

Table of Contents

1. Software Releases.....	3
1.1. Current Release - Release Notes DR Edition.....	50
1.2. Current Release - Release Notes Platform.....	180
1.3. Current Release - Release Notes Ransomware Defender AWS.....	181
1.4. Current Release - Release Notes Ransomware Defender.....	193
1.5. Current Release - Release Notes Ransomware Defender AirGap 2.0.....	239
1.6. Current Release - Release Notes Ransomware Defender.....	267
1.7. Zero Trust API - Release Notes.....	308
1.8. Current Release - Release Notes Easy Auditor.....	311
1.9. Current Release - Release Notes Golden Copy Search.....	348
1.10. Current Release - Release Notes Performance Auditor.....	385
1.11. Current Release - Release Notes ECA.....	393
1.12. Current Release - Release Notes Golden Copy.....	403
1.13. Current Release - Release Notes - Golden Copy Archive Engine.....	492
1.14. Current Release - Release Notes AnyCopy.....	509
1.15. Current Release - Release Notes Ransomware Defender for ECS.....	518
1.16. Current Release Notes Ransomware Defender AirGap 2.0.....	527
1.17. Release 2.5.8 - Release Notes DR Edition.....	548
1.18. Current Release - Release Notes Easy Auditor.....	660
2. What's new Release Information.....	693
2.1. What's new in Release 1.1.12 for Golden Copy.....	695
2.2. What's new in Release 2.5.9.1 for DR, Ransomware Defender, Easy Auditor.....	697
2.3. What's new in Release 2.5.10 for DR Ransomware Defender, Easy Auditor, Airgap.....	702
2.4. What's new in Release 1.1.13 for Golden Copy, CBDM, Archive Engine.....	704
2.5. What's new in Release 1.1.14 for Golden Copy, Archive Engine, Cloud Browser for Data Mobility.....	706
2.6. What's new in Golden Copy Search 1.2.0.....	709
2.7. What's new in Release 2.5.11 for DR, Easy Auditor, Airgap, Ransomware Defender.....	711
2.8. What's new in Release 1.1.15 Golden Copy, CBDM, Archive Engine.....	714
2.9. What's new in Release 2.5.12 Easy Auditor, AIRGAP, Ransomware Defender, Eyeglass DR.....	717
2.10. What's new in the 3.1.0 Release.....	720
2.11. What's new in Release 3.1.1 RWDAWS.....	722
2.12. What's new in Release 1.1.16 Golden Copy, CBDM, Archive Engine.....	725
2.13. What's new in Release 2.6.0 for DR, Easy Auditor, Airgap, Ransomware Defender.....	729
2.14. What's new in Release 1.1.17 for Golden Copy, CBDM, Archive engine.....	735
2.15. What's new Platform 1.0.0.....	737
2.16. What's new in Release 2.6.1 for DR, Easy Auditor, Airgap, Ransomware Defender.....	738
2.17. What's new in Release 1.1.19 for Golden Copy, CBDM, Archive Engine.....	740
2.18. What's new in Release 2.6.2 Easy Auditor, Airgap, Ransomware Defender, Eyeglass DR.....	744

2.19. What's new in Release 3.2.0 RWDAWS.....	745
2.20. What's new in Release 1.1.20 Golden Copy, CBDM, Archive Engine.....	747
2.21. What's new in Release 2.6.3 Easy Auditor, Airgap, Ransomware Defender, Eyeglass DR.....	751
2.22. What's new in Release 2.6.4 Easy Auditor, Airgap, Ransomware Defender, Eyeglass DR.....	754
2.23. What's new in Release 1.1.21 Golden Copy, CBDM, Archive Engine.....	755
3. End of Sale - End of Support - End of Life.....	759
4. Release Roadmap Login.....	760
4.1. Product Release RoadMap.....	761

1. Software Releases

Home Top

Eyeglass PowerScale Edition Releases

Release Date	Release	Version	Release Notes	End of Support	Dell EMC Known Defects that Affect Eyeglass Operations
12/14/2023	Eyeglass Golden Copy, Cloud Browser for Data Mobility, Archive Engine 1.1.21	1.1.21-23252	Current Release - Release Notes Golden Copy, Archive Engine	07/14/2025	
11/28/2023	Eyeglass DR, Ransomware Defender, Eyeglass Ransomware Defender for ECS, Easy Auditor, Airgap Release 2.6.4	2.6.4-23365	Current Release - Release Notes DR Edition Current Release - Release Notes Ransomware Defender Current Release - Release Notes Ransomware	06/28/2025	

			Defender for ECS Current Release - Release Notes Easy Auditor Current Release - Release Notes Ransomware Defender AirGap 2.		
10/05/2023	Eyeglass Golden Copy, Cloud Browser for Data Mobility, Archive Engine 1.1.20	1.1.20-23215	Current Release - Release Notes Golden Copy, Archive Engine	05/05/2025	
09/28/2023	Eyeglass DR, Ransomware Defender, Eyeglass Ransomware Defender for ECS, Easy Auditor, Airgap Release 2.6.3	2.6.3-23292	Current Release - Release Notes DR Edition Current Release - Release Notes Ransomware Defender	04/28/2025	

			Current Release - Release Notes Ransomware Defender for ECS Current Release - Release Notes Easy Auditor Current Release - Release Notes Ransomware Defender AirGap 2.0		
09/09/2023	Ransomware Defender for AWS	3.2.0	Current Release - Release Notes Ransomware Defender AWS	04/09/2025	
09/01/2023	Eyeglass Golden Copy, Cloud Browser for Data Mobility, Archive Engine 1.1.19	1.1.19-23189	Current Release - Release Notes Golden Copy, Archive Engine	04/01/2025	

09/01/2023	Eyeglass DR, Ransomware Defender, Eyeglass Ransomware Defender for ECS, Easy Auditor, Airgap Release 2.6.2	2.6.2-23282	Current Release - Release Notes DR Edition Current Release - Release Notes Ransomware Defender Current Release - Release Notes Ransomware Defender for ECS Current Release - Release Notes Easy Auditor Current Release - Release Notes Ransomware	04/01/2025	

			Defender AirGap 2.0		
08/03/20 23	Eyeglass DR, Ransomware Defender, Eyeglass Ransomware Defender for ECS, Easy Auditor, Airgap Release 2.6.1	2.6.1-23250	Current Release - Release Notes DR Edition Current Release - Release Notes Ransomwa re Defender Current Release - Release	03/03/20 25	

			Notes Easy Auditor Current Release - Release Notes Ransomware Defender AirGap 2.0		
07/27/2023	Eyeglass Golden Copy, Cloud Browser for Data Mobility, Archive Engine 1.1.17	1.1.17-23170	Current Release - Release Notes Golden Copy, Archive Engine	02/27/2025	
06/29/2023	Ransomware Defender for AWS	3.1.1	Current Release - Release Notes Ransomware Defender AWS	01/29/2025	
06/29/2023	Eyeglass DR, Ransomware Defender, Eyeglass Ransomware Defender for ECS, Easy	2.6.0-23219	Current Release - Release Notes DR Edition Current Release - Release	01/29/2025	

	Auditor, Airgap Release 2.6.0		Notes Ransomwa re Defender Current Release - Release Notes Easy Auditor Current Release - Release Notes Ransomwa re Defender AirGap 2.0		
06/07/2023	Eyeglass Golden Copy, Cloud Browser for Data Mobility, Archive Engine 1.1.16	1.1.16-23119	Current Release - Release Notes Golden Copy, Arch ive Engine	12/07/2024	
05/26/2023	Golden Copy Search	1.2.0-23104	Current Release - Release Notes Golden Copy Search	11/26/2024	

05/09/2023	Eyeglass DR, Ransomware Defender, Easy Auditor, Airgap Release 2.5.12	2.5.12-23175	<p>Current Release - Release Notes DR Edition</p> <p>Current Release - Release Notes Ransomware Defender</p> <p>Current Release - Release Notes Easy Auditor</p> <p>Current Release - Release Notes Ransomware Defender AirGap 2.0</p>	11/09/2024	
05/03/2023	Ransomware Defender for AWS	3.0.1-23168	Current Release - Release Notes Ransomware Defender AWS	11/03/2024	

05/03/2023	Eyeglass Golden Copy, Cloud Browser for Data Mobility, Archive Engine 1.1.15	1.1.15-23075	Current Release - Release Notes Golden Copy, Archive Engine	11/03/2024	
04/06/2023	Golden Copy Search	1.1.14-23065	Current Release - Release Notes Golden Copy Search	10/06/2024	
04/04/2023	Eyeglass Golden Copy, Cloud Browser for Data Mobility, Archive Engine 1.1.14	1.1.14-23065	Current Release - Release Notes Golden Copy, Archive Engine	10/04/2024	
04/03/2023	Eyeglass DR, Ransomware Defender, Easy Auditor, Airgap Release 2.5.11	2.5.11-23110	Current Release - Release Notes DR Edition Current Release - Release Notes Ransomware	10/03/2024	

			Defender Current Release - Release Notes Easy Auditor Current Release - Release Notes Ransomware Defender AirGap 2.0		
03/06/2023	Eyeglass Golden Copy, Cloud Browser for Data Mobility 1.1.13	1.1.13-23045	Current Release - Release Notes Golden Copy	09/01/2024	
02/03/2023	Eyeglass Golden Copy, Cloud Browser for Data Mobility 1.1.12	1.1.12-23021	Current Release - Release Notes Golden Copy	08/03/2024	
09/27/2022	Eyeglass Golden Copy 1.1.11	1.1.11-22177	Current Release - Release Notes Golden Copy	03/27/2024	

03/06/2023	Eyeglass DR, Ransomware Defender, Easy Auditor, Airgap Release 2.5.10	2.5.10-23087	Current Release - Release Notes DR Edition Current Release - Release Notes Ransomware Defender Current Release - Release Notes Easy Auditor Current Release - Release Notes Ransomware Defender AirGap 2.0	09/06/2024	
02/14/2023	Eyeglass DR, Ransomware Defender, Easy Auditor, Airgap Release 2.5.9.1	2.5.9.1-23033	Current Release - Release Notes DR Edition Current Release - Release	08/14/2024	

			Notes Ransomware Defender Current Release - Release Notes Easy Auditor Current Release - Release Notes Ransomware Defender AirGap 2.0		
11/30/2022	Eyeglass DR, Ransomware Defender, Easy Auditor, Enterprise Airgap Release 2.5.9	2.5.9-22231	Current Release - Release Notes DR Edition Current Release - Release Notes Ransomware Defender Current Release - Release Notes Easy	05/30/2024	

			<p>Auditor</p> <p>Current Release - Release Notes ECA</p> <p>Current Release - Release Notes Performance Auditor</p> <p>Current Release - Release Notes AnyCopy</p> <p>Zero Trust API Release Notes</p> <p>Current Release - Release Notes Ransomware Defender AirGap 2.0</p>		
1/25/2022	Eyeglass RHEL installer for 7.x			6/30/2022	
6/17/2022	Eyeglass Golden	1.1.9-22118	Current Release -	12/31/2022	

	Copy 1.1.9-22118		Release Notes Golden Copy		
	Eyeglass DR Edition and Data Protection Suite 2.5.8.1-22116	2.5.8.1-22116	Current Release - Release Notes DR Edition Current Release - Release Notes Ransomware Defender Current Release - Release Notes Easy Auditor Current Release - Release Notes ECA Current Release - Release Notes Performance Auditor Current Release - Release Notes		

			AnyCopy Zero Trust API Release Notes Current Release - Release Notes Ransomware Defender AirGap 2.0		
5/30/2022	Eyeglass DR Edition and Data Protection Suite 2.5.8.1-22100	2.5.8.1-22100	Current Release - Release Notes DR Edition Current Release - Release Notes Ransomware Defender Current Release - Release Notes Easy Auditor Current Release - Release	11/30/2023	

			Notes ECA Current Release - Release Notes Performance Auditor Current Release - Release Notes AnyCopy Zero Trust API Release Notes Current Release - Release Notes Ransomware Defender AirGap 2.0		
4/14/2022	Eyeglass Golden Copy 1.1.7-22085	1.1.7-22085	Current Release - Release Notes Golden Copy	12/31/2022	
4/11/2022	Eyeglass Search & Recover 1.1.8-22082	1.1.8-22082	Current Release - Release Notes Search &	10/11/2023	

			Recover		
4/7/2022	Eyeglass Golden Copy 1.1.7-22076	1.1.7-22076	Current Release - Release Notes Golden Copy	12/31/2022	
4/5/2022	Eyeglass DR Edition and Data Protection Suite 2.5.8.1-22080	2.5.8.1-22080	Current Release - Release Notes DR Edition Current Release - Release Notes Ransomware Defender Current Release - Release Notes Easy Auditor Current Release - Release Notes ECA Current Release - Release Notes Performance Auditor Current	10/5/2023	

			Release - Release Notes AnyCopy		
3/11/2022	Eyeglass Search & Recover 1.1.8-22050	1.1.8-22050	Current Release - Release Notes Search & Recover	9/11/2023	
2/17/2022	Eyeglass Search & Recover 1.1.8-22037	1.1.8-22037	Current Release - Release Notes Search & Recover	12/31/2022	
2/8/2022	Eyeglass DR Edition and Data Protection Suite 2.5.8-22028	2.5.8-22028	Current Release - Release Notes DR Edition Current Release - Release Notes Ransomware Defender Current Release - Release Notes Easy Auditor Current Release -	8/8/2023	

			<p>Release Notes ECA</p> <p>Current Release - Release Notes Performance Auditor</p> <p>Current Release - Release Notes AnyCopy</p>		
2/3/2022	Eyeglass Golden Copy 1.1.6-22019	1.1.6-22019	<p>Current Release - Release Notes Golden Copy</p>	12/31/2022	
12/29/2021	Eyeglass DR Edition and Data Protection Suite 2.5.8-21330	2.5.8-21330	<p>Current Release - Release Notes DR Edition</p> <p>Current Release - Release Notes Ransomware Defender</p> <p>Current Release - Release</p>	6/29/2023	

			Notes Easy Auditor Current Release - Release Notes ECA Current Release - Release Notes Performance Auditor Current Release - Release Notes AnyCopy		
12/29/2021	Eyeglass Golden Copy 1.1.6-21224	1.1.6-21224	Current Release - Release Notes Golden Copy	12/31/2022	
12/22/2021	Eyeglass Search & Recover 1.1.5-21225	1.1.5-21225	Current Release - Release Notes Search & Recover	12/31/2022	
12/17/2021	Eyeglass Golden Copy 1.1.6-21223	1.1.6-21223	Current Release - Release Notes Golden Copy	12/31/2022	

12/16/2021	Eyeglass Search & Recover 1.1.5-21221	1.1.5-21221	Current Release - Release Notes Search & Recover	12/31/2022	
12/15/2021	Eyeglass Search & Recover 1.1.5-21211	1.1.5-21211	Current Release - Release Notes Search & Recover	12/31/2022	
12/15/2021	Eyeglass DR Edition and Data Protection Suite 2.5.8-21306	2.5.8-21306	Current Release - Release Notes DR Edition Current Release - Release Notes Ransomware Defender Current Release - Release Notes Easy Auditor Current Release - Release Notes ECA Current Release -	12/31/2022	

			Release Notes Performance Auditor Current Release - Release Notes AnyCopy		
12/3/2021	Eyeglass Golden Copy 1.1.6-21182	1.1.6-21182	Current Release - Release Notes Golden Copy	12/31/2022	
11/29/2021	Eyeglass Golden Copy 1.1.6-21181	1.1.6-21181	Current Release - Release Notes Golden Copy	2/28/2022	
11/15/2021	Eyeglass DR Edition and Data Protection Suite 2.5.8-21240 - Controlled Availability	2.5.8-21240	Current Release - Release Notes Ransomware Defender AirGap 2.0	12/31/2022	
11/11/2021	Eyeglass Search & Recover 1.1.5-21169	1.1.5-21169	Current Release - Release Notes Search & Recover	12/31/2022	
10/27/2021	Eyeglass Golden	1.1.6-21164	Current Release -	12/31/2022	

	Copy 1.1.6-21164		Release Notes Golden Copy		
10/27/2021	Eyeglass Search & Recover 1.1.5-21163- Controlled Availability	1.1.5-21163	Current Release - Release Notes Search & Recover	12/31/2022	
10/19/2021	Eyeglass DR Edition and Data Protection Suite 2.5.8-21222 - Controlled Availability	2.5.8-21222	Current Release - Release Notes Ransomware Defender AirGap 2.0	12/31/2022	
10/18/2021	Eyeglass Golden Copy 1.1.6-21152	1.1.6-21152	Current Release - Release Notes Golden Copy	12/31/2022	
9/20/2021	Eyeglass Golden Copy 1.1.4-21124	1.1.4-21124	Current Release - Release Notes Golden Copy	12/31/2022	
9/16/2021	Eyeglass Search & Recover 1.1.5-21133- Controlled Availability	1.1.5-21133	Current Release - Release Notes Search & Recover	12/31/2022	

9/7/2021	Eyeglass Golden Copy 1.1.4-21119	1.1.4-21119	Current Release - Release Notes Golden Copy	12/31/2022	
8/24/2021	Eyeglass Ransomware Defender for ECS 2.5.8-21189	2.5.8-21189	Release 2.5.8 Release Notes for Ransomware Defender for ECS	12/31/2022	
8/22/2021	Eyeglass DR Edition and Data Protection Suite 2.5.7.1-21161	2.5.7.1-21161	Current Release - Release Notes DR Edition Current Release - Release Notes Ransomware Defender Current Release - Release Notes Easy Auditor Current Release - Release Notes ECA	12/31/2022	

7/28/2021	Eyeglass Golden Copy 1.1.4-21108	1.1.4-21108	Current Release - Release Notes Golden Copy	12/31/2022	
7/23/2021	Eyeglass DR Edition and Data Protection Suite 2.5.7.1-21140	2.5.7.1-21140	Current Release - Release Notes DR Edition Current Release - Release Notes Ransomware Defender Current Release - Release Notes Easy Auditor Current Release - Release Notes ECA	12/31/2022	
7/23/2021	Eyeglass Performance Auditor 2.5.7.1-21140	2.5.7.1-21140	Current Release - Release Notes Performance Auditor	12/31/2022	

7/21/2021	Eyeglass Golden Copy 1.1.4-21107	1.1.4-21107	Current Release - Release Notes Golden Copy	12/31/2022	
7/16/2021	Eyeglass Golden Copy 1.1.4-21105	1.1.4-21105	Current Release - Release Notes Golden Copy	12/31/2022	
6/24/2021	Eyeglass Golden Copy 1.1.4-21093	1.1.4-21093	Current Release - Release Notes Golden Copy	12/31/2022	
5/29/2021	Eyeglass DR Edition and Data Protection Suite 2.5.7-21096	2.5.7-21096	Current Release - Release Notes DR Edition Current Release - Release Notes Ransomware Defender Current Release - Release Notes Easy Auditor Current	12/31/2022	

			Release - Release Notes ECA		
5/29/2021	Eyeglass Performance Auditor 2.5.7-21096	2.5.7-21096	Current Release - Release Notes Performance Auditor	12/31/2022	
5/29/2021	Eyeglass AnyCopy 2.5.7-21096	2.5.7-21096	Current Release - Release Notes AnyCopy	11/29/2022	
5/3/2021	Eyeglass Golden Copy 1.1.4-21074	1.1.4-21074	Current Release - Release Notes Golden Copy	2/28/2022	
4/19/2021	Eyeglass DR Edition and Data Protection Suite 2.5.7-21081	2.5.7-21081	Current Release - Release Notes DR Edition Current Release - Release Notes Ransomware Defender Current Release - Release	10/19/2022	

			Notes Easy Auditor Current Release - Release Notes ECA		
4/19/2021	Eyeglass Performance Auditor 2.5.7-21081	2.5.7-21081	Current Release - Release Notes Performance Auditor	10/19/2022	
4/19/2021	Eyeglass AnyCopy 2.5.7-21081	2.5.7-21081	Current Release - Release Notes AnyCopy	10/19/2022	
4/8/2021	Eyeglass Golden Copy 1.1.4-21062	1.1.4-21062	Current Release - Release Notes Golden Copy	2/28/2022	
4/5/2021	Eyeglass DR Edition and Data Protection Suite 2.5.7-21068	2.5.7-21068	Current Release - Release Notes DR Edition Current Release - Release Notes Ransomware	10/5/2022	

			Defender Current Release - Release Notes Easy Auditor Current Release - Release Notes ECA		
4/5/2021	Eyeglass Performance Auditor 2.5.7-21068	2.5.7-21068	Current Release - Release Notes Performance Auditor	10/5/2022	
4/5/2021	Eyeglass AnyCopy 2.5.7-21068	2.5.7-21068	Current Release - Release Notes AnyCopy	10/5/2022	
2/2/2021	Eyeglass AnyCopy 2.5.7-20289	2.5.7-20289	Current Release - Release Notes AnyCopy	8/2/2022	
1/11/2021	Eyeglass Golden Copy 1.1.4-21002	1.1.4-21002	Current Release - Release Notes Golden Copy	2/28/2022	
12/2/2020	Eyeglass DR Edition and Data Protection	2.5.6-20263	Current Release - Release	12/2/2021	

	Suite 2.5.6-20263		Notes DR Edition Current Release - Release Notes Ransomware Defender Current Release - Release Notes Easy Auditor Current Release - Release Notes ECA		
12/2/2020	Eyeglass Performance Auditor 2.5.6-20263	2.5.6-20263	Current Release - Release Notes Performance Auditor	12/2/2021	
11/26/2020	Eyeglass DR Edition and Data Protection Suite 2.5.6-20258	2.5.6-20258	Current Release - Release Notes DR Edition Current Release - Release Notes Ransomware	12/2/2021	

			re Defender Current Release - Release Notes Easy Auditor Current Release - Release Notes ECA		
11/17/2020	Eyeglass Golden Copy 1.1.4-20229	1.1.4-20229	Current Release - Release Notes Golden Copy	2/28/2022	
9/29/2020	Eyeglass Golden Copy 1.1.4-20178	1.1.4-20178	Current Release - Release Notes Golden Copy	2/28/2022	
11/11/2020	Eyeglass DR Edition and Data Protection Suite 2.5.6-20158	2.5.6-20158	Current Release - Release Notes DR Edition Current Release - Release Notes Ransomwa re	12/2/2021	

			Defender Current Release - Release Notes Easy Auditor Current Release - Release Notes ECA		
9/2/2020	Eyeglass Golden Copy 1.1.4-20133	1.1.4-20133	Current Release - Release Notes Golden Copy	3/2/2022	
8/13/2020	Eyeglass Golden Copy 1.1.4-20121	1.1.4-20121	Current Release - Release Notes Golden Copy	2/13/2022	
7/27/2020	Eyeglass DR Edition and Data Protection Suite 2.5.6-20084	2.5.6-20084	Current Release - Release Notes DR Edition Current Release - Release Notes Ransomwa re	12/2/2021	

			Defender		
			Current Release - Release Notes Easy Auditor		
			Current Release - Release Notes ECA		
7/27/2020	Eyeglass Performance Auditor 2.5.6-20084	2.5.6-20084	Current Release - Release Notes Performance Auditor		
6/18/2020	Eyeglass Golden Copy 1.1.3-20077	1.1.3-20077	Current Release - Release Notes Golden Copy	12/18/2021	
6/10/2020	Eyeglass DR Edition and Data Protection Suite 2.5.6-20069	2.5.6-20069	Current Release - Release Notes DR Edition Current Release - Release Notes Ransomware	12/2/2021	

			Defender		
			Current Release - Release Notes Easy Auditor		
			Current Release - Release Notes ECA		
6/10/2020	Eyeglass Performance Auditor 2.5.6-20069	2.5.6-20069	Current Release - Release Notes Performance Auditor	12/2/2021	
6/4/2020	Eyeglass Golden Copy 1.1.3-20071	1.1.3-20071	Current Release - Release Notes Golden Copy	12/4/2021	
5/28/2020	Eyeglass DR Edition and Data Protection Suite 2.5.6-20063	2.5.6-20063	Current Release - Release Notes DR Edition Current Release - Release Notes Ransomware	12/2/2021	

			Defender		
			Current Release - Release Notes Easy Auditor		
			Current Release - Release Notes ECA		
5/28/2020	Eyeglass Performance Auditor 2.5.6-20063	2.5.6-20063	Current Release - Release Notes Performance Auditor	12/2/2021	
5/15/2020	Eyeglass Golden Copy 1.1.3-20070	1.1.3-20070	Current Release - Release Notes Golden Copy	11/15/2021	
5/12/2020	Eyeglass DR Edition and Data Protection Suite 2.5.6-20056	2.5.6-20056	Current Release - Release Notes DR Edition Current Release - Release Notes Ransomwa	12/2/2021	

			Defender		
			Current Release - Release Notes Easy Auditor		
			Current Release - Release Notes ECA		
5/12/2020	Eyeglass Performance Auditor 2.5.6-20056	2.5.6-20056	Current Release - Release Notes Performance Auditor	12/2/2021	
2/27/2020	Eyeglass Search & Recover 1.1.2-20024	1.1.2-20024	Current Release - Release Notes Search & Recover	2/1/2022	
2/25/2020	Eyeglass Search & Recover 1.1.2-20012	1.1.2-20012	Current Release - Release Notes Search & Recover	8/25/2021	
2/19/2020	Eyeglass DR Edition and Data Protection Suite 2.5.5-20019	2.5.5-20019	Current Release - Release Notes DR Edition Current	10/1/2020	

			Release - Release Notes Ransomw are Defender		
			Current Release - Release Notes Easy Auditor		
			Current Release - Release Notes ECA		
2/20/2020	Eyeglass Performance Auditor 2.5.6-20022	2.5.6-20022	Current Release - Release Notes Performance Auditor	12/2/2021	
12/23/2019	Eyeglass Search & Recover 1.1.2-19108	1.1.2-19108	Current Release - Release Notes Search & Recover	6/23/2020	
12/11/2019	Eyeglass Search & Recover 1.1.2-19105	1.1.2-19105	Current Release - Release Notes Search & Recover	6/11/2020	
12/6/2019	Eyeglass Search	1.1.2-19104	Current	6/6/2020	

9	& Recover 1.1.2- 19104		Release - Release Notes Search & Recover		
11/12/20 19	Eyeglass DR Edition and Data Protection Suite 2.5.5- 19234	2.5.5-19234	Current Release - Release Notes DR Edition Current Release - Release Notes Ransomwa re Defender Current Release - Release Notes Easy Auditor Current Release - Release Notes ECA	10/1/202 0	
10/23/20 19	Eyeglass DR Edition and Data Protection Suite 2.5.5- 19226	2.5.5-19226	Current Release - Release Notes DR Edition	10/1/202 0	

			Current Release - Release Notes Ransomware Defender		
			Current Release - Release Notes Easy Auditor		
			Current Release - Release Notes ECA		
10/11/2019	Eyeglass DR Edition and Data Protection Suite 2.5.5-19219	2.5.5-19219	Current Release - Release Notes DR Edition Current Release - Release Notes Ransomware Defender	10/1/2020	
			Current Release - Release		

			Notes Easy Auditor		
			Current Release - Release Notes ECA		
9/17/2019	Eyeglass DR Edition and Data Protection Suite 2.5.5-19188	2.5.5-19188	Current Release - Release Notes DR Edition	10/1/2020	
9/10/2019	Eyeglass DR Edition and Data Protection Suite 2.5.5-19184	2.5.5-19184	Current Release - Release Notes DR Edition	10/1/2020	
4/26/2019	Eyeglass Search & Recover 1.1-19042	1.1-19042	Current Release - Release Notes Search & Recover	1/1/2020	
5/10/2019	Eyeglass DR Edition 2.5.4-19106	2.5.4-19106	Current Release - Release Notes DR Edition	3/31/2020	
3/26/2019	Eyeglass Search & Recover 1.0-19033	1.0.0-19033	Current Release - Release Notes Search & Recover	1/1/2020	

3/8/2019	Eyeglass Search & Recover 1.0-19022	1.0.0-19022	Current Release - Release Notes Search & Recover	1/1/2020	
2/22/2019	Eyeglass Search & Recover 1.0-19018	1.0.0-19018	Current Release - Release Notes Search & Recover	1/1/2020	
2/22/2019	Eyeglass DR Edition & Data Protection Suite - 2.5.4-19020	2.5.4-19020	Current Release - Release Notes DR Edition	3/31/2020	
1/31/2019	Eyeglass Search & Recover - 1.0	1.0.0-13	Current Release - Release Notes Search & Recover	1/1/2020	
1/22/2019	DR Edition & Ransomware Defender Patch - 2.5.4-18275	2.5.4-18275 Eyeglass only	Current Release - Release Notes DR Edition Current Release - Release Notes Ransomware Defender	3/31/2020	
11/29/20	Eyeglass DR	2.5.4-18266	Current	3/31/	

18	Edition - Cluster Storage Monitor Only 2.5.4-18266	Cluster Storage Monitor only	Release - Release Notes DR Edition	2020	
10/16/2018	Eyeglass Ransomware Defender Only 2.5.3-18257	2.5.3-18257 ECA only	Current Release - Release Notes Ransomware Defender	12/31/2019	
9/19/2018	Eyeglass Unified Release (DR, Easy Auditor, Ransomware Defender) 2.5.3	2.5.3-18251	Current Release - Release Notes DR Edition Current Release - Release Notes Ransomware Defender Current Release - Release Notes Easy Auditor Current Release - Release Notes ECA	12/31/2019	
9/12/2020	Eyeglass Unified Release (DR,	2.5.2-18080	Release Notes 2.5.2 DR	7/31/2019	

	Easy Auditor,Ransomware Defender) 2.5.2		Edition Release Notes 2.5.2 Easy Auditor Release Notes 2.5.2 Ransomware Defender		
7/15/2019	Eyeglass Unified Release (DR, Easy Auditor,Ransomware Defender) 2.5.1	2.5.1-18013	Release notes Easy Auditor 2.5.1 Release Notes 2.5.1 DR Edition Release Notes 2.5.1 Ransomware Defender	7/31/2019	
	Eyeglass Easy Auditor Only Release 2.5.0	2.5-17282	Release Notes Easy Auditor 2.5.0	7/31/2019	
	2.0.0 DR Edition Only EOL Notice Nov 17, 2018	2.0-17245.run	Release Notes 2.0.0 DR Edition	12/17/2018	

	1.9.6 Ransomware Defender Only EOL Notice March 6, 2018	1.9.6- 17219.run	Release notes Ransomwa re Defender only 1.9.6	3/20/201 8	
	1.9.5 DR Edition EOL Notice March 6, 2018	1.9.5- 17172.run	Performa nce Release with 2x CEE density per VM. Enhanced logging with syslog for faster log collection.	3/20/201 8	
	1.9.4 Ransomware Defender EOL Notice March 6, 2018	1.9.4 17166	Release Notes 1.9.4 Ransomwa re Defender	3/20/201 8	
	1.9.4 DR Edition EOL Notice March 6, 2018	1.9.4 17166	Release Notes 1.9.4 DR Edition	3/20/201 8	
	1.9.3 Ransomware Defender EOL Notice March 6, 2018	1.9.3 17152	Release Notes 1.9.3 Ransomwa re Defender	3/20/201 8	

	1.9.3 DR Edition EOL Notice March 6, 2018	1.9.3 17152	Release Notes 1.9.3 DR Edition	3/20/2018	
	1.9.2 Ransomware Defender EOL Notice March 6, 2018	1.9.2.17114	Release Notes 1.9.2 Ransomware Defender	3/20/2018	
	1.9.2 DR Edition EOL Notice March 6, 2018	1.9.2.17114	Release Notes 1.9.2 DR Edition	3/20/2018	
	1.9.1 Ransomware Defender EOL Notice March 6, 2018	1.9.1-17093	Release Notes 1.9.1 Ransomware Defender Release Notes	3/20/2018	
	1.9.0 DR Edition EOL Notice March 6, 2018		Release Notes 1.9.0 DR Edition Release Notes	3/20/2018	
	1.9.0 Ransomware Defender - EOL Notice March 6, 2018		Release Notes 1.9.0 Ransomware Defender Release Notes	3/20/2018	

	1.8.3 Notice July 31st 2017		Release 1.8.3 Release Notes	10/29/20 17	
	1.8.1 Notice July 31st 2017		Release 1.8.1 Release Notes	10/29/20 17	
	1.8.0 Notice July 31st 2017	eyeglass_ui- 1.8.0-16168 eyeglass_rest- 1.8.0-16168 eyeglass_sca- 1.8.0-16168	Release 1.8.0 Release Notes	10/29/20 17	Dell EMC Open files api bug affects all previous releases of Eyeglass.
	1.7.0 EOL Notice July 31st 2017	eyeglass_ui v1.7.0 r16134 eyeglass_rest v 1.7.0 r16134 eyeglass_sca v 1.7.0 r16134	Release 1.7.0 Release Notes	10/29/20 17	
	1.6.3 EOL Notice May 31st 2017	eyeglass_ui v1.6.3 r16100 eyeglass_rest v1.6.3 r16100 eyeglass_sca v1.6.3 r16100	Eyeglass PowerScal e Edition 1.6.3 Release Notes	7/31/201 7	
	1.6.2 EOL Notice May 31st 2017	eyeglass_ui v1.6.2 r16087 eyeglass_rest v1.6.2 r16087 eyeglass_sca v1.6.2 r16087	Eyeglass PowerScal e Edition 1.6.2 Release Notes	7/31/201 7	
	1.6.1 EOL Notice May 31st 2017	eyeglass_ui v1.6.1 r16084 eyeglass_rest v1.6.0 r16084 eyeglass_sca	Eyeglass PowerScal e Edition 1.6.1 Release	7/31/201 7	

		v1.6.1 r16084	Notes		
	1.6.0 EOL Notice May 31st 2017	eyeglass_ui v1.6.0 r16080 eyeglass_rest v1.6.0 r16080 eyeglass_sca v1.6.0 r16080	Eyeglass PowerScal e Edition 1.6.0 Release Notes	7/31/2017	
	1.5.4 EOL Notice Nov 1st 2017	eyeglass_ui v1.5.4 r16061 eyeglass_rest v1.5.4 r16061 eyeglass_sca v1.5.4 r16061	Eyeglass PowerScal e Edition 1.5.4 Release Notes	1/1/2017	Recommended patch for OneFS 8

© Superna Inc

1.1. Current Release - Release Notes DR Edition

[Home](#) [Top](#)

Release date	Version
11/28/2023	2.6.4-23365

- [What's New in Superna Eyeglass PowerScale Edition Release 2.6.4 for DR \(11/28/2023\)](#)
- [Supported OneFS releases](#)
- [DR Edition Feature Release Compatibility](#)
- [Feature Support Matrix](#)
- [End of Life Notifications](#)
- [New in Superna Eyeglass PowerScale Edition Release 2.6.3 for DR \(09/28/2023\)](#)
- [New in 2.6.3](#)
- [Fixed in 2.6.3](#)
 - [DR-1068 IP pool failover - Not able to select multiple pools](#)
- [New in Superna Eyeglass PowerScale Edition Release 2.6.2 for DR \(09/01/2023\)](#)
- [New in Superna Eyeglass PowerScale Edition Release 2.6.1 for DR \(08/03/2023\)](#)
- [Fixed in 2.6.1](#)
 - [DR-995 Getting Isilon Unsupported Error for 9.5.0.1 Isilon when Upgrade eyeglass from 2.5.9.1 to 2.6.0](#)
- [New in Superna Eyeglass PowerScale Edition Release 2.6.0 for DR \(06/29/2023\)](#)
- [Fixed in 2.6.0](#)
 - [DR-753 Access zone failover 'Block Failover on Warnings' does not block selecting zone in the warning](#)
 - [DR-779 igls app pull-config doesn't migrate failover logs](#)
 - [DR-276 Unwanted shadow trace is created when path picker is opened](#)
 - [DR-780 igls app pull-config for file filters & monitor only setting](#)

- DR-205 Zone Readiness Errors when Provider Instance Name mismatched
- New in Superna Eyeglass PowerScale Edition Release 2.5.12 for DR (05/09/2023)
- Fixed in 2.5.12- 23175
 - DR-770-Access Zone Failover - Fails during Networking Operations
 - DR-817 Robot mount is enabled by default
- Security Updates
 - DR-764 Security updates - READ/WRITE ARBITRARY FILES with script editor
 - DR-766 Add system.xml tag to completely block all script editor functionality by default
 - DR-765 Enforce Role on the server side for eyeglass REST API token routes.
 - DR-542 Exception occurs for redhat installer - 2.5.9-22251-rhel8.run
- What's New in Superna Eyeglass PowerScale Edition Release 2.5.11 (04/03/2023)
- New in 2.5.11- 23110
 - Ease of Use
- What's New in Superna Eyeglass PowerScale Edition Release 2.5.10 (03/06/2023)
- New in 2.5.10-23087
- Fixed in 2.5.10
 - DR-428 Cluster Storage is not displayed in Cluster Storage Usage UI
- What's New In Superna Eyeglass PowerScale Edition Release 2.5.9.1 for DR. (02/14/2023)
- Support Removed in Eyeglass Release 2.5.9
- Deprecation Notices
- What's New in Superna Eyeglass PowerScale Edition Release 2.5.9 (11/30/2022)
- New and Fixed in Eyeglass Release 2.5.9
- Fixed in 2.5.9

- DR-254 Onefs 9.4 Unlock My Files Feature Does Not Work
- DR-286 Issue related to Folder permission in /opt/data
- DR-470 Eyeglass logrotate configuration file eca-syslog-logrotate.conf improperly formatted.
- New in 2.5.8.2
- New in 2.5.8.1-22116
- Fixed in 2.5.8.1-22116
- New in 2.5.8.1-22100
- Fixed in 2.5.8.1-22100
- New in 2.5.8.1-22080
 - T20905 Log Parser
- Fixed in 2.5.8.1-22080
 - T21800 Swap file created on Upgrade
 - T22819 2.5.8 rollback DFS policy when resync prep timed out is incorrect it should not rollback ever
- New/Fixed in 2.5.8-22028
 - T22205 RAM Alarm calculation is now based on the total number of clusters managed
- New in 2.5.8-21330
- Fixed in 2.5.8-21330
- Security
 - T22171 - Log4j Vulnerability - Upgrade to Log4j 2.17.0 (2.5.8-21330 and higher Log4j 2.17.0)
- New in 2.5.8-21306
- NEW - Failover
 - T17849 DNS Dual Delegation Failover Readiness Validation disabled
 - NEW - OneFS 9.3 Support
 - NEW - Cluster Storage Monitor new schedule for quota creation
- Fixed in 2.5.8-21306
- Security

- T22033 Log4j Vulnerability - CVE-2021-44228
- T20584 Eyeglass service account password exposed on error connecting to Powerscale
- Failover / Configuration Replication
 - T20628 Cannot disable Zone/IP Pool Readiness AD Delegation Validation (2.5.7.1 and higher)
 - T16888 Configuration Replication fails if the SynclQ Policy source and target path are different and the SynclQ policy path contains a special character
- Features
 - T9652 Unlock My Files inconsistent handling for unreachable PowerScale cluster
- General
 - T19288 Custom Postfix email settings not restored
 - T19275 Syslog alarm forwarding configuration not restored
- Technical Advisories
- Known Issues
- Failover
 - 2666/2723: Problems for Controlled Failover when Source becomes unreachable during failover
 - 2278: Zone Readiness lists Access Zone after all related SynclQ Policies are deleted
 - 2919: Eyeglass Configuration Replication Jobs may not display in the Zone Readiness Eyeglass Configuration Replication Readiness list
 - 3010: Unexpected results for failover where the total number of objects exceeds the published limit
 - 3029: Zone Readiness not calculated correctly for SynclQ subnet pool with a mapping hint
 - 3031: Zone Readiness Policy Path Containment Check results in extra errors
 - 3077: Zone Readiness does not catch pool mapping hint misconfiguration for partial string match
 - T477: No Policy Hot/Hot Validation Error for policy with no share/export

- T482: Zone Readiness shows OK for multiple Smartconnect Zone Mapping errors
- T654: Zone Readiness incorrectly includes SynclQ Policy in System Access Zone
- T1712: Zone Readiness missing Zone when the pool has no SmartConnect Zone - OneFS 7
- T1716: Eyeglass Runbook Robot NFS mount not functioning for RHEL and Centos deployments
- T1482: Zone Readiness SynclQ Readiness not updated after Access Zone associated to a pool
- T3742: No Policy Hostname Validation error if SynclQ Policy Target Host is fully qualified and uses a short name on the target cluster pool that has a Superna Eyeglass mapping hint applied
- T3848: SPNs not updated during failover for OneFS8 non-default groupnet AD provider
- T4009: SPNs creation case sensitive to AD provider name
- T4320: Access Zone not assigned to any Subnet Pools results in many Zone Readiness Errors
- T4316: Runbook Robot Policy Job does not display SynclQ Job Reports
- T4857: Failed SmartConnect Zone Rename step is not displayed in Failover Log
- T4878: Pool Failover - Non Runbook Robot SynclQ policies can be mapped to Robot pool
- T4968: Zone missing from DR Dashboard Zone Readiness tab if a SynclQ Policy has a target host that cannot be resolved
- T5092, T4490: Access Zone Pre and Post Failover Scripting Issues
- T5473: Zone/Pool Readiness Pool Mapping Hint Matching Issue
- T5961: Failover Log shows Incorrect Final Steps
- T5897: Post Failover Inventory step may fail during multiple concurrent failovers
- T5941: Pool Failover Failover Log Summary incorrectly displayed Client Redirection step not run

- T5967: Failover where Quota Sync is disabled has extra lines in Failover Log
- T5934: Access Zone Readiness shows OK for DFS only failed over Access Zone
- T6289: SynclQ policy with no shares or exports is associated with the System Access Zone for failover
- T6311: Selecting the DR Failover Status link on the DR Assistant Summary page may result in an Error
- T6402: Access Zone Failover Post Failover Inventory step runs multiple times
- T6842: Zone Readiness: Zone does not display Failover Over state for Access Zones where custom SmartConnect Zone prefix is being used
- T7184: Pool Readiness: Pool to SynclQ Policy Mapping is not displayed in DR Dashboard until Readiness task is run
- T8824: User Quota creation fails on failover for multiple disjointed AD Domain environment
- T10363 Overlapping Access Zone Failover blocked for System Access Zone
- T10912 Quota Sync fails for quotas where quota container property set to true
- T10935 Pool failover "failovertarget" must be "zone id"
- T7622 Eyeglass will not add custom SPNs if PowerScale Cluster does not return any missing SPN during SPN check (as of 2.5.6)
- T13360 Failover Readiness Validation for Corrupt Failover Snapshots does not check for missing snapshot
- T12434 Concurrent Access Zone or Pool Failover with DFS configured policies may fail DFS share rename step
- T13701 Failover option "Disable SynclQ Jobs on Failover Target" does not reapply schedule
- T13726 Pool Failover error mapping policy to pool on target cluster for disabled job
- T13881 Cannot failover overlapping Access Zones - rel 2.5.6
- T14398 Zone/Pool Failover Readiness FQDN Alias validation incorrectly reports OK when the pool does not have an ignore the hint

- T14931 Policies configured for Pool failover allowed to do DFS or SyncIQ failover until next configuration replication runs
- T14948 Failover log for Uncontrolled Access Zone incorrectly logs status of final readiness job and changes to pool aliases
- T14965 Failover readinessSyncIQ File Pattern Validation has a WARNING state instead of an ERROR
- T14971 DR Assistant validation check screen incorrectly requests acknowledgement of readiness warnings
- T14974 Access Zone Failover with error on DFS share renaming will abort for all policies
- T14988 Eyeglass GUI incorrectly allows pool failover configuration for a policy that is active in failover rehearsal mode
- T15000 DR Rehearsal status lost if fingerprint file deleted
- T15042 REST API policy readiness is missing output for the Target Reachability check
- T15010 DR Rehearsal Revert not blocked for Pool Failover mode when in REHEARSAL_ERROR
- T15609 Alarm time not updated for repeated policy/dfs/zone/ pool readiness alarms
- T15191 Failover Log may show 2 summaries when Rehearsal Mode enabled
- T15192 Rehearsal Mode not disabled for Access Zone associated with Pool Failover
- T15248 Error in DFS failover does not rollback share renaming when failover job includes multiple policies
- T15260 DFS Failover share renaming rollback not done when all share rename fails on source cluster
- T15271 Zone/Pool Failover error in SMB Data Integrity step or run policy step incorrectly attempts to roll back networking
- T15278 Pool Failover job with multiple pools stops failover steps for all pools on DFS share renaming error
- T15290 Pool Failover job with multiple pools does not rollback client redirection when allow writes step fails

- T15298 Quota job run manually after failover may delete quotas on source cluster
- T15530 Policy or DFS Readiness may incorrectly evaluate Policy Hostname validation in error
- T15547 Failover Readiness Domain Mark Validation fails for path with spaces or special characters
- T15610 Policy Readiness Pool Mapping Validation alarm and email indicate Warning severity instead of Error
- T15613 DR Rehearsal Readiness - no alarm or email when DR Rehearsal status changes from OK to Warning or Error
- T15623 REST API - Pool Failover API does not support multiple pool selection
- T15624 REST API - Failover API does not block controlled failover when source cluster unreachable
- T15769 DNS Dual Delegation Validation does not work where NS Record does not resolve directly to an SSIP
- T16154 DR Rehearsal mode issues where source and target path are different
- T17136 Zone Readiness incorrectly shows Error when Access Zone Name, Smartconnect Zone Name and IP Pool name are exactly the same
- T17401 Pool Readiness not displayed with no configured/reachable DNS
- T17477 DFS share suffix not applied for failover or configuration replication
- T17428 REST API - Policy Readiness returns incorrect Access Zone
- T17447 OneFS 9.0 and 9.1 Readiness Validation for Policy Source Nodes Restriction always shows INFO
- T17555 Blank display for Zone or Pool Readiness
- T17731 Policies missing in DR Assistant for Zone or Pool failover
- T17732 Multiple Zone Readiness Jobs
- T18127 DNS Dual Delegation uses wrong SSIP when IP Pool Service Subnet different from the pool subnet
- T18392, T19226 DFS Failover produces extra "null" failover log
- T18779 Overlapping Powerscale cluster and SynclQ Policy names can result in incorrect Failover Readiness assessment

- T18969 Runbook Robot Job in Jobs window disappears when target cluster is unreachable
- T19186 Policy Readiness not updated
- T19553 Zone/Pool Readiness never completes
- T19967 Pool / Zone Readiness does not indicate whether there is a disabled Configuration Replication job in the Zone
- T20181 Policy Hostname Validation Incorrectly show Error
- T21443 Quota failover error when source and target path are different and contain a \$
- T21629 DR Readiness does not indicate source cluster unavailable
- T21750 Deleting SynclQ Policy when Rehearsal Mode is active leaves configuration behind
- T22269 Python Pre and Post Failover Scripts do not work on OpenSUSE 15.3
- T22567 Quota Inventory causes problems during failover
- T21929 igls-original SPN may not be deleted on failover
- Configuration Replication
 - 1683: Export sync where source is 7.1.1.x and target 8.x.x.x
 - 649: Export sync where source and target path on each cluster is different is deleted and recreated in each config cycle (affects onefs 7 to 8 or 8 to 7 replication)
 - 1462 - Export max_file_size cannot be replicated
 - 1355: Edit Job configuration to include share/export deselected from another Job causes share/export to be reselected.
 - 1580: Delete and Create export within same replication cycle orphans deleted export on the target with OneFS 7.1.1.x
 - 1625: Custom QUOTA Jobs require extra replication cycle to be deleted
 - 1639: Able to manually Run Now disabled Custom Job
 - 1641: Custom Job does not include shares/export when source or destination path configured with a trailing /
 - 1788: Delete of unlinked user quota on source may not delete matching quota on the target

- 1789: Able to select shares/exports/quotas outside job path after deselected
- 1887, T3727: Multiple SynclQ policies associated with same Zone will result in transient error on Eyeglass Zone replication creation
- 1924: Quotas on excluded SynclQ directory are selected for replication
- 1998: Custom Eyeglass configuration replication Job does not have an associated Zone replication Job
- 2004: Custom Quota Job is incorrectly listed in the Failover: Quota Failover (RUN MANUALLY) section in the Jobs window
- 2007: Job error after deleting quota
- 2038: Create alias results in temporary error
- 2043: Configuration replication job has error after zone is deleted
- 2045: Edit Configuration for Custom Job has multiple source cluster selected where Eyeglass is managing more than 2 clusters
- 2046: Job Edit Configuration view has the wrong parent selected
- 2049: Delete Zone does not delete associated configuration items on target for custom Jobs and auto jobs with disabled zone Job
- 2235: Eyeglass replication Job does not complete when source cluster becomes unreachable after Job has started
- 2060: Access Zone Replication Error - Error on creation of shared resource
- 2488: Inconsistent behaviour in Run Now for Disabled Jobs
- 1938: Issues with Eyeglass Configuration Replication Jobs after the Access Zone is deleted
- 2308: In EyeGlass, NFS alias health is always 'unknown'
- 2804: Disabled SynclQ Policy is not initially displayed as Policy Disabled in Eyeglass
- T676: Eyeglass Zone replication Job does not replicate all authentication providers for OneFS 8.0
- T723: Job shows OK when there is an Access Eyeglass Zone Replication Error
- T771: Edit Configuration does not show parent node selected

- T805: Eyeglass Configuration Replication Jobs not updated when IP address changed on Source Cluster
- T593: Eyeglass errors for multiple exports with the same path
- T1792: Eyeglass does not auto-detect PowerScale version changes and may use incorrect API version for Configuration Replication
- T1851: Eyeglass Configuration Replication Jobs not removed when there is no SynclQ privilege for the eyeglass service account
- T2193 - Export max_file_size setting not replicated correctly
- T2757: Access Zone is not replicated from OneFS 8 to OneFS 7.2
- T1976 - Eyeglass Jobs Window Edit Configuration does not show related Snapshot Schedules
- T2920: Access Zone Authentication Provider is not replicated to the target cluster
- T3629: Renamed Snapshot Schedule leaves original Snapshot Schedule on the target
- T14803 Set Job Type AUTOSKIPCONFIG does not create associated jobs until configuration replication runs
- T15258 Unable to create Custom Job
- T15321 DFS share name custom suffix may be doubled
- T15884 Some scenarios in networking API failures during Configuration Replication may not block deletes
- T16965 Audit does not consider differences on source and target for SMB share property inheritable_path_acl
- T18812/T23433 Error replicating SMB Share with Run as Root permission
- T19026 Data Config Migration Preview incorrectly shows quotas selected
- T19177 NFS modify properties which are not client list fails with unresolvable host
- T19894 NFS Export replication in DR Test Access Zone incorrectly identifies that update is required
- T20301 User Disabled AUTOSKIPCONFIG job becomes enabled after a rediscover or if policy renamed

- T20369 Configuration Replication Error after running DR Rehearsal failover on SynclQ policy where source and target path are different and contain special characters and or spaces
- T21375 Snapshot schedule replication error on update
- T22875 Configuration Replication audit step incorrect error when path contains a comma
- Features
 - 1138: Eyeglass UI does not block configuration of duplicate remote logging service
 - 2224: Eyeglass Cluster Configuration Report runs when Cluster is unreachable
 - 2061: Access Zone name for Directory Migration is case sensitive
 - 2882: Phone Home Email Disabled
 - 3037: Configure Remote Logging Services in Eyeglass requires manual steps
 - T1515: Eyeglass Shell feature not functioning for RHEL and Centos deployments
 - T3119: Access Zone Migration Preview does not always display Configuration information
 - T3170: Quota Requests History shows Status of Error for processed requests after failover
 - T4280: User Storage View may show all quotas instead of only the User Quotas
 - T4329: DR Test Status does not open
 - T4432: DR Test Mode action on multiple policies do not display in Running Jobs
 - T4968: SynclQ Job Report Troubleshooting section missing information when report is generated on demand
 - T5173: Quota Modification Request window does not close after Submit
 - T8834: Storage Monitor Report missing user information when friendly name cannot be resolved
 - T9561: Unlock my files incorrectly displays directories

- T11807 Alarm for quota synchronization error does not contain error details
- T12307 Cluster Storage Usage may be incomplete
- T13390 DR Testing (Disaster Recovery Testing) Job initially always in User Disabled state
- T14956 No Recovery when DR Test Mode in Entering DR Testing or Exiting DR Testing
- T14962 DR Test Mode Configuration Replication step does not run configuration replication for the DR Test mode job itself
- T15215 Data Config (Zone) Migration Job can not be created where Migration or Destination Path contains special characters
- T15311 Data Config (Zone) Migration Job fails for existing policy when "Migrate only configuration" is checked
- T17535 Quota Search - Display of quota count on modify may not be correct
- T17739 Cannot create quota template for less than 1 GB
- T18148 Incorrect Error Message for unreachable Powerscale cluster when breaking lock
- T19464 AD Group Template incorrectly creates quota on share where user permission is explicitly defined
- T20183 Unlock My Files does not display results if there is a Powerscale node that does not respond
- T22209 igls adv ADGroupThresholds does not scan
- T22622 Active Directory Managed Quotas fails with LDAP configured for retrieving user and groups
- General
 - 924: Inventory View shows + beside component when there are no more children
 - T17694: API token download of CMDB file is blocked by desktop login
 - 943: Inventory View not auto-refreshed
 - 1612,T11989: Some alarms not cleared
 - 2155: Access Zone Networking info does not display in Inventory View
 - 2628/T15193: Job Definitions window does not sort properly

- 2895: Inventory SPN View is truncated
- 2366: EyeGlass does not support special characters in email recipient address
- 2385: Refresh Now does not refresh the Failover History window
- 2744: Failed to Retrieve Inventory Alarm missing information
- 2978: Syslog Log Viewer freezes Eyeglass web page
- T971: Eyeglass End User Interface Tree View Expanders do not collapse
- T1514: Eyeglass Archive cannot be downloaded when Eyeglass is deployed on Redhat or Centos
- T3137 - Eyeglass daily backup not working for RHEL/CentOS Deployments
- T4596: Log Viewer cannot fetch logs
- T12370 Network Visualization does not display Pool Readiness
- T12373 Cluster Storage Window Empty
- T15310 REST API / Widgets creates empty html file
- T15493 Extraneous Post Failover placeholder scripts
- T15511 Historical failover logs may lose formatting after a backup & restore
- T15647 igls app report issues
- T17530 Backup and Restore does not properly set location/permission for Eyeglass log files
- T18000 Quota limit reached on Eyeglass appliance eca logs directory does not have an alarm
- T18983 Multiple licenses applied to same Powerscale cluster
- T19208 Too many open files
- T19276 Configuration file for enhanced HA for misconfigured/unavailable DNS not restored with --anyrelease option
- T19280 Eyeglass services do not start if retrieval of banned file list on startup hangs
- T19523 After anyrelease restore or rediscover quota jobs for main and mirror policy are both enabled
- T19572 Alarms History missing on new 2.5.7 15.2 deployments

- T20371 API error on OneFS 9.x for retrieving DNS settings
- T20407 igls app report error for OneFS 9.2
- T21275 Deleted Powerscale cannot be readded
- T20808 Alarms window info column does not display full text
- T21820 DR Edition - Manage Services window Eyeglass services status does not display CPU and RAM usage info
- T19213 Eyeglass RAM Alarm inconsistent notification
- T21060 Alarms without info cannot be cleared
- T23072 Eyeglass RAM alarm for concurrent user login does not clear
- T23052, T23065, T23066 Log Parser Report Download links not working
- T23043 Restrictions in Log Parser customer name
- T23113 Log Parser does not show link for report when appliance id contains a slash (/)
- T23009 Log parser permission may not be added to admin role on upgrade
- T23328 igls app report errors
- T23161 Upgrade to 2.5.8.1 from 2.5.8.1 earlier build fails
- DR-896 Runbook Robot Options on GUI were exposed in the 2.5.12 release
- DR-1247 All SMB sessions-login, sg, roboaudit don't work on OneFS's Secure hashing algorithms
- DEVSECOPS-258 `libzyp` rpm` bug causes installers to fail
- Known Limitations
- Known Limitations for PowerScale OneFS 8.0.0.x with Eyeglass
 - T507 Cluster Report for OneFS 8.0 missing information
- Known Limitations for Eyeglass Failover
 - T939 Eyeglass Access Zone Replication Job in Error after failover
 - T1785 Cannot set ignore flag on subnet pool after failback
 - T2479: Access Zone Failover fails between OneFS 7.2 clusters if Eyeglass also managing OneFS 7.1
 - T3258: Cannot start failover while Eyeglass initial inventory is running

- T3774: Failover relies on policy naming: <policy name> and <policy name_mirror>
- T4808: SPNs not updated for new authentication providers after Access Zone settings changed to “Use all authentication providers” (OneFS 7.2)
- T6229: Existing Failover Logs cannot be reviewed after upgrade to Eyeglass R2.0
- T14321 Zone/Pool Failover Readiness for AD Delegation validation, SPN Readiness validation not supported for Multi-Site failover configuration
- T15611 Pool Readiness Alarms are reported per Zone
- DNS Dual Delegation Failover Readiness Validation Supported DNS servers
- DNS Dual Delegation Failover Readiness validation uses PowerScale GroupNet DNS server
- T17254 Failover does not take into account Powerscale job retries
- T18556 User Quota Replication requires System Access Zone AD Provider
- T19681 Runbook Robot NFS Export not created on target cluster
- Known Limitations for Eyeglass Configuration Replication
 - Multi-Path Exports
 - T1359 Update NFS Multi-Path Export path(s) may cause transient Configuration Replication Error
 - T1359 Update NFS Multi-Path Export path(s) may cause transient Configuration Replication Error
 - T1743 Multiple export with same path and same client do not show Configuration Replication Error
 - T1847 OneFS 8 Overlapping Access Zone Replication has error
 - T1972 Snapshot schedule replicated with offset
 - T2241 Incorrect missing SPN alarm issued when PowerScale cluster joined to multiple Domains
 - T2779 - Eyeglass Configuration Replication “Full Sync Mode” always updates when Default Settings on Source and Target cluster are not the same
 - T2780 Same host moved to different NFS Export Client list not updated on target

- T2908 New Eyeglass Configuration Replication Job cannot recover state and mode from the Eyeglass Fingerprint file.
- T4289 Delete Share or Export may result in temporary Audit error
- T5972 No Error Message for Duplicate NFS Export on OneFS 7.2 Configuration Replication Failed
- T14936 Short SPN not created during Configuration Replication
- T17097 Eyeglass Configuration Replication direction follows Enable/Disable state of SynclQ policies
- Known Limitations for Eyeglass Features
 - T2350: Quota Self Serve Portal: Local Group Quotas not displayed when logged in with Local Group User
 - T1962: Default Role incorrectly shows Delete option
 - T8362: Cluster Storage Monitor AD Group Template Quota Creation does not respect highest quota setting user quota in nested AD Groups
 - T8193: special characters in Cluster storage monitor AD managed quota templates is not supported
 - T9622: Unlock My Files! does not indicate error when PowerScale node is not reachable
 - T15139 Data Config Migration Concurrent Jobs Limitation
 - DR-136 Login with AD users leads to read-only Eyeglass
- Known Limitations for Eyeglass General
 - T2289 Backup Archive Job is not always displayed in the Running Jobs window
 - T2908 Renamed SynclQ Policy does not link to RPO Reports from original SynclQ Policy Name
 - T3170 Pending Quota Requests are not preserved on failover
 - T4579 Upgrade from 1.5.4 to 1.9 and greater Failover History retrieves Failover Log for SynclQ Job Reports
 - T6300 After an Eyeglass restore with the -anyrelease option the print screen functionality for SynclQ Job Reports and Eyeglass backups may be in error

- T12034 Eyeglass appliance rediscover does not preserve Eyeglass Job state unless Configuration Replication has run
- T16137 Anyrelease restore does not restore all Ransomware Defender and Easy Auditor settings
- T16729 Role Based Access Control (RBAC) Known Limitations
- T16821 anyrelease restore restrictions for restore to 2.5.7
- Eyeglass Upgrade requires disk usage < 80%
- T19368 Copy to Clipboard Size Limitation
- Known Limitations for REST API
 - T18079 REST API - Change Eyeglass Configuration Job Disable/Enable must be done at the same time as Job Type Change
- REST API retrieval of Jobs Known Limitation

What's New in Superna Eyeglass PowerScale Edition Release 2.6.4 for DR (11/28/2023)

Supported OneFS releases

8.2.0.x

8.2.1.x

8.2.2.x

9.0

9.1

9.2.x

9.3

9.4 via the February RUP 9.4.0.12 (PSP-3079) released Feb 8th 2023

9.4.0.14

9.5.x.x (minimum version 9.5.0.1)

9.5.0.5

DR Edition Feature Release Compatibility

Feature	Source Cluster Release	Target SyncIQ Cluster Release
Configuration Replication non-DFS mode		
Configuration Replication	8.2.x.x	8.2.x.x**
Configuration Replication	9.0	9.0
Configuration Replication	9.1	9.1
Configuration Replication	9.2	9.2
Configuration Replication	9.3	9.3
Configuration Replication	9.4	9.4
Configuration Replication	9.5	9.5
Configuration Replication DFS mode		
Configuration Replication - DFS Mode	8.2.x.x	8.2.x.x
Configuration Replication - DFS Mode	9.0	9.0
Configuration Replication - DFS Mode	9.1	9.1
Configuration Replication - DFS Mode	9.2	9.2
Configuration Replication - DFS Mode	9.3	9.3
Configuration Replication - DFS Mode	9.4	9.4
Configuration Replication - DFS Mode	9.5	9.5

SyncIQ Policy Failover non-DFS mode		
SyncIQ Policy Failover	8.2.x.x	8.2.x.x
SyncIQ Policy Failover	9.0	9.0
SyncIQ Policy Failover	9.1	9.1
SyncIQ Policy Failover	9.2	9.2
SyncIQ Policy Failover	9.3	9.3
SyncIQ Policy Failover	9.4	9.4
SyncIQ Policy Failover	9.5	9.5
SyncIQ Policy Failover DFS mode		
SyncIQ Policy Failover - DFS mode	8.2.x.x	8.2.x.x
SyncIQ Policy Failover - DFS mode	9.0	9.0
SyncIQ Policy Failover - DFS mode	9.1	9.1
SyncIQ Policy Failover - DFS mode	9.2	9.2
SyncIQ Policy Failover - DFS mode	9.3	9.3
SyncIQ Policy Failover - DFS mode	9.4	9.4
SyncIQ Policy Failover - DFS mode	9.5	9.5
Access Zone Failover		
Access Zone Failover	8.2.x.x	8.2.x.x
Access Zone Failover	9.0	9.0
Access Zone Failover	9.1	9.1
Access Zone Failover	9.2	9.2
Access Zone Failover	9.3	9.3
Access Zone Failover	9.4	9.4
Access Zone Failover	9.4	9.5
Runbook Robot cluster pairs SyncIQ Policy Failover		
SyncIQ Policy Failover	8.2.x.x	8.2.x.x
SyncIQ Policy Failover	9.0	9.0
SyncIQ Policy Failover	9.1	9.1
SyncIQ Policy Failover	9.2	9.2
SyncIQ Policy Failover	9.3	9.3

SyncIQ Policy Failover	9.4	9.4
SyncIQ Policy Failover	9.5	9.5
Runbook Robot* cluster pairs		
Access Zone Failover		
Access Zone Failover	8.2.x.x	8.2.x.x
Access Zone Failover	9.0	9.0
Access Zone Failover	9.1	9.1
Access Zone Failover	9.2	9.2
Access Zone Failover	9.3	9.3
Access Zone Failover	9.4	9.4
Access Zone Failover	9.5	9.5
Data Config Migration		
Data Config Migration	9.0	9.0
Data Config Migration	9.1	9.1
Data Config Migration	9.2	9.2
Data Config Migration	9.3	9.3
Data Config Migration	9.4	9.4
Data Config Migration	9.5	9.5
Live Ops - DR Test Mode		
Live Ops DR Test Mode	9.0	9.0
Live Ops DR Test Mode	9.1	9.1
Snapshot Schedules	9.0	9.0
Snapshot Schedules	9.1	9.1
Snapshot Schedules	9.2	9.2
Snapshot Schedules	9.3	9.3
Dedupe Path Settings	8.0.x.x	8.0.x.x
Dedupe Path Settings	8.2.x.x	8.2.x.x - pending testing

**** Inter-version capabilities: In the case of inter-version operation, the capabilities of the lower OneFS API version will be applied across both OneFS versions. Capabilities of the higher OneFS version that are not present in the lower OneFS version will not be available.**

Feature Support Matrix

Description	Supported
Overlapping Access Zone with System (/ifs)	
Configuration Replication (non DFS mode)	Yes - Create / Update No - Delete
Configuration Replication (DFS mode)	Yes - Create / Update No - Delete
SyncIQ Failover	Yes
SyncIQ Failover - DFS Mode	Yes
Access Zone Failover	No
Overlapping Access Zone - non System Zones	
Configuration Replication (non DFS mode)	Yes - shares/export / alias No-Access Zone
Configuration Replication (DFS mode)	Yes No - Access Zone
SyncIQ Failover	Yes
SyncIQ Failover - DFS Mode	Yes
Access Zone Failover	No
Runbook Robot Access Zone Multi cluster	No (only cluster pairs with no common cluster)
Failover with SyncIQ Encryption (Access Zone, SyncIQ, DFS, IP pool failover modes)	Yes (8.2 or later only)

End of Life Notifications

End of Life Notifications for all products are available [here](#).

New in Superna Eyeglass PowerScale Edition Release 2.6.3 for DR (09/28/2023)

New in 2.6.3

For What's new in DR [see here](#).

1. Eyeglass UI Enhancements: Appliance ID Copy Button, Appliance OS Version Display.
2. DR Test Mode: Writable Snapshots.
3. Pool Failover: Multiple Pool Selection.
4. Quota Failover: Quotas not Removed from the Source.
5. SupernaOne Support: Filter on AirGap Alarms.

Fixed in 2.6.3

DR-1068 IP pool failover - Not able to select multiple pools

The DR Assistant show no info when trying to initiate IP pool failover for two IP pools, one with igls-ignore and the other with normal igls-hint.

New in Superna Eyeglass PowerScale Edition Release 2.6.2 for DR (09/01/2023)

New in Superna Eyeglass PowerScale Edition Release 2.6.1 for DR (08/03/2023)

Fixed in 2.6.1

**DR-995 Getting Isilon Unsupported Error for 9.5.0.1 Isilon
when Upgrade eyeglass from 2.5.9.1 to 2.6.0**

Getting Isilon Unsupported popup for 9.5.0.1 Isilon when Upgrade eyeglass from 2.5.9.1 to 2.6.0

Before the upgrade in `data/system.xml` and `conf/system.xml`, we have

```
<onefs>
  <latestSupportedVersion>9.4.0</latestSupportedVersion>
</onefs>
```

After the upgrade, we change the value in `conf/system.xml` to

```
<onefs>
  <latestSupportedVersion>9.5.0</latestSupportedVersion>
</onefs>
```

But in `data/system.xml`, we still have 9.4.0 - that's why we get the notice

Workaround:

1. Modify

in `/opt/superna/sca/data/system.xml` from `<latestSupportedVersion>9.4.0</latestSupportedVersion>` to `<latestSupportedVersion>9.5.0</latestSupportedVersion>`

2. `systemctl restart sca`

New in Superna Eyeglass PowerScale Edition Release 2.6.0 for DR (06/29/2023)

Fixed in 2.6.0

DR-753 Access zone failover 'Block Failover on Warnings'
does not block selecting zone in the warning

Blocked warning in the failover option

DR-779 igls app pull-config doesn't migrate failover logs

Failover history is empty on the new Eyeglass appliance after using the restore command: `igls app pull-config`.

It doesn't migrate old failover logs.

DR-276 Unwanted shadow trace is created when path picker is opened

When creating a Writable Snapshot, path picker will leave some shadows on the screen; This does not affect the overall functionality

DR-780 igls app pull-config for file filters & monitor only setting

The custom values for file filters & monitor-only settings are not displayed after `igls app pull-config` it's applied.

But the custom value exists in the file `ransomwareMonitorOnlySettings.json`.

DR-205 Zone Readiness Errors when Provider Instance Name mismatched

When an active directory provider with a provider instance name that doesn't match the actual active directory name has been added to an access zone, the Zone Readiness assessment in eyeglass will show:

- warning in SPN Readiness: Zone does not have any registered SPNs.
- AD Delegation Validation: SPN step shows error: Error processing SPNS: Unable to find domain controller for <provider instance name>

Workaround: remove the active directory provider from the Isilon, and re-add it without an instance provider name so that the name from the AD instance proper gets automatically used.

New in Superna Eyeglass PowerScale Edition Release 2.5.12 for DR (05/09/2023)

Fixed in 2.5.12-23175

DR-770-Access Zone Failover - Fails during Networking Operations

Access Zone Failover - Fails during Networking Operations

DR-817 Robot mount is enabled by default

This function has been disabled by default for several years, but it appears to be defaulting to enabled as of this release.

The impact of this being enabled by default is that any customer that upgrades to 2.5.11 will have a robot job that will start failing.

Security Updates

DR-764 Security updates - READ/WRITE ARBITRARY FILES with script editor

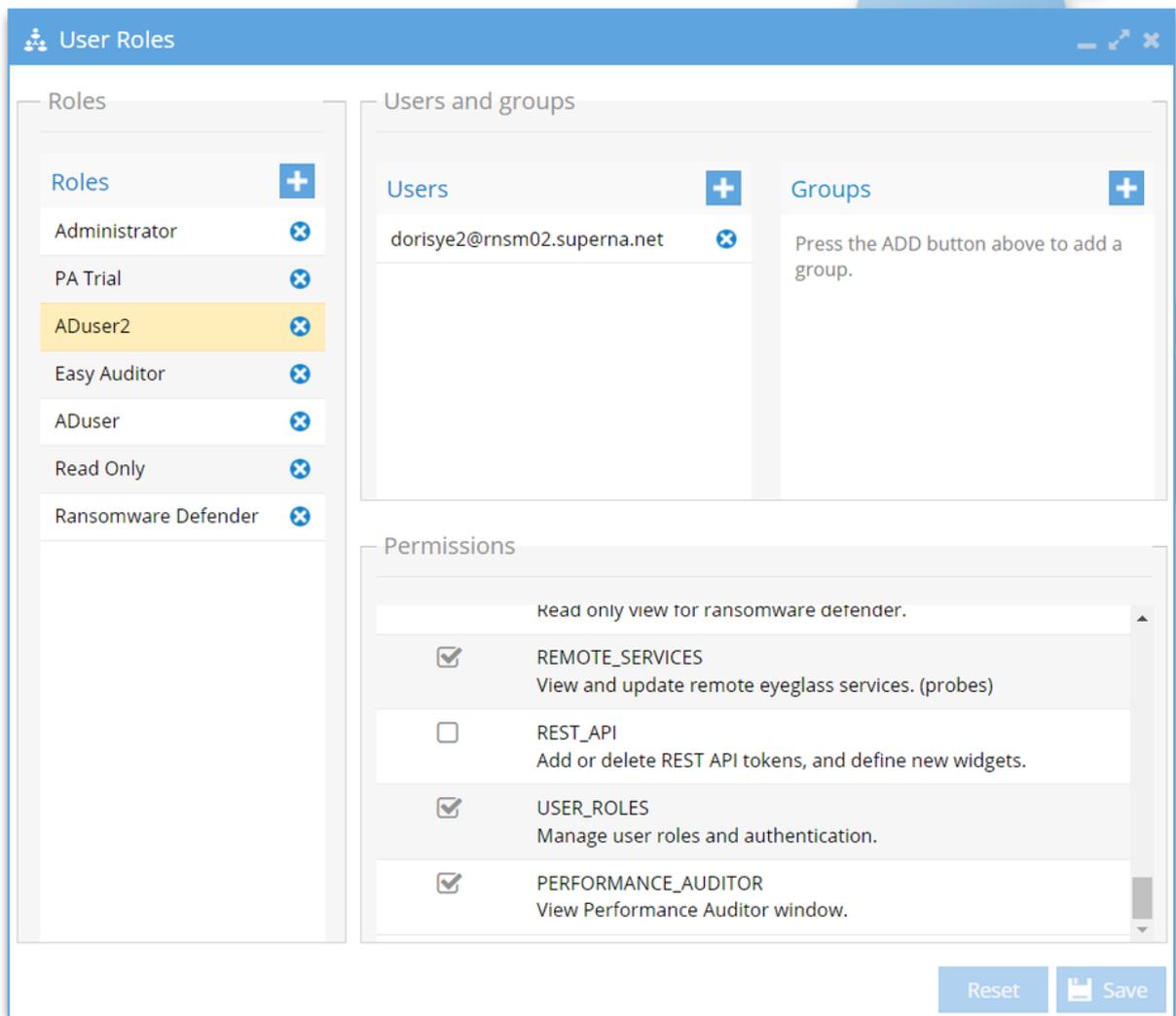
Script editor tool allows execution of OS scripts in context of the system SCA user that runs the eyeglass processes. The potential exist for this to be used to execute arbitrary OS level commands. Scripts are not required for failover with eyeglass and this allows custom logic to be leveraged. Upon upgrade the script editor will be disabled blocking access to scripting. An administrator must enable this logic if it is required. See DR-766.

DR-766 Add system.xml tag to completely block all script editor functionality by default

The `system.xml` tag that will block all server-side functionality was added.

DR-765 Enforce Role on the server side for eyeglass REST API token routes.

A new permission was created that must be granted to a user to allow use of API tokens. This is an explicit permission that must be granted. See the new role below in User Roles.



DR-542 Exception occurs for redhat installer - 2.5.9-22251-rhel8.run

Exception occurs when run ./eyeglass-2.5.9-22251-rhel8.run

What's New in Superna Eyeglass PowerScale Edition Release 2.5.11 (04/03/2023)

New in 2.5.11-23110

Ease of Use

More than one access zone can now be selected from the UI when starting an access zone failover from the DR Assistant.

What's New in Superna Eyeglass PowerScale Edition Release 2.5.10 (03/06/2023)

New in 2.5.10-23087

Refer to previous 2.5.9.1 builds for what's new.

Fixed in 2.5.10

DR-428 Cluster Storage is not displayed in Cluster Storage Usage UI

Cluster Storage info is not displayed in Cluster Storage Usage UI. Toggle between Cluster Storage and Cluster hardware tab no of times, and it shows up sometimes.

What's New In Superna Eyeglass PowerScale Edition Release 2.5.9.1 for DR. (02/14/2023)

1. Zookeeper in restart loop due to 'Unable to load database on disk' was fixed
2. A new popup warning displays if a user adds an Isilon cluster with a OneFS version that's higher than what the current software version

Support Removed in Eyeglass Release 2.5.9

No features removed

Deprecation Notices

Currently no deprecation notices.

What's New in Superna Eyeglass PowerScale Edition Release 2.5.9 (11/30/2022)

New and Fixed in Eyeglass Release 2.5.9

Fixed in 2.5.9

DR-254 Onefs 9.4 Unlock My Files Feature Does Not Work

The unlock my files feature does not work with OneFS version 9.4 or higher due to a deprecated command on OneFS.

Workaround: None available.

DR-286 Issue related to Folder permission in /opt/data

The on-site log parser is not working; The RPO reports and the airgap job (isilon) reports may not work.

Workaround: Run the following commands to the eyeglass appliance:

```
chown sca:users /opt/data/log_reports
```

```
chown sca:users /opt/data/airgap_reports
```

```
chown sca:users /opt/data/syncIQ_reports
```

DR-470 Eyeglass logrotate configuration file eca-syslog-logrotate.conf improperly formatted.

Eyeglass 2.5.9 GA introduced a badly formatted eca-syslog-logrotate.conf file that includes illegal windows indent characters, and an improperly formatted `dateformat` rule which subsequently crashes logrotate.

This will lead to log directories filling up on Eyeglass, preventing us from seeing new ECA logs for health checks, and could cause Eyeglass disk exhaustion issues.

We require a fix that removes the bad windows characters and a proper `dateformat` rule which includes a space between `dateformat` and the preceding dash to allow logrotate to start successfully.

Reproduced on: Eyeglass DR

Superna Version (Reported): 2.5.9-22231

Superna Version (Occurred): 2.5.9-22231

Expected behavior: Logrotate is engaged on the hour and rotates logs successfully

Actual behavior: Logrotate crashes due to bad format in eca-syslog-logrotate.conf, preventing rotation of necessary log files.

New in 2.5.8.2

1. Deprecated Feature notification
 - a. DR Test mode 6-month notice on deprecation. This feature was temporary until writeable snapshots were available. No enhancements to this feature with the end of support in the next 6 months.
 - b. Replacement solution:
 - i. Onefs 9.3 or later
 - ii. Feature Overview: On-demand DR testing with copy-on-first write writeable snapshots enable a new workflow that is faster, consumes less storage and is available on demand.

- iii. The selection of an IP pool with no access zone attached will allow a temporary access zone created for the DR test. A source path of data is selected to test with and a snapshot is created on this path. A new access zone is automatically created and attached to the IP pool and all shares, exports and quotas are cloned into the temporary access zone.
- iv. A writable snapshot is created in the temporary access zone
- v. Testing can begin in seconds and only consume space for writing.
- vi. The test completes and option to clean up the temporary access zone.

2. Cluster Usage Icon

- a. This feature will be deprecated with many options to get disk utilization on the cluster. This functionality will be deprecated.

3. SNMP alarm forwarding

- a. This is a legacy protocol and will be removed from the product. syslog, webhooks, email, rest api should be used for alarm forwarding.

New in 2.5.8.1-22116

Refer to previous 2.5.8.1 builds for what's new.

Fixed in 2.5.8.1-22116

Refer to previous 2.5.8.1 builds for what's new.

New in 2.5.8.1-22100

Refer to previous 2.5.8.1 builds for what's new.

Fixed in 2.5.8.1-22100

Refer to previous 2.5.8.1 builds for what's new.

New in 2.5.8.1-22080

T20905 Log Parser

Log Parser functionality is now available from the Eyeglass desktop that can be used to generate detailed log parsing analysis of DR Edition, Ransomware Defender, Easy Auditor. More information can be found in the documentation [here](#).

Fixed in 2.5.8.1-22080

T21800 Swap file created on Upgrade

Unnecessary swap file created on the upgrade on OpenSUSE 15.3 impacts available disk space.

Resolution: Upgrade to 2.5.8.1 on OpenSUSE 15.3 no longer creates the unnecessary swap file. Note that if the swap file already exists, the upgrade will not remove it.

T22819 2.5.8 rollback DFS policy when resync prep timed out is incorrect it should not rollback ever

If the resync prep step times out or fails, a DFS mode failover will roll back SMB share renames when it should not. Rollback should only execute with allowed writes failures.

Resolution: Rollback only executes on allow writes failure. The failover log now shows the rollback step properly for resync prep failure: Rollback Renaming Shares - was skipped because failover succeeded or proceeded far enough to be successful

New/Fixed in 2.5.8-22028

T22205 RAM Alarm calculation is now based on the total number of clusters managed

In previous releases, RAM Alarm limits were applied per cluster. Now they are applied against all clusters managed. For example, if there is a limit of 5000 objects managed and 2 clusters are managed each with 3000 objects, the alarm will apply.

New in 2.5.8-21330

Refer to previous 2.5.8 builds for what's new.

Fixed in 2.5.8-21330

Security

T22171 - Log4j Vulnerability - Upgrade to Log4j 2.17.0
(2.5.8-21330 and higher Log4j 2.17.0)

New in 2.5.8-21306

NEW - see What's New in 2.5.8 [here](#).

NEW - Failover

T17849 DNS Dual Delegation Failover Readiness

Validation disabled

Access Zone / IP Pool Failover Readiness Validation for DNS Dual Delegation is now disabled by default. Verify DNS Dual Delegation manually. In a future release, this validation is planned to be provided on demand.

NEW - OneFS 9.3 Support

Support for OneFS 9.3 is introduced in release 2.5.8

NEW - Cluster Storage Monitor new schedule for quota creation

If using the Cluster Storage Monitor AD Group template for creating quotas, they are now assessed and created on the quota collection schedule instead of on the Configuration Replication cycle.

Fixed in 2.5.8-21306

Security

T22033 Log4j Vulnerability - CVE-2021-44228

Resolution: log4j version has been updated to 2.15.0, which has a patch for the vulnerability.

T20584 Eyeglass service account password exposed on error connecting to Powerscale

In the case where there is an error connecting to the Powerscale, for example, a timeout or session expired, the eyeglass service account password appears in plain text in the error log and /var/log/messages files.

Resolution: Eyeglass service account password no longer is exposed.

Failover / Configuration Replication

T20628 Cannot disable Zone/IP Pool Readiness AD Delegation Validation (2.5.7.1 and higher)

In 2.5.7.1 and higher, when the AD Delegation validation is disabled the AD Delegation validation steps continue to run. The Zone / Pool Readiness GUI correctly does not show the validation and any error that occurs is not rolled up to the overall readiness status but an alarm is sent related to the failed step. This does not impact the ability to failover.

Resolution: Validation steps no longer run if the validation is disabled.

T16888 Configuration Replication fails if the SynclQ Policy source and target path are different and the SynclQ policy path contains a special character

For the case where a SynclQ Policy path contains a special character and the SynclQ Policy source and target path are different, configuration replication fails for the associated Eyeglass job with the AEC code AEC_NOT_FOUND.

Resolution: The configuration Replication job is now able to replicate shares and exports where SynclQ policy has a different source and target path, and the path has a special character.

Features

T9652 Unlock My Files inconsistent handling for unreachable PowerScale cluster

For the case where Eyeglass is managing multiple clusters and one or more clusters are unreachable, the Unlock My Files sometimes displays the error "Failed ot search:", "Communication failure or timeout searching for open files. Please try again later or try to be more specific in your query.". without displaying results for reachable cluster or may provide results for reachable clusters without providing the error.

Resolution: Unlock My File now requires the selection of one cluster at a time for searching.

General

T19288 Custom Postfix email settings not restored

After a backup and restore, custom Postfix email settings are not restored.

Resolution: Backup and restore now restores custom Postfix email settings.

T19275 Syslog alarm forwarding configuration not restored

After a backup and restore, Syslog alarm forwarding settings are not restored.

Resolution: Backup and restore now restores Syslog alarm forwarding settings are restored with a backup created as of 2.5.8. Backups created in previous versions do not contain the file and the Syslog alarm forwarding configuration will need to be manually backed up from the original Eyeglass appliance off the appliance.

Technical Advisories

Technical Advisories for all products are available [here](#).

Known Issues

Failover

T22819 2.5.8 rollback DFS policy when resync prep timed out is incorrect it should not rollback ever

If resync prep step times out or fails, a DFS mode failover will roll back SMB share renames when it should not. Rollback should only execute with allowed writes failures.

Workaround: rename the shares on the DR cluster and remove the igls-dfs prefix and apply the igls-dfs on the source cluster SMB shares related to the synciq policy SBM shares that are named as rolled back.

2666/2723: Problems for Controlled Failover when Source becomes unreachable during failover

In a Controlled Failover where the requirement is that the Source cluster is reachable, should the Source cluster become unreachable during the failover an error will occur on the failover job but it is possible that no failover log will be generated.

If the Source becomes unreachable after Failover Wizard validation but before the Failover starts, a log is generated with 1 line that states a success. The Running Jobs window has no details

Workaround: None available

2278: Zone Readiness lists Access Zone after all related SynclQ Policies are deleted

For the case where an Access Zone initially had associated SynclQ Policies and then all SynclQ Policies are deleted, the Access Zone will incorrectly appear in the Zone Readiness view with a Status of UNKNOWN.

Workaround: None required. This entry can be ignored.

2919: Eyeglass Configuration Replication Jobs may not display in the Zone Readiness Eyeglass Configuration Replication Readiness list

If an Eyeglass Configuration Replication Job has no associated shares, exports, alias or quotas, the Job will not be displayed under Eyeglass Configuration Replication Readiness if the SynclQ OneFS Readiness is WARNING.

Workaround: None Required. Failover will run all logic and policies as expected.

3010: Unexpected results for failover where the total number of objects exceeds the published limit

Running an Eyeglass assisted failover where the total number of objects exceeds the published maximum limit will lead to unexpected results.

Workaround: Review published limits and do not use Eyeglass assisted failover if your system exceeds the published limit.

Please refer to the Eyeglass Admin Guide for published limits [here](#).

3029: Zone Readiness not calculated correctly for SyncIQ subnet pool with a mapping hint

The subnet: pool which is provisioned against SyncIQ Policies for the Restrict Source Nodes option, requires an igls-ignore hint for Access Zone Failover to prevent the networking in the pool from becoming failed over during an Access Zone Failover. If there is an Eyeglass igls- mapping hint assigned to these subnets: pool which could result in the networking being failed over Zone Readiness, either does not show an error OR it may show the error that mapping is incomplete.

Workaround: Only configure igls-ignore hint on subnet: pool that is provisioned against SyncIQ policy for the Restrict Source Nodes option.

3031: Zone Readiness Policy Path Containment Check results in extra errors

Zone Readiness for an Access Zone which does not meet SyncIQ Policy path requirement "SyncIQ Policy(s) source root directory must be at or below the Access Zone Base Directory" may in errors for every validation category, with the message "Cannot calculate Access Zone Failover Readiness for a zone with no pools".

Workaround: To resolve the error, ensure that the Policy Path Containment Requirement is met.

Eyeglass Assisted Access Zone Failover Requirements are documented in the Access Zone Failover Guide [here](#).

3077: Zone Readiness does not catch pool mapping hint misconfiguration for partial string match

Zone Readiness: Smartconnect Zone Failover Mapping Readiness validation does not detect a pool mapping error when there is a partial string match. For example:

cluster A Smartconnect Zone Mapping Hint = igls-pool

cluster B Smartconnect Zone Mapping Hint = igls-pool1

Readiness check from A to B does not detect the error. Readiness check from B to A shows an error that no mapping is available.

Workaround:

- Ensure that your Smartconnect Zone Mapping Hints are identical for mapped pools

T477: No Policy Hot/Hot Validation Error for policy with no share/export

Zone Readiness incorrectly shows Policy Hot/Hot Validation as OK in an environment where there are one or more policies in the Access Zone which do not have any file sharing objects (shares or exports).

Workaround: Add a file sharing object under the SyncIQ Policy path.

T482: Zone Readiness shows OK for multiple Smartconnect Zone Mapping errors

In the case where Smartconnect Zone Mapping contains many errors, such as multiple hints or a combination of hint and igls-ignore on both clusters, the mapping error may only show for one of the clusters instead of both clusters.

Workaround: Provision Smartconnect Zone Mapping according to requirements documented [here](#).

T654: Zone Readiness incorrectly includes SyncIQ Policy in System Access Zone

For the case where a SynclQ Policy source path corresponds to a non-System Access Zone path (path is at or below the Access Zone path) but there is a share protected by that policy in the System Access Zone, the SynclQ Policy incorrectly is evaluated for Zone Readiness in the System Access Zone.

Workaround: None required. This policy can be ignored in the System Access Zone as in this configuration, the System Access Zone cannot be failed over.

T1712: Zone Readiness missing Zone when the pool has no SmartConnect Zone - OneFS 7

In OneFS 7, When a subnet pool is associated with an Access Zone and does not have a Smartconnect Zone, the Access Zone is not displayed in Eyeglass Zone Readiness window. With OneFS 8, there is an entry in Zone Readiness with an appropriate error.

Workaround: Create SmartConnect Zone for the pools associated with the Access Zone that you want to failover.

T1716: Eyeglass Runbook Robot NFS mount not functioning for RHEL and Centos deployments

If Eyeglass is deployed on a Redhat or Centos operating system, the Eyeglass Runbook Robot pre and post-failover check for file system read/write by making an NFS mount does not work.

Workaround: Disable the Runbook Robot mount step by setting it to false following the instructions here: <http://documentation.superna.net/eyeglass-PowerScale-edition/igls-administration/eyeglass-administration-guide#TOC-Runbook-Robot-Mount-Export-Enable-Disable>

Manually check the read/write status of the filesystem.

T1482: Zone Readiness SynclQ Readiness not updated after Access Zone associated to a pool

For the case where initially an Access Zone with a policy is not associated with a pool, the policy appears in Zone Readiness/SynclQ Readiness under the System Access Zone. Once the Access Zone is associated with the pool the Policy remains associated with the System Access Zone.

Workaround: None Available. This is a display issue, and the policy will failover if the access zone it is a member of is failed over.

T3742: No Policy Hostname Validation error if SynclQ Policy Target Host is fully qualified and uses a short name on the target cluster pool that has a Superna Eyeglass mapping hint applied

If the pool on the target cluster which contains the SmartConnect Zone, which is configured on the source cluster as the SynclQ policy target host, is configured as a “short” name instead of a fully qualified name AND that pool has a Superna Eyeglass mapping hint defined instead of the required igls-ignore hint, Zone Readiness INCORRECTLY does not show an error.

Workaround: Use a fully qualified domain name for SynclQ Policy target host and in the pool SmartConnect Zone name.

T3848: SPNs not updated during failover for OneFS8 non-default groupnet AD provider

For the case where OneFS 8 is configured with multiple groupnet and different AD provider between groupnets, the SPN update during failover does not succeed for non-default groupnet AD providers. SPN are not deleted for source cluster and are not

created for the target cluster. The failover log indicates success. This is due to a OneFS8 defect with multiple AD providers and isi commands.

SPN delete / create for the AD provider defined in groupnet0 is successful.

Workaround: Manually delete and create the SPN for the Smartconnect Zones that were moved from AD ADSI Edit interface.

T4009: SPNs creation case sensitive to AD provider name

If you have domain name in lowercase but smartconnect zone name has upper case domain name then in that case Eyeglass does not add the SPN Host automatically .

Workaround: AD provider name and AD provider in SmartConnect Zone name should have same case.

T4320: Access Zone not assigned to any Subnet Pools results in many Zone Readiness Errors

Zone Readiness error for an Access Zone that is not assigned to any Subnet Pool has multiple rows displayed in the DR Dashboard - 1 per Subnet Pool on the PowerScale Cluster.

Workaround: Associate the Access Zone with at least 1 Subnet pool.

T4316: Runbook Robot Policy Job does not display SynclQ Job Reports

Runbook Robot job creates 2 failover history records - one for policy failover or access zone failover and one for for Runbook Robot. The Runbook Robot SynclQ Reports log incorrectly repeats the Failover log information instead of showing the associated SynclQ Job reports.

Workaround: View the associated Policy or Access Zone Failover results to retrieve the SyncIQ Job Reports.

T4857: Failed SmartConnect Zone Rename step is not displayed in Failover Log

Access Zone Failover which fails at the SmartConnect Zone rename step shows a Major Error in the “Networking updates during failover Job” section of the Failover Log but does not show the actual rename step which failed.

INFO Raised alarm: MAJOR Access Zone Failover Job failed.

```
ERROR ***** Networking updates during failover Job FAILED *****
```

Workaround: Contact Support to assist in determining the rename operation which caused the error.

T4878: Pool Failover - Non Runbook Robot SyncIQ policies can be mapped to Robot pool

Pool failover is not supported for Runbook Robot but pool readiness SyncIQ policy mapping does not block user from mapping a non-Runbook Robot policy to the Runbook Robot pool. This configuration will cause an error during the Runbook Robot job.

Workaround: Do not configure Pool Failover for the Eyeglass Runbook Robot Access Zone.

T4968: Zone missing from DR Dashboard Zone Readiness tab if a SyncIQ Policy has a target host that cannot be resolved

When an Access Zone contains a SynclQ Policy which has a Target Host configured which cannot be resolved by Eyeglass, the Access Zone does not appear in the DR Dashboard Zone Readiness tab.

Workaround: Ensure that all SynclQ Policy Target Host can be resolved by Eyeglass. To verify, ssh to the Eyeglass appliance and test with nslookup <target host> to confirm that it can be resolved.

T5092, T4490: Access Zone Pre and Post Failover Scripting Issues

- There is no specific option to create Pre or Post Failover scripts for a Pool Failover. If there are existing Pre or Post Failover scripts for Access Zone failover those same scripts will be run during pool failover.
- In a multi-pool setup, the failover log may report an error related to executing the post failover script even though the script succeeds.
- Running the Test run script, for Access Zone Failover, Test Run script only shows "loading" status

Workaround: Ensure that any Access zone failover scripts also apply to pool failover if both are configured. Verify manually whether a script has succeeded.

T5473: Zone/Pool Readiness Pool Mapping Hint Matching Issue

Readiness logic to determine whether 2 pools are mapped for Access Zone or Pool failover will map based on partial match instead of an exact match. For example a pool with the mapping hint "igls-8" on the source will match any mapping hint on the target that begins with "igls-8" - for example, "igls-8a", "igls-8b", "igls-8c" etc. This may cause an issue if there are multiple pools on target side which match. It will also cause an issue after failover as the target hint (for example "igls-8a") will not match the source hint (for example "igls-8").

Workaround: When provisioning pool mapping hints, use unique string that do not overlap between pools - for example, igls-1, igls-2, igls-3 instead of igls-1, igls-1a, igls-1b.

T5961: Failover Log shows Incorrect Final Steps

The Failover log always contains following Final steps even when not required:

1. Networking Rollback Steps are incorrectly displayed at end of failover for a failover where Networking Client Redirection steps were not executed.
2. Transfer pool mapping step are incorrectly displayed for non-pool based failovers.

Workaround: In the above conditions these messages can be ignored as they do not apply.

T5897: Post Failover Inventory step may fail during multiple concurrent failovers

When multiple failovers are initiated in parallel and running concurrently the Post Failover Inventory step may fail if the same step is running for one of the concurrent failovers. This leaves the failover in a Failed state.

Workaround: None Required. This step will be completed successfully on a subsequent failover or during regular Configuration Replication to bring the Eyeglass up to date on the latest state of the PowerScale environment. The Failover log must be consulted to determine state of other failover steps such as Client Redirection, Make Writeable and Preparation for Failback.

T5941: Pool Failover Failover Log Summary incorrectly displayed Client Redirection step not run

For Pool Failover, the Failover Log Summary displays the Client Redirection step as not having run:

Client Redirect : This step did not run

When the step in fact did run.

Workaround: Check this section in the Failover Log to determine the status of the Client Redirection steps:

```
INFO ***** Networking updates during failover Job STARTED *****
```

T5967: Failover where Quota Sync is disabled has extra lines in Failover Log

The Failover Log for a failover where Quota Sync is disabled displays the following line multiple times instead of just once:

```
PLEASE RUN QUOTA FAILOVER JOBS MANUALLY
```

Workaround: None Required.

T5934: Access Zone Readiness shows OK for DFS only failed over Access Zone

Zone Readiness status for Access Zone, which only has DFS policies, will show OK as the overall status for the failed over direction instead of Failed Over status.

Workaround: Check which cluster has enabled SynclQ Policies and verify that another cluster is read-only to confirm which failover direction is active.

T6289: SynclQ policy with no shares or exports is associated with the System Access Zone for failover

A SynclQ policy which does not have any associated shares or exports at or underneath the policy path will be associated with the System Access Zone for Access Zone or Pool Failover instead of the Access Zone that the SynclQ policy falls at or under.

Workaround: Create a file-sharing object at or underneath the SynclQ Policy path and in the Access Zone under which the SynclQ Policy falls.

T6311: Selecting the DR Failover Status link on the DR Assistant Summary page may result in an Error

Selecting the DR Failover Status to link on the DR Assistant may result in the following error: No policy data has been provided, and cannot execute the request.

This error does not block the failover from proceeding.

Workaround: Open the DR Dashboard and review the DR Failover Status [here](#).

T6402: Access Zone Failover Post Failover Inventory step runs multiple times

When an Access Zone contains multiple SynclQ Policies and those policies have been configured in Eyeglass for different Job types (DFS or AUTOSKIPCONFIG), the failover Post Failover Inventory runs for each Eyeglass Job type in the Access Zone instead of just once.

Workaround: None Required. While this increases the failover time to include completion of multiple post failover inventories, the critical failover steps for client redirection, make writeable and preparation for failback are completed prior to this step.

These steps are required to complete in order to place a new mirror policy into the corresponding DFS or AUTOSKIPCONFIG state.

T6842: Zone Readiness: Zone does not display Failover Over state for Access Zones where custom SmartConnect Zone prefix is being used

For Eyeglass deployments where the SmartConnect Zone prefix used to disable SmartConnect Zones on failover has been customized to not use the default igls-original prefix the DR Dashboard does not display Failed Over status for the inactive Access Zone failover direction.

Workaround: None Required.

1. This is a display issue only and does not block failover.
2. This issue does not affect SmartConnect Zone rename during failover.
3. While the DR Assistant allows you to select a failover in the wrong direction (inactive -> active) it is blocked further along in the Failover Wizard due to no enabled policies.

T7184: Pool Readiness: Pool to SynclQ Policy Mapping is not displayed in DR Dashboard until Readiness task is run

Pool to SynclQ Policy mapping is not displayed in DR Dashboard Pool Readiness view until a Zone / Pool Failover Readiness task has been run.

Workaround: None Required. This is a display issue only - the mapping is successfully saved and displayed after the next readiness task has run.

T8824: User Quota creation fails on failover for multiple disjointed AD Domain environment

In an PowerScale environment that is configured to use multiple AD Domains and those Domains are not joined, user quota creation for the quotas related to the non-default AD Domain will fail with the error:

Requested persona was not of user or group type

Workaround: None available with Eyeglass.

T10363 Overlapping Access Zone Failover blocked for System Access Zone

For the case where there are multiple access zones overlapping with System Access Zone on /ifs path, DR Assistant will show an error during navigation indicating an invalid configuration and block completion of failover.

Workaround: SynclQ Policy failover with manual client redirection.

T10912 Quota Sync fails for quotas where quota container property set to true

Smartquotas in OneFS configured with the container property set to true fail to be created by quota sync.

Workaround: None available. Quota must be created manually.

T10935 Pool failover "failovertarget" must be "zone id"

The "failovertarget" field must be "zone id" even though the description indicates "ID of the access zone OR synclQ policy to failover".

Workaround: Enter "zone id" for "failovertarget" when initiating pool failover.

T7622 Eyeglass will not add custom SPNs if PowerScale Cluster does not return any missing SPN during SPN check (as of 2.5.6)

As of 2.5.6 Eyeglass can manage custom SPN creation based on Eyeglass configuration - additional information available [here](#). If PowerScale does not identify any missing SPNs Eyeglass Configuration Replication will not insert custom SPNs. If PowerScale identifies any missing SPN, Eyeglass will insert all custom SPN even if PowerScale does not identify it as missing.

Workaround: SPNs to be added manually if required. For failover, no additional steps - failover will manage all SPN updates based on custom SPN definition.

T13360 Failover Readiness Validation for Corrupt Failover Snapshots does not check for missing snapshot

There must be one failover snapshot on the target cluster per SynclQ policy being failed over. The Corrupt Failover Snapshots validation does not check whether that snapshot is missing. Impact: Allow Writes step of failover will fail.

Workaround: Verify presence of snapshot manually on target cluster

```
isi snapshot snapshots list | grep <SynclQ Policy Name>
```

Replacing SynclQ Policy Name iwth your our SynclQ Policy Name

example for expected configuration

```
isi snapshot snapshots list | grep policy1
```

```
12345 SIQ-Failover-policy1-2020-05025_21-33-37 /ifs/data/policy1
```

T12434 Concurrent Access Zone or Pool Failover with DFS configured policies may fail DFS share rename step

When doing concurrent Access Zone or Pool Failover where the Access Zone or Pool have associated jobs in Eyeglass DFS mode the share renaming step may happen in parallel and depending on the OneFS release an PowerScale OneFS API defect may incorrectly handle the request causing the share rename to be in error.

Workaround: Verify with Dell EMC support whether your OneFS version has this issue. For any shares where share renaming fails they will have to be renamed manually - the failover log will indicate which failed and which succeeded.

T13701 Failover option "Disable SyncIQ Jobs on Failover Target" does not reapply schedule

When the failover option "Disable SyncIQ Jobs on Failover Target" is selected the synciq policy schedule is not reapplied to the active synciq policy on the target cluster.

Workaround: The original SyncIQ policy schedule is captured in the failover log. Reapply the schedule to the policy manually on the PowerScale.

T13726 Pool Failover error mapping policy to pool on target cluster for disabled job

If Pool Failover is initiated and there is an associated Eyeglass Configuration Replication job that is disabled, the failover correctly skips failover of the associated synciq policy/data but incorrectly attempts to associate the mirror policy to a pool on the target cluster resulting in an error for the step "Transfer pool mapping" with message "Could not find policy".

Workaround: None required failover has been completed successfully for policies which were enabled. No impact on failback.

T13881 Cannot failover overlapping Access Zones - rel 2.5.6

In Release 2.5.6, overlapping Access Zones cannot be failed over. The network updates that are done during failover are rolled back.

Workaround: Use Release 2.5.5 to failover overlapping access zones

T14398 Zone/Pool Failover Readiness FQDN Alias validation incorrectly reports OK when the pool does not have an ignore the hint

For cases where PowerScale cluster has been provisioned in Eyeglass using FQDN, that FQDN should not be failed over during Zone or Pool failover - it needs to remain associated with its current cluster. This is achieved by configuring the associated IP pool to be "ignored" during failover. The validation that checks whether this configuration is in place incorrectly indicates OK when the "ignore" is not configured.

Note that Eyeglass 2.5.3 and higher, clusters are no longer being added to Eyeglass using FQDN due to PowerScale CSRF not being compatible with Smartconnect and API services.

Workaround: If cluster is still added to Eyeglass using FQDN modify to be added using IP. Please follow [Technical Advisory #17](#) and [Technical Advisory #22](#).

T14931 Policies configured for Pool failover allowed to do DFS or SyncIQ failover until next configuration replication runs

Policies configured for pool failover are blocked from being failed over in DFS or SyncIQ mode except for the period of time between when pool-to-policy mapping for Pool Failover has been completed and the next Configuration Replication cycle has been completed.

Workaround: None required - Do not initiate DFS or SyncIQ mode failover for policies configured for pool failover. Next scheduled Configuration Replication job will rectify and

after that point, the DFS and SynclQ failover mode will not be available for policies configured for Pool Failover.

T14948 Failover log for Uncontrolled Access Zone incorrectly logs status of final readiness job and changes to pool aliases

The failover log for an uncontrolled Access Zone failover will incorrectly report the status of the final failover readiness step as SUCCESS instead of error and will incorrectly summarize the Pool aliases on source after failover and Pool aliases on destination after failover at the end of the log.

Workaround: None required, this is a logging issue only. The failover correctly logs client redirection steps in the Networking updates section of the log which records the changes as they are being executed. The failover readiness status can be viewed on the DR Dashboard / Zone Readiness.

T14965 Failover readiness SynclQ File Pattern Validation has a WARNING state instead of an ERROR

Failover readiness SynclQ File Pattern Validation which detects that SynclQ policy has file patterns, should be ERROR instead of WARNING as PowerScale OneFS Resync Prep function prepares you for failback will fail when SynclQ is configured this way.

Workaround: This setting should not be used for DR purposes.

T14971 DR Assistant validation check screen incorrectly requests acknowledgement of readiness warnings

For cases where the DR Failover status is OK or Info, the DR Assistant Failover wizard validation check step requests acknowledgement that warnings have been reviewed even though the DR failover status has no warning status.

Workaround: Close the DR Assistant window and open the DR Dashboard window and confirm that, indeed failover status has no Warning states. If so, start the failover again and now select the "I have reviewed the warning status" check box and continue with the failover.

T14974 Access Zone Failover with error on DFS share renaming will abort for all policies

For the case where an Access Zone has both DFS and non-DFS configured jobs in Eyeglass, if share renaming fails for all shares associated with a DFS policy, Client redirection will be considered an error for non-DFS policies as well and failover will be aborted instead of continuing for non-DFS configured jobs.

Workaround: The share renaming issue should be resolved before re-attempting the failover.

T14988 Eyeglass GUI incorrectly allows pool failover configuration for a policy that is active in failover rehearsal mode

From the Eyeglass DR Dashboard, you are allowed to map a policy for pool failover when it is in active rehearsal mode, even though you cannot initiate a failover when it is in this state.

Workaround: Review policy status and confirm not in rehearsal mode before configuring pool failover.

T15000 DR Rehearsal status lost if fingerprint file deleted

A fingerprint file is used to persist the DR Rehearsal status. If the fingerprint file is deleted or otherwise removed while rehearsal mode is active, rehearsal status is lost and there is no way to revert to rehearsal mode.

Workaround: Please contact support at support.superna.net to recover from this state.

T15042 REST API policy readiness is missing output for the Target Reachability check

The SynclQ policy readiness retrieved using REST API is missing the output for the Target Reachability check. If the Target Reachability validation fails, the overall Failover Status is correctly in ERROR and failover cannot be initiated

Workaround:

- To assess target reachability:
 - Target reachability alarms related to Inventory or Configuration replication would have been sent.
 - From the Eyeglass web interface, Eyeglass / PowerScale reachability can be viewed from the Continuous Operation Dashboard.
 - All failover readiness criteria can be viewed from the Eyeglass web interface DR Dashboard.
-

T15010 DR Rehearsal Revert not blocked for Pool Failover mode when in REHEARSAL_ERROR

If after enabling DR Rehearsal mode for Pool Failover, the DR failover status is REHEARSAL_ERROR, the failover wizard incorrectly allows you to initiate a revert for rehearsal mode.

Workaround: To recover from this REHEARSAL_ERROR open a support ticket at support.superna.net for assistance.

T15609 Alarm time not updated for repeated policy/dfs/zone/ pool readiness alarms

If a policy, dfs, zone or pool readiness alarm occurs multiple times, the Alarm time will not be updated with each occurrence. It will display only the first time the alarm is raised. Email notification also only sent on initial occurrence of the alarm. Subsequent occurrences will not send an email.

Workaround: Open the DR Dashboard to see the current state of the validations as of the last time the Zone/Pool Readiness job has run.

T15191 Failover Log may show 2 summaries when Rehearsal Mode enabled

When Rehearsal Mode is enabled for an Access which has DFS policies or enabled with multiple pools which also have DFS, the failover log summary shows an interim summary after data access steps and a final summary at end.

Workaround: None required - summary has required information.

T15192 Rehearsal Mode not disabled for Access Zone associated with Pool Failover

From the DR Dashboard, the Access Zone associated with a Pool Failover already active in Rehearsal Mode can be selected for enabling Access zone Rehearsal Mode again even though this is not a valid configuration for Rehearsal Mode.

Workaround: None Required, the next window in DR Assistant identifies the invalid configuration and correctly blocks Rehearsal Mode enabling for the Access Zone.

T15248 Error in DFS failover does not rollback share renaming when failover job includes multiple policies

A DFS failover which contains multiple policies will not rollback share renaming for a policy that encounters an error if the remaining policies succeed.

Workaround: Use PowerScale interface to remove and add igls-dfs prefix for affected shares.

T15260 DFS Failover share renaming rollback not done when all share rename fails on source cluster

If the client redirection step of failover which adds igls-dfs prefix to shares on the source cluster fails for all of the shares associated with the source cluster the failover stops but the share renaming that completed successfully for the target cluster is not rolled back.

Workaround: Use PowerScale interface to add igls-dfs prefix to shares on the target cluster.

T15271 Zone/Pool Failover error in SMB Data Integrity step or run policy step incorrectly attempts to roll back networking

If the initial share lockout for SMB Data Integrity step fails or run policy step fails, the failover is aborted as expected but then steps are executed to roll back networking changes even though none were made. There is no impact other than error in failover log as these commands fail as they are attempting to update to configuration that already exists on the cluster.

Workaround: None required - the commands executed do not result in any changes on the PowerScale cluster.

T15278 Pool Failover job with multiple pools stops failover steps for all pools on DFS share renaming error

If an error which will abort failover occurs for DFS share renaming on one pool where the failover job contains multiple pools, failover will be aborted for all pools instead of continuing for pool which has no error.

Workaround: When failing over multiple pools, execute concurrent failover with 1 pool per failover job.

T15290 Pool Failover job with multiple pools does not rollback client redirection when allow writes step fails

If an error occurs on allow writes for one pool in a failover job that contains multiple pools there is no rollback for networking for failed pool.

Workaround: Networking can be failed back manually using PowerScale interface and using Failover log as a guide. Also can failover multiple pools concurrently with 1 pool at a time.

T15298 Quota job run manually after failover may delete quotas on source cluster

Even if quota failover steps fail on failover from cluster A to cluster B such that no quotas are created on cluster B and all quotas exist on cluster A, the quota failover job from cluster B -> A is created and enabled. If this Quota job is run manually it will delete all related quotas on the source (cluster A) leaving you without related quotas on source or target.

Workaround: Do not run quota jobs manually. Contact support.superna.net for assistance to failover quotas that failed during failover.

T15530 Policy or DFS Readiness may incorrectly evaluate Policy Hostname validation in error

DR Dashboard / DR Assistant Policy Readiness or DFS Readiness may incorrectly evaluate Policy Hostname validation in Error state placing overall failover status in Error. This validation should only be being assessed for Access Zone or Pool failover.

Workaround: Follow steps for Access zone failover configuration to ignore failover for the pool that has the Target Host. Steps to do this are on the target cluster apply "igsl-ignore" hint on the pool which has the SynclQ Policy Target Host. Ignore hints are simply an alias with the name of "igsl-ignore". Note it is best practise to ensure unique hints by using a naming format that uses cluster name - for example: igsl-ignore-`<clustername>`. Documentation reference can be found [here](#) - see section on ignore hints.

Once configured run the Eyeglass Configuration Replication Job to update DR Dashboard / DR Assistant.

T15547 Failover Readiness Domain Mark Validation fails for path with spaces or special characters

The Failover Readiness Domain Mark Validation returns an error for SynclQ policy source path that has a space or contains special characters.

Workaround: Manually confirm presence of domain mark by running command on PowerScale: `isi_classic domain list`. DR Failover Status of Warning does not block failover. For additional information on readiness validations in Warning state please refer to our documentation [here](#) or contact support.superna.net.

T15610 Policy Readiness Pool Mapping Validation alarm and email indicate Warning severity instead of Error

For the cases where an Access Zone is configured for Pool Failover and there are policies which are not mapped to pools the Un-Mapped Policy SmartConnect/IP Pool Status alarm and email incorrectly indicate that this is a Warning level issue. The DR Dashboard correctly identifies the issue as an Error which would block initiating a failover.

Workaround: Review readiness from the DR Dashboard directly.

T15613 DR Rehearsal Readiness - no alarm or email when DR Rehearsal status changes from OK to Warning or Error

No Alarm is raised or email sent when DR Rehearsal readiness status changes from OK to Warning or Error status.

Workaround: Login to the Eyeglass GUI and open the DR Dashboard to review readiness.

T15623 REST API - Pool Failover API does not support multiple pool selection

From Eyeglass DR Assistant a Pool failover can be initiated for multiple pools but this is not supported from the API.

Workaround: Run concurrent failover for multiple pools.

T15624 REST API - Failover API does not block controlled failover when source cluster unreachable

Failover API does not validate source cluster reachability and will allow a controlled failover to start even if source cluster unreachable. Controlled failover in this case is

expected to fail as it will attempt steps against the source cluster. When source cluster is not reachable uncontrolled failover should be used.

Workaround: Use manual process to verify source cluster reachability and initiate the appropriate controlled or uncontrolled failover.

T15769 DNS Dual Delegation Validation does not work where NS Record does not resolve directly to an SSIP

If DNS Dual Delegation is configured with NS Records that resolve to a name (for example configured as CNAME) the DNS Dual Delegation Validation will not work as it is expecting an IP address on resolution of the NS Record.

Workaround: To avoid this warning DNS Dual Delegation validation can be disabled. Please contact support.superna.net for assistance.

T16154 DR Rehearsal mode issues where source and target path are different

Invalid readiness validation for Corrupt Failover Snapshots: For case where SyncIQ Policy involved in DR Rehearsal mode enabled has different source and target paths or space in SyncIQ Policy path or a special character in SyncIQ Policy path, after DR Rehearsal mode enable the DR Failover Status incorrectly shows an Error for Corrupt Failover Snapshots for that policy. This error blocks reverting DR Rehearsal mode.

Failover error: Failover error occurs when data sync option unchecked.

Workaround: Do not use DR Rehearsal mode for policies which have different source and target paths, spaces in paths or special characters in paths. Regular failover is unaffected by this issue and is available. To recover from this REHEARSAL_ERROR open a support ticket at support.superna.net for assistance.

T17136 Zone Readiness incorrectly shows Error when Access Zone Name, Smartconnect Zone Name and IP Pool name are exactly the same

DR Dashboard Zone Readiness incorrectly shows Policy Readiness Status, SmartConnect/IP Pool Settings and Mappings Readiness and Eyeglass Failover Mapping Hints in error when the Access Zone, SmartConnect Zone Name, IP Pool all have exactly the same name.

Workaround: This issue can be resolved by renaming the Access Zone to be different. This change should be assessed for impact in your environment before making this change.

T17401 Pool Readiness not displayed with no configured/reachable DNS

If both Eyeglass and Isilon DNS are not available, the DR Dashboard pool readiness is not displayed.

Workaround: Provide reachable Eyeglass or Isilon DNS.

T17477 DFS share suffix not applied for failover or configuration replication

If a custom suffix is configured for DFS share name on target cluster, suffix is not applied either during configuration replication or during share renaming step of failover.

Workaround: None available.

T17428 REST API - Policy Readiness returns incorrect Access Zone

Failover API to retrieve Policy Readiness information returns the incorrect Access Zone for environments with multiple Access Zones.

Workaround: None required. Access Zone does not affect Policy Failover and Access Zone Readiness and Failover correctly assign policy to correct Access Zone.

T17447 OneFS 9.0 and 9.1 Readiness Validation for Policy Source Nodes Restriction always shows INFO

For OneFS 9.0 and 9.1 even if the Policy Source Nodes Restriction is configured, the Readiness Validation always shows INFO,

Workaround: Verify on PowerScale the source nodes restriction settings. DR Status of INFO does not affect / block ability to failover.

T17555 Blank display for Zone or Pool Readiness

In some instances where Zone and Pool failover is configured the Zone or Pool readiness window may be blank when both the DR Assistant and DR Dashboard are open.

Workaround: Reload the tab or only have one window open at a time.

T17731 Policies missing in DR Assistant for Zone or Pool failover

DR Assistant missing policies in an Access Zone for Zone or Pool failover where there are no SMB shares or NFS exports configured at or below the SyncIQ policy source path. Impact is that failover steps are not executed against these policies and they remain active on the source cluster.

Workaround: In advance of failover, configure a temporary share with restricted permissions at the SyncIQ policy source path. If you have failed and only then

determine the issue, policies can be failed over using Policy failover if the failover was an Access Zone failover. If the failover was a Pool failover manual steps must be used to failover the remaining policies.

T17732 Multiple Zone Readiness Jobs

Under some circumstances multiple Zone Readiness jobs will be running at the same time without any completing. DR Dashboard not updated when in this state. If this occurs during Access Zone failover it does not block failover.

Workaround: Eyeglass sca service restart will address this issue but recommend to contact support.superna.net for assistance and evaluation of the issue.

T18127 DNS Dual Delegation uses wrong SSIP when IP Pool Service Subnet different from the pool subnet

The IP Pool Service Subnet setting that is different than the parent subnet of the IP Pool is not taken into account for the DNS Dual Delegation validation. This could result in incorrect assessment of the DNS delegation configuration or if no SSIP configured in the parent subnet can result in the error "This IP address does not reference valid cluster".

Workaround: Manual inspection of DNS NS Record delegation should be done to confirm that it has been configured correctly.

T18392, T19226 DFS Failover produces extra "null" failover log

Under certain circumstances a DFS failover will generate a second failover "null" log visible in Running Failovers and Failover History. No impact to failover steps.

Diagnostic tool for dark site, igls app report, is not able to summarize failover history. Remainder of report is unaffected.

Workaround: None required for DFS failover. For diagnostic report, failover history can be retrieved from the Eyeglass GUI DR Assistant, Failover History window.

T18779 Overlapping Powerscale cluster and SyncIQ Policy names can result in incorrect Failover Readiness assessment

For the case where source and target Powerscale cluster have overlapping names (for example "cluster1" and "cluster1dr") and there are SyncIQ policies on both cluster with the same name, failover readiness for source cluster may take into account the SyncIQ policy state on the target cluster resulting in an incorrect state for source cluster. For example a SyncIQ policy disabled on the target cluster incorrectly results in Policy Enabling Readiness Warning for the SyncIQ policy on the source cluster.

Workaround: Rename the SyncIQ policy on the target cluster to make it unique between both clusters. For example pre-pend the SyncIQ policy name with the target cluster name.

T18969 Runbook Robot Job in Jobs window disappears when target cluster is unreachable

If there is an unreachable cluster, the Runbook Robot job in the Failover: Runbook Robot (AUTOMATIC) section of the Jobs window disappears for the unreachable cluster.

Workaround: None required. The Runbook Robot job cannot run when there is an unreachable cluster. The job reappears on it's own once the cluster is reachable again.

T19186 Policy Readiness not updated

Under some conditions the database will get into a state where the policy readiness assessment cannot be updated or completed and may contain old information. This

affects policy readiness as well as the policy readiness component of Zone and Pool failover readiness.

Workaround: This requires the database to be refreshed. Contact support.superna.net for assistance.

T19553 Zone/Pool Readiness never completes

Under some circumstances Access Zone Readiness job begins as expected on startup but never completes. Issue has been found to be related to execution of the DNS Dual Delegation validation.

Workaround: Disable the DNS Dual Delegation Validation as documented [here](#). Verification of DNS Dual Delegation for Access Zone and IP Pool failover must be done manually.

T19967 Pool / Zone Readiness does not indicate whether there is a disabled Configuration Replication job in the Zone

Pool / Zone Readiness shows OK and green even when there is an associated disabled Configuration Replication job. Impact: Any associated Configuration Replication Job that is disabled will skip the associated SyncIQ policy during failover.

Workaround: None required. When initiating the failover the DR Assistant Wizard does identify the disabled job and prompts on whether or not to proceed. Also Policy Readiness view can be used to identify disabled jobs.

T20181 Policy Hostname Validation Incorrectly show Error

If the pool mapping hints or ignore hints configured for Access Zone or IP Pool failover overlap with the SyncIQ policy target host then the validation incorrectly flags the Policy

Hostname Validation as Error. For example - SynclQ policy target host is taget.ad2.test and mapping/ignore hint is igls-ignore-a-target.ad2.test.

Workaround: Rename the mapping/ignore hint so there is no overlap. For example as per above change the ignore hint to igls-ignore-a-target-a.ad2.test.

T21443 Quota failover error when source and target path are different and contain a \$

For SynclQ policy where source and target policy path are different and contain a \$ sign, when the quota failover step runs it attempts to create the quota on the source path instead of the target path.

Workaround: Quota configuration must be documented pre-failover and quotas need to be created manually on target after failover.

T21629 DR Readiness does not indicate source cluster unavailable

DR Dashboard does not indicate the condition where the source cluster is not available. This does not impact ability to failover - controlled failover is blocked and uncontrolled failover can proceed.

Workaround: Use the Continuous Op Dashboard to see whether clusters are available to Eyeglass.

T21750 Deleting SynclQ Policy when Rehearsal Mode is active leaves configuration behind

In the configuration file which tracks whether rehearsal mode is active or not, a policy that is deleted while rehearsal mode is active is not removed from the file. Impact: Cannot use Eyeglass to revert rehearsal if the SynclQ policy is deleted.

Workaround: None required. A new policy on the same path would be referenced by a new unique ID.

T22269 Python Pre and Post Failover Scripts do not work on OpenSUSE 15.3

Python based pre and post failover scripts do not run on OpenSUSE 15.3. In the failover log you will see the message: /usr/bin/env: 'python': No such file or directory. Shell scripts are not affected.

Workaround: Use shell scripting for pre and post failover scripts.

T22567 Quota Inventory causes problems during failover

Quota inventory is not blocked from running during failover and can result in system restart and an incomplete failover.

Workaround: Set the quota inventory schedule to run infrequently (example weekly) and for planned failover do not run concurrently.

T21929 igls-original SPN may not be deleted on failover

For the case where a smartconnect alias exists already with an igls-original prefix, on failover, we skip the delete for the igls-original which causes SPN Issues on future failovers. This problem is specific to igls-original prefix SPNs and does not affect data access as the igls-original smartconnect is not used for accessing data.

Workaround: After failover, manually fixes SPN to prevent issues on future failovers or ignore the issue

Configuration Replication

1683: Export sync where source is 7.1.1.x and target 8.x.x.x

Description: Syncing exports does not function between these releases.

Resolution: None unsupported sync, upgrade to 7.2.x.x

649: Export sync where source and target path on each cluster is different is deleted and recreated in each config cycle (affects onefs 7 to 8 or 8 to 7 replication)

Description: When the path on source cluster and target of the SyncIQ policy are different, exports will be deleted on target and then recreated again within the same replication job. No error is seen on the config sync job. May affect other releases as well.

Resolution: None, export is created correctly after config sync job completes.

1462 - Export max_file_size cannot be replicated

Updated export max_file_size parameter is not replicated and replication Job fails.

1355: Edit Job configuration to include share/export deselected from another Job causes share/export to be reselected.

Description: When you edit a Job B configuration to include share/export that had already been deselected from Job A, this causes this share/export to be reselected for Job A as well.

Workaround: None available. Should the share/export subsequently be deselected from Job B it should then also be manually deselected again from Job A.

1580: Delete and Create export within same replication cycle orphans deleted export on the target with OneFS 7.1.1.x

With OneFS 7.1.1.x, a delete and create export operation which occurs within the same replication cycle will replicate the export that was created on the next replication cycle but the export deleted on the source will not be deleted on the target.

Workaround: Manually remove the deleted export from the target using PowerScale OneFS.

1625: Custom QUOTA Jobs require extra replication cycle to be deleted

In the Eyeglass Jobs window, when you delete a CUSTOM Job and then the associated QUOTA Job is not immediately deleted. It is deleted on the next replication cycle.

Workaround: None required.

1639: Able to manually Run Now disabled Custom Job

Eyeglass Jobs window allows you to Run Now on a Custom Job which has been disabled. A message is displayed indicating that the Job has been queued but the share/export configuration replication Job is not run and the associated QUOTA Job is run and quotas are replicated.

Workaround: Do not Run Now for Custom Job that has been Disabled.

1641: Custom Job does not include shares/export when source or destination path configured with a trailing /

If you enter source or destination path for Eyeglass Custom Job with a trailing / (for example /ifs/data/test/), the Custom Job will not pick up the related shares and exports.

Workaround: Source and destination paths must be entered without the trailing / - for example /ifs/data/test.

1788: Delete of unlinked user quota on source may not delete matching quota on the target

Attempting a quota replication after deleting an unlinked user quota may fail to delete the quota on the target with a Job status of success but an Audit failure.

Workaround: Deleted quota manually deleted on the target.

1789: Able to select shares/exports/quotas outside job path after deselected

After a share/export/quota has been deselected from an Eyeglass Job, it can be re-selected for a different Job even if it is outside the Job path. As a result, the Job may have an error for these share/export/quota due to path not found error.

Workaround: Do not customize Eyeglass configuration replication Job and select share/export/quota that are outside the Job path.

1887, T3727: Multiple SynclQ policies associated with same Zone will result in transient error on Eyeglass Zone replication creation

Where there are multiple SynclQ policies which are associated to the same zone and Eyeglass configuration replication is being used to create the zone on the target, the first Zone replication job will succeed, but subsequent Zone replication jobs for the same Zone will fail with the message “Zone ‘<zone name>’ already exists”.

Workaround: None required for OneFS 7.2 - 7.2 or 8 - 8 replication. Error will be cleared on subsequent configuration replication cycle.

For OneFS 7.2 - 8 replication, Zone Replication Readiness always has warning status and alarm is raised for failed audit on zone job. Manually inspect that Access Zones are identical and that Zone Readiness Warning is related to this issue.

1924: Quotas on excluded SynclQ directory are selected for replication

Eyeglass quota job includes quotas related to excluded SynclQ directories. If quota job is run, it will typically fail due to path not found.

Workaround: Customize Quota Job and deselect quotas for excluded directories.

1998: Custom Eyeglass configuration replication Job does not have an associated Zone replication Job

When you create a new custom Eyeglass Job, an associated Zone replication Job is not created.

Workaround: Zone must be created manually or already exist on the target cluster in order for Eyeglass configuration replication to succeed.

2004: Custom Quota Job is incorrectly listed in the Failover: Quota Failover (RUN MANUALLY) section in the Jobs window

When you create a new custom Eyeglass Job, the associated Quota replication Job is created and incorrectly listed under Failover: Quota Failover (RUN MANUALLY) section in the Jobs window. Custom Quota Jobs do not need to be run manually, they are run automatically each time the customer Eyeglass configuration replication Job is run.

Workaround: None required. Custom Quota Jobs do not need to be run manually, they are run automatically each time the customer Eyeglass configuration replication Job is run.

2007: Job error after deleting quota

After running Quota Job and successfully replicating quota to target, if quota is deleted and Quota Job is run again the Quota is successfully deleted from the target but the Quota Job has Error status.

Workaround: None required - quota is deleted.

2038: Create alias results in temporary error

When an nfs alias is replicated to the target, the initial create leaves Job in Error state with related alarm " Alias <alias name> already exists on this zone"

Workaround: None required. Next replication cycle clears the error.

2043: Configuration replication job has error after zone is deleted

For the case where Zone related to a Configuration Replication Job is deleted on the source, the Zone and associated configuration items are successfully deleted on the target, but the Configuration Replication job remains in Error state.

Workaround: None required. Shares and exports are deleted as expected.

2045: Edit Configuration for Custom Job has multiple source cluster selected where Eyeglass is managing more than 2 clusters

For the case where Eyeglass is managing more than 2 clusters, it may occur that the Edit Configuration view incorrect.

Workaround: None required. Shares and exports are replicated as expected.

2046: Job Edit Configuration view has the wrong parent selected

For the case where a configuration replication job contained a configuration items and the last configuration item is deleted - after the configuration item is deleted, the parent in the Edit Configuration view continues to be selected for the Job even though when you expand the tree there are correctly no children selected.

Workaround: None required.

2049: Delete Zone does not delete associated configuration items on target for custom Jobs and auto jobs with disabled zone Job

When a non System zone is deleted on the Source, the Eyeglass Configuration Replication Custom Job or Auto job with disabled Zone Job does not remove the associated configuration items from target related to the deleted Zone.

Workaround: Manually delete the Zone and associated configuration items on the target using OneFS.

2235: Eyeglass replication Job does not complete when source cluster becomes unreachable after Job has started

If the source cluster becomes unreachable after the Eyeglass configuration replication Job has started, the Job does not complete.

Workaround: None required. The Job will eventually complete after all communications timeouts have occurred. This may take an hour.

2060: Access Zone Replication Error - Error on creation of shared resource

Error on Replication for Access Zone which shows Error on creation of shared resource.

Workaround: None required. Once SynclQ Job has run again in OneFS, the next time configuration replication runs the Access Zone is replicated.

2488: Inconsistent behaviour in Run Now for Disabled Jobs

When Run Now is selected for an Eyeglass Job which is disabled, the handling is different depending on Job Type and state:

For Job which is "Policy Disabled" - Run Now is blocked for all Jobs

For Job which is "User Disabled" - Run Now not blocked and all enabled Jobs run

For Robot Job which is disabled - Run Now not blocked, Job is initiated and then fails.

Workaround: Only select enabled Jobs for Run Now.

1938: Issues with Eyeglass Configuration Replication Jobs after the Access Zone is deleted

When you delete an Access Zone in OneFS, the following issues occur in Eyeglass:

- corresponding Eyeglass Zone Configuration Replication Job is not deleted

Workaround: None Required. Job is empty.

2308: In EyeGlass, NFS alias health is always 'unknown'

Eyeglass Inventory, NFS Alias audit and Cluster Configuration Report always have the NFS alias health property set to unknown.

Workaround: Determine the NFS Alias health from the OneFS command line using `isi command..`

2804: Disabled SyncIQ Policy is not initially displayed as Policy Disabled in Eyeglass

When the Eyeglass system setting for INITIALSTATE is set to Disabled for Configuration Replication Jobs (Type = AUTO), the Jobs window State for the Eyeglass Configuration Replication Job where the corresponding SyncIQ Policy is disabled displays as "User Disabled" instead of "Policy Disabled". In this state the Eyeglass GUI allows you to Enable this Job, but in fact after the next Configuration Replication Job the Job is correctly displayed with the Policy Disabled state.

Workaround: None Required.

T676: Eyeglass Zone replication Job does not replicate all authentication providers for OneFS 8.0

For OneFS 8.0, if an Access Zone has multiple authentication providers not all providers will be replicated for the Access Zone on the target cluster.

Workaround: Manually edit the Access Zone on the target cluster and add the required authentication providers.

T723: Job shows OK when there is an Access Eyeglass Zone Replication Error

The Jobs window for an Access Zone replication Job which had a replication error or audit error shows as OK even though an Alarm was issued for the Error.

Workaround: Monitor email for Access Zone replication errors. Address the replication issues.

T771: Edit Configuration does not show parent node selected

If a change is made to a Configuration Replication Job to deselect a file sharing object from the job, the parent node where there still are selected objects is no longer selected in the Edit Configuration window.

Workaround: Expand the Inventory View tree for SMB and NFS to see which objects are contained in the Job.

T805: Eyeglass Configuration Replication Jobs not updated when IP address changed on Source Cluster

An IP address change on the Source Cluster of an Eyeglass Configuration Replication job does not get picked up and the job continues to reference the old IP address resulting in a configuration replication error.

Workaround: Reset Eyeglass to pick up IP address changes for Jobs on the newly active cluster

1. Make a record of the state of all Configuration Replication Jobs in the Eyeglass Jobs window - these states will NOT be preserved on the reset:
 - a. Jobs which are Configuration Replication type
 - b. Jobs that are DFS enabled
 - c. Jobs that are User Disabled
2. SSH to Eyeglass appliance using admin: `sudo -s` enter (must use root) then use admin password (default password: 3y3gl4ss)
3. set the initial state for all Eyeglass Job types to User disabled
 - a. <http://documentation.superna.net/eyeglass-PowerScale-edition/Eyeglass-PowerScale-Edition#TOC-igls-adv-initialstate>
4. `cd /opt/superna/sbin`
5. `./reset.sh`
6. Once reset completes, go to the chrome browser and refresh the browser and log in with the credentials
7. Now, you need to add both of the clusters using Management subnet SSIP.
8. Once it is added, open the Job window - now you will see all the Eyeglass configuration replication jobs are in the “user disabled” state
9. `./Enable` all the Eyeglass configuration Job to DFS Mode if configured

IMPORTANT: You must enable DFS mode before enabling the Job to prevent the creation of active shares on the target cluster.

1. Enable all configuration replication job (except ones that were previously User Disabled) and run it

T593: Eyeglass errors for multiple exports with the same path

If an Eyeglass Configuration Replication Job contains more than one Export with the same path, this may result in an AUDITFAILED state or configuration replication error for the associated Eyeglass Configuration Replication Job in the DR Dashboard or a configuration replication error.

Workaround: The following workaround is available to address this issue:

1. Modify exports on the source to add a second path which is a sub-folder of the existing path. This way Eyeglass will identify each Export uniquely. Example

Initial State:

export 1: /ifs/data/folder

export 2: /ifs/data/folder

Updated State:

export 1: /ifs/data/folder

 /ifs/data/folder/sub-folder

export 2: /ifs/data/folder

- 2) Exports must have different Clients.
-

T1792: Eyeglass does not auto-detect PowerScale version changes and may use incorrect API version for Configuration Replication

You may see Inventory errors after upgrading the PowerScale cluster version or adding a cluster to be managed by Eyeglass which has a different OneFS version than clusters already managed due to wrong version of API being used to connect to the cluster.

Workaround: Restart the Eyeglass sca service as per instructions here for sca service:

<http://documentation.superna.net/eyeglass-PowerScale-edition/Eyeglass-PowerScale-Edition#TOC-Eyeglass-Processes>

T1851: Eyeglass Configuration Replication Jobs not removed when there is no SynclQ privilege for the eyeglass service account

If the eyeglass service account has the SynclQ privilege removed the Eyeglass Jobs are not updated to removed even though the associated SynclQ policy cannot be retrieved. The Jobs run successfully with the message “The job has no data to replicate; skipping it.”

Workaround: eyeglass service account must have the SynclQ privilege as documented in minimum permissions document here: <http://documentation.superna.net/eyeglass-PowerScale-edition/tech-notes/PowerScale-cluster-user-minimum-privileges-for-eyeglass>

T2193 - Export max_file_size setting not replicated correctly

A large export max_file_size parameter is not replicated exactly to target as it is configured on the source which results in an Audit failure during Eyeglass Configuration Replication. For example:

Source 4611686018427388000

Target: 4611686018427387904

Workaround: None available. For smaller values such as 1024 or 1048576 this error does not occur.

T2757: Access Zone is not replicated from OneFS 8 to OneFS 7.2

Access Zone is not replicated from OneFS 8 to OneFS 7.2.

Workaround: Create Access Zone and make updates manually.

T1976 - Eyeglass Jobs Window Edit Configuration does not show related Snapshot Schedules

If a Snapshot Schedule Replication Job is selected in the Jobs window, the Edit Configuration option does not mark the Snapshot Schedules which are included in the Job..

Workaround: Expand the Snapshot Schedule Job in the Jobs window to see the Source Path. Manually review Snapshot schedule paths. Any Snapshot Schedule where the path is at or below the Job source path will be included in the Job.

T2920: Access Zone Authentication Provider is not replicated to the target cluster

Eyeglass Configuration Replication does not sync the Access Zone Authentication Provider to the target cluster.

Workaround: Add Authentication Provider to the Access Zone manually.

T3629: Renamed Snapshot Schedule leaves original Snapshot Schedule on the target

After renaming a Snapshot Schedule, the next Configuration Replication cycle creates the new Snapshot schedule on the target but does not remove the Snapshot schedule with the original name such that on the target they both exist.

Workaround: Manually remove the extra Snapshot Schedule from the target.

T14803 Set Job Type AUTOSKIPCONFIG does not create associated jobs until configuration replication runs

When setting job type for an unconfigured job to type SKIPCONFIG the other related jobs for snapshot schedule, zone, quota are not created until the next Configuration Replication cycle has completed.

Workaround: None required - next scheduled Configuration Replication job will rectify and create the jobs.

T15258 Unable to create Custom Job

After creating a Custom Job, it is removed from the Job list after the next Configuration Replication cycle runs.

Workaround: None Available

T15321 DFS share name custom suffix may be doubled

If you have configured a custom DFS suffix, if the source share name already has the suffix it may be added again to target share on replication instead of being skipped.

Workaround: It is not expected for source share name to have the DFS suffix. Please contact support.superna.net for assistance.

T15884 Some scenarios in networking API failures during Configuration Replication may not block deletes

Some scenarios remain after resolution in 2.5.5 T12773 where when Eyeglass has an incomplete view of PowerScale configuration due to a PowerScale API networking API call failure there is a risk of deleting and readding Eyeglass Configuration Replication jobs and losing their settings such as DFS mode or AutoSkipConfig mode or risk of deleting meta data such as SMB shares or NFS exports.

Workaround: In 2.5.6 all new Eyeglass configuration replication jobs will be in unconfigured state. When activating ensure that you are activating in the correct mode: AUTO, DFS or AUTOSKIPCONFIG.

T16965 Audit does not consider differences on source and target for SMB share property inheritable_path_acl

For the case where an SMB share has been manually created on the target cluster with a different setting for the SMB share property inheritable_path_acl, the Supena Eyeglass compare of the source and target share does not identify the difference and therefore does not update the target share to match the source share.

Workaround: One OneFS manually change the setting for this property, or if the share on the target cluster is not in use delete it and allow Eyeglass to recreate it.

T18812/T23433 Error replicating SMB Share with Run as Root permission

In some cases where an SMB share permission is configured with run as root the run as root permissions are replicated to the target as regular permissions and also subsequent attempts to update results in a duplication of permissions which results in duplicate error and/or AEC Error Failed to insert new run-as-root - Message too long.

Workaround: To skip replication of share permissions and properties you can follow the steps [here](#) to view the shares and exports that are part of the Configuration Replication Job. To skip replication on a share, uncheck it. Once skipped, manual process will be required to keep share properties and permissions up to date on target cluster.

T19026 Data Config Migration Preview incorrectly shows quotas selected

If Data Config migration is configured to not replicate quotas, the Preview window incorrectly displays quotas as selected for replication. This is a display issue only. Quotas are not replicated when the migration job runs.

Workaround: None required.

T19177 NFS modify properties which are not client list fails with unresolvable host

If an NFS export property is modified where the property is not an NSF export client and the client list contains unresolvable hosts, the Eyeglass replication job will fail to update the NFS export on the target with an unresolvable host error even if in Eyeglass the ignoreunresolvablehosts setting is set to true. Note that this is not an issue if an NFS export client list is modified as this results in a delete and create of the export since the client list is part of how we uniquely identify the export.

Workaround: Manually update the export on the target cluster to update for new setting.

T19894 NFS Export replication in DR Test Access Zone incorrectly identifies that update is required

For case where main Configuration Replication job correctly does not identify any changes for an NFS export, the replication to that DR Test Access Zone incorrectly identifies an update is required. Impact: None except for case where replication is subject to issue T19177 NFS modify properties which are not client list fails with unresolvable host you will see an error.

Workaround: None required.

T20301 User Disabled AUTOSKIPCONFIG job becomes enabled after a rediscover or if policy renamed

Upon executing a rediscover command in Eyeglass or if the SyncIQ policy associated with an AUTOSKIPCONFIG job is renamed, the status of the AUTOSKIPCONFIG job changes from User Disabled to Enabled. Impact: As AUTOSKIPCONFIG mode skips the replication of share and export properties there is no impact to any shares or exports on the target cluster if the job becomes enabled. Ability to failover the associated SyncIQ policy changes from being blocked to failover to being able to failover.

Workaround: Manually update AUTOSKIPCONFIG job status after rediscover or policy rename.

T20369 Configuration Replication Error after running DR Rehearsal failover on SyncIQ policy where source and target path are different and contain special characters and or spaces

A configuration replication job that is OK and green prior to executing a DR Rehearsal failover may be in error after the DR Rehearsal revert when the SyncIQ policy source

and target path are different and contain special characters and or spaces. Impact: No impact to subsequent DR Rehearsal failover. Changes to SMB shares or NFS exports for that job will not be replication.

Workaround: SMB Shares and NFS exports on the target will have to be kept up to date manually.

T21375 Snapshot schedule replication error on update

Initial snapshot schedule replication completes successfully, but a change to the snapshot schedule such as changing the snapshot expiration results in following error on update: AEC_CONFLICT Schedule entry already exists with that name: File exists.

Workaround: Snapshot schedule can be updated manually on the target cluster for changes.

T22875 Configuration Replication audit step incorrect error when path contains a comma

For Configuration Replication where the path contains a comma the post audit step incorrectly reports that the share is not identical on source and target. Impact is incorrect result on audit only, the replication of the share itself was successful. This also impacts failover readiness which will show a Warning as a result of this issue.

Workaround: For Configuration Replication none required. For Failover, this Warning can be ignored and to failover with this Warning uncheck block on warning option. Any other Warning must be assessed independently before unchecking block on warning for failover.

Features

1138: Eyeglass UI does not block configuration of duplicate remote logging service

Description: If you configure the same remote logging service twice in Eyeglass, the forwarding of logs to the logging service will fail

Workaround: Only configure 1 instance of a remote logging service.

2224: Eyeglass Cluster Configuration Report runs when Cluster is unreachable

Eyeglass attempts to run the Cluster Configuration Report for Cluster that is not reachable. The Job is started but does not complete.

Workaround: None available. Report will run successfully once cluster is reachable.

2061: Access Zone name for Directory Migration is case sensitive

Check for Access Zone exists on target cluster for Directory migration fails is case sensitive and will fail if Access Zone exists with same name but different case.

Workaround: Access Zone name and case must be identical between source and target for Directory Migration.

2882: Phone Home Email Disabled

Phone home feature is changing and will be disabled . A new web direct option will be used in a future release.

Workaround: Use the Eyeglass Backup Full Archive function to collect Eyeglass configuration and logs. Procedure is described in the document

3037: Configure Remote Logging Services in Eyeglass requires manual steps

After configuring the Remote Log Consumer in Eyeglass, additional manual steps are required on the Eyeglass appliance to update syslog-ng.conf to enable the service.

Workaround: Please refer to Eyeglass Tech Note [Eyeglass PowerScale Remote Logging Service Tech Note](#) section “Setup Eyeglass remote logging manually for log Analysis”.

T1515: Eyeglass Shell feature not functioning for RHEL and Centos deployments

If Eyeglass is deployed on a Redhat or Centos operating system the Eyeglass Shell feature does not work.

Workaround: ssh to the Eyeglass server using other tools such as putty.

T3119: Access Zone Migration Preview does not always display Configuration information

The Access Zone Migration Preview window does not display the shares, exports and quotas that will be migrated if the source path selected for migration does not have an associated SynclQ policy.

Workaround: Review shares/exports/quota paths manually to determine which configuration data will be migrated for the selected source path.

T3170: Quota Requests History shows Status of Error for processed requests after failover

After failover, the Quota Requests History will show state for all processed quota requests as error instead of showing the status of the request as it was when the request was processed.

Workaround: Verify from OneFS that the quota settings are as expected.

T4280: User Storage View may show all quotas instead of only the User Quotas

It may occur that the User Storage View shows all quotas configured instead of just the quotas related to the logged in User.

Workaround: Logout and refresh browser and then log back in and reopen window may clear this condition. If not, the quota path may be used to determine which quota apply to the logged in user.

T4329: DR Test Status does not open

When DR Test Job has first been created, the DR Test Status window does not open and shows the error "Readiness data not found. Please run configuration replication." even though Configuration Replication has run.

Workaround: DR Status window will open once DR Test Mode has been Enabled.

T4432: DR Test Mode action on multiple policies do not display in Running Jobs

When multiple DR Test Jobs are selected in the DR Assistant to enable or disable DR Test mode, the Running Jobs window only shows 1 Job even though action is being applied to all selected Jobs.

Workaround: None required - display issue only. Action completed against all selected jobs.

T4968: SynclQ Job Report Troubleshooting section missing information when report is generated on demand

When a SynclQ Job Report is generated from the Reports on Demand window, the Troubleshooting section may not be populated.

Workaround: Use the scheduled daily report for Troubleshooting information.

T5173: Quota Modification Request window does not close after Submit

After a Quota Modification Request is submitted, the window does not close and remains in a loading state.

Workaround: None required - display issue only. Action was completed and the request can be seen in the Pending Requests window.

T6389: Built-In AD Groups cannot be used with the Cluster Storage Monitor Active Directory Managed Quota feature

When configuring Cluster Storage Monitor AD Group Mode Templates for automated quota creation, AD built-in groups such as "domain users" cannot be used as the users in the group will not be correctly identified.

Workaround: Create new AD Group for quota assignment and add this group to related shares in PowerScale. For additional information on use of AD groups for share security vs quota creation please read [here](#).

T8834: Storage Monitor Report missing user information when friendly name cannot be resolved

User quotas created for users who are not in the default AD Domain, a friendly name cannot be resolved and quota itself is associated with user SID but in the Storage Monitor Report the user is reported as "user" instead of showing user SID.

Workaround: None available.

T9561: Unlock my files incorrectly displays directories

Unlock My Files window incorrectly includes directories in the display instead of just files. If a directory is inadvertently "unlocked" it may disconnect clients or have other unexpected results.

Workaround: Do not use unlock for directories.

T11807 Alarm for quota synchronization error does not contain error details

For case where quota synchronization fails (example advisory threshold configured to be greater than hard threshold), an Eyeglass alarm is raised but the alarm does not contain any details of the error.

Workaround: In Eyelgass Jobs / Running Jobs window tree view under "Group Quota Synchronization Steps" navigate down the tree and find the step with an error. The Info link should contain error details if available.

T12307 Cluster Storage Usage may be incomplete

When the API request for cluster storage usage is returned from PowerScale with information missing for one or more nodes, the Eyeglass Cluster Storage Usage window may not display all information for the nodes where information was returned. For example for a 4 node cluster if the API response only contains information for nodes 1, 3 and 4 the Cluster Storage Usage window may only display information for node 1 even though node 3 and node 4 information is available.

Workaround: Use PowerScale tools to determine storage usage.

T13390 DR Testing (Disaster Recovery Testing) Job initially always in User Disabled state

When an Eyeglass Job first becomes type Disaster Recover Testing it is always in User Disabled state no matter what state it was in as an AUTO job.

Workaround: Select the checkbox for the Disaster Recovery Testing job and then Select a bulk action / Enable/Disable to enable it.

T14956 No Recovery when DR Test Mode in Entering DR Testing or Exiting DR Testing

If DR Test Mode Make Target Writeable/ Make Target Read-Only does not complete and is left in the Entering DR Testing or Exiting DR Testing state there is no way to revert or retry the operation.

Workaround: To assist in recovery from this state please open a support case at support.superna.net .

T14962 DR Test Mode Configuration Replication step does not run configuration replication for the DR Test mode job itself

If Configuration Replication option is selected for Make Target Writeable, the DR Test mode job itself is not included and any changes to SMB shares or NFS exports that had not been previously synced will not be present on shares / exports used for the DR Test.

Workaround: Let scheduled configuration replication job run or manually initiate configuration replication to sync SMB shares and NFS exports to the DR Test mode shares / exports prior to initiating Make Target Writeable.

T15215 Data Config (Zone) Migration Job can not be created where Migration or Destination Path contains special characters

A Data Config Migration Job will fail to be created if the Migration or Destination Path contains special characters (example & or ').

Workaround: None Available

T15311 Data Config (Zone) Migration Job fails for existing policy when "Migrate only configuration" is checked

A Data Config Migration Job will fail when there is an existing SyncIQ policy on the migration path and "Migrate only configuration: is not checked.

Workaround: Select "Migrate only configuration" option to sync the configuration items and separately manage SyncIQ from PowerScale interface to manage data replication.

T17535 Quota Search - Display of quota count on modify may not be correct

The count of quotas modified displayed on the GUI may not be accurate.

Workaround: Verify via OneFS interface that requested changes have all been made.

T17739 Cannot create quota template for less than 1 GB

Quota template creation for Active Directory Managed Quotas (igls csm template add) does not allow creation of a quota limit of less than 1 GB either by entering less than 1024 MB or a decimal in GB.

Workaround: None available - minimum quota size available is 1 GB.

T18148 Incorrect Error Message for unreachable Powerscale cluster when breaking lock

Error message is displayed if Break Lock operation occurs when Powerscale cluster is unreachable, but does not indicate that the issue is an unreachable cluster. Error message may simply say "Error unlocking file!" if a node is unreachable or "Server error when processing request: null" if entire cluster is unreachable.

Workaround: None required

T19464 AD Group Template incorrectly creates quota on share where user permission is explicitly defined

If you have user permission assigned explicitly to share and that user is in an AD Group template for quota assignment, quota will be correctly created on the share(s) with the AD Group template assigned but will also incorrectly create a quota for any share where user permission is assigned explicitly.

Workaround: Use AD groups to assign permission to shares.

T20183 Unlock My Files does not display results if there is a Powerscale node that does not respond

If a Powerscale node does not respond (for example node is down or unreachable) when Unlock My Files is run, locked files on nodes that do respond are not displayed.

Workaround: Ensure that all PowerScale nodes are available.

T22209 igls adv ADGroupThresholds does not scan

The igls adv ADGroupThresholds starts API calls to retrieve AD users and groups but it does not evaluate the template to determine whether any quotas should be applied.

Workaround: None available.

T22622 Active Directory Managed Quotas fails with LDAP configured for retrieving user and groups

With Eyeglass configured to use LDAP to retrieve Active Directory Users and Groups, the Active Directory Managed QUotas feature does not work as the groups cannot be identified.

Workaround: Default collection of Active Directory User and Groups should be used with the Active Directory Managed Quotas feature.

General

924: Inventory View shows + beside component when there are no more children

Description: In the Inventory View, components for which there are no children still show a “+” in the inventory tree. When you select the “+”, it changes to a “-” but there are no children displayed.

Workaround: None Required.

T17694: API token download of CMDB file is blocked by desktop login

Description: The API token download access to the servicenow.xml file is blocked by the web server desktop authentication service.

Workaround: Log in to the desktop and enter the URL <https://isilon-eyeglass/servicenow/servicenow.xml> to view download the file. API token access requires future release to bypass web server desktop login.

943: Inventory View not auto-refreshed

Description: Inventory View is not auto-refreshed and if open when a change occurs does not reflect the change.

Workaround: Use the Refresh Now button or close and reopen the Inventory View.

1612,T11989: Some alarms not cleared

Alarms other than the “Replication job failed to run “ are not cleared automatically once the error condition has been resolved. Example, DR Readiness alarm not cleared once readiness is green.

Workaround: Clear the alarm manually from the Eyeglass UI.

2155: Access Zone Networking info does not display in Inventory View

To see the Networking info for an Access Zone in the Inventory View:

- the Failover Readiness job has to have run
- the Access Zone must have an associated SynclQ Policy

Workaround: Enable Failover Readiness job.

2628/T15193: Job Definitions window does not sort properly

Click on column headings in Jobs window to sort listings does not sort properly and sometimes lists jobs outside of the category groupings.

Workaround: None available

2895: Inventory SPN View is truncated

The Eyeglass Inventory view may be truncated and not display all SPNs stored in the database.

Workaround: Use isi command directly on cluster to determine all SPN.

2366: EyeGlass does not support special characters in email recipient address

Email addresses in Eyeglass do not support special characters.

Workaround: Do not provision email recipients or Email Server user with email address that has special characters.

2385: Refresh Now does not refresh the Failover History window

The Failover History window is not updated by the Eyeglass Refresh Now functionality.

Workaround: Close and reopen the Failover History window to see updates.

2744: Failed to Retrieve Inventory Alarm missing information

For the case where Inventory does not run because another instance of the Inventory Task was already running, the alarm that is raised does not provide this additional information

Workaround: Review the Eyeglass logs at the time that the inventory alarm occurred and search for the string “Another instance of Inventory Task is still running. Not starting”.

2978: Syslog Log Viewer freezes Eyeglass web page

Opening the Eyeglass Syslog Log Viewer window may cause the Eyeglass web page to freeze.

Workaround: Refresh the Eyeglass web page or Fetch the Eyeglass Main Log first and then Fetch the Eyeglass Syslog.

T971: Eyeglass End User Interface Tree View Expanders do not collapse

The Eyeglass End User Interface DR Dashboard tree display '+' can be used to expand the tree but then the '-' does not collapse the tree again.

Workaround: Close and reopen the window

T1514: Eyeglass Archive cannot be downloaded when Eyeglass is deployed on Redhat or Centos

Eyeglass Backup Archive file cannot be downloaded from the Eyeglass web page if Eyeglass is deployed on a Redhat or Centos operating system.

Workaround: The Eyeglass Backup Archive files are stored here on the Eyeglass server: `/srv/www/htdocs/archive/` and can be copied from this location with a tool such as WinSCP.

T3137 - Eyeglass daily backup not working for RHEL/CentOS Deployments

The scheduled daily backup for Eyeglass is not working for RHEL/CentOS deployments.

Workaround: Manually create backup file from the Eyeglass GUI: About/Contact -> Backup -> Create Full Backup

T4596: Log Viewer cannot fetch logs

Under certain conditions the Log View may not be able to Fetch logs.

Workaround: Use the About/Contact -> Backup to create a Backup Archive and then download to your local system to review logs.

The Log View feature will be deprecated in a future release.

T12370 Network Visualization does not display Pool Readiness

The Network Visualization window Info Tab does not have a section for Pool Readiness. If you have Pool Failover configured you may see the related Access Zone in the Zone Readiness tab or related policies in the Policy Readiness tab. If you select status for that object it will open the DR Dashboard to the selected section not the Pool Readiness section.

Workaround: For assessing Pool Failover readiness open the DR Dashboard and select Pool Readiness.

T12373 Cluster Storage Window Empty

Under some conditions, the Cluster Storage Usage / Cluster Storage window is empty when it is opened.

Workaround: In some cases after toggling between Cluster Storage and Cluster Hardware menu or selecting Details the clusters will appear. If this does not resolve the issue, then native Powerscale tools can be used to collect cluster storage information.

T15310 REST API / Widgets creates empty html file

Unable to create web widget for DR Readiness.

Workaround: Use Eyeglass API to retrieve DR Readiness information. Plan to deprecate web widget in 2.5.7.

T15493 Extraneous Post Failover placeholder scripts

There are extraneous postfailover script provided that are not runnable: script1.sh, script2.py, script3.js .

Workaround: None required. These scripts should be ignored as they contain no examples. The environment_example scripts should be used as a reference.

T15511 Historical failover logs may lose formatting after a backup & restore

Failover logs retrieved from the Failover History may not have formatting after backup & restore.

Workaround: None required.

T15647 igls app report issues

The igls app report command to create a dr health summary file does not exit on completion of execution. The report is available for review but the command itself is not exited.

Workaround: Use CtrlC to exit the command.

The igls app report command may report below error and not start.

Starting a log parser service...

```
sh: /opt/superna/java/jre1.8.0_05/bin/java: No such file or directory
```

Workaround: Run the report using command below. Once run this way the correct java version should be available to igls app report command as well.

```
java -jar /opt/superna/bin/LogParserSca-0.0.1-SNAPSHOT-jar-with-dependencies.jar
```

T17530 Backup and Restore does not properly set location/permission for Eyeglass log files

After restoring Eyeglass backup , the Eyeglass log files location and/or permission is not properly set.

Workaround - 2.5.6-20258: Follow the steps below after the restore to correctly set log location:

1. SSH to Eyeglass VM (user: admin, default password: 3y3gl4ss)
2. sudo su (enter admin password)
3. execute below command

```
cd /opt/superna/sca && mkdir -p /opt/data/superna/sca/logs && cp -af logs/* /opt/data/superna/sca/logs && rm -rf logs && ln -s /opt/data/superna/sca/logs && chown -R sca:users /opt/superna/sca/logs
```

4. Done

Workaround - 2.5.6-20263: Follow the steps below after the restore to correctly set log location:

1. SSH to Eyeglass VM (user: admin, default password: 3y3gl4ss)
2. sudo su (enter admin password)
3. execute below command

```
cd /opt/superna/sca && chown -h -R -L sca:users /opt/superna/sca/logs
```

4. Done

T18000 Quota limit reached on Eyeglass appliance eca logs directory does not have an alarm

if the quota limit on the Eyeglass appliance ecal logs directory is reached there is no alarm to notify administrator. Once the limit is reached the collection of ECA logs is affected. Operation of Eyeglass products is not affected.

Workaround: Manually monitor space consumed in this directory.

T18983 Multiple licenses applied to same Powerscale cluster

In some cases, 2 add-on licenses are assigned to a single Powerscale cluster. For example, 2 Ransomware Defender licenses are applied to 1 Powerscale cluster instead of 1 per Powerscale being managed. This prevents additional Powerscale cluster from being licensed.

Workaround: Contact support.superna.net for assistance.

T19208 Too many open files

If Eyeglass is also managing Ransomware Defender, Easy Auditor or Performance Auditor, under some circumstances when the ECA is unhealthy over a period the heartbeat loop results in condition where Eyeglass is in an error state related to too many open files. Impact once file limit is reached is that application no longer functions properly and eventually will restart.

Workaround: Contact support.superna.net for assistance.

T19276 Configuration file for enhanced HA for misconfigured/unavailable DNS not restored with --anyrelease option

A restore which uses the --anyrelease option does not restore the configuration file used by Eyeglass for its enhanced HA solution for misconfigured/unavailable DNS. This is not an issue for same release restore.

Impact: None if DNS is available and configured properly, the file will be rebuilt as the system comes up.

Workaround: For case where DNS is not available / misconfigured the file is available in the restore zip under the data folder data/fqdnipmapping.json and can be replaced on the new restore appliance manually. For assistance please contact support.superna.net.

T19280 Eyeglass services do not start if retrieval of banned file list on startup hangs

If on Eyeglass startup the step that attempts to retrieve the well known banned file list hangs, no Eyeglass services will be able to start. None of the scheduled jobs such as configuration replication, readiness will run.

Workaround: Steps to workaround are below. Contact support.superna.net if you would like assistance.

1. SSH to Eyeglass as admin user
 2. Run command: `sudo vim /opt/superna/sca/data/system.xml`
 3. Find the line that starts with `<rsw_threat_file_url>`
 4. Modify URL to something that does not resolve
 5. Save your changes
 6. restart Eyeglass services: `sudo systemctl restart sca`
-

T19523 After anyrelease restore or rediscover quota jobs for main and mirror policy are both enabled

If you have corresponding mirror policy for your main SynclQ policies, in the Eyeglass QUOTA jobs it is expected that one quota job is enabled (either OK or Pending) and the other job is Policy Disabled based on which SynclQ policy is active. After using anyrelease restore or running the rediscover command to rebuild the database, the job which should have been policy disabled is enabled and in Pending and both jobs are able to be run.

Impact to Configuration Replication of shares/exports/nfs alias: None. This issue does not affect these jobs. These jobs are active / policy disabled as expected.

Impact to Failover: None

Important: Do not run these jobs manually, they will be executed by Eyeglass during a failover. If you manually run the quota job in the wrong direction it will delete all active quotas.

Workaround: None required.

T19572 Alarms History missing on new 2.5.7 15.2 deployments

For Eyeglass deployment on 2.5.7 15.2 OVA, alarm history is not being saved to the database and the alarms history window in the Eyeglass Alarms window is empty.

Impact: This issue has only been seen to impact viewing the Alarm History. Alarm emails and writing to the `igls_alarms.log` used for syslog forwarding of alarms has not been affected.

Workaround: `igls_alarms` log can be used to reivew alarm history if required. Contact support.superna.net to make modification on the appliance to remedy this issue.

T20371 API error on OneFS 9.x for retrieving DNS settings

The inventory that is collected at midnight for the Cluster Configuration report includes an API call for `network/settings/dns`. For OneFS 9.x clusters this API call fails. This information is collected for information purposes only and failure to retrieve this information has no impact on Eyeglass functionality other than this information will not be available in the Cluster Configuration report.

Workaround: Use Powerscale native tools to document DNS settings.

T20407 igls app report error for OneFS 9.2

The igls add report command may return an error that the cluster version is not supported if Eyeglass is managing OneFS 9.2 cluster.

Workaround: None available. Support can provide assistance on information used to assess DR status.

T21275 Deleted Powerscale cannot be readded

A Powerscale cluster that has been added into Eyeglass can be deleted but results in an error if it is readded: The ip address that you have entered belong to <powerscale>. This cluster is already managed by eyeglass

Workaround: Contact support.superna.net for assistance.

T20808 Alarms window info column does not display full text

If the message in the Info column exceeds the available space, it is truncated and cannot be read from the window.

Workaround: Copy the partial text and paste externally (for example into Notepad) to see full text.

T21820 DR Edition - Manage Services window Eyeglass services status does not display CPU and RAM usage info

In the Manage Services window, the Eyeglass services status may not show the CPU and RAM usage.

Workaround: Use external tools to determine Eyeglass CPU and memory usage. The Manage Services view will provide up time.

T19213 Eyeglass RAM Alarm inconsistent notification

The Eyeglass RAM alarm notification is inconsistent. It may appear in the Active Alarms window or just in the Alarm History window. It may appear in one of the Alarms windows but not send email. It may only send an email on initial detection or it may email each time Configuration Replication runs.

Workaround: Use both Alarm GUI and notification to determine whether you have an issue with RAM configured on Eyeglass.

T21060 Alarms without info cannot be cleared

Some alarms may appear in the alarm window without any info in which case they will also be missing the link to clear the alarm.

Workaround: None available

T23072 Eyeglass RAM alarm for concurrent user login does not clear

If the number of concurrent logged in users falls below the alarm threshold, the alarm does not clear and on logout the timestamp associated with the alarm is incorrectly updated.

Workaround: None available

T23052, T23065, T23066 Log Parser Report Download links not working

In the log parser report generated from the Log Parser icon, the following download links do not download related files:

- Download eyeglass backup for this report
- Download full 'managed device alerts' table
- Download full 'RPO analysis' table

Workaround:

- Download eyeglass backup - none required, the backup had previously been downloaded in order to generate the report
- Download managed device alerts - managed device alerts can be viewed from the Alarms -> Managed Device Alerts tab
- Download RPO analysis table - none available

T23043 Restrictions in Log Parser customer name

Submit button is disabled if the customer name entered in the Log Parser Add New Backup window contains an underscore (_) character.

Workaround: Do not use _ in the customer name in log parser.

T23113 Log Parser does not show link for report when appliance id contains a slash (/)

If the appliance id associated with the backup contains a slash character (/), the log parser report is generated but the link to view the log parser report does not appear in the Log Parser window.

Workaround: The log parser report exists on the file system /opt/data/log_reports/<customer name> with an extra sub-folder where the slash occurs in the appliance id. The associated index.html file can be copied from the appliance with WinSCP in order to be viewed.

T23009 Log parser permission may not be added to admin role on upgrade

On upgrade from a previous release, the admin role may not have the LOG_PARSER permission required to see the Log Parser icon.

Workaround: Edit the admin role and select the LOG_PARSER permission. Logout and login to see the icon.

T23328 igls app report errors

The igls app report command encounters errors reading from the database which prevents all information from appearing the report such as configuration information, job information, failover readiness information.

Workaround: Use the Log Parser GUI functionality to generate the log parse report. How to use the Log Parser GUI can be found [here](#).

T23161 Upgrade to 2.5.8.1 from 2.5.8.1 earlier build fails

An upgrade to latest 2.5.8.1 build from an earlier 2.5.8.1 build fails.

Workaround: Contact support.superna.net for workaround.

DR-896 Runbook Robot Options on GUI were exposed in the 2.5.12 release

The options for an upcoming feature to use SMB mounts for the runbook robot were inadvertently exposed in the Add Managed Device GUI on the eyeglass appliance. These fields are not currently used, so any values entered there will be ignored.

DR-1247 All SMB sessions-login, sg, roboaudit don't work on Onefs's Secure hashing algorithms

SMB user authentication is not supported for SHA256 and SHA512 hashed user passwords.

Workaround: Use AD users for eyeglass logins, security guard and robo audit testing.

DEVSECOPS-258 `libzypp`/`rpm` bug causes installers to fail

`libzypp` version `17.31.22` introduces an incompatibility with the currently available version of `rpm` (`4.14.3` at the time of writing). The following error occurs when the installer attempts to install the RPMs:

```
error: Macro %_dump_posttrans has empty body
```

```
error]
```

Workaround: `libzypp` must be downgraded and locked to prevent the broken from being installed either manually or by the Yast2 Auto Update process:

```
sudo zypper in -y --oldpackage --allow-downgrade 'libzypp<17.31.22'
```

```
sudo zypper addlock 'libzypp<17.31.22'
```

```
ssh -o StrictHostKeyChecking=no -o UserKnownHostsFile=/dev/null -o User=admin 172.19.0.55
igls259:/home/admin * zypper in -y --oldpackage --allow-downgrade 'libzypp<17.31.22'
Loading repository data...
Reading installed packages...
Resolving package dependencies...

The following 2 packages are going to be downgraded:
 libzypp zypper

2 packages to downgrade.
Overall download size: 0 B. Already cached: 4.5 MiB. After the operation, 20.1 KiB will be freed.
Continue? [y/n/v/...? shows all options] (y): y
In cache libzypp-17.31.20-150400.3.40.1.x86_64.rpm (1/2), 2.8 MiB
In cache zypper-1.14.64-150400.3.32.1.x86_64.rpm (2/2), 1.7 MiB

Checking for file conflicts: ..... [done]
(1/2) Installing: libzypp-17.31.20-150400.3.40.1.x86_64 ..... [done]
(2/2) Installing: zypper-1.14.64-150400.3.32.1.x86_64 ..... [done]
igls259:/home/admin * _
```

Known Limitations

Known Limitations for PowerScale OneFS 8.0.0.x with Eyeglass

T507 Cluster Report for OneFS 8.0 missing information

The Eyeglass Cluster Configuration Report for OneFS 8.0 is missing the following information:

- DNS and Subnet information
- File System Explorer
- Protocols - new HDFS, FTP, HTTP settings

Known Limitations for Eyeglass Failover

T939 Eyeglass Access Zone Replication Job in Error after failover

The Access Zone Replication Job associated with the SyncIQ mirror policy configuration replication Job has the following error when the SyncIQ policy source and target path are not identical.

Workaround: Create and update Access Zones manually on source and target cluster and disable Eyeglass Access Zone replication Jobs. With the Eyeglass Access Zone replication Jobs disabled, the Zone Configuration Replication Readiness Jobs will have a status of Unknown. This does not block failover.

T1785 Cannot set ignore flag on subnet pool after failback

It is not supported to apply an igls-ignore flag on a subnet pool that has been failed over and failed back such that the SmartConnect Zone has an igls-original prefix due to the fact that on a subsequent failover the igls-original prefix will not be removed and will leave the Access Zone in a state where both directions are failed over.

Workaround: Manually edit SmartConnect Zone on active cluster to remove the igls-original prefix. Run Configuration Replication and then run the Failover Readiness job to update Zone Readiness.

T2479: Access Zone Failover fails between OneFS 7.2 clusters if Eyeglass also managing OneFS 7.1

For the case where Eyeglass is managing OneFS 7.2 and OneFS 7.1 clusters, an Access Zone failover between OneFS 7.2 clusters will fail as OneFS7.1 linmap command is attempted and fails.

Workaround: Access Zone failover in this Configuration is unsupported as for Eyeglass Inter-version management, it is expected to apply capabilities of lower versions to all versions being managed and Access Zone failover for OneFS 7.1 is not supported. No workaround required.

T3258: Cannot start failover while Eyeglass initial inventory is running

For the case where Eyeglass has been restarted and the initial inventory is running for initial discovery, while the initial inventory is running a failover cannot be started. A “Failover configuration is not valid” message will be displayed in the GUI followed by a message that the target cluster is not managed by Eyeglass.

Workaround: Wait for initial inventory to completed before initiating a failover. Check running jobs windows for the initial inventory job to show completed.

T3774: Failover relies on policy naming: <policy name> and <policy name_mirror>

The Superna Eyeglass failover relies on following naming conventions:

1. First failover A to B- policy name = <policy name>.

The first failover name cannot be <policy name>_mirror.

1. Second failover B to A - policy name = <policy name>_mirror.

Workaround: Manual process on naming the convention above must be followed.

T4808: SPNs not updated for new authentication providers after Access Zone settings changed to “Use all authentication providers” (OneFS 7.2)

If an Access Zone is modified from manually defining the authentication providers to using the “Use all authentication providers” setting in OneFS 7.2, Eyeglass will not update SPNs for any new authentication providers that where not previously provisioned.

Workaround: Manual process required to create these SPNs.

T6229: Existing Failover Logs cannot be reviewed after upgrade to Eyeglass R2.0

Failover logs which were generated from previous releases cannot be viewed from the Eyeglass DR Assistant Failover History view after upgrade to Eyeglass R2.0

Workaround: Generate an Eyeglass Backup and download to your local machine. The Failover logs are contained in the backup archive in the folder failover_logs.

T14321 Zone/Pool Failover Readiness for AD Delegation validation, SPN Readiness validation not supported for Multi-Site failover configuration

For multi-site failover configuration the AD Delegation validation is not supported as it runs in parallel for both the A -> B and A->C resulting in conflicts and errors for both the self and cross AD delegation testing.

For multi-site failover configuration SPN Readiness validation is not supported as there are 2 pools on the B and C clusters with the same igls-original.... SmartConnectZone name and this cannot be provisioned in AD as it does not support duplicate SPNs.

Workaround: For multi-site failover manual verification for AD delegation can be done as documented [here](#) and the DR Dashboard AD Delegation validation can be disabled following documentation [here](#).

SPN Readiness validation warning cannot be disabled and after manual verification that correct SPNs are present can be ignored.

T15611 Pool Readiness Alarms are reported per Zone

Instead of reporting Pool Readiness alarms per Pool they are reported against the Access Zone that is configured for Pool Failover.

Workaround: None required.

DNS Dual Delegation Failover Readiness Validation Supported DNS servers

DNS Dual Delegation Failover Readiness validation is only supported by design for Microsoft DNS server. This validation must be disabled if any other DNS server is being used. This can be done from the Eyeglass command line using the command: `igls adv readinessvalidation set --dualdelegation=false`

DNS Dual Delegation Failover Readiness validation uses PowerScale GroupNet DNS server

The DNS Dual Delegation Failover Readiness validation uses the PowerScale Groupnet DNS as the query server. If the Eyeglass appliance does not have access to the PowerScale Groupnet DNS for example due to firewall restrictions the failover readiness validation will fail.

Workaround: There is an option to configure Eyeglass to use the Eyeglass appliance DNS Server for the validation. Details can be found [here](#).

T17254 Failover does not take into account Powerscale job retries

In some cases Powerscale will retry a job after it fails and eventually if it succeeds the overall status of the job remains in Needs Attention. Failover logic takes the success / fail status from the first attempt only.

T18556 User Quota Replication requires System Access Zone AD Provider

The API used for creating user quotas requires System Access Zone to be configured with an AD provider to be able to resolve the user SID. If the user SID cannot be resolved the quota creation will fail with the error AEC_BAD_REQUEST "Requested persona was not of user or group type".

Workaround: Add an AD provider to the System Access Zone that has a trust relationship with the other domains in other Access Zones in order for SIDs to be resolved.

T19681 Runbook Robot NFS Export not created on target cluster

If NFS Export create and mount step are enabled for Runbook Robot, the Robot export is not created as it should have been on the target cluster causing the robot failover job to fail. This issue does only affect the Runbook Robot job. No impact to regular configuration replication or failover. Workaround: Runbook Robot mount and export creation steps are disabled by default and should be left as disabled.

Known Limitations for Eyeglass Configuration Replication

Multi-Path Exports

T1359 Update NFS Multi-Path Export path(s) may cause transient Configuration Replication Error

Eyeglass uniquely identifies an NFS Export based on its path. When the path is changed this results in a Create and Delete operation in Eyeglass. It may occur that the create is attempted before the Delete is executed. In this case a Configuration Replication error occurs. This is automatically resolved in the subsequent replication cycle when the new export is successfully created.

Export cannot have multiple paths that span multiple Eyeglass Jobs

Export with multiple paths that are protected by different SynclQ policies is not supported. This export configuration is not supported for DR as it would not allow per policy failover and is an unsupported configuration for Eyeglass.

The solution for this is to split the single export into multiple exports each with paths that correspond to a single SynclQ policy.

T1359 Update NFS Multi-Path Export path(s) may cause transient Configuration Replication Error

Eyeglass uniquely identifies an NFS Export based on its path. When the path is changed this results in a Create and Delete operation in Eyeglass. It may occur that the create is attempted before the Delete is executed. In this case a Configuration Replication error occurs. This is automatically resolved in the subsequent replication cycle when the new export is successfully created.

T1743 Multiple export with same path and same client do not show Configuration Replication Error

Multiple exports with the same path are required to have different clients in order to be replicated as per PowerScale default behaviour. In the case where they have been provisioned with same client, Eyeglass Configuration Replication will only show error for this condition on the second configuration replication cycle.

T1847 OneFS 8 Overlapping Access Zone Replication has error

In OneFS 8 where there are Access Zones have identical paths, Eyeglass Access Zone Replication will fail with the following error from the PowerScale cluster:

AEC_CONFLICT "field" "path" "message" "access zone base path */ifs* overlaps with base path */ifs/data/zone* in Access Zone Use the force overlap option to override. In this case disable Eyeglass Configuration Replication Jobs for Access Zones and manually create the Access Zone on the target cluster.

T1972 Snapshot schedule replicated with offset

Snapshot schedule expiration offset has OneFS API bug that adds extra time to snapshot expiration when the snapshot schedule is created. This results in an expiration on the DR cluster, that can be greater than entered on the source cluster. example expire in 20 days will be 22 days on the target cluster. Different units of off set all result in a value greater than entered. After failover the DR (target cluster) value will be synced back to the source (Prod cluster). Thereby losing the original expiry offset and extending the expire time by a new offset from the API error. This has been raised with EMC as SR to resolve.

1. Work around: Before failover ensure a cluster report has been generated (cluster reports icon), or an existing emailed cluster report exists. Post Failover re-enter the original values on the DR snapshot schedules using the cluster report values from the source cluster as a reference.
2. Another option is disable Snapshot Sync jobs in the jobs window if the above workaround does not meet your needs to preserve expiry of snapshot settings.

UPDATE: Resolution for this OneFS issue is available in OneFS 8.0.0.3 **T2046**

Access Zone Replication limitation when all user mapping rules are deleted

Access Zone Replication successfully creates and updates user mapping rules and also successfully deletes user mapping rules except when all user mapping rules are removed from the source. In the case where all user mapping rules are deleted from the source, the Access Zone configuration replication job will not delete all on the target - the user mapping rules remain on the target.

T2241 Incorrect missing SPN alarm issued when PowerScale cluster joined to multiple Domains

In an environment where the PowerScale cluster is joined to multiple Domains, the OneFS SPN check command for a specified domain returns list of SPNs from other domains and lists them as missing. In this case Eyeglass issues an SPN alarm for missing SPNs based on the list returned even if there are no missing SPNs in the domain specified in the check command.

T2779 - Eyeglass Configuration Replication “Full Sync Mode” always updates when Default Settings on Source and Target cluster are not the same

If on the Source and Target cluster for an Eyeglass Configuration Replication Job the “Default Settings” say for SMB are not the same, each replication cycle will perform an update operation even though the shares are already synced and identical. Making the Default Settings the same for both clusters will eliminate this behaviour and return to expected behaviour to not perform the update when shares are determined to already be identical.

T2780 Same host moved to different NFS Export Client list not updated on target

For the cases where:

- same host is provisioned on multiple client list and then one host is removed
- Same host is moved from one client list to another

The change in NFS client list is not replicated to the target cluster. Target cluster client list must be updated manually.

T2908 New Eyeglass Configuration Replication Job cannot recover state and mode from the Eyeglass Fingerprint file.

When a SynclQ Policy is renamed, Eyeglass considers it to be a new SynclQ Policy and therefore creates a new Eyeglass Configuration Replication Job with the new name.

The Eyeglass Fingerprint file which holds Eyeglass Configuration Replication Job Mode and State for recovery does not link the original Job name with the new name and can therefore not be used to recover these properties for the new Eyeglass Job.

T4289 Delete Share or Export may result in temporary Audit error

After a share or export is deleted as part of Eyeglass Configuration Replication Job, the next Eyeglass Configuration Replication Job Audit task may incorrectly expect that the object is not deleted resulting in an alarm such as “ Replication job audit failed" - "objects not found on source or target cluster, hence audit fails” . The error is cleared on the next Eyeglass Configuration Replication Job where the Audit task correctly does not try to audit the deleted object.

T5972 No Error Message for Duplicate NFS Export on OneFS 7.2 Configuration Replication Failed

Duplicate NFS Export on OneFS 7.2 Configuration Replication failure is expected, however in this case there is no specific Info associated with failed step to identify the issue.

T14936 Short SPN not created during Configuration Replication

Eyeglass Configuration Replication will only create full version of SPN, no short version is created. Note that Access Zone and Pool Failover update both short and full version of SPN. If short version is required it can be manually added using AD tools.

T17097 Eyeglass Configuration Replication direction follows Enable/Disable state of SyncIQ policies

Eyeglass Configuration Replication source cluster is the cluster of the enabled SyncIQ policy. If there is a mirror policy and both SyncIQ policies are enabled Eyeglass enters a defensive state showing Policy Disabled for both and no Configuration Replication is done. If a SyncIQ policy is mistakenly enabled on the read only cluster Eyeglass does not evaluate the read/write state and will use the read only cluster as the source cluster for its Configuration Replication job.

Known Limitations for Eyeglass Features

T2350: Quota Self Serve Portal: Local Group Quotas not displayed when logged in with Local Group User

Quotas associated with a Local Group (for example wheel) are not displayed in the Quota self serve portal when logged in as a Local Group User for that group.

T1962: Default Role incorrectly shows Delete option

Eyeglass User Roles Default Roles incorrectly provide the option to be deleted when in fact they cannot be deleted.

Workaround: None Required. If the Delete option is selected the Default Role is not deleted.

T7980: Cluster Storage Monitor AD Group Template Quota Creation does not created group quota for nested AD Groups

If an AD Group has sub-groups (nested groups) is configured as a Template for automated group quota creation, no group quotas will be created for sub-groups.

Workaround: Each group that requires automated group quota creation must be explicitly added to the relevant share permissions.

T8362: Cluster Storage Monitor AD Group Template Quota Creation does not respect highest quota setting user quota in nested AD Groups

If an AD Group has sub-groups (nested groups) is configured as a Template for automated user quota creation, user quota creation follows explicitly the quota limit for the sub-group when the user already has a quota for a higher limit. In this case, what should have happened is that template setting is ignored if there is already an existing user quota with a higher limit.

Workaround: Avoid use of nested AD groups for automated user quota creation.

T8193: special characters in Cluster storage monitor AD managed quota templates is not supported

If an AD Group templates, if the AD group name has special characters in the AD group name the quotas will not be applied.

Workaround: Avoid use of special characters when creating AD groups for AD managed quotas.

T9622: Unlock My Files! does not indicate error when PowerScale node is not reachable

If an PowerScale node is unreachable when Eyeglass is searching for open files there is no error message for the unreachable PowerScale nodes.

Workaround: None available.No open files displayed for unreachable nodes.

T15139 Data Config Migration Concurrent Jobs Limitation

When 2 Data Config Migration Jobs are started concurrently, each runs a separate Configuration Replication Job and the Configuration Replication Job cannot run concurrently. First one must complete before the second one can start.

Workaround: Recommend to run 1 Data Config Migration job at a time.

DR-136 Login with AD users leads to read-only Eyeglass

Issue: AD users cannot be added to user roles until a Powerscale cluster has been added.

Workaround: Add the powerscale cluster to inventory before modifying user roles.

Closing this task as done since this is not something we will ever fix.

Known Limitations for Eyeglass General

T2289 Backup Archive Job is not always displayed in the Running Jobs window

In some cases after a Backup Archive job is initiated it will not appear as a running task in the Jobs / Running Jobs window. Archive is still created and available for download on completion.

T2908 Renamed SynclQ Policy does not link to RPO Reports from original SynclQ Policy Name

When a SynclQ Policy is renamed, Eyeglass considers it to be a new SynclQ Policy. Therefore RPO Reporting for the original SynclQ Policy name will not be linked to RPO reporting for the new SynclQ Policy name.

T3170 Pending Quota Requests are not preserved on failover

If a failover is done while there are Quota Pending Requests, the Pending Requests are lost as the quota to which the request was originally made no longer exists on the original cluster after failover. The pending quota request will appear in the Quota Requests History in Error state.

T4579 Upgrade from 1.5.4 to 1.9 and greater Failover History retrieves Failover Log for SynclQ Job Reports

After an upgrade from 1.5.4 to 1.9 or greater, in the DR Assistant -> Failover History list the link to open SynclQ Job Reports opens the Failover Log due to fact that prior to this

release Failover Log and SyncIQ Job Report log were combined. In this case you are able to see the SyncIQ Job Reports related to failover at the bottom of the Failover Log.

T6300 After an Eyeglass restore with the `-anyrelease` option the print screen functionality for SyncIQ Job Reports and Eyeglass backups may be in error

After an Eyeglass restore to a new appliance using the `--anyrelease` option, print screen functionality may no longer be working due to an incorrect permission setting. This impacts SyncIQ Job Reports which will be missing the charts and generating an Eyeglass backup with print screens.

To work around this issue:

1) ssh to the eyeglass appliance and login with the admin account (default password 3y3gl4ss)

2) assume root user by typing

```
sudo su -
```

And entering the admin password

3) vi `/opt/superna/sca/data/Screenshots.json` and write "`<placeholder>`" as a value in the "plain_text" field and then save it.

4) Copy and paste the following commands:

```
str=$(sudo cat /dev/urandom | tr -dc 'a-zA-Z' | fold -w 12 | head -n 1)
```

```
echo -e "$str\n$str" | passwd screenshots
```

```
sed -i "s/<placeholder>/$str/" /opt/superna/sca/data/Screenshots.json
```

5) Start a backup with print screens and follow in Running Jobs to verify the backup completes successfully.

T12034 Eyeglass appliance rediscover does not preserve Eyeglass Job state unless Configuration Replication has run

If a change is made to an Eyeglass Job state or Job type and then there is an appliance rediscover before configuration job has been run the changed Job state / type will be lost.

T16137 Anyrelease restore does not restore all Ransomware Defender and Easy Auditor settings

There is no restore of settings from release 2.5.4 and earlier. For release 2.5.4 and earlier continue to capture all Ransomware settings (False Positive, Ignore List, Allowed Extensions, Security Guard) and Easy Auditor settings (Active Auditor Trigger settings, RoboAudit). Post restore verify settings and update where required before cluster up on ECA.

In all cases, restoring an Eyeglass backup using the --anyrelease option will not restore following Ransomware Defender and Easy Auditor settings:

Ransomware Defender: Event History, Threats Detected

Easy Auditor: Finished Reports, Scheduled Reports, Saved Queries

T16729 Role Based Access Control (RBAC) Known Limitations

- Isilon local users are not supported (Eyeglass local users are supported)
 - Eyeglass doesn't resolve AD groups with @ & or ' in the name
-

T16821 anyrelease restore restrictions for restore to 2.5.7

1) Eyeglass DR Edition with version lower than 2.5.5 cannot be upgraded to 2.5.7 using the anyrelease option. Eyeglass must be upgraded to a minimum of 2.5.5 before anyrelease restore to 2.5.7 can be done.

2) Ransomware Defender, Easy Auditor and Performance Auditor deployments cannot use the anyrelease restore option to upgrade to a new appliance running 2.5.7. For case where a backup & restore is required due to 42.3 OS on original deployment, a backup & restore to 2.5.6 will have to be done first followed by an upgrade to 2.5.7 or in place OS upgrade prior to 2.5.7 upgrade.

Eyeglass Upgrade requires disk usage < 80%

Eyeglass disk usage must be lower than 80% for upgrade run file to succeed. Please contact support.superna.net for assistance to clear up disk space on the Eyeglass appliance.

T19368 Copy to Clipboard Size Limitation

The amount of information that can be copied using the Copy to Clipboard functionality in Eyeglass is limited by the operating system clipboard limits.

- Failover log is available on the Eyeglass appliance here:
`/srv/www/htdocs/failover_logs`
- Where Did My Folder Go set more restrictive filter to produce smaller set of results

T21890 OneFS Effective Cluster Version incorrect

For an Eyeglass installation with multiple clusters with different OneFS versions, adding or removing a cluster may result in temporary assignment of incorrect Effective Cluster Version. This is resolved the next time Configuration Replication runs.

Known Limitations for REST API

T18079 REST API - Change Eyeglass Configuration Job Disable/Enable must be done at the same time as Job Type Change

The API to change Eyeglass Configuration Job state for Disable/Enable must be done together with a job state change in order to succeed.

REST API retrieval of Jobs Known Limitation

Retrieving information about a Configuration Replication Job or DR Readiness Job is available while the job is running and for 15 minutes once the job has completed. This is the same behaviour that is available from the GUI via the Jobs/Running Jobs window.

© Superna Inc© Superna Inc

1.2. Current Release - Release Notes Platform

[Home](#) [Top](#)

Release date	Version
06/19/2023	1.1.0

- [What's New in Superna Platform](#)

What's New in Superna Platform

© Superna Inc

1.3. Current Release - Release Notes

Ransomware Defender AWS

[Home Top](#)

Release Date	Version
09/09/2023	3.2.0

- [What's New in Superna Eyeglass Ransomware Defender AWS Edition Release 3.2.0](#)
- [New in 3.2.0](#)
 - [FSx lockout](#)
- [Fixed in 3.2.0](#)
 - [RWDAWS-744 \[Multi Account Support\] : FSx - permissions to add in cloudformation template for fsx cross account lockout/restore functionality](#)
- [New in Superna Eyeglass Ransomware Defender AWS Edition Release 3.1.1 \(06/29/2023\)](#)
- [Fixed in 3.1.1](#)
 - [RWDAWS-386 \[Webhooks\] : RSW event - do not send Security guard events](#)
 - [RWDAWS-377 \[Webhooks\] : RSW event - remove MINOR option from event severity filter](#)
 - [RWDAWS-419 \[Cyber Recovery Manager\] : Ransomware event gets triggered when recovery job moves file to quarantine directory](#)
 - [RWDAWS-416 \[Cyber Recovery Manager\] : Bucket versioning status is not shown correctly on UI](#)
 - [RWDAWS-482 \[Cyber Recovery Manager\] Bucket versioning enabled - file objects are not restored to the most recent version](#)
 - [RWDAWS-491 \[Active Auditor\] : Can not trigger CRTA policy events](#)
 - [RWDAWS-231 Security Guard Log Viewer - Copy to Clipboard doesn't work](#)
 - [RWDAWS-434 Add Managed Device UI - when select 'show protected buckets only' option, no data is shown](#)

- RWDAWS-236 UI hang issues plus unrelated error messages are shown randomly
- RWDAWS-355 Able to trigger TD15 when bytes match percent tolerance is greater than default value
- RWDAWS-417 [Cyber Recovery Manager] : Missing S3 permissions for CloudFormation template
- What's New in Superna Eyeglass Ransomware Defender AWS Edition Release 3.1.0 (05/03/2023)
- Fixed in 3.1.0
 - RWDAWS-235 [Ignored List] : able to generate TD events from paths added to the ignored list
 - RWDAWS-233 Remove 'Create/Delete Snapshot' option from Actions menu for an active or archived event
 - RWDAWS-182 False alarm about eca node version doesn't match eyeglass version
 - RWDAWS-98 Uploading files to s3 buckets triggers TD15
 - RWDAWS-240 [Monitor Only Settings] : events from path added to the monitor only settings should be in monitor mode
 - RWDAWS-241 Cluster up may get stuck sometimes at Initializing hbase schema step
 - RWDAWS-179 [Active Auditor]: Monitor only mode - generic TD's can be raised as a warning, major and critical
 - RWDAWS-239 Data Start and end times on easy audit reports are sometimes inaccurate
- Known Issues
 - RWDAWS-728 FSx - Audit events can not be read in Eyeglass if the share has space in the name
 - RWDAWS-723 [FSx Agent]: lockout job is stuck when SupernaFSxService is not running
 - RWDAWS-749 [Active Auditor] : S3 - unable to trigger DLP events in eyeglass
 - RWDAWS-672 [Stack Deployment] : unable to delete FSx event capture stack

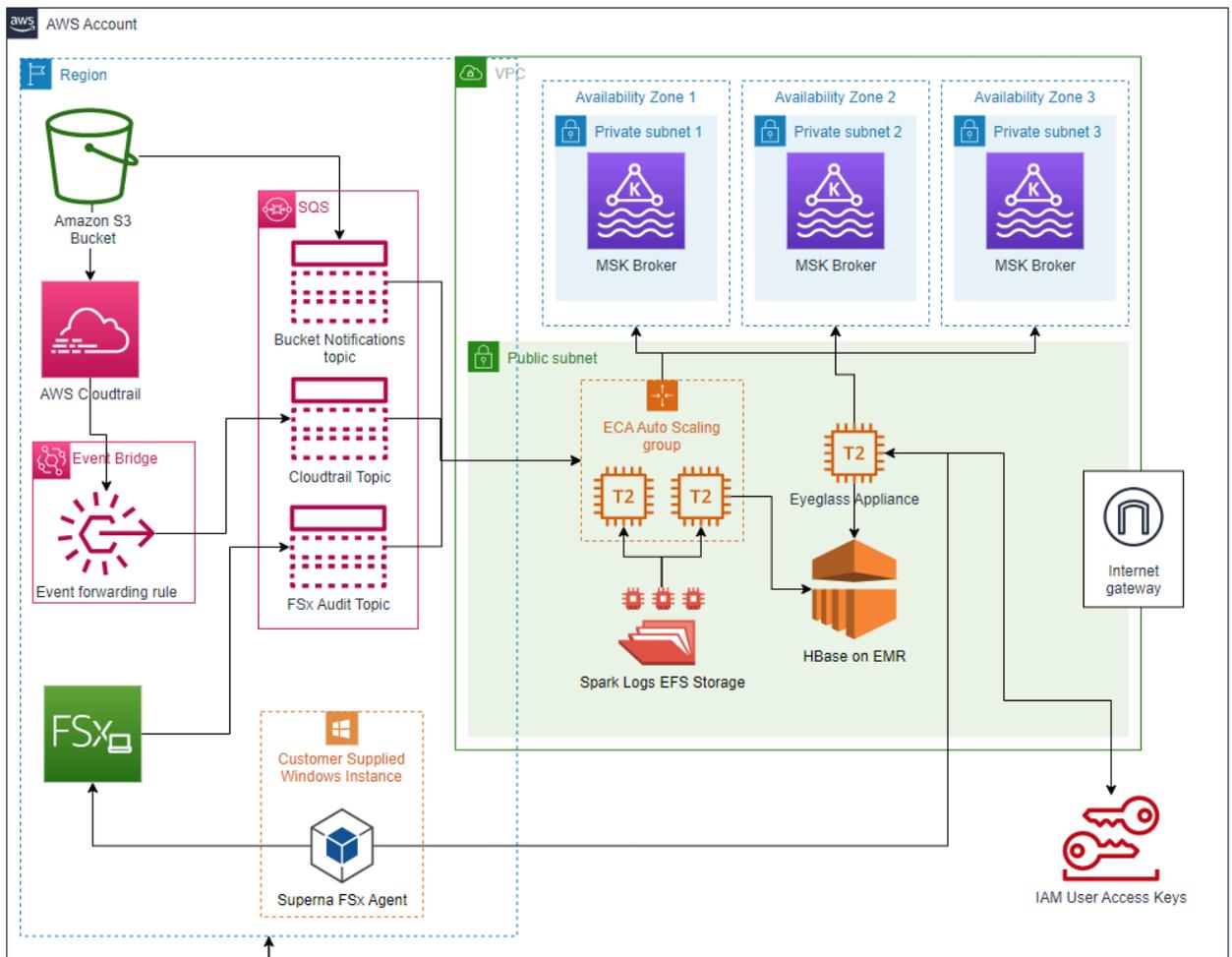
- [RWDAWS-787 \[Stack Deployment\]](#) : unable to delete rwdaws stack as the EC2Role fails to delete
- [RWDAWS-722 \[Fsx Agent\]](#): Unable to install FSx agent installer using the wizard
- [RWDAWS-852 \[Monitor Only Settings\]](#) : FSx - path format supported is not correctly shown in the info section
- [RWDAWS-853 \[Monitor Only Settings\]](#) : FSx - Edit path ui not working correctly
- [RWDAWS-854\[Monitor Only Settings\]](#) : FSx - Add new user UI issues

What's New in Superna Eyeglass Ransomware Defender AWS Edition Release 3.2.0

New in 3.2.0

FSx lockout

The FSx agent is a Windows service that runs on a Windows EC2 instance. The customer provides this instance and must be joined to the same Active Directory Domain as the FSx server.



Fixed in 3.2.0

RWDAWS-744 [Multi Account Support] : FSx - permissions to add in cloudformation template for fsx cross account lockout/restore functionality

FSx - permissions to add in cloudformation template for fsx cross account lockout/restore functionality.

Workaround:

1. Delete the FSx-event-capture stack if already added
2. Add missing permissions manually to EC2Role of the stack
3. And then add the FSx filesystem to eyeglass
4. FSx event detection/lockout/restore works as expected

New in Superna Eyeglass Ransomware Defender AWS Edition Release 3.1.1 (06/29/2023)

Fixed in 3.1.1

RWDAWS-386 [Webhooks] : RSW event - do not send Security guard events

SG events are sent to webhook endpoint if matches filter criteria.

RWDAWS-377 [Webhooks] : RSW event - remove MINOR option from event severity filter

- For RSW events, severity can only be WARNING, MAJOR and CRITICAL.
 - There is no MINOR severity
-

RWDAWS-419 [Cyber Recovery Manager] : Ransomware event gets triggered when recovery job moves file to quarantine directory

Ransomware event gets triggered when recovery job moves file to quarantine directory

RWDAWS-416 [Cyber Recovery Manager] : Bucket versioning status is not shown correctly on UI

In AWS, when bucket version = disabled , on GUI its shows ERROR_GETTING_STATUS

RWDAWS-482 [Cyber Recovery Manager] Bucket versioning enabled - file objects are not restored to the most recent version

Bucket versioning enabled - file objects are not restored to the most recent version

RWDAWS-491 [Active Auditor] : Can not trigger CRTA policy events

CRTA policy events can not be triggered in eyeglass

RWDAWS-231 Security Guard Log Viewer - Copy to Clipboard doesn't work

Security Guard Log Viewer - Copy to Clipboard doesn't work

RWDAWS-434 Add Managed Device UI - when select 'show protected buckets only' option, no data is shown

When select "show protected buckets only" on 'Add Managed Device' UI, it shows no data (even though protected buckets are added)

RWDAWS-236 UI hang issues plus unrelated error messages are shown randomly

Noticing that sometimes eyeglass UI hangs or takes time to load UI elements OR randomly triggers user logoff from GUI. In between also see some random error messages pop up window

RWDAWS-355 Able to trigger TD15 when bytes match percent tolerance is greater than default value

Able to trigger TD15 when bytes match percent tolerance is greater than default value

RWDAWS-417 [Cyber Recovery Manager] : Missing S3 permissions for CloudFormation template

Missing S3 permissions for CloudFormation template

What's New in Superna Eyeglass Ransomware Defender AWS Edition Release 3.1.0 (05/03/2023)

Fixed in 3.1.0

RWDAWS-235 [Ignored List] : able to generate TD events from paths added to the ignored list

1. UI element not shown properly
 2. path hint shows as "<Bucket>/Path/To/Object". Close UI, re-open again, path shows as "/ifs/".
 3. rsw event should not be generated for paths added to ignored paths list.
-

RWDAWS-233 Remove 'Create/Delete Snapshot' option from Actions menu for an active or archived event

For any active or archived TD events, still seeing option to create/delete snapshot.

RWDAWS-182 False alarm about eca node version doesn't match eyeglass version

Seeing informational alarm raised about “ECA node version does not match the Eyeglass version“

RWDAWS-98 Uploading files to s3 buckets triggers TD15

Observing that TD15 is just triggered by uploading files to AWS s3 bucket. For upload the event type is OBJECT_WRITE.



RWDAWS-240 [Monitor Only Settings] : events from path added to the monitor only settings should be in monitor mode

For a path added to Monitor Only Settings, TD events should be generated in monitor mode and warning severity. But currently able to get events as WARNING/MAJOR/CRITICAL.

RWDAWS-241 Cluster up may get stuck sometimes at Initializing hbase schema step

Eca cluster up may get stuck at Initializing hbase schema step.

RWDAWS-179 [Active Auditor]: Monitor only mode - generic TD's can be raised as a warning, major and critical

Monitor only mode - generic TD's can be raised as a warning, major and critical.

RWDAWS-239 Data Start and end times on easy audit reports are sometimes inaccurate

When running an audit report, the timestamps of the resulting dataset's first and last audit records are displayed on the UI.

Known Issues

RWDAWS-728 FSx - Audit events can not be read in Eyeglass if the share has space in the name

FSx - Audit events can not be read in Eyeglass if the share has space in the name.

Workaround: None.

RWDAWS-723 [FSx Agent]: lockout job is stuck when SupernaFSxService is not running

- The lockout job is stuck in this case and keeps running. Unable to cancel this job.

- The event will expire at a set time, but the lockout job will keep running.

Workaround:

Restart SCA service on eyeglass → `systemctl restart sca`

RWDAWS-749 [Active Auditor] : S3 - unable to trigger DLP events in eyeglass

S3 - unable to trigger DLP events in Eyeglass.

Workaround: None.

RWDAWS-672 [Stack Deployment] : unable to delete FSx event capture stack

Unable to delete FSx event capture stack.

Workaround:

1. Login to AWS console where fsx-event-capture stack is deployed
 2. Open Amazon Kineses → Data streams and then delete the created data stream manually
 3. Next, delete the superna-fsx-event-capture stack manually
-

RWDAWS-787 [Stack Deployment] : unable to delete rwdaws stack as the EC2Role fails to delete

When trying to delete the RWDAWS stack manually from the AWS console, the stack fails to delete because the EC2Role logical ID fails to delete.

RWDAWS-722 [Fsx Agent]: Unable to install FSx agent installer using the wizard

Unable to install FSx agent installer using the wizard

RWDAWS-852 [Monitor Only Settings] : FSx - path format supported is not correctly shown in the info section

1. The format to enter monitor-only paths for Fsx shares is not shown correctly in the info section. It shows to enter the path as *share/path/subpaths*.
2. This path shown under the info section is not supported for Fsx - `***.java` - Matches any object name ending in `.java` on any path in any share. “

Workaround: Enter the path using a backward slash as supported by Windows. E.g., *lshare\path*** (instead of `"/`)

RWDAWS-853 [Monitor Only Settings] : FSx - Edit path ui not working correctly

Unable to edit Fsx paths on the monitor-only settings page. The NE information is missing when editing paths, and the save button won't enable it.

Workaround: On the Edit path window, switch between the 'target NE types' field to populate NE information for Fsx server and then can edit paths successfully.

RWDAWS-854[Monitor Only Settings] : FSx - Add new user UI issues

For Monitor only settings page - Add New User UI:

- The new user field does not provide a hint for the only user format we support for AD;
- AD information is not populated.

Workaround:

1. The user name should be entered in the format: user@domainname;
2. Select NE first to populate AD information.

© Superna Inc

1.4. Current Release - Release Notes

Ransomware Defender

[Home](#) [Top](#)

Release date	Version
11/28/2023	2.6.4-23365

- [What's New in Superna Eyeglass Ransomware Defender Edition Release 2.6.4 \(11/28/2023\)](#)
- [Supported OneFS releases](#)
- [Supported Eyeglass releases](#)
- [Active Directory Compatibility](#)
- [End of Life Notifications](#)
- [New in Superna Eyeglass Ransomware Defender Edition Release 2.6.3 \(09/28/2023\)](#)
- [Fixed in 2.6.3](#)
 - [RWD-524 Webhook - missing share list for lockout alarm](#)
- [New in Superna Eyeglass Ransomware Defender Edition Release 2.6.2 \(09/01/2023\)](#)
- [New in 2.6.2-23282](#)
- [What's New in Superna Eyeglass Ransomware Defender Edition Release 2.6.1 \(08/03/2023\)](#)
- [What's New in Superna Eyeglass Ransomware Defender Edition Release 2.6.0 \(06/29/2023\)](#)
- [Fixed in 2.6.0](#)
 - [RWD-279 Lockout API returns response code 500 for ECS IAM User](#)
 - [RWD-365 ECS version 3.8 is now supported in Ransomware Defender for ECS and AirGap for ECS](#)

- [What's New in Superna Eyeglass Ransomware Defender Edition Release 2.5.12 \(05/09/2023\)](#)
- [Fixed in 2.5.12](#)
 - [RWD-380 TD11 is not triggered as described in the documentation when using ECS](#)
- [What's New in Superna Eyeglass Ransomware Defender Edition Release 2.5.11 \(04/03/2023\)](#)
- [New in 2.5.11- 23110](#)
- [What's New in Superna Eyeglass Ransomware Defender Edition Release 2.5.10 \(03/06/2023\)](#)
- [Fixed in 2.5.10](#)
 - [RWD-207 Files displayed after the hour-long wait](#)
 - [RWD-192 Kafka topic empty after cluster down/up](#)
- [Support Removed in Eyeglass Release 2.5.9.1](#)
- [Deprecation Notices](#)
- [What's New in Superna Eyeglass Ransomware Defender Edition Release 2.5.9.1 \(02/14/2023\)](#)
- [Fixed in 2.5.9.1](#)
 - [RWD-228 Syntax error in on-boot preventing proper startup timing.](#)
 - [RWD-222 enable zkcleanup.timer by default](#)
 - [RWD-145 \[RWD-NFS Event\] Major & critical events are locked out with default rule when reach threshold value even if - igls rsw nfsevents set --enabled=snapshotonly](#)
 - [RWD-146 \[RWD-NFS Event\] Lockout option in Actions is also removed for SMB event when set igls rsw nfsevents set --enabled=snapshotonly](#)
 - [RWD-113 Wrong Ransomware event state when created with POST /v2/ransomware/lockout/{user}](#)
 - [RWD-114 Creating Critical Path Snapshots is blocked](#)
- [New in Superna Eyeglass Ransomware Defender Edition Release 2.5.9.1](#)
- [What's New in Superna Eyeglass Ransomware Defender Edition Release 2.5.9 \(11/30/2022\)](#)

- Fixed in 2.5.9
- New in 2.5.8.1-22116
- Fixed in 2.5.8.1-22116
 - Technical Advisory 31 - Ransomware Defender NFS Event Detection Always Enabled in 2.5.8.1-22080/22100
- New in 2.5.8.1-22100
- Fixed in 2.5.8.1-22100
- New in 2.5.8.1-22080
 - T22197 Ransomware Defender Read-Only Role
 - T22328 Ransomware Defender Event csv file storage
 - T20285 Action menu for historical events now has option to restore access
- Fixed in 2.5.8.1-22080
 - T21207 Custom Snapshot Expiry not preserved after modifying Settings on Threshold menu
 - T21261 Cannot edit a user configured in the Ignored List or Monitor Only Settings
- New/Fixed in 2.5.8-22028
- New in 2.5.8-21330
- Fixed in 2.5.8-21330
- Security
 - T22171 - Log4j Vulnerability - Upgrade to Log4j 2.17.0 (2.5.8-21330 and higher Log4j 2.17.0)
- New in 2.5.8-21306
 - Ransomware Defender Snapshot Management Enhancements
 - T19619 Critical Path Snapshot
 - T19823 Snapshot Budget
 - T15666 New Behaviour Detections Enabled
 - T21215 New SmartAirgap API
 - NEW - OneFS 9.3 Support
- Fixed in 2.5.8-21306

- T22033 Log4j Vulnerability - CVE-2021-44228
- T11832 Ransomware Security Event which is promoted from Warning to Major does not respect Major Grace Period
- T18985 igls rsw restoreaccess cannot restore access for unresolvable user
- Technical Advisories
- Known Issues
- Threat Detection
 - T4151 Action Window Event Action History does not show Unreachable Cluster
 - T3732 Restored permission may be incorrect for consecutive lockouts
 - T4081 Time Zone Mismatch between Ransomware Defender Security Guard Job History and Event History dates
 - T22321 Escalation from major to critical will not change GUI status and lockout delay is blocked
 - T4777 Snapshots not created for any Events that are Active when the Snapshot feature is enabled
 - T4819 Empty Event History List
 - T4950 Alarm text for failed Snapshot delete references Snapshot create
 - T4955 Subsequent Create Snapshot action will delete reference to previously created snapshots if an error occurs during the create
 - T5024 Major Events may reappear in the Active Events list after being recovered
 - T5756 Error on restoring permissions does not raise an alarm
 - T5954 Events that are promoted to Major due to multiple event “Upgrade to Major” are locked out immediately
 - T6728 Extensions with special characters cannot be removed from the ignore list
 - T7062 User may not be locked out in a multi-user security event
 - T7190 Active Events may show State of Warning instead of Monitor when Monitor Mode is enabled
 - T11586 NFS Lockout Event Information does not include NFS Export path

- T11590 NFS Lockout Event does not generate an PowerScale snapshot
- T14339 Restore Access Alarm must be manually cleared
- T15198, T15650 Ransomware Events may have inaccurate Signal Strength or may be reprocessed
- T15639 T18812 Error replicating AD Group or Local User Run as Root SMB permissions affects Lockout and Restore
- T16229 GUI incorrectly reports error when manually creating a snapshot
- T16462 NFS lockout may fail
- T18271 Ransomware Event State incorrect shows success when Powerscale is unreachable during restore operation
- T18643, T19217 State of Active Event shows WARNING when it should be MONITOR for File Filter in Monitor
- T18718 igls rsw allowed files remove option not working
- T18852 Ransomware Defender does not detect where path has square brackets []
- T18887 Security Guard in Learned Thresholds prevents Security Guard job from detecting
- T18895 Ransomware Learned Threshold list doesn't open first time
- T19040 After upgrade to 2.5.7, Ransomware Events in Event History do not display the Signal Strength correctly
- T19106 Acknowledge/Archive options not blocked while lockout in progress
- T19198 Multiple concurrent Major Events not upgraded to Critical based on "Upgrade to Critical (events)" setting
- T19236 Honeypot file detector incorrectly crosses Major threshold in Monitor Mode
- T19356 Files/Folders with language characters not displayed properly in CSV and email
- T19409 Well known extension detection not working under some circumstances
- T20094 CLI command to restore access does not work when user name contains special characters

- T23012 Restore access for NFS lockout from Event History does not complete
- Security Guard
 - T4197 Security Guard Error for Unlicensed Cluster
 - T4228 Security Guard Temporary Errors
 - T4965 Security Guard User Authentication Fails
 - T15175 Existing Security Guard Logs lost formatting after upgrade to 2.5.6
- Manage Services
 - T4192 Manage Services status not accurate after ECA Node Down
- General
 - T4230 Blank Ransomware Defender Window
 - T4183 Refresh does not work for Ransomware Defender multi-page lists
 - T15457 HTML 5 vmware vcenter bug on OVA deployment
 - T4336 Eyeglass Restore does not restore Security Guard Job History
 - T4549 Ransomware Defender Settings Submit button enabled when no changes made
 - T6617 PowerScale Directory Selector does not display hidden directories
 - T18810 GUI not updated after cancelling an operation to switch modes
 - T18660 Cannot use cloudapps URL to access Well Known Ransomware File Extension list
 - T22450 Easy Auditor Event Rate alarm for Ransomware Defender Only deployments
 - RWD-301 Error getting events - for NFS exports in Recovery Manager
 - RWD-319 RSW events affected files are not presented in email
 - RWD-362 Support ECS on RWD when turboaudit REST api is configured
 - RWD-443 Easy auditor events only receiving and forwarding one signal and one file in file list despite of number of files and type of events
 - RWD-535 Webhook - redundant lockout alarm when lockout/restore
- Features
 - RWD-217 Event fails to upgrade with multiple user (ECS events only)
 - RWD-85 zookeeper cleanup cron is not running as scheduled

- RWD-74 zookeeper cleanup cron is not running as scheduled
- RWD-246 Files with non-ASCII characters fail to recover
- Known Limitations
- Threat Detection
 - T6914 Some extensions still result in lockout when added to the ignore list
 - T15705 After upgrade to 2.5.6 cannot download CSV for Ransomware Event Files from events detected in prior releases
 - T16723 Error on Lockout of Shares on DR cluster
 - T17287 Many Access Zones slows down creation of snapshots and lockout
 - T7574 Option to set learned threshold for Security Guard in RESTORED_USER_ACCESS state
 - T18733 Ransomware Defender Affected Files Download Menu Naming
- General
 - T16137 Anyrelease restore does not restore all Ransomware Defender and Easy Auditor settings
 - T16821 anyrelease restore restrictions for restore to 2.5.7
 - T20370 Monitor Only Settings Client IP applies to all PowerScale clusters
 - T21852 RSW - Cannot configure and run SG after anyrelease backup and restore from an earlier build
 - T21208 Snapshots taken using Action Menu for Ransomware Defender Event follow Ransomware / Snapshots settings
 - T21110 Ransomware Defender / Snapshots User Share Snapshot Settings also applies for NFS detections
 - Well Known Ransomware File Extension Whitelist management is not available when a proxy used
 - T17624 Ransomware Defender NFS detection creates snapshot on SMB shares with Everyone permission
 - RWD-75 Page-1 gets hide when navigate to Page-2 & archive all events from this page
 - RWD-236 [RWD-NFS Event] User is displayed as "Root" or Sid ID instead of EXP:<client_ip>_<user_id>

- [RWD-453](#) Only 100 affected files are listed in the webhooks event which triggers upon changing the state of RSW event

What's New in Superna Eyeglass Ransomware Defender Edition Release 2.6.4 (11/28/2023)

Supported OneFS releases

8.2.0.x

8.2.1.x

8.2.2.x

9.0

9.1

9.2.x

9.3

9.4 via the February RUP 9.4.0.12 (PSP-3079) released Feb 8th 2023

9.4.0.14

9.5.x.x. (minimum version 9.5.0.1)

9.5.0.5

Supported Eyeglass releases

Superna Eyeglass Ransomware Defender Version	Superna Eyeglass Version
--	--------------------------

2.6.3-23292	2.6.3-23292
2.6.2-23282	2.6.2-23282
2.6.1-23250	2.6.1-23250
2.6.0-23219	2.6.0-23219
2.5.12-23175	2.5.12-23175
2.5.11-23110	2.5.11-23110
2.5.8.1-22080	2.5.8.1-22080
2.5.8-22028	2.5.8-22028
2.5.8-21330	2.5.8-21330
2.5.8-21306	2.5.8-21306
2.5.7.1-21161	2.5.7.1-21161
2.5.7.1-21140	2.5.7.1-21140
2.5.7-21096	2.5.7-21096
2.5.7-21081	2.5.7-21081
2.5.7-21068	2.5.7-21068
2.5.6-20263	2.5.6-20263

Active Directory Compatibility

Ransomware Defender Versions	Supported Active Directory Versions
2.5.9, 2.5.8, 2.5.7, 2.5.6 all versions	Microsoft Active Directory 2012, 2016

End of Life Notifications

End of Life Notifications for all products are available [here](#).

New in Superna Eyeglass Ransomware Defender Edition Release 2.6.3 (09/28/2023)

Fixed in 2.6.3

RWD-524 Webhook - missing share list for lockout alarm

The lockout alarm in the webhook does not list shared information.

Workaround: None.

New in Superna Eyeglass Ransomware Defender Edition Release 2.6.2 (09/01/2023)

New in 2.6.2-23282

We'd like to highlight a specific update. The command `ecactl cluster down` now operates in the background mode by default. If you prefer the previous behaviour, you can still achieve it by running the command with the `-serial` option.

What's New in Superna Eyeglass Ransomware Defender Edition Release 2.6.1 (08/03/2023)

What's New in Superna Eyeglass Ransomware Defender Edition Release 2.6.0 (06/29/2023)

Fixed in 2.6.0

RWD-279 Lockout API returns response code 500 for ECS IAM User

Lockout API returns response code 500 for ECS IAM User

RWD-365 ECS version 3.8 is now supported in Ransomware Defender for ECS and AirGap for ECS

What's New in Superna Eyeglass Ransomware Defender Edition Release 2.5.12 (05/09/2023)

Fixed in 2.5.12

RWD-380 TD11 is not triggered as described in the documentation when using ECS

TD11 is not triggered as described in the documentation when using ECS

What's New in Superna Eyeglass Ransomware Defender Edition Release 2.5.11 (04/03/2023)

New in 2.5.11-23110

Zero Trust API now supports locking out ECS users.

What's New in Superna Eyeglass Ransomware Defender Edition Release 2.5.10 (03/06/2023)

Fixed in 2.5.10

RWD-207 Files displayed after the hour-long wait

Tree View and All File Activity view will show content only after an hour-long wait.

RWD-192 Kafka topic empty after cluster down/up

kafka topic will reset after cluster down/up

Count and Size will reset to zero

- before cluster down/up
- after cluster down/up

Support Removed in Eyeglass Release 2.5.9.1

No features removed at this time

Deprecation Notices

No deprecation notices at this time.

What's New in Superna Eyeglass Ransomware Defender Edition Release 2.5.9.1 (02/14/2023)

Fixed in 2.5.9.1

RWD-228 Syntax error in on-boot preventing proper startup timing.

Workaround: not necessary; verify startup has finished on other nodes, if applicable, before attempting to use the ECA.

RWD-222 enable zkcleanup.timer by default

As an ECA user, I don't want to have to run `systemctl enable --now zkcleanup.timer` to start the service. This should be run by default on install/upgrade.

RWD-145 [RWD-NFS Event] Major & critical events are locked out with default rule when reach threshold value even if - `igls rsw nfsevents set --enabled=snapshotonly`

Major & critical events are locked out with default rule when reach threshold value even if -

`igls rsw nfsevents set --enabled=snapshotonly`

Steps-

- 1.Set `igls rsw nfsevents set --enabled=snapshotonly` in eyeglass
- 2.Raise NFS Event with Major/Critical severity (Detector Mode -Enforcement)
3. Observe Locked out event with critical severity & Major event locked out after expiry

Expected Result -

It should not lockout nfs event even when we reach threshold value for Major & Critical events

RWD-146 [RWD-NFS Event] Lockout option in Actions is also removed for SMB event when set `igls rsw nfsevents set --enabled=snapshotonly`

Lockout option in Actions is also removed for SMB event when set `igls rsw nfsevents set --enabled=snapshotonly`

Workaround: you can set `igls rsw nfsevents set --enabled=true/false/snapshotonly`

RWD-113 Wrong Ransomware event state when created with `POST /v2/ransomware/lockout/{user}`

The Ransomware event that is created using POST /v2/ransomware/lockout/{user} API call has TO_LOCKOUT state. This event should be created with LOCKED_OUT state.

Workaround: manually run the lockout job from the actions menu on the event.

RWD-114 Creating Critical Path Snapshots is blocked

Creating critical path snapshots is blocked when the amount of critical snapshot paths is over the snapshot budget.

Workaround: Raise the snapshot budget and create critical path snapshots again after the cooldown period.

New in Superna Eyeglass Ransomware Defender Edition Release 2.5.9.1

1. `zkcleanup.timer` runs by default on install/upgrade
2. The NFS implementation to be more consistent with SMB processing

What's New in Superna Eyeglass Ransomware Defender Edition Release 2.5.9 (11/30/2022)

Fixed in 2.5.9

Recovery Manager: Now included in ransomware defender is the ability to selectively view and recover all files that were affected by a ransomware event.

New in 2.5.8.1-22116

Refer to previous 2.5.8.1 builds.

Fixed in 2.5.8.1-22116

Technical Advisory 31 - Ransomware Defender NFS Event Detection Always Enabled in 2.5.8.1-22080/22100

[Technical Advisory 31](#) is resolved in 2.5.8.1-22116.

New in 2.5.8.1-22100

Refer to previous 2.5.8.1 builds.

Fixed in 2.5.8.1-22100

Refer to previous 2.5.8.1 builds.

New in 2.5.8.1-22080

T22197 Ransomware Defender Read-Only Role

In the User Roles window there is a new option RANSOMWARE_READONLY to provide read only access to the Ransomware Defender window.

T22328 Ransomware Defender Event csv file storage

To improve disk space management on the operating system disk of the Eyeglass appliance, storage of the Ransomware Defender csv files used to store user event details has been moved to the larger disk used for storing larger application files such as log.

T20285 Action menu for historical events now has option to restore access

The Action menu for Ransomware Defender events in the Event History now has an option to Restore User Access.

Fixed in 2.5.8.1-22080

T21207 Custom Snapshot Expiry not preserved after modifying Settings on Threshold menu

A custom snapshot expiry set using the `igls rsw generalsettings set -- snapshot_expiry_hours` command is reverted to the default value of 48 hours if there are any changes made and saved in the Ransomware Defender Threshold menu. No impact to snapshot creation, only the schedule is reverted to default.

Resolution: Custom snapshot expiry is now preserved.

T21261 Cannot edit a user configured in the Ignored List or Monitor Only Settings

Cannot edit entries for users configured in the Ignored List or Monitor Only Settings. The Save button has no action. Path and IP Address can be edited.

Resolution: User can now be edited in the Ignored List and Monitor Only Settings.

New/Fixed in 2.5.8-22028

Refer to previous 2.5.8 builds.

New in 2.5.8-21330

Refer to previous 2.5.8 builds.

Fixed in 2.5.8-21330

Security

T22171 - Log4j Vulnerability - Upgrade to Log4j 2.17.0
(2.5.8-21330 and higher Log4j 2.17.0)

New in 2.5.8-21306

See What's New in Ransomware Defender [here](#).

Ransomware Defender Snapshot Management Enhancements

The Ransomware Defender window has a new Snapshots menu where the new snapshot related features Snapshot Budget and Critical Path Snapshot will be managed. In addition, it is now possible to disable user share/export snapshots.

Documentation for Snapshot Management can be found [here](#).

To maintain existing snapshot behaviour to take a snapshot at the base path of all shares that associated account has access to, ensure that the User Share Snapshot Settings “Enable Share Snapshots” checkbox is checked.

T19619 Critical Path Snapshot

Introduced in 2.5.8 one or more paths can be configured to always have a snapshot created for any detection.

T19823 Snapshot Budget

Going forward Ransomware Defender (2.5.8 build 21213 and higher) maximum number of snapshots created will be the configured Snapshot Budget (default is 5000). Prior to creating snapshots, Ransomware Defender will determine the number of Ransomware Defender specific snapshots (snapshot name starts with igls) and only if less than the snapshot budget will proceed with the snapshot step. If snapshots cannot be created due to snapshot budget a critical severity alarm is sent and the Event Action History is updated as well.

T15666 New Behaviour Detections Enabled

New behaviour detections are available and enabled by default.

IMPORTANT: This may introduce new detections that will need to be evaluated to determine whether additional tuning of Ransomware Defender settings is required. Recommend to enable Learning Mode after upgrade and verify no new events after several days. NOTE: Learning mode offers full file system protection.

T21215 New SmartAirgap API

New API is available that allows external applications to determine whether there are any active Ransomware Defender or Easy Auditor active events. More information can be found [here](#).

NEW - OneFS 9.3 Support

Support for OneFS 9.3 is introduced in release 2.5.8.

Fixed in 2.5.8-21306

T22033 Log4j Vulnerability - CVE-2021-44228

Resolution: log4j version updated to 2.15.0 which has patch for the vulnerability.

T11832 Ransomware Security Event which is promoted from Warning to Major does not respect Major Grace Period

If a Ransomware Security Event is promoted from Warning to Major threshold, the associated user is locked out right away instead of starting Grace Period timer and only locking out if Grace Period has expired and no manual action has been taken. Note that a Ransomware Defender Security event which is raised at the Major level will respect the configured Grace Period.

Resolution: Major threshold Grace Period timer is now respected.

T18985 igls rsw restoreaccess cannot restore access for unresolvable user

If the user specified in the igls rsw restoreaccess cannot be resolved by the Access Zone AD provider. For example, a lockout might occur on shares provisioned with the Everyone permission even when the Access Zone AD provider cannot resolve the AD user.

Resolution: the igls rsw restoreaccess command can now be used to restore access for unresolvable user. Note that when using CLI to restore access the GUI is not updated with the new state.

Technical Advisories

Technical Advisories for all products are available [here](#).

Known Issues

Threat Detection

T4151 Action Window Event Action History does not show Unreachable Cluster

In the event that a Cluster is unreachable during a Lockout operation, the Active Event state will correctly show ERROR and the Event Action History will show “Partially Locked out” but does not display the cluster that was unreachable or the shares that could not be locked out.

Workaround: Manually inspect the clusters that were locked out. Any missing cluster under management need to review the shares and determine which the affected user has access to and then manually block access.

T3732 Restored permission may be incorrect for consecutive lockouts

In the event that user share access has been locked and subsequently restored and another lockout occurs before Eyeglass inventory has run, the “restore” permissions associated with shares may be the lockout settings from the previous lockout.

Workaround: Permissions should be restored manually by removing the deny permission for the affected user. Use the Event Action History to determine the affected shares.

T4081 Time Zone Mismatch between Ransomware Defender Security Guard Job History and Event History dates

The Ransomware Defender Job History “Run Date” is based on the Eyeglass appliance time zone whereas the Event History “Detected” date is translated to the client browser locale.

Workaround: Translate date for 1 of the dates to the time zone of the other date to correlate Security Guard Jobs to events in the Event History.

T4151 Action Window Event Action History does not show Unreachable Cluster

In the event that a Cluster is unreachable during a Lockout operation, the Active Event state will correctly show ERROR and the Event Action History will show “Partially Locked out” but does not display the cluster that was unreachable or the shares that could not be locked out.

Workaround: Manually inspect the clusters that were locked out. Any missing cluster under management need to review the shares and determine which the affected user has access to and then manually block access.

T22321 Escalation from major to critical will not change GUI status and lockout delay is blocked

multi event escalation will block delayed lockout even if the UI shows delayed lockout.

Workaround: Change the multi event threshold to a higher value or make sure you do not leave many active events collect to avoid escalated response settings on the settings tab. These values should be increased if you plan to leave many active warning events without resolving them.

T4777 Snapshots not created for any Events that are Active when the Snapshot feature is enabled

If there are any Active Events when the Create Snapshot option is enabled, no Snapshots will be created for these already Active Events.

Workaround: Enable the Create Snapshot option when there are no Active Events. Events raised after the Create Snapshot option was enabled will have associated Snapshots created for affected shares.

T4819 Empty Event History List

There may be conditions where having other windows open such as the Event Action History may result in the Event History list being displayed with no entries.

Workaround: Close all Ransomware Defender related windows and then re-open the Ransomware Defender -> Event History tab.

T4950 Alarm text for failed Snapshot delete references Snapshot create

The alarm that is raised when a Snapshot delete fails contains the text "Failed to create snapshots" instead of "Failed to delete snapshots".

Workaround: Check the Action Log for the event to determine whether a snapshot create or delete has failed.

T4955 Subsequent Create Snapshot action will delete reference to previously created snapshots if an error occurs during the create

The Create Snapshot action can be executed multiple times for a given event. If it has been run previously and then run again and the subsequent run has an error on creating any snapshot, the Snapshots list only contains the snapshots from the last run. Previously created snapshots are no longer displayed.

Workaround: Check the Event Action History log for complete list of created snapshots.

T5024 Major Events may reappear in the Active Events list after being recovered

An event which crosses the Major threshold and is recovered to Historical Events without being locked out (Stop lockout timer) may appear in the Active Events list again immediately after being recovered (Mark as recovered).

Workaround: Stop the lockout timer and Mark the event as recovered again. This may have to be repeated several times. Locking the affected user out followed by Restore User Access and then archiving the event as recovered may also resolve this issue.

T5756 Error on restoring permissions does not raise an alarm

If permissions restore action encounters an error there is no associated alarm notification.

Workaround: Review the Action History for the Event to confirm that all restores were successful.

T5954 Events that are promoted to Major due to multiple event “Upgrade to Major” are locked out immediately

For the case where there are multiple Warning events that cross the “Upgrade to Major” limit, when they are promoted to Major they are locked out right away instead of waiting for the configured Grace Period before locking out.

Workaround: The occurrence of this behaviour can be reduced by setting the “Upgrade to Major” threshold to a high number of users.

T6728 Extensions with special characters cannot be removed from the ignore list

Extensions have been added to the extension ignore list using the `igls rsw allowedfiles add --extensions` command cannot be removed from the ignore list using the `igls rsw allowedfiles remove --extensions` command.

Workaround: Contact Superna Support at support.superna.net to assist with removing these extensions.

T7062 User may not be locked out in a multi-user security event

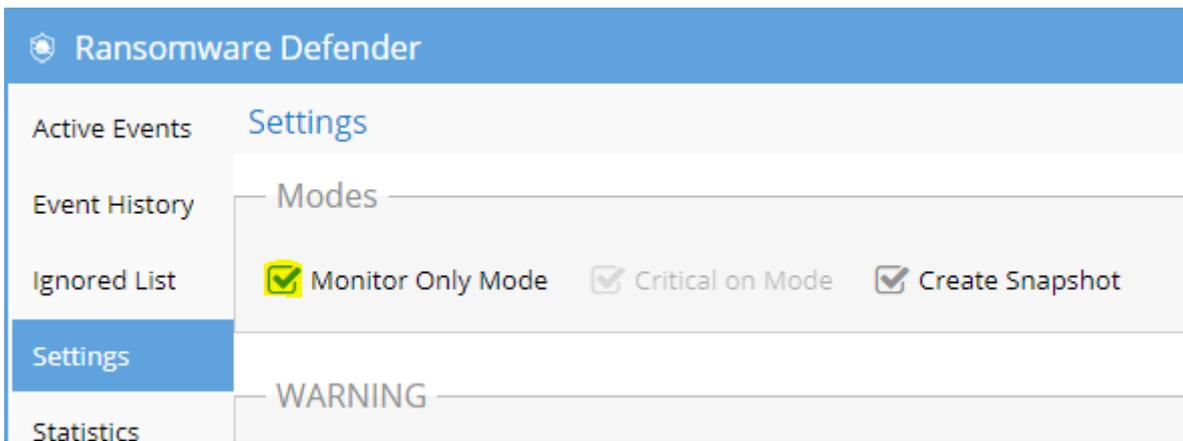
It may occur that a user is only partially locked out when a multi-user lockout is occurring due to an error response from the PowerScale cluster during user resolution in Active Directory. In this case the error is not displayed in the Eyeglass event history.

Workaround: The Event History will contain the shares that were successfully locked out. Should events continue to be generated against the user for the unlocked share, it may be locked out as a result of subsequent event. User may also be locked out manually by adding the deny permission manually to share that was not locked out.

T7190 Active Events may show State of Warning instead of Monitor when Monitor Mode is enabled

Instead of the event state being Monitor in Active Events when Monitor Mode is enabled, the event state may incorrectly display as Warning instead.

Workaround: None Required. This is a display issue only. Verify that Monitor Mode is enabled on the Ransomware Defender / Settings tab.



T7525 Affected Files also shows Active Auditor Affected Files

When viewing the Affected Files for a Ransomware Defender security event, any files associated with an Active Auditor event that has occurred at the same time are also displayed.

Workaround: Download the csv file and use the path associated with the Ransomware Defender event from the GUI to filter the results.

T11586 NFS Lockout Event Information does not include NFS Export path

The Ransomware Defender event GUI for an NFS client displays the NFS Export ID in the Locked out shares view in the "Share" column but does not display the corresponding path in the Path column.

Workaround: Verify NFS Export path from PowerScale directly referencing the NFS Export ID from the Locked out shares window.

T11590 NFS Lockout Event does not generate an PowerScale snapshot

When a Ransomware Security Event is detected for an NFS client, the PowerScale snapshot against related paths is not created.

Workaround: Upgrade to release 2.5.8 and use critical path snapshot feature.

PowerScale scheduled snapshots may also be available for recovery.

T14339 Restore Access Alarm must be manually cleared

A Restore Access alarm is generated when restoring access to user. Subsequent restore will not update an existing restore alarm or send a notification.

Workaround: After restoring access to user, in the Alarms window manually clear the alarm in order to receive notification on a subsequent restore.

T15198, T15650 Ransomware Events may have inaccurate Signal Strength or may be reprocessed

Ransomware Event processing may receive duplicate events and as a result may show a higher Signal Strength than is actually the case. The associated csv will also show duplicate entries for the same file. Ransomware processing may also intermittently skip a signal and as a result may show lower Signal Strength.

In some cases this may also result in a Ransomware Event being reprocessed at a later time.

Workaround: None required. The duplicate events result in early detection of Ransomware events. Skipping of signals is intermittent and subsequent signals cross threshold for detection.

T15639 T18812 Error replicating AD Group or Local User Run as Root SMB permissions affects Lockout and Restore

In some cases an SMB share permission that is configured with an AD group or Local User that has Run as Root privileges has an error on share updates for Ransomware Defender that blocks Lockout such that it does not take effect or on Restore it does not restore the Run as Root SMB share permission.

Important: If you use run as root on shares you are exposing data to very high security risk since no lockout will be possible. This is because the user SID that is sent when an AD user accesses data with run as root enabled is the root user SID not the actual AD user SID.

We recommend to NOT use run as root on shares for the reason above and it fails all security audits of PowerScale in all industry standards (PCI, HIPPA, FedRAMP, ITSG, etc...). Remove run as root option on all shares.

Please review our documentation for more information: [Securing root user on PowerScale](#).

Workaround: Manually restore or lockout user.

T16229 GUI incorrectly reports error when manually creating a snapshot

If you use the Action menu to manually create a snapshot, the GUI shows an error but the snapshot is actually created. Automatic snapshot creation as part of active event detection is not affected by this issue.

Workaround: None required as snapshot is created. Verify snapshot creation using Powerscale OneFS interface.

T16462 NFS lockout may fail

Under some conditions Ransomware Defender successfully detects security event and notifies regarding the event but the associated NFS lockout action fails.

Workaround: Manual steps to block access to the Powerscale cluster are required in this case.

T18271 Ransomware Event State incorrect shows success when Powerscale is unreachable during restore operation

If a Restore operation is initiated on an Active Event when the Powerscale cluster is unreachable, the restore steps will fail but the state of the Event on the Active Events GUI is ACCESS_RESTORED.

Workaround: None required. The Event Action History shows that the restore step failed. Once connectivity to the Powerscale cluster is restored the Restore operation can be retried.

T18643, T19217 State of Active Event shows WARNING when it should be MONITOR for File Filter in Monitor

When Ransomware Defender is configured for Enforcement Mode and Critical on Mode, an Active Event related to a File Filters extension in Monitor will be displayed in Active Events with State of WARNING instead of MONITOR.

No impact on behaviour, no lockout applied.

Impact to Automatic learning - the File Filter extension is not set to disabled.

Workaround: Review events and put File Filter extension into Disabled as required.

T18718 igls rsw allowed files remove option not working

The igls rsw allowed files CLI command executes and reports success but does not actually activate the extension or file entered in the command.

Workaround: Use the Eyeglass GUI to enable items from the File Filter list that had been previously disabled. For more information refer to documentation [here](#).

T18852 Ransomware Defender does not detect where path has square brackets []

If path or file name on Powerscale cluster includes square Ransomware Defender encounters an error on processing and does not detect the security event.

Workaround: None available. Ransomware manipulation of other path/file continue to be monitored and acted upon.

T18887 Security Guard in Learned Thresholds prevents Security Guard job from detecting

If the Security Guard user is deleted from the Learned Threshold list it continues to be enforced and Security Guard events are not detected by Ransomware Defender. This will occur if Security Guard was in the Flag as False Positive list prior to upgrade to 2.5.7. In 2.5.7 Security Guard user cannot be added to the Learned Threshold list.

Workaround: Contact support.superna.net for assistance if after upgrade to 2.5.7 the Security Guard user needs to be removed from the Learned Threshold list.

T18895 Ransomware Learned Threshold list doesn't open first time

Under some conditions where name resolution proceeds slowly and/or Learned Threshold list contains many entries, list will not be displayed before 45s timeout occurs.

Workaround: Selecting the list a second time displays the list.

T19040 After upgrade to 2.5.7, Ransomware Events in Event History do not display the Signal Strength correctly

Signal strength not displayed correctly for Ransomware Events in the Event History after upgrade to 2.5.7 for events that were added to Event History in previous release.

Workaround: None required. These events had already been managed and archived on previous release.

T19106 Acknowledge/Archive options not blocked while lockout in progress

The Acknowledge / Archive options are incorrectly available to be used in the window of time between when the lockout action starts and the active event enters the Locked Out state. Impact: If selected during that window, the event never enters the Locked Out state and even though it is locked out and there for the restore option is not available to restore permissions.

Workaround: The Event Action History correctly documents the shares that were locked out and the account and time of lockout. The account can be restored from the command line following the instructions [here](#) for `igls rsw restoreaccess` command.

T19198 Multiple concurrent Major Events not upgraded to Critical based on "Upgrade to Critical (events)" setting

The setting to promote Active Events from Major to Critical without having to reach the Critical Threshold, "Upgrade to Critical (events) " is not respected. Events are not promoted until their Signal Strength Threshold crosses the Critical setting.

None Required: Events will be promoted if their Signal Strength Threshold crosses into Critical threshold and Lockout will be applied. For events that remain at Major severity if no manual steps taken, Lockout will be applied once grace period expires.

T19236 Honeypot file detector incorrectly crosses Major threshold in Monitor Mode

When Ransomware Defender has Monitor Mode active the Honeypot file detector incorrectly promotes a Honeypot event to Major instead of staying in Monitor state. Once promoted to Major the Grace Period timer begins and if no manual steps taken a lockout of the account will occur once the grace period expires.

Workaround: Upon notification of the Major event, manual steps can be taken from the Active Event Action menu to stop the Lockout timer and resolve the event from the GUI if appropriate. If a lockout occurs access can be restored through the GUI from the Active Event Action menu as well if appropriate.

T19356 Files/Folders with language characters not displayed properly in CSV and email

If the files/folders associated with a detected Ransomware security event contain language specific characters, the path/file names are not displayed correctly in the email sent as well as the CSV.

Workaround: Use the GUI to see the files and folders.

T19409 Well known extension detection not working under some circumstances

Under some circumstances when there have been no customization to the File Filters for well known extension detection, the well known vector for detection of Ransomware security event is skipped.

This does not affect the user behaviour or honeypot detection vectors.

Workaround: User behaviour and honeypot detection vectors still available for monitoring.

T20094 CLI command to restore access does not work when user name contains special characters

The `igls rsw restoreaccess` command does not execute if the user name contains special characters. Impact: No impact on lockout. Impact on ability to restore access.

Workaround: Use the Ransomware Defender Action Event history to identify all shares that were locked out and manually remove the deny permission using Powerscale native tools.

T23012 Restore access for NFS lockout from Event History does not complete

Using the Restore User Access option in the Event History for an unresolved NFS lockout will restore the permissions as expected but the job gets stuck at the Restore job initiated step and the overall status does not change to Recovered and no alarm is sent.

Workaround: Verify manually using OneFS native tools that client list for NFS export has been restored as expected.

Security Guard

T4197 Security Guard Error for Unlicensed Cluster

Security Guard fails when PowerScale Cluster selected to run is not licensed.

Since Ransomware Defender dynamically picks priority PowerScale Clusters to license (refer to [Eyeglass Ransomware Defender Admin Guide](#) for details on selection of licensed cluster) for the case where Eyeglass is managing more clusters than there are

Ransomware Defender Agent Licenses, one cannot be sure the selected Cluster in Security Guard is actually licensed at the run time.

Workaround: Deploy same number of Ransomware Defender Agent Licenses as the number of PowerScale Clusters being managed by Eyeglass.

T8889 Cannot enable Security Guard with default schedule for on a newly deployed 2.5.3 ovf

The drop down list to schedule security has an invalid default.

Workaround: Click the drop down and set a valid schedule.

T4228 Security Guard Temporary Errors

Security Guard may occasionally error with 0 files written.

Workaround: This condition typically clears it self on the next Security Guard run. It does not affect workflow for a real security event.

If it does not clear, follow these steps to recover:

1. Archive as Unresolved
 2. Run Security Guard manually to ensure that it is operational again.
-

T4965 Security Guard User Authentication Fails

When provisioning the Security Guard Active Directory User and password, Eyeglass checks that the username name and password entered can be successfully authenticated. It may occur on initial configuration that you will see the message “user could not be authenticated” even though the username and password are correct.

Workaround: After confirming that the username and password are correct, subsequent provisioning is successful.

T7574 Flag as False Positive Option should not be available for Security Guard Events

Security Guard provides automated end to end validation of Ransomware detection, lockout and restore and therefore should not be flagged as false positive. The Flag as False positive option is currently available to be selected for Security Guard events and should not be.

Workaround: Manual process required to prevent applying Flag as False positive to Security Guard events.

T15175 Existing Security Guard Logs lost formatting after upgrade to 2.5.6

Any existing Security Guard logs viewed from the Eyeglass GUI will have lost the formatting.

Workaround: None required. New logs will have the correct formatting.

Manage Services

T4192 Manage Services status not accurate after ECA Node Down

After an ECA node has been powered off / gone down and subsequently powered back on and rejoined to the ECA cluster it continues to display the Inactive state in the Eyeglass Manage Services window even when it is active again and healthy.

Workaround: Once the node is back up, remove it from the Manage Services window by selecting the X in the node's row. Wait 1 to 2 minutes and the service should be rediscovered with the correct state.

General

T4230 Blank Ransomware Defender Window

After archiving an Event the Ransomware Defender window tabs may appear empty.

Workaround: Close and reopen the Ransomware Defender window.

T4183 Refresh does not work for Ransomware Defender multi-page lists

Ransomware Defender window with multiple pages is not updated by Refresh except for the first page.

Workaround: To update the list go back to the first page of the list.

T15457 HTML 5 vmware vcenter bug on OVA deployment

Some versions of vmware vcenter HTML user interface have a known issue with OVA properties being read correctly post power on, leading to first boot issues.

Workaround: use the Flash client as a work around.

T4336 Eyeglass Restore does not restore Security Guard Job History

Security Guard historical log files are not restored when you restore configuration from backup.

Workaround: None available.

T4549 Ransomware Defender Settings Submit button enabled when no changes made

When the Ransomware Defender Settings window is opened, the Submit button is enabled even though no changes have been made to any settings. If you navigate to another view and come back to Settings, the Submit button is then correctly disabled until a change is made on the page.

Workaround: None required.

T6617 PowerScale Directory Selector does not display hidden directories

Directories that start with a dot (.) are not displayed in the PowerScale Directory Selector.

Workaround: Use the PowerScale Directory Selector to enter `\ifs\` and then enter the remainder of the path manually.

T8807 Deleting cluster from Eyeglass does not clear associated Ignore List and Wiretap settings

When an PowerScale cluster is deleted from management in Eyeglass, any associated Ransomware Defender Ignore List or Wiretap settings are not cleared.

Workaround: Manually delete Ignore List and Wiretap settings for deleted clusters.

T18810 GUI not updated after cancelling an operation to switch modes

In the Ransomware Defender Thresholds window, if you are switching between Advanced and Monitor or Advanced and Enforcement mode and upon being prompted you select No to cancel the operation, the GUI does not refresh and return to the original Advanced mode. Impact: Display issue only, the mode change is cancelled.

Workaround: Switch between tabs in the Ransomware Defender window or use the Eyeglass desktop Refresh Now button.

T18660 Cannot use cloudapps URL to access Well Known Ransomware File Extension list

The cloudapps URL documented [here](#) for accessing the Well Know Ransomware File Extension list does not resolve and returns a 404 response code.

Workaround: Following URL does resolve and can be used to manage the Well Known Ransomware File Extension list:

<https://storage.googleapis.com/rwdefender.superna.net>

T22450 Easy Auditor Event Rate alarm for Ransomware Defender Only deployments

RWD-301 Error getting events - for NFS exports in Recovery Manager

Cyber Recovery manager will show error when trying to display the all activity files affected by NFS export events.

RWD-319 RSW events affected files are not presented in email

RSW events affected files are not presented in email

RWD-362 Support ECS on RWD when turboaudit REST api is configured

Support ECS on RWD when turboaudit REST api is configured

RWD-443 Easy auditor events only receiving and forwarding one signal and one file in file list despite of number of files and type of events

Easy auditor custom real time policy is only receiving and forwarding “one” signal for type create and delete despite of how many files are created or deleted.

RWD-535 Webhook - redundant lockout alarm when lockout/restore

Webhook - redundant lockout alarm when lockout/restore.

Features

RWD-217 Event fails to upgrade with multiple user (ECS events only)

Event fails to upgrade with multiple user (ECS events only)

RWD-85 zookeeper cleanup cron is not running as scheduled

TEST: zookeeper cleanup cron is not running as scheduled

Workaround:

```
lsystemctl enable --now zkcleanup.timer
```

RWD-74 zookeeper cleanup cron is not running as scheduled

zookeeper cleanup cron is not running as scheduled

Workaround:

apply this command to all eca nodes

[Copy Code](#)
JSON

```
lsystemctl enable --now zkcleanup.timer
```

RWD-246 Files with non-ASCII characters fail to recover

2.5.9-22231

Files which will have the extension modified to a known extension like .crypto will trigger TD7 events.

The original files are not recovered even if the Recovery Job finishes successfully.

Known Limitations

Threat Detection

T6914 Some extensions still result in lockout when added to the ignore list

For the following well-known extensions, a lockout will still occur even if these extensions have been added to the extension ignore list using the `igls rsw allowedfiles add --extensions` command:

*.[\[teroda@bigmir.net\]](mailto:teroda@bigmir.net).masterteroda@bigmir.net

*.[\[mich78@usa.com\]](mailto:mich78@usa.com)

*.symbiom_ransomware_locked

*.[\[resque@plague.desi\]](mailto:resque@plague.desi).scarab

Workaround: Alternate Ignore capabilities for User, Path or IP address documented [here](#) may be used to workaround this issue.

T7191 SMB service not enabled when access restored when lockroot is true

If you have Ransomware Defender configured to disable SMB service is a root user event is detected (see Ransomware Admin guide [here](#), section Securing Root User on PowerScale), when you restore user access the SMB service is not automatically enabled.

Workaround: Manually enable SMB service on PowerScale once access is restored and you are ready to resume file access for SMB users.

T7670 Restoring user access via CLI does not update status of Security Event in the GUI

If you have restored user access after a lockout using the CLI command "`igls rsw restoreaccess set --user=DOMAIN\user`", the associated Security Event in the GUI will not be updated and remain in active state.

Workaround: Open the Actions window for the active event, enter a comment that access has been manually restored and then archive the event.

T8744 No event processing once Signal Strength passes 2 times Critical Threshold

Once a Security Event or Active Audit event has passed 2 times the Critical threshold configured in Ransomware Defender Settings, there is no further processing of Signals for the associated user. In all cases actions based on Critical threshold settings would have been already taken prior to reaching the 2x level.

For the case where both Ransomware Defender and Easy Auditor are licensed, reaching Signals processed count of 2 times Ransomware Critical threshold for a particular user limit is applied independently for Ransomware Defender and Easy Auditor.

Workaround: None Available.

T8986 NFS export lockout cannot be restored

An NFS export that has been locked out due to Ransomware Defender detecting a security event cannot be restored using Superna Eyeglass. You are able to select the

Restore option and the Event History indicates that the permissions are restored but in fact the NFS export will still be in read-only state.

Workaround: On lockout NFS clients are moved to "Always Read-Only Clients". They will need to be manually moved to the correct access type using Isilon GUI or CLI to modify the export.

T15705 After upgrade to 2.5.6 cannot download CSV for Ransomware Event Files from events detected in prior releases

After upgrading to Release 2.5.6, csv download of files related to Ransomware events generated on the previous release is not available.

Workaround: GUI can still be used to view the files or files may be found on the Eyeglass appliance in the `/srv/www/htdocs/rsw_event_all_files` directory.

T16723 Error on Lockout of Shares on DR cluster

Under some conditions where a Ransomware Defender Lockout job overlaps with a Configuration Replication job you may see an error locking out some shares on DR cluster with error message code 409 AEC_CONFLICT. No impact to protection from Ransomware as the shares on the DR cluster are providing access to read-only data.

Workaround: You can re-attempt the Lockout from the Ransomware Defender window Action menu for the Active Event. Deny permission can also manually from Powerscale interface as required.

T17287 Many Access Zones slows down creation of snapshots and lockout

In the case where there are many Access Zones configured, analysis of user accessible shares must be done for all Access Zones before snapshot processing or lockout is started.

Workaround: None available

T7574 Option to set learned threshold for Security Guard in RESTORED_USER_ACCESS state

The menu to add Security Guard to the Learned Threshold is incorrectly provided when the event is in the RESTORED_USER_ACCESS state. The option can be selected and indicates that the flag as false positive was applied but it is not actually applied and it does not appear in the Learned Threshold list.

Workaround: None required

T18733 Ransomware Defender Affected Files Download Menu Naming

The Ransomware Defender Affected Files Download Menu is incorrectly named Affected Files - All. As described in the Ransomware Defender documentation [here](#) it is possible to have more files associated with the event than displayed in the file.

General

T16137 Anyrelease restore does not restore all Ransomware Defender and Easy Auditor settings

There is no restore of settings from release 2.5.4 and earlier. For release 2.5.4 and earlier continue to capture all Ransomware settings (False Positive, Ignore List, Allowed

Extensions, Security Guard) and Easy Auditor settings (Active Auditor Trigger settings, RoboAudit). Post restore verify settings and update where required before cluster up on ECA.

In all cases, restoring an Eyeglass backup using the --anyrelease option will not restore following Ransomware Defender and Easy Auditor settings:

Ransomware Defender: Event History, Threats Detected

Easy Auditor: Finished Reports, Scheduled Reports, Saved Queries

T16821 anyrelease restore restrictions for restore to 2.5.7

Ransomware Defender, Easy Auditor and Performance Auditor deployments cannot use the anyrelease restore option to upgrade to a new appliance running 2.5.7. For case where a backup & restore is required due to 42.3 OS on original deployment, a backup & restore to 2.5.6 will have to be done first followed by an upgrade to 2.5.7 or in-place OS upgrade prior to 2.5.7 upgrade.

T20370 Monitor Only Settings Client IP applies to all PowerScale clusters

If multiple Powerscale clusters are licensed for Ransomware Defender a setting in the Client IP list for Monitor Only Settings is applied to all clusters. There is no option to associate the setting to a specific cluster. Also if you convert Ignore List to Monitor list any Client IP setting from Ignore list will also be applied to all cluster.

T21852 RSW - Cannot configure and run SG after anyrelease backup and restore from an earlier build

After a backup and restore from the earlier release to Eyeglass 2.5.8, the Ransomware Defender window may no longer allow you to edit or run the Security Guard.

Workaround: After the restore, execute the 2.5.8 run file (same release as you restored to) to resolve the issue.

T21208 Snapshots taken using Action Menu for Ransomware Defender Event follow Ransomware / Snapshots settings

If the Enable Share Snapshots option in Ransomware / Snapshots is unchecked, selecting the Create Snapshot option from the Action Menu will also not create snapshots.

T21110 Ransomware Defender / Snapshots User Share Snapshot Settings also applies for NFS detections

The option to disable/enable Ransomware Defender snapshot functionality is called User Share Snapshot Settings and Enable Share Snapshots but applies to any Ransomware Defender detection for SMB or NFS.

Well Known Ransomware File Extension Whitelist management is not available when a proxy used

If a proxy has been configured to access the internet, the well-known ransomware file extension management does not account for the proxy and will not be able to resolve the configured URLs.

T17624 Ransomware Defender NFS detection creates snapshot on SMB shares with Everyone permission

A Ransomware Defender detection for operations over NFS protocol also creates snapshots for SMB shares that have the Everyone permission.

RWD-75 Page-1 gets hide when navigate to Page-2 & archive all events from this page

When clearing all of the ransomware events from the second page of the ransomware defender active alerts tab, the pagination of the window can be lost and an empty list is displayed.

Workaround: close and open the window.

RWD-236 [RWD-NFS Event] User is displayed as "Root" or Sid ID instead of EXP:<client_ip>_<user_id>

When using nfs 4 version - it cannot show the EXP:<client_ip>_<user_id>

Workaround: use this command to mount the NFS export.

```
mount -o nfsvers=3 <isilon-ip>:<export-path> <mount-path>
```

RWD-453 Only 100 affected files are listed in the webhooks event which triggers upon changing the state of RSW event

Will not inherit number of files from original event.

1.5. Current Release - Release Notes

Ransomware Defender AirGap 2.0

[Home](#) [Top](#)

Release Date	Version
11/28/2023	2.6.4-23365

- [What's New in Superna Eyeglass Ransomware Defender Edition Release 2.6.4 AirGap 2.0 \(11/28/2023\)](#)
- [Supported OneFS releases](#)
 - [Target Airgap Cluster](#)
- [Supported Eyeglass releases](#)
- [Inter Release Functional Compatibility](#)
- [End of Life Notifications](#)
- [New in Superna Eyeglass Ransomware Defender Edition Release 2.6.3 AirGap 2.0 \(09/28/2023\)](#)
- [New in Superna Eyeglass Ransomware Defender Edition Release 2.6.1 AirGap 2.0 \(08/03/2023\)](#)
- [Fixed in 2.6.1](#)
 - [AIRGAP- 576 AirGap for ECS now supports load balancers in front of ECS clusters](#)
- [New in Superna Eyeglass Ransomware Defender Edition Release 2.6.0 AirGap 2.0 \(06/29/2023\)](#)
- [Fixed in 2.6.0](#)
 - [AIRGAP- 434 CAS jobs are not pushed into Eyeglass](#)
 - [AIRGAP- 523 Security Guard now supports management networks and data networks on different subnets](#)
- [New in Superna Eyeglass Ransomware Defender Edition Release 2.5.12 AirGap 2.0 \(05/09/2023\)](#)

- New in Superna Eyeglass Ransomware Defender Edition Release 2.5.11 AirGap 2.0 (04/03/2023)
- Fixed in 2.5.11
 - AIRGAP-501 9.5 protected cluster cannot be added in AirGap Enterprise
- New in 2.5.11- 23110
- New in Superna Eyeglass Ransomware Defender Edition Release 2.5.10 AirGap 2.0 (03/06/2023)
- New in 2.5.10-23087
- Fixed in 2.5.10
 - AIRGAP-490 The event Retrieval job fails for Basic AirGap
- New in Superna Eyeglass Ransomware Defender Edition Release 2.5.9.1 AirGap 2.0 (02/14/2023)
- End of Support in Release 2.5.9
- Deprecation Notices
- Technical Advisories
- New in Superna Eyeglass Ransomware Defender Edition Release 2.5.9 AirGap 2.0 (11/30/2022)
- New/Fixed for AirGap 2.5.9
- New/Fixed for AirGap 2.5.8.1-22100
- New for AirGap 2.5.8.1-22080
 - T22072 AirGap Enterprise Events and Disk Usage Retrieval is now a push
 - T19599 Migrate Configuration from Protected to Vault Cluster
 - T21214 AirGap Enterprise can now support multiple vaults managed from the same Eyeglass
 - T22123 Command to send vault agent logs manually
 - T21490 Monitor AirGap SynclQ Policies for changes to configuration
 - T21830 AirGap Enterprise Fiber cutter option
- Fixed in AirGap 2.5.8.1-22080
 - T22930 AirGap Enterprise Replication Nodes require access to Production Network

- T20932 AirGap Job Reports CSV does not report failed jobs
- New for AirGap 2.5.8-22028
- New for AirGap 2.5.8-21330
- New for AirGap 2.5.8-21306
 - T20945 AirGap - Alarm Conditions (AirGap Enterprise)
- New for AirGap 2.5.8-21240 - Controlled Availability
 - T21212 AirGap Enterprise does not require Static Route configuration
 - T21042 Automated retrieval of vault cluster logs (AirGap Enterprise required)
- New for AirGap 2.5.8-21213/21222 - Controlled Availability
 - T19522 AirGap Enterprise
- Fixed in 2.5.8-21330
 - T22171 - Log4j Vulnerability - Upgrade to Log4j 2.17.0 (2.5.8-21330 and higher Log4j 2.17.0)
- Fixed in 2.5.8-21306
 - T22033 Log4j Vulnerability - CVE-2021-44228
- Fixed in 2.5.8-21222
 - T20770 AirGap Event Retrieval Job Fails with No route to host
 - T20358 Not able to create an AirGap Job Report for a selected period
 - T19195, T19221 AirGap Job shows success when failed
- Fixed in 2.5.8-21213
 - T20766 Cannot view second page of AirGap Config AirGap job list
- Known Issues
 - T15104 Default schedule does not run the job
 - T15300 Error on manually connecting Airgap not displayed
 - T16199 No alarm if Airgap event retrieval from Powerscale cluster is in error
 - T16436 Airgap Jobs cannot be manually run from the Airgap window
 - T16456 Customized Airgap schedules reset to default after upgrade
 - T16457 Airgap window not refreshed
 - T16470 Renaming Airgap SyncIQ policy does not preserve original settings

- T16476 AirGap Job continues to run after Powerscale cluster deleted from Eyeglass
- T19609, T19632 User Disabled AirGap Job may have status of having been run when it has not
- T19631 AirGap Config window time uses Eyeglass appliance timezone
- T20966 AirGap Job Configuration lost on rediscover or anyrelease restore
- T21134 AirGap Basic Job can be started from Jobs window without AirGap role
- T21863 AirGap Basic static route remains on error
- T21327 Managed Device Alarms have incorrect date and are sorted oldest to newest
- T21224 Snapshot schedule job created for AirGap Job
- T21147 Customizing AirGap policy prefix results in job errors
- T21659 AirGap state - network disconnected in UI
- T20945 AirGap Open Check may not detect vault open
- T23094 Vault Cluster Event Retrieval fails for AirGap Basic in 2.5.8.1
- T20525 Connectivity check does not work for AirGap Enterprise with Fiber Cutter
- T23399 No validation when adding vault cluster
- T23400 Fiber Cutter Error Handling
- AIRGAP- 404 [Airgap Reports] It shows an Error for the Job when creating a report manually
- AIRGAP 416-Vault Agent log archive has incorrect naming
- AIRGAP-429 Data is replicated when there are active ransomware events
- AIRGAP-529 Duplicated heartbeat when the vault cluster is not connecting to the protected cluster
- AIRGAP-528 Error message displayed in vault agent console for failed command needs to be fixed
- Known Issues ECS
 - Airgap-147 Total number of jobs in AirGap report is incorrect

- Airgap-221 NULL is displayed for Source in Managed Devices Alerts
- Airgap-224 Job update to Eyeglass is not working as expected
- Airgap-289 Active RWD events are ignored when starting AirGap ECSSync jobs from UI using Run Now
- Airgap-226 Docker issues in Vault Agent
- AIRGAP-372 Not all the AirGap ECSSync jobs are started when scheduled
- AIRGAP-569 The number of files is different in ECSSync UI than what is displayed in ECS
- Known Limitations
 - T19614 AirGap Job consideration of Easy Auditor Active Auditor Active Event not configurable
 - T21316 Vault stays open for vault cluster event retrieval
 - T21274 Alarm raised for vault open in Eyeglass is not cleared after maintenance window is finished
 - T21851 AirGap Enterprise vault open alarm limitation
 - Airgap-329 Vault agent names must be case-insensitively unique
 - AIRGAP-427 Airgap ECS sync jobs get duplicated sometimes

What's New in Superna Eyeglass Ransomware Defender Edition Release 2.6.4 AirGap 2.0 (11/28/2023)

Supported OneFS releases

Source cluster

8.2.0.x

8.2.1.x

8.2.2.x

9.1

9.2

9.3

9.4 via the February RUP 9.4.0.12 (PSP-3079) released Feb 8th 2023

9.5

Target Airgap Cluster

8.2.2.x

9.1.0.0

9.2.0.x

9.3.x.x

9.4.x.x

Supported Eyeglass releases

Superna Eyeglass Ransomware Defender Version	Superna Eyeglass Version
2.5.10-23087	2.5.10-23087
2.5.9-22231	2.5.9-22231
2.5.8.2-22164	2.5.8.2-22164

Inter Release Functional Compatibility

	OneFS 8.0	OneFS 8.1	OneFS 8.2	OneFS 8.0 - OneFS 8.1	OneFS 8.0 or 8.1 - OneFS 8.2

--	--	--	--	--	--

End of Life Notifications

End of Life Notifications can be found [here](#).

New in Superna Eyeglass Ransomware Defender Edition Release 2.6.3 AirGap 2.0 (09/28/2023)

New in Superna Eyeglass Ransomware Defender Edition Release 2.6.2 AirGap 2.0 (09/01/2023)

New in Superna Eyeglass Ransomware Defender Edition Release 2.6.1 AirGap 2.0 (08/03/2023)

Fixed in 2.6.1

AIRGAP- 576 AirGap for ECS now supports load balancers in front of ECS clusters

New in Superna Eyeglass Ransomware Defender Edition Release 2.6.0 AirGap 2.0 (06/29/2023)

Fixed in 2.6.0

AIRGAP- 434 CAS jobs are not pushed into Eyeglass

CAS jobs are not pushed into Eyeglass

AIRGAP- 523 Security Guard now supports management networks and data networks on different subnets

New in Superna Eyeglass Ransomware Defender Edition Release 2.5.12 AirGap 2.0 (05/09/2023)

New in Superna Eyeglass Ransomware Defender Edition Release 2.5.11 AirGap 2.0 (04/03/2023)

Fixed in 2.5.11

AIRGAP-501 9.5 protected cluster cannot be added in AirGap Enterprise

When trying to add a 9.5 prod cluster in AirGap Enterprise getting the error.

New in 2.5.11-23110

Support for OneFS 9.5 was added.

New in Superna Eyeglass Ransomware Defender Edition Release 2.5.10 AirGap 2.0 (03/06/2023)

New in 2.5.10-23087

Fixed in 2.5.10

AIRGAP-490 The event Retrieval job fails for Basic AirGap

Once the AirGap job starts to run, the Event Retrieval job also starts.

Refer to previous 2.5.9.1 builds for what's new.

New in Superna Eyeglass Ransomware Defender Edition Release 2.5.9.1 AirGap 2.0 (02/14/2023)

What's New! In Superna Eyeglass Ransomware Defender AirGap 2.0 Release 2.5.9.1

1. Initial config settings are lost after cluster down on ECSSync UI. We added a default configuration which will be loaded at cluster up. There is no email in it, and the path of it is at `/opt/emc/ecs-sync/config`
2. We added sync schedules via CLI or cron string to change Airgap jobs schedules

to check the existing schedule:

```
ligls airgap changeschedule --job="<Job-name>"
```

to change the airgap job schedule:

```
ligls airgap changeschedule set --job="<job-name>" --cronstr=<5-fields-cron-string>
```

3. File transfer over SSL can use standard encryption and ports to secure the data.

End of Support in Release 2.5.9

No end of support notices in release 2.5.9.

Deprecation Notices

No deprecation notices at this time.

Technical Advisories

Technical Advisories for all products are available [here](#).

New in Superna Eyeglass Ransomware Defender Edition Release 2.5.9 AirGap 2.0 (11/30/2022)

New/Fixed for AirGap 2.5.9

Stability and bug fixes

New/Fixed for AirGap 2.5.8.2-22164

New/Fixed for AirGap 2.5.8.1-22116

Refer to previous 2.5.8.1 releases.

New/Fixed for AirGap 2.5.8.1-22100

Refer to previous 2.5.8.1 releases.

New for AirGap 2.5.8.1-22080

T22072 AirGap Enterprise Events and Disk Usage

Retrieval is now a push

For AirGap Enterprise deployments, vault cluster events and disk usage are now pushed to Eyeglass when scheduled AirGap jobs are run. Commands are available to be run from the vault agent to manually initiate a push of this information.

Documentation is available [here](#).

T19599 Migrate Configuration from Protected to Vault Cluster

A new tab in the AirGap window, "Migrate Configuration", is now available to copy shares/exports related to AirGap jobs to the vault cluster without the source cluster is available. Documentation is available [here](#) - see the section "Configuration Data Sync Steps Eyeglass".

T21214 AirGap Enterprise can now support multiple vaults managed from the same Eyeglass

AirGap Enterprise can now support [multiple vaults](#) managed from the same Eyeglass. Commands for the maintenance window have been updated to support this and can be found [here](#). New multi-vault commands can be found [here](#).

T22123 Command to send vault agent logs manually

A command is now available manually initiate sending of the vault agent logs to Eyeglass. Requires that the vault has been opened prior to running the command. Documentation can be found [here](#).

T21490 Monitor AirGap SynclQ Policies for changes to configuration

A new job assesses whether there have been any changes to SynclQ policy configuration for those policies configured to copy data into the vault each time inventory runs. If any change is found an alarm is raised with alarm code [SCA0098](#).

T21830 AirGap Enterprise Fiber cutter option

AirGap Enterprise can now be configured with a physical fiber cutter for maximum data separation with full optical light borken with a layer 0 device. Requires purchase of a 3rd party device from Echola.

Fixed in AirGap 2.5.8.1-22080

T22930 AirGap Enterprise Replication Nodes require access to Production Network

For AirGap Enterprise, the production cluster nodes that replicate to the vault must also have network connectivity to Eyeglass.

Resolution: A new flag "--protectedManagementNode" has been introduced for adding the production (protected) cluster in the vault agent to identify which node on the production cluster should be used for communication with Eyeglass.

T20932 AirGap Job Reports CSV does not report failed jobs

AirGap Job reports sent out by schedule or created manually do not report on failed jobs in the attached CSV. Failed jobs are correctly reported in the email summary.

Resolution: AirGap job reports CSV now correctly report on failed SynclQ jobs.

New for AirGap 2.5.8-22028

Refer to the previous 2.5.8 build information.

New for AirGap 2.5.8-21330

Refer to the previous 2.5.8 build information.

New for AirGap 2.5.8-21306

T20945 AirGap - Alarm Conditions (AirGap Enterprise)

New alerts were raised under the following conditions for AirGap Enterprise

- starting AirGap job - Informational alert
- finishing AirGap job; - Informational alert SCA0090 Vault AirGap job <job> Succeeded
- reviewing vault agent for new policies or schedule; - Informational alert SCA0095 Ransomware Defender AirGap Schedules query
- AirGap job not respecting schedule; Critical Alert -SCA0096 - Ransomware Defender AirGap job did not run according to schedule
- failed AirGap job; Critical alert - SCA0082 - Ransomware Defender AirGap job <job> failed - needs attention
- vault is opened when no AirGap job is running; Critical alert - SCA0091 - Vault is opened - No running tasks on vault
- maintenance window alarm. - Critical Alert - SCA0091 Vault is opened - Vault is opened for x minutes; when the maintenance window expires, the alarm is cleared from active alarms

New for AirGap 2.5.8-21240 - Controlled

Availability

T21212 AirGap Enterprise does not require Static Route configuration

Managing AirGap Enterprise incorrectly required that the AirGap Basic static route be configured. The static route configuration is no longer required when the airgap job is managed by the vault agent.

T21042 Automated retrieval of vault cluster logs (AirGap Enterprise required)

Automated retrieval of vault cluster logs can now be configured. More information can be found [here](#).

New for AirGap 2.5.8-21213/21222 - Controlled Availability

T19522 AirGap Enterprise

AirGap solution with an inside-the-vault host and VM that opens and closes the vault from within the vault. This is done by removing the replication interfaces from the IP pool which removes the IP address from the interfaces. This mode places a VM inside the vault and disables the IP stack that connects the vault cluster to any outside network.

Documentation for AirGap Enterprise is available here:

- [Inside the Vault mode Deployment \(Enterprise AirGap License Required\)](#)
- [AirGap Enterprise Additional Requirements](#)

Fixed in 2.5.8-21330

T22171 - Log4j Vulnerability - Upgrade to Log4j 2.17.0
(2.5.8-21330 and higher Log4j 2.17.0)

Fixed in 2.5.8-21306

T22033 Log4j Vulnerability - CVE-2021-44228

Resolution: log4j version has been updated to 2.15.0, which has a patch for the vulnerability.

Fixed in 2.5.8-21222

T20770 AirGap Event Retrieval Job Fails with No route to host

AirGap Event Retrieval job uses the IP address configured in Eyeglass to manage the production Powerscale cluster. If that IP address is not associated with a node that is configured in the AirGap pool for replication to the vault then event retrieval fails because the static route applied to the AirGap pool is only applied to the nodes in the pool.

Resolution: The IP address from a node in the AirGap pool is now used for event retrieval. Note that additional sudoer permissions are required as documented [here](#).

T20790 AirGap SynclQ policy timeout uses a failover timeout setting

The amount of time that RansomwareDefender will wait for an AirGap SynclQ job to complete is defined in the Eyeglass system.xml "failovertimeout" setting. Impact: If the "failovertimeout" setting is lower than the time required for the SynclQ policy to complete, the AirGap job will timeout and remove the static routes causing the AirGap SynclQ job to fail with an incomplete update to the vault copy of the data.

Resolution: Eyeglass system.xml now has a separate tag for the timeout setting for AirGap SynclQ policy: airgapJobTimeout. This tag will need to be upgraded to the desired value. Default is 240 minutes.

T20358 Not able to create an AirGap Job Report for a selected period

The AirGap Reports tab feature to Create Report for a custom time frame results in an error and the report is not produced. Impact: This does not affect the daily AirGap job report that is sent out. The issue is specific to custom report generation.

Resolution: Specific timeframe can now be selected.

T19195, T19221 AirGap Job shows success when failed

Under some circumstances if an AirGap job fails, such as running the AirGap SynclQ job or AirGap job source cluster unreachable, the AirGap Config window job status shows success.

Resolution: Alarm and running job info and job history correctly show the failure.

Fixed in 2.5.8-21213

T20766 Cannot view second page of AirGap Config AirGap job list

The AirGap Config list of AirGap jobs list is limited to 10 jobs per page. If you have configured more than 10 jobs, when you navigate to the second page the display is blank.

Resolution: AirGap Jobs are now displayed on all pages.

Known Issues

T15104 Default schedule does not run the job

Airgap jobs are created with a default schedule (daily at midnight) but Status shows as Not Scheduled and jobs never run.

Workaround: Set a manual schedule.

T15300 Error on manually connecting Airgap not displayed

If the command to manually establish connectivity `igls airgap connect` fails it correctly does not apply the static route but the status message indicates that connectivity has been established.

Workaround: Verify from Isilon interface whether pool has static route applied.

T15333 No notification if Airgap jobs are globally disabled

After using the command `igls airgap disable` to globally disable Airgap jobs there is no alarm to notify administrator of this action and no indication in the GUI that action has been taken.

Workaround: Airgap last run date can be used to determine whether it is running on it's schedule.

T16199 No alarm if Airgap event retrieval from Powerscale cluster is in error

If the job to retrieve events from Powerscale cluster encounters an error there is no alarm raised to notify administrator.

Workaround: Login to the Eyeglass GUI and check the status of the event retrieval job.

T16436 Airgap Jobs cannot be manually run from the Airgap window

Airgap Jobs cannot be manually run from the Airgap window.

Workaround: Airgap jobs must be manually run from the Eyeglass Jobs window.

T16456 Customized Airgap schedules reset to default after upgrade

After an upgrade, the Airgap schedules get reset to the default once a day setting.

Workaround: Document schedules prior to upgrade and reapply post upgrade.

T16457 Airgap window not refreshed

After adding a new job the Airgap window is not refreshed to show the new job.

Workaround: Close and reopen the Airgap window.

T16470 Renaming Airgap SynclQ policy does not preserve original settings

If an Airgap Synclq policy is renamed the settings related to this SynclQ policy are not preserved in Eyeglass.

Workaround: Reapply settings in Eyeglass once Inventory has run and the Airgap job with new name is visible in Eyeglass.

T16476 AirGap Job continues to run after Powerscale cluster deleted from Eyeglass

If there are Airgap jobs related to Powerscale cluster that has been deleted from Eyeglass, Eyeglass will continue to attempt to run them but the job will not succeed.

Workaround: None required. No alarm is generated.

T19609, T19632 User Disabled AirGap Job may have status of having been run when it has not

If an AirGap Job is User Disabled in the Jobs window, it may appear in Running Jobs, AirGap Jobs History or show a Last Run date as though it had run after being user disabled even though it did not actually open the vault and run the airgap SynclQ job.

Workaround: Check on Powerscale directly to confirm that AirGap SynclQ job has not been run.

T19631 AirGap Config window time uses Eyeglass appliance timezone

The date and time shown in the AirGap Config window uses the Eyeglass appliance timezone instead of the timezone of the computer which is accessing Eyeglass as is done elsewhere in the GUI.

Workaround: If Eyeglass appliance and local browser time zone are different, manually convert the date / timestamps in the AirGap Config window to the local browser time zone to be able to compare run times in different windows.

T20966 AirGap Job Configuration lost on rediscover or anyrelease restore

If the `igls rediscover` command is executed on Eyeglass with AirGap configuration or an `anyrelease restore` to a new appliance the AirGap Job Configuration for subnet mask and gateway are lost. Schedule is maintained.

Workaround: Consult with support.superna.net before performing either of those operations. Keep an independent record of AirGap job configuration.

T21134 AirGap Basic Job can be started from Jobs window without AirGap role

Any member of a User Role with the Jobs Modify permission can run an AirGap Basic job.

Workaround: Only include Jobs Modify permission for roles where it is required and limit membership to Roles with the Jobs Modify permission.

T21863 AirGap Basic static route remains on error

If an error occurs which leaves the static route behind, there is no mechanism that will automatically remove the static route and it will cause the next scheduled AirGap job to fail.

Workaround: Static route must be removed manually. Introduced in Release 2.5.8 there is a check every 5 minutes to determine whether the vault is open when it shouldn't be that can be used to alert to this condition and that manual removal of static route is required.

T21327 Managed Device Alarms have incorrect date and are sorted oldest to newest

The vault cluster events displayed in Managed Device Alarms have the date/time they were retrieved rather than the actual event date and are sorted oldest to newest.

Workaround: Use pagination to navigate to newer alerts.

T21224 Snapshot schedule job created for AirGap Job

A Snapshot Schedule Configuration Replication job is incorrectly created for each AirGap job and is enabled. When Configuration Replication runs the Snapshot Schedule jobs are also run and result in error for AirGap jobs as the target cluster (vault cluster) is not reachable.

Workaround: Set the Snapshot Schedule jobs for the AirGap Jobs to User Disabled.

T21147 Customizing AirGap policy prefix results in job errors

If the AirGap Job SynclQ policy prefix is customized, existing and new AirGap jobs are in error.

Workaround: Contact support.superna.net for assistance to remove references to previous prefix jobs.

T21659 AirGap state - network disconnected in UI

If a scheduled AirGap job runs and finishes while a maintenance window is active to keep the vault open, on the GUI the AirGap State shows Network Disconnected even though the AirGap is still open as per the maintenance window parameters. Impact: Display only, the AirGap stays open as expected until the maintenance window timer expires at which point it is closed.

Workaround: None required. Once the maintenance window expires, the vault will be closed and you will receive notification as an informational alert

T20945 AirGap Open Check may not detect vault open

AirGap Open Check uses the IP address configured in Eyeglass to manage the production Powerscale cluster. If that IP address is not associated with a node that is configured in the AirGap pool for replication to the vault then the open check will find that the vault cluster is always closed and not detect an open state.

Workaround: For AirGap basic the next AirGap job will error due to static route still being present. For AirGap Enterprise, the vault agent will detect the open vault and close it without any manual intervention and no alarming.

T23094 Vault Cluster Event Retrieval fails for AirGap Basic in 2.5.8.1

As of 2.5.8.1, the task to retrieve alarms from vault cluster during the AirGap job fails and no alarms from the vault cluster are gathered.

Workaround: None available. Until this issue is fixed, AirGap basic customer should not upgrade. Plan to address in a patch release.

T20525 Connectivity check does not work for AirGap Enterprise with Fiber Cutter

The connectivity check command `ecactl airgap check --prod <cluster>` run from the vault agent does not work for AirGap Enterprise configured with Fiber Cutter.

Workaround: Manually open the vault and manually check connectivity.

T23399 No validation when adding vault cluster

There is no validation when adding vault cluster that all required parameters have been configured and that entries have valid format. If misconfigured, AirGap jobs will not run.

Workaround: Use manual process and connectivity check to verify configuration.

T23400 Fiber Cutter Error Handling

If there is an configuration or environmental issue that prevents connectivity on the Fiber Cutter deployment, no error is provided when the AirGap jobs fail.

Workaround: Contact support.superna.net for assistance.

AIRGAP- 404 [Airgap Reports] It shows an Error for the Job when creating a report manually

Manual report creation test- Failed

Reports are getting generated when create manually but It shows an Error for Job

When clicking on AIRGAP Icon & Navigate to Airgap reports and creating a report you observe an error in the jobs window

AIRGAP 416-Vault Agent log archive has incorrect naming

Vault Agent log archive has incorrect naming

AIRGAP-429 Data is replicated when there are active ransomware events

Setup:

1. Pause data replication when active ransomware events detected option checked
2. ransomware events raised
3. Airgap ECS sync job runs on schedule

Reproduced on: 2.5.9-22231

Expected behaviour: The job failed due to active rsw events

Actual behaviour: the job is finished, data replicated, and only a warning message showed

AIRGAP-529 Duplicated heartbeat when the vault cluster is not connecting to the protected cluster

While the connection between the vault cluster and the protected cluster is broken can be seen that heartbeats are duplicated in vault agent logs.

AIRGAP-528 Error message displayed in vault agent console for failed command needs to be fixed

The vault cluster is not communicating with the protected cluster.

All the heartbeats are failing between them.

Known Issues ECS

Airgap-147 Total number of jobs in AirGap report is incorrect

In some cases, there can be a discrepancy between the total shown in the pagination view of airgap jobs history and the number shown in the job report. The number in the report is accurate.

Workaround: use the job report to determine the actual number of jobs run.

Airgap-221 NULL is displayed for Source in Managed Devices Alerts

When proxying alerts from the vault ECS cluster in the ECS airgap solution, the Source is listed as null.

Workaround: none

Airgap-224 Job update to Eyeglass is not working as expected

When adding a new job to ecssync, sometimes the update does not get pushed to eyeglass and the user has to run `ecactl ecssync updatejobs` to force it to update.

Workaround: run `ecactl ecssync updatejobs` every time after modifying the jobs on ecssync.

Airgap-289 Active RWD events are ignored when starting AirGap ECSSync jobs from UI using Run Now

AirGap ECSSync jobs with the 'Pause data replication when active ransomware events detected' option selected and the jobs are started from UI using Run Now, the jobs will continue to run with active RWD events.

Workaround: Setup the schedule for the jobs or start the job with CLI command `'ecactl ecssync startjob --job xxx'`

Airgap-226 Docker issues in Vault Agent

Docker may stop working if the ECS sync cluster up for a long period of time.

Workaround: Contact Superna customer support or run

- ecactl cluster down
 - sudo systemctl restart docker
 - remove docker network: docker network rm <TAB>
 - ecactl cluster up
-

AIRGAP-372 Not all the AirGap ECSSync jobs are started when scheduled

On the multi-vault system that has 3 vaults managed by the same eyeglass, each vault has 5 jobs. All 15 AirGap ECSSync jobs are scheduled to run at the same time, every 15 minutes. On the second vault agent, only 3 out of 5 jobs are started automatically

AIRGAP-569 The number of files is different in ECSSync UI than what is displayed in ECS

The number of processed files displayed in the ECSSync UI is half of the number that the user actually sees in the ECS UI.

Known Limitations

T19614 AirGap Job consideration of Easy Auditor Active Auditor Active Event not configurable

Suppose in the Easy Auditor Active Auditor "Active Events" list, and there is an Active Event listed at the time when the AirGap job is scheduled to run. In that case, the AirGap Job will be blocked from running with the message "Found active RSW events,

will not run AirGap job..." In the AirGap Config GUI, the job AirGap State is "Disabled for Active Events", and the Status is Error.

Easy Auditor Active Events should be managed and cleared not to impact AirGap jobs. This behaviour may be configurable in a future release to specify whether or not active auditor events block AirGap jobs.

T21316 Vault stays open for vault cluster event retrieval

If event retrieval from the vault cluster takes longer than running the AirGap SyncIQ job, the vault will stay open until the event retrieval step completes after which it will be closed.

T21274 Alarm raised for vault open in Eyeglass is not cleared after maintenance window is finished

Alarm raised when vault manually opened for maintenance window is not cleared once the maintenance window is ended and vault is closed again. Alarm is able to be manually cleared.

T21851 AirGap Enterprise vault open alarm limitation

In the interval between when the the vault is opened and the associated task is started, a vault open alarm may be triggered as the related task has not been started so the condition of vault open when it should not be is detected.

Workaround: Verify that an associated vault task such as running airgap job or checking for schedule has started shortly after the alarm was raised.

Airgap-329 Vault agent names must be case-insensitively unique

Vault agent names must be case-insensitively unique when you have multiple vault agents added.

AIRGAP-427 Airgap ECS sync jobs get duplicated sometimes

Airgap ECS sync jobs get duplicated sometimes

workaround:

Remove the duplicated job from ECS sync UI

© Superna Inc

1.6. Current Release - Release Notes

Ransomware Defender

[Home](#) [Top](#)

- [What's New in Superna Eyeglass Ransomware Defender Edition Release 2.5.9](#)
- [Supported OneFS releases](#)
- [Supported Eyeglass releases](#)
- [Active Directory Compatibility](#)
- [End of Life Notifications](#)
- [Support Removed in Eyeglass Release 2.5.9](#)
- [Deprecation Notices](#)
- [New / Enhanced / Fixed in 2.5.9](#)
- [New in 2.5.8.1-22116](#)
- [Fixed in 2.5.8.1-22116](#)
 - [Technical Advisory 31 - Ransomware Defender NFS Event Detection Always Enabled in 2.5.8.1-22080/22100](#)
- [New in 2.5.8.1-22100](#)
- [Fixed in 2.5.8.1-22100](#)
- [New in 2.5.8.1-22080](#)
 - [T22197 Ransomware Defender Read-Only Role](#)
 - [T22328 Ransomware Defender Event csv file storage](#)
 - [T20285 Action menu for historical events now has option to restore access](#)
- [Fixed in 2.5.8.1-22080](#)
 - [T21207 Custom Snapshot Expiry not preserved after modifying Settings on Threshold menu](#)
 - [T21261 Cannot edit a user configured in the Ignored List or Monitor Only Settings](#)
- [New/Fixed in 2.5.8-22028](#)

- New in 2.5.8-21330
- Fixed in 2.5.8-21330
- Security
 - T22171 - Log4j Vulnerability - Upgrade to Log4j 2.17.0 (2.5.8-21330 and higher Log4j 2.17.0)
- New in 2.5.8-21306
 - Ransomware Defender Snapshot Management Enhancements
 - T19619 Critical Path Snapshot
 - T19823 Snapshot Budget
 - T15666 New Behaviour Detections Enabled
 - T21215 New SmartAirgap API
 - NEW - OneFS 9.3 Support
- Fixed in 2.5.8-21306
 - T22033 Log4j Vulnerability - CVE-2021-44228
 - T11832 Ransomware Security Event which is promoted from Warning to Major does not respect Major Grace Period
 - T18985 igls rsw restoreaccess cannot restore access for unresolvable user
- Technical Advisories
- Known Issues
- Threat Detection
 - T4151 Action Window Event Action History does not show Unreachable Cluster
 - T3732 Restored permission may be incorrect for consecutive lockouts
 - T4081 Time Zone Mismatch between Ransomware Defender Security Guard Job History and Event History dates
 - T22321 Escalation from major to critical will not change GUI status and lockout delay is blocked
 - T4777 Snapshots not created for any Events that are Active when the Snapshot feature is enabled
 - T4819 Empty Event History List

- T4950 Alarm text for failed Snapshot delete references Snapshot create
- T4955 Subsequent Create Snapshot action will delete reference to previously created snapshots if an error occurs during the create
- T5024 Major Events may reappear in the Active Events list after being recovered
- T5756 Error on restoring permissions does not raise an alarm
- T5954 Events that are promoted to Major due to multiple event “Upgrade to Major” are locked out immediately
- T6728 Extensions with special characters cannot be removed from the ignore list
- T7062 User may not be locked out in a multi-user security event
- T7190 Active Events may show State of Warning instead of Monitor when Monitor Mode is enabled
- T11586 NFS Lockout Event Information does not include NFS Export path
- T11590 NFS Lockout Event does not generate a PowerScale snapshot
- T14339 Restore Access Alarm must be manually cleared
- T15198, T15650 Ransomware Events may have inaccurate Signal Strength or may be reprocessed
- T15639 T18812 Error replicating AD Group or Local User Run as Root SMB permissions affects Lockout and Restore
- T16229 GUI incorrectly reports error when manually creating a snapshot
- T16462 NFS lockout may fail
- T18271 Ransomware Event State incorrect shows success when Powerscale is unreachable during restore operation
- T18643, T19217 State of Active Event shows WARNING when it should be MONITOR for File Filter in Monitor
- T18718 igls rsw allowed files remove option not working
- T18852 Ransomware Defender does not detect where path has square brackets []
- T18887 Security Guard in Learned Thresholds prevents Security Guard job from detecting

- T18895 Ransomware Learned Threshold list doesn't open first time
- T19040 After upgrade to 2.5.7, Ransomware Events in Event History do not display the Signal Strength correctly
- T19106 Acknowledge/Archive options not blocked while lockout in progress
- T19198 Multiple concurrent Major Events not upgraded to Critical based on "Upgrade to Critical (events)" setting
- T19236 Honeypot file detector incorrectly crosses Major threshold in Monitor Mode
- T19356 Files/Folders with language characters not displayed properly in CSV and email
- T19409 Well known extension detection not working under some circumstances
- T20094 CLI command to restore access does not work when user name contains special characters
- T23012 Restore access for NFS lockout from Event History does not complete
- Security Guard
 - T4197 Security Guard Error for Unlicensed Cluster
 - T4228 Security Guard Temporary Errors
 - T4965 Security Guard User Authentication Fails
 - T15175 Existing Security Guard Logs lost formatting after upgrade to 2.5.6
- Manage Services
 - T4192 Manage Services status not accurate after ECA Node Down
- General
 - T4230 Blank Ransomware Defender Window
 - T4183 Refresh does not work for Ransomware Defender multi-page lists
 - T15457 HTML 5 vmware vcenter bug on OVA deployment
 - T4336 Eyeglass Restore does not restore Security Guard Job History
 - T4549 Ransomware Defender Settings Submit button enabled when no changes made
 - T6617 PowerScale Directory Selector does not display hidden directories

- T18810 GUI not updated after cancelling an operation to switch modes
- T18660 Cannot use cloudapps URL to access Well Known Ransomware File Extension list
- T22450 Easy Auditor Event Rate alarm for Ransomware Defender Only deployments
- RWD-114 Creating Critical Path Snapshots is blocked
- RWD-113 Wrong Ransomware event state when created with POST `/v2/ransomware/lockout/{user}`
- RWD-228 Syntax error in on-boot preventing proper startup timing.
- Features
 - RWD-146 [RWD-NFS Event] Lockout option in Actions is also removed for SMB event when set `igls rsw nfsevents set --enabled=snapshotonly`
 - RWD-145 [RWD-NFS Event] Major & critical events are locked out with default rule when reach threshold value even if `igls rsw nfsevents set --enabled=snapshotonly`
 - RWD-217 Event fails to upgrade with multiple user (ECS events only)
 - RWD-85 zookeeper cleanup cron is not running as scheduled
 - RWD-74 zookeeper cleanup cron is not running as scheduled
 - RWD -192 Kafka topic empty after cluster down/up
 - RWD-222 enable `zkcleanup.timer` by default
 - RWD-246 Files with non-ASCII characters fail to recover
- Known Limitations
- Threat Detection
 - T6914 Some extensions still result in lockout when added to the ignore list
 - T15705 After upgrade to 2.5.6 cannot download CSV for Ransomware Event Files from events detected in prior releases
 - T16723 Error on Lockout of Shares on DR cluster
 - T17287 Many Access Zones slows down creation of snapshots and lockout
 - T7574 Option to set learned threshold for Security Guard in `RESTORED_USER_ACCESS` state

- T18733 Ransomware Defender Affected Files Download Menu Naming
- General
 - T16137 Anyrelease restore does not restore all Ransomware Defender and Easy Auditor settings
 - T16821 anyrelease restore restrictions for restore to 2.5.7
 - T20370 Monitor Only Settings Client IP applies to all PowerScale clusters
 - T21852 RSW - Cannot configure and run SG after anyrelease backup and restore from an earlier build
 - T21208 Snapshots taken using Action Menu for Ransomware Defender Event follow Ransomware / Snapshots settings
 - T21110 Ransomware Defender / Snapshots User Share Snapshot Settings also applies for NFS detections
 - Well Known Ransomware File Extension Whitelist management is not available when a proxy used
 - T17624 Ransomware Defender NFS detection creates snapshot on SMB shares with Everyone permission
 - RWD-75 Page-1 gets hide when navigate to Page-2 & archive all events from this page

What's New in Superna Eyeglass Ransomware Defender Edition Release 2.5.9

What's New In Superna Eyeglass Ransomware Defender Edition Release 2.5.9 can be found [here](#).

Supported OneFS releases

8.2.0.x

8.2.1.x

8.2.2.x

9.0

9.1

9.2.x

9.3

Supported Eyeglass releases

Superna Eyeglass Ransomware Defender Version	Superna Eyeglass Version
2.5.9-22231	2.5.9-22231
2.5.8.1-22116	2.5.8.1-22116
2.5.8.1-22100	2.5.8.1-22100
2.5.8.1-22080	2.5.8.1-22080
2.5.8-22028	2.5.8-22028
2.5.8-21330	2.5.8-21330
2.5.8-21306	2.5.8-21306
2.5.7.1-21161	2.5.7.1-21161
2.5.7.1-21140	2.5.7.1-21140
2.5.7-21096	2.5.7-21096
2.5.7-21081	2.5.7-21081
2.5.7-21068	2.5.7-21068
2.5.6-20263	2.5.6-20263

Active Directory Compatibility

Ransomware Defender Versions	Supported Active Directory Versions
2.5.9, 2.5.8, 2.5.7, 2.5.6 all versions	Microsoft Active Directory 2012, 2016

End of Life Notifications

End of Life Notifications for all products are available [here](#).

Support Removed in Eyeglass Release 2.5.9

No features removed at this time

Deprecation Notices

No deprecation notices at this time.

New / Enhanced / Fixed in 2.5.9

Recovery Manager: Now included in ransomware defender is the ability to selectively view and recover all files that were affected by a ransomware event.

New in 2.5.8.1-22116

Refer to previous 2.5.8.1 builds.

Fixed in 2.5.8.1-22116

Technical Advisory 31 - Ransomware Defender NFS
Event Detection Always Enabled in 2.5.8.1-22080/22100

[Technical Advisory 31](#) is resolved in 2.5.8.1-22116.

New in 2.5.8.1-22100

Refer to previous 2.5.8.1 builds.

Fixed in 2.5.8.1-22100

Refer to previous 2.5.8.1 builds.

New in 2.5.8.1-22080

T22197 Ransomware Defender Read-Only Role

In the User Roles window there is a new option `RANSOMWARE_READONLY` to provide read only access to the Ransomware Defender window.

T22328 Ransomware Defender Event csv file storage

To improve disk space management on the operating system disk of the Eyeglass appliance, storage of the Ransomware Defender csv files used to store user event details has been moved to the larger disk used for storing larger application files such as log.

T20285 Action menu for historical events now has option to restore access

The Action menu for Ransomware Defender events in the Event History now has an option to Restore User Access.

Fixed in 2.5.8.1-22080

T21207 Custom Snapshot Expiry not preserved after modifying Settings on Threshold menu

A custom snapshot expiry set using the `igls rsw generalsettings set -- snapshot_expiry_hours` command is reverted to the default value of 48 hours if there

are any changes made and saved in the Ransomware Defender Threshold menu. No impact to snapshot creation, only the schedule is reverted to default.

Resolution: Custom snapshot expiry is now preserved.

T21261 Cannot edit a user configured in the Ignored List or Monitor Only Settings

Cannot edit entries for users configured in the Ignored List or Monitor Only Settings. The Save button has no action. Path and IP Address can be edited.

Resolution: User can now be edited in the Ignored List and Monitor Only Settings.

New/Fixed in 2.5.8-22028

Refer to previous 2.5.8 builds.

New in 2.5.8-21330

Refer to previous 2.5.8 builds.

Fixed in 2.5.8-21330

Security

T22171 - Log4j Vulnerability - Upgrade to Log4j 2.17.0
(2.5.8-21330 and higher Log4j 2.17.0)

New in 2.5.8-21306

See What's New in Ransomware Defender [here](#).

Ransomware Defender Snapshot Management Enhancements

The Ransomware Defender window has a new Snapshots menu where the new snapshot related features Snapshot Budget and Critical Path Snapshot will be managed. In addition, it is now possible to disable user share/export snapshots.

Documentation for Snapshot Management can be found [here](#).

To maintain existing snapshot behaviour to take a snapshot at the base path of all shares that associated account has access to, ensure that the User Share Snapshot Settings “Enable Share Snapshots” checkbox is checked.

T19619 Critical Path Snapshot

Introduced in 2.5.8 one or more paths can be configured to always have a snapshot created for any detection.

T19823 Snapshot Budget

Going forward Ransomware Defender (2.5.8 build 21213 and higher) maximum number of snapshots created will be the configured Snapshot Budget (default is 5000). Prior to creating snapshots, Ransomware Defender will determine the number of Ransomware Defender specific snapshots (snapshot name starts with igls) and only if less than the snapshot budget will proceed with the snapshot step. If snapshots cannot be created due to snapshot budget a critical severity alarm is sent and the Event Action History is updated as well.

T15666 New Behaviour Detections Enabled

New behaviour detections are available and enabled by default.

IMPORTANT: This may introduce new detections that will need to be evaluated to determine whether additional tuning of Ransomware Defender settings is required. Recommend to enable Learning Mode after upgrade and verify no new events after several days. NOTE: Learning mode offers full file system protection.

T21215 New SmartAirgap API

New API is available that allows external applications to determine whether there are any active Ransomware Defender or Easy Auditor active events. More information can be found [here](#).

NEW - OneFS 9.3 Support

Support for OneFS 9.3 is introduced in release 2.5.8.

Fixed in 2.5.8-21306

T22033 Log4j Vulnerability - CVE-2021-44228

Resolution: log4j version updated to 2.15.0 which has patch for the vulnerability.

T11832 Ransomware Security Event which is promoted from Warning to Major does not respect Major Grace Period

If a Ransomware Security Event is promoted from Warning to Major threshold, the associated user is locked out right away instead of starting Grace Period timer and only locking out if Grace Period has expired and no manual action has been taken. Note that a Ransomware Defender Security event which is raised at the Major level will respect the configured Grace Period.

Resolution: Major threshold Grace Period timer is now respected.

T18985 igls rsw restoreaccess cannot restore access for unresolvable user

If the user specified in the igls rsw restoreaccess cannot be resolved by the Access Zone AD provider. For example, a lockout might occur on shares provisioned with the Everyone permission even when the Access Zone AD provider cannot resolve the AD user.

Resolution: the igls rsw restoreaccess command can now be used to restore access for unresolvable user. Note that when using CLI to restore access the GUI is not updated with the new state.

Technical Advisories

Technical Advisories for all products are available [here](#).

Known Issues

Threat Detection

T4151 Action Window Event Action History does not show Unreachable Cluster

In the event that a Cluster is unreachable during a Lockout operation, the Active Event state will correctly show ERROR and the Event Action History will show “Partially Locked out” but does not display the cluster that was unreachable or the shares that could not be locked out.

Workaround: Manually inspect the clusters that were locked out. Any missing cluster under management need to review the shares and determine which the affected user has access to and then manually block access.

T3732 Restored permission may be incorrect for consecutive lockouts

In the event that user share access has been locked and subsequently restored and another lockout occurs before Eyeglass inventory has run, the “restore” permissions associated with shares may be the lockout settings from the previous lockout.

Workaround: Permissions should be restored manually by removing the deny permission for the affected user. Use the Event Action History to determine the affected shares.

T4081 Time Zone Mismatch between Ransomware Defender Security Guard Job History and Event History dates

The Ransomware Defender Job History “Run Date” is based on the Eyeglass appliance time zone whereas the Event History “Detected” date is translated to the client browser locale.

Workaround: Translate date for 1 of the dates to the time zone of the other date to correlate Security Guard Jobs to events in the Event History.

T4151 Action Window Event Action History does not show Unreachable Cluster

In the event that a Cluster is unreachable during a Lockout operation, the Active Event state will correctly show ERROR and the Event Action History will show “Partially

Locked out” but does not display the cluster that was unreachable or the shares that could not be locked out.

Workaround: Manually inspect the clusters that were locked out. Any missing cluster under management need to review the shares and determine which the affected user has access to and then manually block access.

T22321 Escalation from major to critical will not change GUI status and lockout delay is blocked

multi event escalation will block delayed lockout even if the UI shows delayed lockout.

Workaround: Change the multi event threshold to a higher value or make sure you do not leave many active events collect to avoid escalated response settings on the settings tab. These values should be increased if you plan to leave many active warning events without resolving them.

T4777 Snapshots not created for any Events that are Active when the Snapshot feature is enabled

If there are any Active Events when the Create Snapshot option is enabled, no Snapshots will be created for these already Active Events.

Workaround: Enable the Create Snapshot option when there are no Active Events. Events raised after the Create Snapshot option was enabled will have associated Snapshots created for affected shares.

T4819 Empty Event History List

There may be conditions where having other windows open such as the Event Action History may result in the Event History list being displayed with no entries.

Workaround: Close all Ransomware Defender related windows and then re-open the Ransomware Defender -> Event History tab.

T4950 Alarm text for failed Snapshot delete references Snapshot create

The alarm that is raised when a Snapshot delete fails contains the text “Failed to create snapshots” instead of “Failed to delete snapshots”.

Workaround: Check the Action Log for the event to determine whether a snapshot create or delete has failed.

T4955 Subsequent Create Snapshot action will delete reference to previously created snapshots if an error occurs during the create

The Create Snapshot action can be executed multiple times for a given event. If it has been run previously and then run again and the subsequent run has an error on creating any snapshot, the Snapshots list only contains the snapshots from the last run. Previously created snapshots are no longer displayed.

Workaround: Check the Event Action History log for complete list of created snapshots.

T5024 Major Events may reappear in the Active Events list after being recovered

An event which crosses the Major threshold and is recovered to Historical Events without being locked out (Stop lockout timer) may appear in the Active Events list again immediately after being recovered (Mark as recovered).

Workaround: Stop the lockout timer and Mark the event as recovered again. This may have to be repeated several times. Locking the affected user out followed by Restore User Access and then archiving the event as recovered may also resolve this issue.

T5756 Error on restoring permissions does not raise an alarm

If permissions restore action encounters an error there is no associated alarm notification.

Workaround: Review the Action History for the Event to confirm that all restores were successful.

T5954 Events that are promoted to Major due to multiple event “Upgrade to Major” are locked out immediately

For the case where there are multiple Warning events that cross the “Upgrade to Major” limit, when they are promoted to Major they are locked out right away instead of waiting for the configured Grace Period before locking out.

Workaround: The occurrence of this behaviour can be reduced by setting the “Upgrade to Major” threshold to a high number of users.

T6728 Extensions with special characters cannot be removed from the ignore list

Extensions have been added to the extension ignore list using the `igls rsw allowedfiles add --extensions` command cannot be removed from the ignore list using the `igls rsw allowedfiles remove --extensions` command.

Workaround: Contact Superna Support at support.superna.net to assist with removing these extensions.

T7062 User may not be locked out in a multi-user security event

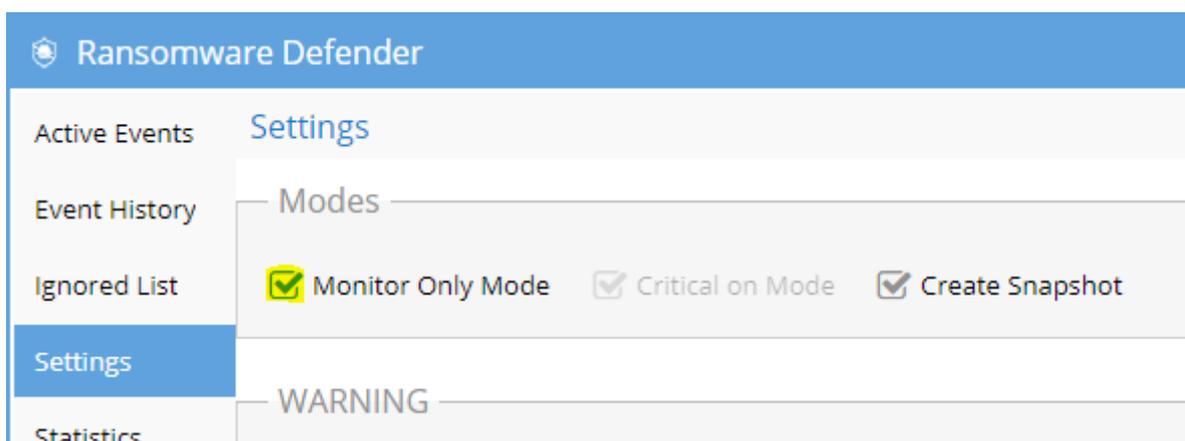
It may occur that a user is only partially locked out when a multi-user lockout is occurring due to an error response from the PowerScale cluster during user resolution in Active Directory. In this case the error is not displayed in the Eyeglass event history.

Workaround: The Event History will contain the shares that were successfully locked out. Should events continue to be generated against the user for the unlocked share, it may be locked out as a result of subsequent event. User may also be locked out manually by adding the deny permission manually to share that was not locked out.

T7190 Active Events may show State of Warning instead of Monitor when Monitor Mode is enabled

Instead of the event state being Monitor in Active Events when Monitor Mode is enabled, the event state may incorrectly display as Warning instead.

Workaround: None Required. This is a display issue only. Verify that Monitor Mode is enabled on the Ransomware Defender / Settings tab.



T7525 Affected Files also shows Active Auditor Affected Files

When viewing the Affected Files for a Ransomware Defender security event, any files associated with an Active Auditor event that has occurred at the same time are also displayed.

Workaround: Download the csv file and use the path associated with the Ransomware Defender event from the GUI to filter the results.

T11586 NFS Lockout Event Information does not include NFS Export path

The Ransomware Defender event GUI for an NFS client displays the NFS Export ID in the Locked out shares view in the "Share" column but does not display the corresponding path in the Path column.

Workaround: Verify NFS Export path from PowerScale directly referencing the NFS Export ID from the Locked out shares window.

T11590 NFS Lockout Event does not generate an PowerScale snapshot

When a Ransomware Security Event is detected for an NFS client, the PowerScale snapshot against related paths is not created.

Workaround: Upgrade to release 2.5.8 and use critical path snapshot feature. PowerScale scheduled snapshots may also be available for recovery.

T14339 Restore Access Alarm must be manually cleared

A Restore Access alarm is generated when restoring access to user. Subsequent restore will not update an existing restore alarm or send a notification.

Workaround: After restoring access to user, in the Alarms window manually clear the alarm in order to receive notification on a subsequent restore.

T15198, T15650 Ransomware Events may have inaccurate Signal Strength or may be reprocessed

Ransomware Event processing may receive duplicate events and as a result may show a higher Signal Strength than is actually the case. The associated csv will also show duplicate entries for the same file. Ransomware processing may also intermittently skip a signal and as a result may show lower Signal Strength.

In some cases this may also result in a Ransomware Event being reprocessed at a later time.

Workaround: None required. The duplicate events result in early detection of Ransomware events. Skipping of signals is intermittent and subsequent signals cross threshold for detection.

T15639 T18812 Error replicating AD Group or Local User Run as Root SMB permissions affects Lockout and Restore

In some cases an SMB share permission that is configured with an AD group or Local User that has Run as Root privileges has an error on share updates for Ransomware Defender that blocks Lockout such that it does not take effect or on Restore it does not restore the Run as Root SMB share permission.

Important: If you use run as root on shares you are exposing data to very high security risk since no lockout will be possible. This is because the user SID that is sent when an AD user accesses data with run as root enabled is the root user SID not the actual AD user SID.

We recommend to NOT use run as root on shares for the reason above and it fails all security audits of PowerScale in all industry standards (PCI, HIPPA, FedRAMP, ITSG, etc...). Remove run as root option on all shares.

Please review our documentation for more information: [Securing root user on PowerScale](#).

Workaround: Manually restore or lockout user.

T16229 GUI incorrectly reports error when manually creating a snapshot

If you use the Action menu to manually create a snapshot, the GUI shows an error but the snapshot is actually created. Automatic snapshot creation as part of active event detection is not affected by this issue.

Workaround: None required as snapshot is created. Verify snapshot creation using Powerscale OneFS interface.

T16462 NFS lockout may fail

Under some conditions Ransomware Defender successfully detects security event and notifies regarding the event but the associated NFS lockout action fails.

Workaround: Manual steps to block access to the Powerscale cluster are required in this case.

T18271 Ransomware Event State incorrect shows success when Powerscale is unreachable during restore operation

If a Restore operation is initiated on an Active Event when the Powerscale cluster is unreachable, the restore steps will fail but the state of the Event on the Active Events GUI is ACCESS_RESTORED.

Workaround: None required. The Event Action History shows that the restore step failed. Once connectivity to the Powerscale cluster is restored the Restore operation can be retried.

T18643, T19217 State of Active Event shows WARNING when it should be MONITOR for File Filter in Monitor

When Ransomware Defender is configured for Enforcement Mode and Critical on Mode, an Active Event related to a File Filters extension in Monitor will be displayed in Active Events with State of WARNING instead of MONITOR.

No impact on behaviour, no lockout applied.

Impact to Automatic learning - the File Filter extension is not set to disabled.

Workaround: Review events and put File Filter extension into Disabled as required.

T18718 igls rsw allowed files remove option not working

The igls rsw allowed files CLI command executes and reports success but does not actually activate the extension or file entered in the command.

Workaround: Use the Eyeglass GUI to enable items from the File Filter list that had been previously disabled. For more information refer to documentation [here](#).

T18852 Ransomware Defender does not detect where path has square brackets []

If path or file name on Powerscale cluster includes square Ransomware Defender encounters an error on processing and does not detect the security event.

Workaround: None available. Ransomware manipulation of other path/file continue to be monitored and acted upon.

T18887 Security Guard in Learned Thresholds prevents Security Guard job from detecting

If the Security Guard user is deleted from the Learned Threshold list it continues to be enforced and Security Guard events are not detected by Ransomware Defender. This will occur if Security Guard was in the Flag as False Positive list prior to upgrade to 2.5.7. In 2.5.7 Security Guard user cannot be added to the Learned Threshold list.

Workaround: Contact support.superna.net for assistance if after upgrade to 2.5.7 the Security Guard user needs to be removed from the Learned Threshold list.

T18895 Ransomware Learned Threshold list doesn't open first time

Under some conditions where name resolution proceeds slowly and/or Learned Threshold list contains many entries, list will not be displayed before 45s timeout occurs.

Workaround: Selecting the list a second time displays the list.

T19040 After upgrade to 2.5.7, Ransomware Events in Event History do not display the Signal Strength correctly

Signal strength not displayed correctly for Ransomware Events in the Event History after upgrade to 2.5.7 for events that were added to Event History in previous release.

Workaround: None required. These events had already been managed and archived on previous release.

T19106 Acknowledge/Archive options not blocked while lockout in progress

The Acknowledge / Archive options are incorrectly available to be used in the window of time between when the lockout action starts and the active event enters the Locked Out state. Impact: If selected during that window, the event never enters the Locked Out state and even though it is locked out and there for the restore option is not available to restore permissions.

Workaround: The Event Action History correctly documents the shares that were locked out and the account and time of lockout. The account can be restored from the command line following the instructions [here](#) for `igls rsw restoreaccess` command.

T19198 Multiple concurrent Major Events not upgraded to Critical based on "Upgrade to Critical (events)" setting

The setting to promote Active Events from Major to Critical without having to reach the Critical Threshold, "Upgrade to Critical (events) " is not respected. Events are not promoted until their Signal Strength Threshold crosses the Critical setting.

None Required: Events will be promoted if their Signal Strength Threshold crosses into Critical threshold and Lockout will be applied. For events that remain at Major severity if no manual steps taken, Lockout will be applied once grace period expires.

T19236 Honeypot file detector incorrectly crosses Major threshold in Monitor Mode

When Ransomware Defender has Monitor Mode active the Honeypot file detector incorrectly promotes a Honeypot event to Major instead of staying in Monitor state. Once promoted to Major the Grace Period timer begins and if no manual steps taken a lockout of the account will occur once the grace period expires.

Workaround: Upon notification of the Major event, manual steps can be taken from the Active Event Action menu to stop the Lockout timer and resolve the event from the GUI if appropriate. If a lockout occurs access can be restored through the GUI from the Active Event Action menu as well if appropriate.

T19356 Files/Folders with language characters not displayed properly in CSV and email

If the files/folders associated with a detected Ransomware security event contain language specific characters, the path/file names are not displayed correctly in the email sent as well as the CSV.

Workaround: Use the GUI to see the files and folders.

T19409 Well known extension detection not working under some circumstances

Under some circumstances when there have been no customization to the File Filters for well known extension detection, the well known vector for detection of Ransomware security event is skipped.

This does not affect the user behaviour or honeypot detection vectors.

Workaround: User behaviour and honeypot detection vectors still available for monitoring.

T20094 CLI command to restore access does not work when user name contains special characters

The `igls rsw restoreaccess` command does not execute if the user name contains special characters. Impact: No impact on lockout. Impact on ability to restore access.

Workaround: Use the Ransomware Defender Action Event history to identify all shares that were locked out and manually remove the deny permission using Powerscale native tools.

T23012 Restore access for NFS lockout from Event History does not complete

Using the Restore User Access option in the Event History for an unresolved NFS lockout will restore the permissions as expected but the job gets stuck at the Restore job initiated step and the overall status does not change to Recovered and no alarm is sent.

Workaround: Verify manually using OneFS native tools that client list for NFS export has been restored as expected.

Security Guard

T4197 Security Guard Error for Unlicensed Cluster

Security Guard fails when PowerScale Cluster selected to run is not licensed.

Since Ransomware Defender dynamically picks priority PowerScale Clusters to license (refer to [Eyeglass Ransomware Defender Admin Guide](#) for details on selection of licensed cluster) for the case where Eyeglass is managing more clusters than there are Ransomware Defender Agent Licenses, one cannot be sure the selected Cluster in Security Guard is actually licensed at the run time.

Workaround: Deploy same number of Ransomware Defender Agent Licenses as the number of PowerScale Clusters being managed by Eyeglass.

T8889 Cannot enable Security Guard with default schedule for on a newly deployed 2.5.3 ovf

The drop down list to schedule security has an invalid default.

Workaround: Click the drop down and set a valid schedule.

T4228 Security Guard Temporary Errors

Security Guard may occasionally error with 0 files written.

Workaround: This condition typically clears it self on the next Security Guard run. It does not affect workflow for a real security event.

If it does not clear, follow these steps to recover:

1. Archive as Unresolved
 2. Run Security Guard manually to ensure that it is operational again.
-

T4965 Security Guard User Authentication Fails

When provisioning the Security Guard Active Directory User and password, Eyeglass checks that the username name and password entered can be successfully authenticated. It may occur on initial configuration that you will see the message “user could not be authenticated” even though the username and password are correct.

Workaround: After confirming that the username and password are correct, subsequent provisioning is successful.

T7574 Flag as False Positive Option should not be available for Security Guard Events

Security Guard provides automated end to end validation of Ransomware detection, lockout and restore and therefore should not be flagged as false positive. The Flag as False positive option is currently available to be selected for Security Guard events and should not be.

Workaround: Manual process required to prevent applying Flag as False positive to Security Guard events.

T15175 Existing Security Guard Logs lost formatting after upgrade to 2.5.6

Any existing Security Guard logs viewed from the Eyeglass GUI will have lost the formatting.

Workaround: None required. New logs will have the correct formatting.

Manage Services

T4192 Manage Services status not accurate after ECA Node Down

After an ECA node has been powered off / gone down and subsequently powered back on and rejoined to the ECA cluster it continues to display the Inactive state in the Eyeglass Manage Services window even when it is active again and healthy.

Workaround: Once the node is back up, remove it from the Manage Services window by selecting the X in the node's row. Wait 1 to 2 minutes and the service should be rediscovered with the correct state.

General

T4230 Blank Ransomware Defender Window

After archiving an Event the Ransomware Defender window tabs may appear empty.

Workaround: Close and reopen the Ransomware Defender window.

T4183 Refresh does not work for Ransomware Defender multi-page lists

Ransomware Defender window with multiple pages is not updated by Refresh except for the first page.

Workaround: To update the list go back to the first page of the list.

T15457 HTML 5 vmware vcenter bug on OVA deployment

Some versions of vmware vcenter HTML user interface have a known issue with OVA properties being read correctly post power on, leading to first boot issues.

Workaround: use the Flash client as a work around.

T4336 Eyeglass Restore does not restore Security Guard Job History

Security Guard historical log files are not restored when you restore configuration from backup.

Workaround: None available.

T4549 Ransomware Defender Settings Submit button enabled when no changes made

When the Ransomware Defender Settings window is opened, the Submit button is enabled even though no changes have been made to any settings. If you navigate to another view and come back to Settings, the Submit button is then correctly disabled until a change is made on the page.

Workaround: None required.

T6617 PowerScale Directory Selector does not display hidden directories

Directories that start with a dot (.) are not displayed in the PowerScale Directory Selector.

Workaround: Use the PowerScale Directory Selector to enter \ifs\ and then enter the remainder of the path manually.

T8807 Deleting cluster from Eyeglass does not clear associated Ignore List and Wiretap settings

When an PowerScale cluster is deleted from management in Eyeglass, any associated Ransomware Defender Ignore List or Wiretap settings are not cleared.

Workaround: Manually delete Ignore List and Wiretap settings for deleted clusters.

T18810 GUI not updated after cancelling an operation to switch modes

In the Ransomware Defender Thresholds window, if you are switching between Advanced and Monitor or Advanced and Enforcement mode and upon being prompted you select No to cancel the operation, the GUI does not refresh and return to the original Advanced mode. Impact: Display issue only, the mode change is cancelled.

Workaround: Switch between tabs in the Ransomware Defender window or use the Eyeglass desktop Refresh Now button.

T18660 Cannot use cloudapps URL to access Well Known Ransomware File Extension list

The cloudapps URL documented [here](#) for accessing the Well Know Ransomware File Extension list does not resolve and returns a 404 response code.

Workaround: Following URL does resolve and can be used to manage the Well Known Ransomware File Extension list:

<https://storage.googleapis.com/rwdefender.superna.net>

T22450 Easy Auditor Event Rate alarm for Ransomware Defender Only deployments

RWD-114 Creating Critical Path Snapshots is blocked

Creating critical path snapshots is blocked when the amount of critical snapshot paths is over the snapshot budget.

Workaround: Raise the snapshot budget and create critical path snapshots again after the cooldown period.

RWD-113 Wrong Ransomware event state when created with POST /v2/ransomware/lockout/{user}

The Ransomware event that is created using POST /v2/ransomware/lockout/{user} API call has TO_LOCKOUT state. This event should be created with LOCKED_OUT state.

Workaround: manually run the lockout job from the actions menu on the event.

RWD-228 Syntax error in on-boot preventing proper startup timing.

Workaround: not necessary, verify startup has finished on other nodes if applicable before attempting to use the ECA.

Features

RWD-146 [RWD-NFS Event] Lockout option in Actions is also removed for SMB event when set `igls rsw nfsevents set --enabled=snapshotonly`

Lockout option in Actions is also removed for SMB event when set `igls rsw nfsevents set --enabled=snapshotonly`

Workaround: you can set `igls rsw nfsevents set --enabled=true/false/snapshotonly`

RWD-145 [RWD-NFS Event] Major & critical events are locked out with default rule when reach threshold value even if - `igls rsw nfsevents set --enabled=snapshotonly`

Major & critical events are locked out with default rule when reach threshold value even if -

`igls rsw nfsevents set --enabled=snapshotonly`

Steps-

- 1.Set igls rsw nfsevents set --enabled=snapshotonly in eyeglass
- 2.Raise NFS Event with Major/Critical severity (Detector Mode -Enforcement)
3. Observe Locked out event with critical severity & Major event locked out after expiry

Expected Result -

It should not lockout nfs event even when we reach threshold value for Major & Critical events

RWD-217 Event fails to upgrade with multiple user (ECS events only)

Event fails to upgrade with multiple user (ECS events only)

RWD-85 zookeeper cleanup cron is not running as scheduled

TEST: zookeeper cleanup cron is not running as scheduled

Workaround:

```
1systemctl enable --now zkcleanup.timer
```

RWD-74 zookeeper cleanup cron is not running as scheduled

zookeeper cleanup cron is not running as scheduled

Workaround:

apply this command to all eca nodes

[Copy Code](#)
JSON

```
1systemctl enable --now zkcleanup.timer
```

RWD -192 Kafka topic empty after cluster down/up

kafka topic will reset after cluster down/up

Count and Size will reset to zero

- before cluster down/up
- after cluster down/up

RWD-222 enable zkcleanup.timer by default

As an ECA user, I don't want to have to run `systemctl enable --now zkcleanup.timer` to start the service. This should be run by default on install/upgrade.

RWD-246 Files with non-ASCII characters fail to recover

2.5.9-22231

Files which will have the extension modified to a known extension like `.crypto` will trigger TD7 events.

The original files are not recovered even if the Recovery Job finishes successfully.

Known Limitations

Threat Detection

T6914 Some extensions still result in lockout when added to the ignore list

For the following well-known extensions, a lockout will still occur even if these extensions have been added to the extension ignore list using the `igls rsw allowedfiles add --extensions` command:

*.[\[teroda@bigmir.net\]](mailto:teroda@bigmir.net).masterteroda@bigmir.net

*.[\[mich78@usa.com\]](mailto:mich78@usa.com)

*.symbiom_ransomware_locked

*.[\[resque@plague.desi\]](mailto:resque@plague.desi).scarab

Workaround: Alternate Ignore capabilities for User, Path or IP address documented [here](#) may be used to workaround this issue.

T7191 SMB service not enabled when access restored when lockroot is true

If you have Ransomware Defender configured to disable SMB service is a root user event is detected (see Ransomware Admin guide [here](#), section Securing Root User on PowerScale), when you restore user access the SMB service is not automatically enabled.

Workaround: Manually enable SMB service on PowerScale once access is restored and you are ready to resume file access for SMB users.

T7670 Restoring user access via CLI does not update status of Security Event in the GUI

If you have restored user access after a lockout using the CLI command "`igls rsw restoreaccess set --user=DOMAIN\user`", the associated Security Event in the GUI will not be updated and remain in active state.

Workaround: Open the Actions window for the active event, enter a comment that access has been manually restored and then archive the event.

T8744 No event processing once Signal Strength passes 2 times Critical Threshold

Once a Security Event or Active Audit event has passed 2 times the Critical threshold configured in Ransomware Defender Settings, there is no further processing of Signals for the associated user. In all cases actions based on Critical threshold settings would have been already taken prior to reaching the 2x level.

For the case where both Ransomware Defender and Easy Auditor are licensed, reaching Signals processed count of 2 times Ransomware Critical threshold for a particular user limit is applied independently for Ransomware Defender and Easy Auditor.

Workaround: None Available.

T8986 NFS export lockout cannot be restored

An NFS export that has been locked out due to Ransomware Defender detecting a security event cannot be restored using Superna Eyeglass. You are able to select the Restore option and the Event History indicates that the permissions are restored but in fact the NFS export will still be in read-only state.

Workaround: On lockout NFS clients are moved to "Always Read-Only Clients". They will need to be manually moved to the correct access type using Isilon GUI or CLI to modify the export.

T15705 After upgrade to 2.5.6 cannot download CSV for Ransomware Event Files from events detected in prior releases

After upgrading to Release 2.5.6, csv download of files related to Ransomware events generated on the previous release is not available.

Workaround: GUI can still be used to view the files or files may be found on the Eyeglass appliance in the /srv/www/htdocs/rsw_event_all_files directory.

T16723 Error on Lockout of Shares on DR cluster

Under some conditions where a Ransomware Defender Lockout job overlaps with a Configuration Replication job you may see an error locking out some shares on DR cluster with error message code 409 AEC_CONFLICT. No impact to protection from Ransomware as the shares on the DR cluster are providing access to read-only data.

Workaround: You can re-attempt the Lockout from the Ransomware Defender window Action menu for the Active Event. Deny permission can also manually from Powerscale interface as required.

T17287 Many Access Zones slows down creation of snapshots and lockout

In the case where there are many Access Zones configured, analysis of user accessible shares must be done for all Access Zones before snapshot processing or lockout is started.

Workaround: None available

T7574 Option to set learned threshold for Security Guard in RESTORED_USER_ACCESS state

The menu to add Security Guard to the Learned Threshold is incorrectly provided when the event is in the RESTORED_USER_ACCESS state. The option can be selected and indicates that the flag as false positive was applied but it is not actually applied and it does not appear in the Learned Threshold list.

Workaround: None required

T18733 Ransomware Defender Affected Files Download Menu Naming

The Ransomware Defender Affected Files Download Menu is incorrectly named Affected Files - All. As described in the Ransomware Defender documentation [here](#) it is possible to have more files associated with the event than displayed in the file.

General

T16137 Anyrelease restore does not restore all Ransomware Defender and Easy Auditor settings

There is no restore of settings from release 2.5.4 and earlier. For release 2.5.4 and earlier continue to capture all Ransomware settings (False Positive, Ignore List, Allowed Extensions, Security Guard) and Easy Auditor settings (Active Auditor Trigger settings, RoboAudit). Post restore verify settings and update where required before cluster up on ECA.

In all cases, restoring an Eyeglass backup using the --anyrelease option will not restore following Ransomware Defender and Easy Auditor settings:

Ransomware Defender: Event History, Threats Detected

Easy Auditor: Finished Reports, Scheduled Reports, Saved Queries

T16821 anyrelease restore restrictions for restore to 2.5.7

Ransomware Defender, Easy Auditor and Performance Auditor deployments cannot use the anyrelease restore option to upgrade to a new appliance running 2.5.7. For case where a backup & restore is required due to 42.3 OS on original deployment, a backup & restore to 2.5.6 will have to be done first followed by an upgrade to 2.5.7 or in-place OS upgrade prior to 2.5.7 upgrade.

T20370 Monitor Only Settings Client IP applies to all PowerScale clusters

If multiple Powerscale clusters are licensed for Ransomware Defender a setting in the Client IP list for Monitor Only Settings is applied to all clusters. There is no option to associate the setting to a specific cluster. Also if you convert Ignore List to Monitor list any Client IP setting from Ignore list will also be applied to all cluster.

T21852 RSW - Cannot configure and run SG after anyrelease backup and restore from an earlier build

After a backup and restore from the earlier release to Eyeglass 2.5.8, the Ransomware Defender window may no longer allow you to edit or run the Security Guard.

Workaround: After the restore, execute the 2.5.8 run file (same release as you restored to) to resolve the issue.

T21208 Snapshots taken using Action Menu for Ransomware Defender Event follow Ransomware / Snapshots settings

If the Enable Share Snapshots option in Ransomware / Snapshots is unchecked, selecting the Create Snapshot option from the Action Menu will also not create snapshots.

T21110 Ransomware Defender / Snapshots User Share Snapshot Settings also applies for NFS detections

The option to disable/enable Ransomware Defender snapshot functionality is called User Share Snapshot Settings and Enable Share Snapshots but applies to any Ransomware Defender detection for SMB or NFS.

Well Known Ransomware File Extension Whitelist management is not available when a proxy used

If a proxy has been configured to access the internet, the well-known ransomware file extension management does not account for the proxy and will not be able to resolve the configured URLs.

T17624 Ransomware Defender NFS detection creates snapshot on SMB shares with Everyone permission

A Ransomware Defender detection for operations over NFS protocol also creates snapshots for SMB shares that have the Everyone permission.

RWD-75 Page-1 gets hide when navigate to Page-2 & archive all events from this page

When clearing all of the ransomware events from the second page of the ransomware defender active alerts tab, the pagination of the window can be lost and an empty list is displayed.

Workaround: close and open the window.

© Superna Inc

1.7. Zero Trust API - Release Notes

Home [Top](#)

- [What's New in Superna Zero Trust API Release 2.5.8.1](#)
- [Supported OneFS releases](#)
- [Feature Support Matrix](#)
- [End of Life Notifications](#)
- [Deprecation Notices](#)
- [Release Notes](#)
- [New in 2.5.8.1 - 22116](#)
- [New in 2.5.8.1 - 22100](#)
- [New in 2.5.8.1 - 22080](#)
 - [T22349 Zero Trust API critical path snapshot rate limits and expiry](#)
- [Known Issues](#)
 - [T22985 Zero Trust API cannot lockout an account with the # in the name](#)
- [Known Limitations](#)
 - [T22990 Zero Trust API cannot lockout ECS user](#)
 - [T22989 Zero Trust API cannot lockout NFS user](#)

What's New in Superna Zero Trust API Release 2.5.8.1

What's New! In Superna Zero Trust API can be found [here](#).

Supported OneFS releases

See [Current Release - Release Notes Ransomware Defender](#)

Feature Support Matrix

See [Data Sheet](#)

End of Life Notifications

NA

End of Life Notifications for all products are available [here](#).

Deprecation Notices

Currently no deprecation notices.

Release Notes

New in 2.5.8.1 - 22116

See New/Fixed for previous 2.5.8.1 releases.

New in 2.5.8.1 - 22100

See New/Fixed for previous 2.5.8.1 releases.

New in 2.5.8.1 - 22080

T22349 Zero Trust API critical path snapshot rate limits and expiry

Critical path snapshot initiated by the Zero Trust API using POST `/v2/ransomware/criticalpaths` will not take another snapshot if a previous snapshot exists that has been taken in the previous configured dead time which is 1 hour by default. Also critical path snapshot created by the API have a 4 hour expiry by default.

Known Issues

T22985 Zero Trust API cannot lockout an account with the # in the name

An account name with a # in the name does not get locked out when using the Zero Trust API /v2/ransomware/lockout API. A 404 not found response is returned.

Workaround: Use manual steps to block access to the account.

Known Limitations

T22990 Zero Trust API cannot lockout ECS user

The Zero Trust API cannot be used to issue a lockout for an ECS user.

T22989 Zero Trust API cannot lockout NFS user

The Zero Trust API cannot be used to issue a lockout for an NFS export.

1.8. Current Release - Release Notes Easy Auditor

[Home](#) [Top](#)

Release Date	Version
11/28/2023	2.6.4-23365

- [What's New in Superna Eyeglass Easy Auditor Edition Release 2.6.4 \(11/28/2023\)](#)
- [Supported OneFS releases](#)
- [Supported Eyeglass releases](#)
- [Inter Release Functional Compatibility](#)
- [End of Life Notifications](#)
- [New in Superna Eyeglass Easy Auditor Edition Release 2.6.3 \(09/28/2023\)](#)
- [New in Superna Eyeglass Easy Auditor Edition Release 2.6.2 \(09/01/2023\)](#)
- [Fixed in 2.6.2](#)
 - [EA-172 Built-In scheduled report results are displayed in the Manual report section](#)
- [New in Superna Eyeglass Easy Auditor Edition Release 2.6.1 \(08/03/2023\)](#)
- [Fixed in 2.6.0](#)
- [New in Superna Eyeglass Easy Auditor Edition Release 2.5.12 \(05/09/2023\)](#)
- [Fixed in 2.5.12](#)
 - [EA-295 Bulk Ingest job fails due to spark workers](#)
- [New in Superna Eyeglass Easy Auditor Edition Release 2.5.11-23110 \(04/03/2023\)](#)
- [Fixed in 2.5.11 - 23110](#)
 - [EA-232 Bulk Ingest with non-default path inter-working with RWD](#)
 - [EA-284 Bulk ingest list does not display all the files](#)
 - [EA-285 bulk ingestion GUI timeout at 3.7 minutes - still need to increase](#)
- [New in Superna Eyeglass Easy Auditor Edition Release 2.5.10 \(03/06/2023\)](#)

- Fixed in 2.5.10
 - EA-241 bulk ingestion GUI timeout to collect gz files for the GUI timeout needs to be increased to 5 minutes
- Support Removed in Eyeglass Release 2.5.9
- Deprecation Notices
- New in Superna Eyeglass Easy Auditor Edition Release 2.5.9.1 (02/14/2023)
- New/Fixed in 2.5.9.1
 - EA-167 Bulk Ingest is not retrieving archives created on the same day
- New in Superna Eyeglass Easy Auditor Edition Release 2.5.9 (11/30/2022)
- New/Fixed in 2.5.8
- New in 2.5.8.1-22116
- Fixed in 2.5.8.1-22116
- New in 2.5.8.1-22100
- Fixed in 2.5.8.1-22100
- Deprecated in 2.5.8.1-22080
 - Built In Reports Deprecated
- New in 2.5.8.1-22080
 - Built-In Access Report Now Reports per share
- Fixed in 2.5.8.1-22080
 - T21840 Easy Auditor - DLP trigger affected by quota sync schedule
- New/Fixed in 2.5.8-22028
- New in 2.5.8-21330
- Fixed in 2.5.8-21330
 - T22171 - Log4j Vulnerability - Upgrade to Log4j 2.17.0 (2.5.8-21330 and higher Log4j 2.17.0)
- New in 2.5.8-21306
- NEW - OneFS 9.3 Support
 - T19711 Easy Auditor new validation that selected path is on an audited Access Zone
- Fixed in 2.5.8-21306

- T22033 Log4j Vulnerability - CVE-2021-44228
- T20936 Bulk Ingest of Old Audit Data is not functional
- Technical Advisories
- Known Issues
- Reporting
 - T5907 No record for failed user query in Finished Reports
 - T6145 User with Eyeglass read-only position cannot run a custom query
 - T6149 Count Table and Access Report queries store unnecessary query parameters
 - T6293 Stale Access Report and Access Report display Cluster GUID instead of Cluster Name
 - T6313 Report Query Builder allows filter on Unlicensed Cluster
 - T6338 File Ext Input-only in the first line
 - T6339 Report Query Naming
 - T6349 Running Report Job State does not immediately reflect a cancelled Job
 - T6350 Easy Auditor Running Reports window inactive
 - T6404 Saved Custom User Queries show unrelated Built-In Query
 - T7049 Finished Report display issue for Duration
 - T9837 Warning on Wait for Spark Job
 - T10911 Share/Stale Access Report issue when AD has nested groups
 - T11752 Custom Real-time Audit policy User selection filtering
 - T11890 Able to save query without a name
 - T13573 Delete parent folder with subfolders shows duplicates in Where Did My Folder Go
 - T14722 Issues with custom report where path selected contains special language characters
 - T15037 Easy Auditor does not report files with multiple extensions correctly
 - T15582 Easy Auditor issues where path has & or brackets
 - T19561 Easy Auditor scheduled reports may not run
 - T20078 Emailed built-in report may contain user SID

- T20661 Large Report cannot be downloaded from Windows
- T22708 Access Report only reports on shares using AD Group permissions
- T22719 Access Report reports extra information when reporting on share with same name in multiple Access Zone
- T22720 Access Report not compatible with LDAP retrieval of AD Users and Groups
- T22731 Access Report cannot be displayed in the GUI with large number of permissions
- T22738 Access Report does not report on nested groups
- Active Auditing
 - T8878 Cannot save DLP trigger for a different NE but same path
 - T6305 Invalid username causes Wiretap error
 - T7547 Wiretap does not show user name for NFS events
 - T12876 DLP trigger cannot be added
 - T15198 Active Auditor Triggers may have inaccurate Signal Strength
 - T15250 The command to reset Active Auditor event queue must be run twice
 - T16980 Active Auditor events Affected Files-CSV may not show all events
 - T19629 Expired Active Auditor Events not archived to Event History if Ransomware Defender has Automatic Learning enabled
 - T21226, T22604 Active Auditor Snapshot functionality follows Ransomware Defender Snapshot configuration
 - T8694 Robo Audit may show Success when it did not run
 - T11880 Robo Audit fails when configured to run on more than one cluster
 - T15175 Existing Robo Audit Logs lost formatting after upgrade to 2.5.6
- General
 - T5858 ecactl commands do not switch to ecaadmin user
 - T5915 Event retrieval stopped by Disable/Enable of Protocol Monitoring on the PowerScale
 - T15457 HTML 5 vmware vcenter bug on OVA deployment
 - T6097 UI Desktop Unexpected Behaviour

- T6617 PowerScale Directory Selector does not display hidden directories
- T8105 Alarm EAU0002 has no detailed information for failed auditor report
- T19929 Easy Auditor Directory Selector returns "Error retrieving directory info from cluster"
- EA-191 Stale Access Report shows incorrect entries
- EA-171 Bulk Ingest folder is not created automatically
- EA-193 Bulk ingest job is not working with turboaudit REST API
- Known Limitations Reporting
 - Conditions under which audit events are not processed
 - T6260 Stale Access Report Known Limitations
 - T6478 Stale Access and Share Access Report AD User Limitation
 - T18936 Rerun of query required
- Active Auditing
 - T11540 Active Auditor may report on Audit Failure events
 - T12380 Ransomware Defender Ignore List settings are applied to Active Auditor analysis
 - EA-79 [Active Auditor-Active Event] Predicted signal doesn't show its type & value
- General
 - T8281 hbase major compaction affects queries
 - T16137 Anyrelease restore does not restore all Ransomware Defender and Easy Auditor settings
 - T16821 anyrelease restore restrictions for restore to 2.5.7
 - T16499 Easy Auditor reports double events

What's New in Superna Eyeglass Easy Auditor Edition Release 2.6.4 (11/28/2023)

Supported OneFS releases

8.2.0.x

8.2.1.x

8.2.2.x

9.0

9.1

9.2.x

9.3

9.4 via the February RUP 9.4.0.12 (PSP-3079) released Feb 8th 2023

9.4.0.14

9.5.x.x (minimum version 9.5.0.1)

9.5.0.5

Supported Eyeglass releases

Superna Eyeglass Easy Auditor Version	Superna Eyeglass Version
2.6.3-23292	2.6.3-23292
2.6.2-23282	2.6.2-23282
2.6.1-23250	2.6.1-23250
2.6.0-23219	2.6.0-23219
2.5.12-23175	2.5.12-23175
2.5.11-23110	2.5.11-23110
2.5.10-23087	2.5.10-23087
2.5.9-22251	2.5.9-22251

2.5.9-22231	2.5.9-22231
2.5.8.1-22116	2.5.8.1-22116
2.5.8.1-22100	2.5.8.1-22100
2.5.8.1-22080	2.5.8.1-22080
2.5.8-22028	2.5.8-22028
2.5.8-21330	2.5.8-21330
2.5.8-21306	2.5.8-21306
2.5.7.1-21161	2.5.7.1-21161
2.5.7.1-21140	2.5.7.1-21140
2.5.7-21096	2.5.7-21096
2.5.7-21081	2.5.7-21081
2.5.7-21068	2.5.7-21068
2.5.6-20263	2.5.6-20263

Inter Release Functional Compatibility

	OneFS 8.2 and 9.x releases	OneFS 9.x releases
Reporting	Untested	Untested
Active Auditing	Untested	Untested

End of Life Notifications

End of Life Notifications for all products are available [here](#).

New in Superna Eyeglass Easy Auditor Edition Release 2.6.3 (09/28/2023)

Built-in scheduled report results are displayed in the Manual report section.

New in Superna Eyeglass Easy Auditor Edition Release 2.6.2 (09/01/2023)

Fixed in 2.6.2

EA-172 Built-In scheduled report results are displayed in the Manual report section

New in Superna Eyeglass Easy Auditor Edition Release 2.6.1 (08/03/2023)

New in Superna Eyeglass Easy Auditor Edition Release 2.6.0 (06/29/2023)

Fixed in 2.6.0

EA-314 'Cannot retrieve report information from DB' error found during Query

Cannot monitor the query job progress during the query job is running.

New in Superna Eyeglass Easy Auditor Edition Release 2.5.12 (05/09/2023)

Fixed in 2.5.12

EA-295 Bulk Ingest job fails due to spark workers

Each time when trying to start a Bulk Ingest job, job fails to to spark workers.

Workaround: make sure that this line `-

`/opt/superna/mnt/bulkingestion:/opt/superna/mnt/bulkingestion:shared` is added on volumes for spark-worker in docker-compose.yml.

If there isn't such line in docker-compose.yml please add it and run `ecactl cluster exec ecactl cluster services restart --container spark-worker`

New in Superna Eyeglass Easy Auditor Edition Release 2.5.11-23110 (04/03/2023)

Refer to the previous 2.5.10 for what's new.

Fixed in 2.5.11 -23110

EA-232 Bulk Ingest with non-default path inter-working with RWD

RWD is not detecting events if Bulk Ingest has an archive path set up to a non-default path.

EA-284 Bulk ingest list does not display all the files

Bulk ingest list does not display all the files

EA-285 bulk ingestion GUI timeout at 3.7 minutes - still need to increase

bulk ingestion GUI timeout at 3.7 minutes

New in Superna Eyeglass Easy Auditor Edition Release 2.5.10 (03/06/2023)

Refer to previous 2.5.9.1 builds for what's new.

Fixed in 2.5.10

EA-241 bulk ingestion GUI timeout to collect gz files for the GUI timeout needs to be increased to 5 minutes

bulk ingestion GUI timeout to collect gz files for the GUI timeout needs to be increased to 5 minutes

Support Removed in Eyeglass Release 2.5.9

Following removed in 2.5.9:

- Data access report - this report is being deprecated due to low usage and is replaced by the Search and Recover Who owns what? report to determine top users consuming space on a path.
- Top users report (creating and deleting) - these reports are being deprecated due to low usage and redundant to the widely used Where Did My Folder Go? reporting and Custom Triggers for Active Auditing.
- Count table report - this report is not required for end user / administrator and is being removed from the user interface
- Threat Detector 01 - this report is not required for end user / administrator and is being removed from the user interface
- Threat Detector 02 - this report is not required for end user / administrator and is being removed from the user interface

Deprecation Notices

No Deprecation Notice in this release.

**New in Superna Eyeglass Easy Auditor Edition
Release 2.5.9.1 (02/14/2023)**

The bulk Ingestion path is updated. The path changed in system.xml to the default one `/ifs/.ifsvar/audit/logs/`. The path can be updated with this command as well : `igls config settings set --tag=<tagname> --value=<value>` where `tagname` is `bulkingestpath` and the value is the new path where the gz files are.

New/Fixed in 2.5.9.1

EA-167 Bulk Ingest is not retrieving archives created on the same day

As a Bulk Ingest user, I want to be able to use archives created in the last 24 hours. Now we can only use it to ingest archives older than 1 day.

New in Superna Eyeglass Easy Auditor Edition Release 2.5.9 (11/30/2022)

Added support for enhanced triggers on directory events in easy auditor. Added GUI support for bulk ingestion of old audit records.

New/Fixed in 2.5.8

New in 2.5.8.1-22116

Refer to previous build information.

Fixed in 2.5.8.1-22116

Refer to previous build information.

New in 2.5.8.1-22100

Refer to previous build information.

Fixed in 2.5.8.1-22100

Refer to previous build information.

Deprecated in 2.5.8.1-22080

Built In Reports Deprecated

The following Built In Reports have been deprecated as indicated in the deprecation notice:

- Data access report - this report has been deprecated due to low usage and is replaced by the Search and Recover Who owns what? report determining top users consuming space on a path.
- Top users report (creating and deleting) - these reports have been deprecated due to low usage and are redundant to the widely used Where Did My Folder Go? reporting and Custom Triggers for Active Auditing.
- Count table report - this report is not required for the end user/administrator and has been removed from the user interface
- Threat Detector 01 - this report is not required for the end user/administrator and has been removed from the user interface
- Threat Detector 02 - this report is not required for the end user/administrator and has been removed from the user interface

New in 2.5.8.1-22080

Built-In Access Report Now Reports per share

The Built-In Access Report now reports on selected share permission rather than all shares for a selected cluster.

Fixed in 2.5.8.1-22080

T21840 Easy Auditor - DLP trigger affected by quota sync schedule

DLP trigger is no longer working in 2.5.8 as the quota inventory collected on the new schedule is not available to assess the trigger.

Resolution: Quota inventory is now available for DLP trigger operation.

New/Fixed in 2.5.8-22028

Refer to previous build information.

New in 2.5.8-21330

Refer to previous build information.

Fixed in 2.5.8-21330

Security

T22171 - Log4j Vulnerability - Upgrade to Log4j 2.17.0
(2.5.8-21330 and higher Log4j 2.17.0)

New in 2.5.8-21306

NEW - see What's New in 2.5.8 [here](#).

NEW - OneFS 9.3 Support

Support for OneFS 9.3 is introduced in release 2.5.8.

T19711 Easy Auditor new validation that selected path is on an audited Access Zone

Easy Auditor path selector now verifies whether the selected path falls under an Access Zone with protocol auditing enabled.

Fixed in 2.5.8-21306

T22033 Log4j Vulnerability - CVE-2021-44228

Resolution: log4j version updated to 2.15.0 which has patch for the vulnerability.

T20936 Bulk Ingest of Old Audit Data is not functional

The ability to bulk ingest old audit data is not functional as of 2.5.7.1-21140 release.

Resolution: Bulk Ingest of audit data is now functional. Requires ECA nodes to be running OpenSUSE 15.3. If ECA nodes not running this OpenSUSE version need to redeploy the 15.3 ECA nodes and backup and restore configuration file and mount file.

The PowerScale Directory selector currently has a maximum list size of 1000 so that environments with more than 1000 directories on the PowerScale some directories will be missing.

Resolution: Directory selector now displays the first 1000 folders and an additional folder shown as ... Select the "..." will display the next 1000 folders and so on.

Technical Advisories

Technical Advisories for all products are available [here](#).

Known Issues

Reporting

T5907 No record for failed user query in Finished Reports

If a user-based query fails, there is no record of the failed report in the Finished Reports.

Workaround: None Required - Email notification is provided for the failed query.

This does not affect path-only queries.

T6145 User with Eyeglass read-only position cannot run a custom query

In the Report Query Builder, a user who only has read-only permissions can only Load a previously saved query to review its setting. From this interface, no load can be run.

Workaround: Administrator with full privileges must create and save a query, after which a user with read-only permission can run it from the list.

T6149 Count Table and Access Report queries store unnecessary query parameters

If you save the Count Table or Access Report query, disabled report parameters may be saved with the report definition even though they do not apply.

Workaround: None required. Extra parameters are ignored.

T6293 Stale Access Report and Access Report display Cluster GUID instead of Cluster Name

In the Stale Access and Access Reports, the cluster is identified by its GUID instead of displaying the cluster name.

Workaround: To verify which cluster the report is for, from the Eyeglass web open the Inventory View. Right click on a cluster name and select "Show Properties" to view the cluster GUID.

T6313 Report Query Builder allows filter on Unlicensed Cluster

The Report Query Builder does not block the selection of an unlicensed cluster.

Workaround: None required. File activity/events are not stored for unlicensed clusters, and as such, any report would return with 0 records.

T6338 File Ext Input-only in the first line

Report Query File Ext filter is only editable in the first line. Clicking anywhere else in the box will not let you enter any text

Workaround: None required. Enter the File Ext filter at the top of the box.

T6339 Report Query Naming

Saved Report Query names can only contain 0 to 9, a to z (lowercase) and A to Z (uppercase) without any spaces, - or _ .

Workaround: None available.

T6349 Running Report Job State does not immediately reflect a cancelled Job

When a Running Auditor Job is cancelled, the Running Jobs view continues to show the Running state until the canceled task has been completed.

Workaround: None required.

T6350 Easy Auditor Running Reports window inactive

The Easy Auditor Running Reports window may become inactive such that expired reports are not removed, and you cannot click on a Report to see details of the execution.

Workaround: Refresh the browser session.

T6404 Saved Custom User Queries show unrelated Built-In Query

A saved Customer User Query details will incorrectly show

Report Picker: Data access report - users who are writing the most/least amount of data even though this custom report is not related to this built-in query.

Workaround: None required - other query information is relevant and accurate.

T7049 Finished Report display issue for Duration

Finished Report Duration column does not display the entire duration required to complete the query.

Workaround: None available. The duration can be seen in the Running Jobs view while the query is still in running state.

T7049 Finished Report display issue for Duration

Finished Report Duration column does not display the entire duration required to complete the query.

Workaround: None available. The duration can be seen in the Running Jobs view while the query is still in running state.

T7437/T12178 Employee Exit Report may not complete

In large environment with high event rate, the 30 day Employee Exit Report may not complete or it may complete with a large number of records but viewing/download of results limited to 10,000 records.

Workaround: Modify the query for less than 30 days to reduce number of records in report or build a custom report using the Report Query Builder.

T7823 Email Report shows success when error with attachment

Emailing report shows as success even when there is an issue in attaching the report.

Workaround: Re-run the report or contact support at support.superna.net for assistance.

T9837 Warning on Wait for Spark Job

A Warning may appear on a Running Report Job Details for the Wait for Spark Job step with info “warning: Applicationid could not be retrieved” without impacting the completion of the query itself.

Workaround: None required

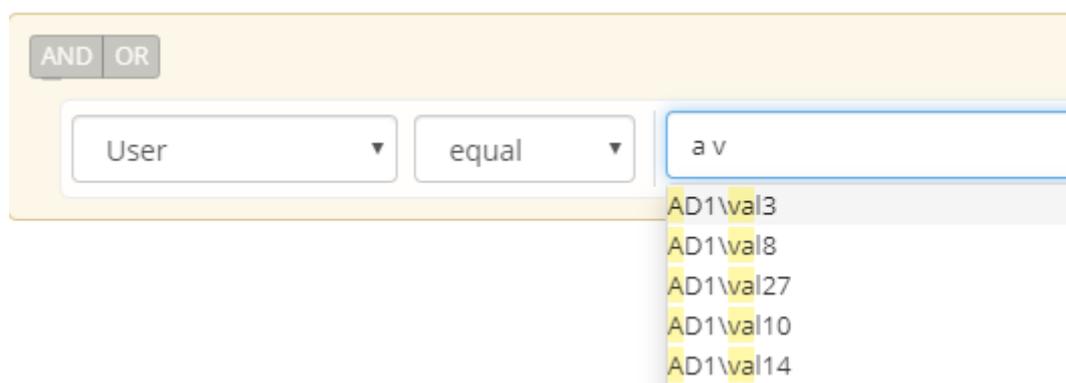
T10911 Share/Stale Access Report issue when AD has nested groups

The built in Share Access and Stale Access Reports do not show user access to a share for those users that are members of a nested subgroup of the AD group configured in the share permissions.

Workaround: None available.

T11752 Custom Real-time Audit policy User selection filtering

To select a name from the User drop-down list on a Custom Real-time Audit policy trigger you must first type the first letter of the user domain (name format is DOMAIN\name) after which you can type any other letter from user name for further filtering. Leave a space between first letter and next letter if letters are not adjacent in user name. Example below



Workaround: None required.

T11890 Able to save query without a name

The GUI allows saving of query without name. Query can be run but cannot be deleted. Only one query without a name will be able to be saved.

Workaround: Enter name when saving a query.

T13573 Delete parent folder with subfolders shows duplicates in Where Did My Folder Go

Where Did My Folder Go search results for a parent deleted folder where subfolders were also deleted duplicates entries for some folders.

Workaround: None required

T14722 Issues with custom report where path selected contains special language characters

Custom report where path selected contains special language characters may either not run or will complete with 0 results.

Workaround: Selecting a path higher up in the directory tree without special language characters may return results where special language characters not displayed correctly. Note that Wiretap and Where Did My Folder Go provide an option for reporting on these paths.

T15037 Easy Auditor does not report files with multiple extensions correctly

For the case where a file has multiple extensions in the Easy Auditor report the first extension only is reported. For example file.pdf.gz is reported as a pdf not as a gz file.

Workaround: None available.

T15582 Easy Auditor issues where path has & or brackets

Easy auditor has following issues for path with &:

- user or path search where path contains & return 0 results
- DLP trigger cannot be saved where path contains &
- Mass Delete trigger where path contains & returns 0 results

Workaround: Select path above path with & when defining custom search, DLP or Mass Delete triggers

Easy auditor has following issues where path contains bracket

- Wiretap, Where did My Folder Go, Active Auditor triggers not functioning

Workaround: No workaround available

T19561 Easy Auditor scheduled reports may not run

Under some circumstances the license state for a Powerscale cluster is lost after which scheduled reports may fail to run.

Workaround: Manually run the scheduled query for the desired timeframe.

T20078 Emailed built-in report may contain user SID

The summary in the email body for some built in reports shows user SID instead of the associated user id.

Workaround: The attached CSV file has SID resolved to user id.

T20661 Large Report cannot be downloaded from Windows

There is an issue downloading reports with very large number of records from Windows using Chrome browser. On download a "Loading" message appears but once the

Loading message stops, no download is started. This issue does not appear on MAC with Chrome browser.

Workaround:

1) On Windows, large reports can be successfully downloaded using Firefox browser build 72

2) The file is generated and present on the Eyeglass appliance and could be retrieved using a tool such as WinSCP. The report files are located on the Eyeglass appliance in the folder: /srv/www/htdocs/csv

T22708 Access Report only reports on shares using AD Group permissions

The Access Report can only be used to report on permissions for shares using AD Groups. Share permissions to AD Users directly or well known user/group such as Everyone results in an error when running the report.

Workaround: None available.

T22719 Access Report reports extra information when reporting on share with same name in multiple Access Zone

If there are multiple Access Zone configured on the PowerScale and those Access Zone contain shares with the same name, reporting on one of those shares will report for all shares of that name and not be filtered on the Access Zone selected.

Workaround: None required.

T22720 Access Report not compatible with LDAP retrieval of AD Users and Groups

If Eyeglass is configured to use LDAP for retrieval of AD Users and Groups, the Access Report cannot report on share access as it relying on PowerScale API calls for that information.

Workaround: None available.

T22731 Access Report cannot be displayed in the GUI with large number of permissions

If the resulting Access Report has more than 1000 permissions, the report cannot be viewed from the Easy Auditor GUI. Opening the report causes the GUI to freeze.

Workaround: Download report with large number of permissions to view it.

T22738 Access Report does not report on nested groups

The Access Report only reports on the users in the parent group where a share has permissions configured with nested groups.

Workaround: None available.

Active Auditing

T8878 Cannot save DLP trigger for a different NE but same path

With 2 licensed clusters a Data loss prevention policy cannot use the exact same path on both clusters if entering 2 different policies one for each cluster.

Work around: none only the first cluster and path can be added.

T6305 Invalid username causes Wiretap error

If you enter an invalid username that cannot be resolved when setting up a Wiretap active auditing job it causes the job creation to fail with the following error:

Failed to create new wiretap:

Server error when processing request: java.lang.NullPointerException

Workaround: Enter a username that can be resolved in the documented supported format.

T7547 Wiretap does not show user name for NFS events

For events generated over NFS protocol, Wiretap does not include user name in the event information. Only client IP address is displayed.

Resolution: A custom query can be built using the Report Query Builder based on path and timeframe in order to view user name.

T12876 DLP trigger cannot be added

An error (Error saving response) occurs when adding a DLP trigger if there is an existing directory quota without data-protection overhead option enabled on the the path that a DLP trigger is being configured for.

Workaround: If possible, delete the existing quota and allow new quota to be created as part of adding the DLP trigger. Note that the directory quota that is created will be created with the data-protection overhead option enabled.

T15198 Active Auditor Triggers may have inaccurate Signal Strength

Active Auditor trigger processing (DLP, Mass Delete, Custom Triggers) may receive duplicate events and as a result show a higher Signal Strength than is actually the case.

Workaround: None required. The duplicate events will cause early detection of configured triggers. The associated CSV for files involved in the detection is correct.

T15250 The command to reset Active Auditor event queue must be run twice

The command `igls adv eventTriggers set --operation=reset --topic=ea` must be run twice to clear the queue.

Workaround: Execute the command a second time to clear the queue.

T16980 Active Auditor events Affected Files-CSV may not show all events

Under some circumstances the Affected Files-CSV may not show all events for the Active Auditor trigger as the timeframe for the report may result in some events being excluded.

Workaround: Use the Report Query Builder to run a query with the same conditions and user as the associated trigger and a timeframe that starts before the detected time. Typically starting query an hour prior to the event would ensure all events were listed but may also include some audit events that are not related to the trigger.

T19629 Expired Active Auditor Events not archived to Event History if Ransomware Defender has Automatic Learning enabled

If the Ransomware Defender settings has Automatically Learn.... setting selected, an Active Auditor event that matches criteria for Automatic Learning encounters an error when it expires which prevents it from being archived to the Event History list. Impact: There is no impact on the detection of the Active Auditor event only on expiry the event is not moved to the event history as it should be.

Workaround: Event can be moved to the Event History by manually archiving as unsolved from the Action menu for the event.

T21226, T22604 Active Auditor Snapshot functionality follows Ransomware Defender Snapshot configuration

The snapshot behaviour for Active Auditor Mass Delete and manual snapshot creation follow the configuration for snapshot budget, and snapshot enable/disable in the Ransomware Defender / Snapshots window. Ransomware Defender snapshot logic for user share snapshot is followed if configured rather than a snapshot for the mass delete path.

Workaround: Do not use the Create Snapshot checkbox in the Easy Auditor / Active Auditor window to manage Active Auditor snapshots. It does not have any effect. Use the Ransomware Defender / Snapshots window to enable / disable snapshots.

Important - configuration here also affects snapshot management for Ransomware Defender. User share snapshot will also protect the mass delete path as user share would provide access to this location in the filesystem.

Robo Audit

T8694 Robo Audit may show Success when it did not run

Robo Audit may show as having successfully completed when in fact it did not run. For example:

- Robo Audit configured but disabled
- Robo Audit misconfigured and enabled

Workaround: Open the Robo Audit logs to see details of Job Execution.

T11880 Robo Audit fails when configured to run on more than one cluster

When configured to run on more than one cluster, Robo Audit job will succeed for one cluster but fail for the subsequent cluster.

Workaround: Configure Robo Audit to only run on one cluster.

T15175 Existing Robo Audit Logs lost formatting after upgrade to 2.5.6

Any existing Robo Audit logs viewed from the Eyeglass GUI will have lost the formatting after upgrading to 2.5.6.

Workaround: None required. New logs will have the correct formatting.

General

T5858 ecactl commands do not switch to ecaadmin user

If you are logged into an ECA node as root user and execute an `ecactl` command, you are prompted to login as the `ecaadmin` user to continue but even though the console indicates that the login as `ecaadmin` is underway the login never completes and the command cannot be executed.

Workaround: Login to ECA as `ecaadmin` user when using `ecactl` commands.

T5915 Event retrieval stopped by Disable/Enable of Protocol Monitoring on the PowerScale

If you disable / enable Protocol Auditing on the PowerScale cluster the ECA does not recover and does not begin reading events once Protocol Auditing enabled again.

Workaround: If you need to disable/enable Protocol auditing down the ECA cluster first

```
Ecactl cluster down
```

Then disable Protocol Auditing on the PowerScale cluster

After you have enabled Protocol Auditing on PowerScale cluster, the bring the ECA back up:

```
ecactl cluster up.
```

T6004 PowerScale Directory Selector Usage

In order to populate a cluster in the Directory Selector a directory must be selected in the file tree.

Workaround: None required. Once cluster is populated a path can be selected from the tree or typed in but must begin with `/ifs` .

T15457 HTML 5 vmware vcenter bug on OVA deployment

Some versions of vmware vcenter HTML user interface have a known issue with OVA properties being read correctly post power on, leading to first boot issues.

Workaround: use the Flash client as a work around.

T6097 UI Desktop Unexpected Behaviour

If you move a window to the edge of the Eyeglass desktop it may become stuck in that position.

Workaround: Refresh browser.

T6617 PowerScale Directory Selector does not display hidden directories

Directories that start with a dot (.) are not displayed in the PowerScale Directory Selector.

Workaround: Use the PowerScale Directory Selector to enter `\ifs\` and then enter the remainder of the path manually.

T8091 Login Monitor Report does not have Sorting

When viewing the Login Monitor Report Built-In query results from the GUI, sorting on columns Logons, Logoffs, and failed Logons is not available.

Workaround: Download the report csv file and open in spreadsheet for sorting and filtering of data.

T8105 Alarm EAU0002 has no detailed information for failed auditor report

The alarm Info for EAU0002 alarm "Auditor report failed" does not have any detailed information on cause of report failure.

Workaround: In Easy Auditor / Running Reports tab select the report that failed and in the Job Details expand the tree and select the Info link for the failed step.

T8249 Canceling Easy Auditor Running Report results in Critical severity alarm

Cancelling a running auditor report results in a Critical Severity alarm.

Workaround: None required. This alarm is informational only and does not indicate any critical issue in Easy Auditor.

T19929 Easy Auditor Directory Selector returns "Error retrieving directory info from cluster"

The Directory Selector directory tree display encounters an issue displaying the tree when the folder structure count (including files) exceeds 100,000.

Workaround: In the Directory Selector, select the cluster and the first folder "ifs" then manually enter the remainder of the path. Important: path is case sensitive and must match the filesystem path.

EA-191 Stale Access Report shows incorrect entries

Stale Access Report shows duplicated entries for users who accessed the share recently

Workaround:

1. import CSV into excel

2. sort by last access date (make sure records that have last access are at the top of the sheet)
 3. remove duplicates on the user column.
 4. Data that remains is accurate.
-

EA-171 Bulk Ingest folder is not created automatically

Bulk Ingest folder is not created automatically

workaround:

```
1 mkdir -p /opt/superna/sca/data/bulkingest
```

```
2touch /opt/superna/sca/data/bulkingest/bulkingest.json
```

```
3chown sca:users /opt/superna/sca/data/bulkingest/bulkingest.json
```

EA-193 Bulk ingest job is not working with turboaudit REST API

Bulk ingest job is not working with turboaudit REST API

Known Limitations Reporting

Conditions under which audit events are not processed

In the following situations, audit events will not be processed, and any audit events which occur while processing is down are dropped - they are not recovered by post processing:

- ECA NFS mount is down: Each ECA node is responsible for reading audit events for a specific set of PowerScale nodes. While the ECA NFS mount is down, audit events for these PowerScale nodes are dropped.
 - ECA down: Each ECA node is responsible for reading audit events for a specific set of PowerScale nodes. While the ECA NFS mount is down, audit events for these PowerScale nodes are dropped.
-

T6260 Stale Access Report Known Limitations

1) The Stale Access Report Built-In query does not report on activity for shares under following conditions:

- Share access by AD user with run as root permissions
- Share access by AD group where AD group has nested group and access by user in sub-group

2) With nested share topology, share access will be reported for "parent" share and "child" share when access was done via "child" share. For example, if PowerScale is configured with the default /ifs share, access by any other share will also be reported as access via the /ifs share.

T6361 Reporting for shares with local user permissions unsupported

Reports generated against shares which have a local PowerScale user permission configured may give unexpected results in the report and may cause email notification to fail.

T6478 Stale Access and Share Access Report AD User Limitation

Reports have been successfully generated against AD environment with up to 4000 users is current limit, Future release to extend this limit.

T2842 Login Monitor Report Known Limitations

The Login Monitor Report Built-In query has following Known Limitations:

- NFS login is not reported
 - Failed login due to invalid password, or invalid user are reported by user SID
 - A login where user does not appropriate share permission is reported as a Logon and Logoff together
-

T18936 Rerun of query required

Query may need to be re-run if the ECA OS product requirements have not been met for disk latency as this can cause search jobs to timeout in Eyeglass. The job may still complete by reviewing the finished jobs report tab. If the report shows error you will need to re-run the job. OS latency or memory issues can cause this and permanent fix should move the ECA VM's to flash based storage. This command can be run to look at disk statistics:

```
ecactl cluster exec iostat -xyz 6 6
```

This command will return a sample of disk IO per ECA. Consult [documentation](#) on latency requirements.

Active Auditing

T6061, T6465 Wiretap event rate display maximum of 25 events / s

Wiretap Watch window is limited to displaying events at a maximum of 25 events/s. If there are more than 25 event/s which match the Wiretap filter this will result in events being dropped and not displayed.

Workaround: Define filter with smaller scope by adding a user and defining more precisely the path in the filter. A report may also be run using same filter to retrieve all related results.

T7500 DLP Known Limitations

DLP Active Auditing has following Known Limitations:

- Small Files DLP threshold affected by PowerScale Quota Usage Reporting

For small files, PowerScale Quota Usage reports a larger usage than actual storage consumed. When setting a DLP threshold you must consider the threshold% against the quota reported usage. For example, if actual space consumed by 1 small files is 20b but quota usage is reported by PowerScale as 8K then the threshold to detect copy of that file is not 100%, it is $20b/8K$.

- DLP generate 1 signal when threshold crossed for any size of copy

Any copy that crosses the configured threshold will generate only 1 signal - whether the copy is one time the threshold configured or many times the threshold configured.

T7525 Active Auditor Affected Files also shows Ransomware Defender Affected Files

When viewing the Affected Files for an Active Auditor event, any files associated with a Ransomware Defender event that has occurred at the same time are also displayed.

Workaround: Download the csv file and use the path associated with the Active Auditor event from the GUI to filter the results.

T8744 No event processing once Signal Strength passes 2 times Critical Threshold

Once a Security Event or Active Audit event has passed 2 times the Critical threshold configured in Ransomware Defender Settings, there is no further processing of Signals for the associated user. In all cases actions based on Critical threshold settings would have been already taken prior to reaching the 2x level.

For the case where both Ransomware Defender and Easy Auditor are licensed, reaching Signals processed count of 2 times Ransomware Critical threshold for a particular user limit is applied independently for Ransomware Defender and Easy Auditor.

Workaround: None available.

T11540 Active Auditor may report on Audit Failure events

Active Auditor may report on failed audit events.

Workaround: Reporting of failed audit events can be disabled on the PowerScale audit settings. Please contact support.superna.net for more information on disabling reporting on failed audit events.

T12380 Ransomware Defender Ignore List settings are applied to Active Auditor analysis

Analysis of file events for Active Auditor triggers will ignore a user, IP or path configured in the Ransomware Defender Ignore list.

Workaround: None available.

EA-79 [Active Auditor-Active Event] Predicted signal doesn't show its type & value

The predicted signal is not supported in Active Auditor.

Workaround: None.

General

T8281 hbase major compaction affects queries

An hbase major compaction will prevent queries happening at the same time from completing.

Workaround: Re-run query once hbase major compaction has been completed.

T16137 Anyrelease restore does not restore all Ransomware Defender and Easy Auditor settings

There is no restore of settings from release 2.5.4 and earlier. For release 2.5.4 and earlier continue to capture all Ransomware settings (False Positive, Ignore List, Allowed Extensions, Security Guard) and Easy Auditor settings (Active Auditor Trigger settings, RoboAudit). Post restore verify settings and update where required before cluster up on ECA.

In all cases, restoring an Eyeglass backup using the --anyrelease option will not restore following Ransomware Defender and Easy Auditor settings:

Ransomware Defender: Event History, Threats Detected

Easy Auditor: Finished Reports, Scheduled Reports, Saved Queries

T16821 anyrelease restore restrictions for restore to 2.5.7

Ransomware Defender, Easy Auditor and Performance Auditor deployments cannot use the anyrelease restore option to upgrade to a new appliance running 2.5.7. For case where a backup & restore is required due to 42.3 OS on original deployment, a backup & restore to 2.5.6 will have to be done first followed by an upgrade to 2.5.7 or in-place OS upgrade prior to 2.5.7 upgrade.

T16499 Easy Auditor reports double events

In some cases it will be expected that a single operation such as deleting a folder is reported by the SMB protocol or Isilon as multiple delete events that appear as duplicates. Easy Auditor will record events as logged by Isilon and display all recorded events which may appear as duplicate but in fact is expected.

© Superna Inc

1.9. Current Release - Release Notes Golden Copy Search

[Home](#) [Top](#)

Release Date	Version
07/27/2023	1.2.0-23173

- [What's New in Superna Eyeglass Search \(07/27/2023\)](#)
- [Release 1.2.0-23173](#)
- [Fixed in 1.2.0-23173](#)
 - [SRCH-396 Twice the number of files are content-indexed](#)
- [What's New in Superna Eyeglass Search \(05/26/2023\)](#)
- [Release 1.2.0](#)
- [Supported OneFS releases](#)
- [End of Life Notifications](#)
- [Deprecation Notices](#)
- [Support Removed in this Release](#)
 - [Support removed for OneFS 8.0.x.x and 8.1.x.x releases.](#)
- [New in this release - 1.1.8-22082](#)
- [Fixed in this release - 1.1.8-22082](#)
 - [T23067 S3 indexing of object names and properties not working](#)
- [New in this release - 1.1.8-22050](#)
- [Fixed in this release - 1.1.8-22050](#)
 - [T20988 Incremental index for multiple folders does not run when Search is managing multiple Powerscale clusters](#)
- [New in this release - 1.1.8-22037](#)
- [Fixed in this release - 1.1.8-22037](#)
 - [T16115 Admin Group configuration allows user login and search](#)
 - [T21075 snapshotmonitor mode is not working](#)

- T21174 File System Browser Tree is not filtered based on End User Security configuration
- Technical Advisories
- Searching
 - T9420 Search does not return results for some non Latin or Cyrillic based languages
 - T9421 Search may return extra results where multiple different language files indexed
 - T9731 Administrator Override Path Search Syntax Issues
 - T9832 Index Folder Last Modified timestamp may not be updated
 - T9894 Indexed files with special characters may not be searchable
 - T9895 Incomplete dataset displayed on GUI after indexing error
 - T10196 Search time reported may not be the total elapsed time
 - T10269 Search csv and cmd writer download may not contain records in same order as GUI
 - T10270 Search results may be duplicated when scrolling through multiple pages or in csv download
 - T10289 Search Advanced Search Filter "File Title" may return unexpected results
 - T12079 Page count on report applied to subsequent reports
 - T12568 Reset button does not reset previously entered options for In the last... and Older than... and File Size
 - T12715 csv download of results has data in incorrect columns
 - T13325 Advanced Search Option File Path does not support wildcard searches
 - T13389 Created At/Last Accessed/Last Modified filters not cleared when changing from 1 option to another.
 - T13407 Not able to find 0 Byte files with Quick Reports
 - T13611 User search does not work for all clusters for multi-cluster deployment
 - T16425 Search incremental index does not handle changelist in waiting state and incremental fails

- T17392 ZoneUNC not displayed properly for multiple clusters
- T20553 What's Growing Old Quick Report default incorrect after filter reset
- T20555 Quick Report Graphs may be inaccurate
- T21037 Who Owns What and Show me the types Quick Report error when sorting by average file size
- T21038 Search scheduled test function does not handle more than 1000 records
- T20811/T21350 File Pool Policy is not cluster aware
- T21033 Searching content in index with special characters returns incorrect results
- T21035 Quick Report result selector not cleared after Quick Report is closed
- T19694 How fast is my data growing Quick Report blank screen
- T21586 API error stops incremental job
- T21635 Modifications to File Pool Policy are not recognized
- T22085 File System Browser is not available
- When Can I delete my worm lock data report hangs when using Show me the files
- T22713 GUI becomes unresponsive after selecting multiple results from time based reports
- T22759 Report Pie Chart reporting on low or no results
- T19924 Snapshot indexing for SNAPSHOT_ONLY folder is not available
- T22315 Scheduling for search on snapshot index not available
- T22316 Search Previous Versions results missing Snapshot Name
- T23162 Search index of /ifs folder also indexes snapshot folder
- T13180 Cannot add Azure for S3 object indexing
- T23449 A snapshotmonitor job ignores includes/excludes options
- T23444 Who owns what report does not report on files with no owner
- T23446 How fast is my data growing report does not display File Size graph
- SRCH-244 snapshotmonitor job fails to run
- SRCH-243 incremental job cannot be run on schedule

- SRCH-317 No search results when using auth-type SHARE_ACL
- File Recover
 - T13292 Recover File in error when file name selected contains non US-ASCII characters
 - T22317 Powerscale name truncated in Recover file dialog
- Classification
 - T19578 Classification Report includes all tags for matching files
 - T22069 Data Classification test command cannot be used with files with single or double quotes
 - T22384 Issue when deselecting tags in the Classification pick list
 - T22388 Classification pick list is not sorted
 - T22391 Classification tags not removed
 - T22402 Issues with Classification report with multiple tags selected
 - T22410 No Classification stats for errors
 - T22836 Classification tags do not support Unicode characters
 - T22867 Classification test command does not work with OneFS 9.3
- Security and Access
 - T9654 Unable to login and search using run as root user
 - T13595 - SHARE_ACL mode does not work if folder name contains non US-ASCII characters
 - T21286 Configuring Data Owner Search Administrator metadata-only option not working
 - T22373 Cannot configure admin user or group with space in name
- Configuration and Management
 - T10485 Newly added folder indexed files do not show up in search results
 - T10533 After disk usage crosses alarm threshold indexing must be manually restarted
 - T10589 Search Folder Stats missing error stat for content indexing
 - T9458 Zoneunc command is case sensitive to Access Zone name for non-System Access Zone

- T10957 searchctl jobs view --follow output may not display issue
- T13520 filerecovery settings command missing view option
- T22086 System Monitoring window is not available
- T22337 Firewall down after node reboot
- T20951 Cannot set filerecovery mode
- T23445 Path picker does not expand
- T10234 Some Language specific characters may not be displayed correctly in csv download
- T10235 Advanced Search chips may not all display in search bar
- T10975 Search session may not be terminated after upgrade
- T13406 Advanced Search chip for Cloudpool status not displayed for reports
- T21073 Phone home may fail when archive folder path contains characters 'id'
- T19765 Fail to add cluster consumes Search license
- T21428 Search Schedule GUI requires refresh to update
- T21562 Path selector does not handle long paths
- T21588 File Path Selector is not refreshed
- T22858 Search GUI shows Golden Copy Interface
- SRCH-352 Not able to add Azure as S3 target
- SRCH-358 Full index job can delete records from solr database
- SRCH-402 Unable to authenticate Isilon without Basic Auth enabled
- General
 - DEVSECOPS-258 `libzypp`/`rpm` bug causes installers to fail
- Known Limitations
 - T9530 Files in linked folders cannot be indexed for full content
 - T10290 Modifying folder index definition takes effect next full or incremental index
 - T10306 Error creating incremental ingestion job loses data from that interval
 - T10434 Changes to share used for authentication or in search results requires Search inventory and new session to take effect
 - T10548 Indexing zip file may exceed maximum index file size

- [T10723 Login to Search GUI with local user with language specific characters in name fails](#)
- [T10725 Change in File Owner only is not picked up during Incremental indexing](#)
- [T18849 Scheduled Report Max Limit](#)

These Release Notes cover the Superna Eyeglass Search and Recover product.

[Release table](#)

What's New in Superna Eyeglass Search (07/27/2023)

Release 1.2.0-23173

What's New! In Superna Eyeglass Search can be found [here](#).

Fixed in 1.2.0-23173

SRCH-396 Twice the number of files are content-indexed

1. index folder has 40 subfolders and 10,240 files in total
2. job done and folder stats show:

FULL/BYTES_INDEXED, FULL/FILES_CONTENT_INDEXED are 2X as expected

FULL/TREEWALK_FOLDERS_WALKED shows 3X

What's New in Superna Eyeglass Search (05/26/2023)

Release 1.2.0

What's New! In Superna Eyeglass Search can be found [here](#).

Supported OneFS releases

8.2.x.x

9.1.x.x

9.2.x.x

9.3.x.x

9.4.x.x

End of Life Notifications

End of Life Notifications for all products are available [here](#).

Deprecation Notices

No deprecation notices at this time.

Support Removed in this Release

Support removed for OneFS 8.0.x.x and 8.1.x.x releases.

New in this release - 1.1.8-22082

Refer to New in previous 1.1.8 releases.

Fixed in this release - 1.1.8-22082

T23067 S3 indexing of object names and properties not working

In 1.1.8, indexing of S3 objects is not working.

Resolution: S3 indexing of objects is now available with the exception of Azure (see T13180).

New in this release - 1.1.8-22050

Refer to New in previous 1.1.8 releases.

Fixed in this release - 1.1.8-22050

T20988 Incremental index for multiple folders does not run when Search is managing multiple Powerscale clusters

For a search deployment with multiple PowerScale clusters, incremental index will only run for 1 of n folders configured.

Resolution: Incremental now runs when Search is managing multiple PowerScale clusters.

New in this release - 1.1.8-22037

Refer to New in previous 1.1.5 releases.

Fixed in this release - 1.1.8-22037

T16115 Admin Group configuration allows user login and search

With Admin Only Login Mode configured and AD Groups configured as administrator or simply with AD Group configured as administrator, non-admin user (users not in AD group) login and searching is incorrectly still allowed.

Resolution: Admin Only Login Mode now restricts the login to users or members of AD group or local user configured as administrator. No login allowed for any other account.

T21075 snapshotmonitor mode is not working

snapshotmonitor mode to index snapshots related to an added folder is not working in current build. Nothing is saved to the index.

Resolution: snapshotmonitor mode is now working. Video with overview on indexing snapshot and recovery can be found [here](#).

T21174 File System Browser Tree is not filtered based on End User Security configuration

The File System Browser tree is exposed to end users but not filtered based on End User Security. This exposes the file system structure to end users.

Resolution: File System Browser is now only visible to administrators.

Technical Advisories

Technical Advisories for all products are available [here](#).

Known Issues

Searching

T9420 Search does not return results for some non Latin or Cyrillic based languages

Search has been found to not return results for some non Latin or Cyrillic based languages such as: Japanese-Kanji Script

Workaround: None available

T9421 Search may return extra results where multiple different language files indexed

For the case where files of multiple languages have been indexed, a search may incorrectly return extra files not related to the search criteria.

Workaround: None required.

T9731 Administrator Override Path Search Syntax Issues

For a user logged into search that has been configured with Administrator Override privileges, the Advanced Search "File Path" has following syntax issues:

1. Cannot search on `/ifs` or `/ifs/`. This will return an error or 0 results.
2. For all other paths, the path entered with a trailing slash will return 0 results.

Workaround:

1. Do not search on `/ifs` path.
 2. For all other paths, enter in the File Path field without the trailing slash - for example: `/ifs/data/path1`
-

T9832 Index Folder Last Modified timestamp may not be updated

A change to a file directly under a folder that has been defined as a search index folder will not update the folder last modified timestamp. Folder last modified is correctly updated if change is made in a subfolder of the index folder.

Workaround: The Last Modified time for files directly beneath the folder is available.

T9894 Indexed files with special characters may not be searchable

Indexed files containing special characters `~@#$$%^&()_+`-={}|;'. ,.` may result in error searching or return an incomplete search set (see T9895).

Workaround: None available.

T9895 Incomplete dataset displayed on GUI after indexing error

Indexing error such as described in T9894 may result in incomplete dataset or duplicates returned to GUI when searching.

Workaround: None available.

T10196 Search time reported may not be the total elapsed time

The search time that is reported in the user search GUI is the time for Search and Recover to complete it's query. For the case where there are multiple concurrent queries in progress, some queries may be queued and in that case the search time displayed may not reflect the actual elapsed time.

Workaround: None required. Plan to include reporting both elapsed and query time in a future release.

T10269 Search csv and cmd writer download may not contain records in same order as GUI

The csv and cmd writer download may not display search results in the same order that they are displayed on the GUI. This may be of particular notice when not all records are downloaded.

Workaround: Download all search results to see all and use spreadsheet sorting and filtering to order results.

T10270 Search results may be duplicated when scrolling through multiple pages or in csv download

In retrieving a large search result, some records may be displayed multiple times while scrolling through results or in downloaded csv.

Workaround: None required.

T10289 Search Advanced Search Filter "File Title" may return unexpected results

When using the "File Title" Advanced Search filter, results may return extra files or unexpected files that do not completely match criteria.

Workaround: When searching for "File Title" use complete filename including extension and also specify the extension in the extension filter.

T10435 % in share name blocks Search

Unable to search if there is a share name on the cluster that includes a % special character

Workaround: None available

T12079 Page count on report applied to subsequent reports

Total page count for a report that is run may be applied to a subsequent report. For example a What's Growing Old report is run and returns 61 pages of results. Navigate to last page of the report. Re-run the What Growing Old report with different criteria that return less results. The previous total pages applied and returns with message: 61-10 of 10, no matching record found

Workaround: Use result navigation tools to return to first page.

T12568 Reset button does not reset previously entered options for In the last... and Older than... and File Size

An Advanced Search option entered for Last Accessed, Last Modified or Created At and In the last... or Older than.. or File Size filters does not return to default setting after Reset. The previously entered value is preserved.

Workaround: Refresh browser or Log out and log back in.

T12715 csv download of results has data in incorrect columns

When search results contain names with spaces or names with multiple languages, the results may be shifted and in this case will not appear in correct column.

Workaround: Review result in Search GUI for any information that cannot be determined from csv.

T13325 Advanced Search Option File Path does not support wildcard searches

An Advanced Search for file path using * to define the path (example /ifs/data/project*) does not return results.

Workaround: Specify full path for file path searches.

T13389 Created At/Last Accessed/Last Modified filters not cleared when changing from 1 option to another.

Change a filter on a report from one of Created At/Last Accessed/Last Modified to another option. The period changes back to 1 month but the report is run against period from previous filter.

Workaround: Reset query parameters and then re-enter Created At/Last Accessed/Last Modified filters.

T13407 Not able to find 0 Byte files with Quick Reports

Specifying an Advanced Search option for Quick Reports with 0B specified for min and max size does not find 0B files.

Workaround: Use regular search with Advanced Search 0B file size options to find 0B files.

T13611 User search does not work for all clusters for multi-cluster deployment

For the case where multiple clusters have been added into Search, User based searching will not work for all clusters. This does not affect searching by administrators, they are able to see results from all clusters.

Workaround: None available.

T16425 Search incremental index does not handle changelist in waiting state and incremental fails

A changelist on the Powerscale which is in waiting state is not handled by Search & Recover which fails the incremental job instead of waiting and applying a timeout.

Workaround: None required - following incremental interval will pick up the changes.

T17392 ZoneUNC not displayed properly for multiple clusters

If Search configured to index from multiple clusters, ZoneUNC configuration may not be displayed properly in the Search Results window.

Workaround: None available

T20553 What's Growing Old Quick Report default incorrect after filter reset

After selecting the Reset button on the Advanced Search criteria for the What's Growing Old report, the default is displayed as Last Modified/Older than... but the report is generate with Last Modified/In the last...

Workaround: Refresh the browser after a Reset of Advanced Search Criteria.

T20555 Quick Report Graphs may be inaccurate

Under some circumstances, the Quick Report graphs are inaccurate or missing elements.

Workaround: Tabular results should be used to review the data.

T21037 Who Owns What and Show me the types Quick Report error when sorting by average file size

If the Advanced Search criteria Sort by Average File Size is selected, the Who Owns What and Show me the types reports do not complete and display the error "Error occurs in graphQL request".

Workaround: Select a different sort by option and then download the results to csv. Import the csv to a spreadsheet and execute the sort function in the spreadsheet.

T21038 Search scheduled test function does not handle more than 1000 records

Testing the scheduled report function where report contains more than 1000 records does not complete and blocks subsequent searches.

Workaround: Refresh browser.

T20811/T21350 File Pool Policy is not cluster aware

For a search deployment with multiple PowerScale clusters managed, the File Pool Policy filter does not get associated to the cluster where it is configured. Incorrect File Pool Policies may be listed when a cluster is selected and report may have incorrect results.

Workaround: None available.

T21033 Searching content in index with special characters returns incorrect results

If searching for a string in the content index where the string contains a special character such as a dash (-) or underscore (_) the results returned will be incorrect.

Workaround: Search content with the portion of the string that does not contain the special character.

T21035 Quick Report result selector not cleared after Quick Report is closed

If a Quick Report is generated and a record in the result table is selected (click the check box), the next report that is generated the same record in the result table will be selected.

Workaround: Close the report and refresh the browser.

T19694 How fast is my data growing Quick Report blank screen

If the filter defined for the How fast is my data growing Quick Report does not contain any search results a blank screen is displayed.

Workaround: Refresh browser window to recover.

T21586 API error stops incremental job

Under some conditions, an API error to the Powerscale will stop the incremental job.

Workaround: Contact support.superna.net for assistance.

T21635 Modifications to File Pool Policy are not recognized

Modifications to a file pool policy are not recognized even after the Search inventory job has run. This will result in old criteria being used in determining search results.

Workaround: A restart is required to recognize the changes. Contact support.superna.net for the proper procedure.

T22085 File System Browser is not available

The File System Browser window cannot be used because the File System Path Selector does not expand.

Workaround: None Available. Plan to fix in a patch release.

When Can I delete my worm lock data report hangs when using Show me the files

If you use the Show me the files option for the When can I delete my worm lock data report, the GUI freezes.

Workaround: To use the GUI again you must exit from current session and open a new session.

T22713 GUI becomes unresponsive after selecting multiple results from time based reports

For the time based reports What's growing old, When can I delete my worm lock data, How fast is my data growing after selecting multiple rows for "Show me the files" the GUI becomes unresponsive.

Workaround: To use the GUI again you must exit from the current session and open a new session.

T22759 Report Pie Chart reporting on low or no results

Report pie charts incorrectly show 0% for no matches rather than no display and 0% when the match is less than 1%

Workaround: None required.

T19924 Snapshot indexing for SNAPSHOT_ONLY folder is not available

In 1.1.8, configuring a folder as SNAPSHOT_ONLY to only index from snapshot is not available.

Workaround: Indexing live data and associated snapshots is available in 1.1.8.

T22315 Scheduling for search on snapshot index not available

If a schedule is created for a search using search previous versions to search the index for files from snapshot, the scheduled search comes back empty.

Workaround: None available.

T22316 Search Previous Versions results missing Snapshot Name

If a schedule is created for a search using search previous versions to search the index for files from snapshot, the Snapshot Name column is empty.

Workaround: None available.

T23162 Search index of /ifs folder also indexes snapshot folder

If search index is configured for the /ifs folder, even with the /ifs/.snapshot/** exclude configured the index job incorrectly indexes folders in the snapshots folder. Impact: Unnecessary indexing and storage of records.

Workaround: Configure index folders below /ifs folder.

T13180 Cannot add Azure for S3 object indexing

The Azure target cannot be added to Search. The target does not get added and an exception is displayed.

Workaround: None available.

T23449 A snapshotmonitor job ignores includes/excludes options

Snapshotmonitor jobs do not respect the includes/excludes configuration on the parent folder. Impact is that extra files are stored in the index.

Workaround: None available.

T23444 Who owns what report does not report on files with no owner

If a file is added to the index without an owner, the Who owns what report does not report on those files. Object indexing from AWS for example does not include an owner in the index.

Workaround: Use adhoc searching.

T23446 How fast is my data growing report does not display File Size graph

The How fast is my data growing report has tabular results for File Size but does not display them in the graphical view.

Workaround: Use the tabular results to review the file size distribution.

SRCH-244 snapshotmonitor job fails to run

NullPointerException when running snapshotmonitor job

SRCH-243 incremental job cannot be run on schedule

incremental job cannot be run on schedule

SRCH-317 No search results when using auth-type SHARE_ACL

No search results when using auth-type SHARE_ACL

File Recover

T13292 Recover File in error when file name selected contains non US-ASCII characters

Using Recover File functionality for files where file name contains non US-ASCII characters results in error and file not recovered.

Workaround: Use Search functionality to search indexed snapshots to determine which snapshot contains file to be recovered and then use manual restore from snapshot procedure from PowerScale.

T22317 Powerscale name truncated in Recover file dialog

In the window that opens when you recover a file, the Powerscale cluster name in the Destination Folder is missing character(s) at the beginning of the name.

Workaround: None available.

Classification

T19578 Classification Report includes all tags for matching files

If the files that match the tag(s) specified in the Classification report have other tags, all tags appear in the report instead of just the tags that were specified. Impact: Low - Additional information appears in the report that was not requested.

Workaround: Results can be downloaded and filtered externally if required.

T22069 Data Classification test command cannot be used with files with single or double quotes

The search classification test command does not work if the file that is being tested has single or double quotes and prints an Invalid Syntax error. Impact is to testing only. The actual classification of files with spaces and special characters does not have an issue.

Workaround: For classification testing use files without single or double quotes in the name or path.

T22384 Issue when deselecting tags in the Classification pick list

With multiple tags selected in the Classification pick list, if you deselect one it may deselects that last one you selected instead of the one you clicked on. Impact: A tag may unexpectedly be deselected. If you have a long list this may be a tag that you currently do not have visibility to.

Workaround: Refresh your browser to clear selections.

T22388 Classification pick list is not sorted

The Classification pick list is not sorted. Impact: It may be difficult to locate a specific tag when there is a long list.

Workaround: Scroll down the list as provided to find the required tag.

T22391 Classification tags not removed

Under some circumstances, when a classification tag is removed using the searchctl classification remove command, the Classification pick list is updated to remove the tag but the tag is not removed in the index itself. Impact: Low - Classification pick list does not provide the option to search on the tag that was removed.

Workaround: None available.

T22402 Issues with Classification report with multiple tags selected

A Classification report that is filtered for multiple tags joined with an AND has the following issues:

- The report will show one of the criteria - not the combined criteria - in the table but the count / size of files reported is accurate. Impact: All criteria are not visible in the report.
- Show me the files will disregard the combined criteria and show all files for a single criteria. Impact: Files that do not match the combined criteria appear in the file list

Workaround: Download the results from show me the files and filter externally.

T22410 No Classification stats for errors

There are no statistics available to identify errors that occur during classification. Impact: No indicator available to identify missing classification tags.

Workaround: None available.

T22836 Classification tags do not support Unicode characters

Classification tag with Unicode characters cannot be added. Impact: With this issue tags language specific characters cannot be added.

Workaround: Tag on subset of string without the Unicode character(s).

T22867 Classification test command does not work with OneFS 9.3

The search classification test command returns an error when the test file is on OneFS 9.3. Impact: Regex expression cannot be tested with test files on OneFS 9.3 Powerscale cluster.

Workaround: Some testing of regex can be done with external tools. Once configured in Search sample files identified for correctness.

Security and Access

T9654 Unable to login and search using run as root user

Cannot login to search GUI with run as root user even if share has run as root user permission configured.

Workaround: None available

T13595 - SHARE_ACL mode does not work if folder name contains non US-ASCII characters

SHARE_ACL security mode cannot be used for folders with non US_ASCII characters.

Workaround: None Available.

T21286 Configuring Data Owner Search Administrator metadata-only option not working

The metadata-only option for configuring a data owner search administrator with the searchctl settings adminaccesslist command does not work. If you set metadata-only to true no search results are returned.

Workaround: Ability to configure data owner search administrator for meta-data and content searching is available. No workaround for the meta-data only option.

T22373 Cannot configure admin user or group with space in name

Cannot add an AD group or user with a space in the name as an administrative user. Running the command to add the administrator group or user results in an exception.

Workaround: For an AD group, the group can be added by replacing the space in the name with %20. For example admin group@x.y would be added using admin%20group@x.y.

For AD user with a space in the name no workaround is available.

Configuration and Management

T9524 Deleting folder does not remove associated snapshots on PowerScale

If a folder that has been added for indexing is subsequently removed from Search and Recover, the associated snapshot alias and snapshots are not deleted from PowerScale.

Workaround: Prior to deleting the folder, take note of the folder ID using the command:

```
searchctl folders list
```

There will be 1 snapshot alias and 2 snapshots present on the PowerScale related to this folder. To identify the related snapshots, the naming convention followed is:

```
iglssrch-<folder id>
```

where <folder id> is the id returned from the searchctl folders list command.

Once identified, the snapshot alias and snapshots should be deleted manually.

T9856 DOMAIN\user format results in error when configuring Administrator Override

When configuring Administrator Override using command

```
searchctl settings admins add --name
```

entering --name using format DOMAIN\username will result in an error.

Workaround: Use format username@example.com or user SID for the --name parameter.

T10214 PowerScale cluster may become unlicensed after stopping and starting Search

After stopping and starting Search, the License information may not be retrieved properly leaving the PowerScale in an unlicensed state and no indexing being performed.

Workaround: Contact support.superna.net for assistance with this issue.

T10485 Newly added folder indexed files do not show up in search results

A newly added folder will not show up in search results until the Search inventory task has run.

Workaround: Run the Search inventory task manually by ssh to the Search cluster node 1 and run the command "searchctl PowerScales runinventory"

T10533 After disk usage crosses alarm threshold indexing must be manually restarted

By design when disk usage threshold is crossed indexing is paused. However once disk usage falls below threshold again indexing is not automatically resumed.

Workaround: Container responsible for indexing must be manually restarted. Contact support.superna.net for assistance.

T10589 Search Folder Stats missing error stat for content indexing

When an error occurs in indexing a file for content, the folder stats may only show the error for the meta-data component of indexing instead of also showing error for content indexing.

Workaround: None available. If error occurred on meta-data component of indexing, no content indexing will be performed.

T9458 Zoneunc command is case sensitive to Access Zone name for non-System Access Zone

When configuring Zoneunc using command

```
searchctl settings zoneunc add
```

if the `--zone` option does not have Access Zone name matching Access Zone name case in PowerScale for non-System Access Zone, login will fail.

Workaround: Ensure that `--zone` option uses exactly same case as is provisioned in PowerScale.

T10957 searchctl jobs view --follow output may not display issue

For case where searchctl jobs view --follow results in large output the screen may not display complete output.

Workaround: None available

T13520 filerecovery settings command missing view option

The command used to enable & set file recovery mode does not have an option to view existing settings.

Workaround: Please open a support case support.superna.net for assistance in viewing settings.

T22086 System Monitoring window is not available

The System Monitoring window is not populated accurately and should not be used.

Workaround: Use native operating system tools to assess Search CPU, RAM etc.

T22337 Firewall down after node reboot

A Search node that is rebooted will no longer have the firewall rules applied.

Workaround: After bringing the node back up run the command:

```
/opt/superna/eca/scripts/eca_iptables.sh
```

Check that the firewall is up by executing the command below from another server to confirm no access to port 3000 (replace <node IP> with the IP address of the Golden Copy node that you are running the command against):

nc -z <node IP> 3000

T20951 Cannot set filerecovery mode

The command to set the filerecovery mode for recovering a file from snapshot returns a Validation error... when used.

Workaround: None available. The default filerecovery mode NO_OVERWRITE_AND_RESTORE will not overwrite existing file and will create a restore file with the prefix igls-restored.

T23445 Path picker does not expand

The path picker control for reports and adhoc searches does not expand to see all sub directories.

Workaround: Manually enter the path.

T8052 Browser Issues

IE 11 - Banners and Headings in GUI not aligned

Workaround: None available

T10234 Some Language specific characters may not be displayed correctly in csv download

There may be some language specific characters that do not display correctly in the csv downloaded version of the search results.

Workaround: None available.

T10235 Advanced Search chips may not all display in search bar

When Advanced Search filter criteria are applied to a search, "chips" to indicate that filtering is in place are added to the main search bar. In the case where there are several filter criteria defined, it may be that not all "chips" will be visible in the main search bar.

Workaround: Expanding the browser window may allow all chips to be displayed or expand the Advanced Search window to view all filters.

T10975 Search session may not be terminated after upgrade

The Search session(s) that are open on upgrade may not be automatically terminated resulting in some changes not being available in current session.

Workaround: In this case all sessions that were open prior to upgrade must be terminated manually and reopened before continuing with any additional commands.

T13406 Advanced Search chip for Cloudpool status not displayed for reports

If a Cloudpool Status advanced search option is selected for a report, the associated chip does not display in the GUI.

Workaround: Expand the Advanced Search options to see what was selected.

T21073 Phone home may fail when archive folder path contains characters 'id'

Phone home may fail if there is an archive folder configured path that ends in 'id' - for example: `/ifs/data/patientid`

Workaround: None available.

T19765 Fail to add cluster consumes Search license

If a cluster fails to be added to Search, a license is still consumed by this cluster.

Workaround: Contact support.superna.net for assistance.

T21428 Search Schedule GUI requires refresh to update

After adding new schedules, modifying schedules, scheduled search run the Search Schedule GUI is not updated.

Workaround: Refresh browser to update the information in the GUI.

T21562 Path selector does not handle long paths

The path selector in the GUI scrolls to the right and hides the submit button if navigating a folder tree with long paths.

Workaround: path can added manually into the field.

T21588 File Path Selector is not refreshed

The File Path Selector does not always refresh after making a selection in one report and selecting a path for a different report.

Workaround: Refresh browser tab.

T22858 Search GUI shows Golden Copy Interface

Due to browser caching, login to the Search product GUI may display the Golden Copy GUI.

Workaround: Hard clear the browser cache or login using incognito.

SRCH-352 Not able to add Azure as S3 target

Not able to add Azure as S3 target

SRCH-358 Full index job can delete records from solr database

When the full index job runs and the `INDEX_WORKER_SOLR_QUERY_CHECK` variable is set to `true`, there is a case where records can be erroneously deleted from the solr database.

Workaround: set `INDEX_WORKER_SOLR_QUERY_CHECK` to `false` in `eca-env-common.conf` and restart.

SRCH-402 Unable to authenticate Isilon without Basic Auth enabled

Basic authentication is required to use the external API for the search product.

General

DEVSECOPS-258 `libzyp`/`rpm` bug causes installers to fail

libzypp version 17.31.22 introduces an incompatibility with the currently available version of rpm (4.14.3 at the time of writing). The following error occurs when the installer attempts to install the RPMs:

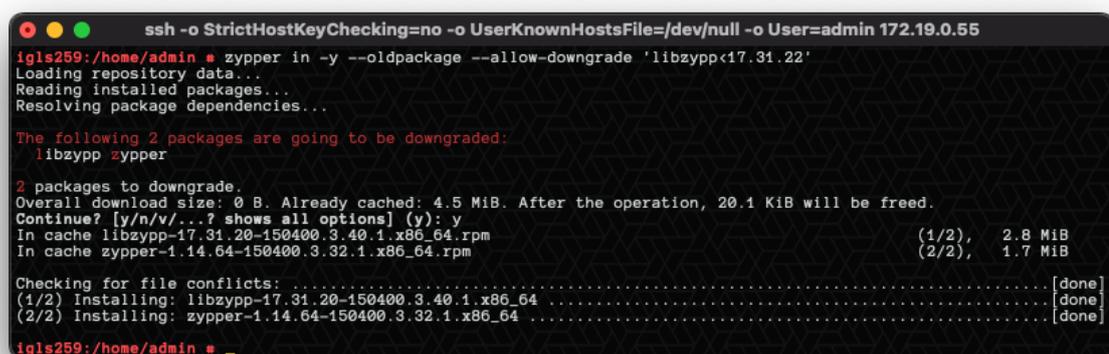
```
error: Macro %_dump_postrans has empty body
```

```
error]
```

Workaround: libzypp must be downgraded and locked to prevent the broken from being installed either manually or by the Yast2 Auto Update process:

```
sudo zypper in -y --oldpackage --allow-downgrade 'libzypp<17.31.22'
```

```
sudo zypper addlock 'libzypp<17.31.22'
```



```
ssh -o StrictHostKeyChecking=no -o UserKnownHostsFile=/dev/null -o User=admin 172.19.0.55
igls259:/home/admin # zypper in -y --oldpackage --allow-downgrade 'libzypp<17.31.22'
Loading repository data...
Reading installed packages...
Resolving package dependencies...

The following 2 packages are going to be downgraded:
 libzypp zypper

2 packages to downgrade.
Overall download size: 0 B. Already cached: 4.5 MiB. After the operation, 20.1 KiB will be freed.
Continue? [y/n/v/...? shows all options] (y): y
In cache libzypp-17.31.20-150400.3.40.1.x86_64.rpm (1/2), 2.8 MiB
In cache zypper-1.14.64-150400.3.32.1.x86_64.rpm (2/2), 1.7 MiB

Checking for file conflicts: ..... [done]
(1/2) Installing: libzypp-17.31.20-150400.3.40.1.x86_64 ..... [done]
(2/2) Installing: zypper-1.14.64-150400.3.32.1.x86_64 ..... [done]

igls259:/home/admin # _
```

Known Limitations

T9530 Files in linked folders cannot be indexed for full content

Files that are in a folder on the PowerScale that is sym-link to another folder cannot be indexed for full content due to the fact the PowerScale snapshots refer to physical path and sym-linked folders cannot be differentiated.

Workaround: Linked folders can be indexed for meta-data.

T10290 Modifying folder index definition takes effect next full or incremental index

If the folder index definition in Search & Recover is modified (for example to change fullIncludes or metaIncludes) the change will only take effect on the next full or incremental index. If the folder definition was modified while a full index was in progress, it would not take effect in that current job but the next job (full or incremental) that starts.

Workaround: None required.

T10306 Error creating incremental ingestion job loses data from that interval

If an error occurs creating the incremental ingestion job, the changes which occurred during that interval are not processed or picked up in the next interval.

Workaround: None required - next modification of file will pick up all changes.

T10434 Changes to share used for authentication or in search results requires Search inventory and new session to take effect

A change to the name or permissions of a share that is related indexed will require effect:

- 1) Search inventory task must run (runs daily at midnight)
- 2) Must open a new Search GUI session. Changes do not take effect on current GUI session for either permissions or share display.

Workaround: None required - Inventory can be run manually by ssh to the Search cluster node 1 and run the command "searchctl PowerScales runinventory"

T10548 Indexing zip file may exceed maximum index file size

On index of a zip file, even if the zip file itself falls below maximum file size for indexing once extracted for indexing it may exceed maximum file size and will be unable to be indexed. There is no recording of error on this indexing error.

Workaround: Consider whether zip files need to be indexed for content, if not they can be excluded from content indexing.

T10723 Login to Search GUI with local user with language specific characters in name fails

The Search GUI login fails when login user is a local user name with language specific characters.

Workaround: None available

T10725 Change in File Owner only is not picked up during Incremental indexing

A change in the file owner property of a previously indexed file will not be updated as part of incremental indexing if this is the only change.

Workaround: Change to content of the file will result in update to meta-data including change to file owner.

T18849 Scheduled Report Max Limit

The maximum number of records in a scheduled report is 50,000.

© Superna Inc

1.10. Current Release - Release Notes

Performance Auditor

[Home](#) [Top](#)

- [What's New in Superna Eyeglass Performance Auditor Release 2.5.8](#)
- [Supported OneFS releases](#)
- [End of Life Notifications](#)
- [End of Support in 2.5.8](#)
- [Deprecation Notices](#)
- [Technical Advisories](#)
- [New/Enhanced/Fixed in 2.5.8](#)
- [New/Fixed in 2.5.8.1 - 22116](#)
- [New/Fixed in 2.5.8.1 - 22100](#)
- [New/Fixed in 2.5.8.1 - 22080](#)
- [New/Fixed in 2.5.8-22028](#)
- [New in 2.5.8-21330](#)
- [Fixed in 2.5.8-21330](#)
 - [T22171 - Log4j Vulnerability - Upgrade to Log4j 2.17.0 \(2.5.8-21330 and higher Log4j 2.17.0 \)](#)
- [New in 2.5.8-21306](#)
 - [NEW - OneFS 9.3 Support](#)
- [Fixed in 2.5.8-21306](#)
 - [T22033 Log4j Vulnerability - CVE-2021-44228](#)
 - [T20097 Performance Auditor History mode is not working in 2.5.7.1](#)
- [Known Issues](#)
 - [T14414 Performance Auditor may double process some events](#)
 - [T14317 Performance Auditor Pin User does not handle special language characters](#)

- [T14175 Performance Auditor Display Intermittently Pauses](#)
- [T16657 Sort By option does not work properly](#)
- [T17476 Performance Auditor Rewind Time Display incorrect when invalid time entered](#)
- [T17480 Performance Auditor Rewind Timer Selector issue](#)
- [T18088 Rewind time does not indicate when no records found](#)
- [T18588 NFS users not resolved](#)
- [T19050 Pinned User initially displayed with SID](#)
- [T14159 Performance Auditor rates may not match Windows File Explorer rates](#)
- [T17567 Performance Auditor Historical Records not preserved on eca cluster down/up](#)

What's New in Superna Eyeglass Performance Auditor Release 2.5.8

What's New! In Superna Eyeglass Performance Auditor can be found [here](#).

Supported OneFS releases

9.0

9.1

9.2

9.3

386

9.4 via the February RUP 9.4.0.12 (PSP-3079) released Feb 8th 2023

9.5.0.1

End of Life Notifications

End of Life Notifications for all products are available [here](#).

End of Support in 2.5.8

Following features will no longer be supported as of 2.5.8:

1. Following OneFS releases no longer supported
 - a. Support for OneFS 8.0.x.x releases removed
 - b. Support for OneFS 8.1.x.x releases removed

Deprecation Notices

No deprecation notices at this time.

Technical Advisories

Technical Advisories for all products are available [here](#).

New/Enhanced/Fixed in 2.5.8

New/Fixed in 2.5.8.1 - 22116

Refer to previous 2.5.8.1 build information.

New/Fixed in 2.5.8.1 - 22100

Refer to previous 2.5.8.1 build information.

New/Fixed in 2.5.8.1 - 22080

Refer to previous 2.5.8 build information.

New/Fixed in 2.5.8-22028

Refer to previous 2.5.8 build information.

New in 2.5.8-21330

Refer to previous 2.5.8 build information.

Fixed in 2.5.8-21330

Security

T22171 - Log4j Vulnerability - Upgrade to Log4j 2.17.0
(2.5.8-21330 and higher Log4j 2.17.0)

New in 2.5.8-21306

NEW - OneFS 9.3 Support

Support for OneFS 9.3 is introduced in release 2.5.8.

Fixed in 2.5.8-21306

T22033 Log4j Vulnerability - CVE-2021-44228

Resolution: log4j version updated to 2.15.0 which has patch for the vulnerability.

T20097 Performance Auditor History mode is not working in 2.5.7.1

When you try to access the Performance Auditor History Mode the new tab opens but the history view is not displayed and browser returns an error message.

Resolution: History view is now available

Known Issues

T14414 Performance Auditor may double process some events

In some cases Performance Auditor may double process some events which will inflate bandwidth reported when this occurs.

Workaround: None available.

T14317 Performance Auditor Pin User does not handle special language characters

You cannot pin an AD name that contains special language characters. The GUI error is:

Error: Username <name> could not be resolved

Workaround: None available.

T14175 Performance Auditor Display Intermittently Pauses

Performance Auditor display may intermittently pause for several seconds before resuming.

Workaround: None required. Display continues and recovers showing trend after several seconds.

T16657 Sort By option does not work properly

Sort By operation is not applied to all categories. For example a Sort By: Write may incorrectly show Read information for some categories.

Workaround: None available.

T17476 Performance Auditor Rewind Time Display incorrect when invalid time entered

If an invalid date and time are selected for Performance Auditor Rewind, an appropriate message indicating that no data was found is provided but the date and time requested are not updated in the display to indicate what the incorrect entry was.

Workaround: None available.

T17480 Performance Auditor Rewind Timer Selector issue

If you select a time for Rewind, you are blocked from setting another time that is ahead of the previously selected time.

Workaround: Refresh window and then a more recent time can be selected.

T18088 Rewind time does not indicate when no records found

If you select a rewind interval beyond where data is available, the "rewind" time displayed is the time when there are records available without any indication that there are no records at selected time

Workaround: None required. Interval selected does not have data. Interval with data is provided.

T18588 NFS users not resolved

NFS access for local users or users that could be resolved in AD are not resolved in Performance Auditor display. They are displayed in format <IP address>:<UID> .

Workaround: Use manual process to determine user associated with UID.

T19050 Pinned User initially displayed with SID

When dragging a user from the Performance Auditor User list to be pinned, it initially is displayed in the Pinned list by SID instead of AD user name. No impact to pinning functionality.

Workaround: Close and reopen the Performance Auditor window and user will be displayed using AD name.

Known Limitations

T14159 Performance Auditor rates may not match Windows File Explorer rates

Performance auditor rates are based on when the application layer commits the data. Applications can copy data but not commit the data to file. This is a key difference to understand between counting packets and MB saved to a file.

For additional information please refer to Performance Auditor documentation [here](#).

Workaround: None required

T17567 Performance Auditor Historical Records not preserved on eca cluster down/up

After issuing an eca cluster down/up (for example done as part of an upgrade), the Performance Auditor historical records are not preserved.

Workaround: None available

© Superna Inc

1.11. Current Release - Release Notes ECA

[Home](#) [Top](#)

- [What's New in Superna Eyeglass Easy Auditor Edition and Ransomware Defender Edition](#)
 - [Release 2.5.8](#)
- [Supported OneFS releases](#)
- [Supported Eyeglass releases](#)
- [End of Life Notifications](#)
- [End of Support in 2.5.8](#)
- [Deprecation Notices](#)
- [New/Fixed in this Release](#)
- [New/Fixed in 2.5.8.1-22116](#)
- [New in 2.5.8.1-22100](#)
 - [T22855 Turboaudit - Use REST API instead of NFS for listing directories](#)
- [Fixed in 2.5.8.1-22100](#)
- [New in 2.5.8.1 - 22080](#)
 - [T20992 ECA Event Rate Alarms](#)
 - [T22857 NFSv4 for ECA](#)
- [Fixed in 2.5.8.1-22080](#)
 - [T20753 Error in Manage Services for vaultagent and taskmaster](#)
- [New in 2.5.8-22028](#)
- [Fixed in 2.5.8-22028](#)
 - [T21992 - Fix for boot issue during OVF deploy](#)
- [New in 2.5.8-21330](#)
- [Fixed in 2.5.8-21330](#)
 - [T22171 - Log4j Vulnerability - Upgrade to Log4j 2.17.0 \(2.5.8-21330 and higher Log4j 2.17.0 \)](#)

- [New in 2.5.8-21306](#)
 - [T20989 Event Retrieval and Send Rates available from GUI](#)
 - [T21097 ECA Cluster disk management optimization](#)
- [Fixed in 2.5.8-21306](#)
 - [T22033 Log4j Vulnerability - CVE-2021-44228](#)
- [Technical Advisories](#)
- [Known Issues](#)
- [General](#)
 - [T8309 ecactl cluster up may continue despite hbase errors](#)
 - [T7367 Issues when ecactl cluster up interrupted](#)
 - [T13247 ECA fails to retrieve audit events from all PowerScales if one PowerScale is unreachable via autonfs](#)
 - [T22210 Intermittent Hbase Validation Warning in Manage Services with Mini ECA](#)
 - [T22450 Audit database save rate alarm raised for Ransomware Defender Only Deployments](#)
 - [T23212 REST API continues to query cluster after removed](#)
- [General](#)
 - [T15457 HTML 5 vmware vcenter bug on OVA deployment](#)
 - [T17103 ECA version intermittently reported incorrectly](#)
 - [T22924 ECA event rate alarm notification first instance](#)

These Release Notes cover the Superna Eyeglass ECA deployed with Superna Eyeglass Ransomware Defender and Superna Eyeglass Easy Auditor and Superna Eyeglass Performance Auditor

What's New in Superna Eyeglass Easy Auditor Edition and Ransomware Defender Edition

Release 2.5.8

What's New! In Superna Eyeglass Easy Auditor Edition and Ransomware Defender Edition Release 2.5.8 can be found [here](#).

Supported OneFS releases

8.2.0.x

8.2.1.x

8.2.2.x

9.0

9.1

9.2

9.3

Supported Eyeglass releases

Superna Eyeglass ECA Version	Superna Eyeglass Version
2.5.8.1-22116	2.5.8.1-22116
2.5.8.1-22100	2.5.8.1-22100
2.5.8.1-22080	2.5.8.1-22080
2.5.8-22028	2.5.8-22028
2.5.8-21330	2.5.8-21330
2.5.8-21306	2.5.8-21306
2.5.7.1-21161	2.5.7.1-21161
2.5.7.1-21140	2.5.7.1-21140
2.5.7-21096	2.5.7-21096
2.5.7-21081	2.5.7-21081
2.5.7-21068	2.5.7-21068
2.5.6-20263	2.5.6-20263
2.5.6-20258	2.5.6-20258
2.5.6-20158	2.5.6-20158
2.5.6-20084	2.5.6-20084

2.5.6-20069	2.5.6-20069
2.5.6-20063	2.5.6-20063
2.5.6-20056	2.5.6-20056
2.5.5-20019	2.5.5-20019
2.5.5-19234	2.5.5-19234
2.5.5-19226	2.5.5-19226
2.5.5-19219	2.5.5-19219
2.5.5-19188	2.5.5-19188
2.5.5-19184	2.5.5-19184

End of Life Notifications

End of Life Notifications for all products are available [here](#).

End of Support in 2.5.8

Following features will no longer be supported as indicated below:

1. As of Release 2.5.8
 - a. Support for OneFS 8.0.x.x releases
 - b. Support for OneFS 8.1.x.x releases

Deprecation Notices

No deprecation notices at this time.

New/Fixed in this Release

New/Fixed in 2.5.8.1-22116

Refer to previous build information.

New in 2.5.8.1-22100

T22855 Turboaudit - Use REST API instead of NFS for listing directories

For cases where high bandwidth consumption by turboaudit listing directories when there are high number of audit log gz files, REST API can be used to list the audit log directories instead of NFS which uses less bandwidth.

Fixed in 2.5.8.1-22100

Refer to previous 2.5.8 build information.

New in 2.5.8.1 - 22080

T20992 ECA Event Rate Alarms

Warning severity alarm for audit event rate ingestion and audit database save rate to detect network issues or NFS mount issues that block processing of audit event data.

T22857 NFSv4 for ECA

NFSv4 is now the default for mount to audit log directory from ECA VMs.

Fixed in 2.5.8.1-22080

T20753 Error in Manage Services for vaultagent and taskmaster

In 2.5.8 Manage Services shows an error for the vaultagent and taskmaster components. Impact: None to Ransomware Defender, Easy Auditor or Performance Auditor as these components are not required for these products.

Resolution: Manage Services no longer shows this error for products where these components are not required.

New in 2.5.8-22028

Refer to previous 2.5.8 build information.

Fixed in 2.5.8-22028

T21992 - Fix for boot issue during OVF deploy

New in 2.5.8-21330

Refer to previous 2.5.8 build information.

Fixed in 2.5.8-21330

Security

T22171 - Log4j Vulnerability - Upgrade to Log4j 2.17.0
(2.5.8-21330 and higher Log4j 2.17.0)

New in 2.5.8-21306

T20989 Event Retrieval and Send Rates available from
GUI

The audit event receive and send rate which the Ransomware Defender, Easy Auditor and Performance Auditor rely on are now available from the Manage Services window

by selecting the ECA Monitor button. Event rate graph opens in a new tab and must be authenticated using the ecaadmin user. More information can be found [here](#).

T21097 ECA Cluster disk management optimization

ECA cluster disk management optimization for event retention will be reduced to reduce disk space requirements in the VM's. Events will be buffered for 1 hour or 512 MB x 9 or 4.6 GB of event data.

Fixed in 2.5.8-21306

T22033 Log4j Vulnerability - CVE-2021-44228

Resolution: log4j version updated to 2.15.0 which has patch for the vulnerability.

Technical Advisories

Technical Advisories for all products are available [here](#).

Known Issues

General

T8309 ecactl cluster up may continue despite hbase errors

In some cases the "ecactl cluster up" command may continue when it encounters hbase errors.

Workaround: Please open a support case support.superna.net for assistance with hbase errors.

T7367 Issues when ecactl cluster up interrupted

Interrupting "ecactl cluster up" before it has completed may result in misconfigured references for ECA nodes. This can result in ECA components starting on incorrect ECA node or may prevent ECA components from coming up at all.

Resolution: Please open a support case support.superna.net for assistance.

T13247 ECA fails to retrieve audit events from all PowerScales if one PowerScale is unreachable via autonfs

When multiple PowerScale clusters are being monitored, an unreachable PowerScale cluster may block ECA turboaudit component from retrieving events from the reachable PowerScale cluster(s).

Workaround: Contact support.superna.net to assist in recovering from this condition.

T22210 Intermittent Hbase Validation Warning in Manage Services with Mini ECA

For deployments with Mini ECA, Hbase validation warning may appear intermittently and recover on its own to OK possibly due to latency from the Mini ECA nodes. Impact: In this case there is no impact to the Ransomware Defender or Easy Auditor functionality.

Workaround: Use the Manage Services ECA Monitor Event Rate graph to confirm that evtarchive component has rate for Received events and Sent events. Configure RoboAudit to run daily to verify Easy Auditor query functionality.

T22450 Audit database save rate alarm raised for Ransomware Defender Only Deployments

The RSW0027 audit database save rate alarm is incorrectly raised for Ransomware Defender only deployments.

Workaround: Contact support.superna.net to change the evtarchive_event_rate_alarm_threshold threshold for this alarm to 0 in your environment so that alert is not triggered.

T23212 REST API continues to query cluster after removed

Turboaudit configured to use REST API to list audit log directories will continue to query clusters that have been removed for management from the Eyeglass interface.

Workaround: Contact support.superna.net for manual procedure for workaround.

Known Limitations

General

T8228 ECA Alarms not cleared automatically

ECA related alarms that appear in the Eyeglass Alarms window will not be cleared automatically.

Workaround: Alarms must be manually cleared. Open the Alarms window on the Eyeglass web interface and select the Clear link for the alarm that you would like to clear.

T15457 HTML 5 vmware vcenter bug on OVA deployment

Some versions of vmware vcenter HTML user interface have a known issue with OVA properties being read correctly post power on, leading to first boot issues.

Workaround: use the Flash client as a work around.

T17103 ECA version intermittently reported incorrectly

At times the ECA nodes report an incorrect version resulting in the RSW0010 alarm that ECA node version does not correspond to eyeglass version. This is an intermittent condition that clears itself without any action and does not impact ECA functionality.

T22924 ECA event rate alarm notification first instance

The ECA event rate alarm notification is sent on the first instance the alarm is raised. If alarm condition is met subsequently without clearing the alarm no further notification is sent.

© Superna Inc

1.12. Current Release - Release Notes Golden Copy

[Home](#) [Top](#)

Release Date	Version
12/14/2023	1.1.21-23252

- [What's New in Superna Eyeglass Golden Copy Release 1.1.21](#)
 - [New in 1.1.21](#)
 - [Usability Enhancements](#)
 - [Feature Enhancements](#)
 - [Better user job monitoring with activefiles summary integrated to job view small and large files](#)
 - [Job view changelist/layers enhancement](#)
 - [What's New in Cloud Browser for Data Mobility 1.1.21](#)
 - [New in 1.1.21](#)
 - [Feature Enhancements](#)
 - [Concurrent Cloud Mover Jobs](#)
 - [New in Superna Eyeglass Golden Copy Release 1.1.20\(10.05.2023\)](#)
 - [New in 1.1.20](#)
 - [Usability Enhancements](#)
 - [Feature Enhancements](#)
 - [Fixed in 1.1.20](#)
 - [GC-2057 Job marked as a FAILURE due to Snapshot Extend step](#)
 - [GC-2614 Archivedfolder Checksum Value Reverting to Default\(Off\) After Upgrade](#)
 - [GC-2409 UI - Recall gauges - Skips counting against success %](#)
 - [New in Cloud Browser for Data Mobility 1.1.20\(10.05.2023\)](#)
 - [New in 1.1.20](#)

- Feature Enhancements
- New in Superna Eyeglass Golden Copy Release 1.1.19(09/01/2023)
- New in 1.1.19 -23189
 - Usability Enhancements
 - Feature Enhancements
- Fixed in 1.1.19-23189
 - GC-2404 Archivedfolders checksum setting resets to Default (Off) after a VM restart
 - GC-2405 UI - Archivedfolders Tab - Edit not populating `Tier`, which seems to be a Requirement
 - GC-1897 Pipeline-Recall Does not skip files with the skip existent export
 - GC-2035 Job Cancel - Job should not be a SUCCESS if cancelled at any step
- New in Cloud Browser for data Mobility 1.1.19-23189 (09/01/2023)
 - Feature Enhancements
- Fixed in 1.1.19 Cloud Browser for data Mobility 1.1.19-23189
 - CBDM-528 Email - SMB share path uses an Incorrect folder separator for the selected sub-folders
 - CBDM-532 Email Needs Attention Causing Job Failure due to Unconfigured SMTP Server
 - CBDM-609 CBDM Browser - Buckets region being labelled incorrectly if there are other regions
 - CBDM-615 Cloud to Premise - Submit SMB Target Button is obscured probably when the path is too long
 - CBDM-614 Cloud Browser - Unable to browse buckets in regions other than the one specified in Credentials
 - CBDM-591 Skipping incremented from failing to move files to SMB due to the limit
- Supported OneFS releases
- New in Superna Eyeglass Golden Copy Release 1.1.17 (07/27/2023)
- Fixed in 1.1.17

- GC-1774 Json and Html report of recall/pipeline recall job is not showing accurate results for skipped files.
- GC-2254 upgrade from 1.1.9 - after upgrading, the running job is not continuing to run
- GC-1687 Can't add AD user to admin for GC, when username contains few special characters.
- GC-2399 Grafana - All Time Gauges - Negative % number
- GC-2237 Issue with login when there are spaces in the AD user name
- GC-1994 Pre Win2k usernames able to be added to Admin but fail at login
- Fixed in 1.1.17 Cloud Browser for data Mobility 1.1.17
 - CBDM-412 Cloud to Premise - Parallel Jobs - Issues including Objects incorrectly Moved into a single SMB path
 - CBDM-428 CBDM - files are recalled on wrong path instead of `ifs/fromcloud/CBDM` its recalling on `ifs/fromcloud/BDM`
- What's New in Superna Eyeglass Golden Copy Release 1.1.16
- Fixed in 1.1.16
 - GC-1879 Auto ReRun - Add Stats for job `ReRun - Folders` and Stats Issues
 - GC-1905 Pipeline Recall with `--trash-after-recall` does not delete original files
 - GC-1697 UI - Editing archivedfolders after the first Edit does not close the Edit box - Changes applied
 - GC-1748 ReRun of Incremental Rename does not work because missing info on previous name
- New in Superna Eyeglass Golden Copy Release 1.1.15 (05/03/2023)
- Fixed in 1.1.15
 - GC-1525 UI-Language change function is not working
 - CBDM-235 Cloud to Premise - Jobs History - Skipped bytes added to Success bytes
 - CBDM-272 Job is marked as done without Recall if the Email is unchecked
 - GC-1987 UI - Missing Edit and Add archivedfolders
 - GC-1205 Backup and recover functionality-Not able to fully recover the system

- GC-1880 When Auto-ReRun is triggered it can use the wrong job data (of another archivedfolders)
- GC-1749 Longpath - Incremental Rename did not update the JSON content - Recall downloaded old name
- New in Superna Eyeglass Golden Copy Release 1.1.14 (04/04/2023)
- Fixed in 1.1.14
 - GC-1750 Longpath- Incremental Modify (Content) did not update the inode for Hardlink
 - CBDM-234 Cloud to Premise - Jobs History and Running - Errors not counted
 - CBDM-262 Local admin is seeing a bucket without adding Credential
 - GC-1700 Remove suffix of downloaded files
- New in 1.1.14
 - Version Based Recall
 - Usability Enhancements
 - Cloud Browser for Data Mobility 1.1.14
 - Usability Enhancements CBDM
- New in Superna Eyeglass Golden Copy Release 1.1.13 (03/06/2023)
- Fixed in 1.1.13 Release
 - GC-1510 Non-admin is able to see all archivedfolders
 - CBDM-213 Cloud to Premise - Jobs data for Running and History should show Target SMB
 - CBDM-190 Cloud to Premise - Keep objects with the same names during Staging
 - GC-970 Long Path Support - Rename fails possibly due to S3 Error that key is too long
- New in 1.1.13-23045
 - Supported Versions of S3 Targets
 - Supported S3 Protocol Targets
 - End of Life Notifications
 - Deprecation Notifications

- Azure default Tier change
- HTML Summary Report to be deprecated
- Support Removed / Deprecated in this Release
 - Recall the "metadata" option
- New in Superna Eyeglass Golden Copy Release 1.1.12 (02/03/2023)
- Fixed in 1.1.12 release:
 - GC-1078 UI - Pause and Start buttons have no action
 - GC-1513 Golden Copy special character regression for ECS, AWS
 - GC-1070 job id is lost after upgrade to 1.1.11 so no jobs running/jobs view/job history and folder stats
 - GC-1069 Multi part files recall issue - Recall files much larger than the original
 - The system view tab works
- New in Superna Eyeglass Golden Copy Release 1.1.11 (09/27/2022)
- New in 1.1.11
 - GC-2 Treewalk Robustness
 - GC-138 Refresh GUI pages
 - GC-337 Custom Metadata from application-specific files
 - GC-341 Keep full history of file and object in objects as they're moved to the cloud
 - GC-373 Bugs
 - GC-586 Download file(s) to User pc from cloud browser
 - GC-762 Cloud file download from GCS for all file types
- Fixed in 1.1.11
 - T23283/GC-396 Golden Copy GUI fully restricted for non-admin user
 - GC-562/563 Jobs view for large file is not accurate
- Not available in 1.1.11
 - T17181 Archive to AWS Snowball
 - T17195 Upload to Azure, Cohesity, ECS or Ceph via Proxy
 - T16247 DR cluster alias / redirected recall

- Technical Advisories
- Known Issues
- Known Issues Archiving
 - T14560 Cloud Browser Access with MacOS
 - T14014 Incremental upload requires 2 cycles before picking up changes
 - T15312 Archive job incorrectly presented as completed
 - T16425 Archive incremental upload does not handle changelist in waiting state/queued and incremental fails
 - T16629 Azure upload error where name contains %
 - T16667 Data integrity audit job size parameter gives incorrect results
 - T17449 Folder missing meta data information for Azure container with legal hold or retention policy
 - T18012 Folders with language specific characters not uploaded
 - T18107 Incremental archive job may miss files on restart, jobid lost
 - T18252 Empty folder uploaded as file on Google Cloud Storage
 - T18241 Cannot add 2 Powerscale cluster to Golden Copy with same archivedfolder configuration
 - T18979 Incremental Archive issues for files with Zone.Identifier suffix
 - T19218 Setting to enable delete for Incremental archive not working
 - T19305 Queued jobs are not managed
 - T19388 Fast Incremental incorrectly stores UID and GID properties
 - T19441/GC-543 Move/Delete operation in a single incremental sync orphans data in S3 target
 - T20379 Canceled archive job continues upload
 - T21370 No message when snapshot for upload from snapshot is not in Golden Copy inventory
 - T21745 s3update with a large number of changes may incorrectly delete folder objects with ACL information
 - T21889 Issues with rerun of recall job
 - T21891 Rerun of Incremental Job does not finish

- T21687 Parallel Full Archive Jobs may have some stuck jobs
- T22208 Cannot run a failed job again
- T22925 Cannot use existing folder to copy from DR cluster
- T23126 Issues with full and incremental jobs for folders when S3 prefix is used
- T23275 Archive job with s3update archive job does not complete
- GC-401 The '--only-folders' option for rerun is not available
- GC-384 Schedule incorrectly applied to a paused job
- GC-63 Same folder archived to different buckets results in error
- GC-675 Archive job does not finish when tree walk fails at the beginning
- General Reporting Issues
 - T17647 After restart stats, jobs view, export report, cloud stats not consistent
 - T17932 searchctl jobs view or folder stats may be missing reporting on small percentage of files uploaded.
 - T18587 isilongateway restart may remove jobs history and running jobs information
 - T19136 Jobs View / Export Report do not correctly calculate job run time if job is interrupted
 - T19466 Statistics may show more than 100% archived/attempted after a cluster down/up
 - T21186 Statistics may not be accurate when there is a rename operation
 - T21257 The 'file change count' column in jobs running always shows 0 for incremental archive
 - T20497 The jobs history '--tail' argument not working
 - T21572 Export report for folder with multiple jobs may only produce 1 report
 - T21668 Copy from flat file does not report errors
 - T21727 s3update stats include count for updated and unchanged objects
 - T21888 Issue with errors command
 - T20445 Jobs view count not accurate when parallel jobs are running
 - T22523 Export command error json files may be missing files

- T23450 Jobs Summary email report always shows running job
- GC-385 jobs view and stats view incorrect for paused job that is resumed after a cluster down/up
- GC-383 Pipeline recall stats may be incorrect
- GC-557 Export Report for incremental job with rename operations shows incorrect stats
- Recall Reporting Issues
 - T16960 Rerun recall job overwrites export report
 - T17893 searchctl archivedfolders history incorrectly shows recall job as job type FULL
 - T18535 Recall reporting issue for accepted file count / interrupted recall
 - T18875/T21574 Recall stats may incorrectly show errored count
 - T19415 Recall stats incorrectly show errors for folder object which store ACLs
 - T20500 'jobs view' for recall job not incrementing meta data related stats
 - T21561/T21577 Recall stats issues
 - T21778 Issues with Export for Recall job with meta-data
 - GC-574 Recall stats are empty when the --older-than and --new-than options are used
- Known Issues Recall
 - T16129 Recall from Cohesity may fail where folder or file contain special characters
 - T16550 Empty folder is recalled as a file for GCS
 - T18338 Recall Rate Limit
 - T18428 Recall for target with S3-prefix result in extra S3 API call per folder
 - T18450 Folder object in S3 that contains folder ACL information incorrectly recalled as a directory when ARCHIVE_S3_PREFIX set
 - T18600 Recall Job where recall path is mounted does not indicate error
 - T19012 Recall of files from Azure fails for files uploaded with Golden Copy earlier than 1.1.4-21050
 - T19438 Files may not be recalled

- T19649 Meta-data not recalled where AD user/group cannot be resolved
- T21291 Version based recall may not apply folder ACLs when using '--apply-metadata'
- T21626 Recall Job for large number of files may get stuck
- T23220 Recall to a different target cluster does not correctly recall objects
- T23312 Recall --start-time and --end-time options do not recall any data
- T23315 Recall --older-than option creates folder structure when there is no matching objects
- T23398 Recall job intermittently fails at step "Create Distributed Kafka topic for LINKS"
- T23474 Recall path incorrect with multiple cluster uses Pipeline configuration for all clusters
- GC-652 Recall - Stats issue with multipart files
- GC-967 Long Path - Recall Metadata not applied correctly for Multipart files
- GC-1079 Recall folder stats sometimes have doubled stats/more than 100% complete stats
- GC-2378 Pipeline Recall and CBDM - job view is intermittently showing `0` recalled Bytes
- Known Issues Media Mode
 - T23160 Failed link archive are not recorded in stats
 - T23159 Hard link percentage saved shows negative value
 - T22022 Error on incremental for link object with suffix
 - T22510 Symlink mode always set to 777
 - T22488 Object storage still contains file after all hard links and original file have been deleted
 - T22484 Deleting original hard link file may result in multiple copies of the file in object storage
 - T23475 Error in Media Mode stops archive job
 - T23479 Golden Copy GUI does not report statistics for hard links / symlinks processed
 - T23546 Media Mode not compatible with checksum on

- GC-544 Symlink not archived without setting ARCHIVE_LINK_SUFFIX
- GC-934 Incremental - Symlinks Rename failed possibly when using export that enables suffix
- GC-971 Long Path - Incremental Delete fail possible due to s3 error that key is too long
- Known Issues Pipeline
 - T23045/T22539 Move to Trash / Delete configuration is not working
 - T23036 No stats for Pipeline recall skipped files
 - T23035 Jobs view does not track delete from source progress
 - T22013 Pipeline recall with the --source-path option does not apply meta-data
- Known Issues Golden Copy GUI
 - T23436 Golden Copy GUI folder and all time stats are inconsistent
 - T23150 Error on adding or editing archivefolder has no details
 - T23131 Golden Copy GUI combines Upload and Recall stats
 - T23087 Golden Copy GUI available for Add/Edit/Delete folder for AWS, Azure and ECS
 - T23076 No validations when editing folder from Golden Copy GUI
 - T22851/T23145 Golden Copy GUI Folder Management GUI Issues
 - T23002 Golden Copy Cloud Browser filters not displayed
 - T22954 Golden Copy GUI does not correctly show Pipeline license
 - T22385 Golden Copy GUI shows Search product on some pages
 - GC-438/GC394 Unable to manage Google Cloud Storage folder from Golden Copy GUI
 - GC-447 Jobs Errors does not display errors with a large number of jobs in the Jobs History
 - GC-607 Cloud Browser - support self signed certificates on local targets
- Known Issues General & Administration
 - T14025 Changing PowerScale user requires a cluster down/up
 - T16640 searchctl schedules uses UTC time

- T16855 Archived Folders for Powerscale cluster added with the --goldencopy-recall-only option does not appear in the archivedfolders list command
- T17987 Alarm for cancelled job shows job failed
- T21073 Phone home may fail when archive folder path contains characters 'id'
- T17200 Error on cluster up after power off/on
- T21227 Backup & Restore missing configuration
- T22337 Firewall down after node reboot
- T22373 Cannot configure admin user or group with space in name
- T22988 searchctl archivedfolders list --verbose incorrectly displays accesskey
- T22957 Modify command does not change Powerscale IP address
- T22912 Golden Copy Advanced and Pipeline licenses cannot be removed
- T22913 Licensing of Powerscale can be lost
- T23223 Golden Copy goldencopy-recall-only Powerscale cannot be licensed
- T23382 Verbose archived folders list shows properties no longer used
- GC-434 The 'recall-only' option set randomly for PowerScale
- GC-426 Adding folder with '--delete-from-source' option does not accept true/false argument
- GC-445 Timeout for delete where --delete-from-source is configured is too long
- GC-1119 some file uploads get errored during the upgrade.
- GC-1482 Azure support for certain character combination
- GC-1540 Unable to add a folder named with double quotes and back slash to GC.
- GC-2233 GoldenCopy - Running a second job with skips enabled causes the job not to complete
- GC-2387 Incremental - Count Accepted is different than Archived possibly due File_Rename
- GC-2450 Backup and Restore Kafka topic's content
- GC-2485 customMetadata 100k characters limit Error
- GC-2692 Large Changelists Max Out Isilongateway RAM

- GC-2631 Single node has errors about multiple zk nodes
- GC-3012 UI - Unable to add AWS `us-east-1` archivedfolders
- DEVSECOPS-258 `libzyp`/`rpm` bug causes installers to fail
- Known Limitations
 - T15251 Upload from snapshot requires snapshot to be in Golden Copy Inventory
 - T15752 Cancel Job does not clear cached files for processing
 - T16429 Golden Copy Archiving rate fluctuates
 - T16628 Upgrade to 1.1.3 may result in second copy of files uploaded for Azure
 - HTML report cannot be exported twice for the same job
 - T16250 AWS accelerated mode is not supported
 - T16646 Golden Copy Job status
 - T17173 Debug logging disk space management
 - T18640 searchctl archivedfolders errors supported output limit
 - GC-1504 Parallel jobs limited to 10 at a time
 - GC-1527 Cloud Browser - Single File Download - Support for downloading symlinks that points to a hardlink
 - GC-1625 Incremental Delete not working for deleted Symlink possibly due to suffix
 - GC-2292 `--follow` option for rerun has an exception error
 - GC-2789 3 Nodes : Folder stats empty `searchctl stats view --folder <folderID>` and `searchctl archivedfolder stats --id <folderID>`
 - GC-2804 Phonehome Logs Upload Issue on HyperV OVF 3-Node
 - GC-3008 Short parallel archive jobs showing 0 stats intermittently
- Fast Incremental Known Limitations
 - Move/Rename identification and management in object storage known limitations
 - T20868 Cannot run incremental update for same folder to multiple targets
 - T21258 Version based recall uses UTC time for inputs

- T21759 Unable to export recall job multiple times
- T21925 Export reporting limit
- T22680 Media Mode Hardlink mode may copy more than 1 copy of the file
- T22469 Media mode does not copy broken symbolic links
- T22630 Media mode may orphan hardlink objects when all Golden Copy nodes are not able to archive
- T23130 Media mode has no stats for broken symlink
- GC-433 PowerScale may return success for recalled file even if PowerScale blocks saving the file
- GC-459 Recall error for multi-part file leaves incomplete file on file system
- GC-450 Golden Copy - Traceback on cluster up
- GC-446 Stats conversion from bytes incorrect
- GC-874 Audit - Job is stalled after hitting exactly 50k files
- GC-938 Incremental - Only the original hardlink is updated possibly due to changelist limitation
- GC-1020 Cloud Browser - Unable to download file from Wasabi
- GC-1308 Increase/Customize/Remove the 1000 error limit
- Cloud Browser for Data Mobility
- Known Issues Cloud Browser for Data Mobility
 - CBDM-168 Wasabi - Unable to add archivedfolders from CLI without using https://
 - CBDM-171 CBDM Browser - List limited to 1000 objects and possibly blocking access to lower 'paths'
 - GC-412 Archive job does not handle a block "b" special file
 - CBDM-512 CSV Export - Special characters probably causing the columns not being populated correctly
 - CBDM-322 Cloud to Premise - Recall phase is not skipping existing files
 - CBDM-502 Cloud to Premise - the staged files should be delete from the bucket even without the recyclebucket
 - CBDM-503 Unable to modify to remove recyclebucket from the folder

- CBDM-383 Cloud to Premise - Stats differences between Staging and Recall
- CBDM-390 Cloud to Premise - Run Copy/move job with unchecked the "Email on job completion" , then should not get an email for that job.
- CBDM-227 Block adding email recipient if no channel
- GC-2410 Recall - Errors from DENY (to download) bucket policy being counted as Skips
- CBDM-692 CBDM Job Fails When Selecting Entire Bucket
- CBDM-693 Staging Path Not Cleared on Skipped Job: Pending Issue Resolution
- CBDM-753 Pinned archiveworker nodes intermittently not assigned to Kafka consumer group `archiveworker`
- CBDM-744 1/4 parallel jobs failed at Staging due to trying to create `-CBDM` topics
- CBDM-761 Round-robin and Pinned archiveworkers behaviour in parallel jobs
- Known Limitations Cloud Browser for Data Mobility
 - CBDM-407 Parallel CBDM jobs stats seems to be incorrect
 - CBDM-543 Cloud to Premise - Stats for Move step
 - CBDM-631 Parallel Job - Error `Fail to lock` when the same user downloads the same data into the same Target
 - CBDM-777 Staging cannot use s3 keys that are over the AWS S3 key limit (1024 bytes)

What's New in Superna Eyeglass Golden Copy Release 1.1.21

New in 1.1.21

Usability Enhancements

Job view output now displays:

- Folders accepted
- Folders succeeded
- Folders failed

Feature Enhancements

1. Job error log and archiveworker logging to include the S3 request ID's.
2. Google (GCS) was added for Admin and Non-Admin users.

Better user job monitoring with activefiles summary integrated to job view small and large files

Active copies of GUI are now showing for each node NODE or CLUSTER:

1. The total # of files being copied
2. Total small file count and the % of the total this represents
3. Total large file count and the % of the total this represents
4. Show the sum of all files in active copies for ALL nodes in TBs
5. Show a table with the following break-down:
 - a. files 1 byte - 100K
 - b. 100K - 1MB
 - c. 1MB - 5MB
 - d. 5MB - 100MB
 - e. 100MB - 1G
 - f. 1G - 100G
 - g. 500G - 1TB
 - h. Greater than 1TB

Job view changelist/layers enhancement

Job view now includes these changelist details for incremental:

- The layer being processed
- How many layers
- The layer size
- The # of files per layer
- Total amount of files in the changelist

What's New in Cloud Browser for Data Mobility

1.1.21

New in 1.1.21

Feature Enhancements

After all files have been moved to SMB shares, the Email notification will be sent.

Concurrent Cloud Mover Jobs

1. Round-robin archived folders. Now, the user can manually create two or more archivedfolders (pipelines) that can be used for recall and have the user jobs select archivedfolders on a round-robin basis so that the user can support multiple concurrent download jobs (by the same user or different users) at the same time.
2. It's possible now manually assign some archivedfolders to specific archivedfolders so that I can separate the archiveworker resources acting on each folder.

New in Superna Eyeglass Golden Copy Release

1.1.20(10.05.2023)

New in 1.1.20

Usability Enhancements

1. The Cancel Job button was added for active running jobs. The user can now easily cancel an active running job with the click of a button.
2. The job status **NEEDS ATTENTION** shows more status and reasons. Now, the job statuses will include three distinct states: "Success," "Failure," and the new "Needs Attention". The reasons - 'High Error Rate', 'Low Error Rate', 'Treewalk Errors'
3. Disk space display script simplifies monitoring disk space usage on users' appliances. This script allows users to effortlessly check the disk space status of their relevant volumes, enabling them to troubleshoot disk space errors more efficiently.

Feature Enhancements

1. Incremental logging was added. Incremental logging will display the total number of files found in the changelist in both the IG log and the searchctl job view.
2. Archiveworker Redis Cache - Redis caching was added to optimize the handling of finished work, ensuring a more efficient and responsive experience. AW restarts can cause us to re-work non-committed events.

Fixed in 1.1.20

GC-2057 Job marked as a FAILURE due to Snapshot Extend step

Job marked as a FAILURE due to Snapshot Extend step. Specifically when the Snapshot Extend step is unable to determine the state of the job

GC-2614 Archivedfolder Checksum Value Reverting to Default(Off) After Upgrade

Following an upgrade, The checksum value unexpectedly reverts to its default state, making all ArchivedFolders added after the upgrade set to the default checksum value.

```
ecaadmin@mpg6160-1:~> searchctl archivedfolders getConfig
{
  "getGoldenCopyConfig": {
    "rateLimit": "",
    "fullArchSnapExpiry": 25,
    "checksum": "DEFAULT"
  }
}
```

- Workaround: Set it back to ON.

```
ecaadmin@mpg6160-1:~> searchctl archivedfolder config --checksum ON
{
  "data": {
    "gcConfigure": {
      "rateLimit": "",
      "fullArchSnapExpiry": 25,
      "checksum": "ON"
    }
  }
}
```

GC-2409 UI - Recall gauges - Skips counting against success %

The UI gauges may show a lower than expected Success % number if, during a Recall job, there were files that were skipped.

New in Cloud Browser for Data Mobility

1.1.20(10.05.2023)

New in 1.1.20

Feature Enhancements

1. Highlighted Folder Icons. The folder icon will be dynamically highlighted when the user selects folders or parent folders within the path selector tree.

New in Superna Eyeglass Golden Copy Release

1.1.19(09/01/2023)

New in 1.1.19-23189

Usability Enhancements

1. Backup notifications and configuration settings added.

Feature Enhancements

1. The function `--follow` when running jobs was added to follow that job's progress within the same command. Existed for other jobs but now includes rerun.
2. The `ecactl` search notifications list is shown chronologically now.
3. Failed hardlink and softlink on rerun jobs are added to the rerun topic to re-download **only** failed files on a job.
4. AW skip existing files using `ARCHIVE_WORKER_RECALL_SKIP_EXISTENT_FILES`.

Fixed in 1.1.19-23189

GC-2404 Archivedfolders checksum setting resets to Default (Off) after a VM restart

If the checksum option has been changed to `On`. A VM restart will set it back to `Default` which is `Off`.

GC-2405 UI - Archivedfolders Tab - Edit not populating `Tier`, which seems to be a Requirement

When using the UI to edit an archivedfolders, the text field `Tier` is a requirement. And it might not be populated because the archivedfolders was added without specifying a Tier. For AWS the default tier is named `DEFAULT`.

GC-1897 Pipeline-Recall Does not skip files with the skip existent export

Existing Files are not getting skipped on the second run for pipeline recall job and instead getting duplicated.

GC-2035 Job Cancel - Job should not be a SUCCESS if cancelled at any step

Job Cancel - Job should not be a SUCCESS if cancelled at any step.

New in Cloud Browser for data Mobility 1.1.19-23189 (09/01/2023)

Feature Enhancements

1. Multipart copy between buckets for user bucket to staging buckets with cross-region support. Users can stage files from the source bucket to the staging bucket even if they are in different regions.
2. It is also implemented for copy-to-trash.
3. This also gets us over the AWS limit of 5G with the standard copy operation.

Fixed in 1.1.19 Cloud Browser for data Mobility

1.1.19-23189

CBDM-528 Email - SMB share path uses an Incorrect folder separator for the selected sub-folders

When a subfolder is selected instead of the root path of the SMB, this email line is incorrect

```
SMB Share Path \\<ip>\<smbName>/subfolder
```

It should be

```
SMB Share Path \\<ip>\<smbName>\subfolder
```

CBDM-532 Email Needs Attention Causing Job Failure due to Unconfigured SMTP Server

When attempting to add an email recipient on the user profile page, if the SMTP server is not properly configured, the email step fails. This failure, in turn, causes the entire job to fail, impacting the overall job status

CBDM-609 CBDM Browser - Buckets region being labelled incorrectly if there are other regions

Buckets region being labelled incorrect if there are other regions.

CBDM-615 Cloud to Premise - Submit SMB Target Button is obscured probably when the path is too long

When selecting an SMB target, the Submit button can be obscured depending on the length of the SMB target.

Workaround: After selecting the path, click outside the path picker, the picker should close, and the selected path should be selected for the Target.

CBDM-614 Cloud Browser - Unable to browse buckets in regions other than the one specified in Credentials

Unable to browse buckets in regions other than the one specified in Credentials.

CBDM-591 Skipping incremented from failing to move files to SMB due to the limit

The incorrect handling of files exceeds the limit when moving them to an SMB path. Instead of failing/getting errors, they are marked as skipped.

Supported OneFS releases

8.2.x.x

9.1.x.x

9.2.x.x

9.3.x.x

9.4 via the February RUP 9.4.0.12 (PSP-3079) released Feb 8th 2023

9.5.x.x (minimum 9.5.0.1)

New in Superna Eyeglass Golden Copy Release 1.1.17 (07/27/2023)

Fixed in 1.1.17

GC-1774 Json and Html report of recall/pipeline recall job is not showing accurate results for skipped files.

Json and Html report of recall/pipeline recall job is not showing accurate results for skipped files.

GC-2254 upgrade from 1.1.9 - after upgrading, the running job is not continuing to run

The archive job was running before the upgrade. Cluster down while the job is running.

after the upgrade, the job is not running; the job is not in running jobs and jobs history - files are not uploaded to the bucket.

GC-1687 Can't add AD user to admin for GC, when username contains few special characters.

Can't add Ad user to admin for Gc, when username contains few special characters like

% ^ * + ` = { } [\ | : ; " < > , ?

GC-2399 Grafana - All Time Gauges - Negative % number

Seeing negative % number in the All-time graphs. Is it possible that if failure is higher than success, it could produce that negative % number?

GC-2237 Issue with login when there are spaces in the AD user name

The issue with login is when there are spaces in the AD user name

GC-1994 Pre Win2k usernames able to be added to Admin but fail at login

Pre Win2k usernames able to be added to Admin but fail at login

Fixed in 1.1.17 Cloud Browser for data Mobility 1.1.17

CBDM-412 Cloud to Premise - Parallel Jobs - Issues including Objects incorrectly Moved into a single SMB path

Parallel jobs seem to have issues with jobs run by the same user or different users.

CBDM-428 CBDM - files are recalled on wrong path instead of `ifs/fromcloud/CBDM` its recalling on `ifs/fromcloud/BDM`

Trailing slash / to recall source path breaks recall. Make sure `--recall-sourcepath` does not have a trailing slash

What's New in Superna Eyeglass Golden Copy Release 1.1.16

Fixed in 1.1.16

GC-1879 Auto ReRun - Add Stats for job `ReRun - Folders` and Stats Issues

Auto ReRun - Add Stats for job `ReRun - Folders` and Stats Issues

GC-1905 Pipeline Recall with `--trash-after-recall` does not delete original files

Pipeline Recall with `--trash-after-recall` does not delete original files

GC-1697 UI - Editing archivedfolders after the first Edit does not close the Edit box - Changes applied

After editing an archivedfolder, trying to edit again (another or the same one) does not close the Edit box

GC-1748 ReRun of Incremental Rename does not work because missing info on previous name

ReRun of a failed Incremental Rename does not work because of missing info on the previous name. Every time a ReRun is initiated on this event, there is also an NPE.

New in Superna Eyeglass Golden Copy Release 1.1.15 (05/03/2023)

Fixed in 1.1.15

GC-1525 UI-Language change function is not working

The drop-down button on the language change is not functioning.

CBDM-235 Cloud to Premise - Jobs History - Skipped bytes added to Success bytes

The skipped bytes are added to the Success bytes.

CBDM-272 Job is marked as done without Recall if the Email is unchecked

For cloud to premise jobs (with email checked) the jobs are basically paused until a Recall job is run.

GC-1987 UI - Missing Edit and Add archivedfolders

Add/Edit of archivedfolders not available in UI.

GC-1205 Backup and recover functionality-Not able to fully recover the system

Backup and recover functionality-Not able to fully recover the system

GC-1880 When Auto-ReRun is triggered it can use the wrong job data (of another archivedfolders)

When Auto-ReRun is triggered it can use the wrong job data (of another archivedfolders)

GC-1749 Longpath - Incremental Rename did not update the JSON content - Recall downloaded old name

Renamed files (regular and hardlink) inside a longpath were not recalled with the new name.

**New in Superna Eyeglass Golden Copy Release
1.1.14 (04/04/2023)**

Fixed in 1.1.14

GC-1750 Longpath- Incremental Modify (Content) did not update the inode for Hardlink

Inside a longpath, after changing the content of a hardlink, the inode did not get updated on s3.

CBDM-234 Cloud to Premise - Jobs History and Running - Errors not counted

Errors are not counted in **Cloud to Premise** job data.

CBDM-262 Local admin is seeing a bucket without adding Credential

The local user sees a bucket when no Credentials have been added.

Local users should only be able to view jobs/history

GC-1700 Remove suffix of downloaded files

Able to download files inside a long path using Cloud Browser. However, the files have a suffix

New in 1.1.14

Version Based Recall

Date Based Recall on the UI is now available. During recall, users can now enter a date and recall the version of the object that was most recently uploaded before the selected date.

Usability Enhancements

1. Auto retry of failed folders and files with new job spawned at the end of archive job
2. `--folder-only` option added to re-run
3. Functionality `--follow` tag to archivedfolders recall is now

Cloud Browser for Data Mobility 1.1.14

Usability Enhancements CBDM

1. Moving data to CBDM share is available now.
2. Job's affected files to CSV file for download can be exported now.
3. Faster jobs history table, with in memory cache

New in Superna Eyeglass Golden Copy Release 1.1.13 (03/06/2023)

Fixed in 1.1.13 Release

GC-1510 Non-admin is able to see all archivedfolders

Regression in the way archivedfolders are listed for non-admin users.

CBDM-213 Cloud to Premise - Jobs data for Running and History should show Target SMB

Running jobs and their history do not show where the Copy/Move is/was going into.

CBDM-190 Cloud to Premise - Keep objects with the same names during Staging

Keep objects with the same names during Staging

GC-970 Long Path Support - Rename fails possibly due to S3 Error that key is too long

Incremental with file renaming on the long path does not work in this release.

Workaround: Run a full archive to re-upload the renamed files.

New in 1.1.13-23045

Refer to previous 1.1.12 builds for what's new.

Supported Versions of S3 Targets

ECS 3.6, 3.7, 3.8

AWS S3 - all

Azure - all

Google Storage - all

Cohesity - contact support

Flashblade - contact support

MinIO - contact support

Wasabi - all

Ceph version 15

Supported S3 Protocol Targets

The supported S3 Protocol targets can be found in the documentation [here](#).

End of Life Notifications

End of Life Notifications can be found [here](#).

Deprecation Notifications

Azure default Tier change

In the next release, the default tier for Azure upload will change from cold to hot. Tier-specific upload to Azure will require an advanced license.

HTML Summary Report to be deprecated

In the next release, the HTML report created using the export command will be deprecated and replaced by a job report that is created and downloadable from the Golden Copy GUI.

Support Removed / Deprecated in this Release

Recall the "metadata" option

The option to recall metadata only or re-apply metadata to a previous recall job is no longer available. The recall job can be run again if required.

New in Superna Eyeglass Golden Copy Release

1.1.12 (02/03/2023)

Fixed in 1.1.12 release:

GC-1078 UI - Pause and Start buttons have no action

Pause and Start buttons in the Archived Folder tab are not available.

GC-1513 Golden Copy special character regression for ECS, AWS

Golden Copy special character regression for ECS, AWS

GC-1070 job id is lost after upgrade to 1.1.11 so no jobs running/jobs view/job history and folder stats

Running job status is possible to lose during the upgrade process.

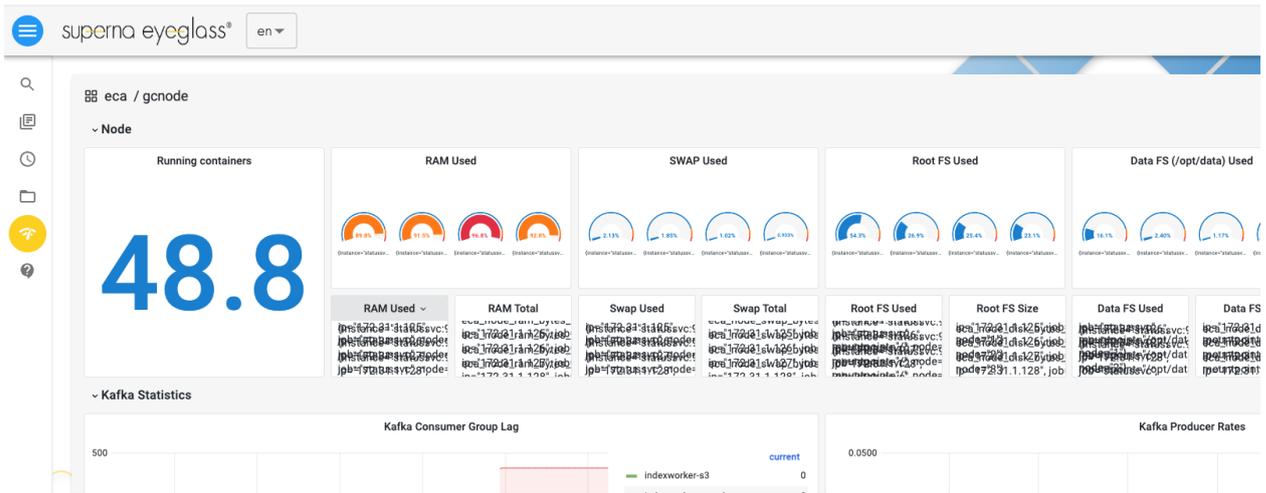
Workaround: Re-archive the files after the upgrade.

GC-1069 Multi part files recall issue - Recall files much larger than the original

Recalled files may have larger sizes than the original file and are not usable.

Workaround: None. Will retest in 1.1.12.

The system view tab works



New in Superna Eyeglass Golden Copy Release 1.1.11 (09/27/2022)

New in 1.1.11

GC-2 Treewalk Robustness

Added robustness to the treewalk process to handle errors and reduce duplication when there are issues in correctly retrieving data during the treewalk phase.

GC-138 Refresh GUI pages

Archive Jobs and Archived Folders pages now auto-refresh.

GC-337 Custom Metadata from application-specific files

Files can be optionally scanned during the upload process and custom metadata can be extracted and appended to the corresponding objects. This includes things like latitude and longitude from images, author from word documents, and more!

GC-341 Keep full history of file and object in objects as they're moved to the cloud

The full history of object to file and file to object transitions can be tracked within the data object itself. For a particular file or object, it is now possible to view the transition history, and the dates when file data moved into object data and vice versa.

GC-373 Bugs

Miscellaneous bug fixes.

GC-586 Download file(s) to User pc from cloud browser

Users can now download individual files from cloud targets directly from their web browsers.

GC-762 Cloud file download from GCS for all file types

When downloading single files from GCS targets, if the file is of a type that can be rendered in the browser, the browser will display it instead of saving it.

Workaround: When the browser displays the file, right-click the page and select save as

→ Save As in your browser to save the file to your computer.

Fixed in 1.1.11

T23283/GC-396 Golden Copy GUI fully restricted for non-admin user

Non - admin users can login to the Golden Copy GUI and are fully restricted from admin functionality.

Non-admin user can see all folders configured and can add new folders. Impact: Impact for folder management only. Folder can be added and job can be started.

Non - admin user can recall files from Cloud Browser. Note: Cloud Browser is properly filtered based on the shares for logged in user.

Resolution: Golden Copy GUI URL should be provided to non- administrative users.

GC-562/563 Jobs view for large file is not accurate

For a job that contains large file, the jobs view is incorrect. Large file bytes archived is reported as less than was actually archived.

Resolution: The stats view command for the folder has full Archive.

Not available in 1.1.11

T17181 Archive to AWS Snowball

Archive to AWS Snowball is not supported with this optimized update release. This is planned in the coming update.

T17195 Upload to Azure, Cohesity, ECS or Ceph via Proxy

Azure, Cohesity, ECS or Ceph clients using http proxy are not supported in this update.

T16247 DR cluster alias / redirected recall

The ability to recall a different cluster than the original source cluster is not supported in this update.

Technical Advisories

Technical Advisories for all products are available [here](#).

Known Issues

Known Issues Archiving

T14560 Cloud Browser Access with MacOS

Certificate handling in MacOS can impact the cloud browser functionality

Work around: Use Windows OS with supported browsers

T14014 Incremental upload requires 2 cycles before picking up changes

For incremental upload, changes are detected by comparing 2 snapshots. After enabling incremental or incremental on a newly added folder will required 2 incremental upload cycles to run and create 2 different point in time snapshots before changes will be detected.

Workaround: none required

T15312 Archive job incorrectly presented as completed

For the case where all files have been uploaded but there is a larger file that is being uploaded in parts and a part is still in progress, the searchctl jobs running command will not show the job as running even though parts are still uploading.

Workaround: None required. The progress can be viewed in the logs. Final summary.html file once completed is correct.

T16425 Archive incremental upload does not handle changelist in waiting state/queued and incremental fails

A changelist on the Powerscale which is in waiting state or any other changelist condition that results in the "Job type Changelist is already running or queued" is not handled by Golden Copy incremental archiving which fails the incremental job instead of waiting and applying a timeout. Impact: Changes for that interval will be missed.

Workaround: A full archive can be run which will skip any files already up to date and will update those that require updating.

T16629 Azure upload error where name contains %

Upload of file or folder with name that contains % character to Azure is not handled and will fail.

Workaround: None available.

T16667 Data integrity audit job size parameter gives incorrect results

Using the searchctl archivedfolders audit command results in an error.

Workaround: None available. The data integrity audit job not available in the current release.

T17449 Folder missing meta data information for Azure container with legal hold or retention policy

For Azure container configured with legal hold or retention policy, upload of folder objects will be missing associated meta data for owner, group, mode bits, date stamps but ACLs are stored and protected. Golden Copy marks this upload as an error but the object is in fact created.

Workaround: None required.

T18012 Folders with language specific characters not uploaded

Folders with language specific characters are not uploaded but the files within the folder are uploaded.

Workaround: None available.

T18107 Incremental archive job may miss files on restart, jobid lost

A cluster down/up while an incremental archive job is running will not recover any files that have not already been added to the queue for upload. Those files will be missed and also will not be identified for upload on the next incremental cycle. The job id associated with the incremental job is also lost and not available in jobs history.

Workaround: Do not cluster down/up while an incremental archive job is running.

T18252 Empty folder uploaded as file on Google Cloud Storage

A folder on the file system that has no sub folders or files will be uploaded to Google Cloud Storage (GCE) as a file instead of a folder. This does not impact upload of overall archive job. On recall, the empty file is incorrectly downloaded as a file.

Workaround: None available.

T18241 Cannot add 2 Powerscale cluster to Golden Copy with same archivedfolder configuration

If you add 2 clusters to Golden Copy you cannot add the same archivedfolder for both as it results in duplicated folder id.

Workaround: Select unique path for archivedfolder for each cluster.

T18979 Incremental Archive issues for files with Zone.Identifier suffix

Under some conditions PowerScale will store files with a Zone.Identifier suffix. These files may be archived without meta-data or error on archive and not be archived at all.

Workaround: These files can be excluded from archive by adding " --excludes=*.Zone.Identifier" to the archivedfolder definition.

T19218 Setting to enable delete for Incremental archive not working

The system setting export ARCHIVE_INCREMENTAL_IGNORE_DELETES=false to enable deletes during incremental archive is not working. Deleted files on PowerScale are not deleted from S3.

Workaround: None available.

T19305 Queued jobs are not managed

Golden Copy executes up to 10 jobs in parallel. If more than 10 jobs are submitted remaining jobs are queued and waiting to fill a job slot once it becomes available. Queued jobs are not visible through any commands such as command for running jobs and they do not survive a restart.

Workaround: On restart any jobs that were queued will need to be restarted. Tracking is available for the 10 jobs that are running and jobs history for jobs that are completed.

T19388 Fast Incremental incorrectly stores UID and GID properties

When Fast Incremental is enabled, the UID and GID are crossed and stored against the wrong attribute. UID is incorrectly stored against the group attribute instead of the owner attribute and the GID is incorrectly stored against the owner attribute instead of the group attribute.

Workaround: When evaluating owner and group, use the owner attribute to determine the group and the group attribute to determine the owner.

T19441/GC-543 Move/Delete operation in a single incremental sync orphans data in S3 target

Under certain circumstances where in the same incremental update there is a move or rename of a folder an empty folder is orphaned in S3 target. For example for a move or rename of a folder and a delete of a sub-folder, the folder move is properly updated on S3 target but the deleted sub-folder is not deleted in S3 target. For a delete and rename of 2 subfolders and edit of a file in the renamed subfolder, the renamed and deleted folders are not deleted on the S3 target.

Workaround: Orphaned folder can be manually removed from S3 target using native S3 tools.

T20379 Canceled archive job continues upload

For an archive job that is cancelled while the phase of walking the filesystem is still in progress, the filesystem walk continues after the cancel and if another archive job on the same folder is started while the original snapshot is still present files from both snapshots will be uploaded. Impact: Any files that are uploaded twice will be skipped if they are already present and uploaded if not. Order of upload is not guaranteed.

Workaround: Please contact support.superna.net for assistance should this situation arise. Planned resolution in 1.1.6.

T21370 No message when snapshot for upload from snapshot is not in Golden Copy inventory

The archive job, which specifies an existing snapshot as the source of the copy requires that the specified snapshot is in the Golden Copy inventory. If an upload job is started without the snapshot in the inventory no error message is displayed.

Workaround: Inventory runs automatically once a day at midnight. If the snapshot specified is not in the inventory, the message will indicate that the job was submitted but there will be no job-id. Ensure that a job-id is returned when starting this job.

T21745 s3update with a large number of changes may incorrectly delete folder objects with ACL information

Under some conditions, running the s3update command will result in the deletion of folder objects for folders that were not modified. This affects the folder object storing the ACL information only, the data itself is still present.

Workaround: None available.

T21889 Issues with rerun of recall job

Rerun of recall job with meta-data fails to download the errored files.

Workaround: Use native tools to download the errored files.

T21891 Rerun of Incremental Job does not finish

Rerun of incremental job does not complete - stays in running state once finished and all previously errored files have been copied successfully.

Workaround: Contact support.superna.net for assistance.

T21687 Parallel Full Archive Jobs may have some stuck jobs

When you add folders and start jobs in short period of time one after another this can result in jobs getting stuck.

Workaround: After adding a folder and starting a job, wait at least 5 minutes before adding another folder and starting a job.

T22208 Cannot run a failed job again

If copy job fails to run, running the job again will also fail.

Workaround: Delete and readd the folder to run the copy again.

T22925 Cannot use existing folder to copy from DR cluster

In the event that original cluster used to copy files to object storage becomes unavailable and a 2nd DR cluster is now being used, incremental updates to the originally uploaded objects is not available. Impact: Impact to incremental updates only. Recall of data uploaded from original cluster to DR cluster is available. Adding a new folder on DR cluster for upload is available.

Workaround: Readd the folder for the DR cluster. Requires full archive for the folder and then incremental.

T23126 Issues with full and incremental jobs for folders when S3 prefix is used

With ARCHIVE_S3_PREFIX configured there are following issues for folders:

-on incremental archive when a folder is deleted, the corresponding folder object in object storage is not deleted resulting in orphaned folder objects - workaround: folder objects must be deleted manually from object storage

-on full archive folder copy is not skipped when it should be resulting in additional unnecessary creation of folder objects - workaround: none required

T23275 Archive job with s3update archive job does not complete

An archive job with the s3update archive option never completes.

Workaround: The s3update job should not be used in this release. Note that this command should not be used to compare the file system to the bucket, run a full archive to validate all data is copied.

GC-401 The '--only-folders' option for rerun is not available

If you specify the '--only-folders' option for rerunning a job to pick up any folders that encountered an issue during the treewalk phase of the initial archive, the job does not start and shows as not run.

Workaround: The folder can be archived again to pick up any missed folders. Any files that were successfully copied previously will be skipped by default.

GC-384 Schedule incorrectly applied to a paused job

If you pause a job for a folder that has a full schedule defined, the job will incorrectly start at the scheduled time but will get stuck and not complete.

Workaround: The stuck job can be cancelled. If you do not want the pause to apply any longer the folder should be updated.

GC-63 Same folder archived to different buckets results in error

The same folder from same source Powerscale configured multiple time to archive to different bucket on the same storage target results in duplicated folder IDs which causes associated archive and/or recall jobs to fail.

Workaround: None available.

GC-675 Archive job does not finish when tree walk fails at the beginning

When an archive job fails on all of the records in the treewalk stage, the job can hang indefinitely and must be manually cancelled.

Workaround: Cancel the job from the CLI using `searchctl jobs cancel --id <jobid>` and resubmit.

Known Issues Reporting

General Reporting Issues

T17647 After restart stats, jobs view, export report, cloud stats not consistent

After a cluster down/up or restart of indexworker, archiveworker or isilongateway containers there will be a mismatch in the stats.

Workaround: None available

T17932 searchctl jobs view or folder stats may be missing reporting on small percentage of files uploaded.

The searchctl jobs view command or folder stats command may not properly report all files uploaded to the S3 target.

Workaround: Verify file count directly on S3 target.

T18587 isilongateway restart may remove jobs history and running jobs information

An isilongateway container restart may result in information on running jobs and jobs history to be lost.

Without running job id, a job cannot be canceled or rerun.

This issue does not affect archiving of files. Any job in progress will continue to archive files.

Workaround: To monitor job progress, use the searchctl archivedfolders stats command which relies on folder id as opposed to job id.

T19136 Jobs View / Export Report do not correctly calculate job run time if job is interrupted

For an archive job that is interrupted - for example cluster down/up while archive job is running - the jobs view and export report show a run time that is shorter than the true duration of the job.

Workaround: None available

T19466 Statistics may show more than 100% archived/attempted after a cluster down/up

If there is an archive job in progress when a cluster down/up is done, the job continues on cluster up but the jobs view and folder stats may show more than 100% for Archived and Attempted files.

Workaround: The archive job can be run again to ensure all files are uploaded. Any files that are already present on the object storage will show as a skipped statistic.

T21186 Statistics may not be accurate when there is a rename operation

If there is an archive job which includes a rename operation, the job and folder stats may not be accurate.

Workaround: Verify in object storage the correct files have been uploaded.

T21257 The 'file change count' column in jobs running always shows 0 for incremental archive

For incremental archive, the searchctl jobs view command will show the number of files in the changelist, but the searchctl jobs running command always shows a 0 count.

Workaround: Use the searchctl jobs view command to see the number of files in the changelist.

T20497 The jobs history '--tail' argument not working

Using jobs history with the --tail option may have the following issues:

- not all job types returned
- results not sorted
- more results retrieved than specified in the tail
- error if tail argument exceeds total number of records but results still displayed

Workaround: None available. The jobs history command without the --tail option is working.

T21572 Export report for folder with multiple jobs may only produce 1 report

If multiple jobs have been run against a folder and then an export job is run for one of the jobs, a subsequent export job for a different job may not generate a report.

Workaround: Use the jobs view command to see the details of the job.

T21668 Copy from flat file does not report errors

On a copy from a flat file, where the copy encounters errors, jobs view and export incorrectly show the job as 100% success.

Workaround: Use folder stats or jobs view "Errors" stats to see error count.

T21727 s3update stats include count for updated and unchanged objects

The s3update statistic report combines counts for updated and unchanged objects in some cases such that the number of updated objects is incorrect. This is a reporting issue only, the correct objects are updated.

Workaround: None available.

T21888 Issue with errors command

Using the --tail and --count options together for the searchctl archivedfolders errors command does not respect the --count option and returns all errors.

Workaround: None available. The last n lines of errors will still be available for review. Note that --count option without tail is respected.

T20445 Jobs view count not accurate when parallel jobs are running

When there are parallel jobs running, the jobs view command may show counts for accepted, archived and skipped that are higher than the actual counts.

Workaround: Use the searchctl stats view command to see the statistics for the folders.

T22523 Export command error json files may be missing files

The export command correctly reports then number of errored files in the HTML summary report but the corresponding json files may be missing some files.

Workaround: None available

T23450 Jobs Summary email report always shows running job

The Jobs Summary email report always shows running jobs even when there are no jobs running. When a job is running the running job count is increased accordingly.

Workaround: There are running jobs if the running job count is higher than the count when system is idle.

GC-385 jobs view and stats view incorrect for paused job that is resumed after a cluster down/up

A paused job that is resumed after a cluster down/up will successfully archive remaining files, but the jobs view and stats view will show incorrect statistics.

Workaround: None available. Inspect on the target to confirm all files have been archived.

GC-383 Pipeline recall stats may be incorrect

The stats view and jobs view may incorrectly show higher number of objects recalled than were actually recalled on pipeline job.

Workaround: Verify on the file system directly the number of objects that were recalled.

GC-557 Export Report for incremental job with rename operations shows incorrect stats

For the case where there are multiple incremental jobs which have a rename operation, the export report statistics are incorrect.

Workaround: Use the searchctl jobs view command to see the statistics for the job.

Recall Reporting Issues

T16960 Rerun recall job overwrites export report

Rerun of a recall job followed by exporting a report will overwrite any previous export report for that folder.

Workaround: Export report from a previous recall can be recreated but running the searchctl archivedfolders export command for the appropriate job id.

T17893 searchctl archivedfolders history incorrectly shows recall job as job type FULL

The output from the searchctl archivedfolders history command will incorrectly show a recall job as job type FULL.

Workaround: searchctl jobs history correctly shows the job type as GoldenCopy Recall.

T18535 Recall reporting issue for accepted file count / interrupted recall

There is no stat for recall accepted file count. Also if a recall is interrupted during the walk to build the recall files, the job reports as success even though not all files were recalled.

Workaround: None available

T18875/T21574 Recall stats may incorrectly show errored count

Under some circumstances a recall job may show stats for Errors when in fact all files were successfully recalled.

Workaround: Use the `searchctl archivedfolders errors` command to check for errors. Manual count of files on the Powerscale may also be used to verify the recall.

T19415 Recall stats incorrectly show errors for folder object which store ACLs

Recall stats and error command incorrectly show errors related to meta data recall for the folder objects created to store folder ACLs.

Workaround: None required. These are not errors associated with the actual folder ACLs. These can be identified in the error command as the Metadata apply failed error will be listed against the folder name where folder has been prefixed with the PowerScale cluster name.

T20500 'jobs view' for recall job not incrementing meta data related stats

The `searchctl jobs view` command may incorrectly show 0 for metadata related stats.

Workaround: Use the folder stats to see cumulative stats for folder metadata recall.

T21561/T21577 Recall stats issues

- For a recall job where some files recalled had an error, the jobs view Accepted and Attempted stats are incorrect.
- Stats unrelated to the recall may get incremented:
FULL/MULTIPART_FILES_ACCEPTED , FULL/MULTIPART_FILES_ARCHIVED
- jobs view Stats for Count (Recall), Count (Metadata), Errors (Recall), Errors (Metadata) may be incorrect
- stats view FULL/FILES_ARCHIVED_RECALLED may not be accurate

Workaround: Use the searchctl archivedfolders errors command to check for errors. Manual count of files on the Powerscale may also be used to verify the recall.

T21778 Issues with Export for Recall job with meta-data

- The report incorrectly shows the Job Type as FULL and the report itself is located in the ./full folder.
- Accepted stats are incorrect
- snapshot path is incorrect

Recall jobs without metadata export as expected.

Workaround: Export report can be retrieved from the ./full folder but some report contents are incorrect as above.

GC-574 Recall stats are empty when the --older-than and -new-than options are used

A recall job using the --older-than or --newer-than options does not show any stats in the stats view. No impact to the recall job itself.

Workaround: Use jobs view to see the count and bytes archived.

Known Issues Recall

T16129 Recall from Cohesity may fail where folder or file contain special characters

Recall of files or folders from Cohesity which contain special characters may fail. Job is started successfully but no files are recalled.

Workaround: None available

T16550 Empty folder is recalled as a file for GCS

Recall from GCS target of an empty folder results in a file on the PowerScale instead of a folder.

Workaround: If the empty directory is required on the file system it will need to be recreated manually.

T18338 Recall Rate Limit

Golden Copy does not have the ability to rate limit a recall.

Workaround: None available within Golden Copy.

T18428 Recall for target with S3-prefix result in extra S3 API call per folder

For S3 target that require a prefix for storing folders, on recall an extra S3 API call is made per folder. This API call results in an error but does not affect overall recall of files and folders.

Workaround: None required

T18450 Folder object in S3 that contains folder ACL information incorrectly recalled as a directory when ARCHIVE_S3_PREFIX set

If Golden Copy is configured to apply ARCHIVE_S3_PREFIX on folder objects, on recall the folder object is incorrectly recalled as a directory to the Powerscale filesystem.

Workaround: None required

T18600 Recall Job where recall path is mounted does not indicate error

No error is displayed if recall path is not mounted. In this case files may be downloaded to the Golden Copy filesystem which is not the requested end location and could also result in disk space issues on the Golden Copy VM.

Workaround: Ensure that mount for recall path exists prior to starting recall job. See information [here](#) on the mount requirements.

T19012 Recall of files from Azure fails for files uploaded with Golden Copy earlier than 1.1.4-21050

Files that were uploaded to Azure with Golden Copy build prior to 1.1.4-21050 cannot be recalled back to PowerScale using Golden Copy.

Workaround: Native S3 tools can be used to recall files from Azure.

T19438 Files may not be recalled

Under some circumstances files may not be recalled without any error indicated in Golden Copy.

Workaround: Files can be manually retrieved using S3 native tools.

T19649 Meta-data not recalled where AD user/group cannot be resolved

For case where files are uploaded and the owner or group was returned by the PowerScale API as Unknown User or Unknown Group because those owner/group no longer exist, on recall the Unknown User/Group cannot be resolved and block any other meta data from being applied.

Workaround: Meta data in S3 target can be used to confirm original meta data settings and manual steps on the operating system to apply them.

T21291 Version based recall may not apply folder ACLs when using '--apply-metadata'

When using version based recall, if the parent folder of an object with multiple versions only has 1 version, the parent folder ACLs may not be applied.

Workaround: Reference for parent folder ACLs are stored as separate folder object in object storage and can be applied manually.

T21626 Recall Job for large number of files may get stuck

For a large recall job, Golden Copy may get stuck with files left to recall or once the recall job is completed.

Workaround: Contact support for assistance.

T23220 Recall to a different target cluster does not correctly recall objects

Recall to a PowerScale cluster that has been added as a --goldencopy-recall-only cluster cannot be used due to the following issues:

- objects may be targeted for recall to an incorrect location on the file system resulting in error on recall or incorrect location on filesystem
- meta data is not applied on recall
- searchctl archivedfolders export report Job Type shows as FULL instead of RECALL

Workaround: None available.

T23312 Recall --start-time and --end-time options do not recall any data

Specifying --start-time and / or --end-time option on recall does not return any results.

Workaround: If the data can be identified based on the object timestamp rather than the file metadata, the --older-than and/or --newer-than option can be used.

T23315 Recall --older-than option creates folder structure when there is no matching objects

Recall using the --older-than option where the input is not in the range of any object timestamp, no files are recalled as expected but the folder structure is created on recall and jobs view stats incorrectly show all files are recalled.

Workaround: None available.

T23398 Recall job intermittently fails at step "Create Distributed Kafka topic for LINKS"

Recall jobs can intermittently fail at the "Create Distributed Kafka topic for LINKS" step. The job view shows a Count for Accepted and Recalled but in fact no objects are recalled.

Workaround: Start the recall job again.

T23474 Recall path incorrect with multiple cluster uses Pipeline configuration for all clusters

If multiple clusters are managed and only one is configured with the recall-source-path for pipeline, the recall-source-path is incorrectly used for the cluster that is not configured for pipeline.

Workaround: Use the recall-source-path as defined for the pipeline cluster as the recall location.

GC-652 Recall - Stats issue with multipart files

The recall stats for multipart files in pipeline jobs are consistently not counted.

Workaround: Use powerscale tools to look at the size of the recall folder.

GC-967 Long Path - Recall Metadata not applied correctly for Multipart files

Metadata recall on multipart files in long path does not work in this release.

Workaround: None

GC-1079 Recall folder stats sometimes have doubled stats/more than 100% complete stats

Folders stats and jobs view for recall job is possible to show wrong file size.

Workaround: Use the searchctl archived folders errors command to check for errors.

Manually check file size on the Powerscale may also be used to verify the recall.

GC-2378 Pipeline Recall and CBDM - job view is intermittently showing `0` recalled Bytes

Run pipeline recall job. The job view is not showing recalled files size. It is showing 0B only.

In the stats, FULL/BYTES_ARCHIVE_RECALLED is showing 0B.

In the GC UI, the job history shows the recalled files size 0B.

GC-2801 Azure Recall - Unable to Recall files inside subfolder uploaded in 1.1.19 using 1.1.20 - Possible HTTP header issues

Azure Recall - Unable to Recall files inside subfolder uploaded in 1.1.19 using 1.1.20 - Possible HTTP header issues.

Known Issues Media Mode

T23160 Failed link archive are not recorded in stats

When there is an error on copy of a link, jobs view and stats view do not have any stats related to the errors.

Workaround: If jobs view has a difference between accepted and uploaded stats this is an indication of errors. For link errors, the errors command can be used to view the errors.

T23159 Hard link percentage saved shows negative value

The jobs view Hardlinks (Size) stat may show a negative percentage saved if the size of the link object json files exceeds the size of the inode actual file.

Workaround: None required.

T22022 Error on incremental for link object with suffix

With Golden Copy configured to add an ARCHIVE_LINK_SUFFIX to links, incremental archive will result in error on delete and rename because the suffix is not applied.

Workaround: Link objects in this case should be deleted manually from object storage.

T22510 Symlink mode always set to 777

When recalling a symlink, the mode is always set to 777 instead of applying the original mode which is stored in the symlink object properties.

Workaround: The symlink object properties store the original mode which then can be applied manually.

T22488 Object storage still contains file after all hard links and original file have been deleted

If all of the hard links to and related inode file are deleted, the the file is still present in the .gcinodes folder in the object storage.

Workaround: Object can be manually deleted from the inodes folder in object storage if required.

T22484 Deleting original hard link file may result in multiple copies of the file in object storage

If a hard link has been copied to object storage and subsequently the original file is deleted, the object storage link object may now store the full original file as well as a copy of the file in the .gcnodes folder in object storage.

Workaround: Objects no longer required may be removed manually from object storage.

T23475 Error in Media Mode stops archive job

Under some circumstances for some file system configurations an error will occur when processing hard link or sym link which blocks all processing for the archive job.

Workaround: Contact support.superna.net. In some cases setting --skip-s3-file-exists to true will workaround this issue. Plan to address in patch build.

T23479 Golden Copy GUI does not report statistics for hard links / symlinks processed

The Golden Copy GUI dashboards underreport on files and bytes archived when hard links and symlinks are being processed.

Workaround: Use the jobs view CLI command to see complete statistics.

T23546 Media Mode not compatible with checksum on

Golden copy archive folder cannot be configured with checksum on when Media Mode is enabled. Hardlink and symlink json files containing the link information are not created.

Workaround: Keep default setting of checksum off when using Media Mode.

GC-544 Symlink not archived without setting ARCHIVE_LINK_SUFFIX

Without setting the ARCHIVE_LINK_SUFFIX in eca-env-common.conf, symlink json file with link information is not created in object storage when symlink processing is enabled. Only the original file is uploaded.

Workaround: Contact support.superna.net to assist in adding the export ARCHIVE_LINK_SUFFIX=.link.json to eca-env-common.conf.

GC-934 Incremental - Symlinks Rename failed possibly when using export that enables suffix

Incremental archiving of renamed symlinks does not work in this release.

Workaround: Run a full archive to re-upload the missing links.

GC-971 Long Path - Incremental Delete fail possible due to s3 error that key is too long

Incremental job with deleted files in long path are not deleted in this release.

Workaround: Delete the files in the cloud manually.

Known Issues Pipeline

T23045/T22539 Move to Trash / Delete configuration is not working

With Pipeline configured with the recall folder using `--source-path` and the corresponding settings to enable `--trash-after-recall` option, objects either downloaded successfully or skipped on recall do not get deleted or moved to recycle bucket.

With Pipeline configured with an archive folder using `--delete-from-source` and the corresponding system settings enabled, files that are successfully copied are deleted but files that are skipped are not.

Workaround: Objects/files on source must be manually removed .

T23036 No stats for Pipeline recall skipped files

The stats view or jobs view command does not report on skipped objects for Pipeline recall folder.

Workaround: None available.

T23035 Jobs view does not track delete from source progress

The jobs view command does not show any progress status for the delete operation when a folder is configured with `--delete-from-source`.

Workaround: The stats view command `FULL/FILES_DELETE_FROM_SOURCE` can be used.

T22013 Pipeline recall with the --source-path option does not apply meta-data

A Pipeline recall from object to file does not apply meta data from the object properties. Owner and Group are set to nobody.

Workaround: Set owner, group and mode manually.

Known Issues Golden Copy GUI

T23436 Golden Copy GUI folder and all time stats are inconsistent

In some cases, the Golden Copy all time stats will not match the per folder stats.

Workaround: Golden Copy stats view and jobs view can be used to view job progress.

T23150 Error on adding or editing archivefolder has no details

When there is an error on adding or editing an archivefolder the message provided is "Error occurs in graphql request" without any details as to what the actual error was.

Workaround: Browser developer tools can be used to see the details of the graphql output.

T23131 Golden Copy GUI combines Upload and Recall stats

The Golden Copy GUI shows Upload and Recall stats combined in some parts of the GUI such as the Data Processed (File Count) graph where queued stat includes both uploaded and recalled files.

Workaround: None required.

T23087 Golden Copy GUI available for Add/Edit/Delete folder for AWS, Azure and ECS

The Golden Copy GUI can only be used to manage folders for AWS, Azure and ECS. Invalid mandatory field requirement prevent management of folders for other targets.

Workaround: Use the CLI to manage folders for other targets.

T23076 No validations when editing folder from Golden Copy GUI

When editing a folder from the Golden Copy GUI there are no checks for valid input on save. Impact: invalid settings can corrupt folders and block functionality.

Workaround: Manually verify inputs for accuracy.

T22851/T23145 Golden Copy GUI Folder Management GUI Issues

When using the Golden Copy GUI to add/edit/delete folders there are the following GUI issues:

- fields are not cleared after changing cloud type selection - workaround: manually clear or overwrite previously entered values
- path field does not allow copy/paste - workaround: use path selector

- summary window does not show scrollbar - workaround: resize window

T23002 Golden Copy Cloud Browser filters not displayed

After selecting Filter Results Files or Folders in Cloud Storage Browser, the GUI does not show that a filter is applied.

Workaround: None required.

T22954 Golden Copy GUI does not correctly show Pipeline license

The license list display in the Golden Copy GUI for the Powerscale under management shows UN instead of a pipeline license.

Workaround: To double check licensing from command line use the command:
searchctl isilons list .

T22385 Golden Copy GUI shows Search product on some pages

On the login page and on some tabs once logged in the product name "search" is displayed instead of "goldencopy". No impact to functionality.

Workaround: None required.

GC-438/GC394 Unable to manage Google Cloud Storage folder from Golden Copy GUI

Unable to create or edit or clone a Google Cloud Storage folder from the Golden Copy GUI.

Workaround: Use the CLI commands for managing Google Cloud Storage folders.

GC-447 Jobs Errors does not display errors with a large number of jobs in the Jobs History

With a large number of jobs in the jobs history, the Golden Copy GUI Archive Folders -> Archive Jobs Errors list does not open. The search logo is displayed and is continuously refreshing.

Workaround: Use the CLI command to see errors related to a job.

GC-607 Cloud Browser - support self signed certificates on local targets

The cloud browser does not work to browse S3 endpoints that are hosted on SSL endpoints using untrusted SSL certificates.

Workaround: Apply a valid signed certificate to your S3 endpoint if possible, or use http instead of https.

Known Issues General & Administration

T14025 Changing PowerScale user requires a cluster down/up

If the user that was used when adding PowerScale to Golden Copy is changed, sessions still established with PowerScale using previous user.

Workaround: A cluster down/up is required to refresh user being used to connect to PowerScale. Contact support.superna.net for assistance.

T16640 searchctl schedules uses UTC time

When configuring schedule using searchctl schedules command time must be entered as UTC time.

Workaround: None required

T16855 Archived Folders for Powerscale cluster added with the --goldencopy-recall-only option does not appear in the archivedfolders list command

The searchctl archivedfolders list command does not list folders for Powerscale clusters that were added to Golden Copy using the --goldencopy-recall-only option.

Workaround: Keep a record of the folder id after adding the folder and then it can be referenced in other commands such as searchctl archived folders remove .

T17987 Alarm for cancelled job shows job failed

The description for an alarm for a cancelled job says "Job failed to run" instead of indicating that the job was cancelled.

Workaround: Check the jobs history for the details of the job.

T21073 Phone home may fail when archive folder path contains characters 'id'

Phone home may fail if there is an archive folder configured path that ends in 'id' - for example: /ifs/data/patientid

Workaround: None available.

T17200 Error on cluster up after power off/on

After power off/on of the Golden Copy VM, the cluster up might fail due to insufficient space for zk-ramdisk.

Workaround: Contact support for assistance.

T21227 Backup & Restore missing configuration

After backup and restore, the following configurations are not restored:

- searchctl archivedfolders config --checksum
- searchctl notifications (including smtp/channel)

Workaround: Keep an external record of configurations that are not restored. After restore, missing configurations must be manually reapplied.

T22337 Firewall down after node reboot

A Golden Copy node that is rebooted will no longer have the firewall rules applied.

Workaround: After bringing the node back up run the command:

```
/opt/superna/eca/scripts/eca_iptables.sh
```

Check that the firewall is up by executing the command below from another server to confirm no access to port 3000 (replace <node IP> with the IP address of the Golden Copy node that you are running the command against):

```
nc -z <node IP> 3000
```

T22373 Cannot configure admin user or group with space in name

Cannot add an AD group or user with a space in the name as an administrative user. Running the command to add the administrator group or user results in an exception.

Workaround: For an AD group, the group can be added by replacing the space in the name with %20. For example admin group@x.y would be added using admin%20group@x.y.

For AD user with a space in the name no workaround is available.

T22988 searchctl archivedfolders list --verbose incorrectly displays accesskey

In the searchctl archivedfolders list --verbose output incorrectly displays the bucket as the accesskey.

Workaround: searchctl archivedfolders list does correctly show the accesskey field.

T22957 Modify command does not change Powerscale IP address

The searchctl isilons modify command cannot be used to change the IP address Golden Copy is using to connect to Powerscale. The command will either give an error or will succeed but the original IP address will continue to be used.

Workaround: Contact support.superna.net for assistance to change IP address.

T22912 Golden Copy Advanced and Pipeline licenses cannot be removed

The Golden Copy Advanced and Pipeline licenses cannot be removed using searchctl commands. Impact: No correction can be made to loaded licenses.

Workaround: Contact support.superna.net for assistance.

T22913 Licensing of Powerscale can be lost

A sequence of operations that deletes and readds clusters may result in licenses being lost on a cluster down/up.

Workaround: Contact support.superna.net for assistance.

T23223 Golden Copy goldencopy-recall-only Powerscale cannot be licensed

A Powerscale cluster that is added to Golden Copy as a goldencopy-recall-only cluster cannot be subsequently licensed for full Golden Copy functionality.

Workaround: Contact support.superna.net for assistance.

T23382 Verbose archived folders list shows properties no longer used

The searchctl archivedfolders list --verbose property shows "recallTargetCluster" and "recallTargetPath" that are no longer used.

Workaround: None required.

GC-434 The 'recall-only' option set randomly for PowerScale

After adding a PowerScale cluster to Golden Copy, the 'recall-only' option may show as true even though it was not explicitly set. Impact: None.

Workaround: None required.

GC-426 Adding folder with '--delete-from-source' option does not accept true/false argument

An error occurs when adding a folder with the '--delete-from-source' option specified using the true argument.

Workaround: When adding the folder, to set the '--delete-from-source' option do not specify true argument or use the modify command to set the '--delete-from-source'.

GC-445 Timeout for delete where --delete-from-source is configured is too long

Current timeout to wait for a delete operation to complete is over 100 days.

Recommend to set this to 15 minutes to avoid job not completing due to a delete operation that is taking a long time.

Workaround: Contact support.superna.net for assistance to set the timeout to 15 minutes (export PIPELINE_FOLDER_DELETE_TIMEOUT 90)

GC-1119 some file uploads get errored during the upgrade.

Files may fail to archive during the cluster down/upgrade/cluster up procedure.

Workaround: Rerun the job to archive those files.

GC-1482 Azure support for certain character combination

Azure support for certain character combinations.

GC-1540 Unable to add a folder named with double quotes and back slash to GC.

Created a folder named with a **double quote and back slash** in Isilon. then I tried to add this folder to GC, but I was unable to add the folder to GC. It got an **invalid syntax error**.

GC-2233 GoldenCopy - Running a second job with skips enabled causes the job not to complete

The initial full job runs without issues and comes to completion but the second full when ran skips files until the job is canceled.

GC-2387 Incremental - Count Accepted is different than Archived possibly due File_Rename

Accepted (count) differs from Archived (count) for incremental jobs. Looking at the jobs view, there are fewer accepted than archived.

GC-2450 Backup and Restore Kafka topic's content

Summary of what is not restored after a backup and Restore as of 1.1.17-23170 v15, single node:

- checksum: Expected to be restored. Need to be fixed.
 - Kafka topics' content. This is expected; no fix is planned. Impact: Tools that rely on data from Kafka topics will show empty results. Example tools:
 - system alarms/notifications (searchctl notifications list).
 - job error details (searchctl archivedfolders errors).
-

GC-2485 customMetadata 100k characters limit Error

When full archiving using `--customMetadata True` , some files ran into error.

GC-2692 Large Changelists Max Out Isilongateway RAM

Multiple large change lists from incremental jobs will cause the Isilongateway container to restart.

Workaround: Spread incremental schedules out to allow more time in between the incremental jobs, check the change list on OneFS, and if over 1M changes are being found, run a full job on the folder instead of an incremental job.

GC-2631 Single node has errors about multiple zk nodes

Single node has errors about multiple zk nodes.

Note: the workaround needs to be applied to any newly deployed single node GC ovf

Workaround:

Add the above zookeeper section to `docker-compose.override.yml` and for node 2 and node 3 turn off the label.

```
eca.cluster.launch.node2: off
```

```
eca.cluster.launch.node3: off
```

GC-3012 UI - Unable to add AWS `us-east-1` archivedfolders

Unable to add archivedfolders in the UI when using `us-east-1`

Workaround: Adding using a different region and CLI.

DEVSECOPS-258 `libzyp`/`rpm` bug causes installers to fail

libzypp version 17.31.22 introduces an incompatibility with the currently available version of rpm (4.14.3 at the time of writing). The following error occurs when the installer attempts to install the RPMs:

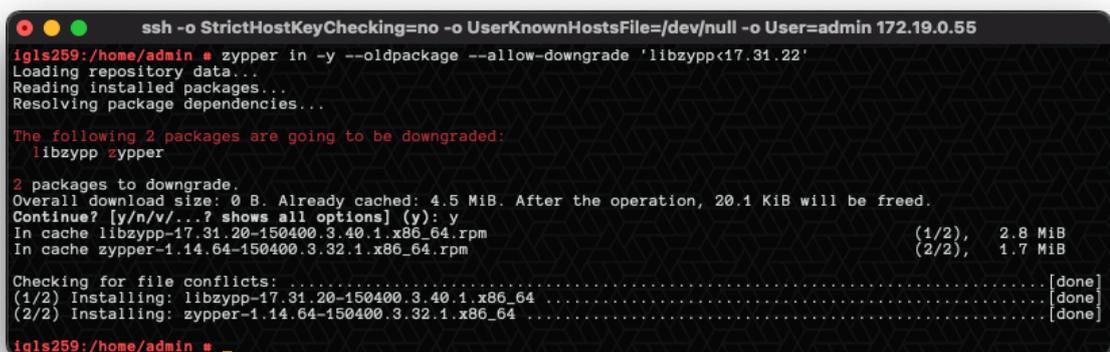
```
error: Macro %_dump_postrans has empty body
```

```
error]
```

Workaround: libzypp must be downgraded and locked to prevent the broken from being installed either manually or by the Yast2 Auto Update process:

```
sudo zypper in -y --oldpackage --allow-downgrade 'libzypp<17.31.22'
```

```
sudo zypper addlock 'libzypp<17.31.22'
```



```
ssh -o StrictHostKeyChecking=no -o UserKnownHostsFile=/dev/null -o User=admin 172.19.0.55
igls259:/home/admin # zypper in -y --oldpackage --allow-downgrade 'libzypp<17.31.22'
Loading repository data...
Reading installed packages...
Resolving package dependencies...

The following 2 packages are going to be downgraded:
 libzypp zypper

2 packages to downgrade.
Overall download size: 0 B. Already cached: 4.5 MiB. After the operation, 20.1 KiB will be freed.
Continue? [y/n/v/...? shows all options] (y): y
In cache libzypp-17.31.20-150400.3.40.1.x86_64.rpm (1/2), 2.8 MiB
In cache zypper-1.14.64-150400.3.32.1.x86_64.rpm (2/2), 1.7 MiB

Checking for file conflicts: ..... [done]
(1/2) Installing: libzypp-17.31.20-150400.3.40.1.x86_64 ..... [done]
(2/2) Installing: zypper-1.14.64-150400.3.32.1.x86_64 ..... [done]

igls259:/home/admin # _
```

Known Limitations

T15251 Upload from snapshot requires snapshot to be in Golden Copy Inventory

Golden Copy upload from an PowerScale snapshot requires snapshot to be in Golden Copy Inventory. Inventory task is run once a day. If you attempt to start archive without snapshot in inventory you will get error message "Incorrect snapshot provided".

Workaround: Wait for scheduled inventory to run or run inventory manually using command: searchctl PowerScales runinventory

T15752 Cancel Job does not clear cached files for processing

Any files that were already cached for archive will still be archived once a job has been cancelled.

Workaround: None required. Once cached files are processed there is no further processing.

T16429 Golden Copy Archiving rate fluctuates

Golden Copy archiving rates may fluctuate over the course of an upload or recall job.

Workaround: None required.

T16628 Upgrade to 1.1.3 may result in second copy of files uploaded for Azure

In the Golden Copy 1.1.3 release, upload to Azure replaced any special characters in the cluster, file or folder names with "_". In 1.1.4 release the special characters are handled so that a subsequent upload in 1.1.4 will re-upload any files/folders because the names are not identical in S3 to what was uploaded in 1.1.3. If the cluster name contained a special character - for example lsilon-1 - then all files will be re-uploaded.

Workaround: None

HTML report cannot be exported twice for the same job

The HTML report cannot be run again after having been previously executed.

Workaround: None required. Use the previously exported report.

T16250 AWS accelerated mode is not supported

Golden Copy does not support adding AWS with accelerated mode as an S3 target.

T16646 Golden Copy Job status

When viewing the status of a Golden Copy Job it is possible that a job which has a status of SUCCESS contains errors in processing files. The job status is used to indicate the whether the job was able to run successfully. Then the searchctl jobs view or searchctl stats view or HTML report should be used to determine the details related to the execution of the job including errors and successes.

T17173 Debug logging disk space management

If debug logging is enable, the additional disk space consumed must be managed manually.

T18640 searchctl archivedfolders errors supported output limit

The searchctl archivedfolders errors command support output limit is 1000.

Workaround: For a longer list use the --tail --count 1000 or --head --count 1000 option to limit the display.

GC-1504 Parallel jobs limited to 10 at a time

If more than 10 are submitted to run (manual, scheduled), the rest will eventually run as well/queued. **GC-1626 Links Bytes Accepted and Archived look different**

Symlink (Size) does not look consistent for found and uploaded.

GC-1527 Cloud Browser - Single File Download - Support for downloading symlinks that points to a hardlink

Summary Single File Download support for Links (hard and sym):

- Single file download of a symlink downloads the file it is linking to if it exists on the bucket. Tested Ok.
 - Single file download of hardlink file (json+inode) tested Ok. Tested with a single and multipart file.
-

GC-1625 Incremental Delete not working for deleted Symlink possibly due to suffix

Symlink that was deleted was not deleted after incremental possibly to using suffix export.

GC-2292 '--follow' option for rerun has an exception error

Using --follow flag immediately after running a rerun job causes error. Wait some time for the job to register and try again.

GC-2789 3 Nodes : Folder stats empty `searchctl stats view --folder <folderID>` and `searchctl archivedfolder stats --id <folderID>`

In some environments (noticed on HyperV test env) with lots of latency, users unable to retrieve stats using `searchctl archivedfolders stats --id` or `searchctl stats view --folder`.

GC-2804 Phonehome Logs Upload Issue on HyperV OVF 3-Node

After successfully sending a heartbeat on Phonehome, the 'logsupload' command appears to be broken.

GC-3008 Short parallel archive jobs showing 0 stats intermittently

For short jobs, especially the ones that run in parallel, there is a possibility that the stats are still not collected before those jobs are marked as Done. The impact is that the stats (such as for Accepted and Archived) could be lost with varying severity (mostly 0, some stats are missing, and so on).

Fast Incremental Known Limitations

- mode bit metadata information is not available in fast incremental mode
- owner and group are stored in numeric UID and GID format in the object header
- PowerScale API only available for OneFS 8.2.1 and higher

- Owner and Group meta-data are not recalled where objects were uploaded with fast incremental due to a bug in PowerScale API they cannot be recalled. Recall should be done without meta-data. There may still be meta-data errors on recall without meta-data, which can be ignored.
-

Move/Rename identification and management in object storage known limitations

- PowerScale API only available for OneFS 8.2.1 and higher for updating S3 target with new location of folder and files and removing folder and files from old location
 - For OneFS version lower than 8.2.1 move/rename objects cannot be identified due to PowerScale API issue and these will be orphaned in S3 target.
-

Backblaze target requires https access

When configuring folder for Backblaze https access must be used, http is not supported.

T20868 Cannot run incremental update for same folder to multiple targets

If incremental update for same folder is run in parallel to multiple targets, only 1 incremental job will run. This impacts incremental update only, parallel full archive for the folder to multiple targets does not have this issue and both complete successfully.

T21258 Version based recall uses UTC time for inputs

When specifying the --newer-than or --older-than options for version based recall, UTC time must be used.

T21759 Unable to export recall job multiple times

After an export of a recall job, the same job cannot be exported again.

Workaround: None available.

T21925 Export reporting limit

When running an export report to view errors or files uploaded, the number of records reported on is limited to 7 million records.

Workaround: Contact support.superna.net if you require reporting on more records. For overall reporting on a job use the Golden Copy GUI or CLI jobs view command.

T22680 Media Mode Hardlink mode may copy more than 1 copy of the file

For the case where there are multiple hardlinks to the same file, due to parallel processing there may be multiple instances of the the real file uploaded until the completion of the copy of the real file is known to all Golden Copy nodes.

Workaround: None available. For a large number of hardlinks to the same file, the duplicate files uploaded is expected to be far less than a very large number of links.

T22469 Media mode does not copy broken symbolic links

A symbolic link that is broken for example due to a renamed or deleted file is not uploaded by Golden Copy.

Workaround: None available.

T22630 Media mode may orphan hardlink objects when all Golden Copy nodes are not able to archive

In the event that a multi-node Golden Copy deployment has nodes that are not able to copy for any reason, it may result in either orphaned inode objects or associated hard link objects due to copy for the partner object being assigned to the node that cannot copy.

Workaround: None available

T23130 Media mode has no stats for broken symlink

If there are broken symlinks encountered during a Golden Copy job, there are no statistics to track this occurrence.

Workaround: None available

GC-433 PowerScale may return success for recalled file even if PowerScale blocks saving the file

In some cases PowerScale has an issue where it returns a success message for a recalled file even though a on the recall directory on the PowerScale has blocked the save of the file.

Impact:

- recall statistics may incorrectly show success for files that are not actually saved on the filesystem
 - Pipeline 'trash-after-recall' option will delete the object due to success message from PowerScale even though the object has not been successfully recalled.
-

GC-459 Recall error for multi-part file leaves incomplete file on file system

For the case where a multi-part recall fails, the error in recalling the file is properly tracked in the statistics and in the errors command, but the partial incomplete file is left behind on the filesystem.

Impact: If configured to skip recall for files already downloaded this may result in a skipped file.

Workaround: Use error command to determine errored files and remove them manually from the filesystem.

GC-450 Golden Copy - Traceback on cluster up

On cluster up, an error and associated stack trace is printed to the console. This error is benign and can be ignored.

Workaround: none needed.

GC-446 Stats conversion from bytes incorrect

Download Single File from Wasabi Cloud Type, in design says only us-east-1 region is supported.

GC-874 Audit - Job is stalled after hitting exactly 50k files

The goldencopy audit job is limited to 50,000 records. Selecting more will cause the job to hang.

Workaround: select less than 50,000 records.

GC-938 Incremental - Only the original hardlink is updated possibly due to changelist limitation

The timestamp on the "other" link object isn't updated. But the metadata is stored on the inode itself, so the correct metadata is applied on a recall.

GC-1020 Cloud Browser - Unable to download file from Wasabi

Cloud browser single file download is not supported for Wasabi cloud type.

GC-1308 Increase/Customize/Remove the 1000 error limit

1. Login to Web UI.
 2. Go to Tab **Archive Jobs**
 3. Scroll down to **Archive Jobs Errors** you will see a list of **archivedfolders**
 4. If you click one it will list the errors.
 5. The limitation: It can only display the last **1000** errors of any job on that archived folder.
-

Cloud Browser for Data Mobility

Known Issues Cloud Browser for Data Mobility

CBDM-168 Wasabi - Unable to add archivedfolders from CLI without using https://

Wasabi used to be able to be added without using the https prefix. Now it's crashing with `String index out of range: -1`

CBDM-171 CBDM Browser - List limited to 1000 objects and possibly blocking access to lower 'paths'

GC-412 Archive job does not handle a block "b" special file

If the archive folder contains block "b" type special files, the archive job will encounter an exception when processing this file.

CBDM-512 CSV Export - Special characters probably causing the columns not being populated correctly

Special characters cause the columns not being populated correctly. Using build 1.1.16-23119 multinode v15.4, AWS, Ofs9501

CBDM-322 Cloud to Premise - Recall phase is not skipping existing files

Ran the same Copy to Premise Copy job twice with export set to skip files on recall, the second Copy job overwrote all files instead of skipping. Using build 1.1.14-23048 v15.4, AWS, OneFS9.4.0.12

CBDM-502 Cloud to Premise - the staged files should be delete from the bucket even without the recyclebucket

When I run CBDM job, the staged objects are not deleted without the recyclebucket. But the staged files should be deleted from the bucket even without the recyclebucket.

It doesn't work, and trash-after-recall still needs a recycle bucket.

CBDM-503 Unable to modify to remove recyclebucket from the folder

It's not able to modify archivedfolder with trash-after-recall option from with trashbucket or recycle bucket to without trashbucket or recycle bucket through Ui or CLI.

CBDM-383 Cloud to Premise - Stats differences between Staging and Recall

After selecting 2 individual files, Staging looks Ok, but the Recall stats are always higher. And there is also always a Skip stat even though skipping is not possible due to the SA collision feature. Using build 1.1.15-23069 (6 nodes) v15.4, AWS, OneFS9.5.0.1.

CBDM-390 Cloud to Premise - Run Copy/move job with unchecked the "Email on job completion" , then should not get an email for that job.

When running Copy/move CBDM job with unchecked the "Email on job completion", even I received an email for that job. Unchecked the "Email on job completion" for Move/Copy CBDM jobs. After the job is done, Emails are sent anyway. The expected result is if we will run copy/move job with unchecked "Email on job completion", then we should not get an email for that job.

CBDM-227 Block adding email recipient if no channel

Block adding email recipient if no channel

GC-2410 Recall - Errors from DENY (to download) bucket policy being counted as Skips

A file failed to download due to a bucket policy that denies the download of certain file types. The following error is counted as a Skip, which looks to be that all indexworker-related errors on the object will be counted as a Skip. Impact: Other than the skips, **no errors are recorded**.

CBDM-692 CBDM Job Fails When Selecting Entire Bucket

The CBDM job encounters a failure when attempting to process the entire bucket at once. Selecting the complete bucket on job execution.

Workaround: Select objects individually inside the bucket instead of selecting the entire bucket.

CBDM-693 Staging Path Not Cleared on Skipped Job: Pending Issue Resolution

Staging Path Not Cleared on Skipped Job: Pending Issue Resolution.

Workaround: None.

CBDM-753 Pinned archiveworker nodes intermittently not assigned to Kafka consumer group `archiveworker`

Pinned archiveworker nodes intermittently not assigned to Kafka consumer group `archiveworker`.

Workaround: Restarting archiveworker/cluster down and up.

CBDM-744 1/4 parallel jobs failed at Staging due to trying to create `-CBDM` topics

1/4 parallel jobs failed at Staging due to trying to create `-CBDM` topics.

Workaround: Run 1 CBDM job initially to make sure the -CBDM topics are created. Subsequent jobs will then skip creating the topics and not run into this issue.

CBDM-761 Round-robin and Pinned archiveworkers behaviour in parallel jobs

When there are more jobs than pipelines, multiple jobs will share the same pipeline. Also, all the parallel jobs sharing a pipeline will need to finish their Copy/Move job steps before they can be marked as finished. Note that email notifications also share this behaviour.

Workaround: Add more pipelines to avoid parallel jobs sharing the same pipeline.

Known Limitations Cloud Browser for Data Mobility

CBDM-407 Parallel CBDM jobs stats seems to be incorrect

All parallel jobs or all jobs that happen to be running when others are running will finish at the same time regardless on the amount of data being copied/moved. This applies to multiple jobs run by the same user or multiple users.

CBDM-543 Cloud to Premise - Stats for Move step

As a CBDM user, I want to closely track CCloud to Premise jobs for stats, including success, skip, and errors. Specifically when CBDM is Moving files from the recall source path to the SMB share target.

CBDM-631 Parallel Job - Error `Fail to lock` when the same user downloads the same data into the same Target

Seeing file lock error when **1 user** is running **2 Parallel** jobs Copying the **Same Data** to the **Same Target**. All files downloaded Ok for this test.

CBDM-777 Staging cannot use s3 keys that are over the AWS S3 key limit (1024 bytes)

Staging may fail if the combination of the CBDM prefix which includes the full path of the target SMB share and the existing s3keys of the copied objects, exceeds the AWS s3key limit of 1024 bytes.

© Superna Inc

1.13. Current Release - Release Notes - Golden Copy Archive Engine

[Home Top](#)

Release Date	Version
12/14/2023	1.1.21-23252

- [New in Superna Archive Engine Release 1.1.21](#)
- [New in 1.1.21](#)
- [Fixed in 1.1.21](#)
 - [SA-1567 Policy based archiving appends extra string to the Powerscale prefix inside bucket](#)
 - [SA-1554 Recall staging/restore from `DEEP_ARCHIVE` shows `0` stats, including with email](#)
 - [SA-1377 Not able to recall from deep_archive when Redis is set](#)
- [New in 1.1.20](#)
- [New configurations/environment variables in 1.1.20](#)
- [Fixed in 1.1.20](#)
 - [SA-1472 Unable to modify the recall schedule](#)
 - [SA-1202 CB only lists folders for 1 cluster](#)
- [New in Superna Archive Engine Release 1.1.19\(09.01.2023\)](#)
- [New in 1.1.19-23189](#)
- [Fixed in 1.1.19-23189](#)
 - [SA-389 Plus sign-in path causes issues with SA archive](#)
 - [SA-1208 Staged For Recall inconsistent listing of folders](#)
- [New in Superna Archive Engine Release 1.1.17 \(07/27/2023\)](#)
- [Fixed in 1.1.17](#)
 - [SA-508 smart-archiver-sourcepaths parameter do not accept comma character](#)
- [New in Superna Archive Engine Release 1.1.16\(06/07/2023\)](#)
- [Fixed in 1.1.16](#)

- SA-875 Isilon Management GUI incorrect display for licenses
- SA-365 Not able to recall if the upload bucket and recall bucket use different access credentials
- SA-946 archive folder path is not cleared after archived completed
- SA-966 User can access share with Deny all permission
- New in Superna Archive Engine Release 1.1.15 (05/03/2023)
- Fixed in 1.1.15
 - SA-60 Archive job cannot finish when there is no data in staging area
 - SA-831 Error rerun pipeline recall job
 - SA-825 importconfig fails to restore SA folder
 - SA-658 Searchbar in SA and Cloud Browser page fails when "\" character is used instead of "/"
 - SA-325 not able to rerun failed pipeline recall job
 - SA-794 Fail to apply metadata error when subdir is skipped for recall
- Supported OneFS releases
- End of Life Notifications
- Technical Advisories
- New in Superna Archive Engine Release 1.1.14 (04/04/2023)
 - Fixed in 1.1.14
 - SA-354 folder object is recalled when recall source path is at the same level
 - SA-773Restore Pipeline Recall job shows "Staged" twice
 - SA-775 folder stats has wrong FULL/DEEP_RESTORED and FULL/DEEP_RESTORE_ACCEPTED
 - SA-848 Restore accepted stats not incrementing
 - SA-246 AD user share paths listing graphql error
- Known Issues
 - SA-363 Safari support for single file download
 - SA-364 Unable to navigate to lower folders when recall folder is not configured

- SA-688 Cloud Browser - graphql error when browsing certain path - DataFetchingException Unclosed character class
- SA-59 Archive folder to work with include/exclude options
- SA-361 Non-alphanumeric character support
- SA-889 SA source paths should be allowed at the same path as a recall folder source path
- SA-1037 archivereport topic not created when running policy walk
- SA-1065 files not in the path listed in smartarchiver meta object are recalled and cleaned up from recall bucket
- SA-1048 Archives only list paths for 1 folder when multiple upload folders are added to the same recall folder
- SA-1070 Blank screen when 'Configured Only' is selected
- SA-1404 GCAE with symlinks and hardlinks
- SA-1016 DEV: Active Jobs GUI to include policy job stats
- SA-1594 Azure restore indicator in Cloud Browser causes a blank screen
- SA-1659 Metadata error when customMetaData is set to true
- SA-1664 Edit AE folders for GCS
- SA-1676 Remove tier for ECS folder in Pipeline config
- SA-1677 The cancelled dry run job needs cleanup
- Known Issues Recall
 - SA-388 Not able to recall if SA archive bucket and recall bucket are in a different region
 - SA-385 add "GoldenCopy Pipeline Recall" job type in GUI
 - SA-382 recall job creates report under full category
 - SA-349 show all staged folders in 'Staged for Recall'
 - SA-324 wrong bucket name in pipeline recall error message
 - SA-792 Recall from Azure archive storage
 - SA-1207 Fail to apply ACL to recalled file with UTF-8 character in the file name
 - SA-566 Language-specific character is replaced with '?'

- [SA-1637 Recall job shows inaccurate stats](#)
- [SA-1639 No archiveengine object is created after the folder is staged for recall](#)
- [Known Limitations](#)
 - [SA-116 Clouds deep archive recall support](#)
 - [SA-942 Pipeline Configuration wizard create folder fails](#)

New in Superna Archive Engine Release 1.1.21

New in 1.1.21

Azure Deep Archive (Or Equivalent) Support

Restore from deep_archive skips now for existing files.

Dry run to calculate the amount of data to be archived before the job is run

The GUI enables users to initiate dry archive runs, giving them a preview of the potential impact of the archive job without actual execution.

Fixed in 1.1.21

SA-1567 Policy based archiving appends extra string to the Powerscale prefix inside bucket

Uploaded data key is incorrect due to issue that occurs when GCAE source path/policy path shares a common parent folder and is similarly named to GCAE upload folder's path. For example, GCAE upload folder path = /ifs/data/folder & archive policy path = /ifs/data/folderPolicies.

SA-1554 Recall staging/restore from `DEEP_ARCHIVE` shows `0` stats, including with email

Recall staging/restore from `DEEP_ARCHIVE` shows 0 stats, including with email.

SA-1377 Not able to recall from deep_archive when Redis is set

Not able to recall from deep_archive when Redis is set

Workaround: add “`export REDIS_PATH_CACHE_FOR_FILES=false`” to `/opt/superna/eca/eca-env-common.conf`

What's New in Superna Archive Engine Release 1.1.20(10/05/2023)

New in 1.1.20

User Driven Archive and Recall notification email

1. The notification email addresses of users are gathered by capturing their email during the user's first login.
2. Email notifications containing details regarding the outcome of the GCAE upload and recall jobs were added.

New configurations/environment variables in 1.1.20

`docker-compose.yml`

- `ERROR_RATE_THRESHOLD_PERCENTAGE`
 - Set in `eca-env-common` to override the default

- added to allow setting the threshold at which the error rate becomes high in the jobs view. 10% is the default - meaning ≤ 10 is considered 'Low Error Rate' and < 10 is considered
- `ECA_ENABLE_PATH_CACHE_ARCHIVWORKER`
 - Set in `eca-env-common` to override the default and to ENABLE
 - This allows caching finished work in archiveworker in order to avoid re-working uncommitted events in the case of an archiveworker restart

Fixed in 1.1.20

SA-1472 Unable to modify the recall schedule

Update recall folder schedule and get the error: Exception while fetching data (/updateArchivedFolder): No value present.

Workaround: Use GUI to edit folder recall schedule.

SA-1202 CB only lists folders for 1 cluster

CB only lists folders for 1 cluster

New in Superna Archive Engine Release

1.1.19(09.01.2023)

New in 1.1.19-23189

1. Dry Run functionality was added.

Fixed in 1.1.19-23189

SA-389 Plus sign-in path causes issues with SA archive

Having plus signs in either staging folder paths or Archive Engine source paths causes content to the archive with an incorrect key.

Workaround: Change names of paths not to include plus signs.

SA-1208 Staged For Recall inconsistent listing of folders

Staged For Recall inconsistent listing of folders

New in Superna Archive Engine Release 1.1.17 (07/27/2023)

Fixed in 1.1.17

SA-508 smart-archiver-sourcepaths parameter do not accept comma character

When the user tries to add different smart archiver sourcepaths with comma, the process to store them is separating that informed paths by comma character so, the configuration of that paths is wrong

New in Superna Archive Engine Release 1.1.16(06/07/2023)

Fixed in 1.1.16

SA-875 Isilon Management GUI incorrect display for licenses

Isilon Management GUI incorrect display for licenses

SA-365 Not able to recall if the upload bucket and recall bucket use different access credentials

Not able to recall if the upload bucket and recall bucket use different access credentials.
Workaround: None.

SA-946 archive folder path is not cleared after archived completed

After folder is successfully uploaded, the staging path is not cleared. all files are deleted but folders stay

SA-966 User can access share with Deny all permission

User can access share with Deny all permission

New in Superna Archive Engine Release 1.1.15 (05/03/2023)

Fixed in 1.1.15

SA-60 Archive job cannot finish when there is no data in staging area

archive job cannot finish when there is no data in staging area

SA-831 Error rerun pipeline recall job

error rerun pipeline recall job

SA-825 importconfig fails to restore SA folder

Import config failed for SA archive folder due to recall folder is not restored first

SA-658 Searchbar in SA and Cloud Browser page fails when "\" character is used instead of "/"

When searching a path on the Smart Archiver page or Cloud Browser page, The "/" and "\" characters should be both accepted and interpreted as "/" in either case, but when "\" is passed an error is thrown from the back end.

SA-325 not able to rerun failed pipeline recall job

Re-running failed Archive Engine recall staging jobs does not work.

Workaround: Run a new recall staging job to rerun.

SA-794 Fail to apply metadata error when subdir is skipped for recall

Fail to apply metadata error when subdir is skipped for recall.

What's New! In Superna Archive Engine can be found [here](#).

Supported OneFS releases

8.2.x.x

9.1.x.x

9.2.x.x

9.3.x.x

9.4 via the February RUP 9.4.0.12 (PSP-3079) released Feb 8th 2023

9.5.0.1

End of Life Notifications

End of Life Notifications for all products are available [here](#).

Technical Advisories

Technical Advisories for all products are available [here](#).

New in Superna Archive Engine Release 1.1.14 (04/04/2023)

Fixed in 1.1.14

SA-354 folder object is recalled when recall source path is at the same level

Archive folder and recall folder have sourcepath at the same level

SA-773 Restore Pipeline Recall job shows "Staged" twice

Pipeline recall from deep-archive, job view shows "Staged:" entry twice

SA-775 folder stats has wrong FULL/DEEP_RESTORED and FULL/DEEP_RESTORE_ACCEPTED

folder stats has wrong FULL/DEEP_RESTORED and FULL/DEEP_RESTORE_ACCEPTED

SA-848 Restore accepted stats not incrementing

The stats for when objects are accepted to be restore are not incrementing.

SA-246 AD user share paths listing graphql error

Giving access to an NFS share that is below the path of another share to a single user can cause errors while navigating the Archive Engine page.

Workaround: Give user access to only the highest of the paths.

Known Issues

SA-363 Safari support for single file download

Single file download is not supported on Safari.

Workaround: None.

SA-364 Unable to navigate to lower folders when recall folder is not configured

Both Archive Engine folders are required to be configured, or GUI has issues loading results for Active Directory users.

Workaround: Make sure both the staging folder and recall folder are configured.

SA-688 Cloud Browser - graphql error when browsing certain path - DataFetchingException Unclosed character class

Unable to browse AWS paths with certain (combination) of non-alphanumeric characters.

SA-59 Archive folder to work with include/exclude options

archive folder to work with include/exclude options

SA-361 Non-alphanumeric character support

test folder and file name with white space and special characters

SA-889 SA source paths should be allowed at the same path as a recall folder source path

The recall button should only allow actions on folders below the SA sourcepath and not the SA sourcepath itself.

Workaround: do not recall from the same level as the recall folder's sourcepath

SA-1037 archivereport topic not created when running policy walk

When an archive job is run where a policy walk step is included, if the archivereport-
<folder id> topic does not already exist, it will not be created until after the policy walk is
done. The policy walk will succeed but it will take a very long time as each event waits
for the archivereport event submission to time out.

Workaround:

Any archived folder that has been given policies should at least begin an archive job
before running an archive job with policies. This can be done by either running the
archive job before adding the policies, or by pausing all the policies linked then running
an archive job. After an archive job has been run, this issue will not occur as long as the
topics aren't deleted.

SA-1065 files not in the path listed in smartarchiver meta object are recalled and cleaned up from recall bucket

Users should not use GCAE staging bucket for non-GCAE data. These will be recalled
and removed from the staging bucket during a GCAE recall

SA-1048 Archives only list paths for 1 folder when multiple upload folders are added to the same recall folder

Archives only list paths for 1 folder when multiple upload folders are added to the same
recall folder

SA-1070 Blank screen when 'Configured Only' is selected

Blank screen when 'Configured Only' is selected

SA-1404 GCAE with symlinks and hardlinks

Symlinks are not archived, hardlinks are treated as individual files.

SA-1016 DEV: Active Jobs GUI to include policy job stats

Run archive job with SA policies enabled; Archive Running Jobs/ Archive History Jobs in Active Job currently does not include any policy-related stats.

p.s. Archived stats do include all archived folders and files.no

SA-1594 Azure restore indicator in Cloud Browser causes a blank screen

1. mouse pointer hovers restore indication in CB, and the application goes blank
 2. restore indicator for the restored AWS object is no longer showing restored status and also gives a blank screen when moving the mouse over it
-

SA-1659 Metadata error when customMetaData is set to true

Metadata error when customMetaData is set to true

SA-1664 Edit AE folders for GCS

Not able to add/edit Archive Engine folders for GCS storage using GUI

Workaround: use CLI for adding/editing Archive Engine folders for GCS storage

SA-1676 Remove tier for ECS folder in Pipeline config

The pipeline config wizard requires input for the tier field when editing the Archive Engine folder to ECS storage

Workaround: either use CLI for editing or enter a space for the tier field

SA-1677 The cancelled dry run job needs cleanup

Sometimes, a cancelled dry run job can still hinder the next archive/recall action.

Workaround: if errors persist in indexworker log, perform a cluster down/up.

Known Issues Recall

SA-388 Not able to recall if SA archive bucket and recall bucket are in a different region

Archive Engine recall will fail if the main bucket and recall staging bucket are in different regions.

SA-385 add “GoldenCopy Pipeline Recall” job type in GUI

Unable to use the filter by job type for “GoldenCopy Pipeline Recall” job type.

SA-382 recall job creates report under full category

Archive Engine recall job report is generated under full instead of recall.

Workaround: Find Archive Engine recall job report under full.

SA-349 show all staged folders in 'Staged for Recall'

Having multiple Archive Engine configurations may make some objects staged for recall not show on UI. This has no effect on the recall process and is purely an issue with the display.

SA-324 wrong bucket name in pipeline recall error message

Error message for failed Archive Engine recall job shows main archive bucket name instead of recall staging bucket name.

SA-792 Recall from Azure archive storage

Recall from Azure Archive storage tier is not supported.

SA-1207 Fail to apply ACL to recalled file with UTF-8 character in the file name

Fail to apply ACL to recalled file with UTF-8 character in the file name

SA-566 Language-specific character is replaced with '?'

Language-specific character is replaced with '?'

SA-1637 Recall job shows inaccurate stats

Recall job shows inaccurate stats

SA-1639 No archiveengine object is created after the folder is staged for recall

No archiveengine object is created after the folder is staged for recall

Known Limitations

SA-116 Clouds deep archive recall support

Archive Engine cannot recall on content with deep archive tiers.

SA-942 Pipeline Configuration wizard create folder fails

Pipeline Configuration wizard create folder fails

© Superna Inc

1.14. Current Release - Release Notes AnyCopy

[Home](#) [Top](#)

- [Supported OneFS releases](#)
- [Supported Eyeglass releases](#)
- [Inter Release Functional Compatibility](#)
- [End of Life Notifications](#)
- [Technical Advisories](#)
- [Fixed in 2.5.8](#)
- [Fixed in 2.5.8.1-22100](#)
- [Fixed in 2.5.8.1-22080](#)
- [Fixed in 2.5.8-22028](#)
- [Fixed in 2.5.8-21330](#)
 - [T22171 - Log4j Vulnerability - Upgrade to Log4j 2.17.0 \(2.5.8-21330 and higher Log4j 2.17.0 \)](#)
- [Fixed in 2.5.8-21306](#)
 - [T22033 Log4j Vulnerability - CVE-2021-44228](#)
- [AnyCopy Job Issues](#)
 - [T18236 AnyCopy Job Not saved](#)
- [Copy Configuration Issues](#)
 - [T15080 Copy Configuration Issue for Multi Path NFS Export](#)
 - [T18282 Copy Configuration Step always fails for NFS Export when rerunning an AnyCopy Job](#)
 - [T18295 Copy Configuration Step fails for rerun Job](#)
 - [T18296 Copy Configuration step fails if overlaps with DR Inventory Task](#)
 - [T19067 AnyCopy Job in Warning does not have an entry in Run History](#)
 - [T18737 AnyCopy Job will not be saved if Notify Progress not selected](#)
 - [T16482 Isilon Shares Path Selector allows entry of invalid path](#)
 - [T16511 AnyCopy Jobs disappear after rediscover](#)
 - [T17471 Allow Scheduling Option not available](#)
 - [T18254 Isilon Shares Path Selector allows selection of FQDN](#)

- [T18273 AnyCopy Job Name format not validated](#)
- [T18375 "Block access to source data to all users during copy" option is not available](#)
- [T18385 Issues when same AnyCopy Job started at same time by multiple users](#)
- [T17220 Policy Job Summary Report UNC path has incorrect format](#)
- **Known Limitations**
 - [Please review the Limitations documented here.](#)
 - [T18277 Transient AnyCopy Job in the Jobs window](#)
 - [T18278 Copy Configuration Error for AnyCopy Job for same cluster and same access zone for source and target path](#)

What's New for AnyCopy

What's New in this AnyCopy release can be found [here](#).

Supported OneFS releases

Source cluster

8.2.1.0 and higher 8.2 versions

Target cluster

8.2.1.0 and higher 8.2 versions

Supported Eyeglass releases

Eyeglass 2.5.8 - please refer to release list [here](#)

Inter Release Functional Compatibility

	Source	Target
--	--------	--------

End of Life Notifications

End of Life Notifications are published [here](#).

Technical Advisories

Technical Advisories for all products are available [here](#).

Fixed in 2.5.8

Fixed in 2.5.8.1-22100

Refer to previous 2.5.8.1 builds.

Fixed in 2.5.8.1-22080

Refer to previous 2.5.8 builds.

Fixed in 2.5.8-22028

Refer to previous 2.5.8 builds.

Fixed in 2.5.8-21330

T22171 - Log4j Vulnerability - Upgrade to Log4j 2.17.0
(2.5.8-21330 and higher Log4j 2.17.0)

Fixed in 2.5.8-21306

T22033 Log4j Vulnerability - CVE-2021-44228

Resolution: log4j version updated to 2.15.0 which has patch for the vulnerability.

Known Issues

AnyCopy Job Issues

T18236 AnyCopy Job Not saved

Under some conditions where the final step of the AnyCopy job fails, there is no record of the job saved or available for review.

Workaround: Try the AnyCopy job again and if the problem persists contact support.superna.net for assistance.

Copy Configuration Issues

T15080 Copy Configuration Issue for Multi Path NFS

Export

Where Copy Configuration step is copying a multi path NFS Export to a different Access Zone on the target cluster, only the first path is adjusted for the new Access Zone path. Remaining path are added with source cluster Access Zone path.

Workaround: Manually update the remaining paths for the NFS Export using PowerScale GUI or CLI.

T18282 Copy Configuration Step always fails for NFS

Export when rerunning an AnyCopy Job

When rerunning an AnyCopy job where configuration includes NFS Exports, a create request is issued instead of an update request for existing NFS Exports resulting in

AEC_EXCEPTION that indicates there is a conflict due to the fact that the export already exists.

Workaround: None Available. If an update is required it will need to be applied manually using PowerScale interface to update the NFS Export.

T18295 Copy Configuration Step fails for rerun Job

If a Copy job is completed and SynclQ policy is deleted, rerun of the Job successfully recreates the SynclQ policy but the Copy Configuration step fails.

Workaround: Configuration from original job completion is in place. Any changes need to be applied manually using Powerscale tools on the target.

T18296 Copy Configuration step fails if overlaps with DR Inventory Task

If a Copy Configuration step timing overlaps with the DR Inventory task, the Copy Configuration step will fail.

Workaround: Check the Jobs / Running Jobs window to see whether DR Inventory Task is in running state. Consult with support.superna.net whether the DR Inventory Task schedule could be changed to reduce conflict.

T19067 AnyCopy Job in Warning does not have an entry in Run History

An AnyCopy Job that ends in Warning state (for example if the step to create the file report fails to create required snapshot) is missing entry in the Run History.

Workaround: If the SynclQ job was preserved, the last run for the job can be verified from the Powerscale native interface.

T18737 AnyCopy Job will not be saved if Notify Progress not selected

The configured AnyCopy Job will run but will not be saved and available in the job history if Notify Progress option is not selected.

Workaround: Select the Notify Progress option for all jobs.

General/Administration Issues

T16482 Isilon Shares Path Selector allows entry of invalid path

The Isilon Shares Path Selector does not validate whether path entered is valid and will accept an invalid path.

Workaround: Use the tree to select the path to ensure it is valid.

T16511 AnyCopy Jobs disappear after rediscover

If rediscover command is used to rebuild the Eyeglass database, existing AnyCopy jobs are gone.

Workaround: Contact support.superna.net before running this command.

T17471 Allow Scheduling Option not available

The Allow Scheduling Option can be selected but no schedule can be configured.

Workaround: None available. Planned for future release.

T18254 Isilon Shares Path Selector allows selection of FQDN

Isilon Shares Path Selector incorrectly allows selection of the FQDN only without an actual path.

Workaround: Be sure to select a path object in the selector.

T18273 AnyCopy Job Name format not validated

The AnyCopy GUI allows you to enter a job name that is not compliant with SynclQ policy name rules. An invalid name causes the AnyCopy Job to fail at the step where the SynclQ policy is created.

Workaround: AnyCopy Job names must be compliant with SynclQ policy naming rules and as such should not contain things such as: spaces, special characters, language specific characters.

T18375 "Block access to source data to all users during copy" option is not available

The "Block access to source data to all users during copy" option if selected for the AnyCopy Job does not have any effect when the job runs. Users still have write access to the data.

Workaround: None available from AnyCopy.

T18385 Issues when same AnyCopy Job started at same time by multiple users

If the same AnyCopy Job is started at the same time by multiple users following issues may occur:

- error running summary report
- snapshots on target not being cleaned up
- Copy Configuration step not run

Workaround: Only one instance of an AnyCopy job should be started at any time.

Reporting Issues

T17220 Policy Job Summary Report UNC path has incorrect format

In the Job Summary, the UNC Path has double \\ in front of share name instead of a single \ .

Workaround: Remove the extra \ in the UNC path before using it.

Known Limitations

Please review the Limitations documented [here](#).

T18277 Transient AnyCopy Job in the Jobs window

The AnyCopy Jobs that appear in the Jobs window are transient and should not be acted upon from that window.

T18278 Copy Configuration Error for AnyCopy Job for same cluster and same access zone for source and target path

For the case where an AnyCopy job is created and source and target path are on same cluster and same access zone the Copy Configuration step will fail for SMB Shares and NFS Alias with an AEC_CONFLICT exception.

Workaround: Since SMB Share and NFS Alias names must be unique within an Access Zone, the Shares and NFS Alias will need to be added manually with a unique name for the new path in the same Access Zone.

© Superna Inc

1.15. Current Release - Release Notes

Ransomware Defender for ECS

[Home Top](#)

Release Date	Version
11/28/2023	2.6.4-23365

- [What's New in Superna Eyeglass Ransomware Defender for ECS - Release 2.6.4 \(11/28/2023\)](#)
- [New in Superna Eyeglass Ransomware Defender for ECS - Release 2.6.3 \(09/28/2023\)](#)
- [Supported ECS releases](#)
- [End of Life Notifications](#)
- [Technical Advisories](#)
- [New in Superna Eyeglass Ransomware Defender for ECS - Release 2.6.2 \(09/01/2023\)](#)
- [New in Superna Eyeglass Ransomware Defender Edition Release 2.6.1 \(08/03/2023\)](#)
- [New in Superna Eyeglass Ransomware Defender Edition Release 2.6.0 \(06/29/2023\)](#)
- [Fixed in 2.6.0](#)
 - [RWD-279 Lockout API returns response code 500 for ECS IAM User](#)
 - [RWD-365 ECS version 3.8 is now supported in Ransomware Defender for ECS and AirGap for ECS](#)
- [New in Superna Eyeglass Ransomware Defender Edition Release 2.5.12 \(05/09/2023\)](#)
- [Fixed in 2.5.12](#)
 - [RWD-380 TD11 is not triggered as described in the documentation when using ECS](#)
- [New in Superna Eyeglass Ransomware Defender Edition Release 2.5.11 \(04/03/2023\)](#)
- [New in 2.5.11- 23110](#)

- New in 2.5.8.1-22116
- New/Fixed in 2.5.8.1-22100
- New in 2.5.8.1-22080
 - T21791 Ransomware Defender API retrieval of ECS active events
- Fixed in 2.5.8.1-22080
 - T20753 Error in Manage Services for vaultagent
 - T17777 ECS bucket versioning option not working
- Build Version: 2.5.8-21189 - First release
- Known Issues
 - T20613 Continuous Operation Dashboard does not show ECS
 - T20616 CLI restore command not available for ECS user
 - T20649 Security Guard Job Identifier null in Security Guard log
 - T20775 Edit ECS Username or Password results in issue with displaying Inventory
 - T20672 Monitor List IP address does not work for ECS
 - T22778 IAM user event does not produce a csv file of events and files
 - T23359 Failed to enable ECS versioning
 - T23435 Flag as false positive does not work for IAM user event
 - RWD-362 Support ECS on RWD when turboaudit REST api is configured
 - RWD-217 Event fails to upgrade with multiple user (ECS events only)
 - Managing Multiple ECS
 - NFS operations on ECS are not monitored by Ransomware Defender (T20683)

What's New in Superna Eyeglass Ransomware Defender for ECS - Release 2.6.4 (11/28/2023)

New in Superna Eyeglass Ransomware Defender for ECS - Release 2.6.3 (09/28/2023)

First release of Ransomware Defender for ECS offering following functionality:

Ransomware Defender Feature	Supported for ECS
Real - time detection	Yes
Behavior based detection	Yes
object tracking per security event	Yes
RBAC	Yes
IAM user lockout support	Yes with 3.7 and 3.8
Ignore list, Monitor list	Yes
Security Guard Test Feature	Yes
Learning Mode	Yes
Bucket level reporting	Yes
Native REST API integration with managed device	Yes
Audit data input over S3	Yes
Source IP of compromised PC	Yes
Per user lockout	Yes
Snapshots	No - not a supported ECS feature
Airgap	No

Supported ECS releases

3.6

3.7

3.8

End of Life Notifications

End of Life Notifications for all products are available [here](#).

Technical Advisories

Technical Advisories for all products are available [here](#).

New in Superna Eyeglass Ransomware Defender for ECS - Release 2.6.2 (09/01/2023)

New in Superna Eyeglass Ransomware Defender Edition Release 2.6.1 (08/03/2023)

New in Superna Eyeglass Ransomware Defender Edition Release 2.6.0 (06/29/2023)

Fixed in 2.6.0

RWD-279 Lockout API returns response code 500 for ECS IAM User

Lockout API returns response code 500 for ECS IAM User

RWD-365 ECS version 3.8 is now supported in Ransomware Defender for ECS and AirGap for ECS

New in Superna Eyeglass Ransomware Defender Edition Release 2.5.12 (05/09/2023)

Fixed in 2.5.12

RWD-380 TD11 is not triggered as described in the documentation when using ECS

TD11 is not triggered as described in the documentation when using ECS

New in Superna Eyeglass Ransomware Defender Edition Release 2.5.11 (04/03/2023)

New in 2.5.11-23110

Zero Trust API now supports locking out ECS users.

New in 2.5.8.1-22116

Refer to previous build versions.

New/Fixed in 2.5.8.1-22100

Refer to previous build versions.

New in 2.5.8.1-22080

T21791 Ransomware Defender API retrieval of ECS active events

The SERA API call /sera/v1/ransomware/rswevents now returns Object Buckets as well as RSW event type.

Fixed in 2.5.8.1-22080

T20753 Error in Manage Services for vaultagent

In 2.5.8 Manage Services shows an error for the vaultagent component. Impact: None to Ransomware Defender. This component is not required for Ransomware Defender.

Resolution: Now vaultagent is removed from component list.

T17777 ECS bucket versioning option not working

The Ransomware Defender Threshold Detection Settings option "ECS bucket versioning" will cause an error if versioning policy not already configured on the ECS.

Impact: This issue has no impact on ability to perform the lockout. This option is planned to be removed in a future release.

Resolution: This option has now been removed.

Build Version: 2.5.8-21189 - First release

Known Issues

T20613 Continuous Operation Dashboard does not show ECS

The Eyeglass desktop Continuous Operation Dashboard used to verify reachability and version of devices managed by Superna Eyeglass does not list this information for the ECS.

Workaround: Reachability alerts are sent if ECS is found to be unreachable from Superna Eyeglass.

T20616 CLI restore command not available for ECS user

The `igls rsw restoreaccess` command which is available to manually restore access to locked out user from the Eyeglass appliance command line does not work for ECS users.

Workaround: Enable the account using ECS native tools.

T20649 Security Guard Job Identifier null in Security Guard log

The Security Guard Job identified appears as "null" at the bottom of the Security Guard log. Impact: No impact to completion of Security Guard Job.

Workaround: None required

T20775 Edit ECS Username or Password results in issue with displaying Inventory

If the Username and/or Password used by Eyeglass to manage the ECS are edited, the change is saved successfully but the Inventory view remains in "... updating..." mode. Impact: No impact to Ransomware Defender security event detection. Unable to view the ECS components discovered by Eyeglass from the GUI.

Workaround: ssh to the Eyeglass appliance and sudo to root and then restart the Eyeglass sca service: `systemctl restart sca`

T20672 Monitor List IP address does not work for ECS

Even if an IP address is configured in the Monitor list, an ECS detection from that IP address will not be in monitor mode. It will be subject to lockout as per the event severity.

Workaround: Use User or path as an alternative in the Monitor Configuration.

T22778 IAM user event does not produce a csv file of events and files

A detection for IAM user will show a sample of affected objects in the GUI but the related csv file is not created. Impact is for IAM user only. The csv file is available for object user.

Workaround: Use the GUI to see a sample of affected objects.

T23359 Failed to enable ECS versioning

A Failed to enable ECS versioning alarm may be raised after upgrade to 2.5.8.1. This alarm has no impact.

Workaround: None required

T23435 Flag as false positive does not work for IAM user event

Learned threshold cannot be updated for an IAM user event either manually using Archive as False Positive or in automatic learning mode.

Workaround: None available. Leave IAM account in monitor mode if you do not want a lockout based on a false positive.

RWD-362 Support ECS on RWD when turboaudit REST api is configured

Support ECS on RWD when turboaudit REST api is configured

RWD-217 Event fails to upgrade with multiple user (ECS events only)

Event fails to upgrade with multiple user (ECS events only)

Known Limitations

Managing Multiple ECS

Managing multiple ECS has the following limitations:

- vdc names must be unique across the ECS being managed as the vdc is used by Superna Eyeglass Ransomware Defender as the unique identifier for the ECS.

NFS operations on ECS are not monitored by Ransomware Defender (T20683)

ECS Web Access Logs that are used to monitor S3 operations against objects on the ECS do not contain NFS operations and therefore NFS operations against objects on the ECS are not monitored by Ransomware Defender.

© Superna Inc

1.16. Current Release Notes Ransomware Defender AirGap 2.0

[Home](#) [Top](#)

- [What's New in Superna Eyeglass Ransomware Defender Edition Release 2.5.9 AirGap 2.0](#)
- [Supported OneFS releases](#)
- [Supported Eyeglass releases](#)
- [Inter Release Functional Compatibility](#)
- [End of Life Notifications](#)
- [End of Support in Release 2.5.9](#)
- [Deprecation Notices](#)
- [Technical Advisories](#)
- [New/Fixed for AirGap 2.5.9](#)
- [New/Fixed for AirGap 2.5.8.1-22100](#)
- [New for AirGap 2.5.8.1-22080](#)
 - [T22072 AirGap Enterprise Events and Disk Usage Retrieval now a push](#)
 - [T19599 Migrate Configuration from Protected to Vault Cluster](#)
 - [T21214 AirGap Enterprise can now support multiple vaults managed from the same Eyeglass](#)
 - [T22123 Command to send vault agent logs manually](#)
 - [T21490 Monitor AirGap SynclQ Policies for changes to configuration](#)
 - [T21830 AirGap Enterprise Fiber cutter option](#)
- [Fixed in AirGap 2.5.8.1-22080](#)
 - [T22930 AirGap Enterprise Replication Nodes require access to Production Network](#)
 - [T20932 AirGap Job Reports csv do not report failed jobs](#)
- [New for AirGap 2.5.8-22028](#)
- [New for AirGap 2.5.8-21330](#)
- [New for AirGap 2.5.8-21306](#)

- T20945 AirGap - Alarm Conditions (AirGap Enterprise)
- New for AirGap 2.5.8-21240 - Controlled Availability
 - T21212 AirGap Enterprise does not require Static Route configuration
 - T21042 Automated retrieval of vault cluster logs (AirGap Enterprise required)
- New for AirGap 2.5.8-21213/21222 - Controlled Availability
 - T19522 AirGap Enterprise
- Fixed in 2.5.8-21330
 - T22171 - Log4j Vulnerability - Upgrade to Log4j 2.17.0 (2.5.8-21330 and higher Log4j 2.17.0)
- Fixed in 2.5.8-21306
 - T22033 Log4j Vulnerability - CVE-2021-44228
- Fixed in 2.5.8-21222
 - T20770 AirGap Event Retrieval Job Fails with No route to host
 - T20358 Not able to create an AirGap Job Report for a selected period
 - T19195, T19221 AirGap Job shows success when failed
 - T20766 Cannot view second page of AirGap Config AirGap job list
- Known Issues
 - T15104 Default schedule does not run the job
 - T15300 Error on manually connecting Airgap not displayed
 - T16199 No alarm if Airgap event retrieval from Powerscale cluster is in error
 - T16436 Airgap Jobs cannot be manually run from the Airgap window
 - T16456 Customized Airgap schedules reset to default after upgrade
 - T16457 Airgap window not refreshed
 - T16470 Renaming Airgap SynclQ policy does not preserve original settings
 - T16476 AirGap Job continues to run after Powerscale cluster deleted from Eyeglass
 - T19609, T19632 User Disabled AirGap Job may have status of having been run when it has not
 - T19631 AirGap Config window time uses Eyeglass appliance timezone
 - T20966 AirGap Job Configuration lost on rediscover or anyrelease restore

- T21134 AirGap Basic Job can be started from Jobs window without AirGap role
- T21863 AirGap Basic static route remains on error
- T21327 Managed Device Alarms have incorrect date and are sorted oldest to newest
- T21224 Snapshot schedule job created for AirGap Job
- T21147 Customizing AirGap policy prefix results in job errors
- T21659 AirGap state - network disconnected in UI
- T20945 AirGap Open Check may not detect vault open
- T23094 Vault Cluster Event Retrieval fails for AirGap Basic in 2.5.8.1
- T20525 Connectivity check does not work for AirGap Enterprise with Fiber Cutter
- T23399 No validation when adding vault cluster
- T23400 Fiber Cutter Error Handling
- AIRGAP- 404 [Airgap Reports] It shows an Error for the Job when creating a report manually
- AIRGAP 416-Vault Agent log archive has incorrect naming
- Known Issues ECS
 - Airgap- 147 Total number of jobs in AirGap report is incorrect
 - Airgap-221 NULL is displayed for Source in Managed Devices Alerts
 - Airgap-224 Job update to Eyeglass is not working as expected
 - Airgap-289 Active RWD events are ignored when starting AirGap ECSSync jobs from UI using Run Now
 - Airgap-226 Docker issues in Vault Agent
 - AIRGAP-372 Not all the AirGap ECSSync jobs are started when scheduled
- Known Limitations
 - T19614 AirGap Job consideration of Easy Auditor Active Auditor Active Event not configurable
 - T21316 Vault stays open for vault cluster event retrieval

- [T21274 Alarm raised for vault open in Eyeglass is not cleared after maintenance window is finished](#)
- [Airgap-329 Vault agent names must be case-insensitively unique](#)
- [AIRGAP-427 Airgap ECS sync jobs get duplicated sometimes](#)

What's New in Superna Eyeglass Ransomware Defender Edition Release 2.5.9 AirGap 2.0

What's New! In Superna Eyeglass Ransomware Defender AirGap 2.0 Release 2.5.9 can be found [here](#).

Supported OneFS releases

Source cluster

8.2.0.x

8.2.1.x

8.2.2.x

9.1

9.2

9.3

9.4

Target Airgap Cluster

8.2.2.x

9.1.0.0

9.2.0.x

9.3.x.x

9.4.x.x

Supported Eyeglass releases

Superna Eyeglass Ransomware Defender Version	Superna Eyeglass Version
2.5.9-22231	2.5.9-22231
2.5.8.2-22164	2.5.8.2-22164

Inter Release Functional Compatibility

	OneFS 8.0	OneFS 8.1	OneFS 8.2	OneFS 8.0 - OneFS 8.1	OneFS 8.0 or 8.1 - OneFS 8.2

End of Life Notifications

End of Life Notifications can be found [here](#).

End of Support in Release 2.5.9

No end of support notices in release 2.5.9.

Deprecation Notices

No deprecation notices at this time.

Technical Advisories

Technical Advisories for all products are available [here](#).

New/Fixed for AirGap 2.5.9

Stability and bug fixes

New/Fixed for AirGap 2.5.8.2-22164

New/Fixed for AirGap 2.5.8.1-22116

Refer to previous 2.5.8.1 releases.

New/Fixed for AirGap 2.5.8.1-22100

Refer to previous 2.5.8.1 releases.

New for AirGap 2.5.8.1-22080

T22072 AirGap Enterprise Events and Disk Usage Retrieval now a push

For AirGap Enterprise deployments, vault cluster events and disk usage are now pushed to Eyeglass when scheduled AirGap jobs are run. Commands are available to be run from the vault agent to manually initiate a push of this information.

Documentation is available [here](#).

T19599 Migrate Configuration from Protected to Vault Cluster

A new tab in the AirGap window "Migrate Configuration" is now available to copy shares/exports related to AirGap jobs to the vault cluster without the source cluster being available. Documentation is available [here](#) - see section "Configuration Data Sync Steps Eyeglass".

T21214 AirGap Enterprise can now support multiple vaults managed from the same Eyeglass

AirGap Enterprise can now support [multiple vaults](#) managed from the same Eyeglass. Commands for maintenance window have been updated to support this and can be found [here](#). New multi-vault commands can be found [here](#).

T22123 Command to send vault agent logs manually

A command is now available manually initiate sending of the vault agent logs to Eyeglass. Requires that the vault has been opened prior to running the command. Documentation can be found [here](#).

T21490 Monitor AirGap SynclQ Policies for changes to configuration

A new job assesses whether there have been any changes to SynclQ policy configuration for those policies configured to copy data into the vault each time inventory runs. If any change is found an alarm is raised with alarm code [SCA0098](#).

T21830 AirGap Enterprise Fiber cutter option

AirGap Enterprise can now be configured with a physical fiber cutter for maximum data separation with full optical light borken with a layer 0 device. Requires purchase of a 3rd party device from Echola.

Fixed in AirGap 2.5.8.1-22080

T22930 AirGap Enterprise Replication Nodes require access to Production Network

For AirGap Enterprise the nodes on the production cluster that are used to replicate to the vault must also have network connectivity to Eyeglass.

Resolution: A new flag "--protectedManagementNode" has been introduced for adding then production (protected) cluster in the vault agent to identify which node on the production cluster should be used for communication with Eyeglass.

T20932 AirGap Job Reports csv do not report failed jobs

AirGap Job reports that are sent out by schedule or created manually do not report on failed jobs in the attached csv. Failed jobs are correctly reported in the email summary.

Resolution: AirGap job reports csv now correctly report on failed SyncIQ jobs.

New for AirGap 2.5.8-22028

Refer to previous 2.5.8 build information.

New for AirGap 2.5.8-21330

Refer to previous 2.5.8 build information.

New for AirGap 2.5.8-21306

T20945 AirGap - Alarm Conditions (AirGap Enterprise)

New alerts raised under following conditions for AirGap Enterprise

- starting AirGap job - Informational alert
- finishing AirGap job; - Informational alert SCA0090 Vault AirGap job <job>
Succeeded
- reviewing vault agent for new policies or schedule; - Informational alert
SCA0095 Ransomware Defender AirGap Schedules query
- AirGap job not respecting schedule; Critical Alert -SCA0096 - Ransomware
Defender AirGap job did not run according to scheduled
- failed AirGap job; Critical alert - SCA0082 - Ransomware Defender AirGap
job <job> failed - needs attention
- vault is opened when no AirGap job is running; Critical alert - SCA0091 -
Vault is opened - No running tasks on vault

- maintenance window alarm. - Critical Alert - SCA0091 Vault is opened - Vault is opened for x minutes, when the maintenance window expires the alarm is cleared from active alarms

New for AirGap 2.5.8-21240 - Controlled Availability

T21212 AirGap Enterprise does not require Static Route configuration

Managing AirGap Enterprise incorrectly required that the AirGap Basic static route be configured. The static route configuration is no longer required when the airgap job is managed by the vault agent.

T21042 Automated retrieval of vault cluster logs (AirGap Enterprise required)

Automated retrieval of vault cluster logs can now be configured. More information can be found [here](#).

New for AirGap 2.5.8-21213/21222 - Controlled Availability

T19522 AirGap Enterprise

AirGap solution with an inside the vault host and VM that opens and closes the vault from within the vault. This is done by removing the replication interfaces from the IP pool which removes the IP address from the interfaces. This mode places a VM inside the vault and disables the IP stack that connects the vault cluster to any outside network.

Documentation for AirGap Enterprise is available here:

- [Inside the Vault mode Deployment \(Enterprise AirGap License Required\)](#)
- [AirGap Enterprise Additional Requirements](#)

Fixed in 2.5.8-21330

T22171 - Log4j Vulnerability - Upgrade to Log4j 2.17.0 (2.5.8-21330 and higher Log4j 2.17.0)

Fixed in 2.5.8-21306

T22033 Log4j Vulnerability - CVE-2021-44228

Resolution: log4j version updated to 2.15.0 which has patch for the vulnerability.

Fixed in 2.5.8-21222

T20770 AirGap Event Retrieval Job Fails with No route to host

AirGap Event Retrieval job uses the IP address configured in Eyeglass to manage the production Powerscale cluster. If that IP address is not associated with a node that is configured in the AirGap pool for replication to the vault then event retrieval fails because the static route applied to the AirGap pool is only applied to the nodes in the pool.

Resolution: IP address from a node in the AirGap pool is now used for event retrieval. Note that additional sudoer permissions required as documented [here](#).

T20790 AirGap SynclQ policy timeout uses failover timeout setting

The amount of time that RansomwareDefender will wait for an AirGap SynclQ job to complete is defined in the Eyeglass system.xml "failovertimeout" setting. Impact: If the "failovertimeout" setting is lower than the time required for the SynclQ policy to complete, the AirGap job will timeout and remove the static routes causing the AirGap SynclQ job to fail with an incomplete update to the vault copy of the data.

Resolution: Eyeglass system.xml now has separate tag for timeout setting for AirGap SynclQ policy: airgapJobTimeout. Post upgrade this tag will need to be set to the desired value. Default is 240 minutes.

T20358 Not able to create an AirGap Job Report for a selected period

The AirGap Reports tab feature to Create Report for a custom time frame results in an error and the report is not produced. Impact: This does not affect the daily AirGap job report that is sent out. The issue is specific to custom report generation.

Resolution: Specific timeframe can now be selected.

T19195, T19221 AirGap Job shows success when failed

Under some circumstances if an AirGap job fails, such as running the AirGap SyncIQ job or AirGap job source cluster unreachable, the AirGap Config window job status shows success.

Resolution: Alarm and running job info and job history correctly show the failure.

Fixed in 2.5.8-21213

T20766 Cannot view second page of AirGap Config AirGap job list

The AirGap Config list of AirGap jobs list is limited to 10 jobs per page. If you have configured more than 10 jobs, when you navigate to the second page the display is blank.

Resolution: AirGap Jobs are now displayed on all pages.

Known Issues

T15104 Default schedule does not run the job

Airgap jobs are created with a default schedule (daily at midnight) but Status shows as Not Scheduled and jobs never run.

Workaround: Set a manual schedule.

T15300 Error on manually connecting Airgap not displayed

If the command to manually establish connectivity *igls airgap connect* fails it correctly does not apply the static route but the status message indicates that connectivity has been established.

Workaround: Verify from Isilon interface whether pool has static route applied.

T15333 No notification if Airgap jobs are globally disabled

After using the command *igls airgap disable* to globally disable Airgap jobs there is no alarm to notify administrator of this action and no indication in the GUI that action has been taken.

Workaround: Airgap last run date can be used to determine whether it is running on it's schedule.

T16199 No alarm if Airgap event retrieval from Powerscale cluster is in error

If the job to retrieve events from Powerscale cluster encounters an error there is no alarm raised to notify administrator.

Workaround: Login to the Eyeglass GUI and check the status of the event retrieval job.

T16436 Airgap Jobs cannot be manually run from the Airgap window

Airgap Jobs cannot be manually run from the Airgap window.

Workaround: Airgap jobs must be manually run from the Eyeglass Jobs window.

T16456 Customized Airgap schedules reset to default after upgrade

After an upgrade, the Airgap schedules get reset to the default once a day setting.

Workaround: Document schedules prior to upgrade and reapply post upgrade.

T16457 Airgap window not refreshed

After adding a new job the Airgap window is not refreshed to show the new job.

Workaround: Close and reopen the Airgap window.

T16470 Renaming Airgap SynclQ policy does not preserve original settings

If an Airgap Synclq policy is renamed the settings related to this SynclQ policy are not preserved in Eyeglass.

Workaround: Reapply settings in Eyeglass once Inventory has run and the Airgap job with new name is visible in Eyeglass.

T16476 AirGap Job continues to run after Powerscale cluster deleted from Eyeglass

If there are Airgap jobs related to Powerscale cluster that has been deleted from Eyeglass, Eyeglass will continue to attempt to run them but the job will not succeed.

Workaround: None required. No alarm is generated.

T19609, T19632 User Disabled AirGap Job may have status of having been run when it has not

If an AirGap Job is User Disabled in the Jobs window, it may appear in Running Jobs, AirGap Jobs History or show a Last Run date as though it had run after being user disabled even though it did not actually open the vault and run the airgap SynclQ job.

Workaround: Check on Powerscale directly to confirm that AirGap SynclQ job has not been run.

T19631 AirGap Config window time uses Eyeglass appliance timezone

The date and time shown in the AirGap Config window uses the Eyeglass appliance timezone instead of the timezone of the computer which is accessing Eyeglass as is done elsewhere in the GUI.

Workaround: If Eyeglass appliance and local browser time zone are different, manually convert the date / timestamps in the AirGap Config window to the local browser time zone to be able to compare run times in different windows.

T20966 AirGap Job Configuration lost on rediscover or anyrelease restore

If the igls rediscover command is executed on Eyeglass with AirGap configuration or an anyrelease restore to a new appliance the AirGap Job Configuration for subnet mask and gateway are lost. Schedule is maintained.

Workaround: Consult with support.superna.net before performing either of those operations. Keep an independent record of AirGap job configuration.

T21134 AirGap Basic Job can be started from Jobs window without AirGap role

Any member of a User Role with the Jobs Modify permission can run an AirGap Basic job.

Workaround: Only include Jobs Modify permission for roles where it is required and limit membership to Roles with the Jobs Modify permission.

T21863 AirGap Basic static route remains on error

If an error occurs which leaves the static route behind, there is no mechanism that will automatically remove the static route and it will cause the next scheduled AirGap job to fail.

Workaround: Static route must be removed manually. Introduced in Release 2.5.8 there is a check every 5 minutes to determine whether the vault is open when it shouldn't be that can be used to alert to this condition and that manual removal of static route is required.

T21327 Managed Device Alarms have incorrect date and are sorted oldest to newest

The vault cluster events displayed in Managed Device Alarms have the date/time they were retrieved rather than the actual event date and are sorted oldest to newest.

Workaround: Use pagination to navigate to newer alerts.

T21224 Snapshot schedule job created for AirGap Job

A Snapshot Schedule Configuration Replication job is incorrectly created for each AirGap job and is enabled. When Configuration Replication runs the Snapshot Schedule jobs are also run and result in error for AirGap jobs as the target cluster (vault cluster) is not reachable.

Workaround: Set the Snapshot Schedule jobs for the AirGap Jobs to User Disabled.

T21147 Customizing AirGap policy prefix results in job errors

If the AirGap Job SyncIQ policy prefix is customized, existing and new AirGap jobs are in error.

Workaround: Contact support.superna.net for assistance to remove references to previous prefix jobs.

T21659 AirGap state - network disconnected in UI

If a scheduled AirGap job runs and finishes while a maintenance window is active to keep the vault open, on the GUI the AirGap State shows Network Disconnected even though the AirGap is still open as per the maintenance window parameters. Impact: Display only, the AirGap stays open as expected until the maintenance window timer expires at which point it is closed.

Workaround: None required. Once the maintenance window expires, the vault will be closed and you will receive notification as an informational alert

T20945 AirGap Open Check may not detect vault open

AirGap Open Check uses the IP address configured in Eyeglass to manage the production Powerscale cluster. If that IP address is not associated with a node that is configured in the AirGap pool for replication to the vault then the open check will find that the vault cluster is always closed and not detect an open state.

Workaround: For AirGap basic the next AirGap job will error due to static route still being present. For AirGap Enterprise, the vault agent will detect the open vault and close it without any manual intervention and no alarming.

T23094 Vault Cluster Event Retrieval fails for AirGap Basic in 2.5.8.1

As of 2.5.8.1, the task to retrieve alarms from vault cluster during the AirGap job fails and no alarms from the vault cluster are gathered.

Workaround: None available. Until this issue is fixed, AirGap basic customer should not upgrade. Plan to address in a patch release.

T20525 Connectivity check does not work for AirGap Enterprise with Fiber Cutter

The connectivity check command `ecactl airgap check --prod <cluster>` run from the vault agent does not work for AirGap Enterprise configured with Fiber Cutter.

Workaround: Manually open the vault and manually check connectivity.

T23399 No validation when adding vault cluster

There is no validation when adding vault cluster that all required parameters have been configured and that entries have valid format. If misconfigured, AirGap jobs will not run.

Workaround: Use manual process and connectivity check to verify configuration.

T23400 Fiber Cutter Error Handling

If there is an configuration or environmental issue that prevents connectivity on the Fiber Cutter deployment, no error is provided when the AirGap jobs fail.

Workaround: Contact support.superna.net for assistance.

AIRGAP- 404 [Airgap Reports] It shows an Error for the Job when creating a report manually

Manual report creation test- Failed

Reports are getting generated when create manually but It shows an Error for Job

When clicking on AIRGAP Icon & Navigate to Airgap reports and creating a report you observe an error in the jobs window

AIRGAP 416-Vault Agent log archive has incorrect naming

Vault Agent log archive has incorrect naming

Known Issues ECS

Airgap-147 Total number of jobs in AirGap report is incorrect

In some cases, there can be a discrepancy between the total shown in the pagination view of airgap jobs history and the number shown in the job report. The number in the report is accurate.

Workaround: use the job report to determine the actual number of jobs run.

Airgap-221 NULL is displayed for Source in Managed Devices Alerts

When proxying alerts from the vault ECS cluster in the ECS airgap solution, the Source is listed as null.

Workaround: none

Airgap-224 Job update to Eyeglass is not working as expected

When adding a new job to ecssync, sometimes the update does not get pushed to eyeglass and the user has to run `ecactl ecssync updatejobs` to force it to update.

Workaround: run `ecactl ecssync updatejobs` every time after modifying the jobs on ecssync.

Airgap-289 Active RWD events are ignored when starting AirGap ECSSync jobs from UI using Run Now

AirGap ECSSync jobs with the 'Pause data replication when active ransomware events detected' option selected and the jobs are started from UI using Run Now, the jobs will continue to run with active RWD events.

Workaround: Setup the schedule for the jobs or start the job with CLI command `'ecactl ecssync startjob -- job xxx'`

Airgap-226 Docker issues in Vault Agent

Docker may stop working if the ECS sync cluster up for a long period of time.

Workaround: Contact Superna customer support or run

- `ecactl cluster down`
- `sudo systemctl restart docker`
- remove docker network: `docker network rm <TAB>`

- ecactl cluster up
-

AIRGAP-372 Not all the AirGap ECSsync jobs are started when scheduled

On the multi-vault system that has 3 vaults managed by the same eyeglass, each vault has 5 jobs. All 15 AirGap ECSsync jobs are scheduled to run at the same time, every 15 minutes. On the second vault agent, only 3 out of 5 jobs are started automatically

Known Limitations

T19614 AirGap Job consideration of Easy Auditor Active Auditor Active Event not configurable

If in the Easy Auditor Active Auditor "Active Events" list there is an Active Event listed at the time when the AirGap job is scheduled to run, the AirGap Job will be blocked from running with the message "Found active RSW events, will not run AirGap job..." and in the AirGap Config GUI the job AirGap State is "Disabled for Active Events" and Status is Error.

Easy Auditor Active Events should be managed and cleared to not impact AirGap jobs. This behaviour may be made configurable in a future release to be able to specify whether or not active auditor events block AirGap jobs.

T21316 Vault stays open for vault cluster event retrieval

If event retrieval from the vault cluster takes longer than running the AirGap SyncIQ job, the vault will stay open until the event retrieval step completes after which it will be closed.

T21274 Alarm raised for vault open in Eyeglass is not cleared after maintenance window is finished

Alarm raised when vault manually opened for maintenance window is not cleared once the maintenance window is ended and vault is closed again. Alarm is able to be manually cleared.

T21851 AirGap Enterprise vault open alarm limitation

In the interval between when the the vault is opened and the associated task is started, a vault open alarm may be triggered as the related task has not been started so the condition of vault open when it should not be is detected.

Workaround: Verify that an associated vault task such as running airgap job or checking for schedule has started shortly after the alarm was raised.

Airgap-329 Vault agent names must be case-insensitively unique

Vault agent names must be case-insensitively unique when you have multiple vault agents added.

AIRGAP-427 Airgap ECS sync jobs get duplicated sometimes

Airgap ECS sync jobs get duplicated sometimes

workaround:

Remove the duplicated job from ECS sync UI

1.17. Release 2.5.8 - Release Notes DR Edition

[Home](#) [Top](#)

- [What's New in Superna Eyeglass PowerScale Edition Release 2.5.9](#)
- [Supported OneFS releases](#)
- [DR Edition Feature Release Compatibility](#)
- [Feature Support Matrix](#)
- [End of Life Notifications](#)
- [Support Removed in Eyeglass Release 2.5.8](#)
- [Deprecation Notices](#)
- [New and Fixed in Eyeglass Release 2.5.8](#)
- [New in 2.5.8](#)
- [New in 2.5.8.1-22116](#)
- [Fixed in 2.5.8.1-22116](#)
- [New in 2.5.8.1-22100](#)
- [Fixed in 2.5.8.1-22100](#)
- [New in 2.5.8.1-22080](#)
 - [T20905 Log Parser](#)
- [Fixed in 2.5.8.1-22080](#)
 - [T21800 Swap file created on Upgrade](#)
 - [T22819 2.5.8 rollback DFS policy when resync prep timed out is incorrect it should not rollback ever](#)
- [New/Fixed in 2.5.8-22028](#)
 - [T22205 RAM Alarm calculation now based on total number of clusters managed](#)
- [New in 2.5.8-21330](#)
- [Fixed in 2.5.8-21330](#)
 - [T22171 - Log4j Vulnerability - Upgrade to Log4j 2.17.0 \(2.5.8-21330 and higher Log4j 2.17.0 \)](#)
- [New in 2.5.8-21306](#)

- NEW - see What's New in 2.5.8 here.
- T17849 DNS Dual Delegation Failover Readiness Validation disabled
- NEW - OneFS 9.3 Support
- NEW - Cluster Storage Monitor new schedule for quota creation
- Fixed in 2.5.8-21306
 - T22033 Log4j Vulnerability - CVE-2021-44228
 - T20584 Eyeglass service account password exposed on error connecting to Powerscale
 - T20628 Cannot disable Zone/IP Pool Readiness AD Delegation Validation (2.5.7.1 and higher)
 - T16888 Configuration Replication fails if SyncIQ Policy source and target path are different and SyncIQ policy path contains special character
 - T9652 Unlock My Files inconsistent handling for unreachable PowerScale cluster
 - T19288 Custom Postfix email settings not restored
 - T19275 Syslog alarm forwarding configuration not restored
- Technical Advisories
- Failover
 - 2666/2723: Problems for Controlled Failover when Source becomes unreachable during failover
 - 2278: Zone Readiness lists Access Zone after all related SyncIQ Policies are deleted
 - 2919: Eyeglass Configuration Replication Jobs may not display in the Zone Readiness Eyeglass Configuration Replication Readiness list
 - 3010: Unexpected results for failover where total number of objects exceeds the published limit
 - 3029: Zone Readiness not calculated correctly for SyncIQ subnet pool with a mapping hint
 - 3031: Zone Readiness Policy Path Containment Check results in extra errors
 - 3077: Zone Readiness does not catch pool mapping hint misconfiguration for partial string match

- T477: No Policy Hot/Hot Validation Error for policy with no share/export
- T482: Zone Readiness shows OK for multiple Smartconnect Zone Mapping errors
- T654: Zone Readiness incorrectly includes SynclQ Policy in System Access Zone
- T1712: Zone Readiness missing Zone when pool has no SmartConnect Zone - OneFS 7
- T1716: Eyeglass Runbook Robot NFS mount not functioning for RHEL and Centos deployments
- T1482: Zone Readiness SynclQ Readiness not updated after Access Zone associated to a pool
- T3742: No Policy Hostname Validation error if SynclQ Policy Target Host is fully qualified and uses short name on target cluster pool that has a Superna Eyeglass mapping hint applied
- T3848: SPNs not updated during failover for OneFS8 non-default groupnet AD provider
- T4009: SPNs creation case sensitive to AD provider name
- T4320: Access Zone not assigned to any Subnet Pools results in many Zone Readiness Errors
- T4316: Runbook Robot Policy Job does not display SynclQ Job Reports
- T4857: Failed SmartConnect Zone Rename step is not displayed in Failover Log
- T4878: Pool Failover - Non Runbook Robot SynclQ policies can be mapped to Robot pool
- T4968: Zone missing from DR Dashboard Zone Readiness tab if a SynclQ Policy has a target host that cannot be resolved
- T5092, T4490: Access Zone Pre and Post Failover Scripting Issues
- T5473: Zone/Pool Readiness Pool Mapping Hint Matching Issue
- T5961: Failover Log shows Incorrect Final Steps
- T5897: Post Failover Inventory step may fail during multiple concurrent failovers

- T5941: Pool Failover Failover Log Summary incorrectly displayed Client Redirection step not run
- T5967: Failover where Quota Sync is disabled has extra lines in Failover Log
- T5934: Access Zone Readiness shows OK for DFS only failed over Access Zone
- T6289: SynclQ policy with no shares or exports is associated with the System Access Zone for failover
- T6311: Selecting the DR Failover Status link on the DR Assistant Summary page may result in an Error
- T6402: Access Zone Failover Post Failover Inventory step runs multiple times
- T6842: Zone Readiness: Zone does not display Failover Over state for Access Zones where custom SmartConnect Zone prefix is being used
- T7184: Pool Readiness: Pool to SynclQ Policy Mapping is not displayed in DR Dashboard until Readiness task is run
- T8824: User Quota creation fails on failover for multiple disjointed AD Domain environment
- T10363 Overlapping Access Zone Failover blocked for System Access Zone
- T10912 Quota Sync fails for quotas where quota container property set to true
 - T10935 Pool failover "failovertarget" must be "zone id"
 - T7622 Eyeglass will not add custom SPNs if PowerScale Cluster does not return any missing SPN during SPN check (as of 2.5.6)
 - T13360 Failover Readiness Validation for Corrupt Failover Snapshots does not check for missing snapshot
 - T12434 Concurrent Access Zone or Pool Failover with DFS configured policies may fail DFS share rename step
 - T13701 Failover option "Disable SynclQ Jobs on Failover Target" does not reapply schedule
 - T13726 Pool Failover error mapping policy to pool on target cluster for disabled job
 - T13881 Cannot failover overlapping Access Zones - rel 2.5.6

- T14398 Zone/Pool Failover Readiness FQDN Alias validation incorrectly reports OK when pool does not have an ignore hint
- T14931 Policies configured for Pool failover allowed to do DFS or SyncIQ failover until next configuration replication runs
- T14948 Failover log for Uncontrolled Access Zone incorrectly logs status of final readiness job and changes to pool aliases
- T14965 Failover readinessSyncIQ File Pattern Validation has WARNING state instead of ERROR
- T14971 DR Assistant validation check screen incorrectly requests acknowledgement of readiness warnings
- T14974 Access Zone Failover with error on DFS share renaming will abort for all policies
- T14988 Eyeglass GUI incorrectly allows pool failover configuration for a policy that is active in failover rehearsal mode
- T15000 DR Rehearsal status lost if fingerprint file deleted
- T15042 REST API policy readiness is missing output for Target Reachability check
- T15010 DR Rehearsal Revert not blocked for Pool Failover mode when in REHEARSAL_ERROR
- T15609 Alarm time not updated for repeated policy/dfs/zone/ pool readiness alarms
- T15191 Failover Log may show 2 summaries when Rehearsal Mode enabled
- T15192 Rehearsal Mode not disabled for Access Zone associated with Pool Failover
- T15248 Error in DFS failover does not rollback share renaming when failover job includes multiple policies
- T15260 DFS Failover share renaming rollback not done when all share rename fails on source cluster
- T15271 Zone/Pool Failover error in SMB Data Integrity step or run policy step incorrectly attempts to roll back networking
- T15278 Pool Failover job with multiple pools stops failover steps for all pools on DFS share renaming error

- T15290 Pool Failover job with multiple pools does not rollback client redirection when allow writes step fails
- T15298 Quota job run manually after failover may delete quotas on source cluster
- T15530 Policy or DFS Readiness may incorrectly evaluate Policy Hostname validation in error
- T15547 Failover Readiness Domain Mark Validation fails for path with spaces or special characters
- T15610 Policy Readiness Pool Mapping Validation alarm and email indicate Warning severity instead of Error
- T15613 DR Rehearsal Readiness - no alarm or email when DR Rehearsal status changes from OK to Warning or Error
- T15623 REST API - Pool Failover API does not support multiple pool selection
- T15624 REST API - Failover API does not block controlled failover when source cluster unreachable
- T15769 DNS Dual Delegation Validation does not work where NS Record does not resolve directly to an SSIP
- T16154 DR Rehearsal mode issues where source and target path are different
- T17136 Zone Readiness incorrectly shows Error when Access Zone Name, Smartconnect Zone Name and IP Pool name are exactly the same
- T17401 Pool Readiness not displayed with no configured/reachable DNS
- T17477 DFS share suffix not applied for failover or configuration replication
- T17428 REST API - Policy Readiness returns incorrect Access Zone
- T17447 OneFS 9.0 and 9.1 Readiness Validation for Policy Source Nodes Restriction always shows INFO
- T17555 Blank display for Zone or Pool Readiness
- T17731 Policies missing in DR Assistant for Zone or Pool failover
- T17732 Multiple Zone Readiness Jobs
- T18127 DNS Dual Delegation uses wrong SSIP when IP Pool Service Subnet different from the pool subnet
- T18392, T19226 DFS Failover produces extra "null" failover log

- T18779 Overlapping Powerscale cluster and SynclQ Policy names can result in incorrect Failover Readiness assessment
- T18969 Runbook Robot Job in Jobs window disappears when target cluster is unreachable
- T19186 Policy Readiness not updated
- T19553 Zone/Pool Readiness never completes
- T19967 Pool / Zone Readiness does not indicate whether there is a disabled Configuration Replication job in the Zone
- T20181 Policy Hostname Validation Incorrectly show Error
- T21443 Quota failover error when source and target path are different and contain a \$
- T21629 DR Readiness does not indicate source cluster unavailable
- T21750 Deleting SynclQ Policy when Rehearsal Mode is active leaves configuration behind
- T22269 Python Pre and Post Failover Scripts do not work on OpenSUSE 15.3
- T22567 Quota Inventory causes problems during failover
- T21929 igls-original SPN may not be deleted on failover
- DR-205 Zone Readiness Errors when Provider Instance Name mismatched
- DR-254 Onefs 9.4 Unlock My Files Feature Does Not Work
- Configuration Replication
 - 1683: Export sync where source is 7.1.1.x and target 8.x.x.x
 - 649: Export sync where source and target path on each cluster is different is deleted and recreated in each config cycle (affects onefs 7 to 8 or 8 to 7 replication)
 - 1462 - Export max_file_size cannot be replicated
 - 1355: Edit Job configuration to include share/export deselected from another Job causes share/export to be reselected.
 - 1580: Delete and Create export within same replication cycle orphans deleted export on the target with OneFS 7.1.1.x
 - 1625: Custom QUOTA Jobs require extra replication cycle to be deleted
 - 1639: Able to manually Run Now disabled Custom Job

- 1641: Custom Job does not include shares/export when source or destination path configured with a trailing /
- 1788: Delete of unlinked user quota on source may not delete matching quota on the target
- 1789: Able to select shares/exports/quotas outside job path after deselected
- 1887, T3727: Multiple SynclQ policies associated with same Zone will result in transient error on Eyeglass Zone replication creation
- 1924: Quotas on excluded SynclQ directory are selected for replication
- 1998: Custom Eyeglass configuration replication Job does not have an associated Zone replication Job
- 2004: Custom Quota Job is incorrectly listed in the Failover: Quota Failover (RUN MANUALLY) section in the Jobs window
- 2007: Job error after deleting quota
- 2038: Create alias results in temporary error
- 2043: Configuration replication job has error after zone is deleted
- 2045: Edit Configuration for Custom Job has multiple source cluster selected where Eyeglass is managing more than 2 clusters
- 2046: Job Edit Configuration view has the wrong parent selected
- 2049: Delete Zone does not delete associated configuration items on target for custom Jobs and auto jobs with disabled zone Job
- 2235: Eyeglass replication Job does not complete when source cluster becomes unreachable after Job has started
- 2060: Access Zone Replication Error - Error on creation of shared resource
- 2488: Inconsistent behaviour in Run Now for Disabled Jobs
- 1938: Issues with Eyeglass Configuration Replication Jobs after the Access Zone is deleted
- 2308: In EyeGlass, NFS alias health is always 'unknown'
- 2804: Disabled SynclQ Policy is not initially displayed as Policy Disabled in Eyeglass
- T676: Eyeglass Zone replication Job does not replicate all authentication providers for OneFS 8.0

- T723: Job shows OK when there is an Access Eyeglass Zone Replication Error
- T771: Edit Configuration does not show parent node selected
- T805: Eyeglass Configuration Replication Jobs not updated when IP address changed on Source Cluster
- T593: Eyeglass errors for multiple exports with the same path
- T1792: Eyeglass does not auto-detect PowerScale version changes and may use incorrect API version for Configuration Replication
- T1851: Eyeglass Configuration Replication Jobs not removed when there is no SynclQ privilege for the eyeglass service account
- T2193 - Export max_file_size setting not replicated correctly
- T2757: Access Zone is not replicated from OneFS 8 to OneFS 7.2
- T1976 - Eyeglass Jobs Window Edit Configuration does not show related Snapshot Schedules
- T2920: Access Zone Authentication Provider is not replicated to the target cluster
- T3629: Renamed Snapshot Schedule leaves original Snapshot Schedule on the target
- T14803 Set Job Type AUTOSKIPCONFIG does not create associated jobs until configuration replication runs
- T15258 Unable to create Custom Job
- T15321 DFS share name custom suffix may be doubled
- T15884 Some scenarios in networking API failures during Configuration Replication may not block deletes
- T16965 Audit does not consider differences on source and target for SMB share property inheritable_path_acl
- T18812/T23433 Error replicating SMB Share with Run as Root permission
- T19026 Data Config Migration Preview incorrectly shows quotas selected
- T19177 NFS modify properties which are not client list fails with unresolvable host

- T20301 User Disabled AUTOSKIPCONFIG job becomes enabled after a rediscover or if policy renamed
- T20369 Configuration Replication Error after running DR Rehearsal failover on SynclQ policy where source and target path are different and contain special characters and or spaces
- T21375 Snapshot schedule replication error on update
- T22875 Configuration Replication audit step incorrect error when path contains a comma
- T17345 - Advanced Quota settings for Configuration sync
- Features
 - 1138: Eyeglass UI does not block configuration of duplicate remote logging service
 - 2224: Eyeglass Cluster Configuration Report runs when Cluster is unreachable
 - 2061: Access Zone name for Directory Migration is case sensitive
 - 2882: Phone Home Email Disabled
 - 3037: Configure Remote Logging Services in Eyeglass requires manual steps
 - T1515: Eyeglass Shell feature not functioning for RHEL and Centos deployments
 - T3119: Access Zone Migration Preview does not always display Configuration information
 - T3170: Quota Requests History shows Status of Error for processed requests after failover
 - T4280: User Storage View may show all quotas instead of only the User Quotas
 - T4329: DR Test Status does not open
 - T4432: DR Test Mode action on multiple policies do not display in Running Jobs
 - T4968: SynclQ Job Report Troubleshooting section missing information when report is generated on demand
 - T5173: Quota Modification Request window does not close after Submit

- T8834: Storage Monitor Report missing user information when friendly name cannot be resolved
- T9561: Unlock my files incorrectly displays directories
- T11807 Alarm for quota synchronization error does not contain error details
- T13390 DR Testing (Disaster Recovery Testing) Job initially always in User Disabled state
- T14956 No Recovery when DR Test Mode in Entering DR Testing or Exiting DR Testing
- T14962 DR Test Mode Configuration Replication step does not run configuration replication for the DR Test mode job itself
- T15215 Data Config (Zone) Migration Job can not be created where Migration or Destination Path contains special characters
- T15311 Data Config (Zone) Migration Job fails for existing policy when "Migrate only configuration" is checked
- T17535 Quota Search - Display of quota count on modify may not be correct
- T17739 Cannot create quota template for less than 1 GB
- T18148 Incorrect Error Message for unreachable Powerscale cluster when breaking lock
- T19464 AD Group Template incorrectly creates quota on share where user permission is explicitly defined
- T20183 Unlock My Files does not display results if there is a Powerscale node that does not respond
- T22209 igls adv ADGroupThresholds does not scan
- T22622 Active Directory Managed Quotas fails with LDAP configured for retrieving user and groups
- DR-281 NFS deletion is not behaving correctly
- DR-282 Warning message needs to be update when deleting a writable snapshot
- DR-277 We need validation for directory on Writable Snapshots Path
- General

- 924: Inventory View shows + beside component when there are no more children
- T17694: api token download of CMDB file is blocked by desktop login
- 943: Inventory View not auto-refreshed
- 1612,T11989: Some alarms not cleared
- 2155: Access Zone Networking info does not display in Inventory View
- 2628/T15193: Job Definitions window does not sort properly
- 2895: Inventory SPN View is truncated
- 2366: EyeGlass does not support special characters in email recipient address
- 2385: Refresh Now does not refresh the Failover History window
- 2744: Failed to Retrieve Inventory Alarm missing information
- 2978: Syslog Log Viewer freezes Eyeglass web page
- T971: Eyeglass End User Interface Tree View Expanders do not collapse
- T1514: Eyeglass Archive cannot be downloaded when Eyeglass is deployed on Redhat or Centos
- T3137 - Eyeglass daily backup not working for RHEL/CentOS Deployments
- T4596: Log Viewer cannot fetch logs
- T12370 Network Visualization does not display Pool Readiness
- T12373 Cluster Storage Window Empty
- T15310 REST API / Widgets creates empty html file
- T15493 Extraneous Post Failover placeholder scripts
- T15511 Historical failover logs may lose formatting after a backup & restore
- T15647 igls app report issues
- T17530 Backup and Restore does not properly set location/permission for Eyeglass log files
- T18000 Quota limit reached on Eyeglass appliance eca logs directory does not have an alarm
- T18983 Multiple licenses applied to same Powerscale cluster
- T19208 Too many open files

- T19276 Configuration file for enhanced HA for misconfigured/unavailable DNS not restored with --anyrelease option
- T19280 Eyeglass services do not start if retrieval of banned file list on startup hangs
- T19523 After anyrelease restore or rediscover quota jobs for main and mirror policy are both enabled
- T19572 Alarms History missing on new 2.5.7 15.2 deployments
- T20371 API error on OneFS 9.x for retrieving DNS settings
- T20407 igls app report error for OneFS 9.2
- T21275 Deleted Powerscale cannot be readded
- T20808 Alarms window info column does not display full text
- T21820 DR Edition - Manage Services window Eyeglass services status does not display CPU and RAM usage info
- T19213 Eyeglass RAM Alarm inconsistent notification
- T21060 Alarms without info cannot be cleared
- T23072 Eyeglass RAM alarm for concurrent user login does not clear
- T23052, T23065, T23066 Log Parser Report Download links not working
- T23043 Restrictions in Log Parser customer name
- T23113 Log Parser does not show link for report when appliance id contains a slash (/)
- T23009 Log parser permission may not be added to admin role on upgrade
- T23328 igls app report errors
- T23161 Upgrade to 2.5.8.1 from 2.5.8.1 earlier build fails
- DR-286 Issue related to Folder permission in /opt/data
- DR-276 Unwanted shadow trace is created when path picker is opened
- Known Limitations for PowerScale OneFS 8.0.0.x with Eyeglass
- T507 Cluster Report for OneFS 8.0 missing information
- Known Limitations for Eyeglass Failover
- T939 Eyeglass Access Zone Replication Job in Error after failover
- T1785 Cannot set ignore flag on subnet pool after failback

- T2479: Access Zone Failover fails between OneFS 7.2 clusters if Eyeglass also managing OneFS 7.1
- T3258: Cannot start failover while Eyeglass initial inventory is running
- T3774: Failover relies on policy naming: <policy name> and <policy name_mirror>
- T4808: SPNs not updated for new authentication providers after Access Zone settings changed to “Use all authentication providers” (OneFS 7.2)
- T6229: Existing Failover Logs cannot be reviewed after upgrade to Eyeglass R2.0
- T14321 Zone/Pool Failover Readiness for AD Delegation validation, SPN Readiness validation not supported for Multi-Site failover configuration
- T15611 Pool Readiness Alarms are reported per Zone
- DNS Dual Delegation Failover Readiness Validation Supported DNS servers
- DNS Dual Delegation Failover Readiness validation uses PowerScale GroupNet DNS server
- T17254 Failover does not take into account Powerscale job retries
- T18556 User Quota Replication requires System Access Zone AD Provider
- T19681 Runbook Robot NFS Export not created on target cluster
- Known Limitations for Eyeglass Configuration Replication
- Multi-Path Exports
- T1359 Update NFS Multi-Path Export path(s) may cause transient Configuration Replication Error
- T1743 Multiple export with same path and same client do not show Configuration Replication Error
- T1847 OneFS 8 Overlapping Access Zone Replication has error
- T1972 Snapshot schedule replicated with offset
- T2046 Access Zone Replication limitation when all user mapping rules are deleted
- T2241 Incorrect missing SPN alarm issued when PowerScale cluster joined to multiple Domains

- T2779 - Eyeglass Configuration Replication “Full Sync Mode” always updates when Default Settings on Source and Target cluster are not the same
- T2780 Same host moved to different NFS Export Client list not updated on target
- T2908 New Eyeglass Configuration Replication Job cannot recover state and mode from the Eyeglass Fingerprint file.
- T4289 Delete Share or Export may result in temporary Audit error
- T5972 No Error Message for Duplicate NFS Export on OneFS 7.2 Configuration Replication Failed
- T14936 Short SPN not created during Configuration Replication
- T17097 Eyeglass Configuration Replication direction follows Enable/Disable state of SyncIQ policies
- Known Limitations for Eyeglass Features
- T2350: Quota Self Serve Portal: Local Group Quotas not displayed when logged in with Local Group User
- T1962: Default Role incorrectly shows Delete option
- T8362: Cluster Storage Monitor AD Group Template Quota Creation does not respect highest quota setting user quota in nested AD Groups
- T8193: special characters in Cluster storage monitor AD managed quota templates is not supported
- T9622: Unlock My Files! does not indicate error when PowerScale node is not reachable
- T15139 Data Config Migration Concurrent Jobs Limitation
- DR-136 Login with AD users leads to read-only Eyeglass
- Known Limitations for Eyeglass General
- T2289 Backup Archive Job is not always displayed in the Running Jobs window
- T2908 Renamed SyncIQ Policy does not link to RPO Reports from original SyncIQ Policy Name
- T3170 Pending Quota Requests are not preserved on failover

- T4579 Upgrade from 1.5.4 to 1.9 and greater Failover History retrieves Failover Log for SynclQ Job Reports
- T6300 After an Eyeglass restore with the -anyrelease option the print screen functionality for SynclQ Job Reports and Eyeglass backups may be in error
- T12034 Eyeglass appliance rediscover does not preserve Eyeglass Job state unless Configuration Replication has run
- T16137 Anyrelease restore does not restore all Ransomware Defender and Easy Auditor settings
- T16729 Role Based Access Control (RBAC) Known Limitations
- T16821 anyrelease restore restrictions for restore to 2.5.7
- Eyeglass Upgrade requires disk usage < 80%
- T19368 Copy to Clipboard Size Limitation
- For an Eyeglass installation with multiple clusters with different OneFS versions, adding or removing a cluster may result in temporary assignment of incorrect Effective Cluster Version. This is resolved the next time Configuration Replication runs.
- Known Limitations for REST API
- T18079 REST API - Change Eyeglass Configuration Job Disable/Enable must be done at same time as Job Type Change
- REST API retrieval of Jobs Known Limitation

What's New in Superna Eyeglass PowerScale Edition Release 2.5.9

What's New! In Superna Eyeglass PowerScale Edition Release 2.5.9 for DR can be found [here](#).

Supported OneFS releases

8.2.0.x

8.2.1.x

8.2.2.x

9.0

9.1

9.2.x

9.3

9.4.x.x

DR Edition Feature Release Compatibility

Feature	Source Cluster Release	Target SyncIQ Cluster Release
Configuration Replication non-DFS mode		
Configuration Replication	8.2.x.x	8.2.x.x**
Configuration Replication	9.0	9.0
Configuration Replication	9.1	9.1
Configuration Replication	9.2	9.2
Configuration Replication	9.3	9.3
Configuration Replication	9.4	9.4
Configuration Replication DFS mode		
Configuration Replication - DFS Mode	8.2.x.x	8.2.x.x
Configuration Replication - DFS Mode	9.0	9.0
Configuration Replication - DFS Mode	9.1	9.1
Configuration Replication - DFS Mode	9.2	9.2
Configuration Replication - DFS Mode	9.3	9.3
Configuration Replication - DFS Mode	9.4	9.4
SyncIQ Policy Failover non-DFS mode		

SyncIQ Policy Failover	8.2.x.x	8.2.x.x
SyncIQ Policy Failover	9.0	9.0
SyncIQ Policy Failover	9.1	9.1
SyncIQ Policy Failover	9.2	9.2
SyncIQ Policy Failover	9.3	9.3
SyncIQ Policy Failover	9.4	9.4
SyncIQ Policy Failover DFS mode		
SyncIQ Policy Failover - DFS mode	8.2.x.x	8.2.x.x
SyncIQ Policy Failover - DFS mode	9.0	9.0
SyncIQ Policy Failover - DFS mode	9.1	9.1
SyncIQ Policy Failover - DFS mode	9.2	9.2
SyncIQ Policy Failover - DFS mode	9.3	9.3
SyncIQ Policy Failover - DFS mode	9.4	9.4
Access Zone Failover		
Access Zone Failover	8.2.x.x	8.2.x.x
Access Zone Failover	9.0	9.0
Access Zone Failover	9.1	9.1
Access Zone Failover	9.2	9.2
Access Zone Failover	9.3	9.3
Access Zone Failover	9.4	9.4
Runbook Robot cluster pairs SyncIQ Policy Failover		
SyncIQ Policy Failover	8.2.x.x	8.2.x.x
SyncIQ Policy Failover	9.0	9.0
SyncIQ Policy Failover	9.1	9.1
SyncIQ Policy Failover	9.2	9.2
SyncIQ Policy Failover	9.3	9.3
SyncIQ Policy Failover	9.4	9.4
Runbook Robot* cluster pairs Access Zone Failover		
Access Zone Failover	8.2.x.x	8.2.x.x

Access Zone Failover	9.0	9.0
Access Zone Failover	9.1	9.1
Access Zone Failover	9.2	9.2
Access Zone Failover	9.3	9.3
Access Zone Failover	9.4	9.4
Data Config Migration		
Data Config Migration	9.0	9.0
Data Config Migration	9.1	9.1
Data Config Migration	9.2	9.2
Data Config Migration	9.3	9.3
Data Config Migration	9.4	9.4
Live Ops - DR Test Mode		
Live Ops DR Test Mode	9.0	9.0
Live Ops DR Test Mode	9.1	9.1
Snapshot Schedules	9.0	9.0
Snapshot Schedules	9.1	9.1
Snapshot Schedules	9.2	9.2
Snapshot Schedules	9.3	9.3
Dedupe Path Settings	8.0.x.x	8.0.x.x
Dedupe Path Settings	8.2.x.x	8.2.x.x - pending testing

**** Inter-version capabilities: In the case of inter-version operation, the capabilities of the lower OneFS API version will be applied across both OneFS versions. Capabilities of the higher OneFS version that are not present in the lower OneFS version will not be available.**

Feature Support Matrix

Description	Supported
-------------	-----------

Overlapping Access Zone with System (/ifs)	
Configuration Replication (non DFS mode)	Yes - Create / Update No - Delete
Configuration Replication (DFS mode)	Yes - Create / Update No - Delete
SynclQ Failover	Yes
SynclQ Failover - DFS Mode	Yes
Access Zone Failover	No
Overlapping Access Zone - non System Zones	
Configuration Replication (non DFS mode)	Yes - shares / export / alias No - Access Zone
Configuration Replication (DFS mode)	Yes No - Access Zone
SynclQ Failover	Yes
SynclQ Failover - DFS Mode	Yes
Access Zone Failover	No
Runbook Robot Access Zone Multi cluster	No (only cluster pairs with no common cluster)
Failover with SynclQ Encryption (Access Zone, SynclQ, DFS, IP pool failover modes)	Yes (8.2 or later only)

End of Life Notifications

End of Life Notifications for all products are available [here](#).

Support Removed in Eyeglass Release 2.5.8

Following feature are no longer available in 2.5.8 as published in the 2.5.7 deprecation notice:

- a. Support for OneFS 8.0.x.x releases removed
- b. Support for OneFS 8.1.x.x releases removed
- c. snmp forwarding 2.5.8.1 release

Deprecation Notices

Currently no deprecation notices.

New and Fixed in Eyeglass Release 2.5.8

New in 2.5.8

1. Deprecated Feature notification

- a. DR Test mode 6 month notice on deprecation. This feature was temporary until writeable snapshot were available. No enhancements to this feature with end of support in the next 6 months.
- b. Replacement solution:
 - i. Onefs 9.3 or later
 - ii. Feature Overview: On demand DR testing with copy on first write writeable snapshots enable a new workflow that is faster, consumes less storage and is available on demand.
 - iii. Selection of an IP pool with no access zone attached , will allow a temporary access zone created for the DR test. A source path of data is selected to test with and a snapshot is created on this path. A new access zone is automatically created and attached to the IP pool and all shares, exports and quotas are cloned into the temporary access zone.
 - iv. A writable snapshot is created in the temporary access zone
 - v. Testing can begin in seconds and only consume space for writes.
 - vi. Test completes and option to clean up the temporary access zone.

2. Cluster Usage Icon

- a. This feature will be deprecated with many options to get disk utilization on the cluster. This functionality will be deprecated.

3. SNMP alarm forwarding

- a. This is a legacy protocol and will be removed from the product. syslog, webhooks, email, rest api should be used for alarm forwarding.

New in 2.5.8.1-22116

Refer to previous 2.5.8.1 builds for what's new.

Fixed in 2.5.8.1-22116

Refer to previous 2.5.8.1 builds for what's new.

New in 2.5.8.1-22100

Refer to previous 2.5.8.1 builds for what's new.

Fixed in 2.5.8.1-22100

Refer to previous 2.5.8.1 builds for what's new.

New in 2.5.8.1-22080

T20905 Log Parser

Log Parser functionality now available from the Eyeglass desktop that can be used to generate detailed log parsing analysis of DR Edition, Ransomware Defender, Easy Auditor. More information can be found in the documentation [here](#).

Fixed in 2.5.8.1-22080

T21800 Swap file created on Upgrade

Unnecessary swap file created on upgrade on OpenSUSE 15.3 impacts available disk space.

Resolution: Upgrade to 2.5.8.1 on OpenSUSE 15.3 no longer creates the unnecessary swap file. Note that if the swap file already exists the upgrade will not remove it.

T22819 2.5.8 rollback DFS policy when resync prep timed out is incorrect it should not rollback ever

If resync prep step times out or fails a DFS mode failover will roll back SMB share renames when it should not. Rollback should only execute with allow writes failures.

Resolution: Rollback only executes on allow writes failure. Failover log now shows rollback step properly for resync prep failure: Rollback Renaming Shares - was skipped because failover succeeded or proceeded far enough to be successful

New/Fixed in 2.5.8-22028

T22205 RAM Alarm calculation now based on total number of clusters managed

In previous releases RAM Alarm limits were applied per cluster. Now they are applied against all clusters managed. For example, if there is a limit of 5000 objects managed and 2 clusters are managed each with 3000 objects, the alarm will apply.

New in 2.5.8-21330

Refer to previous 2.5.8 builds for what's new.

Fixed in 2.5.8-21330

Security

T22171 - Log4j Vulnerability - Upgrade to Log4j 2.17.0 (2.5.8-21330 and higher Log4j 2.17.0)

New in 2.5.8-21306

NEW - see What's New in 2.5.8 [here](#).

NEW - Failover

T17849 DNS Dual Delegation Failover Readiness Validation disabled

Access Zone / IP Pool Failover Readiness Validation for DNS Dual Delegation is now disabled by default. Verify DNS Dual Delegation manually. In a future release this validation is planned to be provided on demand.

NEW - OneFS 9.3 Support

Support for OneFS 9.3 is introduced in release 2.5.8

NEW - Cluster Storage Monitor new schedule for quota creation

If using the Cluster Storage Monitor AD Group template for creating quotas, they are now assessed and created on the quota collection schedule instead of on the Configuration Replication cycle.

Fixed in 2.5.8-21306

Security

T22033 Log4j Vulnerability - CVE-2021-44228

Resolution: log4j version updated to 2.15.0 which has patch for the vulnerability.

T20584 Eyeglass service account password exposed on error connecting to Powerscale

In the case where there is an error connecting to the Powerscale, for example a timeout or session expired, the eyeglass service account password appears in plain text in the error log and /var/log/messages files.

Resolution: Eyeglass service account password no longer is exposed.

Failover / Configuration Replication

T20628 Cannot disable Zone/IP Pool Readiness AD Delegation Validation (2.5.7.1 and higher)

In 2.5.7.1 and higher, when the AD Delegation validation is disabled the AD Delegation validation steps continue to run. The Zone / Pool Readiness GUI correctly does not show the validation and any error that occurs is not rolled up to the overall readiness status but an alarm is send related to the failed step. This does not impact ability to failover.

Resolution: Validation steps no longer run if the validation is disabled.

T16888 Configuration Replication fails if SynclQ Policy source and target path are different and SynclQ policy path contains special character

For the case where a SynclQ Policy path contains a special character and the SynclQ Policy source and target path are different, configuration replication fails for the associated Eyeglass job with the AEC code AEC_NOT_FOUND.

Resolution: Configuration Replication job is now able to replicate shares and exports where SynclQ policy has a different source and target path and path has a special character.

Features

T9652 Unlock My Files inconsistent handling for unreachable PowerScale cluster

For the case where Eyeglass is managing multiple clusters and one or more clusters are unreachable, the Unlock My Files sometimes displays the error "Failed ot search:","Communication failure or timeout searching for open files. Please try again later or try to be more specific in your query.". without displaying results for reachable cluster or may provide results for reachable clusters without providing the error.

Resolution: Unlock My File now requires selection of one cluster at a time for searching.

General

T19288 Custom Postfix email settings not restored

After a backup and restore, custom Postfix email settings are not restored.

Resolution: Backup and restore now restores custom Postfix email settings.

T19275 Syslog alarm forwarding configuration not restored

After a backup and restore, Syslog alarm forwarding settings are not restored.

Resolution: Backup and restore now restores syslog alarm forwarding settings are restored with backup created as of 2.5.8. Backups created in previous versions do not contain the file and the syslog alarm forwarding configuration will need to be manually backed up fro the original Eyeglass appliance off appliance.

Technical Advisories

Technical Advisories for all products are available [here](#).

Known Issues

Failover

T22819 2.5.8 rollback DFS policy when resync prep timed out is incorrect it should not rollback ever

If resync prep step times out or fails a DFS mode failover will roll back SMB share renames when it should not. Rollback should only execute with allow writes failures.

Work around: rename the shares on the DR cluster and remove the igls-dfs prefix and apply the igls-dfs on the source cluster SMB shares related to the synciq policy SBM shares that are named as rolled back.

2666/2723: Problems for Controlled Failover when Source becomes unreachable during failover

In a Controlled Failover where requirement is that Source cluster is reachable, should the Source cluster become unreachable during the failover an error will occur on the failover job but it is possible that no failover log will be generated.

If the Source becomes unreachable after Failover Wizard validation but before the Failover starts, a log is generated with 1 line that states success. The Running Jobs window has no details

Workaround: None available

2278: Zone Readiness lists Access Zone after all related SyncIQ Policies are deleted

For the case where an Access Zone which initially had associated SyncIQ Policies and then all SyncIQ Policies are deleted, the Access Zone will incorrectly appear in the Zone Readiness view with a Status of UNKNOWN.

Workaround: None required. This entry can be ignored.

2919: Eyeglass Configuration Replication Jobs may not display in the Zone Readiness Eyeglass Configuration Replication Readiness list

If an Eyeglass Configuration Replication Job has no associated shares, exports, alias or quotas, the Job will not be displayed under Eyeglass Configuration Replication Readiness if the SyncIQ OneFS Readiness is WARNING.

Workaround: None Required. Failover will run all logic and policies as expected.

3010: Unexpected results for failover where total number of objects exceeds the published limit

Running an Eyeglass assisted failover where the total number of objects exceeds the published maximum limit will lead to unexpected results.

Workaround: Review published limits and do not use Eyeglass assisted failover if your system exceeds the published limit.

Please refer to the Eyeglass Admin Guide for published limits [here](#).

3029: Zone Readiness not calculated correctly for SyncIQ subnet pool with a mapping hint

The subnet:pool which are provisioned against SyncIQ Policies for the Restrict Source Nodes option require an igls-ignore hint for Access Zone Failover to prevent the networking in the pool from becoming failed over during an Access Zone Failover. If there is an Eyeglass igls- mapping hint assigned to these subnet:pool which could result in the networking being failed over Zone Readiness either does not show an error OR it may show the error that mapping is incomplete.

Workaround: Only configure igls-ignore hint on subnet:pool that is provisioned against SyncIQ policy for the Restrict Source Nodes option.

3031: Zone Readiness Policy Path Containment Check results in extra errors

Zone Readiness for an Access Zone which does not meet SyncIQ Policy path requirement "SyncIQ Policy(s) source root directory must be at or below the Access Zone Base Directory" may in errors for every validation category, with the message "Cannot calculate Access Zone Failover Readiness for a zone with no pools".

Workaround: To resolve the error, ensure that the Policy Path Containment Requirement is met.

Eyeglass Assisted Access Zone Failover Requirements are documented in the Access Zone Failover Guide [here](#).

3077: Zone Readiness does not catch pool mapping hint misconfiguration for partial string match

Zone Readiness: Smartconnect Zone Failover Mapping Readiness validation does not detect a pool mapping error when there is a partial string match. For example:

cluster A Smartconnect Zone Mapping Hint = igls-pool

cluster B Smartconnect Zone Mapping Hint = igls-pool1

Readiness check from A to B does not detect the error. Readiness check from B to A shows an error that no mapping is available.

Workaround:

- Ensure that your Smartconnect Zone Mapping Hints are identical for mapped pools

T477: No Policy Hot/Hot Validation Error for policy with no share/export

Zone Readiness incorrectly shows Policy Hot/Hot Validation as OK in an environment where there are one or more policies in the Access Zone which do not have any file sharing objects (shares or exports).

Workaround: Add a file sharing object under the SyncIQ Policy path.

T482: Zone Readiness shows OK for multiple Smartconnect Zone Mapping errors

In the case where Smartconnect Zone Mapping contains many errors such as multiple hints or combination of hint and igls-ignore on both clusters, the mapping error may only show for one of the clusters instead of both clusters.

Workaround: Provision Smartconnect Zone Mapping according to requirements documented [here](#).

T654: Zone Readiness incorrectly includes SyncIQ Policy in System Access Zone

For the case where a SyncIQ Policy source path corresponds to a non-System Access Zone path (path is at or below the Access Zone path) but there is a share protected by that policy in the System Access Zone, the SyncIQ Policy incorrectly is evaluated for Zone Readiness in the System Access Zone.

Workaround: None required. This policy can be ignored in the System Access Zone as in this configuration the System Access Zone cannot be failed over.

T1712: Zone Readiness missing Zone when pool has no SmartConnect Zone - OneFS 7

In OneFS 7 When a subnet pool is associated with an Access Zone and does not have a Smartconnect Zone, the Access Zone is not displayed in Eyeglass Zone Readiness window. With OneFS 8 there is an entry in Zone Readiness with appropriate error.

Workaround: Create SmartConnect Zone for the pools associated with the Access Zone that you want to failover.

T1716: Eyeglass Runbook Robot NFS mount not functioning for RHEL and Centos deployments

If Eyeglass is deployed on a Redhat or Centos operating system the Eyeglass Runbook Robot pre and post failover check for file system read/write by making an NFS mount does not work.

Workaround: Disable the Runbook Robot mount step by setting to false following the instructions here:

<http://documentation.superna.net/eyeglass-PowerScale-edition/igls-administration/eyeglass-administration-guide#TOC-Runbook-Robot-Mount-Export-Enable-Disable>

Manually check read/write status of filesystem.

T1482: Zone Readiness SyncIQ Readiness not updated after Access Zone associated to a pool

For the case where initially an Access Zone with a policy is not associated with a pool, the policy appears in Zone Readiness/SyncIQ Readiness under the System Access Zone. Once the Access Zone is associated with the pool the Policy remains associated with the System Access Zone.

Workaround: None Available. This is a display issue and the policy will failover if the access zone it is a member of is failed over.

T3742: No Policy Hostname Validation error if SyncIQ Policy Target Host is fully qualified and uses short name on target cluster pool that has a Superna Eyeglass mapping hint applied

If the pool on the target cluster which contains the SmartConnect Zone which is configured on the source cluster as the SyncIQ policy target host is configured as "short" name instead of fully qualified name AND that pool has a Superna Eyeglass mapping hint defined instead of the required igls-ignore hint, Zone Readiness INCORRECTLY does not show an error.

Workaround: Use fully qualified domain name for SyncIQ Policy target host and in the pool SmartConnect Zone name.

T3848: SPNs not updated during failover for OneFS8 non-default groupnet AD provider

For the case where OneFS 8 is configured with multiple groupnet and different AD provider between groupnets, the SPN update during failover does not succeed for non-default groupnet AD providers.

SPN are not deleted for source cluster and are not created for the target cluster. The failover log indicates success. This is due to a OneFS8 defect with multiple AD providers and isi commands.

SPN delete / create for the AD provider defined in groupnet0 is successful.

Workaround: Manually delete and create the SPN for the Smartconnect Zones that were moved from AD ADSI Edit interface.

T4009: SPNs creation case sensitive to AD provider name

If you have domain name in lowercase but smartconnect zone name has upper case domain name then in that case Eyeglass does not add the SPN Host automatically .

Workaround: AD provider name and AD provider in SmartConnect Zone name should have same case.

T4320: Access Zone not assigned to any Subnet Pools results in many Zone Readiness Errors

Zone Readiness error for an Access Zone that is not assigned to any Subnet Pool has multiple rows displayed in the DR Dashboard - 1 per Subnet Pool on the PowerScale Cluster.

Workaround: Associate the Access Zone with at least 1 Subnet pool.

T4316: Runbook Robot Policy Job does not display SyncIQ Job Reports

Runbook Robot job creates 2 failover history records - one for policy failover or access zone failover and one for for Runbook Robot. The Runbook Robot SyncIQ Reports log incorrectly repeats the Failover log information instead of showing the associated SyncIQ Job reports.

Workaround: View the associated Policy or Access Zone Failover results to retrieve the SyncIQ Job Reports.

T4857: Failed SmartConnect Zone Rename step is not displayed in Failover Log

Access Zone Failover which fails at the SmartConnect Zone rename step shows a Major Error in the “Networking updates during failover Job” section of the Failover Log but does not show the actual rename step which failed.

```
INFO Raised alarm: MAJOR Access Zone Failover Job failed.  
ERROR ***** Networking updates during failover Job FAILED *****
```

Workaround: Contact Support to assist in determining the rename operation which caused the error.

T4878: Pool Failover - Non Runbook Robot SyncIQ policies can be mapped to Robot pool

Pool failover is not supported for Runbook Robot but pool readiness SyncIQ policy mapping does not block user from mapping a non-Runbook Robot policy to the Runbook Robot pool. This configuration will cause an error during the Runbook Robot job.

Workaround: Do not configure Pool Failover for the Eyeglass Runbook Robot Access Zone.

T4968: Zone missing from DR Dashboard Zone Readiness tab if a SyncIQ Policy has a target host that cannot be resolved

When an Access Zone contains a SyncIQ Policy which has a Target Host configured which cannot be resolved by Eyeglass, the Access Zone does not appear in the DR Dashboard Zone Readiness tab.

Workaround: Ensure that all SyncIQ Policy Target Host can be resolved by Eyeglass. To verify, ssh to the Eyeglass appliance and test with nslookup <target host> to confirm that it can be resolved.

T5092, T4490: Access Zone Pre and Post Failover Scripting Issues

- There is no specific option to create Pre or Post Failover scripts for a Pool Failover. If there are existing Pre or Post Failover scripts for Access Zone failover those same scripts will be run during pool failover.
- In a multi-pool setup, the failover log may report an error related to executing the post failover script even though the script succeeds.
- Running the Test run script, for Access Zone Failover, Test Run script only shows "loading" status

Workaround: Ensure that any Access zone failover scripts also apply to pool failover if both are configured. Verify manually whether a script has succeeded.

T5473: Zone/Pool Readiness Pool Mapping Hint Matching Issue

Readiness logic to determine whether 2 pools are mapped for Access Zone or Pool failover will map based on partial match instead of an exact match. For example a pool with the mapping hint "igls-8" on the source will match any mapping hint on the target that begins with "igls-8" - for example, "igls-8a", "igls-8b", "igls-8c" etc. This may cause an issue if there are multiple pools on target side which match. It will also cause an issue after failover as the target hint (for example "igls-8a") will not match the source hint (for example "igls-8").

Workaround: When provisioning pool mapping hints, use unique string that do not overlap between pools - for example, igls-1, igls-2, igls-3 instead of igls-1, igls-1a, igls-1b.

T5961: Failover Log shows Incorrect Final Steps

The Failover log always contains following Final steps even when not required:

1. Networking Rollback Steps are incorrectly displayed at end of failover for a failover where Networking Client Redirection steps were not executed.
2. Transfer pool mapping step are incorrectly displayed for non-pool based failovers.

Workaround: In the above conditions these messages can be ignored as they do not apply.

T5897: Post Failover Inventory step may fail during multiple concurrent failovers

When multiple failovers are initiated in parallel and running concurrently the Post Failover Inventory step may fail if the same step is running for one of the concurrent failovers. This leaves the failover in a Failed state.

Workaround: None Required. This step will be completed successfully on a subsequent failover or during regular Configuration Replication to bring the Eyeglass up to date on the latest state of the PowerScale environment. The Failover log must be consulted to determine state of other failover steps such as Client Redirection, Make Writeable and Preparation for Failback.

T5941: Pool Failover Failover Log Summary incorrectly displayed Client Redirection step not run

For Pool Failover, the Failover Log Summary displays the Client Redirection step as not having run:

Client Redirect : This step did not run

When the step in fact did run.

Workaround: Check this section in the Failover Log to determine the status of the Client Redirection steps:

```
INFO ***** Networking updates during failover Job STARTED *****
```

T5967: Failover where Quota Sync is disabled has extra lines in Failover Log

The Failover Log for a failover where Quota Sync is disabled displays the following line multiple times instead of just once:

```
PLEASE RUN QUOTA FAILOVER JOBS MANUALLY
```

Workaround: None Required.

T5934: Access Zone Readiness shows OK for DFS only failed over Access Zone

Zone Readiness status for Access Zone which only has DFS policies will show OK as the overall status for the failed over direction instead of Failed Over status.

Workaround: Check which cluster has enabled SyncIQ Policies and then verify that other cluster is read-only to confirm which failover direction is active.

T6289: SyncIQ policy with no shares or exports is associated with the System Access Zone for failover

A SyncIQ policy which does not have any associated shares or exports at or underneath the policy path will be associated with the System Access Zone for Access Zone or Pool Failover instead of the Access Zone that the SyncIQ policy falls at or under.

Workaround: Create a file sharing object at or underneath the SyncIQ Policy path and in the Access Zone under which the SyncIQ Policy falls.

T6311: Selecting the DR Failover Status link on the DR Assistant Summary page may result in an Error

Selecting the DR Failover Status link on the DR Assistant may result in following error: No policy data has been provided, cannot execute request.

This error does not block the failover from proceeding.

Workaround: Open the DR Dashboard and review the DR Failover Status here.

T6402: Access Zone Failover Post Failover Inventory step runs multiple times

When an Access Zone contains multiple SyncIQ Policies and those policies have been configured in Eyeglass for different Job types (DFS or AUTOSKIPCONFIG), the failover Post Failover Inventory runs for each Eyeglass Job type in the Access Zone instead of just once.

Workaround: None Required. While this increases the failover time to include completion of multiple post failover inventories, the critical failover steps for client redirection, make writeable and preparation for fallback are completed prior to this step. These steps are required to complete in order to place a new mirror policy into the corresponding DFS or AUTOSKIPCONFIG state.

T6842: Zone Readiness: Zone does not display Failover Over state for Access Zones where custom SmartConnect Zone prefix is being used

For Eyeglass deployments where the SmartConnect Zone prefix used to disable SmartConnect Zones on failover has been customized to not use the default igls-original prefix the DR Dashboard does not display Failed Over status for the inactive Access Zone failover direction.

Workaround: None Required.

1. This is a display issue only and does not block failover.
2. This issue does not affect SmartConnect Zone rename during failover.
3. While the DR Assistant allows you to select a failover in the wrong direction (inactive -> active) it is blocked further along in the Failover Wizard due to no enabled policies.

T7184: Pool Readiness: Pool to SyncIQ Policy Mapping is not displayed in DR Dashboard until Readiness task is run

Pool to SyncIQ Policy mapping is not displayed in DR Dashboard Pool Readiness view until a Zone / Pool Failover Readiness task has been run.

Workaround: None Required. This is a display issue only - the mapping is successfully saved and displayed after the next readiness task has run.

T8824: User Quota creation fails on failover for multiple disjointed AD Domain environment

In an PowerScale environment that is configured to use multiple AD Domains and those Domains are not joined, user quota creation for the quotas related to the non-default AD Domain will fail with the error:

Requested persona was not of user or group type

Workaround: None available with Eyeglass.

T10363 Overlapping Access Zone Failover blocked for System Access Zone

For the case where there are multiple access zones overlapping with System Access Zone on /ifs path, DR Assistant will show an error during navigation indicating an invalid configuration and block completion of failover.

Workaround: SyncIQ Policy failover with manual client redirection.

T10912 Quota Sync fails for quotas where quota container property set to true

Smartquotas in OneFS configured with the container property set to true fail to be created by quota sync.

Workaround: None available. Quota must be created manually.

T10935 Pool failover "failovertarget" must be "zone id"

The "failovertarget" field must be "zone id" even though description indicates "ID of the access zone OR syncIQ policy to failover".

Workaround: Enter "zone id" for "failovertarget" when initiating pool failover.

T7622 Eyeglass will not add custom SPNs if PowerScale Cluster does not return any missing SPN during SPN check (as of 2.5.6)

As of 2.5.6 Eyeglass can manage custom SPN creation based on Eyeglass configuration - additional information available [here](#). If PowerScale does not identify any missing SPNs Eyeglass Configuration Replication will not insert custom SPNs. If PowerScale identifies any missing SPN, Eyeglass will insert all custom SPN even if PowerScale does not identify it as missing.

Workaround: SPNs to be added manually if required. For failover, no additional steps - failover will manage all SPN updates based on custom SPN definition.

T13360 Failover Readiness Validation for Corrupt Failover Snapshots does not check for missing snapshot

There must be one failover snapshot on the target cluster per SyncIQ policy being failed over. The Corrupt Failover Snapshots validation does not check whether that snapshot is missing. Impact: Allow Writes step of failover will fail.

Workaround: Verify presence of snapshot manually on target cluster

```
isi snapshot snapshots list | grep <SyncIQ Policy Name>
```

Replacing SyncIQ Policy Name iwth your our SyncIQ Policy Name

example for expected configuration

```
isi snapshot snapshots list | grep policy1
```

T12434 Concurrent Access Zone or Pool Failover with DFS configured policies may fail DFS share rename step

When doing concurrent Access Zone or Pool Failover where the Access Zone or Pool have associated jobs in Eyeglass DFS mode the share renaming step may happen in parallel and depending on the OneFS release an PowerScale OneFS API defect may incorrectly handle the request causing the share rename to be in error.

Workaround: Verify with Dell EMC support whether your OneFS version has this issue. For any shares where share renaming fails they will have to be renamed manually - the failover log will indicate which failed and which succeeded.

T13701 Failover option "Disable SyncIQ Jobs on Failover Target" does not reapply schedule

When the failover option "Disable SyncIQ Jobs on Failover Target" is selected the synciq policy schedule is not reapplied to the active synciq policy on the target cluster.

Workaround: The original SyncIQ policy schedule is captured in the failover log. Reapply the schedule to the policy manually on the PowerScale.

T13726 Pool Failover error mapping policy to pool on target cluster for disabled job

If Pool Failover is initiated and there is an associated Eyeglass Configuration Replication job that is disabled, the failover correctly skips failover of the associated synciq policy / data but incorrectly attempts to associate the mirror policy to a pool on the target cluster resulting in an error for the step "Transfer pool mapping" with message "Could not find policy".

Workaround: None required failover has been completed successfully for policies which were enabled. No impact to failback.

T13881 Cannot failover overlapping Access Zones - rel 2.5.6

In Release 2.5.6 overlapping Access Zones cannot be failed over. The network updates that are done during failover are rolled back.

Workaround: Use Release 2.5.5 to failover overlapping access zones

T14398 Zone/Pool Failover Readiness FQDN Alias validation incorrectly reports OK when pool does not have an ignore hint

For case where PowerScale cluster has been provisioned in Eyeglass using FQDN, that FQDN should not be failed over during Zone or Pool failover - it needs to remain associated with its current cluster. This is achieved by configuring the associated IP pool to be "ignored" during failover. The validation that checks whether this configuration is in place incorrectly indicates OK when the "ignore" is not configured.

Note that as of Eyeglass 2.5.3 and higher clusters no longer being added to Eyeglass using FQDN due to PowerScale CSRF not compatible with Smartconnect and API services.

Workaround : If cluster still added to Eyeglass using FQDN modify to be added using IP. Please following [Technical Advisory #17](#) and [Technical Advisory #22](#).

T14931 Policies configured for Pool failover allowed to do DFS or SyncIQ failover until next configuration replication runs

Policies configured for pool failover are blocked from being failed over in DFS or SyncIQ mode except for period of time between when pool to policy mapping for Pool Failover has been completed and next Configuration Replication cycle has completed.

Workaround: None required - Do not initiate DFS or SyncIQ mode failover for policies configured for pool failover. Next schedule Configuration Replication job will rectify and after that point the DFS and SyncIQ failover mode will not be available for policies configured for Pool Failover.

T14948 Failover log for Uncontrolled Access Zone incorrectly logs status of final readiness job and changes to pool aliases

The failover log for an uncontrolled Access Zone failover will incorrectly report the status of the final failover readiness step as SUCCESS instead of error and will incorrectly summarize the Pool aliases on source after failover and Pool aliases on destination after failover at the end of the log.

Workaround: None required, this is a logging issue only. The failover correctly logs client redirection steps in the Networking updates section of the log which records the changes as they are being executed. The failover readiness status can be viewed on the DR Dashboard / Zone Readiness.

T14965 Failover readiness SyncIQ File Pattern Validation has WARNING state instead of ERROR

Failover readiness SyncIQ File Pattern Validation which detects that SyncIQ policy has file patterns should be ERROR instead of WARNING as PowerScale OneFS Resync Prep function that prepares you for failback will fail when SyncIQ is configured this way.

Workaround: This setting should not be used for DR purposes.

T14971 DR Assistant validation check screen incorrectly requests acknowledgement of readiness warnings

For case where DR Failover status is OK or Info, the DR Assistant Failover wizard validation check step requests acknowledgement that warnings have been reviewed even though DR failover status has no warning status.

Workaround: Close the DR Assistant window and open the DR Dashboard window and confirm that indeed failover status has no Warning states. If so, start the failover again and now select the "I have reviewed the warning status" check box and continue with the failover.

T14974 Access Zone Failover with error on DFS share renaming will abort for all policies

For the case where an Access Zone has both DFS and non-DFS configured jobs in Eyeglass, if share renaming fails for all shares associated with a DFS policy Client redirection will be considered an error for non-DFS policies as well and failover will be aborted instead of continuing for non-DFS configured jobs.

Workaround: Share renaming issue should be resolved before re-attempting the failover.

T14988 Eyeglass GUI incorrectly allows pool failover configuration for a policy that is active in failover rehearsal mode

From the Eyeglass DR Dashboard you are allowed to map a policy for pool failover when it is in active rehearsal mode even though you cannot initiate a failover when it is in this state.

Workaround: Review policy status and confirm not in rehearsal mode before configuring pool failover.

T15000 DR Rehearsal status lost if fingerprint file deleted

A fingerprint file is used to persist DR Rehearsal status. If the fingerprint file is deleted or otherwise removed while rehearsal mode is active, rehearsal status is lost and there is no way to revert rehearsal mode.

Workaround: Please contact support at support.superna.net to recover from this state.

T15042 REST API policy readiness is missing output for Target Reachability check

The SyncIQ policy readiness retrieved using REST API is missing the output for the Target Reachability check. If the Target Reachability validation fails, the overall Failover Status is correctly in ERROR and failover cannot be initiated

Workaround:

- To assess target reachability:
 - Target reachability alarms related to Inventory or Configuration replication would have been sent.
 - From the Eyeglass web interface, Eyeglass / PowerScale reachability can be viewed from the Continuous Operation Dashboard.
- All failover readiness criteria can be viewed from the Eyeglass web interface DR Dashboard.

T15010 DR Rehearsal Revert not blocked for Pool Failover mode when in REHEARSAL_ERROR

If after enabling DR Rehearsal mode for Pool Failover the DR failover status is REHEARSAL_ERROR the failover wizard incorrectly allows you to initiate a revert for rehearsal mode.

Workaround: To recover from this REHEARSAL_ERROR open a support ticket at support.superna.net for assistance.

T15609 Alarm time not updated for repeated policy/dfs/zone/ pool readiness alarms

If a policy, dfs, zone or pool readiness alarm occurs multiple times, the Alarm time will not be updated with each occurrence. It will display only the first time the alarm is raised. Email notification also only sent on initial occurrence of the alarm. Subsequent occurrences will not send an email.

Workaround: Open the DR Dashboard to see the current state of the validations as of the last time the Zone/Pool Readiness job has run.

T15191 Failover Log may show 2 summaries when Rehearsal Mode enabled

When Rehearsal Mode is enabled for an Access which has DFS policies or enabled with multiple pools which also have DFS, the failover log summary shows an interim summary after data access steps and a final summary at end.

Workaround: None required - summary has required information.

T15192 Rehearsal Mode not disabled for Access Zone associated with Pool Failover

From the DR Dashboard, the Access Zone associated with a Pool Failover already active in Rehearsal Mode can be selected for enabling Access zone Rehearsal Mode again even though this is not a valid configuration for Rehearsal Mode.

Workaround: None Required, the next window in DR Assistant identifies the invalid configuration and correctly blocks Rehearsal Mode enabling for the Access Zone.

T15248 Error in DFS failover does not rollback share renaming when failover job includes multiple policies

A DFS failover which contains multiple policies will not rollback share renaming for a policy that encounters an error if the remaining policies succeed.

Workaround: Use PowerScale interface to remove and add igls-dfs prefix for affected shares.

T15260 DFS Failover share renaming rollback not done when all share rename fails on source cluster

If client redirection step of failover which adds igls-dfs prefix to shares on the source cluster fails for all of the shares associated with the source cluster the failover stops but the share renaming that completed successfully for the target cluster is not rolled back.

Workaround: Use PowerScale interface to add igls-dfs prefix to shares on the target cluster.

T15271 Zone/Pool Failover error in SMB Data Integrity step or run policy step incorrectly attempts to roll back networking

If the initial share lockout for SMB Data Integrity step fails or run policy step fails, the failover is aborted as expected but then steps are executed to roll back networking changes even though none were made. There is no impact other than error in failover log as these commands fail as they are attempting to update to configuration that already exists on the cluster.

Workaround: None required - the commands executed do not result in any changes on the PowerScale cluster.

T15278 Pool Failover job with multiple pools stops failover steps for all pools on DFS share renaming error

If an error which will abort failover occurs for DFS share renaming on one pool where the failover job contains multiple pools, failover will be aborted for all pools instead of continuing for pool which has no error.

Workaround: When failing over multiple pools, execute concurrent failover with 1 pool per failover job.

T15290 Pool Failover job with multiple pools does not rollback client redirection when allow writes step fails

If an error occurs on allow writes for one pool in a failover job that contains multiple pools there is no rollback for networking for failed pool.

Workaround: Networking can be failed back manually using PowerScale interface and using Failover log as a guide. Also can failover multiple pools concurrently with 1 pool at a time.

T15298 Quota job run manually after failover may delete quotas on source cluster

Even if quota failover steps fail on failover from cluster A to cluster B such that no quotas are created on cluster B and all quotas exist on cluster A, the quota failover job from cluster B -> A is created and enabled. If this Quota job is run manually it will delete all related quotas on the source (cluster A) leaving you without related quotas on source or target.

Workaround: Do not run quota jobs manually. Contact support.superna.net for assistance to failover quotas that failed during failover.

T15530 Policy or DFS Readiness may incorrectly evaluate Policy Hostname validation in error

DR Dashboard / DR Assistant Policy Readiness or DFS Readiness may incorrectly evaluate Policy Hostname validation in Error state placing overall failover status in Error. This validation should only be being assessed for Access Zone or Pool failover.

Workaround: Follow steps for Access zone failover configuration to ignore failover for the pool that has the Target Host. Steps to do this are on the target cluster apply "igsl-ignore" hint on the pool which has the SyncIQ Policy Target Host. Ignore hints are simply an alias with the name of "igsl-ignore". Note it is best practise to ensure unique hints by using a naming format that uses cluster name - for example: igsl-ignore-<clustername>. Documentation reference can be found [here](#) - see section on ignore hints.

Once configured run the Eyeglass Configuration Replication Job to update DR Dashboard / DR Assistant.

T15547 Failover Readiness Domain Mark Validation fails for path with spaces or special characters

The Failover Readiness Domain Mark Validation returns an error for SyncIQ policy source path that has a space or contains special characters.

Workaround: Manually confirm presence of domain mark by running command on PowerScale: `isi_classic domain list`. DR Failover Status of Warning does not block failover. For additional information on readiness validations in Warning state please refer to our documentation [here](#) or contact support.superna.net.

T15610 Policy Readiness Pool Mapping Validation alarm and email indicate Warning severity instead of Error

For the cases where an Access Zone is configured for Pool Failover and there are policies which are not mapped to pools the Un-Mapped Policy SmartConnect/IP Pool Status alarm and email incorrectly indicate that this is a Warning level issue. The DR Dashboard correctly identifies the issue as an Error which would block initiating a failover.

Workaround: Review readiness from the DR Dashboard directly.

T15613 DR Rehearsal Readiness - no alarm or email when DR Rehearsal status changes from OK to Warning or Error

No Alarm is raised or email sent when DR Rehearsal readiness status changes from OK to Warning or Error status.

Workaround: Login to the Eyeglass GUI and open the DR Dashboard to review readiness.

T15623 REST API - Pool Failover API does not support multiple pool selection

From Eyeglass DR Assistant a Pool failover can be initiated for multiple pools but this is not supported from the API.

Workaround: Run concurrent failover for multiple pools.

T15624 REST API - Failover API does not block controlled failover when source cluster unreachable

Failover API does not validate source cluster reachability and will allow a controlled failover to start even if source cluster unreachable. Controlled failover in this case is expected to fail as it will attempt steps against the source cluster. When source cluster is not reachable uncontrolled failover should be used.

Workaround: Use manual process to verify source cluster reachability and initiate the appropriate controlled or uncontrolled failover.

T15769 DNS Dual Delegation Validation does not work where NS Record does not resolve directly to an SSIP

If DNS Dual Delegation is configured with NS Records that resolve to a name (for example configured as CNAME) the DNS Dual Delegation Validation will not work as it is expecting an IP address on resolution of the NS Record.

Workaround: To avoid this warning DNS Dual Delegation validation can be disabled. Please contact support.superna.net for assistance.

T16154 DR Rehearsal mode issues where source and target path are different

Invalid readiness validation for Corrupt Failover Snapshots: For case where SyncIQ Policy involved in DR Rehearsal mode enabled has different source and target paths or space in SyncIQ Policy path or a special character in SyncIQ Policy path, after DR Rehearsal mode enable the DR Failover Status incorrectly shows an Error for Corrupt Failover Snapshots for that policy. This error blocks reverting DR Rehearsal mode.

Failover error: Failover error occurs when data sync option unchecked.

Workaround: Do not use DR Rehearsal mode for policies which have different source and target paths, spaces in paths or special characters in paths. Regular failover is unaffected by this issue and is available. To recover from this REHEARSAL_ERROR open a support ticket at support.superna.net for assistance.

T17136 Zone Readiness incorrectly shows Error when Access Zone Name, Smartconnect Zone Name and IP Pool name are exactly the same

DR Dashboard Zone Readiness incorrectly shows Policy Readiness Status, SmartConnect/IP Pool Settings and Mappings Readiness and Eyeglass Failover Mapping Hints in error when the Access Zone, SmartConnect Zone Name, IP Pool all have exactly the same name.

Workaround: This issue can be resolved by renaming the Access Zone to be different. This change should be assessed for impact in your environment before making this change.

T17401 Pool Readiness not displayed with no configured/reachable DNS

If both Eyeglass and Isilon DNS are not available, the DR Dashboard pool readiness is not displayed.

Workaround: Provide reachable Eyeglass or Isilon DNS.

T17477 DFS share suffix not applied for failover or configuration replication

If a custom suffix is configured for DFS share name on target cluster, suffix is not applied either during configuration replication or during share renaming step of failover.

Workaround: None available.

T17428 REST API - Policy Readiness returns incorrect Access Zone

Failover API to retrieve Policy Readiness information returns the incorrect Access Zone for environments with multiple Access Zones.

Workaround: None required. Access Zone does not affect Policy Failover and Access Zone Readiness and Failover correctly assign policy to correct Access Zone.

T17447 OneFS 9.0 and 9.1 Readiness Validation for Policy Source Nodes Restriction always shows INFO

For OneFS 9.0 and 9.1 even if the Policy Source Nodes Restriction is configured, the Readiness Validation always shows INFO,

Workaround: Verify on PowerScale the source nodes restriction settings. DR Status of INFO does not affect / block ability to failover.

T17555 Blank display for Zone or Pool Readiness

In some instances where Zone and Pool failover is configured the Zone or Pool readiness window may be blank when both the DR Assistant and DR Dashboard are open.

Workaround: Reload the tab or only have one window open at a time.

T17731 Policies missing in DR Assistant for Zone or Pool failover

DR Assistant missing policies in an Access Zone for Zone or Pool failover where there are no SMB shares or NFS exports configured at or below the SyncIQ policy source path. Impact is that failover steps are not executed against these policies and they remain active on the source cluster.

Workaround: In advance of failover, configure a temporary share with restricted permissions at the SyncIQ policy source path. If you have failed and only then determine the issue, policies can be failed over using Policy failover if the failover was an Access Zone failover. If the failover was a Pool failover manual steps must be used to failover the remaining policies.

T17732 Multiple Zone Readiness Jobs

Under some circumstances multiple Zone Readiness jobs will be running at the same time without any completing. DR Dashboard not updated when in this state. If this occurs during Access Zone failover it does not block failover.

Workaround: Eyeglass sca service restart will address this issue but recommend to contact support.superna.net for assistance and evaluation of the issue.

T18127 DNS Dual Delegation uses wrong SSIP when IP Pool Service Subnet different from the pool subnet

The IP Pool Service Subnet setting that is different than the parent subnet of the IP Pool is not taken into account for the DNS Dual Delegation validation. This could result in incorrect assessment of the DNS delegation configuration or if no SSIP configured in the parente subnet can result in the error "This IP address does not reference valid cluster".

Workaround: Manual inspection of DNS NS Record delegation should be done to confirm that it has been configured correctly.

T18392, T19226 DFS Failover produces extra "null" failover log

Under certain circumstances a DFS failover will generate a second failover "null" log visible in Running Failovers and Failover History. No impact to failover steps.

Diagnostic tool for dark site, igls app report, is not able to summarize failover history. Remainder of report is unaffected.

Workaround: None required for DFS failover. For diagnostic report, failover history can be retrieved from the Eyeglass GUI DR Assistant, Failover History window.

T18779 Overlapping Powerscale cluster and SynclQ Policy names can result in incorrect Failover Readiness assessment

For the case where source and target Powerscale cluster have overlapping names (for example "cluster1" and "cluster1dr") and there are SynclQ policies on both cluster with the same name, failover readiness for source cluster may take into account the SynclQ policy state on the target cluster resulting in an incorrect state for source cluster. For example a SynclQ policy disabled on the target cluster incorrectly results in Policy Enabling Readiness Warning for the SynclQ policy on the source cluster.

Workaround: Rename the SynclQ policy on the target cluster to make it unique between both clusters. For example pre-pend the SynclQ policy name with the target cluster name.

T18969 Runbook Robot Job in Jobs window disappears when target cluster is unreachable

If there is an unreachable cluster, the Runbook Robot job in the Failover: Runbook Robot (AUTOMATIC) section of the Jobs window disappears for the unreachable cluster.

Workaround: None required. The Runbook Robot job cannot run when there is an unreachable cluster. The job reappears on it's own once the cluster is reachable again.

T19186 Policy Readiness not updated

Under some conditions the database will get into a state where the policy readiness assessment cannot be updated or completed and may contain old information. This affects policy readiness as well as the policy readiness component of Zone and Pool failover readiness.

Workaround: This requires the database to be refreshed. Contact support.superna.net for assistance.

T19553 Zone/Pool Readiness never completes

Under some circumstances Access Zone Readiness job begins as expected on startup but never completes. Issue has been found to be related to execution of the DNS Dual Delegation validation.

Workaround: Disable the DNS Dual Delegation Validation as documented [here](#). Verification of DNS Dual Delegation for Access Zone and IP Pool failover must be done manually.

T19967 Pool / Zone Readiness does not indicate whether there is a disabled Configuration Replication job in the Zone

Pool / Zone Readiness shows OK and green even when there is an associated disabled Configuration Replication job. Impact: Any associated Configuration Replication Job that is disabled will skip the associated SynclQ policy during failover.

Workaround: None required. When initiating the failover the DR Assistant Wizard does identify the disabled job and prompts on whether or not to proceed. Also Policy Readiness view can be used to identify disabled jobs.

T20181 Policy Hostname Validation Incorrectly show Error

If the pool mapping hints or ignore hints configured for Access Zone or IP Pool failover overlap with the SynclQ policy target host then the validation incorrectly flags the Policy Hostname Validation as Error. For example - SynclQ policy target host is target.ad2.test and mapping/ignore hint is igls-ignore-a-target.ad2.test.

Workaround: Rename the mapping/ignore hint so there is no overlap. For example as per above change the ignore hint to igls-ignore-a-target-a.ad2.test.

T21443 Quota failover error when source and target path are different and contain a \$

For SynclQ policy where source and target policy path are different and contain a \$ sign, when the quota failover step runs it attempts to create the quota on the source path instead of the target path.

Workaround: Quota configuration must be documented pre-failover and quotas need to be created manually on target after failover.

T21629 DR Readiness does not indicate source cluster unavailable

DR Dashboard does not indicate the condition where the source cluster is not available. This does not impact ability to failover - controlled failover is blocked and uncontrolled failover can proceed.

Workaround: Use the Continuous Op Dashboard to see whether clusters are available to Eyeglass.

T21750 Deleting SyncIQ Policy when Rehearsal Mode is active leaves configuration behind

In the configuration file which tracks whether rehearsal mode is active or not, a policy that is deleted while rehearsal mode is active is not removed from the file. Impact: Cannot use Eyeglass to revert rehearsal if the SyncIQ policy is deleted.

Workaround: None required. A new policy on the same path would be referenced by a new unique ID.

T22269 Python Pre and Post Failover Scripts do not work on OpenSUSE 15.3

Python based pre and post failover scripts do not run on OpenSUSE 15.3. In the failover log you will see the message: /usr/bin/env: 'python': No such file or directory. Shell scripts are not affected.

Workaround: Use shell scripting for pre and post failover scripts.

T22567 Quota Inventory causes problems during failover

Quota inventory is not blocked from running during failover and can result in system restart and an incomplete failover.

Workaround: Set the quota inventory schedule to run infrequently (example weekly) and for planned failover do not run concurrently.

T21929 igls-original SPN may not be deleted on failover

For the case where a smartconnect alias exists already with an igls-original prefix, on failover we skip the delete for the igls-original which causes SPN Issues on future failovers. This problem is specific to igls-original prefix SPNs and does not affect data access as the igls-original smartconnect is not used for accessing data.

Workaround: After failover manually fix SPN to prevent issue on future failover or ignore the issue.

DR-205 Zone Readiness Errors when Provider Instance Name mismatched

When an active directory provider with a provider instance name that doesn't match the actual active directory name has been added to an access zone, the Zone Readiness assessment in eyeglass will show:

- warning in SPN Readiness: Zone does not have any registered SPNs.
- AD Delegation Validation : SPN step shows error: Error processing SPNS: Unable to find domain controller for <provider instance name>

Workaround: remove the active directory provider from the Isilon, and re-add it without an instance provider name so that the name from the AD instance proper gets automatically used.

DR-254 Onefs 9.4 Unlock My Files Feature Does Not Work

The unlock my files feature does not work with OneFS version 9.4 or higher due to a deprecated command on OneFS.

Workaround: None available.

Configuration Replication

1683: Export sync where source is 7.1.1.x and target 8.x.x.x

Description: Syncing exports does not function between these releases.

Resolution: None unsupported sync, upgrade to 7.2.x.x

649: Export sync where source and target path on each cluster is different is deleted and recreated in each config cycle (affects onefs 7 to 8 or 8 to 7 replication)

Description: When the path on source cluster and target of the SyncIQ policy are different, exports will be deleted on target and then recreated again within the same replication job. No error is seen on the config sync job. May affect other releases as well.

Resolution: None, export is created correctly after config sync job completes.

1462 - Export max_file_size cannot be replicated

Updated export max_file_size parameter is not replicated and replication Job fails.

1355: Edit Job configuration to include share/export deselected from another Job causes share/export to be reselected.

Description: When you edit a Job B configuration to include share/export that had already been deselected from Job A, this causes this share/export to be reselected for Job A as well.

Workaround: None available. Should the share/export subsequently be deselected from Job B it should then also be manually deselected again from Job A.

1580: Delete and Create export within same replication cycle orphans deleted export on the target with OneFS 7.1.1.x

With OneFS 7.1.1.x, a delete and create export operation which occurs within the same replication cycle will replicate the export that was created on the next replication cycle but the export deleted on the source will not be deleted on the target.

Workaround: Manually remove the deleted export from the target using PowerScale OneFS.

1625: Custom QUOTA Jobs require extra replication cycle to be deleted

In the Eyeglass Jobs window, when you delete a CUSTOM Job and then the associated QUOTA Job is not immediately deleted. It is deleted on the next replication cycle.

Workaround: None required.

1639: Able to manually Run Now disabled Custom Job

Eyeglass Jobs window allows you to Run Now on a Custom Job which has been disabled. A message is displayed indicating that the Job has been queued but the share/export configuration replication Job is not run and the associated QUOTA Job is run and quotas are replicated.

Workaround: Do not Run Now for Custom Job that has been Disabled.

1641: Custom Job does not include shares/export when source or destination path configured with a trailing /

If you enter source or destination path for Eyeglass Custom Job with a trailing / (for example /ifs/data/test/), the Custom Job will not pick up the related shares and exports.

Workaround: Source and destination paths must be entered without the trailing / - for example /ifs/data/test.

1788: Delete of unlinked user quota on source may not delete matching quota on the target

Attempting a quota replication after deleting an unlinked user quota may fail to delete the quota on the target with a Job status of success but an Audit failure.

Workaround: Deleted quota manually deleted on the target.

1789: Able to select shares/exports/quotas outside job path after deselected

After a share/export/quota has been deselected from an Eyeglass Job, it can be re-selected for a different Job even if it is outside the Job path. As a result, the Job may have an error for these share/export/quota due to path not found error.

Workaround: Do not customize Eyeglass configuration replication Job and select share/export/quota that are outside the Job path.

1887, T3727: Multiple SynclQ policies associated with same Zone will result in transient error on Eyeglass Zone replication creation

Where there are multiple SynclQ policies which are associated to the same zone and Eyeglass configuration replication is being used to create the zone on the target, the first Zone replication job will

succeed, but subsequent Zone replication jobs for the same Zone will fail with the message “Zone ‘<zone name>’ already exists”.

Workaround: None required for OneFS 7.2 - 7.2 or 8 - 8 replication. Error will be cleared on subsequent configuration replication cycle.

For OneFS 7.2 - 8 replication, Zone Replication Readiness always has warning status and alarm is raised for failed audit on zone job. Manually inspect that Access Zones are identical and that Zone Readiness Warning is related to this issue.

1924: Quotas on excluded SyncIQ directory are selected for replication

Eyeglass quota job includes quotas related to excluded SyncIQ directories. If quota job is run, it will typically fail due to path not found.

Workaround: Customize Quota Job and deselect quotas for excluded directories.

1998: Custom Eyeglass configuration replication Job does not have an associated Zone replication Job

When you create a new custom Eyeglass Job, an associated Zone replication Job is not created.

Workaround: Zone must be created manually or already exist on the target cluster in order for Eyeglass configuration replication to succeed.

2004: Custom Quota Job is incorrectly listed in the Failover:

Quota Failover (RUN MANUALLY) section in the Jobs window

When you create a new custom Eyeglass Job, the associated Quota replication Job is created and incorrectly listed under Failover: Quota Failover (RUN MANUALLY) section in the Jobs window.

Custom Quota Jobs do not need to be run manually, they are run automatically each time the customer Eyeglass configuration replication Job is run.

Workaround: None required. Custom Quota Jobs do not need to be run manually, they are run automatically each time the customer Eyeglass configuration replication Job is run.

2007: Job error after deleting quota

After running Quota Job and successfully replicating quota to target, if quota is deleted and Quota Job is run again the Quota is successfully deleted from the target but the Quota Job has Error status.

Workaround: None required - quota is deleted.

2038: Create alias results in temporary error

When an nfs alias is replicated to the target, the initial create leaves Job in Error state with related alarm " Alias <alias name> already exists on this zone"

Workaround: None required. Next replication cycle clears the error.

2043: Configuration replication job has error after zone is deleted

For the case where Zone related to a Configuration Replication Job is deleted on the source, the Zone and associated configuration items are successfully deleted on the target, but the Configuration Replication job remains in Error state.

Workaround: None required. Shares and exports are deleted as expected.

2045: Edit Configuration for Custom Job has multiple source cluster selected where Eyeglass is managing more than 2 clusters

For the case where Eyeglass is managing more than 2 clusters, it may occur that the Edit Configuration view incorrect.

Workaround: None required. Shares and exports are replicated as expected.

2046: Job Edit Configuration view has the wrong parent selected

For the case where a configuration replication job contained a configuration items and the last configuration item is deleted - after the configuration item is deleted, the parent in the Edit Configuration view continues to be selected for the Job even though when you expand the tree there are correctly no children selected.

Workaround: None required.

2049: Delete Zone does not delete associated configuration items on target for custom Jobs and auto jobs with disabled zone Job

When a non System zone is deleted on the Source, the Eyeglass Configuration Replication Custom Job or Auto job with disabled Zone Job does not remove the associated configuration items from target related to the deleted Zone.

Workaround: Manually delete the Zone and associated configuration items on the target using OneFS.

2235: Eyeglass replication Job does not complete when source cluster becomes unreachable after Job has started

If the source cluster becomes unreachable after the Eyeglass configuration replication Job has started, the Job does not complete.

Workaround: None required. The Job will eventually complete after all communications timeouts have occurred. This may take an hour.

2060: Access Zone Replication Error - Error on creation of shared resource

Error on Replication for Access Zone which shows Error on creation of shared resource.

Workaround: None required. Once SyncIQ Job has run again in OneFS, the next time configuration replication runs the Access Zone is replicated.

2488: Inconsistent behaviour in Run Now for Disabled Jobs

When Run Now is selected for an Eyeglass Job which is disabled, the handling is different depending on Job Type and state:

For Job which is "Policy Disabled" - Run Now is blocked for all Jobs

For Job which is "User Disabled" - Run Now not blocked and all enabled Jobs run

For Robot Job which is disabled - Run Now not blocked, Job is initiated and then fails.

Workaround: Only select enabled Jobs for Run Now.

1938: Issues with Eyeglass Configuration Replication Jobs after the Access Zone is deleted

When you delete an Access Zone in OneFS, the following issues occur in Eyeglass:

- corresponding Eyeglass Zone Configuration Replication Job is not deleted

Workaround: None Required. Job is empty.

2308: In EyeGlass, NFS alias health is always 'unknown'

Eyeglass Inventory, NFS Alias audit and Cluster Configuration Report always have the NFS alias health property set to unknown.

Workaround: Determine the NFS Alias health from the OneFS command line using isi command..

2804: Disabled SyncIQ Policy is not initially displayed as Policy Disabled in Eyeglass

When the Eyeglass system setting for INITIALSTATE is set to Disabled for Configuration Replication Jobs (Type = AUTO), the Jobs window State for the Eyeglass Configuration Replication Job where the corresponding SyncIQ Policy is disabled displays as "User Disabled" instead of "Policy Disabled". In this state the Eyeglass GUI allows you to Enable this Job, but in fact after the next Configuration Replication Job the Job is correctly displayed with the Policy Disabled state.

Workaround: None Required.

T676: Eyeglass Zone replication Job does not replicate all authentication providers for OneFS 8.0

For OneFS 8.0, if an Access Zone has multiple authentication providers not all providers will be replicated for the Access Zone on the target cluster.

Workaround: Manually edit the Access Zone on the target cluster and add the required authentication providers.

T723: Job shows OK when there is an Access Eyeglass Zone

Replication Error

The Jobs window for an Access Zone replication Job which had a replication error or audit error shows as OK even though an Alarm was issued for the Error.

Workaround: Monitor email for Access Zone replication errors. Address the replication issues.

T771: Edit Configuration does not show parent node selected

If a change is made to a Configuration Replication Job to deselect a file sharing object from the job, the parent node where there still are selected objects is no longer selected in the Edit Configuration window.

Workaround: Expand the Inventory View tree for SMB and NFS to see which objects are contained in the Job.

T805: Eyeglass Configuration Replication Jobs not updated when IP address changed on Source Cluster

An IP address change on the Source Cluster of an Eyeglass Configuration Replication job does not get picked up and the job continues to reference the old IP address resulting in a configuration replication error.

Workaround: Reset Eyeglass to pick up IP address changes for Jobs on the new active cluster

- a. Make a record of the state of all Configuration Replication Jobs in the Eyeglass Jobs window - these states will NOT be preserved on the reset:
 - i. Jobs which are Configuration Replication type
 - ii. Jobs that are DFS enabled

- iii. Jobs that are User Disabled
 - b. SSH to Eyeglass appliance using admin: sudo -s enter (must use root) then use admin password (default password: 3y3gl4ss)
 - c. set the initial state for all Eyeglass Job types to User disabled
 - i. <http://documentation.superna.net/eyeglass-PowerScale-edition/Eyeglass-PowerScale-Edition#TOC-igls-adv-initialstate>
 - d. cd /opt/superna/sbin
 - e. ./reset.sh
 - f. Once reset completes, go to the chrome browser and refresh the browser and login with the credentials
 - g. Now, you need to add both of the cluster using Management subnet SSIP.
 - h. Once it is added, open the Job window - now you will see all the Eyeglass configuration replication jobs are in “user disabled” state
 - i. .Enable all the Eyeglass configuration Job to DFS Mode if configured
- IMPORTANT: You must enable DFS mode before enabling the Job to prevent creation of active shares on target cluster**
- a. Enable all configuration replication job (except ones that were previously User Disabled) and run it

T593: Eyeglass errors for multiple exports with the same path

If an Eyeglass Configuration Replication Job contains more than one Export with the same path, this may result in an AUDITFAILED state or configuration replication error for the associated Eyeglass Configuration Replication Job in the DR Dashboard or a configuration replication error.

Workaround: The following workaround is available to address this issue:

1. Modify exports on the source to add a second path which is a sub-folder of the existing path. This way Eyeglass will identify each Export uniquely. Example

Initial State:

export 1: /ifs/data/folder

export 2: /ifs/data/folder

Updated State:

```
export 1: /ifs/data/folder
        /ifs/data/folder/sub-folder
export 2: /ifs/data/folder
```

2) Exports must have different Clients.

T1792: Eyeglass does not auto-detect PowerScale version changes and may use incorrect API version for Configuration Replication

You may see Inventory errors after upgrading the PowerScale cluster version or adding a cluster to be managed by Eyeglass which has a different OneFS version than clusters already managed due to wrong version of API being used to connect to the cluster.

Workaround: Restart the Eyeglass sca service as per instructions here for sca service:

<http://documentation.superna.net/eyeglass-PowerScale-edition/Eyeglass-PowerScale-Edition#TOC-Eyeglass-Processes>

T1851: Eyeglass Configuration Replication Jobs not removed when there is no SyncIQ privilege for the eyeglass service account

If the eyeglass service account has the SyncIQ privilege removed the Eyeglass Jobs are not updated to removed even though the associated SyncIQ policy cannot be retrieved. The Jobs run successfully with the message "The job has no data to replicate; skipping it."

Workaround: eyeglass service account must have the SyncIQ privilege as documented in minimum permissions document here: <http://documentation.superna.net/eyeglass-PowerScale-edition/tech-notes/PowerScale-cluster-user-minimum-privileges-for-eyeglass>

T2193 - Export max_file_size setting not replicated correctly

A large export max_file_size parameter is not replicated exactly to target as it is configured on the source which results in an Audit failure during Eyeglass Configuration Replication. For example:

Source 4611686018427388000

Target: 4611686018427387904

Workaround: None available. For smaller values such as 1024 or 1048576 this error does not occur.

T2757: Access Zone is not replicated from OneFS 8 to OneFS

7.2

Access Zone is not replicated from OneFS 8 to OneFS 7.2.

Workaround: Create Access Zone and make updates manually.

T1976 - Eyeglass Jobs Window Edit Configuration does not show related Snapshot Schedules

If a Snapshot Schedule Replication Job is selected in the Jobs window, the Edit Configuration option does not mark the Snapshot Schedules which are included in the Job..

Workaround: Expand the Snapshot Schedule Job in the Jobs window to see the Source Path.

Manually review Snapshot schedule paths. Any Snapshot Schedule where the path is at or below the Job source path will be included in the Job.

T2920: Access Zone Authentication Provider is not replicated to the target cluster

Eyeglass Configuration Replication does not sync the Access Zone Authentication Provider to the target cluster.

Workaround: Add Authentication Provider to the Access Zone manually.

T3629: Renamed Snapshot Schedule leaves original Snapshot Schedule on the target

After renaming a Snapshot Schedule, the next Configuration Replication cycle creates the new Snapshot schedule on the target but does not remove the Snapshot schedule with the original name such that on the target they both exist.

Workaround: Manually remove the extra Snapshot Schedule from the target.

T14803 Set Job Type AUTOSKIPCONFIG does not create associated jobs until configuration replication runs

When setting job type for an unconfigured job to type SKIPCONFIG the other related jobs for snapshot schedule, zone, quota are not created until the next Configuration Replication cycle has completed.

Workaround: None required - next scheduled Configuration Replication job will rectify and create the jobs.

T15258 Unable to create Custom Job

After creating a Custom Job, it is removed from the Job list after the next Configuration Replication cycle runs.

Workaround: None Available

T15321 DFS share name custom suffix may be doubled

If you have configured a custom DFS suffix, if the source share name already has the suffix it may be added again to target share on replication instead of being skipped.

Workaround: It is not expected for source share name to have the DFS suffix. Please contact support.superna.net for assistance.

T15884 Some scenarios in networking API failures during Configuration Replication may not block deletes

Some scenarios remain after resolution in 2.5.5 T12773 where when Eyeglass has an incomplete view of PowerScale configuration due to a PowerScale API networking API call failure there is a risk of deleting and readding Eyeglass Configuration Replication jobs and losing their settings such as DFS mode or AutoSkipConfig mode or risk of deleting meta data such as SMB shares or NFS exports.

Workaround: In 2.5.6 all new Eyeglass configuration replication jobs will be in unconfigured state.

When activating ensure that you are activating in the correct mode: AUTO, DFS or AUTOSKIPCONFIG.

T16965 Audit does not consider differences on source and target for SMB share property inheritable_path_acl

For the case where an SMB share has been manually created on the target cluster with a different setting for the SMB share property inheritable_path_acl, the Supena Eyeglass compare of the source and target share does not identify the difference and therefore does not update the target share to match the source share.

Workaround: One OneFS manually change the setting for this property, or if the share on the target cluster is not in use delete it and allow Eyeglass to recreate it.

T18812/T23433 Error replicating SMB Share with Run as Root permission

In some cases where an SMB share permission is configured with run as root the run as root permissions are replicated to the target as regular permissions and also subsequent attempts to update results in a duplication of permissions which results in duplicate error and/or AEC Error Failed to insert new run-as-root - Message too long.

Workaround: To skip replication of share permissions and properties you can follow the steps [here](#) to view the shares and exports that are part of the Configuration Replication Job. To skip replication on a share, uncheck it. Once skipped, manual process will be required to keep share properties and permissions up to date on target cluster.

T19026 Data Config Migration Preview incorrectly shows quotas selected

If Data Config migration is configured to not replicate quotas, the Preview window incorrectly displays quotas as selected for replication. This is a display issue only. Quotas are not replicated when the migration job runs.

Workaround: None required.

T19177 NFS modify properties which are not client list fails with unresolvable host

If an NFS export property is modified where the property is not an NSF export client and the client list contains unresolvable hosts, the Eyeglass replication job will fail to update the NFS export on the target with an unresolvable host error even if in Eyeglass the ignoreunresolvablehosts setting is set to true. Note that this is not an issue if an NFS export client list is modified as this results in a delete and create of the export since the client list is part of how we uniquely identify the export.

Workaround: Manually update the export on the target cluster to update for new setting.

T19894 NFS Export replication in DR Test Access Zone incorrectly identifies that update is required

For case where main Configuration Replication job correctly does not identify any changes for an NFS export, the replication to that DR Test Access Zone incorrectly identifies an update is required. Impact: None except for case where replication is subject to issue T19177 NFS modify properties which are not client list fails with unresolvable host you will see an error.

Workaround: None required.

T20301 User Disabled AUTOSKIPCONFIG job becomes enabled after a rediscover or if policy renamed

Upon executing a rediscover command in Eyeglass or if the SynclQ policy associated with an AUTOSKIPCONFIG job is renamed, the status of the AUTOSKIPCONFIG job changes from User Disabled to Enabled. Impact: As AUTOSKIPCONFIG mode skips the replication of share and export properties there is no impact to any shares or exports on the target cluster if the job becomes enabled. Ability to failover the associated SynclQ policy changes from being blocked to failover to being able to failover.

Workaround: Manually update AUTOSKIPCONFIG job status after rediscover or policy rename.

T20369 Configuration Replication Error after running DR Rehearsal failover on SynclQ policy where source and target path are different and contain special characters and or spaces

A configuration replication job that is OK and green prior to executing a DR Rehearsal failover may be in error after the DR Rehearsal revert when the SynclQ policy source and target path are different and contain special characters and or spaces. Impact: No impact to subsequent DR Rehearsal failover. Changes to SMB shares or NFS exports for that job will not be replication.

Workaround: SMB Shares and NFS exports on the target will have to be kept up to date manually.

T21375 Snapshot schedule replication error on update

Initial snapshot schedule replication completes successfully, but a change to the snapshot schedule such as changing the snapshot expiration results in following error on update: AEC_CONFLICT Schedule entry already exists with that name: File exists.

Workaround: Snapshot schedule can be updated manually on the target cluster for changes.

T22875 Configuration Replication audit step incorrect error when path contains a comma

For Configuration Replication where the path contains a comma the post audit step incorrectly reports that the share is not identical on source and target. Impact is incorrect result on audit only, the replication of the share itself was successful. This also impacts failover readiness which will show a Warning as a result of this issue.

Workaround: For Configuration Replication none required. For Failover, this Warning can be ignored and to failover with this Warning uncheck block on warning option. Any other Warning must be assessed independently before unchecking block on warning for failover.

T17345 - Advanced Quota settings for Configuration sync

Fixed in this release stream. If advanced quota sync options like pre-sync were enabled, the desired behavior will be used as per the admin guide [here](#).

The advanced settings for quota sync behavior and pre-sync options are ignored even if enabled in the system.xml located in data or conf folders. The behavior will revert to normal quota sync which is no syncing of quotas during configuration sync jobs. This is the default behavior.

Features

1138: Eyeglass UI does not block configuration of duplicate remote logging service

Description: If you configure the same remote logging service twice in Eyeglass, the forwarding of logs to the logging service will fail

Workaround: Only configure 1 instance of a remote logging service.

2224: Eyeglass Cluster Configuration Report runs when Cluster is unreachable

Eyeglass attempts to run the Cluster Configuration Report for Cluster that is not reachable. The Job is started but does not complete.

Workaround: None available. Report will run successfully once cluster is reachable.

2061: Access Zone name for Directory Migration is case sensitive

Check for Access Zone exists on target cluster for Directory migration fails is case sensitive and will fail if Access Zone exists with same name but different case.

Workaround: Access Zone name and case must be identical between source and target for Directory Migration.

2882: Phone Home Email Disabled

Phone home feature is changing and will be disabled . A new web direct option will be used in a future release.

Workaround: Use the Eyeglass Backup Full Archive function to collect Eyeglass configuration and logs.

Procedure is described in the document

3037: Configure Remote Logging Services in Eyeglass requires manual steps

After configuring the Remote Log Consumer in Eyeglass, additional manual steps are required on the Eyeglass appliance to update syslog-ng.conf to enable the service.

Workaround: Please refer to Eyeglass Tech Note [Eyeglass PowerScale Remote Logging Service Tech Note](#) section "Setup Eyeglass remote logging manually for log Analysis".

T1515: Eyeglass Shell feature not functioning for RHEL and Centos deployments

If Eyeglass is deployed on a Redhat or Centos operating system the Eyeglass Shell feature does not work.

Workaround: ssh to the Eyeglass server using other tools such as putty.

T3119: Access Zone Migration Preview does not always display Configuration information

The Access Zone Migration Preview window does not display the shares, exports and quotas that will be migrated if the source path selected for migration does not have an associated SyncIQ policy.

Workaround: Review shares/exports/quota paths manually to determine which configuration data will be migrated for the selected source path.

T3170: Quota Requests History shows Status of Error for processed requests after failover

After failover, the Quota Requests History will show state for all processed quota requests as error instead of showing the status of the request as it was when the request was processed.

Workaround: Verify from OneFS that the quota settings are as expected.

T4280: User Storage View may show all quotas instead of only the User Quotas

It may occur that the User Storage View shows all quotas configured instead of just the quotas related to the logged in User.

Workaround: Logout and refresh browser and then log back in and reopen window may clear this condition. If not, the quota path may be used to determine which quota apply to the logged in user.

T4329: DR Test Status does not open

When DR Test Job has first been created, the DR Test Status window does not open and shows the error "Readiness data not found. Please run configuration replication." even though Configuration Replication has run.

Workaround: DR Status window will open once DR Test Mode has been Enabled.

T4432: DR Test Mode action on multiple policies do not display in Running Jobs

When multiple DR Test Jobs are selected in the DR Assistant to enable or disable DR Test mode, the Running Jobs window only shows 1 Job even though action is being applied to all selected Jobs.

Workaround: None required - display issue only. Action completed against all selected jobs.

T4968: SyncIQ Job Report Troubleshooting section missing information when report is generated on demand

When a SyncIQ Job Report is generated from the Reports on Demand window, the Troubleshooting section may not be populated.

Workaround: Use the scheduled daily report for Troubleshooting information.

T5173: Quota Modification Request window does not close after Submit

After a Quota Modification Request is submitted, the window does not close and remains in a loading state.

Workaround: None required - display issue only. Action was completed and the request can be seen in the Pending Requests window.

T6389: Built-In AD Groups cannot be used with the Cluster Storage Monitor Active Directory Managed Quota feature

When configuring Cluster Storage Monitor AD Group Mode Templates for automated quota creation, AD built-in groups such as "domain users" cannot be used as the users in the group will not be correctly identified.

Workaround: Create new AD Group for quota assignment and add this group to related shares in PowerScale. For additional information on use of AD groups for share security vs quota creation please read [here](#).

T8834: Storage Monitor Report missing user information when friendly name cannot be resolved

User quotas created for users who are not in the default AD Domain, a friendly name cannot be resolved and quota itself is associated with user SID but in the Storage Monitor Report the user is reported as "user" instead of showing user SID.

Workaround: None available.

T9561: Unlock my files incorrectly displays directories

Unlock My Files window incorrectly includes directories in the display instead of just files. If a directory is inadvertently "unlocked" it may disconnect clients or have other unexpected results.

Workaround: Do not use unlock for directories.

T11807 Alarm for quota synchronization error does not contain error details

For case where quota synchronization fails (example advisory threshold configured to be greater than hard threshold), an Eyeglass alarm is raised but the alarm does not contain any details of the error.

Workaround: In Eyeglass Jobs / Running Jobs window tree view under "Group Quota Synchronization Steps" navigate down the tree and find the step with an error. The Info link should contain error details if available.

T12307 Cluster Storage Usage may be incomplete

When the API request for cluster storage usage is returned from PowerScale with information missing for one or more nodes, the Eyeglass Cluster Storage Usage window may not display all information for the nodes where information was returned. For example for a 4 node cluster if the API response only contains information for nodes 1, 3 and 4 the Cluster Storage Usage window may only display information for node 1 even though node 3 and node 4 information is available.

Workaround: Use PowerScale tools to determine storage usage.

T13390 DR Testing (Disaster Recovery Testing) Job initially always in User Disabled state

When an Eyeglass Job first becomes type Disaster Recover Testing it is always in User Disabled state no matter what state it was in as an AUTO job.

Workaround: Select the checkbox for the Disaster Recovery Testing job and then Select a bulk action / Enable/Disable to enable it.

T14956 No Recovery when DR Test Mode in Entering DR Testing or Exiting DR Testing

If DR Test Mode Make Target Writeable/ Make Target Read-Only does not complete and is left in the Entering DR Testing or Exiting DR Testing state there is no way to revert or retry the operation.

Workaround: To assist in recovery from this state please open a support case at support.superna.net .

T14962 DR Test Mode Configuration Replication step does not run configuration replication for the DR Test mode job itself

If Configuration Replication option is selected for Make Target Writeable, the DR Test mode job itself is not included and any changes to SMB shares or NFS exports that had not been previously synced will not be present on shares / exports used for the DR Test.

Workaround: Let scheduled configuration replication job run or manually initiate configuration replication to sync SMB shares and NFS exports to the DR Test mode shares / exports prior to initiating Make Target Writeable.

T15215 Data Config (Zone) Migration Job can not be created where Migration or Destination Path contains special characters

A Data Config Migration Job will fail to be created if the Migration or Destination Path contains special characters (example & or ').

Workaround: None Available

T15311 Data Config (Zone) Migration Job fails for existing policy when "Migrate only configuration" is checked

A Data Config Migration Job will fail when there is an existing SyncIQ policy on the migration path and "Migrate only configuration: is not checked.

Workaround: Select "Migrate only configuration" option to sync the configuration items and separately manage SyncIQ from PowerScale interface to manage data replication.

T17535 Quota Search - Display of quota count on modify may not be correct

The count of quotas modified displayed on the GUI may not be accurate.

Workaround: Verify via OneFS interface that requested changes have all been made.

T17739 Cannot create quota template for less than 1 GB

Quota template creation for Active Directory Managed Quotas (igls csm template add) does not allow creation of a quota limit of less than 1 GB either by entering less than 1024 MB or a decimal in GB.

Workaround: None available - minimum quota size available is 1 GB.

T18148 Incorrect Error Message for unreachable Powerscale cluster when breaking lock

Error message is displayed if Break Lock operation occurs when Powerscale cluster is unreachable, but does not indicate that the issue is an unreachable cluster. Error message may simply say "Error unlocking file!" if a node is unreachable or "Server error when processing request: null" if entire cluster is unreachable.

Workaround: None required

T19464 AD Group Template incorrectly creates quota on share where user permission is explicitly defined

If you have user permission assigned explicitly to share and that user is in an AD Group template for quota assignment, quota will be correctly created on the share(s) with the AD Group template assigned but will also incorrectly create a quota for any share where user permission is assigned explicitly.

Workaround: Use AD groups to assign permission to shares.

T20183 Unlock My Files does not display results if there is a Powerscale node that does not respond

If a Powerscale node does not respond (for example node is down or unreachable) when Unlock My Files is run, locked files on nodes that do respond are not displayed.

Workaround: Ensure that all PowerScale nodes are available.

T22209 igls adv ADGroupThresholds does not scan

The igls adv ADGroupThresholds starts API calls to retrieve AD users and groups but it does not evaluate the template to determine whether any quotas should be applied.

Workaround: None available.

T22622 Active Directory Managed Quotas fails with LDAP configured for retrieving user and groups

With Eyeglass configured to use LDAP to retrieve Active Directory Users and Groups, the Active Directory Managed QUotas feature does not work as the groups cannot be identified.

Workaround: Default collection of Active Directory User and Groups should be used with the Active Directory Managed Quotas feature.

DR-281 NFS deletion is not behaving correctly

When removing a Writable Snapshot, both config and snapshot, NFS exports are not removed from the writable snapshot path.

Workaround: no

DR-282 Warning message needs to be update when deleting a writable snapshot

Popup messages are not complete, we remove all resource types: SMB Shares,, NFS Exports and NFS Aliases.

DR-277 We need validation for directory on Writable Snapshots Path

When creating a Writable Snapshot, you need to make sure that the Writable Snapshot path is unique. There is no validation implemented for this yet. If using the same path for multiple Writable Snapshots, the job that is creating them will fail.

General

924: Inventory View shows + beside component when there are no more children

Description: In the Inventory View, components for which there are no children still show a “+” in the inventory tree. When you select the “+”, it changes to a “-” but there are no children displayed.

Workaround: None Required.

T17694: api token download of CMDB file is blocked by desktop login

Description: The API token download access to the servicenow.xml file is blocked by the web server desktop authentication service.

Workaround: Login to the desktop and enter the url <https://isilon-eyeglass/servicenow/servicenow.xml> to view download the file. API token access requires future release to bypass web server desktop login.

943: Inventory View not auto-refreshed

Description: Inventory View is not auto-refreshed and if open when a change occurs does not reflect the change.

Workaround: Use the Refresh Now button or close and reopen the Inventory View.

1612,T11989: Some alarms not cleared

Alarms other than the “Replication job failed to run “ are not cleared automatically once the error condition has been resolved. Example, DR Readiness alarm not cleared once readiness is green.

Workaround: Clear the alarm manually from the Eyeglass UI.

2155: Access Zone Networking info does not display in Inventory View

To see the Networking info for an Access Zone in the Inventory View:

- the Failover Readiness job has to have run
- the Access Zone must have an associated SyncIQ Policy

Workaround: Enable Failover Readiness job.

2628/T15193: Job Definitions window does not sort properly

Click on column headings in Jobs window to sort listings does not sort properly and sometimes lists jobs outside of the category groupings.

Workaround: None available

2895: Inventory SPN View is truncated

The Eyeglass Inventory view may be truncated and not display all SPNs stored in the database.

Workaround: Use isi command directly on cluster to determine all SPN.

2366: EyeGlass does not support special characters in email recipient address

Email addresses in Eyeglass do not support special characters.

Workaround: Do not provision email recipients or Email Server user with email address that has special characters.

2385: Refresh Now does not refresh the Failover History window

The Failover History window is not updated by the Eyeglass Refresh Now functionality.

Workaround: Close and reopen the Failover History window to see updates.

2744: Failed to Retrieve Inventory Alarm missing information

For the case where Inventory does not run because another instance of the Inventory Task was already running, the alarm that is raised does not provide this additional information

Workaround: Review the Eyeglass logs at the time that the inventory alarm occurred and search for the string "Another instance of Inventory Task is still running. Not starting".

2978: Syslog Log Viewer freezes Eyeglass web page

Opening the Eyeglass Syslog Log Viewer window may cause the Eyeglass web page to freeze.

Workaround: Refresh the Eyeglass web page or Fetch the Eyeglass Main Log first and then Fetch the Eyeglass Syslog.

T971: Eyeglass End User Interface Tree View Expanders do not collapse

The Eyeglass End User Interface DR Dashboard tree display '+' can be used to expand the tree but then the '-' does not collapse the tree again.

Workaround: Close and reopen the window

T1514: Eyeglass Archive cannot be downloaded when Eyeglass is deployed on Redhat or Centos

Eyeglass Backup Archive file cannot be downloaded from the Eyeglass web page if Eyeglass is deployed on a Redhat or Centos operating system.

Workaround: The Eyeglass Backup Archive files are stored here on the Eyeglass server:

/srv/www/htdocs/archive/ and can be copied from this location with a tool such as WinSCP.

T3137 - Eyeglass daily backup not working for RHEL/CentOS Deployments

The scheduled daily backup for Eyeglass is not working for RHEL/CentOS deployments.

Workaround: Manually create backup file from the Eyeglass GUI: About/Contact -> Backup -> Create Full Backup

T4596: Log Viewer cannot fetch logs

Under certain conditions the Log View may not be able to Fetch logs.

Workaround: Use the About/Contact -> Backup to create a Backup Archive and then download to your local system to review logs.

The Log View feature will be deprecated in a future release.

T12370 Network Visualization does not display Pool Readiness

The Network Visualization window Info Tab does not have a section for Pool Readiness. If you have Pool Failover configured you may see the related Access Zone in the Zone Readiness tab or related policies in the Policy Readiness tab. If you select status for that object it will open the DR Dashboard to the selected section not the Pool Readiness section.

Workaround: For assessing Pool Failover readiness open the DR Dashboard and select Pool Readiness.

T12373 Cluster Storage Window Empty

Under some conditions, the Cluster Storage Usage / Cluster Storage window is empty when it is opened.

Workaround: In some cases after toggling between Cluster Storage and Cluster Hardware menu or selecting Details the clusters will appear. If this does not resolve the issue, then native Powerscale tools can be used to collect cluster storage information.

T15310 REST API / Widgets creates empty html file

Unable to create web widget for DR Readiness.

Workaround: Use Eyeglass API to retrieve DR Readiness information. Plan to deprecate web widget in 2.5.7.

T15493 Extraneous Post Failover placeholder scripts

There are extraneous postfailover script provided that are not runnable: script1.sh, script2.py, script3.js .

Workaround: None required. These scripts should be ignored as they contain no examples. The environment_example scripts should be used as a reference.

T15511 Historical failover logs may lose formatting after a backup & restore

Failover logs retrieved from the Failover History may not have formatting after backup & restore.

Workaround: None required.

T15647 igls app report issues

The igls app report command to create a dr health summary file does not exit on completion of execution. The report is available for review but the command itself is not exited.

Workaround: Use CtrlC to exit the command.

The igls app report command may report below error and not start.

Starting a log parser service...

```
sh: /opt/superna/java/jre1.8.0_05/bin/java: No such file or directory
```

Workaround: Run the report using command below. Once run this way the correct java version should be available to igls app report command as well.

```
java -jar /opt/superna/bin/LogParserSca-0.0.1-SNAPSHOT-jar-with-dependencies.jar
```

T17530 Backup and Restore does not properly set location/permission for Eyeglass log files

After restoring Eyeglass backup , the Eyeglass log files location and/or permission is not properly set.

Workaround - 2.5.6-20258: Follow the steps below after the restore to correctly set log location:

1. SSH to Eyeglass VM (user: admin, default password: 3y3gl4ss)
2. sudo su (enter admin password)
3. execute below command

```
cd /opt/superna/sca && mkdir -p /opt/data/superna/sca/logs && cp -af logs/* /opt/data/superna/sca/logs && rm -rf logs && ln -s /opt/data/superna/sca/logs && chown -R sca:users /opt/superna/sca/logs
```

4. Done

Workaround - 2.5.6-20263: Follow the steps below after the restore to correctly set log location:

1. SSH to Eyeglass VM (user: admin, default password: 3y3gl4ss)
2. sudo su (enter admin password)
3. execute below command

```
cd /opt/superna/sca && chown -h -R -L sca:users /opt/superna/sca/logs
```

4. Done

T18000 Quota limit reached on Eyeglass appliance eca logs directory does not have an alarm

if the quota limit on the Eyeglass appliance ecal logs directory is reached there is no alarm to notify administrator. One the limit is reached the collection of ECA logs is affected. Operation of Eyeglass products is no affected.

Workaround: Manually monitor space consumed in this directory.

T18983 Multiple licenses applied to same Powerscale cluster

In some cases, 2 add-on licenses are assigned to a single Powerscale cluster. For example, 2 Ransomware Defender licenses are applied to 1 Powerscale cluster instead of 1 per Powerscale being managed. This prevents additional Powerscale cluster from being licensed.

Workaround: Contact support.superna.net for assistance.

T19208 Too many open files

If Eyeglass is also managing Ransomware Defender, Easy Auditor or Performance Auditor, under some circumstances when the ECA is unhealthy over a period the heartbeat loop results in condition where Eyeglass is in an error state related to too many open files. Impact once file limit is reached is that application no longer functions properly and eventually will restart.

Workaround: Contact support.superna.net for assistance.

T19276 Configuration file for enhanced HA for misconfigured/unavailable DNS not restored with --anyrelease option

A restore which uses the --anyrelease option does not restore the configuration file used by Eyeglass for its enhanced HA solution for misconfigured/unavailable DNS. This is not an issue for same release restore.

Impact: None if DNS is available and configured properly, the file will be rebuilt as the system comes up.

Workaround: For case where DNS is not available / misconfigured the file is available in the restore zip under the data folder data/fqdnipmapping.json and can be replaced on the new restore appliance manually. For assistance please contact support.superna.net.

T19280 Eyeglass services do not start if retrieval of banned file list on startup hangs

If on Eyeglass startup the step that attempts to retrieve the well known banned file list hangs, no Eyeglass services will be able to start. None of the scheduled jobs such as configuration replication, readiness will run.

Workaround: Steps to workaround are below. Contact support.superna.net if you would like assistance.

1. SSH to Eyeglass as admin user
 2. Run command: **sudo vim /opt/superna/sca/data/system.xml**
 3. Find the line that starts with <rsw_threat_file_url>
 4. Modify URL to something that does not resolve
 5. Save your changes
 6. restart Eyeglass services: **sudo systemctl restart sca**
-

T19523 After anyrelease restore or rediscover quota jobs for main and mirror policy are both enabled

If you have corresponding mirror policy for your main SynclQ policies, in the Eyeglass QUOTA jobs it is expected that one quota job is enabled (either OK or Pending) and the other job is Policy Disabled based on which SynclQ policy is active. After using anyrelease restore or running the rediscover command to rebuild the database, the job which should have been policy disabled is enabled and in Pending and both jobs are able to be run.

Impact to Configuration Replication of shares/exports/nfs alias: None. This issue does not affect these jobs. These jobs are active / policy disabled as expected.

Impact to Failover: None

Important: Do not run these jobs manually, they will be executed by Eyeglass during a failover. If you manually run the quota job in the wrong direction it will delete all active quotas.

Workaround: None required.

T19572 Alarms History missing on new 2.5.7 15.2 deployments

For Eyeglass deployment on 2.5.7 15.2 OVA, alarm history is not being saved to the database and the alarms history window in the Eyeglass Alarms window is empty.

Impact: This issue has only been seen to impact viewing the Alarm History. Alarm emails and writing to the `igls_alarms.log` used for syslog forwarding of alarms has not been affected.

Workaround: `igls_alarms` log can be used to reivew alarm history if required. Contact support.superna.net to make modification on the appliance to remedy this issue.

T20371 API error on OneFS 9.x for retrieving DNS settings

The inventory that is collected at midnight for the Cluster Configuration report includes an API call for `network/settings/dns`. For OneFS 9.x clusters this API call fails. This information is collected for information purposes only and failure to retrieve this information has no impact on Eyeglass functionality other than this information will not be available in the Cluster Configuration report.

Workaround: Use Powerscale native tools to document DNS settings.

T20407 igls app report error for OneFS 9.2

The `igls add` report command may return an error that the cluster version is not supported if Eyeglass is managing OneFS 9.2 cluster.

Workaround: None available. Support can provide assistance on information used to assess DR status.

T21275 Deleted Powerscale cannot be readded

A Powerscale cluster that has been added into Eyeglass can be deleted but results in an error if it is readded: The ip address that you have entered belong to `<powerscale>`. This cluster is already managed by eyeglass

Workaround: Contact support.superna.net for assistance.

T20808 Alarms window info column does not display full text

If the message in the Info column exceeds the available space, it is truncated and cannot be read from the window.

Workaround: Copy the partial text and paste externally (for example into Notepad) to see full text.

T21820 DR Edition - Manage Services window Eyeglass services status does not display CPU and RAM usage info

In the Manage Services window, the Eyeglass services status may not show the CPU and RAM usage.

Workaround: Use external tools to determine Eyeglass CPU and memory usage. The Manage Services view will provide up time.

T19213 Eyeglass RAM Alarm inconsistent notification

The Eyeglass RAM alarm notification is inconsistent. It may appear in the Active Alarms window or just in the Alarm History window. It may appear in one of the Alarms windows but not send email. It may only send an email on initial detection or it may email each time Configuration Replication runs.

Workaround: Use both Alarm GUI and notification to determine whether you have an issue with RAM configured on Eyeglass.

T21060 Alarms without info cannot be cleared

Some alarms may appear in the alarm window without any info in which case they will also be missing the link to clear the alarm.

Workaround: None available

T23072 Eyeglass RAM alarm for concurrent user login does not clear

If the number of concurrent logged in users falls below the alarm threshold, the alarm does not clear and on logout the timestamp associated with the alarm is incorrectly updated.

Workaround: None available

T23052, T23065, T23066 Log Parser Report Download links not working

In the log parser report generated from the Log Parser icon, the following download links do not download related files:

- Download eyeglass backup for this report
- Download full 'managed device alerts' table
- Download full 'RPO analysis' table

Workaround:

- Download eyeglass backup - none required, the backup had previously been downloaded in order to generate the report
 - Download managed device alerts - managed device alerts can be viewed from the Alarms -> Managed Device Alerts tab
 - Download RPO analysis table - none available
-

T23043 Restrictions in Log Parser customer name

Submit button is disabled if the customer name entered in the Log Parser Add New Backup window contains an underscore (_) character.

Workaround: Do not use _ in the customer name in log parser.

T23113 Log Parser does not show link for report when appliance id contains a slash (/)

If the appliance id associated with the backup contains a slash character (/), the log parser report is generated but the link to view the log parser report does not appear in the Log Parser window.

Workaround: The log parser report exists on the file system /opt/data/log_reports/<customer name> with an extra sub-folder where the slash occurs in the appliance id. The associated index.html file can be copied from the appliance with WinSCP in order to be viewed.

T23009 Log parser permission may not be added to admin role on upgrade

On upgrade from a previous release, the admin role may not have the LOG_PARSER permission required to see the Log Parser icon.

Workaround: Edit the admin role and select the LOG_PARSER permission. Logout and login to see the icon.

T23328 igls app report errors

The igls app report command encounters errors reading from the database which prevents all information from appearing the report such as configuration information, job information, failover readiness information.

Workaround: Use the Log Parser GUI functionality to generate the log parse report. How to use the Log Parser GUI can be found [here](#).

T23161 Upgrade to 2.5.8.1 from 2.5.8.1 earlier build fails

An upgrade to latest 2.5.8.1 build from an earlier 2.5.8.1 build fails.

Workaround: Contact support.superna.net for workaround.

DR-286 Issue related to Folder permission in /opt/data

The on-site log parser is not working; The RPO reports and the airgap job (isilon) reports may not work.

Workaround: Run the following commands to the eyeglass appliance:

```
chown sca:users /opt/data/log_reports
```

```
chown sca:users /opt/data/airgap_reports
```

```
chown sca:users /opt/data/syncIQ_reports
```

DR-276 Unwanted shadow trace is created when path picker is opened

When creating a Writable Snapshot, path picker will leave some shadows on the screen, This does not affect the overall functionality.

Superna Eyeglass Known Limitations

Known Limitations for PowerScale OneFS 8.0.0.x with Eyeglass

T507 Cluster Report for OneFS 8.0 missing information

The Eyeglass Cluster Configuration Report for OneFS 8.0 is missing following information:

- DNS and Subnet information
- File System Explorer
- Protocols - new HDFS, FTP, HTTP settings

Known Limitations for Eyeglass Failover

T939 Eyeglass Access Zone Replication Job in Error after failover

The Access Zone Replication Job associated with the SyncIQ mirror policy configuration replication Job has the following error when the SyncIQ policy source and target path are not identical.

Workaround: Create and update Access Zones manually on source and target cluster and disable Eyeglass Access Zone replication Jobs. With the Eyeglass Access Zone replication Jobs disabled, the Zone Configuration Replication Readiness Jobs will have a status of Unknown. This does not block failover.

T1785 Cannot set ignore flag on subnet pool after failback

It is not supported to apply an igls-ignore flag on a subnet pool that has been failed over and failed back such that the SmartConnect Zone has an igls-original prefix due to the fact that on a subsequent failover the igls-original prefix will not be removed and will leave the Access Zone in a state where both directions are failed over.

Workaround: Manually edit SmartConnect Zone on active cluster to remove the igls-original prefix. Run Configuration Replication and then run the Failover Readiness job to update Zone Readiness.

T2479: Access Zone Failover fails between OneFS 7.2 clusters if Eyeglass also managing OneFS 7.1

For the case where Eyeglass is managing OneFS 7.2 and OneFS 7.1 clusters, an Access Zone failover between OneFS 7.2 clusters will fail as OneFS7.1 linmap command is attempted and fails.

Workaround: Access Zone failover in this Configuration is unsupported as for Eyeglass Inter-version management, it is expected to apply capabilities of lower versions to all versions being managed and Access Zone failover for OneFS 7.1 is not supported. No workaround required.

T3258: Cannot start failover while Eyeglass initial inventory is running

For the case where Eyeglass has been restarted and the initial inventory is running for initial discovery, while the initial inventory is running a failover cannot be started. A “Failover configuration is not valid” message will be displayed in the GUI followed by a message that the target cluster is not managed by Eyeglass.

Workaround: Wait for initial inventory to completed before initiating a failover. Check running jobs windows for the initial inventory job to show completed.

T3774: Failover relies on policy naming: <policy name> and <policy name_mirror>

The Superna Eyeglass failover relies on following naming conventions:

1. First failover A to B- policy name = <policy name>.

The first failover name cannot be <policy name>_mirror.

1. Second failover B to A - policy name = <policy name>_mirror.

Workaround: Manual process on naming the convention above must be followed.

T4808: SPNs not updated for new authentication providers after Access Zone settings changed to “Use all authentication providers” (OneFS 7.2)

If an Access Zone is modified from manually defining the authentication providers to using the “Use all authentication providers” setting in OneFS 7.2, Eyeglass will not update SPNs for any new authentication providers that were not previously provisioned.

Workaround: Manual process required to create these SPNs.

T6229: Existing Failover Logs cannot be reviewed after upgrade to Eyeglass R2.0

Failover logs which were generated from previous releases cannot be viewed from the Eyeglass DR Assistant Failover History view after upgrade to Eyeglass R2.0

Workaround: Generate an Eyeglass Backup and download to your local machine. The Failover logs are contained in the backup archive in the folder failover_logs.

T14321 Zone/Pool Failover Readiness for AD Delegation validation, SPN Readiness validation not supported for Multi-Site failover configuration

For multi-site failover configuration the AD Delegation validation is not supported as it runs in parallel for both the A -> B and A->C resulting in conflicts and errors for both the self and cross AD delegation testing.

For multi-site failover configuration SPN Readiness validation is not supported as there are 2 pools on the B and C clusters with the same igls-original.... SmartConnectZone name and this cannot be provisioned in AD as it does not support duplicate SPNs.

Workaround: For multi-site failover manual verification for AD delegation can be done as documented [here](#) and the DR Dashboard AD Delegation validation can be disabled following documentation [here](#).

SPN Readiness validation warning cannot be disabled and after manual verification that correct SPNs are present can be ignored.

T15611 Pool Readiness Alarms are reported per Zone

Instead of reporting Pool Readiness alarms per Pool they are reported against the Access Zone that is configured for Pool Failover.

Workaround: None required.

DNS Dual Delegation Failover Readiness Validation Supported DNS servers

DNS Dual Delegation Failover Readiness validation is only supported by design for Microsoft DNS server.

This validation must be disabled if any other DNS server is being used. This can be done from the Eyeglass command line using the command: `igls adv readinessvalidation set --dualdelegation=false`

DNS Dual Delegation Failover Readiness validation uses PowerScale GroupNet DNS server

The DNS Dual Delegation Failover Readiness validation uses the PowerScale Groupnet DNS as the query server. If the Eyeglass appliance does not have access to the PowerScale Groupnet DNS for example due to firewall restrictions the failover readiness validation will fail.

Workaround: There is an option to configure Eyeglass to use the Eyeglass appliance DNS Server for the validation. Details can be found [here](#).

T17254 Failover does not take into account Powerscale job retries

In some cases Powerscale will retry a job after it fails and eventually if it succeeds the overall status of the job remains in Needs Attention. Failover logic takes the success / fail status from the first attempt only.

T18556 User Quota Replication requires System Access Zone AD Provider

The API used for creating user quotas requires System Access Zone to be configured with an AD provider to be able to resolve the user SID. If the user SID cannot be resolved the quota creation will fail with the error AEC_BAD_REQUEST "Requested persona was not of user or group type".

Workaround: Add an AD provider to the System Access Zone that has a trust relationship with the other domains in other Access Zones in order for SIDs to be resolved.

T19681 Runbook Robot NFS Export not created on target cluster

If NFS Export create and mount step are enabled for Runbook Robot, the Robot export is not created as it should have been on the target cluster causing the robot failover job to fail. This issue does only affect the

Runbook Robot job. No impact to regular configuration replication or failover. Workaround: Runbook

Robot mount and export creation steps are disabled by default and should be left as disabled.

Known Limitations for Eyeglass Configuration Replication

Multi-Path Exports

[T1359 Update NFS Multi-Path Export path\(s\) may cause transient Configuration Replication](#)

Error

Eyeglass uniquely identifies an NFS Export based on its path. When the path is changed this results in a Create and Delete operation in Eyeglass. It may occur that the create is attempted before the Delete is executed. In this case a Configuration Replication error occurs. This is automatically resolved in the subsequent replication cycle when the new export is successfully created.

[Export cannot have multiple paths that span multiple Eyeglass Jobs](#)

Export with multiple paths that are protected by different SyncIQ policies is not supported. This export configuration is not supported for DR as it would not allow per policy failover and is an unsupported configuration for Eyeglass.

The solution for this is to split the single export into multiple exports each with paths that correspond to a single SyncIQ policy.

T1359 Update NFS Multi-Path Export path(s) may cause transient Configuration Replication Error

Eyeglass uniquely identifies an NFS Export based on its path. When the path is changed this results in a Create and Delete operation in Eyeglass. It may occur that the create is attempted before the Delete is executed. In this case a Configuration Replication error occurs. This is automatically resolved in the subsequent replication cycle when the new export is successfully created.

T1743 Multiple export with same path and same client do not show Configuration Replication Error

Multiple exports with the same path are required to have different clients in order to be replicated as per PowerScale default behaviour. In the case where they have been provisioned with same client, Eyeglass Configuration Replication will only show error for this condition on the second configuration replication cycle.

T1847 OneFS 8 Overlapping Access Zone Replication has error

In OneFS 8 where there are Access Zones have identical paths, Eyeglass Access Zone Replication will fail with the following error from the PowerScale cluster: AEC_CONFLICT "field" "path" "message" "access zone base path */ifs*" overlaps with base path */ifs/data/zone*" in Access Zone Use the force overlap option to override. In this case disable Eyeglass Configuration Replication Jobs for Access Zones and manually create the Access Zone on the target cluster.

T1972 Snapshot schedule replicated with offset

Snapshot schedule expiration offset has OneFS API bug that adds extra time to snapshot expiration when the snapshot schedule is created. This results in an expiration on the DR cluster, that can be greater than entered on the source cluster. example expire in 20 days will be 22 days on the target cluster. Different units of off set all result in a value greater than entered. After failover the DR (target cluster) value will be synced back to the source (Prod cluster). Thereby losing the original expiry offset and extending the expire time by a new offset from the API error. This has been raised with EMC as SR to resolve.

1. **Work around:** Before failover ensure a cluster report has been generated (cluster reports icon), or an existing emailed cluster report exists. Post Failover re-enter the original values on the DR snapshot schedules using the cluster report values from the source cluster as a reference.
2. Another option is disable Snapshot Sync jobs in the jobs window if the above workaround does not meet your needs to preserve expiry of snapshot settings.

UPDATE: Resolution for this OneFS issue is available in OneFS 8.0.0.3

T2046 Access Zone Replication limitation when all user mapping rules are deleted

Access Zone Replication successfully creates and updates user mapping rules and also successfully deletes user mapping rules except when all user mapping rules are removed from the source. In the case where all user mapping rules are deleted from the source, the Access Zone configuration replication job will not delete all on the target - the user mapping rules remain on the target.

T2241 Incorrect missing SPN alarm issued when PowerScale cluster joined to multiple Domains

In an environment where the PowerScale cluster is joined to multiple Domains, the OneFS SPN check command for a specified domain returns list of SPNs from other domains and lists them as missing. In this case Eyeglass issues an SPN alarm for missing SPNs based on the list returned even if there are no missing SPNs in the domain specified in the check command.

T2779 - Eyeglass Configuration Replication “Full Sync Mode” always updates when Default Settings on Source and Target cluster are not the same

If on the Source and Target cluster for an Eyeglass Configuration Replication Job the “Default Settings” say for SMB are not the same, each replication cycle will perform an update operation even though the shares are already synced and identical. Making the Default Settings the same for both clusters will eliminate this behaviour and return to expected behaviour to not perform the update when shares are determined to already be identical.

T2780 Same host moved to different NFS Export Client list not updated on target

For the cases where:

- same host is provisioned on multiple client list and then one host is removed
- Same host is moved from one client list to another

The change in NFS client list is not replicated to the target cluster. Target cluster client list must be updated manually.

T2908 New Eyeglass Configuration Replication Job cannot recover state and mode from the Eyeglass Fingerprint file.

When a SynclQ Policy is renamed, Eyeglass considers it to be a new SynclQ Policy and therefore creates a new Eyeglass Configuration Replication Job with the new name. The Eyeglass Fingerprint file which holds Eyeglass Configuration Replication Job Mode and State for recovery does not link the original Job name with the new name and can therefore not be used to recover these properties for the new Eyeglass Job.

T4289 Delete Share or Export may result in temporary Audit error

After a share or export is deleted as part of Eyeglass Configuration Replication Job, the next Eyeglass Configuration Replication Job Audit task may incorrectly expect that the object is not deleted resulting in an alarm such as " Replication job audit failed" - "objects not found on source or target cluster, hence audit fails" . The error is cleared on the next Eyeglass Configuration Replication Job where the Audit task correctly does not try to audit the deleted object.

T5972 No Error Message for Duplicate NFS Export on OneFS

7.2 Configuration Replication Failed

Duplicate NFS Export on OneFS 7.2 Configuration Replication failure is expected, however in this case there is no specific Info associated with failed step to identify the issue.

T14936 Short SPN not created during Configuration Replication

Eyeglass Configuration Replication will only create full version of SPN, no short version is created. Note that Access Zone and Pool Failover update both short and full version of SPN. If short version is required it can be manually added using AD tools.

T17097 Eyeglass Configuration Replication direction follows Enable/Disable state of SynclQ policies

Eyeglass Configuration Replication source cluster is the cluster of the enabled SynclQ policy. If there is a mirror policy and both SynclQ policies are enabled Eyeglass enters a defensive state showing Policy Disabled for both and no Configuration Replication is done. If a SynclQ policy is mistakenly enabled on the read only cluster Eyeglass does not evaluate the read/write state and will use the read only cluster as the source cluster for its Configuration Replication job.

Known Limitations for Eyeglass Features

T2350: Quota Self Serve Portal: Local Group Quotas not displayed when logged in with Local Group User

Quotas associated with a Local Group (for example wheel) are not displayed in the Quota self serve portal when logged in as a Local Group User for that group.

T1962: Default Role incorrectly shows Delete option

Eyeglass User Roles Default Roles incorrectly provide the option to be deleted when in fact they cannot be deleted.

Workaround: None Required. If the Delete option is selected the Default Role is not deleted.

T7980: Cluster Storage Monitor AD Group Template Quota

Creation does not created group quota for nested AD Groups

If an AD Group has sub-groups (nested groups) is configured as a Template for automated group quota creation, no group quotas will be created for sub-groups.

Workaround: Each group that requires automated group quota creation must be explicitly added to the relevant share permissions.

T8362: Cluster Storage Monitor AD Group Template Quota Creation does not respect highest quota setting user quota in nested AD Groups

If an AD Group has sub-groups (nested groups) is configured as a Template for automated user quota creation, user quota creation follows explicitly the quota limit for the sub-group when the user already has a quota for a higher limit. In this case, what should have happened is that template setting is ignored if there is already an existing user quota with a higher limit.

Workaround: Avoid use of nested AD groups for automated user quota creation.

T8193: special characters in Cluster storage monitor AD managed quota templates is not supported

If an AD Group templates, if the AD group name has special characters in the AD group name the quotas will not be applied.

Workaround: Avoid use of special characters when creating AD groups for AD managed quotas.

T9622: Unlock My Files! does not indicate error when PowerScale node is not reachable

If an PowerScale node is unreachable when Eyeglass is searching for open files there is no error message for the unreachable PowerScale nodes.

Workaround: None available.No open files displayed for unreachable nodes.

T15139 Data Config Migration Concurrent Jobs Limitation

When 2 Data Config Migration Jobs are started concurrently, each runs a separate Configuration Replication Job and the Configuration Replication Job cannot run concurrently. First one must complete before the second one can start.

Workaround: Recommend to run 1 Data Config Migration job at a time.

DR-136 Login with AD users leads to read-only Eyeglass

Issue: AD users cannot be added to user roles until a Powerscale cluster has been added.

Workaround: Add the powerscale cluster to inventory before modifying user roles.

Closing this task as done since this is not something we will ever fix.

Known Limitations for Eyeglass General

T2289 Backup Archive Job is not always displayed in the Running Jobs window

In some cases after a Backup Archive job is initiated it will not appear as a running task in the Jobs / Running Jobs window. Archive is still created and available for download on completion.

T2908 Renamed SyncIQ Policy does not link to RPO Reports from original SyncIQ Policy Name

When a SyncIQ Policy is renamed, Eyeglass considers it to be a new SyncIQ Policy. Therefore RPO Reporting for the original SyncIQ Policy name will not be linked to RPO reporting for the new SyncIQ Policy name.

T3170 Pending Quota Requests are not preserved on failover

If a failover is done while there are Quota Pending Requests, the Pending Requests are lost as the quota to which the request was originally made no longer exists on the original cluster after failover. The pending quota request will appear in the Quota Requests History in Error state.

T4579 Upgrade from 1.5.4 to 1.9 and greater Failover History

retrieves Failover Log for SyncIQ Job Reports

After an upgrade from 1.5.4 to 1.9 or greater, in the DR Assistant -> Failover History list the link to open SyncIQ Job Reports opens the Failover Log due to fact that prior to this release Failover Log and SyncIQ Job Report log were combined. In this case you are able to see the SyncIQ Job Reports related to failover at the bottom of the Failover Log.

T6300 After an Eyeglass restore with the -anyrelease option

the print screen functionality for SyncIQ Job Reports and

Eyeglass backups may be in error

After an Eyeglass restore to a new appliance using the --anyrelease option, print screen functionality may no longer be working due to a incorrect permission setting. This impacts SyncIQ Job Reports which will be missing the charts and generating an Eyeglass backup with print screens.

To workaround this issue:

1) ssh to the eyeglass appliance and login with the admin account (default password 3y3gl4ss)

2) assume root user by typing

```
sudo su -
```

And entering the admin password

3) vi /opt/superna/sca/data/Screenshots.json and write "<placeholder>" as a value in the "plain_text" field and then save it.

4) Copy and paste the following commands:

```
str=$(sudo cat /dev/urandom | tr -dc 'a-zA-Z' | fold -w 12 | head -n 1)
```

```
echo -e "$str\n$str" | passwd screenshots
```

```
sed -i "s/<placeholder>/$str/" /opt/superna/sca/data/Screenshots.json
```

5) Start a backup with print screens and follow in Running Jobs to verify the backup completes successfully.

T12034 Eyeglass appliance rediscover does not preserve

Eyeglass Job state unless Configuration Replication has run

If a change is made to an Eyeglass Job state or Job type and then there is an appliance rediscover before configuration job has been run the changed Job state / type will be lost.

T16137 Anyrelease restore does not restore all Ransomware Defender and Easy Auditor settings

There is no restore of settings from release 2.5.4 and earlier. For release 2.5.4 and earlier continue to capture all Ransomware settings (False Positive, Ignore List, Allowed Extensions, Security Guard) and Easy Auditor settings (Active Auditor Trigger settings, RoboAudit). Post restore verify settings and update where required before cluster up on ECA.

In all cases, restoring an Eyeglass backup using the --anyrelease option will not restore following Ransomware Defender and Easy Auditor settings:

Ransomware Defender: Event History, Threats Detected

Easy Auditor: Finished Reports, Scheduled Reports, Saved Queries

T16729 Role Based Access Control (RBAC) Known Limitations

- Isilon local users are not supported (Eyeglass local users are supported)
- Eyeglass doesn't resolve AD groups with @ & or ' in the name

T16821 anyrelease restore restrictions for restore to 2.5.7

1) Eyeglass DR Edition with version lower than 2.5.5 cannot be upgraded to 2.5.7 using the anyrelease option. Eyeglass must be upgraded to a minimum of 2.5.5 before anyrelease restore to 2.5.7 can be done.

2) Ransomware Defender, Easy Auditor and Performance Auditor deployments cannot use the anyrelease restore option to upgrade to a new appliance running 2.5.7. For case where a backup & restore is required due to 42.3 OS on original deployment, a backup & restore to 2.5.6 will have to be done first followed by an upgrade to 2.5.7 or in place OS upgrade prior to 2.5.7 upgrade.

Eyeglass Upgrade requires disk usage < 80%

Eyeglass disk usage must be lower than 80% for upgrade run file to succeed. Please contact support.superna.net for assistance to clear up disk space on the Eyeglass appliance.

T19368 Copy to Clipboard Size Limitation

The amount of information that can be copied using the Copy to Clipboard functionality in Eyeglass is limited by the operating system clipboard limits.

- Failover log is available on the Eyeglass appliance here:
`/srv/www/htdocs/failover_logs`
- Where Did My Folder Go set more restrictive filter to produce smaller set of results

T21890 OneFS Effective Cluster Version incorrect

For an Eyeglass installation with multiple clusters with different OneFS versions, adding or removing a cluster may result in temporary assignment of incorrect Effective Cluster Version. This is resolved the next time Configuration Replication runs.

Known Limitations for REST API

T18079 REST API - Change Eyeglass Configuration Job Disable/Enable must be done at same time as Job Type Change

The API to change Eyeglass Configuration Job state for Disable/Enable must be done together with a job state change in order to succeed.

REST API retrieval of Jobs Known Limitation

Retrieving information about a Configuration Replication Job or DR Readiness Job is available while the job is running and for 15 minutes once the job has completed. This is the same behaviour that is available from the GUI via the Jobs/Running Jobs window.

© Superna Inc

1.18. Current Release - Release Notes Easy Auditor

[Home](#) [Top](#)

- [Release 2.5.9](#)
- [Supported OneFS releases](#)
- [Supported Eyeglass releases](#)
- [Inter Release Functional Compatibility](#)
- [End of Life Notifications](#)
- [Support Removed in Eyeglass Release 2.5.9](#)
- [Deprecation Notices](#)
- [New / Fixed in 2.5.9](#)
- [New in 2.5.8.1-22116](#)
- [Fixed in 2.5.8.1-22116](#)
- [New in 2.5.8.1-22100](#)
- [Fixed in 2.5.8.1-22100](#)
- [Deprecated in 2.5.8.1-22080](#)
 - [Built In Reports Deprecated](#)
- [New in 2.5.8.1-22080](#)
 - [Built-In Access Report Now Reports per share](#)
- [Fixed in 2.5.8.1-22080](#)
 - [T21840 Easy Auditor - DLP trigger affected by quota sync schedule](#)
- [New/Fixed in 2.5.8-22028](#)
- [New in 2.5.8-21330](#)
- [Fixed in 2.5.8-21330](#)
 - [T22171 - Log4j Vulnerability - Upgrade to Log4j 2.17.0 \(2.5.8-21330 and higher Log4j 2.17.0 \)](#)
- [New in 2.5.8-21306](#)
 - [NEW - OneFS 9.3 Support](#)

- T19711 Easy Auditor new validation that selected path is on an audited Access Zone
- Fixed in 2.5.8-21306
 - T22033 Log4j Vulnerability - CVE-2021-44228
 - T20936 Bulk Ingest of Old Audit Data is not functional
- Technical Advisories
- Known Issues
- Reporting
 - T5907 No record for failed user query in Finished Reports
 - T6145 User with Eyeglass read-only position cannot run a custom query
 - T6149 Count Table and Access Report queries store unnecessary query parameters
 - T6293 Stale Access Report and Access Report display Cluster GUID instead of Cluster Name
 - T6313 Report Query Builder allows filter on Unlicensed Cluster
 - T6338 File Ext Input-only in the first line
 - T6339 Report Query Naming
 - T6349 Running Report Job State does not immediately reflect a cancelled Job
 - T6350 Easy Auditor Running Reports window inactive
 - T6404 Saved Custom User Queries show unrelated Built-In Query
 - T7049 Finished Report display issue for Duration
 - T9837 Warning on Wait for Spark Job
 - T10911 Share/Stale Access Report issue when AD has nested groups
 - T11752 Custom Real-time Audit policy User selection filtering
 - T11890 Able to save query without a name
 - T13573 Delete parent folder with subfolders shows duplicates in Where Did My Folder Go
 - T14722 Issues with custom report where path selected contains special language characters
 - T15037 Easy Auditor does not report files with multiple extensions correctly

- T15582 Easy Auditor issues where path has & or brackets
- T19561 Easy Auditor scheduled reports may not run
- T20078 Emailed built-in report may contain user SID
- T20661 Large Report cannot be downloaded from Windows
- T22708 Access Report only reports on shares using AD Group permissions
- T22719 Access Report reports extra information when reporting on share with same name in multiple Access Zone
- T22720 Access Report not compatible with LDAP retrieval of AD Users and Groups
- T22731 Access Report cannot be displayed in the GUI with large number of permissions
- T22738 Access Report does not report on nested groups
- Active Auditing
 - T8878 Cannot save DLP trigger for a different NE but same path
 - T6305 Invalid username causes Wiretap error
 - T7547 Wiretap does not show user name for NFS events
 - T12876 DLP trigger cannot be added
 - T15198 Active Auditor Triggers may have inaccurate Signal Strength
 - T15250 The command to reset Active Auditor event queue must be run twice
 - T16980 Active Auditor events Affected Files-CSV may not show all events
 - T19629 Expired Active Auditor Events not archived to Event History if Ransomware Defender has Automatic Learning enabled
 - T21226, T22604 Active Auditor Snapshot functionality follows Ransomware Defender Snapshot configuration
 - T8694 Robo Audit may show Success when it did not run
 - T11880 Robo Audit fails when configured to run on more than one cluster
 - T15175 Existing Robo Audit Logs lost formatting after upgrade to 2.5.6
- General
 - T5858 eactl commands do not switch to ecaadmin user

- T5915 Event retrieval stopped by Disable/Enable of Protocol Monitoring on the PowerScale
- T15457 HTML 5 vmware vcenter bug on OVA deployment
- T6097 UI Desktop Unexpected Behaviour
- T6617 PowerScale Directory Selector does not display hidden directories
- T8105 Alarm EAU0002 has no detailed information for failed auditor report
- T19929 Easy Auditor Directory Selector returns "Error retrieving directory info from cluster"
- EA-191 Stale Access Report shows incorrect entries
- EA-171 Bulk Ingest folder is not created automatically
- EA-172 Built-In scheduled report results are displayed in Manual report section
- EA-193 Bulk ingest job is not working with turboaudit REST API
- EA-167 Bulk Ingest is not retrieving archives created on the same day
- Reporting
 - Conditions under which audit events are not processed
 - T6260 Stale Access Report Known Limitations
 - T6478 Stale Access and Share Access Report AD User Limitation
 - T18936 Rerun of query required
- Active Auditing
 - T11540 Active Auditor may report on Audit Failure events
 - T12380 Ransomware Defender Ignore List settings are applied to Active Auditor analysis
 - EA-79 [Active Auditor-Active Event] Predicted signal doesn't show its type & value
- General
 - T8281 hbase major compaction affects queries
 - T16137 Anyrelease restore does not restore all Ransomware Defender and Easy Auditor settings
 - T16821 anyrelease restore restrictions for restore to 2.5.7

- [T16499 Easy Auditor reports double events](#)

What's New in Superna Eyeglass Easy Auditor Edition

Release 2.5.9

What's New! In Superna Eyeglass Easy Auditor Edition Release 2.5.9 can be found [here](#).

Supported OneFS releases

8.2.0.x

8.2.1.x

8.2.2.x

9.0

9.1

9.2

9.3

9.4

Supported Eyeglass releases

Superna Eyeglass Easy Auditor Version	Superna Eyeglass Version
2.5.9-22231	2.5.9-22231

2.5.8.1-22116	2.5.8.1-22116
2.5.8.1-22100	2.5.8.1-22100
2.5.8.1-22080	2.5.8.1-22080
2.5.8-22028	2.5.8-22028
2.5.8-21330	2.5.8-21330
2.5.8-21306	2.5.8-21306
2.5.7.1-21161	2.5.7.1-21161
2.5.7.1-21140	2.5.7.1-21140
2.5.7-21096	2.5.7-21096
2.5.7-21081	2.5.7-21081
2.5.7-21068	2.5.7-21068
2.5.6-20263	2.5.6-20263

Inter Release Functional Compatibility

	OneFS 8.2 and 9.x releases	OneFS 9.x releases
Reporting	Untested	Untested
Active Auditing	Untested	Untested

End of Life Notifications

End of Life Notifications for all products are available [here](#).

Support Removed in Eyeglass Release 2.5.9

Following removed in 2.5.9:

- Data access report - this report is being deprecated due to low usage and is replaced by the Search and Recover Who owns what? report to determine top users consuming space on a path.

- Top users report (creating and deleting) - these reports are being deprecated due to low usage and redundant to the widely used Where Did My Folder Go? reporting and Custom Triggers for Active Auditing.
- Count table report - this report is not required for end user / administrator and is being removed from the user interface
- Threat Detector 01 - this report is not required for end user / administrator and is being removed from the user interface
- Threat Detector 02 - this report is not required for end user / administrator and is being removed from the user interface

Deprecation Notices

No Deprecation Notice in this release.

New / Fixed in 2.5.9

Added support for enhanced triggers on directory events in easy auditor. Added GUI support for bulk ingestion of old audit records.

New / Fixed in 2.5.8

New in 2.5.8.1-22116

Refer to previous build information.

Fixed in 2.5.8.1-22116

Refer to previous build information.

New in 2.5.8.1-22100

Refer to previous build information.

Fixed in 2.5.8.1-22100

Refer to previous build information.

Deprecated in 2.5.8.1-22080

Built In Reports Deprecated

The following Built In Reports have been deprecated as indicated in the deprecation notice:

- Data access report - this report has been deprecated due to low usage and is replaced by the Search and Recover Who owns what? report determining top users consuming space on a path.
- Top users report (creating and deleting) - these reports have been deprecated due to low usage and are redundant to the widely used Where Did My Folder Go? reporting and Custom Triggers for Active Auditing.
- Count table report - this report is not required for the end user/administrator and has been removed from the user interface
- Threat Detector 01 - this report is not required for the end user/administrator and has been removed from the user interface
- Threat Detector 02 - this report is not required for the end user/administrator and has been removed from the user interface

New in 2.5.8.1-22080

Built-In Access Report Now Reports per share

The Built-In Access Report now reports on selected share permission rather than all shares for a selected cluster.

Fixed in 2.5.8.1-22080

T21840 Easy Auditor - DLP trigger affected by quota sync schedule

DLP trigger is no longer working in 2.5.8 as the quota inventory that is collected on the new schedule is not available to assess the trigger.

Resolution: Quota inventory is now available for DLP trigger operation.

New/Fixed in 2.5.8-22028

Refer to previous build information.

New in 2.5.8-21330

Refer to previous build information.

Fixed in 2.5.8-21330

Security

T22171 - Log4j Vulnerability - Upgrade to Log4j 2.17.0
(2.5.8-21330 and higher Log4j 2.17.0)

New in 2.5.8-21306

NEW - see What's New in 2.5.8 [here](#).

NEW - OneFS 9.3 Support

Support for OneFS 9.3 is introduced in release 2.5.8.

T19711 Easy Auditor new validation that selected path is on an audited Access Zone

Easy Auditor path selector now verifies whether the selected path falls under an Access Zone with protocol auditing enabled.

Fixed in 2.5.8-21306

T22033 Log4j Vulnerability - CVE-2021-44228

Resolution: log4j version updated to 2.15.0 which has patch for the vulnerability.

T20936 Bulk Ingest of Old Audit Data is not functional

The ability to bulk ingest old audit data is not functional as of 2.5.7.1-21140 release.

Resolution: Bulk Ingest of audit data is now functional. Requires ECA nodes to be running OpenSUSE 15.3. If ECA nodes not running this OpenSUSE version need to redeploy the 15.3 ECA nodes and backup and restore configuration file and mount file.

The PowerScale Directory selector currently has a maximum list size of 1000 so that environments with more than 1000 directories on the PowerScale some directories will be missing.

Resolution: Directory selector now displays the first 1000 folders and an additional folder shown as ... Select the "..." will display the next 1000 folders and so on.

Technical Advisories

Technical Advisories for all products are available [here](#).

Known Issues

Reporting

T5907 No record for failed user query in Finished Reports

If a user-based query fails, there is no record of the failed report in the Finished Reports.

Workaround: None Required - Email notification is provided for the failed query.

This does not affect path-only queries.

T6145 User with Eyeglass read-only position cannot run a custom query

In the Report Query Builder, a user who only has read-only permissions can only Load a previously saved query to review its setting. From this interface, no load can be run.

Workaround: Administrator with full privileges must create and save a query, after which a user with read-only permission can run it from the list.

T6149 Count Table and Access Report queries store unnecessary query parameters

If you save the Count Table or Access Report query, disabled report parameters may be saved with the report definition even though they do not apply.

Workaround: None required. Extra parameters are ignored.

T6293 Stale Access Report and Access Report display Cluster GUID instead of Cluster Name

In the Stale Access and Access Reports, the cluster is identified by its GUID instead of displaying the cluster name.

Workaround: To verify which cluster the report is for, from the Eyeglass web open the Inventory View. Right click on a cluster name and select "Show Properties" to view the cluster GUID.

T6313 Report Query Builder allows filter on Unlicensed Cluster

The Report Query Builder does not block the selection of an unlicensed cluster.

Workaround: None required. File activity/events are not stored for unlicensed clusters, and as such, any report would return with 0 records.

T6338 File Ext Input-only in the first line

Report Query File Ext filter is only editable in the first line. Clicking anywhere else in the box will not let you enter any text

Workaround: None required. Enter the File Ext filter at the top of the box.

T6339 Report Query Naming

Saved Report Query names can only contain 0 to 9, a to z (lowercase) and A to Z (uppercase) without any spaces, - or _ .

Workaround: None available.

T6349 Running Report Job State does not immediately reflect a cancelled Job

When a Running Auditor Job is cancelled, the Running Jobs view continues to show the Running state until the cancel task has been completed in its entirety.

Workaround: None required.

T6350 Easy Auditor Running Reports window inactive

The Easy Auditor Running Reports window may become inactive such that expired reports are not removed and you cannot click on a Report to see details of the execution.

Workaround: Refresh the browser session.

T6404 Saved Custom User Queries show unrelated Built-In Query

A saved Customer User Query details will incorrectly show

Report Picker: Data access report - users who are writing the most/least amount of data even though this custom report is not related to this built-in query.

Workaround: None required - other query information is relevant and accurate.

T7049 Finished Report display issue for Duration

Finished Report Duration column does not display the entire duration required to complete the query.

Workaround: None available. The duration can be seen in the Running Jobs view while the query is still in running state.

T7049 Finished Report display issue for Duration

Finished Report Duration column does not display the entire duration required to complete the query.

Workaround: None available. The duration can be seen in the Running Jobs view while the query is still in running state.

T7437/T12178 Employee Exit Report may not complete

In large environment with high event rate, the 30 day Employee Exit Report may not complete or it may complete with a large number of records but viewing/download of results limited to 10,000 records.

Workaround: Modify the query for less than 30 days to reduce number of records in report or build a custom report using the Report Query Builder.

T7823 Email Report shows success when error with attachment

Emailing report shows as success even when there is an issue in attaching the report.

Workaround: Re-run the report or contact support at support.superna.net for assistance.

T9837 Warning on Wait for Spark Job

A Warning may appear on a Running Report Job Details for the Wait for Spark Job step with info “warning: Applicationid could not be retrieved” without impacting the completion of the query itself.

Workaround: None required

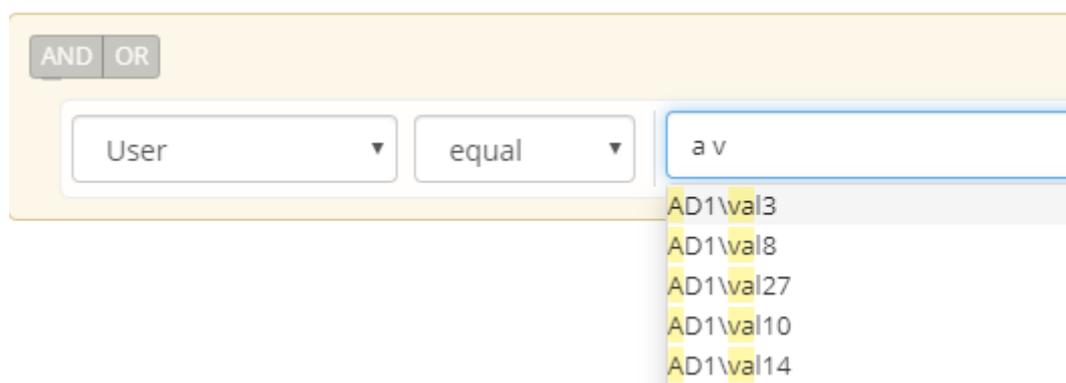
T10911 Share/Stale Access Report issue when AD has nested groups

The built in Share Access and Stale Access Reports do not show user access to a share for those users that are members of a nested subgroup of the AD group configured in the share permissions.

Workaround: None available.

T11752 Custom Real-time Audit policy User selection filtering

To select a name from the User drop-down list on a Custom Real-time Audit policy trigger you must first type the first letter of the user domain (name format is DOMAIN\name) after which you can type any other letter from user name for further filtering. Leave a space between first letter and next letter if letters are not adjacent in user name. Example below



Workaround: None required.

T11890 Able to save query without a name

The GUI allows saving of query without name. Query can be run but cannot be deleted. Only one query without a name will be able to be saved.

Workaround: Enter name when saving a query.

T13573 Delete parent folder with subfolders shows duplicates in Where Did My Folder Go

Where Did My Folder Go search results for a parent deleted folder where subfolders were also deleted duplicates entries for some folders.

Workaround: None required

T14722 Issues with custom report where path selected contains special language characters

Custom report where path selected contains special language characters may either not run or will complete with 0 results.

Workaround: Selecting a path higher up in the directory tree without special language characters may return results where special language characters not displayed correctly. Note that Wiretap and Where Did My Folder Go provide an option for reporting on these paths.

T15037 Easy Auditor does not report files with multiple extensions correctly

For the case where a file has multiple extensions in the Easy Auditor report the first extension only is reported. For example file.pdf.gz is reported as a pdf not as a gz file.

Workaround: None available.

T15582 Easy Auditor issues where path has & or brackets

Easy auditor has following issues for path with &:

- user or path search where path contains & return 0 results
- DLP trigger cannot be saved where path contains &
- Mass Delete trigger where path contains & returns 0 results

Workaround: Select path above path with & when defining custom search, DLP or Mass Delete triggers

Easy auditor has following issues where path contains bracket

- Wiretap, Where did My Folder Go, Active Auditor triggers not functioning

Workaround: No workaround available

T19561 Easy Auditor scheduled reports may not run

Under some circumstances the license state for a Powerscale cluster is lost after which scheduled reports may fail to run.

Workaround: Manually run the scheduled query for the desired timeframe.

T20078 Emailed built-in report may contain user SID

The summary in the email body for some built in reports shows user SID instead of the associated user id.

Workaround: The attached CSV file has SID resolved to user id.

T20661 Large Report cannot be downloaded from Windows

There is an issue downloading reports with very large number of records from Windows using Chrome browser. On download a "Loading" message appears but once the

Loading message stops, no download is started. This issue does not appear on MAC with Chrome browser.

Workaround:

1) On Windows, large reports can be successfully downloaded using Firefox browser build 72

2) The file is generated and present on the Eyeglass appliance and could be retrieved using a tool such as WinSCP. The report files are located on the Eyeglass appliance in the folder: /srv/www/htdocs/csv

T22708 Access Report only reports on shares using AD Group permissions

The Access Report can only be used to report on permissions for shares using AD Groups. Share permissions to AD Users directly or well known user/group such as Everyone results in an error when running the report.

Workaround: None available.

T22719 Access Report reports extra information when reporting on share with same name in multiple Access Zone

If there are multiple Access Zone configured on the PowerScale and those Access Zone contain shares with the same name, reporting on one of those shares will report for all shares of that name and not be filtered on the Access Zone selected.

Workaround: None required.

T22720 Access Report not compatible with LDAP retrieval of AD Users and Groups

If Eyeglass is configured to use LDAP for retrieval of AD Users and Groups, the Access Report cannot report on share access as it relying on PowerScale API calls for that information.

Workaround: None available.

T22731 Access Report cannot be displayed in the GUI with large number of permissions

If the resulting Access Report has more than 1000 permissions, the report cannot be viewed from the Easy Auditor GUI. Opening the report causes the GUI to freeze.

Workaround: Download report with large number of permissions to view it.

T22738 Access Report does not report on nested groups

The Access Report only reports on the users in the parent group where a share has permissions configured with nested groups.

Workaround: None available.

Active Auditing

T8878 Cannot save DLP trigger for a different NE but same path

With 2 licensed clusters a Data loss prevention policy cannot use the exact same path on both clusters if entering 2 different policies one for each cluster.

Work around: none only the first cluster and path can be added.

T6305 Invalid username causes Wiretap error

If you enter an invalid username that cannot be resolved when setting up a Wiretap active auditing job it causes the job creation to fail with the following error:

Failed to create new wiretap:

Server error when processing request: java.lang.NullPointerException

Workaround: Enter a username that can be resolved in the documented supported format.

T7547 Wiretap does not show user name for NFS events

For events generated over NFS protocol, Wiretap does not include user name in the event information. Only client IP address is displayed.

Resolution: A custom query can be built using the Report Query Builder based on path and timeframe in order to view user name.

T12876 DLP trigger cannot be added

An error (Error saving response) occurs when adding a DLP trigger if there is an existing directory quota without data-protection overhead option enabled on the the path that a DLP trigger is being configured for.

Workaround: If possible, delete the existing quota and allow new quota to be created as part of adding the DLP trigger. Note that the directory quota that is created will be created with the data-protection overhead option enabled.

T15198 Active Auditor Triggers may have inaccurate Signal Strength

Active Auditor trigger processing (DLP, Mass Delete, Custom Triggers) may receive duplicate events and as a result show a higher Signal Strength than is actually the case.

Workaround: None required. The duplicate events will cause early detection of configured triggers. The associated CSV for files involved in the detection is correct.

T15250 The command to reset Active Auditor event queue must be run twice

The command `igls adv eventTriggers set --operation=reset --topic=ea` must be run twice to clear the queue.

Workaround: Execute the command a second time to clear the queue.

T16980 Active Auditor events Affected Files-CSV may not show all events

Under some circumstances the Affected Files-CSV may not show all events for the Active Auditor trigger as the timeframe for the report may result in some events being excluded.

Workaround: Use the Report Query Builder to run a query with the same conditions and user as the associated trigger and a timeframe that starts before the detected time. Typically starting query an hour prior to the event would ensure all events were listed but may also include some audit events that are not related to the trigger.

T19629 Expired Active Auditor Events not archived to Event History if Ransomware Defender has Automatic Learning enabled

If the Ransomware Defender settings has Automatically Learn.... setting selected, an Active Auditor event that matches criteria for Automatic Learning encounters an error when it expires which prevents it from being archived to the Event History list. Impact: There is no impact on the detection of the Active Auditor event only on expiry the event is not moved to the event history as it should be.

Workaround: Event can be moved to the Event History by manually archiving as unsolved from the Action menu for the event.

T21226, T22604 Active Auditor Snapshot functionality follows Ransomware Defender Snapshot configuration

The snapshot behaviour for Active Auditor Mass Delete and manual snapshot creation follow the configuration for snapshot budget, and snapshot enable/disable in the Ransomware Defender / Snapshots window. Ransomware Defender snapshot logic for user share snapshot is followed if configured rather than a snapshot for the mass delete path.

Workaround: Do not use the Create Snapshot checkbox in the Easy Auditor / Active Auditor window to manage Active Auditor snapshots. It does not have any effect. Use the Ransomware Defender / Snapshots window to enable / disable snapshots.

Important - configuration here also affects snapshot management for Ransomware Defender. User share snapshot will also protect the mass delete path as user share would provide access to this location in the filesystem.

Robo Audit

T8694 Robo Audit may show Success when it did not run

Robo Audit may show as having successfully completed when in fact it did not run. For example:

- Robo Audit configured but disabled
- Robo Audit misconfigured and enabled

Workaround: Open the Robo Audit logs to see details of Job Execution.

T11880 Robo Audit fails when configured to run on more than one cluster

When configured to run on more than one cluster, Robo Audit job will succeed for one cluster but fail for the subsequent cluster.

Workaround: Configure Robo Audit to only run on one cluster.

T15175 Existing Robo Audit Logs lost formatting after upgrade to 2.5.6

Any existing Robo Audit logs viewed from the Eyeglass GUI will have lost the formatting after upgrading to 2.5.6.

Workaround: None required. New logs will have the correct formatting.

General

T5858 ecactl commands do not switch to ecaadmin user

If you are logged into an ECA node as root user and execute an ecactl command, you are prompted to login as the ecaadmin user to continue but even though the console

indicates that the login as ecaadmin is underway the login never completes and the command cannot be executed.

Workaround: Login to ECA as ecaadmin user when using ecactl commands.

T5915 Event retrieval stopped by Disable/Enable of Protocol Monitoring on the PowerScale

If you disable / enable Protocol Auditing on the PowerScale cluster the ECA does not recover and does not begin reading events once Protocol Auditing enabled again.

Workaround: If you need to disable/enable Protocol auditing down the ECA cluster first

`Ecactl cluster down`

Then disable Protocol Auditing on the PowerScale cluster

After you have enabled Protocol Auditing on PowerScale cluster, the bring the ECA back up:

`ecactl cluster up.`

T6004 PowerScale Directory Selector Usage

In order to populate a cluster in the Directory Selector a directory must be selected in the file tree.

Workaround: None required. Once cluster is populated a path can be selected from the tree or typed in but must begin with `/ifs` .

T15457 HTML 5 vmware vcenter bug on OVA deployment

Some versions of vmware vcenter HTML user interface have a known issue with OVA properties being read correctly post power on, leading to first boot issues.

Workaround: use the Flash client as a work around.

T6097 UI Desktop Unexpected Behaviour

If you move a window to the edge of the Eyeglass desktop it may become stuck in that position.

Workaround: Refresh browser.

T6617 PowerScale Directory Selector does not display hidden directories

Directories that start with a dot (.) are not displayed in the PowerScale Directory Selector.

Workaround: Use the PowerScale Directory Selector to enter \ifs\ and then enter the remainder of the path manually.

T8091 Login Monitor Report does not have Sorting

When viewing the Login Monitor Report Built-In query results from the GUI, sorting on columns Logons, Logoffs, and failed Logons is not available.

Workaround: Download the report csv file and open in spreadsheet for sorting and filtering of data.

T8105 Alarm EAU0002 has no detailed information for failed auditor report

The alarm Info for EAU0002 alarm "Auditor report failed" does not have any detailed information on cause of report failure.

Workaround: In Easy Auditor / Running Reports tab select the report that failed and in the Job Details expand the tree and select the Info link for the failed step.

T8249 Canceling Easy Auditor Running Report results in Critical severity alarm

Cancelling a running auditor report results in a Critical Severity alarm.

Workaround: None required. This alarm is informational only and does not indicate any critical issue in Easy Auditor.

T19929 Easy Auditor Directory Selector returns "Error retrieving directory info from cluster"

The Directory Selector directory tree display encounters an issue displaying the tree when the folder structure count (including files) exceeds 100,000.

Workaround: In the Directory Selector, select the cluster and the first folder "ifs" then manually enter the remainder of the path. Important: path is case sensitive and must match the filesystem path.

EA-191 Stale Access Report shows incorrect entries

Stale Access Report shows duplicated entries for users who accessed the share recently

Workaround:

1. import CSV into excel
2. sort by last access date (make sure records that have last access are at the top of the sheet)
3. remove duplicates on the user column.

4. Data that remains is accurate.

EA-171 Bulk Ingest folder is not created automatically

Bulk Ingest folder is not created automatically

workaround:

```
1 mkdir -p /opt/superna/sca/data/bulkingest
```

```
2touch /opt/superna/sca/data/bulkingest/bulkingest.json
```

```
3chown sca:users /opt/superna/sca/data/bulkingest/bulkingest.json
```

EA-172 Built-In scheduled report results are displayed in Manual report section

Built-In scheduled report results are displayed in Manual report section

EA-193 Bulk ingest job is not working with turboaudit REST API

Bulk ingest job is not working with turboaudit REST API

EA-167 Bulk Ingest is not retrieving archives created on the same day

As a Bulk Ingest user, I want to be able to use archives created in the last 24 hours. Now we can only use it for ingestion archives that are older than 1 day.

Known Limitations

Reporting

Conditions under which audit events are not processed

In the following situations audit events will not be processed and any audit events which occur while processing is down are dropped - they are not recovered by post processing:

- ECA NFS mount is down: Each ECA node is responsible for reading audit events for a specific set of PowerScale nodes. While the ECA NFS mount is down, audit events for these PowerScale nodes are dropped.
- ECA down: Each ECA node is responsible for reading audit events for a specific set of PowerScale nodes. While the ECA NFS mount is down, audit events for these PowerScale nodes are dropped.

T6260 Stale Access Report Known Limitations

1) The Stale Access Report Built-In query does not report on activity for shares under following conditions:

- Share access by AD user with run as root permissions
- Share access by AD group where AD group has nested group and access by user in sub-group

2) With nested share topology, share access will be reported for "parent" share and "child" share when access was done via "child" share. For example, if PowerScale is configured with the default /ifs share, access by any other share will also be reported as access via the /ifs share.

T6361 Reporting for shares with local user permissions unsupported

Reports generated against shares which have a local PowerScale user permission configured may give unexpected results in the report and may cause email notification to fail.

T6478 Stale Access and Share Access Report AD User Limitation

Reports have been successfully generated against AD environment with up to 4000 users is current limit, Future release to extend this limit.

T2842 Login Monitor Report Known Limitations

The Login Monitor Report Built-In query has following Known Limitations:

- NFS login is not reported
- Failed login due to invalid password, or invalid user are reported by user SID
- A login where user does not appropriate share permission is reported as a Logon and Logoff together

T18936 Rerun of query required

Query may need to be re-run if the ECA OS product requirements have not been met for disk latency as this can cause search jobs to timeout in Eyeglass. The job may still complete by reviewing the finished jobs report tab. If the report shows error you will need to re-run the job. OS latency or memory issues can cause this and permanent fix should move the ECA VM's to flash based storage. This command can be run to look at disk statistics:

```
ecactl cluster exec iostat -xyz 6 6
```

This command will return a sample of disk IO per ECA. Consult [documentation](#) on latency requirements.

Active Auditing

T6061, T6465 Wiretap event rate display maximum of 25 events / s

Wiretap Watch window is limited to displaying events at a maximum of 25 events/s. If there are more than 25 event/s which match the Wiretap filter this will result in events being dropped and not displayed.

Workaround: Define filter with smaller scope by adding a user and defining more precisely the path in the filter. A report may also be run using same filter to retrieve all related results.

T7500 DLP Known Limitations

DLP Active Auditing has following Known Limitations:

- Small Files DLP threshold affected by PowerScale Quota Usage Reporting

For small files, PowerScale Quota Usage reports a larger usage than actual storage consumed. When setting a DLP threshold you must consider the threshold% against the quota reported usage. For example, if actual space consumed by 1 small files is 20b but quota usage is reported by PowerScale as 8K then the threshold to detect copy of that file is not 100%, it is 20b/8K.

- DLP generate 1 signal when threshold crossed for any size of copy

Any copy that crosses the configured threshold will generate only 1 signal - whether the copy is one time the threshold configured or many times the threshold configured.

T7525 Active Auditor Affected Files also shows Ransomware Defender Affected Files

When viewing the Affected Files for an Active Auditor event, any files associated with a Ransomware Defender event that has occurred at the same time are also displayed.

Workaround: Download the csv file and use the path associated with the Active Auditor event from the GUI to filter the results.

T8744 No event processing once Signal Strength passes 2 times Critical Threshold

Once a Security Event or Active Audit event has passed 2 times the Critical threshold configured in Ransomware Defender Settings, there is no further processing of Signals for the associated user. In all cases actions based on Critical threshold settings would have been already taken prior to reaching the 2x level.

For the case where both Ransomware Defender and Easy Auditor are licensed, reaching Signals processed count of 2 times Ransomware Critical threshold for a particular user limit is applied independently for Ransomware Defender and Easy Auditor.

Workaround: None available.

T11540 Active Auditor may report on Audit Failure events

Active Auditor may report on failed audit events.

Workaround: Reporting of failed audit events can be disabled on the PowerScale audit settings. Please contact support.superna.net for more information on disabling reporting on failed audit events.

T12380 Ransomware Defender Ignore List settings are applied to Active Auditor analysis

Analysis of file events for Active Auditor triggers will ignore an user, IP or path that is configured in the Ransomware Defender Ignore list.

Workaround: None available.

EA-79 [Active Auditor-Active Event] Predicted signal doesn't show its type & value

The predicted signal is not supported in Active Auditor.

Workaround: None.

General

T8281 hbase major compaction affects queries

An hbase major compaction will prevent queries happening at the same time from completing.

Workaround: Re-run query once hbase major compaction has completed.

T16137 Anyrelease restore does not restore all Ransomware Defender and Easy Auditor settings

There is no restore of settings from release 2.5.4 and earlier. For release 2.5.4 and earlier continue to capture all Ransomware settings (False Positive, Ignore List, Allowed Extensions, Security Guard) and Easy Auditor settings (Active Auditor Trigger settings,

RoboAudit). Post restore verify settings and update where required before cluster up on ECA.

In all cases, restoring an Eyeglass backup using the --anyrelease option will not restore following Ransomware Defender and Easy Auditor settings:

Ransomware Defender: Event History, Threats Detected

Easy Auditor: Finished Reports, Scheduled Reports, Saved Queries

T16821 anyrelease restore restrictions for restore to 2.5.7

Ransomware Defender, Easy Auditor and Performance Auditor deployments cannot use the anyrelease restore option to upgrade to a new appliance running 2.5.7. For case where a backup & restore is required due to 42.3 OS on original deployment, a backup & restore to 2.5.6 will have to be done first followed by an upgrade to 2.5.7 or in place OS upgrade prior to 2.5.7 upgrade.

T16499 Easy Auditor reports double events

In some cases it will be expected that a single operation such as deleting a folder is reported by the SMB protocol or Isilon as multiple delete events that appear as duplicates. Easy Auditor will record events as logged by Isilon and display all recorded events which may appear as duplicate but in fact is expected.

© Superna Inc

2. What's new Release Information

[Home](#) [Top](#)

- [What's new in Release 1.1.12 for Golden Copy](#)
- [What's new in Release 2.5.9.1 for DR, Ransomware Defender, Easy Auditor](#)
- [What's new in Release 2.5.10 for DR Ransomware Defender, Easy Auditor, Airgap](#)
- [What's new in Release 1.1.13 for Golden Copy, CBDM, Archive Engine](#)
- [What's new in Release 1.1.14 for Golden Copy, Archive Engine, Cloud Browser for Data Mobility](#)
- [What's new in Golden Copy Search 1.2.0](#)
- [What's new in Release 2.5.11 for DR, Easy Auditor, Airgap, Ransomware Defender](#)
- [What's new in Release 1.1.15 Golden Copy, CBDM, Archive Engine](#)
- [What's new in Release 2.5.12 Easy Auditor, AIRGAP, Ransomware Defender, Eyeglass DR](#)
- [What's new in the 3.1.0 Release](#)
- [What's new in Release 3.1.1 RWDAWS](#)
- [What's new in Release 1.1.16 Golden Copy, CBDM, Archive Engine](#)
- [What's new in Release 2.6.0 for DR, Easy Auditor, Airgap, Ransomware Defender](#)
- [What's new in Release 1.1.17 for Golden Copy, CBDM, Archive engine](#)
- [What's new Platform 1.0.0](#)
- [What's new in Release 2.6.1 for DR, Easy Auditor, Airgap, Ransomware Defender](#)
- [What's new in Release 1.1.19 for Golden Copy, CBDM, Archive Engine](#)
- [What's new in Release 2.6.2 Easy Auditor, Airgap, Ransomware Defender, Eyeglass DR](#)
- [What's new in Release 3.2.0 RWDAWS](#)
- [What's new in Release 1.1.20 Golden Copy, CBDM, Archive Engine](#)
- [What's new in Release 2.6.3 Easy Auditor, Airgap, Ransomware Defender, Eyeglass DR](#)

- What's new in Release 2.6.4 Easy Auditor, Airgap, Ransomware Defender, Eyeglass DR
- What's new in Release 1.1.21 Golden Copy, CBDM, Archive Engine

© Superna Inc

2.1. What's new in Release 1.1.12 for Golden Copy

Home Top

- [What's new in Release 1.1.12](#)
 - [New in this release:](#)
 - [Fixed in this release:](#)
 - [GC-1078 UI - Pause and Start buttons have no action](#)
 - [GC-1513 Golden Copy special character regression for ECS, AWS](#)

What's new in Release 1.1.12

GoldenCopy Release 1.1.12

New in this release:

1. [Cloud Browser for Data Mobility \(CBDM Browser\)](#)
 - a. This is a new concept in the cloud and on premise data storage management.
Core features:
 - i. Hide the complexity to end users of copying, moving, syncing data from on premise storage to object S3 cloud storage.
 - ii. Enable end users to easily select data on premise or in the cloud for:
 - iii. data movement within the cloud
 - iv. from the cloud to on premise
 - v. from on premise to the cloud

vi. Enables single source of truth concept that defaults to moving data versus copy to avoid the version nightmare.

vii. Compliance with "[The Evolution of Media Creation: A 10-year vision for the future of media production, post and creative technologies](#)"

2. On the Archivedfolders tab, the archivedfolders that don't belong to logged-in users were hidden.

3. Small File Optimization was made. Small file throughput was improved

4. Hard soft links are now supported when doing a subdir recall

5. Job able to resume Archiving and Accepting files after a cluster down and up

6. Pause a folder with a job in progress and cluster down/up - jobs view is preserved

Fixed in this release:

GC-1078 UI - Pause and Start buttons have no action

Pause and Start buttons in the Archived Folder tab are not available.

GC-1513 Golden Copy special character regression for ECS, AWS

Golden Copy special character regression for ECS, AWS

© Superna Inc

2.2. What's new in Release 2.5.9.1 for DR, Ransomware Defender, Easy Auditor

Home Top

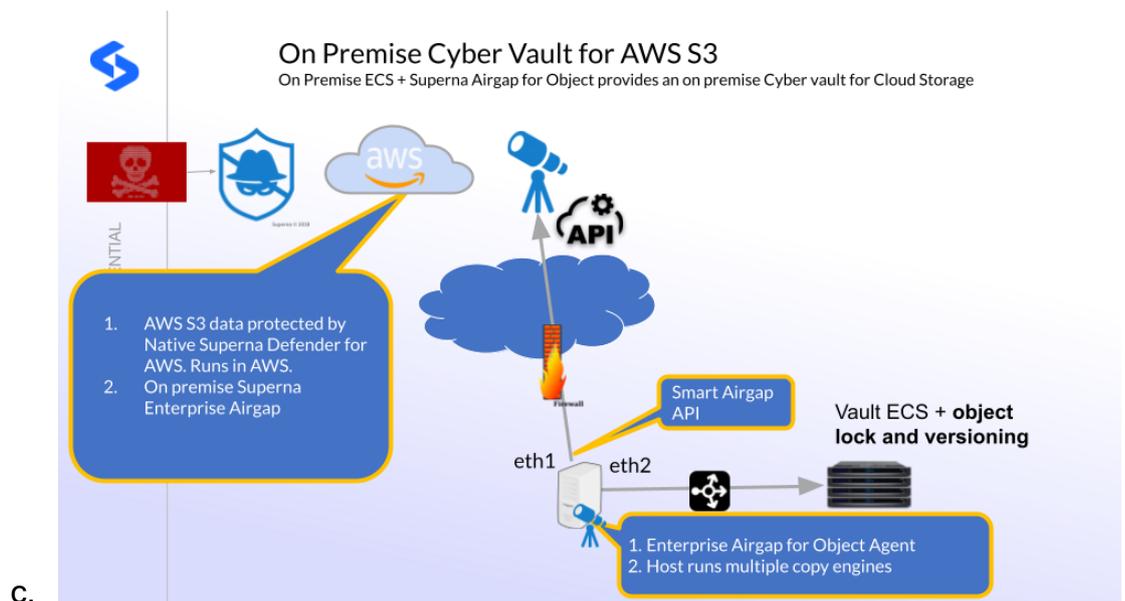
- [What's new in Release 2.5.9.1](#)
- [Ransomware Defender Release 2.5.9.1](#)
 - [New in this release:](#)
 - [Fixed in this release:](#)
 - [RWD-228 Syntax error in on-boot preventing proper startup timing.](#)
 - [RWD-222 enable zkcleanup.timer by default](#)
 - [RWD-145 \[RWD-NFS Event\] Major & critical events are locked out with default rule when reach threshold value even if - igls rsw nfsevents set --enabled=snapshotonly](#)
 - [RWD-146 \[RWD-NFS Event\] Lockout option in Actions is also removed for SMB event when set igls rsw nfsevents set --enabled=snapshotonly](#)
 - [RWD-113 Wrong Ransomware event state when created with POST /v2/ransomware/lockout/{user}](#)
- [Easy Auditor Release 2.5.9.1](#)
 - [New in this release:](#)
 - [Fixed in this release:](#)
- [Eyeglass DR Edition Release 2.5.9.1](#)
 - [New in this release:](#)
- [Ransomware Defender AirGap 2.0 Release 2.5.9.1](#)
 - [New in this release:](#)

What's new in Release 2.5.9.1

Ransomware Defender Release 2.5.9.1

New in this release:

1. zkcleanup.timer Runs by default on install/upgrade
2. The NFS implementation to be more consistent with SMB processing and enabled with snapshot only for NFS globally.
3. Beta - Cloud to on premise Airgap
 - a. Enables AWS Cloud data to be protected to an on premise Dell ECS object platform
 - b. Requires Defender for AWS and Enterprise Airgap for ECS



Fixed in this release:

RWD-228 Syntax error in on-boot preventing proper startup timing.

Workaround: not necessary; verify startup has finished on other nodes, if applicable, before attempting to use the ECA.

RWD-222 enable zkcleanup.timer by default

As an ECA user, I don't want to have to run `systemctl enable --now zkcleanup.timer` to start the service. This should be run by default on install/upgrade.

RWD-145 [RWD-NFS Event] Major & critical events are locked out with default rule when reach threshold value even if - `igls rsw nfsevents set --enabled=snapshotonly`

Major & critical events are locked out with default rule when reach threshold value even if -

`igls rsw nfsevents set --enabled=snapshotonly`

Steps-

- 1.Set `igls rsw nfsevents set --enabled=snapshotonly` in eyeglass
- 2.Raise NFS Event with Major/Critical severity (Detector Mode -Enforcement)
3. Observe Locked out event with critical severity & Major event locked out after expiry

Expected Result -

It should not lockout nfs event even when we reach threshold value for Major & Critical events

RWD-146 [RWD-NFS Event] Lockout option in Actions is also removed for SMB event when set `igls rsw nfsevents set --enabled=snapshotonly`

Lockout option in Actions is also removed for SMB event when set `igls rsw nfsevents set --enabled=snapshotonly`

Workaround: you can set `igls rsw nfsevents set --enabled=true/false/snapshotonly`

RWD-113 Wrong Ransomware event state when created with POST /v2/ransomware/lockout/{user}

The Ransomware event that is created using POST /v2/ransomware/lockout/{user} API call has TO_LOCKOUT state. This event should be created with LOCKED_OUT state.

Workaround: manually run the lockout job from the actions menu on the event.

Easy Auditor Release 2.5.9.1

New in this release:

The bulk Ingestion path is updated. The path changed in system.xml to the default one /ifs/.ifsvar/audit/logs/. The path can be updated with this command as well : igls config settings set --tag=<tagname> --value=<value> where tagname is bulkingestpath and the value is the new path where the gz files are.

Fixed in this release:

EA-167 Bulk Ingest is not retrieving archives created on the same day

Eyeglass DR Edition Release 2.5.9.1

New in this release:

1. OneFS 9.5 is now supported for DR
2. Zookeeper in restart loop due to 'Unable to load database on disk' was fixed

3. A new popup warning displays if a user adds an Isilon cluster with a OneFS version that's higher than what the current software version

Ransomware Defender AirGap 2.0 Release

2.5.9.1

New in this release:

1. Initial config settings are lost after cluster down on ECSsync UI. We added a default configuration which will be loaded at cluster up. There is no email in it, and the path of it is at `/opt/emc/ecs-sync/config`
2. We added sync schedules via CLI or cron string to change Airgap jobs schedules

to check the existing schedule:

```
ligls airgap changeschedule --job="<Job-name>"
```

to change the airgap job schedule:

```
ligls airgap changeschedule set --job="<job-name>" --cronstr=<5-fields-cron-string>
```

3. File transfer over SSL can use standard encryption and ports to secure the data.

2.3. What's new in Release 2.5.10 for DR Ransomware Defender, Easy Auditor, Airgap

[Home](#) [Top](#)

- [Eyeglass DR Release 2.5.10](#)
 - [New in this release:](#)
 - [Supportability](#)
- [Ransomware Defender Release 2.5.10](#)
 - [New in this release:](#)
 - [Usability](#)

What's new in 2.5.10 Release

Eyeglass DR Release 2.5.10

New in this release:

Supportability

1. SPN validation during config replication can now be disabled.
2. Eyeglass Notification Center From address TLD verification was removed.
3. The 9.5.x.x Isilon versions to support Isilon were added.

Ransomware Defender Release 2.5.10

New in this release:

Usability

1. Critical path separation by protocol was added
2. NFS snapshot configuration is now in the UI.

© Superna Inc

2.4. What's new in Release 1.1.13 for Golden Copy, CBDM, Archive Engine

[Home](#) [Top](#)

- [Golden Copy Release 1.1.13](#)
 - [New in this release:](#)
- [Media Mode](#)
- [Archive Engine Release 1.1.13](#)
 - [AWS Deep Archive recall](#)

Golden Copy Release 1.1.13

New in this release:

Media Mode

Support for symlinks and hardlinks. Symlinks and hardlinks are uploaded as a link 'representation', which can then be used during recall to apply the links after download.

1. Support folder paths and their metadata object for paths longer than 1024 characters.
2. The user is now able to download files with paths longer than 1024 characters that have been uploaded with the GoldenCopy long path feature.
3. The BYTES_ERRORED statistic was added for hardlinks, symlinks, and inodes.
4. The recall is now supported for folders with hardlinked data.
5. Broken links are tracked and viewable in the statistics.
6. Symlinks pointing to hardlinks are now supported for archive and recall.

7. Discrete statistics for symlinks uploaded by incremental archiving jobs are now viewable.
8. All statistics related to the long path feature are now viewable in grafana.
9. The optimization to avoid checking for object existence before archive is now compatible with the hardlink feature.

Archive Engine Release 1.1.13

AWS Deep Archive recall

Supports simple recalling of objects from Glacier, Glacier_IR, and Deep Archive tiers without additional configuration required.

1. Copying objects into the staging folder only when they've been successfully staged from the deep archive is now available.
2. Indication in the cloud browser that an object is being staged from the deep archive is shown.
3. The expiration of the restored deep archive object was handled.
4. Stage files from the deep archive, when selected for recall now available.
5. Custom queueing of Deep Archive jobs was implemented
6. A single download button for DEEP_ARCHIVE objects was added.
7. Statistics for deep archive recall are now viewable.
8. DEEP_ARCHIVE_FUNCTIONALITY env var was removed.
9. Support All AWS Tiers for recall now.

© Superna Inc

2.5. What's new in Release 1.1.14 for Golden Copy, Archive Engine, Cloud Browser for Data Mobility

[Home](#) [Top](#)

- [Golden Copy Release 1.1.14](#)
 - [New in this release:](#)
 - [Version Based Recall](#)
 - [Usability Enhancements](#)
 - [Fixed in this release:](#)
- [Archive Engine Release 1.1.14](#)
 - [Fixed in this release:](#)
- [Cloud Browser for Data Mobility 1.1.14](#)
 - [Overview](#)
 - [New in this release:](#)
 - [Usability Enhancements CBDM](#)

What's New 1.1.14

Golden Copy Release 1.1.14

New in this release:

Version Based Recall

1. Date Based Recall on the UI is now available. During recall, users can now enter a date and recall the version of the object that was most recently uploaded before the selected date.

Usability Enhancements

1. Auto retry of failed folders and files with new job spawned at the end of archive job.
2. `--folder-only` option added to re-run.
3. Functionality `--follow` tag to archivedfolders recall is now available.

Fixed in this release:

1. Longpath - Incremental Modify (Content) update the inode for Hardlink. Inside a longpath, after changing the content of a hardlink, the inode now gets updated on s3. [GC-1750](#)

Archive Engine Release 1.1.14

Fixed in this release:

1. The folder object is now not recalled when the recall source path is at the same level. [SA-354](#)
2. The restore Pipeline Recall job doesn't show "Staged" twice now. [SA-773](#)
3. The statistics for the deep archive process are shown properly now. [SA-775](#)

Cloud Browser for Data Mobility 1.1.14

Overview

This feature enables MovieLabs 2030 architecture by combining S3 cloud IAM and on premise SMB share level security to provide a seamless content creator data mobility

solution. The web based user interface stores a view of S3 bucket level access dynamically detected from AWS S3 service and the SMB shares are dynamically detected based on Active Directory login.

The user can select media assets from the cloud and have them moved, copied or synced to on premise storage for editing workflows. Golden Copy has advanced data orchestration features to allow JED (Just Enough Disk) editing workflows to cache on premise data for high speed low latency playback and editing. End of day work is moved back to the cloud automatically and data that stays on premise is backed up automatically.

End users see an endless pool of storage in the cloud and can launch data mobility jobs without IT assistance in the self service portal. The jobs can email the user when the data movement is completed or they can monitor the job from the GUI.

Full multi-tenant user access gives administrators the ability to monitor jobs for all users and track security of data management tasks easily from a single pane of glass showing data assets on premise or in the cloud and who did what when.

New in this release:

Usability Enhancements CBDM

1. Moving data to CBDM share is available now.
2. Job's affected files to CSV file for download can be exported now.
3. Faster jobs history table, with in memory cache

© Superna Inc

2.6. What's new in Golden Copy Search 1.2.0

[Home](#) [Top](#)

What's New 1.2.0

Search Release 1.2.0

New in this release:

1. GC Job Backend - in search

Search supports new features as below:

1. When a user starts a new indexing job on a folder, Search creates a new Kafka topic for the new job.
2. Search supports up to 99 nodes for better performance.
3. Improved the robustness of full indexing for a large number of files.
4. Improved the robustness of incremental job.

2. Option to disable metadata fetch in incremental

Search provides a new option to disable some fields of metadata fetch in incremental which is called `INGESTION_SMART_INCREMENTAL`. It will help the performance of incremental ingestion. Once it sets as true, these fields will be set as

```
OWNER = "N/A"
```

```
GROUP = "N/A"
```

```
UID = "N/A"
```

```
GID = "N/A"
```

```
MODE = "-1"
```


2.7. What's new in Release 2.5.11 for DR, Easy Auditor, Airgap, Ransomware Defender

Home Top

- [Eyeglass DR 2.5.11](#)
 - [New in this release:](#)
 - [Ease of Use](#)
- [Easy Auditor 2.5.11](#)
 - [Fixed in this release:](#)
- [Airgap 2.5.11](#)
 - [New in this release:](#)
- [Ransomware Defender 2.5.11](#)
 - [New in this release:](#)

What's new in the 2.5.11 Release

Eyeglass DR 2.5.11

New in this release:

Ease of Use

1. More than one access zone can now be selected from the UI when starting an access zone failover from the DR Assistant. This enables overall faster failovers that require more than one access zone to failover within a maintenance window. Each zone failover will have a dedicated failover job with a dedicated failover log and threads to execute the failovers at the same time.

Easy Auditor 2.5.11

Fixed in this release:

1. RWD is now detecting events if Bulk Ingest has an archive path setup to a non-default path. [EA-232](#)
2. The bulk ingest list displays all the files now. [EA-284](#)
3. The bulk ingestion GUI timeout was increased. [EA-285](#)
4. Kafka initializes properly during cluster up if the appliance has rebooted.

Airgap 2.5.11

New in this release:

1. Support for OneFS 9.5 was added.
2. Bug fixes and stability fixes were made.

Ransomware Defender 2.5.11

New in this release:

1. Zero Trust API now supports locking out ECS users by specifying local ECS user or IAM user for triggered lockouts.

© Superna Inc

2.8. What's new in Release 1.1.15 Golden Copy, CBDM, Archive Engine

[Home](#) [Top](#)

- [Golden Copy Release 1.1.15](#)
 - [New in this release:](#)
 - [Feature Enhancements](#)
 - [Fixed in this release:](#)
- [Cloud Browser for Data Mobility Release 1.1.15](#)
 - [New in this release:](#)
 - [Usability Enhancements](#)
 - [Fixed in this release:](#)
- [Golden Copy Archive Engine Release 1.1.15](#)
 - [New in this release:](#)
 - [Policy Based Archiving](#)
 - [Fixed in this release:](#)

What's New 1.1.15

Golden Copy Release 1.1.15

New in this release:

Feature Enhancements

1. Jobs History instant loading within the UI. It now uses an in-memory cache.
2. Recall statistics - Multipart stats now update as parts are downloaded on recall providing partial progress updates.

3. Backup statistics for Azure - Multipart stat update - upload for Azure Sdk is now supported.
4. Email notification settings are now part of the config export command to allow migrating configuration data to a new appliance or to restore settings.

Fixed in this release:

1. UI-Language change function is not working [GC-1525](#)

Cloud Browser for Data Mobility Release 1.1.15

New in this release:

Usability Enhancements

1. Cloud to Premise - Refresh SMB target list without logging off was added.
2. gcdm- prefix on share names to be case-in-sensitive is now allowed.
3. The jobs pages have an export button on the job, and User-driven job export in ZIP is supported now.

Fixed in this release:

1. Cloud to Premise - Jobs History - Skipped bytes added to Success bytes [CBDM-235](#)

Golden Copy Archive Engine Release 1.1.15

New in this release:

Policy Based Archiving

1. Enable/Disable policies - Archive policies can now have a new value, "paused", be set.
2. Recall Support for Policies - Policies on Smart Archiver folders can be enabled/disabled (paused or unpaused).
3. The export command for the job was added.
4. Policy configuration (CLI) was added.
5. Policy-based archiving - MVP is available now in BETA mode.

Fixed in this release:

1. The archive job cannot finish when there is no data in staging area [SA-60](#)
2. Error rerun pipeline recall job [SA-831](#)
3. importconfig fails to restore SA folder [SA-825](#)
4. The search bar in SA and Cloud Browser page fails when the "\" character is used instead of "/" [SA-658](#)
5. Users can access share with Deny all permission [SA-966](#)

2.9. What's new in Release 2.5.12 Easy Auditor, AIRGAP, Ransomware Defender, Eyeglass DR

[Home](#) [Top](#)

- [Easy Auditor 2.5.12](#)
 - [New in this release:](#)
 - [Enhancements](#)
 - [Active Auditor Event Triggers](#)
- [AIRGAP 2.0 2.5.12](#)
 - [New in this release:](#)
- [Ransomware Defender 2.5.12](#)
 - [New in this release:](#)
 - [Enhancements](#)
 - [Superna Defender Webhooks](#)
- [Eyeglass DR 2.5.12](#)
 - [New in this release:](#)
 - [Fixed in this release:](#)

What's new in the 2.5.12 Release

Easy Auditor 2.5.12

New in this release:

Enhancements

1. Auditing of NFS events can be selectively enabled or disabled.

Active Auditor Event Triggers

1. Failed Events to Eyeglass UI was added.
1. Failed audit event trigger support.

AIRGAP 2.0 2.5.12

New in this release:

1. Security guard on ECS can now write data to a non-management IP.

Ransomware Defender 2.5.12

New in this release:

Enhancements

1. Ransomware Defender on ECS can be configured together with the turboaudit REST API setting.

Superna Defender Webhooks

Supports:

1. Overview:
 - a. This new solution only exists with Ransomware Defender to integrate alerts with real-time webhooks with customization of the webhook data that allows SIEM and service automation to consume this alert data.

Security Operations teams can now get Defender alert data sent to 1 or more webhook endpoints.

2. Configuration of webhooks to different targets.
3. Filtering by the severity of Ransomware Event (Warning, Major, Critical).
4. Filtering by lifecycle phase.

Eyeglass DR 2.5.12

New in this release:

1. Oracle Java on the Eyeglass Appliance was replaced with OpenJDK.
2. End of support for RHEL 7 and OpenSUSE 15.2 based appliances.

Fixed in this release:

1. Access Zone Failover - Fails during Networking Operations (DR-770).

© Superna Inc

2.10. What's new in the 3.1.0 Release

[Home](#) [Top](#)

What's new in the 3.1.0 Release

Ransomware Defender for AWS 3.1.0

New in this release:

Monitoring

1. The outbound webhook for ZT events to notify 3rd party applications is now available.

Cyber Recovery Manager on AWS Defender

1. Cyber Recovery Manager lists the objects modified during a ransomware event and allows for easy recovery.
2. Objects selected for recovery are rolled back to the most recent version from before the rsw event or else removed if no such version exists.
3. All objects selected for recovery are moved to a quarantine directory for later retrieval and analysis.

Fixed in this release

1. UI hang issues plus unrelated error messages are shown randomly are now fixed [RWDAWS-236](#)
2. Cluster up doesn't get stuck at Initializing hbase schema step. [RWDAWS-241](#)
3. [Active Auditor]: Monitor only mode - generic TD's can be raised as a warning, major and critical [RWDAWS-179](#)
4. Data Start and end times on easy audit reports are sometimes inaccurate [RWDAWS-239](#)
5. [Ignored List]: able to generate TD events from paths added to the ignored list [RWDAWS-235](#)
6. Remove the 'Create/Delete Snapshot' option from the Actions menu for an active or archived event [RWDAWS-233](#)
7. Security Guard Log Viewer - Copy to Clipboard doesn't work [RWDAWS-231](#)
8. Uploading files to s3 buckets triggers TD15 [RWDAWS-98](#)
9. [Monitor Only Settings]: events from the path added to the monitor-only settings should be in monitor mode [RWDAWS-240](#)

2.11. What's new in Release 3.1.1 RWDAWS

Home [Top](#)

- [New in this release:](#)
 - [Multiple AWS Account Support](#)
- [Fixed in this release:](#)

What's new in the 3.1.1 Release

Ransomware Defender for AWS 3.1.1

New in this release:

Multiple AWS Account Support

1. Multiple AWS Account Support is available now so users with multiple AWS accounts are able to forward events to a single location.
2. Lockouts are now supported using a combination of Key, Role, or both. Role Based lockouts are new, and apply a policy at the user's role. They protect service accounts where access keys and secret keys are not being used.

Fixed in this release:

1. [Webhooks] : RSW event - remove MINOR option from event severity filter. [RWDAWS-377](#)
2. [Webhooks] : RSW event - do not send Security guard events. [RWDAWS-386](#)

3. [Cyber Recovery Manager] Bucket versioning enabled - file objects are not restored to the most recent version. [RWDAWS-482](#)
4. [Cyber Recovery Manager] : Ransomware event gets triggered when recovery job moves file to quarantine directory. [RWDAWS-419](#)
5. [Cyber Recovery Manager] : Bucket versioning status is not shown correctly on UI. [RWDAWS-416](#)
6. [Cyber Recovery Manager] Bucket versioning enabled - file objects are not restored to the most recent version RWDAWS-482
7. [Active Auditor] : Can not trigger CRTA policy events RWDAWS-354
8. Security Guard Log Viewer - Copy to Clipboard doesn't work RWDAWS-231
9. Add Managed Device UI - when select 'show protected buckets only' option, no data is shown RWDAWS-434
10. UI hang issues plus unrelated error messages are shown randomly RWDAWS-236
11. Able to trigger TD15 when bytes match percent tolerance is greater than default value RWDAWS-355
12. [Cyber Recovery Manager] : Missing S3 permissions for CloudFormation template RWDAWS-417

© Superna Inc

2.12. What's new in Release 1.1.16 Golden Copy, CBDM, Archive Engine

[Home Top](#)

- [What's New 1.1.16](#)
 - [Golden Copy Release 1.1.16](#)
 - [New in this release:](#)
 - [Usability Enhancements](#)
 - [Feature Enhancements](#)
 - [Fixed in this release:](#)
 - [Key Issues and Release Notes](#)
 - [Cloud Browser for Data Mobility Release 1.1.16](#)
 - [New in this release:](#)
 - [Content Creator Mode version:](#)
 - [Usability Enhancements](#)
 - [Fixed in this release:](#)
 - [Golden Copy Archive Engine Release 1.1.16](#)
 - [New in this release:](#)
 - [Recall via pipeline](#)
 - [Fixed in this release:](#)

What's New 1.1.16

Golden Copy Release 1.1.16

New in this release:

Usability Enhancements

1. The factory-reset command now also removes running jobs when the environment was clustered down.
2. The stats for the job type Rerun - Folders were added.

Feature Enhancements

1. It is available now to set the number of download threads to use separately from the amount used for upload.
2. Backup and restore of jobs history functionality were added.
3. AWS SDK was updated and transport manager 2.0 is included with BETA support, but not enabled by default.

Fixed in this release:

1. UI Editing archivedfolders after the first Edit does not close the Edit box - Changes applied. [GC-1697](#)
2. ReRun of Incremental Rename does not work because missing info on previous name. [GC-1748](#)
3. Pipeline Recall with `--trash-after-recall` does not delete original files. [GC-1905](#)
4. Auto ReRun - Add Stats for job `ReRun - Folders` and Stats Issues. [GC-1879](#)

Key Issues and Release Notes

1. [GC-2254](#) Upgrade from 1.1.12 or earlier - after upgrading, the running job is not continuing to run

Archive jobs that were in progress prior to the upgrade are not resumed after the upgrade is complete. Jobs must be restarted.

Cloud Browser for Data Mobility Release 1.1.16

New in this release:

Content Creator Mode version:

1. Support for recalling to quota-protected share added.

Usability Enhancements

1. To improve the usability, the jobs history affected files CSV download were added:

-three date columns;

-headers to explain table data.

Fixed in this release:

1. Jobs Errors does not display errors with a large number of jobs in the Jobs History. [GC-447](#)

Golden Copy Archive Engine Release 1.1.16

New in this release:

Recall via pipeline

1. Now able to recall data if upload bucket and recall bucket use different access credentials
2. Support for recalling to quota-protected share added.

Fixed in this release:

1. Isilon Management GUI incorrect display for licenses. [SA-875](#)
2. Not able to recall if the upload bucket and recall bucket use different access credentials. [SA-365](#)
3. The archive folder path is not cleared after archived is completed. [SA-946](#)
4. Users can access share with Deny all permission [SA-966](#)

© Superna Inc

2.13. What's new in Release 2.6.0 for DR, Easy Auditor, Airgap, Ransomware Defender

[Home](#) [Top](#)

- [Easy Auditor 2.6.0](#)
 - [New in this release:](#)
 - [Fixed in this release:](#)
- [Eyeglass DR 2.6.0](#)
 - [New in this release:](#)
 - [How to Configure Eyeglass to Connect to the SaaS Portal](#)
 - [What Happens Once the SaaS Portal is Enabled and the Application Registered?](#)
 - [Can the Data Forwarding be Stopped?](#)
 - [Subscription License Support](#)
 - [Fixed in this release:](#)

What's new in the 2.6.0 Release

Easy Auditor 2.6.0

New in this release:

1. Bulk Ingest file selector. Selecting each tree level from File Selector is available now.
2. The command for nfs events auditing from RSW was separated.

`igls rsw rswnfs set --enabled=true/false` Enables or disables RSW NFS events management in sca. The command becomes active when `igls rsw nfsevents set --enabled=true/monitor.`

`igls easyauditor eanfs set --enabled=true/false` Enables or disables EA NFS events management in sca. The command becomes active when `igls rsw nfsevents set --enabled=true/monitor`.

Fixed in this release:

1. 'Cannot retrieve report information from DB' error found during Query [EA-314](#)

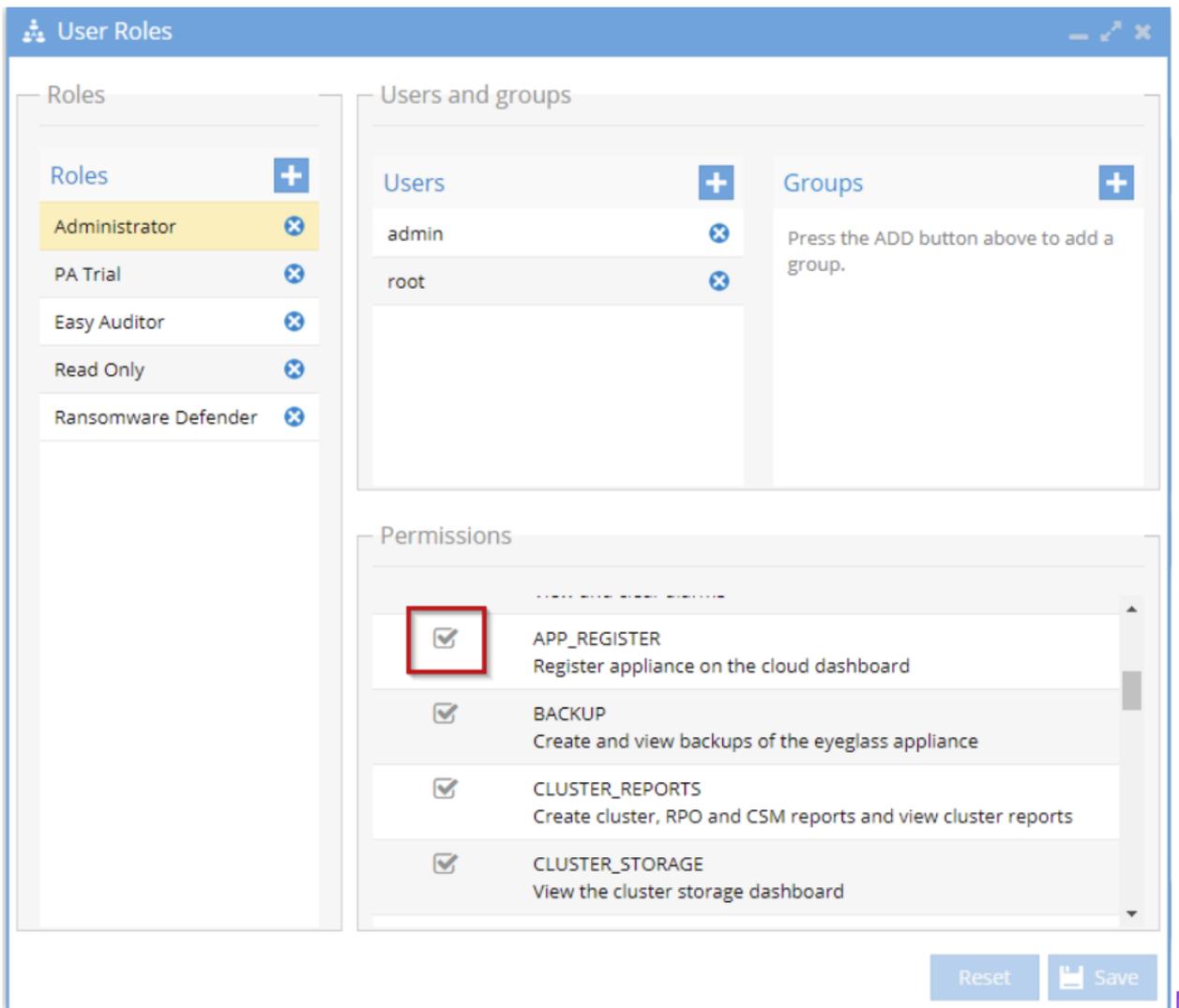
Eyeglass DR 2.6.0

New in this release:

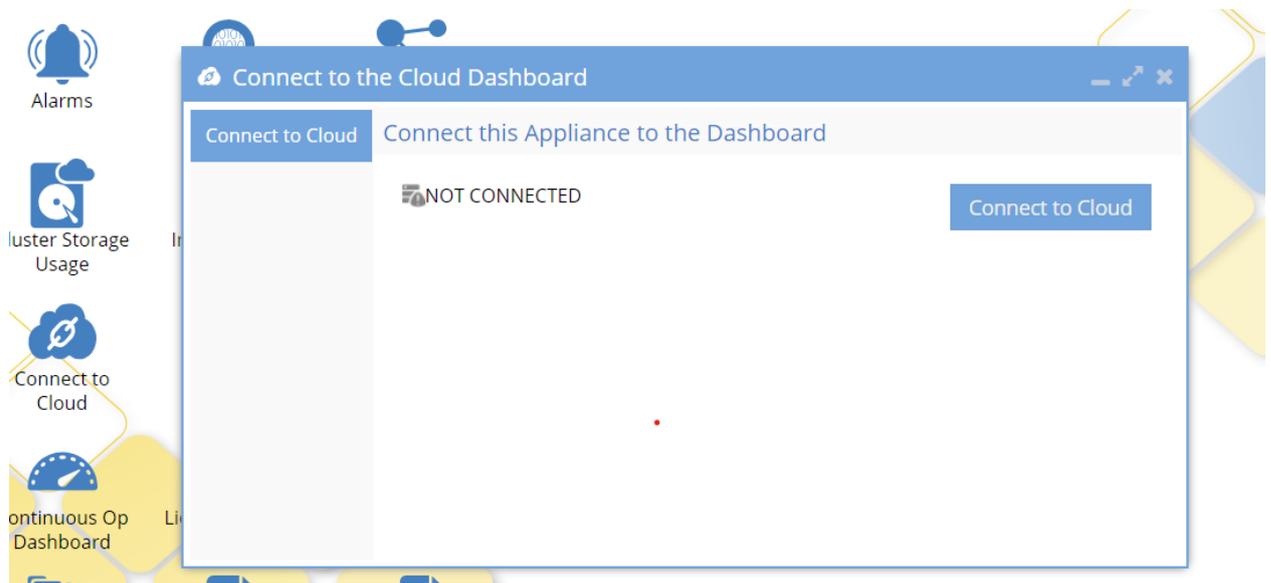
1. Support of the SaaS Portal

How to Configure Eyeglass to Connect to the SaaS Portal

- Upgrade to version 2.6.0.
- Enable the SaaS Portal:
 - SSH to the appliance
 - Execute the command `igls config settings set --tag=saas_portal_enabled -value=true`
- Connect to the Eyeglass appliance.
- Open the User Roles view and grant the `APP_REGISTER` permission to the administrator:



- Logout and login again for the new permission to take effect.
- Once logged in again, the icon Connect to Cloud is visible. Click on the icon; it will open the following dialogue:



- Click on the *Connect to Cloud* button.
- A new tab will open, and you will be prompted to login to the portal if you're not already logged in. Provide a description for your appliance, and click on Register.

The screenshot shows a dark-themed web interface for 'Appliance Registration'. At the top, the title 'Appliance Registration' is displayed in white. Below it, a unique ID is shown: 'Id: M7fuD/Al-S25.9.1v23059U25.9.1v23059-G25.9.1v23059CvD25.9.1v23059.Ip15.4-1682715905'. A 'Description' section contains a text input field with the value 'KylesEyeglass'. Below this is a 'Product list' section with three items, each with a blue icon and a brief description: 'User Behavior Auditing' (with a clipboard icon), 'Disaster Recovery' (with an eye icon), and 'Ransomware Defender' (with a shield icon). At the bottom, there is a blue button labeled 'Register' and a 'Log out' link with a back arrow icon.

Appliance Registration

Id: M7fuD/Al-S25.9.1v23059U25.9.1v23059-G25.9.1v23059CvD25.9.1v23059.Ip15.4-1682715905

Description

KylesEyeglass

Product list

- User Behavior Auditing**
Easy Auditor simplifies and lowers the cost of file access security reporting and introduces real-time audit features.
- Disaster Recovery**
Superna Eyeglass® enables a disaster recovery solution based on the cluster witness concept that is used in highly available disaster recovery solutions.
- Ransomware Defender**
Scalable real-time event processing solution.

If you agree with the above information, register the appliance.

Register

Log out

What Happens Once the SaaS Portal is Enabled and the Application Registered?

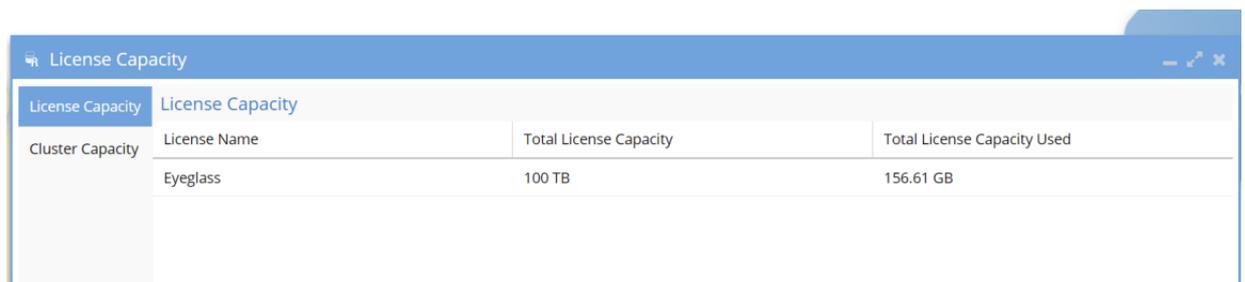
The Eyeglass appliance will forward all alarms issued by any of the licensed applications to the SaaS Portal. The appliance will also send metric data it collects to the portal on a 5 minute schedule.

Can the Data Forwarding be Stopped?

Yes, the flow of data from the Eyeglass appliance to the SaaS Portal may be stopped at any time. To do this, open the *Connect to Cloud* view, the label on the button will show *Pause* once the connection to the SaaS Portal was established. Click the button and the appliance will no longer forward alarms and metric data. If the process is to be restarted, that button may be clicked again to achieve this.

Subscription License Support

If subscription licenses were purchased and loaded to the Eyeglass appliance, it is now possible to monitor the actual and used capacity in a new dialog, the License Capacity view:



License Capacity			
License Capacity	License Capacity		
Cluster Capacity	License Name	Total License Capacity	Total License Capacity Used
	Eyeglass	100 TB	156.61 GB

The dialog has two tabs *License Capacity* and *Cluster Capacity*. The first tab, *License Capacity*, lists all applications for which subscription licenses are available, the granted capacity and the total used capacity. The second tab, *Cluster Capacity*, lists each registered managed device, its capacity and how much the cluster's capacity contributes to the used total capacity per licensed application - in the snapshot below there is just one application licensed with subscription licenses.

Cluster Capacity	Cluster Name	GUID	Cluster Capacity	Eyeglass
	isi-src	005056a4acc3fce508633125508ae...	78.31 GB	50 %
	isi-dr93-42	005056a4e715d029e163f81c8bb5...	78.31 GB	50 %

Fixed in this release:

1. igls app pull-config doesn't migrate failover logs. DR-779
2. Unwanted shadow trace is created when path picker is opened. DR-276
3. Access zone failover 'Block Failover on Warnings' does not block selecting zone in the warning. DR-753
4. igls app pull-config for file filters & monitor only setting. DR-780
5. Zone Readiness Errors when Provider Instance Name mismatched. DR-205

© Superna Inc

2.14. What's new in Release 1.1.17 for Golden Copy, CBDM, Archive engine

Home Top

- [Golden Copy Release 1.1.17](#)
 - Fixed in this release:
- [Cloud Browser for Data Mobility Release 1.1.17](#)
 - Fixed in this release:
- [Archive Engine Release 1.1.17](#)
 - Fixed in this release:

Golden Copy Release 1.1.17

Fixed in this release:

1. Upgrade from 1.1.9 - after upgrading, the running job is not continuing to run. [GC-2254](#)
2. Json and Html report of recall/pipeline recall job is not showing accurate result for skipped files. [GC-1774](#)
3. Can't add AD user to admin for GC, when username contains few special characters. [GC-1687](#)

Cloud Browser for Data Mobility Release 1.1.17

Fixed in this release:

1. CBDM - files are recalled on the wrong path instead of `ifs/fromcloud/CBDM` its recalling on `ifs/fromcloud/BDM` [CBDM-428](#)

Archive Engine Release 1.1.17

Fixed in this release:

1. Smart-archiver-sourcepaths parameter does not accept comma characters in path [SA-508](#)

© Superna Inc

2.15. What's new Platform 1.0.0

[Home](#) [Top](#)

What's new Platform 1.0.0

SupernaOne Platform

All products in one! Now our customers can manage their data in one place.

We're happy to introduce a new software-as-a-service (SaaS) offering that will allow multiple Superna Eyeglass instances to be managed from a single, unified dashboard. Introducing SupernaOne: your single-pane-of-glass for alert triage and summarization, including our new data protection & security summary view.

SupernaOne will simplify how you interact with your Superna products and is being offered at no additional cost to you.

© Superna Inc

2.16. What's new in Release 2.6.1 for DR, Easy Auditor, Airgap, Ransomware Defender

Home Top

- [Eyeglass DR 2.6.1](#)
 - [New in this release:](#)
 - [Failover Script Timeout Customizable](#)
 - [Fixed in this release:](#)

What's new in the 2.6.1 Release

Eyeglass DR 2.6.1

New in this release:

Failover Script Timeout Customizable

DR 2.6.1 allows to overwrite the default failover script timeout setting using the following command:

```
igls adv failoverscripttimeout set --seconds=<time-in-seconds>
```

To set the timeout to 400 seconds, the command would be like this:

```
igls adv failoverscripttimeout set --seconds=400
```

To retrieve the value currently been set, execute:

```
igls adv failoverscriptstimeout
```

Fixed in this release:

1. Getting Isilon Unsupported Error for 9.5.0.1 Isilon when Upgrade eyeglass from 2.5.9.1 to 2.6.0. [DR-955](#)

© Superna Inc

2.17. What's new in Release 1.1.19 for Golden Copy, CBDM, Archive Engine

Home Top

- [Golden Copy Release 1.1.19](#)
 - [New in this release:](#)
 - [Usability Enhancements](#)
 - [Feature Enhancements](#)
 - [Fixed in this release:](#)
- [Cloud Browser for Data Mobility Release 1.1.19](#)
 - [New in this release:](#)
 - [Feature Enhancements](#)
 - [Fixed in this release:](#)
- [Golden Copy Archive Engine Release 1.1.19](#)
 - [New in this release:](#)
 - [Fixed in this release:](#)

What's New 1.1.19

Golden Copy Release 1.1.19

New in this release:

Usability Enhancements

1. Backup notifications and configuration to back up data and settings are available now.

Feature Enhancements

1. The function `--follow` when running jobs was added to follow that job's progress within the same command.
2. The `ecactl` search notifications list is shown chronologically now.
3. Failed hardlink and softlink on rerun jobs are added to the rerun topic to re-download only failed fails on a job.
4. AW skip existing files using `ARCHIVE_WORKER_RECALL_SKIP_EXISTENT_FILES`.

Fixed in this release:

1. Archivedfolders checksum setting resets to Default (Off) after a VM restart. [GC-2404](#)
2. UI - Archivedfolders Tab - Edit not populating `Tier`, which seems to be a Requirement. [GC-2405](#)
3. Grafana - All Time Gauges - Negative % number. [GC-2399](#)
4. Pipeline-Recall Does not skip files with the skip existing export. [GC-1897](#)
5. Job Cancel - Job should not be a SUCCESS if cancelled at any step. [GC-2035](#)

Cloud Browser for Data Mobility Release 1.1.19

New in this release:

Feature Enhancements

1. Multipart copy between buckets for user bucket to staging buckets cross-region. Users can stage files from the source bucket to the staging bucket even if they are in different regions.

Fixed in this release:

1. Email - SMB share path uses an Incorrect folder separator for the selected sub-folders. [CBDM-528](#)
2. Email Needs Attention Causing Job Failure due to Unconfigured SMTP Server. [CBDM-532](#)
3. CBDM Browser - Buckets region being mislabeled if there are other regions. [CBDM-609](#)
4. Cloud to Premise - Submit SMB Target Button is obscured, probably when the path is too long. [CBDM-615](#)
5. Cloud Browser - Unable to browse buckets in regions other than the one specified in Credentials. [CBDM-614](#)
6. Skipping incremented from failing to move files to SMB due to the limit. [CBDM-591](#)

Golden Copy Archive Engine Release 1.1.19

New in this release:

1. Dry Run functionality was added.

Fixed in this release:

1. Plus sign-in path causes issues with the SA archive. [SA-389](#)
2. Staged For Recall inconsistent listing of folders. [SA-1208](#)

© Superna Inc

2.18. What's new in Release 2.6.2 Easy Auditor, Airgap, Ransomware Defender, Eyeglass DR

Home Top

- [Easy Auditor 2.6.2](#)
 - [Fixed in this release:](#)
- [Ransomware Defender 2.6.2](#)
 - [New in this release:](#)

What's new in the 2.6.2 Release

Easy Auditor 2.6.2

Fixed in this release:

1. Built-In scheduled report results are displayed in the Manual report section. [EA-172](#)

Ransomware Defender 2.6.2

New in this release:

We'd like to highlight a specific update. The command `ecactl cluster down` now operates in the background mode by default. If you prefer the previous behaviour, you can still achieve it by running the command with the `-serial` option.

© Superna Inc

2.19. What's new in Release 3.2.0 RWDAWS

[Home](#) [Top](#)

- [Ransomware Defender for AWS 3.2.0](#)
 - [New in this release:](#)
 - [FSx lockout](#)

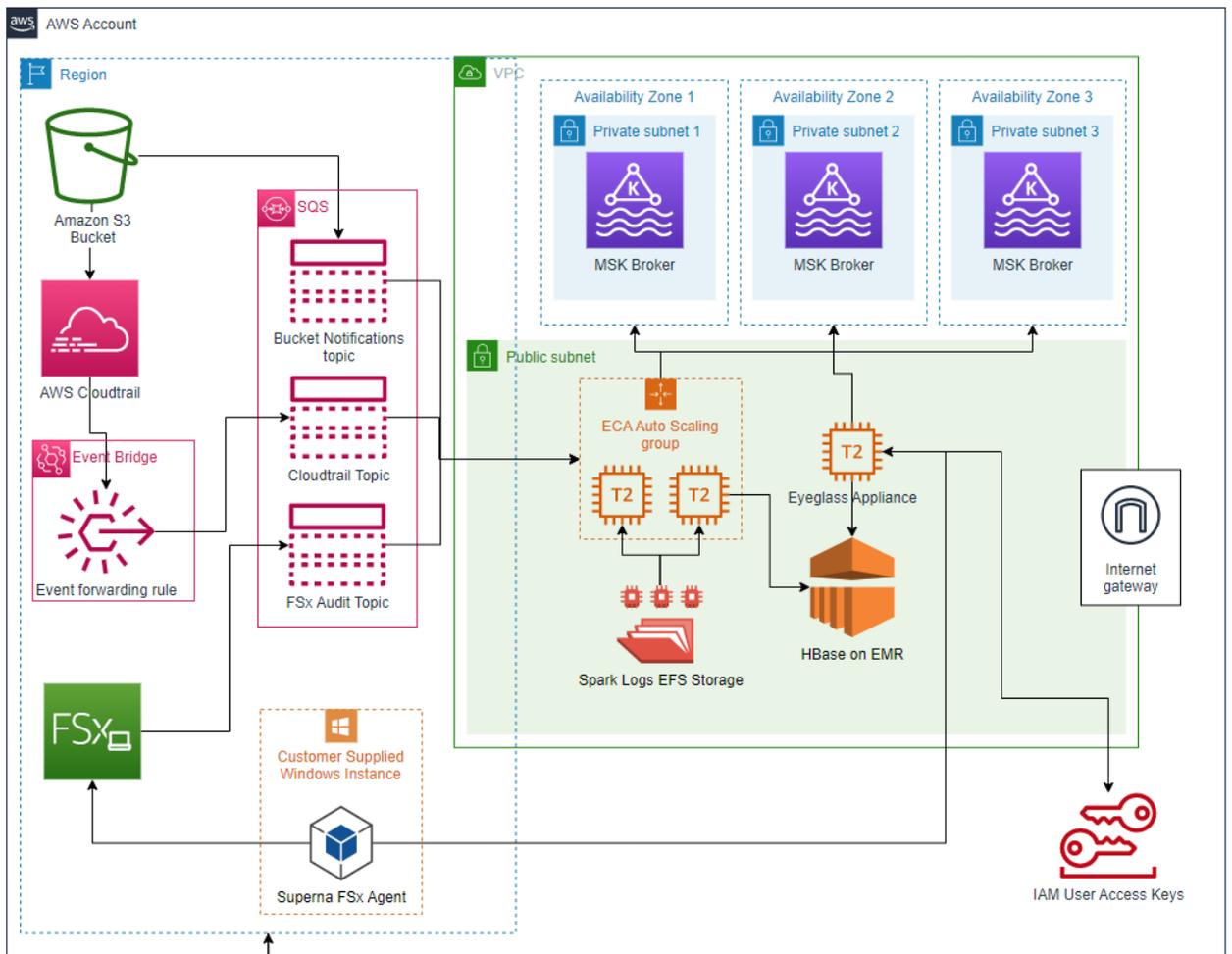
What's new in the 3.2.0 Release

Ransomware Defender for AWS 3.2.0

New in this release:

FSx lockout

The FSx agent is a Windows service that runs on a Windows EC2 instance. The customer provides this instance and **must be joined to the same Active Directory Domain** as the FSx server.



© Superna Inc

2.20. What's new in Release 1.1.20 Golden Copy, CBDM, Archive Engine

[Home](#) [Top](#)

- [Golden Copy Release 1.1.20](#)
 - [New in this release:](#)
 - [Fixed in this release:](#)
- [Cloud Browser for Data Mobility Release 1.1.20](#)
 - [New in this release:](#)
- [Golden Copy Archive Engine Release 1.1.20](#)
 - [New in this release:](#)
 - [Fixed in this release:](#)
 - [New configurations/environment variables in 1.1.20](#)

What's New 1.1.20

Golden Copy Release 1.1.20

New in this release:

Usability Enhancements

1. The Cancel Job button was added for active running jobs. The user can now easily cancel an active running job with the click of a button.
2. The job status **NEEDS ATTENTION** shows more status and reasons. Now, the job statuses will include three distinct states: "Success," "Failure," and the new "Needs Attention".
3. Disk space display script simplifies monitoring disk space usage on users' appliances. This script allows users to effortlessly check the disk space status of

their relevant volumes, enabling them to troubleshoot disk space errors more efficiently.

Feature Enhancements

1. Incremental logging was added. Incremental logging will display the total number of files found in the changelist in both the IG log and the searchctl job view.
2. Archiveworker Redis Cache - Redis caching was added to optimize the handling of finished work, ensuring a more efficient and responsive experience. AW restarts can cause us to re-work non-committed events.

Fixed in this release:

1. Job marked as a FAILURE due to Snapshot Extend step. [GC-2057](#)
2. Archivedfolder Checksum Value Reverting to Default(Off) After Upgrade. [GC-2614](#)
3. UI - Recall gauges - Skips counting against success %. [GC-2409](#)

Cloud Browser for Data Mobility Release 1.1.20

New in this release:

Feature Enhancements

Highlighted Folder Icons. The folder icon will be dynamically highlighted when the user selects folders or parent folders within the path selector tree.

Golden Copy Archive Engine Release 1.1.20

New in this release:

User Driven Archive and Recall notification email

1. The notification email addresses of users are gathered by capturing their email during the user's first login.
2. Email notifications containing details regarding the outcome of the GCAE upload and recall jobs were added.

Fixed in this release:

1. Unable to modify the recall schedule. [SA-1472](#)
2. CB only lists folders for 1 cluster. [SA-1202](#)

New configurations/environment variables in 1.1.20

docker-compose.yml

- [ERROR_RATE_THRESHOLD_PERCENTAGE](#)
 - Set in [eca-env-common](#) to override the default
 - added to allow setting the threshold at which the error rate becomes high in the jobs view. 10% is the default - meaning ≤ 10 is considered 'Low Error Rate' and < 10 is considered
- [ECA_ENABLE_PATH_CACHE_ARCHIVERWORKER](#)
 - Set in [eca-env-common](#) to override the default and to ENABLE
 - This allows caching finished work in archiveworker to avoid re-working uncommitted events in the case of an archiveworker restart

© Superna Inc

2.21. What's new in Release 2.6.3 Easy Auditor, Airgap, Ransomware Defender, Eyeglass DR

[Home](#) [Top](#)

- [Eyeglass DR 2.6.3](#)
 - [New in this release](#)
 - [Eyeglass UI Enhancements: Appliance ID Copy Button, Appliance OS Version Display](#)
 - [DR Test Mode: Writable Snapshots](#)
 - [Pool Failover: Multiple Pool Selection](#)
 - [Quota Failover: Quotas not Removed from the Source](#)
 - [SupernaOne Support: Filter on AirGap Alarms](#)
 - [Fixed in this release:](#)
 - [DR Assistant: Watch Button Inconsistency](#)
 - [RPO Report Viewer: Link to Eyeglass Documentation](#)
- [Ransomware Defender 2.6.3](#)
 - [Fixed in this release:](#)
 - [Webhooks: Missing Share List for Lockout Alarm](#)

What's new in the 2.6.3 Release

Eyeglass DR 2.6.3

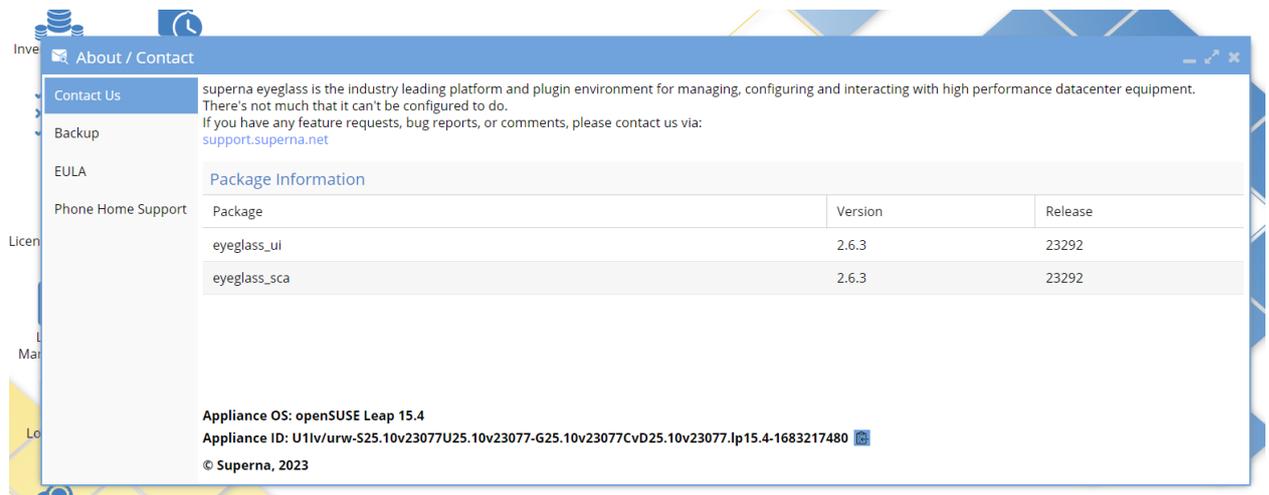
New in this release

Eyeglass UI Enhancements: Appliance ID Copy Button, Appliance OS Version Display

A copy button was added next to the appliance identification to simplify copying the appliance identification value from the About box. Pressing the button will copy the identifier to the clipboard.

The About box will also show the appliance OS and version.

The following picture shows both changes to the About box.



DR Test Mode: Writable Snapshots

Eyeglass 2.6.3 now supports many to 1 writable snapshots into a single zone. If a target directory already exists, UI will grey out the submit button and display the message **A writable snapshot already exists on this path.**

Pool Failover: Multiple Pool Selection

In previous Eyeglass versions, the DR Assistant showed no information when initiating IP pool failover for two IP pools, one with the `igls-ignore` and the other with the `igls-hint` flag being set. [\[DR-1068\]](#)

Quota Failover: Quotas not Removed from the Source

In previous Eyeglass versions, quotas failed over were not removed from the source cluster. This has been changed and represents the default case. Users may overwrite the behaviour by updating the flag `delete_quotas_from_source` in the system.xml file.

SupernaOne Support: Filter on AirGap Alarms

Eyeglass version 2.6.3 no longer lists AirGap alarms as DR alarms but groups them as their own group. This allows filtering on such alarms in either Eyeglass or SupernaOne.

Fixed in this release:

IP pool failover - Not able to select multiple pools. [DR-1068](#)

DR Assistant: Watch Button Inconsistency

In previous Eyeglass versions, the DR Assistant's watch process stopped working in case the logs view was reopened after the watch button was pressed and no update was added to the view.

RPO Report Viewer: Link to Eyeglass Documentation

In previous Eyeglass versions, the link to the Eyeglass documentation included in the RPO Report viewer did not work.

Ransomware Defender 2.6.3

Fixed in this release:

Webhooks: Missing Share List for Lockout Alarm

The previous versions did not list affected shares with the data available as defined with the webhook; this has been corrected. [\[RWD-524\]](#)

© Superna Inc

2.22. What's new in Release 2.6.4 Easy Auditor, Airgap, Ransomware Defender, Eyeglass DR

[Home](#) [Top](#)

What's new in the 2.6.4 Release

Eyeglass DR 2.6.4

New in this release

Non-ASCII Character Support in the Recovery Manager

The Recovery Manager restores files from a snapshot when files were affected by a Ransomware attack. It did not have support for non-ASCII characters in file names. This limitation has been removed.

© Superna Inc

2.23. What's new in Release 1.1.21 Golden Copy, CBDM, Archive Engine

[Home Top](#)

What's New 1.1.21

Golden Copy Release 1.1.21

New in this release:

Usability Enhancements

Job view output now displays:

- Folders accepted
- Folders succeeded
- Folders failed

Feature Enhancements

1. Job error log and archiveworker logging to include the S3 request ID's.
2. Google (GCS) was added for Admin and Non-Admin users.

Better user job monitoring with activefiles summary integrated to job view small and large files

Active copies of GUI are now showing for each node NODE or CLUSTER:

1. The total # of files being copied
2. Total small file count and the % of the total this represents
3. Total large file count and the % of the total this represents

4. Show the sum of all files in active copies for ALL nodes in TBs
5. Show a table with the following break-down:
 - a. files 1 byte - 100K
 - b. 100K - 1MB
 - c. 1MB - 5MB
 - d. 5MB - 100MB
 - e. 100MB - 1G
 - f. 1G - 100G
 - g. 500G - 1TB
 - h. Greater than 1TB

Job view changelist/layers enhancement

Job view now includes these changelist details for incremental:

- The layer being processed
- How many layers
- The layer size
- The # of files per layer
- Total amount of files in the changelist

Cloud Browser for Data Mobility Release 1.1.21

New in this release:

Feature Enhancements

After all files have been moved to SMB shares, the Email notification will be sent.

Concurrent Cloud Mover Jobs

1. Round-robin archived folders. Now, the user can manually create two or more archivedfolders (pipelines) that can be used for recall and have the user jobs select archivedfolders on a round-robin basis so that the user can support multiple concurrent download jobs (by the same user or different users) at the same time.
2. Nodes in the cluster can now be manually assigned/pinned to specific folders, allowing for the distribution of cluster resources to the folders.

Fixed in 1.1.21

1. Unable to find/see buckets in other regions other than `us-east-1`, which is specified in Credentials.([CBDM-714](#))

Golden Copy Archive Engine Release 1.1.21

New in this release:

Azure Deep Archive (Or Equivalent) Support

Restore from deep_archive skips now for existing files.

Dry run to calculate the amount of data to be archived before the job is run

The GUI enables users to initiate dry archive runs, giving them a preview of the potential impact of the archive job without actual execution.

After all files have been moved to SMB shares, the Email notification will be sent.

Fixed in this release:

1. Policy-based archiving appends an extra string to the Powerscale prefix inside the bucket. ([SA-1567](#))
2. Recall staging/restore from `DEEP_ARCHIVE` shows `0` stats, including with email. ([SA-1554](#))
3. Not able to recall from deep_archive when Redis is set. ([SA-1377](#))

© Superna Inc

3. End of Sale - End of Support - End of Life

[Home](#) [Top](#)

Superna Product Lifecycle Information

This page contains announcements of the end of support for all Superna products. After every major release, we support the legacy releases for a considerable period of time to help our customers upgrade or migrate. We recommend that our customers upgrade to the latest versions to get full benefits of our new features, feature enhancements, and critical bug fixes.

General Availability (GA)

General Availability (GA) is the release of a new product version to the general public. When a product version reaches GA, it becomes available through general sales and support channels.

End of Sale (EoS)

This is the date that a specific product version will no longer be available for purchase. This is generally the date that the next major version becomes GA. End of Sale (EoS) versions are fully supported in the form of maintenance builds, however, to gain new functionality beyond defect fixes, customers must upgrade to the latest GA release.

End of Maintenance (EoM)

The End of Maintenance (EoM) milestone marks the start of the product version retirement period. A product version reaches its EoM date 18 months after the EoS date. From this milestone, the product version is no longer maintained by maintenance builds. Superna will continue to offer help desk support, however, in order to address problems encountered with a product version in EoM, the customer must upgrade to the latest GA version, if an existing maintenance build or workaround is not available.

End of Life (EoL)

The End of Life (EoL) milestone marks the date after the technical support for that product version will no longer be available. Customers may continue to use the product version once EoL is announced, however, customer problems reported will not be fixed or worked on by Technical Support. Customers are encouraged to upgrade to the GA version as soon as possible.

© Superna Inc

4. Release Roadmap Login

Superna Product Release Roadmap Login

This page requires registration and login to view the release roadmap.

The usage of this information is covered on Read Me first after login.

Enter a business email address and password.

Loading...

4.1. Product Release RoadMap

- [Overview](#)
- [READ ME First - How to use this information](#)
- [Cloud Native Software](#)
 - [Defender for AWS](#)
 - [Potential Next Release](#)
- [On premise Software](#)
 - [DR Manager for PowerScale](#)
 - [Potential Next Release](#)
 - [Zero Trust API](#)
 - [Ransomware Defender](#)
 - [Potential Next Release](#)
 - [Enterprise Airgap](#)
 - [Potential Next Release](#)
 - [Easy Auditor](#)
 - [Potential Next Release](#)
 - [Golden Copy](#)
 - [Potential Next Release](#)
 - [Golden Copy Cloud Browser for Data Mobility](#)
 - [Golden Copy Archive Engine](#)
 - [Potential Next Release](#)
 - [Search & Recover](#)
 - [Potential Next Release](#)
 - [Performance Auditor](#)

Overview

The software releases and features listed below are subject to change at any time. Superna offers no guarantee regarding any specific feature or timeline on a specific release. This is provided "is is" without any warranty of any kind.

READ ME First - How to use this information

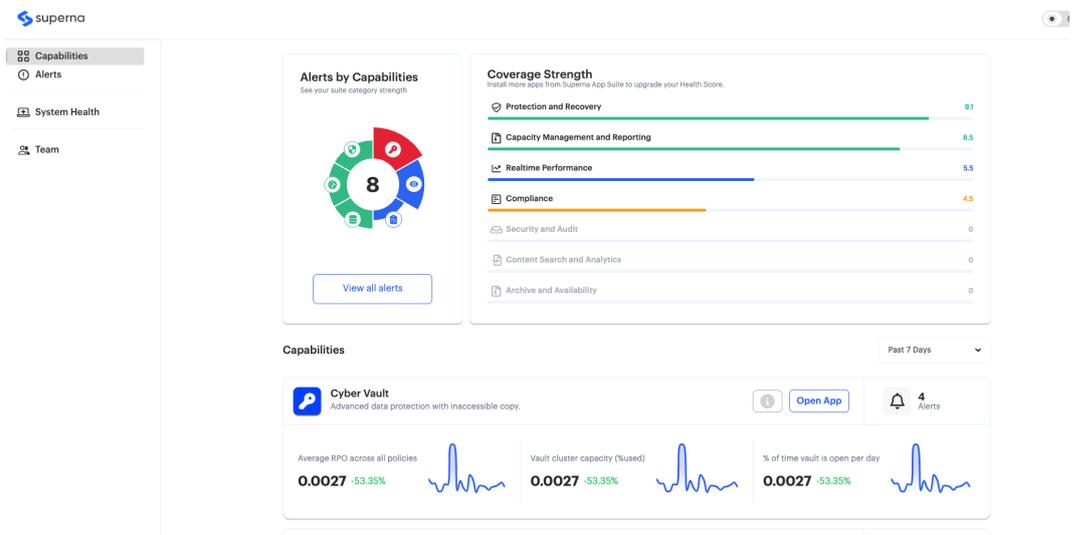
1. All release information is subject to change in Superna's sole discretion. A feature on this page is not guaranteed to be delivered. No timeline is available on any given feature.
2. Information on this page is confidential and should not be re-shared or published
3. This information is for paid licensed customers to gain a view of upcoming features they can leverage.
4. This information also allows customers to request follow up on product offerings and capabilities listed on this page to help with mapping business requirements to our feature roadmap.

Cloud Native Software

Defender for AWS

Potential Next Release

1. FSx for Windows user lockout support with AD integration
2. Cyber Recovery Manager for Object data recovery using object versions **3.1.0 Release**
 - a. Phase II - leverage AWS backup service to restore data automatically from and active event
3. SaaS Portal integration
 - a. SaaS portal is new dashboard to see your cloud and on premise Superna products in a concise simple to dashboard that summarizes your current data protection status.



b.

On premise Software

DR Manager for PowerScale

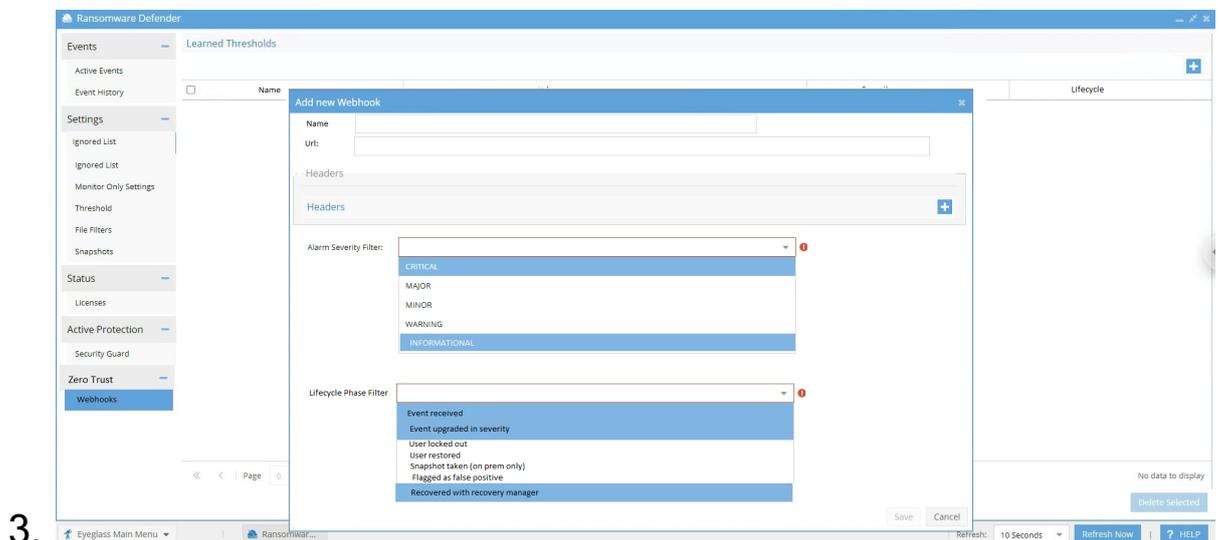
Potential Next Release

1. Application Driven Autonomous Failover (“ADAF”)
 - a. Application Driven Autonomous Failover (“ADAF”) is a combined software and API driven solution that enables host-to-storage based fault monitoring then automatically alerts, initiates and monitors automated PowerScale storage failovers through a combination of technologies listed in the Solution Components section.
2. Concurrent Access Zone failover allows selecting one or more zones to be failed over in parallel without needing to re-open DR Assistant
3. 2FA authentication via email integration within the GUI and CLI
4. Line numbers on failover logs
5. Read only role for all products within Eyeglass
6. New quota failover solution based on OneFS 9.3 or later import and export configuration. It will offer faster failover of quotas.
7. Containerized Eyeglass services to align with ECA architecture. Future integration to run Eyeglass as a container within the ECA cluster itself to offer HA of Eyeglass within the ECA cluster itself.

Zero Trust API

Potential Next Release

1. Webhook support for Ransomware Defender, Easy Auditor alerts. **2.5.12 Release**
2. Dedicated configuration of forwarding and sending real time webhook alerts to 1 or more target URL's for SIEM integration



Ransomware Defender

Potential Next Release

1. Simplifying settings tab with defaults only and hiding settings used only for advanced configurations
2. Export Event History to CSV files for external review of detections
3. Mass Delete Detector from Easy Auditor ported to Defender for ECS. Detects mass delete of objects.
4. SaaS Portal integration with ability to control email alerting rules by product and by alarm within the SaaS portal

5. Cyber Recovery Manager for Object data recovery
6. Defender for Object with split data and management deployment to allow security guard to specify specific ip address for data access

Enterprise Airgap

Potential Next Release

1. Airgap for object with support for CAS to CAS replication plugin
2. Airgap for object with Vault Agent ethernet interface control to enable interface down up controls to open and close the vault.
3. Enterprise Airgap for Powerscale with random airgap start time within a replication window. The random start time is per job and a window of time example 4 hours is specified. The job will start somewhere within the 4 hour window.

Easy Auditor

Potential Next Release

1. Active Auditor triggers will enable failed event types to allow creating triggers when user actions failed to complete due to ACL's blocking the action. Example would be data deletion actions (files or folders) can generate failed audit event that can be used as a trigger for real time notifications. **2.5.12 Release**
2. Easy Auditor query builder to add email list to email the report to a list of emails. These emails do not need to be added to notification center and allows on demand or scheduled reports to be emailed to select users or group emails.
3. Multi-tenant Easy Auditor
 - a. Access Zone level auditing can be delegated to AD users with the zone role assigned and a list of access zones mapped to the role.
 - b. The data browsing UI limits the user to see data under authorized access zones

- c. The user must have at least 1 SMB share with read permissions within each zone before they will be allowed to audit any data within the zone. This is determined by AD group membership on SMB shares.
- d. Triggers are not available to zone administrators due to the possibility of mis configuration causing many alerts. This functionality is blocked.

Golden Copy

Potential Next Release

1. Point in time Restore
 - a. GUI option to leverage version based recall. This allows a simply GUI to select a path of data from the backup and select a data from a calendar interface and Golden Copy will automatically locate object versions that match the requested point in time.
 - b. Simplified controls require only entering a date. Advanced option to select day and time are also available.
 - c. Point and click point in time restore
2. Auto retry job support for recall
 - a. If data fails to restore for any reason it will be tracked and a new job at the end of the current recall job will spawn and retry only the failed files. This is already supported and enabled for backup jobs to retry failed files only.
3. Auto retry tree walk jobs
 - a. During the tree walk phase to locate files to backup, API errors , network issues can cause part of a tree walk to fail. Golden copy tracks all these failed folders and will now automatically spawn a retry of the treewalk of the failed folders
4. Metadata file indexing and Searching
 - a. Indexing of all data copied, processed by Golden Copy to allow searching for the location of data the versions of data based on file name, date

stamps, metadata , including advanced metadata content aware extraction feature that exposes file metadata in the object properties.

- i. Example locate all image data with a resolution of 3000x4000 pixels

Golden Copy Cloud Browser for Data Mobility

1. End user power tools to allow Browsing a cloud S3 data repository and copy or move data to on premise storage on any SMB share the logged in user has access.
2. Email notification of data job completion
3. Pick any folder under any SMB share cluster wide to move/copy your cloud data
4. Enables Movielabs 2030 in 2023 and simplifies content editing workflows.

Golden Copy Archive Engine

Potential Next Release

1. Policy based workflows that allows criteria based treewalk and archive (move data) **1.1.15 Release**
 - a. Support for AWS Deep Archive transparency which allows data to be "tagged" for the AWS Deep Archive storage class without needing life cycle policies in AWS.
 - b. Transparent recall allows Archive Engine to handle the AWS Deep Archive API recall step and then monitor the recall jobs in AWS before restoring data on premise and email the logged in user about the data's availability
 - c. Initial release on CLI configuration support and last modified data stamp criteria using months or years to target data for recall.
2. HTML stubs with portal login will be added in a future release to show users data has been removed from the current folder

Search & Recover

Potential Next Release

1. Simplified Search product launch
 - a. Single VM vertical scaled to enable reporting, chargeback.
 - b. Targeted as administrator only tool for data reporting based on quick reports
 - c. No support for content indexing, data classification, snapshot indexing, user login and searching.
2. Brings job view, pause resume, cancel , active work on hand GUI and CLI
3. GUI Searching, API searching will support multibyte languages
4. 2 Byte language searching with CSV download

Performance Auditor