third party's trademarks or copyright or other proprietary rights notices affixed to or contained within or accessed in conjunction with or through the Software, and (7) make unauthorized copies of the Software (except as necessary for backup purposes). If, notwithstanding the prohibition set forth in subsection (2) above, applicable law permits Reverse Engineering, You will, before commencing or permitting any Reverse Engineering (A) inform CTERA of the planned Reverse Engineering, (B) conduct or allow such Reverse Engineering only to achieve interoperability between the Software and other computer programs, (C) request from

CTERA the information necessary to achieve such interoperability, (D) provide CTERA ample opportunity to supply the information necessary to achieve interoperability.

1.3 CTERA has no obligation to provide support, maintenance, upgrades, modifications, or new releases of the Software under this Agreement. You may contact CTERA or its authorized resellers to determine the availability of such support, maintenance, distribution or upgrade of the Software, and the fees, terms and conditions applicable thereto.

2. Intellectual Property

2.1 You acknowledge that CTERA or other third parties own all right, title and interest, including all intellectual property rights, in and to the Software, portions thereof, or software or content provided through or in conjunction with the Software. Except for the license granted in accordance with Section 1 of this Agreement, all rights in and to the Software are reserved, no licenses, implied or otherwise, are granted by CTERA, You are not authorized to use CTERA's trademarks, service marks, or trade dress, and You agree not to display or use them in any manner.

2.2 If You have comments on the Software or ideas on how to improve it, please contact us. By doing so, You also grant CTERA a perpetual, royalty-free, irrevocable, transferable license, with right of sublicense, to use and incorporate Your ideas or comments into the Software (or third party software, content, or services), and to otherwise exploit Your ideas and comments, in each case without payment of any compensation.

3. GPL License

The Software makes use of free and open source programs (the "**Free Programs**"), licensed under the following license agreements: GNU General Public License (GPL), version 2 or later: www.gnu.org/ licenses/gpl.html, GNU Lesser General Public License (LGPL), version 2.1 or later: www.gnu.org/ licenses/lgpl.html, Apache License, Version 2.0 or later: www.apache.org/licenses/LICENSE-2.0. It is Your responsibility to review and adhere to all licenses to Free Programs.

Notwithstanding anything to the contrary in this Agreement, You may redistribute the Free Programs and/or modify them under the terms of the corresponding license agreement. The Free Programs are distributed in the hope that they will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. To obtain the source code for the Free Programs subject to the terms of the corresponding license agreement, please send a request by mail to: Open Source Requests, CTERA Networks Ltd, 25 Efal St., Petach Tikva, Israel.

4. Third Party Software

Software licensed to CTERA by third parties for direct or indirect distribution to end users ("**Third Party Software**") may be embedded in the Software and sublicensed directly to You. Third Party Software is provided to You subject to separate licenses directly between You and the third party licensor, available from CTERA at Your request. You will have no recourse against CTERA unless CTERA is the stated licensor and then only to the extent provided in such license. You will be responsible to do whatever is necessary or required by the third party licensor for the licenses and related terms to take effect (e.g. online registration). You are also accepting the terms and conditions of the licenses applicable to any Third Party Software (including any open source software) included with the Software.

5. Acceptable Use and Conduct

You shall use the Software in compliance with all applicable laws, ordinances, rules and regulations, shall not violate or attempt to violate CTERA's system or network security, and shall not misuse the Software in any way. You shall be responsible for Your conduct while using the Software.

6. Term and Termination

CTERA shall have the right to terminate this Agreement at any time due to Your breach of this Agreement by providing You with a written notice. Upon CTERA's termination of this Agreement, You shall not be entitled to any compensation, reimbursement or damages of any kind. You shall have the right to terminate this Agreement at any time due to CTERA's breach of this Agreement by providing CTERA with a written notice. You agree that, upon termination or expiration of this Agreement for any reason, You will cease using the Software and either destroy all copies of the Software and CTERA

documentation or return them to CTERA. The provisions of this Agreement, other than the license granted in section 1 ("License to Use Software"), shall survive termination.

7. Disclaimer of Warranties

THE SOFTWARE IS PROVIDED “AS IS”. CTERA AND CTERA'S LICENSORS AND RESELLERS MAKE NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE WITH RESPECT TO THE SOFTWARE. EXCEPT TO THE EXTENT PROHIBITED BY APPLICABLE LAW, CTERA AND ITS LICENSORS AND RESELLERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, QUIET ENJOYMENT, AND ANY WARRANTIES ARISING OUT OF ANY COURSE OF DEALING OR USAGE OF TRADE. CTERA AND ITS LICENSORS AND RESELLERS DO NOT WARRANT THAT THE SOFTWARE WILL FUNCTION AS DESCRIBED, WILL BE UNINTERRUPTED OR ERROR FREE, OR FREE OF HARMFUL COMPONENTS, OR THAT THE DATA YOU STORE BY USING THE SOFTWARE WILL BE SECURE OR NOT OTHERWISE LOST OR DAMAGED. NO ADVICE OR INFORMATION OBTAINED BY YOU FROM CTERA OR FROM ANY THIRD PARTY OR THROUGH THE SOFTWARE SHALL CREATE ANY WARRANTY NOT EXPRESSLY STATED IN THIS AGREEMENT. YOU UNDERSTAND AND AGREE THAT YOU USE THE SOFTWARE, AND ALL THIRD PARTY SOFTWARE OR SERVICES MADE AVAILABLE IN CONJUNCTION WITH OR THROUGH THE SOFTWARE, AT YOUR OWN DISCRETION AND RISK AND THAT YOU WILL BE SOLELY RESPONSIBLE FOR ANY DAMAGES TO YOUR COMPUTER SYSTEM OR LOSS OF DATA THAT RESULTS FROM THE USE OF THE SOFTWARE AND SUCH THIRD PARTY SOFTWARE AND SERVICES. SOME STATES OR OTHER JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO THE ABOVE EXCLUSIONS MAY NOT APPLY TO YOU. YOU MAY ALSO HAVE OTHER RIGHTS THAT VARY FROM STATE TO STATE AND JURISDICTION TO JURISDICTION. THIS SECTION CONSTITUTES A CONTRACT FOR THE BENEFIT OF EACH OF CTERA'S LICENSORS, RESELLERS AND DISTRIBUTORS.

8. Limitation of Liability

NEITHER CTERA NOR ANY OF ITS LICENSORS AND RESELLERS SHALL BE LIABLE TO YOU FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL OR EXEMPLARY DAMAGES (EVEN IF CTERA ITS LICENSORS OR RESELLERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES) IN CONNECTION WITH THIS AGREEMENT, INCLUDING, WITHOUT LIMITATION, ANY SUCH DAMAGES RESULTING FROM: (i) THE USE OR THE INABILITY TO USE THE SOFTWARE; (ii) THE COST OF PROCUREMENT OF SUBSTITUTE GOODS AND SERVICES; OR (iii) UNAUTHORIZED ACCESS TO OR ALTERATION OF YOUR CONTENT. IN ANY CASE AND WITHOUT DEROGATING FROM THE ABOVE, TO THE EXTENT THAT THE AFOREMENTIONED LIMITATION OF LIABILITY SHALL NOT BE ENFORCEABLE, CTERA'S AGGREGATE LIABILITY UNDER THIS AGREEMENT AND ANY OTHER AGREEMENT BETWEEN CTERA AND YOU SHALL BE LIMITED TO THE LOWER OF (I) THE AMOUNT ACTUALLY PAID BY YOU TO CTERA FOR THE SOFTWARE WHICH IS THE SUBJECT MATTER OF THE CLAIM, OR (II) US$1,000,000. THE SOFTWARE IS NOT INTENDED FOR USE IN CONNECTION WITH ANY INHERENTLY DANGEROUS APPLICATION. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF CERTAIN WARRANTIES OR THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES. ACCORDINGLY, SOME OR ALL OF THE ABOVE EXCLUSIONS OR LIMITATIONS MAY NOT APPLY TO YOU, AND YOU MAY HAVE ADDITIONAL RIGHTS. THIS SECTION CONSTITUTES A CONTRACT FOR THE BENEFIT OF EACH OF CTERA'S LICENSORS, RESELLERS AND DISTRIBUTORS.

9. Indemnification by You

9.1 You shall indemnify, defend and hold CTERA, its affiliates and licensors, each of its and their business partners and each of its and their respective employees, officers, directors and representatives, harmless from and against any and all claims, losses, damages, liabilities, judgments, penalties, fines, costs and expenses (including reasonable attorney fees), arising out of or in connection with any claim arising out of (i) Your use of the Software in a manner not authorized by this Agreement, and/or in violation of the applicable restrictions and/or applicable law, (ii) Your violation of any term or condition of this Agreement or any applicable additional policies, or (iii) Your or Your employees’ or personnel’s negligence or willful misconduct.

9.2 CTERA shall promptly notify You of any claim subject to indemnification; provided that CTERA's failure to do so shall not affect Your obligations hereunder, except to the extent that CTERA's failure to promptly notify You materially delays or prejudices Your ability to defend the claim. At CTERA's option, You will have the right to defend against any such claim with counsel of Your own choosing (subject to CTERA's written consent) and to settle such claim as You deem appropriate,

provided that You shall not enter into any settlement without CTERA's prior written consent and provided that CTERA may, at any time, elect to take over control of the defense and settlement of the claim.

10. Indemnification by CTERA

Notwithstanding CTERA's disclaimer of any warranty of non-infringement as set forth in Section 7 above, in special circumstances, in CTERA's sole discretion, CTERA may choose to indemnify You in accordance with the provisions of this Section 10.

10.1 Indemnification. CTERA may defend or settle, at its option and expense, any action brought by a third party against You, only to the extent such action arises from any third party claim brought against You alleging that the Software infringes any patent, copyright, trademark, trade secret, or other intellectual property right of any third party (the "**IP Claim**"), and may pay all costs, liabilities, damages and legal fees finally awarded against You in, or paid in settlement of, such action.

10.2 Remedy by CTERA. In the event that any Software or portion thereof is held, or in CTERA's reasonable opinion may be held, to constitute an infringement, CTERA, at its option and expense, may either (i) obtain for You the right to continue to use such Software as contemplated herein, (ii) modify such Software so that it becomes non-infringing, but without materially altering its functionality, (iii) replace such Software with a functionally equivalent non infringing Product, or (iv) terminate this Agreement and provide you with a refund of the amount paid for the infringing Software.

10.3 Exceptions. The foregoing does not apply to claims to the extent arising from: (i) the combination of a Software with other products not supplied by or on behalf of CTERA where such claim would not have arisen from the use of the Software standing alone, (ii) compliance by CTERA with Your specifications, (iii) any modification of the Software not made by or on behalf of CTERA, where such claim would not have arisen but for such modification, or (iv) where You continue an activity where such claim would not have arisen but for such activity after having received and had a commercially reasonable time to install modifications from CTERA that would have completely avoided the activity.

10.4 Entire Liability. This section 10 states the entire liability of CTERA and Your exclusive remedy for any proceedings or claims that the Software infringes or misappropriates a third party's intellectual property, in respect of which CTERA chooses to provide indemnification.

10.5 Requirements for Indemnity. You agree to provide CTERA with (i) prompt written notice of the IP Claim giving rise to CTERA's indemnity option hereunder, (ii) sole control over the defense or settlement of such claim or action, if CTERA so requests (provided that CTERA shall not, without Your prior written consent, settle any such claim or action if such settlement contains a stipulation to or admission or acknowledgment of any liability or wrongdoing on Your part), and (iii) reasonable information and assistance in the defense and/or settlement any such claim or action at CTERA's option and expense.

11. Miscellaneous Provisions

11.1 The Software may be subject to export control laws of the State of Israel and/or may be subject to additional export control laws applicable to You or in Your jurisdiction. You shall not ship, transfer, or export the Software into any country, or make available or use the Software in any manner, prohibited by law. You warrant and agree that You are not: (i) located in, under the control of, or a national or resident of Cuba, Iran, North Korea, Syria or Sudan, or (ii) on the U.S Treasury Department list of Specially Designated Nationals or the U.S. Commerce Department's Table of Deny Orders.

11.2 This agreement will be governed by and construed in accordance with the laws of the State of Israel, without giving effect to any conflict of laws and provisions that would require the application of the laws of any other jurisdiction. The parties hereby expressly reject any application to this Agreement of (a) the United Nations Convention on Contracts for the International Sale of Goods; and (b) the 1974 Convention on the Limitation Period in the International Sale of Goods, as amended by that certain Protocol, done at Vienna on April 11, 1980.

11.3 All disputes arising out of this Agreement will be subject to the exclusive jurisdiction of the competent courts of Tel Aviv, Israel, and the parties agree and submit to the personal and exclusive jurisdiction and venue of these courts, except

that nothing will prohibit CTERA from instituting an action in any court of competent jurisdiction to obtain injunctive relief or protect or enforce its intellectual property rights.

11.4 The failure of CTERA to exercise or enforce any right or provision of this Agreement does not constitute a waiver of such right or provision. If for any reason a court of competent jurisdiction finds any provision or portion of this Agreement to be unenforceable, the remainder of this Agreement will continue in full force and effect.

11.5 This Agreement constitutes the entire agreement between CTERA and You with respect to the subject matter hereof and supersedes and replaces all prior or contemporaneous understandings or agreements, written or oral, regarding such subject matter. Any waiver of any provision of this Agreement will be effective only if in writing and signed by CTERA.

11.6 You may not assign or transfer any of Your rights or obligations under this Agreement to a third party without the prior written consent of CTERA. CTERA may freely assign this Agreement. Any attempted assignment or transfer in violation of the foregoing will be void.

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.,

51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you

receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program

itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not

distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED

INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

GNU GENERAL PUBLIC LICENSE 3

Version 3, 29 June 2007

Copyright © 2007 Free Software Foundation, Inc.

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The GNU General Public License is a free, copyleft license for software and other kinds of works.

The licenses for most software and other practical works are designed to take away your freedom to share and change the works. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change all versions of a program--to make sure it remains free software for all its users. We, the Free Software Foundation, use the GNU General Public License for most of our software; it applies also to any other work released this way by its authors. You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

Developers that use the GNU GPL protect your rights with two steps: (1) assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger

that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS

0. Definitions.

“This License” refers to version 3 of the GNU General Public License.

“Copyright” also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

“The Program” refers to any copyrightable work licensed under this License. Each licensee is addressed as “you”. “Licensees” and “recipients” may be individuals or organizations.

To “modify” a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a “modified version” of the earlier work or a work “based on” the earlier work.

A “covered work” means either the unmodified Program or a work based on the Program.

To “propagate” a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To “convey” a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays “Appropriate Legal Notices” to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.

The “source code” for a work means the preferred form of the work for making modifications to it. “Object code” means any non-source form of a work.

A “Standard Interface” means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The “System Libraries” of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A “Major Component”, in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The “Corresponding Source” for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically

linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed; section 10 makes it unnecessary.

3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures.

4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice; keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

a) The work must carry prominent notices stating that you modified it, and giving a relevant date.

b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to “keep intact all notices”.

c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts,

regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.

d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an “aggregate” if the compilation and its resulting copyright are not used to limit the access or legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.

b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.

c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b.

d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.

e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A “User Product” is either (1) a “consumer product”, which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, “normally used” refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

“Installation Information” for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed

under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.

“Additional permissions” are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or

b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or

c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or

d) Limiting the use for publicity purposes of names of licensors or authors of the material; or

e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or

f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.

All other non-permissive additional terms are considered “further restrictions” within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits

relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An “entity transaction” is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.

A “contributor” is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's “contributor version”.

A contributor's “essential patent claims” are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further

modification of the contributor version. For purposes of this definition, “control” includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a “patent license” is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To “grant” such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. “Knowingly relying” means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is “discriminatory” if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the special requirements of

the GNU Affero General Public License, section 13, concerning interaction through a network will apply to the combination as such.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License “or any later version” applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

17. Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in

connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

APACHE LICENSE

Version 2.0, January 2004

http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against

any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

a. You must give any other recipients of the Work or Derivative Works a copy of this License; and

b. You must cause any modified files to carry prominent notices stating that You changed the files; and

c. You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

d. If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor

harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

POSTGRESQL DATABASE MANAGEMENT SYSTEM (FORMERLY KNOWN AS POSTGRES, THEN AS POSTGRES95)

Portions Copyright (c) 1996-2013, The PostgreSQL Global Development Group

Portions Copyright (c) 1994, The Regents of the University of California

Permission to use, copy, modify, and distribute this software and its documentation for any purpose, without fee, and without a written agreement is hereby granted, provided that the above copyright notice and this paragraph and the following two paragraphs appear in all copies.

IN NO EVENT SHALL THE UNIVERSITY OF CALIFORNIA BE LIABLE TO ANY PARTY FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, INCLUDING LOST PROFITS, ARISING OUT OF THE USE OF THIS SOFTWARE AND ITS DOCUMENTATION, EVEN IF THE UNIVERSITY OF CALIFORNIA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

THE UNIVERSITY OF CALIFORNIA SPECIFICALLY DISCLAIMS ANY WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE SOFTWARE PROVIDED HEREUNDER IS ON AN "AS IS" BASIS, AND THE UNIVERSITY OF CALIFORNIA HAS NO OBLIGATIONS TO PROVIDE MAINTENANCE, SUPPORT, UPDATES, ENHANCEMENTS, OR MODIFICATIONS.