ctera your files. your cloud.

RELEASE NOTES

CTERA Portal 8.3.3300.40

May 2026

CONTENTS

1

CTERA PORTAL 8.3.3300.40

CTERA Portal 8.3.3300.40 is released as a GA version.

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 to 8.3.x requires first upgrading to 8.2.1500.58 or later and then to the latest 8.3.x 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

Warning: **CTERA Portal 8.3.3300.x requires two networks to support both internal and external IP addresses for servers. This division increases security. Upgrading a portal to this version requires adding another network and configuring the portal for this second network.**

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.

Each server must have two network interfaces for external and internal interfaces, to upgrade to this version.

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.

Storage nodes Considerations

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

Some storage nodes have been deprecated. If one of these storage nodes are being used, the upgrade stops with an error message.

The storage node names have been changed. The upgrade includes updating the names in the user interface.

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-5769, PIM-5772	Improved CTERA Messaging service
PIM-5811, PIM-6289, PIM-6647, PIM-6648, PIM-6760, PIM-7364, SP-28916	Improved security including resolving CVE-2025-66614, CVE-2026-24734, CVE-2026-29146, CVE-2026-24733.
PIM-6171, PIM-6465, PIM-6467, PIM-6468, PIM-6776, PIM-6800, PIM-6839	Microsoft Graph Mail has been integrated to the SMTP configuration, for sending emails securely.
PIM-6786, PIM-6791	The Google Cloud Storage (S3) storage node now supports Direct Mode.
PIM-6843	Pure Storage Flashblade (S3) storage node has been renamed to Everpure.

Resolved Issues

ID Number	Description
PIM-6182	Using the MCP server to copy a folder to the same path, added the timestamp to the original folder instead of the copied folder.
PIM-6401	Changing the owner of an old cloud drive folder failed.
PIM-6675	Setting up a additional servers in a portal cluster sometimes failed.
PIM-6692	In version 8.3.3300.29, the consent banner was not displayed.
PIM-6830	An error was displayed when setting an IP range when **IP-based Access Control** is enabled, under **Control Panel > Global Administrators Access Control**.
PIM-6889	In version 8.3.3300.29, the MCP server status remained as *CollectingStatus*.
PIM-6974	The portal startup was very slow.
PIM-6979	Uploading files with an invalid end date to a portal WORM compliant cloud folder failed.

ID Number	Description
PIM-7229	Single sign-on to a portal from CTERA Drive Connect sometimes failed on the first attempt.
PIM-7262, PIM-7263	Backing up the CTERA Portal database to an S3 Bucket failed when the bucket was Dell ObjectScale (S3).
PIM-7332	CTERA Fusion Gateway failed when the head-object included directories.
PIM-7397	The user interface in **Virtual Portal Settings** for the E**xternal Usr Authentication** section displayed a meaningless error for the **Default** label.
SP-28092	`No static resource` errors were written to the log.

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.
PIM-6031	Upgrading to 8.3.3300.x caused the Thumbnails service to stop working. **Workaround**: Manually disable and then re-enable the Thumbnails service:
SP-16614	Support users with the relevant permissions cannot create user groups, add or remove users in an existing group nor delete users.
SP-17928	After changing a plan name and applying it, the process shows that zero users were updated.

2

CTERA PORTAL 8.3.3300.29 (MARCH 2026)

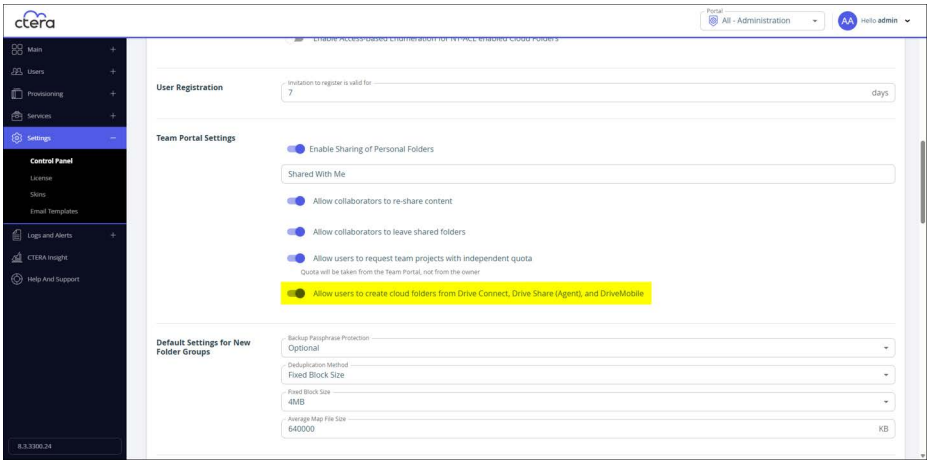
WHAT'S NEW

What's New In the Portal Image

ID Number	Description
PIM-6003, PIM-6121, PIM-6125, PIM-6180, PIM-6181, PIM-6189, PIM-6361, PIM-6551, PIM-6552	Improvements to the MCP service. For example: • When using the MCP service, moving files in the portal did not work. • Multiple file versions are reported when only one version exists.
PIM-6060	Warnings were issued when upgrading a portal from 8.2.1500.x.
PIM-6092, PIM-6208	The docker image for accusoft/prizmdoc-server has been upgraded to 13.28.
PIM-6141, PIM-6145	The portal logs cleaner service failed when run immediately after the server was rebooted.
PIM-6158, PIM-6159, PIM-6160, PIM-6377, PIM-6378	Improved security, including resolving CVE-2022-41946.
PIM-6176	The CTERA Messaging service issued errors even when the status was active and running OK.
PIM-6222	Deleting an offline server failed.
PIM-6270	Portal dumps now include the keep_envoy_alive.log.
PIM-6274	The CTERA Drive Share/Protect Microsoft add-in did not work when the files had ACLs enabled.
PIM-6314	Both upgrading and deploying a portal have been improved.
PIM-6318	If the storage node became disconnected, syncing with the portal stopped until syncing was suspended and then unsuspended.
PIM-6365	When a sync is stalled, the email notification now includes the start date.
PIM-6382	Searching sometimes failed.
PIM-6387	Downloading files using CTERA Drive Connect caused the root partition to reach 100%
PIM-6401	Changing a cloud folder owner failed.
PIM-6464, PIM-6466	In version 8.3.3300.20, the Thumbnails service storage display was not correct: the status was N/A and no usage was displayed.

ID Number	Description
PIM-6492	The **Portal Version** field has been removed from the global administration view for the following: • The **Platform Monitoring** tab in the **Dashboard** screen. • The **Status** option in the **Server** window. Also see SP-28928, SP-29134.
PIM-6607	In version 8.3.3300.20, connecting a new server to the main DB server failed.

New Features

ID Number	Description
SP-28928, SP-29134	The **Portal Version** field has been removed from the global administration view for the following: • The **Platform Monitoring** tab in the **Dashboard** screen. • The **Status** option in the **Server** window. Also see PIM-6492.
SP-29022, SP-29132	The error issued after 2-factor authentication failed six times has been improved to be more informative.
SP-29187	In **Virtual Portal Settings**, you can now prevent end users from creating cloud folders. 

Resolved Software Issues

ID Number	Description
SP-23921, SP-28781	In some cases, a `SignatureDoesNotMatch` error was issued when accessing an S3 storage node, resulting in retries being required to complete uploads.
SP-25194	When Bitdefender antivirus service was enabled, files had to be downloaded for the Thumbnails service to work.
SP-29166	Actions executed using the CTERA MCP service that involved a destination folder were executed in the wrong place.

ID Number	Description
SP-29188, SP-29189	Accessing a CTERA Edge Filer remotely from a team portal failed.
SP-29194	End users could not create subfolders when creating cloud folders was disabled.

3

CTERA PORTAL 8.3.3300.20 (FEBRUARY 2026)

WHAT'S NEW

What's New In the Portal Image

ID Number	Description
PIM-5690	When running `portal-cert.sh import -s` to import a certificate from a remote host, the certificate was not imported.
PIM-5699, PIM-5745, PIM-5816, PIM-5957	Security improvements, including resolving CVE-2024-56337, CVE-2025-30065, CVE-2023-52323, CVE-1999-0524, CVE-2025-9615.
PIM-5801, PIM-6120	Consul has been upgraded to 1.22.2. Nomad versions has been upgraded to 1.11.1.
PIM-6019	The messaging service did not work in 8.3.3300.8.
PIM-6026	The portal dump now includes the portal configuration.
PIM-6037	Azure Entra ID cookie and token issues in 8.3.3300.8 have been resolved.
PIM-6046, PIM-6061, PIM-6064, PIM-6080, PIM-6081	Improvements to the MCP implementation.

New Features

ID Number	Description
–	FIPS PUB 140-3 is supported.
SP-28731, SP-28841	Node.js has been upgraded to 24.x.
SP-28845, SP-28916	Improved security.
SP-28958	Improvements to the MCP implementation.

Resolved Software Issues

ID Number	Description
SP-27403	Uploading to the firmware repository failed.
SP-28685	The MCP status in the **Data Services** tab in the portal dashboard was wrongly displayed as disabled.
SP-28695	The Local Filesystem storage node was disconnected after an upgrade.
SP-28818	Specifying a subfolder path when defining subfolder quotas failed if the path ended with a forward slash (/).

ID Number	Description
SP-28828	Confirming folder permanent deletion prompted for a username instead of a password.
SP-28861	The dashboard storage graphs were empty.
SP-28902	In rare scenarios, an error was issued when a large copy was performed between different folder group.
SP-28919, SP-29008	In the dashboard, when clicking on a notification that related to user quotas and details, the user **Profile** tab was displayed instead of the **Resource Usage** tab
SP-28920	The link to the online help displayed the wrong help.
SP-28971, SP-28972	When confirming permanent deletion with the wrong password, the error message was wrong.
SP-28982	Fetching users did not work with Entra ID Domain Services in all regions and Active Directory 2025.
SP-29061	File uploads failed after upgrading a portal with a storage node with a name that does not conform to the latest S3 naming conventions.
SP-29079	Application servers could restart continuously.
SP-29107	The portal.out logging was flooded with subfolder quota log messages.

4

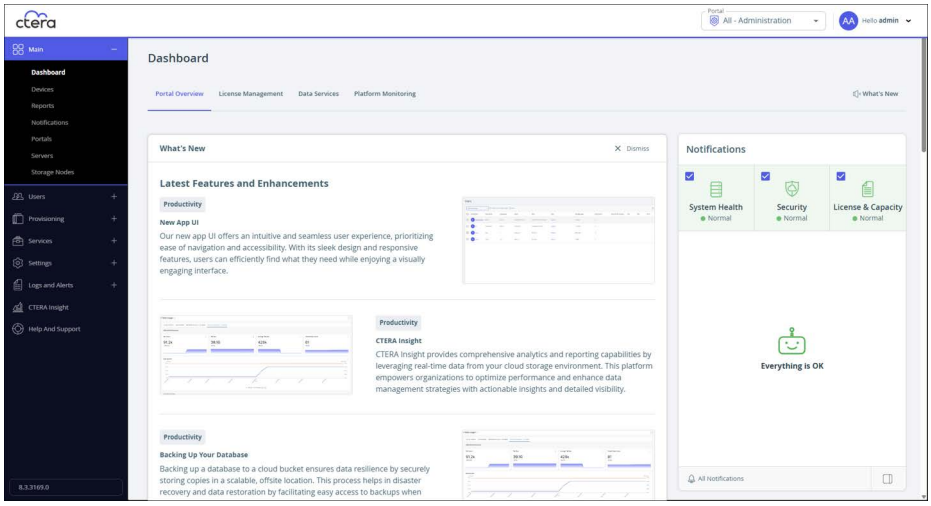
CTERA PORTAL 8.3.3300.8 (JANUARY 2026)

WHAT'S NEW

Global Administration New Features

New Dashboard

The dashboard has been redone to provide more portal monitoring as well as a section detailing the new features.



The Notifications section has been changed to provide the same look and feel that the edge filer administrator has.

MCP Server

The Model Context Protocol (MCP) in CTERA lets AI assistants and agents securely interact with the CTERA platform as a framework for defining and managing a variety of context-based configurations across the platform. This feature facilitates dynamic policy enforcement and adaptive user experiences by leveraging contextual data to tailor services, enhancing both security and efficiency.

Embedding MCP support directly into the CTERA Portal enables LLMs, whether commercial tools like Claude and Cursor, or internally developed agents, to securely:

- Summarize file uploads in a shared folder.
- Retrieve document versions based on content.
- Generate and distribute a public or internal file link without a graphical user interface (GUI).
- Manage files using natural language instead of scripts or dashboards.

The CTERA MCP Server provides a natural language ability to perform actions that can be done using the CTERA SDK. The natural language used to talk to the agent that uses the MCP Server is internally mapped to an API in the CTERA SDK.

These tasks are executed securely control, enforced by encryption, permissions, and audit logging. There's no need to copy data to external AI systems or learn new APIs.

Storage Nodes

The names of storage nodes that support the S3 protocol have been standardized.

The following new storage nodes are supported:

- IBM Storage Ceph (S3)
- PureStorage Flashable (S3)
- VAST Data (S3)

The following storage nodes have had their names changed:

- Caringo S3 has been renamed DataCoreSwarm (S3)
- EMC ECS (S3) has been renamed Dell ObjectScale (S3)
- EMC Isilon (NFS) has been renamed Dell PowerScale (NFS)
- Generic (NFS) has been renamed NFS-Compatible
- Generic (S3) has been renamed S3-Compatible
- Isilon (S3) has been renamed Dell PowerScale (S3)
- NetApp StorageGRID Webscale (S3) has been renamed NetApp StorageGRID (S3)

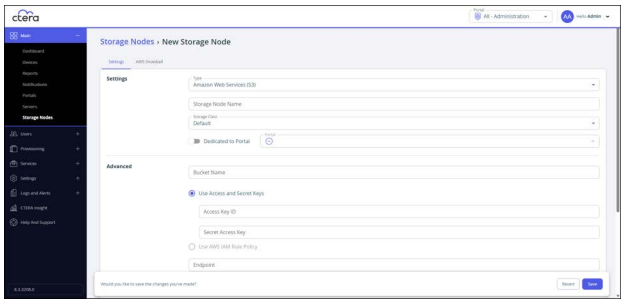
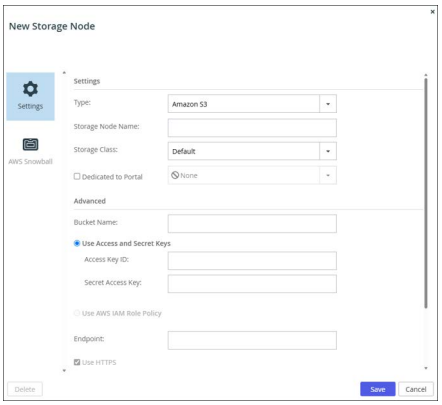
The following storage nodes have been deprecated:

- DDN Web Object Scaler
- HGST Active Archive
- HGST Active Scale
- Hitachi HCP
- IBM Cloud Object Storage (Simple Object API)
- OpenStack Swift (KeyStone)

The **Use S3 Object Lock** option is now also supported for Cloudian and Wasabi Cloud Storage (S3) storage nodes.

Continued Improvements to the Look and Feel

Additional improvements to standardize the look and feel. For example, to manage a storage node.

New	Old
	

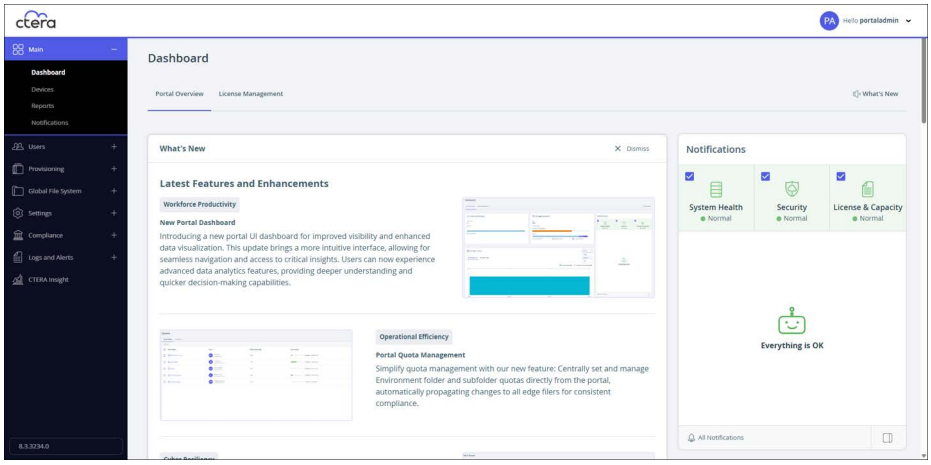
Improvements to Varonis Integration

The Integration with Varonis has been further improved.

TEAM ADMINISTRATION NEW FEATURES

New Dashboard

The dashboard has been redone to provide more portal monitoring as well as a section detailing the new features.



The Notifications section has been changed to provide the same look and feel that the edge filer administrator has.

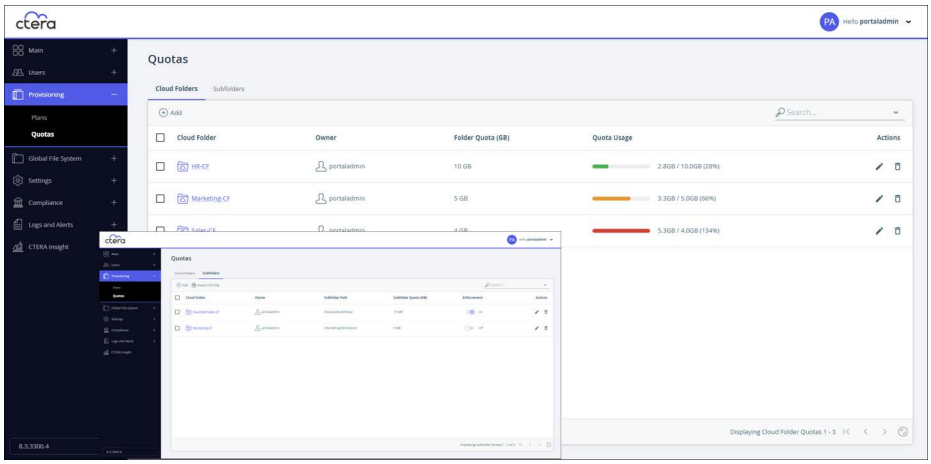
You can hide the new features to display the following:

- Users and devices registered on the portal.
- The number of files and folders and the cloud storage used.
- An overview of either the storage or folder type over time.
- A summary of the number of users and new users over time.
- A summary of the number of files over time.
- A summary of what is licensed and the license quotas and current use and what is remaining.
- License usage over the last week showing both the provisioned licenses and actual licenses in use for the cloud drive or for edge filers.

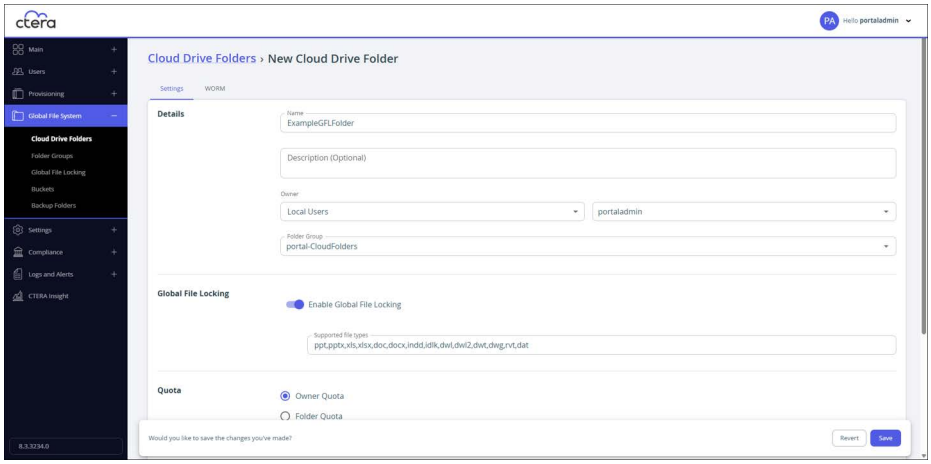
Folder and Subfolder Quota Management

Folder and subfolder quotas can now be managed centrally, automatically propagating changes to all connected edge filers.

Quota management is only applied to edge filers connected to the portal that use the next generation file system. The CTERA Messaging service must be enabled to manage cloud drive folder quotas.



File Types that Support Global File Locking

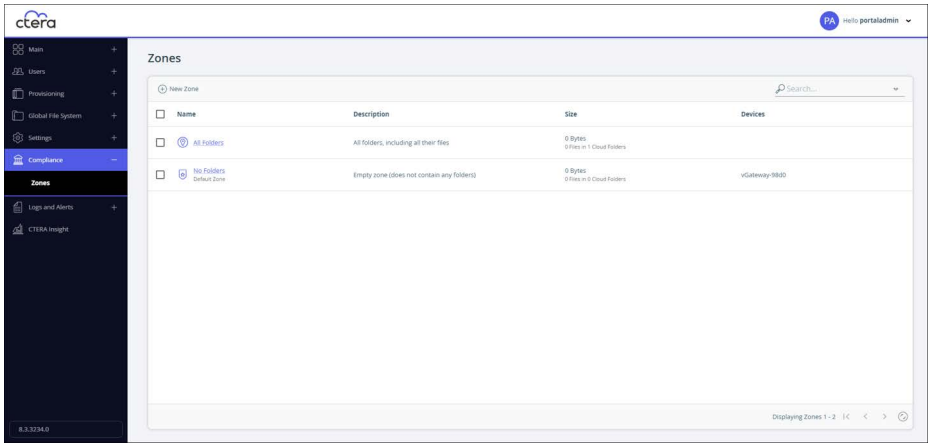


You can edit the Supported file types list with the file types you want locked.

All files in the folder with an extension in the **Supported file types** list are locked when opened for editing so that only one user at a time can edit the file. Locking applies to files that were already in the folder when the locking was applied as well as to files added to the folder after locking is applied. A message is displayed that the file can be opened only for viewing when other users try to open a locked file.

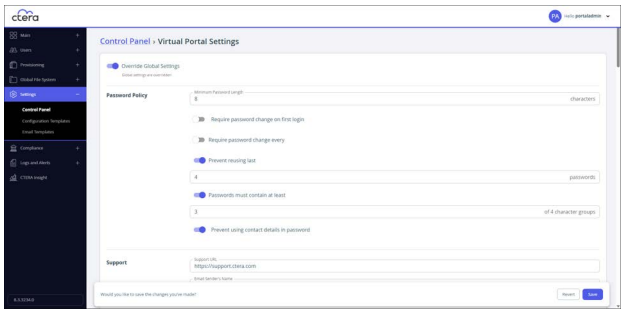
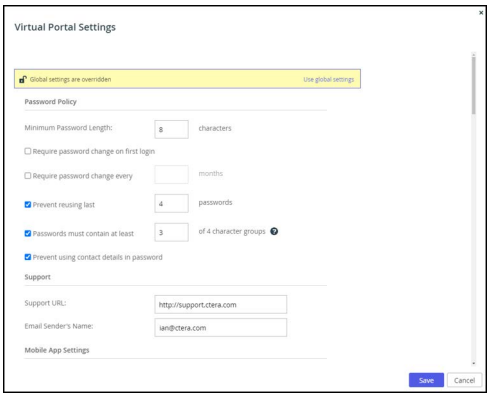
Zones are Enabled By Default

Additional improvements to standardize the look and feel. For example, to manage a storage node.



Continued Improvements to the Look and Feel

Additional improvements to standardize the look and feel. For example, to manage a storage node.

New	Old
	

End User New Features

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.

My Files Not Implemented By Default

New deployments do not include the **My Files** cloud drive folder by default.