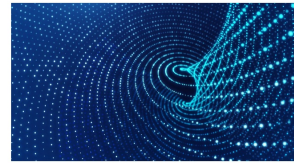




**3.8.0.x ECS Elastic
Cloud Storage**



DELL 3.8.0.x ECS Elastic Cloud Storage User Guide

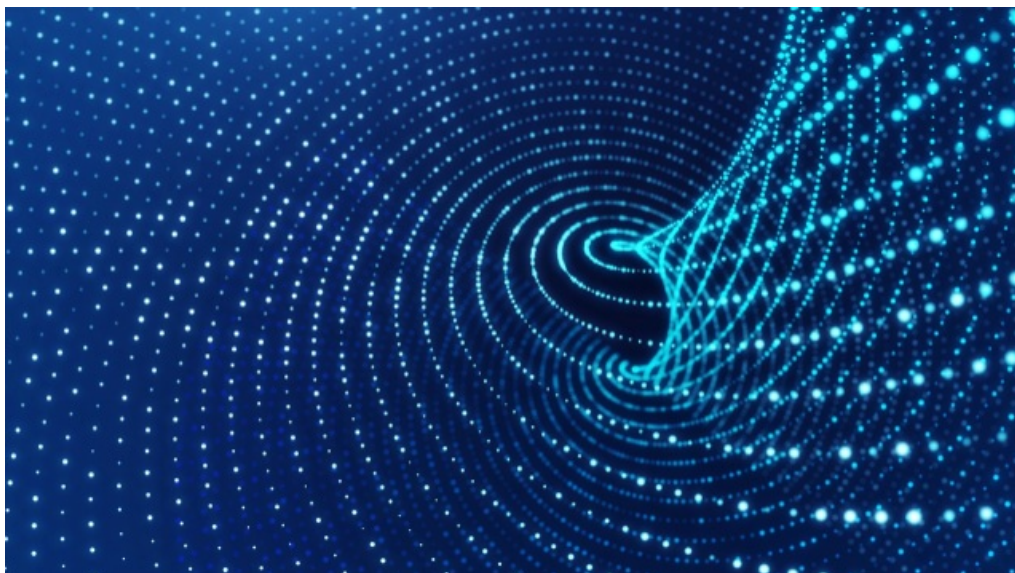
[Home](#) » [Dell](#) » DELL 3.8.0.x ECS Elastic Cloud Storage User Guide 

Contents

- [1 DELL 3.8.0.x ECS Elastic Cloud Storage](#)
- [2 Highlights](#)
- [3 Target Code](#)
- [4 Versioning Information](#)
- [5 Connectivity](#)
- [6 ECS Capacity Dashboard](#)
- [7 ECS Troubleshooting Guide](#)
- [8 Subscribe to our newsletter](#)
- [9 Documents / Resources](#)
 - [9.1 References](#)



DELL 3.8.0.x ECS Elastic Cloud Storage



Highlights

- ECS 3.8.0.4 is available.
- Site Contact Information Update & Product Updates.
- ECS Troubleshooting Guide is now available for customers.
- xDoctor tool is customer downloadable and installable. ****NEW VERSION****

Target Code

Dell Technologies Total Customer Experience (TCE) team regularly monitors the quality and stability of supported code versions across the active customer install base. This data is used to guide what code version is recommended for customers to run to be most stable with the lowest risk. Customers on older code should upgrade to the target code version (or later).

ECS 3.8.0.x (with minimum patch ECS 3.8.0.2) declared Target Code

The TCE team, comprised of key Engineering and Services leadership, recommends the adoption of ECS 3.8.0.x, which achieved target code status in August 2023. It continues to be the best-performing code across all actively supported code versions. The recommendation is to upgrade to the latest patch of the target code, which is currently ECS 3.8.0.4.

You can find a full list of Dell product target codes at: [Target-Revisions-and-Runtime-Hours \(dell.com\)](https://dell.com/target-revisions-and-runtime-hours)

For information on how upgrades are performed, please refer to the following Knowledge Base (KB) article: [KB 14729: ECS Upgrade Planning](#)

Code Recommendations, Published End of Standard Support (EOSS), and Versioning Information



Have you upgraded to the Target Code (or newer) yet?

- Upgrading to the Target Code (or newer) is important. Customers on newer code enjoy greater functionality and fewer outages/service requests.
- Upgrading to the Target Code (or newer) ensures that you can take advantage of the newest features, functionality, fixes, and security enhancements. For ECS that means code level 3.8.0.4.
- [To learn more about the Target Codes, please refer to the Target Revisions document](#).

Published End of Standard Support (EOSS)

This table provides the published EOSS dates for all ECS versions:

Version	General Availability (GA) Date	Published EOSS
3.8.0.4	November 2023	December 2025
3.8.0.3	August 2023	December 2025
3.8.0.2	April 2023	December 2025
3.8.0.1	December 2022	December 2025
3.7.0.6	May 2023	February 2025
3.7.0.5	February 2023	February 2025
3.7.0.4	November 2022	February 2025
3.7.0.3	September 2022	February 2025
3.7.0.2	May 2022	February 2025
3.7.0.1	April 2022	February 2025
3.7.0.0	February 2022	February 2025
3.6.2.x	August 2021*	August 2024
3.6.1.x	February 2021*	February 2024
3.6.0.x and below	Various	EOSS

- Various General Availability (GA) dates for patches.

Additional information on EOSS dates for Dell products can be found by searching for the specific Dell product within the Support by Product section from the Online Support site.

Versioning Information

- This table provides information on the ECS versioning convention:

Release Digit	Release Type	Description
First (X .x.x.x)	Major	Release with functionality that provides substantial generational or architectural changes in the product.
Second (x. X .x.x)	Minor	Release that delivers new incremental functionality to the existing product generation, in addition to fixes for defects.
Third (x.x. X .x)	Service Packs	Release that delivers fixes for important defects, fixes to Security Vulnerabilities, and included fixes delivered by preceding patches and hotfixes.
Fourth (x.x.x. X)	Patches	Release that cumulatively delivers fixes to security vulnerabilities and critical customer-found issues.

Release Information – ECS 3.8.0.x (Latest and Target Code)

ECS 3.8.0.x Release Highlights

Reasons to Upgrade:

- Improved Stability
- Improved Performance
- Improved Security
- Tech Refresh Enhancements
 - Node Evacuation
 - Node Extend

Key Features in 3.8.0.x: (in addition to the existing features from the previous versions)

- Data movement (Copy-to-Cloud)
- IAM STS GetFederationToken
- Extended key management interoperability protocol (KMIP) Support
- Object lock enhancements for ADO
- Memory upgrade expansion
- SSH key rotation Improvements
- Firmware upgrade using the service console
- Simplified bucket delete
- Priority task coordinator
- Metadata search acceleration
- Partial listings
- HDFS protocol support

Release Notes

- [ECS 3.8.0.4 Release Notes](#)

Online Support Page

- [ECS Appliance](#)

Additional Resources

- [ECS 3.8 Product Documentation Index Info Hub](#)
- [ECS technical white papers and videos](#)

Connectivity

Secure Connect Gateway

The Secure Connect Gateway technology is the next-generation consolidated connectivity solution from Dell Technologies Services. Support Assist Enterprise and Secure Remote Services capabilities are integrated into Secure Connect Gateway technology. Our Secure Connect Gateway 5.1 technology is delivered as an appliance and a stand-alone application and provides a single solution for your entire Dell portfolio supporting servers, networking, data storage, data protection, hyper-converged, and converged solutions. For more details refer to the

[Getting Started Guide](#) and [FAQs](#), which are great resources to start with.



Note: If you are having issues getting connected, please make sure to contact customer support.

SRS Customers Will Lose Connectivity as of June 2023

- Effective June 15, 2023, all versions of Secure Remote Services (SRS) will reach end of service life and will be replaced with Secure Connect Gateway (SCG). Upon reaching end of service life, support (including remediation and mitigation of security vulnerabilities) will be discontinued, and Secure Remote Services clients may no longer be able to connect.
- Effective immediately, Secure Remote Services will strive to provide remediation for [critical](#) security vulnerabilities only. This may leave Secure Remote Services exposed to lesser severity vulnerabilities which Dell Technologies will no longer remediate or mitigate for customers. Dell Technologies therefore recommends upgrading to Secure Connect Gateway immediately to ensure that you remain current with security and quality updates.
- Secure Connect Gateway, introduced in 2021, provides customers with the benefits of the latest technologies. Upgrading to Secure Connect Gateway requires a few steps due to technology and security changes that Dell Technologies has made over time.

To upgrade to Secure Connect Gateway

- First, ensure you are running the latest release of Secure Remote Services version 3.52.
- Follow the instructions in the banner to upgrade to Secure Connect Gateway.
- [Click here](#) for additional upgrade details.

Should you choose to keep Secure Remote Services beyond the June 15, 2023, end-of-service life date, please note that you are responsible for any security vulnerabilities experienced.

Site Contact Information Update & Product Updates

Keeping your Site's contact information updated is vital to receive important updates.

- Make sure that your Site's contacts are updated regularly. Refer to Knowledge Base (KB) [Company Administration – View and Manage Sites & Contacts | Dell US](#) for details on how to update your Site's contacts.
- Make sure to subscribe to the Products Update to get notifications about new releases, new DTAs, and new DSAs. [Learn about how you can subscribe here](#).
- For any issues related to site information management, please open a Service Request using the following link: [Administrative Support | Dell US](#).

Dell Technical Advisories (DTAs)

- Dell published no ECS DTAs in the last 90 days.

Dell Security Advisories (DSAs)

- Dell published the following ECS DSAs in the last 90 days:

DSA	Title	Date
DSA-2023-400	Dell ECS Security Update for Dell ECS 3.8.0.4 Multiple Vulnerabilities	November 2023

ECS Capacity Dashboard

A common topic of interest for ECS customers is how to understand their capacity usage. ECS Knowledge Base (KB) article [20748](#) has been updated with a new video that explains how to interpret the data on the Capacity Dashboard.

Additionally, in response to feedback about multiple capacity-related Service Requests (SRs) being created, changes have been made to ECS capacity alerting dial-homes as follows:

- Starting October 2022, Symptom Code 1111 will no longer open Service Requests.
- Instead, an automated email will be sent to the asset's main contact, informing them that they have reached 65-70% of their capacity usage.
- Refer to the "Site Contact Information Update & Product Updates" section to update your contact details. This will ensure you get automated emails to the asset's main contact.

ECS Troubleshooting Guide

This new customer document will assist in basic troubleshooting steps for ECS. It will walk through what to look for in the UI initially (not all-inclusive), as well as some basic CLI read-only commands. It also covers the Advanced Monitoring (Grafana) UI that was introduced in ECS 3.4.0.0.

To download the latest version of the ECS Troubleshooting Guide:

1. Log into the [Dell Support Site](#) and search for "ECS Troubleshooting Guide" using the top search bar.
2. To download the guide, click "Manuals & Documentation" under the "Resources" section on the left side of the page, and the "ECS Troubleshooting Guide" will appear for download.

A new version, ECS Troubleshooting Guide 1.15, has been released in April 2023. It is recommended to follow the

latest published version.

xDoctor Tool

xDoctor is a tool used by Dell Customer Support to monitor, report on, and troubleshoot the health of your ECS Appliance. Keeping xDoctor updated to the most current version enables Dell Customer Support to quickly detect and resolve issues with your ECS Appliance.

To download the latest version of xDoctor:

1. Log into the [Dell Support Site](#) and search for xDoctor using the top search bar.
2. To download the xDoctor code and Release Notes: Click “Downloads & Drivers” under the “Resources” section on the left side of the page, and the latest xDoctor version xDoctor4ECS 4.8-xx will appear for download, as well as the Release Notes.

A new version, xDoctor4ECS-4.8-94.2, has been released on November 17, 2023. It is recommended to upgrade to the latest xDoctor version at the earliest opportunity.

Disks as Customer Replaceable Unit (CRU)

A new feature starting with ECS 3.5.x.x is disks as Customer Replaceable Unit (CRU) for Gen3 racks. This new feature enables customers to replace failed disks without having to schedule an onsite visit with a Dell Technologies technician to manually remove the disks from the ECS VDC. Customers are now able to manage failed disks from the ECS user interface anytime.

Additional Resources

- [CRU Video: ECS: How to replace EX300 Disk](#)
- [CRU Video: ECS: How to replace EX500 Disk](#)
- [CRU Video: ECS: How to replace EX3000 Disk](#)
- [How to replace ECS EXF900 Appliance NVMe SSD](#)

New Knowledgebase (KB) Articles

Article Number	Title
220323	ECS: xDoctor: RAP072: xDoctor reports hardware event – The system inlet temperature is greater than the upper critical threshold.
220197	ECS: xDoctor: Convert Deprecated Email Rules into one CER (Customer Email Rule)
219870	ECS: Unable to write to a bucket during Temporary Site Outage
220402	ECS: Error Message Displayed When Opening the ECS UI “ERR_SSL_KEY_USAGE_INCOMPATIBLE”
220311	ECS: How to disable CAS access to a node

Top Service Topics

Article Number	Title
216334	ECS: Code Upgrade Recommendation
180322	ECS: Minimum requirements for triggering Permanent Site Outage (PSO), Temporary Site Outage (TSO), and Remove VDC from a Replication Group in ECS

Subscribe to our newsletter

- This newsletter is available via Product Update notifications provided by Dell Technologies Online Support.

[Learn about how you can subscribe here](#)

Access the SolVe website here

- <https://solveonline.emc.com/>



We want to hear from you!

Please take a few minutes to fill out this short survey and let us know what you think of the Newsletter. Simply click below:

<https://app.smartsheet.com/b/form/bc5f50c50fbe48fcb04f5576aa7c9869>

Please feel free to suggest any modifications.

Copyright © 2021 Dell Inc. or its subsidiaries. All Rights Reserved. Dell, Dell Technologies, and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners.

Published January 2024

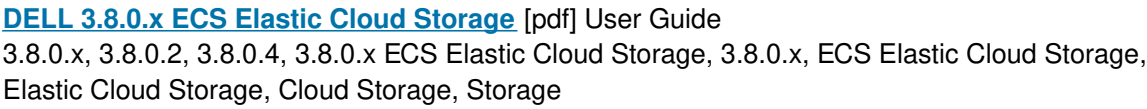
Dell believes the information in this publication is accurate as of its publication date.

The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS-IS." DELL MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND TO THE INFORMATION IN THIS PUBLICATION AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. USE, COPYING, AND DISTRIBUTION OF ANY DELL SOFTWARE DESCRIBED IN THIS PUBLICATION REQUIRES AN APPLICABLE SOFTWARE LICENSE.

Published in USA

Documents / Resources



- User Manual

[Manuals+](#), [Privacy Policy](#)

This website is an independent publication and is neither affiliated with nor endorsed by any of the trademark owners. The "Bluetooth®" word mark and logos are registered trademarks owned by Bluetooth SIG, Inc. The "Wi-Fi®" word mark and logos are registered trademarks owned by the Wi-Fi Alliance. Any use of these marks on this website does not imply any affiliation with or endorsement.