Introduction to the Active Storage mRAID16 Storage System

Active Storage mRAID16 storage systems are innovative mid-range and high-end offerings that are ready to meet your current and future storage requirements. They are designed to provide medium and large-scale enterprises with improved storage performance, efficiency, data security, scalability, and manageability.

mRAID16 NAS Quick Configuration Guide for Windows

Before You Start

a Overview

This document helps you quickly configure the mRAID16.

b Where to get help

You can obtain this document from the documentation CD-ROM delivered with the product or from http://active-storage.com/documents/. You can also submit a request on our website for support and download valuable information.

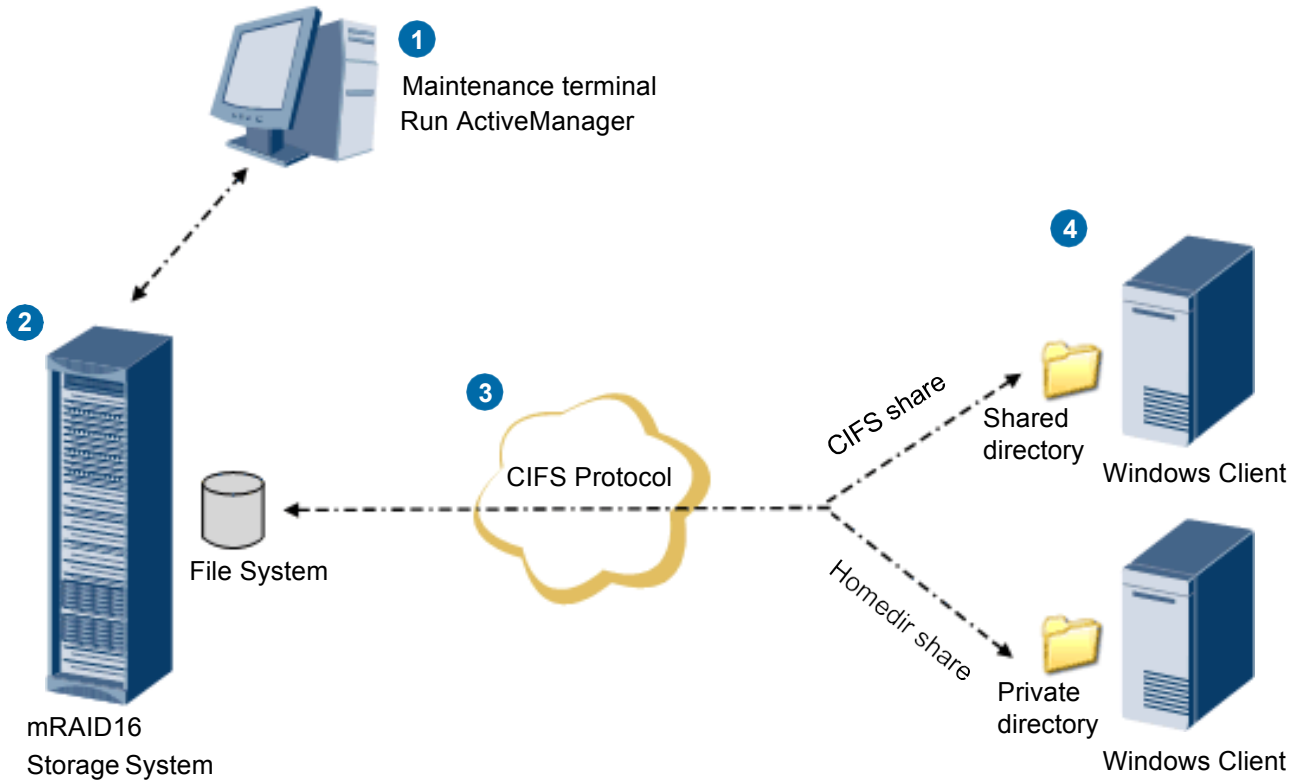
c Feedback

Your feedback is important to us. If you have any comments about this document, please submit them to us on the Active Storage website.

Copyright © Active Storage, LLC 2017. All rights reserved.

1 Introduction

1a Basic Application Scenario



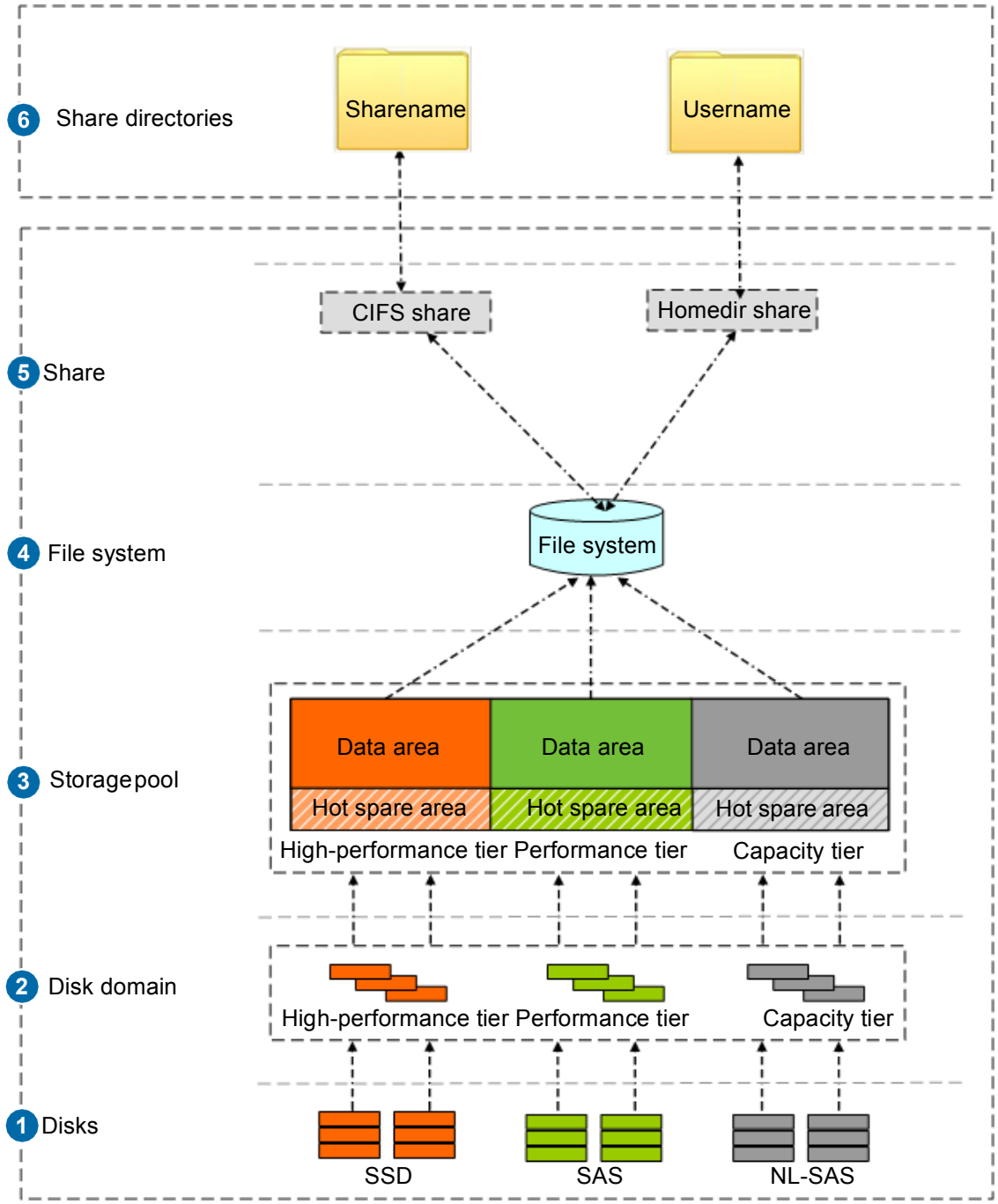
1. Users can manage and maintain the storage system from a maintenance terminal running the ActiveManager program developed by Active Storage. The maintenance terminal connects to the management network port of the storage system.

2. File system of storage system provides file-level data storage services featuring high performance and enhanced security.

3. CIFS is a file system sharing protocol developed by Microsoft and intended for Windows. Through CIFS, files can be transferred and shared between Windows clients.

4. Generally, CIFS shares provided by storage systems are public directories and can be accessed by all authorized users. If you want to set a private directory, enable Homedir so that each user can only access the directory that share the same user name with the user.

1b Storage system



1. The storage system automatically identifies all disks.
2. Disk domains are comprised of different types of disks. Services of different disk domains are isolated from each other.
3. Storage pools are created in disk domains and comprised of RAID groups formed by disks of different performance. Storage pools provide logical storage space.
4. A file system can be created in a storage pool to provide storage space for a CIFS share.
5. After creating a CIFS share, you can set different access permissions for users.
6. A shared file system appears as a directory on a Windows-based client when the client accesses the CIFS share provided by a storage system.
   A storage system shares its file system with a user in CIFS Homedir mode. The shared file system appears as a directory. The directory name is the same as the user name. The Homedir directory can be accessed only by this user.

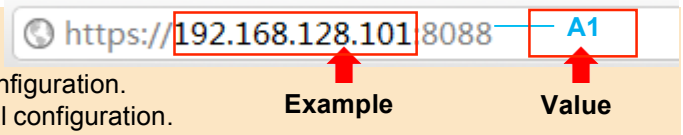
2 Data Preparation and Operation instructions

2a Data Preparation

The CIFS is a value-added feature that requires a license. For details about how to apply for and import a license, see the *mRAID16 Installation Guide*. Before operations, follow instructions in the following table to prepare data and enter actual values in the **Value** column.

CAUTION

This document uses example values to describe the configuration.
Replace example values with actual values during actual configuration.
The figure in the right shows the mappings of example values and actual values in the following table.



Preparation Item	Source	Example	Value
Maintenance terminal: Logging in to the ActiveManager			
Management network port IP addresses	Network administrator	Default value: 192.168.128.101	**A1**
User name and password for logging in to the ActiveManager **NOTE** You are advised to change the default password immediately after you have logged in to the storage system for the first time and periodically change your password in the future. This reduces the password leakage risks.	System administrator	Default user name: admin Default password: Admin@storage	**A2**
Maintenance terminal: Creating a disk domain			
Disk domain name	User-defined	DiskDomain000	**B1**
Disk encryption type	Service provider	Non-Encrypting Disk	**B2**
Number of disks forming disk domains High-performance tier uses SSDs. Performance tier uses SAS disks. Capacity tier uses NL-SAS disks.	Service provider	Performance tier (SAS): 8 Hot Spare Policy: High Capacity tier (NL-SAS): 16 Hot Spare Policy: High	**B3** Multi-choice □ High-performance tier SSDs: Hot Spare Policy: □ Performance tier SAS disks: Hot Spare Policy: □ Capacity tier NL-SAS disks: Hot Spare Policy:
Maintenance terminal: Creating a storage pool			
Storage pool name	User-defined	StoragePool000	**C1**
Usage	Service provider	File Storage Services	**C2**
Storage pool owning to Disk domain	Service provider	DiskDomain000	**C3**

Preparation Item	Source	Value	Value
Storage tier and capacity	Service provider	Performance tier RAID Policy: RAID 5(4D+1P) Capacity: 1 TB Capacity tier RAID Policy: RAID 6(4D+2P) Capacity: 1 TB Total Storage Pool Capacity: 2 TB	**C4** Multi-choice ▭ High-performance tier RAID Policy: Capacity: ▭ Performance tier RAID Policy: Capacity: ▭ Capacity tier RAID Policy: Capacity:
Maintenance Terminal: Creating a File System			
File system name	Customized	FileSystem000	D1
Thin Provisioning After thin provisioning is enabled, the storage system will dynamically allocate storage resources on demand.	Service provider	Enable	**D2**
Capacity	Service provider	200 GB	**D3**
Snapshot Space Ratio	Service provider	20	**D4**
Template	Service provider	User Defined	**D5**
File System Block Size	Service provider	64 KB	**D6**
Quantity	Service provider	1	**D7**
Owning storage pool	Service provider	StoragePool000	**D8**
Maintenance Terminal: Setting CIFS Service Parameters			
CIFS Services	Service provider	Enable	E1
Authentication Mode Local authentication: Applies to scenarios where a local authentication user or user group accesses a CIFS share in a non-domain environment Domain authentication: Applies to scenarios where a domain user or user group accesses a CIFS share in an AD domain. Global authentication: Local authentication is used first. If local authentication fails, domain authentication is used.	Service provider	Global authentication	E2
Performance Settings Notify: Notify: After this parameter is enabled, a client's operations on a directory, such as adding a sub-directory, adding a new file, modifying the directory, and modifying a file, can be sensed by other clients that are accessing this directory or the parent directory of this directory through automatic display refreshing. Oplock: a mechanism that improves client access efficiency. After this mechanism is enabled, files are cached locally before being sent to shared storage.	Service provider	Notify: Enable Oplock: Enable	E3
Security Settings Guest: After the guest service is enabled, users can access shared directories without providing usernames or password. Besides, users have the same permission as the Everyone group.	Service provider	Disable	E3

Preparation Item	Source	Example	Value
Access Settings After ABSE (Access based share enumeration) has been enabled, when user view the CIFS share information, only the CIFS shares that the user has permission to access displays.	Service provider	Disable	E4
Signature Settings Signature: This function is available when clients adopt SMB1.0. After this option is selected, the system supports the signature function. Signature enforcement: After this option is selected, client must adopt the signature function. If the signature function is disabled, the storage system may encounter man-in-the-middle (MITM) attacks, resulting in security risks.	Service provider	Signature: Enable Signature enforcement: Enable	E4
Maintenance Terminal: Creating a CIFS Share			
File system	Service provider	FileSystem000	E5
CIFS share name	Service provider	share01	E6
CA Used for SMB3.0 continuous availability, only applied to the share for Hyper-V.	Service provider	Disable	E7
Maintenance Terminal: Setting Homedir Share			
Homedir In Homedir share mode, a file system is shared to a specific user as an exclusive directory. The user can only view and access the exclusive directory named after its user name.	Service provider	Enable	F1
File system File system for which Homedir is enabled.	Service provider	FileSystem000	F2
Maintenance Terminal: Adding a Storage System to an AD Domain			
Domain Administrator Username and Password	System administrator	User name: **admin** Password: **Admin@123456**	G1
Full Domain Name	System administrator	domain.com	G2
Organization Unit	System administrator	ou=xxx,dc=abc,dc=com	**G3**
System Name	System administrator	storage1	G4
Overwrite System Name	System administrator	Disable	**G5**
Maintenance Terminal: Creating a Local Authentication User Group			
User group name	Service provider	Usergroup	H1
Maintenance Terminal: Creating a Local Authentication User			

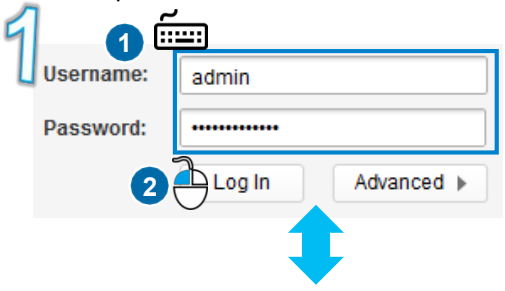
Preparation Item	Source	Example	Value
User name and password used for logging in to a CIFS share The password validity period of a file system's local authentication user is 180 days by default. Change the password in time. If a password expires, the password may not be used and services may be interrupted.	Service provider	User name: **cifsuser** Password: **Admin@123456**	H2
Primary group User group to which a user belongs. Users must belong to a primary group.	Service provider	Usergroup	H3
Maintenance Terminal: Adding a User (User Group) That Can Be Accessed by a CIFS Share			
User/User group	Service provider	a Local Authentication User	I1
User	Service provider	cifsuser	I2
Permission level	Service provider	Read-write	I3
Maintenance Terminal: Creating a Logic Port			
Name	Service provider	logicalip	J1
IP Address Type	Service provider	IPv4 Address	J2
IPv4 Address	Service provider	192.168.29.30	J3
Subnet Mask	Service provider	255.255.255.0	J4
Primary Port	Service provider	CTE0.L1. IOM1.P2	J5
IP Address Floating When the primary port is disabled, the IP address will be floated to another port that can be used.	Service provider	Enable	J6
Failback Mode Failback mode of the IP address: **Automatic and Manual.**	Service provider	Automatic	J7
Active Now	Service provider	Enable	J8

2b Operation instructions

Before operations, learn about the meaning of icons involved in the configuration, as shown in the following table.

Icon	Meaning
	Double-click
	Click
	Right-click
	Input or Set
1 2	Step
1 2	Substep

Example



Substep1: Enter the user name and password.
Substep2: Click **Log In**.

NOTE
The screenshots in this manual may differ

3 Allocating Storage Space

3a Logging in to the DeviceManager

1

2

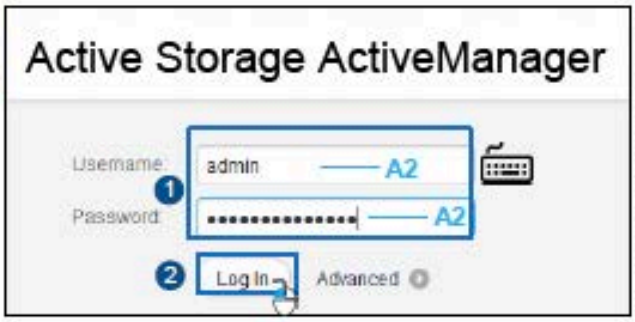
1. Enter **https://***XXX.XXX.XXX.XXX***:8088**, where *XXX.XXX.XXX.XXX* indicates the IP address of the management network port. *192.168.128.101* is used as an example.
2. Click **Enter**.

3

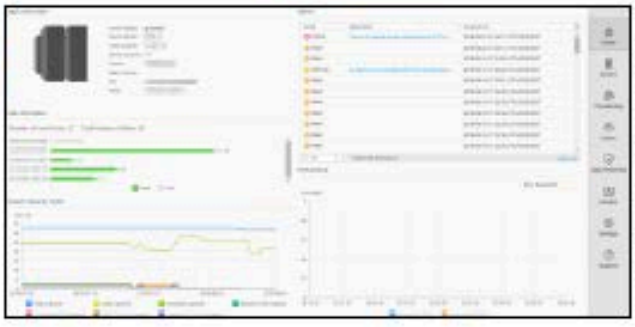
NOTE

The security certificate prompt message varies with operating systems and browser versions of maintenance terminals. Ignore the message and continue accessing storage devices.

4



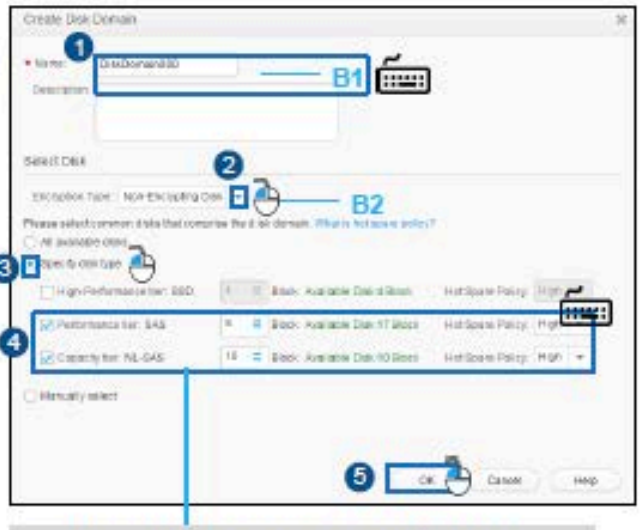
5



3b Creating a disk domain

1

2

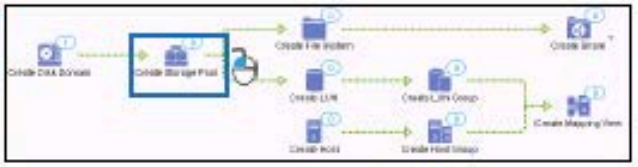


For the actual disk numbers, see **B3** in your data preparation table. The figure above takes performance tier and capacity tier creations as an example.

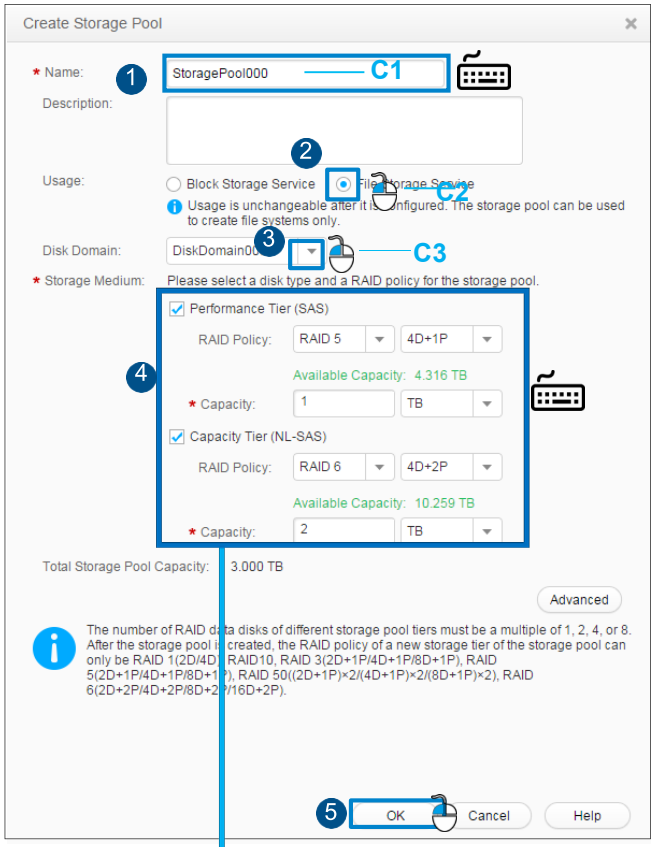
3

3c Creating a storage pool

1



2

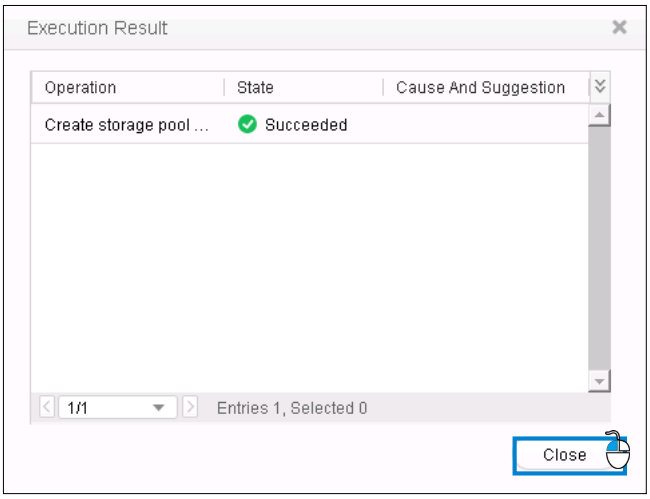


To create storage tiers, see the actual value from **C4** in your data preparation table. The figure above takes performance tier and capacity tier creations as an example.

NOTE

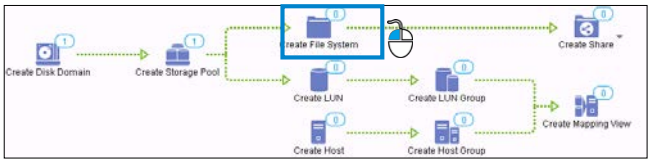
Keep the default values for **RAID Policy.**

3

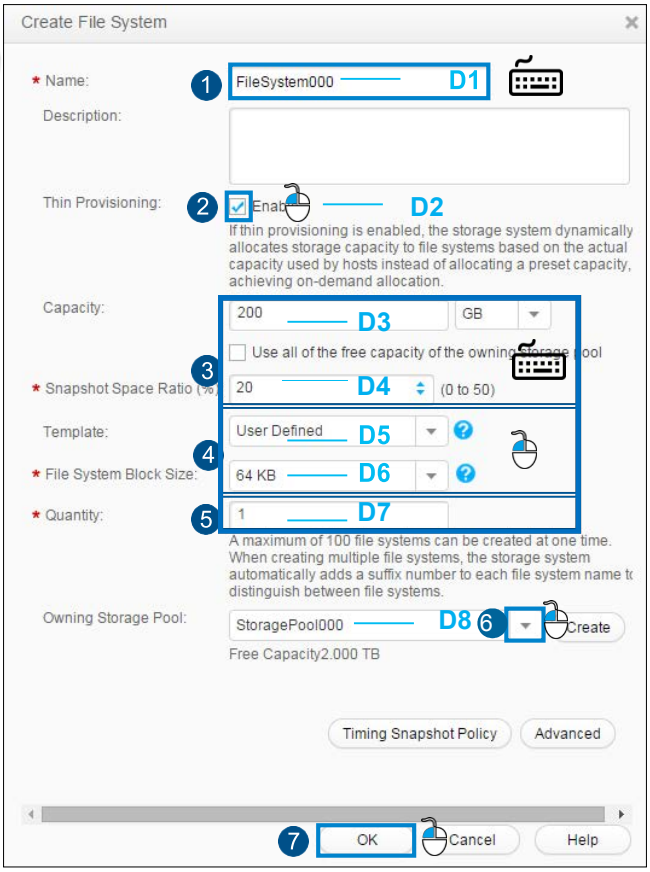


3d Creating a file system

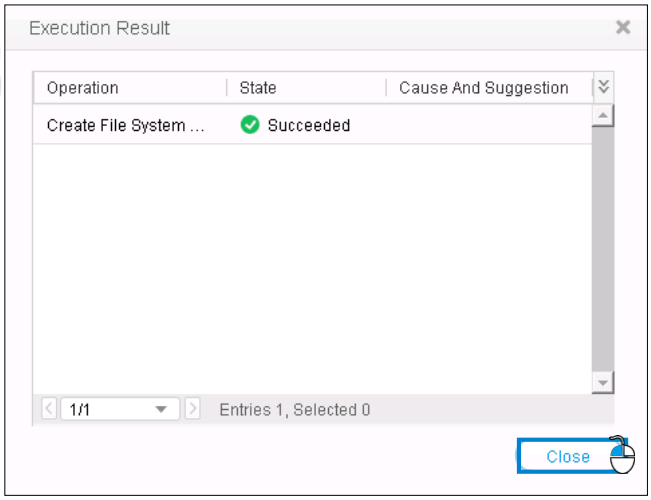
1



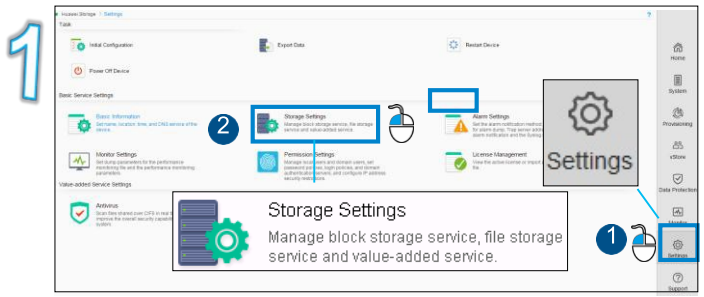
2

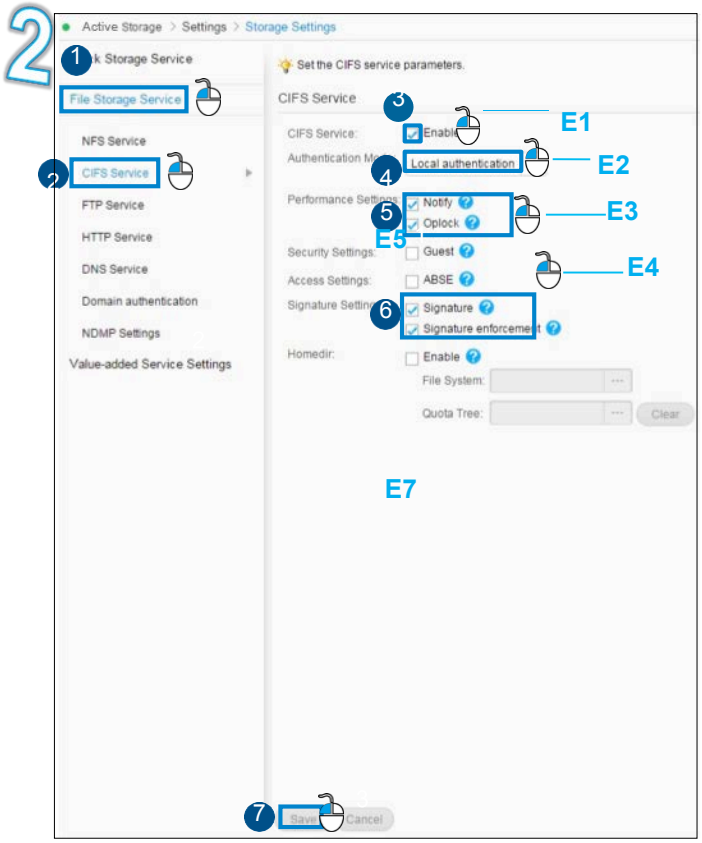


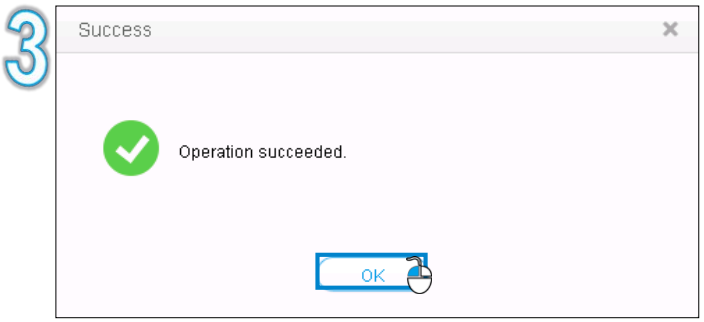
3



3e Setting CIFS Service Parameters



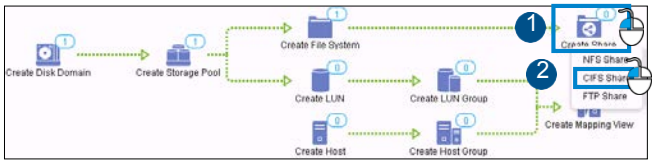


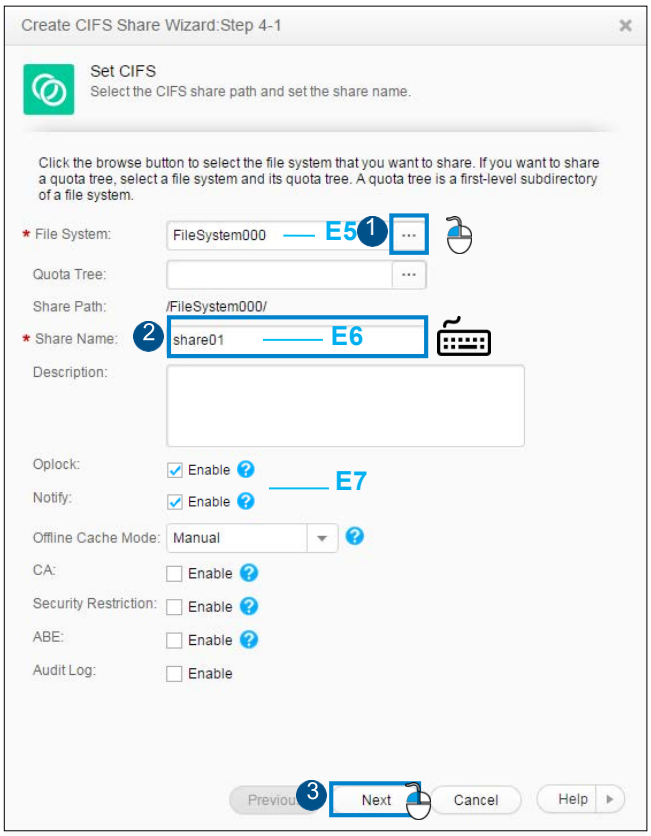


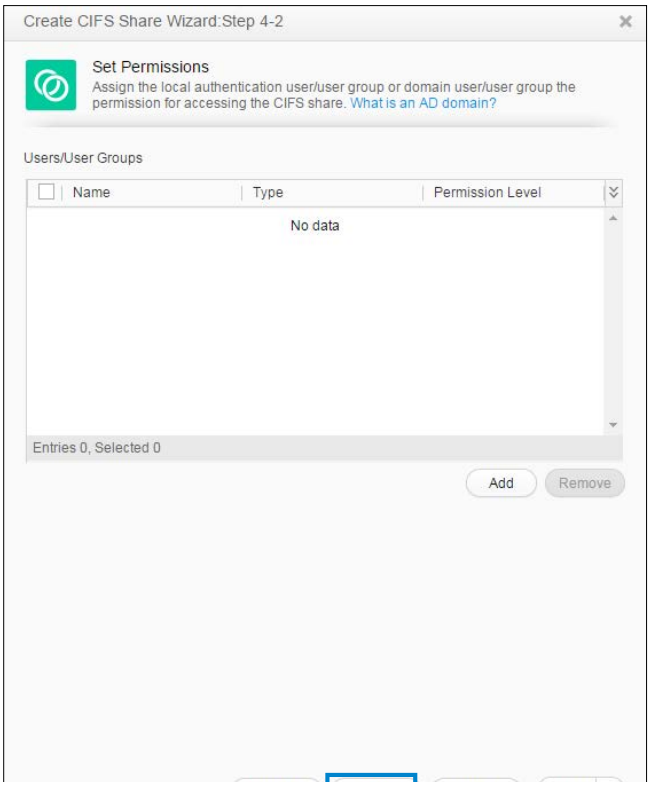
If creating an CIFS Share → 3f Creating an CIFS Share

If creating a Homedir Share → 3g Creating a Homedir Share

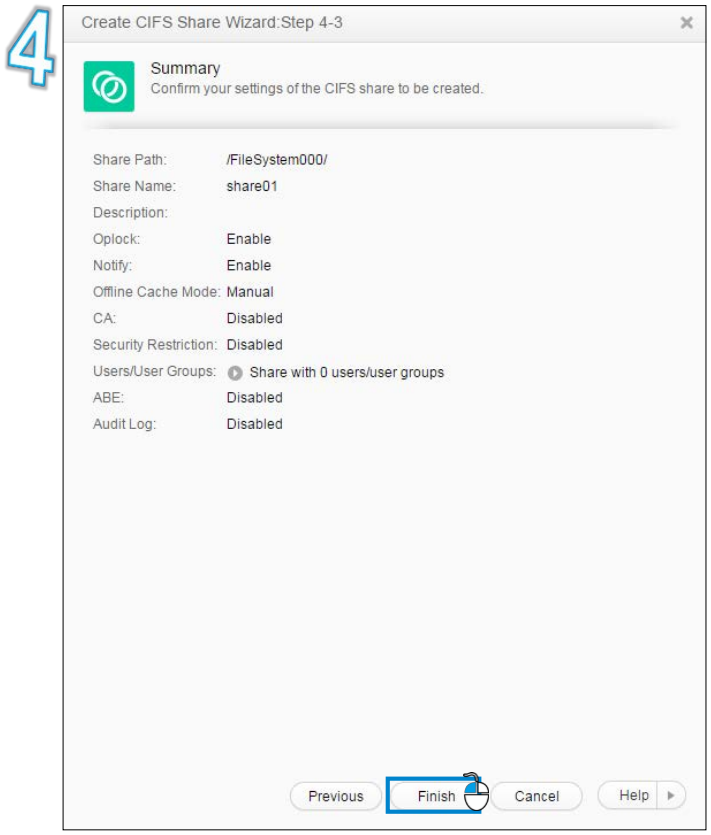
3f Creating a CIFS Share

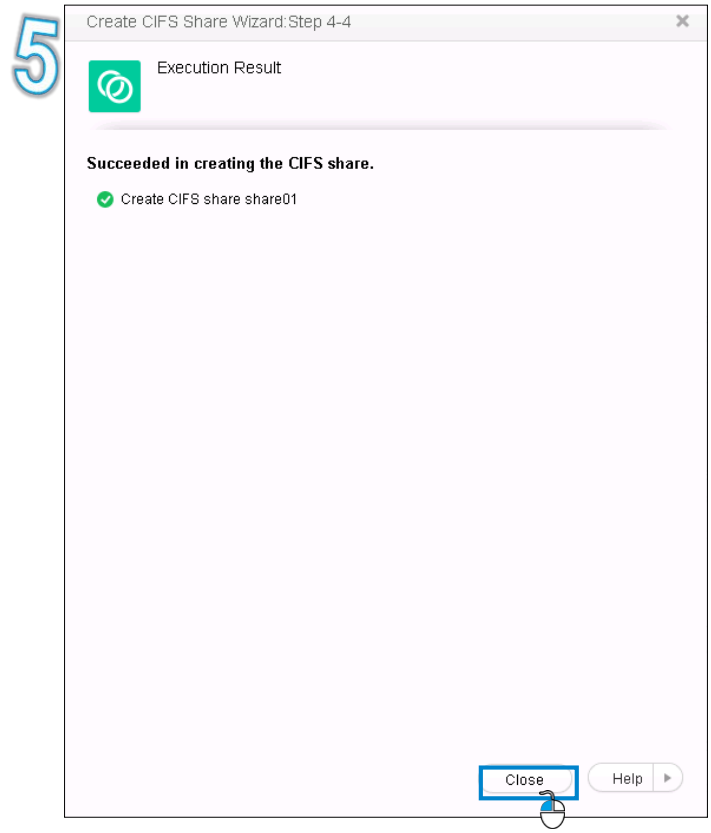


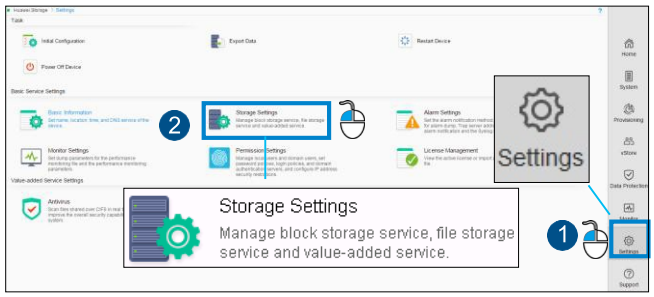


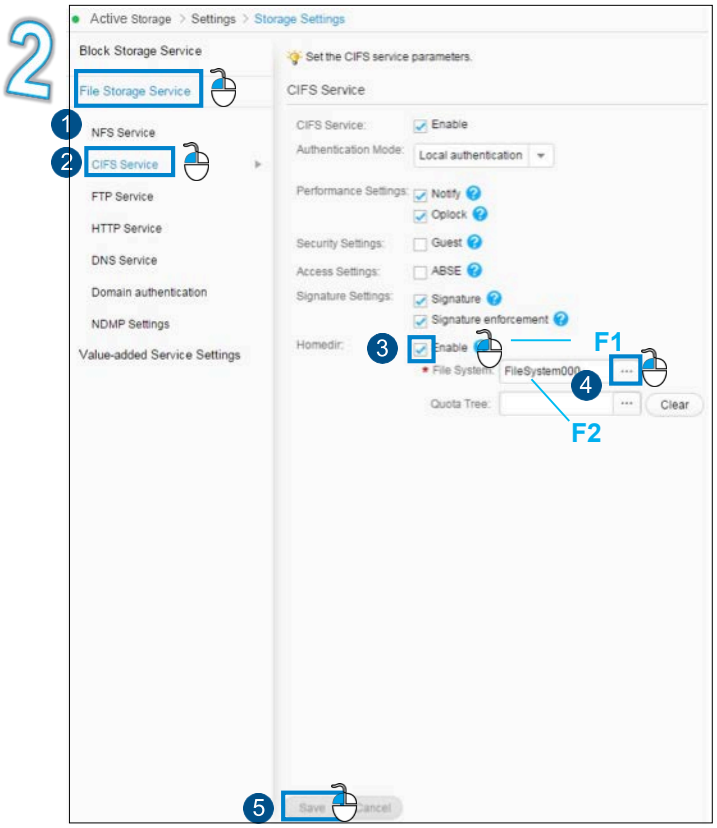


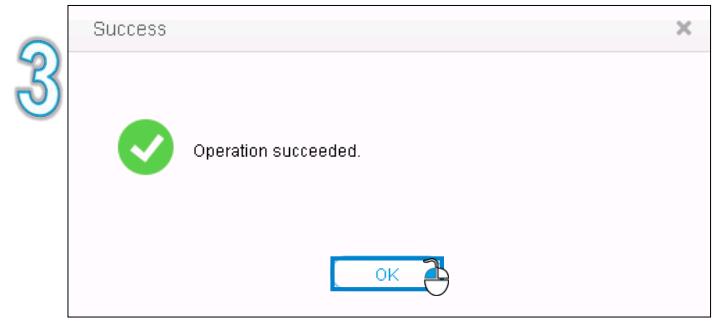
3g Creating a Homedir Share





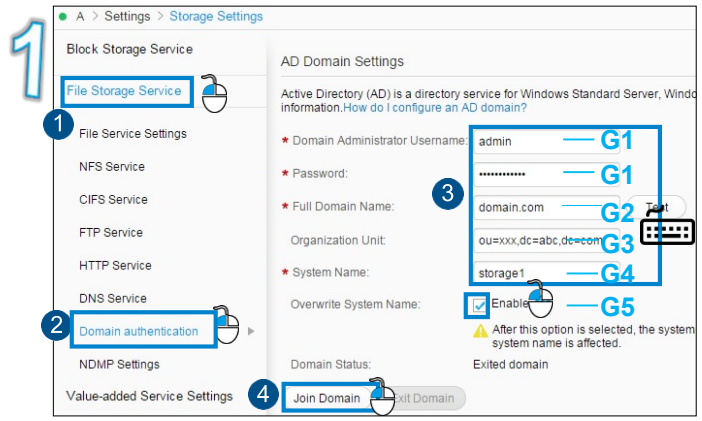


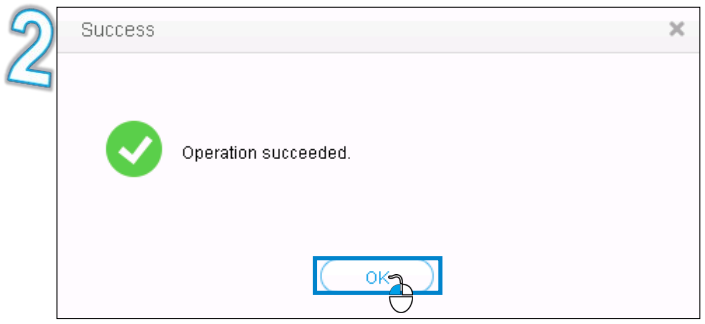




If the CIFS is applied to a domain environment
→ 4 Adding a Storage System to an AD Domain
If the CIFS is applied to a non-domain environment
→ 5 Creating a Local Authentication User (Group)

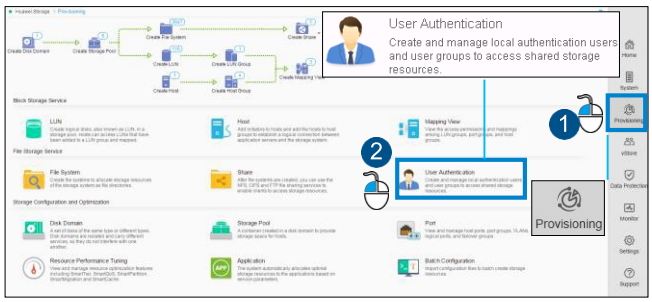
4 Adding a Storage System to an AD Domain

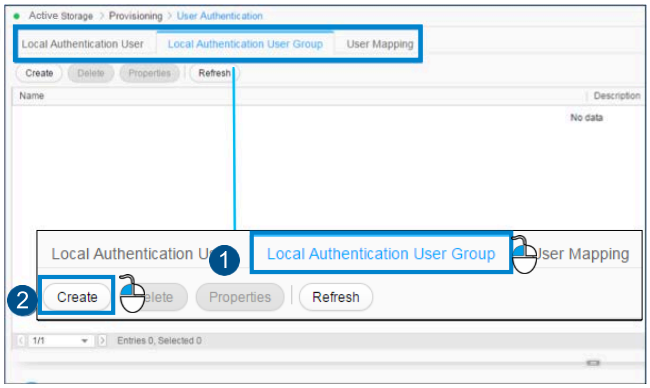


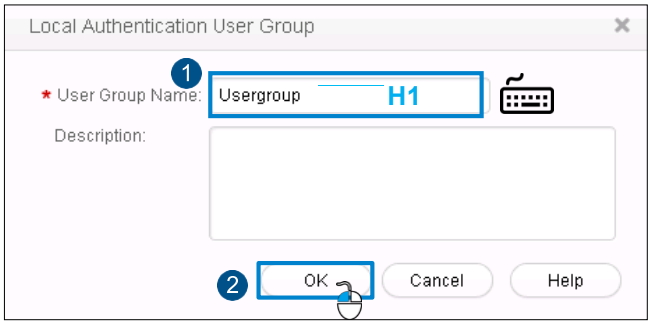


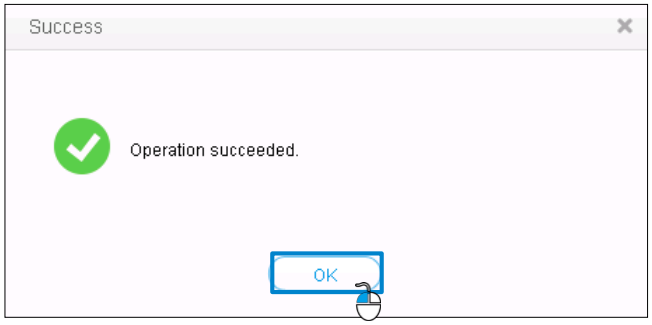
5 Creating a Local Authentication User (Group)

5a Creating a Local Authentication User Group

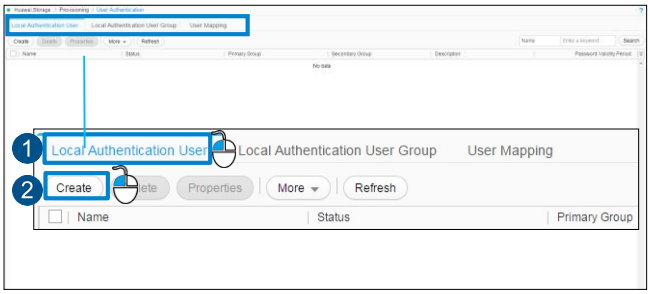


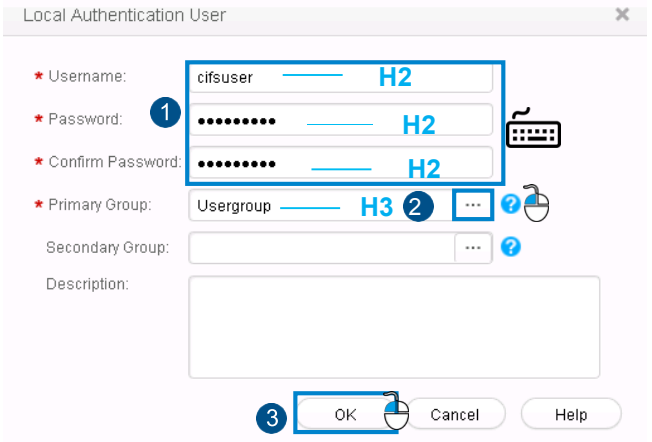






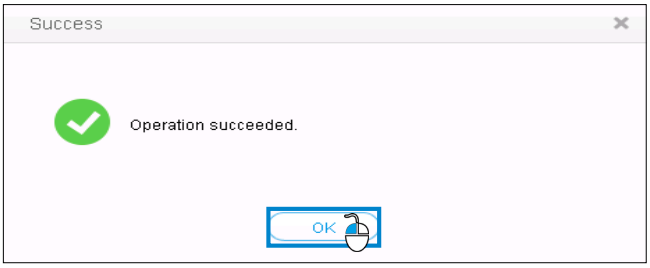
5b Creating a Local Authentication User



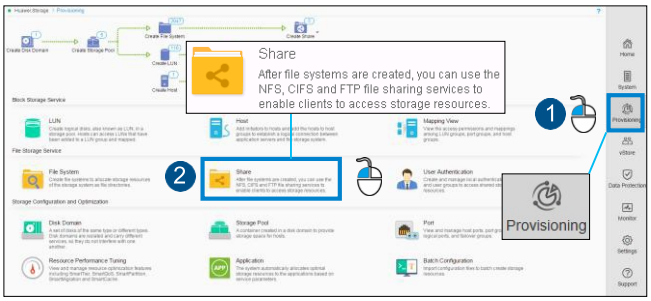


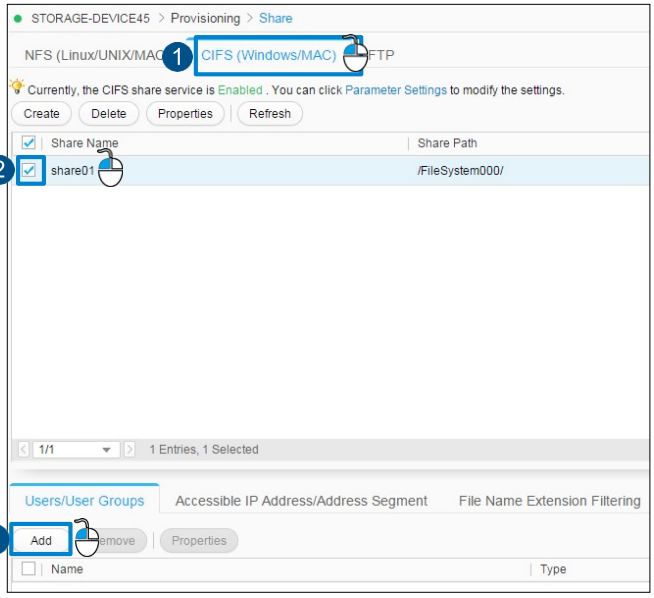
NOTE

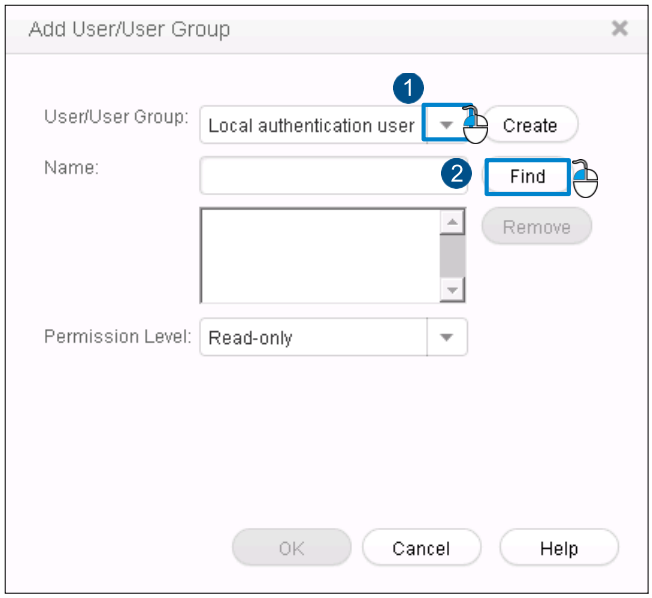
The password validity period of a file system's local authentication user is 180 days by default. Change the password in time. If a password expires, the password may not be used and services may be interrupted.

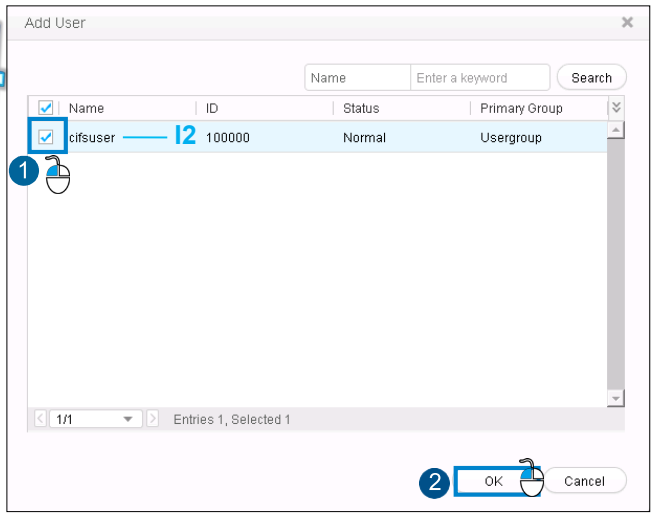


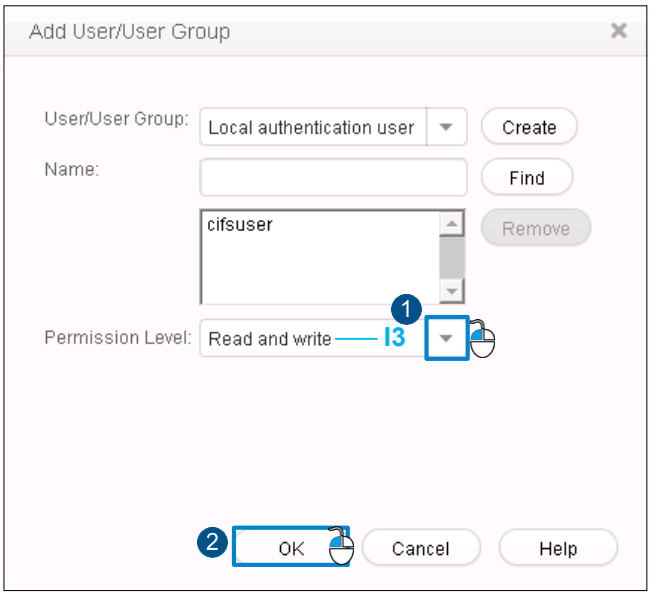
6 Adding a User (User Group) That Can Be Accessed by a CIFS Share





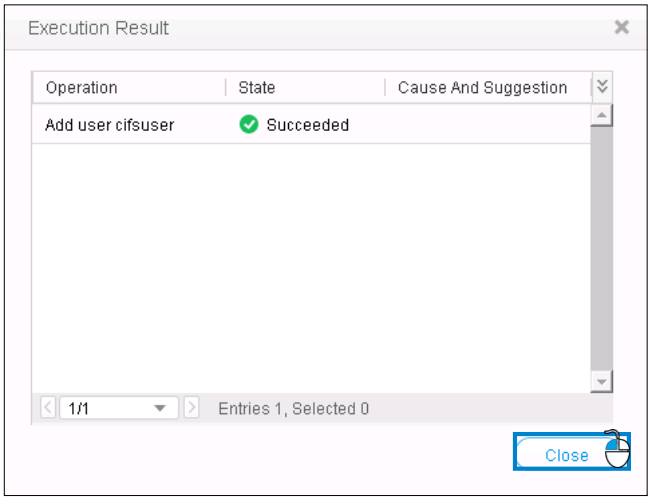






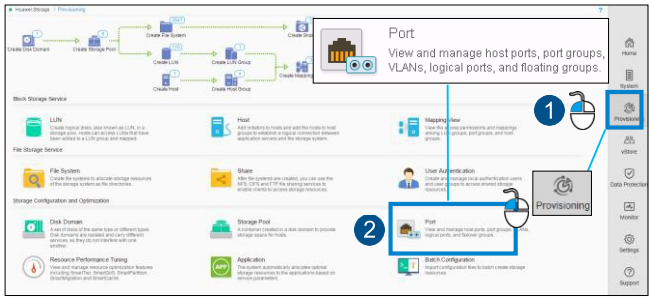
NOTE

In a domain, select a *domain user* or *domain user group* in User/User Group.

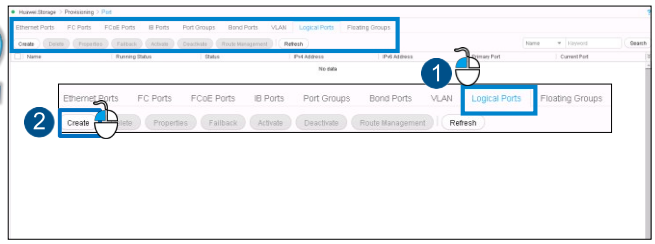


7 Creating a Logical port

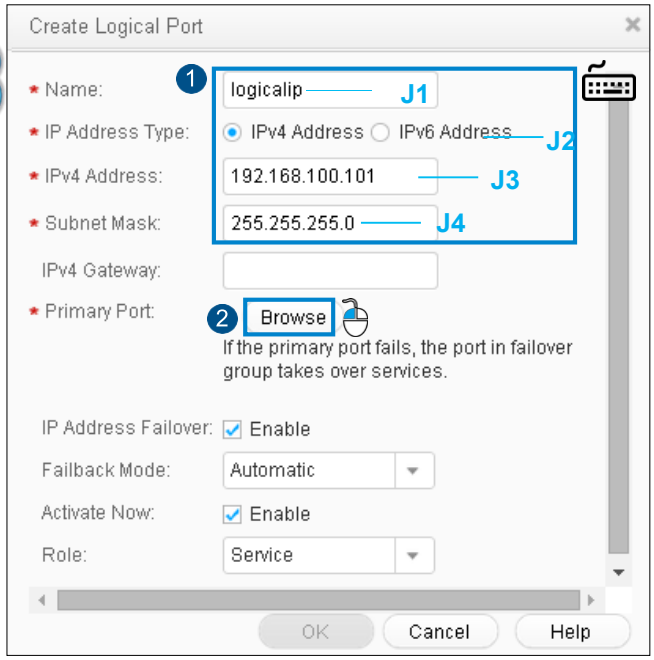
1



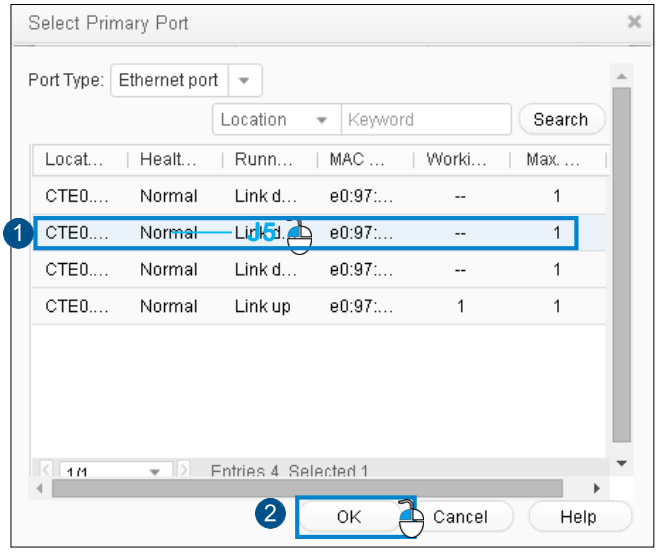
2



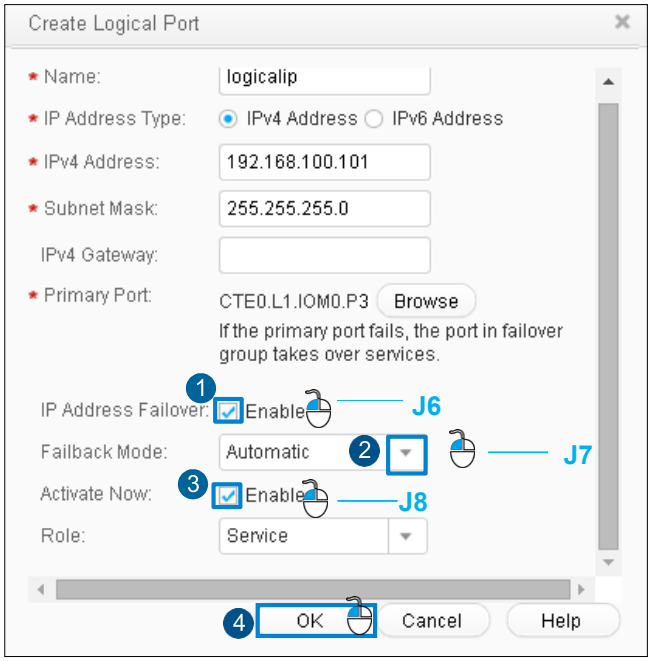
3



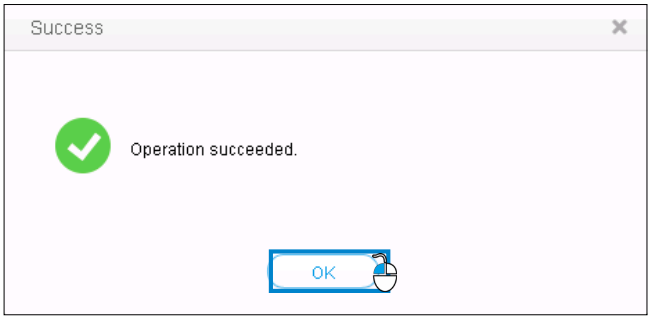
4



5



6



8 Access the Share

8a Optional: Access a CIFS Share.

Operation Instruction	Windows Server 2008
Go to the **Map Network Drive** dialog box.	1. Right-click **Computer**. 2. Choose **Map Network Drive**.
Mount the CIFS Normal share path.	Change parameter values based on the actual values of **J3** and **E2** in your data preparation table. 1. Set **Folder** to ***\\192.168.29.30\share01***. 2. Click **Finish**.
Authenticate the CIFS Normal share.	1. Enter the name and password of the authorized user. If it is a non-domain environment, enter the name and password of the local authentication user. If it is a AD domain environment, enter the name and password of the AD domain user, and the domain user name must be entered in the format of **domain name\user name**. 2. Click **OK**.
Check the CIFS Share	1. Double-click **Computer**. 2. In the **Network Drive** area, view the mapped network drives.

8b Optional: Access a Homedir Share.

Operation Instruction	Windows Server 2008
Go to the **Map Network Drive** dialog box.	1. Right-click **Computer**. 2. Choose **Map Network Drive**.
Mount the Homedir share path.	Change parameter values based on the actual values of **J3** and **H2** in your data preparation table. 1. Set **Folder** to ***\\192.168.29.30\username***. *username* is the user of the Homedir share. If it is a non-domain environment, the *username* is the name of the local authentication user. If it is a AD domain environment, the *username* must be entered in the format of **~domain name~user name**.
Authenticate the Homedir share.	1. Enter the user name and password. If it is a non-domain environment, enter the name and password of the local authentication user. If it is a AD domain environment, enter the name and password of the AD domain user, and the domain user name must be entered in the format of **domain name\user name**. 2. Click **OK**.
Check the Homedir Share.	1.Double-click **Computer**. 2. In the **Network Drive** area, view the mapped network drives.

9 How to Contact Active Storage

●**Active Storage customer service center**
Address: 9233 Eton Ave. Chatsworth, CA 91311 USA
Tel: +1 (818) 709-1133
Email: info@activestorage.com
Website: http://activestorage.com

●**Active Storage technical support personnel**
Obtain contact information from Active Storage offices at http://support.active-storage.com/hc/en-us.