Supplemental Guide

March 2017

Installing and Configuring SnapSync Agent for iOS

Summary

This document describes how to install and configure SnapSync for iOS mobile devices from Apple. It also covers the installation of the SnapSync Agent for iOS. SnapServer NAS appliances or SnapCLOUD servers are used as primary storage targets in a peer-to-peer SnapSync configuration.

Information, Tools, and Files

Before you begin these procedures, the following information should be noted:

- This guide covers both SnapServer appliances (models XSD40, XSR40, and XSR120) and SnapCLOUD servers which use the Guardian OS software. The term "SnapServer" in this document refers to both types of systems and is used interchangeably in the document.
- This document uses the terms "SnapServer Administrator" and "Administrator" interchangeably. When more than one type of administrator is used (such as a System Administrator), the references in this document are for the Storage Administrator.
- This document also covers the roles of both the Administrator and the mobile iOS user, and the tasks that are used for each of these roles.

Prerequisites

- The Administrator should be familiar with the SnapServer Web Management Interface. Additional information on using and accessing the Web Management Interface is found in the *SnapServer Administrator's Guide* for GuardianOS. Refer to the Overland Knowledge Base for the appropriate guide:

  https://community.sphere3d.com/community/documentation/nas/snapserver

- Download the SnapSync Agent for iOS from the Overland Storage SnapSync website:

  http://support.overlandstorage.com/support/snapsync.htm

- Make sure all devices and the host that are part of a SnapSync environment have a date and time that are no more than 10 minutes apart.
- For the purposes of this guide, the following processes are considered to have been done:
  - A SnapSync user folder (`jim-iPadAir2`) for the iOS Client on the SnapServer appliance or SnapCLOUD has already been created by the Administrator for sharing.
  - The SnapSync secret key is available for the iOS mobile client to access the SnapServer storage used as a repository for shared SnapSync files.

  Additional information on SnapSync folder sharing, security key sharing, and SnapSync licensing can be found in the *SnapSync Getting Started Supplemental Guide* or the *SnapSync 2.3 User Guide*.

  https://community.sphere3d.com/docs/DOC-3933 (Getting Started)

  https://community.sphere3d.com/docs/DOC-3839 (User Guide)

Versions Tested

The SnapSync test environment uses the following versions:

- Apple iPad Air 2 iOS 9.3.2 (13F69)
- SnapSync Agent for iOS version 2.3.2
- SnapServer XSR120 running GuardianOS version 7.7.032
- SnapCLOUD server running GuardianOS version 7.7.032

Requirements Before Starting

As noted in the Prerequisites section, before installing the agent, it is recommended that these processes be completed. They must be done by an Administrator.

- Create a SnapSync user folder.
- Create a secret key for sharing files.

SnapSync User Folder Creation

To create SnapSync user folders on the SnapServer so data can be shared, the Administrator uses the Web Management Interface SnapExtensions icon (⚏) to access the SnapSync Management Console to add the folder.

The following example shows a user folder called *jim-iPadAir2*.
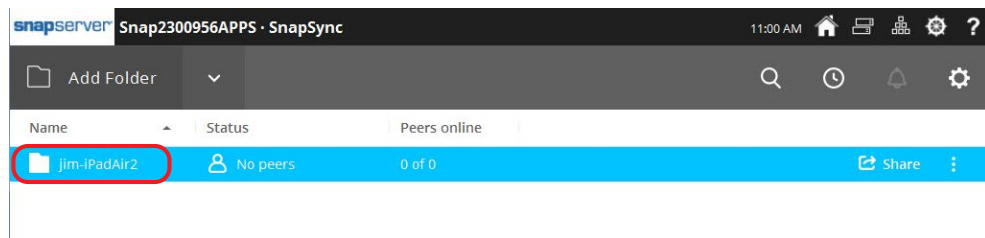
It is recommended that a unique name based on the device type be used to distinguish the device type. The user may have more than one device to synchronize, such as a desktop or laptop.

SnapServer Secret Key Creation

A SnapSync secret key is needed for the iOS client to access the SnapServer storage used as a repository for shared SnapSync files.

NOTE: A preconfigured SnapSync user folder is required. See SnapSync User Folder Creation.

1. At the right end of the user folder line, click **Share** to show the options screen.
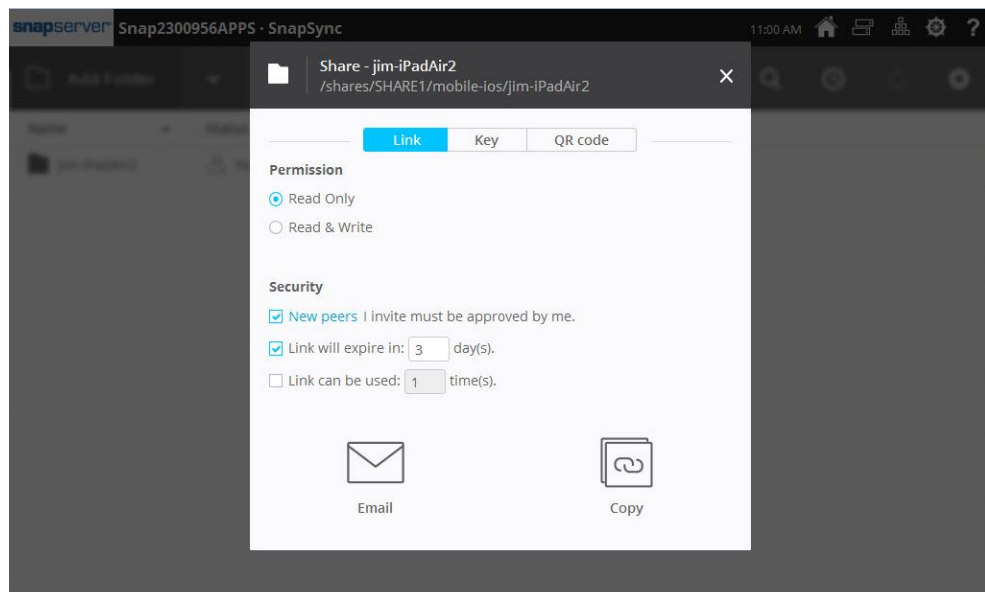
2. Select **Link** at the top of the **Share** options dialog.

3. To share the secret key, select from the following **options**.

   NOTE: Some are selected by default but can be changed.

Option	Choices	Default
Permission	Choose one: • Read Only • Read & Write	Read Only.
Security	Check all that apply: • New peers I invite must be approved by me. • Link will expire in [3] day(s). • Link can be used [1] time(s). Numbers in square brackets can be changed.	New peers and expiration date are checked by default.
Share Method	Click one of these buttons: • Email • Copy	None.

4. The Administrator enables the **Read & Write** permission for the iOS user.

   Read & Write permissions provide the ability to create, modify, and save files to the dedicated folder located on the SnapServer storage.

©2017 Sphere 3D Corp.
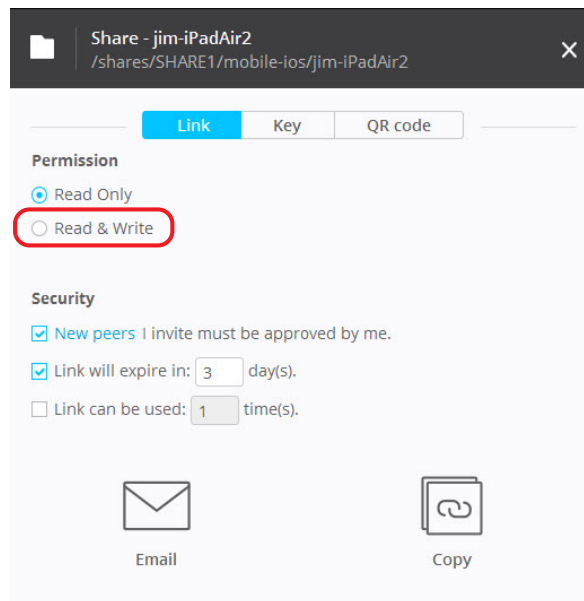
5. The Administrator can either **Email** the link to the user or **Copy** the link to the clipboard.

The **Copy** option allows the Administrator to copy the link displayed and send it by a method other than email. For example, send it via a chat session.

The **Email** option allows an iOS user to click the link in the body of the email. Here is a sample of an email sent from the Administrator to the iOS user.
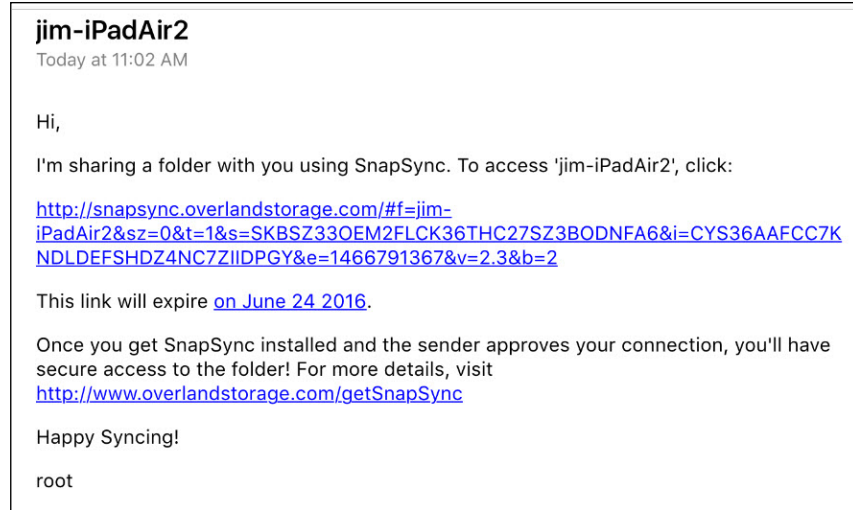

Installation of the SnapSync Agent for iOS

NOTE: If the SnapSync Agent for iOS is already installed, continue with the SnapSync Agent for iOS Synchronization section.

The SnapSync Agent for iOS can be installed when the Administrator provides the secret key via the link to the iOS user. The iOS user is then directed to the SnapSync website and from there the user can click SnapSync for iOS.
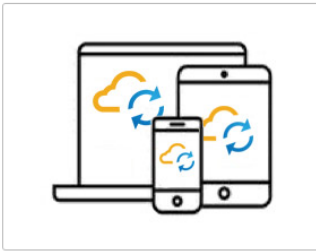
1. When the iOS user receives the email from the Administrator, click the third link:

http://www.overlandstorage.com/getSnapSync
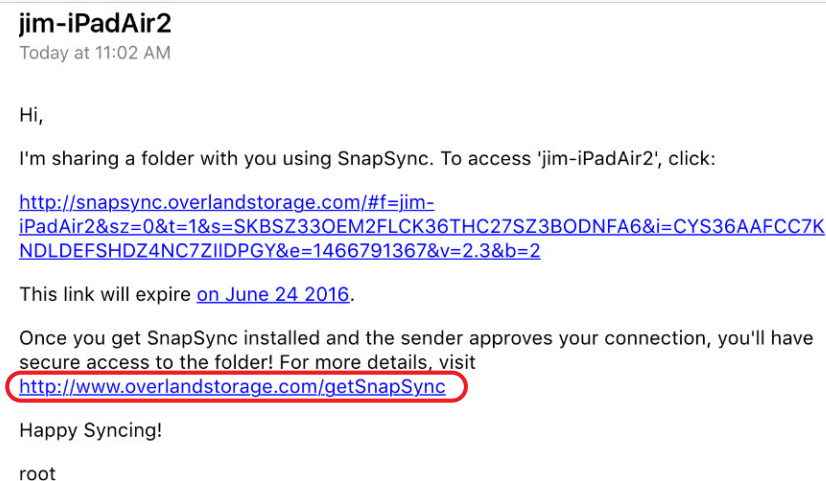
2. Scroll down to the bottom of **Downloads** and, under **Mobile | iOS**, press **AppStore**.

3. At the Apple App Store, press **Get** to install SnapSync.
   The usual circle progress bar is shown as it installs.

4. When the install finishes, press **OPEN**.

5. Once SnapSync **application** is open:

   a. Select whether to accept **notifications** or not.

    b. Choose either skip the **tour** or swipe through it
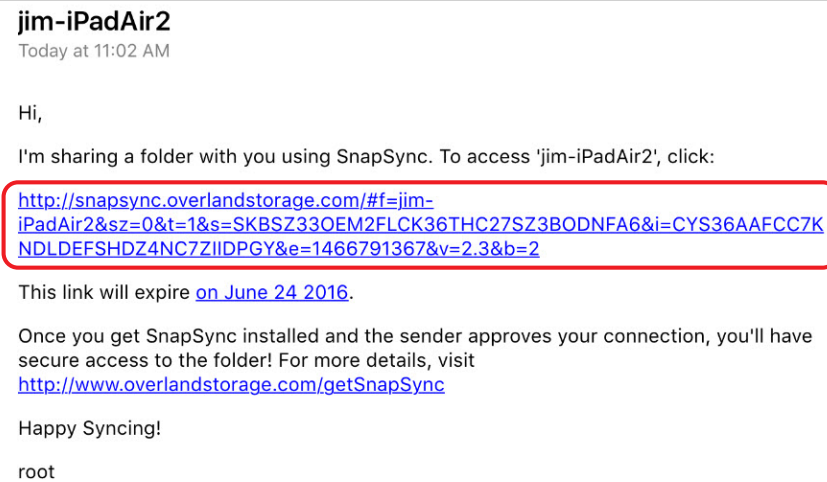
    c. Click **GET STARTED**.
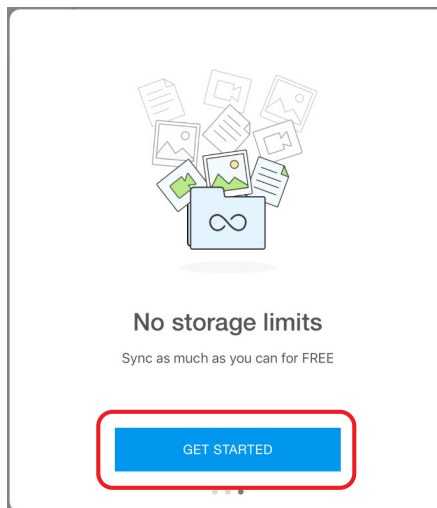
6. When the User Name setup appears, enter a **unique user name**, and press **DONE**.
For clarity, use a descriptive user name for the mobile device.
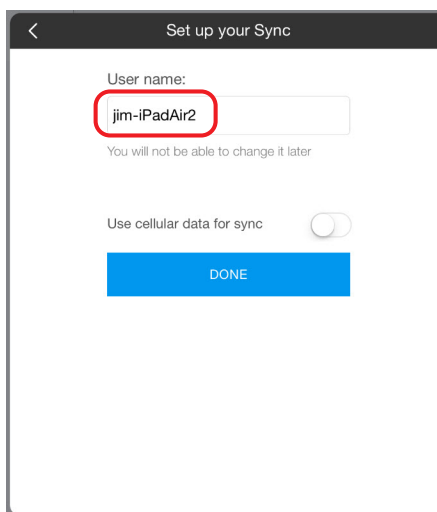
# SnapSync Agent for iOS Synchronization

Use the following steps to synchronize the SnapSync Agent for iOS to the SnapServer storage.

1. Open the original email received from the Administrator and press the **first link**.

   jim-iPadAir2
   Today at 11:02 AM

   Hi,

   I'm sharing a folder with you using SnapSync. To access 'jim-iPadAir2', click:

   http://snapsync.overlandstorage.com/#f=jim-
   iPadAir2&sz=0&t=1&s=SKBSZ33OEM2FLCK36THC27SZ3BODNFA6&i=CYS36AAFCC7K
   NDLDEFSHDZ4NC7ZIIDPGY&e=1466791367&v=2.3&b=2

   This link will expire on June 24 2016.

   Once you get SnapSync installed and the sender approves your connection, you'll have secure access to the folder! For more details, visit http://www.overlandstorage.com/getSnapSync

   Happy Syncing!

   root

2. When the SnapSync link opens in the Safari browser, press **Add Folder** (to add `jim-iPadAir2`), and then press **OK** to confirm.
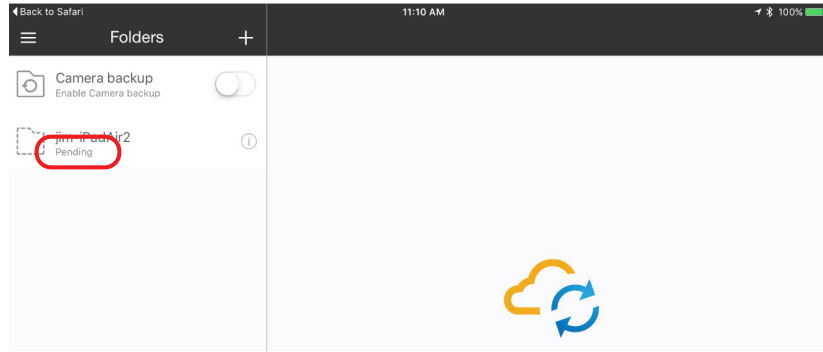   This synchronizes the new local folder with the folder on the SnapServer.
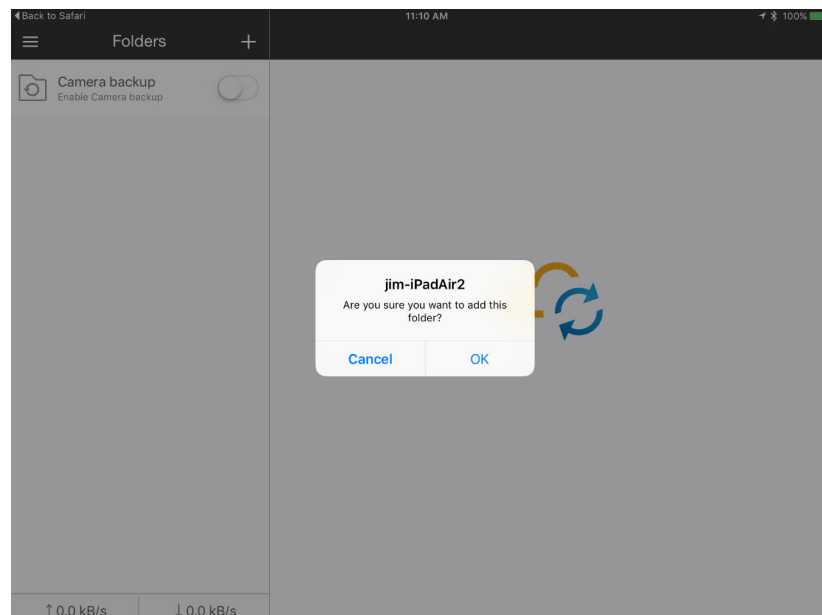
3. If the **New peers I invite must be approved by me** option was enabled, a **Pending** status is displayed.
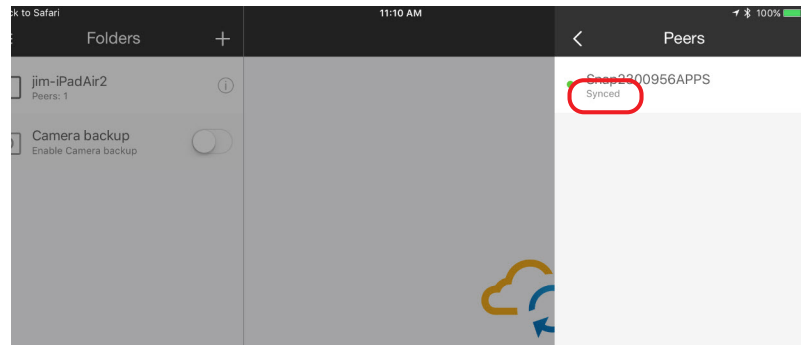   The Administrator must approve it before continuing.

4. When alerted about the pending approval, the Administrator clicks the **check mark** to allow access to the iOS SnapSync folder located on the share of the SnapServer.

Once synchronized, SnapSync Agent for iOS **Peers** list displays the SnapServer as **Synced**.

5. In the SnapSync applet, press the **name** of the folder in the left-pane, then press **ADD FILES**.
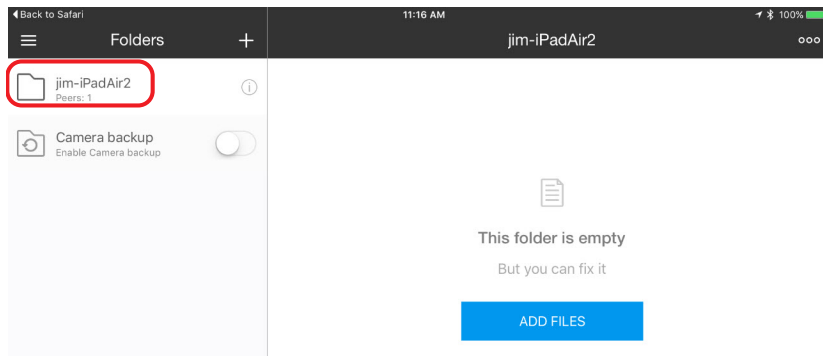
6. Select the **files** to synchronize to the SnapServer.

   At the **"SnapSync" would like to access your photos** message, click **OK**, select the photos or videos you want to synchronize, and press the check icon.
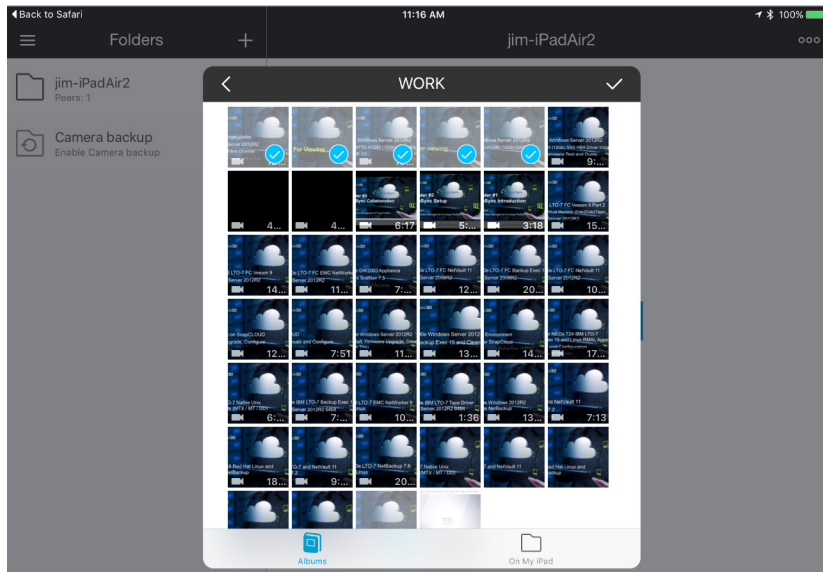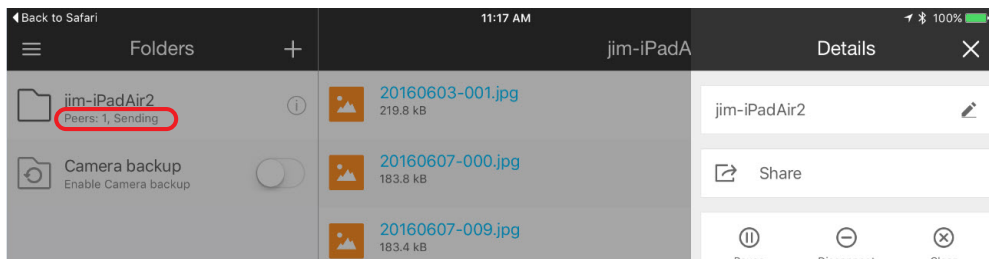

Photos and videos are not the only files that can be synchronized. When you click **Add files**, you have the option to select other shared applications. Choose the appropriate method.
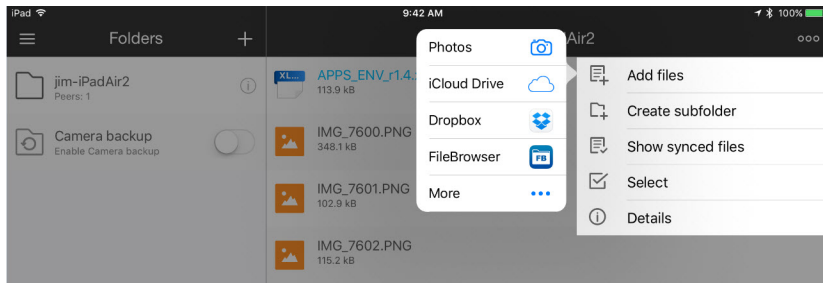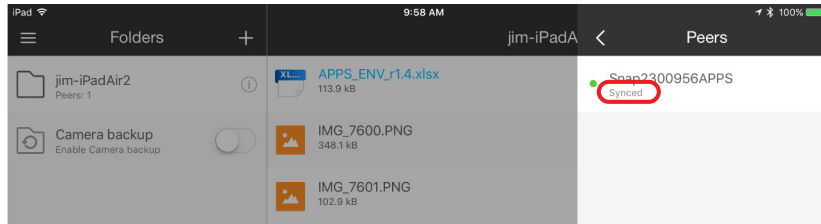

At the SnapServer, the SnapSync status shows **Receiving.**
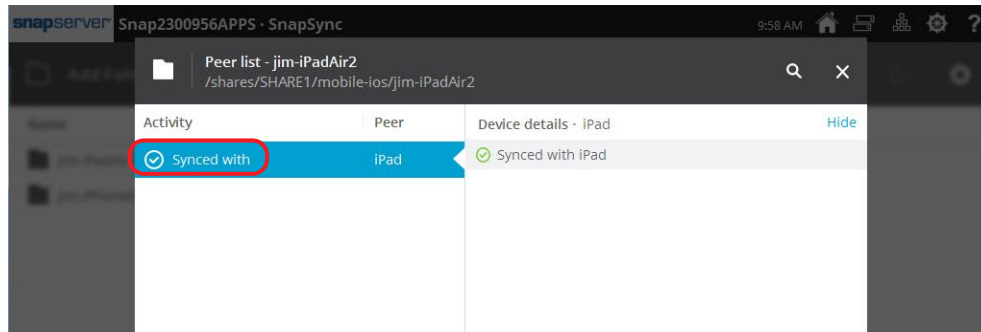

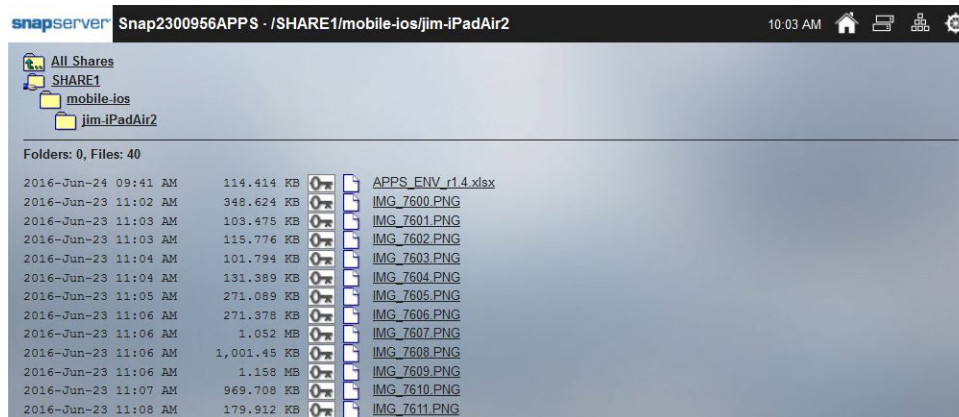The SnapSync app on iOS folder status shows **Sending.**

Once synchronization completes, a status is displayed from the SnapSync Agent for iOS showing that it is in sync with the SnapServer.

Also, the SnapServer shows it is synchronized with the iOS user.


The synchronize data is displayed on the SnapServer at the Home screen for the share.

Create an iOS Camera Automatic Backup with SnapSync

The following steps walk you through syncing photos and videos automatically on the iOS mobile device. This option automatically synchronizes to a SnapServer.
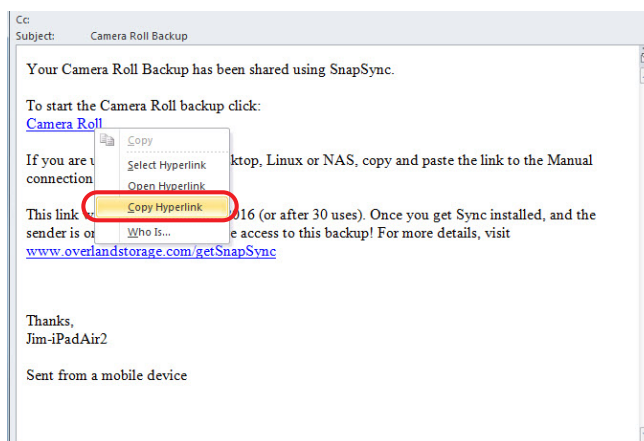
1. From the iOS SnapSync **Folders** menu, enable the **Camera backup** option.
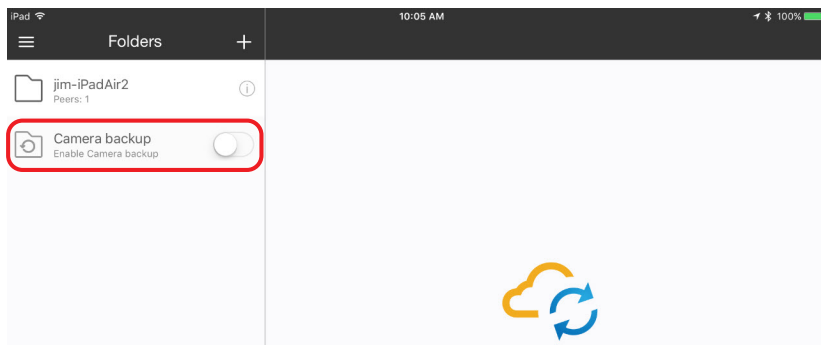
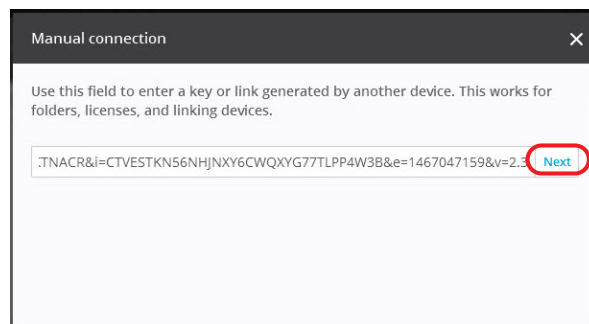2. Press **Email** and send it to the SnapServer Administrator.
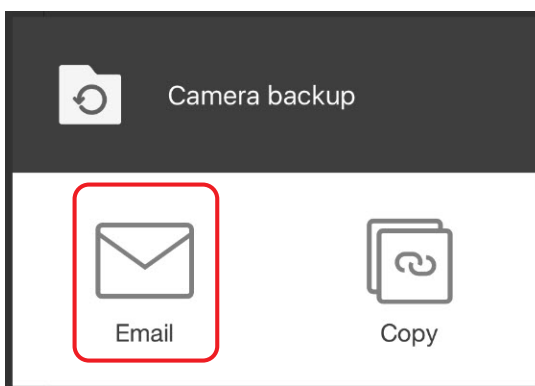
3. The SnapServer Administrator sets up a **folder** for the user:

   a. When the email request is received, right-click the **link** and select **Copy Hyperlink**.

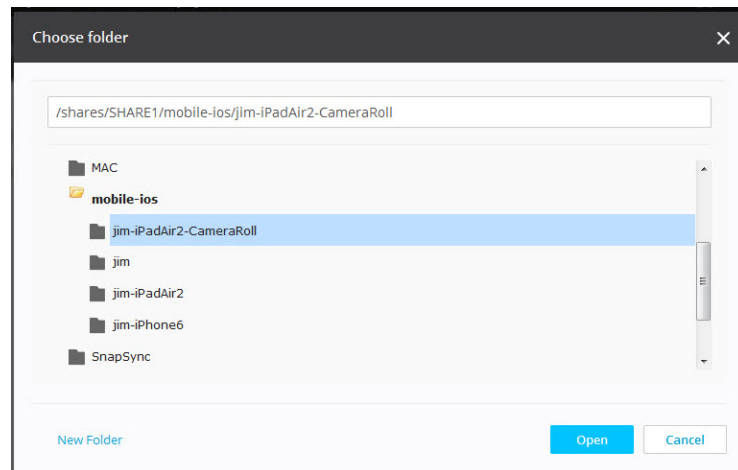**b.** From the SnapServer Web Management Interface, click **Manual Connection**.

c. Paste the copied link in the field and click **Next**.

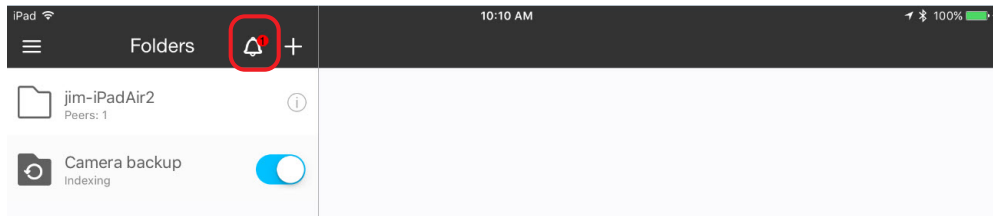As a best practice, the Storage Administrator should create a folder specifically for the mobile iOS user.

d. The Administrator creates a **new folder** for the iOS user's camera roll, and clicks **Open**.
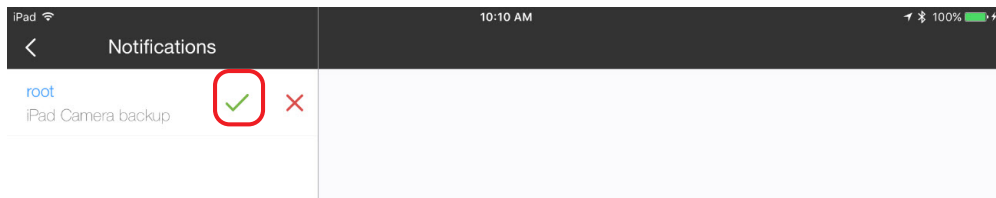
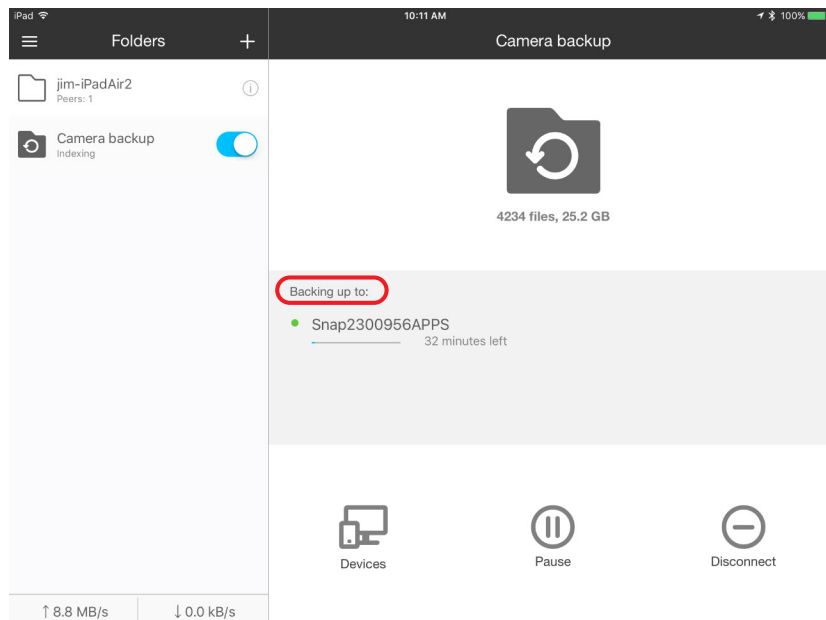A **Pending approval** status is displayed.

4. When the iOS user receives the notification in SnapSync, press the **alert icon**.
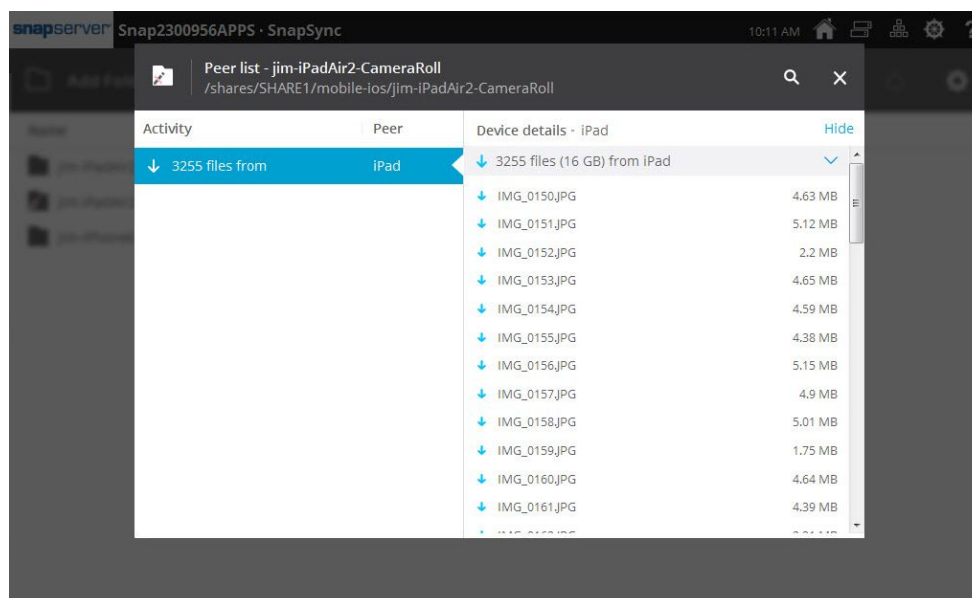

5. The iOS user press the **green check** option in order to start syncing.

SnapSync on iOS will start synchronizing the photos and videos to the SnapServer.

The Web Management Interface shows the following activity.

SnapSync Considerations

For the most recent information and details on SnapSync configuration and use, refer to the documentation on the Overland Storage website:

www.overlandstorage.com/getsnapsync

Additional information is available in the Overland Knowledge Base:

https://community.sphere3d.com/community/documentation/nas/snapserver

• For SnapSync destinations under a UNIX or Mixed security model, SnapSync creates UNIX personality files and directories, and sets the permissions to 644 (files) or 755 (directories) for UNIX owner root/admingrp. As a result, all users and groups can read the files but only root can modify them.

It is recommended that Windows-only security models are used at the destination, and that Windows permissions are set at the top level destination directory to apply the desired permissions to all files and subdirectories created by SnapSync.

• SnapSync cannot be used to replicate snapshots because it requires the ability to write to the sync location and snapshots are read only.

• SnapSync installs as a hidden directory either on a volume (Traditional RAID) or storage pool (DynamicRAID). If the volume or storage pool is deleted or rolled back from a snapshot, SnapServer attempts to automatically relocate the SnapSync hidden directory to another volume or storage pool.

If there are no more volumes or storage pools, or if none can be found that are large enough, SnapSync is disabled and cannot be re-enabled until a suitable volume or storage pool becomes available. Once a re-enabled, SnapSync must be completely reconfigured again.

• There are SnapSync mobile apps that make synced documents available on iOS and Android mobile devices. Refer to our website for details on downloading, configuring, and using SnapSync mobile apps.

- SnapSync changes the files and folders ownership from admin to root after it finishes syncing. If you edit the same file with Administrator credentials on the target server and then try to save it, you will get an "access is denied" error from the windows client.