ctera your files. your cloud.

RELEASE NOTES

CTERA Portal 8.2.1500.64

November 2025

CONTENTS

CTERA Portal 8.2.1500.64 4
- Licensing CTERA Portal 4
- Security Considerations 4
- Installing or Upgrading CTERA Portal 4
- Branding Considerations 5
- Checking the CTERA Portal Cloud File System (FSCK) 5
- What's New 6
- Known Issues 6

CTERA Portal 8.2.1500.62.4 (September 2025) 8

CTERA Portal 8.2.1500.62.2 (August 2025) 9

CTERA Portal 8.2.1500.57 (June 2025) 11

CTERA Portal 8.2.1500.54 (June 2025) 12

CTERA Portal 8.2.1500.50.2 (April 2025) 13

CTERA Portal 8.2.1500.37.2 (January 2025) 18

CTERA Portal 8.2.1500.8.6 (August 2024) 23

CTERA Portal 8.2.1500.5 (May 2024) 25

1

CTERA PORTAL 8.2.1500.64

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
- Security Considerations
- Installing or Upgrading CTERA Portal
- Branding Considerations
- Checking the CTERA Portal Cloud File System (FSCK)
- What's New
- Known Issues

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 7.5.x to 8.2.x requires first upgrading to 8.1.x and then to a version running on CentOS 9 and then the latest 8.2.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

8.2.1500.62.4 runs on CentOS 9.

To upgrade a 7.5.x or 8.1.x portal running on CentOS 7:

- **Upgrading from 7.5.x running on CentOS 9**: Upgrade to the latest 8.1.1417.x version running on CentOS 9 and then to the latest portal 8.2.x.
- **Upgrading from 7.5.x CentOS 7**: Upgrade to the latest 8.1.x running on CentOS 7 and then migrate to the same version of 8.1.x running on CentOS 9 and then upgrade to the latest portal 8.2.x.
- **Upgrading from 8.1.x CentOS 7**: Upgrade to the latest 8.1.x running on CentOS 7 and then migrate to the same version of 8.1.x running on CentOS 9 and then upgrade to the latest portal 8.2.x.
- **Upgrading from 8.1.x CentOS 9**: Upgrade to the latest portal 8.2.x.

Upgrading it to CentOS 9 is described in Upgrading a Portal from Running on CentOS 7 to Run on CentOS 9.

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.

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 8.2.1500.5 included a number of new features for global and team portal administrators and for end users. See What's New in CTERA Portal Version 8.2.x.

What's New In the Portal Image

ID Number	Description
PIM-5696	Improved security including resolving CVE-2024-56337 vulnerability.
PIM-5721	Problems with the Varonis service have been fixed.

Resolved Software Issues

ID Number	Description
SP-28062, SP-28094, SP-28097	Problems with the Varonis service have been fixed.
SP-28067	End users could not see previous versions of subfolders where the parent forlder was shared with them.

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-3977	The Varonis and CTERA Edge Filer Syslog services fail to start after an upgrade from portal version 7.5.x. If the CTERA Portal was integrated with Varonis Data Security Platform on a version before the upgrade, running a version prior to 7.5.1159.46, the integration must be disabled and then reconfigured after the upgrade.
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.

ID Number	Description
SP-21806	Setting a preview server takes approximately 60 seconds to start working.
SP-26464	CTERA Agent users could not log in to the portal running a version from 8.2.1500.37.2 if they logged out.

2

CTERA PORTAL 8.2.1500.62.4 (SEPTEMBER 2025)

WHAT'S NEW

What's New In the Portal Image

ID Number	Description
PIM-5466, PIM-5676, PIM-5681	Improved security including docker security.
PIM-5474	The support report could not be downloaded from the user interface.
PIM-5487	Only one messaging server could be replaced. Attempting to replace a second messaging server failed.

3

CTERA PORTAL 8.2.1500.62.2 (AUGUST 2025)

WHAT'S NEW

What's New In the Portal Image

ID Number	Description
PIM-4650, PIM-5145, PIM-5452, PIM-5486, PIM-5500	Security improvements: • Resolved vulnerabilities with PostgreSQL. • The following vulnerabilities have been resolved: CVE-2025-49796, CVE-2025-49794, CVE-2025-6021, CVE-2022-29458, CVE-2023-29491, CVE-2024-56337
PIM-4883	The SSH configuration files have been hardened.
PIM-5372	Nomad could have started with an internal IP, which caused an error.
PIM-5377	Upgrading the portal failed when there was no Internet access.
PIM-5420	The log file generated after running ctera_firstboot.sh now includes timelines.
PIM-5443	The Varonis log was incorrect since portal version 8.2.1500.50.
PIM-5477	Even when the **portal-storage-util.sh** script completed successfully, the return code reported an error.
PIM-5669	*cloud-init* has been enabled for deployments in all platforms except for Microsoft Azure.

New Software Features

ID Number	Description
SP-27081	Permalinks can be added in a CTERA Portal app integrated in Microsoft Teams.
SP-27800, SP-27815	The new storage node, VSP One Object (S3), is now available.

Resolved Software Issues

ID Number	Description
SP-27248	From portal version 8.2.1500.47 Cloud Backup Log, Cloud Sync Log and Permanent Deletion Log pages were displayed in the global administrator view.
SP-27258	Alert notifications were continuously sent to both portal users and external users.
SP-27381	Improved security with quota allocations.
SP-27443	Attempting to assign the default plan to a new user failed.

ID Number	Description
SP-27454, SP-27475	After upgrading a portal to version 8.2.1500.57, syncing from the portal to an edge filer was delayed when the local time and UTC time were different.
SP-27477	Improved security when using SAML for single sign-on.
SP-27583	Object locking is now supported for Cloudian and Wasabi (S3) storage nodes, in addition to the Amazon S3 storage node.
SP-27648	The portal displayed an incorrect list of available file versions when attempting to restore files.
SP-27748	Permanently deleting files failed when there were files with a missing parent.
SP-27769	Previous versions were displayed empty for **Shared With Me** folders.
SP-27825	Folder statistics were sometimes incorrect.

4

CTERA PORTAL 8.2.1500.57 (JUNE 2025)

WHAT'S NEW

What's New In the Portal Image

ID Number	Description
PIM-5357	The maximum number of storage snapshots was missing after rebooting a server in AWS.
PIM-5361	Additional fields have been added to the access log when `enable-access-logs` CLI is set to `true` to improve traceability and debugging.

New Software Features

ID Number	Description
SP-27087, SP-27111	Improved security including updated crypto policies.

Resolved Software Issues

ID Number	Description
SP-26464	Portal versions 8.2.1500.50.2 and 8.2.1500.54: Local End users could not login to the portal.
SP-27109	The edge filer repeatedly disconnected from the portal after a map file error.
SP-27146	Users could not change their passwords in a team portal that did not use Single Sign-on.

5

CTERA PORTAL 8.2.1500.54 (JUNE 2025)

WHAT'S NEW

What's New In the Portal Image

ID Number	Description
PIM-4658	The prizmdoc-server package was updated to 13.28.
PIM-5111	Improved security.
PIM-5314	The `db_bucket_restore.sh` script has been changed to download archive files from S3 buckets directly to `/usr/local/lib/db_archive`.

New Software Features

ID Number	Description
SP-25512, SP-26409, SP-26827, SP-26995, SP-27083	Improved security, including: • To safeguard against XML Signature Wrapping attacks. • For Content Security Policy (CSP) headers for device-related requests. • Resolution for CVE-2024-6484.
SP-26929, SP-26992	Improvements to the Varonis server, including being able to set debug mode for the Varonis service.

Resolved Software Issues

ID Number	Description
SP-26883, SP-26884	Content Security Policy (CSP) headers were included twice.
SP-26981	Exceptions were issued when attempting to delete an offline server from the portal.
SP-26988	The **Use S3 Object Lock** field could be set for storage nodes where it did not apply (it only applies to than **Amazon S3** and **Hitachi Vantara HCP (S3)**).
SP-27013	Users in the *Domain Users* group in Microsoft Active Directory were not automatically fetched.
SP-27024	An audit log entry was not issued after changing a server configuration by removing the S3 endpoint for that server.

6

CTERA PORTAL 8.2.1500.50.2 (APRIL 2025)

WHAT'S NEW

What's New In the Portal Image

ID Number	Description

—	The upgrade procedure has been improved:
	Instead of manually running `dnf install -y *.rpm`, execute a script, as follows:
	`cd /path/to/upgrade`
	`chmod +x install.sh`
	`./install.sh`
	Note: The script provides additional logging alongside `dnf` output, offering better visibility into the upgrade process.
	The tar file structure remains the same, with the addition of the install.sh script.

PIM-4367, PIM-5035, PIM-5155, PIM-5173	The `ctera_firstboot.sh` has been improved to handle Azure deployments: • It is more secure. • Handle images in Azure Marketplace. • Additional docker validation. • Platform services installation has been improved.
PIM-4658	The prizmdoc package, used by the preview server, was changed to version 13.28.2.
PIM-4692, PIM-4792, PIM-4798, PIM-4836	Improvements to the installation first boot script. For example, docker images are moved to the data pool so that the portal storage is not full.
PIM-4694	The Azure `firewall` command was not persistent and was removed when the portal was rebooted.
PIM-4528, PIM-4736, PIM-4941, PIM-4815, PIM-4871, PIM-4833	Security improvements, including removing SHA1 from the SSH configuration files and resolving advisories such as CVE-2024-50379 and CVE-2024-22243.
PIM-4961, PIM-5019	Setting FIPS-140 caused the messaging service to fail.

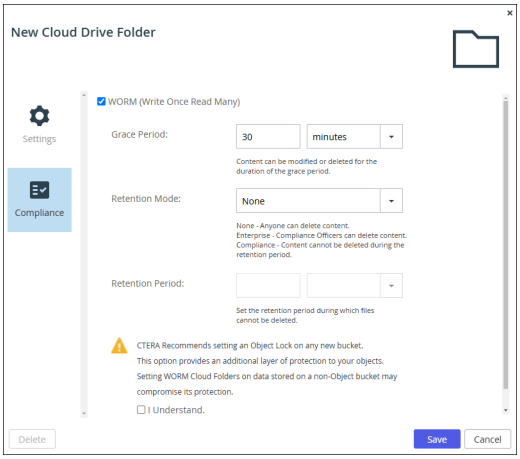
ID Number	Description
PIM-5180, PIM-5182	The apache-tomcat package has been upgraded to 9.0.102 to resolve CVE-2025-24813.
PIM-5195, PIM-5209, PIM-5210, PIM-5265	Improvements to the Syslog management: • MARK message text can be added or removed to keep-alive messages sent to portal and edge filer syslog servers. • A CLI is available to retrieve the host or environment Logstash that is currently running. • A CLI is available to update portal syslog configuration properties.

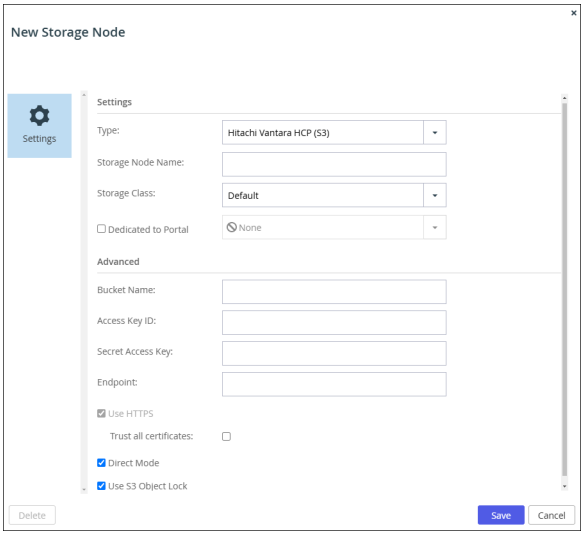
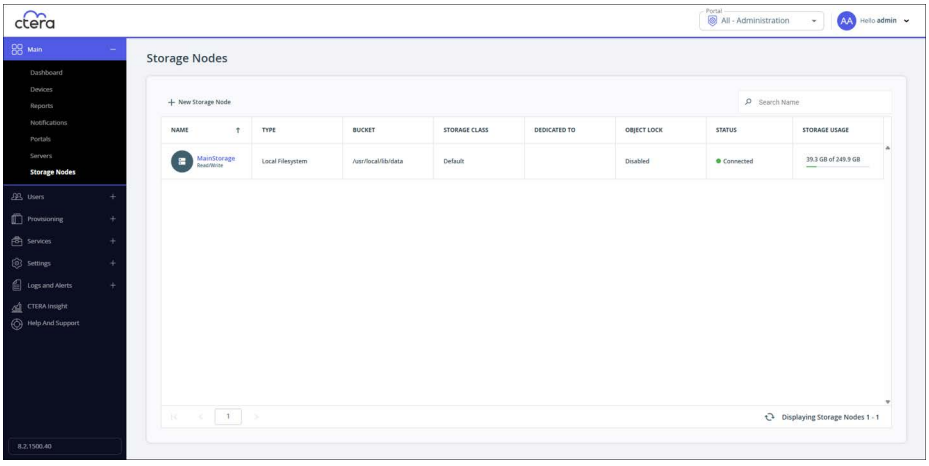
New Software Features

ID Number	Description

SP-20230	The following scripts have been renamed:
	`ctera-db-export.sh` to `portal-db-export.sh`
	`ctera-db-import.sh` to `portal-db-import.sh`
	`ctera-import-export.sh` to `portal-import-export.sh`
	`ctera-import-export-vars.sh` to `portal-import-export-vars.sh`
	`ctera-portal-settings-export.sh` to `portal-portal-settings-export.sh`
	`ctera-portal-settings-import.sh` to `portal-portal-settings-import.sh`

SP-25479	When CTERA Ransom Protect is enabled on the edge filer, the log of blocked users generated on the edge filer is also written to the portal log.
SP-26041, SP-26479	CAC logins are allowed using the Certificate Revocation List (CRL) so there is no need to rely on the Online Certificate Status Protocol (OCSP) server being up.
SP-26223	A new email template, **Crl Failed Download Attempt**. The notification alerts the administrator when there is an error while attempting to retrieve and verify certificate information.

ID Number	Description
SP-26331, SP-26332, SP-26333, SP-26334, SP-26335, SP-26336, SP-26337, SP-26338, SP-26339, SP-26342, SP-26343, SP-26344, SP-26345, SP-26346, SP-26348, SP-26354, SP-26355, SP-26359, SP-26360, SP-26361, SP-26384, SP-26385, SP-26386	The portal cloud folder compliance settings are propagated to the S3-type storage node, for all files in the cloud folder, extending protection from the application level through to the block-level on the storage. **Note:** CTERA recommends that whenever you create a new S3 bucket to use as the backend storage for a storage node, you enable *object lock* when creating the bucket and disable *default retention*. For most S3 buckets, after the bucket is populated with content, you **cannot** set object lock. With AWS S3 buckets, you **can** set object lock after the bucket is populated with content. **For object lock support, object lock must be enabled on the S3 bucket and the retention mode for the bucket must be disabled.** As long as the cloud folders that will write to the bucket have been defined with compliance set, as described in Folder (WORM) Compliance: CTERA Vault, setting object lock on the S3 bucket ensures the following: • Files within dedicated WORM folders are immutable, preventing any modifications or deletions once written. • Retention settings are automatically propagated to the S3 bucket. Customizable retention periods can be set for files within dedicated WORM folders. Setting compliance on a cloud folder in a team portal: 

ID Number	Description
	Object locking is supported for Amazon (S3), Hitachi Vantara HCP (S3) buckets. An example storage node with the **Use S3 Object Lock** field set:  Other storage nodes include the object locking option, **Use S3 Object Lock**, for future use.
	The **Storage Nodes** page also includes a column showing whether the storage node has object locking enabled or disabled.  For details about the different scenarios and their outcomes when setting object locking on a storage node, see Managing Storage Nodes.
SP-26409, SP-26490, SP-26666	Security improvements.
SP-26419	The portal configuration file, `portal.cfg`, has a new field, `CUSTOM_ADDRESS=x.x.x.x`, where x.x.x.x is the NAT IP address. In addition, `portal.sh` can use this NAT IP address.

ID Number	Description
SP-26484, SP-26623, SP-26918	Compliance with OWASP. Every HTTP/HTTPS request can be logged and can be forwarded to a Syslog server. Use `add|remove manage-syslog-additional-log-path` to add or remove custom log paths that the system monitors and `manage-syslog-additional-log-path show` to show all currently monitored custom log paths. Access logs can be forwarded to a Syslog server by running the command `enable-access-logs true`.
SP-26719	The email templates informing the portal administrator that there has been a suspected ransomware attack on an edge filer have been renamed to **Suspected Ransomware Attack Detected**. One template is for suspected attacks identified by the behavioral engine and the other template is for suspected attacks identified by the honeypot engine.

Resolved Software Issues

ID Number	Description
SP-26251	Global administrators could not create an SSO activation code to access the portal.
SP-26408	Files could not be shared with Active Directory users who did not have a last name in Active Directory.
SP-26560	After enabling zones, adding an edge filer to the zone caused a sync error on the edge filer.
SP-26605	When displayed in Tiles view, the rightmost tile in each row was cropped.
SP-26675	After canceling and then restarting CTERA FSCK, it started on the wrong cloud folder group.
SP-26272	A license can be generated for a customer without Internet access and without providing the DNS to CTERA.
SP-26657, SP-26899	Security improvements, for example, preventing malicious users to saturate the quota of space available to other users and resolving the CVE-2018-15546 vulnerability.
SP-26721	Files could not always be recovered from snapshots.

7

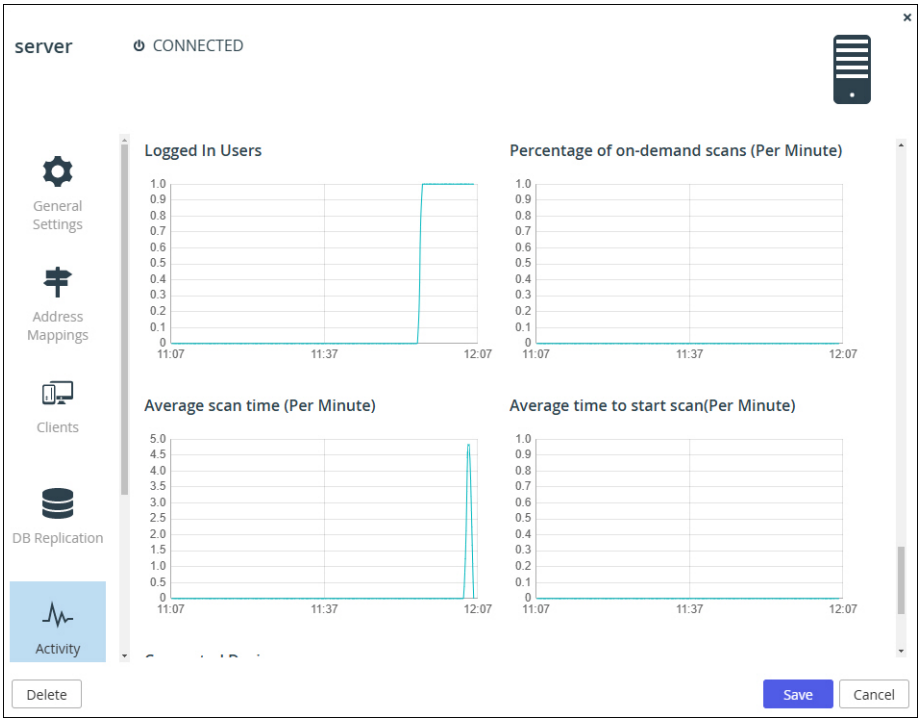
CTERA PORTAL 8.2.1500.37.2 (JANUARY 2025)

WHAT'S NEW

What's New In the Portal Image

ID Number	Description
PIM-4311, PIM-4318, PIM-4349, PIM-4515, PIM-4615, PIM-4650, PIM-4684, PIM-4687, PIM-4691, PIM-4786, PIM-4787, PIM-4789, PIM-4800, PIM-4812, PIM-4816	Security improvements. CVE-2024-7348, CVE-2024-34750, CVE-2024-39689, CVE-2018-20685, CVE-2019-6109, CVE-2019-6110, CVE-2019-6111, CVE-2022-0788, CVE-2022-21476, CVE-2022-21426, CVE-2022-21496, CVE-2022-21434, CVE-2022-21443, CVE-2024-52317, CVE-2024-52316, CVE-2024-21147, CVE-2024-21145, CVE-2024-21140, CVE-2024-21144, CVE-2024-21131, CVE-2024-21138, CVE-2024-50379, CVE-2022-42889 have been resolved.
PIM-4320, PIM-4785	Improved upgrade procedure from CentOS 7 to CentOS 9.
PIM-4360	The portal.dump file includes the server name as part of the filename.
PIM-4374	Improved image upgrade for PostgreSQL.
PIM-4382, PIM-4385, PIM-4388, PIM-4413, PIM-4471, PIM-4473, PIM-4475, PIM-4477	Improvements to the Varonis integration.
PIM-4427, PIM-4460	The local quota service failed when it was initialized but did not complete.
PIM-4544	The `screen` utility has been added to the portal image.
PIM-4504, PIM-4505	The Edge Filer Syslog service failed to start on a portal running on CentOS 9.
PIM-4612	When installing a portal in ESXi, you can customize the name of the portal, the IP address, netmask, gateway and DNS server as a step during the installation.
PIM-4661	prizmdoc-server used by the preview server has been updated to 13.28.
PIM-4761, PIM-4764	The portal configuration file, `portal.cfg`, has a new field, `CUSTOM_ADDRESS=x.x.x.x`, where x.x.x.x is the NAT IP address. In addition, `portal.sh` can use this NAT IP address.
PIM-4823, PIM-4827	The NTP server IP address can be used when configuring NTP in the CTERA Portal server.
PIM-4844	Improvements to `migration.sh`, which is used when upgrading a portal running on CentOS 7 to run on CentOS 9.

New Software Features

ID Number	Description
SP-25184, SP-25564, SP-25635, SP-25650	The CTERA FSCK command has been improved. For example, when run using the `all -r argument`.
SP-25261	Improved performance when accessing content using CTERA Drive Share (Agent).
SP-25262, SP-25263, SP-25301	More information is provided for antivirus scans in new server activity graphs: • The time to initiate an on-demand scan. • Average scan times for antivirus scans. • The percentage of antivirus scans run manually. 
SP-25329, SP-25330, SP-25454, SP-25487, SP-25518, SP-25528, SP-25763, SP-25767, SP-25805, SP-25902, SP-25904, SP-25926, SP-26020, SP-26024, SP-26030, SP-26149, SP-26133, SP-26158, SP-26218, SP-26258, SP-26259, SP-26260	CTERA Insight, a Software as a Service (SaaS) tool, hosted by CTERA, that provides real-time monitoring of the CTERA environment from one central Web-based interface, is now available. CTERA Insight lets portal administrators and IT departments monitor all of the data in real-time, including all the CTERA Edge Filers and endpoints connected to the portal in the environment. By knowing exactly how the CTERA platform is behaving at any given moment means that you can identify any potential problems before they become serious and resolve them.

ID Number	Description
SP-25008, SP-25720	Improvements to CTERA Fusion: • Port 443 for the S3 endpoint is supported to access portal content. • Self-signed certificates can be used.
SP-25404, SP-25408, SP-25409, SP-25437, SP-25438, SP-25439, SP-25469, SP-25476, SP-25549, SP-25589, SP-25638	Improvements to ransomware detection on edge filers: • Ransomware logs are collected from edge filers. • Ransomware attacks are logged in `portal.out`. • Administrators receive an alert in the user interface and an email alert after a ransomware attack is detected by an edge filer. • Two new email templates, both **Suspected Data Exfiltration Attack was detected**, inform the portal administrator that there has been a suspected ransomware attack on an edge filer. One template is for suspected attacks identified by the behavioral engine and the other template is for suspected attacks identified by the honeypot engine.
SP-25430, SP-25473, SP-25705, SP-25837, SP-25839, SP-25841, SP-25843	Improved Security.
SP-25512	Improved security when using SAML to prevent XML signature wrapping (XSW) attacks.
SP-25578	Branding portals is now done on top of the portal image using a separate file.
SP-25698	Improved performance for copy, delete, and restore operations performed in the user interface.
SP-25990	Updating portal software directly in the user interface for portals running on CentOS 9 is no longer available, since the software is not upgraded separately to the image. **Pre-8.2.1500.37.2**:  **From 8.2.1500.37.2**: 

ID Number	Description
SP-26082	The **OCSP Revocation Checking** checkbox has been removed from SSO CAC configuration.

Resolved Software Issues

ID Number	Description
SP-24483	The server status remained `Deployment in Progress` even after the deployment completed.
SP-25027	Setting **Enable Zones** in **Global Settings** did not work.
SP-25263	Average scan times for antivirus scans have been added.
SP-25307	Worm compliant files that were migrated to an edge filer showed the wrong creation date in the portal.
SP-25410	Improvements to the mechanism for sending emails to ensure that they are sent on time.
SP-25453	When Content Security Policy (CSP) was enabled but Microsoft Office Online was disabled, frame-src was not applied to the CSP header.
SP-25507, SP-25524	The wrong port was used when editing an existing CTERA Fusion bucket.
SP-25533	Portal failed to start after an upgrade to 8.2.1500.12
SP-25612	When the snapshots were created at the end of a month, snapshots for months with less days were not retained.
SP-25650	On a Microsoft Azure platform, the CTERA FSCK tool could mark blocks that existed as missing.
SP-25800	A global administrator from Active Directory could not create folders in the end user portal.
SP-25806	Updating user accounts could become stuck.
SP-25818	API keys could not be generated nor deleted by read only or support administrators.
SP-25823	When connecting a new secondary server to the primary server, the connection hanged until the browser was refreshed.
SP-25830	Undeleting a folder failed when the folder contained a deleted populated subfolder.
SP-25855	The notification email to an administrator after a permanent deletion, for two-factor authentication, to complete the permanent deletion was not sent.
SP-25988	Undeleting a deleted subfolder sometimes failed.
SP-26006	The local quota feature did not work when the folder was empty.
SP-26012	The first previous snapshot did not exist after restoring a file from a version before this snapshot.
SP-26029	When LDAP channel binding was enabled, Active Directory domain lookup failed when both SSL and Kerberos were enabled.
SP-26123	When the antivirus service was enabled, the auto vacuum task for `map_file_infected_status` ran for too long.

ID Number	Description
SP-26161	Adding a server sometimes started the server without some internal components being installed.
SP-26220	A virtual private cloud (VPC) endpoint could not be used to connect to an Amazon S3 storage node.

8

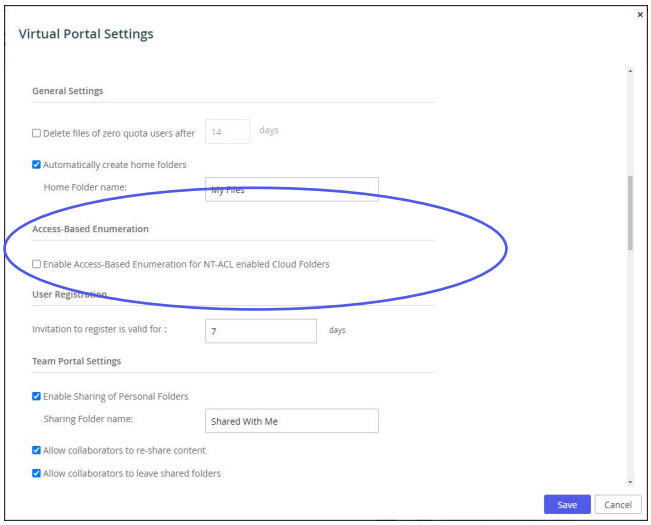
CTERA PORTAL 8.2.1500.8.6 (AUGUST 2024)

WHAT'S NEW

What's New In the Portal Image

ID Number	Description
PIM-4128	The Varonis configuration was removed when upgrading the portal.

New Software Features

ID Number	Description
SP-25069	Backup folders now support fixed block size.
SP-25155	The Verify Sync task has been improved.
SP-25240, SP-25241, SP-25242, SP-25243, SP-25244	Access-Based Enumeration support: End users only see and can access folders and files that they have permission to see. The support is not enabled by default and can be enabled in the Virtual Portal Settings: 

Resolved Software Issues

ID Number	Description
SP-25027	Default zones were not created when enabling zones in the user interface.
SP-25143, SP-25144, SP-25145, SP-25205	Security improvements.
SP-25153	The antivirus log included log messages that were not related to antivirus.
SP-25199	When migrating a file system to a CTERA Edge Filer that is associated with more than one zone, cloud folders were added to these zones even when they should only have been migrated to the configured zone.
SP-25553	Improved security when using SAML to prevent XML signature wrapping (XSW) attacks

9

CTERA PORTAL 8.2.1500.5 (MAY 2024)

WHAT'S NEW

What's New In the Portal Image

ID Number	Description
PIM-4048	Improved support for Varonis Data Security Platform
PIM-3874	When using the Edge Filer Syslog service, some logs were not being sent to the Syslog server,
PIM-3873	`portal.sh pcc_start` did not work.

New Software Features

ID Number	Description
—	See What's New in CTERA Portal Version 8.2.x
SP-23522	In order to share a cloud drive folder with an Active Directory domain account, without using an email address to identify the account, run the following CLI: `set /settings/searchEmailsInAD false`. Users can be retrieved using just the first name and last name.
SP-24356, SP-24295, SP-24220, SP-24218, SP-24217, SP-24210, SP-24205	The Content Security Policy (CSP) feature has been improved. For details about CSP, see https://kb.ctera.com/docs/enable-content-security-policy-csp.

Resolved Software Issues

ID Number	Description
SP-21369	The CTERA FSCK utility displayed milliseconds instead of minutes after failing to load a mapfile from a storage node.
SP-21559	The Angular.js package that caused CVE-2022-25844 has been fixed.
SP-23124	In rare cases, edge filers did not receive requested information, such as folder list or user information.
SP-23291	The snapshot cleaner task took a very long time to complete.

ID Number	Description
SP-23714	The files counter under Cloud Drive Folders was not updated after uploading empty files from the edge filer.
SP-24173	The primary database server did not restart automatically after a power outage.
SP-24189, SP-24682	There was no message for read only administrators that they could not upload firmware to the portal.
SP-24289, SP-24906	Logstash did not restart after an upgrade or when using `portal-manage.sh start` or `portal-manage.sh restart` after stopping the server.
SP-24390	The CTERA FSCK utility failed if it had to handle a block with a NULL location.
SP-24396	If a scheduled task was stopped by the administrator, it could not be restarted manually.
SP-24535	File and folder names were being translated in the Chrome browser.
SP-24613	The same task could run multiple times in parallel, with each task closing the transactions of a parallel task.
SP-24626	Syslog transactions were not always closed which caused tasks to not finish.
SP-24750	Creating an S3-based storage node with an uppercase name created the bucket but with a disconnected status and an error that the name should not use uppercase letters.
SP-24759	The Verify sync task failed for files with circular paths.
SP-24809	When using CTERA Fusion, multipart uploads could fail.
SP-24822	The task `Mapfiles RC Stream Cleaner r`an on all servers and not just the database servers.
SP-24868	The user interface did not show which of the two options, **ADMINISTRATION PALETTE** or **END USER PALETTE**, was being displayed.
SP-24895	Some log files (`amqpconfig` log files) were not being overwritten or cleared.
SP-24901	When using CTERA Fusion, it took a long time to browse to a folder after mounting an S3 cloud folder using S3fs.
SP-24926	An application server log was filled with warnings `WARN [io.milton.http.entity.DefaultEntityTransport] - No response entity to send!`
SP-24954	Clicking **SHOW ALL DEVICES** under **DEVICES** in the Dashboard displayed the **EDGE FILERS** page instead of the **DEVICES** page.
SP-24968	When using CTERA Fusion, folders were displayed as files after mounting an S3 cloud folder using S3fs.
SP-24992	The CTERA FSCK utility was processing empty folder groups for a few days.