

Synology Administrator's  
Guide for

**UC3200**



# Table of Contents

Introduction	01
Quick Start	03
Manage Users	
Modify Network Settings	
Deploy Storage Space	
Manage iSCSI Services	
Back Up and Recover Data	
Monitor Overall System Status	
Optimal UC3200 Deployment	16
UC3200 Deployment	
Initiator Deployment	
UC3200 Deployment after the RMA	21
If a controller is replaced through the RMA	
If the entire UC3200 is replaced through the RMA	
Conclusion	23



# Introduction

Synology is committed to developing a storage solution to meet the growing business needs for deploying virtualization applications and environments. Designed with the concept of service continuity and zero downtime at its core, Synology Unified Controller **UC3200** comes with active-active controllers to ensure that one controller can immediately take over all services if the other controller breaks down.

UC3200 supports a SAS interface, which requires the installation of SAS drives, to provide non-disruptive iSCSI storage services. This device also guarantees flexible storage space deployment and disaster recovery solutions, allowing users to build the most reliable virtualization platform. Please see the following for the key features of UC3200:

## Key Features of UC3200

- Designed with active-active controllers to ensure one controller takes over the other in the event of controller failure.
- Built-in SATA-DOM to provide highly reliable and optimal performance for the operating system DSM UC.
- Expandable up to two expansion units (i.e., RXD1219sas) to flexibly add 24 drives for storage capacity allocation.
- Supports the Btrfs file system to schedule and take up to 4,096 snapshots for LUN protection.
- Protects LUNs by replicating LUN snapshots to another Synology Unified Controller or Synology NAS (DSM 6.2.2 or versions above).
- Supports Self-Encrypting Drive (SED) to enhance data security.
- Offers an intuitive and web-based interface for easy system deployment.
- Supports automatic network failover and iSCSI Multipath I/O (MPIO).
- Ensures non-disruptive iSCSI services by transferring from one controller to the other within 30 seconds.<sup>1</sup>
- Protects data in memory cache to guarantee data integrity.
- Enhances system stability through the pre-installed operating system in SATA DOM (Disk on Module) for isolating the operating system and services.

---

<sup>1</sup> The 30-second transfer time is obtained from Synology's performance test. However, the actual required time may differ in different environments.

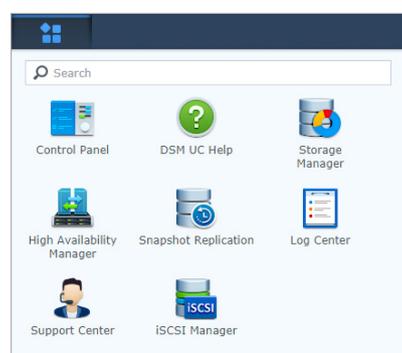
## Get Started with UC3200

Once the hardware setup is complete, please follow the steps below to sign in to DSM UC:

1. Power on your UC3200.<sup>2</sup>
2. Open a web browser on a computer in the same network as your UC3200.<sup>3</sup>
3. Enter [find.synology.com](https://find.synology.com) into the address bar of your web browser.
4. **Web Assistant** will be launched in your web browser. It will search for and find the Synology Unified Controller within the local network. The status of your UC3200 should be **Ready**.
5. Select a controller and click **Connect** to start the setup process and follow the onscreen instructions.<sup>4</sup>
6. Create your administrator account and click **Next**.
7. Select an option for DSM UC update and maintenance. Click **Next**.
8. Create a new Synology Account or use an existing account. Click **Next**.
9. Set the static IP address for the LAN port currently in use to enable network failover automatically.
10. Tick the checkbox and click **Go** to sign in to DSM UC.

For more information on setting up UC3200, please refer to the **Hardware Installation Guide** available at Synology's [Download Center](#). After signing in to DSM UC, click the upper-left **Main Menu** icon to see the built-in applications and start configuring your UC3200.

In this administrator's guide, the second chapter offers an overview of the key features, advantages, and common scenarios of UC3200; the third chapter demonstrates the methods for optimal UC3200 deployment; the fourth chapter guides you through UC3200 deployment after you receive a new controller or an entire UC3200 through the return merchandise authorization (RMA) service; and the fifth chapter concludes this guide and offers links to relevant resources.



<sup>2</sup> If both Controller A and Controller B are powered off, pressing the power on button will simultaneously power on both controllers; however, if Controller A is already powered on, pressing the button will only power on Controller B.

<sup>3</sup> Synology Unified Controller must be connected to the Internet to install DSM UC with Web Assistant. Chrome and Firefox are the suggested browsers.

<sup>4</sup> All the connected network interfaces will be displayed here. For example, if LAN1 on both controllers are connected, then two IP addresses will be listed. You may choose either IP address to sign in.

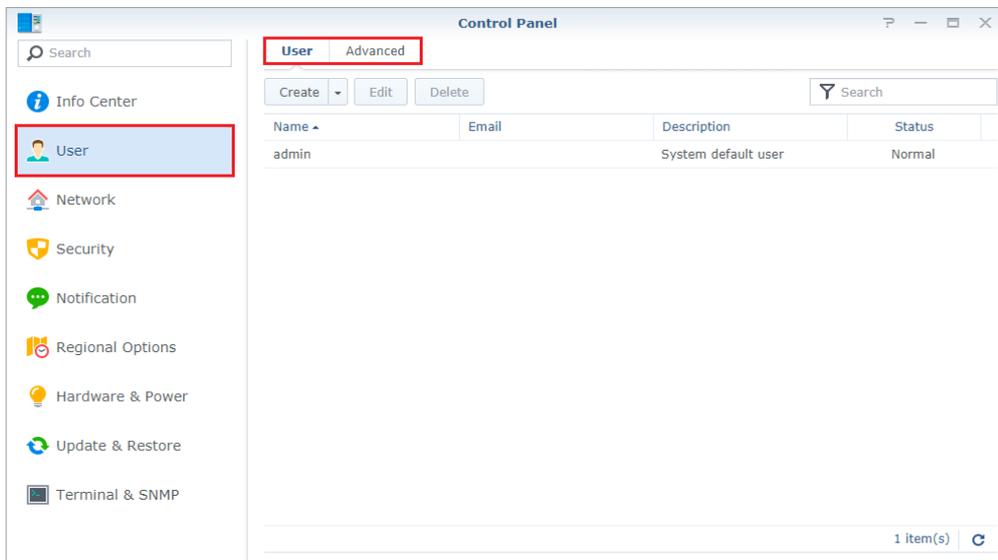
# Quick Start

This chapter provides an overview of UC3200's major features and relevant settings. For step-by-step instructions on feature management and settings, please refer to the [Help articles](#).

## Manage Users

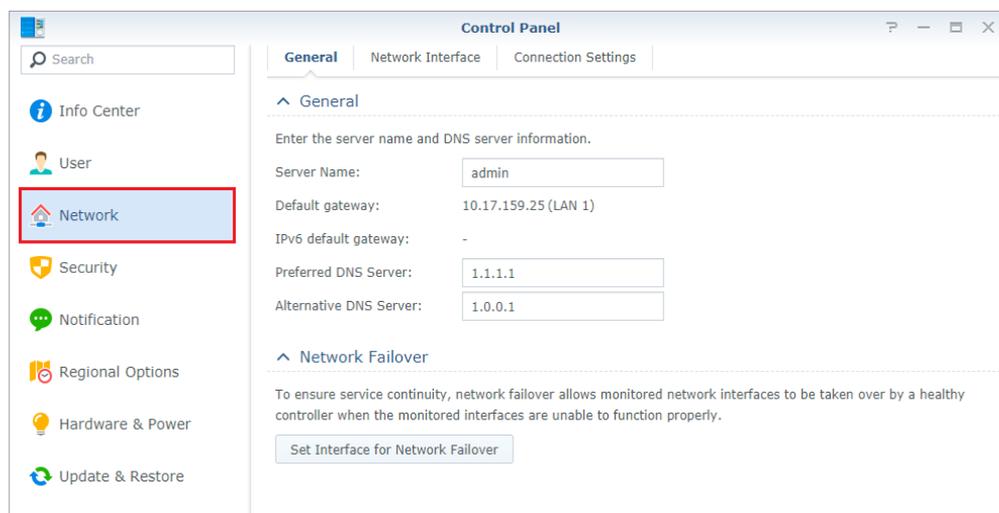
In **Control Panel > User**, the flexible user management options allow you to create and manage administrator user accounts. Please note that only administrator users can be created on UC3200.

- Go to the **User** tab to create, edit, remove, or import administrator users.
- Go to the **Advanced** tab to configure password setting rules and the password expiration schedule, thereby adding an extra layer of protection to user accounts.



## Modify Network Settings

In **Control Panel > Network**, you can configure network settings to connect your UC3200 to the network, aggregate network interfaces, enable the failover feature, and more. Here we'll guide you through some of the key configurations for ensuring data security and network stability.



### Set Static IP Addresses

IP addresses are assigned automatically (DHCP) by default during the initial setup. An IP address may possibly change under certain circumstances such as system reboots; therefore, we highly recommend configuring static IP addresses before proceeding with other configurations.

In fact, IP addresses must be set static first if you want to enable the network failover feature (see the [Enable Network Failover](#) section for details). To set a static IP address, please complete the following steps:

1. Go to **Control Panel > Network > Network Interface** and select a LAN that you want to set a static IP address. Click **Edit**.
2. Select **IPv4** or **IPv6** and select **Use manual configuration**.
3. Enter the IP address and other information, and click **OK** to finish.

### Manage Link Aggregation

Link Aggregation increases the redundancy or bandwidth of your UC3200 by aggregating multiple network interfaces, and provides traffic redundancy to maintain network connection in case connection is down. To combine multiple LANs, please complete the following steps:

1. Go to **Control Panel > Network > Network Interface**.
2. Click **Create > Create Bond**.
3. Select a controller and click **Next**. Follow the on-screen instructions to finish.

## Quick Start

After the LAN interfaces are combined, a new interface named **Bond** will appear in the **Network Interface** tab.

## Enable Network Failover

Network failover is designed to ensure service continuity. Enabling this feature on a LAN port ensures that if a controller breaks down, its tasks and IP addresses will be automatically taken over by and switched to the other controller. Since this feature can only be enabled on LAN ports with static IP addresses, please make sure your IP addresses are set static first.

Once network failover has been enabled and a LAN port has been specified, the port will be protected in the event of network failure or controller malfunctioning. For example, if network failover is enabled on LAN 1 and if Controller A unfortunately breaks down due to hardware issues, network issues, or other unexpected events, then all the incoming connections directed to LAN 1 of Controller A will be re-directed to LAN 1 of Controller B. This ensures service continuity and almost zero downtime.

If you want to perform specific tasks on a certain controller, we do not recommend enabling network failover on a LAN port because an IP address may be assigned to different controllers when this feature is enabled, thus possibly preventing a controller from being identified through its IP address. For example, this feature should not be enabled on a LAN port under the following circumstances:

- If you want to always connect to a controller via a LAN port.
- If you want to retrieve system information via the SNMP protocol.

Before enabling network failover, please make sure the LAN port is connected, the static IP address is set, and the subnet is under the same network environment. Afterward, please complete the following steps:

1. Go to **Control Panel > Network > General**.
2. Go to the **Network Failover** section and click **Set Interface for Network Failover**.
3. Select the preferred network interfaces (only the interface in **Normal** status can be selected) and click **OK**.

## Deploy Storage Space

Before the various UC3200 features can be fully managed, you must create at least one storage pool and one volume in **Storage Manager**. This application is designed for deploying storage spaces, simplifying storage management, and creating flexible storage spaces with data protection, thereby helping you accomplish the following tasks and more:

- Create storage pools and volumes
- Monitor and assign the installed drives
- Improve SSD performance
- View the health status and connection status

## Create Storage Pools and Volumes

Storage pools are storage capacity aggregated by multiple drives, and can be configured in varying sizes to enhance storage performance, management, and data protection. Volumes provide the basic storage space on your UC3200. All data are stored on volumes, and volumes are created on storage pools. Therefore, a storage pool must be created before a volume can be created. UC3200 supports the Btrfs file system.

To create a storage pool and volume, please go to the **Storage Pool** and **Volume** pages respectively and click **Create**.<sup>5</sup> A controller must be selected for storage pool creation, and a RAID type must be selected for data protection.<sup>6</sup> After a storage pool has been created, you can go to **Storage Pool > Action > Change Controller** to change and mount the storage pool on another controller, thereby balancing the CPU usage of the two controllers.

## Monitor and Assign the Installed Drives

In the **HDD/SSD** page, you can monitor drive performance and health status, enable write cache support to enhance system performance, optimize read/write performance of volumes, and more.<sup>7</sup>

In the **Hot Spare** page, you can assign the standby drives as hot spare drives, which will automatically replace the defective drives in a degraded storage pool on UC3200 or its connected expansion units (i.e., RXD1219sas). To replace the defective drives, the hot spare drives must be installed in the same chassis as where the defective drives are located. Standby drives can be assigned as hot spare drives once the following criteria are met:

- The RAID type of the storage pool supports data protection.<sup>8</sup>
- The size of the hot spare drive must be equal to or larger than the size of the smallest drive in the storage pool.

## Improve SSD Performance

In an all-flash volume, we recommend enabling **SSD TRIM**, which improves the read and write performance of the volumes created on SSDs. To enable SSD TRIM, please go to the **Volume** page and select a volume that consists entirely of SSDs, and then click **Action > Configure** and follow the wizard to complete.

In the **SSD Cache** tab, you can mount an SSD cache to a volume to improve the performance of **Random Access**. Please note that an SSD cache and its corresponding volume must be created on drives in the same chassis. UC3200 supports two SSD cache types, namely, read-only cache and read-write cache.<sup>9</sup>

---

<sup>5</sup> Before you create a storage pool, make sure there is no important data on the drives on which the storage pool will be created. All existing data will be deleted during the creation process.

<sup>6</sup> Please refer to [here](#) for the supported RAID types.

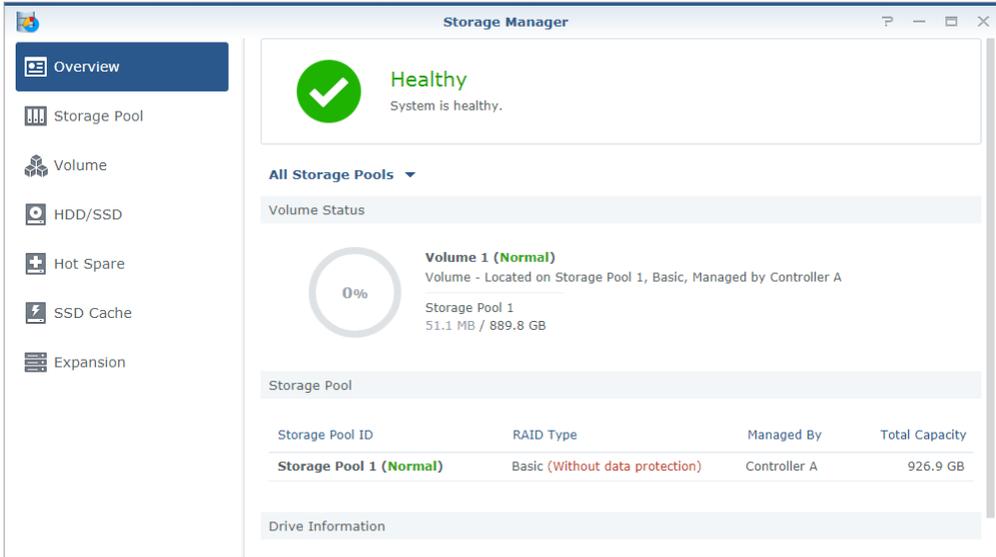
<sup>7</sup> The drives installed in UC3200 cannot be migrated to Synology NAS.

<sup>8</sup> SHR, RAID 1, RAID 5, RAID 6, RAID 10, and RAID F1 are the RAID types that support data protection.

<sup>9</sup> Please make sure your data are properly backed up because there is a high risk of data loss if the volume on which an SSD read-write cache is mounted crashes.

## View Health Status and Connection Status

After the configurations are done, you can go to the **Overview** page to view the health status of volumes, storage pools, and drives, and take corresponding actions whenever an issue occurs. You can also go to the **Expansion** page to see the connection status between your UC3200 and the connected expansion units.<sup>10</sup>



<sup>10</sup> The graphic shown in this page merely depicts the physical condition of the UC3200 and the connected expansion units. It, however, does not reflect the scenario when one controller breaks down and the other controller takes over the task.

## Manage iSCSI Services

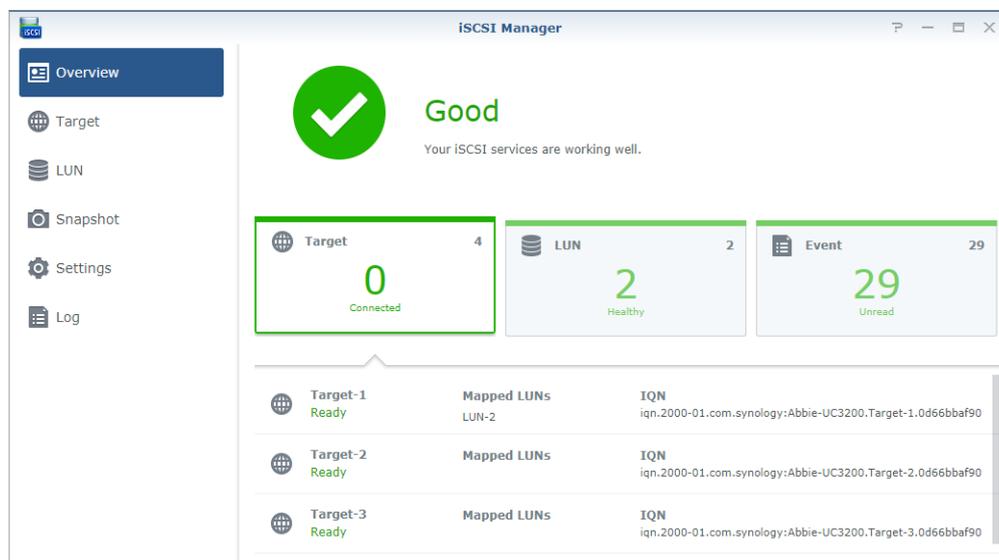
**iSCSI Manager** is designed for managing and monitoring iSCSI services, and creating iSCSI LUNs with thick and thin provisioning.<sup>11</sup> It supports mapping iSCSI LUNs to iSCSI targets, thereby allowing client servers to access storage spaces via their iSCSI initiators as if the spaces were local drives.

### Create iSCSI LUNs

An iSCSI LUN represents an individually addressable portion of an iSCSI Target, and can be mapped to multiple iSCSI Targets for storage operations. An iSCSI LUN is created with thick provisioning by default, ensuring the system to provide consistent performance. The creation time depends on the LUN size. For example, creating a 1TB LUN on a storage pool that is aggregated by HDDs and is in RAID 5 configuration may take more than 30 minutes. For users demanding less latency and higher performance consistency, we recommend selecting thick provisioning for LUN creation.

After a volume has been created in Storage Manager, please complete the following steps to create an iSCSI LUN:

1. Go to **iSCSI Manager > LUN** and click **Create**.
2. Enter the iSCSI LUN properties and click **Next**.
3. Follow the wizard to complete.



<sup>11</sup> Both thick provisioning and thin provisioning are types of storage pre-allocation. With thick provisioning, the total storage capacity of a virtual drive is pre-allocated on the physical storage when the virtual drive is created. The drive consumes all the space allocated to it in the data store right from the start; therefore, the space is unavailable for use by other virtual machines. Contrarily, a thin-provisioned virtual drive consumes only the space that it needs initially, and may consume more space depending on future needs.

## Configure iSCSI Targets

An iSCSI target is a storage resource located on an iSCSI LUN, and UC3200 supports creating multiple targets for mapping LUNs.

### Register iSCSI targets with an iSNS server

An iSNS (Internet Storage Name Service) server provides a mechanism for centralized management. You can register all the iSCSI targets with an iSNS server if you have this server. To enable an iSNS server, please complete the following steps:

1. In the **Settings** page, go to the **iSNS (Internet Storage Name Service)** section and tick **Enable iSNS**.
2. Enter the IP address or domain name of the iSNS server, and click **Apply**.

### Set I/O queue depth for iSCSI targets

I/O queue depth determines the maximum number of iSCSI commands that can be sent to the queue during each iSCSI session. A longer queue depth may help enhance throughput in 10/40 GbE network and SSD environments; a shorter queue depth may help address latency or stability issues. I/O queue depth of all targets can be modified by completing the steps below:

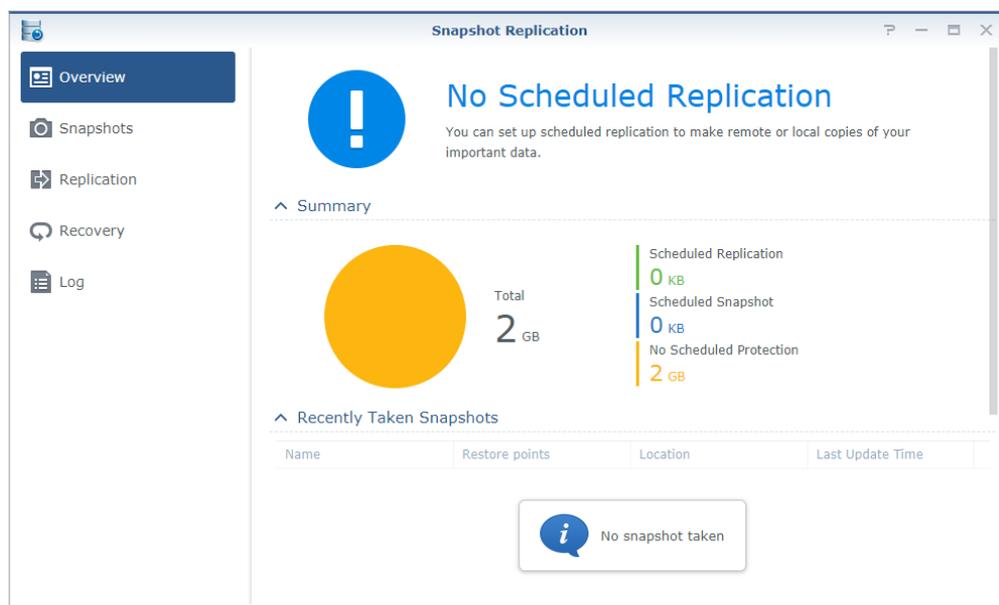
1. In the **Settings** page, go to the **I/O Queue Depth** section.
2. Click the **I/O** drop-down menu and select the preferred value, and click **Apply**. For the recommended value, please refer to the [Set I/O Queue Depth](#) section.

## Protect iSCSI LUNs with Snapshots

A snapshot of an iSCSI LUN is a point-in-time and read-only copy of an iSCSI LUN, aimed for increasing the level of data protection. The snapshot feature is also available in **Snapshot Replication**. Please refer to the [Take snapshots for an iSCSI LUN](#) section for more information.

## Back Up and Recover Data

**Snapshot Replication** is a data backup and recovery solution providing schedulable and near-instantaneous data protection. It ensures that corporate data and virtual machines in iSCSI LUNs remain safe and available in the event of accidental deletion, application crash, data corruption, or other unexpected events.



This application helps you accomplish the following tasks:

- Take and manage snapshots of iSCSI LUNs
- Configure scheduled snapshots and retention settings
- Create and manage replication tasks for iSCSI LUNs
- Configure scheduled replication to periodically sync replication tasks
- Restore data from snapshots, and perform failover/switchover of replication tasks between the source and destination
- View the event logs related to snapshots and replications

UC3200 also supports creating snapshot schedules and replicating data to another UC3200 or Synology NAS running on DSM 6.2.2 or versions above.

### Take snapshots for an iSCSI LUN

The "snapshot" feature is a point-in-time copy of the data being taken. Only thin-provisioning LUNs support taking snapshots, and up to 4,096 snapshots can be taken for LUN protection. Snapshots take up only a small amount of additional storage space, and do not affect system performance. In short, data that are accidentally modified or deleted from a volume can be instantly restored back to the previous time at which the snapshot was taken. To create a snapshot, please complete the following steps:

## Quick Start

1. Go to the **Snapshots** page and select the iSCSI LUN that you want to take a snapshot.
2. Click **Snapshots > Take a Snapshot**.
3. Enter the description and tick or untick the **Lock** checkbox to determine whether to ignore the retention settings when automatic removal is triggered.
4. Click **OK** to start taking a snapshot.

## Create replication tasks for an iSCSI LUN

The "Replication" feature is a mechanism that syncs the iSCSI LUNs snapshots between the source and destination. The replicated snapshots can even be used for performing failover and protecting data if the replication source unfortunately fails. This feature allows you to manage replication tasks, run or stop the syncing, and view information of the replication tasks. To create a replication task, please complete the following steps:

1. In the **Replication** page, click **Create** and select the location and network type for the destination.
2. Click **Next** and follow the wizard to finish.

## Recover iSCSI LUNs

The "Recovery" feature allows recovering data from local snapshots, and restoring the entire iSCSI LUN to the previous point-in-time.<sup>12</sup>

### Restore an iSCSI LUN

If data were deleted accidentally or if you need to restore your data to the previous version, please do the following to restore the data:

1. Select the iSCSI LUN you want to restore and click **Recover**.
2. Select the snapshot version you want to restore from, click **Action**, and select **Restore in-place** from the drop-down list.
3. A confirmation message will appear. Click **Yes** to confirm the action.

### Re-protect a replication task

When a replication task is failed over from the source server (i.e., UC3200) to the destination server (i.e., another UC3200 or Synology NAS), the destination server will act as the new source server and the task will stop syncing data between the two servers. Therefore, you will need to re-protect the task to determine which server should act as the source server once the original source server is recovered. Please complete the following steps to re-protect a task:

1. Select the failed over iSCSI LUN you want to re-protect, and click **Action > Re-protect**.
2. Select the new source, and select the new destination if there are multiple replication tasks of the iSCSI LUN.

---

<sup>12</sup> To ensure that iSCSI LUNs can be fully protected, we highly recommend installing the same version of Snapshot Replication on both the source server and destination server.

3. Select to re-protect the data on either the source or destination.
4. Tick the **Sync immediately after operation** checkbox if you want to sync immediately.
5. Click **Re-protect** to start the action.

### Clone a snapshot to a new iSCSI LUN

If you want to clone a snapshot to a new iSCSI LUN, please complete the following steps:

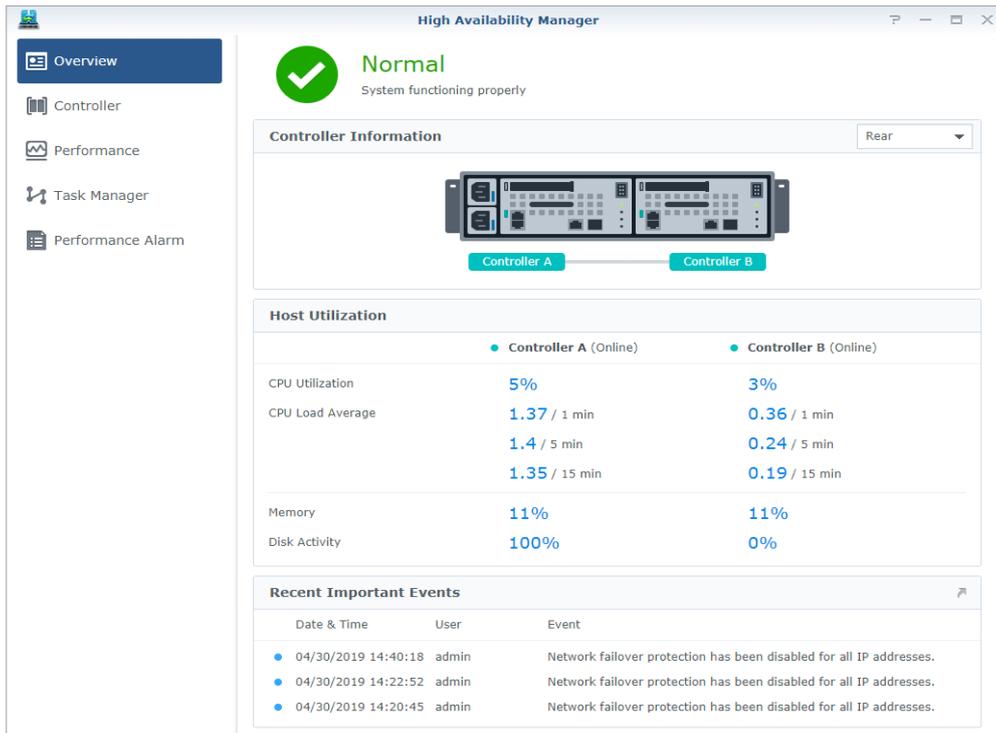
1. Select the iSCSI LUN you want to clone and click **Recover**.
2. Select the snapshot version you want to clone to a new iSCSI LUN, click **Action**, and select **Clone with a new name** from the drop-down list.
3. You will be redirected to the **Clone** page in **iSCSI Manager**. Enter the name of the cloned iSCSI LUN and click **OK** to finish.

To ensure successful recovery of services, applications, and iSCSI LUNs, you can perform **Test Failover** to clone a writable iSCSI LUN on the destination (as the simulated new source) to check whether the cloning works well. Performing failover regularly allows IT administrators to facilitate punctual responses to actual situations when unexpected events occur.

## Monitor Overall System Status

**High Availability Manager** provides a comprehensive overview of the system information, offering a quick glance at the system and health status of both controllers. It reflects real-time system status and alerts you when system errors occur. The following pages are offered on the left panel:

- **Overview:** This page displays the system and controller statuses, shows the system errors, and offers the recommended actions.
- **Controller:** This page lists the detailed hardware information of both controllers.
- **Performance:** This page offers close monitoring of system resource usage (e.g., CPU, memory, and volume).
- **Task Manager:** This page lists the ongoing processes and tasks to instantly identify system resource distribution.
- **Performance Alarm:** This page offers a customizable warning level for critical services.



The **Overview** page lists the overall system statuses (see Table 1) and displays the warning or critical messages that may appear when an error occurs (see Table 2). A message that appears will be followed by cluster details and recommended actions.

System Status	Description
Normal	The overall condition of UC3200 is healthy. Both internal communication and exterior services are functioning properly.
Processing	UC3200 is busy due to certain system processes. Therefore, we highly recommend that all operations be performed after the system process is complete.
Warning	UC3200 has encountered minor issues. The status of the cluster is abnormal, but the services are still functioning. Performing corresponding actions before the issues deteriorate is highly recommended.
Critical	At least one controller has encountered major issues and its services have malfunctioned. Under this condition, the controller in normal operation will take over all services. Following the given instructions to recover the cluster immediately is highly recommended.

Table 1: Overall system status

Warning / Critical Message	Description
Service switchover	A controller is unable to provide services, and the other controller is taking over all services, volumes, and failover-enabled network interfaces, thereby ensuring service continuity. We highly recommend following the on-screen troubleshooting instructions to prevent further errors.
Network interface failover	Some monitored network interfaces on a controller are disconnected, and the other controller will take over those IP addresses until the interfaces are reconnected. Under this condition, all services going through the failover IP addresses will not be interrupted. We highly recommend following the on-screen troubleshooting instructions to prevent further errors.
Unable to switchover	Switchover is not available due to some internal errors. This issue is usually caused by inconsistent system or hardware settings. It is also possible that the entire system is processing critical operations. We recommend following the instructions in the <b>Overview</b> page to repair the system.
Inconsistent firmware version	Firmware versions of the two controllers are inconsistent. The system may encounter unexpected errors if the controllers continue to operate in different versions. We recommend following the instructions in the <b>Overview</b> page to repair the system. Please note that the service will be unavailable during the repair process.
Error on monitored items	The monitored items (e.g., network, service, or storage space) have failed. We recommend following the instructions in the <b>Overview</b> page to repair the system.
Heartbeat malfunction	Heartbeat problems have been detected. Heartbeat is responsible for the communication between the two controllers. When this issue occurs, please contact <a href="#">Synology Technical Support</a> immediately for further assistance.
Controller undetectable	One controller cannot be detected by the other controller. Under this condition, the system is not protected by High Availability Manager.
Inconsistent configuration	User setting of the two controllers is inconsistent. Please go to the <b>Overview</b> page and reboot the suggested controller to resolve this issue.

Table 2: Warning or critical messages

The **Overview** page also displays the following types of information:

### Controller Information

This section graphically displays the basic information of the controllers, allowing you to easily identify which part of UC3200 is malfunctioning and take corresponding actions. The graphic displays the following information:

- **Controller:** A controller will be highlighted if an error occurs to the controller.
- **Storage Space:** Drives in abnormal status will be highlighted if an error exists in the corresponding space. Only the drives installed in UC3200 will be visually displayed if errors occurred; that is, the drives installed in an expansion unit will not be displayed here if errors occurred.
- **Network:** A network interface will be highlighted if the corresponding monitored interface is disconnected. When this happens, the graphic of UC3200 will turn to its rear to highlight the corresponding area.
- **Power:** A power supply will be highlighted if the corresponding power supply is abnormal. When this happens, the graphic of UC3200 will turn to its rear to highlight the corresponding area.
- **Heartbeat Communication:** The communication condition between the controllers is shown here.

### Host Utilization

This section allows you to monitor the important resource usage of the two controllers. Please refer to the following for more information:

- **CPU Utilization and CPU Load Average:** We highly recommend keeping the CPU utilization below 80%, so as to ensure the system can reserve sufficient resource for cluster monitoring. When managing the CPU resource, we highly recommend reserving CPU resource in advance in case one controller needs to take over all services from the other controller during controller failure.
- **Memory:** This indicates how much memory has been occupied. We highly recommend always reserving 20% of the memory for system-related monitoring.
- **Disk Activity:** This indicates whether the drives are running data read/write activities.

### Recent Important Events

The most recent five logs will be listed in this section, allowing you to understand the recent cluster activity information (date, time, user, and event detail) at a glance. You can also instantly trace the most recent activities in the cluster when issues occur to the system. For complete log records, please refer to **Log Center**.

# Optimal UC3200 Deployment

This chapter demonstrates the configurations for optimal UC3200 deployment regarding storage space, network configuration, and iSCSI LUN and targets. Actual configurations can be adjusted according to your environment. The recommended hardware requirements are shown below:

## Recommended client server:

- Installed with a 10 GbE network card
- Installed with either of the following operating systems:
  - Windows Server 2016 or versions above, along with the installation of Windows MPIO
  - VMware 6.0 or versions above
  - Red Hat Enterprise Linux 7 or versions above, along with the installation of Linux Multipath

## Highly-recommended drive deployment for UC3200:

- Install all SSDs to create at least two volumes and accelerate the system performance

## UC3200 Deployment

### Create Storage Pools and Volumes

When creating a storage pool, please select a controller for managing the storage pool. The active-active controller design of UC3200 ensures that both controllers process resources simultaneously. To balance resource usage and ensure optimal performance of the two controllers, we recommend assigning different controllers for storage pool management if you want to create at least two storage pools; that is, at least one storage pool should be created on both Controller A and Controller B. Afterward, create at least one volume on each storage pool.

Please follow the steps below:

1. Go to **Storage Manager > Storage Pool > Create**.
2. Select **Better performance** to ensure that the storage pool provides better performance. Click **Next**.
3. From the drives that are installed in UC3200, select **RAID F1** or **RAID 5** configuration according to your needs.
  - **For deployment with all SSDs:** Create two RAID F1 storage pools with SSDs and assign

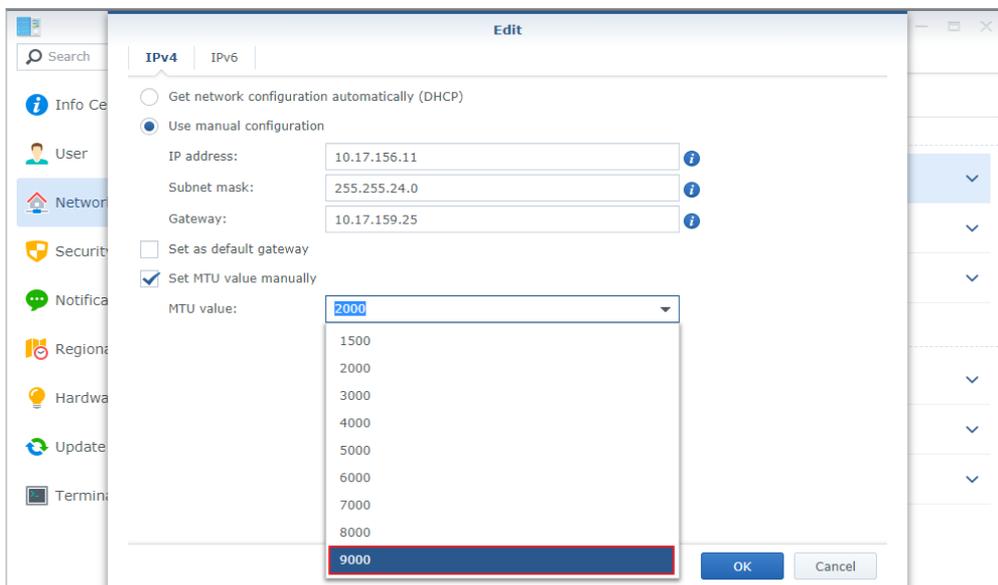
a storage pool to each controller.

- **For deployment with HDDs and SSDs:** Create two RAID 5 storage pools with HDDs; and create and assign an SSD read-write cache to each storage pool.

## Configure Network

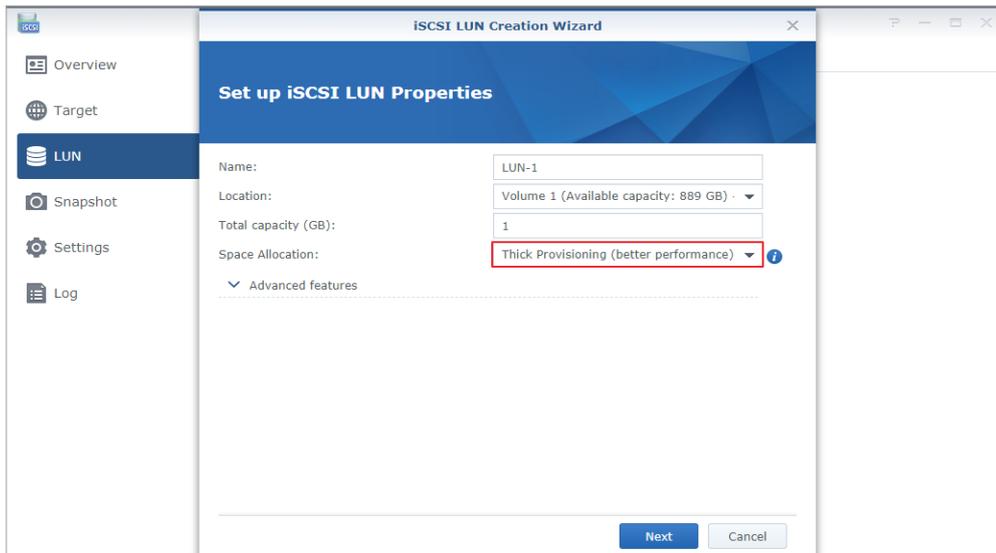
Please refer to the following to configure your network settings:

- **Network failover (IP failover):** When a controller malfunctions, UC3200 will switch its IP address to the corresponding network interface on another controller. Please see the [Enable Network Failover](#) section for more information.
- **MTU value:** We recommend setting the MTU value of a 10 GbE network card to 9000 to enhance the transfer speed. Please also set the MTU value of the connected devices and initiator to 9000 to ensure that they can operate properly. To set the MTU value, please complete the following steps:
  1. Go to **Control Panel > Network > Network Interface**.
  2. Select a LAN of a controller and click **Edit**.
  3. Go to the **IPv4** or **IPv6** tab and tick **Set MTU value manually**. Select **9000** from the drop-down menu in the MTU value field.
  4. Click **OK** to finish.



## Deploy iSCSI LUN

When creating an iSCSI LUN, we recommend selecting thick provisioning because it offers more stabilized performance and less latency. To do so, go to **iSCSI Manager > LUN > Create** and select **Thick Provisioning (better performance)**. Follow the wizard to complete or refer to the [Manage iSCSI Services](#) section for more information.



### Deployment for best performance (multiple LUN creation)

To fully exercise the mechanism of the active-active controller design, we highly recommend creating at least one LUN on each controller, thereby balancing system resources and ensuring optimal system resource usage. For example, creating a LUN on both Controller A and Controller B indicate that system resources are balanced between the two controllers. This deployment guarantees better system performance because each controller only processes 50% of the system resources. If Controller A unfortunately fails, 50% of the resources under its process will be failed over to Controller B, which will immediately take over the task and process 100% of the resources.

Another benefit of this deployment is that the two controllers can balance the sudden system resource burst that may occur from time to time. In short, creating at least one LUN on each controller balances system resources and ensures that both controllers can work actively and simultaneously, thereby optimizing the performance.

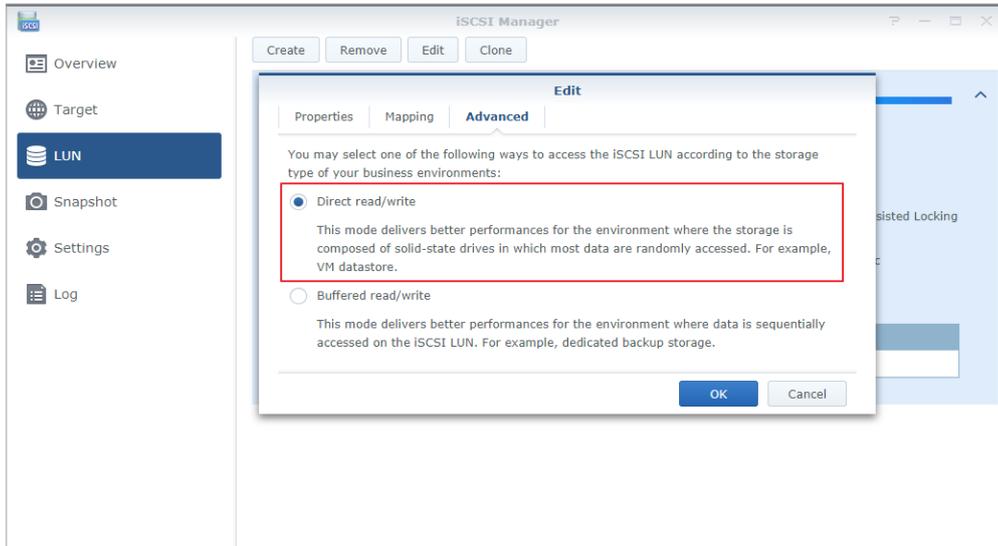
### Deployment for easy management (single volume creation)

The aforementioned and recommended deployment method may, however, not always be the best practice for all environments. To be specific, creating at least one volume on each controller means that storage space must be pre-allocated and reserved for each controller. Some users may only want to create one volume on a controller for high-availability purpose or easy management, and may therefore prefer to create one or multiple LUNs on a volume, store all data all on that volume, and expand the volume capacity only when needed. Under this deployment, only one controller will be activated at a time, while the other controller remains idle. Consequently, if Controller A unfortunately fails, 100% of the system resources will be failed over to Controller B.

Even though creating a volume on only one controller or on both controllers does not affect the failover mechanism, the performance is, however, affected. To be specific, creating a volume only on Controller A cannot fully exert the mechanism of the active-active controller design because Controller A will process 100% of the system resources, without Controller B balancing the workload. Since the resources are processed only by Controller A, the performance will be lowered when compared with the deployment where the resources are balanced between the two controllers.

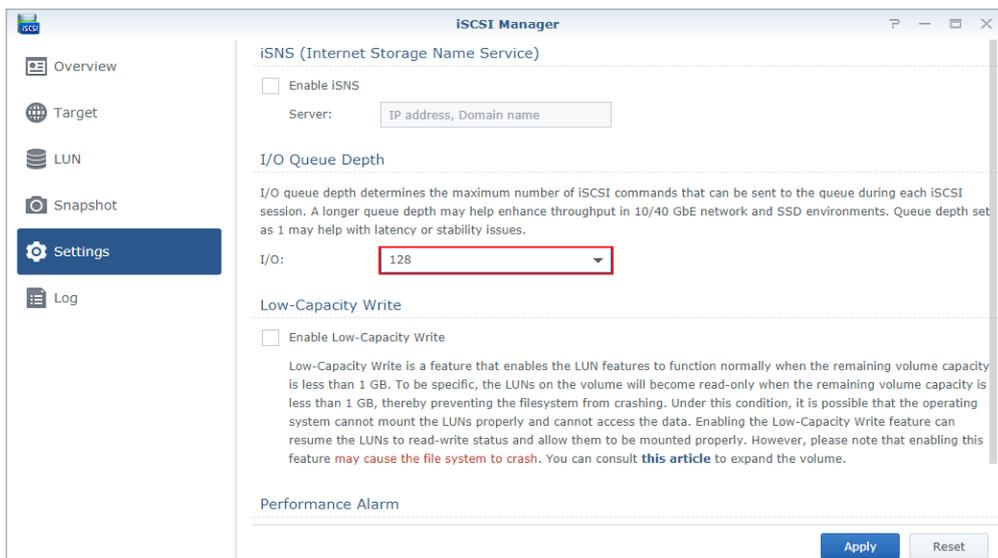
## Configure Advanced LUN Settings

The **Direct read/write** mode delivers better performance for an all-flash storage pool, allowing data to be randomly accessed. The **Buffered read/write** mode delivers better performance when data are sequentially accessed on an iSCSI LUN. After a LUN is created, we recommend selecting the direct read/write mode for randomized I/O pattern. To do so, go to **iSCSI Manager > LUN > Edit > Advanced** and select **Direct read/write**.



## Set I/O Queue Depth

I/O queue depth determines the maximum number of iSCSI commands that can be sent to the queue during each iSCSI session. A short I/O queue depth provides lower latency, and a long queue depth improves the overall throughput. In fact, a longer queue depth may enhance the throughput in a 10/40 GbE network and SSD environment. Therefore, we recommend adjusting the I/O queue depth to 128 if your UC3200 is installed with SSD caches or SSDs and a 10 GbE network card. To do so, please go to **iSCSI Manager > Settings > I/O Queue Depth** and select **128** from the I/O drop-down menu.



## Initiator Deployment

Actual initiator settings may differ according to an initiator's architecture, such as the initiators developed by Microsoft, VMware, or Citrix. However, we highly recommend following the MTU value and multipath I/O settings shown below to ensure optimal initiator deployment.

### MTU Value

We recommend setting the MTU value of a 10 GbE network card as the same as the MTU value on your UC3200 to enhance the transfer speed. Please also set the MTU value of the connected devices and initiator as the same as the MTU value of your UC3200 to ensure that they can operate properly. For more information on setting the MTU value, please refer to the [Configure Network](#) section or the initiator's website.

### Multipath I/O

The server connects to the IP addresses of the two controllers simultaneously to offer multipath I/O, thereby enhancing service reliability. More stabilized performance can be achieved when the initiator correctly recognizes the Asymmetric Logical Unit Access (ALUA). Therefore, we recommend connecting the initiator from the IP addresses of the two controllers to iSCSI Target simultaneously to enable multipath I/O.

If the performance is not as optimal as is expected, it may be because the initiator lacks the corresponding multipath package or its multipath policy does not prioritize performance. Under this circumstance, please refer to the relevant information on the initiator and adjust the multipath policy. Once you have identified which controller the LUN is created on, you can simply connect to the iSCSI Target via the IP address of the controller, thereby ensuring the I/O is routed through optimal paths.

# UC3200 Deployment after the RMA

If hardware malfunction unfortunately occurs to your UC3200, please sign in to your [Synology Account](#) to submit a technical support ticket. Synology Technical Support will assist you in troubleshooting the possible issues and may recommend applying for the return merchandise authorization (RMA) service if your product or certain product parts are defective and need replacement.<sup>13</sup>

In general, the Technical Support team will recommend applying for the RMA to either request for the replacement of **a single controller** or **the entire UC3200**. You should receive a new controller or a new UC3200 shortly after you follow the Technical Support team's instructions and send the defective product part or product back to Synology.<sup>14</sup>

Here we'll guide you through how to deploy your UC3200 after you receive a new controller or a new UC3200. Please refer to the following according to your condition.

## If a controller is replaced through the RMA

Here we assume that one of the controllers is still working properly and can be powered on. Please follow the steps below after you have received a new controller:

1. Insert the new controller in your UC3200 and power on your UC3200.
2. UC3200 will repair the system automatically and synchronize the configurations on the old controller to the new controller automatically.
3. Once the synchronization process is complete, launch **High Availability Manager** and go to the **Overview** page to check if any errors or corresponding suggestions are shown here. Please take corrective actions when necessary.
4. Now you can continue using your UC3200 like before, without needing to adjust any configurations.

## If the entire UC3200 is replaced through the RMA

Here we assume that the drives installed in the new UC3200 are the same as those installed in the previous and defective UC3200. Please follow the instructions below to deploy and restore some of the most important configurations on the new UC3200:

---

<sup>13</sup> You can apply for the RMA only if your product is still within its warranty period and was purchased from a Synology-authorized local distributor or reseller. UC3200 is backed up by Synology's [5-year limited warranty](#). Please refer to [Synology Inc. Limited Product Warranty](#) for more information on Synology's product warranty.

<sup>14</sup> Before sending your UC3200 back to Synology, please click the **Back up configuration** button (at **Control Panel** > **Update & Restore** > **Configuration Backup**) to back up the following system configurations: user, personal, password, password expiration, HTTP connection, notification, security, terminal, auto block, allow list, block list, SNMP, performance alarm, and general iSCSI Manager settings. Please note that the backed up settings do not include **Snapshot Replication** or **iSCSI Target** settings.

1. Install the original drives in the drive slots of your new UC3200 according to their previous order in the old UC3200.
2. Power on your UC3200 and follow the initial set up wizard to sign in to your DSM UC (refer to [Get Started with UC3200](#) for more information).
3. On your DSM UC, go to **Control Panel > Update & Restore > Configuration Backup > Restore configuration** to restore the system configurations that you have previously backed up.
4. Go to **Control Panel > Network** and complete the following to configure your network:
  - a. Set static IP addresses for all the required network interfaces (refer to [Set Static IP Addresses](#) for details)
  - b. Combine multiple LANs into Link Aggregation if needed (refer to [Manage Link Aggregation](#) for details)
  - c. Enable Network Failover (refer to [Enable Network Failover](#) for details)

Because the previously backed up system configurations do not include **iSCSI Target** or **Snapshot Replication** settings, it is necessary to follow the instructions below to restore or configure these settings once you have completed the aforementioned steps.

### To manually restore an iSCSI target

Since the iSCSI target originally mapped to an existing iSCSI LUN is lost after UC3200 replacement, you'll need to restore the iSCSI target and map it to an iSCSI LUN again. Please follow the steps below:

1. Launch **iSCSI Manager** and go to the **Target** page.
2. Click **Create** and enter the target name and tick the IQN options if needed. Click **Next**.
3. Select **Map existing iSCSI LUNs** and select the iSCSI LUN you want to map to. Click **Next**.
4. Confirm the settings and click **Apply**.

### To protect a thin-provisioned iSCSI LUN with snapshots

#### For basic iSCSI LUN protection

An iSCSI LUN created with thin provisioning can be protected by snapshots. Please refer to [Take snapshots for an iSCSI LUN](#) for more information and follow the steps below:

1. Launch **Snapshot Replication** and go to the **Snapshots** page.
2. Select a thin-provisioned iSCSI LUN and click **Snapshot > Take a Snapshot**. Click **OK** to finish.
3. Click **Settings > Schedule** to schedule the snapshot. Click **OK** to finish.

#### For advanced iSCSI LUN protection

iSCSI LUN snapshots can be replicated to another destination (i.e., another Synology NAS or UC3200) for advanced data protection. Please refer to [Create replication tasks for an iSCSI LUN](#) for more information and follow the steps below:

1. Launch **Snapshot Replication** and go to the **Replication** page.
2. Click **Create**, select the destination, and follow the wizard to finish.



# Conclusion

The previous chapters have offered an overview of the key features, advantages, and common scenarios of UC3200; and have guided you through the methods for optimal UC3200 deployment. However, this administrator's guide only touches on a portion of the powerful features offered by UC3200. Please refer to the UC3200 **Datasheet** and **Hardware Installation Guide** at [Download Center](#) for more information on its specifications and hardware setup, and refer to [Knowledge Base](#) for more information on the UC3200 features. Visit our website at [www.synology.com](http://www.synology.com) or [contact us](#) for product inquiries, technical support, or other assistance.



**SYNOLOGY  
INC.**

9F, No. 1, Yuan Dong Rd.  
Banqiao, New Taipei 22063  
Taiwan  
Tel: +886 2 2955 1814

**SYNOLOGY  
AMERICA CORP.**

3535 Factoria Blvd SE, Suite #200,  
Bellevue, WA 98006  
USA  
Tel: +1 425 818 1587

**SYNOLOGY  
UK LTD.**

Unit 5 Danbury Court, Linford Wood,  
Milton Keynes, MK14 6PL, United  
Kingdom  
Tel.: +44 (0)1908048029

**SYNOLOGY  
FRANCE**

102 Terrasse Boieldieu (TOUR W)  
92800 Puteaux  
France  
Tel: +33 147 176288

**SYNOLOGY  
GMBH**

Grafenberger Allee 295  
40237 Düsseldorf  
Deutschland  
Tel: +49 211 9666 9666

**SYNOLOGY  
SHANGHAI**

200070, Room 201,  
No. 511 Tianmu W. Rd.,  
Jingan Dist., Shanghai,  
China

**SYNOLOGY  
JAPAN CO., LTD.**

4F, No. 3-1-2, Higashikanda,  
Chiyoda-ku, Tokyo, 101-0031  
Japan

**Synology®**



[synology.com](https://synology.com)

Synology may make changes to specifications and product descriptions at any time, without notice. Copyright © 2019 Synology Inc. All rights reserved. ® Synology and other names of Synology Products are proprietary marks or registered trademarks of Synology Inc. Other products and company names mentioned herein are trademarks of their respective holders.