RELEASE NOTES

CTERA Portal 8.1.1417.46

August 2025

Note: For legal information and for the end user license agreement, refer to https://www.ctera.com/eula/.

CONTENTS

1

CTERA PORTAL 8.1.1417.46.4

Portals must be upgraded from CentOS 7 to CentOS 9 using earlier CentOS 7 and CentOS 9 versions, as described in Upgrading a Portal Running on CentOS 7 to Run on CentOS 9, and then upgrade the CentOS 9 version to this 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 VDI users, for mobile users, and for zero-minute disaster recovery feature.

You cannot upgrade to CTERA Portal version 8.1.x without a valid license that has not expired. When the portal license is about to expire, notifications appear in the portal user interface and the administrator can contact CTERA for a license renewal. Additionally, emails are sent to the administrator.

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 7.2.x to 8.1.x requires first upgrading to 7.5.x and then to 8.1.x.

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

Note: The minimum version of the CTERA Edge Filer connected to the portal must be 7.6.3111.5 and to migrate WORM compliant shares using CTERA Migrate, the minimum version of the CTERA Edge Filer must be 7.6.3111.22.

Upgrading the CTERA Portal

Warning: You cannot upgrade directly from version 7.5.1159.25 or earlier.

- Upgrading a portal running on CentOS 7 requires a different command to upgrading a portal running on CentOS 9 as described in Upgrading a CTERA Portal.
- 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 or 8.1.1417.13, the integration **must** be removed from both the Varonis Data Security Platform and the CTERA Portal and then reconfigured after the upgrade as described in https://kb.ctera.com/docs/integrating-ctera-with-varonis-data-security-platform-4.
- When using the Edge Filer Syslog service, disable and then re-enable the Edge Filer Syslog service after the upgrade.

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.

Upgrading a Portal Running on CentOS 7 to Run on CentOS 9

The CTERA Portal is upgraded as described in Upgrading a CTERA Portal.

Upgrading a Portal with the CTERA Messaging Service Implemented

CTERA recommends running the following command on every messaging server to ensure that the messaging server is running correctly: `curl http://localhost:8083/connector-plugins`

The expected output:

```
[{"class":"io.confluent.connect.jdbc.JdbcSinkConnector","type":"sink","version":"10.5.1"},
{"class":"io.confluent.connect.jdbc.JdbcSourceConnector","type":"source","version":"10.5.1"},
{"class":"io.debezium.connector.postgresql.PostgresConnector","type":"source","version":"1.9.5.Final"},
{"class":"org.apache.kafka.connect.mirror.MirrorCheckpointConnector","type":"source","version":"7.2.1-ccs"},
{"class":"org.apache.kafka.connect.mirror.MirrorHeartbeatConnector","type":"source","version":"7.2.1-ccs"},
{"class":"org.apache.kafka.connect.mirror.MirrorSourceConnector","type":"so
urce","version":"7.2.1-ccs"}]
```

If there is a different output, run `docker restart kafka_connect_kafka_connect_1`

Active Directory Running on Windows 2003

Support for the weak encryption mode used by Active Directory on Windows Server 2003 is not supported by default on this version. When using CTERA Portal and Active Directory on Windows Server 2003, `set /settings/defaultPortalSettings/activeDirectorySettings/legacyActiveDirectorySupport true`. The default is `false`.

Set true to enable support for the encryption mode used by Active Directory on Windows Server 2003. This setting is false by default.

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.

ENABLING CONTENT SECURITY POLICY (CSP)

Content Security Policy (CSP) can help protect CTERA Portal when a secure policy is defined. The policy must prevent the execution of untrusted scripts using CSP. When CSP is enabled on the CTERA Portal, every request that goes through the portal server has a CSP with strict rules.

Note: In some cases, where strict is colliding with GUI functionalities, the CSP is less strict.

Enabling CSP does not require any addition CTERA resources.

For full details, see https://kb.ctera.com/docs/enable-content-security-policy-csp.

WHAT’S NEW

CTERA Portal version 8.1.1417.2 included a number of new features for global and team portal administrators and for end users. For details, see What's New in CTERA Portal Version 8.1.x.

What’s New In the Portal Image

ID Number	Description
PIM-4526, PIM-5246, PIM-5298, PIM-5300, PIM-5374, PIM-5452 PIM-5466, PIM-5493, PIM-5501, PIM-5677, PIM-5682	Security improvements including: • Resolving CVE-2024-56337, CVE-2025-49796, CVE-2025-49794, CVE-2025-6021, CVE-2022-29458, CVE-2023-29491 • Improved security for TLS renegotiations. • A PostgreSQL vulnerability was resolved.
PIM-4736, PIM-4882	The SSH configuration files have been hardened.
PIM-5366	The CTERA Messaging service did not work after migrating a portal from CentOS7 to CentOS9 in Microsoft Azure.
PIM-5377	Upgrading the portal failed when there was no Internet access.
PIM-5420, PIM-5669	Improvements to the **ctera_firstboot** procedure: • The **ctera_firstboot .log** now includes timelines to identify how long each step takes. • *cloud-init* has been enabled for deployments in all platforms except for Microsoft Azure.
PIM-5478	Even when the **portal-storage-util.sh** script completed successfully, the return code reported an error.
PIM-5488	Replacing a messaging server with another server caused the portal to fail.

New Software Features

ID Number	Description
SP-27086	SSHJ has been upgraded to support SHA2 and comply with updated crypto policies.

Resolved Software Issues

ID Number	Description
SP-27075	The number of files in the edge filer did not match the number on the filer when some files had a zero size.
SP-27110	The edge filer repeatedly disconnected from the portal after a map file error.
SP-27244	Alert notifications were continuously sent to both portal users and external users.
SP-27444	Attempting to assign the default plan to a new user failed.

KNOWN ISSUES

ID Number	Description
CENV-672	Microsoft Defender reports issues when deploying a portal in Azure.
PIM-3977	See the notes in Upgrading the CTERA Portal.

PIM-4632	When upgrading a portal running on CentOS 7, running `install.sh` on the portal blocks the SSH connection and causes the Nomad RPMs to fail.
	Workaround: Reinstall Consul and Nomad by running the following CLI:
	`platform-services rerunlazyinstall --force`
	If the run directory is not removed, do the following:
	1 On all servers run
	`rm -rf /usr/local/lib/ctera/work/microservices/run; systemctl stop nomad;`
	2 On the primary DB server, run the following:
	`su - postgres`
	`psql`
	`update persistent_context set text = '{"state":"INSTALLED"}' where id = 4;`
	`telnet 0`
	3 Login and run `platform-services rerunlazyinstall --force`
	4 Verify that the portal is running on all the servers.
	Servers should be connected one by one after approximately 6-15 min.

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.
SP-21806	Setting a preview server takes approximately 60 seconds to start working.

2

CTERA PORTAL 8.1.1417.44 (MAY 2025)

WHAT’S NEW

New Software Features

ID Number	Description
SP-25513, SP-26193, SP-26996, SP-27090	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-26930, SP-26993	Improvements to the Varonis server, including being able to set debug mode for the Varonis service.

Resolved Software Issues

ID Number	Description
SP-25890	Exception were issued when attempting to delete an offline server from the portal.
SP-27012	Users in the *Domain Users* group in Microsoft Active Directory were not automatically fetched.

3

CTERA PORTAL 8.1.1417.43 (APRIL 2025)

WHAT’S NEW

What’s New In the Portal Image

ID Number	Description
PIM-5246	Security improvements, for example, to prevent TLS renegotiation attacks.

New Software Features

ID Number	Description
SP-26665, SP-26900	Security improvements, for example, preventing malicious users to saturate the quota of space available to other users and resolving the CVE-2018-15546 vulnerability.

Resolved Software Issues

ID Number	Description
SP-26838	Certificates could not be uploaded to the portal.
SP-26950	A Nomad server members amount error could be reported.

4

CTERA PORTAL 8.1.1417.41 (APRIL 2025)

WHAT’S NEW

What’s New In the Portal Image

ID Number	Description
PIM-3882	Improved installation of platform services using a dedicated RPM.
PIM-4164	When starting a CentOS 9 portal under AWS, errors were written to the console.
PIM-4367, PIM-5035, PIM-5155, PIM-5173, PIM-5174, PIM-5178	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-5062	Upgrading a portal has been improved to enable upgrading a portal when offline using the script `rpm_upgrade.sh`.
PIM-5180, PIM-5181	The apache-tomcat package has been upgraded to 9.0.102 to resolve CVE-2025-24813.

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-26224	A new email template, **Crl failed download attempt**, has been added to the global administrator view. The notification alerts the administrator when there is an error while attempting to retrieve and verify certificate information.
SP-26665, SP-26805	Improved security, for example against BREACH attacks.

Resolved Software Issues

ID Number	Description
SP-26367	A new portal server could not be added to the primary server.
SP-26561	After enabling zones, adding an edge filer to the zone caused a sync error on the edge filer.
SP-26676	After cancelling and then restarting CTERA FSCK, it started on the wrong cloud folder group.
SP-26747	When a sync with an edge filer was not successful, the notification remained even after the sync was successful.

5

CTERA PORTAL 8.1.1417.36 (FEBRUARY 2025)

WHAT'S NEW

What's New In the Portal Image

ID Number	Description
PIM-3822	After an upgrade, thumbnails were not generated.
PIM-4185, PIM-4195, PIM-4301, PIM-4690, PIM-4736, PIM-4786, PIM-4788, PIM-4789, PIM-4811, PIM-4816, PIM-4937, PIM-4840, PIM-4939, PIM-4940, PIM-4943, PIM-4944, PIM-4945, PIM-4946, PIM-4947	Security improvements including removing SHA1 from the SSH configuration files and resolving CVE-2024-39689, CVE-2024-50379, CVE-2024-50379, CVE-2024-7264, CVE-2024-37891, RHSA-2024:3588, RHSA-2024:3741, and RHSA-2024:3939 advisories.
PIM-4352	The NTP server IP address can be used when configuring NTP in the CTERA Portal server.
PIM-4463, PIM-4464	From portal version 8.1.1417.24, the Edge Filer Syslog service did not work.
PIM-4692, PIM-4792, PIM-4798, PIM-4836	Improvements to the installation first boot script for versions running on CentOS 9. For example, PIM-4872 is resolved as docker images are moved to the datapool so that the portal storage is not full.
PIM-4760, PIM-4763, SP-26435	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-4843	Improvements to the migration.sh script used when upgrading a portal running on CentOS 7 to run on CentOS 9.
PIM-4856	The PSQL file was missing from the image since portal version 7.5.1159.31.
PIM-4953	With a portal running on CentOS 9, the KMIP client failed to initialize.
PIM-5035	The *ctera_firstboot.sh* script failed to mount the data disk on a portal installed with CentOS 9 on Microsoft Azure.

New Software Features

ID Number	Description
SP-25737	The Australia (Melbourne) region, Availability Zones: 3, is now available.
SP-26040	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-26193	Improved security.

Resolved Software Issues

ID Number	Description
SP-25985	From portal version 8.1.1417.24, a VPC endpoint to an Amazon S3 storage node did not work.
SP-26122	When the antivirus service was enabled, the auto vacuum task for `map_file_infected_status` ran for too long.
SP-26137	Adding a server sometimes started the server without some internal components being installed.
SP-26171	Configuring the Edge Filer Syslog service to use a TLS certificate did not work.
SP-26252	Global administrators could not create an SSO activation code to access the portal.
SP-26407	Files could not be shared with Active Directory users who did not have a last name in Active Directory.
SP-26480	Any exception during the notification process could cause the entire transaction to fail.
SP-26491	Increased security against brute-force attacks.

6

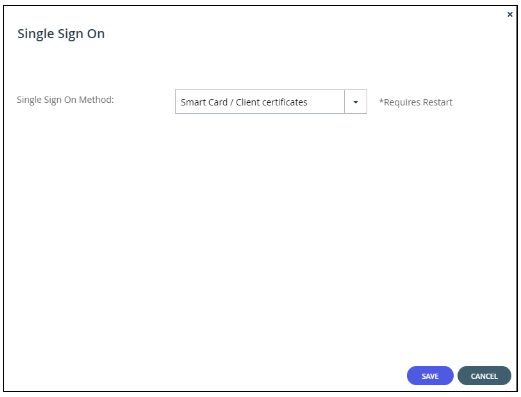
CTERA PORTAL 8.1.1417.32 (DECEMBER 2024)

WHAT'S NEW

What's New In the Portal Image

ID Number	Description
PIM-4373	Upgrading a portal running on CentOS 9 overrode the pg_ident.conf file.
PIM-4663, PIM-4664, PIM-4666, PIM-4667, PIM-4686, PIM-4699, PIM-4700, PIM-4705	Security improvements.

New Software Features

ID Number	Description
SP-26083	The **OCSP Revocation Checking** checkbox has been removed from SSO CAC configuration.  Single Sign On Single Sign On Method: Smart Card / Client certificates *Requires Restart

Resolved Software Issues

ID Number	Description
SP-25838, SP-25840, SP-25842, SP-25844	Security improvements.

ID Number	Description
SP-25913	The server status remained `Deployment in Progress` even after the deployment completed.
SP-25936	Consul and Nomad services were reported as not ready, even when they were ready.
SP-25956	The permanent delete operation in a WORM folder was slow.
SP-25968	Deleting a file on an edge filer that was permanently deleted on the portal caused the sync queue to stall with one file uploading.
SP-26005	The local quota feature did not work when the folder was empty.
SP-26014	The first previous snapshot did not exist after restoring a file from a version before this snapshot.
SP-26028	When LDAP channel binding was enabled, Active Directory domain lookup failed when both SSL and Kerberos were enabled.

7

CTERA PORTAL 8.1.1417.27 (NOVEMBER 2024)

WHAT’S NEW

What’s New In the Portal Image

ID Number	Description
PIM-4226, PIM-4246	After upgrading a Portal running on CentOS 7 to run on CentOS 9, any preview servers failed to start.
PIM-4248, PIM-4488	When connecting a new secondary server to the primary server on a portal running on CentOS 9, Nomad is disabled.
PIM-4383, PIM-4386, PIM-4389, PIM-4414	Improvements to the Varonis integration.
PIM-4423	Logs were not being sent to the syslog server .
PIM-4503	The Edge Filer Syslog service failed to start on a portal running on CentOS 9.
PIM-4516, PIM-4557, PIM-4614, PIM-4616	RHSA-2024:3669, RHSA-2024:3939, CVE-2024-37891, CVE-2024-7264, CVE-2022-42889, CVE-2018-20685, CVE-2019-6109, CVE-2019-6110, and CVE-2019-6111 have been resolved.
PIM-4522	postgres.auto.conf was overridden after an upgrade on a portal running on CentOS 9.
PIM-4561, PIM-4564	Installing a portal in a KVM or Hyper-V environment running on CentOS 9 failed to start the docker services when booted up.
PIM-4574	Installing a portal running on CentOS 9 in a Hyper-V environment did not install the hypervisor agent.

New Software Features

ID Number	Description
SP-25764, SP-25838, SP-25840, SP-25842, SP-25844	Improved security.

Resolved Software Issues

ID Number	Description
SP-24549	The Thumbnails service did not produce thumbnails for some files.
SP-25719	When using a portal with Snowflake, an incorrect certificate was used to access the bucket.
SP-25734	API keys could not be generated nor deleted by read only or support administrators.
SP-25769	The Edge Filer Syslog service failed to start on a portal running on CentOS 9.
SP-25801	A global administrator from Active Directory could not create folders in the end user portal.
SP-25807	Updating user accounts could become stuck.
SP-25822	When connecting a new secondary server to the primary server, the connection hanged until the browser was refreshed.
SP-25829	Undeleting a folder failed when the folder contained a deleted populated subfolder.
SP-25856	The notification email to an administrator after a permanent deletion, for two-factor authentication, to complete the permanent deletion was not sent.

8

CTERA PORTAL 8.1.1417.24 (OCTOBER 2024)

WHAT’S NEW

What’s New In the Portal Image

ID Number	Description
PIM-4153	Local quotas were not being applied to edge filers running version 7.8.x.
PIM-4244	The FIPS module size has been reduced.
PIM-4248	With CentOS 9 servers: Connecting another server to the primary DB server caused Nomad to need restarting.
PIM-4310, PIM-4317, PIM-4348	CVE-2024-7348, CVE-2024-34750, and CVE-2024-39689 have been resolved.
PIM-4319	With CentOS 7 servers: The migration script has been added to the image as a prerequisite to upgrading to CentOS 9.
PIM-4331	`server.xml` has been removed from the server code.
PIM-4359, PIM-4412	The portal dump file name has been changed to include the portal server name.
PIM-4373	Upgrading the image overrode some PostgreSQL configuration.
PIM-4426, PIM-4433	The local quota service failed when it was initialized but did not complete.

New Software Features

ID Number	Description
SP-25513, SP-25704	Improved security when signing in using SSO and when using SAML to prevent XML signature wrapping (XSW) attacks for portals running on CentOS 9.
SP-25579	The mechanism to create a branded portal has been improved.
SP-25702	Local quota support has been improved to take less time.

Resolved Software Issues

ID Number	Description
SP-25613	When the snapshots were created at the end of a month, snapshots for months with less days were not retained.
SP-25259	API keys generated by an end user or administrator were not saved.
SP-25651	On a Microsoft Azure platform, the CTERA FSCK tool could mark blocks that existed as missing.

9

CTERA PORTAL 8.1.1417.20 (SEPTEMBER 2024)

WHAT’S NEW

New Software Features

ID Number	Description
SP-25183, SP-25565	The CTERA FSCK command has been improved. For example, when running using the `all -r argument`.
SP-25260	Improved performance when accessing content using CTERA Drive Share (Agent).
SP-25265, SP-25300	More information is provided for on-demand antivirus scans: • The time to initiate an on-demand scan. • The percentage of antivirus scans run manually.
SP-25311	The Verify Sync task has been improved so that syncing is and file re-hydration is faster.
SP-25513	Improved security when using SAML to prevent XML signature wrapping (XSW) attacks.

Resolved Software Issues

ID Number	Description
SP-25297	The messaging service failed after upgrading from portal version 8.1.1417.13.
SP-25302	Sending a file using the CTERA Outlook add-in did not work.
SP-25308	Migrating a WORM compliant share using CTERA Migrate migrated the files in the share with the wrong creation time.
SP-25416	Setting **Enable Zones** in **Global Settings** did not work.
SP-25429	The session cookie did not contain the *secure* attribute.

10

CTERA PORTAL 8.1.1417.19 (AUGUST 2024)

WHAT’S NEW

What’s New In the Portal Image

ID Number	Description
PIM-4104	Improved security for SSH configuration.

11

CTERA PORTAL 8.1.1417.17 (JULY 2024)

WHAT’S NEW

What’s New In the Portal Image

ID Number	Description
PIM-4067	When upgrading a portal, Microsoft Team values in the old portal configuration are copied to the upgraded portal configuration.
PIM-4098	SHA1 has been removed from SSH configuration to improve security.
PIM-4148	The Varonis configuration was removed when upgrading the portal to an 8.2.x version.

New Software Features

ID Number	Description
—	Security improvements.
SP-25070	Backup folders now support fixed block size.
SP-25156	The Verify Sync task has been improved.
SP-25264	Average scan times for antivirus scans have been added.

Resolved Software Issues

ID Number	Description
SP-24993	The CTERA FSCK utility was processing empty folder groups for a few days.
SP-25137	Default zones were not created when enabling zones in the user interface.
SP-25201	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-25248	Upgrading a portal from version 7.5.x took too long.

12

CTERA PORTAL 8.1.1417.13 (MAY 2024)

WHAT'S NEW

What's New In the Portal Image

ID Number	Description
PIM-4051, PIM-4052, PIM-4053, PIM-4054, PIM-4055, PIM-4056, PIM-4057	Improved support for Varonis Data Security Platform

New Software Features

ID Number	Description
SP-24938, SP-24939, SP-24940, SP-24941, SP-24942, SP-24943, SP-24944, SP-24945	The CTERA Portal Varonis service now supports logs from more than one CTERA Edge Filer. The Varonis service has been hardened to be more resilient. However, the changes to the Varonis service require changes to the setup as follows: • All CTERA Edge Filers must be removed from the Varonis Management Console and re-added. • The Varonis collector hostname and IP address must be added to the `/etc/hosts` file on every portal server in the portal cluster. • You need to run CLIs on each CTERA Edge Filer that you want to send logs to Varonis Data Security Platform. For information, contact CTERA support.

Resolved Software Issues

ID Number	Description
SP-24924	When using CTERA Fusion, it took a long time to browse to a folder after mounting an S3 cloud folder using S3fs.
SP-24947	Syslog transactions were not always closed which caused tasks to not finish.
SP-24969	When using CTERA Fusion, folders were displayed as files after mounting an S3 cloud folder using S3fs.
SP-24973	The Angular.js package that caused CVE-2022-25844 has been fixed.

Known Issues

ID Number	Description
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.
SP-21806	Setting a preview server takes approximately 60 seconds to start working.

13

CTERA PORTAL 8.1.1417.12 (APRIL 2024)

WHAT'S NEW

What's New In the Portal Image

ID Number	Description
PIM-3930	Values in the portal configuration file, portal.cfg, were overridden after an upgrade.
PIM-3963	YUM command-line package-management utility failed to run.
PIM-4028	After implementing the Thumbnail service, after a user viewed the thumbnails and then logged out, the thumbnails remained available to anyone using the page URL. Also see SP-24802.

New Software Features

ID Number	Description
—	Content Security Policy (CSP) has been implemented.
SP-24745	If an administrator attempts to sign in to a portal with incorrect credentials, either the user name or password, when the sign-in page is redisplayed, both the user name and password fields are empty instead of displaying what was originally entered.
SP-24794	In the user interface, Microsoft product names are now displayed with Microsoft before the product name.

Resolved Software Issues

ID Number	Description
SP-24235, SP-24238, SP-24239, SP-24299, SP-24729, SP-24730, SP-24740, SP-24742, SP-24743, SP-24744	Improved handling when Content Security Policy (CSP) is enabled, including: • Remote access to the portal did not work. • Previewing email templates did not display the preview correctly. • CSP headers were not defined on `/common-<version>` responses. • A custom login page did not work. • Logging on to the portal directly with single sign-on, failed. • Connecting to the portal from CTERA Drive Share/Protect with SAML single sign-on, failed. • When Microsoft Office 365 online was not configured the CSP request included `null: frame-src 'self' null://null;` • When Microsoft Office 365 online was configured it did not work.

ID Number	Description
SP-24633	After upgrading a portal from version 7.2.186.63.1 to 7.5.1159.39, the portal failed to start.
SP-24648	Signing in to a portal with Microsoft Entra ID failed if the user name included parentheses.
SP-24693	Deleting a cloud folder from the trashcan also deleted any cloud folder with a name similar to the same name but with different use of upper and lower case letters in the name.
SP-24757	After upgrading a portal, the Varonis and Edge Filer Syslog services did not work.
SP-24783	Deleted cloud folders were displayed in the trashcan with negative sizes.
SP-24786	Attempting to download a stub file when the map file is missing could result in an NFS mount failing and a delay before the error is reported.
SP-24791	Device management did not work when a consent page was enabled.
SP-24801	Modifications of Microsoft Office files by an external user with write permissions, were not saved.
SP-24802	After implementing the Thumbnail service, after a user viewed the thumbnails and then logged out, the thumbnails remained available to anyone using the page URL. Also see PIM-4028.
SP-24803	Using SSO to access a portal failed when the username was over 20 characters.
SP-24833	Cloud folders that were deleted still remained after the retention period passed.
SP-24835	After deleting a cloud folder and then creating a new cloud folder with the same name, ignoring case changes for the name, upgrading the portal caused the cloud folder to be permanently deleted.
SP-24838	When there was an attempt to upload a file while downloading a file with the same name but a different GUID, the folder usage information was wrong leading to an out of quota messages, and the upload being stuck.

14

CTERA PORTAL 8.1.1417.4 (FEBRUARY 2024)

WHAT’S NEW

CTERA Portal version 8.1.1417.2 included a number of new features for global and team portal administrators and for end users. The following sections provide and overview of the new features. For more details, see What's New in CTERA Portal Version 8.1.x.

Note: The **local quota** feature requires a CTERA Edge Filers running version 7.5.2820.13 or higher.

What’s New In the Portal Image

ID Number	Description
PIM-3941	Logs have been added when installing the Key Management (KMIP) service.

15

CTERA PORTAL 8.1.1417.2 (JANUARY 2024)

WHAT’S NEW

What’s New In the Portal Image

The portal image includes the following:

ID Number	Description
—	Ongoing security improvements.
PIM-3637, PIM-3820	PostgreSQL has been upgraded to version 14.9.
PIM-3706	Provisioning in FIPS failed.
PIM-3713, PIM-3719	Nomad has been upgraded to version 1.6.
PIM-3745	Upgrade and Nomad logs were not included when `portal-dump.sh` was run.
PIM-3776	A new argument, `n`, has been added to `portal-dump.sh` to collect more logs.
PIM-3793	S3 routing overrode all other routings.
PIM-3849, PIM-3850	The preview server module has been upgraded to PrizmDoc Viewer 13.25.

Resolved Software Issues

ID Number	Description
—	Ongoing security improvements.
SP-20169, SP-22240, SP-23512, SP-23614	Exception errors were issued when signed in as a global administrator. For example, when a global administrator tried to share a folder or resent a collaboration message to users in a non-default portal or when using the Kerberos protocol with Active Directory to define Single Sign-on.
SP-20662	Errors displayed when configuring a storage node were not removed when changing the storage node type.
SP-21142	Fetching user from Active Directory where the domain service account name started with a special character, such as the $ character, failed.
SP-21613	Accessing a team portal using the reseller portal login URL displayed the login page.
SP-21901	Deleted data was kept after the retention period expired.
SP-22245	When NFS storage was 100% full, the portal did not notify the administrator.
SP-22975	Running manage-quota-messaging-service with an invalid argument issued an exception instead of a clear message.

ID Number	Description
SP-23043	Changing the owner of a team project caused the team project storage amount to be added to the storage amount of the new owner.
SP-23103	The portal server could not start if both PostgreSQL TSL is set along with FIPS.
SP-23196	Online helps did not access the correct help for the version.
SP-23408	Attempting to connect an edge filer to a portal using single sign-on (SSO) failed when the user existed in SAML.
SP-23427	Using CTERA Fusion was slow when downloading.
SP-23464	Previous versions of files in a cloud folder that was set with compliance, after the previous version was created, are marked as WORM compliant.
SP-23466	Moving a file with the same name as a subfolder to the same level as the subfolder deleted the subfolder and all it's content.
SP-23487	After permanently deleting a file from a virtual portal that is not configured as the default portal, the action is not reported in the logs or reports.
SP-23508	Access to a portal failed when SAML was set up on the primary portal server and access was done using the IP address.
SP-23565	When upgrading, a `Storage node full` error was mistakenly issued.
SP-23578	Unchecking **S3 Endpoint** in a server definition, did not remove the setting in the server Tomcat configuration.
SP-23613	When defining an **API Key**, the **Secret Access Key** value was not securely encrypted.
SP-23637	A new user email was not displayed correctly on an iPhone.
SP-23646	When using zones, making changes to a cloud folder when the cache was not updated was not reflected in on the edge filer.
SP-23648	The **New User Notification** email template had a spelling mistake.
SP-23978	A R/W administrator, without the **Manage Compliance Settings** role on the portal, could create a WORM cloud folder from an edge filer.
SP-24089	A read-only global administrator could modify the Varonis and Edge Filer Syslog services in the user interface.
SP-24095, SP-24271	The snapshot cleaner task configuration was not kept when upgrading the portal.
SP-24107	Files could be uploaded to a deleted folder.
SP-24165	Tags defined for a file on the edge filer that was synced to a folder on the portal and then moved to a different folder on the portal, were not moved with the file.
SP-24240	If an email sent to a user failed because of the address, the email was repeatedly resent to all the users every minute.
SP-24267, SP-24379	When the portal is connected to an edge filer configured to use the next generation file system, a sync discrepancy could happen.
SP-24354	Occasionally an error is issued when a service that requires CTERA Messaging is started or removed.