User Guide

CTERA C-Series

July 2013
Version 4.0

Tip

For legal information and for the end user license agreement, refer to ***Legal Information*** (on page 335) in this guide.

Safety Warning

Carefully read the Safety Instructions and Operating Procedures provided in this guide before attempting to install or operate the appliance. Failure to follow these instructions may result in damage to equipment and/or personal injuries, and will void your warranty.

- This product contains no user-serviceable parts. Repair, maintenance and servicing of this appliance are to be carried out only by qualified CTERA personnel.
- This product may only be used for the applications described in the user guide, and only in connection with accessories which have been approved by CTERA.
- This product can only function correctly and safely if it is transported, stored, set up, and installed correctly, and operated and maintained as recommended.
- Operate this product only from the type of power source indicated on the product's marking label.
- You must use only the power supply that originally comes with your product.
- Overloaded AC outlets, extension cords, frayed power cords, damaged or cracked wire insulation, and broken plugs are dangerous. They may result in an electrical shock or fire hazard.
- Route power supply cords so that they are not likely to be walked on or pinched by items placed upon or against them.
- Slots and openings in the enclosure are provided for ventilation, to ensure reliable operation of the product and to protect it from overheating. Do not block or cover these openings.
- Never place this product near or over a heat source. Do not place this product in a built-in installation, such as a bookcase or equipment rack, unless you provide proper ventilation.
- Shutting down the appliance does not disconnect it from the power system. To establish a complete power separation, you must unplug the appliance from the wall outlet.
- Never push objects of any kind into this product through openings, as they may touch dangerous voltage or "short-out" parts, which could result in a fire or electric shock.
- To provide added protection for this product during a lightning storm, or when it is left unattended and unused for long periods of time, unplug it from the wall outlet.
- Refer servicing to qualified service personnel in the following situations:
  - When the power supply cord or plug is damaged
  - If objects have fallen into the product
  - If the product has been exposed to rain or water
  - If the product has been dropped or the enclosure has been damaged

Contents

1

Introduction

This chapter introduces the CTERA appliance and Cloud Attached Storage technology.

In This Chapter

About Cloud Attached Storage

Cloud Attached Storage® combines a Network Attached Storage appliance in your local network with online cloud services. File sharing is performed on the local network, while cloud storage services are used for off-site backup, file sync and share (FSS), and disaster recovery. Automated block-level incremental backup and restore functions include de-duplication, compression, and encryption technologies, for secure and efficient synchronization between the cloud storage service and the CTERA appliance.

About Your CTERA Cloud Attached Storage Appliance

CTERA appliances are ideal for small businesses, branch offices, and workgroups that want to share files, synchronize folders across their network, and enjoy secure, transparent, and disaster-proof backup of critical data.

The CTERA appliances covered in this guide include the CTERA C200, C400, and C800.

Combining the functionalities of a standalone Network Attached Storage (NAS) device, file server, and backup tape drive in a single appliance, the CTERA appliance allows you to do all of following:

- Share files across your network
- Synchronize folders across your network and the cloud
- Back up files online, securely and automatically
- Restore multiple file versions
- Access backed-up files from anywhere, using a Web browser

Using the appliance, data is synchronized between your computer and the appliance drives, then transparently backed up to an offsite storage facility in the cloud. Backups are encrypted using high-grade AES encryption and encoded to maximize bandwidth utilization. Users can recover files stored locally on the appliance, and even in the event that the appliance is damaged, the files can easily be restored from cloud backup using a Web browser.

Once installed, the CTERA appliance can easily be controlled using an intuitive Web-based interface or managed centrally through the CTERA Portal.

Contacting Technical Support

If you require assistance in configuring or using your appliance, contact technical support at http://www.ctera.com/support.

2

CTERA C200 Specifications and Installation

This chapter describes the following:

- The CTERA C200 package contents, hardware, and specifications.
- CTERA C200 installation
- Hard drive installation and removal

In This Chapter

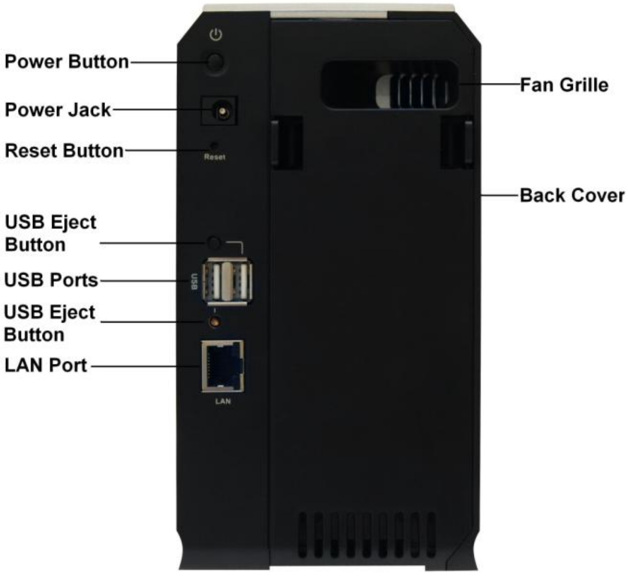
Package Contents

Your appliance package contains the following items:

- CTERA C200
- Power supply cable
- Ethernet LAN cable

Rear Panel

Network and power connections are made via the appliance's rear panel.



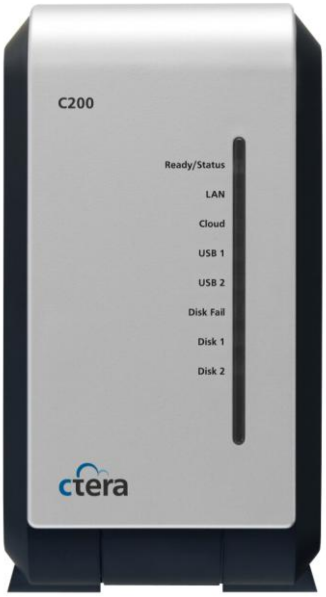
The appliance rear panel contains the following elements:

Table 1: C200 Rear Panel Elements

Element	Description
Power button	A button used for turning the appliance on and off.
Power jack	A power jack used for supplying power to the appliance. Connect the power supply cable provided in the appliance package to this jack.
Reset	A button used for restarting the appliance or resetting it to its default settings. For information, see ***Restarting the CTERA Appliance*** (on page 332) and ***Resetting the CTERA Appliance to Its Default Settings*** (on page 331).
USB	Two USB 2.0 ports used for connecting USB drives. Note that you can connect more than two USB drives, by connecting a powered USB hub. Be sure to use a powered hub, in order to avoid exceeding the power capacity of the USB ports.
LAN	An Ethernet port used for connecting the appliance to your Ethernet LAN switch or router. Connect the Ethernet cable provided in the appliance package to this port. For best performance, use a Gigabit-capable Ethernet switch.
Back cover	The back cover opens to allow insertion of up to two SATA 3.5" hard drives.
Fan grille	Do not cover or obstruct the fan grille as it is needed for proper cooling of your appliance.
USB Eject 1 / USB Eject 2	Buttons used to eject the USB drives. Each button ejects the USB drive connected to the port that is adjacent to the button. After ejecting a USB drive, wait until the USB LED turns off. You can then safely remove the USB drive from the system.

Front Panel

The C200's front panel includes a set of LEDs that indicate the C200's current status.



The following table explains the C200 front panel LEDs:

Table 2: C200 Front Panel LEDs

LED	State	Explanation
Ready/Status	Short red blink, followed by a green blink	The appliance is starting up.
	On (Green)	The appliance is operational.
	Heartbeat (Red)	The appliance is rebooting.
LAN	On	A link has been established for the LAN port.
	Blinking	Data is being transmitted or received.
Cloud	On	The appliance is connected to the CTERA Portal.
	Blinking slowly	The appliance is resolving the CTERA Portal address.
	Blinking fast	The appliance is connecting to the CTERA Portal.
	Off	The appliance is disconnected from the CTERA Portal.
USB 1 /2	On	A USB storage device is attached.
	Off	No USB storage device is attached, or the USB storage device has been successfully ejected and may be unplugged.
Disk Fail	On	An array has failed.
	Blinking fast	A disk has failed.
	Blinking slowly	An array is degraded.
	Heartbeat	A disk is unhealthy.
	Off	There are no disk failures.
Disk 1 / 2	On (Green)	A disk is installed in the SATA bay.
	Blinking (Green)	The disk is in use.
	On (Orange)	The disk format is unrecognized. The disk should be formatted.

Technical Specifications

Software Features

Table 3: Software Features

Feature	Description
CTERA Agents	20 Workstation Agent licenses included Additional Workstation/Server Agent licenses available
Supported File Systems	EXT3, NEXT3™, FAT32, NTFS, ExFAT
Supported File Sharing Protocols	CIFS (Windows File Sharing), NFS, FTP, WebDAV, RSync, AFP (Apple File Sharing)
Supported Discovery Protocols	UPnP, Bonjour
RAID Levels	RAID0, RAID1, JBOD
S.M.A.R.T Monitoring	Yes

Cloud Service Features

Table 4: Cloud Service Features

Feature	Description
Backup Files Security	AES-256 Encryption, SHA-1 fingerprints, optional secret passphrase
Protocol Security	SSL (Secure Socket Layers)
Efficiency	Incremental updates, Data Compression, Block Level Deduplication
Versioning	Retention of previous file versions
Additional Services	Centralized Management, Centralized Monitoring, Reporting, Logging, Remote Access, Offline Backup Seeding

Hardware Features

Table 5: Hardware Features

Feature	Description
Internal Hard Drives	2 x 3.5" SATA Hot Swap (not included)
Maximum Storage Capacity	4TB
Ports	2 x USB 2.0 high-speed ports for external drives, 1 x Gigabit Ethernet
Maximum Power Consumption	50W
Compliance	FCC, CE, RoHS, WEEE
Operating Environment	0-40°C, Humidity 5%-90% (non-condensed)
Dimensions	162.5(H) x 210(D) x 95(W) mm / 6.4(H) x 8.27(D) x 3.74(W) inch
Weight	1.1Kg (excluding hard drives)

Requirements

Hardware Requirements

In order to install the CTERA appliance, you will need the following:

- At least one hard drive (SATA, 3.5")
- A network connection or router with DHCP enabled

Software Requirements

In order to use the appliance Web interface, you will need the following:

- Either Microsoft Internet Explorer 7.0 or later, Mozilla Firefox 3.0 or later, or Google Chrome 5.0 or later
- Adobe Flash Player

Opening Ports on Your Firewall

In order to back up roaming PCs and remote offices *outside* your network using the CTERA Agent, you must open your firewall for the network where the CTERA appliance is located, to allow incoming TCP ports 995 and 873 to the CTERA appliance.

Installing the CTERA C200

To install the CTERA C200

1 Install at least one hard drive in the appliance.

See ***Installing a SATA Hard Drive in the CTERA C200*** (on page 11).

2 Connect one end of the Ethernet cable to the LAN port, and connect the other end to your Ethernet LAN switch or router.

3 Connect the provided power supply cable to the power jack, and connect the power supply to the wall outlet.

4 Press the Power button at the back of the appliance.

The appliance will start up, and the **Ready/Status** LED will flash rapidly in orange and then green. When the LED turns steady green, the appliance is ready.

The appliance automatically obtains an IP address using DHCP.

Tip

If a DHCP server is not available, then after one minute, the appliance will use the IP address 192.168.192.5.

Warning

If you need to unplug the appliance, you must first shut it down as described in ***Shutting Down the CTERA Appliance*** (on page 333). Failure to do so could result in data loss.

Installing a SATA Hard Drive in the CTERA C200

To install a SATA hard drive

1 Open the appliance's back cover, by pressing the two plastic tabs and then pulling backwards.

Two slots are revealed.

2 Insert the SATA hard drive into a vacant slot, pressing it firmly until it is all the way in.

If you install the drive in left-hand slot, the drive's metal cover should be facing left.

If you install the drive in the right-hand slot, the drive's metal cover should be facing right.

3 Close the appliance's back cover, by inserting first the *bottom* of the cover, pressing the tabs, and then pushing forwards.

The cover should click into place.

Removing a SATA Hard Drive from the CTERA C200

Tip

If you want to remove a hard drive safely while the appliance is on, use the Safe Removal procedure described in ***Safely Removing Hard Drives*** (on page 84).

To remove a SATA hard drive

1 Open the appliance's back cover, by pressing the two plastic tabs and then pulling backwards.

2 Remove the SATA hard drive from its slot.

3 Close the appliance's back cover, by inserting first the *bottom* of the cover, pressing the tabs, and then pushing forwards.

The cover should click into place.

Connecting USB Drives

If desired, you can connect a USB drive to the appliance.

To connect a USB drive to the appliance

1. Connect one end of a USB cable into the USB drive.
2. Connect the other end of the USB cable to the appliance's USB port.

3

CTERA C400 Specifications and Installation

This chapter describes the following:

- The CTERA C400 package contents, hardware, and specifications.
- CTERA C400 installation
- Hard drive installation and removal

Tip

The specifications in this chapter relate to the hardware model: CTERA C400-1.

In This Chapter

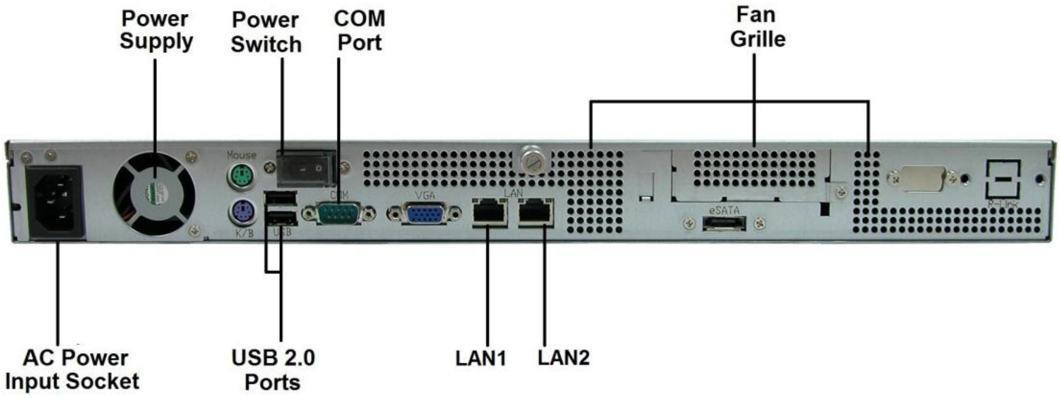
Package Contents

Your appliance package contains the following items:

- CTERA C400
- Power cord
- Two Ethernet LAN cables
- Quick Start Guide
- Rack mounting kit
- Plastic bag containing screws for both hard drive installation and rack mounting

Rear Panel

Network and power connections are made via the appliance's rear panel.



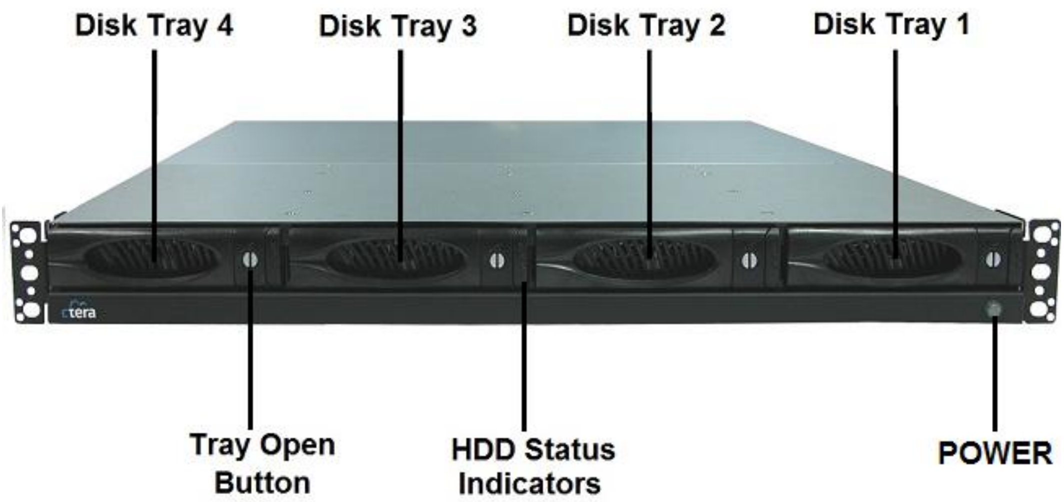
The appliance rear panel contains the following elements:

Table 6: C400 Rear Panel Elements

Element	Description
COM	A serial (RS-232) console port used for connecting to the appliance console. The console can be used for advanced troubleshooting and maintenance operations.
USB	Four USB 2.0 ports used for connecting USB drives. Note that you can connect more than four USB drives, by connecting a powered USB hub. Be sure to use a powered hub, in order to avoid exceeding the power capacity of the USB ports.
LAN1/LAN2	Two Ethernet ports used for connecting the appliance to your Ethernet LAN switch or router. Connect the Ethernet cables provided in the appliance package to these ports. To use both ports in parallel, configure link aggregation, as described in ***Enabling/Disabling Link Aggregation*** (on page 268). For best performance, use a Gigabit-capable Ethernet switch.
Power switch	A switch used for turning the appliance on and off and resetting it.
Fan grille	Do not cover or obstruct the fan grille as it is needed for proper cooling of your appliance.
AC power input socket	A socket used for supplying power to the appliance. Connect the power supply cable provided in the appliance package to this socket.
Power supply	The appliance's power supply.

Front Panel

The C400's front panel appears as follows:



The front panel's interior contains the following elements:

Table 7: C400 Front Panel Interior Elements

Element	Description		
Disk Tray 1-4	Four disk trays for installing hard drives.		
Tray Open Button	Each disk tray has a Tray Open Button, which serves the following purposes: • Indicates whether the disk tray is locked. When the button's groove is horizontal, the disk tray is locked. When it is vertical, the disk tray is open. • Enables you to lock/unlock the disk tray, by using a flat-head screwdriver to turn the button until its groove is horizontal/vertical. • Enables you to open the disk tray. Upon pressing the button, the outer panel of the disk tray (visible in the preceding diagram) becomes a lever that can be used to pull the disk tray out of the appliance.		
HDD Status Indicators	Each disk tray has two LEDs that indicate its status:		
	LED	**State**	**Explanation**
	Upper LED	Blinking (Blue)	Disk activity
	Lower LED	On (Green)	OK
		On (Red)	Disk failure

	Blinking (Red)	RAID array failure
POWER	A LED indicating whether the appliance is operational:	
	State	**Explanation**
	On (Green)	The appliance is on.
	Off	The appliance is off.

Technical Specifications

Software Features

Table 8: Software Features

Feature	Description
CTERA Agents	50 Workstation Agent licenses included Additional Workstation/Server Agent licenses available
Supported File Systems	EXT3, NEXT3™, FAT32, NTFS, ExFAT
Supported File Sharing Protocols	CIFS (Windows File Sharing), NFS, FTP, WebDAV, RSync, AFP (Apple File Sharing)
Supported Discovery Protocols	UPnP, Bonjour
RAID Levels	RAID0, RAID1, RAID5, RAID6, JBOD
S.M.A.R.T Monitoring	Yes

Cloud Service Features

Table 9: Cloud Service Features

Feature	Description
Backup Files Security	AES-256 Encryption, SHA-1 fingerprints, optional secret passphrase
Protocol Security	SSL (Secure Socket Layers)
Efficiency	Incremental updates, Data Compression, Block Level Deduplication
Versioning	Retention of previous file versions
Additional Services	Centralized Management, Centralized Monitoring, Reporting, Logging, Remote Access, Offline Backup Seeding

Hardware Features

Table 10: Hardware Features

Feature	Description
Internal Hard Drives	4 x 3.5” SATA Hot Swap (not included)
Maximum Storage Capacity	8TB
Ports	4 x USB 2.0 high-speed ports for external drives, 2 x Gigabit Ethernet
Maximum Power Consumption	220W
Compliance	FCC, CE, RoHS, WEEE
Operating Environment	10-40°C, Humidity 10%-85% (non-condensed)
Dimensions	44(H) X 446.4(W) X 500(D) mm / 1.73(H) x 17.6(D) x 19.7(D) inch (1U rack mount)
Weight	7.2Kg (excluding hard drives)

Requirements

Hardware Requirements

In order to install the CTERA appliance, you will need the following:

- At least one hard drive (SATA, 3.5")
- A network connection or router with DHCP enabled

Software Requirements

In order to use the appliance Web interface, you will need the following:

- Either Microsoft Internet Explorer 7.0 or later, Mozilla Firefox 2.0 or later, or Google Chrome 3.0 or later
- Adobe Flash Player

Opening Ports on Your Firewall

In order to back up roaming PCs and remote offices *outside* your network using the CTERA Agent, you must open your firewall for the network where the CTERA appliance is located, to allow incoming TCP ports 995 and 873 to the CTERA appliance.

Installing the CTERA C400

To install the CTERA C400

1. Install at least one hard drive in the appliance.

   See ***Installing a SATA Hard Drive in the CTERA C400*** (on page 21).

2. Connect one end of the Ethernet cable to the LAN0 port, and connect the other end to your Ethernet LAN switch or hub.

3. Connect the provided power supply cable to the AC power input socket, and connect the other end to the wall outlet.

4. Turn the power switch at the back of the appliance to the ON position.

   The appliance will start up, and the Power LED will turn green.

   The appliance automatically obtains an IP address using DHCP.

   Tip

   If a DHCP server is not available, then after one minute, the appliance will use the IP address 192.168.192.5.

   Warning

   If you need to unplug the appliance, you must first shut it down as described in ***Shutting Down the CTERA Appliance*** (on page 333). Failure to do so could result in data loss.

Installing a SATA Hard Drive in the CTERA C400

To install a SATA hard drive

1. If the desired disk tray's Tray Open Button indicates that the disk tray is locked (that is, the groove is horizontal), then unlock the disk tray by using a flat-head screwdriver to turn the groove until it is vertical.

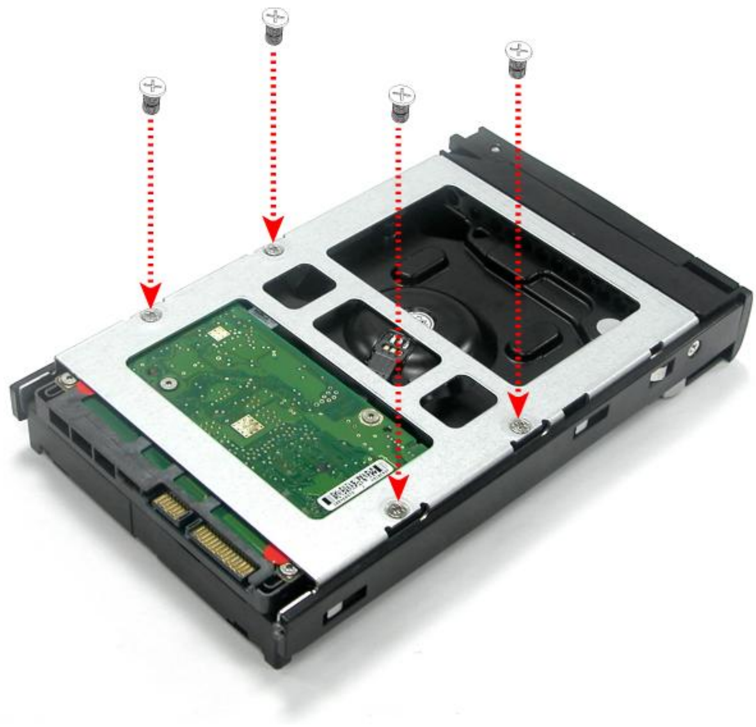
2. Press the disk tray's Tray Open Button.

The disk tray lever pops out.

3 Pull the lever outwards to remove the disk tray from the C400.

4 Place the hard drive in the empty disk tray.

5 Flip over the disk tray, and use the supplied mounting screws to secure the hard drive in the disk tray.



6 Slide the disk tray back into the C400.

7 Press the disk tray lever back into place, until you hear a click.

8 (Optional) If you would like to prevent the disk from being removed, lock the disk tray, by using a flat-head screwdriver to turn the button until the groove is horizontal.

Removing a SATA Hard Drive from the CTERA C400

Tip

If you want to remove a hard drive safely while the appliance is on, use the Safe Removal procedure described in ***Safely Removing Hard Drives*** (on page 84).

To remove a SATA hard drive

1. If the desired disk tray's Tray Open Button indicates that the disk tray is locked (that is, the groove is horizontal), then unlock the disk tray by using a flat-head screwdriver to turn the groove until it is vertical.
2. Press the disk tray's Tray Open Button.

   The disk tray lever pops out.
3. Pull the lever outwards to remove the disk tray from the C400.
4. Flip over the disk tray, and remove the mounting screws from the disk tray.
5. Remove the hard drive from the disk tray.
6. Slide the disk tray back into the C400.
7. Press the disk tray lever back into place, until you hear a click.

Connecting USB Drives

If desired, you can connect a USB drive to the appliance.

To connect a USB drive to the appliance

1. Connect one end of a USB cable into the USB drive.
2. Connect the other end of the USB cable to the appliance's USB port.

4

CTERA C800 Specifications and Installation

This chapter describes the following:

- The CTERA C800 package contents, hardware, and specifications.
- CTERA C800 installation
- Hard drive installation and removal

In This Chapter

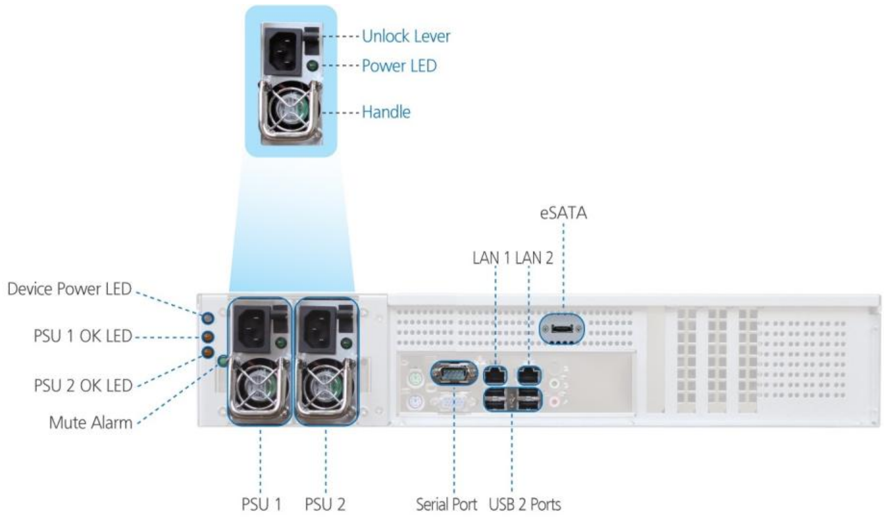
Package Contents

Your appliance package contains the following items:

- CTERA C800
- Two power cords
- Two Ethernet LAN cables
- Two keys for the C800's lockable disk trays

Rear Panel

Network and power connections are made via the appliance's rear panel.



The appliance rear panel contains the following elements:

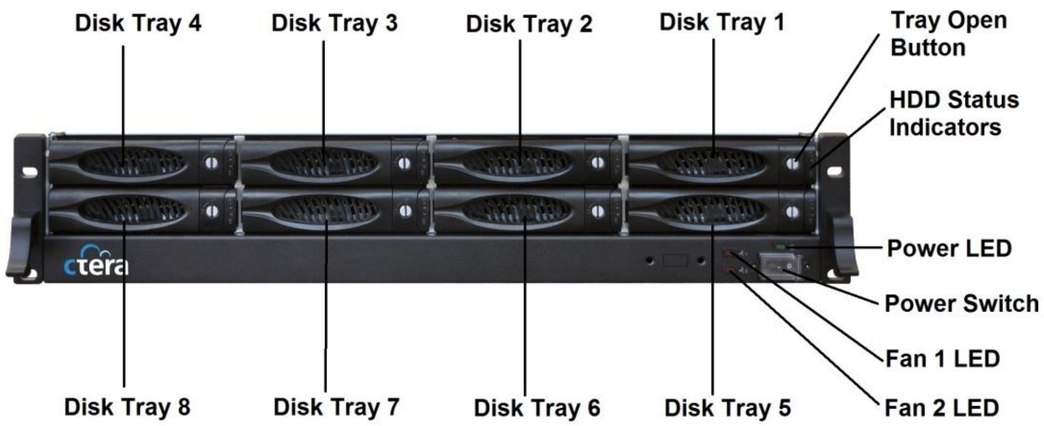
Table 11: C800 Rear Panel Elements

<table>
<tr><th>Element</th><th>Description</th></tr>
<tr><td>Device Power LED</td><td>A LED indicating whether the appliance is operational:
<table>
<tr><th>State</th><th>Explanation</th></tr>
<tr><td>On (Green)</td><td>The appliance is on.</td></tr>
<tr><td>Off</td><td>The appliance is off.</td></tr>
</table></td></tr>
<tr><td>PSU 1 / PSU 2</td><td>The appliance's power supplies.</td></tr>
<tr><td>PSU Power LEDs</td><td>A LED for each power supply, indicating whether it is operational:
<table>
<tr><th>State</th><th>Explanation</th></tr>
<tr><td>On (Green)</td><td>Input power detected.</td></tr>
<tr><td>Off</td><td>No input power.</td></tr>
</table></td></tr>
<tr><td>PSU Unlock Levers</td><td>A lever for each power supply, enabling one to unlock it.</td></tr>
<tr><td>PSU 1 OK LED /
PSU OK 2 LED</td><td>A LED for each power supply, indicating whether it is in use:
<table>
<tr><th>State</th><th>Explanation</th></tr>
<tr><td>On (Yellow)</td><td>The power supply is in use.</td></tr>
<tr><td>Off</td><td>The power supply is not in use.</td></tr>
</table></td></tr>
</table>

PSU Handles	A handle for each power supply, enabling one to remove it.
Mute Alarm	If both power supplies are installed, and one of the power supplies fails or loses power, an alarm signal will sound. Press this button to mute the power supply alarm. See ***Muting the Power Supply Alarm*** (on page 34).
Serial Port	A serial (RS-232) console port used for connecting to the appliance console. The console can be used for advanced troubleshooting and maintenance operations.
USB 2.0 Ports	Four USB 2.0 ports used for connecting USB drives. Note that you can connect more than four USB drives, by connecting a powered USB hub. Be sure to use a powered hub, in order to avoid exceeding the power capacity of the USB ports.
eSATA	An eSATA port used for connecting the appliance to a SATA drive.
LAN 1 / LAN 2	Two Ethernet ports used for connecting the appliance to your Ethernet LAN switch or router. Connect the Ethernet cables provided in the appliance package to these ports. To use both ports in parallel, configure link aggregation, as described in ***Enabling/Disabling Link Aggregation*** (on page 268). For best performance, use a Gigabit-capable Ethernet switch.

Front Panel

The C800's front panel appears as follows:



The front panel's interior contains the following elements:

Table 12: C800 Front Panel Interior Elements

<table>
<tr><th>Element</th><th>Description</th></tr>
<tr><td>Disk Tray 1-8</td><td>Eight disk trays for installing hard drives.</td></tr>
<tr><td>Tray Open Button</td><td>Each disk tray has a Tray Open Button, which serves the following purposes:
Indicates whether the disk tray is locked. When the button's groove is horizontal, the disk tray is locked. When it is vertical, the disk tray is open.
Enables you to lock/unlock the disk tray, by using one of the disk tray keys to turn the button until its groove is horizontal/vertical.
Enables you to open the disk tray. Upon pressing the button, the outer panel of the disk tray (visible in the preceding diagram) becomes a lever that can be used to pull the disk tray out of the appliance.</td></tr>
<tr><td>HDD Status Indicators</td><td>Each disk tray has two LEDs that indicate its status:<table><tr><th>LED</th><th>State</th><th>Explanation</th></tr><tr><td>Upper LED</td><td>Blinking (Blue)</td><td>Disk activity</td></tr><tr><td>Lower LED</td><td>On (Green)</td><td>OK</td></tr><tr><td></td><td>On (Red)</td><td>Disk failure</td></tr><tr><td></td><td>Blinking (Red)</td><td>RAID array failure</td></tr></table></td></tr>
<tr><td>Power LED</td><td>A LED indicating whether the system is operational:<table><tr><th>State</th><th>Explanation</th></tr><tr><td>On (Green)</td><td>The system is operational.</td></tr><tr><td>Off</td><td>The system is not operational.</td></tr></table></td></tr>
<tr><td>Power Switch</td><td>A switch used for turning the appliance on and off and resetting it.
The switch is covered by a clear plastic cover that must be lifted in order to access it.</td></tr>
<tr><td>Fan 1 LED / Fan 2 LED</td><td>A LED for each fan, indicating whether the fan has failed:<table><tr><th>State</th><th>Explanation</th></tr><tr><td>On (Red)</td><td>The fan has failed.</td></tr><tr><td>Off</td><td>The fan is operational.</td></tr></table></td></tr>
</table>

Technical Specifications

Software Features

Table 13: Software Features

Feature	Description
CTERA Agents	50 Workstation Agent licenses included Additional Workstation/Server Agent licenses available
Supported File Systems	EXT3, NEXT3™, FAT32, NTFS, ExFAT
Supported File Sharing Protocols	CIFS (Windows File Sharing), NFS, FTP, WebDAV, RSync, AFP (Apple File Sharing)
Supported Discovery Protocols	UPnP, Bonjour
RAID Levels	RAID0, RAID1, RAID5, RAID6, JBOD
S.M.A.R.T Monitoring	Yes

Cloud Service Features

Table 14: Cloud Service Features

Feature	Description
Backup Files Security	AES-256 Encryption, SHA-1 fingerprints, optional secret passphrase
Protocol Security	SSL (Secure Socket Layers)
Efficiency	Incremental updates, Data Compression, Block Level Deduplication
Versioning	Retention of previous file versions
Additional Services	Centralized Management, Centralized Monitoring, Reporting, Logging, Remote Access, Offline Backup Seeding

Hardware Features

Table 15: Hardware Features

Feature	Description
Internal Hard Drives	8 x 3.5” SATA Hot Swap (not included)
Maximum Storage Capacity	24TB, max 16TB per logical volume
Ports	2 x USB 2.0 high-speed ports for external drives 2 x Gigabit Ethernet
Maximum Power Consumption	256W
Compliance	FCC, CE, RoHS, WEEE
Operating Environment	10~40°C, Humidity 10%-85% (non-condensed)
Dimensions	88(H) X 446.4(W) X 506(D) mm / 3.46(H) x 17.6(D) x 19.9(D) inch (2U rack mount)
Weight	12.5Kg (excluding hard drives)
Power Supplies	2 x 400W, hot-swappable and redundant

Requirements

Hardware Requirements

In order to install the CTERA appliance, you will need the following:

- At least one hard drive (SATA, 3.5")
- A network connection or router with DHCP enabled

Software Requirements

In order to use the appliance Web interface, you will need the following:

- Either Microsoft Internet Explorer 7.0 or later, Mozilla Firefox 2.0 or later, or Google Chrome 3.0 or later
- Adobe Flash Player

Opening Ports on Your Firewall

In order to back up roaming PCs and remote offices *outside* your network using the CTERA Agent, you must open your firewall for the network where the CTERA appliance is located, to allow incoming TCP ports 995 and 873 to the CTERA appliance.

Installing the CTERA C800

To install the CTERA C800

1 Install at least one hard drive in the appliance.

See ***Installing a SATA Hard Drive in the CTERA C800*** (on page 32).

2 Connect one end of an Ethernet cable to a Gigabit Ethernet port, and connect the other end to your Ethernet LAN switch or hub.

3 Connect a provided power supply cable to the AC power input socket of Power Supply 1, and connect the other end to the wall outlet.

4 Connect a provided power supply cable to the AC power input socket of Power Supply 2, and connect the other end to the wall outlet.

Tip

The C800 should normally be used with two power cords . If both power supplies are installed but one is not connected to power, the unit assumes there is a power supply problem, and starts beeping until you dismiss the warning by pressing the Mute Alarm button on the rear panel.

5 Turn the power switch on the front of the appliance to the ON position.

The appliance will start up, and the Power LED will turn green.

The appliance automatically obtains an IP address using DHCP.

Tip

If a DHCP server is not available, then after one minute, the appliance will use the IP address 192.168.192.5.

Warning

If you need to unplug the appliance, you must first shut it down as described in ***Shutting Down the CTERA Appliance*** (on page 333). Failure to do so could result in data loss.

Installing a SATA Hard Drive in the CTERA C800

To install a SATA hard drive

1 If the desired disk tray's Tray Open Button indicates that the disk tray is locked (that is, the groove is horizontal), then unlock the disk tray by using one of the supplied disk tray keys to turn the groove until it is vertical.

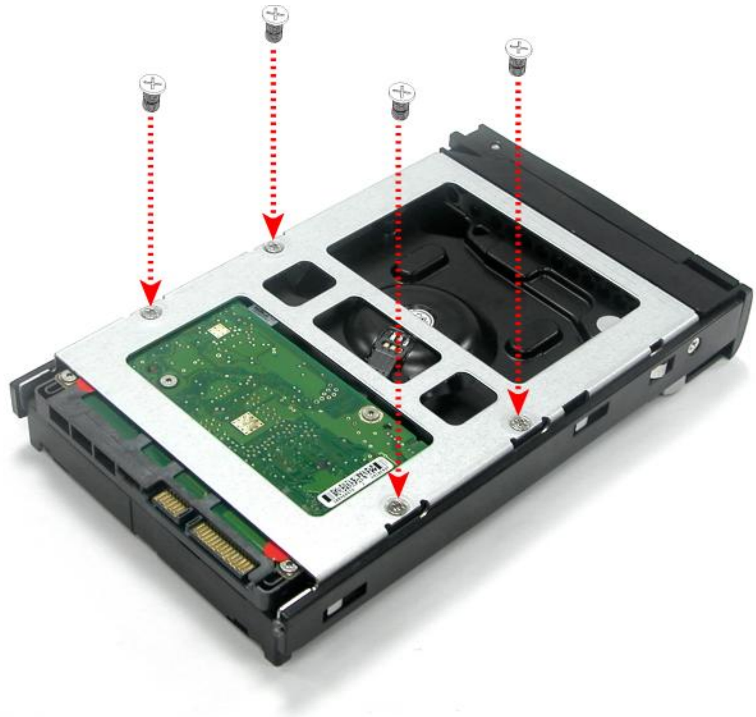
2 Press the disk tray's Tray Open Button.

The disk tray lever pops out.

3 Pull the lever outwards to remove the disk tray from the C800.

4 Place the hard drive in the empty disk tray.

5 Flip over the disk tray, and use the supplied mounting screws to secure the hard drive in the disk tray.



6 Slide the disk tray back into the C800.

7 Press the disk tray lever back into place, until you hear a click.

8 (Optional) If you would like to prevent the disk from being removed, lock the disk tray by using one of the supplied disk tray keys to turn the button until the groove is horizontal.

Removing a SATA Hard Drive from the CTERA C800

Tip

If you want to remove a hard drive safely while the appliance is on, use the Safe Removal procedure described in ***Safely Removing Hard Drives*** (on page 84).

To remove a SATA hard drive

1 If the desired disk tray's Tray Open Button indicates that the disk tray is locked (that is, the groove is horizontal), then unlock the disk tray by using one of the supplied disk tray keys to turn the groove until it is vertical.

2 Press the disk tray's Tray Open Button.

The disk tray lever pops out.

3 Pull the lever outwards to remove the disk tray from the C800.

4 Flip over the disk tray, and remove the mounting screws from the disk tray.

5 Remove the hard drive from the disk tray.

6 Slide the disk tray back into the C800.

7 Press the disk tray lever back into place, until you hear a click.

Connecting USB Drives

If desired, you can connect a USB drive to the appliance.

To connect a USB drive to the appliance

1 Connect one end of a USB cable into the USB drive.

2 Connect the other end of the USB cable to one of the appliance's USB port.

Hot Swapping Power Supplies

You can replace a power supply while the appliance is on.

To hot swap a power supply

1 Remove the power supply as follows: Press the power supply's unlock lever downwards, while simultaneously pulling on the power supply's handle.

2 Install a new power supply as follows: Insert the power supply into the power supply slot, while simultaneously pressing the power supply's unlock lever downwards.

Muting the Power Supply Alarm

The CTERA C800 alerts you when a power supply fails or loses input power, by sounding an alarm. You can mute this alarm.

To mute the power supply alarm

- On the C800's rear panel, press the Mute Alarm button.

  The alarm stops.

5

Getting Started

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

In This Chapter

Connecting to the Web Interface

Windows XP/Vista/7/8

To connect to the appliance Web interface

1 On a computer connected to the same switch as the appliance, view the network neighborhood, by doing one of the following:

- In Microsoft Windows 7® and Microsoft Windows 8®, click **Start > Computer**, then click **Network** in the left pane.

  The appliance is automatically detected using UPnP and appears in the list of network places.

- In Microsoft Windows Vista®, click **Start > Network**.

  The appliance is automatically detected using UPnP and appears in the list of network places.

- In Microsoft Windows XP®, click **Start > My Network Places**.

If your computer is configured to show icons for UPnP devices, the appliance is automatically detected and appears in the list of network places.

Otherwise, do the following:

1 In the **Network Tasks** pane, click **Show icons for networked UPnP devices**.

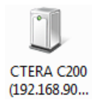
A confirmation message appears.

2 Click **Yes**.

The **Windows Components Wizard** opens and makes the necessary configuration changes.

The appliance now appears in the list of network places.

2 Double-click on the icon named **CTERA appliance**.

In Windows 8, Windows 7 and Vista, the icon is 

; in Windows XP, it is 

.

Tip

After connecting, you can add a bookmark in your Web browser, for easy access to the appliance Web interface.

Mac OS

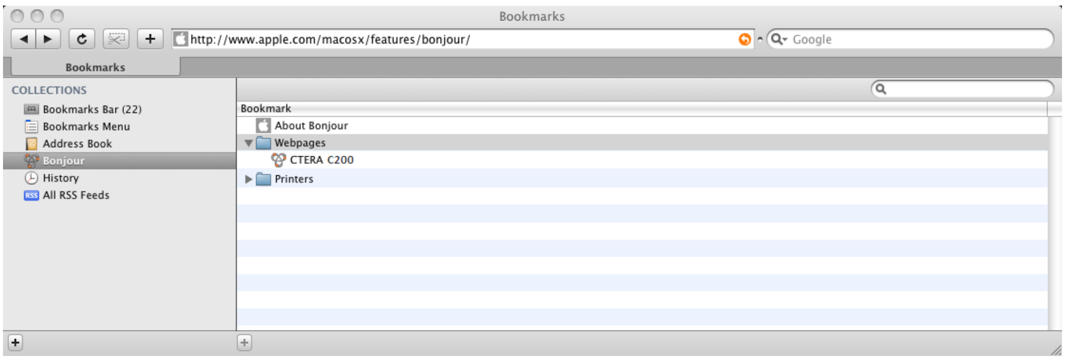
To connect to the appliance Web interface

1 On a computer connected to the same switch as the appliance, run Safari.

2 Open **Bookmarks**.

3 In the **Collections** pane, select **Bonjour**.

4 In the right pane, expand **Webpages**.



5 Double-click on the name of your appliance 

.

Tip

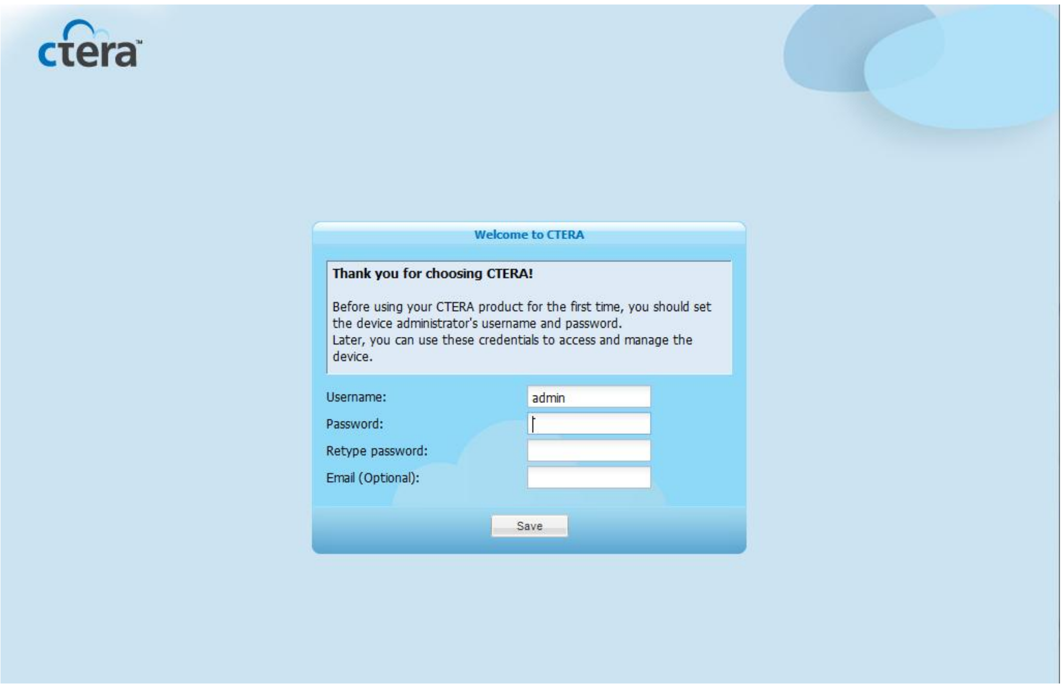
After connecting, you can add a bookmark in your Web browser, for easy access to the appliance Web interface.

Logging in to the Web Interface for the First Time

To log in to the Web interface for the first time

1 Connect to the appliance Web interface as described in ***Connecting to the Web Interface*** (on page 35).

Your Web browser displays the **Welcome to CTERA** page.



In this page, you will choose log in credentials for the appliance administrator, the user you will use to manage the appliance.

2 In the **User Name** field, type a user name for the appliance administrator.

3 In the **Password** field, type a password for the appliance administrator, then retype the same password in the **Retype Password** field for confirmation

The password must be at least 5 characters long.

Tip

Keep these details in a safe place, as you will need them for managing the appliance.

Tip

You can change your user name and password at any time, as described in ***Adding and Editing Users*** (on page 252).

4. In the **Email** field, type the email address of the appliance administrator.
5. Click **Save**.

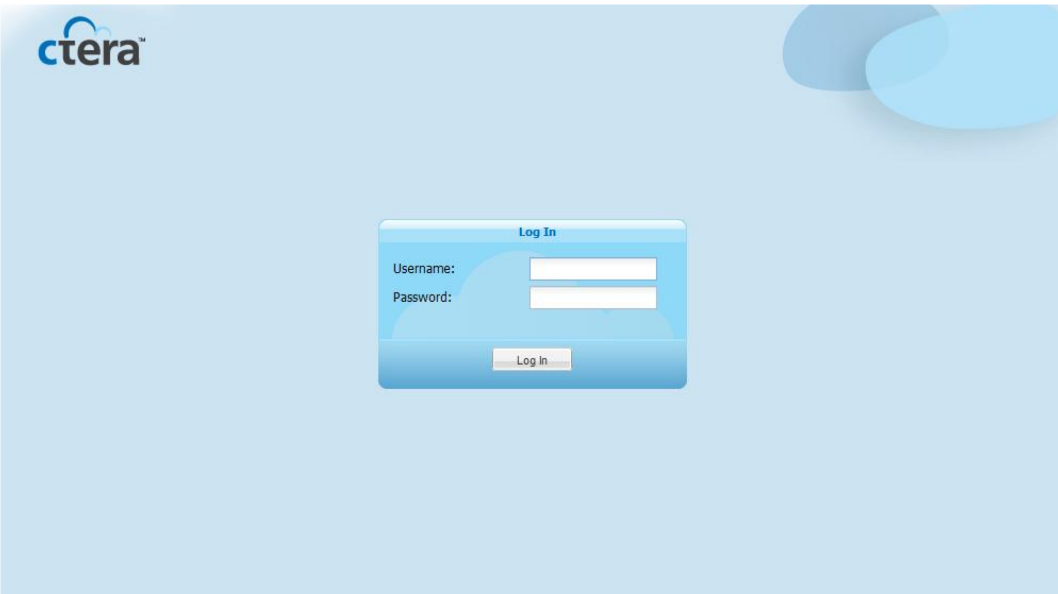
   The **Setup Wizard** opens. Continue at Setting Up the CTERA CloudPlug.

Logging in to the Web Interface

To log in to the Web interface

1. Connect to the appliance Web interface as described in ***Connecting to the Web Interface*** (on page 35).

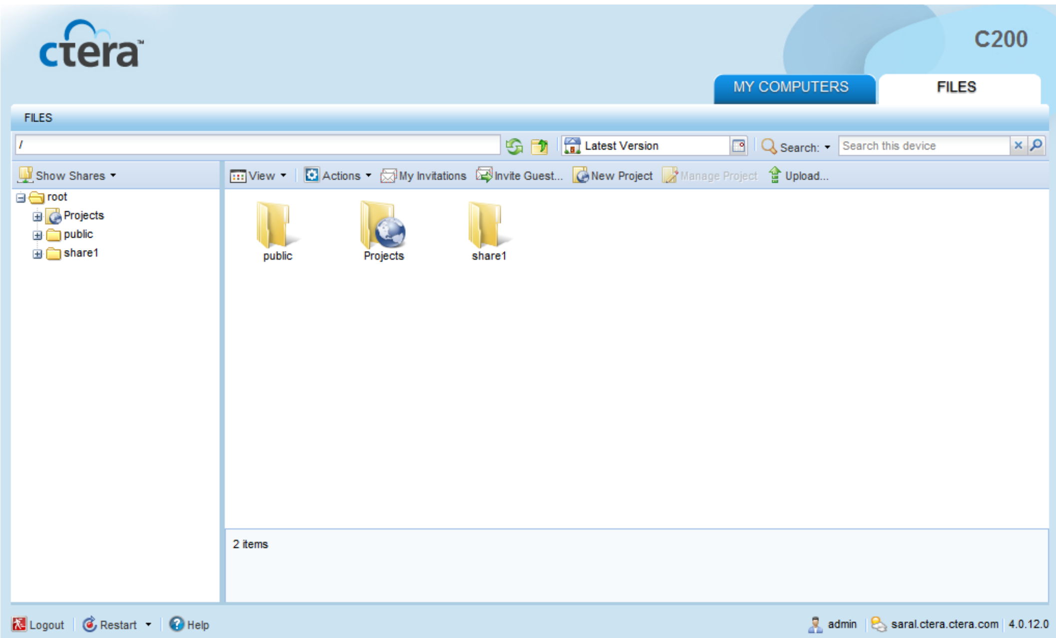
   Your Web browser displays the **Log In** page.



2. In the fields provided, type your user name and password.
3. Click **Log In**.

If you are a member of the Administrators or Read Only Administrators user groups, the **Configuration** tab's **Main > Home** page appears displaying shortcuts to various pages of the appliance Web interface.

Otherwise, the **Files** tab appears displaying the File Manager.



Using the Web Interface

The appliance Web interface consists of the following elements:

- **Tabs**. Used for navigating between the appliance Web interface's tabs: **Configuration**, **Files**, and **My Computers**.

- **Tab content**. The selected tab's content, including information and controls. Content varies between tabs.
- **Status bar**. Displays general and session-specific controls and information.

The Configuration Tab

The **Configuration** tab enables you to manage your appliance settings. It consists of the following elements:

- **Navigation pane**. Used for navigating between pages in the tab.
- **Main frame**. Displays information and controls for the menu section selected in the navigation pane.

Tip

The **Configuration** tab is only visible to users who are members of the Administrators or Read Only Administrators user groups.

Opening Menu Sections

In order to view the contents of a menu section in the navigation pane, you must open it.

To open a menu section

- Do one of the following:
  - Click on the section's name.
  - Next to the section's name, click .

  The section opens, revealing its contents.

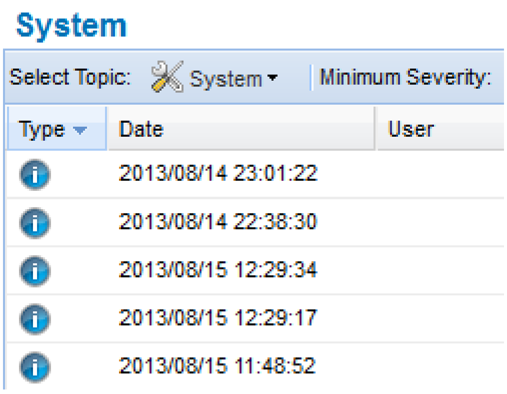
Sorting Tables

You can sort a table according to a specific column, in ascending or descending order.

To sort a table according to a column

1. Click on the desired column's heading.

   The table is sorted according to the column. An arrow in the column's heading indicates that the table is sorted according to the column. The arrow's direction indicates the sort order.

   In this example, the table is sorted according to the **Date** column, in ascending order.

2. To reverse the column's sort order, click on the column's heading again.

   The sort order is reversed.

Navigating Between Table Pages

When a table contains multiple pages, you can navigate between the pages by using the controls at the bottom of the table.

To navigate between pages

- Do any of the following:
  - To navigate to the next page, click .

- To navigate to the previous page, click .
- To navigate to page 1, click .
- To navigate to a specific page, in the **Page** field, type the desired page number.

Refreshing Page and Table Contents

Some of the pages in the main frame contain a button that allows you to refresh the page's contents. Similarly, you can refresh the contents of various tables.

To refresh a page's contents

- In the top-right corner of the main frame, click .

  The page's contents are refreshed.

To refresh a table's contents

At the bottom of the table or list, click .

The table's contents are refreshed.

Accessing the Home Page

The main frame contains a shortcut that enables you to quickly access the **Home** page from any other page in the appliance Web interface's **Configuration** tab.

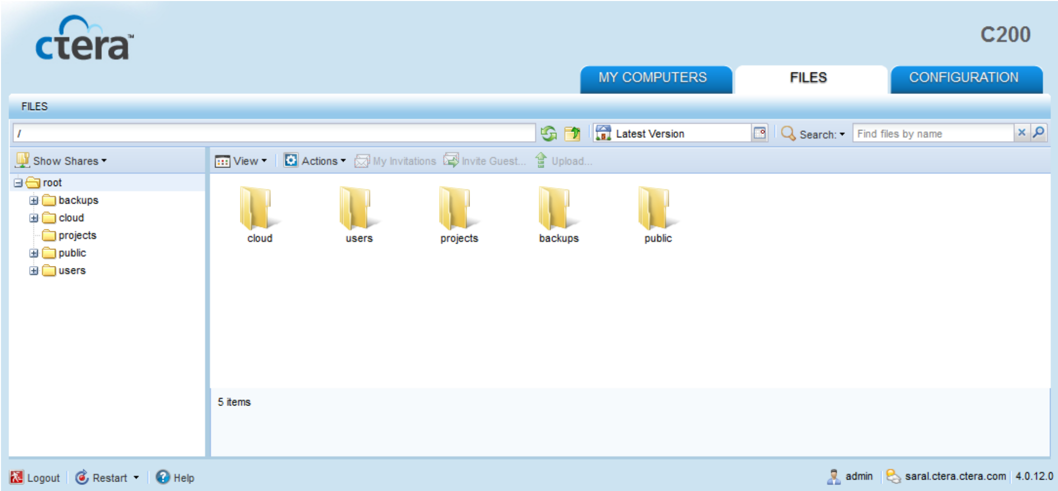
To quickly access the Home page

- In the top-left corner of the main frame, click .

  The **Home** page appears.

The Files Tab

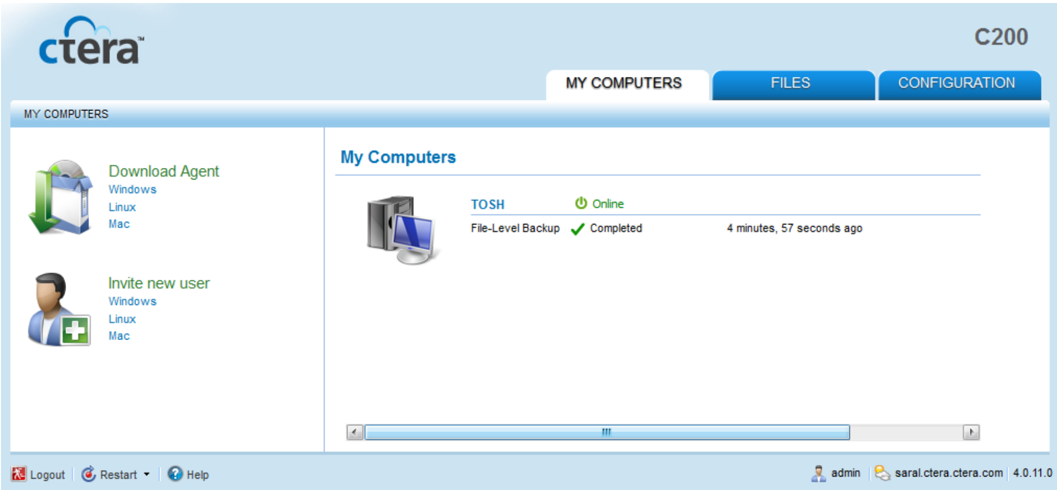
The **Files** tab displays the **File Manager**, which enables you to view and manage the files and folders on the appliance.



For more information on the File Manager, see ***The File Manager*** (on page 277).

The My Computers Tab

The **My Computers** tab allows managing connected CTERA Agents. Users can view their own agents, and administrators can view all defined agents.



The Status Bar

The status bar includes the following elements:

- Controls for logging out of, shutting down, and restarting the appliance
- Controls for accessing online help

- Your user name
- The firmware version

Accessing Online Help

To access online help

- Do one or more of the following:
  - To view the CTERA appliance User Guide, in the status bar, click **Help**.

    This guide opens in a new window or tab.
  - To view tooltips, in the main frame, mouse over the icon.

Setting Up the CTERA Appliance

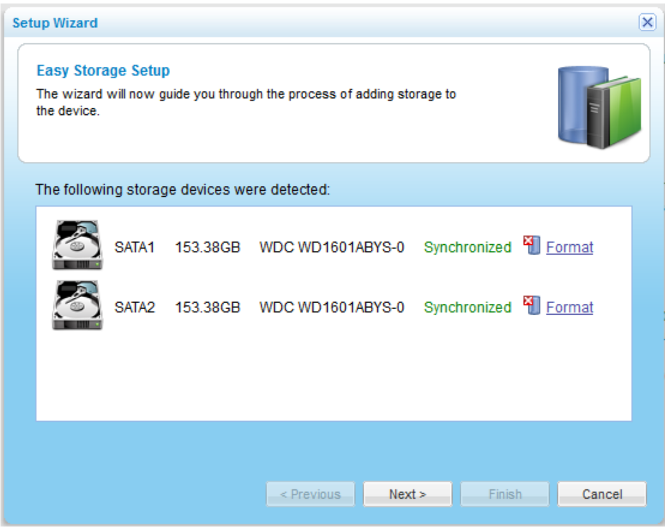
The Web interface includes a Setup Wizard that enables you to quickly configure basic, recommended settings for your appliance. The wizard opens automatically upon initial login; however, if desired, you can close the wizard at any stage, and set up the appliance without the aid of the wizard. You can run the wizard at any time using the following procedure.

To run the Setup Wizard

1. In the **Configuration** tab's navigation pane, click **Main > Home**.

   The **Main > Home** page appears.
2. Click **Setup Wizard**.

   The **Setup Wizard** opens, displaying the **Easy Storage Setup** dialog box.



For each drive, the following information is listed: port number, disk capacity in GB, disk type, and disk model.

If there is already data on a drive, the **Format** option appears next to it.

3 (Optional) To format a drive, do the following:

a Click **Format** next to the drive.

A confirmation message appears.

b Click **Yes**.

The drive is formatted, and all of its contents are erased.

Warning

Formatting erases all data on the drive. If you would like to retain data on a drive, do not format it.

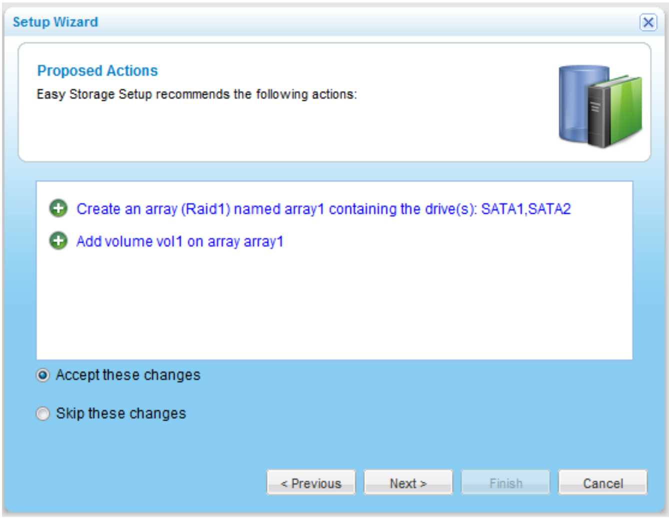
Tip

The appliance supports using hard drives preformatted using the following file systems: FAT32, NTFS, EXT3, NEXT3™. If your hard drive is already formatted using one of these file systems, then you are not required to format it. If you choose to format a drive, it will use the NEXT3 file system.

4 Click **Next**.

The following things happen:

- If the **Setup Wizard** determines that certain storage configuration changes would be beneficial, the **Proposed Actions** dialog box appears describing the changes.



Tip

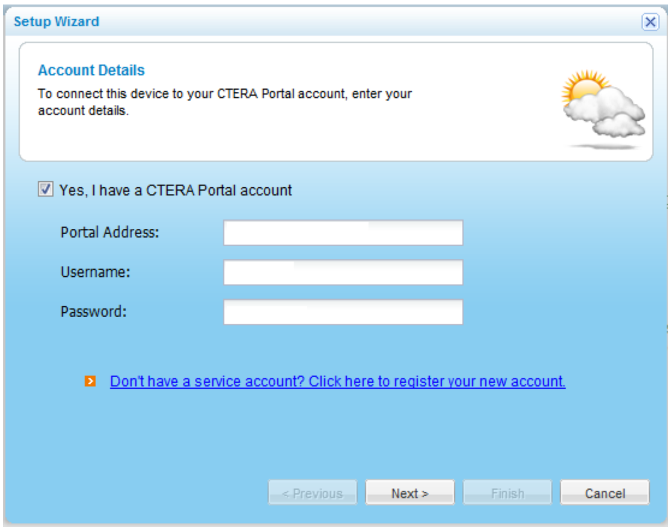
You can configure or modify storage settings later on. See ***Managing Storage*** (on page 63).

Do the following:

1 (Optional) To skip implementing the proposed configuration changes, click **Skip these changes**.

2 Click **Next**.

The **Account Details** dialog box appears.



5 If you have a CTERA Portal account, do the following:

a Select the **Yes, I have a CTERA Portal account** check box.

b In the **Portal Address** field, type the hostname of the CTERA Portal.

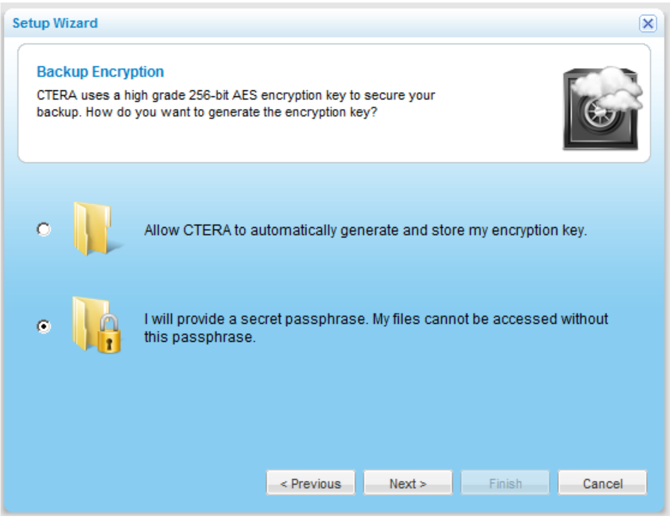
c In the **Username** field, type the user name for your CTERA Portal account.

d In the **Password** field, type the password for your CTERA Portal account.

6 Click **Next**.

Your appliance is added to your CTERA Portal account.

The **Backup Encryption** dialog box appears.

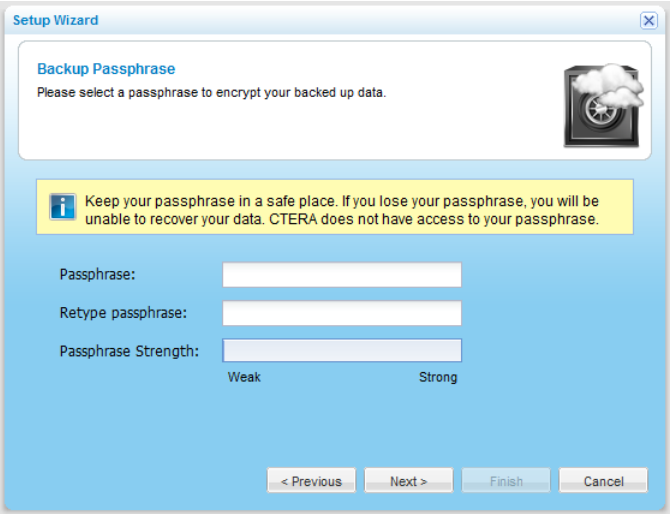


7 Do one of the following:

- To encrypt files using a secure 256-bit encryption key automatically generated by your appliance, before backing up the files online, choose **Allow CTERA to automatically generate and store my encryption key**.
- For increased security, you can optionally secure your files further, with a secret passphrase that is known only to you, by doing the following:

  1. Choose **I will provide a secret passphrase. My files cannot be accessed without this passphrase**.
  2. Click **Next**.

     The **Backup Passphrase** dialog box appears.

  3. In the **Passphrase** and **Retype passphrase** fields, type the passphrase you want to use for accessing your files.

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

Warning

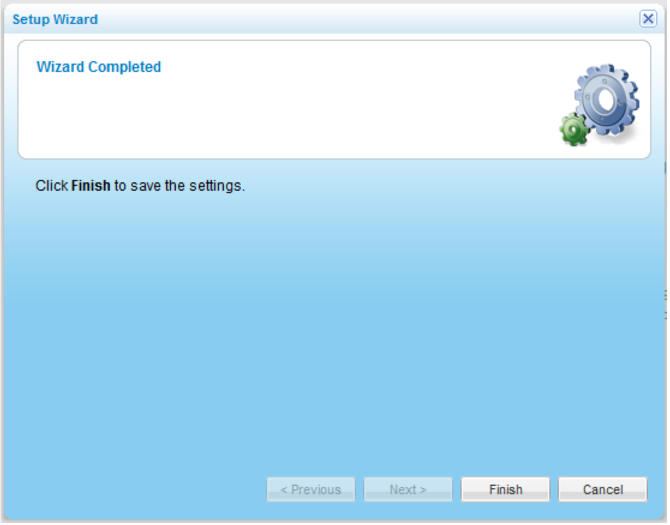
Your passphrase is completely confidential, and CTERA does not retain it online or offline. It is therefore important to keep this passphrase in a safe place, as there is no way of retrieving it if you lose it. Without this passphrase, you cannot access your files.

Tip

You can change your passphrase in the CTERA Portal; however, you need to remember the passphrase in order to do so.

8 Click **Next**.

The **Wizard Completed** screen appears.



9 Click **Finish**.

Logging Out

To log out of the appliance Web interface

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

  You are logged out of the appliance Web interface.

Tip

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

6

Using Cloud Services

This chapter explains how to connect your appliance to cloud services.

In This Chapter

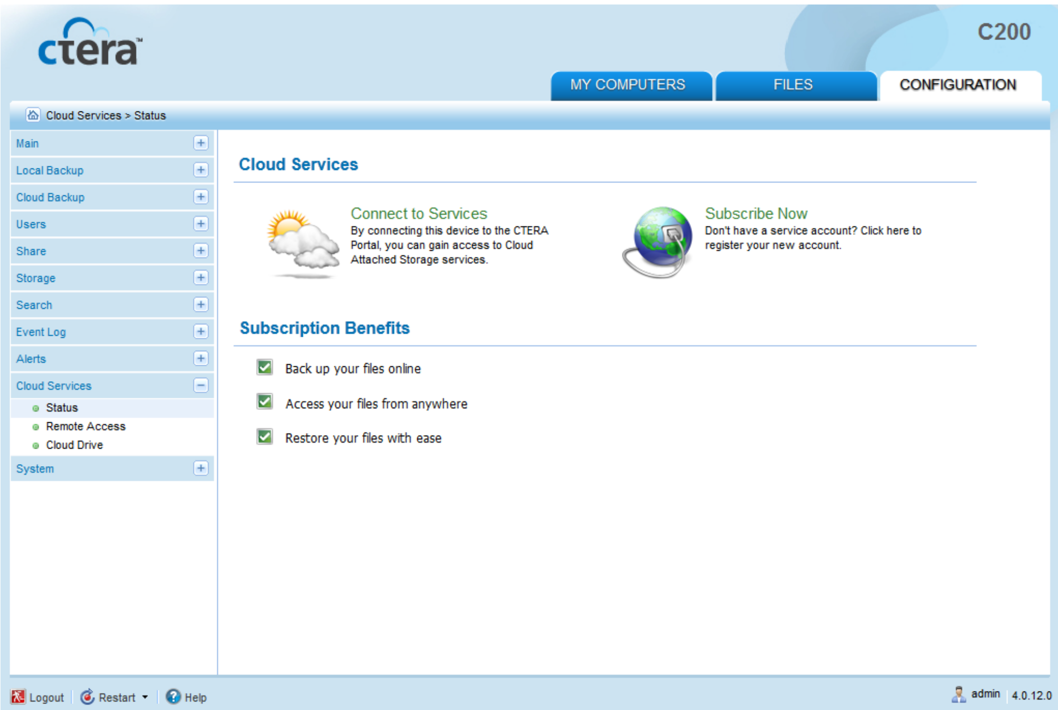
Connecting the Appliance to Your CTERA Portal Account

To enjoy CTERA Cloud Attached Storage services, such as cloud backup, remote monitoring, and reporting, you need to connect the appliance to your CTERA portal account.

To connect the appliance to your CTERA Portal account

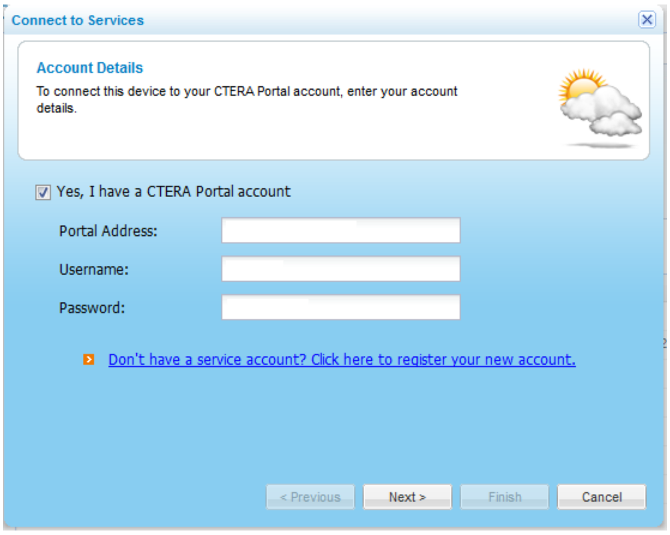
1 In the **Configuration** tab's navigation pane, click **Cloud Services > Status**.

The **Cloud Services > Status** page appears.



2 Click **Connect to Services**.

The **Connect to Services Wizard** opens, displaying the **Account Details** dialog box.



3 Select the **Yes, I have a CTERA Portal account** check box.

4 In the **Portal Address** field, type the hostname of the CTERA Portal.

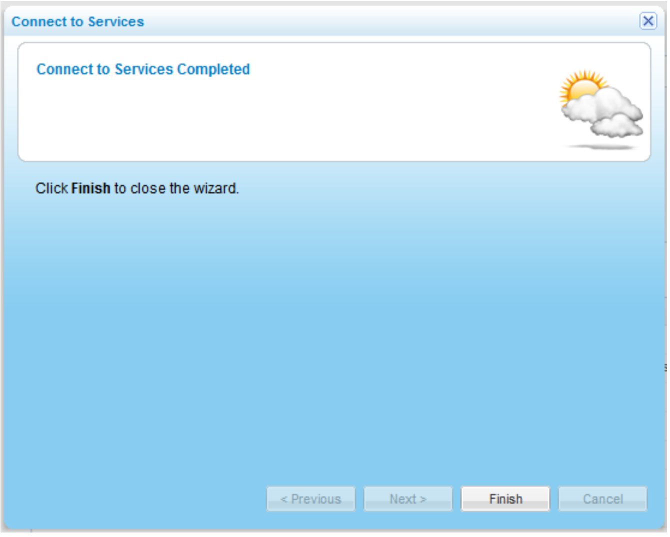
5 In the **Username** field, type the user name for your CTERA Portal account.

6 In the **Password** field, type the password for your CTERA Portal account.

7 Click **Next**.

Your appliance connects to the CTERA Portal and is added to your CTERA Portal account.

The **Connect to Services Completed** screen appears.



8 Click **Finish**.

The **Cloud Services > Status** page displays information about your CTERA Portal account and services.

The **CTERA Portal** area should display "Connected", and the **Subscription Information** area should display "OK" next to the services to which you are subscribed.

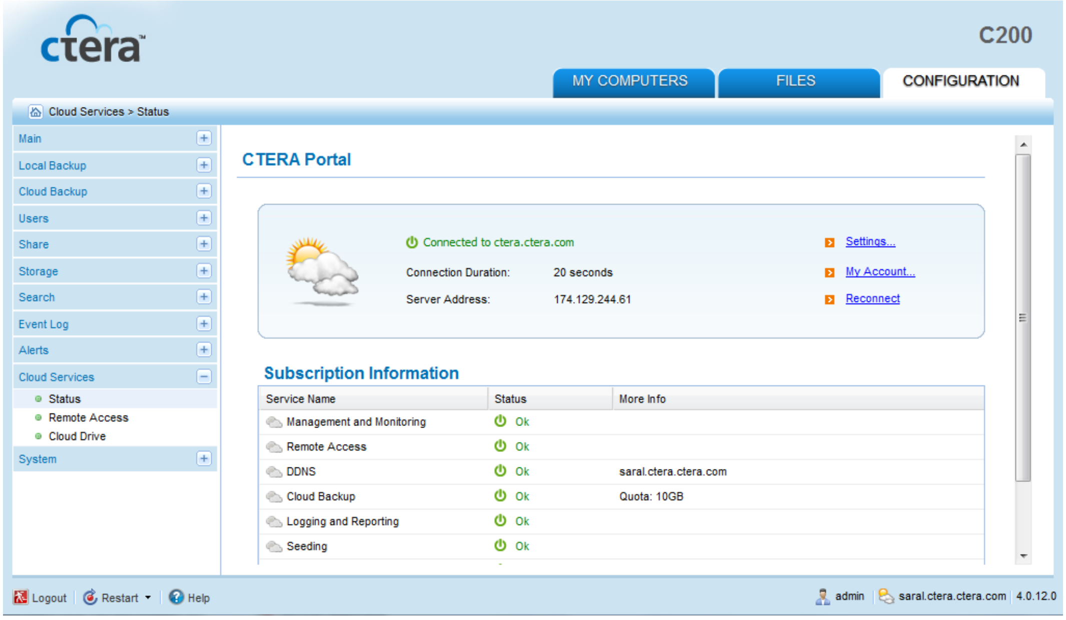
Viewing Service Information

You can view information about your connection to the CTERA Portal and your subscription services.

To view service information

- In the **Configuration** tab's navigation pane, click **Cloud Services > Status**.

The **Cloud Services > Status** page appears.



The following information is displayed:

Table 16: Services Status Information

This field...	Displays...
The connection status	The status of the connection to the CTERA Portal: ▪ **Resolving the portal address**. The appliance is resolving the CTERA Portal address. ▪ **Connected to** *portalName*. The appliance is connected to the CTERA Portal named *portalName*, and the connection is currently in use. ▪ **Connecting**. The appliance is connecting to the CTERA Portal. ▪ **Disconnected**. The appliance is disconnected from the CTERA Portal. You can reconnect as described in ***Reconnecting to Services*** (on page 54) ▪ **Authenticating**. The appliance is authenticating to the CTERA Portal. ▪ **Connection Failed**. The connection to the CTERA Portal failed. You can reconnect as described in ***Reconnecting to Services*** (on page 54).
Connection Duration	The amount of time that the appliance has been connected to the CTERA Portal.
Server Address	The IP address of the CTERA Portal server.
Service Name	The name of each subscription service available from the CTERA Portal.
Status	The status of your subscription to each service: ▪ **OK**. You are connected to the service through the CTERA Portal. ▪ **Disabled**. The service is not currently available. ▪ **Not Subscribed**. You are not subscribed to the service.
More Info	Additional information about the subscription services.

Modifying Your Services Connection Settings

If you need to connect to a different CTERA Portal or enter new login credentials, you can do so using the following procedure.

To modify your connection settings

1. In the **Configuration** tab's navigation pane, click **Cloud Services > Status**.

   The **Cloud Services > Status** page appears.

2. Click **Settings**.

The **Connect to Services Wizard** opens, displaying the **Account Details** dialog box.

3 Modify the fields as needed.

4 Click **Next**.

Your appliance connects to the CTERA Portal using the new settings.

The **Connect to Services Completed** screen appears.

5 Click **Finish**.

Reconnecting to Services

If the connection to the CTERA Portal is lost due to a connectivity failure, the appliance will automatically reconnect when it detects that the CTERA Portal is available. If desired, you can force the appliance to immediately try to reconnect.

To reconnect to services

1 In the **Configuration** tab's navigation pane, click **Cloud Services > Status**.

The **Cloud Services > Status** page appears.

2 Click **Reconnect**.

The appliance reconnects to the CTERA Portal.

Disconnecting from Services

If desired, you can disconnect from managed cloud services.

To disconnect from managed cloud services

1 In the **Configuration** tab's navigation pane, click **Cloud Services > Status**.

The **Cloud Services > Status** page appears.

2 Click **Configure**.

The **Connect to Services Wizard** opens, displaying the **Account Details** dialog box.

3 Clear the **Yes, I have a CTERA Portal account** check box.

4 Click **Next**.

Your appliance disconnects from the CTERA Portal.

The **Connect to Services Completed** screen appears.

5 Click **Finish**.

Accessing Your CTERA Portal Account

To access your CTERA Portal account

1. In the **Configuration** tab's navigation pane, click **Cloud Services > Status**.

   The **Cloud Services > Status** page appears.

2. Click **My Account**.

   The CTERA Portal opens in a new window, and you can log in and access your account.

Using Remote Access

Remote access is a cloud service that enables you to access the files on your appliance from anywhere, as well as to remotely administer your appliance via the Internet.

Your appliance is assigned a unique DNS name, with which you can access it on the Internet.

Tip

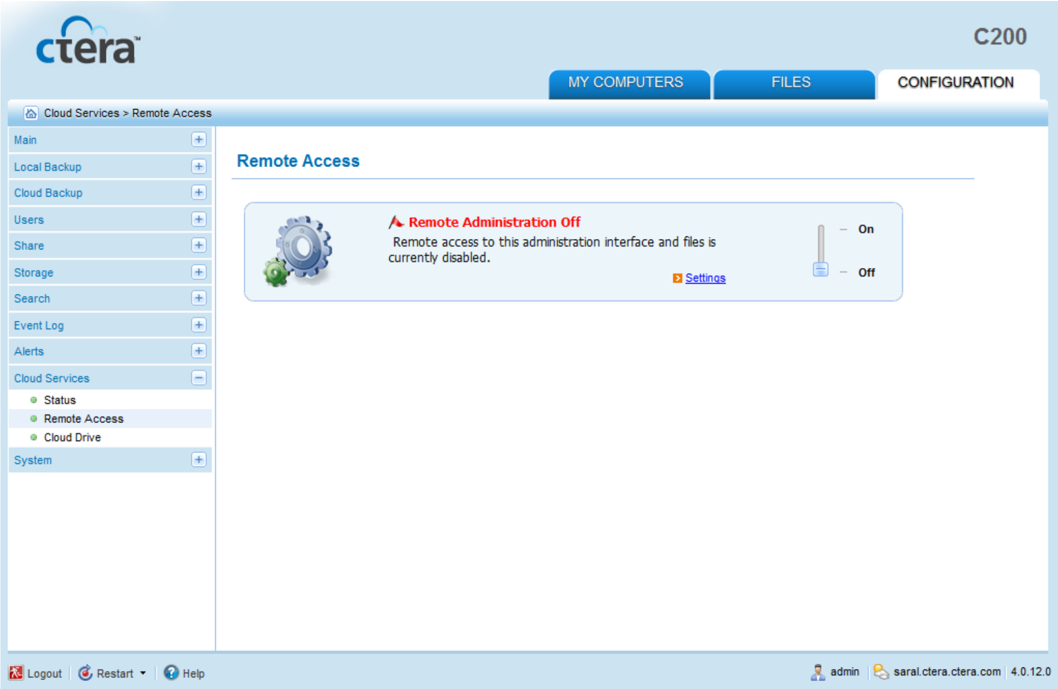
Enabling or disabling remote access controls whether your appliance is accessible *from the Internet*. However, you can always access the appliance from within the local network, regardless of this setting.

Enabling/Disabling Remote Access

To enable remote access

1 In the **Configuration** tab's navigation pane, click **Cloud Backup > Remote Access**.

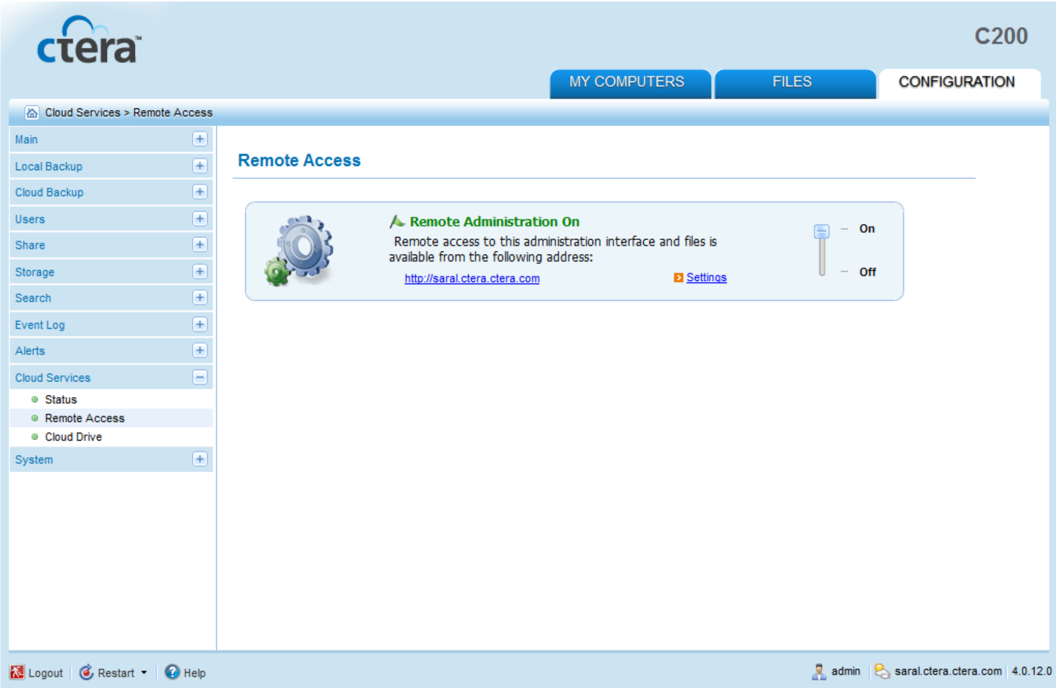
The **Cloud Backup > Remote Access** page appears.



2 Slide the lever to the **On** position.

Remote access is enabled.

A link appears, which you can click on to view a remote management page. You can keep this link in your browser bookmarks, for remote access to this appliance.



To disable remote access

1. In the **Configuration** tab's navigation pane, click **Cloud Backup > Remote Access**.

   The **Cloud Backup > Remote Access** page appears.

2. Slide the lever to the **Off** position.

   Remote access is disabled.

Configuring Remote Access Settings

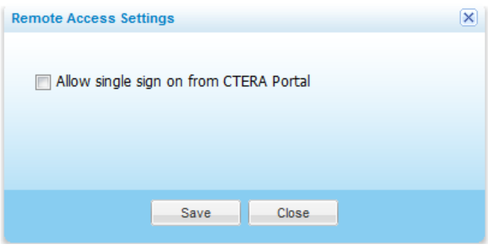
To configure remote access settings

1. In the **Configuration** tab's navigation pane, click **Cloud Backup > Remote Access**.

   The **Cloud Backup > Remote Access** page appears.

2. Click **Settings**.

   The **Remote Access Settings** dialog box opens.



3 To enable remote access to the appliance administration interface from within the CTERA Portal Web interface, without entering the username/password for accessing the appliance, select the **Allow single sign on from CTERA Portal** check box.

4 Click **Save**.

Using Cloud Drive Synchronization

If you are subscribed to the Cloud Drive service on your service provider's CTERA Portal, you can synchronize your portal cloud drive with a specific folder on one or more CTERA appliances, and with CTERA agents in cloud mode.

Synchronization is bi-directional. Conflicts that may occur when a file has been modified on multiple sources are detected and automatically resolved by choosing the most recent version of the file. On a computer or appliance with an older file version, the file is moved to the cloud drive's `.conflicts` folder, called the "conflicts trashcan". Files in the conflicts trashcan are automatically deleted after a configurable time.

Tip

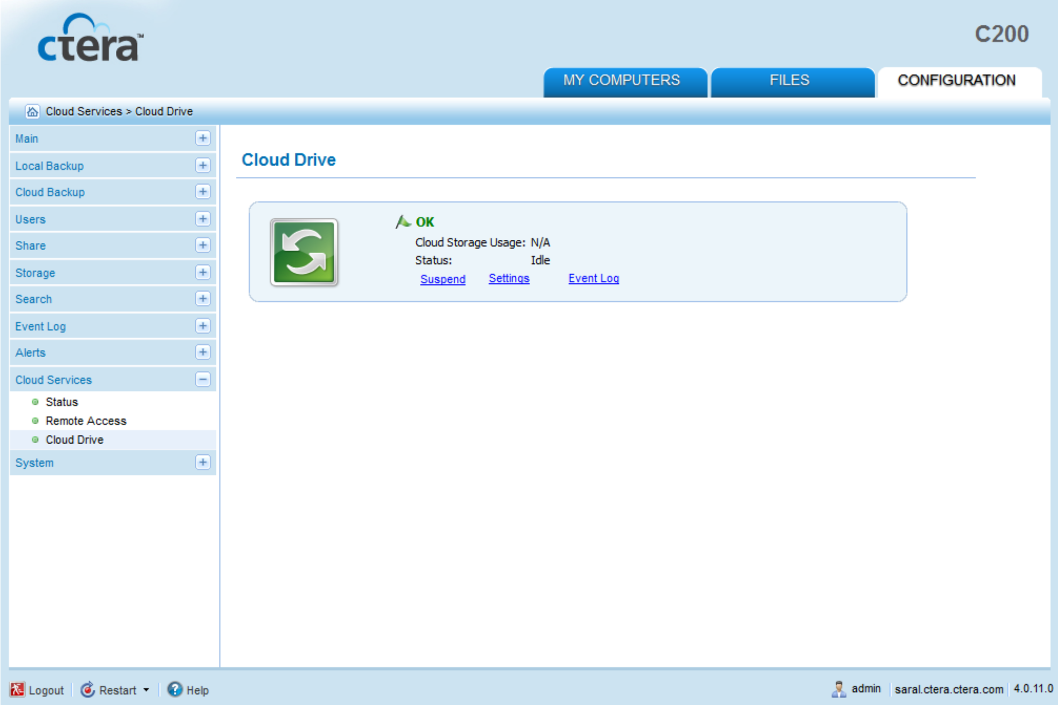
In order for conflict resolution to be performed correctly, the appliance clock must be synchronized with the CTERA Portal clock. If there is more than one hour difference between the two clocks (after taking into account timezone differences), the appliance will show an error message, and will not synchronize the cloud drive folder. It is recommended to use an NTP server to keep the appliance clock accurate. This is the default configuration. For additional information see ***Configuring the CTERA Appliance Time and Date*** (on page 322).

Suspending/Unsuspending Cloud Drive Synchronization

To suspend cloud drive synchronization

1 In the **Configuration** tab's navigation pane, click **Cloud Backup > Cloud Drive**.

The **Cloud Backup > Cloud Drive** page appears.



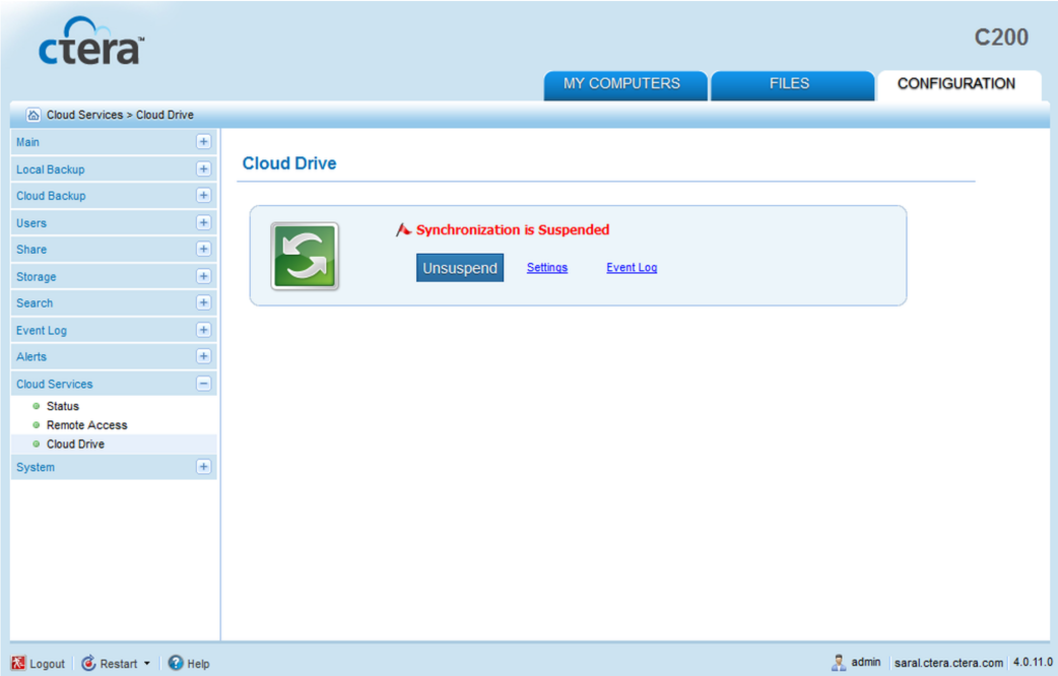
2 Click **Suspend**.

Cloud drive synchronization is suspended.

To unsuspend cloud drive synchronization

1 In the **Configuration** tab's navigation pane, click **Cloud Backup > Cloud Drive**.

The **Cloud Backup > Cloud Drive** page appears.



2 Click **Unsuspend**.

Cloud drive synchronization is no longer suspended, and you can now configure the desired settings.

Selecting Cloud Folders for Synchronization

You can specify which of the portal cloud folders should be synchronized with the appliance.

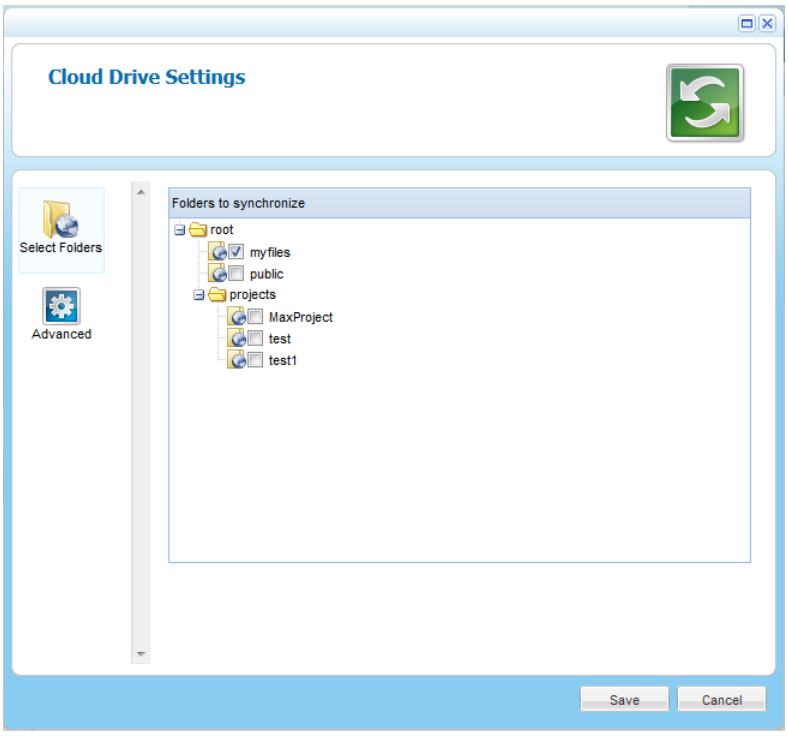
To select portal cloud folders for synchronization

1 In the **Configuration** tab's navigation pane, click **Cloud Services > Cloud Drive**.

The **Cloud Services > Cloud Drive** page appears.

2 Click **Settings**.

The **Cloud Drive Settings** window opens displaying the **Select Folders** tab.



3 Expand the tree nodes and select the check box next to the portal cloud folder you want to synchronize with the appliance.

4 Click **Save**.

Configuring Advanced Cloud Drive Synchronization Settings

You can specify which local folder should be synchronized with the cloud drive, as well as how conflicts between file versions should be handled.

To configure advanced cloud drive synchronization settings

1 In the **Configuration** tab's navigation pane, click **Cloud Services > Cloud Drive**.

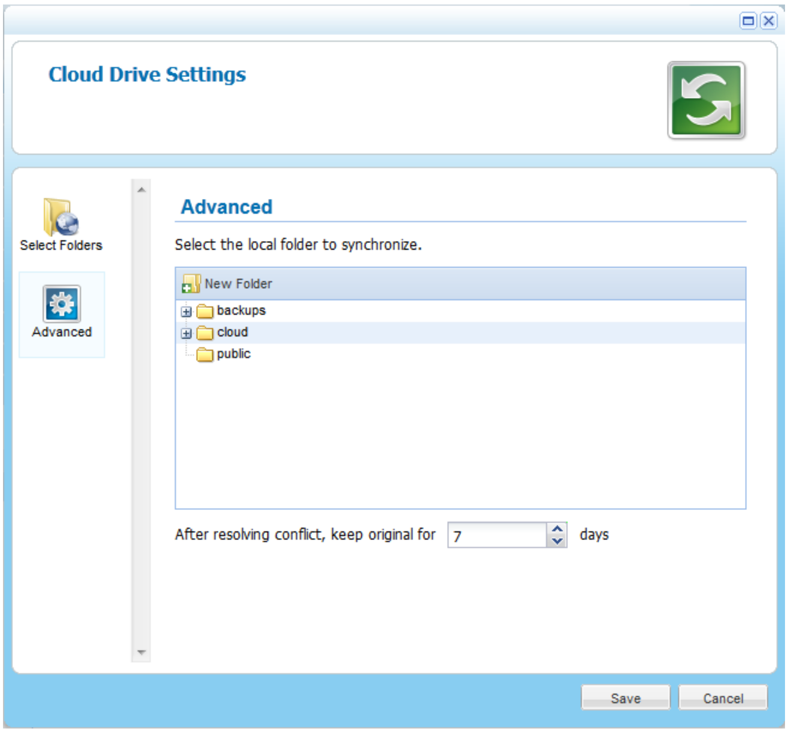
The **Cloud Services > Cloud Drive** page appears.

2 Click **Settings**.

The **Cloud Drive Settings** window opens displaying the **Select Folders** tab.

3 Click the **Advanced** tab.

The **Advanced** tab appears.



4 Expand the tree nodes and select the local folder under which folders should be created for each portal cloud folder you chose for synchronization.

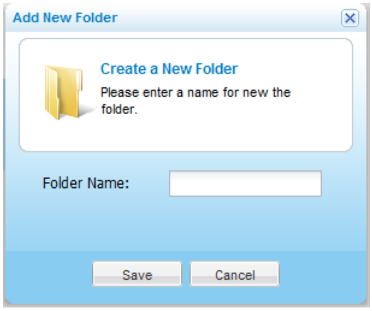
For information on choosing portal cloud folders for synchronization, see ***Selecting Cloud Folders for Synchronization*** (on page 60).

5 (Optional) To create a new folder, do the following:

a In the tree, select the parent folder in which you want to create the new folder.

b Click **New Folder**.

The **Create a New Folder** dialog box opens.



c. In the **Folder Name** field, type a name for the folder.

d. Click **Save**.

   A new folder is added to the selected parent folder.

6. In the **After resolving conflict, keep original for** field, use the arrow buttons to specify the number of days that the appliance should retain the original version of a file that was independently modified on more than one replica.

   After this time, the conflicting copies are deleted. Conflicting copies are stored in the conflicts trashcan folder, `.conflicts`.

7. Click **Save**.

Viewing Cloud Drive Synchronization Status

You can view information on cloud drive synchronization status and the amount of cloud storage used.

To view cloud drive synchronization status

- In the **Configuration** tab's navigation pane, click **Cloud Backup > Cloud Drive**.

  The **Cloud Backup > Cloud Drive** page appears.

  The following information is displayed:

Table 17: Cloud Drive Synchronization Information

This field...	Displays...
Cloud Storage Usage	The amount of used space in your account, followed by the number of files on the cloud drive.
Status	The cloud drive synchronization status. Some possible statuses are: - **Sync in progress**. Synchronization is currently in progress. - **Path is not configured**. The path to the local folder which should be synchronized with the cloud drive is not configured. To configure it, see ***Configuring Advanced Cloud Drive Synchronization Settings*** (on page 60).

7

Managing Storage

This chapter explains how to manage arrays and volumes.

In This Chapter

Overview

On the appliance, storage is divided into *arrays*, each of which consists of one or more physical hard drives. When defining an array you can choose from the following array types. Each provides a different method of data distribution, resulting in various degrees of storage reliability and array capacity.

Table 18: Array Types

Array Type	Description
Linear Concatenation (JBOD)	In JBOD ("Just a Bunch Of Disks"), disks are simply concatenated, so that they act as one large virtual disk. For example, if you have one 500 GB disk and one 250 GB disk in such an array would act as a 750 GB disk. JBOD provides no data redundancy. If any of the drives in the array fails, the array becomes unreadable. The advantage of JBOD is that you can mix disks of different sizes, without losing capacity.
RAID0 (Striped)	In RAID0, data is distributed across multiple disks, in a method called striping. Data is written in small, set amounts to each disk in turn, thus increasing speed with no loss of capacity. Like JBOD, RAID0 provides no redundancy. If one disk fails, the partial data on the other disks will become useless. The size of the array is be the size of the smallest disk in the array, times the amount of drives in the array. RAID0 requires a minimum of two hard drives.
RAID1 (Mirrored)	In RAID1, data is duplicated across all disks in the array, so that there is full redundancy. If a disk fails, the array's performance will be reduced (the array will be marked as "Degraded"), but data will not be lost, so long as there is at least one good disk. Data will only be lost if all the disks in the array fail. Since the exact same data must be written on each disk in the array, the array's capacity is limited to that of the smallest disk. RAID1 requires a minimum of two hard drives.
RAID5 (Striping with distributed parity)	RAID5 requires three or more disks, and combines striping with distributed parity to protect against data loss. If a disk fails, the array's performance will be reduced (the array will be marked as "Degraded"), but data will not be lost. If two disks fail, data will be lost. The array capacity is: `(n-1)*s` Where `n` = number of drives, and `s` = size of smallest disk. RAID5 requires a minimum of three hard drives.

RAID6 (Striping with dual distributed parity)	RAID6 is similar to RAID5; however, it uses dual parity to enable the array to survive two disk failures, without data loss. Array capacity is: `(n-2)*s` Where `n` = number of drives, and `s` = size of smallest disk. RAID6 requires a minimum of four hard drives.

Tip

You can also define a *standalone drive*, which is a single drive with one volume defined on it. To create a standalone drive, format the drive using the Storage Setup Wizard (see ***Setting Up Storage Using the Storage Setup Wizard*** (on page 66)). Then create a volume, and in the **Specify Volume Details** dialog box's **Storage Device** field, select the drive (see ***Adding and Editing Logical Volumes*** (on page 73)).

Tip

RAID1, 5, and 6 support hot swapping, in which drives are replaced without turning off the appliance. The array remains accessible throughout the hot swap procedure. For further information, see ***Hot Swapping a Disk in a RAID1, 5, or 6 Array*** (on page 86).

Each array is divided into *volumes*, which are logical partitions on the array.

The appliance supports the following types of volumes:

- **Network Attached Storage (NAS)**

  A NAS volume is a volume that is formatted with a file system. The appliance acts as a files server for NAS volumes, and the files on such volumes can be accessed using any of the appliance-supported file sharing protocols.

  The appliance enables you to take snapshots of NAS volumes. For more information, see ***Working with Snapshots*** (see "***Working with Volume Snapshots***" on page 87).

- **Storage Area Network (SAN)**

  A SAN volume (also called "Raw") is an unformatted volume. The appliance cannot read files on SAN volumes, and therefore file sharing, synchronization, and cloud backup cannot be used with such volumes. In order to access a SAN volume, an iSCSI target should be defined for this volume. The SAN volume will then appear as if it were a physical disk on your PC or server and can be formatted remotely.

Workflow

In order to manage storage for your appliance, you must do one of the following:

- Use the Storage Setup Wizard to set up storage in a few easy steps.

  See ***Setting Up Storage Using the Storage Setup Wizard*** (on page 66).

- Manually set up storage, by doing the following:
  a. Add one or more arrays.

     See ***Adding and Editing Arrays*** (on page 68).
  b. Create one or more volumes on each array.

     See ***Adding and Editing Logical Volumes*** (on page 73).
  c. If you created a SAN volume, you must add it as an iSCSI target, in order to access it.

     See ***Adding and Editing iSCSI Targets*** (on page 81).

Setting Up Storage Using the Storage Setup Wizard

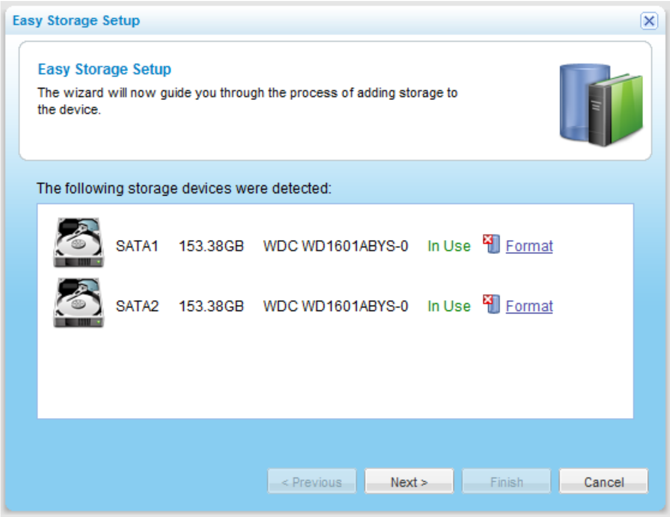
The Storage Setup Wizard enables you to quickly configure basic, recommended storage settings for your appliance.

To set up storage using the Storage Setup Wizard

1. In the **Configuration** tab's navigation pane, click **Storage > Arrays** or **Storage > Volumes**.

   The relevant page appears.
2. Click **Storage Setup Wizard**.

   The **Easy Storage Setup Wizard** opens, displaying the **Easy Storage Setup** dialog box.



   For each installed drive, the following information is listed: port number, disk capacity in GB, disk type, and disk model.

   If there is already data on a drive, the **Format** option appears next to it. If there is no data on the drive, the drive's status will be “Empty”, and the drive will be formatted automatically.
3. (Optional) To format a drive, do the following:

a Click **Format** next to the drive.

A confirmation message appears.

b Click **Yes**.

The drive is formatted, and all of its contents are erased.

Warning

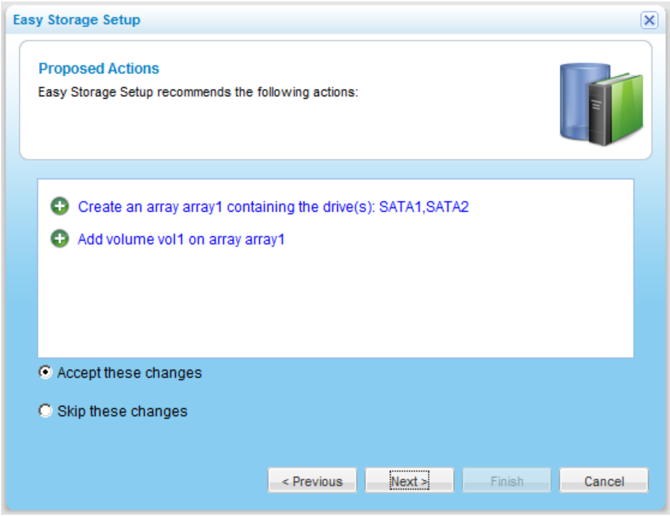
Formatting erases all data on the drive. If you would like to retain data on a drive, do not format it.

Tip

The appliance supports using hard drives preformatted using the following file systems: FAT32, NTFS, EXT3, NEXT3™. If your hard drive is already formatted using one of these file systems, then you are not required to format it. If you choose to format a drive, it will use the NEXT3 file system.

4 Click **Next**.

- If the **Storage Setup Wizard** determines that certain storage configuration changes involving this drive would be beneficial, the **Proposed Actions** dialog box appears describing the changes.

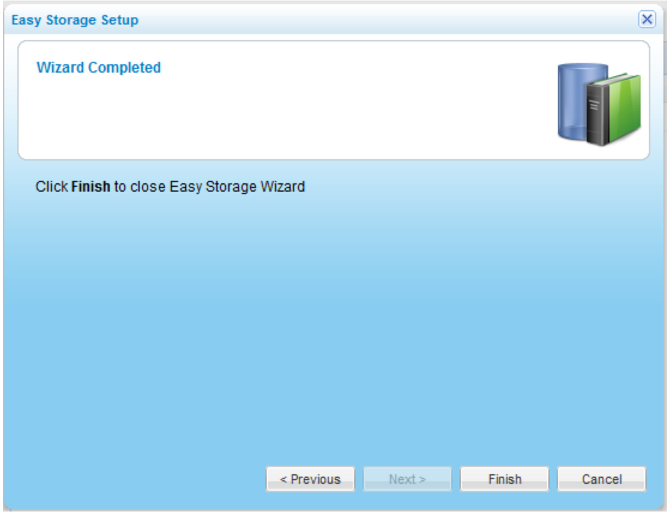


Do the following:

1 (Optional) To skip implementing the proposed configuration changes, click **Skip these changes**.

2 Click **Next**.

The **Wizard Completed** screen appears.



5 Click **Finish**.

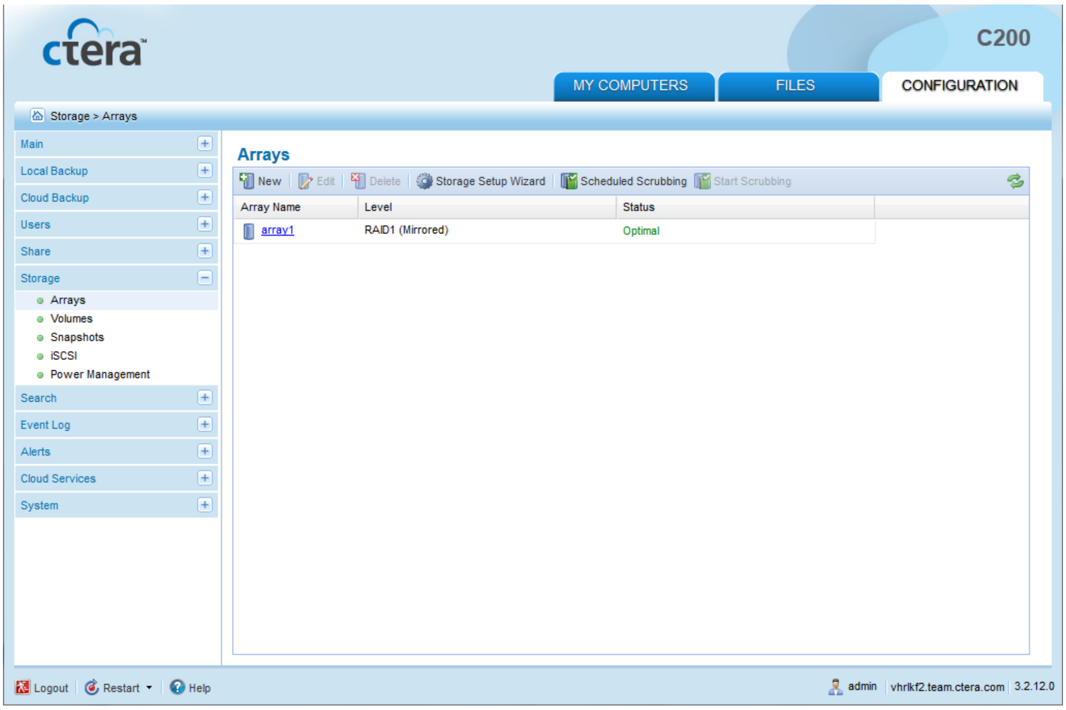
Manually Setting Up Storage

Adding and Editing Arrays

To add or edit an array

1 In the **Configuration** tab's navigation pane, click **Storage > Arrays**.

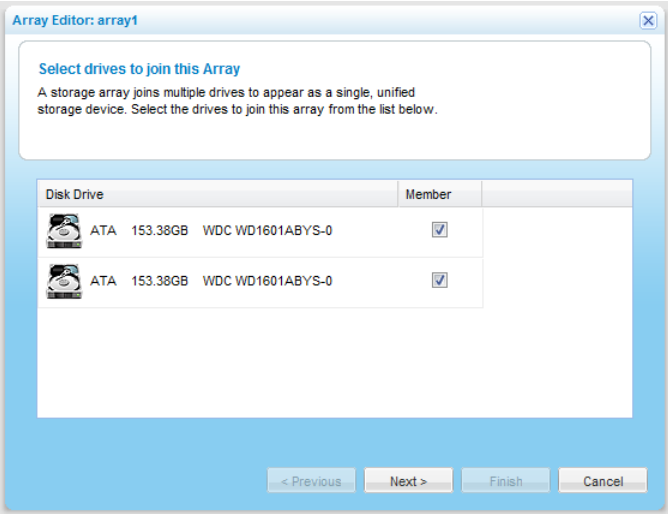
The **Storage > Arrays** page appears.



2 Do one of the following:

- To add a new array, click **New**.
- To edit an existing array, click on its name.

The **Array Editor Wizard** opens, displaying the **Select drives to join this Array** dialog box.



The available drives are listed, along with disk type, disk capacity in GB, and disk model.

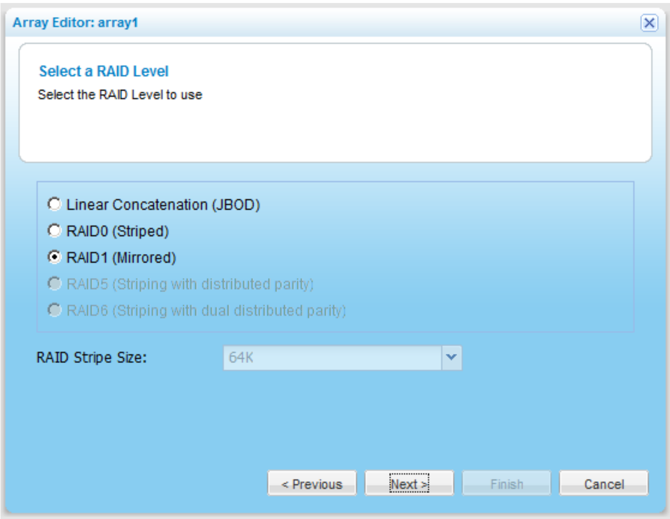
3 Select the check boxes next to the drives you want to include in the array.

Tip

It is not recommended to create an array using USB drives. An array cannot contain both SATA and USB drives.

4 Click **Next**.

The **Select a RAID Level** dialog box appears.



5 Choose the desired array type.

For information about the available types, see ***Array Types*** (page 64).

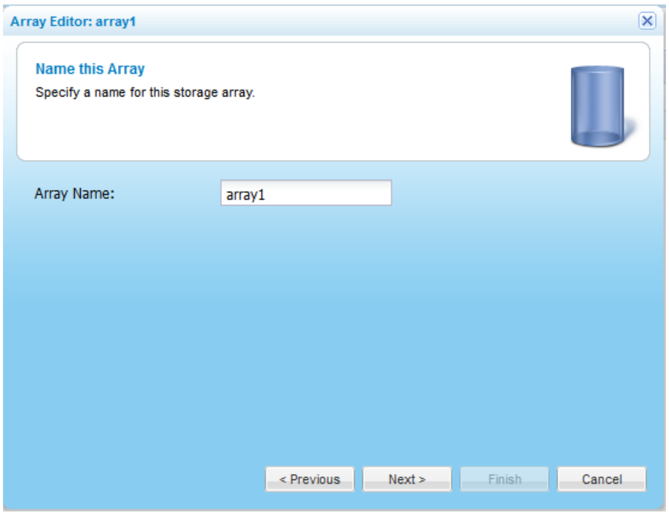
6 If you chose RAID0, RAID5, or RAID6, in the **RAID Stripe Size** field, select the desired stripe size in kilobytes.

The stripe size is the amount of data written to each drive in turn. Reading and writing large data files sequentially generally benefits from a large stripe size. Small random reads and writes generally benefit from a smaller stripe size.

The default value is 64 K.

7 Click **Next**.

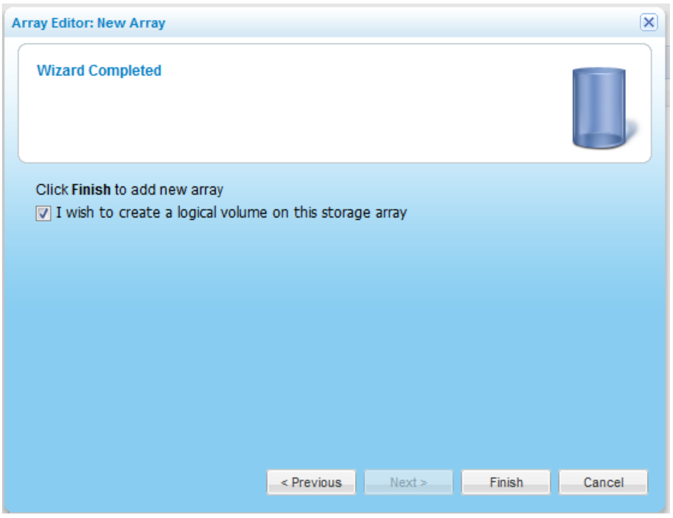
The **Name this Array** dialog box appears.



8 In the **Array Name** field, type a name for the array.

9 Click **Next**.

The **Wizard Completed** screen appears.



10 To immediately create a volume on the array, select the **I wish to create a logical volume on this storage array** check box.

11 Click **Finish**.

Deleting Arrays

Warning

Deleting an array will result in the loss of all existing data on the array.

To delete an array

1 In the **Configuration** tab's navigation pane, click **Storage > Arrays**.

The **Storage > Arrays** page appears.

2 Select the desired array and click **Delete**.

A confirmation message appears.

3 Click **Yes**.

The array is deleted.

Scheduling Automatic Data Scrubbing

You can configure the appliance to perform RAID data scrubbing on a regular basis. During data scrubbing, the appliance reads all the disks in a RAID array and checks for defective blocks, thus reducing the likelihood of silent data corruption and data loss due to bit errors.

By default, automatic scrubbing is performed on a weekly basis for all defined RAID arrays. It can also be run manually for specific arrays, as described in ***Manually Starting Data Scrubbing*** (on page 73).

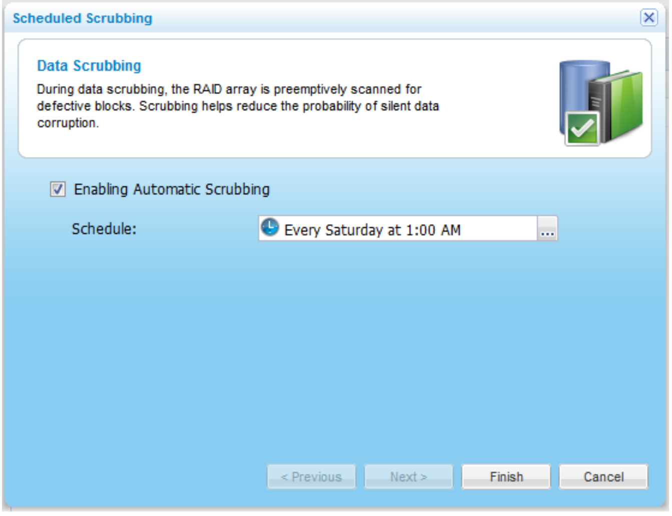
To schedule automatic data scrubbing for all RAID arrays

1 In the **Configuration** tab's navigation pane, click **Storage > Arrays**.

The **Storage > Arrays** page appears.

2 Click **Scheduled Scrubbing**.

The **Data Scrubbing** dialog box appears.



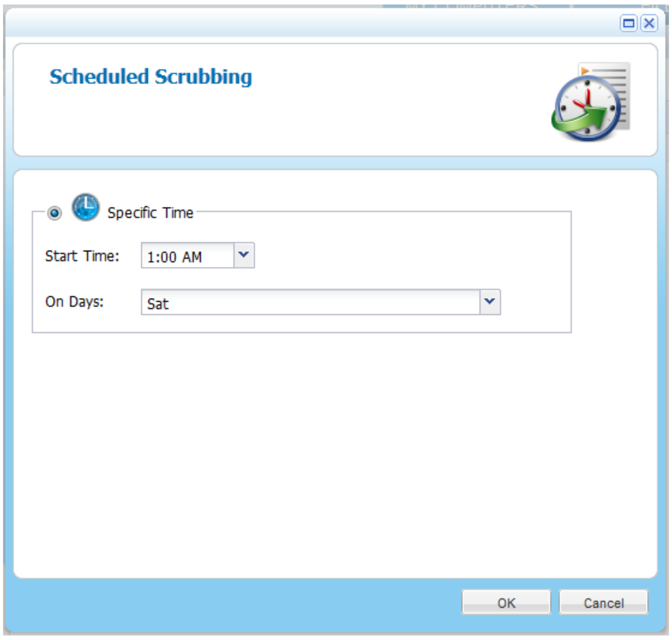
3 Do one of the following:

- To disable automatic data scrubbing, clear the **Enabling Automatic Scrubbing** check box.
- To enable automatic data scrubbing, select the **Enabling Automatic Scrubbing** check box.

4 If you enabled scheduled snapshots, do the following:

a In the **Schedule** field, click ....

The **Scheduled Scrubbing** dialog box appears.



b In the **Start Time** drop-down list, select the hour at which data scrubbing should start.

c In the **On Days** drop-down list, select the days on which data scrubbing should be performed. This can be any of the following:

- One or more specific days
- **Every Day**. Data scrubbing will occur every day.

d Click **OK**.

5 Click **Finish**.

Manually Starting Data Scrubbing

You can manually start data scrubbing for an array at any time.

To manually start data scrubbing for an array

1 In the **Configuration** tab's navigation pane, click **Storage > Arrays**.

The **Storage > Arrays** page appears.

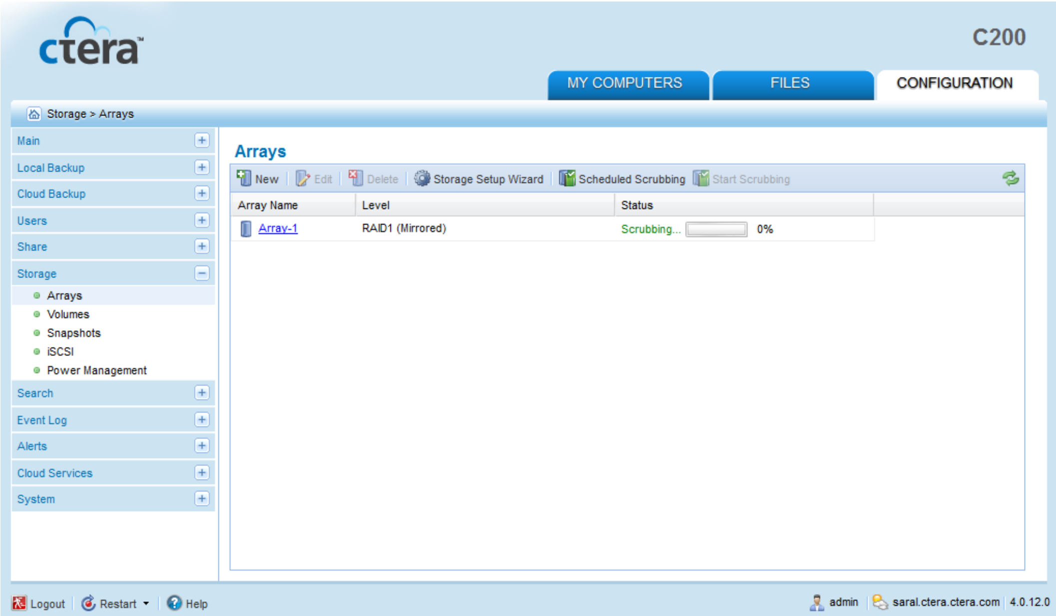
2 Click on the desired array's row.

3 Click **Start Scrubbing**.

Scrubbing starts, and a success message appears.

4 Click **OK**.

A progress bar tracks the scrubbing's progress.

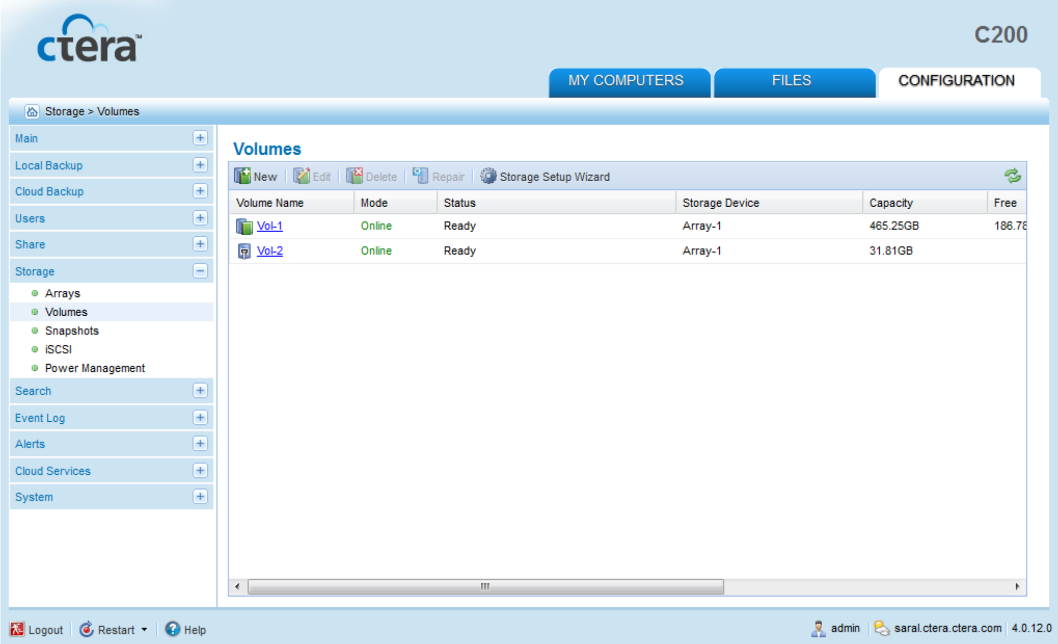


Adding and Editing Logical Volumes

To add or edit a logical volume

1 In the **Configuration** tab's navigation pane, click **Storage > Volumes**.

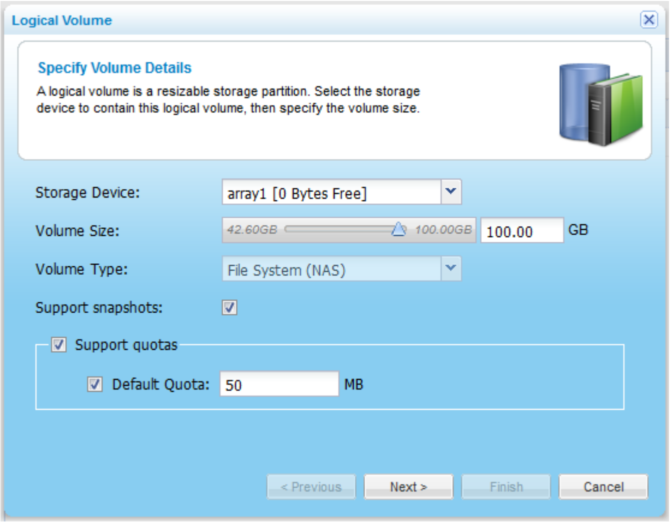
The **Storage > Volumes** page appears.



2 Do one of the following:

- To add a new volume, click **New**.
- To edit an existing volume, click on its name.

The **Logical Volume Wizard** opens, displaying the **Specify Volume Details** dialog box.

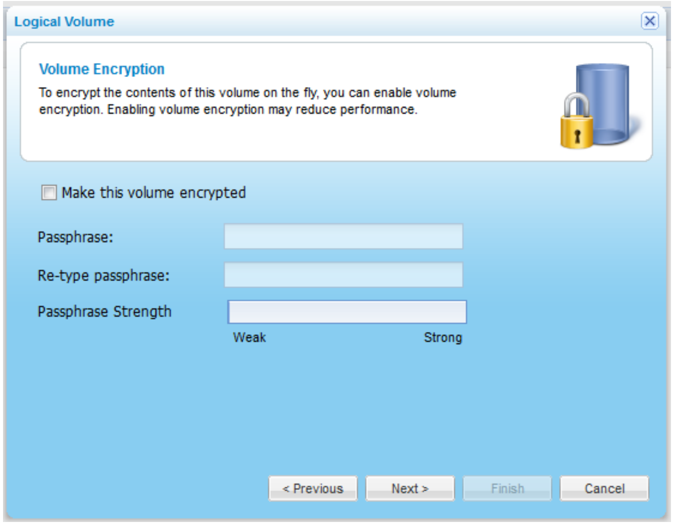


3 Complete the fields using the information in the following table.

4 Click **Next**.

The following things happen:

- If you are adding a new volume or editing an encrypted volume, the **Volume Encryption** dialog box appears.



1 To encrypt the contents of this volume, select the **Make this volume encrypted** check box.

This check box is disabled when editing a volume.

Tip

Volume encryption is supported both for standalone volumes and volumes residing in RAID arrays.

Tip

The encryption method employed is the Advanced Encryption Standard (AES-256 CBC ESSIV). Enabling volume encryption may reduce performance.

2 In the **Passphrase** and **Re-type passphrase** fields, type the passphrase you want to use for accessing the volume.

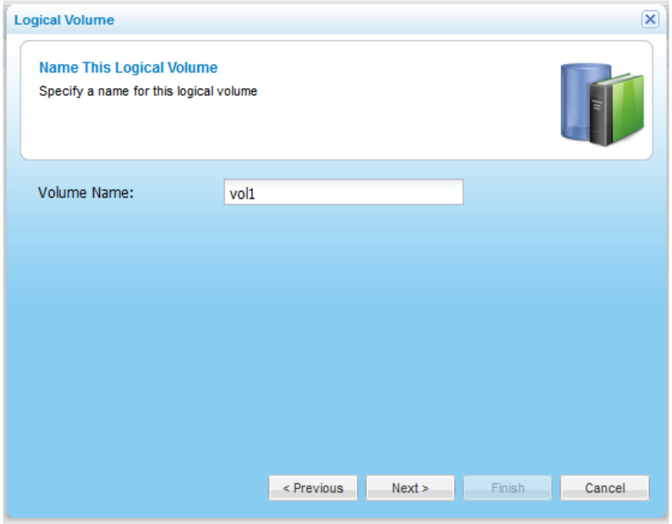
The **Passphrase Strength** field displays the passphrase's strength.

Warning

It is important to keep this passphrase in a safe place, as there is no way of retrieving it if you lose it. If you reset your appliance to its default settings, you cannot access the volume without this passphrase.

3 Click **Next**.

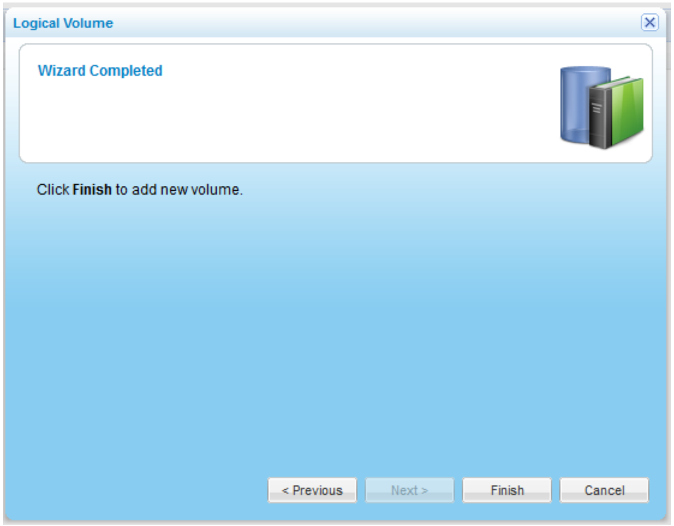
- The **Name this Logical Volume** dialog box appears.



5 In the **Volume Name** field, type a name for the volume.

6 Click **Next**.

The **Wizard Completed** screen appears.



7 Click **Finish**.

Table 19: Volume Details Fields

In this field...	Do this...
Storage Device	Select the array on which you want to create the volume. The size of each array is listed next to its name. You can also create volumes directly on an empty drive. This is called a *standalone drive*.
Volume Size	Do one of the following: - Use the slide to indicate the desired size of the volume out of the total array size. - Type the desired volume size in GB in the field provided. **Note**: If snapshots are enabled, you cannot decrease the size of the volume.
Volume Type	Select the desired volume type: - **File System (NAS)**. A NAS volume, which can be accessed using the various file sharing protocols supported by the appliance. - **Raw volume (SAN)**. A SAN volume, which can be accessed using iSCSI only. For more information on volume types, see ***Overview*** (on page 63). Once set, the volume type cannot be changed.
Support snapshots	Select this option to enable NEXT3 snapshots for the volume. The volume will be installed with the NEXT3 file system, and snapshots will automatically be taken of the volume before each cloud backup or outgoing synchronization rule is performed. **Note**: This option relates to NEXT3 snapshots only, and clearing it will not prevent cloud snapshots from being created. For information on types of snapshots, see ***Working with Snapshots*** (see "***Working with Volume Snapshots***" on page 87). This option is only available if the volume type is **File System (NAS)**.

Support quotas	Select this option limit the amount of storage space allocated to each volume user. Each user can then be allocated a specific storage space quota, as described in ***Allocating Disk Quotas to Users*** (on page 256). If quotas are not enabled, then each user will be able to use unlimited amount of space on this volume.
Default Quota	To set a default storage space quota for volume users, select this option and then type the desired default quota in MB in the field. This quota will be allocated to each user by default. If this option is not enabled, then an unlimited amount of space will be allocated to each user by default. In either case, the default allocated quota can be overridden, as described in ***Allocating Disk Quotas to Users*** (on page 256).

Deleting Logical Volumes

To delete a logical volume

1 In the **Configuration** tab's navigation pane, click **Storage > Volumes**.

The **Storage > Volumes** page appears.

2 Select the desired volume and click **Delete**.

A confirmation message appears.

3 Click **Yes**.

The volume is deleted.

Scanning and Repairing Logical Volumes

You can scan the file system on a volume for errors. Any detected errors are automatically repaired, if possible.

The scan and repair utility supports both EXT3 and NEXT3 volumes.

Warning

During the scanning process, the volume is taken offline. Do not turn off the appliance, while the volume is being scanned.

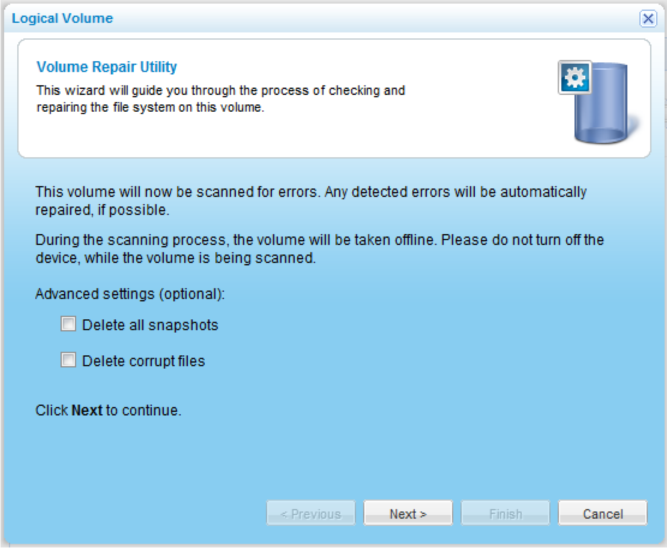
To scan and repair a volume

1 In the **Configuration** tab's navigation pane, click **Storage > Volumes**.

The **Storage > Volumes** page appears.

2 Select the desired volume and click **Repair**.

The **Logical Volume Wizard** opens, displaying the **Volume Repair Utility** dialog box.



3 To delete all snapshots for this volume, select the **Delete all snapshots** check box.

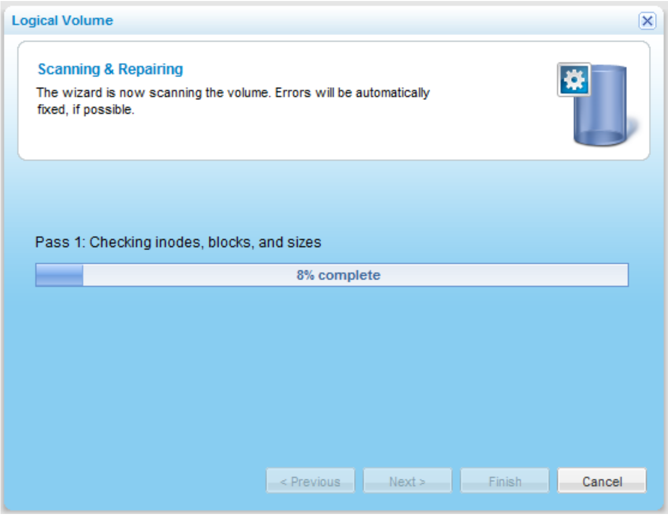
This option is only available when repairing a NEXT3 volume.

4 To delete corrupt files, select the **Delete corrupt files** check box.

If repairing a NEXT3 volume, the **Delete all snapshots** check box is automatically selected.

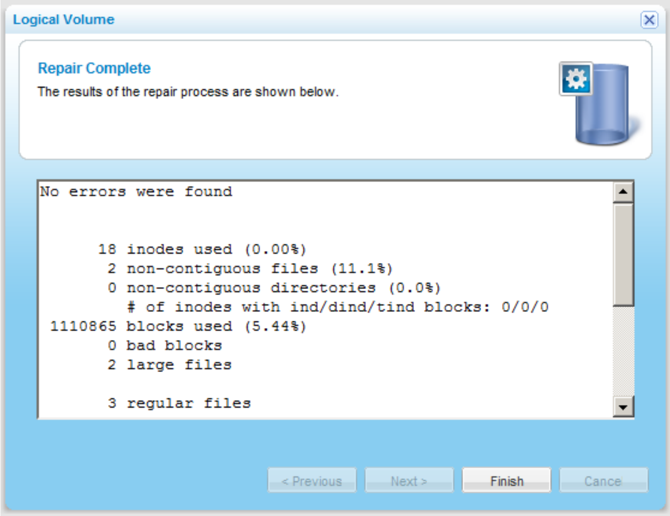
5 Click **Next**.

The **Scanning & Repairing** screen appears with a progress bar.



The files system on the volume is scanned for errors.

The **Repair Complete** screen appears with a list of files system errors that were corrected.



6 Click **Finish**.

Working with iSCSI Targets

iSCSI is a popular storage area network (SAN) protocol, allowing organizations to consolidate storage into data center storage arrays while providing hosts (such as database and web servers) with the illusion of locally-attached disks.

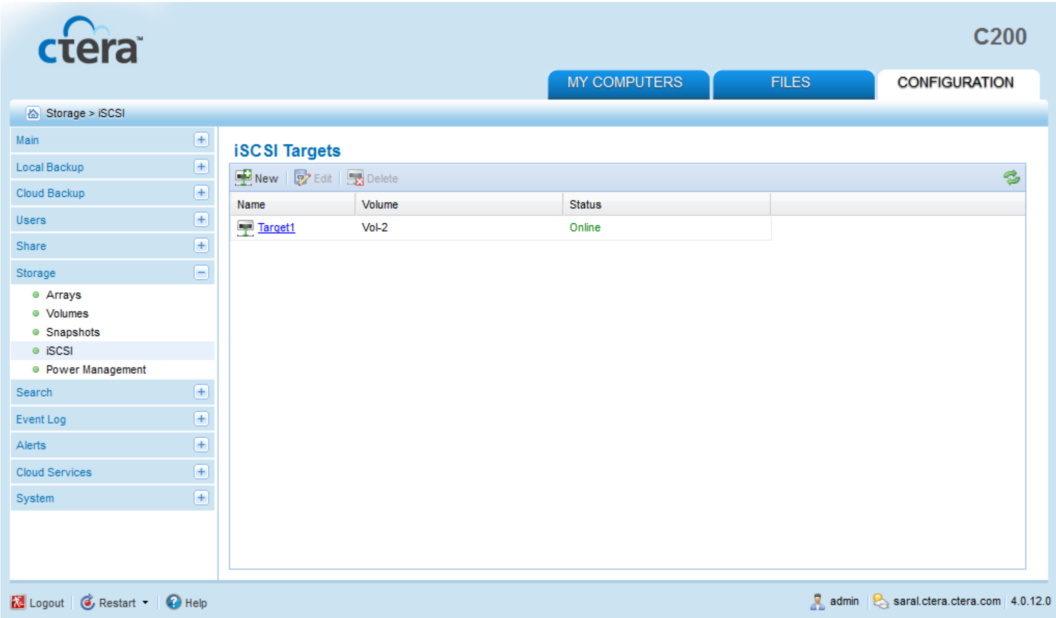
You can define SAN volumes, which are unformatted volumes (also called "Raw"). In order for users to access a SAN volume, an iSCSI target should be defined for this volume. The SAN volume will then appear as if it were a physical disk on the user's PC or server and can be formatted remotely.

Adding and Editing iSCSI Targets

To add or edit an iSCSI target

1 In the **Configuration** tab's navigation pane, click **Storage > iSCSI**.

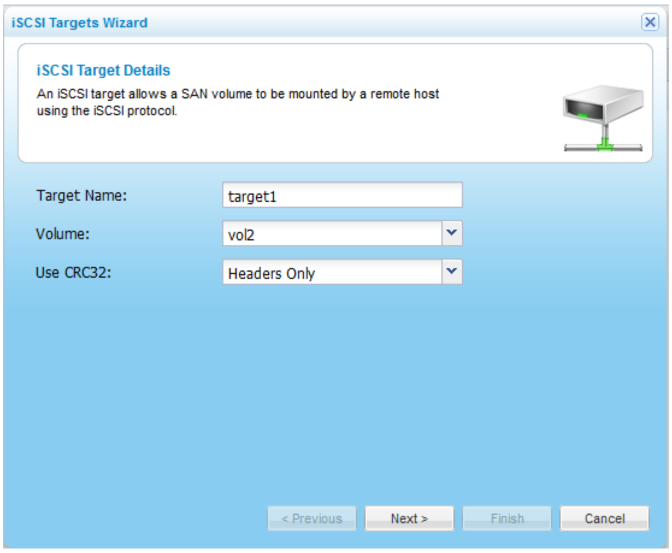
The **Storage > iSCSI** page appears.



2 Do one of the following:

- To add a new target, click **New**.
- To edit an existing target, click on its name.

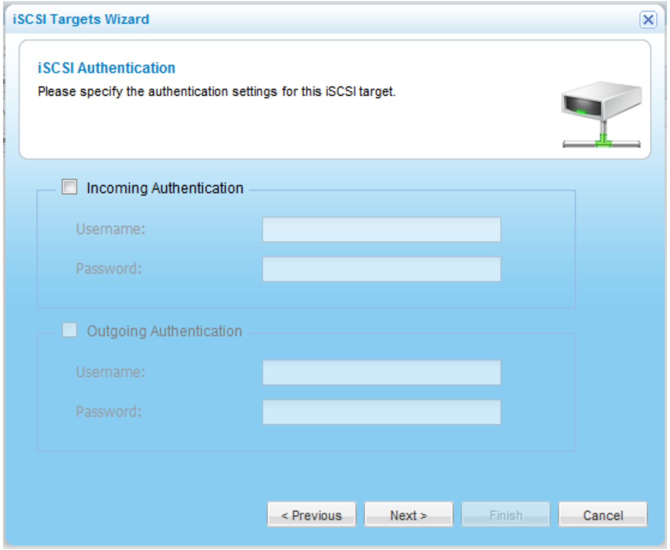
The **iSCSI Targets Wizard** opens, displaying the **iSCSI Target Details** dialog box.



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

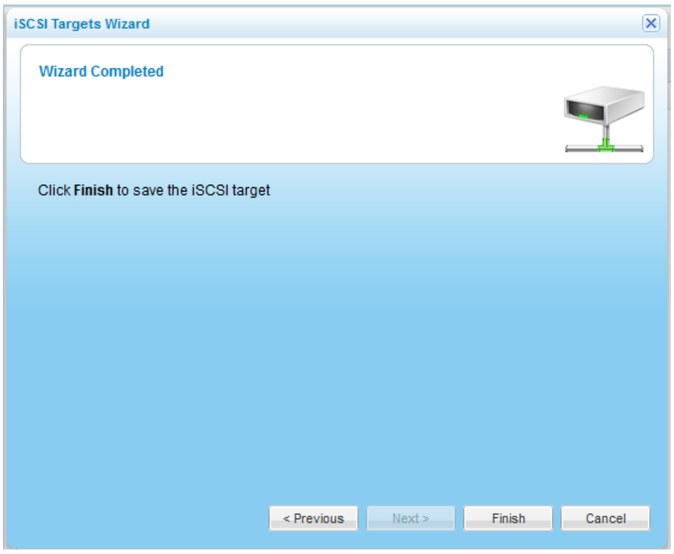
4 Click **Next**.

The **iSCSI Authentication** dialog box appears.



5 Click **Next**.

The **Wizard Completed** screen appears.



6 Click **Finish**.

Table 20: iSCSI Target Fields

In this field...	Do this...
Target Name	Type a name for the target.
Volume	Select the SAN volume to be mounted.
Use CRC32	Specify whether CRC-32 should be used to detect errors in data transmitted between the remote host and the iSCSI target, by selecting one of the following: - **None**. Do not use CRC-32. This setting improves performance slightly. - **Headers Only**. Use CRC-32 to verify the integrity of packet headers. This is the recommended setting. - **Headers and Data**. Use CRC-32 to verify the integrity of packet headers and data. This setting is slightly safer than the other options. The default value is **Headers Only**.
Incoming Authentication	Select this option to configure the authentication settings that the remote host should use when connecting to the iSCSI target. The relevant **Username** and **Password** fields are enabled.
Username	Type the user name to use for incoming authentication.
Password	Type the password to use for incoming authentication.
Outgoing Authentication	Select this option to configure the authentication settings that the iSCSI target should use when connecting to the remote host. The relevant **Username** and **Password** fields are enabled.
Username	Type the user name to use for outgoing authentication.
Password	Type the password to use for outgoing authentication.

Deleting iSCSI Targets

To delete an iSCSI target

1. In the **Configuration** tab's navigation pane, click **Storage > iSCSI**.

   The **Storage > iSCSI** page appears.
2. Select the desired iSCSI target.
3. Click **Delete**.

A confirmation message appears.

4 Click **Yes**.

The target is deleted.

Installing a SATA Hard Drive

Tip

It is possible to install hard drives without switching off the appliance.

For information on installing a SATA hard drive in the C200, see ***Installing a SATA Hard Drive in the CTERA C200*** (on page 11).

For information on installing a SATA hard drive in the C400, see ***Installing a SATA Hard Drive in the CTERA C400*** (on page 21).

For information on installing a SATA hard drive in the C800, see ***Installing a SATA Hard Drive in the CTERA C800*** (on page 32).

Safely Removing Hard Drives

Tip

It is possible to safely uninstall hard drives without switching off the appliance.

Tip

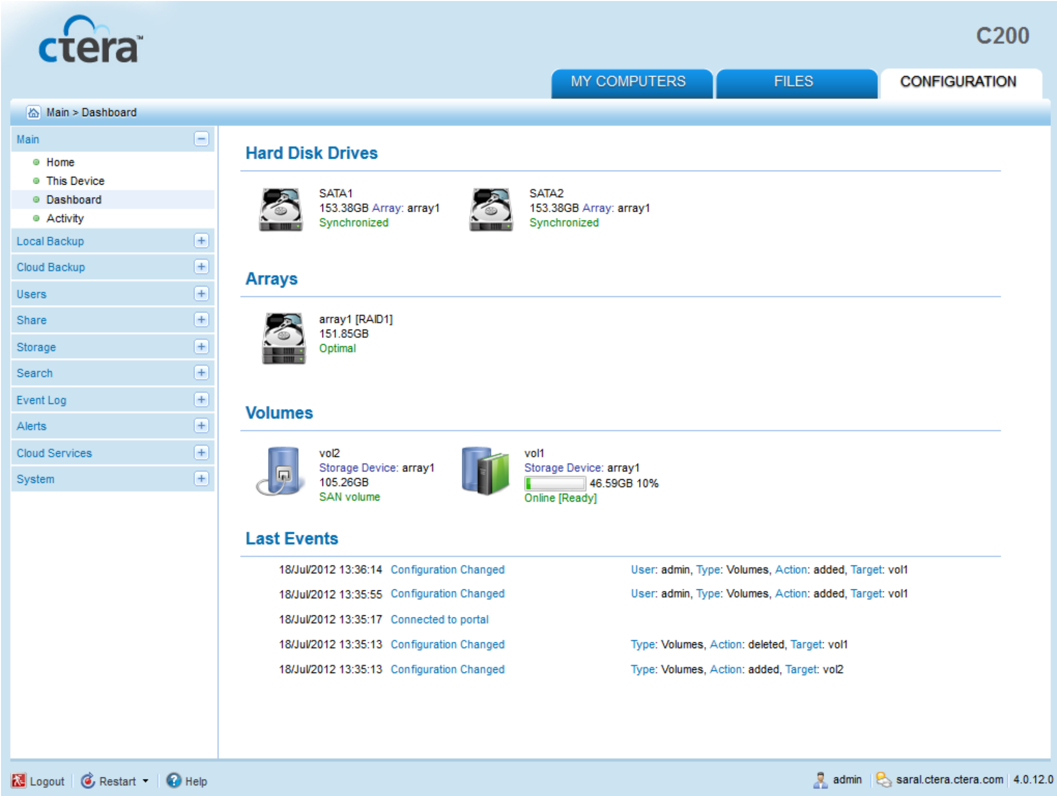
In CTERA C200, it is possible to safely remove USB hard drives, by pressing the Eject button near the USB port.

To remove a hard drive

1 Prepare the drive for safe removal, by doing the following:

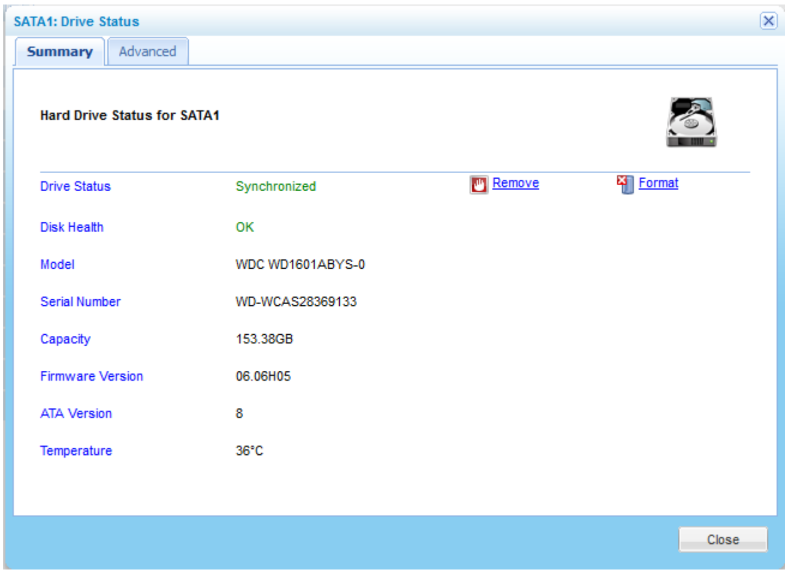
   a In the **Configuration** tab's navigation pane, click **Main > Dashboard**.

The **Main > Dashboard** page appears.



b In the **Hard Disk Drives** area, click on the drive for which you want information.

The **Drive Status** window appears, displaying the **Summary** tab.



c Click **Remove**.

A confirmation message appears.

d Click **Yes**.

The disk is unmounted and can be safely removed.

2 Remove the hard drive as described in one of the following:

- ***Removing a SATA Hard Drive from the CTERA C200*** (on page 12)
- ***Removing a SATA Hard Drive from the CTERA C400*** (on page 23)
- ***Removing a SATA Hard Drive from the CTERA C800*** (on page 33)

Hot Swapping a Disk in a RAID1, 5, or 6 Array

When using RAID1 (mirroring) or RAID 5/6, you can replace any single hard drive without losing any of your data. Your data remains available and online during the entire process.

To hot swap a disk

1 Remove the hard drive as described in ***Safely Removing Hard Drives*** (on page 84).

2 Install a new hard drive into the vacant slot as described in ***Installing a SATA Hard Drive*** (on page 84).

3 In the **Configuration** tab's navigation pane, click **Main > Dashboard**.

The **Main > Dashboard** page appears.

4 Wait until the array's status is optimal.

Enlarging a RAID1 Array

You can use hot swapping to enlarge a RAID1 array. For example, assume you have two hard drives, HDD1 and HDD2, in a RAID1 mirroring configuration and in optimal state. The capacity of HDD1 and HDD2 is 500GB each, meaning the array size is 500GB. You can enlarge the array to 1TB as follows:

1 Hot swap HDD1, replacing it with a 1TB hard drive as described in ***Hot Swapping a Disk in a RAID1, 5, or 6 Array*** (on page 86).

2 Wait until the array's status is optimal.

3 Hot swap HDD2, replacing it with a 1TB hard drive as described in ***Hot Swapping a Disk in a RAID1, 5, or 6 Array*** (on page 86).

4 Wait until the array's status is optimal.

The array will now be 1TB in size.

You can now enlarge volumes on the array to fill the available space, or add new volumes.

8

Working with Volume Snapshots

This chapter explains how to use NEXT3 volume snapshots.

In This Chapter

Overview

The appliance can take snapshots of volumes. A *volume snapshot* is a read-only copy of a volume as it was at a particular point in time.

The appliance automatically takes snapshots before performing a cloud backup or running an outgoing synchronization rule for a NEXT3 volume, so as to ensure that a consistent image of all files is transmitted. In addition, you can schedule automatic daily snapshots and take snapshots manually.

You can use snapshots to access previous versions of your volumes and the files contained therein.

Terminology

The appliance supports two types of snapshots:

- **Cloud Snapshots**

  Cloud snapshots are snapshots that are stored online using CTERA's Cloud Backup service. They are automatically generated with each cloud backup operation.

Cloud snapshots can be accessed via the CTERA Portal and, when Windows File Sharing is enabled, locally.

- **NEXT3™ Volume Snapshots**

  NEXT3 volume snapshots are stored locally on a NEXT3-snapshot-enabled volume and can be accessed at local speeds. NEXT3 was developed by CTERA to add flexible snapshots to EXT3, along with easy transition from and to EXT3.

  NEXT3 snapshots are faster to access locally than cloud snapshots, regardless of the number of stored snapshots. Furthermore, you can configure appliance to automatically take NEXT3 snapshots and retain them according to a specified retention policy. On the downside, NEXT3 snapshots are stored onsite, and so are vulnerable to disasters.

It is recommended to combine NEXT3 snapshots for fast recovery from non-disaster situations (such as an important file being accidentally overwritten by one of your office employees), with cloud snapshots for recovery from major disasters such as flood or fire.

Tip

NEXT3 Snapshots are available for NAS volumes only, SAN volumes do not support snapshots.

Workflow

To use snapshots, do the following:

1. Enable NEXT3 snapshots for specific volumes.

   See ***Adding and Editing Logical Volumes*** (on page 73).

2. Do one or more of the following:

   - Schedule automatic snapshots and a retention policy for all NEXT3-snapshot-enabled volumes.

     See ***Scheduling Automatic Snapshots*** (on page 89).

     Snapshots will be taken for all NEXT3-snapshot-enabled volumes according to the configured schedule, and they will be retained according to the specified retention policy.

   - Manually take a snapshot of a selected NEXT3-snapshot-enabled volume.

     See ***Manually Taking Snapshots*** (on page 93).

     A NEXT3 snapshot is immediately created. The snapshot will be retained until manually deleted.

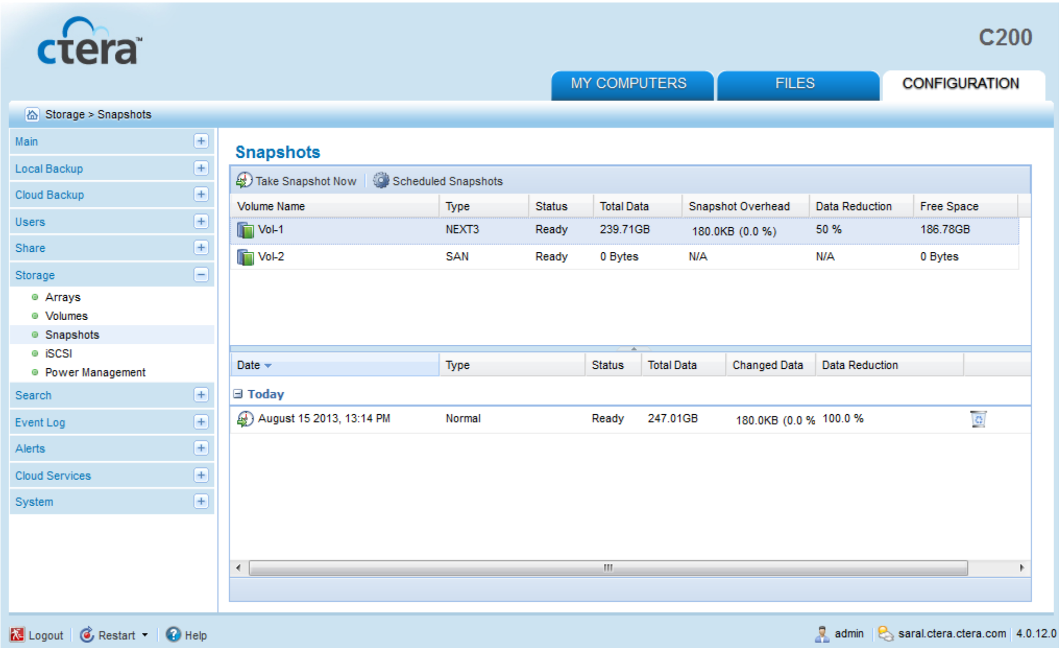
Scheduling Automatic Snapshots

You can schedule automatic daily snapshots and a snapshot retention policy for all NEXT3-snapshot-enabled volumes. For an explanation of retention policies, see ***Understanding Snapshot Retention Policies*** (on page 91).

To schedule automatic snapshots

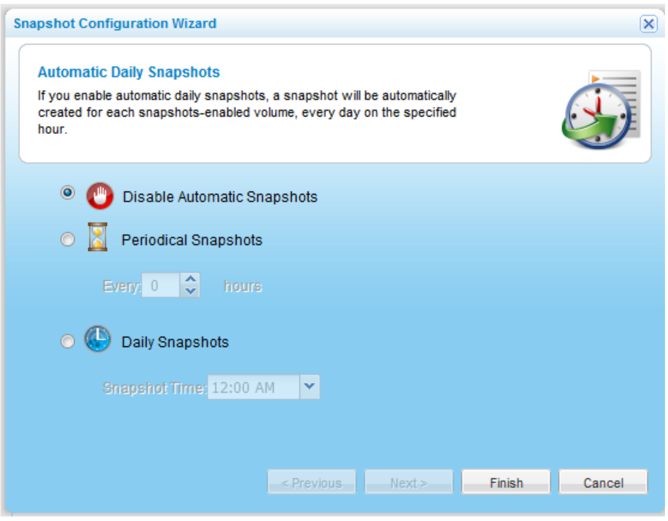
1. In the **Configuration** tab's navigation pane, click **Storage > Snapshots**.

   The **Storage > Snapshots** page appears.



2. Click **Scheduled Snapshots**.

   The **Snapshot Configuration Wizard** opens, displaying the **Automatic Daily Snapshots** dialog box.



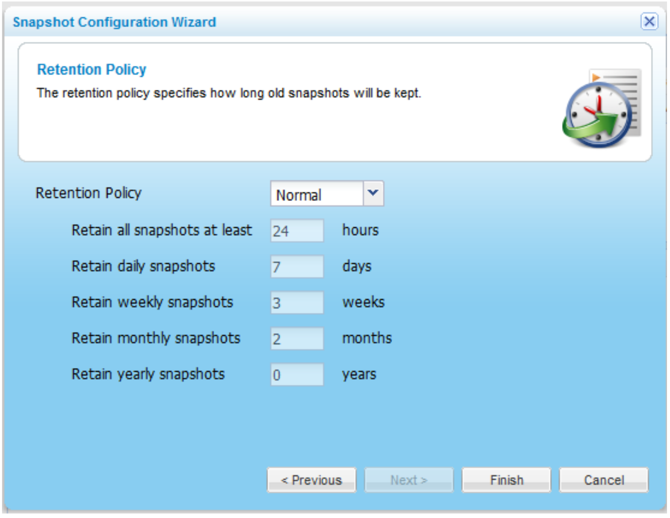
3 Do one of the following:

- To disable automatic scheduled snapshots, choose **Disable Automatic Snapshots**.
- To enable automatic snapshots every certain number of hours, choose **Periodical Snapshots**, then use the arrows in the **Every** field to specify the interval between snapshots, in hours.
- To enable daily automatic snapshots at a certain hour, choose **Daily Snapshots**, then select the hour at which snapshots should be taken in the **Snapshot Time** drop-down list.

4 If you enabled scheduled snapshots, do the following:

a Click **Next**.

The **Retention Policy** dialog box appears.



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

5 Click **Finish**.

Table 21: Retention Policy Fields

In this field...	Do this...
Retention Policy	Select the desired snapshot retention policy: - **Short**. Short-term retention policy. - **Normal**. Medium-term retention policy. - **Long**. Long-term retention policy. - **Custom**. Configure a custom retention policy. The default value is **Normal**. For an explanation of each policy, see ***Understanding Snapshot Retention Policies*** (on page 91). If you selected **Custom**, the other fields in the dialog box are enabled, and you can use them to configure a custom retention policy.
Retain all snapshots at least	Type the minimum number of hours that snapshots of any type should be retained. The default value is 24 hours.
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 yearly snapshots	Type the number of yearly snapshots that should be retained.

Understanding Snapshot Retention Policies

You can configure a snapshot retention policy for all NEXT3-snapshot-enabled volumes. A retention policy specifies the following:

- **The number 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 current daily snapshot will be deleted when the next day starts.

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

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

  Tip

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

  Example 1:

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

Example 2:

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

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

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

  Example 1:

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

  Example 2:

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

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

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

  Example 1:

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

  Example 2:

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

- **The minimum amount of time that snapshots should be retained**

  You can protect recent snapshots from deletion, by specifying the minimum number of hours that snapshots of any type should be retained. After this amount of time has elapsed, the snapshots will be deleted according to the retention policy.

  The default value is 24 hours, meaning that snapshots created less than 24 hours ago will not be deleted.

The appliance offers the following pre-defined retention policies:

Table 22: Predefined Snapshot Retention Policies

This policy...	Retains all snapshots for at least...	Daily snapshots for...	Weekly snapshots for...	Monthly snapshots for...	And yearly snapshots for...
Short	24 hours	10 days	2 weeks	0 months	0 years
Normal	24 hours	7 days	3 weeks	2 months	0 years
Long	24 hours	3 days	2 weeks	6 months	1 year

If desired, you can configure a custom retention policy.

Manually Taking Snapshots

You can manually take a snapshot of an individual NEXT3-snapshot-enabled volume at any time.

Tip

Manually taken snapshots are retained until manually deleted.

To manually take a snapshot

1. In the **Configuration** tab's navigation pane, click **Storage > Snapshots**.

   The **Storage > Snapshots** page appears.

2. In the workspace's upper pane, select the desired NEXT3-snapshot-enabled volume.
3. Click **Take Snapshot Now**.

   A progress bar appears, followed by a success message.

4. Click **OK**.

   The snapshot appears in the lower pane.

   The **Date** field displays the date and time at which the snapshot was created, and the **Size** field displays the snapshot's current size.

   Tip

   A snapshot retains all of the data that has changed on the volume, since the snapshot's creation. Therefore, the snapshot's size is zero upon creation, and its size grows as changes are made to the files on the volume.

Viewing Snapshot Information

You can view the snapshot information for each volume. For information on viewing snapshot contents, see ***Viewing Snapshot Contents*** (on page 96).

To view snapshot information

1 In the **Configuration** tab's navigation pane, click **Storage > Snapshots**.

The **Storage > Snapshots** page appears.

The upper pane displays snapshot information for each volume. For information on the fields displayed, see ***Volume Snapshots Upper Pane Fields*** (page 94).

2 In the workspace's upper pane, select the desired volume.

Snapshots for the volume appear in the lower pane. Deleted snapshots that have not yet been compacted appear in gray.

For information on the fields displayed, see ***Volume Snapshots Lower Pane Fields*** (page 95).

Table 23: Volume Snapshots Upper Pane Fields

This field...	Displays...
Volume Name	The name of the volume.
Type	The volume's type.
Status	The volume's status. This can be either of the following: - **Ready**. No snapshot operation in progress. - **Busy**. A snapshot operation is in progress.
Total Data	The total amount of data on the volume in GB.
Snapshot Overhead	The amount of space on the volume that is used to store snapshots in MB, followed by the percentage of the volume that is used to store snapshots.
Data Reduction	NEXT3 stores snapshots efficiently, by storing only incremental changes. The data reduction field displays the ratio between the actual amount of space used for storing snapshots incrementally, and the amount of space which would have been used had the snapshots been stored non-incrementally, in percentages. In other words, this field represents the amount of space saved by using an incremental method of storing snapshots.
Free Space	The amount of free space on the volume in GB.

Table 24: Volume Snapshots Lower Pane Fields

This field...	Displays...
Date	The date and time at which the snapshot was created.
Type	The snapshot's type. This can be any of the following: - **Online**. A scheduled or manually taken snapshot that has not been deleted. - **System**. The snapshot was taken as part of a system task, such as cloud backup or an outgoing synchronization rule, so as to so as to ensure that a consistent, point-in-time image of all files is transmitted during backup/synchronization. The snapshot will be automatically deleted when the task is completed. - **Deleted**. The snapshot has been deleted, but the space it is using on the volume has not yet been reclaimed (that is, the snapshot has not yet been compacted).
Status	The snapshot's status. This can be any of the following: - **Ready**. The snapshot is mounted and available. - **Pending delete**. The snapshot is in queue for deletion. - **Deleting**. The snapshot is being deleted. A progress bar indicates the deletion's progress. - **Pending compact**. The snapshot will be compacted when the appliance is next rebooted. - **Compacting**. The snapshot is being compacted. A progress bar indicates the compaction's progress. - **Offline**. The snapshot is currently unavailable.
Total Data	The total amount of data contained in the snapshot in GB.
Changed Data	The amount of data that changed between this snapshot and the previous snapshot in GB, followed by the percentage of the data that changed.
Data Reduction	NEXT3 stores snapshots efficiently, by storing only incremental changes. The data reduction field displays the ratio between the actual amount of space used for storing this snapshot incrementally, and the amount of space which would have been used had the snapshot been stored non-incrementally, in percentages. In other words, this field represents the amount of space saved by using an incremental method to store this snapshot.

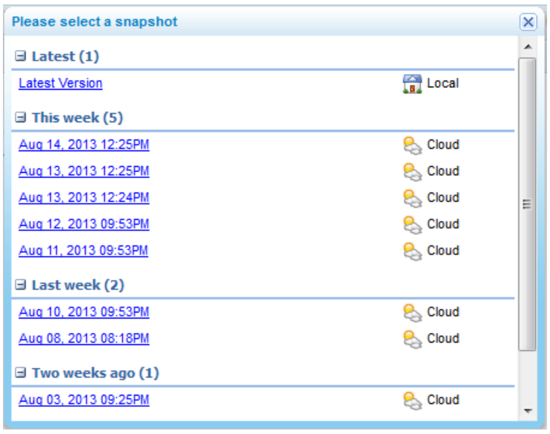
Viewing Snapshot Contents

To view snapshot contents

1 In the **Files** tab's **Show Shares** tree pane view, in the upper bar, click .

For information on changing the tree pane view, see ***Changing the Tree Pane View*** (on page 278).

The **Please select snapshot** dialog box appears.



2 Click on the snapshot whose contents you want to view.

The snapshots are marked according to their type: NEXT3 ( ) or cloud ( ).

The snapshot's contents appear.

Deleting Snapshots

To delete a snapshot

1 In the **Configuration** tab's navigation pane, click **Storage > Snapshots**.

The **Storage > Snapshots** page appears.

2 In the workspace's upper pane, select the desired volume.

Snapshots for the volume appear in the lower pane.

3 Select the desired snapshot.

4 In the snapshot's row, click .

A confirmation message appears.

5 Click **Yes**.

The snapshot is marked for deletion.

Restoring from NEXT3 Snapshots Using Windows File Sharing

When Windows File Sharing (CIFS) is enabled, you can restore files and folders from NEXT3 snapshots on your computer, as described below.

Alternatively, you can restore files and files and folder from the appliance Web interface's File Manager, as described in ***Restoring Files and Folders from a Cloud/NEXT3 Snapshot Using the File Manager*** (on page 182).

To restore an individual file or folder from a NEXT3 snapshot

1. View the network share containing the desired file or folder.

   See ***Viewing Network Shares Using Windows File Sharing*** (on page 146).

2. Open `PreviousVersions\Local`, and browse to the desired file or folder and date.
3. Copy the file or folder to another location.

9

Sharing Files

This chapter explains how to manage network shares to share files with users across your network.

In This Chapter

Overview

You can create *folders* on a volume and share the contents of those folders across your network. In order to share a given folder, you must define a *network share* that includes the folder. A network share can be defined on the entire volume or on a specific folder in the volume.

Once you have defined network shares, users can access them using any of the configured file sharing protocols.

Tip

The following shares are created automatically:

- `public`. A public share with read/write permission for all users.
- `backup`. The default destination for CTERA Agent and Clientless Backups.
- `users`. The default location for storing user home directories. This share is automatically created when the home directories feature is enabled.
- `projects`. The default location for storing projects. This share is automatically created when the collaboration feature is enabled.

Workflow

In order to share files across your network, you must perform the following steps:

1. Configure the folders that you want to share, by doing the following:
   a. Add a network share on a folder.

      See ***Adding and Editing Network Shares*** (on page 101).

   b. If you are using Windows Files Sharing, copy the files that you want to share to the folder.

      See ***Copying Files to a Network Share Using Windows File Sharing*** (on page 108).

2. Set up file sharing protocols, by doing one or more of the following:
   - To enable access to network shares using Windows Files Sharing, see ***Configuring Windows File Sharing*** (on page 114).
   - To enable access to network shares via the CTERA FTP Server, see ***Configuring FTP Access*** (on page 121).
   - To enable access to network shares via the CTERA RSync Server, see ***Configuring RSync Access*** (on page 123).
   - To enable access to network shares using Apple File Sharing, see ***Configuring Apple File Sharing*** (on page 124).
   - To enable access to network shares using NFS, see ***Configuring NFS Access*** (on page 125).

Managing Network Shares

Network shares can be managed in the **Configuration** tab or the File Manager.

Managing Network Shares in the Configuration Tab

Adding and Editing Network Shares

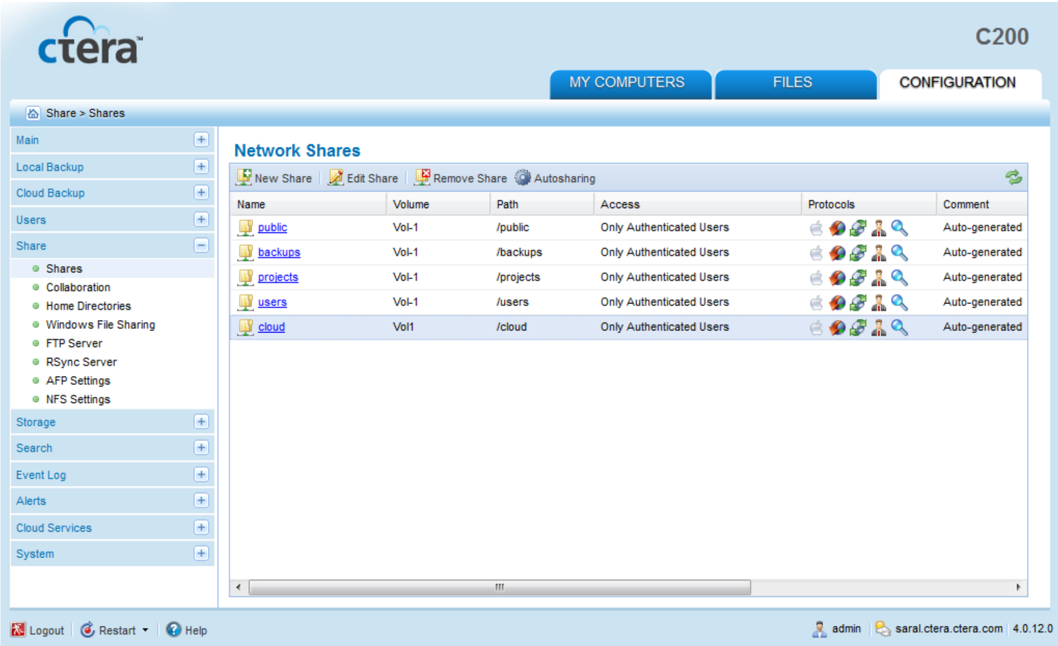
Tip

Network shares must not overlap one another. For example, you cannot share both /a and /a/b.

To add or edit a network share

1 In the **Configuration** tab's navigation pane, click **Share > Shares**.

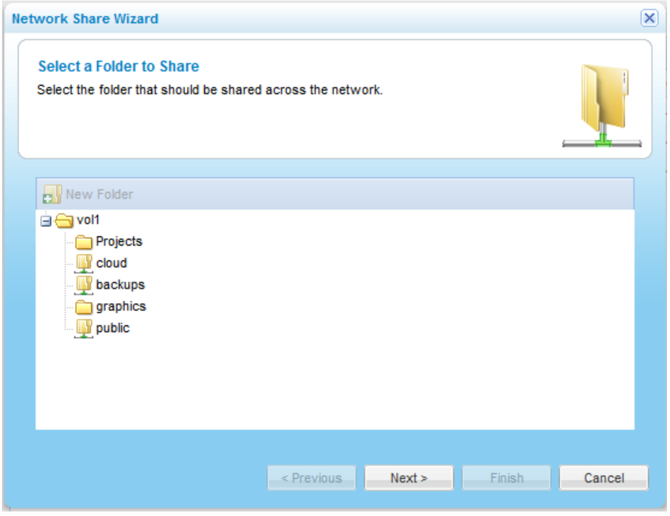
The **Share > Shares** page appears.



2 Do one of the following:

- To add a new network share, click **New Share**.
- To edit an existing network share, click on its name.

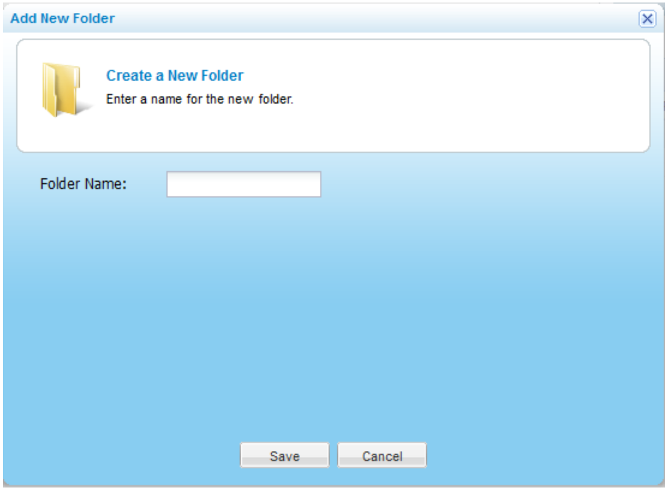
The **Network Share Wizard** opens, displaying the **Select a Folder to Share** dialog box appears.



3 Do one of the following:

- Select the folder on which you want to create the network share.
- To add a folder on which to create the network share, do the following:
  1 Select the parent folder in which to create the new folder.
  2 Click **New Folder**.

  The **Create a New Folder** dialog box opens.

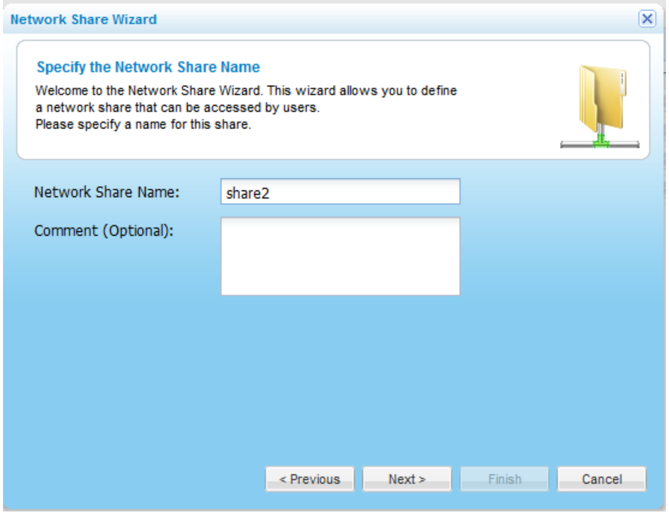


  3 In the **Folder Name** field, type a name for the folder.
  4 Click **Save**.

  The new folder appears in the **Select a folder to Share** dialog box.

4 Click **Next**.

The **Specify the Network Share Name** dialog box appears.

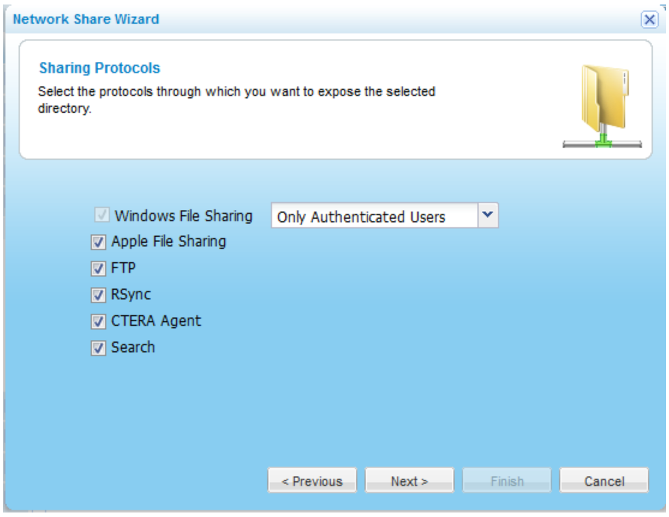


5 In the **Network Share Name** field, type a name for the share.

6 (Optional) In the **Comment** field, type a description of the network share.

7 Click **Next**.

The **Sharing Protocols** dialog box appears.



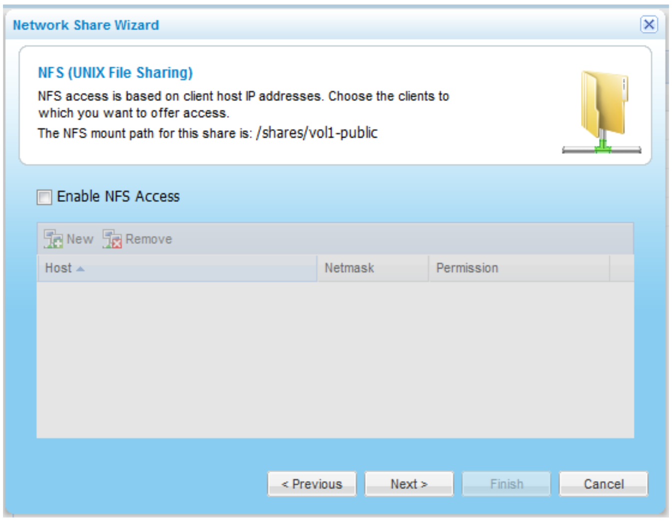
8 Select the protocols through which you want to expose the network share.

Windows File Sharing is selected by default and cannot be unselected.

9 In the **Windows File Sharing** drop-down list, specify the permitted level of access to the network share via Windows File Sharing, by selecting one of the options described in ***Share Access Options*** (page 107).

10 Click **Next**.

The **NFS (UNIX File Sharing)** dialog box appears.



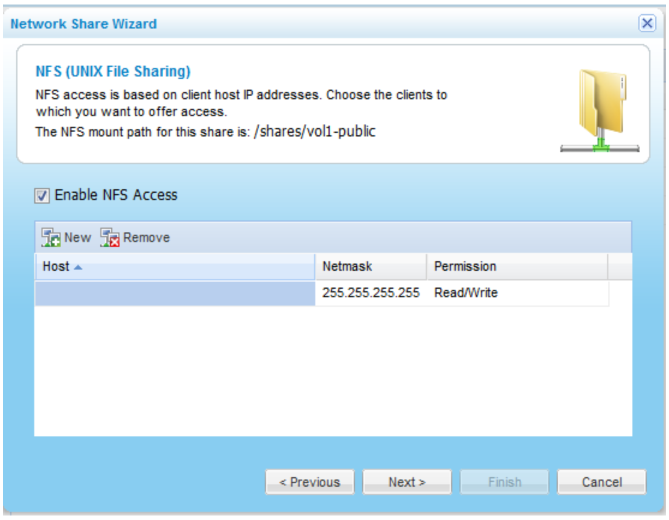
11 To enable NFS access to the network share, do the following:

a Select the **Enable NFS Access** check box.

b Add the IP addresses of clients that should be allowed NFS access to network share, by doing the following:

1 Click **New**.

A row appears in the table.



2 Click in the **Host** column and type the IP address.

3 Click in the **Netmask** column and edit the netmask.

4 Click in the **Permission** column and select the permitted level of access to the network share via NFS.

Options include **None**, **Read Only**, and **Read/Write**.

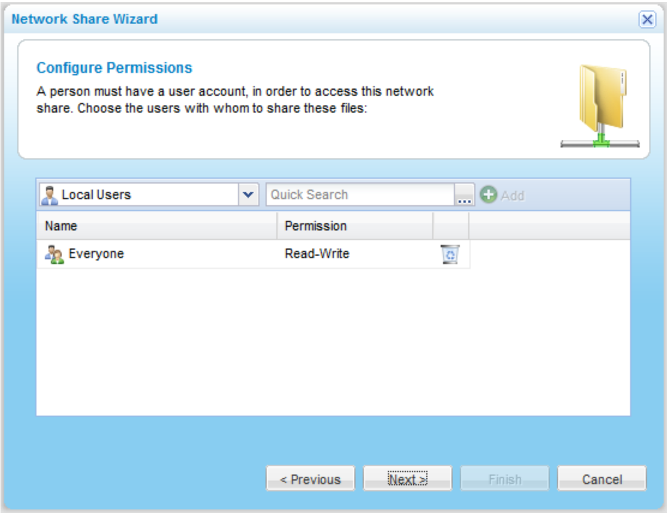
c Remove client host IP addresses, by selecting the desired IP address and clicking **Remove**.

Tip

The NFS mount path for the network share is specified at the top of the dialog box.

12 Click **Next**.

The **Configure Permissions** dialog box appears.



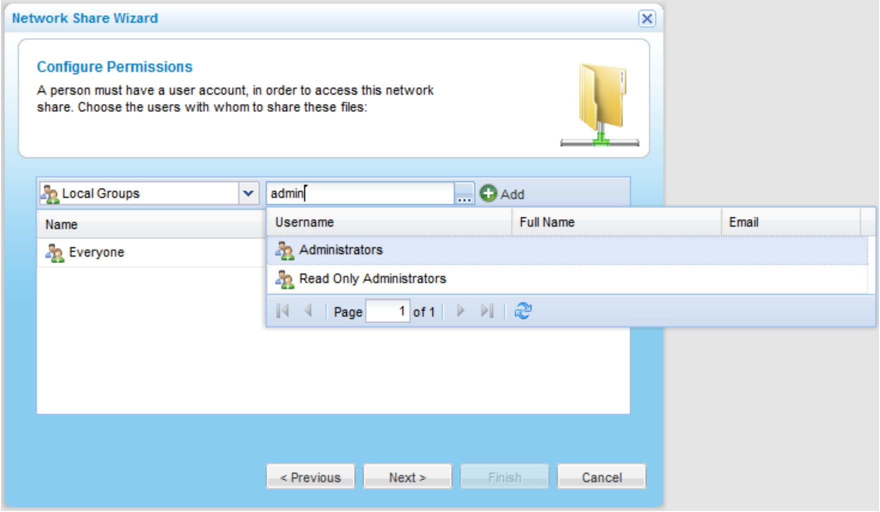
13 Add each user and user group who should have access to the network share, by doing the following:

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

- **Local Users**. Search the users defined locally on the appliance.
- **Domain** *domain* **Users**. Search the users belonging to the domain called *domain*.
- **Local Groups**. Search the user groups defined locally on the appliance.
- **Domain** *domain* **Groups**. Search the user groups belonging to the domain called *domain*.

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

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



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

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

d Click **Add**.

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

For information on editing users, see ***Adding and Editing Users*** (on page 252).

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

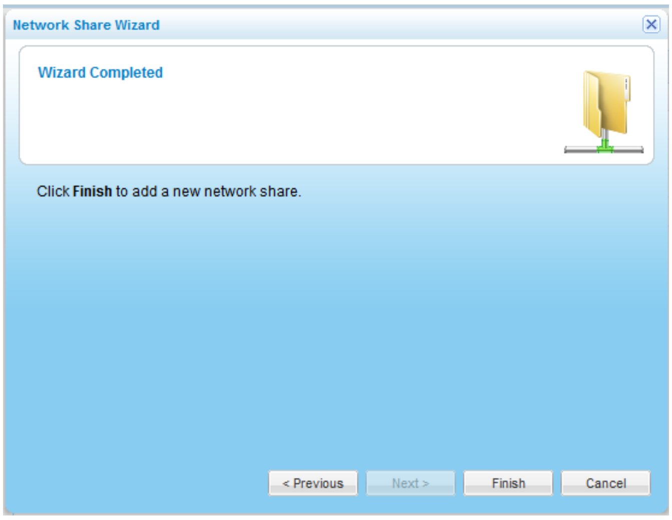
The user or user group is removed from the table.

15 In each user and user group's row, click in the **Permission** column, then select the desired access level from the drop-down list.

Options include **None**, **Read Only**, and **Read/Write**.

16 Click **Next**.

The **Wizard Completed** screen appears.



17 Click **Finish**.

The network share is added.

Table 25: Network Share Access Options

Select this option...	To specify that...
Only Authenticated Users	Users will be required to authenticate using their appliance user name and password, in order to access the network share.
Public Read/Write	Users will be able to read and write to this network share using Windows File Sharing, and will not be required to enter their user name and password.
Public Read	Users will be able to read files from this network share using Windows File Sharing, and will not be required to enter their user name and password.

Deleting Network Shares

To delete a network share

1. In the **Configuration** tab's navigation pane, click **Share > Shares**.

   The **Share > Shares** page appears.

2. Select the desired network share and click **Remove Share**.

   A confirmation message appears.

3. Click **Yes**.

   The network share is deleted.

Copying Files to a Network Share Using Windows File Sharing

To copy files to a network share using Windows File Sharing

1. View the network share containing the desired file or folder.

   See ***Viewing Network Shares Using Windows File Sharing*** (on page 146).

2. Open the relevant network share and folder.
3. Copy the desired files to the folder.

Managing Network Shares in the File Manager

Adding and Editing Network Shares

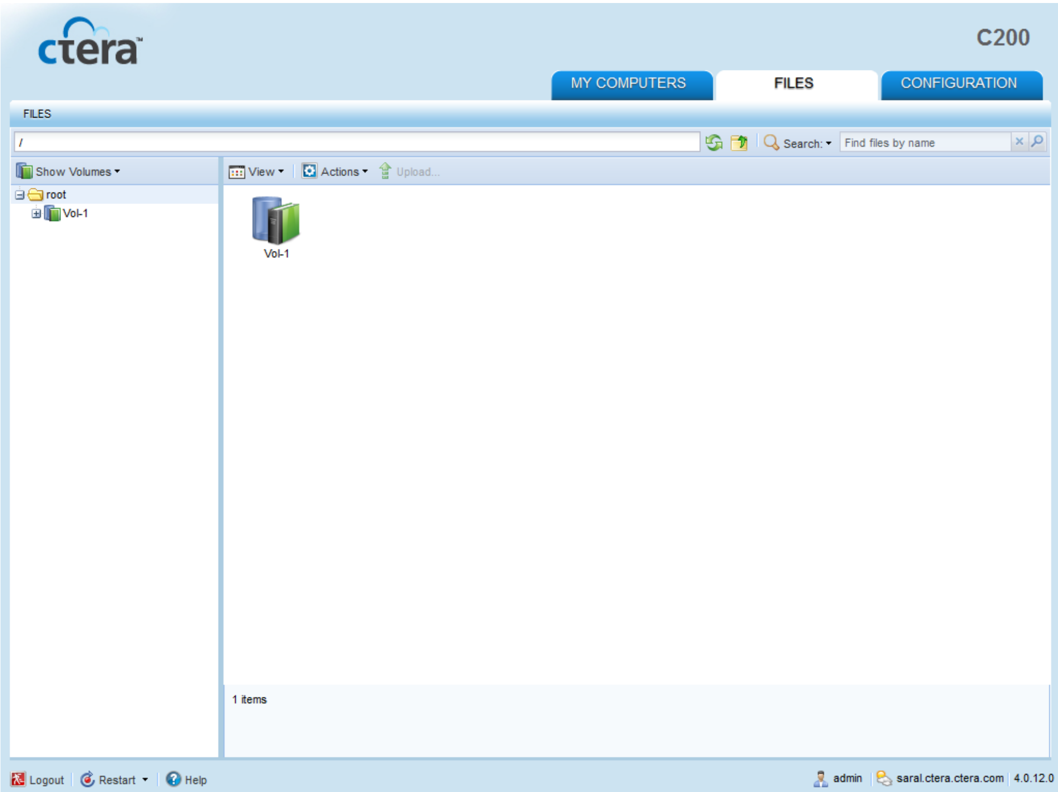
Tip

Network shares must not overlap one another. For example, you cannot share both /a and /a/b.

To add or edit a network share

1. In the File Manager, change to the Volumes view.

   See ***Changing the Tree Pane View*** (on page 278).



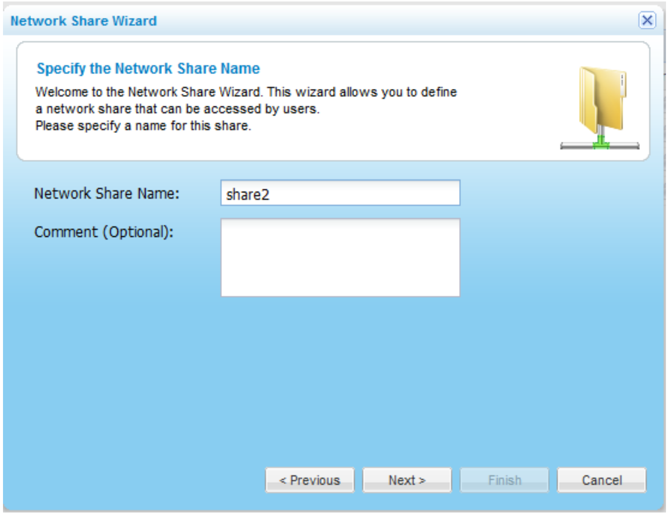
2. Navigate to the desired folder.

   See ***Navigating Between Folders*** (on page 278).

3 In the right pane, select the desired folder.

4 Click **Actions**, and then click **Share**.

The **Network Share Wizard** opens, displaying the **Specify the Network Share Name** dialog box.



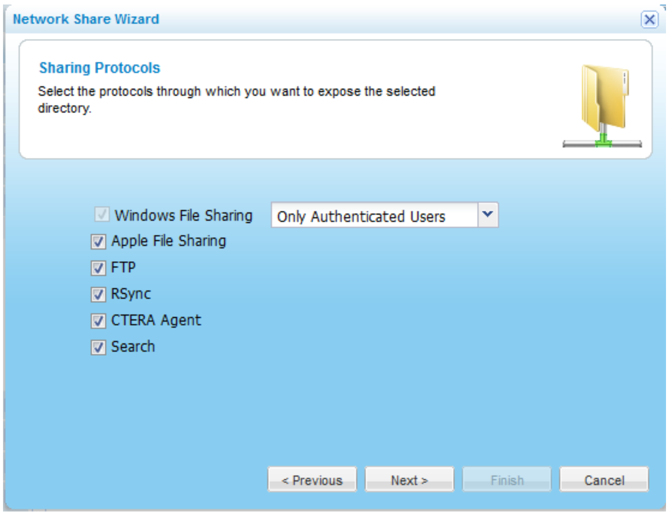
5 In the **Network Share Name** field, type a name for the share.

By default, the folder's name is filled in.

6 (Optional) In the **Comment** field, type a description of the network share.

7 Click **Next**.

The **Sharing Protocols** dialog box appears.



8 Select the protocols through which you want to expose the network share.

Windows File Sharing is selected by default and cannot be unselected.

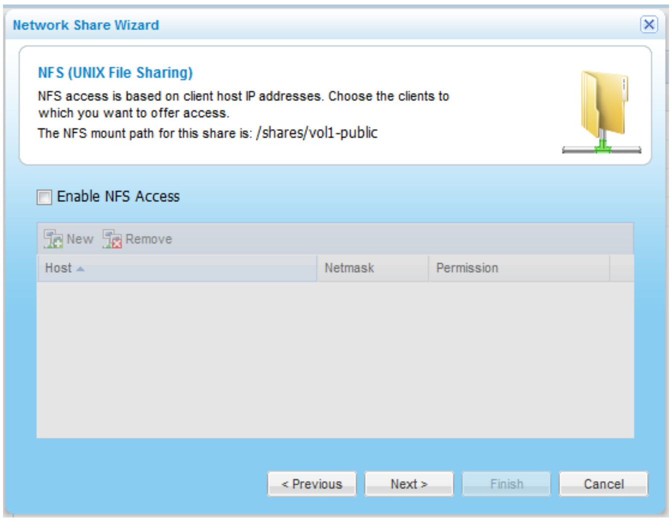
9 To enable full text search for the share, select **Full Text Search**.

For information on full text search, see ***Up Full Text Search*** (see "***Setting Up File Search***" on page 271).

10 In the **Windows File Sharing** drop-down list, specify t***Setting*** (see "***Setting Up File Search***" on page 271)he permitted level of access to the network share via Windows File Sharing, by selecting one of the options described in ***Share Access Options*** (page 107).

11 Click **Next**.

The **NFS (UNIX File Sharing)** dialog box appears.



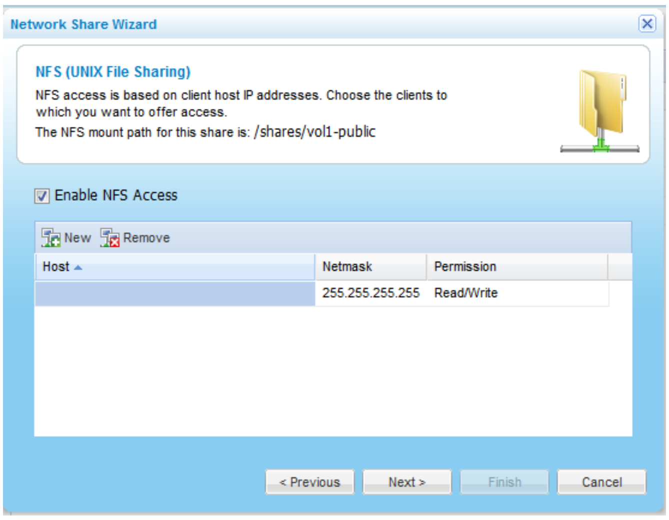
12 To enable NFS access to the network share, do the following:

a Select the **Enable NFS Access** check box.

b Add the IP addresses of clients that should be allowed NFS access to network share, by doing the following:

1 Click **New**.

The IP address 0.0.0.0 appears in the table.



2 Click in the **Host** column and edit the IP address.

3 Click in the **Permission** column and select the permitted level of access to the network share via NFS.

Options include **None**, **Read Only**, and **Read/Write**.

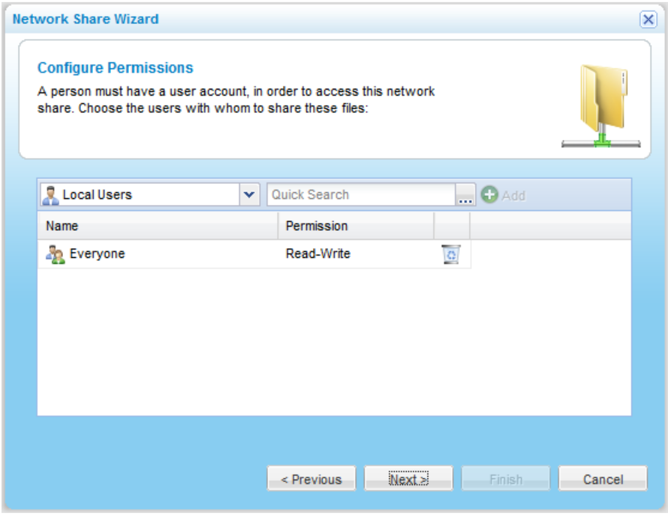
c Remove client host IP addresses, by selecting the desired IP address and clicking **Remove**.

Tip

The NFS mount path for the network share is specified at the top of the dialog box.

13 Click **Next**.

The **Configure Permissions** dialog box appears with a list of users and user groups.



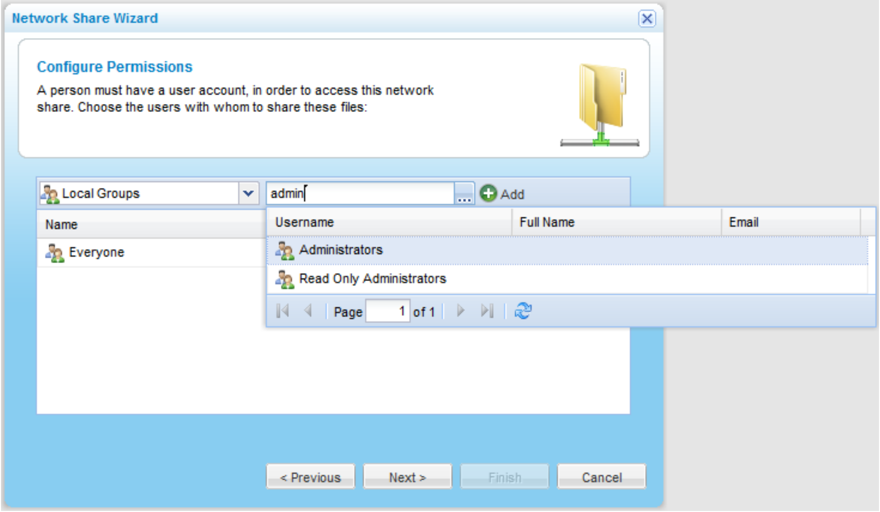
14 Add each user and user group who should have access to the network share, by doing the following:

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

- **Local Users**. Search the users defined locally on the appliance.
- **Domain** *domain* **Users**. Search the users belonging to the domain called *domain*.
- **Local Groups**. Search the user groups defined locally on the appliance.
- **Domain** *domain* **Groups**. Search the user groups belonging to the domain called *domain*.

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

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



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

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

d Click **Add**.

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

For information on editing users, see ***Adding and Editing Users*** (on page 252).

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

The user or user group is removed from the table.

16 In each user and user group's row, click in the **Permission** column, then select the desired access level from the drop-down list.

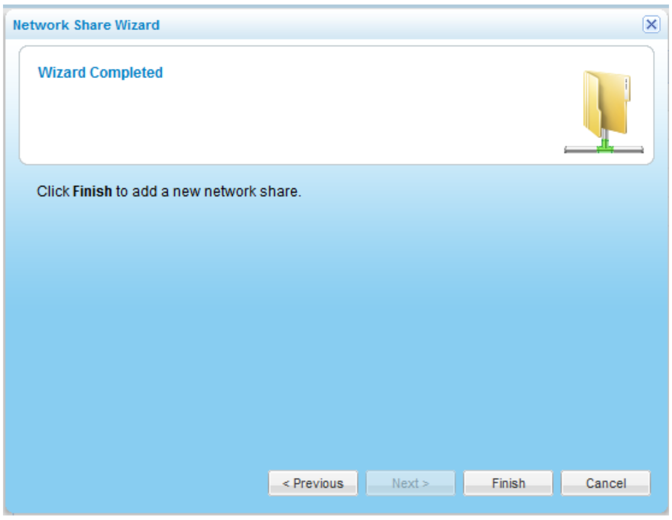
Options include **None**, **Read Only**, and **Read/Write**.

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

The user or user group is removed from the table.

18 Click **Next**.

The **Wizard Completed** screen appears.



19 Click **Finish**.

In the File Manager, the folder's icon changes to .

Removing Network Shares from Folders

To remove a network share from a folder

1. In the File Manager, change to the Volumes view.

   See ***Changing the Tree Pane View*** (on page 278).

2. Navigate to the desired folder.

   See ***Navigating Between Folders*** (on page 278).

3. In the right pane, select the desired folder.
4. Click **Actions**, and then click **Unshare**.

   A confirmation message appears.

5. Click **Yes**.

   The folder is no longer shared.

   In the File Manager, the folder's icon changes to .

Configuring File Sharing Protocols

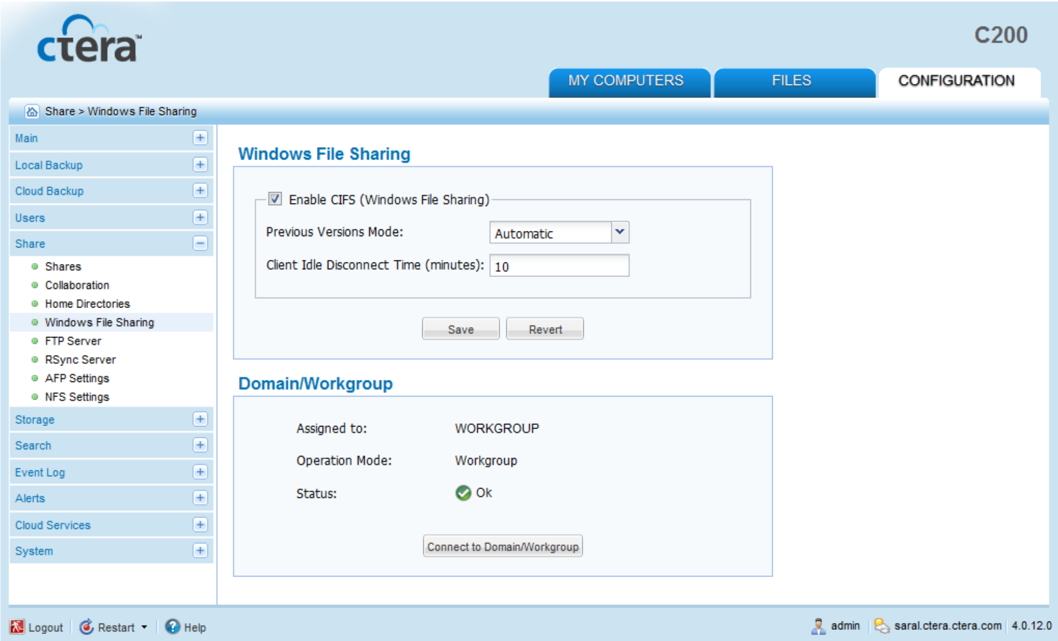
Configuring Windows File Sharing

When Windows Files Sharing is configured, users can view network shares as described in ***Viewing Network Shares Using Windows File Sharing*** (on page 146).

To configure Windows file sharing

1. In the **Configuration** tab's navigation pane, click **Share > Windows File Sharing**.

   The **Share > Windows File Sharing** page appears.



2. Complete the fields using the following table.
3. Click **Save**.
4. (Optional) Do one of the following:
   - To configure Windows file sharing for a network without a domain controller, see ***Configuring Windows File Sharing for a Workgroup*** (on page 115).
   - To configure Windows file sharing for a network with a single domain controller, see ***Configuring Windows File Sharing for an Individual Active Directory Domain*** (on page 117).
   - To configure Windows file sharing for an Active Directory multi-domain environment (that is, a tree or forest), see ***Configuring Windows File Sharing for an Active Directory Tree or Forest*** (on page 117).

- To configure administrative permissions for Active Directory users and/or groups for a single or multi-domain environment, see ***Granting Administrative Permissions to Active Directory Users/Groups*** (on page 119).

Table 26: Windows Sharing Settings Fields

In this field...	Do this...
Enable CIFS (Windows File Sharing)	Select this option to enable Windows file sharing.
Previous Versions Mode	Select the type of snapshots that should be exposed through the "Previous Versions" interface: - **Automatic**. For volumes that are NEXT3 snapshot enabled, display NEXT3 snapshots for all shares. For volumes that are not NEXT3 snapshot enabled, display cloud snapshots for all shares. - **Local Snapshots**. NEXT3 snapshots, which are stored locally on a NEXT3-snapshot-enabled volume - **Cloud Snapshots**. Cloud snapshots, which are stored online using CTERA's Cloud Backup service The default value is **Automatic**. For more information on snapshots, see ***Working with Volume Snapshots*** (on page 87).
Client Idle Disconnect Time	Type the amount of time in minutes after which a client should be disconnected, if the connection is idle. This is an advanced setting, and there is usually no need to change it. The default value is 10 minutes.

Configuring Windows File Sharing for a Workgroup

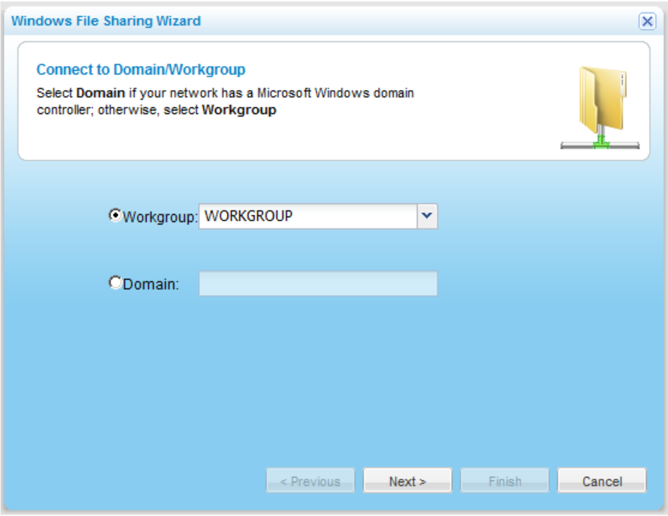
To configure Windows file sharing for a workgroup

1. In the **Configuration** tab's navigation pane, click **Share > Windows File Sharing**.

   The **Share > Windows File Sharing** page appears.

2. Click **Connect to Domain/Workgroup**.

The **Windows File Sharing Wizard** opens, displaying the **Connect to Domain/Workgroup** dialog box.



3 Choose **Workgroup**, then type the name of the workgroup.

Tip

You must assign this same workgroup name to all of the computers in the network.

Tip

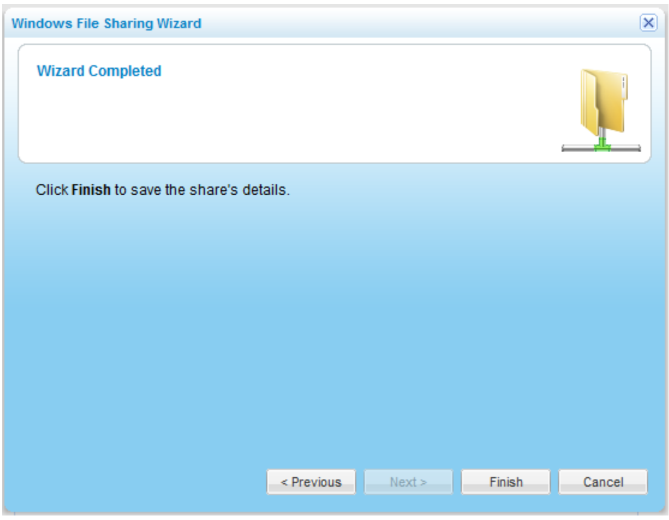
In most Windows versions, the default workgroup name is WORKGROUP.

In Windows XP Home edition, the default workgroup name is MSHOME.

The appliance automatically scans for available workgroups in the LAN. The results of these scans can be selected from the **Workgroup** drop-down list.

4 Click **Next**.

The **Wizard Completed** screen appears.



5 Click **Finish**.

Configuring Windows File Sharing for an Individual Active Directory Domain

To configure Windows file sharing for an individual Active Directory domain

1. In the **Configuration** tab's navigation pane, click **Share > Windows File Sharing**.

   The **Share > Windows File Sharing** page appears.

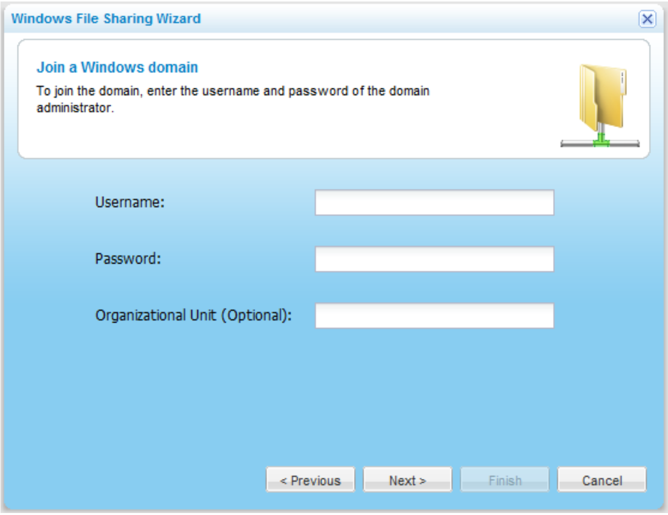
2. Click **Connect to Domain/Workgroup**.

   The **Windows File Sharing Wizard** opens, displaying the **Connect to Domain/Workgroup** dialog box.

3. Choose **Domain**, then type the domain name.

4. Click **Next**.

   The **Join a Windows domain** dialog box opens.



5. In the **Username** and **Password** fields, type the domain administrator's username and password.

6. (Optional) In the **Organizational Unit** field, type the name of the organizational unit within the Active Directory domain.

7. Click **Next**.

   The **Wizard Completed** screen appears.

8. Click **Finish**.

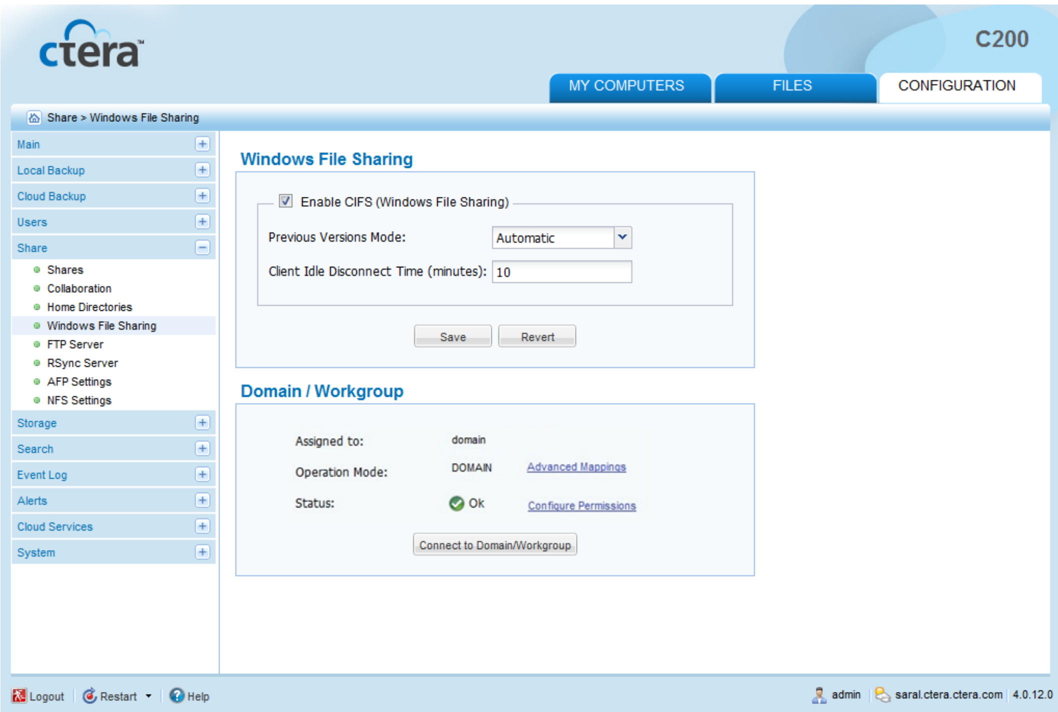
Configuring Windows File Sharing for an Active Directory Tree or Forest

To configure Windows file sharing for an Active Directory tree or forest

1. Configure Windows file sharing for one domain in the tree/forest.

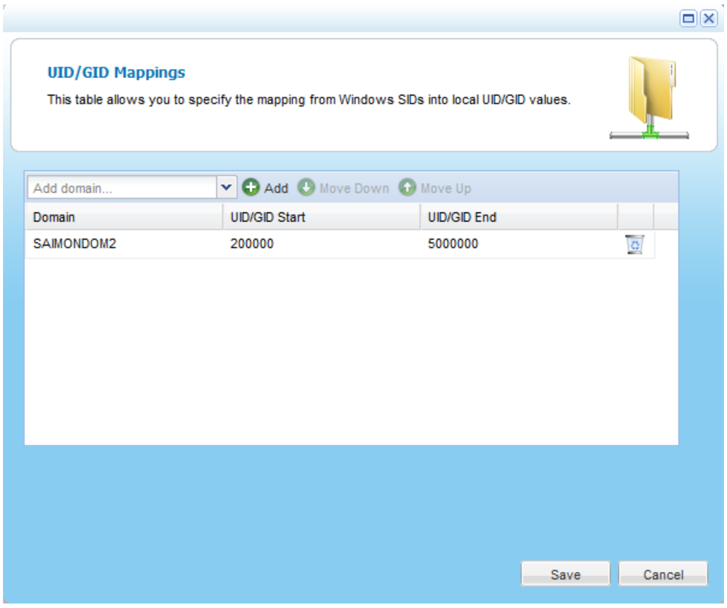
   See ***Configuring Windows File Sharing for an Individual Active Directory Domain*** (on page 117).

New links appear in the **Domain / Workgroup** area.



2 Click **Advanced Mappings**.

The **UID/GID Mapping** dialog box opens.



3 Add the other domains in the tree/forest, by doing the following for each one:

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

b Click **Add**.

The domain appears in the table.

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

4 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 appliance interface, (for example, when managing access rights to projects).

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

The domain is removed from the table.

6 Click **Save**.

Granting Administrative Permissions to Active Directory Users/Groups

By default, all Active Directory users and groups have no administrative permissions. If desired, you can grant them administrative permissions.

To grant administrative permissions to Active Directory users/groups in a domain environment

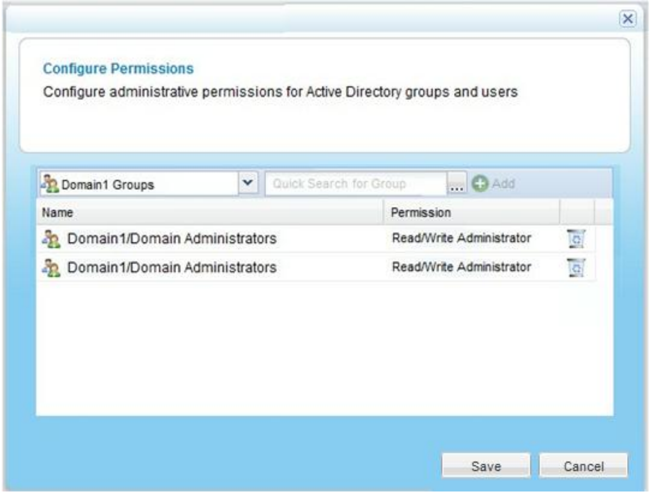
1 Configure Windows file sharing for one domain in the tree/forest.

See ***Configuring Windows File Sharing for an Individual Active Directory Domain*** (on page 117).

New links appear in the **Domain / Workgroup** area.

2 Click **Configure Permissions**.

The **Configure Permissions** dialog box opens.



3 Add each user and group who should have administrative permissions, by doing the following:

a In the drop-down list in the upper-left corner, select one of the following:

- **Domain** *domain* **Users**. Search the users belonging to the domain called *domain*.
- **Domain** *domain* **Groups**. Search the user groups belonging to the domain called *domain*.

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

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

c Select the desired user or group in the table.

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

d Click **Add**.

The user or group is added to the list of users and groups who should have administrative permissions.

4 In each user and user group's row, click in the **Permission** column, then select the desired access level from the drop-down list.

Options include **None**, **Read Only Administrator**, and **Read/Write Administrator**.

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

The user or group is removed from the table.

6 Click **Save**.

Configuring FTP Access

When FTP access is configured, users can access and download shared files from the CTERA FTP Server.

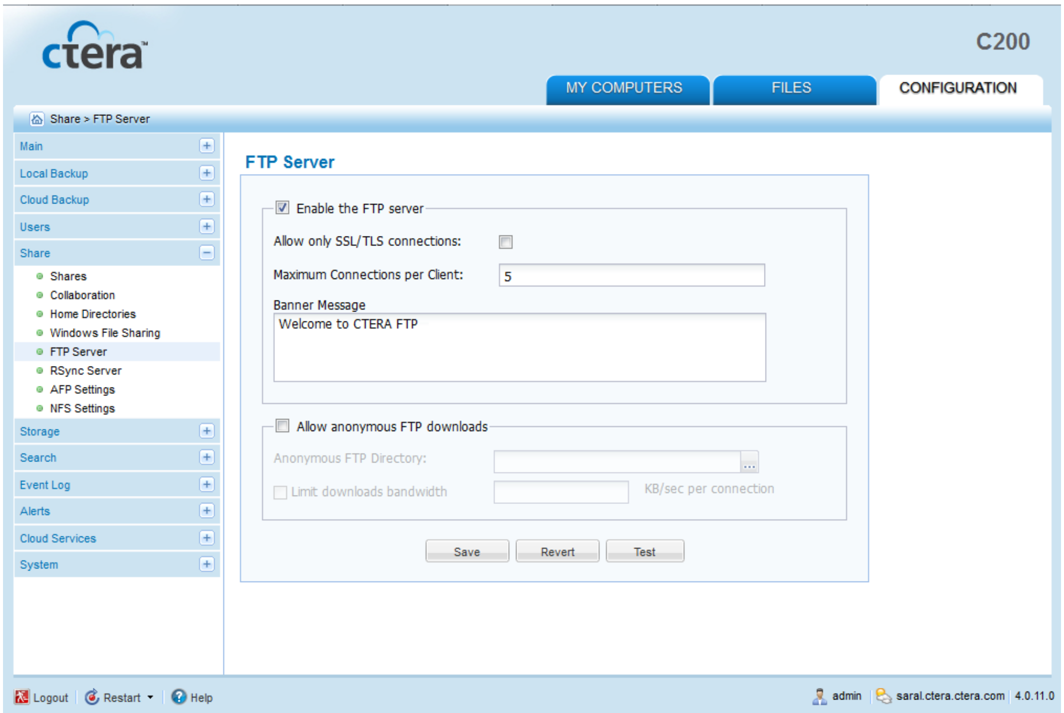
Tip

Users must authenticate to the CTERA FTP Server using the user name and password defined for them in the appliance, in order to access network shares. However, if desired, you can enable anonymous (unauthenticated) downloads from a specific directory.

To configure FTP access

1 In the **Configuration** tab's navigation pane, click **Share > FTP Server**.

The **Share > FTP Server** page appears.

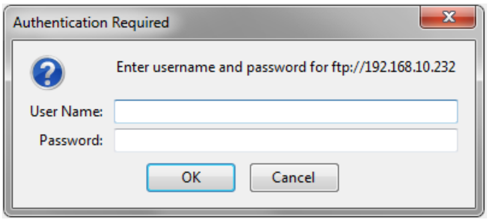


2 Complete the fields using the following table.

3 To test your settings, do the following:

a Click **Test**.

The **Authentication Required** dialog box appears.



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

c Click **OK**.

The FTP index appears.

Tip

FTP testing is not available if you chose to allow only SSL/TLS connections.

4 Click **Save**.

Table 27: FTP Server Fields

In this field...	Do this...
Enable the FTP server	Select this option to enable FTP access to your network shares on the CTERA FTP Server. Additional fields are enabled.
Allow only SSL/TLS connections	Select this option to allow only Secure Socket Layer (SSL) and Transport Layer Security (TLS) connections to your network shares on the FTP Server.
Maximum Connections per Client	Type the maximum number of concurrent FTP connections allowed per client. The default value is 5.
Banner Message	Type the message that should appear at the top of the page when accessing the network shares via FTP. The default value is "Welcome to CTERA FTP."
Allow anonymous FTP downloads	Select this option to allow users to access and download files from a specific directory on the FTP server, without authenticating. The **Anonymous FTP Directory** and **Limit downloads bandwidth** fields are enabled.
Anonymous FTP Directory	Specify the directory from which anonymous downloads should be allowed, by doing one of the following: - Click ..., and select the desired directory in the **Folder Browser**. - Type the path to the desired directory.
Limit downloads bandwidth	Select this option to restrict the bandwidth used for FTP downloads. Then type the maximum bandwidth to use for FTP downloads in kilobytes per second.

Configuring RSync Access

The appliance can act as an RSync Server, allowing users to efficiently synchronize files and folders on their RSync clients or CTERA appliances with the appliance. For information, see ***Synchronizing Files with the appliance RSync Server*** (see "***Synchronizing Files with the RSync Server***" on page 147).

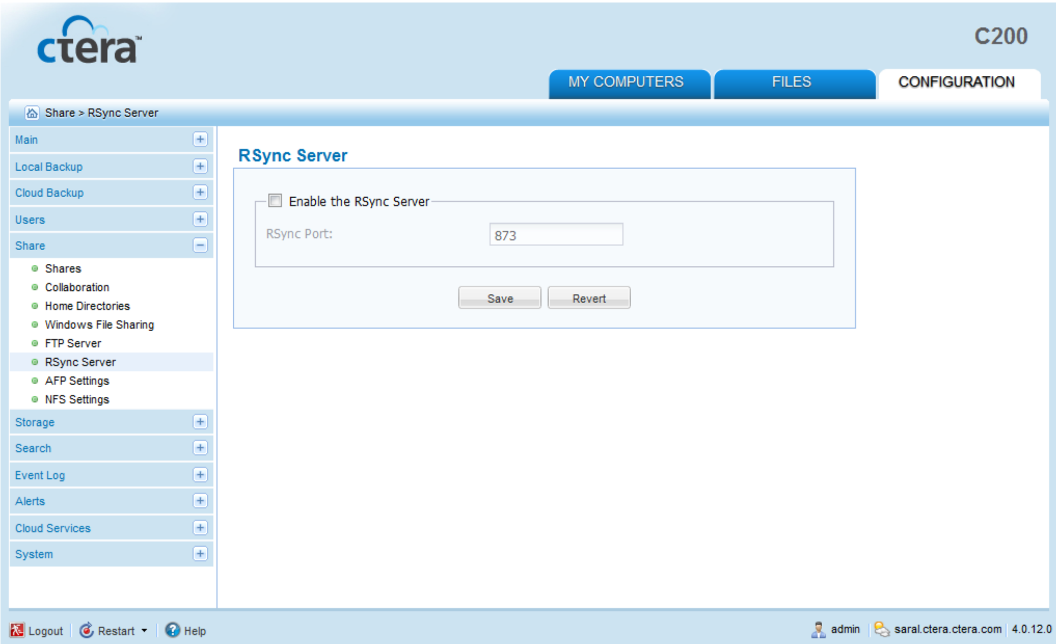
Tip

For operation over untrusted networks, it is recommended to use RSync with SSL/TLS encryption.

To configure RSync access to the appliance

1 In the **Configuration** tab's navigation pane, click **Share > RSync Server**.

The **Share > RSync Server** page appears.



2 To enable the RSync Server, select the **Enable the RSync Server** check box.

3 In the **RSync Port** field, type the port to use for RSync connections.

The default value is 873.

4 Click **Save**.

Configuring Apple File Sharing

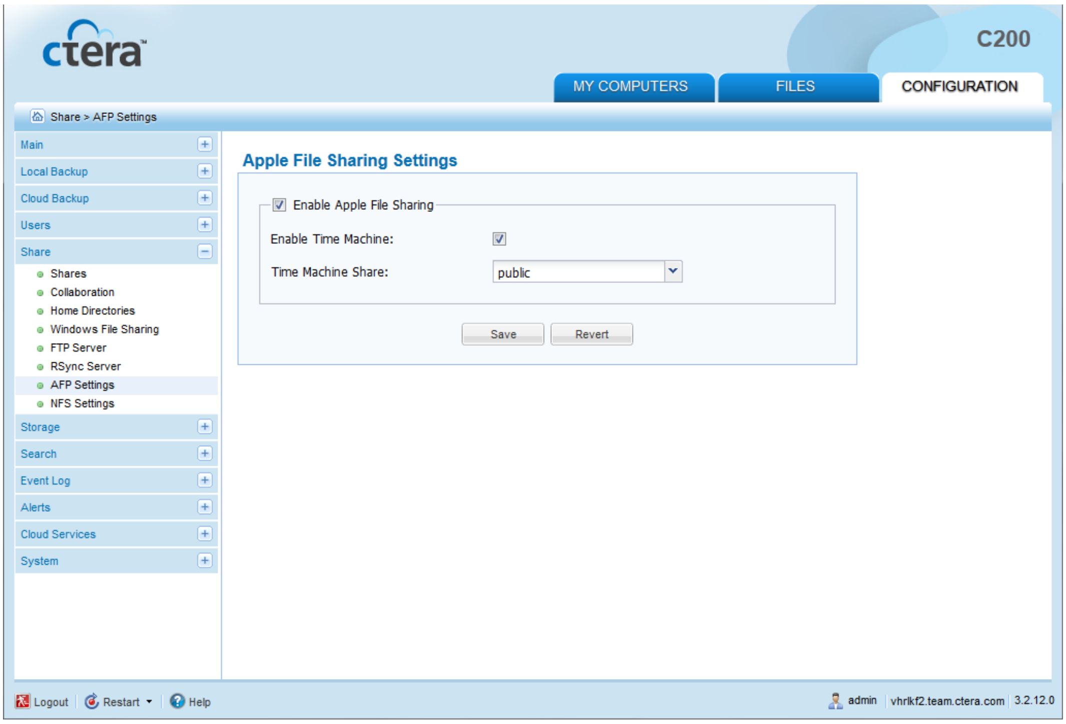
When Apple File Sharing is enabled, users with Mac OS X and Mac OS-based clients can access network shares on the appliance, using the Apple Filing Protocol (AFP). For information, see ***Viewing Network Shares Using Mac OS-X Finder*** (on page 147).

Furthermore, enabling Apple File Sharing allows the appliance to act as a repository for Apple Time Machine backup files.

To configure Apple File Sharing

1 In the **Configuration** tab's navigation pane, click **Share > AFP Settings**.

The **Share > AFP Settings** page appears.



2 Complete the fields using the following table.

3 Click **Save**.

Table 28: AFP Settings Fields

In this field...	Do this...
Enable Apple File Sharing	Select this option to enable Apple File Sharing. The **Enable Time Machine** field is enabled.
Enable Time Machine	Select this option to enable storing Apple Time Machine backup files on the appliance. The **Time Machine Share** field is enabled.
Time Machine Share	Select the network share on which Apple Time Machine backup files should be stored.

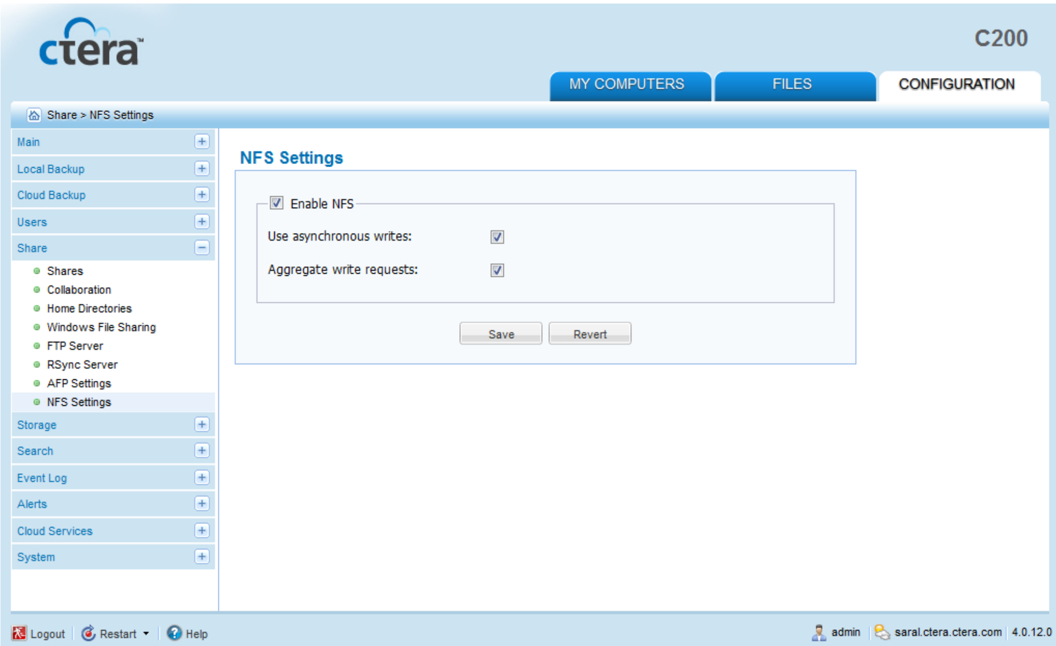
Configuring NFS Access

When Network File System (NFS) access is enabled, clients with certain IP addresses can access network shares on the appliance, as if the shares were located on the client's hard drive. For information, see ***Mounting Network Shares Using NFS*** (on page 148).

To configure NFS access

1. In the **Configuration** tab's navigation pane, click **Share > NFS Settings**.

   The **Share > NFS Settings** page appears.



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

Table 29: NFS Settings Fields

In this field...	Do this...
Enable NFS	Select this option to enable NFS.
Use asynchronous writes	Select this option to enable asynchronous writes. When a client attempts to write data to the appliance, the appliance sends the client an acknowledgment of the write request, *before* actually writing the data to the disk. This enables the client to post additional write requests to the appliance, while the appliance is still writing data from the first request to disk, thereby improving throughput.
Aggregate write requests	Select this option to specify that write requests should be aggregated and sent in a single batch, instead of one at a time. This improves throughput.

Using External Volume Autosharing

By default, the appliance automatically creates a network share with read/write access for all authenticated users, each time a new external drive is inserted. This is called *external volume autosharing*. If desired, you can disable autosharing or modify the access control list for automatically created shares.

Enabling/Disabling External Volume Autosharing

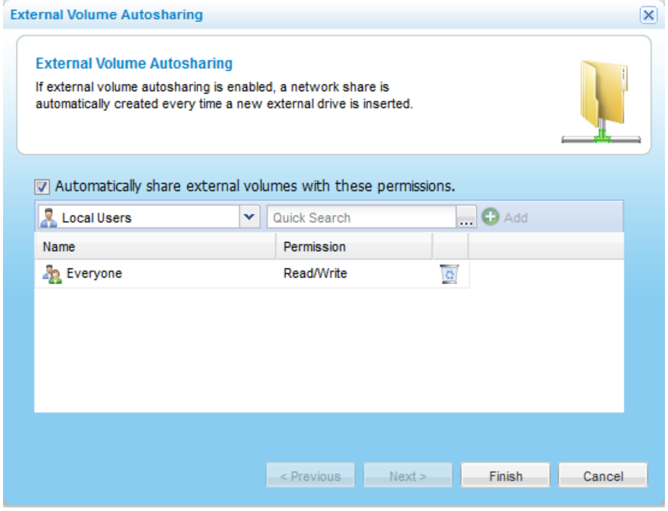
To enable autosharing

1. In the **Configuration** tab's navigation pane, click **Share > Shares**.

   The **Share > Shares** page appears.

2. Click **Autosharing**.

The **External Volume Autosharing** dialog box opens.



3 Select the **Automatically share external volumes with these permissions** check box.

You can now configure access lists. See ***Configuring the Autosharing Access Control List*** (on page 127).

4 Click **Finish**.

To disable autosharing

1 In the **Configuration** tab's navigation pane, click **Share > Shares**.

The **Share > Shares** page appears.

2 Click **Autosharing**.

The **External Volume Autosharing** dialog box opens.

3 Clear the **Automatically share external volumes with these permissions** check box.

4 Click **Finish**.

Configuring the Autosharing Access Control List

The autosharing access control list is used for all new shares created by external volume autosharing.

To configure the autosharing access control list

1 In the **Configuration** tab's navigation pane, click **Share > Shares**.

The **Share > Shares** page appears.

2 Click **Autosharing**.

The **External Volume Autosharing** dialog box opens.

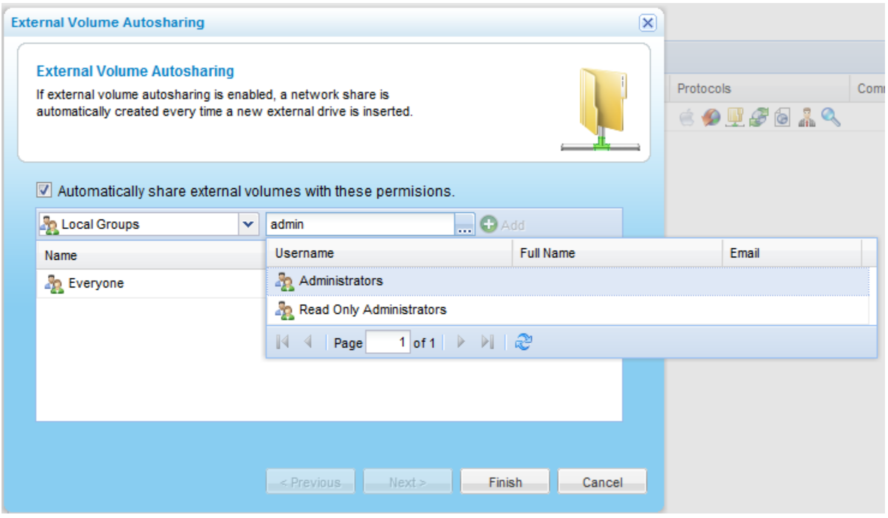
3 Add each user and user group who should have access to automatically created shares, by doing the following:

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

- **Local Users**. Search the users defined locally on the appliance.
- **Domain** *domain* **Users**. Search the users belonging to the domain called *domain*.
- **Local Groups**. Search the user groups defined locally on the appliance.
- **Domain** *domain* **Groups**. Search the user groups belonging to the domain called *domain*.

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

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



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

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

d Click **Add**.

The user or user group is added to the list of users and user groups who should have access to automatically created shares.

For information on editing users, see ***Adding and Editing Users*** (on page 252).

4 In each user and user group's row, click in the **Permission** column, then select the desired access level from the drop-down list.

Options include **None**, **Read Only**, and **Read/Write**.

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

The user or user group is removed from the table.

6 Click **Finish**.

Using Home Directories

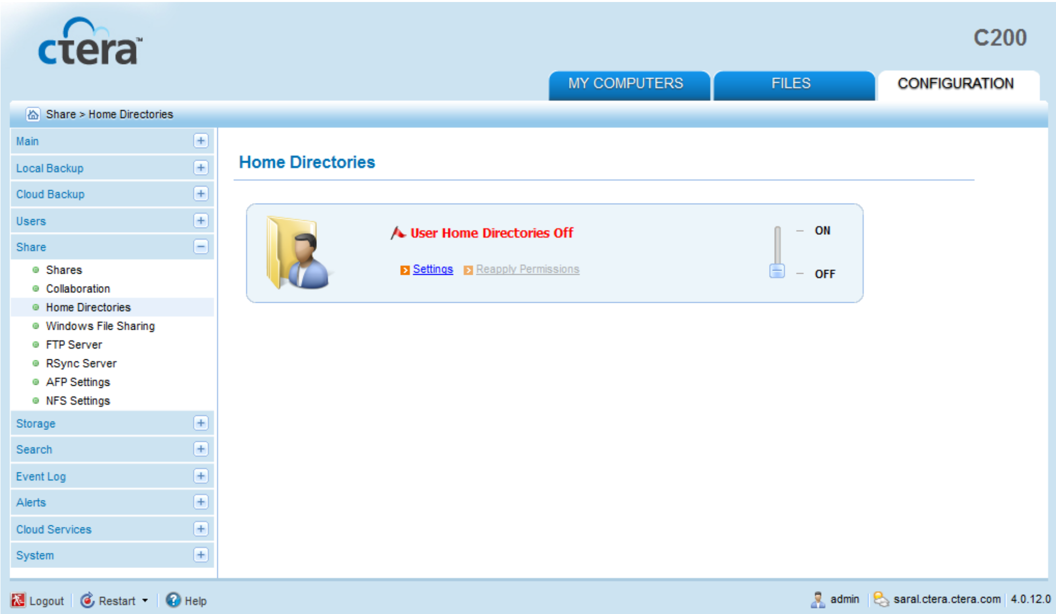
A *home directory* is a folder that contains files owned by a specific user. If desired, you can configure the appliance to dedicate one share to the storage of home directories. The appliance will automatically create a home directory for each user upon their first login.

Enabling/Disabling Home Directories

To enable home directories

1 In the **Configuration** tab's navigation pane, click **Share > Home Directories**.

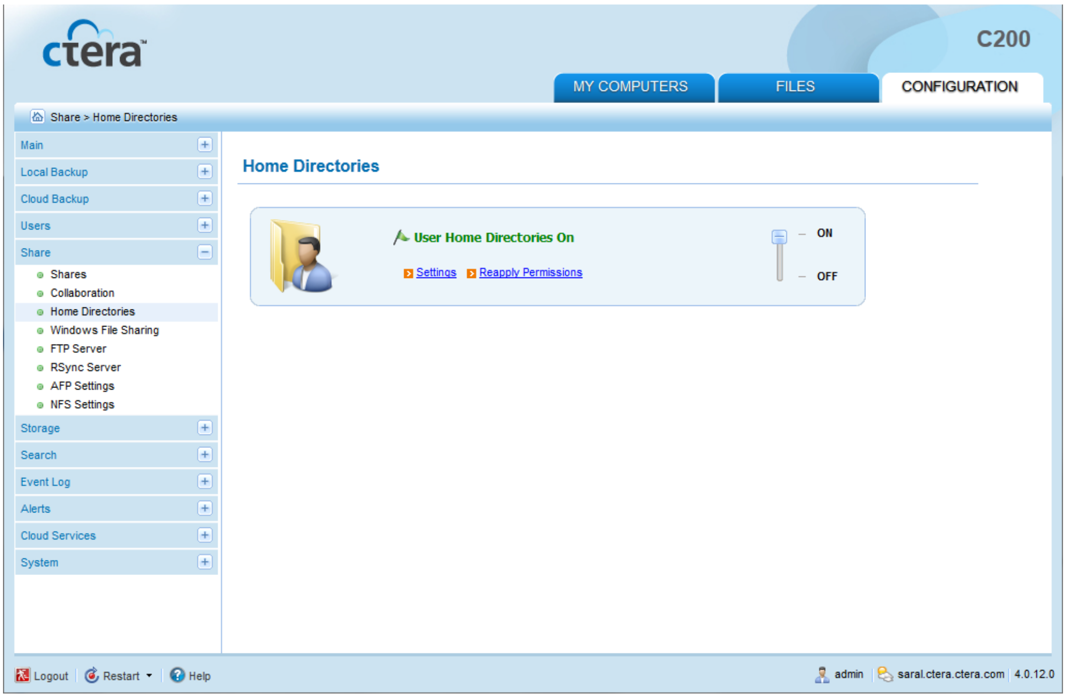
The **Share > Home Directories** page appears.



2 Slide the lever to the **ON** position.

Home directories are enabled, and you can now configure the desired settings. See ***Configuring Home Directory Settings*** (on page 130).

If this is the first time that home directories are enabled, the `users` share is created.



To disable home directories

1 In the **Configuration** tab's navigation pane, click **Share > Home Directories**.

The **Share > Home Directories** page appears.

2 Slide the lever to the **OFF** position.

Home directories are disabled.

Configuring Home Directory Settings

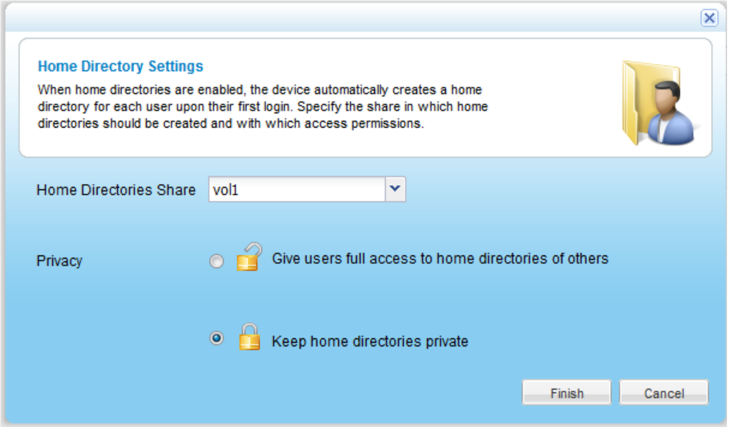
To configure home directory settings

1 In the **Configuration** tab's navigation pane, click **Share > Home Directories**.

The **Share > Home Directories** page appears.

2 Click **Settings**.

The **Home Directory Settings** dialog box opens.



3 In the **Home Directories Share** drop-down list, select the network share in which all home directories should be stored.

Tip

Upon enabling home directories, the `users` share was created for this purpose; however, any share can be used.

The selected share will be used exclusively for storing home directories. Users will not be permitted to store files directly under the share's root folder.

Do not select a share that already contains files or folders that are not home directories.

4 In the **Privacy** area, do one of the following:

- To grant all users access to the home directories of other users, click **Give users full access to home directories of others**.
- To allow only a home directory's owner access to it, click **Keep home directories private**.

5 Click **Finish**.

Resetting Home Directory Permissions

You can reset the home directory permissions to the default settings (i.e. all users will be granted access to the home directories of other users), and set all files to be owned by the home directory owner.

To reset home directory permissions

1 In the **Configuration** tab's navigation pane, click **Share > Home Directories**.

The **Share > Home Directories** page appears.

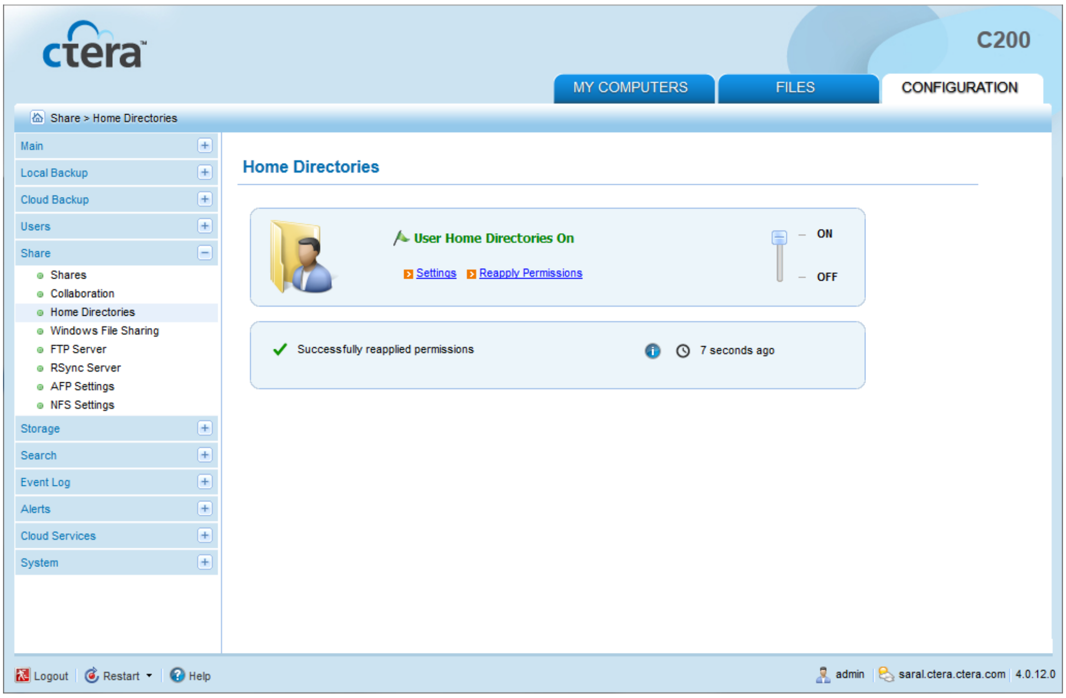
2 Click **Reapply Permissions**.

A confirmation message appears.

3 Click **Yes**.

Home directory permissions are reset.

For information on the results of the process, including the number of home directories processed and the number of errors, mouse-over the icon.



Using Guest Invitations

You can share files and folders stored on the appliance with other people, both inside and outside your network, by sending them a guest invitation for the desired files/folders.

Tip

In order for people outside your network to access your invitations, the remote access service must be enabled. See ***Enabling/Disabling Remote Access*** (on page 56).

The guest invitation includes one or more of the following:

- **An HTTP URL**

  The URL contains a special code, which when clicked allows the invitee to view or edit the files/folders from anywhere, using a Web-based file manager. This method is ideal for collaborating with users over the Internet, as well as users in your local network.

- **A Windows File Sharing path**

The path allows the invitee to view files or collaborate on a project transparently, using the standard Windows Explorer interface, by means of the Windows File Sharing (CIFS) protocol. This method is designed for collaborating with users in your local network, and not over the Internet.

Upon clicking the URL or path, invitation recipients are granted read-only or read-write access to the shared files/folders.

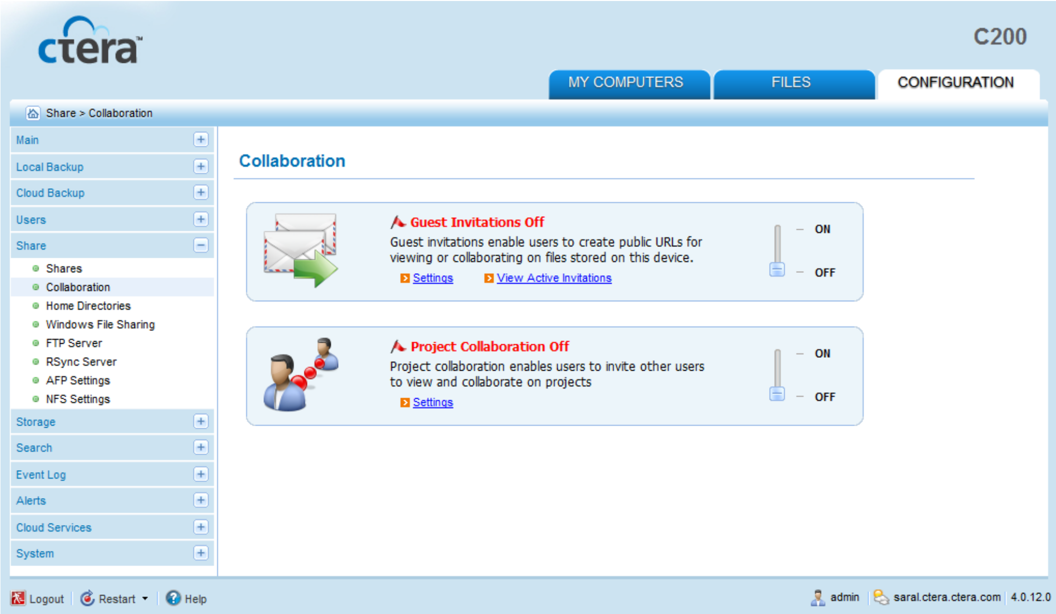
If desired, you can require invitation recipients to authenticate to the appliance using their username and password, before they can access the shared file/folders.

Enabling/Disabling Guest Invitations

To enable guest invitations

1 In the **Configuration** tab's navigation pane, click **Share > Collaboration**.

The **Share > Collaboration** page appears.



2 Slide the **Guest Invitations** lever to the **ON** position.

Guest invitations are enabled, and you can now configure the desired settings. See ***Configuring Guest Invitation Settings*** (on page 134).

To disable guest invitations

1 In the **Configuration** tab's navigation pane, click **Share > Collaboration**.

The **Share > Collaboration** page appears.

2 Slide the **Guest Invitations** lever to the **OFF** position.

Guest invitations are disabled.

Configuring Guest Invitation Settings

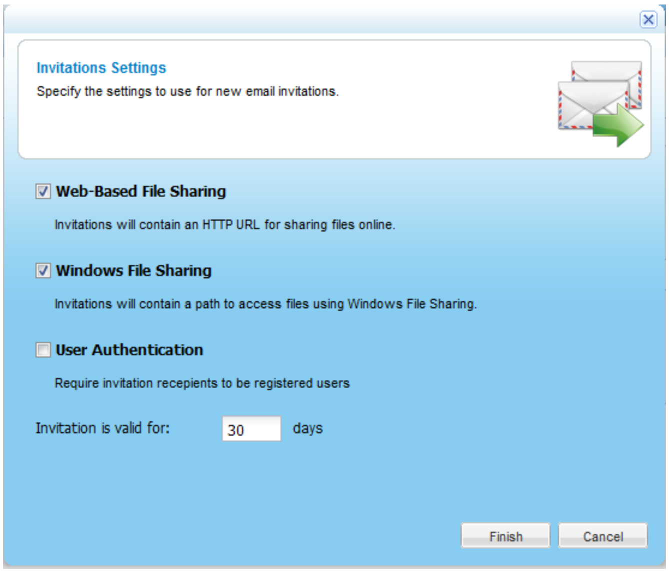
To configure guest invitation settings

1 In the **Configuration** tab's navigation pane, click **Share > Collaboration**.

The **Share > Collaboration** page appears.

2 In the **Guest Invitations** area, click **Settings**.

The **Invitations Settings** dialog box opens.



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

4 Click **Finish**.

Table 30: Invitations Settings Fields

In this field...	Do this...
Web-Based File Sharing	Select this option to specify that guest invitations should include a URL to access files online. This method is ideal for collaborating with users over the Internet (if the remote access service is enabled), as well as users in your local network.
Windows File Sharing	Select this option to specify that guest invitations should include a path to access files using Windows File Sharing. This method is designed for collaborating with users in your local network, and not over the Internet.
User Authentication	Select this option to specify that invitation recipients must successfully authenticate with a valid appliance username and password in order to view shared files and folders. By default, invitations can be viewed by anyone, both authenticated users and unauthenticated guests.
Invitation is valid for	Type the default number of days a guest invitation should remain valid. The user can override this value when creating an invitation. The default value is 30 days.

Sending Guest Invitations

To send a guest invitation for a file or folder

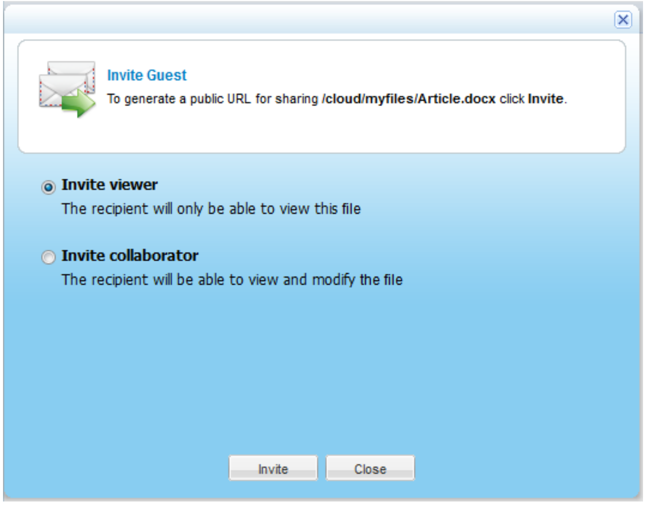
1. In the **Files** tab's **Show Shares** tree pane view, navigate to the desired file/folder.

   For information on changing the tree pane view, see ***Changing the Tree Pane View*** (on page 278).

   For information on navigating between folders, see ***Navigating Between Folders*** (on page 278).

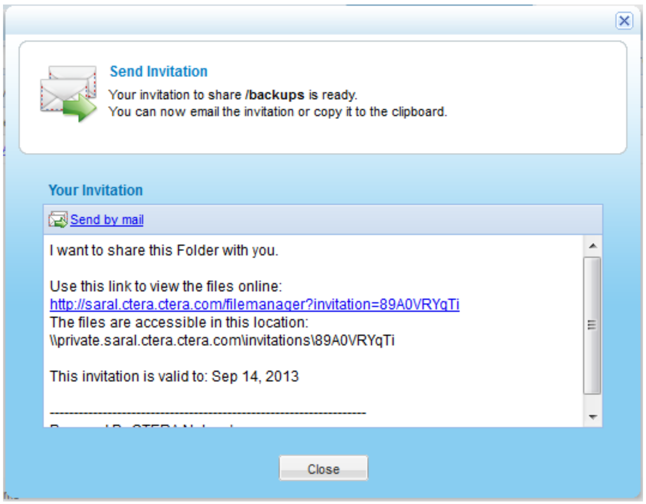
2. In the right pane, click on the file/folder.
3. Click **Invite Guest**.

   The **Invite Guest** dialog box opens.

4. Do one of the following:
   - To grant the invitation recipient read-only access to the file/folder, choose **Invite viewer**.
   - To grant the invitation recipient read-write access to the file/folder, choose **Invite collaborator**.
5. Click **Invite**.

The **Send Invitation** dialog box appears with the content of the guest invitation.



6 Click **Send by mail**.

Your email client opens a new message containing the invitation.

7 In the **To** field, fill in the email address of the person with whom you want to share the file/folder.

8 Click **Send**.

9 In the **Send Invitation** dialog box, click **Close**.

Viewing Active Guest Invitations

To view active guest invitations

1 Do one of the following:

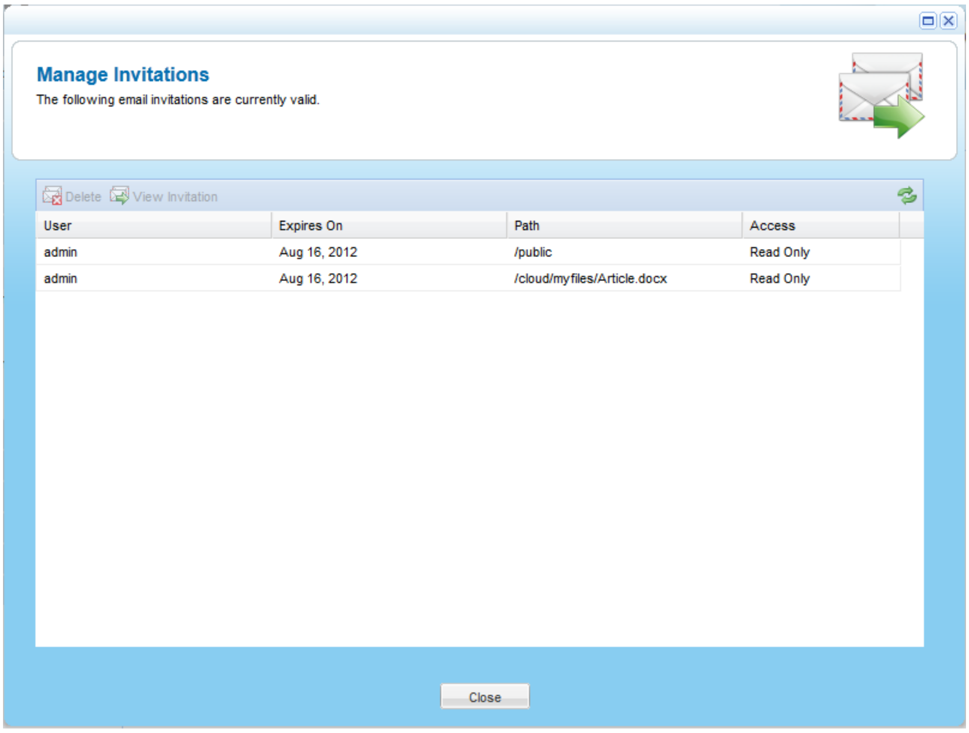
- To view all active guest invitations in the system:

  1 In the **Configuration** tab's navigation pane, click **Share > Collaboration**.

  The **Share > Collaboration** page appears.

  2 Click **View Active Invitations**.

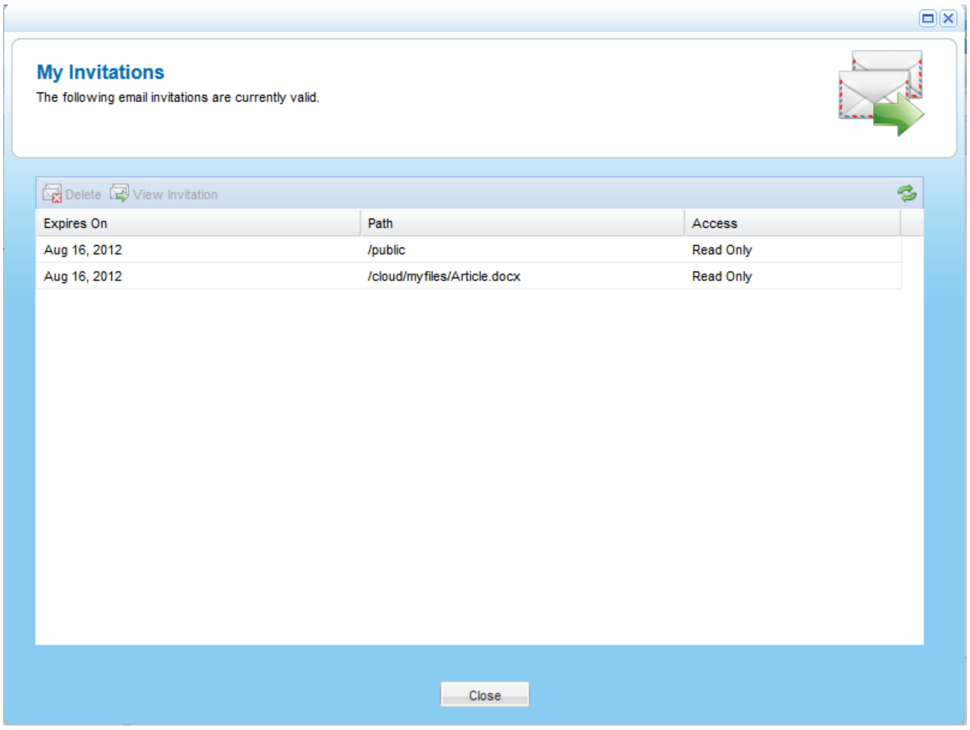
The **Manage Invitations** window opens.



- To view active guest invitations sent by you, in the **Files** tab's **Show Shares** tree pane view, click **My Invitations**.

  For information on changing the tree pane view, see ***Changing the Tree Pane View*** (on page 278).

  The **My Invitations** window opens.



For each invitation the information in the following table is displayed.

2 To view an individual invitation, select the desired invitation, and then click **View Invitation**.

The **Send Invitation** dialog box opens displaying the invitation.

3 Click **Close**.

Table 31: Active Guest Invitations Information

This field...	Displays...
User	The name of the user who sent the guest invitation. This field only appears when viewing all guest invitations in the system.
Expires On	The date on which the guest invitation expires.
Path	The path to the shared file/folder on the appliance.
Access	The type of access granted to the invitation recipient (**Read Only** or **Read/Write**).

Deleting Active Guest Invitations

If you delete an active guest invitation, the path and/or URL it contains can no longer be used to access files.

To delete active guest invitations

1 Do one of the following:

- To select a guest invitation for deletion, out of a list of all active invitations in the system:

  1 In the **Configuration** tab's navigation pane, click **Share > Collaboration**.

  The **Share > Collaboration** page appears.

  2 Click **View Active Invitations**.

  The **Manage Invitations** window opens.

- To select a guest invitation for deletion, out of a list of all active invitations sent by you, in the **Files** tab's **Show Shares** tree pane view, click **My Invitations**.

  For information on changing the tree pane view, see ***Changing the Tree Pane View*** (on page 278).

  The **My Invitations** window opens.

2 Select the desired invitation, and then click **Delete**.

A confirmation message appears.

3 Click **Yes**.

The guest invitation is deleted.

4 Click **Close**.

Collaborating on Projects

You can easily share files and folders with fellow workers, by defining *collaboration projects*.

When project collaboration is enabled, you can create a project and invite co-workers to join the project as *project members*. Project members receive an email notification inviting them to collaborate on the project. They can then view files in the project and/or add files and folders to the project, depending on their permissions.

Enabling/Disabling Project Collaboration

To enable project collaboration

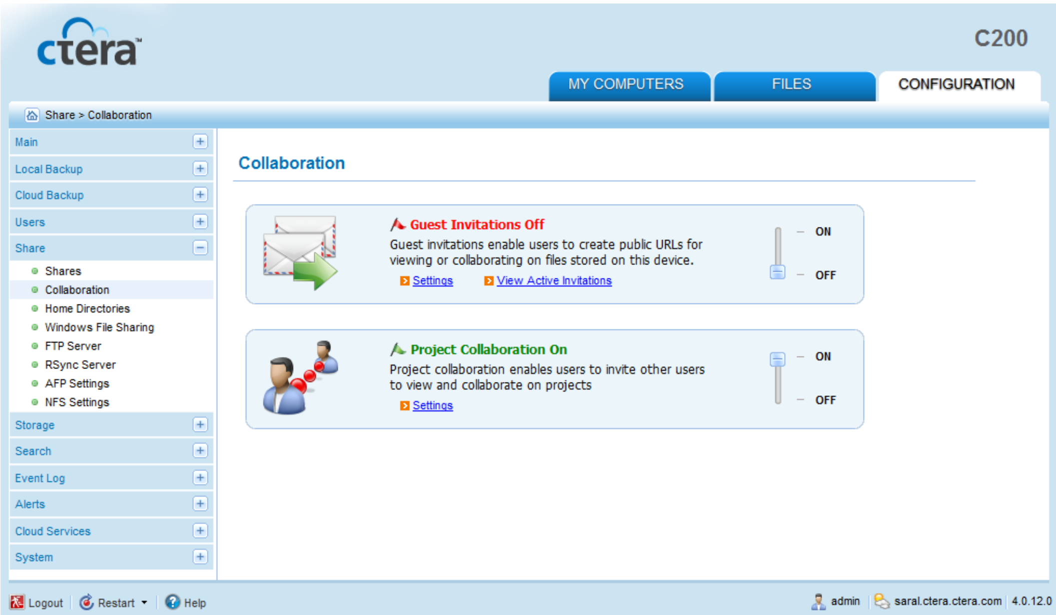
1 In the **Configuration** tab's navigation pane, click **Share > Collaboration**.

The **Share > Collaboration** page appears.

2 Slide the **Project Collaboration** lever to the **ON** position.

Project collaboration is enabled, and you can now configure the desired settings. See ***Configuring Project Collaboration Settings*** (on page 141).

If this is the first time that project collaboration is enabled, the `projects` share is created.



To disable project collaboration

1 In the **Configuration** tab's navigation pane, click **Share > Collaboration**.

The **Share > Collaboration** page appears.

2 Slide the **Project Collaboration** lever to the **OFF** position.

Project collaboration is disabled.

Configuring Project Collaboration Settings

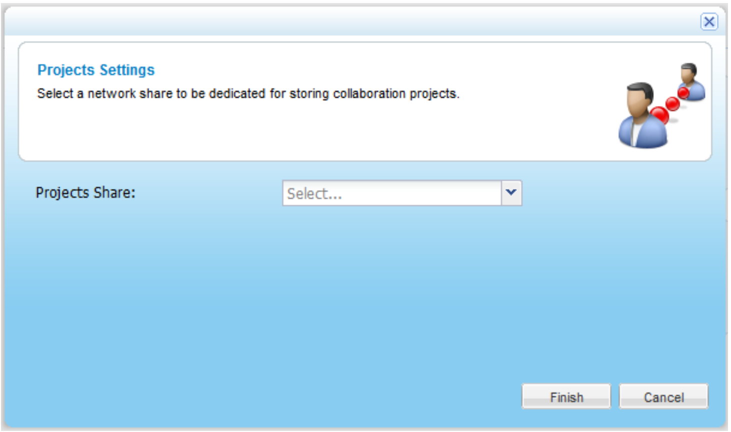
To configure project collaboration settings

1 In the **Configuration** tab's navigation pane, click **Share > Collaboration**.

The **Share > Collaboration** page appears.

In the **Project Collaboration** area, click **Settings**.

The **Projects Settings** dialog box opens.



2 In the **Projects Share** drop-down list, select a share that should be dedicated to the storage of collaboration projects.

Tip

Upon enabling project collaboration, the projects share was created for this purpose; however, any share can be used.

3 Click **Finish**.

Creating Projects

To create a collaboration project

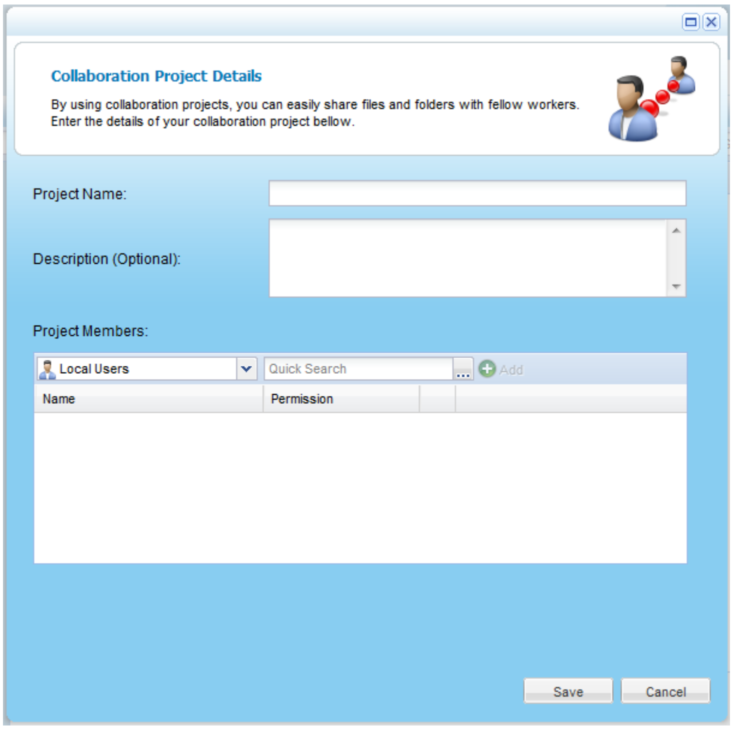
1 In the **Files** tab's **Show Shares** tree pane view, navigate to the project collaboration share you specified in ***Configuring Project Collaboration Settings*** (on page 141).

For information on changing the tree pane view, see ***Changing the Tree Pane View*** (on page 278).

For information on navigating between folders, see ***Navigating Between Folders*** (on page 278).

2 Click **New Project**.

The **Collaboration Project Details** dialog box opens.



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

4 (Optional) In the **Description** field, type a description of the project.

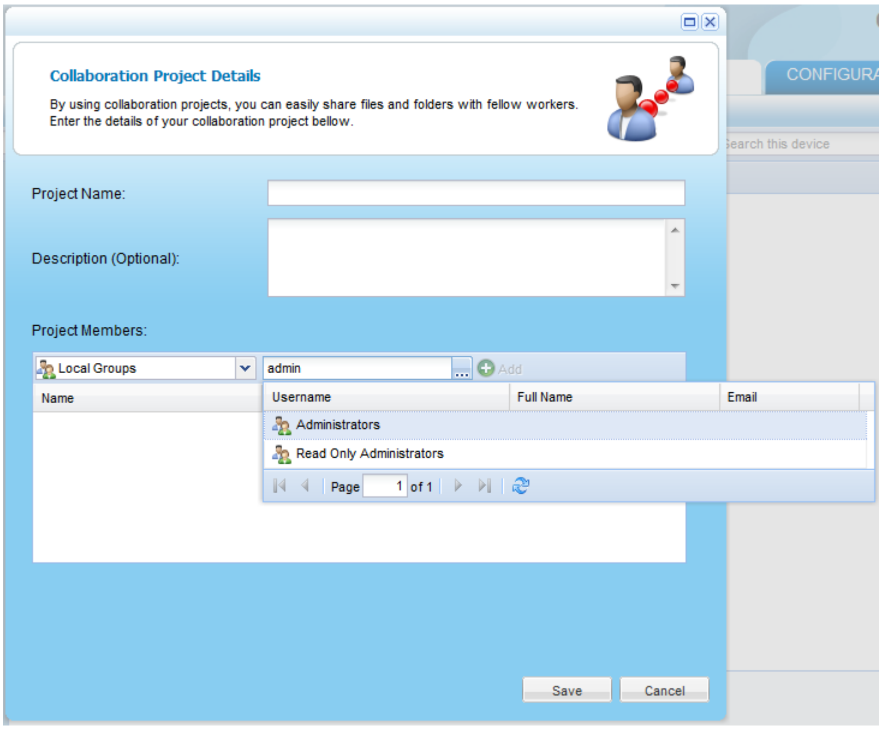
5 To add a project member, do the following:

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

- **Local Users**. Search the users defined locally on the appliance.
- **Domain** *domain* **Users**. Search the users belonging to the domain called *domain*.
- **Local Groups**. Search the user groups defined locally on the appliance.
- **Domain** *domain* **Groups**. Search the user groups belonging to the domain called *domain*.

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

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



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

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

d Click **Add**.

The user or user group appears in the **Project Member** list.

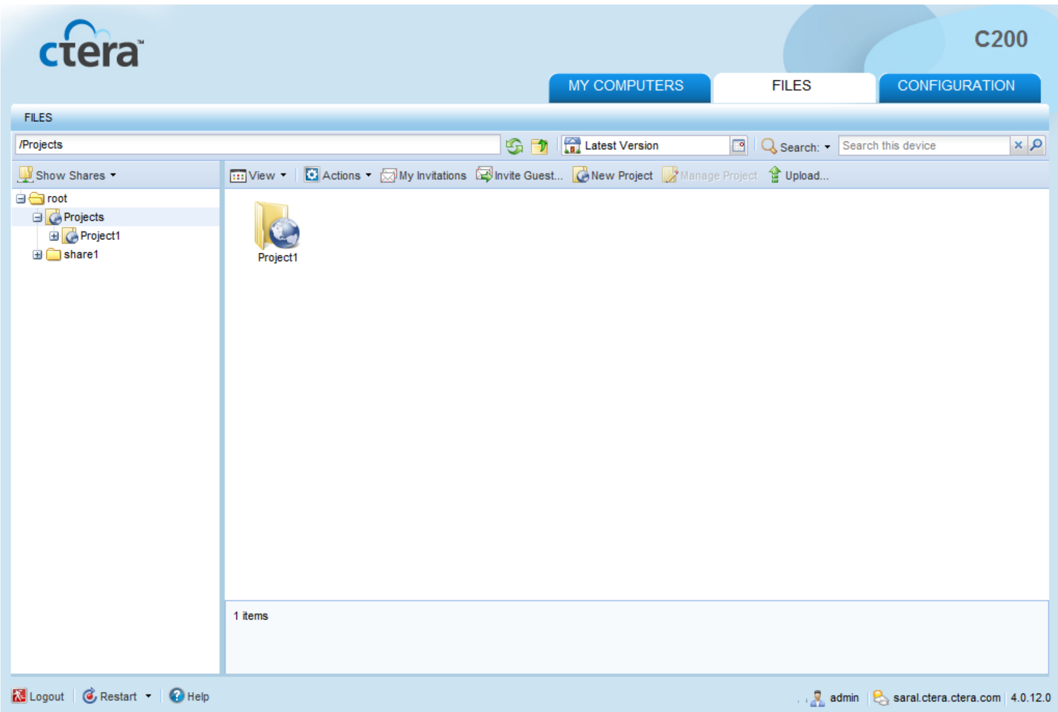
6 In the project member's row, click the **Permission** field, and do one of the following:

- To specify that the member should be able to add, edit, and delete files and folders in this project, select **Read/Write**.
- To specify that the member should only be able to view files and folders in this project, select **Read Only**.
- To specify that the member should bot be able to view files and folders in this project, select **None**.

7 To delete a project member, click in the desired project member's row.

8 Click **Save**.

The project is added to the project share.



If the mail server is set up, and email addresses are defined for the users you added as project members, the appliance will send email notifications to the new project members, inviting them to collaborate on the project.

For information on configuring mail server settings, see ***Configuring Mail Server Settings*** (on page 314). For information on editing users, see ***Adding and Editing Users*** (on page 252).

Editing Projects

To edit a collaboration project

1. In the **Files** tab's **Show Shares** tree pane view, navigate to the desired project.

   For information on changing the tree pane view, see ***Changing the Tree Pane View*** (on page 278).

   For information on navigating between folders, see ***Navigating Between Folders*** (on page 278).

2. Select the project.
3. Click **Manage Project**.

   The **Collaboration Project Details** dialog box opens.

4. In the **Project Name** field, type a name for the project.
5. (Optional) In the **Description** field, type a description of the project.

6 To add a project member, do the following:

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

- **Local Users**. Search the users defined locally on the appliance.
- **Domain** *domain* **Users**. Search the users belonging to the domain called *domain*.
- **Local Groups**. Search the user groups defined locally on the appliance.
- **Domain** *domain* **Groups**. Search the user groups belonging to the domain called *domain*.

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

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

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

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

d Click **Add**.

The user or user group appears in the **Project Member** list.

7 In the project member's row, click the **Permission** field, and do one of the following:

- To specify that the member should be able to add, edit, and delete files and folders in this project, select **Read/Write**.
- To specify that the member should only be able to view files and folders in this project, select **Read Only**.
- To specify that the member should bot be able to view files and folders in this project, select **None**.

8 To delete a project member, click in the desired project member's row.

9 Click **Save**.

If the mail server is set up, and email addresses are defined for the users you added as project members, the appliance will send email notifications to the new project members, inviting them to collaborate on the project.

For information on configuring mail server settings, see ***Configuring Mail Server Settings*** (on page 314). For information on editing users, see ***Adding and Editing Users*** (on page 252).

Deleting Projects

To delete a collaboration project

1 In the **Files** tab's **Show Shares** tree pane view, navigate to the desired project.

For information on changing the tree pane view, see ***Changing the Tree Pane View*** (on page 278).

For information on navigating between folders, see ***Navigating Between Folders*** (on page 278).

2 Select the project.

3 Click **Actions**, and then click **Delete**.

A confirmation message appears.

4 Click **Yes**.

The project is deleted.

Accessing Network Shares

Viewing Network Shares Using Windows File Sharing

Use this procedure to view network shares, when Windows File Sharing is configured. For information, see ***Configuring Windows File Sharing*** (on page 114).

To view a network share using Windows File Sharing

1 On a computer connected to the same switch as the appliance, view the network neighborhood, by doing one of the following:

- In Microsoft Windows 7®, click **Start > Computer**, then click **Network** in the left pane.
- In Microsoft Windows Vista®, click **Start > Network**.
- In Microsoft Windows XP®, click **Start > My Network Places**, then click **View workgroup computers**.

2 Double-click the appliance icon.

In Windows 7 and Vista, the icon is 

; in Windows XP, it is 

.

A list of network shares appears.

Tip

When accessing a network share, if your user name and password on the computer are identical to a user name and password on the appliance, then the computer will automatically log in to the share using that user name and password. You will not be prompted to authenticate. In all other cases, a pop-up window will appear, and you must authenticate using a valid user name and password.

Synchronizing Files with the RSync Server

Use this procedure to synchronize files between the appliance and a local folder, when RSync Access is configured. For information, see ***Configuring RSync Access*** (on page 123).

To synchronize files with the RSync Server

- Run the following command:

  rsync --recursive *userName***@***deviceIP* **:/***shareName localFolder*

  Where:

  - `userName` is the username.
  - `deviceIP` is the appliance IP address.
  - `shareName` is the name of the network share on the appliance.
  - `localFolder` is the name of the local folder.

  For example, if the username is user1, the appliance IP address is 10.1.1.1, the name of the network share is share9, and the local folder is `/var/mnt/share9`, the relevant command would be:

  ```
  rsync --recursive user1@10.1.1.1 :/share9 /var/mnt/share9
  ```

Viewing Network Shares Using Mac OS-X Finder

Use this procedure to view network shares, when Apple File Sharing is configured. For information, see ***Configuring Apple File Sharing*** (on page 124).

To view a network share using Mac OS-X Finder

1. Open Mac OS-X Finder.
2. In the left pane, in the **SHARED** area, click on the name of your appliance CTERA C200.

   A list of network shares appears in the right pane.
3. If the share requires authentication, in the top-right corner of the window, click **Connect As**, then enter your username and password.

Mounting Network Shares Using NFS

Use this procedure to access network shares from a Linux/UNIX computer, when NFS access is configured. For information, see ***Configuring NFS Access*** (on page 125).

To mount a network share using NFS

- Run the following command:

  mount *deviceIP***:***mountPath localFolder*

  Where:

  - deviceIP is the appliance's IP address.
  - mountPath is the network share's mount path.

    Tip

    To view a network share's mount path, in the **Share > Shares** page, click the name of the desired network share. The **Network Share Wizard**'s **NFS (UNIX File Sharing)** dialog box displays the network share's mount path in title area.

  - localFolder is the name of the local folder.

  For example, if the appliance IP address is 10.1.1.1, the mount path is /share/share9, and you want to mount this network share on the local folder /var/mnt/share9, the relevant command would be:

```
mount 10.1.1.1:/share/share9 /var/mnt/share9
```

Accessing the Administrative Share

Administrators can access a hidden administrative share called "/volumes", using Windows File Sharing. For information, see ***Configuring Windows File Sharing*** (on page 114). Alternatively, they can access this share via the appliance Web interface's **File Manager**.

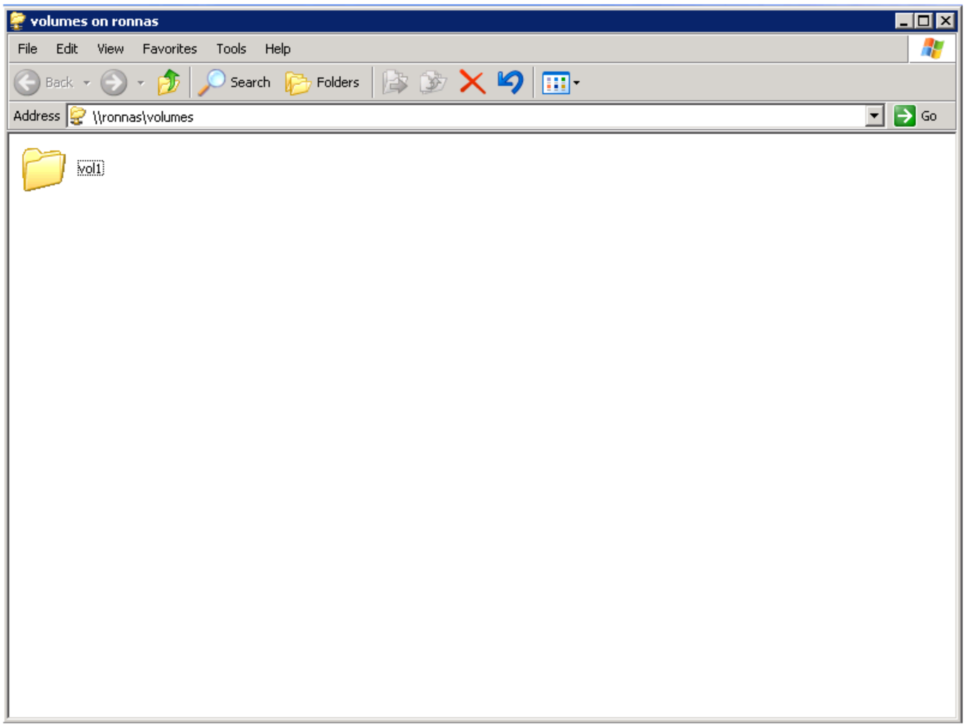
The administrative share allows direct access to the files on each of the appliance's volume.

To access the administrative share via Windows File Sharing

- On a computer connected to the same switch as the appliance, browse to \\<devicename>\volumes\, where <devicename> is the name of your appliance.

  For information on viewing your appliance's name, see ***Viewing the Appliance Details*** (on page 320).

The administrative share appears.



Tip

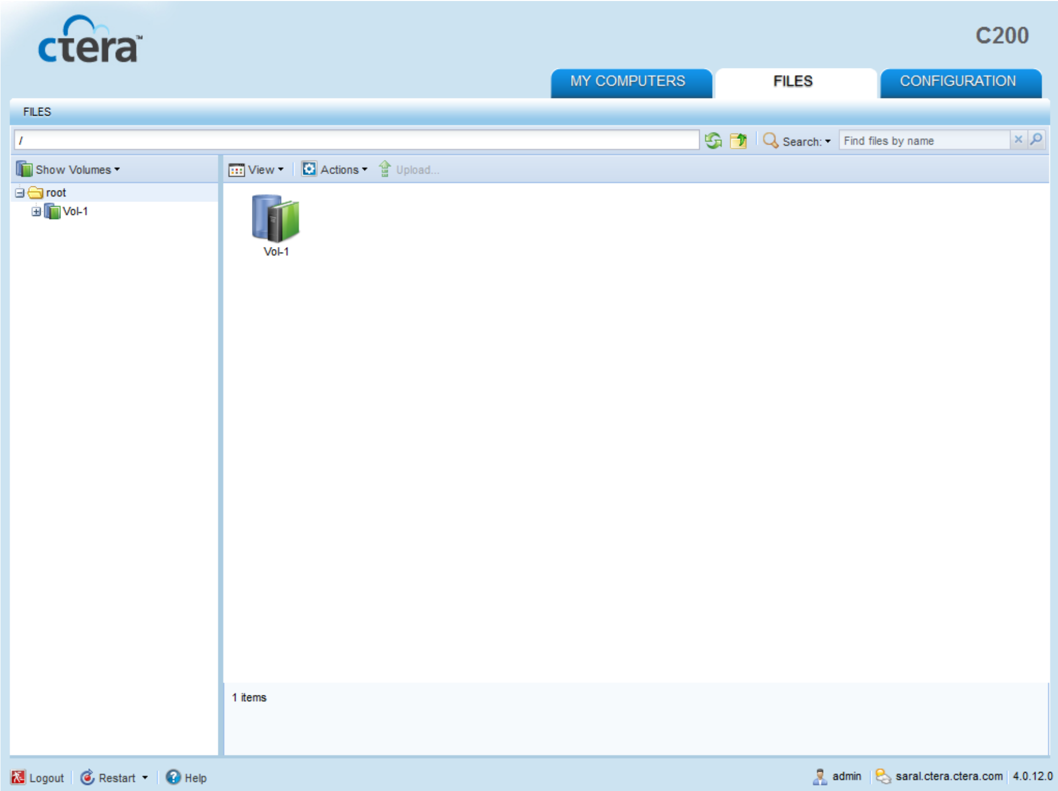
If your user name and password on the computer are identical to a user name and password on the appliance, then the computer will automatically log in to the share using that user name and password. You will not be prompted to authenticate. In all other cases, a pop-up window will appear, and you must authenticate using a valid user name and password.

To access the administrative share via the File Manager

- In the File Manager, change to the Volumes view.

  See ***Changing the Tree Pane View*** (on page 278).

  The administrative share opens displaying all volumes.



10

Using Cloud Backup

This chapter explains how to back up your files to cloud storage.

In This Chapter

About the CTERA Cloud Backup Service

Why Should I Use Cloud Backup?

Backing up your important files enables you to protect them against future data loss. If the original data becomes corrupted or is accidentally deleted, or if your hard drive fails, you can restore the lost data from the backup. Traditional backup methods include zip drives, CD/DVDs, external hard drives, tape units, and more. All of these methods are effective, though not necessarily efficient or convenient.

CTERA appliance provides cloud backup, in which your files are automatically backed up to the cloud and stored remotely. Cloud backup offers numerous advantages over traditional backup methods:

- **Simplicity**

Traditional backup methods require user intervention, complicating the backup process. You may have to insert CDs into drives, change tapes, or even manually initiate the backup.

In contrast, cloud backup requires only a simple, one-time configuration. Once configured, cloud backup runs automatically according to your desired schedule, without any need for user intervention.

Time Efficiency

Due to cloud backup's simplicity of use, there is no need to waste time or effort backing up data. Your valuable time can be spent on other matters.

Security

In cloud backup, your data is automatically encrypted and fingerprinted. For even stronger security, you can configure a secret passphrase for accessing the backed up data.

Versioning

When using traditional backup, users often choose to maintain only the most recent version of their files, due to storage space restrictions. Cloud backup preserves multiple versions of your data, enabling you to restore the version of your choice.

Storage Locations

With traditional backup, your backed up data is usually stored in a single location (for example, in a stack of CDs in your office. This means that if a natural disaster strikes at that location (for example, a fire in your office), you data, along with all of the backups, will be lost. Cloud backup ensures that your data is stored in multiple locations.

Restore Options

When using traditional backup, you must have access to the backup medium, in order to restore your data. In contrast, cloud backup offers multiple restore options, including restoring your data from anywhere by downloading it from the cloud backup site. For additional restore options, see ***What Restore Options Are Available?*** (on page 154).

Appliance Configuration Backup

When cloud backup runs, your appliance's configuration is automatically be backed up to the CTERA Portal, from where it can be easily downloaded and used to restore your appliance settings, as needed.

How Does the Cloud Backup Service Work?

The first time cloud backup runs, the appliance performs a full cloud backup for the selected folders. This may take a long time, depending on the size of your data set. Subsequent backups are performed incrementally and normally take much less time than the initial backup. Only data that has actually changed is uploaded.

CTERA uses state-of-the-art data compression and data deduplication techniques, to ensure the backup happens as quickly and efficiently as possible.

Is My Data Secure?

In addition to using 128-bit SSL (Secure Sockets Layer) connections, the same security mechanism used by banks, all your data is encrypted using 256-bit AES encryption and fingerprinted by 160 bit SHA-1 digest, to ensure your data is protected against eavesdroppers.

For even stronger security, you can use a secret passphrase. If you use a secret passphrase, your data will not be readable by anyone without knowledge of your secret passphrase (not even by CTERA).

How Can I Control Which Files Will Be Backed Up?

The appliance offers the following options for controlling the scope of backup operations:

- **Selecting entire folders for backup**

  When you select an entire folder for backup, all of the folders in it are automatically selected for backup.

- **Selecting specific file types for inclusion in or exclusion from backup, by using backup sets**

  A *backup set* represents a group of files of a certain type and/or located in certain folders, which should either be included in or excluded from backup operations. For more information on backup sets, see ***Working with Backup Sets*** (on page 156).

These options can be used in conjunction.

When all options are used, the appliance determines the final set of files to include in a backup operation, by performing the following checks for each file:

1. Checks whether the file is contained in an excluded set. If so, the file is skipped.
2. Checks whether the file is contained in an included set. If so, the file is backed up.
3. Checks whether the file is contained in a folder that was selected for backup in the folder selection page. If so, the file is backed up.

What Restore Options Are Available?

The appliance enables you to restore files from backup in the following ways:

- By restoring some or all files and folders to a previous version via the appliance Web interface
- By restoring individual files or folders using Microsoft Windows Shadow Copy
- By restoring individual files or folders using the appliance Virtual Cloud Drive
- By downloading files from your CTERA Portal account

Workflow

In order to back up your files using CTERA's Cloud Backup service, you must perform the following steps:

1. Connect to cloud services.

   See ***Connecting the Appliance to Your CTERA Portal Account*** (on page 50).

2. Do one or more of the following:

   - To choose specific files and folders to include in the backup, select the desired files and folders.

     See ***Selecting Files and Folders for Cloud Backup*** (on page 155).

   - To choose specific file types to include in or exclude from backup operations, define and enable backup sets.

     See ***Working with Backup Sets*** (on page 156).

3. Do one or more of the following:

   - Schedule automatic backup of the selected folders.

     See ***Scheduling Automatic Cloud Backup*** (on page 166).

     The files will be backed up according to the configured schedule.

   - Perform a manual backup of the selected folders.

     See ***Manually Starting Cloud Backup*** (on page 168).

     The files will be backed up immediately.

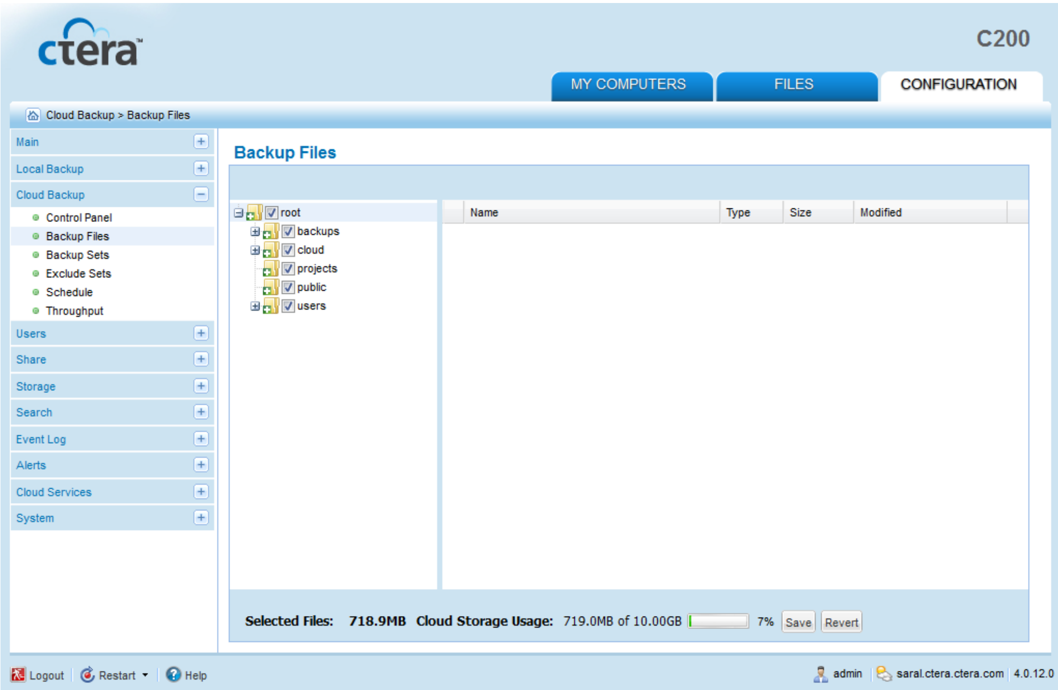
Selecting Files and Folders for Cloud Backup

By default, all folders and files are selected for cloud backup. If desired, you can modify the selection.

To select files and folders for cloud backup

1 In the **Configuration** tab's navigation pane, click **Cloud Backup > Backup Files**.

The **Cloud Backup > Backup Files** page appears.



2 Expand the tree nodes to reveal the folders.

For an explanation of the icons and check boxes next to each folder, see ***Folder Icons*** (page 156).

The folder contents appear in the right pane.

3 Select the check boxes next to the files and folders you want to back up.

4 Click **Save**.

At the bottom of the workspace, the **Selected Files** field indicates the size of the files selected for backup. The **Cloud Storage Usage** field indicates the amount of used space in your account after the next cloud backup operation (including backups from any other CTERA appliances included in your account).

For example, let's say your account includes two appliances, and each appliance will back up 100 MB worth of files in the next cloud backup operation, for a total of 200 MB. Your account already has 350 MB worth of files stored online. In this case, the **Cloud Storage Usage** field will display "550MB".

Table 32: Folder Icons

This icon...	Indicates...
	Existing files in this folder are selected for backup. New files and folders in this folder will be backed up.
	This folder and all of its sub-folders are selected for backup. Note that the check box has a white background.
	Some (but not all) of the folder's sub-folders are selected for backup. Note that the check box has a gray background.
	This folder and all of its sub-folders will not be backed up.

Working with Backup Sets

A *backup set* represents a group of files with certain file extensions and/or located in certain folders. For example, a set called "My Music" may include all files with the extensions *.wav and *.mp3 that are located in the folder **My Documents > Music**.

There are two types of backup sets:

- **Included sets**. Files that should be included in each backup
- **Excluded sets**. Files that should be excluded from each backup

You can use backup sets to fully customize backup operations. For example, if you did not select the **My Documents** folder for backup, but you want to back up all of the PDF files in this folder, you would define an *included set* that includes all files that are located in the **My Documents** folder and have the file extension *.pdf. Conversely, if you selected the **My Documents** folder for backup, but you do *not* want to back up PDF files in this folder, you would define an *excluded set* that includes all files that are located in the **My Documents** folder and have the file extension *.pdf.

Tip

For information on the order in which the appliance processes included sets, excluded sets, and selected folders, see ***How Can I Control the Scope of Backup Operations?*** (see "***How Can I Control Which Files Will Be Backed Up?***" on page 153).

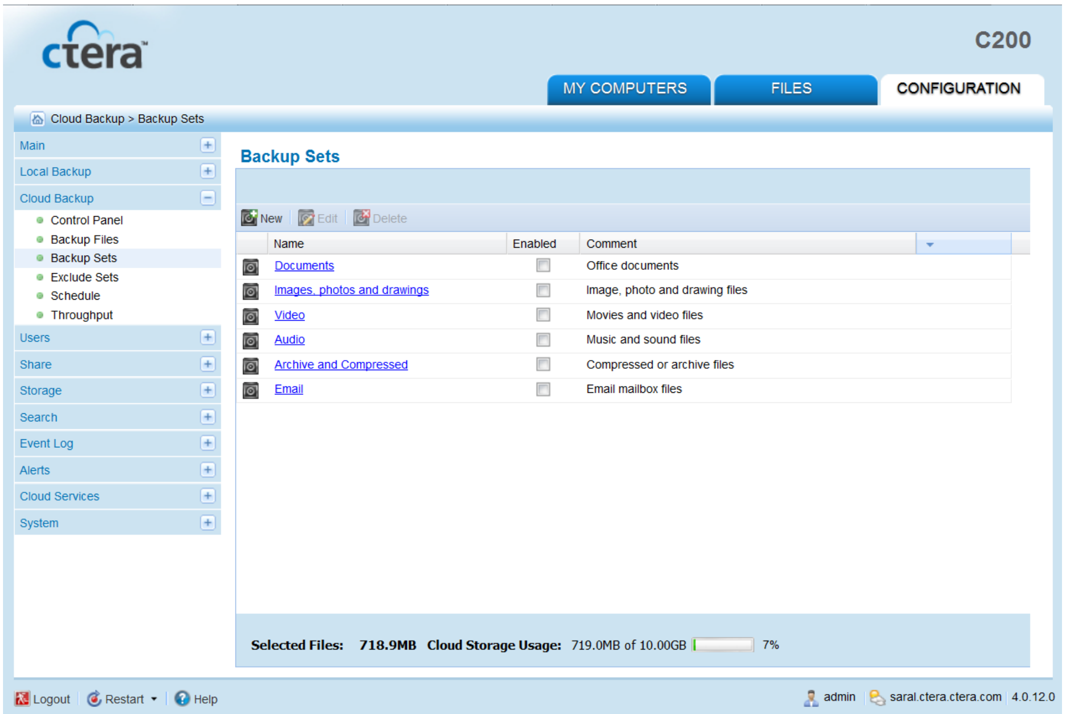
Enabling/Disabling Included Sets

In order for an included set to be used during backup operations, it must be enabled.

To enable an included set

1 In the **Configuration** tab's navigation pane, click **Cloud Backup > Backup Sets**.

The **Cloud Backup > Backup Sets** page appears.



2 Next to the desired included set, in the **Enabled** column, select the check box.

The included set is enabled.

At the bottom of the workspace, the **Selected Files** field indicates the size of the files selected for backup. The **Cloud Storage Usage** field indicates the amount of used space in your account after the next cloud backup operation (including backups from any other CTERA appliances included in your account).

To disable an included set

1 In the **Configuration** tab's navigation pane, click **Cloud Backup > Backup Sets**.

The **Cloud Backup > Backup Sets** page appears.

2 Next to the desired included set, in the **Enabled** column, clear the check box.

The included set is disabled.

At the bottom of the workspace, the **Selected Files** field indicates the size of the files selected for backup. The **Cloud Storage Usage** field indicates the amount of used space in your account after the next cloud backup operation (including backups from any other CTERA appliances included in your account).

Adding and Editing Included Sets

To add or edit an included set

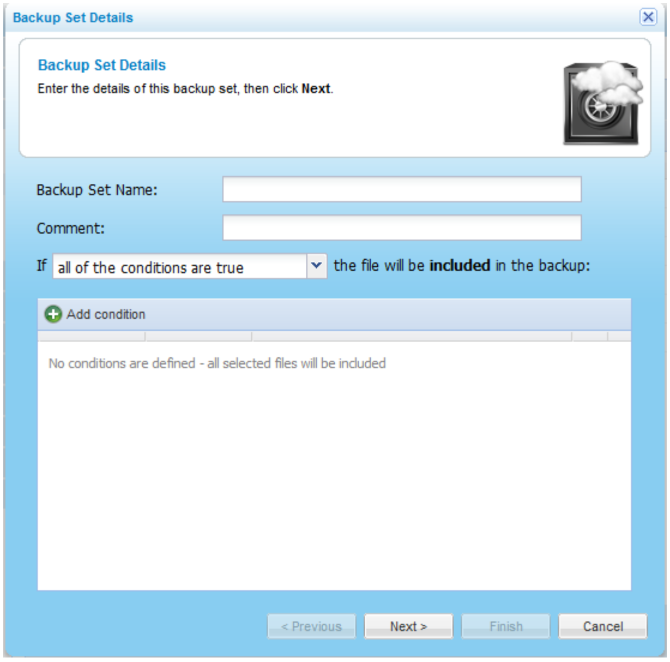
1. In the **Configuration** tab's navigation pane, click **Cloud Backup > Backup Sets**.

   The **Cloud Backup > Backup Sets** page appears.

2. Do one of the following:

   - To add a new included set, click **New**.
   - To edit an existing included set, click on its name.

   The **Backup Set Details Wizard** opens, displaying the **Backup Set Details** dialog box.



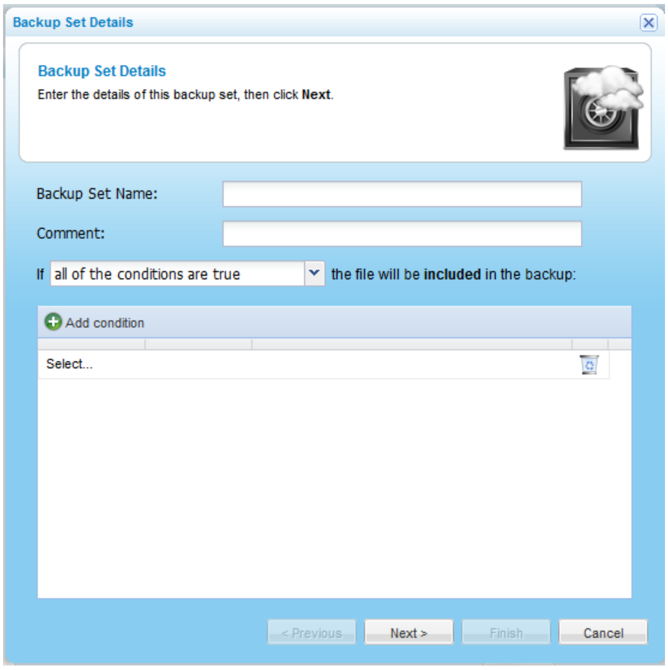
3. In the **Backup Set Name** field, type the name of the backup set.
4. In the **Comment** field, type a description of the backup set.
5. In the **If** field, do one of the following:

   - To specify that all of the conditions 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**.

6 Define the desired conditions for a file to be included in the backup set, by doing the following for each condition:

a Click **Add condition**.

A row appears in the table.



b Click **Select**, then select the desired condition parameter from the drop-down list.

c In the second column, click **Select**, then select the desired condition operator from the drop-down list.

See ***Backup Set Condition Operators*** (page 162).

d 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.

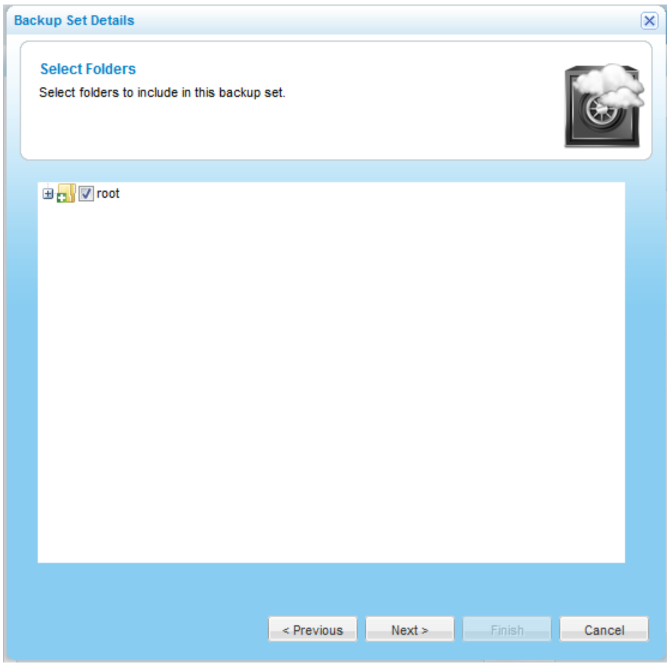
For example, if you select **File Name** as the condition parameter in the first column, select **begins** with as the condition operator in the second column, and type "Work-123-" in the third column, then the backup set will include all files whose names begin with "Work-123-".

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.

7 To delete a condition, click in its row.

8 Click **Next**.

The **Select Folders** dialog box appears.



This dialog box enables you to select the folders to which this backup set applies. By default, the root folder is selected, meaning that the backup set applies to all files in all folders. If desired, you can select specific folders to which this backup set should apply.

For example, you can create an backup set that contains all files that have the extension *.txt and reside in the folder `/share1/textfiles` by entering "txt" in the previous dialog box, and then choosing the folder `/share1/textfiles` in this dialog box.

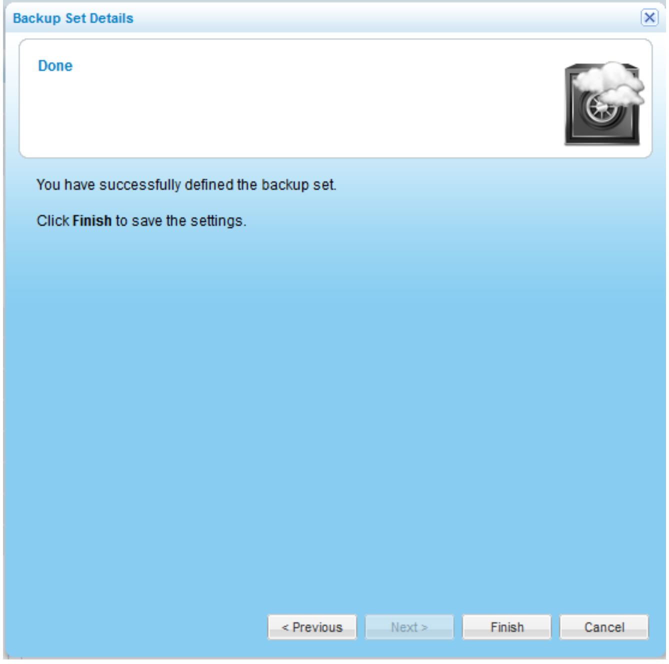
9 Expand the tree nodes to reveal the folders.

For an explanation of the icons and check boxes next to each folder, see ***Folder Icons*** (page 156).

10 Select the check boxes next to the folders you want to include in the included set.

11 Click **Next**.

The **Done** screen appears.



12 Click **Finish**.

Tip

If you added a new included set, it is automatically enabled.

Table 33: 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.

Deleting Included Sets

To delete an included set

1 In the **Configuration** tab's navigation pane, click **Cloud Backup > Backup Sets**.

The **Cloud Backup > Backup Sets** page appears.

2 Select the desired included set's name and click **Delete**.

A confirmation message appears.

3 Click **Yes**.

The included set is deleted.

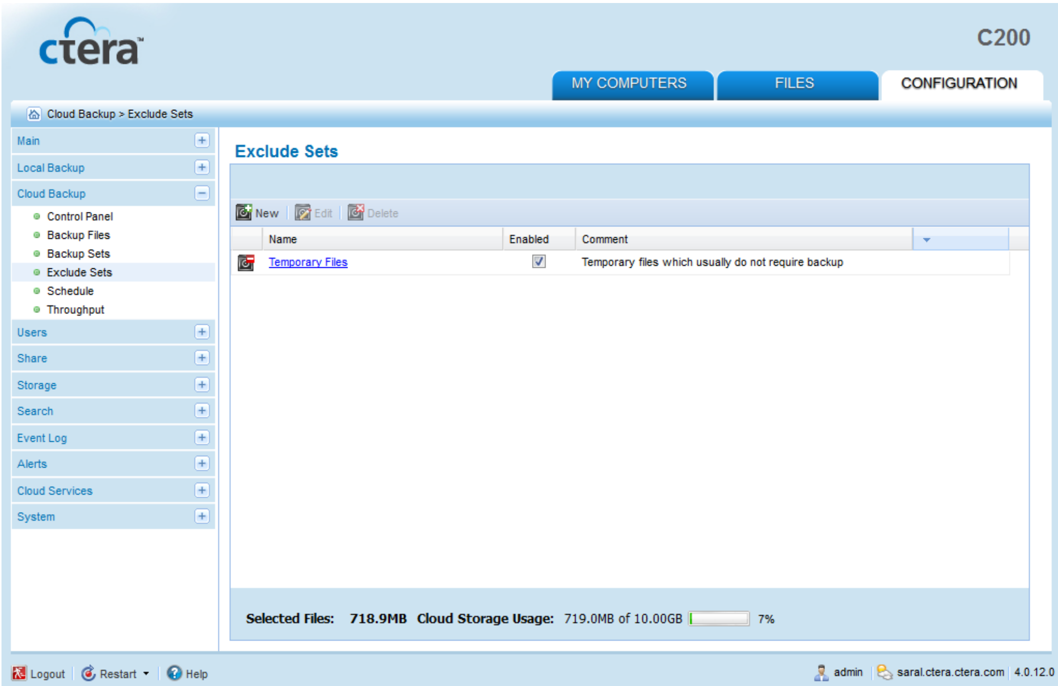
Enabling/Disabling Excluded Sets

In order for an excluded set to be used during backup operations, it must be enabled.

To enable an excluded set

1 In the **Configuration** tab's navigation pane, click **Cloud Backup > Exclude Sets**.

The **Cloud Backup > Exclude Sets** page appears.



2 Next to the desired excluded set, in the **Enabled** column, select the check box.

The excluded set is enabled.

At the bottom of the workspace, the **Selected Files** field indicates the size of the files selected for backup. The **Cloud Storage Usage** field indicates the amount of used space in your account after the next cloud backup operation (including backups from any other CTERA appliances included in your account).

To disable an excluded set

1. In the **Configuration** tab's navigation pane, click **Cloud Backup > Exclude Sets**.

   The **Cloud Backup > Exclude Sets** page appears.

2. Next to the desired excluded set, in the **Enabled** column, clear the check box.

   The excluded set is disabled.

   At the bottom of the workspace, the **Selected Files** field indicates the size of the files selected for backup. The **Cloud Storage Usage** field indicates the amount of used space in your account after the next cloud backup operation (including backups from any other CTERA appliances included in your account).

Adding and Editing Excluded Sets

To add or edit an excluded set

1. In the **Configuration** tab's navigation pane, click **Cloud Backup > Exclude Sets**.

   The **Cloud Backup > Exclude Sets** page appears.

2. Do one of the following:

   - To add a new excluded set, click **New**.
   - To edit an existing excluded set, click on its name.

   The **Backup Set Details Wizard** opens, displaying the **Backup Set Details** dialog box.

3. In the **Backup Set Name** field, type the name of the backup set.

4. In the **Comment** field, type a description of the backup set.

5. In the **If** field, do one of the following:

   - To specify that all of the conditions 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**.

6. Define the conditions that must be met in order for a file to be included in the backup set, by doing the following for each condition:

   a. Click **Add condition**.

      A row appears in the table.

b Click **Select**, then select the desired condition parameter from the drop-down list.

c In the second column, click **Select**, then select the desired condition operator from the drop-down list.

See ***Backup Set Condition Operators*** (page 162).

d 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, then the backup set will include all files with the extension *.avi, *.mov, and *.mpg.

7 To delete a condition, click in its row.

8 Click **Next**.

The **Select Folders** dialog box appears.

This dialog box enables you to select the folders to which this backup set applies. By default, the root folder is selected, meaning that the backup set applies to all files in all folders. If desired, you can select specific folders to which this backup set should apply.

For example, you can create an backup set that contains all files that have the extension *.txt and reside in the folder `/share1/textfiles` by entering "txt" in the previous dialog box, and then choosing the folder `/share1/textfiles` in this dialog box.

9 Expand the tree nodes to reveal the folders.

For an explanation of the icons and check boxes next to each folder, see ***Folder Icons*** (page 156).

10 Select the check boxes next to the folders you want to include in the excluded set.

11 Click **Next**.

The **Done** screen appears.

12 Click **Finish**.

Tip

If you added a new excluded set, it is automatically enabled.

Deleting Excluded Sets

To delete an excluded set

1. In the **Configuration** tab's navigation pane, click **Cloud Backup > Exclude Sets**.

   The **Cloud Backup > Exclude Sets** page appears.

2. Select the desired excluded set's name and click **Delete**.

   A confirmation message appears.

3. Click **Yes**.

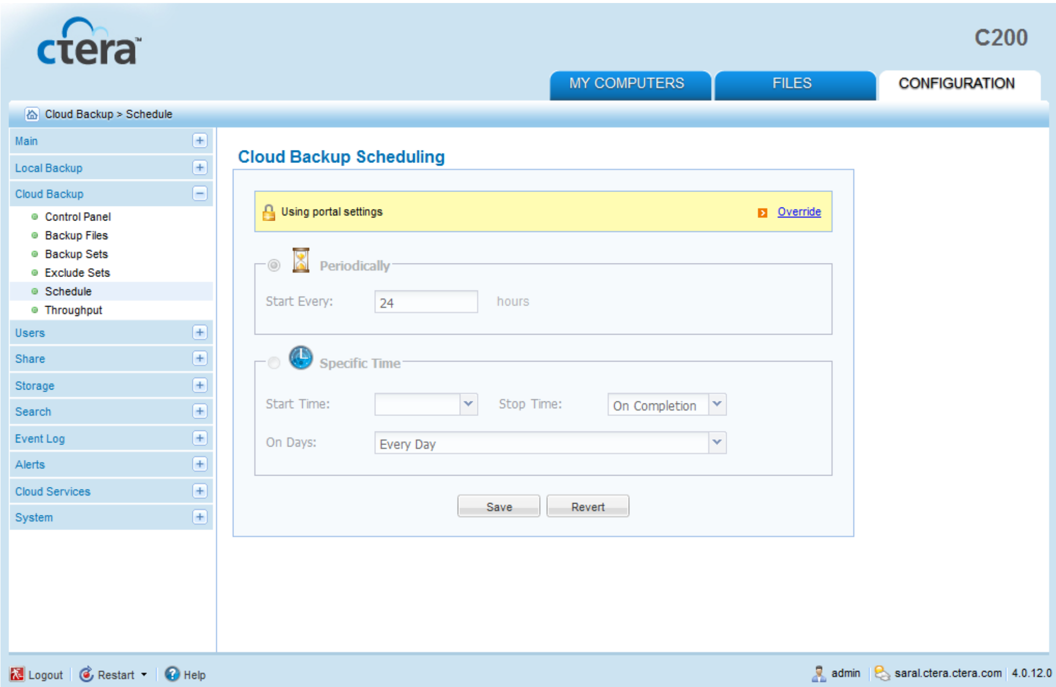
   The excluded set is deleted.

Scheduling Automatic Cloud Backup

To schedule automatic cloud backup

1. In the **Configuration** tab's navigation pane, click **Cloud Backup > Schedule**.

   The **Cloud Backup > Schedule** page appears.



2. Do one of the following:

   - To override settings inherited from the CTERA Portal, click **Override**.

- To use settings configured in the CTERA Portal, click **Use portal settings**.

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

4 Click **Save**.

Table 34: Backup Schedule Fields

In this field...	Do this...
Periodically	Choose this option to automatically back up files every specified number of hours. The **Start Every** field is enabled, and you must complete it.
Start Every	Type the amount of time between automatic cloud backups, in hours. The default value is 24 hours.
Specific Time	Choose this option to automatically back up files according to a specified daily schedule. The **Start Time**, **Stop Time**, and **On Days** fields are enabled, and you must complete them.
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.
Stop Time	Select the time at which cloud backup must end. This can be any of the following: - A specific hour - **On Completion**. The backup operation will only end when cloud backup is complete. The default value is **On Completion**. **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.
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**. Cloud backup will occur every day. The default value is **Every Day**.

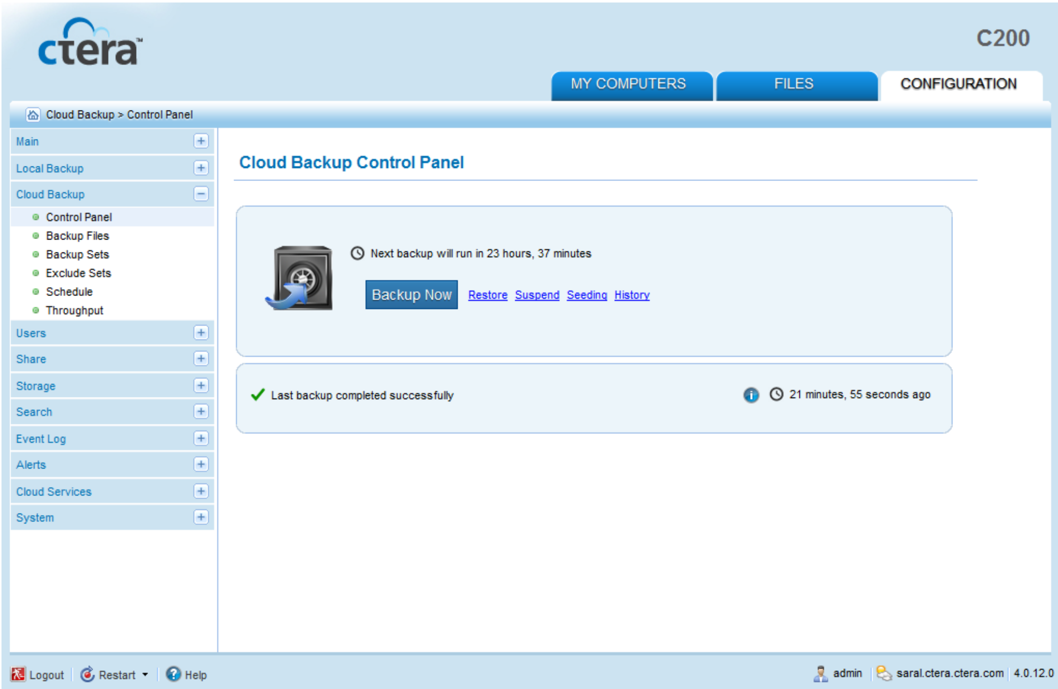
Manually Starting Cloud Backup

You can manually start cloud backup at any time.

To manually start cloud backup

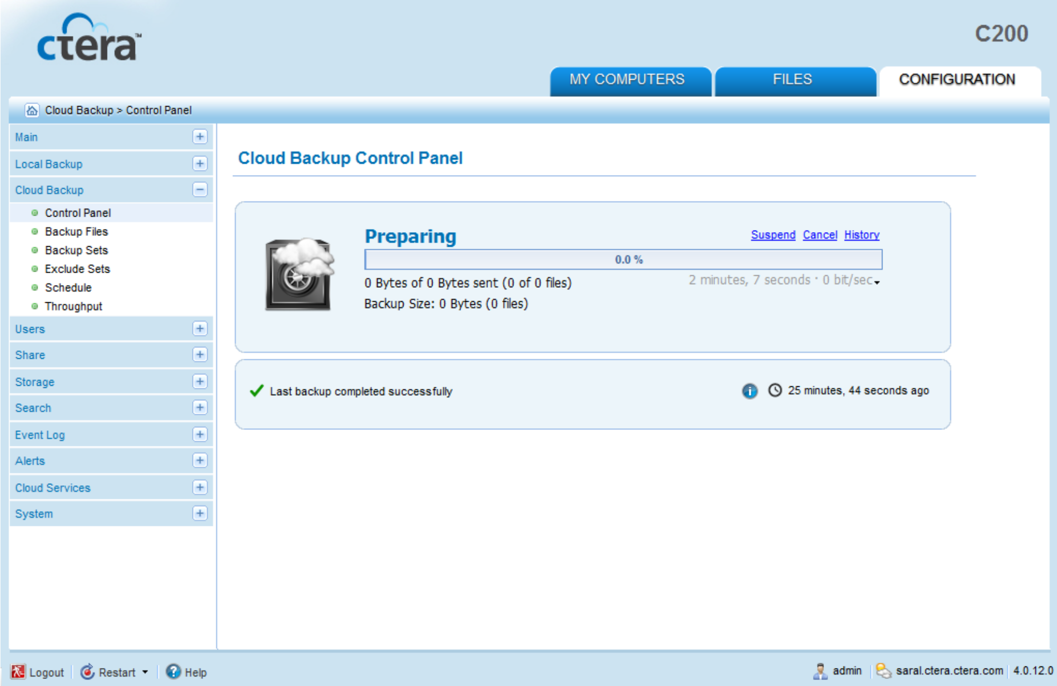
1 In the **Configuration** tab's navigation pane, click **Cloud Backup > Control Panel**.

The **Cloud Backup > Control Panel** page appears.



2 Click **Backup Now**.

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



3 To toggle the information displayed under the progress bar, do one of the following:

- To display the effective throughput (in Kbit/sec), click the ▾ icon, and then click **Show effective throughput**.
- To display the bandwidth usage (in bit/sec), click the ▾ icon, and then click **Show bandwidth usage**.

Canceling the Current Cloud Backup

You can cancel a running cloud backup.

Tip

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

To cancel the current cloud backup

1 In the **Configuration** tab's navigation pane, click **Cloud Backup > Control Panel**.

The **Cloud Backup > Control Panel** page appears.

2 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

Tip

Performing the following procedure is equivalent to suspending the Cloud Backup service via the CTERA Agent tray icon's right-click menu.

To suspend the CTERA Cloud Backup service

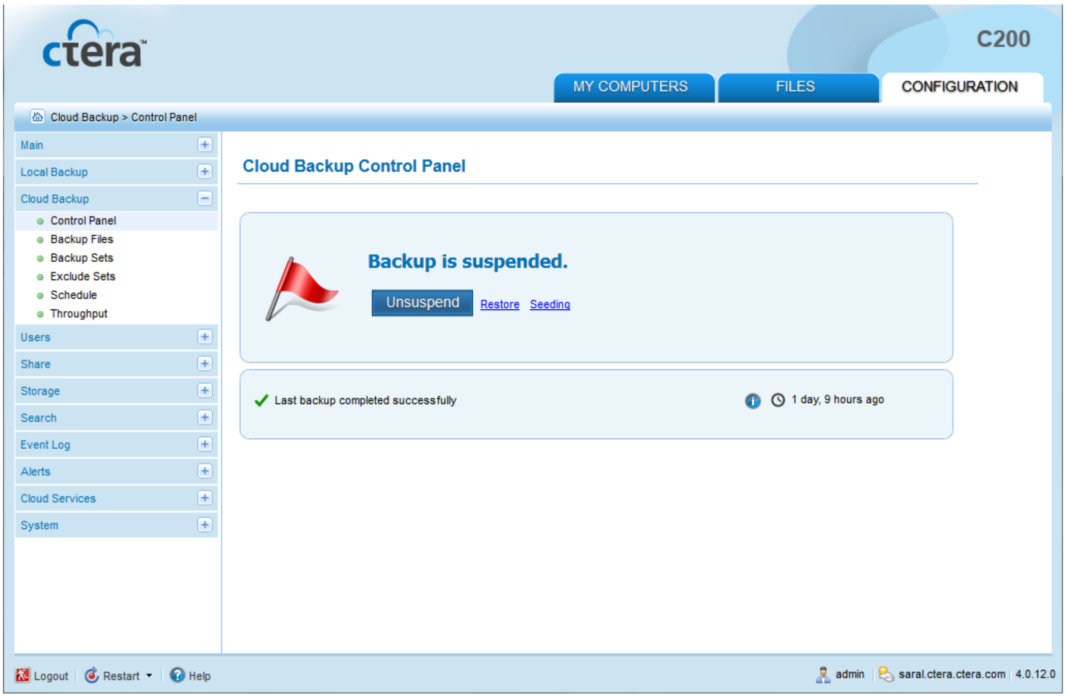
1 In the **Configuration** tab's navigation pane, click **Cloud Backup > Control Panel**.

The **Cloud Backup > Control Panel** page appears.

2 Click **Suspend**.

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

A message appears, indicating that backup has been suspended.



Resuming the Cloud Backup Service

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

Tip

Performing the following procedure is equivalent to resuming the Cloud Backup service via the CTERA Agent tray icon's right-click menu.

To resume the CTERA Cloud Backup service

1. In the **Configuration** tab's navigation pane, click **Cloud Backup > Control Panel**.

   The **Cloud Backup > Control Panel** page appears.

2. 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.

Viewing Cloud Backup Information

You can view information on the last backup performed and the next scheduled back up.

To view cloud backup information

- In the **Configuration** tab's navigation pane, click **Cloud Backup > Control Panel**.

  The **Cloud Backup > Control Panel** page appears.

  The following information is displayed:

Table 35: Cloud Backup Information

This field...	Displays...
Next backup will run in	The amount of time until the next scheduled automatic backup.
The last backup result	The status of the last backup: - **Completed successfully** - **Backup in Progress** - **The last backup has failed**, followed by the reason it failed If an error occurred during backup, refer to the backup logs for details. See ***Viewing Cloud Backup Logs*** (on page 303).
	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.

Preparing a Backup Seeding Hard Drive

When you have a lot of information to back up, the initial backup to the cloud can take a long time. If your CTERA service provider offers a backup seeding service, then you can speed up the initial backup by preparing a backup seeding hard drive, that is, is a drive that contains all of the files you want to include in your initial backup. You then deliver the seeding drive to the service provider, and the service provider uses the seeding drive to create the initial backup.

The seeding drive can optionally be encrypted using AES-256 and RSA public key encryption, so even if the drive is lost, there is very little risk to your sensitive information.

To prepare a backup seeding hard drive

1. Select the files and folders you want to include in the initial backup.

   See ***Selecting Files and Folders for Cloud Backup*** (on page 155).

   These files and folders will be written to the seeding drive.

2. In the **Configuration** tab's navigation pane, click **Cloud Backup > Control Panel**.

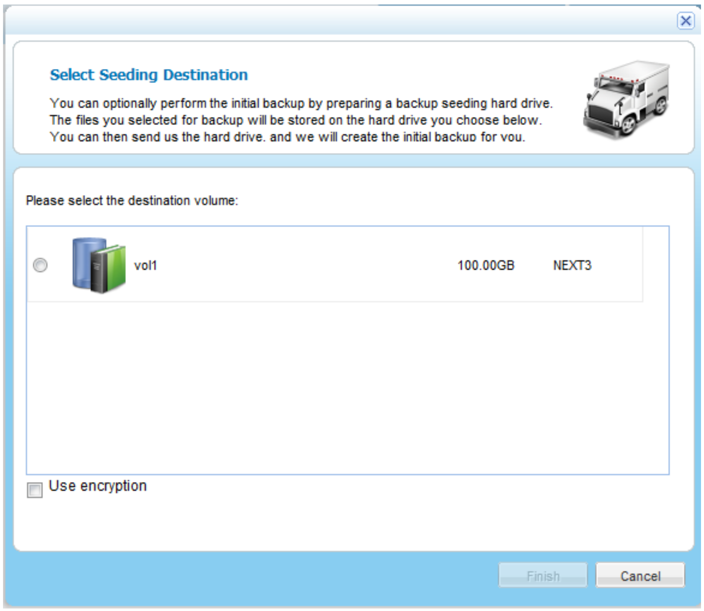
   The **Cloud Backup > Control Panel** page appears.

3. Click **Seeding**.

Tip

This option will appear only if the backup seeding service is supported by your service provider.

The **Select seeding destination** dialog box appears.



4 Choose the drive to use as the seeding drive.

Warning

The contents of this drive will be deleted.

5 To encrypt the seeding drive, select the **Use encryption** check box.

6 Click **Finish**.

A confirmation message appears.

7 Click **Yes**.

The selected files and folders are written to the seeding drive.

You can now deliver the seeding drive to your service provider.

Tip

During the time your service provider is loading the backup seeding drive to your account, the backup service will be temporarily disabled for your appliance.

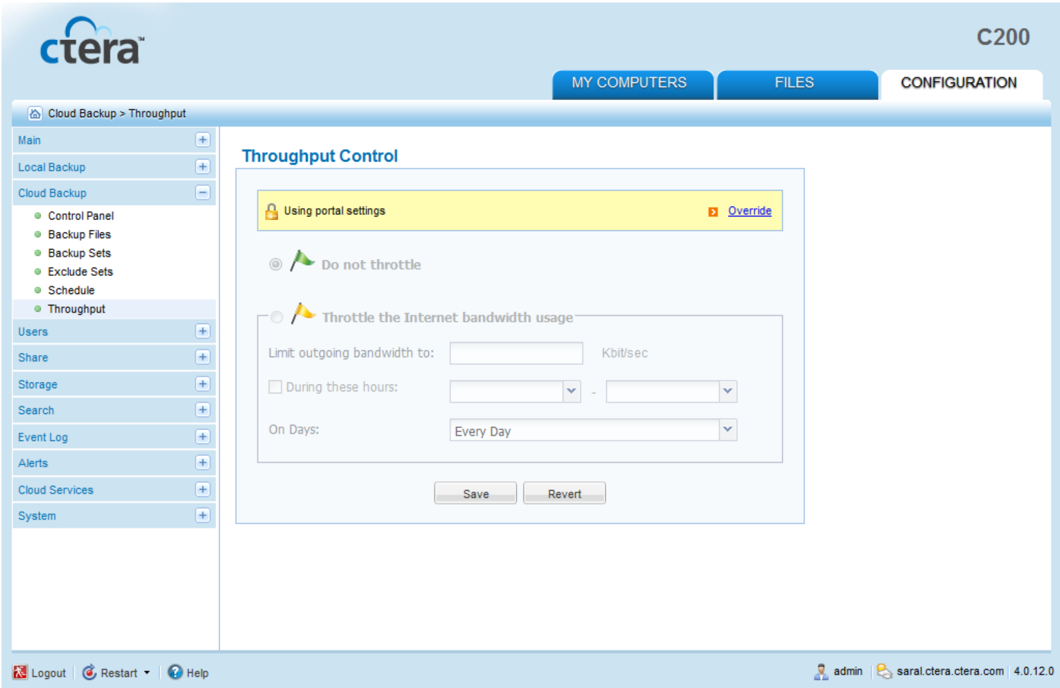
Restricting Throughput

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

To restrict throughput

1 In the **Configuration** tab's navigation pane, click **Cloud Backup > Throughput**.

The **Cloud Backup > Throughput** page appears.



2 Do one of the following:

- To override settings inherited from the CTERA Portal, click **Override**.
- To use settings configured in the CTERA Portal, click **Use portal settings**.

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

4 Click **Save**.

Table 36: Throughput Fields

In this field...	Do this...
Do not throttle	Choose this option to specify that throughput should not be restricted.
Throttle the Internet bandwidth usage	Choose this option to restrict the bandwidth used for cloud backups. The rest of the fields on the page are enabled, and you must complete them.
Limit outgoing bandwidth to	Type the maximum bandwidth to use for cloud backups in kilobytes per second.
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.
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**. Bandwidth used for cloud backup will be restricted every day. The default value is **Every Day**.

Restoring Files from Backup

CTERA appliance provides a number of ways to restore files to previous versions stored on the cloud, or to recover deleted files from the cloud. Some of the methods can be used by administrators, while other methods enable end users to restore their own files.

You can restore files and folders to the appliance using any of the following:

- **The appliance Web interface's Cloud Backup Control Panel**

  This can be done by administrators only. See ***Restoring Files and Folders from the Cloud Backup Control Panel*** (on page 176).

- **The CTERA Portal**

  You can access the CTERA Portal and restore files from there. This can be done by administrators only.

- **The Virtual Cloud Drive**

This can be done by both administrators and end users. See ***Restoring Files and Folders from a Cloud Snapshot Using the Virtual Cloud Drive*** (on page 180).

- **Microsoft Windows Previous Versions Interface**

  This can be done by both administrators and end users. See ***Restoring Files and Folders Using Microsoft Windows Previous Versions Interface*** (on page 181).

- **The appliance Web interface's Files Manager**

  This can be done by both administrators and end users. See ***Restoring Files and Folders from a Cloud/NEXT3 Snapshot Using the File Manager*** (on page 182).

In addition, you can restore files and folders from cloud or NEXT3 snapshots to a CTERA Agent using the following method:

- **The CTERA Agent Manager's Restore tab**

  This can be done by both administrators only. See ***Restoring Files and Folders from the Appliance to the Agent*** (on page 244).

Restoring Files and Folders from the Cloud Backup Control Panel

You can restore individual files or folders that were backed up to cloud storage. Alternatively, you can simultaneously restore *all* backed up files and folders, in order to roll back your disk contents to a previous point in time.

Note that if the same files already exist on your computer, they will be overwritten with the files you selected for restoration. Files that have been deleted since the date of the selected files will be recreated. Files that exist on your computer, but which do not exist in cloud storage or were not selected for restoration, will not be affected.

To restore files, the appliance must be connected to the CTERA Portal.

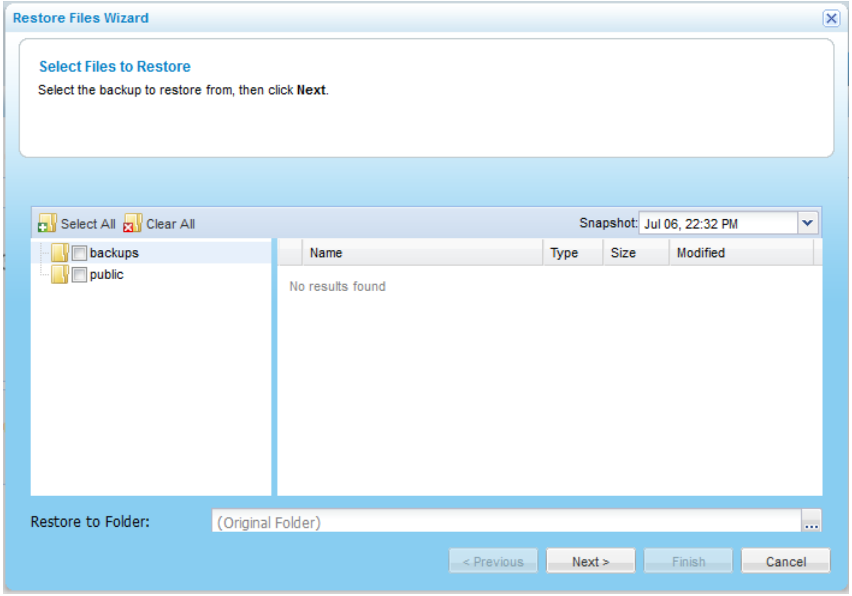
To restore backed up files from the Cloud Backup Control Panel

1. In the **Configuration** tab's navigation pane, click **Cloud Backup > Control Panel**.

   The **Cloud Backup > Control Panel** page appears.

2. Click **Restore**.

The **Restore Files Wizard** opens, displaying the **Select Files to Restore** dialog box.



3 In the **Snapshot** drop-down list, select the date and time of the snapshot from which you want to restore files.

4 Specify which files and folders you want to restore, by doing any of the following:

- To select individual files and folders:

  1 In the left pane, expand the nodes and click on the desired folders.

  The folder contents appear in the right pane.

  2 Select the check boxes next to the desired folders and files.

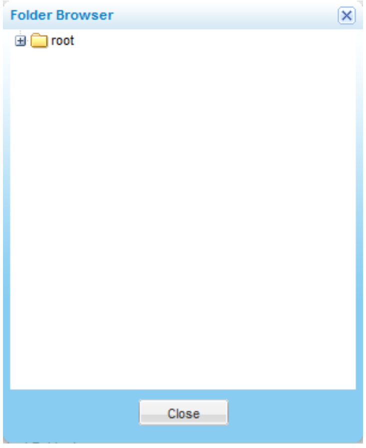
  For an explanation of the icons and check boxes next to each folder, see ***Folder Icons*** (page 156).

- To select all files, click **Select All**.

- To un-select all files, click **Clear All**.

5 If you want to restore files to a location other than the original location:

a Click in the **Restore to Folder** field. The **Folder Browser** dialog box appears.

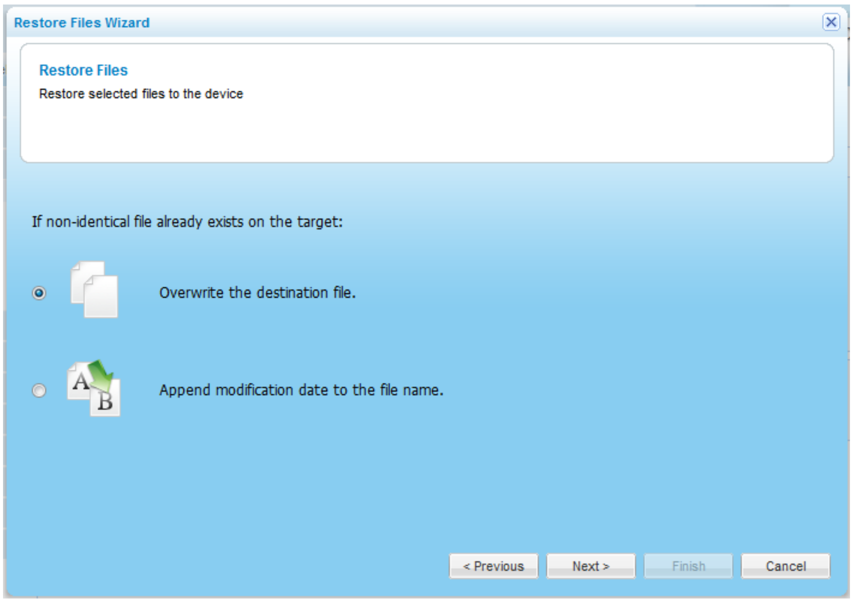


b Select the folder to which you would like to restore the files.

c Click **Close**.

6 Click **Next**.

The **Restore Files** dialog box appears.

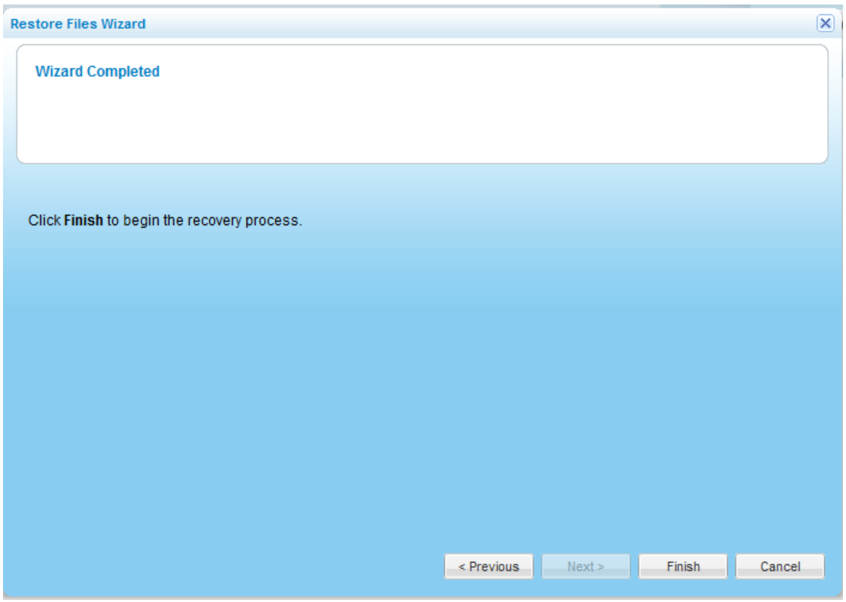


7 Specify how the appliance should handle files that exist both on your drive and in the selected backup, by doing one of the following:

- To specify that the files on your drive should be overwritten by the files in the backup, choose **Overwrite the destination file**.
- To specify that the files on your drive should have the modification date appended to their name, choose **Append modification date to the file name**.

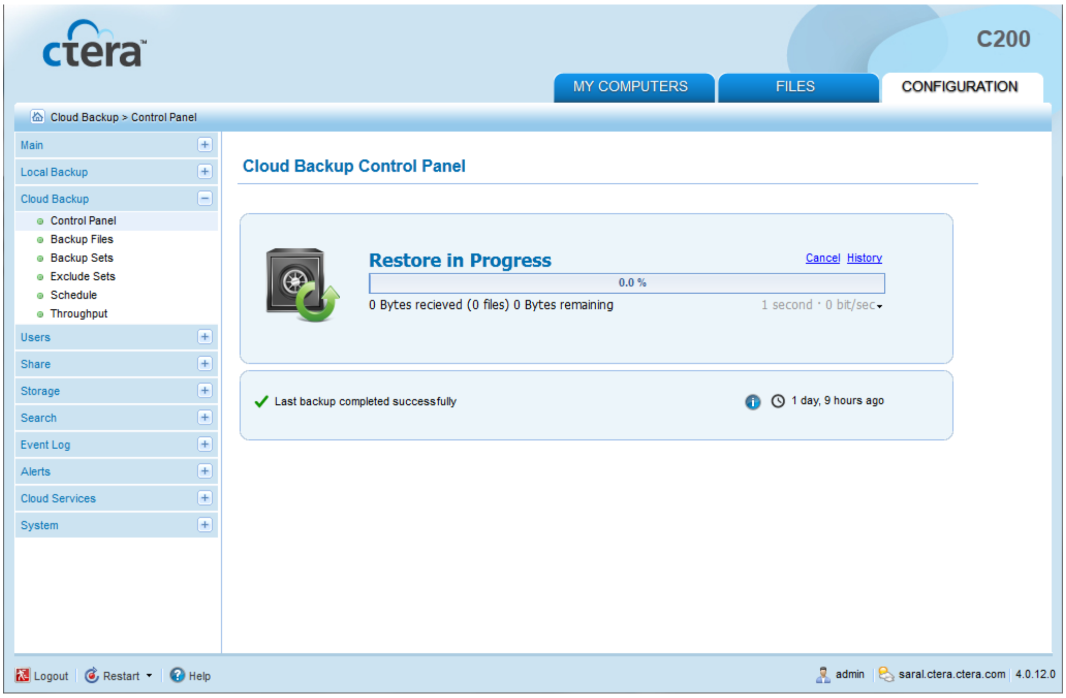
8 Click **Next**.

The **Wizard Completed** screen appears.



9 Click **Finish**.

A progress bar appears, and the files are restored form the selected backup.



10 To toggle the information displayed under the progress bar, do one of the following:

- To display the effective throughput (in Kbit/sec), click the ▾ icon, and then click **Show effective throughput**.
- To display the bandwidth usage (in bit/sec), click the ▾ icon, and then click **Show bandwidth usage**.

Canceling the Current Restore Process

When restoring files from the Cloud Backup Control Panel, you can cancel a running file restore process.

To cancel the current restore process

1. In the **Configuration** tab's navigation pane, click **Cloud Backup > Control Panel**.

   The **Cloud Backup > Control Panel** page appears.

2. Click **Cancel**.

   The current restore process is canceled.

Restoring Files and Folders from a Cloud Snapshot Using the Virtual Cloud Drive

When Windows File Sharing (CIFS) is enabled, you can restore files and folders via the appliance Virtual Cloud Drive.

This method of restoring files and folder is available on operating systems supporting Windows File Sharing.

To restore an individual file or folder to a previous version

1. View the network share containing the desired file or folder.

   See ***Viewing Network Shares Using Windows File Sharing*** (on page 146).

2. Open `PreviousVersions\Cloud`, and browse to the desired file or folder and date.
3. Copy the file or folder to another location.

Restoring Files and Folders Using Microsoft Windows Previous Versions Interface

Microsoft Windows Previous Versions enables you to restore individual files or folders that were backed up to cloud storage, directly from your PC. You can restore files to previous versions, or recover deleted files.

Tip

Microsoft Windows Previous Versions is supported in Microsoft Windows Server 2003, as well as Windows Vista Ultimate, Business, and Enterprise editions, and requires no special software in these editions. It is not supported in Windows Vista Home edition. In earlier versions of Windows, in order to access previous file and folder versions using Microsoft Windows Shadow Copy, you must download and install the Shadow Copy Client from:
`http://technet.microsoft.com/en-us/windowsserver/bb405951.aspx`

To restore an individual file or folder to a previous version

1 View the network share containing the desired file or folder.

See ***Viewing Network Shares Using Windows File Sharing*** (on page 146).

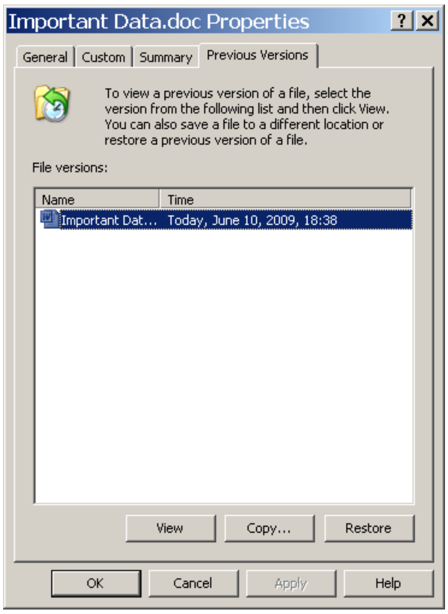
2 Open the relevant network share, and browse to the desired file or folder.

3 Right-click on the file or folder and click **Properties**.

The **Properties** dialog box appears.

4 Click the **Previous Versions** tab.

The **Previous Versions** tab is displayed.



5 In the **File Versions** list, select the version you want to restore.

6 Click **Restore**.

The file is restored to the desired version.

To restore a deleted file

1 View the network share containing the desired file or folder.

See ***Viewing Network Shares Using Windows File Sharing*** (on page 146).

2 Open the relevant network share, and browse to the folder that contained the file, prior to the file's deletion.

3 Right-click on the folder and click **Properties**.

The **Properties** dialog box appears.

4 Click the **Previous Versions** tab.

The **Previous Versions** tab is displayed.

5 In the **File Versions** list, locate the deleted file.

6 Click **Restore**.

The file is restored.

Restoring Files and Folders from a Cloud/NEXT3 Snapshot Using the File Manager

To restore files and folders from the File Manager

1 View the snapshot containing the files and folders you want to restore.

See ***Viewing Previous Versions of Files and Folders*** (on page 286).

2 Copy the desired files/folders.

See ***Copying/Moving Files and Folders*** (on page 284).

3 View the Latest Version snapshot.

See ***Viewing Previous File and Folder Versions*** (see "***Viewing Previous Versions of Files and Folders***" on page 286).

4 Paste the files/folders you copied earlier.

See ***Copying/Moving Files and Folders*** (on page 284).

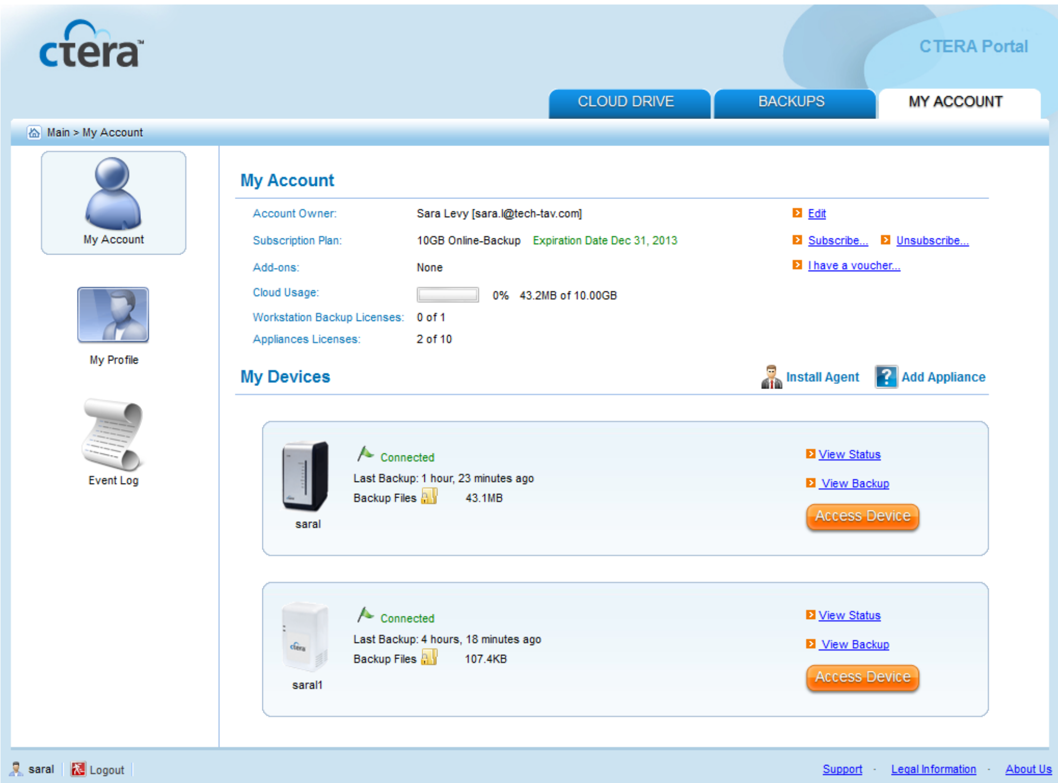
Restoring Appliance Configuration from Cloud Backup

Your appliance's configuration is automatically backed up to the cloud, each time cloud backup runs.

To restore your appliance's configuration from cloud backup

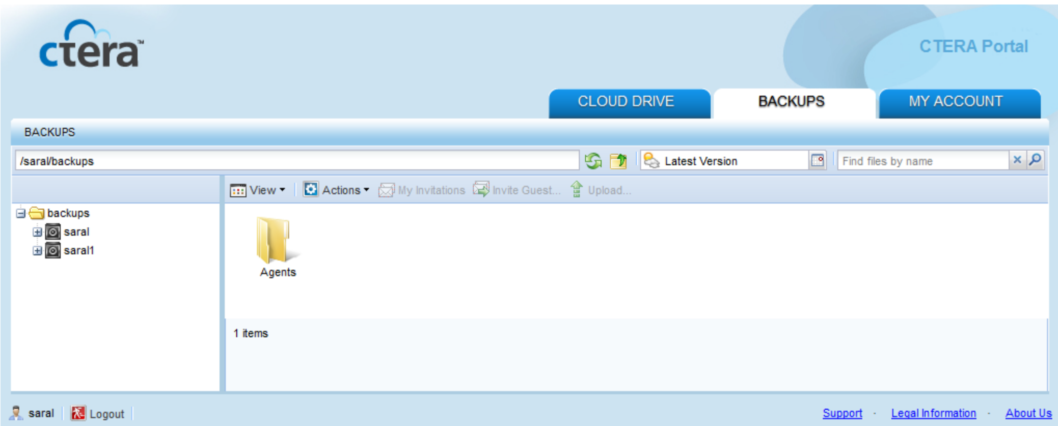
1 Using a Web browser, log in to your CTERA Portal account.

The CTERA Portal opens displaying the **My Account** tab.



2 Click the **Backups** tab.

The **Backups** tab opens.



3 Navigate to `backups/<backupFolder>/Device Configuration`, where `<backupFolder>` is the name of the appliance's backup folder.

4 Select **db.xml**.

5 Click **Actions**, and then click **Download**.

The configuration file is downloaded to your computer.

6 Import the configuration file to your appliance.

See ***Importing the Configuration*** (on page 329).

11

Synchronizing Folders

This chapter explains how to synchronize folders.

For information on bidirectional cloud drive synchronization, see ***Using Cloud Drive Synchronization*** (on page 58).

In This Chapter

Overview

The appliance Web interface provides the following ways of synchronizing folders:

- **Clientless Backup**

  Allows you to synchronize files from any computer on your network to a folder on the appliance, without requiring installation of a software agent on the remote computer.

  Tip

  Clientless Backup uses Windows File Sharing (CIFS) to synchronize data from your computers.

- **Sync Rules**

  Allow you to do the following:

  - Synchronize files from any computer on your network (or on the Internet) to your appliance, and from your appliance to any computer on your network (or on the Internet).
  - Synchronize files between two local folders.

  For example, you can set up your appliance to back up a certain folder on a daily basis to an external USB drive.

Tip

Sync rules support synchronizing data from and to network computers using a variety of methods, including Windows File Sharing (CIFS), WebDAV, and RSync. You can also use sync rules to keep two local folders on the appliance in sync.

- **Cloud drive synchronization**

  Allows you to synchronize your portal cloud drive with a specific folder on one or more CTERA appliances, and with CTERA agents in cloud mode.

  See ***Using Cloud Drive Synchronization*** (on page 58).

Workflow

In order to share files with other users, you must do one of the following:

- To configure file synchronization using Clientless Backup:

  a. If your computer runs Mac OS, you must configure it to be accessible to Clientless Backup.

     See ***Making Mac OS Computers Accessible to Clientless Backup*** (on page 197).

  b. Define Clientless Backup on a shared folder.

     See ***Using Clientless Backup*** (on page 186).

  c. Configure Clientless Backup.

     See ***Configuring Clientless Backup*** (on page 190).

  The network share will be automatically synchronized according to the configured schedule.

- To configure file synchronization using sync rules, add a sync rule.

  See ***Adding and Editing Sync Rules*** (on page 199).

  The network share will be automatically synchronized according to the configured schedule.

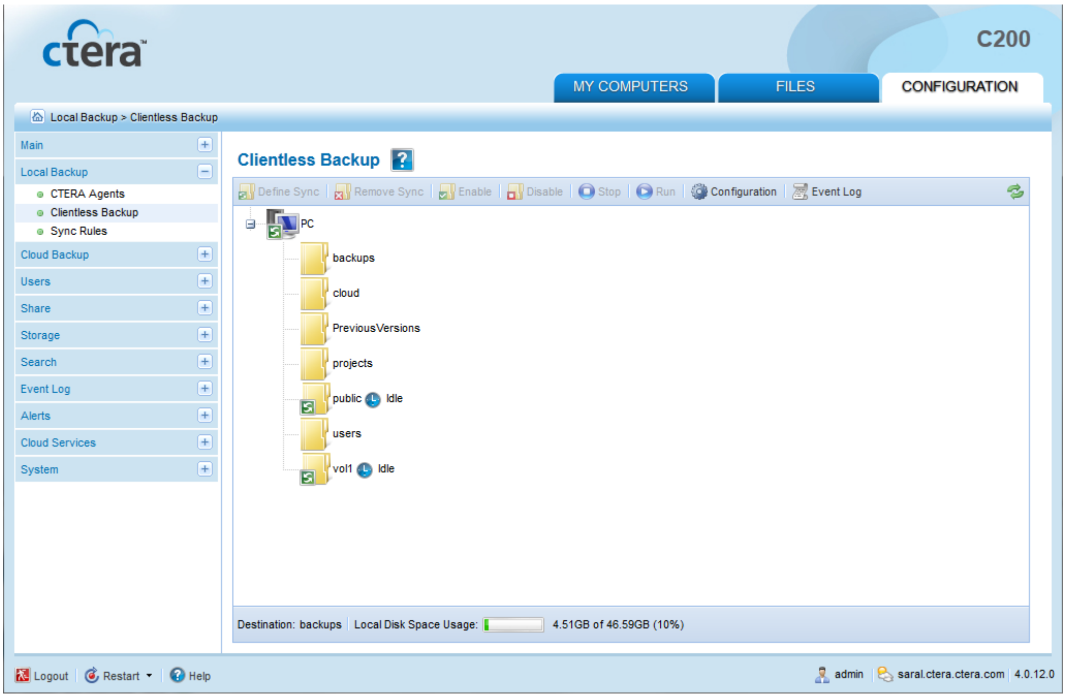
Setting Up Clientless Backup

Using Clientless Backup

To back up a network share using Clientless Backup

1. In the **Configuration** tab's navigation pane, click **Local Backup > Clientless Backup**.

The **Local Backup > Clientless Backup** page appears, displaying all computers in the network neighborhood.



Tip

Computers for which Clientless Backup is defined, but which are currently unavailable, appear in gray.

Tip

If your computer is missing in the list or appears in gray, see ***Enabling File Sharing on a PC*** (on page 194).

2 To rescan the network, click .

3 Next to the desired computer, click to expand the node.

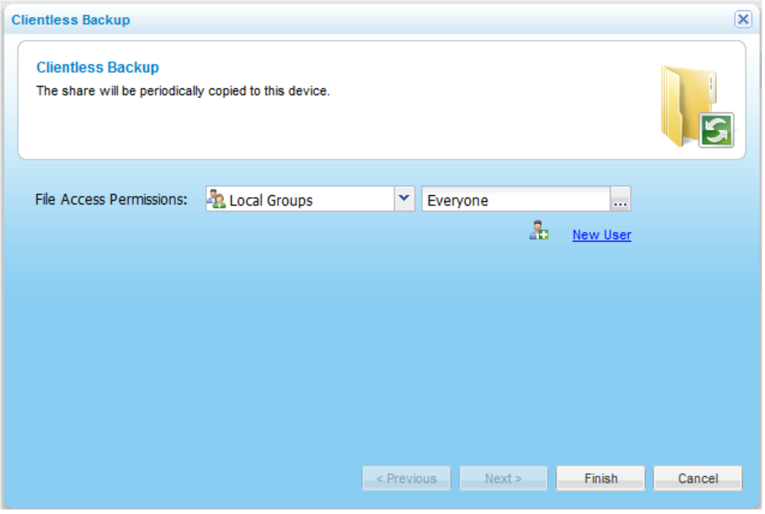
- If the share requires authentication, a pop-up window will open.

Enter the user name and password.

- The network shares on the computer are displayed.

4 Select the desired network share, and click **Define Sync**.

The **Clientless Backup Wizard** opens displaying the **Clientless Backup** dialog box.



5 Specify the user or user group that should be allowed access to the backed up files, by doing the following:

- To specify an existing user or user group, type the name of the user or user in the **Quick Search** field.
- To add a new user, click **New User**.

  For information on editing users, see ***Adding and Editing Users*** (on page 252).
- To search for a user or user group:

  1 In the **Select** drop-down list, select one of the following:

  Local Users. Search the users defined locally on the appliance.

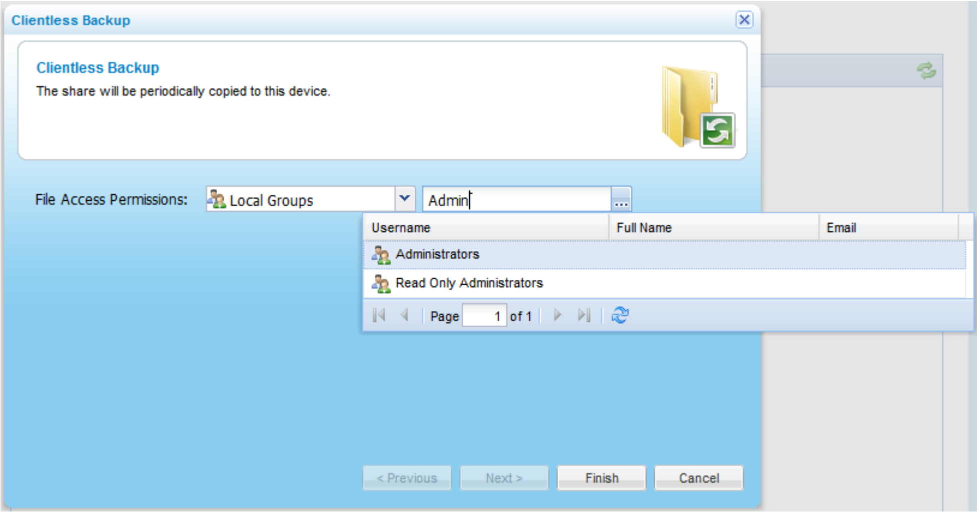
  Domain *domain* **Users**. Search the users belonging to the domain called *domain*.

  Local Groups. Search the user groups defined locally on the appliance.

  Domain *domain* **Groups**. Search the user groups belonging to the domain called *domain*.

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

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



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

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

6 Click **Finish**.

- The folder's icon changes to , and the synchronization status is indicated.
- At the bottom of the workspace, the **Destination** field indicates the folder on the appliance to which files will be backed up. The **Local Disk Space Usage** field indicates the amount of used space on the disk after the next Clientless Backup operation, out of the total amount of space available on the disk.

Removing Clientless Backup

To remove Clientless Backup from folders

1 In the **Configuration** tab's navigation pane, click **Local Backup > Clientless Backup**.

The **Local Backup > Clientless Backup** page appears, displaying all computers in the network neighborhood.

2 Do one of the following:

- To remove Clientless Backup for a single folder:

  1 Next to the desired computer, click to expand the node.

  The shared folders on the computer appear.

  2 Select the desired folder, and click **Remove Sync**.

  A confirmation message appears.

  3 Click **Yes**.

The folder's icon changes to .

To remove Clientless Backup for all the shares in a computer:

1. Select the desired computer, and click **Remove Sync**.

   A confirmation message appears.

2. Click **Yes**.

Configuring Clientless Backup

You can configure Clientless Backup to specify how often backup should occur, and where the resulting files will be stored.

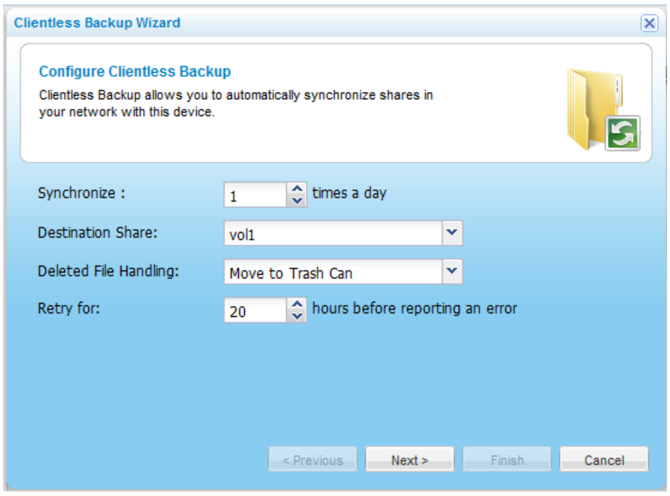
To configure Clientless Backup

1. In the **Configuration** tab's navigation pane, click **Local Backup > Clientless Backup**.

   The **Local Backup > Clientless Backup** page appears, displaying all computers in the network neighborhood.

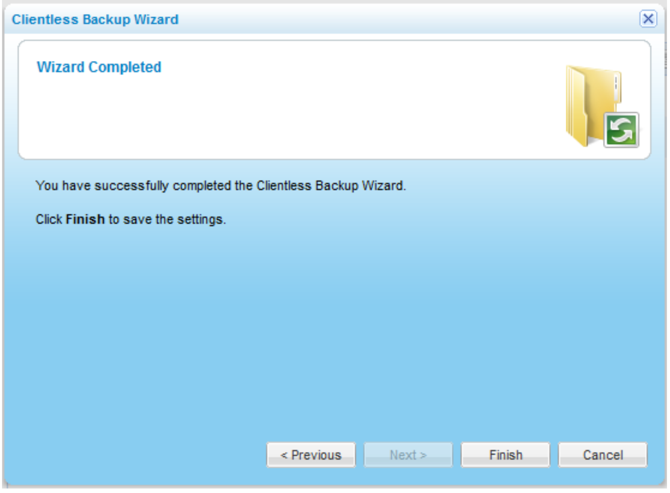
2. Click **Configuration**.

   The **Clientless Backup Wizard** opens, displaying the **Configure Clientless Backup** dialog box.



3. Complete the fields using the information in the following table.
4. Click **Next**.

The **Wizard Completed** screen appears.



5 Click **Finish**.

Table 37: Clientless Backup Wizard Fields

In this field...	Do this...
Synchronize	Use the arrows to specify how many times a day the remote folders should be backed up.
Destination Share	Select the local appliance network share with which the remote folders should be backed up. Clientless Backup will automatically create subdirectories under this network share for each backed up folder.
Deleted File Handling	Specify how deleted files should be handled, by selecting one of the following: - **Keep Deleted Files**. Files deleted in the source folder should be kept and not deleted in the destination folder. For example, if you chose to back up a local folder to a remote server, and one of the files in the folder is deleted locally, the file will not be deleted on the remote server. - **Move to Trash Can**. Files deleted in the source folder should be moved from the destination folder to the Trash Can folder. (The trash can is a folder called ".Trash".) - **Delete**. Files deleted in the source folder should be permanently deleted from the destination folder. The default value is **Delete**.
Retry for	Use the arrows to select the number of hours after Clientless Backup has failed, that the appliance should continue to retry Clientless Backup. The appliance will only log an error once the specified number of hours has elapsed. The default value is 20 hours.

Manually Starting/Stopping Clientless Backup

You can manually start and stop Clientless Backup for a network share at any time.

To manually start Clientless Backup

1. In the **Configuration** tab's navigation pane, click **Local Backup > Clientless Backup**.

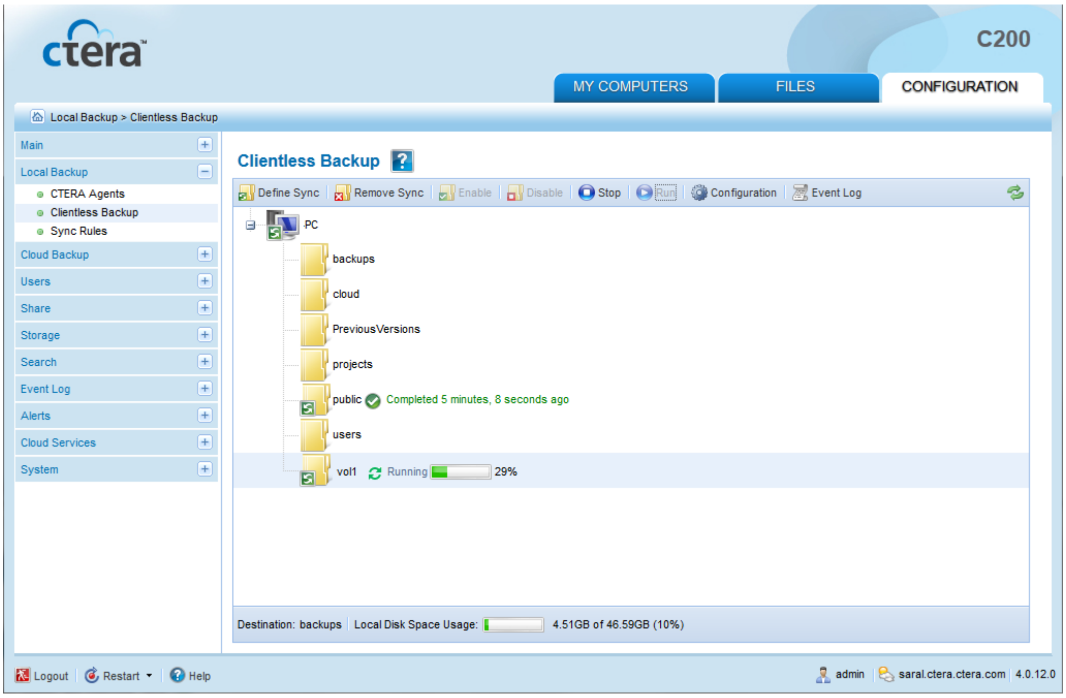
   The **Local Backup > Clientless Backup** page appears, displaying all computers in the network neighborhood.

Tip

If a computer or share does not appear, then file sharing is not set up on the computer. See ***Enabling File Sharing on a PC*** (on page 194).

2 Select the desired share, and click **Run**.

A progress bar appears, and the relevant share is backed up.



To stop a running Clientless Backup

1 In the **Configuration** tab's navigation pane, click **Local Backup > Clientless Backup**.

The **Local Backup > Clientless Backup** page appears, displaying all computers in the network neighborhood.

2 Select the share for which Clientless Backup is running, and click **Stop**.

Backup stops.

Disabling/Enabling Clientless Backup

You can disable Clientless Backup for a network share. The current backup and all future scheduled backups will be suspended for the share, until you enable Clientless Backup for the share again.

To disable Clientless Backup

1 In the **Configuration** tab's navigation pane, click **Local Backup > Clientless Backup**.

The **Local Backup > Clientless Backup** page appears, displaying all computers in the network neighborhood.

2 Select the desired share, and click **Disable**.

Clientless Backup is disabled for the share.

To enable Clientless Backup

1 In the **Configuration** tab's navigation pane, click **Local Backup > Clientless Backup**.

The **Local Backup > Clientless Backup** page appears, displaying all computers in the network neighborhood.

2 Select the desired share, and click **Enable**.

Clientless Backup is enabled for the share.

Enabling File Sharing on a PC

If a computer or share does not appear in the **Local Backup > Clientless Backup** page, then file sharing is not set up on the computer.

Enabling File Sharing in Windows XP

If your Windows XP computer does not appear in the **Clientless Backup** page, or is displayed as a grayed icon, perform the following steps to enable file sharing.

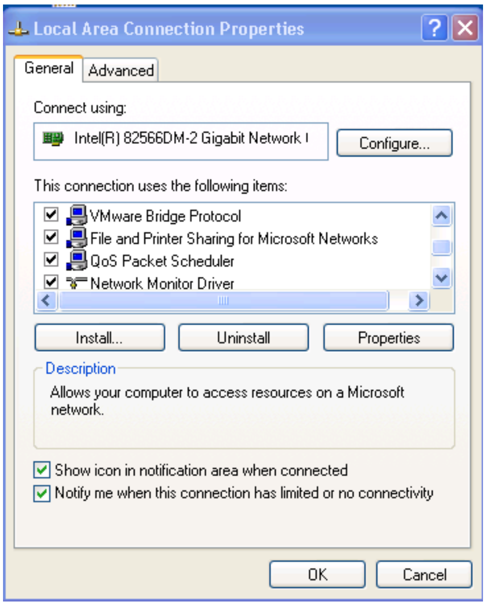
To enable file sharing in Windows XP

1 Click **Start > Control Panel**.

2 Open the **Network Connections** Control Panel applet.

3 Select the **Local Area Connection**.

4 View the properties for this connection by right-clicking on the icon and choosing **Properties** from the menu.



5 Make sure the **File and Printer Sharing for Microsoft Windows** check box is selected.

6 Click **OK**.

If you are still having trouble, make sure Windows Firewall is not blocking File and Printer Sharing. Do the following:

1 Click **Start > Control Panel**.

2 Open the **Windows Firewall** Control Panel applet.

3 In the **General** tab, ensure that the **Do not Allow Exceptions** check box is *not* selected.

4 In the **Exceptions** tab, make sure the **File and Printer Sharing** check box is selected.

5 Click **OK**.

Enabling File Sharing in Windows Vista

If your Windows Vista computer does not appear in the **Clientless Backup** page, or is displayed as a grayed icon, perform the following steps to enable file sharing.

To enable file sharing in Windows Vista

1 Open the Network and Sharing Center, by clicking **Start > Control Panel**, clicking **Network and Internet**, and then clicking **Network and Sharing Center**.

2 If network discovery is off, click the arrow button to expand the section, click **Turn on network discovery**, and then click **Apply**.

3 If file sharing is off, click the arrow button to expand the section, click **Turn on file sharing**, and then click **Apply**.

If you are still having trouble, make sure Windows Firewall is not blocking File and Printer Sharing. Do the following:

1 Open Windows Firewall by clicking the **Start > Control Panel**, clicking **Security**, and then clicking **Windows Firewall**.

2 Click **Allow a program through Windows Firewall**.

3 In the **Program or port** list, make sure the **File and Printer Sharing** check box is selected.

4 Click **OK**.

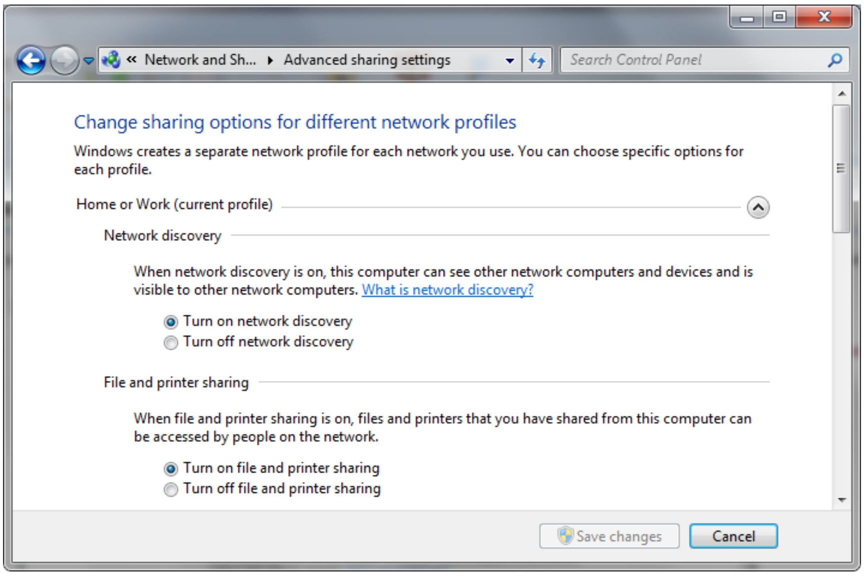
Enabling File Sharing in Windows 7

If your Windows 7 computer does not appear in the **Clientless Backup** page, or is displayed as a grayed icon, perform the following steps to enable file sharing.

To enable file sharing in Windows 7

1 Open the Network and Sharing Center, by clicking **Start > Control Panel**, clicking **Network and Internet**, and then clicking **Network and Sharing Center**.

2 In the left pane, click **Change advanced sharing settings**.



3 Expand your current network profile, by clicking the arrow to the right of its name.

The current network profile is marked "(current profile)" and is usually called "Home or Work".

4 If network discovery is off, click **Turn on network discovery**.

5 If file and printer sharing is off, click **Turn on file and printer sharing**.

6 Click **Save changes**.

If you are still having trouble, make sure Windows Firewall is not blocking File and Printer Sharing. Do the following:

1 Open Windows Firewall by clicking the **Start > Control Panel**, clicking **System and Security**, and then clicking **Allow a program through Windows Firewall**.

2 In the **Allowed programs and features** list, locate **File and Printer Sharing**, and make sure that the check boxes in the **Name** column and the in column for your current network profile (usually "Home or Work") are *both* selected.

3 Click **OK**.

Making Mac OS Computers Accessible to Clientless Backup

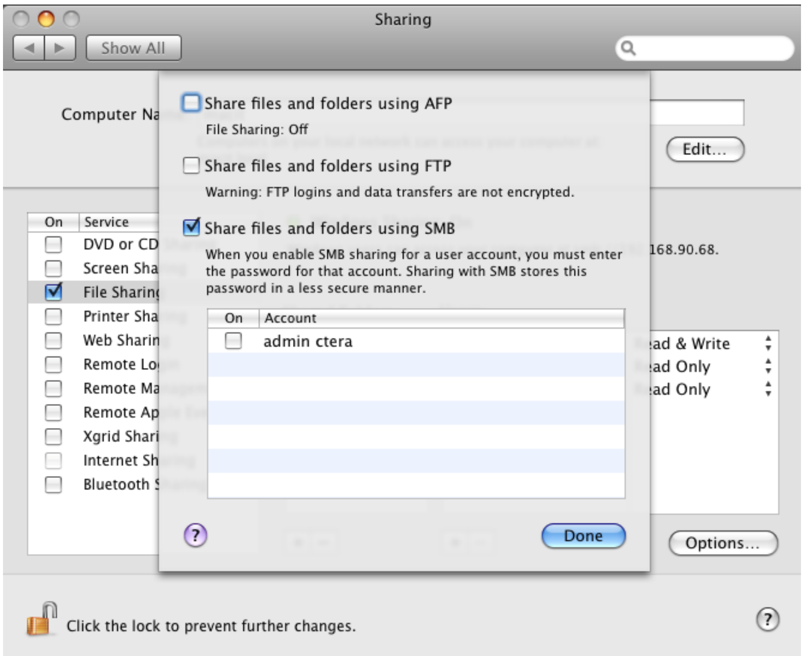
If your computer runs Mac OS, you must configure it to be accessible to Clientless Backup; otherwise the computer will not appear in Clientless Backup.

To make a Mac OS computer accessible to Clientless Backup

1 Go to **System Preferences** > **Sharing**.

2 Click **Options**.

A dialog box opens.



3 Select the **Share files and folders using SMB check** box.

4 Click **Done**.

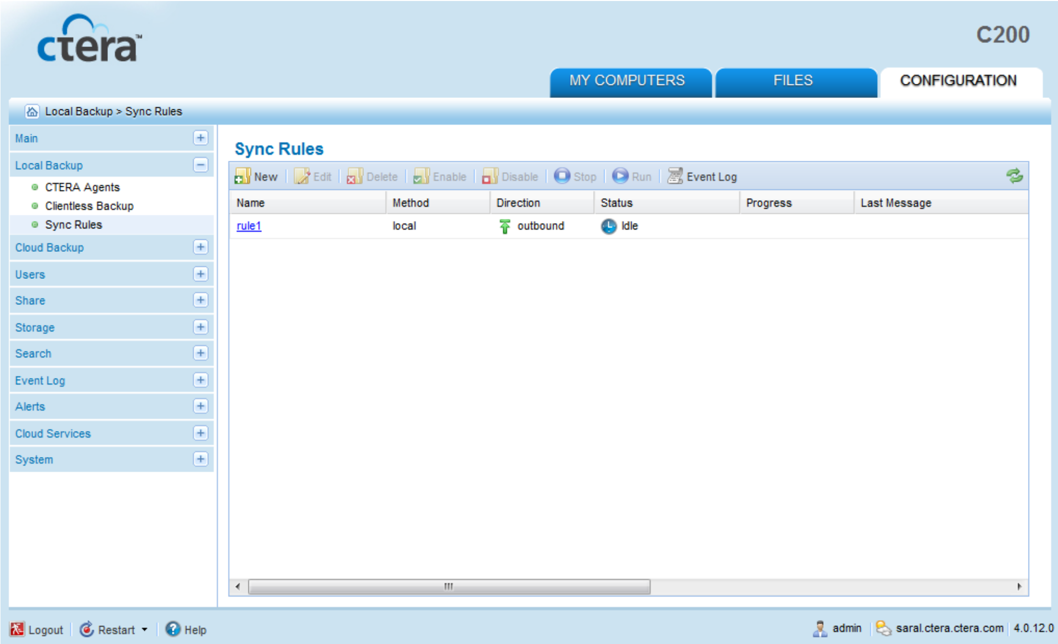
Setting Up Sync Rules

Adding and Editing Sync Rules

To add or edit a sync rule

1 In the **Configuration** tab's navigation pane, click **Local Backup > Sync Rules**.

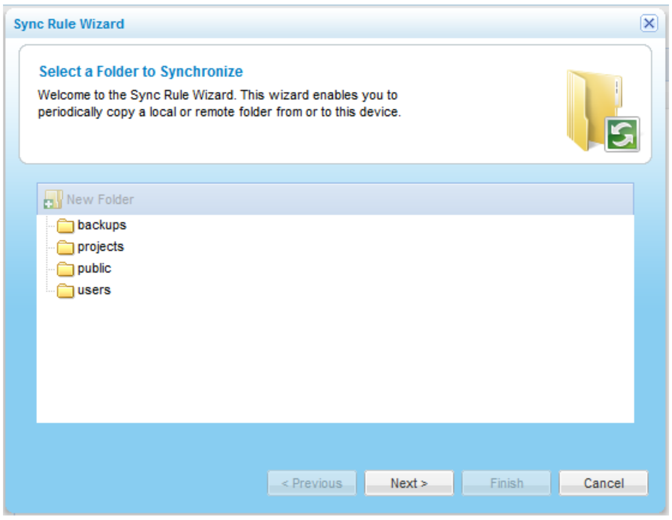
The **Local Backup > Sync Rules** page appears.



2 Do one of the following:

- To add a new sync rule, click **New**.
- To edit an existing sync rule, click on its name.

The **Sync Rule Wizard** opens, displaying the **Select a Folder to Synchronize** dialog box.



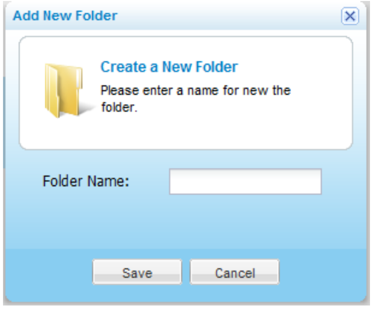
3 Expand the tree nodes and select the folder you want to synchronize.

4 (Optional) To create a new folder, do the following:

a In the tree, select the parent folder in which you want to create the new folder.

b Click **New Folder**.

The **Create a New Folder** dialog box opens.



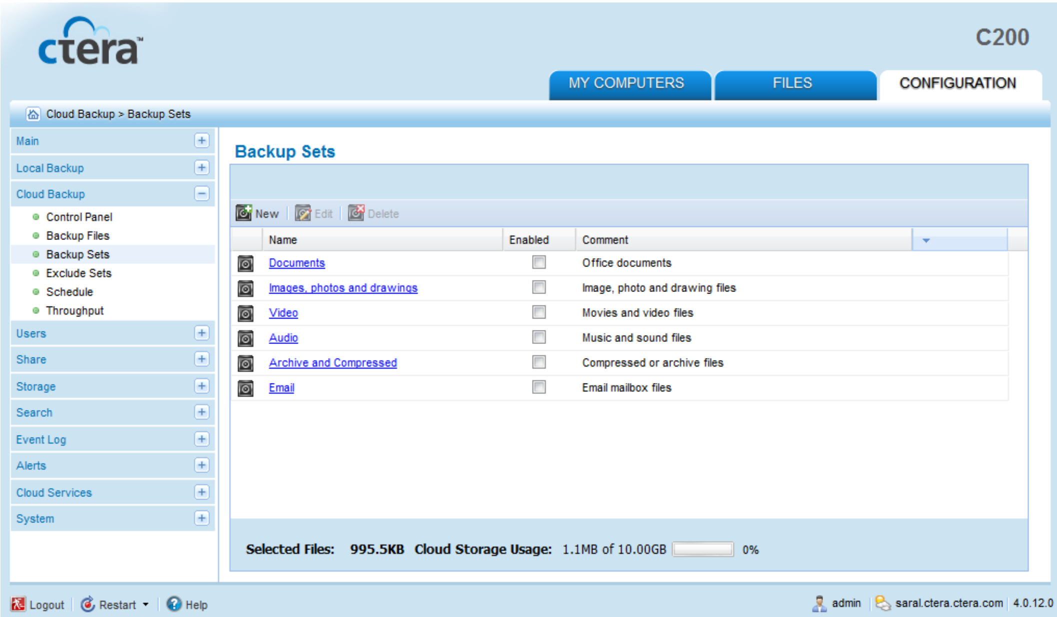
c In the **Folder Name** field, type a name for the folder.

d Click **Save**.

A new folder is added to the selected parent folder.

5 Click **Next**.

The **Specify the Synchronization Method** dialog box appears.



Choose the desired synchronization method using the information in the following table.

6 Click **Next**.

7 Do one of the following:

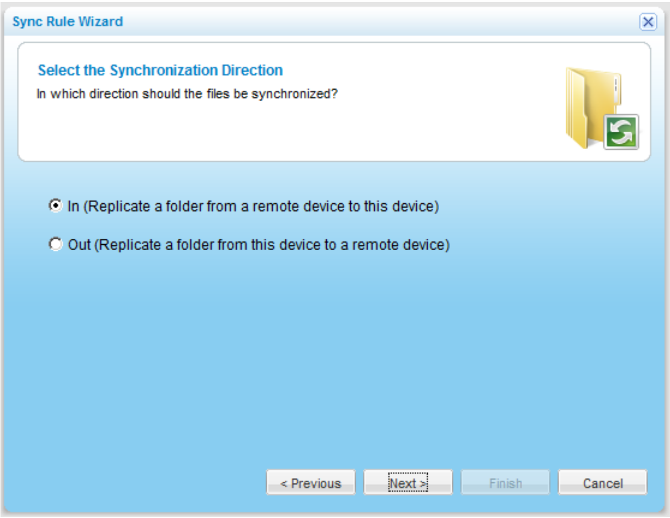
- If you selected **Rsync** or **Windows File Sharing**, continue at ***Synchronizing with a Remote RSync or CIFS Server*** (page 201).
- If you selected **WebDAV**, continue at ***Synchronizing with a Remote WebDAV Server*** (page 205).
- If you selected **Local Folder**, continue at ***Synchronizing Two Local Folders*** (page 206).

Table 38: Synchronization Methods

Select this option...	To specify that...
Rsync	The appliance should synchronize the folder with a remote RSync server. This option is ideal if you have an RSync server and a slow Internet connection.
WebDAV	The appliance should synchronize the folder with a remote WebDAV server.
Windows File Sharing	The appliance should synchronize the folder with a remote server using Windows file sharing (CIFS).
Local Folder	The appliance should synchronize the folder with another local folder. For example, you can set up your appliance to back up a certain folder on a daily basis to an external USB drive.

To synchronize with a Remote RSync or CIFS Server

The **Select the Synchronization Direction** dialog box appears.

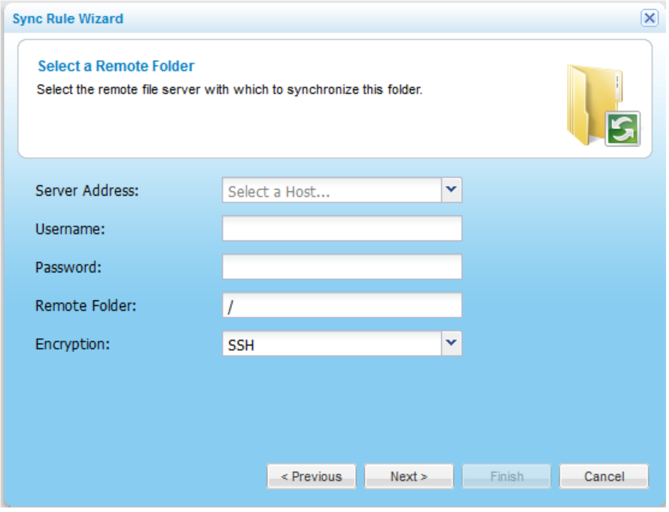


1 Specify the synchronization direction, by doing one of the following:

- To synchronize a folder from a remote server to the appliance, choose **In**.
- To synchronize a folder from the appliance to a remote server, choose **Out**.

2 Click **Next**.

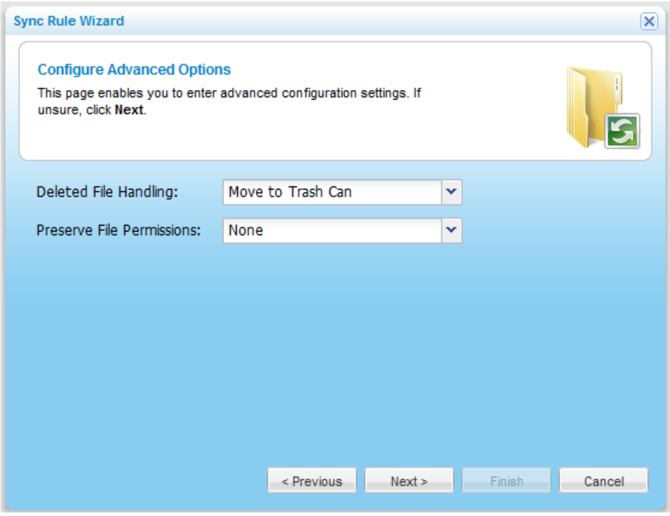
The **Select a Remote Folder** dialog box appears.



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

4 Click **Next**.

The **Configure Advanced Options** dialog box appears.



5 In the **Deleted File Handling** field, specify how deleted files should be handled, by doing one of the following:

- To specify that files deleted in the source folder should be kept and not deleted in the destination folder, select **Keep Deleted Files**.

  For example, if you chose to synchronize a local folder to a remote server, and one of the files in the folder is deleted locally, the file will not be deleted on the remote server.

- To specify that files deleted in the source folder should be moved from the destination folder to the Trash Can, select **Move to Trash Can**, which is a folder called ".Trash".
- To specify that files deleted in the source folder should be permanently deleted from the destination folder, select **Delete.**

6 In the **Preserve File Permissions** drop-down list, specify whether the permissions for synchronized files should be retained, by doing one of the following:

- To specify that permissions configured for a file in the source folder should *not* be retained for the parallel file in the destination folder, select **None**.
- To specify that basic permissions configured for a file in the source folder should be retained for the parallel file in the destination folder, select **Basic**.
- To specify that full permissions configured for a file in the source folder should be retained for the parallel file in the destination folder, select **Full**.

This field only appears if you selected **Rsync**.

7 Click **Next**.

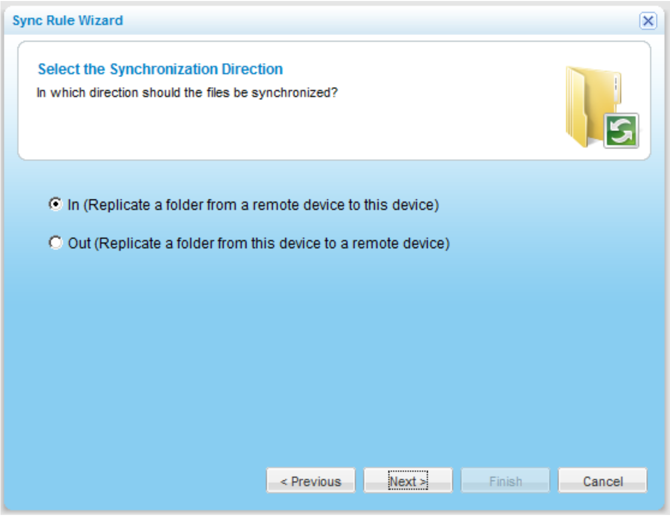
8 Continue at ***Completing Synchronized Folder Configuration*** (page 208).

Table 39: Select a Remote Folder Fields

In this field...	Do this...
Server Address	Type the remote server's IP address or DNS name.
Username	Type the user name with which the appliance should authenticate to the remote server.
Password	Type the password with which the appliance should authenticate to the remote server.
Remote Folder	Type the path to the folder on the remote server, with which you want to synchronize files. When synchronizing between two CTERA appliances, the path must start with the share name, and not with a "/".
Encryption	Specify the encryption method with which to secure the connection to the remote server, by selecting one of the following: • None. Do not encrypt the connection to the remote server. • SSH. Secure the connection to the remote server using SSH (Secure Shell). The remote server must support SSH access. • SSL. Secure the connection to the remote server using SSL (Secure Sockets Layer). The remote server must support SSL access. The default value is SSH. When synchronizing between two CTERA appliances, you must select None. This field is relevant for RSync only.

To synchronize with a remote WebDav Server

The **Select a Synchronization Direction** dialog box appears.

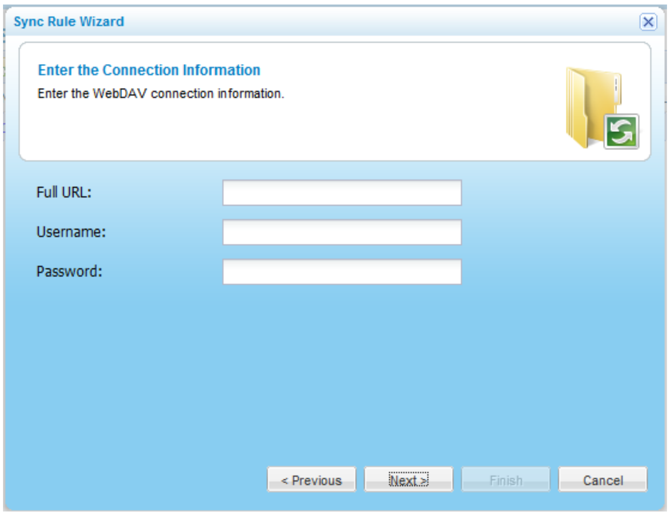


1 Specify the synchronization direction, by doing one of the following:

- To synchronize a folder from a remote server to the appliance, choose **In**.
- To synchronize a folder from the appliance to a remote server, choose **Out**.

2 Click **Next**.

The **Enter the Connection Information** dialog box appears.



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

4 Click **Next**.

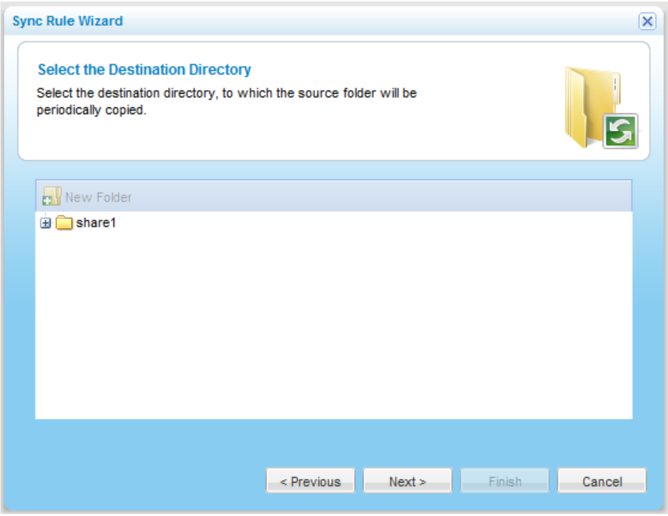
5 Continue at ***Completing Synchronized Folder Configuration*** (page 208).

Table 40: Enter the Connection Information Fields

In this field...	Do this...
Full URL	The full URL of the remote WebDAV server. This must start with http:// or https://.
Username	Type the user name with which the appliance should authenticate to the remote server. If the WebDAV server does not require authentication, you can leave the **Username** and **Password** fields empty.
Password	Type the password with which the appliance should authenticate to the remote server.

To synchronize two local folders

If you selected **Local Folder**, the **Select the Destination Directory** dialog box appears.



1 Expand the tree nodes and select the folder with which you want to synchronize.

2 (Optional) To create a new folder, do the following:

   a In the tree, select the parent folder in which you want to create the new folder.

   b Click **New Folder**.

   The **Create a New Folder** dialog box opens.

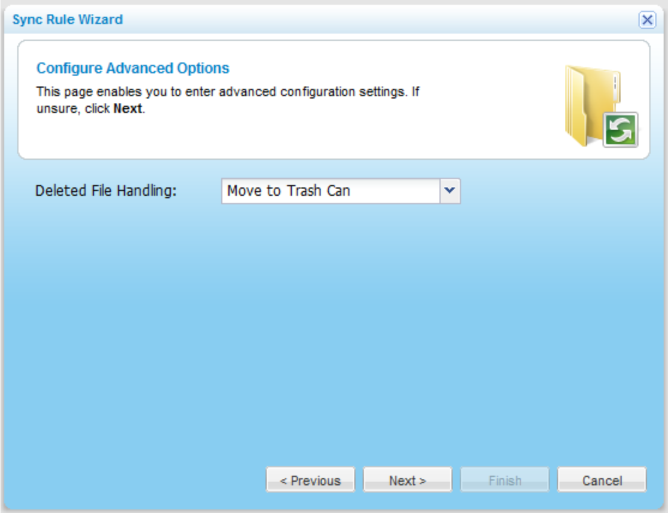
   c In the **Folder Name** field, type a name for the folder.

   d Click **Save**.

   A new folder is added to the selected parent folder.

3 Click **Next**.

The **Configure Advanced Options** dialog box appears.



4 In the **Deleted File Handling** field, specify how deleted files should be handled, by doing one of the following:

- To specify that files deleted in the source folder should be kept and not deleted in the destination folder, select **Keep Deleted Files**.

  For example, if you chose to synchronize a local folder to a remote server, and one of the files in the folder is deleted locally, the file will not be deleted on the remote server.

- To specify that files deleted in the source folder should be moved from the destination folder to the Recycle Bin, select **Move to Trash Can**.

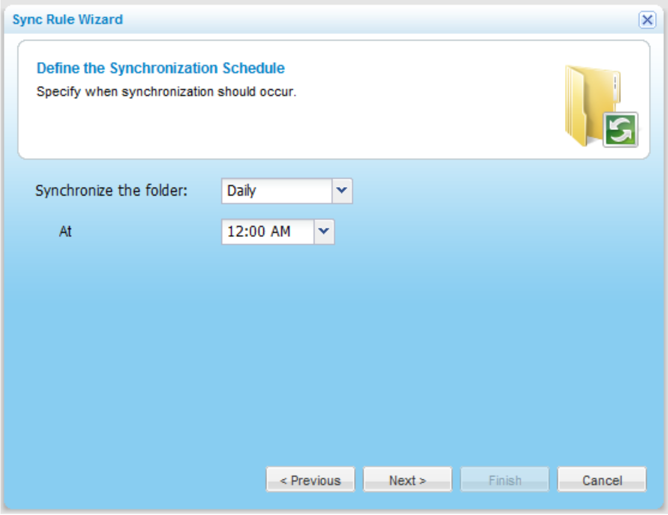
- To specify that files deleted in the source folder should be permanently deleted from the destination folder, select **Delete.**

5 Click **Next**.

6 Continue at ***Completing Synchronized Folder Configuration*** (page 208).

To complete sync rule configuration

The **Define the Synchronization Schedule** dialog box appears.

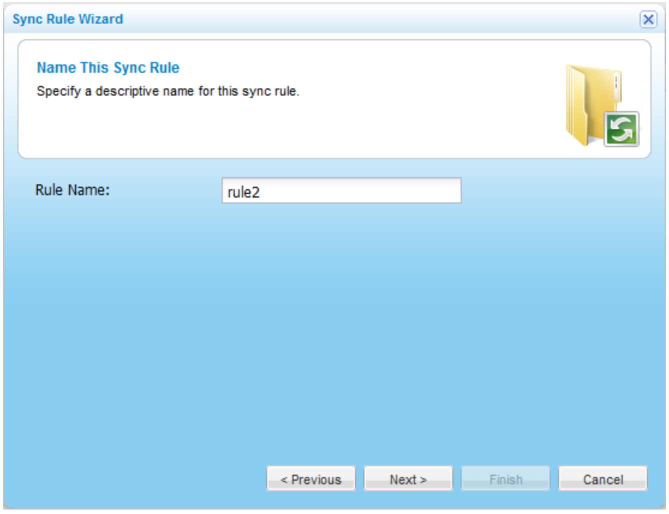


1 In the **Synchronize the Folder** field, select the frequency at which the folder should be synchronized.

2 In the fields that appear, use the controls provided to specify the exact day, date, or hour at which the folder should be synchronized.

3 Click **Next**.

The **Name This Sync Rule** dialog box appears.

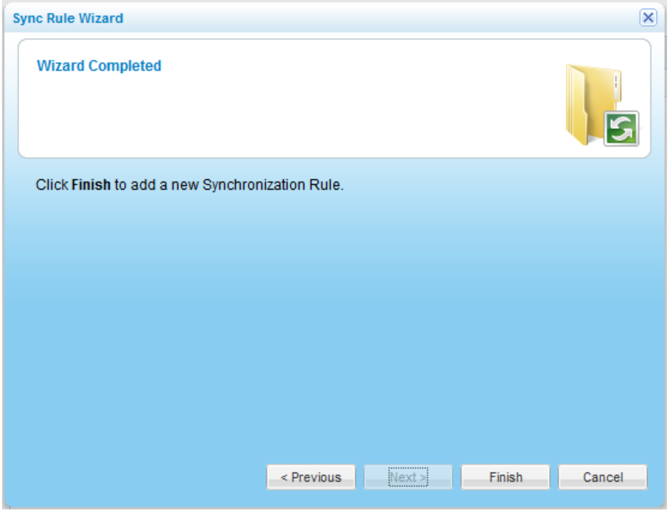


4 In the **Rule Name** field, type a name for the sync rule.

This name will appear in the synchronization logs.

5 Click **Next**.

The **Wizard Completed** screen appears.



6 Click **Finish**.

The sync rule is added for the specified folder, and appears in the **Synchronize > Sync Rules** page.

Deleting Sync Rules

To delete a sync rule

1 In the **Configuration** tab's navigation pane, click **Synchronize > Sync Rules**.

The **Synchronize > Sync Rules** page appears.

2 Select the desired rule and click **Delete**.

A confirmation message appears.

3 Click **Yes**.

The rule is deleted.

Manually Starting/Stopping Synchronization Operations

You can manually start synchronization at any time, and stop a running synchronization operation.

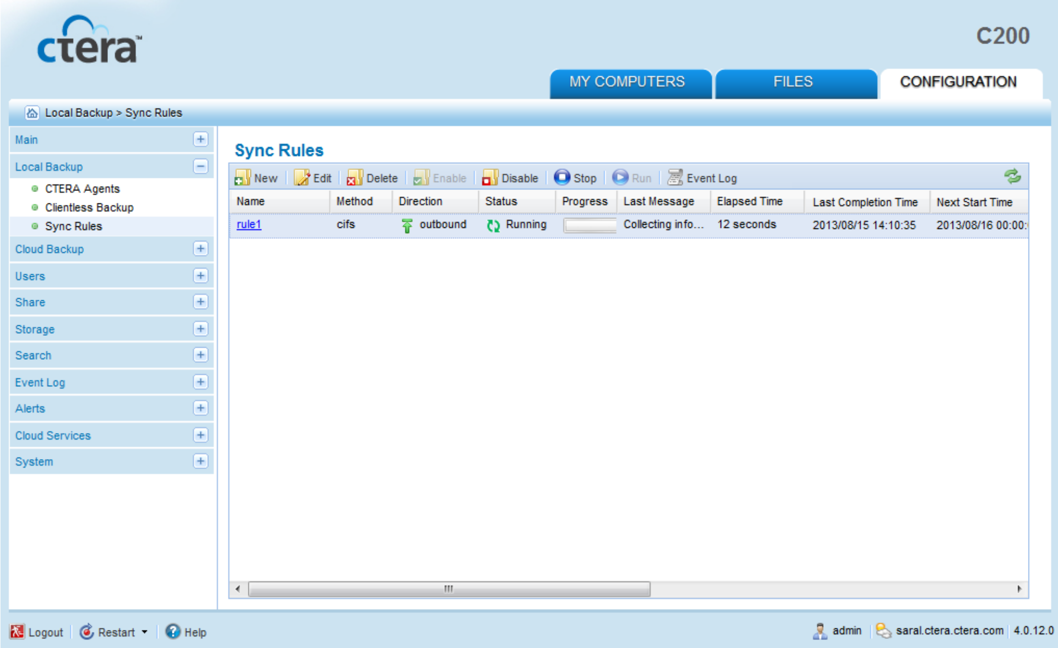
To manually start a synchronization operation

1 In the **Configuration** tab's navigation pane, click **Synchronize > Sync Rules**.

The **Synchronize > Sync Rules** page appears.

2 Select the desired rule, and click **Run**.

A progress bar appears, and the relevant folder is synchronized.



To stop a running synchronization operation

1 In the **Configuration** tab's navigation pane, click **Synchronize > Sync Rules**.

The **Synchronize > Sync Rules** page appears.

2 Select the rule for which synchronization is running, and click **Stop**.

The operation stops running.

Disabling/Enabling Sync Rules

You can disable a sync rule. If a synchronization operation is currently running for this rule, it will be suspended. In addition, all future scheduled synchronization operations for this rule will be suspended, until you enable it again.

To disable a sync rule

1 In the **Configuration** tab's navigation pane, click **Synchronize > Sync Rules**.

The **Synchronize > Sync Rules** page appears.

2 Select the desired sync rule, and click **Disable**.

The sync rule is disabled.

To enable a sync rule

1 In the **Configuration** tab's navigation pane, click **Synchronize > Sync Rules**.

The **Synchronize > Sync Rules** page appears.

2 Select the desired sync rule, and click **Enable**.

The sync rule is enabled.

12

Centrally Managing CTERA Agents

This chapter explains how to centrally manage CTERA Agents using the Web Interface.

Tip

For information on installing and using the CTERA Agent on PC, refer to the *CTERA Agent User Guide*.

In This Chapter

Overview

You can back up data from any computer on your network that is installed with the CTERA Agent, to a network share on the appliance. You can also use the CTERA Agent to easily backup roaming PCs or remote offices even when they are outside your network.

The CTERA Agent supports the following types of backup operations:

- **File-level backup**

File-level backup allows backing up files and folders from the CTERA Agent local interface to the appliance. The CTERA Agent can back up both unlocked and locked files.

In addition, you can back up the following server applications:

- Microsoft SQL Server
- Microsoft Exchange
- Microsoft Active Directory

Tip

Application backup utilizes Microsoft's Volume Shadow Copy Service (VSS). VSS enables backups that are point-in-time and application-level consistent.

The backed up files and applications can later be restored as needed.

- **Disk-level backup**

Disk-level backup, also known as "bare-metal backup", allows backing up an image of the CTERA Agent-installed computer's hard drives to the appliance. In case of an operating system error or a hard drive failure, the computer can be restored in full from the disk-level backup, returning the system to its exact state when the backup was performed. You can also restore disk-level backups to dissimilar hardware (provided it has sufficient disk space), and even to a virtual machine (VM).

When CTERA Agent is used in conjunction with CTERA's Cloud Backup, a copy of disk-level backups is stored offsite for complete disaster protection, while maintaining a local copy for fast restore. CTERA's advanced deduplication efficiently handles the disk-level backups, ensuring that only differences are sent over the Internet.

When CTERA Agent is used in conjunction with CTERA's NEXT3 snapshots, users can easily roll back to earlier versions of their disk-level images. NEXT3 ensures that only differences are stored between versions, thus greatly reducing the required storage space.

In Windows Server 2003, disk-level backups are stored in NTBACKUP format. In all other operating systems, disk-level backups are stored using the industry-standard Virtual Hard Disk (VHD) file format. VHD files can be mounted using standard tools to allow extraction of individual files and folders, and it is even possible to run the VHD disk image on a virtual machine (VM) for immediate disaster recovery after hardware failures. For information on restoring files from disk-level backup, see Restoring Files from Disk-Level Backup.

Tip

Disk-level backup operates over the Windows File Sharing protocol (CIFS). To perform disk-level backups, ensure that the computer running CTERA Agent has access to the appliance using Windows File Sharing.

Tip

Disk-level backup does not support backing up volumes larger than 2TB.

- **System state backup**

  System state backup, available on Windows 2003 Server only, creates a backup file for critical system-related components. The system state data includes the registry, COM+ Class Registration database, files under Windows File Protection, and system boot files. Depending on the server's configuration, additional data may be included in the system state data, as well. For example, if the server is a certificate server, the system state will also contain the Certificate Services database. If the server is a domain controller, Active Directory and the SYSVOL directory are also included in the system state data.

  The system state backup is stored in NTBACKUP format, and the Microsoft NTBACKUP tool can be used to recover the system state from the backup file. For information on restoring your system from a system state backup, see Restoring from a System State Backup on Windows 2003 Server SP2.

Traffic generated by CTERA Agent backup operations of any type can be secured with Secure Socket Layer (SSL) encryption.

CTERA Agents can be remotely managed and monitored from the appliance Web interface. For information, see ***Centrally Managing CTERA Agents*** (on page 213).

Agent Licensing

CTERA Agent is licensed differently, depending on your operating system:

Table 41: Agent Licensing per Operating System

When installed on this OS...	The CTERA Agent is licensed as a...
Windows Server	CTERA Server Agent
Other Windows operating systems	CTERA Workstation Agent
Linux	CTERA Server Agent
Mac OS-X	CTERA Workstation Agent

Both agent types offer the same functionality.

CTERA Agent licenses are taken from the licenses included in your appliance. Licenses that exceed the number included in your appliance are taken from the workstation agent/server agent quotas allocated to your CTERA Portal account. A license is taken for as long as an agent is defined in your appliance. If you are no longer using an agent, as an administrator, you can delete the agent from the appliance using the CTERA Agent Manager.

Table 42: Agent Licenses Included with Your Appliance

Appliance Model	Included Workstation Agents	Included Server Agents
C200	20	0
C400	50	0
C800	50	0

For licensing of additional server or workstation agents, contact your CTERA-authorized reseller.

Workflow

Central management of CTERA Agents is performed in the appliance Web interface.

To centrally manage CTERA Agents, do the following:

1. Configure global settings for all CTERA Agents.

   See ***Configuring Global Settings for All CTERA Agents*** (on page 220).

2. If local configuration of the agent is disabled, do the following:

   a. Configure the agent-specific settings for the CTERA Agent.

See ***Configuring the Agent*** (on page 231).

b If you did not select files and folders for file-level backup while configuring the CTERA Agent's settings (in the previous step), then select the files and folders that should be included in local backup operations.

See ***Selecting Files and Folders for File-Level Backup*** (on page 240).

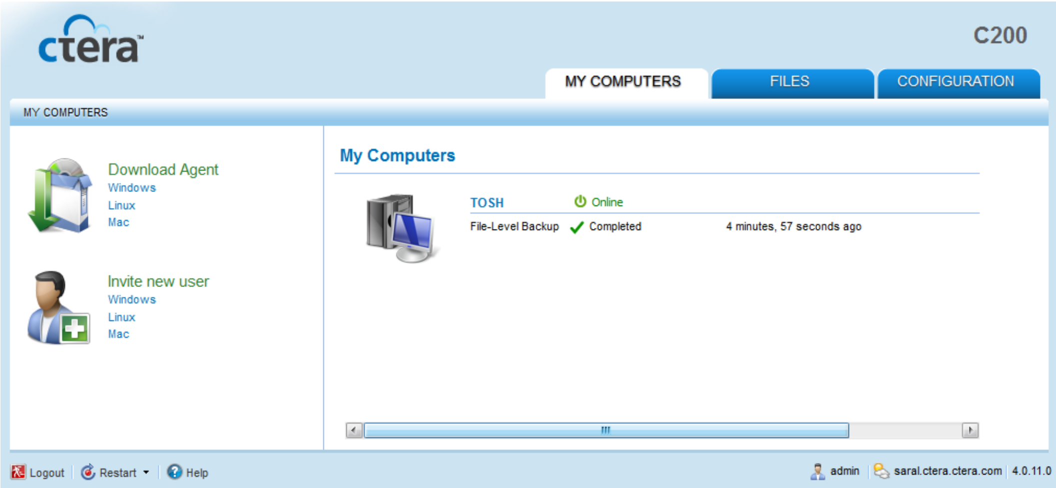
Local configuration is controlled by the **Allow user to configure the agent** check box in the CTERA Agent global settings.

Downloading and Installing CTERA Agent

To download and install CTERA agent

1. Click the **My Computers** tab.

   The My Computers page appears.

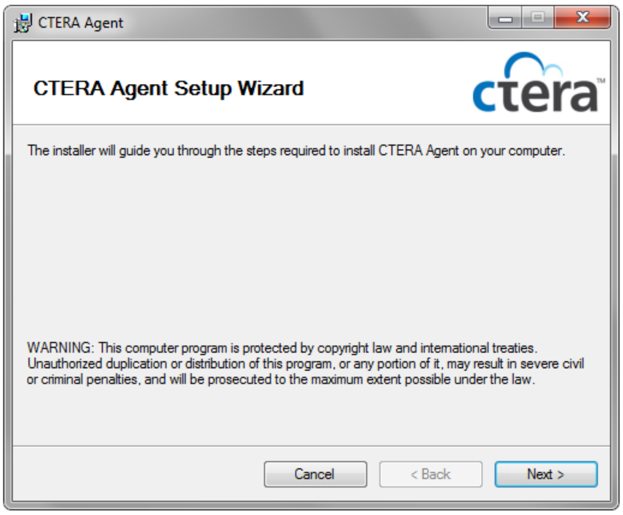


2. Under **Download Agent**, click **Windows**.

   The CTERA Agent installer is downloaded to your computer.

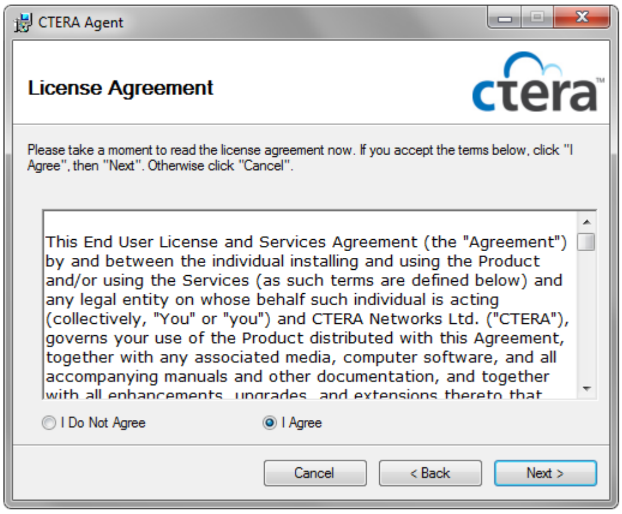
3. Double-click on the installer file.

The **CTERA Agent Setup Wizard** opens, displaying the **CTERA Agent Setup Wizard** screen.



4 Click **Next**.

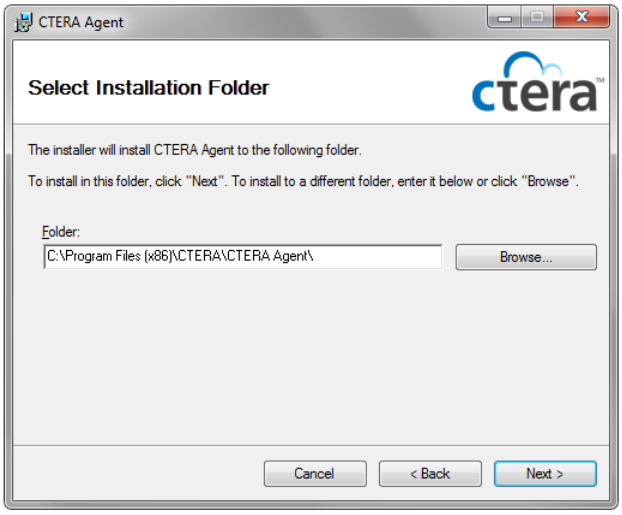
The **License Agreement** dialog box appears.



5 Choose **I Agree**.

6 Click **Next**.

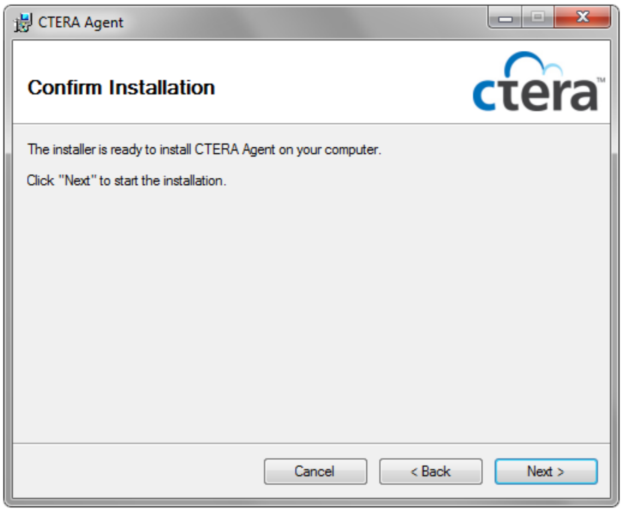
The **Select Installation Folder** dialog box appears.



7 Click **Browse** and browse to the folder in where the CTERA Agent should be installed.

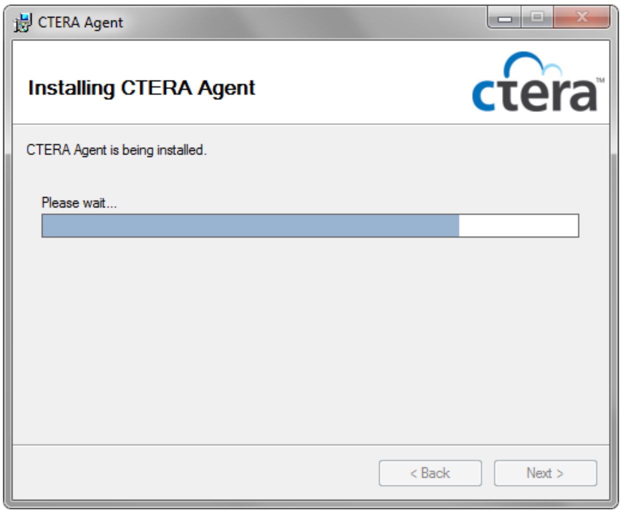
8 Click **Next**.

The **Confirm Installation** screen appears.

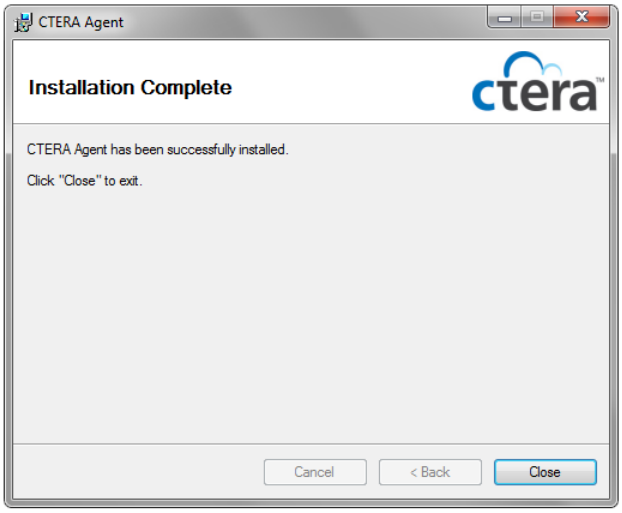


9 Click **Next**.

The **Installing CTERA Agent** screen appears with a progress bar, and the CTERA Agent is installed on your computer.



The **Installation Complete** screen appears.



10 Click **Close**.

CTERA Agent is added to the Windows Start menu, and an icon is added to the Windows taskbar.

Configuring Global Settings for All CTERA Agents

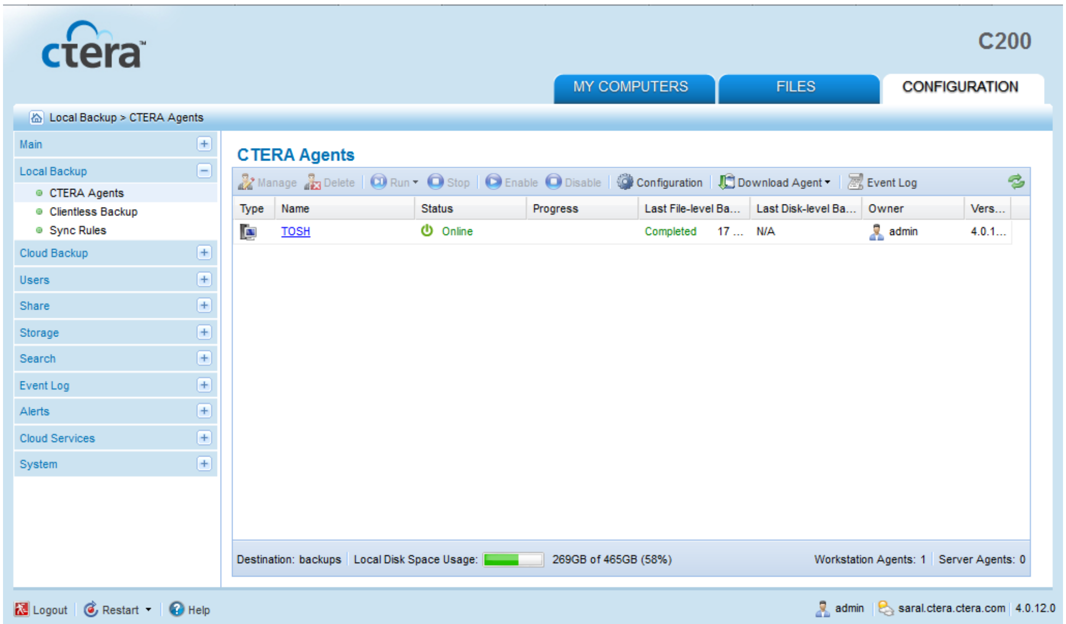
Global configuration settings include automatic file-level and disk-level backup scheduling, selection of the target network share on the appliance, file types that should be backed up, and more.

Configuring Global General Settings

To configure global general settings for all CTERA Agents

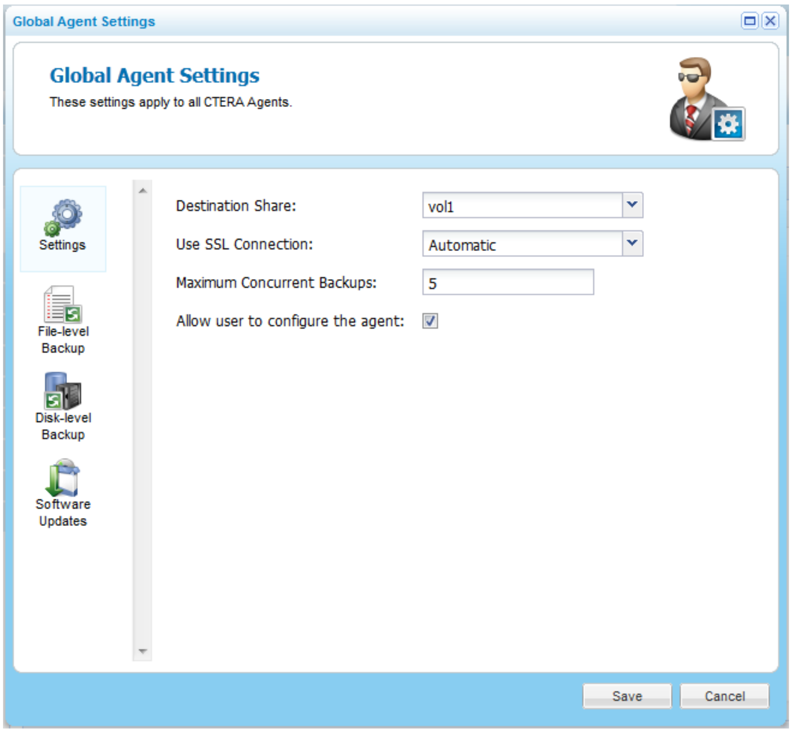
1 In the **Configuration** tab's navigation pane, click **Local Backup > CTERA Agents**.

The **Local Backup > CTERA Agents** page appears.



2 Click **Configuration**.

The **Global Agents Settings** window opens displaying the **Settings** tab.



3. Complete the fields using the information in General Settings Fields.
4. Click **Save**.

Table 43: General Settings Fields

In this field...	Do this...
Destination Share	Select the local appliance network share with which the files and folders from the CTERA Agent-enabled computer should be backed up. Subdirectories will automatically be created under this network share for each backed up folder.
Use SSL Connection	Specify whether to use Secure Socket Layer (SSL) encryption for connections from the CTERA Agent to the appliance: - **Enabled**. The CTERA Agent will use SSL. - **Disabled**. The CTERA Agent will not use SSL. - **Automatic**. The CTERA Agent will not use SSL when in the same LAN as the appliance, and will use SSL when they are not in the same LAN as the appliance. The default value is **Automatic**.
Maximum Concurrent Backups	Type the maximum number of backups that can occur at the same time. **Note**: If the number of CTERA Agents concurrently attempting to perform a backup operation exceeds this limit, each agent over the limit will wait for the number of concurrent backups to drop below this threshold, before commencing its own backup operation. The default value for the C200 is 10, and the default value for the C400 and C800 is 25.
Allow user to configure the agent	Select this option to allow CTERA Agent users to configure their own agent. In order for CTERA Agent users to manage their own agents, this option must be selected, *and* the CTERA Agent users must have the "Back up files and directories" privilege on Windows, or be members of the "ctera" user group on Linux or Mac OS-X. For further information, refer to the *CTERA Agent User Guide*. **Note**: When this option is cleared, selecting files for local backup can only be done by an administrator in the appliance Web interface. The CTERA Agent user cannot select files for backup locally, nor can they configure agent settings via the appliance Web interface. However, the user can still initiate backup and restore operations.

Configuring Global File-Level Backup Settings

To configure global file-level settings for all CTERA Agents

1. In the **Configuration** tab's navigation pane, click **Local Backup > CTERA Agents**.

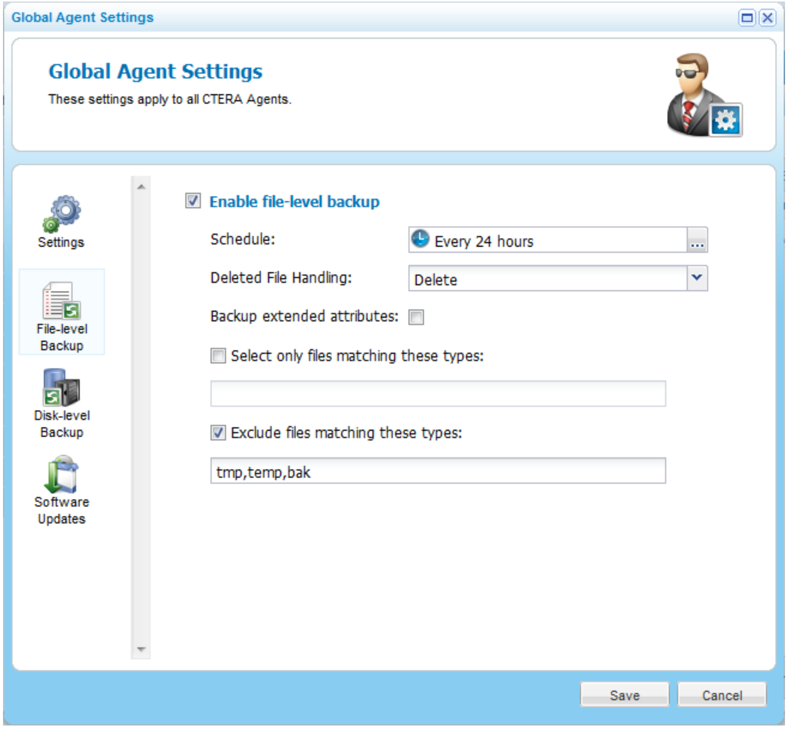
   The **Local Backup > CTERA Agents** page appears.

2. Click **Configuration**.

   The **Global Agents Settings** window opens displaying the **Settings** tab.

3. Click the **File-level Backup** tab.

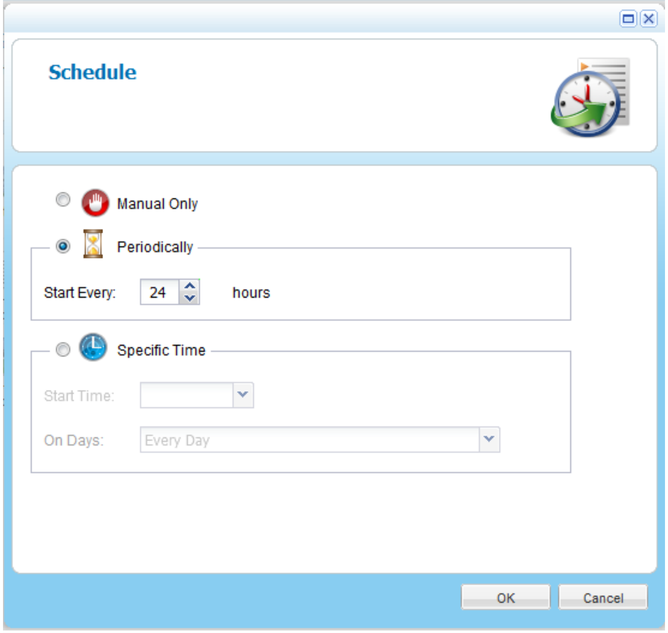
   The **File-level Backup** tab appears.



4. To schedule file-level backup, do the following:

   a. In the **Schedule** field, click .

The **Schedule** dialog box appears.



b Complete the fields using the information in ***Schedule Fields*** (page 227).

c Click **OK**.

The default file-level backup value is **Every 24 hours**.

5. Complete the remaining fields using the information in ***General Settings File-Level Backup Fields*** (page 226).
6. Click **Save**.

Table 44: General Settings File-Level Backup Fields

In this field...	Do this...
Deleted File Handling	Specify how deleted files should be handled, by selecting one of the following: - **Keep Deleted Files**. Files deleted in the source folder should be kept and not deleted in the destination folder. For example, if one of the files in the folder is deleted on the CTERA Agent-enabled computer, the file will not be deleted from the appliance network share. - **Move to Trash Can**. Files deleted in the source folder should be moved from the destination folder to the Recycle Bin, which is a special folder named ".Trash". - **Delete**. Files deleted in the source folder should be permanently deleted from the destination folder. The default value is **Delete**.
Backup extended attributes	Select this option to back up special file permissions and metadata. This is supported only if the target volume is of the EXT3/NEXT3 type.
Select only files matching these types	To specify that only files of certain types should be included in local backup operations, select this option, and then type the relevant file extensions in the field provided. The file extensions must be separated by commas. For example: doc,docx,docm,dotx,dotm
Exclude files matching these types	To specify that files of certain types should be excluded from local backup operations, select this option, and then type the relevant file extensions in the field provided. The file extensions must be separated by commas. For example: tmp,temp,bak

Table 45: File-Level Backup Tab Fields

In this field...	Do this...
Manual Only	Choose this option to disable automatic backups.
Periodically	Choose this option to specify that automatic backups should be performed every certain number of hours. The **Start Every** field is enabled, and you must complete it.
Start Every	Use the arrows to specify the interval between backups, in hours.
Specific Time	Choose this option to specify that automatic backups should be performed at a certain hour on certain days. The **Start Time** and **On Days** fields are enabled, and you must complete them.
Start Time	Select the hour at which backups should start.
On Days	Specify on which days backups should occur, by selecting the relevant check boxes or clicking **Every Day**.

Configuring Global Disk-Level Backup Settings

To configure global disk-level settings for all CTERA Agents

1. In the **Configuration** tab's navigation pane, click **Local Backup > CTERA Agents**.

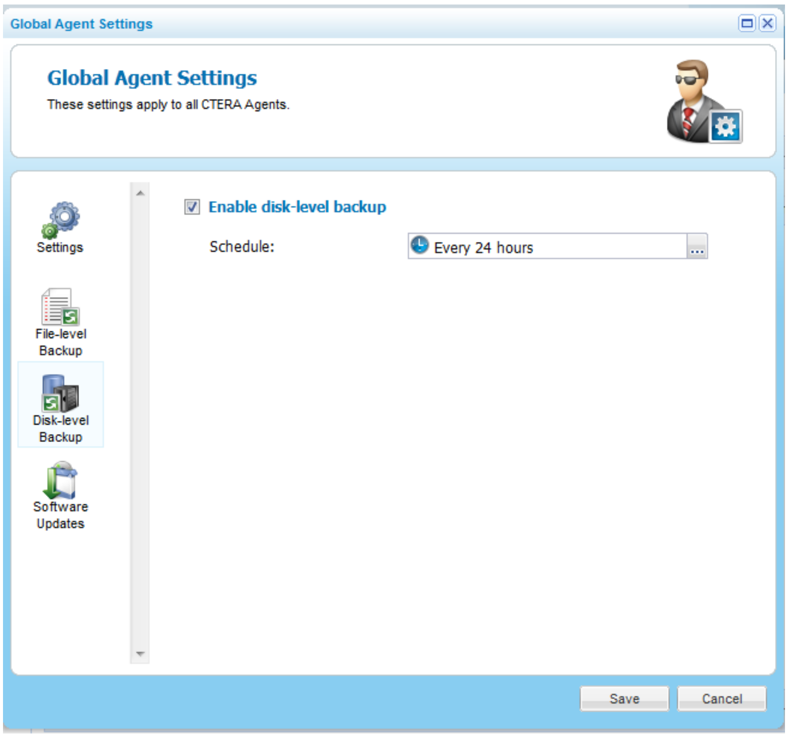
   The **Local Backup > CTERA Agents** page appears.

2. Click **Configuration**.

   The **Global Agents Settings** window opens displaying the **Settings** tab.

3. Click the **Disk-level Backup** tab.

The **Disk-level Backup** tab appears.



4 Select the **Enable disk-level backup** check box.

The **Schedule** field is enabled.

5 To schedule disk-level backup, do the following:

a In the **Schedule** field, click .

The **Schedule** dialog box appears.

b Complete the fields using the information in ***Schedule Fields*** (page 227).

c Click **OK**.

The default disk-level backup value is **Every 24 hours**.

6 Click **Save**.

Configuring Global Software Update Settings

You can configure connected CTERA Agents to automatically download and install software updates. The software updates are downloaded from the CTERA Portal to the appliance, and then the appliance distributes them to connected agents.

Tip

In order to provide automatic software updates to CTERA Agents, the appliance must be connected to cloud services.

To configure global software update settings for all CTERA Agents

1 In the **Configuration** tab's navigation pane, click **Local Backup > CTERA Agents**.

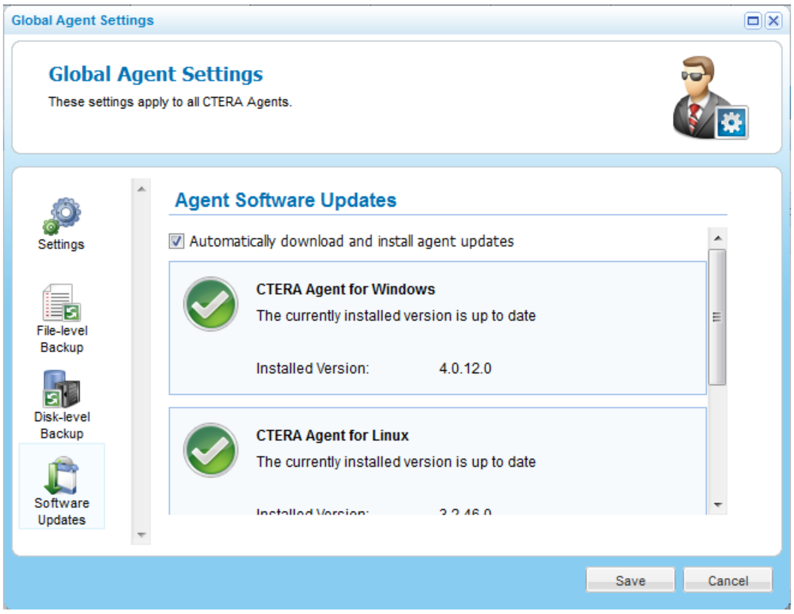
The **Local Backup > CTERA Agents** page appears.

2 Click **Configuration**.

The **Global Agents Settings** window opens displaying the **Settings** tab.

3 Click the **Software Updates** tab.

The **Software Updates** tab appears.



4 Select the **Automatically download and install agent updates** check box.

5 Click **Save**.

Opening the CTERA Agent Manager

The CTERA Agent Manager is used to perform numerous agent-specific tasks in the appliance Web interface.

To open the CTERA Agent Manager

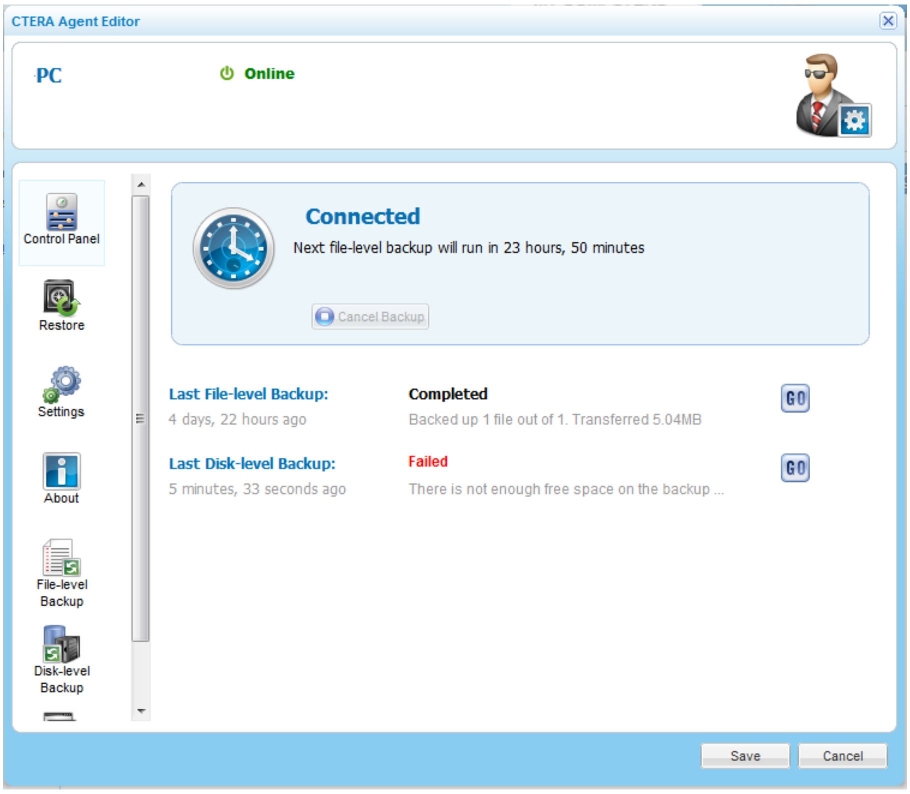
- Do one of the following:
  - In the **Configuration** tab's navigation pane's **Local Backup > CTERA Agents** page, click the desired CTERA Agent's name.

    This can be done by administrators only.
  - In the **My Computers** tab, click **Manage** next to the desired CTERA Agent's name.

    This can be done both by administrators and by end users who want to manage their own CTERA Agent.

    End users can manage their own agents only if the administrator enabled the **Allow end users to configure the agent** option.

The CTERA Agent Manager opens displaying the **Control Panel** tab.



Tip

In order to remotely manage the CTERA Agent, it must be connected to the appliance.

Configuring the Agent

By default, each CTERA Agent inherits settings from the global settings for all CTERA Agents. If desired, you can override the global settings, as well as configure the following agent-specific settings:

- Enable file-level backup for the agent
- Files and folders to back up during file-level backup
- Applications to back up during file-level backup
- Volumes to back up during disk-level backup
- Configure system state backup
- Configure integration with Windows Explorer (relevant for CTERA Agents on Windows only)

Tip

If the **Allow user to configure the agent** check box is selected in the global settings for all CTERA Agents (see ***Configuring Global Settings for All CTERA Agents*** (on page 220)), non-administrative users can centrally manage their own agents using the appliance Web interface. See Configuring the Agent.

Configuring General Settings

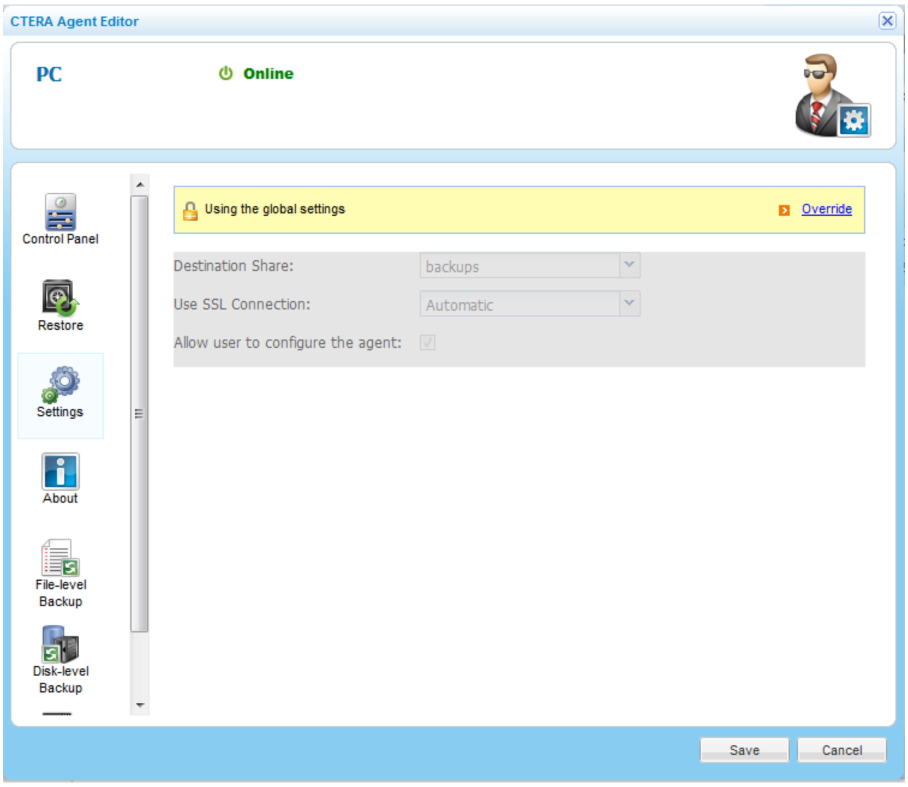
To configure general settings

1 Open the CTERA Agent Manager.

See ***Opening the CTERA Agent Manager*** (on page 230).

2 Click the **Settings** tab.

The **Settings** tab appears.



3 Click **Override**, to override the global general settings.

Tip

You can revert to global general settings at any time, by clicking **Use global settings**.

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

5 Click **Save**.

General Settings Fields

Table 46: General Settings Fields

In this field...	Do this...
Destination Share	Select the local appliance network share with which the files and folders from the CTERA Agent-enabled computer should be backed up. Subdirectories will automatically be created under this network share for each backed up folder.
Use SSL Connection	Specify whether to use Secure Socket Layer (SSL) encryption for connections from the CTERA Agent to the appliance: - **Enabled**. The CTERA Agent will use SSL. - **Disabled**. The CTERA Agent will not use SSL. - **Automatic**. The CTERA Agent will not use SSL when in the same LAN as the appliance, and will use SSL when they are not in the same LAN as the appliance. The default value is **Automatic**.
Allow user to configure the agent	Select this option to allow CTERA Agent users to configure their own agent. In order for CTERA Agent users to manage their own agents, this option must be selected, *and* the CTERA Agent users must have the "Back up files and directories" privilege on Windows, or be members of the "ctera" user group on Linux or Mac OS-X. For further information, refer to the *CTERA Agent User Guide*. **Note**: When this option is cleared, selecting files for local backup can only be done by an administrator in the appliance Web interface. The CTERA Agent user cannot select files for backup locally, nor can they configure agent settings via the appliance Web interface. However, the user can still initiate backup and restore operations.

Configuring File-Level Backup Settings

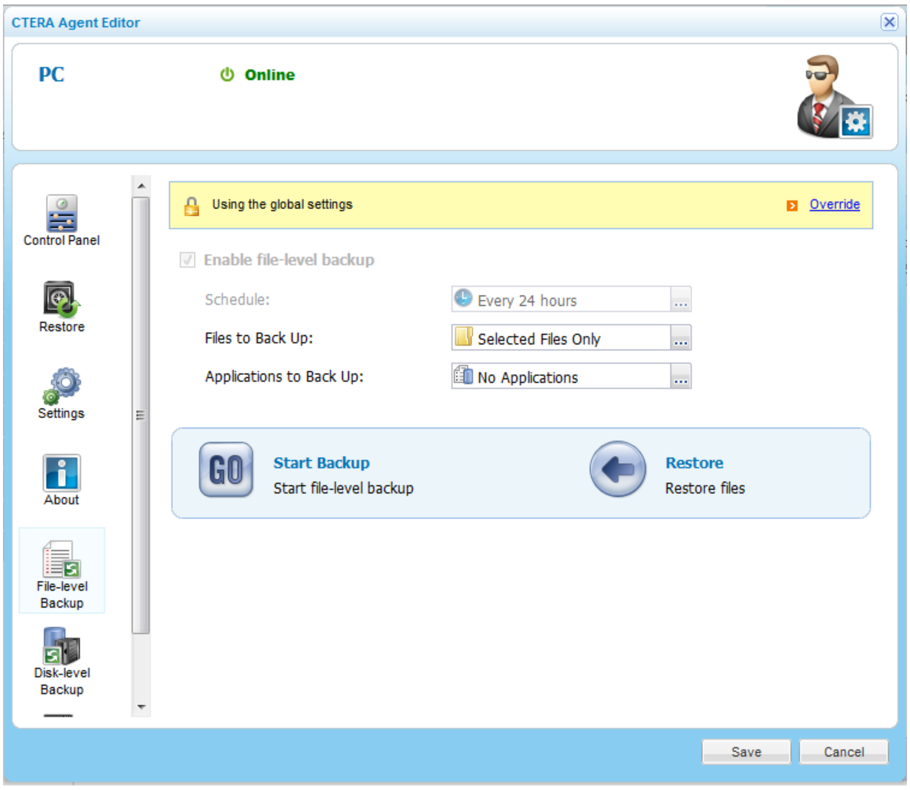
To configure file-level backup settings

1. Open the CTERA Agent Manager.

   See ***Opening the CTERA Agent Manager*** (on page 230).

2. Click the **File-level Backup** tab.

The **File-level Backup** tab appears.



3 To override the global settings for file-level backup, click **Override**.

Global settings include the file-level backup schedule.

Tip

You can revert to global file-level backup settings at any time, by clicking **Use global settings**.

4 To enable file-level backup, select the **Enable file-level backup** check box.

5 To schedule file-level backup, do the following:

a In the **Schedule** field, click ... .

The **Schedule** dialog box appears.

b Complete the fields using the information in ***Schedule Fields*** (page 227).

c Click **OK**.

The default file-level backup value is **Every 24 hours**.

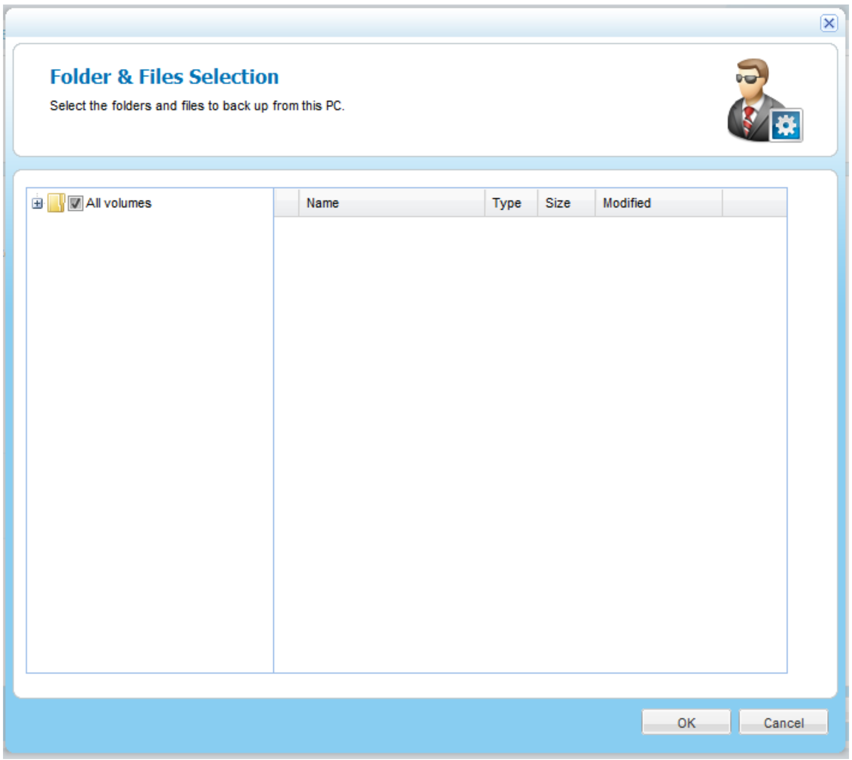
6 To select files and folders for backup, do the following:

Tip

You can also select files and folder for backup on the CTERA Agent installed computer. For information, see Selecting Files and Folders for File-Level Backup.

a In the **Files to Back Up** field, click .

The **Folder & Files Selection** window opens.



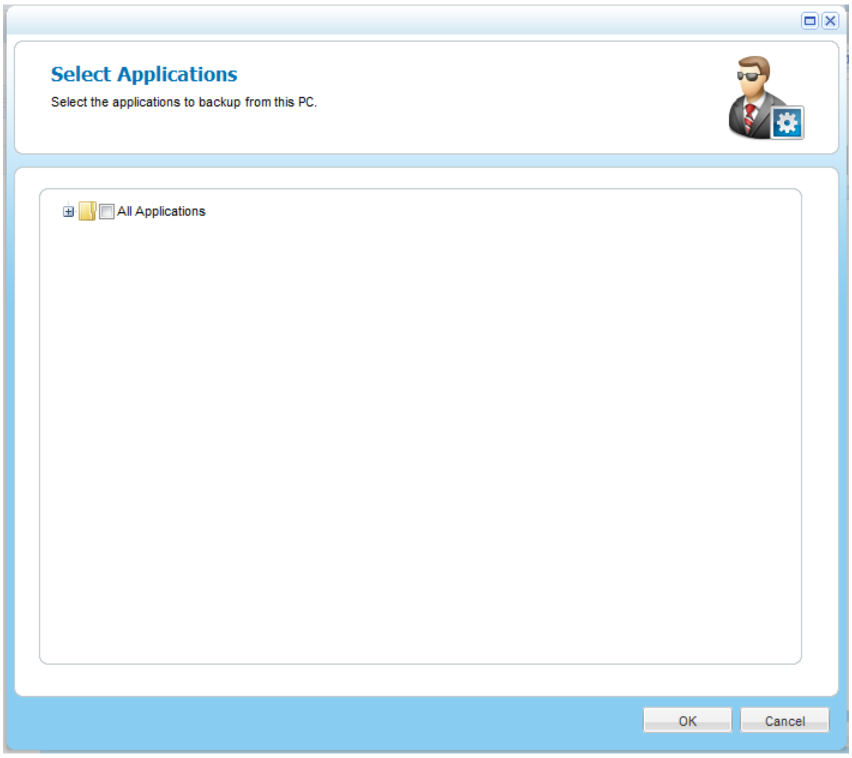
b Expand the tree nodes and select the check boxes next to the folders and files you want to back up.

c Click **OK**.

7 To select applications for backup, do the following:

a In the **Applications to Back Up** field, click .

The **Select Applications** window opens.



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

c Click **OK**.

8 Click **Save**.

At the bottom of the workspace, the **Destination** field indicates the folder on the appliance to which files will be backed up. The **Local Disk Space Usage** field indicates the amount of used space on the disk after the next local backup operation, out of the total amount of space available on the disk.

Configuring Disk-Level Backup Settings

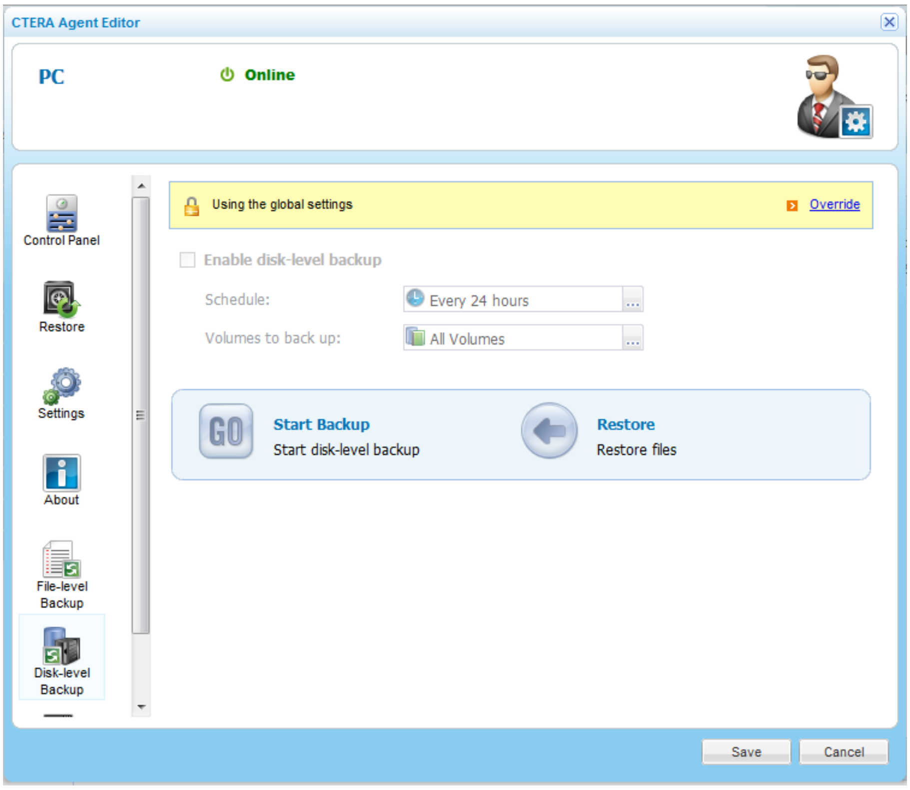
To configure disk-level backup settings

1 Open the CTERA Agent Manager.

See ***Opening the CTERA Agent Manager*** (on page 230).

2 Click the **Disk-level Backup** tab.

The **Disk-level Backup** tab appears.



3 Click **Override**, to override the global settings for disk-level backup.

Global settings include whether disk-level backup is enabled, as well as the disk-level backup schedule.

Tip

You can revert to global disk-level backup settings at any time, by clicking **Use global settings**.

4 Select the **Enable disk-level backup** check box.

5 To schedule disk-level backup, do the following:

a In the **Schedule** field, click .

The **Schedule** dialog box appears.

b Complete the fields using the information in ***Schedule Fields*** (page 227).

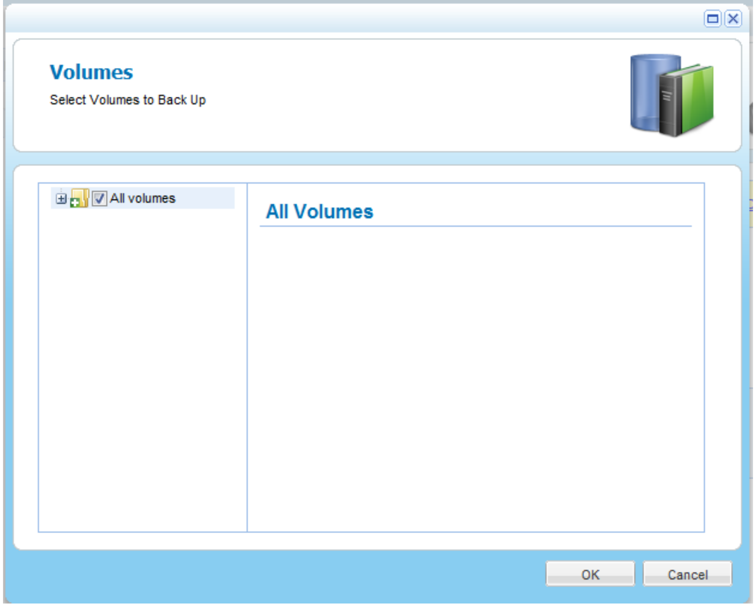
c Click **OK**.

The default disk-level backup value is **Every 24 hours**.

6 To select volumes for backup, do the following:

a In the **Volumes to back up** field, click .

The **Volumes** window opens.



b Expand the tree nodes and select the check boxes next to the volumes you want to back up.

For an explanation of the icons and check boxes next to each folder, see ***Folder Icons*** (page 156).

c Click **OK**.

7 Click **Save**.

Configuring System State Backup Settings

System state backup is performed as a type of file-level backup.

To configure system state backup settings

- Perform file-level backup, and select **System State** as a backup application.

  See ***Configuring File-Level Backup Settings*** (on page 233).

Configuring Windows Explorer Integration Settings

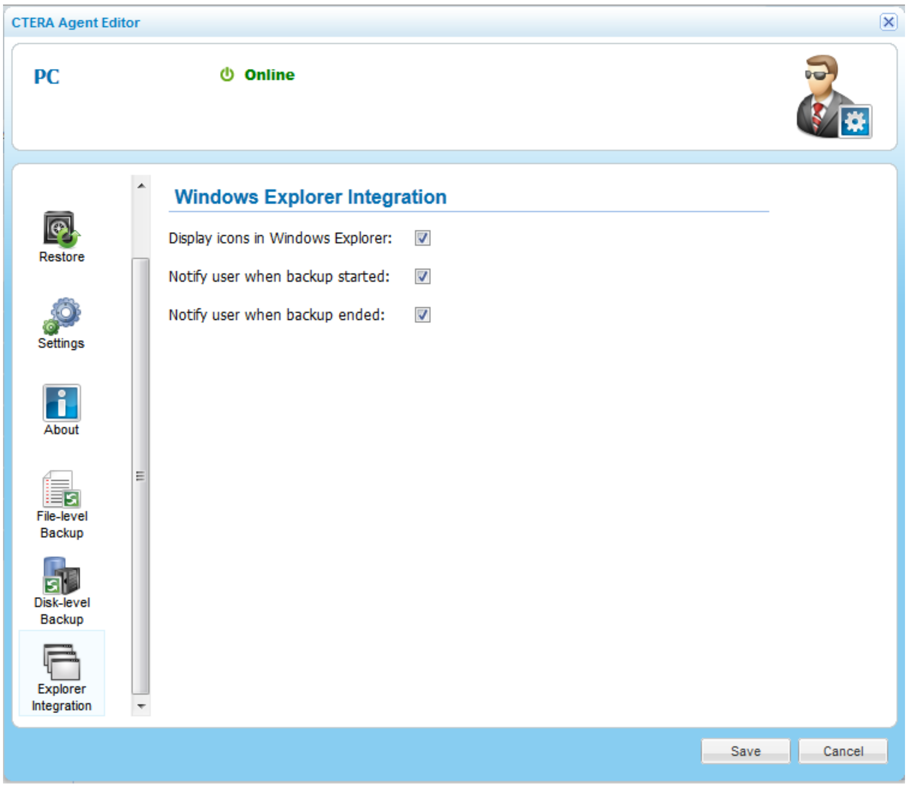
To configure Windows Explorer integration settings

1. Open the CTERA Agent Manager.

   See ***Opening the CTERA Agent Manager*** (on page 230).

2. Click the **Explorer Integration** tab.

The **Explorer Integration** tab appears.



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

4 Click **Save**.

Table 47: CTERA Agent Explorer Integration Fields

In this field...	Do this...
Display icons in Windows Explorer	Select this option to display CTERA backup icons in Windows Explorer. Files and folders that are selected for backup will be marked with the icon in Windows Explorer. Folders for which only part of the contents are selected for backup will be marked with the icon.
Notify user when backup started	Select this option to display a pop-up notification above the CTERA Agent tray icon, when backup starts.
Notify user when backup ended	Select this option to display a pop-up notification above the CTERA Agent tray icon, when backup ends.

Selecting Files and Folders for File-Level Backup

You can select files and folder for file-level backup for individual CTERA Agents.

Tip

If the **Allow user to configure the agent** check box is selected in the global settings for all CTERA Agents, files and folders for file-level backup can be selected in the CTERA Agent local interface. See ***Configuring Global Settings for All CTERA Agents*** (on page 220) and Configuring the Agent.

To select files and folders for file-level backup

1 Open the CTERA Agent Manager.

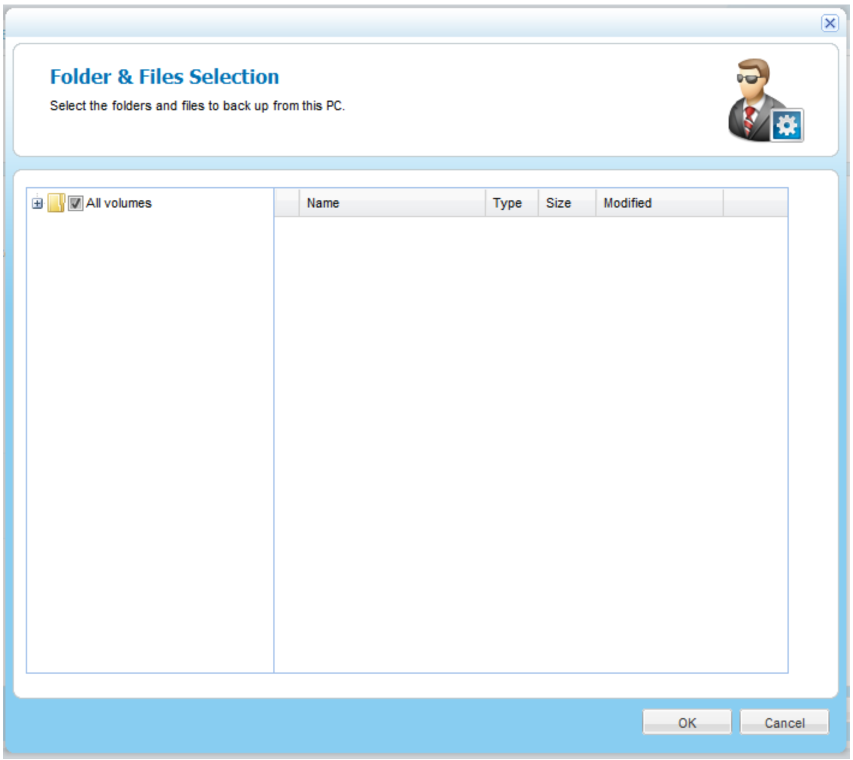
See ***Opening the CTERA Agent Manager*** (on page 230).

2 Click the **File-level Backup** tab.

The **File-level Backup** tab appears.

3 In the **Files to Back Up** field, click ... .

The **Folder & Files Selection** window opens.



4 Expand the tree nodes and select the check boxes next to the folders and files you want to back up.

5 Click **OK**.

6 Click **Save**.

At the bottom of the workspace, the **Destination** field indicates the folder on the appliance to which files will be backed up. The **Local Disk Space Usage** field indicates the amount of used space on the disk after the next local backup operation, out of the total amount of space available on the disk.

Manually Starting Agent Backup

The CTERA Agent will automatically back up files, applications, and volumes to the appliance according to the schedule configured on the appliance. If desired, you can manually trigger backup at any time.

To manually start backup from the CTERA Agents page

1. In the **Configuration** tab's navigation pane, click **Local Backup > CTERA Agents**.

   The **Local Backup > CTERA Agents** page appears.

2. Select the desired CTERA Agent.
3. In the **Run** drop-down list, click the desired backup type.

   The CTERA Agent's status changes to Running, and a progress bar appears.

   The CTERA Agent backs up files to the appliance.

To manually start backup from the CTERA Agent Manager

1. Open the CTERA Agent Manager.

   See ***Opening the CTERA Agent Manager*** (on page 230).

2. Next to the desired backup type, click **Go**.

   A progress bar appears.

   The CTERA Agent backs up files to the appliance.

Stopping the Current Backup Operation of an Agent

To stop the current backup operation from the CTERA Agents page

1. In the **Configuration** tab's navigation pane, click **Local Backup > CTERA Agents**.

   The **Local Backup > CTERA Agents** page appears.

2. Select the desired CTERA Agent.
3. Click **Stop**.

   The current backup operation is stopped.

To stop the current backup operation from the CTERA Agent Manager

1. Open the CTERA Agent Manager.

   See ***Opening the CTERA Agent Manager*** (on page 230).

2. Click **Cancel Backup**.

   The current backup operation is stopped.

Disabling and Enabling Agent Backups

You can disable local backup for a CTERA Agent, including:

- The currently running local backup for the CTERA Agent
- All scheduled automatic local backups for the CTERA Agent

When an agent is disabled, it remains connected and can still be managed centrally; however, no backups are performed.

To disable local backup for an agent

1. In the **Configuration** tab's navigation pane, click **Local Backup > CTERA Agents**.

   The **Local Backup > CTERA Agents** page appears.

2. Select the desired CTERA Agent.
3. Click **Disable**.

   If local backup is currently running, it is paused. All future automatic backups for the CTERA Agent are suspended.

   The CTERA Agent's status changes to **Disabled**.

To enable local backup for an agent

1. In the **Configuration** tab's navigation pane, click **Local Backup > CTERA Agents**.

   The **Local Backup > CTERA Agents** page appears.

2. Select the desired CTERA Agent.
3. Click **Enable**.

   Local backup resumes.

   The CTERA Agent's status changes to **Online**.

Viewing Agent Backups

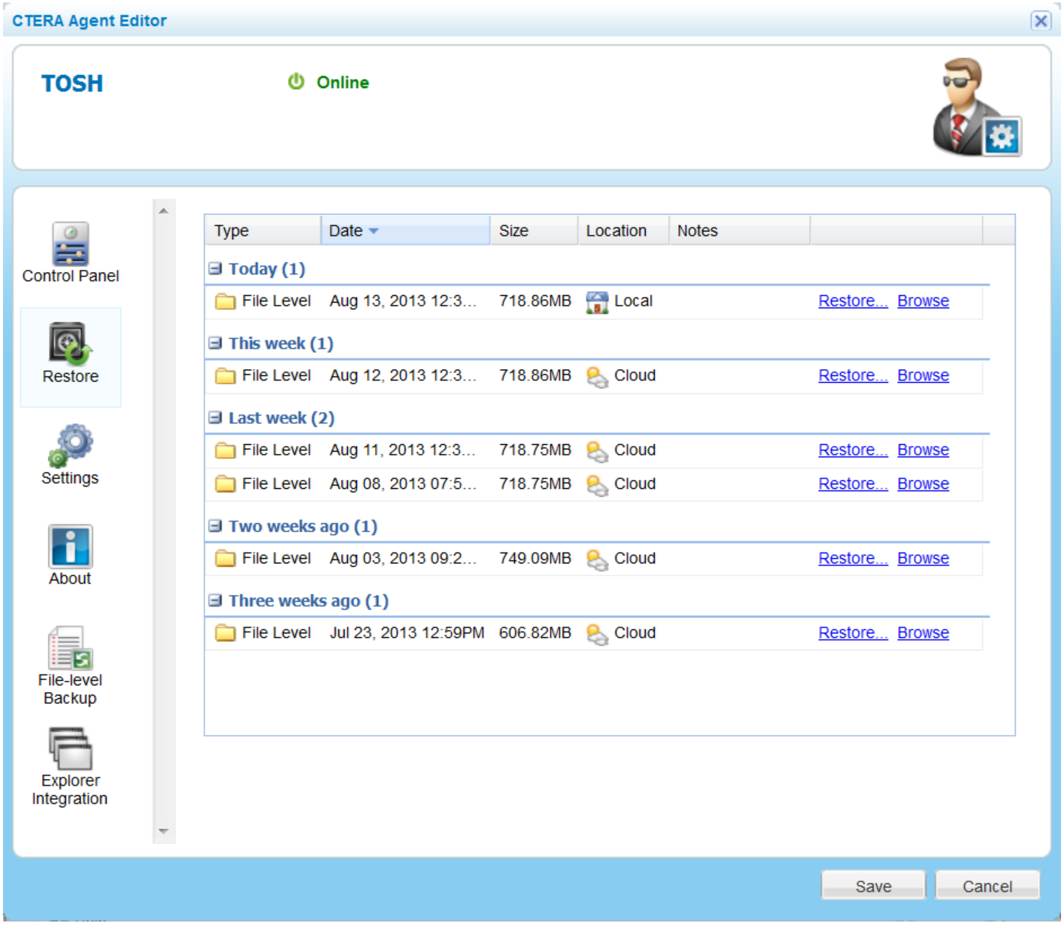
To view CTERA Agent backups

1 Open the CTERA Agent Manager.

See ***Opening the CTERA Agent Manager*** (on page 230).

2 Click the **Restore** tab.

The **Restore** tab appears with a table of backups for the agent.



The **Location** field specifies whether the backup is stored locally in a NEXT3 snapshot ( ) or in the cloud ( ). Accessing local snapshots is faster.

3 To view the files included in a backup, click the **Browse** link for the desired backup.

The **Files** tab opens displaying the files.

Restoring Files and Folders from the Appliance to the Agent

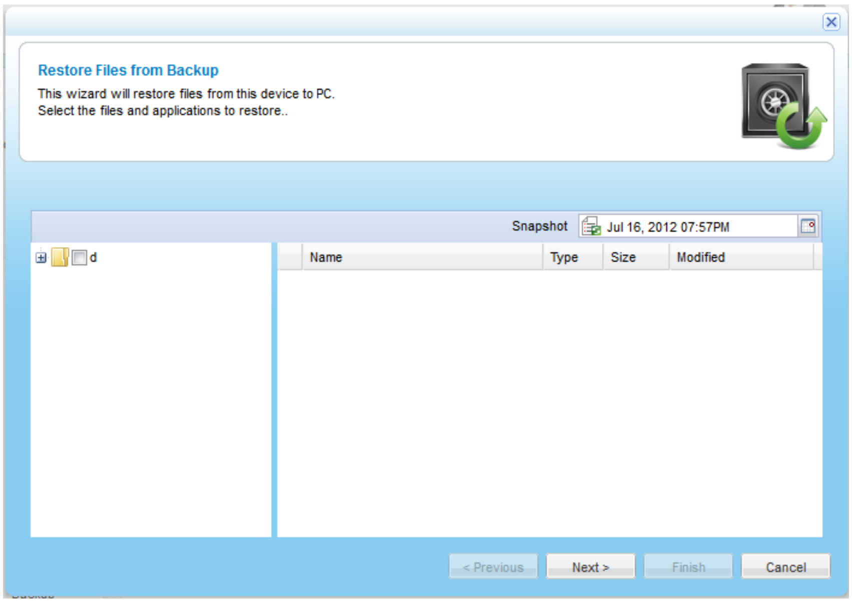
To restore files and folders

1. View CTERA Agent backups.

   See ***Viewing Agent Backups*** (on page 243).

2. Next to the desired backup, click **Restore**.

   The **Restore Files from Backup Wizard** opens.



3. To view a folder's contents, select the folder in the left pane.

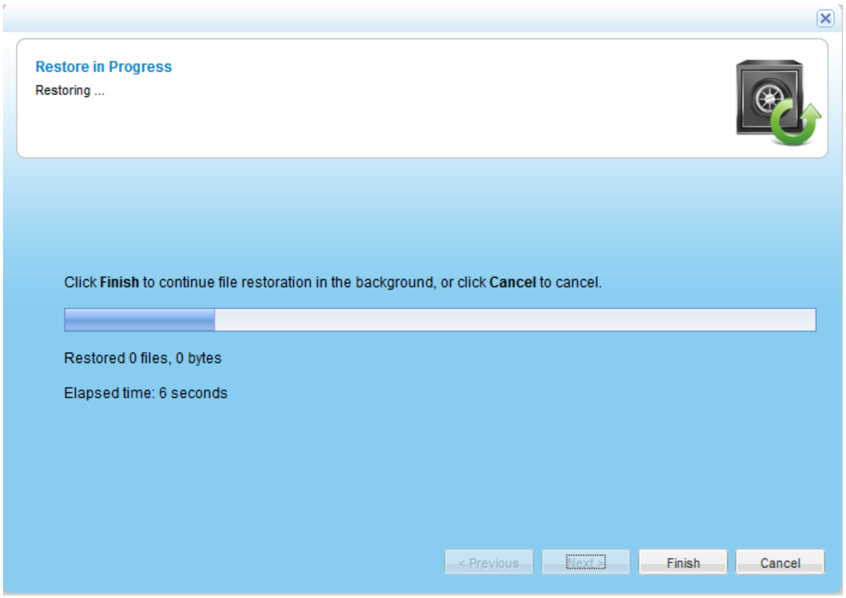
   The selected folder's contents appear in the right pane.

4. In either pane, select the check boxes next to the files and folders you want to restore.

   For an explanation of the icons and check boxes next to each folder, see ***Folder Icons*** (page 156).

5. Click **Next**.

The **Restore In Progress** screen appears with a progress bar.



The selected files and folders are restored.

6 Click **Finish**.

Viewing the Agent Status

The CTERA Agent status can be viewed in the My Computers tab, as described in the following procedure, or when monitoring agents, as described in ***Monitoring Agents*** (on page 247).

To view the CTERA Agent's status in the My Computers tab

- Click the **My Computers** tab.

Each agent's status is displayed next to it.

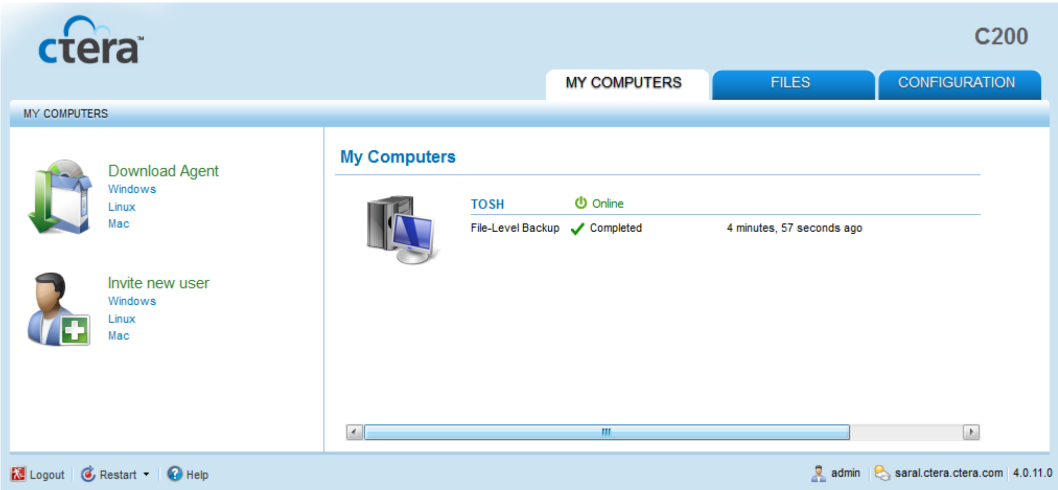


Table 48: CTERA Agent Statuses

This status...	Indicates...
Online	The CTERA Agent is connected and idle.
Disabled	The CTERA Agent is disabled.
Offline	The CTERA Agent is not connected to the appliance.
Running	The CTERA Agent is performing a backup operation.
Retrying	The CTERA Agent is retrying a failed backup operation.

Viewing Agent Details

You can view CTERA Agent details, including its version, the operating system on which it is installed, and copyright information.

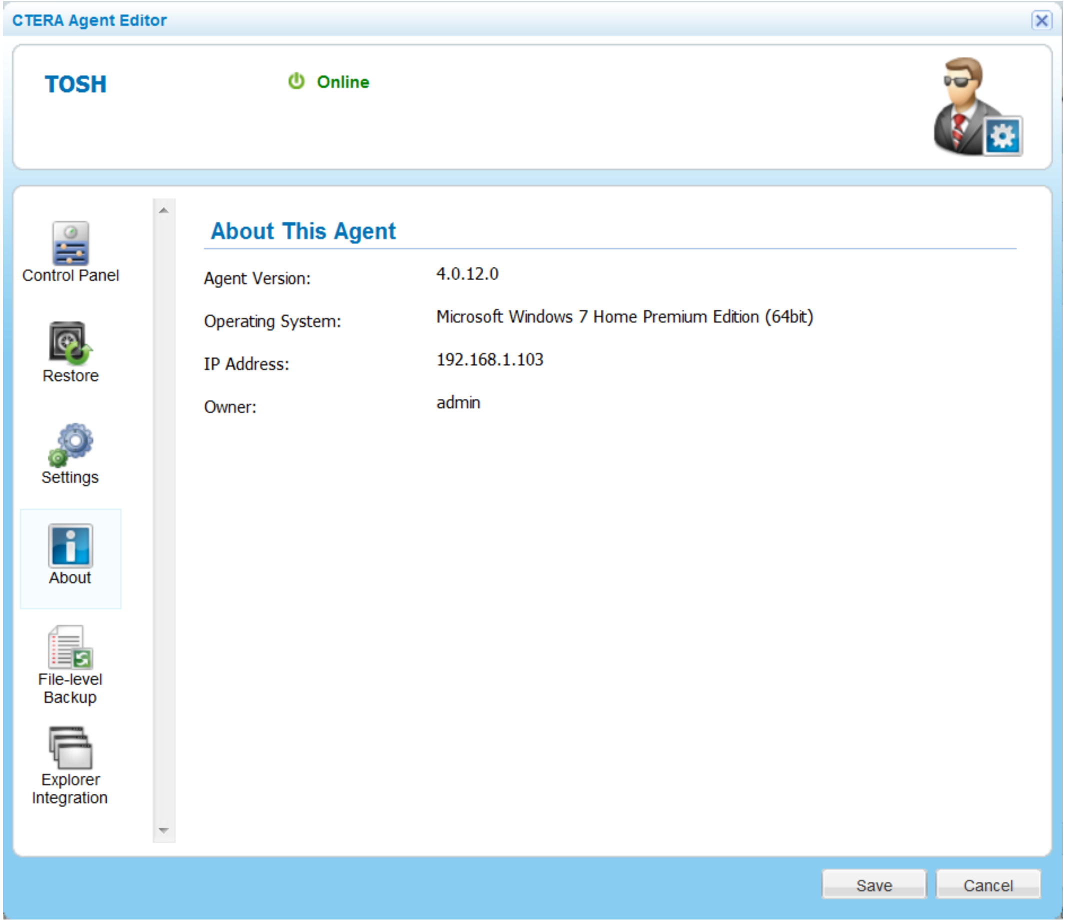
To view CTERA Agent details

1 Open the CTERA Agent Manager.

See ***Opening the CTERA Agent Manager*** (on page 230).

2 Click the **About** tab.

The **About** tab appears.



Monitoring Agents

To monitor CTERA Agents

- In the **Configuration** tab's navigation pane, click **Local Backup > CTERA Agents**.

  The **Local Backup > CTERA Agents** page appears with a table of CTERA Agents.

  The table includes the following columns:

Table 49: CTERA Agent Columns

This column...	Displays...
Type	The CTERA Agent's type. This can be one of the following: - . Server operating system - . Workstation operating system To view the name of the operating system installed on the computer where the agent is running, mouse-over the icon.
Name	The name of the computer on which the CTERA Agent is installed.
Status	The CTERA Agent's current status. For information on possible statuses, see ***Agent Statuses*** (page 246).
Progress	A progress bar indicating the progress of the current local backup operation. If no backup is running for the CTERA Agent, then this column is empty.
Last File-level Backup	The result of the last file-level backup of the CTERA Agent. This can be one of the following: - If the last backup was successful, the backup's status followed by the amount of time that has elapsed since the last backup - If the last backup failed, the backup's status followed by the reason backup failed
Last Disk-level Backup	The result of the last disk-level backup of the CTERA Agent. This can be one of the following: - If the last backup was successful, the backup's status followed by the amount of time that has elapsed since the last backup - If the last backup failed, the backup's status followed by the reason backup failed
Owner	The user name that was used to connect the CTERA Agent to the appliance.
Version	The CTERA Agent's software version.

Deleting Agents

If a CTERA Agent was uninstalled, or you no longer want to manage it, you can delete it from the list of CTERA Agents in the appliance Web interface.

To delete a CTERA Agent

1 In the **Configuration** tab's navigation pane, click **Local Backup > CTERA Agents**.

The **Local Backup > CTERA Agents** page appears.

2 Select the desired CTERA Agent.

3 Click **Delete**.

A confirmation message appears.

4 Click **Yes**.

The CTERA Agent is deleted.

The agent's backup folder is also deleted; however, data is not deleted from previous NEXT3 snapshots, which remain intact.

13

Managing Users

This chapter explains how to manage appliance users and user groups.

In This Chapter

Overview

In order to enable users to access the appliance Web interface and/or shared folders, you must add the users to the appliance Web interface. You can then do any of the following:

- Grant the user access rights to network shares.
- Add a custom user group, and then add the new user to the user group. The entire user group can then be granted access rights to network shares, and the access rights will apply to all members of the user group.
- Add the user to the built-in **Read Only Administrators** user group, which includes read-only access rights to the appliance Web interface. The user will then be able to view the settings in the **Configuration** tab, but not modify them.
- Add the user to the built-in **Administrators** user group, which includes read-write access rights to the appliance Web interface. The user will then be able to view and modify settings in the **Configuration** tab.

Tip

Users and user groups are granted access rights to network shares during share configuration. See ***Sharing Files*** (on page 99).

Tip

Users are added to user groups during user group configuration. See ***Adding and Editing User Groups*** (on page 258).

Tip

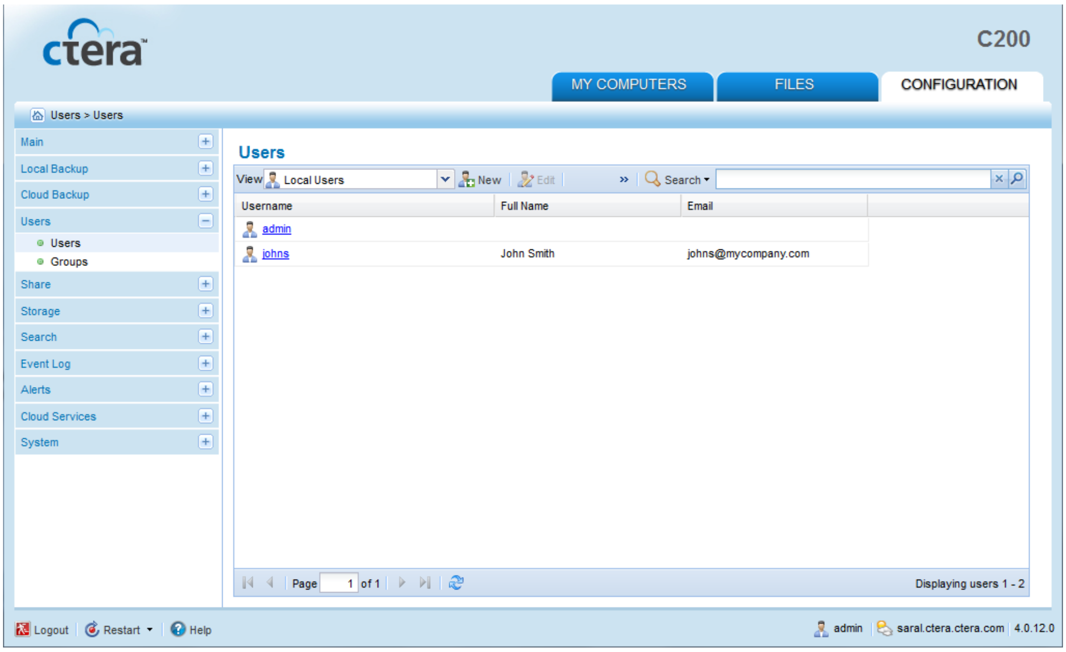
Users that are not members of the Administrators or Read Only Administrators user groups will not be able to view the **Configuration** tab.

Adding and Editing Users

To add or edit a user

1 In the **Configuration** tab's navigation pane, click **Users > Users**.

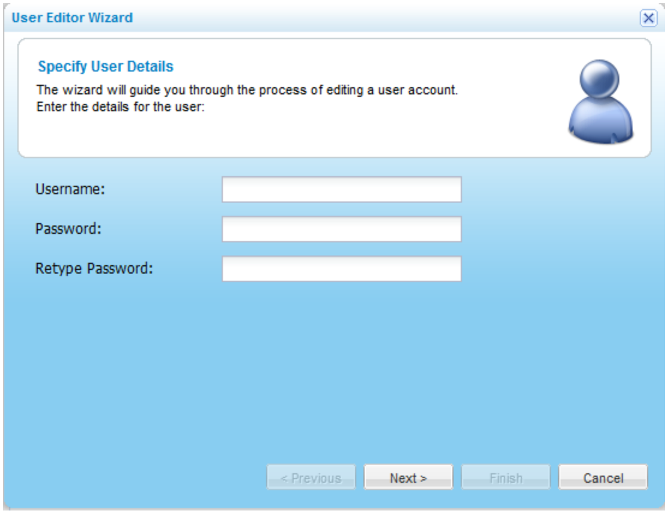
The **Users > Users** page appears.



2 Do one of the following:

- To add a new user, click **New**.
- To edit an existing user, click on its name.

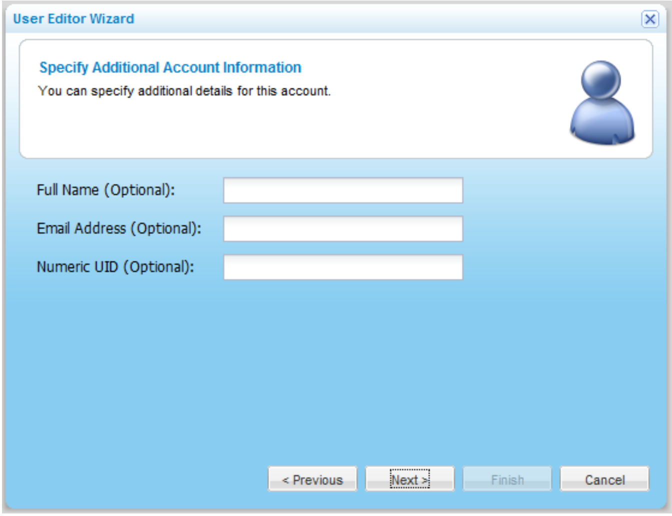
The **User Editor Wizard** opens, displaying the **Specify User Details** dialog box.



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

4 Click **Next**.

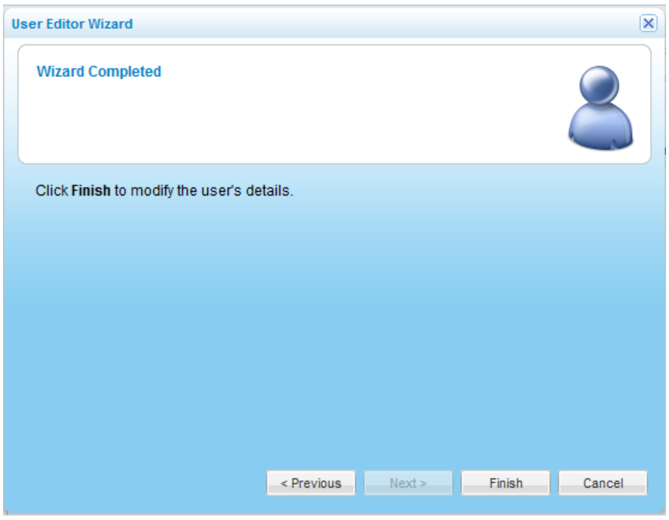
The **Specify Additional Account Information** dialog box opens.



5 Complete the fields using the relevant information in the following table.

6 Click **Next**.

The **Wizard Completed** screen appears.



7 Click **Finish**.

8 To add the user to a user group, add or edit the desired group as described in ***Adding and Editing User Groups*** (on page 258), selecting the user as a member of the group.

Table 50: User Editor Wizard Fields

In this field...	Do this...
Username	Type a user name for the user.
Password	Type a password for the user.
Retype password	Retype the same password you entered in the **Password** field.
Full Name	Type the users' full name. This field is optional.
Email Address	Type the user's email address. This field is optional.
Numeric UID	Type a numeric user ID (UID) to assign the user. This field is optional.

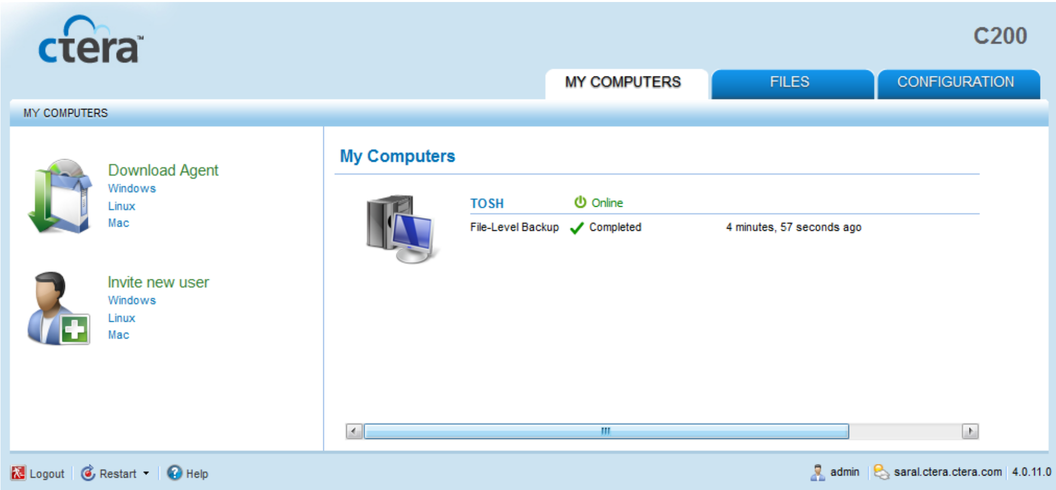
Inviting Users to Install CTERA Agent

You can invite users to install CTERA agent and back up their computers to the appliance. When you invite a user, the user receives an email invitation with a link to download CTERA Agent and a username and password for accessing the appliance. The user's account is added to the appliance and you can see the new user listed in the **Users > Users** page on the **Configuration** tab.

To invite a new user to download CTERA agent

1 Click the **My Computers** tab.

The My Computers page appears.



2 Under **Invite new user**, click **Windows**.

The **Invite New User** dialog box appears.

3 In the **Email Address** field, enter the email address of the user you want to invite.

4 In the **Username** field, enter a user name for the new user.

5 In the **Full Name** field, enter the user's full name.

6 Click **OK**.

A confirmation message appears.

7 Click **OK**. An invitation is sent to the specified email address.

Viewing Users

To view users

1 In the **Configuration** tab's navigation pane, click **Users > Users**.

The **Users > Users** page appears displaying all local users.

2 To display domain users, in the **Local Users** drop-down list, select **Domain** *domain* **Users**, where *domain* is the name of the domain.

All domain users are displayed.

Exporting Users

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

To export users to a *.csv file

1 In the **Configuration** tab's navigation pane, click **Users > Users**.

The **Users > Users** page appears.

2 Click **Export to Excel**. You are asked if you would like to save the file or open the file in Microsoft Excel.

The users are exported.

Allocating Disk Quotas to Users

If disk quotas are enabled for a volume, you can limit the amount of storage space allocated to each volume user.

For information on enabling disk quotas, see ***Adding and Editing Logical Volumes*** (on page 73).

Tip

Administrators are automatically allocated unlimited storage space.

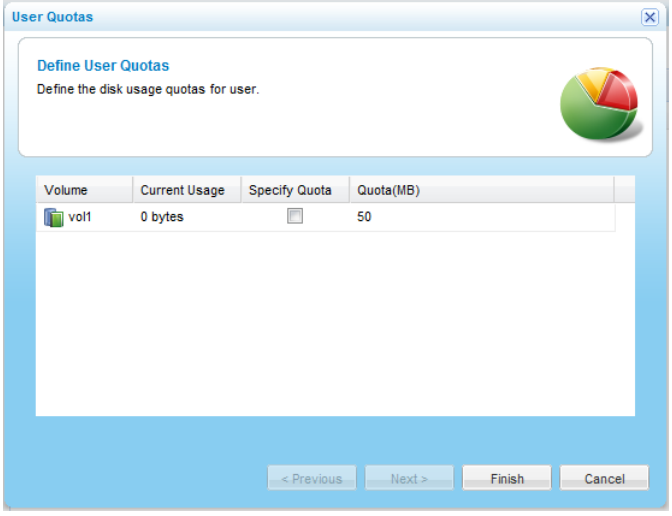
To allocate disk quota to a user

1 In the **Configuration** tab's navigation pane, click **Users > Users**.

The **Users > Users** page appears.

2 Select the desired user name and click **User Quotas**.

The **User Quotas** window appears.



For each disk, the amount of space consumed by the user is listed, along with the user's disk quota.

3 For each volume in which you want to define the user's quota, do the following:

   a In the volume's row, select the **Specify Quota** check box.

   b In the field provided, type the desired quota in MB.

4 For each volume in which you want to revert to the default quota, clear the **Specify Quota** check box.

   For information on setting the default quota, see ***Adding and Editing Logical Volumes*** (on page 73).

5 Click **Finish**.

Deleting Users

Tip

You cannot delete the main administrator account.

To delete a user

1 In the **Configuration** tab's navigation pane, click **Users > Users**.

   The **Users > Users** page appears.

2 Select the desired user name and click **Delete**.

   A confirmation message appears.

3 Click **Yes**.

The user is deleted.

Adding and Editing User Groups

Tip

Users can be members of multiple groups.

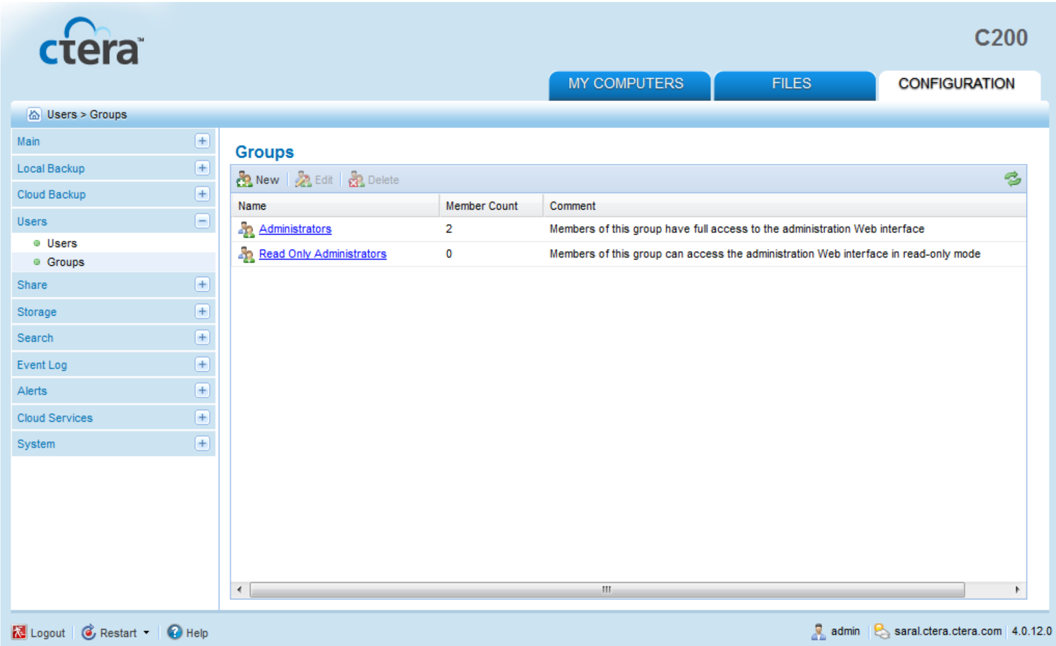
Tip

The groups Read Only Administrators and Administrators are built-in. It is not possible to edit the built-in user groups' names or descriptions.

To add or edit a user group

1 In the **Configuration** tab's navigation pane, click **Users > Groups**.

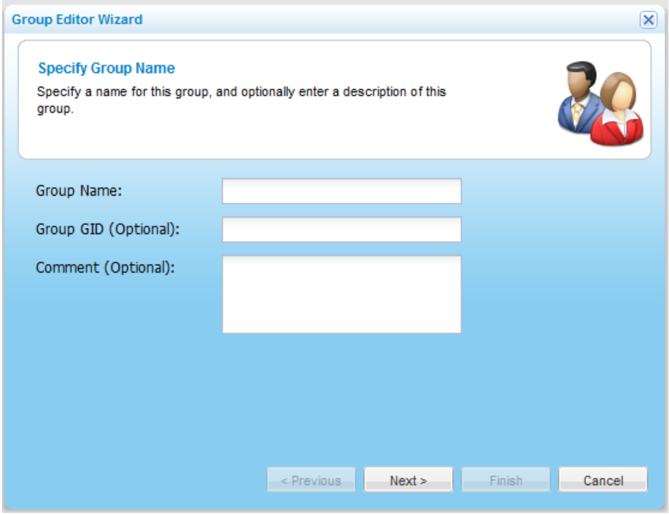
The **Users > Groups** page appears.



2 Do one of the following:

- To add a new user group, click **New**.
- To edit an existing user group, click on its name.

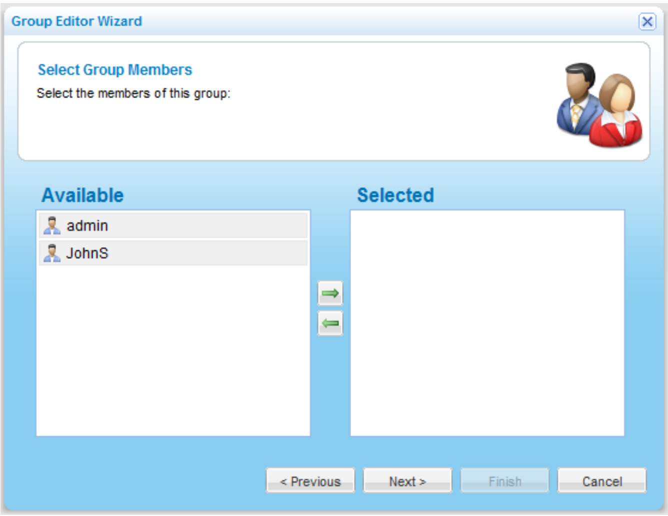
The **Group Editor Wizard** opens, displaying the **Specify Group Name** dialog box.



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

4 Click **Next**.

The **Select Group Members** dialog box opens.



The **Available** pane lists all users that have not yet been assigned to the user group, and the **Selected** pane lists all users who have been assigned to the user group.

5 To add a user to the user group, select the desired user in the **Available** pane, then click .

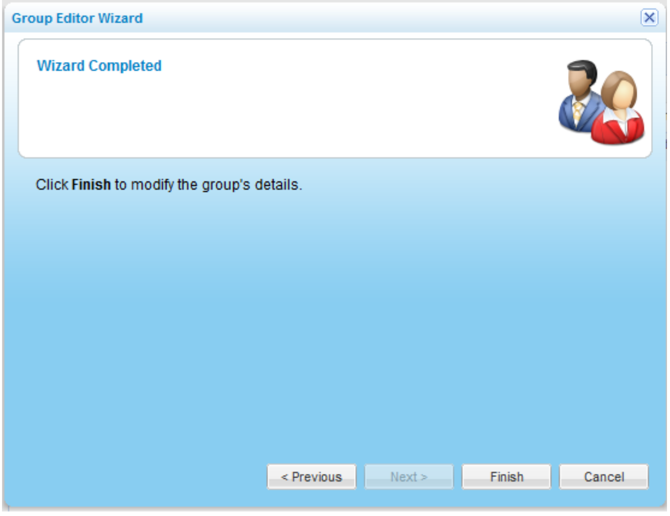
The user appears in the **Selected** pane.

6 To remove a user from the user group, select the desired user in the **Selected** pane, then click .

The user appears in the **Available** pane.

7 Click **Next**.

The **Wizard Completed** screen appears.



8 Click **Finish**.

Table 51: User Group Fields

In this field...	Do this...
Group Name	Type a name for the user group.
Group GID (Optional)	Type a numeric ID to assign the group. This field is optional.
Comment (Optional)	Type a description of the user group. This field is optional.

Deleting User Groups

Tip

Deleting a user group does not delete the group members.

Tip

The groups Read Only Administrators and Administrators are built-in. It is not possible to delete the built-in user groups.

To delete a user group

1 In the **Configuration** tab's navigation pane, click **Users > User Groups**.

The **Users > User Groups** page appears.

2 Select the desired user group and click **Delete**.

A confirmation message appears.

3 Click **Yes**.

The user group is deleted.

Tip

If the deleted user group had been granted access rights to network shares, the group members will no longer have access rights to those network shares. To assign individual users access rights to network shares, see ***Sharing Files*** (on page 99).

14

Managing Network Settings

This chapter explains how to manage and view network settings.

In This Chapter

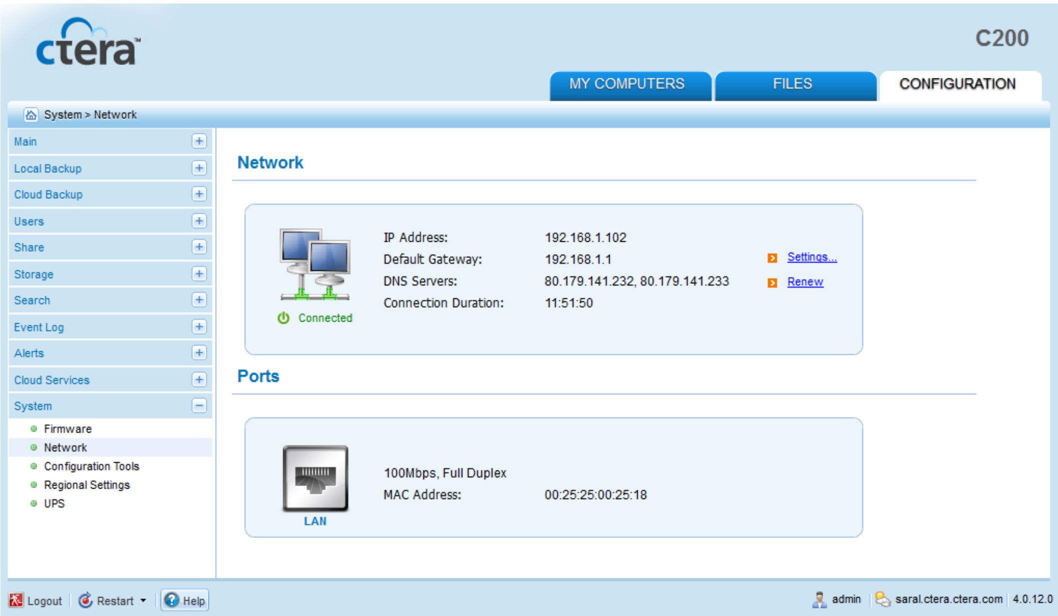
Configuring Network Settings

By default, the appliance is configured to automatically obtain an IP address, as well as the DNS servers to use, from a DHCP server. If your network uses static IP addresses instead of DHCP, you must configure the appliance with the necessary settings.

To configure network settings

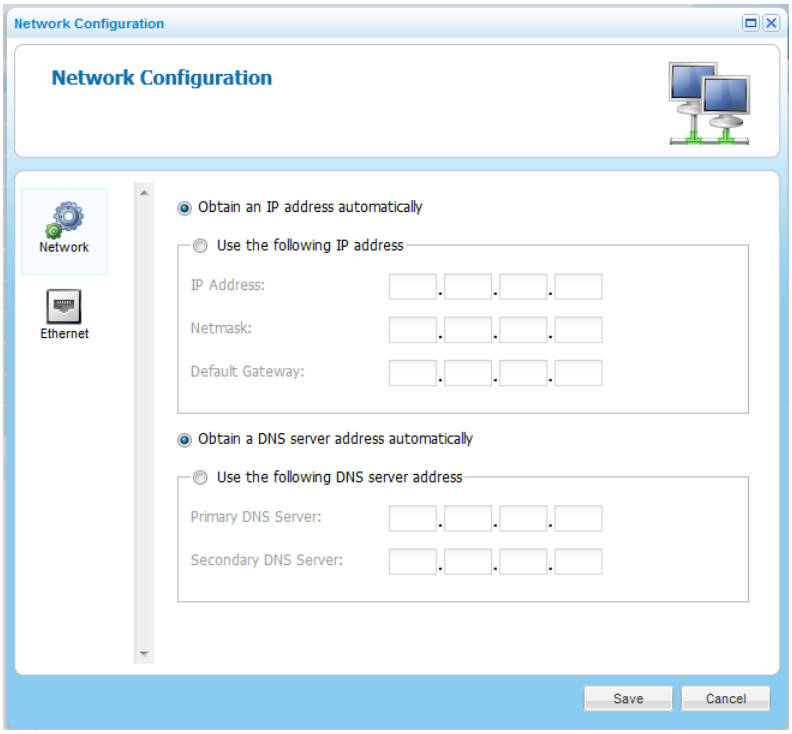
1. In the **Configuration** tab's navigation pane, click **System > Network**.

   The **System > Network** page appears.



2 Click **Settings**.

The **Network Configuration Manager** opens displaying the **Network** tab.



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

4 Click **Save**.

Warning

Set these values with care. If you configure these settings incorrectly, you may lose network connectivity to your appliance.

Table 52: Network Settings Fields

In this field...	Do this...
Obtain an IP address automatically	Choose this option to specify that the appliance should automatically obtain an IP address from the DHCP server in your network. This is the default setting.
Use the following IP address	Choose this option to specify that the appliance should use a static IP address. You must complete the **IP Address**, **Netmask**, and **Default Gateway** fields.
IP Address	Type the IP address to assign the appliance.
Netmask	Type the netmask to assign the appliance.
Default Gateway	Type the IP address of the default gateway.
Obtain a DNS server address automatically	Choose this option to specify that the appliance should automatically obtain DNS server IP addresses from the DHCP server in your network. This is the default setting.
Use the following DNS server address	Choose this option to specify DNS servers for the appliance. You must complete the **Primary DNS Server** and **Secondary DNS Server** fields.
Primary DNS Server	Type the primary DNS server's IP address.
Secondary DNS Server	Type the secondary DNS server's IP address. This field is optional.

Configuring Port Settings

By default, the appliance automatically detects the Ethernet port's link speed and duplex. If desired, you can manually restrict the Ethernet port to a specific link speed and duplex.

You can also configure appliance to use jumbo frames. While the standard Ethernet frame is 1500 bytes, jumbo frames are larger, with the conventional jumbo frame size being 9000 bytes.

Warning

If you enable jumbo frames, you must configure all computers in the appliance's network segment to use the same Ethernet frame size (maximum transmission unit, or MTU). If you do not set the computers to the same MTU, you may lose connectivity to the appliance.

To configure port settings

1 In the **Configuration** tab's navigation pane, click **System > Network**.

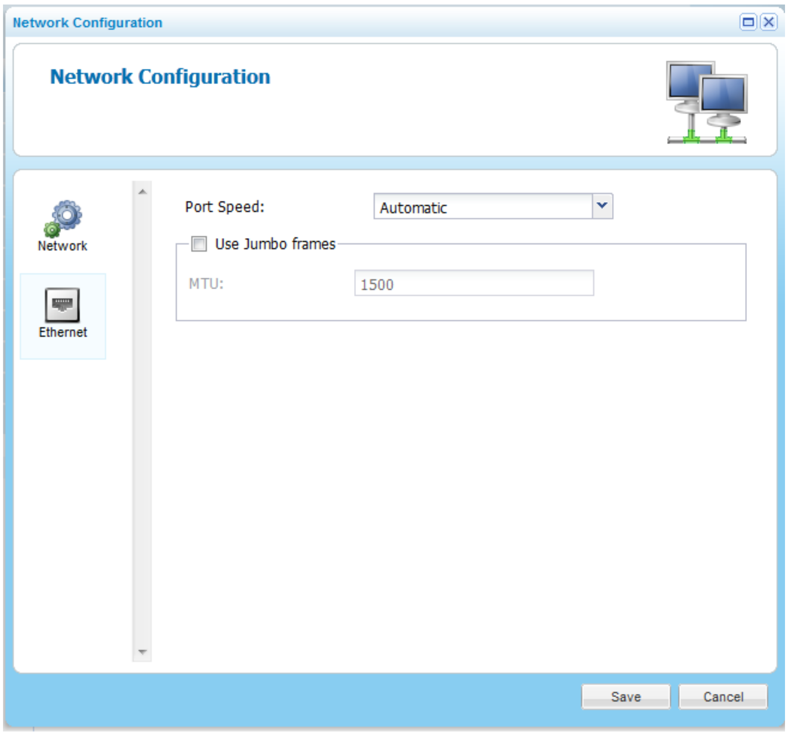
The **System > Network** page appears.

2 Click **Settings**.

The **Network Configuration Manager** opens displaying the **Network** tab.

3 Click the Ethernet tab.

The **Ethernet** tab appears.



4 In the **Port Speed** drop-down list, do one of the following:

- Select **Automatic** to configure the port to automatically detect the link speed and duplex.

  This is the default.

- Select the desired link speed and duplex.

5 To use jumbo frames, do the following:

   a Select the **Use Jumbo frames** check box.

   b In the **MTU** field, type the maximum transmission unit in bytes.

6 Click **Save**.

Viewing Network and Port Settings

You can view the appliance's network and port settings.

To view network and port settings

- In the **Configuration** tab's navigation pane, click **System > Network**.

  The **System > Network** page appears.

  The following information is displayed:

Table 53: Network Status Information

This field...	Displays...
Network	
Connected / Disconnected	The status of the appliance's network connection (**Connected** or **Disconnected**),
IP Address	The appliance's IP address.
Default Gateway	The IP address of the default gateway.
DNS Servers	The IP addresses of the primary and secondary DNS servers.
Connection Duration	The amount of time that the appliance has been connected to the network.
Ports	
Mbps, Duplex	The current Ethernet link speed and duplex.
MAC Address	The MAC address of this appliance.

Renewing the DHCP Lease

The DHCP lease is automatically renewed as needed. You can manually renew as follows.

To renew the DHCP lease

1. In the **Configuration** tab's navigation pane, click **System > Network**.

   The **System > Network** page appears.

2. Click **Renew**.

   The lease is renewed.

Enabling/Disabling Link Aggregation

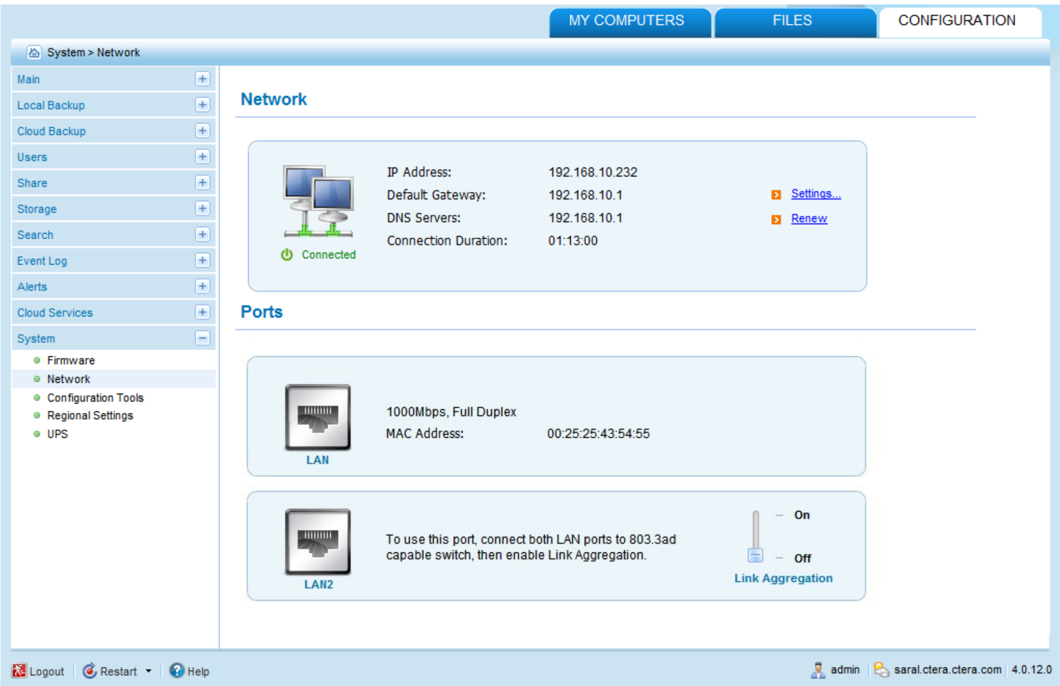
IEEE 802.3ad dynamic link aggregation (also called *port trunking*) is supported by the CTERA C400 and C800. Link aggregation enables you to use both Ethernet ports of the appliance in parallel, to increase the link speed beyond the limits of a single 1Gbps port and to increase redundancy for higher availability.

To enable link aggregation

1. Connect both of the CTERA C400 or C800's LAN ports to a switch that supports IEEE 802.3ad dynamic link aggregation.

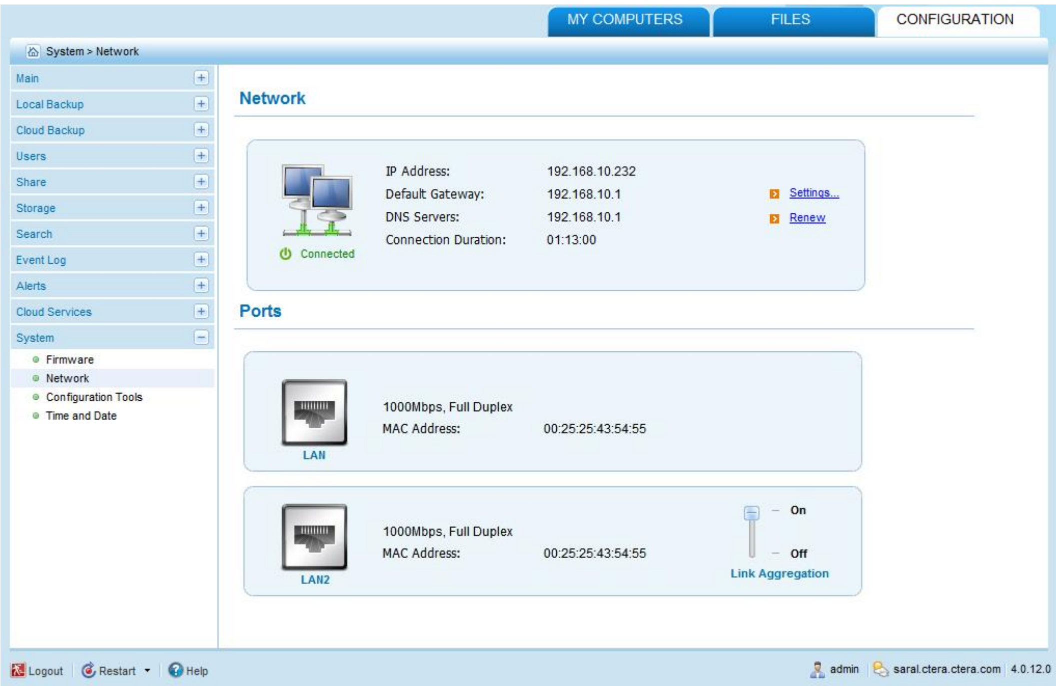
2. In the **Configuration** tab's navigation pane, click **System > Network**.

   The **System > Network** page appears.



3 Slide the lever to the **ON** position.

Link aggregation is enabled.



To disable link aggregation

1 In the **Configuration** tab's navigation pane, click **System > Network**.

The **System > Network** page appears.

2 Slide the lever to the **OFF** position.

Link aggregation is disabled.

15

Setting Up File Search

This chapter explains how to enable and configure file search.

In This Chapter

Overview

The CTERA appliance search engine enables users to search for files by name. The search engine can be enabled and disabled. Updating the search engine's index can be done manually and can be scheduled to be done automatically.

Workflow

To use file search, do the following:

1. Enable file search.

   See ***Enabling/Disabling File Search*** (on page 272).

2. Do one or more of the following:

   - Schedule automatic file index updates.

     See ***Scheduling File Index Updates*** (on page 273).

     The files in cloud storage will be indexed according to the configured schedule.

   - Manually start indexing of the files in cloud storage.

     See ***Manually Starting Index Updates*** (on page 275)

     The files will be indexed immediately.

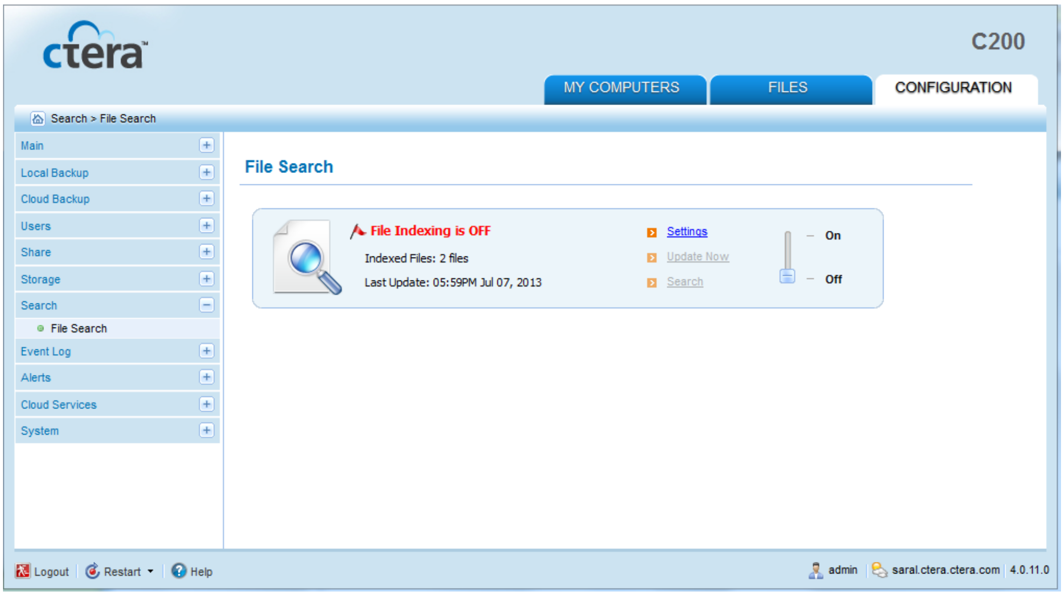
Users can now search for files, as described in ***Searching for Files*** (on page 284).

Enabling/Disabling File Search

To enable file search

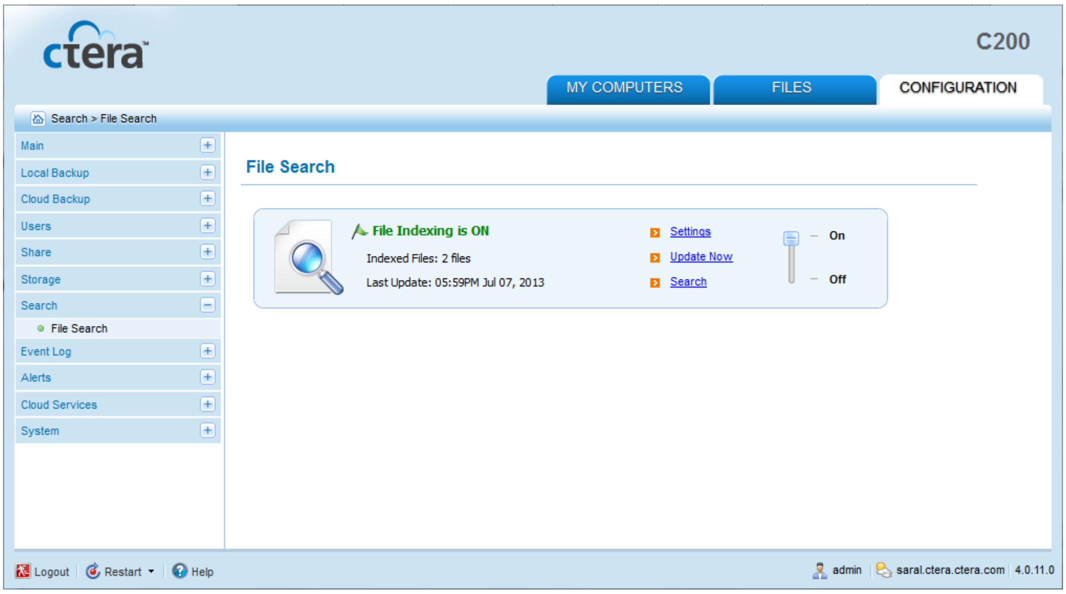
1 In the **Configuration** tab's navigation pane, click **Search > File Search.**

The **File Search** page appears.



2 Slide the lever to the **On** position.

File search is enabled.



To disable file search

1 In the **Configuration** tab's navigation pane, click **Search > File Search.**

The **File Search** page appears.

2 Slide the lever to the **Off** position.

File search is disabled.

Scheduling File Index Updates

When file search is enabled, the appliance will automatically update the file search index according to a configured schedule. If desired, you can modify the schedule.

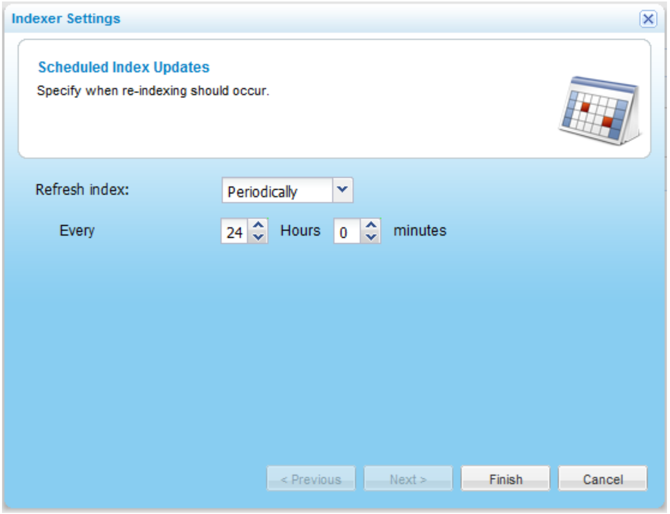
To schedule automatic index updates

1 In the **Configuration** tab's navigation pane, click **Search > File Search.**

The **File Search** page appears.

2 Click **Settings**.

The **Indexer Settings** dialog box appears, displaying the **Scheduled Index Updates** page.



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

4 Click **Finish**.

Table 54: Automatic Index Updates Schedule Fields

In this field...	Do this...
Refresh index	Choose the frequency at which the index should be automatically updated: - **Manual**. Automatic index updates are disabled. Indexing must be started manually. See ***Manually Starting Index Updates*** (on page 275). - **Hourly**. Automatically update the index every specified number of hours. The **On the** field appears. - **Daily**. Automatically update the index every day. The **At** field appears. - **Weekly**. Automatically update the index once a week. The **On** and **At** fields appear. - **Monthly**. Automatically update the index once a month. The **On the X of the month** and **at** fields appear. - **Periodically**. Automatically update the index every specified period of time. The **Every** field appears. The default value is **Periodically**.
On the	Specify the minute of each hour, at which automatic index updates should occur. The default value is 0.
At /at	Specify the hour of the day, at which automatic index updates should occur. The default value when configuring daily index updates is 12:00 AM.
On	Specify the day of the week, on which automatic index updates should occur. The default value is **Sunday**.
Every	Specify the amount of time between automatic index updates backups, in hours and minutes. The default value is 24 hours, 0 minutes.
On the X of the month	Specify the day of the month on which to update the index.

Manually Starting Index Updates

You can manually start an index update at any time.

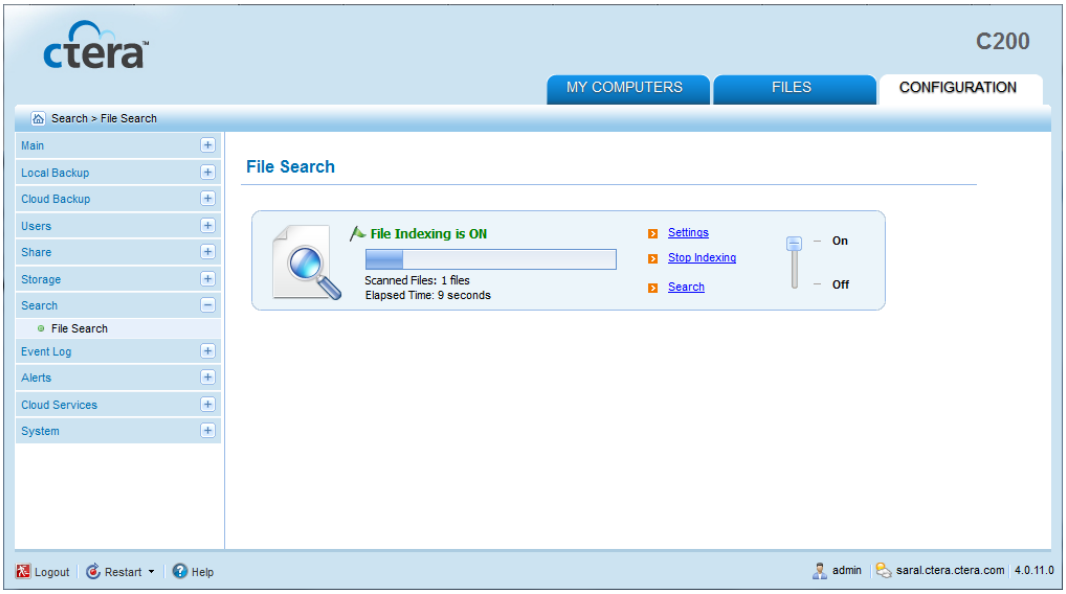
To manually start update the file search index

1 In the **Configuration** tab's navigation pane, click **Search > File Search.**

The **File Search** page appears.

2 Click **Update Now**.

The file search index is updated. A progress bar tracks the indexing progress.



To stop indexing, click **Stop Indexing**.

When indexing is complete, the **Indexed Files** field displays the number of files indexed, and the **Last Update** field displays the date and time at which the last index update occurred.

16

Using the File Manager

This chapter explains how to use the Web-based File Manager to manage files that were stored on the appliance.

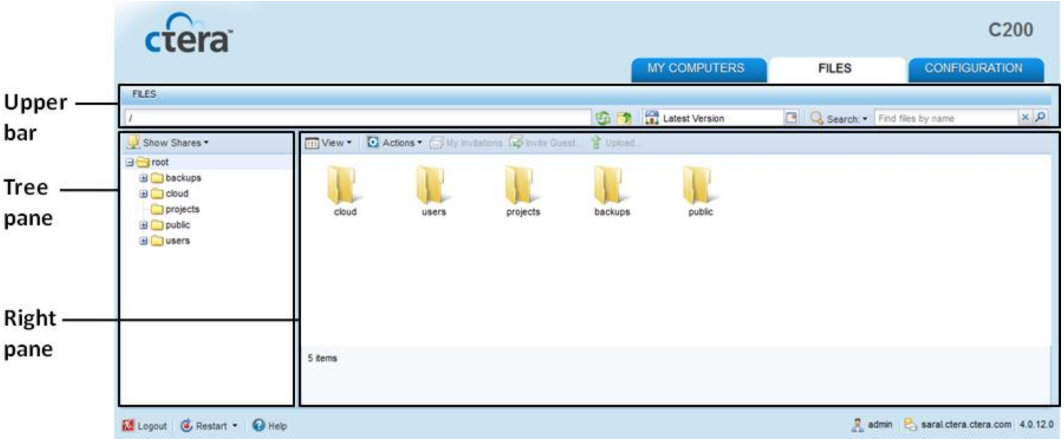
In This Chapter

The File Manager

The File Manager is located in the **Files** tab. It consists of the following elements:

- **Tree pane**. Used for navigating between folders.
- **Right pane**. Displays information and controls for the file or folder selected in the tree pane.

- **Upper bar**. Displays additional navigation options, as well as file restoration and search controls.



Navigating Between Folders

To navigate between folders

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

  The folder's contents appear in the right pane.

Changing the Tree Pane View

The **Files** tab's tree pane offers two views:

- **Shares**

  This is the default view, in which the tree pane displays all network shares and the folders they contain. All File Manager tasks are available in this view.

- **Volumes**

  Users belonging to the Read Only Administrators and Administrators groups can switch to the Volumes view, in which the tree pane displays both physical volumes and network shares. This view allows managing folders that are not included in any network share. File Manager tasks related to guest invitations, project collaboration, and snapshots are not available in this view.

To change the tree pane view

- In the drop-down list the top of the tree pane, select the desired view.

Changing the Right Pane View

The **Files** tab's right pane offers two views:

- **Details**

  This view displays the items in the right pane in a table. You can sort the tables as described in ***Sorting Tables*** (on page 41) and hide/display columns as described in Displaying and Hiding Columns.

- **Large Icons**

  This view displays the items in the right pane as large icons.

To change the right pane view

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

Refreshing the View

To refresh the view

- In the upper bar, click .

  The view is refreshed.

Viewing File or Folder Details

To view a file or folder's details

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

   See ***Navigating Between Folders*** (on page 278).

   The file/folder appears in the right pane.

   When viewing the cloud drive synchronization folder (`root/cloud`), each file is marked with an icon indicating its current synchronization status. In the Large Icons view, files that are in sync are marked with the icon, and files that are currently synchronizing are marked with the icon. When viewing the folder in the Details view, the synchronization status is displayed in the **Sync Status** column.

2. In the right pane, click on the file/folder.

   The file/folder's details appear at the bottom of the right pane.

   If in Details view, the file/folder's details are displayed in the table as well. For information on changing the view, see ***Changing the Right Pane View*** (on page 279).

Downloading Files and Folders

You can download individual files, multiple files, or entire folders.

To download an individual file

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

  See ***Navigating Between Folders*** (on page 278).

2 In the right pane, do one of the following:

  - If in the Large Icons view, double-click on the file.
  - If in the Details view, click once on the file name.

  For information on changing the view, see ***Changing the Right Pane View*** (on page 279).

  The file is downloaded to your computer.

To download multiple files or entire folders

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

  See ***Navigating Between Folders*** (on page 278).

2 In the right pane, select the desired files or folder(s).

  See ***Selecting Files and Folders*** (on page 283).

3 Click **Actions**, and then click **Download**.

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

Uploading Files

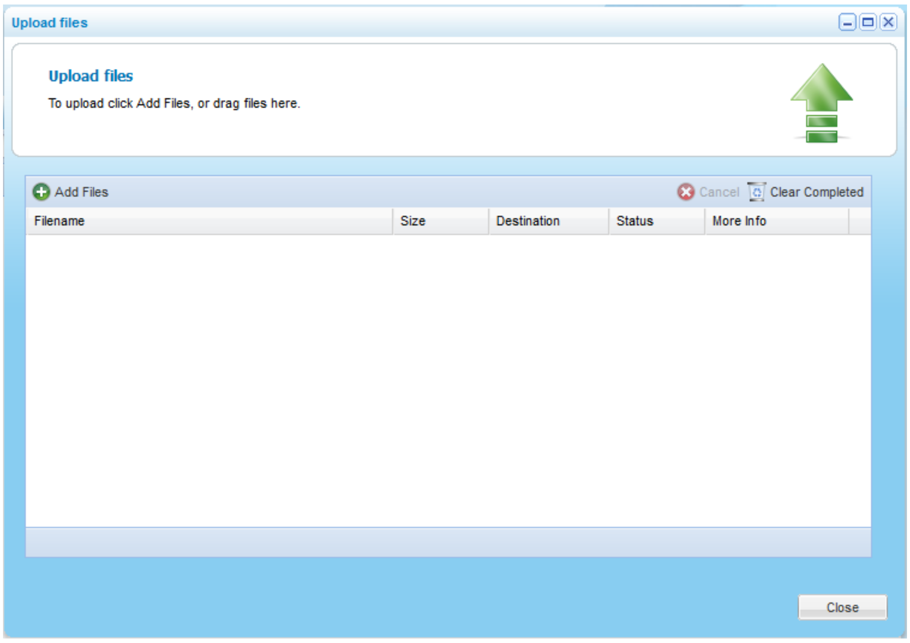
To upload files

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

  See ***Navigating Between Folders*** (on page 278).

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

The **Upload files** window appears.

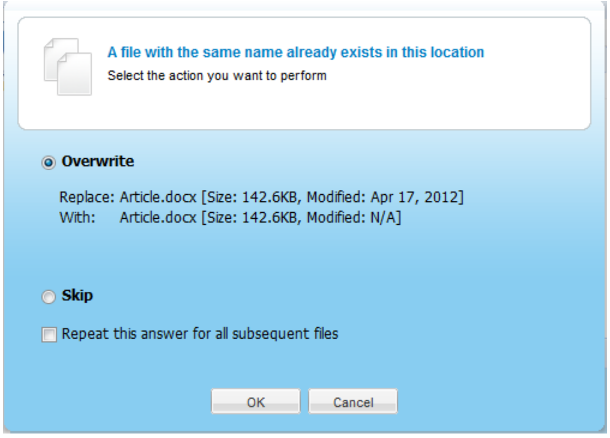


3 For each file you want to upload, do one of the following:

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

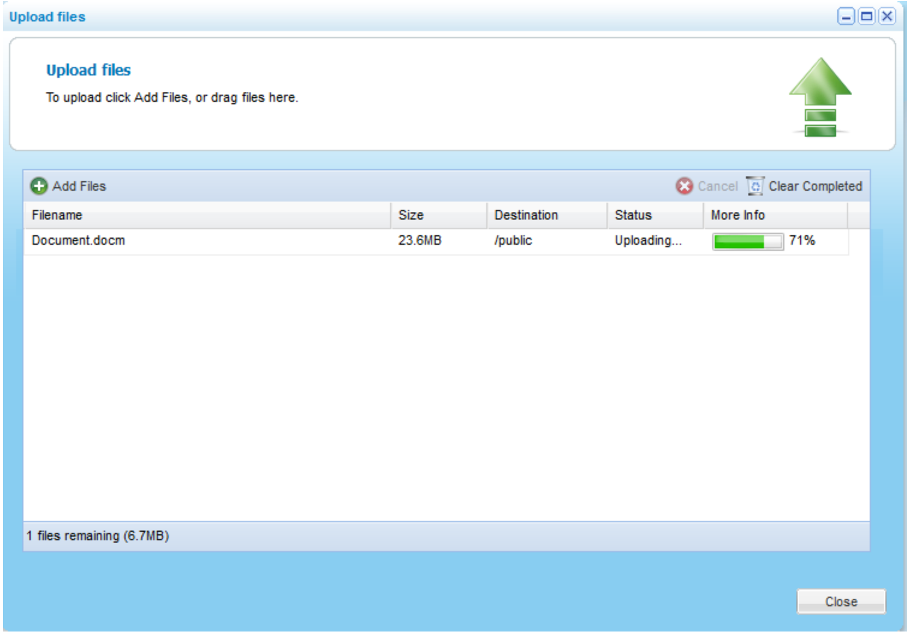
The following things happen:

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



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

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



4 To cancel an upload, select the file whose upload you want to cancel, and then click **Cancel**.

5 To clear the list of completed uploads, click **Clear Completed**.

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

Creating New Folders

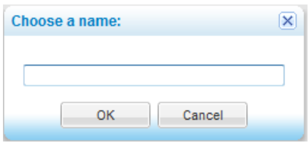
To create a new folder

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

See ***Navigating Between Folders*** (on page 278).

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

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



3 In the field provided, type a name for the new folder.

4 Click **OK**.

Renaming Files and Folders

To rename a file or folder

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

   See ***Navigating Between Folders*** (on page 278).

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

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

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

Selecting Files and Folders

To select a file or folder

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

Deleting Files and Folders

To delete a file or folder

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

   See ***Navigating Between Folders*** (on page 278).

2. Select the desired file or folder.

   See ***Selecting Files and Folders*** (on page 283).

3. Click **Actions** and then click **Delete**.

   A confirmation message appears.

4. Click **Yes**.

The selected items are deleted.

Copying/Moving Files and Folders

To copy or move files or folders

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

   See ***Navigating Between Folders*** (on page 278).

2. Select the desired file or folder.

   See ***Selecting Files and Folders*** (on page 283).

3. Do one of the following:
   - To copy the selected items, click **Actions** and then click **Copy**, or press CTRL+C.
   - To move the selected items, click **Actions** and then click **Cut**, or press CTRL+X.

4. Navigate to the target folder.

   See ***Navigating Between Folders*** (on page 278).

5. Click **Actions** and then click **Paste**, or press CTRL+V.

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

Managing Projects

You can manage projects using the File Manager. For information, see ***Collaborating on Projects*** (on page 140).

Managing Network Shares

You can manage network shares using the File Manager. For information, see ***Managing Network Shares in the File Manager*** (on page 108).

The feature is available to administrators only.

Searching for Files

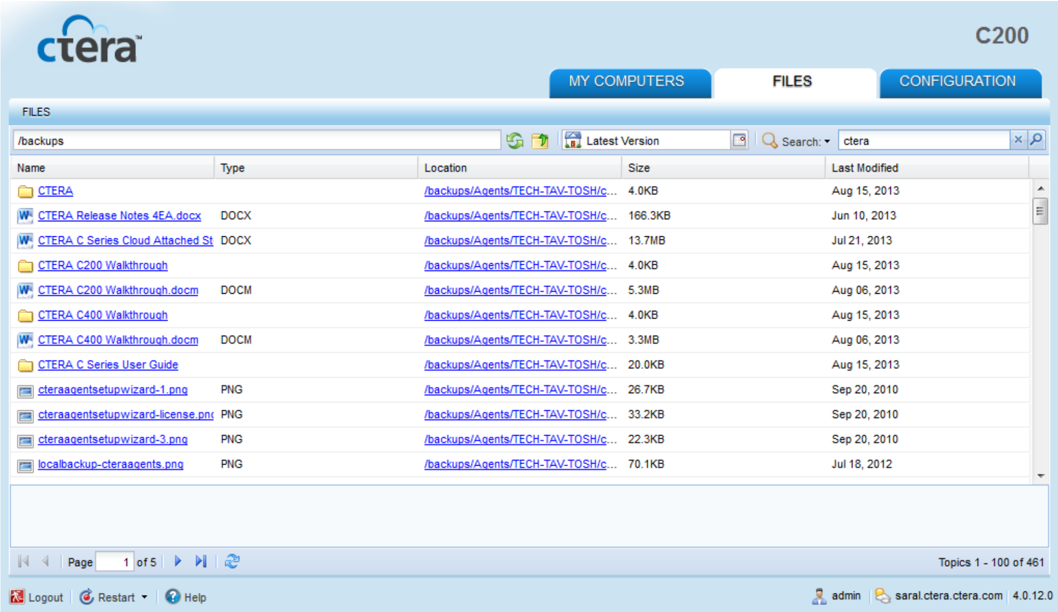
If file search is enabled, you can search for files by name. See ***Enabling/Disabling File Search*** (on page 272).

To search for files

1. In the File Manager, type the name of the file you want to search for in the **Find files by name** field.

2 Click .

The search results appear.



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

4 To clear the search results, click .

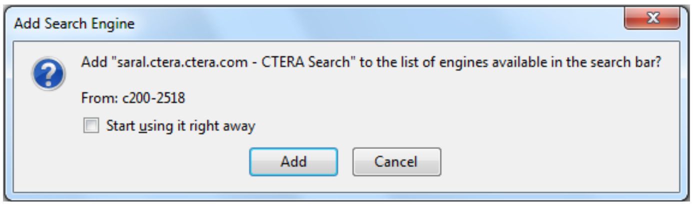
Adding the Appliance as a Search Provider in Your Browser

You can add the appliance as a search provider in your browser. This enables you to search for files directly from your browser's search box.

To add the appliance as a search provider

1 In the File Manager, open the **Search** drop-down list and select **Add as search provider**.

The **Add Search Engine** dialog box appears.



2 To start using the appliance as a search provider immediately, select the **Start using it right away** check box.

If you do not select this option, the appliance will only be added as a search provider upon restarting your browser.

3 Click **Add**.

The appliance is added to your browser's list of search providers.

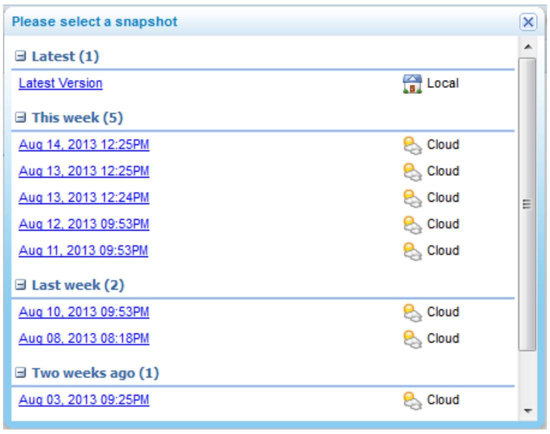
Viewing Previous Versions of Files and Folders

To view previous versions of files and folders

1. In the File Manager's **Show Shares** tree pane view, in the upper bar, click .

   For information on changing the tree pane view, see ***Changing the Tree Pane View*** (on page 278).

   The **Please select snapshot** window opens.

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

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

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

17

Monitoring Your CTERA Appliance

This chapter explains how to use the Status Dashboard, appliance logs, and email alerts to monitor your appliance.

In This Chapter

Viewing the Status Dashboard

The Status Dashboard provides an overview of the appliance's current status, including the following:

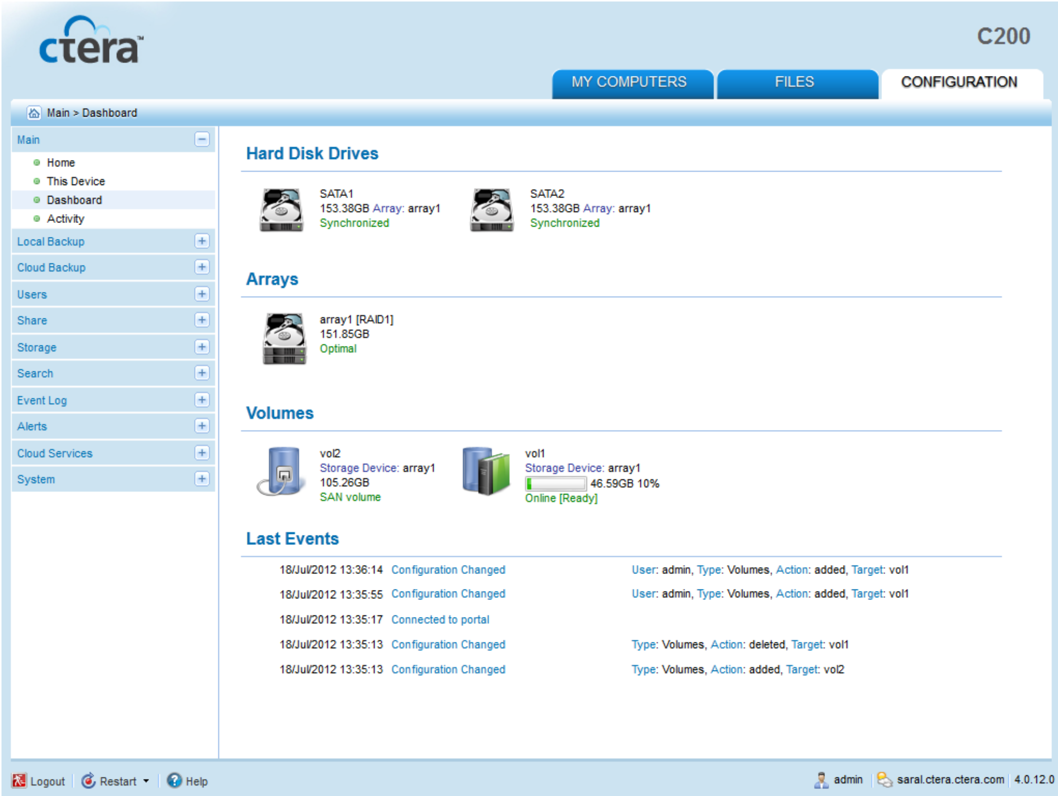
- The disk drive and volume information
- Resource utilization information
- Scheduled backup operations information
- Recent logged events

In addition, it provides shortcuts to configuring arrays, drives, and volumes.

To view the Status Dashboard

- In the **Configuration** tab's navigation pane, click **Main > Dashboard**.

The **Main > Dashboard** page appears.



For information on the fields displayed, see the following table.

Tip

The data is automatically refreshed, every few seconds.

Table 55: Status Dashboard Fields

This field...	Displays...
Hard Disk Drives	All disk drives installed on the appliance. For each drive, the following information is displayed: - The disk type Click on this link to view additional information about the drive. For further information, see ***Viewing Detailed Information About a Disk Drive*** (on page 291). - The disk size in GB - The array to which the disk is assigned - The disk status. For a list of possible statuses, see ***Hard Drive Statuses*** (page 290). Note that you may notice a discrepancy between the disk capacity stated on the disk's packaging and the disk capacity displayed in the appliance Dashboard. This difference is due to the fact that vendors define 1 GB as 1 billion (10^9) bytes, while computers define 1 GB as 2^{30} bytes.
Arrays	All arrays defined on the appliance. For each array, the following information is displayed: - The array name and RAID type Click on this link to edit the array. For further information, see ***Adding and Editing Arrays*** (on page 68). - The array size in GB - The array status. For a list of possible statuses, see ***Array Statuses*** (page 290).
Volumes	All volumes defined on the appliance. For each volume, the following information is displayed: - The volume name and the storage device on which it is located. Click on this link to edit the volume. For further information, see ***Adding and Editing Logical Volumes*** (on page 73). - 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. - The volume's status in the format: `Mode [Status]`. The mode can be **Online** or **Offline**. For a list of possible statuses, see ***Volume Statuses*** (page 291).
Last Events	The last five important events in the appliance Event Log.

	For information on log fields, see Using CTERA appliance Logs.

Table 56: Hard Drive Statuses

This status...	Indicates...
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.

Table 57: Array Statuses

This status...	Indicates...
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 appliance is currently synchronizing out-of-sync members of the array, and performance of the appliance may be reduced. Once the recovery is finished, the array will return to optimal state.
Scrubbing	Data scrubbing is in progress.

Table 58: Volume Statuses

This status...	Indicates...
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.

Viewing Detailed Information About a Disk Drive

From the Status Dashboard, you can choose to view additional, detailed information about a disk drive.

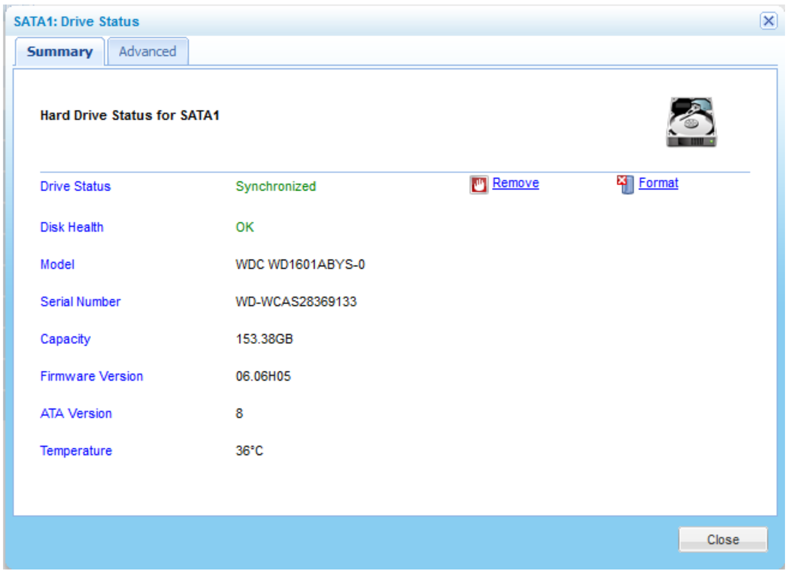
To view additional information about a disk drive

1. In the **Configuration** tab's navigation pane, click **Main > Dashboard**.

   The **Main > Dashboard** page appears.

2. In the **Hard Disk Drives** area, click on the drive for which you want information.

The **Drive Status** window appears, displaying the **Summary** tab.



For information on the fields displayed, refer to the information in ***Drive Status Fields*** (page 294).

3 To format the drive, do the following:

a Click **Format**.

A confirmation message appears.

b Click **Yes**.

The disk is formatted.

4 To prepare the disk for safe removal, do the following:

a Click **Safely Remove**.

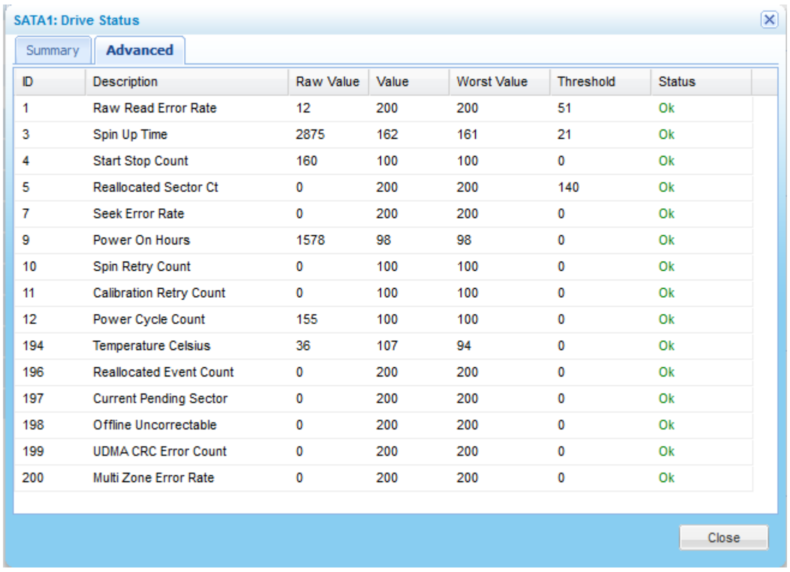
A confirmation message appears.

b Click **Yes**.

The disk is unmounted and can be safely removed.

5 To view advanced information, click the **Advanced** tab.

The **Advanced** tab appears.



SATA1: Drive Status

Summary | Advanced

ID	Description	Raw Value	Value	Worst Value	Threshold	Status
1	Raw Read Error Rate	12	200	200	51	Ok
3	Spin Up Time	2875	162	161	21	Ok
4	Start Stop Count	160	100	100	0	Ok
5	Reallocated Sector Ct	0	200	200	140	Ok
7	Seek Error Rate	0	200	200	0	Ok
9	Power On Hours	1578	98	98	0	Ok
10	Spin Retry Count	0	100	100	0	Ok
11	Calibration Retry Count	0	100	100	0	Ok
12	Power Cycle Count	155	100	100	0	Ok
194	Temperature Celsius	36	107	94	0	Ok
196	Reallocated Event Count	0	200	200	0	Ok
197	Current Pending Sector	0	200	200	0	Ok
198	Offline Uncorrectable	0	200	200	0	Ok
199	UDMA CRC Error Count	0	200	200	0	Ok
200	Multi Zone Error Rate	0	200	200	0	Ok

Close

For drives supporting Self-Monitoring, Analysis, and Reporting Technology, (S.M.A.R.T), this tab displays advanced diagnostics information about the disk drive.

For an explanation of the fields, refer to your disk drive's documentation.

Tip

If your drive does not support S.M.A.R.T, this tab will not appear.

Tip

USB drives do not support S.M.A.R.T.

6 Click **Close**.

Table 59: Drive Status Fields

This field...	Displays...
Drive Status	The disk drive's current status. For a list of possible statuses, see ***Hard Drive Statuses*** (page 290).
Disk Health	The disk's health status (**OK** or **Failed**).
Model	The disk drive's model.
Serial Number	The disk drive's serial number.
Capacity	The disk drive's capacity.
Firmware Version	The disk drive's firmware version.
ATA Version	The disk drive's ATA version.
Temperature	The disk drive's current temperature in degrees Celsius.

Viewing the Activity Monitor

The Activity Monitor provides an overview of the appliance's recent activity, including:

- The disk read rate in KBps (kilobytes per second)
- The disk write rate in KBps (kilobytes per second)
- The percentage of CPU in use
- The percentage of memory in use
- A list of active user sessions

To view the Activity Monitor

- In the **Configuration** tab's navigation pane, click **Main > Activity**.

The **Main > Activity** page appears.

Table 60: User Session Information

This column...	Displays...
Type	The session type: GUI CIFS (Windows File Sharing) CTERA Agent
User	The user connected to the appliance.
Source IP	The IP address from which the user connected to the appliance.
Duration	The amount of time that the user has been connected to the appliance.
More Info	Additional information about the session.

Tip

The data is automatically refreshed, every few seconds.

Configuring Logging

You can configure appliance Event Log settings, as well as Syslog settings.

Configuring Event Log Settings

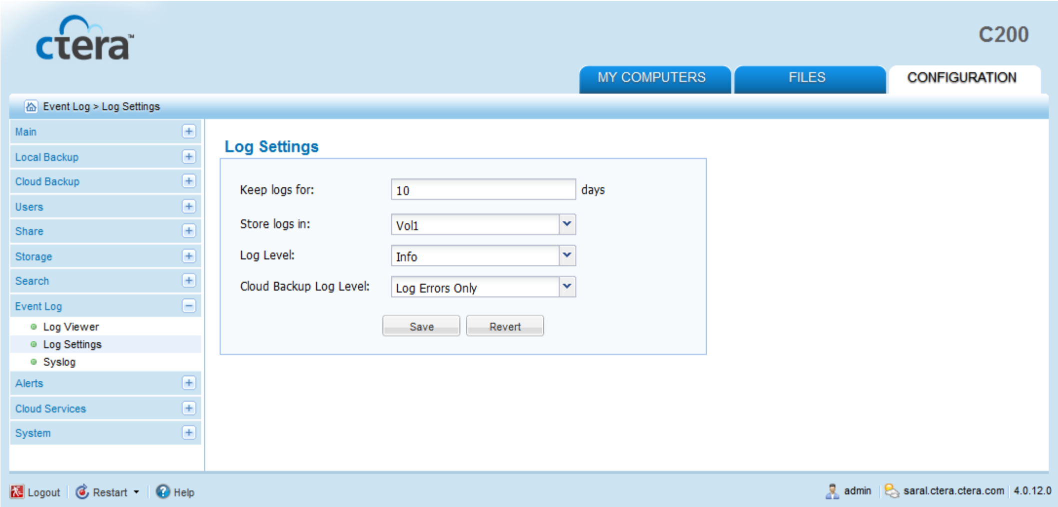
You can configure settings for the appliance Event Log, including log storage and the log level to display.

To configure Event Log settings

1. Do one of the following:
   - In the **Configuration** tab's navigation pane, click **Event Log > Log Settings**.
   - When viewing any log category, click **Settings**.

     See ***Viewing Logs*** (on page 299).

   The **Event Log > Log Settings** page appears.



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

Table 61: Log Settings Fields

In this field...	Do this...
Keep logs For	Type the number of days that the appliance should store logs. The default value is 10 days.
Store logs in	Select the volume where the appliance should store logs. If you choose **Memory**, the logs will be deleted each time you reboot the appliance. This option is selected by default when no disks are installed. If you choose the name of a volume, the logs will be stored on that volume.
Log Level	Select the minimum log level to display in the appliance Web interface. For example, if you select **Critical**, then only **Alert**, **Critical**, and **Emergency** logs will appear in the appliance Web interface. The default value is **Info**.
Cloud Backup Log Level	The appliance automatically logs all backup and restore operations. Specify whether appliance should display additional information about files that are backed up and restored, by selecting one of the following: - **Log Every File**. Provide additional information about all backed up and restored files. - **Log Errors Only**. Only provide additional information about files for which errors occurred during backup and restore operations. - **No Logging**. Do not provide additional information about backed up and restored files. The additional information includes file name, deduplication ratio, and more. See ***Viewing Backup Logs*** (see "***Viewing Cloud Backup Logs***" on page 303). The default level is **Log Errors Only**.

Configuring Syslog Logging

If desired, you can configure the appliance to send logs to a Syslog server located on your network or on the Internet.

While the appliance Event Log is limited by the amount of available storage space, a Syslog server can store an unlimited number of logs.

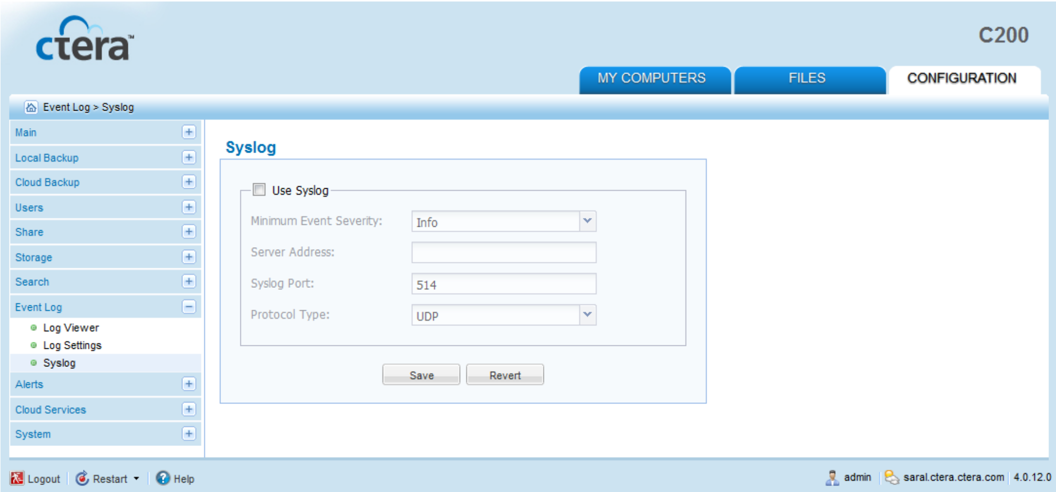
Tip

You can obtain free Syslog servers online, such as Kiwi Syslog Daemon (http://www.kiwisyslog.com/).

To configure Syslog logging

1 In the **Configuration** tab's navigation pane, click **Event Log > Syslog**.

The **Event Log > Syslog** page appears.



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

3 Click **Save**.

Table 62: Syslog Fields

In this field...	Do this...
Use Syslog	Select this option to enable Syslog logging. You must complete the rest of the fields.
Minimum Event Severity	Select the minimum log level to send to the Syslog server. For example, if you select **Critical**, then only **Alert**, **Critical**, and **Emergency** logs will be sent to the Syslog server. The default value is **Info**.
Server Address	Type the Syslog server IP address.
Syslog Port	Type the Syslog server's port number. The default value is 514.
Protocol Type	Select the protocol to use for sending logs to the Syslog server: **TCP** or **UDP**. The default value is **UDP**.

Viewing Logs

The appliance Event Log includes the following log categories:

Table 63: Log Categories

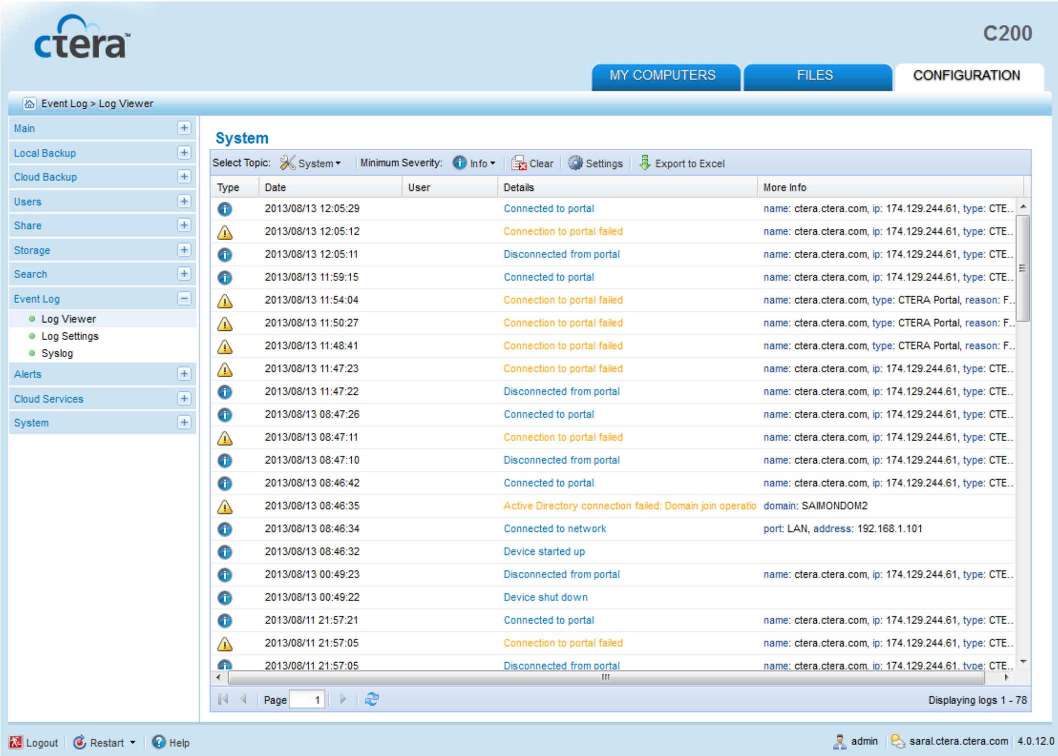
This log category...	Displays...
System	General appliance events, including starting up, connecting to the network and the CTERA Portal, disconnecting from the network and the CTERA Portal, and so on
Local Backup	Events related to synchronization operations
Cloud Backup	Events related to cloud backup or restore operations
Cloud Sync	Events related to cloud drive synchronization operations
Access	Events related to user access to the appliance
Audit	Changes to the appliance configuration
CTERA Agents	Events related to CTERA Agents

Viewing System Logs

To view System logs

- In the **Configuration** tab's navigation pane, click **Event Log > Log Viewer**.

The **Event Log > Log Viewer** page appears displaying the system logs.



Tip

If the **Log Viewer** is already open and a different log category is displayed, in the **Select Topic** drop-down list, select **System**.

The following information is displayed:

Table 64: System Log Fields

This field...	Displays...
Type	An icon indicating the log level. See ***Log Levels*** (page 301).
Date	The date and time at which the event occurred.
User	The user who triggered the event.
Details	A description of the event.
More Info	Additional information about the event.

Table 65: Log Levels

Icon	Log Level
	- Emergency - Alert - Critical - Error
	- Warning
	- Notice - Info
	- Debug

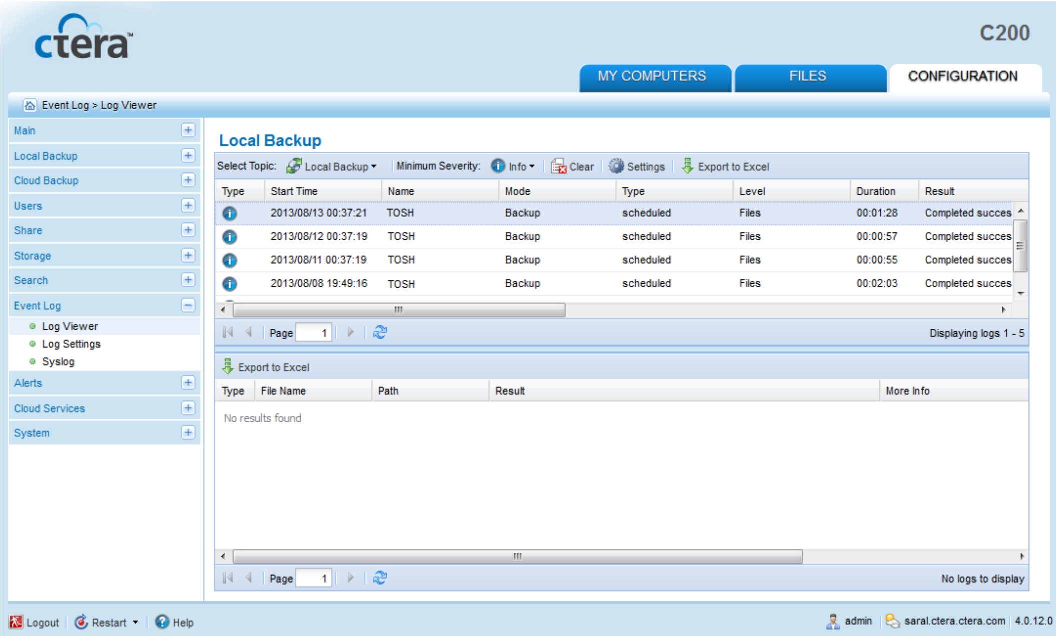
Viewing Local Backup Logs

To view Local Backup logs

1. Do one of the following:
   - To access Local Backup logs from either **Synchronize** page, click **Event Log**.
   - To access Local Backup logs from the Log Viewer:
     1. In the **Configuration** tab's navigation pane, click **Event Log > Log Viewer**.

        The **Event Log > Log Viewer** page appears.
     2. In the **Select Topic** drop-down list, select **Local Backup**.

The Local Backup logs appear. For information on the displayed fields, see the following tables.



2 To view files for which errors occurred during a synchronization operation, click on the desired operation in the upper pane.

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

Table 66: Local Backup Log Upper Pane Fields

This field...	Displays...
Type	An icon indicating the log level. See ***Log Levels*** (page 301).
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 **Disk-level backup**.
Duration	The amount of time the synchronization operation took.
Result	The result of the synchronization operation.
Files	The number of files at the synchronization source.
Size	The total size of the files at the synchronization source in MB.
Transferred Files	The number of files transferred to the synchronization destination.
Transferred Size	The total size of the files transferred to the synchronization destination in MB.
More Info	Additional information about the synchronization operation.

Table 67: Local Backup Log Lower Pane Fields

This field...	Displays...
Type	An icon indicating that an error occurred during synchronization ( ).
File Name	The name of the file for which an error occurred.
Path	The path to the file.
Result	The result of the synchronization operation.
More Info	Additional information about the synchronization operation.

Viewing Cloud Backup Logs

To view Cloud Backup logs

1 Do one of the following:

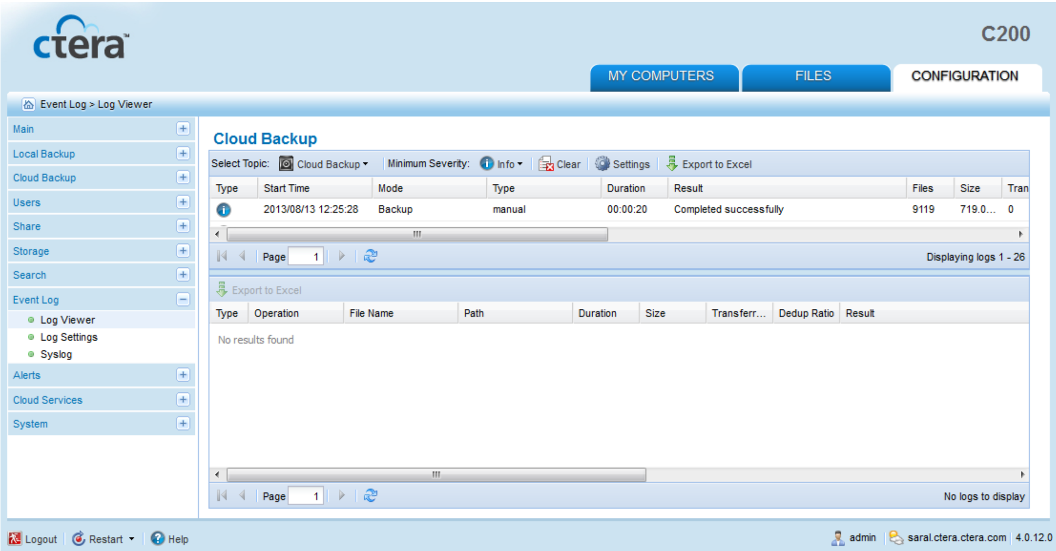
- To access Cloud Backup logs from the **Cloud Backup > Control Panel** page, click **History**.
- To access Cloud Backup logs from the **Log Viewer**:

1 In the **Configuration** tab's navigation pane, click **Event Log > Log Viewer**.

The **Event Log > Log Viewer** page appears.

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

The Cloud Backup logs appear. For information on the displayed fields, see the following tables.



Tip

By default, the lower pane will appear displaying all files for which an error occurred during backup. However, if you disabled additional logging for backup operations, the lower pane will not appear. For information on configuring the logging level, see ***Configuring Event Log Settings*** (on page 296).

2 To view additional logging information for a backup operation, click on the desired operation in the upper pane.

Information about files included in the backup operation appears in the lower pane.

Table 68: Cloud Backup Log Upper Pane Fields

This field...	Displays...
Type	An icon indicating the log level. See ***Log Levels*** (page 301).
Start Time	The date and time at which the backup operation started.
Mode	The operation mode, **Backup** or **Restore**.
Type	The type of backup, **Manual** or **Scheduled**.
Duration	The amount of time the backup operation took.
Result	The result of the backup operation.
Files	The number of files to be backed up.
Size	The total size of the files to be backed up.
Transferred Files	The number of files transferred to cloud storage during the backup operation.
Transferred Size	The size of the files transferred to cloud storage during the backup operation.
Changed Files	The number of files that changed since the last backup operation.
Changed Size	The total size of the files that changed since the last backup operation.
More Info	Additional information about the event.

Table 69: Cloud Backup Log Lower Pane Fields

This field...	Displays...
Type	An icon indicating whether backup was successful ( ) or not ( ).
Operation	The operation performed (**create**, **delete**, **modify**, or **rename**).
File Name	The name of the backed up file.
Path	The path to the backed up file.
Duration	The amount of time backup took for the file.
Size	The size of the file.
Transferred Size	The size of the file transferred to cloud storage.
Dedup Ratio	The deduplication ratio for the file.
Result	The result of the backup operation.
More Info	Additional information about the event.

Viewing Cloud Sync Logs

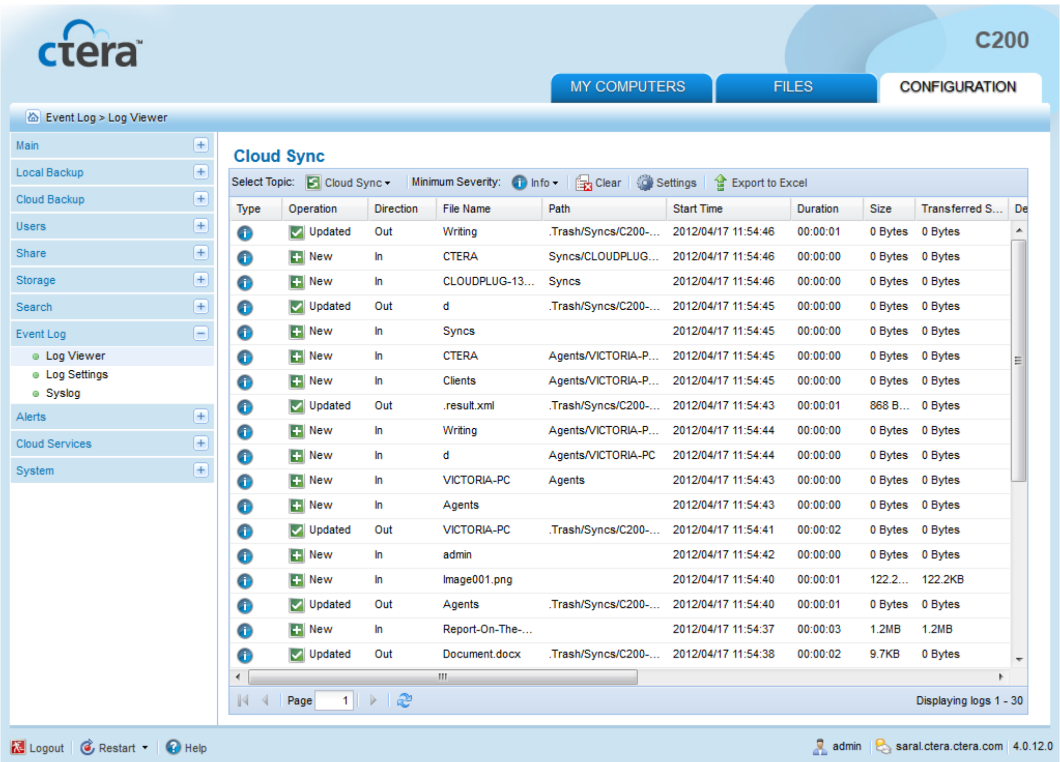
To view Cloud Sync logs

1 In the **Configuration** tab's navigation pane, click **Event Log > Log Viewer**.

The **Event Log > Log Viewer** page appears.

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

The Cloud Sync logs appear.



The following information is displayed:

Table 70: Cloud Sync Log Fields

This field...	Displays...
Type	An icon indicating the log level. See ***Log Levels*** (page 301).
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.
Path	The path to the file transferred during the synchronization operation.
Start Time	The date and time at which the synchronization operation started.
Duration	The amount of time the synchronization operation took.
Size	The size of the synchronized file.
Transferred Size	The actual amount of data transferred.
Dedup Ratio	The deduplication ratio for the file transferred during the synchronization operation.
Result	The result of the synchronization operation.
More Info	Additional information about the event.

Viewing Access Logs

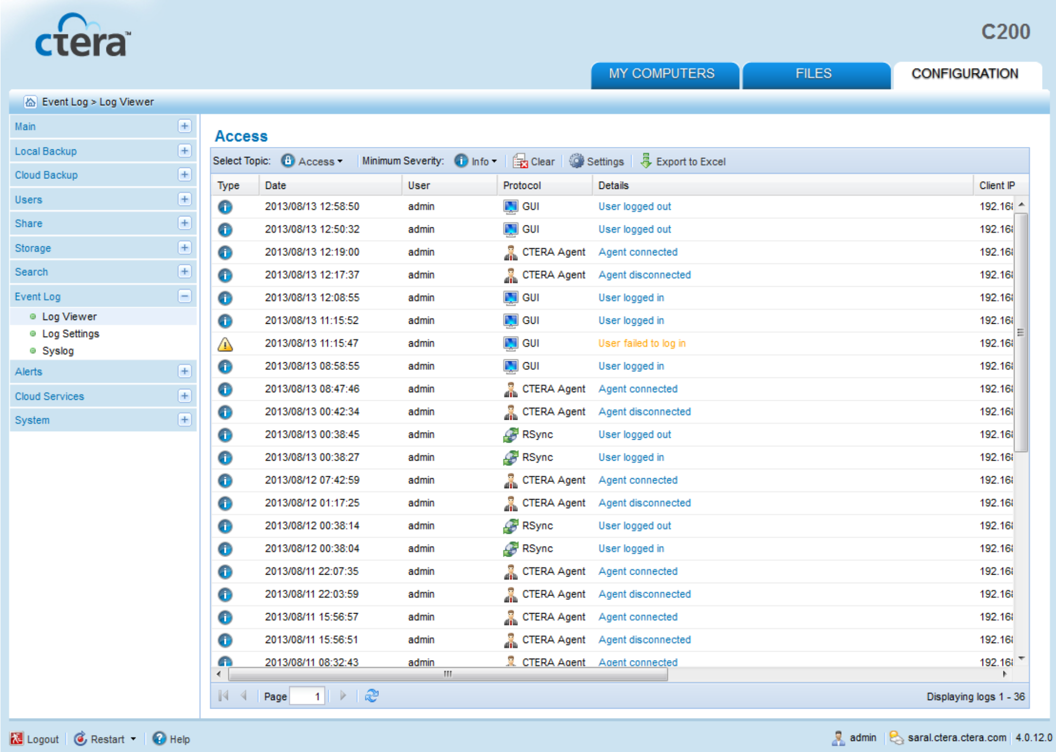
To view Access logs

1. In the **Configuration** tab's navigation pane, click **Event Log > Log Viewer**.

   The **Event Log > Log Viewer** page appears.

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

The Access logs appear.



The following information is displayed:

Table 71: Access Log Fields

This field...	Displays...
Type	An icon indicating the log level. See ***Log Levels*** (page 301).
Date	The date and time at which the event occurred.
User	The user that triggered the event.
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.
More Info	Additional information about the event.

Viewing Audit Logs

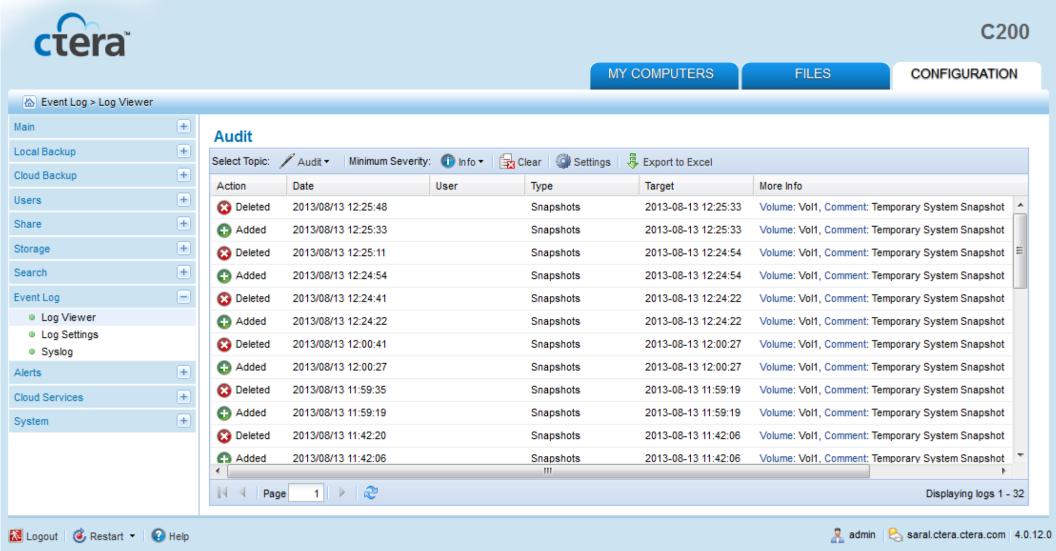
To view Audit logs

1. In the **Configuration** tab's navigation pane, click **Event Log > Log Viewer**.

   The **Event Log > Log Viewer** page appears.

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

The Audit logs appear.



The following information is displayed:

Table 72: Audit Log Fields

This field...	Displays...
Action	The action type. See ***Audit Log Action Types*** (page 310).
Date	The date and time at which the event occurred.
User	The user who performed the action.
Type	The type of setting that was affected by the action. For example, if user JohnS was deleted, this column displays "Users".
Target	The object that was affected by the action. For example, if user JohnS was deleted, this column displays "JohnS".
More Info	Additional information about the event.

Table 73: Action Types

Icon	Label	Description
	Added	An object was added to the appliance Web interface.
	Deleted	An object was deleted from the appliance Web interface.
	Modified	An object was modified.

	Formatted	A disk was formatted.
	Expanded	An array was enlarged.
	Disabled	A setting was disabled.
	Enabled	A setting was enabled.

Viewing CTERA Agents Logs

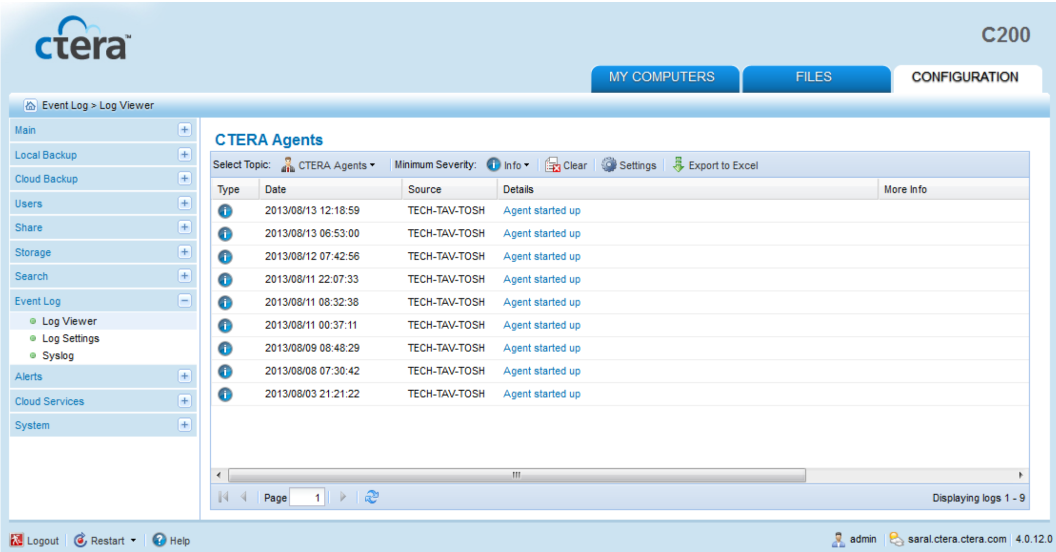
To view CTERA Agents logs

1. In the **Configuration** tab's navigation pane, click **Event Log > Log Viewer**.

   The **Event Log > Log Viewer** page appears.

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

   The CTERA Agents logs appear.



The following information is displayed:

Table 74: CTERA Agents Log Fields

This field...	Displays...
Type	An icon indicating the log level. See ***Log Levels*** (page 301).
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.

Filtering Logs

In any log category, you can filter the logs so that only those with a certain minimum log level are displayed.

Tip

For information on configuring the default minimum log level to display in *all* log pages, see ***Configuring Event Log Settings*** (on page 296).

To filter logs in a log category

1. View the desired log category.

   See ***Viewing Logs*** (on page 299).

2. In the **Minimum Severity** drop-down list, select the minimum log level to display in this category.

   For example, if you select Critical, then only Alert, Critical, and Emergency logs will be displayed.

   The logs are filtered accordingly.

Clearing Logs

You can clear logs for any log category.

To clear logs for a log category

1. View the desired log category.

   See ***Viewing Logs*** (on page 299).

2. Click **Clear**.

   A confirmation message appears.

3. Click **Yes**.

The logs in this category are cleared.

Exporting Logs

You can export logs in any category to a Comma-Separated Values (*.csv) file on your computer, which you can view in Microsoft Excel as a worksheet.

To export logs in a log category

1. View the desired log category.

   See ***Viewing Logs*** (on page 299).

2. Click **Export to Excel**.

   The logs are exported.

Configuring Email Alerts

You can configure the appliance to send alerts upon important events. The alerts can be sent to up to two email addresses.

Workflow

To configure the appliance to send email alerts, do the following:

1. Configure mail server settings.

   See ***Configuring Mail Server Settings*** (on page 314).

2. Configure email alert settings.

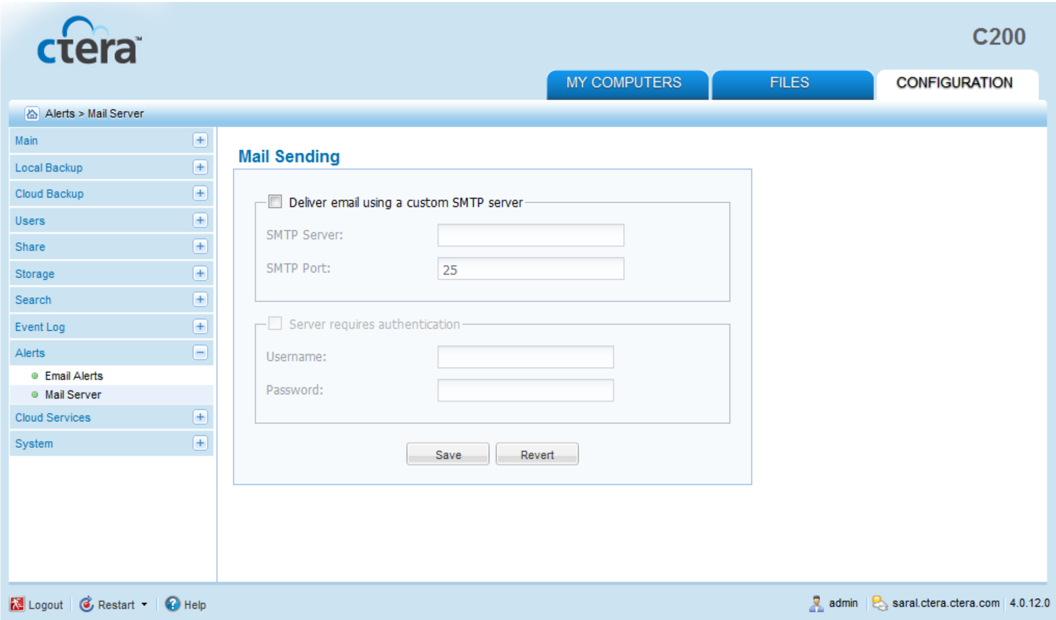
   See ***Configuring Email Alert Settings*** (on page 316).

Configuring Mail Server Settings

To configure mail server settings

1. In the **Configuration** tab's navigation pane, click **Alerts > Mail Server**.

   The **Alerts > Mail Server** page appears.



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

Table 75: Mail Server Fields

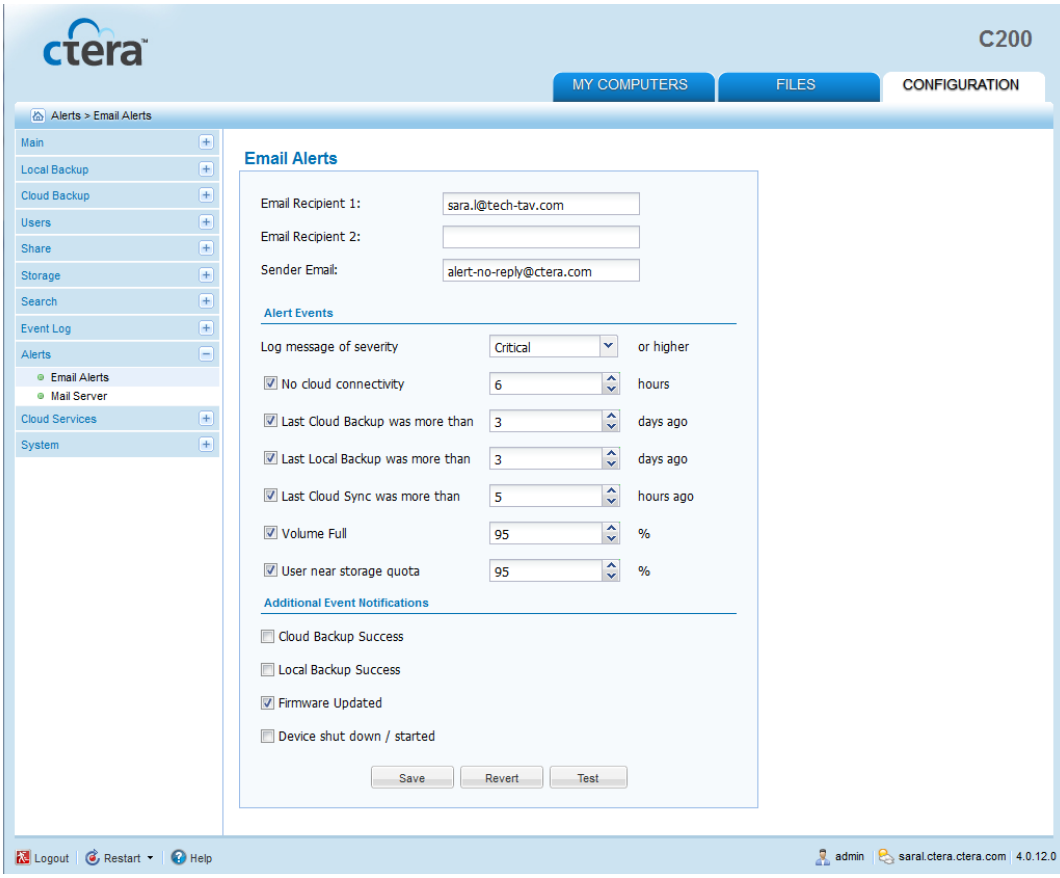
In this field...	Do this...
Deliver email using a custom SMTP server	Select this option to enable email alerts. Additional fields are enabled.
SMTP Server	Type the SMTP server's IP address.
SMTP Port	Type the SMTP server's port number. The default value is 25.
Server requires authentication	Select this option to indicate that the SMTP server requires authentication. The **Username** and **Password** fields are enabled, and you must complete them.
Username	Type the user name to use when authenticating to the SMTP server.
Password	Type the password to use when authenticating to the SMTP server.

Configuring Email Alert Settings

To configure email alerts

1 In the **Configuration** tab's navigation pane, click **Alerts > Email Alerts**.

The **Alerts > Email Alerts** page appears.



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

3 Click **Save**.

4 To test the configuration, click **Test**.

A test email is sent to the specified email addresses.

Table 76: Email Alerts Fields

In this field...	Do this...
Email Recipient 1 / **Email Recipient 2**	Type an email address to which email alerts should be sent.
Sender Email	Type the email address that should appear in the **From** field of email alerts. The default value is alert-no-reply@ctera.com.
Log message of severity	Select the minimum event severity level for which to send email alerts.
No cloud connectivity	To send an email alert when there is no cloud connectivity for more than a certain number of hours, select this option, then use the arrows to specify the desired number of hours. The default value is 6 hours.
Last Cloud Backup was more than	To send an email alert when the last cloud backup operation was performed more than a certain number of days ago, select this option, then use the arrows to specify the desired number of days. The default value is 6 days.
Last Local Backup was more than	To send an email alert when the last local backup operation was performed more than a certain number of days ago, select this option, then use the arrows to specify the desired number of days. The default value is 6 days.
Last Cloud Sync was more than	To send an email alert when the last cloud synchronization operation was performed more than a certain number of hours ago, select this option, then use the arrows to specify the desired number of hours. The default value is 5 hours.
Volume Full	To send an email alert when a volume is more than a certain percentage full, select this option, then use the arrows to specify the desired percentage. The default value is 95%.
User near storage quota	To send an email alert when more than a certain percentage of a user's disk storage quota has been consumed, select this option, then use the arrows to specify the desired percentage. The default value is 95%.

Cloud Backup Success	To send an email alert when an cloud backup operation has been performed successfully, select this option.
Local Backup Success	To send an email alert when a local backup operation has been performed successfully, select this option.
Firmware Updated	To send an email alert when the appliance firmware has been updated, select this option.
Device shut down / started	To send an email alert upon appliance startup and shutdown, select this option.

18

Maintenance

In This Chapter

Viewing the Appliance Details

You can view general information about the appliance, including serial number, appliance model, and installed firmware version.

To view the appliance details

- In the **Configuration** tab's navigation pane, click **Main > This Device**.

  The **Main > This Device** page appears, displaying the product information.

Configuring the CTERA Appliance Name and Location

You can configure the appliance's details, including its name and location.

The appliance name is used as a unique identifier of this appliance on your network. This name must be different than any other appliance or PC on your network. The location field enables you to document your appliance’s physical location, and is optional.

To configure the appliance name and location

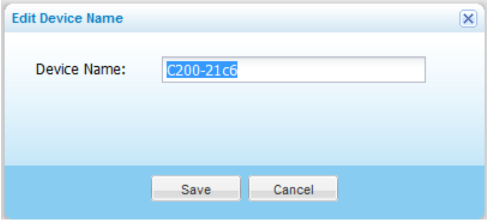
1. In the **Configuration** tab's navigation pane, click **Main > This Device**.

   The **Main > This Device** page appears, displaying the product information.

2. To configure the appliance name, do the following:

   a. Next to the **Device Name** field, click **Edit**.

The **Edit Device Name** dialog box appears.



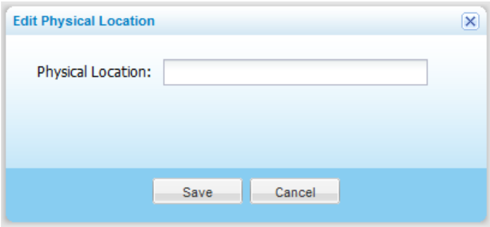
b In the **Device Name** field, type the name that should represent the appliance in your network neighborhood.

c Click **Save**.

3 To configure the appliance's physical location, do the following:

a Next to the **Physical Location** field, click **Edit**.

The **Edit Physical Location** dialog box appears.



b In the **Physical Location** field, type the appliance's location.

For example: “Delaware Branch Office”.

c Click **Save**.

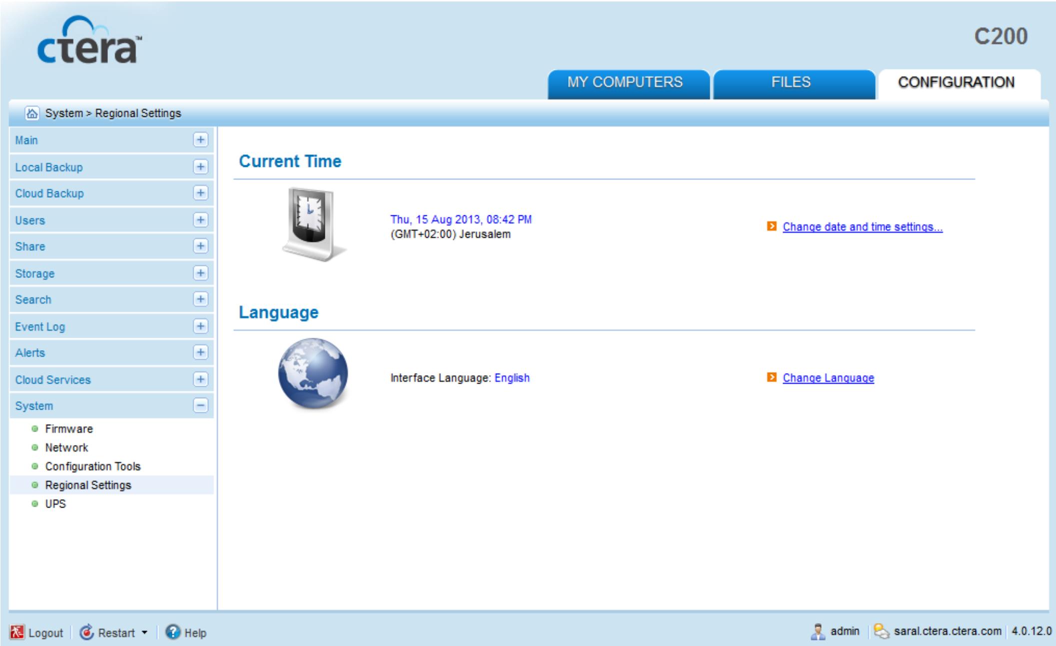
Configuring the CTERA Appliance Time and Date

You can configure the appliance to obtain the time and date from a time server, or you configure the time and date manually.

To configure the appliance time and date

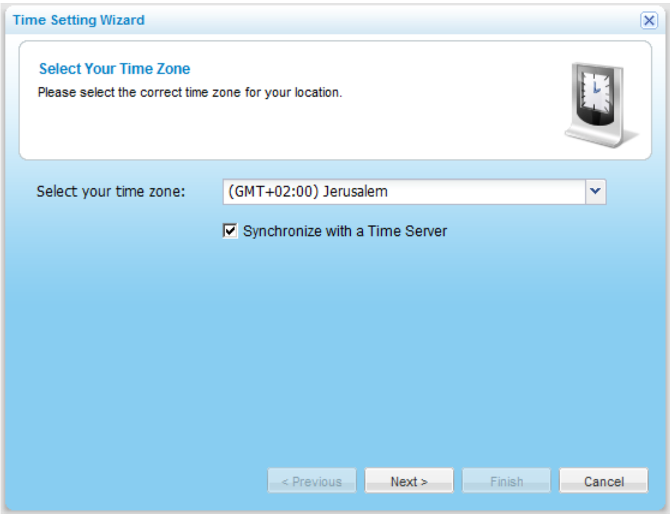
1 In the **Configuration** tab's navigation pane, click **System > Regional Settings**.

The **System > Regional Settings** page appears, displaying the date, time, and time zone currently configured on the appliance.



2 Click **Change date and time settings**.

The **Time Setting Wizard** opens, displaying the **Select Your Time Zone** dialog box.



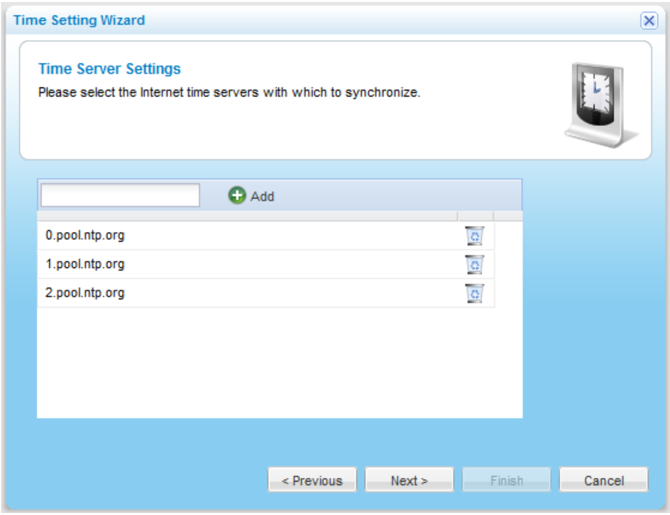
3 In the **Select your time zone** drop-down list, select your time zone.

4 Do one of the following:

- To synchronize the appliance with a time server, select the **Synchronize with a Time Server** check box.
- To manually configure time and date settings on the appliance, clear the **Synchronize with a Time Server** check box.

5 Click **Next**.

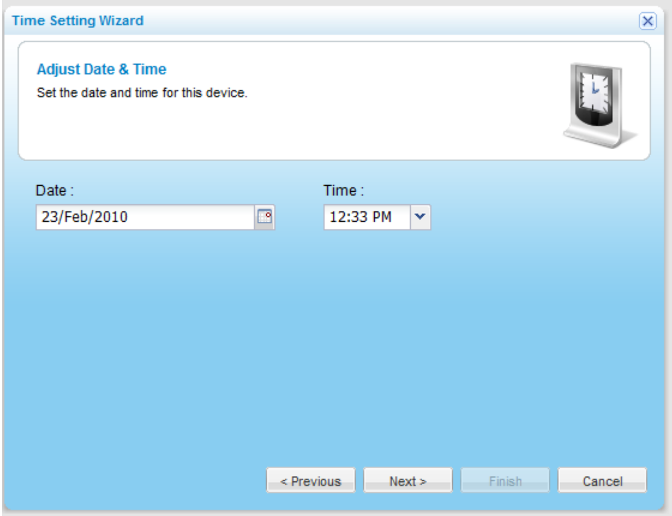
- If you chose to synchronize the appliance with a time server, the **Time Server Settings** dialog box appears with a list of time servers with which the appliance will synchronize time and date settings.



Do the following:

1. To add a time server to the list, type the server's URL in the field provided, then click **Add**.
2. To remove a time server from the list, in the server's row, click  .

- If you chose to manually configure time and date settings on the appliance, the **Adjust Date & Time** dialog box appears.



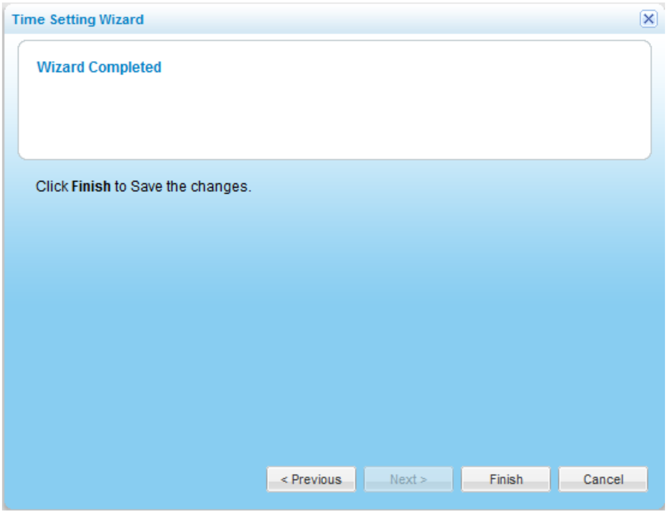
Do the following:

1 In the **Date** field, type the current date, or click  to select the date from a calendar.

2 In the **Time** drop-down list, select the current time.

6 Click **Next**.

The **Wizard Completed** screen appears.



7 Click **Finish**.

Configuring the User Interface Language

You can configure the language to be displayed in the appliance's interface.

The following languages are supported: English, French, German, Hebrew, Italian, Polish, and Spanish.

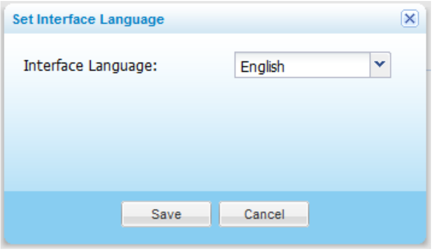
To configure the user interface language

1. In the **Configuration** tab's navigation pane, click **System > Regional Settings**.

   The **System > Regional Settings** page appears, displaying the date, time, and time zone currently configured on the appliance.

2. Click **Change Language**.

   The **Set Interface Language** dialog box appears.



3. In the **Interface Language** drop-down list, select your language.
4. Click **Save**.

Updating the Firmware

You can configure your appliance to automatically download and install firmware updates. Alternatively, you can install firmware updates manually.

Configuring Automatic Firmware Updates

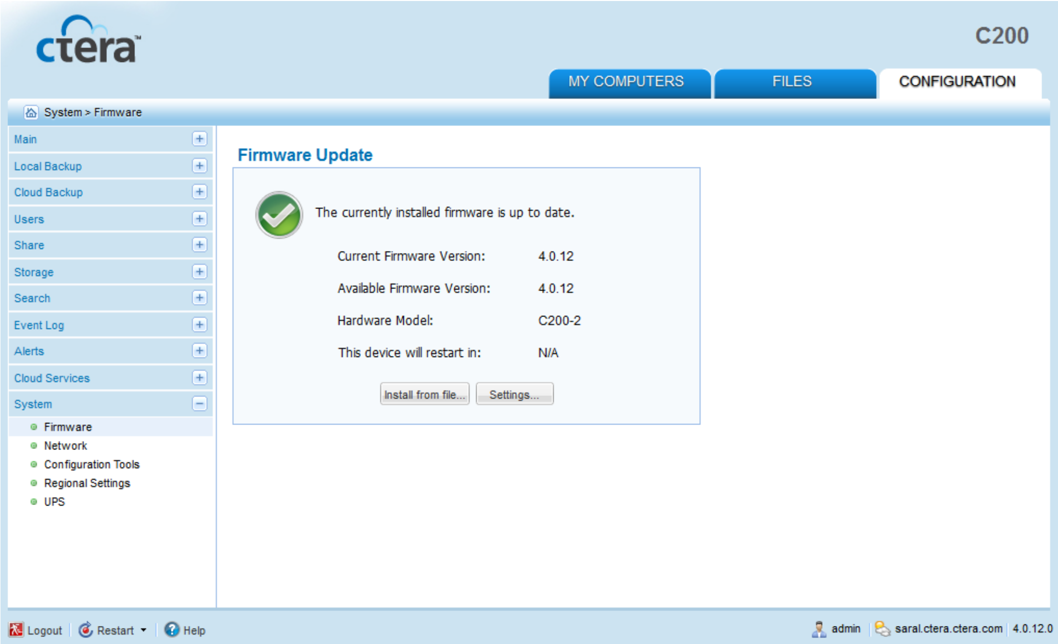
To configure automatic firmware updates

1. In the **Configuration** tab's navigation pane, click **System > Firmware**.

   The **System > Firmware** page appears, displaying the following information:

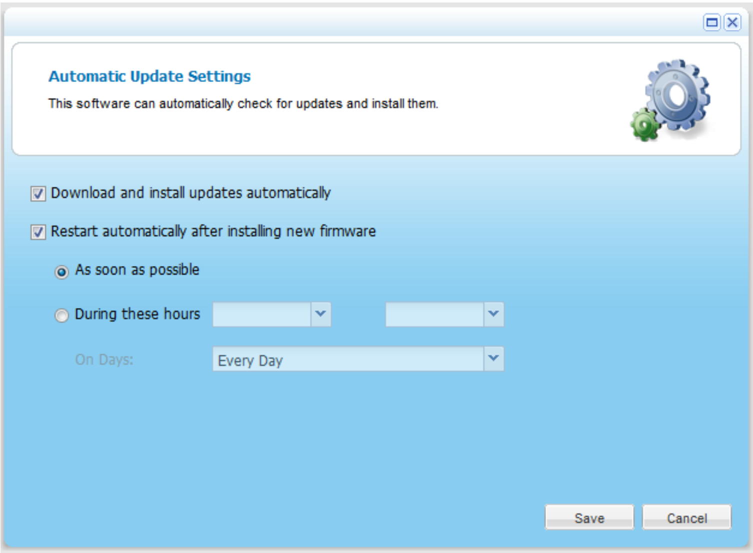
   - The currently installed firmware version
   - The most recent available firmware version
   - The appliance model

- The amount of time remaining until the appliance restarts. This information is displayed if a firmware has been downloaded, and the appliance is configured to reboot automatically.



2 Click **Settings**.

The **Automatic Update Settings** dialog box opens.



3 To specify that the appliance should download and install firmware updates automatically, click **Download and install updates automatically**.

If you do not select this option, you must perform firmware updates manually, as described in ***Manually Updating the Firmware*** (on page 327).

4 To specify that the appliance should automatically reboot after installing new firmware updates, do the following:

a Click **Restart automatically after installing new firmware**.

b 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 appliance will reboot as soon as it is recommended to do so. For example, the automatic reboot might be deferred, if the appliance is undergoing system maintenance that should not be interrupted.

- To reboot only during specific hours, choose **During these hours**, then use the drop-down down lists to specify the desired time range.

If you do not enable automatic rebooting, then you will need to reboot the appliance as described in ***Restarting the CTERA Appliance*** (on page 332), when this page indicates that a new update has been installed.

5 Click **Save**.

Manually Updating the Firmware

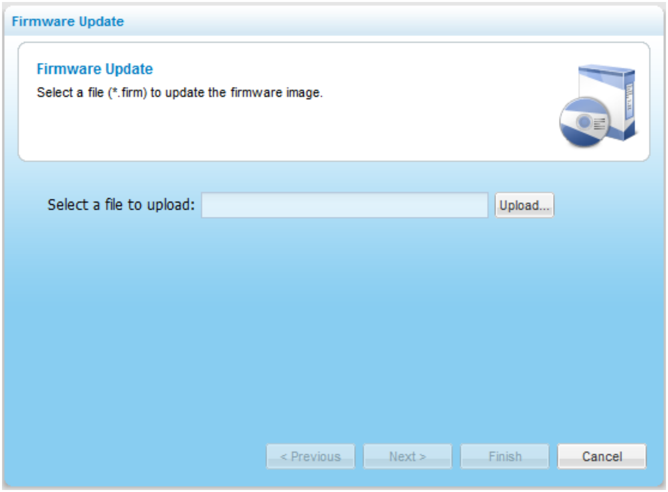
To manually update the firmware

1 In the **Configuration** tab's navigation pane, click **System > Firmware**.

The **System > Firmware** page appears, displaying the currently installed firmware version, as well as the appliance model.

2 Click **Install from file**.

The **Firmware Update Wizard** opens, displaying the **Firmware Update** dialog box.



3 Click **Upload** and browse to your firmware (*.firm) file.

The firmware file is uploaded.

The **Completing the Firmware Update Wizard** appears.

The appliance automatically reboots.

Exporting and Importing CTERA Appliance Settings

You can manually export the appliance configuration to an *.xml file on your computer, and use this file to restore the appliance settings as needed.

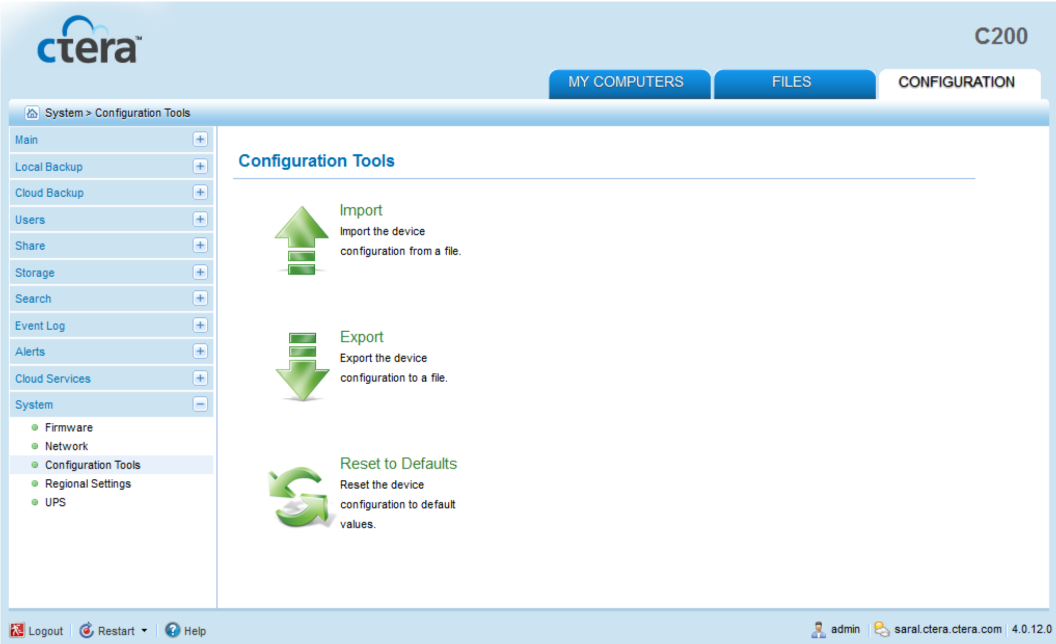
In addition, the appliance automatically backs up its configuration to the CTERA Portal each time cloud backup runs. The backed up settings can be downloaded from the CTERA Portal and restored as needed. See ***Restoring Appliance Configuration from Cloud Backup*** (on page 183).

Exporting the Configuration

To export the appliance configuration

1 In the **Configuration** tab's navigation pane, click **System > Configuration Tools**.

The **System > Configuration Tools** page appears.



2 Click **Export**.

The appliance configuration are exported to an *.xml file on your computer.

Tip

For security reasons, all passwords are stored in a format that makes them non-human-readable. Despite this, the export file information is sensitive, and it is therefore recommended to keep it in a safe place.

Importing the Configuration

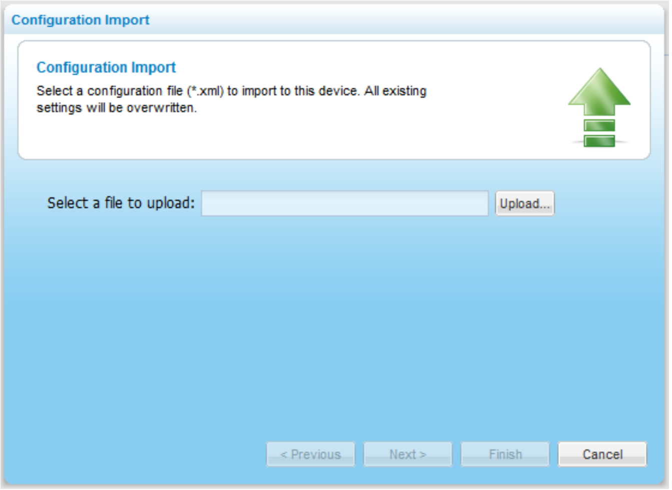
To import the appliance configuration from a previously exported configuration file

1 In the **Configuration** tab's navigation pane, click **System > Configuration Tools**.

The **System > Configuration Tools** page appears.

2 Click **Import**.

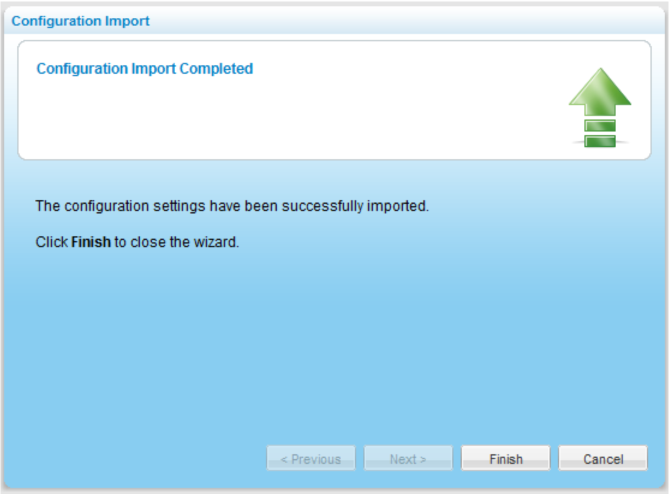
The **Configuration Import** wizard opens, displaying the **Configuration Import** dialog box opens.



3 Click **Upload** and browse to the appliance configuration file.

The configuration file is imported.

Once the upload is complete, the **Configuration Import Completed** screen appears.



If any errors occurred during the import, they are displayed.

4 Click **Finish**.

Viewing Attached UPS Device Details

You can view general information about attached USB-based UPS (Uninterruptible Power Supply) devices, including vendor and model, power status, estimated remaining protection time, and battery charge level.

If the UPS device's reported state is "Low Battery", the appliance will automatically initiate an orderly shut down procedure.

UPS devices that support the USB HID power device class, such as those from APC and TrippLite, are supported. For additional information, contact the device vendor.

To view details about attached UPS devices

- In the **Configuration** tab's navigation pane, click **System > UPS**.

  The **System > UPS** page appears displaying the information in the following table.

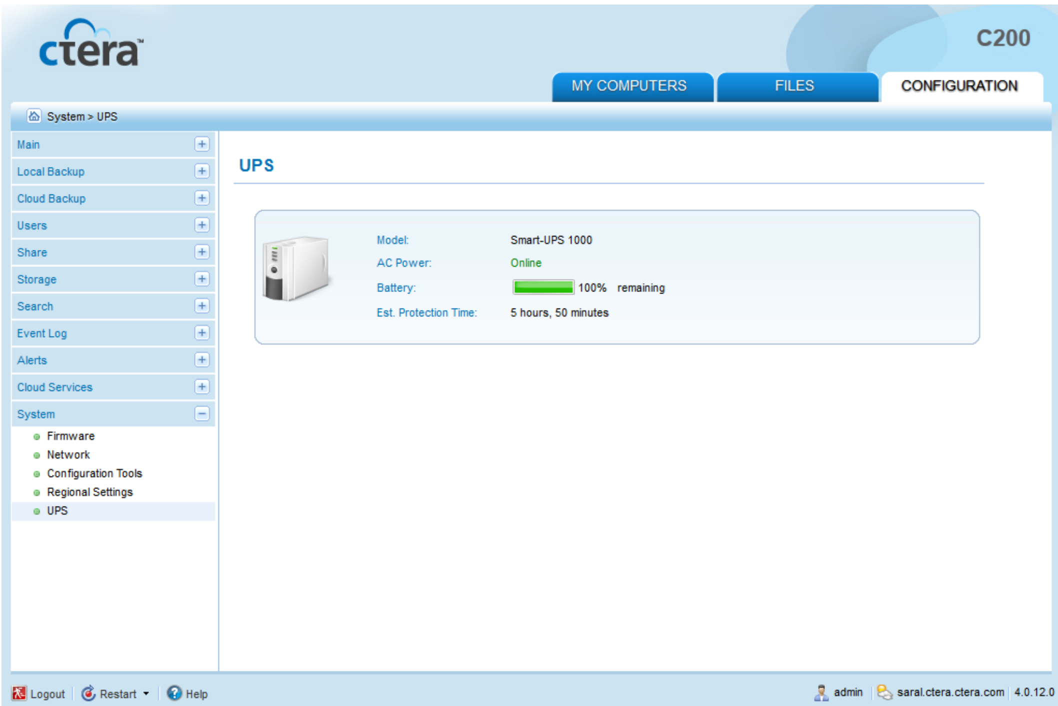


Table 77: UPS Fields

In this field...	Do this...
Model	The UPS device model.
AC Power	The UPS device's power status. This can be any of the following: - **Online** - **On Battery** - **Low Battery**
Battery	The amount of battery charge remaining.
Est. Protection Time	The estimated amount of protection time remaining.

Resetting the CTERA Appliance to Its Default Settings

You can reset the appliance to its default settings.

Warning

This action erases all of your passwords and settings, and you will need to reconfigure the appliance as described in ***Setting Up the CTERA Appliance*** (on page 44).

The appliance can be reset to defaults via the appliance Web interface or using the **Reset** button on its rear panel.

To reset the appliance to its default settings via the appliance Web interface

1. In the **Configuration** tab's navigation pane, click **System > Configuration Tools**.

   The **System > Configuration Tools** page appears.

2. Click **Reset to Defaults**.

   A confirmation message appears.

3. Click **Yes**.

   The appliance is reset to its default settings.

   The **Login** page appears.

To reset the C200 to its default settings using the Reset button

- While the appliance is up and running, press the **Reset** button for at least 10 seconds.

  The appliance is reset to its default settings and reboots.

To reset the C400/C800 to its default settings using a serial cable

1. Shut down the appliance.

See ***Shutting Down the CTERA Appliance*** (on page 333).

2 Connect to the appliance's COM port using a serial cable, and follow the displayed instructions.

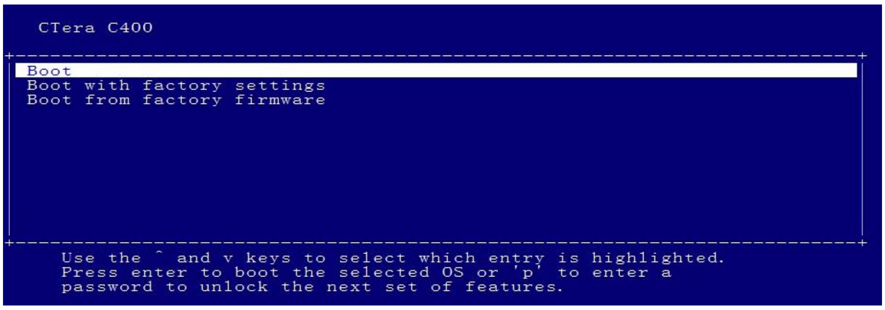
For information on locating the C400's COM port, see ***Rear Panel*** (on page 16).

For information on locating the C800's COM port, see ***Rear Panel*** (on page 26).

The terminal program must be set to operate using the following specifications: 115200-N-8-1.

3 Switch on the appliance. While the appliance is starting up, the message “Press ESC to enter the menu” will be displayed in the terminal for three seconds. During the three seconds, press the ESC key.

The following menu appears:



4 Select **Boot with factory settings**.

The appliance boots with the default settings.

Restarting the CTERA Appliance

If you are experiencing problems with your appliance, you can restart it. This may solve the problem.

The appliance can be restarted via the appliance Web interface or using the **Reset** button on its rear panel.

To restart the appliance via the Web interface

1 In the status bar, in the **Shutdown** pop-up list, click **Restart**.

A confirmation message appears.

2 Click **Yes**.

The appliance restarts.

To perform a hard restart

- While the appliance is on, do one of the following:

- In the C200, press the **Reset** button briefly.
- In the C400, turn the power switch at the back of the appliance to the OFF position and then back to the ON position.
- In the C800, turn the power switch at the front of the appliance to the OFF position and then back to the ON position.

Shutting Down the CTERA Appliance

The appliance can be shut down via the appliance Web interface or using the **Power** button on its rear panel.

Warning

Do not disconnect the power supply cable from the wall outlet without first shutting down the appliance. Doing so could result in data loss.

To shut down the appliance via the appliance Web interface

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

A confirmation message appears.

2 Click **Yes**.

The appliance shuts down.

To shut down the appliance using the Power button

- Do one of the following:
  - In the C200, press the **Power** button until the appliance shuts down.
  - In the C400, turn the power switch at the back of the appliance to the OFF position.
  - In the C800, turn the power switch at the front of the appliance to the OFF position.

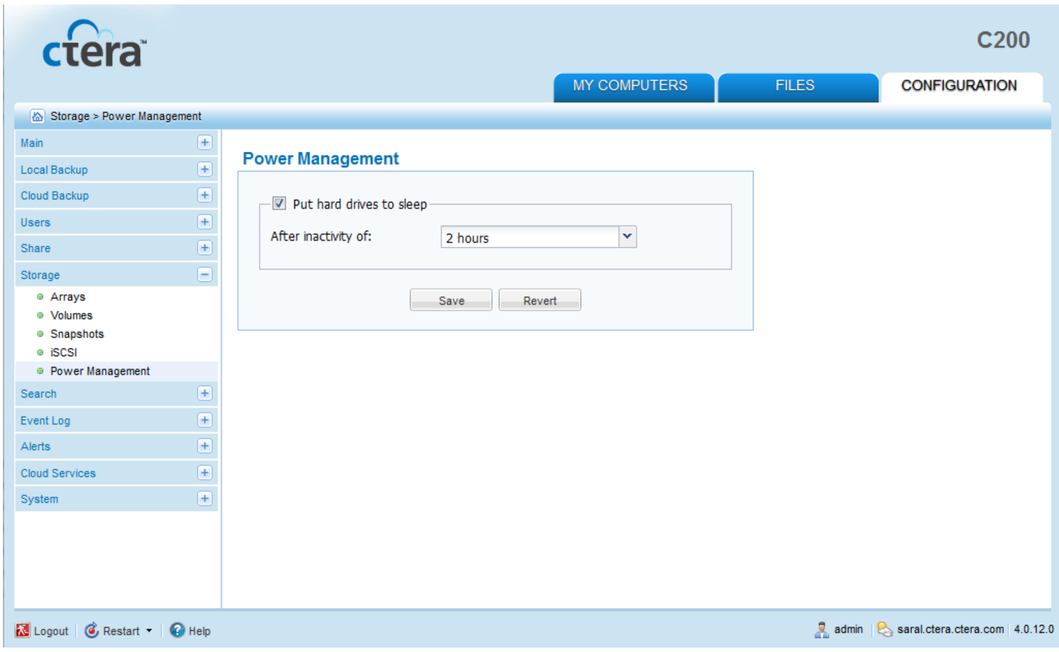
Managing Power Usage

You can conserve power by configuring the appliance to turn off its hard drives after a period of inactivity.

To manage appliance power usage

1 In the **Configuration** tab's navigation pane, click **Storage > Power Management**.

The **Storage > Power Management** page appears.



2 Select the **Put hard drives to sleep** check box.

3 In the **After inactivity of** drop-down list, select the amount of time after which the hard drives should be put to sleep if inactive.

4 Click **Save**.

19

Legal Information

This chapter contains important legal information about your CTERA products.

In This Chapter

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, Imber 24, 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 User 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 agrees 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.

CTERA Limited Hardware Warranty

Limited Hardware Warranty. CTERA warrants that the hardware components of the product supplied to you by CTERA or its authorizes partners (the "**Hardware Product**") shall be free from material defects in design, materials, and workmanship and will function, under normal use and circumstances, materially in accordance with the documentation provided with such Hardware Products for a period of one year from the date of shipment by CTERA. Your sole and exclusive remedy, and CTERA's sole and exclusive liability for defective hardware components shall be that CTERA, at its sole option, subject to the terms and conditions of this Warranty, and solely upon confirmation of a defect or failure of a hardware component to perform as warranted, shall either repair or replace the nonconforming hardware component. All replacement parts furnished to You under this warranty shall be new or refurbished and equivalent to new, and shall be warranted as new for the remainder of the original warranty period. All defective parts, which have been replaced, shall become the property of CTERA. All defective parts that have been repaired shall remain Your property.

Procedures. A Hardware Product or one of its component parts may only be returned to CTERA with CTERA's prior written approval. Any such approval shall reference a returned material authorization number issued by an authorized CTERA service representative. Transportation costs, if any, incurred in connection with the return of a defective item to CTERA shall be borne by You. Any transportation costs incurred in connection with the redelivery of a repaired or replacement item to You by CTERA shall be borne by CTERA; provided, however, that if CTERA determines, in its sole discretion, that the allegedly defective item is not covered by the terms of the warranty or that a warranty claim is made after the warranty period, the cost of the repair by CTERA, including all shipping expenses, shall be reimbursed by You.

Exclusions. The foregoing warranties and remedies shall be void as to any Hardware Products damaged or rendered unserviceable by one or more of the following: (1) improper or inadequate maintenance by anyone other than CTERA or CTERA's authorized agents, (2) software or interfacing supplied by anyone other than CTERA, (3) modifications, alterations or additions to the Hardware Products by personnel not certified by CTERA or CTERA's authorized agents to perform such acts, or other unauthorized repair, installation or opening or other causes beyond CTERA's control, (4) unreasonable refusal to agree with engineering change notice programs, (5) negligence by any person other than CTERA or CTERA's authorized agents, (6) misuse, abuse, accident, electrical irregularity, theft, vandalism, fire, water or other peril, (7) damage caused by containment and/or operation outside the environmental specifications for the Hardware Products, (8) alteration or connection of the Hardware Products to other systems, equipment or devices (other than those specifically approved by CTERA) without the prior approval of CTERA, or (9) any use that is inconsistent with the user manual supplied with the Hardware Product.

Limitation of Liability. NOTWITHSTANDING ANYTHING ELSE IN THIS WARRANTY OR OTHERWISE, NEITHER CTERA NOR ITS SUPPLIERS WILL BE LIABLE WITH RESPECT TO ANY SUBJECT MATTER OF THIS WARRANTY UNDER ANY CONTRACT, NEGLIGENCE, STRICT LIABILITY, OR OTHER LEGAL OR EQUITABLE THEORY, REGARDLESS OF WHETHER CTERA WAS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES: (i) FOR ANY PUNITIVE, INCIDENTAL OR CONSEQUENTIAL DAMAGES OR LOST DATA OR LOST PROFITS. IN THE EVENT THAT CTERA FAILS TO EITHER REPAIR OR REPLACE THE NONCONFORMING HARDWARE COMPONENT IN ACCORDANCE WITH THIS WARRANTY, YOU SHALL ONLY BE ENTITLED, AS A SOLE AND EXCLUSIVE REMEDY, TO A REFUND OF THE AMOUNT PAID FOR THE HARDWARE PRODUCT.

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

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.

Declaration of Conformity

The product described in this guide and associated peripherals manufactured by CTERA Networks Ltd., to which this declaration relates is in conformity with:

European Community

This product complies with the essential requirements specified in Article 3.1 (a) and 3.1 (b) of:

- **Directive 2004/108/EC and 89/336/EEC (EMC Directive).**
- **Directive 73/23/EEC (Low Voltage Directive – LVD).**
- **Directive 99/05/EEC (Radio Equipment and Telecommunications Terminal Equipment Directive).**

In accordance with the following Harmonized Standards-

The products are compliant with the following standards and other normative documents:

EMC:	EN 55022: 2006 Class B
	EN 55024: 1998 +A1: 2001 +A2: 2003
	EN 61000-3-2: 2006 Class A
	EN 61000-3-3: 1995 +A1: 2001 +A2:2005

Safety / Low Voltage:	IEC 60950-1: 2005
	EN 60950-1: 2006

Regulatory Notice to European Customers

The "CE" mark is affixed to this product to demonstrate conformance to the R&TTE Directive 99/05/EEC (Radio Equipment and Telecommunications Terminal Equipment Directive).

USA & Canada

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference, and
2. this device must accept any interference received, including interference that may cause undesired operation

This Class B Digital apparatus, Complies with Canadian Standard ICES-003.

The products are compliant with the following standards:

EMC:	FCC Part 15, Class B
	CISPR 22: 1997 +A1: 2000
	ICES-003: 2004
Safety / Low Voltage:	CAN/CAS C22.2 No. 60950-1
	UL60950-1

Federal Communications Commission Radio Frequency Interference Statement

Products comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules.

These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment.

This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications.

Shielded cables must be used with this equipment to maintain compliance with FCC regulations.

Changes or modifications not expressly approved by the manufacturer could void the user's authority to operate the equipment.

RoHS & WEEE

CTERA Networks is proudly committed to the protection and preservation of the environment.

This device complies with EU Directive on the Restriction of the use of certain Hazardous Substances in electrical and electronic equipment (RoHS – 2002/95/EC), and Directive of the European Parliament and of the Council on Waste Electrical and Electronic Equipment (WEEE – 2002/96/CE).

Environmental Data – Product's Materials Information Restricted Substances

CTERA products do NOT contain any of the following substances in concentrations exceeding legal threshold limits:

- Asbestos
- colorants in components that come into direct contact with human skin
- Cadmium and its compounds (except for use in applications exempted by the EU RoHS Directive)
- Class I and Class II CFCs (chlorofluorocarbons) and HCFCs (hydro fluorocarbons)
- Chloroparaffins, short chained (10-13 carbon chain)
- Chromium VI and its compounds (except for use in applications exempted by the EU RoHS Directive)
- Halogenated dioxins or furans (i.e. polychlorinated dibenzodioxines, polychlorinated dibenzofurans)
- Lead and its compounds (except for use in applications exempted by the EU RoHS Directive)

- Mercury (except for use in applications exempted by the EU RoHS Directive)
- Nickel and its compounds in components that are likely to result in prolonged skin exposure
- PCBs (polychlorobiphenyls) or PCTs (polychloroterphenyls)
- PBBs (polybromobiphenyls) or PBDEs (polybrominated diphenylethers)
- PVC (polyvinyl chloride) in plastic parts greater than 25 grams
- Polychlorinated naphthalenes (PCNs)
- Tributyl tin (TBT) and triphenyl tin (TPT) compounds

Additional Materials Information

- The cables may use PVC as an insulating material to ensure product safety
- Product may contain post-industrial recycled content (plastics, metal, glass)

No CFCs (chlorofluorocarbons), HCFCs (hydrofluorocarbons) or other ozone depleting substances are used in packaging material.

Chromium, lead, mercury, or cadmium are not intentionally added to packaging materials and are not present in a cumulative concentration greater than 100 ppm as incidental impurities. No halogenated plastics or polymers are used for packaging material.

The System fully complies with the EU Directive 94/62/EEC.

The product has been tested in a typical configuration.

For a copy of the original signed declaration (in full conformance with EN45014), please contact CTERA Technical Support at www.ctera.com/support.

Index

D

E

W