Abstract
This user guide introduces and provides instructions on how to configure, use and troubleshoot
the HPE 3PAR File Persona Software suite, a feature of the HPE 3PAR OS. The File Persona
feature allows the storage administrator to provision storage capacity for file services used on a
HPE 3PAR array for use cases supported by File Persona. This guide is for all levels of system
and storage administrators.
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>File Persona Overview</strong></td>
<td>9</td>
</tr>
<tr>
<td>File Persona Components</td>
<td>9</td>
</tr>
<tr>
<td><strong>File Persona Prerequisites</strong></td>
<td>11</td>
</tr>
<tr>
<td>System and OS Support for File Persona Software</td>
<td>11</td>
</tr>
<tr>
<td><strong>Configuring File Persona</strong></td>
<td>13</td>
</tr>
<tr>
<td>Displaying File Persona Configuration Settings</td>
<td>13</td>
</tr>
<tr>
<td>Displaying Static Route Configuration Settings</td>
<td>13</td>
</tr>
<tr>
<td>Starting File Persona</td>
<td>14</td>
</tr>
<tr>
<td>Stopping/Disabling/Removing File Persona</td>
<td>15</td>
</tr>
<tr>
<td>Restarting File Persona</td>
<td>16</td>
</tr>
<tr>
<td>Configuring File Persona Network Settings</td>
<td>17</td>
</tr>
<tr>
<td>Setting the Bond Mode for File Persona Nodes</td>
<td>17</td>
</tr>
<tr>
<td>Setting the Maximum Transmission Unit Size for File Persona Nodes</td>
<td>17</td>
</tr>
<tr>
<td>Configuring Node IP Addressing for File Persona Nodes</td>
<td>18</td>
</tr>
<tr>
<td>Setting the Default Gateway Address for File Persona</td>
<td>18</td>
</tr>
<tr>
<td>Configuring Static Routes for File Persona</td>
<td>19</td>
</tr>
<tr>
<td>Setting DNS Addresses and Domain Suffixes for File Persona</td>
<td>21</td>
</tr>
<tr>
<td>Reverting to an Earlier Version of HPE 3PAR OS with File Persona</td>
<td>21</td>
</tr>
<tr>
<td><strong>Authentication</strong></td>
<td>23</td>
</tr>
<tr>
<td>Active Directory (AD)</td>
<td>23</td>
</tr>
<tr>
<td>Joining File Persona Nodes to an Active Directory Domain</td>
<td>23</td>
</tr>
<tr>
<td>Removing File Persona Nodes from an Active Directory Domain</td>
<td>23</td>
</tr>
<tr>
<td>Configuring RFC2307 to use with Active Directory</td>
<td>24</td>
</tr>
<tr>
<td>Active Directory (AD)</td>
<td>25</td>
</tr>
<tr>
<td>Local Users and Groups</td>
<td>25</td>
</tr>
<tr>
<td>Displaying Settings for Local Users and Groups</td>
<td>25</td>
</tr>
<tr>
<td>Creating Local Users</td>
<td>25</td>
</tr>
<tr>
<td>Removing Local Users</td>
<td>26</td>
</tr>
<tr>
<td>Modifying Settings for Local Users</td>
<td>27</td>
</tr>
<tr>
<td>Creating Local Groups</td>
<td>27</td>
</tr>
<tr>
<td>Removing Local Groups</td>
<td>28</td>
</tr>
<tr>
<td>Modifying Membership of Local Groups</td>
<td>29</td>
</tr>
<tr>
<td>Lightweight Directory Access Protocol (LDAP)</td>
<td>30</td>
</tr>
<tr>
<td>Configuring LDAP Servers</td>
<td>30</td>
</tr>
<tr>
<td>Removing LDAP Servers</td>
<td>31</td>
</tr>
<tr>
<td>Configuring the Authentication Provider Stacking Order</td>
<td>31</td>
</tr>
<tr>
<td><strong>User Mapping</strong></td>
<td>32</td>
</tr>
<tr>
<td>User Identification</td>
<td>33</td>
</tr>
<tr>
<td>User Mapping Rules</td>
<td>33</td>
</tr>
<tr>
<td>Rules and Operators for User Mapping</td>
<td>34</td>
</tr>
<tr>
<td>Displaying User Mapping for File Persona Nodes</td>
<td>36</td>
</tr>
<tr>
<td>Configuring User Mapping for File Persona</td>
<td>39</td>
</tr>
<tr>
<td>Displaying Mapped User/Group Entries</td>
<td>39</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Permission Conversion Rules for Converged ACLs</td>
<td>123</td>
</tr>
<tr>
<td>Comparison of Security Modes</td>
<td>122</td>
</tr>
<tr>
<td>Security Modes</td>
<td>119</td>
</tr>
<tr>
<td>Legacy</td>
<td>119</td>
</tr>
<tr>
<td>NTFS</td>
<td>120</td>
</tr>
<tr>
<td>Security Enforcement</td>
<td>120</td>
</tr>
<tr>
<td>Share Folder Permissions</td>
<td>121</td>
</tr>
<tr>
<td>Cross-protocol Access</td>
<td>119</td>
</tr>
<tr>
<td>Configuring Access Control for FTP shares</td>
<td>96</td>
</tr>
<tr>
<td>Protocol and Message Format</td>
<td>97</td>
</tr>
<tr>
<td>FTP File Share Connection Mode Configuration</td>
<td>96</td>
</tr>
<tr>
<td>SSL Enabled FTP File Share</td>
<td>97</td>
</tr>
<tr>
<td>Certificates for FTP Share</td>
<td>97</td>
</tr>
<tr>
<td>Home Directory Support</td>
<td>97</td>
</tr>
<tr>
<td>Authentication and Permissions</td>
<td>98</td>
</tr>
<tr>
<td>FTP File Share Configuration Options</td>
<td>99</td>
</tr>
<tr>
<td>cURL Commands</td>
<td>103</td>
</tr>
<tr>
<td>cURL Examples</td>
<td>103</td>
</tr>
<tr>
<td>Managing FTP File Shares</td>
<td>104</td>
</tr>
<tr>
<td>Displaying FTP File Shares</td>
<td>104</td>
</tr>
<tr>
<td>Creating File Shares</td>
<td>105</td>
</tr>
<tr>
<td>Removing FTP File Shares</td>
<td>106</td>
</tr>
<tr>
<td>Modifying FTP File Shares</td>
<td>107</td>
</tr>
<tr>
<td>Object Access API File Share</td>
<td>111</td>
</tr>
<tr>
<td>Configuring Global Object Access API Settings</td>
<td>111</td>
</tr>
<tr>
<td>Managing Object Access API File Shares</td>
<td>112</td>
</tr>
<tr>
<td>Displaying Object Access API File Shares</td>
<td>112</td>
</tr>
<tr>
<td>Creating Object Access API File Shares</td>
<td>112</td>
</tr>
<tr>
<td>Removing Object Access API File Shares</td>
<td>114</td>
</tr>
<tr>
<td>Modifying Object Access API File Shares</td>
<td>114</td>
</tr>
<tr>
<td>FTP File Share</td>
<td>95</td>
</tr>
<tr>
<td>FTP File Share Overview</td>
<td>96</td>
</tr>
<tr>
<td>FTP File Shares and File Store Security Modes</td>
<td>96</td>
</tr>
<tr>
<td>Configuring Access Control for FTP shares</td>
<td>96</td>
</tr>
<tr>
<td>Protocol and Message Format</td>
<td>97</td>
</tr>
<tr>
<td>FTP File Share Connection Mode Configuration</td>
<td>96</td>
</tr>
<tr>
<td>SSL Enabled FTP File Share</td>
<td>97</td>
</tr>
<tr>
<td>Certificates for FTP Share</td>
<td>97</td>
</tr>
<tr>
<td>Home Directory Support</td>
<td>97</td>
</tr>
<tr>
<td>Authentication and Permissions</td>
<td>98</td>
</tr>
<tr>
<td>FTP File Share Configuration Options</td>
<td>99</td>
</tr>
<tr>
<td>cURL Commands</td>
<td>103</td>
</tr>
<tr>
<td>cURL Examples</td>
<td>103</td>
</tr>
<tr>
<td>Managing FTP File Shares</td>
<td>104</td>
</tr>
<tr>
<td>Displaying FTP File Shares</td>
<td>104</td>
</tr>
<tr>
<td>Creating File Shares</td>
<td>105</td>
</tr>
<tr>
<td>Removing FTP File Shares</td>
<td>106</td>
</tr>
<tr>
<td>Modifying FTP File Shares</td>
<td>107</td>
</tr>
<tr>
<td>NFS File Share</td>
<td>85</td>
</tr>
<tr>
<td>NFS File Share Overview</td>
<td>86</td>
</tr>
<tr>
<td>NFS Export Options</td>
<td>86</td>
</tr>
<tr>
<td>Managing NFS File Shares</td>
<td>87</td>
</tr>
<tr>
<td>Displaying NFS File Shares</td>
<td>87</td>
</tr>
<tr>
<td>Creating NFS File Shares</td>
<td>88</td>
</tr>
<tr>
<td>Removing NFS File Shares</td>
<td>90</td>
</tr>
<tr>
<td>Modifying NFS File Shares</td>
<td>91</td>
</tr>
<tr>
<td>NFS File Share</td>
<td>85</td>
</tr>
<tr>
<td>Object Access API File Share</td>
<td>111</td>
</tr>
<tr>
<td>Configuring Global Object Access API Settings</td>
<td>111</td>
</tr>
<tr>
<td>Managing Object Access API File Shares</td>
<td>112</td>
</tr>
<tr>
<td>Displaying Object Access API File Shares</td>
<td>112</td>
</tr>
<tr>
<td>Creating Object Access API File Shares</td>
<td>112</td>
</tr>
<tr>
<td>Removing Object Access API File Shares</td>
<td>114</td>
</tr>
<tr>
<td>Modifying Object Access API File Shares</td>
<td>114</td>
</tr>
<tr>
<td>FTP File Share</td>
<td>95</td>
</tr>
<tr>
<td>FTP File Share Overview</td>
<td>96</td>
</tr>
<tr>
<td>FTP File Shares and File Store Security Modes</td>
<td>96</td>
</tr>
<tr>
<td>Configuring Access Control for FTP shares</td>
<td>96</td>
</tr>
<tr>
<td>Protocol and Message Format</td>
<td>97</td>
</tr>
<tr>
<td>FTP File Share Connection Mode Configuration</td>
<td>96</td>
</tr>
<tr>
<td>SSL Enabled FTP File Share</td>
<td>97</td>
</tr>
<tr>
<td>Certificates for FTP Share</td>
<td>97</td>
</tr>
<tr>
<td>Home Directory Support</td>
<td>97</td>
</tr>
<tr>
<td>Authentication and Permissions</td>
<td>98</td>
</tr>
<tr>
<td>FTP File Share Configuration Options</td>
<td>99</td>
</tr>
<tr>
<td>cURL Commands</td>
<td>103</td>
</tr>
<tr>
<td>cURL Examples</td>
<td>103</td>
</tr>
<tr>
<td>Managing FTP File Shares</td>
<td>104</td>
</tr>
<tr>
<td>Displaying FTP File Shares</td>
<td>104</td>
</tr>
<tr>
<td>Creating File Shares</td>
<td>105</td>
</tr>
<tr>
<td>Removing FTP File Shares</td>
<td>106</td>
</tr>
<tr>
<td>Modifying FTP File Shares</td>
<td>107</td>
</tr>
<tr>
<td>Object Access API File Share</td>
<td>111</td>
</tr>
<tr>
<td>Configuring Global Object Access API Settings</td>
<td>111</td>
</tr>
<tr>
<td>Managing Object Access API File Shares</td>
<td>112</td>
</tr>
<tr>
<td>Displaying Object Access API File Shares</td>
<td>112</td>
</tr>
<tr>
<td>Creating Object Access API File Shares</td>
<td>112</td>
</tr>
<tr>
<td>Removing Object Access API File Shares</td>
<td>114</td>
</tr>
<tr>
<td>Modifying Object Access API File Shares</td>
<td>114</td>
</tr>
<tr>
<td>Cross-protocol Access</td>
<td>119</td>
</tr>
<tr>
<td>Security Modes</td>
<td>119</td>
</tr>
<tr>
<td>Legacy</td>
<td>119</td>
</tr>
<tr>
<td>NTFS</td>
<td>120</td>
</tr>
<tr>
<td>Security Enforcement</td>
<td>120</td>
</tr>
<tr>
<td>Share Folder Permissions</td>
<td>121</td>
</tr>
<tr>
<td>Comparison of Security Modes</td>
<td>122</td>
</tr>
<tr>
<td>Permission Conversion Rules for Converged ACLs</td>
<td>123</td>
</tr>
<tr>
<td>File Access Auditing</td>
<td>125</td>
</tr>
<tr>
<td>File Access Auditing Framework</td>
<td>125</td>
</tr>
<tr>
<td>Auditing SMB File Shares</td>
<td>126</td>
</tr>
<tr>
<td>Auditing NFS File Shares</td>
<td>130</td>
</tr>
<tr>
<td>Displaying File Access Auditing Policy</td>
<td>134</td>
</tr>
</tbody>
</table>
Storage Quotas

Displaying Storage Quota Settings.............................................................. 144
Setting Storage Quotas................................................................................ 146
Archiving and Restoring Storage Quota Settings....................................... 147
  Archiving Usage Quotas......................................................................... 147
  Restoring and Importing Usage Quotas..................................................... 148

Antivirus Scanning

Antivirus Scan Integration........................................................................... 150
Antivirus Scanning....................................................................................... 150
Antivirus Installation and Configuration...................................................... 151
Initiating an Antivirus Scan........................................................................ 152
Pausing and Stopping Antivirus Scans......................................................... 153
Resuming an Antivirus Scan on a VFS or File Store................................... 154
Displaying Status for Antivirus Scans, Policies, and Quarantined Files....... 155
Configuring Antivirus Scanning Policies...................................................... 155
Managing Quarantine Settings and Files.................................................... 157
  Quarantine operations - Exporting, Resetting, Moving, Deleting and Count Clearing
  Infected Files.......................................................................................... 158
Updating Virus Definitions........................................................................ 160
Enabling Virus Definitions.......................................................................... 160

File Lock

File Lock Enterprise.................................................................................. 161
  Conversion of a Normal File to WORM File........................................... 162
    Transforming a Normal File to a WORM file without Autocommit period.. 162
    Transforming a Normal File to a WORM File with Autocommit period.... 163
File Lock Compliance.................................................................................. 163
  Compliance Officer................................................................................. 163
  Enabling Dual Admin Authentication..................................................... 165
  Managing Dual Admin Authentication Requests................................. 166
Data Retention............................................................................................ 174
  Managing Data Retention...................................................................... 174
  Data Retention Policy and Attributes.................................................... 175
  Defining Data Retention Policies......................................................... 175
    Configuring and Enabling Data Retention Policies.............................. 176
    Policy Inheritance.............................................................................. 177
    Viewing Data Retention Policies....................................................... 177
    Viewing Data Retention Information................................................. 177
WORM File Administration....................................................................... 178
  Changing Retention Period.................................................................... 179
  Removing the Retention Period............................................................. 179
Troubleshooting File Persona ................................................................. 197

Monitoring File Persona ........................................................................ 191

File Persona Prerequisite Checklist ........................................................ 205

Data Protection ........................................................................................ 187

Montioring File Persona Performance using SSMC.................................... 192
Performance Monitoring for Object Access API Statistics........................ 192
Performance Parameters for Object Access API........................................ 196

Troubleshooting File Persona ................................................................. 197

Data Protection........................................................................................ 187

Monitoring File Persona........................................................................ 191

Troubleshooting File Persona ................................................................. 197

File Persona Prerequisite Checklist........................................................ 205

Data Validation Scan.............................................................................. 181
Initiating Data Validation Scan................................................................. 182
Resuming Data Validation Scan................................................................. 182
Removing Data Validation Scan............................................................... 182
Stopping/Pausing Data Validation Scan................................................... 182
Viewing Validation Scan Results............................................................... 183
Data Validation Tasks on Failed Node...................................................... 184
Using Hard links for Normal and WORM files........................................ 184
Backup Support for Data Retention......................................................... 184
Archiving Audit Logs............................................................................. 184
Copyfile Support...................................................................................... 185

Data Protection........................................................................................ 187
Backin Up and Restoring File Shares......................................................... 187
Using NDMP over iSCSI............................................................................. 187
Using NDMP for File Store Backup using Snapshots................................ 188
Using Virtual Copy for Local Disaster Recovery....................................... 188
Using Remote Copy for Disaster Recovery.............................................. 189
Configuration Backup and Restore using ACL Inheritance...................... 190
ACLs and Ownership............................................................................. 190
File Store Security.................................................................................. 190

Monitoring File Persona........................................................................ 191
Checking Health of Hardware and Software Components........................ 191
Monitoring File Persona Performance...................................................... 191
Monitoring File Persona Performance using SSMC................................ 192
Monitoring File Persona Performance using SNMP................................ 192
Performance Monitoring for Object Access API Statistics........................ 192
Performance Parameters for Object Access API........................................ 196

Troubleshooting File Persona ................................................................. 197

File Persona Prerequisite Checklist........................................................ 205
File Persona configuration preparation.................................................... 205
File Persona controller node worksheet.................................................. 205
File Persona Activation and Networking worksheet.............................. 206
File Persona Authentication settings worksheet....................................... 207
File Persona protocol settings worksheet............................................... 209
File Persona Local Groups and Users worksheet..................................... 210
File Persona User Identity Mapping with RFC2307 for Active Directory worksheet......................................................... 211
File Persona Virtual File Server worksheet............................................. 212
File Persona File Store Snapshot worksheet.......................................... 213
File Persona SMB Shares worksheet...................................................... 213
File Persona NFS Shares worksheet....................................................... 214
File Persona Object Access API Shares worksheet................................. 215
File Persona Cross-protocol Share Access worksheet............................. 216
Support and other resources........................................................................................................... 219
  Accessing Hewlett Packard Enterprise Support.................................................................... 219
  Accessing updates................................................................................................................... 219
  Customer self repair................................................................................................................ 219
  Remote support....................................................................................................................... 220
  Warranty information............................................................................................................. 220
  Regulatory information.......................................................................................................... 220
  Documentation feedback...................................................................................................... 221

List of Port Numbers.................................................................................................................. 222
File Persona Overview

The HPE 3PAR File Persona Software provides a converged storage solution for file services and object access along with block services on HPE 3PAR StoreServ systems. The HPE 3PAR File Persona Software is a feature of the HPE 3PAR OS first released in 3PAR OS 3.2.1 MU3 that enables a rich set of file protocols and core file data services on the following converged HPE 3PAR StoreServ storage systems:

- HPE 3PAR StoreServ 7000c
- HPE 3PAR StoreServ 8000
- HPE 3PAR StoreServ 9000
- HPE 3PAR StoreServ 20000

It requires the use of an add-on 1GbE or 10GbE NIC on HPE 3PAR StoreServ to provide network ports to serve file services. Alternatively, on-board Remote Copy ports can be used for simple file sharing needs.

Primary File Persona Use Cases

Primary use cases supported by the File Persona software include:

- Home directory consolidation and user shares over SMB or NFS protocols
- Content management and collaboration for SharePoint BLOB storage or Enterprise File Sync and Share
- Data preservation and governance for structured and unstructured data preservation and retention of business records, enterprise information archiving and cold storage for video surveillance
- Binary and configuration storage over NFS shares for SAP HANA
- Custom cloud applications using the Object Access API

NOTE:

- File Persona can only be used when the PersonaProfile parameter set to "Block-preferred" in an HPE 3PAR OS. If the PersonaProfile is set to "Block-only" and you would like to configure File Persona on an HPE 3PAR array, please contact HPE Support to change the setting.
- File Persona cannot be used on older platform generations earlier than HPE StoreServ 7000c.

File Persona Components

The following diagram shows the hierarchy and relationships of the File Persona logical components:

![Diagram of File Persona components]

Figure 1: Logical view of File Persona components
**File Provisioning Group (FPG)**

File Provisioning Groups (FPGs) are an instance of the HPE intellectual property Adaptive File System and is the highest level File Persona managed object in the HPE 3PAR file service hierarchy. FPGs control how files are stored and retrieved. Each FPG is transparently constructed from one or multiple Virtual Volumes (VVs) and is the unit for replication and disaster recovery for the File Persona software. There are up to 16 FPGs supported on a node pair. The FPGs contain the Virtual File Servers (VFSs).

**Virtual File Server (VFS)**

Virtual File Servers (VFSs) act as virtual servers that present virtual IP addresses to clients, participate in user authentication services, and can enforce policies for user and group quota management and antivirus policies. There are up to 16 VFSs supported on a node pair, one per FPG. Many management tasks and policy decisions can be made at the VFS level. VFSs contain the File Stores.

**File Store**

File Stores are created in Virtual File Servers and are the slice of File Provisioning Groups. At the File Store level, you can take snapshots, manage capacity quotas, and customize antivirus scan policies. Up to 256 File Stores are supported on a node pair, 16 File Stores per VFS.

**File Share**

File Shares provide data access to clients through the SMB, NFS, FTP protocols and an Object Access API. Multiple File Shares can be created in a File Store and File Shares may be configured at different directory levels within a File Store.
File Persona Prerequisites

To enable, configure and use the features available in File Persona on an HPE 3PAR StoreServ Storage system, certain prerequisites must be in place.

- Your StoreServ Storage system and HPE 3PAR OS must support File Persona depending on the HPE 3PAR StoreServ Storage platform.
- You must have an active license for File Persona.
- The PersonaProfile parameter needs to be set to "Block-preferred" in the HPE 3PAR OS, if not set already.
- One or more add-on NICs (1GbE or 10GbE) must be dedicated for use by File Persona. In 3PAR OS version 3.2.2 or later, File Persona can be enabled on controller nodes using add-on NICs or if needed, built-in RCIP port can be used. Note that RCIP port is constrained in bandwidth and availability. Both add-on NICs and built-in RCIP port cannot be used together, File Persona can be configured either using ports from add-on NICs or RCIP port.
- Each node in a node pair on which File Persona is to be enabled will require its own IP address and must be connected to your network.
- You will need to have one IP address per controller node reserved in your network infrastructure, plus at least one IP address for each VFS created.

To view and compile a prerequisite checklist for setting up File Persona, visit File Persona configuration preparation.

System and OS Support for File Persona Software

Following is a list of HPE 3PAR StoreServ Storage systems and operating systems that support File Persona.

NOTE:
Storage systems with a * require a separate license to activate File Persona. For more information on viewing the license and activating File Persona, see the HPE 3PAR Command Line Interface Administrator Guide and HPE 3PAR Command Line Interface Reference, available at the HPE Storage Information Library (http://www.hpe.com/info/storage/docs).

For more information about system support and limits for File Persona, see the HPE Single Point of Connectivity Knowledge (SPOCK) website: SPOCK (http://www.hpe.com/storage/spock)

<table>
<thead>
<tr>
<th>Storage System</th>
<th>Operating System</th>
</tr>
</thead>
<tbody>
<tr>
<td>HPE 3PAR StoreServ 7200c *</td>
<td>HPE 3PAR OS 3.2.1 MU3</td>
</tr>
<tr>
<td></td>
<td>HPE 3PAR OS 3.2.2</td>
</tr>
<tr>
<td></td>
<td>HPE 3PAR OS 3.3.1</td>
</tr>
<tr>
<td>HPE 3PAR StoreServ 7400c *</td>
<td>HPE 3PAR OS 3.2.1 MU3</td>
</tr>
<tr>
<td></td>
<td>HPE 3PAR OS 3.2.2</td>
</tr>
<tr>
<td></td>
<td>HPE 3PAR OS 3.3.1</td>
</tr>
<tr>
<td>HPE 3PAR StoreServ 7440c *</td>
<td>HPE 3PAR OS 3.2.1 MU3</td>
</tr>
<tr>
<td></td>
<td>HPE 3PAR OS 3.2.2</td>
</tr>
<tr>
<td></td>
<td>HPE 3PAR OS 3.3.1</td>
</tr>
</tbody>
</table>

Table Continued
<table>
<thead>
<tr>
<th>Storage System</th>
<th>Operating System</th>
</tr>
</thead>
<tbody>
<tr>
<td>HPE 3PAR StoreServ 7450c *</td>
<td>HPE 3PAR OS 3.2.1 MU3</td>
</tr>
<tr>
<td></td>
<td>HPE 3PAR OS 3.2.2</td>
</tr>
<tr>
<td></td>
<td>HPE 3PAR OS 3.3.1</td>
</tr>
<tr>
<td>HPE 3PAR StoreServ 8200</td>
<td>HPE 3PAR OS 3.2.2</td>
</tr>
<tr>
<td></td>
<td>HPE 3PAR OS 3.3.1</td>
</tr>
<tr>
<td>HPE 3PAR StoreServ 8400</td>
<td>HPE 3PAR OS 3.2.2</td>
</tr>
<tr>
<td></td>
<td>HPE 3PAR OS 3.3.1</td>
</tr>
<tr>
<td>HPE 3PAR StoreServ 8440</td>
<td>HPE 3PAR OS 3.2.2</td>
</tr>
<tr>
<td></td>
<td>HPE 3PAR OS 3.3.1</td>
</tr>
<tr>
<td>HPE 3PAR StoreServ 8450</td>
<td>HPE 3PAR OS 3.2.2</td>
</tr>
<tr>
<td></td>
<td>HPE 3PAR OS 3.3.1</td>
</tr>
<tr>
<td>HPE 3PAR StoreServ 9450</td>
<td>HPE 3PAR OS 3.3.1</td>
</tr>
<tr>
<td>HPE 3PAR StoreServ 20450</td>
<td>HPE 3PAR OS 3.2.2</td>
</tr>
<tr>
<td></td>
<td>HPE 3PAR OS 3.3.1</td>
</tr>
<tr>
<td>HPE 3PAR StoreServ 20800</td>
<td>HPE 3PAR OS 3.2.2</td>
</tr>
<tr>
<td></td>
<td>HPE 3PAR OS 3.3.1</td>
</tr>
<tr>
<td>HPE 3PAR StoreServ 20850</td>
<td>HPE 3PAR OS 3.2.2</td>
</tr>
<tr>
<td></td>
<td>HPE 3PAR OS 3.3.1</td>
</tr>
<tr>
<td>HPE 3PAR StoreServ 20840</td>
<td>HPE 3PAR OS 3.2.2</td>
</tr>
<tr>
<td></td>
<td>HPE 3PAR OS 3.3.1</td>
</tr>
</tbody>
</table>
Configuring File Persona

Displaying File Persona Configuration Settings

To display the configuration information for all File Persona nodes in a StoreServ Storage system from the command line, choose your options and issue the following command:

```
```

where the options are as follows:

- **-obj**
  displays the port configuration information for the File Persona nodes.

- **-net**
  displays the network configuration information for the File Persona nodes.

  **NOTE:**
  The `showfs [-net]` command displays only the default gateway for the node-specific IP addresses.

- **-ad**
  displays the Active Directory configuration information for the File Persona nodes.

- **-ldap**
  displays the LDAP configuration information for the File Persona nodes.

- **-auth**
  displays the authentication provider stacking order.

- **-idmap**
  displays the NFSv4 domain name.

- **-rfc2307**
  displays the RFC2307 setting.

- **-smb**
  displays the configured parameters for the SMB protocol.

- **-usermap**
  displays the user mapping, mapped user/group profiles or copies the exported users/group entries or mapping configuration to the client storage. See section Displaying User Mapping for File Persona Nodes on page 36 for detailed subcommand options.

  **NOTE:** The `showfs` command when used with the `usermap` option will return an error message if both the LDAP and AD are not configured.

Displaying Static Route Configuration Settings

To display the static route configuration for File Persona, issue the following command:

```
showfsroute [-d]
```

The command displays the default gateway for the node-specific IP addresses. Static route definitions (such as those for VFS VLANs) also get displayed with the `showfsroute` command.
For more information about the showfs command, see the HPE 3PAR Command Line Interface Reference.

To display the configuration information for File Persona nodes using the SSMC:

- From the main menu, select File Persona > Persona Configuration.
- On the list pane, select the system, and then select Configure File Persona on the Actions menu.
- Select the Advanced options checkbox to display advanced configuration options.

## Starting File Persona

File Persona can be started only on a pair of matched controller nodes.

### Starting File Persona using HPE 3PAR CLI

To start File Persona on a node pair in a StoreServ Storage System from the command line, issue the following command:

```bash
startfs [-cpgname <name>] [<node>:<slot>:<port> <node>:<slot>:<port>]...
```

where,

- `<name>`

  The name of the CPG where the File Persona configuration information will be stored. If CPG name is not provided, or if the specified CPG does not exist, a new CPG will be created automatically. HPE 3PAR StoreServ will first try to create the CPG using FC disks, if that attempt fails for any reason, the system will try to create a CPG using NL disks and lastly it will create using SSD disks.

- `<node>:<slot>:<port>`

  Node, slot, and port number on which File Persona will be started. Node pairs must be specified. Only one valid port for each network interface controller (NIC) needs to be specified to start File Persona on all of the ports on a NIC. If multiple NICs per node are to be used with File Persona (where supported), include one `<node>:<slot>:<port>` specification from each NIC intended for File Persona use.

**NOTE:**

When File Persona is started on a node pair, 150 GB of space is initially allocated from the specified CPG per each node for use by File Persona for configuration data.

The type of network interface (whether an add-on NIC or an on-board interface) for the ports on each node intended to run File Persona must be of same type. File Persona cannot be started using both the onboard port and an add-on NIC at the same time.

If File Persona is already started on a specified port, executing the `startfs` command will generate an error message stating that the port is already reserved for File Persona. In this situation, verify that File Persona is configured on the correct nodes with the `showfs` command. The `showfs` command displays the nodes on which File Persona is started, the status and version of File Persona and more basic configuration information.

Verify the changes with the `showfs` command. For more information about the `startfs` and `showfs` commands, see the HPE 3PAR Command Line Interface Reference.

### Starting File Persona using SSMC

Use the following procedure to start File Persona in the SSMC:

- From the main menu, select File Persona > Persona Configuration.
- On the list pane, select the system, and then select Configure File Persona on the Actions menu.
- In the Node Pairs section, configure a given node pair by clicking the edit icon.
- Toggle the State value for the node pair to Configured.
- Select or add a NIC pair (node:slot:port designation) and specify an IP address for each node in the NIC pair and click OK.
• Specify a subnet mask and a gateway IP address.
• Click Configure.

Starting File Persona on Additional nodes

You can start File Persona on additional nodes after you have initially configured File Persona on a given node pair on a StoreServ Storage system. For example, on an HPE 3PAR array with four nodes, you may have initially configured File Persona on a node pair comprising nodes 0 and 1. You can subsequently start File Persona on the node pair comprising nodes 2 and 3. After starting File Persona on the additional nodes with the startfs command, proceed using the following steps to maintain a consistent File Persona configuration across all nodes in the system:

1. Set a consistent bond mode for all File Persona started nodes by using the setfs bond command or the SSMC. For information on setting the bond mode, see Setting the Bond Mode for File Persona Nodes on page 17.
2. Establish a consistent MTU setting for all File Persona started node by using the setfs mtu command or the SSMC. For information on the MTU setting, see Setting the Maximum Transmission Unit Size for File Persona Nodes on page 17.
3. Add IP addresses to the newly started nodes by using the setfs nodeip command or the SSMC. Use the same subnet mask and VLAN values for all the nodes running File Persona. For information on configuring IP addresses for File Persona nodes, see Configuring Node IP Addressing for File Persona Nodes on page 18.
4. Execute setfs ad or join File Persona using the SSMC again. For information about joining File Persona to AD domains, see Joining File Persona Nodes to an Active Directory Domain on page 23.
5. Optionally, use the setfpg -primarynode command to migrate a subset of the FPGs from the original nodes to the additional nodes in order to balance the load across all of the nodes. For information about setting the primary node for an FPG, see Setting the Primary Node for a File Provisioning Group on page 49.

Please make sure the following necessary steps are taken to ensure that the added node pair is correctly networked.

1. Configure the default gateway
2. Verify user mapping
3. Remove LDAP or rejoin LDAP
4. Reconfigure RFC2307

The array must be joined to Active Directory again after the cluster expansion. All other settings must be verified.

Stopping/Disabling/Removing File Persona

To stop or disable File Persona from running on a node pair by using the command line, issue the following command:

stopfs [<nodeid>,<nodeid>...]

where,
• <nodeid>

specifies the node on which to stop File Persona.

When File Persona running in compliance lock mode is stopped, a warning message with the following message will be displayed:
If all the nodes are stopped, CO requests will not be able to be processed until "startfs -enable" is executed to bring FS into running state.

On user confirmation, FS will be disabled.

To stop and remove File Persona from a node pair, issue the following command:

```
stopfs -remove <node>:<slot>:<port> <node>:<slot>:<port> [{<node>:<slot>:<port> <node>:<slot>:<port}>]...
```

where,

- `-remove` specifies File Persona will be stopped and removed from the specified nodes. If no nodes are specified, you will receive an error.
- `<node>:<slot>:<port>` specifies the nodes on which to stop and remove File Persona. The node pairs indicated must match the node pairs used when File Persona was enabled.

If File Persona in compliance mode is stopping and removed, the operations will be successful for all specified nodes except the last node. Error will be returned for the last node with the following message:

```
Could not remove FS on last node. ComplianceOfficerApproval is enabled. Disable this system parameter before removing the File Services.
```

Verify the changes with the `showfs` command. For more information about the `stopfs` and `showfs` commands, see the HPE 3PAR Command Line Interface Reference.

**NOTE:** File Persona cannot be removed from a node pair until all associated FPGs are assigned to a different node pair or removed. You can use the command to assign FPGs to a different node pair. You can use the `setfpg -primarynode` command to assign FPGs to a different node pair. To remove an FPG without permanently destroying the data associated with an FPG, you can execute the `removefpg` command with the `-forget` option. FPGs removed with the `-forget` option can subsequently be recovered with the `createfpg -recover` command. If File Persona is stopped and removed from all nodes, global configurations (as seen in the `showfs` subcommand) will be lost. Hewlett Packard Enterprise recommends making a note of all such configurations if you plan to re-enable the File Persona in the future.

File Persona related schedules could be still retained, even after removing File Persona, which may lead to failed scheduled tasks. To remove File Persona completely, delete all related scheduled tasks.

### Stopping or disabling FilePersona using the SSMC:

- From the main menu, select **File Persona > Persona Configuration**.
- On the list pane, select the system, and then select **Pause File Persona node** on the **Actions** menu.
- Follow the instructions in the dialog box that opens.

### Restarting File Persona

To restart File Persona on all node pairs or on a specified node pair where File Persona had been previously initialized and enabled, but subsequently stopped and disabled, issue the following command:

```
startfs -enable [<nodeid>[,<nodeid>]...]
```

where:

- `-enable`
specifies that previously stopped File Persona will be re-enabled on the specified nodes. If no nodes are specified, File Persona is restarted on all nodes on which File Persona had been previously enabled.

- `<nodeid>`

specifies the node ID number on which File Persona will start. Multiple node ID numbers may be listed in the execution of the command.

# Configuring File Persona Network Settings

Once File Persona has been enabled on a node pair, configure the network settings before using File Persona. The default values for some settings may be suitable for your configuration and may require no modification. The following settings are available for configuration:

- Bond mode for File Persona ports
- Maximum Transmission Unit (MTU) size
- File Persona node IP addressing
- Default gateway for File Persona
- Auxiliary static routes for File Persona or Virtual File Servers
- DNS server addresses and suffixes for File Persona

NTP is required for Active Directory and SMB Shares. Use the `setnet` command to setup NTP. See the HPE 3PAR Command Line Interface Reference.

The following sections include instructions for configuring these settings using the `setfs` command from the HPE 3PAR CLI and, where applicable, the HPE 3PAR StoreServ Management Console (SSMC).

## Setting the Bond Mode for File Persona Nodes

When installed the bond mode is set to 6 by default. For both 1 GbE and 10 GbE ports, the acceptable bond mode values are 1 and 6. Please take note of the fact that there is no bonding mode option available for the RCIP port.

### Setting Bond mode using HPE 3PAR CLI

To set the bond mode for all File Persona nodes from the command line, issue the following command:

```
setfs bond <bond_mode>
```

where,

- `<bond_mode>`

  indicates the bond mode used to aggregate File Persona ports on the HPE 3PAR StoreServ Storage system.

### Setting Bond mode using SSMC

- From the main menu, select File Persona > Persona Configuration.
- On the list pane, select the system, and then select Configure File Persona on the Actions menu.
- Select the Advanced options checkbox to display advanced configuration options.
- In the Network Settings section, specify the bond mode.

## Setting the Maximum Transmission Unit Size for File Persona Nodes

The size for the maximum transmission unit (MTU) can be altered.

### Setting the Maximum Transmission Unit (MTU) size using HPE 3PAR CLI

To set the Maximum Transmission Unit (MTU) size for all File Persona nodes on a StoreServ Storage system from the command line, issue the following command:

```
setfs mtu <mtu_size>
```

---

Configuring File Persona Network Settings 17
where,

- `<mtu_size>`

  specifies the maximum size (in bytes) for individual IP packets transferred through a File Persona port. If not specified, a port uses the default of 1,500 bytes. The valid range is 1500 – 9000 bytes.

### Setting the Maximum Transmission Unit (MTU) size using SSMC

- From the main menu, select **File Persona > Persona Configuration**.
- On the list pane, select the system, and then select **Configure File Persona** on the **Actions** menu.
- Select the **Advanced options** checkbox to display advanced configuration options.
- In the **Network Settings** section, specify an MTU size.
- Click **Configure**.

### Configuring Node IP Addressing for File Persona Nodes

The IPv4 addressing for a File Persona node can be configured.

#### Configuring IPv4 addressing using HPE 3PAR CLI

To configure IPv4 addressing for a File Persona node from the command line, issue the following command:

```
setfs nodeip -ipaddress <ipaddress> -subnet <subnet> -vlantag <vlanid> <nodeid>
```

where,

- `<ipaddress>`
  
  specifies the IPv4 address to be used for the File Persona node.

- `<subnet>`

  specifies the subnet mask to be used for the File Persona node.

- `<vlanid>`

  specifies the VLAN ID (tag) used for the File Server node IP address (FSIP).

- `<nodeid>`

  specifies the node ID number for a node in the File Persona node pair on the StoreServ Storage system.

#### Configuring IPv4 addressing using SSMC

- From the main menu, select **File Persona > Persona Configuration**.
- On the list pane, select the system, and then select **Configure File Persona** on the **Actions** menu.
- Select the **Advanced options** checkbox to display advanced configuration options. (The VLAN tag value is an advanced option)
- In the **Node Pairs** section, edit or specify an IP address for each node in the node pair by clicking the edit icon.
- In the **Network Settings** section, specify a subnet mask and, optionally, a VLAN tag value.
- Click **Configure**.

### Setting the Default Gateway Address for File Persona

The IPv4 address of the default gateway can be set for File Persona nodes.

#### Setting the IPv4 address of the default gateway using the HPE 3PAR CLI

To set the IPv4 address of the default gateway for File Persona, issue the following command:

```
setfs gw <ipaddress>
```

where,

- `<ipaddress>`
specifies the IPv4 address of the default gateway for File Persona on the LAN.

If static routes are being defined for VFS access, the default gateway can be defined as a static route. Refer to section Configuring Static Routes for File Persona on page 19 for configuring static routes. Please note that the default gateway is a special case of a static route. If the Virtual File Servers (VFS) are provisioned on different VLANs than the File Persona nodes, then the clients accessing the VFS must be either in the same subnet as the VFS in order to access its shares, or else appropriate static routes should be defined for these VLANs.

To delete a gateway IPv4 address (in order, for example, to configure File Persona nodes on a different subnet), issue the following command:

```
setfs gw -delete
```

Setting the IPv4 address of the default gateway using the SSMC

- From the main menu, select File Persona > Persona Configuration.
- On the list pane, select the system, and then select Configure File Persona on the Actions menu.
- In the Network Settings section, specify a gateway IP address.
- Click Configure.

Configuring Static Routes for File Persona

In order to configure a static route for File Persona from the command line, set the IPv4 address of the gateway for File Persona to use with a subnet or VLAN.

Creating a File Persona Static Route

To create a File Persona static route for a target subnet, issue the `createfsroute` CLI command:

```
createfsroute [-vlan <vlantag>] <targetaddr> <subnet>|<prefixlen> <gateway>
```

where,

- `<vlantag>` is the VLAN tag for the route (defaults to 0)
- `<targetaddr>` is the target subnet address address for which the gateway is to be assigned.
- `<subnet>|<prefixlen>` is the subnet mask or prefix length for the subnet address
- `<gateway>` is a new gateway to be assigned to the target subnet address

Only a single default route (target address of "0.0.0.0" and a subnet mask of "0.0.0.0" or prefix length of "0") can be configured per VLAN as required by the VFS definitions. Except for this, any given combination of target subnet and its subnet mask must be unique across all VLANs.

For any given route definition, the associated gateway address must be in the same VLAN and subnet as a local address on a file-serving node. That address can be the per-node IP address, or that of a VFS. Route definitions only become active if the associated gateway address has a corresponding local address on File Persona, in the same VLAN and subnet. As VFS addresses can be defined after setting up the route definitions, the `createfsroute` and `setfsroute` commands do not restrict the entry of route definitions with gateway addresses that do not yet have a corresponding local address.

When in doubt, check the health details using the `showfsroute -d` command. "Route is inactive" implies that there is no active local address that is enabling the use of that route definition.

Modifying the Gateway of the Route
The `setfsroute` command modifies the gateway of the route specified. The syntax for the command is as follows:

```
setfsroute modifygw [-f] {<targetaddr>,{<subnet>|<prefixlen>,<vlantag>|<routeidentifier>} <gateway>
```

where the options are as follows:

- `-f` suppresses confirmation from user before modifying the route
- `<targetaddr>` is the target subnet address for which the route is to be modified
- `<subnetmask>|<prefixlen>` is the subnet mask or prefix length for the subnet address
- `<vlantag>` is the vlan tag associated with route which needs to be modified
- `<routeidentifier>` is the route ID. Instead of providing a combination of `<targetaddr, subnetmask>|prefixlen, vlantag>` - a route identifier can be provided. Obtain the route identifier using the `showfsroute -d` command
- `<gateway>` is the new gateway that will be assigned to the target subnet address

### Displaying Routes

The `showfsroute` command displays all the routes including default and/or the routes created with the `createfsroute` command. The syntax for the `showfsroute` command is as follows:

```
showfsroute [-d] [-target <targetaddr>] [-vlan <vlantag>] [-gateway <gatewayaddr>]
```

where,

- `-d` displays the detailed information for each route
- `-target <targetaddr>` is the subnet address and lists all routes for this address
- `-vlan <vlantag>` takes an integer value and lists routes configured on this vlan
- `-gateway <gatewayaddr>` displays all routes using this gateway

### Removing Existing Route

Use the `removefsroute` command to remove an existing route for a target address. The syntax for the `removefsroute` command is as follows:

```
removefsroute [-f] {<targetaddr>,{<subnetmask>|<prefixlen>,<vlantag>|<routeidentifier>}
```

where,

- `-f` suppresses confirmation from user before removing the route
- `<targetaddr>` is the target subnet address for which the route is to be removed
• <subnet>|<prefixlen>
  is the subnet mask or prefix length for the subnet address
• <vlantag>
  is the vlan tag associated with route which needs to be removed
• <routeidentifier>
  is the route ID; instead of providing a combination of {targetaddr, subnet mask|prefixlen, vlantag} a route ID can be given. This value can be fetched from the showfsroute -d command.

Setting DNS Addresses and Domain Suffixes for File Persona

The Domain Name System (DNS) server address and suffixes needs to be specified.

Setting DNS address using HPE 3PAR CLI

To specify the Domain Name System (DNS) servers used by File Persona (and, optionally, domain search suffixes) from the command line, issue the following command:

```
setfs dns <ipaddress-list> [ <suffix-list> ]
```

where,

• <ipaddress-list>
  specifies the DNS addresses used by File Persona. For example,
  123.45.67.89,123.101.112.131
• <suffix-list>
  specifies the DNS suffixes used by File Persona. Any DNS search suffix can be used. If you are planning to join File Persona to Active Directory Domain Services (AD DS), use the same AD DS domain names here.

The suffix-list must include the name of the domain the StoreServ will join. The DNS provided must be able to resolve the domain name or the domain join will fail.

Setting DNS address using SSMC

• From the main menu, select File Persona > Persona Configuration.
• On the list pane, select the system, and then select Configure File Persona on the Actions menu.
• In the DNS Settings section, specify IP addresses for up to three DNS servers and up to three domain suffixes.
• Click Configure.

Reverting to an Earlier Version of HPE 3PAR OS with File Persona

Reverting to a version of the HPE 3PAR OS earlier than 3.2.2 that still supports File Persona (for example, 3.2.1 MU3) is possible. Reverting from 3.2.2 to an earlier version of the OS is not supported under the following circumstances:

• File Persona was enabled on the StoreServ Storage system after the OS was upgraded to version 3.2.2.
• FPGs were created using thinly deduplicated volumes.
• File Persona was expanded to use additional nodes after the OS was upgraded to version 3.2.2.
• Any 10 GbE NICs used for File Persona are configured with a bond mode setting of 6.
• Any non-default static routes are configured.
• Any virus scan engines of type Trend Micro are configured.

If the user mapping feature is enabled, revert to a File Persona version that does not support user mapping.
NOTE:
Revert is not supported for FPGs with On-Disk Version (ODV) higher than the revert version of HPE 3PAR OS with File Persona. Revert will fail for all FPGs that have had an ODV upgrade.
Authentication

Authentication in a multiprotocol environment happens when a supplied credential such as an account name and password is matched or validated to an account name and password stored in a name service. As part of this process, name resolution happens by performing a lookup for an account or group based on a property such as SID, user name or UID/GID. In a cross-protocol environment, there must be a mapping between the schemas using an identity mapping service to evaluate the access privilege of any file or directory accessed from any protocol.

Active Directory (AD)

Active Directory (AD) is a directory service primarily used in a Windows environment but can also be used in LINUX/UNIX environments. Active Directory performs name lookups and authentications for user accounts and groups. All user-name lookups are stored in an Active Directory name cache on the File Persona node. This cache is referenced or populated for every user-name request and will be cleared when File Persona is restarted. File Persona must be joined to a single Active Directory domain, so that all nodes running File Persona will be joined to the same Active Directory domain. All name resolutions and authentications for File Persona are limited to that Active Directory domain and all trusted domains.

Joining File Persona Nodes to an Active Directory Domain

To join File Persona nodes to an Active Directory domain, issue the following command:

```
setfs ad [-passwd <password>] <user> <domain>
```

where,

- `<password>` specifies the password of a user authorized to join the specified Active Directory domain. If a password is not specified as a parameter, you will be prompted for the password
- `<user>` specifies the name of a user authorized to join the specified Active Directory domain
- `<domain>` specifies the name of the Active Directory domain that File Persona is to join

The system clock of the HPE 3PAR StoreServ Storage system should be synchronized with that of your network and AD domain controller. If the system clocks are not synchronized, you may be unable to join the AD domain. Use the `setnet ntp <server_address>` command to configure the HPE 3PAR StoreServ Storage system to use the same NTP server as the Active Directory domain controller on your network.

**NOTE:**

File Persona can only join a single AD domain.

Joining an AD domain using the SSMC

- From the main menu, select **File Persona > Persona Configuration**.
- On the list pane, select a given system, and then select **Configure File Persona** on the **Actions** menu.
- In the **Authentication Settings** section, click **Active Directory Settings** to display the AD options.
- Specify an AD domain, a user name, and a password.
- Click **Configure**.

Removing File Persona Nodes from an Active Directory Domain

To remove File Persona from an AD domain, issue the following command:
To remove File Persona from a given AD domain using the SSMC:

- From the main menu, select **File Persona > Persona Configuration**.
- On the list pane, select a given system, and then select **Configure File Persona** on the **Actions** menu.
- In the **Authentication Settings** section, click **Active Directory Settings** to display the AD options.
- Clear any value specified in the **AD Domain** field.
- Click **Configure**.

### Configuring RFC2307 to use with Active Directory

#### Enabling or Disabling RFC2307 from HPE 3PAR CLI

To enable or disable RFC2307 for Active Directory services, issue the following command:

```
setfs rfc2307 [-f] {disable | enable}
```

#### Enabling or Disabling RFC2307 from SSMC

- From the main menu, select **File Persona > Persona Configuration**.
- On the list pane, select the system, and then select **Configure File Persona** on the **Actions** menu.
- Select the **Advanced options** checkbox to display advanced configuration options.
- In the **Authentication Settings** section, click **Identity Mapping Settings** to display the **UID/GID mapping** option.
- Toggle the option to enable or disable it and click **Configure**.

RFC2307 is a global setting, all users and groups requiring access to SMB shares must have User Identifiers (UIDs) and Group Identifiers (GIDs) defined in the AD if RFC2307 is enabled.

When the RFC2307 setting is disabled (default), File Persona automatically generates UIDs and GIDs for all Active Directory (AD) users and groups based on their Security Identifier (SID). When RFC2307 is enabled in File Persona, it will look up the UIDs and GIDs in Active Directory RFC2307 attributes that are configured as UNIX attributes of the AD user and groups.

If the RFC2307 setting in File Persona is enabled but the user does not have a configured UID or GID in the AD, the user is not granted write access even if the access is granted through an Access Control List (ACL).

In most scenarios, the RFC2307 setting should be set during the initial File Persona configuration. Changing the setting by enabling or disabling RFC2307 after the File Persona is in use, will affect user and group access to data. If changing the RFC2307 setting is required after files have been written to the system, an administrator needs to reassign permissions to the files to match the users' modified UID and GID values (can be retrieved using the `showfs -usermap` command).

When migrating from unprovisioned mode (non-RFC2307) to provisioned mode (RFC2307) chances are you might lose access to existing data. This is because the UNIX attributes get changed from the synthesized values to the ones manually configured in the Active Directory, that is if they are different.

If the user and group objects in the Active Directory are getting configured with UNIX attributes for the first time, the administrator can display the user/group object(s) with the `showfs -usermap` command with mapped option set to false and obtain the synthesized ID so it can be used in the Active Directory for UNIX attributes.

It is recommended that any open user sessions that are impacted by the identity change be disconnected prior to the change and reconnect after the change so that the new identity mapping can take effect. It is also recommended that the Administrator issues a `setfs auth clearcache` command after changing the RFC2307 setting to ensure any cached identity is properly cleared.
Active Directory (AD)

When creating a user in an Active Directory, there are two name fields. One is called "User logon name" and the other is called "User logon name (pre-Windows 2000)". To prevent confusion between users and groups, and to prevent any possible problems with names stored in ACLs, the following is recommended:

• Make sure that neither of the two name fields is the same as the name of any other user or group in the domain.
• Set both of the name fields to the same name when creating a user.

Local Users and Groups

Displaying Settings for Local Users and Groups

To display information for a given File Persona local user, issue the following command:

```
showfsuser [<username>]
```

where,

• `<username>` specifies the name of the user for which information is to be displayed.

If no `<username>` is specified, all File Persona users will be displayed.

To display information for a File Persona group, issue the following command:

```
showfsgroup [<groupname>]
```

where,

• `<groupname>` specifies the name of the group for which the information is to be displayed. If no `<groupname>` is specified, all File Persona groups will be displayed.

For more information about the `showfsuser` and `showfsgroup` commands, see the HPE 3PAR Command Line Interface Reference.

Displaying local File Persona users using SSMC

• From the main menu, select File Persona > Persona Configuration.
• On the list pane, select the system, and then select Configure local users on the Actions menu.
• In the Local users section, available local users are displayed.

Displaying File Persona groups using SSMC

• From the main menu, select File Persona > Persona Configuration.
• On the list pane, select the system, and then select Configure local groups on the Actions menu.
• In the Local groups section, available local groups are displayed.

Creating Local Users

To create a File Persona local user, issue the following command:

```
createfsuser [-passwd <password>] [-primarygroup <groupname>] [-enable {true | false}] [-uid <userid>] [-grplist <grouplist>] <username>
```

where,

• `-passwd <password>`
specifies the password to allow the user to access File Shares in a File Store. If a password is not supplied when the command is executed, you will be prompted to enter one.

- **-primarygroup <groupname>**

  specifies the name of the local group to which the user will belong.

- **-enable {true | false}**

  specifies whether access is enabled or disabled after the user is created. If you specify a value of false, the user is disabled after being created and will not be able to access File Shares. If not specified, the default is enabled (true).

- **-uid <userid>**

  specifies the user ID. If no value for <userid> is specified, -uid will be given a default value. The -uid option can accept any value between 1000 and 65533.

- **-grplist <grouplist>**

  specifies a list of local groups of which the user will be a member. Use commas to separate the group names.

- **<username>**

  specifies the name of the user to be created. A user name may be up to 20 characters in length. Valid characters are alphanumeric characters, periods, dashes (except as the first character), and underscores. File Persona supports valid UTF-8 characters for usernames. Also, please note that the ^ special character cannot be used for SMB File Share user names as it is a reserved character for File Persona. The ! special character can be used in SMB File Share user names but the resulting name must be enclosed in single quotes, for example, 'abc!123'.

**NOTE:** Using BUILTIN groups as the primary group for local users is not supported.

Verify changes with the showfsuser command. For more information about the createfsuser and showfsuser commands, see the HPE 3PAR Command Line Interface Reference.

**Adding a File Persona user using SSMC**

- From the main menu, select File Persona > Persona Configuration.
- On the list pane, select the storage system, and then select Configure local users on the Actions menu.
- Below the list of any current local users, click Add.
- In the Add Local User dialog box, specify a user name, a password, a group to which the new user will belong, and whether the user will be enabled or disabled.
- Click Add and then click Configure.

**Removing Local Users**

Removing a user who is still referenced in file/folder permissions, share permissions, or quotas may create additional complexity in managing those objects. Disabling users with the setfsuser command is often preferred to avoid these concerns.

To remove a File Persona local user, issue the following command:

```
removefsuser <username | uid>
```

where,

- `<username | uid>`

  specifies either the name or the UID of the user to be removed.

Verify changes with the showfsuser command. For more information about the removefsuser command, see the HPE 3PAR Command Line Interface Reference.

**Removing a File Persona local user or users using SSMC**
• From the main menu, select **File Persona > Persona Configuration**.
• On the list pane, select the relevant storage system, and then select **Configure local users** on the **Actions** menu.
• Click the delete icon, select the users to be removed in the dialog box and click **Remove**.
• Click **Configure**.

**Modifying Settings for Local Users**

To modify the settings of a File Persona local user, such as the password of a user or the user's group membership, issue the following command:

```
setfsuser [-passwd <password>] [-passprompt] [-primarygroup <groupname>] [-enable {true | false}] [-grplist [+|-] <grouplist>] <username>
```

where,

- **-passwd <password>**
  specifies the password to allow the user to access File Shares in a File Store.
- **-passprompt**
  prompts for a new password.
- **-primarygroup <groupname>**
  specifies the name of the primary group to which the user belongs.
- **-enable {true | false}**
  specifies whether access is enabled or disabled for the user. If you specify a value of `false`, the user is disabled and will not be able to access File Shares. If not specified, the default is enabled (`true`).
- **-grplist [+|-] <grouplist>**
  specifies a list of groups of which the user is a member. Use commas to separate group names.

  - If specified, the prefix (+ or -) is applied to the entire `<grouplist>`. If the value for `<grouplist>` is specified without a prefix, `<grouplist>` will replace the user's current list of groups.
  - If `<grouplist>` has a + prefix, for example `+group_1`, the `<grouplist>` is added to the existing list of a user's group names. The group names specified in `<grouplist>` must not be in the existing list of the user's group names.
  - If `<grouplist>` has a - prefix, the `<grouplist>` is removed from the existing list of user's group names. The group names specified in `<grouplist>` must exist in the user's current group names.

- **<username>**
  specifies the name of the user to be modified.

Verify changes with the `showfsuser` command. For more information about the `setfsuser` command, see the **HPE 3PAR Command Line Interface Reference**.

**Modifying settings for a File Persona user using SSMC**

- From the main menu, select **File Persona > Persona Configuration**.
- On the list pane, select the storage system, and then select **Configure local users** on the **Actions** menu.
- In the list of current local users, click the edit icon.
- In the dialog box that appears, specify a different password for the user or a different primary group or disable or enable the user and click **OK**.
- Click **Configure**.

**Creating Local Groups**

To create a File Persona local group, issue the following command:

```
createfsgroup [-gid <number>] [-memberlist <list>] <groupname>
```
where,

- `<number>`
  specifies the ID number to be used for the group ID. This value can be any number between 1000 and 65533.
- `<list>`
  specifies the names of the users in the group, as a comma-separated list.
- `<groupname>`
  specifies the name of the group to be created. The group name may be up to 20 characters in length. Valid characters are alphanumeric characters, periods, dashes (except for the first character), and underscores. File Persona supports valid UTF-8 characters for groupnames. Please note that the `^` special character cannot be used in SMB File Share group names as it is a reserved File Persona character. The `!` special character can be used in File Share group names but must be used in single quotes, for example 'abc!123'.

Verify changes with the `showfsgroup` command. For more information about the `createfsgroup` and `showfsgroup` commands, see the `HPE 3PAR Command Line Interface Reference`.

Creating a File Persona group using SSMC

- From the main menu, select `File Persona > Persona Configuration`.
- On the list pane, select the storage system, and then select `Configure local groups` on the Actions menu.
- Below the list of any current local groups on the system, click `Add`.
- Specify a group name.
- Optionally, select the Advanced options checkbox to display a field for specifying a GID for the new group.
- Specify members to be included in the new group, if necessary.
- Click `Add` and then click `Configure`.

Removing Local Groups

All references to groups for file/folder permissions, share permissions or quotas should be removed before the group is removed. It is recommended that all users within a group are removed with the `setfsgroup` command.

To remove a File Persona local group, issue the following command:

`removefsgroup <groupname>`

where,

- `<groupname>`
  specifies the name of the group to be removed.

Verify changes with the `showfsgroup` command. For more information about the `removefsgroup` command, see the `HPE 3PAR Command Line Interface Reference`.

Removing File Persona local groups using SSMC

- From the main menu, select `File Persona > Persona Configuration`.
- On the list pane, select the storage system, and then select `Configure local groups` on the Actions menu.
- In the list of current local groups, click the delete icon, select the groups to be removed in the dialog box and click `Remove`.
- Click `Configure`.
Modifying Membership of Local Groups

To modify the list of members of a File Persona local group, issue the following command:

```
setfsgroup [-memberlist [+|-] <list>] <groupname>
```

where,

- **-memberlist [+|-] <list>**
  
  specifies the members of the group. Use commas to separate user names in the `<list>` specification.
  
  ◦ If specified, the prefix (+ or -) is applied to the entire member list. If the member list has no prefix, the `<list>` specification will replace the current members of the group.
  
  ◦ If the member list has a `+` prefix, for example `+username_1`, the user name is added to the existing list of user names. The user names specified in the member list must not be in the existing list of user names.
  
  ◦ If the member list has a `-` prefix, the user names are removed from the existing list of user names. The user names specified in the member list must exist the list of user names of the group.

- **<groupname>**

  specifies the name of the group to be modified.

Verify changes with the `showfsgroup` command. For more information about the `setfsgroup` command, see the HPE 3PAR Command Line Interface Reference.

Adding members to a File Persona local group using SSMC

- From the main menu, select **File Persona > Persona Configuration**.
- On the list pane, select the relevant storage system, and then select **Configure local groups** on the **Actions** menu.
- In the list of current local groups, click the edit icon.
- In the dialog box that appears, expand the **Members** section.
- Click **Add**.
- Specify the name of a local user, an LDAP user, an LDAP group, an Active Directory user, or an Active Directory group in the **Name** field.
- Click **Add** to add the member to the group. (Or click **Add +** to add the member to the group and to clear the **Name** field for the specification of another member.)
- Click **OK** and then click **Configure**.

Removing members from a File Persona local group using SSMC

- From the main menu, select **File Persona > Persona Configuration**.
- On the list pane, select the storage system, and then select **Configure local groups** on the **Actions** menu.
- In the list of current local groups, click the edit icon.
- In the dialog box that appears, expand the **Members** section.
- Below the list of current members of the group, click **Remove**.
- Select the names of users to remove from the group and click **Remove**. Note that only the users that can be removed from the group will be listed.
- Click **OK** and then click **Configure**.

**NOTE:**

Local users for whom the specified group serves as the primary group cannot be removed from the specified group.
Lightweight Directory Access Protocol (LDAP)

Lightweight Directory Access Protocol (LDAP) is most commonly used in Linux/UNIX environments, where users connect to file shares on File Persona using the NFS protocol. LDAP authentication can be used in a multiprotocol or cross-protocol environment. When SMB clients (most likely Windows clients) are present, an AD domain will probably be available, making AD the preferred choice for authentication. When NFS, FTP or Object Access API are the primary protocols, there might not be an AD domain available to integrate. In this case, LDAP services would be a viable alternative for authentication.

Configuring LDAP Servers

The LDAP configuration for the HPE 3PAR array and the LDAP configuration for File Persona are different. The `setfs ldap` command is used to configure LDAP authentication for mostly for UNIX users connecting to file shares on File Persona. The LDAP configuration set with the `setauthparam` command is used for authenticating management interface administrators for the HPE 3PAR array. Before LDAP can be used to authenticate users and groups it must be added to the authentication provider stacking order in File Persona configuration.

**Configuring LDAP servers using HPE 3PAR CLI**

To ensure that File Persona communicates with an LDAP server, issue the following command:

```
setfs ldap [-passwd <binddnpwd>] [-schema <schema>] [{-usetls | -usessl} {-certfile <file_name> | -certdata <data>} -certcn <certcn>] <server> <binddn> <searchbase> <netbios>
```

where,

- **-passwd <binddnpwd>**
  
  specifies the password associated with the Bind Distinguished Name (DN) supplied by the `<binddn>` option. When File Persona needs to read LDAP data, it uses the `<binddn>` with the `<binddnpwd>` to authenticate. If you do not specify the password with this command, you will be prompted for the password.

- **-schema <schema>**
  
  specifies the name of the schema used to create user and group accounts on the LDAP server. Valid options are `posix` and `samba`; the default is `posix`. The schema provides an interface for software compatibility across various operating systems.

- **-usetls/-usessl**
  
  specifies the type of secure connection between File Persona and the LDAP server. Use `-usetls` to specify a TLS connection. The `-usessl` option (not recommended) specifies an SSL connection. If neither of these options are specified, the connection between File Persona nodes and the LDAP server is not encrypted, and the certificate specified by the `-certfile` option or the `-certdata` option is ignored.

- `{ -certfile <file_name> | -certdata <data> }`
  
  specifies how to establish encrypted connections between File Persona and the LDAP server. Use the `-certfile` option to specify a certificate file name. Use the `-certdata` option to specify the certificate attributes. When either the `-usetls` option or the `-usessl` option is used, you must specify how to establish encrypted connections with `-certfile` or `-certdata`.

- **-certcn <certcn>**
  
  specifies the Common Name (CN) used when the certificate is generated. The CN must be the fully qualified hostname of the LDAP server. When either the `-usetls` option or the `-usessl` option is used, you must specify this option.

- **<server>**
specifies the fully qualified hostname or IPv4 address of the LDAP server you want to configure. If the port used for the LDAP server is not 389 or 636, the port number must be specified with the server in the format `<server>:<port>`.

- `<binddn>`
  binds File Persona to the LDAP server, allowing File Persona to read data from the LDAP server (such as user or group accounts configured in LDAP). This account must have privileges to read the subtree specified by the value supplied for the `<searchbase>` option. Write permissions are not required.

- `<searchbase>`
  specifies the DN of the search base object that defines where to begin the search for user and group accounts.

- `<netbios>`
  specifies the name of the LDAP Domain. It can be up to 15 alphanumeric characters with no spaces. The name must be unique on the network. To access an SMB share, specify `<netbios>\<ldap username>` as the username.

**Configuring LDAP servers using SSMC**

- From the main menu, select **File Persona > Persona Configuration**.
- On the list pane, select the system, and then select **Configure File Persona** on the **Actions** menu.
- Select the **Advanced options** checkbox to display advanced configuration options.
- In the **Authentication Settings** section, click **LDAP Configuration Settings** to display options for LDAP configuration.
- Specify the appropriate settings for your LDAP configuration, including an LDAP server host name, a Bind DN, a NetBIOS name, and any other necessary settings.
- Click **Configure certificate** if you are using secure communications (SSL or TLS) in connections with the LDAP server.
- Click **Configure**.

**Removing LDAP Servers**

To remove the LDAP configuration from File Persona, issue the following command:

```bash
setfs ldap -delete [-f]
```

To remove the LDAP configuration from File Persona using the SSMC:

- From the main menu, select **File Persona > Persona Configuration**.
- On the list pane, select the system, and then select **Delete LDAP configuration** on the **Actions** menu.
- Click **Delete**.

**NOTE:**

If you are not using LDAP to authenticate users and groups, LDAP should be removed from the authentication provider stacking order.

**Configuring the Authentication Provider Stacking Order**

The order in which user and group name authentication providers process requests should be customized for your environment. The most commonly used authentication provider services should be first in the stacking order to optimize the name lookups. When the first authentication provider in the order cannot authenticate a name, a search is performed by the next authentication provider in the stacking order. A complete search is performed by each provider in the stacking order until the user is authenticated, passed to the next provider for authentication, or denied access.
There are three valid authentication service providers:

- Active Directory
- Local
- LDAP

The providers can be listed in any order. The default stacking order is:

1. Active Directory
2. Local

The Active Directory and LDAP authentication providers are optional and should be removed from the stack if they are not used in your network. The local provider must always appear somewhere in the stack order because BUILTIN names are resolved by the local provider. If the user authentication environment allows duplicate names, the preferred authentication provider should be first in the stacking order. Allowing duplicate names is not recommended because it increases search times.

**Configuring the authentication provider stacking order using HPE 3PAR CLI**

To specify the user and group name authentication provider stacking order, issue the following command:

```
setfs auth <provider>
```

where,

- `<provider>` is a list of authentication providers separated by spaces. The list must include the `Local` provider. For example: `ActiveDirectory Ldap Local`. Any providers not being used should be removed from the stacking order. To remove a provider issue the `setfs auth <provider>` command and omit the provider name from the list. The valid provider values are: `ActiveDirectory`, `Ldap`, and `Local`.

To display the user and group name authentication provider stacking order, issue the `showfs auth` command.

**User Mapping**

User mapping plays an important role for shared data access in a cross-protocol environment, where Windows users and Linux/UNIX users need to be mapped. SMB clients may need access to files which have POSIX permissions with UNIX identity (UID/GID) and NFS clients may need access to files which have NTFS ACLs with Windows identity (SID). User mapping is an essential requirement for customers accessing same file shares from multiple protocols at the same time.

The User mapping feature maps an incoming user (from an authentication provider) to a different user (from the same or different authentication provider) to generate a security profile. The security profile contains UNIX IDs (UID, GID) and/or SIDs. These IDs are used to authorize the user's access rights to the file system objects/shares.

File Persona supports four access protocols (SMB, NFS, FTP and Object Access API). The SMB protocol uses SIDs to represent the user’s identity; whereas POSIX access protocols such as NFS, FTP and Object Access API use UIDs and GIDs. To support cross-protocol access, File Persona needs to identify a user with both SID and UID/GID as a valid identity, consistent with the corresponding clients. Typically, SMB clients use Active Directory (AD) as the authentication provider. AD always stores the SID as the identity unless it is configured to store UNIX attributes too (such as RFC2307 mode). Typically, POSIX clients use LDAP as their authentication provider; LDAP normally stores UID/GID as the identity under POSIX schema unless it's configured with a SAMBA schema.

User mapping comprises of a set of rules to map a “From” user to a “To” user. These rules enable unidirectional replacement style mapping, bidirectional static mapping, join rule and dynamic mapping with the use of wild cards.

Based on the mapping operator the incoming user identity can either be joined or replaced with the "To" user name’s identity.
File Persona supports unidirectional replace rule for static mapping where the "From" user name's identity is replaced completely with the configured "To" user name's identity. A bidirectional join/merge rule can be used for static and dynamic mapping that would enable the use of both the "From" user name's identity (SID for Active Directory or UID/GID for LDAP) and the "To" user name's identity (SID for active directory or UID/GID for LDAP). Therefore, if the "From" user name is an AD user, its SID can be used to access an SMB share and the mapped "To" user name's UID/GID's can be used to access NFS shares for the same folders.

### User Identification

File persona supports authentication providers such as Active Directory (AD) and LDAP that provide name services to resolve identity. Both AD and LDAP support different configuration modes to perform name service resolution for cross-protocol access and File Persona behaves accordingly to each specific mode of each Name Service authentication.

**Active Directory configuration modes:**

- **Unprovisioned Mode**
  
  The Local Security Authority Subsystem Service (LSASS) in File Persona doesn’t expect to find UID/GID attributes in Active Directory entries. If they exist, they are ignored and LSASS synthesizes UIDs and GIDs, based on the Active Directory SID. Permissions are set and evaluated based on the synthesized values.

- **Provisioned Mode (RFC2307)**
  
  LSASS in File Persona looks up and uses UID and GID attributes in Active Directory entries. No synthesizing of UIDs or GIDs is performed on File Persona if they are not found in the Active Directory. The SMB protocol permits read-only connections to shares if the IDs are missing. NFSv4 connections with missing IDs are not permitted.

**LDAP schemas:**

- **POSIX Schema**
  
  User and group objects in LDAP don’t include an SID attribute. LSASS in File Persona synthesizes the SIDs.

- **Samba Schema**
  
  User and group objects are expected to have an SID attribute. If they don’t, one is synthesized from the corresponding UID or GID. The SID is not assigned in the LDAP user or group entry.

**User Mapping Rules**

To ensure a coherent cross-protocol access each protocol’s client and server should resolve names to the same IDs. File Persona adds a name mapping capability with various Join and Replace rules to map an AD user to an LDAP user. It provides an account with all the necessary ID and SID attributes to provide expected access across SMB and POSIX protocols.

File Persona supports rules based on user mapping imported from a file. Maximum number of rules supported will be 1024. The mapping configuration file cannot be larger than 1 MB. Since authentication providers configuration is a global setting for all the nodes running File Persona in an HPE 3PAR array, the user mapping configuration also applies globally for that array.

**NOTE:**

The user mapping configuration is not included in the Config Backup and Restore operations. Prior to restoring the configuration to a new array, along with the authentication configuration, the administrator must also re-import the user mapping configuration and only then should the administrator enable user mapping.
To better support cross-protocol access, File Persona supports an enumeration capability so that synthesized IDs for AD in unprovisioned mode or LDAP in POSIX schema can be exported to a file to help setup an authentication provider for clients that are using the same IDs or have migrated to AD with RFC2307 using synthesized IDs as the real IDs. The enumeration process is a resource-intensive process as it needs to enumerate all the entries from the provider over the network. For better performance, only a single enumeration request will be active at any time. Any other enumeration request while one is active will be denied. Enumeration is a two-step process as it could run for a long duration depending on the number of entries in the provider.

To export an enumeration, the administrator must first issue a `setfs usermap` command to initiate the enumeration process. Once the enumeration process is complete, it can be exported with a `showfs usermap` command within 24 hours of enumeration. The enumeration process can be scheduled using the CLI to run at off-peak time to reduce performance impact.

**Rules and Operators for User Mapping**

A valid rule contains a “From” user followed by an operator, followed by the “To” user. A mapping file may contain comments denoted by “#” or “;” as the first character of the line. Rules are evaluated in the order in which they appear in the mapping file until there is a match. The mapping operation can be configured to decide how to process the incoming user’s identity (“From” name) to a mapped user (“To” name). Based on the mapping operator the incoming “From” user identity can either be joined or replaced to/with the “To” name’s identity. Once a rule is matched the user mapping processing stops.

If there is no match for a given user name, a synthesized ID is assigned. Data created with this ID needs to be migrated when the user mapping is created. The following is a list of possible scenarios showcasing how the mapping will be created:

- By identifying the synthesized ID with the `showfs usermap` command
- By identifying the synthesized ID with the `-mapped false` option
- By changing the ownership of the data to the mapped id
- By assigning the synthesized ID to the mapped user

The typical placement of rules in a mapping file is as follows:

- **Static Mapping**
  
  Static Mapping is configured when mapping is desired in a specific way. It could be either a unidirectional `Replace` or a bidirectional `Join`, depending on the deployment scenario. This would override subsequent dynamic or default mapping rules.

- **Dynamic Mapping**
  
  Dynamic mapping rules map users and groups with the same name across providers.

The user mapping feature in File Persona supports the following rules:
<table>
<thead>
<tr>
<th>Operator</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>=&gt;</td>
<td>Unidirectional Replace rule for static mapping.</td>
<td>Once the “From” user is authenticated, this operator Replaces the “From” user identity with the “To” user identity.</td>
</tr>
<tr>
<td>==</td>
<td>Bidirectional Join rule for static and dynamic mapping.</td>
<td>The operator performs a Join on the native IDs of the “From” user and the “To” user in both directions. If an AD user logs in, the user’s identity includes the SID for the AD user and maps to UID/GID of the LDAP user and vice versa. If an LDAP user logs in, the user’s identity includes UID/GID of the LDAP user and SID of the mapped AD user. By using a wildcard for both “From” and “To”, instead of a specific name this rule can be used for dynamic mapping. For example, * == * would result in any user from a provider to be mapped to another user with the same name from another provider.</td>
</tr>
</tbody>
</table>

**Group Mapping**

Bidirectional rules require primary group mapping rules. If the group names between both the providers are the same across the providers and if the mapping file has a dynamic rule, the dynamic mapping rule also applies to groups. However, if the group names are not the same across the providers, then there has to be a specific mapping rule for the desired group names. For bidirectional mapping to work, the primary group has to be mapped either through a specific static rule or through a dynamic rule. Two or more mapped users with the same AD primary group name cannot have different LDAP primary group names. This would cause incorrect mapping which is not permitted in bidirectional mapping.

The primary purpose of the group mapping rule is to map a primary group id of one provider to another. File Persona does not support mapping of group membership. Group mapping rules are mainly required to support mapping of primary group’s identity. A group mapping rule will not have members of one group to have the same access privileges as the mapped group’s members unless the members themselves can be mapped. This also means quota accounting for groups will not account for the members of the mapped group unless there is an explicit mapping for the member.

The following example shows when to use dynamic mapping rules instead of static mapping rules:

```plaintext
DOM\user1 == LDAP\user1
DOM\user2 == LDAP\user2
DOM\priGroupUsers1-5 == LDAP\priGroupUsers1-5
```

In this example, there is a static mapping between user 1 and user 2. This requires a mapping of the primary groups for user 1 and user 2. The user names and group names are the same, so the following dynamic mapping rule can be used in place of the three static mapping rules:

* == *

**User Mapping and User Quota**

Quotas for user/groups have to be cleared before performing user mapping for those user/groups, otherwise only newly mapped users will be shown and file system will not track quotas for older user ids.

User quotas are always parsed using a UID number and name resolution is used when entering or listing quotas. If a UID for a user name is changed (i.e. by changing the UID in an authentication provider or by changing UIDs by mapping to a different user or by enabling RFC2307), then quota reporting may be incorrect. The administrator should reapply the permissions on affected files/directories for correct quota calculations or update the quota entry.
Displaying User Mapping for File Persona Nodes

To display the user mapping information for File Persona nodes, issue the following command:

```
showfs [-usermap]
```

where,

- `-usermap`
  
  displays the user mapping, mapped user/group profiles or copies the exported users/group entries or mapping configuration to the client storage.

See the following list for the subcommand options.

- `-usermap [-d] {–username <username> | –groupname <groupname> | –userid <uid|sid> | –groupid <gid|sid>} [-mapped <true|false>]`
- `-usermap -exportconf -file <client_filepath>`
- `-usermap -export {users|groups} -provider <provider> -file <client_filepath>`

The options are explained below:

- `-username <username>`
  
  Displays the mapped information for the specified username.

- `-groupname <groupname>`
  
  Displays the mapped information for the specified groupname.

- `-userid <uid|sid>`
  
  Displays the mapped information for the specified user gid/sid.

- `-groupid <gid|sid>`
  
  Displays the mapped information for the specified group gid/sid.

- `-mapped <true|false>`
  
  Specifies whether mapped user details are to be displayed or its own details are to be displayed. By default, the mapped user details will be displayed. This option can only be used with options `-username` and `-userid`.

- `-exportconf`

  Exports and copies the mapping configuration to the client storage. If this option is specified `-file` must also be specified.

- `-export {users|groups}`

  Specifies the type of exported entries to be copied to the client storage. If this option is specified then options `-provider` and `-file <filepath_on_client>` must also be specified.

- `-provider <provider>`

  Specifies the type of authentication provider to be used to copy the exported entries. The `<provider>` must be either “Local”, “LDAP” or “ActiveDirectory”. This option can be used with only `-export`.

- `-file <filepath_on_client>`

  Specifies the file path on client storage to which the mapping configuration or exported users/groups to be copied. This option can be used with options `export` and `-exportconf`.

Following are some examples showing the various options defined above:
**showfs -usormap**

<table>
<thead>
<tr>
<th>Mapping Enabled</th>
<th>true</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>OK</td>
</tr>
<tr>
<td>Health Description</td>
<td>Component is healthy.</td>
</tr>
<tr>
<td>Corrective Action</td>
<td>--</td>
</tr>
</tbody>
</table>

**showfs -usormap -username trk1@2008ad**

----------Mapping----------

<table>
<thead>
<tr>
<th>From</th>
<th>Type</th>
<th>To</th>
</tr>
</thead>
<tbody>
<tr>
<td>2008AD\trk1</td>
<td>=&gt;</td>
<td>2008ad\trk2</td>
</tr>
</tbody>
</table>

**showfs -usormap -userid 1176528713 –d –mapped true**

<table>
<thead>
<tr>
<th>SID</th>
<th>S-1-5-21-2943099029-2375420575-3763763779-550730</th>
</tr>
</thead>
<tbody>
<tr>
<td>UID</td>
<td>1176528714</td>
</tr>
<tr>
<td>GID</td>
<td>1175978497</td>
</tr>
<tr>
<td>UPN</td>
<td><a href="mailto:trk2@2008AD.LAB">trk2@2008AD.LAB</a></td>
</tr>
<tr>
<td>NetBIOS Name</td>
<td>2008AD</td>
</tr>
<tr>
<td>SAM Account Name</td>
<td>trk2</td>
</tr>
<tr>
<td>Domain</td>
<td>CN=trk2,DC=2008ad,DC=lab</td>
</tr>
<tr>
<td>Primary Group Name</td>
<td>2008AD\domain\users</td>
</tr>
<tr>
<td>Alias Name</td>
<td>--</td>
</tr>
<tr>
<td>Map Found</td>
<td>true</td>
</tr>
<tr>
<td>Primary Group SID</td>
<td>S-1-5-21-2943099029-2375420575-3763763779-513</td>
</tr>
<tr>
<td>Additional Info</td>
<td>trk2</td>
</tr>
<tr>
<td>Password Expired</td>
<td>false</td>
</tr>
<tr>
<td>Password Never Expires</td>
<td>true</td>
</tr>
<tr>
<td>Prompt Password Change</td>
<td>false</td>
</tr>
<tr>
<td>User Can Change Password</td>
<td>true</td>
</tr>
<tr>
<td>Account Disabled</td>
<td>false</td>
</tr>
<tr>
<td>Account Expired</td>
<td>false</td>
</tr>
<tr>
<td>Account Locked</td>
<td>false</td>
</tr>
<tr>
<td>Mapping From</td>
<td>2008AD\trk1</td>
</tr>
<tr>
<td>Mapping To</td>
<td>2008ad\trk2</td>
</tr>
<tr>
<td>Mapping Type</td>
<td>=&gt;</td>
</tr>
</tbody>
</table>
showfs -usermap -userid -d S-1-5-21-2943099029-2375420575-3763763779-550730
SID : S-1-5-21-2943099029-2375420575-3763763779-550730
UID : 1176528714
GID : 1175978497
UPN : trk2@2008AD.LAB
NetBIOS Name : 2008AD
SAM Account Name : trk2
Domain : CN=trk2,DC=2008ad,DC=lab
Primary Group Name : 2008AD\domain\users
Alias Name : --
Map Found : true
Primary Group SID : S-1-5-21-2943099029-2375420575-3763763779-513
Additional Info : trk2
Password Expired : false
Password Never Expires : true
Prompt Password Change : false
User Can Change Password : true
Account Disabled : false
Account Expired : false
Account Locked : false
Mapping From : 2008AD\trk1
Mapping To : 2008ad\trk2
Mapping Type : =>

showfs -usermap -groupname trk1_group@2008ad
----------------Mapping----------------
From              Type To
2008AD\trk1_group =>   2008ad\trk2_group
Displaying detailed mapped information for the specified group id:
showfs -usermap -groupid 1176528715 -d
GID              : 1176528716
SID              : S-1-5-21-2943099029-2375420575-3763763779-550732
NetBIOS Name     : 2008AD
UNIX Name        : 2008AD\trk2_group
SAM Account Name : trk2_group
Domain           : CN=trk2_group,DC=2008ad,DC=lab
Alias Name       : --
Map Found        : true
Mapping From     : 2008AD\trk1_group
Mapping To       : 2008ad\trk2_group
Mapping Type     : =>

showfs -usermap -groupid 1176528715 -d
GID              : 1176528716
SID              : S-1-5-21-2943099029-2375420575-3763763779-550732
NetBIOS Name     : 2008AD
UNIX Name        : 2008AD\trk2_group
SAM Account Name : trk2_group
Domain           : CN=trk2_group,DC=2008ad,DC=lab
Alias Name       : --
Map Found        : true
Mapping From     : 2008AD\trk1_group
Mapping To       : 2008ad\trk2_group
Mapping Type     : =>
showfs -usermap -d -groupid S-1-5-21-2943099029-2375420575-3763763779-550732
GID              : 1176528716
SID              : S-1-5-21-2943099029-2375420575-3763763779-550732
NetBIOS Name     : 2008AD
UNIX Name        : 2008AD\trk2_group
SAM Account Name : trk2_group
Domain           : CN=trk2_group,DC=2008ad,DC=lab
Alias Name       : --
Map Found        : true
Mapping From     : 2008AD\trk1_group
Mapping To       : 2008ad\trk2_group
Mapping Type     : =>

Configuring User Mapping for File Persona

To enable and disable user mapping, issue the following command:

```
setfs usermap [-f] -enable {true|false}
```

where,

- **-enable {true|false}**
  
  Enables or disables the user mapping. Default is disabled. This option cannot be used with any other options except `-f`.
- **-f**
  
  Suppresses the warning message. If this option is not used, the command may require a confirmation before proceeding with its operation.

The following example showcases how to enable user mapping:

```
setfs usermap -enable true
WARNING: This operation may momentarily cause I/O errors for SMB clients.
Do you wish to continue ?
select y=yes n=no:
```

The following example showcases how to disable user mapping:

```
setfs usermap -f -enable false
```

The **enable** option restarts the SMB registry server and may disrupt other services that are using the registry. A warning message will be displayed to the user asking for confirmation, as shown below.

```
“WARNING: This operation may momentarily cause I/O errors for SMB clients.
Do you wish to continue ?
select y=yes n=no:”
Note: Selecting “n” will stop the execution of the command.
```

Displaying Mapped User/Group Entries

The **showfs -usermap** command displays the mapped user/group entries using options: username, grouppname, userid or groupid. If no option is specified it will display the status of mapping configuration. The command can be executed with various options. The syntax for each command style is as follows:

```
showfs -usermap
```
showfs -usermap [-d] | -username <username> | -groupname <groupname> | -userid <uid|sid> | -groupid <gid|sid>}

showfs -usermap -exportconf -file <client_filepath>

showfs -usermap -export {users|groups} -provider <provider> -file <client_filepath>

The following list displays the options used in the subcommand:

- **-username <username>**
  Displays the mapped information for the specified username.
- **-userid <uid|sid>**
  Displays the mapped information for the specified user UID/SID.
- **-groupname <groupname>**
  Displays the mapped information for the specified groupname.
- **-groupid <gid|sid>**
  Displays the mapped information for the specified group GID/SID
- **-d**
  Displays the detailed information of mapped users/groups.
- **-exportconf**
  Exports and copies the mapping configuration to the client storage. If this option is specified -file option must also be specified
- **-export {users|groups}**
  Specifies the type of exported entries to be copied to the client storage. If this option is specified -provider and -file <filepath_on_client> must also be specified. See setfs usermap for the command to create the exports.
- **-provider <provider>**
  Specifies the type of <provider> to be used to copy the exported entries. The <provider> must be a Local, LDAP or Active Directory. This option can be used with -export.
- **-file <filepath_on_client>**
  Specifies the file path on client storage to which the mapping configuration or exported users/groups to be copied. This option can be used with only -export and -exportconf.

**NOTE:**

File persona does not support mapping of group membership. Group mapping rules are mainly required to support mapping of primary group’s identity. A group mapping rule will not have members of one group to have the same access privileges as the mapped group’s members unless the members themselves can be mapped. This also means quota accounting for groups will not account for the members of the mapped group unless there is an explicit mapping for the member.

Following is an example showcasing how to display user mapping configuration:

```
showfs -usermap
Mapping Enabled : True
Health State : OK
Health Description : Component is healthy.
Corrective Action : --
```

Following is an example showcasing how to display mapped information for a specified user name:
showfs -usermap -username user1@2008AD.LAB
SID : S-1-5-21-964874337-1665363193-2846560699-501
UID : 10501
GID : 10546
UPN : user1@2008AD.LAB
NetBIOS Name : 2008AD
SAM Account Name : group1
Domain : CN=Domain Users,CN=Users,DC=2008ad,DC=1a

Following is an example showcasing how to display mapped information for a specified user sid:

showfs -usermap -userid S-1-5-21-964874337-1665363193-2846560699-501
SID : S-1-5-21-964874337-1665363193-2846560699-501
UID : 10501
GID : 10546
UPN : user1@2008AD.LAB
NetBIOS Name : 2008AD

Following is an example showcasing how to display detailed mapped information for a specified user id:

showfs -usermap -userid 10501 -d
SID : S-1-5-21-964874337-1665363193-2846560699-501
UID : 10501
GID : 10546
UPN : user1@2008AD.LAB
NetBIOS Name : 2008AD
SAM AccountName : group1
Domain : CN=Domain Users,CN=Users,DC=2008ad,DC=1a
primaryGroupName : test
aliasName : aliastest
UsernameMapFoundInfo : --
pszGecos : --
pszPrimaryGroupSid : --
PasswordExpired : --
PasswordNeverExpires : --
PasswordChange : --
UserCanChangePassword : --
AccountDisabled : --
AccountExpired : --
AccountLocked : --

Following is an example showcasing how to display detailed mapped information for a specified group name:

showfs -usermap -groupname ADE\group1
GID : 50002
SID : S-1-5-21-964874337-1665363193-2846560699-800
NetBIOS Name : 2008AD
UNIX Name : ADE\group1
SAM Account Name : group1
Domain : CN=Domain Users,CN=Users,DC=2008ad,DC=1a

Following is an example showcasing how to display detailed mapped information for a specified group id:
showfs -usermap -groupid 50002 -d
GID                          : 50002
SID                          : S-1-5-21-964874337-1665363193-2846560699-800
NetBIOS Name                 : 2008AD
UNIX Name                    : ADE\group1
SAM Account Name             : group1
Domain                       : CN=Domain Users,CN=Users,DC=2008ad,DC=la
aliasName                    : --
UsernameMapFoundInfo         : --

Following is an example showcasing how to display mapped information for a specified SID:

showfs -usermap -groupid S-1-5-21-964874337-1665363193-2846560699-800
GID                          : 50002
SID                          : S-1-5-21-964874337-1665363193-2846560699-800
NetBIOS Name                 : 2008AD
UNIX Name                    : ADE\group1
SAM Account Name             : group1
Domain                       : CN=Domain Users,CN=Users,DC=2008ad,DC=la

Following is an example showcasing how to export and copy mapping configuration to a client storage:

showfs -usermap -exportconf -file conf.txt

Following is an example showcasing how to Copy exported LDAP user entries to a client storage:

showfs -usermap -export users -provider Ldap -file /home/exports/Ldap.txt

Importing User Mapping Configuration

To import the user mapping configuration from a file specified on a client storage, issue the following command:

setfs usermap [-f] -importconf <file_path_on_client>

where,

• -importconf <filepath_on_client>
  Imports the user mapping configuration from the file specified on the client storage. This option cannot be used with any other options except -f.
• -f
  Suppresses the warning message. If this option is not used, the command requires a confirmation before proceeding with its operation.

Exporting Users/Groups Mapping Entries

To export the user/group mapping entries to a file, issue the following command

setfs usermap -export {users|groups} -provider <provider>

where,

• -export {users|groups}
Exports the users/groups entries to a file. If the export option is specified then the <provider> must also be specified. See the showfs -usermap command to learn about coping the exports file to a client storage. This option will generate a task id.

- **-provider <provider>**

  Specifies the type of authentication provider to be used to export users/groups entries. The authentication provider must be a “Local”, “LDAP” or “Active Directory”. If the provider option is specified the export option must also be specified.
File Provisioning Group

File Provisioning Group Overview

File Provisioning Groups (FPGs) represent the highest level component in the File Persona hierarchy. FPGs are logical containers on a storage system that hold the Virtual File Servers (VFSs). Each FPG can support one VFS.

NOTE:

Direct management of FPGs through the SSMC is only available in the advanced mode for File Persona configuration. When advanced mode is not enabled, an FPG is implicitly created as part of VFS provisioning.

Displaying Configuration Settings for File Provisioning Groups

To display information about an FPG, issue the following command:

```
showfpg -d <fpg_name>
```

where,

- `− d` displays a verbose listing of details about the specified FPG.
- `<fpg_name>` specifies the name of the FPG you want to investigate.

The following is the description of some of the key fields:

- **Active State**
  Indicates whether the FPG is currently activated. If the state is not ACTIVATED, shares will be unavailable.

- **Freeze/Isolation State**
  If the reported state is not NOT_FROZEN/ACCESSIBLE, File Persona may need to be restarted on a node using the `stopfs` and `startfs -enable` commands.

- **Files**
  Indicates how many inodes are currently consumed by file system objects in the FPG.

- **Files Free**
  Indicates the physically remaining inodes in the FPG irrespective of best practices.

- **Default CPG**
  If the FPG is grown, the additional storage will be consumed from this CPG.

- **Current Node**
  The node where the FPG is currently activated. If this is not the primary node, the FPG should be failed back to its primary node using the `setfpg -failover` command to reestablish proper balance.

The following example shows a sample output of the `showfpg` command with its various key fields and some possible values:
Creating File Provisioning Groups

To create an FPG on an HPE 3PAR StoreServ Storage system, issue the following command:

```
createfpg [{-full | -tdvv}] <nodeid> <cpgname> <fpg_name> <size>{t|T} -comment <comment_string>
```

where,

- `-full` specifies that the FPG will be created using fully provisioned volumes.
- `-tdvv` specifies that the FPG will be created using thinly deduplicated volumes.

**NOTE:** When using the `-tdvv` option, the underlying VV limit is 16Tib therefore a `createfpg -tdvv` of > 16Tib results in creation of multiple VVs to satisfy this tdvv VV restriction.

By default the underlying volumes are thinly provisioned if neither options such as `-full` nor `-tdvv` are specified. Tuning the underlying volumes between these settings is accomplished with the `tunevv` command. For more information on the `tunevv` command, see the *HPE 3PAR Command Line Interface Administrator Guide*.

- `<cpgname>`
specifies the name of the CPG used to contain the volumes associated with the file system.

- `<fpg_name>`

specifies the name of the FPG to be created.

- `<size>{t|T}`

specifies the size of the FPG to be created. The minimum FPG size is 1TiB, and the maximum file system size is 64 TiB. For example: 16T.

**NOTE:**
Filling a file system beyond 90% of its defined capacity can result in throughput degradation. The degree of degradation may vary depending on the amount of file system fragmentation and the write request sizes and patterns.

- `<nodeid>`

binds the created FPG to the specified node.

**NOTE:**
For information on balancing client access to File Persona across the available nodes, see Setting the Primary Node for a File Provisioning Group on page 49.

- `<comment_string>`

is the text you are adding to the description of the FPG.

The FPG is activated by the `createfpg` command. You can verify that the FPG was created with the `showfpg` command. For more information about the `createfpg` and `showfpg` commands, see the HPE 3PAR Command Line Interface Reference. You can also create an FPG with a more limited set of options in a combined step with the creation of a VFS. For more details, see "Creating Virtual File Servers on page 53".

To add a description for the FPG that is to be displayed when the `showfpg -d` command is used, issue the following command:

```
setfpg -comment <comment_string> <fpg_name>
```

where,

- `<comment_string>`

is the text you are adding to the description of the FPG.

- `<fpg_name>`

specifies the name of the FPG.

Creating an FPG using the SSMC:

- From the main menu, select File Persona > File Provisioning Groups.
- Click + Create File Provisioning Group or select Create on the Actions menu.
- Follow the instructions in the dialog box that opens and click Create.

**NOTE:**
File Provisioning Group (FPG) names must be unique across all systems even when using Remote Copy for replication of the FPGs. Using duplicate names across systems will result in shares being unavailable upon recovery on the target system.
Removing and Recovering File Provisioning Groups

To remove an FPG and its associated components issue the following command. Note that you must remove all File Shares in the FPG before removing the FPG itself.

⚠️ CAUTION:

If the removefpg command is executed without the -forget option, the FPG is permanently deleted and cannot be recovered. If there are scheduled tasks setup for this FPG, also delete these schedules to avoid errors for these scheduled tasks.

Removing an FPG using HPE 3PAR CLI

To remove an FPG, issue the following command:

```
removefpg [-forget] [-wait] [-pat] [-f] <fpg_name | pattern> ...
```

where,

- `-forget`
  specifies the FPG is removed, but can be restored with the `createfpg -recover` command, keeping the virtual volumes intact.

- `-wait`
  specifies that the removal task waits until the associated task is completed before proceeding. This option produces verbose task information.

- `-pat`
  stipulates that glob-style patterns for names of FPGs are to be used and any FPGs with names matching the specified pattern are removed. By default, confirmation is required to proceed with the command unless the `-f` option is specified. This option must be included in order to supply glob-style name patterns to the command using the `<pattern>` specifier.

- `-f`
  specifies that the command is forced. If this option is not used, the command requires confirmation before proceeding with the operation.

- `<fpg_name>`
  specifies the name of the FPG to be removed. This specifier can be repeated to remove multiple FPGs.

- `<pattern>`
  specifies a glob-style pattern to match the names of multiple FPGs. This specifier can be repeated to remove multiple FPGs. If this specifier is not used, the `<fpg_name>` specifier must be used.

The command output will follow the order below:

- In case of syntactical error, an error will be displayed to the user.
- If File Lock Compliance mode is not enabled (see [File Lock Compliance mode](#)) for the underlying VFS and File Store, then a task ID is returned the user.
- If the VFS or File Store under the FPG has the File Lock Compliance mode enabled, an error message will be displayed "Request ID: <request-id>. Command sent for Compliance Officer (CO) approval for execution".

**NOTE:**

When deleting a Virtual Volume that belongs to File Lock Compliance mode enabled FPG (see [File Lock Compliance mode](#)), the removevv command will return an error message "Cannot remove VV <VVname>. It belongs to a Compliance enabled FPG".

Recovering an FPG using HPE 3PAR CLI

To recover an FPG that was removed with the `removefpg -forget <fpg_name>` command, issue the following command:
createfpg -recover [-wait] {{<vv_1> <vv_2>...} | [set:<setname>]} 

where,

- **-recover**
  
  specifies that an FPG removed with the removefpg -forget command is to be restored.

- **-wait**
  
  specifies that the recover task waits until the associated task is completed before proceeding. This option produces verbose task information.

- **<vv_1> <vv_2>**
  
  specifies a list of Virtual Volumes to be attached. Any FPGs on them will be discovered.

- **set:<setname>**
  
  as an alternative to specifying a list of VVs, specifies a Virtual Volume set which contains the set of Virtual Volumes to be recovered. A VV set is automatically created for each FPG, so this syntax is often simpler.

You can verify that an FPG was removed or recovered by using the showfpg command. For more information about the removefpg and showfpg commands, see the HPE 3PAR Command Line Interface Reference.

**IMPORTANT:**

Attempting to recover an FPG with a newer On-Disk version than what is supported by the running version of software will be rejected. Make sure not to try replication of FPGs with a newer On-Disk version until the target array has had its software upgraded to support the new On-Disk version. The following are the supported On-Disk versions based on the software version:

- HPE 3PAR OS 3.3.1 <= 12.1
- HPE 3PAR OS 3.2.2 MU2 <= 12.0
- HPE 3PAR OS 3.2.2 MU1 and earlier <= 11.0

### Activating and Deactivating File Provisioning Groups

To make an FPG and all of its resources available or unavailable, issue the following command:

```
setfpg -forced [-activate | -deactivate] <fpg_name>
```

where,

- **-activate**
  
  activates the FPG and makes its resources available.

- **-deactivate**
  
  deactivates the FPG, making its resources unavailable.

- **<fpg_name>**
  
  specifies the name of the FPG you are activating or deactivating.

- **-forced**
  
  specifies that in the event that a graceful failover is not possible, the failover operation will be forced. If this option is used, it may be necessary to stop and start File Persona on the node before the FPG can be activated again.

**NOTE:**

If an FPG is deactivated and there are scheduled tasks for this FPG setup, these tasks will report errors if they are executed during the time the FPG is not active.
In case of a planned shutdown or deactivation of an FPG, it is recommended that File Share users (NFS and SMB) reduce their workload or stop using the File Share before the file system on which the File Share exists is disabled or failed-over to another node. Otherwise, the production load could throttle and bring down the cluster. This would also allow the event framework to drain its logs to disk quickly.

**Activating a File Provisioning Group using the SSMC:**
- From the main menu, select **File Persona**, and then select **File Provisioning Groups**.
- To activate a File Provisioning Group, select the group, select the **Actions** menu, select **Edit**, and then click **Activate**.

**Deactivating a File Provisioning Group using the SSMC:**
- From the main menu, select **File Persona**, and then select **File Provisioning Groups**
- To deactivate a File Provisioning Group, select the group, select the **Actions** menu and then click **Deactivate**.

### Expanding the Size of File Provisioning Groups

To expand the size of an FPG by a specified amount, issue the following command:

```
growfpg <fpg_name> <size>{t|T}
```

where,
- `<fpg_name>` specifies the name of the FPG targeted for resizing.
- `<size>{t|T}` specifies the amount of additional space to add to the FPG. The minimum growth increment is 100 GiB and the maximum FPG size is 64 TiB. The specified additional space will be added by growing the existing volume(s) that make up the FPG.

**NOTE:** If the FPG was created using Thinly Deduplicated Virtual Volumes (TDVV), the max FPG size is 64 TiB. There are performance implications to using `growfpg` excessively, so it is not practical to start at 100 GiB and grow in 100 GiB increments to a large size like 64 TiB. It is recommended to grow the FPG by larger increments of at least 10% or 1 TiB (whichever is lesser). If the FPG grow operation is interrupted, the FPG may not have access to the newly allocated storage in the underlying volume(s). If this condition occurs, an additional request to grow the FPG by a small amount (e.g., 100 GiB) will cause the new storage to be incorporated in addition to the previously requested storage.

You can verify changes by using the `showfpg` command. For more information about the `growfpg` and `showfpg` commands, see the [HPE 3PAR Command Line Interface Reference](https://www.hpe.com/us/en/solutions/3par/3-par-command-line-interface-reference.html).

### Setting the Primary Node for a File Provisioning Group

When a File Provisioning Group (FPG) is initialized, File Persona will assign it a default primary node with the objective of balancing File Persona services across the available nodes. Depending on the network configuration and traffic, the default primary node assignment for a given FPG may not provide an ideal balance. If an imbalance exists, it may be worthwhile to set the primary node for an FPG to a specific node in order to create a better balance. This operation may result in a short disruption of client connections.

When you specify the primary node for an FPG, the other node in the node pair becomes the default alternate node. For example, in a node pair constituted by nodes 2 and 3 on a system, if you set node 2 to be the primary node for the FPG, then node 3 is automatically the default alternate node in the node pair.

To assign an FPG to use a specific primary node, issue the following command:

```
setfpg -primarynode <nodeid> <fpg_name>
```

where:
- `<nodeid>`
  specifies the ID number of the node to be used as the primary node for the FPG.
- `<fpg_name>`
  specifies the name of the FPG for which the primary node is to be set.

The `-primarynode` option cannot be used with the `-failover` option in the execution of the `setfpg` command.

### NOTE:
Although NFS clients are able to enumerate exports from all VFSs through any of the VFS IP addresses active on a node, it is important to connect only to the exports through the IP address specifically associated with a given export's VFS. Failure to do so may lead to failures in migration of FPGs from one node in a node pair to another using the `setfpg -primarynode` command or the `setfpg -failover` command.

When using `setfpg -primarynode` there is a momentary loss of access to the share while the FPG is unmounted and mounted.

---

## Failover Nodes for File Provisioning Groups

An FPG can be moved back and forth between the primary and failover node in the node pair. An FPG is automatically moved to the failover node during an online upgrade, a hardware failure, or when the `stopfs` command is issued on the node. It can also be moved manually when servicing a node. If a failover operation is attempted for an FPG and the secondary (failover) node is unavailable, the FPG is failed back to the primary node. If reverting from the primary node is not possible, then access to the FPG and its File Shares is terminated.

If an attempt to switch to the failover node is unsuccessful it is possible to force the operation. To move the FPG to the failover node in a node pair, issue the following command:

```bash
setfpg -failover [-forced] <fpg_name>
```

where,

- `-failover`
  indicates that if the FPG is currently hosted on the primary node, the FPG is moved to the failover node. If the FPG is currently hosted on the failover node, the FPG is moved back to the primary node.
- `-forced`
  specifies that in the event that a graceful failover is not possible, the failover operation will be forced. The isolation/freeze state results displayed from the `showfpg -d` command may indicate the need to force a failover. If the `-forced` option is used, it may be necessary to stop and start File Persona on the primary node before the FPG can be activated again.
- `<fpg_name>`
  specifies the name of the FPG.

The `-primarynode` option cannot be used with the `-failover` option in the execution of the `setfpg` command.
NOTE:
An FPG failover can sometimes be unsuccessful. The following error message will be displayed:

Failed to failover <fpg_name>: Existing operation mountFileSystem for FPG <fpg_name> is already pending that is in conflict with requested operation mountFileSystem.

In a situation like this, wait for a few seconds and retry the failover on the FPG again.

On-disk Version in relation to File Persona Features

The following table lists the required On-Disk Version (ODV) in relation to the specific File Persona features:

<table>
<thead>
<tr>
<th>File Persona Feature</th>
<th>On-Disk Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quota Accounting (excluding snapshots)</td>
<td>ODV &gt;= 11.1</td>
</tr>
<tr>
<td>Online FSCK</td>
<td>ODV &gt;= 12.1</td>
</tr>
<tr>
<td>NTFS Security Mode</td>
<td>ODV &gt;= 12.1</td>
</tr>
<tr>
<td>Sophos Antivirus</td>
<td>ODV &gt;= 12.1</td>
</tr>
<tr>
<td>File Lock</td>
<td>ODV &gt;= 12.1</td>
</tr>
<tr>
<td>Native ACL format on disk</td>
<td>ODV &gt;= 12.2</td>
</tr>
<tr>
<td>File Access Auditing</td>
<td>ODV &gt;= 12.2</td>
</tr>
</tbody>
</table>

Checking Whether FPG is Upgradable or Not

A symbol, *, is added next to the Version output of the showfpg command if the FPG is upgradable from its current version. It signifies that the FPG is upgradable from the current version.

After performing a software upgrade, the state of File Provisioning Groups (FPGs) may be reported as "degraded", due to the On-Disk version no longer being at the latest available version. This will additionally be indicated with an asterisk next to the Version value in the showfpg output. When displaying FPG details with the showfpg -d command, the Upgrade State will be reported as UPGRADABLE. If the software does not have to be reverted but the arrays where the FPG gets replicated are upgraded to the same 3PAR OS version, the On-Disk version can be upgraded to the latest version using the setfpg -upgrade <fpgname> command.

The following is a sample output of the showfpg command where an FPG named testFpg0 is degraded to On-Disk version 11.0. The symbol * signifies that the FPG can be upgraded.
### Upgrading On-disk Version

The On-Disk version of an FPG can be upgraded using the `setfpg -upgrade` CLI command. This command will upgrade the On-Disk version of an FPG to the latest supported version. Before the upgrade gets executed, a warning message will be displayed to the user to confirm whether the user wants to proceed ahead with the upgrade. This confirmation can be suppressed with the `-f` option.

To upgrade the On-Disk version of an FPG, issue the following command:

```
setfpg -upgrade [-f] <fpgname>
```

where,

- `upgrade`  
  The `upgrade` option upgrades the On-Disk version
- `<fpgname>`  
  Name of the FPG that needs to be upgraded
- `-f`  
  Suppresses confirmation from user for upgrading the disk

The output of the command is a `task-id`. The `showtask -d <task-id>` command displays the progress of the task.

**Examples**

The following example shows how to upgrade an FPG with confirmation

```
setfpg -upgrade testFpg0  
This action will upgrade the current On-Disk version of the FPG  
to the latest supported version.  
select y=yes n=no :  y  
8778
```

The following example shows how to upgrade an FPG without confirmation

```
setfpg -upgrade -f testFpg0  
8779
```

**NOTE:**

After an offline upgrade of the HPE 3PAR OS and the File Persona feature, the health of all existing FPGs will be degraded. The On-Disk version of the FPG needs to be upgraded to remove the degraded state.
Virtual File Server

Virtual File Server Overview

Virtual File Servers (VFSs) act as a virtual device used to control many of the network policies for communication between File Persona managed objects and your network. Many management tasks and policy decisions can be performed at the VFS level. The VFSs are associated with File Provisioning Groups (FPGs) and contain the File Stores.

Displaying Configuration Settings for Virtual File Servers

To display information and configuration settings for a VFS, issue the following command:

```
showvfs [-d] [-fpg <fpg_name>] [-vfs <vfs>]
```

where,

- `-d` displays detailed output.
- `<fpg_name>` limits the displayed output to VFS contained within the specified FPG.
- `<vfs>` limits the displayed output to the specified VFS name.

**NOTE:**

Be sure to note the "Certificate Valid Until" field in the displayed output. This serves as a reminder to update the certificate before the indicated date, to avoid interruption of service for clients of Object Access.

Displaying information and settings for Virtual File Servers using the SSMC:

- Select File Persona > Virtual File Servers.
- A list of VFSs, detail views and an Actions menu is displayed.

Creating Virtual File Servers

To create a VFS, issue the following command:

```
createvfs [options] <ipaddr> <subnet> <vfsname>
```

- `[options]`

  are:

  - `-bgrace <time>` specifies the block grace time in seconds for quotas within the VFS.
  - `-igrace <time>` specifies the inode grace time in seconds for quotas within the VFS.
  - `-snapquota {enable | disable}`

    If `snapquota` is enabled, then snapshot blocks are included for quotas accounting. If disabled, then the snapshot blocks are excluded for quotas accounting.
NOTE:
snapquota is disabled by default if the snapquota value is not specified during creation of VFS. Modifying or switching the snapquota setting is not permitted. snapquota is always enabled for FPGs where On-Disk version <= 11.1.
User and group quotas never reflect snapshots. Only capacity quotas are impacted by this setting.

- One of the following certificate options can be specified.
  - -nocert
    does not create a self signed certificate associated with the VFS.
  - -certfile <certfile>
    specifies the file containing the certificate data you want to use.
  - -certdata <certificate string>
    specifies the string containing the certificate data you want to use.
- -fpg <fpg_name>
specifies the name of an existing FPG for which the VFS should be created.

When creating a new FPG as part of creating a VFS, the following options can be specified:
- -cpg <cpgname>
specifies the CPG in which the FPG should be created.
- -size <size>
specifies the size of the FPG to be created.
- -tdvv
  creates the FPG with tdvv volumes.
- -full
  creates the FPG with fully provisioned volumes.
- -node <nodeid>
specifies the node to which the FPG should be assigned. This can only be used when creating the FPG with the -cpg option.
- -vlan <vlanid>
specifies the VLAN ID associated with the VFS IP address.

NOTE: If the VLAN ID does not match the VLAN ID associated with the default gateway, only clients on the same subnet will be able to access shares for the VFS, unless additional static routes are defined for the VFS or its VLAN. The showfs -net command displays node and VLAN IDs.

- -wait
  waits until the associated task is completed before proceeding. This option will produce verbose task information.
- -comment
  specifies any additional textual information.
- <ipaddr>
specifies the IP address to which the VFS should be assigned.
- <subnet>
specifies the subnet mask for the IP address.

- `<vfsname>` 

specifies the name of the VFS to be created.

Go to the Configuring Network Settings for Virtual File Servers section for advanced configuration settings.

To create a VFS using the SSMC, follow these steps:

Creating a Virtual File Server from a File Persona Configuration screen

- From the main menu, select File Persona > File Persona Configuration > Virtual File Servers.
- Select Actions, and then select Create Virtual File Server.
- Follow the instructions on the dialog that opens.

Creating a Virtual File Server from a File Provisioning Groups screen

This path is only available in advanced mode of File Persona configuration in SSMC.

- From the main menu, select File Persona > File Provisioning Groups > Virtual File Servers.
- Select Actions, and then select Create Virtual File Server.
- Follow the instructions on the dialog that opens.

Creating a Virtual File Server from a Virtual File Servers screen

- From the main menu, select File Persona > Virtual File Servers.
- Select Actions, and then select Create.
- Follow the instructions on the dialog that opens.

Deleting Virtual File Servers

Only an empty VFS can be deleted. If the VFS contains File Stores that are not prepared for deletion, you must first prepare the File Stores for deletion, or remove them. See Removing File Stores.

To delete an empty VFS (after removing the File Stores) and its underlying components, issue the following command:

```
removevfs [-f] [-fpg <fpg_name>] <vfs>
```

where,

- `-f` specifies that the command is forced. If this option is not used, the command requires confirmation before proceeding with its operation.
- `<fpg_name>` specifies the name of the parent FPG.
- `<vfs>` specifies the name of the containing VFS.

Deleting an empty Virtual File Server using SSMC:

- From the main menu, select File Persona > Virtual File Servers.
- On the list pane, select the VFS, select the Actions menu, and then select Delete.
- If you are not sure that the VFS should be deleted, click Cancel; otherwise, click Delete to start the action and close the dialog.

Configuring Network Settings for Virtual File Servers

Displaying Network Settings for Virtual File Servers

To display network settings of a VFS, issue the following command:

```
showvfs [options]
```
where,

- **-d**
  
  displays detailed output.

- **-fpg <fpg>**
  
  limits the display to VFSs contained within the FPG.

- **-vfs <vfs>**
  
  limits the display to the specified VFS name.

You can also display the network settings of a VFS using the following command:

```
showfsip [-fpg <fpg>] <vfs>
```

where,

- **-fpg <fpg>**
  
  specifies the FPG in which the VFS was created.

- **<vfs>**
  
  specifies the VFS name to which the display is limited.

Network settings for a VFS are available in the **Overview** pane when a VFS is selected in the SSMC.

### Assigning IP Addresses to Virtual File Servers

To assign an IP address to a VFS, issue the following command:

```
createfsip [-vlantag <tag>] <ipaddr> <subnet> <vfs>
```

where,

- **<tag>**
  
  specifies the VLAN tag used for the VFS IP address (VFSIP).

- **<fpg_name>**
  
  specifies the name of the FPG to which the VFS belongs.

- **<ipaddr>**
  
  specifies the IPv4 address assigned to the VFS.

- **<subnet>**
  
  specifies the subnet for the IP address used in the **<ipaddr>** variable.

- **<vfs>**
  
  specifies the name of the VFS that is being created.

Multiple IP addresses can be used in disaster recovery solutions. An alternate IP address can be configured for a VFS when using Remote Copy to replicate an FPG to another array. When the FPG and VFS are activated on the other array, the IP address will be ready for use.

Verify changes with the **showfsip** command. For more information about the **createfsip** and **showfsip** commands, see the **HPE 3PAR Command Line Interface Reference**.

---

**NOTE:**

If you attempt to add a VFS IP address while the FPG containing this VFS is being deactivated, an error may be returned (with a message saying “FPG is not mounted”) even though the actual operation was completed successfully. After the FPG is activated again, you should verify if the configuration was successful and retry the request if needed.

Assigning an IP address to a VFS using the SSMC:
• On the main menu, select File Persona > Virtual File Servers.
• On the list pane, select the VFS, and then select Edit on the Actions menu.
• In the Networking panel on the dialog that opens, click Add.
• Follow the instructions on the dialog that opens.

Removing Network Settings from Virtual File Servers

To remove an IP address to a VFS, issue the following command:

```
removefsip [options] <vfs> <id|ip>
```

where,

- `<fpg_name>` specifies the FPG name in which the VFS was created.
- `-f` specifies that the operation is forced. If this option is not used, the command requires confirmation before proceeding with its operation.
- `<id|ip>` specifies the ID/IP for the network configuration.
- `<vfs>` specifies the VFS which is to have its network configuration removed.

Removing an IP address to a VFS using the SSMC:

• From the main menu, select File Persona > Virtual File Servers.
• On the list pane, select the VFS, select the Actions menu, and then select Edit.
• Click the X next to the IP address you want to remove.

Modifying Network Settings of Virtual File Servers

To modify an IP address of a VFS, issue the following command:

```
setfsip [options] <vfs> <id>
```

where,

- `<tag>` specifies the VLAN Tag to be used.
- `<ipaddr>` specifies the new IP address.
- `<subnet>` specifies the new subnet mask.
- `<fpg_name>` specifies the FPG in which the VFS was created.
- `-f` specifies that the operation is forced. If this option is not used, the command requires confirmation before proceeding with its operation.
- `<vfs>` specifies the VFS which is to have its network configuration modified.
- `<id>` specifies the ID for the network configuration.

Modifying an IP address of a VFS using SSMC:

• From the main menu, select File Persona > Virtual File Servers.
• On the list pane, select the VFS, and then select Edit on the Actions menu.
• In the Networking panel on the dialog that opens, click the edit icon.
• Follow the instructions on the dialog that opens.

Modifying Settings for Virtual File Servers

You can specify the parameters of a VFS when you create the VFS, and modify the parameters after the VFS is created.

To modify configuration settings for a VFS, issue the following command:
setvfs [{-certfile <cert_file>|-certdata <cert_string>|-certgen|-rmcert <cert_name>}] [-comment "<comment_string>"] [-bgrace <bgrace_time>] [-igrace <igrace_time>] <fpg_name> <vfs>

where,

- [{-certfile <certfile>]
  specifies the file containing the certificate data you want to use.
- {-certdata <certificate_string>]
  specifies the string containing the certificate data you want to use.
- {-certgen]
  generates and sets a certificate for the VFS.
- {-rmcert]
  removes the certificate from the VFS.
- {<comment_string>]
  specifies any additional textual information.
- {-bgrace <time>]
  specifies the block grace time in seconds for quotas within the VFS.
- {-igrace <time>]
  specifies the inode grace time in seconds for quotas within the VFS.
- {<fpg_name>]
  specifies the name of an existing FPG in which the VFS should be modified.
- {<vfs>]
  specifies the name of the VFS to be modified.

Modifying settings for Virtual File Servers with the SSMC:

- From the main menu, select File Persona > Virtual File Servers.
- On the list pane, select the VFS, and then select Edit on the Actions menu.
- Follow the instructions on the dialog that opens.

Backup and Recovery of Configuration settings of Virtual File Servers

Back up configuration settings for virtual file servers

The `backupfsconf` command creates a configuration backup for a VFS. A configuration backup file is created with a standard name (\(<\text{fpg}_1\_<\text{vfs}_1\>_\text{configbackup.tar}\)) in the .admin File Store under the VFS in a directory named `configbackup`.

A backup file is created for each VFS. Any subsequent backup overwrites the backup file. File Stores in legacy security mode can be restored in NTFS security mode.

The `backupfsconf` command captures the following details of a VFS:

- VFS IPs
- Certificate
- File Stores: The supported security modes for each File store is backed up along with the security mode error flag
- File Share definitions of protocols defined on a specified VFS
- Access Control List (ACLs) & ownership of the shared folders - The ACLs & ownership details of the share folders may include default values or could be set using the command `setfshare` or could be set by the
client. The current release supports backup of ACLs and ownership details of the share folders. There is only one set of permissions stored on the disk using Application Data Environment (ADE) ACLs which will be backed up

- Antivirus polices that are applied at the VFS and File Store level
- Quota limits - this includes user, group and File Store quota limits at the VFS level
- File Access Audit settings

NOTE:
The backup process does not cover settings that were made outside the VFS. Those settings should be recorded for further reference using the `showfs` subcommands and the `showfsav` command. The settings made at a higher level than the VFS with `setfs` and `setfsav` are not included in this restoration process and should be configured before attempting the VFS restoration. As quota limits are applied on UIDs/GIDs/File Store, for successful restoration of correct quota limits for user, group and File Stores, user IDs and group IDs need to be configured with the same values as on the original array.

Initially, the ACL's format is derived from the On-Disk Version (ODV) of the backup FPG (e.g. 12.1) but it gets converted to the new format (Native ACL format On-Disk) on restoration if the ODV of the restored FPG is 12.2 or later.

Restoring a configuration backed up from an FPG with ODV 12.1 or earlier will force the ACL principles to be validated when restored to ODV 12.2 or later. This would report all potential name resolution issues related to invalid ACLs. Once the configuration is restored to an FPG with ODV 12.2 or later, it is recommended that the configuration should be backed up once again to prevent re-translation issues during subsequent restorations.

WARNING:
Configuration backups for a VFS may not be restorable on older versions of HPE 3PAR OS. If you revert the HPE 3PAR OS to a previous version, you should run a new configuration backup to ensure that it is compatible with that version of software.

To back-up configuration settings for a VFS, issue the following command:
```
backupfsconf [-fpg <fpg_name>] <vfs>
```
where,

- `<fpg_name>` specifies the name of an existing FPG in which the VFS should be backed up.
- `<vfs>` specifies the name of the VFS to be backed up.

Do the following to complete the configuration backup:

1. Run the `backupfsconf` command.
   This will create a standard backup file (`<fpg>_vfs_configbackup.tar`) in the `.admin` File Store under the VFS in a directory named `configbackup`. This file will be used at the time of configuration restoration.

2. Create an NFS/SMB share on the `.admin` File Store without the `sharedir` option specified to copy the backup artifact to another location/client.

Example:
```
createfs hypn -fpg fs1 -options rw no_root_squash -fstore .admin mtree1 adminshare
```

Or
createfshare smb –allowperm Everyone:fullcontrol –fpg fs1 –fstore .admin mtreel adminshare

3. Export/mount the share created in step 2, copy the backup artifact found in the configbackup directory to another location/client or have it backed up using a supported backup application.

The process of executing the backupfsconf command and backing up the generated backup artifact using the share on .admin or supported backup application should be repeated periodically.

As the backupfsconf command only captures the configuration settings and not data found in the File Store, perform data backup of this data separately using supported backup applications such as Symantec Net backup, HPE Data protector etc. For more details, refer to section "Backup and Disaster Recovery for File Persona".

Restoring Configuration Settings for Virtual File Servers

The restorefsconf command restores the configuration settings for a VFS. The restore feature will fail if the VFS has existing contents. The restorefsconf command restores the configuration settings using the backup artifact file found in the .admin File Store under the VFS in the configbackup directory.

To restore configuration settings for a VFS, issue the following command:

restorefsconf [-fpg <fpg_name>] <vfs>

where,

• <fpg_name>
  specifies the name of an existing FPG in which the VFS should be restored.

• <vfs>
  specifies the name of the VFS to be restored.

When restoring a VFS after a backup, you must do the following before running the restorefsconf command:

1. Manually reconfigure any global settings captured at the time of backup.
2. Create a new FPG with same name as the backup file.
3. Create a new VFS with the same name as the backup file and with the nocert option.
4. Create an NFS/SMB share on the target .admin File Store without the sharedir option.

Example

createfshare nfs –fpg fs1 –options rw no_root_squash –fstore .admin mtreel adminshare

Or

createfshare smb –allowperm Everyone:fullcontrol –fpg fs1 –fstore .admin mtreel adminshare

5. Export the mount share created in step 4, copy the backed up backup artifact file (previously copied to other location/client) into the configbackup folder in the target .admin File Store of VFS or by using a supported backup application.

6. Remove the share created in step 4 from the target .admin File Store.
7. Remove all VFS IPs found on the target VFS, use the removefsip command to remove IPs previously assigned to VFS.
8. As the backupfsconf command backs up and recreates the VFS IP address during restoration it is required to remove the VFS IPs from the source VFS prior to restoration.
9. Run the `restoresconf` command.

10. **NOTE:**

    If the backup VFS certificate has expired, the restoration on the VFS will not take place. If the VFS to be restored has a certificate assigned to it, the certificate will get overwritten with the backup certificate.

After the restoration operation has been completed successfully, verify the restoration operation by examining all the backed up details determine whether they are restored properly or not.

If data restoration is required in a VFS, perform data restoration using supported backup applications such as Symantec Net backup and HPE Data protector.
File Store

File Store Overview

File Stores are created in Virtual File Servers (VFSs). At the File Store level the user can take snapshots, manage capacity quotas and designate security modes. The user can also create File Shares for different access protocols and customize antivirus scan service policies. Up to 256 File Stores are supported on a node pair: 16 File Stores supported for each VFS.

HPE 3PAR SSMC can automatically create File Stores whenever you create a File Share. You can specify the properties and settings of File Stores on a storage system. For example, you can specify the File Store’s name, the parent VFS, and additional settings such as antivirus scan policies and quotas for file sizes and number of files.

If the File Stores option is not listed in the SSMC main menu, you can unhide the menu item by selecting the advanced options in the main menu. When a VFS is created, a File Store with a name .admin is automatically created. The .admin File Store is used as part of antivirus scanning, quotas, File Lock, audit logs and configuration backup features.

**NOTE:**

It is advised not to set quotas in the .admin File Store. The File Store, .admin, is a system created File Store and is used for system internal and support activities.

Displaying Configuration Settings for File Stores

To display information and configuration settings for File Stores and their underlying components, issue the following command:

```
showfstore [-fpg <fpg_name>] [-vfs <vfs>] [-fstore <fstore>]
```

where,

- `<fpg_name>` limits the display to a VFS contained within the specified FPG.
- `<vfs>` limits the display to the specified VFS.
- `<fstore>` limits the display to the specified File Store.

Following are some examples showcasing the `showfstore` command in its various forms:

<table>
<thead>
<tr>
<th>FStore</th>
<th>VFS</th>
<th>FPG</th>
<th>State</th>
<th>Mode</th>
<th>ErrorSuppression</th>
<th>Security</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>.admin</td>
<td>vfs1</td>
<td>fpg1</td>
<td>normal</td>
<td>legacy</td>
<td>false</td>
<td></td>
<td></td>
</tr>
<tr>
<td>fstore1</td>
<td>vfs1</td>
<td>fpg1</td>
<td>normal</td>
<td>legacy</td>
<td>false</td>
<td></td>
<td></td>
</tr>
<tr>
<td>.admin</td>
<td>vfs2</td>
<td>fpg1</td>
<td>normal</td>
<td>NTFS</td>
<td>true</td>
<td></td>
<td></td>
</tr>
<tr>
<td>fstore2</td>
<td>vfs2</td>
<td>fpg1</td>
<td>normal</td>
<td>NTFS</td>
<td>false</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

4 total
Creating File Stores

File Persona supports multiple access protocols such as SMB, NFS, Object Access API and FTP. Special care is required when exported files are accessed using the four protocols as they use different security and identity semantics. SMB clients use NTFS ACLs for security and SIDs for identity. NFS, Object Access API and FTP clients use POSIX ACLs for enforcement (if they exist) otherwise they use mode bits. NFS and Object Access API both use UID/GID for identity.

File Persona introduces protocol-compliant dedicated security modes to provide native experience for preferred protocol access. The following list describes the security modes:

- **LEGACY**
  
The Legacy security mode allows backward compatibility, where a File Store can be configured to use security semantics from HPE 3PAR OS 3.3.1 File Persona and earlier. If the user desires, File Stores can still be configured in this mode. In Legacy mode, one protocol has read/write access and other protocols have read-only access. However, this mode should not be used if the user wants read/write access on both Windows and non-Windows clients. If the user desires read/write access on both Windows and non-Windows clients in a cross-protocol environment, NTFS security mode should be used.

- **NTFS**
  
The NTFS security mode allows read/write access to any file protocol supported by File Persona. Read/write access is granted to both Windows and non-Windows clients, such as; create/read/write/delete/rename files and directories. It enforces NTFS-style security behavior on file/folders in the File Store. Non-Windows clients can view permissions but cannot set permissions.

Refer to chapter **Cross-protocol Access** for more details on security modes and shared folder permissions.

Creating a File Store using the HPE 3PAR CLI

To create a File Store and its underlying components, issue the following command:

```bash
createfstore -secmode {NTFS|legacy} [-secop_errsuppress {true|false}] [-comment <comment>] [-fpg <fpgname>] <vfs> <fstore>
```

The options described in the following list:

- `-secmode {NTFS|legacy}`
- `-secop_errsuppress {true|false}`

The `-secmode` option is a mandatory parameter. The second option is used only when creating File Stores in NTFS security mode. If this option is not specified, the value will be set as `false`.

The various parameters for the `createfstore` CLI command are listed below:

- `-secmode {NTFS|legacy}`
  
specifies the security mode of the File Store. Valid values are NTFS or Legacy.
- `-secop_errsuppress {true | false}`
In NTFS security mode, permission changing operations will report error messages for non-root users when `-secop_errsuppress` is `false`. This may not be the ideal behavior for some applications trying to implicitly perform a permission changing operation such as `chmod` and `setfacl` over an NFSv3 client. This option can be set to `true` to allow applications to work with NFSv3 clients. If not specified, the option will be set to `false`. This is an optional parameter and can be used only for File Stores in NTFS security mode.

**NOTE:** Files created in UNIX will inherit permissions in NTFS style. Setting this attribute to `true` does not allow the user to set UNIX permissions. However, because permissions are set, although they are based on NTFS inheritance rules, error reporting will be suppressed to allow UNIX applications to succeed without error. Some of the UNIX utilities which are known to fail or partially fail on an NFSv3 mount on an NTFS security mode File Store if `secop_errsuppress` is set to `false` are: "vi", "mkdir" and creating a file using the Linux I/O output redirector (for example: "echo hello > filename"). Over an NFSv4 mount, "vi" will also partially fail (will fail to create swap files). If the user is accessing an NTFS File Store cross-protocol from a UNIX client, the user will be prompted an error message "Operation not permitted" with the above mentioned utilities or with any other UNIX utilities that implicitly changed permissions. The recommendation is to set the File Store security attribute `secop_errsuppress` to `true`.

- `-comment <comment>`
  This option is used to specify the comment for the given File Store.
- `-fpg <fpgname>`
  Specifies the File Provisioning Group (FPG) that the `<vfs>` is associated with. If this is not specified, the command will find the FPG based on the specified `<vfs>`. However, if `<vfs>` exists under multiple FPGs, `-fpg` must be specified.
- `<vfs>`
  This option specifies the Virtual File Server name on which the File Store is to be created.
- `<fstore>`
  This option specifies the name of the File Store to be created.

### Creating a File Store using the SSMC
- From the main menu, select **File Persona > File Stores.**
- Click **+ Create File Store** or select **Create** on the **Actions** menu.
- Follow the instructions on the dialog that opens.

#### Example
**Examples for `createfstore`:**

```
createfstore --secmode NTFS --secop_errsuppress true --fpg fpg1 vfs1 fstore1

createfstore --secmode NTFS --secop_errsuppress false --fpg fpg1 vfs1 fstore2

createfstore --secmode legacy --comment "File Store with legacy mode" vfs1 fstore3
```

### Removing File Stores
You must prepare the File Stores for deletion before removing them. To prepare File Stores for deletion:
1. Remove all snapshots on the File Store.
2. Remove all files and folders from the File Store using an administrative share at the root of the File Store, e.g. at /<fpg_name>/<vfs_name>/<fstore_name>/. 
3. Remove all shares from the File Store.

**IMPORTANT:**

The File Store removal operation will only succeed if all snapshots for it were removed successfully first. Ensure all snapshots and snapshot schedules are removed prior to issuing the File Store deletion operation.

To remove a File Store from the system, issue the following command:

```
removefstore [-f] [-fpg <fpg_name>] <vfs> <fstore>
```

where,

- `-f`
  - specifies that the command is forced. If this option is not used, the command requires confirmation before proceeding with its operation.
- `<fpg_name>`
  - specifies the name of the parent FPG.
- `<vfs>`
  - specifies the name of the containing VFS.
- `<fstore>`
  - specifies the name of the File Store to be removed.

Verify changes with the `showfstore` command. For more information about the `removefstore` and `showfstore` commands, see the HPE 3PAR Command Line Interface Reference.

**Removing a File Store using the SSMC:**

- From the main menu, select **File Persona > File Stores.**
- On the list pane, select the File Store, and then select **Delete** on the **Actions** menu.
- Follow the instructions on the dialog that opens.

## Modifying File Stores

To modify configuration settings for File Stores and their underlying components, issue the following command:

```
setfstore [-fpg <fpiname>] [-secop_errsuppress {true|false}] [-comment <comment>] <vfs> <fstore>
```

The various options for the `setfstore` command are as follows:

- `-fpg <fpgname>`
  - Specifies the File Provisioning Group (FPG) that the `<vfs>` belongs. If this is not specified, the command will find the FPG based on the specified `<vfs>`. However, if `<vfs>` exists under multiple FPGs, `-fpg` must be specified.
- `-secop_errsuppress {true | false}`
  - Enables or disables the security operations error suppression for the File Stores in NTFS security mode. In NTFS security mode, permission changing operations will report error messages for non-root users when the `secop_errsuppress` is **false**. This may not be the ideal behavior for some applications trying to implicitly perform a permission changing operations such as `chmod` over an NFSv3 client. This parameter
can be set to true to allow these applications to work with NFSv3 clients. This is an optional parameter and is applicable only for File Stores in NTFS security mode.

- **-comment <comment>**
  
  This option is used to specify the comment for the given File Store.

- **<vfs>**
  
  This option specifies the Virtual File Server name on which the File Store to be created.

- **<fstore>**
  
  This option specifies the name of the File Store to be created

**Modifying a File Store using the SSMC:**

- From the main menu, select **File Persona > File Stores**.
- On the list pane, select the File Store, and then select **Edit** on the **Actions** menu.
- Follow the instructions on the dialog that opens.

Following are a few examples showcasing the `setfstore` command in its various forms:

```plaintext
setfstore -secop_errsuppress true vfs1 fstore1

setfstore -secop_errsuppress false -fpg fpg1 vfs1 fstore1

setfstore -secop_errsuppress true -comment "File Store with legacy mode" vfs1 fstore1
```

### Creating File Shares on Non-existing File Stores

A warning message will be displayed when a user tries to create a File share on a File Store that does not exist. This happens when the `createfshare` command is used when a File Store does not exist. Legacy File Stores are mostly created for backwards compatibility and are not recommended in cross-protocol environments where read-write access is desired from both Windows and LINUX/UNIX clients. It is recommended that the user explicitly creates File Stores in the desired security mode before creating File Shares for any protocol.

However, if the user uses the `createshare` CLI command to create a File Share and the specified File Store does not exist, File Persona will create the File Store for the user. The procedure used is as follows: if the File Share being created is an SMB share, File Persona will create a File Store in the NTFS security mode; if the File Share being created is for NFS, FTP or Object Access API protocol, File Persona will create the File Store in the Legacy security mode.

The following list displays possible warning messages for each File Share type when the File Store does not exist:

- **NFS/FTP/OBJ shares**
  
  No warning message will be displayed. File store will be created in Legacy mode.

- **SMB shares**

  ```plaintext
  "Warning: File store <filestore_name> does not exist. A new File Store with the name <filestore_name> will be created in NTFS security mode and then the share will be created. Do you wish to continue? Select q=quit y=yes n=no:
  
  Select q=quit y=yes n=no:""
  ```

The following list displays possible warnings when creating File Shares and the File Store already exists:
• **NFS/FTP/OBJ shares on File Store with NTFS security mode**

A warning message is displayed if the user tries to create an NFS/FTP/OBJ share on a File Store with security mode as **NTFS**. The clients accessing these shares are not allowed to perform permission changing operations.

- **NFS shares (If File Store is in NTFS mode)**

  "Warning: NFS share is being created on a NTFS mode File Store. Clients accessing this share will not be allowed to perform permission changing operations.
  Do you wish to continue?
  Select q=quit y=yes n=no:"

- **FTP shares (If File Store is in NTFS mode)**

  "Warning: FTP share is being created on a NTFS mode File Store. Clients accessing this share will not be allowed to perform permission changing operations.
  Do you wish to continue?
  Select q=quit y=yes n=no:"

- **OBJ shares (If File Store is in NTFS mode)**

  "Warning: OBJ share is being created on a NTFS mode File Store. Clients accessing this share will not be allowed to perform permission changing operations.
  Do you wish to continue?
  Select q=quit y=yes n=no:"

• **Cross-protocol access in Legacy mode**

When creating shares in a cross-protocol environment on a File Store in Legacy mode, a warning message is displayed. This warning is shown only when the user tries to create shares across different protocols on a File Store with Legacy Security mode.

The warning message is displayed as follows:

WARNING: Folders are allowed to be shared as writable for one protocol only and as read-only for all other protocols. For specific procedures on creating cross-protocol access shares, refer to Setup Guide for "HPE 3PAR File Persona in a Cross-Protocol Environment" at the location provided below. Configuring shares within the same File Store with write access for multiple protocols will result in unexpected behavior. Do you wish to continue? select q=quit y=yes n=no:"

---

**File Store Snapshots Overview**

**IMPORTANT:**

Snapshots of File Stores are not the same as snapshots of virtual volumes. File Store snapshots are Redirect-On-Write (ROW) instantaneous snapshots that are client accessible for single file or folder recovery and stored within the File Provisioning Group. Virtual Copy snapshots are used for administrators to recover entire FPGs and are not exposed to file sharing clients. There are 1024 snapshots supported per File Store.
Displaying File Store Snapshots

To display a list of snapshots of a File Store on a VFS, issue the following command:

```
showfsnap [-fpg <fpg_name>] [-vfs <vfs>] [-fstore <fstore>] [[-pat <pattern>] | [<snapname>]]
```

- **<fpg_name>**
  The FPG to which the VFS belongs. This option limits the display of snapshots to those associated with the specified FPG.

- **<vfs>**
  The VFS to which the File Store belongs. This option limits the snapshot output to those snapshots associated with the specified VFS name.

- **<fstore>**
  The name of the File Store for which you are displaying snapshots. This option limits the display to snapshots associated with the specified File Store name.

- **<pattern>|<snapname>**
  Displays the snapshots with names matching a glob-style pattern, or displays a specified snapshot. Use the -pat option with a given <pattern> value to specify a glob-style pattern or the <snapname> specifier to display a given snapshot by name. The -pat option must be used in order to specify patterns with the <pattern> value. Patterns can be repeated using a comma-separated list.

Creating File Store Snapshots

To create a snapshot of a File Store on a VFS, issue the following command:

```
createfsnap [-retain <retain_count>] [-f] [-fpg <fpg_name>] <vfs> <fstore> <tag>
```

where,

- **<retain_count>**
  The number of snapshots to retain for the specified File Store with the specified <tag>. Snapshots exceeding the count will be deleted beginning with the oldest snapshot. The valid range of snapshots to retain is from 1 to 1024. If the -retain option with a given <retain_count> value is included in the execution of the command and the count value for the specified tag has already been reached, the oldest snapshot is deleted before the new snapshot is created. If the command fails to create the new snapshot, the deleted snapshot will not be restored.

- **-f**
  Specifies not to ask for confirmation before creating a snapshot when retention count (<retain>). This option is ignored if option -retain is not specified.

- **<fpg_name>**
  The FPG to which the VFS belongs. If the FPG name is not specified, the command discovers the name based on the specified VFS name. If the VFS name exists in multiple FPGs, the FPG name must be specified.

- **<vfs>**
  The VFS to which the File Store belongs.

- **<fstore>**
  The File Store of which you are creating the snapshot.

- **<tag>**
  The suffix to be appended to the timestamp of snapshot creation to form a snapshot name in the format <timestamp>_<tag>. The timestamp is in ISO8601 date and time format. If snapshot1 is specified as the value of <tag>, the snapshot name will be, for example, 2015-12-17T215020_snapshot1.
Verify changes with the `showfsnap` command.

Creating a File Store snapshot using the SSMC:

- From the main menu, select **File Persona -> Virtual File Servers -> Actions -> Create File Snapshot**.
- Follow the instructions on the dialog that opens.

### Removing File Store Snapshots

To delete or remove a File Store snapshot from a VFS, issue the following command:

```
removefsnap [-f] [-fpg <fpg_name>] [-snapname <snapname>] <vfs> <fstore>
```

- **-f**
  Specifies not to ask for confirmation before removing a snapshot.
- **<fpg_name>**
  The FPG to which the VFS belongs. If the FPG name is not specified, the command discovers the name based on the specified VFS. If the VFS name exists in multiple FPGs, the FPG name must be specified.
- **[-snapname <snapname>]**
  The snapshot you are removing. If this is not specified, all snapshots of the File Store specified by `<fstore>` will be removed.
- **<vfs>**
  The VFS to which the File Store belongs.
- **<fstore>**
  The File Store of which you are removing the snapshot.

**NOTE:** If the name of the snapshot is not specified, all of the snapshots of the File Store are removed.

Verify changes with the `showfsnap` command. For more information about the `removefsnap` and `showfsnap` commands, see the **HPE 3PAR Command Line Interface Reference**.

You can also search for and delete snapshots with specific tag names using the SSMC to display matching snapshots in the **File Snapshots** detail pane of the **Virtual File Server** or **File Store** screens. You can then select the displayed snapshots and delete them.

### Recovering File Store Snapshots

Users can access snapshot copies by accessing the `.snapshot` directory from any folder within an NFS, SMB, FTP, or Object Access API File share. While the `ls -altr` command does not list the contents of the `.snapshot` from any arbitrary folder, it can be accessed by specifically navigating to it. From any arbitrary directory within the share, an explicit name-based lookup is necessary. Use commands such as `ls -altr .snapshot` or `cd .snapshot` to display the contents of the `.snapshot` directory.

When using the SMB protocol, access to snapshots under the `.snapshot` directory from any folder within the share will be denied and the following error will be displayed:

"<snap_name> is not accessible. <name of file> cannot be resolved by the system."

To recover a snapshot on any platform:
1. In the .snapshot directory, navigate to the folder with the date and time of the file or folder to recover.
2. Locate the file or folder to recover in the directory tree and copy it to the original directory.

If a file gets accidentally deleted, e.g. on path: /FPG1/VFS_X/FStore_Y/user_one/photos/, a snapshot of the file can be found using the .snapshot directory. E.g.: A snapshot created on October 1st 2014 - /FPG1/VFS_X/FStore_Y/.snapshot/Monday-10-01-2014/user_one/photos/.

NOTE:
The file name ".snapshot" is restricted. Users cannot create files or folders with this name.

File Store snapshots are read-only, moving files from a snapshot back to the original folder is not supported. Always use a copy operation when recovering files from a snapshot.

Displaying the Status of a Snapshot Space Reclamation Task

To display the status of a File Store snapshot reclamation task on an FPG, issue the following command:

```
showfsnapclean <fpg_name>
```

where,

- `<fpg_name>` specifies the name of the FPG for which the File Store snapshot reclamation status should be displayed.

The command displays active snap reclamation tasks as well as historical tasks that were completed or stopped earlier. It restricts the records to the last 20 to 22 tasks or maintains a history up to 30 days (whichever is a smaller set). For more information about the `stopfsnapclean` and `showfsnapclean` commands, see the HPE 3PAR Command Line Interface Reference.

Displaying the status of a snapshot space reclamation task using SSMC:

- From the main menu, select File Persona > File Provisioning Groups screen > Manage File Snapshots Reclaim Tasks.
- A list of file snapshot reclaim tasks is displayed.
- You can filter the list by entering text in the Search box. When filtered, the list shows only the items that contain the search text in the list columns.
- When you have completed your choices, click OK to start any action and close the dialog.

Stopping a Snapshot Space Reclamation Task

To stop or pause a File Store snapshot reclamation task for an FPG, issue the following command:

```
stopfsnapclean [-pause] <fpg_name>
```

where,

- `<fpg_name>` specifies the name of the FPG for which the File Store snapshot reclamation task will be paused or stopped.
- `-pause` specifies the snapshot space reclamation task is temporarily paused until it is started again. If this option is not specified, the snapshot space reclamation task is permanently stopped.

NOTE: Use the `startfsnapclean` command to resume a paused task.

View the status of a snapshot reclamation task with the `showfsnapclean` command. For more information about the `stopfsnapclean` and `showfsnapclean` commands, see the HPE 3PAR Command Line Interface Reference.
Stopping a snapshot space reclamation task using SSMC:

- From the main menu, select **File Persona > File Provisioning Groups screen > Manage File Snapshots Reclaim Tasks**.
- A list of file snapshot reclaim tasks is displayed.
- To specify that a running task is to be stopped, click **Stop**. In the **Task State** column, the state will change to **stop**.
- Click **OK** to start the stop action and close the dialog.

Reclaiming Storage Space from Deleted Snapshots

Use the `startfsnapclean` command to start a snapshot space reclamation task on an FPG. Any space from snapshots which are marked as deleted is reclaimed and made available to the FPG.

---

**NOTE:**

Only one snapshot space reclamation task can be run on an FPG at one time.

To reclaim space from deleted snapshots of a File Store, issue the following command:

```
startfsnapclean [-resume] [-reclaimStrategy {<maxspeed>|<maxspace>}] <fpg_name>
```

where,

- **<fpg_name>** specifies the name of the FPG from which the File Store snapshots will be removed.
- **-resume** starts a previously paused snapshot space reclamation task.

---

**NOTE:** Use the `stopfsnapclean` command to stop or pause a File Store snapshot reclamation task started with the `startfsnapclean` command.

- **-reclaimStrategy <maxspeed>|<maxspace>** specifies the strategy or preference for the reclamation task. The `<maxspeed>` option specifies the task is optimized for speed. The `<maxspace>` option specifies the task is optimized for reclaiming the maximum amount of space.

View the status of snapshot reclamation tasks with the `showfsnapclean` command. For more information about the `startfsnapclean` and `showfsnapclean` commands, see the **HPE 3PAR Command Line Interface Reference**.

Reclaiming Snapshot space from a File Provisioning Groups screen using SSMC:

- From the main menu, select **File Persona > File Provisioning Groups**.
- On the list pane, select the File Provisioning Group, and then select **Manage file snapshot reclaim tasks**, or **Reclaim file snapshot space** on the **Actions** menu.
- Follow the instructions on the dialog that opens.

Reclaiming file snapshot space from a Virtual File Servers screen using SSMC:

- From the main menu, select **File Persona > Virtual File Servers**.
- On the list pane, select the VFS, and then select **Reclaim file snapshot space** on the **Actions** menu.
- Follow the instructions on the dialog that opens.

Scheduling the Creation of File Store Snapshots

To schedule the creation of File Store snapshots, issue the following command:

```
createsched [options] <cmd> <taskschedule> <schedname>
```

---

Reclaiming Storage Space from Deleted Snapshots    71
where,

- **-run_once**
  The task will only run once at the specified time.
- **-no_alert**
  Specifies that the task will not generate alerts if the task fails
- **-f**
  Overwrites the preventive check for exceeding the recommended number of scheduled task starts per minute.
- **<cmd>**
  The CLI command or script that has been distributed by HPE 3PAR. For creating File Store snapshots use the command explained in Creating File Store Snapshots. Can be up to 127 characters in length
- **<taskschedule>**
  Specifies the use of the **crontab-style** schedule. Each field can be up to 127 characters in length.
- **<schedname>**
  specifies the name given to the schedule. The name can be up to 31 characters in length.
File Share

File Share Overview

File Shares are shared folders on a storage system that hold files which users and groups can access over a network.

File Persona offers four types of File Shares based on a defined NAS protocol: SMB, NFS, FTP and Object Access API; each one accessed using an appropriate network protocol. Each network protocol enables the client to access the files or directories stored in File Shares for that protocol type over the network. File Shares properties include share type (which defines the access protocol), share path, client filters list and share-level permissions. Each File Share has a share path that specifies the VFS, File Store and FPG upon which the File Share has been created. All File Shares offered by File Persona are managed through a common set of commands, with some unique parameters that are specific to the access protocol.

To interact with a File Share, a user must have the appropriate share permissions to be able to map/mount the File Share (from an SMB or NFS client). In File Persona, such permissions are referred to as share-level permissions (or in some interfaces simply share permissions) and are set on the File Share using the StoreServ Management Console (SSMC) or the HPE 3 PAR CLI `createshare` command when the File Share is created.

The share-level permissions are not part of the ownership and ACLs on files and folders. They are used to allow discretionary access, including access to the shared folder. Once the user has cleared the share-level permissions access check, the user has to clear the permission check of the folder at the root of the share to be able to access the shared folder. These permissions are referred as the share folder permissions throughout the user guide, and can be viewed using the `showfshare` (option: `-dirperm`) CLI command and modified using the `setfshare` CLI command (options: `-acl`, `-mode`, `-owner`, `-group`).

SMB File Share

The Server Message Block (SMB) protocol is a network file sharing protocol. The SMB protocol is the default protocol used by Windows clients.

SMB File Share Overview

File Persona supports SMB version 3.1.1, 3.0, 2.1, 2.0, and 1.0. The following SMB features are supported:

- SMB Transparent Failover across nodes in a node pair
  
  SMB Transparent Failover enables administrators to configure Windows file shares, in Windows Failover Clustering configurations, to be continuously available. Using continuously available file shares enables administrators to perform hardware or software maintenance on any file services node without interrupting the server applications that are storing their data files on these file shares.

- SMB Multi-Credit (Large MTU) Operations

  Larger MTU size significantly boosts the performance in large sequential transfers.

- Offloaded Data Transfer (ODX)

  ODX enables data transfers within without transferring the data through the client. It minimizes network bandwidth for file copies between two locations of a storage array. Offloaded data transfers are not persistent across failover operations. If a file copy using ODX is interrupted during a failover or an FPG is assigned to a new primary node the data transfer should be repeated.

File Persona does not support the following SMB 3.0 features:

- SMB multichannel
- SMB direct
Access-based Enumeration (ABE)

Access-based Enumeration (ABE) allows users to only see files and folders that they have access rights to on a SMB share. Administrators who want to control which files and folders are visible to a user may enable ABE at the share level.

For example, in a home directory use case, the administrator may enable ABE on a shared folder that contains home directories for multiple users so that the users who wish to access the shared folder will only see their own user folder and no other user's home directory.

Configuring Global SMB Settings

To configure various parameters related to the functionality of SMB in the context of File Persona, issue the following command:

```
setfs smb {smb-options}
```

where the various smb-options are listed below,

- **-enableoplocks {true | false}**
  Enables or disables opportunistic locks (oplocks) on SMB files. Default is true.
  For persistent handles to work correctly, options `enableoplocks` and `enablesmbleases` must be both enabled or both disabled.

- **-signingenabled {true | false}**
  Enables or disables SMB signing (security signatures). Default is true.

- **-signingrequired {true | false}**
  Specifies whether SMB signing is required or not. Default is false.

- **-ignorewritethroughrequests {true | false}**
  Specifies whether write-through requests are ignored or not. Default is true.

- **-supportpersistenthandles {true | false}**
  Enables or disables support for persistent file handles. Default is true.

- **-smb3dialectenable {true | false}**
  Enables or disables the SMB3 dialect. Default is true.

- **-enablesmb2ad {true | false}**
  Enables or disables SMB2 connections to Active Directory servers only. Default is true.

- **-enablesmbleases {true | false}**
  Specifies whether SMB leases are enabled or disabled. Default is true.
  For persistent handles to work correctly options `enablesmbleases` and `enableoplocks` must be both enabled or both disabled.

- **-enabledirleases {true | false}**
  Specifies whether or not directory leases are available to clients. Default is true.

- **-enablesmb2 {true | false}**
  Enables or disables SMB2 globally for client connections. Default is true.
NOTE:
In general, most of these settings can remain at their default settings. Only in special situations will these settings need to be tuned to a particular environment.

Multiple configuration options can be specified at the same time for the `setfs smb` command and at least one of the configuration options must be supplied to the command for it to execute. In addition to the configuration options, the command can be executed with the `-f` option to suppress confirmation to proceed.

⚠️ CAUTION:
Changing Global SMB Settings will result in a restart of the services and cause a temporary disruption in client access.

Managing SMB File Shares

Displaying SMB File Shares

To display an SMB File Share, issue the following command:

```
showfshare smb -dirperm [-fpg <fpgname>] -vfs <vfs> -fstore <fstorename> <sharename>
```

where,

- `smb` displays File Shares information for the SMB.
- `-d` displays shared attributes that are not displayed with other options. Shows details of all shares or a single share.
- `-dirperm` displays the share folder permissions: the ACL in the Converged ACL format, UNIX mode bit permissions, owner, and group information of the share directory. If this option is used, `-fstore` and `<sharename>` must also be specified.

NOTE:
To understand how permissions are translated to Windows and UNIX clients permission enforcement, see [Permission Conversion Rules: Converged ACL to/from POSIX ACLs](#).

- `-fpg <fpg_name>` specifies the FPG name. This limits the share output to those shares associated with the specified FPG.
- `-vfs <vfs>` specifies the VFS name. This limits the share output to those shares associated with the specified VFS. If this option is specified, but `-fpg` is not specified, the command will find out the FPG based on `<vfs>`. However, if `<vfs>` exists under multiple FPGs, `-fpg` must be specified.
- `-fstore <fstorename>` specifies the File Store name. This limits the share output to only those shares associated with the specified File Store. If this is specified, option `-vfs` must be specified.
- `-pat` specifies the File Share names using the glob-style pattern. Shares which have the name matching any of the specified glob-style patterns will be displayed. The `-pat` option can specify a list of patterns.
- `<pattern|sharename>`
displays only shares with names matching the specified <sharename> or one of the glob-style patterns.

Displaying File Share configuration using the SSMC:

- From the main menu, select File Persona.
- Select File Share.
- File Share screen displays a list of storage systems that have File Persona capabilities, detail views, and an Actions menu.

Creating SMB File Shares

NOTE: File shares can be created for multiple supported protocols. However, note that simultaneous write access from multiple protocols to the same File Share under a File Store in legacy security mode is not supported. Currently the default number of shares per node is 4000. However, this registry is tunable and can be changed by contacting HPE support.

To create an SMB File Share, issue the following command:

createfshare smb [options <arg>][-f] [-fpg <fpgname>] [-fstore <fstore>][-sharedir <sharedir>][-comment <comment>] <vfs> <sharename>

where,

- smb
  creates an SMB File Share.
- -f
  specifies that the command is forced. When creating a share for a secondary protocol type for a given File Store, if this option is not used, the command requires confirmation before proceeding with its operation.
- -fpg
  specifies the FPG that the <vfs> belongs to. If this is not specified, the command will determine whether the FPG is based on the specified <vfs>. However, if the <vfs> exists under multiple FPGs, then the -fpg must be specified.
- -fstore
  specifies the File Store under which the share will be created. If this is not specified, the command uses the <sharename> as the File Store name. The File Store will be created if it does not exist. In this case, the File Store that will be created depends on the type of File Share (i.e. if the share is SMB, the File Store will be created in NTFS security mode, otherwise legacy).
- -sharedir
  specifies the directory path to share. It can be a full path starting from "/", or a relative path under the File Store. If this is not specified, the share created will be rooted at the File Store. If a relative path is specified, option -fstore must be specified. If the directory path does not exist, it will be created.
- -comment
  specifies any comments or additional information for the share. The comment can be up to 255 characters long. Unprintable characters are not allowed.
- <vfs>
  specifies the VFS under which the File Store, if it does not exist, and the share will be created.
- <sharename>
  specifies the share name to be created.

Subcommand options

The list below provides the possible options for the createfshare command in relation to the SMB protocol:
createfshare smb [options <arg>]

- -abe {true|false}
  
  Access Based Enumeration

  specifies whether users can see or not see the files and directories to which they have been allowed
  access on the shares. The default is false.

- -allowip <iplist>
  
  specifies the client IP addresses that are allowed access to the share. Use commas to separate the IP
  addresses. The default is "", which allows all IP addresses (i.e. empty means all are allowed).

  Use net mask if range of the IP address needs to be specified. E.g.: 10.10.1.1/28

- -denyip <iplist>
  
  specifies the client IP addresses that are denied access to the share. Use commas to separate the IP
  addresses. The default is "", which denies none of IP addresses (i.e. empty means no one is denied).

  Use net mask if range of the IP addresses needs to be specified. E.g.: 10.10.1.1/28

- -allowperm <permlist>
  
  specifies share-level permissions to allow a user or a group a specific type of access: fullcontrol", 
  "read", or "change. The <permlist> must be specified in following format: <user1>:<perm1>, 
  <user2>:<perm2>,... . The <user> is a user, group name or Everyone. <perm> must be either 
  "fullcontrol", "read", or "change".

  NOTE:

  The allowperm option controls the share-level permissions. In addition, a user needs to have 
  access to the folder (share-folder permissions) associated with the share in order to be granted 
  access. Use the acl/mode/owner/group option in the setfshare command to control the folder 
  permissions.

  It is recommended to create the File Share with -allowperm Everyone:fullcontrol 
  permissions and then use the share-folder permissions per user.

- -denyperm <permlist>
  
  specifies share-level permissions to deny a user or group access to a share. the permission(s) that a user 
  or group is denied to access the share. <permlist> must be specified in the following format: 
  
  "<user1>:<perm1>,<user2>:<perm2>,... . The specification of <user> for deny permissions uses 
  the same rules as allow permissions shown above.

- -audit {operation1:value1[,operation2:value2]...}
  
  specifies the operations to be audited at share level for SMB protocol on specified VFS. The specified 
  operations can be modified and all the operations that are not specified will be set to their default values.
  The event can be audited based on operations such as: success, failure, none or all. The 
  operation/values are case insensitive. The following operations will generate events when:

  ° TreeConnect
    
    connect to a share. To create an audit record for a user trying to access a share that is not configured 
    on the VFS, use the following command:

    setfsaudit smb -audit Global:failure <vfs>.
  ° TreeDisconnect
    
    disconnect from a share. Note: Clients using SMB 1.0 may not trigger a TreeDisconnect event when 
    the client logs off.
  ° Open
    
    open/create a file or directory.
- Close
  close a file or directory.
- Rename
  rename a file or directory.
- Delete
  delete a file or directory.
- Read
  read from a file. Only the first read is reported once the file opens.
- Write
  write to a file. Only the first write is reported once the file opens.
- ChangeSecurity
  change the security attributes.
- `-cache {off|manual|optimized|auto}`
  specifies client-side caching for offline files. Valid values are:
  - off
    The client must not cache any files from this share. The share is configured to disallow caching.
  - manual
    The client must allow only manual caching for the files open from this share.
  - optimized
    The client may cache every file that it opens from this share. Also, the client may satisfy the file requests from its local cache. The share is configured to allow automatic caching of programs and documents.
  - auto
    The client may cache every file that it opens from this share. The share is configured to allow automatic caching of documents. If this is not specified, the default is "manual".
- `-ca {true|false}`
  specifies whether the SMB continuous availability feature should be enabled for this share. If nothing is specified, the default is "true". If the continuous availability feature is enabled transparent migration of shares is permitted between nodes during software upgrades, or when migrating an FPG between the nodes of a node pair. There is some performance impact when having this feature enabled due to write caching being disabled for the share.

**NOTE:**

This option is applicable only to SMB 3.0.

If an SMB share is created with invalid characters like * / \ | < > : ’ ” [ ] ; , = @ or a trailing ? in the share’s name then the share creation will not be permitted. An error message "ERROR_UNSUPPORTED_CHARACTER_IN_SHARENAME" will be generated.

Creating File Shares Using SSMC

Using the SSMC, open File Persona screens and select the File Shares screen to create and manage one or more File Shares on each of the VFSs. You can also open the File Stores screen or the Virtual File Servers screen and select Create File Share.

Creating a File Share from a File Shares screen
• From the main menu, select **File Persona > File Shares**.
• Click **+ Create File Share** or select **Create** on the **Actions** menu.
• Follow the instructions on the dialog that opens.

**Creating a File Share from a Virtual File Servers screen**
• From the main menu, select **File Persona > File Shares**.
• Click **Create File Share**.
• Follow the instructions on the dialog that opens.

### Removing SMB File Shares

**To remove an SMB File Share**, issue the following command:

```
removefshare smb [-f] [-fpg <fpgname>] [-fstore <fstore>] <vfs> <sharename>
```

where,
- **smb** removes an SMB File Share.
- **-f** option specifies that the command is forced. If this option is not used, the command requires confirmation before proceeding with its operation.
- **-fpg <fpg_name>** option specifies the FPG that <vfs> belongs. If this is not specified, the command will find out the FPG based on the specified <vfs>. However, if <vfs> exists under multiple FPGs, -fpg must be specified.
- **-fstore <fstore>** option specifies the File Store that the File Share to be removed belongs. If this is not specified, the <sharename> will be used as -fstore.
- **<vfs>** specifies the VFS name.
- **<sharename>** specifies the name of the share to be removed.

**NOTE:**
Removing a File Share only removes access to files and folders. It does not physically remove any files or folders.

**Removing a File Share using SSMC**
• From the main menu, select **File Persona > File Shares**.
• Select the File Share you want to delete, and then select the **Actions** menu.
• Select **Delete**

### Modifying SMB File Shares

**To modify an SMB File Share**, issue the following command:

```
```

where,
- **smb**
sets the File Share options for the SMB protocol.

- `acl [+|-]<permlist>`

specifies the access control list (ACL) permissions that are allowed on a share directory. This option cannot be used when `mode` is used. If the ACL permissions are set improperly, the cross-protocol functionality can break and may cause loss of mode bits information. A warning prompt is displayed to the users asking if they wish to proceed.

**IMPORTANT:**

This is the system Converged ACL. To understand how these permissions are translated to Windows and UNIX clients permission enforcement, see [Permission Conversion Rules for Converged ACLs](#) on page 123.

The `acl` option is provided primarily for the NTFS security mode. In the Legacy security mode, if the File Store is being used in a cross-protocol environment and the NFS clients are configured as read/write clients (SMB clients are read-only), it is recommended that do not use the `acl` option to change permissions of the share folder. Use the `mode` option instead.

The ACL in the share folder permissions that are created by default (by inheritance from the File Store directory) in the NTFS security mode are more restrictive than the default ACLs in the share folders in the Legacy security mode. Use the `showfshare -dirperm` CLI command to view the given ACL, and the `setfshare -acl` CLI command in the NTFS security mode to change the share folder ACL.

The values for `<permlist>` fields `type:flag:principal:permissions` are as follows:

**type**

The `type` field can take only one of the following values:

- `A` -allow
- `D` -deny
- `U` -audit
- `L` -alarm

**flag**

The `flag` field is optional and can take one or more of the following values:

- `f` -file-inherit
- `d` -directory-inherit
- `p` -no-propagate-inherit
- `i` -inherit-only
- `S` -successful-access
- `F`
- failed-access
  - g
    - group (denotes that <principal> is a group)

principal
The principal field can be any named user or group or one of the following values:
  - OWNER@
  - GROUP@
  - EVERYONE@

permissions
The permissions field can take one or more of the following values:
  - r
    - read-data | list-directory
  - w
    - write-data | create-file
  - a
    - append-data | create-subdirectory
  - x
    - execute
  - d
    - delete
  - D
    - delete-child (directories only)
  - t
    - read-attrs
  - T
    - write-attrs
  - n
    - read-named-attrs
  - N
    - write-named-attrs
  - c
    - read-ACL
  - C
    - write-ACL
  - o
    - write-owner
  - y
    - synchronize

If specified, the prefix will be applied to the entire <permlist>. If <permlist> has no prefix, the information will be used to create a <permlist>. The <permlist> contains the list of Access Control Entries (ACEs). Use commas to separate ACEs. Each ACE contains four values named type, flag,
principal, and permissions. Separate the four values with a ":". The format of the ACE corresponds to the
NFSv4 ACL format. See Linux NFS4_acl (5) man page for additional information.

Example:
A:fd:OWNER@:rwx,A:fdg:GROUP@:rwax

If <permlist> has a prefix;

Example: +A:fd:OWNER@:rwa,A:g:GROUP@:rwxa

◦ If + or - is not specified: The entire ACL on the file object is replaced with the specified <permlist>. The
  order specified will be maintained. There will be no checks for duplicate ACEs (that is, duplicates
  are allowed).
◦ If + prefix is specified: -acl +<permlist> The new <permlist> is inserted at the head of the
  existing ACL, in the same order as specified. There will be no checks for duplicate ACEs (that is,
  duplicates are allowed).
◦ If - is specified: -acl -<permlist> For each ACE in the specified <permlist>, the current ACL
  will be searched, in an order, until the first entry that matches is found. The first matching entry will be
  removed. If no matching ACE is found, the action will fail.

• -mode <modebits>
specifies the <modebits> permissions that are allowed on a share directory. This option cannot be used
when -acl is used. Setting mode bits may break cross-protocol functionality if used improperly, and may
cause loss of ACL information. A warning prompt is displayed to the users asking if they wish to proceed.

**NOTE:**

The -acl, -mode, -user, and -group options can be used to ensure that the resulting settings are
appropriate for the protocol through which file writes and directory creations are going to occur. In the
Legacy security mode, the -acl option should be used for shares with SMB-based writers and the -mode option
should be used with NFS/FTP/OBJ-based writers. In the NTFS security mode, the -acl options should be used. The -mode option is not allowed as it is allowed only in the legacy security mode.

• -f

specifies that the command is forced. When setting ACL permissions or mode bits of a share directory, if
this option is not used, the command requires confirmation before proceeding with its operation.

• -owner <name>
specifies the name of the owner to whom the share directory belongs. The format of <name> is the same
as with the allowperm option above.

**NOTE:**

In the NTFS security mode when the owner is changed, the new owner does not get any
permissions. An ACE has to exist for the new owner and if it does not exist it has to be created. Any
previous OWNER@ ACES in the converged ACL will become named ACES for the previous owner.
If the owner is changed, and the user wants the owner to have permissions (assuming the new
owner does not have any preassigned ACE), then the user has to assign the new owner an ACE
with the desired permissions. Execute the setfshare -acl command on the ACE.

• -group <name>
specifies the name of the group to which the share directory belongs. The format of <name> is the same
as with the allowperm option above.
NOTE:

In the NTFS security mode when the group is changed, the new group does not get any permissions. An ACE has to exist for the new group and if it does not exist it has to be created. Any previous GROUP@ ACES in the converged ACL will become named ACES for the previous group. If the group is changed, and the user wants the group to have permissions (assuming the new group does not have any preassigned ACE), then the user has to assign the new group an ACE with the desired permissions. Execute the setfshare -acl command on the ACE.

• -audit {[operation1:value1[,operation2:value2]]...}

  specifies the operations to be audited on a share level for the SMB protocol. The specified operations will be audited and all the operations that are not specified will be set to their default values. All the operations will be audited based on the outcome of the operations: success, failure, none and all. If the -audit option is set to "" all operations will be set to none. All the possible operations are mentioned in the table below:

<table>
<thead>
<tr>
<th>SMB Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>TreeConnect</td>
</tr>
<tr>
<td>TreeDisconnect</td>
</tr>
<tr>
<td>Open</td>
</tr>
<tr>
<td>Close</td>
</tr>
<tr>
<td>ChangeSecurity</td>
</tr>
<tr>
<td>Read</td>
</tr>
<tr>
<td>Write</td>
</tr>
<tr>
<td>Delete</td>
</tr>
<tr>
<td>Rename</td>
</tr>
</tbody>
</table>

• -fpg <fpiname>

  specifies the FPG to which <vfs> belongs. If this option is not specified, the command will find out the FPG based on the specified <vfs>. However, if <vfs> exists under multiple FPGs, -fpg must be specified.

• -fstore <fstore>

  specifies the File Store that the share to be modified belongs. If this is not specified, the <sharename> will be used as the File Store name to identify the share.

• -comment <comment>

  specifies any comments or additional information for the share. The comment can be up to 256 characters long. Unprintable characters are not allowed.

• <sharename>

  specifies the File Share.

File Share Options for SMB protocol

The following options are specific to the setfshare smb [options <arg>] subcommand:

• -abe {true|false}

  Access Based Enumeration. Specifies if users can see only the files and directories to which they have been allowed access on the shares.

• -allowip [+]<iplist>

• -denyip [+]<iplist>
specifies client IP addresses that are allowed access to the share. Use commas to separate the IP addresses. If <iplist> has a prefix (for example: +1.1.1.0, 2.2.2.0), the meaning is as follows:

- +
  adds <iplist> to the existing allowed list. The IP addresses in <iplist> must not already be in the existing allowed list.
- –
  removes <iplist> from the existing allowed list. The IP addresses in <iplist> must be in the existing allowed list.

If specified, the prefix will be applied to the entire <iplist>. If <iplist> has no prefix, <iplist> will be used to create the new allowed list.

- denyip [+|-]<iplist>

specifies client IP addresses that are denied access to the share. Use commas to separate the IP addresses. If <iplist> has a prefix (for example: +1.1.1.0, 2.2.2.0), the meaning is as follows:

- +
  adds <iplist> to the existing denied list. The IP addresses in <iplist> must not already be in the existing denied list.
- –
  removes <iplist> from the existing denied list. The IP addresses in <iplist> must be in the existing denied list.

If specified, the prefix will be applied to the entire <iplist>. If <iplist> has no prefix, <iplist> will be used to create the new denied list.

- allowperm [+|-|=]<permlist>

specifies the share-level permissions for user or groups. <permlist> must be specified in the format of: "<user1>:<perm1>,<user2>:<perm2>,...". The <user> can be a user, group name, or Everyone specified using the same format as described in createfshare. <perm> must be "fullcontrol", "read", or "change". If <permlist> has a prefix (for example: +Everyone:read), the meaning is as follows:

- +
  adds <permlist> to the existing allowed list. Users/groups in <permlist> must not already be in the existing allowed list.
- –
  removes <permlist> from the existing allowed list. Users/groups in <permlist> must be in the existing allowed list.
- =
  modifies the existing allowed list with <permlist>. Users/groups in <permlist> must already be in the existing allowed list.

If specified, the prefix will be applied to the entire <permlist>. If <permlist> has no prefix, <permlist> will be used to create the new allowed list.

- denyperm [+|-|=]<permlist>

specifies the share-level permissions for user or groups. <permlist> must be specified in the format of: "<user1>:<perm1>,<user2>:<perm2>,...". The <user> can be a user, group name, or Everyone specified using the same format as described in createfshare. <perm> must be "fullcontrol", "read", or "change". If <permlist> has a prefix (for example: +Everyone:read), the meaning is as follows:

- +
  adds <permlist> to the existing denied list. Users/groups in <permlist> must not already be in the existing denied list.
- –
  removes <permlist> from the existing denied list. Users/groups in <permlist> must be in the existing denied list.
adds `<permlist>` to the existing denied list. Users/groups in `<permlist>` must not already be in the existing denied list.

- `=` removes `<permlist>` from the existing denied list. Users/groups in `<permlist>` must be in the existing denied list.

- `-` modifies the existing denied list with `<permlist>`. Users/groups set in `<permlist>` must already be in the existing denied list.

If specified, the prefix will be applied to the entire `<permlist>`. If `<permlist>` has no prefix, `<permlist>` will be used to create the new denied list. `-cache {off|manual|optimized|auto}` specifies client-side caching for offline files. Valid values are:

- `off`   
The client must not cache any files from this share. The share is configured to disallow caching.

- `manual`   
The client must specify the files and folders that need to be cached manually to be accessed from this share (available offline).

- `optimized`   
The client may cache every file that it opens from this share. Also, the client may satisfy the file requests from its local cache. The share is configured to allow automatic caching of programs and documents.

- `auto`   
The client may cache every file that it opens from this share. The share is configured to allow automatic caching of documents.

- `-ca {true|false}`   
specifies if SMB3 continuous availability features should be enabled for this share.

### Modifying Configuration Settings for File Shares using SSMC

SSMC can be used to specify the properties and settings of File Shares on a storage system. The File Share name, share type (SMB in this case), share path (parent File Store and VFS), and additional settings such as client filters and access permissions can be specified. To configure access settings for a File Share, complete the following steps:

- From the main menu, select **File Persona > File Shares**.
- Do one of the following:
  - Click **+ Create File Share** or select **Create** on the **Actions** menu.
  - On the list pane, select the **File Share**, and then select **Edit** or **Delete** on the **Actions** menu.
- Follow the instructions on the dialog that opens.

### NFS File Share

The **Network File System** (NFS) is a client/server application that lets a computer user view and optionally store and update files on a remote computer as though they were on the user's own computer. The NFS protocol is one of the several distributed file system standards for network-attached storage (NAS). The NFS protocol is the default protocol used by UNIX/Linux clients. File Persona supports NFSv4 and NFSv3, and supports a variety of Linux/UNIX operating systems.

For more information about client interoperability, see the SPOCK website: [SPOCK](http://www.hpe.com/storage/spock)
NFS File Share Overview

File Persona supports the following NFS features:

- Failover across nodes in a node pair
- AUTH SYS authentication
- POSIX ACL enforcement

NFS Export Options

File Persona supports the following NFS export options:

<table>
<thead>
<tr>
<th>Export Options</th>
<th>Recommended Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ro/rw</td>
<td>rw</td>
<td>&quot;rw&quot; option allows the remote client to modify the exported file system. To disallow changes to the exported file system, use read-only(&quot;ro&quot;) option. If none given, it defaults to &quot;ro&quot;.</td>
</tr>
<tr>
<td>secure/insecure</td>
<td>secure</td>
<td>&quot;secure&quot; option grants access to client request only if they had originated form secured internet ports 1 - 1024. To clear this option, specify &quot;insecure&quot;. By default, &quot;secure&quot; option is chosen.</td>
</tr>
<tr>
<td>sync/async</td>
<td>sync</td>
<td>If &quot;sync&quot; option is enabled, nafs server replies to client only after the changes made by the request have been committed to stable storage. To allow nafs serve to reply requests before committing the changes to stable storage, specify &quot;async&quot; option&quot;. If none given, it defaults to &quot;sync&quot;. **We would strongly recommend NOT to use &quot;async&quot; option as it would lead to data loss and corruption.</td>
</tr>
<tr>
<td>hide/nohide</td>
<td>hide</td>
<td>If nafs server exports two file system one of which is mounted on the other, specifying &quot;hide&quot; option makes the nafs client to mount both the file system explicitly to get access to them. To turn off this feature, specify &quot;nohide&quot; option which makes the nafs client to get access to both parent and child file system by mounting just the parent file system. By default, &quot;hide&quot; is chosen. This &quot;hide&quot; option does not apply to NFS V4. In NFS v4, any file system that is exported is visible to clients.</td>
</tr>
<tr>
<td>crossmnt/</td>
<td>crossmnt</td>
<td>When there is a file system mounted on another file system, using &quot;crossmnt&quot; option, nafs client can access both parent and child file system by just mounting the parent file system. And, the nafs server need not want to export the child file system explicitly. &quot;nocrossmnt&quot; disables this function. By default, &quot;crossmnt&quot; option is chosen.</td>
</tr>
<tr>
<td>nocrossmnt</td>
<td></td>
<td></td>
</tr>
<tr>
<td>wdelay/no_wdelay</td>
<td>wdelay</td>
<td>&quot;wdelay&quot; makes the nafs server to delay committing write requests to stable storage, if it anticipates that another related write request is in progress. To make the nafs server not to wait, specify &quot;no_wdelay&quot;. Default option is &quot;wdelay&quot;. **This option does not apply to NFS V3 &amp; V4 protocol; applies only to NFS V2 protocol.</td>
</tr>
</tbody>
</table>

Table Continued
<table>
<thead>
<tr>
<th>Feature</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>root_squash/ all_squash</td>
<td>root_squash</td>
<td>&quot;root_squash&quot; prevents the NFS client root user from having root privileges on an NFS exported file system by mapping remote root user's uid and gid to anonymous user's uid and gid. To provide root privileges to NFS client root user, specify &quot;no_root_squash&quot;. &quot;no_root_squash&quot; option is not allowed in NTFS security mode enabled file store. If none given, it defaults to &quot;root_squash&quot;.</td>
</tr>
<tr>
<td>no_root_squash/ no_all_squash</td>
<td>no_all_squash</td>
<td>&quot;all_squash&quot; options maps all the remote users uid and gid to anonymous user's uid and gid. To turn this off feature, specify &quot;no_all_squash&quot;. Default option is &quot;no_all_squash&quot;.</td>
</tr>
<tr>
<td>subtree_check/ no_subtree_check</td>
<td>subtree_check</td>
<td>&quot;no_subtree_check&quot; option verifies if the requested file is in the exported subdirectory's file system. In &quot;subtree_check&quot; option, it does the same thing as &quot;no_subtree_check&quot;. Additionally it also checks whether the accessed file is in exported subdirectory of a file system. Default is &quot;subtree_check&quot; <strong>no_subtree_check is NOT supported in File Persona</strong></td>
</tr>
</tbody>
</table>

**Managing NFS File Shares**

**Displaying NFS File Shares**

To display an NFS File Share, issue the following command:

```bash
showfshare nfs -dirperm [-fpg <fpgname>] -vfs <vfs> -fstore <fstorename> <sharename>
```

where,

- `nfs`  
  displays File Shares information for NFS.
- `-d`  
  option shows share attributes that are not displayed by other options. Shows details of all shares or a single share
- `-dirperm`  
  displays the share folder permissions: ACL in Converged ACL format, Unix mode bits permissions, owner, and group information of the share directory. If this option is used, `-fstore` and `<sharename>` must also be specified.

**NOTE:**

This is the system Converged ACL. To understand how these permissions are translated to Windows and UNIX client permission-enforcement, please see Permission Conversion Rules: Converged ACL to/from POSIX ACLs.

- `-fpg <fpg_name>`  
  specifies the FPG name. This limits the share output to those shares associated with the specified FPG.
- **-vfs <vfs>**
  specifies the VFS name. This limits the share output to those shares associated with the specified VFS. If this option is specified, but -fpg is not specified, the command will find out the FPG based on<vfs>. However, if <vfs> exists under multiple FPGs, -fpg must be specified.

- **-fstore <fstorename>**
  specifies the File Store name. This limits the share output to only those shares associated with the specified File Store. If this is specified, option -vfs must be specified.

- **-pat**
  specifies the File Share names using the glob-style pattern. Shares which have the name matching any of the specified glob-style patterns will be displayed. The -pat option can specify a list of patterns.

- **<pattern|sharename>**
  displays only shares with names matching the specified <sharename> or one of the glob-style patterns.

**Displaying File Share configuration using the SSMC:**
- From the main menu, select File Persona.
- Select File Share.
- File Share screen displays a list of storage systems that have File Persona capabilities, detail views, and an Actions menu.

### Creating NFS File Shares

**NOTE:** File shares can be created for multiple supported protocols. However, please note that simultaneous write access from multiple protocols to the same File Share under a File Store in legacy security mode is not supported. Currently the default number of shares per node is 4000. However, this registry is tunable and can be changed by contacting HPE support.

To create an NFS File Share, issue the following command:

```
```

where,

- **nfs**
  creates an NFS File Share

- **-f**
  specifies that the command is forced. When creating a share for a secondary protocol type for a given File Store, if this option is not used, the command requires confirmation before proceeding with its operation.

- **-fpg**
  specifies the FPG the <vfs> belongs to. If this is not specified, the command will determine the FPG based on the specified <vfs>. However, if the <vfs> exists under multiple FPGs, the -fpg must be specified.

- **-fstore**
  specifies the File Store under which the share will be created. If this is not specified, the command uses the <sharename> as the File Store name. The File Store will be created if it does not exist. In this case, the File Store that will be created will depend on the type of File Share.

- **-sharedir**
  specifies the directory path to share. It can be a full path starting from "/", or a relative path under the File Store. If this is not specified, the share created will be rooted at the File Store. If a relative path is specified, option -fstore must be specified. If the directory path does not exist, it will be created.

- **-comment**
specifies any comments or additional information for the share. The comment can be up to 255 characters long. Unprintable characters are not allowed.

- `<vfs>`
  specifies the VFS under which the File Store, if it does not exist, and the share will be created.

- `<sharename>`
  specifies the share name to be created.

**Subcommand options**

The following options are specific to the `NFS` subcommand:

```
createfshare nfs[options <arg>]
```

- `-options <options>`
  specifies options to use for the share to be created. Standard NFS export options except "no_subtree_check" are supported. Do not enter option "fsid", which is provided. If not specified, the following options will be automatically set: `sync`, `auth_nlm`, `wdelay`, `sec=sys`, `no_all_squash`, `crossmnt`, `secure`, `subtree_check`, `hide`, `root_squash`, `ro`. Visit section **NFS Export Options** to view the export options in detail.

  The various File Access Auditing options are as follows: `audit_open`, `audit_close`, `audit_meta`, `audit_attr`, `audit_read`, `audit_audit_write`. Visit section **File Access Auditing Framework** to view the File Access Auditing options in detail.

- `-clientip <clientlist>`
  specifies the clients that can access the share. The NFS client can be specified in three ways:
  - Name
    Example: `sys1.hpe.com`
  - Name with a wildcard
    Example: `*.hpe.com`
  - IP address. Use comma to separate the IP addresses. If this is not specified, the default is "**"

  When restricting access to domain NFS shares, a fully qualified domain name (FQDN) of the host has to be specified. If the wildcard option is used when specifying the client IP there might be an issue. Reverse lookup needs to be setup to allow clients on the domain access to mount the share. When configuring Reverse lookup configure the FQDN and not an alias.

  Example:

  ```
sys1.hpe.com
Do not use aliases: sys1
Use net mask if range of the IP address needs to be specified. E.g.: 10.10.1.1/28
```

**File Naming Convention for NFS Shares**

On HPE 3PAR OS 3.2.1 or later versions using File Persona, the customer’s file name should be compatible with all network clients from where access to the file or directory on File Persona controller is planned. The use of special characters or characters that cannot be displayed may make file access difficult. File Persona supports the use of any encoded character in the file name, except for NUL (0x00).

For example, in a cross-protocol environment, a UNIX network client can create a file or directory with a name that has a “space” (0x20) as the last character in the file name but a Microsoft (MS) Windows network client will have difficulty accessing the file because it does not support use of a “space” as the last character of a file or directory name; the “space” character is truncated by the MS Windows commands.
IMPORTANT:
HPE recommends that the customer uses a POSIX portable file name character set in the file naming convention.

The POSIX portable file name character set is as follows:
• Uppercase A to Z
• Lowercase a to z
• Numbers 0 to 9
• Period (.)
• Underscore (_)
• Hyphen (-)

Creating File Shares Using SSMC

Using the SSMC, open File Persona screens and select the File Shares screen to create and manage one or more File Shares on each of the VFSs. You can also open the File Stores screen or the Virtual File Servers screen and select Create File Share.

Creating a File Share from a File Shares screen
• From the main menu, select File Persona > File Shares.
• Click + Create File Share or select Create on the Actions menu.
• Follow the instructions on the dialog that opens.

Creating a File Share from a Virtual File Servers screen
• From the main menu, select File Persona > Virtual File Servers.
• Click Create File Share.
• Follow the instructions on the dialog that opens.

Removing NFS File Shares

To remove an NFS File Share, issue the following command:

```
removefshare nfs [-f] [-fpg <fpgname>] [-fstore <fstore>] <vfs> <sharename>
```

where,
• nfs
  removes an NFS File Share.
• -f
  option specifies that the command is forced. If this option is not used, the command requires confirmation before proceeding with its operation.
• -fpg <fpg_name>
  option specifies the FPG that <vfs> belongs. If this is not specified, the command will find out the FPG based on the specified <vfs>. However, if <vfs> exists under multiple FPGs, -fpg must be specified.
• -fstore <fstore>
  option specifies the File Store that the File Share to be removed belongs. If this is not specified, the <sharename> will be used as -fstore.
• <vfs>
  specifies the VFS name.
• <sharename>
  specifies the name of the share to be removed.
NOTE:
Removing a File Share only removes access to files and folders. It does not physically remove any files or folders.

Removing a File Share using SSMC

- From the main menu, select File Persona > File Shares.
- Select the File Share you want to delete, and then select the Actions menu.
- Select Delete

Modifying NFS File Shares

To modify NFS File Share settings, issue the following command:

```bash
```

where,
- `nfs`
  sets File Share options for NFS protocol.
- `+ acl [+|-]<permlist>`
  specifies the access control list (ACL) permissions that are allowed on a share directory. This option cannot be used when `-mode` is used. Setting ACL permissions can break cross-protocol functionality if used improperly, and may cause loss of mode bits information. A warning prompt is displayed to the users asking if they wish to proceed.

**IMPORTANT:**
This is the system CONVERGED ACL. To understand how these permissions are translated to Windows and UNIX clients permission-enforcement, see Permission Conversion Rules for Converged ACLs on page 123.

The `-acl` option is provided primarily for the NTFS security mode. In the Legacy security mode, if the File Store is being used in a cross-protocol environment and the NFS clients are configured as read/write clients (SMB clients are read-only), it is recommended that do not use the `-acl` option to change permissions of the share folder. Use the `-mode` option instead.

The ACL in the share folder permissions that are created by default (by inheritance from the File Store directory) in the NTFS security mode are more restrictive than the default ACLs in the share folders in the Legacy security mode. Use the `showfshare -dirperm` CLI command to view the given ACL, and the `setfshare -acl` CLI command in the NTFS security mode to change the share folder ACL.

The values for `<permlist>` fields type:flag:principal:permissions is as follows:

**type**

The `type` field can take only one of the following values:

- A
  -allow
- D
  -deny
- U
The flag field is optional and can take one or more of the following values:

- f
  - file-inherit
- d
  - directory-inherit
- p
  - no-propagate-inherit
- i
  - inherit-only
- S
  - successful-access
- F
  - failed-access
- g
  - group (denotes that $<$principal$>$ is a group)

The principal field can be any named user or group or one of the following values:

- OWNER@
- GROUP@
- EVERYONE@

The permissions field can take one or more of the following values:

- r
  - read-data | list-directory
- w
  - write-data | create-file
- a
  - append-data | create-subdirectory
- x
  - execute
- d
  - delete
- D
  - delete-child (directories only)
- t
  - read-attrs
- T
-write-attrs
  ◦ n
-read-named-attrs
  ◦ N
-write-named-attrs
  ◦ c
-read-ACL
  ◦ C
-write-ACL
  ◦ o
-write-owner
  ◦ y
-synchronize

If specified, the prefix will be applied to the entire <permlist>. If <permlist> has no prefix, the information will be used to create a permlist. The <permlist> contains the list of Access Control Entries (ACEs). Use commas to separate ACEs. Each ACE contains four values named type, flag, principal, and permissions. These four values should be separated by a ".". The format of the ACE corresponds to the NFSv4 ACL format. See LINUX NFS4_acl (5) man page for additional information.

Example:
A:fd:OWNER@:rwax,A:fdg:GROUP@:rwax

If <permlist> has a prefix;
Example: +A:fd:OWNER@:rwa,A:gd:GROUP@:rwx

◦ If + or – is not specified: The entire ACL on the file object is replaced with the specified <permlist>. The order specified will be maintained. There will be no checks for duplicate ACEs (that is, duplicates are allowed)
◦ If + prefix is specified: -acl +<permlist> The new <permlist> is inserted at the head of the existing ACL, in the same order as specified. There will be no checks for duplicate ACEs (that is, duplicates are allowed).
◦ If – is specified: -acl -<permlist> For each ACE in the specified <permlist>, the current ACL will be searched, in an order, until the first entry that matches is found. The first matching entry will be removed. If no matching ACE is found, the action will fail.

• -mode <modebits>

specifies the -mode permissions that are allowed on a share directory. This option cannot be used when -acl is used. Setting mode bits may break cross-protocol functionality if used improperly, and may cause loss of ACL information. A warning prompt is displayed to the users asking if they wish to proceed.

**NOTE:**

Use the -acl, -mode, -user, and -group options carefully as each option is specific to the protocol through which the file writes and directory creations are going to occur. Use the -acl option in the Legacy security mode for SMB-based shares and the -mode option for NFS/FTP/OBJ based shares. The -mode option is allowed only in Legacy security mode, not in NTFS security mode.

• -f

specifies that the command is forced. When setting ACL permissions or mode bits of a share directory, if this option is not used, the command requires confirmation before proceeding with its operation.

• -owner <name>
specifies the name of the owner to whom the share directory belongs. The format of \texttt{<name> is the same as with the allowperm option above.}

\textbf{NOTE:}

In the NTFS security mode when the owner is changed, the new owner does not get any permissions. An ACE has to exist for the new owner and if it does not exist it has to be created. Any previous OWNER@ ACES in the converged ACL will become named ACES for the previous owner. If the owner is changed, and the user wants the owner to have permissions (assuming the new owner does not have any preassigned ACE), then the user has to assign the new owner an ACE with the desired permissions. Execute the \texttt{setfshare -acl} command on the ACE.

In the NTFS security mode, when the owner is changed, the new owner does not get any permissions.

- \texttt{-group <name>}

specifies the name of the group to which the share directory belongs. The format of \texttt{<name> is the same as with the allowperm option above.}

\textbf{NOTE:}

In the NTFS security mode when the group is changed, the new group does not get any permissions. An ACE has to exist for the new group and if it does not exist it has to be created. Any previous GROUP@ ACES in the converged ACL will become named ACES for the previous group. If the group is changed, and the user wants the group to have permissions (assuming the new group does not have any preassigned ACE), then the user has to assign the new group an ACE with the desired permissions. Execute the \texttt{setfshare -acl} command on the ACE.

In the NTFS security mode, when the group is changed, the new group does not get any permissions.

- \texttt{-fpg <fpgname>}

 specifies the FPG to which \texttt{<vfs>} belongs. If this option is not specified, the command will find out the FPG based on the specified \texttt{<vfs>}. However, if \texttt{<vfs>} exists under multiple FPGs, \texttt{-fpg} must be specified.

- \texttt{-fstore <fstore>}

 specifies the File Store that the share to be modified belongs. If this is not specified, the \texttt{<sharename>} will be used as the File Store name to identify the share.

- \texttt{-comment <comment>}

 specifies any comments or additional information for the share. The comment can be up to 256 characters long. Unprintable characters are not allowed.

- \texttt{<sharename>}

 specifies the File Share.

\textbf{File Share Options for NFS protocol}

The following options are specific to the \texttt{setfshare nfs [options <arg>} subcommand:

- \texttt{-options}

 specifies the new options to use for the File Share. This overwrites all the options set previously. Standard NFS export options except \texttt{"no_subtree_check"} are supported. Do not enter option \texttt{"fsid"}, which is provided. If not specified, the following options will be automatically set: \texttt{sync, auth_nlm, wdelay, sec=sys, no_all_squash, crossmnt, secure, subtree_check, hide, root_squash, ro.}

In addition to the options above, File Access Auditing operations are also supported for the NFS protocol. The operations will generate events when:
<table>
<thead>
<tr>
<th>NFS operation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>audit_open</td>
<td>Audit event is generated when a file is opened. This applies to NFSv4 only.</td>
</tr>
<tr>
<td>audit_close</td>
<td>Audit event is generated when a file is closed. This applies to NFSv4 only.</td>
</tr>
<tr>
<td>audit_meta</td>
<td>Audit event is generated when a file is created, removed, or a file or a directory is renamed.</td>
</tr>
<tr>
<td>audit_attr</td>
<td>Audit event is generated when file/directory attributes are changed.</td>
</tr>
<tr>
<td>audit_read</td>
<td>Audit event is generated when a file is read. Subsequent file reads are suppressed for a specific time (currently 10 minutes).</td>
</tr>
</tbody>
</table>
|               | **NOTE:**
|               | Reads from a directory are never suppressed. |
| audit_write   | Audit event is generated when a file is written. Subsequent writes are suppressed for a specific time (currently 10 minutes). |

- `-clientip [+|-]<iplist>`

  specifies the clients that can access the share. The NFS client can be specified by the name (for example, sys1.hpe.com), the name with a wildcard (for example, *.example.com), or by its IP address. Use a comma to separate the IP addresses.

  If `<iplist>` has a prefix (for example, +1.1.1.0,2.2.2.0), the meaning is as follows:
  - `+` adds `<iplist>` to the existing list. IP addresses in `<iplist>` must not already be in the existing list.
  - `-` removes `<iplist>` from the existing list. IP addresses in `<iplist>` must be in the existing list.

  If specified, the prefix will be applied to the entire `<iplist>`. If `<iplist>` has no prefix, `<iplist>` will be used as the new list.

### Modifying Configuration Settings for File Shares using SSMC

Using SSMC, you can specify the properties and settings of File Shares on a storage system. You can specify File Share names, share type (SMB, NFS, FTP, or Object), share path (parent File Store and VFS), and additional settings such as client filters and access permissions. To configure access settings for a File Share, complete the following steps:

- From the main menu, select **File Persona > File Shares**.
- Do one of the following:
  - Click `+ Create File Share` or select `Create` on the **Actions** menu.
  - On the list pane, select the **File Share**, and then select **Edit** or **Delete** on the **Actions** menu.
- Follow the instructions on the dialog that opens.

### FTP File Share

FTP is a client-server protocol that relies on control and data connection channels between a client and a server. File Persona provides client access to files and folders using the FTP protocol.

An FTP File Share defines parameters such as access permissions, enabling/disabling local/anonymouse users and FTPS related SSL options. You can create multiple shares on the same share path, but with different configurations.
To use non-secure FTP, set SSL tag to false during File Share creation. To use secure FTPS, set SSL to true during File Share creation. The network port for FTP is 21 and for FTPS is 990. FTP File shares support implicit and explicit modes of connection in FTPS.

The following FTP related attributes of an FTP share:

- FTP in both non-secure and secure mode
- FTP in read-only mode
- FTP File Share with one or more VIF IP address
- VFS IP can be used only for one FTP share

The following are the FTP related tasks that can be performed in an FTP share:

- Addition/deletion of an IP for an FTP File Share
- Modification of configuration settings of FTP File Share options
- Home directory based on UNIX user names

NOTE:

An FTP Share can have one or more VFS IPs but a VFS IP can belong to only one FTP Share at a time. If a VFS IP is already added to an FTP Share, it cannot be added to different FTP Share unless the VFS IP is deleted from the former FTP share. Since a VFS supports a maximum of four IP’s, we can create a maximum of four FTP Shares per VFS when each FTP share uses a unique VFS IP address.

FTP File Share Overview

FTP File Shares support the following features:

- Upload, download, append, rename and delete files
- Create, rename and delete directories
- Enumerate files
- Get the current working directory.

FTP File Shares and File Store Security Modes

File Persona uses dedicated security modes to ensure appropriate access to data shared across multiple protocols. The security modes are configurable at the File Store level. An FTP File Share can be created on a File Store in either legacy or NTFS security mode. For more information on security modes refer to section Security Modes in chapter Cross-protocol Access.

NOTE:

Anonymous user logins are not allowed when an FTP Share is created on a File Store in NTFS mode.

Configuring Access Control for FTP shares

Legacy Security mode

1. If the directory does not exist, the local administrator and members of the local administrator group get full control.
2. When an FTP File Share is created in an existing directory, and the existing directory is not empty, the access permissions remain the same. If the directory is empty, the FTP File Share gets the default permissions.

NTFS Security mode

When an FTP share is created:
1. If the directory does not exist, the resulting share folder permissions will follow the NTFS inheritance rules (will inherit from the parent directory).

2. If the directory exists, the existing permissions in the directory will be maintained.

**NOTE:**

File Persona doesn’t allow UNIX root account (UID is 0) for authentication. If a user tries to login to an FTP File Share as a UNIX root the authentication will fail.

To create an FTP File Share in read-only mode use the `file_access_mode` parameter and set it to "read".

**Protocol and Message Format**

Clients communicate with the FTP server using the FTP Protocol commands (RFC 959). The server responds to client requests with appropriate status codes and error strings as defined in the RFC.

**FTP File Share Connection Mode Configuration**

An FTP File Share can have an active or passive (or both) `connection_mode` configuration.

When an FTP File Share is in active mode the client connects from a random unprivileged network port (N > 1023) to the FTP server’s network port 21. The client starts listening to network port N+1 and sends the FTP command port N+1 to the FTP server. The server connects back to the client’s specified data port from its local data network port: port 20. The disadvantage with the active mode is that FTP process takes place at the client side. The FTP client doesn't make the actual connection to the data network port of the server. It simply tells the server what network port it is listening on and the server connects back to the specified network port on the client. The client side firewall thinks that this is an outside system initiating a connection to an internal client. If the active mode is enabled please ensure that the client side firewall rules allow the connection from the FTP server to the client.

When an FTP File Share is in passive mode the client initiates both the connections to the server, solving the problem of firewall filtering the incoming data network port connection from the server to the client.

**SSL Enabled FTP File Share**

FTP File Share configuration with SSL support allows an implicit mode of connection. An implicit mode makes sure that both the command/control connection and data connection gets encrypted by default and the client cannot disable the use of encryption. This is useful when confidential data is to be sent over the data connection. File Persona enabled FTP servers support TLSv1 encryption.

**Certificates for FTP Share**

An FTP share can be created with an SSL option. The SSL option will get enabled if the SSL option is `true`. A certificate should be assigned to the VFS before the SSL option can be enabled.

**Creating VFS with a Certificate**

Issue the following command using the HPE 3PAR CLI:

```bash
createvfs [-nocert|-certfile <certfile>|-certdata <certificate string>]
```

**Modifying VFS with a Certificate**

Issue the following command using the HPE 3PAR CLI:

```bash
setvfs [-rmcert|-certfile <certfile>|-certdata <certificate string>]
```

**Home Directory Support**

When an administrator enables the home directory configuration in a share; `home_dir_support=YES`, the administrator should ensure that the home directories of all users are set up. The home directories cannot be
created using the FTP protocol. The administrator should use the NFS/SMB protocol to create the home directories to make the share usable.

If a user tries to access a home directory using the FTP protocol but the home directory was not created, the server throws an error. A cURL client would get an error message as follows:
"curl: (56) SSL read: error:1408F10B:SSL routines:SSL3_GET_RECORD:wrong version number, errno 0"

If the home directories are available under the FTP share directory then the users logging in an FTP File Share get access to their home directories. If a users' home directory is not present in the FTP File Share directory the login will fail.

User Name Convention

An FTP File Share cannot be accessed by a user if the user name contains any of the following:

- User name starts with `.` or `_`
- User name has spaces
- User name has unprintable characters
- User name has characters which are not alphanumeric

Home Directory Use Case

Let us say there are 100 users: 1 ... 100. Their UNIX user names are user1 ..... user100. Their corresponding home directories are sharepath/home/staff/user1 ... sharepath/home/staff/user100. Set home_dir_prefix to `/home/staff`. User1 can access shares using FTP with a shared path sharepath/home/staff/user1; which is user1’s home directory. If user2 accesses the same share using FTP, user2’s shared path and home directory will be sharepath/home/staff/user2.

The following example shows how to find the UNIX name of a user using the showfs command:

```
showfs -usermap -username trk1@2008ad -d
SID : S-1-5-21-2943099029-2375420575-3763763779-550729
UID : 1176528713
GID : 1175978497
UPN : trk1@2008AD.LAB

The user is trk1 and domain is 2008AD.LAB. The UPN is trk1@2008AD.LAB and UNIX name is 2008AD\trk1.
```

Authentication and Permissions

An FTP Share uses the File Persona FTP Server to provide access through FTP protocol. The FTP server implements the FTP protocol and returns error codes as per the FTP Protocol RFC.

The FTP server requires basic authentication for all requests. Any user accessing the FTP share must authenticate as one of the valid users listed in the local user database, in LDAP, Active Directory (AD) or as anonymous user. Any user who can be authenticated according to the HPE 3PAR OS authentication settings for the File Persona can access the share and can be provided with read-write permissions.

A user will be able to perform operations such as upload/download/delete on FTP File Shares and directories as per the permissions set on the files/directories. Example: If a user A doesn’t have the write permission to the FTP Share, the user will not be able to upload any files. However, the HPE 3PAR Administrator can change the FTP Share directory permissions to provide write permissions to user A.
NOTE: LDAP authentication requires a temporary connection with the LDAP server with the user's credentials. If the LDAP server is configured to log bind/unbind a request and the load is heavy then the LDAP server log could grow very fast.

## FTP File Share Configuration Options

### GENERAL OPTIONS

<table>
<thead>
<tr>
<th></th>
<th>ascii_mode</th>
<th>default = both</th>
<th>Supported Values</th>
<th>Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td>off</td>
<td>No ASCII mode data transfers will be honored on downloads/uploads.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>download</td>
<td>ASCII mode data transfers will be honored only on downloads.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>upload</td>
<td>ASCII mode data transfers will be honored only for uploads.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>both</td>
<td>ASCII mode data transfers will be honored on downloads and uploads.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>file_access_mode</th>
<th>default = both</th>
<th>Supported Values</th>
<th>Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td></td>
<td></td>
<td>off</td>
<td>No reads (downloads) and writes to ftpshare are allowed on the share. Writes include any changes to ftp share files/directory like remove directory, delete file etc including uploads.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>read</td>
<td>Reads (downloads) are allowed but no writes to ftpshare are allowed. writes include any changes to ftp share files/directory like remove directory, delete file etc. including uploads</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>write</td>
<td>Reads (downloads) are allowed but writes are allowed. writes include any changes to ftp share files/directory like remove directory, delete file etc. including uploads</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>both</td>
<td>Read (downloads) and writes to ftpshare are allowed. writes include any changes to ftp share files/directory like remove directory, delete file etc. including uploads</td>
</tr>
<tr>
<td></td>
<td>login_access_mode</td>
<td>default = local</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>------------------</td>
<td>-----------------</td>
<td>---</td>
<td></td>
</tr>
<tr>
<td></td>
<td>off</td>
<td>Disallows login of users as configured in HPE 3PAR File Persona Authentication Settings and anonymous’ user login is not allowed</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>local</td>
<td>Allows login of users as configured in HPE 3PAR File Persona Authentication Settings but ‘anonymous’ user login is not allowed</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>anon</td>
<td>Disallows login of users as configured in HPE 3PAR File Persona Authentication Settings but ‘anonymous’ user login is allowed</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>both</td>
<td>Allows login of users as configured in HPE 3PAR File Persona Authentication Settings and ‘anonymous’ user login is allowed</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>home_dir_support</th>
<th>default = NO</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>If set to yes, ftp share will support for home directory usecase. i.e. if NFS share has home directories of various users inside it, these home directories can be access through ftp by creating ftp share on NFS share and providing appropriate home_dir_prefix ftp configuration option</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>home_dir_prefix</th>
<th>default = /</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Supports empty or absolute path. Absolute path starting with / which is same as shareroot directory. Default is empty which is same as giving “/”.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**NETWORK OPTIONS**

<table>
<thead>
<tr>
<th></th>
<th>connection_mode</th>
<th>default = passive</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Controls passive (PASV) or active (PORT) style of data connections. Supported values: ‘passive’, ‘active’, or ‘both’.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>pasv_min_port</th>
<th>default = 49251</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The minimum port to allocate for PASV style data connections. Can be used to specify a narrow port range to assist firewalling. <strong>Support values:</strong> 0 (use any port) or 1024-65535</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>pasv_max_port</th>
<th>default = 49500</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The maximum port to allocate for PASV style data connections. Can be used to specify a narrow port range to assist firewalling. <strong>Support values:</strong> 0 (use any port) or 1024-65535</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Table Continued*
<table>
<thead>
<tr>
<th></th>
<th>max_clients</th>
<th>default = 250</th>
<th>The maximum number of clients which may be connected. Any additional clients connecting will get an error message. If passive connection mode is enabled, ensure pasv_min_port and pasv_max_port has at least 250 ports allowed. <strong>Support values:</strong> 0(unlimited) or non-negative integer.</th>
</tr>
</thead>
</table>

**LOCAL AUTH USER OPTIONS**

<table>
<thead>
<tr>
<th></th>
<th>file_open_mode</th>
<th>default = 0777</th>
<th>The permissions with which uploaded files are created. Umasks are applied on top of this value. <strong>NOTE!</strong> If you want to specify octal values, remember the &quot;0&quot; prefix otherwise the value will be treated as a base 10 integer!</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>local_umask</td>
<td>default = 0022</td>
<td>The value that the umask for file creation is set to for local users. <strong>NOTE!</strong> If you want to specify octal values, remember the &quot;0&quot; prefix otherwise the value will be treated as a base 10 integer!</td>
</tr>
</tbody>
</table>

**ANONYMOUS USER OPTIONS**

<table>
<thead>
<tr>
<th></th>
<th>anon_upload_enable</th>
<th>default = YES</th>
<th>If set to YES, anonymous users will be permitted to upload files under certain conditions. For this to work, the option write_enable must be activated, and the anonymous ftp user must have write permission on desired upload location.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>chown_upload_mode</td>
<td>default = 0600</td>
<td>The file mode to force for anonymous uploads. <strong>NOTE!</strong> If you want to specify octal values, remember the &quot;0&quot; prefix otherwise the value will be treated as a base 10 integer!</td>
</tr>
<tr>
<td></td>
<td>anon_umask</td>
<td>default = 0077</td>
<td>The value that the umask for file creation is set to for anonymous users. <strong>NOTE!</strong> If you want to specify octal values, remember the &quot;0&quot; prefix otherwise the value will be treated as a base 10 integer!</td>
</tr>
<tr>
<td></td>
<td>no_anon_password</td>
<td>default = YES</td>
<td>When enabled, this prevents server from asking for an anonymous password - the anonymous user will log straight in.</td>
</tr>
<tr>
<td></td>
<td>anon_world_readable_only</td>
<td>default = NO</td>
<td>When enabled, anonymous users will only be allowed to download files which are world readable.</td>
</tr>
<tr>
<td></td>
<td>anon_other_write_enable</td>
<td>default = NO</td>
<td>If set to YES, anonymous users will be permitted to perform write operations other than upload and create directory, such as deletion and renaming. This is generally not recommended but included for completeness.</td>
</tr>
<tr>
<td></td>
<td>anon_mkdir_write_enable</td>
<td>default = YES</td>
<td>If set to YES, anonymous users will be permitted to create new directories under certain conditions. For this to work, the option write_enable must be activated, and the anonymous ftp user must have write permission on the parent directory.</td>
</tr>
</tbody>
</table>

*Table Continued*
**SSL OPTIONS**

<table>
<thead>
<tr>
<th></th>
<th>Variable</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ssl_enable</td>
<td>NO</td>
<td>If enabled, share will support secure connections via SSL.</td>
</tr>
<tr>
<td>2</td>
<td>require_ssl_reuse</td>
<td>NO</td>
<td>If set to yes, all SSL data connections are required to exhibit SSL session reuse (which proves that they know the same master secret as the control channel). Although this is a secure default, it may break many FTP clients, so you may want to disable it.</td>
</tr>
</tbody>
</table>

**Advanced Options (Only available through CLI)**

<table>
<thead>
<tr>
<th></th>
<th>Variable</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>dirlist_enable</td>
<td>YES</td>
<td>If set to NO, all directory list commands will give permission denied.</td>
</tr>
<tr>
<td>2</td>
<td>lock_upload_files</td>
<td>YES</td>
<td>When enabled, all uploads proceed with a write lock on the upload file. All downloads proceed with a shared read lock on the download file. Be aware that malicious readers could starve a writer wanting to e.g. append a file if enabled. Disable it if locking is not required.</td>
</tr>
<tr>
<td>3</td>
<td>mdtm_write</td>
<td>YES</td>
<td>When enabled, this setting will allow MDTM to set file modification times (subject to the usual access checks).</td>
</tr>
<tr>
<td>4</td>
<td>hide_ids</td>
<td>NO</td>
<td>If enabled, all user and group information in directory listings will be displayed as &quot;ftp&quot;.</td>
</tr>
<tr>
<td>5</td>
<td>text_userdb_names</td>
<td>NO</td>
<td>By default, numeric IDs are shown in the user and group fields of directory listings. You can get textual names by enabling this parameter. It is off by default for performance reasons.</td>
</tr>
<tr>
<td>6</td>
<td>accept_timeout</td>
<td>60</td>
<td>The timeout, in seconds, for a remote client to establish connection with a PASV style data connection.</td>
</tr>
<tr>
<td>7</td>
<td>connect_timeout</td>
<td>60</td>
<td>The timeout, in seconds, for a remote client to respond to our PORT style data connection.</td>
</tr>
<tr>
<td>8</td>
<td>data_connection_timeout</td>
<td>300</td>
<td>The timeout, in seconds, which is roughly the maximum time we permit data transfers to stall for with no progress. If the timeout triggers, the remote client is kicked off.</td>
</tr>
<tr>
<td>9</td>
<td>idle_session_timeout</td>
<td>300</td>
<td>The timeout, in seconds, which is the maximum time a remote client may spend between FTP commands. If the timeout triggers, the remote client is kicked off.</td>
</tr>
<tr>
<td>10</td>
<td>anon_max_rate</td>
<td>0</td>
<td>The maximum data transfer rate permitted, in bytes per second, for anonymous clients. <strong>Support values:</strong> 0(unlimited) or non-negative integer</td>
</tr>
<tr>
<td></td>
<td>local_max_rate</td>
<td>default = 0 (unlimited)</td>
<td>The maximum data transfer rate permitted, in bytes per second, for local authenticated users. <strong>Support values:</strong> 0(unlimited) or non-negative integer</td>
</tr>
<tr>
<td>---</td>
<td>----------------</td>
<td>-------------------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>12</td>
<td>ssl_version</td>
<td>default = tlsv1</td>
<td>SSL version to be used for protocol connections. Supported are ss1v3, tlsv1</td>
</tr>
<tr>
<td>13</td>
<td>implicit_ssl</td>
<td>default = YES</td>
<td>If enabled, an SSL handshake is the first thing expect on all connections (the FTPS protocol).</td>
</tr>
<tr>
<td>14</td>
<td>allow_anon_ssl</td>
<td>default = YES</td>
<td>Only applies if ssl_enable is active. If set to YES, anonymous users will be allowed to use secured SSL connections</td>
</tr>
<tr>
<td>15</td>
<td>force_anon_data_ssl</td>
<td>default = NO</td>
<td>Only applies if ssl_enable is activated. If activated, all anonymous logins are forced to use a secure SSL connection in order to send and receive data on data connections.</td>
</tr>
<tr>
<td>16</td>
<td>force_anon_logins_ssl</td>
<td>default = NO</td>
<td>Only applies if ssl_enable is activated. If activated, all anonymous logins are forced to use a secure SSL connection in order to send the password.</td>
</tr>
<tr>
<td>17</td>
<td>force_local_data_ssl</td>
<td>default = NO</td>
<td>Only applies if ssl_enable is activated. If activated, all non-anonymous logins are forced to use a secure SSL connection in order to send and receive data on data connections.</td>
</tr>
<tr>
<td>20</td>
<td>force_local_logins_ssl</td>
<td>default = YES</td>
<td>Only applies if ssl_enable is activated. If activated, all non-anonymous logins are forced to use a secure SSL connection in order to send the password.</td>
</tr>
</tbody>
</table>

**cURL Commands**

The cURL software program allows users to send FTP requests and receive responses from a UNIX or DOS command line. cURL is especially useful when creating automated shell or batch scripts that perform repeated actions against a server.

If you use a tool such as cURL to send the FTP request, the tool might have support for FTP protocol commands using various options. The exact behavior and options depends on the tool and version used.

**cURL Examples**

- To download a file from an FTP share using curl to access the FTP share directory:
  
  ```
  #curl -u <username>:<password> ftp://vfs_address/file_name
  ```

- To upload a file to FTP share using curl to share directory:
  
  ```
  #curl -u <username>:<password> ftp://vfs_address/file_name -T <path to file to be uploaded>
  ```

- To download a file from FTP share's anonymous user area:
  
  ```
  #curl -u anonymous:anonymous ftp://vfs_address/pub/file_name
  ```

- To upload a file to FTP share anonymous user area:
  
  ```
  #curl -u anonymous:anonymous ftp://vfs_address/pub/file_name -T <path to file to be uploaded>
  ```

- To download a file through FTP Share with SSL enabled (implicit mode):
Managing FTP File Shares

Displaying FTP File Shares

To display an FTP File Share, issue the following command:

```
showfshare ftp -dirperm [-fpg <fpgname>] -vfs <vfs> -fstore <fstorename> <sharename>
```

where,
- `ftp` displays File Shares information for FTP.
- `-d` option shows share attributes that are not displayed by other options. Shows details of all shares or a single share.
- `-dirperm` Displays the share folder permissions: the ACL in Converged ACL format, UNIX mode bits permissions, owner and group information of the share directory.
- `-fpg <fpg_name>` specifies the FPG name. This limits the share output to those shares associated with the specified FPG.
- `-vfs <vfs>` specifies the VFS name. This limits the share output to those shares associated with the specified VFS. If this option is specified, but `-fpg` is not specified, the command will find out the FPG based on `<vfs>`. However, if `<vfs>` exists under multiple FPGs, `-fpg` must be specified.
- `-fstore <fstorename>` specifies the File Store name. This limits the share output to only those shares associated with the specified File Store. If this is specified, option `-vfs` must be specified.
- `-pat` specifies the File Share names using the glob-style pattern. Shares which have the name matching any of the specified glob-style patterns will be displayed. The `-pat` option can specify a list of patterns.
- `<pattern|sharename>` displays only shares with names matching the specified `<sharename>` or one of the glob-style patterns.

Displaying File Share configuration using the SSMC:
From the main menu, select **File Persona**.

Select **File Persona Configuration**.

**File Persona Configuration** screen displays a list of storage systems that have File Persona capabilities, detail views, and an **Actions** menu.

### Creating File Shares

**NOTE:** File shares can be created for multiple supported protocols. However, please note that simultaneous write access from multiple protocols to the same File Share under a File Store in legacy security mode is not supported. Currently the default number of shares per node is 4000. However, this registry is tunable and can be changed by contacting HPE support.

To create an FTP File Share, issue the following command:

```
```

where,

- **ftp** creates an FTP File Share.
- **-f** specifies that the command is forced. When creating a share for a secondary protocol type for a given File Store, if this option is not used, the command requires confirmation before proceeding with its operation.
- **-fpg** specifies the FPG the `<vfs>` belongs to. If this is not specified, the command will find out the FPG based on the specified `<vfs>` . However, if the `<vfs>` exists under multiple FPGs, `-fpg` must be specified.
- **-fstore** specifies the File Store under which the share will be created. If this is not specified, the command uses the `<sharename>` as the File Store name. The File Store will be created if it does not exist. In this case, the File Store that will be created depends on the type of File Share (i.e. if the share is smb, the File Store will be created in NTFS security mode, otherwise legacy).
- **-sharedir** specifies the directory path to share. It can be a full path starting from `/`, or a relative path under the File Store. If this is not specified, the share created will be rooted at the File Store. If a relative path is specified, option `-fstore` must be specified. If the directory path does not exist, it will be created.
- **-comment** specifies any comments or additional information for the share. The comment can be up to 255 characters long. Unprintable characters are not allowed.
- **<vfs>** specifies the VFS under which the File Store, if it does not exist, and the share will be created.
- **<sharename>** specifies the share name to be created.

### Subcommand options

The subcommand `createfshare ftp` creates FTP File Shares:

```
createfshare ftp [options <arg>]
```

The following option is specific to the `createfshare ftp [options <arg>]` subcommand:

- **-ssl {true|false}**
specifies if SSL is enabled. The default is false.

NOTE:
To enable SSL, the VFS must have a valid certificate configured.

If a user’s quota has exceeded on a VFS, the user will not be permitted to write on the FTP Share and the connection to the server will automatically close while trying to write on the FTP Share. The error message received by user depends on the client behavior. A user using cURL as the FTP client will get an error message saying "Select/poll returned error". For all other clients the connection will be closed. Check with your Administrator for the specific error message based on the client you are using.

Creating File Shares Using SSMC

Using the SSMC, open File Persona screens and select the File Shares screen to create and manage one or more File Shares on each of the VFSs. You can also open the File Stores screen or the Virtual File Servers screen and select Create File Share.

Creating a File Share from a File Shares screen
• From the main menu, select File Persona > File Shares.
• Click + Create File Share or select Create on the Actions menu.
• Follow the instructions on the dialog that opens.

Creating a File Share from a Virtual File Servers screen
• From the main menu, select File Persona > Virtual File Servers.
• Click Create File Share.
• Follow the instructions on the dialog that opens.

Removing FTP File Shares

To remove an FTP File Share, issue the following command:
removefshare ftp [-f] [-fpg <fpgname>] [-fstore <fstore>] <vfs> <sharename>
where,
• ftp
  removes an FTP File Share.
• -f
  option specifies that the command is forced. If this option is not used, the command requires confirmation before proceeding with its operation.
• -fpg <fpg_name>
  option specifies the FPG that <vfs> belongs. If this is not specified, the command will find out the FPG based on the specified <vfs>. However, if <vfs> exists under multiple FPGs, -fpg must be specified.
• -fstore <fstore>
  option specifies the File Store that the File Share to be removed belongs. If this is not specified, the <sharename> will be used as -fstore.
• <vfs>
  specifies the VFS name.
• <sharename>
  specifies the name of the share to be removed.
NOTE:
Removing a File Share only removes access to files and folders. It does not physically remove any files or folders.

Removing a File Share using SSMC

• From the main menu, select File Persona > File Shares.
• Select the File Share you want to delete, and then select the Actions menu.
• Select Delete

Modifying FTP File Shares

To modify an FTP File Share, issue the following command:

```
```

where,

• ftp
  sets File Share options for FTP protocol.
• -acl [+|-]<permlist>
  specifies the access control list (ACL) permissions that are allowed on a share directory. This option cannot be used when -mode is used. Setting ACL permissions can break cross-protocol functionality if used improperly, and may cause loss of mode bits information. A warning prompt is displayed to the users asking if they wish to proceed.

IMPORTANT:
This is the system CONVERGED ACL. To understand how these permissions are translated to Windows and UNIX clients permission enforcement, please see Permission Conversion Rules for Converged ACLs on page 123.

The -acl option is provided primarily for the NTFS security mode. In the Legacy security mode, if the File Store is being used in a cross-protocol environment and the NFS clients are configured as read/write clients (SMB clients are read-only), it is recommended that do not use the -acl option to change permissions of the share folder. Use the -mode option instead.

The ACL in the share folder permissions that are created by default (by inheritance from the File Store directory) in the NTFS security mode are more restrictive than the default ACLs in the share folders in the Legacy security mode. Use the showfshare -dirperm CLI command to view the given ACL, and the setfshare -acl CLI command in the NTFS security mode to change the share folder ACL.

The values for <permlist> fields type:flag:principal:permissions is as follows:

type
The type field can take only one of the following values:

• A
  -allow
• D
  -deny
• U
-audit
  • L
  -alarm

flag
The flag field is optional and can take one or more of the following values:
  • f
    -file-inherit
  • d
    -directory-inherit
  • p
    -no-propagate-inherit
  • i
    -inherit-only
  • S
    -successful-access
  • F
    -failed-access
  • g
    -group (denotes that <principal> is a group)

principal
The principal field can be any named user or group or one of the following values:
  • OWNER@
  • GROUP@
  • EVERYONE@

permissions
The permissions field can take one or more of the following values:
  • r
    -read-data | list-directory
  • w
    -write-data | create-file
  • a
    -append-data | create-subdirectory
  • x
    -execute
  • d
    -delete
  • D
    -delete-child (directories only)
  • t
    -read-attrs
  • T
-write-attrs
  ◦ n
  -read-named-attrs
  ◦ N
  -write-named-attrs
  ◦ c
  -read-ACL
  ◦ C
  -write-ACL
  ◦ o
  -write-owner
  ◦ y
  -synchronize

If specified, the prefix will be applied to the entire <permlist>. If <permlist> has no prefix, the information will be used to create a new permlist. The <permlist> contains the list of Access Control Entries (ACEs). Use commas to separate ACEs. Each ACE contains four values named type, flag, principal, and permissions. These four values should be separated by a ":". The format of the ACE corresponds to the NFSv4 ACL format. See linux NFS4_acl (5) man page for additional information.

Example:
A:fd:OWNER@:rwax,A:fdg:GROUP@:rwax
If <permlist> has a prefix;
Example: +A:fd:OWNER@:rwa,A:g:GROUP@:rwxa
  ◦ If + or – is not specified: The entire ACL on the file object is replaced with the specified <permlist>. The order specified will be maintained. There will be no checks for duplicate ACEs (i.e. duplicates are allowed).
  ◦ If + prefix is specified: -acl +<permlist> The new <permlist> is inserted at the head of the existing ACL, in the same order as specified. There will be no checks for duplicate ACEs (i.e. duplicates are allowed).
  ◦ If – is specified: -acl -<permlist> For each ACE in the specified <permlist>, the current ACL will be searched, in an order, until the first entry that matches is found. The first matching entry will be removed. If no matching ACE is found, the action will fail.

• -mode <modebits>

specifies the modebits permissions that are allowed on a share directory. This option cannot be used when -acl is used. Setting mode bits may break cross-protocol functionality if used improperly, and may cause loss of ACL information. A warning prompt is displayed to the users asking if they wish to proceed.

NOTE:

Caution is required when using the -acl, -mode, -user, and -group commands to ensure the resulting settings are appropriate for the protocol through which file writes and directory creations are going to occur. Generally, the -acl option should be used for shares with SMB based writers and the -mode option should be used with NFS/FTP/OBJ based writers. The -mode option is allowed only in Legacy security mode, not in NTFS security mode.

• -f

specifies that the command is forced. When setting ACL permissions or mode bits of a share directory, if this option is not used, the command requires confirmation before proceeding with its operation.

• -owner <name>
specifies the name of the owner to whom the share directory belongs. The format of <name> is the same as with the allowperm option above.

**NOTE:**
In the NTFS security mode when the owner is changed, the new owner does not get any permissions. An ACE has to exist for the new owner and if it does not exist it has to be created. Any previous OWNER@ ACES in the converged ACL will become named ACES for the previous owner. If the owner is changed, and the user wants the owner to have permissions (assuming the new owner does not have any preassigned ACE), then the user has to assign the new owner an ACE with the desired permissions. Execute the setfshare -acl command on the ACE.

In the NTFS security mode, when the owner is changed, the new owner not get any permissions.

- **-group <name>**

  specifies the name of the group to which the share directory belongs. The format of <name> is the same as with the allowperm option above.

**NOTE:**
In the NTFS security mode when the group is changed, the new group does not get any permissions. An ACE has to exist for the new group and if it does not exist it has to be created. Any previous GROUP@ ACES in the converged ACL will become named ACES for the previous group. If the group is changed, and the user wants the group to have permissions (assuming the new group does not have any preassigned ACE), then the user has to assign the new group an ACE with the desired permissions. Execute the setfshare -acl command on the ACE.

In the NTFS security mode, when the group is changed, the new group does not get any permissions.

- **-fpg <fpgname>**

  specifies the FPG to which <vfs> belongs. If this option is not specified, the command will find out the FPG based on the specified <vfs>. However, if <vfs> exists under multiple FPGs, -fpg must be specified.

- **-fstore <fstore>**

  specifies the File Store that the share to be modified belongs. If this is not specified, the <sharename> will be used as the File Store name to identify the share.

- **-comment <comment>**

  specifies any comments or additional information for the share. The comment can be up to 256 characters long. Unprintable characters are not allowed.

- **<sharename>**

  specifies the File Share.

### File Share Options for FTP protocol

The following options are specific to the setfshare ftp [options <arg>] subcommand:

- **-ssl {true|false}**

  specifies whether to enable or disable SSL.

### Modifying Configuration Settings for File Shares using SSMC

Using SSMC, you can specify the properties and settings of File Shares on a storage system. You can specify File Share names, share type (SMB, NFS, FTP or Object), share path (parent File Store and VFS), and additional settings such as client filters and access permissions. To configure access settings for a File Share, complete the following steps:
• From the main menu, select **File Persona > File Shares**.
• Do one of the following:
  ◦ Click **+ Create File Share** or select **Create** on the **Actions** menu.
  ◦ On the list pane, select the **File Share**, and then select **Edit** or **Modify** on the **Actions** menu.
• Follow the instructions on the dialog that opens.

**Object Access API File Share**

File Persona supports access to files and directories using an Object Access API. Object Access API protocol enables integration of access to files from and into applications.

**Object Access API File Share Overview**

The Object Access API supports the following operations:

- Create, replace, rename, download, retrieve and delete a file
- Create, retrieve and delete a directory
- Change owner and user permissions
- Change groups
- Set, retrieve and remove extended attributes
- Commit data to a disk

For more information, see the **HPE 3PAR Object Access API Reference**, available at the following website:

[HPE Storage Information Library](http://www.hpe.com/info/storage/docs)

**Configuring Global Object Access API Settings**

To configure global Object Access API parameters, issue the following command:

```
setfs obj [-keepalive {true | false}] [-timeout <secs>] [-maxclients <num>] [-rblksize <size>] [-wblksize <size>]
```

where,

- **-keepalive {true | false}**
  specifies if persistent connections are allowed or not for the default object profile. The default value is true, persistent connections are allowed.
- **-timeout <secs>**
  specifies the timeout value in seconds for the persistent connections for the default object profile. The valid range is from 1 to 2592000. The default value is 5 seconds.
- **-maxclients <num>**
  specifies the maximum number of simultaneous connections for the default object profile. The valid range is from 1 to 128. The default value is 50 connections.
- **-rblksize <size>**
  specifies the socket read block size for the default object profile. The size can be specified with a K or M to indicate the value is in kilobytes or megabytes, for example, -rblksize 10K. The valid range is from 8 KB to 2048 MB. The default value is 8K.
- **-wblksize <size>**
  specifies the file write block size for the default object profile. The size can be specified with a K or M to indicate the value is in kilobytes or megabytes, for example, -wblksize 1M. The valid range is from 8 KB to 2047 MB. The default value is 8K.
Managing Object Access API File Shares

Displaying Object Access API File Shares

To display an Object Access API File Share, issue the following command:

```bash
showfshare obj -dirperm [-fpg <fpgname>] -vfs <vfs> -fstore <fstorename> <sharename>
```

where,

- **obj**
  - displays File Share information for Object Access API.
- **-d**
  - option shows share attributes that are not displayed by other options. Shows details of all shares or a single share
- **-dirperm**
  - displays the share folder permissions: the ACL in Converged ACL format, UNIX mode bits permissions, owner and group information of the share directory.
- **-fpg <fpg_name>**
  - specifies the FPG name. This limits the share output to those shares associated with the specified FPG.
- **-vfs <vfs>**
  - specifies the VFS name. This limits the share output to those shares associated with the specified VFS. If this option is specified, but -fpg is not specified, the command will find out the FPG based on <vfs>. However, if <vfs> exists under multiple FPGs, -fpg must be specified.
- **-fstore <fstorename>**
  - specifies the File Store name. This limits the share output to only those shares associated with the specified File Store. If this is specified, option -vfs must be specified.
- **-pat**
  - specifies the File Share names using the glob-style pattern. Shares which have the name matching any of the specified glob-style patterns will be displayed. The -pat option can specify a list of patterns.
- **<pattern|sharename>**
  - displays only shares with names matching the specified <sharename> or one of the glob-style patterns.

Displaying File Share configuration using the SSMC:

- From the main menu, select File Persona.
- Select File Persona Configuration.
- File Persona Configuration screen displays a list of storage systems that have File Persona capabilities, detail views, and an Actions menu.

Creating Object Access API File Shares

**NOTE:** File shares can be created for multiple supported protocols. However, please note that simultaneous write access from multiple protocols to the same File Share under a File Store in legacy security mode is not supported. Currently the default number of shares per node is 4000. However, this registry is tunable and can be changed by contacting HPE support.
To create an Object Access API File Share, issue the following command:

```
```

where,

- **obj** creates an Object Access API File Share.
- **-f** specifies that the command is forced. When creating a share for a secondary protocol type for a given File Store, if this option is not used, the command requires confirmation before proceeding with its operation.
- **-fpg** specifies the FPG the `<vfs>` belongs to. If this is not specified, the command will find out the FPG based on the specified `<vfs>` . However, if the `<vfs>` exists under multiple FPGs, `-fpg` must be specified.
- **-fstore** specifies the File Store under which the share will be created. If this is not specified, the command uses the `<sharename>` as the File Store name. The File Store will be created if it does not exist. In this case, the File Store that will be created depends on the type of File Share (i.e. if the share is smb, the File Store will be created in NTFS security mode, otherwise legacy).
- **-sharedir** specifies the directory path to share. It can be a full path starting from "/", or a relative path under the File Store. If this is not specified, the share created will be rooted at the File Store. If a relative path is specified, option `-fstore` must be specified. If the directory path does not exist, it will be created.
- **-comment** specifies any comments or additional information for the share. The comment can be up to 255 characters long. Unprintable characters are not allowed.
- **<vfs>** specifies the VFS under which the File Store, if it does not exist, and the share will be created.
- **<sharename>** specifies the share name to be created.

### Creating Object Access API File Shares

The subcommand `createfshare obj` creates Object Access API File Shares:

```
createfshare obj [options <arg>]
```

The following options are specific to the `createfshare obj [options <arg>]` subcommand:

- **-ssl {true|false}** specifies if SSL is enabled. The default is false.
- **-urlpath <urlpath>** specifies the URL that clients will use to access the share. If this is not specified, the command uses `<sharename>` as `<urlpath>`.

**NOTE:**

To enable SSL, the VFS must have a valid certificate configured.
Creating File Shares Using SSMC

Using the SSMC, open File Persona screens and select the File Shares screen to create and manage one or more File Shares on each of the VFSs. You can also open the File Stores screen or the Virtual File Servers screen and select Create File Share.

Creating a File Share from a File Shares screen

• From the main menu, select File Persona > File Shares.
• Click + Create File Share or select Create on the Actions menu.
• Follow the instructions on the dialog that opens.

Creating a File Share from a Virtual File Servers screen

• From the main menu, select File Persona > Virtual File Servers.
• Click Create File Share.
• Follow the instructions on the dialog that opens.

Removing Object Access API File Shares

To remove an Object Access API File Share, issue the following command:

removefshare obj [-f] [-fpg <fpgname>] [-fstore <fstore>] <vfs> <sharename>

where,

• obj
  removes an Object access API File Share.
• -f
  option specifies that the command is forced. If this option is not used, the command requires confirmation before proceeding with its operation.
• -fpg <fpg_name>
  option specifies the FPG that <vfs> belongs. If this is not specified, the command will find out the FPG based on the specified <vfs>. However, if <vfs> exists under multiple FPGs, -fpg must be specified.
• -fstore <fstore>
  option specifies the File Store that the File Share to be removed belongs. If this is not specified, the <sharename> will be used as -fstore.
• <vfs>
  specifies the VFS name.
• <sharename>
  specifies the name of the share to be removed.

NOTE:
Removing a File Share only removes access to files and folders. It does not physically remove any files or folders.

Removing a File Share using SSMC

• From the main menu, select File Persona > File Shares.
• Select the File Share you want to delete, and then select the Actions menu.
• Select Delete

Modifying Object Access API File Shares

To modify an Object Access API File Share, issue the following command:

where,

- obj
  sets File Share options for Object Access API protocol.
- -acl [+|-]<permlist>
  specifies the access control list (ACL) permissions that are allowed on a share directory. This option cannot be used when -mode is used. Setting ACL permissions can break cross-protocol functionality if used improperly, and may cause loss of mode bits information. A warning prompt is displayed to the users asking if they wish to proceed.

1 IMPORTANT:
   This is the system CONVERGED ACL. To understand how these permissions are translated to Windows and UNIX clients permission enforcement, please see Permission Conversion Rules for Converged ACLs on page 123.

   The -acl option is provided primarily for the NTFS security mode. In the Legacy security mode, if the File Store is being used in a cross-protocol environment and the NFS clients are configured as read/write clients (SMB clients are read-only), it is recommended that do not use the -acl option to change permissions of the share folder. Use the -mode option instead.

   The ACL in the share folder permissions that are created by default (by inheritance from the File Store directory) in the NTFS security mode are more restrictive than the default ACLs in the share folders in the Legacy security mode. Use the showfshare -dirperm CLI command to view the given ACL, and the setfshare -acl CLI command in the NTFS security mode to change the share folder ACL.

The values for <permlist> fields type:flag:principal:permissions is as follows:

type
   The type field can take only one of the following values:
   ◦ A
     -allow
   ◦ D
     -deny
   ◦ U
     -audit
   ◦ L
     -alarm

flag
   The flag field is optional and can take one or more of the following values:
   ◦ f
     -file-inherit
   ◦ d
     -directory-inherit
   ◦ p
     -no-propagate-inherit
principal
The principal field can be any named user or group or one of the following values:

- OWNER@
- GROUP@
- EVERYONE@

permissions
The permissions field can take one or more of the following values:

- r
  - read-data | list-directory
- w
  - write-data | create-file
- a
  - append-data | create-subdirectory
- x
  - execute
- d
  - delete
- D
  - delete-child (directories only)
- t
  - read-attrs
- T
  - write-attrs
- n
  - read-named-attrs
- N
  - write-named-attrs
- c
  - read-ACL
- C
  - write-ACL
- o
-write-owner
  
- synchronize

If specified, the prefix will be applied to the entire <permlist>. If <permlist> has no prefix, the information will be used to create a new permlist. The <permlist> contains the list of Access Control Entries (ACEs). Use commas to separate ACEs. Each ACE contains four values named type, flag, principal, and permissions. These four values should be separated by a ":". The format of the ACE corresponds to the NFSv4 ACL format. See linux NFS4_acl (5) man page for additional information.

Example:
A:fd:OWNER@:rwax,A:fdg:GROUP@:rwax

If <permlist> has a prefix;

Example: +A:fd:OWNER@:rwa,A:g:GROUP@:rwxa

-+ or - is not specified: The entire ACL on the file object is replaced with the specified <permlist>. The order specified will be maintained. There will be no checks for duplicate ACEs (i.e. duplicates are allowed)

-+ prefix is specified: -acl +<permlist> The new <permlist> is inserted at the head of the existing ACL, in the same order as specified. There will be no checks for duplicate ACEs (i.e. duplicates are allowed).

-- is specified: -acl -<permlist> For each ACE in the specified <permlist>, the current ACL will be searched, in an order, until the first entry that matches is found. The first matching entry will be removed. If no matching ACE is found, the action will fail.

• -mode <modebits>

specifies the modebits permissions that are allowed on a share directory. This option cannot be used when -acl is used. Setting mode bits may break cross-protocol functionality if used improperly, and may cause loss of ACL information. A warning prompt is displayed to the users asking if they wish to proceed.

NOTE:
Caution is required when using the -acl, -mode, -user, and -group commands to ensure the resulting settings are appropriate for the protocol through which file writes and directory creations are going to occur. Generally, the -acl option should be used for shares with SMB based writers and the -mode option should be used with NFS/FTP/OBJ based writers. The -mode option is allowed only in Legacy security mode, not in NTFS security mode.

• -f

specifies that the command is forced. When setting ACL permissions or mode bits of a share directory, if this option is not used, the command requires confirmation before proceeding with its operation.

• -owner <name>

specifies the name of the owner to whom the share directory belongs. The format of <name> is the same as with the allowperm option above.

NOTE:
In the NTFS security mode when the owner is changed, the new owner does not get any permissions. An ACE has to exist for the new owner and if it does not exist it has to be created. Any previous OWNER@ ACES in the converged ACL will become named ACES for the previous owner. If the owner is changed, and the user wants the owner to have permissions (assuming the new owner does not have any preassigned ACE), then the user has to assign the new owner an ACE with the desired permissions. Execute the setfshare -acl command on the ACE.

In the NTFS security mode, when the owner is changed, the new owner not get any permissions.
- **group** <name>

specifies the name of the group to which the share directory belongs. The format of <name> is the same as with the allowperm option above.

**NOTE:**

In the NTFS security mode when the group is changed, the new group does not get any permissions. An ACE has to exist for the new group and if it does not exist it has to be created. Any previous GROUP@ ACES in the converged ACL will become named ACES for the previous group. If the group is changed, and the user wants the group to have permissions (assuming the new group does not have any preassigned ACE), then the user has to assign the new group an ACE with the desired permissions. Execute the setfshare -acl command on the ACE.

In the NTFS security mode, when the group is changed, the new group does not get any permissions.

- **-fpg** <fpgname>

specifies the FPG to which <vfs> belongs. If this option is not specified, the command will find out the FPG based on the specified <vfs>. However, if <vfs> exists under multiple FPGs, -fpg must be specified.

- **-fstore** <fstore>

specifies the File Store that the share to be modified belongs. If this is not specified, the <sharename> will be used as the File Store name to identify the share.

- **-comment** <comment>

specifies any comments or additional information for the share. The comment can be up to 256 characters long. Unprintable characters are not allowed.

- **<sharename>**

specifies the File Share.

**File Share Options for Object Access API protocol**

The following options are specific to the `setfshare obj [options <arg>]` subcommand:

- **-ssl** {true|false}

  specifies whether to enable or disable SSL.

**Modifying Configuration Settings for File Shares using SSMC**

Using SSMC, you can specify the properties and settings of File Shares on a storage system. You can specify File Share names, share type (SMB, NFS, FTP or Object), share path (parent File Store and VFS), and additional settings such as client filters and access permissions. To configure access settings for a File Share, complete the following steps:

- From the main menu, select **File Persona > File Shares**.
- Do one of the following:
  - Click **Create File Share** or select **Create** on the **Actions** menu.
  - On the list pane, select the **File Share**, and then select **Edit** or **Delete** on the **Actions** menu.
- Follow the instructions on the dialog that opens.
Cross-protocol Access

File Persona enables access to file shares in a cross-protocol environment over SMB, NFS, Object Access API, and FTP file protocols. Every protocol has different types of access permissions and different ways to identify users who are trying to access the files. For example, SMB clients use NTFS ACLs and Windows SID for user identity whereas NFS clients use UNIX mode bits or POSIX ACLs and UID/GID for user identity. Object Access API and FTP clients use UNIX mode bits and UID/GID for user identity.

If applications or users use different protocols to access a common data set on a File Share, the security modes and file locks need to be translated and unified to allow proper security enforcement and data integrity.

Users are allowed to access data with read/write access from more than one protocol using a mechanism known as cross-protocol locking. It ensures that NFS clients can access files opened by SMB clients through share mode locks and vice versa.

File Persona supports native ACLs with On-Disk Version (ODV) 12.2 or higher. Files and folders ACLs are stored in native ACL format and native identity of the access protocol is saved. The primary protocol's ACL is always stored first while the secondary protocol's ACL is stored after the first access.

NTFS ACLs are used for evaluating effective permissions when accessing from SMB clients. POSIX permissions, such as UNIX mode bits and POSIX ACLs are used for evaluating effective permissions when accessing from POSIX clients (NFS, Object Access API and FTP).

**Security Modes**

File Persona uses dedicated security modes to ensure the appropriate access to data shared across multiple protocols. Following are some of the benefits achieved when using dedicated security modes:

- Configurable security modes per File Store to provide near native user experience for the preferred protocol
- Consistent default permissions specific to the preferred protocol
- Prevents fidelity loss by restricting permission changes from the non-preferred protocol

The security modes are configurable at the File Store level. They are listed below:

**Legacy**

Legacy security mode is supported to ensure backward compatibility for FPGs created with ODV 12.0 or earlier. If the user desires, the File Store can still be configured in the Legacy mode but it will have restricted read/write access from one protocol and read-only access from the other protocol. This mode should not be used if the user wants read/write access on both Windows and non-Windows clients. If the user desires read/write access on both Windows and non-Windows clients in a cross-protocol environment, **NTFS security mode should be used**.

The following are the salient features of the Legacy security mode:

- The access protocol dictates the inheritance rules. NTFS inheritance rules are applied when Windows Clients desire access. POSIX clients use UMASK, create-mode, and the POSIX default ACL.

With ODV 12.2 or later, the native ACLs format on disk gets enabled. For the Legacy security mode, an NFSv4 ACL with UIDs and GIDs will always be stored on the disk. For SMB clients an NTFS ACL with SID will be generated on first successful access to be stored on disk. Once authenticated, the POSIX clients (NFS, Object Access API, and FTP) would not go through any name resolution during access whereas the SMB clients would go through name resolutions at least once (during first access).

When creating shares in a cross-protocol environment on a File Store in Legacy mode, a warning message is displayed. The warning message is displayed as follows:
WARNING: Folders are allowed to be shared as writable for one protocol only and as read-only for all other protocols. For specific procedures on creating cross-protocol access shares, refer to Setup Guide for "HPE 3PAR File Persona in a Cross-Protocol Environment" at the location provided below. Configuring shares within the same File Store with write access for multiple protocols will result in unexpected behavior. Do you wish to continue? select q=quit y=yes n=no:

NTFS

The NTFS security mode allows concurrent read and write access to any file protocol supported by File Persona. The allowed operations for files and folders in a cross-protocol access use-case are:

- Create
- Read
- Write
- Delete
- Rename

In contrast to the Legacy security mode, it enforces NTFS ACLs in the file system independent of protocol in use, and maintains NTFS inheritance rules and NTFS ACL fidelity. As a security mechanism it prevents non-SMB clients to alter permissions and only permits read permissions.

This allows a near-native experience for Microsoft Windows clients with support for:

- Case insensitivity for files and folders
- Full fidelity NTFS ACL enforcement for SMB protocol clients
- Full compliance with NTFS inheritance rules for new files and folders
- Unperceivable conversion of NTFS ACLs to POSIX permissions when files or folders are accessed using other protocols.

With ODV 12.2 or later, the NTFS security mode stores both NTFS and POSIX ACLs in their native format. These contain Windows security descriptors with Security identifiers (SIDs) for identity and POSIX ACLs with UIDs and GIDs for identity. File Stores in NTFS security mode primarily maintain NTFS ACLs, and convert and store POSIX ACLs after first access of a file or folder from a non-SMB protocol client (NFS, Object Access API, and FTP). This loosens the dependency on name service availability for user name resolution and increases the robustness and the performance of file system metadata operations.

Security Enforcement

In the NTFS security mode, permissions and ownership of file objects can only be modified using one of the following methods:

- The NTFS ACL from an SMB client can be modified only by users that have the required permissions to modify the NTFS ACLs.
- The system’s NFSv4 ACL (synthesized from the On-Disk NTFS ACL) can be modified by the means of the HPE 3PAR CLI, but only for directories in the root of a share (share folders).

File Persona will store and preserve the fidelity of the NTFS ACL set from an SMB client or an NTFS ACL generated using the NTFS inheritance rules.

If an attempt is made to change the share folder permissions using the HPE 3PAR CLI, File Persona will convert the permissions to an NTFS ACL. If the attempt is successful and the SIDs are generated, the NTFS ACL will be stored on disk. However, on access from an NFS client, File Persona uses the on disk ACLs and translates them to POSIX ACLs to enforce permissions for the NFS client.
• The server translates the higher fidelity ACL to its best approximation of POSIX ACLs.
• The resulting granted permissions could be more restrictive than the Windows ACL permissions.
• Beware of permission fidelity loss during conversions and its implication on non-SMB clients while setting permissions.

Share Folder Permissions

The default permissions in the share folder are specific to the security mode, independent of the protocol that the folder is shared over. The administrator can modify the permissions in the share folder level using the `setfshare` CLI command in a converged ACL format as native ACL format changes are not allowed from the CLI.

The NTFS security mode has a default ACL defined at the File Store root level folder which allows the files and directories to inherit the ACEs.

A share can be created either at the root of a File Store or in a subdirectory below the File Store root. If a subdirectory does not exist, the subdirectory will be created and the permissions are inherited from the parent directory using the NTFS inheritance rules.

ACEs are added or inserted at the beginning of the ACL. If the user wants to replace all the ACEs, then the user must replace the entire ACL.

The ACEs are examined in order, until one of the following happens:

- An ACE is encountered that explicitly denies permissions to the user
- Enough ACEs are encountered to grant access to the user
- All ACEs are exhausted

ACL permissions for the share directory (SMB and NFS) contain a list of ACEs permission list. Each ACE contains four values named: type, flag, principal and permissions. These four values should be separated by ":" and the values for the permission list fields are `type:flag:principal:permissions`. To add or remove ACEs, prefix such as "+" and "-" are used. To add permissions in the existing ACEs for a particular "principal", permission must not be there in the existing list. To remove permission from the existing ACEs for a particular "principal", permission must already be there in the existing list. The "principal" field can be any of the following values: OWNER@, GROUP@ and EVERYONE@. Duplicate ACLs can exist with different permissions for the same principal.

Assuming that the administrator has done no modifications to the share folder permissions, the default share folder permissions logic is as follows:

If a file share is created at the root of a File Store:

- From an SMB Client:
  - Everyone has the permission to mount and traverse to the mount point from a Windows client (non-inheritable permissions).
  - Only SYSTEM@NT_AUTHORITY (equivalent to root in Windows) and members of the Administrators group in the Windows domain have additional permissions. SYSTEM@NT_AUTHORITY and members of Administrators@B-LOCAL_CLUSTER have full-control and these permissions are inheritable.

- From an NFS Client:
  - Everyone has permissions to traverse to the mount point (non-inheritable permissions).
  - Only members of the Administrators group (if client has joined the same domain as File Persona node) have additional permissions: full-control and inheritable permissions.

The following example illustrates the default ACLs of the share folder when a File Share is created at the root of a File Store:
In the example above, the ACL at the root of the share has three ACEs that are inheritable: OWNER@, GROUP@ and CREATOR^OWNER@. When converted to an NTFS ACL, all shares created for the subdirectories at the File Store root will inherit these three ACEs. However, the EVERYONE@ ACE is not inheritable, and provides only read permissions (no create/write or modify permissions). This means that by default, shares created at the root of the File Store will have an extra EVERYONE@ ACE that will allow everyone to traverse the root of a File Store, but not below (unless the administrator grants different permissions that override the default).

**Comparison of Security Modes**

The following table shows a simple overview and comparison between the two security modes:

<table>
<thead>
<tr>
<th></th>
<th>Legacy</th>
<th>NTFS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Native ACL format</strong></td>
<td>NFSv4 ACL with UIDs and GIDs is present on-disk by default. There's no dependency on name services availability for POSIX clients (NFS, Object Access API, FTP) upon successful authentication. Access from SMB client will generate an NTFS ACL with SID as an identity on first successful access to be stored on-disk. Subsequent access from SMB clients will not require name service lookup unless the primary POSIX on-disk ACL has changed.</td>
<td>NTFS ACL with SIDs is present on-disk by default. There's no dependency on name services availability for SMB clients upon successful authentication. Access from POSIX client (NFS, Object Access API, FTP) will generate a POSIX ACL with UIDs and GIDs as an identity on first successful access to be stored on-disk. Subsequent access from POSIX clients will not require name service lookup unless the primary NTFS on-disk ACL has changed.</td>
</tr>
<tr>
<td><strong>ACL Fidelity</strong></td>
<td>Precedence for either NTFS ACLs or POSIX ACLs, based on permissions last applied on files/folders. Please note that the POSIX ACLs will have less fidelity and be more restrictive.</td>
<td>NTFS ACLs security is applied on files/folders to maintain full fidelity NTFS ACLs.</td>
</tr>
<tr>
<td><strong>Native experience</strong></td>
<td>No preferred access.</td>
<td>Near native for SMB clients.</td>
</tr>
<tr>
<td><strong>Inheritance</strong></td>
<td>Default permissions for new files follow Windows rules for SMB clients and POSIX rules for NFS clients.</td>
<td>Default permissions for new files always follow Windows inheritance rules. Windows security descriptor is always present with SIDs on disk for identity.</td>
</tr>
<tr>
<td><strong>Access</strong></td>
<td>R/W access for one protocol and R/O for others for Share Folder.</td>
<td>R/W access allowed for both SMB and NFS clients through Share mode locks.</td>
</tr>
<tr>
<td>Legacy</td>
<td>NTFS</td>
<td></td>
</tr>
<tr>
<td>-------</td>
<td>------</td>
<td></td>
</tr>
<tr>
<td><strong>Setting permission</strong></td>
<td>Only primary R/W protocol is allowed.</td>
<td>Non-SMB clients are not allowed.</td>
</tr>
<tr>
<td><strong>Case sensitivity</strong></td>
<td>File names are case insensitive for SMB clients and case sensitive for NFS clients.</td>
<td>File names are case insensitive as expected by SMB clients.</td>
</tr>
</tbody>
</table>

**Permission Conversion Rules for Converged ACLs**

The following table describes the mapping of system Converged ACL permissions bits to NTFS and POSIX ACLs:

<table>
<thead>
<tr>
<th>Mapping</th>
<th>Converged ACL (3PAR CLI and GUI)</th>
<th>Windows ACLs</th>
<th>POSIX ACLs (perm bits)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read</td>
<td>r ReadData/ListDirectories</td>
<td>ReadData/List Folders</td>
<td>r: ReadFile/ListDir</td>
</tr>
<tr>
<td></td>
<td>n ReadNamedAttributes</td>
<td>ReadExtendedAttributes</td>
<td></td>
</tr>
<tr>
<td>Execute/traverse</td>
<td>x ExecuteFile/TraverseDirectory</td>
<td>ExecuteFile/TraverseFolder</td>
<td>x: ExecuteFile/TraverseDirectory</td>
</tr>
<tr>
<td>Write</td>
<td>w WriteData/CreateFiles</td>
<td>WriteData/CreateFiles</td>
<td>w: Write file object (all four attributes &quot;w,a,t,n&quot; required to have &quot;w&quot; for write o directory.)</td>
</tr>
<tr>
<td></td>
<td>a AppendData/CreateDirectories</td>
<td>AppendData/CreateFolders</td>
<td></td>
</tr>
<tr>
<td></td>
<td>T WriteAttributes</td>
<td>WriteAttributes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>N WriteNamedAttributes</td>
<td>WriteExtendedAttributes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>D DeleteChild (dirs only)</td>
<td>DeleteSubfoldersAndFiles</td>
<td>only required for 'w' for directories and not files</td>
</tr>
<tr>
<td>Special</td>
<td>o ChangeOwnership (of file/dir)</td>
<td>TakeOwnership</td>
<td></td>
</tr>
<tr>
<td></td>
<td>t ReadAttributes</td>
<td>ReadAttributes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>c ReadACLs</td>
<td>ReadPermissions</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C Write ACLs</td>
<td>ChangePermissions</td>
<td></td>
</tr>
<tr>
<td></td>
<td>d Delete object</td>
<td>Delete</td>
<td></td>
</tr>
</tbody>
</table>

**NOTE:**

A conversion from NFS4 ACL to POSIX ACL could result in loss of ACL fidelity. POSIX ACLs are unordered; the order in which the POSIX access checking algorithm considers the entries is determined entirely by the type of the entries, so the entries do not need to be kept in any particular order.

File Shares in Legacy security mode follow NFSv4 inheritance during file or folder creation for an NFS protocol share. All the NFSv4 ACEs in the parent folder that are "inheritable" are brought forward to the child. These inherited ACLs would be converted to POSIX ACLs. The converted POSIX ACLs would be used for permission enforcement during file access. So, it is important that the parent should have meaningful inheritable ACEs so that the child would inherit meaningful permissions. Improper parent ACL can lead to improper permission enforcement.

When file permission modebits are displayed from a POSIX client (for example an NFS client) using the `ls -l` command, it is not possible to perfectly match the NTFS Windows ACL to the modebits. The permissions
and the fidelity of the permissions mask do not match. However, an approximation can be used. The POSIX modebits have 'owner', 'group', and 'other' permission bits.

The 'owner' permissions are based on the combined permissions of the Windows ACE(s) that the file object has for the object's owner and for EVERYONE.

The 'group' permissions are based on the superset of any of the three Windows ACEs that the file object has: the owning group ACEs, additional group ACEs, and non-owner user ACEs. Note that this will result in the group class potentially showing more permissions than what the owning (primary) group of the file object has, something that traditional Linux users might not be used to.

The 'other' permissions are based on any Windows EVERYONE ACEs that the file object has.

The resulting permission mask is converted from Windows 17 bits format to the POSIX 3-bit mask.

**NOTE:**

Sometimes, POSIX clients try to convert the file modebits to a POSIX ACL and display modebits for the owning group based on the group modebits, potentially showing more permissions than are really enforced.

For example, in the output of the `getfacl` command, the ACE could show 'rwx' when the group in actuality only had 'r-x' permissions enforced. This is a known issue with NFS v3 mounts and the `getfacl` command. It is just a display issue on the client, enforcement is not affected.
File Access Auditing

HPE 3PAR File Access Auditing is a robust file access notification framework that is used to manage file access events on HPE 3PAR File Persona. The framework supports event notifications for files and directories that are accessed using NFS and SMB. It logs who, what, when & where information for all file and directories at File Share level. The framework allows integration with third-party applications to achieve regulatory compliance requirements.

File Access Auditing Framework

The File Access Auditing (FAA) framework in File Persona allows clients or end users to collect audit events in two ways, either as an internal consumer of processed log files or as an external consumer using third party ISV applications by streaming events from a message queue exposed over the network.

Internal consumers generate processed log files in raw protocol buffer, XML or JSON. They use a time-based dial or a size-based dial to rotate the logs. External consumers such as ISV software can write their own collection logic and read the live streaming events by connecting to the message queue in the File Persona node over the standard Advanced Message Queuing Protocol (AMQP) port. The internal and external mechanisms are mutually exclusive; that is at any given time only one of the two mechanisms can be enabled per FPG. The FAA framework architecture allows third-party Independent Software Vendors (ISVs) to integrate their solutions with minimal dependency.

Connection to the Rabbit MQ server is authenticated using LDAP or Microsoft Active Directory (AD). Authentication is also available using local users on File Persona. The external consumer can be authorized on a File Persona node using FAA-specific HPE 3PAR CLI commands.

The FAA framework uses Google protocol buffers to serialize the audit events before publishing for real-time consumption by ISV software. The protocol buffer message definitions for the audit events can be downloaded using the supported CLI and can be used for de-serializing the audit events.

When the external option is disabled, the audit log files are written and collected by an internal audit log writer and saved into a specific file share under ".admin" folder, which is configured by the administrator in a specific File Share. Otherwise, one can use HPE 3PAR CLI commands to manage the audit log files.

The FAA framework supports three types of log formats: raw protocol buffer, XML, and JSON-formatted messages. The saved audit logs can be downloaded securely from the SMB or NFS File Share which is configured under the .admin/fileauditing namespace.

NOTE:

File Access Audit logs are stored in the file system/VFS. Make sure there is sufficient space available in the file system for the audit logs to be written. If there is not enough space in the file system the audit logs will not be written.

File Access Auditing - Event Flow

The following figure shows the FAA framework and how the audit log events are consumed by the end users:
Auditing SMB File Shares

The audit events are generated based on the SMB operations that a client (redirector) initiates. In other words, these events reflect the SMB protocol interactions between the client and server.

The following table describes the SMB-specific auditing events that File Persona will be generating. The event parameters column shows the event-specific parameters (common event parameters are listed at the end of the table). The audit configuration setting column shows the CLI configuration setting for the event. Valid values for a configuration setting are "none", "success", "failure" or "all". Success or failure is determined by the status of the operation (success is 0, otherwise failure). Specifying success or failure provides more specific control of whether an event should be generated. For example, open=success will only generate audit events for successful audit operations whereas open=all will generate audit events for both successful and failed operations.

The syntax for creating and modifying SMB File Shares can be found in sections Creating SMB File Shares and Modifying SMB File Shares.

<table>
<thead>
<tr>
<th>Event</th>
<th>Event Specific Parameters (*)</th>
<th>Audit Configuration Settings (CLI) (**)</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>LOGON</td>
<td>logon</td>
<td>logon</td>
<td>Indicates a logon to the SMB server which is part of connecting to a File Share. Note: If there is a logon failure (invalid/user password), the user SID and name will be empty and status = 0. The logon configuration setting is at the VFS level and therefore applies to all File Shares that are configured on the VFS.</td>
</tr>
<tr>
<td>Event</td>
<td>Description</td>
<td>Example</td>
<td>Notes</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>LOGOFF</td>
<td>Indicates a log off from the SMB server.</td>
<td>logoff</td>
<td>Note:</td>
</tr>
<tr>
<td></td>
<td>• Changing this setting while a session has already been established (logon)</td>
<td></td>
<td>• Changing this setting while a session has already been established (logon) has no effect. This setting is only evaluated at the beginning of a session.</td>
</tr>
<tr>
<td></td>
<td>• Depending on the client implementation, the LOGOFF event may not always be</td>
<td></td>
<td>• Depending on the client implementation, the LOGOFF event may not always be sent immediately when the client logs off (example: net use * /del).</td>
</tr>
<tr>
<td></td>
<td>sent immediately when the client logs off (example: net use * /del).</td>
<td></td>
<td>The logoff configuration setting is at the VFS level and therefore applies to all File Shares that are configured on the VFS.</td>
</tr>
<tr>
<td>TREE_CONNECT</td>
<td>Indicates a connection operation to a File Share.</td>
<td>treecconnect</td>
<td>Note:</td>
</tr>
<tr>
<td></td>
<td>By default connections to unknown File Shares or share permission violations</td>
<td></td>
<td>• By default connections to unknown File Shares or share permission violations are not logged. To enable logging for these conditions, specify &quot;global:failure&quot; on the VFS audit settings. The event will be a treecconnect and the File Share name will typically be empty (the treecconnect config setting is ignored in these cases). The treecconnect configuration setting is set at the File Share level.</td>
</tr>
<tr>
<td>TREE_DISCONNECT</td>
<td>Indicates a disconnect operation from a File Share (example: net use * /del).</td>
<td>treedisconnect</td>
<td>Note:</td>
</tr>
<tr>
<td></td>
<td>Certain clients that use SMB v1.0 may not trigger a treedisconnect event when</td>
<td></td>
<td>• Certain clients that use SMB v1.0 may not trigger a treedisconnect event when the client logs off.</td>
</tr>
<tr>
<td>OPEN</td>
<td>Indicates a file/directory open or create operation. The create flags,</td>
<td>open</td>
<td>Note:</td>
</tr>
<tr>
<td></td>
<td>disposition flags and File Share access mask provide additional details of</td>
<td></td>
<td>• For more information, refer to the SMB2 specification. The open configuration setting is set at the File Share level.</td>
</tr>
<tr>
<td></td>
<td>the operation. For example, the disposition flags specify whether the file/dir was opened or created.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>share name</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>object path</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>create flags [SMB2]</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>disposition flags [SMB2]</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>share access mask [SMB2]</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table Continued
<table>
<thead>
<tr>
<th>Operation</th>
<th>Share Name</th>
<th>Object Path</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CLOSE</td>
<td>share name</td>
<td>object path</td>
<td>close</td>
<td>Indicates a file/directory close operation. The close configuration setting is set at the File Share level.</td>
</tr>
<tr>
<td>DELETE_OBJECT</td>
<td>share name</td>
<td>object path</td>
<td>delete</td>
<td>Indicates a file/directory delete operation.</td>
</tr>
<tr>
<td>READ</td>
<td>share name</td>
<td>object path</td>
<td>read</td>
<td>Indicates a file read operation. Note:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Only the first read is reported. All further reads are suppressed until the file is closed and opened again.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>The read configuration setting is set at the File Share level.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>This prevents FAA framework from creating excessive log entries when a single client opens an object and performs many successive read operations to the same object.</td>
</tr>
<tr>
<td>WRITE</td>
<td>share name</td>
<td>object path</td>
<td>write</td>
<td>Indicates a file write operation. Note:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Only the first write is reported. All further writes are suppressed until the file is closed and opened again.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>The write configuration setting is set at the File Share level.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>This prevents FAA framework from creating excessive log entries when a single client opens an object and performs many successive write operations to the same object.</td>
</tr>
</tbody>
</table>

Table Continued
<table>
<thead>
<tr>
<th>RENAME</th>
<th>share name</th>
<th>object path</th>
<th>disposition flags [SMB2]</th>
<th>create flags [SMB2]</th>
<th>rename</th>
<th>Indicates a file/directory rename operation. The rename configuration setting is set at the File Share level.</th>
</tr>
</thead>
<tbody>
<tr>
<td>CHANGE_SECURITY</td>
<td>share name</td>
<td>object path</td>
<td>new owner sid (when OWNER_SECURITY_INFORMATION is set)</td>
<td>new group sid (when GROUP_SECURITY_INFORMATION is set)</td>
<td>changesecurity</td>
<td>Indicates a change in security attributes (owner/group/DACL change). If the owner/group changes, the new owner/group information is reported as part of the event. DACL changes are indicated by the DACL_SECURITY_INFORMATION flag. Security attributes as defined in [SMB2]: OWNER_SECURITY_INFORMATION - 0x00000001 GROUP_SECURITY_INFORMATION - 0x00000002 DACL_SECURITY_INFORMATION - 0x00000004 SACL_SECURITY_INFORMATION - 0x00000008 LABEL_SECURITY_INFORMATION - 0x00000010 ATTRIBUTE_SECURITY_INFORMATION - 0x00000020 SCOPE_SECURITY_INFORMATION - 0x00000040 BACKUP_SECURITY_INFORMATION - 0x00010000 Note: • Object path is null for changes on the drive letter. • This event is not generated for general file/directory property changes, such as modifications to the read-only attribute. The changesecurity configuration setting is set at the File Share level.</td>
</tr>
</tbody>
</table>

(*) Common event parameters are version (current fixed to 1), timestamp (epoch), SMB protocol version (either SMB1 or SMB2 - does not reflect negotiated dialect), user name (including domain (**)), user sid, client IP and SMB operation status (0 == SUCCESS).


(**) Audit configuration settings are case insensitive.

(***) Note: For SMB v1.0 clients that use NTLM for authentication, the user name will not contain the domain portion.

**Example**

The following is a list of examples for each SMB event. Note that these are JSON log entries:
Auditing NFS File Shares

Audit events are generated based on the NFS operations that a client sends to the File Persona. In other words, these events reflect the NFS protocol interactions between client and server. The following table
describes the NFS specific auditing events that File Persona generates. The event parameters column shows the event specific parameters (common event parameters are listed at the end of the table). The audit configuration setting column shows the CLI configuration setting for enabling the event. Unlike SMB access auditing, the configuration for NFS access auditing enables event generation for both error and success scenarios.

**NOTE:**

File Access Auditing can be configured on NFS File Shares within NTFS File Stores. When an NFS File Share uses an NTFS File Store with the "ErrorSuppress=true" option, any chmod operation on the NFS File Share will appear to be successful, even though no chmod operation was executed. This happens because the NTFS File Store is configured with the Error Suppress=true option, errors are inhibited to not break applications. In such a case, auditing for the chmod operation will report success for these operations.

The syntax for creating and modifying NFS File Shares can be found in sections **Creating NFS File Shares** and **Modifying NFS File Shares**.

The following table displays the NFS File Share events and the corresponding parameters:

<table>
<thead>
<tr>
<th>Event</th>
<th>Parameters (*)</th>
<th>Audit Configuration Settings (CLI)</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>OP_OPEN</td>
<td>NFS export path object path</td>
<td>audit_open</td>
<td>Event is generated when a file is opened. Note: There is no event throttling for this event. This event is for NFSv4 only.</td>
</tr>
<tr>
<td>OP_CLOSE</td>
<td>NFS export path object path</td>
<td>audit_close</td>
<td>Event is generated when file is closed. Note: There is no event throttling for this event. This event is for NFSv4 only.</td>
</tr>
<tr>
<td>OP_REMOVE</td>
<td>NFS export path object path</td>
<td>audit_meta</td>
<td>Event is generated when file or directory is removed (example: rm/rmdir).</td>
</tr>
<tr>
<td>OP_RENAME</td>
<td>NFS export path object path</td>
<td>audit_meta</td>
<td>Event is generated when file or directory is renamed.</td>
</tr>
<tr>
<td>OP_CREATE</td>
<td>NFS export path object path</td>
<td>audit_meta</td>
<td>Event is generated when file or directory is created.</td>
</tr>
<tr>
<td>OP_LINK</td>
<td>NFS export path object path</td>
<td>audit_meta</td>
<td>Event is generated when hardlink for a file is created.</td>
</tr>
</tbody>
</table>

*Table Continued*
<table>
<thead>
<tr>
<th>Operation</th>
<th>NFS export path</th>
<th>Event Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OP_READ</td>
<td>path object path</td>
<td>audit_read</td>
<td>Event is generated when a file is read.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Note: All subsequent file reads are suppressed (throttled) for a specific time (currently 10m). Note: A read from a directory is never suppressed. Clients can cache data and avoid reads, thus avoiding a round trip RPC request to the server.</td>
</tr>
<tr>
<td>OP_WRITE</td>
<td>path object path</td>
<td>audit_write</td>
<td>Event is generated when a file is written.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Note: All subsequent writes are suppressed (throttled) for a specific time (currently 10m).</td>
</tr>
<tr>
<td>OP_SETATTR</td>
<td>path object path</td>
<td>audit_attr</td>
<td>Event is generated when file or directory attributes are changed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Note: For NFSv4, file creates will also generate OP_SETATTR events.</td>
</tr>
</tbody>
</table>

**NOTE:** As NFS events are noisy and consumes system resources, only the initial reads and writes are logged and the information about the operation is stored in a hash map. This prevents FAA framework from creating excessive log entries when a single client opens an object and performs many successive read or write operations to the same object.

(*) Common event parameters are timestamp (epoch), NFS version, user/group IDs, client IP, POID (internal id) and NFS operation status (0 == SUCCESS).

**Example**

Following is a list of examples for each event (NFS):
When workload has heavy metadata it could impact the performance of the SMB and NFS protocols. Also, the performance can degrade when File Access Auditing is enabled. This could result in a situation where not all audit events will be logged (up to 5%).

Heavy meta data gets generated when a lot of files are renamed, security parameters are changed or reading/writing/deleting a large number of small files (> 1 million files) takes place (< 32 KB in size) in a short period of time. In all such cases, a large number of open and close operations occur and consequently many events get generated that influence the performance of the system running File Persona. It is recommended that auditing open and close events should be enabled only when necessary or when advised by the ISVs.
Displaying File Access Auditing Policy

To display the details of the file access audit policy (such as client type, authorized user, queue names, exchange name and replication status), issue the following command:

```
showfsaudit pol [-fpg <fpgname>] [-vfs <vfsname>]
```

where,

- **pol**
  - displays the details of the file access audit policy
- **<fpgname>**
  - limits the display to Virtual File Servers (VFS) contained within the FPG.
- **<vfsname>**
  - limits the display to the specified Virtual File Server (VFS).

The following example displays a sample output of file access audit policies defined for a specified VFS in a cluster using the `showfsaudit pol` command:

```
# showfsaudit pol -vfs mtree0
VFS name : mtree0
FPG name : mytestfsp0
Audit host: e83d4baf-8c04-405b-a46f-26d4fe71e0a5
Queue names: nfs,smb
Authorized user: --
Exchange name: hpe.exchange
Replica Enabled: on
ClientType: internal
LogRotationCriteria: 500mb
RetentionPeriod: --
Format: json
```

The following example displays the file access audit policies defined for all VFS' present in a cluster:
# showfsaudit pol

<table>
<thead>
<tr>
<th>VFS name</th>
<th>mtree5</th>
</tr>
</thead>
<tbody>
<tr>
<td>FPG name</td>
<td>mytestfsp5</td>
</tr>
<tr>
<td>Audit host</td>
<td>f375ee6f-970e-474e-a8a4-49f9f51d95ae</td>
</tr>
<tr>
<td>Queue names</td>
<td>nfs,smb</td>
</tr>
<tr>
<td>Authorized user</td>
<td>--</td>
</tr>
<tr>
<td>Exchange name</td>
<td>hpe.exchange</td>
</tr>
<tr>
<td>Replica Enabled</td>
<td>on</td>
</tr>
<tr>
<td>ClientType</td>
<td>internal</td>
</tr>
<tr>
<td>LogRotationCriteria</td>
<td>500mb</td>
</tr>
<tr>
<td>RetentionPeriod</td>
<td>--</td>
</tr>
<tr>
<td>Format</td>
<td>json</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>VFS name</th>
<th>mtree2</th>
</tr>
</thead>
<tbody>
<tr>
<td>FPG name</td>
<td>mytestfsp2</td>
</tr>
<tr>
<td>Audit host</td>
<td>fb50b072-987e-475b-a391-861a85bb4c58</td>
</tr>
<tr>
<td>Queue names</td>
<td>nfs,smb</td>
</tr>
<tr>
<td>Authorized user</td>
<td>--</td>
</tr>
<tr>
<td>Exchange name</td>
<td>hpe.exchange</td>
</tr>
<tr>
<td>Replica Enabled</td>
<td>on</td>
</tr>
<tr>
<td>ClientType</td>
<td>internal</td>
</tr>
<tr>
<td>LogRotationCriteria</td>
<td>500mb</td>
</tr>
<tr>
<td>RetentionPeriod</td>
<td>--</td>
</tr>
<tr>
<td>Format</td>
<td>json</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>VFS name</th>
<th>mtree6</th>
</tr>
</thead>
<tbody>
<tr>
<td>FPG name</td>
<td>mytestfsp6</td>
</tr>
<tr>
<td>Audit host</td>
<td>1d60535d-2ace-4201-9040-b0b236ef97a2</td>
</tr>
<tr>
<td>Queue names</td>
<td>nfs,smb</td>
</tr>
<tr>
<td>Authorized user</td>
<td>--</td>
</tr>
<tr>
<td>Exchange name</td>
<td>hpe.exchange</td>
</tr>
<tr>
<td>Replica Enabled</td>
<td>on</td>
</tr>
<tr>
<td>ClientType</td>
<td>internal</td>
</tr>
<tr>
<td>LogRotationCriteria</td>
<td>500mb</td>
</tr>
<tr>
<td>RetentionPeriod</td>
<td>--</td>
</tr>
<tr>
<td>Format</td>
<td>json</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>VFS name</th>
<th>mtree1</th>
</tr>
</thead>
<tbody>
<tr>
<td>FPG name</td>
<td>mytestfsp1</td>
</tr>
<tr>
<td>Audit host</td>
<td>b6b25d71-3c95-4a23-8b3e-9464bad85d89</td>
</tr>
<tr>
<td>Queue names</td>
<td>nfs,smb</td>
</tr>
<tr>
<td>Authorized user</td>
<td>andad1\u_g1k_1</td>
</tr>
<tr>
<td>Exchange name</td>
<td>hpe.exchange</td>
</tr>
<tr>
<td>Replica Enabled</td>
<td>on</td>
</tr>
<tr>
<td>ClientType</td>
<td>external</td>
</tr>
<tr>
<td>LogRotationCriteria</td>
<td>500mb</td>
</tr>
<tr>
<td>RetentionPeriod</td>
<td>--</td>
</tr>
<tr>
<td>Format</td>
<td>json</td>
</tr>
</tbody>
</table>

## Displaying File Access Auditing Logs

To display a list of file access audit policy logs, issue the following command:

```
showfsaudit log [-fpg <fpgname>] <vfs>
```

**where,**
- **log**
  - displays a list of compressed file access audit policy log files.
- **<fpgname>**
specifies the FPG that the <vfs> belongs to. If the <fpgname> is not specified, the command will locate the FPG based on the specified <vfs>. However, if the <vfs> exists under multiple FPGs, the <fpgname> option must be specified.

- <vfs>
  the VFS for which the file access audit log file details are to be displayed.

**NOTE:**

File access audit log names contain a date which is in the UTC format and the event specific epoch time in audit logs refers to the UTC format.

The following example lists the compressed log files for a specified VFS:

```
# showfsaudit log vfs1
Audit Logs for vfs1
-------------------------------
nfs.log_2017-01-17-10-37-23.zip
```

### Displaying File Access Auditing Global Configuration for SMB

To display the file access audit configuration settings for the SMB protocol at a global level, issue the following command:

```
showfsaudit smb [-fpg <fpgname>] [-vfs <vfsname>]
```

where,

- **smb**
  displays the file access audit global settings for the SMB protocol.
- **<fpgname>**
  specifies the FPG that the <vfs> belongs to.
- **<vfsname>**
  specifies the VFS for which the file access audit global settings are to be displayed.

The following example lists the global details for all the VFS:

```
#showfsaudit smb
VFS   FPG   AuditOptions
----------------------------------
VFS1  FPG1  global:failure,logon:success,logoff:all
VFS2  FPG2  global:failure,logon:all,logoff:failure
```

The following example lists the global details for VFS1:

```
#showfsaudit smb -vfs vfs1
VFS   FPG   AuditOptions
----------------------------------
VFS1  FPG1  global:failure,logon:success,logoff:all
```
Exporting File Access Auditing Google Protocol Buffer Files

To export Google protocol buffer event definition files specific to the NFS and SMB protocols, issue the following command:

```
showfsaudit protobuf -export <client_filepath>
```

where,

- protobuf
  exports the file access audit policy-related and protocol-specific Google protocol buffer event definition files.
- -export
  exports the protocol-specific event definition files.
- `<client_filepath>`
  specifies the target path on the client where the protocol-specific event definition files have to be exported.

The file extension of the `<client_filepath>` must be `.tar`.

The following example lists the Google protocol buffer event definition files:

```
# showfsaudit protobuf -export /home/cluster1_protofiles.tar
File "/home/cluster1_protofiles.tar" successfully exported.
```

Exporting File Access Auditing Logs

Exporting an auditing log file to the .admin directory

To export an active log file to the .admin directory, issue the following command:

```
showfsaudit log -export [-fpg <fpgname>] <vfs>
```

where,

- `<fpgname>`
  specifies the FPG that the `<vfs>` belongs to. If the `<fpgname>` is not specified, the command will locate the FPG based on the specified `<vfs>`. However, if the `<vfs>` exists under multiple FPGs, the `<fpgname>` option must be specified.
- `<vfs>`
  the VFS for which the file access audit log file details are to be exported.

There could be a maximum of nine duplicate events reported into audit log files when the `showfsaudit log -export` operation is performed.

The following example shows how to export an active log file for a specified VFS:
# showfsaudit log -export vfs1
6432

To display the contents of the task:

# showtask -d 6432

<table>
<thead>
<tr>
<th>Id</th>
<th>Type</th>
<th>Name</th>
<th>Status</th>
<th>Phase</th>
<th>Step -------</th>
</tr>
</thead>
<tbody>
<tr>
<td>6432</td>
<td>background_command</td>
<td>getfsaudit_log_task</td>
<td>done</td>
<td>---</td>
<td>2017-06-15</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>15:26:55</td>
<td>EDT</td>
<td>15:27:10</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>n/a</td>
<td></td>
<td>pars svc</td>
</tr>
</tbody>
</table>

Detailed status:
2017-06-15 15:26:55 EDT Created task.
2017-06-15 15:26:55 EDT Updated Executing "getfsaudit_log_task" as 3:48598
2017-06-15 15:26:59 EDT Updated Executing "showfsaudit log -export mtree0"
2017-06-15 15:27:10 EDT Updated File has been exported to /faatest0/mtree0/.admin/fileauditing/activeLogs_2017-06-15-19-26-59.zip
2017-06-15 15:27:10 EDT Completed scheduled task.

Exporting a file access auditing log file to a client path (with options)

To export a specific log file to a client path with options, issue the following command:

```
showfsaudit log -export -file <client_filepath> [-fpg <fpgname>] <vfs> <logfile>
```

where,
- `<logfile>`
  - the log file to be exported.
- `<client_filepath>`
  - specifies the target path on the client machine to where the log file is to be exported.
- `<fpgname>`
  - specifies the FPG that the `<vfs>` belongs to. If the `<fpgname>` is not specified, the command will locate the FPG based on the specified `<vfs>`. However, if the `<vfs>` exists under multiple FPGs, the `<fpgname>` option must be specified.
- `<vfs>`
  - the VFS for which the file access audit log file details are to be exported.

The following example shows how to export a log file to a client path:

```
# showfsaudit log -export -file /home/smblog.zip mtree0
smb_log_2017-06-14-08-26-26.zip
File "/home/smblog.zip" successfully exported.
```

Deleting File Access Auditing Logs

To delete file access auditing compressed logs, issue the following command:

```
setfsaudit log -delete [-fpg <fpgname>] <logfile> <vfs>
```

where,
- `-delete`
  - delete the specified audit log.
- `<fpgname>`
specifies the FPG that the <vfs> belongs to. If the <fpgname> is not specified, the command will locate the FPG based on the specified <vfs>. However, if the <vfs> exists under multiple FPGs, the <fpgname> must be specified.

- <logfile>
  name of the compressed log file to be deleted from the system.

- <vfs>
  specifies the VFS to which the audit log belongs to.

The following example deletes the compressed log file that belongs to vfs1:

```
setfsaudit log -delete -fpg fpg1 activeLogs_2017-06-01-11-29-24.zip vfs1
```

Sample Output:
If the command is successfully executed, no output will be generated. If an error occurs, the error will be displayed.

### Modifying File Access Auditing Client Type

To set the type of client intended for consumption of the file access audit logs, issue the following command:

```
setfsaudit client -type {internal|external} [-fpg <fpgname>] <vfs>
```

where,

- **client**
  the type of client intended for consumption of the file access audit logs.

- **-type {<internal|external>}**
  specifies the type of client that is authorized to consume the file access audit logs. An internal client consumes the stored logs. External clients are third-party ISVs. These clients have a built-in software to consume and analyze the logs. The default is internal client.

**NOTE:** All clients are either internal or external consumers. If a node fails and the client was set for external consumption, the client which is running outside the File Persona domain has to be restarted to continue the external consumption of the audit events.

- **<fpgname>**
  specifies the FPG that the <vfs> belongs to. If this is not specified, the command will locate the FPG based on the specified <vfs>. However, if the <vfs> option exists under multiple FPGs, the <fpgname> must be specified.

- **<vfs>**
  specifies the VFS for which the file access auditing client type needs to be set.

The following example enables the internal client as a consumer for a specified VFS:

```
#setfsaudit client -type internal -fpg fpg1 vfs1
```

Sample Output:
If the command is successfully executed, no output will be generated. If an error occurs, the error will be displayed.

### Modifying File Access Auditing Log Policy

To modify the file access audit log policy for a specified VFS, issue the following command:
setfsaudit logpol [options] <vfs>

where,

• logpol

  configures the log policy for internal audit logs specific to the VFS.

  **NOTE:**

  This command is valid only when the client is set as internal.

  There may be a maximum of nine duplicate events reported into audit log files when the
  setfsaudit logpol operation is performed.

• -size <number>

  specifies the size of the log file to be generated in MBs. Once the log file reaches the size, the raw file
  would be exported to the defined format and compressed. The default size is 100 MB. The supported size
  range is between 50 MB and 500 MB.

• -time <number>

  specifies the time in minutes for which log file is to be generated. When the log file is created, the time
  counter is started.

• -retention number[m|d|h]

  Retention is either a number of logs to keep, or duration in months/days/hours to keep log files. When the
  duration is exceeded, the compressed log file is deleted. Auto deletion of log files is disabled by default. If
  only a number is specified, the log file count is -retention number (maximum 50). After the specified
  number is reached, the oldest log file will be removed. Maximum possible values for duration in months/
  days/hours are 1m/30d/720h respectively. 1 month is equivalent to 30 days.

  **NOTE:**

  When the log rotation policy with retention enabled (-retention != 0), there could be a delay of
  up to a maximum of 5 minutes of audit log file accumulation that meet the retention criteria before the
  policy acts on it.

• -format {proto|xml|json}

  specifies the supported log file formats; {proto|xml|json}. The {proto} format generates the audit
  events stored in the Google protocol buffer binary format. The audit client should use the
  {proto} definition file and decode the binary format to a desired format. See showfsaudit protobuf for more
  details. The default format is json.

  **NOTE:**

  Whenever the -format changes, the log file rotates and the entries are written on a new log file.

• <fpgname>

  specifies the FPG that the <vfs> belongs to. If the <fpgname> is not specified, the command will locate
  the FPG based on the specified <vfs>. However, if the <vfs> option exists under multiple FPGs, the
  <fpgname> must be specified.

• <vfs>

  specifies the VFS for which the file access audit logs are to be modified.

The following example enables and overwrites the existing file access audit log policy with a log file size of 50
MB, retention period of seven days and log format as XML:
Modifying File Access Auditing Message Replication

To mitigate the risk of losing critical audit events in case of system crash, a replica of the event is maintained in a queue on a partner node. Since these audit events copied to the partner node are not synchronized to the primary audit event queue, there could be scenario that the client may consume duplicate events. This feature allows users to configure a certain degree of crash durability for the most recent events and provides mitigation to critical event loss during a crash scenario. However, enabling the replica feature does not guarantee preservation of all single in-flight events during crash, including memory events that might have happened before a crash.

NOTE:
As each audited event consumes system resources, it is recommended not to turn on the replication feature on all the FPGs and enable it only on FPGs where recovering the events after a crash is critical to the business use case.

To enable or disable replicating a message queue to a partner node, issue the following command:

```
setfsaudit replica -enable {true|false} [-fpg <fpgname>] <vfs>
```

where,
- **-enable {true|false}** enables or disables the replication of the message queue. Default is disabled.
- **<fpgname>** specifies the FPG that the <vfs> belongs to. If the <fpgname> is not specified, the command will locate the FPG based on the specified <vfs>. However, if the <vfs> option exists under multiple FPGs, the <fpgname> must be specified.
- **<vfs>**

The <vfs> for which replication is to be enabled/disabled.

The following example enables replication for vfs1 related audit logs:

```
#setfsaudit replica -enable true -fpg fpg1 vfs1
```

Sample Output:
If the command is successfully executed, no output will be generated. If an error occurs, the error will be displayed.

Modifying File Access Auditing Global Configuration for SMB

To modify or set the file access audit configuration settings for the SMB protocol at a global level (per VFS), issue the following command:

```
setfsaudit smb -audit {operation1:value[,operation2:value]...} [-fpg <fpgname>] <vfs>
```

Modifying File Access Auditing Message Replication
where,

• **smb** modifies or sets the file access audit global settings for the SMB protocol.

  -audit `{operation1:value[,operation2:value]...}` specifies the events to be audited at a global level for the SMB protocol. The possible operations are {logon, logoff, global}. The supported values are {success, failure, none (no logging), all (logging for both success and failure)}. By default, all operations are set to none.

• **<fpgname>** specifies the FPG that the <vfs> belongs to. If the <fpgname> is not specified, the command will locate the FPG based on the specified <vfs>. However, if the <vfs> exists under multiple FPGs, the <fpgname> must be specified.

• **<vfs>** specifies the VFS for which the file access audit global settings are being modified or set.

The following example enables the auditing event in vfs1 as a successful logon operation (SMB protocol):

```bash
#setfsaudit smb -audit logon:success vfs1
```

**Sample Output:**

If the command is successfully executed, no output will be generated. If an error occurs, the error will be displayed.

---

### Modifying File Access Auditing User Authorization

The external consumers (ISV auditing software applications) get access to the AMQP queues by issuing the following command:

```bash
setfsaudit user [-delete] [-fpg <fpgname>] <username> <vfs>
```

**where,**

• **user** adds or removes user authorization to access the AMQP queues. By default, the add operation will be performed.

  **NOTE:**

  One audit user per audit host is allowed. Adding a new audit user to an audit host will overwrite the existing user.

• **-delete** removes the user's authorization to the file access audit log messages.

• **<fpgname>** specifies the FPG that the <vfs> belongs to. If the <fpgname> is not specified, the command will locate the FPG based on the specified <vfs>. However, if the <vfs> exists under multiple FPGs, the <fpgname> must be specified.

• **<username>** name of the user that needs to be added or removed for authorization.

• **<vfs>** specifies the VFS for which the user has to be authorized to access the audit logs.

**Examples**
The following example authorizes LOCAL_CLUSTER user Administrator to access vfs1 related audit logs:

```
# setfsaudit user "Administrator@LOCAL_CLUSTER" vfs1
```

The following example authorizes an AD user user2 to access vfs1 related audit logs:

```
# setfsaudit user 2008ad.lab\user2 vfs1
```

The following example unauthorizes local user user1 from accessing vfs1 related audit logs:

```
# setfsaudit user -delete user1 vfs1
```

The following example authorizes LOCAL_CLUSTER user administrator to access vfs1 related audit logs:

```
# setfsaudit user "Administrator@LOCAL_CLUSTER" vfs1
```
Storage Quotas

User and group quotas are set in the Virtual File Server (VFS). Whereas File Store quotas are set at the File Store level. The maximum number of quotas that can be set for a VFS is 2,000.

Hard quotas are enforced immediately and halt any additional writes. Soft quotas have a grace period, which is a time that they are allowed to be exceeded before they are enforced. The grace period associated with soft quotas can be specified with the igrace and bgrace parameters in the VFS, as described in Creating Virtual File Servers on page 53.

Displaying Storage Quota Settings

To display usage quotas for users, groups or File Stores, issue the following command:

```
```

where,

- `<username>` specifies the name of the user for which you are displaying quota information.
- `<gname>` specifies the name of the group for which you are displaying quota information.
- `<fstore>` specifies the name of the File Store for which you are displaying quotas information.
- `<vfs>` specifies the name of the VFS associated with the objects for which you are displaying quota information.
- `<fpg_name>` specifies the name of the FPG to which the VFS belongs.

File Formats

When the quota entities are set for the first time, the import format A and B should be used. The K format should be used when the quota entities need to be displayed in greater detail, not when importing quotas. The K format should be used to import a modified quota only when the {FPG_id},{generation_id},{id}, {VFS_id} information is specified correctly. K format files can be converted to an A or B format file.

When you import quota settings from a file, the import file must use one of the following formats:

- **A** format specifies settings based on a user, group or File Store ID value:

  ```
  A,{type},{block_hardlimit},{block_softlimit},{inode_hardlimit}, {inode_softlimit},{id}
  ```

- **B** format specifies settings based on a user, group or File Store name value:

  ```
  B,{type},{block_hardlimit},{block_softlimit},{inode_hardlimit}, {inode_softlimit},{name}
  ```

**NOTE:**

All three formats; A, B and K, have three values for the `type` field: 0, 1, and 2. The values 0, 1, and 2 indicate user, group and File Store respectively.

Example of an A Format file
Example of a B Format file

B,0,2048,1024,12,10,"u1"
B,1,2048,1024,12,10,"g1"
B,2,2048,1024,12,10,"s1"

Converting a K format file to an A format file

The following procedure describes the steps required to convert a K format file to an A format file.

1. Replace the letter K with the letter A.
2. Remove all the values after inode_softlimit from the K format line except the quota entity id {user/group/file_store id}.

Refer to the following examples and apply the changes as suggested:

Use Case 1:

K, 2,10485760000,9437184000,1000000000,80000000,0,0,7eac25c4-4b1d-4d79-8b13-9fce65fe5026,1,3,0,2
to:
A,2,10485760000,9437184000,1000000000,80000000,3

Use Case 2:

K, 0,1048576000,94371840,1000000,800000,0,0,7eac25c4-4b1d-4d79-8b13-9fce65fe5026,1,204605,0,2
to:
A,0,1048576000,94371840,1000000,800000,204605

Use Case 3:

K, 1,1048576000,943718400,10000000,80000000,0,0,7eac25c4-4b1d-4d79-8b13-9fce65fe5026,4,100001,0,2
to:
A,1,1048576000,943718400,10000000,80000000,100001

Converting a K format file to a B format file

The following procedure describes the steps required to convert a K format file to a B format file.

1. Replace the letter K with the letter B.
2. Remove all the values after inode_softlimit from the K format line and write the quota entity name {user/group/file_store name}. Replace the entity id with entity name {user/group/file_store name}.

Refer to the following examples and apply the changes as suggested:
### Setting Storage Quotas

To set the usage quotas for users, groups, or File Stores, issue the following command:

```
```

where,

- `<fpg_name>` specifies the name of the FPG to which the VFS belongs.
- `<username>` specifies the name of the user for which you are setting the quota.
- `<groupname>` specifies the name of the group for which you are setting the quota.
- `<fstore>` specifies the name of the File Store for which you are setting the quotas.
- `<soft_capacity_limit>` specifies an integer value in MB for the soft capacity storage quota. The maximum value is the maximum size supported by FPG in MiB.
- `<hard_capacity_limit>` specifies an integer value in MB for the hard capacity storage quota. The maximum value is the maximum size supported by FPG in MiB.

**IMPORTANT:**

The `<soft_capacity_limit>` option specifies the storage quota in MB.

- `<hard_capacity_limit>` specifies an integer value in MB for the hard capacity storage quota. The maximum value is the maximum size supported by FPG in MiB.
IMPORTANT:
The `<hard_capacity_limit>` option specifies the storage quota in MB.

- `<soft_file_limit>`
  specifies the soft limit for the number of stored files. The maximum value is 250,000,000. A value of 0 specifies there is no limit.
- `<hard_file_limit>`
  specifies the hard limit for the number of stored files. The maximum value is 250,000,000. A value of 0 specifies there is no limit.
- `-clear`
  clears the quotas for the specified objects.
  - `-uid <uid>`
    option specifies the user id of the quotas to be deleted. This is supported only with -clear.
  - `-gid <gid>`
    option specifies the group id of the quotas to be deleted. This is supported only with -clear.

NOTE:
Options `-uid`, `-gid`, `<username>` and `<groupname>` are mutually exclusive.

- `<vfs>`
  specifies the name of the VFS associated with the objects for which you are setting the quotas.

NOTE:
If a user’s quota has exceeded on a VFS, the user will not be permitted to write on the FTP Share and the connection to the server will automatically close while trying to write on the FTP Share. The error message received by user depends on the client behavior. A user using cURL as the FTP client will get an error message saying "Select/poll returned error". For all other clients the connection will be closed. Check with your Administrator for the specific error message based on the client you are using.

WARNING:
Setting hard storage usage limit for a roaming profile user, and then exceeding the quota might lead to a loss of data synchronization between the Windows client and the SMB share.

Archiving and Restoring Storage Quota Settings

Quota settings can be archived to make bulk edits to the settings and then imported again. This may be a more efficient alternative than using the `setfsquota` command for modifying a large number of quotas at once.

Archiving Usage Quotas

To archive the quotas for a VFS, issue the following command:
```
setfsquota [-fpg <fpg_name>] -archive [-vfs <vfs>]
```

where,
- `<fpg_name>`
specifies the name of the FPG to which the VFS belongs.

- **-archive**

stores the quota information associated with the VFS in a file in the .admin File Store.

The quota capacity limits in the export archive file created by the `setfsquota -archive` command is specified in KB.

- **<vfs>**

specifies the name of the VFS associated with the quotas you are archiving.

The exported archive file is located in the following directory:

`/examplefpg/examplevfs/.admin/Quotas`

### Importing quota settings from an FPG or a VFS

If you wish to import quota settings from an FPG and a VFS and apply them to another FPG and VFS, the export file must use the following format:

```
V,{major version},{minor version}
K,{type},{block_hardlimit},{block_softlimit},{inode_hardlimit},{inode_softlimit},
   {block_grace_time},{inode_grace_time},{FFP_id},{generation_id},{id},
   {over_limits},{VFS_id}
F,{FFP_id},{FFP_name},{block_grace_time},{inode_grace_time},{VFS_id}
```

The following is an example showcasing the output of a **K** format file:

```
V,1,0 K,0,2048,1024,12,10,0,0,bd436b92-e919-41b8-95ec-b0211258202a,1,4001,0,3
K,1,2048,1024,12,10,0,0,bd436b92-e919-41b8-95ec-b0211258202a,1,5001,0,3 K,
2,2048,1024,12,10,0,0,bd436b92-e919-41b8-95ec-b0211258202a,1,5,0,3
F,bd436b92-e919-41b8-95ec-b0211258202a,examplefpg,700,300,3
```

The **V** format specifies the version number.

The **K** format appears for each user, group or File Store that are assigned a quota.

The **F** format is created only when the default grace period is changed to some other value.

### Restoring and Importing Usage Quotas

You can manage User and Group quotas for the File Persona on a storage system.

#### Restoring Usage Quota

To restore the quotas for a VFS, issue the following command:

```
setfsquota -restore <file> <fpg_name> <vfs_name>.
```

where,

- `<file>`

stores the quota information from the FPG and VFS.

- `<fpg_name>`

specifies the name of the FPG to which the VFS belongs.

- `<vfs>`

specifies the name of the VFS associated from which you are restoring the quotas.

This restores the quota settings located in `/<fpg_name>/<vfs_name>/admin/Quotas`

#### Importing Usage Quota
To import the quotas from one VFS and apply them to another VFS, issue the following command:

```
setfsquota -restore <import_file> <fpg_name> <vfs_name>
```

where,

- `<import_file>` applies the quota information stored in the specified archive file to the FPG and VFS.
- `<fpg_name>` specifies the name of the FPG to which the VFS belongs.
- `<vfs>` specifies the name of the VFS associated to which you are applying the quotas.

**NOTE:** If a user’s quota has exceeded on a VFS, the user will not be permitted to write on the FTP Share and the connection to the server will automatically close while trying to write on the FTP Share. The error message received by user depends on the client behavior. A user using cURL as the FTP client will get an error message saying "Select/poll returned error". For all other clients the connection will be closed. Check with your administrator for the specific error message based on the client you are using.

**Managing User Quotas using SSMC:**

- From the main menu, select **File Persona > Virtual File Servers**.
- On the list pane, select the Virtual File Server, and then select **Manage quotas** on the **Actions** menu.
- Click the **Import** button to import the usage quotas or the **Export** button to export usage quotas.
- Follow the instructions on the dialog that opens.
Antivirus Scanning

File Persona provides easy and centralized management of user data for home directory consolidation and group or corporate shares on HPE 3PAR StoreServ storage system. Most storage vendors implement an external dedicated server for running a Virus Scan Engine (VSE) to scan the files stored on the storage system and to offload the virus scanning task to an external server. File Persona also integrates with external antivirus servers running a Virus Scan Engine (VSE) to provide the on-access or on-demand scanning of the files stored in the HPE 3PAR StoreServ array.

HPE 3PAR StoreServ storage system can be managed via a truly converged streamlined management interface called HPE 3PAR StoreServ Management Console (SSMC). The SSMC manages both blocks and files together.

The HPE 3PAR CLI command `setfsav` is used to manage antivirus functions for HPE StoreServ File Persona.

The HPE StoreServ Storage system supports external Virus Scan Engines (VSEs) running McAfee, TrendMicro, Symantec, Kaspersky and Sophos antivirus software.

Antivirus Scan Integration

Antivirus software cannot be installed natively on enterprise-class storage running a non-Microsoft® operating system. Any files accessed by the users that require virus scanning are sent over the network to external servers running Microsoft Windows® and a third-party vendor’s antivirus software designed to offer virus scanning services to storage systems. These servers are referred to as Virus Scan Engines, or simply VSEs.

Antivirus scanning on File Persona can use the VSEs to scan files dynamically as they are opened or closed. This scan is called an on-access scan. It can also provide scheduled or on-demand scans for a given File Store or virtual file server (VFS). In general, both of these optional approaches can and should be used.

File Persona running on the HPE 3PAR StoreServ system determines which files need to be scanned through scheduled tasks or user actions such as on file open and file close from SMB clients as well as on file read from NFS and Object Access application programming interface (API) clients. It will also record the results of the scan and quarantine any infected files for subsequent review and action by the administrator. Any file changes and file scans are tracked by the antivirus function of File Persona. After a file has been scanned, it is not scanned again until it is modified or until the virus definitions have been updated. If no VSEs are available to perform the scan, HPE 3PAR StoreServ can allow or deny access to the files based on the policy configured for VSE unavailability.

Antivirus Scanning

The following figure describes the antivirus scanning process:

![Figure 3: Antivirus Scanning](image)

The following steps describe the scanning process:
1. The antivirus VSE is set up and the 3PAR is scanned for policies.
2. The client requests an open (read) or close (write) of an SMB file or read for an NFS or Object Access API file.
3. The storage system determines if the file needs to be scanned based on the antivirus policies.
4. The VSE scans the file and reports the scan results back to the StoreServ system.
5. If no virus is found, then access will be allowed to the file.
6. If a virus is found, then access will be denied to the SMB client, permission will be denied to the NFS client, and transfer will be closed to the Object Access API client. The file is then quarantined.

**Antivirus Installation and Configuration**

The minimum system requirements for installing and running the Virus Scan Engines (VSEs) are set by the third-party antivirus vendors. Consult the vendor-specific documentation for their system requirements.

Virtualized VSEs may be used. Consult the vendor-specific documentation for the system requirements when running virtualized scan engines. The recommendations in this document apply to both physical and virtualized VSEs.

For Sophos and Kaspersky antivirus, the VSE should be a physical machine with internet connectivity. For optimum performance, it is required to tune a few parameters in the SAVDI config file. The following parameters need to be changed:

- Channel: ICAP
- Port: 1344
- Service: AVSCAN
- Allow204: Yes
- Keepalive: Yes
- Threadcount: 32
- Maxqueuedsessions: 1024

**NOTE:**
For TrendMicro antivirus, the file size limit is 2GB. File size 2GB and beyond will not be scanned by TrendMicro. For Kaspersky antivirus, the scan size limitation is 4GB.

**Antivirus Software Vendor Configuration**

A single antivirus vendor can be associated with each HPE 3PAR StoreServ system (2-node or 4-node). The antivirus vendor type can be managed using the HPE 3PAR CLI or SSMC. The first step in configuring the antivirus scanning is configuring the vendor, followed by the Virus Scan Engine configuration (VSE).

**Modifying the Antivirus Vendor Type**

To set a vendor type on the HPE 3PAR StoreServ system, follow the steps below in order:

1. Modify the vendor type to NA for every VFS on the HPE 3PAR StoreServ System, using the following command:
   ```
   setfsav pol -vendor NA <vfs>
   ```
2. Remove all the previously configured VSEs (if any) using the following command:
   ```
   setfsav vse
   ```
3. Add the first VSE for the new vendor type before setting the new vendor type. Use the command following command:
   ```
   setfsav vse +<IP address>:<port>
   ```
   The default `<port>` is 1344.
4. Set the vendor type for a specific VFS using the following command:
   ```
   setfsav pol -scan enable -vendor <VENDOR> <vfs>
   ```
Adding and Deleting a VSE using HPE 3PAR CLI

To add or delete a VSE, issue the following command:

```
setfsav vse +/-<IP_address>:<port>
```

where,

- `+/-` adds (+) or removes (−) the specified VSE.
- `vse` specifies the virus scan engine.
- `<IP_address>:<port>` specifies the IP address and port number of an external virus scan engine (VSE). The default port number for a VSE is 1344, since it uses the ICAP protocol. The port is optional when using the `remove vse` command.

**NOTE:**

A warning message is displayed when a port number to remove a VSE is specified:

"Warning: Port number not allowed while removing VSE."

A VSE cannot be removed if it is the last VSE and the VFS is associated with the a vendor. In such cases, we need to modify the VFS policy and assign the vendor type to "NA" and only then the VSE can be removed.

---

Adding a VSE using SSMC

- On the main SSMC menu, select **File Persona > Persona Configuration**.
- On the list pane, select the File Persona, and then select **Configure File Persona** on the **Actions** menu.
- On the dialog that opens, select the **Advanced options** check box.
- On the **Antivirus Settings** panel, under **Antivirus Servers**, click **Add**.
- Follow the instructions on the dialog that opens.

Deleting a VSE using SSMC

- On the main SSMC menu, select **File Persona > Persona Configuration**.
- On the list pane, select the File Persona, and then select **Configure File Persona** on the **Actions** menu.
- On the dialog that opens, select the **Advanced options** check box.
- On the **Antivirus Settings** panel, under **Antivirus Servers**, click **Delete**.
- Follow the instructions on the dialog that opens.

---

Initiating an Antivirus Scan

It is not always feasible to use on-access file scanning on a daily basis. Infrequently accessed files are infrequently scanned, which increases the chances of them becoming infected. To avoid this risk, it is therefore recommended that the Virtual File Server (VFS) should be scanned. The scanning could be initiated to run instantly or could be scheduled as a recurring event. Use the SSMC or the HPE 3PAR CLI to schedule on-demand scanning.

When reverting to a prior version, unsupported vendors will throw an error. Customers are advised to switch to a supported vendor before reverting to a prior version.
NOTE:
Antivirus scans are background processes and take time to run. When running an on-demand or scheduled antivirus scan for a large set of files, the expected processing rate is no greater than 2 million files per day, depending on the load. If an unscanned file is read by a user before the scan gets completed, it is automatically scanned on access before the data is returned to the user.

An antivirus scan can not be initiated on a File Provisioning Group that is full.

The VSE should be added to the cluster and the configured antivirus policy/policies on the VFS or File Store. Also, the policy can be set at the VFS level but can be overridden at the File store level.

TIP:
Schedule antivirus scans periodically in addition to dynamic scans (on-demand scans) to increase the antivirus protection. It is recommended to schedule the scan tasks outside of peak usage times.

Starting an Antivirus Scan on a VFS or File Store
To start an antivirus scan on a Virtual File Server (VFS) or a File Store, issue the following command:

```
startfsav scan [-fpg <fpgname>] [-fstore <fstore>] <vfs_name>
```

where,

- `scan` starts an antivirus scan.
- `-fpg <fpg_name>` specifies the name of the File Provisioning Group in which the VFS was created.
- `-fstore <fstore_name>` specifies the File Store name, using up to 31 characters.
- `<vfs_name>` specifies the Virtual File Server (VFS) name (using up to 31 characters) on which the antivirus scan is to start.

Initiating an Antivirus Scan from a File Stores screen

- On the main SSMC menu, select File Persona > File Stores.
- On the list pane, select the Actions menu.
- Select the Create antivirus scan
- Follow the instructions on the dialog that opens.

Initiating an Antivirus Scan from a Virtual Files Servers screen

- On the main SSMC menu, select File Persona > Virtual Files Servers.
- On the list pane, select the Actions menu.
- Select the Create antivirus scan
- Follow the instructions on the dialog that opens.

Pausing and Stopping Antivirus Scans

Stopping an Antivirus Scan
To stop an antivirus scan on a Virtual File Server (VFS) or File Store, issue the following command:

```
stopfsav scan [-fpg fpgname] [-fstore fstore] <vfs_name> <scan_id>
```

where,
Pausing an Antivirus Scan

To pause an antivirus scan on a Virtual File Server (VFS) or File Store, issue the following command:

```
stopfsav scan [-pause] [-fpg fpgname] [-fstore fstore] <vfs_name> <scan_id>
```

where,

- `[-pause]` pauses, rather than stops, the specified scan.
- `[-fpg fpgname]` specifies the name of the File Provisioning Group in which the VFS was created.
- `[-fstore fstore]` specifies the File Store name, using up to 31 characters.
- `<vfs_name>` specifies the name of the Virtual File Server (VFS).
- `<scan_id>` specifies the scan task identifier, as provided by `startfsav scan` command, and displayed by the `showfsav -scan` command.

Stopping an Antivirus Scan from the VFS screen using SSMC

From the main menu, select File Persona > Virtual File Servers.

On the list pane, select the Virtual File Server, and then select Manage existing antivirus scans on the Actions menu.

To specify that a running task is to be stopped, click Stop. In the Task State column, the state will change to stop.

Click OK to start the action and close the dialog.

Stopping an Antivirus Scan from the File Store screen using SSMC

Tip: Tasks for working with File Stores are considered advanced tasks. If the File Stores screen is not listed in the main menu, you can add it from the Global Settings screen.

From the main menu, select File Persona > File Stores.

On the list pane, select the File Store, and then select Manage existing antivirus scans on the Actions menu.

To specify that a running task is to be stopped, click Stop. In the Task State column, the state will change to stop.

Click OK to start the action and close the dialog.

Resuming an Antivirus Scan on a VFS or File Store

To resume an antivirus scan on a Virtual File Server (VFS) or a File Store, issue the following command:
startfsav scan [-resume <scan_id>] [-fpg <fpgname>] [-fstore <fstore>] <vfs_name>

where,

- **-resume <scan_id>**
  - resumes a paused scan. The `scan_id` specifies the scan task identifier and it corresponds to an ongoing scan that is in a paused state. It is provided by the `startfsav scan` command, and can be displayed using the `showfsav -scan` command.

- **-fpg <fpg_name>**
  - specifies the name of the File Provisioning Group in which the VFS was created.

- **-fstore <fstore_name>**
  - specifies the File Store name, using up to 31 characters.

- **<vfs_name>**
  - specifies the Virtual File Server (VFS) name (using up to 31 characters) on which the antivirus scan is to be resumed.

### Resuming an Antivirus Scan from the VFS screen using SSMC

- From the main menu, select **File Persona > Virtual Files Servers**.
- On the list pane, select the **Virtual Files Servers**, and then select **Manage existing antivirus scans** on the **Actions** menu.
- To specify that a paused scan is to be resumed, click **Resume**. In the Task State column, the state will change to resume.

### Resuming an Antivirus Scan from a File Store screen using SSMC

- From the main menu, select **File Persona > File Stores**.
- On the list pane, select the **File Stores**, and then select **Manage existing antivirus scans** on the **Actions** menu.
- To specify that a paused scan is to be resumed, click **Resume**. In the Task State column, the state will change to resume.

### Displaying Status for Antivirus Scans, Policies, and Quarantined Files

To display a list of existing virus scanning engines by IP addresses, including their port numbers, using the HPE 3PAR CLI, issue the following command:

```
showfsav
```

⚠️ **CAUTION:**

Do not use the `setfsav vse` command without any options to display virus scan engines. Doing so will clear the list of virus scanning engines.

### Displaying the status for antivirus scans using SSMC

- From the main menu, select **File Persona > File Persona Configuration**
- Select **Antivirus Settings**.

### Configuring Antivirus Scanning Policies

To configure antivirus policies using the HPE 3PAR CLI, issue the following command:

```
setfsav pol [-scan {enable|disable|inherit}] [-vendor <vendor_name>] [-fileop {open|openclose|inherit}] [-unavail {allow|deny|inherit}] [-excludesize {<size>}]```
The scan option specifies the state of the antivirus service for the VFS/File Store. The following are the possible values:

- enable
  enables the antivirus scan.
- disable
  disables the antivirus scan.
- inherit
  inherit the scan setting from the VFS.

The vendor option sets the vendor name. For example, the vendor name can be set to SYMANTEC/ MCAFEE/TRENDMICRO/SOPHOS/KASPERSKY. The vendor cannot be set/overridden at File Store level.

The fileop option specifies the policy that determines which file operation triggers the antivirus scan. The policies could be as follows:

- open
  scans on file open.
- openclose
  scans on file open and file close.

\[\text{\textbf{CAUTION:}}\]
Please remember when selecting the antivirus scan policy the -fileop openclose option can cause file open failures for files reopened shortly after the files are closed.

- inherit
  option inherits the fileop setting from VFS.

If a fileop policy is not specified, the default is open when applied to a VFS and inherit when applied to a File Store.

The unavail option specifies the scan policy to determine how targeted file operations are handled when an external Virus Scan Engine (VSE) is not available. It can also be used when the file cannot get scanned.

- allow
  allows all operations triggering scans to run to completion.
- deny
  blocks all operations triggering scans and returned with an error.
- inherit
  inherits the unavail setting from VFS.

If an unavail policy is not specified, the default is allow when applied to a VFS, and inherit when applied to a File Store.

The excludesize option specifies the size of files to be excluded from the antivirus scan.
The `excludesize` option excludes all files larger than the specified size (MB). The value of size is an integer from 0 to 2,147,483,647. If this option is not specified or size is 0, all the files will be included in the antivirus scan. If `inherit` is specified, the `excludesize` setting will be inherited from VFS.

**NOTE:**
- When using Symantec VSEs, attempting to scan files larger than 2GB may cause the scan engine to be reported as **DOWN**. To avoid this issue, a policy can be set to exclude scanning files larger than 2GB with the `excludesize` option of the `setsav pol` command. When using Sophos VSEs, if we are not adjusting the tunable parameters (`threadcount`, `maxqueuedsessions` and `Allow204`), scan engine can be reported as **DOWN**.
- For TrendMicro antivirus, the file size limit is 2GB. File size 2GB and beyond will not be scanned by TrendMicro. When using TrendMicro set the `excludesize` policy to 2GB to avoid scanning failures.
- When using Kaspersky VSEs, the file size limit is 4GB. Anything more than that is not supported.

- **-excludeext** `<ext>[,<ext>,...] | inherit`  
The `excludeext` option excludes all files having a specified extension. If this option is not specified or `ext` is `'`, all files will be included in the antivirus scan. If "inherit" is specified, the `excludeext` setting will be inherited from VFS.
- **-inheritall**  
The `inheritall` option inherits all the settings from the VFS for the specified File Store, overriding any previous settings in File Store. Only valid when `-fstore` option is specified.

- **-fstore** `<fstore_name>`  
The `fstore` option specifies the File Store name, using up to 31 characters.
- **-fpg** `<fpg_name>`  
The `fpg` option specifies the name of the FPG in which the VFS was created.
- **<vfs_name>**  
The `vfs_name` option specifies the name of the VFS.

### Configuring antivirus policies using SSMC:
- On the main SSMC menu, select **File Persona > Virtual File Servers screen** > **antivirus**.
- Select the **Actions** menu, and then select **Modify antivirus policy**.
- Follow the instructions on the dialog that opens.

## Managing Quarantine Settings and Files

When a virus is detected in a file by the VSE, the HPE 3PAR StoreServ modifies an extended attribute of the infected file and marks it as **quarantined**. It also prevents access to the file until the storage administrator moves, deletes or resets the file. The quarantined file can be managed using the HPE 3PAR CLI or the SSMC.

Several actions could be taken on the quarantined files such as reset, move or delete. The storage administrator can perform the quarantine operations (reset/move/delete) on all the infected files found within a VFS or on all infected files found within a File Store or on a selective set of infected files found within a VFS or File Store. All quarantine operations are performed either at the VFS or the File Store level. The quarantined files only can be moved to a default location with a timestamp in the `.admin` folder of the Virtual File Server (VFS) or the files can be deleted altogether. Additionally, the quarantine flag can be reset on all the quarantined files on the Virtual File Server. Other actions can be taken as well, such as to clear the quarantined file count and to export a list of quarantined files.
The HPE 3PAR CLI command `setfsav quar exportlist` can export 3,000 quarantined files at a time. The list of the quarantined files is located at:

`/<fpg>/<vfs>/admin/AV/Quarantine/quar_<fpg>_<vfs>.txt`

or

`/<fpg>/<vfs>/admin/AV/Quarantine/quar_<fpg>_<vfs>_<fstore>.txt`

depending on the output of the `setfsav quar exportlist` command.

**NOTE:**
Please make sure that the set of 3,000 quarantined files must be reset, moved, or deleted from any previous exports before exporting another set of 3,000 files.

Selective bulk quarantine operation is also available. Operations such as move, reset and delete is available for a bulk of files from the set of 3000 files obtained from `exportlist` operation. For this, edit the file located in the Quarantine folder, remove the entries of the files that don’t need to moved, reset or deleted and perform the required quarantine operation.

**NOTE:**
There is an upper limit on the `inode` quota in the system. When the limit is reached, the user will get a warning. The user is supposed to perform further action, such as remove files or increase the limit to make quota available. When a file is scanned and is found infected, a quarantined link pointing to the infected file is created and the permission of the file is changed to `access denied`. If the creation of the quarantine link fails due to limitations on quota, the file is not stamped as scanned. Since the file is not marked as scanned, the file system will trigger the file for scanning whenever accessed till the quarantined link to the file has been created successfully and has been marked as stamped.

**Quarantine operations - Exporting, Resetting, Moving, Deleting and Count Clearing Infected Files**

There is a set of quarantine operations that can be applied on infected files: `export`, `reset`, `move`, `delete` and `clear count`. The `setfsav quar` command is used to perform the various quarantine operations. The syntax of the command is as follows:

```
setfsav quar {exportlist|move|reset|delete|clearcount} [-fpg <fpg_name>] [-fstore <fstore>] [-quar_file <filepath>] <vfs>
```

where,

- `quar`
  
  specifies the management of quarantined files.

- `<fpg_name>`
  
  specifies the name of the FPG to which the VFS belongs to.

- `<fstore>`
  
  specifies the name of the File Store.

- `quar_file <filepath>`

  contains the file path of the container file. The `quar_file` is used to provide a subset of the quarantined files.
NOTE: When using the `quar_file` option, quarantine operations such as Move/Delete/Reset can be performed on a subset of infected files specified inside the container file. Each infected file inside the container file is delimited by a new line character. The container file should be present in the `/fpgname/vfsname/.admin/AV/Quarantine` location. Container file is formed based on the `exportlist quarantine` operation. The `quar_file` is called a container file.

- `<vfs>`
  specifies the name of the Virtual File Server (VFS).
- `{exportlist|move|reset|delete|clearcount}`
  specifies:
  - The `exportlist` specifies the list of quarantined files and is exported to the default location in the VFS to which the specified File Store belongs to `- /fpgname/vfsname/.admin/AV/Quarantine`. This operation can be performed within a VFS or a File Store.
  - The `move` option specifies that the quarantined files are to be moved to a directory under the Quarantine directory in the VFS to which the specified File Store belongs to `- /fpgname/vfsname/.admin/AV/Quarantine`. The files can be identified with their timestamp. This operation can be performed either on the entire VFS, File Store or the container file.
  - The `reset` option specifies that the quarantined files in the specified VFS, File Store or container file that are to be reset. It removes an extended attribute from each of the infected files. The attribute is set on scan when the VSE indicates that a file is infected. It does not move the file.
  - The `delete` option specifies that the quarantined files under the VFS, File Store or container file that are to be deleted.

  **NOTE:** The snapshot infected files cannot be moved or deleted, but can be reset.

  - The `clearcount` option deletes the AV statistics for the specified VFS.

Exporting quarantined files using SSMC

- On the main SSMC menu, select **File Persona > Virtual File Servers screen > Manage Antivirus Quarantine**.
- Select the **Actions** menu, and then select **Export**.

Moving quarantined files using SSMC

- On the main SSMC menu, select **File Persona > Virtual File Servers screen > Manage Antivirus Quarantine**.
- Select the **Actions** menu, and then select **Move**.

Resetting quarantined files using SSMC

- On the main SSMC menu, select **File Persona > Virtual File Servers screen > Manage Antivirus Quarantine**.
- Select the **Actions** menu, and then select **Reset**.

Deleting quarantined files using SSMC

- On the main SSMC menu, select **File Persona > Virtual File Servers screen > Manage Antivirus Quarantine**.
- Select the **Actions** menu, and then select **Delete Quarantined Counter**.
- The **Delete Quarantined Counter** dialog opens.
- If you are not sure that these quarantined files should be deleted, click **Cancel**; otherwise, click **Delete** to start the action and close the dialog.

Clearing statistics for quarantined files using SSMC
• On the main SSMC menu, select File Persona > Virtual File Servers screen > Manage Antivirus Quarantine.
• Select the Actions menu, and then select Clear Total Quarantined Counter.
• The Clear Total Quarantined Counter dialog opens.
• Review the clearing information. If you are not sure that this total quarantine counter should be cleared, click Cancel; otherwise, click Yes, clear to start the action and close the dialog.

Updating Virus Definitions

If the virus definitions on the VSE are not in sync with the virus definitions on the HPE 3PAR StoreServ Storage system, files already scanned may not have been scanned based on the updated virus definitions. When a new file is read on the StoreServ Storage system, the virus definitions are automatically updated with the definitions from the VSE.

To update the virus definitions, issue the following command:

```
startfsav update
```

Updating virus definitions using the SSMC

• On the main SSMC menu, select File Persona > File Persona Configuration screen > Antivirus Settings.
• Select the Actions menu, and then select Update virus definition.
• Follow the instructions on the dialog that opens.

Enabling and Disabling Antivirus Services

To enable the antivirus services, issue the following command:

```
startfsav svc
```

To disable the antivirus services, issue the following command:

```
stopfsav svc
```

Enabling or disabling the antivirus services using the SSMC

• On the main menu, select File Persona > Persona Configuration.
• On the list pane, select the File Persona, and then select Configure File Persona on the Actions menu.
• On the dialog that opens, select the Advanced options check box.
• On the Antivirus Settings panel, enable or disable the Antivirus service, as appropriate.
Protecting critical data from accidental deletion or malicious alteration is a key requirement for most organizations today. To support this, File Persona introduces a feature known as File Lock for data immutability. File Lock Enterprise mode provides data retention for a period of time as required by legal statute or internal governance.

Once a file is written it can be converted into a read-only file with no write permissions thereafter. A Write-Once Read-Many (WORM) file cannot be modified, however, it can be deleted at any time.

A WORM file can be retained. This file will remain in the “retained” state until a specific time period. A retained file cannot be deleted.

To detect alteration of a WORM file, File Persona introduces a feature known as Data Validation. For example if a bit is flipped by a cosmic ray, the Data Validation feature should be able to detect the flipped bit.

File Persona categorizes files into four distinct categories, which are the following:

- **Normal**
  A file is normal when it is created in read-only mode or read/write mode, and it can be modified and deleted at any time. A checksum is not calculated for normal files and they are not managed by data retention.

- **WORM**
  A WORM file cannot be modified but it can be deleted at any time. WORM files can also be retained once a retention time is applied. In case when the Data Validation feature is turned on, a checksum is calculated for WORM files. Checksums are used for validation scans and validating the integrity of data. A WORM file’s content and permissions/ACLs can NEVER be modified.

- **WORM-retained**
  A WORM file becomes a WORM-retained file when a retention period is applied to it. If the Data Validation feature is enabled then a checksum is calculated.

- **On-Hold**
  An On-Hold file is retained indefinitely and cannot be modified or deleted even if the original retention period has expired. Files revert to their original retention period when the legal hold is revoked.

If additional security is desired when using file administrative commands, File Persona offers another mode known as File Lock Compliance mode. In a compliance-enabled namespace, a user request needs to be approved by a Compliance Officer using a Dual Admin Authentication functionality. The Compliance Officer is required to approve all File Lock management user requests.

### File Lock Enterprise

A file goes through a series of transformations. The following is the procedure it follows:

1. A file gets transformed to WORM state when the file is set to read-only or when an autocommit period expires.

   **NOTE:**
   The Autocommit feature is a service that automatically sets a file to the WORM state if the file has not been accessed for a period of time. After the file is set to the WORM state, a retention period may be applied.

2. If a retention period is set, a WORM file transforms to a WORM-retained file.
3. A file can be transformed to "On-Hold" if a legal-hold is applied to a WORM file or a WORM-retained file.
4. Files in "On-Hold" state are indefinitely retained and cannot be deleted or modified even if the retention periods expires.
5. Once the legal-hold is revoked the file reverts to its original retention period.
6. A file can be deleted once the retention period expires.

The figure below describes the lifecycle of a file in File Lock Enterprise:

![Lifecycle of a file in File Lock Enterprise](image)

**Conversion of a Normal File to WORM File**

All files in a File Store start off as normal files. There are two ways to transform a normal file to a WORM file. The first one requires that the user explicitly changes the mode of the file to read-only. The second method is associated with setting a retention policy and enabling the autocommit feature. With the retention policy set, files get automatically transformed into WORM or WORM-retained files.

The following scenarios demonstrate how to transform a normal file to a WORM file and a WORM file to a WORM-retained file:

**Transforming a Normal File to a WORM file without Autocommit period**

Files can be transformed to WORM files without the autocommit period. The user needs to change the mode of the file to read-only. Explicitly changing the mode of the file to read-only will transform the normal file to a WORM file.

**Changing a file to read-only mode:**

**NFS clients**

Once the NFS File Share is mounted, issue the `chmod` command to change the mode of the file to read-only.

```
chmod 444 <filename>
```

This results in removing the write permission.

To clear all write bits without changing any other bits, enter the following command:

```
chmod -w <filename>
```

**SMB clients**

An SMB client trying to access a File Share should issue the `attrib` command to change the file to read-only mode.

```
2:\mydir> attrib +r <filename>
```
The Z drive specifies the current directory as a mapped share drive.

**Transforming a Normal File to a WORM File with Autocommit period**

The Autocommit period is used to transform a Normal file to a WORM file, without the user explicitly changing the mode of the file to read-only. If the Autocommit period is set to a certain value, a background process scans all the files in the File Store or VFS and compares the last access date/time recorded in the individual file's metadata with the system date/time. If (last access date/time + autocommit time) is greater than (system date/time) the file is transformed to a WORM state. If the retention policy has a retention period, the file is retained for that amount of time.

Once the autocommit period expires, Normal files (both data and metadata) automatically transform into WORM or WORM-retained files. To disable the Autocommit feature, set the autocommit period to zero.

**File Lock Compliance**

File lock Compliance provides an additional level of security when using file administrative commands. In a compliance-enabled namespace, a user has to get the user request approved using a Dual Admin Authentication functionality by a "Compliance Officer" (CO). The Compliance Officer approves all WORM management user requests. File Lock Compliance uses a compliance clock to prevent tampering with the system time and to ensure retention periods are enforced in accordance with legal requirements. The alteration of the system clock is protected under Dual Admin Authentication.

**NOTE:**
Currently, File Lock Compliance does not support the regulations defined by U.S. Securities and Exchange Commission (SEC) rule 17 a-4.

**Prerequisites for File Lock Compliance**

1. At least one VFS or File Store has its retention policy set in Compliance mode.
2. There is one user in a Compliance Officer role. Refer to section **Compliance Officer** for details.
3. Set the flag `ComplianceOfficerApproval` to yes to enable the Dual Admin Authentication functionality/Compliance mode in the system.

   Issue the `setsys [-f] ComplianceOfficerApproval {yes|no}` command to set the Compliance flag. The `showsys -param` command displays the "ComplianceOfficerApproval" flag and a value "yes" denotes that the system is Compliance enabled.

   **NOTE:**
   The Compliance mode policy can be set on a VFS or File Store on an FPG with On-Disk version 12.2 or later.

**Compliance Officer**

A Compliance Officer approves all File Lock Compliance management user requests. The Compliance Officer performs the following operations when a Dual Admin Authentication request is received from a user:

- Approves/denies a pending Dual Admin Authentication request.
- Removes a request or all requests specific to states such as: executed, cancelled or rejected.
- Sets the size of the request queue (max size limit: 99).

**NOTE:** When the queue reaches its maximum size limit, the next request would get rejected automatically.
Operations that need Compliance Officer approval

Below is a list of operations that need the Compliance Officer to approve:

- **createuser**
  This command creates all Compliance Officer users. Note that the first Compliance Officer creation succeeds without Compliance Officer approval.

- **removeuser**
  This command removes all Compliance Officer users except the last Compliance Officer user. The last Compliance Officer user cannot be removed if the cluster level flag is enabled.

- **setuser**
  This command maps the Compliance Officer role to the existing local browse users.

- **setsys [-f] ComplianceOfficerApproval {yes|no}**
  - This command enables/disables File Lock Compliance mode.

- **setnet ntp**
  This command sets the NTP system server and synchronizes all clocks.

- **setdate**
  This command changes the date.

Note that the timezone command does not require approval from the Compliance Officer.

**NOTE:**
Commands such as createuser, removeuser, setuser, setsys ComplianceOfficerApproval, setnet ntp and setdate will not be audited when there is no compliance enabled VFS and File Store.

- **setfsarchive pol**
  Refer to section Defining Data Retention Policy.

- **setfsarchive pol_inherit**
  Refer to section Policy Inheritance.

- **setfsarchive legalhold -set**
  Refer to section Setting or Clearing a Legal-Hold on WORM files.

- **setfsarchive legalhold -clear**
  Refer to section Setting or Clearing a Legal-Hold on WORM files.

- **setfsarchive retention**
  Refer to section Changing Retention Period.

- **removefsarchive scan**
  Refer to section Removing Data Validation Scan.

- **removefsarchive files**
  Refer to section Deleting a WORM File Administratively.

- **removefsarchive retention**
  Refer to section Removing the Retention Period.

- **removefsarchive auditlogs**

- **removefstore**
  Refer to section Removing File Stores.

- **removefpg**
Refer to section **Removing and Recovering File Provisioning Groups**.

- `removevfs`

Refer to section **Deleting Virtual File Servers**.

**Enabling Dual Admin Authentication**

Operations on a Compliance enabled namespace have to be approved by the Compliance Officer to allow the submitter to execute the command. If the Compliance Officer approves/rejects the request (using the "setcorequest" command), the status will be updated in the request queue. A request ID will be returned. The requester can execute the approved request using "setcorequest execute" command.

**NOTE:** Once the mode is set to Compliance, it cannot be changed to Enterprise mode.

**Dual Admin Authentication request states**

Following are the states a Dual Admin Authentication request can exist at any given time:

- **PENDING**
  
  Once a request gets added to the request queue, the request is assigned a PENDING state.

- **INPROGRESS**
  
  Once a request gets approved and the command execution is in progress the request is assigned a INPROGRESS state.

- **CANCELLED**
  
  If a request gets cancelled, the request is assigned a CANCELLED state.

- **REJECTED**
  
  If a request gets rejected (when the queue reaches its maximum size), the request is assigned a REJECTED state.

- **EXECUTED**
  
  If a request gets executed, it is assigned an EXECUTED state.

- **DELETED**
  
  If a request gets deleted from the queue, it is assigned a DELETED state.

**Request Queue Flowchart**

The following diagram depicts the flow of a request queue from an end user to the Compliance Officer:
NOTE:

All subsequent archival commands after Dual Admin Authentication are audited. Audit logs are collected per VFS. Compression of the audit log is initiated once it reaches its size limit (100 MB). The audit logs can be deleted using only Dual Admin Authentication. A user can access these audit logs if a File Share (SMB or NFS) is defined for the .admin File Store under the VFS where the audit logs are stored.

Managing Dual Admin Authentication Requests

This section describes commands to approve, deny, execute, and cancel a pending Dual Admin Authentication request. Also, it describes commands how to remove a request once it attains a certain state and how to set the request queue size.

Displaying request details

To view the request details, issue one of the following HPE 3PAR CLI commands:

```bash
showcorequest [-d]
showcorequest [-request <requestid>]
```

where the options are,

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-d</code></td>
<td>Specifies the detailed output to be displayed.</td>
</tr>
<tr>
<td><code>-request &lt;requestid&gt;</code></td>
<td>This option takes the request ID for which status is to be displayed.</td>
</tr>
</tbody>
</table>

Examples:
The `showcorequest -d` command displays a list of all the requests and their details:

```
showcorequest -d
------------------Request: 8 details---------------------
Request ID               : 8
Command                  : removefpg fp1
Approval Status          : pending
Submission Time          : 2016-08-23 23:17:25 IST
Completion Time          : -
Requestor Name           : tstEdit
Requestor Role           : super
Requestor Source Address : 127.0.0.1
Comments                 : -
Command Output           : Approval Pending
------------------Request: 6 details---------------------
Request ID               : 6
Command                  : setfsarchive pol_inherit -inheritance disable -fstore fstore1 vfs1
Approval Status          : rejected
Submission Time          : 2016-08-23 07:16:31 IST
Completion Time          : -
Requestor Name           : tstEdit
Requestor Role           : edit
Requestor Source Address : 127.0.0.1
Comments                 : -
Command Output           : Approval rejected
------------------Request: 1 details---------------------
Request ID               : 1
Command                  : setfsarchive pol_mode compliance -defperiod 4M -minperiod 4d -maxperiod 3y -autocommperoid 1h -fstore fstore1 vfs1
Approval Status          : executed
Submission Time          : 2016-08-23 06:47:11 IST
Completion Time          : 2016-08-23 06:48:37 IST
Requestor Name           : superuser
Requestor Role           : super
Requestor Source Address : 127.0.0.1
Comments                 : -
Command Output           : TaskID: 2391: Passed
------------------Request: 4 details---------------------
Request ID               : 4
Command                  : removeuser tst2CO
Approval Status          : executed
Submission Time          : 2016-08-23 07:10:39 IST
Completion Time          : 2016-08-23 07:11:52 IST
Requestor Name           : superuser
Requestor Role           : super
Requestor Source Address : 127.0.0.1
Comments                 : -
Command Output           : Succeeded. User removed
------------------Request: 5 details---------------------
Request ID               : 5
Command                  : setfsarchive pol_retenvalidation enable -fstore fstore1 vfs1
Approval Status          : approved
Submission Time          : 2016-08-23 07:16:03 IST
Completion Time          : -
Requestor Name           : tstEdit
Requestor Role           : edit
```

```
Requestor Source Address : 127.0.0.1
Comments : -
Command Output : Execution pending

------------------Request: 2 details---------------------
Request ID : 2
Command : removeuser tstCO
Approval Status : cancelled
Submission Time : 2010-08-24 02:55:31 AST
Completion Time : -
Requestor Name : 3parsvc
Requestor Role : super
Requestor Source Address : 127.0.0.1
Comments : -
Command Output : Request cancelled

The `showcorequest -request` command shows the status of request ID 8:

```
#showcorequest -requestid 8
Request Approval  Requestor  Submission
ID    Status     Name       Time
Command
8    pending    tstEdit    2016-08-23 23:17:25 IST  removefpg fpg1

1 total
```

Detailed output:
```
#showcorequest -d -requestid 8
------------------Request: 8 details---------------------
Request ID : 8
Command : removefpg fpg1
Approval Status : pending
Submission Time : 2016-08-23 23:17:25 IST
Completion Time : -
Requestor Name : tstEdit
Requestor Role : super
Requestor Source Address : 127.0.0.1
Comments : -
Command Output : Approval Pending
```

Filtering requests based on the status

To filter requests based on a specific state, issue the following HPE 3PAR CLI command:

```
showcorequest [-state {approved|pending|rejected|executed|inprogress|cancelled}]
```

where the options are,

- `-state {approved|pending|rejected|executed|inprogress|cancelled}`

This option filters the approved/rejected/executed/pending/cancelled/inprogress requests.

**Examples:**
showcorequest showcasing an approved request:

```
# setcorequest approve 34

8400MAX cli% showcorequest -state approved
RequestID ApprovalStatus RequestorName SubmissionTime
Command

34 approved 3parsvc  2017-07-19 12:08:12 EDT createuser

user2 ******** all co

-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
----------------
1
total
8400MAX cli%
```

showcorequest showcasing a pending request:

```
# showcorequest -state pending

RequestID ApprovalStatus RequestorName SubmissionTime
Command

33 pending 3parsvc  2017-07-19 12:08:12 EDT createuser

user1 ******** all co

-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
----------------
1
total
8400MAX cli%
```

showcorequest showcasing an executed request:

```
# showcorequest -state executed

RequestID ApprovalStatus RequestorName SubmissionTime
Command

35 executed 3parsvc  2017-07-19 12:08:40 EDT createuser

user3 ******** all co

-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
----------------
1
total
```

showcorequest showcasing a rejected request:

```
# showcorequest -state rejected

RequestID ApprovalStatus RequestorName SubmissionTime
Command
```
showcorequest showcasing an inprogress request:

```
# showcorequest -state inprogress
RequestID ApprovalStatus RequestorName SubmissionTime  
-------------------------  ------------------  -----------------------------
                       32 inprogress  3parsvc      2017-07-19 11:07:16 EDT  
Command
legalhold -set -basepath /fpg_cWORM -files 
{vfs_cWORM/fstore_NTFS_cWORM/patient_records/PatientD6/PatientD5-3[0-9][0-9][0-9][0-9]_PatientD5.*} -fpg 
fpg_cWORM -fstore fstore_NTFS_cWORM vfs_cWORM
```

showcorequest showcasing a cancelled request:

```
# showcorequest -state cancelled
RequestID ApprovalStatus RequestorName SubmissionTime                
-------------------------  ------------------  -----------------------------
                       37 cancelled  3parsvc      2017-07-19 12:09:38 EDT  
Command
legalhold -set -basepath /fpg_cWORM -files 
{vfs_cWORM/fstore_NTFS_cWORM/patient_records/PatientD6/PatientD5-3[0-9][0-9][0-9][0-9]_PatientD5.*} -fpg 
fpg_cWORM -fstore fstore_NTFS_cWORM vfs_cWORM
```
The `showcorequest` command displays all the requests together:

```
# showcorequest
```

<table>
<thead>
<tr>
<th>RequestID</th>
<th>ApprovalStatus</th>
<th>RequestorName</th>
<th>SubmissionTime</th>
</tr>
</thead>
<tbody>
<tr>
<td>33</td>
<td>pending</td>
<td>3parsvc</td>
<td>2017-07-19 12:08:12 EDT createuser</td>
</tr>
<tr>
<td>34</td>
<td>approved</td>
<td>3parsvc</td>
<td>2017-07-19 12:08:12 EDT createuser</td>
</tr>
<tr>
<td>35</td>
<td>executed</td>
<td>3parsvc</td>
<td>2017-07-19 12:08:40 EDT createuser</td>
</tr>
<tr>
<td>36</td>
<td>rejected</td>
<td>3parsvc</td>
<td>2017-07-19 12:09:13 EDT createuser</td>
</tr>
<tr>
<td>37</td>
<td>cancelled</td>
<td>3parsvc</td>
<td>2017-07-19 12:09:38 EDT createuser</td>
</tr>
</tbody>
</table>

Displaying request queue limit

To view the request queue limit, issue the following HPE 3PAR CLI command:

```
showcorequest [-queueSize]
```

where the options are,

- `-queueSize` This option displays the queue size.

Examples:

The `showcorequest -queueSize` command displays the queue size:

```
#showcorequest -queueSize
The queue size is: 20
```

Approving/denying a request

To approve or reject a Dual Admin Authentication user request, issue the following HPE 3PAR CLI command:

```
setcorequest {approve|deny} [-comment <comment>] <requestid>
```

where the subcommands are,

<table>
<thead>
<tr>
<th>Subcommand</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>approve</td>
<td>Approves a pending command execution request</td>
</tr>
<tr>
<td>deny</td>
<td>Rejects a pending command execution request</td>
</tr>
</tbody>
</table>

and the options are,
<table>
<thead>
<tr>
<th><code>&lt;requestid&gt;</code></th>
<th>Specifies the request ID that needs to be approved or denied.</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-comment &lt;comment&gt;</code></td>
<td>Specifies comments (if any).</td>
</tr>
</tbody>
</table>

**NOTE:**
- Once a request is approved, it cannot be denied. Also, once a request is denied it cannot be approved.

**Examples:**

1. Approve a request with ID 12345:
   ```
   cli% setcorequest approve 12345
   ```
2. Deny a request with ID 12345:
   ```
   cli% setcorequest deny 12345
   ```

**Executing/cancelling a request**

To execute/cancel a request, issue the following HPE 3PAR CLI command:

```
setcorequest {execute|cancel} <requestid>
```

where the subcommands are,

- **execute**: Executes an approved request.
- **cancel**: Cancels a pending request.

and the option is,

<table>
<thead>
<tr>
<th><code>&lt;requestid&gt;</code></th>
<th>Specifies the request ID that needs to be approved or denied.</th>
</tr>
</thead>
</table>

**NOTE:**
- Once a request is executed, it cannot be executed again.
- A pending/cancelled/rejected request cannot be executed.

**Examples:**
1. Execute an approved request with ID 12345:

   cli% setcorequest execute 12345

   #showtask -d 687

   Id  Type               Name              Status  Phase  Step -------
       StartTime------ FinishTime------ -Priority- -User--
   2014 background_command setfsarchive_task done     ---  ---  2015-11-03
   04:06:39 PST 2015-11-03 04:06:40 PST n/a  test_super

   Detailed status:
   2015-11-03 04:06:39 PST Created     task.
   2015-11-03 04:06:39 PST Updated     Executing "setfsarchive_task" as 0:30490
   2015-11-03 04:06:40 PST Updated     Policy has been set successfully.
   2015-11-03 04:06:40 PST Completed   scheduled task.

2. Execute a pending request with ID 12345:

   cli% setcorequest execute 12345
   Cannot execute the command of state: pending

3. Cancel an approved request:

   cli% setcorequest cancel 12345
   Request queue could not be updated: Cannot change the state from approved to cancelled.

4. Cancel a rejected request:

   cli% setcorequest cancel 12346
   Request queue could not be updated: Cannot change the state from rejected to cancelled.

5. Cancel an executed request:

   cli% setcorequest cancel 12347
   Request queue could not be updated: Cannot change the state from executed to cancelled.

6. Cancel a pending request:

   cli% setcorequest cancel 1234

   NOTE:
   Only submitter can execute or cancel the request.

Modifying the request queue size

To set the queue size, issue the following HPE 3PAR CLI command:

   setcorequest queuesize <size>

   and the option is,

   queuesize                Modifies the queue size. Default size of queue: 20
   Min size of queue: 1 Max size of queue: 99

Examples:
1. Set a queue size:

```
cli% setcorequest queuesize 30
```

Removing requests from the queue

To delete a request from the queue, issue one of the following HPE 3PAR CLI commands:

```
removecorequest [-f] <requestid>
removecorequest [-f] -state {executed|cancelled|rejected}
```

where the options are,

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;requestid&gt;</code></td>
<td>Specifies the request ID that needs to be deleted.</td>
</tr>
<tr>
<td>`-state {executed</td>
<td>rejected</td>
</tr>
<tr>
<td><code>-f</code></td>
<td>Suppress confirmation from user while removing the request.</td>
</tr>
</tbody>
</table>

**NOTE:** Requests that are in a pending or approved state cannot be removed.

Examples:

1. Remove a specific request with ID 12345:

```
cli% removecorequest 12345
This command will remove the request with id 12345.
Do you wish to continue?
select y=yes n=no: y
```

2. Remove a specific request with ID 12345 forcibly:

```
cli% removecorequest -f 12345
```

3. Remove all the executed requests forcibly:

```
cli% removecorequest -f -state executed
```

4. Remove all the rejected requests forcibly:

```
cli% removecorequest -f -state rejected
```

**Data Retention**

Data retention with the File Lock feature enables electronic records to be both unalterable and rapidly accessible.

**Managing Data Retention**

Data retention gets enforced and defined through a data retention policy. The policy can be enabled on a specific File Store or all the File Stores in a Virtual File Server (VFS). The policy includes the minimum retention period, the maximum retention period, and a default retention period that specifies how long a file must be retained. If no retention is desired, the minimum retention period can be set to zero.
If the retention policy is enabled at the VFS level, the same policy is passed to all File Stores under it. Optionally, a File Store can be excluded from policy inheritance of the parent VFS. Moreover, a File Store can have its own local policy, which could differ from its parent’s (VFS) policy.

### Data Retention Policy and Attributes

Data retention attributes that are configured on a File Store or a VFS are collectively known as a retention policy (sometimes referred as a retention profile). The policy pertains to a File Store or VFS, and gets applied to all the files in the File Store or VFS. The following is a list of the main attributes of a retention policy:

- **Default retention period**
  - The default retention period that is defined in the retention policy states how long the WORM file will be retained. If a file in a VFS or File Store needs to be WORMed but no retention is required, then the default retention parameter should be set to zero. To transform the file into a WORM-Retained file, the default retention period should be set to a period in the future. This value is applied by default to the WORM file as soon as it transitions to a retained-state.

- **Minimum and Maximum Retention periods**
  - The valid range for minimum and maximum retention period is 2s - 100y. Regardless of the File Store or VFS’s retention policy, the retained files cannot be deleted until their associated retention period expires. The retention period for a file must be within the minimum and maximum retention periods associated with the File Store or VFS policy. If the retention period is less than the minimum retention period, the expiration time of the period will be adjusted to match the retention period. Similarly, if the retention period exceeds the maximum retention period, the expiration time will be adjusted to match the maximum retention period. If the policy does not have a specific retention period set for the file, the default retention period is automatically applied. If the default retention period is zero, the file will not be retained and it will remain a WORM file.

- **Autocommit period**
  - The autocommit period is used to automatically WORM a normal file, without the user explicitly changing the mode of the file to read-only. If the autocommit period is set to a certain time period, a background process scans all the files in the File Store or VFS and compares the last access datetime recorded in the file's metadata to the current time. If last access datetime + autocommit time is greater than current time the file is WORMed. If the retention policy has a retention period, the file is retained.
  
  Files that are not changed (both data and/or metadata) during the autocommit period, automatically transform into WORM or WORM-retained files. once the autocommit period expires. To disable the autocommit feature, set the autocommit period to zero.

- **Mode**
  - Mode controls how the expiration time for the retention period can be adjusted. File Persona currently supports an Enterprise or Compliance mode retention feature where the expiration date of the retention period can be extended to a future date.

- **Legal-hold**
  - Files are retained indefinitely during the periods of legal discovery. Files cannot be modified nor deleted even if the original retention period has expired. A file reverts to its original retention period when the legal-hold is revoked.

### Defining Data Retention Policies

The `setfsarchive pol` defines the retention policy that is applied to the File Store or VFS. The syntax for the `setfsarchive pol` CLI command is as follows:

```
setfsarchive pol [-mode {enterprise|compliance} -defperiod <defaultperiod> -minperiod <period> -maxperiod <period> -autocommerperiod <period>] [-retenvalidation {enable|disable}] [-fstore <fstorename>] [-fpg <fpgname>] <vfs>
```

where,
-mode
data retention mode - Enterprise or Compliance

-defperiod
default retention period

-minperiod
minimum retention period

-maxperiod
maximum retention period

-autocommperiod
autocommit period

-retenvalidation
this is an optional parameter. Once enabled, the system generates data and metadata checksums for each file when it transitions from Normal state to WORM/WORM-Retained state. These checksums are later used by Data Validation Scan for consistency check.

-fstore
name of File Store. This is optional and if provided, it sets the retention policy at File Store level.

-fpg
name of FPG.

-vfs
name of VFS. This sets the retention policy at VFS level.

To set the retention policy in compliance mode issue the following HPE 3PAR CLI command:

For all the <period> options the value can be any decimal number followed by one of the time units: s (seconds), m (minutes), h (hours), d (days), w (weeks), M (months), y (years).

Following is an example showcasing the setfsarchive pol command:

```
setfsarchive pol -mode compliance -defperiod 1M -minperiod 1h -maxperiod 3y -autocommperiod 0h -fstore fstoreCW2 -fpg sfpg2  svfs2
```

The "0h" for autocommit means it is "OFF".

Configuring and Enabling Data Retention Policies

To enable a data retention policy on a new or an existing File Store or VFS and other optional features that require a retention-enabled file system, such as Validation scan; issue the following command:

```
setfsarchive pol
```

The setfsarchive pol CLI command is used to set the data retention and archival policy for the File Store or VFS. The retention policy specifies the following properties:

- Default retention mode
- Minimum and maximum retention periods
- Validation enable
- Autocommit period

The setfsarchive pol CLI command DOES NOT differentiate between a new and an existing File Stores or VFSs.
Policy Inheritance

A policy can be enabled or disabled for inheritance at the File Store level. Policy inheritance can be enabled or disabled only on a File Store that does not contain files and does not have a local retention policy. The CLI command `setfsarchive pol_inherit` is used to enable or disable the policy inheritance. The following is the syntax of the command:

```
setfsarchive pol_inherit -inheritance {enable|disable} -fstore <fstorename> [-fpg <fpgname>] <vfs>
```

- **-inheritance**
  Whether policy inheritance should be enabled or disabled
- **-fstore**
  Name of the File Store
- **-fpg**
  Name of the FPG
- **vfs**
  Name of the VFS

Viewing Data Retention Policies

The `showfsarchive pol` command is used to view the retention policy of a File Store or a VFS. The syntax for the CLI command is as follows:

```
showfsarchive pol [-fstore <fstorename>] [-fpg <fpgname>] [<vfs>]
```

where,

- **-fstore**
  Name of File Store. This is optional and if provided, it lists the retention policy at File Store level.
- **-fpg**
  Name of FPG.
- **vfs**
  Name of VFS. This is optional and if provided, it lists the retention policy at VFS level.

Viewing Data Retention Information

The `showfsarchive files` CLI command is used to list the retention information of a file (or a set of files). The syntax of the CLI command is as follows:

```
showfsarchive files [-basepath <basepath>] {-files <filepath>[,<filepath>,...] | -importfile <source_path> | -inputfile <pathoffile>} [-fpg <fpgname>] <vfs>
```

Refer to the following example:
showfsarchive files -files /testfs/vfs1/fstore1/foo.txt vfs1
12628

#showtask -d 12628

<table>
<thead>
<tr>
<th>Id</th>
<th>Type</th>
<th>Name</th>
<th>Status</th>
<th>Phase</th>
<th>Step</th>
</tr>
</thead>
<tbody>
<tr>
<td>12628</td>
<td>background_command</td>
<td>getfsarchive_task</td>
<td>done</td>
<td>---</td>
<td>---</td>
</tr>
</tbody>
</table>

startTime------- ------ finishTime--------      priority user--

2016-04-27 11:38:37 UTC 2016-04-27 11:38:48 UTC n/a      3parsvc

Detailed status:
2016-04-27 11:38:37 UTC Created task.
2016-04-27 11:38:37 UTC Updated Executing "getfsarchive_task"
as 3:32012
2016-04-27 11:38:37 UTC Updated Executing "showfsarchive files
-files /testfs/vfs1/fstore1/foo.txt -fpg fp1 vfs1"
2016-04-27 11:38:48 UTC Updated Task is initiated. check the output
file /testfs/vfs1/.admin/archiving/retenadm/
result_task_0497d7753db94a48b051922912e6340e.txt
for intermediate results.
2016-04-27 11:38:48 UTC Updated Success. Please refer
/testfs/vfs1/.admin/archiving/retenadm/
result_task_0497d7753db94a48b051922912e6340e.txt
for more details.
2016-04-27 11:38:48 UTC Completed scheduled task.

Output file

The result of the command will be saved in a .admin share and the user can mount the .admin share on
any client to check the result. A sample of the output file is as follows:

```
# cat /testfs/vfs1/.admin/archiving/retenadm/
result_task_0497d7753db94a48b051922912e6340e.txt
/testfs/vfs1/fstore1/foo.txt: state={retained} retain-to:{2015-Dec-16 08:43:09}
```

The file foo.txt is a retained file and its retention period expires on 2015-Dec-16 08:43:09.

**WORM File Administration**

When using CLI commands for file administration, the file paths affected by the retention action need to be
specified. The following are the two supported methods to pass file paths to the CLI command:

- A path list containing one or more entries separated by commas.
- An input file containing one or more entries. Multiple entries on the same line is not allowed. Input files can
  contain both file and directories.

**NOTE:**

All WORM administration commands apply to both File Lock Enterprise and Compliance modes but File
Lock Compliance mode requires Dual Admin Authentication request approval.

An entry could be an absolute path, such as /fp1/vfs1/fstore1/foo.txt or a relative path to the base
path using the -basepath option. For example, if the base path is /fp1/vfs1/fstore1, the path
foo.txt is a valid entry.

When using captive CLI commands, use the "\" character to escape wild cards. Otherwise, errors will be
encountered.
The following rules apply when specifying path lists:

- The base path must include the root of the filesystem and also the mount point; it cannot be relative to the user’s current directory, unlike other UNIX commands.
- Base path does not support wildcards.
- Input file does not support wildcards.
- A directory cannot be specified in a path list. Directories have no retention settings, and the command will return an error message if a directory is entered. The directory path in the input file and the process will be repeated for all files in the path mentioned in the input file.

To have the process repeated recursively for all files in a directory, mention the directory path in the input file and the process will be repeated for all files in the path in the input file.

### Changing Retention Period

The retention period can only be extended. For example, if you want to change the retention period (greater than the current retention period) of a retained file currently using the default retention period. This is done by setting the access time to a new retention expiration with a future timestamp.

To update the expiry time of a retained file, issue the following command:

```shell
setfsarchive retention [-basepath <basepath>] {-files <filepath>[,<filepath>]... | -importfile <source_path> | -inputfile <pathoffile>} -expdate <expirydate> -fstore <fstorename> [-fpg <fpgname>] <vfs>
```

The `-expdate <expirydate>` option supports the time/date format supported by the standard Linux `touch` command. See the `touch (1)` man page documentation for the time/date formats permitted.

The expiration date of the file will be set to `-expdate <expirydate>` only if the date provided is a valid and absolute date. File Lock will make sure that any attempt to set the retention period to an earlier timestamp will fail. The retention period will not be updated if the new retention expiration date is more than the current time + maximum retention period.

### Removing the Retention Period

When the retention period from a WORM-Retained file is removed, the WORM-Retained file becomes a WORM file. To remove the retention period from a file or a list of files, issue the following command:

```shell
removefsarchive retention [-basepath <basepath>] {-files <filepath>[,<filepath>]... | -importfile <source_path> | -inputfile <pathoffile>} -fstore <fstorename> [-fpg <fpgname>] <vfs>
```

### Removing the WORM Attribute from a WORM File

You cannot remove the WORM attribute from a WORM file. If you need to modify a WORM file that has been WORM-retained, copy the file elsewhere, delete the original file (administratively if necessary), then copy the file back as a normal file. Once a normal file gets transformed into a WORM file, it can never be reverted back to a normal file again in its entire lifecycle. It can only be deleted if the retention period is not set on it.

### Deleting a WORM File Administratively

To delete a WORM file, issue the following command:

```shell
removefsarchive files [-basepath <basepath>] {-files <filepath>[,<filepath>]... | -importfile <source_path> | -inputfile <pathoffile>} -fstore <fstorename> [-fpg <fpgname>] <vfs>
```
**WARNING:**
Deleting files administratively removes them from the File Store, regardless of the data retention policy. The removefsarchive files command does not delete a normal file. This command can be exercised only by the admin.

### Setting or Clearing a Legal-Hold on WORM files

When a legal-hold is set on a WORM file, the file cannot be modified or deleted until the hold is released, even if the retention period has expired. File reverts to its original retention period when the legal hold is revoked.

To set or clear a legal-hold on or from a WORM file two options have been provided: `-set` or `-clear`. The syntax of the command is as follows:

```plaintext
setfsarchive legalhold {-set | -clear} [-basepath <basepath>] {-files <filepath>[,<filepath>]|-importfile <source_path> | -inputfile <pathoffile>}
-fstore <fstorename> [-fpg <fpclassname>] <vfs>
```

### How to Calculate Autocommit period and Data Retention period

Autocommit period is computed primarily based on the modifications of the file, that is mtime period, however the metadata changes, that is ctime period are also used as a reference for the final computed retention period. The final retention period applied to the file (in its access time) will always be computed with respect to the mtime.

Whether a normal file transitions to a WORM file with the autocommit period or an explicit change into read-only mode (e.g. `chmod 444`), the process to calculate the final retention period remains the same. However, there is an extra computation step when transforming using the autocommit period. The fact that when the transition would begin needs to be accommodated. The section below highlights these computations.

#### Autocommit Calculation

The formula to calculate whether autocommit should be applied or not is as follows:

If

\[
\text{mtime (T)} + \text{ autocommit} \times \text{min} \] AND [ctime(T) + autocommit (x min)] >= current system time

then,

**Autocommit is applied**

For example, let's say the autocommit period is 10 minutes. If [mtime (T) AND ctime(T)] + autocommit (10 min), which is T+10, and the current system time is equal to or greater than T+10, then autocommit is applied.

#### Data Retention Calculation

The formula to calculate the retention expiration time is as follows:

Retention expiration time = mtime + autocommit period + retention period

If

Retention expiration time > current system time

then,
Time file is retained = retention expiration time - current system time
else if,
Retention expiration time < current system time
then,
File is not retained

Following is an example showcasing data retention calculation:

A file a.txt is created on a non-File Persona file system - fstore1. On fstore1, the ctime and mtime both are equal to T. The a.txt file is copied to a File Persona File Store: fStore2 one hour later.

On fStore2, the ctime is T+1 hour and mtime is still T.

fStore2 has an autocommit period of 10 minutes and a data retention period of 30 minutes. When the 10 minute autocommit period has passed (T + 1 hour + 10 min), the file copy is autocommitted.

For retention of the file on fStore2, the mtime is T, the autocommit period is 10 minutes and the retention period is 30 minutes.

Mtime (T) + autocommit period (10 min) + retention period (30 min) < current system time (T + 1 hour + 10 min) = the retention period has expired.

If the retention period has expired at the time autocommit is applied, the file is not retained. This implies that the file has already been through its retention period and the retention has expired.

---

Data Validation Scan

Data Validation Scan ensures the integrity of the stored data through checksum verification. The system generates data and metadata checksums for each file when it transitions from normal state to WORM/WORM-retained state. These checksums are used for consistency purposes. The Data Validation Scan feature applies only to WORM files and is not applicable to normal files. The scan is initiated only at the File Store level. A data validation summary file is generated per scan and the administrator can find the list of corrupted files in the summary file.

To ensure that WORM files remain unchanged a data validation scan should be run periodically. Circumstances such as the following could cause a file to change unexpectedly:

- System hardware errors; such as write errors
- Degradation of On-Disk data over time can change the stored bit values, even if no access to the data has ever been performed
- Malicious or accidental changes to the file

A hash-sum is computed of the WORM files in the scanned File Store or sub-directory. A comparison to the original hash-sum is performed. If the two entities do not match the administrator can replace the corrupted file with an unchanged copy from an earlier backup.

The total time taken by a data validation scan is directly proportional to the number of files and the size of files in the File Store or subdirectory.

NOTE:

Normal files are not validated. Data validation scans are directed only to WORM files since hash sums get computed only for WORM files.

Following is a list of actions that are performed when data validation scans are initiated:

- Start
Initiating Data Validation Scan

Data validation scan can be initiated only at the File Store level. To initiate a scan on a File Store, issue the following command:

```
startfsarchive scan [-path <path>] [-fpg <fpgname>] -fstore <fstorename> <vfs>
```

The command starts the data validation scan on the File Provisioning Group (FPG) at the File Store level on the given path. This command gives the scan an ID which can be used to query the status of the scan:

```
stop/pause/resume/remove the scan.
```

**NOTE:**

File Persona supports one validation job in running state at any given time on a per node basis. Additionally, File Persona supports 50 more jobs to be queued per node. Any subsequent tasks beyond 50 queued tasks will be rejected until the queue is available again for new tasks to be queued.

Resuming Data Validation Scan

A data validation scan can be paused by the user and can be resumed anytime later. To resume a data validation scan on a File Store, issue the following command:

```
startfsarchive scan -resume <jobid> [-fpg <fpgname>] -fstore <fstorename> <vfs>
```

Once a running job moves to paused state, there will not be any other active validation task running on the node, so administrators cannot pause a job and start a different job or expect such an action to happen automatically. User has to resume the paused job to get the validation can to continue. Only when an active job has been completed can another job start. The next job is picked from a priority queue. When the next job starts the previous job should be all complete (the queue order is strictly maintained by the subsystem).

Removing Data Validation Scan

A data validation scan can be deleted only once it has been stopped. To delete a scan, issue the following command:

```
removefsarchive scan [-fpg <fpgname>] -fstore <fstorename> <vfs> <jobid>
```

Stopping/Pausing Data Validation Scan

A data validation scan can be stopped/paused. To stop/paused a scan, issue the following command:

```
stopfsarchive scan [-f] [-fpg <fpgname>] -fstore <fstorename> <vfs> <jobid>
```

```
stopfsarchive scan -pause [-fpg <fpgname>] -fstore <fstorename> <vfs> <jobid>
```

where the options are,
### Viewing Validation Scan Results

To view a data validation scan, issue the following command:

```
showfsarchive scan [-jobid <jobid>] [-exportsummary | -export <target_path>] -fstore <fstorename> [-fpg <fpgname>] <vfs>
```

When a data validation scan for a File Store is queried, information about the tasks that are currently running, paused, completed and stopped is displayed. The information includes the following:

- **ID** assigned to the task
- **Status** of the task
- Time the task was started
- Time the task was stopped

The validation task management subsystem in File Persona maintains a history of past tasks that includes tasks that were completed successfully or got terminated due to some issue. The administrator can view the last 50 tasks per File Store.

A unique summary file is generated at the end of the data validation scan. When the summary file is queried using the `-exportsummary` or `-export <target_path>` options, the summary file will be placed under `/<FPG>/<VFS>/..admin/archiving/` validation path and the summary file path will be provided to the user or be placed in the `-export <target_path>`. The user has to mount the admin File Store to view the validation summary file.

Validation summary files are named with the following encoding:

```
validation_<ID-n>.sum
```

For example: `validation_1-0.sum` and `validation_2-0.sum`

The ID signifies the scan id assigned by the file services software when the scan was started. The `-n` (`-0` in the example) shows the increment file number. If there exists a summary file with the same task ID, file number increments to make the validation summary filename unique.

### Data Validation Summary File

A sample data validation summary file is displayed below:

```
cat /testfs/vfs1/.admin/archiving/validation/validation_1-0.sum
JOB_ID=1
JOB_STATUS=COMPLETED
FILESYSTEM_NAME=testfs
FILESYSTEM_MOUNT_DIR=/testfs
PATH=/testfs/vfs1/fstore1
SCANTYPE=hashsum
CREATE_TIME=Wed Dec 15 08:44:47 2015
START_TIME=Wed Dec 15 08:44:47 2015
STOP_TIME=Wed Dec 15 08:44:51 2015
NUM_FILES_VALIDATED=0
NUM_FILES_SKIPPED=0
NUM_CONTENT_INCONSISTENCIES=0
NUM_METADATA_INCONSISTENCIES=2
NUM_JOB_ERRORS=0
METADATA_HASHSUM_ERROR=/testfs/vfs1/fstore1/abc
METADATA_HASHSUM_ERROR=/testfs/vfs1/fstore1/file
```

Data Retention and Validation Output Files will be stored under the admin File Store /<FPG>/<VFS>/admin/archiving. User has to mount the admin File Store on the client to view the results.

Data Validation Tasks on Failed Node

Whether a node gracefully fails or a node crashes, all the validation tasks on the failed node that are in the following state - running, paused or queued will be terminated. The administrator is expected to check the status of the tasks and review them and make a note of what tasks were queued for running or were running in the original node. Such failed tasks will show up as aborted state and the administrator needs to take action to restart all tasks on the failed node (backup node). The event log will also reflect the status of the failed tasks.

Using Hard links for Normal and WORM files

Use the Linux command `ln` without the `-s` option to create a hard link for a normal (non-WORM) file on retention-enabled File Store. If a normal file is transformed to a WORM file, the following restrictions apply until the file is deleted:

- No new hard links to WORM file can be made. Doing this would increment the file's inode link count (stored as metadata), which is not permitted for WORM files as their content and metadata can never change.
- Deletion of hard links (the original File Store entry or a hard-link entry) is permitted without deleting the other file system entries or the file itself. WORM rules allow the link count to be decremented.

Backup Support for Data Retention

The supported method for backing up and restoring WORM files is Network Data Management Protocol (NDMP) with Data Management applications. Other backup methods will back up the file data but will lose the retention configuration. Other mechanisms (non-NDMP) backup most of the WORM attributes but leave specific attributes such as legal-hold settings. Share-based backup applications cannot read from the extended attribute of the file.

Archiving Audit Logs

File Persona audits logs for all Compliance commands issued on the VFS. All commands that require Dual Admin Authentication will be implicitly audited when the Compliance mode is enabled. The audit logs will be created on per VFS basis.

Displaying Audit Logs at the VFS level

To view the audit log details at the VFS level, issue the following HPE 3PAR CLI command:

```
showfsarchive auditlogs [-export {all|<logname>}] [-fpg <fpname>] <vfs>
```

where the options are,

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>export</td>
<td>Export either all or a specific log to the &quot;.admin&quot; File Store. If the string &quot;all&quot; is specified, the command will export all the log files. If a specific log name is specified, the command will export the specified log. The command supports a single log file export.</td>
</tr>
</tbody>
</table>

The auditlogs CLI subcommand exports and removes audit logs at the VFS level.

Examples:
The following example lists all logs at the VFS level:

```
#showfsarchive auditlogs vfs1
audit_fpg1_vfs11_2016-01-14_2016-01-15.log.zip
audit_fpg2_vfs12_2016-01-15_2016-01-16.log.zip
```

The following example exports all logs of a VFS to the .admin File Store:

```
#showfsarchive auditlogs -export all vfs1
Exported all logs for vfs1 to /fpg1/vfs1/.admin/auditing/
```

The following example exports a specific log of a VFS to the .admin File Store:

```
#showfsarchive auditlogs -export audit_fpg2_vfs12_2016-01-15_2016-01-16.log.zip vfs1
Exported audit_fpg2_vfs12_2016-01-15_2016-01-16.log.zip for vfs1 to /fpg1/vfs1/.admin/auditing/
```

**Removing Audit Logs**

To remove all audit logs or a specific audit log, issue the following HPE 3PAR CLI command:

```
removefsarchive auditlogs [-f] [-log <logname>] [-fpg <fpgname>] <vfs>
```

where the options are,

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-f</td>
<td>Suppress warning</td>
</tr>
<tr>
<td>-log</td>
<td>The Log name. Note that active logs cannot be deleted. If the -log option is not given, all compressed logs will be deleted. This subcommand generates a task ID.</td>
</tr>
</tbody>
</table>

**Examples:**

The following example removes all audit logs at the VFS level:

```
#removefsarchive auditlogs vfs1
```

This will delete all compressed logs at VFS level

Do you wish to continue(y=yes, n=no)? y

2346

The following example removes a specific audit log at the VFS level:

```
#removefsarchive auditlogs -f -log audit_fpg2_vfs12_2016-01-15_2016-01-16.log.zip vfs1
```

5478

**Copyfile Support**

Following are the commands that are involved in file operations. The following commands support copyfile (import):

- `setfsarchive legalhold {-set | -clear} [-basepath<basepath>] {-files <filepath> [,<filepath>]... | -inputfile<pathoffile>} [-fpg<fpgname>] <vfs>`
• setfsarchive retention [-basepath<basepath>] {-files <filepath> [,<filepath>]... | -inputfile<pathoffile>} -expdate<expirydate> [-fpg<fpgname>] <vfs>

• removefsarchive files [-basepath<basepath>] {-files <filepath> [,<filepath>]... | -inputfile<pathoffile>} [-fpg<fpgname>] <vfs>

• removefsarchive retention [-basepath<basepath>] {-files <filepath> [,<filepath>]... | -inputfile<pathoffile>} [-fpg<fpgname>] <vfs>

• showfsarchive files [-basepath<basepath>] {-files <filepath> [,<filepath>]... | -inputfile<pathoffile>} [-fpg<fpgname>] <vfs>

where,

| -inputfile<pathoffile> | If the path of the source file is on client machine (eg. /home/client/inputfile.txt), then the file will be imported to/support/WORM/import/<archiveCLI_[clock microseconds].txt> of the active FS VM. |

186 File Lock
## Data Protection

### Backing Up and Restoring File Shares

The specific process for backing up File Persona File Shares depends on the particular backup software in use in your configuration. The general approach to backing up File Shares is as follows:

1. Backup the configuration settings for the VFS associated with the File Store containing the File Shares you intend to backup. For information on backing up VFS configuration settings, see [Backup and Recovery of Configuration settings of Virtual File Servers](#) on page 58.
2. Configure your backup software to backup the top-level shares in each File Store on the VFS, including the File Shares in the `.admin` File Store.
3. Initiate a backup operation in your backup software.

In order to restore a VFS and its associated File Stores that have been backed up in this manner, follow these steps:

- If necessary, re-create a VFS having the same name as that of the VFS previously backed up. For information on creating a VFS, see [Creating Virtual File Servers](#) on page 53.
- If the creation of a VFS was necessary, create a top-level File Share in the `.admin` File Store.
- Restore the configuration settings previously backed up. For information on restoring VFS configuration settings, see [Backup and Recovery of Configuration settings of Virtual File Servers](#) on page 58.
- Initiate a restoration operation in your backup software to restore the contents of those File Shares.

### Using NDMP over iSCSI

The Network Data Management Protocol (NDMP) is an open standard for backing up Network Attached Storage (NAS) systems. In order to use NDMP with File Persona, the NDMP service must be started and configured on the HPE 3PAR system.

#### NOTE:

The throughput will drop if the file system has a large number (greater than 100 K) of small files (files of size < 10 KB).

#### Procedure

1. Ensure that File Persona node networking is configured and working properly. The NDMP backup software will require network connectivity in order to access File Persona objects.
2. Start the NDMP service for File Persona by using the `startfsndmp` command:

   ```
   startfsndmp
   ```

3. Verify that the service has started and obtain the auto-generated cluster iSCSI Qualified Name (IQN) by using the `showfsndmp` command:

   ```
   showfsndmp
   GlobalServiceStatus      --------ClusterIqn----------------------
   STARTED  ign.1994-05.com.redhat:ce331a3b2568;
   ```

4. Create a Virtual Tape Library (VTL) in your backup storage system (for example, an HPE StoreOnce Storage system) using the generated IQN.
5. Configure File Persona to use VTL by using the `setfsndmp` command, as in the following example (with an IP address of 10.10.0.1 for the VTL):
6. You can display configured VTLs by using the `showfsndmp -vtl {vtldevices | vtltapes}` command.

7. Configure NDMP with basic settings such as the DMA address, user name, and password, as per the following example:

```
setfsndmp conf -dma +10.10.0.2 -username ndmpuser -password ndmppw -
enable_sessions true
NDMP configuration has been modified successfully
```

8. Perform any necessary additional steps to configure your supported NDMP backup software. Consult the administrative documentation for your NDMP backup software for configuration details.

Using NDMP for File Store Backup using Snapshots

The Network Data Management Protocol (NDMP) protects a list of files and directories as directed by the Data Management Application (DMA). Permissions, time stamp, mode, and all the extended attribute of an object are backed up and restored. The backup and recover module will restore the object’s permissions, time stamp, mode, extended attributes, and Alternate Data Stream (if any).

The `.snapshot` directory is a hidden directory created during the creation of a File Store. Whenever a File Store’s snapshot is created, it is available in the `.snapshot` directory. Each individual snapshot is represented by its own subdirectory found under the `.snapshot` directory.

NDMP can be used to back up the `.snapshot` directory. In general, the user should not try to back up the whole `.snapshot` directory using the backup mechanism, since the user will be backing up the same files over and over again. It is recommended to backup a specific snapshot subdirectory under the `.snapshot` directory.

**NOTE:**
Once the snapshot is backed up under the `.snapshot` directory, the restoration needs to be targeted to the live view and not the `.snapshot` directory. The `.snapshot` directory is strictly read-only.

NDMP Incremental Backup

When doing an NDMP incremental backup for a directory that has been moved between two different directories will result in a full sized backup; that is, all the content will be backed up. All the files/directories underneath the directory will be backed up even though the content in the files/directories has not been modified.

Using Virtual Copy for Local Disaster Recovery

Local recovery of an FPG uses snapshots of the virtual volumes associated with the FPG. Local recovery can be used to recover from file system corruption or from a change to the file system that needs to be rolled back, e.g. a file system version upgrade. In preparation for using virtual copy for local recovery, take snapshots of the relevant virtual volumes:

**Procedure**

1. Identify all the Virtual Volumes associated with a given File Provisioning Group (FPG) by using the `showvvset` command, specifying an FPG by name, as in the following example:
2. Create a group Virtual Copy of all members of the Virtual Volume set associated with the FPG (as determined from the list of Members in step 1):

```bash
cli% creategroupsv -ro myfpg.0 myfpg.1
CopyOfVV  SnapshotVV
    myfpg.0  myfpg.0.ro
    myfpg.1  myfpg.1.ro
```

The `creategroupsv` command ensures that the Virtual Volumes are consistent with each other with respect to the time that the snapshots were taken.

To recover the snapshots in the Virtual Volumes for a given FPG, perform the following procedure:

1. Remove the FPG by using the `removefpg` command and specifying the `-forget` option, as in the following example:

```bash
removefpg -f -forget myfpg
Removing fpg: myfpg
```

2. Promote the Virtual Copies (snapshots) (follow example below):

```bash
promotegroupsv myfpg.0.ro myfpg.1.ro
```

3. Recover the FPG using the promoted volumes (follow example below):

```bash
createfpg -recover set:myfpg
```

### Using Remote Copy for Disaster Recovery

Refer to the *HPE 3PAR Remote Copy Software User Guide* available at the [HPE Storage Information Library](#) for more information on how to use the Remote Copy feature to create a remote copy for an FPG.

To perform disaster recovery on Remote Copy groups when using SSMC, follow these steps:

1. From the main menu, select **Replication > Remote Copy Groups**.
2. On the list pane, select the Remote Copy Group, and then select **Failover**, **Revert failover**, **Recover**, or **Restore** on the **Actions** menu.
3. Follow the instructions on the dialog that opens.

**NOTE:**

If the source node (FPG) is File Lock Compliance enabled, the recovery node has to be File Lock Compliance enabled too (see **File Lock Compliance mode**). Otherwise, operations such as listed below will fail:

- `createfpg -recover`
- `setfpg -primarynode`
- `setfpg -activate`
- `setfpg -failover`
Configuration Backup and Restore using ACL Inheritance

File Persona supports backing up and restoring ACL's of the share folders created for protocols such as NFS, SMB FTP and Object Access API. File system ACLs associated with each share folder get included in the backup artifact. During the restore operation, the information from the backup artifact is used to restore the ACL's for the respective share folders.

Also the feature backs up and restores the security mode set for every File store. During the backup, the security mode and its error flag of a File Store are collected. This information is reset on the respective File Store on restore.

NOTE:

The configuration backup of a Compliance enabled FPG cannot be restored if the compliance flag is not enabled in the VFS or File Store (see File Lock Compliance mode).

ACLs and Ownership

There is only one set of permissions stored On-Disk using file system ACL's. These ACLs are backed up and restored. Along with the ACL’s, the ownership details of each share are backed up and restored folder individually.

File Store Security

In both security modes (NTFS and Legacy), File Stores are backed up including their security mode error flag. The security mode and error flag is set back on each File Store during restore.
Monitoring File Persona

Checking Health of Hardware and Software Components

The HPE 3PAR checkhealth CLI command checks the status of system hardware and software components, and reports any issues encountered.

From the CLI issue the checkhealth command. The syntax is as follows:

```
checkhealth [<options> | <component>...]  
```

where the following options are supported,

- **lite**
  - option performs a minimal health check.

- **svc**
  - option performs a thorough health check. This is the default option.

- **full**
  - option performs the maximum health check. This option cannot be used with the -lite option.

- **list**
  - option lists all components that can be checked.

- **quiet**
  - option will not display which component is currently being checked. Does not display the footnote if used with the -list option.

- **detail**
  - option displays detailed information regarding the status of the system.

- **<component>**
  - indicates the component to check. For example, fs for File Persona. Use the -list option to get the list of components that can be checked.

Monitoring File Persona Performance

In order to monitor File Persona’s Performance, use the srstatfs CLI command.

The following table summarizes the HPE 3PAR CLI System Reporter commands. See the HPE 3PAR Command Line Interface Reference for details about each command.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>srstatfsav</td>
<td>Displays system reporter performance reports for File Persona anti-virus.</td>
</tr>
<tr>
<td>srstatfsblock</td>
<td>Displays System reporter performance reports for File Persona block devices.</td>
</tr>
<tr>
<td>srstatfscpu</td>
<td>Displays system reporter performance reports for File Persona CPU usage.</td>
</tr>
<tr>
<td>srstatfsfpg</td>
<td>Displays system reporter performance reports for File Persona file provisioning groups.</td>
</tr>
</tbody>
</table>

Table Continued
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>srstatfsmem</td>
<td>Displays system reporter performance reports for File Persona memory usage.</td>
</tr>
<tr>
<td>srstatfsnet</td>
<td>Displays system reporter performance reports for File Persona Ethernet</td>
</tr>
<tr>
<td></td>
<td>interfaces.</td>
</tr>
<tr>
<td>srstatfsnfs</td>
<td>Displays system reporter performance reports for File Persona NFS.</td>
</tr>
<tr>
<td>srstatfssmb</td>
<td>Displays system reporter performance reports for File Persona SMB.</td>
</tr>
<tr>
<td>srstatfsftp</td>
<td>Displays system reporter performance reports for File Persona FTP.</td>
</tr>
<tr>
<td>srstatfssnapshot</td>
<td>Displays system reporter performance reports for File Persona snapshots.</td>
</tr>
<tr>
<td>srstatfshttp</td>
<td>Displays system reporter performance reports for File Persona Object Access API.</td>
</tr>
</tbody>
</table>

**NOTE:** SMB read and write statistics reported by `statfs -smb` or `srstatfssmb` commands will not account for data transferred via ODX.

---

**Monitoring File Persona Performance using SSMC**

From the system reporter in SSMC, follow the steps below:

- From the main menu, select Storage Systems > Systems.
- Select the System Reporter.
- Follow the instructions on the dialog that opens.

**Monitoring File Persona Performance using SNMP**

Services for File Persona can be pro-actively monitored with the help of the HPE 3PAR SNMP agent as described in the [HPE 3PAR CLI Admin Manual](#) (starting at page 162).

Information on the relevant alert references for File Persona is available in the [HPE 3PAR OS 3.2.2 MU3 Alerts Reference](#). File Persona can be monitored using objects such as File Provisioning Group, Virtual File Server, File Store, File Share, File Store snapshot and network state.

**Performance Monitoring for Object Access API Statistics**

File Persona's system's performance can be monitored using Object Access API statistics. The required CLI will display performance data reports for File Persona Object Access API. A new option `-http` has been added to the `statfs` HPE 3PAR Storeserv CLI command. Additionally, a new CLI command `srstatfshttp` has been implemented to provide additional performance reporting with greater flexibility of output formatting.

**statfs -http**

The `statfs -http` command shows Object Access API statistics for File Persona. The following is the syntax of command:

```
statfs -http [-iter <number> -d <secs> -node <nodeid> [,<nodeid>]... -verbose]
```

where,

- `-http`
  Displays Object Access API statistics.
- `-iter <number>`
Specifies that the statistics are to stop after the indicated number of iterations using an integer from 1 through 2147483647.

- **-d <secs>**

  Specifies the interval in seconds that statistics are sampled using an integer from 1 through 2147483. If no count is specified, the command defaults to 60 seconds. Information will only be updated every 60 seconds, any more frequent checks will redisplay same information

- **-node <nodeid>[,<nodeid>]...**

  Specifies the node for which statistics have to be reported.

- **-verbose**

  Specifies that all statistics will be displayed. Each statistic will be displayed on a separate line.

The option **-http** can be added to the statfs command to continuously display the performance report for each interval of 1 minute by default. This period can be changed by specifying the **-d** option.

Throughput rates for total bytes and number of I/O requests are given by default. For more detailed output, an option **-verbose** can be added. Output may exceed a single line, when the **-verbose** option is given. This option will print all the recorded statistics. Each statistic will be displayed on a separate line.

```
statfs -http
HTTP
22:45:22 11/30/2014
Node Requests/sec  KBServed/sec  bytes/request
 0            0           0.0           0.0
 1            0           0.0           0.0
---------------------------------------------
 2          0.0           0.0           0.0

Press the enter key to stop...
```

The following sample output displays the performance statistics in detail. Use the **-verbose option**.
```
statfs -http -verbose
22:01:06 12/03/2014
HTTP
--------Node 0--------
TotalAccess             :   6
TotalBytesServed       :   25
ApacheCPULoad           :   0.1565
ServerUptime            :   198
AverageRequestsPerSec   :   0.030303
AverageBytesPerSec      :   129.293
AverageBytesPerRequest  :   4266.67
BusyWorkerCount         :   1
IdleWorkerCount         :   4
Scoreboard              :   ........W..........(can be 128 characters long)
--------Node 1--------
TotalAccess             :   6
TotalBytesServed       :   25
ApacheCPULoad           :   0.1565
ServerUptime            :   198
AverageRequestsPerSec   :   0.030303
AverageBytesPerSec      :   129.293
AverageBytesPerRequest  :   4266.67
BusyWorkerCount         :   1
IdleWorkerCount         :   4
Scoreboard              :   ........W..........(can be 128 characters long)
Press the enter key to stop...
```

**srstatfshttp**

The `srstatfshttp` command displays File Persona Object Access API usage. The following is the syntax of the `srstatfshttp` command:

```
srstatfshttp [-attime -btsecs <secs> -etsecs <secs> -hires -hourly -daily -
groupby <node> -node <node>[,<node>...] -sortcol <col>[,<dir>]
[:<col>[,<dir>]...]]
```

where,

- **-attime**
  
  Performance is shown at a particular time interval, specified by the `--etsecs` option, with one row per object group described by the `--groupby` option. Without this option performance is shown versus time, with a row per time interval.

- **-btsecs <secs>**

  Select the begin time in seconds for the report. The value can be specified as either one of the following:

  - The absolute epoch time (e.g. 1351263600).
  - The absolute time as a text string in one of the following formats:
    - Full time string including time zone: "2012-10-26 11:00:00 PDT"
    - Full time string excluding time zone: "2012-10-26 11:00:00"
    - Date string: "2012-10-26" or 2012-10-26
    - Time string: "11:00:00" or 11:00:00
    - A negative number indicating the number of seconds before the current time. Instead of a number representing seconds, `--btsecs <secs>` can be specified with a suffix of m, h or d to represent time in minutes (e.g. -30m), hours (e.g. -1.5h) or days (e.g. -7d). If it is not specified then the time at which the report begins depends on the sample category (`-hires`, `-hourly`, `-daily`):
      - For hires, the default begin time is 12 hours ago (`-btsecs -12h`).```
- For hourly, the default begin time is 7 days ago (-btsecs -7d).
- For daily, the default begin time is 90 days ago (-btsecs -90d). If begin time and sample category are not specified then the time the report begins is 12 hours ago and the default sample category is hires. If -btsecs 0 is specified then the report begins at the earliest sample.

- -etsecs <secs>
  Select the end time in seconds for the report. If -attime is specified, select the time for the report. The value can be specified as either
  - The absolute epoch time (for example 1351263600).
  - The absolute time as a text string in one of the following formats:
    - Full time string including time zone: "2012-10-26 11:00:00 PDT"
    - Full time string excluding time zone: "2012-10-26 11:00:00"
    - Date string: "2012-10-26" or 2012-10-26
    - Time string: "11:00:00" or 11:00:00
    - A negative number indicating the number of seconds before the current time. Instead of a number representing seconds, -etsecs <secs> can be specified with a suffix of m, h or d to represent time in minutes (e.g. -30m), hours (e.g. -1.5h) or days (e.g. -7d). If it is not specified then the report ends with the most recent sample.

- -hires
  Select high resolution samples (5 minute intervals) for the report. This is the default.

- -hourly
  Select hourly samples for the report.

- -daily
  Select daily samples for the report.

- -groupby <groupby>[,<groupby>...]
  For -attime reports, generate a separate row for each combination of -groupby items. Each -groupby must be different and one of the following:
  - NODE The controller node
  - -node <node>[,<node>...]
  Limit the data to that corresponding to one of the specified nodes.

- -sortcol <col>[,<dir>][:<col>[,<dir>]...]
  Sorts command output based on column number (<col>). Columns are numbered from left to right, beginning with 0. At least one column must be specified. In addition, the direction of sorting (<dir>) can be specified as follows:

  inc
    Sort in increasing order (default).
  dec
    Sort in decreasing order.

  Multiple columns can be specified and separated by a colon (:). Rows with the same information in them as earlier columns will be sorted by values in later columns.

  By default the activity report for past 12 hours is displayed with a high sampling frequency of 5 minutes, which can be changed as per requirement.

  The following is a sample output of the srstatfshttp command:
Performance Parameters for Object Access API

The following table lists the parameters that can be used to measure the performance for Object Access API.

<table>
<thead>
<tr>
<th>CLI Output Name</th>
<th>XML Tag name from PML</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total accesses</td>
<td>TotalAccess</td>
<td>Total number of accesses to the Object share</td>
</tr>
<tr>
<td>Total KBserved</td>
<td>TotalBytesServed</td>
<td>Total number of bytes served in Kilo Bytes</td>
</tr>
<tr>
<td>Apache cpuload</td>
<td>ApacheCPULoad</td>
<td>CPU percentage used by the Apache(httpd) process</td>
</tr>
<tr>
<td>Server uptime</td>
<td>ServerUptime</td>
<td>Uptime since the last restart of the httpd server</td>
</tr>
<tr>
<td>Requests/sec</td>
<td>RequestsPerSec</td>
<td>Average number of requests served per second</td>
</tr>
<tr>
<td>bytes/sec</td>
<td>BytesPerSec</td>
<td>Average number of Bytes per second</td>
</tr>
<tr>
<td>bytes/request</td>
<td>BytesPerRequest</td>
<td>Average number of Bytes per request</td>
</tr>
<tr>
<td>Worker_count Busy</td>
<td>BusyWorkerCount</td>
<td>Number of Busy httpd workers</td>
</tr>
<tr>
<td>Worker_count Idle</td>
<td>IdleWorkerCount</td>
<td>Number of idle httpd workers</td>
</tr>
<tr>
<td>Scoreboard</td>
<td>Scoreboard</td>
<td>Representation on the server's current state.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>It is a group of 58 characters by default, it can be upto 128 characters.</td>
</tr>
</tbody>
</table>
Troubleshooting File Persona

Refer to the following list of possible troubleshooting scenarios that could arise when using File Persona.

1. **Problem:**
   Windows 2012 clients cannot see new/updated NFS files without refreshing the Windows Explorer window
   
   **Cause:**
   This is a Microsoft Windows Server 2012 (without R2) bug. Windows Server 2012 does not handle the SMB Notification of NFS updated files correctly. Whenever clients write something new, the Directory Change Notification (DCN) feature should show the Windows user the new files on the Windows Explorer window without having the user refresh the window.
   
   **Solution:**
   - Upgrade to Windows Server 2012 R2.
   - Use the function key F5 to refresh the window if the file you expect to see does not appear.

2. **Problem:**
   Performance of directory listing of a File Persona NFS share with an NFSv4 client slow when using LDAP
   
   **Cause:**
   There are known performance issues when NFSv4 and LDAP are paired that result in slow directory listing.
   
   **Solution:**
   There is no solution that exists from the File Persona side as this is an NFSv4 related issue. Alternatively, NFSv3 performs better.

3. **Problem:**
   NFS and Object Access API users don’t have folder access if permissions are given with the built-in “Domain Users” group
   
   **Cause:**
   This is an Active Directory behavior when the System Security Services Daemon (SSSD) is being used on a client in RFC2307 provisioned mode. The SSSD does not resolve the “Domain Users” group in an Active Directory.
   
   **Solution:**
   This is not a File Persona related issue. To resolve this, opt for BeyondTrust’s PowerBroker Identity Services Open instead of using SSSD on the client experiencing the issue. BeyondTrust’s PowerBroker Identity Services Open will resolve the "Domain Users" group in both provisioned mode (RFC2307 is on) and non-provisioned mode (RFC2307 is off).

4. **Problem:**
   Setting LSASS provisioned mode fails to provide NFSv4 ID mapping
   
   **Cause:**
   Setting the Local Security Authority Subsystem Service (LSASS) in provisioned mode will fail to provide NFSv4 ID mapping without the Schmmgmt.dll file installed. This is only seen when the RFC2307 mode is on, and only on Active Directory servers that do not have the Schmmgmt.dll file loaded.
   
   **Solution:**
Load the Schmmgmt.dll provided by Microsoft Windows. Windows Server 2012 R2 has the Schmmgmt.dll file loaded by default. Windows Server 2008 doesn't load it by default. To load the Schmmgmt.dll on the Windows Server 2008 run the command: regsvr32 schmmgmt.dll

5. Problem:
When restricting access to domain NFS shares if wildcard option is used to specify the Client IP an error is generated

Cause:
When restricting access to domain NFS shares, a Fully Qualified Domain Name (FQDN) of the host should be specified. If the wildcard option is used when specifying the client IP there might be an issue.

Solution:
Reverse lookup allows clients on the domain access to mount an NFS share. When restricting access to domain NFS shares, specify an FQDN. When configuring Reverse lookup configure the FQDN and not an alias. Example: Do not use an alias like sys1. Use the FQDN: sys1.hpe.com.

6. Problem:
Incorrect scan count found when a read operation is performed on infected files using Object Access API

Cause:
When a file is scanned and is found to be infected, a quarantined link pointing to the infected file is created and the permission of the file is changed to "access denied". If the creation of the quarantine link fails due to limitations on quota, the file is not stamped as scanned. Since the file is not marked as scanned, the filesystem will trigger the file for scanning whenever accessed till the quarantined link to the file has been created successfully and has been marked as stamped.

Solution:
There is an upper limit on the inode quota in the system. When the limit is reached, the user will get a warning and the user is expected to perform further action, such as remove files or increase the limit to make quota available.

7. Problem:
When editing WORM files in the vi editor, empty files are being created in File Store

Cause:
If you attempt to edit a WORM file in the retained state, applications such as the vi editor will be unable to edit the file, but will leave empty temporary files on the File Store. User must manually delete these temporary files.

Solution:
This is a typical vi editor behavior, WORM logic has no control over how these temporary files are created or deleted by the vi application. This condition is benign for the end user.

8. Problem:
Applications such as vi editor appear to update WORM files with the default retention period

Cause:
If you use an editor such as vi to edit a WORM file that is not in the retained state, the file will be modified and it will be retained with the default retention period.

Solution:
This is expected behavior. The file modification occurs because the vi editor edits a temporary copy of the file, tries to rename it to the real file, and when this fails, it deletes the original file and then renames it, which succeeds (because unretained WORM files are allowed to be deleted). Avoid the use of vi to edit WORM files that are not in retained state.

9. Problem:
The retention period of a WORM or retained files extracted from a tar file is different from the original file

**Cause:**
When a tar file with WORM or retained files is extracted, the retention period of the extracted files will be reset to the default retention period from the time of file extraction.

**Solution:**
This is expected behavior. This will be observed if the Tar tool version is v1.16_1 or above.

10. **Problem:**
   Failed to failover `fpg_name`:
   **Cause:**
   Existing operation mountFileSystem for FPG `fpg_name` is already pending and is in conflict with the requested mountFileSystem operation.
   **Solution:**
   Wait for a few seconds and retry the failover on the FPG.

11. **Problem:**
    Error message "Argument list too long" error message in showfsarchive, removefsarchive or setfsarchive commands
    **Cause:**
    This error occurs when the command line length exceeds the kernel limitation.
    **Solution:**
    Use the `inputfile` option in the `showfsarchive/removefsarchive/setfsarchive` commands. Please make note of the following:
    - Wild card characters are not supported when using the `inputfile` option.
    - All the files/directories inside the directory provided in the `inputfile` are accounted recursively.

12. **Problem:**
    Difference in quota capacity when passed from an archived config file in comparison to the values listed using `showfsquota` command
    **Cause:**
    When quota is set using `setfsquota` command the soft and hard limit of quota is set in MB. Whereas, the archived quota config file has its quota values set in KB.
    **Solution:**
    The configurations settings of the `setfsquota` command and archive quota config file are structured this way. There is no solution to this problem, but being aware of the difference in the quota units.

13. **Problem:**
    Antivirus scan on a Virtual File Server (VFS) or a File Store failing
    **Cause:**
    Check to see whether the File Provisioning Group is full or not.
    **Solution:**
    The File Provisioning Group (FPG) cannot initiate an antivirus scan if it is full.
    Remove files or increase the size of the FPG to make space available.

14. **Problem:**
User/group name/ID/SID lookup fails with error 40, 404 or 40, 405 when username mapping is enabled

**Cause:**
This condition happens when the "ToName" user or group has been configured with a UID/GID value of less than 1

**Solution:**
Ensure that UID/GID values less than 1 are not used in the "ToName" user or group.

15. **Problem:**
Unable to mount an SMB share. Error Access denied. Can mount SMB share only with the Local_cluster\administrator user. The share was created on an NTFS enabled File Store with Everyone:fullcontrol permissions

**Cause:**
The Everyone:fullcontrol permission given at the share creation is specific to the SMB share which is checked before the Access Control List (ACL) is read. This problem is NOT related to the ACL on the share root directory. This is a general Windows behavior and is not specific to File Persona.

**Solution:**
The share root directory must have an ACL that permits specific users access. In NTFS security mode, the default permissions at the share root directory can be changed from:

- Windows Client's SYSTEM@NT_AUTHORITY or Window's Domain Administrator
- Via the 3PAR CLI or GUI (SSMC)

In NTFS security mode, if a share is created at the File Store root, default share directory permissions are as follows:

- From a Windows Client:
  - Everyone has permissions to mount and traverse to the mount point from a Windows client (non-inheritable permissions).
  - Only SYSTEM@NT_AUTHORITY (equivalent to root in Windows), and members of the Administrators group in the Windows domain have additional permissions, full-control (inheritable permissions).

- From an NFS Client (or a POSIX client):
  - Everyone has permissions to traverse to the mount point (non-inheritable permissions)
  - Only members of the Administrators group (if in the same domain as server node) have additional permissions, full-control (inheritable permissions).

If a share is created at any level below the File Store root, share directory permissions are inherited from the parent directory.

- From a Windows Client:
  - Only SYSTEM@NT_AUTHORITY (equivalent to root in Windows), and members of the Administrators group in the Windows domain have any permissions, full-control (inheritable permissions).

- From an NFS Client (or a POSIX client):
  - Only members of the Administrators group (if in the same domain as server node) have permissions, full-control (inheritable permissions).

16. **Problem:**
When Robocopy is run to copy files in an SMB share, all new, edited and unedited files are being copied.

**Cause:**
Robocopy incorrectly detects files as new when copying between different file systems. Robocopy compares the time stamp for each file at a very granular level and due to this assumes that each file has been edited. Consequently it copies each file at every run.

**Solution:**

Use the command `robocopy` with the `/FFT` option: `robocopy /FFT`. This forces robocopy to use FAT style time stamps which have a 2-second granularity. This granularity allows enough time difference to account for when copying a file from NTFS to another file system.

17. **Problem:**

No alert generated when LDAP is configured incorrectly.

Customers may think their LDAP is configured correctly when it isn't working properly.

**Cause:**

Using incorrect settings to configure LDAP.

**Solution:**

Run the `showfs -ldap` command and check the base parameter value whether it is being shown correctly or not.

Try querying any LDAP user. If the user query is successful then the configuration is correct.

18. **Problem:**

Changing bond mode when file services were active resulted in loss of network access

**Cause:**

Once file services have been put into operation and are in active use, changing the network bond mode from 6 to 1 (or vice versa) may result in loss of network access to file services.

**Solution:**

It is recommended that file services be taken temporarily out of operation before changing bond mode and then returned to operation. The following steps can be used to set bond mode safely (note that this process will cause a temporary outage, so choose a time of low usage when performing these steps).

Issue the series of commands below and follow instructions:

- `#setfs bond 1`
- Stop and restart file services on all nodes.
- `#stopfs -f`
- `#waittask`
- `#startfs -enable`
- `#waittask`
- Check that all nodes have restarted the file services correctly or not.
- `#showfs`
- Verify that all the FPGs are in the expected states.
- `#showfpg`

19. **Problem:**

Object Access API client is hanging for hours in the event of a slow network, a network link not working or when the server node is down

**Solution:**

To avoid this, use the timeout option provided by the client. It will prevent the Object Access API client requests from hanging. Use this client timeout option when running Object Access API I/O.

20. **Problem:**
The ACL of a file in an NFSv3 File Share in NTFS security mode can be changed

**Cause:**
This is not expected behavior. Ignore this result.

**Solution:**
In order to ensure that NTFS ACLs are preserved, POSIX clients in NTFS security mode are not allowed to execute permission changing operations. This is enforced by not allowing the "no_root_squash" to be mounted and by denying operations that can change the mode bits, ownership or ACLs on files when issued from POSIX clients. To avoid any unforeseen impact on POSIX applications, the "secop_errsupress" option exists. If this option is set to "true" on an NTFS File Store, File Persona treats that permission changing operation as a NO-OP and returns success without actually performing the operation. While this allows for the application to continue without any impact, this might yield false-positive results while checking permissions on the files/directories that just got changed from the client due to client-side caching. The client might think this operation succeeded and cache the attribute’s value. If the user desires to use POSIX ACLs, please be aware of this side effect and ignore this result.

21. **Problem:**
NDMP restore is throwing an error message as "Restore partially successful" even though the all of the data is being restored

**Solution:**
When selecting the file list for restore using NetBackup, it is recommended that the user expands the restore file path selection tree and makes the selection on the lower levels. This will make sure that the proper status of restore operation is returned. If the user clicks on a box at root level, it will cause NetBackup to throw the error message saying "Operation partially successful.

22. **Problem:**
The `showfsquota` command does not show the NetBIOS name in the LDAP user quota

**Cause:**
Name lookups for local and LDAP providers don't require any domain component. If the same name is added to both the providers, the first provider in the provider-stacking will resolve the name. A NetBIOS name was added for LDAP as a domain component to provide a way to distinguish duplicate names. POSIX names don't commonly have domain components, so the domain component was made optional as is the case for local user names. NFS passes POSIX/LDAP names without any domain component so it is critical that we continue to resolve LDAP names without them.

**Solution:**
It is recommended that customers don't use the same name in multiple name services. Entering quotas without a domain component for local and LDAP accounts should be seen as bad practice even though it isn't a requirement because of the potential for quotas being enforced on the wrong account. The quota written to the cache and reported should report the domain component to protect against a change in the provider stacking from changing accounts where quotas are enforced. This would be a very severe issue.

23. **Problem:**
Files written by an unmapped AD user with a mapped primary group fail to be counted in the group quota

**Cause:**
File persona does not support mapping of group membership.

**Solution:**
Group mapping rules are mainly required to support mapping of primary group's identity. A group mapping rule will not have members of one group to have the same access privileges as the mapped group’s members unless the members themselves can be mapped. This also means quota accounting
for groups will not account for the members of the mapped group unless there is an explicit mapping for
the member.

24. Problem:
When an SMB share is created with user mapping an error message is being returned: "File too
large - The file '<%1 NULL:NameDest>' is too large for the destination file
system"

Cause:
This happens when the user's primary group is not mapped.

Solution:
If the group names between both the providers are the same and if the mapping file has a dynamic rule,
the dynamic mapping rule also applies to groups. However, if the group names are not the same across
the providers then there has to be a specific mapping rule for the desired group names. While the
mapping rule for supplemental groups may be added as needed, for a bidirectional mapping to work, the
user's primary group has to be mapped either using a specific static rule or a dynamic rule.

25. Problem:
Permissions are given to a specific user for read/write but the user cannot read/write from the NFS client

Cause:
The setting permissions in the NTFS security mode can only be done from a Windows client or the HPE
3PAR CLI (for share folders). Both of these have a higher fidelity than UNIX permissions. The system
converts these permissions to UNIX permissions for enforcement on UNIX clients (like NFS).

Solution:
The user must be aware of the mapping in the conversion. Refer to the Permission Conversion Rules:
Converged ACL to/from POSIX ACLs section to understand the permissions that will be granted to a
Windows or a POSIX client.

Example: If "user2" has “read” permissions for a directory but “user2” is still getting permission errors
when reading from an NFS client:
Set both ‘r’ and ‘n’ permissions using the Windows or Converged ACL.

26. Problem:
The ownership is set properly and the user has the required permissions to create files but still the files
cannot be created

Solution:
Check whether the associated ID with the user is consistent across the server and client. In Active
Directory, the client and server should be RFC2307 enabled. For NFSv4 to work properly using AD with
RFC2307 enabled, both the client and server should be configured with the same NFSv4 domain for
proper ID mapping. Whereas, in LDAP, even though the IDs are consistent, the parent directory on the
server in the export path will not permit the user. Access will not be allowed as LDAP does not support
the SeChangeNotify command. A possible solution is that the parent directory is shared without any
permissions and the permissions are modified using the setfshare command.

27. Problem:
Could not map or access the File Share as a regular domain user even though it was possible in Legacy
mode

Cause:
The default permissions in the share folder are specific to the security mode, independent of the protocol
of the share. The default permissions at the share folder in the NTFS security mode are more restrictive
than the SMB share folder permissions in the Legacy mode.
Solution:
The administrators have the option to modify the permissions at the share folder using the HPE 3PAR
CLI (setfshare command with -acl option). Make sure the permissions are added in the share folder
for the user that desires access.

28. Problem:
Even though it was possible to create, read and write files from both Windows and NFS clients on an
NTFS File Store, now the NFS client is returning an error

Cause:
With native ACLs On-Disk, there are no dependencies on name services for the primary protocol access
(in NTFS mode once authentication has been completed). However, there are a few dependencies on
the name services for the secondary protocol once it is accessed. So name services can create
intermittent access issues for the secondary protocol in a cross-protocol environment.

Solution:
Check whether the name services are working or not. Also, check whether the name resolution is
configured consistently across the server and clients.

29. Problem:
FTP and Object Access API requests are flooding the LDAP server with bind requests

Cause:
If the LDAP server is configured to log bind or unbind requests, the LDAP server log could grow fast.

Solution:
FTP and Object Access API access protocols require LDAP authentication to make a temporary
connection with the LDAP server. To overcome this issue, try disabling the LDAP server log for bind/
unbind. Also, implement the LDAP server log maintenance (log rotation)

30. Problem:
Error occurring when using wild cards in captive CLI.

Example:
```
removefsarchive retention -files /fpg2/vfs2/fstore2N/patient_records/
PatientD1-1[0-9].txt -fpg fpg2 -fstore fstor2N vfs2
invalid command name "0-9"
```

Solution:
Use "\" character to escape the wild card error.

Example:
```
setfsarchive legalhold -set -files "/fpg2/vfs2/fstore2N/patient_records/
PatientD1/PatientD1-1\[0-9\]_PatientD1.Jun_06_2017" -fstore fstore2N -fpg
fpg2 vfs2
```
File Persona configuration preparation

Once the storage system has been installed, the following tasks are involved in preparing for the configuration of File Persona:

1. **Cabling for File Persona**—Install network cables to connect the ports on the NIC PCIe host adapters that are configured for File Persona to the network switch infrastructure.

2. **Configure the controller nodes for File Persona**—Enable File Persona on the controller node pairs and define the File Persona controller node networking and naming services.

3. **Define Virtual File Server for File Persona**—Define Virtual File Servers and IP addresses to present shares.

4. **Define and present file shares for File Persona**

5. **Configure Data Management for File Persona**—Backup, snapshots, and replication

File Persona controller node worksheet

<table>
<thead>
<tr>
<th>Item</th>
<th>Answer/Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>For which of the following controller-node pairs will the File Persona be enabled?</td>
<td>• Controller node 0 and controller node 1&lt;br&gt; • Controller node 2 and controller node 3&lt;br&gt;<strong>If hardware supports:</strong>&lt;br&gt; • Controller node 4 and controller node 5&lt;br&gt; • Controller node 6 and controller node 7</td>
</tr>
<tr>
<td>What type of NIC PCIe host adapters have been installed for slot 2 of each controller node for use with File Persona?</td>
<td>• 4-port 1 GbE NIC&lt;br&gt; • 2-port 10 GbE NIC&lt;br&gt;• <strong>Only for the HPE 3PAR StoreServ 8000:</strong>&lt;br&gt; 4-port 10 Gb iSCSI/10 Gb Ethernet combo&lt;br&gt; 2-port 16 Gb FC/2-port 10 Gb Ethernet combo</td>
</tr>
<tr>
<td>How many connections will be made from each network card to the network switch?</td>
<td>File Persona requires at least one network connection from each 3PAR controller where File Persona is to be enabled.</td>
</tr>
</tbody>
</table>

Table Continued
### File Persona controller node worksheet

<table>
<thead>
<tr>
<th>Item</th>
<th>Answer/Value</th>
</tr>
</thead>
</table>
| Which bond mode will be used? | File Persona supports the following bond modes:  
- 4-port 1 GbE NIC: Mode 1 (Active/Passive) or Mode 6 (Adaptive load balancing)  
- 2-port 10 GbE NIC: Mode 1 (Active/Passive)  
- Only for the HPE 3PAR StoreServ 8000: 4-port 10 Gb iSCSI/10 GbE NIC combo  
- Only for the HPE 3PAR StoreServ 8000: 4-port 16 Gb FC/10 GbE NIC combo  
All controller nodes will use the same bond mode. |
| Has the switch infrastructure been configured to support the controller-nodes connection for File Persona? | Answer: Yes or No |

### File Persona Activation and Networking worksheet

The following worksheet captures the information necessary to activate and install File Persona and includes the information necessary for the controller-node networking and services such as naming, authentication, anti-virus and backup. Each controller node configured for File Persona is assigned an IP address that is used to connect to services such as Active Directory and DNS. These IP addresses are not used for share access.

**IMPORTANT:**

The File Persona controller nodes use the same time as is set for the storage system controller nodes. Ensure that the storage system controller nodes are synchronized to an authoritative time source. If using Active Directory with File Persona, ensure that the storage system and the Active Directory domain controllers synchronize their time with the same source.

<table>
<thead>
<tr>
<th>Item</th>
<th>Answer/Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address for File Persona controller node 0</td>
<td>An IPv4 address is required for each controller node that will have File Persona enabled.</td>
</tr>
<tr>
<td>IP address for File Persona controller node 1</td>
<td></td>
</tr>
<tr>
<td>IP address for File Persona controller node 2</td>
<td></td>
</tr>
<tr>
<td>IP address for File Persona controller node 3</td>
<td></td>
</tr>
</tbody>
</table>

*Table Continued*
### File Persona Activation and Networking worksheet

<table>
<thead>
<tr>
<th>Item</th>
<th>Answer/Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address for File Persona controller node 4</td>
<td></td>
</tr>
<tr>
<td>IP address for File Persona controller node 5</td>
<td></td>
</tr>
<tr>
<td>IP address for File Persona controller node 6</td>
<td></td>
</tr>
<tr>
<td>IP address for File Persona controller node 7</td>
<td></td>
</tr>
<tr>
<td><strong>Network Settings: VLAN Tag for File Persona controller node</strong></td>
<td>Use of VLAN tags is optional. 0 is the default tag.</td>
</tr>
<tr>
<td><strong>Network Settings: Subnet Mask for File Persona controller node</strong></td>
<td>The subnet mask is applicable to all File Persona nodes.</td>
</tr>
<tr>
<td><strong>Network Settings: Gateway</strong></td>
<td></td>
</tr>
<tr>
<td>File Persona supports a single default gateway which is used both for access to network services such as DNS and during the presentation of shares to clients.</td>
<td></td>
</tr>
<tr>
<td><strong>Network Settings: MTU size</strong></td>
<td></td>
</tr>
<tr>
<td>The default MTU size is 1500. Only change from the default if all components in the network switch infrastructure support the custom frame size.</td>
<td></td>
</tr>
<tr>
<td><strong>List the DNS servers to be used by File Persona.</strong></td>
<td>File Persona supports up to 3 DNS servers.</td>
</tr>
<tr>
<td><strong>List the DNS Search Suffixes.</strong></td>
<td></td>
</tr>
</tbody>
</table>

### File Persona Authentication settings worksheet

File Persona supports resolution of user credentials through Active Directory, LDAP or local users and groups. Use the following table to capture the configuration information for the selected Authentication providers.
<table>
<thead>
<tr>
<th>Item</th>
<th>Answer/Value</th>
</tr>
</thead>
</table>
| **Which external Authentication providers will be used?** | • Active Directory:
• LDAP: |
| In addition to local, File Persona supports Active Directory and LDAP. | |
| **Active Directory**? | Answer: Yes or No |
| **LDAP**? | Answer: Yes or No |
| **List the order in which Authentication providers should be used to resolve user credentials.** | • 1st:
• 2nd:
• 3rd: |
| Answer example: If File Persona was used to present SMB shares to Windows clients, the following would be the order: 1st: Active Directory, 2nd: Local, and 3rd: Not Used | |
| **Active Directory: Domain Name** | |
| Record the Active Directory Domain Name that the system will join for Authentication services. All File Persona controller nodes will join the same Domain. | By default, an account will be created in the Computers OU for each node using the naming format &lt;3PAR Serial number&gt;-&lt;node number&gt;.

**Active Directory: User name and password** | |
| Identify an Active Directory user that has sufficient privileges to allow the File Persona nodes to join the Active Directory Domain. | |
| **Active Directory: File Persona Share Administrator** | |
| Optional: If an account with domain administrator privileges cannot be used to manage the File Persona share(s) permissions. Then an account must be defined which can be used to manage File Persona share(s) permissions to the “BUILTIN\Administrators” group with the HPE 3PAR CLI command setfsgroup -memberlist +&lt;domain account&gt; Administrators. | |
| **LDAP: Server Host** | |
| **LDAP: Bind DN** | |
| **LDAP: Base of search** | |
| **LDAP: NetBios name** | |
| **LDAP: Password (optional)** | |
| Password associated with the bind DN | |
| **LDAP: Schema** | Answer: Posix or Samba |
| Posix is the default. | |

*Table Continued*
<table>
<thead>
<tr>
<th>Item</th>
<th>Answer/Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>LDAP: Provide a Certificate (optional)</strong></td>
<td></td>
</tr>
<tr>
<td>Answer: Yes or No</td>
<td></td>
</tr>
<tr>
<td>Use of an LDAP certificate is optional</td>
<td></td>
</tr>
<tr>
<td><strong>LDAP: Certificate Protocol</strong></td>
<td></td>
</tr>
<tr>
<td>Answer: TLS or SSL</td>
<td></td>
</tr>
<tr>
<td>Only needed if using an LDAP certificate</td>
<td></td>
</tr>
<tr>
<td><strong>LDAP: Certificate common name</strong></td>
<td></td>
</tr>
<tr>
<td><strong>LDAP: Certificate file</strong></td>
<td></td>
</tr>
<tr>
<td>Identify the file containing the the LDAP certificate</td>
<td></td>
</tr>
</tbody>
</table>

**File Persona protocol settings worksheet**

Use the following tables to configure the NFSv4 and Object.

### File Persona NFSv4 worksheet

<table>
<thead>
<tr>
<th>Item</th>
<th>Answer/Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>NFSv4 idmap domain</strong></td>
<td></td>
</tr>
<tr>
<td>NFSv4 domain name and Active Directory names are not synonymous.</td>
<td></td>
</tr>
<tr>
<td>Specifies NFSv4 domain name for ID mapping. For NFSv4 to work correctly, the NFSv4 client and the NFSv4 server need to be in the same NFSv4 domain.</td>
<td></td>
</tr>
<tr>
<td>If NFSv4 is intended to be used with IDs instead of UPN names like NFSv3, do not configure NFSv4 ID map domain both at the server and the client.</td>
<td></td>
</tr>
</tbody>
</table>

### File Persona Object worksheet

<table>
<thead>
<tr>
<th>Item</th>
<th>Answer/Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Allow persistent connections</strong></td>
<td></td>
</tr>
<tr>
<td>Answer: True or False</td>
<td></td>
</tr>
<tr>
<td>The default value is True.</td>
<td></td>
</tr>
<tr>
<td><strong>Connection timeout (seconds)</strong></td>
<td></td>
</tr>
<tr>
<td>Specifies the timeout value in seconds for the persistent connections for the default Object profile. The valid range is from 1 to 2592000.</td>
<td></td>
</tr>
<tr>
<td>The default value is 5 seconds.</td>
<td></td>
</tr>
</tbody>
</table>
**File Persona Object worksheet**

<table>
<thead>
<tr>
<th>Item</th>
<th>Answer/Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Maximum simultaneous connections</strong></td>
<td></td>
</tr>
<tr>
<td>Specifies the maximum number of simultaneous connections for the default Object profile. The valid range is from 1 to 128. The default value is 50 connections.</td>
<td></td>
</tr>
<tr>
<td><strong>Read block size</strong></td>
<td></td>
</tr>
<tr>
<td>Specifies the socket read block size for the default Object profile. The valid range is from 8 K to 2048 M bytes. The default value is 8 K.</td>
<td></td>
</tr>
<tr>
<td><strong>Write block size</strong></td>
<td></td>
</tr>
<tr>
<td>Specifies the file write block size for the default Object profile. The valid range is from 8 K to 2047 M bytes. The default value is 8 K.</td>
<td></td>
</tr>
</tbody>
</table>

**File Persona Local Groups and Users worksheet**

If local groups and users are to be used for user authentication, complete the following tables. Valid UID and GID are in the range 1000 to 65535.

**NOTE:**
The maximum number of Local User accounts supported using the local authentication provider is 200. However, the optimal number of user accounts recommended by Hewlett Packard Enterprise is 50 or less. In environments requiring 50 or more user accounts, Hewlett Packard Enterprise recommends the use of a directory service (Active Directory or Lightweight Directory Access Protocol) as authentication providers.

<table>
<thead>
<tr>
<th>Local Group Name</th>
<th>GID (Optional)</th>
<th>Group Members</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
File Persona Local and Primary Groups worksheet

<table>
<thead>
<tr>
<th>Local User Name</th>
<th>UID (Optional)</th>
<th>Primary Group</th>
<th>Additional Groups</th>
<th>Enable User on Creation?</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

File Persona User Identity Mapping with RFC2307 for Active Directory worksheet

File Persona supports RFC2307 for Active Directory. When RFC2307 is enabled, the Active Directory (AD) service provides the GIDs and UIDs.

Enable the user identity Mapping (RFC2307) feature only when recommended.

If the default setting is disabled, the HPE 3PAR StoreServ Storage formulates the UIDs and GIDs for all AD users and groups based on the Security Identifier (SID).

When RFC2307 is enabled, you must specify a unique UID for every user and a unique GID for every group in AD. If RFC2307 is enabled and the user does not have a configured UID or GID in AD, the user is not given write access even if they are granted access through an Access Control List (ACL).

File Persona User Identity Mapping worksheet

<table>
<thead>
<tr>
<th>Item</th>
<th>Answer/Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Identity Mapping (RFC2307) for the Active Directory provider</td>
<td></td>
</tr>
<tr>
<td>Answer: <strong>Enable</strong> or <strong>Disable</strong></td>
<td></td>
</tr>
<tr>
<td><em>(Disable is the default and recommended value)</em></td>
<td></td>
</tr>
</tbody>
</table>

This should be enabled only if the Active Directory is configured with Windows Services for UNIX(SFU) with each user and group object is configured with UID and GID values properly. Active Directory is supposed to be used as the authentication provider for cross-protocol access between the server, Windows and POSIX clients without any user mapping.

If enabled, File Persona expects UIDs and GIDs to be found in Active Directory and not formulated using the SID as is the default behavior. This allows user to customize UIDs and GIDs. If RFC2307 is enabled and the user does not have a configured UID/GID in Active Directory, write access is prevented, even if granted through an ACL.
A Virtual File Server (VFS) presents virtual IP addresses to allow clients to access shares. Policies for user and group quota management and antivirus policies are managed at the VFS level. A VFS comprises up to 4 IP addresses and a minimum of 1 TiB of storage.

Each VFS leverages a File Provisioning Group (FPG), an instance of the HPE Adaptive File System (AFS), to control how files are stored and retrieved. The FPG has a minimum size of 1 TiB and is assigned storage from a HPE 3PAR Common Provisioning Group (CPG). There is a 1:1 mapping between a VFS and an FPG.

Replicate the following table for each VFS.

**IMPORTANT:**

DO NOT use the `fs_cpg` Common Provisioning Group (CPG) when provisioning File Provisioning Groups (FPGs). The `fs_cpg` is the default CPG for the File Persona Software and should not be used.

**NOTE:**

Anti-Virus Policies, Quotas and Snapshots can be defined against a VFS post installation.

<table>
<thead>
<tr>
<th>Item</th>
<th>Answer/Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the VFS.</td>
</tr>
<tr>
<td>Comment</td>
<td>Optional description of the VFS</td>
</tr>
<tr>
<td><strong>Storage Allocation: Size</strong></td>
<td>The minimum size allowed for an FPG is <strong>1</strong> TB. Maximum FPG size is <strong>32</strong> TB. Each pair of nodes can manage a maximum of <strong>64</strong> TB.</td>
</tr>
<tr>
<td><strong>Storage Allocation: CPG</strong></td>
<td>Identify the CPG to be used to provide storage for this VFS. File Persona will automatically create an FPG when you create the VFS and specify the CPG.</td>
</tr>
<tr>
<td><strong>Networking: IP Address, Subnet mask, VLAN TAG</strong></td>
<td>List the IP address(es) to be assigned to the VFS. The VLAN TAG is optional and defaults to <strong>0</strong>. Each VFS supports up to 4 IP addresses.</td>
</tr>
<tr>
<td><strong>Primary Node</strong></td>
<td>Optional: File Persona will automatically assign a Primary Node for the FPG associated with the VFS. This can be manually assigned if necessary</td>
</tr>
<tr>
<td><strong>VFS level SMB File Access Audit settings</strong></td>
<td></td>
</tr>
</tbody>
</table>
File Persona File Store Snapshot worksheet

File based snapshots policies are assigned to File Stores. Describe the snapshot requirements for each File Store including any scheduling of snapshots required.

<table>
<thead>
<tr>
<th>File Persona File Store Snapshot worksheet</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notes:</td>
</tr>
</tbody>
</table>

File Persona SMB Shares worksheet

The following table can be used to capture the configuration information for an SMB share. Replicate the following table for each Share.

**IMPORTANT:**
In most cases, it will be necessary to customize an SMB share’s NTFS level permissions before putting it into production use. SMB share level permissions can be managed using HPE 3PAR SSMC, but NTFS level permissions must be managed from an SMB client. From an SMB client, any account with Domain Administrator privileges can manage NTFS level permissions on a mapped share using standard Windows tools such as Windows Explorer. If you want to grant other domain users or groups the rights to manage share permissions, add them to the File Persona “BUILTIN\Administrators” group with the HPE 3PAR CLI `setfsgroup -memberlist +<domain account> Administrators` command.

<table>
<thead>
<tr>
<th>Item</th>
<th>Answer/Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Share Name</td>
<td>Name of the SMB Share.</td>
</tr>
<tr>
<td>Comment</td>
<td>Optional description of the Share.</td>
</tr>
<tr>
<td>Share Path: Virtual File Server</td>
<td>Identify the VFS used to present the share.</td>
</tr>
<tr>
<td>Share Path: File Store</td>
<td>Name of the File Store to use for the Share.</td>
</tr>
<tr>
<td>Share Path: Subdirectory</td>
<td>Additional path within the File Store to be used for this share.</td>
</tr>
<tr>
<td>Client Filter: Allow list</td>
<td>Optional: List the clients allowed to access the Share.</td>
</tr>
</tbody>
</table>
### File Persona SMB Shares worksheet

<table>
<thead>
<tr>
<th>Item</th>
<th>Answer/Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Client Filter: Deny list</strong></td>
<td></td>
</tr>
<tr>
<td>Optional: List the clients denied access to the Share.</td>
<td></td>
</tr>
<tr>
<td><strong>Permissions: User/Group, Type, Setting</strong></td>
<td></td>
</tr>
<tr>
<td>By default, the Share will be created without any access permissions.</td>
<td></td>
</tr>
<tr>
<td>Type options: <strong>Allow</strong> or <strong>Deny</strong>.</td>
<td></td>
</tr>
<tr>
<td>Setting options: <strong>Read Only</strong>, <strong>Change</strong>, or <strong>Full Control</strong>.</td>
<td></td>
</tr>
<tr>
<td>Example answer: <strong>Everyone, Allow, Read Only</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Settings: Access Based Enumeration</strong></td>
<td></td>
</tr>
<tr>
<td>Answer: <strong>Enable</strong> or <strong>Disable</strong></td>
<td></td>
</tr>
<tr>
<td>Access Based Enumeration is disabled by default.</td>
<td></td>
</tr>
<tr>
<td><strong>Settings: Continuous Availability</strong></td>
<td></td>
</tr>
<tr>
<td>Answer: <strong>Enable</strong> or <strong>Disable</strong></td>
<td></td>
</tr>
<tr>
<td>Specifies if SMB3 continuous availability features should be enabled for this share, enabled by default.</td>
<td></td>
</tr>
<tr>
<td><strong>Settings: Offline File Support</strong></td>
<td></td>
</tr>
<tr>
<td>Answer: <strong>off</strong>, <strong>manual</strong>, <strong>optimized</strong>, or <strong>auto</strong></td>
<td></td>
</tr>
<tr>
<td>Specifies client-side caching for offline files. The default is manual.</td>
<td></td>
</tr>
<tr>
<td><strong>Settings: File Access Audit</strong></td>
<td></td>
</tr>
</tbody>
</table>

### File Persona NFS Shares worksheet

The following table can be used to capture the configuration information for an NFS share. Replicate the following table for each NFS share.

**NOTE:**

The following will be the export path for an NFS share:

```text
<VFS IP>:<FPG>/<VFS>/<File Store>/<subdirectory>
```

<table>
<thead>
<tr>
<th>Item</th>
<th>Answer/Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Share Name</strong></td>
<td>Name of the NFS Share.</td>
</tr>
<tr>
<td><strong>Comment</strong></td>
<td>Optional description of the Share.</td>
</tr>
</tbody>
</table>
### File Persona NFS Shares worksheet

<table>
<thead>
<tr>
<th>Item</th>
<th>Answer/Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Share Path: Virtual File Server</td>
<td></td>
</tr>
<tr>
<td>Identify the VFS used to present the share.</td>
<td></td>
</tr>
<tr>
<td>Share Path: File Store</td>
<td></td>
</tr>
<tr>
<td>Name of the File Store to use for the Share.</td>
<td></td>
</tr>
<tr>
<td>Share Path: Subdirectory</td>
<td></td>
</tr>
<tr>
<td>Additional path within the File Store to be used for this share.</td>
<td></td>
</tr>
<tr>
<td>Settings: Client Filter List</td>
<td></td>
</tr>
<tr>
<td>Specifies the clients that can access the share.</td>
<td></td>
</tr>
<tr>
<td>If this is not specified, the default is &quot;*&quot;.</td>
<td></td>
</tr>
<tr>
<td>It is recommended that a proper client IP list is specified for each export to ensure only valid clients are allowed to access the share. Also, the exports with no_root_squash are recommended to be allowed only from the clients where the administrator will mount the export to perform folder administration. Multiple exports for the same path can be created as long as the client IPs don't overlap for unique share privilege and Share Permission combination.</td>
<td></td>
</tr>
<tr>
<td>Share Permission</td>
<td></td>
</tr>
<tr>
<td>Answer: Read Only or Read Write</td>
<td></td>
</tr>
<tr>
<td>Share Privilege</td>
<td></td>
</tr>
<tr>
<td>Answer: root_squash or no_root_squash</td>
<td></td>
</tr>
<tr>
<td>Additional Share options</td>
<td></td>
</tr>
<tr>
<td>List additional share options to be defined.</td>
<td></td>
</tr>
<tr>
<td>Settings: File Access Audit</td>
<td></td>
</tr>
</tbody>
</table>

### File Persona Object Access API Shares worksheet

The following table can be used to capture the configuration information for an Object Access API share. Replicate the table for each Object Access API share.
## File Persona Object Access API Shares worksheet

<table>
<thead>
<tr>
<th>Item</th>
<th>Answer/Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Share Name</strong></td>
<td></td>
</tr>
<tr>
<td>Name of the Object Access API share.</td>
<td></td>
</tr>
<tr>
<td><strong>Comment</strong></td>
<td></td>
</tr>
<tr>
<td>Optional description of the share.</td>
<td></td>
</tr>
<tr>
<td><strong>Share Path: Virtual File Server</strong></td>
<td></td>
</tr>
<tr>
<td>Identify the VFS used to present the share.</td>
<td></td>
</tr>
<tr>
<td><strong>Share Path: File Store</strong></td>
<td></td>
</tr>
<tr>
<td>Name of the File Store to use for the share.</td>
<td></td>
</tr>
<tr>
<td><strong>Share Path: Subdirectory</strong></td>
<td></td>
</tr>
<tr>
<td>Additional path within the File Store to be used for this share.</td>
<td></td>
</tr>
<tr>
<td><strong>SSL</strong></td>
<td></td>
</tr>
<tr>
<td>Answer: Enabled or Disabled</td>
<td></td>
</tr>
<tr>
<td><strong>Path</strong></td>
<td></td>
</tr>
<tr>
<td>This value is appended to http(s)://&lt;vfs_ip&gt;:&lt;port&gt;/v1/ to form the full URL path for the Object Access API share.</td>
<td></td>
</tr>
</tbody>
</table>

## File Persona Cross-protocol Share Access worksheet

File Persona supports scenarios where one protocol is configured to be the writing protocol and others are configured as read-only for Legacy security mode file stores, using Active Directory with RFC2307 or LDAP in samba schema or internal user mapping between Active Directory and LDAP providers.

The specific supported options within a given File Store are as follows:

- Share a folder over SMB protocol as read/write and with NFS as read-only
- Share a folder over NFS protocol as read/write and with SMB as read-only
- Share a folder for Object Access API as read/write and with SMB and NFS as read-only

File Persona supports scenarios where all protocols can be write protocols for near native experience for SMB Clients with NTFS security mode file store using Active Directory with RFC 2307 or internal user mapping between Active Directory and LDAP or LDAP as authentication providers.

Describe the cross-protocol share access requirements.
**File Persona Antivirus Settings worksheet**

If the antivirus service is to be used with File Persona shares, list the antivirus server below.

<table>
<thead>
<tr>
<th>Antivirus Scan Engine IP Address</th>
<th>Antivirus Scan Engine Port</th>
<th>Vendor</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**File Persona Backup worksheet**

File Persona supports network share based backup over SMB or NFS protocols and NDMP over iSCSI based backup.

<table>
<thead>
<tr>
<th>Item</th>
<th>Answer/Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NDMP Target VTL devices</td>
<td>List the IP address of each NDMP iSCSI VTL target</td>
</tr>
<tr>
<td>NDMP DMA IP address</td>
<td>List the IP address of the DMA machines</td>
</tr>
<tr>
<td>NDMP DMA Username and Password</td>
<td>Define the username and password to be verified while connecting from the DMA</td>
</tr>
</tbody>
</table>

**File Persona Replication worksheet**

HPE 3PAR Remote Copy feature can be used with the File Persona Software to replicate the File Persona File Provisioning Groups (FPG) to another HPE 3PAR StoreServ Storage running File Persona. Consideration should be given to the Remote Copy replication link definition to ensure that there is adequate bandwidth available to ensure that replication can cope with the anticipated file usage.

Describe the replication requirements for File Persona:

<table>
<thead>
<tr>
<th>Item</th>
<th>Primary system</th>
<th>Secondary system</th>
</tr>
</thead>
<tbody>
<tr>
<td>System name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>System ID</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nodes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nodes dedicated to Remote Copy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Secondary system name</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Table Continued*
<table>
<thead>
<tr>
<th>File Persona Replication worksheet</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Primary system</strong></td>
</tr>
<tr>
<td><strong>Target IP address</strong></td>
</tr>
<tr>
<td><strong>Virtual Volumes and Virtual Volume groups</strong></td>
</tr>
<tr>
<td><strong>Notes</strong></td>
</tr>
</tbody>
</table>
Support and other resources

Support and other resources

Accessing Hewlett Packard Enterprise Support

• For live assistance, go to the Contact Hewlett Packard Enterprise Worldwide website:
  http://www.hpe.com/assistance
• To access documentation and support services, go to the Hewlett Packard Enterprise Support Center website:
  http://www.hpe.com/support/hpesc

Information to collect

• Technical support registration number (if applicable)
• Product name, model or version, and serial number
• Operating system name and version
• Firmware version
• Error messages
• Product-specific reports and logs
• Add-on products or components
• Third-party products or components

Accessing updates

• Some software products provide a mechanism for accessing software updates through the product interface. Review your product documentation to identify the recommended software update method.
• To download product updates:
  Hewlett Packard Enterprise Support Center
  www.hpe.com/support/hpesc
  Hewlett Packard Enterprise Support Center: Software downloads
  www.hpe.com/support/downloads
  Software Depot
  www.hpe.com/support/softwaredepot
• To subscribe to eNewsletters and alerts:
  www.hpe.com/support/e-updates
• To view and update your entitlements, and to link your contracts and warranties with your profile, go to the Hewlett Packard Enterprise Support Center More Information on Access to Support Materials page:
  www.hpe.com/support/AccessToSupportMaterials

IMPORTANT:

Access to some updates might require product entitlement when accessed through the Hewlett Packard Enterprise Support Center. You must have an HPE Passport set up with relevant entitlements.

Customer self repair

Hewlett Packard Enterprise customer self repair (CSR) programs allow you to repair your product. If a CSR part needs to be replaced, it will be shipped directly to you so that you can install it at your convenience.
Some parts do not qualify for CSR. Your Hewlett Packard Enterprise authorized service provider will determine whether a repair can be accomplished by CSR.

For more information about CSR, contact your local service provider or go to the CSR website:

http://www.hpe.com/support/selfrepair

Remote support

Remote support is available with supported devices as part of your warranty or contractual support agreement. It provides intelligent event diagnosis, and automatic, secure submission of hardware event notifications to Hewlett Packard Enterprise, which will initiate a fast and accurate resolution based on your product's service level. Hewlett Packard Enterprise strongly recommends that you register your device for remote support.

If your product includes additional remote support details, use search to locate that information.

Remote support and Proactive Care information

HPE Get Connected
  www.hpe.com/services/getconnected
HPE Proactive Care services
  www.hpe.com/services/proactivecare
HPE Proactive Care service: Supported products list
  www.hpe.com/services/proactivecaresupportedproducts
HPE Proactive Care advanced service: Supported products list
  www.hpe.com/services/proactivecareadvancedsupportedproducts

Proactive Care customer information

Proactive Care central
  www.hpe.com/services/proactivecarecentral
Proactive Care service activation
  www.hpe.com/services/proactivecarecentralgetstarted

Warranty information

To view the warranty for your product, see the Safety and Compliance Information for Server, Storage, Power, Networking, and Rack Products document, available at the Hewlett Packard Enterprise Support Center:

www.hpe.com/support/Safety-Compliance-EnterpriseProducts

Additional warranty information

HPE ProLiant and x86 Servers and Options
  www.hpe.com/support/ProLiantServers-Warranties
HPE Enterprise Servers
  www.hpe.com/support/EnterpriseServers-Warranties
HPE Storage Products
  www.hpe.com/support/Storage-Warranties
HPE Networking Products
  www.hpe.com/support/Networking-Warranties

Regulatory information

To view the regulatory information for your product, view the Safety and Compliance Information for Server, Storage, Power, Networking, and Rack Products, available at the Hewlett Packard Enterprise Support Center:
Additional regulatory information

Hewlett Packard Enterprise is committed to providing our customers with information about the chemical substances in our products as needed to comply with legal requirements such as REACH (Regulation EC No 1907/2006 of the European Parliament and the Council). A chemical information report for this product can be found at:

www.hpe.com/info/reach

For Hewlett Packard Enterprise product environmental and safety information and compliance data, including RoHS and REACH, see:

www.hpe.com/info/ecodata

For Hewlett Packard Enterprise environmental information, including company programs, product recycling, and energy efficiency, see:

www.hpe.com/info/environment

Documentation feedback

Hewlett Packard Enterprise is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback (docsfeedback@hpe.com). When submitting your feedback, include the document title, part number, edition, and publication date located on the front cover of the document. For online help content, include the product name, product version, help edition, and publication date located on the legal notices page.
List of Port Numbers

Below is a list of port numbers and protocols that need to be open for the File Persona feature to function properly. Open the port(s) as and when needed.

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Source</th>
<th>Port Number</th>
<th>TCP/UDP</th>
<th>Usage</th>
<th>Flow of Traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td>FTP</td>
<td>Node IP</td>
<td>21</td>
<td>TCP</td>
<td>FTP</td>
<td>Incoming</td>
</tr>
<tr>
<td>DNS</td>
<td>Node IP</td>
<td>53</td>
<td>UDP/TCP</td>
<td>DNS</td>
<td>Outbound</td>
</tr>
<tr>
<td>SMB</td>
<td>Node IP</td>
<td>137</td>
<td>UDP</td>
<td>NetBIOS Name Service</td>
<td>Incoming</td>
</tr>
<tr>
<td>SMB</td>
<td>Node IP</td>
<td>138</td>
<td>UDP</td>
<td>NetBIOS datagram service</td>
<td>Incoming</td>
</tr>
<tr>
<td>SMB</td>
<td>Node IP</td>
<td>139</td>
<td>TCP</td>
<td>NetBIOS Session service</td>
<td>Incoming</td>
</tr>
<tr>
<td>SMB</td>
<td>Node IP</td>
<td>464</td>
<td>TCP/UDP</td>
<td>Kerberos V Change &amp; Set Password (SET_CHANGE )</td>
<td>Outbound</td>
</tr>
<tr>
<td>SMB</td>
<td>Node IP</td>
<td>749</td>
<td>TCP/UDP</td>
<td>Kerberos V Change &amp; Set Password (RPCSEC_GSS )</td>
<td>Outbound</td>
</tr>
<tr>
<td>LDAP</td>
<td>Node IP</td>
<td>389</td>
<td>TCP</td>
<td>LDAP</td>
<td>Outbound</td>
</tr>
<tr>
<td>SMB</td>
<td>Node IP</td>
<td>445</td>
<td>TCP</td>
<td>SMB over IP</td>
<td>Incoming</td>
</tr>
<tr>
<td>LDAP</td>
<td>Node IP</td>
<td>636</td>
<td>TCP</td>
<td>LDAP over TLS/SSL</td>
<td>Outbound</td>
</tr>
<tr>
<td>ISCSI</td>
<td>Node IP</td>
<td>3260</td>
<td>TCP</td>
<td>iSCIS for NDMP backups</td>
<td>Outbound</td>
</tr>
<tr>
<td>NDMP</td>
<td>Node IP</td>
<td>10000</td>
<td>TCP</td>
<td>NDMP</td>
<td>Incoming</td>
</tr>
<tr>
<td>Object</td>
<td>VFS IP</td>
<td>80</td>
<td>TCP</td>
<td>Non-SSL Object Port</td>
<td>Incoming</td>
</tr>
<tr>
<td>NFS</td>
<td>VFS IP</td>
<td>111</td>
<td>UDP/TCP</td>
<td>rpcbind/sunrpc</td>
<td>Incoming</td>
</tr>
<tr>
<td>Object</td>
<td>VFS IP</td>
<td>443</td>
<td>TCP</td>
<td>SSL Object Port</td>
<td>Incoming</td>
</tr>
</tbody>
</table>

*Table Continued*
<table>
<thead>
<tr>
<th>Protocol</th>
<th>Source</th>
<th>Port Number</th>
<th>TCP/UDP</th>
<th>Usage</th>
<th>Flow of Traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMB</td>
<td>VFS IP</td>
<td>445</td>
<td>TCP</td>
<td>SMB File sharing</td>
<td>Incoming</td>
</tr>
<tr>
<td>NFS</td>
<td>VFS IP</td>
<td>662</td>
<td>UDP/TCP</td>
<td>NFS statd</td>
<td>Incoming</td>
</tr>
<tr>
<td>NFS</td>
<td>VFS IP</td>
<td>875</td>
<td>UDP/TCP</td>
<td>NFS quota</td>
<td>Incoming</td>
</tr>
<tr>
<td>NFS</td>
<td>VFS IP</td>
<td>892</td>
<td>UDP/TCP</td>
<td>NFS mountd</td>
<td>Incoming</td>
</tr>
<tr>
<td>AntiVirus</td>
<td>VFS IP</td>
<td>1344</td>
<td>UDP/TCP</td>
<td>LCAP - AV</td>
<td>Outbound</td>
</tr>
<tr>
<td>NFS</td>
<td>VFS IP</td>
<td>2020</td>
<td>UDP/TCP</td>
<td>NFS stat outgoing</td>
<td>Outbound</td>
</tr>
<tr>
<td>NFS</td>
<td>VFS IP</td>
<td>2049</td>
<td>UDP/TCP</td>
<td>NFSv4</td>
<td>Incoming</td>
</tr>
<tr>
<td>NFS</td>
<td>VFS IP</td>
<td>32769</td>
<td>UDP</td>
<td>NFS Lock Manager</td>
<td>Incoming</td>
</tr>
<tr>
<td>NFS</td>
<td>VFS IP</td>
<td>32803</td>
<td>TCP</td>
<td>NFS Lock Manager</td>
<td>Incoming</td>
</tr>
<tr>
<td>Rabbit MQueue</td>
<td></td>
<td>5672</td>
<td>TCP</td>
<td>File Access Auditing</td>
<td>Incoming</td>
</tr>
</tbody>
</table>