COHESITY

Protect VMware Cloud Foundation 5.x with Cohesity

Backup and Recovery for VMware Cloud Foundation with Cohesity

Version 2.0

January 2026

ABSTRACT

In today's large organizations and enterprises, VMware Cloud Foundation provides a flexible and simplified private cloud platform with public cloud extensibility. The products included are vSphere (Compute), vSAN (Storage), NSX (Networking), VCF operations, and VCF automation, all of which are combined into a single solution. Therefore, it is essential to protect that infrastructure efficiently and reliably. Read these practical recommendations for configuring Cohesity protection for VMware Cloud Foundation, with a focus on in-place recovery. You will find descriptions, technical recommendations, and notes describing common mistakes to avoid.

Table of Contents

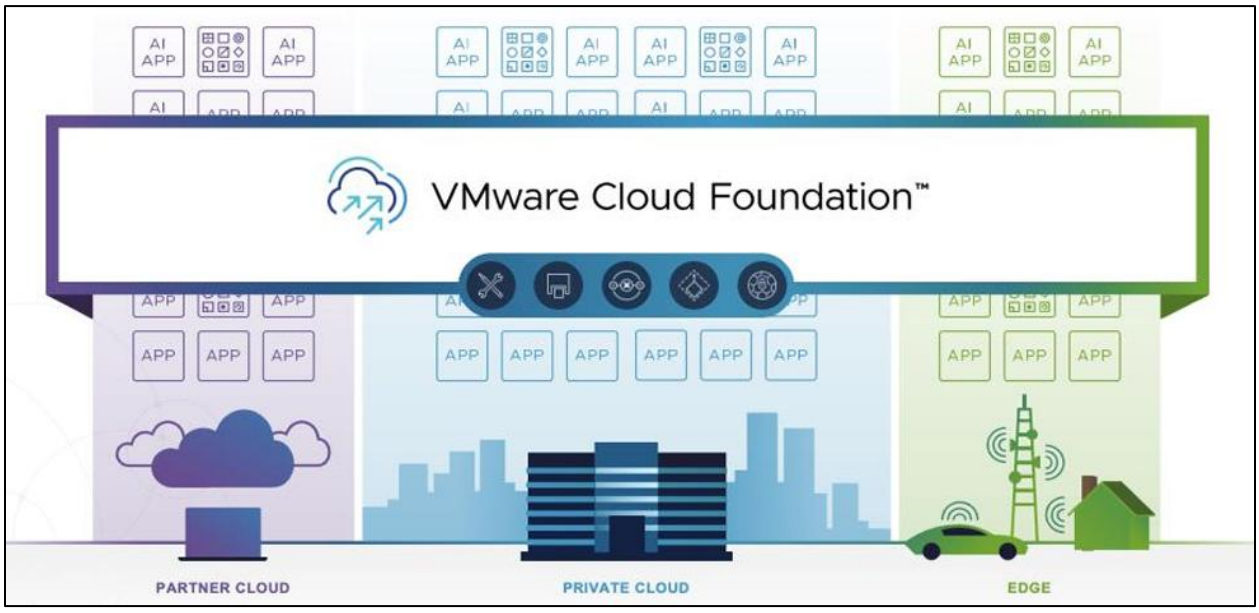
VMware Cloud Foundation 4
VCF Data Protection Challenges 5
Cohesity SecureView App 6
Install SecureView App 7
Pre-requisite for Installation 7
Installation Steps 8
Accessing the SecureView App 12
Protect VMware Cloud Foundation 13
Create Users 14
Create Directory 16
Register Sources 17
Edit VCF Source 20
Discover VCF Components 21
Protect VCF Components—SDDC Manager 24
Modify SDDC Manager Backup Configuration 27
Backup Now ─ On-demand Backup 29
Refresh Backup Summary 31
Protect VCF Components—NSXT Cluster 32
Setup Data View's Storage Lifecycle Management Rules for NSXTCluster Backup Retention 35
Protect VCF Components—vCenter 38
Edit SFTP Details of Component 40
On-demand Backup 42
VCF SmartFiles Views 43
Protect SmartFiles Views 43
SecureView App Recovery 46
Access Backup Data 48
Recovery Process for VCF 50
API Spec 50

Appendix 51
Your Feedback 54
About the Authors 54
Document Version History 54

VMware Cloud Foundation

In today's world, organizations want to use the digital-first approach to innovate faster and more efficiently. The organization needs faster technologies to achieve it, and the VMware Cloud foundation serves the organization's purposes. VMware Cloud Foundation (VCF) is VMware infrastructure that has the Compute (vSphere and ESXi), Storage (vSAN), networking (NSX), and VCF operations and VCF automation into a single solution. VCF is deployed with the parent entity as SDDC (Software Defined Data Center), a collection of hosts with the standard set of VMware software. SDDC is a unified platform integrated with all the child entities of the VMware architecture, such as computing, Storage, and networking, and it majorly reduces technological debt.

Figure 1: VCF Overview



An organization can use the cloud-first approach to run the workload on the cloud or use the hybrid model of the IT infrastructure. VCF platform allows the organization to leverage the applications/services on-prem or with the partner cloud. Ease of use of the applications will increase the scalability of IT infrastructure, and data protection is the primary need to protect and secure the applications/workloads and their data.

Cohesity provides a radically simplified way to protect, secure, govern, and analyze your data. Cohesity data protection provides the functionality to protect your VCF environment, seamlessly integrating and providing the functionality of protection and recovery.

VCF Data Protection Challenges

The customer may face multiple challenges with the VCF solution as it is a complex solution that integrates various components, such as SDDC, NSX, vCenter, etc. Data protection is one of the primary needs that has the following challenges:

- To back up multiple platforms and components
- One solution compatibility and seamless integration with VMware
- Secure data transfer between customer and backup vendor infrastructure
- Scalable backup solution w.r.t the scalability of customer workloads
- Protection from ransomware attacks
- Long-term retention and disaster recovery of production workloads
- Granular control on backup and file/folder recovery

To overcome the above challenges, Cohesity provides a marketplace app named “SecureView” that will seamlessly integrate with the VMware Cloud Foundation.

Cohesity SecureView App

Cohesity provides the SecureView App, a secure and efficient solution for VMware cloud foundation data protection. SecureView App will transfer and manage files using the secure file transfer protocol (SFTP) through its Cohesity SecureView marketplace App. This application bridges the gap by offering a streamlined and user-friendly interface for configuring and managing SFTP access to Cohesity storage infrastructure via the Cohesity native capabilities of SFTP service. The goal is to provide users with an intuitive application that can be easily set up with minimal effort, enabling SFTP access to the underlying Cohesity SmartFiles view.

By introducing the Cohesity SecureView Marketplace App, Cohesity enhances its overall data protection capabilities and meets the diverse needs of customers who rely on SFTP-enabled applications for their backup and data transfer requirements. The app's intuitive design and seamless integration with Cohesity view enables users to securely transfer files without complex configurations or dedicated SFTP server setups.

Backup capabilities for the following VCF components:

- SDDC managers
- NSXT Cluster
- vCenter

> **NOTE**: All NSX Edge configurations (logical routers and edge services gateways) are backed up as part of NSX Manager data backup.

Refer to VMware documentation for more information.

The SecureView App will have the following components for the data protection of the VCF infrastructure:

1. Source
2. User
3. Directory
4. Cohesity Views

Source: This is the VCF environment registered on the Cohesity Secure View App.

User: The initial step is configuring the SFTP user, which you must configure on the SecureView App. This isolated user belongs to SFTP, only to transfer the data securely from the VCF infrastructure to the user's directory, which resides on the Cohesity SmartFiles Views. SFTP users are not part of the Cohesity cluster or the VCF infrastructure. These users have access to the SFTP client to transfer the data.

Directory: This is the SFTP directory located inside the Cohesity SmartFiles View, which stores the backup data. This directory belongs to DataView as it stores only the VCF infrastructure data.

Views: The Cohesity SecureView App needs two SmartFiles Views: Configuration and DataView. The user aligns with SFTP and has access to both views as these are in co-relation with each other.

Configuration Views: This stores the metadata of the configuration of the VCF environment (along with the SFTP users/directory config), which co-relates with the data view or the backed data in the Data view. This has information about all the registered sources and their components.

DataViews: All the VCF environment data are backed up in DataView with the co-relation of metadata/index in the Configuration View.

Install SecureView App

Installation of the SecureView App is an easy process, and it will provide the UI to configure and manage the SFTP user access to Cohesity storage infrastructure. Before installation, make sure that the prerequisites below are met.

Pre-requisite for Installation

1. VMware Cloud Foundation
   - 5.1 and 5.2
2. Cohesity Cluster version
   - 7.1.2_u3 or higher
   - 7.2 or higher
   - 7.3 or higher
3. Managed Firewall ports
   - Ensure TCP port 63795 is enabled between the VCF components and Cohesity Cluster. This port is used for SFTP access to transfer backup data.
   - Ensure TCP port 63800 is enabled between the HTTP Client and Cohesity Cluster. This port is used to launch the SecureView App UI.
4. Cohesity Views Setup
   - Two Cohesity views need to be created on the Cohesity cluster, each with NFS read/write protocol support. These views are mounted on the pod during the application's initialization process.
   - The first view, referred to as "**ConfigView**," stores VCF source configurations, including SFTP username, UID, GID, encrypted password, and home directory, as .conf files.
   - The second view, referred to as "**DataView,"** acts as the repository for all files (backup) transferred by VCF users.
5. User Permissions
   - Ensure a cluster user with the **Manage Cohesity Views** privilege is available to access SecureView App endpoints.
   - Marketplace Access: The Marketplace App management should be enabled on the Cohesity cluster to ensure you can install and run apps. Refer to Manage Apps in product documentation for more information.

- To register the VCF source, ensure the provided user account has **Administrator role** privileges in the VCF environment.

6. Resource Availability
   - Ensure the cluster has sufficient computing and memory resources for the app instance.
   - The memory and compute requirements depend on the size of the app instance.
   - The small instance of the application can handle 175-200 concurrent SFTP client connections without impacting performance. In case of more clients, medium/large instances are recommended.

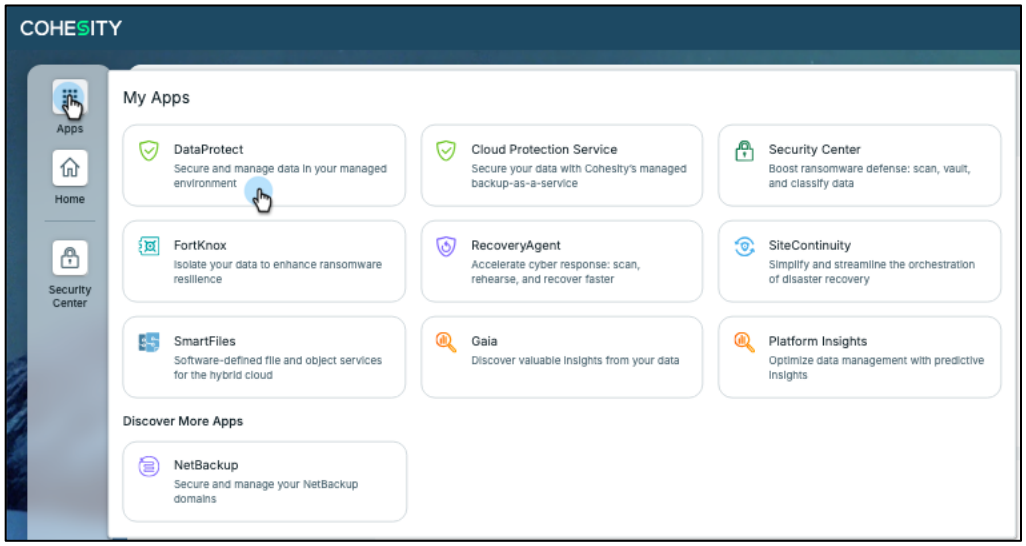
App Instance Size	Memory	Compute	Compute node
Small	2 Gb	4000 millicores	No
Medium	4 Gb	6000 millicores	Yes
Large	6 Gb	10000 millicores	Yes

NOTE: The app instance size is set to small by default.

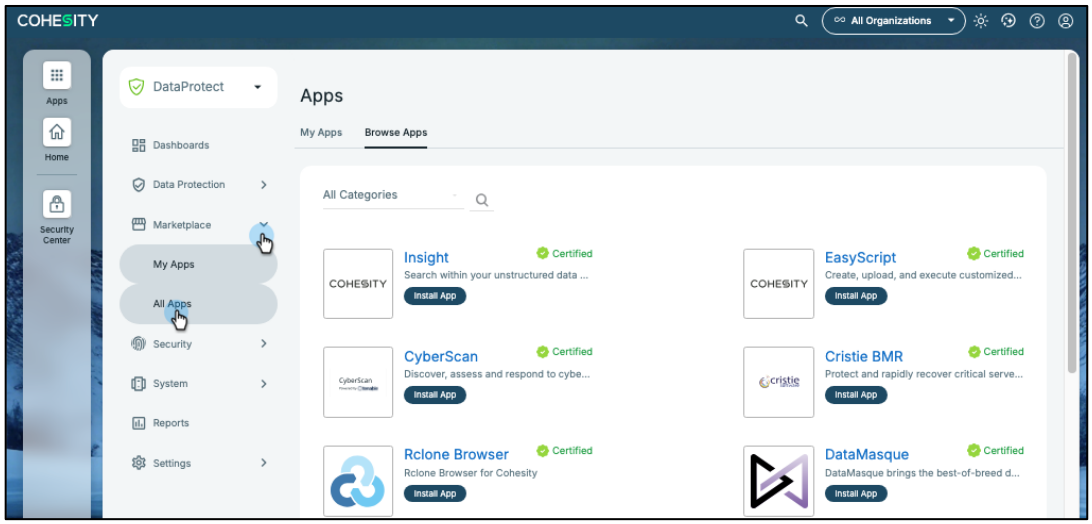
Installation Steps

To install the SecureView App, follow the steps below.

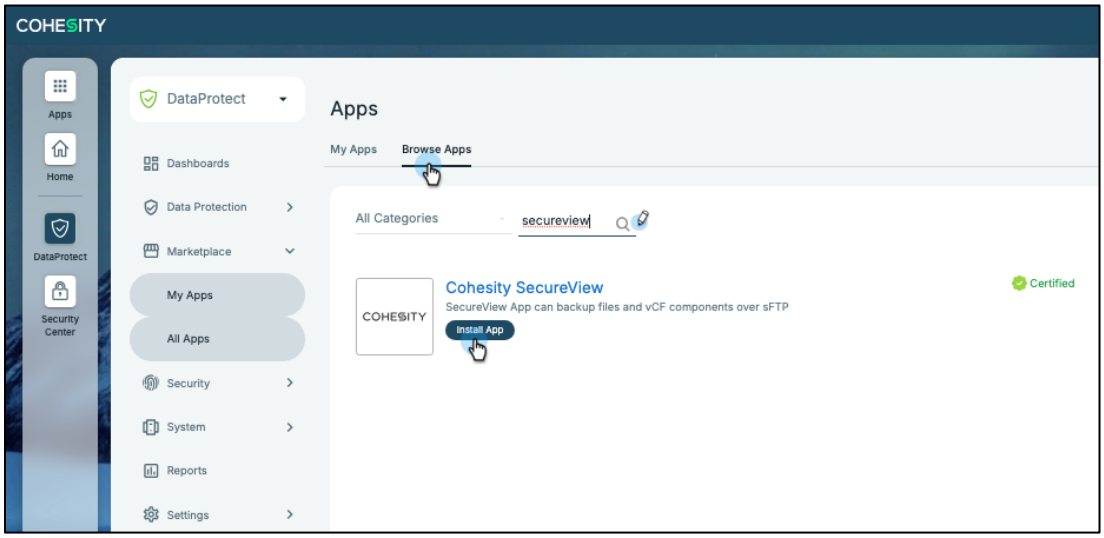
1. Login to **Helios**.
2. Click **Apps** Launcher and select **DataProtect**.



3. Go to **Marketplace – All Apps.**

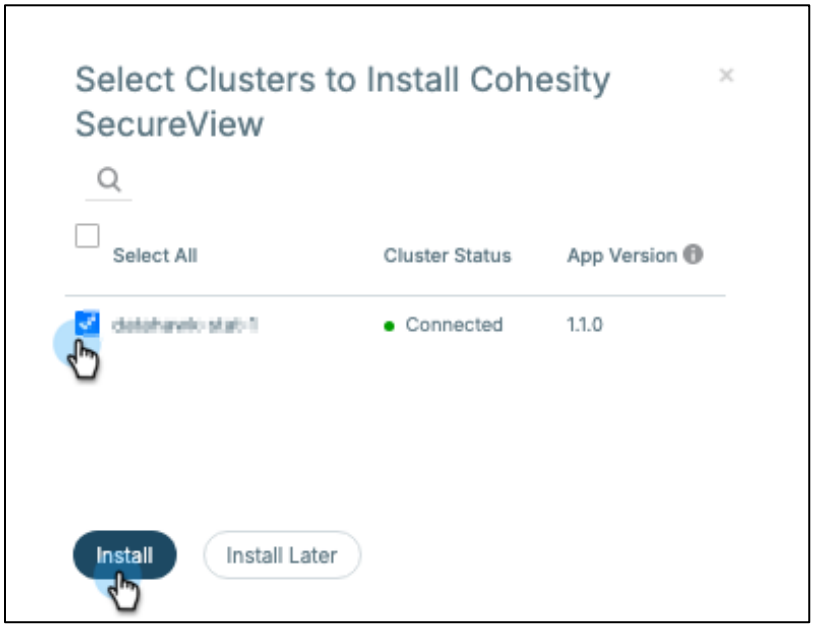


4. Under **Browse Apps** search for SecureView and click **Cohesity SecureView – Install App.**

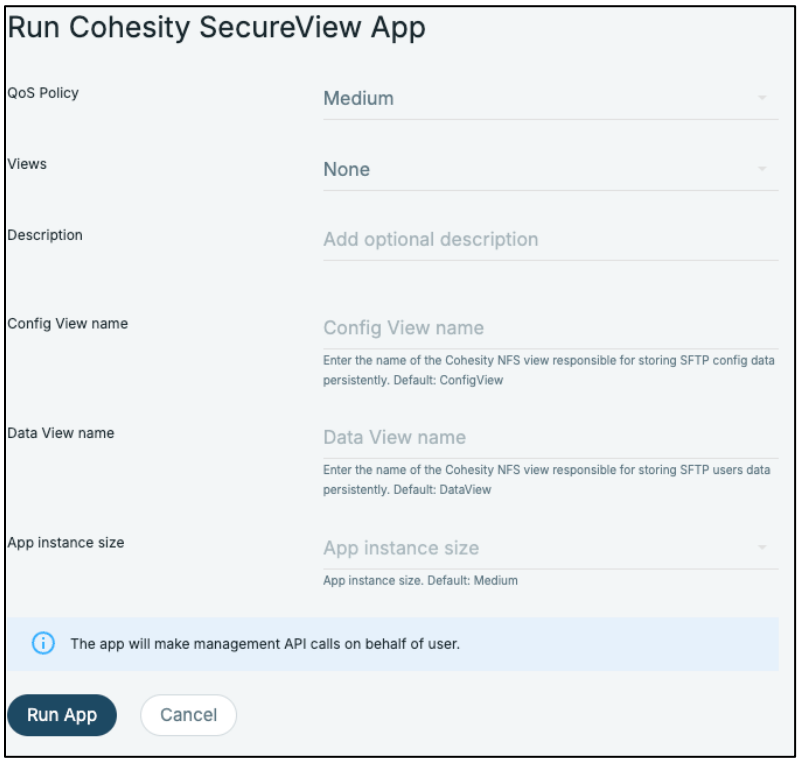


NOTE: Optionally, you can use app package files to perform an offline installation using the Upload App option. Refer to Appendix for offline installation steps.

5. From the Cluster list, Select the Cohesity cluster to install the SecureView App and click **Install.**



6. The Cohesity SecureView App will be listed in the **My Apps** section of Helios. It will first download the application and then install it automatically.
7. Create the two SmartFiles Views, one for Configuration (**ConfigView**) and the other for Data (**DataView**) with NFS read/write protocol. Refer to the section to create the SmartFiles View.
8. To run the App, click **Run App** in the **My App** section. Enter the details.



a. **QOS Policy**: This has four options: Low, Medium, High, and Max.

b. **Views**: This option is not applicable for VCF backups and should be set to None.

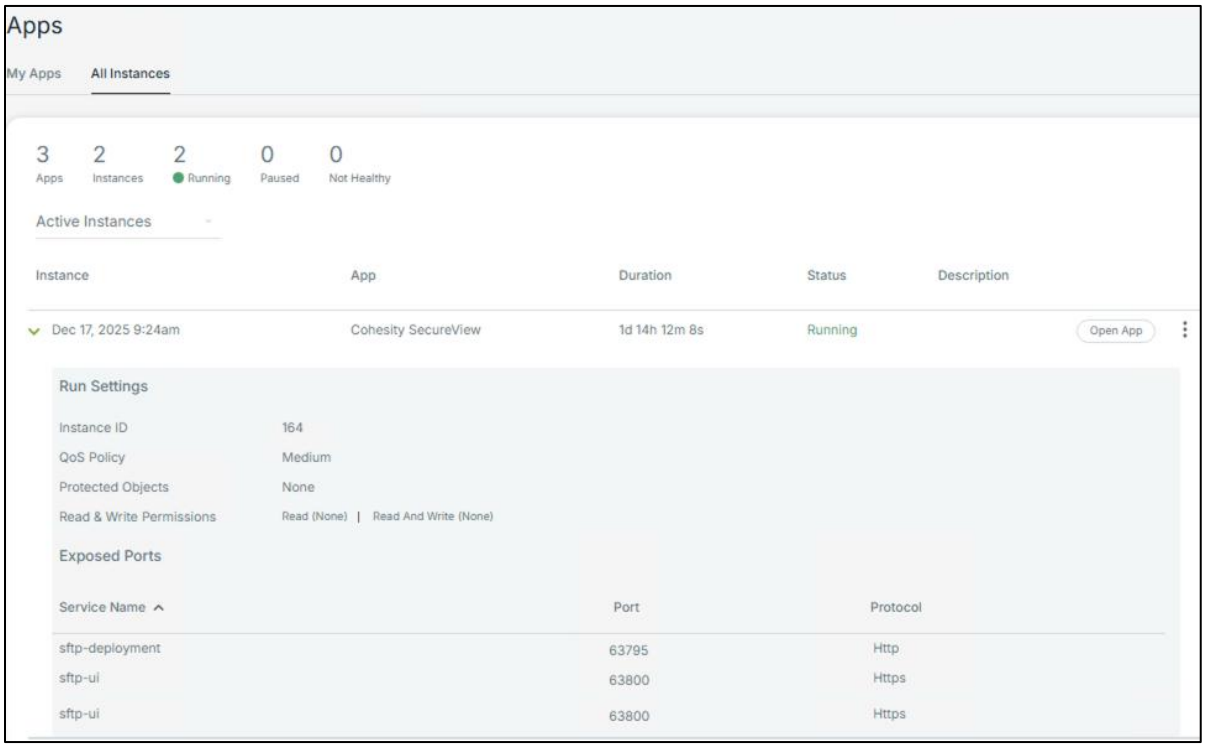
c. **Description**: Enter the description of the application.

d. **Config View Name**: Enter the Config View name (**ConfigView)** created in step 7. This view will store VCF source configurations, including SFTP username, UID, GID, encrypted password, and home directory, as .conf files.

e. **Data View Name**: Enter the Data View name (**DataView)**, created in step 7. This view will be used as the repository for all backup files transferred by VCF users.

f. **App Instance Size**: There are three sizes available: **small, medium**, and **large**. The default size is small.

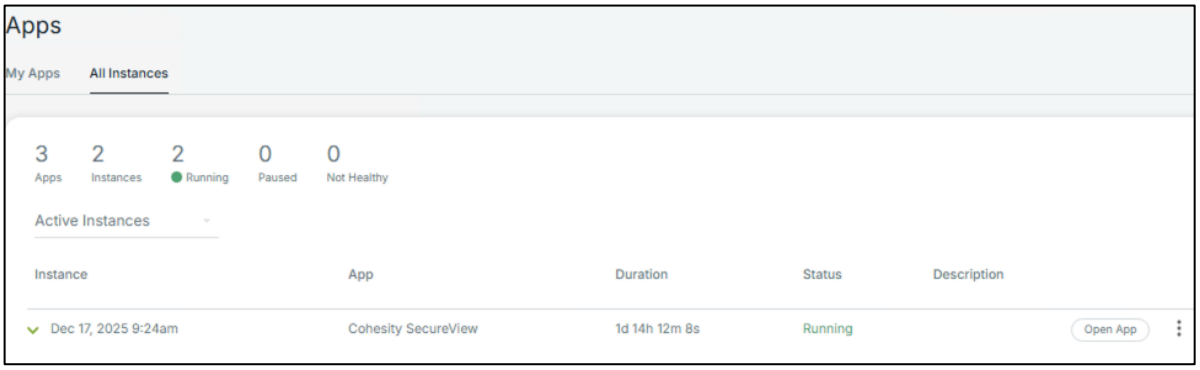
9. Once the app instance is running, its state will appear healthy after initialization.



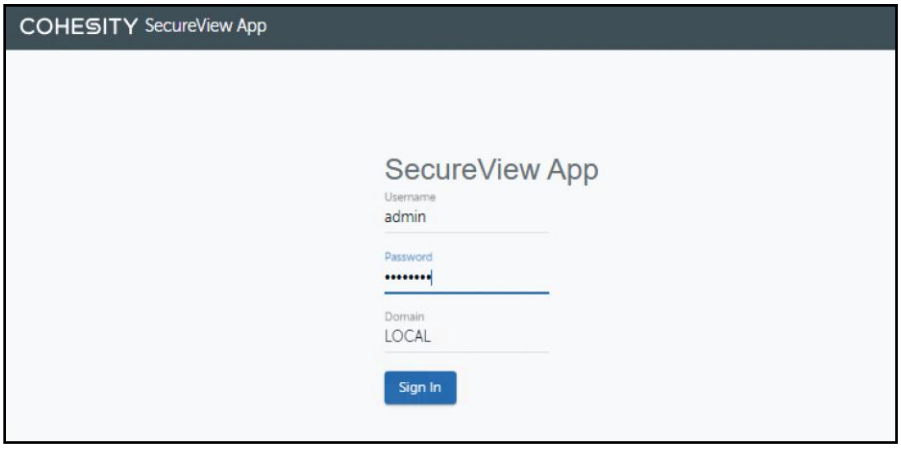
Accessing the SecureView App

To launch the app, follow the steps below:

1. Log in to **Helios**.
2. Navigate to **DataProtect** > **Marketplace** > **My Apps**.
3. In the **All Instances** tab,
   g. Verify that the SecureView App instance status is Running.
   h. Click **Open App** to launch the GUI in a new tab.



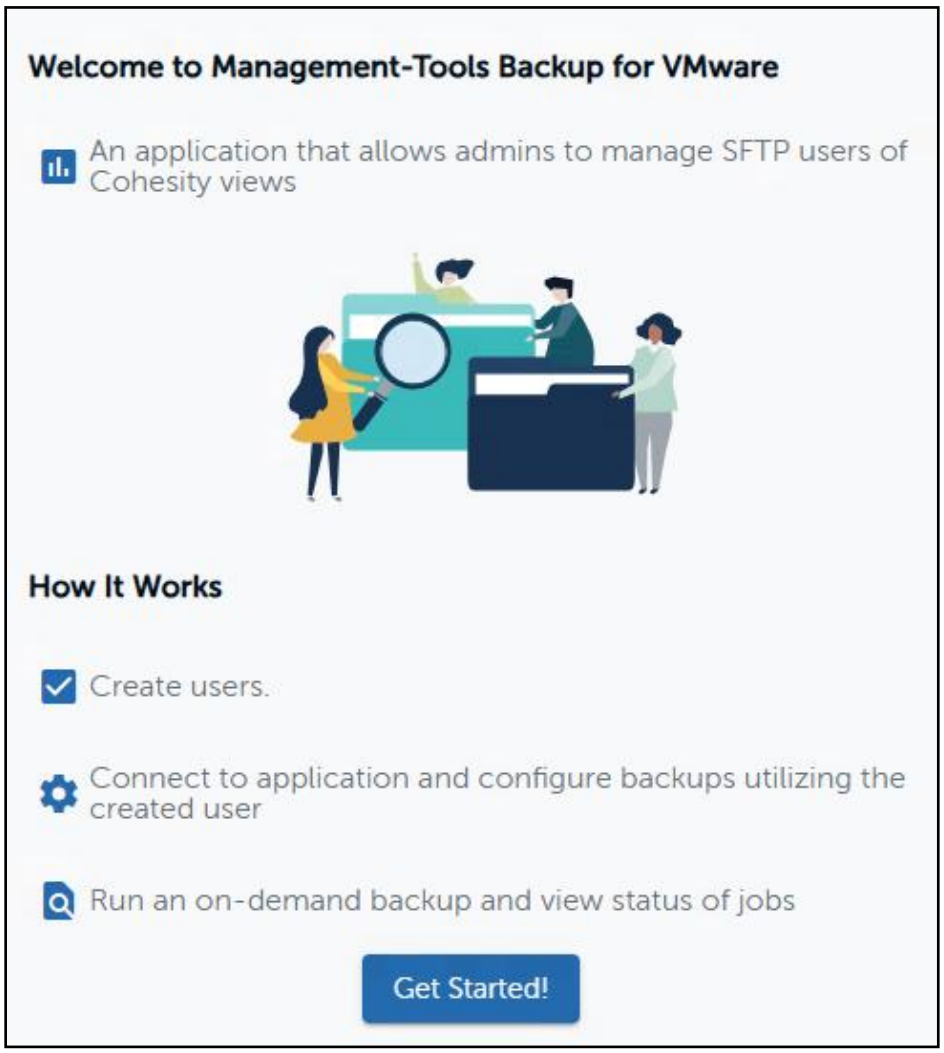
4. Enter the username and password to log in to the SecureView App. Local and AD users with Manage Cohesity Views privileges can access the SecureView App.



NOTE: The **SecureView App UI** is launched using TCP port 63800.

Protect VMware Cloud Foundation

To protect the VCF environment configuration, there are self-guided steps available to configure the file-based backup in the Cohesity SecureView App with the following three steps:

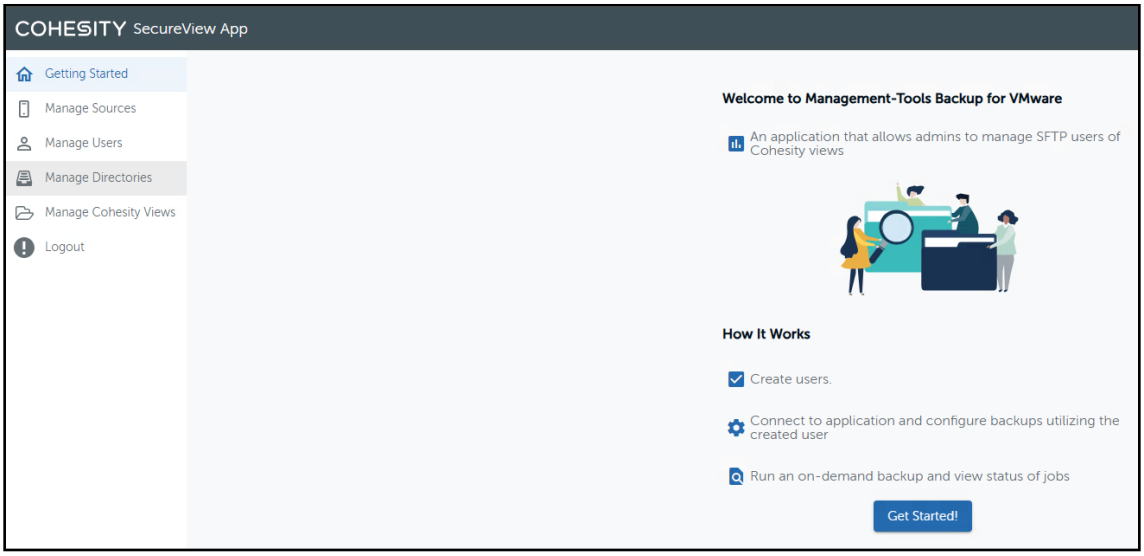


The Cohesity SecureView App has the following four components:

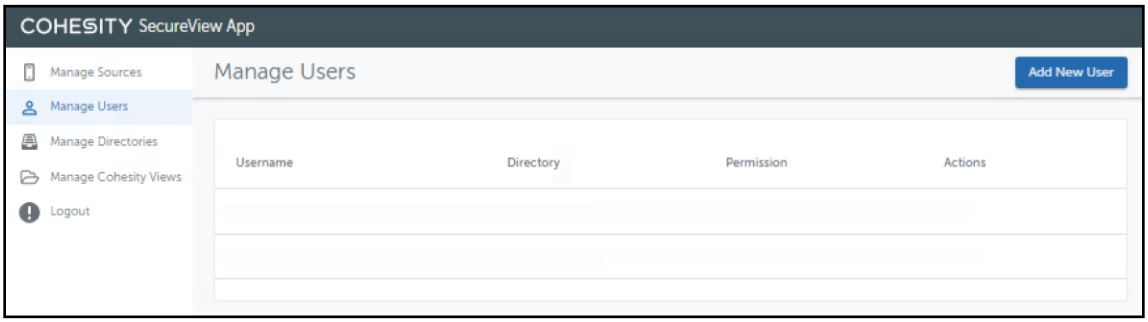
1. Users
2. Source
3. Directory
4. Cohesity SmartFiles Views

Create Users

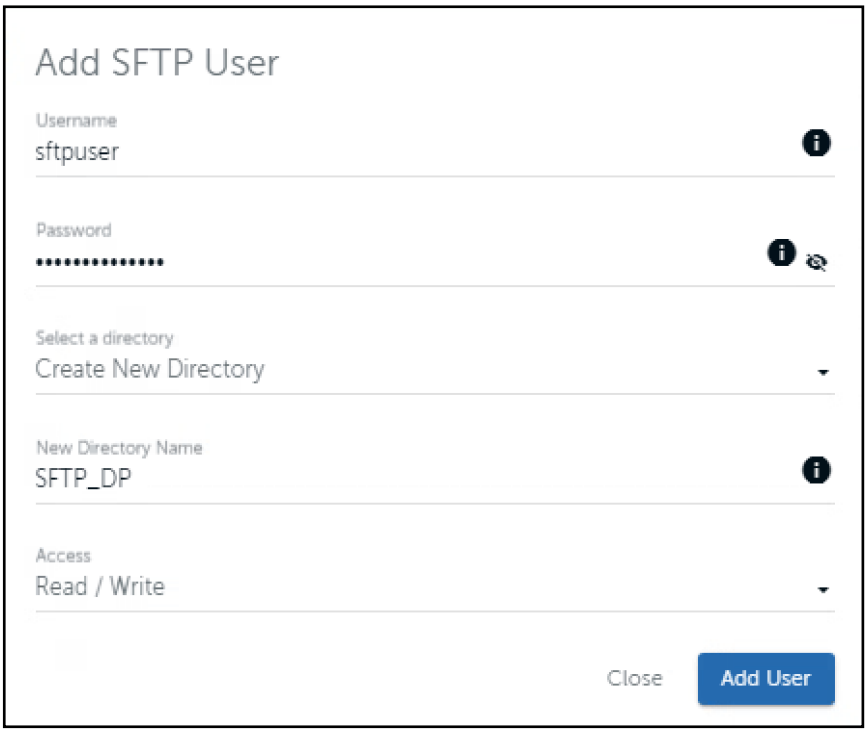
1. To create the SFTP user, click **Get Started** and follow the steps, or you can create a user from the **Manage Users** option.



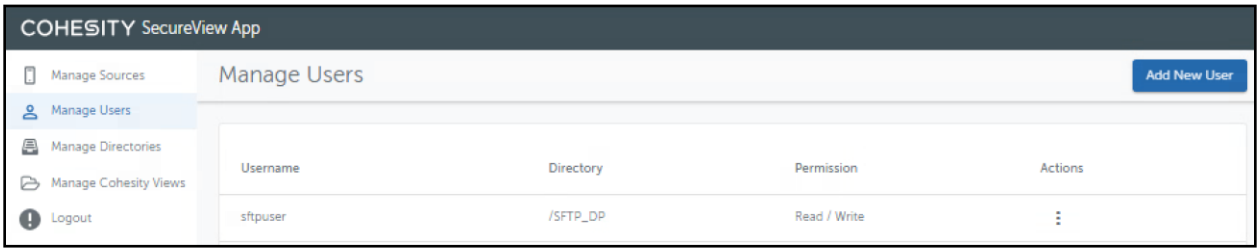
2. For this guide, we will follow the self-guided option. Click **Get Started** > **Add New User**.



3. Enter the following details and click **Add User**.
   a. Username
   b. Password
   c. Select an existing directory or add a new directory and assign the access privileges

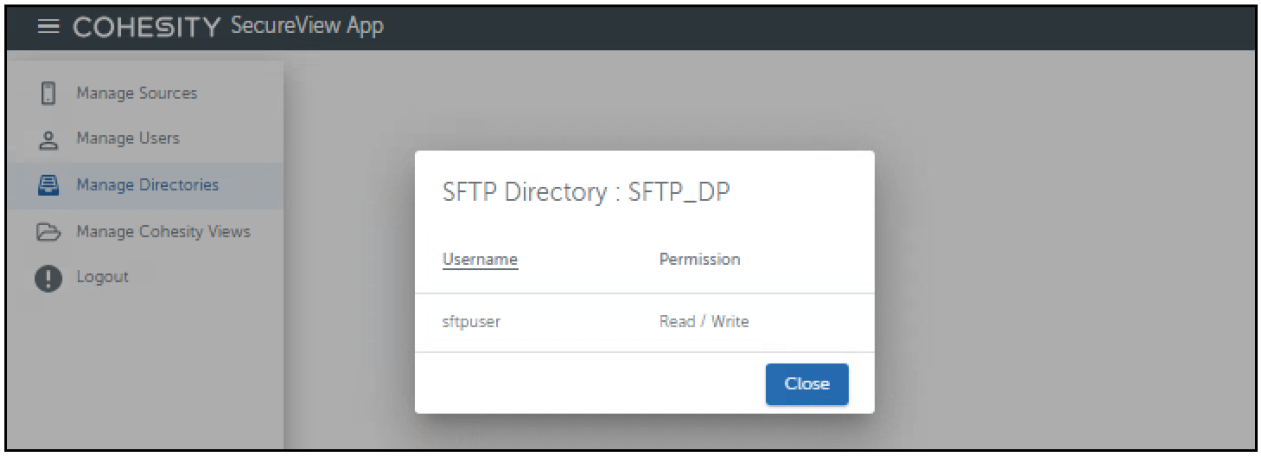


After being added to the system, the users can securely transfer files using any SFTP (Secure File Transfer Protocol) client. The port used for SFTP communications is standardized across all users, with the default setting configured to **63795**. This allows for consistent connectivity and ease of use. Additionally, you have the flexibility to assign multiple users to access the same directory. After the user creation process is complete, the new user will appear in the **Manage Users** tab, where you can view, edit, or manage their permissions and access rights accordingly.

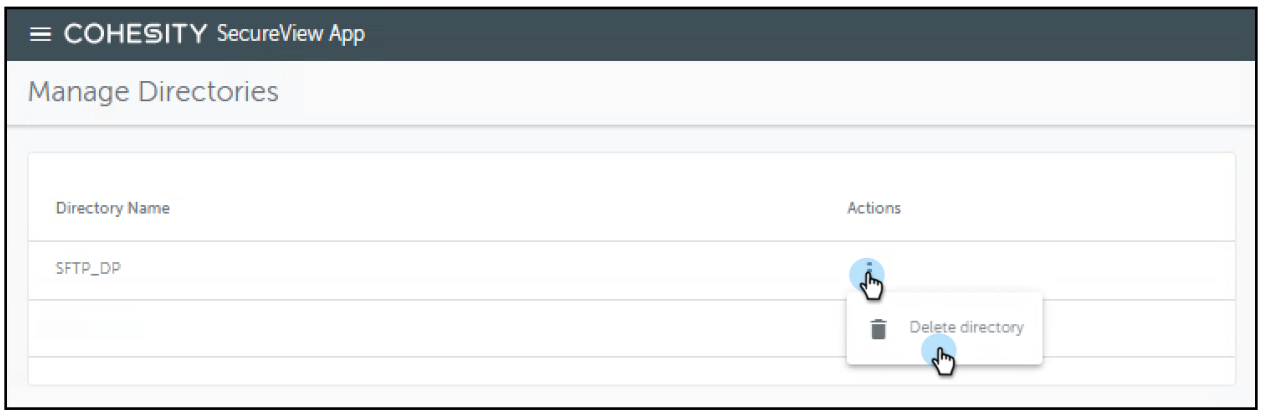


Create Directory

You can create the directory at the time of the user creation and use the one directory with multiple users. All the created directories are listed in the **Manage Directories** tab, where Directory Management allows you to view all the SFTP directories. It will list the permissions and usernames that are aligned with that directory.



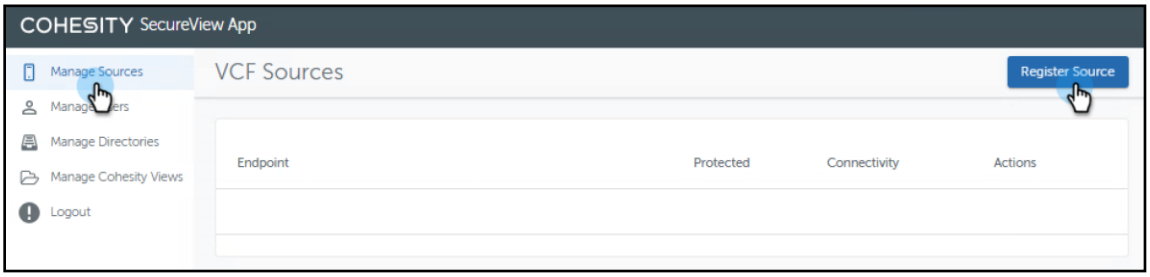
Delete Directory: Delete a directory using the delete directory action. This will also delete all users mapped to this directory and their files.



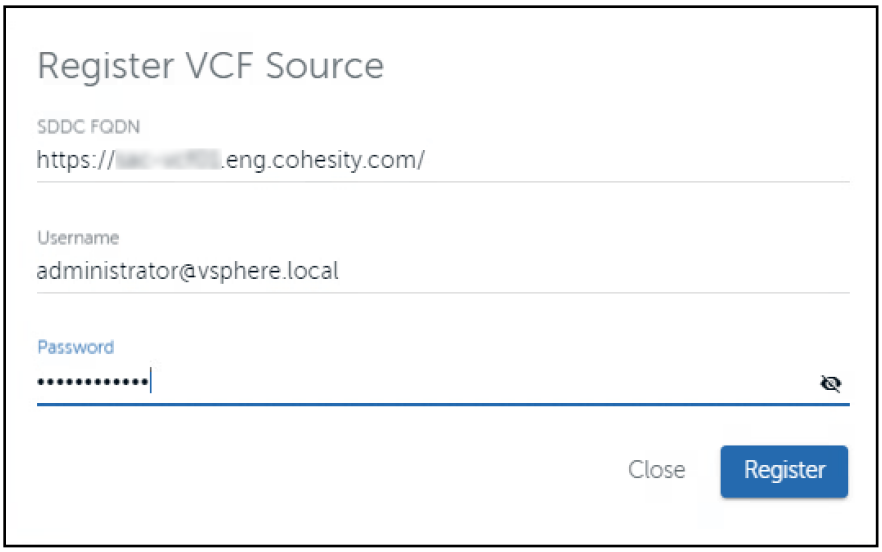
Register Sources

To protect the VCF components, including SDDC manager, NSX-T cluster, and vCenter, one must use the **File-based backup approach**, for which you need to register the sources under the **Manage Sources** tab in SecureView. You can follow the steps below to register the VCF SDDC manager.

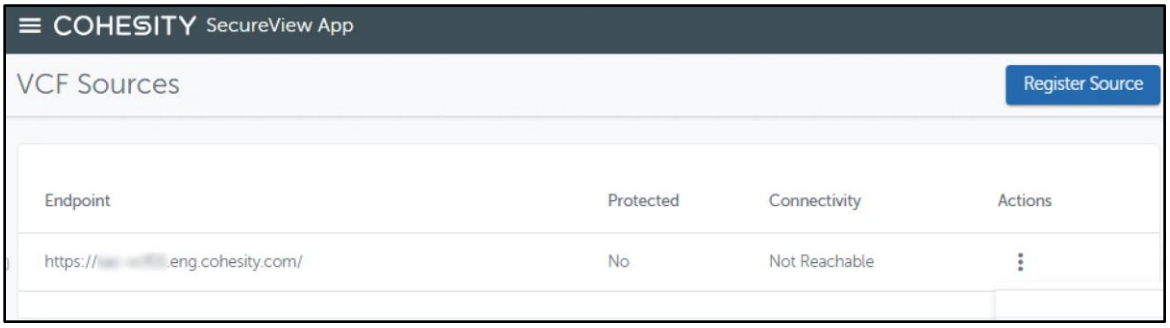
1. On the Cohesity SecureView app landing page, navigate to **Manage Sources** > **Register Source**.



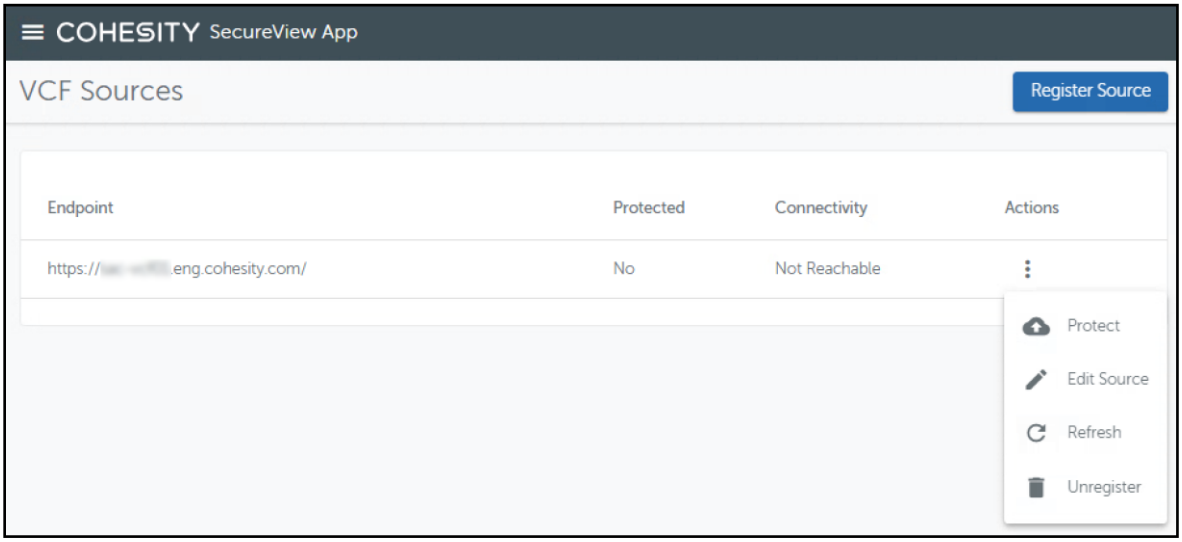
2. On the **Register VCF Source** page, enter the information below and click **Register**.



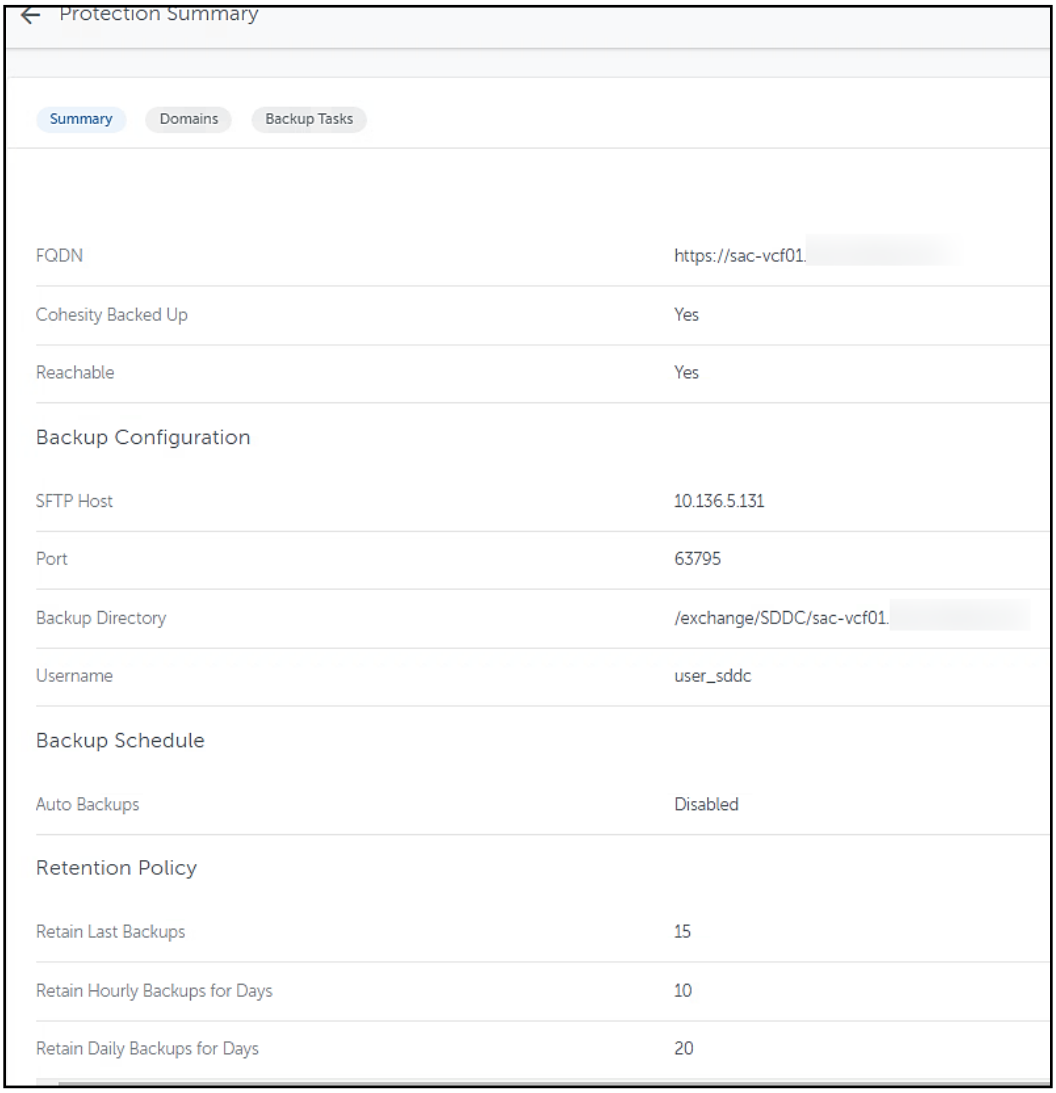
After registering the source, the user will be able to view the following fields:



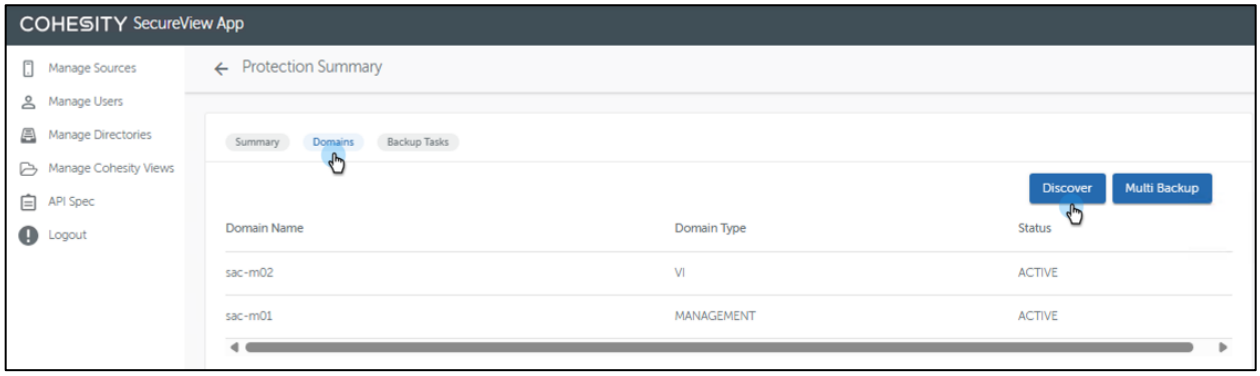
- **Endpoint** - Displays the URL of the endpoint.
- **Protected** - Displays the current protection status of the registered VCF source. This field displays **Yes** if the endpoint is protected and **No** if it is not.
- **Connectivity** - Displays the current connectivity status of the VCF source. This field displays **Reachable** when the endpoint is reachable, and user credentials are valid, and **Not Reachable** otherwise.
- **Actions** - The available actions are:
  - **Protect -** Configures backup\protection of the selected VCF source endpoint.
  - **Backup Now** - After a source has been protected, users can trigger an on-demand backup.
  - **Edit Source -** Option is only available when the endpoint connectivity status is **NOT Reachable**. This option allows you to update the endpoint URL or its credentials.
  - **Refresh -** This option allows you to refresh the endpoint details.
  - **Unregister -** Unregister the VCF source if not in use.



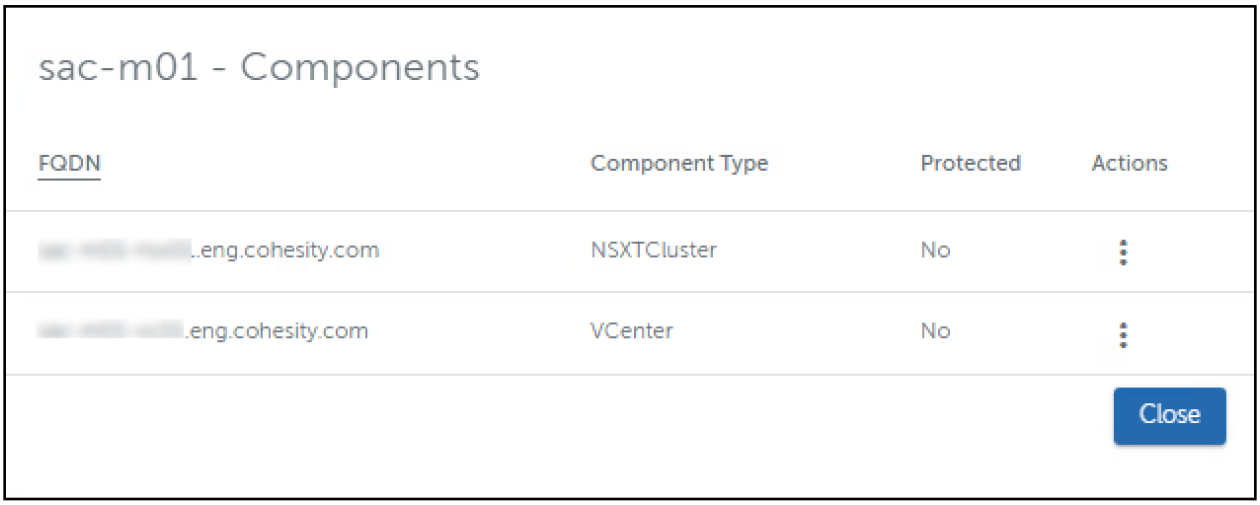
3. You can click the endpoint URL to see the summary of the VCF SDDC manager, backup configuration, and backup schedule, Domain and Backup task.



4. Navigate to the **Domain** tab and click **Discover**. It will discover all the available domains available under the VCF.



5. You can view the discovered domain's component types NSX-T Cluster and vCenter and its protection status by clicking on the Domain name.



Edit VCF Source

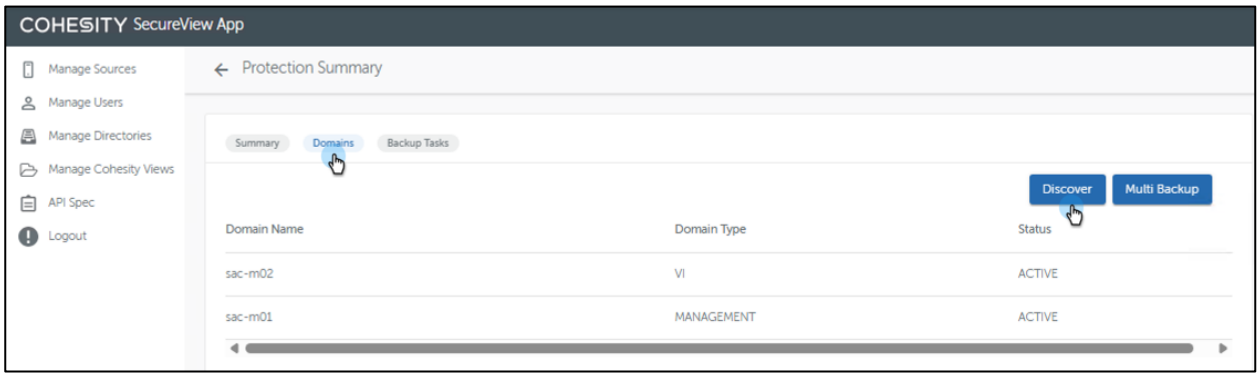
Users can follow the steps below to modify the registration details of the VCF source:

1. On the **VCF Sources** page, navigate to **Actions** > **Edit Source**.
   The **Edit VCF Source** pop-up appears.
2. Edit the username and password fields.
3. Click **Edit**.

NOTE: Edit Source Option will only be available under **VCF Sources** > **Actions** > **Edit Source** when the Source Connectivity is lost, and Connectivity status is **Not Reachable**.

Discover VCF Components

1. On the **VCF Sources** page, click the required endpoint URL.
   The **Protection Summary** page appears.
2. Click **Domains** > **Discover**.

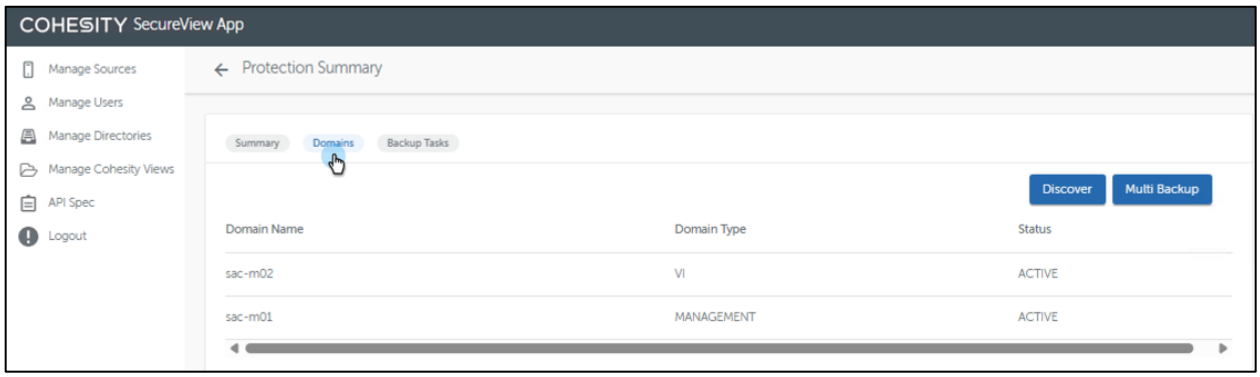


The system performs a call to the VCF endpoint and fetches all the domains configured for that VCF endpoint along with the different components such as NSX and vCenter servers, which are part of that domain.

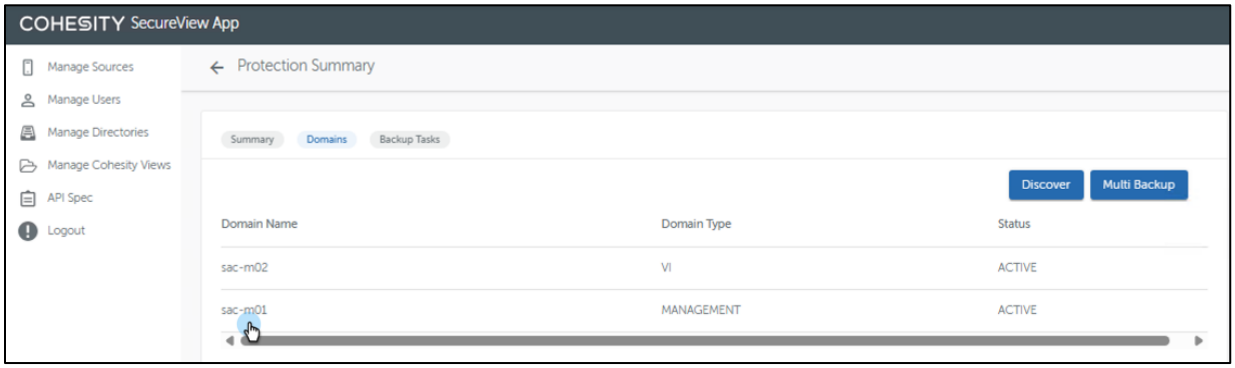
NOTE: If a new component or a domain is added to the VCF environment, then the user needs to re-discover the domains and the components to view them in the app.

View Backup Configuration of VCF Components

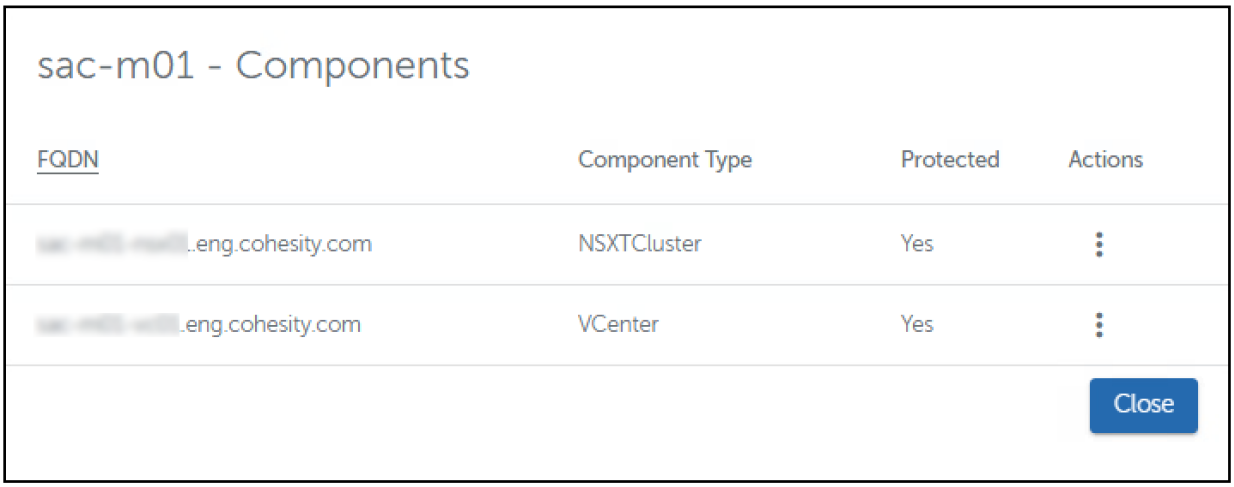
1. On the **Protection Summary** page, click **Domains**.



2. Click the domain name.



A pop-up showing the components of the selected domain appears.



The pop-up displays the following fields:

a. **FQDN** - Displays the FQDN URL of the component.

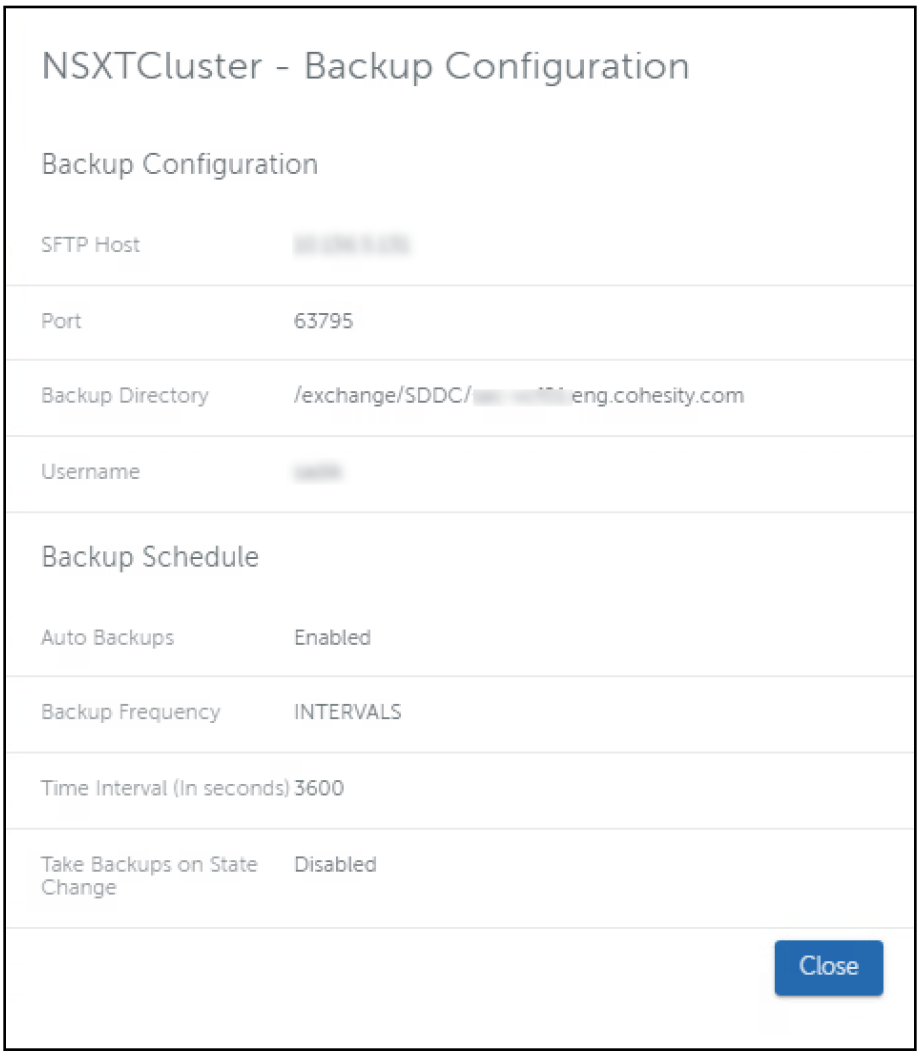
b. **Component** Type - Displays the component type. The available component types are:

- NSXTCluster
- VCenter

c. **Protected** - Displays the current component protection status.

d. **Actions** - Displays the available actions.

3. Click on the FQDN link of the required component to view its current backup configuration.

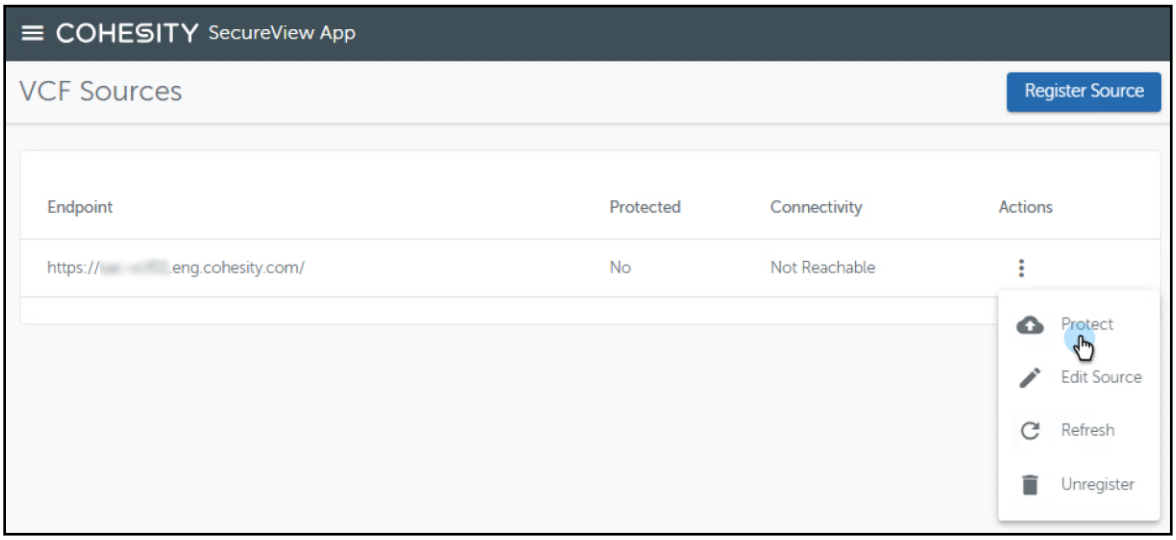


Protect VCF Components—SDDC Manager

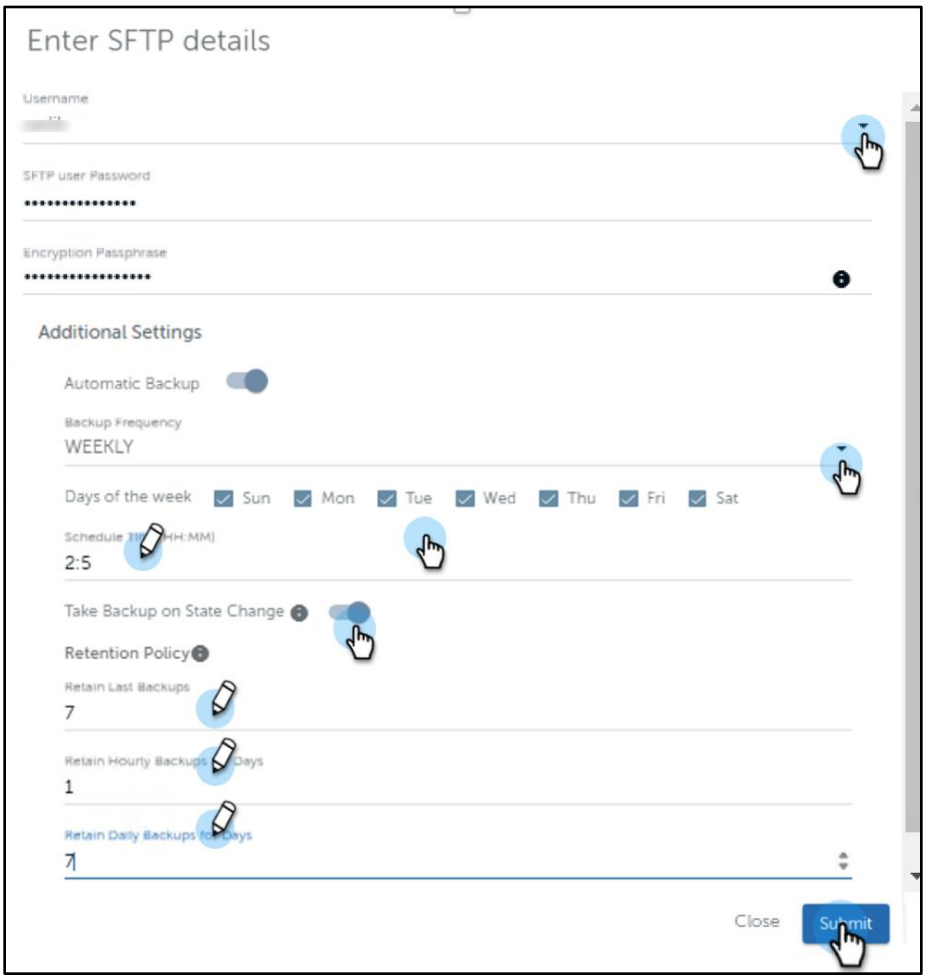
Configuring protection of the registered VCF source will protect the SDDC manager. To backup the NSXT Manager and vCenter component of VCF, it will have to be configured explicitly. Refer to the section for protecting the NSXT and vCenter.

Steps to protect the SDDC Manager.

1. On the **VCF Sources** page, navigate to **Actions** > **Protect**.



The **Enter SFTP details** pop-up appears.



2. Provide the necessary information in the following fields.
   a. **Username** - From the dropdown, select the SFTP username which you have created in the Create user section.
   b. **SFTP User Password** - Enter the SFTP user password.
   c. **Encryption Passphrase** - Enter the encryption passphrase. The encryption passphrase must satisfy the following criteria:
      - Twelve or more characters
      - At least one uppercase letter
      - At least two digits
      - At least one special character

NOTE:

- The encryption passphrase is mapped to the backup file and is required during recovery. Hence, it needs to be stored in a secure location.
- Editing the passphrase will not update the configured passphrase for previously backed-up files.
- In case you are editing the passphrase, you must store the passphrase in a secure location separate from the backup files and from the Cloud Foundation environment.

d. **Additional Settings**

- **Automatic Backup** - By default, the automatic backup toggle is disabled. To enable automatic backups, turn on this toggle switch. If the toggle is not enabled, you must perform an on-demand backup of the source to trigger the backup.
  Once the automatic backup is enabled, the following settings become available:

  a. **Backup Frequency** - From the drop-down, select the required frequency. The available options are:

     i. **Hourly** - If you select this frequency, the following fields appear:

        1. **Schedule time (minutes after the hour)** - Enter the minute of the hour at which the backup runs.
        2. **Take Backup on State Change** - By default the backup is disabled. Enable the toggle to take the backups on stage change.

     ii. **Weekly** - If you select this frequency, the following fields appear:

        1. **Days of the Week** - Select the required days of the week.
        2. **Schedule Time** - Enter the required time at which the weekly backup runs.

     iii. **Take Backup on State Change** - By default the backup is disabled. Enable the toggle to take the backups on stage change.

  NOTE: You must configure the backup jobs for the SDDC Manager instance and all vCenter Server instances in the vCenter Single Sign-On domain to start within the same 5-minute window.

- **Retention policy** - *(Applies to SDDC manager backups only)* The backup retention policy is designed to retain as many latest backups as possible and to retain the optimal number of backups for a long period of time. For more information, see the notes below.
  - **Retain Last Backups** - Retains the most recent backups defined.
  - **Retain Hourly Backups for Days** - Retains the hourly backups for days defined.
  - **Retain Daily Backups for Days** - Retains the daily backups for days defined.

3. Click **Submit** to submit the SFTP details for the source protection or click **Close** to exit the pop-up.

NOTE:

- SDDC Manager's backup retention policy is designed to retain a given number of most recent backups, hourly backups (only the latest backup is retained in an hour) for a given number of days, and daily backups (only the latest backup is retained per day) for a given number of days. For example, as per the policy,

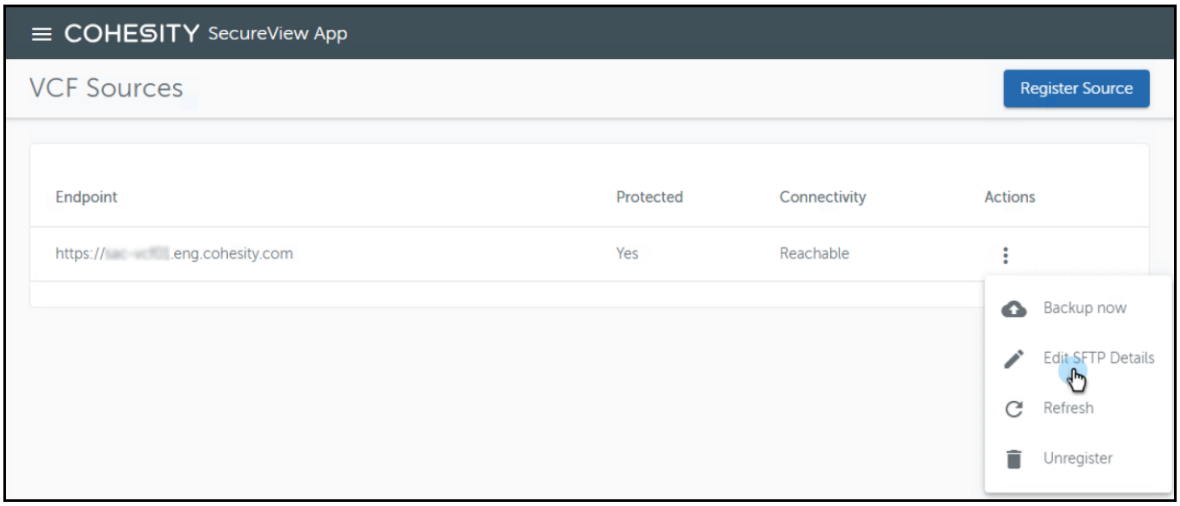
  {"numberOfMostRecentBackups" : 10, "numberOfDaysOfHourlyBackups" : 2, "numberOfDaysOfDailyBackups" : 15}

  The very recent 10 backups will be retained, and on top of that hourly backups will be retained for the last 2 days, and on top of that daily backups will be retained for the last 15 days.
- Configuring the VCF backup from the Endpoint URL will only backup the SDDC manager and NSX-T components. The vCenter backup will have to be configured explicitly. Refer to the section on protecting the vCenter.

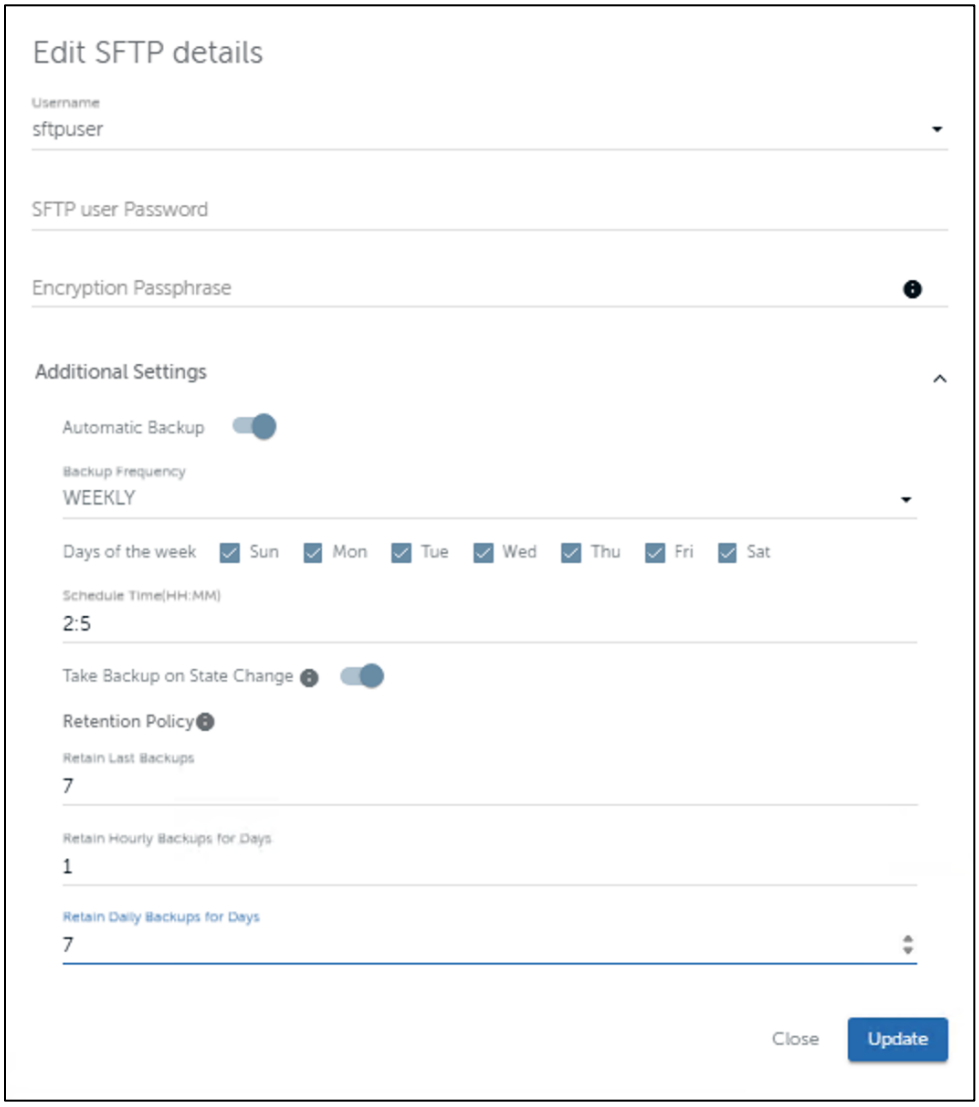
Modify SDDC Manager Backup Configuration

Once the SDDC Manager is protected, you have the provision to edit the SFTP details of the SDDC Manager.

1. On the **VCF Sources** page, navigate to **Actions** > **Edit SFTP Details**.



The **Edit SFTP Details** pop-up appears.

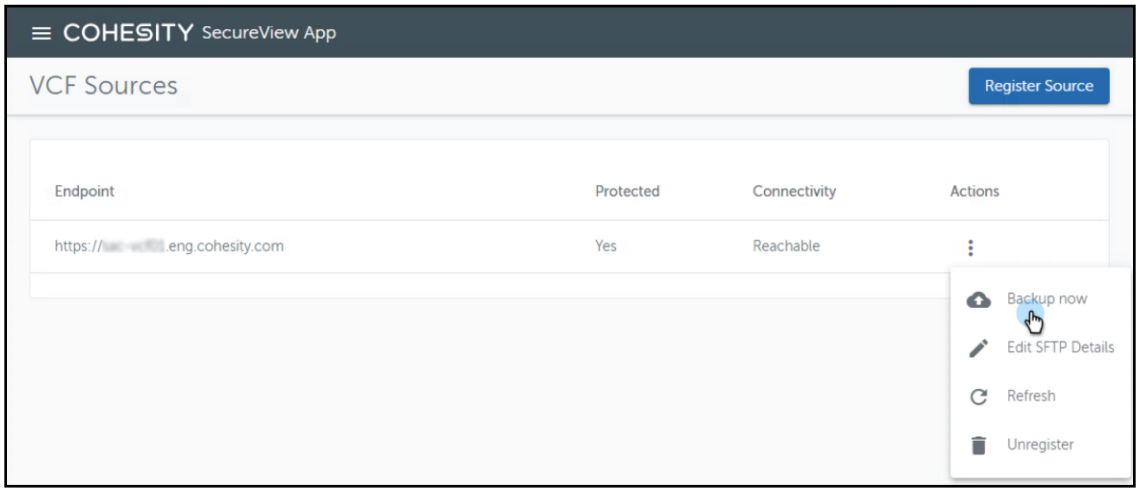


2. Update the required information in the necessary fields and click **Update** to update the SFTP details for the source protection or click **Close** to exit the pop-up.

Backup Now — On-demand Backup

Once the protection is enabled on the registered VCF source, you can perform On-Demand backup as needed. The retention policy defined in the source applies to the automatic as well as on-demand backup runs.

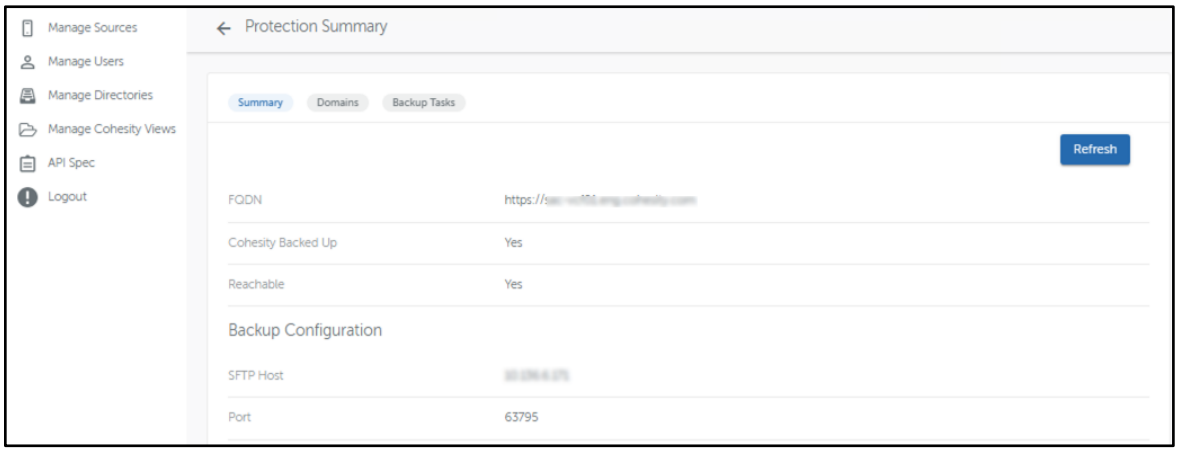
To perform the on-demand backup, on the **VCF Sources** page, navigate to **Actions** > **Backup Now**. The system creates an on-demand backup run for the source.



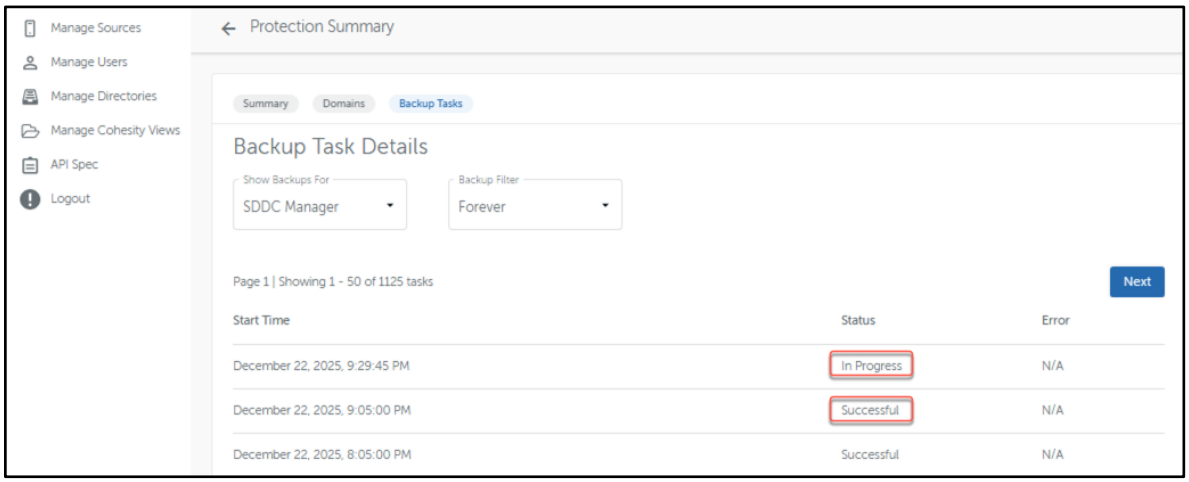
View Status of Backup Run

The Backup Tasks page displays the details of on-demand and scheduled backup runs that are currently running or completed for SDDC, NSXT and vCenter.

1. On the VCF Sources page, click the endpoint URL.
   The **Protection Summary** page appears.



2. Go to **Backup Tasks**.
   The **Backup Task Details** page appears.



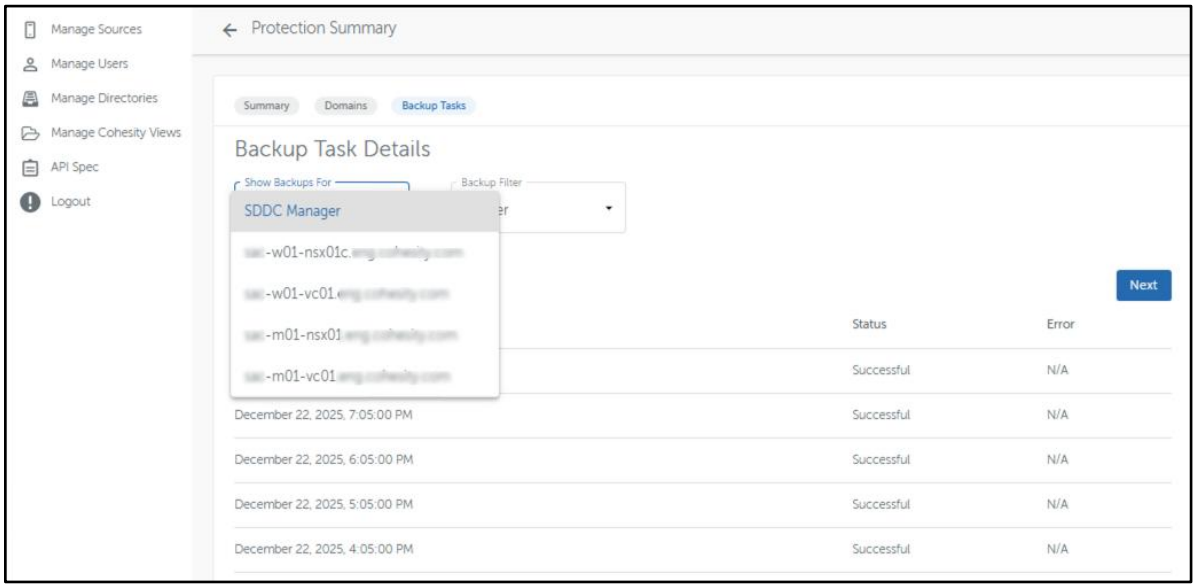
   This page displays the following fields:

   a. **Start Time** - Displays the start time of the backup run.

   b. **Status** - Displays the current status (In Progress, Successful or Failed) of the backup run.

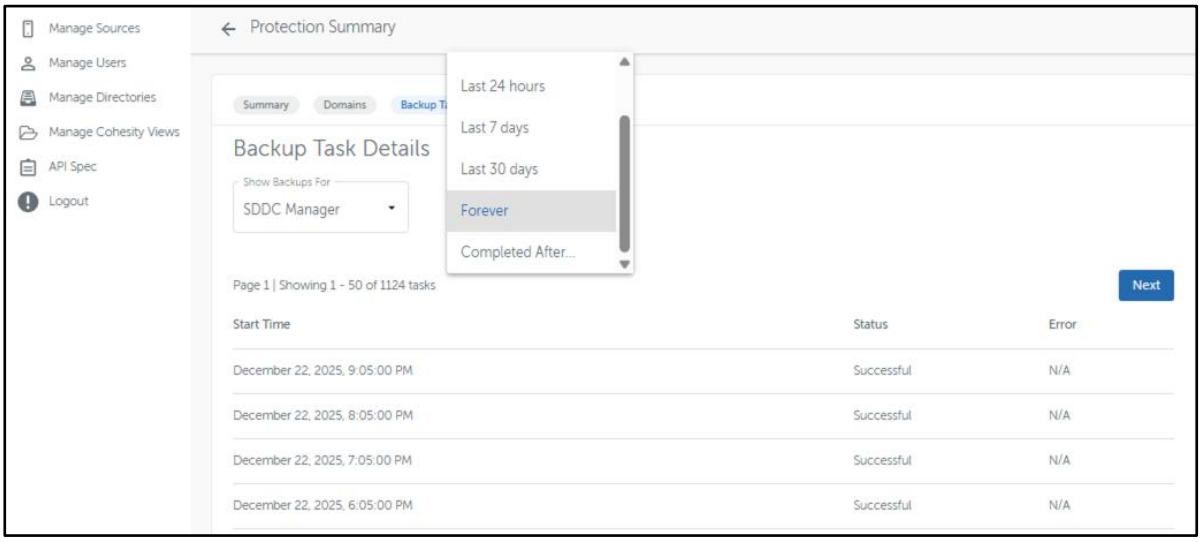
   c. **Error** - Displays any error message encountered during the backup run.

3. Use the **Show Backup For** drop down menu to view the backup task for a VCF component (SDDC Manager, NSXT or vCenter)



4. Use the **Backup Filter** drop-down menu to select the SDDC Manager backup task history you wish to see.

> **NOTE**: The Backup Filter option is only applicable to the SDDC Manager. This is due to the Broadcom VMWare API limitations.

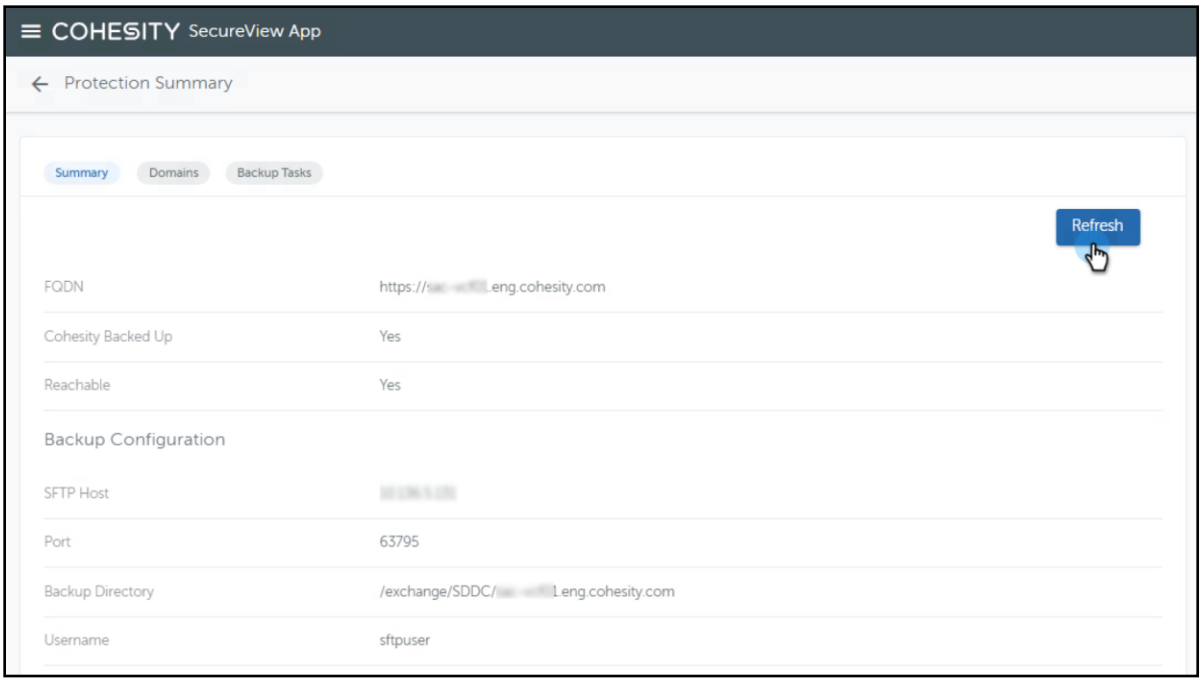


Refresh Backup Summary

The user can refresh the backup summary to obtain the current backup configuration details of the VCF source. If the backup configuration of the VCF source has been manually modified, the Protection Summary page does not display the updated details until the refresh is performed.

Perform the following steps to refresh the backup summary:

1. On the **VCF Sources** page, click the required endpoint URL.
   The **Protection Summary** page appears. This page displays the current backup configuration details of the VCF source.
2. Click **Refresh** to obtain the current backup configuration details of the VCF source.



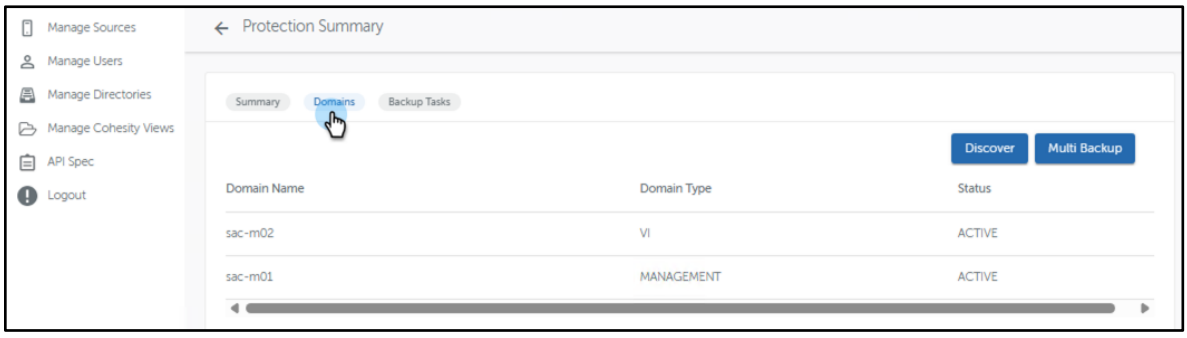
Protect VCF Components—NSXT Cluster

NSXT cluster backup is not configured by default. To configure the NSXT cluster backup, follow the steps below. Please note that when the on-demand backup of the source run is executed, it backs up both the components (SDDC Manager and NSXT Cluster). However, the following are the exceptions to keep in mind.

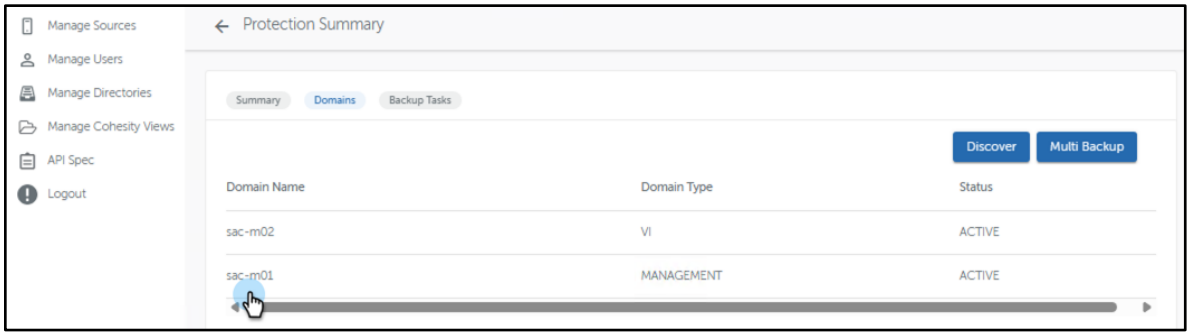
- The Backup Frequency is defined in Intervals (time interval in seconds). The default is 3600 seconds.
- The retention policy configured in the registered VCF source does not apply to NSX-T backups. It only applies to the SDDC manager backups.
- To set up retention on NSXTCluster backups, refer to the section.

Steps to configure the NSX-T Cluster component backup.

1. On the **Protection Summary** page, click **Domain**.



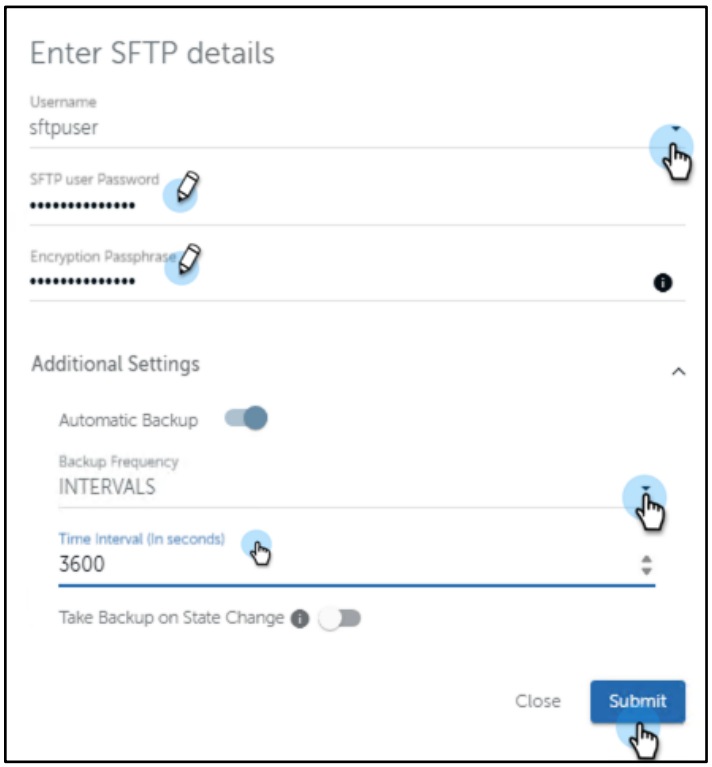
2. Click the domain name.



A pop-up showing the components of the selected domain appears.

3. Under Component Type "**NSXTCluster**", select **Actions > Protect**.

4. Enter the required information in the displayed fields, click **Submit** to update the SFTP details for component protection.



a. **Username** - From the dropdown, select the SFTP username.

b. **SFTP user password** - Enter the SFTP user password.

c. **Encryption Passphrase** - Enter the encryption passphrase.

d. **Additional Settings**

Automatic Backup - By default, the automatic backup toggle is disabled. To enable automatic backups, turn on the toggle. If the toggle is not enabled, you must perform the on-demand backup of the component to trigger the backup.
Once the automatic backup is enabled, the following settings become available:

1. **Backup Frequency** - From the drop-down, select the required frequency. The available options are:
    a. **Intervals** - Select this frequency, the following fields appear:
        i. **Time Interval (in seconds)** - Enter the time interval between two backups.
    b. **Weekly** - If you select this frequency, the following fields appear:
        i. **Days of the week** - Select the required days of the week.
        ii. **Schedule Time** - Enter the required time at which the weekly backup runs.
    c. **Take Backup on State Change** - By default the backup is disabled.

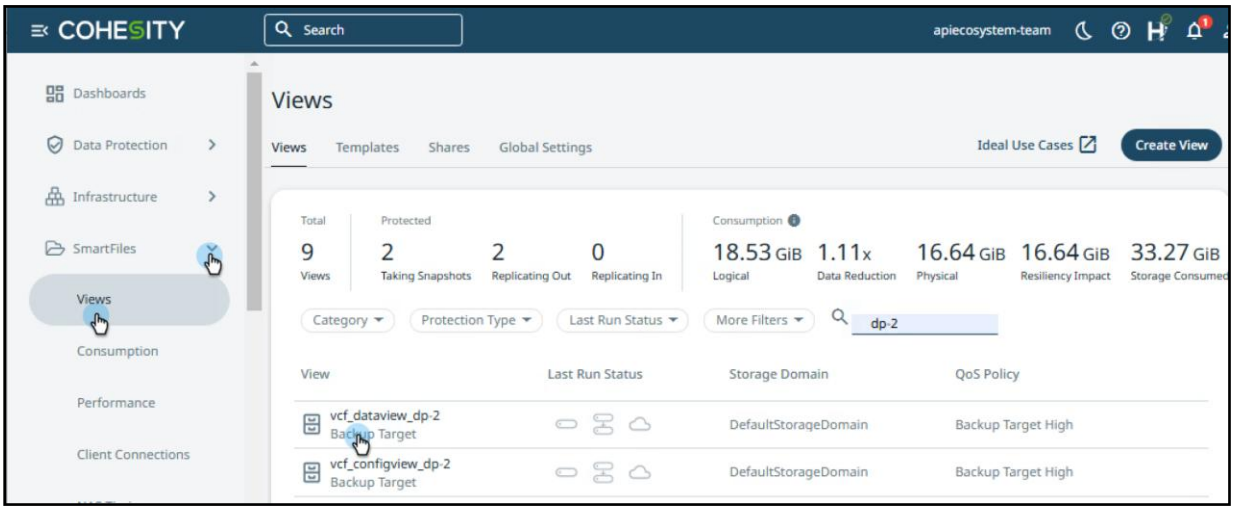
Setup Data View's Storage Lifecycle Management Rules for NSXTCluster Backup Retention

Due to VMware API limitations, the retention policy configured in the registered VCF source backup configuration does not apply to the NSX-T Cluster protection. It only applies to the SDDC manager backups.

To ensure that you maintain a retention period on the NSX-T Cluster backups, you need to configure Storage Lifecycle Management rule on the SmartFiles view (SecureView App's Data View).

Steps to configure Lifecycle Management on the Data View.

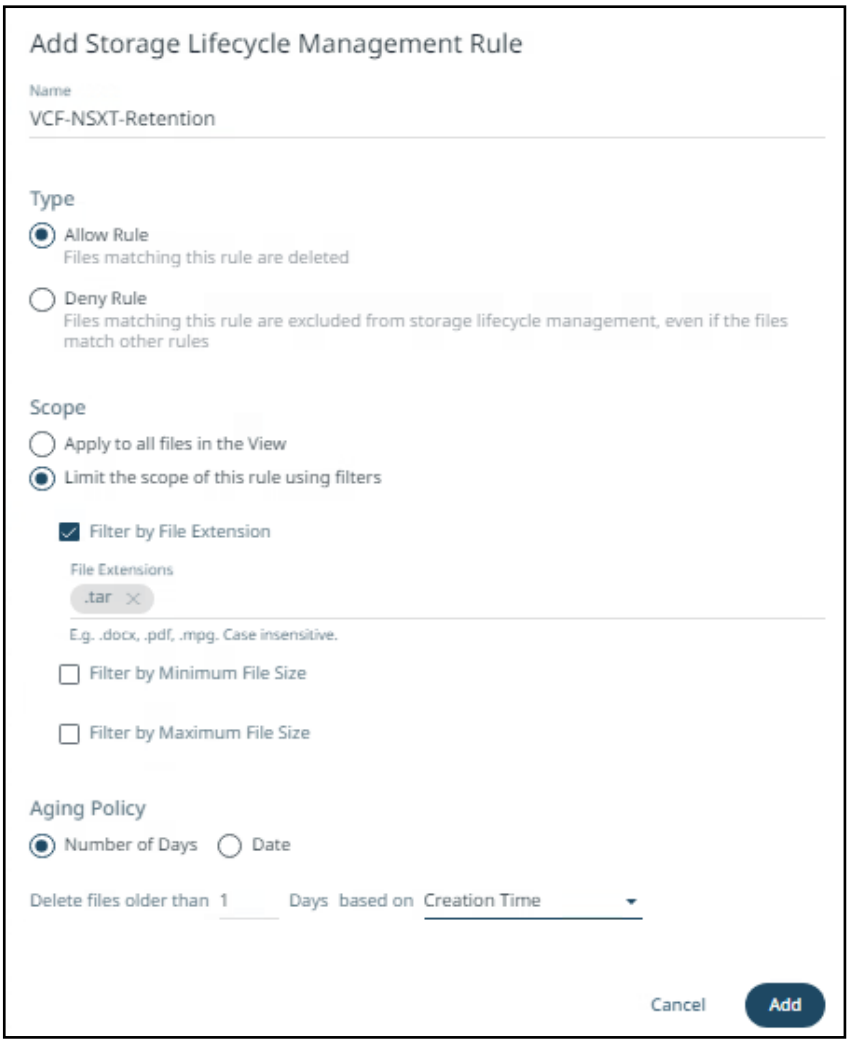
1. Browse **Cohesity UI > SmartFiles > Views** and locate the data view.



2. Click ⋮ and select **Edit**.
3. In the Edit View window, click **Add Rule** under **Storage Lifecycle Management Rules**.
4. In the Add Storage Lifecycle Management Rules window, input the following details.

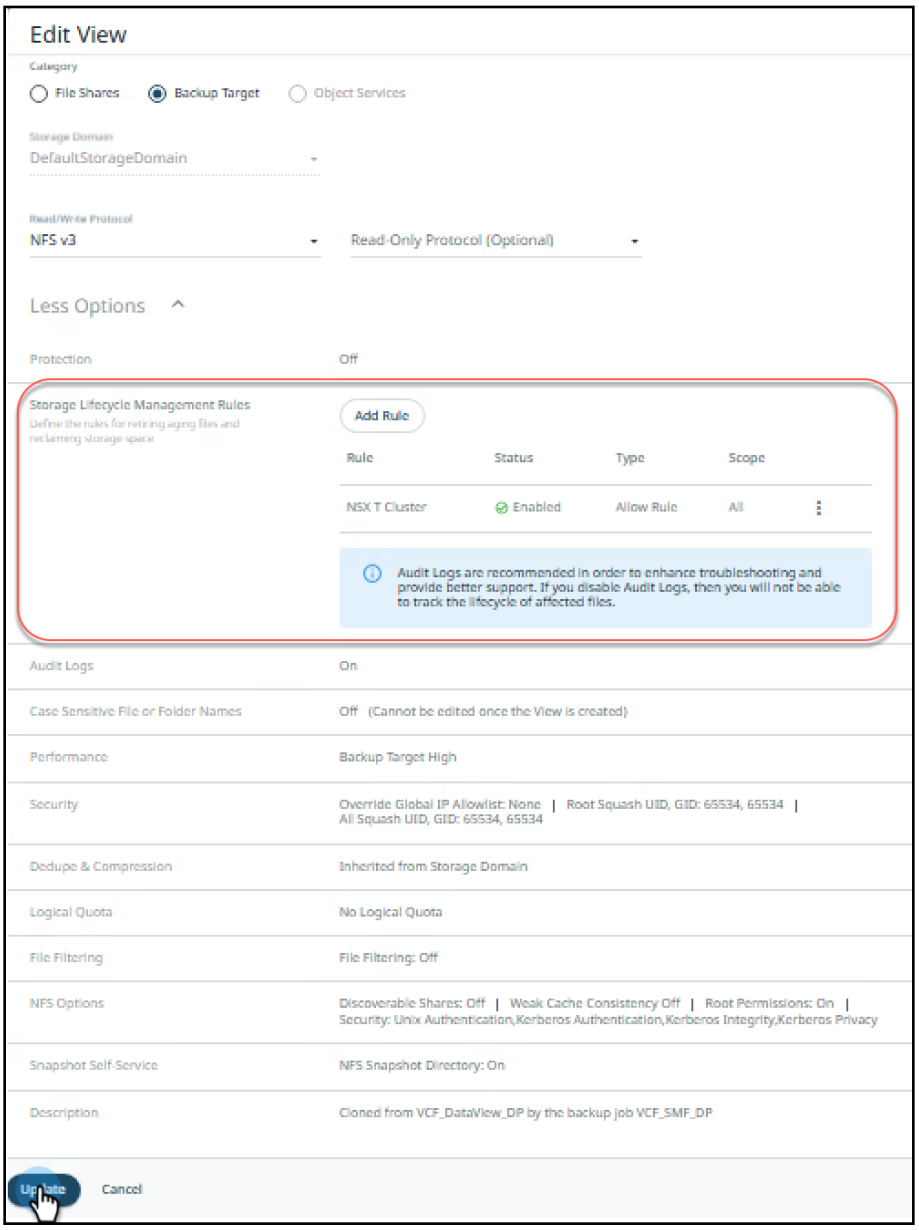
> **NOTE**: The NSXTCluster backup files are of .tar extension.

   - **Name**—Enter a name for the rule.
   - **Type**—Select **Allow Rule.**
   - **Scope**—Select **Limit the scope of this rule using filters.**
   - Select **Filter by File Extension** and add **.tar** as the File Extension.
   - **Aging Policy**—Select **Number of Days.**
   - In "**Delete files older than"** field, define the number days to retain the .tar files based on **"Creation Time".**



5. Click the **Add** button to add the rule to the view.

6. Click the **Update** button to apply the changes.

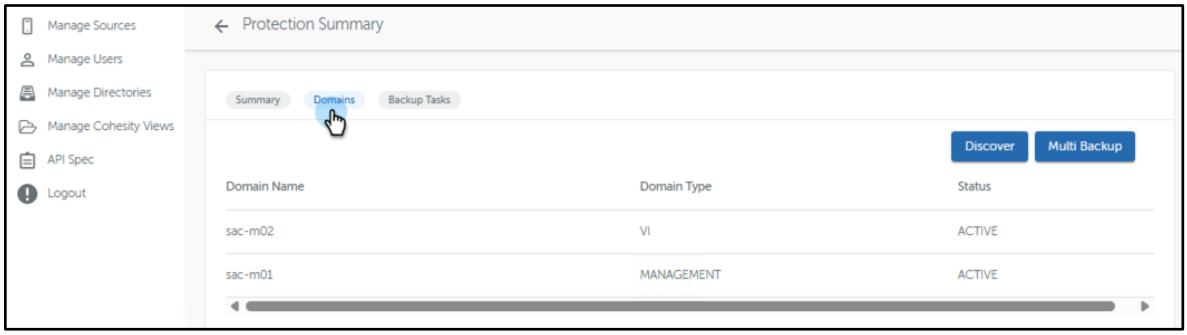


NOTE: Refer to Storage Lifecycle Management Rules in product documentation for more information.

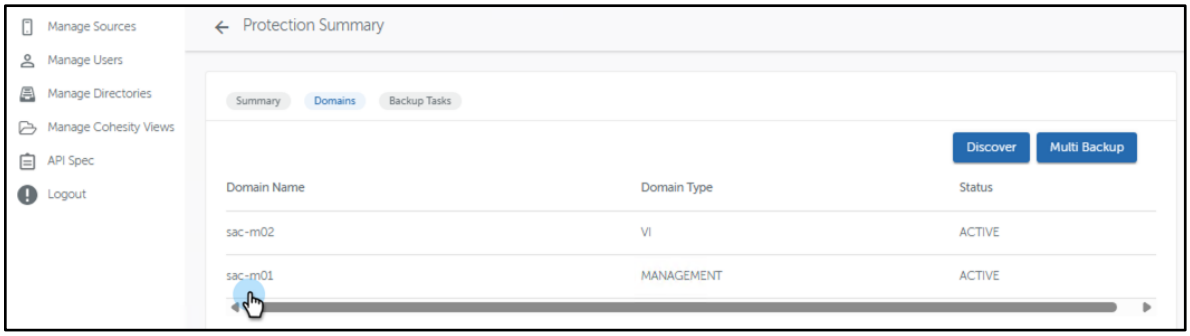
Protect VCF Components—vCenter

The 3rd component of VCF—the vCenter, does not inherit the backup configuration from the registered VCF source. You need to explicitly configure protection of the vCenter component by following the steps below.

1. On the **Protection Summary** page, click **Domains**.



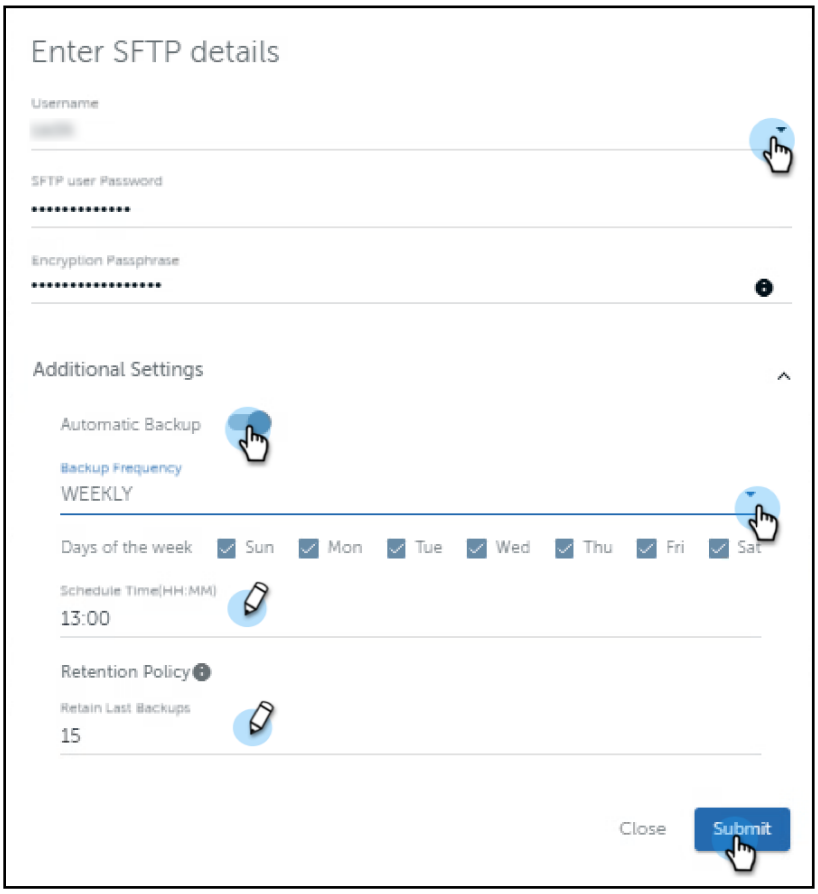
2. Click the domain name.



A pop-up showing the components of the selected domain appears.

3. Under Component Type **“VCenter”** select option **Actions** > **Protect.**

4. Provide the necessary information in the following fields.



a. **Username** - From the dropdown, select the SFTP username.

b. **SFTP user password** - Enter the SFTP user password.

c. **Encryption Passphrase** - Enter the encryption passphrase.

d. **Additional Settings.**

Automatic Backup - By default, the automatic backup toggle is disabled. To enable automatic backups, turn on the toggle. If the toggle is not enabled, you have to perform the on-demand backup of the component to trigger the backup.
Once the automatic backup is enabled, the following settings become available:

1. **Backup Frequency** - From the drop-down, select the frequency. The only available option is:
    a. **Weekly** - Select this frequency, the following fields appear:
        i. **Days of the week** - Select the required days in a week.
        ii. **Schedule Time** - Enter the required time at which the weekly backup runs.

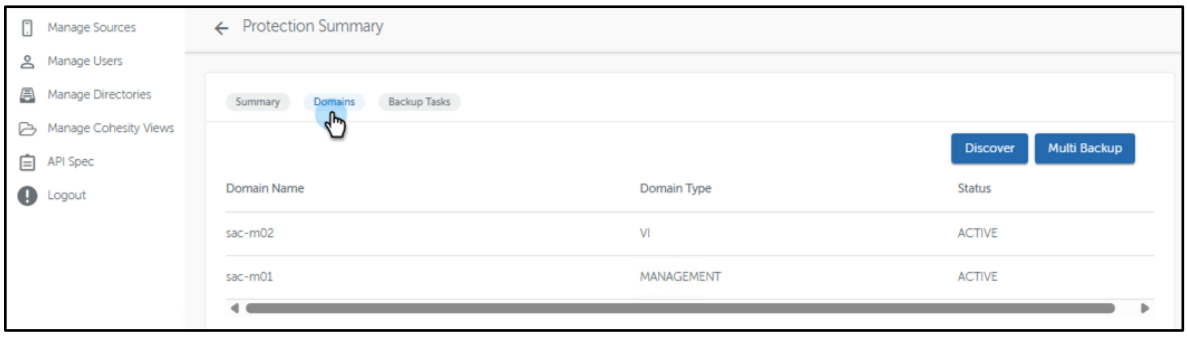
NOTE: You must configure the backup jobs for the SDDC Manager instance and all vCenter Server instances in the vCenter Single Sign-On domain to start within the same 5-minute window.

5. Click **Submit** to submit the SFTP details for the component protection or click **Close** to exit the pop-up.

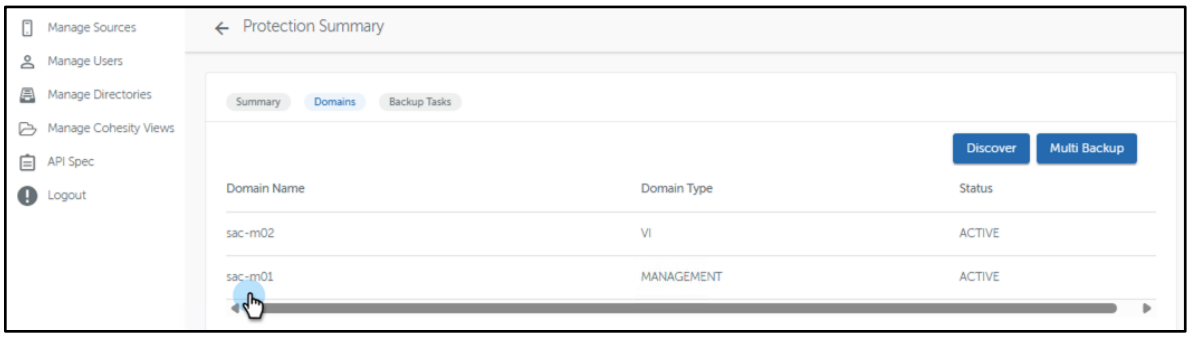
Edit SFTP Details of Component

Once the component is protected, you have the provision to edit the SFTP details of the component.

1. On the **Protection Summary** page, click **Domains**.

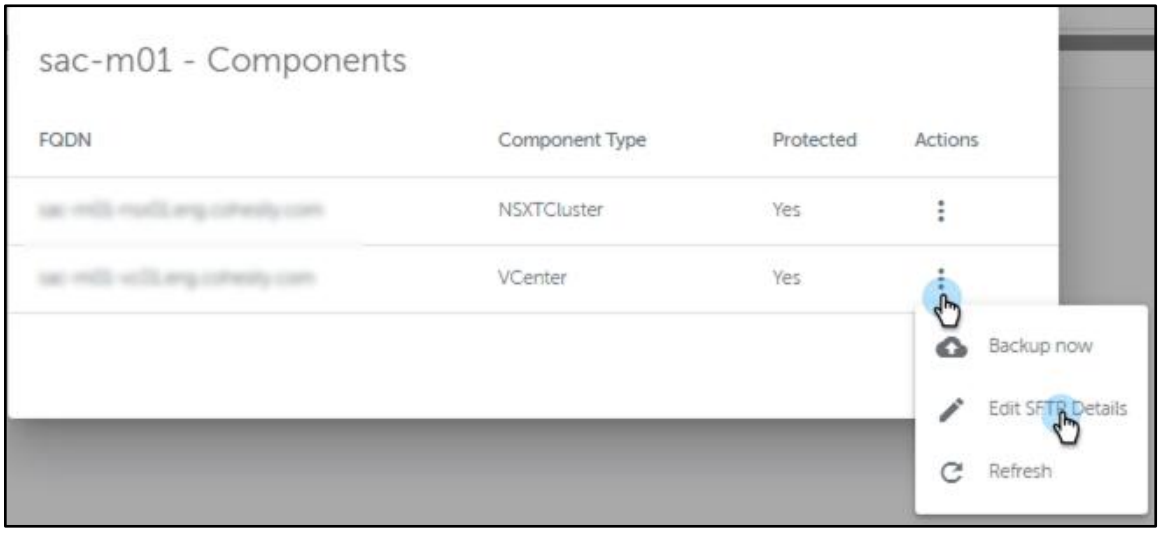


2. Click the domain name.



A pop-up showing the components of the selected domain appears.

3. Under Component Type **"VCenter"** select option **Actions** > **Edit SFTP Details**
   The **Edit SFTP Details** pop-up appears.

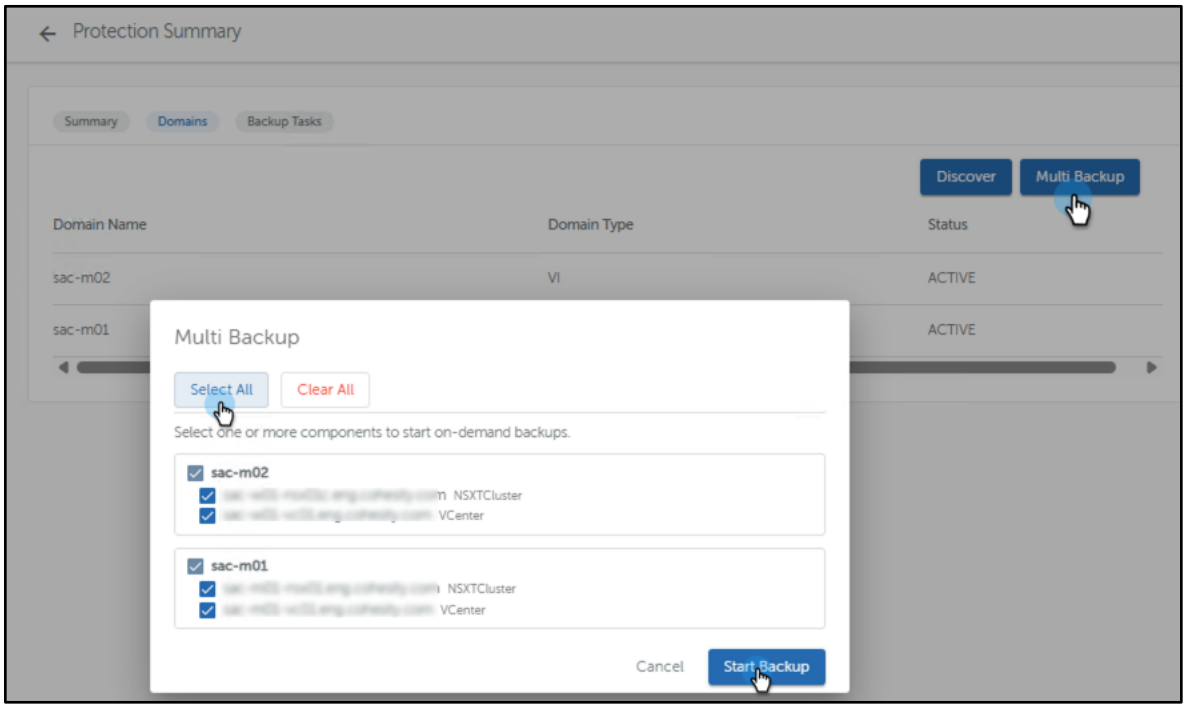


4. Update the required information in the necessary fields, click **Update** to update the SFTP details for component protection, or click **Close** to exit the pop-up.

On-demand Backup

On-demand backups on components can be executed using the **Multi Backup** option. This option allows you to perform On-demand backup of all components across all available domains or on-demand backup of selective components.

1. On the **Protection Summary** page, click **Domains**.
2. Click **Multi Backup** button.
3. Click **Select All** button to perform on-demand backup of all components across all available domains. Or select the individual components for selective backup. Then click **Start Backup**.



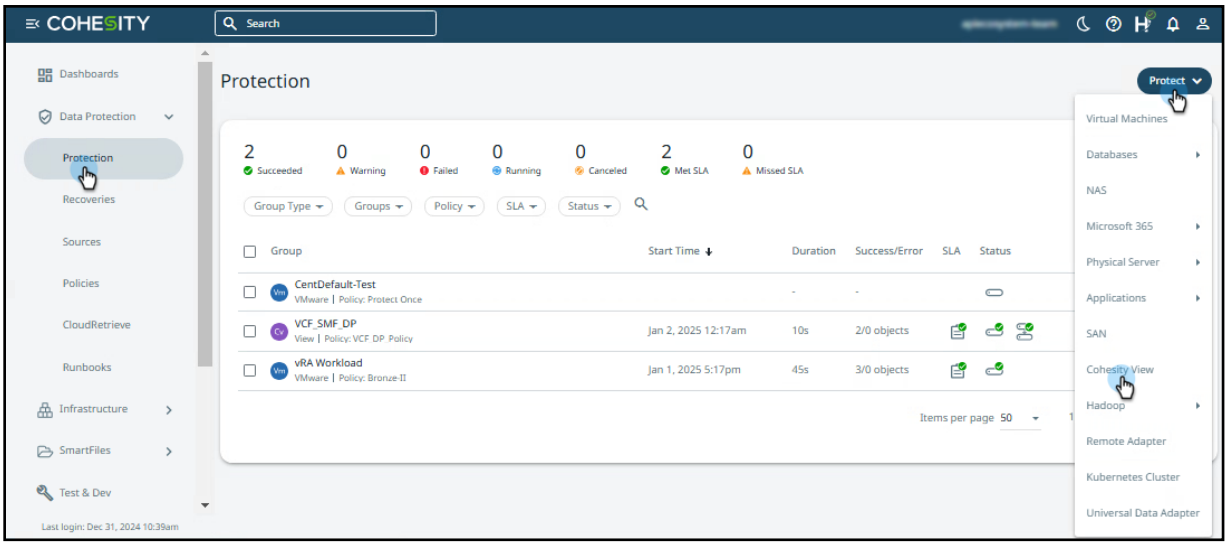
VCF SmartFiles Views

The VCF backups are stored in the Cohesity SmartFiles Views and it is important to protect these SmartFiles Views to safeguard against loss of primary Cohesity cluster in an unlikely event such as Disaster. You can protect these views in a Protection Group and then replicate to a remote Cohesity cluster.

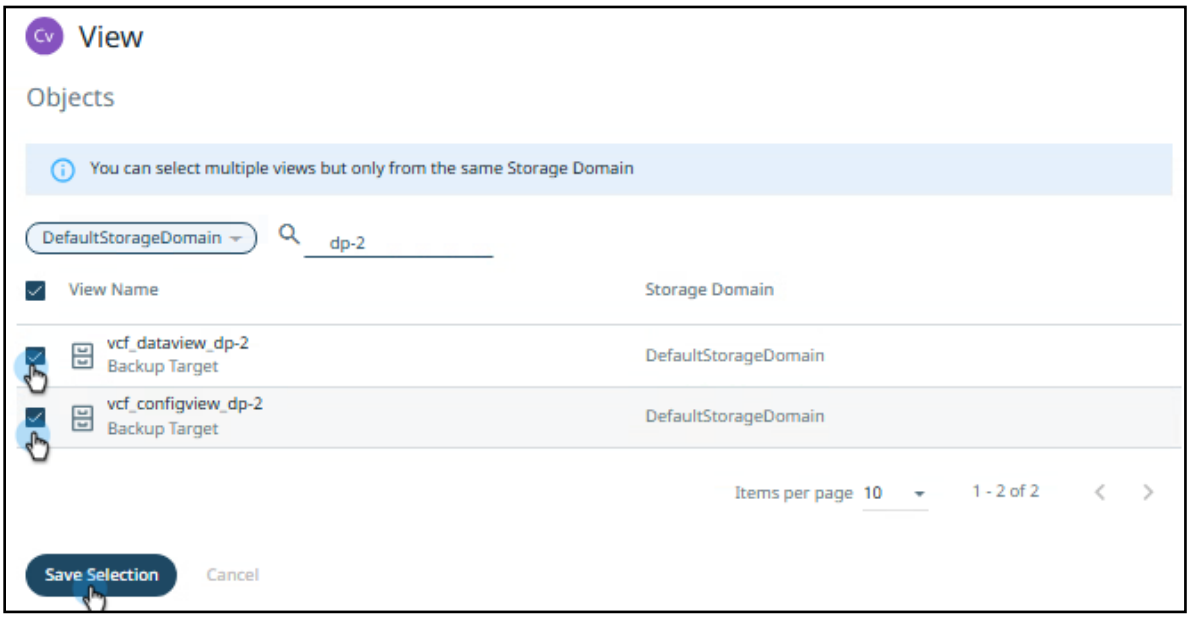
Protect SmartFiles Views

NOTE: Refer to Protect Cohesity Views and Add or Edit a Protection Group for a View in product documentation for more information.

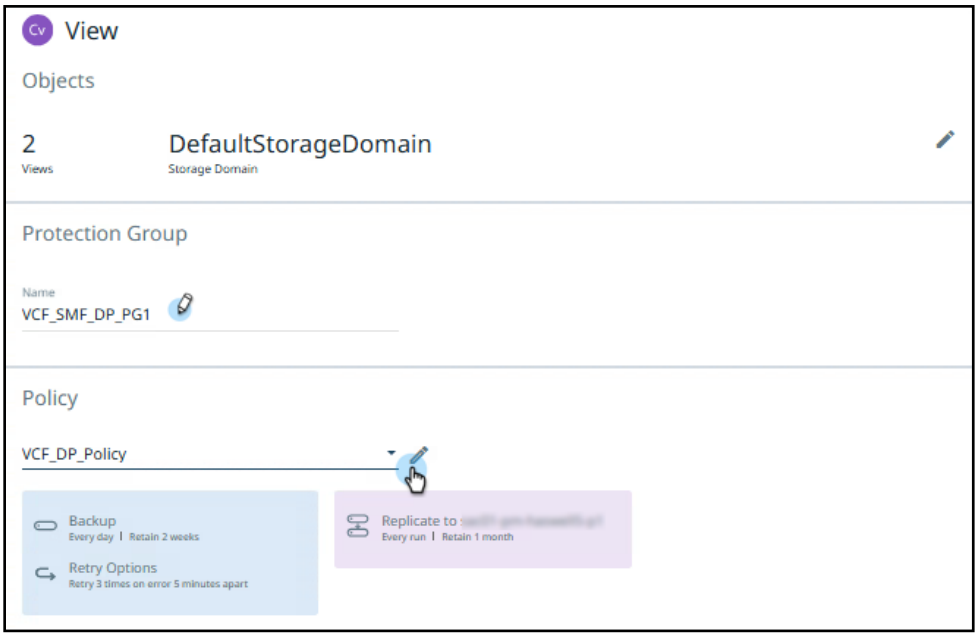
1. Navigate to **Data Protection** > **Protection** > **Protect** > **Cohesity View**.



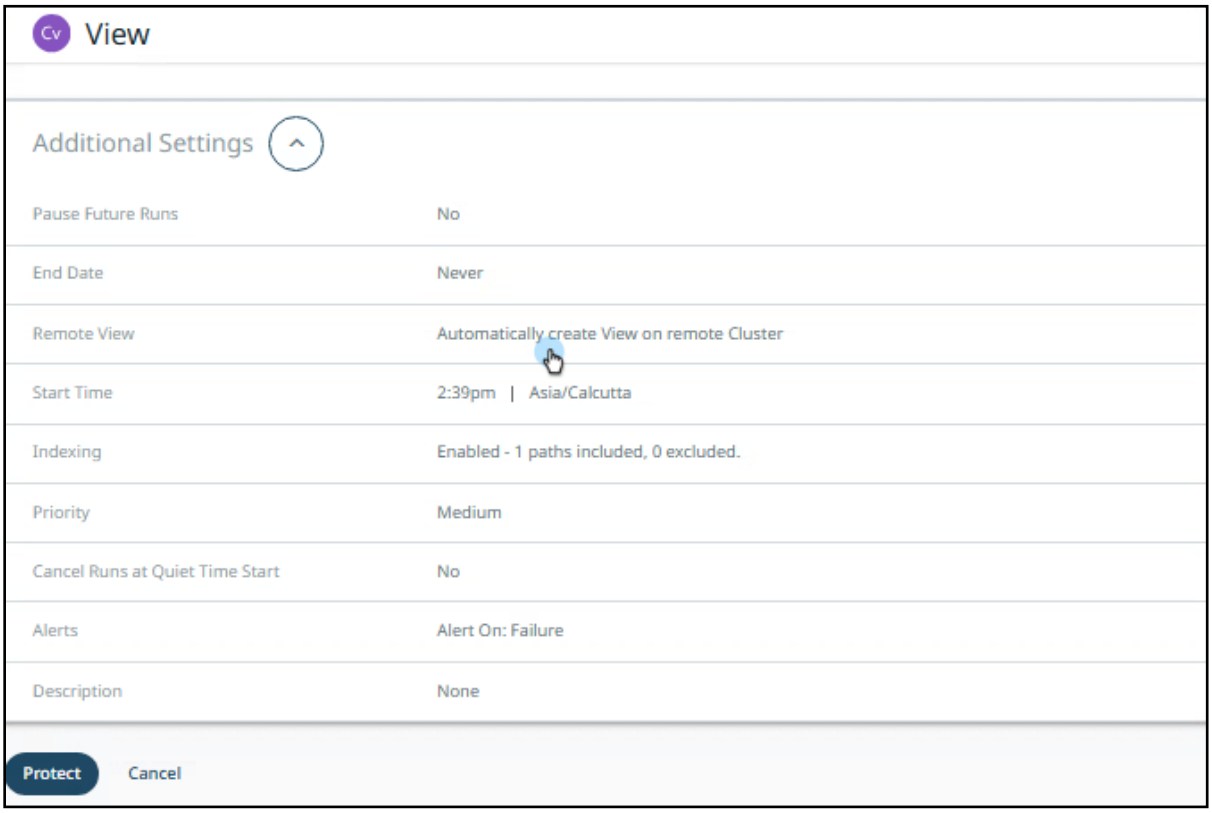
2. Select both the Config and Data View for protection. Click **Save Selection**.



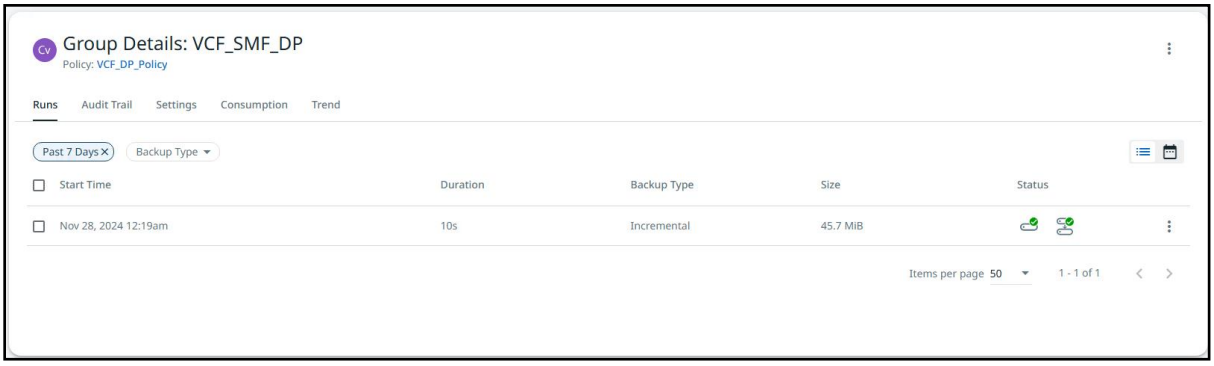
3. Provide a name for the Protection Group.
4. Select the pre-configured policy or create a new one with the replication setup of the remote cluster. Refer to Create or Edit a Standard Policy for more information.



5. Review the option **Remote View** under the **Additional Settings**. This option is available only if the policy you selected has replication enabled.



6. Click **Protect**. It will start the protection run of the SmartFiles Views. You can verify the protection and replication from the status tab.



SecureView App Recovery

Cohesity supports the recovery operation of the SecureView App. Following are the likely scenarios of SecureView App failure.

Scenario 1 — SecureView App fails and SmartFiles Views are available on the primary Cohesity cluster.

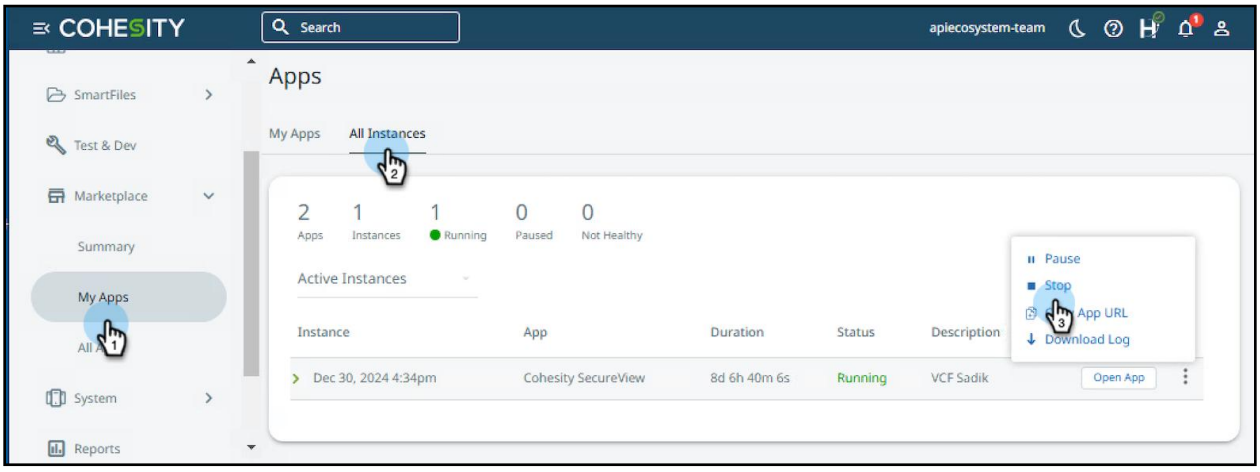
In this scenario follow the below steps

1. Fix the environmental errors if any.
2. Initiate a new SecureView App run on the primary Cohesity cluster by following installation steps section.
3. In the Run Cohesity SecureView App run window, provide the existing SmartFiles Views from the primary cluster that were used earlier.

Scenario 2 — SmartFiles views are unavailable, or some backup data is manually deleted (intentionally or accidentally) from the views. The SecureView App is intact and running.

In this scenario, follow the steps below.

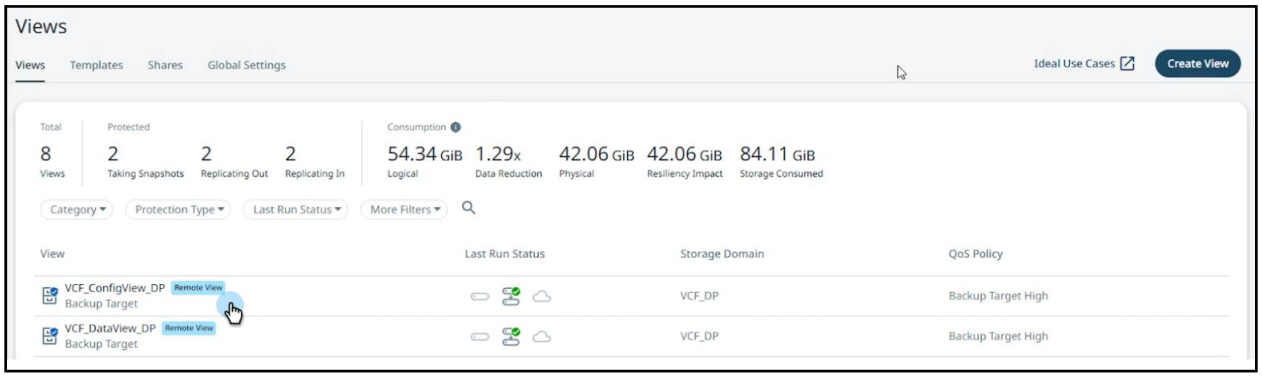
1. Terminate the existing SecureView running instance using the **Stop** action.



2. Identify a suitable and non-impacted SmartFiles view backup snapshot (local) on the primary Cohesity cluster.
3. Clone the Views (Config and Data view) using the identified backup snapshot on the primary Cohesity cluster. Refer to Clone a View From a Snapshot for more information.
4. Initiate a new SecureView App run on the target Cohesity cluster by following the installation steps section.
5. In the Run Cohesity SecureView App window, provide details of the cloned SmartFiles Views from step1.

Scenario 3 — Disaster Recovery — SecureView App fails and SmartFiles Views are unavailable on the primary Cohesity cluster.

NOTE: The SmartFiles Views are protected and replicated to the remote cluster. The replicated views are listed on the target cluster as the “Remote View.”



In this scenario, follow the steps below:

1. Clone the replicated Views on the target Cohesity cluster. Refer to Clone a View From a Snapshot for more information.
2. Initiate a new SecureView App run on the target Cohesity cluster by following the installation steps section.
3. In the Run Cohesity SecureView App window, provide details of the cloned SmartFiles Views from step1.

Access Backup Data

Recovery of the VCF components from the file-based backups requires following the recovery procedures provided by VMware. The first step towards the recovery is gaining access to the backup data residing in the SFTP directory on the Cohesity SmartFiles. You may use any third-party SFTP tool or access the data from any host that has an SFTP binary. We will be using a Linux host to access the SFTP in the following section.

Table 1: Location of the Backup Data

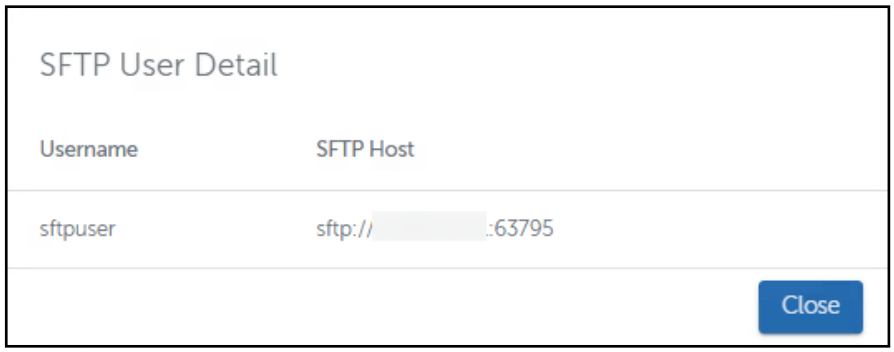
VCF Component	Automatic Backup/On-Demand backup	Location
SDDC manager	Automatic Backup	/exchange/SDDC/VCF_FQDN/sddc-manager-backup
NSX-T	Automatic & On-Demand Backup	/exchange/SDDC/VCF_FQDN/Cluster-node-backup
NSX-T *Applies only when the default SFTP setting is changed for NSXTCluster	Automatic & On-Demand Backup	/exchange/NSXTCluster/NSX_Cluster_FQDN
vCenter	Automatic Backup & On-Demand backup	/exchange/VCenter/sn_vCetner_FQDN/

To access the backup data, follow the steps below:

1. Login to the server that has the SFTP binary.
2. Run the sftp command with the “-P” switch to use port 63795.

   ```
   sftp -P 63795 SFTPUSER@sftpIP
   ```

   - You can use the Sftp user and password you created in the create user section.
   - To get the SFTP IP, navigate to Manage **Users >** Click **User**`.



3. Once you enter in sftp prompt, the Remote working directory is “/exchange”.

```
root@                    /# sftp -P 63795 sftpuser@10.
sftpuser@                's password:
Connected to             .
sftp> pwd
Remote working directory: /exchange
sftp>
```

You can navigate and list the files with Windows or Linux commands such as ls, dir, cd.

```
sftp> ls -latr
drwxr-xr-x    1 root     root            1 Nov 27 15:49 ..
drwxrwxr-x    1 root     1000            1 Nov 27 18:00 NSXTCluster
drwxrwxr-x    1 root     1000            1 Nov 28 06:43 SDDC
drwxrwxr-x    1 root     1000            3 Nov 28 08:15 .
drwxrwxr-x    1 root     1000            1 Nov 28 08:15 VCenter
sftp> cd SDDC
sftp> ls -latr
drwxrwxr-x    1 root     1000            1 Nov 28 06:43 .
drwxrwxr-x    1 root     1000            3 Nov 28 08:15 ..
drwxrwxr-x    1 root     1000            3 Nov 28 10:22 .cohesity.com
sftp> cd .cohesity.com/
sftp> ls -latr
drwxrwxr-x    1 root     1000            1 Nov 28 06:43 ..
drwxrwxr-x    1 1000     1000            1 Nov 28 06:48 inventory-summary
drwxrwxr-x    1 root     1000            3 Nov 28 10:22 .
drwxrwxr-x    1 1000     1000            2 Nov 28 11:07 cluster-node-backups
drwxrwxr-x    1 1000     1000           46 Nov 29 05:40 sddc-manager-backup
sftp> cd sddc-manager-backup/
sftp> ls -latr
-rw-rw-r--    1 1000     1000     12621056 Nov 28 06:48 cohesity-com-2024-11-28-06-48-17.tar.gz
-rw-rw-r--    1 1000     1000           64 Nov 28 06:48 cohesity-com-2024-11-28-06-48-17.sha256
-rw-rw-r--    1 1000     1000     12622288 Nov 28 07:40 cohesity-com-2024-11-28-07-40-00.tar.gz
-rw-rw-r--    1 1000     1000           64 Nov 28 07:40 cohesity-com-2024-11-28-07-40-00.sha256
```

4. You can use the *“get”* command to download the backup file. It will download the file to the current working directory.

```
sftp> get vcf-backup-                -cohesity-com-2024-11-29-05-40-00.tar.gz
vcf-backup-sac-                      -com-2024-11    0%     0     55.3MB/s   00:00 ETAF
etching /exchange/SDDC/              .cohesity.com/sddc-manager-backup/vcf-backup
-                    -cohesity-com-2024-11-29-05-40-00.tar.gz to vcf-backup-
 -cohesity-com-2024-11-29-05-40-00.tar.gz
vcf-backup-                          -cohesity-com-2024-11 100%   12MB  80.4MB/s   00:00
```

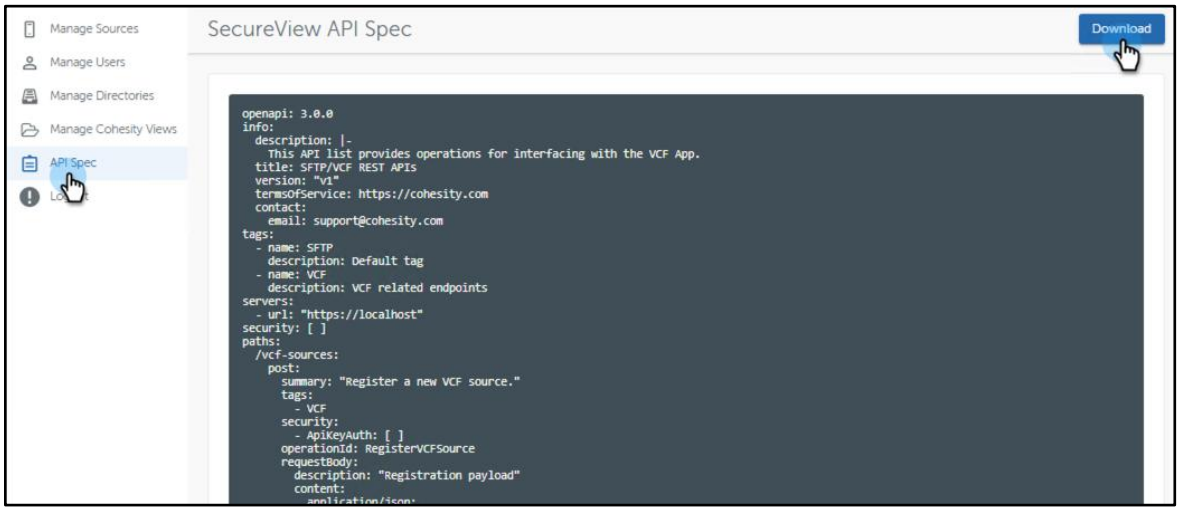
Recovery Process for VCF

Recovering the VCF environment and its components is a stepwise process provided by VMware due to the limitations of VMware API's. Refer to Broadcom VMware documentation for recovery procedures that you must follow for each VCF component.

API Spec

SecureView API specs are now available within SecureView UI. You may download and consume it as appropriate for workflow automation.

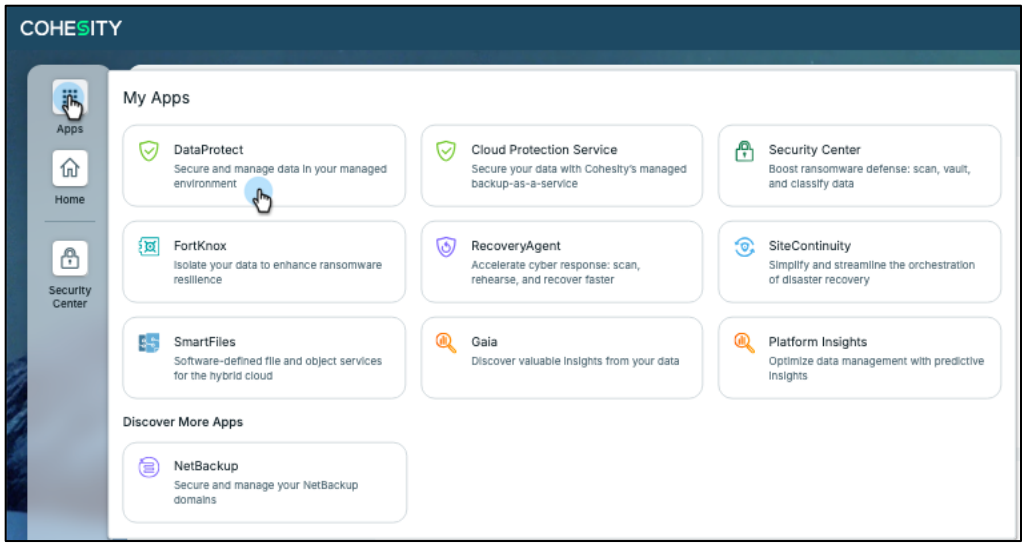
1. Login to SecureView UI.
2. Navigate to API Spec and click on Download button. File named **secureview-api-spec.yaml** will be downloaded to your local system.



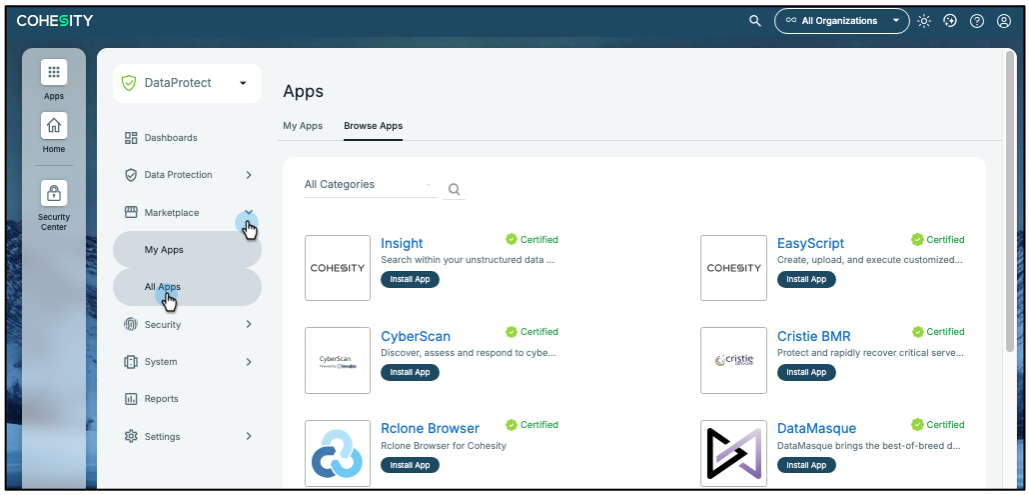
Appendix

For manual installation of SecureView Marketplace app, download the app via Helios.

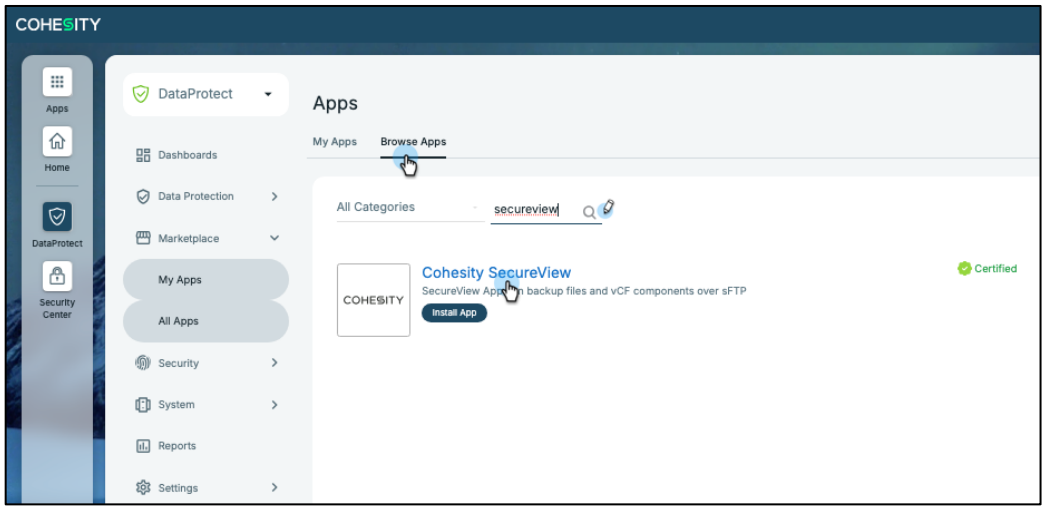
1. Log in to Helios.
2. Click on **Apps** launcher and select **DataProtect**.



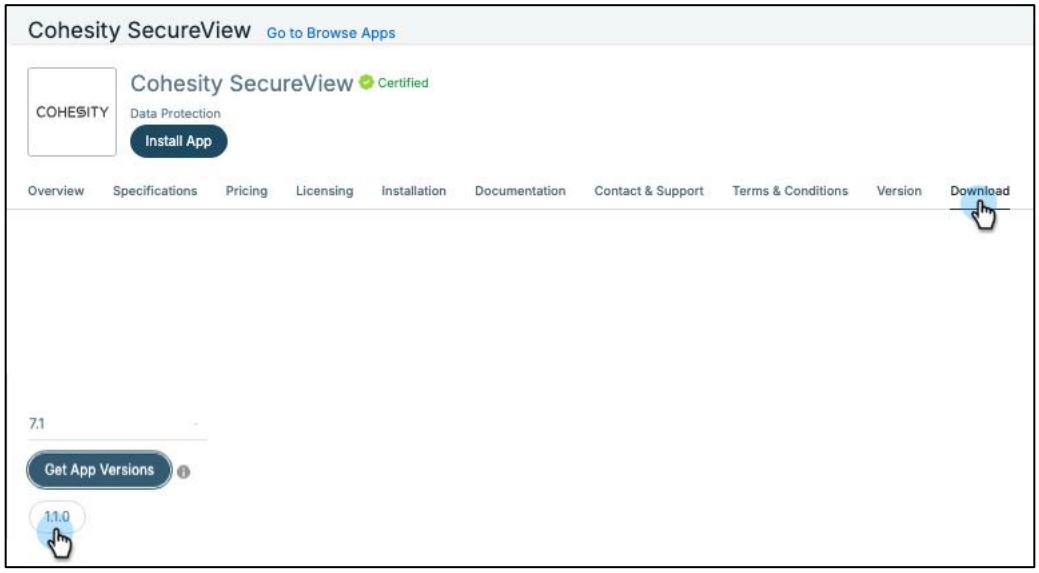
3. Then, click **Marketplace > All Apps**.



4. Under **Browse Apps** search for SecureView and select **Cohesity SecureView.**

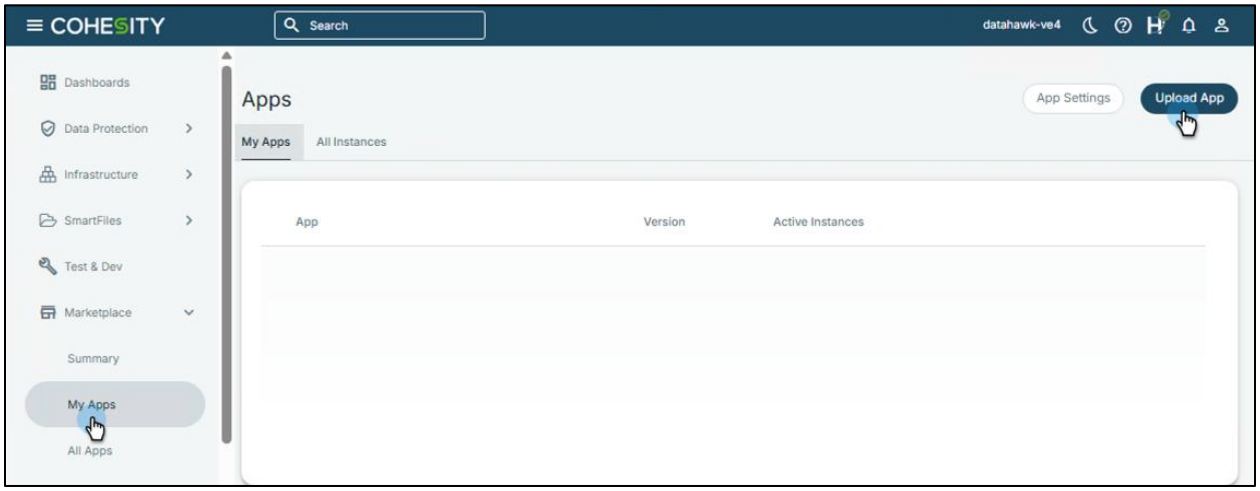


5. Go to **Download** tab and download the App.



6. The App package will be downloaded to your local machine.
7. Login to Cohesity Cluster UI.

8. Browse to **My Apps** and click on **Upload App.**



9. Select the downloaded App file and Click **Upload and Install.**
10. Follow the Install Menus to completion.

Your Feedback

Was this document helpful? Send us your feedback!

About the Authors

Sadik Sayed is a Snr. Solution Architect at Cohesity. In his role, he focuses on NAS and Virtualization backup solutions with Cohesity.

Other essential contributors include:

- Kshitij Parashar, Product Management
- Kavin Agarwal, Engineering
- Punit Gupta, Principal Solutions Architect
- Mary Juliya, Technical Editor

Document Version History

VERSION	DATE	DOCUMENT HISTORY
2.0	Jan 2026	SecureView Enhancements and VCF 5.2.x support
1.1	Feb 2025	Minor update – vCF 5.1 support
1.0	Jan 2025	First release

ABOUT COHESITY

Cohesity is a leader in AI-powered data security and management. Aided by an extensive ecosystem of partners, Cohesity makes it easier to protect, manage, and get value from data – across the data center, edge, and cloud. Cohesity helps organizations defend against cybersecurity threats with comprehensive data security and management capabilities, including immutable backup snapshots, AI-based threat detection, monitoring for malicious behavior, and rapid recovery at scale. Cohesity solutions are delivered as a service, self-managed, or provided by a Cohesity-powered partner. Cohesity is headquartered in San Jose, CA, and is trusted by the world's largest enterprises, including six of the Fortune 10 and 44 of the Fortune 100.

Visit our website and blog, follow us on Twitter and LinkedIn , and like us on Facebook.