

Table of Contents

1. Software Releases.....	2
1.1. Current Release - Release Notes DR Edition.....	30
1.2. Current Release - Release Notes Ransomware Defender.....	147
1.3. Current Release - Release Notes Easy Auditor.....	182
1.4. Current Release - Release Notes Search and Recover.....	209
1.5. Current Release - Release Notes Performance Auditor.....	241
1.6. Current Release - Release Notes ECA.....	248
1.7. Current Release - Release Notes Golden Copy.....	255
1.8. Current Release - Release Notes Ransomware Defender AirGap 2.0.....	280
1.9. Current Release - Release Notes AnyCopy.....	302
1.10. Release 2.5.8 - Release Notes Ransomware Defender for ECS.....	312
1.11. Release 1.1.2 - Search and Recover.....	317
1.12. Release 1.1.4 - Golden Copy.....	341
1.13. Release 2.5.6 - Release Notes DR Edition.....	372
1.14. Release 2.5.6 - Release Notes Easy Auditor.....	490
1.15. Release 2.5.6 - Release Notes Ransomware Defender.....	518
1.16. Release 2.5.6 - Release Notes Performance Auditor.....	545
1.17. Release 2.5.6 - Release Notes ECA.....	550

1. Software Releases

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

- [Eyeglass Search & Recover 1.1.5-21169](#)
- [Eyeglass Golden Copy 1.1.6-21164](#)
- [Eyeglass Search & Recover 1.1.5-21163-Controlled Availability](#)
- [Eyeglass DR Edition and Data Protection Suite 2.5.8-21222 - Controlled Availability](#)
- [Eyeglass Golden Copy 1.1.6-21152](#)
- [Eyeglass Golden Copy 1.1.4-21124](#)
- [Eyeglass Search & Recover 1.1.5-21133-Controlled Availability](#)
- [Eyeglass Golden Copy 1.1.4-21119](#)
- [Eyeglass Ransomware Defender for ECS 2.5.8-21189](#)
- [Eyeglass DR Edition and Data Protection Suite 2.5.7.1-21161](#)
- [Eyeglass Golden Copy 1.1.4-21108](#)
- [Eyeglass DR Edition and Data Protection Suite 2.5.7.1-21140](#)
- [Eyeglass Performance Auditor 2.5.7.1-21140](#)
- [Eyeglass Golden Copy 1.1.4-21107](#)
- [Eyeglass Golden Copy 1.1.4-21105](#)
- [Eyeglass Golden Copy 1.1.4-21093](#)
- [Eyeglass DR Edition and Data Protection Suite 2.5.7-21096](#)
- [Eyeglass Performance Auditor 2.5.7-21096](#)
- [Eyeglass AnyCopy 2.5.7-21096](#)
- [Eyeglass Golden Copy 1.1.4-21074](#)
- [Eyeglass DR Edition and Data Protection Suite 2.5.7-21081](#)

- Eyeglass Performance Auditor 2.5.7-21081
- Eyeglass AnyCopy 2.5.7-21081
- Eyeglass Golden Copy 1.1.4-21062
- Eyeglass DR Edition and Data Protection Suite 2.5.7-21068
- Eyeglass Performance Auditor 2.5.7-21068
- Eyeglass AnyCopy 2.5.7-21068
- Eyeglass AnyCopy 2.5.7-20289
- Eyeglass Golden Copy 1.1.4-21002
- Eyeglass DR Edition and Data Protection Suite 2.5.6-20263
- Eyeglass Performance Auditor 2.5.6-20263
- Eyeglass DR Edition and Data Protection Suite 2.5.6-20258
- Eyeglass Golden Copy 1.1.4-20229
- Eyeglass Golden Copy 1.1.4-20178
- Eyeglass DR Edition and Data Protection Suite 2.5.6-20158
- Eyeglass Golden Copy 1.1.4-20133
- Eyeglass Golden Copy 1.1.4-20121
- Eyeglass DR Edition and Data Protection Suite 2.5.6-20084
- Eyeglass Performance Auditor 2.5.6-20084
- Eyeglass Golden Copy 1.1.3-20077
- Eyeglass DR Edition and Data Protection Suite 2.5.6-20069
- Eyeglass Performance Auditor 2.5.6-20069
- Eyeglass Golden Copy 1.1.3-20071
- Eyeglass DR Edition and Data Protection Suite 2.5.6-20063

- Eyeglass Performance Auditor 2.5.6-20063
- Eyeglass Golden Copy 1.1.3-20070
- Eyeglass DR Edition and Data Protection Suite 2.5.6-20056
- Eyeglass Performance Auditor 2.5.6-20056
- Eyeglass Search & Recover 1.1.2-20024
- Eyeglass DR Edition and Data Protection Suite 2.5.5-20019
- Eyeglass Performance Auditor 2.5.6-20022
- Eyeglass Search & Recover 1.1.2-19108
- Eyeglass Search & Recover 1.1.2-19105
- Eyeglass Search & Recover 1.1.2-19104
- Eyeglass DR Edition and Data Protection Suite 2.5.5-19234
- Eyeglass DR Edition and Data Protection Suite 2.5.5-19226
- Eyeglass DR Edition and Data Protection Suite 2.5.5-19219
- Eyeglass DR Edition and Data Protection Suite 2.5.5-19188
- Eyeglass DR Edition and Data Protection Suite 2.5.5-19184
- Eyeglass Search & Recover 1.1-19042
- Eyeglass DR Edition 2.5.4-19106
- Eyeglass Search & Recover 1.0-19033
- Eyeglass Search & Recover 1.0-19022
- Eyeglass Search & Recover 1.0-19018
- Eyeglass DR Edition & Data Protection Suite - 2.5.4-19020
- Eyeglass Search & Recover - 1.0
- DR Edition & Ransomware Defender Patch - 2.5.4-18275

- Eyeglass DR Edition - Cluster Storage Monitor Only 2.5.4-18266
- Eyeglass Ransomware Defender Only 2.5.3-18257
- Eyeglass Unified Release (DR, Easy Auditor, Ransomware Defender) 2.5.3
- Eyeglass Unified Release (DR, Easy Auditor, Ransomware Defender) 2.5.2
- Eyeglass Unified Release (DR, Easy Auditor, Ransomware Defender) 2.5.1
- Eyeglass Easy Auditor Only Release 2.5.0
- 2.0.0 DR Edition Only EOL Notice Nov 17, 2018
- 1.9.6 Ransomware Defender Only EOL Notice March 6, 2018
- 1.9.5 DR Edition EOL Notice March 6, 2018
- 1.9.4 Ransomware Defender EOL Notice March 6, 2018
- 1.9.4 DR Edition EOL Notice March 6, 2018
- 1.9.3 Ransomware Defender EOL Notice March 6, 2018
- 1.9.3 DR Edition EOL Notice March 6, 2018
- 1.9.2 Ransomware Defender EOL Notice March 6, 2018
- 1.9.2 DR Edition EOL Notice March 6, 2018
- 1.9.1 Ransomware Defender EOL Notice March 6, 2018
- 1.9.0 DR Edition EOL Notice March 6, 2018
- 1.9.0 Ransomware Defender - EOL Notice March 6, 2018
- 1.8.3 Notice July 31st 2017
- 1.8.1 Notice July 31st 2017
- 1.8.0 Notice July 31st 2017

- 1.7.0 EOL Notice July 31st 2017
- 1.6.3 EOL Notice May 31st 2017
- 1.6.2 EOL Notice May 31st 2017
- 1.6.1 EOL Notice May 31st 2017
- 1.6.0 EOL Notice May 31st 2017
- 1.5.4 EOL Notice Nov 1st

Eyeglass PowerScale Edition Releases

Release	Support With Drawn Date (EOS)	Version	Software downloads OVF, OVA and upgrades	Release Notes	Dell EMC Known Defects that Affect Eyeglasses Operations
Eyeglass Search & Recover 1.1.5-21169		1.1.5-21169		Current Release - Release Notes Search & Recover	

<p>Eyeglass Golden Copy 1.1.6-21164</p>		<p>1.1.6-21164</p>		<p>Current Release - Release Notes Golden Copy</p>	
<p>Eyeglass Search & Recover 1.1.5- 21163- Controlled Availability</p>		<p>1.1.5-21163</p>		<p>Current Release - Release Notes Search & Recover</p>	
<p>Eyeglass DR Edition and Data Protection Suite 2.5.8- 21222 - Controlled Availability</p>		<p>2.5.8-21222</p>		<p>Current Release - Release Notes Ransomware Defender AirGap 2.0</p>	
<p>Eyeglass Golden Copy 1.1.6-21152</p>		<p>1.1.6-21152</p>		<p>Current Release - Release Notes Golden Copy</p>	
<p>Eyeglass</p>		<p>1.1.4-21124</p>		<p>Current Release - Release</p>	

Golden Copy 1.1.4-21124				Notes Golden Copy	
Eyeglass Search & Recover 1.1.5- 21133- Controlled Availability		1.1.5-21133		Current Release - Release Notes Search & Recover	
Eyeglass Golden Copy 1.1.4-21119		1.1.4-21119		Current Release - Release Notes Golden Copy	
Eyeglass Ransomware Defender for ECS 2.5.8- 21189				Release 2.5.8 Release Notes for Ransomware Defender for ECS	
Eyeglass DR Edition and Data Protection Suite 2.5.7.1-				Current Release - Release Notes DR Edition Current Release - Release Notes Ransomware Defender	

21161				Current Release - Release Notes Easy Auditor Current Release - Release Notes ECA	
Eyeglass Golden Copy 1.1.4-21108		1.1.4-21108		Current Release - Release Notes Golden Copy	
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	
Eyeglass Performance Auditor 2.5.7.1-21140		2.5.7.1-21140		Current Release - Release Notes Performance Auditor	

Eyeglass Golden Copy 1.1.4-21107		1.1.4-21107		Current Release - Release Notes Golden Copy	
Eyeglass Golden Copy 1.1.4-21105		1.1.4-21105		Current Release - Release Notes Golden Copy	
Eyeglass Golden Copy 1.1.4-21093		1.1.4-21093		Current Release - Release Notes Golden Copy	
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 Release - Release Notes ECA	
Eyeglass Performance		2.5.7-21096		Current Release - Release Notes Performance Auditor	

Auditor 2.5.7-21096					
Eyeglass AnyCopy 2.5.7-21096		2.5.7-21096		Current Release - Release Notes AnyCopy	
Eyeglass Golden Copy 1.1.4-21074		1.1.4-21074		Current Release - Release Notes Golden Copy	
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 Notes Easy Auditor Current Release - Release Notes ECA	
Eyeglass Performance Auditor 2.5.7-		2.5.7-21081		Current Release - Release Notes Performance Auditor	

21081					
Eyeglass AnyCopy 2.5.7 -21081		2.5.7-21081		Current Release - Release Notes AnyCopy	
Eyeglass Golden Copy 1.1.4-21062	end of support	1.1.4-21062		Current Release - Release Notes Golden Copy	
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 Defender Current Release - Release Notes Easy Auditor Current Release - Release Notes ECA	
Eyeglass Performance Auditor 2.5.7- 21068		2.5.7-21068		Current Release - Release Notes Performance Auditor	

Eyeglass AnyCopy 2.5.7 -21068		2.5.7-21068		Current Release - Release Notes AnyCopy	
Eyeglass AnyCopy 2.5.7 -20289		2.5.7-20289		Current Release - Release Notes AnyCopy	
Eyeglass Golden Copy 1.1.4-21002	end of support	1.1.4-21002		Current Release - Release Notes Golden Copy	
Eyeglass DR Edition and Data Protection Suite 2.5.6- 20263	Dec 2, 2021	2.5.6-20263		Current Release - Release Notes DR Edition Current Release - Release Notes Ransomware Defender Current Release - Release Notes Easy Auditor Current Release - Release Notes ECA	
Eyeglass Performance	Dec 2, 2021	2.5.6-20263		Current Release - Release Notes Performance Auditor	

Auditor 2.5.6-20263					
Eyeglass DR Edition and Data Protection Suite 2.5.6-20258	Dec 2, 2021	2.5.6-20258		Current Release - Release Notes DR Edition Current Release - Release Notes Ransomware Defender Current Release - Release Notes Easy Auditor Current Release - Release Notes ECA	
Eyeglass Golden Copy 1.1.4-20229	end of support	1.1.4-20229		Current Release - Release Notes Golden Copy	
Eyeglass Golden Copy 1.1.4-20178	end of support	1.1.4-20178		Current Release - Release Notes Golden Copy	
Eyeglass DR Edition and Data Protection	Dec 2, 2021	2.5.6-20158		Current Release - Release Notes DR Edition Current Release - Release	

Suite 2.5.6-20158				Notes Ransomware Defender Current Release - Release Notes Easy Auditor Current Release - Release Notes ECA	
Eyeglass Golden Copy 1.1.4-20133	end of support	1.1.4-20133		Current Release - Release Notes Golden Copy	
Eyeglass Golden Copy 1.1.4-20121	end of support	1.1.4-20121		Current Release - Release Notes Golden Copy	
Eyeglass DR Edition and Data Protection Suite 2.5.6-20084	Dec 2, 2021	2.5.6-20084		Current Release - Release Notes DR Edition Current Release - Release Notes Ransomware Defender Current Release - Release Notes Easy Auditor Current Release - Release	

				Notes ECA	
Eyeglass Performance Auditor 2.5.6-20084	Dec 2, 2021	2.5.6-20084		Current Release - Release Notes Performance Auditor	
Eyeglass Golden Copy 1.1.3-20077	end of support	1.1.3-20077	General Availability	Current Release - Release Notes Golden Copy	
Eyeglass DR Edition and Data Protection Suite 2.5.6-20069	Dec 2, 2021	2.5.6-20069	General Availability	Current Release - Release Notes DR Edition Current Release - Release Notes Ransomware Defender Current Release - Release Notes Easy Auditor Current Release - Release Notes ECA	
Eyeglass Performance Auditor 2.5.6-	Dec 2, 2021	2.5.6-20069	General Availability	Current Release - Release Notes Performance Auditor	

20069					
Eyeglass Golden Copy 1.1.3-20071	end of support	1.1.3-20071	General Availability	Current Release - Release Notes Golden Copy	
Eyeglass DR Edition and Data Protection Suite 2.5.6-20063	Dec 2, 2021	2.5.6-20063	General Availability	Current Release - Release Notes DR Edition Current Release - Release Notes Ransomware Defender <div style="border: 1px solid black; padding: 2px;"> Current Release - Release Notes Easy Auditor </div> Current Release - Release Notes ECA	
Eyeglass Performance Auditor 2.5.6-20063	Dec 2, 2021	2.5.6-20063	General Availability	Current Release - Release Notes Performance Auditor	
Eyeglass Golden Copy 1.1.3-20070	end of support	1.1.3-20070	General Availability	Current Release - Release Notes Golden Copy	

Eyeglass DR Edition and Data Protection Suite 2.5.6-20056	Dec 2, 2021	2.5.6-20056	General Availability	Current Release - Release Note Edition Current Release Release Note Ransomware Defender Current Release - Release Notes Easy Auditor Current Release Release Note ECA	
Eyeglass Performance Auditor 2.5.6-20056	Dec 2, 2021	2.5.6-20056	General Availability	Current Release - Release Notes Performance Auditor	
Eyeglass Search & Recover 1.1.2-20024		1.1.2-20024	General Availability	Current Release - Release Notes Search & Recover	
Eyeglass Search & Recover 1.1.2-20012	end of support	1.1.2-20012	General Availability	Current Release - Release Notes Search & Recover	
Eyeglass DR	Oct 1, 2020	2.5.5-20019	General Availability	Current Release - Release	

Edition and Data Protection Suite 2.5.5-20019				Notes DR Edition Current Release - Release Notes Ransomware Defender	
				Current Release - Release Notes Easy Auditor	
				Current Release - Release Notes ECA	
Eyeglass Performance Auditor 2.5.6-20022	Dec 2, 2021	2.5.6-20022	General Availability	Current Release - Release Notes Performance Auditor	
Eyeglass Search & Recover 1.1.2-19108	end of support	1.1.2-19108	General Availability	Current Release - Release Notes Search & Recover	
Eyeglass Search & Recover 1.1.2-19105	end of support	1.1.2-19105	General Availability	Current Release - Release Notes Search & Recover	
Eyeglass	end of support	1.1.2-19104	General Availability	Current Release - Release Notes Search	

Search & Recover 1.1.2-19104				& Recover	
Eyeglass DR Edition and Data Protection Suite 2.5.5-19234	Oct 1, 2020	2.5.5-19234	General Availability	Current Release - Release Notes DR Edition	
				Current Release - Release Notes Ransomware Defender	
				Current Release - Release Notes Easy Auditor	
				Current Release - Release Notes ECA	
Eyeglass DR Edition and Data Protection Suite 2.5.5-19226	Oct 1, 2020	2.5.5-19226	General Availability	Current Release - Release Notes DR Edition	
				Current Release - Release Notes Ransomware Defender	
				Current Release - Release Notes Easy Auditor	
				Current Release - Release	

				Notes ECA	
Eyeglass DR Edition and Data Protection Suite 2.5.5-19219	Oct 1, 2020	2.5.5-19219	General Availability	Current Release - Release Notes DR Edition Current Release - Release Notes Ransomware Defender Current Release - Release Notes Easy Auditor Current Release - Release Notes ECA	
Eyeglass DR Edition and Data Protection Suite 2.5.5-19188	Oct 1, 2020	2.5.5-19188	General Availability	Current Release - Release Notes DR Edition	
Eyeglass DR Edition and Data Protection Suite 2.5.5-	Oct 1, 2020	2.5.5-19184	General Availability	Current Release - Release Notes DR Edition	

19184					
Eyeglass Search & Recover 1.1-19042	Jan 1, 2020	1.1-19042	General Availability	Current Release - Release Notes Search & Recover	
Eyeglass DR Edition 2.5.4-19106	March 31, 2020	2.5.4-19106	General Availability	Current Release - Release Notes DR Edition	
Eyeglass Search & Recover 1.0-19033	Jan 1, 2020	1.0.0-19033	General Availability	Current Release - Release Notes Search & Recover	
Eyeglass Search & Recover 1.0-19022	Jan 1, 2020	1.0.0-19022	General Availability	Current Release - Release Notes Search & Recover	
Eyeglass Search & Recover 1.0-19018	Jan 1, 2020	1.0.0-19018	General Availability	Current Release - Release Notes Search & Recover	
Eyeglass DR	March 31, 2020	2.5.4-19020	General Availability	Current Release - Release Notes DR Edition	

Edition & Data Protection Suite - 2.5.4-19020					
Eyeglass Search & Recover - 1.0	Jan 1, 2020	1.0.0-13	General Availability	Current Release - Release Notes Search & Recover	
DR Edition & Ransomware Defender Patch - 2.5.4-18275	March 31, 2020	2.5.4-18275 Eyeglass only	General Availability	Current Release - Release Notes DR Edition Current Release - Release Notes Ransomware Defender	
Eyeglass DR Edition - Cluster Storage Monitor Only 2.5.4-18266	March 31, 2020	2.5.4-18266 Cluster Storage Monitor only	General Availability	Current Release - Release Notes DR Edition	
Eyeglass Ransomware Defender Only 2.5.3-	Dec 31st, 2019	2.5.3-18257 ECA only	General Availability	Current Release - Release Notes Ransomware Defender	

18257					
Eyeglass Unified Release (DR, Easy Auditor, Ransomware Defender) 2.5.3	Dec 31st, 2019	2.5.3-18251	General Availability	Current Release - Release Notes DR Edition Current Release - Release Notes Ransomware Defender Current Release - Release Notes Easy Auditor Current Release - Release Notes ECA	
Eyeglass Unified Release (DR, Easy Auditor, Ransomware Defender) 2.5.2	July 31, 2019	2.5.2-18080	Software upgrade installers are now available from the support page. Login at https://support.superna.net paste applianceID in the "Download the latest Eyeglass upgrade installers" Dialog box.	Release Notes 2.5.2 DR Edition Release Notes 2.5.2 Easy Auditor Release Notes 2.5.2 Ransomware Defender	
Eyeglass Unified Release (DR, Easy Auditor) 2.5.1	July 31, 2019	2.5.1-18013	Software upgrade installers are now available from the support page. Login at https://support.superna.net paste applianceID in the "Download the latest Eyeglass upgrade installers" Dialog box.	Release notes Easy Auditor 2.5.1 Release Notes 2.5.1 DR Edition Release Notes 2.5.1 Ransomware Defender	

Auditor,Ranso mware Defender) 2.5.1					
Eyeglass Easy Auditor Only Release 2.5.0	July 31, 2019	2.5-17282	Software upgrade installers are now available from the support page. Login at https://support.superna.net paste applianceID in the "Download the latest Eyeglass upgrade installers" Dialog box.	Release Notes Easy Auditor 2.5.0	
2.0.0 DR Edition Only EOL Notice Nov 17, 2018	Dec 17, 2018	2.0-17245.run	Software upgrade installers are now available from the support page. Login at https://support.superna.net paste applianceID in the "Download the latest Eyeglass upgrade installers" Dialog box.	Release Notes 2.0.0 DR Edition	
1.9.6 Ransomware Defender Only EOL Notice March 6, 2018	March 20, 2018	1.9.6- 17219.run		Release notes Ransomware Defender only 1.9.6	
1.9.5 DR Edition EOL Notice March 6, 2018	March 20, 2018	1.9.5- 17172.run		Performance Release with 2x CEE density per VM. Enhanced logging with syslog for faster log collection.	

1.9.4 Ransomware Defender EOL Notice March 6, 2018	March 20, 2018	1.9.4 17166		Release Notes 1.9.4 Ransomware Defender	
1.9.4 DR Edition EOL Notice March 6, 2018	March 20, 2018	1.9.4 17166		Release Notes 1.9.4 DR Edition	
1.9.3 Ransomware Defender EOL Notice March 6, 2018	March 20, 2018	1.9.3 17152		Release Notes 1.9.3 Ransomware Defender	
1.9.3 DR Edition EOL Notice March 6, 2018	March 20, 2018	1.9.3 17152		Release Notes 1.9.3 DR Edition	
1.9.2 Ransomware Defender EOL	March 20, 2018	1.9.2.17114		Release Notes 1.9.2 Ransomware Defender	

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

1.8.3 Notice July 31st 2017	October 29, 2017			Release 1.8.3 Release Notes	
1.8.1 Notice July 31st 2017	October 29, 2017			Release 1.8.1 Release Notes	
1.8.0 Notice July 31st 2017	October 29, 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	Dell EMC Open files api bug affects all previous releases of Eyeglass.
1.7.0 EOL Notice July 31st 2017	October 29, 2017	eyeglass_ui v1.7.0 r16134 eyeglass_rest v1.7.0 r16134 eyeglass_sca v1.7.0 r16134		Release 1.7.0 Release Notes	
1.6.3 EOL Notice May 31st 2017	July 31, 2017	eyeglass_ui v1.6.3 r16100 eyeglass_rest v1.6.3 r16100 eyeglass_sca v1.6.3 r16100		Eyeglass PowerScale Edition 1.6.3 Release Notes	
1.6.2 EOL Notice May 31st 2017	July 31, 2017	eyeglass_ui v1.6.2 r16087 eyeglass_rest v1.6.2 r16087 eyeglass_sca v1.6.2 r16087		Eyeglass PowerScale Edition 1.6.2 Release Notes	
1.6.1 EOL Notice May	July 31, 2017	eyeglass_ui v1.6.1 r16084 eyeglass_rest v1.6.0 r16084 eyeglass_sca v1.6.1 r16084		Eyeglass PowerScale Edition 1.6.1 Release Notes	

31st 2017					
1.6.0 EOL Notice May 31st 2017	July 31, 2017	eyeglass_ui v1.6.0 r16080 eyeglass_rest v1.6.0 r16080 eyeglass_sca v1.6.0 r16080		Eyeglass PowerScale Edition 1.6.0 Release Notes	
1.5.4 EOL Notice Nov 1st	Jan 1, 2017	eyeglass_ui v1.5.4 r16061 eyeglass_rest v1.5.4 r16061 eyeglass_sca v1.5.4 r16061		Eyeglass PowerScale Edition 1.5.4 Release Notes	Recommen ded patch for OneFS 8

© Superna LLC

1.1. Current Release - Release Notes DR Edition

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

- [What's New in Superna Eyeglass PowerScale Edition Release 2.5.7](#)
- [Supported OneFS releases](#)
- [DR Edition Feature Release Compatibility](#)
- [Feature Support Matrix](#)
- [End of Life Notifications](#)
- [Support Removed in Eyeglass Release 2.5.7](#)
- [Deprecation Notices](#)
- [New and Fixed in Eyeglass Release 2.5.7](#)
- [New in 2.5.7.1-21161](#)
 - [NEW - Eyeglass OVA released on the OpenSUSE 15.3 operating system. All other feature and functionality equivalent to 2.5.7.1-21140.](#)
- [New in 2.5.7.1-21140](#)
 - [T15777 Pool / Zone Failover AD Delegation Validation Readiness Check Enhancement](#)
 - [T18968 Pool / Zone Failover DNS Dual Delegation Validation Readiness Check Default changed to Disabled](#)

- NEW - Security
- T17897 Eyeglass audit action log enhancement to include action details
- T18655, T18764, T18778 Updated/Deprecated components
- NEW - General
- T19489 Websocket Upgrade
- T19517 Backup & Restore enhancement
- T19744 License Status Check
- T19463/T19746 OneFS 9.2 settings
- T19866 Add Managed Device window field description update
- T20079 Open File Limit Increase
- Fixed in 2.5.7.1-21140
 - T17522 Failover Scripting Engine SOURCE and TARGET variables expose password
 - T18523 DR Rehearsal Mode Enable / Revert Error when multiple policies selected
 - T18789 Unnecessary container running
 - T18896 Double URL on Eyeglass login
 - T18984 Configuration Replication Audit Error due to trailing slash
 - T19244 OneFS 9 Policy Hostname Validation failover readiness validation always shows success
 - T19728 Unlock My Files is case sensitive
- Fixed in 2.5.7-21096

- Fixed in 2.5.7-21081
 - T19175 Cannot modify PowerScale IP, user, password, RPO
- New in 2.5.7-21068
 - NEW - Eyeglass REST API for Eyeglass Automation
 - NEW - DR Assistant Final Screen shows summary of failover options (Enhancement)
 - NEW - Syslog alarm log
 - NEW - Security Updates
- Fixed in 2.5.7-21068
- Configuration Replication
 - T17618 SPN repair during Configuration Replication Job does not create missing SPNs
- General
 - T17408 Role Based Access Control doesn't handle user names with special characters
- 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 SyncIQ 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 SyncIQ Readiness not updated after Access Zone associated to a pool
- 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
- 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 SyncIQ Job Reports
- T4857: Failed SmartConnect Zone Rename step is not displayed in Failover Log
- T4878: Pool Failover - Non Runbook Robot SyncIQ policies can be mapped to Robot pool
- T4968: Zone missing from DR Dashboard Zone Readiness tab if a SyncIQ 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: SyncIQ 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 SyncIQ 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 SyncIQ 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
- T20628 Cannot disable Zone/IP Pool Readiness AD Delegation Validation (2.5.7.1 and higher)
- T21443 Quota failover error when source and target path are different and contain a \$
- 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 SyncIQ policies associated with same Zone will result in transient error on Eyeglass Zone replication creation
- 1924: Quotas on excluded SyncIQ 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

- T16888 Configuration Replication fails if SynclQ Policy source and target path are different and SynclQ policy path contains special character
- T16965 Audit does not consider differences on source and target for SMB share property inheritable_path_acl
- T18812 Error replicating SMB Share Run as Root permission with local user
- 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
- 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
- T9652 Unlock My Files inconsistent handling for unreachable PowerScale cluster

- 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
- General
 - 924: Inventory View shows + beside component when there are no more children
 - T17694: api token download of CMDDB 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
- T19274 Syslog alarm forwarding configuration not restored
- 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
- T19288 Custom Postfix email settings not restored
- 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
- T20584 Eyeglass service account password exposed on error connecting to Powerscale

- 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
- 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 same time as Job Type Change
- REST API retrieval of Jobs Known Limitation

What's New in Superna Eyeglass PowerScale Edition Release 2.5.7

What's New! In Superna Eyeglass PowerScale Edition Release 2.5.7 for DR can be found [here](#).

Supported OneFS releases

8.0.0.x

8.0.1.x

8.1.x.x

8.1.2.x

8.1.3.x

8.2.0.x

8.2.1.x

8.2.2.x

9.0

9.1

9.2.0.x (Requires 2.5.7.1)

9.2.1.x (Requires 2.5.7.1 and support case to provide a mapping file)

DR Edition Feature Release Compatibility

Feature	Source Cluster Release	Target SyncIQ Cluster Release
Configuration Replication non-DFS mode		
Configuration Replication	8.0.x.x	8.0.x.x 8.1.x.x** 8.2.x.x**

Configuration Replication	8.1.x.x	8.1.x.x*** 8.2.x.x** 8.0.x.x**
Configuration Replication	8.2.x.x	8.2.x.x** 8.1.x.x**
Configuration Replication	9.0	9.0
Configuration Replication	9.1	9.1
Configuration Replication	9.2	9.2
Configuration Replication DFS mode		
Configuration Replication - DFS Mode	8.0.x.x	8.0.x.x 8.1.x.x** 8.2.x.x**
Configuration Replication - DFS Mode	8.1.x.x	8.1.x.x*** 8.0.x.x** 8.2.x.x**
Configuration Replication - DFS Mode	8.2.x.x	8.2.x.x 8.1.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
SyncIQ Policy Failover non-DFS mode		
SyncIQ Policy Failover	8.0.x.x	8.0.x.x 8.1.x.x** 8.2.x.x**
SyncIQ Policy Failover	8.1.x.x	8.1.x.x*** 8.0.x.x** 8.2.x.x**
SyncIQ Policy Failover	8.2.x.x	8.2.x.x

		8.1.x.x** 8.0.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 DFS mode		
SyncIQ Policy Failover - DFS mode	8.0.x.x	8.0.x.x 8.2.x.x**
SyncIQ Policy Failover - DFS mode	8.1.x.x	8.1.x.x***
SyncIQ Policy Failover - DFS mode	8.2.x.x	8.2.x.x 8.1.x.x** 8.0.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
Access Zone Failover		
Access Zone Failover	8.0.x.x	8.0.x.x 8.1.x.x** 8.2.x.x**
Access Zone Failover	8.1.x.x	8.1.x.x*** 8.0.x.x** 8.2.x.x**
Access Zone Failover	8.2.x.x	8.2.x.x 8.1.x.x** 8.0.x.x**
Access Zone Failover	9.0	9.0
Access Zone Failover	9.1	9.1
Access Zone Failover	9.2	9.2

Runbook Robot cluster pairs SynclQ Policy Failover		
SynclQ Policy Failover	8.0.x.x	8.0.x.x 8.1.x.x** 8.2.x.x**
SynclQ Policy Failover	8.1.x.x	8.1.x.x*** 8.0.x.x** 8.2.x.x**
SynclQ Policy Failover	8.2.x.x	8.2.x.x 8.1.x.x** 8.0.x.x**
SynclQ Policy Failover	9.0	9.0
SynclQ Policy Failover	9.1	9.1
SynclQ Policy Failover	9.2	9.2
Runbook Robot* cluster pairs Access Zone Failover		
Access Zone Failover	8.0.x.x	8.0.x.x 8.1.x.x** 8.2.x.x**
Access Zone Failover	8.1.x.x	8.1.x.x*** 8.0.x.x** 8.2.x.x**
Access Zone Failover	8.2.x.x	8.2.x.x 8.1.x.x** 8.0.x.x**
Access Zone Failover	9.0	9.0
Access Zone Failover	9.1	9.1
Access Zone Failover	9.2	9.2
Live Ops - DR Test Mode		
Live Ops DR Test Mode	8.1.x.x	8.1.x.x***
Live Ops DR Test Mode	8.2.x.x	8.2.x.x

Live Ops DR Test Mode	9.0.x.x	9.0.x.x
Live Ops DR Test Mode	9.1.x.x	9.1.x.x
Snapshots and Schedules	8.0.x.x	8.0.x.x
Snapshots and Schedules	8.1.x.x	8.1.x.x***
Snapshots and Schedules	8.2.x.x	8.2.x.x - pending testing 8.1.x.x - pending testing
Dedupe Path Settings	8.0.x.x	8.0.x.x
Dedupe Path Settings	8.1.x.x	8.1.x.x**
Dedupe Path Settings	8.2.x.x	8.2.x.x - pending testing 8.1.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.**

*****Due to PowerScale OneFS PAPI API defect, the following configuration change must be made on the Eyeglass appliance to support OneFS releases lower than these releases:**

- Not Required on lower releases than below but note the bug is present and does not affect Eyeglass
 - OneFS 8.0.0.6 (Fixed)
 - OneFS 8.0.1.3 (Fixed)
- Requires Change below on lower Releases
 - OneFS 8.1.0.2 (Fixed does not require change below)
 - OneFS 8.1.1.1 (Fixed does not require change below)

ssh to the Eyeglass appliance

1. Elevate to root user by using command below and entering admin password


```
sudo su -
```

2. cd /opt/superna/sca/data
3. edit system.xml
4. Find the line

```
<runconfigsyncinparallel>true</runconfigsyncinparallel>
```

5. And modify to false

```
<runconfigsyncinparallel>>false</runconfigsyncinparallel>
```

6. Save your changes
7. Restart the sca service

```
systemctl restart sca
```

9. Done

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
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](#).

Support Removed in Eyeglass Release 2.5.7

Following feature are no longer available in 2.5.7 as posted in the Release 2.5.6 Deprecation Notices:

1. OpenSUSE 42.3 operating system: Upgrade on OpenSUSE 42.3 operating system is no longer supported. Use Backup & Restore to the latest OVF to be on a supported release.
2. Custom Jobs: Eyeglass custom jobs for configuration replication is no longer supported.

Config Migration feature can be used to replicate SMB Shares or NFS Exports where no SyncIQ policy exists. Refer to documentation [here](#).

1. Configuration of SYSLOG forwarding from /var/log/messages.
The new alarm architecture in 2.5.7 uses a dedicated log that will roll over and provide alarm history external from the database and alarm history in the GUI. Refer to documentation [here](#).

Deprecation Notices

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

New and Fixed in Eyeglass Release 2.5.7

New in 2.5.7.1-21161

NEW - Eyeglass OVA released on the OpenSUSE 15.3 operating system. All other feature and functionality equivalent to 2.5.7.1-21140.

New in 2.5.7.1-21140

NEW - Failover

T15777 Pool / Zone Failover AD Delegation Validation Readiness Check Enhancement

For environments configured for Access Zone failover for multiple Access Zones or IP Pool failover for multiple pools, the AD Delegation Validation Readiness check is now only run once per Active Directory Domain Provider rather than for each Access Zone or IP Pool reducing queries to AD and time to complete the readiness validation.

T18968 Pool / Zone Failover DNS Dual Delegation Validation Readiness Check Default changed to Disabled

For new deployments of 2.5.7.1 or upgrade from a pre 2.5.6 release the DNS Dual Delegation validation is disabled. Plan to replace this with a button to check this configuration in a future release. Existing deployments upgraded to 2.5.7.1 from 2.5.6 or 2.5.7 will retain their existing enable/disable setting for DNS Dual Delegation validation.

NEW - Security

T17897 Eyeglass audit action log enhancement to include action details

The Eyeglass audit action log (/opt/superna/sca/logs/apiaudit.log) in addition to logging which windows were accessed on the Eyeglass desktop now includes information about the operation that was performed while the window was open.

T18655, T18764, T18778 Updated/Deprecated components

- tomcat deprecated and no longer required or running
- jquery version update to v3.6.0
- java version update to v1.8.0_291

NEW - General

T19489 Websocket Upgrade

Websocket functionality required for watching logs, real time displays such as Easy Auditor WireTap or Performance Auditor now runs over port 443 on different URLs. Ports 2011, 2012, 2013, 2014 are no longer required to be open and are closed on upgrade to 2.5.7.1.

T19517 Backup & Restore enhancement

For restore of Eyeglass configuration from an old Eyeglass appliance to a new Eyeglass appliance, new import command "igls app pull-config" can be run on the new appliance and manages creation of the restore backup, transfer to new appliance and restoring configuration. Details on using this command are available in Eyeglass upgrade documentation [here](#).

T19744 License Status Check

New health check runs every 5 minutes to ensure that Powerscale cluster license state set in Eyeglass for Ransomware Defender, Easy Auditor and Performance Auditor is correctly set on ECA nodes.

T19463/T19746 OneFS 9.2 settings

Settings to support OneFS 9.2 are available by default now as of 2.5.7.1.

T19866 Add Managed Device window field description update

In the Add Managed Device window the field description for entering the IP address for PowerScale cluster now correctly indicates that a Node IP address is required and that SSIP is not supported.

T20079 Open File Limit Increase

Eyeglass open files limit has been increased to reflect additional functionality requirements.

Fixed in 2.5.7.1-21140

T17522 Failover Scripting Engine SOURCE and TARGET variables expose password

The Failover Scripting Engine SOURCE and TARGET environment variable information includes the password of the account used to connect from Eyeglass to PowerScale in plain text.

Resolution: Password is no longer included for SOURCE and Target variables.

T18523 DR Rehearsal Mode Enable / Revert Error when multiple policies selected

A DR Rehearsal Mode Enable / Revert where more than 3 SynclQ policies are involved either selected for SynclQ or DFS mode or an Access Zone with more than 3 SynclQ policies, the final step which updates Eyeglass with the rehearsal status fails with a lock conflict error..

Resolution: Final step to update eyeglass with the rehearsal status no longer results in a lock conflict error.

T18789 Unnecessary container running

Deployments without Performance Auditor licensed will either show an error due to Prometheus and Grafana containers not running or will unnecessarily have them running. No impact to product functionality.

Resolution: Prometheus and Grafana now only run when Performance Auditor is licensed.

T18896 Double URL on Eyeglass login

Under some conditions the connections to port 2011 on the Eyeglass appliance are not managed properly resulting in double URL on login.

Resolution: This is no longer an issue as of 2.5.7.1 and addressed as part of enhancement T19489 Eyeglass Websocket Upgrade.

T18984 Configuration Replication Audit Error due to trailing slash

Configuration Replication under some circumstances will not replicate the trailing slash on an SMB share, NFS export or NFS Alias path. For example, `/ifs/data/path/` on the source and `/ifs/data/path` on the target after replication. This will result in a post replication audit error when comparing path on source and target. This has no impact to failover functionality of Eyeglass.

Resolution: Trailing slash is now handled and does not result in a post replication audit error.

T19244 OneFS 9 Policy Hostname Validation failover readiness validation always shows success

For OneFS 9 PowerScale cluster Policy Hostname Validation for failover readiness incorrectly shows success when the IP pool associated with the SyncIQ policy target host does not have an `igls-ignore` hint.

Impact for Policy and DFS Failover: None. This validation is not required for these failover types.

Impact for Pool and Access Zone failover: if `igls-ignore` hint is missing from the replication pool, the SyncIQ policy target host could be failed over and active on the wrong cluster.

Resolution: Policy Hostname validation now correctly identifies whether `igls-ignore` hint is present for PowerScale OneFS 9 version.

T19728 Unlock My Files is case sensitive

Unlock My Files searching now is case sensitive instead of case insensitive.

Resolution: Unlock My Files search is now case insensitive.

Fixed in 2.5.7-21096

See fixes in previous 2.5.7 releases.

Fixed in 2.5.7-21081

T19175 Cannot modify PowerScale IP, user, password, RPO

When updating PowerScale IP, user, password or RPO from the Inventory view Edit window the change fails with the error "failed to update job with new cluster ip".

Resolution: PowerScale IP, user, password and RPO can now be edited from the Inventory view Edit window.

New in 2.5.7-21068

NEW - Eyeglass REST API for Eyeglass Automation

2.5.7 introduces versioned API support as well as following new APIs:

- Run a configuration replication job on demand and get status
- Run a DR Readiness job on demand and get status
- Set new configuration replication job type (AUTO, AUTODFS, or AUTOSKIPCONFIG)
- Enable/Disable configuration replication jobs

NEW - DR Assistant Final Screen shows summary of failover options (Enhancement)

Final screen of DR Assistant wizard for starting a failover now includes a summary display of failover options selected on the initial screen of the failover wizard for final confirmation.

NEW - Syslog alarm log

New alarm architecture will use a dedicated log that will roll over and provide alarm history external from the database and alarm history available in the GUI. Information on Configuration of Syslog alarm forwarding can be found [here](#) - see Configuration of SYSLOG Forwarding -> 2.5.7 .

Note: Prior configuration in older releases using /var/log/messages is no longer supported - please review deprecation notice.

NEW - Security Updates

Web server hardening with default hardening applied upon upgrade for XSS and many other vulnerabilities. More information on security hardening can be found [here](#).

New audit log for Eyeglass login and desktop operations. More information available in Eyeglass Access Security API Auditing section of the hardening guide [here](#).

Fixed in 2.5.7-21068

Configuration Replication

T17618 SPN repair during Configuration Replication Job does not create missing SPNs

The SPN repair component of the Eyeglass Configuration Job does not create missing SPNs.

Impact: This only impacts creation of SPNs for new SmartConnect zones added in Powerscale. This does not affect SPN create/delete during failover.

Resolution: SPN repair component of Eyeglass Configuration Replication Job now creates missing SPNs.

General

T17408 Role Based Access Control doesn't handle user names with special characters

RBAC can be setup with users that have special characters or language specific characters or groups where users have special or language characters, but on login the name is not resolved properly and the proper role is not assigned. User gets read only desktop view.

Resolution: Login where RBAC has been configured with user that have special characters or language specific characters now succeeds.

Technical Advisories

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

Known Issues

Failover

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 SynclQ 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: 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 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 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 SyncIQ 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 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
```

```
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 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 "igls-ignore". Note it is best practise to ensure unique hints by using a naming format that uses cluster name - for example: igls-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 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 - SyncIQ 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.

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.

Workaround: Related alarm can be ignored if the validation is disabled.

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.

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 SynclQ 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 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 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.

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

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

Workaround: Configuration objects such as SMB shares and NFS exports must be kept in sync on the DR cluster manually. To avoid the replication error on each cycle and keep the SyncIQ policy available for failover the Eyeglass Configuration Replication job can be set to AUTOSKIPCONFIG as per instructions [here](#).

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 Error replicating SMB Share Run as Root permission with local user

In some cases where an SMB share permission is configured with run as root and local users the run as root permissions are replicated to the target as regular permissions and also subsequent attempts to update results in a duplicate permission error.

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.

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.

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.

Workaround: Resolve PowerScale cluster reachability issue.

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.

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.

T19274 Syslog alarm forwarding configuration not restored

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

Workaround: Manually backup the syslog alarm forwarding configuration from the original Eyeglass appliance off appliance should it need to be restored.

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**

T19288 Custom Postfix email settings not restored

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

Workaround: Manually backup the custom Postfix email settings from the original Eyeglass appliance off appliance should it need to be restored.

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 SyncIQ 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 SyncIQ 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.

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.

Workaround: None available. Patch pending.

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 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 SyncIQ Policy is renamed, Eyeglass considers it to be a new SyncIQ 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.

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 SynclQ Job Report log were combined. In this case you are able to see the SynclQ 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 SynclQ 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 SynclQ 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

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 LLC

1.2. Current Release - Release Notes

Ransomware Defender

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

- [What's New in Superna Eyeglass Ransomware Defender Edition Release 2.5.7](#)
- [Supported OneFS releases](#)
- [Supported Eyeglass releases](#)
- [Active Directory Compatibility](#)
- [Inter Release Functional Compatibility](#)
- [End of Life Notifications](#)
- [Support Removed in Eyeglass Release 2.5.7](#)
- [Deprecation Notices](#)
- [New / Enhanced / Fixed in 2.5.7](#)
- [New in 2.5.7.1-21161](#)
 - [NEW - ECA OVF released with configuration files for 1, 3, 6 node deployments on the OpenSUSE 15.3 operating system. All other feature and functionality equivalent to 2.5.7.1-21140.](#)
- [New in 2.5.7.1-21140](#)
 - [NEW - T14329 Security Guard now supports SMB3](#)
 - [NEW - T16838 Well Known Ransomware File Extension List Versioning](#)
 - [NEW - T17804 Learned Thresholds Management Enhancements](#)
- [Fixed in 2.5.7.1-21140](#)

- T15234 igls rsw restore leaves share without permission where user permission configured
- T17747 Honeypot detections incorrectly able to be added with Learned Thresholds
- T17900 Clients column for Ransomware events may not display all IP addresses
- T18170 Adding custom File Filter requires 2 Save operations
- T18913 Ransomware Defender Thresholds Advanced Mode cannot disable all detectors
- Fixed in 2.5.7-21096
 - T19467 ECA logs missing from backup on new OVA deployment
- New/Fixed in 2.5.7-21081
- New / Enhanced / Fixed in 2.5.7-21068
- New in 2.5.7-21068
 - NEW - Learning Mode
 - NEW - Monitor Mode by User, Path or IP Address
 - NEW - Dual Vector Warning Detection
 - NEW - File Filters List
 - NEW - Ransomware Events "Actions" Copy to Clipboard
 - NEW - Archive as False Positive for TD7
- Fixed in 2.5.7-21068
 - T14798 Well Known user Authenticated Users not handled

- T16830 TD 7 Extension flag as false positive will add to the UI but will not take affect
- 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
 - T4337 Modifying Ransomware Defender Settings or Running the lock root command removes lock root settings
 - 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
- T11832 Ransomware Security Event which is promoted from Warning to Major does not respect Major Grace Period
- 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
- T18985 igls rsw restoreaccess cannot restore access for unresolvable user
- 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
- 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 canceling an operation to switch modes
 - T21207 Custom Snapshot Expiry not preserved after modifying Settings on Threshold menu
- Known Limitations
 - 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

What's New in Superna Eyeglass Ransomware Defender Edition Release 2.5.7

What's New! In Superna Eyeglass Ransomware Defender Edition Release 2.5.7 can be found [here](#).

Supported OneFS releases

8.0.0.x

8.0.1.x

8.1.x.x

8.1.2.x

8.1.3.x

8.2.0.x

8.2.1.x

8.2.2.x

9.0

9.1

9.2 (requires modification by support for Eyeglass VM before 2.5.7.1)

Supported Eyeglass releases

Superna Eyeglass Ransomware Defender Version	Superna Eyeglass Version
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
2.5.7, 2.5.6 and 2.5.5 all versions	Microsoft Active Directory 2012, 2016

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
Threat Detection	Yes	Yes	Yes	Untested	Untested
Security Guard	Yes	Yes	Yes	Untested	Untested

End of Life Notifications

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

Support Removed in Eyeglass Release 2.5.7

1. Operating System OpenSUSE 42.3: Upgrade for OpenSUSE 42.3 is no longer supported. Use Backup & Restore to a new OVF or in place OS Upgrade to be on a supported release.

Deprecation Notices

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

New / Enhanced / Fixed in 2.5.7

New in 2.5.7.1-21161

NEW - ECA OVF released with configuration files for 1, 3, 6 node deployments on the OpenSUSE 15.3 operating system. All other feature and functionality equivalent to 2.5.7.1-21140.

New in 2.5.7.1-21140

NEW - T14329 Security Guard now supports SMB3

Security Guard can now successfully authenticate with either SMB2 or SMB3.

NEW - T16838 Well Known Ransomware File Extension List Versioning

Version of the banned file list can now be selected, auto selected and differenced from the Eyeglass command line. Details are available in documentation [here](#).

NEW - T17804 Learned Thresholds Management Enhancements

Following enhancements have been made to the Ransomware Defender -> Learned Thresholds window:

- search bar added to be able to search for User
- multiple entries on the Learned Threshold list can now be selected and deleted at once

Note: Known Issue T20194 Deleted items stay in delete window

Fixed in 2.5.7.1-21140

T15234 igls rsw restore leaves share without permission where user permission configured

If you have assigned share permission using AD user permission directly (no AD group permission). if that user is locked out and you are unable to restore access from the GUI the igls rws restoreaccess command that would usually be used to restore access will remove the deny permission but will not put back the original user permission.

Resolution: Permission is now restored where share permission is using AD user permission directly. When using the igls rsw restore command the user must be specified in format '<DOMAIN>\<user>'.

T17747 Honeypot detections incorrectly able to be added with Learned Thresholds

Either in automated Learning Mode or manual Archive as False Positive a honeypot detection can be added to the Learned Thresholds list. This is not desired behaviour as any activity against a honeypot file is considered suspicious.

Resolution: Honeypot detections are no longer added to the Learned Threshold list in automatic learning mode or when a manual Archive as False Positive is applied to the active event..

T17900 Clients column for Ransomware events may not display all IP addresses

For a security event where there are signals for the same User (account) from different IP addresses, the Clients column may not list all IP addresses.

Resolution: the Clients column now shows all IP addresses.

T18170 Adding custom File Filter requires 2 Save operations

When adding a custom File Filter, the initial save shows "File filter added successfully" but at this point the custom filter is not saved yet. The Save button on the File Filters main window must also be selected to make the change.

Resolution: Initial save after selecting now permanently saves the custom filter. Additionally

- the File Filter list now also includes a "Type" column to identify whether the entry on the list is a default or custom entry
- custom entries on the file filter list can be deleted (default entries cannot)

T18913 Ransomware Defender Thresholds Advanced Mode cannot disable all detectors

In the Ransomware Defender Thresholds you cannot disable all detectors. The GUI incorrectly changes to Enforcement mode and does not allow to switch back to Advanced Mode.

Resolution: It is not possible to disable all detectors in Advanced Mode.

IMPORTANT: Advanced Mode should never be changed without support advising when to use this option. Changing these settings can disable detection without understanding the impact of the changes.

Fixed in 2.5.7-21096

T19467 ECA logs missing from backup on new OVA deployment

ECA OVA missing symbolic link resulted in logs not being included in a backup.

Resolution: OVA symbolic link is now present.

New/Fixed in 2.5.7-21081

Refer to Enhancements/Fixes in previous 2.5.7 versions.

New / Enhanced / Fixed in 2.5.7-21068

New in 2.5.7-21068

NEW - Learning Mode

Automates the process of monitoring user behavior and applying settings needed to tune Ransomware Defender and reduce false positive detections. Learning mode will manage both user behaviors and extension based detections from the banned list of files.

- On the Ransomware Defender Threshold window there is a new checkbox “Automatically learn from events in monitor state”. When this is checked, once an active **MONITOR** event in Warning expires the following 2 updates will be made automatically:
 - Automatically “Archive as False Positive” to add the events to the Learned Thresholds (renamed from False Positive) list for a user behaviour detection. This is the same as manually selecting Archive as False Positive from the GUI Action menu in previous releases.
 - Automatically add well known extensions to the File Filters list (renamed from Allowed Extensions) if the event was related to the detection of an extension from the banned file list.It is the Customer responsibility to review changes made by Learning Mode and accept them or remove them to back them out.

Detailed documentation on Learning Mode is available here:

- [How to Teach Ransomware Defender about false positives - Learning Mode](#)
- [Deployment Overview with Learning Mode](#)

NEW - Monitor Mode by User, Path or IP Address

This new feature removes the need to whitelist and allows monitor mode to be applied to a Path, AD User account or IP Address while Enforcement mode is enabled. This retains detection and snapshots for items on the Monitor Only Settings list without any lockout. This will replace whitelisting in most cases.

Detailed documentation on Monitor Mode by User, Path or IP Address is available here:

[Monitor Mode List Overview](#)

[How to Configure Monitor Mode List](#)

[Planning new workloads best practice](#)

We recommend that all customers convert their existing Ignored List settings to Monitor Only Settings to take advantage of the detection and snapshot protection without lockout.

Note: This is likely to result in new detections that will have to be assessed. Help on assessing an active event is available [here](#). You may choose to enable Learning Mode to automatically apply flag as false positive settings or the entry can be moved back to the Ignored List.

Detailed documentation to convert your existing Ignore List entries to Monitor Only entries is available [here](#):

[How to convert whitelists to monitor mode lists](#)

NEW - Dual Vector Warning Detection

A new behavioral detection option looks for different behaviors within the Warning severity. This new option will add one additional pattern of suspicious user activity that is designed to ignore spikes in user detection signals and provides a new analysis vector on user IO behavior to generate warnings.

We recommend that all customers configure the 2nd Warning vector as per documentation.

Note: Adding this second vector may result in new detections that will need to be assessed and if false positive managed by flagging the event as false positive or updating the File Filters list. Help on assessing an active event is available [here](#).

Detailed documentation available here:

[Dual Vector Warning Detection in 2.5.7 or later](#)

NEW - File Filters List

Allowed File List from earlier releases has been redesigned and is now called File Filters. Updates from previous releases:

- All items on the banned file list are now visible and searchable from the File Filters GUI
- Entries on the banned file list can be enabled/disabled or put into monitor state from the GUI
- Custom entries can be added to the banned file list
- Archive as False Positive action against an Active Event that was related to a banned file list entry now updates the list to disable analysis for that extension
- Banned file list is now managed from the Eyeglass appliance and new versions can be retrieved over the internet leveraging existing phone home firewall and URL whitelisting

Detailed documentation is available here:

- [How to Manage Banned File Extensions with Enforcement Modes \(2.5.7 >\)](#)
- [How to add Custom File extensions \(2.5.7 or greater\)](#)
- [How to switch banned file url to latest, default or a newer file](#)

NEW - Ransomware Events "Actions" Copy to Clipboard

The Ransomware Defender Active Events and Events History Actions window now have a Copy to Clipboard option to easily and quickly make a copy of all actions related to an event and paste into external document for easy review.

NEW - Archive as False Positive for TD7

Manually applying the Archive as False Positive action against a Ransomware event associated with an entry in the File Filters list will now disable that entry in the File Filters list instead of adding the account to the Learned Threshold list.

Fixed in 2.5.7-21068

T14798 Well Known user Authenticated Users not handled

When well known user "Authenticated User" is used for share permissions Ransomware Defender does not translate this permission into users and therefore does not affect a deny for any users against that share.

Resolution: Ransomware Defender now translates "Authenticated User" into users and can affect a lockout against a user where share permission configured with "Authenticated User".

T16830 TD 7 Extension flag as false positive will add to the UI but will not take affect

Flagging TD 7 detection as false positive will add to the UI but will not take effect. This is not a user behavior detection and requires a CLI command to whitelist the extension. This is by design and a future release will block this in the GUI and will allow adding to the extension whitelist automatically from the GUI. In the current release the CLI is required to add an extension to the whitelist.

Resolution: Now when archiving a TD 7 extension event with flag as false positive either in Learning Mode or manually, the associated extensions are automatically disabled from the banned file list so that they will no longer be considered during analysis for Ransomware. More information on managing the banned file list can be found here: [How to Manage Banned File Extensions with Enforcement Modes \(2.5.7 >\)](#)

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.

T4337 Modifying Ransomware Defender Settings or Running the lock root command removes lock root settings

Lock root settings applied using command

```
igls admin lockroot --lock_root
```

.are lost each time a change is made to Ransomware Settings or running the igls admin lockroot command. If lock root was enabled it becomes disabled.

Workaround: Each time a Ransomware Settings change is made, the lock root setting must be reapplied manually. Please contact support.superna.net for assistance.

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

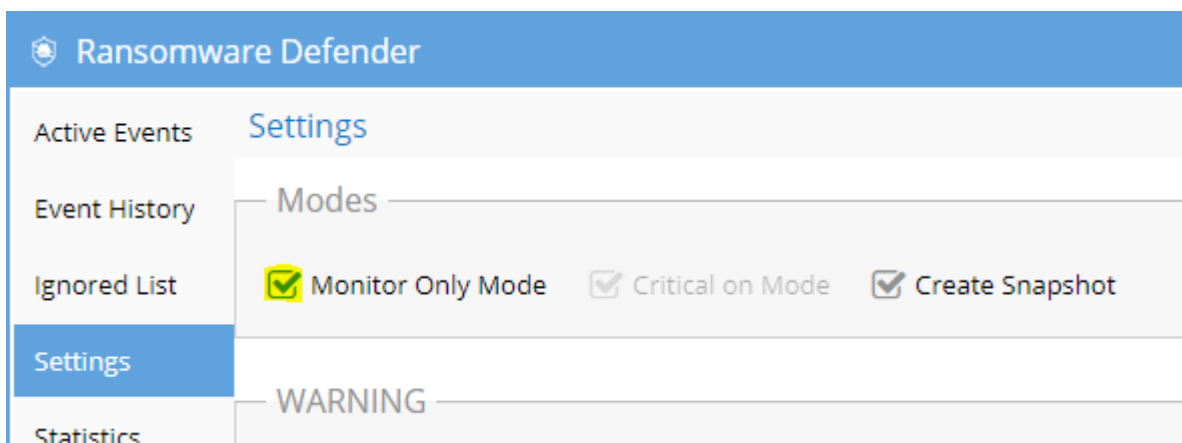
It may occur that a user is only partially locked out when a multi-user lockout is occurring due to an error response from the PowerScale cluster during user resolution in Active Directory. In this case the error is not displayed in the Eyeglass event history.

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 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: None available. PowerScale scheduled snapshots may be available for recovery.

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.

Workaround: None available.

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.

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.

Workaround: The Ransomware Defender GUI can restore access in this case while the event is in the Active Events list. If the event has already been archived to the Event History contact support.superna.net for assistance.

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.

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 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 canceling 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.

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.

Workaround: After making a change in the Threshold window, re-run the `igls` command to set the custom snapshot expiry.

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]

*.symbiom_ransomware_locked

*.[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 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

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.

© Superna LLC

1.3. Current Release - Release Notes Easy Auditor

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

- [What's New in Superna Eyeglass Easy Auditor Edition](#)
- [Supported OneFS releases](#)
- [Supported Eyeglass releases](#)
- [Inter Release Functional Compatibility](#)
- [End of Life Notifications](#)
- [Deprecation Notices](#)
- [New / Issues Fixed in 2.5.7](#)
- [New in 2.5.7.1-21161](#)
 - [NEW - ECA OVF released with configuration files for 1, 3, 6 node deployments on the OpenSUSE 15.3 operating system. All other feature and functionality equivalent to 2.5.7.1-21140.](#)
- [New in 2.5.7.1-21140](#)
 - [T19805 Path search speed optimization](#)
- [Fixed in 2.5.7-21096](#)
 - [T19467 ECA logs missing from backup on new OVA deployment](#)
- [New/Fixed in 2.5.7-21081](#)
- [Enhancements and Fixes in 2.5.7-21068](#)
- [New in 2.5.7-21068](#)
 - [Where Did My Folder Go Enhancements](#)
- [Fixed in 2.5.7-21068](#)

- T13539 PowerScale Directory selector missing directories
- T16978 Display of files for Mass Delete always shows 1 file
- 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 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
- 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
- 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"
 - T20936 Bulk Ingest of Old Audit Data is not functional
- 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
- T11540 Active Auditor may report on Audit Failure events
- T12380 Ransomware Defender Ignore List settings are applied to Active Auditor analysis
- 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 2.5.7

What's New! In Superna Eyeglass Easy Auditor Edition Release 2.5.7 can be found [here](#).

Supported OneFS releases

8.0.0.x

8.0.1.x

8.1.x.x

8.1.2.x

8.1.3.x

8.2.0.x

8.2.1.x

8.2.2.x

9.0

9.1

9.2 (requires modification by support for Eyeglass VM before 2.5.7.1)

Supported Eyeglass releases

Superna Eyeglass Easy Auditor Version	Superna Eyeglass Version
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 8.0 - OneFS 8.0.1	OneFS 8.0.1 - OneFS 8.1	OneFS 8.0 - OneFS 8.1	OneFS 8.0.x , 8.1.x - OneFS 8.2.x	OneFS 9.1 or 9.2
Reporting	Untested	Untested	Untested	Untested	Untested
Active Auditing	Untested	Untested	Untested	Untested	Untested

End of Life Notifications

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

Deprecation Notices

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

New / Issues Fixed in 2.5.7

New in 2.5.7.1-21161

NEW - ECA OVF released with configuration files for 1, 3, 6 node deployments on the OpenSUSE 15.3 operating system. All other feature and functionality equivalent to 2.5.7.1-21140.

New in 2.5.7.1-21140

T19805 Path search speed optimization

A custom path query for selected audit events now uses a new table for optimized searching and has been shown to improve the speed of some searches up to 400% faster. The audit events that are being stored for fast path search are: DIR_RENAME, DIR_DELETE, FILE_RENAME, FILE_DELETE. In the Finished Reports if the new optimized searching is used the Report ID will be appended with "quickscan".

Fixed in 2.5.7-21096

T19467 ECA logs missing from backup on new OVA deployment

ECA OVA missing symbolic link resulted in logs not being included in backup.

Resolution: OVA symbolic link now present.

New/Fixed in 2.5.7-21081

Refer to Enhancements/Fixes in previous 2.5.7 versions.

Enhancements and Fixes in 2.5.7-21068

New in 2.5.7-21068

Where Did My Folder Go Enhancements

Where Did My Folder Go performance enhancements to improve speed of retrieval of results using display limit configured.

Fixed in 2.5.7-21068

T13539 PowerScale Directory selector missing directories

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.

T16978 Display of files for Mass Delete always shows 1 file

On the GUI for Active Auditor > Active Events as well as in associated alarm information the number of affected files is always displayed as 1. This is a display issue only. The number of files as configured in the trigger was correctly used in the detection.

Resolution: The Affected Files count displays the count of files that triggered the detection and the GUI file view shows the last file that was associated with the detection in the "Affected Files - Sample" tab.

Full list of files that were part of the detection can be retrieved by using the "Affected Files - All" tab.

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 save query to review it's 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 then 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 the 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 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 first line

Report Query File Ext filter is only editable in first line. Clicking anywhere else in the box will not let you enter any text

Workaround: None required. Enter 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 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

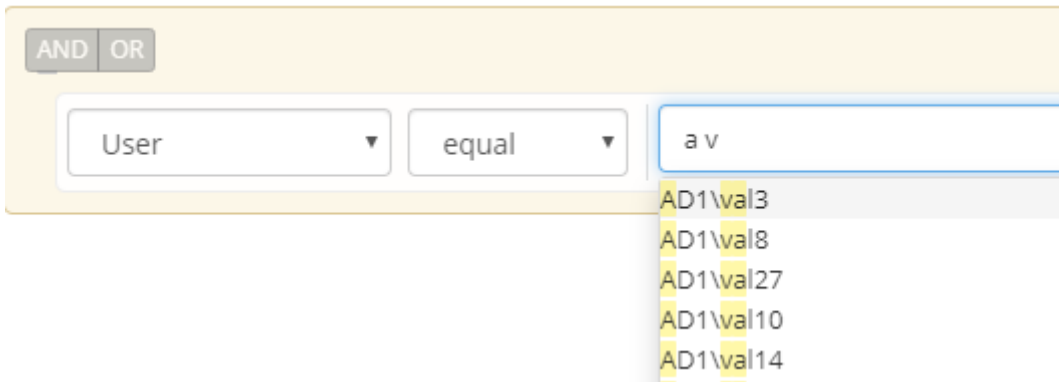
T10911 Share/Stale Access Report issue when AD has nested groups

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



The screenshot shows a search filter interface. At the top, there are two buttons labeled 'AND' and 'OR'. Below them, there is a dropdown menu labeled 'User' with a downward arrow. To its right is another dropdown menu labeled 'equal' with a downward arrow. To the right of these is a text input field containing 'a v'. Below the text input field, a list of suggestions is displayed: 'AD1\val3', 'AD1\val8', 'AD1\val27', 'AD1\val10', and 'AD1\val14'. Each suggestion is highlighted with a yellow background.

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

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.

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 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 upgrade to 2.5.6.

Workaround: None required. New logs will have 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.

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.

Workaround: Contact support.superna.net for assistance.

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.

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.

Known Limitations

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.

1.4. Current Release - Release Notes Search and Recover

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

- [What's New in Superna Eyeglass Search and Recover](#)
- [Supported OneFS releases](#)
- [End of Life Notifications](#)
- [Deprecation Notices](#)
- [New in this release - 1.1.5-21169](#)
- [Beta in this release - 1.1.5-21169](#)
 - [File System Browser - Beta](#)
 - [Data Classification - Beta](#)
- [Fixed in this release - 1.1.5-21169](#)
 - [T20488 File Size filter not applied correctly on scheduled report](#)
 - [T21123 Error running test report after editing schedule for Whats in the file pools](#)
 - [T15679 / T21593 Issues with File Pool Policy Reporting](#)
- [New in this release - 1.1.5-21163 \(Controlled Availability\)](#)
 - [New Quick Reports](#)
 - [When can I delete my worm lock data? Find more information in our Quick Reports Guide here.](#)
- [New in this release - 1.1.5-21133 \(Controlled Availability\)](#)
 - [New Quick Reports](#)
 - [Scheduled Reports](#)

- Beta in this release - 1.1.5-21133/21163
 - S3 Indexing (meta data only)
- Coming in a patch release - 1.1.5-21169
 - Snapshot Mode
- Fixed in this release - 1.1.5-21163
 - T20473 File Path Selector not working
 - T21026 Incremental Index does not handle Alternate Data Stream (ADS) Files
 - T21259, T21260 What's in the file pools quick reports issues
 - T20501 How fast is my data growing Quick Report may be missing data
 - T21030 Scheduled report test for What's growing old has incorrect results
 - T21253 Index job does not finish
- Fixed in this release - 1.1.5-21133
 - T9378, T17560 File or Folder rename may return results for both old and new name - files orphaned in search index
 - T15808 Advanced Search and Quick Report File Owner filter is not working
 - T13557 CMD Writer file not created when number of rows specified
 - T13542 Require 2 clicks to see Recover File option
 - T15540 Search Email Notification Test Feature not functional
- 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...
 - 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
- T20988 Incremental index for multiple folders does not run when Search is managing multiple Powerscale clusters
- T21033 Searching content in index with special characters returns incorrect results
- T21035 Quick Report result selector not cleared after Quick Report is closed
- T21075 snapshotmonitor mode is not working

- 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
- File Recover
 - T13292 Recover File in error when file name selected contains non US-ASCII characters
- 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
 - T16115 Admin Group configuration allows user login and search
 - T21174 File System Browser Tree is not filtered based on End User Security configuration
 - T21588 File Path Selector is not filtered based on End User Security Configuration
- 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
- General
 - 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
- 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.

What's New in Superna Eyeglass Search and Recover

Release 1.1.5

What's New! In Superna Eyeglass Search and Recover can be found [here](#).

Supported OneFS releases

8.0.0.x

8.0.1.x

8.1.x.x

215

8.2.x.x

9.1.x.x

9.2.x.x

End of Life Notifications

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

Deprecation Notices

Following features will no longer be supported as indicated below:

1. As of February 1, 2022
 - a. Support for OneFS 8.0.x.x releases
 - b. Support for OneFS 8.1.x.x releases

New in this release - 1.1.5-21169

Refer to New in previous releases.

Beta in this release - 1.1.5-21169

File System Browser - Beta

Interactive file system capacity browser. Find more information [here](#).

Data Classification - Beta

Custom tagging to read contents of files based on regex pattern matching.

Classification tags available in Advanced Criteria for any search or Quick Report. Find more information in the [Content Classification Feature Guide](#).

Fixed in this release - 1.1.5-21169

T20488 File Size filter not applied correctly on scheduled report

Scheduled report does not correctly apply the File Size filter and the scheduled report will have the incorrect results.

Resolution: The File Size filter is now correctly saved for a scheduled report.

T21123 Error running test report after editing schedule for Whats in the file pools

For the Whats in the file pool? quick report, if an existing schedule is edited the schedule test function no longer works and displays a "null" error. Impact is only on test function. Modification to schedule can be saved and will be respected.

Resolution: Test report can now be run after editing the schedule.

T15679 / T21593 Issues with File Pool Policy Reporting

File Pool Policy reporting has following issues

- last modified older filter is not working
- path match filter may not work under some conditions
- in some cases combining filters that work independently does not work

Resolution: Last modified older than, path match and combining filters are now working.

Note:

- For path match, the path is displayed in format "folder/sub-folder" and the full path "/ifs/folder/sub-folder" is assumed.
- If a file pool policy is modified or deleted, a restart is required for Search to recognize this change. Contact support.superna.net for assistance for proper procedure.

New in this release - 1.1.5-21163 (Controlled Availability)

New Quick Reports

When can I delete my worm lock data? Find more information in our Quick Reports Guide [here](#).

Scheduled Reports

Scheduled Searches GUI (T19699)

New GUI that shows which searches are scheduled, when they last ran and last run status. Find more information in the ShowBack and ChargeBack Guide [here](#).

New in this release - 1.1.5-21133 (Controlled Availability)

New Quick Reports

What's in the file pools? Find more information in our Quick Reports Guide [here](#).

Note: File Pool Policies can now be added in Advanced Search Criteria for any search or Quick Report.

How fast is my data growing? Find more information in our Quick Reports Guide [here](#).

Scheduled Reports

Any Search or Quick Report can now be configured to be emailed on a schedule. Find more information in the [ShowBack and ChargeBack Guide](#).

Beta in this release - 1.1.5-21133/21163

S3 Indexing (meta data only)

Index object names and properties into the search index. Find more information in the Search & Recover Cluster Configuration Guide [here](#).

Coming in a patch release - 1.1.5-21169

Snapshot Mode

Indexing snapshots only - Coming in a patch release

Fixed in this release - 1.1.5-21163

T20473 File Path Selector not working

The File Path Selector in the Advanced Search Criteria does not expand to show all folders.

Resolution: File path selector can now display all folders 20 at a time.

T21026 Incremental Index does not handle Alternate Data Stream (ADS) Files

Incremental Index does not identify changes for Alternate Data Stream (ADS) files and they do not get updated in the index.

Resolution: Search now properly handles add, update, delete of ADS files in the index.

T21259, T21260 What's in the file pools quick reports issues

T21259 Show me the files for the file pools quick report are now working

T21260 Now able to schedule report for file pools quick report

T20501 How fast is my data growing Quick Report may be missing data

Under some circumstances, the How fast is my data growing Quick Report may be missing months in forecast and may not forecast file count correctly.

Resolution: Issue has been addressed.

T21030 Scheduled report test for What's growing old has incorrect results

A scheduled report test for the What's growing old Quick Report has incorrect or no data in the report attachment. Impact is only on the test function, regularly scheduled report does not have this issue.

Resolution: A scheduled report test now contains the expected data.

T21253 Index job does not finish

Under some circumstances, an index job gets stuck while walking the file system.

Resolution: Corner case of file system changes while walk is occurring is now handled.

Fixed in this release - 1.1.5-21133

T9378, T17560 File or Folder rename may return results for both old and new name - files orphaned in search index

When a file or folder has been renamed, search may return results for both the old and new name if search is referencing data that was added with old name.

Resolution: Due to a bug in the PowerScale changelist API for OneFS 8.2.0 and earlier (internal Dell bug #234779), renamed folders and files are not included in the changelist and the index therefore cannot be updated to remove original items. Resolution is now available for OneFS 8.2.1 and higher where PowerScale changelist API identifies renamed folders and files. When indexing a renamed folder or file, the original location/name of folder or file is also removed from the index.

T15808 Advanced Search and Quick Report File Owner filter is not working

A Quick Report or Advanced Search using a File Owner filter does not return any results.

Resolution: Search on other filter which will return File Owner now returns correct results. If File Owner contains a space in the name, quotes must be used around the name - for example "AD02\name"

T13557 CMD Writer file not created when number of rows specified

CMD Writer has option to create file with selected number of rows or with all rows. If the option to select number of rows is used the file will not be created.

Resolution: Now able to create the file with "Number of rows in file" specified.

T13542 Require 2 clicks to see Recover File option

To see the Recover File option in the GUI requires 2 clicks on the file to be recovered. The first click will show the options: Display Details and Copy File Location. The second click will then additionally display the Recover File option.

Resolution: The Recover File option is now available on 1 click.

T15540 Search Email Notification Test Feature not functional

The test function for search email notification is not functional. Regular email notification is not affected.

Resolution: Email test function now working.

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...

An Advanced Search option entered for Last Accessed, Last Modified or Created At and In the last... or Older than.. 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.

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.

Workaround: A full index could be re-run to pick up changes missed by incremental.

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.

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.

Workaround: None available. Plan to address in a patch release.

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.

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.

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.

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.

Workaround: Configure administrator as individual AD users using command searchctl settings
admins add --name [username@domain.com](#) .

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.

Workaround: None available. Planned for fix in patch release.

T21588 File Path Selector is not filtered based on End User Security Configuration

The File Path Selector is exposed to end users but not filtered based on End User Security. This exposes the file system structure to end users.

Workaround: None available. Planned for fix in a patch release.

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.

General

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 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.

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 LLC

1.5. Current Release - Release Notes

Performance Auditor

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

- [What's New in Superna Eyeglass Performance Auditor Release 2.5.7](#)
- [Supported OneFS releases](#)
- [End of Life Notifications](#)
- [Deprecation Notices](#)
- [Technical Advisories](#)
- [New/Enhanced/Fixed in 2.5.7](#)
- [Fixed in 2.5.7.1-21161](#)
 - [NEW - ECA OVF released with configuration files for 1, 3, 6 node deployments on the OpenSUSE 15.3 operating system. All other feature and functionality equivalent to 2.5.7.1-21140.](#)
- [Fixed in 2.5.7.1-21140](#)
- [New/Fixed in 2.5.7-21081](#)
- [New in 2.5.7-21068](#)
 - [New: History View](#)
- [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
- T20097 Performance Auditor History mode is not working in 2.5.7.1
- 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 2.5.7

What's New! In Superna Eyeglass Performance Auditor can be found [here](#).

Supported OneFS releases

8.1.x.x

8.2.x.x

9.0

End of Life Notifications

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

Deprecation Notices

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

Technical Advisories

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

New/Enhanced/Fixed in 2.5.7

Fixed in 2.5.7.1-21161

NEW - ECA OVF released with configuration files for 1, 3, 6 node deployments on the OpenSUSE 15.3 operating system. All other feature and functionality equivalent to 2.5.7.1-21140.

Fixed in 2.5.7.1-21140

Refer to Enhancements/Fixes in previous 2.5.7 versions.

Fixed in 2.5.7-21096

T19467 ECA logs missing from backup on new OVA deployment

ECA OVA missing symbolic link resulted in logs not being included in a backup.

Resolution: OVA symbolic link is now present.

New/Fixed in 2.5.7-21081

Refer to Enhancements/Fixes in previous 2.5.7 versions.

New in 2.5.7-21068

New: History View

Historical cluster node reads, writes and total IO is now available historically in a live graph. Documentation for History View can be found here: [How to Trend cluster IO over time for top cluster nodes](#)

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.

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.

Workaround: None available

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 LLC

1.6. Current Release - Release Notes ECA

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

- [What's New in Superna Eyeglass Easy Auditor Edition and Ransomware Defender Edition](#)
- [Supported OneFS releases](#)
- [End of Life Notifications](#)
- [Deprecation Notices](#)
- [Issues Fixed in this Release](#)
- [New in 2.5.7.1-21161](#)
 - [NEW - ECA OVF released with configuration files for 1, 3, 6 node deployments on the OpenSUSE 15.3 operating system. All other feature and functionality equivalent to 2.5.7.1-21140.](#)
- [New in 2.5.7.1-21140](#)
 - [NEW Health Checks](#)
 - [NEW Disk Space Management](#)
 - [NEW Alarm Management](#)
 - [NEW Default Settings](#)
- [Fixed in 2.5.7-21096](#)
- [T19467 ECA logs missing from backup on new OVA deployment](#)
- [Fixed in 2.5.7-21081/21068](#)
- [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
 - T15457 HTML 5 vmware vcenter bug on OVA deployment
 - T17103 ECA version intermittently reported incorrectly

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 2.5.7

What's New! In Superna Eyeglass Easy Auditor Edition and Ransomware Defender Edition Release 2.5.7 can be found [here](#).

Supported OneFS releases

8.0.0.x

8.0.1.x

8.1.x.x

8.1.2.x

8.1.3.x

8.2.0.x

8.2.1.x

8.2.2.x

9.0

9.1

9.2

Supported Eyeglass releases

Superna Eyeglass ECA Version	Superna Eyeglass Version
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](#).

Deprecation Notices

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

Issues Fixed in this Release

New in 2.5.7.1-21161

NEW - ECA OVF released with configuration files for 1, 3, 6 node deployments on the OpenSUSE 15.3 operating system. All other feature and functionality equivalent to 2.5.7.1-21140.

New in 2.5.7.1-21140

NEW Health Checks

- T17074 Check for issues with the NFS mount used to read the Powerscale audit logs and execute a remount if issue is found.
- T18095 Check for stuck processing in containers responsible for real time analysis and writing audit events to the hdfs database and if found restart containers (fastanalysis and evtarchive)
- T18218 Check for condition where ECA nodes have been powered off without executing cluster down first leaving ECA in non functional state and if found execute a cluster down/up sequence to gracefully stop and start ECA services and containers.

NEW Disk Space Management

- T19123 Turboaudit logs retrieved for rollover processing stored in separate partition with quota
- T19691 Zookeeper ramdisk management interval changed to from 1 hour to 15 minutes

NEW Alarm Management

- T19212 ECA Node Inactive timeout increased to 15 minutes in order to be considered inactive and generate alarm to reduce intermittent false positive notifications.

NEW Security

- T7965 User and password now required to login to management GUI for ECA services: hbase-master, hbase-rs, spark-master, spark-worker, spark-history, kafkahq. Use default user ecaadmin and password set during upgrade to 2.5.7.1.
- T19158 New iptable rules which allow communication on all ports between ECA nodes, within ECA containers themselves and to Eyeglass but all other traffic is limited to port 443 required to use ECA services management GUIs and port 22 for ssh.

NEW Default Settings

- T19109 Turboaudit default event processing rate increased to 30,000

Fixed in 2.5.7-21096

T19467 ECA logs missing from backup on new OVA deployment

ECA OVA missing symbolic link resulted in logs not being included in a backup.

Resolution: OVA symbolic link is now present.

Fixed in 2.5.7-21081/21068

No changes in 2.5.7. Refer to Release 2.5.6 - Release Notes ECA for latest changes

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.

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.

© Superna LLC

1.7. Current Release - Release Notes Golden Copy

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

- [What's New in Superna Eyeglass Golden Copy Release 1.1.6](#)
- [Supported OneFS releases](#)
- [End of Life Notifications](#)
- [Deprecation Notifications](#)
 - [Azure default Tier change](#)
 - [Remove support for OneFS 8.1](#)
- [New in 1.1.6-21152/21164](#)
- [Fixed in 1.1.6-21164](#)
 - [T21357 Export job intermittently not creating the export report](#)
 - [T19357 Export Report not generated for a recall job](#)
 - [T19137 Export report does not report failed and skipped files](#)
- [Fixed in 1.1.6-21152](#)
 - [T21026 Incremental Archive does not handle Alternate Data Stream \(ADS\) Files](#)
 - [T20001 Issue with errors command](#)
 - [T18876 Jobs history deleted after cluster up if s3 stats job run](#)
- [Not available in 1.1.6](#)
 - [T16667 Data Integrity Audit Job](#)
 - [T17181 Archive to AWS Snowball](#)
 - [T17195 Upload to Azure, Cohesity, ECS or Ceph via Proxy](#)

- T16247 DR cluster alias / redirected recall
- Golden Copy beta GUI not supported in this update.
- Known Issues
- Known Issues Archiving
 - T14014 Incremental upload requires 2 cycles before picking up changes
 - T15312 Archive job incorrectly presented as completed
 - T16427 Incremental archive does not run with multiple Powerscale clusters added
 - T16425 Archive incremental upload does not handle changelist in waiting state and incremental fails
 - T16629 Azure upload error where name contains %
 - T17449 Folder missing meta data information for Azure container with legal hold or retention policy
 - T17493 Upload of files and folders fail where owner or group meta-data contains language specific characters
 - 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
- T19387/T20731 Incremental sync does not store folder ACL & clears ACL for parent folder
- T19388 Fast Incremental incorrectly stores UID and GID properties
- T19441 Move/Delete operation in a single incremental sync orphans deleted 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
- T21586 API error stops incremental job
- Known Issues Reporting
 - General Reporting Issues
 - 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
 - T19466 Statistics may show more than 100% archived/attempted after a cluster down/up
 - T21257 The 'file change count' column in jobs running always shows 0 for incremental archive

- T21084 The jobs view and jobs running have inconsistent phases
- T19316 searchctl jobs view does not show the size of errored files for incremental archive
- T20497 The jobs history '--tail' argument not working
- T21572 Export report for folder with multiple jobs may only produce 1 report
- Recall Reporting Issues
- T16960 Rerun recall job overwrites export report
- T17746 Recall reporting issues for metadata only recall
- T17893 searchctl archivedfolders history incorrectly shows recall job as job type FULL
- T18535 Recall reporting issue for accepted file count / interrupted recall
- T18875 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
- 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'
- 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
 - T20175 Beta GUI not available
 - 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
- 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
 - 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

What's New in Superna Eyeglass Golden Copy Release 1.1.6

What's New! In Superna Eyeglass Golden Copy can be found [here](#).

Supported OneFS releases

8.1.x.x

8.2.x.x

9.1.x.x

Supported S3 Protocol Targets

Amazon S3 version 4 of the authentication is supported (details here)

Dell ECS version 2

Azure blob services using S3 version of the authenticated protocol

Cohesity 6.3.1e AWS version 4 signature (ask about other versions) See vendor documentation for versioning support and object retention policy support.

OpenIO - versioning not tested. Requires --meta-prefix when adding folders and value of oo-

Ceph version 15 or later Octopus (aws v4 signature only)

Google Cloud Storage

End of Life Notifications

End of Life Notifications can be found [here](#).

Deprecation Notifications

Azure default Tier change

In next release the default tier for Azure upload will change from cold to hot. Tier specific upload to Azure will require advanced license.

Remove support for OneFS 8.1

Support for OneFS 8.1 will be removed as of February 1, 2022.

New in 1.1.6-21152/21164

- Backup reporting statistics for Backup paths by folder and rollup stats (Advanced License Required)
- Native Cloud provider tier support enhancements (Advanced License Required)
 - Allows copying data directly into the target tier without transition costs between tiers.
- Version Aware recall Enhancements - newer than and older than per object version check to select files based on the closest date match. Supports version aware S3 targets with bucket versioning enabled (Advanced License Required)
- Ransomware Defender Zero Trust Backup API integration to allow zero trust backup. Golden copy checks the threat level on the source data and will block backups if any active alerts. Extends file system real time monitoring to your backups.
- Stats Engine Updates - more detailed break down of file sizes backed up (adv license required). All time roll up of stats on a folder. Stats updates for all license levels.
- Job Engine - Storing of job history is now streamed from a database and more history is available for all folders configured on the system. Filter job history by folder.
- Incremental Isilon v2 API support - Supports 8.2 and later change list api to mirror file system to S3 bucket with all scenarios covered, layer approach ensures order dependent updates are mirrored to the S3 bucket
- Flat file copy - The ability to accept a flat file with files listed anywhere under a managed folder to allow custom copy jobs based on a file list. Use case: build a flat file based on date stamps for backing up files with last accessed older than x months and then scripting the delete of these files using the flat file.

Fixed in 1.1.6-21164

T21357 Export job intermittently not creating the export report

Under some circumstances, the export report does not get created.

Resolution: Export report is now created.

T19357 Export Report not generated for a recall job

Running an export report for a recall jobs shows a job status of SUCCESS but the export summary report is not generated.

Resolution: Export report is now created.

T19137 Export report does not report failed and skipped files

For an archive job where there are failed and skipped files the export report shows 100% success.

Resolution: Export report now reports accurately the errored and skipped files.

Fixed in 1.1.6-21152

T21026 Incremental Archive does not handle Alternate Data Stream (ADS) Files

Incremental archive job does not identify changes to files with Alternate Data Streams and therefore these files are not uploaded as part of incremental job.

Resolution: New, updated and deleted ADS files are now updated in object storage correctly.

T20001 Issue with errors command

If the archivedfolders errors command is used with the tail and count options and the actual number of errors is less than specified in the count option, the errors command will fail.

Resolution: Condition where the tail parameter exceeds the number of errors is now handled.

T21144 Incremental Archive may not complete for job which includes rename operation and Azure target

Incremental archive job to Azure may not complete when the job includes rename operations. The may not finish and/or objects may not be updated.

Resolution: Rename operation now handled.

T18876 Jobs history deleted after cluster up if s3 stats job run

Subsequent cluster down/up after searchctl archivedfolders s3stats command was run deletes all entries in the job history.

Impact is that the job cannot be re-run, cancelled, view job statistics without the job-id from the history.

Resolution: job history is no longer affected by running s3 stats job

Not available in 1.1.6

T16667 Data Integrity Audit Job

Data Integrity Audit Job (searchctl archivedfolders audit) should not be used in this release. It will be removed in future release as it is not intended for the Golden Copy base license.

It will require the advanced Golden Copy license.

T17181 Archive to AWS Snowball

Archive to AWS Snowball is not supported with this optimized update release. This is planned in a coming update.

T17195 Upload to Azure, Cohesity, ECS or Ceph via Proxy

Azure, Cohesity, ECS or Ceph clients using http proxy not supported in this update.

T16247 DR cluster alias / redirected recall

Ability to recall to a different cluster than the original source cluster is not supported in this update.

Golden Copy beta GUI not supported in this update.

Technical Advisories

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

Known Issues

Known Issues Archiving

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.

T16427 Incremental archive does not run with multiple Powerscale clusters added

When multiple Powerscale clusters are added to Golden Copy, incremental archive is blocked and does not run.

Workaround: None available.

T16425 Archive incremental upload does not handle changelist in waiting state and incremental fails

A changelist on the Powerscale which is in waiting state is not handled by Golden Copy incremental archiving which fails the incremental job instead of waiting and applying a timeout.

Workaround: None required - following incremental interval will pick up the changes.

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.

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.

T17493 Upload of files and folders fail where owner or group meta-data contains language specific characters

For all S3 targets except ECS, if a folder or file meta-data for owner or group contains non-ASCII language specific (Unicode) characters, the file or folder upload will fail.

Workaround: None available. Issue only affects files and folders with above configuration. Other files and folders in upload job continue to be processed.

T18012 Folders with language specific characters not uploaded

Folders with language specific characters are not upload 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.

T19387/T20731 Incremental sync does not store folder ACL & clears ACL for parent folder

On incremental sync where a new folder is archived, the associated folder ACLs are not stored with the object properties in S3 target. Also an incremental which includes an update to a file or folder clears the ACL for the parent folder. Note this issue does not affect full archive.

Workaround: None available. Manual process required to track folder ACLs.

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 Move/Delete operation in a single incremental sync orphans deleted data in S3 target

Under certain circumstances where in the same incremental update there is 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.

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.

T21586 API error stops incremental job

Under some conditions, an API error to the Powerscale will stop an incremental job.

Workaround: Contact support.superna.net for assistance.

Known Issues Reporting

General Reporting Issues

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.

T21084 The jobs view and jobs running have inconsistent phases

For an incremental archive job, the searchctl jobs running output last phase is GC_METADATA but the searchctl jobs view shows additional phases including a phase for Data Archive.

Workaround: Use the searchctl jobs view command to see the status of all phases.

T19316 searchctl jobs view does not show the size of errored files for incremental archive

The searchctl jobs view command for an incremental job will show a count for any errored files but will always show size as 0B instead of the actual size of errored files.

Workaround: Use folder stats to see cumulative stats for a folder.

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.

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.

T17746 Recall reporting issues for metadata only recall

Recalling metadata only for a previous recall job using the command: searchctl archivedfolders metadata --jobid has the following issues:

- The resulting job cannot be monitored using the jobs view --follow command. Running the command results in an error if run against a metadata only recall job.
- The jobs history view does not list the metadata only recall jobs.
- Export report has doubled count and errors not reported accurately

Workaround:

Run the jobs view command multiple times to see progress.

Keep a manual record of the metadata only recall 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 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.

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.

Known Issues General & Administration

T14025 Changing PowerScale user requires a cluster down/up

If the iuser 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.

T20175 Beta GUI not available

On Golden Copy 1.1.4-21105 and higher the Beta GUI is not available due to searchmw container restarting.

Workaround: None available. Delivery of the GUI is planned for 1.1.6 Golden Copy.

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.

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 Isilon-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 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.

Fast Incremental Known Limitations

- mode bit meta data 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 not recalled where objects were uploaded with fast incremental due to 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.

© Superna LLC

1.8. Current Release - Release Notes

Ransomware Defender AirGap 2.0

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

- [What's New in Superna Eyeglass Ransomware Defender Edition Release 2.5.7 AirGap 2.0](#)
- [Controlled Availability Ransomware Defender Edition Release 2.5.8 AirGap 2.0](#)
- [Supported OneFS releases](#)
- [Supported Eyeglass releases](#)
- [Inter Release Functional Compatibility](#)
- [End of Life Notifications](#)
- [Deprecation Notices](#)
- [Technical Advisories](#)
- [AirGap Enterprise Controlled Availability](#)
- [NEW AirGap Enterprise Controlled Availability](#)
- [New for AirGap 2.5.8-21213/21222](#)
 - [T19522 AirGap Enterprise](#)
- [New for Ransomware Defender 2.5.8-21213/21222](#)
 - [Ransomware Defender Snapshot Management Enhancements](#)
 - [T15666 New Behaviour Detections Enabled](#)
- [New for DR Edition 2.5.8-21213/21222](#)

- T17849 DNS Dual Delegation disabled
- New for Easy Auditor 2.5.8-21222
 - T19711 Easy Auditor new validation that selected path is on an audited Access Zone
- Fixed in 2.5.8-21222
 - T20770 AirGap Event Retrieval Job Fails with No route to host
 - T21112 Eyeglass log shows vault cluster password in clear text during event retrieval
 - T19619 Critical Path Snapshot not applied to all managed clusters
 - T20668 Cannot save or run query in Report Query Builder
 - T20966 AirGap Job Configuration lost on rediscover or anyrelease restore
 - T20790 AirGap SynclQ policy timeout uses failover timeout setting
 - T20358 Not able to create an AirGap Job Report for a selected period
- Fixed in 2.5.8-21213
 - T20766 Cannot view second page of AirGap Config AirGap job list
 - T11832 Ransomware Security Event which is promoted from Warning to Major does not respect Major Grace Period
 - T20936 Bulk Ingest of Old Audit Data is not functional
- Known Issues in 2.5.8-21222
 - AirGap

- 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
- T20932 AirGap Job Reports do not report failed jobs
- Ransomware Defender
- T21334 Snapshots may not be created
- T21261 Cannot edit a user configured in the Ignored List or Monitor Only Settings
- Easy Auditor
- T21226 Active Auditor Snapshot functionality follows Ransomware Defender Snapshot configuration
- DR Edition
- T21375 Snapshot schedule replication error on update
- General
- T21275 Powerscale cannot be deleted
- Known Limitations in 2.5.8-21222
 - 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
 - T21208 Snapshots taken using Action Menu for Ransomware Defender Event follow Ransomware / Snapshots settings
- Fixed in 2.5.7.1-21140
- Fixed in 2.5.7-21096

- Fixed in 2.5.7-21081
- Fixed in 2.5.7-21068
 - T16196 Eyeglass Backup & Restore does not restore Airgap Settings
- 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
 - T19195, T19221 AirGap Job shows success when failed
 - 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
 - T20766 Cannot view second page of AirGap Config AirGap job list

- [T21134 AirGap Basic Job](#) can be started from Jobs window without AirGap role
- **Known Limitations**
- [T19614 AirGap Job consideration of Easy Auditor Active Auditor Active Event](#) not configurable

What's New in Superna Eyeglass Ransomware Defender Edition Release 2.5.7 AirGap 2.0

What's New! In Superna Eyeglass Ransomware Defender Edition Release 2.5.7 can be found [here](#).

Controlled Availability Ransomware Defender Edition Release 2.5.8 AirGap 2.0

What's New! In Superna Eyeglass Ransomware Defender Edition Release 2.5.8 can be found [here](#).

Controlled Availability release is available for new deployments and upgrades approved by support.

Supported OneFS releases

Source cluster

8.1.2.x

8.1.3.x

8.2.0.x

8.2.1.x

8.2.2.x

Target Airgap Cluster

8.2.2.x

Supported Eyeglass releases

Superna Eyeglass Ransomware Defender Version	Superna Eyeglass Version
2.5.8-21222 Controlled Availability	2.5.8-21222 Controlled Availability
2.5.8-21213 Controlled Availability	2.5.8-21213 Controlled Availability
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
2.5.7-20129	2.5.7-20129

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](#).

Deprecation Notices

Following features will no longer be supported as indicated below:

1. As of Release 2.5.8

a. Support for OneFS 8.1.x.x releases

Technical Advisories

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

AirGap Enterprise Controlled Availability

NEW AirGap Enterprise Controlled Availability

New for AirGap 2.5.8-21213/21222

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](#)

New for Ransomware Defender 2.5.8-21213/21222

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.

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.

T19619 Critical Path Snapshot

Introduced in 2.5.8 (build 21213 and higher) one or more paths can be configured to always have a snapshot created for any detection.

T15666 New Behaviour Detections Enabled

New behaviour detections are available and enabled by default.

NOTE: 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.

New for DR Edition 2.5.8-21213/21222

T17849 DNS Dual Delegation disabled

Access Zone Failover Readiness DNS Dual Delegation is now disabled by default.

Workaround: None required. Verify DNS Dual Delegation manually. In future release this validation is planned to be provided on demand.

New for Easy Auditor 2.5.8-21222

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 2.5.8-21222

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 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 ability to failover.

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

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](#).

T21112 Eyeglass log shows vault cluster password in clear text during event retrieval

The Eyeglass logs show the vault cluster password in clear text during event retrieval.

Resolution: Password is now redacted.

T19619 Critical Path Snapshot not applied to all managed clusters

If multiple clusters are managed by Ransomware Defender, a configured critical path snapshot is only created on the cluster where the suspicious behaviour was detected. This issue is for critical path snapshots only. Regular user snapshots continue to be taken on all managed clusters.

Resolution: Critical path snapshot now created on applicable clusters.

T20668 Cannot save or run query in Report Query Builder

Clicking Save Query As or Run Report Using Query for Easy Auditor Report Query Builder has no effect. The query is not saved or run. This does not affect other Easy Auditor menus.

Resolution: Query can now be saved and run.

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.

Resolution: AirGap Job configuration preserved on rediscover or anyrelease restore.

T20790 AirGap SyncIQ policy timeout uses failover timeout setting

The amount of time that RansomwareDefender will wait for an AirGap SyncIQ 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 SyncIQ policy to complete, the AirGap job will timeout and remove the static routes causing the AirGap SyncIQ 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 SyncIQ 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.

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.

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.

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.

Known Issues in 2.5.8-21222

For complete list of known issues please also refer to current release notes:

- [AirGap Current Release Notes](#)
- [Ransomware Defender Release Notes](#)
- [Easy Auditor Release Notes](#)
- [DR Edition Release Notes](#)

AirGap

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.

T20932 AirGap Job Reports do not report failed jobs

AirGap Job reports that are sent out by schedule or created manually do not report on failed jobs. Failed jobs always shows 0.

Workaround: Alarms must be monitored to be advised of failed jobs. Job history can also be reviewed for failed jobs.

Ransomware Defender

T21334 Snapshots may not be created

In some cases, Ransomware Defender snapshots are not created for an active event when they should have been. In the Event History the snapshot step states: No snapshots were created.

Workaround: Contact support.superna.net for assistance.

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.

Workaround: Delete and readd user to the list.

Easy Auditor

T21226 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.

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.

DR Edition

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.

General

T21275 Powerscale cannot be deleted

A Powerscale cluster that has been added into Eyeglass cannot be deleted. The delete function results in an error: Error when submitting job to remove network element. Cannot locate network element with id:

Workaround: Contact support.superna.net for assistance.

Known Limitations in 2.5.8-21222

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.

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.

Fixed in 2.5.7.1-21140

Refer to previous 2.5.7 fixes/enhancements.

Fixed in 2.5.7-21096

Refer to previous 2.5.7 fixes/enhancements.

Fixed in 2.5.7-21081

Refer to previous 2.5.7 fixes/enhancements.

Fixed in 2.5.7-21068

T16196 Eyeglass Backup & Restore does not restore Airgap Settings

An Eyeglass backup & restore operation will not restore Airgap settings.

Resolution: Airgap settings now backed up and restored.

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.

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.

Workaround:

The AirGap Reports would indicate that less than expected number of SynclQ jobs had run/succeeded.

The PowerScale reporting for the AirGap SynclQ policy can be used.

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 SyncIQ job.

Workaround: Check on Powerscale directly to confirm that AirGap SyncIQ 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.

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.

Workaround: Use Powerscale native reporting tools for SyncIQ jobs to view jobs for a specific timeframe.

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.

Workaround: Sort the the AirGap job list by policy name after which switching between pages displays all policies.

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.

Workaround: In Eyeglass use a node IP from the System Access Zone that corresponds to a different interface of a node that is configured in the AirGap pool.

T20790 AirGap SyncIQ policy timeout uses failover timeout setting

The amount of time that RansomwareDefender will wait for an AirGap SyncIQ 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 SyncIQ policy to complete, the AirGap job will timeout and remove the static routes causing the AirGap SyncIQ job to fail with an incomplete update to the vault copy of the data.

Workaround: If the AirGap SyncIQ policy requires more time to complete the /opt/superna/sca/data/system.xml failovertimeout setting must be increased to required time (in minutes) and then the main Eyeglass sca

service must be restarted. Impact: This setting is shared by failover timeout. Changing this setting will also change the time that Eyeglass DR Edition will wait for SyncIQ related failover steps to complete and could increase failover time for failover where timeout applies. Plan in future release to have separate setting for AirGap and DR Edition.

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.

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.

1.9. Current Release - Release Notes AnyCopy

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

Current Release - Release Notes AnyCopy

- [Supported OneFS releases](#)
- [Supported Eyeglass releases](#)
- [Inter Release Functional Compatibility](#)
- [End of Life Notifications](#)
- [Technical Advisories](#)
- [Fixed in 2.5.7](#)
- [Fixed in 2.5.7-21096](#)
- [Fixed in 2.5.7-21081](#)
- [Fixed in 2.5.7-21068](#)
- [T15987 Share Deny All Permission does not block creation of AnyCopy Job](#)
- [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
- 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 2.5.7 - please refer to release list [here](#)

Inter Release Functional Compatibility

	Source	Target
AnyCopy Job	8.2.1.0 and higher 8.2 versions	8.2.1.0 and higher 8.2 versions

End of Life Notifications

End of Life Notifications are published [here](#).

Technical Advisories

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

Fixed in 2.5.7

Fixed in 2.5.7-21096

Refer to fixes/enhancements in previous 2.5.7 versions.

Fixed in 2.5.7-21081

Refer to fixes/enhancements in previous 2.5.7 versions.

Fixed in 2.5.7-21068

T15987 Share Deny All Permission does not block creation of AnyCopy Job

AnyCopy Jobs can be created for shares with Everyone Deny All permission or by a user for a share where they specifically have a Deny All permission.

Resolution: Share with Deny All permission for the logged in user are no longer listed as an option for creating an AnyCopy job.

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 SyncIQ job was preserved, the last run for the job can be verified from the Powerscale native interface.

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 SyncIQ policy name rules. An invalid name causes the AnyCopy Job to fail at the step where the SyncIQ policy is created.

Workaround: AnyCopy Job names must be compliant with SyncIQ 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 LLC

1.10. Release 2.5.8 - Release Notes

Ransomware Defender for ECS

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

- [What's New in Superna Eyeglass Ransomware Defender for ECS - Release 2.5.8](#)
- [Supported ECS releases](#)
- [End of Life Notifications](#)
- [Technical Advisories](#)
- [Build Version: 2.5.8-21189 - First release](#)
- [Known Issues](#)
 - [T17777 ECS bucket versioning option not working](#)
 - [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](#)
 - [T20753 Error in Manage Services for vaultagent](#)
 - [T20775 Edit ECS Username or Password results in issue with displaying Inventory](#)
 - [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 2.5.8

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
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

3.5

3.6

End of Life Notifications

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

Technical Advisories

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

Build Version: 2.5.8-21189 - First release

Known Issues

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.

Workaround: If there is a business requirement for versioning this will need to be configured on the ECS directly.

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

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.

Workaround: Contact support.superna.net to update configuration so that vaultagent is removed from component list.

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`

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 LLC

1.11. Release 1.1.2 - Search and Recover

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

- [What's New in Superna Eyeglass Search and Recover](#)
- [Supported OneFS releases](#)
- [End of Life Notifications](#)
- [Fixed in this release - 1.1.2-20024](#)
 - [T14119 Enhancement to initial file system tree walk](#)
 - [T14361 Incremental index should use snapshot alias for content indexing](#)
 - [T14433 Too may read operations by solr](#)
 - [T13663 Search initial index stops on unknown exception](#)
 - [T11762 Extra changelist jobs initiated when snapshot mode is enabled](#)
 - [T13331 manual commit for indexed files does not commit files indexed in snapshots](#)
 - [T13513 Recover File dialog Last Modified on is incorrect](#)
 - [T13286 SNAPSHOTMONITOR folder stats issues](#)
 - [T13553 CMD Writer option for csv download does not respect search criteria](#)
- [Fixed in this release - 1.1.2-19104](#)
 - [T11849 Quick Reports Average File Size may not be accurate](#)
- [Searching](#)
 - [T9378 File or Folder rename may return results for both old and new name](#)

- 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...
- 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
- T13557 CMD Writer file not created when number of rows specified
- T13611 User search does not work for all clusters for multi-cluster deployment
- T158080 Advanced Search and Quick Report File Owner filter is not working
- T16425 Search incremental index does not handle changelist in waiting state and incremental fails
- T17392 ZoneUNC not displayed properly for multiple clusters
- T17560 Renamed Folders and Files orphaned in search index
- File Recover
 - T13292 Recover File in error when file name selected contains non US-ASCII characters
 - T13542 Require 2 clicks to see Recover File option
 - 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
 - T16115 Admin Only Login Mode allows user login and search
 - 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
- T15540 Search Email Notification Test Feature not functional
- 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
- 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](#)

These Release Notes cover the Superna Eyeglass Search and Recover product.

What's New in Superna Eyeglass Search and Recover

Release 1.1.2

What's New! In Superna Eyeglass Search and Recover can be found [here](#).

Supported OneFS releases

8.0.0.x

8.0.1.x

8.1.x.x

8.2.x.x

9.1.x.x

9.2.x.x

End of Life Notifications

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

Fixed in this release - 1.1.2-20024

T14119 Enhancement to initial file system tree walk

Enhancement to improve performance of initial tree walk.

T14361 Incremental index should use snapshot alias for content indexing

In large environment with high change rate, snapshot used for content indexing may expire before indexing is done.

Resolution: Refer to snapshot using snapshot alias.

T14433 Too may read operations by solr

Ratio of read to write for solr during indexing seen to be too high in some environments.

Resolution: solr memory configuration modified to resolve this issue.

Fixed in this release - 1.1.2-19108

T13663 Search initial index stops on unknown exception

Search initial index would stop due to an unknown exception and mark the job as SUCCESS.

Resolution: Search initial index now continues on error and correctly identifies the error.

Fixed in this release - 1.1.2-19105

T11762 Extra changelist jobs initiated when snapshot mode is enabled

When snapshot mode is configured, a changelist job is initiated on the PowerScale at the Search & Recover incremental ingestion schedule setting (default 1 hour) instead of the snapshot schedule. This results in additional changelist jobs running on the PowerScale but no additional indexing on the Eyeglass Search Appliance.

Resolution: Extra changelist jobs no longer initiated.

T13331 manual commit for indexed files does not commit files indexed in snapshots

The searchctl solr commit does not commit files indexed from snapshots.

Resolution: Command now also commits files indexed from snapshots

T13513 Recover File dialog Last Modified on is incorrect

The Recover File dialog displays the "Last Modified on" time for file being recovered but may incorrectly display the day, date or time.

Resolution: Recover File dialog now correctly displays the Last Modified time.

T13286 SNAPSHOTMONITOR folder stats issues

Some SNAPSHOTMONITOR stats such as FILES_ACCEPTED do not have a separate count and instead are added towards INCREMENTAL stats. Also the SNAPSHOTMONITOR/FILES_CONTENT_INDEXED stat is not required.

Resolution: Snapshotmonitor stats are now correct.

T13553 CMD Writer option for csv download does not respect search criteria

Download to csv from cmd writer feature results in file that does not respect search criteria returning some results that do not match criteria. Any commands entered will be applied against all files including those that fell outside the search.

Resolution: Proper filters are now applied.

Fixed in this release - 1.1.2-19104

T11849 Quick Reports Average File Size may not be accurate

The Average File Size in Quick Reports may not be accurate.

Resolution: Correct average size is now accurate.

Technical Advisories

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

Known Issues

Searching

T9378 File or Folder rename may return results for both old and new name

When a file or folder has been renamed, search may return results for both the old and new name if search is referencing data that was added with old name.

Workaround: None available

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...

An Advanced Search option entered for Last Accessed, Last Modified or Created At and In the last... or Older than.. 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.

T13557 CMD Writer file not created when number of rows specified

CMD Writer has option to create file with selected number of rows for with all rows. If the option to select number of rows is used the file will not be created.

Workaround: Use the Create for All to create the file and editor to further filter the file as required.

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.

T158080 Advanced Search and Quick Report File Owner filter is not working

A Quick Report or Advanced Search using a File Owner filter does not return any results.

Workaround: Search on other filter which will return File Owner which can then be assessed for required owner.

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

T17560 Renamed Folders and Files orphaned in search index

Due to bug in PowerScale changelist API for OneFS 8.2.0 and earlier (internal Dell bug# 234779), renamed folders and files are not reported resulting in files and folders in old location orphaned in the index. This could lead to additional counts in reports due to duplicated records.

Workaround: Reports can be run with a path filter using new path to avoid orphaned records. This bug is fixed as of OneFS 8.2.1 and planned to be included in next Search release to manage index updates.

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.

T13542 Require 2 clicks to see Recover File option

To see the Recover File option in the GUI requires 2 clicks on the file to be recovered. The first click will show the options: Display Details and Copy File Location. The second click will then additionally display the Recover File option.

Workaround: None required.

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.

T16115 Admin Only Login Mode allows user login and search

With Admin Only Login Mode configured and AD Groups configured as administrator non-admin user (users not in AD group) login and searching is incorrectly still allowed.

Workaround: Configure administrator as individual AD users using command `searchctl settings admins add --name username@domain.com .`

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.

T15540 Search Email Notification Test Feature not functional

The test function for search email notification is not functional. Regular email notification is not affected.

Workaround: Monitor email for regular email notification to verify email is functioning.

General

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 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.

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.

© Superna LLC

1.12. Release 1.1.4 - Golden Copy

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

- [What's New in Superna Eyeglass Golden Copy Release 1.1.4](#)
- [Supported OneFS releases](#)
- [End of Life Notifications](#)
- [Deprecation Notifications](#)
 - [Azure default Tier change](#)
- [Fixed in 1.1.4-21124](#)
 - [T20857 Large changelist handling](#)
- [Fixed in 1.1.4-21119](#)
 - [T20688 Large changelist handling](#)
- [Fixed in 1.1.4-21108](#)
 - [T20266 Incremental changelist handling enhancement](#)
- [Fixed in 1.1.4-21107](#)
 - [T20266 Incremental Archive job gets stuck](#)
- [New/Fixed in 1.1.4-21105](#)
 - [T16450 searchctl jobs view incorrect](#)
 - [T18092 Files have wrong permission after initial cluster up for multi-node Golden Copy deployment](#)
 - [T19130 Cannot rerun for errors from incremental job](#)
 - [New - T19766 Prioritize Incremental Archive Jobs](#)
 - [New - T19768 Slow initial treewalk based on upload lag](#)

- T19436, T19480 File/Folder mode bit meta data not recalled correctly
- T19435 Recall of empty folder does not have owner/group meta data applied
- New/Fixed in 1.1.4-21074
 - New - T18492 Fast Incremental
 - T16368 Recall of folder ACLs
 - T17560 Renamed Folders and Files orphaned in S3 target
 - T18396 / T18880 Manual incremental job results in 2 running jobs
 - T19129 rerun job does not exit
 - New - T17155 Recall
 - New - T17490 Google Cloud Storage (GCE) Support
 - New - T18499 Security update to reduce impact of CVE-2020-25684, CVE-2020-25685, and CVE-2020-25686
 - New - T18077 searchctl archived folders archive has new --follow flag
 - New - T17475 Golden Copy Beta GUI
 - T17677 Load balancing for ECS nodes not available
 - T18164 Empty archive folder blocks all archive jobs
 - T18064 Archive rerun job does not upload errored files
 - T15689 Command to manually initiate an incremental upload does not run
 - T18007 Export report hangs

- T18275 Jobs marked as completed while it is still running
- T17200 PowerScale and Archive Folder configuration gone after Golden Copy Power Off/On
- T15758 Unable to restore Golden Copy configuration to a new VM
- T18113 Additional steps required to shape bandwidth of archive jobs
- Not available in 1.1.4-21062/21074
 - T16667 Data Integrity Audit Job
 - T17181 Archive to AWS Snowball
 - T17195 Upload to Azure, Cohesity, ECS or Ceph via Proxy
 - T18090 Azure option to specify tier for data copy
- New/Fixed in 1.1.4-21002
 - New: T18032 Improved Upload Performance
 - New: 6 node Golden Copy Deployment
 - New: T16242 Authenticated login log (Pending Testing)
 - T17991 Record reprocessing & parallel jobs
 - T15810 Archive job affected by external issues
 - T17155 Recall of files from S3 target using Golden Copy
- Technical Advisories
- Known Issues Archiving
 - T14014 Incremental upload requires 2 cycles before picking up changes
 - T15312 Archive job incorrectly presented as completed

- T16427 Incremental archive does not run with multiple Powerscale clusters added
- T16425 Archive incremental upload does not handle changelist in waiting state and incremental fails
- T16629 Azure upload error where name contains %
- T17449 Folder missing meta data information for Azure container with legal hold or retention policy
- T17493 Upload of files and folders fail where owner or group meta-data contains language specific characters
- 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
- T19387/T20731 Incremental sync does not store folder ACL & clears ACL for parent folder

- T19388 Fast Incremental incorrectly stores UID and GID properties
- T19441 Move/Delete operation in a single incremental sync orphans deleted data in S3 target
- T20379 Canceled archive job continues upload
- T21026 Incremental Archive does not handle Alternate Data Stream (ADS) Files
- Known Issues Reporting
 - General Reporting Issues
 - 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
 - T18876 Jobs history deleted after cluster up if s3 stats job run
 - T19137 Export report does not report failed and skipped files
 - T19466 Statistics may show more than 100% archived/attempted after a cluster down/up
 - T20001 Issue with errors command
 - Recall Reporting Issues
 - T16960 Rerun recall job overwrites export report
 - T17746 Recall reporting issues for metadata only recall
 - T17893 searchctl archivedfolders history incorrectly shows recall job as job type FULL

- T18535 Recall reporting issue for accepted file count / interrupted recall
- T18875 Recall stats may incorrectly show errored count
- T19357 Export Report not generated for a recall job
- T19415 Recall stats incorrectly show errors for folder object which store ACLs
- 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
- 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
- T20175 Beta GUI not available
- 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
- 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

What's New in Superna Eyeglass Golden Copy Release 1.1.4

What's New! In Superna Eyeglass Golden Copy can be found [here](#).

Supported OneFS releases

8.1.x.x

8.2.x.x

9.1.x.x

Supported S3 Protocol Targets

Amazon S3 version 4 of the authentication is supported (details here)

Dell ECS version 2

Azure blob services using S3 version of the authenticated protocol

Cohesity 6.3.1e AWS version 4 signature (ask about other versions) See vendor documentation for versioning support and object retention policy support.

OpenIO - versioning not tested. Requires --meta-prefix when adding folders and value of oo-

Ceph version 15 or later Octopus (aws v4 signature only)

Google Cloud Storage

End of Life Notifications

End of Life Notifications can be found [here](#).

Deprecation Notifications

Azure default Tier change

In next release the default tier for Azure upload will change from cold to hot. Tier specific upload to Azure will require advanced license.

Fixed in 1.1.4-21124

T20857 Large changelist handling

Further enhancements and robustness for handling incremental archive with large changelist.

Fixed in 1.1.4-21119

T20688 Large changelist handling

Enhancement with additional robustness for handling incremental archive with large changelist.

Fixed in 1.1.4-21108

T20266 Incremental changelist handling enhancement

Better handling of cluster changelist resource management for concurrent incrementals.

Fixed in 1.1.4-21107

T20266 Incremental Archive job gets stuck

Incremental Archive job may get stuck when the job has an extremely low change rate or no change rate at all.

Resolution: Update to incremental archive to handle low change rate / no change rate incremental updates.

New/Fixed in 1.1.4-21105

Fixed

T16450 searchctl jobs view incorrect

Under some circumstances, jobs view will have the incorrect stats. For example jobs view may show more than 100% for files attempted and archived.

Resolution: Percentage completion does not go over 100%

T18092 Files have wrong permission after initial cluster up for multi-node Golden Copy deployment

After first cluster up some configuration files have the wrong permission which causes archiving to only be done from node 1.

Resolution: Configuration file now have correct permissions.

T19130 Cannot rerun for errors from incremental job

The rerun job does not identify errors from an incremental job and cannot be used to reupload those files.

Resolution: rerun job can now be used to reuploaded errored files from an incremental job.

New/Fixed in 1.1.4-21093

New

New - T19766 Prioritize Incremental Archive Jobs

For the case where full and incremental archive jobs are running concurrently, resources will be prioritized for the incremental job.

New - T19768 Slow initial treewalk based on upload lag

Monitor the upload lag and adjust the initial treewalk to not exceed configured retention.

Note: requires additional configuration - contact support.superna.net for assistance.

Fixed

T19436, T19480 File/Folder mode bit meta data not recalled correctly

On recall of files and folder from object storage to PowerScale, the file and folder mode bits are not restored. Files/folders have no read/write/execute permissions.

Resolution: File/Folder mode bit are now recalled.

T19435 Recall of empty folder does not have owner/group meta data applied

Empty folders that are recalled do not have the owner and group meta data applied. This may result in Powerscale root user mapping settings on the NFS export used to mount the recall directory being applied.

Resolution: Empty folder owner/group are now applied.

New/Fixed in 1.1.4-21074

New

New - T18492 Fast Incremental

For large changelist a fast incremental mode is now available that takes owner and group meta-data provided in changelist instead of making a separate API call to PowerScale to retrieve the meta-data. This feature is available for OneFS 8.2.1 and higher as it requires the newer API version available with these releases. This mode requires additional configuration to enable it - contact support.superna.net for assistance.

Known Limitations:

- mode bit meta data information is not available in fast incremental mode
- owner and group are stored in numeric UID and GID format in the object header
- API only available for OneFS 8.2.1 and higher

Fixed

T16368 Recall of folder ACLs

Recall of folder ACLs is now available as of 1.1.4-21074. Original folder ACLs are stored in S3 target and can be reviewed there. On recall folder ACLs are applied against the folder on PowerScale. To enable ACL recall requires an additional configuration - contact support.superna.net for assistance.

T17560 Renamed Folders and Files orphaned in S3 target

Due to bug in PowerScale changelist API for OneFS 8.2.0 and earlier (internal Dell bug# 234779), renamed folders and files are not reported resulting in files and folders in old location orphaned in the S3 target. This could lead to additional counts in S3 due to duplicated records.

Resolution: Golden Copy can now be configured to use the PowerScale changelist API for OneFS 8.2.1 and higher which identifies renamed folders and files. In this configuration, the original folder/file is deleted from S3 target and object is archived in it's new location.

T18396 / T18880 Manual incremental job results in 2 running jobs

Starting a manual incremental job results in 2 running jobs. The Isilon Incremental Archive job is a parent job. The actual incremental job is tracked by the second incremental archive - <uuid> job. Jobs view should be run against the incremental archive - <uuid> job to track the incremental progress. Jobs view against the Incremental Archive job results in an error.

Resolution: Only 1 job is displayed now for manual incremental which is the active job.

T19129 rerun job does not exit

The rerun job to upload errored files after an archive job does not exit after all of the files identified for the job have been uploaded.

Resolution: Job now terminates once completed without any manual intervention.

New/Fixed in 1.1.4-21062

New

New - T17155 Recall

Recall of files from S3 target of all archived files or a sub-directory of archived files to a staging area on same PowerScale cluster is now available. Documentation on Recall and it's supported options can be found [here](#) in the section "How to Recall Data from Object Back to File".

New - T17490 Google Cloud Storage (GCE) Support

Support for archive to Google Cloud Storage (GCE) is now available. Golden Copy for Google Cloud Storage documentation can be found [here](#) in the section "Archiving to Google Cloud Storage".

New - T18499 Security update to reduce impact of CVE-2020-25684, CVE-2020-25685, and CVE-2020-25686

dnsmasq cache disabled to reduce impact from CVE-2020-25684, CVE-2020-25685, and CVE-2020-25686.

New - T18077 searchctl archived folders archive has new --follow flag

Command to start archive job searchctl archived folders archive now has a --follow option which will open the jobs view after starting the job to more easily monitor progress of the newly started job.

New - T17475 Golden Copy Beta GUI

The Golden Copy and Archived Folder Beta GUI is now available.

Fixed

T17677 Load balancing for ECS nodes not available

The option to set load balancing of Golden Copy requests to multiple ECS nodes is not available in current release.

Resolution: Golden Copy can load balance archive across multiple ECS nodes using the --endpoint-ips option in this build.

T18164 Empty archive folder blocks all archive jobs

If an empty folder is added to Golden Copy and an archive jobs is started on that folder, that archive job will hang and block all other archive jobs.

Resolution: Empty folder added as archive job folder no longer hangs when the job is started.

T18064 Archive rerun job does not upload errored files

The rerun job to upload errored files can be started but no files are uploaded.

Resolution: Rerun job is working and able to be used to upload errored files from a completed archive job.

T15689 Command to manually initiate an incremental upload does not run

The command `searchctl archivedfolders archive --incremental` encounters an error which prevents it from running.

Resolution: Incremental archive job can now be initiated by using the `--incremental` option as documented [here](#) in the section "How to start a Full or Incremental Archive Job".

T18007 Export report hangs

Export report job can be started but never finishes.

Resolution: Export job is now able to run and finish.

T18275 Jobs marked as completed while it is still running

Under certain circumstances a job may be incorrectly identified as completed and marked as success when in fact it is still running.

Resolution: Job now correctly reports running and completed status.

T17200 PowerScale and Archive Folder configuration gone after Golden Copy Power Off/On

After power Off/On of the Golden Copy VM, when Golden Copy comes back up previously added clusters and folders are no longer configured.

Resolution: After a power Off/On, run the following commands to restore prior configuration:

```
ecactl cluster down
```

```
ecactl cluster up
```

T15758 Unable to restore Golden Copy configuration to a new VM

The `ecactl cluster restore` command runs but does not actually restore any of the Golden Copy configuration to the new VM.

Resolution: Backup & restore operations now restore:

- licensing
- clusters added
- archive folders added & definitions
- `eca-evn-common.conf` custom settings

Job history and reports are not restored.

For a multi-node deployment, restore will be done to node 1 and remaining nodes deployed as new OVF.

T18113 Additional steps required to shape bandwidth of archive jobs

Additional configuration required to the steps documented [here](#) to shape bandwidth of archive jobs.

Resolution: Additional steps are no longer required. Steps as documented can be used to shape bandwidth usage for archive jobs.

Not available in 1.1.4-21062/21074

T16368 Recall of folder ACLs (applies to 1.1.4-21062 only)

Recall of folder ACLs is not available in this release. Original folder ACLs are stored in S3 target and can be reviewed there.

T16667 Data Integrity Audit Job

Data Integrity Audit Job (`searchctl archivedfolders audit`) should not be used in this release. It will be removed in future release as it is not intended for the Golden Copy base license.

It will require the advanced Golden Copy license.

T17181 Archive to AWS Snowball

Archive to AWS Snowball is not supported with this optimized update release. This is planned in a coming update.

T17195 Upload to Azure, Cohesity, ECS or Ceph via Proxy

Azure, Cohesity, ECS or Ceph clients using http proxy not supported in this update.

T18090 Azure option to specify tier for data copy

The option to specify the Azure tier that is target of upload should not be used. It will be removed in future release as it is not intended for the Golden Copy base license. It will require the advanced Golden Copy license.

New/Fixed in 1.1.4-21002

New

New: T18032 Improved Upload Performance

Build 1.1.4-21002 comes with improved upload performance.

New: 6 node Golden Copy Deployment

Golden Copy can now be deployed as a 6 node cluster for increased archive performance.

New: T16242 Authenticated login log (Pending Testing)

A log that makes available a record of authenticated login to Golden Copy.

Fixed

T17991 Record reprocessing & parallel jobs

Single or parallel archive jobs may queue files multiple times for upload. Files appear multiple times in the queue are not re-uploaded but marked as skipped.

Resolution: Management of the archive queue updated to avoid files being added to queue multiple times. This fix also provides support for parallel archive jobs up to a maximum of 3.

T17182, T17692 Rate limiting for multi node deployments

Rate limiting cannot be applied to Golden Copy VMs in a multi node Golden Copy deployment as it will cause issues such as rearchiving of files.

Resolution: Golden Copy now has a traffic shaping capability for bandwidth management by coordinating file upload so that over time the bandwidth would average out to the desired rate. As such at any point in time the bandwidth usage may exceed the setting for short bursts based on infrastructure bandwidth capabilities. Additional information for this feature is available [here](#). This solution applies to single and multi-VM deployments.

T15810 Archive job affected by external issues

Upload archive job under certain conditions external to Golden Copy such as persistent sustained networking issues, permission issues or DNS resolution issues will continue to process files for upload that result in errored uploads for those files. The job automatically resumes once the external condition has been resolved. In this case stats may not properly reflect failed files.

Resolution: External issue handling has been improved.

Not available in 1.1.4-21002

T17155 Recall of files from S3 target using Golden Copy

This is planned in a coming update. Files continue to be able to be recalled using native S3 tools.

T17181 Archive to AWS Snowball

Archive to AWS Snowball is not supported with this optimized update release. This is planned in a coming update.

T17195 Upload to Azure, Cohesity, ECS or Ceph via Proxy

Azure, Cohesity, ECS or Ceph clients using http proxy not supported in this update.

Golden Copy and Archived Folder GUI view not available

Technical Advisories

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

Known Issues

Known Issues Archiving

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.

T16427 Incremental archive does not run with multiple Powerscale clusters added

When multiple Powerscale clusters are added to Golden Copy, incremental archive is blocked and does not run.

Workaround: None available.

T16425 Archive incremental upload does not handle changelist in waiting state and incremental fails

A changelist on the Powerscale which is in waiting state is not handled by Golden Copy incremental archiving which fails the incremental job instead of waiting and applying a timeout.

Workaround: None required - following incremental interval will pick up the changes.

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.

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.

T17493 Upload of files and folders fail where owner or group meta-data contains language specific characters

For all S3 targets except ECS, if a folder or file meta-data for owner or group contains non-ASCII language specific (Unicode) characters, the file or folder upload will fail.

Workaround: None available. Issue only affects files and folders with above configuration. Other files and folders in upload job continue to be processed.

T18012 Folders with language specific characters not uploaded

Folders with language specific characters are not upload 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.

T19387/T20731 Incremental sync does not store folder ACL & clears ACL for parent folder

On incremental sync where a new folder is archived, the associated folder ACLs are not stored with the object properties in S3 target. Also an incremental which includes an update to a file or folder clears the ACL for the parent folder. Note this issue does not affect full archive.

Workaround: None available. Manual process required to track folder ACLs.

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 Move/Delete operation in a single incremental sync orphans deleted data in S3 target

Under certain circumstances where in the same incremental update there is 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.

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.

T21026 Incremental Archive does not handle Alternate Data Stream (ADS) Files

Incremental archive job does not identify changes to files with Alternate Data Streams and therefore these files are not uploaded as part of incremental job.

Workaround: None available. Plan to address indexing of main data stream in patch release.

T21144 Incremental Archive may not complete for job which includes rename operation and Azure target

Incremental archive job to Azure may not complete when the job includes rename operations. The may not finish and/or objects may not be updated.

Workaround: None available. Plan to address in patch release.

Known Issues Reporting

General Reporting Issues

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.

T18876 Jobs history deleted after cluster up if s3 stats job run

Subsequent cluster down/up after searchctl archivedfolders s3stats command was run deletes all entries in the job history.

Impact is that the job cannot be re-run, cancelled, view job statistics without the job-id from the history.

Workaround: Folder stats are available for summary view of archive statistics for a folder.

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

T19137 Export report does not report failed and skipped files

For an archive job where there are failed and skipped files the export report shows 100% success.

Workaround: The jobs view command for the archive job does correctly report on the errored and skipped files.

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.

T20001 Issue with errors command

If the archivedfolders errors command is used with the tail and count options and the actual number of errors is less than specified in the count option, the errors command will fail.

Workaround: Use the errors command without the tail option to see errors if less than 10, otherwise specify a lower count option.

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.

T17746 Recall reporting issues for metadata only recall

Recalling metadata only for a previous recall job using the command: `searchctl archivedfolders metadata --jobid` has the following issues:

- The resulting job cannot be monitored using the jobs view `--follow` command. Running the command results in an error if run against a metadata only recall job.
- The jobs history view does not list the metadata only recall jobs.
- Export report has doubled count and errors not reported accurately

Workaround:

Run the jobs view command multiple times to see progress.

Keep a manual record of the metadata only recall 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 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.

T19357 Export Report not generated for a recall job

Running an export report for a recall jobs shows a job status of SUCCESS but the export summary report is not generated.

Workaround: Use the jobs view command for details of the recall job.

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.

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.

Known Issues General & Administration

T14025 Changing PowerScale user requires a cluster down/up

If the iuser 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.

T20175 Beta GUI not available

On Golden Copy 1.1.4-21105 and higher the Beta GUI is not available due to searchmw container restarting.

Workaround: None available. Delivery of the GUI is planned for 1.1.6 Golden Copy.

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 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 enabled, 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.

Fast Incremental Known Limitations

- mode bit meta data 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 not recalled where objects were uploaded with fast incremental due to 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/renamed 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.

© Superna LLC

1.13. Release 2.5.6 - Release Notes DR Edition

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

- [What's New in Superna Eyeglass PowerScale Edition Release 2.5.6](#)
- [Supported OneFS releases](#)
- [DR Edition Feature Release Compatibility](#)
- [Feature Support Matrix](#)
- [End of Life Notifications](#)
- [Support Removed in Eyeglass Release 2.5.6](#)
- [Deprecation Notices](#)
- [Issues Fixed in Eyeglass Release 2.5.6](#)
- [Enhancements and Fixes in 2.5.6-20263](#)
- [OneFS Version Support](#)
 - [New: T17099 OneFS 9.1 Support](#)
- [Configuration Replication](#)
 - [T15639 Error replicating AD Group Run as Root SMB Share permissions](#)
- [Failover](#)
 - [New: T16448 Zone/Pool Readiness DNS Dual Delegation Validation SSIP reachability check removed](#)
 - [New: T16455 Zone/Pool Readiness AD SPN Delegation Validation Configurable Delay between create and delete test](#)
 - [New: T16564 Zone/Pool Readiness AD SPN Delegation Validation Retry](#)

- New: T16597 New settings for DNS Dual Delegation
- New: T16747 Zone/Pool Readiness AD SPN Delegation Validation Logging Enhancement
- New: T16949 DR Rehearsal Mode available for OneFS 9.0, 9.1
- T15111 DR Rehearsal Enable incorrectly results in REHEARSAL_ERROR status when failover includes AUTOSKIPCONFIG type jobs
- T15249 Post Failover script runs even if failover fails
- T15628 Zone/Pool Readiness in DR Dashboard not updated when source cluster is unreachable
- T15830, T17232 OneFS 9.0 Known Limitations with Eyeglass
- Features
 - New: Unlock My Files Enhancements
 - New: Quota Search
 - T11882/T14354 Storage Monitor Report - UserGroupQuotasReport is empty
 - T9621, T14813: Unable to break lock for filenames/path with special characters
 - T16555 Unlock My Files incorrectly reports Error when unlocking file
- General
 - New: RBAC 2.0
 - T15280 Web widgets: Embeddable Widgets functionality Deprecated

- T16683 Phone Home Dedicated Log
- T16955 ssh command issued as part of daily Eyeglass backup
- New: T15063 Failover Readiness Date-Time Validation has increased tolerance for time skew between Isilon nodes
- T16496 Config Only Migration deletes existing objects in the Destination Access Zone
- T16340 Customization of alarm settings for SCA0080 and SCA0081 result in "Invalid alarm code" error
- T16372 Disk Space Management for OpenSUSE 42.3
- T16381, T16382 Firewall port fix for ECA clusters on 42.3
- T11893 Eyeglass unable to create Configuration Replication Jobs for OneFS 8.2 SyncIQ policy using SSIP as target host
- T15481 Failover Readiness Warning Alarm Additional Information
- T15870 Failover Readiness does not show readiness for both directions
- T15359 Backup & Restore does not restore Ransomware Defender or Easy Auditor settings
- T15504 Threshold for SCA0075 Disk Space Consumption Alarm Increased
- T15638 Daily Eyeglass Backup may not run
- Enhancements and Fixes in 2.5.6-20069
 - T14913 Eyeglass API enhanced to accept list of policies for SyncIQ or DFS failover

- T15036 Failover Readiness Warning or Error emails not sent in some cases
- T15469 Access Zone Readiness may take a long time with cluster unreachable
- T15502 Configuration Replication may take a long time with cluster unreachable
- Fixed in 2.5.6-20063
 - T12905 Failover Pre and Post Script "target" variable empty for SynclQ and DFS failover
 - T15403 SPN Validation Error - Zone does not have any registered SPNs
 - T15404 DR Dashboard Access Zone appears in Zone Readiness tab even though Pool Failover is configured, Pool Failover Configuration blocked
 - T15229 Eyeglass Archive creation does not complete due to stale NFS mount
- Enhancements / Fixed in 2.5.6-20056
 - T5808: Inconsistent Zone Readiness Status between DR Dashboard and Eyeglass API
 - T7881, T7893: Missing Validations for SPN readiness
- T10479 Limit on number of Parallel Failovers
 - T11585 DR Dashboard incorrectly displays SSIP when IP Pool Smartconnect Subnet is not in same subnet as pool
- T11697 API call corner case may affect failover for Ransomware Defender and Easy Auditor customers

- T14142 SMB Encryption enable/disable not synced
- T11083 Restore from backup does not preserve failover scripts
- T15457 HTML 5 vmware vcenter bug on OVA deployment
- 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 SyncIQ 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 readinessSynclQ 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 has invalid readiness validation for Corrupt Failover Snapshots

- 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
- T17522 Failover Scripting Engine SOURCE and TARGET variables expose password
- 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
- T18253 DR Rehearsal Mode Enable / Revert Error when multiple policies selected
- T18779 Overlapping Powerscale cluster and SyncIQ Policy names can result in incorrect Failover Readiness assessment
- 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 SyncIQ policies associated with same Zone will result in transient error on Eyeglass Zone replication creation
- 1924: Quotas on excluded SyncIQ 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
- T16888 Configuration Replication fails if SynclQ Policy source and target path are different and SynclQ policy path contains special character
- T16965 Audit does not consider differences on source and target for SMB share property inheritable_path_acl
- T17618 SPN repair during Configuration Replication Job does not create missing SPNs
- T18812 Error replicating SMB Share Run as Root permission with local user
- T19177 NFS modify properties which are not client list fails with unresolvable host
- 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
- T8716: Upgrade issues for Cluster Storage Monitor Quota or Data Recovery requests
- 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
- T9652 Unlock My Files inconsistent handling for unreachable PowerScale cluster

- 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
- General
 - 924: Inventory View shows + beside component when there are no more children
 - T17694: api token download of CMDDB 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
- 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
- T17408 Role Based Access Control doesn't handle user names with special characters
- T19208 Too many open files

- 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

- T17254 Failover does not take into account Powerscale job retries
- T18556 User Quota Replication requires System Access Zone AD Provider
- 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
- 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 SyncIQ Job Reports
- T6300 After an Eyeglass restore with the -anyrelease option the print screen functionality for SyncIQ 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

What's New in Superna Eyeglass PowerScale Edition Release 2.5.6

What's New! In Superna Eyeglass PowerScale Edition Release 2.5.6 for DR can be found [here](#).

Supported OneFS releases

8.0.0.x

8.0.1.x

8.1.x.x

8.1.2.x

8.1.3.x

8.2.0.x

8.2.1.x

8.2.2.x

9.0 ** as of 2.5.6-20258

9.1 ** as of 2.5.6-20258

DR Edition Feature Release Compatibility

Feature	Source Cluster Release	Target SynclQ Cluster Release
Configuration Replication non-DFS mode		
Configuration Replication	8.0.x.x	8.0.x.x 8.1.x.x** 8.2.x.x**
Configuration Replication	8.1.x.x	8.1.x.x*** 8.2.x.x** 8.0.x.x**
Configuration Replication	8.2.x.x	8.2.x.x** 8.1.x.x**
Configuration Replication	9.0	9.0
Configuration Replication	9.1	9.1
Configuration Replication DFS mode		
Configuration Replication - DFS Mode	8.0.x.x	8.0.x.x 8.1.x.x** 8.2.x.x**
Configuration Replication - DFS Mode	8.1.x.x	8.1.x.x*** 8.0.x.x** 8.2.x.x**

Configuration Replication - DFS Mode	8.2.x.x	8.2.x.x 8.1.x.x**
Configuration Replication - DFS Mode	9.0	9.0
Configuration Replication - DFS Mode	9.1	9.1
SyncIQ Policy Failover non-DFS mode		
SyncIQ Policy Failover	8.0.x.x	8.0.x.x 8.1.x.x** 8.2.x.x**
SyncIQ Policy Failover	8.1.x.x	8.1.x.x*** 8.0.x.x** 8.2.x.x**
SyncIQ Policy Failover	8.2.x.x	8.2.x.x 8.1.x.x** 8.0.x.x**
SyncIQ Policy Failover	9.0	9.0
SyncIQ Policy Failover	9.1	9.1
SyncIQ Policy Failover DFS mode		
SyncIQ Policy Failover - DFS mode	8.0.x.x	8.0.x.x 8.2.x.x**
SyncIQ Policy Failover - DFS mode	8.1.x.x	8.1.x.x***
SyncIQ Policy Failover - DFS mode	8.2.x.x	8.2.x.x 8.1.x.x** 8.0.x.x**
SyncIQ Policy Failover - DFS mode	9.0	9.0
SyncIQ Policy Failover - DFS mode	9.1	9.1
Access Zone Failover		
Access Zone Failover	8.0.x.x	8.0.x.x

		8.1.x.x** 8.2.x.x**
Access Zone Failover	8.1.x.x	8.1.x.x*** 8.0.x.x** 8.2.x.x**
Access Zone Failover	8.2.x.x	8.2.x.x 8.1.x.x** 8.0.x.x**
Access Zone Failover	9.0	9.0
Access Zone Failover	9.1	9.1
Runbook Robot cluster pairs SynclQ Policy Failover		
SynclQ Policy Failover	8.0.x.x	8.0.x.x 8.1.x.x** 8.2.x.x**
SynclQ Policy Failover	8.1.x.x	8.1.x.x*** 8.0.x.x** 8.2.x.x**
SynclQ Policy Failover	8.2.x.x	8.2.x.x 8.1.x.x** 8.0.x.x**
SynclQ Policy Failover	9.0	9.0
SynclQ Policy Failover	9.1	9.1
Runbook Robot* cluster pairs Access Zone Failover		
Access Zone Failover	8.0.x.x	8.0.x.x 8.1.x.x** 8.2.x.x**
Access Zone Failover	8.1.x.x	8.1.x.x*** 8.0.x.x** 8.2.x.x**

Access Zone Failover	8.2.x.x	8.2.x.x 8.1.x.x** 8.0.x.x**
Access Zone Failover	9.0	9.0
Access Zone Failover	9.1	9.1
Live Ops - DR Test Mode		
Live Ops DR Test Mode	8.1.x.x	8.1.x.x***
Live Ops DR Test Mode	8.2.x.x	8.2.x.x
Live Ops DR Test Mode	9.0.x.x	9.0.x.x
Live Ops DR Test Mode	9.1.x.x	9.1.x.x
Snapshots and Schedules	8.0.x.x	8.0.x.x
Snapshots and Schedules	8.1.x.x	8.1.x.x***
Snapshots and Schedules	8.2.x.x	8.2.x.x - pending testing 8.1.x.x - pending testing
Dedupe Path Settings	8.0.x.x	8.0.x.x
Dedupe Path Settings	8.1.x.x	8.1.x.x**
Dedupe Path Settings	8.2.x.x	8.2.x.x - pending testing 8.1.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.**

*****Due to PowerScale OneFS PAPI API defect, the following configuration change must be made on the Eyeglass appliance to support OneFS releases lower than these releases.**

- Not Required on lower releases than below but note the bug is present and does not affect Eyeglass
 - OneFS 8.0.0.6 (Fixed)
 - OneFS 8.0.1.3 (Fixed)
- Requires Change below on lower Releases

- OneFS 8.1.0.2 (Fixed does not require change below)
- OneFS 8.1.1.1 (Fixed does not require change below)

ssh to the Eyeglass appliance

1. Elevate to root user by using command below and entering admin password

```
sudo su -
```

2. cd /opt/superna/sca/data

3. edit system.xml

4. Find the line

```
<runconfigsyncinparallel>true</runconfigsyncinparallel>
```

5. And modify to false

```
<runconfigsyncinparallel>>false</runconfigsyncinparallel>
```

6. Save your changes

7. Restart the sca service

```
systemctl restart sca
```

9. Done

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](#).

Support Removed in Eyeglass Release 2.5.6

Support for following OneFS releases has been removed in Release

2.5.6:

7.1.1.x

7.2.x.x

7.2.1.x

Deprecation Notices

Following features will no longer be supported as indicated below:

1. As of Release 2.5.7

- a. OpenSUSE 42.3 operating system: Upgrade on OpenSUSE 42.3 operating system will no longer be supported. Use Backup & Restore to the latest OVF to be on a supported release.
- b. Custom Jobs: Eyeglass custom jobs for configuration replication will no longer be supported.
- c. Configuration of SYSLOG forwarding from `/var/log/messages`. The new alarm architecture in 2.5.7 will use a dedicated log that will roll over and provide alarm history external from the database and alarm history in the GUI.

1. As of Release 2.5.6

- a. Quota Request Management Icons: Affects User Storage icon, Quota Request Management workflow, Cluster Storage Usage Icon quotas tab are **unsupported as of 2.5.6**. The Icons will be removed from the GUI in the next update release. **Recommended solution for user managed quota is through AD Managed quota solution documented [here](#).**
 - i. Release 2.5.6 update 2

1. The cluster usage icon has a quota share export tab that will be removed.
 2. The Quota Request Management Icon will remove the requests, history and auto tabs along with request column. This Icon's search features and bulk apply of quotas will be retained and enhanced in later releases.
 3. The share export report CSV will be removed along with the AD group and user CSV report.
 4. The User role for User Storage will be removed from the RBAC roles list.
 5. Replacement Report: The master CSV report contains all quotas and all information that was provided in the other two CSV reports is already available in the quota CSV report.
- b. Data Recovery Management Icons: Part of cluster storage monitor are removed.
 - c. Web widgets: Embeddable Widgets functionality will no longer be available. Eyeglass API now can be used to retrieve DR readiness information - please refer to documentation [here](#).

Issues Fixed in Eyeglass Release 2.5.6

Enhancements and Fixes in 2.5.6-20263

Refer to Enhancements and Fixes in 2.5.6-20258

Enhancements and Fixes in 2.5.6-20258

OneFS Version Support

New: T17099 OneFS 9.1 Support

As of 2.5.6-20258 build OneFS 9.1 is supported.

Configuration Replication

T15639 Error replicating AD Group Run as Root SMB Share permissions

In some cases an SMB Share permission that is configured with an AD group that has Run as Root privileges results in errors when replication the share to the target cluster due to duplication of the permissions. This may result in an AEC Duplicate Permission error from the PowerScale cluster or no error until duplicate permissions exceeds allowed space and an AEC Message Too Long error occurs.

Resolution: Permissions no longer duplicated for AD Group Run as Root SMB Share permissions.

Failover

New: T16448 Zone/Pool Readiness DNS Dual Delegation Validation SSIP reachability check removed

The Zone/Pool Readiness DNS Dual Delegation Validation no longer checks for PowerScale SSIP reachability from Eyeglass as the reachability of SSIP from Eyeglass is not related to client access to PowerScale.

New: T16455 Zone/Pool Readiness AD SPN Delegation Validation Configurable Delay between create and delete test

The time between the create and delete steps for the AD SPN Delegation Validation is now configurable. If AD domain controllers do not execute the create and delete fast enough this can fail the validation test. Default is no delay. This delay is not applied to SPN steps during failover. Related documentation is available [here](#).

New: T16564 Zone/Pool Readiness AD SPN Delegation Validation Retry

AD SPN Validation steps will not be retried for 20 s (default) until they succeed or fail. Retry interval is configurable. Contact support.superna.net for assistance.

New: T16597 New settings for DNS Dual Delegation

These settings allow control over DNS query servers and recursion options required for some environments:

1. If Eyeglass has no access to reach the groupnet DNS due to firewall option is provided to use local Eyeglass DNS.
2. If DNS is Bluecat, Bind or Infoblox recommendation is to use option provided to disable recursive lookup.

Related documentation is [here](#).

New: T16747 Zone/Pool Readiness AD SPN Delegation Validation Logging Enhancement

Additional logging provided for AD SPN Delegation Validation.

New: T16949 DR Rehearsal Mode available for OneFS 9.0, 9.1

DR Rehearsal Mode is now available for OneFS 9.0 and OneFS 9.1 clusters.

T15111 DR Rehearsal Enable incorrectly results in REHEARSAL_ERROR status when failover includes AUTOSKIPCONFIG type jobs

When you enable DR Rehearsal mode and it includes an Eyeglass job that is of AUTOSKIPCONFIG type the end result status will incorrectly be REHEARSAL_ERROR for local target and corrupt failover snapshots for those policies.

This has no impact to the failover itself, steps to enable rehearsal mode complete successfully and no impact to dr test.

The Rehearsal_Error does block the revert for rehearsal mode.

Resolution: DR Rehearsal Mode is now available where Eyeglass job is of AUTOSKIPCONFIG for rehearsal enable and rehearsal revert.

T15249 Post Failover script runs even if failover fails

If a post failover script is configured, it will run once the failover finishes even if the failover has failed.

Resolution: Post failover scripting now has additional variables available to indicate whether or not a failover has run and its status. These can be used in scripting to determine whether steps in a script should run in the case of a failure of the failover.

T15628 Zone/Pool Readiness in DR Dashboard not updated when source cluster is unreachable

If Zone/Pool Readiness job runs when source cluster is unreachable the Readiness job does not complete (shows as ERROR status in Jobs window) and the Zone/Pool DR Failover Status is not updated in the DR Dashboard. The DR Dashboard shows the results from the previous successful execution of the Readiness Job.

Resolution: Zone/Pool Readiness job now completes successfully when the source cluster is unreachable and shows the correct time that job was run and DR Status in the DR Dashboard.

T15830, T17232 OneFS 9.0 Known Limitations with Eyeglass

OneFS 9.0 has following limitations with Eyeglass:

1) Access Zone Readiness Validation

- DNS Dual Delegation readiness validation does not work and should be disabled and verified manually.
- AD SPN Delegation readiness validation does not work and should be disabled and verified manually.

2) IP Pool Failover not supported for OneFS 9.0

Resolution:

1) Access Zone Readiness validations for DNS Dual Delegation and AD SPN Delegation are not available for OneFS 9.0 and 9.1.

2) IP Pool failover is now available for OneFS 9.0 and 9.1

Features

New: Unlock My Files Enhancements

1. Unlock My Files now executed on selected cluster.
2. Partial results will be shown when search times out. GUI will indicate this with message "Result list is truncated - please use a more restrictive search term!".
3. Audit of unlock command will be completed after breaking lock to confirm state of lock.
4. Maximum results limit is now applied per Access Zone instead of per cluster.

New: Quota Search

Cluster Storage Monitor User Storage and Quota Requests Management have been deprecated and replaced with Quota Search window. Quota Search window continues to have Quota Search and bulk Quota Modify capabilities. Quota workflow features have been removed.

T11882/T14354 Storage Monitor Report - UserGroupQuotasReport is empty

The UserGroupQuotasReport which reports on quotas created by the Superna Eyeglass Quota Automation is generated with no content.

Resolution: UserGroupQuotas and ShareExportUsage reports have been deprecated. The Quota Summary report should be used and contains all quotas and user/group information for user/group quotas.

T9621, T14813: Unable to break lock for filenames/path with special characters

When a filename/path contains special characters, Unlock My Files is unable to break the lock.

Message displayed says "No open session...."

Resolution: Able to break lock now for filenames/path with special characters.

T16555 Unlock My Files incorrectly reports Error when unlocking file

In some cases the Unlock My Files will successfully unlock a file but the GUI presents the message "Error unlocking file!".

Resolution: Audit feature to verify that lock has been broken.

General

New: RBAC 2.0

Role Based Access Control now validates AD groups and users when saving the role and blocks save if cannot be resolved. Upon resolution the user or group SID is saved in the configuration. This will ensure that the login process can easily match the user.

1. Adding user s or groups with any case is now supported.
2. Adding group with syntax group@domain is now supported.

Note:

- PowerScale local users not supported going forward (Eyeglass local users are supported)
 - AD groups with @ & or ' in the name is not supported
 - T17408 AD user with language specific characters or special characters such as ',.{}() is not supported
-

T15280 Web widgets: Embeddable Widgets functionality Deprecated

Embeddable widgets functionality is no longer be available. Eyeglass API now can be used to retrieve DR readiness information - please refer to documentation [here](#).

T16683 Phone Home Dedicated Log

Phone home logging can now be found in the dedicated log /opt/superna/sca/logs/phonehome.log .

T16955 ssh command issued as part of daily Eyeglass backup

Unnecessary ssh commands for open files, network information and array status issued when creating daily Eyeglass backup.

Resolution: ssh commands no longer issued when backup is created.

Enhancements and Fixes in 2.5.6-20158

Failover

New: T15063 Failover Readiness Date-Time Validation has increased tolerance for time skew between Isilon nodes

By default a 1 second time skew tolerance between Isilon nodes is now taken into account when executing the Date-Time Validation for failover readiness. Contact support.superna.net if you continue to get a warning with the default time skew tolerance setting.

Features

T16496 Config Only Migration deletes existing objects in the Destination Access Zone

A config only migration job to a Destination Access Zone with existing shares and nfs exports, will delete any shares or exports in the Destination Access Zone which fall at or under the Migration Path of the migration job such that at the end of the migration job shares and exports on source and destination are an exact match. For example if your source and destination path is `/ifs/data/Zone1` and on source you have nfs export `/ifs/data/Zone1/project1` but on Destination Access Zone you have other share or exports with path `/ifs/data/Zone1` or subfolders thereof, after the config migration job runs the destination access zone will only have the nfs export `/ifs/data/Zone1/project1` such that source and destination are an exact match.

Resolution: Config Only Migration job now only creates/updates/deletes based on the source access zone. Any shares or exports that are unrelated (extra) on the target access zone are not affected.

T16370 DR Runbook Robot create export / mount steps disabled by default

Note: To be replaced with SMB data access testing feature in future release

General

T16340 Customization of alarm settings for SCA0080 and SCA0081 result in "Invalid alarm code" error

Using the isi alarm settings set command to customize settings for SCA0080 or SCA0081 alarms results in "Invalid alarm code" error.

Resolution: Settings for SCA0080 or SCA0081 can now be set using the isi alarm settings set command.

T16372 Disk Space Management for OpenSUSE 42.3

Resolution: Improved management of disk space related to Eyeglass backups.

T16381, T16382 Firewall port fix for ECA clusters on 42.3

Resolution: Correct settings for transfer of ECA logs for OpenSUSE 42.3

Enhancements and Fixes in 2.5.6-20084

Configuration Replication

T11893 Eyeglass unable to create Configuration Replication Jobs for OneFS 8.2 SyncIQ policy using SSIP as target host

When using OneFS 8.2 if the SyncIQ policy target host is set to use SSIP of target cluster Eyeglass will be unable to create the related Configuration Replication job. This could also affect mirror policy jobs that are created by PowerScale OneFS as part of failover where PowerScale has selected SSIP as target host.

Resolution: Eyeglass now able to create Configuration Replication job for OneFS 8.2 SyncIQ policy that has target host configured as SSIP of target cluster.

Failover

T15481 Failover Readiness Warning Alarm Additional Information

The Failover Readiness Alarm for Warning state SCA0081 has been updated to include additional information on the details of the warning state in the Alarm info.

T15870 Failover Readiness does not show readiness for both directions

In some environments where source and target cluster names are overlapping (example cluster1 and cluster1dr) after failover only one direction is displayed in DR Dashboard.

Resolution: For above environments, DR Dashboard now displays readiness in both directions.

General

T15359 Backup & Restore does not restore Ransomware Defender or Easy Auditor settings

A Backup & Restore does not restore the Ransomware Defender or Easy Auditor settings.

Resolution: Ransomware Defender settings now restored on restore from release 2.5.5 to 2.5.6 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. Following Expected to not be restored on an AnyRelease restore: Ransomware Defender Event History, Threats Detected, Easy Auditor: Finished Reports, Scheduled Reports, Saved Queries

T15504 Threshold for SCA0075 Disk Space Consumption Alarm Increased

The alarm threshold for SCA0075 Disk Space Consumption on the /srv/www.htdocs/archive has been increased from 800 MB to 2100 MB to more accurately reflect size of archive stored for most deployments and reduce unnecessary alarm notifications.

T15638 Daily Eyeglass Backup may not run

In some environments the daily Eyeglass backup may not run as per schedule.

Resolution: Daily restore backup is now created.

Enhancements and Fixes in 2.5.6-20069

Failover

T14913 Eyeglass API enhanced to accept list of policies for SyncIQ or DFS failover

Eyeglass REST API will now accept a list of policies to group multiple targets into a single failover job for SyncIQ policy or DFS failover. More information is available [here](#).

T15036 Failover Readiness Warning or Error emails not sent in some cases

Under some conditions if you are using zone or pool failover, zone/pool/policy/dfs readiness emails for readiness warning or error are not sent.

Resolution: Change of Readiness status from Ok, Info or Error to Warning now sends email notification. Change of Readiness status from OK, Info, Warning to Error also now sends email notification. No alarm or email when status changes to OK or Info.

T15469 Access Zone Readiness may take a long time with cluster unreachable

When you have an unreachable cluster, Access Zone Readiness may take a long time.

Resolution: If cluster is unreachable when Access Zone Readiness job starts no attempt is made to retrieve information from unreachable cluster to reduce time for the job to complete.

T15502 Configuration Replication may take a long time with cluster unreachable

When you have an unreachable cluster, Configuration Replication may take a long time.

Resolution: Policy Readiness steps that are run as a part of Configuration Replication no longer attempt to retrieve information from unreachable cluster to reduce the time for the job to complete.

Fixed in 2.5.6-20063

Failover

T12905 Failover Pre and Post Script "target" variable empty for SynclQ and DFS failover

The Failover pre and post failover scripting engine "target" variable will be empty for SynclQ and DFS failover types. It is populated for Access Zone failover type.

Resolution: Target is populated for SynclQ and DFS failover.

T15403 SPN Validation Error - Zone does not have any registered SPNs

Access Zone and Pool Failover Readiness may incorrectly display error for SPN validation that "Zone does not have any registered SPNs" when in fact it does.

Resolution: Readiness validation now correctly identifies the SPNs that are present.

T15404 DR Dashboard Access Zone appears in Zone Readiness tab even though Pool Failover is configured, Pool Failover Configuration blocked

In some cases, an Access Zone that was configured for Pool Failover was displayed in the Zone Readiness tab of DR Dashboard. In this case configuration of Pool Failover for that Zone was also blocked.

Resolution: Access Zone configured for Pool failover now appears in Pool Readiness tab and functionality to configure Pool Failover is available.

General

T15229 Eyeglass Archive creation does not complete due to stale NFS mount

If you have configured Eyeglass appliance for Warm Standby with NFS mount to store backup on the PowerScale, creating an Eyeglass archive will get stuck and not complete if there is an issue with the NFS mount which prevents a command that collects disk space information on the Eyeglass appliance from completing.

Resolution: NFS mount issue no longer blocks backup.

Enhancements / Fixed in 2.5.6-20056

Failover

T5808: Inconsistent Zone Readiness Status between DR Dashboard and Eyeglass API

The Eyeglass web UI DR Dashboard shows Zone Readiness in Info state and the Eyeglass API explorer incorrectly shows zone readiness in error state.

Resolution

: Readiness now matched between DR Dashboard and Eyeglass API.

T7881, T7893: Missing Validations for SPN readiness

Zone Readiness and Pool Readiness SPN validations do not check for the conditions below.

IMPACT: These conditions will cause SPN delete/create to fail during a failover:

1) SPN has been created in AD with lower case host (example: host/SPN_name) instead of uppercase HOST (example: HOST/SPN_name)

2) SPN has been created in AD where SPN_name has different case than associated SmartConnect Zone name (example: for SmartConnectZone prod.example.com SPN is configured as HOST/Prod.Example.com)

Resolution: Zone and Pool SPN Readiness validation now include check for service class (HOST) case mismatch and SPN name vs Smartconnect Zone name case mismatch

T10479 Limit on number of Parallel Failovers

If the number of concurrent (parallel) failovers including some quota failover steps exceeds 10, a deadlock occurs and failovers will not complete.

Resolution: Default concurrent failovers allowed is 5. If a higher number of concurrent failovers is required please contact support.superna.net for assistance.

T11585 DR Dashboard incorrectly displays SSIP when IP Pool Smartconnect Subnet is not in same subnet as pool

When the Smartconnect Subnet on a IP pool is different that the subnet the IP pool was created in the DR Dashboard displays the incorrect SSIP.

Resolution: DR Dashboard now displays the correct SSIP.

T11697 API call corner case may affect failover for Ransomware Defender and Easy Auditor customers

There is a small probability for Ransomware Defender and Easy Auditor customers that a corner case condition could affect a critical API call during failover that does not have a retry.

Resolution: Corner case has been addressed.

Configuration Replication

T14142 SMB Encryption enable/disable not synced

Smb3 Encryption Enabled setting for shares on source cluster is not replicated to target cluster for OneFS 8.2.

Resolution: Smb3 Encryption Enabled setting for shares is now synced.

General

T11083 Restore from backup does not preserve failover scripts

If you have configured pre or post failover scripts, the restore from backup does not restore the scripts to the new appliance.

Resolution: Failover pre/post scripts now restored from backup.

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.

Technical Advisories

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

Known Issues

Failover

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 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 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
```

```
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 succeed.

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 has invalid readiness validation for Corrupt Failover Snapshots

For case where SynclQ Policy involved in DR Rehearsal mode enabled has different source and target paths or space in SynclQ Policy path or a special character in SynclQ 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.

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.

T17522 Failover Scripting Engine SOURCE and TARGET variables expose password

The Failover Scripting Engine SOURCE and TARGET environment variable information includes the password of the account used to connect from Eyeglass to PowerScale in plain text.

Workaround: Do not use these variables in scripting.

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.

T18253 DR Rehearsal Mode Enable / Revert Error when multiple policies selected

A DR Rehearsal Mode Enable / Revert where more than 3 SyncIQ policies are involved either selected for SyncIQ or DFS mode or an Access Zone with more than 3 SyncIQ policies, the final step which updates Eyeglass with the rehearsal status fails with a lock conflict error..

Workaround: For SyncIQ or DFS Mode Rehearsal Enable or Revert do not select more than 3 policies at a time. For Access Zone Rehearsal mode where Access Zone has more than 3 SyncIQ policies run the Rehearsal exercise as a SyncIQ policy Rehearsal selecting a maximum of 3 policies at a time.

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.

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 SyncIQ policies associated with same Zone will result in transient error on Eyeglass Zone replication creation

Where there are multiple SyncIQ 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.

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

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

Workaround: Configuration objects such as SMB shares and NFS exports must be kept in sync on the DR cluster manually. To avoid the replication error on each cycle and keep the SyncIQ policy available for failover the Eyeglass Configuration Replication job can be set to AUTOSKIPCONFIG as per instructions [here](#).

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.

T17618 SPN repair during Configuration Replication Job does not create missing SPNs

The SPN repair component of the Eyeglass Configuration Job does not create missing SPNs.

Impact: This only impacts creation of SPNs for new SmartConnect zones added in Powerscale. This does not affect SPN create/delete during failover.

Workaround: Create required SPNs for new SmartConnect zones in AD manually.

T18812 Error replicating SMB Share Run as Root permission with local user

In some cases where an SMB share permission is configured with run as root and local users the run as root permissions are replicated to the target as regular permissions and also subsequent attempts to update results in a duplicate permission error.

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.

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.

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](#).

T8716: Upgrade issues for Cluster Storage Monitor Quota or Data Recovery requests

After upgrade to new release see following issues for Quota or Data Recovery requests:

- 1) Data Recovery does not show any pending requests or history
- 2) Quota Request shows history but with incorrect status

Workaround: None available for history. For Data Recovery pending request, re-issue the request.

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.

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.

Workaround: Resolve PowerScale cluster reachability issue.

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.

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.

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

T17408 Role Based Access Control doesn't handle user names with special characters

RBAC can be setup with users that have special characters or language specific characters or groups where users have special or language characters, but on login the name is not resolved properly and the proper role is not assigned. User gets read only desktop view.

Workaround: None available

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.

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.

2. 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`

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.

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 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 charaters 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.

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 SynclQ Job Report log were combined. In this case you are able to see the SynclQ 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 SynclQ 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 SynclQ 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

© Superna LLC

1.14. Release 2.5.6 - Release Notes Easy Auditor

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

- [What's New in Superna Eyeglass Easy Auditor Edition](#)
- [Supported OneFS releases](#)
- [Supported Eyeglass releases](#)
- [Inter Release Functional Compatibility](#)
- [End of Life Notifications](#)
- [Issues Fixed in 2.5.6](#)
- [Enhancements and Fixes in 2.5.6-20263](#)
- [Refer to Enhancements/Fixes in previous 2.5.6 versions.](#)
- [Enhancements and Fixes in 2.5.6-20258](#)
 - [New: Where Did My Folder Go default results retrieved increased to 5000](#)
 - [T16668 Cannot load saved Built-In Query](#)
- [Enhancements and Fixes in 2.5.6-20158](#)
- [Reporting](#)
 - [New: T16126 Logon/Logoff event report now generated from Report Query Builder](#)
- [Active Auditing](#)
 - [New: T15327 Where Did My Folder Go now also reports on File Rename and File Delete Events](#)

- Fixed in 2.5.6-20084
- General
 - T15359 Backup & Restore does not restore Ransomware Defender or Easy Auditor settings
 - T15834 Bulk Ingest of Old Audit Data 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 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
- T20661 Large Report cannot be downloaded from Windows
- 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
 - T16978 Display of Files for Mass Delete always shows 1 file

- T16980 Active Auditor events Affected Files-CSV may not show all events
- 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
 - T13539 PowerScale Directory selector missing directories
 - _____
- 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
- T11540 Active Auditor may report on Audit Failure events
- T12380 Ransomware Defender Ignore List settings are applied to Active Auditor analysis
- T16137 Anyrelease restore does not restore all Ransomware Defender and Easy Auditor settings
- T16499 Easy Auditor reports double events

What's New in Superna Eyeglass Easy Auditor Edition

Release 2.5.6

What's New! In Superna Eyeglass Easy Auditor Edition Release 2.5.6 can be found [here](#).

Supported OneFS releases

8.0.0.x

8.0.1.x

8.1.x.x

8.1.2.x

8.1.3.x

8.2.0.x

8.2.1.x

8.2.2.x

9.0

9.1

Supported Eyeglass releases

Superna Eyeglass Easy Auditor Version	Superna Eyeglass Version

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
2.5.4-19106	2.5.4-19106
2.5.4-18266	2.5.4-19106 2.5.4-18275 2.5.4-18266
2.5.3-18257	2.5.4-18275 2.5.4-18266 2.5.3-18251

Inter Release Functional Compatibility

	OneFS 8.0 - OneFS 8.0.1	OneFS 8.0.1 - OneFS 8.1	OneFS 8.0 - OneFS 8.1	OneFS 8.0.x , 8.1.x - OneFS 8.2.x
Reporting	Untested	Untested	Untested	Untested
Active Auditing	Untested	Untested	Untested	Untested

End of Life Notifications

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

Issues Fixed in 2.5.6

Enhancements and Fixes in 2.5.6-20263

Refer to Enhancements/Fixes in previous 2.5.6 versions.

Enhancements and Fixes in 2.5.6-20258

New: Where Did My Folder Go default results retrieved increased to 5000

The Where Did My Folder Go default results retrieved for files or folder search has been increased to 5000.

T16668 Cannot load saved Built-In Query

A saved Built-In Query cannot be loaded or acted upon. After attempting to load a saved query the Eyeglass desktop window appears blank.

Resolution: A saved Built-In Query can now be loaded and run.

Enhancements and Fixes in 2.5.6-20158

Reporting

New: T16126 Logon/Logoff event report now generated from Report Query Builder

Report for Logon/Logoff audit events is now generated from the Easy Auditor -> Query -> Report query Builder window. Built-In Query for Logon/Logoff has been removed. From the Report Query Builder select

Path: Select the cluster of interest and path /ifs (no other path can be selected as a path is not specified for a LOGON or LOGOFF audit event)

Event Type: LOGON and/or LOGOFF as required

Query can be further filtered by User Name and Time Frame as required.

Note that in the Report, the Powerscale Cluster will appear in the Cluster column. Path is also populated but with Systemnull value as the LOGON/LOGOFF events are not associated with a path.

Active Auditing

New: T15327 Where Did My Folder Go now also reports on File Rename and File Delete Events

Easy Auditor -> Active Auditing -> Where Did My Folder Go window by default will continue to search for Folder Renames and Deletes but now includes the option to perform the same search for File Rename and Delete events. Select the Folder path as before as well as timeframe then select either Folder or Files as the subject of the search. With the addition of this capability you will see following additional changes as well:

- Time Frame for the search is now a Start time with a configurable number of hours to bound the search backwards in time: 1, 2, 4, 6 or 24 hours
- Total records retrieved is limited to a maximum number of records returned. If your search returned matches equal to the limit you may need to further narrow your search by either modifying the path or picking a shorter timeframe to find your result. Note that records retrieved contain both delete and rename events, the Show Deleted Objects checkbox will only filter them in the GUI.

Documentation details can be found [here](#).

Fixed in 2.5.6-20084

General

T15359 Backup & Restore does not restore Ransomware Defender or Easy Auditor settings

A Backup & Restore does not restore the Ransomware Defender or Easy Auditor settings

Resolution: Ransomware Defender settings now restored on restore from 2.5.5 to 2.5.6. 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. Following expected to not be restored on an AnyRelease restore: Ransomware Defender Event History, Threats Detected, Easy Auditor: Finished Reports, Scheduled Reports, Saved Queries.

T15834 Bulk Ingest of Old Audit Data not functional

The ability to bulk ingest old audit data is not functional as of 2.5.6 release.

Resolution: Bulk ingest of old audit data is now functional.

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 save query to review it's 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 then 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 the 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 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 first line

Report Query File Ext filter is only editable in first line. Clicking anywhere else in the box will not let you enter any text

Workaround: None required. Enter 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 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

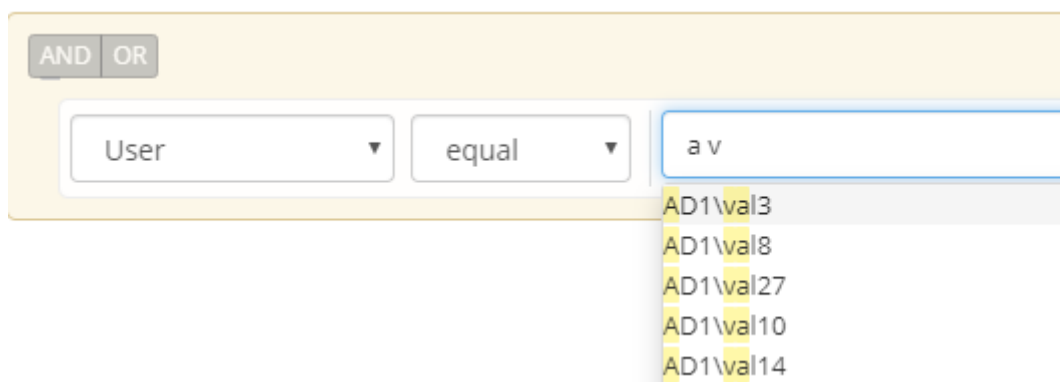
T10911 Share/Stale Access Report issue when AD has nested groups

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



The screenshot shows a search filter interface. At the top, there are two buttons labeled 'AND' and 'OR'. Below them, there is a dropdown menu labeled 'User' with a downward arrow. To its right is another dropdown menu labeled 'equal' with a downward arrow. To the right of these is a text input field containing 'a v'. Below the text input field, a list of suggestions is displayed: AD1\val3, AD1\val8, AD1\val27, AD1\val10, and AD1\val14. The suggestions are listed vertically and are highlighted with a light blue background.

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

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

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.

T16978 Display of Files for Mass Delete always shows 1 file

On the GUI for Active Auditor > Active Events as well as in associated alarm information the number of affected files is always displayed as 1. This is a display issue only. The number of files configured in the trigger was correctly used in the detection.

Workaround: To see the full list of files, download the report containing the files by selecting the Files link in the GUI and then Affected Files - CSV.

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.

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 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 upgrade to 2.5.6.

Workaround: None required. New logs will have 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, then 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.

T13539 PowerScale Directory selector missing directories

The PowerScale Directory selector currently has a maximum list size of 1000 so that environments with more than 1000 directories on the PowerScale will be missing directories in the directory selector.

Workaround: Use the PowerScale Directory Selector to enter \ifs\ and then enter the remainder of the path manually.

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. Reports against larger AD environments may fail.

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.

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

Known Limitations

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 LLC

1.15. Release 2.5.6 - Release Notes

Ransomware Defender

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

- [What's New in Superna Eyeglass Ransomware Defender Edition Release 2.5.6](#)
- [Supported OneFS releases](#)
- [Supported Eyeglass releases](#)
- [Active Directory Compatibility](#)
- [Inter Release Functional Compatibility](#)
- [End of Life Notifications](#)
- [Support Removed in Eyeglass Release 2.5.6](#)
- [Enhancements / Fixes in 2.5.6-20258](#)
 - [New: T16769 New behaviour detections enabled by default](#)
 - [T16510 Flag as False Positive settings may not take effect](#)
 - [T15926 Invalid user format in ignore list stops threat detection analysis](#)
 - [T16148 Paths or Files that contain the string ****analytics**** are ignored for user behaviour Ransomware detection algorithms](#)
 - [T16149 New behaviour detections enabled by default](#)
 - [T15359 Backup & Restore does not restore Ransomware Defender or Easy Auditor settings](#)
 - [T15230 Configuration of Ransomware Defender Thresholds requires temporary exit from Monitor Mode](#)
 - [T15040 New Behaviour detections available](#)

- T15427 Security Guard Restore Access updates GUI for other Active Events as restored
- Technical Advisories
 - 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
 - T4337 Modifying Ransomware Defender Settings or Running the lock root command removes lock root settings
 - 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
- T11832 Ransomware Security Event which is promoted from Warning to Major does not respect Major Grace Period
- T14798 Well Known user Authenticated Users not handled
- T15198, T15650 Ransomware Events may have inaccurate Signal Strength
- T15234 igls rsw restore leaves share without permission where user permission configured
- 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
- T16830 TD 7 Extension flag as false positive will add to the UI but will not take affect

- T17900 Clients column for Ransomware events may not display all IP addresses
- T18985 igls rsw restoreaccess cannot restore access for unresolvable user
- 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
- Known Limitations

- 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
- General
 - T16137 Anyrelease restore does not restore all Ransomware Defender and Easy Auditor settings

What's New in Superna Eyeglass Ransomware Defender Edition Release 2.5.6

What's New! In Superna Eyeglass Ransomware Defender Edition Release 2.5.6 can be found [here](#).

Supported OneFS releases

8.0.0.x

8.0.1.x

8.1.x.x

8.1.2.x

8.1.3.x

8.2.0.x

8.2.1.x

8.2.2.x

9.0

9.1

Supported Eyeglass releases

Superna Eyeglass Ransomware Defender Version	Superna Eyeglass Version
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
2.5.4-19106	2.5.4-19106
2.5.4-18266	2.5.4-19106 2.5.4-18275 2.5.4-18266
2.5.3-18257	2.5.4-18275 2.5.4-18266 2.5.3-18251
2.5.2-18080	2.5.2-18080
2.5.1-18013	2.5.1-18012

Active Directory Compatibility

Ransomware Defender Versions	Supported Active Directory Versions
2.5.6 and 2.5.5 all versions	Microsoft Active Directory 2008, 2012, 2016

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
Threat Detection	Yes	Yes	Yes	Untested	Untested
Security Guard	Yes	Yes	Yes	Untested	Untested

End of Life Notifications

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

Support Removed in Eyeglass Release 2.5.6

1. Support for following OneFS releases has been removed in Release 2.5.6:

7.1.1.x

7.2.x.x

7.2.1.x

2. The Internet version of the well known ransomware extension list is deprecated and a cached version built into the code is used. In next release 2.5.7, the file will be managed from Eyeglass and will have access to versioned files reachable via same URL required for Phone Home for simplicity. More details on the 2.5.7 release can be found [here](#) and on the new management of the extension list from the Eyeglass Ransomware Defender window [here](#).

Enhancements / Fixes in 2.5.6-20258

Refer to Enhancements/Fixes in previous 2.5.6 versions.

Enhancements in 2.5.6-20258

Threat Detection

New: T16769 New behaviour detections enabled by default

Ransomware new behaviour detections available in 2.5.6-20158 now enabled by default.

Fixed in 2.5.6-20158

Threat Detection

T16510 Flag as False Positive settings may not take effect

Under some conditions initiating Archive as False Positive from the Ransomware Defender Active Events GUI does not take effect. There is no visible error related to this issue.

Resolution: Issue was related to one threat detection area and has been resolved. Archive as False Positive from the Ransomware Defender Active Events GUI now takes effect.

Enhancements/Fixed in 2.5.6-20084

Threat Detection

T15926 Invalid user format in ignore list stops threat detection analysis

Adding a user to the ignore list (local or AD) where user entry has invalid format blocks threat detection analysis.

Resolution: Entry of user to ignore list with invalid format is now blocked.

T16148 Paths or Files that contain the string ****analytics**** are ignored for user behaviour Ransomware detection algorithms

The user behaviour Ransomware detection algorithms skip any folders or files that contain the string ****analytics****. Honeypot share and well known extension matching is not affected by this issue.

Resolution: Paths and filenames containing the string "analytics" are now included in user behaviour Threat Detection analysis.

T16149 New behaviour detections enabled by default

Ransomware new behaviour detections introduced in 2.5.6-20069 now enabled by default. NOTE:TD 12 is not active in the flag as false positive action menu and will be added in a future release.

NOTE: This may introduce new detections that will need to be evaluated to determine whether additional tuning of Ransomware Defender settings is required.

General

T15359 Backup & Restore does not restore Ransomware Defender or Easy Auditor settings

A Backup & Restore does not restore the Ransomware Defender or Easy Auditor settings.

Resolution: Ransomware Defender settings now restored on restore from release 2.5.5 to 2.5.6 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. Following Expected to not be restored on an AnyRelease restore: Ransomware Defender Event History, Threats Detected, Easy Auditor: Finished Reports, Scheduled Reports, Saved Queries

Enhancements/Fixed in 2.5.6-20069

Threat Detection

T15230 Configuration of Ransomware Defender Thresholds requires temporary exit from Monitor Mode

If you have Monitor Mode active, it is necessary to exit from Monitor Mode temporarily while making changes to Ransomware Defender Threshold settings. While temporarily exited from Monitor Mode, lockouts can occur based on existing settings. You should enter Monitor Mode again immediately after making the change.

Resolution: All threshold levels can now be modified without exiting Monitor mode. With Monitor Mode enabled, additional description "Not Applied (Monitor Mode)" to clarify that values updated are not active while in Monitor Mode.

T15040 New Behaviour detections available

Contact support.superna.net to upgrade.

Security Guard

T15427 Security Guard Restore Access updates GUI for other Active Events as restored

When the Security Guard restore access step is executed, if there are other active events in the Ransomware Defender / Active Events list in the LOCKED_OUT "State" those other active events "State" will also be updated to "ACCESS_RESTORED" in the GUI but no actual restore step is done - the other user accounts still have the deny permission applied on their PowerScale shares.

Resolution: Access is restored now only for the Security Guard user. Other Active Events are not updated as part of the Security Guard job.

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.

T4337 Modifying Ransomware Defender Settings or Running the lock root command removes lock root settings

Lock root settings applied using command

```
igls admin lockroot --lock_root
```

.are lost each time a change is made to Ransomware Settings or running the `igls admin lockroot` command. If lock root was enabled it becomes disabled.

Workaround: Each time a Ransomware Settings change is made, the lock root setting must be reapplied manually. Please contact support.superna.net for assistance.

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

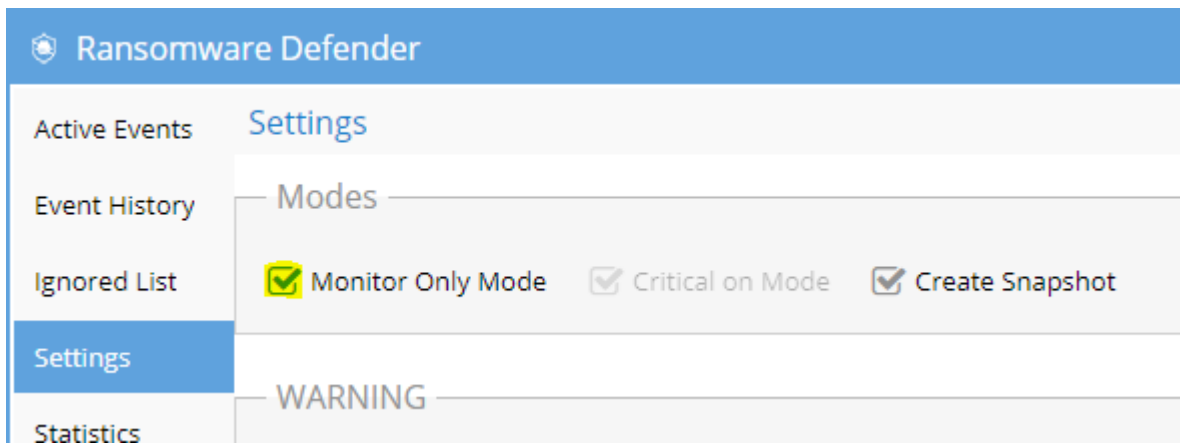
It may occur that a user is only partially locked out when a multi-user lockout is occurring due to an error response from the PowerScale cluster during user resolution in Active Directory. In this case the error is not displayed in the Eyeglass event history.

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 a PowerScale snapshot

When a Ransomware Security Event is detected for an NFS client, the PowerScale snapshot against related paths is not created.

Workaround: None available. PowerScale scheduled snapshots may be available for recovery.

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.

Workaround: None available.

T14798 Well Known user Authenticated Users not handled

When well known user "Authenticated User" is used for share permissions Ransomware Defender does not translate this permission into users and therefore does not affect a deny for any users against that share.

Workaround: Use Everyone permission and leave the Guest account disabled as the Guest account is insecure and should never be enabled because this exposes data to Ransomware.

T15198, T15650 Ransomware Events may have inaccurate Signal Strength

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.

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.

T15234 igls rsw restore leaves share without permission where user permission configured

If you have assigned share permission using AD user permission directly (no AD group permission). if that user is locked out and you are unable to restore access from the GUI the `igls rws restoreaccess` command that would usually be used to restore access will remove the deny permission but will not put back the original user permission.

Workaround: Restore user access for this case by directly editing the share on PowerScale to remove the deny and add user with correct level of access. The shares that are affected are displayed in the Ransomware Defender Active Events or Event History tabs in the Shares column.

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.

T16830 TD 7 Extension flag as false positive will add to the UI but will not take effect

Flagging TD 7 detection as false positive will add to the UI but will not take effect. This is not a user behavior detection and requires a CLI command to whitelist the extension. This is by design and a future release will block this in the GUI and will allow adding to the extension whitelist automatically from the GUI. In the current release the CLI is required to add an extension to the whitelist.

Resolution: Use the CLI guide to add a whitelist for the extension. See guide [here](#). Future release to remove flag as false positive for TD 7 detections.

T17900 Clients column for Ransomware events may not display all IP addresses

For a security event where there are signals for the same User (account) from different IP addresses, the Clients column may not list all IP addresses.

Workaround: If you also have Superna Eyeglass Easy Auditor an audit report for the User associated with the event may contain file activity which shows additional IP addresses.

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.

Workaround: The Ransomware Defender GUI can restore access in this case while the event is in the Active Events list. If the event has already been archived to the Event History contact support.superna.net for assistance.

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 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.

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].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 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

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

© Superna LLC

1.16. Release 2.5.6 - Release Notes

Performance Auditor

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

- [What's New in Superna Eyeglass Performance Auditor Release 2.5.6](#)
- [Supported OneFS releases](#)
- [End of Life Notifications](#)
- [Technical Advisories](#)
 - [New: T14175 Rewind mode for Performance Auditor](#)
 - [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](#)
 - [T17476 Performance Auditor Rewind Time Display incorrect when invalid time entered](#)
 - [T17480 Performance Auditor Rewind Timer Selector issue](#)
 - [T18088 Rewind time invalid when no records found](#)
 - [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 2.5.6

What's New! In Superna Eyeglass Performance Auditor can be found [here](#).

Supported OneFS releases

8.1.x.x

8.2.x.x

9.0

9.1

End of Life Notifications

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

Technical Advisories

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

Enhancements in 2.5.6-20263

New: T14175 Rewind mode for Performance Auditor

- Real time data stored for 14 days allowing administrators ability to rewind and playback real time data from the past

- Share a day and time in the past with other administrators using a book mark

Documentation for Rewind Mode can be found [here](#).

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.

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 invalid when no records found

If you select a rewind interval beyond where data is available, the "rewind" time displayed is incorrect.

Workaround: None required. Interval selected does not have data.

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 LLC

1.17. Release 2.5.6 - Release Notes ECA

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

- [What's New in Superna Eyeglass Easy Auditor Edition and Ransomware Defender Edition](#)
- [Supported OneFS releases](#)
- [End of Life Notifications](#)
- [Issues Fixed in this Release](#)
- [Enhancements/Fixed in 2.5.6-20084](#)
 - [T15608 Syslog communication between ECA and Eyeglass now uses TCP](#)
- [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](#)
 - [T15457 HTML 5 vmware vcenter bug on OVA deployment](#)
 - [T17103 ECA version intermittently reported incorrectly](#)

These Release Notes cover the Superna Eyeglass ECA deployed with Superna Eyeglass Ransomware Defender and Superna Eyeglass Easy Auditor

What's New in Superna Eyeglass Easy Auditor Edition and Ransomware Defender Edition

Release 2.5.6

What's New! In Superna Eyeglass Easy Auditor Edition and Ransomware Defender Edition Release 2.5.6 can be found [here](#).

Supported OneFS releases

8.0.0.x

8.0.1.x

8.1.x.x

8.1.2.x

8.1.3.x

8.2.0.x

8.2.1.x

8.2.2.x

9.0

9.1

Supported Eyeglass releases

Superna Eyeglass ECA Version	Superna Eyeglass Version
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](#).

Issues Fixed in this Release

Enhancements/Fixed in 2.5.6-20084

T15608 Syslog communication between ECA and Eyeglass now uses TCP

Syslog communication between ECA and Eyeglass was previously using UDP and now uses TCP protocol. If you have a firewall between ECA and Eyeglass specific to UDP on port 514 this will need to be updated to TCP.

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.

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.

© Superna LLC