

**IntelliFlash**

# **IntelliFlash User Guide**

IntelliFlash 3.11.6.2 (Part Number: 96-00567-001)



---

# Notice

---

## Legal Disclaimer

---

Tintri by DDN, Inc. does not recommend the use of its IntelliFlash products in life support applications wherein a failure or malfunction of the product may directly threaten life or injury.

Accordingly, in any use of IntelliFlash products in life support systems or other applications where failure could cause damage, injury, or loss of life, the products should only be incorporated in systems designed with appropriate redundancy, fault tolerant or back-up features. The user of IntelliFlash products in life support or other such applications assumes all risk of such use and agrees to indemnify, defend, and hold harmless Tintri by DDN, Inc. against all damages.

This document and related material are for information use only and are subject to change without prior notice. Tintri by DDN, Inc. assumes no responsibility for any errors that may appear in this document or related material, nor for any damages or claims resulting from the furnishing, performance, or use of this document or related material. Absent a written agreement signed by Tintri by DDN, Inc. or its authorized representative to the contrary, Tintri by DDN, Inc. explicitly disclaims any express and implied warranties and indemnities of any kind that may, or could, be associated with this document and related material, and any user of this document or related material agrees to such disclaimer as a precondition to receipt and usage hereof.

Each user of this document or any product referred to herein expressly waives all guaranties and warranties of any kind associated with this document any related materials or such product, whether expressed or implied, including without limitation, any implied warranty of merchantability or fitness for a particular purpose or non-infringement. Each user of this document or any product referred to herein also expressly agrees Tintri by DDN, Inc. shall not be liable for any incidental, punitive, indirect, special, or consequential damages, including without limitation physical injury or death, property damage, lost data, loss of profits or costs of procurement of substitute goods, technology, or services, arising out of or related to this document, any related materials or any product referred to herein, regardless of whether such damages are based on tort, warranty, contract, or any other legal theory, even if advised of the possibility of such damages.

This document and its contents, including diagrams, schematics, methodology, work product, and intellectual property rights described in, associated with, or implied by this document, are the sole and exclusive property of Tintri by DDN, Inc. No intellectual property license, express or implied, is granted by Tintri by DDN, Inc. associated with the document recipient's receipt, access and/or use of this document or the products referred to herein; Tintri by DDN, Inc. retains all rights hereto.

### **Contact information**

#### **Address**

9351 Deering Avenue, Chatsworth, California 91311, USA

#### **Phone**

+1 800-837-2298 or +1 818-700-4000

© 2023 Tintri by DDN, Inc. All rights reserved.

<https://www.tintri.com>.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means: electronic, mechanical, photocopying, recording or otherwise, without the prior written consent of Tintri by DDN, Inc.

IntelliCare, IntelliFlash, the IntelliFlash logo, and IntelliShell are registered trademarks or trademarks of Tintri by DDN, Inc. in the US and/or other countries. VMware, VMware ESXi, VMware vSphere, and VMware vCenter are registered trademarks or trademarks of VMware, Inc. in the United States and/or other jurisdictions. All other marks are the property of their respective owners. Product specifications subject to change without notice. Pictures shown may vary from actual products. Not all products are available in all regions of the world.

# Contents

<b>Chapter 1: Introduction to IntelliFlash Systems.....</b>	<b>1</b>
Components in IntelliFlash Storage Arrays.....	2
Dual Controllers.....	2
Redundant Hardware.....	2
Multiprotocol.....	2
Multiprotocol for NAS.....	2
Multipathing.....	2
Capacity Expansion.....	2
IntelliFlash Operating Environment.....	3
Media Management.....	3
Advanced Data Services.....	4
Protocol Choice.....	4
Management Flexibility.....	4
<b>Chapter 2: Unified IntelliFlash Web UI.....</b>	<b>7</b>
Logging in to the IntelliFlash Web UI.....	8
Logging out from the IntelliFlash Web UI.....	9
System Information Window.....	9
Enabling Maintenance Mode.....	11
Viewing IntelliShell Session Status.....	11
Accessing Online Help.....	12
Accessing BMC from the IntelliFlash Web UI.....	12
Rebooting an IntelliFlash system Controller.....	12
Powering off an IntelliFlash system Controller.....	13
<b>Chapter 3: Dashboard.....</b>	<b>15</b>
Dashboard sections.....	16
Array tab and pool name tabs.....	17
Savings.....	18
Capacity.....	19
Performance.....	20
Storage objects with Top 10 or Bottom 10 workloads.....	22
System Monitor.....	23
Dashboard variations.....	24
No pools.....	25
No projects.....	26
Single pool view.....	27
Multi pool view.....	28
Viewing pool or array performance details.....	29
Viewing pool or array space saving and capacity.....	30

Viewing Top 10 or Bottom 10 LUNS, Shares, or VMs with maximum or minimum workload.....	30
Viewing CPU and cache hits usage of the array.....	31
<b>Chapter 4: IntelliFlash Analytics.....</b>	<b>33</b>
Live and Historical Views.....	34
Analytics UI.....	35
Analytics graphs.....	39
Sources for Graphs.....	39
Different views for graphs.....	39
UI controls in the graphs.....	40
Graphs in Data Performance.....	41
Graphs in Pool Performance.....	44
Graphs in System Performance.....	45
Viewing Array analytics.....	46
Selecting Sources for Data Performance.....	46
Viewing Data Performance Analytics.....	47
Viewing Pool Performance Analytics.....	47
Viewing System Performance Analytics.....	48
Switching between Live and Historical views.....	48
Zooming in and out on a time interval in a graph.....	49
Viewing custom historical analytics.....	49
Hiding or unhiding a data point in a graph.....	50
Customizing the Analytics view.....	51
Adding a new Array Statistics tab.....	51
Duplicating an Array Statistics tab.....	51
Renaming an Array Statistics tab.....	52
Deleting an Array Statistics tab.....	52
Selecting graphs for Analytics.....	52
Selecting time intervals for graphs.....	53
Exporting Analytics data.....	54
Hiding or unhiding graph controls and legends.....	54
<b>Chapter 5: Pools.....</b>	<b>55</b>
Understanding Pools.....	56
Hybrid Pool.....	56
NVMe Pool.....	56
System Pool.....	56
Disk Group Types in a Pool.....	56
Pool Types Based on Redundancy Level.....	58
Pool Naming Convention.....	58
Pools page.....	59
Overview tab in the Pools page.....	59
Disks tab in the Pools page.....	59
Create Pool Window.....	60
Creating a New Pool.....	61
Active and Exported Pool.....	62

Viewing Active Pool Details.....	63
Managing a Pool.....	63
Expanding a Pool.....	64
Exporting a Pool.....	65
Importing a Pool.....	65
Resetting Pool Errors.....	66
Performing Pool Integrity Check.....	66
Deleting a Pool.....	66
Deleting an Exported Pool.....	67
Managing Disk Drives of a Pool.....	67
Viewing Disks on the IntelliFlash Systems.....	68
Viewing serial number of a controller.....	69
Searching disks by an alias name.....	69
Setting a Disk to Offline.....	69
Replacing a Disk Manually.....	70
Setting a Disk to Online.....	71
Adding a Hot Spare Disk.....	71
Removing a Hot Spare Disk.....	71
Managing System Pool.....	72
Viewing System Pool Details.....	72
Resetting System Pool Errors.....	72
Running Pool Integrity Check on System Pool.....	73
<b>Chapter 6: Projects.....</b>	<b>75</b>
IntelliFlash Projects.....	76
Project Templates.....	76
SQL Server Template.....	77
Virtual Server Template.....	78
VMware VDI Template.....	79
Hyper-V VDI Template.....	80
Generic Template.....	80
Microsoft Exchange Server Template.....	80
Differences Between Generic and Other Project Templates.....	81
Overriding Project Level Properties.....	83
Projects Menu.....	83
NPIV Ports and Projects after Upgrade.....	84
Creating Projects.....	84
Creating an iSCSI Project for SQL Server.....	84
Creating an iSCSI Project for Virtual Server Application.....	88
Creating an iSCSI Project for VMware VDI.....	92
Creating an iSCSI Project for Hyper-V VDI.....	95
Creating an iSCSI Project for Exchange Server.....	99
Creating an iSCSI Project for Generic Purpose.....	103
Creating an FC Project for SQL Server.....	106
Creating an FC Project for Virtual Server Application.....	108
Creating an FC Project for VMware VDI.....	110
Creating an FC Project for Hyper-V VDI.....	112
Creating an FC Project for Exchange Server.....	114

Creating an FC Project for Generic Purpose.....	116
Creating an NFS Project for Virtual Server Application.....	117
Creating an NFS Project for VMware VDI.....	119
Creating an NFS Project for Generic Purpose.....	121
Creating an SMB Project for SQL Server.....	123
Creating an SMB Project for Hyper-V VDI.....	124
Creating an SMB Project for Generic Purpose.....	126
Managing Projects.....	128
Modifying Project Mountpoint.....	128
Viewing the Purpose of a Project.....	128
Modifying Compression Type in a Project.....	129
Modifying Project Quota Size.....	129
Modifying Project Space Reservation.....	130
Enabling or Disabling Project Deduplication Status.....	130
Modifying Project Cache.....	131
Enabling or Disabling Read Only Status.....	131
Setting LUN Creation Default Options.....	132
Modifying Space Usage Threshold Levels for a Project.....	132
iSCSI and FC Mappings.....	133
Adding iSCSI Mapping for a Project.....	133
Adding FC Mapping for a Project.....	133
Deleting an iSCSI Mapping at a Project Level.....	134
Deleting FC Mappings at a Project Level.....	134
Share Creation Defaults.....	134
Enabling or Disabling Share Creation Default Options.....	135
Deleting a Project.....	135

## **Chapter 7: Shares.....** **137**

Shares.....	138
Shares in Project Templates.....	138
Creating a Share.....	139
Creating a Folder in a Share.....	141
Deleting a Share.....	141
Deleting a Folder in a Share.....	141
Managing Shares.....	142
Modifying Share-Level Quota.....	142
Setting Quota Limit for Users and Groups.....	142
Modifying Space Reservation for a Share.....	143
Modifying a Share Mountpoint.....	144
Overriding Compression Class in a Share.....	145
Overriding Deduplication Setting at Share Level.....	146
Overriding Read Only Property for a Share.....	146
Overriding ACL Inheritance Setting at Share-Level.....	147
Overriding the Block Size for a Share.....	147
Overriding Cache Behavior at Share Level.....	148
Setting Access Time for a Share.....	148
Setting NBMAND.....	148
Viewing the Purpose of a Share.....	149

Overriding NFS Project Level Settings for a Share.....	149
Configuring Anonymous User IDs or Groups IDs on an NFS Share.....	150
Enabling or Disabling Kerberos on an NFS Share.....	150
Overriding SMB Project Level Settings for a Share.....	151
Changing SMB Share Display Name.....	151
Creating a Hidden SMB Share.....	152
Modifying Space Usage Threshold Levels for a Share.....	152
Autohome Share.....	153
Creating an Autohome Share.....	153
Setting up Access Permissions to the Autohome Share.....	154
Enabling or Disabling Autohome Share Service.....	155
Offline Files.....	155
Creating an Offline Share.....	155
Converting an Existing Share to Offline Share.....	156
Subshares.....	156
Considerations for Using Subshares.....	157
Enabling Subshares Creation Option.....	158
Creating a Subshare.....	158
Creating a Folder in a Subshare.....	160
Managing Subshares.....	160
Deleting a Subshare.....	160
<b>Chapter 8: Access Control Lists.....</b>	<b>163</b>
Access Control Lists.....	164
Network ACLs.....	164
Network ACLs.....	164
Adding a Network ACL for an NFS Project.....	165
Adding a Network ACL for an NFS Share.....	166
Adding a Network ACL for an SMB Project.....	166
Adding a Network ACL for an SMB Share.....	167
Deleting a Network ACL for an NFS Project.....	168
Deleting a Network ACL for an NFS Share.....	168
Deleting a Network ACL for an SMB Project.....	169
Deleting a Network ACL for an SMB Share.....	169
User ACLs.....	169
User ACLs.....	169
ACL Migration.....	170
Permissions.....	171
Adding User-Level ACLs.....	171
Deleting a User ACL.....	172
User ACL Access Privileges.....	173
Folder ACLs.....	174
Adding an ACL to a Folder.....	174
Deleting Folder-Level ACLs.....	175
<b>Chapter 9: LUNs.....</b>	<b>177</b>
LUNs in Project Templates.....	178

LUN Purpose.....	178
LUNs.....	179
Creating an iSCSI LUN.....	179
Creating an FC LUN.....	182
Deleting a LUN.....	184
Managing LUNs.....	185
Expanding the size of a LUN.....	185
Modifying the Protocol of a LUN.....	186
Overriding Compression Type on a LUN.....	186
Overriding Deduplication on a LUN.....	187
Overriding Cache Behavior for a LUN.....	188
Overriding Read only Property for a LUN.....	188
Setting a Management IP Address for a LUN.....	189
Viewing the Purpose of a LUN.....	189
Adding LUN Mappings.....	190
Modifying Space Usage Threshold Levels for a LUN.....	190
<b>Chapter 10: Create a copy of a Share or LUN.....</b>	<b>193</b>
Share or LUN Copy in the Local IntelliFlash System.....	194
Share or LUN Copy on a Remote IntelliFlash System.....	194
Creating share or LUN copies.....	194
Prerequisites for Share or LUN copy creation.....	194
Creating a copy of a share on the current array.....	195
Creating a copy of a share on a remote array.....	196
Creating a copy of a LUN on the current array.....	197
Creating a copy of a LUN on a remote array.....	198
Aborting a share or LUN copy operation.....	199
Share or LUN copy failure scenarios.....	200
<b>Chapter 11: Snapshots and Clones.....</b>	<b>201</b>
Understanding Snapshots and Clones.....	202
Snapshots with Quiesce Option.....	203
Project Level Snapshots.....	204
Snapshot Schedule.....	204
Preset Profiles for Snapshots.....	204
Custom Snapshot Schedules.....	206
Overriding a Project Snapshot Schedule.....	206
Understanding Snapshot Space Usage.....	207
How IntelliFlash takes VMware Consistent Snapshots.....	207
Snapshot Rollback.....	208
Snapshot Deletion.....	209
Best Practices for Configuring Snapshots.....	210
Managing Snapshots.....	210
Adding a Manual Snapshot of a Project.....	210
Adding a Custom Snapshot Schedule for a Project.....	211
Deleting a Frequency of a Project Snapshot Schedule.....	212
Viewing Snapshots Schedule in the Timeline.....	213

Viewing Details of a Project Snapshot.....	213
Viewing Details of a LUN Snapshot.....	214
Viewing Details of a Share Snapshot.....	215
Deleting a Project Snapshot from the Graph view.....	215
Deleting a Project Snapshot from the Table View.....	216
Adding Custom Snapshots Schedule for a Share.....	217
Adding a Manual Snapshot of a Share.....	218
Adding Custom Snapshots Schedule for a LUN.....	218
Adding a Manual Snapshot of a LUN.....	219
Refreshing Snapshots List.....	220
Deleting a Frequency of a Snapshot Schedule for a Share or LUN.....	220
Deleting LUN or Share Snapshots Manually from the Graph View.....	221
Deleting LUN or Share Snapshots Manually from the Table View.....	222
Rolling Back to a Project Snapshot.....	222
Rolling Back to a Share Snapshot.....	223
Rolling Back to a LUN Snapshot.....	224
Rolling Back to a Snapshot with VMware Datastores.....	225
<b>Managing Clones.....</b>	<b>227</b>
Cloning a Project Snapshot.....	227
Cloning a Snapshot of a Share.....	227
Cloning a Snapshot for Creating an iSCSI LUN.....	228
Cloning a Snapshot for Creating an FC LUN.....	232
<b>Chapter 12: NAS Services.....</b>	<b>235</b>
Introduction to Network-Attached Storage (NAS).....	236
Virtualization File Services.....	237
SMB 3.0 Features Overview.....	237
Managing the IP Exclusion List.....	239
Enabling Virtualization File Services.....	240
General File Services.....	241
Multiprotocol NAS Overview.....	241
SMB 3.0 Server Limitations for General and Virtualization File Services.....	244
Configuring the NFS Server.....	244
Authenticating Shares.....	245
Requirements for Using Active Directory with Kerberos for Authentication.....	247
Joining the IntelliFlash Array to an Active Directory Domain.....	249
Configuring IntelliFlash to use Kerberos-based Authentication.....	251
Unconfiguring Kerberos-based Authentication.....	252
Removing the IntelliFlash Array from the Active Directory Domain.....	253
Joining the IntelliFlash Array to a Different Active Directory Domain.....	253
Requirements for Joining the IntelliFlash Array to an LDAP Server.....	254
Joining the IntelliFlash Array to an LDAP Server for User or Group Authentication on NFS Shares.....	254
Applying User-Level ACLs after Configuring an LDAP Server.....	255
Removing the IntelliFlash Array from the LDAP Server.....	256
Editing the Identity Management Details.....	256
User Services.....	256
Introduction to Users Tab.....	256

Adding a New ID Mapping.....	257
Clearing IDmap Cache.....	258
Deleting an ID Mapping.....	258
Adding a Local User.....	259
Deleting a Local User.....	259
Changing a User Password.....	259
Adding a Local User Group.....	260
Deleting a Local User Group.....	260
<b>Chapter 13: NAS Auditing.....</b>	<b>261</b>
NAS Auditing Overview.....	262
NAS Auditing Requirements.....	262
Accessing NAS Auditing Feature in IntelliFlash Web UI.....	263
Enabling NAS Auditing Feature in IntelliFlash Web UI.....	265
Configuring Auditing for SMB Shares through the Windows Client.....	265
Configuring Auditing for NFS Shares through the Windows Client.....	270
Configuring Audit Share Quota.....	271
Configuring Space Usage Threshold Levels.....	271
Configuring Retention Policy of Audit Logs.....	272
Generating XML Audit Logs on Demand.....	272
Enabling SMB Access of Audit Log Share.....	272
Enabling NFS Access of Audit Log Share.....	273
Connecting to Audit Log Share from NFS or SMB Client.....	273
XML Log Reports Examples.....	275
<b>Chapter 14: SAN Services.....</b>	<b>277</b>
Introduction to iSCSI and Fibre Channel.....	278
SAN Services Overview.....	278
LUN Mappings.....	280
Understanding NPIV.....	281
Hardware Requirements for Supporting NPIV.....	281
Support Considerations for NPIV.....	282
Migrating Non-NPIV Projects to NPIV after Upgrading to 3.7.x.x or Later.....	282
iSCSI Page.....	283
Adding an iSCSI Target.....	284
Naming Conventions for iSCSI Targets and Target Groups.....	285
Modifying an iSCSI Target.....	286
Configurable iSCSI Target Properties.....	287
Deleting an iSCSI Target.....	287
Adding an iSCSI Target Group.....	288
Modifying an iSCSI Target Group.....	288
Removing an iSCSI Target Group.....	289
Adding an iSCSI Initiator.....	289
Modifying an iSCSI Initiator.....	290
Deleting an iSCSI Initiator.....	290
Adding an iSCSI Initiator Group.....	290
Modifying an iSCSI Initiator Group.....	291

Removing an iSCSI Initiator Group.....	291
Fibre Channel page.....	291
Adding an FC Initiator.....	292
Modifying an FC Initiator.....	293
Adding an FC Initiator Group.....	293
Modifying an FC Initiator Group.....	294
Removing an FC Initiator Group.....	294
<b>Chapter 15: Live LUN Migration.....</b>	<b>295</b>
Overview of LUN Migration.....	296
Prerequisites for Live LUN Migration.....	296
Scenarios in which migration is not supported.....	297
Project Migration.....	297
Migrating a Project within an Array.....	298
Migrating a Project to a Remote Array.....	299
LUN Migration.....	302
Migrating a LUN within an Array.....	302
Migrating a LUN to a Remote Array.....	303
Monitoring the Migration.....	305
Viewing Migration Status.....	306
Modifying the Migration Configuration.....	307
Manual Cutover.....	308
Aborting a Migration.....	309
Restarting a Migration.....	309
<b>Chapter 16: Synchronous Replication.....</b>	<b>311</b>
Introduction to Synchronous Replication.....	312
Synchronous Replication Considerations.....	312
Synchronous Replication Limitations.....	312
Terms Used in Synchronous Replication.....	313
Quorum Witness Server.....	313
Downloading Quorum Witness Server Installation Package.....	314
Host Requirements.....	314
Installing Quorum Witness Server.....	314
Verifying the Status of Quorum Witness Server.....	316
Obtaining Passphrase for the Quorum Witness Server.....	316
Updating Certificate File.....	317
Cleaning up the Quorum Witness Server.....	318
Setting up Synchronous Replication Configuration.....	318
Editing Synchronous Replication Configuration.....	319
Viewing Synchronous Replication Configuration.....	320
Deleting Synchronous Replication Configuration.....	320
Viewing Synchronous Replication Relationship Details.....	321
Viewing Write Latency Details.....	321
Deleting Synchronous Replication Relationship of a Project.....	322
Disabling Auto Takeover Option.....	322
Manual Takeover Using the Partner Array Web UI.....	322

Manual Giveover Using the Source Array Web UI.....	323
Enabling Auto Failback.....	323

## Chapter 17: Asynchronous Replication..... **325**

Introduction to IntelliFlash Asynchronous Replication.....	327
Terms Used in Asynchronous Replication.....	327
Asynchronous Replication Uses.....	329
How IntelliFlash Replicates Data.....	329
Project-Level Asynchronous Replication.....	330
Ports used for Asynchronous Replication.....	331
Asynchronous Replication Preferred IP Address.....	331
Asynchronous Replication Modes.....	331
Asynchronous Replication Options.....	332
Asynchronous Replication Roles.....	333
Asynchronous Replication Configuration.....	333
Asynchronous Replica Snapshot.....	334
Additional Asynchronous Replica Snapshots.....	334
Asynchronous Replication Snapshots Retention Policy on the Target Array.....	335
Switch Replication Source.....	335
Multi-site Replication Relationships.....	336
Asynchronous Replication Topologies.....	338
Monitoring Asynchronous Replication.....	339
Asynchronous Replication Status Messages.....	339
Asynchronous Replication in an HA Environment.....	339
Asynchronous Replication Relationship During Upgrades.....	340
Reasons for Failure of an Asynchronous Replication Process.....	340
Setting up and Managing Asynchronous Replication.....	341
Replication Prerequisites.....	341
Setting Up a Replication Relationship.....	341
Starting Replication Manually.....	344
Modifying a Replication Options.....	344
Modifying a Replication Schedule.....	344
Pausing Replication.....	345
Resuming a Paused Replication.....	346
Stopping Replication.....	346
Resolving a Conflict Situation.....	346
Switch Replication Source: Target to Source.....	347
Switch Replication Source: Source to Target.....	348
Deleting a Replication Relationship.....	348
Managing outbound Replications systems.....	349
Monitoring Inbound Replication systems.....	350
Adding Replication Target System from Partner Systems Page.....	350
Modifying Replication Target host name or IP address.....	350
Deleting Replication Target System from Partner Systems Page.....	351
Viewing Replication Source Systems from Partner Systems Page.....	351
Managing Asynchronous Replica Projects.....	351
Managing Snapshot Schedule for a Replica Project.....	351
Setting a Quota Limit on a Replica Project.....	352

Setting a Quota Limit on a Share in a Replica Project.....	352
Promoting a Replica Project.....	353
Cloning a Project Snapshot from a Replica Project.....	353
Cloning a LUN Snapshot from a Replica Project.....	354
Cloning a Share Snapshot from a Replica Project.....	355
Deleting a Replica of a Project.....	356
Deleting a Replica of a Share.....	356
Deleting a Replica of a LUN.....	357
<b>Chapter 18: Network Settings.....</b>	<b>359</b>
Understanding the Network Interfaces.....	360
Physical and Logical Network Interfaces.....	360
Types of Logical Network Interfaces.....	360
Understanding Link Aggregates.....	361
Understanding Interface Groups.....	362
Understanding Floating IP Addresses.....	362
Default Interface Groups.....	363
Using the Array Management IP Address.....	363
Unified Configuration of the Network.....	364
General.....	364
Configuring the System Date and Time.....	364
Changing Passwords for Administrator Accounts.....	365
Modifying the Network Settings.....	366
Interface.....	366
Using the Network Interface Page.....	367
Enabling the Unified Interface.....	367
Modifying the Maximum Transmission Unit (MTU).....	368
Adding a Link Aggregate.....	369
Modifying a Link Aggregate.....	370
Deleting a Link Aggregate.....	370
Adding an Interface Group.....	371
Modifying an Interface Group.....	372
Deleting an Interface Group.....	373
SMTP.....	373
Understanding SMTP.....	373
Configuring SMTP.....	373
Certificate.....	374
Securing Communications with TLS/SSL Certificates.....	374
Disabling TLS 1.0.....	375
Generating a Self-Signed Certificate.....	376
Generating a Certificate Signing Request.....	377
Exporting the Current Certificate or Private Key.....	378
Importing a New Certificate or Private Key.....	378
Viewing a CA Certificate.....	379
Deleting a CA Certificate.....	379
Importing a CA Certificate.....	379
Resetting CA Certificates.....	380
Advanced.....	380

Enabling HTTP Proxy Settings.....	380
Enabling SOCKS Proxy Settings.....	381
Adding a Static Route.....	381
Modifying a Static Route.....	382
Deleting a Static Route.....	382
Adding a Local Host.....	382
Deleting a Local Host.....	383
<b>Chapter 19: High Availability Settings.....</b>	<b>385</b>
Setting up High Availability.....	386
High Availability Advanced Settings.....	386
Modifying the High Availability Global Settings.....	387
Configuring the Plugin Management IP Address.....	387
Understanding Quorum Disks.....	387
Refreshing the Quorum Disks.....	388
Switching Over Resource Groups between Controllers.....	388
Manually Setting Resource Groups to Offline.....	389
Manually Setting Resource Groups to Online.....	389
Guidelines for Creating Floating IP Addresses.....	389
Configuring the Floating IP Address.....	390
Removing High Availability Configuration.....	390
<b>Chapter 20: SNMP Settings.....</b>	<b>393</b>
Introduction to SNMP.....	394
Using the SNMP Management Information Base (MIB) File.....	395
Setting Up SNMP Tools.....	395
Downloading MIB File from the IntelliFlash Web UI.....	395
Loading MIB File to NMS or MIB Browser.....	396
Configuring SNMP on the IntelliFlash Web UI.....	396
Enabling SNMP on the IntelliFlash System.....	396
Modifying the Community String.....	396
Adding an SNMP Trap Listener.....	397
Deleting an SNMP Trap Listener.....	397
Sending a Test Trap to SNMP Trap Listeners.....	397
Supported SNMP Traps.....	398
<b>Chapter 21: Administration Settings.....</b>	<b>413</b>
Access and Permissions.....	414
Controlling Access through Accounts and Permissions.....	414
Adding a Role.....	414
Adding a User Account.....	415
Adding Authorities to a Role.....	416
Adding Additional Roles or Authorities to an Account.....	417
Configuring LDAP Accounts to log in to IntelliFlash.....	418
Deleting Authorities from a Role.....	421
Deleting Authorities from a User Account.....	421

Deleting a Role.....	421
Deleting a User Account.....	422
Disabling a User Account.....	422
IntelliFlash Software Upgrade.....	422
Software Upgrade Page.....	423
Pre-Upgrade Health Check on the Array.....	423
Upgrading IntelliFlash Software Using the Software Upgrade Wizard.....	424
Upgrading IntelliFlash Software Manually.....	426
Viewing Upgrade History.....	427
Customer Support.....	428
Adding or Modifying your Contact Details, Array Location, and FRU Shipment Address.....	428
Enabling or Disabling CallHome.....	429
Testing CallHome.....	429
IntelliCare Overview.....	429
Enabling or Disabling IntelliCare.....	430
Testing IntelliCare.....	430
IntelliShell Overview.....	430
Managing IntelliShell.....	430
Disk Encryption.....	432
Enabling Encryption of NVMe Drives.....	432
Encryption Passcode for Securing Data on Pools.....	433
Exporting an Encryption Key.....	435
Importing an Encryption key.....	435
Erasing Data Securely from Encrypted Drives.....	436
Downloading Plugins and SNMP MIB File.....	437
Including a Custom Message in IntelliFlash Login Page.....	438
<b>Chapter 22: Two-Factor Authentication (2FA).....</b>	<b>439</b>
Two-Factor Authentication (2FA) Overview.....	440
Two-Factor Authentication (2FA) Requirements.....	440
Accessing 2FA Feature in IntelliFlash Web UI.....	440
Enabling 2FA in IntelliFlash Web UI.....	441
Disabling 2FA in IntelliFlash Web UI.....	444
2FA Access Privileges.....	446
<b>Chapter 23: MPIO Settings.....</b>	<b>447</b>
Configuring Windows MPIO Settings to IntelliFlash Array.....	448
Adding MPIO on Windows Server 2016, 2019, and 2022.....	448
Windows MSDSM Parameters.....	451
Configuring MPIO Timers using the Device Manager.....	451
Set-MPIOSetting.....	452
<b>Chapter 24: Notifications.....</b>	<b>455</b>
About Notifications.....	456
Notifications Types and Categories.....	456

Notification Example.....	457
Notifications Quick View Window.....	458
Notifications Tasks.....	458
Viewing and Acknowledging Notifications.....	459
Viewing Notification Details.....	460
Filtering Notifications.....	460
Clearing Notification Filters.....	461
Configuring Notification Settings.....	461
Modifying Global Default Settings.....	463
Managing Global Customized Settings.....	463
Viewing Default Event-Level Configurations.....	465
Customizing Event-Level Configurations.....	465
Deleting Customized Event-Level Notifications.....	466
Filtering Notification Configurations.....	466
Modifying Default Space Usage Thresholds.....	467
Adding Custom Space Usage Thresholds.....	468
Modifying Default Meta Usage Thresholds.....	468
Adding Custom Meta Usage Thresholds.....	469
Modifying Time Drift.....	469
Setting Auto Delete for Older Notifications.....	469
<b>Chapter 25: Reporting Services.....</b>	<b>471</b>
Report Types.....	472
Generating Pool Usage Report.....	472
Generating Project Usage Report.....	472
Generating Dataset Report.....	473
Scheduling Reports.....	473
Scheduling Space Usage Reports.....	473
Scheduling Pool Space Usage Report.....	474
Scheduling Project Usage Report.....	474
Scheduling Dataset Space Usage Report.....	475
Editing Scheduled Report.....	475
Deleting Scheduled Report.....	476
<b>Chapter 26: NDMP Server Support.....</b>	<b>477</b>
Introduction to NDMP Server Support.....	478
How the NDMP Backup Works.....	478
Supported NDMP Features.....	479
NDMP Server Page.....	480
Configuring NDMP on an IntelliFlash system.....	481
Considerations for Adding the IntelliFlash System in the NDMP Backup Client.....	481
Backing Up Data from Replication Target through NDMP Client.....	482
Monitoring Active NDMP Backup or Restore Sessions.....	482
Editing NDMP Server Details.....	483
<b>Chapter 27: SMI-S Support.....</b>	<b>485</b>

Introduction to SMI-S.....	486
IntelliFlash SMI-S Server Plugin.....	486
Supported Versions for IntelliFlash SMI-S Server.....	486
Loading SMI-S Server Container Image.....	486
Configuring SMI-S Server Container.....	487
Editing the SMI-S Server Configuration File.....	489
Starting SMI-S Server Container.....	489
Stopping SMI-S Server Container.....	490
Connecting to SMI-S Server from SCVMM.....	490
Viewing Logs for SMI-S Server Plugin.....	490
SMI-S Support for Block Data Access.....	490
Enabling SMI-S and Editing the Default Name Prefixes.....	491
Adding an IntelliFlash system as SMI-S Integrated Storage Device in SCVMM.....	492
Default Settings of LUNs Created using SMI-S.....	493
Configuring an Array as an iSCSI Target for Hyper-V Hosts using SCVMM.....	494
Creating iSCSI Sessions using SCVMM.....	494
Creating LUNs in Existing IntelliFlash Projects using SCVMM.....	495
Creating and Mapping a LUN as a Shared Volume using SCVMM.....	495
Viewing LUNs.....	497
Unmapping a LUN.....	497
Deleting LUNs with SCVMM.....	497
Working with IntelliFlash Clones in SCVMM.....	498
Deleting Clones with SCVMM.....	498
Creating an SCVMM Library Share.....	498
Creating a VM.....	499
Converting a VM to a Template.....	500
Deploying a VM Template Using SAN Copy.....	500
Hyper-V Host-to-Host VM Migration with SCVMM and SMI-S.....	502
SMI-S Support for SMB 3.0 Shares.....	503
Adding SMB 3.0 Shares in SCVMM.....	503
Adding SMB 3.0 Shares to the SCVMM Library.....	505
Adding SMB 3.0 Share to a Hyper-V Host.....	505
Adding a Virtual Hard Disk to SCVMM Library.....	505
Creating a VM from a Blank Virtual Hard Disk.....	506
Creating a VM using Existing VM, VM Template, or Virtual Hard Disk File.....	507
Converting a VM to a Template.....	509
Migrating VMs between Hyper-V Hosts.....	509
<b>Chapter 28: IntelliFlash Manager Plugin.....</b>	<b>511</b>
About IntelliFlash Manager plugin.....	512
IntelliFlash Manager plugin support for Linked vCenter Servers.....	513
Supported VMware vCenter Server versions for the IntelliFlash Manager plugin... .....	513
IntelliFlash Manager plugin backward compatibility support.....	513
Managing the VMware vCenter Server.....	514
VMware Servers Page.....	514
Adding a vCenter Server.....	515
Editing vCenter Server details.....	516
Refreshing the VMware Servers page.....	517

Removing a vCenter Server from the VMware Servers page.....	517
Installing the IntelliFlash Manager plugin on a vCenter Server.....	518
Upgrading the IntelliFlash Manager plugin.....	519
Uninstalling the IntelliFlash Manager plugin on a vCenter Server.....	519
Resolving network Issue.....	519
Accessing the ESXi host settings from the IntelliFlash Web UI.....	520
Using the IntelliFlash Manager plugin.....	521
Accessing the IntelliFlash Manager plugin.....	522
Registering a new IntelliFlash Array.....	522
Viewing the Summary of an array.....	523
Editing array details to update credentials.....	524
Unregistering an array.....	524
Host settings.....	524
Accessing ESXi hosts on the vCenter server.....	526
Installing IntelliFlash NAS VAAI Plugin using IntelliFlash Manager plugin.....	526
Uninstalling the IntelliFlash NAS VAAI Plugin using IntelliFlash Manager plugin....	526
Multipathing rules.....	527
Setting ESXi Host Settings from the IntelliFlash Manager plugin.....	528
Datastores management.....	535
Adding a NAS datastore using the IntelliFlash Manager plugin.....	535
Adding a SAN datastore using the IntelliFlash Manager plugin.....	536
Resizing a NAS or SAN datastore using the IntelliFlash Manager plugin.....	537
Viewing datastores.....	538
Viewing storage performance of a datastore.....	539
Filtering datastores.....	539
Accessing datastores.....	539
Deleting datastores.....	540
Snapshots and Clones management.....	540
Viewing snapshots of a datastore.....	541
Creating a manual snapshot of a datastore.....	542
Cloning a snapshot of a datastore.....	542
Rolling back to a snapshot.....	543
Deleting a snapshot of a datastore.....	544
Virtual machines management.....	545
Viewing all virtual machines on an array.....	545
Viewing virtual machines inside a datastore.....	546
Accessing virtual machines in a datastore.....	547
Viewing storage performance of a virtual machine.....	547
Cloning a virtual machine using the Hyperclone option.....	548
Role-based access control in the IntelliFlash Manager plugin.....	550
Privileges for sample roles in IntelliFlash Manager plugin.....	550
Adding additional privileges for the IntelliFlash Manager plugin sample roles.....	552
<b>Chapter 29: IntelliFlash Storage Replication Adapter.....</b>	<b>555</b>
Overview of IntelliFlash Storage Replication Adapter (SRA).....	556
Prerequisites for Installing IntelliFlash SRA.....	557
Installing and Connecting Site Recovery Manager Instances on Protected and Recovery Sites.....	557

Predefined SRA Role for Site Recovery Manager (SRM).....	557
Setting up Additional Configurations.....	557
Installing Containerized IntelliFlash SRA 2.0.0 Plugin.....	558
Prerequisites for the Containerized IntelliFlash SRA 2.0.0 Plugin.....	558
Installing Containerized IntelliFlash SRA 2.0.0 Plugin.....	558
Uninstalling Containerized IntelliFlash SRA 2.0.0 Plugin.....	559
Configuring Array Managers in VMware Site Recovery Manager (SRM).....	560
Discovering Devices in Site Recovery Manager.....	561
Create, Test, and Run Recovery Plan.....	562
Create Array Based Replication Protection Group.....	562
Create a Recovery Plan.....	562
Perform a Planned Recovery or Disaster Recovery.....	562
Reprotect After Recovery.....	562
<b>Chapter 30: IntelliFlash Plugin for Veeam Backup and Replication... 563</b>	
About IntelliFlash Plugin for Veeam Backup and Replication.....	564
How the IntelliFlash Plugin for Veeam Backup and Replication works.....	564
Veeam Snapshots.....	564
Tasks you can perform using the IntelliFlash Plugin for Veeam Backup and Replication.....	565
Prerequisites for using the IntelliFlash Plugin for Veeam Backup and Replication.....	566
Adding a Veeam User Account on the IntelliFlash Array.....	566
Downloading the IntelliFlash Plugin for Veeam Backup and Replication.....	567
Installing IntelliFlash Plugin for Veeam Backup and Replication.....	567
Adding IntelliFlash Array to IntelliFlash Plugin for Veeam Backup and Replication.....	568
Remove the array using the IntelliFlash Plugin for Veeam Backup and Replication.....	569
<b>Chapter 31: IntelliFlash NAS VAAI Plugin for VMware..... 571</b>	
IntelliFlash NAS VAAI Plugin for VMware.....	572
IntelliFlash NAS VAAI Plugin Limitations.....	572
Supported NAS VAAI Primitive.....	572
Managing the IntelliFlash NAS VAAI Plugin.....	573
Prerequisites for Installing the IntelliFlash NAS VAAI Plugin.....	573
Installing IntelliFlash NAS VAAI Plugin using IntelliFlash Manager plugin.....	573
Uninstalling the IntelliFlash NAS VAAI Plugin using IntelliFlash Manager plugin....	574
Installing IntelliFlash NAS VAAI Plugin Using the ESXi Server CLI.....	574
Installing the IntelliFlash NAS VAAI Plugin using the VMware vSphere Update Manager.....	576
Uninstalling the IntelliFlash NAS VAAI Plugin using the ESXi Server CLI.....	576
<b>Chapter 32: Cloud Connect..... 577</b>	
Backing up Data to S3-Compliant Cloud Targets.....	578
Terms Used in Cloud Connect.....	578
Uses of Cloud Connect for Backup.....	578
Configuring Cloud Connect.....	579
Adding a Cloud Target.....	579

Configuring Backup for a Project.....	583
<b>Managing Active Backups.....</b>	<b>586</b>
Viewing All Active Backups.....	586
Viewing Active Backups in a Specific Project.....	587
Viewing Backup Configuration Details.....	587
Starting Backups Manually.....	588
Starting Backups Manually for a Specific Project.....	588
Aborting Backups.....	589
Pausing Backups.....	589
Resuming Paused Backups.....	590
Deleting a Cloud Backup Configuration.....	590
Modifying Cloud Backup Configuration.....	591
Searching for Backup Targets.....	591
Restoring Cloud Backup of a Specific Project Within the Same Array.....	591
Restoring Cloud Backups Within the Same Array.....	592
Restoring Cloud Backups to a Different Array.....	593
Backing up and Restoring Data through 10G Interfaces.....	594
Deleting a Cloud Backup.....	595
<b>Chapter 33: IntelliFlash PowerShell Toolkit Overview.....</b>	<b>597</b>
Introduction to IntelliFlash PowerShell Toolkit.....	598
<b>Chapter 34: IntelliFlash Data Protection Services (IDPS).....</b>	<b>599</b>
Introduction to IntelliFlash Data Protection Services (IDPS).....	600
Components of the Backup Solution for Windows Hosts.....	601
How IDPS Works.....	602
How IDPS Works in a Physical Windows Environment.....	603
How IDPS Works in an Hyper-V Environment.....	603
How IDPS Works in a VMware Environment.....	606
Guidelines for Creating LUNs or Shares for Application-consistent Backup with IDPS....	607
Installing and Setting Up IDPS.....	607
Downloading the IDPS Installer.....	608
Running the IDPS Installer.....	608
Registering IDPS-enabled Windows Clients on the Array.....	610
Adding the IDPS PowerShell SnapIn.....	611
Managing IDPS Connections to Arrays.....	612
Adding a Storage System Connection.....	612
Editing a Storage System Connection.....	614
Removing a Storage System Connection.....	614
Updating IDPS.....	615
IDPS PowerShell Cmdlets.....	615
Using the IDPS PowerShell Cmdlets to Update IDPS.....	616
IDPS Support Log Utility.....	617
IDPS Support Log Utility Functions.....	617
Configuring Logging for IDPS.....	619
Configuring Microsoft SQL Server Logins.....	619
Troubleshooting Storage Connection Configurations.....	620

Collecting Log Files.....	621
Reproducing the Problem.....	621
Uploading Compressed Files.....	622
Manually Uncompressing Logs.....	623
Restoring Snapshots and LUNs created by IDPS.....	623
Converting VSS Snapshots to Read/Write through the Web UI.....	624
Converting VSS Snapshots to Read/Write through the Diskpart Utility.....	625
Adding a Cloned LUN to a Microsoft Failover Cluster.....	627
Recovering Hyper-V VMs.....	628
<b>Appendix A: IntelliFlash Support Logs and IntelliCare Data.....</b>	<b>631</b>
IntelliFlash Log Files and Analytics Data Files.....	632
<b>Appendix B: NDMP Backup Configuration for Netbackup 8.1 and Commvault V11.....</b>	<b>635</b>
NDMP Backup Configuration with NetBackup 8.1.....	636
NDMP Backup Configuration with Commvault V11.....	640
<b>Appendix C: IntelliFlash 3.11.6.2 Interoperability Matrix.....</b>	<b>647</b>
Interoperability Matrix IntelliFlash 3.11.6.2.....	648



---

# Preface

---

## Audience

---

The IntelliFlash User Guide contains detailed information about using and managing IntelliFlash H-Series Hybrid Flash Storage Systems and N-Series NVMe-Flash Storage Systems through the IntelliFlash Web UI and related plugins.

This guide is intended for storage administrators who are familiar with data storage concepts, methods, and protocols, such as pools, LUNs, deduplication, NAS, SAN, NFS, SMB iSCSI, and Fibre Channel.

## IntelliFlash Documentation

---

The following table lists the technical documentation library available for the IntelliFlash systems.

**Table 1: IntelliFlash Documentation**

Name	Description
IntelliFlash N-Series N6100/N6200 NVMe Storage Systems Hardware Guide	Contains detailed descriptions, hardware specifications, and rack installation instructions for the N-Series N6100/N6200 NVMe Storage Systems.
IntelliFlash H-Series H6100/H6200 Hybrid Storage Systems Hardware Guide	Contains detailed descriptions, hardware specifications, and rack installation instructions for the H-Series H6100/H6200 Hybrid Storage Systems.
IntelliFlash User Guide	Contains detailed instructions on how to configure, use, and administer IntelliFlash H-Series Hybrid Storage Systems and N-Series NVMe Storage Systems.
IntelliFlash API Reference	Contains detailed descriptions of the IntelliFlash REST APIs.
IntelliFlash Configuration Guide	Contains instructions on configuring IntelliFlash arrays.
IntelliFlash CSI File Driver User Guide	Contains instructions on installing and using the CSI File driver.
IntelliFlash Release Notes	Contains information about new features, enhancements, fixed issues, and known issues in IntelliFlash releases.

Name	Description
IntelliFlash PowerShell Toolkit Guide	Contains information about IntelliFlash PowerShell Toolkit.

## Support

---

IntelliFlash support services give you access to online, telephone, and onsite support. IntelliFlash support provides multiple levels of support through a Technical Support team and Field Engineers. For details on support offerings, contact your account team.

## Revision History

---

**Table 2: Revision History**

Date	Description
November 28, 2023	Added Appendix C "IntelliFlash 3.11.6.2 Interoperability Matrix."
June 30, 2023	Updates for IntelliFlash 3.11.6.0. <ul style="list-style-type: none"> <li>• Updated the "Pools" chapter.</li> <li>• Added Appendix C "IntelliFlash 3.11.6.0 Interoperability Matrix."</li> </ul>
April 17, 2023	Updates for IntelliFlash 3.11.5.0. <ul style="list-style-type: none"> <li>• Updated the section "Creating a New Pool" to include mixed NVMe drive configuration details.</li> <li>• Added a new chapter "Two-Factor Authentication (2FA)".</li> <li>• Updated the section "NAS Auditing Overview"</li> <li>• Added support for VMware vSphere version 8.0.</li> <li>• Updated the "Commvault" section in Appendix B.</li> <li>• Added Appendix C "IntelliFlash 3.11.5.0 Interoperability Matrix."</li> <li>• Removed the chapter "Installing Windows IntelliFlash SRA 1.0.3 Plugin"</li> </ul>
December 16, 2022	Updates for IntelliFlash 3.11.4.2. <ul style="list-style-type: none"> <li>• Added a new chapter "MPIO Settings".</li> <li>• Added Appendix B "NDMP Backup Configuration for NetBackup 8.1 and Commvault V11".</li> <li>• Added Appendix C "IntelliFlash 3.11.4.2 Interoperability Matrix."</li> <li>• Removed the "IntelliFlash Object Data Manager Plugin for AIX" chapter.</li> </ul>

Date	Description
August 5, 2022	Updates for IntelliFlash 3.11.4.0.
February 23, 2022	Updates for IntelliFlash 3.11.3.0.
September 27, 2021	Updates for IntelliFlash 3.11.2.0.
March 5, 2021	Updates for IntelliFlash 3.11.1.0.

---

# Chapter 1

---

## Introduction to IntelliFlash Systems

---

**Topics:**

- *Components in IntelliFlash Storage Arrays*
- *IntelliFlash Operating Environment*

## Components in IntelliFlash Storage Arrays

---

All IntelliFlash arrays feature dual controllers, redundant hardware, and multipathing support for resiliency and high system availability. All IntelliFlash arrays support SAN and NAS protocols for block and file access to data. You can scale storage capacity by adding expansion shelves.

### Dual Controllers

IntelliFlash arrays have dual controllers. In the event of a controller failure, the storage pools on the controller can automatically and transparently fail over to the other controller with no disruption to data access. You can also manually fail over the storage pool on a controller to the other controller, if required.

### Redundant Hardware

IntelliFlash arrays include redundant fans and power supplies. Media in the arrays can be configured with various levels of redundancy. All of these components also have hot plug capabilities.

### Multiprotocol

IntelliFlash arrays support both block and file protocols. You can access data over iSCSI, Fibre Channel, NFS, and SMB. You can configure the array to access multiple protocols simultaneously.

Depending on the protocols that you want to use, you can opt for quad-port 1 GbE, dual-port or quad-port 10 GbE, dual-port 40 GbE, 4/8 G (dual-port) or 16G (dualport or quad-port) Fibre Channel (FC) cards.

### Multiprotocol for NAS

IntelliFlash supports multiprotocol NAS to access data from different clients providing storage efficiency, high performance, and scalability to petabytes. In a multiprotocol NAS environment, IntelliFlash array acts as a single data store to Unix and Windows clients and the users can access their data from different protocols. In addition, IntelliFlash provides two SMB server modes; General File Services and Virtualization File Services.

### Multipathing

The arrays support multiple redundant paths between server hosts and the storage array for both SAN and NAS protocols.

### Capacity Expansion

You can expand storage capacity when needed by simply adding SAS-connected hybrid or all flash expansion shelves. Adding expansion shelves is a non-disruptive operation. You can create new storage pools with the added capacity or expand the capacity of existing pools.

When expanding the capacity of existing pools, the expansion shelves can consist of larger disks than the head controller disks. When adding disks to an expansion shelf that already has disks,

the new disks can be of larger size than the existing disks. IntelliFlash does not support disks of lower capacity than the existing drives when expanding pools.

## IntelliFlash Operating Environment

---

All IntelliFlash systems are powered by IntelliFlash Operating Environment, which provides the same feature set and a uniform user experience across the storage product lines.

This fast, flexible operating environment is designed to leverage different grades of storage media—hard disk, high-performance flash, high-density flash, and so on—with the same storage system. IntelliFlash Operating Environment understands the inherent characteristics of the different storage media and intelligently manages the placement of data for optimal performance. It also includes advanced data services, multiprotocol support, and flexible management capabilities, enabling you to accelerate performance, significantly shrink your storage footprint, maximize uptime, consolidate workloads, and simplify storage administration.

The following are key features of the IntelliFlash Operating Environment:

- Media management
- Advanced data services
- Protocol choice
- Management flexibility

### Media Management

The IntelliFlash architecture provides the foundation for reliably storing data on different types of storage media and optimizing the use of media within the storage system to boost performance, protect against data corruption, and extend the life of the system's media.

- **Metadata Acceleration**—Patented metadata acceleration technology aggregates metadata that includes block pointers and deduplication tables, and places the aggregated metadata on logically isolated, high performance media for optimizing I/O paths and accelerating all I/O operations in the array.
- **Dynamic Caching**—Intelligent caching algorithms keep the most frequently accessed data in the Read Cache, which resides on DRAM and flash (for Hybrid arrays). The data cached in flash media is stored in a compressed format to give you more available cache space with no performance degradation. These caching algorithms are optimized for various I/O patterns and dynamically adapt to differing media latencies across multiple levels of cache. The array proactively fetches and populates the read cache with the hottest data. This happens dynamically in real time using intelligent, pre-fetch algorithms without user intervention.
- **Data Integrity**—To protect against silent data corruption, the IntelliFlash Operating Environment performs a checksum process to match data blocks for reads and writes and automatically fixes corrupt blocks. It also stores the checksum and data in separate nodes of the block tree for further protection.
- **Flash Endurance**—IntelliFlash aligns writes to the geometry of the flash media, ensuring even wear and extending the life of the system's flash drives. IntelliFlash is optimized for the underlying geometry of the medium (flash or disk) to ensure long life even under high I/O workload.

## Advanced Data Services

The IntelliFlash Operating Environment includes a full suite of advanced data services.

- **Data Reduction**—IntelliFlash provides inline compression and deduplication. Data is compressed and redundant blocks are removed before they are written to disk. These techniques not only reduce the storage footprint, they also act as a performance multiplier by maximizing the amount of data cached in high-speed media.
- **Data Protection**—Built-in snapshots, replication, and instant restore capabilities provide efficient methods of disaster recovery. You can also create read/write clones. Clones are space-efficient: similar to snapshots, they allocate storage only for changed blocks. Application awareness and integration provides VM and application-consistent snapshots for backup and recovery.
- **Disaster Recovery**—Replication functionality in the IntelliFlash Operating Environment enables you to replicate data between All Flash Arrays, between Hybrid Arrays, or between All Flash and Hybrid Arrays for a cost-effective DR solution.
- **Data Security**—To keep sensitive data secure, IntelliFlash delivers inline encryption of data on flash and hard disk drives with no impact on performance and data reduction. Data is also encrypted during replication across sites.

## Protocol Choice

IntelliFlash natively supports both block and file access, so you can meet the needs of different workloads, and consolidate workloads on a single array. The IntelliFlash architecture is also extensible so that other protocols can easily be added in the future.

## Management Flexibility

IntelliFlash includes flexible management capabilities to streamline and simplify storage management.

- **Web UI**—IntelliFlash offers a web-based user interface for configuring, managing, and monitoring IntelliFlash systems. Its dashboard lets you quickly and easily monitor space usage, performance, cache hits, CPU hits, and network throughput. Application-optimized templates simplify provisioning. You can use these templates to choose the type of workload and IntelliFlash will preselect the optimum configuration properties for the LUNs and shares. Advanced settings are also available to customize and fine tune storage attributes and properties.
- **Call-Home Alerts**—IntelliFlash provides pro-active capacity and health alerts. Notifications are automatically sent to IntelliFlash Technical Support and support cases are created for critical alerts. You can configure the arrays to send email notifications to other appropriate personnel.
- **VM Management**—IntelliFlash systems can be managed through VMware vCenter, enabling you to provision datastores, manage snapshots and restores, and monitor I/O status, space usage and latency from within the vCenter interface.
- **RESTful API**—A programmable, task-oriented RESTful API enables you to script and automate storage management.
- **Cloud Monitoring and Analytics (IntelliCare)**—IntelliFlash includes an opt-in feature that allows IntelliFlash systems to send capacity, performance, and health-related statistics and notifications to the cloud-based, analytics portal of Tintri. The IntelliCare cloud portal uses

this data to allow you to quickly and easily monitor the health, performance, and usage of all your IntelliFlash systems from anywhere. The portal also provides trend analysis for storage consumption for pro-active capacity planning. A separate portal presents analytics to IntelliFlash Technical Support for pro-active customer care.



---

## Chapter 2

---

### Unified IntelliFlash Web UI

---

**Topics:**

- [\*Logging in to the IntelliFlash Web UI\*](#)
- [\*Logging out from the IntelliFlash Web UI\*](#)
- [\*System Information Window\*](#)

The IntelliFlash Web UI provides unified access to both controllers of the IntelliFlash Array. It enables you to configure, monitor, and manage both controllers. You can view system settings, analytics, and notifications for both controllers. You can also apply the same configuration settings on both controllers.

You can access the IntelliFlash Web UI using the array management name or IP address. See [\*Using the Array Management IP Address\*](#).

## Logging in to the IntelliFlash Web UI

---

Prerequisites to log in to the IntelliFlash Web UI:

- Complete the initial configuration of the array using the Configuration Wizard (CW).
- Use one of the following Web browsers to access the IntelliFlash Web UI:

Browser	Version
Google Chrome	57.0 or later
Mozilla Firefox	53.0 or later
Safari	10.0 or later
Microsoft Edge	40.15063.0 or later

- (Recommended) Enable the TLS 1.2 protocol on the Web browser you are using to access the IntelliFlash Web UI.

To log in to the IntelliFlash Web UI, complete the following steps:

1. Enter the array management host name (FQDN) or IP address of the array in the address bar of the Web browser.

The login page of the IntelliFlash Web UI appears.

 **Note:** Access the IntelliFlash Web UI using the array management IP address or host name. If you have provided the IP address or host name of one of the controllers, a **Redirect Confirmation** dialog box appears. Click **Yes** to redirect to the array management IP address or host name. If you want to continue using the controller, click **No**. Select **Remember this choice** before clicking **Yes** or **No** for the system to remember your choice.

2. Enter the **Username** and **Password**.

 **Note:**

- Enter the credentials specified during the initial configuration of the array.
- If LDAP is configured on IntelliFlash Web UI, LDAP users can log in to the array using LDAP credentials.

3. Click **Login**.

When you log in to the IntelliFlash Web UI for the first time, the **Terms of Service** screen appears. You must accept the terms of service to use the IntelliFlash Web UI.

## Logging out from the IntelliFlash Web UI

 **Note:** When you cold reboot your array (rebooting both controllers in the array) and if you have provided an encryption passcode, the IntelliFlash Web UI prompts you to provide the **Encryption Passcode** when you log in after the reboot.

To log out from the IntelliFlash Web UI, complete the following steps:

1. Click the array name at the top-right corner of the IntelliFlash Web UI.  
The **System Information** window appears.
2. In the **Information** tab, click **Logout** at the bottom-right corner.  
You are redirected to the IntelliFlash Web UI login page.

## System Information Window

The **System Information** window includes information about the IntelliFlash system controllers. To view the **System Information** window, click the array name at the top-right corner of the IntelliFlash Web UI menu bar.

The **System Information** window consists of the following tabs:

- *Information tab*
- *Support tab*
- *Help tab*
- *System Operations list*

### Information tab

The Information tab displays the following details.

- **Array Information**
  - **IntelliFlash OS Version:** The IntelliFlash Operating Environment version installed on the IntelliFlash system controller.
  - **Array Management IP:** The IntelliFlash system management IP address.
  - **Hardware Model:** The IntelliFlash system hardware model name.
  - **Processor:** Details of the type and the number of processors installed in the IntelliFlash system.
  - **Memory (DRAM):** Total size of the memory (DRAM) installed in the IntelliFlash system.
  - **Disks:** Number of disks, type of disks, and their sizes in the IntelliFlash system and the attached expansion shelves, if any.

- **GUID:** Globally unique identifier number.
- **Controller-A Information**
  - **Controller-A Serial:** Serial number of Controller-A.
  - **Controller-A IP:** Controller management IP address of Controller-A.
  - **Uptime:** The amount of time (in number of days, hours, and minutes) Controller-A has been successfully running.
- **Controller-B Information**
  - **Controller-B Serial:** Serial number of Controller-B.
  - **Controller-B IP:** Controller management IP address of Controller-B.
  - **Uptime:** The amount of time (in number of days, hours, and minutes) Controller-B has been successfully running.
- **User Information**
  - **User name:** Displays the name of the user.
  - **User role:** Displays the role of the user.
  - **Last Logged in:** Displays when the user last logged (in day, month, date, time, time zone, year).

## Support tab

IntelliFlash might generate email notifications that are redundant during a planned maintenance activity. You can disable these email notifications by enabling the maintenance mode in the **Support** tab.

The Support tab also helps you to check the health of the IntelliFlash system. Use the **Check Now** option to check the health of the IntelliFlash system.

The tab displays the last health status, and the date and the time the last health check was done.

The status of the IntelliShell sessions also appears in the **Support** tab. You can view this status only when IntelliShell is enabled and a support engineer is accessing the array.

## Help tab

The Help tab consists of the following sections:

- **User Docs:** Includes the User Guide and the API Guide.
- **What's new (Quick Tour):** Provides information about the major new features added in the current version of the IntelliFlash OS.
- **Terms of Service:** Displays the end user license agreement.

## System Operations list

The System Operations list is a menu link in the **System Information** window that enables you to:

- Access the BMC interface of each controller.
- Reboot each controller.
- Power off each controller.

## Enabling Maintenance Mode

IntelliFlash might generate email notifications that are redundant during a planned maintenance activity. You can disable these email notifications by enabling the maintenance mode from the IntelliFlash Web UI.

When the maintenance mode is enabled, all alerts are shown only in the **Notifications** page. No email notification is sent. If maintenance mode is not disabled within two hours from the time it is enabled, IntelliFlash disables it automatically.

To enable or disable the system maintenance mode, complete the following steps:

1. Click the array name at the top-right corner of the IntelliFlash Web UI.  
The **System Information** window appears.
2. In the **System Information** window, click the **Support** tab.
3. In the **Support** tab, drag the **Maintenance Mode** toggle button to the right to enable system maintenance mode.  
The **Maintenance Mode** toggle button appears in green. To disable the system maintenance mode, drag the button to the left.

## Viewing IntelliShell Session Status

Enabling IntelliShell allows administrative access to the array as long as the session is open. When IntelliShell is enabled, the status of the IntelliShell session appears in the **Support** tab.



**Note:** To enable the IntelliShell feature, see [Enabling or Disabling IntelliShell](#).

To view the status of the session, complete the following steps:

1. Click the array name at the top-right corner of the IntelliFlash Web UI.  
The **System Information** window appears.
2. In the **System Information** window, click the **Support** tab.
3. In the **Support** tab, the following information appears:
  - **Active Users:** The number of users currently logged in to your array.
  - **Login Duration:** The duration of the session.

## Accessing Online Help

IntelliFlash systems include online help that you can access from the IntelliFlash Web UI. The online help includes the IntelliFlash User Guide and the IntelliFlash API Reference.

To access online help, complete the following steps:

1. Click the array name at the top-right corner of the IntelliFlash Web UI.  
The **System Information** window appears.
2. In the **System Information** window, click the **Help** tab.
3. In the **Help** tab, you can do one of the following:
  - Click **User Docs** to access user documentation.
  - Click **What's new (Quick Tour)** to view information about the new features added in the current version of the IntelliFlash Operating Environment.
  - Click **Terms of Service** to view the end user license agreement.

When you click **User Docs**, the **Documentation** page opens in a new tab. In the **Documentation** page, click the format type (PDF or HTML) of the guide you want to access. The document opens in a new tab.

## Accessing BMC from the IntelliFlash Web UI

To access the BMC interface of either controllers, complete the following steps:

1. Click the array name at the top-right corner of the IntelliFlash Web UI.  
The **System Information** window appears.
2. In the **System Information** window, click the **System Operations** list at the bottom-left corner.
3. In the **System Operations** list, under the **KVM** section, click the controller for which you want to access the BMC interface.  
The BMC interface of the controller appears in a new tab.

## Rebooting an IntelliFlash system Controller

The reboot option enables you to select and reboot an IntelliFlash system controller. When you reboot a controller, the pools and floating IP addresses on that controller fail over to the other controller. If you reboot the controller to which the Web UI is connected, the Web UI switches over to the other controller.



**Note:** Before you reboot a controller, you should manually switch over all the resources to the other controller from the **Settings > High Availability** page. For more information, see [Switching Over Resource Groups between Controllers](#).

To reboot an IntelliFlash system controller, complete the following steps:

1. Click the array name at the top-right corner of the IntelliFlash Web UI.

The **System Information** window appears.

2. In the **System Information** window, click the **System Operations** list at the bottom-left corner.
3. In the **System Operations** list, under the **Reboot** section, click the controller you want to reboot.
4. In the Confirmation dialog box, click **Yes**.

The selected controller is rebooted.

 **Note:** If you are rebooting the current controller, the IntelliFlash Web UI may be unresponsive for some time until the Web UI is loaded again.

## Powering off an IntelliFlash system Controller

The **Power off** option enables you to power off an IntelliFlash system controller.

 **Note:** To power on the controller again, use the BMC interface.

To power off an IntelliFlash system controller, complete the following steps:

1. Click the array name at the top-right corner of the IntelliFlash Web UI.  
The **System Information** window appears.
2. In the **System Information** window, click the **System Operations** list at the bottom-left corner.
3. In the **System Operations** list, under the **Power off** section, click the controller you want to power off.
4. In the Confirmation dialog box, click **Yes**.

The selected controller is powered off.



---

# Chapter 3

---

## Dashboard

---

### Topics:

- *Dashboard sections*
- *Dashboard variations*
- *Viewing pool or array performance details*
- *Viewing pool or array space saving and capacity*
- *Viewing Top 10 or Bottom 10 LUNS, Shares, or VMs with maximum or minimum workload*
- *Viewing CPU and cache hits usage of the array*

The **Dashboard** in the IntelliFlash Web UI provides you with a quick view of the space utilization and performance based on the protocols used for individual pools on the array, and the array as a whole. It lists the top ten or bottom ten LUNs, shares, or virtual machines with storage operations (latency, IOPs, throughput) after applying a filter. You can also view the CPU usage and cache hits percentage per controller.

The **Dashboard** provides uses easy-to-read charts, ratios and percentages, and plain numbers to display metrics related to space utilization and performance.

If you have not created any pools when configuring your IntelliFlash Array, the **Dashboard** allows you to create pool from the **Dashboard** itself. The **Dashboard** UI also allows you to create a project if it does not exist on your array.

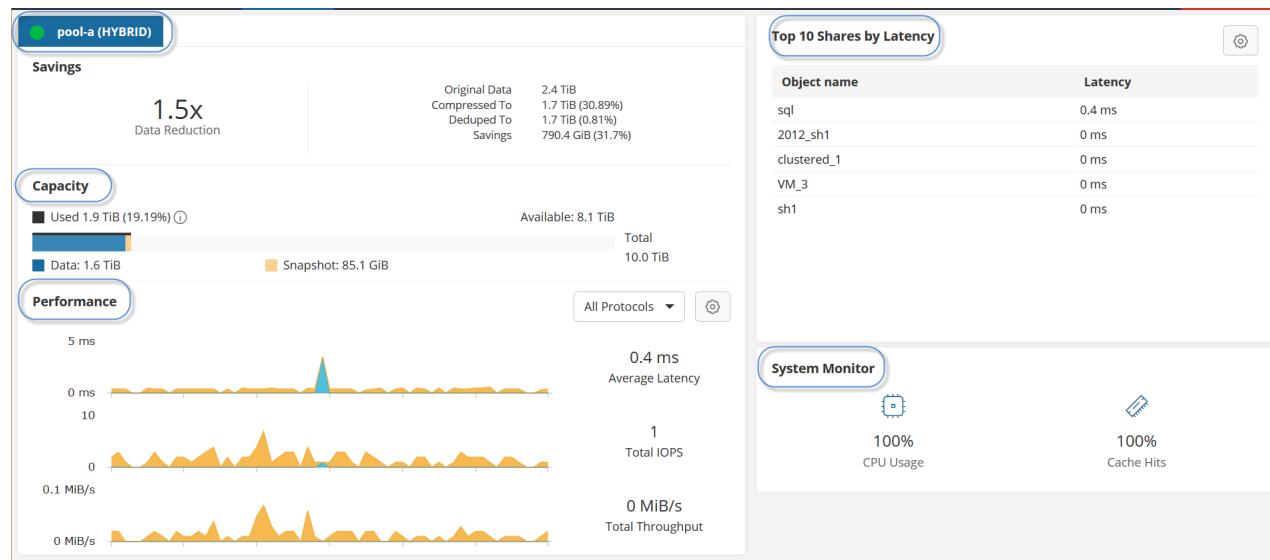
## Dashboard sections

The **Dashboard** has three different sections to provide information on different aspects of your array.

**Note:** The three sections of the **Dashboard** will show details for an individual pool or the array itself based on your tab selection (**Array** or pool name).

- The first vertical section on the left hand side has three subsections under the *pool name* tabs and the **Array** tab:
  - **Saving**
  - **Capacity**
  - **Performance**
- The first section on the right hand side of the **Dashboard** displays the **Top 10** or **Bottom 10** LUNs, shares, or virtual machines by high or low workload depending on the applied filter.
- The second section at the bottom-right, **System Monitor**, displays the CPU and cache hits usage percentage.

The following image shows an example of the various sections and subsections of the **Dashboard**.



### Related Topics

[Array tab and pool name tabs](#)

[Savings](#)

[Capacity](#)

[Performance](#)

[Storage objects with Top 10 or Bottom 10 workloads](#)

## [System Monitor](#)

### [Dashboard variations](#)

## Array tab and pool name tabs

The **Array** tab and pool name tabs are part of the first vertical section of the dashboard.

 **Note:** The **Array** tab is displayed only if the array has two or more pools.

### Array tab

The **Array** tab displays the metrics for the array as a whole. These metrics are aggregates and averages of the pool-level metrics.

### Pool name tabs

The pool tabs display the pool name itself as the tab name and pool type in brackets. The pool type can be:

- **HYBRID**
- **SSD**



The pool tabs also display the pool status depending on the set space usage threshold. The color of the icon in the pool tab changes when the space utilization crosses a threshold that you have set:

- **Green:** Indicates the pool's space usage remains within the set threshold levels.
- **Amber:** Indicates the pool's space usage has crossed the warning threshold.
- **Red:** Indicates the pool's space usage has crossed the critical threshold.



**Figure 1: Pool name tab with the warning threshold**

You can click the pool name to view details of an individual pool.



**Figure 2: Pool name tab with the critical threshold**

## Related Topics

[Dashboard sections](#)

## Savings

The **Savings** subsection of the **Dashboard** displays the following details both by size and percentage for the selected pool or the array.

- **Original Data:** The original data size is the size of the data before performing compression or deduplication.
- **Compressed To:** This is the data size after running compression. Compression is performed on the original data size. The percentage is calculated as: Compressed To percentage (%) = Difference between original data and compressed/original data size \* 100
- **Deduped To:** This is the data size after running deduplication. Deduplication is performed on the compressed data size. The percentage is calculated as: Deduped To Percentage = (Space saved due to deduplication / (Space used after compression + Space saved from compression)) \* 100
- **Savings:** Savings is the amount of space saved after compression and deduplication in the entire array. The percentage is calculated as: Savings percentage (%) = Space savings data size/original data size \* 100  
Savings = original data size - deduplicated data size
- **Data Reduction:** The data reduction ratio shows the ratio of the original data to the space used after deduplication and compression.

This ratio is calculated as:

Data reduction = original data size / data size after deduplication

**Figure 3: Example of Savings subsection for an array**



## Related Topics

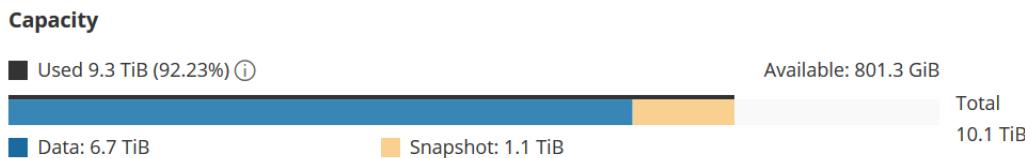
[Dashboard sections](#)

## Capacity

The **Capacity** subsection of the **Dashboard** displays the following on a horizontal bar graph for the selected pool or the array:

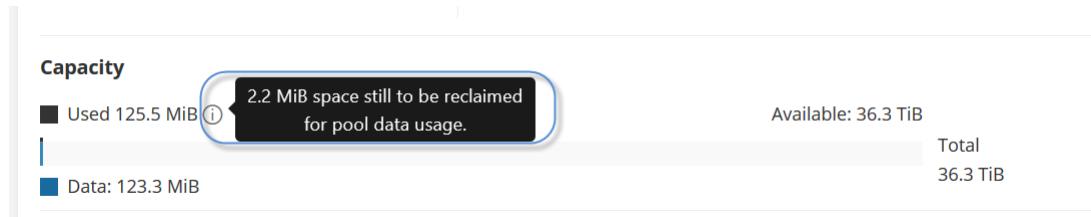
- **Total:** The total amount of space in the pool is shown as a number and is also represented as the length of the chart.
- **Available:** The amount of space available in the pool is shown as a number and is also represented by the empty part of the chart.
- **Used:** The amount of space used in the pool or array is displayed as a number and is also represented as bar in the chart. The color of the line above the bar changes to denote that space utilization has crossed a threshold that you have set.
- The following details about used space are shown below the bar chart:
  - **Data:** The amount of space in the pool that is used for storing the actual data after compression and deduplication.
  - **Snapshot:** The amount of space used by all snapshots in the pool.
  - **Reserved:** The amount of space reserved by all shares and LUNs in the pool.

**Figure 4: Image displaying the Capacity sub-section**



- **Reclaimable space details**

The **Capacity** section of the IntelliFlash Web UI **Dashboard** displays the reclaimable space details when any delete operations are in progress and until the deleted space reclaimed. To view the details, you can the mouse hover the info icon next to the **Used** space details.



## Related Topics

[Viewing pool or array space saving and capacity](#)

[Dashboard sections](#)

## Performance

### Performance

The **Performance** subsection of the **Dashboard** displays the performance parameters individually for each protocol (iSCSI, FC, NFS, SMB) or aggregate of all protocols for the selected pool or the array. Also, you can view average and total performance of the performance parameters in the **Combine View** or read and write performance individually. By default, the graph displays the aggregate of all protocols for the last five minutes.

The following are the performance parameters:

- Latency
- IOPS
- Throughput

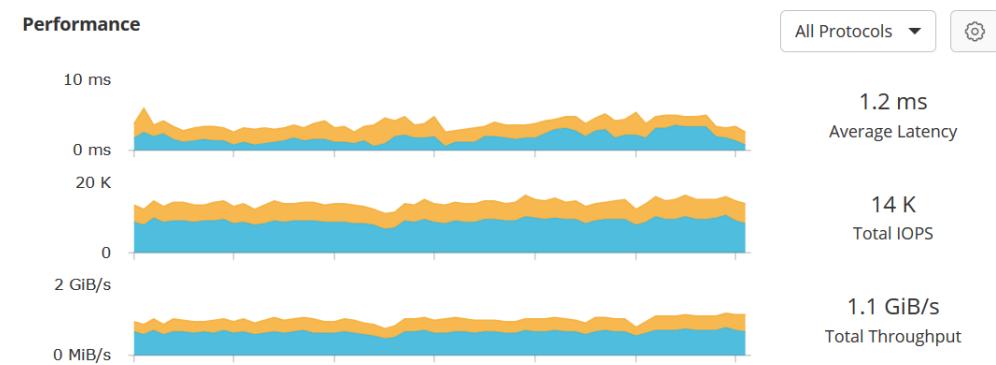
The metrics for the above performance parameters are displayed based on your selection of the pool or array, and all protocols or a single protocol.

 **Note:** All graphs display metrics for the last five minutes.

The following image displays the combine view of the **Performance** graphs for an individual pool or array depending on your selection.

 **Note:** The Y-axis of graphs display the minimum and possible maximum performance value attained in the last five minutes.

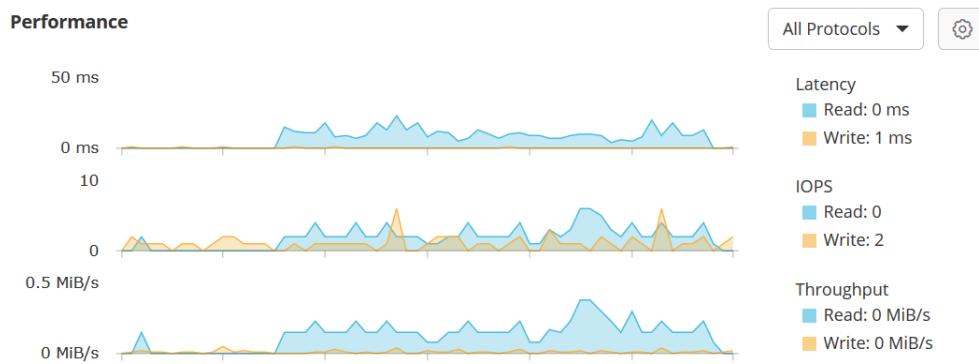
**Figure 5: Image displaying Combine View (Average and Totals)**



- **Average Latency:** The average latency for all protocols or an individual protocol active on the pool or the array.
- **Total IOPS:** The total input-output operations per second. This is an average for all protocols or an individual protocol active on the pool or the array.
- **Total Throughput:** The network throughput—the amount of data read or written in MiB (mebibyte), GiB (gibibyte) , TiB (tebibyte) by all the protocols active or an individual protocol on the pool or the array.

The following image displays the detailed read and write view of the **Performance** graphs for an individual pool or array depending on your selection:

**Figure 6: Image displaying Read and Write performance**



- **Latency:** The read and write latency in milliseconds for all protocols or an individual protocol active on the pool or the array.
- **IOPS:** The read and write IOPS for all applicable protocols active on the pool or an individual protocol active on the pool or the array. Values greater than 9999 use the letter 'K' to denote thousand. For example, 12000 is denoted as 12K. The total input-output operations per second.
- **Throughput:** The read and write throughput for all applicable protocols or an individual protocol on the pool or the array. .

## Related Topics

[Viewing pool or array performance details](#)

[Dashboard sections](#)

## Storage objects with Top 10 or Bottom 10 workloads

### LUNs, shares, or VMs with Top 10 or Bottom 10 workloads

The **Top 10 or Bottom 10** section on the right hand side of the **Dashboard** displays the LUNs, shares, or VMs with the top ten or bottom ten workloads. You can apply filters based on LUNs, shares, or VMs and performance parameters (latency, IOPS, throughput).

Based on the applied filter the section displays top ten or bottom ten performers.

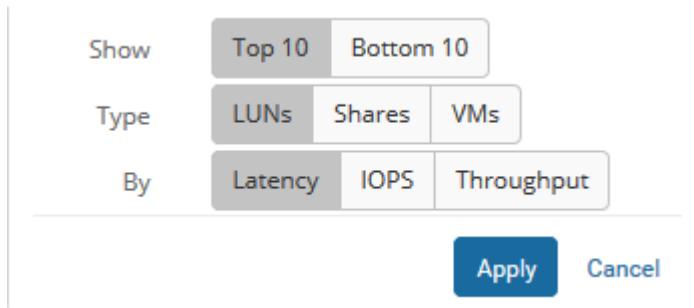
Top 10 Shares by Latency			
Object name	Latency	IOPs	Throughput
sql	0.4 ms	1	0 MiB/s
VM_5	0 ms	0	0 MiB/s
sh58cj	0 ms	0	0 MiB/s
VM_3	0 ms	0	0 MiB/s
sh1	0 ms	0	0 MiB/s
2012_sh1	0 ms	0	0 MiB/s
clustered_1	0 ms	0	0 MiB/s

**Figure 7: Example for the Top 10 Shares filtered by latency**

To view the top ten or bottom ten list of storage objects (LUNs, shares, VMs), you can apply filters based on the type of storage objects and performance parameters (latency, IOPS, throughput).

 **Note:** To view workload for VMs, the IntelliFlash Manager plugin should be configured.

If you apply a filter for top ten or bottom ten lists of storage objects (LUNs, shares, VMs), the IntelliFlash Web UI persists the applied filter in that browser. However, if no IO is running on the set filter, the IntelliFlash Web UI displays the list of entities on which IO is running and if no filter is applied the list displays details of the storage entities with IO running.



**Figure 8: Filter to view top ten or bottom ten LUNs, shares, VMs by latency, IOPS, or throughput**

### Related Topics

[Viewing Top 10 or Bottom 10 LUNS, Shares, or VMs with maximum or minimum workload](#)

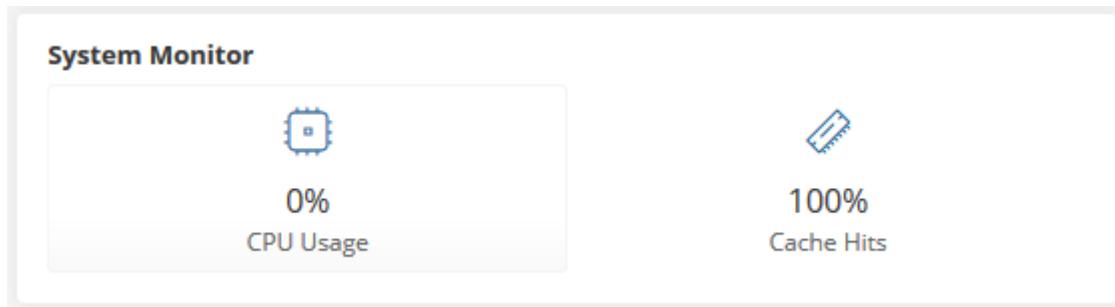
[Dashboard sections](#)

## System Monitor

### System Monitor

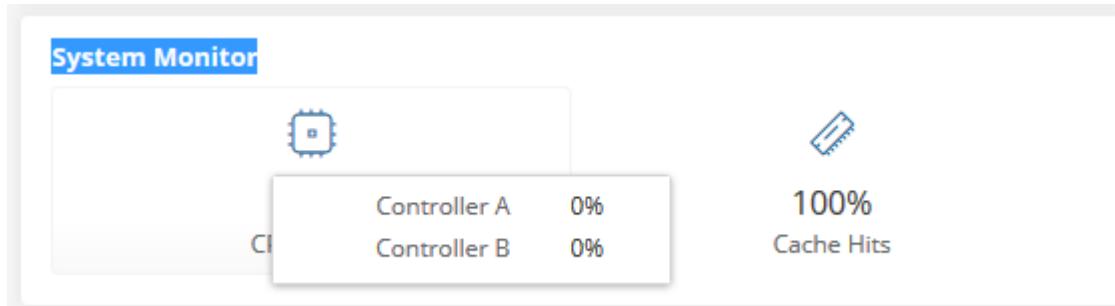
The **System Monitor** section of the **Dashboard** displays the following:

- **CPU Usage** percentage on each controller.
- **Cache Hits** percentage on each controller.



**Figure 9: System Monitor section**

Mousing over the **CPU Usage** and **Cache Hits** icons displays the percentages for individual controllers, as shown in following figure.



**Figure 10: System Monitor displaying Controller A and Controller B details**

### Related Topics

- [\*Viewing CPU and cache hits usage of the array\*](#)
- [\*Viewing pool or array space saving and capacity\*](#)
- [\*Viewing Top 10 or Bottom 10 LUNS, Shares, or VMs with maximum or minimum workload\*](#)
- [\*Viewing pool or array performance details\*](#)

## Dashboard variations

---

The **Dashboard** presents different variations in the IntelliFlash Web UI depending on the state of your storage array. The appearance depends on the following factors:

- Number of pools in the array
- Whether or not a pool has a project, share or LUN
- Which protocols are enabled for the shares and LUNs in a pool

**Table 3: Dashboard Variations**

Array State	Dashboard Appearance
Array has no pool	The <b>Dashboard</b> displays static informational panels and the <b>Create a Pool</b> button,
Array has a single pool with projects and shares or LUNs	The <b>Dashboard</b> displays a single pool tab that displays the metrics for the pool.
Array has two or more pools	The <b>Dashboard</b> displays the <b>Array</b> tab and tabs for each pool that display the metrics for the array and pool.

Array State	Dashboard Appearance
Any of the following are true for the array: <ul style="list-style-type: none"> <li>• A pool does not have any project</li> <li>• A pool has a project but no share or LUN</li> <li>• A pool has a project with one or more shares or LUNs, but no protocol is enabled for any of the shares or LUNs</li> </ul>	The corresponding pool tab displays a <b>Create a Project</b> button.
A protocol is not enabled on any of the shares and LUNs in a pool.	The dropdown list for selecting protocols in the <b>Pool Performance</b> section does not display the protocol that is not enabled.

### Related Topics

[\*No pools\*](#)

[\*No projects\*](#)

[\*Single pool view\*](#)

[\*Multi pool view\*](#)

[\*Viewing pool or array performance details\*](#)

### No pools

When there is no pool in the array, the **Dashboard** just displays a screen with a button that enables you to create a pool with all sections that normally appear in the **Dashboard**.

Welcome to your IntelliFlash Dashboard  
All the mission critical information about your array, at-a glance!

**Savings**  
The data reduction ratio shows the ratio of the original data to the space used after deduplication.

**Capacity**  
This section shows the space used and the available space in the pool. The following metrics are shown below the bar chart.

**Performance**  
Get the average latency, total input-output operations per second, and details of amount of data broken down by read and write for all protocols active on the pool.

**Create a Pool**

**Top 10 Performers**  
Find your LUNs, Shares and VMs with the highest or lowest latency and IOPS.

Create a pool and project to monitor your top performers.

**System Monitor**

XX% CPU Usage      XX% Cache Hits

**Figure 11:** Dashboard with no pools

**Note:** You might see this screen only if you skip creating a pool when you configure your array using the **Configuration Wizard**.

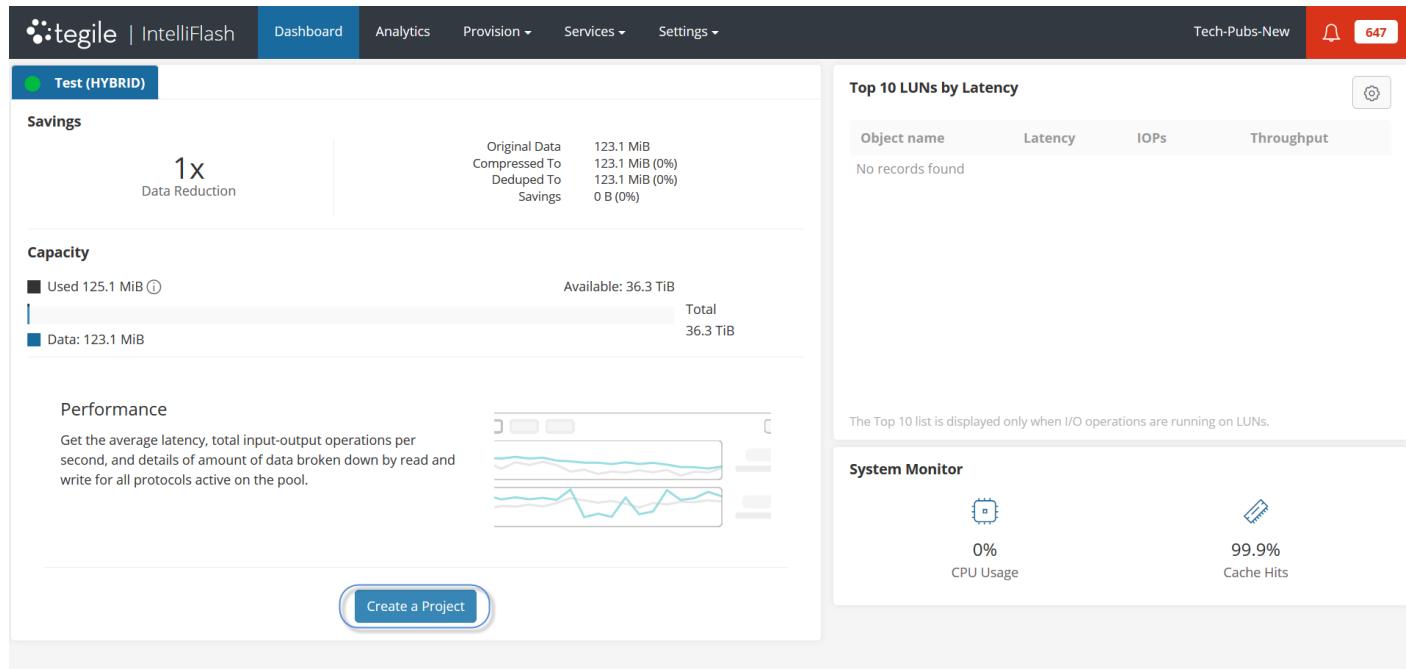
## Related Topics

[Dashboard variations](#)

## No projects

When there is a pool created in the array but no projects, the **Dashboard** displays all sections of the **Dashboard** with a button that enables you to create a project.

**Figure 12:** Dashboard with no projects



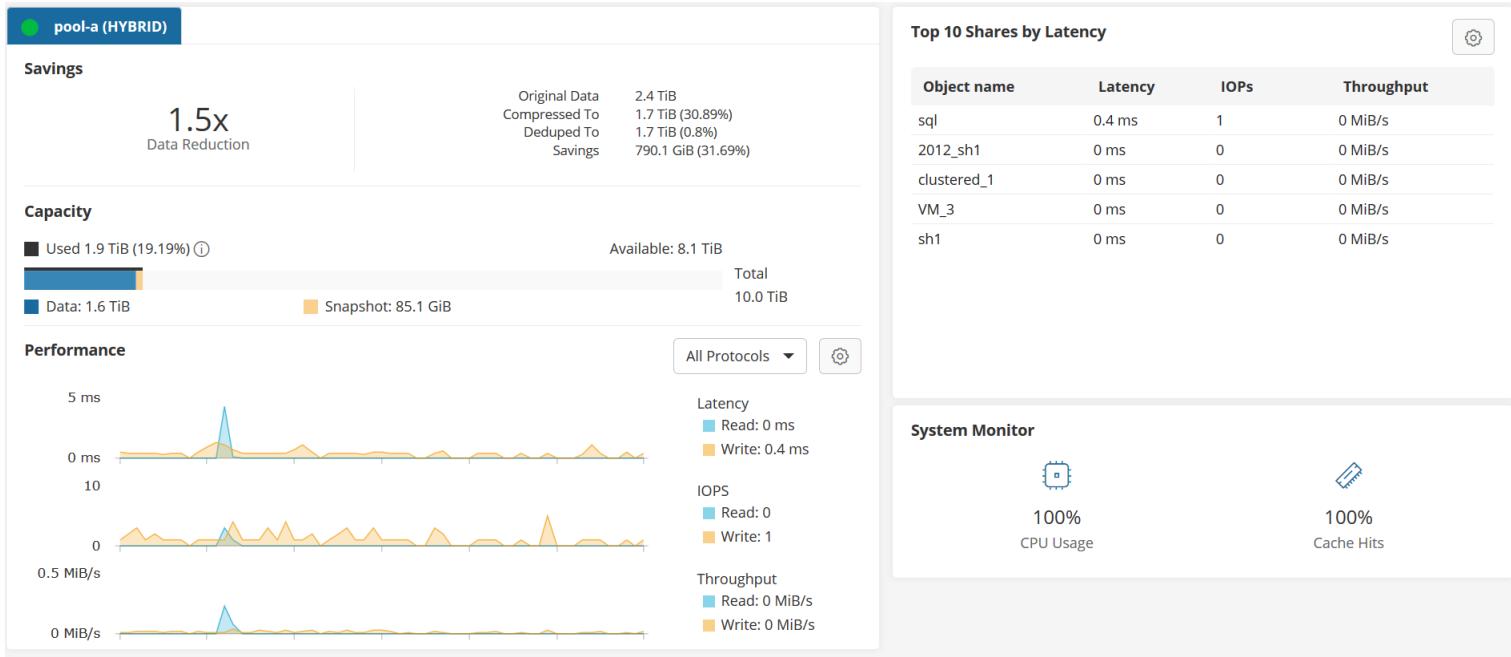
## Related Topics

[Dashboard variations](#)

## Single pool view

The **Dashboard** displays a single pool tab that displays the metrics for the pool.

**Figure 13: Dashboard with single pool**



## Related Topics

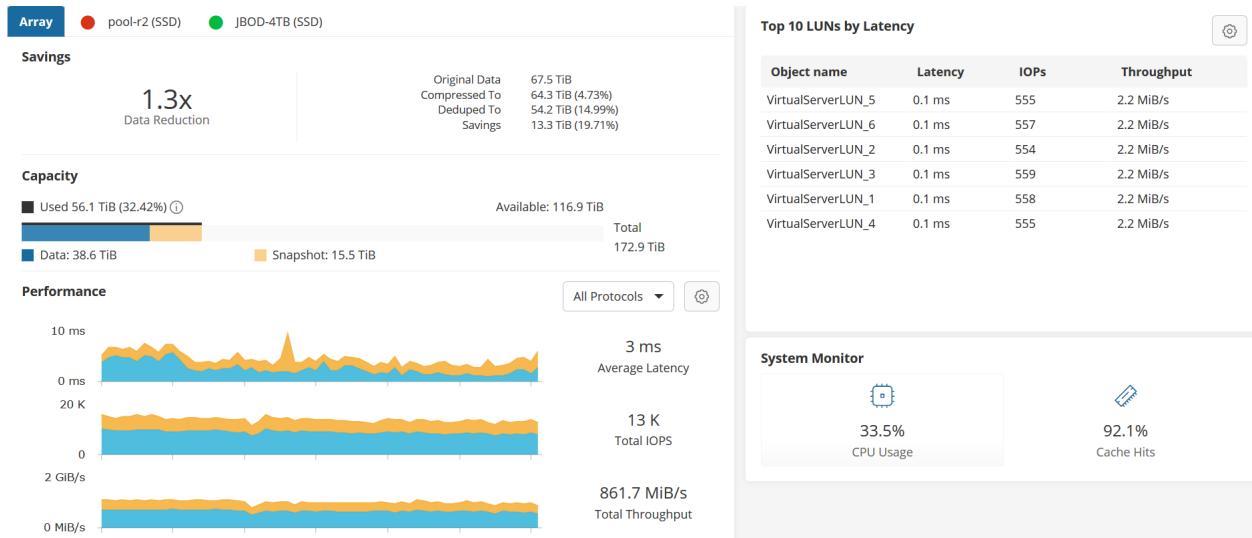
[Dashboard variations](#)

## Multi pool view

### Multi pool view

The **Dashboard** displays the default **Array** tab and one tab for each of the pools in the array.

**Figure 14: Dashboard with two pools**



## Related Topics

[Dashboard variations](#)

## Viewing pool or array performance details

The **Performance** subsection of the **Dashboard** allows you to view the performance parameters individually for each protocol (iSCSI, FC, NFS, SMB) or aggregate of all protocols for the selected pool or the array, and you can view average and total performance of the parameters in the **Combine View** or read and write performance individually. By default, the graph displays the aggregate of all protocols. The following are the performance parameters:

- Latency
- IOPs
- Throughput

The metrics for the above performance parameters are displayed based on your selection of the pool or array and all protocols or a single protocol.

To view the performance parameters of a pool or the array, complete the following steps:

1. Click **Dashboard**.
2. In the **Dashboard**, click a tab with the pool name or the **Array** tab and look for the **Performance** subsection.

 **Note:** The **Array** tab is displayed only if the array has two or more pools.

3. In the **Performance** subsection, you can view average and total performance metrics or read and write performance parameters for the selected pool or the array.

- You can view performance parameters for all protocols by default. By default, **All Protocols** is selected.
- To view performance for a specific protocol, in the **All Protocols** dropdown list, select a protocol.
- To view average and total performance parameters, click the settings icon  and enable **Combine View**

#### Related Topics

[Dashboard sections](#)

[Dashboard variations](#)

## Viewing pool or array space saving and capacity

---

To view the space savings and capacity of a pool or the array, complete the following steps:

1. Click **Dashboard**.
2. In the **Dashboard**, click a tab with the pool name or the **Array** tab and look for the **Savings** and **Capacity** sub-sections.



**Note:** The **Array** tab is displayed only if the array has two or more pools.

#### Related Topics

[Dashboard sections](#)

[Dashboard variations](#)

## Viewing Top 10 or Bottom 10 LUNS, Shares, or VMs with maximum or minimum workload

---

You can view a list of top ten or bottom ten LUNS, shares, or VMs for maximum or minimum workloads by applying filters.

To view the top ten or bottom ten list, complete the following steps:

1. Click **Dashboard**.
2. In the **Top 10** or **Bottom 10** section, click the settings icon  and complete the following steps:



**Note:** The section displays the label **Top 10** or **Bottom 10** depending on the already applied filter. For example: **Top 10 Shares by Latency** or **Bottom 10 LUNs by IOPS**.

- a) Select **Top 10** or **Bottom 10**.
- b) Select **LUNs**, **Shares**, or **VMs**.

- c) Select **Latency, IOPS, or Throughput**.
- d) Click **Apply**.

#### Related Topics

[Dashboard sections](#)

[Dashboard variations](#)

## Viewing CPU and cache hits usage of the array

---

The **System Monitor** section of the **Dashboard** displays the CPU usage and cache hits usage percentage for the complete array and per controller.

To view CPU usage and cache hits usage, complete the following steps:

1. Click **Dashboard**.
2. In the **System Monitor** section, place the mouse pointer over the **CPU Usage** icon or **Cache Hits** icon to view the percentage of usage per controller.

The **System Monitor** section displays the **CPU Usage** and **Cache Hits** percentage.

#### Related Topics

[Dashboard sections](#)

[Dashboard variations](#)



---

# Chapter 4

---

## IntelliFlash Analytics

---

### Topics:

- [\*Live and Historical Views\*](#)
- [\*Analytics UI\*](#)
- [\*Analytics graphs\*](#)
- [\*Viewing Array analytics\*](#)
- [\*Customizing the Analytics view\*](#)

The **Analytics** feature provides a number of statistics and metrics to help you monitor different aspects of the array. You can monitor metrics for both controllers of your array.

You can view live and historical analytics, and perform all tasks from both the live and history views.

The **Analytics** page by default displays live analytics. You can customize your **Analytics** page according to your requirements by adding multiple new tabs for different metrics. You can modify the parameters and metrics on each tab to monitor your array according your specific requirements.

The graphs for data, pools, and system performance in the **Analytics** page help you to understand your array performance. You can select different sources within the graphs to monitor a specific metric in your array.

You can view the graphs in the **Analytics** page synchronously for different metrics. The UI allows you to drag your cursor inside any graph to zoom in on a time interval for detailed analysis. You can use the **Zoom Out** option inside the graph to reset the view. You can also drag handles at the bottom of each graph to expand the graph size for a magnified view.

You can export both live and historical analytics data from your array for further analysis in the .csv file format. The **Analytics** page also allows you to disable the legends and controllers in the graphs for a simplified view.

## Live and Historical Views

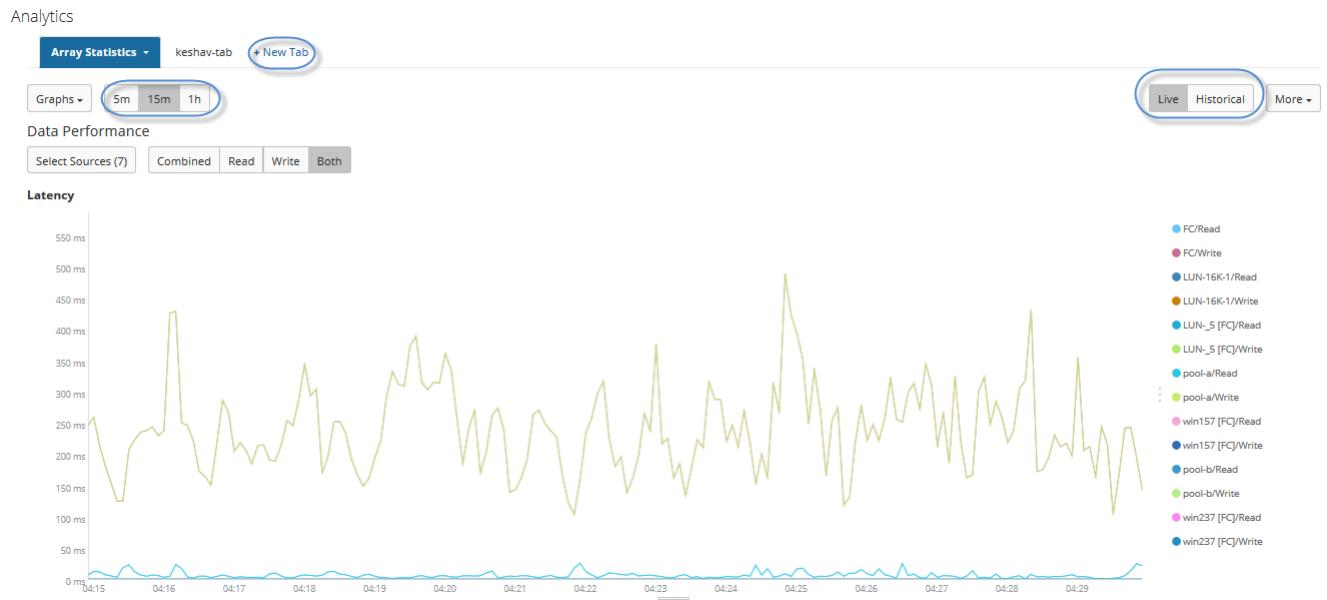
The **Analytics** feature in IntelliFlash provides various graphs for analyzing your storage array performance. You can view the real time metrics in the **Live** view and historical metrics in the **Historical** view of your array plotted on different graphs. You can switch between **Live** and **Historical** views.

### Live view

The **Live** view is the default view of the **Analytics** page, and displays the real time metrics from five-minutes to one-hour time intervals. You can view metrics for data, pool, network, CPU, and cache hits in different sections of the page in respective graphs.

The **Live** view page has the following three sections with several graphs:

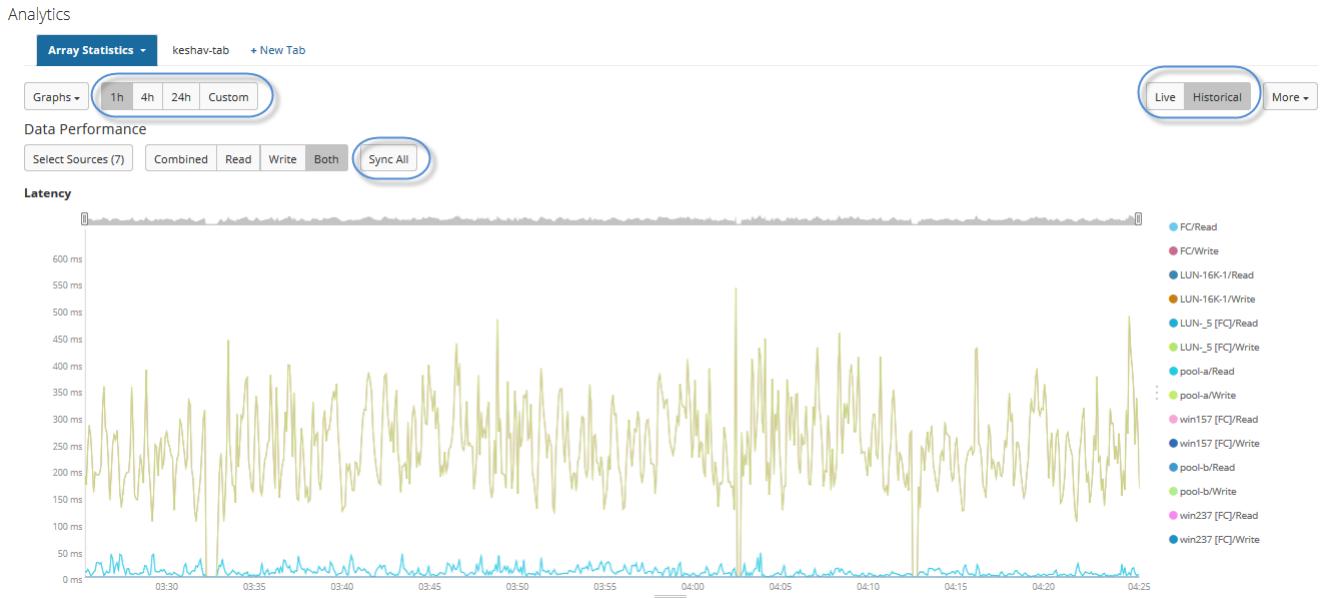
- Data Performance
- Pool Performance
- System Performance



**Figure 15: Live view**

### Historical view

The historical view displays the same graphs as the **Live** view. However, in the historical view, you can view metrics from past 1-hour, 4-hour, and 24-hour time intervals. You can also choose calendar dates to view the past metrics between the two selected dates.



**Figure 16: Historical view page**

### Sync All option

The **Sync All** is unique to the **Historical** view.

When you click the **Sync All** button and you zoom a graph to a particular time interval, other graphs on the **Historical** page will also sync to the same time interval.

You can use the **Sync All** option when you zoom a graph to a particular time interval and you want to sync the same time interval to the other graphs on the page.

### Related Topics

[Viewing Array Analytics](#)

[Customizing Array Analytics](#)

[Analytics UI](#)

[Select Sources Window](#)

[Analytics Graphs](#)

## Analytics UI

---

The **Analytics** page provides different UI options to enable optimal use of the **Analytics** feature.

The following UI options are important to understand to get the most out of the feature:

- **Array Statistics** and **New Tab** tab
- **Graphs** menu

- Tab with time intervals
- **Live** and **Historical** tabs
- **More** dropdown list to export data and hide UI controls and legends

### Array Statistics tab

The **Array Statistics** tab is a default tab in the **Analytics** page. The graphs under this tab provide the metrics for your array. The IntelliFlash Web UI allows you to add similar tabs to include required graphs for monitoring your storage array metrics. You can also duplicate an existing tab or rename an existing tab.

 **Note:** Inside each of the tabs in the **Analytics** page, you can switch between the live analytics view and historical analytics view.



Array Statistics ▾ + New Tab

**Figure 17: Array Statistics and New tab**

You can name a tab according to the metrics that you want to monitor in the tab. For example, you can monitor a specific pool by removing other graphs in the tab. You can simply keep pool related graphs and exclude remaining graphs.

 **Note:** The applied customizations are specific to each tab in the **Analytics** page.

Similarly, you can have tabs specific to CPU, Network, Data Performance, or tabs for your specific requirements with different combinations.

### New Tab

**New Tab** enables you to add a new tab or duplicate an existing tab in the **Analytics** page.

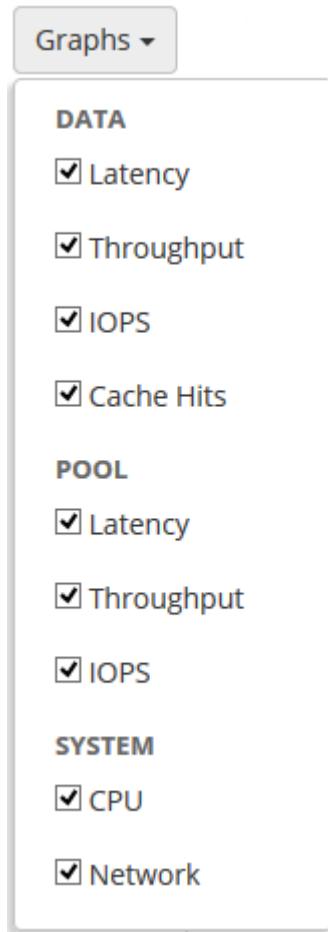
### Graphs menu

The **Graphs** menu is a control that allows you to exclude or include a particular graph from your **Analytics** page.

By default, all graph types are selected and displayed on the **Analytics** page. You can clear the check box next to the graph name in the list to exclude a particular graph.

The **Graphs** dropdown menu lists three sections of the **Analytics** page: **Data**, **Pool**, **System**. The menu allows you to enable or disable different graphs under each section.

The dropdown lists three sections of the **Analytics** page and different graphs under each section. Available graphs are organized under three sections on the **Analytics** page: **Data**, **Pool**, **System**.



**Figure 18:** Graphs menu

#### Related Links

[Customizing the Analytics view](#)

[Selecting graphs for Analytics](#)

#### Time interval buttons

The time intervals buttons next to the **Graphs** menu enable you to select time intervals for the graphs on the **Analytics** page.

The IntelliFlash Web UI provides different time intervals for live analytics and historical analytics.

 **Note:** The selected time interval applies to all the graphs in the **Analytics** page.

You can select the following time intervals for the live analytics:

- 5 minutes (**5m**)
- 15 minutes (**15m**)

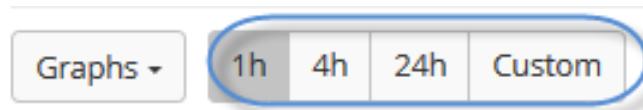
- 1 hour (**1h**)



**Figure 19: Time interval buttons - Live view**

You can select the following time intervals for historical analytics:

- 1 hour (**1h**)
- 4 hour (**4h**)
- 24 hours (**24h**)



**Figure 20: Time interval buttons - Historical view**

Only in the historical view, you can additionally select a **Custom** time interval to display an interval between two dates and times.

### Related Links

[Selecting time intervals for graphs](#)

[Viewing custom historical analytics](#)

### Live and Historical tabs

The **Live** and **Historical** tabs allow you to switch between the live **Analytics** page and the historical **Analytics** page. The **Live** view is displayed by default.

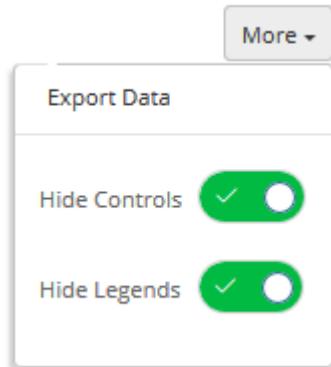


**Figure 21: Live and Historical tabs**

**Note:** There are only minor UI differences between the **Live** view and **Historical** view.

### More menu list for exporting data, hiding UI controls and legends

The **More** menu list allows you to export analytics data and hide the UI controls and legends in the graphs.



**Figure 22: More menu**

 **Note:** The **More** menu is available in both the live and historical analytics views.

### Related Topics

[Customizing the Analytics view](#)

[Viewing Array analytics](#)

[Analytics graphs](#)

## Analytics graphs

---

The **Analytics** pages contain graphs for storage performance and array performance monitoring under different sections of the page.

### Sources for Graphs

The parameters on which the graphs provide data are called sources.

The sources can vary depending on the sections of the **Analytics** page and graph type.

For example, the graphs in the **Data Performance** section of the page have multiple source types. You can select pools, projects, datasets, and protocols as sources or combinations of these sources for graphs. For the graphs in the **Pool Performance** section of the page, pools and the disks used by the pools in your array are the sources. Similarly, for the **CPU** and **Network** graphs the controllers and network ports are the sources respectively.

### Different views for graphs

In all the graphs, you can view **Read** and **Write** operations separately or in combination. You can also view both **Read** and **Write** operations independently in the same graphs.

The following table describes the **View** options you can use for the monitoring graphs:

**Table 4: View options for graphs**

<b>Button</b>	<b>Description</b>
<b>Combined</b>	The <b>Combined</b> option displays the aggregate of both read and write operations in a single line in the graph.
<b>Read</b>	The <b>Read</b> option displays only the read operations in a single line in the graph.
<b>Write</b>	The <b>Write</b> option displays only the write operations in a single line in the graph.
<b>Both</b>	The <b>Both</b> option displays read and write operations in two separate lines in the graph.

You can view all four graphs metrics synchronously, which allows you to easily understand the performance of source entities.

## UI controls in the graphs

The following table describes the common UI controls used to navigate the graphs:

**Table 5: UI controls for graphs**

<b>UI control/Action</b>	<b>Description</b>
	Click this UI control at the bottom of a graph to expand or reduce the size of a graph
	Click this UI toggle to temporarily hide the legend of a graph. Click the same button to unhide the graph legend.
	The Zoom Out UI control UI control appears when you select/zoom in on an area of a graph. Click <b>Zoom Out</b> to revert to the default view.
	You can toggle the legend to the right of each graph to enable or disable the appearance of the metric in the graph.

## Graphs in Data Performance

The **Data Performance** section of the **Analytics** page displays the following Graphs:

- Latency
- Throughput
- IOPs
- Cache Hits



**Figure 23: Graphs in the Data Performance section**

You can click the legend to the right of the graph to enable or disable the appearance of the metric in the graph.

### Latency

The **Latency** graph displays the average operation latency of the selected sources in milliseconds.

### Throughput

The **Throughput** graph displays the amount of data read or written in mebibyte per second (MiBps) by all the selected sources individually.

### IOPs

The **IOPs** graph displays the total input-output operations per second of the selected sources for the graph.

## Cache Hits

The **Cache Hits** graph displays the total percentage of data that is served directly from RAM and the SSDs to users during the selected time interval from both controllers and individual controllers. You can select Controller–A or Controller–B from the dropdown menu to view details of any one controller. By default, the graph displays details for both controllers.

## Related Topics

[Analytics graphs](#)

[Viewing Array Analytics](#)

[Customizing Analytics page](#)

[Select Sources Window](#)

## Select Sources Window

The **Select Sources** window allows you to add sources for the graphs in the **Data Performance** section. You can access the **Select Sources** window by clicking the **Select Sources** button at the top left of the page under the **Data Performance** section.

The **Select Sources** button displays the selected number of sources.

You can select the source type from the **Type** dropdown menu of the Select Sources window.

You can apply the filters based on the selected **Source** type. Depending on your source type selection, respective filters dropdown options appear next to the **Filter** field. You can filter based on protocols, pools, projects, and datasets. You must select the **View** type (Latency, Throughput, IOPS) from the dropdown list.



**Remember:** The **Select Sources** window actually displays all the sources and their metrics available on the array. However, the graphs in the **Analytics** page only display the selected sources for plotting on the graphs. Therefore, you can use the **Select Sources** window as a monitoring tool to view the metrics for sources that are not part of the sources for graphs in the **Analytics** page.

**Figure 24: Select Sources window**

The screenshot shows the 'Select Sources' dialog box. At the top, there are dropdown menus for 'Type' (set to 'Dataset'), 'View' (set to 'Latency'), and 'Filter' (set to 'All Protocols', 'All Pools', and 'All Projects'). Below these are search and clear buttons. To the right, a sidebar titled 'Selected Sources (7)' lists items under 'Protocols', 'Pools', 'Projects', and 'Datasets', each with a delete 'X' button. The main table lists 28 datasets with columns for Name, Avg Lat., R Latency, W Latency, and Graph. Each row has a selection switch. A message at the bottom says 'Showing 28 Datasets (values as of 6/16 04:01:08)'. At the bottom right are 'Cancel' and 'Save' buttons.

The live data displayed on the UI corresponds to your source **Type**, **View** and **Filter** dropdown menu selections in the **Selected Sources** window.

The following table details the **Selected Sources** columns that are displayed depending on your **Type**, **View** and **Filters** menu choices.

**Table 6: Select Sources window per Type, View, and Filter options**

Select Sources window column	Details
Name	<p>Displays the names of sources based on the selected source <b>Type</b>:</p> <ul style="list-style-type: none"> <li>• Protocols (SMB, NFS, iSCSI, FC)</li> <li>• Pool names</li> <li>• Project names</li> <li>• Dataset names</li> <li>• VM names</li> </ul>

Select Sources window column	Details
Second, third, and fourth columns	<p>Displays data depending the selected <b>View</b> type:</p> <p><b>Latency</b></p> <ul style="list-style-type: none"> <li>• Avg Lat (Average latency)</li> <li>• Read Latency</li> <li>• Write Latency</li> </ul> <p><b>Throughput</b></p> <ul style="list-style-type: none"> <li>• Total MiB/s</li> <li>• R MiBs</li> <li>• W MiBs</li> </ul> <p><b>IOPS</b></p> <ul style="list-style-type: none"> <li>• Total Ops</li> <li>• R Ops (Read Ops)</li> <li>• W Ops (Write Ops)</li> </ul>
Graph	When the <b>Graph</b> toggle button is selected for a Name, the green color indicates that the source is part of the <b>Selected Sources</b> . Click the <b>Graph</b> button to toggle it to green to include that source for graph plotting. Click or drag the <b>Graph</b> button to the left to deselect this source from the graphs.

### Selected Sources section

The **Selected Sources** section on the right side of the **Selected Sources** window displays the list of sources used to plot the graphs. You can delete a particular source from the list by clicking the cross icon (X) and click the **Clear All** link at the top of the section to delete all sources.

### Search box

The search box in the window allows you to search entities from the applied filter.

### Related Topics

[Selecting Sources for Data Performance](#) on page 46

[Sources for Graphs](#)

[Customizing Analytics page](#)

[Viewing Array Analytics](#)

[Analytics Graph](#)

### Graphs in Pool Performance

The graphs in the **Pool Performance** section display the average storage operation metrics per disk.

**Figure 25: Graphs in the Pool Performance section**



The **Pool Performance** section of the **Analytics** page has the following graphs:

- Latency (Average per disk)
- Throughput (Average per disk)
- IOPs (Average per disk)

The graphs display metrics for all pools on the array or you can select a specific pool and monitor the performance. The graphs display metrics separately for the iFlash part and data part of a pool. The displayed metrics on the graph are the average per disk of the pool.

## Related Topics

[Analytics graphs](#)

[Viewing Array analytics](#)

[Customizing the Analytics view](#)

## Graphs in System Performance

The **System Performance** section of the Analytics page display the following graphs:

- CPU
- Network

### CPU

The **CPU** graph displays the CPU usage percentage for both controllers by default. The graph displays the percentage of CPU usage by the:

- Total processor utilization by all processes (**Total**)
- Processor utilization by user processes (**User**)
- Processor utilization by system processes (**System**)

The graph also displays total percentage per controller. You can toggle the dropdown list or toggle (strikethrough to exclude and clear the strikethrough to include) the entries at the right of the graph to view CPU usage details for all controllers or an individual controller.

## Network

The **Network** graph displays analytics for the transmit and receive speeds for each network interface card in the array, except for Fibre Channel. The graph also displays consolidated receive and transmit statistics per controller. The **Network** graph displays network speed in Mb/s (megabit per second)

### Related Topics

[Analytics graphs](#)

[Viewing Array analytics](#)

[Customizing the Analytics view](#)

## Viewing Array analytics

---

### Selecting Sources for Data Performance

To select sources for **Data Performance** graphs, complete the following steps:

1. Click **Analytics**.
2. In the **Analytics** page, click the required **Array Statistics** tab or custom created tab. You can provide custom names for the tabs for easy identification apart from the default name **Array Statistics**.
3. (Optional) Click **Live** or **Historical**.  
Ignore this step if you are already in the required view.
4. Click **Select Sources**.
5. In the **Select Sources** window, complete the following steps:
  - a) Click the **Type** dropdown and select a required option.  
Protocol, Pool, Project, Dataset, or VM.
  - b) Click the **View** dropdown and select a required option.  
Latency, Throughput, and IOPS.
  - c) Click the **Graph** button to toggle it to green to include that source for graph plotting.
  - d) Use the the search box in the window to search entities from the applied filter.
6. (Optional) In the **Selected Sources**, you can delete a particular source from the list by clicking the cross icon (X) and click the Clear All link at the top of the section to delete all sources.
7. Click **Save**.

## Related Topics

[Graphs in Data Performance](#)

[Sources for Graphs](#)

## Viewing Data Performance Analytics

The **Data Performance** analytics of the **Analytics** page display latency, throughput, and IOPs for the selected protocols, pools, shares, LUNs, or VMs. The graph also displays the cache hits details.

To view Data Performance analytics, complete the following steps:

1. Click **Analytics**.
2. In the **Analytics** page, click the required **Array Statistics** tab or custom created tab. You can provide custom names for the tabs for easy identification apart from the default name **Array Statistics**.
3. (Optional) Click **Live** or **Historical**.  
Ignore this step if you are already in the required view.
4. In the selected tab, look for the **Data Performance** section.  
If the selected tab is customized for not showing the **Data Performance** section or a graph in the section, the section or the graph may not be available. You can verify this from the **Graphs** dropdown list.

## Related Topics

[Graphs in Data Performance](#)

[Sources for Graphs](#)

[Selecting Sources for Data Performance](#)

## Viewing Pool Performance Analytics

The **Pool Performance** analytics of the **Analytics** page displays latency, throughput, and IOPs average per disk for the selected pools or all pools.

1. Click **Analytics**.
2. In the **Analytics** page, click the required **Array Statistics** tab or custom created tab. You can provide custom names for the tabs for easy identification apart from the default name **Array Statistics**.
3. (Optional) Click **Live** or **Historical**.  
Ignore this step if you are already in the required view.
4. In the selected tab, look for the **Pool Performance** section.

If the selected tab is customized for not showing the **Pool Performance** section or a graph in the section, the section or the graph may not be available. You can verify this from the **Graphs** dropdown list.

### Related Topics

[Graphs in Pool Performance](#)

[Sources for Graphs](#)

## Viewing System Performance Analytics

The **System Performance** analytics of the **Analytics** page displays the percentage of CPU usage by the controllers, and the network speed on each port of the controllers. The **Network** graph displays network speed in Mb/s (megabit per second)

To view **System Performance** analytics, complete the following steps:

1. Click **Analytics**.
2. In the **Analytics** page, click the required **Array Statistics** tab or custom created tab. You can provide custom names for the tabs for easy identification apart from the default name **Array Statistics**.
3. (Optional) Click **Live** or **Historical**.  
Ignore this step if you are already in the required view.
4. In the selected tab, look for the **System Performance** section.  
If the selected tab is customized for not showing the **System Performance** section or a graph in the section, the section or the graph may not be available. You can verify this from the **Graphs** dropdown list.

### Related Topics

[Graphs in Pool Performance](#)

[Sources for Graphs](#)

## Switching between Live and Historical views

You can switch between the **Live** and **Historical** pages as needed. All the UI controls are the same for both views and you can perform all actions in the **Historical** view that you can normally perform in the **Live** view.

To switch between the **Live** and **Historical** views, complete the following steps:

1. Click **Analytics**.
2. In the **Analytics** page, click the required **Array Statistics** tab or custom created tab.

You can provide custom names for the tabs for easy identification apart from the default name **Array Statistics**.

3. In the selected tab, click **Live** or **Historical** to toggle between the views.

The selected tab is highlighted to indicate the current view .

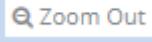
### Related Topics

[Live and Historical views](#)

## Zooming in and out on a time interval in a graph

You can zoom in and out of a time interval in a graph to have a detailed view of the graph.

To zoom on a time interval, complete the following steps:

1. Click **Analytics**.
2. In the **Analytics** page, click the required **Array Statistics** tab or custom created tab.  
You can provide custom names for the tabs for easy identification apart from the default name **Array Statistics**.
3. (Optional) Click **Live** or **Historical**.  
Ignore this step if you are already in the required view.
4. Click and drag your cursor inside the required graph to a select a specific time interval.  
All graphs in the selected section (For example, **Pool Performance**) section magnify and display metrics for the selected time interval.
5. Click the **Zoom Out** icon  inside the right part of the graph to revert to the normal view

### Related Topics

[Sources for graphs](#)

## Viewing custom historical analytics

To view custom historical analytics, complete the following steps:

1. Click **Analytics**.
2. In the **Analytics** page, click the required **Array Statistics** tab or custom created tab.  
You can provide custom names for the tabs for easy identification apart from the default name **Array Statistics**.
3. Click **Historical**.
4. In the **Historical** view, click the **Custom** tab.



**Note:** The **Custom** tab does not appear if you are on the default Array Statistics tab.

5. Select **From** and **To** dates.
6. Click **Apply**.

## Related Topics

[Sources for graphs](#)

## Hiding or unhiding a data point in a graph

You can hide or unhide a data point in a graph to have a clear view. When you hide a data point, metrics related to that data point in the graph are not displayed. You can hide or unhide the data point, by clicking the legend for the required data point.

To hide or unhide a data point in a graph, complete the following steps:

1. Click **Analytics**.
2. In the **Analytics** page, click the required **Array Statistics** tab or custom created tab.  
You can provide custom names for the tabs for easy identification apart from the default name **Array Statistics**.
3. (Optional) Click **Live** or **Historical**.  
Ignore this step if you are already in the required view.
4. In the required graph of any section of the page, click the legend item to hide or unhide it.  
The legend item that you want to hide is crossed out.

- LUN-16K-1
- LUN\_5 [FC]
- EC
- win237 [FC]
- pool-a
- win157 [FC]
- pool-b

## Related Topics

[IntelliFlash Analytics](#)

[Sources for Graphs](#)

## Customizing the Analytics view

---

### Adding a new Array Statistics tab

You can duplicate the default **Array Statistics** tab, or add a **New** tab to create custom tabs with custom graphs and sections in the **Analytics** page. For easy identification, you can use a meaningful name when you create the custom tab.

To add a new **Array Statistics** tab, complete the following steps:

1. Click **Analytics**.
2. In the **Analytics** page, click **+ New Tab**.
3. In the **Create New Tab** window, complete the following steps:
  - a) In the **Tab Name** field, type a name.
  - b) Select **New tab** or **Duplicate another tab**.  
Duplicating an existing tab helps you to quickly customize the graphs or sections.
  - c) If you selected the **Duplicate another tab** option, select a tab name from the **Duplicate** list.
  - d) Click **Create**.

A new tab appears with the new name provided.

### Related Topics

[IntelliFlash Analytics](#)

[Sources for graphs](#)

### Duplicating an Array Statistics tab

You can duplicate an existing Array Statistics tab for quick customization.

To duplicate an Array Statistics tab, complete the following steps:

1. Click **Analytics**.
2. In the **Analytics** page, click the required **Array Statistics** tab or custom created tab.  
You can provide custom names for the tabs for easy identification apart from the default name **Array Statistics**.
3. In the dropdown list, click **Duplicate**.
4. In the **Name Duplicate Tab** window, type a name for the tab.
5. Click **Create**.  
The duplicated tab appears with the new name provided.

## Related Topics

[IntelliFlash Analytics](#)

[Sources for Graphs](#)

## Renaming an Array Statistics tab

To rename any **Array Statistics** tab, complete the following steps:

1. Click **Analytics**.
2. In the **Analytics** page, click the required **Array Statistics** tab or custom created tab.  
You can provide custom names for the tabs for easy identification apart from the default name **Array Statistics**.
3. In the dropdown list, click **Rename**.
4. In the **Rename Tab** window, type a new name for the tab.
5. Click **Rename**.

## Related Topics

[IntelliFlash Analytics](#)

[Sources for graphs](#)

## Deleting an Array Statistics tab

You can delete an **Array Statistics** tab when you no longer need the tab.

To delete an Array Statistics tab, complete the following steps:

1. Click **Analytics**.
2. In the **Analytics** page, click the required **Array Statistics** tab or custom created tab.  
You can provide custom names for the tabs for easy identification apart from the default name **Array Statistics**.
3. In the dropdown list, click **Delete**.

## Related Topics

[IntelliFlash Analytics](#)

[Sources for graphs](#)

## Selecting graphs for Analytics

You can include or exclude graphs from the sections of an **Array Statistics** tab as part of customizing the metrics in a tab of the **Analytics** page. When you exclude a graph, the graph

does not appear under its respective section. You can later include the excluded graph according to your customization requirements.

To include or exclude graphs for the **Analytics** page, complete the following steps:

1. Click **Analytics**.
2. In the **Analytics** page, click the required **Array Statistics** tab or custom created tab.  
You can provide custom names for the tabs for easy identification apart from the default name **Array Statistics**.
3. (Optional) Click **Live** or **Historical**.  
Ignore this step if you are already in the required view.
4. Click **Graphs**.
5. In the dropdown menu, click the checkbox next to the graph name to exclude or include it.  
By default, all graphs are selected in the menu. A checkbox with a check mark indicates that the graph is included and an empty checkbox indicates that the graph is excluded.

## Related Topics

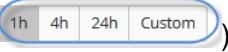
[IntelliFlash Analytics](#)

[Sources for Graphs](#)

## Selecting time intervals for graphs

The **Analytics** page provides an option to view graphs in different time intervals. You can change the time interval for each tab. The changed time interval is applicable for all the graphs in the tab.

To change the time interval for a graph, complete the following steps:

1. Click **Analytics**.
2. In the **Analytics** page, click the required **Array Statistics** tab or custom created tab.  
You can provide custom names for the tabs for easy identification apart from the default name **Array Statistics**.
3. (Optional) Click **Live** or **Historical**.  
Ignore this step if you are already in the required view.
4. Select the time interval depending on the selected page:
  - For **Live** page: click **5m**, **15m**, or **1h** (  )
  - For **Historical** page: click **1h**, **4h**, **24h** or **Custom** (  )

## Related Topics

[Viewing custom historical analytics](#)

## Exporting Analytics data

You can export the analytics data from the graphs in both the **Live** and **Historical** views into a .CSV file. The **Export Data** window provides details that will be part of the exported .csv file.

To export the analytics data, complete the following steps:

1. Click **Analytics**.
2. In the **Analytics** page, click the required **Array Statistics** tab or custom created tab.  
You can provide custom names for the tabs for easy identification apart from the default name **Array Statistics**.
3. (Optional) Click **Live** or **Historical**.  
Ignore this step if you are already in the required view.
4. In the selected tab, click  and select **Export Data**.
5. In the **Export Data** window, click **Export**.  
The **Export Data** dialog provides these details: Tab Name, Period (interval dates), Time (interval times), and available Graphs.
6. Save the downloaded .csv file.

### Related Topics

[IntelliFlash Analytics](#)

[Sources for graphs](#)

## Hiding or unhiding graph controls and legends

You can hide or unhide the UI controls and legends of the graphs.

To hide or unhide the UI controls or legends of the graphs, complete the following steps:

1. Click **Analytics**.
2. In the **Analytics** page, click the required **Array Statistics** tab or custom created tab.  
You can provide custom names for the tabs for easy identification apart from the default name **Array Statistics**.
3. In the selected tab, click the More dropdown menu and click the **Hide Controls** or **Hide Legends** toggle button.

When the controls or legends are hidden the toggle button color is green .

### Related Topics

[IntelliFlash Analytics](#)

[Sources for graphs](#)

---

# Chapter 5

---

## Pools

---

### Topics:

- *Understanding Pools*
- *Pools page*
- *Create Pool Window*
- *Creating a New Pool*
- *Active and Exported Pool*
- *Viewing Active Pool Details*
- *Managing a Pool*
- *Managing Disk Drives of a Pool*
- *Managing System Pool*

## Understanding Pools

A pool is a collection of physical disks configured with underlying data redundancy levels. A pool provides storage space to shares and LUNs.

On IntelliFlash systems, you can create the following types of pools based on the hardware model:

- Hybrid pool
- NVMe pool



**Note:** You can only create a maximum of two pools on IntelliFlash systems.

The **Dashboard** in the IntelliFlash Web UI displays the pool type based on the hardware model and space usage details. The **Dashboard** allows you to know the space used for data, snapshots, and reserved space in a pool.

### Hybrid Pool

A pool consisting of both HDDs and NVMe SSDs is called a hybrid pool. The hybrid pool uses the HDDs for data storage and NVMe SSDs for metadata and cache storage. The size and capacity of drives might differ depending on your array model.

### NVMe Pool

A pool consisting of NVMe disks is called an NVMe pool. An NVMe pool does not have dedicated metadata, read-cache or write-cache drives.

### System Pool

The System Pool is a preconfigured mirrored pool that contains the IntelliFlash Operating Environment. The location of the System pool depends on the hardware model.

You can view the System pool under **Settings > Administration > System OS**.



**Note:** Do not perform any action on the System pool without contacting IntelliFlash Technical Support.



**Attention:** Contact IntelliFlash Technical Support if you notice any problems with the System pool.

### Disk Group Types in a Pool

The HDDs and NVMe SSDs that are available on an IntelliFlash Array are grouped into specific disk types when creating a pool. The pool creation wizard groups the disks depending on your array model.

The following are the different disk group types shown for a pool:

- Data disks
- iFlash disk group
- Spare disks

- NVL (NVDIMM)

## Data disks

Data disks can be HDDs and NVMe SSDs depending on the IntelliFlash Array model. The arrays use these disks to store normal data. The number of data disks in a pool depends on the IntelliFlash Array model and the attached expansion shelves.

You can group data disks into RAID groups to create different pool types.

## iFlash Disk Group

An iFlash disk group is a set of NVMe SSDs in a hybrid pool used for storing and managing the metadata, read cache, and write cache, depending on the pool type. IntelliFlash groups the available NVMe SSDs into a single virtual disk group when creating a hybrid pool.

When creating a pool, IntelliFlash automatically allocates NVMe SSDs for the iFlash disk group depending on the available number of disks. The iFlash disk group can have an even or odd number of SSDs.

By default, IntelliFlash maintains two copies of metadata and write cache data in separate SSDs. Therefore, IntelliFlash has disk drive failure protection equivalent to a mirror RAID. You can maintain more than two copies. However, for optimal performance, two copies is recommended and set as the default.

IntelliFlash allocates a percentage of the iFlash disk group for metadata, a portion for write cache and the remainder for read cache of the iFlash disk group. These values are automatically adjusted based on the workload of the system.

## Spare Disks

A spare disk is a normal HDD or NVMe SSD that automatically replaces a failed data disk.

Before you can create a pool, you need to select a Spare Disk policy option.

The spare disk policy has the following options:

- **No spare:** No spare disks are allotted.
- **1 drive per pool per chassis:** Allots 1 disk per pool per expansion shelf as a spare disk. For example, if there is one pool and two expansion shelves, then the pool is allotted a spare disk in each of the expansion shelves.
- **1 drive per pool:** Allots 1 disk per pool as a spare disk. If there are two pools, then each pool is allotted 1 disk.
- **1 drive per chassis (shared):** Allots 1 disk per expansion shelf as a spare disk. This spare disk is open for use to any pool as needed.

- **1 drive system wide (shared):** Allots one disk for use as a spare disk. This is open for use to any pool.



**Note:** The size of the spare disks must be the same as the size of the data disks.

When a disk fails in a RAID group, the available spare disk replaces it automatically. If the failed drive is replaced with a new drive before the RAID rebuild process, then the spare drive returns to the spare disks group. However, if the RAID rebuild process starts on the spare disk, you must detach the failed drive. Detaching the failed drive allows the spare disk to work as a normal data disk and it disappears from the spare disks group. You can add the new replacement disk to the spare disks group.

### NVL (Non-Volatile Log) NVDIMM Modules

The NVL section of the **Disks** page displays details about the NVDIMMs (Non-Volatile Dual In-line Memory Modules). Each controller has two NVDIMMs.

### Pool Types Based on Redundancy Level

IntelliFlash systems have two pool types based on the disk types and hardware models. A pool with combination of HDDs and NVMe SSDs is called a hybrid pool and a pool with all NVMe SSDs is called an NVMe pool.

In IntelliFlash systems, you can create these two pool types based on RAID technology for data redundancy. The RAID technology provides various levels of data redundancy and storage capacity.

The following are the data redundancy level for hybrid and NVMe pools:

- Double Parity
- Triple Parity
- 2 Way Mirror

### Pool Naming Convention

When naming a pool, the following naming conventions are mandatory:

- Names must use alphanumeric characters with no spaces between the characters
- Names must start with an alpha character
- Names must be unique on the IntelliFlash Array
- Names cannot include a percent sign (%)
- Names cannot start with (# = 0 to 9)
- Names cannot use special characters. However, the following characters are allowed:
  - Underscore (\_)
  - Hyphen (-)
- Do not use the following predefined names that are used in the IntelliFlash Operating Environment:
  - *log*

- *raidz*
- *spare*
- *mirror*
- *local*

## Pools page

---

You can create and manage pools from the **Pools** page. The **Pools** page can be accessed from **Provision > Pools**.

The **Pools** page has two tabs:

- **Overview**
- **Disks**

You can create, export and import a pool, expand, and delete a pool using the IntelliFlash Web UI. However, you cannot reduce the size of a pool.



**Note:** Consult the IntelliFlash Technical Support team before making changes to a pool.

### Overview tab in the Pools page

The **Overview** tab in the **Pool** page provides details about the pool and enables you to perform pool management operations.

The **Disks** tab provides details about the disks in pool and disks group. You can perform disk-related management operations and know the status of the disks in a pool.

The **Overview** tab of the **Pools** page has the following sections:

- Pool Details
- Space Savings
- Space Usage
- Metadata Usage

In the **Overview** tab of the pools, you can perform the following operations:

- Export a pool
- Expand a pool
- View active and exported pool details
- View space saving and space usage details
- Reset pool errors
- Perform pool integrity check
- View details of disks in a pool
- Delete a pool

### Disks tab in the Pools page

You can view and manage disks in pools from the **Disks** tab of the **Pools** page.

The **Disks** page can be accessed under **Provision > Pools > Active Pools > Disks**.

In the **Disks** page, you can perform the following operations:

- Add hot spare disks
- View disks groups and disks details
- Replace a disk
- Remove a disk
- Take a disk offline
- Bring a disk online
- View read, write errors
- View state of disks
- View size of disks
- View available spare disks

## Create Pool Window

---

A pool enables you to provide disk space for shares and LUNs.

Using the **Create Pool** screen in the IntelliFlash Web UI, you can define the pool configuration and create a combination of NVMe and Hybrid pools in a few steps.

You can create a maximum of two pools on IntelliFlash systems.

The IntelliFlash Web UI allows you to select any one of the following pool types for an H-Series Hybrid Flash Storage System:

- **One NVMe pool with half of the NVMe drives and One Hybrid pool with half NVMe drives and all HDDs:** This option enables you to create an NVME pool first with half of the available NVMe SSDs, followed by a hybrid pool with the remaining half of the available NVMe SSDs and all the available HDDs.
- **One Hybrid pool with half of drives:** This option enables you to create one hybrid pool with half of the available NVMe SSDs and HDDs.
- **One Hybrid pool with all of drives:** This option enables you to create one hybrid pool with all the available NVMe SSDs and HDDs.

You can define the following redundancy types for the pool:

- **Double Parity**
- **Triple Parity**
- **2 Way Mirror**

By default, IntelliFlash automatically performs a disk integrity check during pool creation.

The **Pool Summary** in the **Create Pool** window displays the type of disks, total number of available disks for each type, and number of disks allocated for creating a pool. IntelliFlash automatically allocates available disks for data and metadata based on the model and displays usable storage space capacity in the Pool Summary.

## Creating a New Pool

A pool enables you to provide disk space for shares and LUNs. Using the **Create Pool** window in the IntelliFlash Web UI, you can create a pool in a few steps. In the **Create Pool** window, you can define the pool configuration. Before adding a new pool, make sure that the system is configured. When naming the pool, follow the pool naming conventions.

 **Note:** You can only create a maximum of two pools on the IntelliFlash systems.

 **Note:** The FIPS certified drives and standard drives are not compatible in the same system. All drives in the system must either be FIPS-certified or standard; and mixing them is not allowed. If a system is detected with FIPS-certified drives and standard drives, then IntelliFlash will not allow you to create a new pool.

To create a pool, complete the following steps:

1. Click **Provision > Pools**.
2. In the **Pools** page, click **New**.  
The **Spare Policy** options appear.
3. Select the spare disk policy from the following options:
  - **No spare**: No spare disks are allotted.
  - **1 drive per pool per chassis**: Allots 1 disk per pool per expansion shelf. For example, if there is one pool and two expansion shelves, then the pool is allotted a spare disk in each of the expansion shelves.
  - **1 drive per pool**: Allots 1 disk per pool. If there are two pools, then each pool is allotted 1 disk.
  - **1 drive per chassis (shared)**: Allots 1 disk per expansion shelf, which is open for use to any pool as needed.
  - **1 drive system wide (shared)**: Allots one disk for use, which is open for use to any pool.

The **Confirmation** pop-up of encryption keys appear.

4. Click **Yes** after you export and back-up the encryption keys.
5. In the **Create Pool** screen, select any one of the following pool types:

 **Note:** For IntelliFlash systems with mixed NVMe drive configuration, only **One NVMe pool with half of the NVMe drives and One Hybrid pool with half NVMe drives and all HDDs** option is shown. The other two options **One Hybrid pool with half of NVMe drives** and **One Hybrid pool with all the NVMe drives** are not available.

- **One NVMe pool with half of the NVMe drives and One Hybrid pool with half NVMe drives and all HDDs**: This option enables you to create an NVME pool first with half of the available NVMe SSDs, followed by a hybrid pool with the remaining half of the available NVMe SSDs and all the available HDDs.

- **One Hybrid pool with half of drives:** This option enables you to create one hybrid pool with half of the available NVMe SSDs and HDDs.
- **One Hybrid pool with all of drives:** This option enables you to create one hybrid pool with all the available NVMe SSDs and HDDs.

 **Note:** The above options are not available for an IntelliFlash N-Series system. You can only create NVMe pools in an N-Series system.

6. Click **Proceed** after selecting the pool type.

 **Note:** When you select both NVMe and hybrid pool types, the IntelliFlash Web UI always first creates the NVMe pool type followed by the hybrid pool.

7. In the **Pool Configuration** section, complete the following steps:
  - a) Type a name for the pool.
  - b) Select the **Redundancy Type: Double Parity, Triple Parity , or 2 Way Mirror.**
  - c) Select a **Pool Size** from the dropdown list:
    - **Use all disks**
    - **Use half of total disks**

The **Use half of total disks** option appears in the IntelliFlash Web UI only when a sufficient number of disks are available to create a second pool in the array.

 **Note:** The **Pool Size** options are available only for an N-Series NVMe-Flash Storage System.

8. Review the pool configuration in the **Pool Summary** section and then click **Create**.  
The **Pool Summary** section displays the number of disks allocated for data, spare, metadata, unused disk, and total usable storage space capacity.
9. Monitor the notifications in the **Progress Notification** screen.

The new pool appears in the **Pools** page under the **Active Pools** list.

You can create a project and then create shares and LUNs for storage provisioning.

 **Note:** On array models with the encryption feature support, it is recommended that you back up the encryption master key and keep one copy locally and another copy at a remote location for redundancy. The backed-up master key is required if you have to move all of the drives from one array chassis to another or if the master key gets corrupted due to any reason.

## Active and Exported Pool

---

The **Active** and **Exported** lists in the **Pools** page display the pools that are in the active or exported state.

## Active Pools

An active pool is the pool on the array that is currently in use for storage provisioning. The active pool is used to create projects, LUNs, shares. The **Active Pools** list in the **Pools** page displays the active pools available in the array. You can select a pool from the list to view the pool details and perform pool related operations.

## Exported Pools

An exported pool is a pool in the array that is currently not in use for storage provisioning. When a pool is exported, all shares, LUNs, and the pool itself are unmounted and hosts cannot access data. Generally a pool is moved to the **Exported** state during maintenance operations. The **Exported Pools** list in the **Pools** page displays the pools in the exported state.

You can import the exported pool or delete it. Once the pool is imported back as an active pool, you can use it for storage provisioning.

## Viewing Active Pool Details

---

The **Pools** page provides details about the pools. The page displays the list of active and exported pools with their details, as well as the space usage details of the pool.

To view details for an active pool, complete the following steps:

1. Click **Provision > Pools**.
2. Select a pool from the **Active Pools** list.
3. The **Overview** tab displays the following details.
  - **Pool Details**
  - **Space Savings**
  - **Space Usage**
  - **Metadata Usage**

You can perform the following pool related operations from the **Overview** tab of the **Pools** page:

- **Export**
- **Expand**
- **Delete**
- **Reset Pool Errors** and **Perform Pool Integrity Check** using the **More** dropdown menu.

## Managing a Pool

---

## Expanding a Pool

For hybrid pools, the IntelliFlash Web UI provides you the option to add data disks and metadata disks or expand only the metadata disks. In an NVME pool, you can only expand the data disks.

 **Note:** Do not expand a hybrid pool when the metadata size is insufficient. The IntelliFlash Web UI displays a warning message when the metadata space is insufficient for expanding the pool size.

 **Note:** The FIPS certified drives and standard drives are not compatible in the same system. All drives in the system must either be FIPS-certified or standard; and mixing them is not allowed. If a system is detected with FIPS-certified drives and standard drives, then IntelliFlash will not allow you to expand a pool.

To expand an existing pool, complete the following steps:

1. Click **Provision > Pools**.
2. Select a pool from the **Active Pools** list.
3. In the **Overview** tab page, click the **Expand** button.
4. In the **Expand Pool** window, complete the following steps:
  - a) Select a disk size from the **Select disk size** dropdown.
  - b) Select the required disk types to expand the pool:
    - **Data**
    - **iFlash**
  - c) Select **Match disk group size**.

The **Match disk group size** option enables you to expand a pool with the same disk group size as the existing group size in the pool. The **Match disk group size** option is by default enabled.
  - d) (Optional) You can disable the disk integrity check by dragging the slider to the right. By default, IntelliFlash performs the disk integrity check when creating a pool. It is recommended to run the disk integrity check.
  - e) Click **Review**.

After clicking the **Review** option, the **Expand Pool** displays expanded data and metadata details.
  - f) Click **Expand**.
5. Monitor the notifications in the **Progress Notification** screen.

You can view the expanded pool in the **Overview** tab of the **Pools** page.

## Exporting a Pool

You might need to move an active pool to a different IntelliFlash Array for various maintenance operations. This enables you to safely move a pool by exporting it. When a pool is exported, all of the pending data is flushed into the disks and the disks are made ready for removal from the storage array chassis.



**Caution:** Exporting a pool unmounts all shares, LUNs, and the pool itself.

Exporting a pool in the proper way ensures that all data is safe and enables the IntelliFlash OS to import the exported pool with ease.

When you export a pool that is part of an HA pair, the IntelliFlash OS removes it from the HA managed resources. You can import the exported pool to the other controller of the array or to a different array.

To export a pool, complete the following steps:

1. Click **Provision > Pools**.
2. Select a pool from the **Active Pools** list.
3. In the **Overview** tabbed page, click **Export**.
4. In the **Confirmation** screen, click **Yes**.



**Caution:** Exporting a pool unmounts all shares, LUNs, and the pool itself.

The exported pool appears in the **Exported Pools** list.

The exported pool can be imported to a different array or to the same array.

## Importing a Pool

You can import an exported pool to a different storage array after physically adding the disks to a storage array chassis or after completing maintenance operations.

To import a pool, complete the following steps:

1. Click **Provision > Pools**.
2. Select a pool from the **Exported Pools** list.
3. In the exported pool page, click **Import**.
4. In the **Confirmation** screen, click **Yes**.

The imported pool displays in the **Active Pools** list.

## Resetting Pool Errors

When you replace a failed disk with a new disk, the IntelliFlash OS resilvers the newly added disk. However, the pool might have previous errors. You must manually reset the errors to avoid any future disk failures. You can reset the errors from the Pool properties window.



**Note:** Write errors that occur for NVDIMMs will appear in the **Disks** tab of the **Pool** page when the peer controller is down.

To reset the pool errors, complete the following steps:

1. Click **Provision > Pools**.
2. Select a pool from the **Active Pools** list.
3. In the **Overview** tabbed page, click **More** and select **Reset Pool Errors**.
4. In the **Confirmation**, click **Yes**.

## Performing Pool Integrity Check

In general, the IntelliFlash OS automatically performs the checksum, scrubbing, and resilvering processes when required. You can also manually check the integrity of a pool from the **Pools** page.

The **Perform Pool Integrity Check** option verifies the checksums among the disks in a pool, and performs scrubbing and resilvering appropriately.

To check the integrity of a pool, complete the following steps:

1. Click **Provision > Pools**.
2. Select a pool from the **Active Pools** list.
3. In the **Overview** tab, click **More** and select **Perform Pool Integrity Check**.

The IntelliFlash OS performs the pool integrity check on the pool and displays the status. You can stop the pool integrity check in before the process completes.



**Note:** The pool integrity check process can be a time consuming and resource intensive activity.

## Deleting a Pool

### Prerequisites

- Remove all network mappings
- Remove ACLs
- Remove all replication relationships



**Caution:** Deleting a pool from a storage array deletes all of the data and the settings for the pool.

To delete a pool, complete the following steps:

1. Click **Provision > Pools**.
2. Select a pool from the **Active Pools** list.
3. In the **Overview** tabbed page, click **Delete**.
4. In the **Delete Pool** window, select **I acknowledge**.
5. Type the exact name of the pool.
6. If *Two-Factor Authentication (2FA)* is enabled for the user, enter the 2FA application code retrieved from your mobile device to delete the pool.
7. Click **Delete**.
8. In the **Information** window, click **OK**.

## Deleting an Exported Pool



**Caution:** Deleting a pool from a storage array deletes all of the data and the settings for the pool.

To delete an exported pool, complete the following steps:

1. Click **Provision > Pools**.
2. Select a pool from the **Exported Pools** list.
3. In the **Exported Pools** list, select a pool to delete.
4. Click **Delete**.
5. In the **Delete Pool** window, select **I acknowledge**.
6. Type the exact name of the pool.
7. Click **Delete**.
8. In the **Information** window, click **OK**.

## Managing Disk Drives of a Pool

---

## Viewing Disks on the IntelliFlash Systems

The **Settings > Hardware > Disks** page displays information about the drives in the IntelliFlash Array and the expansion shelves connected to it. You can view and identify all of the disks on the IntelliFlash Array using this page.

This page also displays how the disk is being used: the **Disk Type** column indicates whether a disk is used for data, metadata, secondary read cache, secondary write cache, or a spare for legacy pools. For pools created with IntelliFlash Web UI 3.5.x and later, the Disk Type column indicates whether a disk is a data disk (HDD/SSD/NVMe), iFlash disk, or a spare disk for pools. If a disk is part of a pool, the **Pool Name** column displays the name of the pool.

If your array has self-encrypting drives (SEDs), the disk images display the lock icon indicating that they are SEDs.

 **Note:** On array models with the encryption feature support, it is recommended that you back up the encryption master key and keep one copy locally and another copy at a remote location for redundancy. The backed-up master key is required if you have to move all of the drives from one array chassis to another or if the master key gets corrupted due to any reason.

For information about managing SEDs, see [Encryption Overview](#).

The **Settings > Hardware > Disks** displays the following information about the storage controller and expansion shelf:

- A graphical representation of the storage array and expansion shelves
- Storage array model name and serial number
- Expansion shelf name
- Disk (Bay) number
- Disk type (a data disk (HDD/SSD), an iFlash disk, or a spare disk) or (HDD, Meta SSD, Data SSD, Read/Write cache SSD)
- Pool name in which the disk is used
- Size of the disks
- Disk alias
- Toggle button to identify disks on the storage array

On the **Hardware** page, SSDs are indicated by a flash icon in the storage array graphical representation to differentiate them from the HDDs.

The storage array and expansion shelf graphical representations in the **Disk Array** page display a yellow flash icon to indicate the metadata and cache disks for all hardware models (All- Flash and Hybrid) and a white flash icon to indicate data disks for All-Flash models.

To view disks in a storage array, complete the following steps:

1. Click **Settings > Hardware > Disks**.
2. Click on a disk to identify it.  
The IntelliFlash Web UI highlights the disk in the graphic to identify it.
3. Click the **Identify Disk** toggle button to physically identify the drive on the IntelliFlash Array.  
An LED light toggles to on for the selected disk on the storage array.

## Viewing serial number of a controller

You can view the serial numbers of the controllers of an array from the **Disks** page.

To view the serial number of a controller, complete the following steps:

1. Click to **Settings > Hardware > Disks**.
2. In the **Disks** page, next to the array model name, click **View Serials**.

## Searching disks by an alias name

When you receive an email to report any issue with the disk in the IntelliFlash Array. You can use the alias name mentioned in the mail to search the disk on the from **Disks** page.

To search the disk by alias name, complete the following steps:

1. Click **Settings > Hardware > Disks**.
2. Specify the Alias name, in the **Search alias** box.
3. Click the search icon.

## Setting a Disk to Offline

You can change a disk that is part of a pool to the offline state when you discover a problem with the disk, or if you need to offline a disk to carry out maintenance operations. After changing a disk's state to offline, all write or read operations stop on the disk.

 **Note:** Do not offline all of the disks in a RAID group at the same time. For example, if you have a 2-way mirrored RAID group, you can change only one disk to offline in the group. Changing all disks to offline in a group at the same time leads to a pool in the faulted state.

 **Note:** A disk that is in offline state continues to be in the offline state until you bring it online manually. The offline state of a disk does not change even after the system reboots.

After taking a disk offline, the state of the disk is shown as **Offline** and the pool state as **Degraded**.

To offline a disk in a pool, complete the following steps:

1. Click **Provision > Pools**.
2. Select a pool from the **Active Pools** list.
3. In the **Pools** page, click **Disk**s.
4. In the **Disk**s page, select a disk from disk group (**iFlash** or **Data**).
5. Click **More** and select **Take Disk Offline**.
6. In the **Confirmation** screen, click **Yes**.

The disk group displays the state as **Degraded** and the disk state as **Offline**. You can bring the disk back online after completing maintenance operations.

## Replacing a Disk Manually

Before replacing a disk either physically in the array or through the IntelliFlash Web UI, you must take the disk offline using the IntelliFlash Web UI.

 **Note:** The replacement disk must be of the same size as the failed disk or have a larger capacity. The replacement disk cannot be of smaller size than the failed disk.

 **Note:** A replaced disk will resilver. The resilvering process can be a time consuming process, so you need to plan appropriately before the disk replacement.

 **Note:** The FIPS certified drives and standard drives are not compatible in the same system. All drives in the system must either be FIPS-certified or standard; and mixing them is not allowed. If a system is detected with FIPS-certified drives and standard drives, then IntelliFlash will not allow you to replace a disk.

To replace a disk manually, complete the following steps:

1. Click **Provision > Pools**.
2. Select a pool from the **Active Pools** list.
3. In the **Pools** page, click **Disk**s.
4. In the **Disk**s page, select a disk from disk group (**iFlash** or **Data**) that is in the *Offline* state.
5. Click **More** and select **Replace Disk**.
6. In the **Select a disk to replace <disk label>** window, select the **Chassis** number to select a disk for replacement.
7. In the confirmation screen, click **Yes**.
8. Click **OK**.

You can check the resilvering process status in the **Provision > Pools > Active Pools** page.

## Setting a Disk to Online

You can return an offline disk to the online state after completing maintenance operations. After a disk is set to online, the disk syncs with the other disks in the RAID group.

To change a disk to the online state, complete the following steps:

1. Click **Provision > Pools**.
2. Select a pool from the **Active Pools** list.
3. In the **Pools** page, click **Disks**.
4. In the **Disks** page, select the disk with the state **Offline** from disk group (**iFlash or Data**).
5. Click **More** and select **Bring Disk Online**.
6. In the confirmation message screen, click **Yes**.

## Adding a Hot Spare Disk

You can add a spare HDD disk for data disks without disturbing the pool.

 **Note:** For the H-Series Hybrid Storage systems, you cannot add a NVMe disk as a hot spare for meta and iFlash disk groups.

You can view all available disks from the **Settings > Hardware > Disks** page.

To add a hot spare disk, complete the following steps:

1. Click **Provision > Pools**.
2. Select a pool from the **Active Pools** list.
3. In the **Pools** page, click **Disks**.
4. In the **Disks** page, click **Add Hot Spare**.
5. In the **Select a Hot Spare Disk** window, select the **Chassis** and **Disk** number, and then click **Add**.
6. In the confirmation message, click **Yes**.

A new spare disk displays under the **Hot Spare** disks and the **State** field displays as **Available**.

## Removing a Hot Spare Disk

You can remove a hot spare disk from the spare disks group and use it as a data disk to expand the pool.



**Note:** You cannot remove a spare disk that is being actively used in the pool.

To remove a hot spare disk from the **Hot Spare** list, complete the following steps:

1. Click **Provision > Pools**.
2. Select a pool from the **Active Pools** list.
3. In the **Pools** page, click **Disks**.
4. In the **Disks** page, select the **Hot Spare** disk group.
5. From the **Hot Spare** disk group list, select a disk.
6. Click **More** and select **Remove Disk**.
7. In the confirmation screen, click **Yes**.  
The disk disappears from the **Hot Spare** disks list.

## Managing System Pool

---

### Viewing System Pool Details

To view system pool details, complete the following step:

Click **Settings > Administration > System OS**.

You can view the status of the system pools on ha-controller-a and ha-controller-b and the space usage of the pool. From the **System OS** page, you can also reset system pool errors and perform a pool integrity check for the system pool.



#### Attention:

Contact IntelliFlash Technical Support if you notice any problems with the System pool.

### Related Topics

[System Pool](#)

### Resetting System Pool Errors

To reset errors in the system pool, complete the following steps:

1. Click **Settings > Administration > System OS**.
2. In the **System OS** page, click **More** and select **Reset Pool Errors**.



**Attention:** Contact IntelliFlash Technical Support if you notice any problems with the System pool.

## Related Topics

[System Pool](#)

### Running Pool Integrity Check on System Pool

To perform the pool integrity check on the system pools, complete the following steps:

1. Click **Settings > Administration > System OS**.
2. In the **System OS** page, click **More** and select **Perform Pool Integrity Check**.  
The IntelliFlash OS performs the pool integrity check on the pool and displays the status.



**Note:** The pool integrity check process can be a time consuming and resource intensive activity. If necessary, you can stop the pool integrity check before the process completes.

## Related Topics

[System Pool](#)



---

# Chapter 6

---

## Projects

---

### Topics:

- *IntelliFlash Projects*
- *Project Templates*
- *Overriding Project Level Properties*
- *Projects Menu*
- *NPIV Ports and Projects after Upgrade*
- *Creating Projects*
- *Managing Projects*
- *iSCSI and FC Mappings*
- *Share Creation Defaults*
- *Deleting a Project*

## IntelliFlash Projects

---

IntelliFlash projects are logical containers for grouping storage components. Projects simplify storage management tasks. Projects can include Shares and LUNs, Snapshots, Clones, and Replicas (replication snapshots) created from those Shares and LUNs.

Projects possess common data storage configuration properties which are applicable to the contents of projects. The LUNs and shares created within a project inherit most of the configurations defined at the project level.

With the IntelliFlash OS, you can create projects based on NAS and SAN protocols. By using the **Add Project** wizard, you can create various project types such as an iSCSI project, an SMB project, an NFS project, an FC project or a multi-protocol project. However, as projects are simply logical containers, the IntelliFlash OS enables you to use any project for both NAS or SAN protocols regardless of which protocol you use when creating it.

To achieve this, the IntelliFlash OS enables you to perform the following:

- Modify the project properties
- Override the project level configuration setting when creating a share or LUN
- Provide an option to enable SMB and NFS sharing
- Add initiator and target mapping details

 **Note:** The IntelliFlash OS might not allow you to edit some properties if you use project templates.

The following changes have been made in the IntelliFlash Web UI:

- The compression types are changed in the UI. The new options are **High Compression** and **Optimal Performance**, with Optimal Performance being the default compression type.
- The compression algorithm for **Optimal Performance** is lz4. The compression algorithm for **High Compression** is igzip.
- IntelliFlash automatically assigns the **Optimal Performance** compression type for projects created from the project templates. However, when you are creating generic projects, you have the option to choose **Optimal Performance** or **High Compression**. You can also disable the compression by selecting **OFF**.
- You can change the compression type or disable compression in the **Advanced Settings** tab.
- The older compression types are renamed as **Legacy** and will continue to be supported.
- The **Data Synchronization** and the **LogBias** fields are removed from the web UI. Internally in IntelliFlash, Data Synchronization is set to **Always** and LogBias is set to **Latency**.
- The **Primary Cache** and **Secondary Cache** fields are combined and renamed as **Read Cache**.

## Project Templates

---

IntelliFlash also includes project templates that enable you to create Shares and LUNs that are preconfigured for specific applications, such as VMware, SQL Server, Exchange, and VDI.

You can use the project templates based on the purpose for which you are providing the storage. IntelliFlash provides the following project templates:

- **SQL Server**
- **Virtual Server**
- **VMware VDI**
- **Hyper-V VDI**
- **Exchange Server**
- **Generic**

You can select the desired project template from the **Purpose** property of **Add Project** wizard. The Purpose property describes the purpose for which the project has been created.

Depending on the selected project template, the IntelliFlash OS adds shares or LUNs with predefined properties. You can create projects for the iSCSI, FC, NFS, and SMB protocols. The wizard provides a template for required LUNs or shares. You can name the LUNs and shares, or use the default names, provide the LUN size and number of LUNs. The IntelliFlash OS automatically creates those LUNs or shares within that project.

The app-centric project template specific to the protocol and purpose displays only the shares specific to that project's purpose. For example, an NFS project created for the purpose of VMware VDI allows creating a share for VMware VDI purpose and Generic purpose only.

After creating a new project using a project template, you can create additional LUNs or shares for the selected protocol.

 **Note:** Use the configuration settings provided by the project templates for storage efficiency and data protection.

For LUNs and Shares, the project templates create different types of LUNs and Shares with the required values for the configuration properties such as:

- Block size for LUNs and shares
- Default snapshot policy
- Compression type
- Deduplication status
- Primary Cache (DRAM)
- Secondary Cache (SSD)

## SQL Server Template

The **SQL Server** project template provides a template of required LUN types. You can select the required type and the number of LUNs. The templates preselect the configuration properties which are optimum for SQL Server.

The SQL Server template creates the following LUN types:

- DataLUN
- LogLUN
- SqlBackupLUN
- TempDBDataLUN
- TempDBLogLUN

- LargeObjLUN

You can configure iSCSI, FC, and SMB 3.0 protocols with the **SQL Server** project template.

You can create a maximum of 100 LUNs for each LUN type using this project template. The project template recommends the size of the additional LUN types, based on the database LUN (DataLUN) size.

By default, the size of other LUN types is 10% the size of the database LUN. For example, if the database LUN is 20 GiB, other LUN types have a size of 2 GiB each.

The following table lists the default and recommended settings for the **SQL Server** project template.

Configuration Property	Default value
Compression type	lz4 for all LUN types
Deduplication	off
Block Size	64KB
Snapshot Policy	30minutes-Daily-Weekly+Quiesce
Purpose	SQL Server
Primary and Secondary cache	Enabled (All) for DB LUNs and none for log LUNs
Log Compression	Enabled



**Note:** From the **Summary** page of the wizard, click the **More** link to view the Compression, Deduplication and Block Size settings per LUN or Share.

## Virtual Server Template

You can use the **Virtual Server** project template to provide storage for VMware virtualization environments. The template pre-selects the configuration properties which are optimum for VMware environments. You can configure iSCSI, FC, NFS, and SMB 3.0 protocols with the **Virtual Server** project template.

By default, the **New Project** wizard prompts you to create a **VirtualServerLUN** of 10 GiB for the FC and iSCSI protocols and a **VirtualServerShare** for the NFS protocol.

The following table lists the default and recommended settings for **Virtual Server** project template:

Configuration Property	Default value
Compression type	lz4 for LUN and Share
Deduplication	ON for LUN and Share
Block size	32 KB for LUN and Share
Snapshot Policy	Hourly-Daily-Weekly+Quiesce

Configuration Property	Default value
Primary and Secondary cache	Enabled (All) for DB LUNs and none for log LUNs
Purpose	Virtual Server

 **Note:** From the **Summary** page of the wizard, click the **More** link to display the Compression, Deduplication and Block Size settings per LUN or Share.

## VMware VDI Template

You can use the VMware VDI project template to provide storage for deploying VMware Virtual Desktop Infrastructure (VDI) VMs. This template enables you to create storage for persistent and non-persistent VDI desktops. The VMware VDI project template helps you calculate the LUN size and creates a single share based on the estimated number of virtual desktops and average size of a desktop.

For the VMware VDI project, the NFS share size is set as quota. You can use the iSCSI, NFS, or FC protocol when creating a VMware VDI project template.

 **Note:** The VMware VDI project template automatically calculates the size of the LUN using the estimated number of virtual desktops and average size of each desktop. The **New Project** wizard creates one **VMwareVDILUN** for the iSCSI or FC protocol, and one **VMwareVDIShare** for the NFS protocol with the calculated size.

The following table lists the default and recommended settings for the **VMware VDI** project template:

Configuration Property	Default value
Compression type	Iz4 for LUN and Share
Deduplication	ON for LUN and Share
Block size	32 KB for LUN and Share
Snapshot Policy	Hourly-Daily-Weekly
Primary and Secondary cache	Enabled (All) for LUN and Share
Purpose	VMware VDI
Estimated total number virtual desktops	<ul style="list-style-type: none"> <li>• 40 for persistent desktops</li> <li>• 100 for non-persistent desktops</li> <li>• 100 for NFS project template</li> </ul>
LUN/Share size	<ul style="list-style-type: none"> <li>• 800 GiB for persistent desktop</li> <li>• 2000 GiB for non-persistent desktop</li> <li>• 800 GiB for an NFS share</li> </ul>

## Hyper-V VDI Template

You can use the Hyper-V VDI project template to provide storage for deploying Hyper-V Virtual Desktop Infrastructure (VDI). You can use the iSCSI, FC and SMB protocols when creating a project with the Hyper-V VDI project template.

 **Note:** The Hyper-V VDI project template automatically calculates the size of the LUN using the estimated number of virtual desktops and the average size of each desktop. The **New Project** wizard creates one **HyperVVDILUN** for the iSCSI or FC protocol, and one **HyperVVDIShare** for the SMB protocol with the calculated size.

The following table lists the default and recommended settings for the **Hyper-V VDI** project template.

Configuration Property	Default value
Compression type	Iz4
Deduplication	ON for LUN and Share
Block Size	32 KB for LUN and Share
Snapshot Policy	Daily-Weekly
Primary and Secondary cache	Enabled (All) for DB LUNs and none for log LUNs
Purpose	HyperV VDI

 **Note:** From the **Summary** page of the wizard, click the **More** link to display the Compression, Deduplication and Block Size settings per LUN or Share.

## Generic Template

The **Generic** project template is a flexible project template that creates a blank project with no LUNs or shares. You can use the Generic project template when the other project templates do not serve your requirements.

 **Note:** For double parity RAID pool, use a **Block size** greater than or equal to **16 KB** for better space utilization.

You can use one or more protocols when creating a project using the Generic project template. For more information, see [Differences Between Generic and Other Project Templates](#).

## Microsoft Exchange Server Template

You can use the Exchange Server project template to provide storage for Exchange Servers. The Exchange Server project template supports Exchange Server 2010 and Exchange Server 2013.

Each of these two templates allows you to provision storage for multiple Exchange Servers. They create one database LUN and one log LUN for each Exchange Server. These templates also help you to estimate the size of the LUN based on the number of email users, the email frequency, and the average size of an email.

The Exchange Server template provides the **Enable Exchange Database Availability Group (Enable Exchange DAG)** option. When you select the DAG option, which creates a passive DB LUN for each Exchange Server when enabled.

You can use the iSCSI and the FC protocols with the Exchange Server project templates.

### DB LUN Calculator

The IntelliFlash Web UI provides a calculator for estimating the DB LUN size in Exchange Servers. In the **Add Project** wizard, click **Calculate Exchange DB Size** to estimate the DB LUN size that you require.

- Average number of email messages per day
- Average size of an email message
- Email messages retention period (in years)
- Number of mailboxes

The size of the LUN is updated when you click **Calculate & Update**.

The following table lists the default and recommended settings for the **Exchange Server** project template:

Configuration Property	Default value
Compression type	Iz4
Deduplication status	on for DB LUNs and off for log LUNs
Block size	32 KB for DB LUNs and 64 KB for log LUNs
Default snapshot policy	30minutes-Daily-Weekly+Quiesce
Primary and Secondary cache	Enabled (All ) for DB LUNs and none for log LUNs
Purpose	Exchange Server
Log Compression	Enabled for DB LUNs and Disabled for Log LUNs

### Differences Between Generic and Other Project Templates

The following compares the **Generic** project template to other project templates. Knowing these differences might help you in selecting an appropriate project template during storage provision.

Other Project Templates	Generic Project
Use the application-specific project templates for providing storage space for specific applications. Project templates are available for applications, such as SQL Server, server virtualization, VMware VDIs, Hyper-V VDI, and Exchange Server.	Use a project with <i>Generic</i> purpose only when the available project templates do not serve your requirements.

Other Project Templates	Generic Project
Project templates make storage provisioning simple and quick.	A project created with the Generic project template has very few predefined project properties and does not include any shares or LUNs. Therefore, you need to manually configure most project properties. Further, you need to manually create and configure shares and LUNs in the project. This may be complex and time consuming in some scenarios for some users.
Projects created support the required protocols.	Project can support multiple (any or all) protocols.
Project templates apply default configuration properties that are optimum for a particular application type. The <b>Add Project</b> wizard preselects properties such as, deduplication, compression type, block size, default snapshot policy and so on.	Generic project wizard provides you a choice to select the configuration properties suitable for your requirements.
Project templates wizard automatically creates required type of LUNs or Shares during project creation. You can provide LUN or Share names, provide required size, and number of LUNs or Shares.	The Generic project wizard does not create LUNs or Shares automatically.
All LUNs created automatically by project templates wizard are thin LUNs.	You can create both thin and thick LUNs.
In a project template, you can create supported additional LUNs or Shares only for the allowed protocol.	In a Generic project, you can create LUNs or Shares for any protocol.
The count of the LUN is added as a suffix to the LUN name.	LUNs and Shares are created after creating a project and hence no such option of LUN count is available.
Project templates wizard automatically selects the optimum default snapshot policy type.	You need to plan and select a suitable default snapshot policy type.
The VMware VDI project template automatically calculates required storage space after you providing the required number of VDIs.	You need to calculate required storage space manually. Generic project does not calculate required storage space automatically.
The Exchange Server project templates automatically calculates required storage space after you providing the required number mail boxes, number of Exchange Servers and other details.	You need to calculate manually. Generic project does not calculate automatically.

Other Project Templates	Generic Project
You can create LUNs and shares for any application-specific purpose using the protocol (iSCSI, FC, NFS, or SMB) allowed for the selected purpose .	In all of the project templates you can create a LUN or Share with Generic purpose using any of the supported protocols (iSCSI, FC, NFS, or SMB).

## Overriding Project Level Properties

---

Overriding project level properties is the process of disabling the global properties set at the project level for a share or LUN, and adding properties specific only to that share or LUN.

You can override general properties, snapshot properties, NFS and SMB sharing, and LUN mapping details of an existing share or LUN. IntelliFlash also permits overriding properties when creating a share or LUN. However, you can still revert to the project level settings after you have overridden them.

In IntelliFlash, you can set properties specific to a share or LUN from the **Share Settings** and **LUN Settings** windows, respectively.

### Related Topics

[Managing Projects](#)

## Projects Menu

---

In the IntelliFlash Web UI, the project details can be accessed under the **Provision > Projects** menu.

You can do the following in the **Projects** page:

- Create projects using project templates.
- View and manage all projects (Local and Replica) in the array from the left pane of the **Projects** page.
- View details of projects by clicking the right arrow icon at the top-right of the pane.
- Filter projects based on pool and project names.
- Perform project-related operations from the **Manage** dropdown menu in the pane.
- Manage advanced and general project settings from the **Generic Project Settings** page (**Provision > Projects > Manage > Settings**)
- Manage project snapshots and replication from the **Data Protection** page (**Provision > Projects > Manage > Data Protection**)
- Provide access permissions for shares and LUNs in a project from the **Project Access** page (**Provision > Projects > Manage > Access**)
- Migrate projects within the same array or a remote array from the **Project Access** page (**Provision > Projects > Manage > Migration**)
- Migrate LUNs within the same array or a remote array from the **Project Access** page (**Provision > LUNs > Manage > Migration**)

 **Note:** The **Back** button in all the project UI pages allows you to return to the main **Projects** page.

## NPIV Ports and Projects after Upgrade

NPIV is enabled when the array is upgraded to version 3.7.x.x or later. After upgrading the array, the migration of LUNs from the physical HBA FC target groups to the default NPIV target groups is performed at a project level to avoid disruption. For each LUN mapped with a physical HBA FC target group, the default NPIV target groups are added automatically in the **Project > Manage > Access > FC** page.

When initiators discover the NPIV target groups, a **Use NPIV Ports** button appears in the project access page, indicating that the LUNs in the project are now ready to be mapped to the NPIV target group and thus change their representation to the **ActiveOnly** representation.

Click **Use NPIV Ports** to change the LUNs to ActiveOnly. After the LUNs are migrated to ActiveOnly state, the physical HBA FC target groups are deleted and only the NPIV target groups are retained.

 **Note:**

- If you migrate all the non-NPIV projects to ActiveOnly LUNs after upgrading to 3.7.x.x or later, then any new LUNs you create can only have ActiveOnly representation..
- To support the Cisco UCS Manager, the format for the WWPN and WWNN of the NPIV Fibre Channel ports is changed to NAA 5h format from the 3h format.

### Related Topics:

[Understanding NPIV](#)

[Migrating Non-NPIV Projects to NPIV after Upgrade](#)

## Creating Projects

### Creating an iSCSI Project for SQL Server

For more information about the SQL Server OLTP Application project template, see [SQL Server Template](#). For more information on project templates, see [Project Templates](#).

To create an iSCSI project for SQL Server, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab on the left pane, click **New**.  
The **New Project** wizard appears.
3. In the **Name and Space configuration for Project** screen, complete the following steps:
  - a) In the **Project Name** field, type a name for the project.

- b) In the **Pool** field, select the pool.
- c) In the **Purpose** field, select **SQL Server** as the purpose of the project.
- d) In the **Configure Access** area, select **iSCSI**.
- e) Select **Create Project without LUNs and Shares** if you do not want to include LUNs and shares in the new project.  
The **App Config** page does not appear when you enable this option.
- f) Click **Next**.
4. In the **SQL Server** screen, complete the following steps:
- a) In the **SQL Server** section, type a name for the **DataLUN** (or use the default name). Select or type the size, the unit of memory (MiB, GiB, or TiB), and the count for the LUN.
-  **Note:** The default size of a database LUN is 10 GiB and the count is one. The LUN count is added as a suffix to the LUN name.
- b) In the **Additional LUNs** section, type names for the **LogLUN**, **SqlBackupLUN**, **TempDBDataLUN**, **TempDBLogLUN**, and **LargeObjLUN**. Select size and count for the additional LUNs.
-  **Note:**
- The size of additional LUNs is 10% of the database LUN. The wizard automatically calculates the additional LUNs size based on the DB LUN size. However, you can modify the size.
  - The wizard does not create large object LUN type automatically. If you need it, you must select the required count.
  - The default count for **LargeObjLUN** is **0** and hence the field is disabled. Increase the count to modify the **LargeObjLUN** size.
- c) Click **Next**.
5. In the **iSCSI Target Configuration** screen, complete the following steps:

If...	Then...
<b>You want to select the default target.</b>	<ol style="list-style-type: none"> <li>1. Click <b>Default Target</b>.</li> <li>2. Click <b>Next</b>.</li> </ol>
<b>You want to select an existing target.</b>	<p>Complete the following steps:</p> <ol style="list-style-type: none"> <li>1. Click <b>Choose Target</b>.</li> <li>2. Select the target from the <b>Choose Target</b> dropdown.</li> </ol> <p>The target group and status of the selected target appear.</p>

If...	Then...
	<p>3. (Optional) Select <b>Authentication for Target</b> to authenticate CHAP. You can select <b>None</b>, <b>CHAP</b>, or <b>Mutual</b>.</p> <p> <b>Note:</b></p> <ul style="list-style-type: none"> <li>When you change <b>Authentication for Target</b> from <b>None</b> to <b>CHAP</b>, IntelliFlash displays the message: <b>Modifying the authentication mechanism affects the existing iSCSI sessions. Do you want to continue? [Yes   No]</b>. Click <b>Yes</b> to continue.</li> <li>When you change <b>Authentication for Target</b> from <b>None</b> to <b>Mutual</b>, provide the CHAP username and password. The credentials are used by the initiator to authenticate the target.</li> </ul> <p>4. Click <b>Next</b>.</p>
<b>You want to create a new target.</b>	<p>Complete the following steps:</p> <ol style="list-style-type: none"> <li>Click <b>Create Target</b>.</li> <li>In the <b>Target Name</b> field, type a name. The wizard uses the provided target name to create a new target group and displays it in the <b>Target Group</b> field.</li> <li>To add the target to an existing target group, click the <b>select group</b> link and select the target group from the list. To select the default target group instead, select <b>default</b>.</li> <li>In the <b>Choose Network Bindings</b> section, select the required IP address.</li> <li>(Optional) Select <b>Authentication for Target</b> to authenticate CHAP. You can select <b>None</b>, <b>CHAP</b>, or <b>Mutual</b>.</li> </ol> <p> <b>Note:</b></p> <ul style="list-style-type: none"> <li>When you change <b>Authentication for Target</b> from <b>None</b> to <b>CHAP</b>, IntelliFlash displays the message: <b>Modifying the authentication mechanism affects the existing iSCSI sessions. Do you want to continue? [Yes   No]</b>. Click <b>Yes</b> to continue.</li> </ul>

If...	Then...
	<p>existing iSCSI sessions. Do you want to continue? [Yes   No]. Click <b>Yes</b> to continue.</p> <ul style="list-style-type: none"> <li>When you change <b>Authentication for Target</b> from <b>None</b> to <b>Mutual</b>, provide the CHAP username and password. The credentials are used by the initiator to authenticate the target.</li> </ul> <p>6. Click <b>Next</b>.</p>

6. In the **iSCSI Initiator Group Configuration** screen, complete the following steps:

If...	Then...
<b>You want to provide access to the LUN without any restrictions.</b>	<p>Click <b>All</b> and then click <b>Next</b>.</p> <p> <b>Note:</b> When you select <b>All</b>, it enables existing initiators as well as new initiators to access the newly created LUN.</p>
<b>You want to use an existing initiator group.</b>	<p>Complete the following steps:</p> <ol style="list-style-type: none"> <li>Click <b>Choose Initiator Group</b>.</li> <li>Click the <b>Initiator Group</b> dropdown and select an initiator group from the list.</li> <li>Click <b>Next</b>.</li> </ol>
<b>You want to create a new initiator group.</b>	<p>Complete the following steps:</p> <ol style="list-style-type: none"> <li>Click <b>Create Initiator Group</b>.</li> <li>In the <b>Initiator Group</b> field, type a name for the group.</li> <li>In the <b>Initiator</b> field, type an initiator name. A valid initiator name must start with <i>iqn.yyyy-mm.[reverse-domain-name]</i> or must be an EUI-64 identifier.</li> <li>Click <b>Add Initiator</b>.</li> <li>Repeat steps (c) and (d) to add additional initiators to the group.</li> <li>To provide CHAP authentication, select <b>CHAP Credentials</b> and provide the CHAP username</li> </ol>

If...	Then...
	<p>and password. The credentials are used by the initiator to authenticate the target.</p> <p>7. Click <b>Next</b>.</p>

7. (Optional) In the **Snapshot Schedules** screen, the wizard selects the recommended snapshot policy depending on the project's purpose.
  - If you want to retain the recommended preset profile, click **Next**.
  - If you want to customize the profile, select a profile from the **Schedule** list and customize it according to your requirements. You can add more conditions by clicking the **Add** (+) icon.

For more information, see [Preset Profiles for Snapshots](#) and [Custom Snapshot Schedules](#).

8. (Optional) In the **Snapshot Schedules** screen, the default snapshot policy of the project is automatically selected. You can retain the default preset profile or customize the profile.
  - If you want to retain the default preset profile, click **Next**.
  - If you want to customize the profile, click **Override project snapshot policy**. Select a profile from the **Schedule** list and customize it according to your requirements. You can add more conditions by clicking the **Add** (+) icon.

For more information, see [Preset Profiles for Snapshots](#), [Custom Snapshot Schedules](#), and [Overriding a Project Snapshot Schedule](#).

9. In the **Summary** screen, review the summary and click **Create**.

You can click the **More** link in the **Summary** page to see complete summary details.

## Creating an iSCSI Project for Virtual Server Application

For more information about the Virtual Server project template, see [Virtual Server Template](#).

To create an iSCSI project for virtual server, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab on the left pane, click **New**.  
The **New Project** wizard appears.
3. In the **Name and Space configuration for Project** screen, complete the following steps:
  - a) In the **Project Name** field, type a name for the project.
  - b) In the **Pool** field, select the pool.
  - c) In the **Purpose** field, select **Virtual Server** as the purpose of the project.
  - d) In the **Configure Access** area, select **iSCSI**.
  - e) Select **Create Project without LUNs and Shares** if you do not want to include LUNs and shares in the new project.  
The **App Config** page does not appear when you enable this option.

- f) Click **Next**.
4. In the **Virtual Server** screen, complete the following steps:
- In the **Virtual Server** section, type a name for the Virtual Server LUN (or use the default name). Select or type the size, the unit of memory (MiB, GiB, or TiB), and the count for the LUN.
-  **Note:** The default size of a database LUN is 10 GiB and the count is one. The LUN count is added as a suffix to the LUN name.
- Click **Next**.
5. In the **iSCSI Target Configuration** screen, complete the following steps:

If...	Then...
<b>You want to select the default target.</b>	<ol style="list-style-type: none"> <li>Click <b>Default Target</b>.</li> <li>Click <b>Next</b>.</li> </ol>
<b>You want to select an existing target.</b>	<p>Complete the following steps:</p> <ol style="list-style-type: none"> <li>Click <b>Choose Target</b>.</li> <li>Select the target from the <b>Choose Target</b> dropdown.</li> </ol> <p>The target group and status of the selected target appear.</p> <ol style="list-style-type: none"> <li>(Optional) Select <b>Authentication for Target</b> to authenticate CHAP. You can select <b>None</b>, <b>CHAP</b>, or <b>Mutual</b>.</li> </ol> <p> <b>Note:</b></p> <ul style="list-style-type: none"> <li>When you change <b>Authentication for Target</b> from <b>None</b> to <b>CHAP</b>, IntelliFlash displays the message: <b>Modifying the authentication mechanism affects the existing iSCSI sessions. Do you want to continue? [Yes   No]</b>. Click <b>Yes</b> to continue.</li> <li>When you change <b>Authentication for Target</b> from <b>None</b> to <b>Mutual</b>, provide the CHAP username and password. The credentials are used by the initiator to authenticate the target.</li> </ul> <ol style="list-style-type: none"> <li>Click <b>Next</b>.</li> </ol>

If...	Then...
<b>You want to create a new target.</b>	<p>Complete the following steps:</p> <ol style="list-style-type: none"> <li>1. Click <b>Create Target</b>.</li> <li>2. In the <b>Target Name</b> field, type a name. The wizard uses the provided target name to create a new target group and displays it in the <b>Target Group</b> field.</li> <li>3. To add the target to an existing target group, click the <b>select group</b> link and select the target group from the list. To select the default target group instead, select <b>default</b>.</li> <li>4. In the <b>Choose Network Bindings</b> section, select the required IP address.</li> <li>5. (Optional) Select <b>Authentication for Target</b> to authenticate CHAP. You can select <b>None</b>, <b>CHAP</b>, or <b>Mutual</b>.</li> </ol> <div style="background-color: #f0f0f0; padding: 10px;"> <p> <b>Note:</b></p> <ul style="list-style-type: none"> <li>• When you change <b>Authentication for Target</b> from <b>None</b> to <b>CHAP</b>, IntelliFlash displays the message: <b>Modifying the authentication mechanism affects the existing iSCSI sessions. Do you want to continue? [Yes   No]</b>. Click <b>Yes</b> to continue.</li> <li>• When you change <b>Authentication for Target</b> from <b>None</b> to <b>Mutual</b>, provide the CHAP username and password. The credentials are used by the initiator to authenticate the target.</li> </ul> </div> <ol style="list-style-type: none"> <li>6. Click <b>Next</b>.</li> </ol>

6. In the **iSCSI Initiator Group Configuration** screen, complete the following steps:

If...	Then...
<b>You want to provide access to the LUN without any restrictions.</b>	<p>Click <b>All</b> and then click <b>Next</b>.</p> <div style="background-color: #f0f0f0; padding: 10px;"> <p> <b>Note:</b></p> </div>

If...	Then...
	When you select <b>All</b> , it enables existing initiators as well as new initiators to access the newly created LUN.
<b>You want to use an existing initiator group.</b>	<p>Complete the following steps:</p> <ol style="list-style-type: none"> <li>Click <b>Choose Initiator Group</b>.</li> <li>Click the <b>Initiator Group</b> dropdown and select an initiator group from the list.</li> <li>Click <b>Next</b>.</li> </ol>
<b>You want to create a new initiator group.</b>	<p>Complete the following steps:</p> <ol style="list-style-type: none"> <li>Click <b>Create Initiator Group</b>.</li> <li>In the <b>Initiator Group</b> field, type a name for the group.</li> <li>In the <b>Initiator</b> field, type an initiator name. A valid initiator name must start with <i>iqn.yyyy-mm.[reverse-domain-name]</i> or must be an EUI-64 identifier.</li> <li>Click <b>Add Initiator</b>.</li> <li>Repeat steps (c) and (d) to add additional initiators to the group.</li> <li>To provide CHAP authentication, select <b>CHAP Credentials</b> and provide the CHAP username and password. The credentials are used by the initiator to authenticate the target.</li> <li>Click <b>Next</b>.</li> </ol>

- (Optional) In the **Snapshot Schedules** screen, the wizard selects the recommended snapshot policy depending on the project's purpose.
  - If you want to retain the recommended preset profile, click **Next**.
  - If you want to customize the profile, select a profile from the **Schedule** list and customize it according to your requirements. You can add more conditions by clicking the **Add** (+) icon.

For more information, see [Preset Profiles for Snapshots](#) and [Custom Snapshot Schedules](#).

- (Optional) In the **Snapshot Schedules** screen, the default snapshot policy of the project is automatically selected. You can retain the default preset profile or customize the profile.
  - If you want to retain the default preset profile, click **Next**.

- If you want to customize the profile, click **Override project snapshot policy**. Select a profile from the **Schedule** list and customize it according to your requirements. You can add more conditions by clicking the **Add** (+) icon.

For more information, see [Preset Profiles for Snapshots](#), [Custom Snapshot Schedules](#), and [Overriding a Project Snapshot Schedule](#).

9. In the **Summary** screen, review the summary and click **Create**.

You can click the **More** link in the **Summary** page to see complete summary details.

## Creating an iSCSI Project for VMware VDI

For more information about the VMware VDI project template, see [VMware VDI Template](#).

To create an iSCSI project for VMware VDI, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab on the left pane, click **New**.  
The **New Project** wizard appears.
3. In the **Name and Space configuration for Project** screen, complete the following steps:
  - a) In the **Project Name** field, type a name for the project.
  - b) In the **Pool** field, select the pool.
  - c) In the **Purpose** field, select **VMware VDI** as the purpose of the project.
  - d) In the **Configure Access** area, select **iSCSI**.
  - e) Select **Create Project without LUNs and Shares** if you do not want to include LUNs and shares in the new project.  
The **App Config** page does not appear when you enable this option.
  - f) Click **Next**.
4. In the **VMware VDI** screen, complete the following steps:
  - a) Select **Persistent** or **Non-Persistent** desktop type.
  - b) Type **Estimated total number of Desktops**.
  - c) Type **Average Size of a Desktop**.
  - d) Type **Prefix of the LUN**.



**Note:** The **Add Project** wizard creates one Share of 2000 GiB per 100 non-persistent desktops. The wizard creates one Share of 800 GiB per 40 persistent desktops. By default, the average virtual desktop size is 20 GiB.

5. In the **iSCSI Target Configuration** screen, complete the following steps:

If...	Then...
<b>You want to select the default target.</b>	<ol style="list-style-type: none"> <li>Click <b>Default Target</b>.</li> <li>Click <b>Next</b>.</li> </ol>
<b>You want to select an existing target.</b>	<p>Complete the following steps:</p> <ol style="list-style-type: none"> <li>Click <b>Choose Target</b>.</li> <li>Select the target from the <b>Choose Target</b> dropdown. The target group and status of the selected target appear.</li> <li>(Optional) Select <b>Authentication for Target</b> to authenticate CHAP. You can select <b>None</b>, <b>CHAP</b>, or <b>Mutual</b>.</li> </ol> <p> <b>Note:</b></p> <ul style="list-style-type: none"> <li>When you change <b>Authentication for Target</b> from <b>None</b> to <b>CHAP</b>, IntelliFlash displays the message: <i>Modifying the authentication mechanism affects the existing iSCSI sessions. Do you want to continue? [Yes   No]</i>. Click <b>Yes</b> to continue.</li> <li>When you change <b>Authentication for Target</b> from <b>None</b> to <b>Mutual</b>, provide the CHAP username and password. The credentials are used by the initiator to authenticate the target.</li> </ul> <ol style="list-style-type: none"> <li>Click <b>Next</b>.</li> </ol>
<b>You want to create a new target.</b>	<p>Complete the following steps:</p> <ol style="list-style-type: none"> <li>Click <b>Create Target</b>.</li> <li>In the <b>Target Name</b> field, type a name. The wizard uses the provided target name to create a new target group and displays it in the <b>Target Group</b> field.</li> <li>To add the target to an existing target group, click the <b>select group</b> link and select the target group from the list. To select the default target group instead, select <b>default</b>.</li> </ol>

If...	Then...
	<p>4. In the <b>Choose Network Bindings</b> section, select the required IP address.</p> <p>5. (Optional) Select <b>Authentication for Target</b> to authenticate CHAP. You can select <b>None</b>, <b>CHAP</b>, or <b>Mutual</b>.</p> <p> <b>Note:</b></p> <ul style="list-style-type: none"> <li>When you change <b>Authentication for Target</b> from <b>None</b> to <b>CHAP</b>, IntelliFlash displays the message: <b>Modifying the authentication mechanism affects the existing iSCSI sessions. Do you want to continue? [Yes   No]</b>. Click <b>Yes</b> to continue.</li> <li>When you change <b>Authentication for Target</b> from <b>None</b> to <b>Mutual</b>, provide the CHAP username and password. The credentials are used by the initiator to authenticate the target.</li> </ul> <p>6. Click <b>Next</b>.</p>

6. In the **iSCSI Initiator Group Configuration** screen, complete the following steps:

If...	Then...
<b>You want to provide access to the LUN without any restrictions.</b>	<p>Click <b>All</b> and then click <b>Next</b>.</p> <p> <b>Note:</b></p> <p>When you select <b>All</b>, it enables existing initiators as well as new initiators to access the newly created LUN.</p>
<b>You want to use an existing initiator group.</b>	<p>Complete the following steps:</p> <ol style="list-style-type: none"> <li>Click <b>Choose Initiator Group</b>.</li> <li>Click the <b>Initiator Group</b> dropdown and select an initiator group from the list.</li> <li>Click <b>Next</b>.</li> </ol>
<b>You want to create a new initiator group.</b>	<p>Complete the following steps:</p> <ol style="list-style-type: none"> <li>Click <b>Create Initiator Group</b>.</li> </ol>

If...	Then...
	<ol style="list-style-type: none"> <li>2. In the <b>Initiator Group</b> field, type a name for the group.</li> <li>3. In the <b>Initiator</b> field, type an initiator name. A valid initiator name must start with <i>iqn.yyyy-mm.[reverse-domain-name]</i> or must be an EUI-64 identifier.</li> <li>4. Click <b>Add Initiator</b>.</li> <li>5. Repeat steps (c) and (d) to add additional initiators to the group.</li> <li>6. To provide CHAP authentication, select <b>CHAP Credentials</b> and provide the CHAP username and password. The credentials are used by the initiator to authenticate the target.</li> <li>7. Click <b>Next</b>.</li> </ol>

7. (Optional) In the **Snapshot Schedules** screen, the wizard selects the recommended snapshot policy depending on the project's purpose.
- If you want to retain the recommended preset profile, click **Next**.
  - If you want to customize the profile, select a profile from the **Schedule** list and customize it according to your requirements. You can add more conditions by clicking the **Add** (+) icon.

For more information, see [Preset Profiles for Snapshots](#) and [Custom Snapshot Schedules](#).

8. In the **Summary** screen, review the summary and click **Create**.

You can click the **More** link in the **Summary** page to see complete summary details.

## Creating an iSCSI Project for Hyper-V VDI

For more information about the Hyper-V VDI project template, see [Hyper-V VDI Template](#).

To create an iSCSI project for Hyper-V VDI, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab on the left pane, click **New**.  
The **New Project** wizard appears.
3. In the **Name and Space configuration for Project** screen, complete the following steps:
  - a) In the **Project Name** field, type a name for the project.
  - b) In the **Pool** field, select the pool.
  - c) In the **Purpose** field, select **Hyper-V VDI** as the purpose of the project.

- d) In the **Configure Access** area, select **iSCSI**.
- e) Select **Create Project without LUNs and Shares** if you do not want to include LUNs and shares in the new project.  
The **App Config** page does not appear when you enable this option.
- f) Click **Next**.
4. In the **Hyper-V VDI** screen, complete the following steps:
- Select **Persistent** or **Non-Persistent** desktop type.
  - Type **Estimated total number of Desktops**.
  - Type **Average Size of a Desktop**.
  - Type **Prefix of the LUN**. Include # as part of the LUN name to provide for the count. For example, **HyperVVDI\_#\_LUN**. If you have selected 2 desktops, then they are named as **HyperVVDI\_1\_LUN** and **HyperVVDI\_2\_LUN**.
-  **Note:** The **Add Project** wizard creates one Share of 2000 GiB per 100 non-persistent desktops. The wizard creates one Share of 800 GiB per 40 persistent desktops. By default, the average virtual desktop size is 20 GiB.

5. In the **iSCSI Target Configuration** screen, complete the following steps:

If...	Then...
<b>You want to select the default target.</b>	<ol style="list-style-type: none"> <li>Click <b>Default Target</b>.</li> <li>Click <b>Next</b>.</li> </ol>
<b>You want to select an existing target.</b>	<p>Complete the following steps:</p> <ol style="list-style-type: none"> <li>Click <b>Choose Target</b>.</li> <li>Select the target from the <b>Choose Target</b> dropdown. The target group and status of the selected target appear.</li> <li>(Optional) Select <b>Authentication for Target</b> to authenticate CHAP. You can select <b>None</b>, <b>CHAP</b>, or <b>Mutual</b>.</li> </ol> <p> <b>Note:</b></p> <ul style="list-style-type: none"> <li>When you change <b>Authentication for Target</b> from <b>None</b> to <b>CHAP</b>, IntelliFlash displays the message: <b>Modifying the authentication mechanism affects the existing iSCSI sessions. Do you want to proceed?</b></li> </ul>

If...	Then...
	<p><b>you want to continue? [Yes   No]. Click Yes to continue.</b></p> <ul style="list-style-type: none"> <li>When you change <b>Authentication for Target</b> from <b>None</b> to <b>Mutual</b>, provide the CHAP username and password. The credentials are used by the initiator to authenticate the target.</li> </ul> <p>4. Click <b>Next</b>.</p>
<b>You want to create a new target.</b>	<p>Complete the following steps:</p> <ol style="list-style-type: none"> <li>Click <b>Create Target</b>.</li> <li>In the <b>Target Name</b> field, type a name. The wizard uses the provided target name to create a new target group and displays it in the <b>Target Group</b> field.</li> <li>To add the target to an existing target group, click the <b>select group</b> link and select the target group from the list. To select the default target group instead, select <b>default</b>.</li> <li>In the <b>Choose Network Bindings</b> section, select the required IP address.</li> <li>(Optional) Select <b>Authentication for Target</b> to authenticate CHAP. You can select <b>None</b>, <b>CHAP</b>, or <b>Mutual</b>.</li> </ol> <p> <b>Note:</b></p> <ul style="list-style-type: none"> <li>When you change <b>Authentication for Target</b> from <b>None</b> to <b>CHAP</b>, IntelliFlash displays the message: <b>Modifying the authentication mechanism affects the existing iSCSI sessions. Do you want to continue? [Yes   No]. Click Yes to continue.</b></li> <li>When you change <b>Authentication for Target</b> from <b>None</b> to <b>Mutual</b>, provide the CHAP username and password. The credentials are used by the initiator to authenticate the target.</li> </ul>

If...	Then...
	6. Click <b>Next</b> .

6. In the **iSCSI Initiator Group Configuration** screen, complete the following steps:

If...	Then...
<b>You want to provide access to the LUN without any restrictions.</b>	<p>Click <b>All</b> and then click <b>Next</b>.</p> <p> <b>Note:</b> When you select <b>All</b>, it enables existing initiators as well as new initiators to access the newly created LUN.</p>
<b>You want to use an existing initiator group.</b>	<p>Complete the following steps:</p> <ol style="list-style-type: none"> <li>1. Click <b>Choose Initiator Group</b>.</li> <li>2. Click the <b>Initiator Group</b> dropdown and select an initiator group from the list.</li> <li>3. Click <b>Next</b>.</li> </ol>
<b>You want to create a new initiator group.</b>	<p>Complete the following steps:</p> <ol style="list-style-type: none"> <li>1. Click <b>Create Initiator Group</b>.</li> <li>2. In the <b>Initiator Group</b> field, type a name for the group.</li> <li>3. In the <b>Initiator</b> field, type an initiator name. A valid initiator name must start with <i>iqn.yyyy-mm.[reverse-domain-name]</i> or must be an EUI-64 identifier.</li> <li>4. Click <b>Add Initiator</b>.</li> <li>5. Repeat steps (c) and (d) to add additional initiators to the group.</li> <li>6. To provide CHAP authentication, select <b>CHAP Credentials</b> and provide the CHAP username and password. The credentials are used by the initiator to authenticate the target.</li> <li>7. Click <b>Next</b>.</li> </ol>

7. (Optional) In the **Snapshot Schedules** screen, the wizard selects the recommended snapshot policy depending on the project's purpose.
- If you want to retain the recommended preset profile, click **Next**.

- If you want to customize the profile, select a profile from the **Schedule** list and customize it according to your requirements. You can add more conditions by clicking the **Add** (+) icon.

For more information, see [Preset Profiles for Snapshots](#) and [Custom Snapshot Schedules](#).

8. In the **Summary** screen, review the summary and click **Create**.

You can click the **More** link in the **Summary** page to see complete summary details.

## Creating an iSCSI Project for Exchange Server

For more information on Exchange Server project template, see [Exchange Server Template](#).

To create an iSCSI project for Exchange Server, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab on the left pane, click **New**.  
The **New Project** wizard appears.
3. In the **Name and Space configuration for Project** screen, complete the following steps:
  - a) In the **Project Name** field, type a name for the project.
  - b) In the **Pool** field, select the pool.
  - c) In the **Purpose** field, select **Exchange Server** as the purpose of the project.
  - d) In the **Configure Access** area, select **iSCSI**.
  - e) Select **Create Project without LUNs and Shares** if you do not want to include LUNs and shares in the new project.  
The **App Config** page does not appear when you enable this option.
  - f) Click **Next**.
4. In the **Exchange Server** screen, complete the following steps:
  - a) Type **Number of Exchange Servers**.  
A DB LUN and a Log LUN are created for each server.
  - b) (Optional) To create a passive LUN for database availability group, select **Enable Exchange DAG**. When you select the **Enable Exchange DAG** option, IntelliFlash creates a passive DB LUN for each Exchange Server.
  - c) In the **Size of each Database LUN** field, type the size required for the database LUN.  
To calculate the exact size required, click the **Calculate Exchange DB Size** link and type the following details:
    - The average number of messages per day
    - The average size of the message
    - The retention period
    - The number of email accounts

Click **Calculate & Update** link for the system to automatically calculate and populate the **Size of each Database LUN** field.

The maximum size for Exchange Server is 1 TiB. If you require bigger size, create a Generic project.

d) Click **Next**.

5. In the **iSCSI Target Configuration** screen, complete the following steps:

If...	Then...
<b>You want to select the default target.</b>	<ol style="list-style-type: none"> <li>1. Click <b>Default Target</b>.</li> <li>2. Click <b>Next</b>.</li> </ol>
<b>You want to select an existing target.</b>	<p>Complete the following steps:</p> <ol style="list-style-type: none"> <li>1. Click <b>Choose Target</b>.</li> <li>2. Select the target from the <b>Choose Target</b> dropdown.</li> </ol> <p>The target group and status of the selected target appear.</p> <ol style="list-style-type: none"> <li>3. (Optional) Select <b>Authentication for Target</b> to authenticate CHAP. You can select <b>None</b>, <b>CHAP</b>, or <b>Mutual</b>.</li> </ol> <div style="background-color: #f0f0f0; padding: 10px; margin-top: 10px;">  <b>Note:</b> <ul style="list-style-type: none"> <li>• When you change <b>Authentication for Target</b> from <b>None</b> to <b>CHAP</b>, IntelliFlash displays the message: <b>Modifying the authentication mechanism affects the existing iSCSI sessions. Do you want to continue? [Yes   No]</b>. Click <b>Yes</b> to continue.</li> <li>• When you change <b>Authentication for Target</b> from <b>None</b> to <b>Mutual</b>, provide the CHAP username and password. The credentials are used by the initiator to authenticate the target.</li> </ul> </div> <ol style="list-style-type: none"> <li>4. Click <b>Next</b>.</li> </ol>
<b>You want to create a new target.</b>	<p>Complete the following steps:</p> <ol style="list-style-type: none"> <li>1. Click <b>Create Target</b>.</li> <li>2. In the <b>Target Name</b> field, type a name.</li> </ol>

If...	Then...
	<p>The wizard uses the provided target name to create a new target group and displays it in the <b>Target Group</b> field.</p> <ol style="list-style-type: none"> <li>3. To add the target to an existing target group, click the <b>select group</b> link and select the target group from the list. To select the default target group instead, select <b>default</b>.</li> <li>4. In the <b>Choose Network Bindings</b> section, select the required IP address.</li> <li>5. (Optional) Select <b>Authentication for Target</b> to authenticate CHAP. You can select <b>None</b>, <b>CHAP</b>, or <b>Mutual</b>.</li> </ol> <div style="background-color: #f0f0f0; padding: 10px; margin-top: 10px;"> <p> <b>Note:</b></p> <ul style="list-style-type: none"> <li>• When you change <b>Authentication for Target</b> from <b>None</b> to <b>CHAP</b>, IntelliFlash displays the message: <b>Modifying the authentication mechanism affects the existing iSCSI sessions. Do you want to continue? [Yes   No]</b>. Click <b>Yes</b> to continue.</li> <li>• When you change <b>Authentication for Target</b> from <b>None</b> to <b>Mutual</b>, provide the CHAP username and password. The credentials are used by the initiator to authenticate the target.</li> </ul> </div> <ol style="list-style-type: none"> <li>6. Click <b>Next</b>.</li> </ol>

6. In the **iSCSI Initiator Group Configuration** screen, complete the following steps:

If...	Then...
<b>You want to provide access to the LUN without any restrictions.</b>	<p>Click <b>All</b> and then click <b>Next</b>.</p> <div style="background-color: #f0f0f0; padding: 10px;"> <p> <b>Note:</b></p> <p>When you select <b>All</b>, it enables existing initiators as well as new initiators to access the newly created LUN.</p> </div>
<b>You want to use an existing initiator group.</b>	<p>Complete the following steps:</p> <ol style="list-style-type: none"> <li>1. Click <b>Choose Initiator Group</b>.</li> </ol>

If...	Then...
	<p>2. Click the <b>Initiator Group</b> dropdown and select an initiator group from the list.</p> <p>3. Click <b>Next</b>.</p>
<b>You want to create a new initiator group.</b>	<p>Complete the following steps:</p> <ol style="list-style-type: none"> <li>1. Click <b>Create Initiator Group</b>.</li> <li>2. In the <b>Initiator Group</b> field, type a name for the group.</li> <li>3. In the <b>Initiator</b> field, type an initiator name. A valid initiator name must start with <i>iqn.yyyy-mm.[reverse-domain-name]</i> or must be an EUI-64 identifier.</li> <li>4. Click <b>Add Initiator</b>.</li> <li>5. Repeat steps (c) and (d) to add additional initiators to the group.</li> <li>6. To provide CHAP authentication, select <b>CHAP Credentials</b> and provide the CHAP username and password. The credentials are used by the initiator to authenticate the target.</li> <li>7. Click <b>Next</b>.</li> </ol>

7. (Optional) In the **Snapshot Schedules** screen, the wizard selects the recommended snapshot policy depending on the project's purpose.
  - If you want to retain the recommended preset profile, click **Next**.
  - If you want to customize the profile, select a profile from the **Schedule** list and customize it according to your requirements. You can add more conditions by clicking the **Add** (+) icon.

For more information, see [Preset Profiles for Snapshots](#) and [Custom Snapshot Schedules](#).

8. (Optional) In the **Snapshot Schedules** screen, the default snapshot policy of the project is automatically selected. You can retain the default preset profile or customize the profile.
  - If you want to retain the default preset profile, click **Next**.
  - If you want to customize the profile, click **Override project snapshot policy**. Select a profile from the **Schedule** list and customize it according to your requirements. You can add more conditions by clicking the **Add** (+) icon.

For more information, see [Preset Profiles for Snapshots](#), [Custom Snapshot Schedules](#), and [Overriding a Project Snapshot Schedule](#).

9. In the **Summary** screen, review the summary and click **Create**.

You can click the **More** link in the **Summary** page to see complete summary details.

## Creating an iSCSI Project for Generic Purpose

For more information about the Generic project template, see [Generic Template](#).

To create an iSCSI project for generic purpose, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab on the left pane, click **New**.  
The **New Project** wizard appears.
3. In the **Name and Space configuration for Project** screen, complete the following steps:
  - a) In the **Project Name** field, type a name for the project.
  - b) In the **Pool** field, select the pool.
  - c) In the **Purpose** field, select **Generic** as the purpose of the project.
  - d) In the **Configure Access** area, select **iSCSI**.
  - e) Set **Project Quota** and **Project Reservation**.
  - f) Click **Next**.
4. In the **iSCSI Target Configuration** screen, complete the following steps:

If...	Then...
<b>You want to select the default target.</b>	<ol style="list-style-type: none"> <li>1. Click <b>Default Target</b>.</li> <li>2. Click <b>Next</b>.</li> </ol>
<b>You want to select an existing target.</b>	<p>Complete the following steps:</p> <ol style="list-style-type: none"> <li>1. Click <b>Choose Target</b>.</li> <li>2. Select the target from the <b>Choose Target</b> dropdown. The target group and status of the selected target appear.</li> <li>3. (Optional) Select <b>Authentication for Target</b> to authenticate CHAP. You can select <b>None</b>, <b>CHAP</b>, or <b>Mutual</b>.</li> </ol> <div style="background-color: #f0f0f0; padding: 10px; margin-top: 10px;"> <p> <b>Note:</b></p> <ul style="list-style-type: none"> <li>• When you change <b>Authentication for Target</b> from <b>None</b> to <b>CHAP</b>, IntelliFlash displays the message: <b>Modifying the authentication mechanism affects the existing iSCSI sessions. Do you want to proceed?</b></li> </ul> </div>

If...	Then...
	<p><b>you want to continue? [Yes   No]. Click Yes to continue.</b></p> <ul style="list-style-type: none"> <li>When you change <b>Authentication for Target</b> from <b>None</b> to <b>Mutual</b>, provide the CHAP username and password. The credentials are used by the initiator to authenticate the target.</li> </ul> <p>4. Click <b>Next</b>.</p>
<b>You want to create a new target.</b>	<p>Complete the following steps:</p> <ol style="list-style-type: none"> <li>Click <b>Create Target</b>.</li> <li>In the <b>Target Name</b> field, type a name. The wizard uses the provided target name to create a new target group and displays it in the <b>Target Group</b> field.</li> <li>To add the target to an existing target group, click the <b>select group</b> link and select the target group from the list. To select the default target group instead, select <b>default</b>.</li> <li>In the <b>Choose Network Bindings</b> section, select the required IP address.</li> <li>(Optional) Select <b>Authentication for Target</b> to authenticate CHAP. You can select <b>None</b>, <b>CHAP</b>, or <b>Mutual</b>.</li> </ol> <p> <b>Note:</b></p> <ul style="list-style-type: none"> <li>When you change <b>Authentication for Target</b> from <b>None</b> to <b>CHAP</b>, IntelliFlash displays the message: <b>Modifying the authentication mechanism affects the existing iSCSI sessions. Do you want to continue? [Yes   No]. Click Yes to continue.</b></li> <li>When you change <b>Authentication for Target</b> from <b>None</b> to <b>Mutual</b>, provide the CHAP username and password. The credentials are used by the initiator to authenticate the target.</li> </ul>

If...	Then...
	6. Click <b>Next</b> .

5. In the **iSCSI Initiator Group Configuration** screen, complete the following steps:

If...	Then...
<b>You want to provide access to the LUN without any restrictions.</b>	<p>Click <b>All</b> and then click <b>Next</b>.</p> <p> <b>Note:</b> When you select <b>All</b>, it enables existing initiators as well as new initiators to access the newly created LUN.</p>
<b>You want to use an existing initiator group.</b>	<p>Complete the following steps:</p> <ol style="list-style-type: none"> <li>1. Click <b>Choose Initiator Group</b>.</li> <li>2. Click the <b>Initiator Group</b> dropdown and select an initiator group from the list.</li> <li>3. Click <b>Next</b>.</li> </ol>
<b>You want to create a new initiator group.</b>	<p>Complete the following steps:</p> <ol style="list-style-type: none"> <li>1. Click <b>Create Initiator Group</b>.</li> <li>2. In the <b>Initiator Group</b> field, type a name for the group.</li> <li>3. In the <b>Initiator</b> field, type an initiator name. A valid initiator name must start with <i>iqn.yyyy-mm.[reverse-domain-name]</i> or must be an EUI-64 identifier.</li> <li>4. Click <b>Add Initiator</b>.</li> <li>5. Repeat steps (c) and (d) to add additional initiators to the group.</li> <li>6. To provide CHAP authentication, select <b>CHAP Credentials</b> and provide the CHAP username and password. The credentials are used by the initiator to authenticate the target.</li> <li>7. Click <b>Next</b>.</li> </ol>

6. In the **Data Configuration** screen, complete the following steps:

- a) Click the **Deduplication** button to enable deduplication.
- b) Select the compression type from the **Compression** list.

The compression types are as follows:

- **Optimal Performance:** This is the default compression type. The compression algorithm for Optimal Performance is lz4.  
lz4 is the fastest lossless compression method. It is recommended that you use lz4 for speed, compression and balance.
  - **High Compression:** The compression algorithm for High Compression is igzip. igzip is slower than lz4, but provides better compression. When compared to the standard gzip, igzip is significantly faster, but results in a bit less compression.
  - **OFF:** Select this option to disable compression.
- c) Click **Next**.
7. (Optional) In the **Snapshot Schedules** screen, the wizard selects the recommended snapshot policy depending on the project's purpose.
- If you want to retain the recommended preset profile, click **Next**.
  - If you want to customize the profile, select a profile from the **Schedule** list and customize it according to your requirements. You can add more conditions by clicking the **Add** (+) icon.
- For more information, see [Preset Profiles for Snapshots](#) and [Custom Snapshot Schedules](#).
8. (Optional) In the **Snapshot Schedules** screen, the default snapshot policy of the project is automatically selected. You can retain the default preset profile or customize the profile.
- If you want to retain the default preset profile, click **Next**.
  - If you want to customize the profile, click **Override project snapshot policy**. Select a profile from the **Schedule** list and customize it according to your requirements. You can add more conditions by clicking the **Add** (+) icon.
- For more information, see [Preset Profiles for Snapshots](#), [Custom Snapshot Schedules](#), and [Overriding a Project Snapshot Schedule](#).
9. In the **Summary** screen, review the summary and click **Create**.  
You can click the **More** link in the **Summary** page to see complete summary details.

## Creating an FC Project for SQL Server

For more information about the SQL Server OLTP Application project template, see [SQL Server Template](#). For more information on project templates, see [Project Templates](#).

To create an FC project for SQL Server, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab on the left pane, click **New**.  
The **New Project** wizard appears.
3. In the **Name and Space configuration for Project** screen, complete the following steps:
  - a) In the **Project Name** field, type a name for the project.
  - b) In the **Pool** field, select the pool.

- c) In the **Purpose** field, select **SQL Server** as the purpose of the project.
- d) In the **Configure Access** area, select **FC**.



**Note:** You must have installed an FC card on your array. Otherwise, you do not see the **FC** option in the page.

- e) Select the **NPIV** option if you want the LUNs in the project to have ActiveOnly representation.

The **NPIV** option appears only when LUNs in existing projects are not yet migrated to ActiveOnly LUN representation after upgrading to 3.7.x.x or later. For a fresh installation, or when all existing projects are migrated to ActiveOnly LUN representation, the LUNs created in new projects are by default in ActiveOnly representation. See [Migrating Non-NPIV Projects to NPIV after Upgrade](#).

- f) Select **Create Project without LUNs and Shares** if you do not want to include LUNs and shares in the new project.

The **App Config** page does not appear when you enable this option.

- g) Click **Next**.

#### 4. In the **SQL Server** screen, complete the following steps:

- a) In the **SQL Server** section, type a name for the **DataLUN** (or use the default name). Select or type the size, the unit of memory (MiB, GiB, or TiB), and the count for the LUN.



**Note:** The default size of a database LUN is 10 GiB and the count is one. The LUN count is added as a suffix to the LUN name.

- b) In the **Additional LUNs** section, type names for the **LogLUN**, **SqlBackupLUN**, **TempDBDataLUN**, **TempDBLogLUN**, and **LargeObjLUN**. Select size and count for the additional LUNs.



**Note:**

- The size of additional LUNs is 10% of the database LUN. The wizard automatically calculates the additional LUNs size based on the DB LUN size. However, you can modify the size.
- The wizard does not create large object LUN type automatically. If you need it, you must select the required count.
- The default count for **LargeObjLUN** is **0** and hence the field is disabled. Increase the count to modify the **LargeObjLUN** size.

- c) Click **Next**.

#### 5. In the **Select FC Target Group** screen, select from the default FC target groups and click **Next**.



**Note:** For a fresh IntelliFlash installation or when you have migrated all the projects to ActiveOnly LUNs after upgrading, you can no longer create FC target groups. You can only select from the default virtual target groups.

#### 6. In the **Select or Create FC Initiator Group** screen, complete the following steps:

If...	Then...
<b>You want to select an existing initiator</b>	Complete the following steps: 1. Click <b>Choose Initiator group</b> . 2. Click <b>Initiator Group</b> and select an initiator group from the list. 3. Click <b>Next</b> .
<b>You want to create a new initiator group</b>	Complete the following steps: 1. Click <b>Create Initiator group</b> . 2. In the <b>Initiator Group</b> field, type a name. 3. From the <b>Ungrouped Initiators</b> list, select the required initiators. 4. Click <b>Next</b> .

7. (Optional) In the **Snapshot Schedules** screen, the wizard selects the recommended snapshot policy depending on the project's purpose.
  - If you want to retain the recommended preset profile, click **Next**.
  - If you want to customize the profile, select a profile from the **Schedule** list and customize it according to your requirements. You can add more conditions by clicking the **Add** (⊕) icon.

For more information, see [Preset Profiles for Snapshots](#) and [Custom Snapshot Schedules](#).

8. In the **Summary** screen, review the summary and click **Create**.

You can click the **More** link in the **Summary** page to see complete summary details.

## Creating an FC Project for Virtual Server Application

For more information about the Virtual Server project template, see [Virtual Server Template](#).

To create an FC project for SQL Server, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab on the left pane, click **New**.  
The **New Project** wizard appears.
3. In the **Name and Space configuration for Project** screen, complete the following steps:
  - a) In the **Project Name** field, type a name for the project.
  - b) In the **Pool** field, select the pool.
  - c) In the **Purpose** field, select **Virtual Server** as the purpose of the project.
  - d) In the **Configure Access** area, select **FC**.



**Note:** You must have installed an FC card on your array. Otherwise, you do not see the **FC** option in the page.

- e) Select the **NPIV** option if you want the LUNs in the project to have ActiveOnly representation.

The **NPIV** option appears only when LUNs in existing projects are not yet migrated to ActiveOnly LUN representation after upgrading to 3.7.x.x or later. For a fresh installation, or when all existing projects are migrated to ActiveOnly LUN representation, the LUNs created in new projects are by default in ActiveOnly representation. See [Migrating Non-NPIV Projects to NPIV after Upgrade](#).

- f) Select **Create Project without LUNs and Shares** if you do not want to include LUNs and shares in the new project.

The **App Config** page does not appear when you enable this option.

- g) Click **Next**.

4. In the **Virtual Server** screen, complete the following steps:

- a) In the **SQL Server** section, type a name for the **DataLUN** (or use the default name). Select or type the size, the unit of memory (MiB, GiB, or TiB), and the count for the LUN.



**Note:** The default size of a database LUN is 10 GiB and the count is one. The LUN count is added as a suffix to the LUN name.

- b) Click **Next**.

5. In the **Select FC Target Group** screen, select from the default FC target groups and click **Next**.



**Note:** For a fresh IntelliFlash installation or when you have migrated all the projects to ActiveOnly LUNs after upgrading, you can no longer create FC target groups. You can only select from the default virtual target groups.

6. In the **Select or Create FC Initiator Group** screen, complete the following steps:

If...	Then...
<b>You want to select an existing initiator</b>	<p>Complete the following steps:</p> <ol style="list-style-type: none"> <li>1. Click <b>Choose Initiator group</b>.</li> <li>2. Click <b>Initiator Group</b> and select an initiator group from the list.</li> <li>3. Click <b>Next</b>.</li> </ol>
<b>You want to create a new initiator group</b>	<p>Complete the following steps:</p> <ol style="list-style-type: none"> <li>1. Click <b>Create Initiator group</b>.</li> <li>2. In the <b>Initiator Group</b> field, type a name.</li> </ol>

If...	Then...
	<p>3. From the <b>Ungrouped Initiators</b> list, select the required initiators.</p> <p>4. Click <b>Next</b>.</p>

7. (Optional) In the **Snapshot Schedules** screen, the wizard selects the recommended snapshot policy depending on the project's purpose.
  - If you want to retain the recommended preset profile, click **Next**.
  - If you want to customize the profile, select a profile from the **Schedule** list and customize it according to your requirements. You can add more conditions by clicking the **Add** (+) icon.

For more information, see [Preset Profiles for Snapshots](#) and [Custom Snapshot Schedules](#).

8. In the **Summary** screen, review the summary and click **Create**.

You can click the **More** link in the **Summary** page to see complete summary details.

## Creating an FC Project for VMware VDI

For more information about the VMware VDI project template, see [VMware VDI Template](#).

To create an FC project for VMware VDI, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab on the left pane, click **New**.  
The **New Project** wizard appears.
3. In the **Name and Space configuration for Project** screen, complete the following steps:
  - a) In the **Project Name** field, type a name for the project.
  - b) In the **Pool** field, select the pool.
  - c) In the **Purpose** field, select **VMware VDI** as the purpose of the project.
  - d) In the **Configure Access** area, select **FC**.

 **Note:** You must have installed an FC card on your array. Otherwise, you do not see the **FC** option in the page.

- e) Select the **NPIV** option if you want the LUNs in the project to have ActiveOnly representation.

The **NPIV** option appears only when LUNs in existing projects are not yet migrated to ActiveOnly LUN representation after upgrading to 3.7.x.x or later. For a fresh installation, or when all existing projects are migrated to ActiveOnly LUN representation, the LUNs created in new projects are by default in ActiveOnly representation. See [Migrating Non-NPIV Projects to NPIV after Upgrade](#).

- f) Select **Create Project without LUNs and Shares** if you do not want to include LUNs and shares in the new project.

The **App Config** page does not appear when you enable this option.

- g) Click **Next**.

4. In the **VMware VDI** screen, complete the following steps:
  - a) Select **Persistent** or **Non-Persistent** desktop type.
  - b) Type **Estimated total number of Desktops**.
  - c) Type **Average Size of a Desktop**.
  - d) Type **Prefix of the LUN**.



**Note:** The Add Project wizard creates one Share of 2000 GiB per 100 non-persistent desktops. The wizard creates one Share of 800 GiB per 40 persistent desktops. By default, the average virtual desktop size is 20 GiB.

5. In the **Select FC Target Group** screen, select from the default FC target groups and click **Next**.



**Note:** For a fresh IntelliFlash installation or when you have migrated all the projects to ActiveOnly LUNs after upgrading, you can no longer create FC target groups. You can only select from the default virtual target groups.

6. In the **Select or Create FC Initiator Group** screen, complete the following steps:

If...	Then...
<b>You want to select an existing initiator</b>	Complete the following steps: <ol style="list-style-type: none"> <li>1. Click <b>Choose Initiator group</b>.</li> <li>2. Click <b>Initiator Group</b> and select an initiator group from the list.</li> <li>3. Click <b>Next</b>.</li> </ol>
<b>You want to create a new initiator group</b>	Complete the following steps: <ol style="list-style-type: none"> <li>1. Click <b>Create Initiator group</b>.</li> <li>2. In the <b>Initiator Group</b> field, type a name.</li> <li>3. From the <b>Ungrouped Initiators</b> list, select the required initiators.</li> <li>4. Click <b>Next</b>.</li> </ol>

7. (Optional) In the **Snapshot Schedules** screen, the wizard selects the recommended snapshot policy depending on the project's purpose.

- If you want to retain the recommended preset profile, click **Next**.

- If you want to customize the profile, select a profile from the **Schedule** list and customize it according to your requirements. You can add more conditions by clicking the **Add** (+) icon.

For more information, see [Preset Profiles for Snapshots](#) and [Custom Snapshot Schedules](#).

8. In the **Summary** screen, review the summary and click **Create**.

You can click the **More** link in the **Summary** page to see complete summary details.

## Creating an FC Project for Hyper-V VDI

For more information about the Hyper-V VDI project template, see [Hyper-V VDI Template](#).

To create an FC project for Hyper-V VDI, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab on the left pane, click **New**.  
The **New Project** wizard appears.
3. In the **Name and Space configuration for Project** screen, complete the following steps:
  - a) In the **Project Name** field, type a name for the project.
  - b) In the **Pool** field, select the pool.
  - c) In the **Purpose** field, select **Hyper-V VDI** as the purpose of the project.
  - d) In the **Configure Access** area, select **FC**.



**Note:** You must have installed an FC card on your array. Otherwise, you do not see the **FC** option in the page.

- e) Select the **NPIV** option if you want the LUNs in the project to have **ActiveOnly** representation.

The **NPIV** option appears only when LUNs in existing projects are not yet migrated to **ActiveOnly** LUN representation after upgrading to 3.7.x.x or later. For a fresh installation, or when all existing projects are migrated to **ActiveOnly** LUN representation, the LUNs created in new projects are by default in **ActiveOnly** representation. See [Migrating Non-NPIV Projects to NPIV after Upgrade](#).

- f) Select **Create Project without LUNs and Shares** if you do not want to include LUNs and shares in the new project.  
The **App Config** page does not appear when you enable this option.
  - g) Click **Next**.
4. In the **Hyper-V VDI** screen, complete the following steps:
    - a) Select **Persistent** or **Non-Persistent** desktop type.
    - b) Type **Estimated total number of Desktops**.
    - c) Type **Average Size of a Desktop**.

- d) Type **Prefix of the LUN**. Include # as part of the LUN name to provide for the count. For example, **HyperVVDI\_#\_LUN**. If you have selected 2 desktops, then they are named as **HyperVVDI\_1\_LUN** and **HyperVVDI\_2\_LUN**.



**Note:** The **Add Project** wizard creates one Share of 2000 GiB per 100 non-persistent desktops. The wizard creates one Share of 800 GiB per 40 persistent desktops. By default, the average virtual desktop size is 20 GiB.

5. In the **Select FC Target Group** screen, select from the default FC target groups and click **Next**.



**Note:** For a fresh IntelliFlash installation or when you have migrated all the projects to ActiveOnly LUNs after upgrading, you can no longer create FC target groups. You can only select from the default virtual target groups.

6. In the **Select or Create FC Initiator Group** screen, complete the following steps:

If...	Then...
<b>You want to select an existing initiator</b>	<p>Complete the following steps:</p> <ol style="list-style-type: none"> <li>Click <b>Choose Initiator group</b>.</li> <li>Click <b>Initiator Group</b> and select an initiator group from the list.</li> <li>Click <b>Next</b>.</li> </ol>
<b>You want to create a new initiator group</b>	<p>Complete the following steps:</p> <ol style="list-style-type: none"> <li>Click <b>Create Initiator group</b>.</li> <li>In the <b>Initiator Group</b> field, type a name.</li> <li>From the <b>Ungrouped Initiators</b> list, select the required initiators.</li> <li>Click <b>Next</b>.</li> </ol>

7. (Optional) In the **Snapshot Schedules** screen, the wizard selects the recommended snapshot policy depending on the project's purpose.

- If you want to retain the recommended preset profile, click **Next**.
- If you want to customize the profile, select a profile from the **Schedule** list and customize it according to your requirements. You can add more conditions by clicking the **Add** (⊕) icon.

For more information, see [Preset Profiles for Snapshots](#) and [Custom Snapshot Schedules](#).

8. In the **Summary** screen, review the summary and click **Create**.

You can click the **More** link in the **Summary** page to see complete summary details.

## Creating an FC Project for Exchange Server

For more information on Exchange Server, see [Exchange Server Template](#).

To create an FC project for Exchange Server, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab on the left pane, click **New**.  
The **New Project** wizard appears.
3. In the **Name and Space configuration for Project** screen, complete the following steps:
  - a) In the **Project Name** field, type a name for the project.
  - b) In the **Pool** field, select the pool.
  - c) In the **Purpose** field, select **Exchange Server** as the purpose of the project.
  - d) In the **Configure Access** area, select **FC**.



**Note:** You must have installed an FC card on your array. Otherwise, you do not see the **FC** option in the page.

- e) Select the **NPIV** option if you want the LUNs in the project to have ActiveOnly representation.  
The **NPIV** option appears only when LUNs in existing projects are not yet migrated to ActiveOnly LUN representation after upgrading to 3.7.x.x or later. For a fresh installation, or when all existing projects are migrated to ActiveOnly LUN representation, the LUNs created in new projects are by default in ActiveOnly representation. See [Migrating Non-NPIV Projects to NPIV after Upgrade](#).
- f) Select **Create Project without LUNs and Shares** if you do not want to include LUNs and shares in the new project.  
The **App Config** page does not appear when you enable this option.
- g) Click **Next**.

4. In the **Exchange Server** screen, complete the following steps:
  - a) Type **Number of Exchange Servers**.  
A DB LUN and a Log LUN are created for each server.
  - b) (Optional) To create a passive LUN for database availability group, select **Enable Exchange DAG**. When you select the **Enable Exchange DAG** option, IntelliFlash creates a passive DB LUN for each Exchange Server.
  - c) In the **Size of each Database LUN** field, type the size required for the database LUN.

To calculate the exact size required, click the **Calculate Exchange DB Size** link and type the following details:

- The average number of messages per day
- The average size of the message
- The retention period

- The number of email accounts

Click **Calculate & Update** link for the system to automatically calculate and populate the **Size of each Database LUN** field.

The maximum size for Exchange Server is 1 TiB. If you require bigger size, create a Generic project.

- d) Click **Next**.
5. In the **Select FC Target Group** screen, select from the default FC target groups and click **Next**.



**Note:** For a fresh IntelliFlash installation or when you have migrated all the projects to ActiveOnly LUNs after upgrading, you can no longer create FC target groups. You can only select from the default virtual target groups.

6. In the **Select or Create FC Initiator Group** screen, complete the following steps:

If...	Then...
<b>You want to select an existing initiator</b>	<p>Complete the following steps:</p> <ol style="list-style-type: none"> <li>1. Click <b>Choose Initiator group</b>.</li> <li>2. Click <b>Initiator Group</b> and select an initiator group from the list.</li> <li>3. Click <b>Next</b>.</li> </ol>
<b>You want to create a new initiator group</b>	<p>Complete the following steps:</p> <ol style="list-style-type: none"> <li>1. Click <b>Create Initiator group</b>.</li> <li>2. In the <b>Initiator Group</b> field, type a name.</li> <li>3. From the <b>Ungrouped Initiators</b> list, select the required initiators.</li> <li>4. Click <b>Next</b>.</li> </ol>

7. (Optional) In the **Snapshot Schedules** screen, the wizard selects the recommended snapshot policy depending on the project's purpose.
  - If you want to retain the recommended preset profile, click **Next**.
  - If you want to customize the profile, select a profile from the **Schedule** list and customize it according to your requirements. You can add more conditions by clicking the **Add** (+) icon.

For more information, see [Preset Profiles for Snapshots](#) and [Custom Snapshot Schedules](#).

8. In the **Summary** screen, review the summary and click **Create**.  
You can click the **More** link in the **Summary** page to see complete summary details.

## Creating an FC Project for Generic Purpose

For more information about the Generic project template, see [Generic Template](#).

To create an FC project for generic purpose, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab on the left pane, click **New**.  
The **New Project** wizard appears.
3. In the **Name and Space configuration for Project** screen, complete the following steps:
  - a) In the **Project Name** field, type a name for the project.
  - b) In the **Pool** field, select the pool.
  - c) In the **Purpose** field, select **Generic** as the purpose of the project.
  - d) In the **Configure Access** area, select **FC**.



**Note:** You must have installed an FC card on your array. Otherwise, you do not see the **FC** option in the page.

- e) Select the **NPIV** option if you want the LUNs in the project to have ActiveOnly representation.

The **NPIV** option appears only when LUNs in existing projects are not yet migrated to ActiveOnly LUN representation after upgrading to 3.7.x.x or later. For a fresh installation, or when all existing projects are migrated to ActiveOnly LUN representation, the LUNs created in new projects are by default in ActiveOnly representation. See [Migrating Non-NPIV Projects to NPIV after Upgrade](#).

- f) Set **Project Quota** and **Project Reservation**.
- g) Click **Next**.
4. In the **Select FC Target Group** screen, select from the default FC target groups and click **Next**.



**Note:** For a fresh IntelliFlash installation or when you have migrated all the projects to ActiveOnly LUNs after upgrading, you can no longer create FC target groups. You can only select from the default virtual target groups.

5. In the **Select or Create FC Initiator Group** screen, complete the following steps:

If...	Then...
<b>You want to select an existing initiator</b>	Complete the following steps: <ol style="list-style-type: none"> <li>1. Click <b>Choose Initiator group</b>.</li> <li>2. Click <b>Initiator Group</b> and select an initiator group from the list.</li> <li>3. Click <b>Next</b>.</li> </ol>

If...	Then...
<b>You want to create a new initiator group</b>	<p>Complete the following steps:</p> <ol style="list-style-type: none"> <li>1. Click <b>Create Initiator group</b>.</li> <li>2. In the <b>Initiator Group</b> field, type a name.</li> <li>3. From the <b>Ungrouped Initiators</b> list, select the required initiators.</li> <li>4. Click <b>Next</b>.</li> </ol>

6. In the **Data Configuration** screen, complete the following steps:
  - a) Click the **Deduplication** button to enable deduplication.
  - b) Select the compression type from the **Compression** list.  
The compression types are as follows:
    - **Optimal Performance:** This is the default compression type. The compression algorithm for Optimal Performance is lz4.  
lz4 is the fastest lossless compression method. It is recommended that you use lz4 for speed, compression and balance.
    - **High Compression:** The compression algorithm for High Compression is igzip. igzip is slower than lz4, but provides better compression. When compared to the standard gzip, igzip is significantly faster, but results in a bit less compression.
    - **OFF:** Select this option to disable compression.
  - c) Click **Next**.
7. (Optional) In the **Snapshot Schedules** screen, the wizard selects the recommended snapshot policy depending on the project's purpose.
  - If you want to retain the recommended preset profile, click **Next**.
  - If you want to customize the profile, select a profile from the **Schedule** list and customize it according to your requirements. You can add more conditions by clicking the **Add** (+) icon.

For more information, see [Preset Profiles for Snapshots](#) and [Custom Snapshot Schedules](#).

8. In the **Summary** screen, review the summary and click **Create**.  
You can click the **More** link in the **Summary** page to see complete summary details.

## Creating an NFS Project for Virtual Server Application

For more information about the Virtual Server project template, see [Virtual Server Template](#).

To create an NFS project for virtual server, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab on the left pane, click **New**.

The **New Project** wizard appears.

3. In the **Name and Space configuration for Project** screen, complete the following steps:
  - a) In the **Project Name** field, type a name for the project.
  - b) In the **Pool** field, select the pool.
  - c) In the **Purpose** field, select **Virtual Server** as the purpose of the project.
  - d) In the **Configure Access** area, select **NFS**.
  - e) Select **Create Project without LUNs and Shares** if you do not want to include LUNs and shares in the new project.  
The **App Config** page does not appear when you enable this option.
  - f) Click **Next**.
4. In the **Name and Space configuration for Share** screen, complete the following steps:
  - a) Type a name in the **Share Name** field.
  - b) Select **Mountpoint** and modify the mountpoint.
  - c) Type the **Count** for share.
  - d) Select and set the **Share Quota** and **Share Reservation**.
  - e) Click **Next**.
5. In the **Configure NFS Access** screen, complete the following steps:
  - a) By default, **NFS Sharing** is **on**.  
You can add a new network access control list (ACL) from the **Configure NFS Access** screen. The default ACL policy is *allow all*.
  - b) Click the **Access Mode** dropdown list and then select **Read-Only** or **Read-Write** to add a new network ACL.
  - c) Click the **Access Type** dropdown list and select **IP Address** (internet protocol) or **FQDN** (fully qualified domain name).  
Depending on the selection you made, the **IP Address** or **FQDN** field activates.
  - d) Type an IP address in the **IP** field or type a domain name in the **FQDN** field.



**Note:** For network IP addresses, you can provide the network part of an IP address or you can provide the complete IP address. For a **Class A** network IP address, you can provide the first octet of the address, for a **Class B** network IP address, you can provide the first two octets of the address, and for a **Class C** network IP address you can provide the first three octets of the address.

- e) To provide root access to the array, select **Root Access**.



**Note:** This option preserves the root UID without squashing.

- f) Click **Add**.

The added ACL appears in the **Current Network ACLs** section. If you want to delete an incorrect or unwanted IP address, click **Delete** to remove it and add the correct IP address.

- g) Click **Next**.
6. (Optional) In the **Snapshot Schedules** screen, the wizard selects the recommended snapshot policy depending on the project's purpose.
  - If you want to retain the recommended preset profile, click **Next**.
  - If you want to customize the profile, select a profile from the **Schedule** list and customize it according to your requirements. You can add more conditions by clicking the **Add** (+) icon.

For more information, see [Preset Profiles for Snapshots](#) and [Custom Snapshot Schedules](#).

7. (Optional) In the **Snapshot Schedules** screen, the default snapshot policy of the project is automatically selected. You can retain the default preset profile or customize the profile.
  - If you want to retain the default preset profile, click **Next**.
  - If you want to customize the profile, click **Override project snapshot policy**. Select a profile from the **Schedule** list and customize it according to your requirements. You can add more conditions by clicking the **Add** (+) icon.

For more information, see [Preset Profiles for Snapshots](#), [Custom Snapshot Schedules](#), and [Overriding a Project Snapshot Schedule](#).

8. In the **Summary** screen, review the summary and click **Create**.

You can click the **More** link in the **Summary** page to see complete summary details.

## Creating an NFS Project for VMware VDI

For more information about the VMware VDI project template, see [VMware VDI Template](#).

To create an NFS project for VMware VDI, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab on the left pane, click **New**.  
The **New Project** wizard appears.
3. In the **Name and Space configuration for Project** screen, complete the following steps:
  - a) In the **Project Name** field, type a name for the project.
  - b) In the **Pool** field, select the pool.
  - c) In the **Purpose** field, select **VMware VDI** as the purpose of the project.
  - d) In the **Configure Access** area, select **NFS**.
  - e) Select **Create Project without LUNs and Shares** if you do not want to include LUNs and shares in the new project.

The **App Config** page does not appear when you enable this option.

- f) Click **Next**.
4. In the **VMware VDI** screen, complete the following steps:
- Type **Estimated total number of Desktops**.
  - Type **Average Size of a Desktop**.
  - Type **Prefix of the Share**.
-  **Note:** The **Add Project** wizard creates one Share of 2000 GiB per 100 non-persistent desktops. The wizard creates one Share of 800 GiB per 40 persistent desktops. By default, the average virtual desktop size is 20 GiB.
5. In the **Configure NFS Access** screen, complete the following steps:
- By default, **NFS Sharing** is **on**. You can add a new network access control list (ACL) from the **Configure NFS Access** screen. The default ACL policy is *allow all*.
  - Click the **Access Mode** dropdown list and then select **Read-Only** or **Read-Write** to add a new network ACL.
  - Click the **Access Type** dropdown list and select **IP** (internet protocol) or **FQDN** (fully qualified domain name). Depending on the selection you made, the **IP** or **FQDN** field activates.
  - Type an IP address in the **IP** field or type a domain name in the **FQDN** field.
-  **Note:** For network IP addresses, you can provide the network part of an IP address or you can provide the complete IP address. For a **Class A** network IP address, you can provide the first octet of the address, for a **Class B** network IP address, you can provide the first two octets of the address, and for a **Class C** network IP address you can provide the first three octets of the address.
- To provide root access to the array, select **Root Access**.
-  **Note:** This option preserves the root UID without squashing.
- Click **Add**. The added ACL appears in the **Current Network ACLs** section. If you want to delete an incorrect or unwanted IP address, click **Delete** to remove it and add the correct IP address.
  - Click **Next**.
6. (Optional) In the **Snapshot Schedules** screen, the wizard selects the recommended snapshot policy depending on the project's purpose.
- If you want to retain the recommended preset profile, click **Next**.
  - If you want to customize the profile, select a profile from the **Schedule** list and customize it according to your requirements. You can add more conditions by clicking the **Add** (+) icon.

For more information, see [Preset Profiles for Snapshots](#) and [Custom Snapshot Schedules](#).

7. (Optional) In the **Snapshot Schedules** screen, the default snapshot policy of the project is automatically selected. You can retain the default preset profile or customize the profile.
  - If you want to retain the default preset profile, click **Next**.
  - If you want to customize the profile, click **Override project snapshot policy**. Select a profile from the **Schedule** list and customize it according to your requirements. You can add more conditions by clicking the **Add** (+) icon.

For more information, see [Preset Profiles for Snapshots](#), [Custom Snapshot Schedules](#), and [Overriding a Project Snapshot Schedule](#).

8. In the **Summary** screen, review the summary and click **Create**.

You can click the **More** link in the **Summary** page to see complete summary details.

## Creating an NFS Project for Generic Purpose

For more information about the Generic project template, see [Generic Template](#).

To create an NFS project for generic purpose, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab on the left pane, click **New**.  
The **New Project** wizard appears.
3. In the **Name and Space configuration for Project** screen, complete the following steps:
  - a) In the **Project Name** field, type a name for the project.
  - b) In the **Pool** field, select the pool.
  - c) In the **Purpose** field, select **Generic** as the purpose of the project.
  - d) In the **Configure Access** area, select **NFS**.
  - e) Set **Project Quota** and **Project Reservation**.
  - f) Click **Next**.
4. In the **Configure NFS Access** screen, complete the following steps:
  - a) By default, **NFS Sharing** is **on**.  
You can add a new network access control list (ACL) from the **Configure NFS Access** screen. The default ACL policy is *allow all*.
  - b) Click the **Access Mode** dropdown list and then select **Read-Only** or **Read-Write** to add a new network ACL.
  - c) Click the **Access Type** dropdown list and select **IP Address** (internet protocol) or **FQDN** (fully qualified domain name).  
Depending on the selection you made, the **IP Address** or **FQDN** field activates.
  - d) Type an IP address in the **IP Address** field or type a domain name in the **FQDN** field.



**Note:** For network IP addresses, you can provide the network part of an IP address or you can provide the complete IP address. For a **Class A** network IP address, you can provide the first octet of the address, for a **Class B** network IP address, you can provide the first two octets of the address, and for a **Class C** network IP address you can provide the first three octets of the address.

- e) To provide root access to the array, select **Root Access**.



**Note:** This option preserves the root UID without squashing.

- f) Click **Add**.

The added ACL appears in the **Current Network ACLs** section. If you want to delete an incorrect or unwanted IP address, click **Delete** to remove it and add the correct IP address.

- g) Click **Next**.

5. In the **Data Configuration** screen, complete the following steps:

- a) Click the **Deduplication** button to enable deduplication.
- b) Select the compression type from the **Compression** list.

The compression types are as follows:

- **Optimal Performance:** This is the default compression type. The compression algorithm for Optimal Performance is lz4.  
lz4 is the fastest lossless compression method. It is recommended that you use lz4 for speed, compression and balance.
- **High Compression:** The compression algorithm for High Compression is igzip. igzip is slower than lz4, but provides better compression. When compared to the standard gzip, igzip is significantly faster, but results in a bit less compression.
- **OFF:** Select this option to disable compression.

- c) Click **Next**.

6. (Optional) In the **Snapshot Schedules** screen, the wizard selects the recommended snapshot policy depending on the project's purpose.

- If you want to retain the recommended preset profile, click **Next**.
- If you want to customize the profile, select a profile from the **Schedule** list and customize it according to your requirements. You can add more conditions by clicking the **Add** (+) icon.

For more information, see [Preset Profiles for Snapshots](#) and [Custom Snapshot Schedules](#).

7. (Optional) In the **Snapshot Schedules** screen, the default snapshot policy of the project is automatically selected. You can retain the default preset profile or customize the profile.

- If you want to retain the default preset profile, click **Next**.
- If you want to customize the profile, click **Override project snapshot policy**. Select a profile from the **Schedule** list and customize it according to your requirements. You can add more conditions by clicking the **Add** (+) icon.

For more information, see [Preset Profiles for Snapshots](#), [Custom Snapshot Schedules](#), and [Overriding a Project Snapshot Schedule](#).

8. In the **Summary** screen, review the summary and click **Create**.

You can click the **More** link in the **Summary** page to see complete summary details.

## Creating an SMB Project for SQL Server

For more information about the SQL Server OLTP Application project template, see [SQL Server Template](#). For more information on project templates, see [Project Templates](#).

To create an SMB project for SQL Server, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab on the left pane, click **New**.  
The **New Project** wizard appears.
3. In the **Name and Space configuration for Project** screen, complete the following steps:
  - a) In the **Project Name** field, type a name for the project.
  - b) In the **Pool** field, select the pool.
  - c) In the **Purpose** field, select **SQL Server** as the purpose of the project.
  - d) In the **Configure Access** area, select **SMB**.
  - e) Select **Create Project without LUNs and Shares** if you do not want to include LUNs and shares in the new project.  
The **App Config** page does not appear when you enable this option.
  - f) Click **Next**.
4. In the **Name and Space configuration for Share** screen, complete the following steps:
  - a) In the **Share Name** field, type a name for the share.
  - b) Enable the **Mountpoint** field, and type the path of the share.
  - c) Set the count for the share.
  - d) Enable **Share Quota** and set the quota.
  - e) Enable **Share Reservation** and set the quota.
  - f) Click **Next**.
5. In the **Configure SMB Access** screen, complete the following steps:
  - a) By default, **SMB Sharing** is enabled.  
You can add a new network access control list (ACL) from the **Configure SMB Access** screen. The default ACL policy is *allow all*.
  - b) Click the **Access Mode** dropdown list and then select **Read-Only** or **Read-Write** to add a new network ACL.

- c) Click the **Access Type** dropdown list and select **IP** or **FQDN** (fully qualified domain name). Depending on the selection you made, the **IP Address** or the **FQDN** field activates.
- d) Type an IP address in the **IP Address** field or type a domain name in the **FQDN** field.



**Note:** For network IP addresses, you can provide the network part of an IP address or you can provide the complete IP address. For a **Class A** network IP address, you can provide the first octet of the address, for a **Class B** network IP address, you can provide the first two octets of the address, and for a **Class C** network IP address you can provide the first three octets of the address.

- e) Click **Add**.

The added ACL appears in the **Current Network ACLs** section. If you want to delete an IP address, select the IP address and click **Delete**.

- f) Click **Next**.

6. (Optional) In the **Snapshot Schedules** screen, the wizard selects the recommended snapshot policy depending on the project's purpose.

- If you want to retain the recommended preset profile, click **Next**.
- If you want to customize the profile, select a profile from the **Schedule** list and customize it according to your requirements. You can add more conditions by clicking the **Add** (+) icon.

For more information, see [Preset Profiles for Snapshots](#) and [Custom Snapshot Schedules](#).

7. In the **Summary** screen, review the summary and click **Create**.

You can click the **More** link in the **Summary** page to see complete summary details.

## Creating an SMB Project for Hyper-V VDI

### Prerequisites

SMB 3.0 protocol must be enabled in the **Services > NAS > SMB** page.

To create an SMB project for Hyper-V VDI, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab on the left pane, click **New**.  
The **New Project** wizard appears.
3. In the **Name and Space configuration for Project** screen, complete the following steps:
  - a) In the **Project Name** field, type a name for the project.
  - b) In the **Pool** field, select the pool.
  - c) In the **Purpose** field, select **Hyper-V VDI** as the purpose of the project.
  - d) In the **Configure Access** area, select **SMB**.

- The **SMB** option does not appear if you have not enabled the SMB 3.0 protocol in the **Services > NAS > SMB** page.
- e) Select **Create Project without LUNs and Shares** if you do not want to include LUNs and shares in the new project.  
The **App Config** page does not appear when you enable this option.
  - f) Click **Next**.
4. In the **Hyper-V VDI** screen, complete the following steps:
- a) Type **Estimated total number of Desktops**.
  - b) Type **Average Size of a Desktop**.
  - c) Type **Prefix of the LUN**. Include # as part of the LUN name to provide for the count. For example, **HyperVVVDI\_#\_LUN**. If you have selected 2 desktops, then they are named as **HyperVVVDI\_1\_LUN** and **HyperVVVDI\_2\_LUN**.
-  **Note:** The **Add Project** wizard creates one Share of 2000 GiB per 100 non-persistent desktops. The wizard creates one Share of 800 GiB per 40 persistent desktops. By default, the average virtual desktop size is 20 GiB.
5. In the **Configure SMB Access** screen, complete the following steps:
- a) By default, **SMB Sharing** is **on**.  
You can add a new network access control list (ACL) from the **Configure SMB Access** screen. The default ACL policy is *allow all*.
  - b) Click the **Access Mode** dropdown list and then select **Read-Only** or **Read-Write** to add a new network ACL.
  - c) Click the **Access Type** dropdown list and select **IP** (internet protocol) or **FQDN** (fully qualified domain name).  
Depending on the selection you made, the **IP** or **FQDN** field activates.
  - d) Type an IP address in the **IP** field or type a domain name in the **FQDN** field.
-  **Note:** For network IP addresses, you can provide the network part of an IP address or you can provide the complete IP address. For a **Class A** network IP address, you can provide the first octet of the address, for a **Class B** network IP address, you can provide the first two octets of the address, and for a **Class C** network IP address you can provide the first three octets of the address.
- e) Click **Add**.  
The added ACL appears in the **Current Network ACLs** section. If you want to delete an incorrect or unwanted IP address, click **Delete** to remove it and add the correct IP address.
  - f) Click **Next**.
6. (Optional) In the **Snapshot Schedules** screen, the wizard selects the recommended snapshot policy depending on the project's purpose.
- If you want to retain the recommended preset profile, click **Next**.

- If you want to customize the profile, select a profile from the **Schedule** list and customize it according to your requirements. You can add more conditions by clicking the **Add** (⊕) icon.

For more information, see [Preset Profiles for Snapshots](#) and [Custom Snapshot Schedules](#).

7. In the **Summary** screen, review the summary and click **Create**.

You can click the **More** link in the **Summary** page to see complete summary details.

## Related Topics

[Hyper-V VDI Template](#)

## Creating an SMB Project for Generic Purpose

For more information about the Generic project template, see [Generic Template](#).

To create an SMB project for generic purpose, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab on the left pane, click **New**.  
The **New Project** wizard appears.
3. In the **Name and Space configuration for Project** screen, complete the following steps:
  - a) In the **Project Name** field, type a name for the project.
  - b) In the **Pool** field, select the pool.
  - c) In the **Purpose** field, select **Generic** as the purpose of the project.
  - d) In the **Configure Access** area, select **SMB**.
  - e) Set **Project Quota** and **Project Reservation**.
  - f) Click **Next**.
4. In the **Configure SMB Access** screen, complete the following steps:
  - a) By default, **SMB Sharing is on**.  
You can add a new network access control list (ACL) from the **Configure SMB Access** screen. The default ACL policy is *allow all*.
  - b) Click the **Access Mode** dropdown list and then select **Read-Only** or **Read-Write** to add a new network ACL.
  - c) Click the **Access Type** dropdown list and select **IP** or **FQDN** (fully qualified domain name).  
Depending on the selection you made, the **IP Address** or the **FQDN** field activates.
  - d) Type an IP address in the **IP Address** field or type a domain name in the **FQDN** field.



**Note:** For network IP addresses, you can provide the network part of an IP address or you can provide the complete IP address. For a **Class A** network IP address, you can provide the first octet of the address, for a **Class B** network IP

address, you can provide the first two octets of the address, and for a **Class C** network IP address you can provide the first three octets of the address.

- e) Click **Add**.  
The added ACL appears in the **Current Network ACLs** section. If you want to delete an incorrect or unwanted IP address, click **Delete** to remove it and add the correct IP address.
  - f) Click **Next**.
5. In the **Data Configuration** screen, complete the following steps:
- a) Click the **Deduplication** button to enable deduplication.
  - b) Select the compression type from the **Compression** list.  
The compression types are as follows:
    - **Optimal Performance**: This is the default compression type. The compression algorithm for Optimal Performance is lz4.  
lz4 is the fastest lossless compression method. It is recommended that you use lz4 for speed, compression and balance.
    - **High Compression**: The compression algorithm for High Compression is igzip. igzip is slower than lz4, but provides better compression. When compared to the standard gzip, igzip is significantly faster, but results in a bit less compression.
    - **OFF**: Select this option to disable compression.
  - c) Click **Next**.
6. (Optional) In the **Snapshot Schedules** screen, the wizard selects the recommended snapshot policy depending on the project's purpose.
- If you want to retain the recommended preset profile, click **Next**.
  - If you want to customize the profile, select a profile from the **Schedule** list and customize it according to your requirements. You can add more conditions by clicking the **Add** (+) icon.
- For more information, see [Preset Profiles for Snapshots](#) and [Custom Snapshot Schedules](#).
7. (Optional) In the **Snapshot Schedules** screen, the default snapshot policy of the project is automatically selected. You can retain the default preset profile or customize the profile.
- If you want to retain the default preset profile, click **Next**.
  - If you want to customize the profile, click **Override project snapshot policy**. Select a profile from the **Schedule** list and customize it according to your requirements. You can add more conditions by clicking the **Add** (+) icon.
- For more information, see [Preset Profiles for Snapshots](#), [Custom Snapshot Schedules](#), and [Overriding a Project Snapshot Schedule](#).
8. In the **Summary** screen, review the summary and click **Create**.  
You can click the **More** link in the **Summary** page to see complete summary details.

## Managing Projects

---

After creating projects, you can manage them according to your requirements. You need to edit various project configuration properties if you want to apply the modifications to all the contents of a project. If you want to modify properties for an individual share or LUN, modify the properties individually.

### Modifying Project Mountpoint

A project mountpoint is an access point (directory) for NFS and SMB shares (file systems). By default, IntelliFlash uses `/export/<project_name>` as the default mountpoint when creating a project. However, you can change mountpoint according to your requirements.

To modify a project's mountpoint, complete the following steps:

1. Click **Provision > Projects**.
  2. You must turn off SMB and NFS sharing before modifying a project mountpoint. To turn off SMB and NFS sharing, do the following:
    - a) In the **Local** tab, select the project from the **Projects** list and click **Manage > Access**. The **Project Access** page appears.
    - b) In the **NFS** and the **SMB** tabs, disable the **NFS Sharing** and **SMB Sharing** options.
  3. In the **Local** tab on the left pane, select the project from the **Projects** list and click **Manage > Settings**. The **Generic Project Settings** page appears.
  4. In the **General** tab, type a new mountpoint location in the **Mountpoint** field.
-  **Note:** When you change the project's mountpoint to a new mountpoint, you cannot revert it back to the original mountpoint.
5. Click **Save**.
  6. Turn on the **NFS Sharing** and **SMB Sharing** options in **Manage > Access > SMB and NFS** tabs after changing the mountpoint path.

### Viewing the Purpose of a Project

To view the purpose of a project, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab on the left pane, select the project from the **Projects** list and click **Manage > Settings**. The **Generic Project Settings** page appears.
3. In the **General** tab, look up the **Purpose** field.

## Modifying Compression Type in a Project

You can change the compression type depending on the data type that you want to store in shares and LUNs.

 **Note:** Compression is only applied on new and modified data. If you enable or disable compression after adding data to a project, compression is not applied to the existing data.

To modify data compression, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab on the left pane, select the project from the **Projects** list and click **Manage > Settings**.  
The **Generic Project Settings** page appears.
3. In the **Advanced** tab, in the **Override Settings** section, select the compression type from the **Compression** list.
  - The compression types are **High Compression** and **Optimal Performance**. **Optimal Performance** is the default compression type.
  - If you do not want compression enabled, select **OFF**.
  - When you select the compression type, the corresponding compression algorithm appears below the **Compression** text box. The compression algorithm for Optimal Performance is lz4. The compression algorithm for High Compression is igzip.
  - The older compression types are renamed as **Legacy** and will continue to be supported.
4. Click **Save**.

## Modifying Project Quota Size

After creating a project, you can increase or decrease the defined quota size of the project.

A quota is the maximum limit for the amount of storage space that a project can consume. Meaning, the set quota can be distributed among shares within a project. However, an individual share or all the shares together cannot exceed the quota set at the project level.

To modify project quota size, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab on the left pane, select the project from the **Projects** list and click **Manage > Settings**.  
The **Generic Project Settings** page appears.
3. In the **General** tab, complete the following steps:
  - a) Select **Project Quota**.  
If the **Project Quota** checkbox is not selected, no quota limits are applied.
  - b) In the text field, type or select the quota size.

- c) Select the required storage unit.
4. Click **Save**.

## Modifying Project Space Reservation

After creating a project, you can increase or decrease the defined space reservation for the project. The IntelliFlash OS enables you to exceed the space reservation for shares if any quota is not set at the project level. However, if the quota is defined for a project, then the space reservation must be less than the defined quota size at project level.

To modify space reservation of a project, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab on the left pane, select the project from the **Projects** list and click **Manage > Settings**.  
The **Generic Project Settings** page appears.
3. In the **General** tab, complete the following steps:
  - a) Select **Project Reservation**.  
If the **Project Reservation** checkbox is not selected, no space is reserved.
  - b) In the field, type or select the reservation size.
  - c) Select the required storage unit.
4. Click **Save**.

## Enabling or Disabling Project Deduplication Status

You can disable the deduplication status, if you are planning to store data that might not benefit from deduplication, such as videos and graphics.

You can enable the deduplication status, if you are planning to store data that has a lot of duplicate blocks. For example, virtual machines and virtual desktops. If you want to obtain the maximum benefit for deduplication, you must enable it before you add data to a project.

 **Note:** When enabling deduplication for shares or volumes that have a block size lesser than 32 KiB (for Hybrid arrays) and lesser than 8 KiB (for All-Flash arrays), a warning message appears that the recommended block size is higher than the assigned block size.

Deduplication is only applied on new and modified data. If you enable or disable deduplication after adding data to a project, deduplication is not applied to the existing data.

To change the deduplication status of a project, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab on the left pane, select the project from the **Projects** list and click **Manage > Settings**.  
The **Generic Project Settings** page appears.
3. In the **Advanced** tab, enable or disable the **Deduplication** option.
4. Click **Save**.

## Modifying Project Cache

When you enable **Read Cache**, the IntelliFlash OS caches the normal data in both the system RAM and SSD. When you disable **Read Cache**, the IntelliFlash OS does not cache the normal data.



**Note:** IntelliFlash OS always caches the metadata in the system RAM, even when the **Read Cache** is disabled.

To modify the cache for a project, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab on the left pane, select the project from the **Projects** list and click **Manage > Settings**.  
The **Generic Project Settings** page appears.
3. In the **Advanced** tab, enable or disable **Read Cache**.
4. Click **Save**.

## Enabling or Disabling Read Only Status

You can protect the data in a project from changes by enabling the **Read Only** property of the project. By default, the option is disabled. When the option is enabled, you cannot add or modify any data to the shares or LUNs of a project.

To change the **Read Only** property of a project, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab on the left pane, select the project from the **Projects** list and click **Manage > Settings**.  
The **Generic Project Settings** page appears.
3. In the **Advanced** tab, enable or disable the **Read Only** option.
4. Click **Save**.

## Setting LUN Creation Default Options

You can set LUN creation defaults—default LUN size and thin provisioning—when creating a project. When you create a LUN in a project, IntelliFlash, by default, uses the defined settings. If you do not set LUN creation defaults when creating a new project, IntelliFlash enables you to set them later or modify existing default settings from the **Generic Project Settings** window. You can modify the default LUN size and enable or disable thin provisioning on an already created project. After modifying, when you create a new LUN, IntelliFlash automatically creates a LUN according to the new settings.

To set LUN creation defaults, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab on the left pane, select the project from the **Projects** list and click **Manage > Settings**.  
The **Generic Project Settings** page appears.
3. In the **LUN** tab, complete the following steps:
  - a) In the **Default LUN Size** field, type or select LUN size and select the storage unit.
  - b) (Optional) Select the **Thin Provisioning** option.
4. Click **Save**.

## Modifying Space Usage Threshold Levels for a Project

The default space usage threshold is defined in the **Settings > Notifications > Threshold** page.

You can now override the default threshold levels and set custom threshold levels for a specific project.

To set custom threshold levels for a project, do the following:

1. Click **Provision > Projects**.
2. Select the project and click **Manage > Settings**.  
The **Generic Project Settings** page appears.
3. In the **General** tab, in the **Project Thresholds** section, click **Enable Project Threshold**.  
Enabling this button overrides the default threshold levels.
4. Select new values for **Warning threshold** and **Critical threshold**.
5. Click **Save**.

When the project exceeds the space usage thresholds, the Web UI now indicates that the project is running out of space. Warning or Critical icon appears next to the project. When you mouse over the Warning or Critical icon, the Web UI displays the free space remaining. If you have not defined a quota for the project, you do not see the warnings.

## iSCSI and FC Mappings

---

You can add iSCSI and FC mappings for a project. The mappings are applicable to the LUNs in the project. You can also edit and override project-level mappings and provide different mappings to a LUN, if required.

### Adding iSCSI Mapping for a Project

#### Prerequisites

Before adding mappings, you must add targets and initiators in the **Services > SAN** page and add target groups. For more information on adding iSCSI initiators, see [Adding an iSCSI Initiator](#).

To add iSCSI mappings for an iSCSI project, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab, select the project from the **Projects** list and click **Manage > Access**. The **Project Access** page appears.
3. In the **iSCSI** tab, click **Add**.
4. In the **Add Mapping** window, complete the following steps:
  - a) Select the initiator group from the **Initiator Group** list. Select **All** if you want to add all the available initiator groups.
  - b) Select **Read Only** if you want to make this a read only mapping.
  - c) Click **Add**.

### Adding FC Mapping for a Project

#### Prerequisites

Before adding mappings, you must add targets and initiators in the **SAN Services** page and add target groups and initiator groups. For more information on adding FC initiators, see [Adding an FC Initiator](#).

To add FC mappings for an FC project, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab, select the project from the **Projects** list and click **Manage > Access**. The **Project Access** page appears.
3. In the **FC** tab, click **Add**.
4. In the **Add Mapping** window, complete the following steps:
  - a) Select the initiator group from the **Initiator Group** list. Select **All** if you want to add all the available initiator groups.

- b) Select **Read Only** if you want to make this a read only mapping.
- c) Click **Add**.

## Deleting an iSCSI Mapping at a Project Level

To delete an iSCSI mapping set at the project-level, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab, select the project from the **Projects** list and click **Manage > Access**. The **Project Access** page appears.
3. In the **iSCSI** tab, select the mapping you want to delete, and click **Delete**.
4. In the **Confirmation** window, click **OK**.

## Deleting FC Mappings at a Project Level

To delete a FC mapping set at the project-level, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab, select the project from the **Projects** list and click **Manage > Access**. The **Project Access** page appears.
3. In the **FC** tab, select the mapping you want to delete, and click **Delete**.
4. In the **Confirmation** window, click **OK**.

## Share Creation Defaults

---

You can set share creation defaults — ACL inheritance and block size— from the **Generic Project Settings** page.

### ACL inheritance

The **ACL inheritance** property enables you to enable or disable the ACL inheritance. If ACL Inheritance is enabled, when a new file is created inside a share, the new file inherits the project level ACL settings. If it is disabled, the new file does not inherit ACLs; you can set ACLs specific to the file.

### Block size

The **Block size** property enables you to set the block size for file systems in a share. The default record size is 32 KB. You can change the record size based on the type of file system stored in

a share. You can reduce the block size if you are using a share for storing any database. The record size can be equal to the block size of the database.

## Enabling or Disabling Share Creation Default Options

You can enable share creation default options at the project level—ACL inheritance and block size—from the **Settings** menu in the **Generic Project Settings** page.

To set a share creation defaults, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab on the left pane, select the project from the **Projects** list and click **Manage > Settings**.  
The **Generic Project Settings** page appears.
3. In the **Share** tab, complete the following steps:
  - a) Enable or disable **ACL Inheritance**.
  - b) Select the block size from the **Block size** list.
4. Click **Save**.

### Related Topics

[Share Creation Defaults](#)

## Deleting a Project

---

Deleting a project deletes all shares, LUNs, snapshots, clones, and breaks existing replication relationships.



**Warning:** Before deleting a project, make sure that the data in the project is not required anymore.

To delete a project, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab, select the project you want to delete from the **Projects** list, and click **Delete**.
3. In the **Delete Project** confirmation window, enter the name of the project you want to delete.
4. If [Two-Factor Authentication \(2FA\)](#) is enabled for the user, enter the 2FA application code retrieved from your mobile device to delete the project.
5. Click **Delete**.



---

# Chapter 7

---

## Shares

---

**Topics:**

- *Shares*
- *Managing Shares*
- *Autohome Share*
- *Offline Files*
- *Subshares*



## Shares

---

A share is a file system which is shared over the network by using the NFS or SMB 1.0/2.0/3.0 protocols.

### IntelliFlash Support for Network File System (NFS)

Network File System (NFS) is a NAS protocol used for file sharing over a network. IntelliFlash supports NFSv2, NFSv3, NFSv4, NFSv4.1. In IntelliFlash, you can configure an NFS server from the **Services > NAS** page.

### IntelliFlash Support for Server Message Block (SMB) Protocols

IntelliFlash systems support the Server Message Block (SMB) protocols, which are typically used in Microsoft Windows environments. IntelliFlash supports SMB 1.0 (CIFS), SMB 2.0, and SMB 3.0.

SMB 1.0 or Common Internet File System (CIFS) is a NAS protocol. It enables file sharing with network permissions for Microsoft Windows clients over the network. You can configure an IntelliFlash Array for CIFS file sharing for either a Windows domain or a Windows workgroup.

IntelliFlash supports both SMB 2.0 and SMB 3.0 simultaneously. As certain features and IntelliFlash Web UI elements are applicable to both, they might be referred to as SMB2/SMB3 in the IntelliFlash Web UI.



**Restriction:** The array can support either SMB 1.0 (CIFS) or SMB 2.0/SMB 3.0 at a time. When you select one, support for the other is disabled at the array level.

## Shares in Project Templates

With project templates, IntelliFlash allows you to create shares specific to the application and protocol. For example, if you create an NFS project for the purpose of a **VMware VDI** application, IntelliFlash allows you to create only shares required for the **VMware VDI** application using the NFS protocol. However, if you have created a project with the **Generic** purpose, you can create shares and then enable NFS and SMB.

For more information, see [Project Templates](#).

You can create shares for the following purposes:

- Backup
- Database
- File sharing
- Virtual Server
- VMware VDI
- HyperV VDI
- SQL Server

- Generic



**Note:** When deduplication is enabled in a project, and when you create shares that have a block size lesser than 32 KiB (for Hybrid arrays) and lesser than 8 KiB (for All-Flash arrays), a warning message appears that recommended block size is higher than the assigned block size.

The following changes have been made in the IntelliFlash Web UI:

- The compression types are changed in the UI. The new options are **High Compression** and **Optimal Performance**, with Optimal Performance being the default compression type.
- The compression algorithm for **Optimal Performance** is lz4. The compression algorithm for **High Compression** is igzip.
- You can change the compression type for a share or disable compression in the **Advanced Settings** tab.
- The older compression types are renamed as **Legacy** and will continue to be supported.
- The **Data Synchronization** and the **LogBias** fields are removed from the web UI. Internally in IntelliFlash, Data Synchronization is set to **Always** and LogBias is set to **Latency**.
- The **Primary Cache** and **Secondary Cache** fields are combined and renamed as **Read Cache**.

## Creating a Share

### Prerequisites

A pool and project should be created already.

To create a share in a project, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab on the left pane, select the project from the **Projects** list.
3. In the right pane, click the **Shares** tab.
4. In the **Shares** tab, click **New > Share**.  
The **New Share Creation** wizard appears.
5. In the **Name and Size Configuration** screen, complete the following steps:
  - a) In the **Quantity** field, select **Single** or **Multiple**.  
Select **Multiple** to create multiple shares of the same type.
  - b) Type the share name in **Share Name**.  
If you select **Multiple**, include # with the share name.
  - c) If you select **Multiple**, enter the number of shares you want in the **Count** field, and specify where the count should start in the **Start** field.  
For example, if you have provided **Share Name** as Share\_Name, **Count** as 4, and **Start at** as 1, then four shares with the names, Share\_Name\_1, Share\_Name\_2, Share\_Name\_3, and Share\_Name\_4 are created.
  - d) Select **Mountpoint** and modify the mountpoint.

IntelliFlash uses the default mountpoint: `/export/ < project name>/< share name>`. However, you can change the mountpoint.

- e) Select **Share Quota** and set a quota limit.
  - f) Type or select a unit for the share quota.
  - g) Select **Share Reservation** to reserve space.
  - h) Type or select a unit for space reservation.
  - i) From the **Purpose** dropdown, select the purpose of the share. For more information on purpose, see [Shares in Project Templates](#).
  - j) Select the size from the **Block size** dropdown list.
  - k) Click **Next**.
6. In the **Permissions and Sharing** screen, complete the following:
- a) From the **Grant Access** list, select **Everyone**, **User**, or **Group**. By default, **No Access** is selected for the **Grant Access** list.
  - b) (Optional) Click **Override project settings** and then enable **NFS Sharing** and **SMB Sharing**.
  - c) (Optional) If you select **SMB Sharing**, type the display name in the **SMB Display name** field.
-  **Note:**

  - The **SMB Display name** field does not appear in the wizard when you create a share within a VMware VDI or Virtual Server project.
  - To hide the share, you can use the "\$" symbol at the end of the display name for the share.
- d) Click **Next**.
7. (Optional) In the **Snapshot Schedules** screen, the default snapshot policy of the project is automatically selected. You can retain the default preset profile or customize the profile.
- If you want to retain the default preset profile, click **Next**.
  - If you want to customize the profile, click **Override project snapshot policy**. Select a profile from the **Schedule** list and customize it according to your requirements. You can add more conditions by clicking the **Add** (+) icon.
- For more information, see [Preset Profiles for Snapshots](#), [Custom Snapshot Schedules](#), and [Overriding a Project Snapshot Schedule](#).
8. In the **Summary** screen, review the summary and click **Create**.

## Creating a Folder in a Share

To create a folder in a share, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab on the left pane, select the project from the **Projects** list.
3. In the right pane, click the **Shares** tab.
4. In the **Shares** tab, select the share and click **New > Folder**.  
The **Add Folder** dialog box appears.
5. In the **Add Folder** dialog box, type a name in the **Folder Name** box.
6. Click **Add**.

## Deleting a Share

When you delete a share, all the data inside the share is also deleted. Deleting a parent share that has subshares deletes all of the child shares and dependent clones.

To delete a share, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab on the left pane, select the project from the **Projects** list.
3. In the right pane, click the **Shares** tab.
4. In the **Shares** page, select the share you want to delete and click **Delete**.
5. In the **Conformation** dialog box, click **OK** to continue.
6. In the **Delete Share** confirmation window, enter the name of the share to be deleted.
7. If [Two-Factor Authentication \(2FA\)](#) is enabled for the user, enter the 2FA application code retrieved from your mobile device to delete the share.
8. Click **Delete**.

## Deleting a Folder in a Share

When you delete a folder, all the files and subfolders inside the folder are also deleted.

To delete a folder in a share, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab on the left pane, select the project from the **Projects** list.
3. In the right pane, click the **Shares** tab.
4. Select the share that contains the folder.
5. In the share, select the folder you want to delete and click **Delete**.
6. In the **Confirmation** dialog box, click **OK**.

## Managing Shares

---

After creating shares, you need to manage share properties for various purposes.

To manage a share, select the share and click **Manage > Settings**, **Manage > Access**, and **Manage > Snapshots**.

The following sections provide detailed information on managing a share.

### Modifying Share-Level Quota

You can increase, decrease, or set the quota on an already existing share.

To modify a share-level quota, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab on the left pane, select the project from the **Projects** list.
3. In the right pane, click the **Shares** tab.
4. In the **Shares** tab, select the share and click **Manage > Settings**.  
The **Share Settings** page appears.
5. In the **General** tab, select **Share Quota** if the quota has not been set previously.
6. Type or modify the share quota size.
7. Select a unit for space reservation.
8. Click **Save**.

### Setting Quota Limit for Users and Groups

IntelliFlash allows you to set the quotas at share level for users and groups. You can search for the user or group and set the quota for both local and domain user/groups.

When the usage reaches certain limit, the user gets a notification with the following threshold values:

1. **Warning Threshold:** when the usage value reaches 80% of the assigned quota.
2. **Critical Threshold:** when the usage reaches 95% of the assigned quota.

User can customize the values of these two thresholds based on requirements.

To set the quota for a new user or group, perform the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab on the left pane, select the project from the **Projects** list.
3. In the right pane, click the **Shares** tab.
4. In the **Shares** tab, select the share and click **Manage > Access**.  
The **Share Access** page appears.
5. In the **Quota** tab, click **Add**.  
The **Set Quota** dialog box appears.
6. To set quota for an user:
  - a) Select **User** from the **Type** dropdown list to set quota for an user.
  - b) Click **Enter User** if you know the username, otherwise click **Search User** to search for the user.
  - c) Enter or select the user name from the **User Name** dropdown list.
  - d) In the **Quota** field, set the required quota for the user.
7. To set quota for a group:
  - a) Select **Group** from the **Type** dropdown list to set quota for a group.
  - b) Click **Enter Group** if you know the group name, otherwise click **Search Group** to search for the user.
  - c) Enter or select the group name from **Group Name** dropdown list.
  - d) In the **Quota** field, set the required quota for the group.



**Note:** Local user/group quotas applies when the array is in workgroup mode and not in domain mode.

## Modifying Space Reservation for a Share

You can increase, decrease, or set space reservation on an already existing share.

To modify the space reservation, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab on the left pane, select the project from the **Projects** list.
3. In the right pane, click the **Shares** tab.
4. In the **Shares** tab, select the share and click **Manage > Settings**.  
The **Share Settings** page appears.
5. In the **General** tab, select **Share Reservation** if it has not been set previously.
6. In the text field, enter or modify the share reservation size.
7. Select a unit for space reservation.
8. Click **Save**.

## Modifying a Share Mountpoint

### Prerequisites

- Disable NFS and SMB sharing before modifying the mountpoint.

When you modify a mountpoint for a share, you are overriding the mountpoint set at the project-level. You can revert to the project-level mountpoint whenever you need to by clearing the mountpoint option in the **Share Settings** page.

To modify the mountpoint of a share, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab on the left pane, select the project from the **Projects** list.
3. In the right pane, click the **Shares** tab.
4. In the **Shares** tab, select the share and click **Manage > Settings**.  
The **Share Settings** page appears.
5. Click the **Advanced** tab.
6. In the **Advanced** tab, click **Edit** in the **Inherited Settings** section.
7. In the **Edit Settings** dialog box, click **Enable Override** and then click **Mountpoint**.
8. Click **Save**.
9. In the **Advanced** tab, in the **Override Settings** section, modify the path in the **Mountpoint** field.

The mountpoint path should start with a forward slash (/). For example, /example/share.

10. Click **Save**.
11. Enable SMB and NFS sharing after modifying the mountpoint. For more information, see [Enabling and Disabling SMB Project Level Settings for a Share](#) and [Enabling and Disabling NFS Project Level Settings for a Share](#).

## Overriding Compression Class in a Share

To override the compression type set at the project level for a share, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab on the left pane, select the project from the **Projects** list.
3. In the right pane, click the **Shares** tab.
4. In the **Shares** tab, select the share and click **Manage > Settings**.  
The **Share Settings** page appears.
5. Click the **Advanced** tab.
6. In the **Advanced** tab, click **Edit** in the **Inherited Settings** section.
7. In the **Edit Settings** dialog box, click **Enable Override** and then click **Compression**.
8. Click **Save**.  
The **Compression** text box appears in the **Override Settings** section.
9. In the **Advanced** tab, in the **Override Settings** section, select the compression type from the **Compression** list.
  - The compression types are **High Compression** and **Optimal Performance**. **Optimal Performance** is the default compression type.
  - If you do not want compression enabled, select **OFF**.
  - When you select the compression type, the corresponding compression algorithm appears below the **Compression** text box. The compression algorithm for Optimal Performance is lz4. The compression algorithm for High Compression is igzip.
  - The older compression types are renamed as **Legacy** and will continue to be supported.
10. Click **Save**.

## Overriding Deduplication Setting at Share Level

To override the deduplication setting for a specific share, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab on the left pane, select the project from the **Projects** list.
3. In the right pane, click the **Shares** tab.
4. In the **Shares** tab, select the share and click **Manage > Settings**.  
The **Share Settings** page appears.
5. In the **Advanced** tab, click **Edit** in the **Inherited Settings** section.
6. In the **Edit Settings** dialog box, click **Enable Override** and then click **Deduplication**.
7. Click **Save**.
8. In the **Advanced** tab, in the **Override Settings** section, enable or disable **Deduplication**.
9. Click **Save**.

## Overriding Read Only Property for a Share

To override the Read only property setting for a specific share, using the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab on the left pane, select the project from the **Projects** list.
3. In the right pane, click the **Shares** tab.
4. In the **Shares** tab, select the share and click **Manage > Settings**.  
The **Share Settings** page appears.
5. In the **Advanced** tab, click **Edit** in the **Inherited Settings** section.
6. In the **Edit Settings** dialog box, click **Enable Override** and then click **Read Only**.
7. Click **Save**.
8. In the **Advanced** tab, in the **Override Settings** section, enable or disable **Read Only**.
9. Click **Save**.

## Overriding ACL Inheritance Setting at Share-Level

To override the ACL Inheritance setting for a specific share, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab on the left pane, select the project from the **Projects** list.
3. In the right pane, click the **Shares** tab.
4. In the **Shares** tab, select the share and click **Manage > Settings**.  
The **Share Settings** page appears.
5. Click the **Advanced** tab.
6. In the **Advanced** tab, click **Edit** in the **Inherited Settings** section.
7. In the **Edit Settings** dialog box, click **Enable Override** and then click **ACL Inheritance**.
8. Click **Save**.
9. In the **Advanced** tab, in the **Override Settings** section, enable or disable **ACL Inheritance**.
10. Click **Save**.

## Overriding the Block Size for a Share

To override the block size set at the project level of a share, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab on the left pane, select the project from the **Projects** list.
3. In the right pane, click the **Shares** tab.
4. In the **Shares** tab, select the share and click **Manage > Settings**.  
The **Share Settings** page appears.
5. Click the **Advanced** tab.
6. In the **Advanced** tab, click **Edit** in the **Inherited Settings** section.
7. In the **Edit Settings** dialog box, click **Enable Override** and then click **Block Size**.
8. Click **Save**.
9. In the **Advanced** tab, in the **Override Settings** section, enable or disable **Block Size**.
10. Click **Save**.

## Overriding Cache Behavior at Share Level

To override the cache behavior set at the project level for a share, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab on the left pane, select the project from the **Projects** list.
3. In the right pane, click the **Shares** tab.
4. In the **Shares** tab, select the share and click **Manage > Settings**.  
The **Share Settings** page appears.
5. Click the **Advanced** tab.
6. In the **Advanced** tab, click **Edit** in the **Inherited Settings** section.
7. In the **Edit Settings** dialog box, click **Enable Override** and then click **Read Cache**.
8. Click **Save**.
9. In the **Advanced** tab, in the **Override Settings** section, select the required compression type from the **Read Cache** list.
10. Click **Save**.

## Setting Access Time for a Share

To change the access time property set at the project level of a share, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab on the left pane, select the project from the **Projects** list.
3. In the right pane, click the **Shares** tab.
4. In the **Shares** tab, select the share and click **Manage > Settings**.  
The **Share Settings** page appears.
5. Click the **Advanced** tab.
6. In the **Advanced** tab, in the **Other Settings** section, enable or disable **Access time**.
7. Click **Save**.

## Setting NBMAND

You can enable or disable the non-blocking mandatory locks (NBMAND) on a share. The NBMAND property only applies to shares which are in General File Services. This property provides access of an SMB share to NFS clients. NBMAND is, by default, enabled for SMB

shares and disabled for NFS shares. Enable NBMAND if the share is accessed by both the SMB and NFS clients.

To set NBMAND after share creation, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab on the left pane, select the project from the **Projects** list.
3. In the right pane, click the **Shares** tab.
4. In the **Shares** tab, select the share and click **Manage > Settings**.  
The **Share Settings** page appears.
5. Click the **Advanced** tab.
6. In the **Advanced** tab, in the **Other Settings** section, enable or disable **NBMAND**.
7. Click **Save**.

## Viewing the Purpose of a Share

To view the purpose of a share, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab on the left pane, select the project from the **Projects** list.
3. In the right pane, click the **Shares** tab.
4. In the **Shares** tab, select the share and click **Manage > Settings**.  
The **Share Settings** page appears.
5. In the **General** tab, view the purpose in the **Purpose** field.

## Overriding NFS Project Level Settings for a Share

To override NFS settings at the project level, complete the following steps.

1. Click **Provision > Projects**.
2. In the **Local** tab on the left pane, select the project from the **Projects** list.
3. In the right pane, click the **Shares** tab.
4. In the **Shares** tab on the right, select the share and click **Manage > Access**.  
The **Share Access** page appears.
5. In the **Sharing** tab, select **Override Project Settings**.
6. In the **NFS** tab, enable or disable **NFS Sharing**.

## Configuring Anonymous User IDs or Groups IDs on an NFS Share

When a user connects to an NFS share without valid credentials, the configured anonymous user ID or group ID is used to determine the security access to the share and folder-files.

To configure anonymous user IDs or group IDs on NFS shares, do the following:

1. Click **Provision > Projects**.
2. In the **Local** tab on the left pane, select the project from the **Projects** list.
3. In the right pane, click the **Shares** tab.
4. In the **Shares** tab on the right, select the share and click **Manage > Access**. The **Share Access** page appears.
5. In the **NFS** tab, click **Edit** under **Anonymous** section. The **Edit Anonymous ID** dialog box appears. The anonymous ID is set to "Nobody" by default.
6. In the **Edit Anonymous ID** dialog box, select from the following values:
  - **Nobody (default)**: When you select this option, the client access request is mapped to the user "Nobody." The client access to files and folders is based on the permissions available for the IntelliFlash "nobody" user account. This is the default choice. The anonymous ID for the **Nobody** option is set to 60001.
  - **Other**: When you select this option, the client access request is mapped to the anonymous ID specified here. The client secures access based on the permissions configured for the IntelliFlash "Other" user account. The anonymous ID for the **Other** option can be set to any value up to 2147483647.
  - **root**: When you select this option, the client root access request is mapped to the user "root." The client secures access based on the permissions set for the IntelliFlash "root" user account. The anonymous ID is set to 0 for the **root** option.
  - **Disabled**: When you select this option, the client access request is denied for anonymous users. The anonymous ID for the **Disabled** option is set to -1.

## Enabling or Disabling Kerberos on an NFS Share

Enable the Kerberos option on an NFS share if you want to mount the share using the sec=krb5 option. You can disable the option if you do not want to use Kerberos for authentication. After disabling the Kerberos option, you might need to remount the share.

To enable or disable the Kerberos option on an NFS share, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab on the left pane, select the project from the **Projects** list.
3. In the right pane, click the **Shares** tab.
4. In the **Shares** tab on the right, select the share and click **Manage > Access**.

The **Share Access** page appears.

5. In the **Sharing** tab, select **Override Project Settings**.
6. In the **NFS** tab, select or clear **Enable Kerberos**.

## Overriding SMB Project Level Settings for a Share

To override the SMB settings at the project level, complete the following steps.

1. Click **Provision > Projects**.
2. In the **Local** tab on the left pane, select the project from the **Projects** list.
3. In the right pane, click the **Shares** tab.
4. In the **Shares** tab on the right, select the share and click **Manage > Access**.  
The **Share Access** page appears.
5. In the **Sharing** tab, select **Override Project Settings**.
6. In the **SMB** tab, enable or disable **SMB Sharing**.

## Changing SMB Share Display Name

To change the SMB share display name, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab on the left pane, select the project from the **Projects** list.
3. In the right pane, click the **Shares** tab.
4. In the **Shares** tab on the right, select the share and click **Manage > Access**.  
The **Share Access** page appears.
5. In the **Sharing** tab, select **Override Project Settings**.
6. In the **SMB** tab, enable **SMB Sharing**.
7. Click **Edit** for the **Display Name** field.
8. In the **Display Name** text box, type a new name.
9. Click **Save**.

## Creating a Hidden SMB Share

To create a hidden SMB share, complete the following steps:

1. Click **Provision > Projects**.
  2. In the **Local** tab on the left pane, select the project from the **Projects** list.
  3. In the **Shares** tab, click **New > Share**.
- The **New Share Creation** wizard appears.
4. In the **Name** and **Space** screen, enter the required details.
  5. In the **Permissions** screen, type **SMB share name** and append **\$** in the end to hide the SMB share.
  6. Fill in the required details in **Snapshots** and **Summary** screens. For more information, see [Creating a Share](#).



**Note:** Users can access a hidden SMB share with its name.

## Modifying Space Usage Threshold Levels for a Share

The default space usage threshold is defined in the **Settings > Notifications > Threshold** page.

You can now override the default threshold levels and set custom threshold levels for a specific share.

To set custom threshold levels for a share, do the following:

1. Click **Provision > Projects**.
2. Select the share and click **Manage > Settings**.  
The **Share Settings** page appears.
3. In the **General** tab, in the **Share Thresholds** section, click **Enable Share Threshold**.  
Enabling this button overrides the default threshold levels.
4. Select new values for **Warning threshold** and **Critical threshold**.
5. Click **Save**.

When the share exceeds the space usage thresholds, the Web UI now indicates that the share is running out of space. Warning or Critical icon appears next to the share. When you mouse over the Warning or Critical icon, the Web UI displays the free space remaining. If you have not defined a quota for the share, you do not see the warnings.

## Autohome Share



**Note:** Autohome shares support is only for SMB in both General File Services and Virtualization File Services.

The Autohome Share feature automatically creates a home directory when a new user logs in to the system for the first time. This enables the user to securely access only their home directory and maintain them from any system. You can configure an Autohome share in both domain or workgroup environments. By default, Autohome share is configured for continuous availability mode and can be configured for Offline mode if required.

In a Workgroup environment, you can add users to the IntelliFlash Array and provide access to them. Users must provide the user name and password which you provided in the IntelliFlash OS, to access the home directory share. The IntelliFlash OS creates shares with the user login name and the users can access their individual home directory shares from any system within the workgroup or domain.

Similarly, in a domain environment, the IntelliFlash OS utilizes user names from Active Directory (AD) to create home directory shares.

You can also add users in the IntelliFlash OS and map them to AD users to provide access to the home directory shares.

The IntelliFlash OS allows you to create a single Autohome share per storage array. By using the Autohome share, you can set and manage user-level quotas.

### Creating an Autohome Share

#### Prerequisites

- Enable SMB.
- Configure SMB in a workgroup or domain.
- Obtain proper user ID mapping.



**Caution:** Creating a share with the same name as an existing or future Autohome share is not supported. As the names of Autohome shares are based on LDAP/AD user names, make sure you do not create a share with the same name as an LDAP/AD user name.

To create an autohome share, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab on the left pane, select the project from the **Projects** list.
3. In the right pane, click the **Shares** tab.
4. In the **Shares** tab, click **New > Share**.  
The **New Share Creation** wizard appears.
5. In the **Name and Size Configuration** screen, complete the following steps:

**Quantity** field gets disabled after selecting **Autohome** from the **Purpose** dropdown list.

- a) Type the share name in **Share Name**.
  - b) Select **Share Quota** and set a quota limit.
  - c) Type or select a unit for the share quota.
  - d) Select **Share Reservation** to reserve space.
  - e) Type or select a unit for space reservation.
  - f) From the **Purpose** dropdown list, select **Autohome**
  - g) Select a **Block size** from the dropdown list.
  - h) Select **Per User Quota** and set the quota limit.
  - i) Click **Next**.
6. In the **Summary** screen, review the summary and click **Create**.

## Setting up Access Permissions to the Autohome Share

After creating the Autohome share, set up access permissions. You can allow or deny access to the Autohome share for a user, group, or everyone.

To set up access permissions for the Autohome share, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab on the left pane, select the project from the **Projects** list.
3. In the right pane, click the **Shares** tab.
4. In the **Shares** tab, select the **Autohome** share, and click **Manage > Access**.  
The **Share Access** page appears.
5. Click the **Autohome** tab.
6. In the **Autohome** tab, click **New**.  
The **Add Autohome Permissions** dialog box appears.
7. In the **Add Autohome Permissions** dialog box, complete the following steps:
  - a) From the **Type** dropdown list, select the user type.
  - b) From the **Mode** dropdown list, select the access type.
  - c) Select the user or group name, depending on the user type you selected.
  - d) Type the domain or workgroup name.
  - e) Click **Add**.

## Enabling or Disabling Autohome Share Service

To enable or disable the Autohome share service, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab on the left pane, select the project from the **Projects** list.
3. In the right pane, click the **Shares** tab.
4. In the **Shares** tab, select the **Autohome** share, and click **Manage > Access**.
5. Click the **Autohome** tab.
6. In the **Autohome** tab, select or clear **Enable autohome service**.

## Offline Files

---

IntelliFlash Array supports offline files to enable the user to work offline for SMB protocol in Virtualization File Services mode. The user can either configure a file for offline use during creation of a file or modify an existing file to work in offline mode. After the user configures an offline folder in the server, client manages the client-side caching process.

### Creating an Offline Share

To create an offline share, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab on the left pane, select the project from the **Projects** list.
3. In the right pane, click the **Shares** tab.
4. In the **Shares** tab, click **New > Share**.  
The **New Share Creation** wizard appears.
5. In the **Name and Size Configuration** screen, complete the following steps:
  - a) Select **Single or Multiple**. Select **Multiple** to create multiple shares of the same type.
  - b) In the **Share Name** field, type a share name.  
If you have selected **Multiple** in step a, include # with the share name.
  - c) If you select **Multiple**, enter the number of shares you want in the **Count** field, and specify where the count should start in the **Start** field.  
For example, if you have provided Share Name as Share\_Name, Count as 4, and Start at as 1, then four shares with the names, Share\_Name\_1, Share\_Name\_2, Share\_Name\_3, and Share\_Name\_4 get created.
  - d) Select **Share Mountpoint** and modify the mountpoint.
  - e) Select **Share Quota** and set a quota limit.
  - f) Select **Share Reservation** to reserve space.

- g) Select the **Purpose** and **Block** size from dropdown.
6. Click **Next**.
7. In the **Permissions and Sharing** screen, complete the following:
- a) From the **Grant Access** list, select **Everyone**, **User**, or **Group** from the list. The default option is **No Access**.
  - b) (Optional) Click **Override project settings** and then enable **SMB Sharing**.
  - c) Enter the share name in **SMB Share Name** field.
  - d) Select **Enable Offline Files** to make your share **SMB Share Name** available in offline mode.
  - e) Select **Manual** to cache only selected files in a share on the client or **Automatic** to cache all the files of a share on the client.
8. Click **Next**, provide snapshot information in the **Snapshot schedules** screen.
9. Click **Next**, review the summary in the **Summary** screen and then click **Create**.

## Converting an Existing Share to Offline Share

To convert an existing share as Offline share, perform the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab on the left pane, select the project from the **Projects** list.
3. In the right pane, click the **Shares** tab.
4. In the **Shares** tab on the right, select the share and click **Manage > Access**.
5. In the **Sharing** tab, select **Override Project Settings**.
6. In the **SMB** tab, click **Edit** and select **Enable Offline Folders**.
7. Select **Manual** to cache only selected files in a share on the client or **Automatic** to cache all the files of a share on the client.
8. Click **Save**.

## Subshares

---

A share created within a share is called a subshare. The share in which a subshare is created is called a parent share. Subshare creation is supported only in Virtualization File Services mode.

In IntelliFlash, you can create subshares only with the SMB 1.0 (CIFS) protocol. Though IntelliFlash does not impose any limit on the number of levels of subshares, do not nest shares beyond three levels.

When you create subshares in the IntelliFlash Web UI, all the subshares appear at the same level as the parent share for a Windows user. You can also map a subshare as a network drive.

## Considerations for Using Subshares

Before creating and using subshares, read through the following considerations.

### General Considerations

- IntelliFlash arrays support subshares only for Virtualization File Services.
- To create subshares, you must enable **Subshare Creation** in the **Services > NAS > SMB** page.
- A subshare inherits properties from its parent share. However, you can override the parent share settings when creating a subshare or after creating it.
- You can set properties for a subshare in the same way you set properties for a share.
- When you delete a parent share, IntelliFlash deletes all the subshares within it and all the dependent clones.
- You cannot create an Autohome share using a subshare.
- The subshare properties might vary depending on the purpose of the subshare. You can select the purpose for a subshare in the Subshare creation wizard.
- When deduplication is enabled in a project, and when you create subshares that have a block size lesser than 32 KiB (for Hybrid arrays) and lesser than 8 KiB (for All-Flash arrays), a warning message appears that the recommended block size is higher than the assigned block size.

### Quota and Space Reservation

- You can set a quota limit for subshares. The quota limit cannot be greater than the parent share quota limit or project quota limit and space reserved.
- You can reserve space for subshares. However, the space reservation cannot be greater than the parent share and project space reservation.

### ACLs

- The default access permission for a subshare is: **No Access**. You must provide access to the subshare while creating it or after creation.
- When setting up a user ACL for a share, you can enable the ACL inheritance for subshares as well.
- You can hide a subshare in Windows by adding the “\$” symbol at the end of the display name of the subshare. You can hide the parent share similarly.

## Snapshots and Clones

- The Manage Settings page in a subshare does not list the snapshots of a subshare. However, IntelliFlash creates snapshots of all the subshares when it takes the snapshots of the parent share.
- Subshares always inherit the snapshot policy from the parent share. You cannot set a snapshot policy specific to a subshare.
- When you clone a parent snapshot, IntelliFlash clones all of the subshares retaining the subshare names and hierarchy.

## Replication

- Replicating a parent share also replicates the subshares within it.
- Restoring a replica clone restores the share and all the subshares within it.

## Analytics

You can view the metrics for subshares from the SMB widget in **Analytics**.

## Usage Reports

You can generate subshares space usage reports using the **Subproject** report type. (**Services > Report > Usage Reports**).

## Enabling Subshares Creation Option

You can create subshares only with Virtualization File Services. You must enable the **Subshare creation** option in the **SMB Server Configuration** page to create and use subshares. The Subshare creation option is disabled by default.

To enable the subshares feature, complete the following steps:

1. Click **Services > NAS > SMB**.
2. In the **SMB Server Configuration** page, make sure the Virtualization File Services mode is enabled.
3. Enable **Subshare creation**.
4. Click **Save**.

## Creating a Subshare

### Prerequisites

A pool, project, and share are already created.

To create a subshare, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab on the left pane, select the project from the **Projects** list.
3. In the right pane, click the **Shares** tab.
4. In the **Shares** tab, select the share in which you want to create a subshare.
5. Click **New > Sub-Share**.  
The **New Sub-Share Creation** wizard appears.
6. In the **Name and Size Configuration** screen, complete the following steps:
  - a) Type the share name in the **Share Name** box.
  - b) Select **Mountpoint** and modify the mountpoint.  
IntelliFlash uses the default mountpoint: `/export/<project name>/<share name>`. However, you can change the mountpoint.
  - c) Select **Share Quota** and set a quota limit.
  - d) Type or select a unit for the share quota.
  - e) Select **Share Reservation** to reserve space.
  - f) Type or select a unit for space reservation.
  - g) From the **Purpose** dropdown, select the purpose of the share.
  - h) Select a **Block size**.
  - i) Click **Next**.
7. In the **Permissions and Sharing** screen, complete the following:
  - a) From the **Grant Access** list, select **Everyone**, **User**, or **Group** from the list. The default option is **No Access**.
  - b) (Optional) Click **Override parent settings** and then enable **SMB Sharing**.
  - c) (Optional) If you select **SMB Sharing**, type the display name in the **SMB Display name** field.
8. In the **Summary** screen, review the summary and click **Create**.



**Note:**

- The **SMB Display name** field does not appear in the wizard when you create a share within a VMware VDI or Virtual Server project.
- To hide the share, you can use the "\$" symbol at the end of the display name for the share.

- d) Click **Next**.

8. In the **Summary** screen, review the summary and click **Create**.

## Creating a Folder in a Subshare

To create a folder in a subshare, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab on the left pane, select the project from the **Projects** list.
3. In the right pane, click the **Shares** tab.
4. In the **Shares** tab, select the parent share.
5. From the list of subshares in the parent share, select the required subshare.  
If a subshare has multiple levels of subshares, click the arrow icon of the child share to access the desired subshare.
6. Click **New > Folder**.  
The **Add Folder** dialog box appears.
7. In the **Add Folder** dialog box, type a name in the **Folder Name** box.
8. Click **Add**.

## Managing Subshares

After you create a subshare, you can manage the properties of the subshare for various purposes. You can:

- Override the general and advanced properties of a parent share and set configurations specific to a subshare.
- Enable or disable SMB sharing.
- Modify the subshare display names.
- Manage user ACLs.

To manage a subshare, select the subshare and click **Manage > Access** or click **Manage > Settings**.

## Deleting a Subshare

Deleting a subshare deletes all the data inside the subshare and users can no longer access that subshare.



**Note:** Deleting a parent share deletes all the subshares and dependent clones.

To delete a subshare, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab on the left pane, select the project from the **Projects** list.
3. In the right pane, click the **Shares** tab.
4. In the **Shares** tab, select the parent share.
5. From the list of subshares in the parent share, select the required subshare.  
If a subshare has multiple levels of subshares, click the arrow icon of the child share to access the desired subshare.
6. Click **Delete**.
7. In the **Delete Share** confirmation window, enter the name of the share to be deleted and click **Delete**.



---

# Chapter 8

---

## Access Control Lists

---

**Topics:**

- *Access Control Lists*
- *Network ACLs*
- *User ACLs*
- *Folder ACLs*

## Access Control Lists

---

Using Access Control List (ACL), you can define access permissions for networks and users on shares. An ACL can have multiple Access Control Entries (ACEs).

An ACL specifies which network IP address, group, or user can access a particular share and its data. With network ACLs, you can define read-only or read-write access permissions for a project or a share. With user ACLs, you can allow or deny access to a share. You can define network ACLs on both projects and shares, but define user ACLs only on shares.

The IntelliFlash OS supports both network ACLs and user ACLs. Use a combination of network ACLs and user ACLs to manage access permissions.

You can search for Windows Active Directory users along with local users when adding user level ACLs for shares. The IntelliFlash OS can communicate with the Windows Active Directory Server to access user and group names for authentication.

 **Note:** For the IntelliFlash OS to search Active Directory users or groups, you must first add users and groups in the AD Server and enable the UNIX attributes for the users and groups.

If you need to add ACLs for AD users and groups using the IntelliFlash OS, you must configure the Active Directory and AD/Kerberos Setup settings on the IntelliFlash OS and also enable the **IDMU** setting. You can configure these settings under **Services > NAS > Identity Management**.

## Network ACLs

---

### Network ACLs

You can define network ACLs on projects and shares. Network ACLs provide access permissions for NFS clients to mount and SMB clients to access a share.

The default network ACL is *allow all*. If no network ACL is defined, any system within the network can mount or access the shares in a project.

In IntelliFlash, a network ACL has the following properties:

- **Access Mode:** Read-only or Read-write
- **Access Type:** IP address or fully qualified domain name (FQDN)

 **Note:** You can add a partial IP address to cover the complete subnet. For example, 192.168.2.

When defining network ACLs using an IP address, you can provide the network part of an IP address or the complete IP address.

- For a **Class A** network IP address, you can provide the first octet of the address.
- For a **Class B** network IP address, you can provide the first two octets of the address.
- For a **Class C** network IP address, you can provide the first three octets of the address.

You can define network ACLs when creating or after creating a project or a share.

## Adding a Network ACL for an NFS Project

### Prerequisites

- The NFS project is already created.  
For more information, see [Creating Projects](#).
- NFS sharing must be enabled on the project to add Network ACLs.

The default ACL policy is *allow all*.

To add a Network ACL for a project, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab on the left pane, select the project from the **Projects** list and click **Manage > Access**.  
The **Project Access** page appears.
3. Click the **NFS** tab.
4. If NFS is not enabled, enable **NFS Sharing**.
5. In the **Network ACLs** section, click **Add**.
6. In the **NFS ACLs for Project** dialog box, complete the following steps:
  - a) Select the access mode from the **Access Mode** dropdown list.
  - b) Select the access type from the **Access Type** dropdown list.
  - c) Type the **IP address** or **FQDN**, according to the access type you had chosen earlier.  
You can add a partial IP address to cover the complete subnet.
    - For a **Class A** network IP address, you can provide the first octet of the address.
    - For a **Class B** network IP address, you can provide the first two octets of the address.
    - For a **Class C** network IP address, you can provide the first three octets of the address.
  - d) (Optional) Select **Root Access**.
- e) Click **Add**.



**Note:** This option preserves the root UID without squashing.

## Adding a Network ACL for an NFS Share

You must override the project-level network ACL policy and provide a network ACL specific to a share. To add an NFS network ACL for a share, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab on the left pane, select the project from the **Projects** list.
3. In the **Shares** tab on the right, select the share and click **Manage > Access**.  
The **Share Access** page appears.
4. In the **Share Access** page, enable **Override Project settings**, if it is not enabled already.
5. In the **Share Access** page, click the **NFS** tab.
6. Enable **NFS Sharing**, if it is not enabled already.
7. In the **Network ACLs** section, click **Add**.
8. In the **Add NFS ACL for Share** dialog box, complete the following steps:
  - a) Select the access mode from the **Access Mode** dropdown list.
  - b) Select the access type from the **Access Type** dropdown list.
  - c) Type the **IP address** or **FQDN**, according to the access type you had chosen earlier.  
You can add a partial IP address to cover the complete subnet.
    - For a **Class A** network IP address, you can provide the first octet of the address.
    - For a **Class B** network IP address, you can provide the first two octets of the address.
    - For a **Class C** network IP address, you can provide the first three octets of the address.
  - d) (Optional) Select **Root Access**.
 

 **Note:** This option preserves the root UID without squashing.
  - e) Click **Add**.

## Adding a Network ACL for an SMB Project

### Prerequisites

- The SMB project is already created.  
For more information, see [Creating Projects](#).
- SMB sharing must be enabled on the project to add Network ACLs.

The default ACL policy is *allow all*.



**Caution:** When adding network ACLs in an SMB project, a share might not be available for a few seconds or the active I/Os might fail.

To add a network ACL for an SMB project, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab on the left pane, select the project from the **Projects** list and click **Manage > Access**.  
The **Project Access** page appears.
3. Click the **SMB** tab.
4. In the **SMB** tab, enable **SMB Sharing** if it has not been enabled.
5. In the **Network ACLs** section, click **Add**.
6. In the **SMB ACLs for Project** dialog box, complete the following steps:
  - a) Select the access mode from the **Access Mode** dropdown list.
  - b) Select the access type from the **Access Type** dropdown list.
  - c) Type the **IP address or FQDN**, according to the access type you had chosen earlier.  
You can add a partial IP address to cover the complete subnet.
    - For a **Class A** network IP address, you can provide the first octet of the address.
    - For a **Class B** network IP address, you can provide the first two octets of the address.
    - For a **Class C** network IP address, you can provide the first three octets of the address.
  - d) Click **Add**.

## Adding a Network ACL for an SMB Share

To add an SMB network ACL for a share, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab on the left pane, select the project from the **Projects** list.
3. In the **Shares** tab on the right, select the share and click **Manage > Access**.  
The **Share Access** page appears.
4. In the **Share Access** page, enable **Override Project settings**, if it is not enabled already.
5. In the **Share Access** page, click the **SMB** tab.
6. Enable **SMB Sharing**, if it is not enabled already.
7. In the **SMB ACLs for Share** dialog box, complete the following steps:
  - a) Select the access mode from the **Access Mode** dropdown list.
  - b) Select the access type from the **Access Type** dropdown list.
  - c) Type the **IP address or FQDN**, according to the access type you had chosen earlier.  
You can add a partial IP address to cover the complete subnet.

- For a **Class A** network IP address, you can provide the first octet of the address.
  - For a **Class B** network IP address, you can provide the first two octets of the address.
  - For a **Class C** network IP address, you can provide the first three octets of the address.
- d) Click **Add**.

## Deleting a Network ACL for an NFS Project

After deleting a network ACL policy for an NFS project, the associated IP address or FQDN cannot access the shares inside the project. If no additional ACL policy is set for the project, IntelliFlash implements the default ACL of *allow all*.

To delete a network ACL policy for an NFS project, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab on the left pane, select the project from the **Projects** list and click **Manage > Access**.  
The **Project Access** page appears.
3. Click the **NFS** tab.
4. In the **Network ACLs** section, select the required ACL and click **Delete**.
5. In the **Confirmation** dialog box, click **Yes**.

## Deleting a Network ACL for an NFS Share

After deleting a network ACL policy for an NFS share, the IP address or FQDN cannot access the share. If no additional ACL policy is set for the share, IntelliFlash implements the default ACL of *allow all*.

To delete a share-level NFS ACL, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab on the left pane, select the project from the **Projects** list.
3. In the **Shares** tab on the right, select the share and click **Manage > Access**.  
The **Share Access** page appears.
4. In the **Share Access** page, click the **NFS** tab.
5. In the **Network ACLs** section, select the required ACL and click **Delete**.
6. In the **Confirmation** dialog box, click **Yes**.

## Deleting a Network ACL for an SMB Project

After deleting a network ACL policy for an SMB project, the IP address or FQDN cannot access the shares inside the project. If no additional ACL policy is set for the project, IntelliFlash implements the default ACL of *allow all*.

To delete a project-level SMB ACL, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab on the left pane, select the project from the **Projects** list and click **Manage > Access**.  
The **Project Access** page appears.
3. Click the **SMB** tab.
4. In the **Network ACLs** section, select the required ACL and click **Delete**.
5. In the **Confirmation** dialog box, click **Yes**.

## Deleting a Network ACL for an SMB Share

After deleting a network ACL policy for an SMB share, the IP address or FQDN cannot access the share. If no additional ACL policy is set on the share, IntelliFlash implements the default ACL of *allow all*.

To delete a share-level network ACL, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab on the left pane, select the project from the **Projects** list.
3. In the **Shares** tab on the right, select the share and click **Manage > Access**.  
The **Share Access** page appears.
4. In the **Share Access** page, click the **SMB** tab.
5. In the **Network ACLs** section, select the required ACL and click **Delete**.
6. In the **Confirmation** dialog box, click **Yes**.

## User ACLs

---

### User ACLs

A user ACL consists of the following properties:

- Type
- Mode
- Inheritance

 **Note:** You must have the correct Windows and UNIX user ID mapping before defining user-level ACLs for users added in IntelliFlash.

 **Important:** Add or delete user ACLs only from the IntelliFlash Web UI.

## Type

The ACL Type property defines for whom an ACL applies. The standard ACL type options are: *Everyone*, *User*, and *Group*. You can select the required ACL Type when setting up a user-level ACL on a share.

- **Everyone:** Provides access permissions to any user or group that does not match with any other ACL for that share. All users can access and create files in the share, but they cannot view files and folders created by other users.
- **User:** Provides access permissions to a specific user.
- **Group:** Provides access permissions to a specific group.

## Mode

The ACL Mode property defines access permissions on a share and its contents. The standard ACL modes are *Allow* or *Deny*.

## Inheritance

The ACL inheritance property defines whether files and folders within a share can inherit the ACLs set for the share. When ACL inheritance is set, new files and folders created in the share inherit the ACLs for that share.

The following are the ACL inheritance methods:

- **Default (No inheritance):** All new files and folders within a share do not inherit the ACLs defined for the share. The ACL set applies only to the share.
- **Files:** All new files in a share inherit the ACLs defined for the share.
- **Directories:** All new folders in a share inherit the ACLs defined for the share.
- **Both:** All new files and directories in a share inherit the ACLs defined for the share.

## ACL Migration

In IntelliFlash, if you add a new ACL with an inheritance method of *files*, *directories*, or *both* on a share which has existing ACLs, then the IntelliFlash OS enforces the newly added ACLs for all of the existing files, folders, or both, depending on the inheritance method for that particular user ACL type.

After the IntelliFlash OS applies the new ACLs to the existing files and folders, users can access them according to the defined ACLs. Similarly, if you delete an ACL, it removes the access permissions on all files and folders in that share.

You can see in-progress notifications about ACL migration in the **Notifications** page. The ACL migration processing time depends on the number of files and folders in a share.

## Permissions

You can use preconfigured ACL sets to apply ACLs to groups, users, and folders.

The ACL sets and the privileges included in them are:

- **full\_set**: All privileges are included.
- **modify\_set**: All privileges are included, except *Delete Child*, *Write ACL*, and *Write Owner*.
- **read\_set**: Only the *List Directory*, *Execute File*, *Read Attributes*, *Read XAttr*, *Read ACL*, and *Synchronize* privileges are included.
- **write\_set**: All privileges are included, except *Delete File*, *Delete Child*, *Write ACL*, and *Write Owner*.



**Attention:** Users with the Write set privileges can create new files and folders but they cannot rename them, because renaming requires delete permissions.

For more information on the individual access privileges, see [User ACL Access Privileges](#).

## Adding User-Level ACLs

### Prerequisites

- Add users and groups in the Active Directory (AD) server before adding user-level ACLs for AD users and groups.



#### Note:

- For the IntelliFlash Array to search Active Directory users or groups, you must first add users and groups in the AD Server and enable the UNIX attributes for the users and groups.
- Ensure that you do not have same user names or group names on both the local groups and users (on the IntelliFlash Array) and the AD Server. If duplicate names exist, then the IntelliFlash OS uses the local user or group name on the IntelliFlash Array.

- If you do not use an Active Directory Server, add local users and groups in the IntelliFlash Array before adding user-level ACLs.



**Note:** If you are adding user ACLs on an existing share with files and folders, the IntelliFlash OS automatically starts ACL migration and applies the new ACL to the existing files and folders.

- You can add users and groups from the **Services > NAS > Users** menu.

To add user-level ACLs, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab on the left pane, select the project from the **Projects** list.
3. In the **Shares** tab on the right, select the share and click **Manage > Access**.  
The **Share Access** page appears.
4. In the **Share Access** page, click the **ACLs** tab.
5. In the **ACLs** tab, click **New**.  
The **Add ACL** dialog box appears.
6. In the **Add ACLs** dialog box, complete the following steps:
  - a) Select the ACL type (Everyone, User, Group) from the **Type** dropdown list.  
If you select **Users**, IntelliFlash Web UI displays **User Details**. If you select **Group**, IntelliFlash Web UI displays **Group Details**. If you select ACL type as **Everyone**, the User Details or the Group Details section does not appear.
  - b) In the **User Details** or the **Group Details** section, enter or search for the user or group name.  
The user and group names search is case sensitive. You must search by user name or group name. Do not use a first name or last name for search.
  - c) Select the access type from the **Access** dropdown list.
  - d) Select the inheritance type from the **Inheritance** dropdown list.
  - e) If the share includes subshares, enable **Include Sub-share** if you want to define the same permissions on the subshare as well.
  - f) Select the ACL set from the **Permissions** list.  
Alternatively, select or clear the privileges based on your requirement.  
For more information, see [Permissions](#) and [User ACL Access Privileges](#).
  - g) Click **Save**.

## Related Topics

[Permissions](#)

[ACL Migration](#)

## Deleting a User ACL

Deleting a user-level ACL removes the control set on a share for a user.

To delete a user ACL:

1. Click **Provision > Projects**.
2. In the **Local** tab on the left pane, select the project from the **Projects** list.
3. In the **Shares** tab on the right, select the share and click **Manage > Access**. The **Share Access** page appears.
4. In the **Share Access** page, click the **ACLs** tab.
5. In the **ACLs** tab, select the ACL from the list and click **Delete**.

## User ACL Access Privileges

In the IntelliFlash Web UI, the user ACL access privileges are grouped for various users. The grouped access privileges are called ACL sets. You can modify the ACL access privileges according to your requirements before adding a user ACL or ACL sets. Each ACL privilege is represented with an alpha character for easy identification.

The following table displays ACL access privileges details:

Access Privilege	Assigned Alpha Character	Description
List Directory	r	Permission to view the contents of a share.
Add File	w	Permission to add a new file to a share.
Execute File	x	Permission to execute a file or search the contents of a share.
Add Sub-Directory	p	Permission to create a sub-folder in a folder.
Delete File	d	Permission to delete a file.
Delete Child	D	Permission to delete a file or a folder within a share.
Read Attributes	a	Permission to read basic attributes (non-ACLs) of a file.
Write Attributes	A	Permission to change the times associated with a file or directory to an arbitrary value.
Read XAttr	R	Permission to read the extended attributes of a file or perform a lookup in the file's extended attributes directory.
Write XAttr	W	Permission to create extended attributes or write to the extended attributes directory.
Read ACL	c	Permission to create extended attributes or read the extended attributes directory.

Access Privilege	Assigned Alpha Character	Description
Write ACL	C	Permission to write the ACL or the ability to modify the ACL.
Write Owner	o	Permission to change the file's owner or group.
Synchronize	S	Placeholder. Not currently implemented.

## Folder ACLs

---

You can use folder-level ACLs to set access permissions on a folder inside a share. Using folder-level ACLs, you can allow or deny access to a folder to everyone, a group, or a user, and set ACL inheritance for files and sub-folders.

### Adding an ACL to a Folder

A folder inside a share inherits the share-level default ACL. However, you can specify a unique ACL for a folder and control the access.

To add ACLs for a folder, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab on the left pane, select the project from the **Projects** list.
3. In the **Shares** tab on the right, select the folder and click **Manage > Access**.
4. In the **ACLs** tab, click **New**.  
The **Add ACL** dialog box appears.
5. In the **Add ACLs** dialog box, complete the following steps:
  - a) Select the ACL type (Everyone, User, Group) from the **Type** dropdown list.  
If you select **Users**, IntelliFlash Web UI displays **User Details**. If you select **Group**, IntelliFlash Web UI displays **Group Details**. If you select ACL type as **Everyone**, the User Details or the Group Details section does not appear.
  - b) In the **User Details** or the **Group Details** section, enter or search for the user or group name.  
The user and group names search is case sensitive. You must search by user name or group name. Do not use a first name or last name for search.
  - c) Select the access type from the **Access** dropdown list.
  - d) Select the inheritance type from the **Inheritance** dropdown list.
  - e) If the folder includes subshares, enable **Include Sub-share** if you want to define the same permissions on the subshare as well.
  - f) Select the ACL set from the **Permissions** list.

Alternatively, select or clear the privileges based on your requirement.

- g) Click **Save**.

## Deleting Folder-Level ACLs

To delete a folder-level ACLs, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab on the left pane, select the project from the **Projects** list.
3. In the **Shares** tab on the right pane, select the folder and click **Manage > Access**.  
The **Share Access** page appears.
4. In the **ACLs** tab, select the ACL from the list and click **Delete**.



---

# Chapter 9

---

## LUNs

---

### Topics:

- [\*LUNs in Project Templates\*](#)
- [\*LUN Purpose\*](#)
- [\*LUNs\*](#)
- [\*Managing LUNs\*](#)

A logical unit number (LUN) or a volume is storage space carved out from a pool. A LUN is used for block-level data storage.

In the IntelliFlash OS, you can create thick and thin LUN types. For a thick LUN, the required storage space is reserved and for a thin LUN, storage space is provided as needed. The IntelliFlash OS creates a thick LUN unless you select the **Thin provisioning** option in the LUN wizard.

You can map a LUN to an initiator using the iSCSI and FC protocols. The IntelliFlash OS allows you to assign a LUN number manually, or it can allocate LUN numbers automatically.

The IntelliFlash OS enables you to create LUNs based on their purpose. For example, you can create a LUN for virtualization, database, backup, and raw storage. The IntelliFlash OS optimizes block size based on the purpose of the LUN.

On a thin-provisioned or thick-provisioned LUN, you can enable compression and deduplication to optimize the storage space. You can increase a LUN size depending on the availability of storage space in the pool. You can also take LUN snapshots for data protection.

### Supported Protocols

The IntelliFlash OS supports the iSCSI protocol and Fibre Channel protocol (FCP) for configuring SAN. The iSCSI protocol transmits SCSI commands over an IP network. FCP is a SCSI commands transmission protocol over Fibre Channel networks.

## LUNs in Project Templates

---

With project templates, IntelliFlash allows you to create LUNs specific to an application and a protocol. For example, if you create a project for Microsoft iSCSI Exchange Server, IntelliFlash allows you to create only the LUN types required for the Exchange Server using the iSCSI protocol. However, regardless of the project template, IntelliFlash allows you to create a LUN with the **Generic** purpose for both iSCSI and FC protocols.

 **Note:** When deduplication is enabled in a project, and when you create LUNs that have a block size lesser than 32 KiB (for Hybrid arrays) and lesser than 8 KiB (for All-Flash arrays), a warning message appears that the recommended block size is higher than the assigned block size.

When you are creating LUNs in a project, you can override project settings and select properties specific to the LUN. You can also override the default snapshot policy settings defined at the project level. For general information, see [Overriding Project Level Properties](#).

The following changes have been made in the IntelliFlash Web UI:

- The compression types are changed in the UI. The new options are **High Compression** and **Optimal Performance**, with Optimal Performance being the default compression type.
- The compression algorithm for **Optimal Performance** is lz4. The compression algorithm for **High Compression** is igzip.
- You can change the compression type or disable the compression in the **Advanced Settings** tab.
- The older compression types are renamed as **Legacy** and will continue to be supported.
- The **Data Synchronization** and the **LogBias** fields are removed from the web UI. Internally in IntelliFlash, Data Synchronization is set to **Always** and LogBias is set to **Latency**.
- The **Primary Cache** and **Secondary Cache** fields are combined and renamed as **Read Cache**.

## LUN Purpose

---

You can create LUNs for the following types of applications:

- Database
- Storage
- Backup
- Virtual Server
- VMware VDI
- Hyper-V VDI
- SQL Data
- SQL Log
- SQL Backup
- SQL TempDB Data
- SQL TempDB Log
- SQL Large Object

- Exchange Server Database
- Exchange Server Log

Depending on the purpose of the project, some or all of these applications appear as options in the **Purpose** dropdown list when you are creating a new LUN for the project. For example, all the applications appear in the **Purpose** dropdown list when creating a LUN in a **Generic** purpose project.

## LUNs

---

### Creating an iSCSI LUN

**Prerequisites:** You need a pool and a project available.

The LUN Creation wizard provides the option to inherit or customize project settings. Using the **Inherit** option, you can inherit LUN properties from the project and create a LUN quickly or customize the LUN according to your requirements.

To create an iSCSI LUN, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab on the left pane, select the project from the **Projects** list.
3. In the right pane, click the **LUNs** tab.
4. In the **LUNs** tab, click **New**.  
The **New LUN** wizard appears.
5. In the **Name and Size configuration** page, complete the following steps:
  - a) In the **Quantity** field, select **Single or Multiple**.  
Select **Multiple** to create multiple LUNs of the same type.
  - b) Type a LUN name in the **LUN Name** text box.  
If you select **Multiple**, include # with the LUN name.
  - c) If you select **Multiple**, enter the number of LUNs you want in the **Count** field, and specify where the count should start in the **Start** field.  
For example, if you have provided **LUN\_Name\_#** as LUN\_Name, **Count** as 4, and **Start at** as 1, then four LUNs with the names, LUN\_Name\_1, LUN\_Name\_2, LUN\_Name\_3, and LUN\_Name\_4 are created.
  - d) Type or select **LUN Size**.
  - e) Select the storage unit.
  - f) (Optional) By default, the IntelliFlash OS creates a thin LUN.  
Clear **Thin Provisioning** if you do not want IntelliFlash to create a thin LUN.
  - g) Select the required purpose for the LUN from the **Purpose** list.

- h) Select a block size from the **Block Size** list.



**Note:** Depending on the LUN purpose, the wizard automatically selects the block size. You can retain the default size or choose a different size.

- i) Select **iSCSI** from the **Protocol** list.
- j) In the **Settings** section, select any of the following options:
- Select **Inherit** if you want the LUN properties to be inherited from the project. If you select this option, go to [Step 9](#).
  - Select **Customize** to customize the LUN properties, and click **Next**.
6. In the **iSCSI Target Configuration** screen, complete the following steps:

If...	Then...
<b>You want to select the default target.</b>	<ol style="list-style-type: none"> <li>1. Click <b>Default Target</b>.</li> <li>2. Click <b>Next</b>.</li> </ol>
<b>You want to select an existing target.</b>	<p>Complete the following steps:</p> <ol style="list-style-type: none"> <li>1. Click <b>Choose Target</b>.</li> <li>2. Select the target from the <b>Choose Target</b> dropdown.</li> </ol> <p>The target group and status of the selected target appear.</p> <ol style="list-style-type: none"> <li>3. (Optional) Select <b>Authentication for Target</b> to authenticate CHAP. You can select <b>None</b>, <b>CHAP</b>, or <b>Mutual</b>.</li> </ol> <div style="background-color: #f0f0f0; padding: 10px;"> <p> <b>Note:</b></p> <ul style="list-style-type: none"> <li>• When you change <b>Authentication for Target</b> from <b>None</b> to <b>CHAP</b>, IntelliFlash displays the message: <b>Modifying the authentication mechanism affects the existing iSCSI sessions. Do you want to continue? [Yes   No]</b>. Click <b>Yes</b> to continue.</li> <li>• When you change <b>Authentication for Target</b> from <b>None</b> to <b>Mutual</b>, provide the CHAP username and password. The credentials are used by the initiator to authenticate the target.</li> </ul> </div> <ol style="list-style-type: none"> <li>4. Click <b>Next</b>.</li> </ol>

If...	Then...
<b>You want to create a new target.</b>	<p>Complete the following steps:</p> <ol style="list-style-type: none"> <li>1. Click <b>Create Target</b>.</li> <li>2. In the <b>Target Name</b> field, type a name. The wizard uses the provided target name to create a new target group and displays it in the <b>Target Group</b> field.</li> <li>3. To add the target to an existing target group, click the <b>select group</b> link and select the target group from the list. To select the default target group instead, select <b>default</b>.</li> <li>4. In the <b>Choose Network Bindings</b> section, select the required IP address.</li> <li>5. (Optional) Select <b>Authentication for Target</b> to authenticate CHAP. You can select <b>None</b>, <b>CHAP</b>, or <b>Mutual</b>.</li> </ol> <div style="background-color: #f0f0f0; padding: 10px;"> <p> <b>Note:</b></p> <ul style="list-style-type: none"> <li>• When you change <b>Authentication for Target</b> from <b>None</b> to <b>CHAP</b>, IntelliFlash displays the message: <b>Modifying the authentication mechanism affects the existing iSCSI sessions. Do you want to continue? [Yes   No]</b>. Click <b>Yes</b> to continue.</li> <li>• When you change <b>Authentication for Target</b> from <b>None</b> to <b>Mutual</b>, provide the CHAP username and password. The credentials are used by the initiator to authenticate the target.</li> </ul> </div> <ol style="list-style-type: none"> <li>6. Click <b>Next</b>.</li> </ol>

7. In the **iSCSI Initiator Group Configuration** screen, complete the following steps:

If...	Then...
<b>You want to provide access to the LUN without any restrictions.</b>	<p>Click <b>All</b> and then click <b>Next</b>.</p> <div style="background-color: #f0f0f0; padding: 10px;"> <p> <b>Note:</b></p> </div>

If...	Then...
	When you select <b>All</b> , it enables existing initiators as well as new initiators to access the newly created LUN.
<b>You want to use an existing initiator group.</b>	<p>Complete the following steps:</p> <ol style="list-style-type: none"> <li>Click <b>Choose Initiator Group</b>.</li> <li>Click the <b>Initiator Group</b> dropdown and select an initiator group from the list.</li> <li>Click <b>Next</b>.</li> </ol>
<b>You want to create a new initiator group.</b>	<p>Complete the following steps:</p> <ol style="list-style-type: none"> <li>Click <b>Create Initiator Group</b>.</li> <li>In the <b>Initiator Group</b> field, type a name for the group.</li> <li>In the <b>Initiator</b> field, type an initiator name. A valid initiator name must start with <i>iqn.yyyy-mm.[reverse-domain-name]</i> or must be an EUI-64 identifier.</li> <li>Click <b>Add Initiator</b>.</li> <li>Repeat steps (c) and (d) to add additional initiators to the group.</li> <li>To provide CHAP authentication, select <b>CHAP Credentials</b> and provide the CHAP username and password. The credentials are used by the initiator to authenticate the target.</li> <li>Click <b>Next</b>.</li> </ol>

- (Optional) In the **Snapshot Schedules** screen, the default snapshot policy of the project is automatically selected. You can retain the default preset profile or customize the profile.
  - If you want to retain the default preset profile, click **Next**.
  - If you want to customize the profile, click **Override project snapshot policy**. Select a profile from the **Schedule** list and customize it according to your requirements. You can add more conditions by clicking the **Add** (+) icon.

For more information, see [Preset Profiles for Snapshots](#), [Custom Snapshot Schedules](#), and [Overriding a Project Snapshot Schedule](#).

- In the **Summary** screen, review the details and click **Create**.

## Creating an FC LUN

**Prerequisites:** You need a pool and a project available.

The Add LUN Creation wizard provides the option to **Inherit** or **Customize** project settings. Using the **Inherit** option, you can inherit LUN properties from the project and create a LUN quickly or customize the LUN according to your requirements.

To create an FC LUN, complete the following steps:

1. Click **Provision > Projects**.
  2. In the **Local** tab on the left pane, select the project from the **Projects** list.
  3. In the right pane, click the **LUNs** tab.
  4. In the **LUNs** tab, click **New**.  
The **New LUN** wizard appears.
  5. In the **Name and Space configuration** page, complete the following steps:
    - a) In the **Quantity** field, select **Single or Multiple**.  
Select **Multiple** to create multiple LUNs of the same type.
    - b) Type a LUN name in the **LUN Name** text box.  
If you select **Multiple**, include # with the LUN name.
    - c) If you select **Multiple**, enter the number of LUNs you want in the **Count** field, and specify where the count should start in the **Start** field.  
For example, if you have provided **LUN Name** as LUN\_Name, **Count** as 4, and **Start at** as 1, then four LUNs with the names, LUN\_Name\_1, LUN\_Name\_2, LUN\_Name\_3, and LUN\_Name\_4 are created.
    - d) Type or select **LUN Size**.
    - e) Select the storage unit.
    - f) (Optional) By default, the IntelliFlash OS creates a thin LUN. Clear **Thin Provisioning** if you do not want IntelliFlash to create a thin LUN.
    - g) Select the required purpose for the LUN from the **Purpose** list.
    - h) Select a block size from the **Block Size** list.
-  **Note:** Depending on the LUN purpose, the **Add LUN** wizard automatically selects the block size. You can retain the default size or choose a different size.
- i) Select **FC** from the **Protocol** list.
  - j) In the **Settings** section, select any of the following options:
    - Select **Inherit** if you want the LUN properties to be inherited from the project. After selecting this option, go to [Step 9](#).
    - Select **Customize** to customize the LUN properties. Click **Next**.
  6. In the **Select FC Target Group** screen, select from the default FC target groups and click **Next**.

 **Note:** For a fresh IntelliFlash installation or when you have migrated all the projects to ActiveOnly LUNs after upgrading, you can no longer create FC target groups. You can only select from the default virtual target groups.

- In the **Select or Create FC Initiator Group** screen, complete the following steps:

If...	Then...
<b>You want to select an existing initiator</b>	Complete the following steps: 1. Click <b>Choose Initiator group</b> . 2. Click <b>Initiator Group</b> and select an initiator group from the list. 3. Click <b>Next</b> .
<b>You want to create a new initiator group</b>	Complete the following steps: 1. Click <b>Create Initiator group</b> . 2. In the <b>Initiator Group</b> field, type a name. 3. From the <b>Ungrouped Initiators</b> list, select the required initiators. 4. Click <b>Next</b> .

- (Optional) In the **Snapshot Schedules** screen, the default snapshot policy of the project is automatically selected. You can retain the default preset profile or customize the profile.
  - If you want to retain the default preset profile, click **Next**.
  - If you want to customize the profile, click **Override project snapshot policy**. Select a profile from the **Schedule** list and customize it according to your requirements. You can add more conditions by clicking the **Add** (+) icon.

For more information, see [Preset Profiles for Snapshots](#), [Custom Snapshot Schedules](#), and [Overriding a Project Snapshot Schedule](#).

- In the **Summary** page, review the details and click **Create**.

## Deleting a LUN

You can delete any LUN type using the IntelliFlash Web UI.



**Caution:** Deleting a LUN deletes the dependent snapshots and cloned LUNs.

To delete a LUN, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab on the left pane, select the project from the **Projects** list.
3. In the right pane, click the **LUNs** tab.
4. In the LUNs tab, select the LUN you want to delete and click **Delete**.  
The **Delete LUN** confirmation dialog box appears. The **Delete LUN** confirmation dialog box displays the details about dependent snapshots and cloned LUNs.
5. In the **Delete** confirmation dialog box, enter the name of the LUN to be deleted.  
When deleting a LUN, IntelliFlash deletes the dependent snapshots and cloned LUNs.
6. If *Two-Factor Authentication (2FA)* is enabled for the user, enter the 2FA application code retrieved from your mobile device to delete the LUN.
7. Click **Delete**.

## Managing LUNs

---

After you create a LUN, you can manage the properties of the LUN. You can:

- Override project level configuration settings and set configurations specific to a LUN.
- Modify the LUN size, enable or disable Disk Write Back Cache, and enable or change the LUN protocol type.
- Perform multiple LUN management operations, including setting compression or deduplication at the LUN level.

To manage a LUN, select the LUN and click **Manage > Settings**, **Manage > Access**, and **Manage > Snapshots**.

The following sections provide in-depth information on managing a LUN.

### Expanding the size of a LUN

To expand the size of a LUN, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab on the left pane, select the project from the **Projects** list.
3. In the right pane, click the **LUNs** tab.
4. In the **LUNs** tab, select the LUN and click **Manage > Settings**.

The **LUN Settings** page appears.

5. In the **General** tab, modify the size in the **LUN size** field.
6. Select the storage unit.
7. Click **Save**.

## Modifying the Protocol of a LUN

 **Note:** Changing the protocol deletes the previous views associated with the protocol.

To modify the protocol type for a LUN, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab on the left pane, select the project from the **Projects** list.
3. In the right pane, click the **LUNs** tab.
4. In the **LUNs** tab, select the LUN and click **Manage > Settings**.  
The **LUN Settings** page appears.
5. In the **General** tab, enable the **Protocol** field.
6. In the **Information** dialog box, click **OK**.
7. Select **FC or iSCSI** from the dropdown list.
8. Click **Save**.

## Overriding Compression Type on a LUN

You can change the compression type depending on the data type that you want to store in shares and LUNs.

 **Note:** Compression is only applied on new and modified data. If you enable or disable compression after adding data to a LUN, compression is not applied to the existing data.

To override the data compression type set at the project level, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab on the left pane, select the project from the **Projects** list.
3. In the right pane, click the **LUNs** tab.
4. In the **LUNs** tab, select the LUN and click **Manage > Settings**.

The **LUN Settings** page appears.

5. Click the **Advanced** tab.
6. In the **Advanced** tab, click **Edit** in the **Inherited Settings** section.
7. In the **Edit Settings** dialog box, click **Enable Override** and then click **Compression**.
8. Click **Save**.  
The **Compression** text box appears in the **Override Settings** section.
9. In the **Advanced** tab, in the **Override Settings** section, select the compression type from the **Compression** list.
  - The compression types are **High Compression** and **Optimal Performance**. **Optimal Performance** is the default compression type.
  - If you do not want compression enabled, select **OFF**.
  - When you select the compression type, the corresponding compression algorithm appears below the **Compression** text box. The compression algorithm for Optimal Performance is lz4. The compression algorithm for High Compression is igzip.
  - For shares created in previous releases, the older compression types are renamed as **Legacy** and will continue to be supported.
10. Click **Save**.

## Overriding Deduplication on a LUN

When deduplication is enabled, it is only applicable on the new data. IntelliFlash does not run deduplication on the previous existing data in a LUN. Similarly, when deduplication is disabled, IntelliFlash does not undo the deduplication process on the previous data. It just stops checking for duplicate blocks on the new data.

To override the deduplication setting defined at the project level, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab on the left pane, select the project from the **Projects** list.
3. In the right pane, click the **LUNs** tab.
4. In the **LUNs** tab, select the LUN and click **Manage > Settings**.

The **LUN Settings** page appears.

5. Click the **Advanced** tab.
6. In the **Advanced** tab, click **Edit** in the **Inherited Settings** section.
7. In the **Edit Settings** dialog box, click **Enable Override** and then click **Deduplication**.
8. Click **Save**.
9. In the **Advanced** tab, in the **Override Settings** section, enable or disable **Deduplication**.
10. Click **Save**.

## Overriding Cache Behavior for a LUN

To override the cache behavior set at the project level for a LUN, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab on the left pane, select the project from the **Projects** list.
3. In the right pane, click the **LUNs** tab.
4. In the **LUNs** tab, select the LUN and click **Manage > Settings**.  
The **LUN Settings** page appears.
5. Click the **Advanced** tab.
6. In the **Advanced** tab, click **Edit** in the **Inherited Settings** section.
7. In the **Edit Settings** dialog box, click **Enable Override** and then click **Read Cache**.
8. Click **Save**.
9. In the **Advanced** tab, in the **Override Settings** section, enable or disable **Read Cache**.
10. Click **Save**.

## Overriding Read only Property for a LUN

To override the read only property set at the project level and to set it specific to a LUN, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab on the left pane, select the project from the **Projects** list.
3. In the right pane, click the **LUNs** tab.
4. In the **LUNs** tab, select the LUN and click **Manage > Settings**.

The **LUN Settings** page appears.

5. Click the **Advanced** tab.
6. In the **Advanced** tab, click **Edit** in the **Inherited Settings** section.
7. In the **Edit Settings** dialog box, click **Enable Override** and then click **Read only**.
8. Click **Save**.
9. In the **Advanced** tab, in the **Override Settings** section, enable or disable **Read only**.
10. Click **Save**.

## Setting a Management IP Address for a LUN

You can provide one of the floating IP addresses as a LUN management IP address in the LUN advanced properties. IDPS uses the LUN management IP address for taking snapshots.

To set a management IP address for a LUN, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab on the left pane, select the project from the **Projects** list.
3. In the right pane, click the **LUNs** tab.
4. In the **LUNs** tab, select the LUN and click **Manage > Settings**.  
The **LUN Settings** page appears.
5. Click the **Advanced** tab.
6. In the **Advanced** tab, enter the IP address in the **Management IP** field.
7. Click **Save**.

## Viewing the Purpose of a LUN

To view the purpose of a LUN, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab on the left pane, select the project from the **Projects** list.
3. In the right pane, click the **LUNs** tab.
4. In the **LUNs** tab, select the LUN and click **Manage > Settings**.  
The **LUN Settings** page appears.
5. In the **General** tab, view the purpose in the **Purpose** field.

## Adding LUN Mappings

A LUN mapping allows you to connect a specific LUN to specific initiators. You must use both target and initiator groups to manage the access to the LUN. A LUN mapping enables you to select the targets that can export the current LUN and the initiators that can see the LUN.

To map a LUN to a target group or initiator group, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab on the left pane, select the project from the **Projects** list.
3. In the right pane, click the **LUNs** tab.
4. In the **LUNs** tab, select the LUN and click **Manage > Access**.  
The **LUN Mappings** page appears.
5. In the **LUN Mappings** page, select the **Override project view map settings** option to manually add new mappings.
6. In the **Confirmation** dialog box, click **Yes**.
7. In the **LUN Mappings** page, click **Add**.  
The **Add Mapping** dialog box appears.
8. Select a new target group from the **Target Group** dropdown list.
9. Select any of the following options for the **Initiator Group** field:
  - Click **All** to select all the available initiator groups.
  - Click **Select** and then select one or more initiator groups from the dropdown list.
10. Select any of the following options for the **LUN#** field:
  - Select **Default** to use the assigned LUN number.
  - Select **Choose** and type or select a new number in the text box.
11. Enable **Read Only** to expose the LUN as read only.
12. Click **Add**.  
The new target group and the initiator groups are added to the mapping table.

## Modifying Space Usage Threshold Levels for a LUN

The default space usage threshold is defined in the **Settings > Notifications > Threshold** page.

You can now override the default threshold levels and set custom threshold levels for a specific LUN.

To set custom threshold levels for a LUN, do the following:

1. Click **Provision > Projects**.
2. Select the LUN and click **Manage > Settings**.  
The **LUN Settings** page appears.
3. In the **General** tab, in the **LUN Thresholds** section, click **Enable LUN Threshold**.  
Enabling this button overrides the default threshold levels.
4. Select new values for **Warning threshold** and **Critical threshold**.
5. Click **Save**.

When the LUN exceeds the space usage thresholds, the Web UI now indicates that the LUN is running out of space. Warning or Critical icon appears next to the LUN. When you mouse over the Warning or Critical icon, the Web UI displays the free space remaining. If you have not defined a quota for the LUN, you do not see the warnings.



---

# Chapter 10

---

## Create a copy of a Share or LUN

---

### Topics:

- [\*Share or LUN Copy in the Local IntelliFlash System\*](#)
- [\*Share or LUN Copy on a Remote IntelliFlash System\*](#)
- [\*Creating share or LUN copies\*](#)
- [\*Share or LUN copy failure scenarios\*](#)

The IntelliFlash Operating Environment provides a feature to create a copy of an existing share or LUN. You can create a copy of a share or LUN on the current array or on a remote array.

On both the current array or remote array, you can use the existing pool and project or a different pool and project. Or, you can create a new project to create a copy of a share or LUN.

When you create a copy of a share or LUN, the copy works as an independent share or LUN. The copy uses the same amount of storage space and also inherits most of the properties of the its original share or LUN.

A copy of a share inherits all of the original share's properties. Similarly, a copy of a LUN also inherits properties from the original LUN, except the LUN mapping details. Therefore, you must configure the LUN mappings after creating a copy of a LUN.

You can create multiple copies of a share or LUN at one time. The IntelliFlash Web UI appends a number to the share or LUN name to facilitate counting and identification.

Using the **Abort** option in the IntelliFlash Web UI, you can stop the copying operation before the operation is complete.



**Note:** When you create a copy of share or LUN, you should provide an appropriate name for the new project as well as the share or LUN copy for easy identification.

## Share or LUN Copy in the Local IntelliFlash System

---

When you create a copy of a share or LUN in the local IntelliFlash system, the IntelliFlash Web UI provides you the option to select a pool from the list of pools on the array.

You can use the existing project type to create a copy of a share or LUN. If you select the existing **Project Type** option, the dropdown list displays all projects in that pool using the same **Project Type**. You can select a required project to create a copy.

If you choose to create a new project type, the IntelliFlash Web UI by default creates the **Generic** project type. However, the copy inherits properties from the original share or LUN. If needed, you can change the project properties later.

## Share or LUN Copy on a Remote IntelliFlash System

---

When you create a copy of share or LUN in a remote IntelliFlash system, the IntelliFlash Web UI provides you the option to select a remote IntelliFlash system that are already configured as replication target arrays.

 **Note:** You must configure a replication relationship between your local (source) array and the remote (destination) array to create a copy of a share or LUN on the remote array.

If you choose to create a new project type, the by default creates the **Generic** project type. However, the copy inherits properties from the original share or LUN. If needed, you can change the project properties later.

## Creating share or LUN copies

---

### Prerequisites for Share or LUN copy creation

The following are prerequisites to create a share or LUN copy:

- To create a copy on the remote array, you must first configure the replication relationship between source and target (destination) array.
- The pool or project must have sufficient space to create a copy of a share or LUN.
- You must use a unique name when you create a copy of a share or LUN.
- You must use a unique name when you create a new project to create a copy of a share or LUN.
- In the DNS server, add entries of the hostnames of the Node-A, Node-B, and array management. This makes sure that the share or lun is copied when the array is accessed using hostname.

## Creating a copy of a share on the current array

To create a copy of a share on the current array, complete the following steps:

1. Click **Provision > Projects > Local**.
2. In the **Local** tab on the left pane, select the project from the **Projects** list.
3. In the right pane, click the **Shares** tab.
4. In the **Shares** tab, select a share and click **Copy > New Copy**.
5. In the **Destination** section of the **Copy <share name>** wizard, select **Current Array** and click **Next**.
6. In the **Configuration** section, choose a pool from the **Select Pool** dropdown list.
7. Select **Project Type: Existing or New**.
8. Complete the following step depending on the previous step selection.

If...	Then...
<b>If you have selected Existing:</b>	Choose a project from the <b>Select Project</b> dropdown list.
<b>If you have selected New:</b>	Provide a unique <b>Project Name</b> .

9. Type a unique **Share Name**.
10. Select number of **Copies**.  
Use this option when you need to create multiple copies of a share or LUN
11. Select **Start Count**.  
When creating two or more copies, choose the **Start Count** option. The count number is appended to the name of the copied share or LUN.
12. Click **Next**.
13. Review the copy operation summary and click **Copy**.



### Note:

- When the copy operation is in progress, the label **Copying** appears next to the share that is being copied.
- You can also view copy operation notifications in the **Notification** page.
- You can abort the copy operation while the operation is in progress (**Copy > Abort**).

## Creating a copy of a share on a remote array

### Prerequisite

- To create a copy on the remote array, you must first configure a replication relationship between the source and target (remote) array. If a replication relationship already exists, the Copy wizard displays the IP address for the remote array.
- The remote (destination) array must have a pool.

To create a copy of a share on a remote array, complete the following steps:

1. Click **Provision > Projects > Local**.
2. In the **Local** tab on the left pane, select the project from the **Projects** list.
3. In the right pane, click the **Shares** tab.
4. In the **Shares** tab, select a share and click **Copy > New Copy**.
5. In the **Destination** section of the **Copy <share name>** wizard, select **Remote Array** and click **Next**.
6. Choose the IP address of the remote array from the **Select Host** dropdown list.
7. Click **Next**.
8. In the **Configuration** section, choose a pool from the **Select Pool** dropdown list.
9. Select **Project Type: Existing or New**.
10. Complete the following step depending on the previous step selection.

If...	Then...
<b>If you have selected Existing:</b>	Choose a project from the <b>Select Project</b> dropdown list.
<b>If you have selected New:</b>	Provide a unique <b>Project Name</b> .

11. Type a unique **Share Name**.
12. Select number of **Copies**.  
Use this option when you need to create multiple copies of a share or LUN
13. Select **Start Count**.  
When creating two or more copies, choose the **Start Count** option. The count number is appended to the name of the copied share or LUN.
14. Click **Next**.
15. Review the copy operation summary and click **Copy**.

**Note:**

- When the copy operation is in progress, the label **Copying** appears next to the share that is being copied.
- You can also view copy operation notifications in the **Notification** page.
- You can abort the copy operation while the operation is in progress (**Copy > Abort**).

## Creating a copy of a LUN on the current array

After you create a copy of a LUN, you must configure the LUN mappings.



**Note:** When a copy of LUN is created, the signature of the LUN is also copied. Therefore, Microsoft Windows Server cannot mount the copy of the LUN that is added as a Cluster Shared Volume.

To create a copy of a LUN on the current array, complete the following steps:

- Click **Provision > Projects > Local**.
- In the **Local** tab on the left pane, select the project from the **Projects** list.
- In the right pane, select the **LUNS** tab.
- In the **LUNS** tab, select a LUN and click **Copy > New Copy**.
- In the **Destination** section of the **Copy <LUN name>** wizard, select **Current Array** and click **Next**.
- In the **Configuration** section, choose a pool from the **Select Pool** dropdown list.
- Select **Project Type: Existing or New**.
- Complete the following step depending on the previous step selection.

If...	Then...
<b>If you have selected Existing:</b>	Choose a project from the <b>Select Project</b> dropdown list.
<b>If you have selected New:</b>	Provide a unique <b>Project Name</b> .

- Type a unique **LUN Name**.
- Select the number of **Copies**.  
Use this option when you need to create multiple copies of a share or LUN
- Select **Start Count**.

When creating two or more copies, choose the **Start Count** option. The count number is appended to the name of the copied share or LUN.

12. Click **Next**.
13. Review the copy operation summary and click **Copy**.

 **Note:**

- When the copy operation is in progress, the label **Copying** appears next to the share that is being copied.
- You can also view copy operation notifications in the **Notification** page.
- You can abort the copy operation while the operation is in progress (**Copy > Abort**).

## Creating a copy of a LUN on a remote array

After you create a copy of a LUN, you must configure the LUN mappings.

 **Note:** When a copy of LUN is created, the signature of the LUN is also copied. Therefore, Microsoft Windows Server cannot mount the copy of the LUN that is added as a Cluster Shared Volume.

### Prerequisites:

- To create a copy on the remote array, you must first configure a replication relationship between the source and target (remote) array. If a replication relationship already exists, the Copy wizard displays the IP address for the remote array.
- The remote (destination) array must have a pool.

1. Click **Provision > Projects > Local**.
2. In the **Local** tab on the left pane, select the project from the **Projects** list.
3. In the right pane, select the **LUNS** tab.
4. In the **LUNS** tab, select a LUN and click **Copy > New Copy**.
5. In the **Destination** section of the **Copy <LUN name>** wizard, select **Remote Array** and click **Next**.
6. Select the IP address of the remote array from the **Select Host** dropdown list.
7. Click **Next**.
8. Choose the IP address of the remote array from the **Select Host** dropdown list.
9. Select **Project Type: Existing or New**.
10. Complete the following step depending on the previous step selection.

If...	Then...
If you have selected Existing:	Choose a project from the <b>Select Project</b> dropdown list.
If you have selected New:	Provide a unique <b>Project Name</b> .

11. In the **Configuration** section, choose a pool from the **Select Pool** dropdown list.
12. Type a unique **LUN Name**.
13. Select the number of **Copies**.  
Use this option when you need to create multiple copies of a share or LUN
14. Select **Start Count**.  
When creating two or more copies, choose the **Start Count** option. The count number is appended to the name of the copied share or LUN.
15. Click **Next**.
16. Review the copy operation summary and click **Copy**.



**Note:**

- When the copy operation is in progress, the label **Copying** appears next to the share that is being copied.
- You can also view copy operation notifications in the **Notification** page.
- You can abort the copy operation while the operation is in progress (**Copy > Abort**).

## Aborting a share or LUN copy operation

You can only abort an in-progress copy operation. When a share or LUN copy operation is in progress, the label **Copying** appears next to the share or LUN.

To abort an in-progress share or LUN copy operation, complete the following steps:

1. Click **Provision > Projects > Local**.
2. In the **Local** tab on the left pane, select the project from the **Projects** list.
3. In the right pane, click the **Shares** or **LUNS** tab.
4. In the **Shares** or **LUNS** tab, select a share or LUN with the **Copying** label and click **Copy > Abort**.

## Share or LUN copy failure scenarios

The share or LUN copy operation might fail in the following scenarios:

- If you provide an existing share, LUN, or project name to create a copy.
- If there is an issue with the replication configuration when creating a copy on the remote array.
- If there is not enough storage space on the destination project or remote array.
- If there are any errors in snapshots and share or LUN properties.
- If the source pool or destination pool moves to the peer controller as part of the HA failover or switchover process during the copy operation.

A multiple share or LUN copy creation operation might fail in the following scenario:

- If the source pool or destination(target) pool moves to the peer controller as part of the HA failover or switchover process while the first share or LUN copy creation is in progress.



**Note:** If the source pool fails over after the first copy operation is complete, there will be no impact on the copy operation. Similarly, the multiple share or LUN operation will resume if the target pool fails over after the first copy operation is complete.



**Note:** If the source pool and destination pool are the same, the copy operation will restart after the HA failover or switchover operation.

---

# Chapter 11

---

## Snapshots and Clones

---

**Topics:**

- *Understanding Snapshots and Clones*
- *Snapshots with Quiesce Option*
- *Project Level Snapshots*
- *Snapshot Schedule*
- *Understanding Snapshot Space Usage*
- *How IntelliFlash takes VMware Consistent Snapshots*
- *Snapshot Rollback*
- *Snapshot Deletion*
- *Best Practices for Configuring Snapshots*
- *Managing Snapshots*
- *Managing Clones*

## Understanding Snapshots and Clones

---

### Snapshots

IntelliFlash snapshots are point-in-time collection of references to the data blocks of a share or LUN.

IntelliFlash creates snapshots instantaneously. They virtually do not consume any disk space at creation time. Snapshots consume disk space when storing references for old data blocks and when the data in a share or LUN changes.

You can have an unlimited number of snapshots on an IntelliFlash Array. However, your storage array capacity and the rate of data changes can impose practical limits on the number of snapshots that you can take.

Snapshots help in restoring lost data to a certain point-in-time state, replicating data to another storage array, creating a clone of the data, and using the clone as a readable or writable copy.

Snapshots are created based on time. You can schedule snapshot creation on a minute, hourly, daily, weekly, or monthly basis, or you can take them manually.

IntelliFlash provides default snapshot schedule policies. These default snapshot policies enable you to schedule automatic snapshot creation. However, you can create custom snapshot schedules of your choice. IntelliFlash creates snapshots according to the custom snapshot schedules.

Integration of VMware APIs and Windows Volume Shadow Copy Service (VSS) with IntelliFlash enable you to take VM-consistent snapshots and application-consistent snapshots respectively. The VM-consistent and application-consistent snapshots are quiesced snapshots.

As snapshots are point-in-time references to the data blocks, deletion of snapshots is fast. However, it depends on the changes occurring in the data. Snapshots are auto-deleted according to the limit set on the number of snapshots to retain, or you can delete the snapshots manually.

### Related Topics

#### Clones

You can clone an IntelliFlash snapshot instantaneously and use it as a read, write storage object. The cloned snapshots are called *thin clones*. In IntelliFlash, *thin clones* initially share the same data blocks that are referred by a parent snapshot. Therefore, *thin clones* virtually do not occupy any disk space when cloning. However, they start consuming disk space when new data is written to them.

You can create *thin clones* using project, share, or LUN snapshots. IntelliFlash allows creating multiple clones from a single snapshot.

The cloned share or LUN name is prefixed with the letter "c." The mouse over text displays the parent share or LUN name.

You can use *thin clones* as a regular share or LUN. When you clone a snapshot of a share or LUN, IntelliFlash provides an option to mount a share clone and provides a LUN ID for a LUN clone.

Using IntelliFlash, you can create share clones as read-only copies and allow them to inherit parent share properties. LUN clones can inherit mapping details from a project, LUN, or new mapping.

 **Note:** As thin clones refer to the same data blocks that are being referred to by snapshots, IntelliFlash does not automatically delete the snapshots associated with clones.

You can use thin clones for different purposes. You can use IntelliFlash thin clones to:

- Restore data deleted by users accidentally.
- Carry out back up and restore processes.
- Create read-only copies for testing purposes.
- Create multiple virtual machines with the same configuration.

## Snapshots with Quiesce Option

---

Quiescing is a process of moving a system to a stable state by flushing the outstanding (cached) I/Os from the system memory to disks to create consistent usable snapshots.

IntelliFlash can create quiesced snapshots of VMware Servers and Windows Servers. To create quiesced snapshots, IntelliFlash provides default snapshot schedule policies with an option to select **Quiesce On** or **Off** when creating a custom schedule, and when creating a manual snapshot.

 **Note:** To take quiesced snapshots on a share or LUN, the share or LUN must have a virtual machine created in it and VMware Tools is installed on the virtual machine.

 **Note:** Add the VMware and Windows Servers to the IntelliFlash Array in the **Settings > App-Aware > VMware Servers or Windows Servers** page.

### Difference between quiesce and non-quiesce

When the **Quiesce** option is **On** while creating a snapshot, IntelliFlash checks whether the VMware Server or Windows Server is using the share or LUN.

If IntelliFlash discovers that the VMware Server is using the share or LUN, it requests the VMware Server to take VMware quiesced snapshots.

If IntelliFlash discovers that the Windows Server is using the share or LUN, it requests IDPS installed on the Windows Server to take snapshots.



**Note:** Creating snapshots with the **Quiesce** option *On* requires more time. The extra time is because of the data size and time to quiesce data in a Share or LUN on a VMware Server or Windows Server. Therefore, you must consider this point and plan the snapshot schedules, accordingly.

When the **Quiesce** option is **Off**, IntelliFlash creates the standard IntelliFlash snapshots instantaneously.

## Project Level Snapshots

---

Using project level snapshots, you can restore all shares and LUNs inside a project with a consistent data image in a single step. The project is acting as a Consistency Group in this case.

You can also clone project snapshots for creating copies of shares and LUNs with a consistent data image.

## Snapshot Schedule

---

A snapshot schedule is a set of snapshot frequencies.

A snapshot schedule consists of a predefined time for taking snapshots and a maximum number of snapshots to be retained.

A snapshot schedule enables you to schedule snapshot creation automatically. To schedule snapshot creation, IntelliFlash provides you with two scheduling options: the default preset profiles and an option to create a custom snapshot schedule.

## Preset Profiles for Snapshots

IntelliFlash provides the default preset profiles for taking snapshots as per the schedule. The default snapshot preset profiles provided in IntelliFlash removes the overhead of manual planning for snapshot schedules.

You can select the default preset profiles when creating a project, share, or LUN. Select a profile depending on the criticality of your data. Snapshots are automatically created according to the selected snapshot profile.



**Note:** The project, share, and LUN creation wizards automatically select optimal default preset profile depending on the project template, share and LUN type.

A default snapshot preset profile selected for a Project is applicable to all of the contents of that particular Project. However, you can select a different Project snapshot profile for a project

and override the default snapshot profile when creating a Share or LUN. You can also create a custom snapshot schedule.

A default snapshot preset profile consists of non-overlapping rules and a predefined maximum number of snapshots to be retained. They are available with and without the quiesce option.

The following are the default snapshot preset profiles:

- **Weekdays-Monthly**
- **Weekdays-Monthly+Quiesce**
- **Daily-Weekly**
- **Daily-Weekly+ Quiesce**
- **Hourly-Daily-Weekly**
- **Hourly-Daily-Weekly+Quiesce**
- **30minutes-Daily-Weekly**
- **30minutes-Daily-Weekly +Quiesce**

 **Note:** You can select the option **Custom Profile** if you do not want to use the default preset profiles.

 **Note:** In the following explanation, details are provided for the policies without the quiesce option. However, the same snapshot rules are applicable for policies with quiesce option as well.

### **Weekdays-Monthly**

The **Weekdays-Monthly** policy type has Monday through Friday frequencies. IntelliFlash creates snapshots as per the following rules:

- Monday through Friday at 20:15 and retains the snapshots for a month.
- Last day of every month at 20:30 and retains the snapshots for a year.

### **Hourly-Daily-Weekly**

The **Hourly-Daily-Weekly** policy type has hourly, daily, and weekly snapshot rules. IntelliFlash creates snapshots as per the following rules:

- Every hour from 00:00 to 23:59 and retains a maximum one day hourly snapshots.
- Every day at 22:15 hours and retains a maximum of four weeks snapshots.
- Every week on Sunday at 22:30 hours and retains a maximum six months snapshots.

### **Daily-Weekly**

The **Daily-Weekly** policy type has daily and weekly snapshot rules. IntelliFlash creates snapshots as per the following rules:

- Every day at 21:15 hours and retains a maximum number four weeks snapshots.
- Every week on Sunday at 21:30 hours and retains a maximum six months snapshots.

### 30minutes-Daily-Weekly

The **30minutes-Daily-Weekly** policy type has minute, daily, and weekly snapshot rules.

IntelliFlash creates snapshots as per the following rules:

- Every 30 minutes from the time of scheduling and retains a maximum snapshots taken in one hour.
- Every day at 23:15 hours and retains a maximum four weeks snapshots.
- Every week on Sunday at 23:45 hours and retains a maximum six months snapshots.

### Custom Snapshot Schedules

IntelliFlash enables you to create custom snapshot schedules. Custom snapshot schedules provide the flexibility to define frequencies snapshots schedule according to your requirements. You can create custom snapshot schedules for a project, share, or LUN.

You can create a custom snapshot schedule (Preset profiles) with the time intervals of minute, hourly, daily, weekly, and monthly. According to your snapshot rule, IntelliFlash creates the snapshots automatically.

To take quiesced snapshots, select the **Quiesce** option **On** when creating a project, share or LUN for VMware Servers or Windows Servers. When you create a custom snapshot schedule for a project, the snapshot rule applies to all the contents of that particular project.

 **Note:** When creating a new custom snapshot schedule with **Quiesce** option **On**, try to create schedules that are not overlapping with other snapshot schedules.

If you want to create a custom schedule specific to a share or LUN, you must override the project snapshot schedule settings.

### Overriding a Project Snapshot Schedule

IntelliFlash provides an option to override the project snapshot schedule for a share or LUN. You can use this override project schedule option to exclude a Share or LUN from creating snapshots using the snapshot schedule of a Project or if you want to create a custom schedule for a particular share or LUN.

You can enable or disable the **Override project snapshot schedule setting** option from the Share or LUNs tab.

If you enable the **Override project snapshot schedule settings** by selecting the option, the regular Project snapshot schedule excludes that particular share or LUN from creating snapshots.

If you enable the **Override project snapshot schedule settings** by selecting the option and add a custom snapshot schedule specific to that particular share or LUN, IntelliFlash takes the snapshots according to the custom snapshot schedule, overriding the project snapshot schedule.

Disabling the **Override project snapshot schedule settings** by clearing the option restores the project snapshot schedule and deletes the custom snapshot schedule rule. However, the snapshots associated with the frequency remain in the storage array. You might need to delete these snapshots manually.

## Understanding Snapshot Space Usage

---

IntelliFlash snapshot creation does not occupy any disk space; it refers to the data blocks of a share or LUN at a point in time. Therefore, the logical size of a snapshot is the total size of the data blocks to which a snapshot is referring.

### For example:

When you create a snapshot of a 10 MiB share, the snapshot of the share refers to the 10 MiB of data blocks of that share. So you can state that the logical size of the snapshot is 10 MiB.

A snapshot starts consuming disk space when the data blocks within a Share or LUN change (overwritten). When the snapshot needs to store the references for the old (changed) data blocks, the snapshot size starts growing. The space used for keeping references of the old (changed) data blocks is the actual snapshot used space.

A snapshot size might also grow if you delete previous snapshots, as the existing snapshot also stores the references of the deleted snapshots. In any circumstance, a snapshot used space cannot exceed the logical size of the snapshot.

## How IntelliFlash takes VMware Consistent Snapshots

---

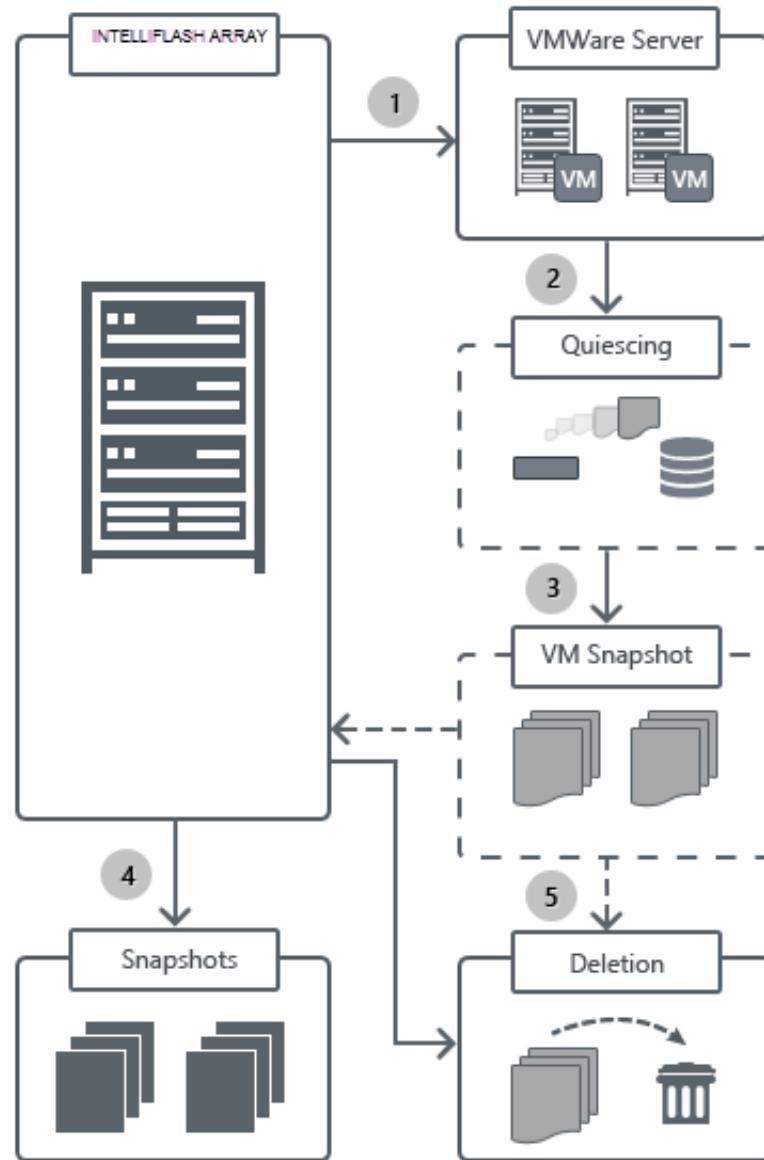
You can take VM-consistent snapshots by using IntelliFlash when you need to take snapshots of all virtual machines within a share or LUN.

 **Note:** If you want to take a snapshot of a single VM, you must use VMware vSphere client and take VMware-specific snapshots

IntelliFlash communicates with the VMware server by using the VMware APIs. When IntelliFlash receives a request to take snapshots, it takes VM-consistent snapshot in the following manner:

1. IntelliFlash verifies whether the VMware server is using the share or LUN.
2. If the VMware Server uses the share or LUN, then IntelliFlash requests that the VMware server quiesce all virtual machines.
3. The VMware server takes VMware-specific temporary snapshots of the virtual machines within that share or LUN.
4. Once it takes the VMware-specific snapshots, IntelliFlash starts taking snapshots of the share or LUN on the IntelliFlash Array.
5. After it creates snapshots on the IntelliFlash Array, IntelliFlash requests the VMware server to delete the VMware-specific temporary snapshots that were created earlier.

The following illustration shows how IntelliFlash takes VM-consistent snapshots.



## Snapshot Rollback

Snapshot rollback is a process for reverting the state of a share or LUN back to a point-in-time state when the snapshot was taken.

You can rollback using snapshots of a project, share, or LUN. When you rollback using a project snapshot, all shares and LUNs inside the project are rolled back in a single step.

There might be instances where data is lost due to an accidental deletion, virus attack, or other reasons. The rollback option enables you to restore the lost data.



**Note:** You should roll back to the latest available snapshot in order to restore the maximum amount of lost data.

If you lose a small portion of data, such as a few files or folders, consider cloning a snapshot to restore the lost data instead of a snapshot rollback.



**Caution:** Use the rollback process only when you are absolutely sure you must return the share or LUN to an earlier point-in-time state. You cannot undo the rollback process. Rolling back to a particular state of a share or LUN by using a snapshot might result in permanent loss of the data changes that happened between rollback time and snapshot creation time.

#### For example:

You want to roll back to a snapshot because you accidentally deleted a large amount of data at 9:30 a.m. from one of your shares. You know that you have an hourly snapshot schedule for that share. According to the schedule, IntelliFlash took a snapshot of the share at 9:00 a.m. To restore the lost data, you roll back to this latest snapshot at 10:00 a.m. However, after the rollback, the changes that happened in the data after snapshot creation (after 9:00 a.m.) and before the roll back time (10:00 a.m.) are permanently lost, and the state of the data is exactly the same as it was at the time of snapshot creation, at 9:00 a.m.



**Caution:** If you select an older snapshot for rollback purposes, the snapshots created later than the selected snapshot and all dependent clones are permanently deleted.

## Snapshot Deletion

IntelliFlash deletes snapshots using two different methods—automatic deletion and manual deletion. The space achieved after snapshots deletion is added back to the storage pool.

The auto deletion mechanism monitors the maximum number of snapshots to save and deletes them after exceeding the limit according to the defined snapshot rule. As part of auto deletion, IntelliFlash deletes the oldest snapshot first in the snapshot list.

#### For example:

If you have created a snapshot rule that retains a maximum number of 20 hourly snapshots, then IntelliFlash retains the 20 hourly snapshots until it creates the newest hourly snapshot. Once it creates the newest hourly snapshot, it deletes the oldest hourly snapshot in the list automatically.

In the above example, when IntelliFlash creates the 21<sup>st</sup> hourly snapshot, IntelliFlash deletes the first hourly snapshot. When IntelliFlash creates the 22<sup>nd</sup> hourly snapshot, it deletes the second hourly snapshot in the list. This automatic deletion process continues while the rule exists.



**Note:** All manually created snapshots remain in the storage array until you delete them manually.

When you delete a snapshot, IntelliFlash Operating Environment deletes the dependent cloned datasets (Shares and LUNs) as well. The IntelliFlash Web UI prompts you to enter DELETE to complete the snapshot delete operation.

## Best Practices for Configuring Snapshots

---

The following list describes the recommended best practices for configuring snapshots.

1. Separate the management network from the data path.
2. Configure a snapshot schedule at the project level, which serves as a volume consistency group. This ensures that the snapshots are created at the same time with an consistent data image.
3. Only include the relevant LUNs within a project, and limit the number of LUNs, as well. Too many LUNs in a project may cause the quiesce process to take too long, which could cause snapshot creation to fail.
4. Limit the number of applications running on the same LUN. If too many applications are running, the application quiesce may take a long time to complete, which could cause snapshot creation to fail.
5. In a virtual environment, separate the Virtual Machine OS image and applications (for example, Microsoft Exchange and Microsoft SQL Server) on different LUNs, as the virtual machine quiesce may take a long time to complete, which again could cause snapshot creation to fail.
6. In a virtual environment, separate the LUNs for different applications in different projects. For example, the LUNs for VM OS images should be in one project, Exchange Server LUNs should be in another project.
7. In a virtual environment, when using Hyper-V CSV LUNs, limit the number of VMs running on each LUN.
8. Run scheduled snapshots for Microsoft cluster nodes for Exchange DAG and Hyper-V at different times to avoid conflicts.
9. When using Hyper-v CSV LUNs, limit the number of VMs running from each LUN.
10. Run scheduled snapshots on Microsoft cluster nodes for Exchange DAG and Hyper-V at different times to avoid conflicts.

## Managing Snapshots

---

Snapshots management is easy when using IntelliFlash Web UI. It enables you to perform various snapshot management tasks. Snapshots can be managed collectively for all shares and LUNs in a project and individually.

### Adding a Manual Snapshot of a Project

A manual snapshot is a snapshot created by you instantly without using any snapshot rule. You can create a manual snapshot of a project, share, or LUN.

When you create a manual snapshot of a project, IntelliFlash creates snapshots of all of the shares and LUNs belonging to that project and a project snapshot. You can view the project snapshots list in the **Snapshots** tab of the **Data Protection** page. You can create a manual snapshot whenever you need it. A manual snapshot name can have alphanumeric characters without spaces. The word **Manual Project Snapshot** is prefixed to all manual snapshot names.

To add a manual snapshot of a project, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab, select the required project.
3. Click **Manage > Data Protection**.
4. In the **Snapshots** tab of the **Data Protection** page, click the **New Snapshot** button.
5. In the **Create new Snapshot** window, type the **Snapshot Name**.

 **Note:** A manual snapshot name should be without spaces. It cannot have special characters. However, you can use an underscore (\_) and a dash (-).

6. (Optional) Enable the **Quiesce** option.
7. Click **Create**.

IntelliFlash creates a manual snapshot of all the shares and LUNs for the selected project.

## Adding a Custom Snapshot Schedule for a Project

Custom snapshot schedules provide the flexibility to define the snapshot rules.

The IntelliFlash OS enables you to create a custom schedule with a quiesce option.

To create a custom schedule for a project, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab, select the required project.
3. Click **Manage > Data Protection**.
4. In the **Snapshots** tab of the **Data Protection** page, click the **Manage Schedules** button.
5. In the **Manage Schedules** window, you can follow one of the following procedures:

If you select this...	Do this...
A Preset Profiles snapshot schedules from the dropdown menu.	Go to <a href="#">this step</a> .

If you select this...	Do this...
<b>Select a default snapshot schedules from the dropdown menu and edit it to make it a custom snapshot schedule.</b>	Go to <a href="#">this step</a> .
<b>Click the plus icon  to add a snapshot schedule frequency.</b>	Go to <a href="#">this step</a> .

 **Note:** If you make any modifications to the selected default snapshot schedule, the default snapshot schedule turns to a **Custom** snapshot schedule.

6. Select **Frequency** from dropdown list.
7. Type duration next to the **every** field.  
For example, every 1 month, every 2 hours, every 30 minutes, and so on.
8. Click the time schedule link for modifying the **Frequency Options**.

 **Note:** The schedule **Options** differ depending on the **Frequency** type.

 **Note:** In the **Options** screen for the frequency, you can set time, date, and day for taking snapshots. You can also enable or disable the **Quiesce** option for the frequency.

9. Type snapshot retention duration in the text box under **Retain for** field.  
IntelliFlash automatically calculates the number of snapshots to retain and displays under the **Snapshots** field.
-  **Note:** Modification of any field other than **Retain for** resets the **start on** date to the date of modification.
10. If [Two-Factor Authentication \(2FA\)](#) is enabled for the user, enter the 2FA application code retrieved from your mobile device to create a custom schedule for a project.
11. Click **Save**.

## Related Topics

[Custom Snapshot Schedules](#)

[Snapshots with Quiesce Option](#)

## Deleting a Frequency of a Project Snapshot Schedule

Delete a frequency of a snapshot schedule when you want IntelliFlash to stop taking auto-snapshots for all shares and LUNs that belong to that project.

After you delete a snapshot frequency, the latest auto-snapshots taken as part of the rule remain in the storage array. You need to delete these snapshots manually.

To delete a project snapshot schedule rule, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab, select the required project.
3. Click **Manage > Data Protection**.
4. In the **Snapshots** tab of the **Data Protection** page, click the **Manage Schedules** button.
5. In the **Manage Schedules** window, click  next to the required snapshot frequency.
6. Click **Save**.

The snapshot frequency disappears from the **Frequency** section. IntelliFlash does not take any snapshots with this rule in the future.

## Viewing Snapshots Schedule in the Timeline

You can view the frequencies of a snapshot schedule in the **Timeline** section of the **Manage Schedules** window for planning snapshot schedules and clarity.

1. Click **Provision > Projects**.
2. In the **Local** tab, select the required project.
3. Click **Manage > Data Protection**.
4. In the **Snapshots** tab of the **Data Protection** page, click the **Manage Schedules** button.
5. In the **Manage Schedules** window, click  in the **Timeline** section.
6. In the **Timeline** section, click and drag the button on the timeline bar.

You can view snapshots frequency from 1 day to 60 days. The X-axis of the Timeline chart displays the frequencies and Y-axis displays the calendar month names.



## Viewing Details of a Project Snapshot

You can view details of a snapshot from the **Graph view** tab of the **Data Protection** page.

To view a project snapshot details, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab, select the required project.
3. Click **Manage > Data Protection**.
4. In the **Snapshots** tab of the **Data Protection** page, click **Graph view**.
5. Select a snapshot frequency in the graph.  
The table below the graph displays the list of snapshots in the selected frequency.
6. In the snapshots table below the graph, select a snapshot from the list to view the details of a snapshot.  
The **Details** section displays the **Project Name**, **Schedule** of the snapshot, snapshot **Creation Time**, **Quiesced**, **Used Space**, and **Logical Size**.

## **Viewing Details of a LUN Snapshot**

You can view details of a LUN snapshot from the **Graph view** tab of the **LUN Snapshots** page.

To view the details of a LUN snapshot, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab, select the required project.
3. In the right pane, click the **LUNs** tab.
4. In the **LUNs** tab, select the required LUN and click **Manage > Snapshots**.  
The **LUN Snapshots** page appears.
5. In the **LUN Snapshots** page, click **Graph view**.
6. Select a snapshot frequency in the graph.  
The table below the graph displays the list of snapshots in the selected frequency.
7. In the snapshots table below the graph, select a snapshot from the list to view the details of the snapshot.  
The **Details** section displays the following details of the LUN:
  - **LUN GUID**
  - **Schedule**
  - **Creation Time**
  - Whether the LUN is **Quiesced**
  - **Used Space**
  - **Logical Size**

## Viewing Details of a Share Snapshot

You can view details of a share snapshot from the **Graph view** tab of the **Share Snapshots** page.

To view the details of a share snapshot, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab, select the required project.
3. In the right pane, click the **Shares** tab.
4. In the **Shares** tab, select the required share and click **Manage > Snapshots**.  
The **Share Snapshots** page appears.
5. In the **Share Snapshots** page, click **Graph view**.
6. Select a snapshot frequency in the graph.  
The table below the graph displays the list of snapshots in the selected frequency.
7. In the snapshots table below the graph, select a snapshot from the list to view the details of the snapshot.

The **Details** section displays the following details of the share:

- **Share Name**
- **Schedule**
- **Creation Time**
- Whether the share is **Quiesced**
- **Used Space**
- **Logical Size**

## Deleting a Project Snapshot from the Graph view

You can delete snapshots at the project level. The IntelliFlash Web UI allows you to delete from the **Graph view** and **Table view**.

 **Note:** Deleting a project snapshot deletes all depended shares, LUNs, and snapshots inside the project. You can delete an individual project snapshot or all snapshots.

To delete a project snapshot, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab, select the required project.
3. Click **Manage > Data Protection**.
4. In the **Snapshots** tab of the **Data Protection** page, click **Graph view**.
5. Select a snapshot frequency in the graph.

The table below the graph displays the list of snapshots in the selected frequency.

6. You can select required snapshots for deletion or delete all snapshots in the selected frequency.
  - Select a snapshot or multiple snapshots and click **Delete**.
  - Click the **Delete** dropdown and select **Delete All**.
7. In the **Delete Snapshot** window, type the word **DELETE**.  
The **Delete Snapshot** window displays the total number snapshots selected for deletion and its dependents.
8. If *Two-Factor Authentication (2FA)* is enabled for the user, enter the 2FA application code retrieved from your mobile device to delete the project snapshot.
9. Click **Delete**.

## Deleting a Project Snapshot from the Table View

You can delete snapshots at the project level. The IntelliFlash Web UI allows you to delete from the **Graph view** and **Table view**.

 **Note:** Deleting a project snapshot deletes all depended shares, LUNs, and snapshots inside the project. You can delete an individual project snapshot or all snapshots.

To delete a project snapshot, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab, select the required project.
3. Click **Manage > Data Protection**.
4. In the **Snapshots** tab of the **Data Protection** page, click **Table view**.
5. In the snapshots table, you can select required snapshots for deletion or delete all snapshots in the selected frequency.
  - Select a snapshot or multiple snapshots and click **Delete**.
  - Click the **Delete** dropdown and select **Delete All**.
6. In the **Delete Snapshot** window, type the word **DELETE**.
7. If *Two-Factor Authentication (2FA)* is enabled for the user, enter the 2FA application code retrieved from your mobile device to delete the project snapshot.
8. Click **Delete**.

## Adding Custom Snapshots Schedule for a Share

The IntelliFlash OS provides an option to override the project snapshot schedule and create a specific snapshot schedule for a share with quiesce option.

You can create a custom snapshot schedule for a share.

To add a custom snapshots schedule for a share, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab, select the required project.
3. Click the **Shares** tab and select a required share.
4. Click **Manage > Snapshots**.

You can click the **Back** button in the Data Protection to go back to the previous page.

5. In the **Snapshots** tab of the **Share Snapshots** page, click the **Manage Schedules** button.
6. Enable **Override project snapshot schedule settings**.

7. In the **Manage Schedules** window, you can follow one of the following procedures:

If you select this...	Do this...
<b>Select a default snapshot schedules from the dropdown menu.</b>	Go to <a href="#">this step</a> .
<b>Select a default snapshot schedules from the dropdown menu and edit it to make it a custom snapshot schedule.</b>	Go to <a href="#">this step</a> .
<b>Click the plus icon  to add a snapshot schedule frequency.</b>	Go to <a href="#">this step</a> .

 **Note:** If you make any modifications to the selected default snapshot schedule, the default snapshot schedule turns to a **Custom** snapshot schedule.

8. Select **Frequency** from dropdown list.
9. Type duration next to the **every** field.  
For example, every 1 month, every 2 hours, every 30 minutes, and so on.
10. Click the time schedule link for modifying the **Frequency Options**.

 **Note:** The schedule **Options** differ depending on the **Frequency** type.

 **Note:** In the **Options** screen for the frequency, you can set time, date, and day for taking snapshots. You can also enable or disable the **Quiesce** option for the frequency.

11. Type snapshot retention duration in the text box under **Retain for** field. IntelliFlash automatically calculates the number of snapshots to retain and displays under the **Snapshots** field.
12. Click **Save**

## Adding a Manual Snapshot of a Share

You can create a manual snapshot of a share when you do not want to wait for the snapshot schedule to take snapshots, or whenever there is a need for a snapshot immediately. The manual snapshots remain in the storage array until you delete them.

You can take quiesced or non-quiesced manual snapshots.

To create a manual snapshot of a share, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab, select the required project.
3. Click the **Shares** tab and select a required share.
4. Click **Manage > Snapshots**.  
You can click the **Back** button in the Data Protection to go back to the previous page.
5. Click **New Snapshot**.
6. In the **Create** window, type the **Snapshot Name**.

 **Note:** A manual snapshot name should be without spaces. It cannot have special characters. However, you can use an underscore (\_) and a dash (-).

7. (Optional) Enable the **Quiesce** option.
8. Click **Create**.  
The **Information** window opens and displays the message.

## Adding Custom Snapshots Schedule for a LUN

You can add a custom snapshot schedule for a LUN. The IntelliFlash OS provides an option to override the project snapshot schedule and create a specific snapshot schedule for the LUN.

You can create a custom schedule with a quiesce option.

To add a custom snapshots schedule for a LUN, complete the following steps:

1. Click **Provision > Projects**.

2. In the **Local** tab, select the required project.

3. Click **LUNS** tab and select a required LUN.

4. Click **Manage > Snapshots**.

You can click the **Back** button in the Data Protection to go back to the previous page.

5. In the **LUN Snapshots** page, click the **Manage Schedules** button.

6. In the **Manage Schedules** window, you can follow one of the following procedures:

If you select this...	Do this...
Select a default snapshot schedules from the dropdown menu.	Go to <a href="#">this step</a> .
Select a default snapshot schedules from the dropdown menu and edit it to make it a custom snapshot schedule.	Go to <a href="#">this step</a> .
Click the plus icon  to add a snapshot schedule frequency.	Go to <a href="#">this step</a> .

7. Select **Frequency** from dropdown list.

8. Type duration next to the **every** field.

For example, every 1 month, every 2 hours, every 30 minutes, and so on.

9. Click the time schedule link for modifying the **Frequency Options**.



**Note:** The schedule **Options** differ depending on the **Frequency** type.



**Note:** In the **Options** screen for the frequency, you can set time, date, and day for taking snapshots. You can also enable or disable the **Quiesce** option for the frequency.

10. Type snapshot retention duration in the text box under **Retain for** field.

IntelliFlash automatically calculates the number of snapshots to retain and displays under the **Snapshots** field.

11. Click **Save**.

## Adding a Manual Snapshot of a LUN

You can create a manual snapshot of a LUN when you need one immediately. The manual snapshots remain in the storage array until you delete them.

To add a manual snapshot of a LUN, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab, select the required project.
3. Click **LUNS** tab and select a required LUN.
4. Click **Manage > Snapshots**.

You can click the **Back** button in the Data Protection to go back to the previous page.

5. In the **LUN Snapshots** page, click the **New Snapshot** button.
6. In the **Create new Snapshot** window, type the **Snapshot Name**.
7. (Optional ) Enable the **Quiesce** option.

8. Click **Create**.

The **Information** window opens and displays the message.

In the **Snapshots** tabbed page, you can see the newly created manual snapshot.

## Refreshing Snapshots List

Refreshing the snapshots list enables you to see the latest snapshots of Shares and LUNs from their respective snapshots listing page.

To refresh the snapshots list, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab, select the required project.
3. Click **Manage > Data Protection**.
4. In the **Snapshots** tab of the **Data Protection** page, click **Graph view** or **Table view**.
5. In the **Graph view** or **Table view**, click **Refresh List**.

## Deleting a Frequency of a Snapshot Schedule for a Share or LUN

Delete a snapshot schedule frequency when you want IntelliFlash to stop taking auto-snapshots for a share or LUN.

After you delete a snapshot frequency, the latest auto-snapshots taken as part of the rule remain in the storage array. You must delete them manually.

To delete a share or LUN snapshot schedule frequency, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab, select the required project.
3. Click **LUNS or Shares** tab.
4. In the **LUNS or Shares** tab, click **Manage > Snapshots**.
5. In the **LUN Snapshots** or **Share Snapshots** page, click **Manage Schedules**.
6. In the **Manage Schedules** window, click  to delete a frequency.
7. Click **Save**.

The frequency of a snapshot schedule disappears from the snapshot **Frequency** section, and takes no snapshots with this rule in the future.

### **Deleting LUN or Share Snapshots Manually from the Graph View**

You can delete unwanted snapshots manually from the storage system and regain the storage space.

To delete the unwanted snapshots, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab, select the required project.
3. Click **LUNS or Shares** tab.
4. In the **LUNS or Shares** tab, click **Manage > Snapshots**.
5. In the **LUN Snapshots** or **Shares Snapshots** page, click **Graph view**.
6. Select a snapshot frequency in the graph.  
The table below the graph displays the list of snapshots in the selected frequency.
7. You can select required snapshots for deletion or delete all snapshots in the selected frequency.
  - Select a snapshot or multiple snapshots and click **Delete**.
  - Click the **Delete** dropdown and select **Delete All**.
8. In the **Delete Snapshot** window, type the word **DELETE**.  
The **Delete Snapshot** window displays the total number snapshots selected for deletion and its dependents.
9. If [Two-Factor Authentication \(2FA\)](#) is enabled for the user, enter the 2FA application code retrieved from your mobile device to delete the unwanted snapshots.
10. Click **Delete**.

The deleted snapshot disappears from the snapshots list.

### Related Topics

[Snapshot Deletion](#)

## Deleting LUN or Share Snapshots Manually from the Table View

You can delete unwanted snapshots manually from the storage system and regain the storage space.

To delete the unwanted snapshots, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab, select the required project.
3. Click **LUNS** or **Shares** tab.
4. In the **LUNS** or **Shares** tab, click **Manage > Snapshots**.
5. In the **LUN Snapshots** or **Shares Snapshots** page, click **Table view**.
6. In the snapshots table, you can select required snapshots for deletion or delete all snapshots in the selected frequency.
  - Select a snapshot or multiple snapshots and click **Delete**.
  - Click the **Delete** dropdown and select **Delete All**.
7. In the **Delete Snapshot** window, type the word **DELETE**.

The **Delete Snapshot** window displays the total number snapshots selected for deletion and its dependents.

8. If [Two-Factor Authentication \(2FA\)](#) is enabled for the user, enter the 2FA application code retrieved from your mobile device to delete the unwanted snapshots.
9. Click **Delete**.

The deleted snapshot disappears from the snapshots list.

## Rolling Back to a Project Snapshot

Rollback is a process that reverts the state of a share back to a point-in-time state when the snapshot was taken.



**Caution:** The rollback process results in permanent data loss. You might permanently lose the data changes that happened between rollback time and snapshot creation time.

To roll back to a snapshot of a project, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab, select the required project.
3. In the **Snapshots** tab of the **Data Protection** page you can perform one of the following choices:
  - Click **Graph view** and select a snapshot frequency in the graph. The table below the graph displays the list of snapshots in the selected frequency.
  - Click **Table view** and select a snapshot frequency in the table.
4. Select a snapshot from the table.
5. Click the **Rollback** button.

 **Note:** Before you perform a rollback operation on a snapshot, you must ensure that no IO operations are running on shares or LUNs in the project.

6. In the **Confirmation** screen, click **Yes**.
7. In the **Rollback Snapshot** window, type the snapshot name to roll back.
8. Click **Rollback**.
9. In the **Information** screen, click **OK**.

The project state reverts to the point-in-time state when the snapshot was taken.

## Rolling Back to a Share Snapshot

Rollback is a process that reverts the state of a share back to a point-in-time state when the snapshot was taken.



**Caution:** The rollback process results in permanent data loss. You might permanently lose the data changes that happened between rollback time and snapshot creation time.



**Note:** Roll back to the latest available snapshot in order to restore the maximum amount of lost data.

To roll back to a snapshot of a share, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab, select the required project.
3. Click the **Shares** tab and select a required share.
4. In the **Shares** tab, click **Manage > Snapshots**.
5. In the **Share Snapshots** page you can perform one of the following choices:

- Click **Graph view** and select a snapshot frequency in the graph. The table below the graph displays the list of snapshots in the selected frequency.
  - Click **Table view** and select a snapshot frequency in the table.
6. Select a snapshot from the table.
  7. Click the **Rollback** button.
-  **Note:** Before you perform a rollback operation on a snapshot, you must ensure that no IO operations are running on shares or LUNs in the project.
8. In the **Confirmation** screen, click **Yes**.
  9. In the **Rollback Snapshot** window, type the snapshot name to roll back.
  10. Click **Rollback**.
  11. In the **Information** screen, click **OK**.

The share state reverts to the point-in-time state when the snapshot was taken.

## Rolling Back to a LUN Snapshot

Rollback is a process of reverting the state of a LUN back to a point-in-time state when the snapshot was taken.



**Caution:** The rollback process results in some permanent data loss. You might permanently lose the data changes that happened between rollback time and snapshot creation time.



**Note:** Roll back to a latest available snapshot in order to restore the maximum amount of lost data.

To roll back to a LUN snapshot, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab, select the required project.
3. Click **LUNS** tab and select a required LUN.
4. In the **LUNS** tab, click **Manage > Snapshots**.
5. In the **LUN Snapshots** page you can perform one of the following choices:
  - Click **Graph view** and select a snapshot frequency in the graph. The table below the graph displays the list of snapshots in the selected frequency.
  - Click **Table view** and select a snapshot frequency in the table.
6. Click the **Rollback** button.



**Note:** Before you perform a rollback operation on a snapshot, you must ensure that no IO operations are running on shares or LUNs in the project.

7. In the **Confirmation** screen, click **Yes**.
8. In the **Rollback Snapshot** window, type the snapshot name to roll back.
9. Click **Rollback**.
10. In the **Information** screen, click **OK**.

The LUN state reverts to the point-in-time state when the snapshot was taken.

## Rolling Back to a Snapshot with VMware Datastores

Power off the virtual machine before starting the rollback process.

You need to follow extra steps to roll back to a snapshot of a share or LUN which is used for storing the VMware datastores. Rollback is a process for reverting the state of a share or LUN back to a point-in-time state when the snapshot was taken.



**Caution:** The rollback process results in permanent data loss. You might permanently lose the data changes that happened between rollback time and snapshot creation time.



**Note:** This task explains the restore process for a Share snapshot. You can follow the same process when rolling back to a LUN snapshot.

To roll back to a snapshot of a Share, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab, select the required project.
3. Click the **Shares** tab and select a required share.
4. In the **Shares** tab, click **Manage > Snapshots**.
5. In the **Share Snapshots** page you can perform one of the following choices:
  - Click **Graph view** and select a snapshot frequency in the graph. The table below the graph displays the list of snapshots in the selected frequency.
  - Click **Table view** and select a snapshot frequency in the table.
6. Select a snapshot from the table.



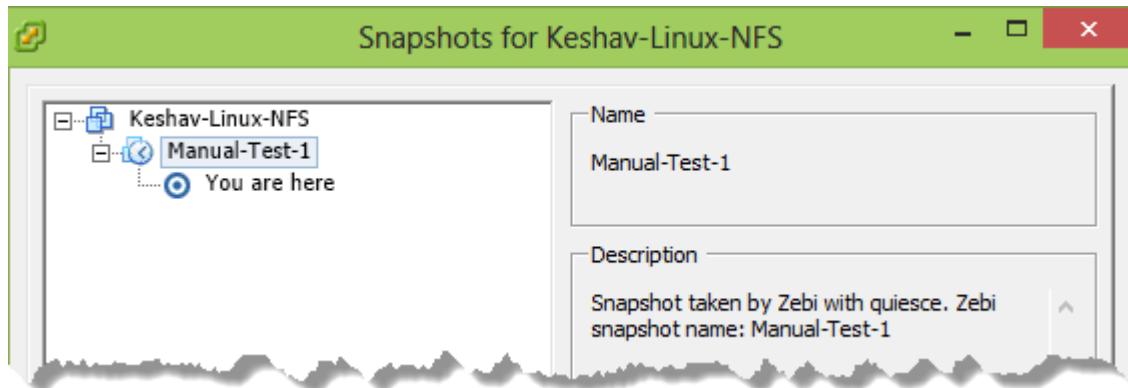
**Caution:** If you select an old snapshot for the rollback purpose, then the subsequent snapshots and all dependent clones are permanently deleted.

7. Click the **Rollback** button.

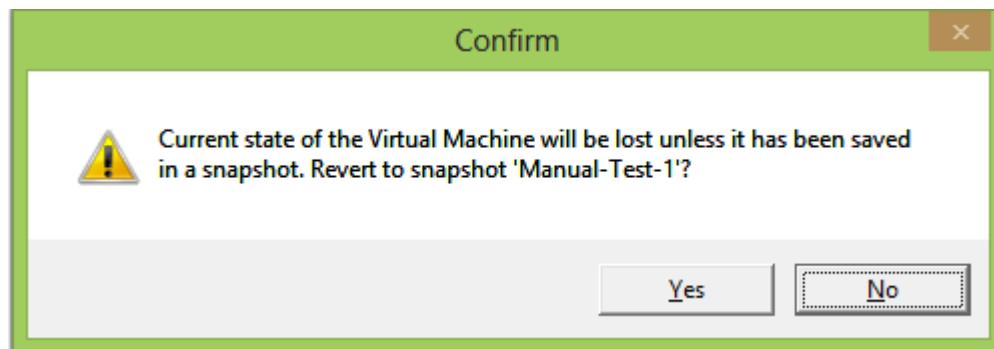
 **Note:** Before you perform a rollback operation on a snapshot, you must ensure that no IO operations are running on shares or LUNs in the project.

8. In the **Confirmation** screen, click **Yes**.
9. In the **Rollback Snapshot** window, type the snapshot name to roll back.
10. In the **Confirmation** screen, click **OK**.
11. Log in to vSphere Client and access the virtual machine on which the Share is mounted.
12. From the virtual machines list, right-click the virtual machine and select **Snapshot > Consolidate**.  
**Confirm Consolidate** window displays.
13. Read the on-screen confirmation message and click **Yes**.
14. From the virtual machines list, right-click the virtual machine and select **Snapshot > Snapshot Manager**.

The Snapshot Manager dialog opens. In the dialog, you can see the roll back snapshot details.



15. In the Snapshot process tree, select the roll backed snapshot and click **Go to**. A confirmation window opens.



16. Read the confirmation message and click **Yes**.  
You can see the **Revert snapshot** task in the **Recent Tasks** pane.
17. Power on the virtual machine and check the status.

## Managing Clones

---

IntelliFlash clone is a read, write copy of a snapshot. You can clone the snapshots of Shares and LUNs by using the IntelliFlash Web UI.

### Cloning a Project Snapshot

Cloning a snapshot of a project allows cloning all shares and LUNs inside the project.

The cloned shares and LUNs display the parent share or LUN, and the clone name is prefixed with the alpha character, "c".

To clone a snapshot project, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab, select the required project.
3. In the **Snapshots** tab of the **Data Protection** page you can perform one of the following choices:
  - Click **Graph view** and select a snapshot frequency in the graph. The table below the graph displays the list of snapshots in the selected frequency.
  - Click **Table view** and select a snapshot frequency in the table.
4. Select a snapshot from the table.
5. Click the **Clone** button.
6. In the **Confirmation** window, click **Yes**.
7. In the **Clone Snapshot** window, type a name for the clone.
8. (Optional) Select **Inherit Project Settings**.
9. Click **Clone**.

A cloning in-progress notification appears.

### Cloning a Snapshot of a Share

You can clone a snapshot of a share and use it as a regular share.

You can select to inherit the parent share settings when creating a clone of a share. If you select to inherit them, the clone inherits these settings: share general settings, NFS and SMB sharing details, user ACLs, and snapshot scheduling.

To clone a snapshot of a Share, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab, select the required project.
3. Click the **Shares** tab and select a required share.
4. In the **Shares** tab, click **Manage > Snapshots**.
5. In the **Share Snapshots** page you can perform one of the following choices:
  - Click **Graph view** and select a snapshot frequency in the graph. The table below the graph displays the list of snapshots in the selected frequency.
  - Click **Table view** and select a snapshot frequency in the table.
6. Select a snapshot from the table.
7. Click **Clone**.
8. In the **Clone Snapshot** window, complete the following steps:
  - a) Type a name for the clone.
  - b) (Optional) Select **Read Only**.
  - c) Select **Inherit Share Settings**.
  - d) Click **Clone**.
9. In the Information window, click **OK**.

## Cloning a Snapshot for Creating an iSCSI LUN

You can clone a snapshot of a LUN and use it as a regular LUN. Clones are useful for quickly retrieving lost data.

You can inherit LUN mapping details from the project or LUN when cloning a snapshot of a LUN.

To clone a snapshot of a LUN, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab, select the required project.
3. Click **LUNS** tab and select a required LUN.
4. In the **LUNS** tab, click **Manage > Snapshots**.
5. In the **LUN Snapshots** page you can perform one of the following choices:

- Click **Graph view** and select a snapshot frequency in the graph. The table below the graph displays the list of snapshots in the selected frequency.
  - Click **Table view** and select a snapshot frequency in the table.
- Select a snapshot from the table.
  - Click **Clone**.
  - In the **Clone Snapshot** window, type in a **Clone name**.
  - Click the protocol dropdown and select **iSCSI**.

 **Note:** You can inherit the LUN mapping details from the parent LUN, Project, or create a new mapping when creating a clone of a LUN snapshot. However, to inherit the parent LUN mapping details, you must select the same protocol type as the parent LUN.

- To create **LUN mapping**, complete the following steps:

<b>Inherit from Project</b> or <b>Inherit from LUN</b> <b>Create New mapping</b> and selected iSCSI protocol in the previous step.	<ol style="list-style-type: none"> <li>Click <b>Next</b>. The <b>Summary</b> screen displays.</li> <li>Review the summary and click <b>Clone</b>.</li> </ol> <ol style="list-style-type: none"> <li>Click <b>Next</b> and complete the following steps.</li> </ol>
---	--

- In the **iSCSI Target Configuration** screen, complete the following steps:

If...	Then...
<b>You want to select the default target.</b>	<ol style="list-style-type: none"> <li>Click <b>Default Target</b>.</li> <li>Click <b>Next</b>.</li> </ol>
<b>You want to select an existing target.</b>	<p>Complete the following steps:</p> <ol style="list-style-type: none"> <li>Click <b>Choose Target</b>.</li> <li>Select the target from the <b>Choose Target</b> dropdown.</li> </ol> <p>The target group and status of the selected target appear.</p> <ol style="list-style-type: none"> <li>(Optional) Select <b>Authentication for Target</b> to authenticate CHAP. You can select <b>None</b>, <b>CHAP</b>, or <b>Mutual</b>.</li> </ol> <p> <b>Note:</b></p>

If...	Then...
	<ul style="list-style-type: none"> <li>When you change <b>Authentication for Target</b> from <b>None</b> to <b>CHAP</b>, IntelliFlash displays the message: <i>Modifying the authentication mechanism affects the existing iSCSI sessions. Do you want to continue? [Yes   No]</i>. Click <b>Yes</b> to continue.</li> <li>When you change <b>Authentication for Target</b> from <b>None</b> to <b>Mutual</b>, provide the CHAP username and password. The credentials are used by the initiator to authenticate the target.</li> </ul> <p>4. Click <b>Next</b>.</p>
<b>You want to create a new target.</b>	<p>Complete the following steps:</p> <ol style="list-style-type: none"> <li>Click <b>Create Target</b>.</li> <li>In the <b>Target Name</b> field, type a name. The wizard uses the provided target name to create a new target group and displays it in the <b>Target Group</b> field.</li> <li>To add the target to an existing target group, click the <b>select group</b> link and select the target group from the list. To select the default target group instead, select <b>default</b>.</li> <li>In the <b>Choose Network Bindings</b> section, select the required IP address.</li> <li>(Optional) Select <b>Authentication for Target</b> to authenticate CHAP. You can select <b>None</b>, <b>CHAP</b>, or <b>Mutual</b>.</li> </ol> <p> <b>Note:</b></p> <ul style="list-style-type: none"> <li>When you change <b>Authentication for Target</b> from <b>None</b> to <b>CHAP</b>, IntelliFlash displays the message: <i>Modifying the authentication mechanism affects the existing iSCSI sessions. Do you want to continue? [Yes   No]</i>. Click <b>Yes</b> to continue.</li> <li>When you change <b>Authentication for Target</b> from <b>None</b> to <b>Mutual</b>,</li> </ul>

If...	Then...
	<p>provide the CHAP username and password. The credentials are used by the initiator to authenticate the target.</p> <p>6. Click <b>Next</b>.</p>

12. In the **iSCSI Initiator Group Configuration** screen, complete the following steps:

If...	Then...
<b>You want to provide access to the LUN without any restrictions.</b>	<p>Click <b>All</b> and then click <b>Next</b>.</p> <p> <b>Note:</b> When you select <b>All</b>, it enables existing initiators as well as new initiators to access the newly created LUN.</p>
<b>You want to use an existing initiator group.</b>	<p>Complete the following steps:</p> <ol style="list-style-type: none"> <li>1. Click <b>Choose Initiator Group</b>.</li> <li>2. Click the <b>Initiator Group</b> dropdown and select an initiator group from the list.</li> <li>3. Click <b>Next</b>.</li> </ol>
<b>You want to create a new initiator group.</b>	<p>Complete the following steps:</p> <ol style="list-style-type: none"> <li>1. Click <b>Create Initiator Group</b>.</li> <li>2. In the <b>Initiator Group</b> field, type a name for the group.</li> <li>3. In the <b>Initiator</b> field, type an initiator name. A valid initiator name must start with <i>iqn.yyyy-mm.[reverse-domain-name]</i> or must be an EUI-64 identifier.</li> <li>4. Click <b>Add Initiator</b>.</li> <li>5. Repeat steps (c) and (d) to add additional initiators to the group.</li> <li>6. To provide CHAP authentication, select <b>CHAP Credentials</b> and provide the CHAP username and password. The credentials are used by the initiator to authenticate the target.</li> </ol>

If...	Then...
	7. Click <b>Next</b> .

13. Click **Next**.
14. In the **LUN Clone Summary** screen, review the summary and click **Clone**.
15. In the **Confirmation** screen, click **OK**.

## Cloning a Snapshot for Creating an FC LUN

You can clone a snapshot of a LUN and use it as a regular LUN. Clones are useful for quickly retrieving lost data.

You can inherit LUN mapping details from the project or LUN when cloning a snapshot of a LUN.

To clone a snapshot of a LUN, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab, select the required project.
3. Click **LUNS** tab and select a required LUN.
4. In the **LUNS** tab, click **Manage > Snapshots**.
5. In the **LUN Snapshots** page you can perform one of the following choices:
  - Click **Graph view** and select a snapshot frequency in the graph. The table below the graph displays the list of snapshots in the selected frequency.
  - Click **Table view** and select a snapshot frequency in the table.
6. Select a snapshot from the table.
7. Click **Clone**.
8. In the **Clone Snapshot** window, type in a **Clone name**.
9. Click the protocol dropdown and select **FC**.



**Note:** You can inherit the LUN mapping details from the parent LUN, Project, or create a new mapping when creating a clone of a LUN snapshot. However, to inherit the parent LUN mapping details, you must select the same protocol type as the parent LUN.

10. To create **LUN mapping**, complete the following steps:

<b>Inherit from Project or Inherit from LUN</b>	1. Click <b>Next</b> . The <b>Summary</b> screen displays. 2. Review the summary and click <b>Create</b> .
<b>Create New mapping</b> and selected FC protocol in the previous step.	1. Click <b>Next</b> and complete the following steps.

11. In the **Select FC Target Group** screen, select from the default FC target groups and click **Next**.

 **Note:** For a fresh IntelliFlash installation or when you have migrated all the projects to ActiveOnly LUNs after upgrading, you can no longer create FC target groups. You can only select from the default virtual target groups.

12. In the **Select or Create FC Initiator Group** screen, complete the following steps:

If...	Then...
<b>You want to select an existing initiator</b>	Complete the following steps: 1. Click <b>Choose Initiator group</b> . 2. Click <b>Initiator Group</b> and select an initiator group from the list. 3. Click <b>Next</b> .
<b>You want to create a new initiator group</b>	Complete the following steps: 1. Click <b>Create Initiator group</b> . 2. In the <b>Initiator Group</b> field, type a name. 3. From the <b>Ungrouped Initiators</b> list, select the required initiators. 4. Click <b>Next</b> .

13. In the **LUN Clone Summary** screen, review the summary and click **Clone**.

14. In the **Confirmation** screen, click **OK**.



---

# Chapter 12

---

## NAS Services

---

**Topics:**

- *Introduction to Network-Attached Storage (NAS)*
- *Virtualization File Services*
- *General File Services*
- *SMB 3.0 Server Limitations for General and Virtualization File Services*
- *Configuring the NFS Server*
- *Authenticating Shares*
- *User Services*

## Introduction to Network-Attached Storage (NAS)

IntelliFlash systems support both the Server Message Block (SMB) and Network File System (NFS) protocols.

Starting from 3.11.0.x, IntelliFlash provides two SMB server modes: **General File Services** and **Virtualization File Services**. The **General File Services** mode is recommended for multi-protocol (SMB and NFS) file sharing and **Virtualization File Services** mode is recommended primarily for SMB file sharing in HyperV. In both cases, NFS should be utilized for VMWare environments.

Regardless of the SMB modes that the user chooses, user can continue to access NFS for virtualization or file server use cases.

### Upgrade Considerations

- If you have chosen CIFS/SMB1 option in previous releases, the SMB server mode will be set to General File Services mode after upgrading to 3.11.0.x. When the clients remap shares based on the Windows client versions, the SMB version will be negotiated between the Client and the Server. Older Windows clients such as XP continue to use SMB1 and all other clients use SMB2/3 based on the negotiation.
- If you have chosen SMB 2.0 or SMB 3.0 in previous releases, the SMB server mode will be set to Virtualization File Services. In this mode, you can continue to use Virtualization File Services for HyperV VDI or Virtual server use cases.



**Note:** Users cannot change the SMB server mode after upgrading to IntelliFlash 3.11.0.x or higher. The mode can be changed only after a fresh installation. In a fresh 3.11.0.x or higher installation, the **General File Services** mode or the **Virtualization File Services** mode can be selected from the **Services > NAS > SMB** page.

### Server Message Block (SMB) Protocols

IntelliFlash systems support the Server Message Block (SMB) protocols, which are typically used in Microsoft Windows environments. The SMB versions supported include SMB 2.0 and SMB 3.0 for both General File Services and Virtualization File Services. IntelliFlash 3.11.0.x release has limited support for SMB 1.0 in General File Services mode and the support will be deprecated in future releases.



**Note:** In Virtualization File Services mode, upgrade the IDPS agent to the latest 2.1.x.x version to enable quiescing SMB 3.0 shares in Windows hosts.

### Network File System Protocols

Network File System (NFS) is an industry standard protocol for sharing files over a network. IntelliFlash systems support NFSv2, NFSv3, NFSv4, and NFSv4.1.

For multi-protocol NAS environments, Tintri recommends using NFSv4.1 for optimal performance. For other virtualized workloads, Tintri recommends using either NFSv3.0 or NFSv4.1 for optimal performance.

IntelliFlash systems support NFSv4.1 for the following clients:

- Linux clients
- ESXi 7.0 and later

 **Note:** The Kerberos security mode is not supported for NFSv4.1 when using ESXi 7.0 clients.

 **Note:** IntelliFlash supports NFSv4.1 delegations, but does not support referrals and pNFS.

## Virtualization File Services

---

The Virtualization File Services mode is for virtualized environments using VMware ESXi or HyperV. IntelliFlash supports NFS access through VMware ESXi and SMB access through HyperV.

### SMB 3.0 Features Overview

#### SMB 3.0 Features Supported

The following SMB 3.0 features are supported in Virtualization File Services mode:

- **Improved SMB 3.0 Server**

IntelliFlash introduces a more scalable, efficient, and faster SMB 3.0 Server. The new SMB 3.0 Server supports 10,000 multi-channel sessions, 40,000 connections, and a maximum of 500,000 open files.

- **SMB 3.0 Continuous Availability**

SMB 3.0 Continuous Availability allows applications such as Hyper-V and SQL Server to leverage the simplicity of SMB 3.0 shares and enables administrators of Failover Clusters to provide transparent failover to clients during maintenance operations.

The standard IntelliFlash High Availability (HA) is the first level of protection against any disruption. IntelliFlash SMB 3.0 provides an additional level of availability that is SMB 3.0 specific.

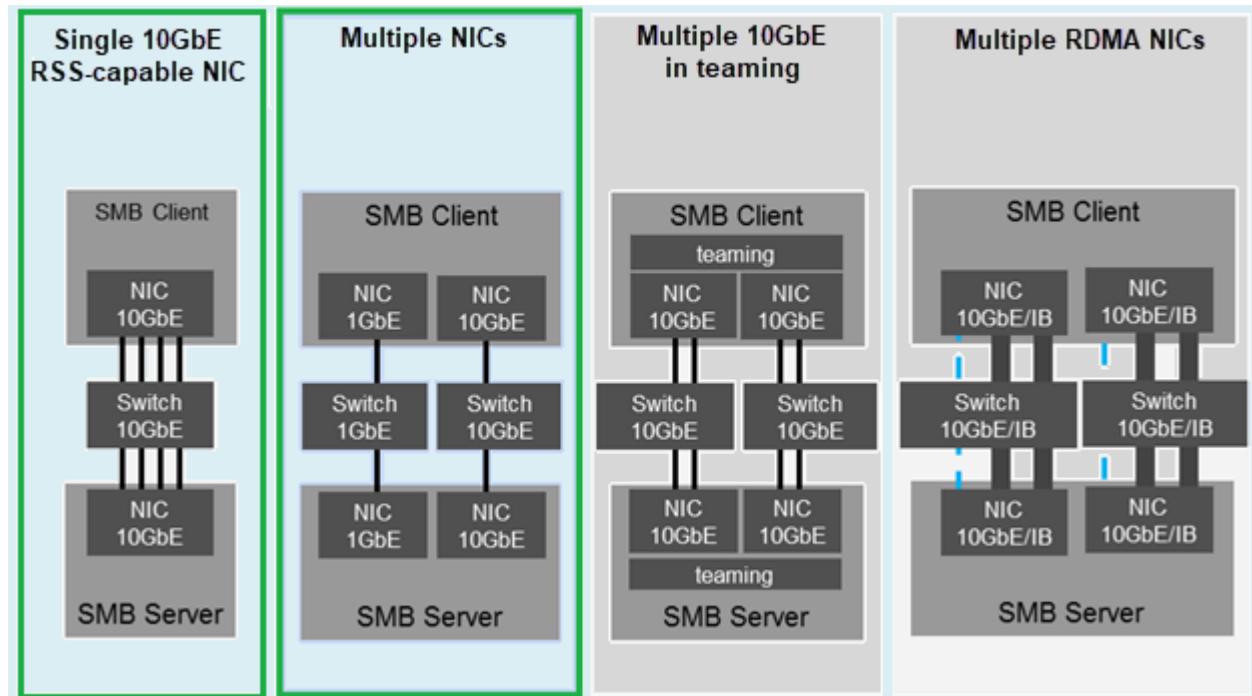
The IntelliFlash SMB server has persistent file handles that maintain state across a failover. In a failover scenario, SMB 3.0 clients use the persistent file handles to reconnect and resume from where they left off.



**Note:** SMB Witness service is not supported in the current release.

- **SMB 3.0 Multichannel**

SMB 3.0 Multichannel enables the IntelliFlash array to provide multiple TCP/IP connections from an SMB 3.0 client to the array, providing higher performance through bandwidth aggregation. The IntelliFlash OS supports multi-NIC and Receive Side Scaling (RSS) configurations that are highlighted by green borders in the following figure.



**Figure 26: SMB 3.0 Multichannel**

The SMB multichannel feature supports heterogeneous interfaces (a combination of 10GbE and 1GbE NICs). Asymmetric interfaces are effective in network resiliency. A separate IP address for each interface is required for multichannel to be effective.

- **Receive Side Scaling (RSS) Support**

The 10GbE interfaces on the IntelliFlash array are now enabled with Receive Side Scaling (RSS). RSS enables IntelliFlash to support SMB Multichannel even with a single 10GbE NIC. SMB creates multiple TCP/IP connections for a single session, avoiding a potential bottleneck on a single CPU core when additional IOs are required.

- **VSS and RVSS support for SMB File Shares**

The Volume Shadow Copy Service (VSS) and Remote VSS (RVSS) for SMB file shares feature is supported.



**Note:** SMB 3.0 share quiesce for Windows Server 2016 is not fully supported.

- **Offloaded Data Transfer (ODX)**

Offloaded Data Transfer (ODX) is a feature that enables an SMB client to offload file transfer operations, such as large file copies and Hyper-V virtual machine import, to the array. This frees the client from the resource impact of moving data. ODX works by enabling IntelliFlash to directly transfer data between the datasets within the array, bypassing the SMB client.

ODX (offloaded data transfer) operations offer the following advantages:

- Direct copy within the array reduces latencies and CPU/Memory resource consumption on the client.
- Reduces the amount of network traffic used for transferring large files from the client to the array.
- Improves the performance of operations such as Virtual Machine live migrations.



**Note:** Though ODX is enabled by default, it is supported only by SMB 3.0.

- **Sparse File Support**

IntelliFlash provides support for sparse files on SMB 3.0 stacks. Sparse files add to efficient SQL server snapshot and checkpoint operations.

## Supported Operating Systems

The Microsoft SMB 3.0 stack supports the following operating systems:

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows 10

## Managing the IP Exclusion List

### Prerequisites

- Virtualization File Services mode must be enabled on the array to access this feature.

You can disable the IP addresses that you do not want SMB to use. This feature is available for Virtualization File Services. Further, this feature is useful only if you have enabled SMB 3.0 Multichannel or the traffic from SMB 3.0 is not isolated and is on the same subnet as any of the following:

- Other IP-based protocols, such as NFS and iSCSI
- Array Management IP addresses

- Any other floating IP addresses in use

 **Note:** Though you can manipulate the IP exclusion list when SMB shares have active I/O operations, it is recommended that you configure the IP exclusion list before using any SMB share.

1. Click **Services > NAS > SMB**.

 **Note:** Verify that Virtualization File Services are enabled. If not, complete the procedure described in *Enabling Virtualization File Services* on page 240.

2. In the **IP Exclusion List** section, click **IP Management**.

The **IP Exclusion Management** dialog box appears.

3. To add an IP address to the exclusion list, in the **Available List** section, click an IP address that you want to exclude, and click the toggle right () icon.

The selected IP address is added to the **Exclusion List** section.

4. To remove an IP address from the exclusion list, In the **Exclusion List** section, click the IP address that you want to remove, and click the toggle left () icon.

The selected IP address is included in the **Available List** section.

5. Click **Submit** to save the changes to the **IP Exclusion Management** dialog box.

6. In the **SMB Server Configuration** page, click **Save** to save the changes.

## Enabling Virtualization File Services

IntelliFlash systems have General File Services enabled by default. You need to enable Virtualization File Services if required.

 **Note:** Before enabling Virtualization File Services, make sure that none of the shares have both NFS and SMB enabled. You cannot enable Virtualization File Services if any share has both NFS and SMB enabled.

To enable Virtualization File Services, complete the following steps:

1. Click **Services > NAS > SMB**.
2. In the **SMB Server Configuration section**, select the **Virtualization File Services** mode.
3. Optional: Enter the IP address or the FQDN of the **Primary Domain Controller (PDC)**.
4. Optional: Click **Subshare Creation** to enable creating subshares (shares within an SMB share)
5. Click **Save**.

## General File Services

---

The **General File Services** mode supports multi-protocol NFS and SMB data access. This mode serves as a general purpose file server and supports large number of shares for the file server environments.

### Multiprotocol NAS Overview

A multiprotocol NAS system introduces challenges in authorization paradigms, security, as locking mechanisms differ between Unix and Windows operating systems.

#### Authentication and Directory Services

File sharing deployments commonly leverage Directory Services to manage users and network resources. SMB deployments utilize Microsoft Active Directory (AD) and NFS deployments typically use Lightweight Directory Access Protocol (LDAP) in a single protocol environment. In a multiprotocol NAS environment, IntelliFlash should be configured to use Active Directory for authenticating NFS and SMB shares. You can authenticate shares for local users and groups. Local authentication is suitable only when a few users need to access storage on the array.

For more information on share authentication, see [Authenticating Shares](#) on page 245.

#### NAS File Permissions and ACLs

Multiprotocol NAS environments introduce new challenges for managing user access and file permissions. SMB protocol ownership and permissions are based on a Windows Security Identifier (SID) and Windows group SID for ownership along with a list of Access Control Entries (ACE) that comprise the Access Control List (ACL). The ACL defines the permissions applied to a given file or directory based on SMB Windows security descriptors. NFS protocol file ownership and permissions are based on User ID (UID) and Group ID (GID) for ownership with POSIX style permissions (User, Group, Others).

IntelliFlash implements NFSv4-style ACLs on its file systems. You can create and modify individual ACE using the IntelliFlash UI or Windows clients. IntelliFlash ACLs are compatible with both NFS and SMB so that the ACL you create for a file system applies to clients using either protocol. This compatible ACL model provides the foundation for full-featured, concurrent SMB, and NFS sharing of IntelliFlash file systems using Microsoft ID Mapping. The IntelliFlash ACL model is comparatively easy to set up/configure and avoids complex security style configurations.

#### File Locking between Protocols

File locking saves the file from simultaneous modification of the file from two processes, thereby eliminating the potential data loss or dataset corruption. SMB and NFS v3/v4 have different paradigms with regards to file locking. SMB and NFSv4 have three types of locks:

#### Share Locks

SMB protocol allows share modes or share locks feature that allows clients to announce the type of parallel access to be allowed by other clients when the file is open. NFSv4 share reservations are the equivalent of SMB share modes for the NFS protocol. IntelliFlash coordinates clients from these two protocols. There is no equivalent in NFSv3.

## Delegation

SMB protocol also supports oplocks or delegations feature that allows clients to cache files locally on the client and improve responsiveness. For example, updates to a Microsoft Office file are cached on a local system rather than sending it to an SMB share provider until the user actively “saves” the file. If the SMB server is set to propagate oplocks, other clients such as NFS can break SMB oplocks. Similarly, if the NFS server is set to propagate NFSv4 delegations, other SMB clients can break the delegations when they want to access the file. IntelliFlash manages clients with oplocks or delegations. NFSv3 protocol does not support delegations.

## Byte-range Locks

Byte range locks allow an application to lock a portion (byte-range) of a file so that other applications can modify other ranges in a file. Byte range locks from SMB clients are propagated into the IntelliFlash file system and NFS clients are made aware of those locks. Similarly, byte-range locks taken from NFS (NFSv3, NFSv4.0, and NFSv4.1) clients are seen by the SMB clients and IntelliFlash coordinates seamless access to files.

 **Note:** Parallel access to the same file by multiple clients over multi-protocol NAS environment requires the clients to ensure serialization to prevent file corruption. This is typically handled through file-locking mechanism so that two (or more) applications do not overwrite the changes made from another client. The SMB protocol assumes mandatory locking, but UNIX traditionally uses advisory locking. You can configure IntelliFlash array to use mandatory locking per-share with the non-blocking mandatory locking (**nbmand**) option. When set, the **nbmand** mount option enforces mandatory multi-protocol share reservations and byte-range locking across NFS, SMB, and local processes. When the **nbmand** mount option is not set, the SMB service enforces mandatory share reservations and byte-range locking internally for all SMB clients. However, without **nbmand** set, there is only limited coordination with NFS and local processes leading to file corruption. Hence, to configure shares for multi-protocol data access enable **nbmand** option without fail to prevent data corruption.

 **Note:** The mandatory locking (**nbmand**) option enforces only mandatory multi-protocol share reservations and byte-range locking. The semantics does not protect files that are locked from being deleted from another protocol.

 **Note:** NFSv3 does not support share mode lock and delegations and the lock enforcement is advisory with NFSv3. Besides, NFSv3 does not use the same access control model as SMB. Thus, usage of NFSv4.1 clients is highly recommended for data access in multi-protocol NAS environment.

## User Mapping in Multiprotocol NAS

A multiprotocol NAS system allows each SMB user mapping to a corresponding NFS user with common access privileges, regardless of the protocol being used by the user to access their file system data. By default, users with the same name in Active Directory and the UNIX Directory service have their SMB and NFS identities mapped, allowing for multi-protocol NAS access across each protocol.

In a multiprotocol NAS environment, for file access, the NAS server should know the mapping between the SID <=> SMB Name <=> UNIX Name <=> UID. This facilitates the mapping between Windows and a UNIX user, and vice versa to enforce file security when the other

protocol is used for access. This multiprotocol mapping is essentially performed by matching names between the protocols, but each protocol also requires a method to map their respective names to their IDs.

For more information, see [User Services](#) on page 256.

## File Change Notifications

SMB clients can request notifications when objects change in the file system. The SMB server informs its clients about the changes. File changes initiated by NFS clients also will trigger a notification. The following operations trigger change notification:

- create/mkdir
- remove/rmdir
- rename
- link/symlink

## File Naming Conventions

NFS and SMB protocols differ in their file naming conventions, differences are listed below:

- File naming in NFS protocol is case sensitive. For example, two files `foo.txt` and `Foo.txt` can reside in the same folder. In SMB protocol, file naming is case-aware or case-preserving but not case sensitive, so `foo.txt` and `Foo.txt` are treated as same files.
- Reserved characters such as {`<`, `>`, `:`, `"`, `/`, `\`, `|`, `?`, `*`} are not supported on multiprotocol enabled shares.
- Files and folders with a dot (.) character, commonly called a dot file will not be hidden on Windows. For example, `/home/user/.config`. There is no option to hide such files from Windows.

## Capabilities in General File Services Mode

The new SMB 3.0 Server supports 10,000 sessions, 20,000 connections, and a maximum of 300,000 open files.

General File Services mode supports the following features:

- SMB 3.0 Continuous Availability
- Offloaded Data Transfer (ODX)
- Limited support for Sparse Files

For more information, refer [SMB 3.0 Features Overview](#) on page 237.

The following features are not supported in 3.11.x.x when the SMB server is in the General File Services mode:

- SMB Multichannel and IP exclusion list
- Receive Side Scaling (RSS) Support
- Offline shares
- Subshares
- Quiesce snapshot using VSS agent
- Symlinks and hardlinks are not supported over SMB. The symlinks can be created from NFS and such symlinks are accessible from SMB

## Enabling General File Services

After you set the General File Services mode, you cannot change the mode.

To enable the General File Services mode, complete the following steps:

1. Click **Services > NAS > SMB**.
2. In the **SMB Server Configuration** section, select the **General File Services** mode.

## SMB 3.0 Server Limitations for General and Virtualization File Services

---

The following SMB 3.0 features are not supported for General and Virtualization File services:

- SMB Direct
- SMB Encryption
- SMB Witness service
- VDI with roaming profiles or folder redirection

## Configuring the NFS Server

---

The NFS server configuration page displays the various default server properties. However, you can change the property settings based on your requirements.

To configure the NFS server, complete the following steps:

1. Click **Services > NAS > NFS**.
2. In the **NFS Server Configuration** page, set the NFS Server configuration properties as described in the following table:

**Table 7: NFS Server Configuration Fields (and defaults)**

Property	Description
Server Minimum Version	Controls the minimum version of NFS to support. The default is version 2.
Server Maximum Version	Controls the maximum version of NFS to support. The default is version 4.1.
Servers	Sets the maximum number of NFS servers to support. Default is 256.
Listen Backlog	Sets the number of connect requests that are queued and waiting to be processed before new connect requests are denied. Default value is 32.
Lockd Servers	Sets the maximum number of concurrent lockd requests. Default number is 256.

Property	Description
Lockd Listen Backlog	Sets the connection queue length for lockd requests over a connection-oriented transport protocol. Default and minimum value is 32.
Grace Period (seconds)	Grace period, in seconds, that all clients have to reclaim locks after a server reboot or switchover/failover. Default value is 20 seconds.
Maximum Connections	Use the default value (-1) for unlimited connections.
NFSv4 Domain Name	Domain name of the IntelliFlash Array.

3. Click **Save**.
4. In the **Information** dialog box, click **Yes**.

## Authenticating Shares

---

### Using Local Users and Groups for Authenticating Shares

You can control access to SMB shares even if you are in a Windows Workgroup or do not have a Windows domain with a Kerberos KDC configured. In this case, you can use local users and groups on the IntelliFlash array for authentication of the storage clients that connect to the array.

Local authentication is suitable only when a few users need to access storage on the array and you do not want to use features such as SMB shares for VMs, or AutoHome shares.



**Warning:** You should implement and use only one method for authenticating users: local users or Active Directory. Do not attempt to implement or use both methods simultaneously as it can lead to unexpected results. If you are using Active Directory but had previously created local users that could conflict with users in Active Directory, you should delete the local users.

You can define local users and groups on the IntelliFlash Array using the IntelliFlash Web UI. For more information, see [User Services](#).

### Configuring Unix Attributes for Windows AD Server 2016

Microsoft has discontinued support for IDMU/NIS Server role from Windows Server 2016.

Though the NIS server role, UNIX attributes plugin and MMC snapin are removed, RFC2307 attributes in Active Directory continue to exist. If you use Windows Server 2016 and above that does not support IDMU, refer and perform the following steps to configure Unix attributes:

1. Run the below command in elevated command prompt:

```
regsvr32 schmmgmt.dll
```

2. Replicate the following UNIX attributes for IDMU across the Active Directory Domain Controller Global Catalog:

- UID
- UID Number
- UNIX Home Directory
- UNIX User Password
- GID Number

 **Note:** The UNIX attributes listed in the previous point must be unique for every user across the domain.

3. Go to **Active Directory Users and Groups**, enable **Advanced Feature View**, **View > Advanced Features**.

- a. Open **Domain Users Properties > Attribute Editor tab**.
- b. Configure/set values for all the below attributes:

```
GID <example: 4000>
```

- c. Click **Apply and Save**.

4. Open properties of the user for whom you want to set the attributes from **Attribute tab**.

Configure/set values for all the below attributes:

- UID <name of the user>
- UIDNumber <a unique id number>
- GIDNumber <same gid number given for above group>
- loginshell /bin/sh
- UnixHomedirectory </home/name of the user>

 **Note:** To use **NFSv4**, you must ensure the following prerequisites are met:

- No multiple domains
- The user name, group name, UID, GID must be unique
- All users in an Active Directory Forest must use the same NFSv4 domain

## Using Microsoft Active Directory with Kerberos for Authenticating SMB and NFS Shares

IntelliFlash systems can be joined to a Microsoft Active Directory Domain Controller for Kerberos-based authentication of SMB and NFS shares. This is required if you want to use any of the following functionality:

- Use SMB 3.0 shares to host Hyper-V Virtual Machines.
- Enforce and manage user-level access control more easily on shares. You can search for Active Directory users and groups from the IntelliFlash Web UI and define what privileges they have on a specific share or group of shares.
- Automatically create and provision shares and enforce access control on the new share by using the AutoHome feature.
- Provide a higher level of security for NFSv4 shares with Kerberos.

## Configuring Active Directory and Kerberos-based Authentication

To use Active Directory and Kerberos for authentication and identity management, complete the following tasks:

1. Meet all the requirements mentioned in [Requirements for using Active Directory with Kerberos for Authentication](#).
2. Join the IntelliFlash array to the required Active Directory domain, as described in [Joining the IntelliFlash Array to an Active Directory Domain](#).
3. Integrate IntelliFlash Identity Management with Active Directory, as explained in [Configuring IntelliFlash to use Kerberos-based Authentication](#).

## Using LDAP Users and Groups to Authenticate NFS Shares

IntelliFlash enables you to look up LDAP users and groups directly from an LDAP server, and to apply ACLs on NFS shares. Earlier, if LDAP users had to access the NFS shares, you had to add local accounts of the LDAP users with the same credentials.

To join to an LDAP server, complete the following tasks:

1. Meet all the requirements mentioned in [Requirements for Joining IntelliFlash array to an LDAP Server](#).
2. Join the IntelliFlash array to the required LDAP server, as described in [Joining the IntelliFlash Array to an LDAP Server](#).

## Requirements for Using Active Directory with Kerberos for Authentication

### Mandatory Requirements

Before you configure the IntelliFlash Array to use Active Directory with Kerberos for authentication of shares, you must make sure the following requirements are met on the Active Directory Domain Controller:

- **Active Directory Domain Services** with the **Active Directory Domain Controller** role are installed and running on Windows Server 2008 R2 or later for integration with SMB and NFS.

- The Kerberos **Key Distribution Center** server must be running on each domain controller as part of the Active Directory Domain Services.



**Note:** Refer Configuring Unix Attributes for Windows AD Server 2016 section in [Authenticating Shares](#) on page 245 if your Windows Active Directory version is 2016 and above.

- If you are using Active Directory on a Microsoft Windows Server 2012 R2 and below, the following **Active Directory Domain Services** roles need to be installed and running:
  - **Identity Management for UNIX (IDMU)** role is installed with **Server for Network Information Services** on all domain controllers for which users need to be resolved.
  - **Administration Tools**.



**Warning:** **Password Synchronization** for **Active Directory Domain Controller** is not supported.

- The Global Catalog must be accessible on the non-SSL port number 3268. The IntelliFlash OS does not support SSL over port 3269. If the Active Directory Domain Controller is behind a firewall, ensure that the required ports are accessible..
- A Global Catalog must be set up and configured in at least one domain controller in an Active Directory Forest.

## Additional Requirements

- Replicate the following UNIX attributes for IDMU across the Active Directory Domain Controller Global Catalog:
  - UID
  - UID Number
  - memberUid
  - UNIX Home Directory
  - UNIX User Password
  - GID Number
- The UNIX attributes listed in the previous point must be unique for every user across the domain.
- To use **NFSv4**, you must ensure the following prerequisites are met:
  - No multiple domains.
  - The user name, group name, UID, GID must be unique.
  - All users in an Active Directory Forest must use the same NFSv4 domain.

## General Requirements

- The IntelliFlash Array, the Active Directory domain controllers, the DNS servers, and the clients should use the same NTP server as the Kerberos KDC server. This makes sure that the date and time on all systems are synchronized. If that is not possible, you must manually make sure that time is synchronized between these systems.
- The DNS server used by the Active Directory Domain Controller is accessible from the IntelliFlash Array.
- To use Active Directory with NFS shares, all participating Active Directory Domain Controllers and IntelliFlash controllers must be able to successfully perform forward and reverse DNS lookups of each other. Therefore, you must add the required IP addresses to the DNS server; including floating IP addresses and IP addresses used for NFS shares, interface groups, and management interfaces.
- When the IntelliFlash Array tries to join the Active Directory domain, it tries to join from both controllers simultaneously. Therefore, make sure that both IntelliFlash controllers have the correct domain name and DNS server configured.
- The floating IP addresses used by shares must have DNS entries that allow clients to access and map the shares using FQDNs. This is required for Kerberos to authenticate the requests.

## Joining the IntelliFlash Array to an Active Directory Domain

### Prerequisites

You must have completed the prerequisites described in [Requirements for using Active Directory with Kerberos for Authentication](#).

The IntelliFlash Array uses SMB 2.0 to join to the Microsoft Active Directory domain.

To join the IntelliFlash Array to an Active Directory domain and use Active Directory and Kerberos for authentication, complete the following steps:

1. Click **Services > NAS > Identity Management**.
2. In the **Identity Management** page, click **Configure**.
3. In the **Configure Identity Management** dialog box, select the **DOMAIN** mode.



**Note:** When the **WORKGROUP** mode is selected, only the **Workgroup name** and **LAN Manager (LM) Authentication** fields are enabled. All other fields are disabled. If you want to use the WORKGROUP option, provide a name for the workgroup in **Workgroup name** and go directly to [step 5](#).

4. Configure the following settings to join the array to a Windows domain and use an Active Directory domain controller for Kerberos-based authentication.

- **Domain Name:** Enter the Fully Qualified Domain Name (FQDN) of the Active Directory Domain as defined on the Domain Controller. The FQDN must match the network settings of the IntelliFlash array controller.

- **Admin Name:** Enter the name of the organizational unit group administrator.
- **Admin Password:** Enter the password of the organizational unit group administrator.
- **Add Kerberos Key Distribution Center (KDC) Server:** Add multiple KDC servers, if required. To add a server, enter the hostname of the server and click **Add**.

 **Note:** The KDC servers you add appear below this field. Click the cross symbol (x) next to the server name to remove it from the list.

- **IDMU:** Enable the **IDMU** option to enable lookups on the Active Directory. When the IDMU option is enabled, lookups for users and groups will first search the Active Directory and then the local users and groups.

 **Note:**

- When **IDMU** is disabled, you cannot search for users on the Active Directory from the IntelliFlash Web UI to add ACL to shares. Use identity mapping (IDMAP) to add the ACL. Alternatively, add the ACL from the Windows client after mapping the share.
- If unix attributes (like UID, GID, homeDirectory and so on) are not configured for users/groups on the Active Directory, then disable IDMU while joining the IntelliFlash Array to an Active Directory.

- **OU:** The **OU** field allows you to specify the Active Directory Organizational Unit in which computer accounts for the array controllers will be created. This enables the array to be joined to a Windows domain in a secure manner that conforms with Windows DC hardening guidelines.

You can use this field to provide a distinguished name, such as:

```
OU=it,OU=deptt,DC=newyork,DC=d1,DC=example,DC=com
```

If an OU name contains blank spaces, you must enclose the name within double quotes. For example:

```
OU="IT Admin",OU=deptt,DC=newyork,DC=d1,DC=example,DC=com
```



**Important:** You must provide an Active Directory Organization Unit (OU) and not a container. If you provide an Active Directory container that is not an OU, the domain join operation will fail.

- **Windows Server Version:** Select the version from the dropdown menu (2000, 2003, 2008, 2012, 2016, 2019). The default is 2008.

The Windows Server version must be the same version as the Domain Functional Level on the Domain Controller.

- **Signing Enabled:** Select this option to add an electronic signature, if needed.
- **Signing Required:** Select this option if signing is required.

5. Select the LAN Manager (LM) Authentication level.

- **Level-2:** Sends NTLM response only. Domain controllers accept LM, NTLM, and NTLM 2 authentication.
- **Level-3:** Sends NTLM 2 response only. Domain controllers accept LM, NTLM, and NTLM 2 authentication.
- **Level-4:** Domain controllers refuse LM authentication (that is, they accept NTLM and NTLM2).
- **Level-5:** Domain controllers refuse LM and NTLM response (accept only NTLM 2).

Based on the Windows Server version you select, the **LAN Manager (LM) Authentication** field is automatically populated with the recommended level.

#### 6. Click **Save**.

On success, a message prompts you to confirm if you want to configure AD/Kerberos. You must complete the AD/Kerberos configuration to enable the IntelliFlash array to use the Active Directory with Kerberos.



**Important:** For information on how to complete the AD/Kerberos setup, see [Configuring IntelliFlash to use Kerberos-based Authentication](#).

#### 7. On the message box that prompts you to configure AD/Kerberos:

Click...	If you want to...
<b>Configure</b>	Start configuring IntelliFlash to use Active Directory with Kerberos. You can configure this later from the <b>AD/Kerberos Setup</b> page if you click <b>No</b> .
<b>No</b>	Skip the procedure for configuring IntelliFlash to use Active Directory with Kerberos.



#### Note:

- While the AD join is done at the array level, AD accounts are created at the controller level. As a result of completing this procedure successfully, two AD computer accounts are created: one for each array controller; and both accounts are joined to the AD domain that you entered.
- The IntelliFlash OS limits the number of LDAP search entries to 20000. To increase the number of search entries returned by Active Directory, complete the procedure described on this Microsoft Support page: [How to view and set LDAP policy in Active Directory](#).
- Click **Edit** to modify the Active Directory details.

## Configuring IntelliFlash to use Kerberos-based Authentication

### Prerequisites

- You must have completed the prerequisites described in [Requirements for using Active Directory with Kerberos for Authentication](#).
- You must have completed the procedure to join the array to an Active Directory domain as described in [Joining the IntelliFlash Array to an Active Directory Domain](#).

You must configure which floating IP addresses you want to enable for authentication with Active Directory and Kerberos. Client requests must use the hostname/FQDN instead of the IP address and be authenticated with Active Directory and Kerberos to access a protected share or LUN.

To configure which floating IP addresses you want to enable for authentication with Active Directory and Kerberos, complete the following steps:

1. Click **Services > NAS > Identity Management**.
2. In the **Kerberos Configuration** section, click **Configure**.
3. In the **Authentication** dialog box, enter the Active Directory administrator name and password.
4. Click **Submit**.

On success, the page displays the following details:

- Domain Name: The Active Directory domain to which the array is joined.
- Searched Base DN: The Base DN from which the search for a user or group will start.
- Global Catalog Servers: The Global Catalog Server for the domain.

This page also shows a table that lists the floating IP addresses created on the array and the host names of the floating IP addresses as defined on the Active Directory Domain Name Server. By default, all floating IP addresses are selected. You can disable the IP addresses that you do not want to protect with Kerberos authentication.

5. Click **Save** after unchecking the hostnames/IP addresses that you do not want to protect with Kerberos authentication.

For NFS clients to authenticate against Active Directory and Kerberos, and access shares on the IntelliFlash Array, the NFS client should be integrated with Active Directory.

## Unconfiguring Kerberos-based Authentication



**Important:** If you want to use a different AD server, unconfigure the existing AD/Kerberos Setup configuration as described in the following procedure, and then remove the existing AD configuration as described in [Removing the IntelliFlash Array from the Active Directory Domain](#).

If IntelliFlash is joined with an AD server with **IDMU** enabled, Unconfigure options are available in both the Identity Management and Kerberos Configuration sections. But if IntelliFlash is joined with an AD server with **IDMU** not enabled, Unconfigure option is available in only the Identity Management section, and not in the Kerberos Configuration section.

Complete the following steps on either of the two controllers in an IntelliFlash Array:

1. Click **Services > NAS > Identity Management**.
2. In the **Kerberos Configuration** section, click **Edit**.
3. In the **Edit Kerberos Configuration** dialog box, disable all the IP addresses.
4. Click **Save**.
5. In the **Kerberos Configuration** section, click **Unconfigure**.

## Removing the IntelliFlash Array from the Active Directory Domain

To remove the IntelliFlash array from the current Active Directory (AD) domain, complete the following steps:

1. Unconfigure **AD/Kerberos Setup** if it is configured, as described in [Unconfiguring Kerberos-based Authentication](#).
2. Remove the IntelliFlash array from the current Active Directory (AD) domain:
  - a) Click **Service > NAS > Identity Management**.
  - b) Click **Unconfigure**.
  - c) In the Confirmation dialog box, click **Yes**.

## Removing the IntelliFlash System from an AD Domain with Kerberos

In an AD deployment that includes Kerberos, all Kerberos tickets for a computer account on the AD server are identified with a unique version number, known as the Key-Version Number or KVNO. The KVNO is updated every time the computer account is modified. Even when the array re-joins the domain, a new KVNO for the array is generated.



**Caution:** In a deployment that uses Kerberos authentication in a Windows environment, if the domain join procedure is re-run on an array without deleting the array's computer account from the AD, it is possible that the Kerberos service tickets in the array cache contain multiple KVNOs. In such scenarios, SMB operations are susceptible to failure as old Kerberos service tickets may be used during client authentication and other workflows.

Given this behavior, you must delete the computer accounts of both array controllers from the AD after you remove the array from the AD domain.

## Joining the IntelliFlash Array to a Different Active Directory Domain

IntelliFlash Array uses SMB 2.0 to join to the Microsoft Active Directory domain.

To join the IntelliFlash array to a different Active Directory domain, complete the following steps:

1. Remove the array from the current AD domain, as described in [Removing the IntelliFlash Array from the Active Directory Domain](#).
2. If you had Kerberos set up, make sure to delete the computer accounts of both array controllers from the AD after you remove the array from the AD domain.  
See [Removing the IntelliFlash Array from the Active Directory Domain](#) for more details.
3. Add the array to the new Active Directory domain, as described in [Joining the IntelliFlash Array to an Active Directory Domain](#).

## Requirements for Joining the IntelliFlash Array to an LDAP Server

The following prerequisites must be met before you can join IntelliFlash array to an LDAP Server:

- Configure your DNS servers with the hostname and the IP address of the LDAP servers. This enables LDAP server hostname to be resolved, if there are any connection issues.
- Configure NFSv4 domain name in the **NFS Server Configuration** page in the IntelliFlash Web UI.  
For information on configuring NFSv4 domain name, see [Configuring the NFS Server](#).
- For joining the IntelliFlash array to a secure LDAP server, you need to import a CA-signed certificate to the IntelliFlash OS trust store, or generate a self-signed certificate.  
For information on importing a CA-signed certificate or to create a self-signed certificate, see [Importing a CA Certificate](#) and [Generating a Self-Signed Certificate](#).

## Joining the IntelliFlash Array to an LDAP Server for User or Group Authentication on NFS Shares



**Note:** This LDAP configuration is qualified only for OpenLDAP 2.4 (LDAP and LDAPS).

1. Click **Services > NAS > Identity Management**.
2. In the **Identity Management** page, click **Configure**.
3. In the **Configure Identity Management** dialog box, click **LDAP**.
4. In the **LDAP Server** field, provide the fully-qualified domain name of the LDAP server. The format is `server.domain.com`.
5. Enable **Secure LDAP** to configure secure LDAP.

For joining the IntelliFlash array to a secure LDAP server, you need to import a CA-signed certificate to the IntelliFlash OS trust store, or generate a self-signed certificate.

For information on importing a CA-signed certificate or to create a self-signed certificate, see [Importing a CA Certificate](#) and [Generating a Self-Signed Certificate](#).

6. In the **Search Base DN** field, enter the location (base DN) from where the LDAP search begins. For example, dc=example,dc=com.
7. In the **Bind DN** field, enter the user name that authenticates to the LDAP server to query LDAP users and groups. For example, cn=user,dc=example,dc=com.  
The user must have permission for LDAP directory lookups.
8. In the **Bind Password** field, enter the password for the user.
9. Enable **Show Password** to view the password.
10. (Optional) In the **User Search Base** field, enter the value to be used in addition to the base DN to search and load users. The default value is ou=People,dc=example,dc=com.
11. (Optional) In the **Group Search Base** field, enter the value to be used in addition to the base DN to search and load groups. The default value is ou=Group,dc=example,dc=com.
  - After this configuration, when you apply ACLs on a share, you can look up user credentials from an LDAP server (either over a secure or non-secure LDAP server port).

## Applying User-Level ACLs after Configuring an LDAP Server

After configuring an LDAP server, you can add user-level ACLs on shares. To apply user-level shares, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab on the left pane, select the project from the **Projects** list.
3. In the **Shares** tab on the right, select the share and click **Manage > Access**.  
The **Share Access** page appears.
4. In the **Share Access** page, click the **ACLs** tab.
5. In the **ACLs** tab, click **New**.  
The **Add ACL** dialog box appears.
6. In the **Add ACLs** dialog box, complete the following steps:
  - a) Select **User** from the **Type** dropdown list.
  - b) In the **User Details** section, click **Search User**.
  - c) Enter the user name.
  - d) Enter the password in the **Password** field.
  - e) After entering the search string, click the **Search** icon.
  - f) Select the user from the list.
  - g) Select the access type from the **Access** dropdown list.

- h) Select the inheritance type from the **Inheritance** dropdown list.
- i) Select the ACL set from the **Permissions** list.  
Alternatively, select or clear the privileges based on your requirement.
- j) Click **Save**.

## Removing the IntelliFlash Array from the LDAP Server

To unjoin the IntelliFlash array from the LDAP server, complete the following steps:

1. Click **Service > NAS > Identity Management**.
2. In the **Identity Management** page, click **Unconfigure**.
3. In the **Confirmation** dialog box, click **Yes**.

## Editing the Identity Management Details

To modify the LDAP server or Active Directory details, complete the following steps:

1. Click **Service > NAS > Identity Management**.
2. In the **Identity Management** page, click **Edit**.
3. Modify the LDAP server or Active Directory details.

# User Services

---

## Introduction to Users Tab

You can create local users and groups on an IntelliFlash Array and use these accounts to control access to NAS shares through group permissions, user permissions, passwords, and ID mapping.

### Local Users

You can create local users on the IntelliFlash Array to authenticate NAS shares.

Local users are authenticated with a username password. If you integrate the IntelliFlash Array with an Active Directory, the username-password authentication is not required.

If you integrate the IntelliFlash Array with an Active Directory, the IntelliFlash OS does not use the password entered because users do not authenticate against the IntelliFlash Array. Windows authenticates users with Active Directory producing the KDC service ticket for IntelliFlash Array. This ticket also includes information about the username and the group name of the user.

## Local Groups

Local Groups allow you to control access to IntelliFlash NAS services for a groups of users or applications. Each member of the group is granted the same access rights through the group. As a user can be a member of several groups, the access rights of individual users may vary.

## ID Mapping

ID mapping allows you to associate the Windows Active Directory users and groups with their IntelliFlash counterparts.

You can add, delete, and clear ID Map cache.

### Adding a New ID Mapping

To add a new ID mapping, complete the following steps:

1. Click **Services > NAS > Users**.
2. Click **ID Mapping**.
3. In the **ID Mapping** page, click **Add IDMap User**.
4. In the **Add ID Mapping** dialog box, type a domain name in the **Domain name** field.
5. Select any one of the following options from the **Select Mapping Type** dropdown list:
  - **User**: An individual user's Windows Active Directory name.
  - **Group**: A group of users. Use the group Windows Active Directory name.
  - **Global**: Everyone in the entire domain.

If you selected...	Then, do the following...
<b>User</b>	1. Type a <b>Windows User Name</b> . 2. Select a <b>Local User Name</b> from the dropdown menu. 3. Click <b>Add</b> .
<b>Group</b>	1. Type a <b>Windows Group Name</b> . 2. Select a <b>Local Group Name</b> from the dropdown menu. 3. Click <b>Add</b> .
<b>Global</b>	Click <b>Add</b> .

6. Click **Add**.

## Clearing IDmap Cache

Clear ID Map Cache flushes the identity mapping cache so that future mapping requests will be fully processed based on the current rules and directory information.

A rule change automatically flushes the cache. This manual operation forces the newly changed directory information to take effect.



**Caution:** This operation can potentially disrupt operations that are in process, so only use it on an inactive system.

To clear the ID Map cache, complete the following steps:

1. Click **Services > NAS > Users**.
2. Click **ID Mapping**.
3. In the **ID Mapping** page, click **More**.
4. Select **Clear ID Map Cache** from the dropdown list.
5. In the **Confirmation** dialog box, click **Yes**.
6. In the **Information** dialog box, click **OK**.

## Deleting an ID Mapping

To delete an ID mapping, complete the following steps:

1. Click **Services > NAS > Users**.
2. Click **ID Mapping**.
3. In the **ID Mapping** page, select the ID mapping and click **Delete**.
4. In the **Confirmation** dialog box, click **Yes**.
5. In the **Information** dialog box, click **OK**.

## Adding a Local User

To add a local user, complete the following steps:

1. Click **Services > NAS > Users**.
2. Click **Local Users**.
3. In the **Local Users** page, click **Add**.
4. In the **Local User** dialog box, type the user name, password, and user ID in the appropriate fields.
5. Select a group from the **Group** dropdown list.
6. Click **Add**.
7. In the **Information** dialog box, click **OK**.

## Deleting a Local User

To delete a local user you created on the IntelliFlash Array, complete the following steps:

1. Click **Services > NAS > Users**.
2. Click **Local Users**.
3. In the **Local Users** page, select the user name and click **Delete**.
4. In the **Confirmation** dialog box, click **Yes**.
5. In the **Information** dialog box, click **OK**.

## Changing a User Password

To change a user password, complete the following steps:

1. Click **Services > NAS > Users**.
2. Click **Local Users**.
3. In the **Local Users** page, select the user and click **Change Password**.
4. In the **Change Password** dialog box, type a new password.
5. Type the password again for confirmation.
6. Click **Change**.
7. In the **Information** dialog box, click **OK**.

## Adding a Local User Group

To add a local user group, complete the following steps:

1. Click **Services > NAS > Users**.
2. Click **Local Groups**.
3. In the **Local Groups** page, click **Add**.  
The **Local Group** dialog box appears.
4. In the **Local Group** dialog box, type a group name in the **Group Name** field.
5. (Optional) Type an ID in the **Group ID** field.
6. Click **Add**.
7. In the **Information** dialog box, click **OK**.

## Deleting a Local User Group

Deleting a group does not delete the users within the group, it only moves them out of the no longer existing group.



**Note:** If you delete a group that is used in an ID mapping, the ID mapping is lost.

To delete a local user group, complete the following steps:

1. Click **Services > NAS > Users**.
2. Click **Local Groups**.
3. In the **Local Groups** page, select the group name and click **Delete**.
4. In the **Confirmation** dialog box, click **Yes**.
5. In the **Information** dialog box, click **OK**.

---

# Chapter 13

---

## NAS Auditing

---

**Topics:**

- *NAS Auditing Overview*
- *NAS Auditing Requirements*
- *Accessing NAS Auditing Feature in IntelliFlash Web UI*
- *Enabling NAS Auditing Feature in IntelliFlash Web UI*
- *Configuring Auditing for SMB Shares through the Windows Client*
- *Configuring Auditing for NFS Shares through the Windows Client*
- *Configuring Audit Share Quota*
- *Configuring Space Usage Threshold Levels*
- *Configuring Retention Policy of Audit Logs*
- *Generating XML Audit Logs on Demand*
- *Enabling SMB Access of Audit Log Share*
- *Enabling NFS Access of Audit Log Share*
- *Connecting to Audit Log Share from NFS or SMB Client*
- *XML Log Reports Examples*

## NAS Auditing Overview

---

NAS audit logging enables you to secure NFS and SMB files by tracking operations on files and shares such as:

- Creating, modifying, reading, moving, renaming, closing, and deleting files and folders
- Failed and successful access to files and folders
- Other events such as taking ownership, kernel panic, symlink creation, and hardlink file creation

When the NAS audit feature is enabled, IntelliFlash creates a read-only audit log share per pool. The audit logs are collected in binary form on the audit log share. The binary logs are then generated into XML files once in every 24 hours. The XML files are stored in the XML directory of the audit log share.

The NAS audit log shares can be accessed through the SMB or NFS protocol.

When the NAS audit feature is disabled, you can still access the audit share logs from the bin and xml folders for the mounted audit share on SMB and NFS client. Only the latest records will not be maintained when the audit is disabled.

### Limitations of NAS Auditing

- Events such as file close, log on, and log off are not audited.
- Audit ACLs cannot be set on a mapped share when the IntelliFlash system is in the workgroup mode.
- Audit ACLs cannot be set on user autohome shares.
- Power cycle (off and on) both the nodes at the same time through BMC disables audit service.
- When you disable NAS auditing, the Audit Log tab is also disabled. The configuration of the audit log share persists as previously set.
- On rare occasions, under heavy workloads, when a large number of audit events are generated, audit records might not be included in the audit logs.

## NAS Auditing Requirements

---

### Enabling General File Services Mode

The NAS audit feature in IntelliFlash is supported only when the **General File Services** mode is enabled first. The General File Services mode serves as a general purpose file server, and supports both NFS and SMB data access.

For additional information, see [Enabling General File Services](#).

The NAS auditing feature is not protocol-specific. Events will be logged for both the NFS and SMB shares when you enable NAS auditing.

## Windows Active Directory Configuration

For the NAS audit feature to work, IntelliFlash shares should be authenticated by Windows Active Directory.

### NFS Server Version

The NAS Auditing feature is supported for NFS versions 4.0 and 4.1. For auditing NAS shares, the NFS client needs to mount the shares as 4.0 or 4.1.

For configure the NFS Server, see [Configuring the NFS Server](#).

### SMB Server Version

The SMB server needs to be at SMB 2.0 or above.

## Accessing NAS Auditing Feature in IntelliFlash Web UI

---

### Accessing NAS Auditing Feature

To access NAS auditing, do the following:

- From the **Services** menu, select **NAS** and then click **Audit**.

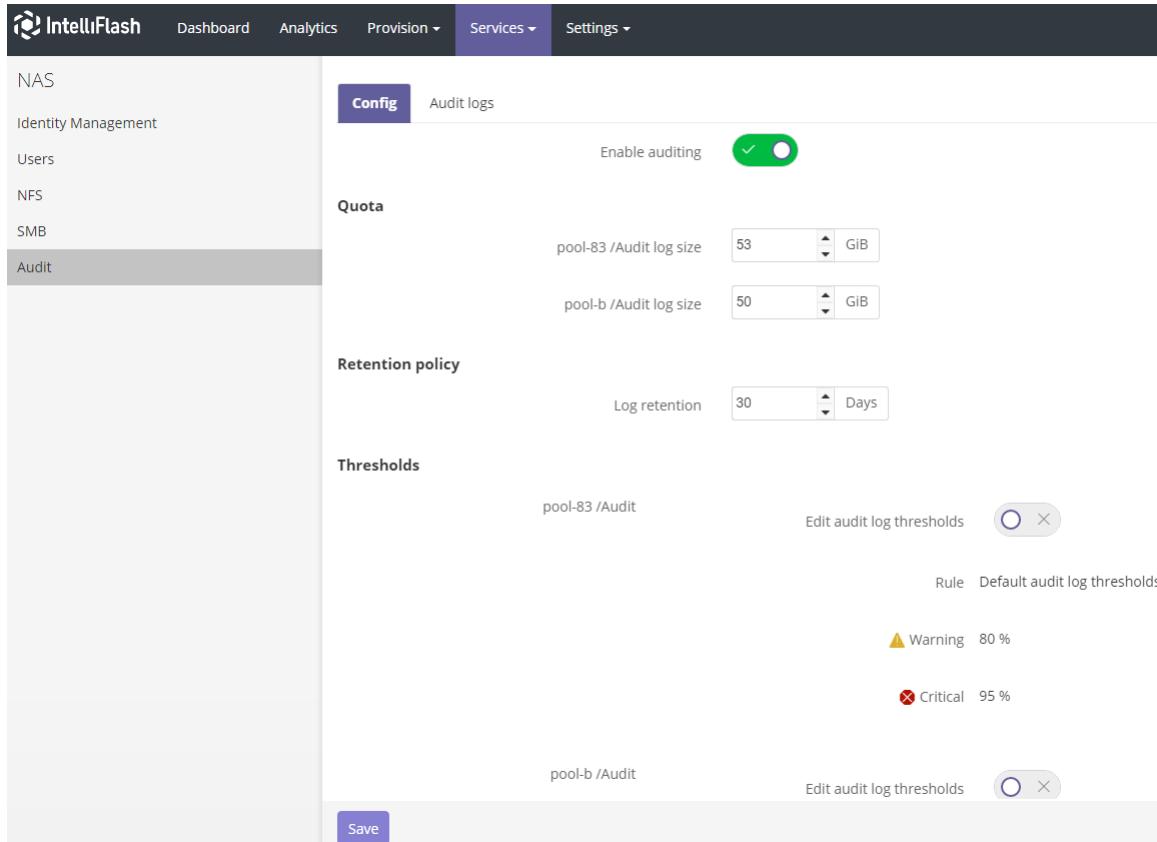


**Note:** The **NAS Audit** page consists of two tabs: **Config** and **Audit logs**.

### Config Tab

In the **Config** tab, you can

- Enable NAS auditing
- Configure audit share quota
- Configure space usage threshold levels
- Configure retention policy of audit log



**Figure 27: NAS Auditing – Config Tab**

### Audit logs Tab

In the **Audit logs** tab, you can

- Generate XML audit logs on demand
- Enable SMB access of audit log share
- Enable NFS access of audit log share

The screenshot shows the IntelliFlash Web UI interface. At the top, there is a navigation bar with links for Dashboard, Analytics, Provision, Services (selected), and Settings. The main content area is titled 'Audit' under the 'NAS' section. On the left sidebar, there are links for Identity Management, Users, NFS, SMB, and Audit (which is selected). Under the Audit section, there are tabs for Config and Audit logs (selected). A sub-section titled 'Update audit logs' contains a note about generating XML files every 24 hours and a 'Start' button. Below this is a section titled 'NFS and SMB Access' with tabs for NFS (selected) and SMB. It shows 'NFS Sharing:' is enabled (green toggle switch). 'NFS log details:' lists 'pool-83 mount point: /pool-83/Audit' and 'pool-b mount point: /pool-b/Audit'. 'NFS access:' has 'Add' and 'Delete' buttons and a dropdown for 'IP Address / Machine name' which shows 'No records found'.

**Figure 28: NAS Auditing – Audit logs Tab**

## Enabling NAS Auditing Feature in IntelliFlash Web UI

---

To enable NAS auditing, complete the following steps:

1. From the **Services** menu, select **NAS** and then click **Audit**.
2. In the **Audit** page, click **Config**.
3. Select **Enable auditing**.

The NAS auditing service is enabled and the NAS audit shares (one audit share per pool) are initialized.

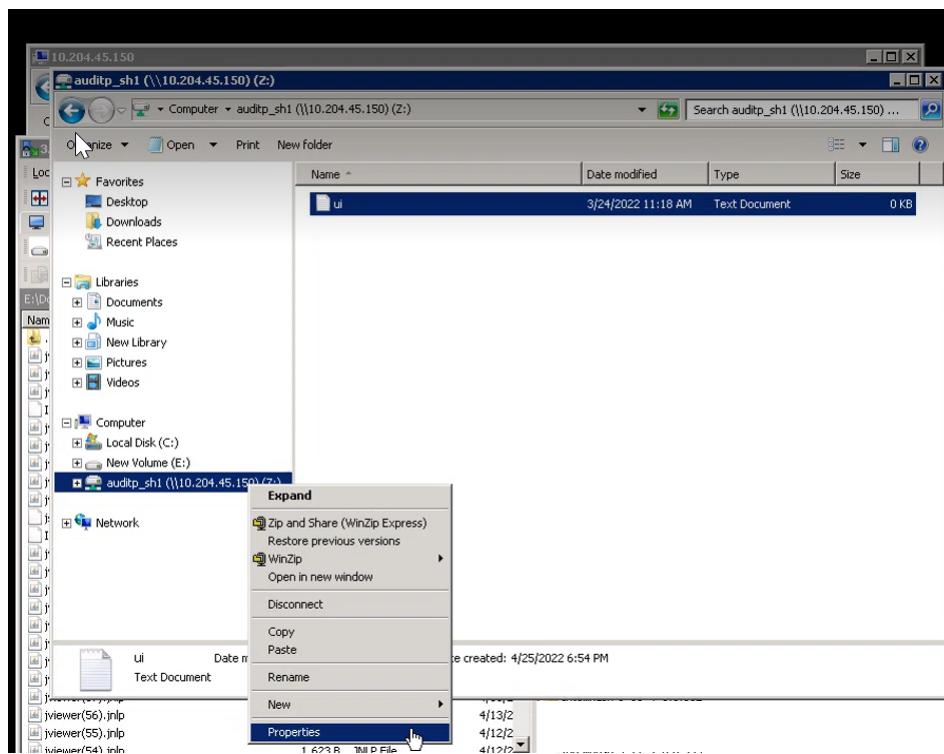
## Configuring Auditing for SMB Shares through the Windows Client

---

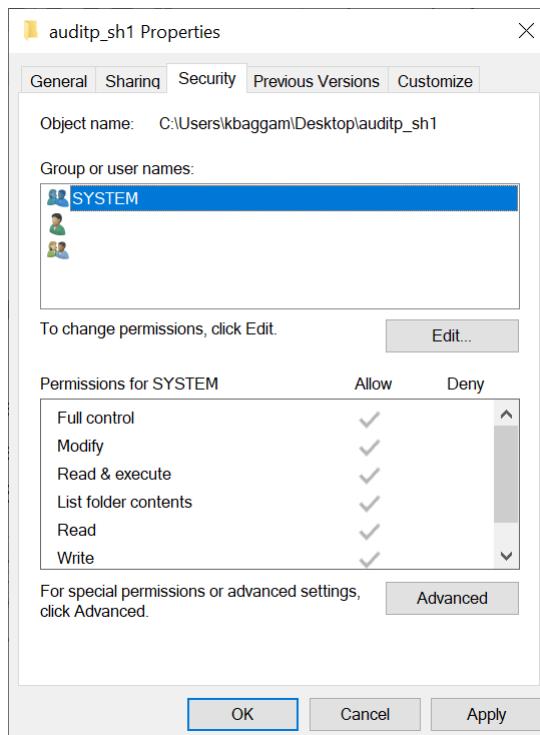
Audit ACLs for SMB shares cannot be set through IntelliFlash Web UI. The following procedure describes how you can set audit ACLs on SMB shares from the Windows client.

To configure auditing for SMB shares through the Windows client, complete the following steps:

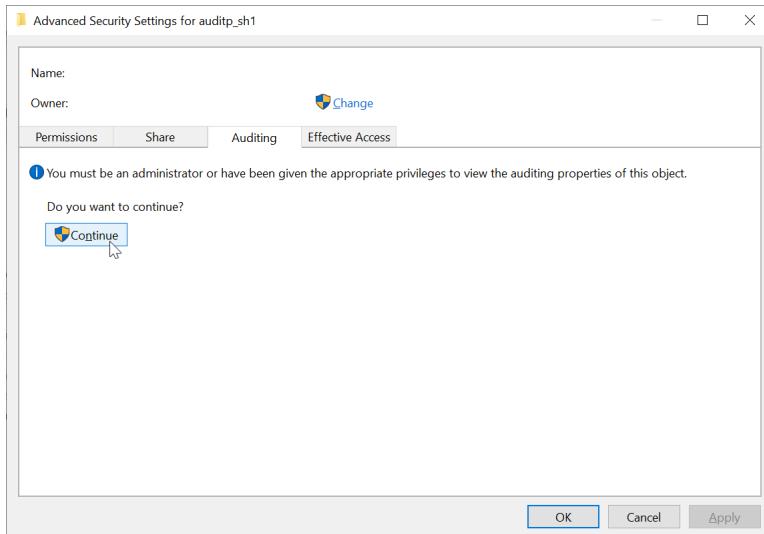
1. On the Windows client, select the connected IntelliFlash SMB share's file or folder that you want to audit, right-click and select **Properties**.



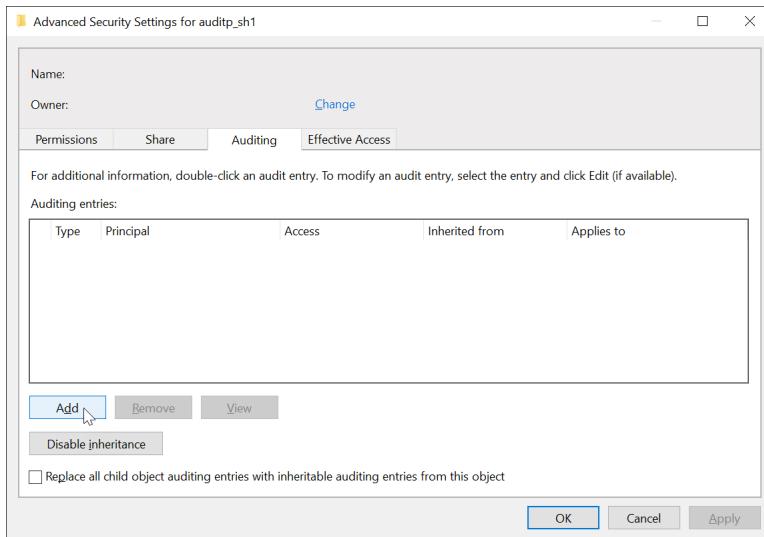
2. Select the **Security** tab and then click **Advanced**.



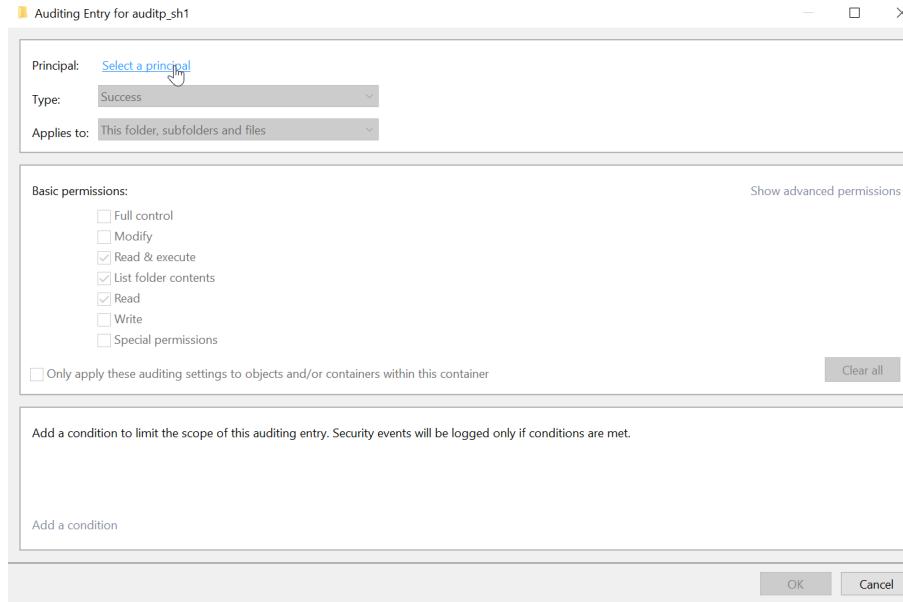
3. In the **Advanced Security Settings** dialog box, click the **Auditing** tab and then click **Continue**.



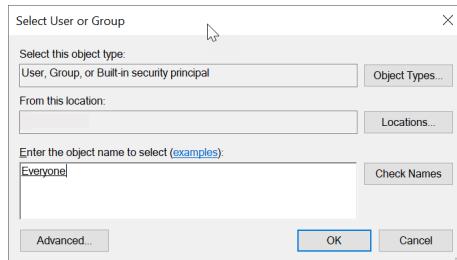
4. In the **Advanced Security Settings** dialog box, click **Add**.



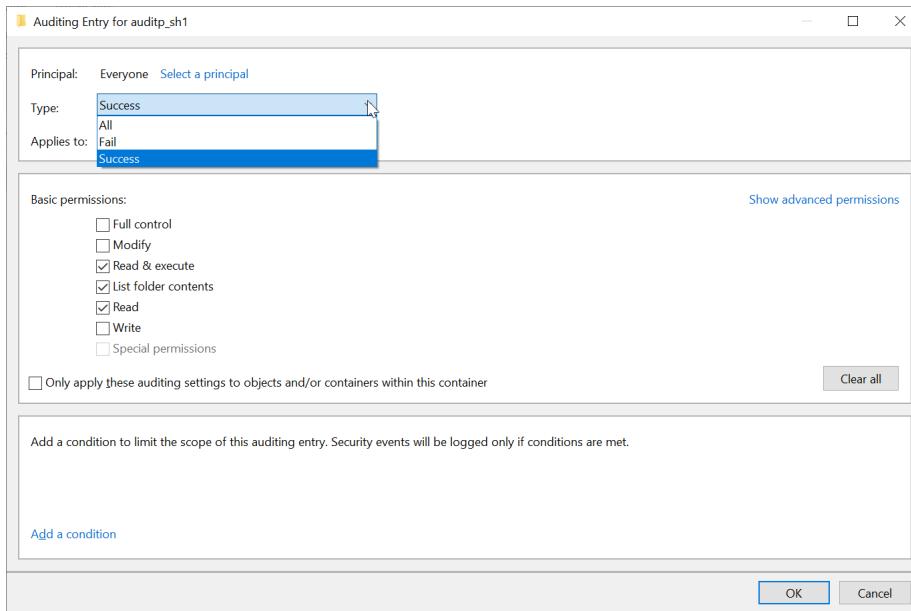
5. In the **Auditing Entry** dialog box, click **Select a principal**.



- In the **Select User or Group** dialog box, type the names of the users and groups to audit. For example, type **Everyone** so that all users are audited.

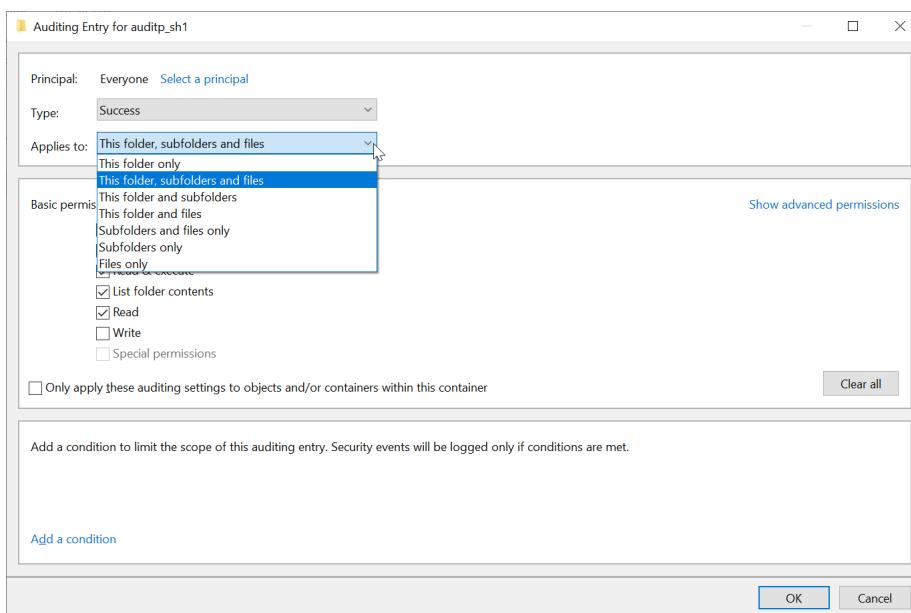


- After selecting the principal, in the **Type** list in the **Auditing Entry** dialog box, select **Successful**, **Failed**, or **All** for auditing successful events, failed events, or all events.



8. In the **Applies to** list in the **Auditing Entry** dialog box, select the objects to which the audit of events apply:

- This folder only
- This folder, subfolders and files
- This folder and subfolders
- This folder and files
- Subfolders and files only
- Subfolders only
- Files only

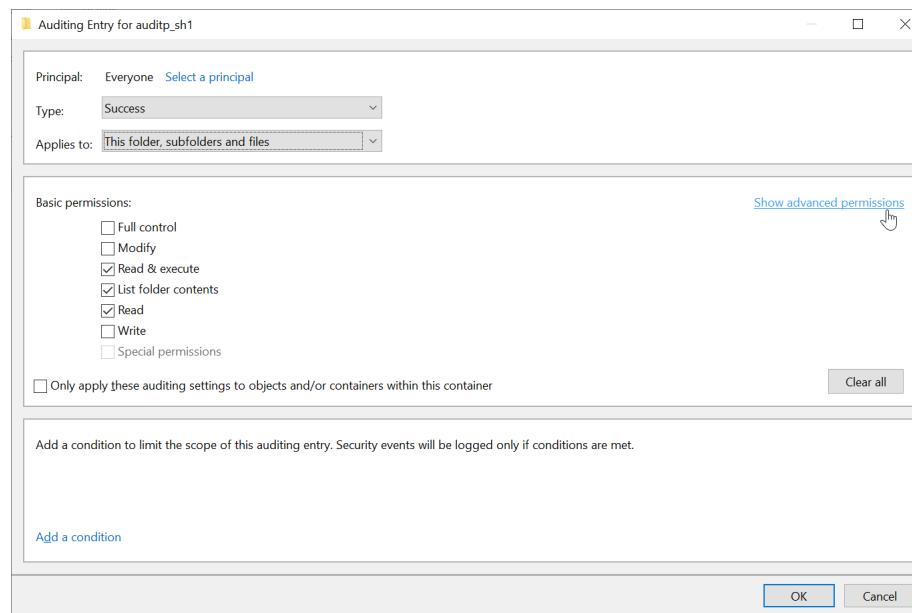


9. By default, the following **Basic Permissions** are selected for auditing:

- Read and execute
- List folder contents
- Read

Additionally, you can also select the following basic permissions: **Full control**, **Modify**, and **Write**.

Click **Show Advanced Permissions** to view additional permissions.



10. In the **Auditing Entry** dialog box, click **OK**.

## Configuring Auditing for NFS Shares through the Windows Client

To set audit SACLs for the NFS share, you need to mount the NFS share on a Windows system and use the Windows UI.

To configure auditing for an NFS share, do the following:

1. Mount the NFS share on the Windows client.
2. Set audit SACLs on the NFS share from the Windows client.

This process is same as configuring SMB shares. For more information, see the [Configuring SMB Shares](#) topic.

After the audit SACLs is set, mount the NFS share on the Linux System and start performing operations. IntelliFlash starts recording auditing events for the NFS shares.

## Configuring Audit Share Quota

---

Quota is the maximum size that the audit log share can grow to. Quota applies to space needed to log audit events for both the pools. Quota is measured in gibibyte (GiB). 1GiB is  $2^{30}$  bytes.

By default, the quota size for an audit log share is set to 1024GiB (1TiB). The minimum quota size is 50GiB, while the maximum is 5120GiB (5TiB).

Each pool has one audit log share. However, if both pools are on the same controller, then all the events are logged to the audit share in one pool. For example, suppose pool-a and pool-b are in controller-A. The events from both pool-a and pool-b are recorded in the same audit share.

To configure the quota size for audit shares, complete the following steps:

1. From the **Services** menu, select **NAS** and then click **Audit**.
2. In the **Audit** page, click **Config**.
3. In the **Quota** section, specify the number (in GiB) that the audit log share can grow to.
4. Click **Save**.

Based on the threshold levels defined, notifications appear in the IntelliFlash Web UI when the audit share space usage reaches warning levels and critical levels.

Each audit log share must have enough quota. Otherwise, the audit events are not saved. Increase the quota size when the quota size reaches warning or critical levels.

## Configuring Space Usage Threshold Levels

---

The warning and critical space usage thresholds are defined in percentage. When the audit share space usage reaches the defined warning and critical levels, notifications appear in the IntelliFlash Web UI.

If the space usage thresholds are not defined, the default system values are considered. The default warning notification is set to 60%, while the critical percentage is set to 80%.

To configure the threshold levels, complete the following steps:

1. From the **Services** menu, select **NAS** and then click **Audit**.
2. In the **Audit** page, click **Config**.
3. In the **Thresholds** section, enable **Edit audit log thresholds**.
4. Enter the values for **Warning Threshold %** and **Critical Threshold %**.
5. Click **Save**.

## Configuring Retention Policy of Audit Logs

---

Retention policy determines the number of days that the audit events are stored in the audit log share. The default retention period is 30 days. The minimum log retention period is also 30 days.

To configure retention policy, complete the following steps:

1. From the **Services** menu, select **NAS** and then click **Audit**.
2. In the **Audit** page, click **Config**.
3. In the **Retention policy** section, specify the number of days for which the audit logs can be stored.
4. Click **Save**.

## Generating XML Audit Logs on Demand

---

The Audit logs are collected in binary form on the audit log share. The binary logs are then generated into XML files once in every 24 hours. However, you can generate the XML logs of the most recent events on demand.

The XML files are stored in the XML directory of the audit log share.

To generate the most current XML logs on demand,, complete the following steps:

1. From the **Services** menu, select **NAS** and then click **Audit**.
2. In the **Audit** page, click the **Audit logs** tab.
3. In the **Update audit logs** section, click **Start**.

## Enabling SMB Access of Audit Log Share

---

To enable SMB access of audit log share, complete the following steps:

1. In the **Audit** page, click the **Audit logs** tab.
2. In the **NFS and SMB Access** section, click the **SMB** tab.
3. Enable **SMB Sharing**.
4. Click **OK** in the **Confirmation** screen.

The path name of the Audit log share is shown in this section. The audit log share name is generated automatically. For SMB access, use the full name of the audit log (including the \$ symbol).

5. To control the systems that access the audit log share, you can add network ACLs. In **SMB Access** section, click **Add**.

The **Add Network ACLs** dialog box appears.

6. In the **Access Type** list, select **IP or FQDN**.

The **Access Mode** is always **Read-Only**.

7. Provide the FQDN or the IP address of the client host.

8. Click **Add**.

## Enabling NFS Access of Audit Log Share

---

The NFS protocol does not grant root access for audit shares.

To enable NFS access of audit log share, complete the following steps:

1. In the **Audit** page, click the **Audit logs** tab.

2. In the **NFS and SMB Access** section, click the **NFS** tab.

3. Enable **NFS Sharing**.

4. Click **OK** in the **Confirmation** screen.

The path name of the Audit log share is shown in this section.

5. In the **NFS Access** section, click **Add**.

The **Add Network ACLs** dialog box appears.

6. In the **Access Type** list, select **IP or FQDN**.

The **Access Mode** is by default **Read-Only**.

7. Provide the FQDN or the IP address of the host.

8. Click **Add**.

## Connecting to Audit Log Share from NFS or SMB Client

---

To access audit log share from an SMB client, do the following:

1. On the IntelliFlash system, enable SMB access for the audit log share.



**Note:** The path name of the audit log share appears when you enable SMB access. Use the full name of the audit log share (including the \$ symbol) to access it through an SMB client.

2. Add network ACLs, if you want to control which SMB clients can access the audit log share. For more information, see [Enabling SMB Access of Audit Log Share](#).
3. On the Windows client, map the SMB share using File Explorer.
  - a. Open File Explorer by pressing the Windows+E shortcut.
  - b. Navigate to **This PC** menu on the left. Under the **Computer** menu, select **Map network drive**.
  - c. Select the drive letter and enter the path of the audit log file share in the following format:

```
\\"<IP address or host name of the IntelliFlash system>\audit log share name
```

For example:

```
\\"mgt9-pool-a.eco8.local\pool-a_Audit_30096416$
```

- d. Check the **Connect using different credentials** checkbox. Select **Finish**.
- e. Select **More choices > Use a different account**. Enter the administrator credentials of the IntelliFlash system that contains the audit log share.
4. The audit log share is mapped. Browse through the share to access the XML files.

To access audit log share from an NFS client, do the following:

1. On the IntelliFlash system, enable NFS access for the audit log share.



**Note:** The mount point of the audit log share appears when you enable NFS access.

2. Add network ACLs, if you want to control which NFS clients can access the audit log share. For more information, see [Enabling NFS Access of Audit Log Share](#).
3. Mount the audit log share on the NFS client using the following command:

```
mount -o vers=<NFS Version> <Data IP Address>:<Mount Point of Share>
<Local Directory>
```

For example:

```
mount -o vers=3 192.100.24.22:/pool-a/Audit /mnt/Audit
```

Here, Audit is the audit log share in pool-a of the IntelliFlash system. /mnt/Audit is the local directory on the NFS client.

## XML Log Reports Examples

---

The following sections list examples of XML audit logs recorded for a few audit events.

### Example 1: XML Log for Creating a File

```
</record>
<record version="2" event="SACL-based File Access Auditing"
host="IF.test.com"
iso8601="2022-05-19 18:08:42.947 +05:30">
<path>/export/NFS_Audit_Testing/auditshare</path>
<access mask>add_file/write_data</access mask>
<subject audit-uid="nfsuser1" uid="nfsuser1" gid="6020" ruid="nfsuser1"
rgid="6020"
pid="6143" sid="241963356" tid="0 1010 192.100.100.39"/>
</record>
```

### Example 2: XML Log for Writing a File

```
</record>
<record version="2" event="SACL-based File Access Auditing"
host="IF.test.com"
iso8601="2022-05-23 08:33:53.670 +05:30">
<path>/export/NFS_Audit_Testing/auditshare/file.txt</path>
<access mask>add_file/write_data</access mask>
<subject audit-uid="nfsuser1" uid="nfsuser1" gid="6020" ruid="nfsuser1"
rgid="6020" pid="6143" sid="1653826240" tid="0 1010 192.100.100.39"/>
</record>
```

### Example 3: XML Log for Deleting a File

```
</record>
<record version="2" event="SACL-based File Access Auditing"
host="IF.test.com"
iso8601="2022-05-20 11:45:46.522 +05:30">
<path>/export/NFS_Audit_Testing/auditshare/file.txt</path>
<access mask>delete</access mask>
<subject audit-uid="nfsuser1" uid="nfsuser1" gid="6020" ruid="nfsuser1"
rgid="6020" pid="6143" sid="684385116" tid="0 1010 192.100.100.39"/>
</record>
```

### Example 4: XML Log for Locking a File

```
</record>
```

```
<record version="2" event="SACL-based File Access Auditing"
host="IF.test.com"
iso8601="2022-06-23 17:28:33.993 +05:30">
<path>/export/NFS_Audit_Testing/auditshare/adil-ldap.test/lockfile8153</path>
<access mask>read_attributes</access mask>
<subject audit-uid="nfsuser1" uid="nfsuser1" gid="6020" ruid="nfsuser1"
rgid="6020" pid="14856" sid="1665758068" tid="0 966 192.100.100.39"/>
</record>
```

### Example 5: XML Log for Renaming a File

```
Deleting the existing file:
</record>
<record version="2" event="SACL-based File Access Auditing"
host="IF.test.com"
iso8601="2022-05-23 12:34:59.596 +05:30">
<path>/export/NFS_Audit_Testing/auditshare/Adnt.txt</path>
<access mask>delete</access mask>
<subject audit-uid="nfsuser1" uid="nfsuser1" gid="6020" ruid="nfsuser1"
rgid="6020" pid="6143" sid="3717357735" tid="0 1010 192.100.100.39"/>
</record>
Creating a new file:
</record>
<record version="2" event="SACL-based File Access Auditing"
host="IF.test.com"
iso8601="2022-05-23 12:34:59.596 +05:30">
<path>/export/NFS_Audit_Testing/auditshare</path>
<access mask>add_file/write_data</access mask>
<subject audit-uid="nfsuser1" uid="nfsuser1" gid="6020" ruid="nfsuser1"
rgid="6020" pid="6143" sid="3717357735" tid="0 1010 192.100.100.39"/>
</record>
```

---

# Chapter 14

---

## SAN Services

---

**Topics:**

- *Introduction to iSCSI and Fibre Channel*
- *SAN Services Overview*
- *LUN Mappings*
- *Understanding NPIV*
- *iSCSI Page*
- *Fibre Channel page*

## Introduction to iSCSI and Fibre Channel

---

### iSCSI

Internet Small Computer System Interface (iSCSI) is one of the block protocols supported by IntelliFlash systems.

The iSCSI initiator is a client that relays SCSI commands to an iSCSI target on a storage array over an Internet Protocol (IP) network. It communicates with an iSCSI target, which is usually a storage device that supports the iSCSI protocol.

The iSCSI protocol supports the Challenge-Handshake Authentication Protocol (CHAP) for authentication. CHAP is a Point-to-Point Protocol (PPP) for authentication. CHAP can be used for uni-directional or bi-directional authentication.

Uni-directional CHAP is commonly used with iSCSI to ensure that only authorized users access the data. To use uni-directional CHAP, you have to provide the initiator secret to the IntelliFlash Array.

Mutual CHAP provides bi-directional authentication protection between the initiator and the target. It requires the initiator to authenticate the target, and also the target to authenticate the initiator. You can use bi-directional CHAP to secure iSCSI connections. Set up a CHAP user name and password on the target side by choosing the CHAP authentication method when you create the iSCSI target.

 **Note:** IntelliFlash systems do not support Internet Storage Name Service (iSNS) for automatic discovery of iSCSI targets.

### Fibre Channel

Fibre Channel (FC) is a high-speed network technology that is primarily used for connecting one or more systems to data storage. FC commonly operates at 2-, 4-, 8- and 16-Gbps transfer rates.

IntelliFlash systems can support 2-, 4-, 8- and 16-gigabits per second transfer rates. The actual transfer rate also depends on the speeds supported by the FC switch connected to the array.

 **Note:** If the highest speeds of the array and the FC switch do not match, the two devices negotiate and use the highest speed supported by both—provided the "auto-negotiate" mode is enabled on the FC switch.

## SAN Services Overview

---

IntelliFlash systems support both the SAN protocols—Fibre Channel (FC) and iSCSI—for block-based access.



**Important:** Use the Tintri-provided 10-GbE and FC cards on the array for iSCSI and FC access respectively.

In a direct attached FC configuration, both FC-AL (loop mode) and Point-To-Point topologies can be configured. IntelliFlash systems, however, support only Point-To-Point topology, and do not support FC-AL (loop mode).

## Target Groups and Initiator Groups

An initiator in the context of the block protocols (iSCSI and FC) is a host- or client-side endpoint that uses the storage LUN. Correspondingly, a target is the endpoint on the array that provides the LUN.

The IntelliFlash OS groups both FC and iSCSI targets and initiators into target groups and initiator groups for easier management of SAN endpoints. Target groups and initiator groups are logical group that enables you to associate LUNs and projects with initiators and makes it easier for you to control the access to the LUNs. Initiator groups and target groups are protocol-specific. iSCSI initiators and iSCSI targets can be only added to iSCSI initiator groups and iSCSI target groups. FC initiators and FC targets can only be added to FC initiator groups and FC target groups.

## Default Fibre Channel Targets and Target Groups

The default targets and target groups for FC are created at the array level during the initial configuration of the array. By default, IntelliFlash systems that ship with FC cards include the default FC target groups. The default FC target groups include the FC targets on the array. In addition, IntelliFlash Operating Environment automatically creates an NPIV port (also called virtual FC port) for each FC port in a pool. A default NPIV target group is also created for every pool. The NPIV ports associated to the pool are added to the default NPIV target group. You cannot delete the default FC target groups and virtual FC target groups.

You can view the default FC targets and target groups in the **FC** page. To access this page, click **Services > SAN > FC**.

## Default iSCSI Targets and Target Groups

The IntelliFlash Operating Environment automatically creates a default iSCSI target and a default iSCSI target group when you create a pool. The default target is automatically associated with the default target group.

The IntelliFlash OS automatically recognizes the floating IP addresses (except those created on management interfaces) in the resource group during pool creation and binds them with the iSCSI default target. All new floating IP addresses (except those created on management interfaces) that are added to the resource group of the pool are also automatically bound with

the default iSCSI target. Further, the IntelliFlash OS automatically binds all floating IP addresses created over 10-GbE interfaces with the default iSCSI target of the same resource group.

You can bind floating IP addresses with multiple iSCSI targets. Therefore, you can bind the floating IP addresses that are bound to default iSCSI target with custom iSCSI targets also.

 **Note:**

- You can edit the default iSCSI targets to add or remove floating IP addresses. However, avoid removing floating IP addresses from the default iSCSI target.
- Floating IP addresses over 1-GbE interfaces are not automatically bound to the default target. Users who have only 1-GbE interfaces need to modify the default target and add the required floating IP addresses.

If you delete a pool, then the related default target and default target group are also deleted. Otherwise, you cannot delete the default iSCSI target and target group.

 **Note:** Use the Default Target unless you have a specific need for a separate target.

You can manage the default iSCSI targets and target group in the **iSCSI** page. To access this page, click **Services > SAN > iSCSI**.

## LUN Mappings

---

To expose a LUN to a host, you need to first define a LUN mapping. LUN mappings are defined in the IntelliFlash Web UI by associating a LUN with an initiator group and a target group. When you map a LUN or a project with a target group, they are associated with all the targets in the selected target group. As an initiator group can have multiple initiators, you can expose a LUN to multiple hosts by mapping it to one initiator group.

 **Note:** A LUN mapping may also use the **ALL** keyword instead of a specific initiator group. If a LUN mapping has the **ALL** keyword for the initiator group, any initiator can view and use the LUN by accessing a target in the mapped target group.

You can map a LUN or a project with a target group either when creating the project or LUN, or when modifying them.

LUN mappings have the following features:

- A LUN can have multiple LUN mappings.
- Initiator groups and target groups can be used in multiple LUN mappings, if required.
- You can add multiple targets to a target group. However, a target can be associated with only one target group.

- You can add multiple initiators to a initiator group. However, an initiator can be associated with only one initiator group.
- For iSCSI, multiple floating IP addresses can be bound to a single iSCSI target.

## Understanding NPIV

---

IntelliFlash creates an NPIV port (also called virtual FC port) for each Fibre Channel port associated to a storage pool. IntelliFlash creates a default NPIV target group for every pool, and adds the NPIV ports to the default NPIV target group.

For example, assume that a controller consists of two pools (pool-a and pool-b) and one dual-port Fibre Channel card. The system automatically creates two NPIV ports (one NPIV port for each FC port) for pool-a and two NPIV ports for pool-b. It then creates a default NPIV target group for each pool and adds the NPIV ports associated with the pool to the target group.

The NPIV ports access the FC fabric through the physical HBA FC ports and maintain their WWPN identities across controllers. When the IntelliFlash LUNs are mapped with NPIV ports, the hosts only see the active paths to the LUNs. There are no standby paths. This simplifies the switchover of resources between controllers. During a failover, NPIV transparently redirects host FC traffic without involving the multi-pathing layer of the host, which is often error prone in detecting path state changes and might result in path loss.

Additionally, NPIV simplifies FC adapter replacement. You no longer have to:

- Reconfigure FC zones on the switches
- Boot from SAN information in the host's BIOS
- Modify LUN mapping information on IntelliFlash

When you replace an FC card, the same WWPN identities of the old FC card are used for the new card.

The **Fibre Channel NPIV Ports** section in the **Settings > Network > Interface** page displays the NPIV ports. Each NPIV port is identified by its world wide port name (WWPN), and is associated to a pool and a physical Fibre Channel port from each controller. The NPIV ports also appear in the **Settings > High Availability** page.

You can view the NPIV ports and the default NPIV target groups in the **Services > SAN > FC** page.

## Hardware Requirements for Supporting NPIV

Make sure that the FC adapters in both the controllers meet the following hardware requirements:

- **8G or 16G FC adapter:** A minimum of one 8G or 16G FC adapter needs to be present in each controller.
- **Fabric topology:** Make sure your SAN environment uses a Fabric topology. NPIV ports are supported only with Fabric topology, and not with Point-to-Point topology.
- **FC Switch:** The FC switch must have NPIV enabled on all ports connected to the array and the client.

## Support Considerations for NPIV

The following factors must be considered for the NPIV feature to work properly:

- **No support for Point-to-Point Topology:** The NPIV feature works only in the Fabric topology. If a Point-to-Point topology is detected, the system automatically disables the NPIV feature.
- **No additional FC target groups:** No additional FC target groups must exist other than the default FC target group. If there are additional FC target groups, the NPIV feature is not enabled.
- **New FC cards:** When new FC cards are added, the system automatically creates new NPIV ports. Make sure that you add new FC cards to both the controllers. The number of FC cards on both the controllers must be equal.
- **FC card replacement:** When you replace an FC card, the same WWPN identities of the old FC card is used for the new card.
- **Limitation of 32 NPIV ports per physical FC port:** You cannot create more than 32 NPIV ports on a physical FC port.

## Migrating Non-NPIV Projects to NPIV after Upgrading to 3.7.x.x or Later

NPIV is enabled when the array is upgraded to version 3.7.x.x or later. After the upgrade, the migration of a LUN from a physical HBA FC target group to a default NPIV target group is performed at a project level to avoid disruption.

### Step 1: Creating NPIV Ports and NPIV Target Groups (System Action)

After upgrading to 3.7.x.x or later, IntelliFlash does the following:

- Creates an NPIV port for each FC physical port for every pool in the controller.
- Creates a default NPIV target group per pool, and adds all the NPIV ports associated to the pool into the default NPIV target group.
- Adds the newly created default NPIV target group to the LUN or Project level mappings.

### Step 2: Zoning the NPIV Ports (User Action)

After the system creates the NPIV ports and target groups, you must do the following:

- Zone the NPIV port WWPNs to the appropriate FC zone in the Fabric.

### Step 3: NPIV Ports Discovery by Initiators (System Action)

- After you zone the NPIV ports, the initiators discover the NPIV targets.
- When initiators discover the NPIV target groups, the **Use NPIV Ports** option appears in the **LUN Mappings** page in the IntelliFlash Web UI. This indicates that the LUN is now ready to be mapped to the NPIV target group and thus change its representation to ActiveOnly.

## Step 4: Migrating the Project (User Action)

Click **Use NPIV Ports** in the **LUN Mappings** page to change the LUN to ActiveOnly representation. After the LUN is migrated to ActiveOnly state, the physical FC target groups are deleted and only the NPIV target groups are listed in the **LUN Mappings** page.

 **Note:**

- Before you migrate the Boot from SAN (BFS) LUNs to NPIV, set the virtual target WWPNS in the boot parameters in the initiator card BIOS. If you do not make this change, the host OS does not reboot after migrating an existing BFS LUN to NPIV.
- If you migrate all the existing projects to ActiveOnly LUNs after upgrading to 3.7.x.x or later, then any new LUNs you create can only have ActiveOnly representation. If you still have projects that have not been migrated to ActiveOnly LUNs after the upgrade to 3.7.x.x or later, then the IntelliFlash Web UI provides you with the option to create either an ActiveOnly LUN or Active-Standby LUN. If you have not migrated any existing project yet, you can create only Active-Standby LUNs.

## iSCSI Page

You can manage the default iSCSI targets and target group in the **iSCSI** page. To access this page, click **Services > SAN > iSCSI**.

The iSCSI page consists of the following tabs:

- Targets
- Target Groups
- Initiators
- Initiator Groups

### Targets tab

The Targets tab displays the iSCSI target names, the alias name, the target groups they belong to, and the authentication mode. You can add or modify targets in this tab. You can delete user-created targets, but not the default targets.

### Target Groups tab

The Target Groups tab displays the default and user-created iSCSI target groups. You can add new target groups in this tab. You can remove targets from user-created target groups, but not from default target groups. You can also not delete the default target groups.

## Initiators tab

The Initiators tab displays the initiator names, the initiator groups they belong to, and the CHAP credentials for accessing initiators. You can add, modify, or delete initiators in this tab.

## Initiator Groups

The Initiator Groups lists the existing Initiator groups. You can add or delete initiator groups in this tab. You can also remove initiators from initiator groups.

## Adding an iSCSI Target

A target refers to the combination of an IQN, IP address, and the TCP port number by which an initiator can contact the target.

To manually add an iSCSI target, complete the following steps:

 **Note:** You cannot delete default iSCSI targets.

1. Click **Services > SAN > iSCSI**.
2. In the **iSCSI** page, click the **Targets** tab.
3. In the **Targets** tab, click **Add**.  
The **Add Target** dialog box appears.
4. In the **Add Target** dialog box, complete the following steps:
  - a) In the **Target Name** field, type the user specified portion of the IQN.  
The alias name field auto-populates with this user-specified portion of the IQN.
  - b) (Optional) Edit the auto-generated **Target Alias**.
  - c) In the **Select mode** field, select **Existing group** to add the target to an existing target group or select **New group** to create a new target group.
  - d) In the **Target Group** field, if you have selected **Existing group** in the previous step, select an existing target group from the list. If you have selected **New group**, type a new name to create a new target group.
  - e) Select the pool from the **Pool Group** list.
  - f) In the **Add Target IP** field, select one or more IP addresses to which the target will be bound, enter the TCP port (the default TCP port for iSCSI is 3260), and click **Add**.



### Important:

- For an HA system, use a floating IP address defined in the same resource group as the data pool.
- For single controller IntelliFlash systems, select the IP address of an interface group.

- g) To enforce authentication for the target, select an authentication type from the **Authentication** options.
- h) If you select the **CHAP** option, no additional information is required. CHAP enables the IntelliFlash OS to authenticate the iSCSI initiator.
- i) If you select the **Mutual** option, set the following values:
  - In the **CHAP User Name** field, type a user name.
  - In the **CHAP Secret** field, type the password.

 **Note:**

- When you enable **Mutual** option, CHAP credentials are required on both the iSCSI initiator and the iSCSI target.
- To view the password in the **CHAP Secret** field, select the **Show Secret** option.

5. Click **Add**.

See [Configurable iSCSI Target Properties](#) for more information on the properties that you can add.

The new target appears in the **iSCSI Targets** tab.

 **Note:** When you run a dynamic discovery from an initiator, the discovery result does not display the IntelliFlash OS targets that do not have a LUN mapping for the initiator. To view the target during dynamic discovery, you must create a LUN and map it to an initiator.

## Naming Conventions for iSCSI Targets and Target Groups

### Naming Conventions for the Default iSCSI Target

The default iSCSI target name has the standard iSCSI Qualified Name (IQN) format:

```
iqn.2012-02.com.tegile:<controller name>-<pool name>
```

The following is an example of a default iSCSI target name:

```
iqn.2012.02.com.tegile:array2-pool-new
```

This format includes the following:

- The name starts with the standard prefix: **iqn** followed by a dot (or period)
- The year and month in which the naming authority was established: **2012-02** followed by a dot (or period)
- The top-level domain of the naming authority in reverse order: **com.tegile** followed by a colon
- Unique name of the target, which includes:

- Hostname of the controller on which the pool was created, followed by a hyphen
- Pool name



**Note:** If the unique name is more than twenty characters, the IntelliFlash OS uses the first 20 characters of the name and appends the pool GUID to it.

## Naming Conventions for the Default iSCSI Target Group

The default iSCSI target group name has the following format:

```
default-<pool name>-iscsi-target-group
```

The following is an example of a default iSCSI target group name:

```
default-test_1_pool-iscsi-target-group
```

This format includes the following:

- The name starts with the string **default** followed by a hyphen
- Name of the pool



**Note:** If the pool name is more than twenty characters, the IntelliFlash OS uses the first 20 characters of the pool name and appends the pool GUID to it.

- The string **iscsi-target-group**

## Modifying an iSCSI Target

You can modify both the default and user-created iSCSI targets.



**Note:**

- You can modify a default target created along with the pool and modify the floating IP address which is bound to it. However, avoid removing floating IP addresses from the default iSCSI target.
- You cannot modify the name of an iSCSI target.

To modify an iSCSI target, complete the following steps:

1. Click **Services > SAN > iSCSI**.
2. In the **iSCSI** page, click the **Targets** tab.
3. In the **Targets** tab, select the target you want to edit and click **Edit**. The **Edit Target** dialog box appears.
4. In the **Edit Target** dialog box, make the required changes and click **Save**. See [Configurable iSCSI Target Properties](#) for more information on the properties that you can modify.

## Configurable iSCSI Target Properties

The following table describes the iSCSI target configurable properties:

Property	Description
Target Name	The IQN (iSCSI qualified name) for this target. This is the user-specified part of the IQN.
Target Alias	The name specified for the target.
Target Group Association	Assigns the target to a specific group. You can select an existing group or create a new group.
Target Group	Select an existing group or type a name for the new group and select its Pool Group.
Network Bindings	Combination of IP address and TCP port that an initiator will use to discover and connect to the target.
Authentication for Target	The type of authentication enabled for the target. Available options are: None, CHAP, and Mutual (bi-directional).
CHAP Username	If mutual CHAP authentication is enabled, provide the CHAP username. This is used by the initiator to authenticate the target.   <b>Note:</b> Only available when Mutual is selected in Authentication for Target.
CHAP Secret	If mutual CHAP authentication is enabled, provide the CHAP secret. This is used by the initiator to authenticate the target.   <b>Note:</b> Only available when Mutual is selected in Authentication for Target.

## Deleting an iSCSI Target

You cannot delete default iSCSI targets created along with the pool. To delete an user-created iSCSI target, complete the following steps.

1. Click **Services > SAN > iSCSI**.
2. In the **iSCSI** page, click the **Targets** tab.
3. In the **Targets** tab, select the target you want to delete and click **Delete**.
4. In the **Confirmation** dialog box, click **OK** to confirm the deletion.

## Adding an iSCSI Target Group

An iSCSI target group is a collection of iSCSI targets. It is a logical group that enables you to associate LUNs and projects with targets and makes it easier for you to control the access to the LUNs.

To add a target group, complete the following steps:

1. Click **Services > SAN > iSCSI**.
2. In the **iSCSI** page, click the **Target Groups** tab.
3. In the **Target Groups** page, click **Add**.  
The **Add Target Group** dialog box appears.
4. In the **Group name** field, type a name.
5. From the **Pool Group** list, select a pool.  
A Pool Group is a group of pools that are associated with an HA resource group. The **Pool Group** field displays all the pools that exist within an HA resource group.
6. In the **Available targets** section, select the iSCSI targets that you want to include in the group.

 **Note:** The IntelliFlash OS only displays those targets that are currently not associated with any existing target group.

7. Click **Add**.

## Modifying an iSCSI Target Group

You can remove an iSCSI target from an iSCSI target group.

 **Note:** You cannot remove targets from a default iSCSi target group.

To modify a target group, complete the following steps:

1. Click **Services > SAN > iSCSI**.
2. In the **iSCSI** page, click the **Target Groups** tab.
3. Select the target group name and click **Edit**.  
The **Target Group members and LUNs** dialog box appears.
4. In the **Target Group members and LUNs** dialog box, clear (uncheck) the target you want to remove.  
Click the **LUN List** tab to view the LUN path.
5. Click **Save**.

## Removing an iSCSI Target Group

To delete a target group, complete the following steps:



**Note:** You cannot remove default iSCSI target groups.

1. Click **Services > SAN > iSCSI**.
2. In the **iSCSI** page, click the **Target Groups** tab.
3. In the **Target Groups** page, select a target group name and click **Delete**.
4. In the **Confirmation** dialog box, click **Yes** to confirm deletion.



**Note:** If the target group is mapped to a LUN, you cannot delete the target group.

## Adding an iSCSI Initiator

You must manually add the iSCSI initiators that will access LUNs on the array. To add an iSCSI initiator, complete the following steps:

1. Click **Services > SAN > iSCSI**.
2. In the **iSCSI** page, click the **Initiators** tab.
3. In the **Initiators** tab, click **Add**.  
The **Add Initiator** dialog box appears.
4. In the **Add Initiator** dialog box, complete the following steps:
  - a) In the **Initiator name** field, type the initiator name.  
You must enter a valid node name, which can be either:
    - A reverse domain name in the format iqn.yyyy-mm
    - An EUI-64 bit identifier that has 16 ASCII encoded hexadecimal digits, such as eui.02004567A425678D.
  - b) Select the **Allow non-standard iSCSI initiator name** option to allow users to enter non-IQN or non-EUI based initiator names.
  - c) Select the **Initiator group association** from the list.
  - d) Select the **CHAP Credential** option to enable the array target to authenticate the initiator. Type the user credentials.
  - e) Click **Add**.

The new initiator appears in the **iSCSI Initiators** tab.

### Multipathing with the New iSCSI Initiator

To use multipathing with the new iSCSI initiator, do the following:

- If the initiator is on a Windows host running directly (bare metal) on the hardware or in a virtual machine hosted on Hyper-V or ESX/ESXi, install Microsoft MPIO.
- If the initiator is on a host running ESX/ESXi, configure the VMware SATP rules that are provided by Tintri.

## Modifying an iSCSI Initiator

To modify an iSCSI initiator, complete the following steps:

 **Note:** You cannot modify the name of the initiator. However, you can modify other properties.

1. Click **Services > SAN > iSCSI**.
2. In the **iSCSI** page, click the **Initiators** tab.
3. In the **Initiators** tab, select the initiator you want to edit and click **Edit**. The **Edit Initiator** dialog box appears.
4. In the **Edit Initiator** dialog box, make the required changes and click **Save**.

## Deleting an iSCSI Initiator

To delete an iSCSI initiator, complete the following steps:

1. Click **Services > SAN > iSCSI**.
2. In the **iSCSI** page, click the **Initiators** tab.
3. In the **Initiators** tab, select the initiator you want to delete and click **Delete**.
4. In the **Confirmation** dialog box, click **Yes** to confirm deletion.

## Adding an iSCSI Initiator Group

An iSCSI initiator group is a collection of iSCSI initiators. It is a logical group that enables you to associate LUNs and projects with initiators and makes it easier for you to control the access to the LUNs. To add an iSCSI initiator group, complete the following steps:

1. Click **Services > SAN > iSCSI**.
2. In the **iSCSI** page, click the **Initiator Groups** tab.
3. In the **Initiator Groups** page, click **Add**. The **Add Initiator Group** dialog box appears.
4. In the **Group Name** field, type a name for the group.
5. Select the initiators that you want to include in the group from the **Available Initiators** list.

Only those initiators that are currently not associated with any initiator group appear in this list.

6. Click **Add**.

## Modifying an iSCSI Initiator Group

You can remove an iSCSI initiator from an iSCSI initiator group.

To modify an iSCSI initiator group, complete the following steps:

1. Click **Services > SAN > iSCSI**.
2. In the **iSCSI** page, click the **Initiator Groups** tab.
3. In the **Initiator Groups** page, select the initiator group and click **Edit**.  
The **Initiator Group members and LUNs** dialog box appears.
4. Uncheck the initiator you want to remove from the group. In the **Confirmation** dialog box, click **Yes** to confirm.
5. Click **Save**.

## Removing an iSCSI Initiator Group

To delete an iSCSI initiator group, complete the following steps:

1. Click **Services > SAN > iSCSI**.
2. In the **iSCSI** page, click the **Initiator Groups** tab.
3. In the **Initiator Groups** page, select the initiator group you want to delete and click **Delete**.
4. In the **Confirmation** dialog box, click **Yes** to confirm deletion.

## Fibre Channel page

---

In the **FC** page, you can view the default FC targets and target groups. Also, you can manage the FC initiators and initiator groups. To access this page, click **Services > SAN > FC**.

The FC page consists of the following tabs:

- Targets
- Target Groups
- Initiators
- Initiator Groups

### Targets tab

The Targets tab displays the FC target names, the status (green indicates target is online, orange indicates target is offline), the default FC target groups they belong to, the target type

(NPIV or HBA), the node that the targets are active on, the initiators that are connected to the target, and the port speeds.

You cannot delete the default FC targets. You can reset the FC cards by clicking **Reset**.

### Target Groups tab

The Target Groups tab displays the default FC target groups and the default virtual FC target groups. You can also view the targets associated to the target group and the LUNs mapped to the target group. To view additional details of the default target groups, select the default target group and click **Details**.

You cannot delete default FC target groups or remove targets from the default target groups.

### Initiators tab

The Initiators tab displays the initiator names, the initiator groups they belong to, and the FC targets connected to the initiators. You can add, modify, or delete initiators in this tab.

### Initiator Groups

The Initiator Groups lists the existing Initiator groups. You can add or delete initiator groups in this tab. You can also remove initiators from the initiator groups.

## Adding an FC Initiator

FC initiators that are accessible by the IntelliFlash Array automatically appear on the **FC Initiators** page. If the FC ports are not connected to an FC switch, initiators do not appear on the **FC Initiators** page.

You can manually add FC initiators as well. Use this feature when configuring a virtual WWN (world wide name) for NPIV (N-port ID virtualization), or when the FC ports are not connected to an FC switch.

To manually add an FC initiator, complete the following steps:

1. Click **Services > SAN > FC**.
2. In the **FC** page, click the **FC Initiators** tab.
3. In the **FC Initiators** tab, click **Add**.  
The **Add Initiator** dialog box appears.
4. In the **Add Initiator** dialog box, complete the following steps:
  - a) In the **Initiator name** field, type an initiator name.



**Note:** All FC initiator names must begin with wwn.

- b) In the **Select mode** field, select **Existing group** to add the initiator to an existing initiator group or select **New group** type to create a new initiator group.
  - c) If you have selected the **Existing group** option in the previous step, select an existing initiator group from the **Initiator Group** list. If you have selected the **New group** option in the previous step, type a new name in the **Initiator Group** field to create a new initiator group.
5. Click **Add**.

## Modifying an FC Initiator

You can move FC initiators to a different FC initiator group.

To move an FC initiator, complete the following steps:

1. Click **Services > SAN > FC**.
2. In the **FC** page, click the **FC Initiators** tab.
3. In the **FC Initiators** tab, select the FC initiator you want to edit and click **Edit**.
4. To change the FC initiator group, perform one of the following steps:
  - Select a different initiator group from the **Initiator Group** drop down list.
  - To add the initiator to a new initiator group, select the **New group** option in **Mode** and type a new group name in the **Initiator Group** field.
5. Click **Save**.

## Adding an FC Initiator Group

An FC initiator group is a collection of FC initiators. It is a logical group that enables you to associate LUNs and projects with initiators and makes it easier for you to control the access to the LUNs. To add an FC initiator group, complete the following steps:

1. Click **Services > SAN > FC**.
2. In the **FC** page, click the **FC Initiators** tab.
3. In the **FC Initiators** tab, click **Add**.  
The **Add Initiator Group** dialog box appears.
4. In the **Group Name** field, type a name for the group.
5. Select the initiators that you want to include in the group from the **Available Initiators** list.  
Only those initiators that are currently not associated with any initiator group appear in this list.
6. Click **Save**.

## Modifying an FC Initiator Group

You can remove initiators from an initiator group.

To remove an initiator, complete the following steps:

1. Click **Services > SAN > FC**.
2. In the **FC** page, click the **FC Initiators** tab.
3. In the **FC Initiators** tab, select the initiator group and click **Edit**.  
The **Initiator Group members and LUNs** dialog box appears.
4. Clear (uncheck) the initiators that you want to remove from the group. In the **Confirmation** dialog box, click **Yes** to confirm.
5. Click **Save**.

## Removing an FC Initiator Group

To delete an FC initiator group, complete the following steps:

1. Click **Services > SAN > FC**.
2. In the **FC Initiators** page, click the **Initiator Groups** tab.
3. In the **Initiator Groups** page, select the initiator group and click **Delete**.
4. In the **Confirmation** dialog box, click **Yes** to confirm deletion.

---

# Chapter 15

---

## Live LUN Migration

---

**Topics:**

- *Overview of LUN Migration*
- *Prerequisites for Live LUN Migration*
- *Project Migration*
- *LUN Migration*
- *Monitoring the Migration*

## Overview of LUN Migration

---

Live LUN Migration moves data from LUNs on one IntelliFlash system to another or within the same array seamlessly serving data to the host without any downtime or disruption. During LUN migration, LUNs from one IntelliFlash system (source) are migrated to another array (destination) or within the same array. After the migration, the source is redirected to the destination LUN without any downtime. You can configure multiple migration jobs. The configured migrations are queued and are carried out one at a time.

### Types of Migration

#### *LUN Migration*

You can migrate an individual LUN to an existing or new project on the destination. After the migration, the destination LUN will have the same properties as the source LUN.

#### *Project Migration*

You can migrate multiple LUNs from a source to a destination. Only those LUNs which inherit the project properties can be migrated as part of project migration. LUNs can be migrated to a new or existing project.

## Prerequisites for Live LUN Migration

---

The following are the prerequisites for configuring and migrating Project and LUNs from source to destination:

- The destination pool should have sufficient free space. This ensures that there is sufficient space to migrate data without any error.
- Installing multipath I/O feature on the client host machine is recommended for seamless LUN migration.
- The floating IP address should be configured for the source and destination arrays. There should be at least one IP address that can be pinged from source to destination and vice versa, so that the source and destination can communicate with each other during LUN migration.
- The floating IP address of 1G is required, in the case of 10g or 40g cards.
- The source and destination arrays should be HA enabled. This ensures that even if anyone of source or destination controllers are not reachable, migration still continues.
- To configure project migration, there should be at least one LUN which inherits the project mappings. Project migration uses project mappings to migrate each configured LUN.
- You can migrate a project to another pool in the same array provided the pool resides in the other controller.
- The destination project should not have a LUN with the same name.
- The destination pool resource group should be online for migration.
- The array Management IP address should be configured for both source and destination arrays.
- Both source and destination arrays must be in the same network for the migration.

- MPIO (multipathing feature) should be enabled on all hosts in order to discover active and stand-by paths to target.
- The CPU usage of the controller for the destination pool should not exceed 80%.
- Configure network ports with 9000 MTU setting on both source and destination arrays, and on the switch ports.

 **Note:**

- Migration will fail if one of the source controller or one of destination controllers is not reachable during migration configuration and preparation.
  - LUNs which override project settings cannot be migrated through project migration and have to be migrated individually.
  - The host mappings that are added to the destination Project\LUN are restricted to those mapped to source. You can add new mappings once the migration is complete.
  - The earliest time that a migration can be scheduled is 30 minutes after the current migration time.
  - To add a new migration partner, destination host's array management IP should be used.
  - As part of project migration, you can configure up to 10 LUNs for migration. If there are more LUNs, a separate migration configuration should be created.

## Scenarios in which migration is not supported

- LUN or destination project mapped and accessed only using Array's FC Physical ports (Non NPIV) by host.
- Source or destination IntelliFlash version is earlier than 3.10.0.0 .
- For generic projects, project migration is not supported. LUNs in generic projects can be migrated only through LUN migration.
- The source project/LUN and destination project\LUN are using different protocol.
- Legacy LUN with product ID ZEBI-ISCSI.

## Project Migration

---

You can migrate multiple LUNs from a source to a destination. Only those LUNs which inherit project properties can be migrated as part of project migration.. The LUNs which override project settings have to be migrated individually. LUNs can be migrated to a new or existing project. Project migration creates new project on destination or uses existing project and migrates all the LUNs configured as part of migration. You can choose to migrate all the existing snapshots, migrate snapshots in range, or decide not to move any. The LUNs which have overriding properties cannot be migrated as part of Project Migration, but it can be migrated as part of [LUN Migration](#).

**Note:** Make sure that the [prerequisites](#) are met before starting the migration.

## Migrating a Project within an Array

You can migrate a project to another pool in the same array provided the pool resides in the other controller. Migration within an array is not supported if both the pools are in the same controller. All LUNs selected during configuration are migrated to the destination project.

To migrate a project to another pool in the same array, complete the following steps:

1. On the IntelliFlash **Web UI**, click **Provision > Projects**.
2. From the list of projects, select the project that you want to migrate.



**Note:** When you migrate a project, all the LUNs in the project are also migrated. The LUNs which have overriding properties cannot be migrated as part of Project Migration.

3. Under **Projects**, click **Manage > Migration**
4. In the **Migration** screen, click **New**. The **Migration Configuration Wizard** appears.
5. On the **Migration Configuration Wizard**:
  - a) Select a **Migration Partner**.
    1. Select **Current Array** if you want to migrate your data to another pool in the same array.
  - b) Under **Pool & Project**
    1. Select the pool to which you want to migrate.
    2. Select the project to which you want to migrate the LUNs. You can either move the LUNs to an another project in the same array or create a new project and then move the LUNs to the new project.
    3. Select the new project, and then click **Next**.
  - c) Under **Scope** all the LUNs in the project are listed.
    1. Select the LUNS you want to migrate. Click **Next**.
  - d) Under **Mapping**, the current target and initiator mappings are listed.
    1. Select the mapping for migration and click **Next**.
 

**Note:** Since the migration configuration is within the array, all the targets for destination pool and all the initiators from the array are listed. The default target is mapped to the initiator group which is available at the source. If you want to add more mappings click the Add + button or remove a mapping by clicking the remove - button in the mappings page. You can also edit an existing mapping.
  - e) Under **Snapshots**, you can choose to copy the existing snapshot to the destination project. You can select one of the following options:

- **Migrate all snapshots:** You can move all snapshots in the source project to the destination project.
  - **Migrate Snapshots in Range:** You can give a date from which you want to migrate snapshots from the source project to the destination project.
  - **Do not Migrate Snapshots:** You can decide not to move snapshots to the destination project.
6. Under **Preferences**, you can select options such as Schedule Migration, Cutover, and Test Connectivity before starting the migration.
- **Schedule Migration**
    1. Select **Start Migration Now** to start the migration immediately.
    2. Select **Schedule a Time** to set a date and time for migration.
-  **Note:**  

You can configure and schedule as many migrations that you require. However, IntelliFlash carries out only one migration at a time. The other configured migrations are queued as per the configured schedule.
7. **Cutover**
1. Choose **Automatically** if you want an automatic cutover after the migration.
  2. Choose **Manually** if you want human intervention during the cutover.
8. **Test Connectivity**
1. Enable test connectivity to check whether the mappings are correct in the host and target before starting the migrations. If the mappings are not correct, the migration may fail.
-  **Note:** The test connectivity checks whether the host is visible to the target. If the host is not visible to the target, an error message appears. You can then do a [manual cutover](#) and make sure that the mappings are correct to proceed with the migration.
9. **Summary**
- Shows all the configuration for migration. The source, destination, mapping, whether the snapshots in the project need to be migrated, the schedule, and the cutover for the migration.

Click **START**. The migration begins.

## Migrating a Project to a Remote Array

You can migrate a project to a remote array. When you migrate a project, all the LUNs in the project are migrated.

To migrate a project to a remote array, complete the following steps:

1. On the IntelliFlash **Web UI**, click **Provision > Projects**.
2. From the list of projects, select the project that you want to migrate.

 **Note:** When you migrate a project, all the LUNs in the project are also migrated. The LUNs which have overriding properties cannot be migrated as part of Project Migration.

3. Under **Projects**, click **Manage > Migration**
4. In the **Migration** screen, click **New**. The **Migration Configuration Wizard** appears.
5. On the **Migration Configuration Wizard**:
  - a) Select a **Migration Partner**.
    1. Click the option **New** if you want to migrate your data to a remote array. Enter a Hostname/IP, Username, and Password of the remote array.  
OR
    2. Click the option **Existing** if you want to migrate your data to an existing remote system. Then, select the IP of the remote array.
  - b) Under **Pool & Project**
    1. Select the pool to which you want to migrate.
    2. Select the project to which you want to migrate the LUNs. You can either move the LUNs to an another project in the remote array or create a new project and then move the LUNs to the new project.
    3. Select the new project, and then click **Next**.
  - c) Under **Initiators**

The initiators of the source project which are not available on the destination are listed. Create a new initiator group or choose an existing initiator group on destination where the new initiator needs to be added.

 **Note:**  
If the source project initiators groups are present in the destination, they are by default selected.

    1. Click the link to select the initiator and then click **Next**.
  - d) Under **Initiator Groups**
    1. Choose an Initiator group for the migration mapping.

 **Note:** If all the source project initiators are present in the destination, those initiator group will be selected by default.
  - e) Under **Scope** all the LUNs in the project are listed. Select the LUNS you want to migrate. Click **Next**.



**Note:** You can migrate up to 10 LUNS in a project.

- f) Under **Mapping**, the current target and initiator mappings are listed. You can add a new mapping or delete an existing mapping.
  - 1. Select the mapping for migration.
- g) Under **Snapshots**, you can choose to copy the existing snapshot to the destination project. You can choose one of the following options:
  - 1. **Migrate all snapshots**: You can move all snapshots in the source project to the destination project.
  - 2. **Migrate Snapshots in Range**: You can give a date from which you want to migrate snapshots from the source project to the destination project.
  - 3. **Do not Migrate Snapshots**: You can decide not to move snapshots to the destination project.
- h) Under **Preferences**, you can select options such as Schedule Migration, Cutover, and Test Connectivity before starting the migration.
  - **Schedule Migration**
    - 1. Select **Start Migration Now** to start the migration immediately.
    - 2. Select **Schedule a Time** to set a date and time for migration.



**Note:**

You can configure and schedule as many migrations that you require. However, IntelliFlash carries out only one migration at a time. The other configured migrations are queued as per the configured schedule.

- **Cutover**
  - 1. Choose **Automatically** if you want an automatic cutover after migration.
  - 2. Choose **Manually** if you want human intervention during the cutover.
- **Test Connectivity**
  - 1. Enable test connectivity to check whether the mappings are correct in the host and target before starting the migrations. If the mappings are not correct, the migration may fail.



**Note:** The test connectivity checks whether the host is visible to the target. If the host is not visible to the target, an error message appears. You can then do a [\*manual cutover\*](#) and make sure that the mappings are correct to proceed with the migration.

- i) **Summary**
  - Shows all the configuration for migration. The source, destination, mapping, whether the snapshots in the project need to be migrated, the schedule, and the cutover for the migration.

Click **START**. The migration begins.

## LUN Migration

You can migrate a LUN within an array, from one pool to another, or to a remote array. In LUN migration, you can migrate only one LUN to an existing or a new project in an array or a remote array.

Note: Make sure that the [prerequisites](#) are met before starting the migration.

### Migrating a LUN within an Array

You can migrate a LUN to another pool in the same array provided the pool resides in the other controller. Migration within an array is not supported if both the pools are in the same controller. Make sure that the prerequisites for LUN migration are met before you start the migration.

To migrate a LUN to another pool in the same array, complete the following steps:

1. On the IntelliFlash **Web UI**, click **Provision > Projects > LUN**.
2. From the list of LUNs, select the LUN that you want to migrate and click **Manage > Migration > Configure and Start**.



**Note:** You can migrate only one LUN at a time.

3. On the Migration window, click **New**. The Migration configuration wizard appears.
4. On the **Migration Configuration Wizard**:
  - a) Select a **Migration Partner**.
    1. Select **Current Array** if you want to migrate a LUN to another pool in this array.
    - b) Under **Pool & Project**
      1. Select the LUN you want to migrate. You can migrate only one LUN at a time. You can either move the LUN to an another project in the same array or create a new project and then move the LUNs to the new project.
      2. Enter the LUN name. You can choose to retain the existing LUN name in the destination or give a new name for the LUN.
      3. Click **Next**.
    - c) Under **Mappings**, the current target mapping is listed.
      1. Select the mapping for migration.
    - d) Under **Snapshots**, you can choose to copy the existing snapshot to the destination LUN. You can choose one of the following options:
      1. **Migrate all snapshots**: You can move all snapshots in the source LUN to the destination.
      2. **Migrate Snapshots in Range**: You can give a date from which you want to migrate snapshots from the source LUN to the destination.

- 3. **Do not Migrate Snapshots:** You can decide not to move snapshots to the destination.
- e) Under **Preferences**, you can select options such as Schedule Migration, Cutover, and Test Connectivity before starting the migration.
  - **Schedule Migration**
    1. Select **Start Migration Now** to start the migration immediately.
    2. Select **Schedule a Time** to set a date and time for migration.



**Note:**

You can configure and schedule as many migrations that you require. However, IntelliFlash carries out only one migration at a time. The other configured migrations are queued as per the configured schedule.

- **Cutover**

1. Choose **Automatically** if you want an automatic cutover after migration.
2. Choose **Manually** if you want human intervention during the cutover.

- **Test Connectivity**

1. Enable test connectivity to check whether the mappings are correct in the source and target before starting the migrations. If the mappings are not correct, the migration may fail.



**Note:** The test connectivity checks whether the host is visible to the target. If the host is not visible to the target, an error message appears. You can then do a *manual cutover* and make sure that the mappings are correct to proceed with the migration.

- f) **Summary**

- Shows all the configuration for migration. The source, destination, mapping, whether the snapshots in the project need to be migrated, the schedule, and the cutover for the migration.

Click **START**. The migration begins.

## Migrating a LUN to a Remote Array

You can migrate a LUN to a new remote system or an existing remote array. Make sure that the [prerequisites](#) for LUN migration are met before you start the migration.

To migrate a LUN to a new remote system or an existing remote array, complete the following steps:

1. On the IntelliFlash **Web UI**, click **Provision > Projects > LUN**.
2. From the list of LUNs, select the LUN that you want to migrate and click **Manage > Migration > Configure and Start**.



**Note:** You can migrate only one LUN at a time.

3. On the Migration window, click **New**. The Migration configuration wizard appears.
4. On the **Migration Configuration Wizard**:
  - a) Select a **Migration Partner**
    1. Click the option **New** if you want to migrate a LUN to a remote array. Enter a Hostname/IP, Username, and Password of the remote array.  
OR
    2. Click the option **Existing** if you want to migrate a LUN to an existing remote system. Then, select the IP of the remote array.
  - b) Under **Pool & Project**
    1. Select the LUN you want to migrate. You can migrate only one LUN at a time. You can either move the LUN to an another project in the same array or create a new project and then move the LUNs to the new project.
    2. Enter the LUN name. You can choose to retain the existing LUN name in the destination or give a new name for the LUN.
    3. Click **Next**.
  - c) Under **Initiators**

The initiators of the source LUN which are not available on the destination are listed. You can choose to add the initiator to the destination. Create a new initiator group or choose an existing initiator group on destination where the new initiator needs to be added.

    1. Click the link to select the initiator and then click **Next**.
  - d) Under **Initiator Groups**
    1. Choose an Initiator group for the migration mapping
  - e) Under **Mapping**, the current target and initiator mappings are listed. You can add a new mapping or delete an existing mapping.
    1. Select the mapping for migration
  - f) Under **Snapshots**, you can choose to copy the existing snapshot to the destination LUN. You can choose one of the following options:
    1. **Migrate all snapshots**: Move all snapshots in the source LUN to the destination.
    2. **Migrate Snapshots in Range**: You can give a date from which you want to migrate snapshots from the source LUN to the destination.
    3. **Do not Migrate Snapshots**: You can decide not to move snapshots to the destination.
  - g) Under **Preferences**, you can select options such as Schedule Migration, Cutover, and Test Connectivity before starting the migration.
    - **Schedule Migration**

1. Select **Start Migration Now** to start the migration immediately.
2. Select **Schedule a Time** to set a date and time for migration.

 **Note:**

You can configure and schedule as many migrations that you require. However, IntelliFlash carries out only one migration at a time. The other configured migrations are queued as per the configured schedule.

- **Cutover**

1. Choose **Automatically** if you want an automatic cutover after migration.
2. Choose **Manually** if you want human intervention during the cutover.

- **Test Connectivity**

1. Enable test connectivity to check whether the mappings are correct in the host and target before starting the migrations. If the mappings are not correct, the migration may fail.



**Note:** The test connectivity checks whether the host is visible to the target. If the host is not visible to the target, an error message appears. You can then do a *manual cutover* and make sure that the mappings are correct to proceed with the migration.

h) **Summary**

- Shows all the configuration for migration. The source, destination, mapping, whether the snapshots in the project need to be migrated, the schedule, and the cutover for the migration.

Click **START**. The migration begins.

## Monitoring the Migration

---

In the Migration page you can monitor migration jobs and see the timeline view of the migration process. During migration, the data is moved from one pool to another without interrupting the I/O. Data can be moved to the pool of a remote array or to the pool of the same array.

In the **Outbound** tab, you can view the destination project, the start time, the type of migration (Project or LUN), the number of LUNs to be migrated and the migration status. In this tab you can configure a **New** migration, **Abort** an ongoing migration, view and edit the migration **Configuration** for the selected migration, and **Restart** migration.

- Click **Configuration**, if you want to see the settings of the ongoing migration.
- Click **New** to configure a new migration.



**Note:** You can configure and schedule as many migrations that you require. However, IntelliFlash carries out only one migration at a time. The other configured migrations are queued as per the configured schedule.

### Different stages of the migration

In the **Outbound** tab of the **Migration** page, you can view the progress of the migration process in timeline view.

The flow of a configured migration is as follows:

**Successfully Configured > Preparing for Migration > Data Migration Started > Data Transfer Completed > Connection Established > Migration Completed.**

In the **Inbound** tab, you can view **Configuration** settings of the selected migration, the source project, the start time, the type of migration (Project or LUN), the number of LUNs to be migrated and the migration status.

### Related Topics:

[Aborting a Migration](#)

[Modifying the Migration Configuration](#)

[Restarting a Migration](#)

## Viewing Migration Status

You can view the status of all the configured migrations for a project in the **Migration > Status** page. You can also go to the **Project access page** to view the status of the migration.

Once you configure and start a migration, click **Project access page > Provision > Manage > Migration > Status** to view the status of all the configured migrations for a project.

- A rolling progress indicator is displayed next to the project or LUN that is being migrated. Hover over the rolling progress indicator to see whether it is an inbound migration or an outbound migration. Inbound migration indicates that the selected array or project is the destination for a migration. Outbound migration indicates that the selected project or LUN is being migrated.
- A green tick mark is displayed next to the project that is migrated successfully.
- Once a project or a LUN is successfully migrated, it is automatically deleted from the source after the cutover. The deleted LUN or project name is highlighted in red color in the project listing page.
- When a migration is going on, you cannot perform the following functions on the project page:
  1. Changing project settings. Projects settings are read-only.
  2. Modifying LUN level settings such as LUN size and threshold.
  3. Copying a LUN.
  4. Taking a new manual snapshot. Automatic snapshots are taken as per the existing schedules.
  5. Adding, editing, or deleting the snapshot schedules.
  6. Cloning, rollback, or deleting the snapshots.
  7. Configuring a new replication or deleting an existing one.

8. Adding or deleting project LUN mappings.
- IntelliFlash also displays notifications at every stage of migration. Click **Notifications** to view the migration notifications.

## Modifying the Migration Configuration

At any point, if the system aborts the configured migration due to technical errors, or if you want to change the settings or mappings of an existing migration, you can abort the migration and then go to the configuration tab to make the necessary changes and then **Restart** the migration.

You can modify existing migration configurations of a migration job if the status of the job is 'Aborted' or 'Error'. To change the configurations of a migration job at any other stage of migration, you need to first abort the migration job.

After aborting the migration job, proceed to the **Configuration** tab to modify **Mappings**, **Snapshots**, and other settings which are part of configuration and then **Restart** migration.

### Viewing the Migration Configuration Details

You can view the summary of the configuration for the selected migration.

Go to **Migration > Configuration > View**.

The **View Configuration Details** window appears. You can view the details on migration destination, mapping (target and initiator groups), snapshots selected for migration, the schedule of the migration and the cutover type (Automatic or Manual).

### Change Mappings

You can change the mappings of the migrated project.

Under **Mappings** you can add new initiators or delete existing initiators.

1. Click **Migration** tab and then select the migration project for which you want to change the mappings.
2. Click **Configuration > Mappings**.  
The **Edit Migration** window appears.
3. Click **Add +** to add a new target group or initiator group.
4. Click **Delete -** to delete a target group or initiator group.

### Change Snapshots

Under **Snapshots**, you can choose to copy the existing snapshots to the destination project.

1. Click **Migration** tab and then select the migration project for which you want to change the mapping.
2. Click **Configuration > Snapshots** for changing the snapshot settings. Select one of the options and save the changes.

- **Migrate all snapshots:** Move all snapshots in the source project to the destination project.
- **Migrate Snapshots in Range:** You can give a date from which you want to migrate snapshots from the source project to the destination project.
- **Do not Migrate Snapshots:** You can choose not to move snapshots to the destination project.

## Change Settings

Under settings you can change the schedule of the migration.

1. Click **Migration** tab and then select the migration project for which you want to change the mapping.
2. Click **Configuration > Settings** for changing the settings.
3. Under **Settings** you can change the migration schedule.
4. Update the date and time scheduled for migration.

## Deleting a Migration Configuration

You can delete a migration configuration once the migration is complete, in case there is an error, or if the migration is aborted.

To delete a migration configuration, complete the following steps:

1. Go to **Migration > Configuration > Delete**
2. Select the migration configuration that you want to delete.
3. Click **Delete**.

## Manual Cutover

You can choose **Manual cutover** or **Automatic cutover** during migration configuration. Manual cutover option is also enabled if the hosts that are mapped to source are not able to connect to the target. **Test Connectivity** checks whether the host is able to connect to the target. If the target is not visible to the host, an error message appears stating that the initiators are not connected. In this case you need to rescan to ensure that the hosts are now connected and then do a manual cutover.

To perform a manual cutover:

1. Select the migration configuration and click **Manual Cutover**.
2. Rescan and make sure that the problem is resolved.

After the manual cutover, the host is redirected to the target LUN and the I/Os are resumed to the target LUN. After the migration is complete, the source LUN is automatically deleted.

## Aborting a Migration

You can abort a migration at any stage before the cutover and after the initial configuration.

You can abort a migration in case you want to make the following changes to the configuration:

- Change the mappings.
- Change the existing migration settings.

To abort the migration, complete the following steps:

1. On the Migration page, click **Outbound** tab.
2. Select the configured migration that you want to abort and then click **Abort**. The migration is successfully aborted.



**Note:** The system may abort a migration in the following cases:

- Internal error during migration
- During same array migration, if there is a switchover of source or destination pool.

## Related Topics

[Change Mappings](#)

## Restarting a Migration

At any point, if you want to change the settings or mappings of an existing migration, you can **Abort** the migration and then go to the configuration tab to make the necessary changes and then **Restart** the migration. You can also restart the migration jobs that is in the 'Error' status after rectifying the error.

To restart a migration:

After making necessary changes to the [configuration](#), click **Restart**.



**Note:** The **Restart** option is enabled only if the migration is aborted or in case there is an error in the migration process.



---

# Chapter 16

---

## Synchronous Replication

---

**Topics:**

- *Introduction to Synchronous Replication*
- *Synchronous Replication Considerations*
- *Synchronous Replication Limitations*
- *Terms Used in Synchronous Replication*
- *Quorum Witness Server*
- *Setting up Synchronous Replication Configuration*
- *Editing Synchronous Replication Configuration*
- *Viewing Synchronous Replication Configuration*
- *Deleting Synchronous Replication Configuration*
- *Viewing Synchronous Replication Relationship Details*
- *Viewing Write Latency Details*
- *Deleting Synchronous Replication Relationship of a Project*
- *Disabling Auto Takeover Option*
- *Manual Takeover Using the Partner Array Web UI*
- *Manual Giveover Using the Source Array Web UI*
- *Enabling Auto Fallback*

## Introduction to Synchronous Replication

---

Synchronous Replication is a business continuity capability that maintains data consistency between iSCSI or FC LUNs on two IntelliFlash systems. Synchronous replication is configured between a source IntelliFlash array and a partner IntelliFlash array (1:1 topology). Synchronous replication ensures that both the source array and the partner array are in sync and that there is no data loss if the source array fails.

## Synchronous Replication Considerations

---

- Both the source and partner IntelliFlash arrays should be running on the same IntelliFlash version (3.11.0.0 or higher).
- IntelliFlash systems should be separated by a network round-trip-latency of no more than 10 milliseconds.
- IntelliFlash systems in the replication pair should be separated by a network round-trip-latency of no more than 200 milliseconds from the quorum witness server.
- IntelliFlash systems in a replication pair should communicate over Ethernet interface.

## Synchronous Replication Limitations

---

- A synchronous replication project cannot have a mix of active or standby LUNs.
- A synchronous replication project can be active on only one array.
- Synchronous replication cannot be set up on a project, if LUN migration is already configured on the array.
- Synchronous replication cannot be set up on a project, if asynchronous replication is already configured on the project.
- Rollback operation is not allowed on LUNs that have synchronous replication enabled.
- Up to a maximum of 10 LUNs are allowed in a synchronous replication project.
- Up to a maximum of 10 projects are allowed in a synchronous replication array pair.
- Offloaded data transfer (ODX) is not supported for synchronous replication.
- Snapshots cannot be deleted (either manually or when automatically scheduled) in synchronous replication projects, when the projects are syncing.
- Snapshot schedules on LUNs in a synchronous replication project cannot be modified as the LUNs inherit schedules from the project.
- A new LUN or a copy of LUN in a synchronous replication project is not replicated until the synchronous replication configuration is removed and added again.
- Clone creation is allowed on a synchronous replication project LUN through the Web UI or the REST API on the active array, except when replication is currently syncing or the snapshot has not replicated yet.
- Some IntelliFlash Data Protection Services (IDPS) and Veeam snapshots and clones are excluded from synchronous replication.

## Terms Used in Synchronous Replication

---

This section defines the terms used in the synchronous replication screens in the IntelliFlash Web UI.

### **Source Array**

The IntelliFlash Array from which the original data is replicated.

### **Partner Array**

The IntelliFlash Array that receives replicated data from the source array and stores the data securely for future use.

### **Quorum Witness Server**

The quorum witness server is a host-side component required for synchronous replication. Quorum Witness server helps IntelliFlash arrays to decide whether to do an automatic takeover in the event of a disaster.

### **Active Array**

The IntelliFlash Array where all the LUNs in a project are active.

### **Standby Array**

The IntelliFlash Array where all the LUNs in a project are on standby.

### **Replication Statuses**

- **In Sync:** The data between the source array and the partner array is identical, thus protecting the data. In this state, new data is synchronously written on both the arrays.
- **Out of Sync:** When the data replication between the source array and the partner array is paused.
- **Syncing:** When the data replication between the source array and the partner array is still in progress. The data between the source array and the partner array is not identical yet.

## Quorum Witness Server

---

The quorum witness server is a host-side component required for synchronous replication. The quorum witness server consists of 3 docker containers, one persistent docker volume, and a docker network.

The quorum witness server is deployed on a host that is network accessible by both the source array and the partner array targeted for synchronous replication. The quorum witness server helps the IntelliFlash arrays to decide whether to do an automatic takeover during a disaster.

## Downloading Quorum Witness Server Installation Package

To download the quorum witness server installation package, complete the following steps:

1. Click **Settings > Administration > Plugins**.
2. In the **Quorum Witness** section, click **Download**.

Untarring the quorum witness server package creates a new folder, `quorum_witness-<version>`.

The `quorum_witness-<version>` folder contains the following files:

- `docker-compose.yml`: Contains the docker deployment steps that `witness.sh` uses to install or deploy containers.
- `witness.sh`: Installation file (requires execute permission).
- `nginx.conf`: NGINX reverse proxy configuration file.
- `ReadMe` file: The ReadMe file contains detailed instructions on how to install the quorum replication witness server.

## Host Requirements

- The host (the system where the quorum witness server is installed) can be a physical machine, VM, or an EC2 instance.
- The host should be running CentOS Linux 7 or above.
- The docker should be installed on the host.
- The docker-compose should be installed on the host.
- The docker server must be running on the host.
- The host should have Internet connectivity to reach docker hub and quay.io for docker to download the required docker images.
- The host should have trusted CA signed certificate for witness server, if not a self-signed certificate should be created and imported into the IntelliFlash arrays.

## Installing Quorum Witness Server

1. Download the quorum witness server installation package from the IntelliFlash Web UI to the host.  
For more information, see [Downloading Quorum Witness Server Installation Package](#).
2. Make sure that the host has docker server running. Additionally, install docker and docker-compose on the host machine.  
For more information, see [Install Docker and Docker Compose \(Centos 7\)](#).

3. Untar the installation package in the host machine.

This creates a new folder, `quorum_witness-<version>`. The `quorum_witness-<version>` folder contains the following files:

- `docker-compose.yml`: Contains the docker deployment steps that `witness.sh` uses to install/deploy containers.
- `witness.sh`: Installation file (requires execute permission).
- `nginx.conf`: NGINX reverse proxy configuration file.
- `ReadMe` file: The `ReadMe` file contains detailed instructions on how to install the quorum replication witness server.

4. To use the quorum witness server, you need a signed certificate file and key file. If a trusted CA signed certificate is not available, create a self-signed certificate.

```
[root@localhost witness-host]# openssl req -x509 -nodes -days 365 -newkey rsa:2048
-keyout <output_key_file_name> -out <output_certificate_file_name>
-subj "/CN=<host_name>"
```

Replace `<host_name>` with the appropriate host name.

 **Note:** If you are using a self-signed certificate, import the certificate to IntelliFlash to enable access to the quorum witness server.

5. Install the quorum witness server (witness server and dependent containers) using the `witness.sh` file.

```
./witness.sh install -c <a PEM certificate file> -k <key file>
```

For example, using the `install` command might result in the following output:

```
[root@localhost quorum_witness-1.0.0]#
./witness.sh install -c ~/certs/cert.crt -k ~/certs/cert.key
Creating network "witness_network" with driver "bridge"
Creating volume "witness_dbase" with local driver
Pulling witness_etcd (quay.io/coreos/etcd:v3.3.13)...
Pulling witness_apisvr (nex/ifwitness:1.0.2)...
Pulling nginx-proxy (nginx:1.17.8)...
Creating witness_etcd ... done
Creating witness_apisvr ... done
Creating witness_nginx ... done
[root@localhost quorum_witness-1.0.0]#
```

After installation, additional folders are created for retaining certificate files and log files.

```
[root@localhost quorum_witness-1.0.0]# tree
.
├── certs
│   ├── cert.crt
│   └── cert.key
└── docker-compose.yml
```

```

└── witness.sh
    └── logs
        ├── nginx_logs
        │   └── error.log
        └── witness_apisvr_logs
            └── 2020_03_02_190234
    └── nginx.conf
    └── README
4 directories, 8 files
[root@localhost quorum_witness-1.0.0]#

```

 **Note:** If SELINUX is disabled in the host, update `ENABLE_UPDATE_CONTEXT=0` in `witness.sh` before running the install command.

## Verifying the Status of Quorum Witness Server

Use the `docker ps` command to check the status of all the three docker containers.

Example:

```

[root@localhost quorum_witness-1.0.0]# docker ps
-----
CONTAINER ID   IMAGE          COMMAND                  CREATED     STATUS        PORTS
b5b53ab56a   nginx:1.17.8    "nginx -g 'daemon of..."  32 min ago
edc6522175   nex/ifwitness:1.0.0  "/apisvr/apisvr -etc..."  32 min ago
8c062f2c57   quay.io/coreos/etcd:v3.3.13  "/usr/local/bin/etcd..."  32 min ago
-----
STATUS        PORTS          NAMES
Up 32 min    80/tcp, 0.0.0.0:443->443/tcp  witness_nginx
Up 32 min    80/tcp          witness_apisvr
Up 32 min    2379-2380/tcp    witness_etcd
-----
[root@localhost quorum_witness-1.0.0]#

```

Check `witness_apisvr` log to see whether the quorum witness server is running and capturing logs.

Example:

```

[root@localhost witness_apisvr_logs]# pwd
/root/witness-1.0.0/logs/witness_apisvr_logs
[root@localhost witness_apisvr_logs]# ls
2020_03_02_190234
[root@localhost witness_apisvr_logs]# cat 2020_03_02_190234
2020/03/02 19:02:34 main.go:54: Starting the
application:[/apisvr/apisvr -etcdURL=witness_etcd:2379]
2020/03/02 19:02:34 app.go:47: Setting up handlers for ArrayHandler
2020/03/02 19:02:34 app.go:47: Setting up handlers for SRGHandler
[root@localhost witness_apisvr_logs]#

```

## Obtaining Passphrase for the Quorum Witness Server

To obtain the passphrase for the quorum witness server, do the following:

1. Log in to the host machine where the quorum witness server is deployed.
2. Run the following command to read the `passphrase.txt` file from the witness docker container:

```
docker exec -it witness_apisvr sh -c "cat /apisvr/passphrase.txt"
```

**Example:**

```
[root@localhost quorum_witness-1.0.0]# docker exec -it witness_apisvr sh
-c "cat /apisvr/passphrase.txt"
39avhrTnKYHj!jK-uuy2mDx1H6wZQqa1 <--- This is the new passphrase (32
characters)
[root@localhost quorum_witness-1.0.0]#
```

 **Note:** A new passphrase is generated every time the quorum witness server restarts.

## Updating Certificate File

To update the certificate and key files for quorum witness server, use `updatecertificate` command in `witness.sh`.

**Example:**

```
[root@localhost quorum_witness-1.0.0]#
./witness.sh updatecertificate -c <a PEM certificate file> -k <key file>
```

After the execution of this command, only the `witness_nginx` docker is restarted.

**Example:**

```
[root@localhost quorum_witness-1.0.0]#
./witness.sh updatecertificate -c ~/certs/cert.crt -k ~/certs/cert.key
[root@localhost quorum_witness-1.0.0]#
[root@localhost quorum_witness-1.0.0]# docker ps
-----
CONTAINER ID IMAGE COMMAND CREATED
b5b53ab56a   nginx:1.17.8   "nginx -g 'daemon of..." 49 min ago
edc6522175   nex/ifwitness:1.0.0  "/apisvr/apisvr -etc..." 49 min ago
8c062f2c57   quay.io/coreos/etcd:v3.3.13  "/usr/local/bin/etcd..." 49 min ago
-----
STATUS      PORTS          NAMES
Up 1 second  80/tcp, 0.0.0.0:443->443/tcp  witness_nginx
Up 49 min    80/tcp          witness_apisvr
Up 49 min    2379-2380/tcp    witness_etcd
-----
[root@localhost quorum_witness-1.0.0]#
```

## Cleaning up the Quorum Witness Server

Use the `cleanup` command to clean up the docker containers.

For example:

```
[root@localhost quorum_witness-1.0.0]# pwd
/root/quorum_witness-1.0.0
[root@localhost quorum_witness-1.0.0]# ls
certs  docker-compose.yml  witness.sh  logs  nginx.conf  README
[root@localhost quorum_witness-1.0.0]# docker ps
CONTAINER ID  IMAGE               COMMAND                  CREATED     STATUS    PORTS      NAMES
b5b53ab56a   nginx:1.17.8        "nginx -g 'daemon of..."  52 min ago
edc6522175   nex/ifwitness:1.0.0  "/apisvr/apisvr -etc..."  52 min ago
8c062f2c57   quay.io/coreos/etcd:v3.3.13  "/usr/local/bin/etcd..."  52 min ago
-----
STATUS        PORTS              NAMES
Up 52 min    80/tcp, 0.0.0.0:443->443/tcp  witness_nginx
Up 52 min    80/tcp              witness_apisvr
Up 52 min    2379-2380/tcp       witness_etcd
-----
[root@localhost quorum_witness-1.0.0]# ./witness.sh cleanup
Stopping witness_nginx ... done
Stopping witness_apisvr ... done
Stopping witness_etcd ... done
Removing witness_nginx ... done
Removing witness_apisvr ... done
Removing witness_etcd ... done
Removing network witness_network
[root@localhost quorum_witness-1.0.0]# ls
certs  docker-compose.yml  witness.sh  logs  nginx.conf  README
[root@localhost quorum_witness-1.0.0]# docker ps
CONTAINER ID  IMAGE               COMMAND                  CREATED     STATUS    PORTS      NAMES
[root@localhost quorum_witness-1.0.0]#
```

## Setting up Synchronous Replication Configuration

You need to configure synchronous replication in the source array.

To set up a new synchronous replication configuration, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab, select the required project.
3. Click **Manage > Data Protection > Sync Replication**.
4. In the **Sync Replication** tab, click **Start**.  
The **Start Sync Replication** configuration wizard appears.
5. In the **Partner & Witness** screen, register the partner array and quorum witness server by completing the following steps:

- a) In the **Partner System** section, provide the IP address or the host name of the partner array in the **IP/Hostname** field, and the credentials for the partner array in the **UserName** and **Password** fields.
  - b) In the **Quorum Witness** section, provide the IP address or the FQDN (in case of an EC2 instance) of the quorum witness server in the **IP/Hostname** field, and the passphrase in the **Passphrase** field.
  - c) Click **Next**.  
After the the partner and quorum witness server are registered, the **Pool & Network** screen appears.
6. In the **Pool & Network** screen, select the pool in the partner array and the floating IP addresses by completing the following steps:
    - a) Select the pool from the **Partner's Pool** list.  
The list displays the pools on the replication partner array that match the pool type of the source array.
    - b) In the **Network** section, add additional floating IP addresses of the source array and the partner array, if required.  
The recommended floating IP addresses are already added in the **Network** section.
  - c) Click **Next**.  
The **Summary** screen appears.
7. In the **Summary** screen, review the settings you added for the synchronous replication configuration.
    - a) To modify the settings, click **Back**.
    - b) After all the configuration settings are complete, click **Finish**.



**Note:** The above steps are necessary only when you configure sync replication for the first time. To set up synchronous replication for the subsequent projects, click **Start** in the **Sync Replication** tab for the project. In the **Start Sync Replication** wizard, click **Start** again.

The synchronous replication configuration is set up in the **Sync Replication** tab.

## Editing Synchronous Replication Configuration

You can modify an existing synchronous replication configuration. You can change the IP address of the partner array or quorum witness server, add or remove floating IP addresses of the source and partner pools, or delete the configuration.

To modify configuration settings, complete the following steps:

1. In the IntelliFlash Web UI, click **Services > Sync Replication**.

The **Synchronous Replication Overview** page appears.

2. **Modifying the IP address of the partner array:** If the IP address of the partner system has changed, you can modify the IP address. Click **Configuration > Edit Partner System** and modify the IP address of the partner array. Click **Save** after making the changes.
3. **Modifying the quorum witness server:** To modify the quorum witness server, click **Configuration > Edit Quorum Witness** and modify the IP address of the quorum witness server and the passphrase. Click **Save** after making the changes.
4. **Modifying the network settings:** To add or remove floating IP addresses of local and partner arrays, click **Configuration > Edit Network** and add or remove floating IP addresses of local and partner arrays. Click **Save** after making the changes.

 **Note:** IntelliFlash does not allow you to change floating IP addresses of the source array or the partner array, if atleast one synchronous replication group exists. Workaround: Delete all the synchronous replication groups and then modify the IP addresses of the source array or the partner array.

## Viewing Synchronous Replication Configuration

---

To view the synchronous replication configuration settings, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab, select the required project.
3. Click **Manage > Data Protection > Sync Replication**. Alternatively, go to **Services > Sync Replication**. The **Synchronous Replication Overview** page appears. Select the project.
4. Click **More > View Configuration**.

The **View Configuration** screen appears with the partner system, quorum witness server, and the floating IP addresses of the pools.

## Deleting Synchronous Replication Configuration

---

You can delete the synchronous replication configuration if you have deleted the existing synchronous replication relationships of all the projects. Deleting the synchronous replication configuration de-registers the partner array from the quorum witness server.

To delete synchronous replication configuration, complete the following steps:

1. In the IntelliFlash Web UI, click **Services > Sync Replication**.

- The **Synchronous Replication Overview** page appears.
2. Click **Configuration > Delete Configuration**.  
The **Delete Pair Configuration** screen appears.
  3. Type **Delete** in the text box and click **Delete**.

## Viewing Synchronous Replication Relationship Details

---

After the synchronous replication configuration is complete, the **Sync Replication Overview** (**Services > Sync Replication**) page displays the following information:

- Synchronous replication configuration details such as the IP addresses of the source array, quorum witness server, and the partner array.
- Write latency details (both historical and live data) for the projects and LUNs.
- Project details such as the mode (active or passive) of the array, number of LUNs, and the replication status (In Sync, Syncing, or Out of Sync).

To view synchronous replication details for a specific project, select the project in the **Provision > Projects** page and click **Manage > Data Protection > Sync Replication**.

## Viewing Write Latency Details

---

To view the write latency details of a synchronous replication project, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab, select the required project.
3. Click **Manage > Data Protection > Sync Replication**.  
Alternatively, go to **Services > Sync Replication**. The **Synchronous Replication Overview** page appears.
4. Click the **Write Latency** tab.

By default, you can see the write latency graph of the last one hour for a pool (if you are viewing from the **Synchronous Replication Overview** page) or the project (if you are on the **Synchronous Replication** tab of a project). You can also view the write latency of the previous five minutes or one hour.

If you are viewing from the **Synchronous Replication Overview** page, you can view the write latency data for a specific project. If you are on the **Synchronous Replication** tab of a project, you can view the write latency data for a specific LUN.

5. To view the historical write latency data, click **Historical**, select a custom period, and click **Apply**.

## Deleting Synchronous Replication Relationship of a Project

---

Deleting the synchronous replication relationship of a project cleans up all the data at the replication partner array.

To delete synchronous replication relationship of a project, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab, select the required project.
3. Click **Manage > Data Protection > Sync Replication**. Click **Delete**.
4. Alternatively, go to **Services > Sync Replication**. In the **Synchronous Replication Overview** page, click the **Delete** button above the list of projects.  
The **Delete Sync Replication** dialog box appears.
5. Type the name of the project you want to delete and click **Delete**.

## Disabling Auto Takeover Option

---

To prevent automatic take over by the standby array if the active array is down, you can disable the **Auto Takeover** option.

To disable auto takeover, complete the following steps in the active or standby array:

1. Click **Provision > Projects**.
2. In the **Local** tab, select the required project.
3. Click **Manage > Data Protection > Sync Replication**.  
Alternatively, browse to **Services > Sync Replication**. The **Synchronous Replication Overview** page appears. Select the project.
4. Click the **Settings** icon and disable the **Auto Takeover** tab.
5. Click **Save**.

## Manual Takeover Using the Partner Array Web UI

---

You can manually change the partner array to Active mode from Standby mode. Complete the following steps in the partner array:

1. Click **Provision > Projects**.
2. In the **Local** tab, select the required project.
3. Click **Manage > Data Protection > Sync Replication**.

Alternatively, browse to **Services > Sync Replication**. The **Synchronous Replication Overview** page appears. Select the project.

4. Click **More > Takeover**.
5. In the **Takeover Confirmation** dialog box, click **Takeover**.

## Manual Giveover Using the Source Array Web UI

---

You can manually change the source array from Active mode to Standby mode. Complete the following steps in the source array:

1. Click **Provision > Projects**.
2. In the **Local** tab, select the required project.
3. Click **Manage > Data Protection > Sync Replication**.  
Alternatively, browse to **Services > Sync Replication**. The **Synchronous Replication Overview** page appears. Select the project.
4. Click **More > Giveover**.
5. In the **Giveover Confirmation** dialog box, click **Giveover**.

## Enabling Auto Failback

---

If you enable auto failback and a failover occurs, IntelliFlash automatically fails back the writes and IOs to the preferred array as soon as it becomes available again.

To enable auto failback, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab, select the required project.
3. Click **Manage > Data Protection > Sync Replication**.  
Alternatively, browse to **Services > Sync Replication**. The **Synchronous Replication Overview** page appears.
4. Click the **Settings** icon.
5. Enable the **Auto Failback** option.
6. Select the preferred array or pool from the **Pool** list.
7. Click **Save**.



---

# Chapter 17

---

## Asynchronous Replication

---

**Topics:**

- *Introduction to IntelliFlash Asynchronous Replication*
- *Terms Used in Asynchronous Replication*
- *Asynchronous Replication Uses*
- *How IntelliFlash Replicates Data*
- *Project-Level Asynchronous Replication*
- *Ports used for Asynchronous Replication*
- *Asynchronous Replication Preferred IP Address*
- *Asynchronous Replication Modes*
- *Asynchronous Replication Options*
- *Asynchronous Replication Roles*
- *Asynchronous Replication Configuration*
- *Asynchronous Replica Snapshot*
- *Switch Replication Source*
- *Multi-site Replication Relationships*
- *Asynchronous Replication Topologies*
- *Monitoring Asynchronous Replication*
- *Asynchronous Replication in an HA Environment*
- *Asynchronous Replication Relationship During Upgrades*
- *Reasons for Failure of an Asynchronous Replication Process*
- *Setting up and Managing Asynchronous Replication*

- *Managing Asynchronous Replica Projects*



## Introduction to IntelliFlash Asynchronous Replication

---

IntelliFlash provides secure, snapshot-based asynchronous data replication over a network from a source IntelliFlash Array to a remote IntelliFlash Array. You can use the replicated data for disaster recovery and reuse.

In IntelliFlash, you can replicate data only at the project level. IntelliFlash supports various topologies for data replication. You can set up a one-time manual replication relationship or schedule regular automatic replication updates. You can clone and use the replicated data for restoring your data in the event of data loss or to make a copy of the data on a target IntelliFlash Array. After cloning and restoring the data on a target storage array, you can use the data for various purposes.

IntelliFlash allows you to reverse the replication relationship in a single step. When you reverse the replication relationship, your replication source array starts performing the target operations and your target array starts performing the source operations immediately.

IntelliFlash supports setting up a replication relationship for VMware SRM environments.

 **Note:** IntelliFlash can replicate a project with a replication role of SRM Partner only to one replication target array. However, you can set up a replication relationship for backup purposes using other replication roles.

The **Pause** and **Resume** options in IntelliFlash allows you to pause an ongoing replication and resume it later.

The **Promote** feature on the replication target array enables you to break a replication relationship to use the replicated data on the replication target array.

A best practise before setting up asynchronous replication is to make sure that the snapshot interval is more than 15 minutes for all the shares and LUNS. Also delete the existing snapshots if they exceed 1000 in number.

## Terms Used in Asynchronous Replication

---

This section defines the terms used to describe IntelliFlash replication.

### Replication Configuration

A replication configuration consists of the details for the replication setup such as target system details, replica project name, replication role, replication options, list of included or excluded shares and LUNs, schedules, and so on.

### Replication Scope

Replication scope defines which shares and LUNs to include or exclude in a project.

## Replica Snapshot

A replica snapshot is a point-in-time collection of references to the data blocks of a source project consisting of shares and LUNs. It replicates data changes from a replication source storage array to a replication target storage array.

## Replication Source

IntelliFlash Array from which the original data is replicated to a single or multiple IntelliFlash systems.

## Replication Target

IntelliFlash Array that receives replicated data from a single or multiple IntelliFlash systems and stores the data securely for future use.

 **Note:** An individual IntelliFlash Array can act as both replication source and replication target.

## Target Pool

A pool on a Replication target storage array used for storing replicated data.

## Replica Project

A new project created on the Replication target storage array for storing replicated data and its properties.

## Replication Options

Replication Options defines the way you want to replicate data from a source storage array to the target array. You can select these options when configuring a replication relationship in the replication wizard.

- Secured
- Ignore source quota
- Sparse - The **Sparse** replication option helps you in deciding whether to include all snapshots from the snapshot schedule or just the latest snapshot from each schedule.

## Promote

The **Promote** option allows you to break the replication relationship and converts a **Replica** project to **Local** project on your replication target array. Once you promote, you cannot reverse this process.

## Switch Replication Source

The **Switch Replication Source** option enables you to reverse the replication relationship. When you use this option, your source array starts performing the target role and your target array starts performing the source role. You can use this option from either the source array or the target array.

## Resolve Conflict

In a replication source conflict situation, both the replication source and replication target systems assume that they are the source at the same time. The **Resolve Conflict** option in the replication feature allows you to correct the replication source conflict issue. The system from which you use the **Resolve Conflict** option becomes the replication source array.

## Related Topics

[Resolving the Conflicting Situation](#)

## Asynchronous Replication Uses

---

The following are the major uses for asynchronous replication:

- Restoring data in the event of data loss
- Providing read-only access to remote sites
- Providing faster access to users in remote sites
- Consolidating data from different replication source storage arrays
- Testing the application data
- Backing up data onto backup devices

## How IntelliFlash Replicates Data

---

IntelliFlash replicates data at the project level. It replicates a project that contains shares and LUNs from a replication source storage array to a remote replication target storage array over a network. IntelliFlash uses the snapshot technology to perform replication.

To set up a replication relationship, you should identify and add a replication target storage array in a replication source storage array. After the target array is added, the source replication storage array establishes a communication with the target array.

You should identify a pool with a sufficient storage space on the target storage array for replicating a project. The IntelliFlash Web UI lists all pools available on the replication target array. You must ensure that the target project name is unique from the existing project names on the target storage array.

The IntelliFlash Web UI allows you to set up different replication roles. A replication role can be reversible, not reversible or SRM partner.

The IntelliFlash Web UI allows you to select different replication options, such as **Secured**, **Ignore source quota**, , and **Sparse** (an option to replicate all snapshots or the latest snapshot). You can also include or exclude shares and LUNs from a replication configuration. Using the IntelliFlash Web UI, you can set up a one-time manual replication relationship or a scheduled replication relationship.

After setting up the replication relationship, IntelliFlash completes the following process:

1. IntelliFlash creates a **Replica** project on the replication target array. Replication configuration remains in **Standby** status until replication starts, either according to the schedule or when you start it manually.
2. When replication starts, IntelliFlash creates a replica snapshot of the project (includes shares and LUNs) on the replication source storage array.
3. IntelliFlash estimates the total data size to replicate.
4. IntelliFlash replicates all shares and LUNs with complete data to the replication target array during the first time data transfer for a new replication relationship. Along with data, IntelliFlash also replicates the project configuration. The project configuration includes project, share, and LUN properties. Additionally, IntelliFlash replicates snapshot schedules for **Reversible** and **SRM Partner** replication roles.

For an existing replication relationship, IntelliFlash finds the incremental data and takes a replica snapshot.

5. IntelliFlash verifies whether it has to replicate all scheduled snapshots or latest snapshot based on the **Sparse** option.
6. Depending on the verification, IntelliFlash replicates all scheduled snapshots for each share and LUN along with the latest replica snapshot or replicates only the latest snapshot.
7. IntelliFlash calculates and displays the average data transfer rate and total time remaining to complete the replication process.
8. The **Replication** tab displays the percentage of data transferred and current status.
9. After completing the replication, on the target array you can view the replica project in the **Replica** tab and its contents (shares, LUNs, auto snapshots, replica snapshot).
10. According to the replication schedule, IntelliFlash continuously replicates incremental data to the replication target array in the form of replica snapshots.

## Project-Level Asynchronous Replication

---

IntelliFlash replicates data at the project level. A replicated project on a target storage array is called a **Replica** project.

The project-level replication simplifies the process of managing replication relationships. When a project is replicated, all the shares and LUNs within the project are replicated to the target storage array. However, you can choose the shares and LUNs for replication from the project when setting up the replication relationship. After setting up the relationship, a **Replica** project and its contents (shares and LUNs) inherit source project properties.

If you change the properties of a project, share, or LUN after setting up the replication relationship, the new changes are replicated to the target Replica project in the next replication update.

## Ports used for Asynchronous Replication

---

IntelliFlash uses fixed ports for replication to simplify managing ports. By default, replication uses the following TCP ports:

- 1300: for unsecured data channel
- 1301: for secured data channel
- 9998 and 9999: for replication control traffic and inter-controller communication.

 **Note:** You should never block the ports 9998 and 9999.

## Asynchronous Replication Preferred IP Address

---

IntelliFlash replicates data using pool floating IP address, array management IP address, and controller IP address depending on the availability.

 **Note:** Though IntelliFlash allows you to use pool floating IP address, use the array management IP address for configuring a replication relationship. IntelliFlash uses the IP address that is used for configuring a replication relationship for replicating the configuration changes from a replication source array to replication target array.

IntelliFlash automatically uses the available IP address in the following priority:

1. Pool floating IP address
2. Array management IP address
3. Controller IP address

## Asynchronous Replication Modes

---

You can configure replication relationships and schedule replication updates. If you are not scheduling the replication updates, the replication wizard automatically sets to the manual replication mode.

### Schedule

You can use the **Enable Scheduling** option in the replication wizard and **Replication** tab to schedule the replication updates. The available options are: **By Minutes**, **Hourly**, **Daily**, **Weekly**, and **Monthly**.

 **Note:** If you are not using the **Enable Scheduling** option in the replication wizard, the wizard automatically sets the replication mode to manual.

## Manual Replication

If no schedule is selected for a replication relationship, the replication mode automatically sets to manual.

In manual replication mode, you must manually start the replication after setting up the replication relationship. After the first data transfer to the target storage array, the replication relationship exists, but the updates stop. You can send the replication updates manually according to your requirements.

You can find the last replication update date and time in the **Replication** tab of the project configuration window. If you need to, you can schedule the replication updates from the **Replication** tab in the **Data Protection** window (**Provision > Projects > Local > Manage > Data Protection > Replication**).

## Asynchronous Replication Options

---

You can replicate data using three different options depending on your requirements.

The replication wizard provides the following replication options:

- **Secured**

Allows data to replicate from the replication source securely, using SSL, to the replication target storage array. Data is encrypted at the source storage array and decrypted on the target storage array. It uses public cryptography for encryption.

- **Sparse**

Allows you to include all snapshots from the snapshot schedule or just the latest snapshot from each schedule.

By default, IntelliFlash replicates all snapshots from the snapshot schedule defined on the replication source array.

If you set the option to **Yes**, only the latest snapshot from each schedule is included as part of the replication.

- **Ignore source quota**

When you enable the **Ignore Source quota** option in the **Replication Configuration Wizard**, the storage quota set on the replication source is disabled and you can set the quota for the replica project on replication target array.

This option is useful in the case where snapshots use space exceeding the quota applied on source and resulting in replication failure.

You can set quota for a replica project and share inside the replica project.

## Asynchronous Replication Roles

---

When configuring replication, you can select replication roles. The following are the three supported Replication Roles:

### **Not Reversible**

When you select the Not Reversible option, data replication occurs only from the source array to target array. IntelliFlash Web UI does not allow you to reverse the replication process. If you need to change the replication role, you must edit the replication configuration and change the replication role.

### **Reversible**

The Reversible replication role allows you to convert your replication target array to a source array and your current replication source array to a target array, if required. The **Switch Replication Source** option in the UI allows to you to perform this operation.

### **SRM Partner**

You can use the replication role **SRM Partner** replication role if you are planning to use array-based replication with the VMware SRM Server.

## Asynchronous Replication Configuration

---

A replication configuration consists of the following information:

- Target storage array DNS name or an IP address
- Target pool name
- Replica project name
- Details about shares and LUNs included in the replication configuration (Replication scope)
- Replication role : Reversible, Not Reversible, and SRM partner.
- Replication option(s)
  - Secured
  - Stream Deduplication
  - Sparse
  - Ignore source quota
- Replication mode:
  - Scheduled (Automatic)
  - Manual - If no schedule is selected.

After setting up the replication relationship, you cannot change the following configuration details:

- Target pool

- Replica project

You can modify other configuration details that are excluded from the above list according to your requirements.

 **Note:**

If snapshot schedule is not set in the source while configuring replication, system generates the following alert so that the user can create a snapshot schedule:

**No snapshot schedules found. Target will not have additional snapshots.**

## Asynchronous Replica Snapshot

An asynchronous replica snapshot is a point-in-time collection of references to the data blocks of a source project consisting of shares and LUNs. It is used for data transfer and promote.

A replica snapshot contains incremental changes in the data. IntelliFlash replicates data changes from a replication source storage array to a target storage array using replica snapshots. On a replication target storage array, a replica snapshot is used to restore the data.

IntelliFlash does not display the replica snapshots in the **Listing** tab of the source array.

By default, the replication target retains only the latest replica snapshot. You can clone a replica snapshot and use it on the replication target array.



**Note:** The **Promote** operation uses only the latest replica snapshot for promoting a replica project.

A replica snapshot name begins with the word **replica**, suffixed by a time stamp, and followed by a replica serial number. The time stamp is in the format: YYYYMMDDHHMMSS000. The zeros or other numbers at the end of the time stamp represent the replica snapshot serial number. You can view the replica snapshots from the **Replication** page on target array.

## Additional Asynchronous Replica Snapshots

The IntelliFlash Web UI allows you to retain a specific number of additional replica snapshots when modifying the replication relationship apart from the scheduled auto-snapshots. These additional replica snapshots help you to restore data when data is corrupted on the source. By default, replication does not create any replica snapshot on the target if you do not set any *additional replica snapshots* during replication configuration. However, IntelliFlash allows you to change the default value of additional replica snapshots of an existing schedule.



**Tip:** Additional replica snapshots are useful if you turn on the **Sparse** option when setting up the replication relationship.

Auto-snapshots and additional replica snapshots each have their own retention policy. Having separate retention policies for auto-snapshots and replica snapshots allows you to have a longer retention policy for the replica snapshots. You can use the auto-snapshots or replica snapshots to restore data in the case of data corruption or data loss on the source array.

### Replica snapshot behavior in the case of role reversal

When you perform the role reversal operation to make your current source as the new target and current target as the new source, the new replication configuration maintains the required number of auto-snapshots and replica snapshots according to the schedule and the retention policy. The old replica snapshots are not immediately deleted from the old target array after role reversal. IntelliFlash will start deleting the old replica snapshots from the old target array after replicating the required number of additional replica snapshots to the new target. However, the IntelliFlash Web UI does not display these replica snapshots on the old target (new source).

## Asynchronous Replication Snapshots Retention Policy on the Target Array

IntelliFlash replicates scheduled auto-snapshots based on the **Sparse** option available in the replication wizard in addition to the default replica snapshot. The replication wizard also enables you to create *additional replica snapshots* on the replication target array when setting up a replication relationship.

There are separate retention policies for scheduled auto-snapshots and replica snapshots.

The scheduled auto-snapshots follow the retention policy defined at the source and the replica snapshots follow the retention policy defined by the replication schedule.



**Caution:** IntelliFlash allows you to retain additional snapshots in the target by customising snapshot schedules during configuration.

IntelliFlash starts deleting the oldest snapshot after reaching the maximum number of snapshots defined in the snapshot policy on the source, and retains the remaining snapshots. Similarly, IntelliFlash starts deleting the oldest replica snapshot first, based on the number of additional replica snapshots defined in the replication schedule.

## Switch Replication Source

---

The **Switch Replication Source** option enables you to reverse the replication relationship. When you use this option your source array your source array assumes the target role of the replication, and the target array assumes the source role.

You can use this option from the source array or target array. When you perform the switch replication source operation, regardless of from which array you perform the operation, a **Local** project converts to a **Replica** project and a **Replica** project converts to a **Local** project.



**Caution:** The **Switch Replication Source** operation causes immediate disconnection of all active LUNs and shares within the project from the mapped hosts regardless of whether they participate in replication or not.

### Prerequisite

At least one replication should have successfully completed before you attempt to switch the replication source and the selected **Replication role** should be **Reversible**.

### Switch Replication Source from Replication target array

You can perform the **Switch Replication Source** operation from your replication target array if your original replication source array is down due to an outage.

When you perform the **Switch Replication Source** operation on a replication target array, you are making your target array into a replication source array. This is possible as your target array also contains source array configuration details. In this scenario, your target array uses the latest available replica snapshot and converts your **Replica** project to a **Local** project. After performing the operation, you can start using the array that has become the source. You should add mapping for your LUNs and mount shares.

 **Note:** When you perform the **Switch Replication Source** operation from a target array in a disaster recovery scenario, your target array may not have the latest data because your original replication source array failed to replicate due to an outage.

 **Note:** If you perform the **Switch Replication Source** operation from a target array when your source array is live, IntelliFlash does not replicate the latest changes from Replication source to a Replication target array.

### Switch Replication Source from Replication source array

You can perform the **Switch Replication Source** operation from your replication source array in the following scenarios:

- When you want to convert your replication source array into a replication target array for maintenance or other requirements.
- When you previously converted your replication target array to a replication source array to recover from a disaster and now you want to bring back to the original configuration.

When you perform the **Switch Replication Source** operation from a replication source array, you are making your current target array into the source array. The operation converts your **Local** project to a **Replica** project. Before converting a **Local** project to a **Replica** project, IntelliFlash replicates the latest data to the new replication target array to ensure the latest data is on both arrays.

 **Note:** Ensure that your target array is up and working when performing this operation.

### Related Topics

[Switch Replication Source: Target to Source](#)

[Switch Replication Source: Source to Target](#)

## Multi-site Replication Relationships

---

IntelliFlash supports multi-site replication relationships. In the multi-site replication relationship setup, you can replicate a single project to multiple replication targets using independent replication configuration for each target. In this scenario, when you perform the **Switch Replication Source** operation from the replication source array to the replication target array,

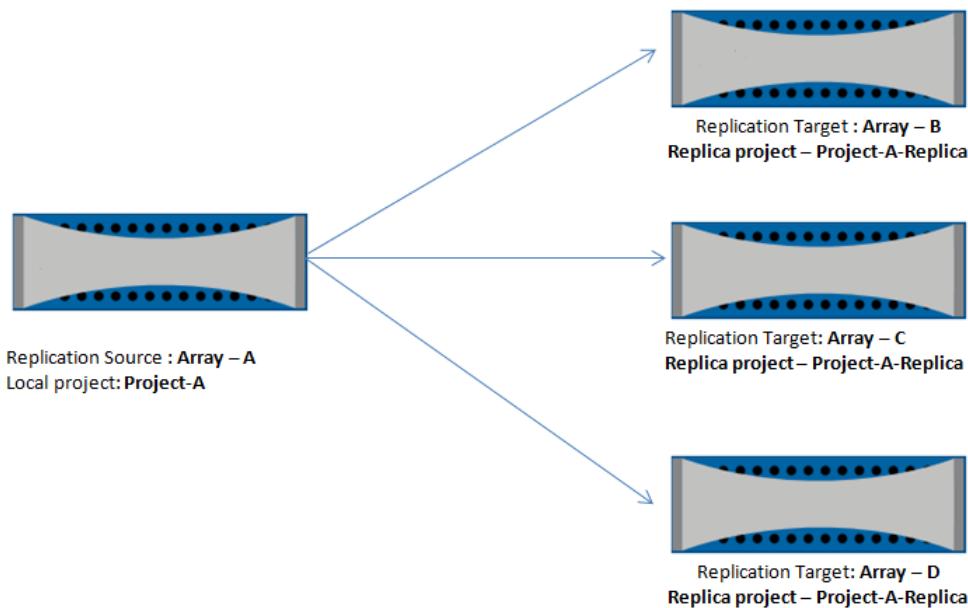
the new replication source array automatically becomes the replication source array for other replication relationships in the setup and starts replicating to targets.

**Note:** In a multi-site replication environment, you cannot perform the **Switch Replication Source** operation for a replication relationship with the **Replication Role** as **Not Reversible**.

The following example illustrates how the **Switch Replication Source** operation works for multi-site replication relationships:

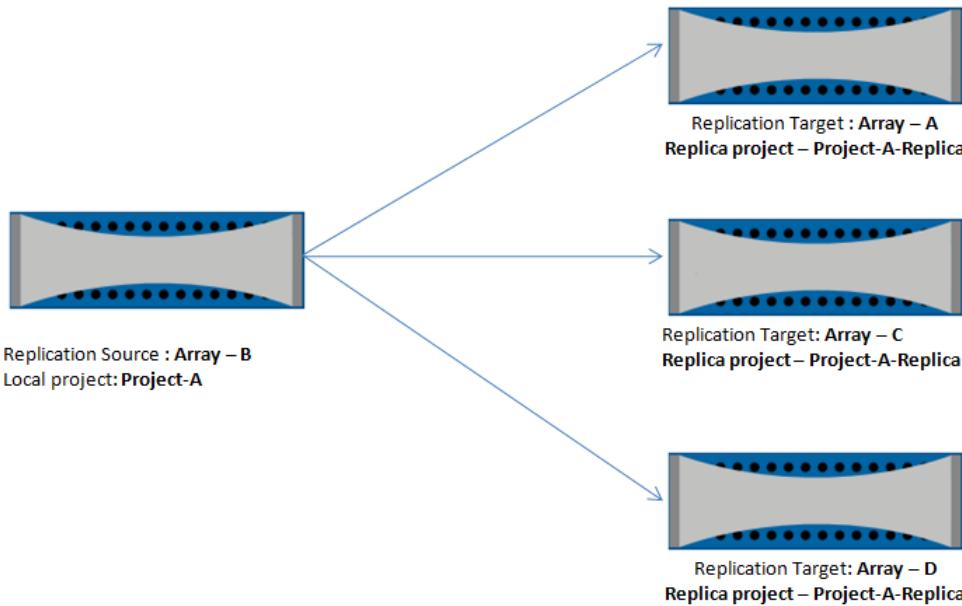
1. You replicate **Project –A** from replication source **Array – A** to three different replication target arrays using three different replication configurations: **Array - B**, **Array - C**, and **Array - D**, respectively.
2. You perform the **Switch Replication Source** operation from replication source **Array-A** to **Array-B**
3. This causes **Array-B** to automatically become the Replication Source Array and **Array-A** to become the target array.
4. After the switch, **Array-B** continues to replicate data to **Array-A**, **Array-C**, and **Array-D**.

The following Illustration displays the initial multi-site replication relationship from Replication Source Array- A (with three separate replication configurations) to Replication Targets: **Array-B**, **Array-C**, **Array-D** for Project-A.



**Figure 29: Initial multi-site replication relationship**

The following Illustration displays the replication relationship after performing the Switch Replication Source operation on Replication Source Array-A. In this case, only Array- A and Array-B switch roles.



**Figure 30: Multi-site replication relationship after Switch Replication Source operation**

## Asynchronous Replication Topologies

IntelliFlash supports the following types of asynchronous replication topologies for IntelliFlash systems:

- **One-to-One**

In the one-to-one replication relationship, IntelliFlash replicates data from one replication source storage array to a different replication target storage array.

- **One-to-Many**

In the one-to-many replication relationship, IntelliFlash replicates data from one replication source storage array to multiple replication target remote storage array.

- **Many-to-Many**

In the many-to-many replication relationship, all IntelliFlash storage arrays act as both replication sources and targets. They receive and send data to and from multiple remote IntelliFlash systems.

- **Many-to-One**

In the many-to-one replication relationship, multiple replication source IntelliFlash systems replicate data to a single replication target storage array.

**Note:** In all of the above replication topologies, a single IntelliFlash Array can act as a replication source storage array and a replication target storage array.

## Monitoring Asynchronous Replication

You can monitor the replication process and status from the **Replication** page (**Services > Replication**) and from the **Notifications** page.

### Asynchronous Replication Status Messages

The **Replication** page displays all of the existing replication configuration details. You can access the configuration details page by clicking **Provision > Projects > Manage > Data Protection > Replication**. The following are the different possible status messages that a replication configuration can display in the **Status** field.

- **Standby**

Displays when the replication relationship is configured and waiting for replication to start manually or according to the schedule.

- **In progress**

Displays along with percentage completion when IntelliFlash is taking snapshots and transmitting the replica snapshots to a replication target. It also displays replication progress in percentage.

- **Paused**

Displays when you manually interrupt an ongoing replication by clicking the pause button. You can restart the paused replication from the state where it was interrupted.

- **Stopped**

Displays when you manually stop an ongoing replication by clicking the stop button. You can restart a stopped replication. However, a replication which is stopped restarts.

- **Failed**

Displays when replication fails for any reason.



**Note:** You can check the **Notifications** page for the failure reason.

- **Completed**

Displays once the replication process is complete.

- **Suspended**

Displays when a Project converts to a Replica project, but the array still holds the replication source configuration. You can see this state in a VMware SRM setup up where reprotect operation is pending after planned or disaster recovery.

## Asynchronous Replication in an HA Environment

In an HA environment, the replication process fails when switchover/switchback is in progress on the replication source or target storage arrays.



**Note:** It is recommended to use an array management IP address for an HA environment when setting up a replication relationship.

IntelliFlash restarts the replication process according to the defined replication schedule. If the replication relationship is manual, you must restart the process manually.

## Asynchronous Replication Relationship During Upgrades

---

During an IntelliFlash Operating Environment upgrade, the replication process fails and it restarts automatically according to the next schedule.

When upgrading,

- Upgrade both the replication source and target storage arrays.
- Upgrade the target storage array first for the replication to work smoothly.
- Check the replication schedule before the IntelliFlash Operating Environment upgrade process and plan your IntelliFlash Operating Environment upgrade accordingly. Do not upgrade while the array is replicating data.

You can view the upgrade-related notifications in the **Notifications** page.

## Reasons for Failure of an Asynchronous Replication Process

---

A replication relationship might fail due to issues with storage space, networking, HA switchover/switchback, or a manual abort.

IntelliFlash provides replication failure notifications for most of the issues.

After a failure, IntelliFlash attempts to restart the replication on the next schedule. However, for manual replication, you should restart the replication after resolving the issue that caused the failure.

### Storage Related Reasons

The following are some pool-related reasons for replication failure:

- No space on the replication target pool
- Quota exceeded
- Reserved space not available on the target pool
- Target pool is exported
- Replica project is deleted

### Network Related Reasons

The following are some network related reasons for replication failure:

- Cannot reach the IP address or domain
- DNS changes
- Replication source or target IP changes

## HA Switchover or Switchback

All ongoing replication updates abort and restarts automatically according to schedule when an HA switchover or switchback occurs.

# Setting up and Managing Asynchronous Replication

---

You can configure replication relationships and manage them from the **Data Protection** window (**Provision > Projects > Local > Manage > Data Protection > Replication**) and from the **Replication (Services > Replication)** menu option.

## Replication Prerequisites

The following are the prerequisites for setting up a replication relationship:

- You must use array management IP address when adding a replication target array.
- You must have target IntelliFlash Array name or array management IP address and password.
- The replication target must have sufficient storage space for data and replica snapshots.
- Provide user name, contact email ID, and the other information requested in the **Customer Support** page (**Settings > Administration > Customer Support**).
- In an HA environment, you must use a floating array management IP address or DNS for replication. The name must resolve to the array management IP address.
- Ensure that the Replica project name is unique from the existing projects on the Replication target storage array.
- You must have both replication source and replication target running the same IntelliFlash version.



### Important:

Use the FQDN of the target system's array management IP address while defining replication relationships. Using an FQDN enables you to change the IP address of a target system without breaking the replication relationship.

## Setting Up a Replication Relationship

The IntelliFlash replication wizard enables you to set up a replication configuration (relationship).

Before setting up the replication relationship, read through the replication prerequisites and understand replication related concepts.

To set up a new replication configuration (relationship), complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab, select the required project.
3. Click **Manage > Data Protection > Replication**.
4. In the **Replication** tab, click **Add**.

The **Replication Configuration Wizard** displays.

- In the **Target System** page of the **Replication Configuration Wizard** screen, complete the following steps:

If...	Then...
<b>You want to use an existing target.</b>	<p>Complete the following steps:</p> <ol style="list-style-type: none"> <li>Click <b>Select a Target System</b>.</li> <li>Click <b>Target System</b> and select a Replication target.</li> <li>Click <b>Next</b>.</li> </ol> <p>The wizard communicates with the target and verifies the credentials.</p>
<b>You want add a new Replication target.</b>	<p>Complete the following steps:</p> <ol style="list-style-type: none"> <li>Click <b>Add New Target System</b>.</li> <li>Type <b>Target System</b> name or IP address.</li> <li>Type the username of the target system (Replication Target).</li> <li>Type the target storage array password.</li> </ol> <p><b>Note:</b> You must use the target system floating IP address or host name.</p> <p><b>Note:</b></p> <ol style="list-style-type: none"> <li>From the <b>Replications Systems</b> page, you can set port numbers used by source system on the target system.</li> <li>You must enable port numbers defined for replication in the target system network firewall.</li> <li>Data port numbers are per storage array.</li> </ol> <p>5. Click <b>Next</b>.</p> <p>The wizard communicates with the target and verifies the credentials.</p>

- In the **Replica Destination** screen, complete the following steps:

- a) Select the **Target Pool** from the list.

The list displays all available pools on the Replication target storage array.

- b) In the **Replica Project** field, type a name for the Replica project.



**Note:** Replica project name should be unique from the existing replica project names.

- c) Click **Next**.

7. In the **Replication Options** screen, complete the following steps:

- a) Select a **Replication Role** from the dropdown list. (**Not Reversible**, **Reversible**, or **SRM Partner**)
- b) Click required replication options:
  - **Secured**
  - **Sparse**
  - **Ignore source quota**



**Note:** The **Sparse** option allows you to include all snapshots from the snapshot schedule or just the latest snapshot from each schedule. If you enable the **Sparse** option, only the latest snapshot from each schedule is included as part of the replication.

- c) To include or exclude shares or LUNs from the replication scope, click **All** or **Include** or **Exclude**.

The **All** scope option includes all the shares and LUNs within the project for replication. The **Include** and **Exclude** scope option allows you to select shares and LUNs to include or exclude for replication.

- d) Click **Next**.

8. Click **Enable Scheduling**.

- a) Select a **Schedule** type.

Options are: **By Minutes**, **Hourly**, **Daily**, **Weekly**, and **Monthly**.

- b) Click the link next to the **every** text box to set the time/day rule as per the selected schedule type.

9. To retain extra replica snapshots, type the required number in the **Additional Snapshots** field.

10. Click **Create**.

A new replication configuration displays in the **Replication Settings** page.

For manual replication, you must start the replication manually. For Automatic replication, the replication process starts automatically according to the schedule.

## Starting Replication Manually

You can manually start a stopped, failed, paused, standby, or completed replication. You can also manually start a replication configuration manually after setting up the replication relationship.

To start a replication process, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab, select the required project.
3. Click **Manage > Data Protection**.
4. In the **Data Protection** page, click **Replication**.
5. In the **Replication** tab, click **Start**.

The **Status** column in the **Replication** page displays the status as **In Progress**.

## Modifying a Replication Options

The **Replication Options** window enables you to modify the replication configuration.

You can modify a replication role, replication options, replication scope, and replica snapshots. The modified replication configuration starts functioning at the next replication update.

To modify a replication relationship (configuration), complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab, select the required project.
3. Click **Manage > Data Protection > Replication**.
4. In the **Data Protection** page, click **Replication**.
5. In the **Replication** tab, click **Options** for the replication configuration.
6. In the **Replication Options** window, you can modify the following configuration details.
  - **Role (Not Reversible, Reversible, SRM Partner)**
  - **Options (Secured, Ignore source quota , Sparse, and )**
  - **Scope**
  - **Additional Snapshots**
7. Click **Save**.

## Modifying a Replication Schedule

You can enable or disable the replication schedule and modify the schedule for running replication.

To modify the replication schedule, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab, select the required project.
3. Click **Manage > Data Protection > Replication**.
4. In the **Data Protection** page, click **Replication**.
5. In the **Replication** tab, click **Schedule** for the replication configuration.
6. In the **Replication Schedule** window, complete the following steps:
  - a) (optional) Click the toggle button enable or disable scheduling.  
If the button is green color with the tick mark, the scheduling is enabled to run replication automatically.  
Select a frequency from the dropdown list.  
Click the link next to the **every** text box to modify the schedule in the **Options** screen.
  - b) Click **Apply**.
7. Click **Save**.

## Pausing Replication

You can pause an ongoing replication due to any technical problems or other requirements.

When you restart /resume a paused replication, it starts from the point where it was paused.

When you pause a replication, IntelliFlash temporarily stops the data transfer to the target. The **Status** field displays as **Paused**.

Paused replications will resume automatically according to the schedule, or you can manually start the replication.

1. Click **Provision > Projects**.
2. In the **Local** tab, select the required project.
3. Click **Manage > Data Protection > Replication**.
4. In the **Data Protection** page, click **Replication**.
5. In the **Replication** tab, click **Pause** for the required configuration.

IntelliFlash pauses the replication update and the status changes to **Paused**.

## Resuming a Paused Replication

You can resume a paused replication. When you restart /resume a paused replication, it starts from the point where it was paused.

1. Click **Provision > Projects**.
2. In the **Local** tab, select the required project.
3. Click **Manage > Data Protection > Replication**.
4. In the **Data Protection** page, click **Replication**.
5. In the **Replication** tab, click **Start**.

## Stopping Replication

You can stop an ongoing or failed replication. You may need to stop replication to address storage space, networking, or other technical problems.

When you stop a replication, IntelliFlash stops the data transfer to the target. The **Status** field displays **Stopped** after completing the process. The stopping process can be time consuming. The duration depends on your configuration details.

Aborted replications restart automatically according to the schedule, or you can manually restart the replication.

1. Click **Provision > Projects**.
2. In the **Local** tab, select the required project.
3. Click **Manage > Data Protection > Replication**.
4. In the **Data Protection** page, click **Replication**.
5. In the **Replication** tab, click **Stop**.

IntelliFlash stops the replication update and the status changes to **Stopped**.

## Resolving a Conflict Situation

The IntelliFlash Web UI provides the **Resolve Conflict** option to resolve a conflict situation where both your replication source and replication target assume they are the source at the same time.

For example, a conflict may arise when your original replication source array is not accessible due an outage and you switch the replication role. Later, when your original replication source array comes back after the outage, both your source and target arrays have the source role and this results in a conflict situation.

For this type of conflict, you can select the **Resolve Conflict** option from the replication source or target.

 **Note:** The array (source or target) from which you use the **Resolve Conflict** option becomes the replication source.

To resolve the conflict situation from the replication source or target, complete the following steps:

1. Log in to your replication source or target array.
2. Click **Provision > Projects > Local**.
3. In the **Local** tab, select a project and click **Manage > Data Protection > Replication** for the required project.
4. In the **Replication** tab, click the **Resolve Conflict** option in the replication conflict UI notification.

## Switch Replication Source: Target to Source

The **Switch Replication Source** option enables you to reverse the replication relationship. When you use this option your source array starts performing the target role and your target array becomes the source. You can use this option from the source array or target array.

 **Note:** The **Switch Replication Source** operation fails if there is an existing project with the same LUN GUID and/or mountpoint that conflicts with the replica project.

 **Note:** If you perform the **Switch Replication Source** operation from a target array when your source array is live, IntelliFlash Web UI does not replicate the latest changes from Replication source to a Replication target array.

 **Caution:** The **Switch Replication Source** operation causes immediate disconnection of all active LUNs and shares within the project from the mapped hosts regardless of whether they participate in replication or not.

1. Log in to your replication target array.
2. Click **Provision > Projects > Replica**.
3. In the **Replica** tab, select a replica project and click **Manage > Data Protection > Replication** for the required project.
4. In the **Replication** tab, click **More > Switch Replication Source**.
5. In the confirmation, click **Yes**.

## Switch Replication Source: Source to Target

The **Switch Replication Source** option enables you to reverse the replication relationship. When you use this option your source array becomes the target and your target array becomes the source. You can use this option from the source array or target array.



**Caution:** The **Switch Replication Source** operation causes immediate disconnection of all active LUNs and shares within the project from the mapped hosts regardless of whether they participate in replication or not.

When you switch over from replication source array, the replication source array replicates the latest data to the target and reverse the relationship.



**Note:** The **Switch Replication Source** operation fails if there is an existing project with the same LUN GUID and/or mountpoint that conflicts with the replica project.

1. Log in to your replication source array.
2. Click **Provision > Projects**.
3. In the **Local** tab, select the required project.
4. Click **Manage > Data Protection > Replication**.
5. In the **Replication** tab, click **More > Switch Replication Source**.
6. In the confirmation, click **Yes**.

## Deleting a Replication Relationship

You cannot delete an ongoing replication. You can only delete a replication configuration that is in the Completed, Failure, or Aborted status.



**Note:** When you delete a replication configuration, IntelliFlash provides you the option to delete replicated projects and its dependents.

To delete a replication relationship, complete the following steps:

1. Click **Provision > Projects**.
2. In the **Local** tab, select the required project.
3. Click **Manage > Data Protection > Replication**.
4. In the **Replication** tab, click **Delete**.
5. In the **Delete Replication** window, complete the following steps:
  - a) (Optional) Click the toggle button to enable deleting snapshots and its dependent clones on the replication target array.



**Remember:** Do not enable this option if you need any of the shares or LUNs in the replica project on the target array.

- b) Type the word **Confirm** in the text box.
6. Click **Delete**.

The IntelliFlash Web UI displays a message when the deletion is in progress and the relationship disappears from the list.

### Related Topics

[Promoting a Replica Project](#)

## Managing outbound Replications systems

You can manage all your outbound replication configurations from the **Services > Replication > Overview** page. The page has **Inbound** and **Outbound** tabs. From the **Outbound** tab, you can view all replication target systems and their configuration details. You can manage all outbound replication relationships from this single page.

You can perform the following replication operations in the **Outbound** tab:

- **Start**
- **Pause**
- **Stop**

To manage outbound replication systems, complete the following steps:

1. Log in to the replication source storage array.
2. Click **Services > Replication > Overview**.
3. In the **Overview** page, click the **Outbound** tab.
4. In the **Outbound** tab, click the required replication configuration to view the replication configuration details and perform required operations.

## Monitoring Inbound Replication systems

You can monitor all your inbound replication configurations from the **Replication > Overview** page. The page has Inbound and Outbound tabs. From the Inbound tab, you can view all replication source systems and their configuration details from a single page.

1. Log in to the replication source storage array.
2. Click **Services > Replication > Overview**.
3. In the **Overview** page, click the **Inbound** tab.
4. In the **Inbound**, click the required replication configuration to view the replication configuration details.

## Adding Replication Target System from Partner Systems Page

To add a replication target system from **Services > Replication > Partner Systems** page, complete the following steps:

1. Click **Services > Replication > Partner Systems > Replication Targets**.
2. In the **Replication Targets** page, click **Add**.
3. In the **Add Replication Target** window, complete the following steps:
  - a) Type **Target Name/IP Address**.
  - b) Type **Username**.
  - c) Type the **Password**.



**Note:** Changing the username or password of the target array after setting up the replication relationship does not break the replication relationship.

4. Click **Add**.

## Modifying Replication Target host name or IP address

When you change the hostname or IP address of your replication target array, you can update it in the replication source array without breaking or disturbing the existing replication relationship.

You can modify replication target host name or IP address of a replication target array from the **Services > Replication > Partner Systems > Replication Targets** tab.

1. Click **Services > Replication > Partner Systems > Replication Targets**.
2. In the **Replication Targets** tab, select a partner hostname from the list and click **Edit Replication Host**.
3. In the **Edit Replication Host** window, modify the hostname or IP address.
4. Click **Save**.

## Deleting Replication Target System from Partner Systems Page

You can delete a replication target from the **Partner Systems** page.



**Note:** You must delete the replication configuration before deleting a replication target.

To delete a replication target from **Partner Systems**, complete the following steps:

1. Click **Services > Replication > Partner Systems > Replication Targets**.
2. In the **Replication Targets** tab, select a partner hostname from the list and click **Delete**.
3. In the confirmation screen, click **Yes**.

## Viewing Replication Source Systems from Partner Systems Page

You can view all replication source systems from the **Partner Systems** page.

To view a replication source systems from the **Partner Systems**, complete the following steps:

Click **Services > Replication > Partner Systems > Replication Sources**.

The **Replication Sources** tab displays the details.

## Managing Asynchronous Replica Projects

---

You can manage your replica project from your replication target systems. From the replica project's window (**Provision > Projects > Replica > Manage > Data Protection > Replication**).

### Managing Snapshot Schedule for a Replica Project

You can manage a snapshot schedule for replication process by specifying the duration for retaining the snapshot.

To create a custom snapshot schedule for a project, complete the following steps:

1. Click **Provision > Projects > Replica**.
2. In the **Replica** tab, select the required project.
3. Click **Manage > Data Protection**.
4. In the **Snapshots** tab, click the **Manage Schedules**.
5. In the **Manage Schedules** window, click **Override retention**.
6. In **Retain for** field, type the number of hours to retain the snapshot for the specified number of hours/weeks/months.
7. Click **Save**.

This preserves the snapshot for the specified duration.

 **Note:** IntelliFlash allows you to manage the snapshot schedule in both Graph and Table view.

## Setting a Quota Limit on a Replica Project

You can set storage quota limit on a replica snapshot on your replication target array.

 **Note:** Quota is the only option that you can edit on a replica project.

To set quota on a replica project, complete the following steps:

1. Click **Provision > Projects > Replica**.
2. In the **Replica** tab, select a required replica project.
3. Click **Manage > Settings**.
4. In the **General** tab, complete the following steps:
  - a) Select **Project Quota**.  
If the **Project Quota** checkbox is not selected, no quota limits are applied.
  - b) In the text field, type or select the quota size.
  - c) Select the required storage unit.
5. Click **Save**.

This preserves the snapshot for the specified duration.

 **Note:** IntelliFlash allows you to manage the snapshot schedule in both Graph and Table view.

## Setting a Quota Limit on a Share in a Replica Project

To set quota for a share or LUN on a replica project, complete the following steps:

1. Click **Provision > Projects > Replica**.
2. In the **Replica** tab, select a required replica project.
3. Click **Share**.
4. Click **Manage > Settings**.
5. In the **General** tab, complete the following steps:
  - a) Select **Share Quota**.  
If the **Share Quota** check box is not selected, no quota limits are applied.
  - b) In the text field, type or select the quota size.

- c) Select the required storage unit.
6. Click **Save**.

## Promoting a Replica Project

The **Promote** option allows you to break the replication relationship and converts a **Replica** project to **Local** project on your replication target array. Once you promote you cannot reverse this process. The replica project will become local project on your target array after performing the promote operation.

 **Note:** The promote operation fails if there is an existing project with the same LUN GUID and/or mountpoint that conflicts with the replica project.

 **Important:** After promoting a replica project, you should contact the IntelliFlash Technical Support team to delete the replica snapshot on the target array that is not visible in the UI.

### Prerequisite

At least one replication should have successfully completed before you attempt to promote the replica.

To promote a replication relationship, complete the following steps:

1. Log in to your replication target array.
2. Click **Provision > Projects > Replica**.
3. In the **Replica** tab, select a project and click **Manage > Data Protection** for the required project.
4. In the **Data Protection** window, click **Replication**.
5. In the **Replication** tab, click **More > Promote**.

 **Note:** The **Promote** operation uses only the latest replica snapshot for promoting a replica project.

6. (Optional) In the Promote to Local Project, disable the **Retain Snapshot Schedules** option.
7. Click **Promote**.

## Cloning a Project Snapshot from a Replica Project

You can clone a project snapshot from a replica project on the replication target storage array and reuse the project. After cloning you can see the project in the **Local** projects page.

You can clone using replica snapshots. When you clone a project snapshot from a replica project, all the shares and LUNs with the replica project are cloned.

 **Note:**

- Use a different name from the Replica project name when cloning a project. Using the same name as the Replica project might result in conflict with mountpoints or LUN GUIDs.
- No space reservation is applied when cloning a replica snapshot.

To clone a project snapshot on a target storage array, complete the following steps:

1. Log in to the replication target storage array.
2. Click **Provision > Projects > Replica**.
3. In the **Replica** tab, select a project and click **Manage > Data Protection > Snapshots** for the required project.
4. In the **Graph view** of the **Snapshots** tab, select a date in the graph.  
You can also select snapshots from the **Table view**.
5. In the **Snapshots** list, select a **Replication Snapshot** or a required snapshot from the list and click **Clone**.
6. In the **Clone Replica Snapshot** screen, complete the following steps:
  - a) Type in a **Target Project Name**.  
Target project name cannot be the same as any of the existing project names.
  - b) (Optional) Modify the **Target Project Mount Point**.
  - c) Select **Keep LUN GUID** option if it is required.
  - d) Click **Create**.

The cloned replica snapshot appears as a project in the **Local** page.

### Cloning a LUN Snapshot from a Replica Project

You can clone a LUN snapshot from a LUN that is part of a replica project on the replication target storage array and reuse the LUN. You can access the cloned LUN from the **LUN** page.



**Note:** No space reservation is applied when cloning a replica snapshot.

To clone a LUN snapshot on a target storage array, complete the following steps:

1. Log in to the replication target storage array.
2. Click **Provision > Projects > Replica**.
3. Select a required project from the **Replica** projects list.
4. Click **LUNs**.
5. In the **LUNs** tab, select a LUN and click **Manage > Snapshots** for the required project.
6. In the **Graph view** of the **Snapshots** tab, select a date in the graph.  
You can also select snapshots from the **Table view**.
7. In the **Snapshots** list, select a **Replication Snapshot** or a required snapshot from the list and click **Clone**.
8. In the **Clone Replica Snapshot** screen, complete the following steps:
  - a) Type in a **Target Project Name**.  
Target project name cannot be the same as any of the existing project names.
  - b) (Optional) Modify the **Target Project Mount Point**.
  - c) Click **Create**.

The cloned replica snapshot appears as a project in the **Local** page. You can access the cloned share from the **Share** page of the **Dataset** panel.

## Cloning a Share Snapshot from a Replica Project

You can clone a share snapshot from a share that is part of a replica project on the replication target storage array and reuse the share. You can access the cloned share from the **Share** page of the **Dataset** panel.



**Note:** No space reservation is applied when cloning a replica snapshot.

To clone a share snapshot on a target storage array, complete the following steps:

1. Log in to the replication target storage array.
2. Click **Provision > Projects > Replica**.
3. Select a required project from the **Replica** projects list.
4. Click **Shares**.
5. In the **Shares** tab, select a share and click **Manage > Snapshots** for the required share.
6. In the **Graph view** of the **Snapshots** tab, select a date in the graph.

You can also select snapshots from the **Table view**.

7. In the **Snapshots** list, select a **Replication Snapshot** or a required snapshot from the list and click **Clone**.
8. In the **Clone Replica Snapshot** screen, complete the following steps:
  - a) Type in a **Target Project Name**.  
Target project name cannot be the same as any of the existing project names.
  - b) (Optional) Modify the **Target Project Mount Point**.
  - c) Click **Create**.

The cloned replica snapshot appears as a project in the **Local** page. You can access the cloned share from the **Share** page of the **Dataset** panel.

## Deleting a Replica of a Project

Deleting a Replica project on a Replication target storage array deletes all shares, LUNs, replica snapshots, and breaks the replication relationship. The Replication source storage array displays the replication status as **Failure**.



**Caution:** Before deleting a replica project, ensure that you do not need the replica project for disaster recovery.

To delete a Replica project, complete the following steps:

1. Log in to your target storage array.
2. Click **Provision > Projects > Replica**.
3. Select a required project from the **Replica** projects list. and click **Delete**.
4. In the **Delete Replica Project** window, complete the following steps:
  - a) (Optional) Check to promote the latest snapshot.
  - b) Type the name of the replica project snapshot.
  - c) If *Two-Factor Authentication (2FA)* is enabled for the user, enter the 2FA application code retrieved from your mobile device to delete the replica project.
  - d) Click **Delete**.

IntelliFlash deletes the replica project and breaks the replication relationship.

## Deleting a Replica of a Share

You may need to delete a replica of a share to manage storage space on your replication target array.



**Note:** Deleting a replica of share on a Replication target storage array deletes all snapshots and dependent clones.

To delete a replica of a share, complete the following steps:

1. Log in to your target storage array.
2. Click **Provision > Projects > Replica**.
3. In the **Replica** projects list, select a required project from the list.
4. Click **Shares** and select a required share from the list.
5. Click **Delete**.
6. In the **Delete Share** window, complete the following steps:
  - a) Type the name of the replica share.
  - b) Click **Delete**.

## Deleting a Replica of a LUN

You may need to delete a replica of a LUN to manage storage space on your replication target array.



**Note:** Deleting a replica of a LUN on a Replication target storage array deletes all snapshots and dependent clones.

To delete a replica of a LUN, complete the following steps:

1. Log in to your target storage array.
2. Click **Provision > Projects > Replica**.
3. In the **Replica** projects list, select a required project from the list.
4. Click **LUNS** and select a required LUN from the list.
5. Click **Delete**.
6. In the **Delete LUN** window, complete the following steps:
  - a) Type the name of the replica LUN.
  - b) Click **Delete**.



---

# Chapter 18

---

## Network Settings

---

**Topics:**

- *Understanding the Network Interfaces*
- *Default Interface Groups*
- *Using the Array Management IP Address*
- *Unified Configuration of the Network*
- *General*
- *Interface*
- *SMTP*
- *Certificate*
- *Advanced*

## Understanding the Network Interfaces

IntelliFlash provides several networking features that allow you to configure IntelliFlash systems for different network environments and deployment scenarios.

### Physical and Logical Network Interfaces

#### Types of Physical Network Interfaces

Depending on the network interface cards installed, a schematic on the **Settings > Network > Interfaces** page of the IntelliFlash Web UI shows the exact location of the cards and their port numbers.

#### Names of Physical Interfaces

Physical network ports are named by the IntelliFlash OS and use the following naming conventions:

- For N-Series and H-Series systems, the on-board management ports start with *i40*. For example, *i40e0* and *i40e1*.
- Ethernet port names start with "cxgbe". For example, *cxgbe0* and *cxgbe1*
- Fibre Channel port names start with "qlt". For example: *qlt0* and *qlt1*.
- The names of the ports on the additional add-on card of the same type will be sequential. For example, if the array has two 100 GbE dual port cards, the names of the ports on the second card are *cxgbe2* and *cxgbe3*.



**Warning:** You must not alter the default names assigned to the network ports.

#### Types of Logical Network Interfaces

IntelliFlash systems support the following types of logical network interfaces:

- Aggregated links
- Interface groups
- Floating IP addresses

The physical network interfaces in an IntelliFlash array controller can be logically combined into aggregated links and interface groups. In addition, interface groups on the two controllers can be associated with a floating IP address.

When you use aggregate links, incoming traffic is spread over the multiple physical links that comprise the aggregate, and outbound traffic is spread based on the user-specified outbound policy. Therefore, adding more physical network interfaces to an aggregate link enhances the performance of the aggregate.

Interface groups improve overall network performance by automatically spreading outbound network traffic across the set of interfaces in the interface group when there are multiple IP data streams with different IP addresses.



**Attention:** Aggregate links and interface groups can be used together. However, as the configuration for creating interface groups over aggregate links is complex, contact IntelliFlash Technical Support team before you attempt such a configuration.

Floating IP addresses facilitate controller redundancy at the network level. In an IntelliFlash Array, if one controller fails, the other controller takes over. Floating IP addresses ensure that the IP addresses get bound to the other controller quickly and transparently.

For more information on the logical interfaces on an IntelliFlash array controller, see the following topics:

- [Understanding Link Aggregates](#)
- [Understanding Interface Groups](#)
- [Understanding Floating IP Addresses](#)

## Understanding Link Aggregates

Link aggregation, also referred to as port trunking, provides various methods for combining (or aggregating) several interfaces into a single, logical unit to increase the throughput of network traffic. It adds functionality beyond what a single connection could sustain, and provides redundancy in case one of the links fails.

Aggregated links work at the Data Link layer (Layer 2 of the OSI model) and employ a single logical MAC address to aggregate the bandwidth of the two or more physical interfaces.

Aggregated links also provide connection redundancy as the aggregated link works even if only one physical interface in the aggregate is functioning.

### LACP

IntelliFlash also supports creating aggregated links that are Link Aggregation Control Protocol (LACP) compliant. LACP is useful as it dynamically determines which aggregated links are available and how data should be distributed across them.

To create link aggregations that use LACP, you must set the **LACP Mode** field on the IntelliFlash array controller to either "Active" or "Passive". You must also set the LACP Mode for the corresponding ports on the switch to a matching value.

LACP uses LACP Data Units (*LACPDUs*) for exchanging information about the link aggregation between two nodes. The "Active" and "Passive" LACP modes determine when and how frequently a node generates LACPDUs. In the "Active" mode, the physical interfaces included in the aggregation transmit LACPDUs at regular (one of the two predefined) intervals.

- **Active**

The IntelliFlash OS generates LACPDUs at selected intervals, long (30 seconds) or short (1 second). In response, the corresponding switch must also send an LACPDU. Because LACP

allows only three attempts, the IntelliFlash OS terminates the LACP session if it does not get a response in either 90 seconds (three attempts over the "long" interval) or 3 seconds (three attempts over the "short" interval).

- **Passive**

The IntelliFlash OS generates an LACPDU only when it receives an LACPDU from the switch.



**Note:** If you configure both the aggregated link and the switch to passive mode, they cannot exchange LACPDUs. Therefore to use LACP, set the LACP mode on the switch to "active", and the LACP mode on the IntelliFlash array controller to "passive".

## Understanding Interface Groups

Interface groups improve overall network performance if there are multiple IP data streams with different destination IP addresses. In such situations, interface groups spread outbound network traffic across the interfaces in the interface group.



**Attention:** Interface groups are required for creating floating IP addresses on an IntelliFlash Array.

Interface groups allow a group of physical or logical interfaces to use one IP address. IP-layer links to the common IP address are distributed across the group in a round-robin manner. If an active interface fails, the IP address is immediately assigned to another interface in the group.

The IntelliFlash Array comes pre-configured with a number of Interface groups, as described in [Default Interface Groups](#).

## Understanding Floating IP Addresses

Floating IP addresses facilitate controller redundancy at the network level. In an IntelliFlash Array, if one controller fails, the other controller takes over. Floating IP addresses ensure that the IP addresses get bound to the other controller quickly and transparently.

Floating IP addresses can be used with the following types of services:

- Data access over NFS, SMB, and iSCSI
- Replication
- Plugins (the IDPS and the IntelliFlash NAS VAAI Plugin for VMware plugin)
- IntelliFlash REST APIs

The following list describes the various aspects of floating IP addresses.

- Floating IP addresses can be bound to interface groups only:
  - A floating IP address requires one interface group on each controller.
  - Interface groups that are used by a floating IP address are not required to have separate IP addresses. However, configure IP addresses for the interface groups for troubleshooting purposes.
- Together the pool and the floating IP addresses that are created on a controller constitute the resource group for that controller. A floating IP address is bound to all the pools in its resource group.
- There is no limit on the number of floating IP addresses you can define on a controller.

- You can include an interface group in multiple floating IP addresses.
- Defining as many floating IP addresses as the number of physical ports on a controller helps the IntelliFlash OS to optimally distribute the incoming traffic.
- Floating IP addresses automatically switchover to the other controller if the controller fails or if you explicitly perform a switchover.

## Default Interface Groups

All the arrays with a standard configuration have the following interface groups on each controller:

- *mgmt0*: The *mgmt0* Interface group is a required Interface group.
- *data\_10g\_0*: The *data\_10g\_0* interface group is created if the array includes an add-on 10-GbE card.
- *data\_40g\_0*: The *data\_40g\_0* interface group is created if the array includes an add-on 40-GbE card.



**Important:** It is recommended that you use the default interface groups listed above. However, if required, you can also create your own interface groups using available data ports.

## Using the Array Management IP Address

The Array Management IP address is a floating IP address that enables you to use a single IP address to manage your dual-controller IntelliFlash Array. You can use the Array Management IP address for the following purposes:

- To access the IntelliFlash Web UI and IntelliFlash REST APIs.
- To interface with 'App-Aware' plug-ins such as the IntelliFlash Manager plugin and IDPS.



**Note:** You can continue to use both the Controller Management IP addresses and the Array Management IP address after configuring the Array Management IP address.

### Configuring the Array Management IP Address after an Upgrade

The Array Management IP address is a required field for all new installs of IntelliFlash version 3.0.0 and higher. However, if the array is upgraded from a lower version, such as IntelliFlash version 2.1.3.5, the Array Management IP address is blank after the upgrade.



**Important:** For arrays upgraded to IntelliFlash version 3.5.0 or higher, you must:

- Configure an Array Management IP address in the **Management Network settings** section in the **Settings > Network > General** page.
- Generate an SSL certificate for the array using the array host name (Common Name or CN) and the array IP address in the **Settings > Network > Certificate** page.

## Unified Configuration of the Network

The **Network** page provides a unified interface that enables you to configure the network settings on both the controllers. Any change that you make using the unified interface is applied to both controllers simultaneously. All **Network** pages support the unified interface.

The **Interface** page in the Network Settings menu also allows you to configure the network interfaces on both controllers separately, if required. To configure the network interface settings separately, you must disable the unified interface. For more information, see [Using the Network Interface Page](#).



**Note:** The **Certificate** page also supports the unified interface and enables you to configure an SSL for both controllers. Use a Common Name (CN) that is applicable to the array hostname to generate the self-signed certificate.

## General

You can configure the following system-level settings from the **General** page:

- Date and time
- Passwords for the system accounts
- Management network



**Warning:** You must be careful while configuring these settings because incorrect settings can impair the functioning of the array at the system level, or disrupt existing data connections either permanently or temporarily.

### Configuring the System Date and Time

You can set the system date and time on the IntelliFlash array controller manually or synchronize the date and time with the Network Time Protocol (NTP) servers. The date and time setting is applied to both controllers when you save your changes.

To synchronize the date and time with NTP servers, you must select the **Automatic** option and add the NTP servers.

To configure the system date and time settings, complete the following steps:

1. Click **Settings > Network > General**.
2. In the **Date and Time Settings** section, select how you want to configure the date and time on the array. You have the following options:

Select	To...
<b>Automatic</b>	Synchronize the system time on both controllers with NTP servers. If you select this option, you must also ensure the

Select	To...
	required NTP servers are included by completing the following steps: 1. To add a new NTP server, type an IP address or hostname in <b>Add NTP Server</b> and click <b>Add</b> . 2. To delete an NTP server, click  for the corresponding NTP server.
<b>Manual</b>	Enter the date and time manually.

3. Select the required time zone.
4. Click **Save** to save the changes.

## Changing Passwords for Administrator Accounts

You can modify the passwords for the following accounts from the **Settings > Network > General** page:

- IntelliFlash Console administrator
- IntelliFlash Web UI administrator
- IPMI/BMC administrator

To modify passwords for any of these accounts, complete the following steps:

1. Click **Settings > Network > General**.
2. In the **Access Settings** section, select the accounts for which you want to change the passwords.
  - Select **Change Console Password** to change the password for the **zebiadmin** (console administrator) account.
  - Select **Change Web Password** to change the password for the **admin** (IntelliFlash Web UI administrator) account.
  - Select **Change KVM Password** to change the password for the **sfabmc** (IPMI/BMC administrator) account.



**Note:** The BMC password cannot contain more than 20 characters.

3. Type a new password and confirm it by retyping it in the **Confirm Password** field. Select **Show Password** to view the new password.
4. Click **Save**.



**Note:** When you change the IntelliFlash Web UI administrator password, use the new password at the next login.

## Modifying the Network Settings

You can use the IntelliFlash Web UI to modify the network settings of your array, including its domain, array, controller and BMC IP addresses, subnet, gateway, and DNS servers.



**Caution:** Changing the Array Management IP address also changes the plugin management IP address when the plugin management IP address is blank or the same as the previous Array Management IP address.

To modify the management network settings, complete the following steps:

1. Click **Settings > Network > General**.
2. In the **Management Network settings** section, enter the following array details:
  - Array host name
  - Domain
  - Array Management IP address
  - Subnet
  - Gateway
3. To add a DNS server, type the IP address of the DNS server in the **Add DNS Server** field and click **Add**.  
To add more DNS servers, repeat this step.  
The DNS servers you add appear in the **DNS server** section.
4. To delete a DNS server, click the delete icon ( ) for its corresponding IP address.
5. To modify the controller names, type a new name in the **Host Name** field for each controller.
6. In the **KVM Settings** section, you can do the following:
  - a) Enter a different subnet and gateway for the BMC.
  - b) Set the VLAN on the BMC if required.
  - c) Modify the BMC IP addresses for each controller.
7. Click **Save** to save the changes.

### Related Topics

[Using the Array Management IP Address](#)

## Interface

You can configure the network interfaces from the **Settings > Network > Interface** page.

## Using the Network Interface Page

The **Network Interface** page enables you to configure the physical and logical network interfaces in an IntelliFlash Array.

The **Interface** page includes the following sections:

- **Hardware:** Expand the **Hardware** section on top of the **Interface** page to view the Hardware schematic of the array. You can see the Ethernet and Fibre Channel cards present in each of the two controllers. When you mouse over the ports, you can view information such as the connection status, the speed, and the location. The ports are numbered consistently in the schematic.
- **Ethernet Interfaces:** The **Ethernet Interfaces** section displays the Ethernet physical ports and the link aggregates. This section enables you to:
  - Change the MTU values of the physical ports and the link aggregates
  - Add, modify, or delete a link aggregate
- **Ethernet Interface Groups:** The **Ethernet Interface Groups** section displays the interface groups, and the VLANs and IP addresses (fixed and floating) created on those interface groups. This section enables you to:
  - Add, modify, or delete an interface group
  - Add or delete VLANs in an interface group
  - Add or delete fixed and floating IP addresses in an interface group
- **Fibre Channel HBA Ports:** The **Fibre Channel HBA Ports** section lists the physical Fibre Channel HBA ports present in each controller. For each physical Fibre Channel port, you can see its status, the speed, world wide port name (WWPN), and the Nport ID.
- **Fibre Channel NPIV Ports:** The **Fibre Channel NPIV Ports** section displays the Fibre Channel NPIV ports (also called virtual FC ports). Each NPIV port is identified by its world wide port name (WWPN), and is associated to a pool and a physical Fibre Channel port from each controller.

When you mouse over a WWPN, you can view information such the N-Port ID, the associated pool, the associated physical port, and the controller on which it is active.

You can now edit the WWPN and WWNN of the automatically generated NPIV ports. The new WWPN you specify should be unique (should not exist already in the FC fabric) and follow the recommended OUI format, 51:c5:a0:b0:xx:xx:xx:xx.

In this section, you can change the association of an NPIV port to the physical FC port in the controller.

 **Note:** Only a single NPIV port can be associated to a physical FC port per pool. No two NPIV ports from the same pool can be mapped to the same FC port.

## Enabling the Unified Interface

To provide flexibility, the **Ethernet** tab under the **Settings > Network > Interface** section includes the **Unified UI** toggle button. This toggle button allows you to enable or disable the unified interface for the **Interface** page only.

When the unified interface is enabled, the **Interface** page displays a unified view of the controllers and the changes you make in the **Interface** page are applied on both the controllers.

The **Unified UI** button is automatically hidden if the Interface settings on both controllers do not match, or when the other controller is not accessible, or if you have manually disabled the feature to apply different settings on the controllers).

If you have manually disabled the **Unified UI** button, the system does not automatically enable the unified interface feature.

### Automatic Disabling and Enabling of the Unified Interface

The system periodically checks the state of the two controllers and compares their Interface settings. The system disables the unified interface feature if either of the following conditions is true:

- The other controller is inaccessible.
- Interface settings on both controllers do not match.

The system continues to perform periodic checks even after it has disabled the unified interface. If it detects that the other controller is accessible and the Interface settings on both controllers match, it automatically enables the unified interface.

### Manually Enabling the Unified Interface

When the **Unified UI** is disabled, the **Interface** page displays the two controllers. The interfaces on each controller can be configured separately and independently.

If you have manually disabled the unified interface, you cannot create floating IP addresses from the **Interfaces** page. To create floating IP addresses when the unified interface is disabled, use the **Settings > High Availability** page.

When you manually disable the unified interface, the system does not automatically re-enable the unified interface. You can manually switch back to the unified interface with the following steps:

1. Click **Settings > Network > Interface**
2. In the **Interface** tab, edit the interface settings to make them identical.
3. Click **Save**.  
This enables the **Unified UI** toggle button to appear.
4. Click the **Unified UI** toggle button.
5. In the **Confirmation** dialog box, click **Yes**.

### Modifying the Maximum Transmission Unit (MTU)

The Maximum Transmission Unit (MTU) value determines the size of the payload transmitted by a network interface. You can modify this value to enable Jumbo Frames, if your network infrastructure including the network interfaces on the host systems support it.

 **Note:**

- You cannot modify the MTU size on one controller, when the peer controller is down.
- You must consult the documentation for your network infrastructure to determine the exact MTU value you can use for enabling Jumbo Frames.
- MTU of all physical links is set to 9000 for new installations. In the case where you have not enabled end-to-end Jumbo Frames for the Ethernet ports supporting a given Interface Group, you need to change the MTU on that Interface Group to 1500.

To modify an MTU, complete the following steps:

1. Click **Settings > Network > Interfaces**.
2. In the **Ethernet** section, click **Interfaces** tab, and then click the **Edit** () icon corresponding to the interface or link aggregate you want to edit.
3. Edit the MTU as required.
4. Click **Done**.

## Adding a Link Aggregate

### Prerequisite

- You must have at least two physical ports available to create a link aggregate.

The Link Aggregation Control Protocol (LACP) provides a method to control a link aggregate. LACP allows a network device to negotiate an automatic bundling of links by sending LACP packets to the network switch (or another peer device) that is directly connected and implements LACP.



**Tip:** Set the LACP Mode as follows:

- **Passive** on the IntelliFlash array controller
- **Active** on the network switch

To add a link aggregate, complete the following steps:

1. Click **Settings > Network > Interface**.
2. In the **Ethernet** section, click the **Interfaces** tab, and then click **New Link Aggregate**.
3. Type a name for the **Link Aggregate Group Name**.
4. Select the ports you want to include in the link aggregate.  
Clicking a port selects or deselects it.



**Note:** A port is not available for link aggregation if it is already assigned to an Interface group.

## 5. Set the **Outbound Policy**.

The Outbound Policy specifies how packets are distributed across the available links in a link aggregate. You can select any of the following methods:

- **L2:** Hashes the MAC header of each packet to determine the outgoing link.
- **L3:** Hashes the IP header of each packet to determine the outgoing link.
- **L4:** Hashes the TCP, UDP, or other ULP header of each packet to determine the outgoing link

## 6. Set the **Mode**:

- **Off (Default):** The array does not generate LACP Data Units (LACPDUs).
- **Active:** The array generates LACPDUs at selected intervals, short or long.
- **Passive:** The array generates an LACPDU only when it receives an LACPDU from the switch.



**Warning:** If both the link aggregate and the network switch are in the passive mode, they cannot exchange LACPDUs.

## 7. Type a new value for the MTU, if needed.

## 8. Select the **LACP Timer**. You can set the timer as either **Long** or **Short**.

## 9. Click **Create**.

## 10. In the **Interfaces** section, click **Save**.

The link aggregate appears in the **Interfaces** section with the bundled interfaces. To view the complete names of the interfaces bundled, mouse over the link aggregate.

## Modifying a Link Aggregate

You can modify the link aggregate to change the aggregated link properties. To modify the link aggregate properties, complete the following steps:

### 1. Click **Settings > Network > Interface**.

### 2. In the **Ethernet** section, click the **Interfaces** tab.

### 3. Click the **Edit** ( ) icon for the link aggregate you want to edit.

### 4. Modify the required settings, and click **Done**.

The modified link aggregate appears in the **Interfaces** section with the bundled interfaces. To view the complete names of the interfaces bundled, mouse over the link aggregate.

## Deleting a Link Aggregate

### Prerequisites

You cannot delete a link aggregate if it is part of any interface group. You must first delete the interface group associated to the link aggregate that you want to delete.

To delete a link aggregate, complete the following steps:

1. Click **Settings > Network > Interface**.
2. In the **Ethernet** section, click the **Interfaces** tab.
3. Click the **Delete** (trash bin) icon for the link aggregate you want to delete.
4. In the **Interfaces** tab, click **Save**.

## Adding an Interface Group

### Prerequisites

When you add an interface group, add at least one floating or fixed IP address. You can add a floating IP address only if the unified interface is enabled on the **Interface** section.

 **Note:** To add a floating IP address when the **Unified UI** toggle button is disabled, use the **Settings > High Availability** page.

You must add at least one IP address when creating an interface group.

To create an interface group, complete the following steps:

1. Click **Settings > Network > Interface**.
2. In the **Ethernet** tab, click **Interface Groups**.
3. In the **Interface Groups** page, click **New Interface Group**.
4. Type a name for the interface group.  
The name can have a maximum of 11 characters.
5. To use a specific VLAN ID, select **VLAN ID** and type the required VLAN ID.

 **Note:** Use the **Default VLAN** unless a specific VLAN ID is required.

6. Select the interfaces you want to include in the interface group.  
Clicking a port selects or deselects it.
7. Complete the following steps to add a fixed or floating IP address to the group.
  - a) Enter an IP address and a netmask.
  - b) Select the type: **Fixed** or **Floating** from the dropdown list.

 **Note:** It is a good practice to add a fixed IP address to the interface group for traffic monitoring and troubleshooting issues.

- c) For a fixed IP address, select the controller to which it will be bound.

- d) For the floating type, select the required resource group and **Failover Mode**.

The **Failover Mode** determines the conditions for a failover. Valid options are:

- **Immediately**: Failure of the new IP address triggers a failover immediately. This is the default option.
- **Never**: Failure of the new IP address does not trigger a failover.
- **Wait until all IP addresses fail**: Failure of the new IP address does not trigger a failover if there are other floating IP addresses that are reachable.

- e) Click **Add**.

The new IP address is added to the interface group.

8. Click **Create**.

9. In the **Interface Groups** section, click **Save**.

## Modifying an Interface Group

### Prerequisites

You can add floating IP addresses from the **Settings > Network > Interface** page only if the **Unified UI** toggle button is enabled.

 **Note:** To add a floating IP address when the **Unified UI** toggle button is disabled, use the **Settings > High Availability** page.

You can modify an interface group to change the group properties—such as group name, VLAN ID, and ports included in the group—or to add or delete fixed or floating IP addresses.

 **Note:** If the unified interface is enabled you cannot delete the last IP address in the interface group. However, you can delete the interface group to delete all the associated IP addresses.

To edit an interface group, complete the following steps:

1. Click **Settings > Network > Interface**.

2. In the **Ethernet** section, click the **Interface Groups** tab.

3. Click the **Edit** () icon for the interface group you want to edit.

4. You can make the following changes:

- a) To add or remove physical interfaces from the group, click the network interface icons to select or deselect them.

 **Note:** Selected interfaces appear with a blue background. Interfaces that have not been selected appear with a white background.

- b) To add a fixed or floating IP address, enter the required fields and click **Add**.

- c) To remove a fixed or floating IP address, select the row and click the **Delete** () icon.

- d) To edit a fixed or floating IP address, remove the existing fixed or floating IP address and add a new interface with the required values.
5. Click **Done**.
  6. In the **Interface Groups** section, click **Save**.

## Deleting an Interface Group



**Warning:** Deleting an interface group also deletes all the VLANs, link aggregates, floating and fixed IP addresses defined within it.

To delete an interface group, complete the following steps:

1. Click **Settings > Network > Interface > Ethernet**.
2. In the **Interface Groups** section, click the **Delete** (trash bin) icon for the interface group you want to delete.
3. In the **Interface Groups** section, click **Save**.

## SMTP

---

### Understanding SMTP

The IntelliFlash OS includes a Simple Mail Transfer Protocol (SMTP) agent for sending email notifications to the required email addresses. You can secure the connection to the mail server through the SSL/TLS protocol.

Configure the SMTP settings on the array to:

- Connect to your SMTP server.
- Specify the email addresses to which email notifications will be sent.
- Use the CallHome feature to send email notifications to the Support team.

### Configuring SMTP

1. Click **Settings > Network > SMTP**.
2. In the **SMTP Settings** screen, click the **SMTP** toggle button to enable SMTP.
3. In the **Host** field, type the name or IP address of the SMTP mail server.
4. In the **Security** field, select the secure connection type.
  - **None:** Choose this option if you want a normal connection to the mail server. The default port number is 25.
  - **SSL/TLS:** Choose this option if you want to make a secure connection to the mail server through SSL/TLS from the beginning. The default port number is 465.

- **STARTTLS:** Choose this option if you want to open a normal connection to the mail server, and upgrade later to a secure connection using SSL/TLS. The default port number is 587.
5. In the **Port** field, the port number is automatically filled depending on the secure connection type you choose. Enter a different port number, if required.
  6. If the server requires authentication, click the **Authentication** toggle button to enable it.
    - a) In the **Username** field, type the user name of the account to be used for sending the emails.
    - b) In the **Password** field, type the password for the user account.
  7. In the **Senders Email** field, type the email address that will be identified as the sender of the notifications.
  8. In the **Send Notifications to** field, enter the email address to which notifications have to be sent, and click **Add**.  
If required, repeat this step to add more email addresses. Notifications are sent to the email addresses you provide here.
  9. Click **Save**.
  10. After saving the SMTP details, click the **Test Settings** button to test the SMTP settings.

## Certificate

---

### Securing Communications with TLS/SSL Certificates

IntelliFlash systems use TLS to secure the following types of connections:

- Connections that are required for High Availability (HA) between the two array controllers
- Connections with web browsers that access the IntelliFlash Web UI
- Connections with other IntelliFlash systems for replication
- Connections with Active Directory (AD) servers or other Lightweight Directory Access Protocol (LDAP) servers
- Connections with VMware Servers, vCenter Servers, and Hyper-V hosts
- Communication with IntelliFlash upgrade and support servers
- Communication with the IntelliCare server
- Connections with applications using the IntelliFlash REST APIs.
- Connections with IDPS running on Windows hosts
- Connections with SMI-S client software

IntelliFlash systems include root certificates of many root and intermediate Certificate Authorities (CAs). You can view these root certificates and install additional root certificates by following the procedures described in [Viewing a CA Certificate](#) and [Importing a CA Certificate](#).

IntelliFlash systems also include a Tegile root certificate and a Tegile intermediate CA certificate that you can use to create a self-signed certificate for the array. For more information, see [Generating a Self-Signed Certificate](#).



**Important:** The Tegile root (CA) certificate and the Tegile intermediate CA certificate are required in the IntelliFlash OS trust store for replication and HA features to function properly. If you delete the Tegile root certificate, it breaks the HA between the two controllers of the array and also breaks the replication relationships with the other IntelliFlash arrays, if any.

The **Certificate** page enables you to manage the TLS/SSL certificate and CA root certificates. You can access the **Certificate** page from the **Settings > Network** menu.



**Important:** You need to generate a new SSL certificate if you change the array host name or the array host IP address. This is mandatory for CA-signed certificates as the older certificate is not accepted by browsers and other clients.

## Support for TLS 1.2

TLS 1.2 addresses the security vulnerabilities observed in the earlier TLS versions. By default, both TLS 1.2 and TLS 1.0 are enabled in IntelliFlash. This ensures that all your existing replication relationships continue to work without any impact. When both TLS 1.0 and TLS 1.2 are enabled, the client and server generally negotiate to the highest protocol version that they both support.



**Warning:** If your replication source or replication target system does not support TLS 1.2, the existing replication relationship will break when you disable TLS 1.0. Contact IntelliFlash Technical Support for information and assistance on switching completely to TLS 1.2.

## Disabling TLS 1.0

By default, both TLS 1.2 and TLS 1.0 are enabled in IntelliFlash. This ensures that all your existing replication relationships continue to work without any impact. When both TLS 1.0 and TLS 1.2 are enabled, the client and server generally negotiate to the highest protocol version that they both support. TLS 1.2 addresses the security vulnerabilities observed in the earlier TLS versions.



**Note:** If you want to use secure HTTPS connection, disable TLS 1.0. However, some clients that do not support TLS 1.2 (for example IDPS) might fail to connect.

You can disable TLS 1.0 after performing the following prerequisites:

- Upgrading your IntelliFlash Operating Environment replication source and target systems to the IntelliFlash version that supports TLS 1.2.
- Configuring all other servers or clients that connect to the array to use TLS 1.2.

To disable TLS 1.0, complete the following steps:

1. Click **Settings > Network > Certificate**.  
The **TLS Settings** section displays the TLS versions that are currently enabled.
2. To disable TLS 1.0, select or clear the **Enable TLS v1.0** option.

## Generating a Self-Signed Certificate

A self-signed certificate is a certificate that is signed by the array itself, with Tegile Certificate Authority (CA). Generating self-signed certificates generates public and private key pairs and installs a temporary self-signed SSL/TLS certificate.



### Note:

- In IntelliFlash Operating Environment, array management is unified across both controllers. Therefore, a single TLS certificate is created and applied on both controllers.
- The Tegile public key infrastructure (PKI) contains an Intermediate CA added below the Tegile root CA certificate in the certificate chain. As a result, the self-signed certificate is signed by the Tegile intermediate CA Certificate instead of the root CA certificate.
- Enter the array name in the Common Name (CN) format when generating the self-signed certificate.

To generate a self-signed certificate, complete the following steps:

1. Click **Settings > Network > Certificate**.
2. In the **Current Certificate** section, click **New**.  
The **New Certificate** dialog box appears.
3. In the **New Certificate** dialog box, select **Create a self-signed certificate**, and type the following details:
  - Common Name (Required)
  - Alternate Name (Optional)
  - Organization Unit (Required)
  - Organization (Required)
  - City/Location (Required)
  - State/Province (Required)
  - Country (Required)
4. The **Alternate Name** field lists the controller-specific host names and host IP addresses. To add by a host name or IP address, type the host name or the IP address and click **Add**. To remove the names and IP addresses that you do not want to include, click the **Delete (X)** icon against the entry.
5. Click **Create**.

After the certificate is generated, the **Restart** dialog box prompts you to restart the IntelliFlash Web UI.

6. Click **Restart** to restart the IntelliFlash Web UI immediately (recommended).

## Generating a Certificate Signing Request

You can generate a Certificate Signing Request (CSR) file if you want to use a Certificate Authority (CA) signed certificate instead of a self-signed certificate. After generating the CSR, you can download the CSR file and send it to a CA for signing. After you receive the signed certificate back from the CA you have to import it, as explained in [Importing a CA Certificate](#). Because the Array Management IP address is unified across both the controllers, only one certificate is required for the array,



**Warning:** The CSR includes only the public key that is sent to the CA. Do not share the private key.



**Important:** Download and securely back up the private key, because there is no way to recover it when it is corrupted or accidentally overwritten.

To generate a certificate signing request, complete the following steps:

1. Click **Settings > Network > Certificate**.
2. In the **Current Certificate** section, do any of the following:
  - Click the **Download Request File** link.  
The CSR file is downloaded to the local system.
  - Alternatively, click **New** and complete the following steps:
    1. In the **New Certificate** dialog box, select **Create a request for Certificate from a certification authority**.
    2. Click **Create**.
    3. In the **Download Certificate Request File** dialog box, click **Download File**.  
The CSR file is downloaded to the local system.
    4. Click the **Close (X)** icon to close the **Download Certificate Signing Request** dialog box.

### Related Topics

[Importing a CA Certificate](#)

[Exporting the Current Certificate or Private Key](#)

## Exporting the Current Certificate or Private Key

You can export and back up the current certificate and the private key used by the IntelliFlash Array.

To export the current certificate or private key, complete the following steps:

1. Click **Settings > Network > Certificate**.
2. In the **Current Certificate** section, click **Export**.  
The **Export Certificate** dialog box appears.
3. Select **Certificate** or **Private key**, depending on what you want to export.
4. Click **Export**.

The certificate or the private key is downloaded to your local system.



**Warning:** The private key is required only on the IntelliFlash Array. You must back it up safely and not share it with unauthorized personnel, as it can compromise the safety of the array.

5. After downloading the certificate or the private key, click the **Close** (X) icon to close the **Export Certificate** dialog box.

### Related Topics

[Importing a CA Certificate](#)

## Importing a New Certificate or Private Key

You might need to import a certificate if you used a third-party application to generate it or when you receive the CA-signed certificate back from a Certificate Authority (CA). Similarly, you might need to import a private key if you generated the CSR using a third-party application or if the private key in the keystore of the IntelliFlash Array was changed after you generated the CSR.



**Warning:** Importing a certificate or a private key overwrites the existing certificate or private key.

To import a private key into the IntelliFlash Array, complete the following steps:

1. Click **Settings > Network > Certificate**.
2. In the **Current Certificate** section, click **Import**.  
The **Import Certificate** dialog box appears.
3. Select **Certificate** or **Private key**, depending on what you want to import.
4. Click **Browse** and select the file.
5. Click **Import**.

IntelliFlash checks the integrity of the certificate and then imports it. To complete the import, IntelliFlash is automatically restarted.

## Related Topics

- [Exporting the Current Certificate or Private Key](#)
- [Generating a Certificate Signing Request](#)

## Viewing a CA Certificate

To view a CA certificate, complete the following steps:

1. Click **Settings > Network > Certificate**.
2. In the **Installed CA Certificates** section, select the CA certificate that you want to view and click **View**.  
The **Certificate Details** dialog box appears. Use the scroll bar to view the complete details.
3. Click **Close** (☒) to close the **Certificate Details** dialog box.

## Deleting a CA Certificate



**Important:** The Tegile root (CA) certificate and the Tegile intermediate CA certificate are required in the IntelliFlash OS trust store for replication and HA features to function properly. If you delete the Tegile root certificate, it breaks the HA between the two controllers of the array and also breaks the replication relationships with other IntelliFlash arrays, if any.



**Warning:** Deleting a required CA certificate can disrupt communications within the array or between the array and other systems. Before you delete a CA certificate, make sure that it is not required.

To delete a CA certificate, complete the following steps:

1. Click **Settings > Network > Certificate**.
2. In the **Installed CA Certificates** section, select the CA certificates that you want to delete and click **Delete**.
3. In the **Confirmation** dialog box, click **Yes**.

## Importing a CA Certificate

IntelliFlash systems include several CA certificates by default. You can also import CA certificates to add new CA certificates or update existing ones with newer versions.



**Attention:** Importing a CA certificate restarts the IntelliFlash Web UI.

To import a certificate chain, complete the following steps:

1. Click **Settings > Network > Certificate**.
2. In the **Installed CA Certificates** section, click **Import CA Certificates**.
3. In the confirmation dialog box, click **Yes** to continue.
4. In the **Open** dialog box, browse to the folder that contains the CA certificate file that you want to import and click **Open**.

The CA certificate is imported if the file is valid and the IntelliFlash Web UI is restarted.

## Resetting CA Certificates

You can use the **Reset CA Certificates** option to restore the CA certificate store to factory default settings. This command removes any CA certificates that you may have imported, and adds back any factory default CA certificates that you may have removed.

To reset CA certificates, complete the following steps:

1. Click **Settings > Network > Certificate**.
2. In the **Installed CA Certificates** section, click **Reset CA Certificates**.
3. In the **Confirmation** dialog box, click **Yes** to continue.



**Note:** The IntelliFlash Web UI restarts after generating the trust store for the controller.

## Advanced

---

### Enabling HTTP Proxy Settings

A proxy server is a server that acts as an intermediary for requests from servers seeking resources from other servers. A client connects to the proxy server to request a service (for example, a file, connection, web page, or another resource) available from a different server. The proxy server evaluates and sends the request.

IntelliFlash systems communicate with the IntelliFlash support server in the cloud to download software updates and to upload IntelliFlash Manager plugin information. You can configure a web proxy server to enable the IntelliFlash Array to communicate with the IntelliFlash support server.

To enable and configure a proxy server, complete the following steps:

1. Click **Settings > Network > Advanced**.
2. In the **Proxy** section, enable the **HTTP Proxy** button.
3. In the **Host** field, type the host name or IP address of the proxy server.
4. In the **Port** field, type the port number of the proxy server.
5. Click **Save** in the **Advanced Settings** page to save the changes.

## Enabling SOCKS Proxy Settings

You can configure a SOCKS proxy to enable the IntelliFlash Array to communicate with IntelliShell for remote access.

To enable and configure a SOCKS proxy server, complete the following steps:

1. Click **Settings > Network > Advanced**.
2. In the **Proxy** section, enable the **SOCKS Proxy** button.
3. For the **SOCKS Version**, select **Version 4** or **Version 5**.
4. In the **Host** field, type the host name or IP address of the proxy server.
5. In the **Port** field, type the port number of the proxy server.
6. Click **Save** in the **Advanced Settings** page to save the changes.

## Adding a Static Route

A static route is not required, but it can be useful in certain conditions. For example, when a network has multiple routers or IP subnets, or when you need to provide SMB share access to end users across a LAN.

To configure a static route, complete the following steps:

1. Click **Settings > Network > Advanced**.
2. In the **Routing** section, click **Add**.  
The **Add Routing** dialog box appears.
3. In the **Add Routing** dialog, select the type of route you want to add and enter the required values:

If you select...	Enter...
<b>default</b>	The <b>Gateway</b> IP address and the <b>Interface</b> on which the route applies.

If you select...	Enter...
<b>network</b>	Type the <b>Gateway</b> IP address, select an <b>Interface</b> , and type a <b>Network Address</b> and <b>Subnet mask</b> .
<b>host</b>	Type the <b>Gateway</b> IP address, select an <b>Interface</b> , and type a <b>Host IP</b> address.

4. Click **Add** to add the route.
5. In the **Advanced Settings** page, click **Save** to save the changes.

## Modifying a Static Route

To modify a static route, complete the following steps:

1. Click **Settings > Network > Advanced**.
2. In the **Routing** section, select the route that you want to edit and click **Edit**.  
The **Edit Routing** dialog box appears.
3. In the **Advanced Settings** page, click **Save** to save the changes.

## Deleting a Static Route

To delete a static route, complete the following steps:

1. Click **Settings > Network > Advanced**.
2. In the **Routing** section, select the route that you want to delete and click **Delete**.
3. In the **Advanced Settings** page, click **Save** to save the changes.

## Adding a Local Host

To add a host, complete the following steps:

1. Click **Settings > Network > Advanced**.
2. In the **Local Hosts** section, click **Add**.
3. In the **Advanced Settings** page, click **Save** to save the changes.  
The newly added host appears in the **Local Hosts** section.

## Deleting a Local Host

To delete a host in the local hosts file, complete the following steps:

1. Click **Settings > Network > Advanced**.
2. In the **Local Hosts** section, select the local host entry you want to delete and click **Delete**.
3. In the **Advanced Settings** page, click **Save** to save the changes.



---

# Chapter 19

---

## High Availability Settings

---

**Topics:**

- [\*Setting up High Availability\*](#)
- [\*High Availability Advanced Settings\*](#)
- [\*Switching Over Resource Groups between Controllers\*](#)
- [\*Manually Setting Resource Groups to Offline\*](#)
- [\*Manually Setting Resource Groups to Online\*](#)
- [\*Guidelines for Creating Floating IP Addresses\*](#)
- [\*Configuring the Floating IP Address\*](#)
- [\*Removing High Availability Configuration\*](#)

High Availability (HA) provides the redundancy needed to make sure that the IntelliFlash Array services are live and online with a minimum of downtime. The IntelliFlash controllers maintain availability by using a storage pool-sharing service. When the IntelliFlash OS detects a failure, it automatically transfers ownership of the shared pool to the other controller.

When a failure occurs, all configured pool services automatically switch over to the other controller. The IntelliFlash OS ensures service continuity during exceptional events, including power outages, network connectivity failures, and appliances crashing. The switchover and recovery time is largely dependent on the amount of time it takes to switch over the data pool to the alternate controller.



**Warning:** Do not change any HA setting or use any HA feature on your own. Contact IntelliFlash Technical Support if you need to change an HA setting or use an HA feature described in this chapter.

The **High Availability** menu option does not appear for a single controller array. HA is supported only on the dual controller models.

## Setting up High Availability

---

High Availability (HA) is pre-configured in IntelliFlash systems. For these arrays, you need to set up High Availability only if you remove the HA configuration for maintenance purposes, such as replacing a failed controller.

To set up High Availability, complete the following steps:

1. Log in to the new controller.
2. Click **Configure HA**.
3. Type the webadmin account credentials of the peer controller.
4. Click **Add**.

IntelliFlash configures HA on both controllers and reboots each controller, one at a time, starting with the current controller.

Log in to the IntelliFlash Web UI again. If you had completed a fresh install on the array before you configured High Availability, the Configuration Wizard (CW) appears. If it is not a fresh install, you can open the **Settings > High Availability** page to confirm that HA has been set up successfully.

## High Availability Advanced Settings

---

The advanced settings for High Availability are as follows:

- **Global Fencing:** Fencing is the process of isolating a node in an High Availability environment and protecting shared resources when a node malfunctions.  
The default option is SCSI-3 like reservation.
- **Heartbeat Interval:** A heartbeat is a periodic communication attempt in which nodes exchange information about their states and the services running on them.
- **Heartbeat Timeout:** Before switching a pool to another node, the IntelliFlash Array must first detect a failure. The failure is determined by counting consecutive missed heartbeats. The heartbeat timeout is the amount of time for which a node can fail to communicate, or send heartbeats, before the IntelliFlash Array switches the pool to the active node.
- **Pingpong Interval:** This option prevents a service that fails to start from endlessly looping, which results in the service migrating back and forth between cluster nodes. After the switchover, if the service experiences problems on the new node, then the IntelliFlash Array does not switch the service back to its original node unless the time period, as defined by the resource group's pingpong interval, has passed.
- **Auto Fallback (switchback):** When the IntelliFlash Array detects the failures are fixed, this option enables the IntelliFlash Array to automatically switch the resource group back to its predefined auto-failback node after that node is rebooted.

## Modifying the High Availability Global Settings

To modify the High Availability (HA) settings, complete the following steps:

1. Click **Settings > High Availability**.
2. In the **High Availability** page, click the **Settings** (⚙️) icon.  
The **Advanced Settings** window appears.
3. In the **Global** tab, change the settings as required.  
For information on the Global settings, see [High Availability Advanced Settings](#). Contact IntelliFlash Technical Support team before you edit these settings.
4. Click **Save**.

## Configuring the Plugin Management IP Address

External plugins use the Plugin Management IP address to communicate with the IntelliFlash Array.

In arrays that have a fresh installation of IntelliFlash version 3.x, the Plugin Management IP address is the same as the Array Management IP address. However, you can use a different floating IP address as the Plugin Management IP address, if desired.

To use a different IP address for plugin management, you can directly change the Plugin Management IP address by using the **Advanced Settings** in the **High Availability** page .

 **Note:** Changing the Plugin Management IP address directly and using an IP address that is different from the Array Management IP address decouples the plugin management IP address from the Array Management IP address. Future changes to the Array Management IP address do not impact the Plugin Management IP address.

For more information, see [Using the Array Management IP Address](#).

To change the **Plugin Management** IP address, complete the following steps:

1. Click **Settings > High Availability**.
2. In the **High Availability** page, click the **Settings** (⚙️) icon.  
The **Advanced Settings** window appears.
3. In the **Plugin Address** tab, select a floating IP address from the **Plugin Management Address** dropdown list.
4. Click **Save**.

## Understanding Quorum Disks

A cluster node shares data and resources with the other node in the cluster. Therefore, a cluster must never split into separate partitions that are active at the same time. Multiple active partitions

might cause confusion and data corruption. The quorum algorithm guarantees that only one instance of the same resource is operational at any time, even if the cluster interconnect is partitioned.

Two types of problems arise from cluster partitions:

- **Split Brain:** Occurs when the cluster interconnect between nodes is lost. Each partition believes that it is the only surviving partition because the node in one partition cannot communicate with the node in the other partition.
- **Amnesia:** Amnesia occurs when the cluster node restarts after a shutdown with cluster configuration data older than the time of the shutdown.

IntelliFlash systems avoid these problems by allowing the quorum disks to govern the cluster, ensuring that integrity is maintained when the partitions are separated.

Additionally, when upgrading the IntelliFlash OS, the upgrade script checks to make sure that the quorum is healthy. A quorum is considered healthy if the controller is in HA-mode. If the controller is not in HA-mode, then the IntelliFlash Array triggers a warning message.

## Refreshing the Quorum Disks

You must refresh the Quorum disks every time you replace, remove, or add a drive in the array.

To refresh the quorum, complete the following steps:

1. Click **Settings > High Availability**.
2. In the **High Availability** page, click the **Settings** (⚙) icon.  
The **Advanced Settings** window appears.
3. In the **Quorum Device** tab, click **Refresh Quorum Disks**.

## Switching Over Resource Groups between Controllers

---

High Availability allows you to manually switch over a resource group from one controller to the other.

To manually switch a resource group, complete the following steps:

1. Click **Settings > High Availability**.
2. In the **High Availability** page, click the down arrow in the controller resource group, and select **Switch over resource group**.
3. In the **Confirmation** dialog box, click **OK**.
4. To transfer the resource group back to the original controller, click the down arrow in the corresponding controller resource group, and click **Switch back resource group**.
5. In the **Confirmation** dialog box, click **OK**.

## Manually Setting Resource Groups to Offline

---

You can manually take a resource group to offline. You might want to do this to upgrade, add hardware, or repair the system.

To take a resource group offline, complete the following steps:

1. Click **Settings > High Availability**.
2. In the **High Availability** page, click the down arrow in the corresponding resource group tab, and select **Take All Resources Offline**.
3. In the **Confirmation** dialog box, click **OK**.

## Manually Setting Resource Groups to Online

---

If a resource group is offline, you can easily set it back to online status.

To manually bring a resource group online, complete the following steps:

1. Click **Settings > High Availability**.
2. In the **High Availability** page, click the down arrow in the corresponding resource group tab, and click **Bring All Resources Online**.
3. In the **Confirmation** dialog box, click **OK**.

## Guidelines for Creating Floating IP Addresses

---

For more information about floating IP addresses, see [Understanding Floating IP Addresses](#) and [Configuring the Floating IP Address](#).



**Notice:** All guidelines given in this topic are optional, but proven to be effective in many deployment scenarios. You must carefully evaluate your requirements before you implement any of these guidelines. You can also discuss these guidelines with the IntelliFlash Technical Support team, if required.

Follow these guidelines while creating floating IP addresses:

- To load balance the traffic, create floating IP addresses for all the switches connected to the IntelliFlash array controller.
- On each controller, create one floating IP address for each physical interface that is to be used for data access.
- On each controller, create a floating IP address for accessing the IntelliFlash plugins and the IntelliFlash REST APIs. Create this floating IP address on the management interface groups.



**Note:** Depending on your requirements and IP address availability, you can also use separate floating IP addresses for accessing the IntelliFlash plugins and the IntelliFlash REST APIs.

- When setting up a replication, you must provide a floating IP address that is associated with a pool.

## Configuring the Floating IP Address

---

A pool can contain IP-based storage resources, such as iSCSI LUNs, SMB, and NFS file shares. To share these resources, configure a floating IP address for the controller that contains the pool. The pool and the floating IP addresses that were created on a controller constitute the **resource group** for that controller.

To configure the floating IP address, complete the following steps.

1. Click **Settings > High Availability**.
2. In the controller tab, click **Add Floating IP**.  
The **Add Floating IP** dialog box appears.
3. In the **Add Floating IP** dialog box, type an IP address and netmask.
4. Select the **Interface Group** on which the floating IP address is to be created.



**Note:** If the IntelliFlash Web UI is in non-unified mode, you have to select an **Interface Group** on both the controllers.

5. Select the required **Failover Mode**.

The Failover Mode determines the condition for failover. Valid options are:

- **Immediately (default)**: Failure of the new IP address triggers a failover immediately.
- **Never**: Failure of the new IP address does not trigger a failover.
- **Wait until all IPs fail**: Failure of the new IP address does not trigger a failover if there are other floating IP addresses that are reachable.

If you do not select any value, the "Immediately" option is used, by default.

6. Click **Add**.

## Removing High Availability Configuration

---

To perform any maintenance activity on the array that requires a controller to be powered down, you must first remove the controller from the High Availability (HA) configuration.

Removing a controller from the HA configuration involves two tasks:

- Booting the controller in non-HA mode

- Removing the controller from the HA mode

You can perform both these tasks from the **Settings > High Availability** page of the IntelliFlash Web UI.

To remove a controller from the HA configuration, complete the following steps:

1. Click **Settings > High Availability**.
2. Do the following to reboot the controller in non-HA mode:
  - a) Click **Reboot**.
  - b) In the **Reboot Options** dialog box, select **Reboot this controller to Non-HA mode**.
  - c) Click **Reboot**.
  - d) In the **Confirmation** dialog box, click **Yes**.  
Before the controller reboots, its resource group is shifted to the other controller.
3. If you are connected to the controller you have rebooted, the web page refreshes and returns to the login screen. Log on to IntelliFlash Web UI of the controller.
4. Do the following to remove the controller from the HA pair:
  - a) Click **Settings > High Availability**.
  - b) Click **Reboot** for the same controller.
  - c) In the **Reboot Options** dialog box, select **Remove this controller from the HA pair**.
  - d) Click **Reboot**.
  - e) In the **Confirmation** dialog box, click **Yes**.



---

# Chapter 20

---

## SNMP Settings

---

**Topics:**

- *Introduction to SNMP*
- *Using the SNMP Management Information Base (MIB) File*
- *Setting Up SNMP Tools*
- *Configuring SNMP on the IntelliFlash Web UI*
- *Supported SNMP Traps*

## Introduction to SNMP

IntelliFlash systems support the Simple Network Management Protocol (SNMP). SNMP is a management protocol for configuring and collecting information from network devices and routers over an Internet Protocol (IP) network. The SNMP Agent is included in the IntelliFlash Operating Environment. The SNMP Agent listens to SNMP requests on port 161 and sends SNMP traps or notifications to the port specified by the user (typically port 162).

The IntelliFlash Plugins page provides a Management Information Base (MIB) file separately. The MIB file mirrors the information provided on the Dashboard and Analytics tabs of the IntelliFlash Web UI from IntelliFlash data objects such as Pools, Projects, LUNs, and so on. The MIB file can be downloaded through the IntelliFlash Web UI (under **Settings > Administration > Plugins**). See [Setting Up SNMP Tools](#) for details.

 **Note:** Use the Array Management IP address when specifying the address of the IntelliFlash System in your SNMP manager software (NMS or MIB browser). If one of the controllers is down, the Array Management IP address allows you to access the array without having to specify the IP address of the other controller.

### Features supported by the SNMP Agent

The following features are supported by the SNMP Agent:

- SNMP v2c
- SNMP Traps
- GET, GET NEXT and, GET BULK SNMP commands

### Limitations of the SNMP Agent

The following are the limitations of the SNMP Agent:

- SNMP v1 and SNMP v3 are not supported.
- SET and INFORM SNMP commands are not supported.
- The SNMP manager software (NMS or MIB browser) performs read-only operations and does not set or configure information on IntelliFlash systems.
- You cannot select or filter which traps to send to the SNMP Trap listeners. Either all SNMP Traps are sent or none are sent from the SNMP Agent.
- I/O information is shown in MBps not KBps.

 **Note:** Earlier, the 64-bit values were split into high and low 32-bit values. The SNMP values are now represented as 64-bit values.

For the complete list of supported SNMP traps, see [Supported SNMP Traps](#).

## Using the SNMP Management Information Base (MIB) File

You can use the SNMP Management Information Base (MIB) file with your MIB browser or SNMP management software to view supported SNMP alerts sent by the SNMP agent on the IntelliFlash array. The IANA Private Enterprise Number (PEN) is 43906.

For example, the object identifier (OID) for “haControllerA-Name” is .1.3.6.1.4.1.43906.1.1.1. This can be described as:

```
iso(1).identified-organization(3).dod(6).internet(1).private(4)
.enterprise(1).tegile(43906).tegile(1).Properties(1).haControllerA-Name(1)
```

The OID indexes of the table entries are now retained even after adding or deleting objects, or when the array is rebooted. Earlier, the OIDs of object rows changed whenever objects were added or deleted.

IntelliFlash also includes support for the following new SNMP tables:

- Hyper-V VM analytics
- Data Link Aggregates (network)
- Interface Group (network)



### Note:

The OIDs for some of the fields in the MIB file have changed to accommodate adding the new tables. See the MIB file to view the new OIDs.

## Setting Up SNMP Tools

- Make sure your SNMP Network Management Software (NMS) or MIB browser is ready to use.
- Specify the management IP address and community string of the IntelliFlash system in your MIB browser or NMS to connect to the SNMP Agent on the IntelliFlash system. Make sure that you specify the same community string as the one mentioned in the **SNMP Settings** page, otherwise, GET requests will be ignored.



**Note:** Earlier, the SNMP MIB split 64-bit values into high and low 32-bit values. Now, the SNMP values are represented as 64-bit values.

## Downloading MIB File from the IntelliFlash Web UI

You can download the SNMP MIB file from the IntelliFlash Web UI.

1. Click **Settings > Administration > Plugins**.
2. In the **Plugins** page, under the **SNMP MIB** section, click the **Download** button.
3. Save the MIB file locally.

The current IntelliFlash version includes SNMP MIB version 2.0.0.1.

## Loading MIB File to NMS or MIB Browser

### Prerequisites

Open your NMS or MIB browser and specify the array management IP address of your IntelliFlash system in **Address** field to connect to the SNMP Agent on your IntelliFlash system.

1. Open the downloaded SNMP MIB file.
2. Follow the NMS specific instructions to retrieve information from the IntelliFlash system.

## Configuring SNMP on the IntelliFlash Web UI

---

You need to use the IntelliFlash Web UI to enable SNMP and add SNMP listeners on the IntelliFlash system.

### Enabling SNMP on the IntelliFlash System

By default, SNMP is disabled on IntelliFlash systems. You must enable SNMP to retrieve information and capture important events (traps) from the IntelliFlash system.

To enable SNMP on the IntelliFlash system, complete the following steps:

1. Click **Settings > Network > SNMP**.
2. Click **Edit**.  
The **SNMP Settings** page appears.
3. In the **SNMP Settings** page, check the **Enable SNMP** field.
4. Click **Save**.  
All changes are committed only after the **Save** button is clicked.

### Modifying the Community String

After SNMP is enabled on the array, you can modify the community string of the SNMP Agent, if needed.



**Note:** The default community string is not provided for the IntelliFlash system. The SNMP Community String cannot be longer than 64 characters and it cannot contain blank spaces or any of the following special characters: / \ ! ? @ < > ` # \$ % ^ \* ( ) : ~ + = { } , | [ ] ; \ &.

1. Click **Settings > Network > SNMP**.
2. Click **Edit**.

The **SNMP Settings** page appears.

3. In the **SNMP Settings** page, select the **Enable SNMP** field.
4. Select the **Change Community String** field.
5. Enter the new community string in the **Community String** field.
6. Re-enter the community string in the **Confirm Community string** field.
7. To view the community string while typing a new string, select the **Show String** field.
8. Click **Save**.

## Adding an SNMP Trap Listener

You will need to add the IP address of the server (NMS or MIB browser) that receives or listens to the traps sent by the SNMP Agent on the IntelliFlash system.

To add an SNMP Trap listener, complete the following steps:

1. Click **Settings > Network > SNMP**.
2. In the **Add Trap Listener IP** text box, type the IP address of the device which will receive SNMP traps from the SNMP Agent. By default, the port field defaults to 162, but you can change this if you want to use another port.
3. Click **Add**. The entry appears in the list below.
4. Click **Save**. All changes are committed only after the **Save** button is clicked.



**Note:** A maximum of 10 trap listeners can be configured. If 10 trap listeners already exist, a warning appears when you try to add another trap listener.

## Deleting an SNMP Trap Listener

To delete an SNMP Trap listener, complete the following steps:

1. Click **Settings > Network > SNMP**.
2. In the **Trap Listener List** section, click against the SNMP listener that you want to delete.
3. Click **Save**.

## Sending a Test Trap to SNMP Trap Listeners

- SNMP is enabled.
- Trap listener(s) is added.
- The settings are saved.

You can use the **Send Test Trap** button to send a test trap to all trap listeners in the list, after you have added them and saved the settings. This verifies that the IntelliFlash system can

broadcast to the trap listeners and that the trap listeners can receive traps from the SNMP Agent on the IntelliFlash system. Test traps are treated like any other events that occur on the IntelliFlash system.

The description of the test trap is:

```
Test trap sent by SNMP Agent (2.0.0.1).
```

To send a test trap to SNMP Trap listener, complete the following steps:

1. Click **Settings > Network > SNMP**.
2. In the **Trap Listener** section, click **Send Test Trap**. The test trap is sent to the SNMP Trap listener.

 **Note:** If the Trap Listener does not receive trap, ping and ensure that the Trap Listener server is reachable from the IntelliFlash system.

## Supported SNMP Traps

---

**Table 8: Supported SNMP Traps**

Event Notification Type	Event ID Description
Disk	<b>diskIsOnline</b> Disk is online.
	<b>diskGoneOffline</b> Disk is offline.
	<b>diskError</b> Disk error
	<b>spareDiskReplaced</b> Spare disk replaced.
	<b>diskSlowIo</b> Slow I/O operations observed on Disk.

Event Notification Type	Event ID Description
Array	<p><b>dnsServersUnreachable</b>            Some DNS servers are not reachable.</p> <p><b>allDnsServersUnreachable</b>            All configured DNS servers are not reachable.</p> <p><b>intellishellSessionStarted</b>            Intellishell session started.</p> <p><b>intellishellSessionEnded</b>            Intellishell session ended.</p>
Pool	<p><b>poolCreated</b>            Pool is created.</p> <p><b>poolDiskReplaced</b>            Disk replaced with a new disk in the pool.</p> <p><b>poolDeleted</b>            Pool is deleted.</p> <p><b>poolDeletionFailed</b>            Pool deletion attempt failed.</p> <p><b>poolExpanded</b>            Pool is expanded.</p> <p><b>poolDegraded</b>            Pool is degraded.</p> <p><b>poolExported</b>            Pool is exported.</p> <p><b>poolImported</b>            Pool is imported.</p> <p><b>poolUpgraded</b>            Pool is upgraded.</p>

Event Notification Type	Event ID Description
	<p><b>poolQuotaExceedThresholdWarning</b> Pool quota exceeded the threshold limit.</p> <p><b>poolMetaDataQuotaExceedThresholdWarning</b> Pool metadata quota exceeded the threshold limit.</p> <p><b>poolAvailableMetaToDataRatioBelowThresholdWarning</b> Available Pool metadata to data ratio is below the threshold limit.</p> <p><b>poolQuotaFinished</b> Pool quota finished.</p>
Project	<p><b>projectCreatedSuccessfully</b> Project created successfully.</p> <p><b>projectDeletionFailed</b> Project deletion failed.</p> <p><b>projectDeleted</b> Project is deleted.</p> <p><b>projectModified</b> Project is modified.</p> <p><b>projectThresholdExceedWarning</b> Project data size exceeds the threshold value set.</p> <p><b>projectQuotaFinished</b> Project quota is finished.</p> <p><b>projectCreatedWithNonOptimalBlockSize</b> Project is created with non-optimized block size.</p>
Volume	<p><b>volumeCreatedSuccessfully</b> Volume created successfully.</p> <p><b>volumeDeleteCompleted</b> Volume is deleted.</p>

Event Notification Type	Event ID Description
	<p><b>volumeOnline</b> Volume is back online.</p> <p><b>volumeOffline</b> Volume is offline.</p> <p><b>volumeDeleteFailed</b> Volume deletion failed.</p> <p><b>volumeExceedsThresholdWarning</b> Volume exceeds the threshold.</p> <p><b>volumeQuotaFinished</b> Volume quota finished.</p> <p><b>volumeModifyCompleted</b> Volume modification completed.</p> <p><b>volumeCreatedWithNonOptimalBlockSize</b> Volume is created with non-optimal block size.</p>
Share	<p><b>shareCreatedSuccessfully</b> Share created successfully.</p> <p><b>shareDeletionFailed</b> Share deletion failed.</p> <p><b>shareDeleted</b> Share is deleted.</p> <p><b>shareExceedThresholdWarning</b> Share exceeds the threshold limit.</p> <p><b>shareQuotaFinished</b> Share quota is finished.</p> <p><b>shareCreatedWithNonOptimalBlockSize</b> Share is created with non-optimal block size.</p>

Event Notification Type	Event ID Description
ACL	<b>aclMigrationStarted</b> ACL migration started.
	<b>aclMigrationCompleted</b>
Folder	<b>deleteFolderCompleted</b> Folder deleted.
	<b>deleteFolderFailed</b>
Snapshot	<b>snapshotCreatedSuccessfully</b> Snapshot created successfully.
	<b>snapshotCreationFailed</b> Snapshot creation failed.
	<b>snapshotDeletedSuccessfully</b> Snapshot deleted successfully.
	<b>snapshotDeleteFailed</b> Snapshot deletion failed.
	<b>snapshotRollbackFailed</b> Snapshot rollback failed.
	<b>snapshotRollbackCompleted</b> Snapshot rollback completed.
	<b>snapshotCloningFailed</b> Snapshot cloning failed.
	<b>snapshotCloneCompleted</b> Snapshot clone completed.
	<b>haResourceGroupTakeBackCompleted</b> HA resource group taken back.

Event Notification Type	Event ID Description
	<b>haResourceGroupTakeOverCompleted</b> HA resource group taken over.
Controller	<b>controllerUp</b> Controller is up.
	<b>controllerDown</b> Controller is down.
	<b>intelliFlashSoftwareUp</b> IntelliFlash software is up.
	<b>intelliFlashSoftwareDown</b> IntelliFlash software is down.
	<b>controllerTimeDrift</b> Controller time drift detected.
Miscellaneous	<b>adServerTimeDrift</b> AD server time drift detected.
	<b>maintenanceModeEnabled</b> IntelliFlash maintenance mode enabled.
	<b>maintenanceModeDisabled</b> IntelliFlash maintenance mode disabled.
	<b>alertsCleanupCompleted</b> Alerts clean-up completed.
	<b>testNotification</b> A Test notification
	<b>userLoginFailed</b> Login attempt to the IntelliFlash array failed.
	<b>ntpServerTimeDrift</b> Time Difference has been detected between NTP Server and controller.

Event Notification Type	Event ID Description
SMB	<b>smbSocketFailure</b> SMB socket failure detected.
	<b>netbiosSocketFailure</b>
Service	<b>snmpServiceStarted</b> SNMP Service started.
	<b>snmpServiceStartFailed</b> SNMP Service failed to start.
	<b>snmpServiceStopped</b> SNMP Service stopped.
	<b>snmpServiceStopFailed</b> SNMP Service failed to stop.
	<b>smisServiceStarted</b> SMIS Service started.
	<b>smisServiceStartFailed</b> SMIS Service failed to start.
	<b>smisServiceStopped</b> SMIS Service stopped.
	<b>smisServiceStopFailed</b> SMIS Service failed to stop.
IPMI	<b>ipmiTemperature</b> An IPMI event was raised related to array's temperature.
	<b>ipmiVoltage</b> An IPMI event was raised related to array's voltage.
	<b>ipmiCurrent</b> An IPMI event was raised related to array's current.

Event Notification Type	Event ID Description
	<p><b>ipmiFan</b> An IPMI event was raised related to array's fans.</p> <p><b>ipmiPowerSupply</b> An IPMI event was raised related to array's power supply.</p> <p><b>ipmiMemory</b> A memory error was detected.</p> <p><b>ipmiCriticalInterrupt</b> An IPMI critical interrupt was received.</p> <p><b>ipmiThreshold</b> An IPMI threshold event was generated.</p> <p><b>ipmiOther</b> An IPMI event was detected.</p>
NVDIMM	<p><b>nvdimmFailDeviceError</b> NVDIMM device is not detectable.</p> <p><b>nvdimmFailSoftError</b> NVDIMM device has encountered some errors.</p> <p><b>nvdimmFailInitializationError</b> Failed to initialize NVDIMM Device.</p> <p><b>nvdimmFailUnknownError</b> NVDIMM failure encountered. Please see the IntelliFlash UI event details.</p>
Network	<p><b>networkIpmpGroupUp</b> IPMP group is up.</p> <p><b>networkIpmpGroupDown</b> IPMP group is down.</p> <p><b>networkIpmpMemberInterfaceAdded</b> Network interface added to IPMP group.</p>

Event Notification Type	Event ID Description
	<b>networkIpmpMemberInterfaceRemoved</b> Network interface removed from IPMP group.
	<b>networkInterfaceUp</b> Network interface is up.
	<b>networkInterfaceDown</b> Network interface is down.
	<b>networkIpmpGroupCreated</b> Network interface group created.
	<b>networkIpmpGroupDeleted</b> Network interface group deleted.
	<b>networkIpmpGroupModified</b> Network interface group modified.
	<b>networkIpmpMemberLinkAggregateAdded</b> Network link aggregate added to IPMP group.
	<b>networkIpmpMemberLinkAggregateRemoved</b> Network link aggregate removed from IPMP group.
	<b>networkLinkAggregateCreated</b> Network Link aggregate is created.
	<b>networkLinkAggregateDeleted</b> Network Link aggregate is deleted.
	<b>networkLinkAggregateModified</b> Network Link aggregate is modified.
	<b>clusterInterconnectUp</b> Cluster interconnect is now up.
	<b>clusterInterconnectDown</b> Cluster interconnect is down.

Event Notification Type	Event ID Description
FC	<b>fcInitiatorCreateCompleted</b> FC Initiator create completed.
	<b>fcInitiatorCreateFailed</b> FC Initiator create failed.
	<b>fcTargetResetHbaPortCompleted</b> FC Target reset HBA port completed.
	<b>fcTargetResetHbaPortFailed</b> FC Target reset HBA port failed.
	<b>fcPortOnline</b> FC port is online.
	<b>fcPortOffline</b> FC port is offline.
Initiator Group	<b>initiatorGroupCreateCompleted</b> Initiator Group create completed.
	<b>initiatorGroupMemberAdded</b> Initiator Group member added.
	<b>initiatorGroupMemberRemoved</b> Initiator Group member removed.
	<b>initiatorGroupDeleteCompleted</b> Initiator Group delete completed.
iSCSI	<b>iscsiInitiatorCreateCompleted</b> iSCSI Initiator create completed.
	<b>iscsiInitiatorCreateFailed</b> iSCSI Initiator create failed.
	<b>iscsiInitiatorModifyCompleted</b> iSCSI Initiator modify completed.

Event Notification Type	Event ID Description
	<p><b>iscsiInitiatorDeleteCompleted</b> iSCSI Initiator delete completed.</p> <p><b>iscsiTargetCreateCompleted</b> iSCSI Target create completed.</p> <p><b>iscsiTargetModifyCompleted</b> iSCSI Target modify completed.</p> <p><b>iscsiTargetDeleteCompleted</b> iSCSI Target delete completed.</p> <p><b>iscsiTargetError</b> iSCSI Target error.</p> <p><b>iscsiTargetGroupError</b> iSCSI Target Group error.</p> <p><b>iscsiImproperTargetGroup</b> iSCSI improper target group.</p>
Target Group	<p><b>targetGroupCreateCompleted</b> Target Group create completed.</p> <p><b>targetGroupMemberAdded</b> Target Group member added.</p> <p><b>targetGroupMemberRemoved</b> Target Group member removed.</p> <p><b>targetGroupDeleteCompleted</b> Target Group delete completed.</p>
Maintenance	<p><b>maintenanceModeEnabled</b> Maintenance mode enabled.</p> <p><b>maintenanceModeDisabled</b> Maintenance mode disabled.</p>

Event Notification Type	Event ID Description
Diagnostic Data	<b>diagnosticDataUploaded</b> Diagnostic data uploaded.
	<b>diagnosticDataUploadingFailed</b> Diagnostic data upload failed.
Fault Management	<b>memoryFailure</b> Memory failure.
	<b>sensorFailureEvent</b> Sensory failure.
	<b>unknownSensorEvent</b> Unknown sensor event.
Upgrade	<b>upgradeStarted</b> Upgrade started.
	<b>upgradeCompleted</b> Upgrade completed.
	<b>upgradeFailed</b> Upgrade failed.
	<b>upgradeTimeout</b> Upgrade timed out.
	<b>upgradeCantProcessFilesManually</b> Upgrade can not process files manually.
	<b>upgradeDownloadStarted</b> Upgrade download started.
	<b>upgradeDownloadCompleted</b> Upgrade download completed.
	<b>upgradeDownloadFailed</b> Upgrade download failed.

Event Notification Type	Event ID Description
TDPS	<b>tdpsUpgradeCompleted</b> TDPS upgrade completed.
	<b>tdpsUpgradeFailed</b> TDPS upgrade failed.
	<b>tdpsUpgradeTimeout</b> TDPS upgrade timed out.
	<b>tdpsUpgradeDownloadStarted</b> TDPS upgrade download started.
	<b>tdpsUpgradeDownloadCompleted</b> TDPS upgrade download completed.
	<b>tdpsUpgradeDownloadFailed</b> TDPS upgrade download failed.
Webdocs	<b>webdocsUpgradeDownloadStarted</b> Webdocs upgrade download started.
	<b>webdocsUpgradeDownloadCompleted</b> Webdocs upgrade download completed.
	<b>webdocsUpgradeDownloadFailed</b> Webdocs upgrade download failed.
	<b>webdocsUpgradeCompleted</b> Webdocs upgrade completed.
	<b>webdocsUpgradeFailed</b> Webdocs upgrade failed.
vmware NFS	<b>vmwareNFSDatastoreCreated</b> vmware NFS datastore created.
	<b>vmwareNFSDatastoreDeleted</b> vmware NFS datastore deleted.

Event Notification Type	Event ID Description
Replication	<b>replicationTargetDeleted</b> Replication target deleted.
	<b>replicationComplete</b> Replication completed.
	<b>replicationAborted</b> Replication aborted.
	<b>replicationAbandoned</b> Replication abandoned.
	<b>replicationResumed</b> Replication resumed.
	<b>replicationStarted</b> Replication started.
	<b>replicationFailed</b> Replication failed.
	<b>replicationSourceRegistered</b> Replication source registered.
	<b>replicationPaused</b> Replication paused.



---

# Chapter 21

---

## Administration Settings

---

**Topics:**

- [\*Access and Permissions\*](#)
- [\*IntelliFlash Software Upgrade\*](#)
- [\*Customer Support\*](#)
- [\*Disk Encryption\*](#)
- [\*Downloading Plugins and SNMP MIB File\*](#)
- [\*Including a Custom Message in IntelliFlash Login Page\*](#)

## Access and Permissions

---

### Controlling Access through Accounts and Permissions

You can control access to the IntelliFlash Web UI by

- Creating accounts and granting or restricting permissions and roles.
- Providing access to only specific modules in the IntelliFlash Web UI.

You can specify the following general permissions for each role or account:

- Read
- Create
- Delete
- Update
- Operate

You can provide restricted access to the following modules:

- **Data:** Restricts access to all pools, projects and datasets.
- **Data Services:** Restricts access to all NAS, SAN, user, and report services.
- **Network:** Restricts access to all network settings.
- **HA:** Restricts access to all high availability functions.
- **Upgrade:** Prevents user from upgrading the system.
- **Replication:** Restricts access to setting up and executing replication sources and targets.
- **Hardware:** Prevents user from changing some hardware settings.
- **Administrator:** Restricts access to administrator services.
- **Role:** Restricts access to creating and changing roles.



**Note:** Some modules include contextual permissions.

You can also now configure LDAP accounts in the IntelliFlash Web UI, and enable users to log into the array using their LDAP credentials.

### Adding a Role

Roles allow you to grant the same permissions to a group of users without having to define the permissions for each user. Typical roles include User, Admin, Root (super-user), and Operator. As you assign roles to each user account, you must create roles before you create user accounts.

To create a role, complete the following steps:

1. Click **Settings > Administration > Management Access**.
2. Click the **Admin Roles** tab.
3. Click **Add**.

The **Create New Role** dialog box appears.

4. Type a name in the **Name** box.
5. (Optional) Provide a description in the **Description** box.
6. To provide access to the modules in the IntelliFlash Web UI, click **Add Authority**.
7. Select a module from the **Module** dropdown list.  
Select \* to assign the same permissions to all the modules.
8. Based on the module selected, the following options appear:
  - If the **data** module is selected, select the required pool, project, and share or LUN. Select \* to assign permissions to all pools, projects, and shares or LUNs in the module.
  - If the **data-service**, **network**, **ha**, **upgrade**, **replication**, or **hardware** module is selected, select the required service or select \* to assign permissions to all the services in the module.
  - If the **admin** module is selected, select the required account from the **Account** list or select \* to assign permissions to all the accounts in the admin module.
  - If the **role** module is selected, select the required role from the **Role** list or select \* to assign permissions to all the roles in the module.
9. Click the **Permissions** checkboxes as required.
10. Click **Add**.
11. If you want to assign access to additional modules, repeat steps 7 to 10.
12. Click **Save**.

## Adding a User Account

You can add a user account to control user access to the IntelliFlash Array.

To add a user account, complete the following steps:

1. Click **Settings > Administration > Management Access**.
2. In the **Local Admins** tab, click **Add**.

The **User Account** dialog box appears.

3. Type a name in the **Username** box.
4. Type a password in the **Password** box.
5. Type the password again in the **Confirm Password** box.
6. (Optional) Provide a description in the **Description** box.
7. Click **Enable** to activate the user account.
8. In the **Roles** tab, select the required roles for the user account.
9. To add additional permissions to specific modules in the IntelliFlash Web UI, click **Add Authority**.
10. Select a module from the **Module** dropdown list.  
Select \* to assign the same permissions to all the modules.
11. Based on the module selected, the following options appear:
  - If the **data** module is selected, select the required pool, project, and share or LUN. Select \* to assign permissions to all pools, projects, and shares or LUNs in the module.
  - If the **data-service, network, ha, upgrade, replication, or hardware** module is selected, select the required service or select \* to assign permissions to all the services in the module.
  - If the **admin** module is selected, select the required account from the **Account** list or select \* to assign permissions to all the accounts in the admin module.
  - If the **role** module is selected, select the required role from the **Role** list or select \* to assign permissions to all the roles in the module.
12. Click the **Permissions** checkboxes as required.
13. Click **Add**.
14. If you want to assign access to additional modules, repeat steps 9 to 13.
15. Click **Save**.

## Adding Authorities to a Role

You can add specific permissions to a role after creating a role.

To add permissions, complete the following steps:

1. Click **Settings > Administration > Management Access**.
2. Click the **Admin Roles** tab.
3. Select the role you want to edit and click **Edit**.



**Note:** You cannot add additional permissions to a predefined user account.

4. In the Authorities section, click **Add Authority**.
5. Select a module from the **Module** dropdown list.  
Select \* to assign the same permissions to all the modules.
6. Based on the module selected, the following options appear:
  - If the **data** module is selected, select the required pool, project, and share or LUN. Select \* to assign permissions to all pools, projects, and shares or LUNs in the module.
  - If the **data-service, network, ha, upgrade, replication, or hardware** module is selected, select the required service or select \* to assign permissions to all the services in the module.
  - If the **admin** module is selected, select the required account from the **Account** list or select \* to assign permissions to all the accounts in the admin module.
  - If the **role** module is selected, select the required role from the **Role** list or select \* to assign permissions to all the roles in the module.
7. Click the **Permissions** checkboxes as required.
8. Click **Add**.
9. If you want to assign access to additional modules, repeat steps 5 to 8.
10. Click **Save**.

## Adding Additional Roles or Authorities to an Account

You can add specific permissions to a user account after creating the account. To add permissions to an account, complete the following steps:

1. Click **Settings > Administration > Management Access**.
2. Click the **Local Admins** tab.
3. Select the user account and click **Edit**.



**Note:** You cannot add additional permissions to a predefined user account.

4. In the **Roles** tab, select or clear the required roles.
5. In the **Extra Permissions** tab, click **Add Authority**.
6. Select a module from the **Module** dropdown list.  
Select \* to assign the same permissions to all the modules.
7. Based on the module selected, the following options appear:

- If the **data** module is selected, select the required pool, project, and share or LUN. Select \* to assign permissions to all pools, projects, and shares or LUNs in the module.
  - If the **data-service**, **network**, **ha**, **upgrade**, **replication**, or **hardware** module is selected, select the required service or select \* to assign permissions to all the services in the module.
  - If the **admin** module is selected, select the required account from the **Account** list or select \* to assign permissions to all the accounts in the admin module.
  - If the **role** module is selected, select the required role from the **Role** list or select \* to assign permissions to all the roles in the module.
8. Click the **Permissions** checkboxes as required.
  9. Click **Add**.
  10. If you want to assign access to additional modules, repeat steps 5 to 9.
  11. Click **Save**.

## Configuring LDAP Accounts to log in to IntelliFlash

You can log in to IntelliFlash arrays using LDAP credentials. To support LDAP user authentication, you must first configure the LDAP settings in the IntelliFlash Web UI.

1. Add the host name of the directory server in the **Network** page.  
To add the host name, do the following:
  - a) Click **Settings > Network > General**.
  - b) In the **Management Networking Settings** section, enter the host name of the directory server in the **Domain** field.
  - c) In the **Add DNS Server** box, enter the IP address of the DNS server, and click **Add**.
  - d) Click **Save**.
2. Add the LDAP server and schema settings in the **Directory Services** page.  
To add the LDAP server and schema settings, do the following:
  - a) Click **Settings > Administration > Management Access > Directory Services**.
  - b) In the **External Directories** tab, click **New**.  
The **New Directory Service** window appears.
  - c) In the **Directory Configuration** section, enter the LDAP directory server settings.

**Table 9: Directory Configuration**

Option	Description
Enable Service	This is enabled by default. If you want to enter the LDAP configuration details now and enable the service later, drag the button to the left to disable it.
Domain	Enter the host name of the LDAP directory server.
Auto Discovery URLs	This is disabled by default. If you want IntelliFlash to automatically discover the LDAP URLs, drag the button to the right to enable it.
Use SSL	When <b>Auto Discovery URLs</b> is enabled, select the <b>Use SSL</b> option if the connection to the directory server is an SSL connection. You must configure an SSL certificate to use this setting.
LDAP URL	When <b>Auto Discovery URLs</b> is not enabled, enter the URL of the LDAP server in the format, <code>ldap://hostname:port</code> and click the <b>Add (+)</b> button. For example, <code>ldap://f3.example.com:389</code> If you have enabled SSL, the format is <code>ldaps://hostname:port</code> . For example, <code>ldaps://f3.example.com:686</code> .
User name	Enter the credentials for IntelliFlash to use when connecting to the directory server.
Password	

- d) In the **Directory Schema** section, enter the directory schema settings.

**Table 10: Directory Schema**

Option	Description
Directory Type	AD is the default <b>Directory Type</b> . Choose <b>Custom</b> for a custom LDAP directory type.
Base DN	The root distinguished name (DN) to use when running queries against the directory server. For example, <code>dc=f3,dc=example,dc=com</code> .
User Search Base	The value used in addition to the base DN to search and load users. For example, <code>ou=Users</code> .

Option	Description
User Search Filter	The filter to use when searching users. For example, (& (sAMAccountName={0}) (objectClass=user) ) or (uid={0}).
Group Search Base	The value used in addition to the base DN to search and load groups. For example, ou=Groups.
Group Search Filter	The filter to use when searching groups. For example, (& (cn={0}) (objectCategory=group) ) or (& (cn={0}) (  (objectclass=groupOfNames) (objectclass=groupOfUniqueNames) (objectclass=posixGroup) ) ).
Group Membership	The attribute or filter to use when loading the user's groups. For example, attribute could be memberOf; filter could be (& (objectCategory=group) (member={0})) or (  (member={0}) (uniqueMember={0}) (memberUid={1})).

- e) Click **Test** to test the directory service.
  - f) Click **Save** to save the settings.
3. Map user groups to the LDAP directory service.

To map the user groups to the LDAP directory service, do the following:

- a) Click **Settings > Administration > Management Access > Directory Services**.
- b) In the **Directory groups** tab, select the directory you configured from the **Directory Service** list, and then click **New**.
- c) In the **New Group Mapping** window, enter the group name. Alternatively, click the **Directory Lookup** button to search for the group name.

The **Directory Lookup** window consists of the **Group Lookup** and **User Lookup** tabs. Both the tabs display the existing groups and their roles. Either select the group from the list and click **Apply**, or search for the group in the tabs (in the **User Lookup** tab, you can search for the group by looking up the users that belong to the group). When the group name appears in the results, select the group from the list and click **Apply**.

- d) Select the role for the group.  
To add a new role, see [Adding a Role](#) topic.

- e) Click **Add**.

LDAP users can now authenticate to IntelliFlash arrays using LDAP credentials.



**Note:** If the same user is in multiple LDAP domains, the LDAP user must specify the domain name as well in the **Username** field when logging into the array.

## Deleting Authorities from a Role

When you delete authorities from a role, you delete the entire authority. You cannot delete specific permissions in the authority.

To delete authorities from a role, complete the following steps:

1. Click **Settings > Administration > Management Access**.
2. Click the **Admin Roles** tab.
3. Select the role and click **Edit**.

 **Note:** Predefined roles cannot be modified.

4. In the **Authorities** section, select the authority and click **Delete**.
5. Click **Save**.

## Deleting Authorities from a User Account

When you delete authorities or permissions from a user account, you delete the entire authority. You cannot delete specific permissions in the authority.

To delete authorities from a user account, complete the following steps:

1. Click **Settings > Administration > Management Access**.
2. In the **Local Admins** tab, select the user account and click **Edit**.
3. Click the **Extra Permissions** tab.
4. Select the authority and click **Delete**.
5. Click **Save**.

 **Note:** Predefined user accounts cannot be modified.

## Deleting a Role

You cannot delete a role that is associated to any existing user accounts.

To delete a role, complete the following steps:

1. Click **Settings > Administration > Management Access**.
2. Click the **Admin Roles** tab.
3. Select the role you want to delete and click **Delete**.

 **Note:**

- You cannot delete predefined roles.

- You cannot delete a role that is associated to user accounts. If the role is associated to an existing user account, an error message appears when you click **Delete**.

4. In the **Confirmation** dialog box, click **OK**.

## Deleting a User Account

You cannot delete predefined user accounts and user accounts that are currently logged in to the IntelliFlash Web UI.

To delete a user account, complete the following steps:

1. Click **Settings > Administration > Management Access**.
2. In the **Local Admins** tab, select the account you want to delete and click **Delete**.

 **Note:** You cannot delete predefined user accounts and user accounts that are currently logged in to the IntelliFlash Web UI.

3. In the **Confirmation** dialog box, click **OK**.

## Disabling a User Account

You can disable a user account without deleting it. This saves you from having to recreate the entire account and assigning roles and permissions all over again.

To disable an account, complete the following steps:

1. Click **Settings > Administration > Management Access**.
2. In the **Local Admins** tab, select the user account and click **Edit**.
3. Clear **Enable** checkbox to disable the account.
4. Click **Save**.

## IntelliFlash Software Upgrade

---

Upgrading your IntelliFlash systems with the latest IntelliFlash Operating Environment enables you to use new features and enhancements in the IntelliFlash Operating Environment. It also provides fixes to the bugs discovered in previous releases.

The IntelliFlash Web UI automatically checks the IntelliFlash upgrade server for the latest software as follows:

- Once every 24 hours.
- Whenever you access the **Software Upgrade** page.

If available, the latest software build is downloaded.

 **Note:** To automatically download the IntelliFlash Operating Environment, your array must have access to an Internet connection and the **Automatic Download** option must be enabled. If your array is not connected to the Internet, you can manually upload the latest IntelliFlash Operating Environment and upgrade.

The IntelliFlash Operating Environment upgrade process is generally a non-disruptive process if the upgrade process is followed as recommended by the IntelliFlash Technical Support engineer.

 **Caution:** The upgrade process reboots the IntelliFlash controller that is being upgraded. If the guidelines are not followed correctly, storage services can be disrupted.

The IntelliFlash Web UI provides a **Software Upgrade** wizard that allows you to upgrade both controllers of the array one after the other.

To simplify the upgrade process, you can upgrade both controllers of the array in a single step by using the **Upgrade both nodes** option in the **Software Upgrade** wizard.

## Software Upgrade Page

You can perform the following IntelliFlash Operating Environment related tasks from the **Software Upgrade** page:

- Upgrade IntelliFlash Operating Environment version
- Manually upload the latest IntelliFlash Operating Environment
- Check for availability of the latest IntelliFlash Operating Environment versions
- View currently running IntelliFlash Operating Environment version
- Enable or disable the automatic software download option
- View the upgrade history
- Know if your controllers are on separate versions of the IntelliFlash Operating Environment versions

### Related Topics

[Pre-Upgrade Health Check on the Array](#) on page 423

[Upgrading IntelliFlash Software](#)

[Upgrading IntelliFlash Software Manually](#)

[Enabling or Disabling Upgrade Option](#)

[Viewing Upgrade History](#)

## Pre-Upgrade Health Check on the Array

The **Software Upgrade** wizard performs a health check on the array. As part of the health check process, IntelliFlash performs checks for the following:

- The array is a single or dual controller array.
- The controller is booted in the HA mode.
- A minimum of one quorum disk is present and all quorum disks are online and contribute votes.
- The status of the 'Installmode' property of HA.

- The resource groups in the HA pair are online.
- The management interface group state.
- The metadata space usage in all hybrid pools is not more than 93%.
- The layer 1 SAS expander firmware of T3100/T3200 hardware models.
- The number of drives visible from both the nodes in a system is the same.
- The IPMP groups with a floating IP address are up on both controllers.
- The array uptime time is more than 200 days.
- The FC initiators are visible on both controllers and FC ports associated with listed NPIV ports are online or not.
- The "Armed" status and RAM partitions of all NVDIMMs on the array.
- The space available in the System pool. The System pool must have at least 30% free space for the software upgrade.
- The physical error count on all SAS links.
- The health of SATADOMs.

 **Note:** If any of the above checks fail, the upgrade will not proceed further. Contact the IntelliFlash Technical Support team for assistance. Also, the IntelliFlash Web UI generates a system health-check notification irrespective of whether the upgrade fails or proceeds successfully. For details, see the **Notifications** page in the IntelliFlash Web UI.

 **Note:** The array health check operation is performed on the array once every 24 hours and relevant notifications are displayed in the **Notifications** page.

## Upgrading IntelliFlash Software Using the Software Upgrade Wizard

### Prerequisites

- All of the disk drives and pools in the storage system must be healthy.
- The system time on both controllers of the array must be the same.

 **Note:**

- Contact the IntelliFlash Technical Support team to upgrade the IntelliFlash Operating Environment.
- When you start the web upgrade process, the **Maintenance** mode turns on automatically and IntelliFlash stops sending all email notifications to the administrator and IntelliFlash Technical Support team. However, you can view the notifications in the **Notifications** page. The **Maintenance** mode turns off automatically after the upgrade is complete and IntelliFlash sends an email notification about the upgrade status.

The **Software Upgrade** wizard guides you through the IntelliFlash Operating Environment upgrade process. The **Software Upgrade** page displays downloaded IntelliFlash Operating Environment versions if the **Automatic Download** option is enabled.

The **Software Upgrade** wizard performs pre-upgrade checks. If any of the pre-upgrade checks fail, the **Software Upgrade** wizard does not proceed further with the upgrade process.

 **Note:** The IntelliFlash Operating Environment upgrade is a nondisruptive process. As part of the nondisruptive upgrade process, the resource groups and all in-progress management tasks will move to the peer controller.

 **Important:** The replication target storage array should be running on the same or higher IntelliFlash Operating Environment version as the replication source. Therefore, if a replication relationship is configured on the array that you are upgrading, you might also need to upgrade your replication partner array to the same version.

When upgrading one controller, the IntelliFlash Operating Environment ensures that clients have access to the data by moving pools and resource groups to the other controller.

The **Software Upgrade** wizard upgrades both controllers of the array one after the other.

 **Note:** The **Software Upgrade** wizard first upgrades the controller that is not holding the array management IP address, then the other controller later.

 **Note:** Beginning with IntelliFlash 3.7.1.0, the **Software Upgrade** wizard first upgrades the controller with no pools and later the peer controller.

 **Caution:** The upgrade process reboots the IntelliFlash controller that is being upgraded. If the guidelines are not followed correctly, storage services can be disrupted.

### Option to skip the upgrade process after upgrading one controller

After upgrading one controller, the wizard provides the option to skip upgrading the other controller. This option is provided only for monitoring and diagnostic purposes.

 **Note:** The skip upgrading the other controller option is not available if you select the **Upgrade both nodes** option.

 **Caution:** IntelliFlash systems require both controllers to run the same version of the IntelliFlash Operating Environment. Different versions on the two controllers can cause unexpected behavior.

### Activity Monitor

The **Activity Monitor** available in the **Software Upgrade** wizard allows you to monitor the performance of the controller that is not being upgraded (the controller that is serving data to the clients). You can monitor average latency, total IOPS, and total throughput. The **Activity Monitor** also allows you to view read and write parameters for latency, IOPS, and throughput.

To upgrade the IntelliFlash Operating Environment, complete the following steps:

1. Click **Settings > Administration > Software Upgrade**.
2. If multiple versions are available for upgrade, select the required version.
3. Click **Upgrade Now**.
4. In the **Software Upgrade Confirmation** window, click **Yes**.



**Note:** If the pre-upgrade checks fail, contact the IntelliFlash Technical Support team.



**Note:** If the pre-upgrade health check finds any warning type issues, the wizard provides a warning message and requests a confirmation to continue.

5. Select **Upgrade both nodes**.

Selecting this option upgrades both controllers without your intervention.



**Note:** If you do not select the **Upgrade both nodes** option in this step, you must manually select the **Upgrade Other Node** option in the **Software Upgrade** wizard after the upgrade is complete on one controller.

6. Complete the upgrade by following the instructions available in the wizard.

## Related Topics

[IntelliFlash Software Upgrade](#)

[Pre-Upgrade Health Check on the Array](#)

[Upgrading IntelliFlash Software Manually](#)

## Upgrading IntelliFlash Software Manually

You might need to manually upgrade the IntelliFlash Operating Environment if your array is not connected to the Internet or your array is not able to download the software from the upgrade server due to any technical problems.

### Prerequisites

- All of the disk drives and pools in the storage system must be healthy.
- System time on both the IntelliFlash controllers must be the same.
- You must obtain a copy of the required manual upgrade file of type **.tar.gz** or **.bz2** from the IntelliFlash Technical Support team. The IntelliFlash Web UI allows you to upload only the **.tar.gz** or **.bz2** file type.



**Caution:** The upgrade process reboots the IntelliFlash controller that is being upgraded. If the guidelines are not followed correctly, storage services can be disrupted.

 **Note:** Contact the IntelliFlash Technical Support team to upgrade the IntelliFlash Operating Environment on your array.

 **Note:** Beginning with IntelliFlash 3.7.1.0, the **Software Upgrade** wizard first upgrades the controller with no pools and later the peer controller.

 **Note:** The IntelliFlash Operating Environment generates a system health check notification. For details, see the **Notifications** page in the IntelliFlash Web UI.

If your array does not have access to the Internet, you can upgrade your IntelliFlash Operating Environment manually.

To upgrade your IntelliFlash Array manually, complete the following steps:

1. Click **Settings > Administration > Software Upgrade**.
2. Disable the **Automatic Download** option if enabled.
3. In the **Software Upgrade** page, click **Manual Upgrade**.
4. In the **Manual Software Upload** window, click **Browse** and select the upgrade binary file from your local system (.tar.gz or tar.bz2).
5. Click **Upload**.
6. The IntelliFlash Web UI uploads the file to the array.
7. (Optional) If multiple versions are available for upgrade, select the required version.
8. In the **Software Upgrade** window, click **Upgrade Now**.
9. In the **Software Upgrade Confirmation** window, click **Yes**.

 **Note:** If the pre-upgrade checks fail, contact the IntelliFlash Technical Support team.

 **Note:** If the pre-upgrade health check finds any warning type issues, the wizard provides a warning message and requests a confirmation to continue.

10. Select **Upgrade both nodes**.

Selecting this option upgrades both controllers without your intervention.

 **Note:** If you do not select the **Upgrade both nodes** option in this step, you must manually select the **Upgrade Other Node** option in the **Software Upgrade** wizard after the upgrade is complete on one controller.

11. Complete the upgrade by following the instructions available in the wizard.

## Viewing Upgrade History

You can view the upgrade history from the **Software Upgrade** page. The upgrade history provides a list of the IntelliFlash versions from which your array was upgraded and when it was

upgraded. You might need this information when you are in communication with the IntelliFlash Technical Support team.

To view the upgrade history, complete the following steps:

1. Click **Settings > Administration > Software Upgrade**.
2. The **Upgrade History** section in the **Software Upgrade** page displays the details.

## Customer Support

---

You should provide the required details in the **Customer Info** and **Support** tabs for technical support.

In the **Customer Info** tab, provide your address, contact details, array location, FRU shipment address.

In the **Support** tab, you can enable or disable IntelliCare, CallHome, and manage IntelliShell.

You must provide the required information in the **Customer Support** tab to use the CallHome and the IntelliCare features.

## Adding or Modifying your Contact Details, Array Location, and FRU Shipment Address

Add the IntelliFlash Array administrator contact details in the **Customer Info** page. IntelliFlash appends the contact details in all support logs sent to the IntelliFlash Technical Support team. The contact details enable us to reach you faster and provide technical assistance. You can also add the address for sending field replacement units (FRUs) in the **Customer Info** page.

To add or modify IntelliFlash administrator or user contact details, complete the following steps:

1. Click **Settings > Administration > Customer Support > Customer Info**.
2. In the **Customer Info** page, type in appropriate details for the following fields:
  - Account Name
  - Contact Name
  - Contact Email (required)
  - Contact Phone
3. Provide **Asset Location**.
  - Street
  - City
  - State
  - Country
  - ZIP code
4. (Optional) Provide the **FRU Shipment Location** by turning off the toggle button against **Same as asset location** option, if the address is different from the asset location.

- Street
- City
- State
- Country
- ZIP code

5. Click **Save**.

## Enabling or Disabling CallHome

Enabling the CallHome option allows the IntelliFlash OS to send email notifications that contain critical system alerts to the IntelliFlash Technical Support team. These email notifications enable the IntelliFlash Technical Support team to provide proactive support for the issue.

By default, after you enable CallHome all notifications of severity level **High** or **Critical** are sent to the IntelliFlash Technical Support team. You can control which email notifications are sent by customizing the notification settings. For more information, see [Notifications](#).



**Important:** The CallHome requires SMTP settings to be enabled and configured. For more information on configuring SMTP, see [Configuring SMTP](#).

To enable or disable the CallHome feature, complete the following steps:

1. Click **Settings > Administration > Customer Support > Support**.
2. In the **Support** page, click the **CallHome** toggle button to enable it.

## Testing CallHome

To test the CallHome feature, the option should be enabled. To test the CallHome feature, complete the following steps:

1. Click **Settings > Administration > Customer Support > Support**.
2. In the **Support** page, click the **Test CallHome** toggle button to enable it.

An information screen displays the test result.

## IntelliCare Overview

IntelliCare enables you to quickly and easily monitor the health, performance, and space usage of all your IntelliFlash systems from a single web portal without logging into the individual IntelliFlash Web UI. It also allows you to predict future storage requirements and detect problems before they develop into component and system failures.

The *IntelliCare agent* and *IntelliCare server* are the two components of the IntelliCare feature. You can enable or disable the IntelliCare option from the **Support** page.

The IntelliCare agent runs on your IntelliFlash Array and performs the following functions:

- Runs various commands once in a day and collects data points (logs)
- Checks for errors in the logs relating to IntelliFlash Array hardware, software, pools, disks, network, and overall system
- Uploads the collected logs to the IntelliCare server

 **Note:** The IntelliFlash Array must have access to the Internet to upload the collected logs.

For more information, see [Enabling or Disabling IntelliCare](#).

## Enabling or Disabling IntelliCare

Enabling the IntelliCare feature allows you to collect system information automatically and upload it to the IntelliCare server.

To enable or disable IntelliCare, complete the following steps:

1. Click **Settings > Administration > Customer Support > Support**.
2. In the **Support** page, click the **IntelliCare** toggle button to enable or disable the IntelliCare feature.

 **Note:** You can click the **Test IntelliCare** button to verify if IntelliFlash is connected to IntelliCare.

### Related Topics

[Enabling HTTP Proxy Settings](#)

## Testing IntelliCare

1. Click **Settings > Administration > Customer Support > Support**.
2. In the **Support** page, click the **Test IntelliCare** button.  
The Information screen displays the IntelliCare connection status.

## IntelliShell Overview

IntelliShell allows the IntelliFlash Technical Support team to access your IntelliFlash system. You can enable or disable the IntelliShell feature, configure IntelliShell settings and set a fixed duration for the session to be accessed by IntelliFlash Technical Support. You can also enable or disable and configure **IntelliShell Server Notifications** to be notified of remote logins. To allow the IntelliFlash Technical Support engineer to access your IntelliFlash system, share the Remote Access URL with the IntelliFlash Technical Support engineer.

 **Note:** Do not share the **Authentication Token**. You can use it to monitor the IntelliShell session.

For more information, see [Enabling or Disabling IntelliShell](#).

## Managing IntelliShell

## Enabling or Disabling IntelliShell

Enabling the IntelliShell option allows IntelliFlash Technical Support administrative access to the array as long as the session is open.



**Note:** Do not share the **Authentication Token**. You can use it to monitor the IntelliShell session.

To enable or disable IntelliShell, complete the following steps:

1. Click **Settings > Administration > Customer Support > Support**.
2. In the **Support** page, click the **IntelliShell** toggle button to enable or disable the IntelliShell feature.

### Related Topics

[Enabling SOCKS Proxy Settings](#)

## Configuring IntelliShell Settings

You can set the duration for IntelliShell session expiry, and enable, disable, and configure **IntelliShell Server Notifications**.

To configure IntelliShell settings and **IntelliShell Server Notifications**, complete the following steps:

1. Click **Settings > Administration > Customer Support > Support**.
2. In the **Customer Support** page, after enabling **IntelliShell**, click **Edit**.
3. Select **Session Expires In** and set the duration or select **Never**.
4. Click the **Send Notifications** toggle button to enable or disable **IntelliShell Server Notifications**.
5. Enter the email ID in the **Send Notifications To** field.

### Related Topics

[Enabling SOCKS Proxy Settings](#)

## Refreshing IntelliShell Token(s)

The Authentication Token is used to monitor the IntelliShell session. Refreshing the token(s) will prevent new IntelliShell logins from using previously generated tokens.



**Note:** Do not share the **Authentication Token**. You can use it to monitor the IntelliShell session.

To refresh the IntelliShell token(s), complete the following steps.

1. Click **Settings > Administration > Customer Support > Support**.
2. In the **Support** page, after enabling **IntelliShell**, click **Refresh Token(s)**.

## Disk Encryption

The Disk Encryption feature in IntelliFlash systems encrypts data after writing the data to disks.

The Disk Encryption feature secures your data against unauthorized access. Data can be read from encrypted drives only by using the secure key available on the IntelliFlash system.



### Warning:

Export the authorization key and save it securely. Your data is at risk if you don't have a back up of the authorization key.



**Note:** By default, disk encryption is enabled on all SEDs when you create a pool, expand a pool, and replace a failed disk.

Disk Encryption works seamlessly with other features, such as deduplication and compression.



**Note:** The commands in the **Encryption** tab of the IntelliFlash Web UI are enabled only if the array or an attached expansion shelf has at least one encrypted drive.

## Enabling Encryption of NVMe Drives

IntelliFlash 3.11.3.0 supports encryption for NVMe pools.

To enable encryption of NVMe drives, the firmware upgrade of NVMe drives must be performed.

The firmware upgrade consists of the following two stages:

- **Loading of firmware on NVMe drives:** When you freshly install or upgrade IntelliFlash 3.11.3.0, the firmware is loaded onto all the NVMe drives.
- **Activating the NVMe drives to boot into the new firmware:** Either power cycle the chassis (both PSUs unplugged) or run the NVMe Drive Firmware Upgrade wizard.

### Activating the NVMe Drives Using IntelliFlash Web UI

When you log in, the IntelliFlash Web UI displays a **NVMe Drives Firmware Upgrade** warning dialog box if it detects that the firmware has not been activated to the latest version. This warning dialog box continues to appear until you finish activating the new NVMe drive firmware.

1. In the **NVMe Disks Firmware Upgrade** screen, click **I acknowledge and accept the upgrade**.

The **Start** button is enabled.

If you clicked **Cancel** to upgrade the firmware later, the **NVMe Disks Firmware Upgrade** wizard can be launched from the **Support** tab of the **System Information** window. Click

on the system name at the top-right corner of the IntelliFlash web UI for the **System Information** window to appear.

2. Click **Start**.

The firmware upgrade screen displays the "Upgrade in progress" message.

3. During this process, on the live IntelliFlash system, each drive is reset in turn. If it is part of a pool, the drive is added back into the pool and the pool resilvered before the next drive is reset.

Each drive reset generates a UI notification that can safely be ignored.

4. If there are errors when activating all the NVMe drives in the pools, re-run the NVMe Disks Firmware Upgrade Wizard (this could have been a transient issue). If the issue persists, call IntelliFlash Technical Support team.
5. After the drives are successfully upgraded, encryption is enabled on the NVMe drives in all pools.

### Conditions Affecting Firmware Upgrade of NVMe Drives

The firmware upgrade of NVMe drives will not be allowed to start if any with any of the following conditions:

- When one controller is down during the firmware upgrade.
- When either controller has not successfully upgraded to the latest IntelliFlash version (for example, IntelliFlash 3.11.3.0 or higher).
- When system health check fails (for example, due to wrong or old appliance firmware or because the NVDIMM is not armed).
- When pool is degraded (failed disks) or pool is resilvering. Pool must be online and stable for successful firmware upgrade.

### Encryption Passcode for Securing Data on Pools

The **Encryption Passcode** option in the Encryption feature secures data in pools from unauthorized access when both controllers in the array are rebooted at the same time or a cold reboot is performed for any reason, such as maintenance operations or relocation of your business or datacenter. The IntelliFlash Web UI allows you to enter a passcode and generate an encryption key based on the passcode. You can enable or disable the **Encryption Passcode** option in the IntelliFlash Web UI.

Consider the following guidelines when using the **Encryption Passcode** option:

- By default, when you create a pool using SEDs the disks are locked/authorized using the array-generated master key. After creating the pool, you can add a passcode to generate a new master key.
- You must have the passcode to unlock your array after a power cycle or cold reboot of both controllers in the array.
- You must export the encryption master key every time you perform any operation related to the **Encryption Passcode** option.
- You must always use the latest encryption master key when importing an encryption key.

- You must provide the encryption passcode when exporting or importing your encryption master key if the **Encryption Passcode** option is enabled on your array.
- Contact the IntelliFlash Technical Support team if you forgot the encryption passcode for your array.
- After you download the encryption master key, it is recommended to rename the master key appropriately for easy identification.

### Enabling and Setting up Encryption Passcode

You can enable the **Encryption Passcode** option whenever required. Provide a passcode for your array to secure your array from unauthorized access. When you enable the **Encryption Passcode** option, the IntelliFlash Web UI prompts you to set a passcode.

#### Note:

- You must remember the passcode for future usage. You require the passcode to export and import the master encryption key.
- If you have set an **Encryption Passcode**, you require it when you cold reboot the system (rebooting both controllers in the array), and when you log in to IntelliFlash Web UI after the reboot.

To enable the **Encryption Passcode** option, complete the following steps:

1. Click **Settings > Administration > Encryption**.
2. In the **Encryption** page, enable the **Encryption Passcode** option.
3. In the **Enable Encryption Passcode** window, type a new encryption passcode and confirm the passcode.  
A passcode can have a minimum of eight characters and a maximum of 15 characters.
4. Click **Enable**.

### Modifying the Encryption Passcode

To modify the encryption passcode for your array, complete the following steps:

1. Click **Settings > Administration > Encryption**.
2. In the **Encryption** page, click **Change Passcode**.
3. In the **Change Encryption Passcode** window, complete the following steps:
  - a) Type the current passcode.
  - b) Type a new passcode.
  - c) Confirm the new passcode.
  - d) Click **Change**.

## Disabling the Encryption Passcode

You can disable the **Encryption Passcode** option whenever required.



**Note:** You must export the encryption master key after disabling the **Encryption Passcode**.

To disable the **Encryption Passcode** option, complete the following steps:

1. Click **Settings > Administration > Encryption**.
2. In the **Encryption** page, disable the **Encryption Passcode** option.
3. Type the encryption passcode for the system.
4. Click **Confirm**.

## Exporting an Encryption Key

The **Export** option enables you to take a backup of the authorization keys.

When you export the encryption key using the IntelliFlash Web UI, the key file name contains the IntelliFlash system name, the date, and the time the authorization keys were exported.



**Note:** You can export your encryption key only after creating the first pool.

To export an encryption key to your local management system, complete the following steps:

1. Click **Settings > Administration > Encryption**.
2. In the **Encryption** page, click **Export**.  
The encryption key is saved to the Download directory in the local management system.
3. An **Information** screen displays the md5 checksum of the downloaded file. Click **OK**.

## Related Topics

[Importing an Encryption Key](#)

## Importing an Encryption key

Import the key file only in a disaster recovery scenario where both canisters copies of the authorisation key have been lost. In case of a disaster recovery scenario, import the most recent authorisation key that was previously saved for this system.

When importing an authorisation key, IntelliFlash checks the key. If the key fails to unlock any drives that have SED authorisation enabled, it does not allow the key to be imported. If you import an authorisation key on a running system, it will only allow you to import the current valid key.

To import an encryption key into an IntelliFlash system, complete the following steps:

1. Click **Settings > Administration > Encryption**.
2. In the **Encryption** page, click **Browse** and select the key from your local system.
3. If *Two-Factor Authentication (2FA)* is enabled for the user, enter the 2FA application code retrieved from your mobile device to import an encryption key.
4. Click **Import**.
5. In the **Confirmation** screen, verify details such as the md5 checksum, IntelliFlash system name, IP address of the system, the date and the time the authorization keys were exported. The details help you to identify whether the encryption key belongs to the current system and that the key is the most recent.
6. Click **OK** in the **Confirmation** screen after verifying the details.
7. In the **Confirm Passcode** screen, type your **Encryption Passcode** and click **Confirm**. This step is applicable only if the **Encryption Passcode** option is enabled on your system.
8. If the correct key has been imported, an **Information** screen appears with the message that the key has been successfully imported. Click **OK**.
9. If you try to import an incorrect key file, an **Error** screen appears.

 **Note:** Identify the correct key and upload it.

## Erasing Data Securely from Encrypted Drives

You can securely erase the data from an SED using the **Secure Erase** option. You can run the secure erase operation if you want to reuse a drive, or if a drive has failed and you want to send the drive for replacement. Data cannot be read from a securely erased drive. The IntelliFlash Web UI allows you to erase data from a single drive or multiple drives.

 **Note:** You cannot perform the secure erase operation if the SED is part of a pool. To securely erase data from an SED that is part of a pool, you must first replace the SED with a new SED.

 **Caution:** The secure erase operation erases the data in the drives. You cannot recover the data from the drives after performing the operation.

To securely erase data from an SED, complete the following steps:

1. Click **Settings > Administration > Encryption**.
2. In the **Encryption** page, click **Secure Erase**.

In the **Encryption** page, you can choose to securely erase data for a single SED, or the SEDs displayed on the page, or all SEDs.

- To select a single SED, click the check box next to the alias ID.
  - To select SEDs displayed in the page, single click the check box next to the **Alias** field.
  - To select all the SEDs, double click the check box next to the **Alias** field.
3. In the **Confirmation** screen, click **Yes**.  
The **Confirmation** screen displays the selected number of drives.
4. In the **Confirmation** screen, click **OK**.

To identify the secure erased drive on the array, you can copy the drive alias number from the **Encryption** page and identify it from the **Disk Array** page (**Settings > Disk Array**).

## Downloading Plugins and SNMP MIB File

---

From the **Plugins** page, you can download the SNMP MIB file and the following plugins:

- IntelliFlash Object Data Manager for AIX
- NAS-VAAI
- PowerShell Toolkit
- SNMP MIB
- SRA
- IDPS (64-bit)
- IntelliFlash Manager

The **Plugins** page displays version number of each plugin.

To download plugins or SNMP MIB, complete the following steps:

1. Click **Settings > Administration > Plugins**.
2. Click **Download** button corresponding to the plugin or SNMP MIB file name.
3. Click **OK** to save the plugin or MIB file.

## Including a Custom Message in IntelliFlash Login Page

---

You can now customize the IntelliFlash login page to include a message. The message can be a customer compliance notice or any other custom message. To add the custom message, do the following:

1. Click **Settings > Administration > Compliance and Security**.
2. In the **Compliance and Security** page, click the **Enable** toggle button to add the custom message.
3. In the **Notice Content** box, add the content you want the users to see.
4. Click **Save**.

The custom message you add in the **Compliance and Security** page appears in the IntelliFlash login page.

---

# Chapter 22

---

## Two-Factor Authentication (2FA)

---

**Topics:**

- *Two-Factor Authentication (2FA) Overview*
- *Two-Factor Authentication (2FA) Requirements*
- *Accessing 2FA Feature in IntelliFlash Web UI*
- *Enabling 2FA in IntelliFlash Web UI*
- *Disabling 2FA in IntelliFlash Web UI*
- *2FA Access Privileges*

## Two-Factor Authentication (2FA) Overview

---

The Two-Factor Authentication (2FA) feature provides an additional layer of security protecting from ransomware.

The 2FA requires a two-step verification process to access the IntelliFlash Web UI.

- The first step is to enter your **Username** and **Password**.
- The second step is to enter **2FA application code**.

The 2FA application code is defined as the six-digit Time-based One Time Password (TOTP) passcode returned by your mobile device authenticator application such as Google Authenticator or Microsoft Authenticator every 30 seconds. The users will authenticate with this six-digit TOTP passcode as a second credential.

From the IntelliFlash Web UI, the 2FA can be enabled as a second step of authentication process.

After you enable 2FA, you need to enter 2FA application code to perform the below tasks:

- Deletion of Pools
- Deletion of Projects
- Deletion of LUNs
- Deletion of Shares
- Deletion of Snapshots
- Manage Schedules of Snapshots, Shares, and LUNs

## Two-Factor Authentication (2FA) Requirements

---

Below are the basic requirements for Two-Factor Authentication (2FA):

- The 2FA feature in IntelliFlash is supported only with IntelliFlash 3.11.5.0 version.
- The users need to install any one authenticator application such as Google Authenticator or Microsoft Authenticator or any similar application on their mobile/desktop device. This authenticator application can be downloaded from the Apple App Store or the Google Play Store.

## Accessing 2FA Feature in IntelliFlash Web UI

---

To access 2FA option, do the following:

- Go to **Settings > Administration > Management Access**.
- Click the **Local Admins** tab.
- Select the desired user account and click **Edit**. You can now see the 2FA toggle button in the figure on next page.

User Account: testuser

Username *	<input type="text" value="testuser"/>	Enable <input checked="" type="checkbox"/>														
Password *	<input type="password" value="*****"/>	Confirm Password * <input type="password" value="*****"/>														
Description	<input type="text"/>															
2FA <input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>																
<table border="1"> <thead> <tr> <th>Roles</th> <th>Extra Permissions</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/> Role</td> <td><b>Description</b></td> </tr> <tr> <td><input type="checkbox"/> sra</td> <td>Storage Replication Adapter Role</td> </tr> <tr> <td><input checked="" type="checkbox"/> root</td> <td>Array Admin Role</td> </tr> <tr> <td><input type="checkbox"/> read_only</td> <td>Read-Only Admin Role</td> </tr> <tr> <td><input type="checkbox"/> storage_admin</td> <td>Storage Admin Role</td> </tr> <tr> <td><input type="checkbox"/> veeam</td> <td>Veeam Role</td> </tr> </tbody> </table>			Roles	Extra Permissions	<input type="checkbox"/> Role	<b>Description</b>	<input type="checkbox"/> sra	Storage Replication Adapter Role	<input checked="" type="checkbox"/> root	Array Admin Role	<input type="checkbox"/> read_only	Read-Only Admin Role	<input type="checkbox"/> storage_admin	Storage Admin Role	<input type="checkbox"/> veeam	Veeam Role
Roles	Extra Permissions															
<input type="checkbox"/> Role	<b>Description</b>															
<input type="checkbox"/> sra	Storage Replication Adapter Role															
<input checked="" type="checkbox"/> root	Array Admin Role															
<input type="checkbox"/> read_only	Read-Only Admin Role															
<input type="checkbox"/> storage_admin	Storage Admin Role															
<input type="checkbox"/> veeam	Veeam Role															
<input type="button" value="Cancel"/> <input type="button" value="Save"/>																

## Enabling 2FA in IntelliFlash Web UI

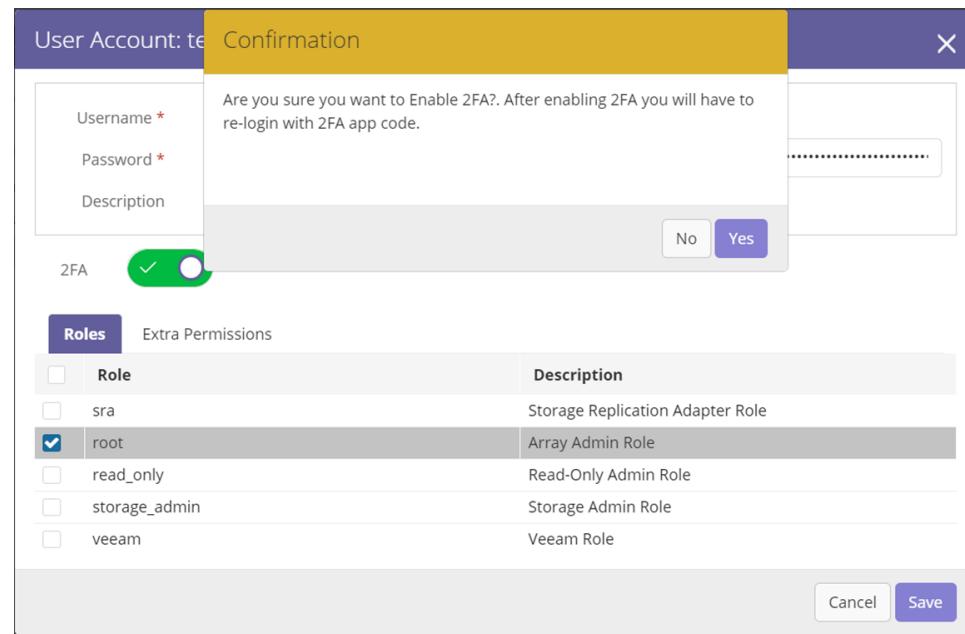
To enable 2FA, complete the following steps:

**Note:** When you create a user, you cannot grant 2FA access and the toggle button does not work. Only the user can enable the 2FA option.

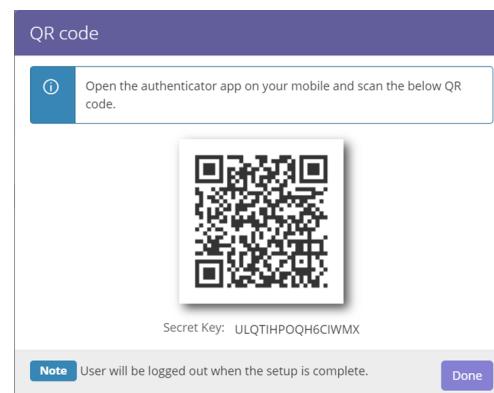
1. Go to **Settings > Administration > Management Access**.
2. Click the **Local Admins** tab. You can see the selected user's 2FA status as disabled.

The screenshot shows the IntelliFlash Web UI interface. The top navigation bar includes links for Dashboard, Analytics, Provision, Services, and Settings. The Settings dropdown is open, showing options like Administration, Management Access (which is selected), System OS, Software Upgrade, Customer Support, Encryption, Plugins, and Compliance and Security. On the left, a sidebar under 'Administration' lists Management Access, System OS, Software Upgrade, Customer Support, Encryption, Plugins, and Compliance and Security. The main content area has tabs for Local Admins, Directory Services, and Admin Roles, with Local Admins selected. Below these tabs are buttons for Add, Edit, and Delete. A table lists three users: admin (Role: root, 2FA: Enabled), satishg (Role: root, 2FA: Enabled), and testuser (Role: root, 2FA: Disabled). The 'testuser' row is highlighted with a red box.

3. Select the user account and click **Edit**.
4. Enable the 2FA option by clicking on the toggle button. The **Confirmation** message is displayed.



5. Click **Yes**.
  6. Open the authenticator application on your mobile device.
  7. Scan the QR code generated on your system to register.  
(Or)
- Enter the **Secret Key** (alphanumeric code present below QR code) to register, if you face any issue with QR code scan.

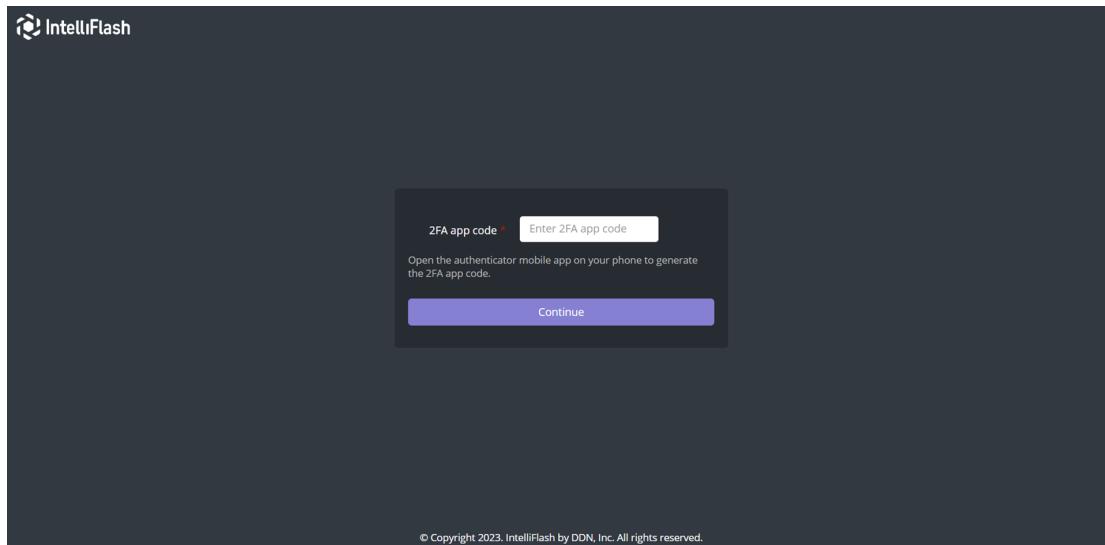


8. Click **Done**.

You will be logged out when the setup is complete.

9. Login again to the IntelliFlash Web UI with your credentials.

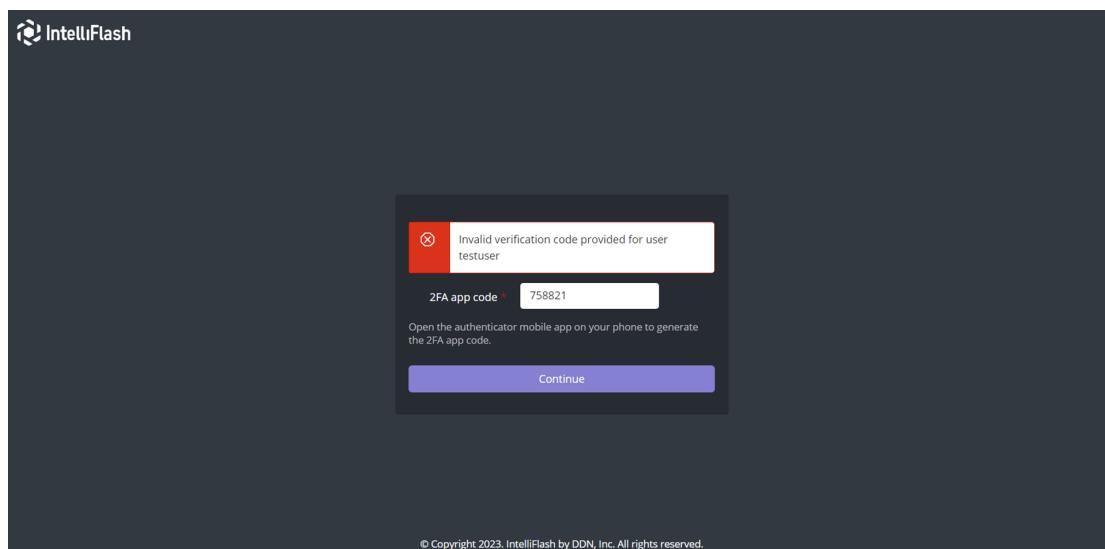
After successful login verification, the 2FA application code page is displayed.



10. Open the authenticator application on your mobile device to get the 2FA application code.

11. Enter the 2FA application code and click **Continue**.

If you enter a wrong 2FA application code, the below error message is displayed.



12. Go to **Settings > Administration > Management Access**.

13. Click the **Local Admins** tab. You can now see the selected user's 2FA status as enabled.

Name	Role	2FA
admin	root	Enabled
satishg	root	Enabled
testuser	root	Enabled

The 2FA is enabled for the desired user account.

## Disabling 2FA in IntelliFlash Web UI

---

To disable 2FA, complete the following steps:

1. Go to **Settings > Administration > Management Access**.
2. Click the **Local Admins** tab. You can see the selected user's 2FA status as enabled.

Name	Role	2FA
admin	root	Enabled
satishg	root	Enabled
testuser	root	Enabled

3. Select the user account and click **Edit**.

4. Disable the 2FA option by clicking on the toggle button. The **2FA Confirmation** message is displayed.

2FA Confirmation

2FA app code is required to confirm the action. Open the mobile authenticator app to get the code and then enter the code below to continue.

2FA app code: \*

Enter 2FA app code

**Note** User will be logged out when the setup is complete.

**Continue**

Roles		Extra Permissions
<input type="checkbox"/>	Role	Description
<input type="checkbox"/>	sra	Storage Replication Adapter Role
<input checked="" type="checkbox"/>	root	Array Admin Role
<input type="checkbox"/>	read_only	Read-Only Admin Role
<input type="checkbox"/>	storage_admin	Storage Admin Role
<input type="checkbox"/>	veeam	Veeam Role

**Cancel** **Save**

5. Enter the 2FA application code. Click **Continue**.  
You will be logged out when the setup is complete.
6. Login again to the IntelliFlash Web UI with your user-password credentials.
7. Go to **Settings > Administration > Management Access**.
8. Click the **Local Admins** tab. You can see the selected user's 2FA status as disabled.

IntelliFlash

Dashboard Analytics Provision Services Settings

Administration		Local Admins	Directory Services	Admin Roles
Management Access		Add Edit Delete		
System OS				
Software Upgrade				
Customer Support				
Encryption				
Plugins				
Compliance and Security				
Name	Role	2FA		
admin	root	Enabled		
satishg	root	Enabled		
testuser	root	Disabled		

The 2FA is disabled for the desired user account.

## 2FA Access Privileges

---

The below table contains the details of 2FA access privileges for different user types.



**Note:** It is mandatory to enter 2FA application code to enable/disable the 2FA for the user.

**Table 11: 2FA Privileges**

User Type	2FA State
Admin	<ul style="list-style-type: none"> <li>Can disable 2FA for all user types, if 2FA is already enabled for the admin user.</li> <li>Can enable 2FA for self account only.</li> <li>Can disable 2FA for self account.</li> </ul>
Non Admin	<ul style="list-style-type: none"> <li>Can enable 2FA for self account only.</li> <li>Can disable 2FA for self account only.</li> </ul>
Root	Any logged-in user having root permission can disable 2FA for other accounts, provided 2FA is already enabled for the root user.
All users	The user will be logged out after enabling or disabling 2FA for self account.

---

# Chapter 23

---

## MPIO Settings

---

**Topics:**

- *Configuring Windows MPIO Settings to IntelliFlash Array*

MultiPath Input Output (MPIO) is a framework that allows administrators to configure load balancing and failover processes for Fibre Channel and iSCSI connected storage devices. Load Balancing can be configured to use up to 32 independent paths from connected storage devices.

This chapter contains details on how to configure Windows MPIO settings to IntelliFlash Array.

## Configuring Windows MPIO Settings to IntelliFlash Array

Even though an IntelliFlash Array provides redundancy and failover through HA Clustering and RAID, Windows hosts still need a method for spreading the load and managing individual path failure. This is where MPIO provides an advantage. Without MPIO, there is no method for a Windows host to identify multiple paths as representing the same LUN.

The MPIO framework uses Device Specific Modules (DSM) to allow path configuration. Currently, there are two options available:

- Microsoft DSM (MSDSM) for Windows Server 2016, 2019, and 2022
- Vendor specific DSM for Windows

 **Note:** IntelliFlash is SPC-3 compliant, and uses the Microsoft DSM for Windows MPIO.

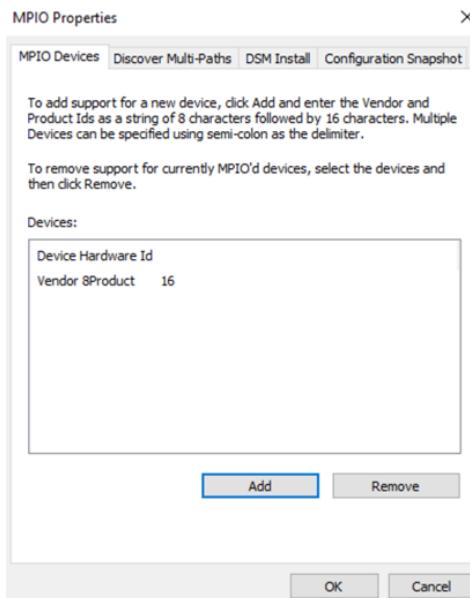
 **Note:** For a full list of MPIO Timers available in Windows, and their functions; see the section [Available MPIO Timers to be Configured](#).

 **Important:** The MPIO settings in this chapter are only recommendations from Tintri. For more information, the customers are advised to contact the vendor directly.

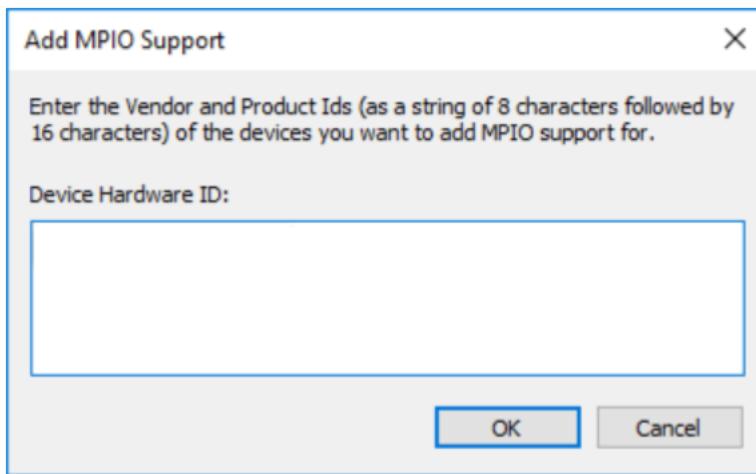
### Adding MPIO on Windows Server 2016, 2019, and 2022

To add MPIO on a server running Windows Server 2016, 2019, and 2022:

1. Install MPIO on the system.
2. After you finish MPIO installation, go to **Control Panel** and double-click **MPIO** to open **MPIO Properties** dialog box.



3. Click **Add** to show the **Add MPIO Support** dialog box.

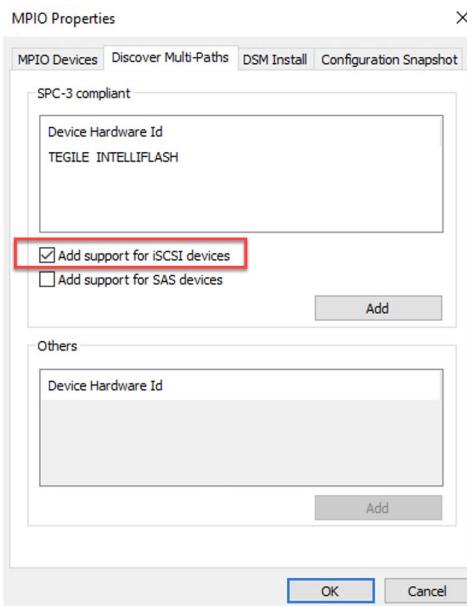


4. Add IntelliFlash specific Device Hardware ID in **Add MPIO Support** dialog box.

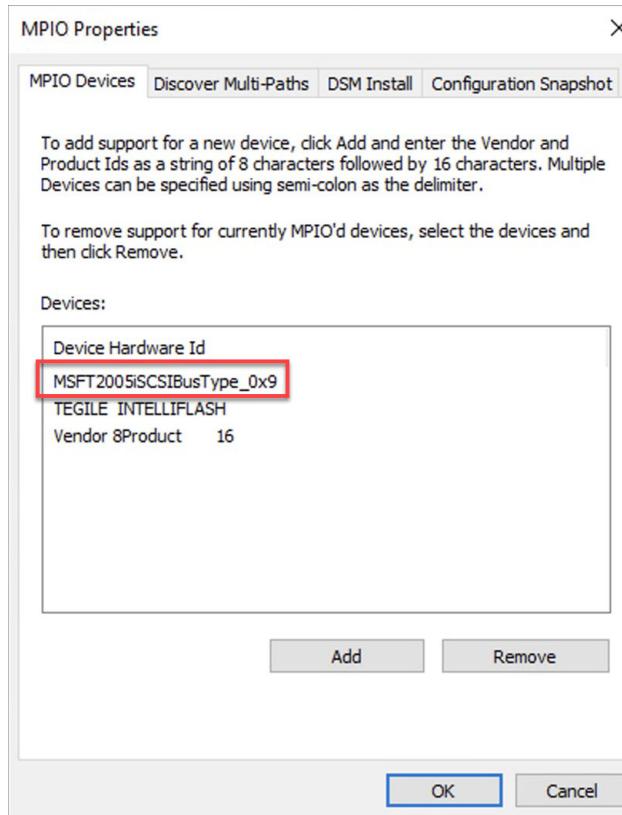


**Note:** Make sure to check the instructions in the dialog box for Device Hardware ID creation. You need to give two extra spaces after **TEGILE** and four extra spaces after **INTELLIFLASH**.

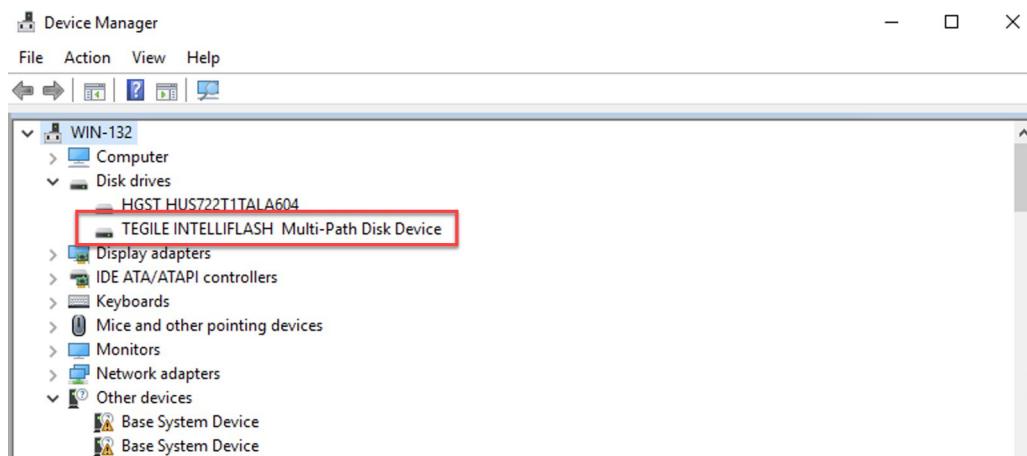
5. Go to **Discover Multi-Paths** tab in the **MPIO Properties** dialog box. Select **Add support for iSCSI devices**. Click **OK**.



6. Go to **MPIO Devices** tab, you will now see **MSFT2005iSCSIBusType\_0x9** device is added. Click **OK**.



7. Now the device manager should list the LUN as **TEGILE INTELLIFLASH Multi-Path Disk Device**.



## Windows MSDSM Parameters

The following Windows MSDSM parameters are required settings for HA failover to work properly:

- PathVerificationState: **Enabled**
- PathVerificationPeriod: **5**
- PDORemovePeriod: **180**
- RetryCount: **100**
- RetryInterval: **1**
- UseCustomPathRecoveryTime: **Enabled**
- CustomPathRecoveryTime: **40**
- DiskTimeoutValue: **180**

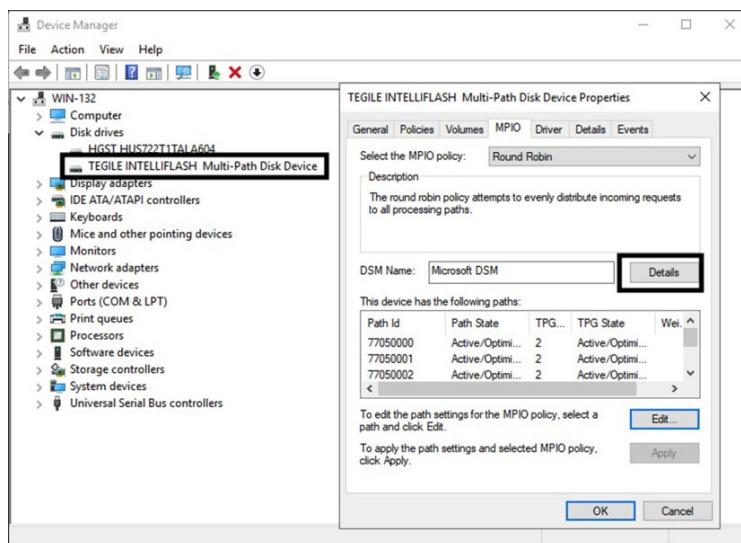
It is also recommended to make the below settings for iSCSI Initiator:

- MaxRequestHoldTime: **60**
- LinkDownTime: **15**
- MaxTransferLength: **131072 (decimal)**
- FirstBurstLength: **131072 (decimal)**

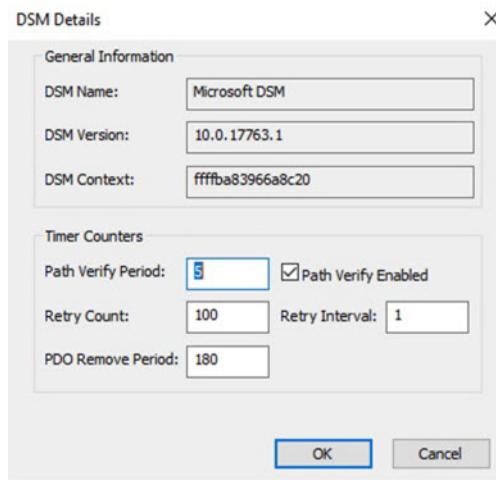
## Configuring MPIO Timers using the Device Manager

To configure MPIO timers using the Device Manager:

1. Open the Device Manager.
2. Right click on the **TEGILE INTELLIFLASH Multi-Path Disk Device** entry under Disk drives.
3. Set the MPIO policy to **Round Robin**.
4. Click **MPIO** tab.



5. Click **Details** next to **DSM Name: Microsoft DSM** to open the **DSM Details** window.



6. Set the values as mentioned in [Windows MSDSM Parameters](#) on page 451.

## Set-MPIOSetting

The **Set-MPIOSetting** cmdlet changes Microsoft Multipath I/O (MPIO) settings. The settings are as follows:

- `NewPathVerificationState`
- `NewPathVerificationPeriod`
- `NewPDORemovePeriod`
- `NewRetryCount`
- `CustomPathRecovery`
- `NewPathRecoveryInterval`
- `NewDiskTimeout`

### Example 1: Executing NewPathVerificationState command

In the following example, you set the `PathVerificationState` from `Disabled` to `Enabled`.

```
PS C:\> Set-MPIOSetting -NewPathVerificationState Enabled
WARNING: Settings changed, reboot required.
PS C:\>
```

### Example 2 - Executing NewPathVerificationPeriod command

In this example, you set the `PathVerificationPeriod` from 30 to 5.

```
PS C:\> Set-MPIOSetting -NewPathVerificationPeriod 5
WARNING: Settings changed, reboot required.
```

```
PS C:\>
```

### Example 3 - Executing NewPDORemovePeriod command

In the following example, you change the PDORemovePeriod from 20 to 180.

```
PS C:\> Set-MPIOSetting -NewPDORemovePeriod 180
WARNING: Settings changed, reboot required.
PS C:\>
```

### Example 4 - NewRetryCount command

In this example, you set the new RetryCount to 100.

```
PS C:\> Set-MPIOSetting -NewRetryCount 100
WARNING: Settings changed, reboot required.
PS C:\>
```

### Example 5 - CustomPathRecovery command

In the following example, you set the CustomPathRecovery state from Disabled to Enabled.

```
PS C:\> Set-MPIOSetting -CustomPathRecovery Enabled
WARNING: Settings changed, reboot required.
PS C:\>
```

### Example 6 - NewPathRecoveryInterval command

In this example, you set the new PathRecoveryInterval to 40.

```
PS C:\> Set-MPIOSetting -NewPathRecoveryInterval 40
WARNING: Settings changed, reboot required.
PS C:\>
```

### Example 7 - NewDiskTimeout command

In this example, you set the new DiskTimeout value from 60 to 180.

```
PS C:\> Set-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Services
\Disk' -Name TimeoutValue -Value 180
PS C:\>
```

### Example 8 - Get-MPIOSetting command

In this example, Get-MPIOSetting command will list the latest MPIO settings.

```
PS C:\> Get-MPIOSetting
```

```

PathVerificationState      : Enabled
PathVerificationPeriod    : 5
PDORemovePeriod           : 180
RetryCount                 : 100
RetryInterval               : 1
UseCustomPathRecoveryTime : Enabled
CustomPathRecoveryTime     : 40
DiskTimeoutValue           : 180

```

```
PS C:\>
```

### Example 9 - iSCSI Initiator

In the following example, the four settings below are set to initiate iSCSI.

- MaxRequestHoldTime = 60
- LinkDownTime = 15
- MaxTransferLength = 131072 (decimal)
- FirstBurstLength = 131072 (decimal)

```

PS C:\> $iscsipath = Get-ChildItem HKLM:\SYSTEM\CurrentControlSet\Control
\Class\"{4d36e97b-e325-11ce-bfc1-08002be10318}" -Recurse -ErrorAction
SilentlyContinue |Get-ItemProperty -name DriverDesc -ErrorAction
SilentlyContinue|Where {$_.DriverDesc -like "Microsoft iSCSI Initiator"} |
foreach {echo $_.PSPPath}
PS C:\> $iscsipath = "$isccipath\Parameters"
PS C:\> get-item -path $isccipath |Set-ItemProperty -ErrorAction
SilentlyContinue -name MaxRequestHoldTime -value 60
PS C:\> get-item -path $isccipath |Set-ItemProperty -ErrorAction
SilentlyContinue -name LinkDownTime -value 15
PS C:\> get-item -path $isccipath |Set-ItemProperty -ErrorAction
SilentlyContinue -name MaxTransferLength -value 131072
PS C:\> get-item -path $isccipath |Set-ItemProperty -ErrorAction
SilentlyContinue -name FirstBurstLength -value 131072
PS C:\>

```

---

# Chapter 24

---

## Notifications

---

**Topics:**

- *About Notifications*
- *Notifications Types and Categories*
- *Notification Example*
- *Notifications Quick View Window*
- *Notifications Tasks*
- *Configuring Notification Settings*

## About Notifications

---

IntelliFlash Operating Environment sends notifications about important events and problems occurring on your IntelliFlash Array. Notifications provide details about the event or problem and in some cases, a possible solution. For example, if an HA pair node fails, IntelliFlash generates a notification and suggests that you check the network connection.

The IntelliFlash Operating Environment automatically deletes low priority notifications after a two-week period by default. However, it retains high-priority notifications and notifications that require an acknowledgement. IntelliFlash retains these notifications until you acknowledge them. You cannot manually delete a notification, but you can configure the duration for which IntelliFlash retains the notifications.

You can customize your email notifications and CallHome notifications in **Settings > Notifications**. You can set notification thresholds for space and meta space usage, and time drift between the controllers and NTP or AD servers. You can modify default notification thresholds that apply across the system or configure custom settings on a per pool or per event basis.

## Notifications Types and Categories

---

### Notification Types

IntelliFlash has the following notification types:

- Critical
- High
- Medium
- Low



**Note:** If you have not customized your notifications, the IntelliFlash Web UI automatically sends email notifications for **Critical** events to you and the IntelliFlash Technical Support team.

### Notification Categories

IntelliFlash notifications are grouped into different categories. For some categories, IntelliFlash automatically sends emails to the email IDs provided in the **SMTP Settings** page. If you have enabled **CallHome** in the **Settings > Administration > Customer Support** page, emails are sent to **IntelliFlash Technical Support**.

The notifications are grouped into the following categories:

- ACL
- Controller
- Disk

- Encryption
- Fault Management (FM)
- Fiber Channel (FC)
- Folder
- High Availability
- Host Group
- IntelliCare
- IntelliFlash Web UI
- IPMI
- iSCSI
- LUN
- Maintenance Mode
- Microsoft AD Server
- Network
- NVDIMM
- Pool
- Project
- Replication
- Service
- Share
- SMB
- Snapshot
- Target Group
- TDPS
- Upgrade Related
- VMware

## Notification Example

---

IntelliFlash generates the following notification when share usage has exceeded a threshold:

**Table 12: Share Usage Exceeded Threshold**

Event Code	SHR4603W46005
Description	Space usage for the share '<share_name>' exceeded warning threshold of <threshold>%.
Details	Share usage exceeded threshold.
Notification Type	High

Email Notification	true
CallHome	true

Notifications include an **Event Code** parameter, which helps you to identify the notification event. The event code is a string that encodes the Event Originator, Event Category, Event Result Type (S: Success, W: Warning, E:Error, A: Abnormal End, and I: Information), and Event Type (numeric). For example, the above notification has an event code **SHR4603W46005**.

The default threshold limit for the above event is 90. This means that the following notification is sent when the usage reaches 90%:

```
Share: '<share_name>' usage has exceeded threshold: 90%.
```

Notification is sent immediately if the scenario recurs before the specified time interval. For example, in the above notification, if you delete a few files in the share and bring down the space utilization below 90%, and then subsequently add more files to the share so that the space utilization again exceeds 90%, the notification is sent as soon as the 90% threshold is crossed.

The **Email notification/CallHome** field in the description table for a notification indicates whether IntelliFlash automatically sends an email alert for that particular notification.

## Notifications Quick View Window

---

Click the Notifications ( ) icon at the top-right corner of the IntelliFlash Web UI menu bar to view the **Notifications** quick view window.

In the **Notifications** quick view window enables you to view the most recent 10 notifications: in-progress notifications appear first, notifications that require acknowledgement appear second in the list, followed by other notifications that are sorted based on timestamp.

You can quickly acknowledge notifications that require an acknowledgement by clicking the **ACK** tab for the notification. Some Critical or High notifications require acknowledgement, as they require user intervention or warn the user of impending issues. To acknowledge all the notifications that require acknowledgement, click the **Acknowledge All** button.

You can also open the **Notifications** page to view more details about the notifications and acknowledge them. Click the **View All Notifications** link at the bottom left corner of the Notifications quick view window to open the **Notifications** page.

## Notifications Tasks

---

The **Notifications** page displays all system notifications. Click the **View All Notifications** link at the bottom left corner of the **Notifications** quick view window to view the **Notifications** page.

You can perform the following tasks in the **Notifications** page:

- View all notifications.
- Acknowledge a single notification or all notifications by using the **ACK** or **ACK All** tab.
- View the event state of the notification.
- View the description and details of a notification.

- Filter notifications and view required notifications by **Type**, **Event State**, **Event Code**, and **Event Time**.

The **Notifications** page has the following components:

- **ACK All tab**

Enables you to acknowledge all of the notifications with one click.

- **ACK Filtered tab**

 **Note:** The **ACK Filtered** tab appears only when you have filtered notifications.

You can filter notifications in the IntelliFlash Web UI and acknowledge only the filtered notifications. The IntelliFlash Web UI allows you to filter notifications by Type, Event State, Event Code, and Event Time columns. You can also use a combination of these filters and acknowledge notifications using the **ACK Filtered** tab.

- **Refresh button**

Allows you to refresh the **Notifications** page and see the latest notifications.

- **Notifications columns:**

- **Type** – The severity of the notification (Critical, High, Medium, Low).
- **Message** – A brief description of the notification.
- **Event State** – Stage of the notification (Initial, Started, In Progress, Waiting, Completed, Failed, Aborted, and Abandoned).
- **Event Code** - Displays the identification code for the notification.
- **Event Time** – The timestamp of the notification.
- **Actions** – The **Details** link under this column expands to display more information about the notification, including the event code.
- **ACK button** – Click this button to acknowledge a notification.

 **Note:** The **ACK** button appears only for those notifications that are not yet acknowledged.

## Viewing and Acknowledging Notifications

To view the **Notifications** page, complete the following steps:

1. Click the Notifications () icon at the top-right corner of the IntelliFlash Web UI menu bar to access the **Notifications** quick view.
2. In the **Notifications** quick view, click **View All Notifications**.  
The **Notifications** page appears.
3. In the **Notifications** page, you can acknowledge notifications in one of the following ways:
  - Click the **ACK** tab in the **Notifications** page to acknowledge a single notification.
  - Filter notifications by **Type**, **Event State**, **Event Code**, or **Event Time**. After selecting the criteria, click the **ACK Filtered** tab to acknowledge the selected notifications.
  - Click the **ACK All** tab to acknowledge all notifications.

## Viewing Notification Details

To view details of a notification, complete the following steps:

1. Click the Notifications () icon at the top-right corner of the IntelliFlash Web UI menu bar to access the Notifications quick view window.
2. In the **Notifications** quick view window, click **View All Notifications**.  
The **Notifications** page appears.
3. In the **Notifications** page, click the **Details** link or click the **Expand ( > )** button in the first column to view the details of the selected notification.
4. (Optional) To hide the details of a notification, click the **Hide Details** link.

## Filtering Notifications

You can filter notifications based on the notification type, event state, event code, and time to view a subset of notifications. For example, you can apply a filter to view only **Critical** notifications or only notifications with the **Completed** event state.

Make sure to clear any filter that is applied if you want to view all notifications in the **Notifications** page.

Complete the following steps to filter notifications:

1. Click the Notifications () icon at the top-right corner of the IntelliFlash Web UI menu bar to access the Notifications quick view window.
2. In the Notifications quick view window, click **View All Notifications**.
3. In the **Notifications** page, click the Filter () icon next to the desired filter.
4. Select the desired option from the dropdown list that appears, and then click the **Filter** button to filter notifications by that criteria. Criteria are as follows:

Filter	Options
Type	Critical, High, Medium, Low.
Event State	Initial, Started, In Progress, Waiting, Completed, Failed, Aborted, Abandoned.
Event Code	In the text box, enter an event code.
Event Time	Click the calendar button next to the =, <, or < icons to filter events by a range of dates that is equal to, later than, or earlier than the selected date. From the dropdown list, select

Filter	Options
	the date range for which you want to view notifications.

The **Notifications** page refreshes and displays the selected notifications types.

## Clearing Notification Filters

To clear notification filters, complete the following steps:

1. Click the Notifications ( ) icon at the top-right corner of the IntelliFlash Web UI menu bar to access the **Notifications** quick view window.
2. In the **Notifications** quick view window, click **View All Notifications**.  
The **Notifications** page appears.
3. In the **Notifications** page, click the icon in the column where you applied the filter and then click **Clear**.

## Configuring Notification Settings

---

The **Settings > Notifications** menu consists of the following pages:

- [Profiles](#)
- [Threshold](#)
- [Delete Config](#)

### Profiles page

The **Profiles** page allows you to manage **Global Default Settings** and **Global Customized Settings**. You can either retain **Global Default Settings** or enable **Global Customized Settings**. You cannot enable both the settings at the same time.

#### Global Default Settings section

**Global Default Settings** apply to all notifications in IntelliFlash by default. **Global Default Settings** are enabled by default for email and CallHome Notifications. Email notifications are sent for notifications with severity, High and above. All CallHome alerts are sent only once a day and are sent to the IntelliFlash Technical Support team and the email ID you configured to receive CallHome alerts.

#### Global Customized Settings section

You can customize notifications using **Global Customized Settings**. When customizing notifications, you can select the severity level of alerts for which you want email or CallHome

notifications and you can set a limit on the number of alerts sent. You can set limits based on the number of instances and by time interval.

In the **Global Customized Settings** section, you can enable or disable the following properties for each notification event:

- Requires Acknowledgement
- Send Email Notifications
- Set limit on email alerts
- Enable CallHome alerts
- Set limit on CallHome alerts

In the **Notifications Configurations** window in **Global Customized Settings**, you can view the default configuration and customized configuration settings. To customize an individual alert, select an alert from the filtered list and customize in the **Event Properties** section.

### **Threshold page**

The **Threshold** page consists of the following tabs:

- Space Usage
- Time Drift
- Meta Usage

### **Space Usage tab**

IntelliFlash by default sends notifications for space usage in pools, projects, shares, and LUNs based on the default threshold. The IntelliFlash Web UI provides warning and critical notification thresholds.

The default thresholds are as follows:

- When a pool, project, share, or LUN uses 80% of the total capacity, IntelliFlash sends an email notification to you every 24 hours.
- When a pool, project, share, or LUN uses 95% of the total capacity, IntelliFlash sends an email notification to you and IntelliFlash Technical Support every hour.
- When a pool, project, share, or LUN uses 100% of the total capacity, IntelliFlash sends an email notification to you and IntelliFlash Technical Support every 30 minutes.

 **Note:** By default, you receive one email per day if space usage reaches the warning threshold. If space usage reaches the critical threshold, IntelliFlash sends you and the IntelliFlash Technical Support team one email per day. However, you can configure the frequency of emails in **Global Customized Settings**.

You can add custom thresholds to send notifications for individual pools, projects, shares, or LUNs. You can customize thresholds for all pools, all projects, all shares, or all LUNs, or you can

add a custom threshold for a specific pool, project, share or LUN. When you add custom rules, IntelliFlash overrides the default settings.

### Time Drift tab

IntelliFlash sends a notification when it detects a defined time drift between the controllers, or between the NTP server and a controller, or between the AD Server and a controller. The default time drift is 120 seconds.

### Meta Usage tab

IntelliFlash maintains default notification thresholds for meta space usage of all pools. When meta space usage reaches 70% of the total space (warning threshold), you receive an email alert. When meta space usage reaches 85% of the total space (critical threshold), you and the IntelliFlash Technical Support team receive an email alert.

### Delete Config page

The **Delete Config** page allows you to configure how notifications are deleted. By default, IntelliFlash deletes all low severity notifications that are two weeks old.

## Modifying Global Default Settings

You can modify the default notification settings globally. You can enable or disable Email notifications and CallHome notifications for notifications with Type **High and higher**. The changes to the default notification settings are applied to all the notifications.

To modify global default settings for all notifications, complete the following steps:

1. Click **Settings > Notifications**.
2. In the **Notifications** pane on the left, click **Profiles**.
3. Enable or disable **Global Default Settings**.
4. Enable or disable **Email Notifications**.  
When you enable **Email Notifications**, emails are sent for events with **High** severity and other higher severity levels.
5. Enable or disable **CallHome Notifications**.  
When you enable **CallHome Notifications**, notifications are sent for events with **Critical** severity only.
6. Click **Save** to apply the settings.

## Managing Global Customized Settings

You can customize global notification settings. Changes to default notification settings are applied to all notifications. You can modify the following settings:

- Enable or disable email and CallHome notifications.
- Set the severity of the notifications for which email and CallHome notifications are to be sent.  
For example, selecting the **Critical Only** severity level sends **Email/CallHome Notifications** for **Critical** severity notifications only.
- Set limit for email and CallHome notifications based on instance or time.

 **Note:** IntelliFlash automatically adds 12 preconfigured customized notification rules.

To customize global notification settings, complete the following steps:

1. Click **Settings > Notifications**.
2. In the **Notifications** pane on the left, click **Profiles**.
3. In the **Profiles** page, select **Global Customized Settings**.
4. Enable **Email Notifications** and select the severity level from the dropdown list. The options are **Critical Only**, **High and Higher**, **Medium and higher**, or **All**.
  - **Critical Only** sends email alerts for events with the **Critical** severity type.
  - **High and higher** sends email alerts for events with the **High** and **Critical** severity levels.
  - **Medium and higher** sends email alerts for events with the **Medium**, **High**, and **Critical** severity type.
  - **All** sends email alerts for all events.
5. To set **Email alert limit**, click **More** and select the required limit from the **Limit By** dropdown list and click **Done**.
  - To send all email notifications, select **No Limit (Send All)**.
  - To set a limit based on a number of instances, select **Limit by Instance** and select the number of occurrences from the **One every** dropdown list.
  - To set a limit based on time, select **Limit by Time** and select the time from the **One every** dropdown list.
6. Enable **CallHome Notifications** and select the severity level. The options are **Critical Only**, **High and Higher**, **Medium and higher**, or **All**.
  - **Critical Only** sends CallHome notifications for events with **Critical** severity.
  - **High and higher** sends CallHome notifications for events with **High** and **Critical** severity types.
  - **Medium and higher** sends CallHome notifications for events with **Medium**, **High**, and **Critical** severity type.
  - **All** sends CallHome notifications for all events.
7. To set **CallHome alert limit**, click **More** and select the required limit from the **Limit By** dropdown list and click **Done**.
  - To send all CallHome notifications, select **No Limit (Send All)**.
  - To set a limit based on a number of instances, select **Limit by Instance** and select the number of occurrences from the **One every** dropdown list.

- To set a limit based on time, select **Limit by Time** and select the time from the **One every** dropdown list.
8. Click **Save** to apply the settings.

## Viewing Default Event-Level Configurations

To view default event-level notification configurations, complete the following steps:

1. Click **Settings > Notifications**.
2. In the **Notifications** pane on the left, click **Profiles**.
3. Click **Edit** in the **Global Customized Settings** section.  
In the Profile page, the number of customized notifications appear against the **Edit** button. If there are no notifications enabled, the UI displays **Edit(0)**.
4. In the **Notification Configurations** window, select **Default Configurations** from the **View Event-Level Notification Configurations** dropdown list to view the list of default notifications.

## Customizing Event-Level Configurations

You can customize the notification settings for each event. To set notification configurations for a specific event, complete the following steps:

1. Click **Settings > Notifications**.
2. In the **Notifications** pane on the left, click **Profiles**.
3. In the **Profiles** page, click **Edit** in the **Global Customized Settings** section.  
In the Profile page, the number of customized notifications appear against the **Edit** button. If there are no notifications enabled, the UI displays **Edit(0)**.
4. In the **Notification Configurations** window, select **Default Configurations** in **View Event-Level Notification Configurations** dropdown list to view the list of default notifications. Select **Customized Configurations** to view the list of customized configurations.
5. Select the required notification and modify the properties in **Event Properties** section:
  - a) Enable or disable the **Requires Acknowledgement**.
  - b) To set the email alert limit, select one of the following options in the **Email Notifications** section:
    - To send all email notifications, select **No Limit (Send All)**.
    - To set a limit based on a number of instances, select **Limit by Instance** and select the number of occurrences from the **One every** dropdown list.
    - To set a limit based on time, select **Limit by Time** and select the time from the **One every** dropdown list.
  - c) To set the CallHome alert limit, select one of the following options in the **CallHome** section:

- To send all CallHome notifications, select **No Limit (Send All)**.
  - To set a limit based on a number of instances, select **Limit by Instance** and select the number of occurrences from the **One every** dropdown list.
  - To set a limit based on time, select **Limit by Time** and select the time from the **One every** dropdown list.
6. Click **Save** to save the settings.

## Deleting Customized Event-Level Notifications

When you remove the customized properties of a selected event or events, the properties revert to the global customized settings.

To delete customized event-level notifications, complete the following steps:

1. Click **Settings > Notifications**.
2. In the **Notifications** pane on the left, click **Profiles**.
3. In the **Profiles** page, click **Edit** in the **Global Customized Settings** section.  
In the Profile page, the number of customized notifications appear against the **Edit** button. If there are no notifications enabled, the UI displays **Edit(0)**.
4. In the **Notification Configurations** page, select **Customized Configurations** from the **View Event- Level Notifications Configurations** dropdown list to view the list of customized configurations.
5. Select the required notification and click **Remove** to remove the selected notification settings. Click **Remove All** to remove all customized notification settings.
6. Click **Yes** to confirm deletion and click **Save**.

## Filtering Notification Configurations

In the **Notifications Configurations** window, you can filter notifications based on the notification class, code (Event Code), name, and severity of the notification. You can also filter based on whether Acknowledgement, Email, and CallHome are enabled.

 **Note:** You can filter the notifications by their configurations only when you use **Global Customized Settings**.

Clear any filter that you have applied earlier to view all notifications in the **Notifications Configurations** window.

To filter notifications, complete the following steps:

1. Click **Settings > Notifications**.
2. In the **Notifications** pane on the left, click **Profiles**.
3. In the **Profiles** page, click **Edit** in the **Global Customized Settings** section.  
In the Profile page, the number of customized notifications appear against the **Edit** button. If there are no notifications enabled, the UI displays **Edit(0)**.
4. In the **Notification Configurations** window, select **Customized Configurations** from the **View Event- Level Notification Configurations** dropdown list.
5. Click the filter icon (  ) next to **Class**, **Code**, **Name**, **Severity**, **Ack**, **Email**, or **CallHome** and select from the following criteria:
  - In the **Class** column, select the required notification class and click the **Filter** button to filter notifications by class.
  - In the **Code** column, enter the event code in the **Code =** field and click the **Filter** button to filter notifications by code.
  - In the **Name** column, enter the name in the **Name =** field and click the **Filter** button to filter notifications based on name.
  - In the **Severity** column, select the required severity (Critical, High, Low, or Medium), and click the **Filter** button to filter notifications based on severity.
  - In the **Ack** column, select **On** or **Off** and click the **Filter** button to filter notifications based on whether acknowledgement is required for notifications.
  - In the **Email** column, select **On** or **Off** and click the **Filter** button to filter notifications based on email notification setting.
  - In the **CallHome** column, select **On** or **Off** and click the **Filter** button to filter notifications based on CallHome notification setting.

The **Notification Configuration** window refreshes and displays the notifications based on the filter applied.

## Modifying Default Space Usage Thresholds

You can set warning and critical threshold values to receive notifications when the space usage changes for pool, projects, shares, or LUNs.

To modify the settings for space usage notifications, complete the following steps:

1. Click **Settings > Notifications**.
2. In the **Notifications** pane on the left, click **Threshold > Space Usage**.
3. In the **Default Space Usage Thresholds** section, set the **Warning Threshold** and **Critical Threshold** values. These values define the threshold rule for the space usage of all pools, projects, shares, and LUNs.
4. Click **Save**.

## Adding Custom Space Usage Thresholds

You can add custom space usage thresholds to receive notifications when the space usage changes for pool, projects, shares, or LUNs.

To add custom settings for space usage notifications, complete the following steps:

1. Click **Settings > Notifications**.
2. In the **Notifications** pane on the left, click **Threshold > Space Usage**.
3. In the **Custom Space Usage Thresholds** section, click **Add** to add custom rules for individual pools, projects, shares, and LUNs.
4. In the **Add Space Usage Rule** window, do any of the following:
  - To set rules for all projects, shares, and LUNs, select the pool from the **Scope** dropdown list and then select **All Projects**, **All Shares**, or **All LUNs**.
  - To set rule for a specific project, select the pool from the **Scope** dropdown list and then select **Specific Project > Project Name**.
  - To set rule for a specific share, select the pool from the **Scope** dropdown list and then select **Specific Share > Share Name**.
  - To set rule for a specific LUN, select the pool from the **Scope** dropdown list and then select **Pool Name > Specific LUN > LUN Name**.
5. Set the **Warning Threshold** and **Critical Threshold** values and click **Add**.

## Modifying Default Meta Usage Thresholds

To modify the default settings for meta space usage notifications, complete the following steps:

1. Click **Settings > Notifications**.
2. In the **Notifications** pane on the left, click **Threshold** and then click the **Meta Usage** tab.
3. In the **Default Rule** section, set the **Warning Threshold** and **Critical Threshold** values. These values define the threshold rule for the meta space usage of all pools, projects, shares, and LUNs.
4. Click **Save**.

## Adding Custom Meta Usage Thresholds

To modify the settings for meta space usage notifications, complete the following steps:

1. Click **Settings > Notifications**.
2. In the **Notifications** pane on the left, click **Threshold** and then click the **Meta Usage** tab.
3. In the **Custom Rule** section, click **Add** to add custom rules for individual pools, projects, shares, and LUNs meta space usage.
4. In the **Add Meta Space Usage Rule** window, select the pool from the **Scope** dropdown list.
5. Set the **Warning Threshold** and **Critical Threshold** values and click **Add**.

## Modifying Time Drift

To modify the settings for time drift notifications, complete the following steps:

1. Click **Settings > Notifications**.
2. In the **Notifications** pane on the left, click **Threshold** and then click the **Time Drift** tab.
3. Set time drift rules for the following:
  - Critical Time Drift Threshold between the two controllers
  - Critical Time Drift Threshold between the NTP Server and a controller
  - Critical Time Drift Threshold between the AD Server and a controller
4. Click **Save**.

## Setting Auto Delete for Older Notifications

IntelliFlash automatically deletes older notifications of low severity level notifications that are older than two weeks.

To enable deleting old notifications, to change the severity levels or the duration of the notifications, complete the following steps:

1. Click **Settings > Notifications > Auto Delete**.
2. Click the **Auto Delete Notifications** toggle button to enable deleting the old notifications and to change the severity levels.
3. Select any of the following options from the **Severity** dropdown list:
  - **All** deletes all notifications.
  - **High and lower** deletes notifications with the **High**, **Medium**, and **Low** severity levels.
  - **Medium and lower** deletes notifications with the **Medium** and **Low** severity levels.
  - **Low only** deletes notifications with the **Low** severity level.
4. Set the duration (days, weeks, months, or years) from the **After** dropdown list.

IntelliFlash automatically deletes notifications older than the time defined here.

5. Click **Save**.

---

# Chapter 25

---

## Reporting Services

---

**Topics:**

- *Report Types*
- *Generating Pool Usage Report*
- *Generating Project Usage Report*
- *Generating Dataset Report*
- *Scheduling Reports*

## Report Types

---

The reporting services feature enables you to monitor and analyze storage space usage on your IntelliFlash Array. You can generate instant reports or schedule to send reports to the IntelliFlash administrator or a designated email ID. You can generate the space usage reports for the following:

- Pool
- Project
- Dataset

A dataset contains shares and LUNs.

## Generating Pool Usage Report

---

The pool usage report helps you to analyze the space consumption, available free space, reserved space usage, space saving percentage, and space saving achieved with deduplication, and compression. You can select to view reports for all pools in an IntelliFlash Array or a single pool.

To generate a pool usage report, complete the following steps:

1. Click **Services > Report > Usage Reports**.
2. Select **Pool** from the **Scope** list.
3. Select **All Pools** or a specific pool from the **Pool** list.  
You can generate system pools and data pools space usage.
4. Click **Get Report**.

The **Pool Usage Report** displays.

## Generating Project Usage Report

---

The Project usage report helps you to analyze the size of a project, used space, available space, number of shares or LUNs in a project, and space saving achieved per project. You can select to view a report for all projects in a pool or a single project.

To generate a project usage report, complete the following steps:

1. Click **Services > Report > Usage Reports**.
2. Select **Project** from the **Scope** list.
3. Select a **Pool** from the list.
4. Select **All Projects** or a specific project from the **Project** list.  
You can generate reports for **Local** and **Replica** projects.
5. Click **Get Report**.

The **Project Usage Report** appears.

## Generating Dataset Report

---

A dataset contains shares, subshares, and LUNs. The dataset usage report helps you to analyze space utilization, available space, and space saving for individual shares, subshares, and LUNs in each project. You can select to view a report for all shares, subshares, and LUNs in a particular project or a single share, subshare, or LUN.

To generate a dataset report, complete the following steps:

1. Click **Services > Report > Usage Reports**.
2. Select **Dataset** from the **Scope** list.
3. Select a **Pool** from the list.
4. Select a **Project** from the list.
5. Select **All Datasets** or a specific dataset from the **Dataset** list.
6. Click **Get Report**.

The **Dataset Usage Report** appears.

## Scheduling Reports

---

### Scheduling Space Usage Reports

You can set up a schedule to send storage space usage reports to your default administrator email ID or you can provide a desired email ID.

IntelliFlash reporting services enable you to schedule reports for pools, projects, and datasets. The reports provide information about used space, free space, space saving, and so on.

You can schedule reports by minute, hourly, daily, weekly, and monthly intervals.



**Note:** You must configure the SMTP server before you can schedule IntelliFlash storage usage reports. You can configure SMTP from **Settings > Network > SMTP**.

## Related Topics

[Configuring SMTP](#)

### Scheduling Pool Space Usage Report

The SMTP server is configured on the IntelliFlash Array.

To schedule a pool usage email report, complete the following steps:

1. Click **Services > Report > Schedule Reports**.
2. Click **New**.
3. In the **New Report Schedule** page, select **Pool** from the **Scope** list.
4. Select **All Pools** or a specific pool from the **Pool** list.
5. Select the **Email to system admin** option or type a different **Email address**.
6. Select a **Schedule** type.  
Options are: **By Minutes, Hourly, Daily, Weekly, and Monthly**.
7. Click the link next to the **every** text box to set the time/day rule as per the selected schedule type.
8. Click **Save**.

An email schedule is added to the **Scheduled Reports** list. Space usage reports will be sent to the specified email ID as per the schedule.

### Scheduling Project Usage Report

To schedule a project usage email report, complete the following steps:

1. Click **Services > Report > Schedule Reports**.
2. Click **New**.
3. In the **New Report Schedule** page, select **Project** from the **Scope** list.
4. Select a pool from the **Pool** list.
5. Select **All Projects** or a specific project from the **Project** list.
6. Select the **Email to system admin** option or type a different **Email address**.
7. Select a **Schedule** type.

Options are: **By Minutes**, **Hourly**, **Daily**, **Weekly**, and **Monthly**.

8. Click the link next to the **every** text box to set the time/day rule as per the selected schedule type.
9. Click **Save**.

An email schedule is added to the **Scheduled Reports** list. Space usage reports will be sent to the specified email ID as per the schedule.

## Scheduling Dataset Space Usage Report

To schedule a dataset usage email report, complete the following steps:

1. Click **Services > Report > Schedule Reports**.
2. Click **New**.
3. In the **New Report Schedule** page, select **Dataset** from the **Scope** list.
4. Select a **Pool** from the **Pool** list.
5. Select a **Project** from the **Project** list.
6. Select **All Datasets** or a specific dataset from the **Dataset** list.
7. Select the **Email to system admin** option or type a different **Email address**.
8. Select a **Schedule** type.

Options are: **By Minutes**, **Hourly**, **Daily**, **Weekly**, and **Monthly**.

9. Click the link next to the **every** text box to set the time/day rule as per the selected schedule type.
10. Click **Save**.

An email schedule is added to the **Scheduled Reports** list. Space usage reports will be sent to the specified email ID as per the schedule.

## Editing Scheduled Report

To edit an existing scheduled space usage report, complete the following steps:

1. Click **Services > Report > Schedule Reports**.
2. In the **Report Type** list, select the required schedule.
3. Click **Edit**.
4. In the **Edit Report Schedule** window, you can perform the following:
  - a) Modify the report type below the **Report Type** section.

- b) Modify the report schedule below the **Schedule** section.
5. Click **Save**.

## Deleting Scheduled Report

To delete a scheduled space usage report, complete the following steps:

1. Click **Services > Report > Schedule Reports**.
2. In the **Report Type** list, select the required schedule.
3. Click **Delete**.

IntelliFlash deletes the email schedule rule from the list and stops sending the automatic email reports.

---

# Chapter 26

---

## NDMP Server Support

---

**Topics:**

- *Introduction to NDMP Server Support*
- *How the NDMP Backup Works*
- *Supported NDMP Features*
- *NDMP Server Page*
- *Configuring NDMP on an IntelliFlash system*
- *Considerations for Adding the IntelliFlash System in the NDMP Backup Client*
- *Backing Up Data from Replication Target through NDMP Client*
- *Monitoring Active NDMP Backup or Restore Sessions*
- *Editing NDMP Server Details*

## Introduction to NDMP Server Support

Network Data Management Protocol (NDMP) is an open-source protocol to control backup and restore between primary storage systems (such as an IntelliFlash system) and secondary storage systems in a heterogenous network environment.

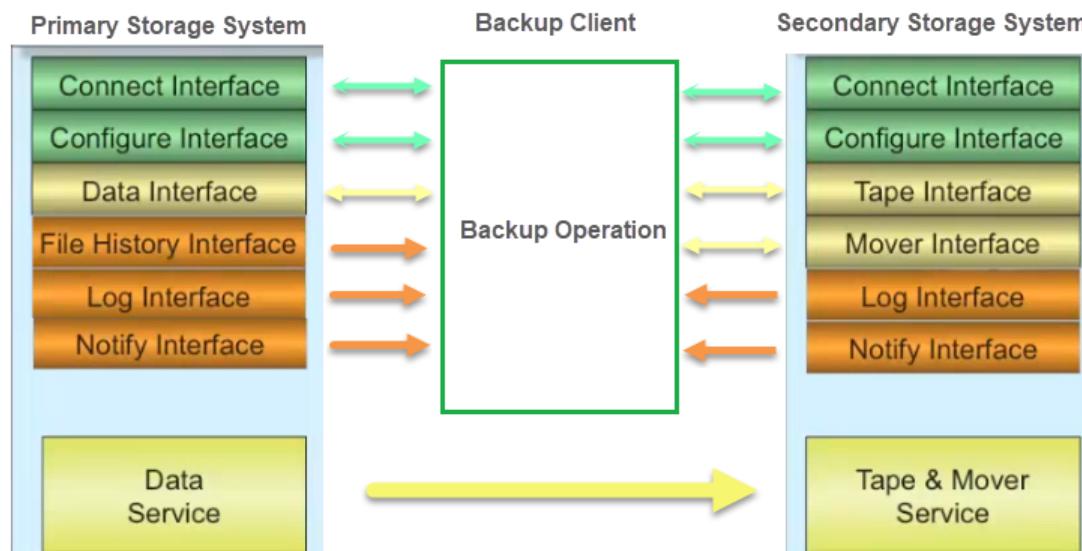
You can now use NDMP clients (such as NetBackup 8.1 or Commvault v11) to back up data from an IntelliFlash system to secondary storage devices, and restore data to the IntelliFlash system. IntelliFlash operating environment supports NDMP versions 3 and 4.

IntelliFlash operating environment supports the remote backup topology. In remote backup, the backup client establishes the data connection between the primary storage system and the secondary storage systems, and facilitates the data backup or restore. The backup client maintains the file history information and the status of the data transfer.

If replication is set up between two IntelliFlash systems, you can back up data from both the source and the target systems through NDMP. To backup and restore data from the replication target using NDMP, clone a share from the replica snapshot and add the cloned share to the NDMP backup client to take backup.

## How the NDMP Backup Works

The Network Data Management Protocol (NDMP) architecture allows you to centralize backup and restore by separating the network-attached backup client (such as NetBackup or Commvault), the data server (primary storage system such as an IntelliFlash system), and the secondary storage system. NDMP runs on top of TCP/IP and uses the external data representation (XDR) record marking, which helps in seamless communication between different computer systems. NDMP also provides low-level control of tape devices and SCSI media changers.



**Figure 31: NDMP Architecture**

As shown in the architecture diagram, NDMP is a typical client/server architecture. IntelliFlash operating environment uses the remote tape backup topology.

The NDMP backup operation workflow is as follows.

1. First, the backup client does the following on the secondary storage system:
  - Creates a control connection to the secondary storage system.
  - Uses the tape library media changer to load the required tape by starting the SCSI service.
  - Prepares the tape interface for the backup operation by starting the tape service.
  - Initializes the backup tape.
  - Prepares the mover interface for the backup operation by starting the mover service.
2. After the secondary storage system is ready, the backup client opens a control connection to the primary storage system.
3. The backup client queries both the primary storage system (for configuration capabilities) and the secondary storage system (for the supported connection types).
4. The backup client establishes a data connection between the two storage systems by starting the data service on the primary storage system. The data service connects to the specified IP address and port of the secondary storage system.
5. The backup client initiates the transfer of backup data. The data service begins sending the backup stream over the data connection.
6. During the data transfer, the NDMP data service sends file history information to the backup client.
7. The NDMP tape service sends notifications to the backup client when any intervention is required. For example, a notification is sent when the tape has to be changed. After the tape is changed, the backup client again prepares the mover interface for continuing the backup operation.
8. After the backup is complete, the data service notifies the backup client that the operation is complete and closes the data connection to the secondary storage system.
9. The backup client closes the control connection with the primary storage system.
10. The secondary storage system detects the data connection closure with the primary storage system.
11. The backup client closes the control connection with the secondary storage system.

## Supported NDMP Features

---

IntelliFlash supports the following NDMP features:

- **NDMP versions:** IntelliFlash supports NDMP versions 3 and 4.
- **NDMP client:** IntelliFlash supports NetBackup 8.1 and Commvault v11.
- **Backup of SMB and NFS shares:** IntelliFlash supports back up and restore of both SMB and NFS shares.

- **Remote tape backup:** IntelliFlash supports only remote tape backup topology.
- **Selective file restore:** This feature helps restore only the required files, instead of restoring the entire backup image.
- **Authentication support:** IntelliFlash supports the `cram-md5-challenger` authentication.
- **Direct Access Recovery (DAR):** Direct Access Recovery (DAR) reduces the time it takes to restore files. DAR enables the array to directly move to the exact file location, instead of sequentially reading the full backup image.
- **Concurrent NDMP sessions:** IntelliFlash allows concurrent NDMP sessions. This enables you to start multiple NDMP sessions for backup.
- **Incremental backup and restore:** IntelliFlash enables to quickly back up only the modified data, instead of taking a full backup every time. This makes backup and restore more efficient for larger shares.
- **Alternative location restore:** When restoring data to the array, IntelliFlash allows you to restore the data to the same pool or to a different pool.
- **File attributes and ACLs:** IntelliFlash maintains the file attributes and ACLs for all the backups and restores.

## NDMP Server Page

---

You can configure NDMP in the **Services > NDMP Server** page. The NDMP service is disabled by default in IntelliFlash.

In the **NDMP Server** page, after NDMP configuration is complete, you can view the active backup or restore sessions.

The **NDMP Server** page displays the following information:

- **Start Time:** The time the backup or restore session started.
- **Elapsed Time:** The time elapsed since the start of the session.
- **Client:** The IP address of the NDMP backup client.
- **Share:** The share that is being backed up or restored.
- **Resource group:** The resource group to which the share belongs.
- **Size:** The size of the backup.
- **Operation Type:** Whether backup or restore operation.
- **Progress:** The progress (in percentage) of the backup or restore operation.

## Configuring NDMP on an IntelliFlash system

---

To facilitate NDMP data backup and restore between an IntelliFlash system and a secondary storage system, you must first configure the NDMP server on the IntelliFlash Web UI. To configure the NDMP server on the IntelliFlash Web UI, complete the following steps:

1. Click **Services > NDMP Server**.
2. In the **NDMP Server** page, click **Edit**.
3. In the **NDMP Server Settings** dialog box, click the **Enable Server** option.  
You must enable the NDMP service, as it is disabled by default.
4. Enter the port number in the **Server Port** box.  
The default port number is 10000. If a firewall is configured between the NDMP Server (IntelliFlash system) and the NDMP client (backup server), then the default port should be opened in your firewall.
5. Enter the user name in the **Server Username** box.
6. Click **Change server password** to enable entering the password for the user.
7. Type the password in the **Server Password** box.
8. Type the password again in the **Confirm Server Password** box.
9. (Optional) Enable **Show Password** to view the password.
10. Click **Save**.

## Considerations for Adding the IntelliFlash System in the NDMP Backup Client

---

After configuring the NDMP service on the IntelliFlash system, add the array in the NDMP backup client. Then set up a backup policy in the NDMP backup client.

Consider the following criteria when you add the IntelliFlash system in the NDMP backup client:

- In the NDMP backup client, add the same user credentials that you saved in the **NDMP Server** page in the IntelliFlash Web UI.
- Use a floating IP address available from a resource group when you provide the IP address of the IntelliFlash system. You can use any of the floating IP addresses available in the resource group or configure a separate floating IP address in the resource group for backup.

 **Note:** When you add a floating IP address, only shares of the pool corresponding to that IP address are visible for backup. If there are two pools in separate resource groups, then add the two floating IP addresses belonging to those resource groups.

- Set up a backup policy in the NDMP backup client. When you select the IntelliFlash system from the list of NDMP hosts, you can drill down to select the share and create the policy for that specific share.
- To back up and restore data from the replication target (when replication is set up between two IntelliFlash systems), clone a share from the replica snapshot through the IntelliFlash Web UI. Add the cloned share from the replication target in the NDMP backup client to take backup.

After you have configured the NDMP server in the **NDMP Server** page, added the IntelliFlash system in the NDMP backup client, and set up a backup policy in the NDMP client, the NDMP client facilitates data backup and restore between the IntelliFlash system and the secondary storage system.

Based on the backup policy, the NDMP backup client starts a backup of the selected shares. You can also restore data to the array after the backup is completed.

## Backing Up Data from Replication Target through NDMP Client

---

To back up data from the replication target through NDMP client, do the following:

1. Configure replication between the two IntelliFlash systems. Schedule snapshots between the systems.
2. In the replication target, identify the replica snapshot (visible under the replica project).
3. Clone a share of the replica snapshot through the IntelliFlash Web UI.
4. *Configure the NDMP service* on the replication target.
5. Add the replication target in the NDMP backup client (for example, Commvault application). Add the same user credentials that you saved in the **NDMP Server** page in the IntelliFlash Web UI of the replication target.  
Use a floating IP address available from a resource group when you provide the IP address of the replication target.
6. Set up a backup policy in the NDMP backup client. When you select the replication target from the list of NDMP hosts, drill down to select the cloned share for the replication target and create the policy.  
The NDMP client now facilitates data backup between the backup target and the secondary storage system.

## Monitoring Active NDMP Backup or Restore Sessions

---

To monitor the active backup or restore sessions, do the following:

1. Click **Services > NDMP Server**.
2. The **NDMP Server** page displays the active backup or restore sessions.

## Editing NDMP Server Details

---

After you have configured the NDMP service in IntelliFlash, you can modify the server details such as the user credentials or the port number. To edit the NDMP server, do the following:

1. Click **Services > NDMP Server**.
2. In the **NDMP Server** page, click **Edit**.
3. In the **NDMP Server Settings** dialog box, modify the NDMP server details.
4. Click **Save**.



---

# Chapter 27

---

## SMI-S Support

---

**Topics:**

- *Introduction to SMI-S*
- *IntelliFlash SMI-S Server Plugin*
- *SMI-S Support for Block Data Access*
- *SMI-S Support for SMB 3.0 Shares*

## Introduction to SMI-S

The Storage Management Initiative Specification (SMI-S) is a standard created by the Storage Networking Industry Association (SNIA) to simplify the management of heterogeneous storage systems. Storage systems that support SMI-S can be managed using SMI-S management software such as Microsoft's System Center Virtual Machine Manager (SCVMM).

## IntelliFlash SMI-S Server Plugin

IntelliFlash now supports SMI-S integration with Open Pegasus SMI-S server plugin that can be run in a docker container.

To continue supporting SMI-S integration with IntelliFlash systems, upgrade your systems to IntelliFlash 3.11.0.4 or later. After upgrading to IntelliFlash 3.11.0.4 or later, install and configure Open Pegasus SMI-S server plugin in a docker container.

You can download the IntelliFlash SMI-S server plugin from the following URL:

<https://github.com/DDNStorage/Intelliflash-smi-s-plugin>

After installing and configuring the SMI-S server, add the IP address of the SMI-S docker container in SCVMM.

## Supported Versions for IntelliFlash SMI-S Server

The following table lists the versions of Docker, IntelliFlash, and SCVMM that are supported for the IntelliFlash SMI-S server container.

**Table 13: Supported Versions**

Docker Version	IntelliFlash Version	SCVMM Version
19.03 and later	3.x.x.x and later	2016 and later   <b>Note:</b> Shares already created using the earlier versions of SCVMM are supported.

## Loading SMI-S Server Container Image

The IntelliFlash SMI-S server plugin can be installed on hosts that run Docker version 19.03 and later.

To load the SMI-S server container image, use the following Linux commands:

1. To clone repository:

```
git clone
```

```
https://github.com/DDNStorage/Intelliflash-smi-s-plugin /opt/
Intelliflash-smi-s-plugin
```

2. To untar and load image:

```
tar -zxvf
/opt/Intelliflash-smi-s-plugin/bin/smis-server.tar.gz | xargs docker load
-i
```

## Configuring SMI-S Server Container

Configure the SMI-S server container using the configuration yaml file. By default, the name of the configuration yaml file is **config.yaml**. The yaml file should be mapped into **/etc/cimserver/config.yaml** inside the cimserver container.

```
# 
# Proposal yaml for cimserver configuration
#
cimserver:
    properties: # map to describe cimserver start props
        enableAuthentication: true
        sslBackwardCompatibility: true
    #      enableNamespaceAuthorization: true
    #      logLevel: TRACE
    #      traceComponents: XmlIO
    #      traceLevel: 5
    #      traceFacility: Log
    cert:
        #      countryName: US # default value US
        #      stateOrProvinceName: California # default value California
        #      organizationName: # default value is 'DataDirect Networks, Inc'
        #      organizationalUnitName: # default value 'OpenPegasus cimserver
        instance'
        #      commonName: cimserver.IP # IP or FQDN of the Cimserver certificate
        #      expiration: 365 # Certificate expiration in days, default value is 365
        #      privateKeyPath: <externalPrivateKeyPath>
        #      certificatePath: <externalCertificatePath>
    array: #IntelliFlash array credentials
        endpoint: 10.20.30.40
        user: admin
        password: dA==
    users:
        - user: user1
          password: dXNlcjE=
          permissions:
              - namespace: Intelliflash
                rights: "RW"
```

## SMI-S Server Configuration File Properties

Configure the following fields in the SMI-S server configuration file.

 **Note:** Fields marked \* are mandatory.

**Table 14: Fields in the SMI-S Configuration File**

Field Name	Value	Description
cimserver.properties*	map	The initial properties of OpenPegasus cimserver.
array*	struct	The configuration for the remote IntelliFlash system.
array.endpoint*	string	The IP address or FQDN of the IntelliFlash system.
array.user*	string	The user name for connecting to the IntelliFlash system.
array.password*	string	The password for connecting to the IntelliFlash system.   <b>Note:</b> The password should be encoded in BASE64. For example, <code>echo -n 'password'</code> .
array.users	array	The users for the Cimserver. Enables BASICAUTH for every remote request. Should be used when <code>enableAuthentication=true</code> .
array.users.[n].user	string	The user name for the Cimserver.
array.users.[n].password	string	The password of the Cimserver.   <b>Note:</b> The password should be encoded in BASE64. For example, <code>echo -n 'password'</code> .
array.users.[n].permissions	string	The user namespace permissions for the Cimserver.
array.users.[n].permissions.namespace	string	The user namespace name for the Cimserver.
array.users.[n].permissions.rights	string	The user namespace permissions for the Cimserver. <b>R</b> is for READ authorization, and <b>W</b> is for WRITE authorization.
cimserver.cert	cert	The certificate configuration struct for the Cimserver.
cimserver.cert.countryName	cert	Self-signed certificate 'C' attribute. The default value is <b>US</b> .
cimserver.cert.stateOrProvinceName	cert	Self-signed certificate 'ST' attribute. The default value is <b>California</b> .

Field Name	Value	Description
cimserver.cert.organizationName	cert	Self-signed certificate 'O' attribute. The default value is <b>DataDirect Networks, Inc.</b>
cimserver.cert.organizationalUnitName	cert	Self-signed certificate 'OU' attribute. The default value is <b>OpenPegasus cimserver instance</b> .
cimserver.cert.commonName	cert	Self-signed certificate 'CN' attribute. If the attribute is not defined, the IP address of the container is used.
cimserver.cert.expiration	cert	Self-signed certificate expiration in days. The default value is <b>365</b> .
cimserver.cert.privateKeyPath	cert	External private key file path. <b>certificatePath</b> must be specified too. This path should be the container path, and not the host.
cimserver.cert.certificatePath	cert	The external certificate file path. <b>privateKeyPath</b> must be specified too. This path should be the container path, and not the host.

 **Note:**

- Provide any user's credentials when **enableAuthentication** option is set to **true**.
- If **privateKeyPath** and **certificatePath** are specified, then **cert** options are omitted.
- An example of SMI-S configuration is available here: <https://github.com/DDNStorage/Intelliflash-smi-s-plugin/blob/master/config/config.yaml>.

## Editing the SMI-S Server Configuration File

To modify the SMI-S Server configuration file, run the following command:

```
vim /opt/Intelliflash-smi-s-plugin/config/config.yaml
```

See [SMI-S Server Configuration File Properties](#) for information about the fields and attributes in the configuration file.

## Starting SMI-S Server Container

To use SMI-S management software with the IntelliFlash array, enable SMI-S using IntelliFlash web UI. After enabling SMI-S, edit the default names that IntelliFlash uses for SMI-S requests that do not include a required pool, project, or dataset name.



**Note:** For more information about default SMI-S names, see [SMI-S Default Names](#).

To start the SMI-S container, run the following command:

```
docker run -dit -p 5988:5988 -p 5989:5989  
-v /opt/Intelliflash-smi-s-plugin/config:/etc/cimserver smis-server:1.0
```

To use individual IP address for SMI-S container, create a static IP address (for example 10.10.10.10) on your docker host and run the container with the following modified option:

```
docker run -dit -p 10.10.10.10:5988:5988 -p 10.10.10.10:5989:5989  
-v /opt/Intelliflash-smi-s-plugin/config:/etc/cimserver smis-server:1.0
```

## Stopping SMI-S Server Container

To stop the SMI-S docker container, run the following command:

```
docker ps | grep -i -m 1 smis-server | awk '{print $1}' |  
xargs docker kill
```

## Connecting to SMI-S Server from SCVMM

To connect to the SMI-S provider from SCVMM, use the IP address or the FQDN of the SMI-S server and the ports that are specified in the docker run command.

See [Adding IntelliFlash arrays in SCVMM](#) for more information.

## Viewing Logs for SMI-S Server Plugin

View the SMI-S logs to troubleshoot issues that might occur when starting or working with the SMI-S Server plugin. The SMI-S logs include information such as connection errors and password problems.

To view the SMI-S logs, run the following command:

```
docker ps | grep -i -m 1 smis-server | awk '{print $1}' |  
xargs docker logs
```

## SMI-S Support for Block Data Access

IntelliFlash supports SMI-S with block protocols (FC and iSCSI). You can use SCVMM to create, delete, map-unmap, and clone LUNs. You can also use SCVMM to rapidly provision Hyper-V VMs from a gold master template.

## Enabling iSCSI on a Windows Host that has both FC and iSCSI

If a Windows host server has both FC and iSCSI configured to access the IntelliFlash system, SCVMM always uses FC. This is as designed by Microsoft. If you prefer to use iSCSI instead of FC, you have to remove FC access to the IntelliFlash system from that host.

### SMI-S Default Names

Pool, project, or LUN names are optional in some SMI-S operations. Correspondingly, SMI-S management software allows you to perform such operations without specifying the optional names. However, the IntelliFlash array might require the optional names to determine the complete path for the objects on which the operation has to be performed.

To address this discrepancy, the IntelliFlash OS allows you to specify default pool, project, and LUN names for SMI-S. The IntelliFlash OS uses a default name if it requires a name for a particular operation, but the SMI-S management software does not provide the same.

The following table lists the predefined default names that the IntelliFlash OS uses for the SMI-S operations. You can view and change the default SMI-S names from the **Settings > App-Aware > SMI-S Settings** page.

The following table lists the predefined default names.

**Table 15: Default SMI-S Names**

Object	Default Name	Description
Pool	SMIPool	The default pool name is used if you do not provide a pool name.
Project	SMIProject	The default project name is used if you do not provide a specific project name.
Dataset	SMIVolume	The default volume name is used if you do not provide a specific volume name.

## Enabling SMI-S and Editing the Default Name Prefixes

You must enable SMI-S on an IntelliFlash system to use SMI-S management software with the array. After enabling SMI-S, you can edit the default names that IntelliFlash uses for SMI-S requests that do not include a required pool, project, or dataset name.

 **Note:** For more information about default SMI-S names, see [SMI-S Default Names](#).

To enable SMI-S on an IntelliFlash system, complete the following steps in the IntelliFlash Web UI:

1. Click **Settings > App-Aware > SMI-S Settings**.
2. In the **SMI-S Settings** page, enable **SMI-S**.  
The SMI-S default name fields are enabled and can be edited.
3. Modify the default names, as desired.
4. Click **Save**.



**Note:** Enabling SMI-S does not create any project or LUN.

## Adding an IntelliFlash system as SMI-S Integrated Storage Device in SCVMM

To add the IntelliFlash system as a storage device, complete the following steps in SCVMM:

1. In SCVMM, select the **Fabric** workspace.
2. Click **Add Resources** in the **Home** tab of the SCVMM ribbon.
3. Click **Storage Devices** in the **Add Resources** menu.  
The **Add Storage Devices Wizard** appears.
4. Select **SAN and NAS devices discovered and managed by a SMI-S provider** and click **Next**.
5. Enter the IP address or the FQDN of the SMI-S Server container in the **Provider IP address or FQDN** field.
6. Select the **Use Secure Sockets Layer (SSL) connection** option.
7. Create a **Run As account** by completing the following steps:
  - a) Click **Browse** next to **Run As account**.  
The **Select a Run As Account** dialog box appears.
  - b) Click **Create Run As Account**.  
The **Create Run As Account** dialog box appears.
  - c) Enter the following details in the **Create Run As Account** dialog box:
    - **Name:** Enter a name that helps you identify the Run As account. For example, a name that includes the array name.
    - **User name:** Enter the web administrator user name for the IntelliFlash system.
    - **Password:** Enter the password for the web administrator account.



**Important:** Ensure that the **Validate domain credentials** option is not selected as the web administrator account does not exist on the domain's Active Directory servers.

Click **Finish** after entering the above details.

- d) Select the newly created **Run As account** in the **Select a Run As Account** dialog box.
  - e) Click **OK**.  
The **Add Storage Devices Wizard** appears again.
8. Click **Next**.  
The **Import Certificate** dialog box appears.
9. Click **Import** to import the SSL certificate of the array.  
If you had previously imported a controller-specific SSL certificate you need to remove it and import the new array-specific SSL certificate.
10. When the SSL import and inventory is complete, the array details appear. Click **Next** to continue.  
The **Select Storage Devices** page displays the pools discovered on the array. You must associate each pool with a Storage Classification, and optionally a default host group.
11. To create a new **Storage Classification** and associate it with a pool, complete the following steps:
- a) Select the pool.
  - b) Click **Create Classification**.
  - c) Enter a name, and optionally, a description.
  - d) Click **Add**.
  - e) Click the dropdown in the **Classification** column and select the new classification.
  - f) Click the dropdown in the **Host Group** column and select the desired host group.
  - g) Click **Next**.
12. Review the summary, and click **Finish**.  
When you click **Finish**, the Storage Provider addition job window appears.

After the job is complete, click

- **Storage > Classifications and Pools** to verify the pools and their associated storage classifications.
- **Storage > Providers** to verify the listed SMI-S providers.
- **Storage > Arrays** to verify the arrays.

## Default Settings of LUNs Created using SMI-S

LUNs that you create on an IntelliFlash system using an SMI-S management software such as SCVMM have the following default settings:

- Block Size = 32K
- Deduplication = ON
- Compression = LZ4
- Primary and Secondary Cache = ON

The above settings are fixed when you create a LUN from SCVMM—you cannot configure them.

If the LUN is created in a pre-existing project, the settings in the project (except block size) are used. However, project-level snapshot schedules defined in the IntelliFlash Web UI are enforced; they are not overridden by any settings from SCVMM/SMI-S.

Further, when you use SMI-S software to create LUNs in a pre-existing project, those LUNs do not inherit LUN mappings from the project. Only the LUN mappings that you specifically assign to these LUNs after creating them are applied. Protocol settings are also determined from the LUN mappings created using SMI-S.

## Configuring an Array as an iSCSI Target for Hyper-V Hosts using SCVMM

The process for creating and mapping iSCSI LUNs is the same as the process for creating and mapping FC LUNs. However, you need to perform a few additional steps in SCVMM to configure an array as an iSCSI target for Hyper-V hosts.

To configure an array as an iSCSI target for Hyper-V hosts, complete the following steps in SCVMM:

1. In the **Fabric** section of SCVMM, right-click the Hyper-V host for which you want to customize the iSCSI connection and click **Properties**.
2. In the **Properties** dialog, click the **Storage** tab.
3. Click **Add** and select the required array.

## Creating iSCSI Sessions using SCVMM

The default iSCSI connections created by SCVMM work with IntelliFlash arrays, but do not comply with some of the iSCSI best practices. You must customize the iSCSI connections to apply these best practices when using SCVMM.

To create a customized iSCSI session with an IntelliFlash array for Hyper-V hosts, complete the following steps in SCVMM:

1. In the **Fabric** section of SCVMM, right-click the Hyper-V host for which you want to customize the iSCSI connection and click **Properties**.
2. In the **Properties** dialog box, click the **Storage** tab.
3. Click the array that you want to select as the target of the new session.
4. Click **Create Session**.

After creating the iSCSI connections in SCVMM, you can verify the sessions you created by remotely logging into the Windows server (using the Windows RDP client) and checking the iSCSI initiator settings. You should see all the sessions you created.

## Creating LUNs in Existing IntelliFlash Projects using SCVMM

To create a LUN in an existing project from SCVMM, you must provide the name of the project along with the LUN name. If you do not provide a project name when creating a new LUN from SCVMM, IntelliFlash uses the default project name specified in the **SMI-S Settings** page in the IntelliFlash Web UI.

To provide the name of the project along with the LUN name in SCVMM, enter the project name followed by a forward slash, and then the LUN name.

For example, to create a LUN with "EU\_Sales\_Q3" name in the "sales" project, enter the following text in the LUN name field in SCVMM:

```
sales/EU_Sales_Q3
```



**Note:** Project and LUN names are case-sensitive in IntelliFlash.

## Creating and Mapping a LUN as a Shared Volume using SCVMM

You can add a LUN using either the **Available Storage** or **Shared Volumes** section in SCVMM. Shared volumes are configured as Cluster Shared Volumes (CSVs) when they are created. LUNs added to **Available Storage** can be converted to CSVs after creation.

To create and map a LUN as a Shared Volume, complete the following procedure in SCVMM:

1. Allocate capacity for the Pool that will contain the LUN by completing the following steps:
  - a) Click **Fabric > Storage > Classifications and Pools**.
  - b) In the top navigation bar, select **Capacity > Allocate Capacity**.
  - c) In the dropdown for Host Groups, select the host group that contains the cluster or host that will use the pool. You can also select the **All Hosts** option.
  - d) Click **Allocate Storage Pools**.
  - e) Select the pool on which you want to create the LUN.
2. Right-click the cluster that will use the new LUN and select **Properties**.
3. Select **Shared Volumes**, and then click the **Add** button.
4. Click **Create Logical Unit**.
5. Enter the details for the LUN:
  - Pool on which the LUN will be created
  - Name of the new LUN
  - Optionally, a description
  - Size of the LUN

- Select whether the LUN is thin provisioned or thick provisioned
6. Click **OK**.
7. Define the properties of the new volume:

- Select the partition type
- Enter a volume label
- Select quick or full format
- Select to force the format

At this point, nothing has been created or formatted. Click **OK** when you are ready to start the creation, mapping, and formatting process.

8. Click **OK**.



**Tip:** After you click **OK**, you can switch to the **Jobs** section in SCVMM and monitor the progress of the process.

9. In the **Fabric** section of SCVMM, right-click the host that you want to use as the SCVMM library and select **Properties**.

10. Click **Storage**.

11. Click **Add** in the **Storage** page.

12. Click **Add Disk** in the **Add** menu.

13. Click **Create Logical Unit**.

14. Enter the following:

- Name
- Size
- Select **Create thin storage logical unit with capacity committed on demand** if you require thin provisioning, or **Create a fixed size storage logical unit with capacity fully committed** if you require a thick LUN.

15. Click **OK**.

You now have a new LUN that is being shared from the selected host. The next step is to configure the LUN as a volume.

16. Select the desired classification.

17. Format the new disk by selecting or entering the following values:

- Partition style
- Volume label
- Allocation unit style
- **Quick format** if you want to perform a quick format on the new disk
- **Force format even if a filesystem is found** if you want to format the disk even it has a filesystem

- Mount point

18. Click **OK**.

In the **Data** page of the IntelliFlash Web UI, a new LUN is created based on the SMI-S settings you provided. If you did not specify a project, and the pool does not have a default project, a new project is created. The LUN is also mounted on the hosts that you specified. If you are using a Microsoft Failover Cluster, you can verify the cluster shared volume from the Failover Cluster Manager.

**Related Topics:**

- SMI-S Default Names
- Default Settings of LUNs Created using SMI-S

## Viewing LUNs

To view LUNs, complete the following steps in SCVMM:

1. Click **Fabric**.
2. In the **Storage** navigation menu, select **Classifications and Pools**.  
All the LUNs that were created from SCVMM appear under their respective storage classifications and pools. Mapped LUNs show as assigned. Unmapped LUNs show **No** in the **Assigned** column.

## Unmapping a LUN

To unmap a LUN without deleting it, complete the following steps in SCVMM:

1. Expand the host group to which the LUN was mapped.
2. Find the LUN in either **Shared Volumes** or **Available Storage**.
3. Right-click and select **Remove**.  
The LUN is no longer assigned under **Classifications and Pools** in SCVMM, and the LUN mapping is removed in the IntelliFlash Web UI also.

By performing this procedure, you only remove the LUN mapping for this host or cluster. To delete the LUN, see [Deleting LUNs with SCVMM](#).

## Deleting LUNs with SCVMM



**Warning:** By deleting a LUN in SCVMM, you also delete the LUN in the IntelliFlash system. The Delete operation is not reversible.



**Important:** You cannot delete a LUN that is **Assigned**.

To delete a LUN, complete the following steps in SCVMM:

1. View the LUN, as described in [Viewing LUNs](#).
2. Right-click the LUN.
3. Click **Remove** in the shortcut menu.

## Working with IntelliFlash Clones in SCVMM

Cloning in SCVMM is not the same as cloning in IntelliFlash. There are underlying conceptual differences between cloning in SCVMM and cloning in IntelliFlash. Moreover, the verbiage and nomenclature of SCVMM does not align with IntelliFlash—some terms are used differently in the two products. Therefore, use the IntelliFlash Web UI to clone LUNs.

### Deleting Clones with SCVMM

If you have not mapped the clones, you can delete them. If you have already attempted to map the clones, and the mapping partially succeeded, you might not be able to remove the clones very easily.



**Warning:** Deleting a clone in SCVMM also deletes the clone from the IntelliFlash system. It additionally deletes the IntelliFlash snapshot created during the clone-creation process. As there is no facility in SCVMM or the IntelliFlash system for undeleting a clone or a snapshot, this could lead to data loss if you are not careful.

To delete a clone, complete the following steps in SCVMM:

1. Right-click the clone.
2. Select **Remove** from the menu.

## Creating an SCVMM Library Share

### Prerequisites

Before you begin, make sure that you have a shared folder or volume on a host that is managed by SCVMM.

To add an SCVMM library, complete the following steps in SCVMM:

1. Click **Library** in the left navigation pane.
2. Right-click the host under **Library Servers** and click **Add Library Shares**.  
The **Add Library Shares** wizard appears.
3. Select the library share you have created and click **Next**.
4. Click **Add Library Shares**.  
The volume now appears under the **Library** section in SCVMM.

## Creating a VM

To create a VM, you must first create a LUN for the VM as described in [Creating and Mapping a LUN as a Shared Volume](#). After creating the LUN, you have to deploy the VM by completing the following steps in SCVMM:

1. Click **VMs and Services** in the left navigation pane.
2. Right-click the host on which you want to create the VM and select **Create Virtual Machine**.  
The **Create Virtual Machine Wizard** appears.
3. Select **Create the new virtual machine with a blank virtual hard disk** and click **Next**.
4. Enter a name for the virtual machine and select **Generation 2**.
5. Click **Next**.  
The **Configure Hardware** page appears.
6. Modify the hardware configuration as desired and click **Next**.  
The **Select Destination** page appears.
7. Select the host group as the destination under **Place the virtual machine on a host** and click **Next**.  
The **Select Host** page appears.
8. Select the host you want to use and click **Next**.  
The **Configure Settings** page appears.
9. In the **Locations** tab, change the **Virtual machine path** to the LUN that has been formatted as a volume on the host.
10. Click **Virtual Hard Disk** under **Machine Resources** and change the **Destination path** to same LUN used in the previous step.
11. Click **Next**.  
The **Select Networks** page appears.
12. Customize the network settings as desired and click **Next**.  
The **Add Properties** page appears.
13. Select the desired **Automatic actions** and **Operating system**.
14. Click **Next**.  
The **Summary** page appears.
15. Review the summary and click **Create**.

## Converting a VM to a Template

To convert a virtual machine to a template, complete the following steps in SCVMM:

1. In the **VMs and Services** section in SCVMM, select the host on which you had created the VM.
2. From the list of VMs on the host, right-click the VM you want to convert and click **Create > Create VM Template**.
3. Click **Yes** to confirm.
4. Enter a **VM Template name** and click **Next**.  
The **Configure Hardware** page appears.
5. Modify the default hardware configuration as desired and click **Next**.  
The **Configure Operating System** page appears.
6. Select an existing guest OS profile or create a new one, and click **Next**.  
The **Select Library Server** page appears.
7. Select the Library Server with the type SAN and click **Next**.  
The **Select Path** page appears.
8. Click **Browse...** and select a destination folder.
9. Click **Next**.  
The **Summary** page appears.
10. Click **Create**.

You can verify that the template is created, by clicking **Library > Templates > VM Templates**.

## Deploying a VM Template Using SAN Copy

When you deploy a VM template using SAN copy, the source volume is cloned, mapped, and a corresponding mount point is created where you define the target. Therefore, you do not need an additional LUN for VMs deployed from this template.

- Once the environment is set up, deploying VMs with SAN copy takes minutes regardless of the VM size. The process by which the VM is deployed is as follows:
  - SAN copy creates an IntelliFlash snapshot.
  - A clone of the snapshot is then created.
  - The clone is then presented to the Hyper-V host.
  - The Hyper-V host mounts the volume as a mount point in the target directory that you specified during VM creation.

- Snapshots created with SAN copy are not application consistent. Because SAN-copy snapshots are taken on a VM template, which are not run, application consistency is not a concern.

## Prerequisites

- A VM template created on a SAN LUN.
- A target LUN on which the new VM will be created.

1. Click **Library > Templates > VM Templates**.
2. Right-click on the template that you want to deploy and select **Create Virtual Machine**.  
The **Create Virtual Machine Wizard** appears.
3. Enter a name for the VM and click **Next**.  
The **Configure Hardware** page appears.
4. Modify the hardware configuration as desired and click **Next**.  
The **Select Destination** page appears.
5. Select the host group as the destination under **Place the virtual machine on a host** and click **Next**.  
The **Select Host** page appears.
6. Select the host you want to use and click **Next**.  
The **Configure Settings** page appears.
7. In the **Locations** tab, for the **Virtual machine path** select the folder in which you want to create the VM.
8. Click **Next**.  
The **Select Networks** page appears.
9. Customize the network settings as desired and click **Next**.  
The **Add Properties** page appears.
10. Select the desired **Automatic actions** and **Performance and Resource Optimizations** options.
11. Click **Next**.  
The **Summary** page appears.
12. Review the summary and click **Create**.

This creates an IntelliFlash system snapshot and a clone of the snapshot. The VM name is appended to the clone name. The clone is mapped to the host that hosted the original VM from which the template was created. The mount point of the new VM is based on the VM name.

In SCVMM, you can observe the following:

- A new VM in the **VMs and Services** section. When you open the properties of the new VM, you will see a dependency on the volume that holds the template.
- A clone created for the VM in the **Fabric** section.

## Hyper-V Host-to-Host VM Migration with SCVMM and SMI-S

- SMI-S support enables the “SAN transfer” or SAN copy method of VM migration between hosts.
- Both the source and destination host must have FC or iSCSI access to the IntelliFlash system that contains the VM.

### Using SAN Transfer for VM Migration between Hosts

The process of migrating a VM from one host to another using the SAN transfer method is as follows:

- If the VM is online, the current running state is saved and the VM is paused.
- SMI-S adjusts the LUN access from the source host to the destination host.
- A mount point is created in the directory specified as the target path on the target host.
- The mount point is a logical pointer to the LUN.
- After LUN access is switched, if the VM had been running, it is returned to its previously saved state.
- If the VM is running Windows, it will not crash but the operating system might seem suspended during migration.
- If the VM is running a different OS, check with Microsoft Support whether the OS is supported.

### Considerations for migrating VMs with SAN Transfer

- If a VM shares a LUN with any other VM, you cannot use SAN transfer.
- For each LUN per VM, the migration time is around four minutes.
- With small VMs, it is better to disable SAN transfer and use network transfer instead. However, you should consider network performance and host resource availability before you select the network transfer method.
- Migration is performed serially for each LUN, so VMs with multiple LUNs attached take roughly four minutes per LUN.
- SAN transfer can be used for VMs that have multiple VHDx files in multiple LUNs.

### Migrating VMs between None-Clustered Hyper-V hosts

1. In SCVMM, click the **VMs and Services** workspace.
2. In **All Hosts** folder, select the host that contains the VM you want to migrate.
3. Right-click the VM you want to migrate, and select **Migrate Virtual Machine**.

If the source host can leverage SMI-S to migrate a VM to another host, you will see the Transfer Type "SAN" available.

4. In the **Select Host** screen, select the target Hyper-V host and click **Next**. A dialog box prompts you to specify the target location on the target Hyper-V host. This location need not be a location on the SAN, because as explained earlier, the LUN is mounted as a mount point in whatever directory you define.
5. Review and click **Move**. After you click **Move**, the VM is moved to a suspended state. The applications in the VM do not crash, but they are paused until the migration is complete. You can monitor the migration from the **Jobs** section in SCVMM. The migration uses "SAN Transfer." After the migration is complete, the VM state moves from Suspended to Running.

## SMI-S Support for SMB 3.0 Shares

IntelliFlash supports SMI-S with SMB 3.0 share protocols. You can use SMI-S management software such as Microsoft's System Center Virtual Machine Manager (SCVMM) to add and manage SMB 3.0 shares available in an IntelliFlash array. You can also use SCVMM to rapidly provision Hyper-V VMs on an SMB 3.0 share.



**Important:** Make sure that the shares created by SCVMM through SMI-S in **Virtualization File Services** mode do not have the non-blocking mandatory locks (NBMAND) set. By default, NBMAND is disabled for SMB shares created through SCVMM. If you enable NBMAND on these shares, you might not be able to access the shares through SCVMM.

### Adding SMB 3.0 Shares in SCVMM

To add the IntelliFlash array and the SMB 3.0 shares present in the array, complete the following steps :

1. In SCVMM, click the **Fabric** workspace.
2. Click **Add Resources** in the **Home** tab of the SCVMM ribbon.
3. Click **Storage Devices** in the **Add Resources** menu.  
The **Add Storage Devices Wizard** appears.
4. Select **SAN and NAS devices discovered and managed by a SMI-S provider** and click **Next**.
5. Enter the IP address or the FQDN of the of the SMI-S server container in the **Provider IP address or FQDN** field.
6. Select the **Use Secure Sockets Layer (SSL) connection** option.
7. Create a **Run As account** by completing the following steps:
  - a) Click **Browse**.  
The **Select a Run As Account** dialog box appears.

- b) Click **Create Run As Account**.  
The **Create Run As Account** dialog box appears.
  - c) Enter the following details in the **Create Run As Account** dialog box:
    - **Name:** Enter a name that helps you identify the Run As account. For example, a name that includes the array name.
    - **User name:** Enter the web administrator user name for the IntelliFlash system.
    - **Password:** Enter the password for the web administrator account.
    - Select **Validate domain credentials**.
-  **Note:** SCVMM prefers domain authenticated users. So provide a domain authenticated user. In the IntelliFlash Web UI, the domain is configured in **Services > NAS > Identity Management**.
- Click **OK**.
  - d) Select the newly created **Run As account** in the **Select a Run As Account** dialog box.
  - e) Click **OK**.
8. In the **Add Storage Devices** wizard, click **Next**.  
The **Import Certificate** dialog box appears.
  9. Click **Import** to import the SSL certificate of the array.  
If you had previously imported a controller-specific SSL certificate you need to remove it and import the new array-specific SSL certificate.
  10. When the SSL import and inventory is complete, the array details appear. Click **Next**.  
The **Select Storage Devices** page displays the SMB 3.0 shares and pools discovered on the array. You must associate each pool with a storage classification, and optionally a default host group.
  11. To create a new **Storage Classification** and associate it with a pool, complete the following steps:
    - a) Select the pool.
    - b) Click **Create Classification**.
    - c) Enter a name, and optionally, a description.
    - d) Click **Add**.
    - e) Click the dropdown in the **Classification** column and select the new classification.
    - f) Click the dropdown in the **Host Group** column and select the desired host group.
    - g) Click **Next**.
  12. Review the summary, and click **Finish**.  
When you click **Finish**, the Storage Provider addition job window appears.
- After the job is complete, click
- **Storage > File Servers** to verify the SMB 3.0 shares.

- **Storage > Classifications and Pools** to verify the pools and their associated storage classifications.
- **Storage > Providers** to verify the listed SMI-S providers.
- **Storage > Arrays** to verify the arrays.

## Adding SMB 3.0 Shares to the SCVMM Library

To add an SMB 3.0 share to the SCVMM library, complete the following steps in SCVMM:

1. In SCVMM, click the **Library** workspace.
2. Expand the **Library Servers** node.
3. Right-click the library server to which you want to add the share and click **Add Library Shares**.  
The **Add Library Shares** wizard appears.
4. For shares managed by SCVMM, select the discovered SMB 3.0 share and click **Next**.
5. For unmanaged shares, click **Add Unmanaged Shares** and enter the UNC path of the share, and click **Next**.
6. Click **Add Library Shares**.  
The SMB 3.0 share now appears under the **Library** section in SCVMM.

## Adding SMB 3.0 Share to a Hyper-V Host

You can add an SMB 3.0 share to a Hyper-V host managed by Microsoft System Center Virtual Machine Manager (SCVMM). To add an SMB 3.0 share, complete the following steps:

1. In SCVMM, click the **VMs and Services** workspace.
2. In the **Servers > All Hosts** folder on the left pane, right-click the Hyper-V host to which you want to add the SMB 3.0 share, and select **Properties**.
3. In the **Properties** dialog box, select **Storage**, and then click **Add > Add File Share**.
4. In the **File Share Path** field, type the UNC path of the unmanaged SMB 3.0 share. If the SMB 3.0 share is managed by SCVMM, select the share from the dropdown list.
5. Click **OK**.

## Adding a Virtual Hard Disk to SCVMM Library

You can add a blank virtual hard disk to the SCVMM library by using the Explorer or Import option.

## **Adding a Virtual Hard Disk to SCVMM Library Using the Import Option**

To add a virtual hard disk to the SCVMM library using the Import option, complete the following steps in SCVMM:

1. In SCVMM, click the **Library** workspace.
2. From the **Library Servers** list, select the library server.
3. In the Home tab, click **Import Physical Resource**.

The **Import Library Resource** wizard appears.

4. Click **Add Resource**.
5. In the **Add Resource** screen, select the virtual hard disk and click **OK**.
6. In the **Import Library Resource** wizard, click **Browse** and select the required library server.
7. Click **Import**.

## **Adding a Virtual Hard Disk to SCVMM Library Using the Explorer Option**

To add a virtual hard disk to the SCVMM library using the Explorer option, complete the following steps in SCVMM:

1. In SCVMM, click the **Library** workspace.
2. From the **Library Servers** list, select the library server.
3. Right-click the library server and select the **Explorer** option.

A new Explorer appears with the library server and share location.

4. Drag and drop the virtual hard disk file in the Explorer.

## **Creating a VM from a Blank Virtual Hard Disk**

After adding SMB 3.0 share to the Hyper-V host, you can fast provision a VM on the SMB 3.0 share, using a virtual hard disk.

To create a VM from a virtual hard disk, you must have added the virtual hard disk to the library. See [\*Adding a Virtual Hard Disk to SCVMM Library\*](#) for more information.

1. Select **VMs and Services**.
2. Right-click the host on which you want to create the VM and select **Create Virtual Machine**. The **Create Virtual Machine Wizard** appears.
3. In the **Select Source** screen, **Create a new virtual machine with a blank virtual hard disk** to create a VM from a blank virtual hard disk.
4. Click **Next**.

The **Identity** screen appears.

5. Enter a name for the virtual machine, select **Generation 2** and click **Next**.  
The **Configure Hardware** screen appears.

6. Add the hardware configuration and click **Next**.  
The **Select Destination** screen appears.

7. Select the host group as the destination under **Place the virtual machine on a host** and click **Next**.  
The **Select Host** screen appears.

8. Select the host you want to use and click **Next**.

The **Details > Deployment and Transfer Explanation** section in the **Select Host** screen displays the information that the host is available for SAN migration (fast copy, also known as ODX).

The **Configure Settings** screen appears.

9. In the **Locations** tab, change the **Virtual machine path** to the SMB 3.0 share that has been added to the host.

10. Click **Virtual Hard Disk** under **Machine Resources** and change the **Destination path** to the same SMB 3.0 share used in the previous step.

11. Click **Next**.

The **Select Networks** page appears.

12. Customize the network settings as desired and click **Next**.

The **Add Properties** page appears.

13. Select the desired **Automatic actions** and **Operating system**.

14. Click **Next**.

The **Summary** page appears.

15. Review the summary and click **Create**.

## Creating a VM using Existing VM, VM Template, or Virtual Hard Disk File

After adding SMB 3.0 share to the Hyper-V host, you can fast provision a VM on the SMB 3.0 share, using an existing VM, a VM template, or a virtual hard disk file.

If you use a VM template, you can customize both the hardware and operating system settings. If you use an existing virtual machine, you can only customize the hardware settings.

1. Select **VMs and Services**.

2. Right-click the host on which you want to create the VM and select **Create Virtual Machine**.

The **Create Virtual Machine Wizard** appears.

3. In the **Select Source** screen, select **Use an existing virtual machine, VM template, or virtual hard disk** to create a VM from an existing VM, VM template, or virtual hard disk.

4. Click **Browse** and select the source virtual machine, virtual hard disk file, or the VM template.

5. **Next.**

The **Identity** screen appears.

6. Enter a name for the virtual machine, select **Generation 2** and click **Next**.

The **Configure Hardware** screen appears.

7. Modify the hardware configuration as desired and click **Next**.

The **Select Destination** screen appears.

8. Select the host group as the destination under **Place the virtual machine on a host** and click **Next**.

The **Select Host** screen appears.

9. Select the host you want to use and click **Next**.

The **Details > Deployment and Transfer Explanation** section in the **Select Host** screen displays the information that the host is available for SAN migration (fast copy, also known as ODX).

The **Configure Settings** screen appears.

10. In the **Locations** tab, change the **Virtual machine path** to the SMB 3.0 share that has been added to the host.

11. Click **Virtual Hard Disk** under **Machine Resources** and change the **Destination path** to the same SMB 3.0 share used in the previous step.

12. Click **Next**.

The **Select Networks** page appears.

13. Customize the network settings as desired and click **Next**.

The **Add Properties** page appears.

14. Select the desired **Automatic actions** and **Operating system**.

15. Click **Next**.

The **Summary** page appears.

16. Review the summary and click **Create**.

## Converting a VM to a Template

To convert a virtual machine to a template, complete the following steps in SCVMM:

1. In SCVMM, click the **VMs and Services** workspace.
2. Expand **All Hosts** and select the Hyper-V host on which you had created the VM.
3. From the list of VMs on the host, select the VM you want to convert.
4. Right-click the VM you want to migrate and click **Create > Create VM Template**.
5. In the **Confirmation** dialog box, click **Yes**.
6. Enter a **VM Template name** and click **Next**.  
The **Configure Hardware** page appears.
7. Modify the default hardware configuration as desired and click **Next**.  
The **Configure Operating System** page appears.
8. Select an existing guest OS profile or create a new one, and click **Next**.  
The **Select Library Server** page appears.
9. Select the library server that contains the SMB 3.0 shares and click **Next**.  
The **Select Path** page appears.
10. Click **Browse** and select a destination folder.
11. Click **Next**.  
The **Summary** page appears.
12. Click **Create**.

You can verify that the template is created, by clicking **Library > Templates > VM Templates**.

## Migrating VMs between Hyper-V Hosts

1. In SCVMM, click the **VMs and Services** workspace.
2. In **All Hosts** folder, select the host that contains the VM you want to migrate.
3. Right-click the VM you want to migrate, and select **Migrate Virtual Machine**.  
The **Select Host** screen appears.
4. In the Select Host screen, select the target Hyper-V host and click **Next**.
5. In the Summary page, review the settings and click **Move**.

After you click **Move**, the VM is moved to a suspended state. The applications in the VM do not crash, but they are paused until the migration is complete. You can monitor the migration from the **Jobs** section in SCVMM. After the migration is complete, the VM state moves from Suspended to Running.



---

# Chapter 28

---

## IntelliFlash Manager Plugin

---

**Topics:**

- *About IntelliFlash Manager plugin*
- *IntelliFlash Manager plugin backward compatibility support*
- *Managing the VMware vCenter Server*
- *Using the IntelliFlash Manager plugin*
- *Host settings*
- *Datastores management*
- *Snapshots and Clones management*
- *Virtual machines management*
- *Role-based access control in the IntelliFlash Manager plugin*

## About IntelliFlash Manager plugin

---

The IntelliFlash Manager plugin is an HTML5-based plugin to manage IntelliFlash systems in VMware vCenter environments. You can install the IntelliFlash Manager plugin on a VMware vCenter Server. The installed plugin on the VMware vCenter server allows you to manage multiple IntelliFlash systems.

### Linked Mode

You can install the IntelliFlash Manager plugin in the vCenter Server environments with Enhanced Linked Mode and Embedded Linked Mode.

### Manage datastores, VMs, snapshots, and clones

The plugin enables you to create and manage NAS and SAN datastores for virtual machines, and also view analytics for datastores and virtual machines. To protect your datastores and VMs, the plugin enables you to create manual snapshots and clone them.

### Hyperclone

The **Hyperclone** feature in the plugin allows you to quickly create multiple clones of your virtual machines. It also provides the option to roll back the datastore or virtual machine to a point-in-time state when the snapshots are taken.

The **Hyperclone** feature also allows you to power on all virtual machines or power on a group of five virtual machines at a time when cloning the virtual machines. You can also create clones of the virtual machines in the powered off state.

### Install IntelliFlash NAS VAAI Plugin

You can install and uninstall the IntelliFlash NAS VAAI Plugin and apply ESXi host settings using the IntelliFlash Manager plugin.

### Role-based access control

The IntelliFlash Manager plugin provides role-based access control to manage access to vCenter Servers. It provides sample roles that you can use to customize a role and assign it to vCenter Users (vSphere Users).

### Host settings

The IntelliFlash Manager plugin enables you to manage host settings. You can update multipathing rules and various recommended settings for the hosts. The **Host settings** page lists the ESXi host name, version number, and status of the host.

### Related Topics

[IntelliFlash Manager plugin support for Linked vCenter Servers](#)

[Managing VMware vCenter Server](#)

[Supported vCenter Server versions](#)

[Using IntelliFlash Manager](#)

[Host Settings](#)

[Datastore Management](#)

[\*Snapshots and Clones management\*](#)

[\*Virtual machines management\*](#)

[\*Role based access control in IntelliFlash Manager plugin\*](#)

## IntelliFlash Manager plugin support for Linked vCenter Servers

You can install the IntelliFlash Manager plugin in the vCenter Server environments with Enhanced Linked Mode and Embedded Linked Mode.

After installing the plugin on any one of the vCenter Servers in the Enhanced Linked Mode and Embedded Linked Mode vCenter environments, the plugin is automatically connected to the other vCenter Servers on the array. As a best practice, you need to install and register the IntelliFlash Manager plugin on each vCenter Server.

You can perform all IntelliFlash Manager plugin supported tasks on linked vCenters Servers. The IntelliFlash Manager plugin interface displays the details of virtual machines and datastores on linked vCenter Servers.

After installing the plugin, the **VMware Servers** page in the IntelliFlash Web UI displays all linked VMware vCenter Servers.

### Related Topics

[\*Adding a NAS datastore using IntelliFlash Manager plugin\*](#)

[\*Adding a SAN datastore using IntelliFlash Manager plugin\*](#)

## Supported VMware vCenter Server versions for the IntelliFlash Manager plugin

You can install the IntelliFlash Manager plugin on the following VMware vSphere versions:

- VMware vCenter Server 7.0 for local VCP
- VMware vCenter Server 8.0 for remote VCP

Refer to the [\*VMware documentation\*](#) to view the ESX versions supported.



**Note:** You can use the IntelliFlash Manager plugin in both Flex and HTML versions of the VMware vSphere Client. However, you might not be able to use the context menu options in the Flex version.

### Related Topics

[\*Using the IntelliFlash Manager\*](#)

## IntelliFlash Manager plugin backward compatibility support

You can now use the IntelliFlash Manager plugin to manage IntelliFlash systems from IntelliFlash versions 3.10.1.0, 3.10.0.0, 3.9.1.x, and 3.7.1.x.



**Note:** After upgrading to IntelliFlash 3.10.1.0, you must install the IntelliFlash Manager plugin from the IntelliFlash Web UI (**Settings > App-Aware > VMware Servers > Plugin Management > Install**) to take advantage of the backward compatibility support.

In a setup where you have multiple IntelliFlash systems running on different IntelliFlash versions, then the IntelliFlash Manager plugin works with IntelliFlash 3.10.1.0, 3.10.0.0, 3.9.1.x, and 3.7.1.x.

However, there are a few limitations when managing IntelliFlash systems prior to IntelliFlash version 3.10.0.0:

- You should not manage or perform operations on an IntelliFlash Array using the IntelliFlash Manager plugin if the IntelliFlash Array is going through an upgrade.
- When cloning a snapshot of a datastore using the IntelliFlash Manager plugin, if you select the **Enable read-only** option, you cannot mount the cloned datastore.
- When creating a datastore using the IntelliFlash Manager plugin, the **Alarm** feature may not work properly.

## Managing the VMware vCenter Server

---

VMware vCenter Server is a data center management server application developed by VMware Inc. to monitor virtualized environments.

vCenter Server provides centralized management and operation, resource provisioning and performance evaluation of virtual machines residing in a distributed virtual data center. VMware vCentre Server is designed primarily for vSphere, VMware's platform for building virtualized cloud infrastructures.

Once you add the vCenter Server from the IntelliFlash Web UI, you will be able to manage arrays through the IntelliFlash Manager plugin. You can also monitor VM analytics from the IntelliFlash Web UI.

### Related Topics

[Adding a vCenter Server](#)

[Installing IntelliFlash Manager plugin on a vCenter Server](#)

[Registering a new IntelliFlash System](#)

### VMware Servers Page

You can add VMware servers and manage settings for the IntelliFlash Web UI by accessing **Settings > App-Aware Settings > VMware Servers**.

The following table lists the components of the **VMware Servers** page in the IntelliFlash Web UI.

**Table 16: Components of the VMware Servers page**

Component	Description
Hostname	Displays the name or IP address of a VMware Server (vCenter, ESXi).
vSphere Version	Displays the version of the vSphere.

Component	Description
Quiesce Enabled	Displays whether the quiesce option is enabled or disabled. The possible values are <b>true</b> or <b>false</b> . When the field value is <b>true</b> , the plugin is enabled for quiesced snapshots for the vCenter. You can still choose to manually take a quiesced snapshot with the plugin. But if it is disabled, no snapshots can be quiesced.
Plugin	Displays whether or not the plugin is installed with the vCenter Server. After installation, the field displays <b>Yes</b> and also displays the plugin management IP address or IntelliFlash Array IP address.
Connection	Displays the connection status between the IntelliFlash Manager plugin and the IntelliFlash Array for the credentials provided. The possible values are <b>Good</b> or <b>Cannot connect</b> .
Array	Displays whether or not the array is registered.
<b>Add</b>	Allows you to add a VMware Server (vCenter, ESXi) to the IntelliFlash Array.
<b>Edit</b>	Allows you to edit the VMware Server details.
<b>More</b>	<p>The <b>More</b> dropdown provides the following functions:</p> <ul style="list-style-type: none"> <li>• <b>Refresh</b> - Refreshes the connection and updates the connection status.</li> <li>• <b>ESXi Settings/VAAI</b> - Allows you to manage the IntelliFlash NAS VAAI Plugin and configure VMware ESXi Servers.</li> </ul>
<b>Plugin management</b>	<p>Allows you install and manage the IntelliFlash Manager plugin:</p> <ul style="list-style-type: none"> <li>• <b>Install</b> or <b>Upgrade</b> IntelliFlash Manager plugin</li> <li>• <b>Uninstall</b> IntelliFlash Manager plugin</li> </ul>

## Adding a vCenter Server

### Prerequisites

Check whether the IntelliFlash Manager plugin is already installed on the vCenter Server that you want to add to the IntelliFlash Array. If the IntelliFlash Manager plugin is installed, continue with registering your array from the IntelliFlash Manager plugin. If not, add the VMware vCenter to the IntelliFlash Array.

Once you add the vCenter Server, you can manage the arrays through the IntelliFlash Manager plugin and monitor VM analytics from the IntelliFlash Web UI.

 **Note:** The IntelliFlash Manager plugin user must have VMware vCenter admin privileges to perform any action related to vCenter Server and to use the plugin.

To add a vCenter Server, complete the following steps:

1. From the IntelliFlash Web UI, go to **Settings > App-Aware > VMware Servers**.
2. Click **Add**.
3. In the **vCenter/ESXi Host Details** window, enter the following details:
  - a) In the **Host Name/IP Address** field, type the host name or IP address.
  - b) Type the vCenter Server **User name**.
  - c) Type the vCenter Server **Password**.

 **Note:** *In the case of a network issue*, the array status may show as unregistered. An error message appears with Resolve now link. Click **Resolve now** to resolve the issue.

4. (Optional) Select the **Enable Quiesce** option.

 **Note:** The **Enable Quiesce** option allows IntelliFlash to take quiesced snapshots for all of the datastores, provided the quiesce option is also enabled at the project level.

5. Click **Test**.

Once the verification test is successful, the **ADD** button becomes active.

 **Note:** The **Test** function checks whether the provided host name or IP address, user name and password are correct for the VMware Server, as well as the connection with the server. If the test fails, verify the host name or IP address and provide the correct details.

6. Click **ADD**.
7. Click **Refresh** to check the plugin connection status.

## Related Topics

[Installing the IntelliFlash Manager plugin on a vCenter Server](#)

## Editing vCenter Server details

You can edit the **vCenter/ESXi Host details** on the IntelliFlash Web UI.

 **Note:** The IntelliFlash Manager plugin user must have VMware vCenter admin privileges to perform any action related to vCenter Server.

To modify vCenter server details, complete the following steps:

1. From the IntelliFlash Web UI, go to **Settings > App-Aware > VMware Servers**.
2. Select the **vCenter Server or ESXi Host** that you want to edit.
3. Click **EDIT**.
4. In the **vCenter/ESXi Host Details** window, enter the following details:
  - a) In the **Host Name/IP Address** field, type the host name or IP address.
  - b) Type the vCenter Server **Password**.
  - c) (Optional) Select the **Enable Quiesce** option.



**Note:** The Enable Quiesce option allows IntelliFlash to take quiesced snapshots for all of the datastores, provided the quiesce option is also enabled at the project level.

5. Click **TEST**.

Once the verification test is successful, the **ADD** button becomes active.



**Note:** The **Test** function checks whether the provided host name or IP address, user name and password are correct for the VMware Server, and the connection with the server. If the test fails, verify the host name or IP address and provide the correct details.

6. Click **ADD**.
7. Click **Refresh** to check the plugin connection status.

## Refreshing the VMware Servers page

After adding or modifying the vCenter Server or VMware Server details, use the **REFRESH** option on the **VMware Servers** page to check the plugin connection status.

To refresh the **VMware Servers** page, complete the following steps:

1. From the IntelliFlash Web UI, click **Settings > App-Aware > VMware Servers**.
2. Click the **vCenter Server** to select it.
3. In the **VMware Servers** page, click **More > Refresh** for the required registered vCenter Server.
4. You can also click the **REFRESH** button on the VMware Servers page.

## Removing a vCenter Server from the VMware Servers page

You can delete a vCenter Server anytime.

To remove a vCenter Server from the VMware Server, complete the following steps:

1. From the IntelliFlash Web UI, click **Settings > App-Aware > VMware Servers**.
2. Click an existing **vCenter Server** to be removed.
3. In the **VMware Servers** page, click **DELETE**.



**Note:** Removing vCenter Server breaks the communication between the array and vCenter Server. Once you remove the vCenter Server, you will not be able to manage the arrays through the IntelliFlash Manager plugin and you cannot monitor VM analytics from the IntelliFlash Web UI.

## Installing the IntelliFlash Manager plugin on a vCenter Server

To install the IntelliFlash Manager plugin on vCenter server, complete the following steps:

1. From the IntelliFlash Web UI, go to **Settings > App-Aware > VMware Servers**.
2. Click **Plugin Management > Install**. The **Install Plugin** window appears.
3. In the **Install Plugin** window, complete the following steps:
  - a) Select the **vCenter** from the list of already added vCenters or select the option **New Host** on which you want to install the IntelliFlash Manager plugin.
  - b) Type the **Host Name/IP Address**.
  - c) Type the **User name**.
  - d) Type the **Password**.
  - e) Click **Install**.
  - f) A confirmation message appears. Click **YES**.



**Note:** The installation may take some time to complete.

4. Log in to **vSphere Client**.
5. Restart the vSphere-ui and vSphere-client services for the changes to take effect.  
Reference steps <https://kb.vmware.com/s/article/2109887>
6. Log out from the **vSphere Client** and log in again.
7. The **Finish installation** message appears. This step is mandatory.
  - a) Type the vCenter **User name**.
  - b) Type the vCenter **Password**.
  - c) Click **Continue**.

The IntelliFlash Manager plugin installation is now complete.

## Related Topics

## *Using IntelliFlash Manager*

### Upgrading the IntelliFlash Manager plugin

Starting from IntelliFlash version 3.7.1.2, you have the option to upgrade the Tegile vCenter plugin version 1.0 to IntelliFlash Manager plugin version 2.0 or later. If a new version of the IntelliFlash Manager plugin is available, the **Upgrade** button is enabled.

To upgrade to the latest version of the IntelliFlash Manager plugin, complete the following steps:

1. From the IntelliFlash Web UI, go to **Settings > App-Aware > VMware Servers**.
2. Click **Plugin Management > Upgrade**. The **Upgrade Plugin** window appears.
3. Select the latest version of the IntelliFlash Manager plugin available for upgrade.
4. Click **UPGRADE**.
5. Restart the vSphere-ui and vSphere-client services for the changes to take effect.

Reference steps <https://kb.vmware.com/s/article/2109887>



**Note:** When you upgrade the plugin, you need to re-register the array on the plugin.

### Uninstalling the IntelliFlash Manager plugin on a vCenter Server

You can uninstall the IntelliFlash Manager plugin from the vCenter Server anytime. Once you uninstall the IntelliFlash Manager plugin, all the arrays go into monitoring mode. You will not be able to manage arrays from the vCenter Server.

To uninstall the IntelliFlash Manager plugin, complete the following steps:

1. From the IntelliFlash Web UI, go to **Settings > App-Aware > VMware Servers**.
2. Click **Plugin Management > Uninstall**. The **Uninstall Plugin** window appears.
3. After reading the confirmation message, type **I understand** in the text box displayed.
4. Click **Uninstall**.
5. Restart the vSphere-ui and vSphere-client services for the changes to take effect.

Reference steps <https://kb.vmware.com/s/article/2109887>



**Note:** Uninstalling the IntelliFlash Manager plugin affects all arrays. You need to unregister all the arrays in IntelliFlash Manager plugin and then register again.

### Resolving network Issue

The connection between the IntelliFlash Array and the vCenter Server can fail in the case of network issues. If there is a connection failure, the connection status of the vCenter Server

shows **Cannot connect**. An error message will display: **There is a problem connecting to vCenter Server. Resolve now.**

To resolve the network issue and connect to the vCenter Server, complete the following steps:

1. Click **Resolve now** in the error message that is displayed.
2. In the **vCenter/ESXi Host Details** window, enter the following details:
  - a) In the **Host Name/IP Address** field, type the host name or IP address.
  - b) Type the vCenter Server **User name**.
  - c) Type the vCenter Server **Password**.
3. Click **Test**.  
Once the verification test is successful, the **ADD** button becomes active.
4. Click **ADD**.
5. Click **Refresh** to check the plugin connection status.

## Accessing the ESXi host settings from the IntelliFlash Web UI

The **ESXi Settings/VAAI** page displays all the ESXi hosts that are connected to the vCenter Server. Through the IntelliFlash Web UI, you can install and manage the VAAI plugin on the hosts and update the recommended settings.

To access ESXi hosts from the IntelliFlash Web UI, complete the following steps:

1. From the IntelliFlash Web UI, go to **Settings > App-Aware > VMware Servers**.
2. Click **More**, and then select **ESXi Settings/VAAI**.

### ESXi settings for the host

To configure settings for ESXi hosts from the IntelliFlash Web UI, complete the following steps:

1. From the IntelliFlash Web UI, go to **Settings > App-Aware > VMware Servers**.
2. Click **More**, and then select **ESXi Settings/VAAI**.
3. Select the host for which you want to update the settings, and then click **Configuration**.
4. Under **Settings** enter values for the following parameters:
  - Max Queue Depth
  - Delete RPC Timeout
  - Heartbeat Frequency
  - Disk Schedule Request
5. Click **Save**.



**Note:** The newly applied settings take effect after you reboot the host.

### Installing or upgrading the IntelliFlash NAS VAAI Plugin

You can install or upgrade the VAAI plugin for a host from the IntelliFlash Web UI.

To install or upgrade the VAAI plugin, complete the following steps:

1. From the IntelliFlash Web UI, go to **Settings > App-Aware > VMware Servers**.
2. Click **More**, and then select **ESXi Settings/VAAI**.
3. Select the host(s) for which you want to install or upgrade the VAAI plugin, and then click **Install or Upgrade VAAI plugin**.

### Uninstalling the IntelliFlash NAS VAAI Plugin from the IntelliFlash Web UI

To uninstall the VAAI plugin from the IntelliFlash Web UI, complete the following steps:

1. From the IntelliFlash Web UI, go to **Settings > App-Aware > VMware Servers**.
2. Click **More**, and then select **ESXi Settings/VAAI**.
3. Select the host(s) for which you want to uninstall the VAAI plugin, and then click **Uninstall VAAI plugin**.
4. A confirmation message appears. Click **Yes**.
5. In the **Reboot ESXi host** window, select the host(s) you want to reboot, and then click **Reboot**.



**Note:** The newly applied settings take effect after you Reboot the host.

## Using the IntelliFlash Manager plugin

After installing the IntelliFlash Manager plugin on the vCenter Server, you can log in to the vSphere client to access the IntelliFlash Manager plugin. Once you complete the installation of the IntelliFlash Manager plugin on the vSphere client, you can perform the following tasks:

- Register multiple IntelliFlash systems to the IntelliFlash Manager plugin.
- View details of the array, such as IntelliFlash version number, hardware model name, storage performance, and total number of datastores and virtual machines.
- Create SAN and NAS datastores and manage them.
- View storage performance per datastore.
- Access virtual machine details and their performance.
- Access your IntelliFlash systems from the IntelliFlash Manager plugin.
- Clone your virtual machines faster using the Hyperclone feature with the IntelliFlash NAS VAAI Plugin installed.
- Install or uninstall the IntelliFlash NAS VAAI Plugin .

- Configure multipathing rules for your datastores.
- Set recommended ESXi host settings in a few steps.
- View and manage ESXi host settings.
- View the VMware vSphere versions running on different ESXi hosts that are using IntelliFlash systems.

### Related Topics

[Accessing the IntelliFlash Manager plugin](#)

[Viewing the summary of an array](#)

[Host settings](#)

[Upgrading the IntelliFlash Manager](#)

## Accessing the IntelliFlash Manager plugin

After installing the IntelliFlash Manager plugin on the vCenter Server, you need to log in to the vSphere client to complete the installation. You can access the IntelliFlash Manager plugin only after completing the installation.

To access the IntelliFlash Manager plugin, complete the following steps:

1. Log in to the vSphere client.
2. You can access **IntelliFlash Manager** in one of the following ways:
  - Click **Menu > IntelliFlash Manager**.
  - Click **vSphere Client > Shortcuts > Monitoring > IntelliFlash Manager**.
  - Click **vSphere Client**. In the left navigation pane, click **IntelliFlash Manager**.



**Note:** If the IntelliFlash Manager plugin is successfully installed, it appears in the Home page, under **Installed Plugins**.

### Related Topics

[Installing IntelliFlash Manager on a vCenter Server](#)

## Registering a new IntelliFlash Array

Prerequisites for registering the IntelliFlash Array:

- When registering an array, you must have admin privileges.
- The array SSL certificate must have the array IP address in the **Subject Alternative Name** for successful registration of the array on the IntelliFlash Manager plugin.



**Note:** Array registration on the IntelliFlash Manager plugin may fail if any one of the controllers is down or when the upgrade is in progress.

To register a new IntelliFlash Array, complete the following steps:

1. Log in to **vSphere Client**.
  2. Click **Menu > IntelliFlash Manager > Inventory > ACTIONS**.
  3. Click **REGISTER**.
  4. In the **Register new array** dialog box:
    - a) Type the **Registered IP or FQDN**.  
It is recommended to use the Array Management IP address.
    - b) Type the **User name**.
-  **Note:** User the IntelliFlash user with "root"as the role.
- c) Type the **Password**.
  - d) Click **REGISTER**.

The newly added array is successfully registered. Now you can monitor and manage this array through the IntelliFlash Manager plugin.



**Note:** If you have not added the vCenter Server through the array, it will be automatically added after the registration is complete.

## Related Topics

[Using IntelliFlash Manager](#)

[Host Settings](#)

[Removing a vCenter Server from the VMware Server page](#)

## Viewing the Summary of an array

You can access, manage, and monitor IntelliFlash systems through the IntelliFlash Manager plugin. Once you access the array, you can view details of the array on the **Summary** page. The **Summary** page captures the version and model of the array. It also shows the *number of disks and pools on the array, the storage performance, and the datastores and VMs* connected to this array. You can also go to the IntelliFlash Web UI from the **Summary** page.

To view details of the array on the Summary page, complete the following steps:

1. Log in to the **vSphere Client**.
2. Click **Menu > IntelliFlash Manager > Inventory**.
3. Click the menu button next to the array and select **Go to**.  
This opens the **Summary** page.

## Related Topics

[Dashboard](#)

[Editing an array](#)

[Refreshing the VMware Servers page](#)

## Editing array details to update credentials

You can modify the array username and password in case you have changed the credentials of the array in IntelliFlash.

To edit the username and password, complete the following steps:

1. Log in to the **vSphere Client**.
2. Click **Menu > IntelliFlash Manager > Inventory > ACTIONS**.
3. Select the array you want to edit, and then click **Edit**.
4. In the **Edit array** window, type the new user name and password, and then click **EDIT**.

## Unregistering an array

You can unregister an array from the IntelliFlash Manager plugin. Once you unregister it, you cannot manage or monitor the array through the IntelliFlash Manager plugin.

To unregister an array, complete the following steps:

1. Log in to the **vSphere Client**.
2. Click **Menu > IntelliFlash Manager > Inventory > ACTIONS**.
3. Click **Unregister Array**.
  - a) In the **Unregister array** window, select the array that you want to unregister.
  - b) Click **UNREGISTER**.

## Host settings

---

The **Host settings** page displays all the ESXi hosts that are managed by the vCenter Server. Through the IntelliFlash Manager plugin you can install and manage the IntelliFlash NAS VAAI Plugin on the hosts, and update multipathing rules and various IntelliFlash recommended settings for the hosts. The **Host settings** page lists the ESXi host name, version number, and status of the host.



**Note:** If your array is running on IntelliFlash version 3.10.1.0 and you are using IntelliFlash Manager plugin 2.1, you must use the plugin to make any host settings.

Although, IntelliFlash versions earlier than 3.10.0.0 allow you to make changes to the host settings from the IntelliFlash Web UI.

ESXi host	Version	Status
10.xx.x.xxx	6.5.0	REQUIRES REBOOT
10.xx.x.xxx	6.7.0	REQUIRES REBOOT
10.xx.x.xxx	6.5.0	--
10.xx.x.xxx	6.0.0	REQUIRES REBOOT

**Figure 32: Host settings**

The following table describes the host status messages.

**Table 17: Host status**

Host status	Definition
REQUIRES REBOOT	After installing or uninstalling the IntelliFlash NAS VAAI Plugin, the system needs to reboot for the changes to take effect.
APPLY PERFORMANCE SETTINGS	The current ESX host performance settings are not set to the recommended values.
UNMANAGED STORAGE	None of the ESX host storage detected is part of the arrays registered with this IntelliFlash Manager plugin.
REQUIRES UPGRADE	The VAAI version installed on the ESX host is lower than the highest version found on the registered arrays.
MULTIPATHING SATP RULE IS NOT OPTIMAL	The SATP rules are not optimal/not installed.
MULTIPATHING PSP IS NOT OPTIMAL	The Path Selection Policy (PSP) is set to something other than the recommended value.
--	Error detected retrieving the host status. (For example, the ESX host was offline.)
GOOD	There are no further recommendations for optimal storage access. (For example, host connection was established, VAAI is installed, multipathing is optimal, array storage was detected, performance settings are in the recommended range.)

## Accessing ESXi hosts on the vCenter server

The **Host Settings** page displays all the ESXi hosts that are connected to the vCenter Server. Through the IntelliFlash Manager plugin you can install and manage the IntelliFlash NAS VAAI Plugin on the hosts and update multipathing rules and adjust the performance settings.

To access ESXi hosts, complete the following steps:

1. Log in to **vSphere Client**.
2. Click **Menu > IntelliFlash Manager > Host settings**.

The **Host Settings** page is displayed. This page lists the ESXi hosts, VMware ESXi host software version, and the host status.

### Related Topics

[Installing IntelliFlash NAS VAAI Plugin using IntelliFlash Manager Plugin](#)

## Installing IntelliFlash NAS VAAI Plugin using IntelliFlash Manager plugin

You can use the IntelliFlash Manager plugin to install or upgrade the IntelliFlash NAS VAAI Plugin on ESXi servers.



**Note:** You must be logged in to the vSphere Client.

To install the VAAI Plugin using the IntelliFlash Manager plugin, complete the following steps:

1. Log in to the **vSphere Client**.
2. Click **Menu > IntelliFlash Manager > Host settings**.
3. Go to **ACTIONS**.
4. Under **VAAI**, click **Install**.
  - a) In the **Install VAAI** window that appears, select the **ESXi host** from the drop-down list.
  - b) Click **Install**.



**Note:** Reboot the ESXi host for the changes to take effect.

## Uninstalling the IntelliFlash NAS VAAI Plugin using IntelliFlash Manager plugin

You can use the IntelliFlash Manager plugin to uninstall the IntelliFlash NAS VAAI Plugin on ESXi servers.

You must be logged in to the **vSphere Client**.

To uninstall the VAAI Plugin using the IntelliFlash Manager plugin, complete the following steps:

1. Log in to the **vSphere Client**.
2. Click **Menu > IntelliFlash Manager > Host settings**.
3. Click **ACTIONS** or click the menu button next to the host that you want to uninstall.
4. Under **VAAI**, click **UNINSTALL**.



**Note:** Reboot the ESXi host for the changes to take effect.

## Multipathing rules

In storage networking, the physical path between a server and the storage device can sometimes fail. When there is only one physical path between the two devices, there is a single point of failure (SPoF), which can be a problem. SAN multipathing establishes multiple routes between the hardware.

Multipathing in the IntelliFlash Manager plugin helps to intelligently control path selection from storage adapters in a host to storage devices. This can act as a useful failover mechanism, and assist with load balancing, which spreads I/O across multiple paths to reduce latency.

The default policies that are used to route I/O are:

- **Most Recently Used (MRU):** The host selects the path that it used most recently. When the path becomes unavailable, the host selects an alternative path. The host does not revert back to the original path when that path becomes available again. There is no preferred path setting with the MRU policy.
- **Fixed Path (FP):** The host continues to use the same path until a failure with the path occurs. Once the failed path is restored, it switches back to the path that had failed.
- **Round Robin (RR):** The host will alternate I/O on each path in a round-robin fashion to spread the load across multiple components.

The IntelliFlash plugin's **Adjust Path Selection Policy** helps users to automate the configuration of the Path Selection Policy (PSP) to the IntelliFlash recommended path selection policy of Round Robin (from MRU, Fixed Path, and so on.).



**Note:** If the SATP rules are not set, starting with IntelliFlash 3.10.0.0, you must install the SATP rules using the ESXi Server CLI.

## Adjusting path selection policy (PSP)

You can handle path management operations more intelligently using the **Adjust** multipathing feature. This feature enables you to change the policy for I/Os from Fixed path or MRU to Round Robin. Using the Round Robin policy ensures efficient load balancing, which translates to better I/O bandwidth and better failover path selection.

To adjust the path selection policy, complete the following steps:

1. Log in to **vSphere Client**.
2. Click **Menu > IntelliFlash Manager > Host settings**.
3. Select the **ESXi host** for which you want to enable multipathing.
4. Click  next to the ESXi host or go to **Actions > Multipathing rules > Adjust**.
5. In the **Adjust path selection policy (PSP)** window click **ADJUST**.



**Note:** The newly applied settings take effect after you Reboot the host.

## Setting ESXi Host Settings from the IntelliFlash Manager plugin

The IntelliFlash Manager plugin allows you to set some of the required parameters on the VMware ESXi Host.

- [NFS Max Queue Depth](#)
- [NFS Delete RPC Timeout](#)
- [NFS Heartbeat Frequency](#)
- [NFS Max Volume](#)
- [TCP/IP Heap Size](#)
- [TCP/IP Heap Max](#)
- [Maximum Disk IO Size](#)
- [ATS for VMFS Heartbeat](#)



If the ESXi host does not comply with the recommended settings, the host status shows **APPLY PERFORMANCE SETTINGS**.

You can select any of the recommended values, or select the **USE RECOMMENDED**, button to select all the optimal settings for your ESXi host, for each setting type.

## Applying settings for the host

Using the IntelliFlash Manager plugin you can set the following parameters on the VMware ESXi Host:

- **NFS Max Queue Depth:** This defines the number of pending I/O requests from an ESXi Server to an IntelliFlash share.
- **NFS Delete RPC Timeout:** This sets NFS delete timeout in seconds.
- **NFS Heartbeat Frequency:** NFS heartbeats are used to determine if an NFS volume is still available.
- **NFS Max Volume:** Limits the number of NFS datastores which can be mounted by the vSphere ESXi host concurrently.
- **TCP/IP Heap Size:** The initial amount of heap memory, measured in megabytes, which is allocated for managing VMkernel TCP/IP network connectivity.

- **TCP/IP Heap Max:** The maximum amount of heap memory, measured in megabytes, which can be allocated for managing VMkernel TCP/IP network connectivity.
- **Maximum Disk IO Size:** Limits maximum IO size in KB sent to your storage array.
- **ATS for VMFS Heartbeat:** Disables validation step on storage array and instead uses VMWare ESX reads and writes for validation.

To apply recommended settings for the host:

1. Log in to **vSphere Client**.
2. Click **Menu > IntelliFlash Manager > Host settings**.
3. Go to **ACTIONS > IntelliFlash recommended settings**.
4. In the **IntelliFlash recommended settings** window, select the **ESXi host** from the drop-down list.
5. Click the drop-down list to select a value for each parameter.  
If there is a current ( Example: Default) value outside the acceptable range, when selected, it will warn you that this value can degrade the performance of the ESX Host.
6. If you want to go by the recommended setting, click the **USE RECOMMENDED** button, or select the value with the **[Recommended]** tag.
7. Click **SAVE**.



**Note:** Most newly applied settings take effect only after you reboot the host. It is highly recommended you safely reboot your ESX host after changing these settings. If the ESXi host does not comply with the recommended settings, the host status shows **APPLY PERFORMANCE SETTINGS**.

## Setting NFS Max Queue Depth on VMware Server Using the IntelliFlash Manager plugin

The NFS max queue depth parameter defines the number of pending I/O requests from an ESXi Server to an IntelliFlash share. You can set the NFS max queue depth parameter on the ESXi Server, depending on the number of shares and ESXi hosts.

Use the following formula to set the NFS max queue depth:

**Formula:**  $NFS.\text{MaxQueueDepth} * \text{Number of Shares} * \text{Number of ESXi hosts} \leq 1024$



**Note:** The available values for the NFS max queue depth parameter are 32, 64, and 128.

**Example:** In the formula, if you use 64 for NFS max queue depth, the result is 640 ( $64*5*2=640$ ), which is less than the limit ( $<1024$ ). When you use 128 for NFS max queue depth, the result is 1280 ( $128*5*2=1280$ ), which is greater than 1024. So, in this example you should use 64 as the NFS max queue depth.

To set the NFS max queue depth on the VMware Server using the IntelliFlash Manager plugin, complete the following steps:

1. Log in to **vSphere Client**.
2. Click **Menu > IntelliFlash Manager > Host settings**.
3. Select the ESXi host for which you need to update the settings.
4. Click  next to the ESXi host.
5. In the **IntelliFlash recommended settings** window, click the **NFS Max Queue Depth** drop-down list and select a value.  
If there is a current ( Example: Default) value outside the acceptable range, when selected, it will warn you that this value can degrade the performance of the ESX Host.
6. If you want to go by the recommended setting, click the **USE RECOMMENDED** button, or select the value with the **[Recommended]** tag.
7. Click **SAVE**.



**Note:** Most newly applied settings take effect only after you reboot the host. It is highly recommended you safely reboot your ESX host after changing these settings. If the ESXi host does not comply with the recommended settings, the host status shows **APPLY PERFORMANCE SETTINGS**.

## Setting NFS Heartbeat Frequency on VMware Server Using the IntelliFlash Manager plugin

If you are using NFS shares to create virtual machines, you must set the **NFS .HeartbeatFrequency** value to a recommended value. The IntelliFlash Web UI fetches the default value defined on the ESXi server and displays it. You can change the value to a recommended value.

To set the **NFS .HeartbeatFrequency** value on a VMware ESX/ESXi server using the IntelliFlash Manager plugin, complete the following steps:

1. Log in to the **vSphere Client**.
2. Click **Menu > IntelliFlash Manager > Host Settings**.
3. Select the ESXi host for which you need to update the settings.
4. Click  next to the ESXi host.
5. In the **IntelliFlash recommended settings** window, click the **NFS Heartbeat Frequency** drop-down list and select a value.

If there is a current ( Example: Default) value outside the acceptable range, when selected, it will warn you that this value can degrade the performance of the ESX Host.

6. If you want to go by the recommended settings, click the **USE RECOMMENDED**.
7. Click **SAVE**.



**Note:** Most newly applied settings take effect only after you reboot the host. It is highly recommended you safely reboot your ESX host after changing these settings. If the ESXi host does not comply with the recommended settings, the host status shows **APPLY PERFORMANCE SETTINGS**.

### Setting NFS Delete RPC Timeout Using the IntelliFlash Manager plugin

The DeleteRPCTimeout parameter can be set on the ESXi host to increase the default NFS Delete timeout value. If this is not set to the recommended value, the NFS client on the ESXi host times out the request after 10 seconds. The IntelliFlash Manager plugin lists different recommendations for these values. Set the DeleteRPCTimeout according to the recommended value.

To set the DeleteRPCTimeout on the VMware Server using the IntelliFlash Manager plugin, complete the following steps:

1. Log in to **vSphere Client**.
2. Click **Menu > IntelliFlash Manager > Host settings**.
3. Select the ESXi host for which you need to update the settings.
4. Click  next to the ESXi host.
5. In the **recommended settings** window, click the **NFS.DeleteRPCTimeout** drop-down list and select a value.

If there is a current ( Example: Default) value outside the acceptable range, when selected, it will warn you that this value can degrade the performance of the ESX Host.

6. If you want to go by the recommended settings, click the **USE RECOMMENDED**.
7. Click **SAVE**.



**Note:** Most newly applied settings take effect only after you reboot the host. It is highly recommended you safely reboot your ESX host after changing these settings. If the ESXi host does not comply with the recommended settings, the host status shows **APPLY PERFORMANCE SETTINGS**.

### Setting NFS Max Volumes Using the IntelliFlash Manager plugin

By default, the NFS Max Volumes value is 8. This means that 8 is the maximum number of NFS volumes which can be mounted to an ESXi host. This can be changed, as VMware supports a maximum of 256 NFS volumes mounted to an ESXi host. Through the IntelliFlash Manager

plugin you can set the NFS.MaxVolumes value. This setting applies to a single ESXi host at a time, so this must be set on all ESXi hosts.

To set the NFS Max Volumes on the VMware Server using the IntelliFlash Manager plugin, complete the following steps:

1. Log in to **vSphere Client**.
2. Click **Menu > IntelliFlash Manager > Host settings**.
3. Select the ESXi host for which you need to update the settings.
4. Click  next to the ESXi host.
5. In the **IntelliFlash recommended settings** window, click the **NFS Max Volumes** drop-down list and select a value.  
If there is a current ( Example: Default) value outside the acceptable range, when selected, it will warn you that this value can degrade the performance of the ESX Host.
6. If you want to go by the recommended settings, click the **USE RECOMMENDED**.
7. Click **SAVE**.



**Note:** Most newly applied settings take effect only after you reboot the host. It is highly recommended you safely reboot your ESX host after changing these settings. If the ESXi host does not comply with the recommended settings, the host status shows **APPLY PERFORMANCE SETTINGS**.

### Setting TCP/IP Heap Size Using the IntelliFlash Manager plugin

TCP/IP Heap Size is the size of the memory (in MB) which is allocated up front by the VMkernel to TCP/IP heap. The default value for TCP/IP Heap Size is 0 MB. The maximum value for TCP/IP Heap Size is 128 MB. If you change the default NFS.MaxVolumes, you should also adjust the heap space settings for TCP/IP accordingly. IntelliFlash Manager plugin lists different recommendations for these values. Set the TCP/IP Heap Size according to the recommended values. This setting applies to a single ESXi host at a time, so this must be set on all ESXi hosts.

To set the TCP/IP Heap Size on the VMware Server using the IntelliFlash Manager plugin, complete the following steps:

1. Log in to **vSphere Client**.
2. Click **Menu > IntelliFlash Manager > Host settings**.
3. Select the ESXi host for which you need to update the settings.
4. Click  next to the ESXi host.
5. In the **IntelliFlash recommended settings** window, click the **TCP/IP Heap Size** drop-down list and select a value.
6. If you want to go by the recommended settings, click the **USE RECOMMENDED**.  
If there is a current ( Example: Default) value outside the acceptable range, when selected, it will warn you that this value can degrade the performance of the ESX Host.
7. Click **SAVE**.



**Note:** Most newly applied settings take effect only after you reboot the host. It is highly recommended you safely reboot your ESX host after changing these settings. If the ESXi host does not comply with the recommended settings, the host status shows **APPLY PERFORMANCE SETTINGS**.

### Setting TCP/IP Heap Max Using IntelliFlash Manager plugin

TCP/IP Heap Max is the maximum amount of heap memory, measured in megabytes, which can be allocated for managing VMkernel TCP/IP network connectivity. When increasing the number of NFS datastores, increase the maximum amount of heap memory as well, up to the maximum specific to the version of ESXi/ESX host.

To set the TCP/IP Heap Max on the VMware Server using the IntelliFlash Manager plugin, complete the following steps:

1. Log in to **vSphere Client**.
2. Click **Menu > IntelliFlash Manager > Host settings**.
3. Select the ESXi host for which you need to update the settings.
4. Click  next to the ESXi host.
5. In the **IntelliFlash recommended settings** window, click the **TCP/IP Heap Max** drop-down list and select a value.
6. If you want to go by the recommended settings, click the **USE RECOMMENDED**.  
If there is a current ( Example: Default) value outside the acceptable range, when selected, it will warn you that this value can degrade the performance of the ESX Host.
7. Click **SAVE**.



**Note:** Most newly applied settings take effect only after you reboot the host. It is highly recommended you safely reboot your ESX host after changing these settings. If the ESXi host does not comply with the recommended settings, the host status shows **APPLY PERFORMANCE SETTINGS**.

### Setting Maximum Disk IO Size on VMware Server Using the IntelliFlash Manager plugin

The Limits maximum IO size in KB sent to your storage array.

1. Log in to the **vSphere Client**.
2. Click **Menu > IntelliFlash Manager > Host Settings**.
3. Select the ESXi host for which you need to update the settings.
4. Click  next to the ESXi host.
5. In the **IntelliFlash recommended settings** window, click the **Maximum Disk IO Size** drop-down list and select a value.  
If there is a current ( Example: Default) value outside the acceptable range, when selected, it will warn you that this value can degrade the performance of the ESX Host.
6. If you want to go by the recommended settings, click the **USE RECOMMENDED**.
7. Click **SAVE**.



**Note:** Most newly applied settings take effect only after you reboot the host. It is highly recommended you safely reboot your ESX host after changing these settings. If the ESXi host does not comply with the recommended settings, the host status shows **APPLY PERFORMANCE SETTINGS**.

### Setting ATS for VMFS Heartbeat on VMware Server Using the IntelliFlash Manager plugin

The ATS for VMFS Heartbeat setting disables validation step on the storage array and instead uses VMWare ESX reads and writes for validation.

1. Log in to the **vSphere Client**.
2. Click **Menu > IntelliFlash Manager > Host Settings**.
3. Select the ESXi host for which you need to update the settings.
4. Click  next to the ESXi host.
5. In the **IntelliFlash recommended settings** window, click the **ATS for VMFS Heartbeat** drop-down list and select a value.

If there is a current ( Example: Default) value outside the acceptable range, when selected, it will warn you that this value can degrade the performance of the ESX Host.

6. If you want to go by the recommended settings, click the **USE RECOMMENDED**.
7. Click **SAVE**.



**Note:** Most newly applied settings take effect only after you reboot the host. It is highly recommended you safely reboot your ESX host after changing these settings. If the ESXi host does not comply with the recommended settings, the host status shows **APPLY PERFORMANCE SETTINGS**.

## Datastores management

---

You can create NAS and SAN (VMFS) datastores using the IntelliFlash Manager plugin installed on a vCenter Server. When you create a datastore using the IntelliFlash Manager plugin, a share or LUN is created on the IntelliFlash Array. Datastores allow you to store your virtual machines and their files.

### Related Topics

[Adding a NAS datastore using IntelliFlash Manager plugin](#)

[Adding a SAN datastore using IntelliFlash Manager plugin](#)

### Adding a NAS datastore using the IntelliFlash Manager plugin

Adding a NAS datastore enables you to provide storage space for virtual machines.

#### Prerequisites

- You must have a NAS compatible project type created on the IntelliFlash Array.

To create a NAS datastore using the IntelliFlash Manager plugin, complete the following steps:

1. Log in to the **vSphere Client**.
2. Click **Menu > IntelliFlash Manager > Inventory**.
3. In the **Inventory** section, for the required array, click and select **Go to**.
4. In the array details page, click the **ACTIONS** menu and select **Add**.
5. In the **Add Datastore** window, complete the following steps:
  - a) Select a **vCenter server**.  
The **vCenter Server** option is available for vCenter Servers systems in the Linked Mode only.
  - b) Type a name for the datastore.
  - c) Select the **NAS Type** datastore from the dropdown list.
  - d) Select **Protocol**.

- e) Select **ESXi Host**.  
You can select all ESXi hosts or select required hosts individually from the list.
- f) Select a **Pool** from the dropdown list.
- g) Select a **Project** from the dropdown list.
- h) Select a **Purpose** for the project.
- i) Select **Alert threshold** and **Warning threshold**.  
The vCenter Server UI displays alarms for Alert and Warning thresholds when the set threshold is reached for the datastore.
- j) Select a **Floating IP** address.
- k) Select **Quota size**.



**Note:** The default quota size is zero indicating no quota is applied for the datastore.

- l) Select **Network ACL: Inherit from Project** or **Access from selected hosts**.  
The **Access from selected hosts** option inherits the network ACL from the selected ESXi hosts.

## 6. Click **ADD**.

You can view the newly created datastore in the **Datastores** tab (**Menu > IntelliFlash Manager > Datastores**).

### Related Topics

[Resizing a NAS or SAN datastore using IntelliFlash Manager plugin](#)

[Deleting datastores](#)

## Adding a SAN datastore using the IntelliFlash Manager plugin

Adding a SAN datastore enables you to provide storage space for virtual machines.

### Prerequisites

- You must have a SAN compatible project created on the IntelliFlash Array.
- Target and initiator mapping is configured.

To create a SAN datastore using the IntelliFlash Manager plugin, complete the following steps:

1. Log in to the **vSphere Client**.
2. Click **Menu > IntelliFlash Manager > Inventory**.
3. In the **Inventory** section, for the required array, click  and select **Go to**.
4. In the array details page, click the **ACTIONS** menu and select **Add**.
5. In the **Add Datastore** window, complete the following steps:
  - a) Select a **vCenter server**.  
The **vCenter Server** option is available for vCenter Servers systems in the Linked Mode only.
  - b) Type a name for the datastore.
  - c) Select the **SAN Type** datastore from the dropdown list.
  - d) Select **Protocol**.
  - e) Select **ESXi Host**.
  - f) Select a **Pool** from dropdown list.
  - g) Select a **Project** from dropdown list.
  - h) Select a **Purpose** for the project.
  - i) Select **Alert threshold** and **Warning threshold**.  
The vCenter Server UI displays alarms for Alert and Warning thresholds when the set threshold is reached for the datastore.
  - j) Select **File system version** (VMFS5 or VMFS6).
  - k) Enter a size for the datastore.
  - l) (Optional) Enable **Thin provisioning**.
6. Click **ADD**.

### Related Topics

[Resizing a NAS or SAN datastore using IntelliFlash Manager plugin](#)

## Resizing a NAS or SAN datastore using the IntelliFlash Manager plugin

You can resize a datastore to provide more storage space for virtual machines. The resize operation only allows increasing to increase the size of a datastore.

### Prerequisite:

A project on the array must have sufficient quota to expand a datastore.



**Note:** You can also resize a datastore from the **Datastores** tab.

To resize a NAS datastore using the IntelliFlash Manager plugin, complete the following steps:

1. Log in to the **vSphere Client**.
2. Click **Menu > IntelliFlash Manager > Inventory**.
3. In the **Inventory** section, for the required array, click  and select **Go to**.
4. In the array details page, click the **ACTIONS** menu and select **Resize**.
5. In the **Resize Datastore** window, complete the following steps:
  - a) Select a datastore from the dropdown list.
  - b) Enter a new size for the datastore.
  - c) Click **RESIZE**.

## Viewing datastores

From the **Datastores** tab, you can view all datastores and their details on a particular IntelliFlash Array. The **Datastores** tab displays the following:

- Name of a datastore
- Project in which the datastore is created.
- IP address of the ESXi Server using the datastore.
- Storage protocol of each datastore
- Storage capacity of the datastore
- Data compression percentage

You can apply filter for the datastores to view required details.

To view datastores, complete the following steps:

1. Log in to the **vSphere Client**.
2. Click **Menu > IntelliFlash Manager > Inventory**.
3. In the **Inventory** section, for the required array, click  and select **Go to**.
4. In the array details page, click the **Datastores** tab.

## Related Topics

[\*Adding a SAN datastore using IntelliFlash Manager plugin\*](#)

[\*Adding a NAS datastore using IntelliFlash Manager plugin\*](#)

## Viewing storage performance of a datastore

To view storage performance of a datastore, complete the following steps:

1. Log in to the **vSphere Client**.
2. Click **Menu > IntelliFlash Manager > Inventory**.
3. In the **Inventory** section, for the required array, click  and select **Go to**.
4. In the array details page, click the **Datastores** tab.
5. In the **Datastores** page, click  for the required datastore and select **Go to**.
6. In the **Summary** tab of the datastore details page, look for the **Storage Performance** section.

The **Storage Performance** section displays space savings and data size in the datastore.

## Filtering datastores

You can set filters for datastores to view specific datastores with the required details.

1. Log in to the **vSphere Client**.
2. Click **Menu > IntelliFlash Manager > Inventory**.
3. In the **Inventory** section, for the required array, click  and select **Go to**.
4. In the array details page, click the **Datastores** tab.
5. In the **Datastores** tab, search and set filters for any of these: **Name**, **Project**, **ESX Server**, **Protocol**, **Capacity**, and **Compression** fields.

 **Note:** You can remove the filters by clearing the text and clicking the close button for the set filter.

## Accessing datastores

To access datastores, complete the following steps:

1. Log in to the **vSphere Client**.
2. Click **Menu > IntelliFlash Manager > Inventory**.
3. In the **Inventory** section, for the required array, click  and select **Go to**.
4. In the array details page, click the **Datastores** tab.
5. In the **Datastores**, click  and select **Go to**

## Deleting datastores

When you delete a datastore all contents of the datastore are permanently deleted and corresponding shares or LUNs on the array also deleted.

The IntelliFlash array reclaims the space after deleting the datastore by deleting the share or LUN on the array.

 **Note:** Before deleting a datastore, review the prerequisites for deleting datastores in the VMware documentation.

To delete a datastore, complete the following steps:

1. Log in to the **vSphere Client**.
2. Click **Menu > IntelliFlash Manager > Inventory**.
3. In the **Inventory** section, for the required array, click  and select **Go to**.
4. In the array details page, click the **Datastores** tab.
5. In the **Datastores** tab, click  for the required datastore and select **Delete**.
6. In the **Delete Datastore** window, move the **Delete IntelliFlash backing** toggle button to delete a share or LUN on the array.  
If the **Delete IntelliFlash backing** option is not enabled, the share or LUN on the array is not deleted.
7. In the **Delete Datastore** window, click **Delete**.

### Related Topics

[Adding a SAN datastore using IntelliFlash Manager plugin](#)

[Adding a NAS datastore using IntelliFlash Manager plugin](#)

## Snapshots and Clones management

---

The IntelliFlash Manager plugin displays the automatic snapshots taken according to the project-level snapshot policy set in the IntelliFlash Web UI and manual snapshots. You can view the auto-snapshots in the plugin from the **Snapshot** tab. If you need to change the automatic snapshot policy or create a custom snapshot policy, you can change it from the IntelliFlash Web UI.

### Quiesced snapshots

If you want the IntelliFlash OS to take quiesced snapshots for manual snapshots, you must enable the option **Enable Quiesce** when adding a vCenter Server from the IntelliFlash Web UI.

You must also turn on the quiesce option at the project level for the IntelliFlash Web UI to take automatic quiesce snapshots. The plugin can overwrite the project-level quiesce setting.



**Note:** A datastore must have virtual machines to take quiesce snapshots.

You can enable or disable the quiesce option from the **Settings > App-Aware > VMware Servers** section of the IntelliFlash Web UI by editing the VMware vCenter Server details.

## Related Topics

[\*Viewing snapshots of a datastore\*](#)

[\*Creating a manual snapshot of a datastore\*](#)

[\*Cloning a snapshot of a datastore\*](#)

[\*Rollback to a snapshot\*](#)

[\*Deleting a snapshot of a datastore\*](#)

## Viewing snapshots of a datastore

You can view automatic and manual snapshots of a datastore in the .

To view snapshots of a datastore, complete the following steps:

1. Log in to the **vSphere Client**.
2. Click **Menu > IntelliFlash Manager > Inventory**.
3. In the **Inventory** section, for the required array, click and select **Go to**.
4. In the array details page, click the **Datastores** tab.
5. In the **Datastores** page, click and select **Go to**
6. In the datastore details screen, click **Monitor**.
7. On the **Monitor** tab, select **IntelliFlash > Snapshots**.

## Related Topics

[\*Snapshots and Clones management\*](#)

[\*Cloning a snapshot of a datastore\*](#)

[\*Rollback to a snapshot\*](#)

[\*Deleting a snapshot of a datastore\*](#)

## Creating a manual snapshot of a datastore

You can create a manual snapshot of a datastore and clone it. After creating a manual snapshot, you should refresh the snapshots list page to see the new manual snapshot.

 **Note:** You can take a quiesce snapshot only if the **Quiesce** option is selected when adding a vCenter Server to your array.

To create a manual snapshot, complete the following steps:

1. Log in to the **vSphere Client**.
2. Click **Menu > IntelliFlash Manager > Inventory**.
3. In the **Inventory** section, for the required array, click  and select **Go to**.
4. In the array details page, click the **Datastores** tab.
5. In the **Datastores** page, click  for the required datastore and select **Go to**.
6. In the datastore details screen, click **Monitor**.
7. On the **Monitor** tab, select **IntelliFlash > Snapshots**.
8. In the Snapshots screen, click **MANUAL SNAPSHOT**.
9. In the **Manual Snapshot** window, type a name for the snapshot.
10. (Optional) Select **Enable quiesce**.
11. Click **Add**.

### Related Topics

[Snapshots and Clones management](#)

[Cloning a snapshot of a datastore](#)

[Rollback to a snapshot](#)

[Deleting a snapshot of a datastore](#)

## Cloning a snapshot of a datastore

You can clone a manual or an auto snapshot and use it as a read-only datastore or use it for creating virtual machines.

To clone a snapshot, complete the following steps:

1. Log in to the vSphere client.
2. Click **Menu > IntelliFlash Manager > Inventory**.
3. In the **Inventory** section, for the required array, click  and select **Go to**.
4. In the array details page, click the **Datastores** tab.
5. In the **Datastores**, click  for the required datastore and select **Go to**
6. In the datastore details screen, click **Monitor**.
7. In the **Monitor** tab, select **IntelliFlash > Snapshots**.
8. In the snapshots list page, click  for the required datastore and select **Clone**.
9. In the **Clone Snapshot** window, type a name for the clone.
10. (Optional) Select the **Enable read only** option.
11. Select an **ESXi host** from the list.
12. Click **CLONE**.

### Related Topics

[\*Snapshots and Clones management\*](#)

[\*Cloning a snapshot of a datastore\*](#)

[\*Rollback to a snapshot\*](#)

[\*Deleting a snapshot of a datastore\*](#)

### Rolling back to a snapshot

Snapshot rollback is a process for reverting the state of a datastore or virtual machine back to a point-in-time state when the snapshot was taken.

The rollback process results in permanent data loss. You might permanently lose the data changes that happened between rollback time and snapshot creation time.



**Note:** Power off the virtual machine before starting the rollback process.

To roll back to a snapshot, complete the following steps:

1. Log in to the vSphere client.
2. Click **Menu > IntelliFlash Manager > Inventory**.
3. In the **Inventory** section, for the required array, click  and select **Go to**.
4. In the array details page, click the **Datastores** tab.
5. In the **Datastores**, click  for the required datastore and select **Go to**
6. In the datastore details screen, click **Monitor**.
7. In the **Monitor** tab, select **IntelliFlash > Snapshots**.
8. In the snapshots list page, click  for the required datastore and select **Rollback**.
9. In the **Rollback Snapshot** window, read the details of effected snapshots and clones, then click **ROLLBACK**.

### Related Topics

[Creating a manual snapshot of a datastore](#)

[Rolling back to a snapshot](#)

[Deleting a snapshot of a datastore](#)

### Deleting a snapshot of a datastore

The automatically deletes all auto-snapshots as per the snapshot schedule set on a project.

If you want to manually delete any snapshots, you can delete them using the .

 **Note:** When you delete a snapshot, IntelliFlash Web UI deletes the dependent cloned datastores as well.

To delete a snapshot, complete the following steps:

1. Log in to the **vSphere Client**.
2. Click **Menu > IntelliFlash Manager > Inventory**.
3. In the **Inventory** section, for the required array, click  and select **Go to**.
4. In the array details page, click the **Datastores** tab.
5. In the **Datastores**, click  for the required datastore and select **Go to**
6. In the datastore details screen, click **Monitor**.
7. In the **Monitor** tab, select **IntelliFlash > Snapshots**.
8. In the snapshots list page, click  for the required s and select **Delete**.
9. In the **Delete Snapshot** window, click **DELETE**.

#### Related Topics

[Creating a manual snapshot of a datastore](#)

[Rolling back to a snapshot](#)

## Virtual machines management

---

The enables you to manage virtual machines independently in each datastore. You can view average latency, total IOPS, and total throughput per virtual machine and a consolidated view of all virtual machines in the **VM** details page.

You can view the storage performance of each virtual machine and clone them using the **Hyperclone** feature.

#### Related Topics

[Viewing all virtual machine on an array](#)

[Viewing virtual machines inside a datastore](#)

[Accessing virtual machines in a datastore](#)

[Viewing storage performance of a virtual machine](#)

[Cloning a virtual machine using the Hyperclone option](#)

[Virtual machines management](#)

### Viewing all virtual machines on an array

The **VM** tab in the array details page lists all virtual machines. You can view read and write latency, IOPS, and throughput of virtual machines.

To view all virtual machines on an array, complete the following steps:

1. Log in to the **vSphere Client**.
2. Click **Menu > IntelliFlash Manager > Inventory**.
3. In the **Inventory** section, for the required array, click and select **Go to**.
4. In the array details page, click the **VM** tab.

### Related Topics

[\*Viewing virtual machines inside a datastore\*](#)

[\*Accessing virtual machines in a datastore\*](#)

[\*Viewing storage performance of a virtual machine\*](#)

[\*Cloning a virtual machine using the Hyperclone option\*](#)

## Viewing virtual machines inside a datastore

To view details of virtual machines inside a datastore, complete the following steps:

1. Log in to the **vSphere Client**.
2. Click **Menu > IntelliFlash Manager > Inventory**.
3. In the **Inventory** section, for the required array, click and select **Go to**.
4. In the array details page, click the **Datastores** tab.
5. In the **Datastores**, click for the required datastore and select **Go to**.
6. In the datastore details screen, click **Monitor**.
7. Click **IntelliFlash > VMs**.
8. In the **VM** details page, you can click the **TOTAL, READ, WRITE** tabs to view performance of the VMs inside a datastore.

### Related Topics

[\*Viewing all virtual machine on an array\*](#)

[\*Accessing virtual machines in a datastore\*](#)

[\*Viewing storage performance of a virtual machine\*](#)

[\*Cloning a virtual machine using the Hyperclone option\*](#)

## Accessing virtual machines in a datastore

To access virtual machines in a datastore, complete the following steps:

1. Log in to the **vSphere Client**.
2. Click **Menu > IntelliFlash Manager > Inventory**.
3. In the **Inventory** section, for the required array, click  and select **Go to**.
4. In the array details page, click the **Datastores** tab.
5. In the **Datastores**, click  for the required datastore and select **Go to**
6. In the datastore details screen, click **Monitor**.
7. Click **IntelliFlash > VMs**.
8. In the VMs list, click  for the required VM and select **Go to**.

### Related Topics

[\*Virtual machines management\*](#)

[\*Viewing all virtual machine on an array\*](#)

[\*Accessing virtual machines in a datastore\*](#)

[\*Viewing storage performance of a virtual machine\*](#)

[\*Cloning a virtual machine using the Hyperclone option\*](#)

## Viewing storage performance of a virtual machine

The **Performance** page only displays details of a virtual machine hosted on IntelliFlash datastore.

You can view read and write for latency, throughput, and IOPs. The page displays real time, a day, week, and month on graphs.

To view performance of a virtual machine, complete the following steps:

1. Log in to the vSphere client.
2. Click **Menu > IntelliFlash Manager > Inventory**.
3. In the **Inventory** section, for the required array, click  and select **Go to**.
4. In the array details page, click the **Datastores** tab.
5. In the **Datastores**, click  for the required datastore and select **Go to**
6. In the datastore details screen, click **Monitor**.
7. Click **IntelliFlash > Performance**.
8. In the **Performance** page, select **Real-time, Day, Week, or Month**.
9. Click **TOTAL, READ, and WRITE** to view latency, throughput, and IOPS.

### Related Topics

[\*Virtual machines management\*](#)

[\*Viewing all virtual machine on an array\*](#)

[\*Accessing virtual machines in a datastore\*](#)

[\*Cloning a virtual machine using the Hyperclone option\*](#)

### Cloning a virtual machine using the Hyperclone option

You must have the installed to use the **Hyperclone** feature to create VM clones faster.

You can create clones of virtual machines without having the IntelliFlash NAS VAAI Plugin installed, however, it is a time-consuming task as the cloning operation falls back to regular cloning operations.

You can select to power on the virtual machines while cloning VMs. The **Hyperclone** wizard provides the option to power on all VMs or power on VMs in a staggered way. If you select the stagger option, the IntelliFlash Manager plugin will power on a batch of five (5) VMs in a staggered way.

The **Hyperclone** wizard also provides the option not to power on the VMs after cloning the VMs.

To clone a virtual machine inside a datastore, complete the following steps:

1. Log in to the vSphere client.
2. Click **Menu > IntelliFlash Manager > Inventory**.
3. In the **Inventory** section, for the required array, click and select **Go to**.
4. In the array details page, click the **Datastores** tab.
5. In the **Datastores**, click for the required datastore and select **Go to**
6. In the datastore details screen, click **Monitor**.
7. Click **IntelliFlash > VMs**.
8. In the VMs list, click for the required VM and select **Hyperclone**.
9. In the **Hyperclone** window, complete the following steps:
  - a) In the **Details** screen, type a name for the clone.
  - b) Enter a count for clones.  
You can mention the number of clones you need.
  - c) Enter starting number for clones.  
If you want to create multiple clones, you can mention the number from which the count of the clones to start.
  - d) Click **NEXT**.
  - e) In the **Target** screen, select **Hosts and Clusters**.
  - f) Select **Resource pool**.
  - g) Select **Power options**.
    - Power off
    - Power on stagger
    - Power on all

**Note:** The Power on stagger option will power on a batch of five VMs in a staggered way.
  - h) Click **NEXT**.
  - i) Review the **Summary** and click **FINISH**.

You can view the VMs power on status in the Recent task pane of the vCenter Server UI.

## Related Topics

[Virtual machines management](#)

[Viewing all virtual machine on an array](#)

[Accessing virtual machines in a datastore](#)

*Viewing storage performance of a virtual machine*

## Role-based access control in the IntelliFlash Manager plugin

---

The IntelliFlash Manager plugin provides role-based access control to manage access to the IntelliFlash Manager plugin features for vCenter users (vSphere users).

The IntelliFlash Manager plugin supports the following sample roles:

- IntelliFlash Admin
- IntelliFlash User
- IntelliFlash Read-only

Using the sample roles provided with the IntelliFlash Manager plugin, you can customize and provide privileges to the vCenter users. The vCenter users with customized privileges can perform tasks according to the defined privileges.

 **Note:** To perform certain tasks, you must add additional vCenter Server privileges to IntelliFlash Manager plugin predefined privileges.

### Related Topics

[Privileges for sample roles in IntelliFlash Manager plugin](#)

[Adding a NAS datastore using IntelliFlash Manager plugin](#)

[Adding a SAN datastore using IntelliFlash Manager plugin](#)

## Privileges for sample roles in IntelliFlash Manager plugin

The IntelliFlash Manager plugin sample roles have the privileges described as follows.

### IntelliFlash Admin

A user with the **IntelliFlash Admin** role can perform all the tasks in the plugin. The following are privileges of the **IntelliFlash Admin** sample role.

 **Note:** You will need to add a few additional privileges that are not available in the IntelliFlash Manager plugin sample roles. The additional privileges allow you perform operations which you cannot perform otherwise.

- **Host Management**
  - **List Hosts** - A privilege to list hosts.
  - **Set Advanced Host Options** - A privilege to set host options.
  - **Set Host PSP Policy** - A privilege to set PSP policy on hosts.
  - **Set Host SATP Rules** - A privilege to enable a user to reboot an ESX host.
  - **Set Host VAAI State** - A privilege to enable VAAI on an ESX host.
- **IntelliFlash Datastores**

- **Add Datastore** - A privilege to add a datastore on the IntelliFlash Array .
- **Add Datastore Snapshot** - A privilege to add a datastore snapshot on the IntelliFlash Array.
- **Clone Datastore** - A privilege to clone a datastore on the array.
- **Configure Datastore** - A privilege to change properties of a datastore.
- **List Datastores** - A privilege to list datastores on the array from **Datastores** page of the IntelliFlash Manager plugin.
- **Remove Datastore** - A privilege to remove a datastore on the IntelliFlash Array.
- **Remove Datastore Snapshot** - A privilege to remove a datastore on the IntelliFlash Array.
- **Rollback Datastore Snapshot** - A privilege to rollback to a datastore snapshot on the array.
- **IntelliFlash Inventory**
  - **Add IntelliFlash Array** - A privilege to add an IntelliFlash Array from the **Inventory** page of the IntelliFlash Manager plugin.
  - **List IntelliFlash Arrays** - A privilege to view an IntelliFlash Array in **Inventory** page of the IntelliFlash Manager plugin.
  - **Remove IntelliFlash Array** - A privilege to remove IntelliFlash Array in **Inventory** page of the IntelliFlash Manager plugin.
- **IntelliFlash VM Operations**
  - **HyperClone VM** - A privilege to use the HyperClone feature of the IntelliFlash Manager plugin to clone VMs faster.
  - **List VMs** - A privilege to list VMs on the selected IntelliFlash Manager plugin array.

## IntelliFlash User

A user with the **IntelliFlash User** sample role has permissions for the following: **Inventory**, **Datastores**, and **Virtual machines (VMs)**.

 **Note:** By default, the **IntelliFlash User** sample role only has the privileges from the **Host Management** and **IntelliFlash Inventory** list of privileges.

- **Host Management**
  - List Hosts
- **IntelliFlash Datastores**
  - Add Datastore
  - Add Datastore Snapshot
  - Clone Datastore
  - Configure Datastore

- List Datastores
- Remove Datastore
- Remove Datastore Snapshot
- Rollback Datastore Snapshot
- **IntelliFlash Inventory**
  - List IntelliFlash Systems
- **IntelliFlash VM Operations**
  - HyperClone VM
  - List VMs

### **IntelliFlash Read-only**

The user **IntelliFlash Read-only** sample role has the following permissions:

- **Host Management**
  - List Hosts
- **IntelliFlash Datastores**
  - List Datastores
- **IntelliFlash Inventory**
  - List IntelliFlash Systems
- **IntelliFlash VM Operations**
  - List VMs

### **Related Topics**

[\*Role based access control in IntelliFlash Manager plugin\*](#)

[\*Adding additional privileges for IntelliFlash Manager sample roles\*](#)

### **Adding additional privileges for the IntelliFlash Manager plugin sample roles**

The sample roles in the IntelliFlash Manager plugin: **IntelliFlash Admin** and **IntelliFlash User**, are not designed to be used as-is, because certain operations require additional privileges defined by VMware vCenter. These additional privileges are not defined in the sample roles.

For example, for Hyperclone VM operations, users need to have the privilege to create VMs, which is a privilege defined by VMware. If a user is assigned the sample **IntelliFlash User** role, **Create VM** privilege needs to be added to the role for Hyperclone to complete successfully.

To add additional required privileges for IntelliFlash Manager plugin sample roles, complete following steps:

1. Log in to the **vSphere Client**.
2. Click **Menu > Administration > Roles**.
3. In the **Roles** menu, select **IntelliFlash Admin** or **IntelliFlash User** and click the **Edit role action** icon.
4. In the **Edit Role** window, complete the following steps for **IntelliFlash Admin** or **IntelliFlash User**.
  - a) Select **Datastore > Allocate space**.
  - b) Select **Resource > Assign vApp to resource pool**.
  - c) Select **vApp > All vApp privileges**.
  - d) Select **Virtual Machine > Interaction**.
  - e) Select **Virtual Machine > Inventory**.
  - f) Select **Virtual Machine > Provisioning**.
  - g) Select **Host > All Host privileges**.
  - h) Select **Host > Configuration > Maintenance**.
5. Click **Next**.
6. (Optional) Provide a description.
7. Click **FINISH**.

The **IntelliFlash Admin** or **IntelliFlash User** displays the new additional privileges added. Now, you can use the IntelliFlash Manager plugin sample roles when creating a new vCenter User (vSphere User) and assign IntelliFlash Manager plugin sample roles.



---

# Chapter 29

---

## IntelliFlash Storage Replication Adapter

---

**Topics:**

- *Overview of IntelliFlash Storage Replication Adapter (SRA)*
- *Prerequisites for Installing IntelliFlash SRA*
- *Installing Containerized IntelliFlash SRA 2.0.0 Plugin*
- *Configuring Array Managers in VMware Site Recovery Manager (SRM)*
- *Discovering Devices in Site Recovery Manager*
- *Create, Test, and Run Recovery Plan*
- *Create Array Based Replication Protection Group*
- *Create a Recovery Plan*
- *Perform a Planned Recovery or Disaster Recovery*
- *Reprotect After Recovery*

## Overview of IntelliFlash Storage Replication Adapter (SRA)

The IntelliFlash Storage Replication Adapter (SRA) plugin works with the VMware vCenter Site Recovery Manager (SRM) and enables you to plan, test, and implement array-based replication in VMware environments for disaster recovery. You can use IntelliFlash systems as replication partners in the Site Recovery Manager (SRM) environment.

Install the IntelliFlash SRA plugin on your VMware Site Recovery Manager Servers to use IntelliFlash systems as replication partners.

Use the Windows IntelliFlash SRA 1.0.3 plugin for Windows-based Site Recovery Manager (SRM) 8.3 or lower versions.

Use the containerized IntelliFlash SRA 2.0.0 plugin for Photon-based Site Recovery Manager (SRM) 8.2 or higher versions. This plugin is distributed as a Docker image and can be hosted on a Docker Hub or on a private registry.

### Project-level replication

IntelliFlash replicates data at the project level. A replicated project on a target storage array is called a **Replica** project.

Project-level replication simplifies the process of managing replication relationships. When a project is replicated, all the shares and LUNs within the project are replicated to the target storage array.

When configuring a replication relationship in the IntelliFlash Web UI for a VMware Site Recovery Manager environment, select **SRM Partner** as the Replication role and include all shares and LUNs within that project.

#### Note:

- You must configure a replication relationship before configuring the SRM setup.
- All datasets (shares/LUNs) that need to be included in the SRM replication group must be kept in one project.

In the IntelliFlash Web UI, replication relationships are configured for projects using the Replication Configuration Wizard which is accessed under:

**Provision > Projects > Manage > Data Protection > Replication.**

### Array GUID for VMware Site Recovery Manager setups

IntelliFlash SRA uses the GUID of the IntelliFlash systems as the Array ID for communicating with the Site Recovery Manager and when pairing with another SRA.

You can view the IntelliFlash system GUID from the **System Information** panel, under the **Array Information** section of the **Information** tab. Click the array name at the top right corner of the IntelliFlash Web UI to view the *System Information* panel.

The array GUID helps you to identify the correct array when pairing with another VMware Site Recovery Manager.

For more information about VMware Site Recovery Manager, refer to the VMware product documentation:

<https://docs.vmware.com/en/Site-Recovery-Manager/index.html>

## Prerequisites for Installing IntelliFlash SRA

---

### Installing and Connecting Site Recovery Manager Instances on Protected and Recovery Sites

You must install the supported VMware Site Recovery Manager (SRM) server at the protected site and recovery site. The installed SRM servers must be able to connect to the respective vCenter Server at the protected and recovery sites.

After installing the VMware SRM server, the Site Recovery Manager (SRM) server appears in the vSphere Web Client. You can use the plugin in the vSphere Web Client to configure and manage the Site Recovery Manager Server.

After installing a supported VMware Site Recovery Manager (SRM) version on both the protected site and recovery site, you must pair the sites.

Refer to the VMware documentation for prerequisites and detailed instructions on how to install the VMware Site Recovery Manager Server:

<https://docs.vmware.com/en/Site-Recovery-Manager/index.html>

### Predefined SRA Role for Site Recovery Manager (SRM)

A predefined SRA role for VMware Site Recovery Manager environments is available in the IntelliFlash Web UI. You can add a user account in the IntelliFlash Web UI, assign the SRA role for the user account, then use the SRA role user account when configuring the Array Manager in the VMware SRM Server.

You can add a user account for the SRA role under:

**Settings > Administration > Management Access > Local Admins.**

### Setting up Additional Configurations

Before installing IntelliFlash SRA on the Site Recovery Manager Servers (protected and recovery sites), you need to complete the following configurations:

- On the IntelliFlash Web UI, set up a replication relationship between the replication source array and the replication target array and assign the **SRM Partner** replication role to it.
- Install SATP rules.

You need to install Tegile SATP rules for iSCSI and FC on the ESXi Servers of the protected and recovery sites. You can install the rules from the IntelliFlash Manager plugin and from the ESXi CLI. To install Tegile SATP rules using the IntelliFlash Manager plugin, you should add your vCenter Servers and register them on the IntelliFlash systems.

- If you are using iSCSI, you must add iSCSI initiators of the ESXi Servers on both the replication source and target arrays.
- You must add iSCSI target details of both the replication source and replication target on their respective ESXi Servers.
- You must create datastores and VMs on your ESXi Servers.

## Installing Containerized IntelliFlash SRA 2.0.0 Plugin

---

### Prerequisites for the Containerized IntelliFlash SRA 2.0.0 Plugin

 **Note:** Use the containerized IntelliFlash SRA 2.0.0 plugin for Photon-based Site Recovery Manager (SRM) 8.2 or higher versions. This plugin is distributed as a Docker image and can be hosted on Docker Hub or on a private registry.

You need to meet the following prerequisites before you install the containerized IntelliFlash SRA 2.0.0 plugin.

#### Hardware

Two IntelliFlash systems – one array for the protected site and another array for the recovery site.

#### IntelliFlash Operating Environment

- IntelliFlash 3.11.0.0 or higher is installed on your systems.
- IntelliFlash SRA 2.0.0 plugin is installed on both the Site Recovery Manager servers for the protected and recovery sites.

#### Supported VMware ESXi

- VMware ESXi 7.0 or later – Installed on both the protected site and the recovery site.
- VMware vCenter 7.0 or later – Installed on both the protected site and the recovery site.
- For VMFS 5 datastores, disable the VAAI ATS heartbeat.

You can disable this using the ESXi CLI. Use the following command to disable the VAAI ATS heartbeat:

```
# esxcli system settings advanced set -i 0 -o /VMFS3/
UseATSForHBOOnVMFS5
```

#### Supported VMware Site Recovery Manager Versions

Photon-based VMware Site Recovery Manager 8.2 and higher

## Installing Containerized IntelliFlash SRA 2.0.0 Plugin

Install IntelliFlash SRA 2.0.0 plugin on both the sites that have the Photon-based SRMs installed.

The IntelliFlash SRA plugin allows you to use the SRM to make recovery plans for VMs on replicated IntelliFlash storage arrays.

**Prerequisite:** Install the two Photon-based SRMs and then pair them.

1. Download the containerized IntelliFlash SRA 2.0.0 plugin.

To download the containerized IntelliFlash SRA 2.0.0 plugin, perform the following steps:

- a) Navigate to the [IntelliFlash SRA Plugin Github](#) page.
- b) Click the **IntelliFlash-Containerized-SRA.2.0.0.tar.gz** file.
- c) Click the **Download** button to download the file.
- d) Save the **SRA Plugin** in the required folder on your host system.

2. Install the containerized IntelliFlash SRA plugin in the paired SRM sites.

To install the containerized IntelliFlash SRA plugin, perform the following steps:

- a) Log in to the **vSphere Client**.
- b) Click **Menu** and select **Site Recovery**.
- c) In the **Site Recovery** page, click **Configure**.  
This takes you to **VMware SRM Appliance Management** site.
- d) Log in to the **SRM Appliance Management** site.
- e) In the left navigation pane, select **Storage Replication Adapters** and then click **New Adapter**.
- f) Click **Upload** and then choose IntelliFlash SRA 2.0.0 installer (**.tar.gz** file) downloaded earlier.  
You receive a notification on SRA upload.
- g) Repeat the above steps on the other SRM site.

This installs IntelliFlash SRA plugin in both the SRM sites and you discover SRA on both the sites. If you do not discover SRA, then rescan.

## Uninstalling Containerized IntelliFlash SRA 2.0.0 Plugin

1. Log in to the **vSphere Client**.
2. Click **Menu** and select **Site Recovery**.
3. In the **Site Recovery** panel, click **Configure**.

This takes you to **VMware SRM Appliance Management** site.

4. Log in to the **SRM Appliance Management** site
5. In the left navigation pane, select **Storage Replication Adapters**.
6. Click **(More)** icon  in the **IntelliFlash Storage Replication Adapter** section and choose **Delete**.
7. In the **Delete Adapter** dialog box, select both the check boxes and then click **Delete**.

This deletes the IntelliFlash Storage Replication Adapter. A confirmation message appears after the SRA is deleted.

## Configuring Array Managers in VMware Site Recovery Manager (SRM)

---

Add IntelliFlash systems to your SRM Server so that the SRM Server can discover replicated devices, compute datastore groups, and initiate storage operations. You can use the VMware vSphere Web client to add both IntelliFlash systems at the same time.

Depending on the version of the VMware Site Recovery Manager (SRM) you are using, some of the steps might vary. Refer to VMware product documentation for additional information.

### Prerequisites

- IntelliFlash SRA Plugin is installed.
- After setting up the replication relationship with the SRM Partner replication role, you must ensure that one successful run of replication is complete before adding IntelliFlash systems to the SRM.

To configure Array Managers, complete the following steps:

1. Log in to the VMware vSphere Web Client of your protected or recovery site (you can log into either one).
2. In the left hand side navigator, click **Site Recovery**.
3. In the **Site Recovery** panel, click **Sites**.
4. Right-click a site and select **Add Array Manager**.
5. In the **Add Array Manager** window, select **Add a pair of array managers** and click **Next**.
6. In the **Location** page, click **Next**.
7. Select the **IntelliFlash Storage Replication Adapter** from the **SRA Type** dropdown and click **Next**.
8. In the **Configure array manager** page, complete the following steps:

- a) Type a name for the array in the **Display Name** text box.
  - b) Type the array management IP address of the replication source system in the **Host** text box.
  - c) Type the **Username** of the replication source system.  
The Username can be the IntelliFlash admin username or the SRA role user account created in the IntelliFlash Web UI.
  - d) Type **Password** for the replication source system.
  - e) Click **Next**.
9. In the **Configure paired array manager** page, complete the following steps:
    - a) Type a name in the **Display Name** text box.
    - b) Type the Array management IP address of replication target system in the **Host** text box.
    - c) Type the **Username** of the replication target system.
    - d) Type **Password** for the replication target system.
    - e) Click **Next**.
  10. In the **Enable array pairs** page, select Array pair.
  11. Review the configuration and click **Finish**.

## Discovering Devices in Site Recovery Manager

---

You can rescan arrays if you made changes in the IntelliFlash configuration or added new arrays.

 **Note:** Every time you add a LUN and mount it, you must rerun replication and rescan.

Depending on the version of the VMware Site Recovery Manager (SRM) you are using, some of the steps might vary. Refer to VMware product documentation.

To rescan IntelliFlash systems, complete the following steps:

1. In the vSphere Web Client, click **Home > Recovery Site > Protected and Recovery Site > Array Based Replication**.
2. Select an array
3. In the **Manage** tab, select **Array Pairs**.
4. Right-click an array pair and select **Discover Devices** to rescan the arrays and recompute the datastore groups.

## Create, Test, and Run Recovery Plan

---

After configuring array managers and discovering devices in VMware Site Recovery Manager, you should create a protection group, a recovery plan, test the recovery plan, clean up the test, and then test a recovery plan for planned recovery and disaster recovery. You can also reprotect after a planned or disaster recovery.

For more information about VMware Site Recovery Manager, refer to the VMware product documentation:

<https://docs.vmware.com/en/Site-Recovery-Manager/index.html>

## Create Array Based Replication Protection Group

---

When you create a protection group, the **Protection group** type page of the **Create Protection Group** wizard of the **SRM Server** displays the IntelliFlash system pair in the **Array pair** section. In the wizard, you must select the **Array Based Replication** option.

## Create a Recovery Plan

---

When you create a recovery plan, you should select the recovery site that has the replication target array added.

## Perform a Planned Recovery or Disaster Recovery

---

When you perform a planned recovery, IntelliFlash takes the latest snapshot from the IntelliFlash system on the protected site array and replicates it to the replication target array on the recovery site. It also moves the project from the **Local** to the **Replica** tab of the project pane and stops the data service.

On the recovery site array, IntelliFlash moves the project from the **Replica** to the **Local** tab of the project pane and starts the data service.

When you perform a disaster recovery, on the recovery site array, IntelliFlash moves the project from the **Replica** to the **Local** tab of the project pane and starts the data service.

## Reprotect After Recovery

---

The reprotect operation reverses the replication direction, and the replication exits the suspended state and allows a future replication to execute.

Your recovery site becomes the new protected site and your replication target array becomes your replication source array.

---

# Chapter 30

---

## IntelliFlash Plugin for Veeam Backup and Replication

---

### Topics:

- [\*About IntelliFlash Plugin for Veeam Backup and Replication\*](#)
- [\*How the IntelliFlash Plugin for Veeam Backup and Replication works\*](#)
- [\*Tasks you can perform using the IntelliFlash Plugin for Veeam Backup and Replication\*](#)
- [\*Prerequisites for using the IntelliFlash Plugin for Veeam Backup and Replication\*](#)
- [\*Adding a Veeam User Account on the IntelliFlash Array\*](#)
- [\*Downloading the IntelliFlash Plugin for Veeam Backup and Replication\*](#)
- [\*Installing IntelliFlash Plugin for Veeam Backup and Replication\*](#)
- [\*Adding IntelliFlash Array to IntelliFlash Plugin for Veeam Backup and Replication\*](#)
- [\*Remove the array using the IntelliFlash Plugin for Veeam Backup and Replication\*](#)

## About IntelliFlash Plugin for Veeam Backup and Replication

---

The IntelliFlash Plugin for Veeam Backup and Replication enables you to add IntelliFlash arrays to the Veeam server and perform backup and restore operations for VMware virtual machines.

The plugin creates snapshots of the virtual machines on the IntelliFlash Array for backup and restore operations to provide VM-consistent and application-consistent snapshots of the VMware VMs. Using the navigation pane in the Veeam application, you can browse individual storage snapshots of virtual machines and restore them.

### **Supported Veeam version**

The IntelliFlash Plugin for Veeam Backup and Replication is supported on *Veeam Back up and Replication version 9.5 Update 4b* and later.

### **Related Topics**

[Adding Veeam User Account](#)

[How the IntelliFlash Plugin for Veeam Backup and Replication works](#)

[Tasks you can perform using the IntelliFlash Plug-In for Veeam Backup and Replication](#)

[Installing IntelliFlash Plug-In for Veeam Backup and Replication](#)

## How the IntelliFlash Plugin for Veeam Backup and Replication works

---

The IntelliFlash Plugin for Veeam Backup and Replication backs up VMware virtual machines that are using NFS shares, iSCSI, and FC LUNs from the IntelliFlash Array to a secondary storage device, backup device, or direct-attached storage.

The Veeam software considers all storage objects (shares and LUNs) as volumes.

You can download the plugin from the Veeam website and install it on the system running the Veeam server.

After installing the IntelliFlash Plugin for Veeam Backup and Replication, you can add the IntelliFlash Array to establish a connection between the Veeam server and the IntelliFlash Array. When adding the IntelliFlash Array, you can select the NFS shares and LUNs for the plugin to back up the VMs that are using these shares and LUNs.

The plugin scans the selected shares and LUNs and creates temporary clones of the snapshots on the array to find the VMs. After finding the VMs, the temporary clones are deleted.

The plugin creates Veeam-specific snapshots when you schedule a backup task or take a manual snapshot. These snapshots are stored on the IntelliFlash Array. The plugin uses these Veeam-specific snapshots for restoring the VMs.

The plugin also enables you to create manual snapshots of the VMs.

### **Veeam Snapshots**

When you use the IntelliFlash Plugin for Veeam Backup and Replication to back up your VMware virtual machines, you can view veeam-specific snapshots in the IntelliFlash Web UI. The plugin

creates Veeam production snapshots and Veeam manual snapshots on the IntelliFlash Array using array level snapshots.

### Veeam Production snapshots

The Veeam-production snapshots are the automatic snapshots created as part of planned backup operations scheduled using the plugin from the Veeam application.

**Example of a Veeam-Production snapshot:** *Unmanaged snapshot: "Veeam-Production-fullsnapbackup-2019-05-03To05:54:18.833-07:00"*

### Veeam manual snapshots

The plugin also provides you the option to take a manual snapshot of VMware virtual machines from the Veeam application. You can view these manual snapshots from the IntelliFlash Web UI. You can use these manual snapshots for restoring your virtual machines using the plugin.

**Example of a Veeam-manual snapshot:** *Unmanaged snapshot: "Veeam-Manual-my-manual-2019-05-03To05:20:29.818-07:00"*

In the IntelliFlash Web UI, the Veeam production snapshots and Veeam manual snapshots appear in the **LUN Snapshots** and **Share Snapshots** screens of the respective LUNs and shares along with regular snapshots.

## Tasks you can perform using the IntelliFlash Plugin for Veeam Backup and Replication

---

Using the IntelliFlash Plugin for Veeam Backup and Replication, you can perform the following tasks on the Veeam Back up and Replication software:

- Add and remove IntelliFlash systems
- Schedule backup jobs for VMware virtual machines for datastores that are using IntelliFlash systems
- Create a manual snapshot of the VMs
- Perform full backup of volumes
- Rescan the snapshots
- Restore an entire VM
- File level restore from full backup or storage snapshot
- Instant VM recovery
- Full restore
- Restore disks

### Related Topics

[Adding Veeam User Account](#)

[How the IntelliFlash Plugin for Veeam Backup and Replication works](#)

[Tasks you can perform using the IntelliFlash Plug-In for Veeam Backup and Replication](#)

[Installing IntelliFlash Plugin for Veeam Backup and Replication](#) on page 567

## Prerequisites for using the IntelliFlash Plugin for Veeam Backup and Replication

---

The following are the prerequisites for installing and registering the plugin:

- IntelliFlash Web UI 3.9.2.0 or 3.10.1.0 and later
- Veeam Back up and Replication version 9.5 Update 4b or later
- If you have an FC environment, on the IntelliFlash Array, add FC initiators of the Veeam Server
- Add Veeam proxies specific iSCSI and FC initiators and initiator groups on the IntelliFlash Array. Create one initiator group for one Windows host.
- Download the IntelliFlash Plugin for Veeam Backup and Replication from the <https://www.veeam.com/backup-replication-download.html> website.
- When scheduling a backup job, you should select the **IntelliFlash Snapshot (Primary Storage Snapshot only)** as the backup repository to have snapshots stored in the IntelliFlash Array.
- If you want to back up data to a secondary storage using the plugin, you should select the default backup repository.
- To back up to a secondary repository, you must have the Veeam Enterprise Plus license.
- All license levels of Veeam are included for the ability to create a primary storage snapshot only backup.

### Related Topics

[Downloading the IntelliFlash Plug-In for Veeam Backup and Replication](#)

[Installing IntelliFlash Plug-In for Veeam Backup and Replication](#)

[Adding IntelliFlash Array on IntelliFlash Plug-In for Veeam Backup and Replication](#)

## Adding a Veeam User Account on the IntelliFlash Array

---

IntelliFlash provides a default Veeam role with defined privileges for the plugin administrator to access the IntelliFlash Array. You can create a user account on the IntelliFlash Web UI and assign the default Veeam role to the user account.

To add a Veeam user role, complete the following steps:

1. Click **Settings > Administration > Management Access**.
2. In the **Local Admins** tab, click **Add**.

The **User Account** dialog box appears.

3. Type a name in the **Username** box.
4. Type a password in the **Password** box.
5. Type the password again in the **Confirm Password** box.
6. (Optional) Provide a description in the **Description** box.
7. Click **Enable** to activate the user account.
8. In the **Roles** tab, select the **veeam** role for the user account.
9. Click **Save**.

## Downloading the IntelliFlash Plugin for Veeam Backup and Replication

---

To download the plugin from the Veeam website, complete the following steps:

1. Go to this download page: <https://www.veeam.com/backup-replication-download.html>.
2. If not already logged in, log in with your Veeam login credentials to access the page.
3. Follow the on screen steps to download the IntelliFlash Plugin for Veeam Backup and Replication.

### Related Topics

[Prerequisites for using the IntelliFlash Plug-In for Veeam Backup and Replication](#)

[Installing IntelliFlash Plug-In for Veeam Backup and Replication](#)

[Adding IntelliFlash Array on IntelliFlash Plug-In for Veeam Backup and Replication](#)

## Installing IntelliFlash Plugin for Veeam Backup and Replication

---

The [Veeam Help Center provides](#) provides the details for how to install IntelliFlash Plugin for Veeam Backup and Replication.

To install the IntelliFlash Plugin for Veeam Backup and Replication, complete the following step:

Access the Veeam Help Center documentation and follow the instructions to install the plugin: [Veeam Help Center provides](#).

### Related Topics

[Prerequisites for using the IntelliFlash Plug-In for Veeam Backup and Replication](#)

[How the IntelliFlash Plugin for Veeam Backup and Replication works](#)

*Tasks you can perform using the IntelliFlash Plug-In for Veeam Backup and Replication*

## Adding IntelliFlash Array to IntelliFlash Plugin for Veeam Backup and Replication

---

### Prerequisites

*Prerequisites for using the IntelliFlash Plug-In for Veeam Backup and Replication*

To add the IntelliFlash Array, complete the following steps:

1. Log in to the Veeam application.
2. In the lower section of the inventory pane, click the **STORAGE INFRASTRUCTURE** button.
3. In the **STORAGE INFRASTRUCTURE** view of the inventory pane, click the **Storage Infrastructure** node.
4. In the working area, click **Add Storage**.
5. In the **Add Storage** window, navigate to IntelliFlash from the list.
6. In the IntelliFlash Storage window, complete the following steps:
  - a) Type the array management IP address of the IntelliFlash Array or DNS name.
  - b) (Optional) Provide description for the array.
  - c) Click **Next**.
  - d) In the **Credentials** screen, click **Add** to provide array credentials.
  - e) Use the default port number 443.  
Do not change the port number.
  - f) Click **Next**.
  - g) In the **Access Options** screen, select the required protocols you want to use.  
Veeam supports the FC, iSCSI, and NFS protocols.
  - h) In the **Volumes to scan** field, click **Choose** and follow the instructions on the **Choose Volumes** window to select the volumes to scan.



**Note:** To save time, when scanning volumes for VMs, select shares or LUNs containing VMs that you want to back up using the Veeam software. Selecting all volumes might consume a lot of time to scan.

- a) In the **Back up proxies to use** field , click **Choose** and follow instructions the on the **Back up proxies** window.
- b) Click **Next**.
- c) In the **Summary** screen, review the summary and click **Finish**.

### Related Topics

[How the IntelliFlash Plugin for Veeam Backup and Replication works](#)

[Tasks you can perform using the IntelliFlash Plug-In for Veeam Backup and Replication](#)

## Remove the array using the IntelliFlash Plugin for Veeam Backup and Replication

---

When you remove the array from the storage infrastructure, the plugin deletes all temporary Veeam snapshots, clones, iSCSI mappings, and disconnects the connection. However, the plugin retains the production snapshots on the IntelliFlash Array created by the plugin as part of scheduled backup operations.

To remove the IntelliFlash Array registered with the plugin, complete the following steps:

1. Log in to the Veeam application.
2. In the lower section of the inventory pane, click the **STORAGE INFRASTRUCTURE** button.
3. In the **STORAGE INFRASTRUCTURE** view of the inventory pane, click the **Storage Infrastructure** node.
4. Right-click the array name or IP address in the inventory pane and select **Remove storage**.
5. In the **Veeam Backup and Replication** confirmation window, click **Yes**.

### Related Topics

[How the IntelliFlash Plug-In for Veeam Backup and Replication works](#)

[Tasks you can perform using the IntelliFlash Plug-In for Veeam Backup and Replication](#)

[Installing IntelliFlash Plug-In for Veeam Backup and Replication](#)

[Adding IntelliFlash Array on IntelliFlash Plug-In for Veeam Backup and Replication](#)



---

# Chapter 31

---

## IntelliFlash NAS VAAI Plugin for VMware

---

**Topics:**

- *IntelliFlash NAS VAAI Plugin for VMware*
- *Managing the IntelliFlash NAS VAAI Plugin*

## IntelliFlash NAS VAAI Plugin for VMware

Integration of the VMware vSphere Storage APIs for Array Integration (VAAI) with IntelliFlash establishes communication between VMware hosts and an IntelliFlash Array.

VMware vSphere Storage APIs for Array Integration (VAAI) is a set of primitives provided by VMware for storage vendors. The primitives help in managing the VMware I/O efficiently.

The IntelliFlash NAS VAAI Plugin for VMware plugin enables the offloading of some storage-related operations to the IntelliFlash Array, thereby improving the performance of the VMware host.

You can install the IntelliFlash NAS VAAI Plugin on an ESXi Server after you add a vCenter Server that manages ESXi Servers. You can install, upgrade, and uninstall the IntelliFlash NAS VAAI Plugin for VMware on a VMware ESXi Server from the IntelliFlash Manager plugin or using the ESXi Server CLI.

You can also install the IntelliFlash NAS VAAI Plugin using vSphere Update Manager (VUM).

 **Note:** IntelliFlash allows you to install the plugin on multiple ESXi Servers or you can install the plugin on a single ESXi Server.

The IntelliFlash NAS VAAI Plugin version bundled with IntelliFlash 3.7.x.x and later is a **VMwareAccepted** acceptance level plugin. However, the IntelliFlash NAS VAAI Plugin versions bundled with older IntelliFlash versions are **PartnerSupported**.

### Download IntelliFlash NAS VAAI Plugin

You can download the IntelliFlash NAS VAAI Plugin from the **Plugins** page under **NAS VAAI** section of the IntelliFlash Web UI (**Settings > Administration > Plugins**).

 **Note:** The plugin is supported on VMware ESXi 7.0 and later versions.

### IntelliFlash NAS VAAI Plugin Limitations

The IntelliFlash NAS VAAI Plugin has the following limitations:

- The plugin supports a maximum of 64 concurrent clones.
- The plugin does not offload the cloning operations from an ESXi Server to an IntelliFlash Array if a quiesce-enabled replication relationship's schedule on a source IntelliFlash Array coincides with VM cloning operations on the ESXi Server.
- The plugin does not offload the cloning operations from an ESXi Server to an IntelliFlash Array if quiesced snapshots scheduled on an IntelliFlash Array coincide with VM cloning operations on the ESXi Server.

### Supported NAS VAAI Primitive

The IntelliFlash NAS VAAI Plugin supports the Full File Clone or Full Copy NAS VAAI primitive and Fast File Clone.

The VAAI Full File Clone primitive offloads the cloning operation of the virtual disks to the IntelliFlash Array and reduces the ESXi Server usage of CPU, memory, and network bandwidth.

## Managing the IntelliFlash NAS VAAI Plugin

---

You can install, upgrade, and uninstall the plugin on an ESXi Server using any of following methods:

- IntelliFlash Web UI
- IntelliFlash Manager plugin
- ESXi Server CLI
- vSphere Update Manager (VUM).

### Prerequisites for Installing the IntelliFlash NAS VAAI Plugin

To install the IntelliFlash NAS VAAI Plugin on an ESXi Server, ensure to meet the following prerequisites:

- IntelliFlash version 2.1.2 or later is running on your IntelliFlash System.
- You have added a VMware vCenter Server that is managing ESXi Servers to IntelliFlash. If you do not use a VMware vCenter Server, you can directly install the plugin using the ESXi Server CLI.
- You are running VMware ESXi Server 7.0 or a later version.
- SSH is enabled on the ESXi Server
- The Host Acceptance Level is PartnerSupported (VMwareAccepted for version 1.0-15.67 and higher versions bundled with IntelliFlash 3.7.x.x. and later)
- The NFS Server Maximum version is set to 4.0 or higher.



**Note:** You can set the value from the **NFS Server Configuration** page (**Services > NAS > NFS**).

### Related Topics

[Adding a vCenter Server](#)

### Installing IntelliFlash NAS VAAI Plugin using IntelliFlash Manager plugin

You can use the IntelliFlash Manager plugin to install or upgrade the IntelliFlash NAS VAAI Plugin on ESXi servers.



**Note:** You must be logged in to the vSphere Client.

To install the VAAI Plugin using the IntelliFlash Manager plugin, complete the following steps:

1. Log in to the **vSphere Client**.
2. Click **Menu > IntelliFlash Manager > Host settings**.
3. Go to **ACTIONS**.
4. Under **VAAI**, click **Install**.
  - a) In the **Install VAAI** window that appears, select the **ESXi host** from the drop-down list.

- b) Click **Install**.



**Note:** Reboot the ESXi host for the changes to take effect.

## Uninstalling the IntelliFlash NAS VAAI Plugin using IntelliFlash Manager plugin

You can use the IntelliFlash Manager plugin to uninstall the IntelliFlash NAS VAAI Plugin on ESXi servers.

You must be logged in to the **vSphere Client**.

To uninstall the VAAI Plugin using the IntelliFlash Manager plugin, complete the following steps:

1. Log in to the **vSphere Client**.
2. Click **Menu > IntelliFlash Manager > Host settings**.
3. Click **ACTIONS** or click the menu button next to the host that you want to uninstall.
4. Under **VAAI**, click **UNINSTALL**.



**Note:** Reboot the ESXi host for the changes to take effect.

## Installing IntelliFlash NAS VAAI Plugin Using the ESXi Server CLI

To install the IntelliFlash NAS VAAI Plugin using the ESXi Server CLI, complete the following steps:

1. You need to first copy the plugin binary from the IntelliFlash systems to any folder on the ESXi Server. The location of the plugin file on the array is `/zebi/apps/vaai-nas/tgl-vaai-nas-diskplugin.vib`.  
After copying this file to a folder (COPIED\_DIR\_PATH in this example) use the ESXi Server CLI to complete the following steps.
2. On the ESXi Server, set the software acceptance level to **PartnerSupported** or **VMwareAccepted**(for version 1.0-15.67), using this command:

```
# esxcli software acceptance set --level=PartnerSupported.
```



**Note:** The command output might vary according to the ESXi Server version and IntelliFlash NAS VAAI Plugin version.

The output of this command is as follows: **Host acceptance level changed to 'PartnerSupported' or VMwareAccepted**.



**Note:** The installation requires a reboot to complete. You should perform this operation in a maintenance mode.

3. Install the IntelliFlash NAS VAAI Plugin.

```
For PartnerSupported # esxcli software vib install --
viburl="file:COPIED_DIR_PATH/tgl-vaaai-nas-diskplugin.vib" --no-sig-
check
```

```
For VMwareAccepted # esxcli software vib install --
viburl="file:COPIED_DIR_PATH/tgl-vaaai-nas-diskplugin.vib"
```

The output of this command is as follows: Installation Result Message:  
The update completed successfully, but the system needs to be rebooted for the changes to be effective. Reboot Required: true  
VIBs Installed: Tegile\_bootbank\_tgl-vaaai-nas-diskplugin\_1.0-14 VIBs  
Removed: VIBs Skipped:

4. Reboot the ESXi Server.

5. Run the following command to confirm the installation.

```
~ # esxcli software vib get -n tgl-vaaai-nas-diskplugin
```

The output of this command is as follows:

```
Tegile_bootbank_tgl-vaaai-nas-diskplugin_1.0-14
Name: tgl-vaaai-nas-diskplugin
Version: 1.0-14
Type: bootbank
Vendor: Tegile
Acceptance Level: VMware Accepted
```

```
Summary: Tegile VAAI NAS Plugin
Description: Tegile VAAI NAS Disk Plugin
Reference URLs:
Creation Date: 2014-01-14
Depends:
Conflicts:
Replaces:
Provides:
Maintenance Mode Required: False
Hardware Platforms Required:
Live Install Allowed: False
Live Remove Allowed: False
Stateless Ready: False
Overlay: False
Tags:
Payloads: tgl-vaaai-nas-di
~ #
```

 **Note:** The command output might vary according to the ESXi Server version and IntelliFlash NAS VAAI Plugin version.

You can also confirm that the plugin has installed by using this command:  
`# esxcli software vib list | grep tgl`

The output of this command is as follows:

```
tgl-vaaai-nas-diskplugin 1.0-14
Tegile VMwareAccepted 2014-01-11
```

## Installing the IntelliFlash NAS VAAI Plugin using the VMware vSphere Update Manager

You can install the IntelliFlash NAS VAAI Plugin using VMware vSphere Update Manager (VUM). You need to download the plugin from the IntelliFlash Web UI and use the Update Manager to install.

1. Download the IntelliFlash NAS VAAI Plugin from **Settings > Administration > Plugins > NAS VAAI**.
2. Click **Download** and save the file.
3. Complete the installation procedure using the Update Manager.  
Refer to the VMware documentation for the procedure.

[https://docs.vmware.com/en/VMware-vSphere/5.5/com.vmware.vsphere.update\\_manager.doc/GUID-BBD753EE-6E80-40A6-A212-F7251B5ADF31.html](https://docs.vmware.com/en/VMware-vSphere/5.5/com.vmware.vsphere.update_manager.doc/GUID-BBD753EE-6E80-40A6-A212-F7251B5ADF31.html)

## Uninstalling the IntelliFlash NAS VAAI Plugin using the ESXi Server CLI

To uninstall the IntelliFlash NAS VAAI Plugin using the ESXi Server CLI, complete the following steps:

1. To uninstall the plugin, run the following command:

```
# esxcli software vib remove -n tgl-vaaai-nas-diskplugin
```

The output of this command is as follows:

```
Removal Result
Message: The update completed successfully, but the system needs to
be rebooted for the changes to be effective.
Reboot Required: true
VIBs Installed:
VIBs Removed: Tegile_bootbank_tgl-vaaai-nas-diskplugin_1.0-11
VIBs Skipped:
```

2. Reboot the ESXi server.

```
#reboot
```



**Caution:** You must cautiously select the ESXi Servers for reboot. It is recommended that you uninstall the plugin when ESXi hosts are in maintenance mode.

---

# Chapter 32

---

## Cloud Connect

---

**Topics:**

- *Backing up Data to S3-Compliant Cloud Targets*
- *Terms Used in Cloud Connect*
- *Uses of Cloud Connect for Backup*
- *Configuring Cloud Connect*
- *Managing Active Backups*
- *Restoring Cloud Backup of a Specific Project Within the Same Array*
- *Restoring Cloud Backups Within the Same Array*
- *Restoring Cloud Backups to a Different Array*
- *Backing up and Restoring Data through 10G Interfaces*
- *Deleting a Cloud Backup*

## Backing up Data to S3-Compliant Cloud Targets

**Cloud Connect** helps back up snapshots of a project, share, or LUN to an S3-compliant cloud target and to restore the snapshots back to the same IntelliFlash system or a different IntelliFlash system.

An S3-compliant cloud target allows access to the data that it stores over an AWS Simple Storage Service (S3) compliant interface. **Cloud Connect** supports S3-compliant cloud targets such as ActiveScale targets, AWS targets, or any custom S3-compliant cloud targets.

Using the IntelliFlash Web UI, you can back up data to the S3-compliant target either manually or through a schedule. You can also decide options for retention of backups in the cloud target.

Backups on an S3 target are not human readable. Use the IntelliFlash Web UI to manage the backups to the cloud target. When you want to initiate a restore, you can select from among the most recent full backups to get to the desired point in time.

 **Note:** Tintri recommends backing up only local projects to S3-compliant cloud targets.

## Terms Used in Cloud Connect

### Bucket

A bucket is a container for storing the backup data on the cloud. To create a bucket, you specify a unique name, the geographical location where the bucket will be stored, and the credentials to write to it.

### S3-Compliant Cloud Target

A bucket and the credentials to write to it constitute a cloud target. An S3-compliant cloud target allows access to the data that it stores over an AWS Simple Storage Service (S3) compliant interface.

IntelliFlash Cloud Connect supports S3-compliant cloud targets such as AWS and ActiveScale to back up projects, shares or LUNs from the IntelliFlash system.

## Uses of Cloud Connect for Backup

Backing up to S3-compliant cloud targets through Cloud Connect is useful for the following cases:

- As a backup target supplemental to a standard replication schedule. The cloud backup target can play the role of an offsite disaster recovery target when an offsite IntelliFlash system is not available. You can use the backup from the original unavailable array and restore it to a new IntelliFlash system.

- When you require data older than the data locally available in the IntelliFlash system.
- When a private, local ActiveScale system is used as a backup target, that ActiveScale system can be configured with multi-site resiliency and offer both local and offsite disaster recovery capabilities in one package.

## Configuring Cloud Connect

---

To back up data of a project, share, or LUN from the IntelliFlash system to an S3 cloud target, you must first add the cloud target through the IntelliFlash Web UI. After adding the S3-compliant cloud target, configure the backup for the project.

### Adding a Cloud Target

The IntelliFlash Web UI enables you to add any of the following S3-compliant targets:

- AWS
- ActiveScale
- Custom

### Adding a Bucket

When adding a cloud target, first create a bucket. A bucket holds the backup snapshots. To create a bucket, you specify a unique name, the geographical location where the bucket will be stored (for AWS and custom targets), and the credentials to write to it. The bucket along with the region and credentials constitutes the cloud target.

### Bucket Naming Requirements

The rules for adding a bucket name are as follows:

- The bucket name can be between 3 and 63 characters long.
- The bucket name can contain only lower-case characters, numbers, periods, and dashes.
- The bucket name must start with a lowercase letter or number.
- The bucket name cannot contain underscores, end with a dash, have consecutive periods, or use dashes adjacent to periods.
- The bucket name cannot be formatted as an IP address (for example, 198.10.10.10).

### Adding an ActiveScale Target

To add an ActiveScale target, do the following:

1. Click **Services > Cloud Connect > Cloud Targets**.
2. In the **Cloud Targets** page, click **Add**.

The **Cloud Backup** window appears.

3. Provide a name for the target in the **Target Alias** field.
  4. Select **ActiveScale** from the **Target Type** list.
  5. Create a new bucket or select an existing bucket by doing the following:
    - a) Select **New** to create a new bucket or select **Existing** to use an existing bucket.
    - b) Enter a unique name (for a new bucket) or an existing bucket name in the **Bucket Name** field.
    - c) Enter the access key ID in the **Access Key** field.
    - d) Enter the secret access key in the **Secret Key** field.
  6. Click **Next**.
- The **Endpoints** screen appears.
7. Enter the IP address of the primary ActiveScale target in the **Primary** field and click **Add**.

 **Note:**

- You can add multiple ActiveScale targets.
- If you are adding the host name of the target, the valid format is as follows:

```

hostname
hostname.domain.com
hostname:443
hostname.domain.com:443
http://hostname
http://hostname.domain.com
https://hostname
https://hostname.domain.com
https://hostname:443
https://hostname.domain.com:443
  
```

- If you are adding the IP address of the target, the valid format is as follows:

```

<IP address of the ActiveScale target>. For example,
10.204.88.158.
<IP address of the ActiveScale target:8282>. For example,
10.204.88.158:8282.
<IP address of the ActiveScale target:443>. For example,
10.204.88.158:443.
http://<IP address of the ActiveScale target>. For example,
http://10.204.88.158.
https://<IP address of the ActiveScale target>. For example,
https://10.204.88.158.
https://<IP address of the ActiveScale target:443>. For example,
https://10.204.88.158:443.
  
```

- Cloud Connect performs a round-robin request between the configured primary endpoints. If one primary endpoint is not available, Cloud Connect stops using it temporarily and retries connecting to it every 5 minutes.

8. Enter the IP address of the secondary ActiveScale target in the **Secondary** field and click **Add**.

9. Click **Next**.

The **Summary** screen appears.

10. Review the information and click **Add**.

The new cloud target is listed in the **Cloud Targets** page.

### Adding an AWS Target

To add an AWS target, do the following:

1. Click **Services > Cloud Connect > Cloud Targets**.

2. In the **Cloud Targets** page, click **Add**.

The **Cloud Backup** window appears.

3. Provide a name for the target in the **Target Alias** field.

4. Select **AWS** from the **Target Type** list.

5. Create a new bucket or select an existing bucket by doing the following:

a) Select **New** to create a new bucket or select **Existing** to use an existing bucket.

b) Enter a unique name (for a new bucket) or an existing bucket name in the **Bucket Name** field.

c) Select the geographical region from the **Select Region** list.

d) Enter the access key ID in the **Access Key** field.

e) Enter the secret access key in the **Secret Key** field.

6. Click **Next**.

The **Summary** screen appears.

7. Review the information and click **Add**.

The new cloud target is listed in the **Cloud Targets** page.

### Adding a Custom Cloud Target

To add a custom S3-compliant custom cloud target, do the following:

1. Click **Services > Cloud Connect > Cloud Targets**.

2. In the **Cloud Targets** page, click **Add**.

The **Cloud Backup** window appears.

3. Provide a name for the target in the **Target Alias** field.
4. Select **Custom** from the **Target Type** list.
5. Create a new bucket or select an existing bucket by doing the following:
  - a) Select **New** to create a new bucket or select **Existing** to use an existing bucket.
  - b) Enter a unique name (for a new bucket) or an existing bucket name in the **Bucket Name** field.
  - c) Enter the geographical location in the **Region Name** field.
  - d) Enter the access key ID in the **Access Key** field.
  - e) Enter the secret access key in the **Secret Key** field.
6. Click **Next**.

The **Endpoints** screen appears.

7. Enter the IP address of the primary S3 target in the **Primary** field and click **Add**.

 **Note:**

- You can add multiple targets.
- If you are adding the host name of the target, the valid format is as follows:

```

hostname
hostname.domain.com
hostname:443
hostname.domain.com:443
http://hostname
http://hostname.domain.com
https://hostname
https://hostname.domain.com
https://hostname:443
https://hostname.domain.com:443
  
```

- If you are adding the IP address of the target, the valid format is as follows:

```

<IP address of the ActiveScale target>. For example,
10.204.88.158.
<IP address of the ActiveScale target:8282>. For example,
10.204.88.158:8282.
<IP address of the ActiveScale target:443>. For example,
10.204.88.158:443.
http://<IP address of the ActiveScale target>. For example,
http://10.204.88.158.
https://<IP address of the ActiveScale target>. For example,
https://10.204.88.158.
https://<IP address of the ActiveScale target:443>. For example,
https://10.204.88.158:443.
  
```

- Cloud Connect performs a round-robin request between the configured primary endpoints. If one primary endpoint is not available, Cloud Connect stops using it temporarily and tries reconnecting to it every 5 minutes.

8. Enter the IP address of the secondary S3 target in the **Secondary** field and click **Add**.
9. Click **Next**.  
The **Summary** screen appears.
10. Review the information and click **Add**.

The new cloud target is listed in the **Cloud Targets** page.

## Configuring Backup for a Project

A project cannot have multiple cloud backup configurations to the same S3 target. However, a project can back up to multiple cloud targets available in different regions.



**Note:** Tintri recommends backing up only local projects to S3-compliant cloud targets.

To configure backup for a project, do the following:

1. Click **Provision > Projects**.
2. In the **Local** tab, select the project you want to back up.
3. Click **Manage > Data Protection > Cloud Connect**.
4. In the **Cloud Connect** tab, click **Add**.  
The **New Backup Schedule** window appears.
5. In the **Target** screen, select the target from the **Select Target** list.  
If no targets are available, add a cloud target in the **Services > Cloud Connect > Cloud Targets** page.
6. Click **Next**.
7. In the **Scope** screen, you can select the shares or LUNs you want to include or exclude from the backup.
  - **All:** Select this option to include all the shares or LUNs in the project for backup.
  - **Include:** Select **Include** and then individually select the shares or LUNs from the list that you want to include for backup.
  - **Exclude:** Select **Exclude** and then individually select the shares or LUNs from the list that you want to exclude from backup.
8. In the **Schedule** screen, select from the following schedules for full and incremental backups.

Option	Steps
<b>Monthly-Weekly</b>	<ul style="list-style-type: none"> <li>Select this option when you want a full backup every month and an incremental backup every week.</li> <li>In the <b>Full backups monthly</b> and <b>Incremental backups weekly</b> fields that appear, enter the frequency of the schedule.</li> <li>Click the hyperlink text next to the <b>Full backups monthly</b> and <b>Incremental backups weekly</b> fields.</li> <li>In the <b>Options</b> dialog box, select the exact day of the month or week (use the calendar to specify the date or use the UI controls to select which day of the month or week you want the backup to start).</li> <li>Select the exact time.</li> <li>Click <b>Apply</b>.</li> </ul>
<b>Monthly-Daily</b>	<ul style="list-style-type: none"> <li>Select this option when you want a full backup every month and an incremental backup every day.</li> <li>In the <b>Full backups monthly</b> and <b>Incremental backups daily</b> fields that appear, enter the frequency of the schedule.</li> <li>Click the hyperlink text next to the <b>Full backups monthly</b> and <b>Incremental backups daily</b> fields.</li> <li>In the <b>Options</b> dialog box, select the exact day (use the calendar to specify the date or use the UI controls to select which day of the month or week you want the backup to start).</li> <li>Select the exact time.</li> <li>Click <b>Apply</b>.</li> </ul>
<b>Weekly-Daily</b>	<ul style="list-style-type: none"> <li>Select this option when you want a full backup every week and an incremental backup every day.</li> <li>In the <b>Full backups weekly</b> and <b>Incremental backups daily</b> fields that appear, enter the frequency of the schedule.</li> </ul>

Option	Steps
	<ul style="list-style-type: none"> <li>Click the hyperlink text next to the <b>Full backups weekly</b> and <b>Incremental backups daily</b> fields.</li> <li>In the <b>Options</b> dialog box, select the exact day (use the calendar to specify the date or use the UI controls to select which day of the week you want the backup to start).</li> <li>Select the exact time.</li> <li>Click <b>Apply</b>.</li> </ul>
<b>Weekly-Hourly</b>	<ul style="list-style-type: none"> <li>Select this option when you want a full backup every week and an incremental backup every hour.</li> <li>In the <b>Full backups weekly</b> and <b>Incremental backups hourly</b> fields that appear, enter the frequency of the schedule.</li> <li>Click the hyperlink text next to the <b>Full backups weekly</b> and <b>Incremental backups hourly</b> fields.</li> <li>In the <b>Options</b> dialog box, select the exact day (use the calendar to specify the date or use the UI controls to select which day of the week or for what duration during the day).</li> <li>Select the exact time.</li> <li>Click <b>Apply</b>.</li> </ul>
<b>Daily-Hourly</b>	<ul style="list-style-type: none"> <li>Select this option when you want a full backup every day and an incremental backup every hour.</li> <li>In the <b>Full backups daily</b> and <b>Incremental backups hourly</b> fields that appear, enter the frequency of the schedule.</li> <li>Click the hyperlink text next to the <b>Full backups daily</b> and <b>Incremental backups hourly</b> fields.</li> <li>In the <b>Options</b> dialog box, select the exact day (use the calendar to specify the date or use the UI controls to select which day or for what duration during the day).</li> <li>Select the exact time.</li> </ul>

Option	Steps
	<ul style="list-style-type: none"> <li>Click <b>Apply</b>.</li> </ul>

9. In the **Retention** section, select the number of full and incremental backups you want to retain in the cloud target:
- In the **Total full backups to retain** box, select the number of most recent full backups to retain.
  - In the **Retain Incremental** list, select whether to retain incremental backups for all the full backups or only for a selected number of the latest full backups.

 **Note:** Cloud Connect automatically deletes the older backups and retains only the specified number of latest full backups.

10. Click **Add**.

A new backup schedule appears in the **Cloud Target** page of the project. The backup configuration also appears in the **Services > Cloud Connect > Active Backups** page.

## Managing Active Backups

You can manage all the active cloud backups from the **Services > Cloud Connect > Active Backups** page in the IntelliFlash Web UI.

The active backups for a particular project can also be managed from the **Data Protection** page (**Provision > Projects > Local > Manage > Data Protection > Cloud Connect**).

### Viewing All Active Backups

To view all the active backups, do the following:

- Click **Services > Cloud Connect > Active Backups**.
- The **Active Backups** page displays all the existing backups.
- An active backup can display the following statuses:
  - In progress:** A progress bar appears when Cloud Connect is taking a backup and uploading the backup to the cloud target.
  - Paused:** This status appears when you manually interrupt an ongoing cloud backup by clicking the **Pause** button. You can resume the paused backup from the state where it was interrupted.
  - Stopped:** This status appears when you manually stop an ongoing cloud backup by clicking the **Abort** button. You can start a stopped backup again.
  - Failed:** This status appears when the cloud backup fails for any reason.

 **Note:** You can check the **Notifications** page for the reason of the failure.

- Complete:** This status appears after the backup is complete.

## Viewing Active Backups in a Specific Project

To view the active backups in a project, do the following:

1. Click **Provision > Projects**.
  2. In the **Local** tab, select the project.
  3. Click **Manage > Data Protection > Cloud Connect**.
  4. The **Cloud Connect** tab displays all the active backups in the project.
  5. An active backup can display the following statuses:
    - **In progress**: A progress bar appears when Cloud Connect is taking a backup and uploading the backup to the cloud target.
    - **Paused**: This status appears when you manually interrupt an ongoing cloud backup by clicking the **Pause** button. You can resume the paused backup from the state where it was interrupted.
    - **Stopped**: This status appears when you manually stop an ongoing cloud backup by clicking the **Abort** button. You can start a stopped backup again.
    - **Failed**: This status appears when the cloud backup fails for any reason.
-  **Note:** You can check the **Notifications** page for the reason of the failure.

  - **Complete**: This status appears after the backup is complete.

## Viewing Backup Configuration Details

To view backup configuration details, do the following:

1. Click **Services > Cloud Connect > Active Backups**.
2. Select a backup.  
The **Configuration** tab displays the configuration details of the backup.
3. To select a backup of a specific project, do the following:
  - a) Click **Provision > Projects** page.
  - b) In the **Local** tab, select the project.
  - c) Click **Manage > Data Protection > Cloud Connect**.
  - d) Select a backup.  
The **Configuration** tab displays the configuration details of the backup.
4. To view the statistics, click the **History** tab.  
The complete statistics of the backups appear, with details such as the number of completed backups, failed backups, and total backups (including full and incremental backups).

A graph under the **History** section displays the full and incremental backups that were completed for the scheduled dates.

5. To view a history of the previous backups in the chart, drag the Hand icon to the left in the **Timeline** bar.

## Starting Backups Manually

To start backups manually, do the following:

1. Click **Services > Cloud Connect > Active Backups**.
2. Select the backup.
3. Click **Start**.  
The **Manual Cloud Backup** window appears.
4. Select **Full** or **Incremental** backup type.
5. Click **Backup**.

IntelliFlash starts the backup to the cloud target and the progress bar appears indicating that the backup is in progress. After the backup is successfully completed, the status changes to **Complete**.

## Starting Backups Manually for a Specific Project

To start backups manually for a particular project, do the following:

1. Click **Provision > Projects**.
2. In the **Local** tab, select the project.
3. Click **Manage > Data Protection > Cloud Connect**.
4. Select the backup.
5. Click **Start**.  
The **Manual Cloud Backup** window appears.
6. Select **Full** or **Incremental** backup type.
7. Click **Backup**.

IntelliFlash starts the backup for the particular project. The progress bar appears indicating that the backup is in progress. After the backup is successfully completed, the status changes to **Complete**.

## Aborting Backups

You can abort an ongoing or failed backup. When you abort the backup, IntelliFlash stops the data transfer to the cloud target. Aborted backups restart automatically according to the schedule, or you can manually start the backup again.

To abort an ongoing or failed backup, do the following:

1. Click **Services > Cloud Connect > Active Backups**.
2. Select the failed or ongoing backup.
3. To select the backup configuration for a particular project, do the following:
  - a) Click **Provision > Projects** page.
  - b) In the **Local** tab, select the project.
  - c) Click **Manage > Data Protection > Cloud Connect**.
  - d) Select the failed or ongoing backup.
4. Click **Abort**.

IntelliFlash stops the backup to the cloud target and the status changes to **Stopped**.

## Pausing Backups

You can pause an ongoing backup. When you pause a backup, IntelliFlash temporarily stops uploading the snapshot to the cloud target. The **Status** field changes to **Paused**.

Paused backup will resume automatically according to the schedule, or you can manually restart the backup. When you resume a backup, it starts from the point where it was paused.

To pause an ongoing backup, do the following:

1. Click **Services > Cloud Connect > Active Backups**.
2. Select the backup.
3. To select the backup configuration for a particular project, do the following:
  - a) Click **Provision > Projects** page.
  - b) In the **Local** tab, select the project.
  - c) Click **Manage > Data Protection > Cloud Connect**.
  - d) Select the backup.
4. Click **Pause**.

IntelliFlash pauses the backup and the status changes to **Paused**.

## Resuming Paused Backups

Paused backup will resume automatically according to the schedule, or you can manually restart the backup. When you resume a backup, it starts from the point where it was paused.

To resume a backup, do the following:

1. Click **Services > Cloud Connect > Active Backups**.
2. Select the backup that has been paused.
3. To select the backup that has been paused for a particular project, do the following:
  - a) Click **Provision > Projects** page.
  - b) In the **Local** tab, select the project.
  - c) Click **Manage > Data Protection > Cloud Connect**.
  - d) Select the backup.
4. Click **Resume**.

IntelliFlash resumes the backup and the status changes to **Complete** after the backup is successfully uploaded to the cloud target.

## Deleting a Cloud Backup Configuration

To delete the backup configuration of a project from Cloud Connect, perform the following steps:

1. Click **Services > Cloud Connect > Active Backups**.
2. Select the active backup configuration
3. To select the backup configuration for a particular project, do the following:
  - a) Click **Provision > Projects** page.
  - b) In the **Local** tab, select the project.
  - c) Click **Manage > Data Protection > Cloud Connect**.
  - d) Select the backup configuration.
4. Click **More > Delete**.  
The **Delete Backup Schedule** window appears.
5. If you do not want to retain the backups for the project on the cloud target, disable the **Keep backups for this project on the target** option.  
If you disable this option, all the backups are deleted along with the configuration.
6. Click **Delete**.  
The backup configuration is deleted.

## Modifying Cloud Backup Configuration

The **Active Backups** page enables you to modify the configuration of a backup. You can modify the schedules and the retention options for the backup.

To modify the configuration, do the following:

1. Click **Services > Cloud Connect > Active Backups**.
2. Select the backup.
3. To select the backup configuration for a particular project, do the following:
  - a) Click **Provision > Projects** page.
  - b) In the **Local** tab, select the project.
  - c) Click **Manage > Data Protection > Cloud Connect**.
  - d) Select the backup.
4. To modify the schedule, click **More** and then choose **Schedule**.  
In the **Manage Schedule** screen, you can change the target, the scope, and the schedule type for the backups. Click **Save** after making the changes.
5. To modify the retention options, click **More** and then choose **Options**.  
In the **Options** screen, you can change the number of latest full backups to retain in the cloud target. Click **Save** after making the changes.
6. Click **Save**.

## Searching for Backup Targets

To search for the S3-compliant cloud targets added in the IntelliFlash Web UI, do the following:

1. Click **Services > Cloud Connect > Cloud Browser**.
2. In the Search bar, type the name of the target you are searching for and click the **Search** icon.

The **Cloud Browser** page displays the targets matching the search query.

## Restoring Cloud Backup of a Specific Project Within the Same Array

---

To restore the snapshot of a particular project within the same array, do the following:

1. Click **Provision > Projects**.
2. In the **Local** tab, select the project.
3. Click **Manage > Data Protection > Cloud Connect**.

The **Cloud Connect** tab displays all the active backups in the project.

4. Select the backup.
5. Click **More** and then choose **Restore**.

The **Restore Backup** window appears. The **Source** screen displays the array to which the data will be restored and the selected backup.

6. In the **Source** screen, click **Next**.
7. In the **Backups** screen, select the specific backup that you want to restore.
8. Click **Next**.
9. In the **Destination** screen, complete the following steps:
  - a) Select the destination pool.
  - b) Provide the name for the new project, share or LUN.
  - c) Select a different project mount, if required.
  - d) (optional) Click **Retain Incremental Snapshots** to retain any incremental snapshots used in restoring the backup.
  - e) Click **Next**

The **Summary** screen appears with the backup download size.

10. Review the summary and click **Finish**.

The backup project is restored to the specified destination path.

## Restoring Cloud Backups Within the Same Array

---

The **Cloud Browser** page displays the backups from which you can restore. You can specifically choose the snapshot of a project, share or LUN that you want to restore.

To restore a backup, do the following:

1. Click **Services > Cloud Connect > Cloud Browser**.
2. In the **Cloud Browser** page, browse to the project or the specific share or LUN that has been backed up in the cloud target.
3. Click **Restore**.

The **Restore Backup** window appears. The **Source** screen displays the array to which the data will be restored and the selected backup.

4. In the **Source** screen, click **Next**.
5. In the **Backups** screen, select the specific backup that you want to restore.
6. Click **Next**.
7. In the **Destination** screen, complete the following steps:
  - a) Select the destination pool.
  - b) Provide the name for the new project, share or LUN.
  - c) Select a different project mount, if required.
  - d) (optional) Click **Retain Incremental Snapshots** to retain any incremental snapshots used in restoring the backup.
  - e) Click **Next**

The **Summary** screen appears with the backup download size.

8. Review the summary and click **Finish**.

The backup project, LUN, or share is restored to the specified destination path.

## Restoring Cloud Backups to a Different Array

---

When an IntelliFlash system is lost entirely or not available, you can use the backup from the original array and restore it to a new IntelliFlash system.

To restore the data to a new IntelliFlash system, do the following:

1. Log in to the Web UI of the new IntelliFlash system.
2. Add the cloud target in the **Services > Cloud Connect > Cloud Targets** page.

 **Note:** When adding the cloud target, select the existing bucket where the data was backed up from the original IntelliFlash system.  
For more information, see [Adding a Cloud Target](#).
3. After adding the target, browse to the **Services > Cloud Connect > Cloud Browser** page.
4. In the **Cloud Browser** page, go to the project or the specific share or LUN that has been backed up in the cloud target.
5. Click **Restore**.

The **Restore Backup** window appears. The **Source** screen displays the array to which the data will be restored and the selected backup.

6. In the **Source** screen, click **Next**.
7. In the **Backups** screen, select the specific backup that you want to restore.
8. Click **Next**.
9. In the **Destination** screen, complete the following steps:
  - a) Select the destination pool.
  - b) Provide the name for the new project, share or LUN.
  - c) Select a different project mount, if required.
  - d) (optional) Click **Retain Incremental Snapshots** to retain any incremental snapshots used in restoring the backup.
  - e) Click **Next**.

The **Summary** screen appears with the backup download size.

10. Review the summary and click **Finish**.

The backup project, LUN, or share is restored to the specified destination path.

## Backing up and Restoring Data through 10G Interfaces

---

To back up data to cloud targets and restore data through 10G interfaces, do the following:

1. Create a new interface group in the **Settings > Network > Interface** page. For more information on creating a new interface group, see [Adding an Interface Group](#).
2. Populate the routing table in the **Settings > Network > Advanced** page with the IP addresses of each region from where the data is backed up and restored.

For example, the IP subnet details can be as follows:

Destination/Mask	Gateway	Interface
54.231.0.0/255.255.128.0	10.204.208.1	d_s3
54.216.0.0/255.254.0.0	10.204.208.1	d_s3
54.92.16.0/255.255.240.0	10.204.208.1	d_s3

For information about adding static routes, see [Adding a Static Route](#).

## Deleting a Cloud Backup

---

The **Cloud Browser** page consists of all the backup snapshots. You can choose to delete the complete backup of a project, LUN, or a share, or delete just the single backup.

To delete a cloud backup, do the following:

1. Click **Services > Cloud Connect > Cloud Browser**.
2. In the **Cloud Browser** page, browse to the project or the specific share or LUN that has been backed up in the cloud target.
3. Select the backup and click **Delete**.  
The **Delete** window appears.
4. In the **Scope** screen, select whether you want to delete the whole backup or a single instance of the backup.
5. Click **Next**.
  - If you selected **Backup**, the **Backups** screen appears.
  - If you selected **Dataset**, the **Summary** screen appears. Go to [Step 9](#).
6. In the **Backups** screen, select the backup you want to delete.  
The **Dependents** screen appears with a list of all the dependent incremental backups.
7. In the **Dependents** screen, type **Delete** in the text box to confirm the deletion of the single backup.
8. Click **Next**.  
The **Summary** screen appears.
9. In the **Summary** screen, review the information and click **Finish**.



---

# Chapter 33

---

## IntelliFlash PowerShell Toolkit Overview

---

**Topics:**

- *Introduction to IntelliFlash PowerShell Toolkit*

## Introduction to IntelliFlash PowerShell Toolkit

---

The IntelliFlash Powershell Toolkit (PSTK) conforms to Powershell standards and provides intuitive script management of the storage array.

Administrators can download this scripted module of cmdlets from the below link. Each cmdlet function is prefixed with "-Ifa".

For the latest IntelliFlash PSTK information, refer to <https://github.com/DDNStorage/intelliflash-powershell-toolkit>.

The Powershell Toolkit provides Powershell sample code for users to do their own scripting, and allows administrators to do most of what the IntelliFlash Web UI does through Windows Powershell.

The Powershell script primarily calls the IntelliFlash REST APIs. You can create, delete, modify, or enumerate operations on LUNs, shares, projects, snapshots, initiators, and targets within the ecosystem.

---

# Chapter 34

---

## IntelliFlash Data Protection Services (IDPS)

---

**Topics:**

- *Introduction to IntelliFlash Data Protection Services (IDPS)*
- *Components of the Backup Solution for Windows Hosts*
- *How IDPS Works*
- *Guidelines for Creating LUNs or Shares for Application-consistent Backup with IDPS*
- *Installing and Setting Up IDPS*
- *Managing IDPS Connections to Arrays*
- *Updating IDPS*
- *IDPS Support Log Utility*
- *Restoring Snapshots and LUNs created by IDPS*

## Introduction to IntelliFlash Data Protection Services (IDPS)

---

IntelliFlash Data Protection Services (IDPS) is a Microsoft Volume Shadow Copy Service (VSS) based backup solution for IntelliFlash LUNs and shares hosted on Windows systems. IDPS works with VSS to take consistent, point-in-time data snapshots of the LUNs and shares provided by IntelliFlash systems to Windows hosts. The Windows hosts may be running on bare metal or in a hypervisor (as a virtual machine).

IDPS can connect to and take backups on multiple IntelliFlash systems. Usually, backups are requested by the IntelliFlash Array based on the snapshot schedule of the respective LUNs or shares. However, they can also be initiated from the IntelliFlash Web UI or a third-party backup application. IntelliFlash is compatible with all the new and the older IDPS versions.

You can download the latest IDPS installer from the **Settings > Administration > Plugins** page in the IntelliFlash Web UI.

When you upgrade to IntelliFlash 3.7.x.x or later, the existing IDPS clients continue to take snapshots of LUNs and shares mapped to the Windows clients in the previous IntelliFlash versions.

When you upgrade to IntelliFlash 3.7.x.x or later, either upgrade to or perform a fresh install of IDPS 2.1.x.x, as it supports several new features such as quiescing of SMB 3.0 shares, and obtaining application-consistent snapshots on Hyper-V hosts or SQL Server 2014 CSV Clusters.

When the IDPS agent installed on the Windows hosts is not the latest version, the following message appears in the **Settings > App-Aware > Windows Servers** page:

**Upgrade the IDPS agent to the latest version to use all the features.**

TLS 1.2 and 1.0 protocols should be supported. It should negotiate to the TLS level set on your array. If you require a particular TLS protocol for your Windows host, you can adjust by running the supportLogs.exe utility installed in your IDPS directory.

### New Features in IDPS 2.1.x.x

The latest IDPS 2.1.x.x supports the following new features:

- **Application-consistent snapshots on SQL Server 2014 CSV Clusters:** IDPS 2.1.x.x enables application-consistent snapshots on SQL Server 2014 when the databases are stored on Cluster CSVs.

To support this feature, during the IDPS installation, the installer requests the SQL authentication credentials when it detects SQL Server 2014 CSV Clusters. The authentication credentials help discover the cluster node on which the SQL database instance is running and quiesces it.

- **Application-consistent Hyper-V snapshots:** With IntelliFlash 3.7.x.x and later, when you perform a fresh install of IDPS 2.1.x.x (not just upgrade from an older version to IDPS 2.1.x.x, but uninstall the older version of IDPS and install IDPS 2.1.x.x), you can take fully transaction-consistent Hyper-V snapshots. This is applicable only for Windows Server 2012 / 2012 R2 /

2016. For Windows 2008 R2 Hyper-V snapshots, if you upgrade to IDPS 2.1.x.x and do not perform a fresh install, you will continue to get file system or crash consistent Hyper-V snapshots.

IntelliFlash 3.7.x.x and later versions do not support rollback for the auto-recovered Hyper-V snapshots.

- **Quiescing SMB 3.0 shares in Windows hosts:** With IDPS 2.1.x.x, you can quiesce SMB 3.0 shares in Windows Server 2012 / 2012 R2. You can also quiesce SMB 3.0 shares for SQL in Windows 2016 hosts.

For IDPS to detect SMB 3.0 shares, enable **SMB 3.0** in the IntelliFlash Web UI (through the **Services > NAS > SMB** menu). You must also set up the DNS and floating IP addresses in the IntelliFlash Web UI (through the **Services > NAS > Identity Management > AD/Kerberos Setup** menu).

IDPS 2.1.x.x supports only those shares that are connected using DNS or NETBIOS, for example, \\payroll-a-group\yourShareName1. IP server names are disabled by default. For SMB quiesced snapshots, the Hypervisor and Hyper-V VMs should be connected to the same domain forest as the IntelliFlash array.

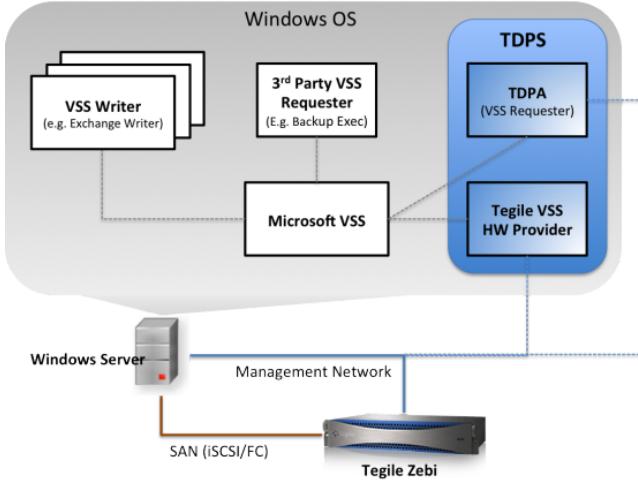
- **Quiescing SAN datasets in Windows 2016 hosts:** You can now quiesce SAN datasets (iSCSI or Fibre Channel) on Windows 2016 hosts.
- **Enhancements in Support Log Utility:** Using the IDPS, you can now configure Microsoft SQL Server logins. You can also verify the storage connection configurations using the support utility.

## Components of the Backup Solution for Windows Hosts

---

IDPS consists of two Windows services: the IDPA and the VSS Hardware Provider. These services communicate with the VSS on the same system/host and with the IntelliFlash Array to create backups.

The following figure illustrates the components that comprise a IDPS-based backup solution.



**Figure 33: Components of a IDPS-based backup solution for a Windows host running on physical hardware**

A IDPS-based backup solution for a Windows host running on physical hardware has the following components:

- **Microsoft Volume Shadow Copy Service (VSS):** VSS is a Windows framework that enables backup software, such as IDPS, to take backups of volumes mounted on a Windows host—even as the host and applications on the host continue to write to the volumes. VSS enables coordination among applications that generate the data (VSS Writers), applications that initiate the backup requests (VSS Requesters), and applications or systems that provide storage services (providers). It enables these different applications to work together and take transaction-consistent backups known as Volume Shadow Copies.

VSS is available for all editions of Windows starting from Windows XP, Service Pack 2 and Windows Server 2003. However, some IDPS features require specific versions of VSS/Windows Servers. For example, IDPS requires Windows Server 2012 or later for taking single-node backups of Cluster Shared Volumes (CSVs).

- IDPS consists of the following Windows services:
  - **IDPA:** This service functions as the VSS requester.
  - **VSS Hardware Provider:** This service functions as a VSS abstraction of each storage vendor's backup APIs allowing native IntelliFlash storage OS snapshots, clones, and LUN initiator mappings to be requested by a generic VSS coordinator. It works with requester applications, such as the IDPA or other third-party backup software, to provide VSS coordinated transaction-complete native IntelliFlash OS snapshots on the IntelliFlash Array.

## How IDPS Works

The following sections contain information about how IDPS works in different environments.

**!** **Warning:** You should include all the volumes used by an application (example: a Hyper-V VM or a SQL Server database) in one project. This is because IDPS takes snapshots

one project at a time. If an application uses volumes across two or more projects, the snapshots (backups) are inconsistent.

## How IDPS Works in a Physical Windows Environment

IDPS enables you to backup LUNs or shares on Windows systems that are physically installed on hardware (bare metal).

At a high-level, the process for backing up a LUN or share mounted on a Windows system is as follows:

1. The IntelliFlash OS instructs IDPS to create a snapshot.
2. IDPA (the VSS Requester) sends a request to the VSS service to create a snapshot of the specified LUNs or shares.
3. VSS instructs the relevant VSS Writers of the applications that use the LUNs or shares to:
  - Quiesce the applications
  - Flush the application cache to the volume
  - Hold incoming writes
4. For IntelliFlash LUNs, the VSS requester (such as IDPA or a third party backup) instructs the VSS Hardware Provider to create the snapshots. For IntelliFlash NAS SMB Shares, the VSS requester instructs the Microsoft File Share Shadow Copy Provider to create snapshots. Microsoft File Share Shadow Copy Provider forwards the request to the Remote VSS (RVSS) Provider running on the IntelliFlash array.
5. Both the VSS Hardware Provider for SAN and RVSS provider for NAS SMB communicate with the IntelliFlash OS to create fast optimized snapshots on the IntelliFlash array.
6. VSS instructs the writers to thaw the applications and resume the writes to the LUNs or shares.
7. IDPA reports the status of the requested snapshots to the IntelliFlash OS, or retries the operation if the VSS Writer requests it. The IntelliFlash OS might rename snapshots from the VSS name to a human-readable name based on the schedule.



### Important:

- If multiple applications are using the same LUN or share, or if there are multiple LUNs or shares in a project, the writers might take longer time to complete flushing the cache to all relevant LUNs. This might result in a timeout and VSS snapshots creation might fail. To reduce the possibility of a timeout, limit the LUNs or shares per project and the applications per LUN or share.
- Ensure that the IDPS Windows host can ping the network addresses configured during the IDPS installation or while running the ConnectSystem.exe utility.

## How IDPS Works in an Hyper-V Environment

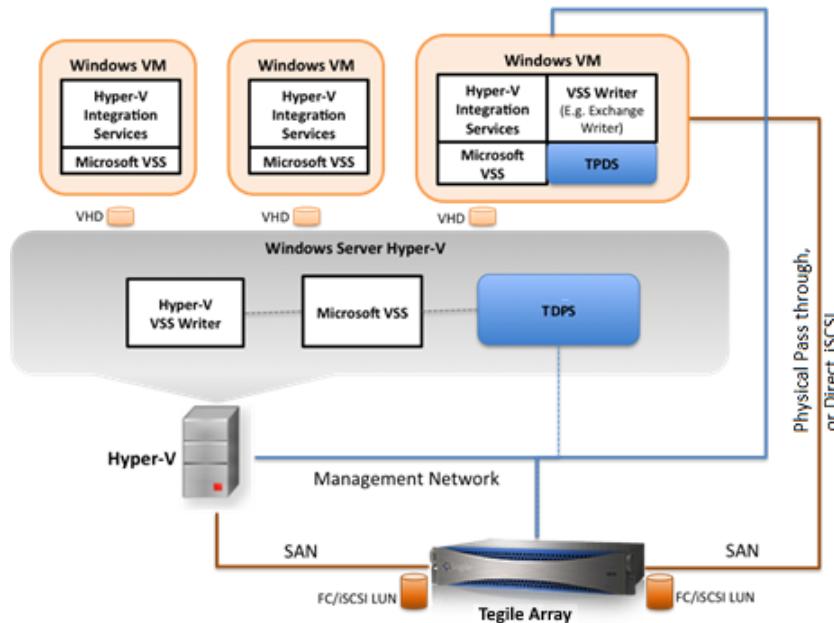
IDPS enables you to take backups of Windows VMs hosted on Hyper-V. Depending on how the Hyper-V environment is set up and how you want to use IDPS, you might have to install IDPS on the parent partition of Hyper-V and on the individual child Windows VMs.

The following sections describe the components of the IDPS backup solution for Hyper-V and how these components work together to take backups of Hyper-V VMs.

**Note:** Starting with IDPS 2.0 and above, backup of all MS Cluster CSVs from a single node of Windows 2012 (or later) cluster can be done.

### Components of the IDPS backup solution for Hyper-V

The following figure illustrates the different components of a IDPS solution for Hyper-V.



**Figure 34: Components of a IDPS-based backup solution for Hyper-V**

The above figure illustrates a Hyper-V environment in which LUNs are being used.



**Important:** Ensure that the IDPS Windows host (parent partition hypervisor or Hyper-V VM) can ping the network addresses configured during the IDPS installation or while running the ConnectSystem.exe utility.

In an Hyper-V environment, LUNs or shares can be mapped at both the hypervisor level and at the Hyper-V VM level. To take snapshots of LUNs or shares at both the levels, install IDPS and Hyper-V integration services on the parent partition and the Windows Hyper-V VM.

### How IDPS Backs Up Hyper-V VMs

The process for creating a snapshot on a LUN or a share that is directly accessed by a Windows VM is similar to the process used in a physical Windows environment. The only difference is that instead of communicating with the IDPS on a physical server, the IntelliFlash OS communicates with the IDPS on a Windows VM.

The following steps describes the process of creating a child VM snapshot of a guest VM from the parent partition hypervisor host:

1. The IntelliFlash OS communicates with IDPS on the Hyper-V hypervisor parent partition host OS to initiate a snapshot creation request on the LUN.
2. On the hypervisor parent partition, IDPS sends the snapshot creation request to VSS.
3. On the hypervisor parent partition OS, VSS informs the Hyper-V Writer to quiesce the VMs.
4. Hyper-V Writer informs the Hyper-V Integration Services in each VM on the LUN to quiesce the applications on the VM, flush the I/O cache, and hold the writes.
5. In the VM, Hyper-V takes an internal snapshot of the guest OS.
6. During this internal snapshot, for SAN LUNs connected directly from the VM, the VSS informs the VSS Hardware Provider installed within the VM. The VSS Hardware Provider communicates with the array to create snapshots. For direct NAS SMB IntelliFlash shares, VSS contacts the Microsoft File Share Shadow Copy Provider that forwards the snapshot request to the Remote VSS (RVSS) Provider running on the IntelliFlash array.
7. The VSS Hardware Provider for SAN and the Microsoft File Share Shadow Copy Provider for NAS create the IntelliFlash OS snapshots for the requested IntelliFlash LUNs or shares that have VHD files located on them; reconciling the differences with the guest OS snapshot.
8. VSS informs the Hyper-V VSS Writer to thaw the application.
9. On each VM, Hyper-V Integration Services thaw the applications and they resume the writes.



**Note:** If your Hyper-V VMs do not directly access the array (they do not use physical pass-through disks or iSCSI), then you only need to install IDPS on the parent partition hypervisor machine and back up from there with third-party backup or IDPA. For application consistency with third party backup, you must install Hyper-V Integration services on all Windows VMs.

Limit the number of VMs running on a LUN or share. Also, have the VM OS images on one LUN or share, and other running applications on separate LUNs or shares.

### Single Node Backups of Hyper-V Clusters on Cluster Shared Volumes

With IDPS 2.0 or higher, you can back up every CSV from the single MS cluster master node of a Windows Server 2012 and above cluster.

## How IDPS Works in a VMware Environment

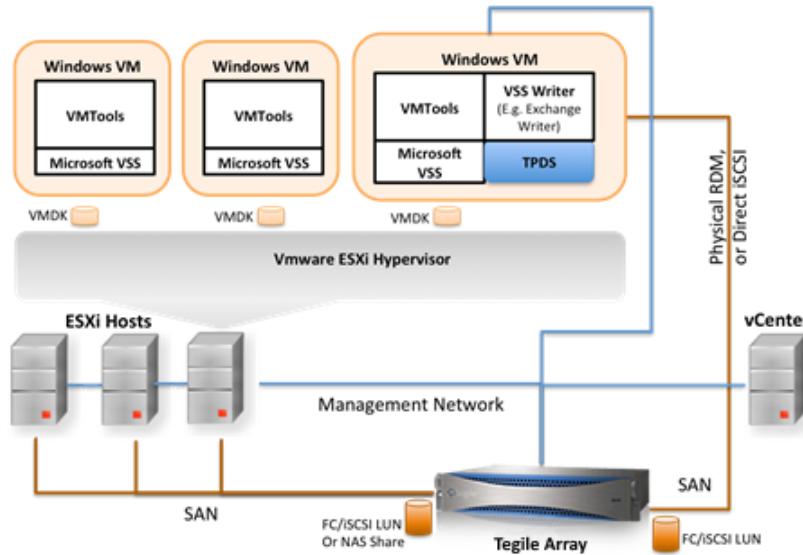
### Backing up LUNs directly accessed by Windows VMs on VMware ESXi

In a VMware environment, IDPS enables you to take backups of IntelliFlash LUNs or shares that are directly accessed by Windows VMs. When creating a snapshot on a LUN or a share that is directly accessed by the Windows VM (example: VMware physical Raw Device Mapping, or storage connections initiated by the VM and not the ESX server), the process is similar to a physical Windows environment. For more information, see [How IDPS Works in a Physical Windows Environment](#).

### Backing up Windows Virtual Machines running on VMware ESXi

IntelliFlash also supports snapshots for virtual machines running in a VMware ESXi virtualized environment through the VMware Snapshot Provider and VMware Tools. The VMware Snapshot provider quiesces VMDKs and virtual RDM volumes on the IntelliFlash array that are created by SAN or NFS NAS connections initiated by the ESX server and not the individual VM.

The following figure shows the components of a IDPS-based backup solution for VMware environments.



**Figure 35: IDPS in a VMware Environment**

**Note:**

- To ensure consistent data protection, install VMware Tools, and ensure that the VMware Snapshot Provider and Volume Shadow Copy Services start automatically on all Windows VMs.

- The IntelliFlash Array communicates with the VMware ESXi host and VMware vCenter using the Array Management IP address.

## Guidelines for Creating LUNs or Shares for Application-consistent Backup with IDPS

---

For IntelliFlash to take application consistent backups, you must follow these guidelines:

- IDPS detects which application is using the LUN or share based on:
  - The application type specified in the **Settings > App-Aware > Windows Servers or VMware Servers** page.
  - The project template used while creating the project that contains the LUN or share.
- VSS can take application-consistent backups without timing out if the number of LUNs or shares in the project are limited and only one application is using the LUNs or shares in a project.
  - If possible, use the pre-defined project templates. Avoid adding any additional LUNs or shares beyond what is created by the template. If you must add more LUNs or shares, restrict the number of LUNs or shares in the project to the recommended range.
  - If you are using the generic template, restrict the number of LUNs or shares in the project to the recommended range.
- Currently, you can backup LUNs or shares used by only one application type in an application-consistent manner. If you want backups of more than one application from the same server, distribute those applications across different hosts.

## Installing and Setting Up IDPS

---

You can download the IDPS installer from the IntelliFlash Array and run it on the following systems:

- Windows hosts that use IntelliFlash LUNs or shares.
- Hyper-V parent partitions on which you intend to map IntelliFlash LUNs or shares (directly at the Hyper-V hypervisor level).

The following table lists the different IDPS installers and the Windows platforms on which they can be installed.

**Table 18: IDPS Installers**

IDPS Installer	Windows OS
IntelliFlashDataProtectionSetupX64.msi	Windows Server 2022 Windows Server 2019 Windows Server 2016

## Downloading the IDPS Installer

To download the IDPS installer, complete the following steps:

1. Click **Settings > Administration > Plugins**.
2. Click **Download** for the 64-bit installer and save the file.

## Running the IDPS Installer

### Prerequisites

- Connect and configure the network for IntelliFlash, the hypervisors, and the VMs.
- Install VM Tools or Hyper-V Integration Services, as applicable, on each Windows VM.
- Install or enable Windows PowerShell on each Windows VM.
- Ensure each Windows VM has .NET Framework 4.0 and above versions.

 **Note:** For .NET Framework 3.5 support on Windows 2008, you need to use the prior version of IDPS (For example, IDPS 2.0.x).

- Download the appropriate IDPS installer on the Hyper-V parent partition and Windows hosts that require IDPS functionality.
- IDPS communicates with the IntelliFlash system using the DNS name or IP address that you specify while adding a storage system. If you intend to add a storage system after installing IDPS, you must ensure that the Windows system can connect to the required subnets and access the array using the IP address that you specify.

To install IDPS, complete the following steps:

1. On the Windows host, double-click the IDPS installer to start the installation.
2. Click **Next** on the Welcome screen.
3. Read through the license agreement.
  - If you agree with the terms, select **I accept the terms of the license agreement** and click **Next**.
  - If you do not agree with the terms, click **Cancel**.
4. Select the Windows account under which the IDPS services will run on the Windows host.
  - **System Account Login**.  
It is recommended that you use the default **System Account Login** option.
  - **Configure Login**

To use another account, select **Configure Login** and enter the credentials.

5. Click **Next**.
6. If you do not want IDPS to use the predefined (default) TCP/IP port of 4438, enter a different port.
7. To add an exception in the Windows Firewall for the port you entered, select **Add Windows Firewall port exception**.
  - To add the exception for all networks, select **Add exception for All networks**.
  - To add the exception only for the domain and private networks, select **Add exception only for Domain and Private networks**.



**Note:** The IDPS installer can add an exception only to the Windows Firewall. For third-party firewall software, you have to manually add the required firewall exception.

8. Select the folder in which IDPS will be installed and click **Next**.
  9. Click **Install**.  
The **Installation Wizard Complete** screen appears when the installation is complete.
  10. If you want to proceed with adding storage systems on which IDPS will take backups after closing the installation wizard, select **Add Storage System**.
  11. Click **Finish**.  
The **Configure Storage System Connections** dialog box appears.
  12. Click **Add**.  
The **Add Storage System** dialog box appears.
  13. Select how you want to use the administrator account credentials that you enter in this dialog box.
    - Select the **'default' connection settings (for any unspecified system)** option if you want IDPS to use the same IntelliFlash administrator credentials to connect to all IntelliFlash systems.
    - Select the **Specific settings for a particular storage system** option if one or more arrays have IntelliFlash Web Administrator credentials that are different from the Web Administrator credentials of other arrays.
- 
- Note:** Use the **Specific settings for a particular storage system** option if you want IDPS to connect to more than one array.
14. Enter the IP address of the IntelliFlash Array you want to add.

Use a management floating IP address that is associated with the pool you want to protect.

15. In the **Storage System Credentials** pane, type the user name and password of the **webadmin** account.
16. Enter the password again for confirmation.
17. Click **Connect**.  
If the IP address and credentials are valid, the **Configure Storage System Connections** dialog box appears again. The array you just added is included in the table and its status is “connected”.
18. To add more storage systems, click **Add** and repeat steps 13 through 17.
19. After you have added the required storage systems, click **OK** to exit the **Configure Storage System Connections** dialog box.
20. During the installation, if the IDPS installer detects SQL Server 2014 CSV Clusters, it requests the SQL authentication credentials. This enables application-consistent snapshots on SQL Server 2014 when the databases are stored on Cluster CSVs. The authentication credentials help discover the cluster node on which the SQL database instance is running and quiesces it.

In the **Configure Microsoft SQL Server Logins** dialog box, do the following:

1. Click **Add**.  
The **Add Login** dialog box appears.
2. Select the SQL Server instance name from the dropdown list.
3. In the **Authentication** dropdown list, select **Windows Authentication** or **SQL Server Authentication**.
4. Enter the user name and password.
5. Enter the password again for confirmation.
6. Click **OK**.

You can also add or modify existing Microsoft SQL Server logins using the IDPS Support Utility. See [Configuring Microsoft SQL Server Logins](#) for more information.

#### After you finish

You must register the Windows host on which you have installed IDPS with the array to which it is connected. For more information, see [Registering IDPS-enabled Windows Hosts on the Array](#).

## Registering IDPS-enabled Windows Clients on the Array

You must register the IDPS-enabled Windows clients with the IntelliFlash system that provides LUNs and shares to those clients.

#### Prerequisites

- IDPS must be installed on the Windows clients that you want to register. The array connects with the IDPS running on the client during the registration process. For more information, see [Running the IDPS Installer](#).
- For each Windows client that you want to register, you must have the following details:
  - Windows client name or IP address.
  - The port number used by IDPS.
  - The application that is using each LUN or share on the client.

To register the Windows client with IntelliFlash, complete the following steps:

1. Log into the IntelliFlash Web UI.
2. Click **Settings > App-Aware > Windows Servers**.
3. Click **Add**.

The **Windows Server Details** dialog box appears.

4. In the **Host Name** field, type the host name or the IP address of the Windows client. Enter a different port number if you do not want to use the default port: 4438.



**Note:** The port number must match with the port number you entered when installing IDPS on that client.

5. Select an appropriate **Application**.
6. Click **Save** to save the configuration.

- Verify that the Windows Server status list displays **OK**. If not, edit the Windows Server information to provide the correct information. If the status is still not OK, check the network connections.
- The IDPS Agent always backs up a copy without truncating the logs. This is ideal for interoperability with third party backups that rely on log truncation.
- In the **Windows Servers** list, if the IDPS Agent installed in the Windows host is not the latest version, an information icon appears in the **IDPS Version** column. When you mouse over the icon, you see the following message:

**Upgrade the IDPS agent to the latest version to use all the features.**

## Adding the IDPS PowerShell SnapIn

The IDPS cmdlets are included in the IDPS PowerShell SnapIn. To ensure that the IDPS cmdlets are accessible from the **Windows PowerShell Console**, add the IDPS PowerShell SnapIn.

To add the IDPS PowerShell SnapIn, complete the following steps:

1. Open the **Windows PowerShell Console** under an administrative account.
2. Run the following command: `add-pssnapin IntelliFlash.DataProtection.SnapIn`

## Managing IDPS Connections to Arrays

---

You must configure IDPS to connect to the arrays that provide LUNs or shares to the Windows client.

To connect to an array, IDPS requires the following information:

- The floating management IP for the array (or alternatively the DNS if a DNS Server is configured for the array).  
For DNS, configure a DNS name on the DNS server for the floating management IP associated with the pool being protected by the backups. For SMB share backup, create a DNS reverse DNS lookup for those pool mgt floating IPs as well.
- User name and password of the `webadmin` account. This is the same account that you use to log into the IntelliFlash Web UI. The Webadmin account used to log into the IntelliFlash Web UI can be a windows Active directory domain account, as long as the AD account has been configured to map to an array administrator.

 **Note:** Use a management floating IP address that is associated with the pool you want to protect.

You can add and manage storage system connections using either of the following two tools:

- The `ConnectSystem` tool provided in the IDPS installation folder. This tool can also be launched by the IDPS installer after installing IDPS.
- The IDPS PowerShell cmdlets.

IDPS includes the following PowerShell cmdlets:

- The `Get-IdpsStorageSystem` cmdlet retrieves storage connection attributes from the IntelliFlash Data Protection Agent configuration.
- The `Add-IdpsStorageSystem` cmdlet adds IntelliFlash Array connection settings into the IntelliFlash Data Protection Agent configuration.
- The `Remove-IdpsStorageSystem` cmdlet removes storage connection settings from the IntelliFlash Data Protection Agent configuration.

## Adding a Storage System Connection

### Prerequisites

- Use the floating IP address that is bound to the same resource group as the pool that contains the LUNs or shares used by the current Windows client. If the Windows client uses multiple LUNs or shares and those LUNs or shares are on different arrays or resource groups, you must have the floating IP address corresponding to each of those LUNs or shares.

- Use the credentials of the **webadmin** account (the same account that you use to log into the IntelliFlash Web UI). The webadmin account used to login to the array can be either a native IntelliFlash administrator account or an LDAP-Active directory account mapped to be an administrator.
- The Windows client on which you are running `ConnectSystem.exe` must be able to connect to the required subnets and access the array using the IP address that you specify.



**Tip:** You can also use the cmdlets described in [Managing IDPS Connections to Arrays](#) to add a storage system connection.

To add a storage system connection for IDPS, complete the following steps:

1. Open the IDPS installation folder on the Windows client.
2. Run **ConnectSystem.exe**.  
The **Configure Storage System Connections** dialog box appears.
3. Click **Add**.  
The **Add Storage System** dialog box appears.
4. Select how you want to use the administrator account credentials that you enter in this dialog box.
  - Select the **'default' connection settings (for any unspecified system)** option if you want IDPS to use the same IntelliFlash administrator credentials to connect to all IntelliFlash systems.
  - Select the **Specific settings for a particular storage system** option if one or more arrays have IntelliFlash Web Administrator credentials that are different from the Web Administrator credentials of other arrays.



**Note:** Use the **Specific settings for a particular storage system** option if you want IDPS to connect to more than one array.

5. Enter the IP address of the IntelliFlash Array you want to add.  
Use a management floating IP address that is associated with the pool you want to protect.
6. In the **Storage System Credentials** pane, type the user name and password of the **webadmin** account.
7. Enter the password again for confirmation.
8. Click **Connect**.  
If the IP address and credentials are valid, the **Configure Storage System Connections** dialog box appears again. The array you just added is included in the table and its status is "connected".
9. To add more storage systems, click **Add** and repeat steps 4 through 8.
10. After you have added the required storage systems, click **OK** to exit the **Configure Storage System Connections** dialog box.

## Editing a Storage System Connection

To edit an existing storage system connection in IDPS, complete the following steps:

1. Open the IDPS installation folder on the Windows client..
2. Run **ConnectSystem.exe**.  
The **Configure Storage System Connections** dialog box appears.
3. Select a storage system and click **Edit**.
4. Enter the IP address of the IntelliFlash Array you want to add.  
Use a management floating IP address that is associated with the pool you want to protect.
5. In the **Storage System Credentials** pane, type the user name and password of the **webadmin** account.
6. Enter the password again for confirmation.
7. Click **Connect**.  
If the IP address and credentials are valid, the **Configure Storage System Connections** dialog box appears again. The array you just added is included in the table and its status is “connected”.
8. To edit another storage system, repeat steps 3 through 7.
9. Click **Connect**.  
If the IP address and credentials are valid, the **Configure Storage System Connections** dialog box appears again and the status of the array that you just edited shows as “connected”.
10. To edit another storage system, repeat steps 3 through 7.
11. After you have edited the required storage systems, click **OK** to exit the **Configure Storage System Connections** dialog box.

## Removing a Storage System Connection

To delete a storage system connection from the IDPS, complete the following steps:

1. Open the IDPS installation folder on the Windows client.
2. Run **ConnectSystem.exe**.  
The **Configure Storage System Connections** dialog box appears.
3. Select a storage system and click **Remove**.

The **Remove Storage System** window displays details of the array and a confirmation message appears.

4. Click **Yes** to delete the array connection that is displayed.
5. After you have removed the required storage systems, click **OK** to exit the **Configure Storage System Connections** dialog box.

 **Note:** You must have at least one array connection configured in the **Configure Storage System Connections** for IDPS to work.

## Updating IDPS

---

New versions of the IDPS software are bundled with the IntelliFlash Operating Environment and become available when you upgrade the IntelliFlash Operating Environment on an IntelliFlash system. After you upgrade the IntelliFlash Operating Environment on the array, you can update IDPS using the IDPS PowerShell Cmdlets.

For more information, see *IDPS PowerShell Cmdlets* and *Using the IDPS PowerShell Cmdlets to Update IDPS*.

 **Note:**

- To view the IDPS version installed on different Windows clients, see the **IDPS Version** column on the **Settings > App Aware > Windows Servers** page of the IntelliFlash Web UI.
- To ensure that the Windows client can always detect the latest update, you should configure specific array connections with `ConnectSystem.exe` as described in *Adding a Storage System Connection*.

## IDPS PowerShell Cmdlets

IDPS includes the following PowerShell cmdlets that enable you to update IDPS on Windows clients:

- The `Get-IdpsVersion` cmdlet retrieves the currently installed version of IDPS on the Windows client.
- The `Find-IdpsUpdate` cmdlet checks the configured arrays for a new version of IDPS. If IDPS is connected to multiple IntelliFlash systems, it checks each IntelliFlash Array for a new version of IDPS.
- The `Get-IdpsStorageSystem` cmdlet confirms whether the IntelliFlash system, where you want to check for IDPS updates, is configured with IDPS.
- The `Install-IdpsUpdate` cmdlet updates IDPS. If IDPS is connected to multiple IntelliFlash systems, and the cmdlet detects multiple new versions, it selects the latest update.

 **Note:** During the update process, you might see invalid component errors in the Event Viewer in Windows Server 2012 R2. If so, close the Event Viewer and start it after the update has completed.

The `Install-IdpsUpdate` cmdlet performs the following steps:

1. Downloads the IDPS update.
2. Stops IDPS.
3. Installs the update. Depending on the installer choice and the type of update, the installer will either update or uninstall and re-install IDPS.
4. Starts IDPS.

## Using the IDPS PowerShell Cmdlets to Update IDPS

### Prerequisites

- You must have added the IDPS PowerShell SnapIn to use the IDPS PowerShell Cmdlets. For more information, see Adding the IDPS PowerShell SnapIn.
- You should ensure that all the storage you want to use for backup is online, formatted, and connected because it uses these LUN connections to look for software updates.
- Ensure that IDPS can connect to all arrays that provide LUNs or shares to the Windows client on which it is installed. Besides basic network connectivity, you must ensure that IDPS uses the correct IP address and administrator credentials for each array. For more information, see [Editing a Storage System Connection](#).
- If the Windows system is part of a cluster, the cluster should be in a running state before you start the update.
- If the Windows system is part of a cluster, ensure all the cluster nodes have Storage System Connections configured to the IntelliFlash system that has the latest IDPS version.



**Warning:** You need to either reboot the system or close all dependent applications for the IDPS installation to complete the upgrade. If you choose the reboot option, you must reboot the system later to complete the installation.



**Tip:** Make sure the array from which you download IDPS is added to the arrays connections by running ConnectSystem.exe. This is important when running on a Windows cluster as the storage that it normally uses to detect the array might be owned by another node.

To update an existing version of IDPS, complete the following steps:

1. Start a **PowerShell** console as an administrator.
2. Add the IDPS SnapIn by running the command: `add-pssnapin IntelliFlash.DataProtection.SnapIn`
3. Optional: Run the `Get-IDpsVersion` cmdlet to check the version currently installed.
4. Optional: Run the `Get-IDpsStorageSystem` cmdlet to confirm that the IntelliFlash system, where you want to check for IDPS updates, is configured with IDPS.
5. Optional: Run the `Find-IDpsUpdate` cmdlet to confirm that the IDPS version downloaded to the IntelliFlash Array is more recent than the currently installed version.
6. Run the `Install-IDpsUpdate` cmdlet to install the IDPS update.

 **Note:** Make sure that you run the `Install-IDpsUpdate` cmdlet on all the Microsoft cluster nodes to update IDPS on all nodes.

## IDPS Support Log Utility

---

The IDPS Support Log utility facilitates the collection of Windows and IDPS logs. The IDPS installer installs IDPS Support Log utility on the Windows client.

The logs collected by the utility capture the events related to the Microsoft Volume Shadow Copy Service (VSS), the network, and storage. These logs are useful for resolving issues related to IDPS. You can use the utility to gather and compress IDPS and client system logs and send the compressed file to the IntelliFlash Technical Support team over FTP.



**Important:** The support logs utility generates batch scripts to gather client system information each time it runs. It then displays the location of the scripts for you to review them before you run them. This enables you to ensure that no sensitive data is shared with IntelliFlash Technical Support team.

## IDPS Support Log Utility Functions

When you enable logging in the IDPS Support Log utility, you can perform the following functions.

### Collecting Log Files

The **Collect Log Files** feature performs the following tasks:

- Automatically gathers the IDPS log files that are in the logs directory and generates new logs for the various Windows features.
- Collects the IDPS log files if they meet the following criteria:
  - The log files were created in the past one week.
  - The number of log files collected is 300 or more.

- The uncompressed size of the log files is less than 5GB.
- Copies the log files into the ..\support\logs folder.
- Compresses the log files.
- Uploads the compressed log files.
- Deletes the log files from the local system after compressing and uploading them.

You can select the type of data this utility gathers. By default, the data collection scripts collect all of the following information:

- IDPS logs
- Event logs (gathers event log entries for one week from the application and system hives)
- OS version
- VSS state (VSS Metadata, VSS Writer and VSS Provider states)
- Diskpart output for each drive
- SCSI inquiries that list the IntelliFlash Array paths for each LUN and drive letter
- iSCSI
- MPIO
- SMB
- Driver versions
- Tasks running
- Cluster logs

See [Collecting Log Files](#) for more information.

## Reproducing the Problem

The **Reproduce the Problem** feature enables you to perform the following tasks:

- Collect the selectable data logs such as IDPS, OS version, network, and SMB storage
- Enable VSS and IDPS tracing
- Prompt the user to reproduce the problem
- Reset VSS and IDPS tracing to the original state
- Compress your log data in the support directory
- Upload the compressed file to IntelliFlash Technical Support

See [Reproducing the Problem](#) for more information.

## Uploading Compressed Files

The IDPS Support Log utility uses the 7za.exe compression utility to compress the logs before you upload them to the support site through FTP. After the logs are compressed, the IDPS Support Log utility deletes the logs in the support directory.

See [Uploading Compressed Files](#) for more information.

## Configuring Microsoft SQL Server Logins

You can add or modify existing Microsoft SQL Server logins using the IDPS Support Utility.

The SQL Server authentication credentials help discover the cluster node on which the SQL database instance is running and quiesces it. This enables application-consistent snapshots on SQL Server 2014 when the databases are stored on Cluster CSVs.

See [Configuring Microsoft SQL Server Logins](#) for more information.

## Troubleshooting Storage Connection Configurations

You can verify the storage connection configurations using the IDPS Support Utility.

See [Troubleshooting Storage Connection Configurations](#) for more information.

## Configuring Logging for IDPS

To enable logging for IDPS, complete the following steps:

1. In the Windows host where IDPS has been installed, open the Windows command prompt as an administrator.
2. Navigate to the IDPS installation folder and type `supportLogs.exe`.  
The **IntelliFlash Data Protection Support Utility** dialog box appears.
3. Click **Configure IntelliFlash Data Protection Services**.
4. Select one of the following options:
  - Enable IDPS logging
  - Disable IDPS logging
5. Click **Apply**.

## Configuring Microsoft SQL Server Logins

During the IDPS installation, the installer requests the SQL authentication credentials when it detects SQL Server 2014 CSV Clusters. This enables application-consistent snapshots on SQL Server 2014 when the databases are stored on Cluster CSVs. The authentication credentials help discover the cluster node on which the SQL database instance is running and quiesces it.

You can add or modify existing Microsoft SQL Server logins using the IDPS Support Utility.

To configure Microsoft SQL Server logins, complete the following steps:

1. In the Windows host where IDPS has been installed, open the Windows command prompt as an administrator.
2. Navigate to the IDPS installation folder and type **supportLogs.exe**.  
The **IntelliFlash Data Protection Support Utility** dialog box appears.
3. Click **Configure IntelliFlash Data Protection Services**.
4. Click **Configure Microsoft SQL Server Login**.
5. Select one of the following options:
  - **Add**: Click **Add** to add new SQL Server login.  
The **Add Login** dialog box appears.
  - **Edit**: Select the existing SQL Server login and click **Edit** to modify the login information.  
The **Edit Login** dialog box appears.
  - **Remove**: Select the SQL Server login you want to remove and click **Remove**.
6. In the **Add Login** or **Edit Login** dialog box, add or modify the following information:
  1. When you are adding a new login, select the SQL Server instance name from the dropdown list.
  2. In the **Authentication** dropdown list, select **Windows Authentication** or **SQL Server Authentication**.
  3. Enter the user name and password.
  4. Enter the password again for confirmation.
  5. Click **OK**.
7. In the **Configure Microsoft SQL Server Logins** dialog box, click **Close**.

## Troubleshooting Storage Connection Configurations

You can verify the storage connection configurations using the Support Utility. The IDPS installer and the IDPS service automatically upgrade connections, but if you want to troubleshoot or manually repair connections, you can use the supportLogs.exe utility.

To troubleshoot storage connection configurations, complete the following steps:

1. In the Windows host where IDPS has been installed, open the Windows command prompt as an administrator.
2. Navigate to the IDPS installation folder and type **supportLogs.exe**.  
The **IntelliFlash Data Protection Support Utility** dialog box appears.
3. Click **Configure IntelliFlash Data Protection Services**.
4. Click **Validate connection configuration**.

- If any of the storage connections require upgrading, a dialog box appears with the appropriate message. Click **Yes** to upgrade the configurations automatically. You can also click **No** and then remove older connections or add new connections manually in the **Configure Storage System Connections** dialog box.
- If all the storage connections are up-to-date, a dialog box appears with the message that all connections are valid.

5. Click **Close**.

## Collecting Log Files

To run the IDPS support utility and collect log files, complete the following steps:

1. In the Windows host where IDPS has been installed, open the Windows command prompt as an administrator.
2. Navigate to the IDPS installation folder and type **supportLogs.exe**.  
The **IntelliFlash Data Protection Support Utility** dialog box appears.
3. Click **Configure IntelliFlash Data Protection Services**.  
The **Configure IntelliFlash Data Protection Services** dialog box appears.
4. Click **Collect Log Files**.
5. Select the log files that you want to collect in the Collected Data field.
6. Type the support ticket number.
7. Type the company name.
8. Type a short description of the error.
9. Select **Upload collected data and logs**.  
After the IDPS Support utility collects, compresses, and uploads the logs, it deletes the logs that were gathered into a compressed file from your local system.
10. Click **Collect Data**.

## Reproducing the Problem

The **Reproduce Problem** command in the **Support Log** utility helps you to gather logs while you reproduce a problem. When you invoke this command, it enables VSS logging and prompts you to reproduce the problem. Once the problem is reproduced, it resets the logging state and gathers the required logs for the problem being reproduced. It can also compress and upload the logs if the **Upload collected data and logs** option is selected.

To run the utility and reproduce the problem, complete the following steps:

1. In the Windows host where IDPS has been installed, open the Windows command prompt as an administrator.
2. Navigate to the IDPS installation folder and type **supportLogs.exe**.  
The **IntelliFlash Data Protection Support Utility** dialog box appears.
3. Click **Configure IntelliFlash Data Protection Services**.  
The **Configure IntelliFlash Data Protection Services** dialog box appears.
4. Click **Reproduce Problem**.
5. In the **Collect Logs** dialog box, select the log files that you want to collect in the **Collected Data** field.
6. Type the support ticket number.
7. Type your company name.
8. Type a short description of the error.
9. Select **Upload collected data and logs**.
10. Click **Reproduce**.

## Uploading Compressed Files

 **Note:** You need to use this command only if you did not select the **Upload collected data and logs** option when collecting the log files. If you select the **Upload collected data and logs** option when collecting the log files, the IDPS Support Log utility deletes the compressed log files from your local system after it successfully uploads them.

To run the utility and upload files, complete the following steps:

1. In the Windows host where IDPS has been installed, open the Windows command prompt as an administrator.
2. Navigate to the IDPS installation folder and type **supportLogs.exe**.  
The **IntelliFlash Data Protection Support Utility** dialog box appears.
3. Click **Configure IntelliFlash Data Protection Services**.
4. Click **Upload Compressed Files**.
5. In the **Select file for Upload** dialog box, click **Browse**, navigate to the \support directory and select a compressed log file.
6. Click **Upload**.

## Manually Uncompressing Logs

The utility uses the `7za.exe` compression utility to compress the logs before uploading. You can choose to manually uncompress the log files.



**Note:** The output for the logs is captured in NNNNN\_OUT.TXT files. NNNN is usually a combination of the time run and the operation. For example:  
`sup_storage_102345-234_OUT.txt`

To uncompress the log files:

1. In the Windows host where IDPS has been installed, open the Windows command prompt as an administrator.
2. Navigate to the directory where you saved the logs and type:  
`..\Scripts\7za.exe e ..\support\<log_collection_name.zip>`

## Restoring Snapshots and LUNs created by IDPS

---

### Snapshots and LUNs

Snapshots created by IDPS have a higher fidelity or application consistency where every transaction is guaranteed by Windows to be consistent (either committed or reverted, but not broken or partial transactions within the snapshot). Snapshots created by IDPS are labeled as "quiesced" in the IntelliFlash Web UI. Snapshots created within the IntelliFlash Web UI are labeled as "unquiesced", but cannot be guaranteed as consistent.

Active LUNs that require constant modifications leverage IDPS to gain consistency. LUNs that are offline, unformatted, or have few outstanding changes, can use the unquiesced snapshots.

IDPS is installed in the Windows host, and communicates to the storage array through the **Windows Application Aware** page in the IntelliFlash Web UI. IDPS leverages a feature of Windows called the Volume Shadow Copy Service (VSS) to make sure applications such as Exchange, SQL, and HYPER-V are consistent at the time of the snapshot.

### Read-Only LUNs

A lun-clone made from a snapshot and surfaced to a Windows host is always a readonly disk. This is governed by the current SAN policy. This readonly state can be reset through the `diskmgmt.msc` feature, the **DiskPart** utility and the **ClearSnapshotInfo.exe** utility.

When you run the DISKPART SAN command, it displays the current policy governing the import of a LUN to a Windows Operating System.

SAN displays the policy used on the current system. The policies can be as follows:

- **OfflineShared:** This is the default policy for Windows Servers. The boot disk is brought online. Also, the disks not located on a shared bus such as SCSI, iSCSI, and SAS are brought online. The offlined shared disks are read-only by default.
- **OnlineAll:** On all other versions of Windows (e.g. desktop), the default policy is to bring all disks online. In this case, the disks are online and read/write.
- **OfflineAll:** All disks, except the boot disk, are offline and read-only by default.
- **OfflineInternal:** This policy keeps the newly discovered internal disks offline and read-only.

### **Read-Only Volume Snapshots**

VSS Shadow copies are read-only. If you want to convert a shadow copy to a read/write LUN, you can use the IDPS ClearSnapshotInfo.exe, DiskPart.exe, a Virtual Disk Service (VDS) based application, or some requesters such as diskshadow and vshadow. VSS sets a readonly attribute, a hidden attribute, a snapshot attribute, and a special snapshot state for CSVs.

Snapshots created purely in the IntelliFlash Web UI as 'unquiesced' without IDPS-VSS do not have read-only volume clones or rolled back readonly volume restores. However, when the disk is brought online after restore, they might have the read-only flag set for the entire disk that the volume resides on.

When you create a new LUN clone of the original LUN from a VSS snapshot, you must reset the following attributes of the VSS snapshots:

- Read-Only
- Hidden
- ShadowCopy
- Snapshot management ownership info

### **Converting VSS Snapshots to Read/Write through the Web UI**

Complete the following steps to convert VSS snapshots to read/write through the Web UI:

1. Clone the snapshot in the IntelliFlash Web UI:
  - a) Click **Provision > Projects > Local**.
  - b) Select the project and click the **Snapshots** tab on the right pane.
  - c) Select the desired snapshot.
  - d) Click **Clone**.
  - e) In the **Confirmation** dialog box, click **Yes**.
  - f) In the **Clone Project** window, type a name for the clone and use the initiators that are the same as the rest of the Microsoft cluster LUNs.
2. Use the **Disk Management** snap-in for **Microsoft Management Console (MMC)** to set the status of the cloned LUN to online (read-write):

- a) Press **Windows** and **R** keys to open the **Run** dialog box.
  - b) Type `diskmgmt.msc` in the **Run** dialog box to open the Disk Management snap-in GUI.
  - c) Click **Actions > Rescan Disks** to add new disks.
  - d) Click **Actions > Refresh** to verify the new clone lun exists.
  - e) Right-click the LUN clone and select **Online** to change the status to online (read-write status).
  - f) Right-click the LUN clone and click **Change Drive Letter and Paths**.
  - g) In the **Change Drive Letter and Paths** dialog box, click **Add** and assign a drive letter. ClearSnapshotInfo.exe requires a drive letter.
3. Clear the snapshot attributes of the LUN clone:
- a) Press **Windows** and **R** keys to open the **Run** dialog box.
  - b) Type `cmd.exe` in the **Run** dialog box to open the **Command Prompt** window.
  - c) Navigate to the IntelliFlash Data Protection Services folder.  
For example, type `cd c:\program files\IntelliFlash\IntelliFlash Data Protection Services`.
  - d) Type `ClearSnapshotInfo.exe <drive letter>`:  
For example, type `ClearSnapshotInfo.exe X:`  
This command clears the snapshot attributes on the drive.

## Converting VSS Snapshots to Read/Write through the Diskpart Utility

Complete the following steps to convert VSS snapshots to read/write LUNs through the DISKPART utility:

1. Clone the snapshot in the IntelliFlash Web UI:
  - a) Click **Provision > Projects > Local**.
  - b) Select the project and click the **Snapshots** tab on the right pane.
  - c) Select the desired snapshot.
  - d) Click **Clone**.
  - e) In the **Confirmation** dialog box, click **Yes**.
  - f) In the **Clone Project** window, type a name for the clone and use the initiators that are the same as the rest of the Microsoft cluster LUNs.
2. On the Windows host, run the **DiskPart** utility:  

```
C:\Windows\System32\diskpart.exe
```
3. Run the following commands to find the cloned disk that you want to import to the Windows host.

This step makes sure the disk has been surfaced and visible on the Windows host. You might have to adjust the iSCSI or Fibre initiator or target if the disk is not visible at this stage.

The following command displays the policy used on the current machine to online or offline a newly arrived disk or cloned disk.

```
DISKPART> san
```

Use the following commands to scan for newly added disk.

```
DISKPART> rescan disk
```

Use the following command to view the disks.

```
DISKPART> list disk
```

For example:

Disk	###	Status	Size	Free	Dyn	Gpt
Disk 0		Online	730 GB	1024 KB		
Disk 1		Online	1024 MB	1984 KB		
Disk 2		Offline	1024 MB	1984 KB		

This command helps you select a specific disk.

```
DISKPART> select disk <disk Number X>
```

For example, 'select disk 2'. You can identify it by number, size or partition type. This should be the same size as the original source disk.

Disk 2 now has an asterisk.

Disk	###	Status	Size	Free	Dyn	Gpt
Disk 0		Online	730 GB	1024 KB		
Disk 1		Online	1024 MB	1984 KB		
* Disk 2		Offline	1024 MB	1984 KB		

#### 4. Clear the offline, read-only, hidden and snapshot attributes.

Often due to SAN policy, new disks are added to a Windows server as offline and read-only by design.

This command clears the read only attributes of the disk.

```
DISKPART> attributes disk clear readonly
```

```
DISKPART> select disk <disk Number X>
```

For example, 'select disk 2'.

This command brings the disk online.

```
DISKPART> online disk
```

This command displays the disks. Disk 2 is now online.

```
DISKPART> list disk
```

Disk #	Status	Size	Free	Dyn	Gpt
Disk 0	Online	730 GB	1024 KB		
Disk 1	Online	1024 MB	1984 KB		
Disk 2	Online	1024 MB	1984 KB		

This command shows the volume number.

```
DISKPART> select volume <volume Number X>
```

For example, type 'select volume 10'

Volume #	Ltr	Label	Fs	Type	Size	Status	Info
Volume 10	F	_IS134_1	NTFS	Partition	1021 MB	Healthy	

This command is for clearing the attributes of clones created from the quiesced Volume Shadow Copy (VSS) snapshots.

```
DISKPART> attributes volume clear readonly hidden shadowcopy
```

 **Note:** Clones made from unquiesced array snapshots have read-write attribute. They do not require the attributes to be reset. However these unquiesced manual snapshots may have lower fidelity and application consistency.

## Adding a Cloned LUN to a Microsoft Failover Cluster

Complete the following steps to add a cloned LUN to a Microsoft Failover Cluster:

1. Press **Windows** and **R** keys to open the **Run** dialog box.
2. Type `CluAdmin.msc` in the **Run** dialog box to open the **Failover Cluster Manager** snap-in.
3. Remove the original LUN that the clone is based on from the MS cluster:
  - a) Mark the original LUN disk resources as offline in the Cluster Manager.
  - b) Remove the original LUN as part of the clustered storage.

- c) Mask the original LUNs from this computer (and all other nodes if the computer is in a cluster), through the IntelliFlash Web UI.
- 4. Create the clone from the snapshot of the original LUN.  
Make sure the new clone has initiator and target mappings on the IntelliFlash array that can be accessed by all nodes in the MS Cluster.
- 5. Bring the cloned LUN online and clear its snapshot attributes with the ClearSnapshotInfo.exe or Diskpart utility.
- 6. In the Failover Cluster Manager snap-in, browse to the available storage and add the new clone to the cluster.
- 7. If you want the CSV volume, add the cloned LUN to the Cluster Shared Volumes.

## Recovering Hyper-V VMs

With IDPS 2.1.x, Hyper-V backups are application consistent, on a fresh install. For VM recovery, you can use the snapshot of the VM share or the LUN. You can either roll back the snapshot (in this case the VM is back online) or you can clone the snapshot (in this case, the user creates a new VM based on the cloned VM).

To recover a Hyper-V VM, start with merging the AVHDX file chain. This provides the point in time of the VSS snapshot. After the rollback or cloning, do not start the VM right away. First, merge the VSS snapshot with AVHDX chain to get a fully merged parent VHDX file. This prevents accidental changes to the AVHDX chains and prevents confusion with other backup chains. The AVHDX merge process should be done for both clone and rollback.

After the VM starts successfully, it's a best practice to delete all other VM snapshot chains either manually or in the Hyper-V Manager to prevent conflicts.

### Recovering VMs Using Recovery Script

Run the **Recover-TsVM** command from the PowerShell module. This script helps find and merge the VHDS.

1. For rolling back a snapshot of a VM, run the following PowerShell Module command:

```
Recover-TsVM <your-vm-name>
```

This script makes sure the VM is powered down, finds all the auto-recovery VHDX and merges them, and re-attaches the merged VHDX files to the VM.

2. For cloning a VM from a snapshot, run the following Powershell module command:

```
Recover-TsVM <-VhdPath xxxxxxxxx-autoRecovery.AVHDX path>
```

This script merges all the differencing VHDX in the specified clone path. You can then take this newly merged VHDX file and create a cloned VM using the **Create VM** wizard or from Powershell.

## Recovering VMs from Hyper-V Manager

Complete the following steps to recover VMs from Hyper-V Manager:

1. Select **Inspect Disk** from the Hyper-V Manager UI to obtain properties of each VHD in the backup chain.
  - **Inspect Disk** lists the parent VHDX (this chain must be merged).
  - **Inspect Disk** helps follow the dependency chain (however this inspection is optional and is not required for the merge).
  - Start **Inspect Disk** command with the the most recent xxxxxxxxxxxxxxxx-AutoRecovery.avdx differencing VHD.
2. Select **Edit Disk** from the Hyper-V Manager UI to merge the parent VHDX.
  - Select the most recent auto-recovery.avhdx in each of your vhdx directories.
  - Then select to merge the AVHDX.
  - Then select to merge with the parent.
  - Repeat these steps until there are no more parent VHDs.
3. Fix the VM disk paths to point to the completely merged VHDX path (i.e. the original VHDX not the AVHDX differencing VHD).

After rollback, the VM disk path might have been set to the AVHDX file that is the start of the last VSS backup. This needs to be set to the now fully merged VHDX file (not the AVHDX file).
4. After setting the VM disk path to the fully merged VHDX, restart the VM.

The VM is now ready to be used.



---

# Appendix

## A

---

### IntelliFlash Support Logs and IntelliCare Data

---

**Topics:**

- *IntelliFlash Log Files and Analytics Data Files*

## IntelliFlash Log Files and Analytics Data Files

---

The IntelliFlash array zips analytics data files and log files into one zip file for upload to the IntelliCare portal. The IntelliCare portal processes the uploaded files from the zip file to help analyze your storage array usage. Table 2 provides details on the .zip file uploaded from the IntelliFlash array to the IntelliCare portal.

**Table 19: Zip Upload File Contents**

File name	Description
adm.messages	Contains system log files
audit log	Contains GUI operations audit log
Cbce log	GUI back end command log
exec log	CLI command log
Analytics data files	<p>The following are different analytics data files uploaded to IntelliCare depending on the array usage:</p> <ul style="list-style-type: none"> <li>• CPU analytics</li> <li>• IO analytics</li> <li>• Protocol analytics</li> <li>• Network analytics</li> <li>• Protocol analytics (NFS, CIFS, FC, iSCSI)</li> <li>• Pool performance analytics</li> <li>• VM analytics</li> </ul>
fmdump-error	Contains fault management error details.
fmdump-info	Contains fault management information details.
fmdump-info-high-val	Contains additional fault management information details.

File name	Description
Metadata log	<p>The metadata log file can include the following details:</p> <ul style="list-style-type: none"> <li>• SAN info – target and initiator</li> <li>• IPMI</li> <li>• SATADOM</li> <li>• System event log details</li> <li>• Disks list</li> <li>• SAN group details</li> <li>• Array model</li> <li>• Chassis ID</li> <li>• Replication details – Replication history</li> <li>• Array name</li> <li>• Upgrade history</li> <li>• Network interfaces</li> <li>• Scheduled tasks list</li> <li>• List of log files and their names</li> <li>• Snapshot rules</li> <li>• Pool names and their details</li> <li>• Pool configuration details</li> <li>• SAN group host details</li> <li>• Projects and their details</li> <li>• Disks and their details</li> <li>• iSCSI initiator details</li> <li>• SMTP configuration details</li> <li>• IntelliFlash version details</li> <li>• Expansion shelf details</li> <li>• SAN iSCSI target details</li> </ul>
watcher log	Monitors the different services in the array and logs the details.
Zebirep log	Contains complete replication related details.
Zebiui log	Contains IntelliFlash Web UI IntelliFlash Web UI logs details.
Light Support log	Disk Status log: Contains the log files related to disk status
	FC log: Contains FC remote, HBA and ports related log details
	HA log: Contains the cluster and nodes log details

File name	Description
	History log: Contains the last login, uptime, and last reboot log details
	IPMI log: Contains the chassis status BMC info and other IPMI related log files.
	iSCSI: Contains the iSCSI connection, iSCSI session, trace target portals, initiator list, target list, LUN error logs, STMF and other iSCSI related log details files
	Memory log: Contains system logs, stack logs and other memory related log details
	Network log: Contains IPMP, netstat and other network related log files
	NFS log: Contains output from NFS related commands that contain configuration and status log details
	Process log: Contains open file descriptors and currently open processes log files
	SMB log: Contains outputs from SMB related commands that contain configuration and status log details
	SVCS: Contains log details of the temporary connection created during data transfer
	Swap log: Contains logs related to swap operation
	System_config: Contains system configuration log details
	System_messages log: Contains logs related to system messages

---

# Appendix

## B

---

## NDMP Backup Configuration for Netbackup 8.1 and Commvault V11

---

**Topics:**

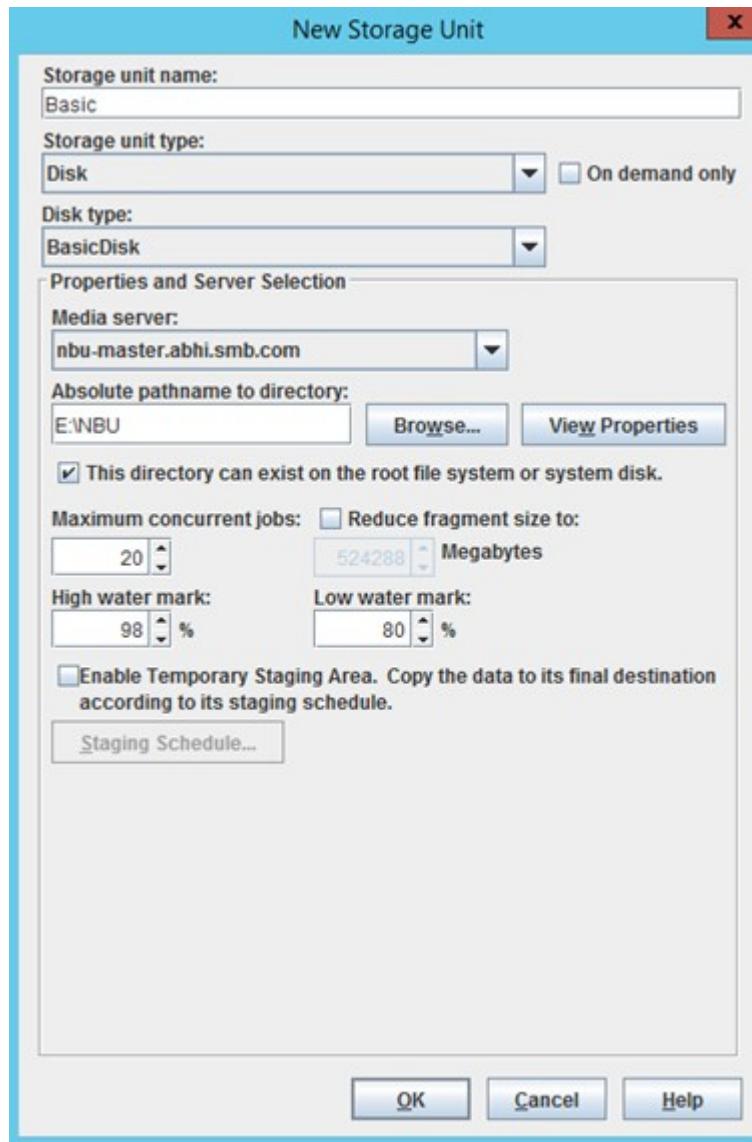
- *NDMP Backup Configuration with NetBackup 8.1*
- *NDMP Backup Configuration with Commvault V11*

## NDMP Backup Configuration with NetBackup 8.1

Make sure that the NBU master server installation is finished before you start NDMP backup configuration.

To configure NDMP backup with NetBackup 8.1, complete the following steps:

1. Create NBU storage units. In NBU console, go to *NetBackup Management > Storage > Storage Units > New Storage Unit*.

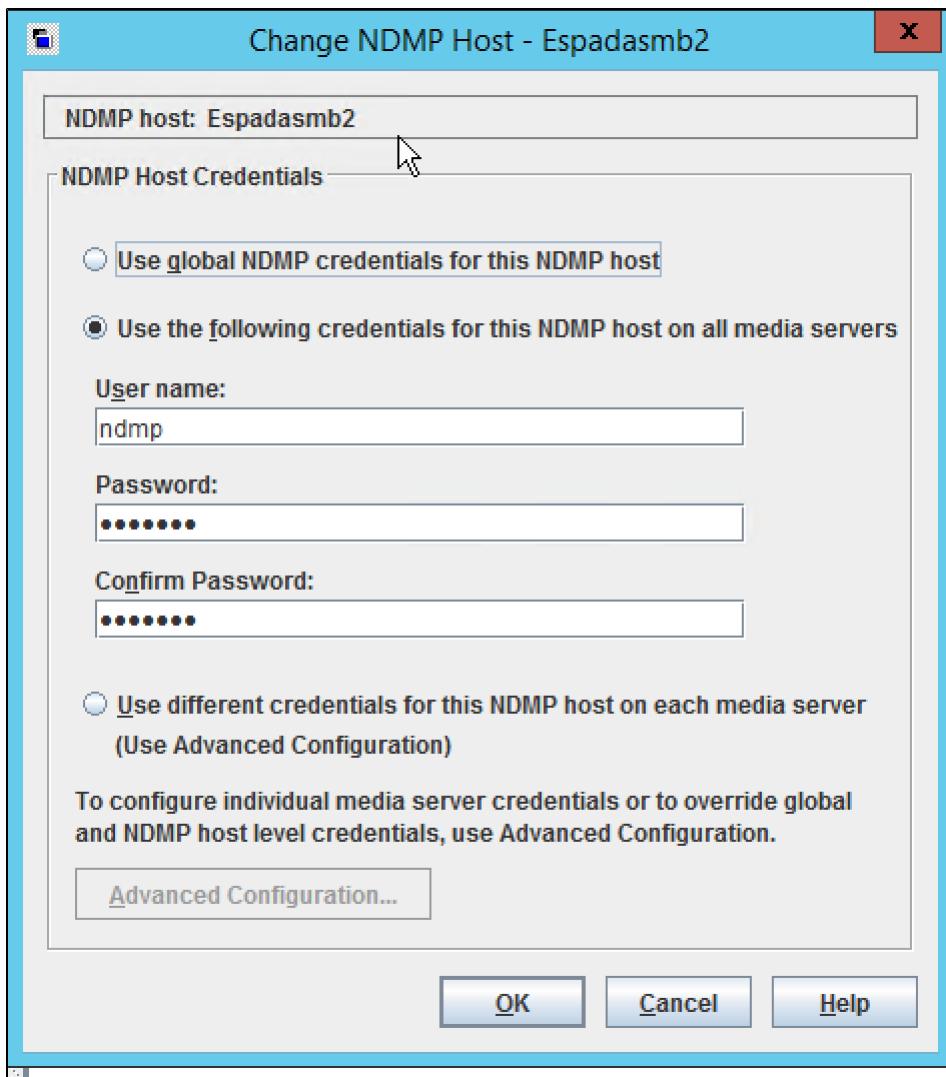


**Figure 36: New Storage Unit**

This STU Can be used to take backups from the clients.

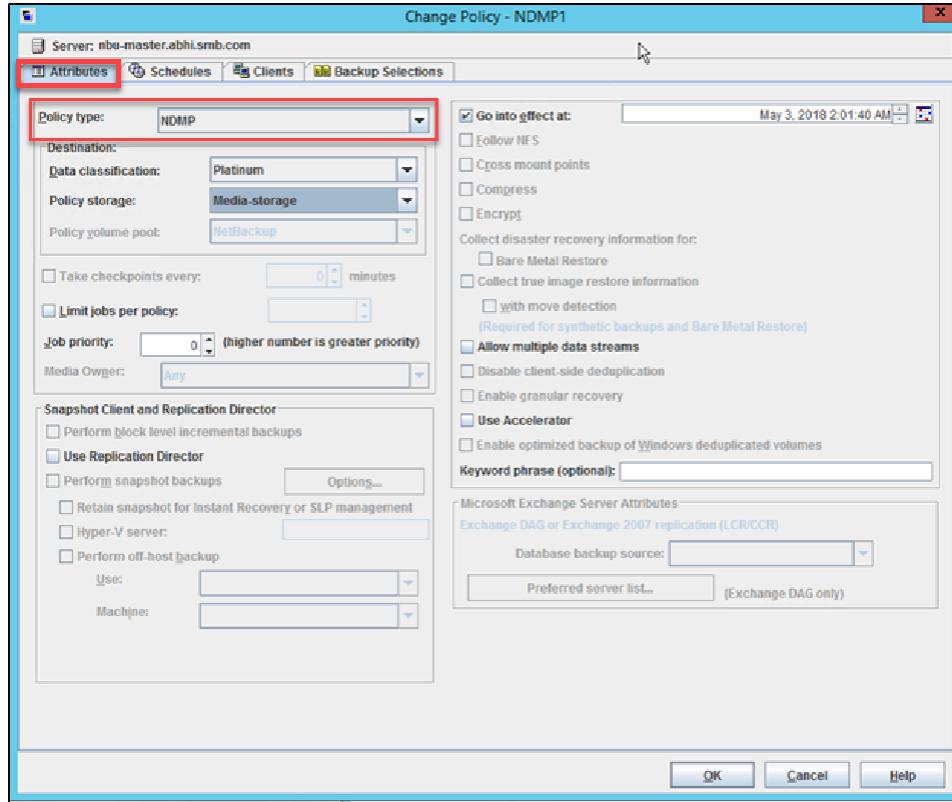
2. Add Zebi as NDMP host in the NBU console. After enabling the NDMP server, go to *Console > Media and Device Management > Credentials > NDMP Hosts > New NDMP host*.

User should use the 10G floating IP/FQDN for this purpose.



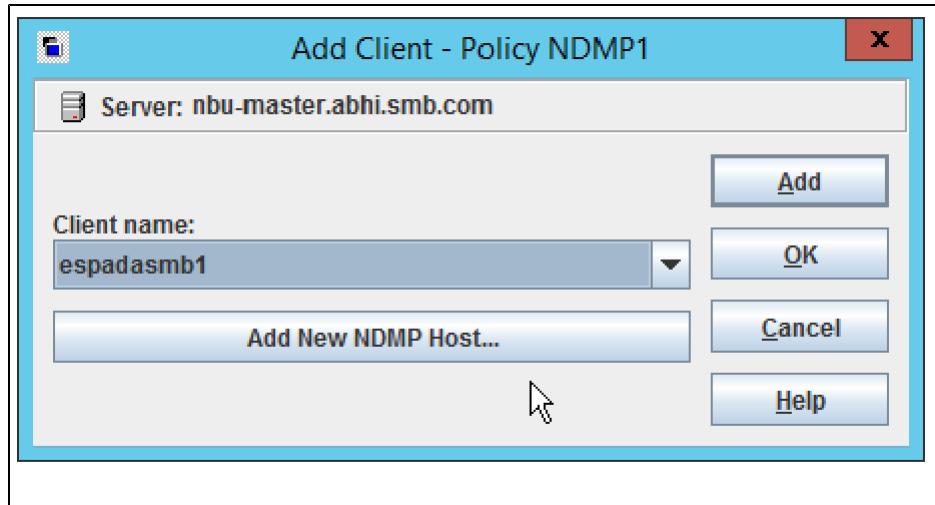
**Figure 37: NDMP Host**

3. Create a new policy from the policy window. In **Attributes** tab, select **Policy type** as **NDMP**.



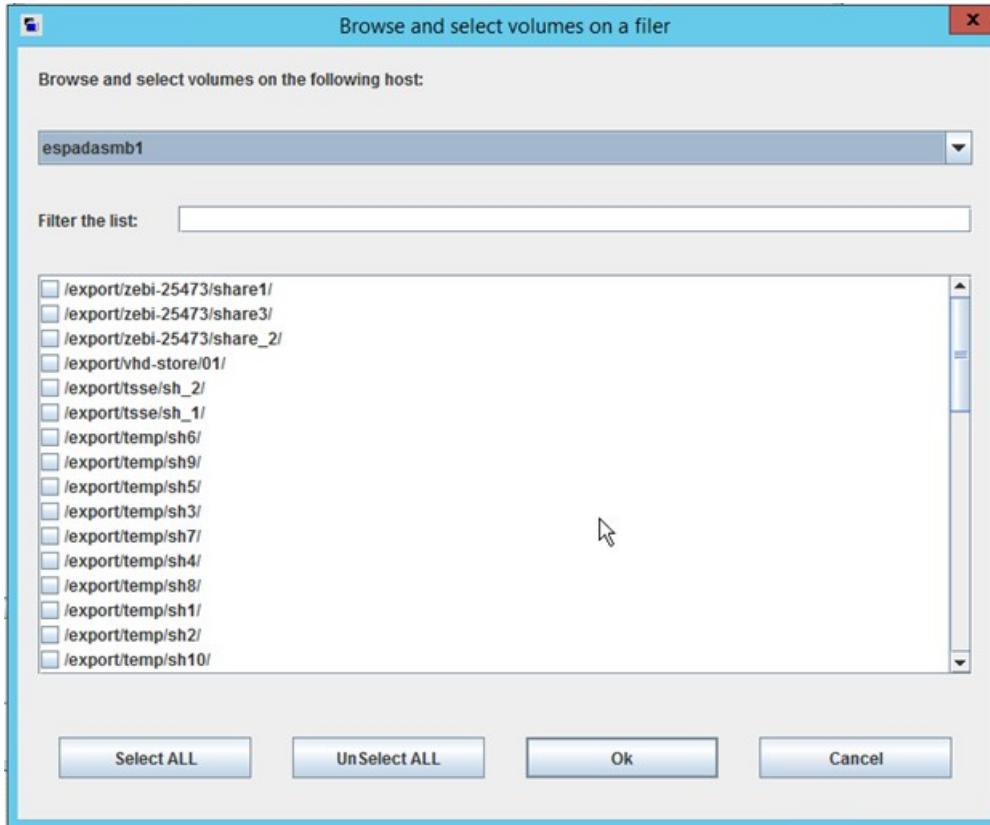
**Figure 38: Change Policy NDMP1**

4. In the **Clients** tab, select **NDMP Host (zebi)** which we added in step 2.



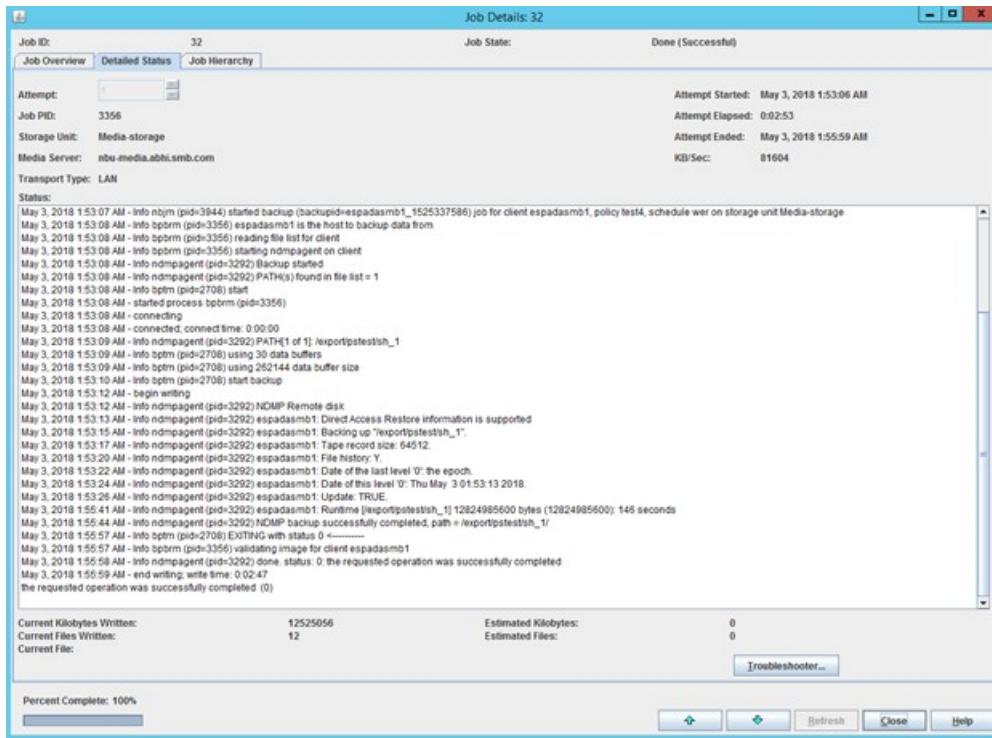
**Figure 39: Adding Client Policy**

5. From the **Backup Selections** tab, click **New selection** and then **Browse**. This will list all the data sets associated with the IP address.



**Figure 40: Data Sets**

6. Make selection for the shares which need to be backed up along with the policy.
7. Run the policy now from the policy window by right clicking and Manual Backup.
8. When the NDMP backup job is in progress, the backup status and throughput can be monitored from the job details window in activity monitor.



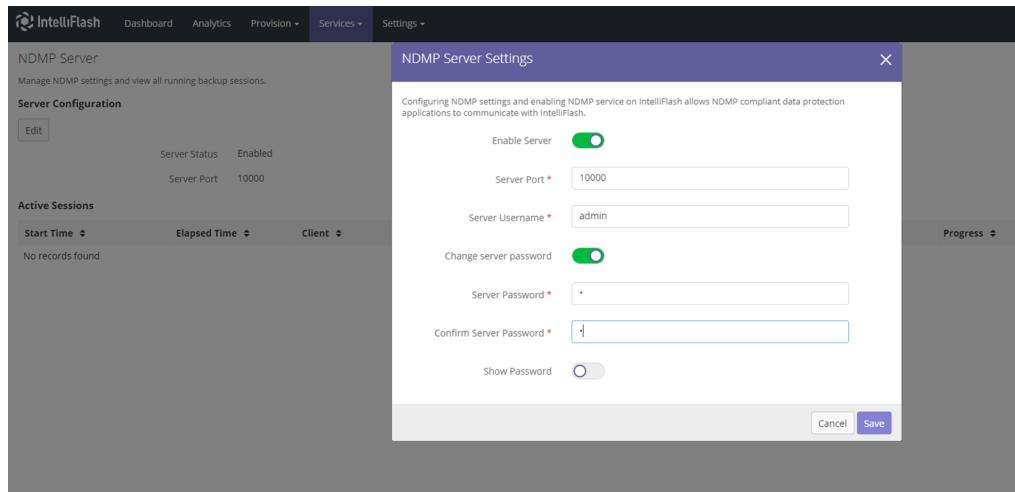
**Figure 41: Job Details**

## NDMP Backup Configuration with Commvault V11

To configure NDMP backup with Commvault:

Complete the following steps on IntelliFlash side:

1. Login to IntelliFlash web UI.
2. Go to **Services > NDMP Server**.
3. Click **Edit**. The **NDMP Server Settings** window is displayed.
4. Click **Enable Server** toggle button.



5. Enter the **Server Username** and **Server Password** for NDMP connections.

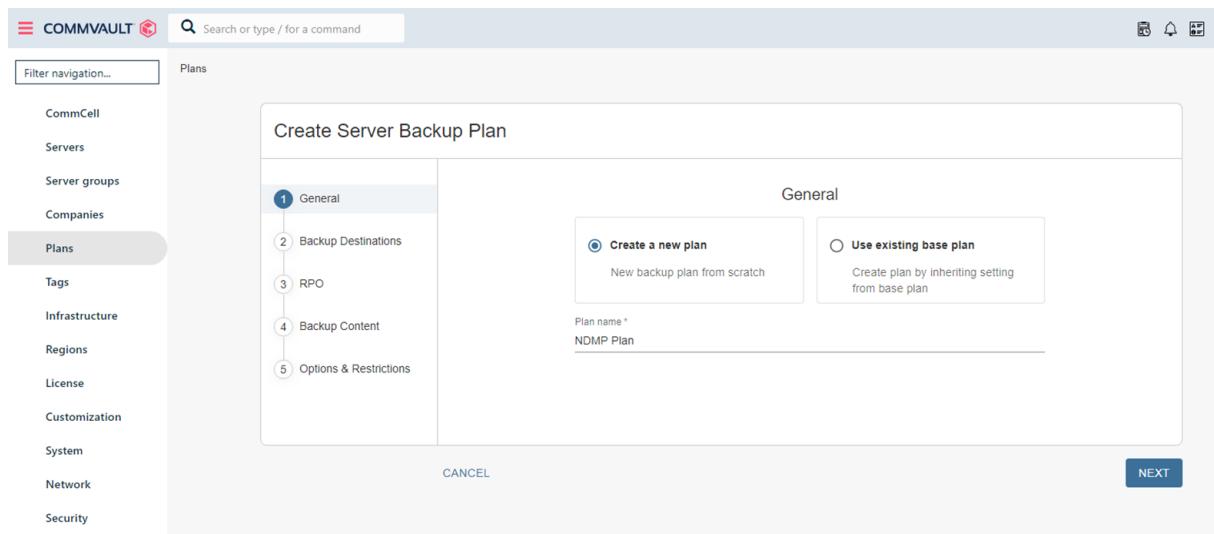
6. Click **Save**.

Complete the following steps on Commvault side:

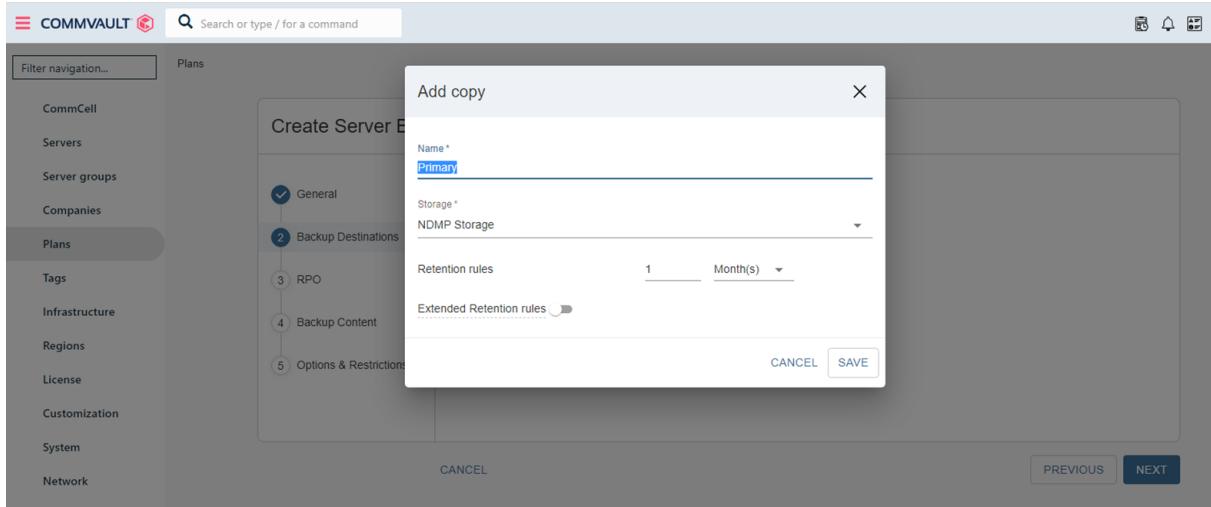
1. Login to Commvault Command Center.
2. To add the storage:
  - a. Go to **Storage > Disk**.
  - b. Click **Add disk storage**.
  - c. Enter the **Name** to new disk storage.

The screenshot shows the Commvault Command Center interface. On the left, there's a navigation sidebar with icons for Activate, Disaster recovery, Jobs, Reports, Monitoring, Storage, HyperScale X, Metallic Cloud Stor..., Distributed Storage, Disk (which is selected and highlighted in grey), Cloud, and Tape. The main area has a search bar at the top right. Below it, under the 'Disk' section, there's a sub-section titled 'Add disk storage'. A modal dialog box is open in the center. It has a header 'Disk' and 'Add disk storage'. Inside, there's a form with a 'Name\*' field containing 'NDMP Storage'. Below that is a 'Backup location' section with a table showing 'MediaAgent' as 'win-232-cmvt' and 'Backup location' as 'F:\Backup'. There's also a 'Use deduplication' toggle switch which is turned on. Underneath, there's a 'Deduplication DB location' section with the message 'No deduplication db location added'. At the bottom of the dialog are 'EQUIVALENT API' buttons for 'CANCEL' and 'SAVE'.

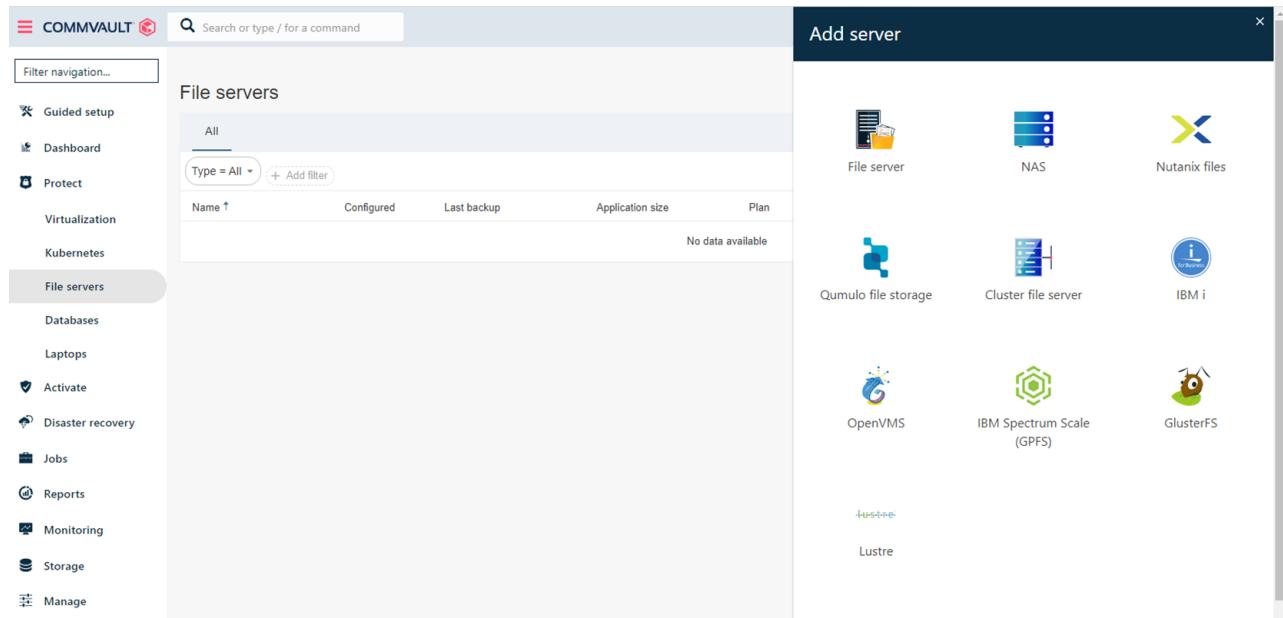
- d. Add a **Backup location**.
  - e. Click **Save**.
3. To add the server plan:
- a. Go to **Manage > Plans**.
  - b. Click **Create Server Backup Plan**.
  - c. Click **General** tab.
  - d. Select **Create a new plan**.



- e. Enter the **Plan name**.
- f. Click **Next**.
- g. Go to the next tab **Backup Destinations**.
- h. Click **Add copy**.



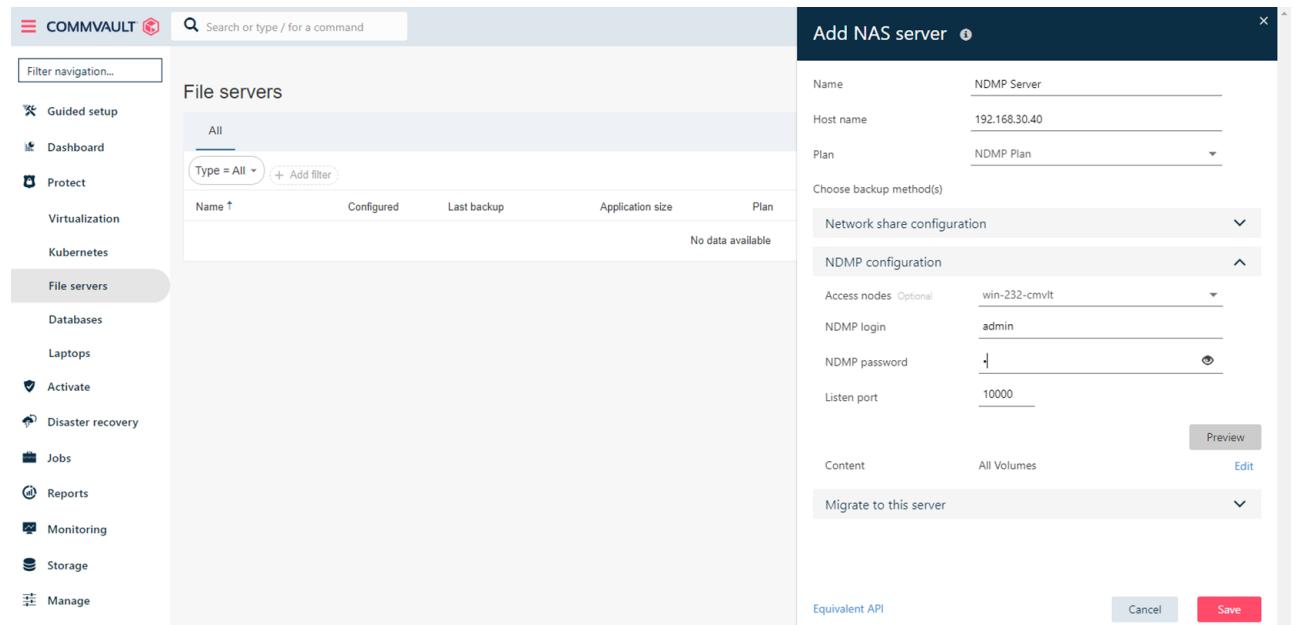
- i. Enter the below details:
  - **Name**
  - **Storage**, add your Backup Destination (Storage that you have created before)
  - **Retention rules**
- j. Click **SAVE**.
- k. Click **NEXT**. The other tabs are optional.
- l. Go to the last tab, click **SUBMIT**.
4. To add the file servers:
  - a. Go to **Protect > File servers**.
  - b. Click **Add server** and choose **NAS**.



The window **Add NAS server** is displayed.

c. Enter the below details:

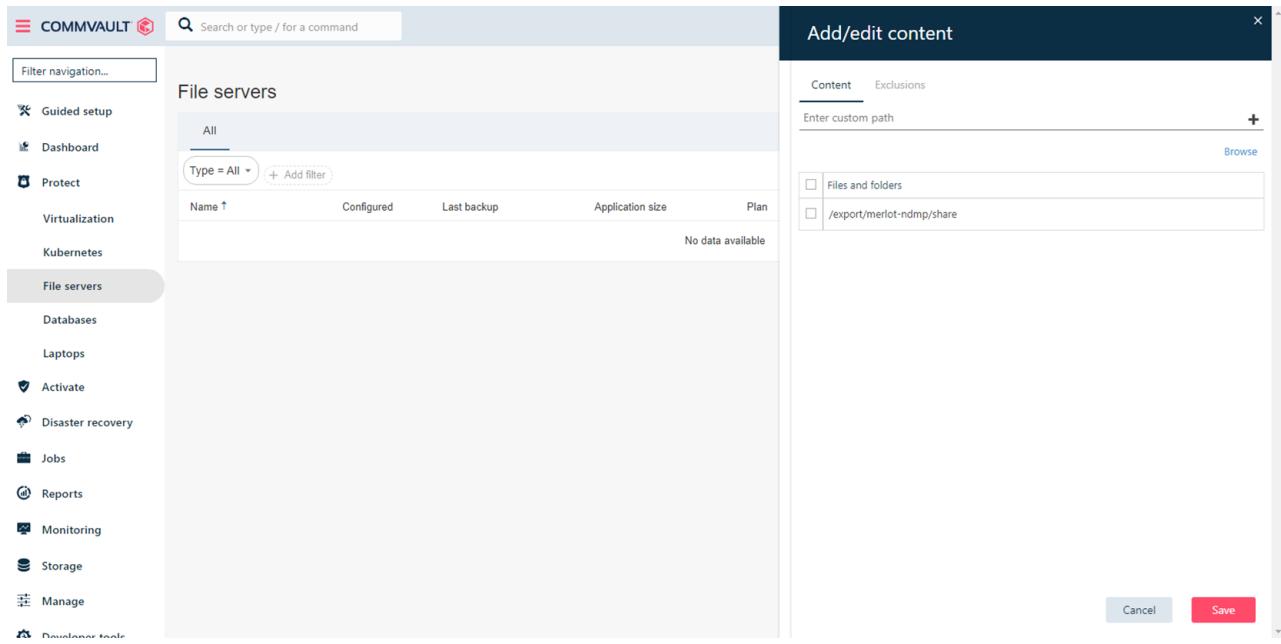
- **Name** of the server.
- Add **Host name** (it should be FQDN/IP of 10G interface of your NDMP server).
- Choose newly created **Plan**.



d. Enter the below in **NDMP configuration** section:

- **Access nodes**
- **NDMP login** and **NDMP password** that you use on IntelliFlash side

e. Click **Edit**. Add the content that you are going to backup.



f. Click **Save**.

5. To backup the NDMP server content:

- a. Go to **Protect > File servers**.
- b. From **Actions** column, click on (...) button.

The screenshot shows the CommVault interface with the 'File servers' list. A context menu is open for the 'NDMP Server' entry, with 'Back up' selected.

Name	Configured	Last backup	Application size	Plan	SLA status	Tags	Actions
NDMP Server	✓	Never backed up	0 B	Not assigned	Excluded	No tags	<i>[More options]</i>

c. Click on **Back up**. The **Select backup level** screen is displayed.

d. Choose **Full** for the first time and click **OK**.

The screenshot shows the CommVault interface with the 'File servers' list. A context menu is open for the 'NDMP Server' entry, with 'Select backup level' chosen, opening a sub-dialog.

**Select backup level**

Subclient or instance being backed up : default

Backup level

Full

Incremental

Differential

When the job completes, notify me via email

Equivalent API

Cancel OK

You can find the progress of back up process in **Jobs** list.

---

## Appendix C

---

### IntelliFlash 3.11.6.2 Interoperability Matrix

---

**Topics:**

- *Interoperability Matrix*  
*IntelliFlash 3.11.6.2*
- 

## Interoperability Matrix IntelliFlash 3.11.6.2

Refer to the table below for IntelliFlash 3.11.6.2 interoperability matrix.

**Table 20: Interoperability Matrix - IntelliFlash 3.11.6.2 Release**

Host OSs / Plug-ins	IntelliFlash OS Version	Supported Block Protocols	Supported File/NAS Protocols	IntelliFlash Arrays
IntelliFlash v3.11.6.2				N6000 and H6000-Series
<b>VMware ESXi</b>				
ESXi 8.0 U1	3.11.6.2	FC, iSCSI	NFS (3.0), NFS (4.1)	Yes
ESXi 7.0 U1, U2, U3	3.11.6.2	FC, iSCSI	NFS (3.0), NFS (4.1)	Yes
IntelliFlash Manager Local VCP vCenter 7.0	3.11.6.2	FC, iSCSI	NFS (3.0)	Yes
IntelliFlash Manager Remote VCP vCenter 8.0*	3.11.6.2	FC, iSCSI	NFS (3.0)	Yes
VMware VAAI NASPlugin ESXi 7.0	3.11.6.2	-	NFS (3.0), NFS (4.1)	Yes
VMware VAAI NASPlugin ESXi 8.0	3.11.6.2	-	NFS (3.0), NFS (4.1)	Yes
IF SRA 2.0.0 for SRM 8.2, 8.3, 8.4, 8.5, 8.6	3.11.6.2	FC, iSCSI	NFS (3.0), NFS (4.1)	Yes
<b>Microsoft Windows Server</b>				
Server 2016	3.11.6.2	FC, iSCSI	SMB3	Yes
Server 2019	3.11.6.2	FC, iSCSI	SMB3	Yes
Server 2022	3.11.6.2	FC, iSCSI	SMB3	Yes
Windows/Hyper-V	3.11.6.2	Support for Server 2016, 2019, and 2022		Yes
SMI-S (SCVMM)	3.11.6.2	Support for SCVMM-2016, 2019, and 2022		Yes
IntelliFlash Data Protection Service (IDPS)	3.11.6.2	Support for Server 2016, 2019, and 2022		Yes

Host OSs / Plug-ins	IntelliFlash OS Version	Supported Block Protocols	Supported File/NAS Protocols	IntelliFlash Arrays
PowerShell Tool Kit	3.11.6.2	Support for Server 2016, 2019, 2022, and .NET Core Powershell		Yes
<b>CSI Driver</b>				
IF CSI driver for File and Block	3.11.6.2	iSCSI	NFS	Yes
<b>3rd Party Backup/Snapshot Applications</b>				
Veeam (Plugin)	3.11.6.2	FC, iSCSI	NFS, SMB	Yes
Commvault - NDMP	3.11.6.2	-	NFS, SMB	Yes
Commvault IntelliSnap	3.11.6.2	FC, iSCSI	-	Yes
Dataflow	3.11.6.2	-	NFS, SMB	Yes
<b>RedHat Linux</b>				
RHEL 8.x	3.11.6.2	FC, iSCSI	NFS	Yes
<b>Ubuntu Linux</b>				
Ubuntu 20.x	3.11.6.2	FC	NFS	Yes

\*Remote VCP vCenter 8.0 is in progress.

