ctera your files. your cloud.

RELEASE NOTES

CTERA Portal 8.3.3000.44

May 2026

CONTENTS

1

CTERA PORTAL 8.3.3000.44

The CTERA Portal is an enterprise file services delivery platform comprising a multi-cloud Global File System as well as multi-tenant management of CTERA Edge Filers and CTERA Drive Share and Drive Protect clients.

This chapter contains the following topics:

LICENSING CTERA PORTAL

A *Cloud Drive Connect* license is available which is a subset of the existing full license for users who do not need to collaborate on shared documents and folders with other users, for mobile users, and for zero-minute disaster recovery.

SECURITY CONSIDERATIONS

CTERA Networks Ltd. is constantly looking at ways to improve security, for example by resolving external threats. CTERA recommends using the latest portal image as many of the security fixes require upgrading the portal image as well as the software.

INSTALLING OR UPGRADING CTERA PORTAL

Note: **You can only upgrade to a new version from an immediate previous version. If you have an older version, you must first upgrade in steps, first to an intermediate previous version and then to the new version. For example, to upgrade from 8.1.x requires first upgrading to 8.2.1500.58 or later and then to this version.**

For full installation details, refer to your environment under Installing a CTERA Portal.

Warning: **Before changing the IP address for the portal server instance you must wait until all the portal services, such as Nomad and Consul, have loaded. Loading the portal services take at least 5 minutes.**

Upgrading the CTERA Portal

Both the CTERA Portal image and software on all portal servers can be upgraded as described in Upgrading a CTERA Portal. Upgrading the portal image also upgrades the portal software. After upgrading the portal image on every server in the cluster, you must reboot every server in the CTERA Portal environment.

Pre-upgrade Requirements

If SHA-1 certificates are in use, they must be replaced with SHA-2-based signatures before starting the upgrade.

You can only upgrade from CTERA Portal version 8.2.1500.58 or later.

You cannot upgrade the portal while running a storage node migration.

General Considerations

If you are using the Thumbnails service, after upgrading the portal, from the latest 8.2.x version (or at least from 8.2.1500.58), you must disable and then re-enable the service.

After the first server boot at the end of the upgrade, portal components are loaded on to the data pool. Only after these components have successfully been loaded will the user interface become available.

BRANDING CONSIDERATIONS

CTERA recommends branding the portal using the Palette Generator. The CSS files generated can then be incorporated in the branded skin.

Refer to the *CTERA Software Branding Guide* for more details. Contact CTERA support for help branding your portal.

CHECKING THE CTERA PORTAL CLOUD FILE SYSTEM (FSCK)

In order to check the consistency between the CTERA Portal database and the actual data in the storage node, CTERA has a utility, FSCK, similar to the Linux FSCK utility. CTERA FSCK **must** be run only with approval from CTERA support.

WHAT'S NEW

CTERA Portal version 8.3.x was first released with version 8.3.3000.12 and included a number of infrastructure changes as well new features for global and team portal administrators. See What's New in CTERA Portal Version 8.3.x.

New Features

ID Number	Description
—	Support for new access to CTERA Insight.
PIM-7012	Cloudwatch VPC endpoiunts are now supported using the following commands: Get the Cloudwatch endpoint: `cloudWatchVpcEndpoint get <sn_name>` Set the endpoint for the storage node: `cloudWatchVpcEndpoint set <sn_name> <vpc_endpoint>` Remove the endpoint (like setting it to ""): `cloudWatchVpcEndpoint remove <sn_name>` Where *sn_name* `is the storage node name.`

Resolved Issues

ID Number	Description
PIM-7074, PIM-7075	Upgrading a portal caused the CTERA Messaging service status to fail.
PIM-7185	*S3 API Failed* notifications were being sent too frequently.
PIM-7263	Backing up to a Dell OpjectScale (S3) storage node failed.
PIM-7310	*Messaging status has stalled* notifications were being sent too frequently.

KNOWN ISSUES

ID Number	Description
–	Changing the IP address after installing a portal server but prior to the full deployment of portal services like Nomad and Consul causes the deployment to fail. **Workaround**: Wait until all the portal services have been loaded before changing the IP address. If you changed the IP address after the installation but before the full deployment of portal services like Nomad and Consul, run `portal-manage.sh resetdb`. **Warning:** **You must run `portal-manage.sh resetdb` before initializing the portal or joining it to an existing portal cluster.**
CENV-672	Microsoft Defender reports issues when deploying a portal in Azure.
SP-16614	Support users with the relevant permissions cannot create user groups, add or remove users in an existing group nor delete users.

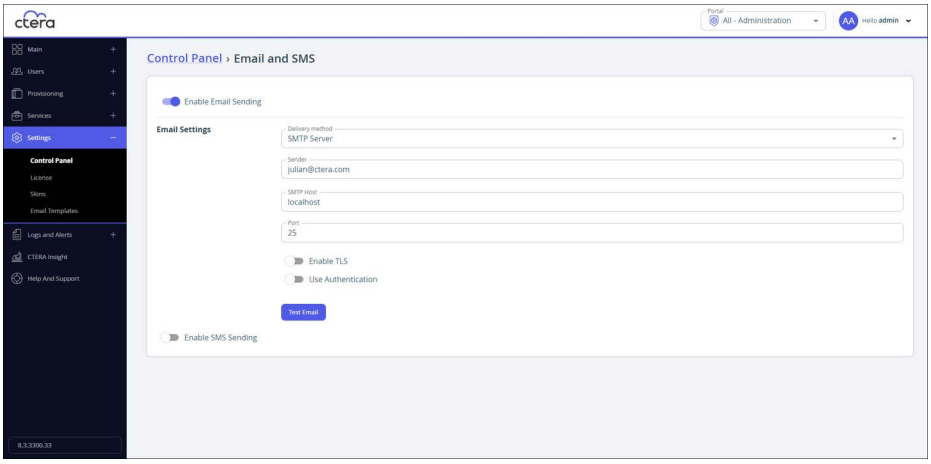
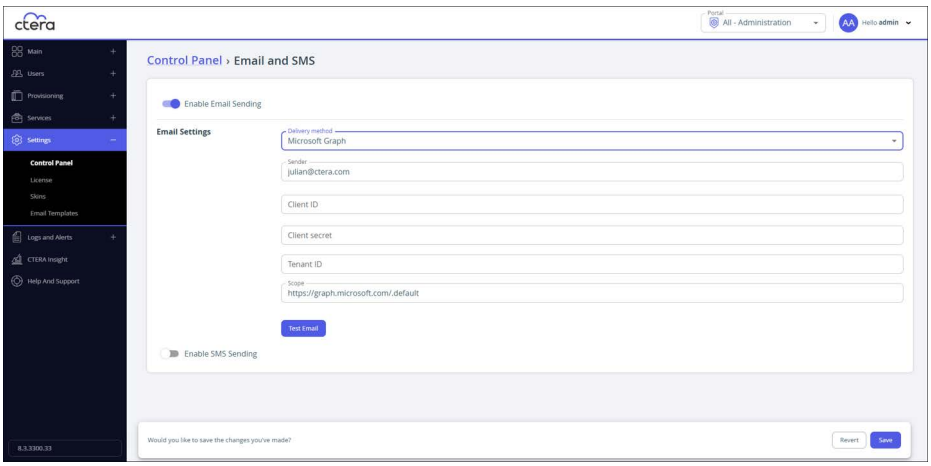
ID Number	Description
SP-17928	After changing a plan name and applying it, the process shows that zero users were updated.
SP-27912	SHA1 is still displayed in the TLS certificate page.
SP-27973	Consul and Nomad do not update after removing a server. Manually refresh the environment.
SP-28514	A file in upload and locked in the database does not appear locked in the GUI.

2

CTERA PORTAL 8.3.3000.40 (APRIL 2026)

WHAT'S NEW

New Features

ID Number	Description
PIM-6171, PIM-6463, PIM-6467, PIM-6469, PIM-6774, PIM-6800, PIM-6840	Microsoft Graph Mail has been integrated to replace SMTP for sending emails securely. **SMTP**:  **Microsoft Graph**:  **Note:** When installing a CTERA Portal, during the initial setup, only the SMTP option is available.

ID Number	Description
PIM-5472, PIM-6158, PIM-6159, PIM-6160	Improved security, including resolving CVE-2025-30065, CVE-2022-41946.

Resolved Issues

ID Number	Description
PIM-6735	pg_wal files were not being removed in a timely way.
PIM-6741	In the **Users** page for a user, selecting a folder in the **Cloud Drive Folders** tab and clicking **View Files** displayed the **Dashboard** and not the folder.
PIM-6975	From version 8.3.3000.36, portal startup was slow.

3

CTERA PORTAL 8.3.3000.36 (MARCH 2026)

WHAT'S NEW

What's New In the Portal Image

ID Number	Description
PIM-4248, PIM-4488, PIM-4490, PIM-4492	When connecting a new secondary server to the primary server on a portal, Nomad is disabled.
PIM-5797	The output from running `portal-dump.sh` now includes `ctera_firstboot.log`.
PIM-5816, PIM-6259	Improved security, including resolving CVE-1999-0524.
PIM-5819	The output when running the command `portal.sh configure-db-recovery n` was malformed.
PIM-5996, PIM-6208, PIM-6668	The docker image for accusoft/prizmdoc-server has been upgraded to 13.28.
PIM-6110	In version 8.3.3000.26, a new portal server could not be added to the portal cluster.
PIM-6273, PIM-6276	Using the CTERA Drive Share email add-in did not send attachments to the portal that had ACLs enabled.
PIM-6318	If the storage node went offline, after the storage node was reconnected, syncing with the portal was stopped until syncing was suspended and then unsuspended.
PIM-6383	A storage node with object lock enabled became offline after upgrading to portal version 8.3.3000.26.
PIM-6399	Portal dumps now include the keep_envoy_alive.log.
PIM-6406	File uploads failed after upgrading a portal with a storage node with a name that does not conform to the latest S3 naming conventions.
PIM-6449	Changing a cloud folder owner failed.
PIM-6628, PIM-6629	In version 8.3.3000.26, after creating a main DB server the setup wizard had to be run twice, running `portal-manage.sh restart` after the first time.

New Features

ID Number	Description
SP-29170	Improved security.

Resolved Software Issues

ID Number	Description
SP-27782	Attempting to generate a monthly report in the user interface returned an error.
SP-28726	Using the AWS SDK for Java to validate a checksum that was returned in the S3 response failed.
SP-29018	In version 8.3.3000.26, skins could not be uploaded to the portal.
SP-29089	In version 8.3.3000.26, after defining a proxy server, both the Thumbnails service and the backup to an S3 bucket failed.
SP-29112	AWS fields were displayed in the VSP One Object (S3) storage node.
SP-29133	The portal report included bad files when files were uploaded to the portal directly and via an edge filer.
SP-29146	`HikariPool-2 - Closing connection` debug messages were logged even when the portal log level was INFO.
SP-29189	Accessing a CTERA Edge Filer remotely from a team portal failed.

4

CTERA PORTAL 8.3.3000.26 (FEBRUARY 2026)

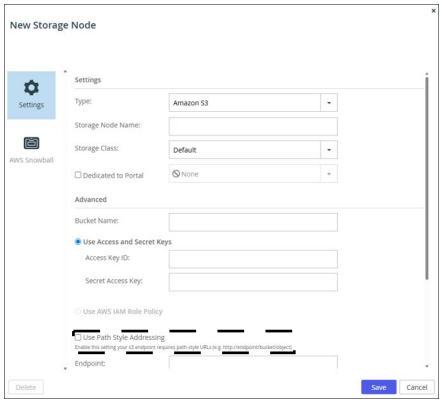
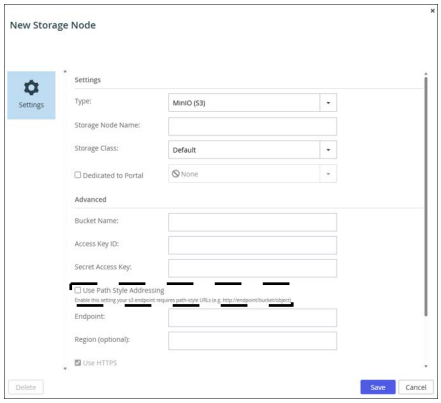
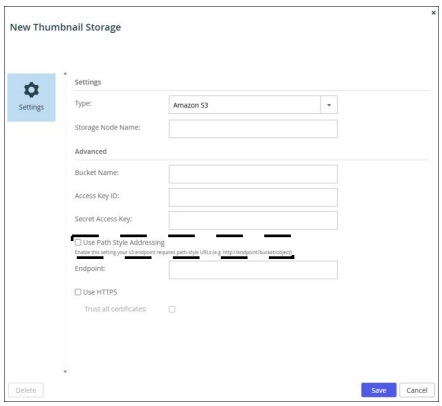
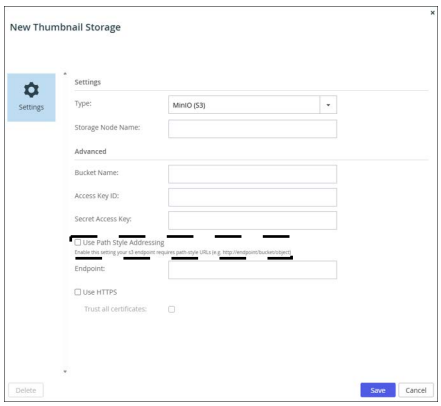
WHAT'S NEW

What's New In the Portal Image

ID Number	Description
PIM-4255	Replacing a messaging server and then replacing the replacement server back to the original server failed.
PIM-5381, PIM-5466, PIM-5499, PIM-5700, PIM-5724	Improved security, including resolving CVE-2024-56337 vulnerability.
PIM-5474	The support report could not be downloaded from the user interface.
PIM-5507, PIM-5686, PIM-5718	Improvements to the Varonis service.

New Features

ID Number	Description
SP-27774, SP-27845, SP-28915	**Upload Only File Sharing Permission** A new permission has been added to file sharing, via public links and collaboration: *Upload Only*, 📤. Upload Only share recipients are able to upload content to the folder but cannot see any of the content that is in the folder.
SP-27817	Better accessibility integration when changing the portal page.
SP-28005, SP-28087	Improved security, including resolving CVE-2024-45216 vulnerability (Apache Solr).
SP-28026, SP-28060, SP-28061, SP-28094, SP-28096	Improvements to the Varonis service.
SP-28235	The name of the user that shared a folder is no longer displayed.

ID Number	Description
SP-28354, SP-28355, SP-28434	The endpoint for both **Amazon S3** and **MinIO (S3)** storage nodes can be specified as either the virtual host, with a certificate provided per bucket, or path style. The option to use the path style is displayed for **Amazon S3** and **MinIO (S3)** storage nodes defined for the portal or defined to be used as storage for the Thumbnails service. For a storage node:   For a thumbnail storage node:   **Note:** Amazon deprecated using the path style, but most products still support its use. The default is to use the virtual host style.
SP-28731, SP-28884	Node.js has been upgraded to Node.js.24.

Resolved Software Issues

ID Number	Description
SP-27025	The portal could not be initialized in FIPS mode.
SP-27509	When using CTERA Insight to monitor the portal, file analytics were not correct.
SP-27989	The *Starting Replication* task progress does not account for rsync of database archive files.

ID Number	Description
SP-28034	An error was issued when changing a storage node to disabled.
SP-28068	Viewing snapshots of subfolders of a shared folder did not work.
SP-28088	The URL to download a support report was wrong.
SP-28177, SP-28211	The online help accessed the wrong version.
SP-28194	Setting folder level deduplication
SP-28198	Setting the cloud drive deduplication level for a user to **Folder**, created many folder groups.
SP-28222	A proxy could not be initialized which led to access problems.
SP-28312	Users accessing a portal with CTERA Drive Share on macOS could still edit shared folders after permission to access the folder was revoked.
SP-28346	The notifications *Envoy Unhealthy* and *S3 API Failed* were repeatedly issued.

5

CTERA PORTAL 8.3.3000.19 (SEPTEMBER 2025)

WHAT'S NEW

What's New In the Portal Image

ID Number	Description
PIM-5466	Improved docker security.
PIM-5669	*cloud-init* has been enabled for deployments in all platforms except for Microsoft Azure.

Resolved Software Issues

ID Number	Description
SP-27460	Setting CAC under SSO blocked access to the portal for the global administrator without using CAC.
SP-27550	Login attempts with wrong passwords were sometimes recorded in the System log instead of the Access log.
SP-27787	After entering details for a new **Amazon S3** storage node and then accessing the **AWS Snowball** option and returning to **Settings** option without making changes in the **AWS Snowball** option, resulted in a `Name is null` error.
SP-27826	Folder statistics were sometimes incorrect.
SP-27899	The primary database server could not start if the secondary, replication. server was down.
SP-27942	In rare cases a file copied during a migration was not assigned a unique ID.

6

CTERA PORTAL 8.3.3000.17 (AUGUST 2025)

WHAT'S NEW

What's New In the Portal Image

ID Number	Description
PIM-5415, PIM-5471	Improvements when restoring the database from an S3 bucket: • The archive pool size was not checked before restoring a database backed up to an S3 bucket. • Attempting to restore the database using the wrong bucket name failed with an error message that was not connected to the issue.
PIM-5442	Upgrading from an 8.2.x portal failed.
PIM-5452	A PostgreSQL vulnerability was resolved.
PIM-5476	Even when the **portal-storage-util.sh** script completed successfully, the return code reported an error.

New Software Features

ID Number	Description
SP-27410	Portal notifications have clearer categories.
SP-27423	Graph details are displayed for licenses in use and provisioned.
SP-27584	Object locking is now supported for Cloudian and Wasabi (S3) storage nodes, in addition to the Amazon S3 storage node.
SP-27734, SP-27784	Map file migration can be disabled by setting `set /settings/cloudFSSettings/mapFileMigrationTaskInterval 0`.
SP-27799	The new storage node, VSP One Object (S3), is now available.

Resolved Software Issues

ID Number	Description
SP-27486	The portal user interface displayed the wrong version number.
SP-27549, SP-27576	Addon functionality was missing from the 8.3.3000.3 release.
SP-27565	**amqpconfig** logs were not being overwritten or cleared.
SP-27635	Backing up the database to an S3 bucket did not generate any audit log actions.

ID Number	Description
SP-27643	An error occurred when trying to send a permanent delete file to some edge filers.
SP-27647	The portal displayed an incorrect list of available file versions when attempting to restore files.
SP-27708, SP-27767	The root partition of the application server could become full, casing the portal mode to be degraded.
SP-27732	Backups failed with edge filers running version 7.11.5100.5.
SP-27747	Permanently deleting files failed when there were files with a missing parent.
SP-27770	Previous versions were displayed empty for **Shared With Me** folders.

7

CTERA PORTAL 8.3.3000.12 (JULY 2025)

WHAT'S NEW

Infrastructure Improvements

Ability to Send Logs to More than One Syslog Server

After enabling a Syslog server in the portal, you can add Syslog servers using the following CLI:

```
portal-syslog-client add_syslog_server <ip> <port> <protocol> [name]
[ca_cert] [client_cert] [client_key]
```

Required Parameters

<ip> – IP address of the syslog server
<port> – Port number of the syslog server
<protocol> – Protocol to use (UDP, TCP/TLS, or TCP/ClientCertAuth)

Optional Parameters

[name] – Unique identifier for the server (auto-generated if not provided).
[ca_cert] – CA certificate file (required for TLS).
[client_cert] – Cient certificate file (required for client authentication).
[client_key] – Client private key file (required for client authentication).

Note:

- You cannot add multiple servers with the same IP and port combination.
- If you add a server with a name that already exists, the existing server will be updated.
- All certificate files must exist and be readable. All certificates need to be placed under `/usr/local/lib/ctera/syslog/logstash/tls`.
- The service automatically creates a new logstash pipeline configuration for each server.

Core Infrastructure Upgrades

Key infrastructure components have been upgraded including:

- The Tomcat server
- The JDK
- The Blocks table has been changed to include map files instead of having the map files stored as objects in the storage node.

  Note: You cannot upgrade the portal while running a storage node migration.

FIPS 140-3 Validation

The portal now supports FIPS 140-3.

Global Administration

New Look and Feel

The global administrator portal user interface has been modernized.

Backup to an S3 Bucket

In addition to PostgreSQL's built-in continuous archiving mechanism and PostgreSQL streaming replication that enables the continuous streaming and replication from a primary database server to a secondary, replication, server, you can also backup and restore the CTERA portal database to and from an S3 bucket.

Using CTERA Backup to S3 allows administrators to back up the portal settings, base database backup, and archival logs automatically to a designated S3 bucket, ensuring data integrity and availability through consistent backups while providing administrators with a user-friendly interface for backup configuration and status monitoring.

QumuloS3 Storage Node

The new storage node, Qumulo, is now available.

Devices Report

The Reports page has a new report, **Devices**.

New Email Templates

The following email templates have been added:

- Consul Service Unhealthy
- Database Backup to Bucket has Errors
- Envoy Service Unhealthy
- Nomad Service Unhealthy
- S3 API Service Failed

Support for Bitdefender Antivirus

The Bitdefender antivirus software is supported.

Deprecated Features

Features that are not supported have been removed, such as:

- Support for seeding stations (was under Settings > Seeding Stations).
- Ability to create a reseller portal.

Team Administration

New Look and Feel

The team administrator portal user interface has been modernized.

Global File Locking

When files are shared by users CTERA provides, in addition to conflict file handling, the option to lock files. Cloud drive folders can be configured so that only one user at a time can access the file for editing and the file will be locked for all other users.

Note: A license is required to enable global file locking.
CTERA Edge Filer 7.11.4900.11 or later is required.

Deprecated Features

Features that are not supported have been removed, such as:

- Local backup log.
- The Applications configuration template.