CyberSnap.io
User Guide

Version 1.70



October 2026

Introduction

CyberSnap.io specializes in monitoring the well-being of your NetApp volumes and the virtual machines contained within them. The platform scans all your NetApp snapshots, as well as the VMs inside the volumes, to identify both infrastructure and cybersecurity threats. These findings are then organized in a comprehensive Volume SnapMap©. With CyberSnap, it's easy to establish multiple cybersecurity sandboxes for in-depth forensic analysis of any digital threats. The solution provides insights that allow you to understand the consistency of your storage volumes over time.

In this guide, we will take a step-by-step approach to walking you through how to install, use, and most importantly – how to leverage the advanced capabilities of CyberSnap.io!

Contents

Feedback 1
Support 1
Online Documents 1
About User Guide 1
System Architecture 2
CyberSnap Prerequisites 3
Hardware and Software 3
Firewall Setup 3
Internet Access URL 3
S3 Bucket 4
AI-Driven Cyber Findings Analysis 4
CyberSnap Git Repository Access 4
NetApp ONTAP 4
AD Service Account 5
Antivirus Prerequisites 5
Supported Virtual Machines 5
VMware vCenter – DRS 6
VMware vCenter – Cluster Datastore Heartbeat 6
VMware vCenter – Backup and Snapshots 8
CyberSnap Console Server – Backup Application 8
CyberSnap Console Server – VMware Snapshot 8
CyberSnap Proxy Server – Backup Application 8
CyberSnap Proxy Server – VMware Snapshot 8
VMware vCenter – Resource Pool 9
VMware vCenter – Customize Alarm Rules 9
Fine tuning of Datastore Alarm definition 10
Reconfiguring Disk Usage Alarm in vSphere 11
ECE Installation 14
CyberSnap Installation 17
CyberSnap Initial Configuration 20
Configuring CyberSnap Policy 27
General Information 27
CSI Proxy 27
Infrastructure 28
Storage 28
Scan Type 28
CyberSnap Policy 28
Scan Configuration 29
Example of a CyberSnap Cyber Policy 30
NFS/iSCSI/FC (VMFS) as source volume 31

SMB/CIFS as source volume 31
Executing the Policy 32
Executing Policy Manually 32
Executing Policy Automatically 32
Scheduled option 33
Hourly Execution 33
Daily Execution 33
Weekly Execution 33
Monthly Execution 34
Sync option 35
Policies 35
Policy ribbon 36
THREATS 36
SNAPS VERSIONS 36
VMS VERSIONS 36
TOTAL VOLUME 36
Policy menu options 37
Executing Policy Scan Manually 38
Scanning Process Overview 39
Note: NETAPP 39
Note: VMware vCenter 39
SNAPS 39
Virtual Machine List 41
The Ribbon 41
INFRA THREATS 41
SNAPS VERSIONS 42
VMS VERSIONS 42
TOTAL VOLUME 42
SnapMap © 43
Infra Policy 43
Cyber Policy 44
CyberSnap AI reports 45
Summary Report 45
Validate Threats 46
Show Affected Components 47
Suggest Next Actions 48
Detect Anomalies 49
Analyze Threat Details 49
Sandbox 50
Single VM Sandbox 51
Single Snapshot Sandbox 52
Multi VMs Sandbox 54

Sandbox Result 55
Reverting the Sandbox 55
Logs 56
Reports 57
Report Information 58
Report Status 58
Report Filters 58
Policy Filter 58
Scan Type Filter 58
Result Status Filter 59
Date Time Picker Filter 59
Detections 59
Detection Results 59
Path Exclusions 60
New Path 61
Configuring Email Reporting 62
Licensing 63
License details 63
Adding new License 63
License Overcommit 64
Light and Dark mode 66
Login 67
Session timeout 67
Notification 67
Task Drawer 69
Troubleshooting 69
CyberSnap Remote Service Connectivity 69
Automated Residual Cleanup 69
Manual Cleanup 69
Scan leftover 70
Sandbox leftover cleanup 70
Understanding Your License and Support Services 72
Create Custom Roles for Dedicated Accounts 73
Configuring limited permissions for a VMware vCenter Server account 73
Assign Roles 78
Configuring limited permissions for a NetApp account 79
Upgrading to the Latest Version of CyberSnap 82
Applying custom PFX certificate 84
PFX File 84
Utility to encrypt the PFX password 84
Editing the CSI configuration file 86
Service Restart 87

Feedback

At CyberSnap.io, customer feedback is highly valued as it significantly contributes to not only enhancing user experience but also advancing our product development. Our mission encompasses listening to and integrating customer input to tailor our products to meet their needs and expectations.

Support

Should you encounter any technical issues or have questions, we encourage you to reach out for support. You can open a case via the CyberSnap support portal or send an email to support@cybersnap.io.

Online Documents

For additional support, our online resources are available to provide more information about our platform. Visit our website at:

- https://www.cybersnap.io/

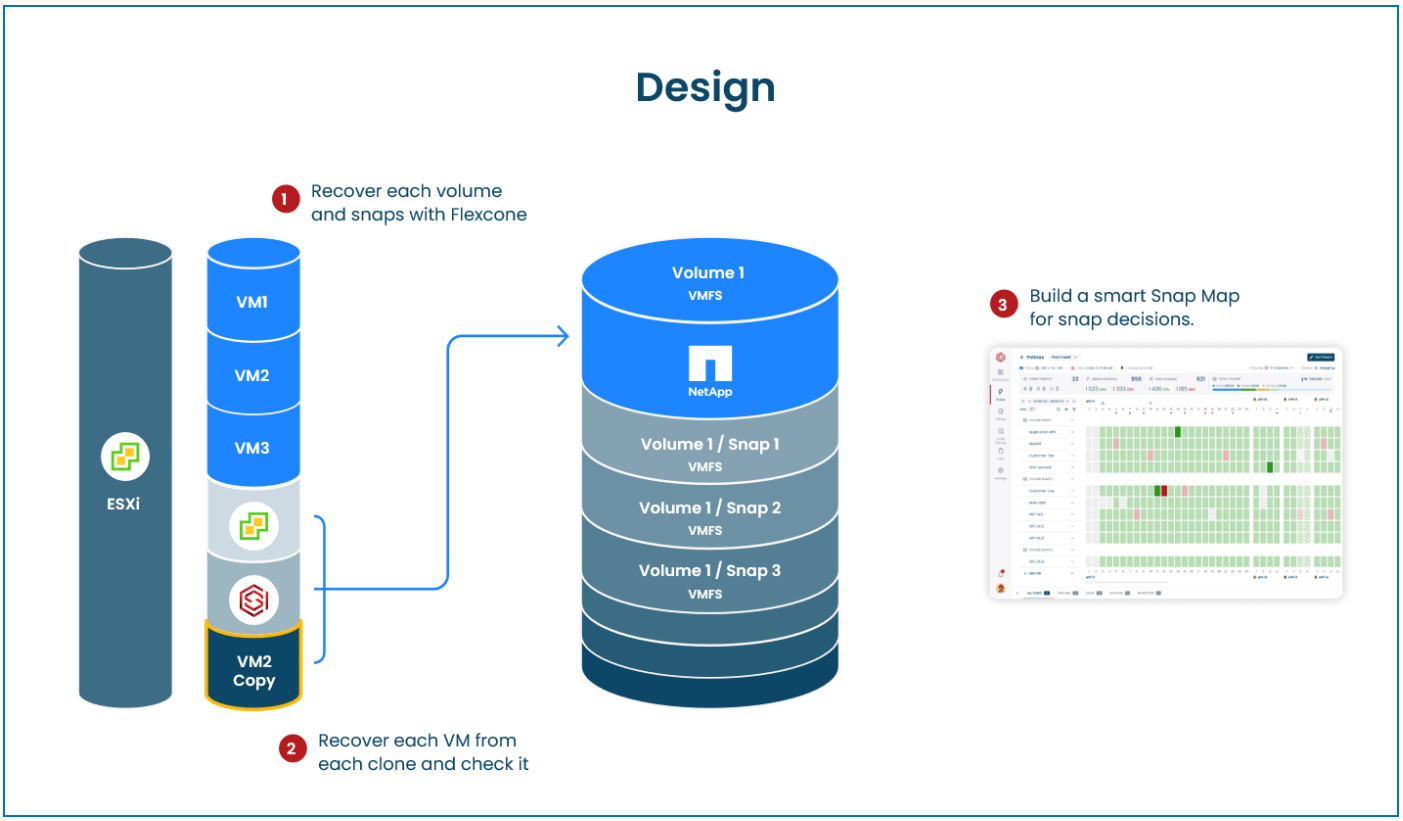
About User Guide

This document elucidates the primary features, installation process, and usage of CyberSnap, aiding you in maximizing the benefits of our platform.

System Architecture

CyberSnap is designed to operate on a single server, running a Windows OS, within your VMware ecosystem. It interfaces directly with your NetApp storage and VMware vCenter setups to scrutinize snapshots and virtual machines for both infrastructure and cybersecurity vulnerabilities. A single installation enables the scanning and mapping of an unlimited number of NetApp clusters and VMware vCenter environments.

Here is the CyberSnap design.



CyberSnap Prerequisites

To ensure the correct operation of CyberSnap, certain prerequisites must be set up before installation.

Hardware and Software

CyberSnap server	Windows 2019/2022/2025 One server with 16 GB RAM, 4 CPUs, disk size 250 GB The latest VMware VM tools need to be installed on the server. The correct time zone should be set
Proxy server requirements for the CyberSnap ECE service	Windows 2022/2025 **The VMware SCSI Paravirtual controller must be used for virtual machine setup** Add three additional VMware SCSI Paravirtual controllers, bringing the total number of SCSI Paravirtual controllers attached to the proxy server to four One server with 20 GB RAM, 6 CPUs (Cores per Socket: 1), disk size 250 GB The latest VMware VM tools need to be installed on the server The correct time zone should be set
Supported Virtual Environment	VMware vCenter version 7 or above VMware ESXi version 7 or above
Windows credentials	The CyberSnap service should be configured to use the default Local System account
VMware Credentials	A dedicated VMware vCenter account with either full administrative privileges or the limited role described in "Configuring limited permissions for a VMware vCenter Server account"
NetApp Credentials	A dedicated NetApp account with either full administrative privileges or the limited role described in “Configuring limited permissions for a NetApp account”
Networking	Servers must have a single NIC and assign a static IP
Supported Browser	Google Chrome, Microsoft Edge and Mozilla Firefox
UAC	Our best practice is to disable User Access Control (UAC) if possible

Firewall Setup

If your company enforces strict rules requiring all network segments to be configured with a firewall, the following ports will need to be enabled:

Source	Destination	Port	Type	Notes
CyberSnap	VMware vCenter	443	TCP	VMware default port
CyberSnap	ESXi(s)	443	TCP	ESXi default port
CyberSnap	NetApp	443	TCP	NetApp default port
CyberSnap	CyberSnap Proxy	5000	TCP	CyberSnap Proxy default port

All the ports listed are default ones. If you have customized your setup with different ports, you will need to define firewall rules for those specific ports.

Internet Access URL

S3 Bucket

To automatically provide policy log files to CyberSnap Support, you must first enable HTTPS access to the AWS S3 CyberSnap bucket. This secure connection ensures that log files are transmitted safely and efficiently. Each customer is assigned a dedicated folder for log file sharing. This design ensures strict access control and prevents any possibility of data exposure or leakage between different customers.

Once HTTPS access is configured, log file sharing can be activated from the Settings page within the CyberSnap Console. By default, this feature is disabled for security and privacy reasons and can only be enabled manually by the customer.

To enable the automatic upload of CyberSnap log files, the following URL must be accessible.

- https://cybersnap-customer-logs.s3.eu-west-1.amazonaws.com/

AI-Driven Cyber Findings Analysis

For advanced analysis of Cyber findings, CyberSnap integrates with an AI-based recommendation engine. This AI agent assists in interpreting scan results and provides actionable insights to enhance incident understanding and response.

To protect customer privacy and data integrity, CyberSnap does not upload or share any sensitive company information such as server names, IP addresses, usernames, or similar identifiers. Only non-sensitive metadata—such as the file name, triggered rule, and other relevant scan attributes—is transmitted to the AI agent. This ensures that the AI can perform an accurate contextual analysis without compromising data security.

The AI Analysis feature is enabled by default. However, to receive AI-generated recommendations, users must manually activate the process by clicking the AI button. For successful communication with the AI agent, the following URL must be accessible from both servers:

- https://ai.cybersnap.io

CyberSnap Git Repository Access

CyberSnap provides a dedicated Git repository that contains essential files maintained and updated by the CyberSnap team. To ensure your system receives the latest updates, the following URL must be accessible:

- https://bitbucket.org/cybersnap/

By default, CyberSnap automatically checks the Git repository each time a scan is initiated to verify whether new updates are available and download them if necessary. This ensures the system always operates with the most recent configurations and definitions.

NetApp ONTAP

To access CyberSnap capabilities, specific NetApp prerequisites must be fulfilled:

- Applied the FlexClone license
  - To successfully utilize the NetApp FlexClone license, a minimal amount of free space is required in the aggregate, depending on the size of your snapshot.

- NFS volumes, create a new export policy or update the existing NetApp ONTAP Export Policy to include all specified VMware ESXi hosts in the CyberSnap Policy.
- Ensure that an initiator group (igroup) is created for each ESXi host or cluster. This step is necessary for establishing connections between the ESXi hosts and the NetApp LUNs. (iSCSI/FC only)
    - *Note:* If INFRA scanning will be performed only using specific ESXi hosts, configure an igroup for each of those specific ESXi hosts.
- Set up snapshot policies on volumes that will be configured in CyberSnap.

AD Service Account

CyberSnap does not require a dedicated Windows account. Upon successful setup, the CyberSnap, CyberSnap Bridge, and ECE services are created on the CyberSnap servers, and the Local System account is configured for use by these services.

If your company policy restricts the use of the Local System account, you must create a service account with local administrator privileges on the CyberSnap server and assign it to the CyberSnap service. This service account can be either a local or domain account, depending on your company's policies.

Antivirus Prerequisites

An antivirus program running on CyberSnap servers may interfere with CyberSnap's operation by intercepting files that need to be scanned. To prevent conflicts in the scanning process, we recommend adding a folder exclusion:

CSI main server

- EXE Files:
    - C:\Program Files (x86)\CyberSnap.io\CyberSnap\web server\BridgeProxy.exe
    - C:\Program Files (x86)\CyberSnap.io\CyberSnap\web server\CyberSnap.API.exe
- PowerShell scripts:
    - Whole folder (all scripts): C:\Program Files (x86)\CyberSnap.io\CyberSnap\web server\scripts

CSI Proxy server

- Exclude folder:
    - C:\scan_folder
    - C:\Program Files\ECE Cyber Scan
- File
    - C:\Program Files\ECE Cyber Scan\ece_scan.exe

Supported Virtual Machines

Depending on the policy type and the virtual machine's multiple-disk configuration, there are certain limitations in CyberSnap, which we list below:

- CyberSnap relies on NetApp snapshots to scan and validate virtual machines. Therefore, it is crucial that the virtual machine selected in the policy does not have multiple disks spread across different

datastores. Such virtual machines will appear greyed out in the policy list, as this configuration is not supported by CyberSnap.

- The Cyber policy type does not support Linux virtual machines at the moment.
- The Infra policy type supports both Linux and Windows virtual machines.

Note: Virtual machines that use deprecated Windows dynamic volume types are not supported when configured with a Cyber policy type.

VMware vCenter – DRS

In a VMware vSphere environment, when working with clusters, you may have configured DRS (Distributed Resource Scheduler), which focuses on load balancing by automatically migrating VMs between hosts to optimize performance and resource usage.

Because CyberSnap scans VMDK disks attached to the Proxy server, it's essential to understand that migrating the server to a different host may disrupt the connection to the datastore, resulting in lost access to the attached VMDK disks.

To prevent this, create VM Override rules that disable VMware DRS for the CyberSnap Proxy virtual machine. This ensures that CyberSnap Proxy server remains connected to the dedicated datastore throughout the scanning process.

VMware vCenter – Cluster Datastore Heartbeat

In VMware vSphere, HA (High Availability) datastore heartbeating provides a secondary communication mechanism between ESXi hosts when the management network becomes unavailable. By default, vSphere automatically selects accessible datastores for HA heartbeating.

During the CSI scanning process, datastores are temporarily attached to the vSphere environment to allow controlled access for analysis and validation operations. These attachments are transient by design and exist only for the duration of the scan.

During CSI scans, automatic datastore selection can cause operational issues. Datastores automatically selected for HA heartbeating may become locked by the VMware HA mechanism, preventing CSI from unmounting and removing the temporary datastores after the scan completes.

To avoid this condition, it is mandatory to disable automatic datastore selection and explicitly define which datastores are used for HA heartbeating.

Procedure:

Step 1: Select the Target Cluster

1. Log in to the vSphere Client.
2. Navigate to the desired cluster that will be used with CSI scanning.
3. Click Configure.

Step 2: Access vSphere HA Settings

1. Under Services, select vSphere Availability.
2. Click Edit (or Edit Cluster Settings).

Step 3: Disable Automatic Heartbeat Datastore Selection

1. In the vSphere HA settings window, expand Datastore Heartbeating.
2. Locate the Datastore Heartbeat option.
3. Change the selection from:
    - Automatically select datastores accessible from the hosts

to:

    - Use datastores only from the specified list

This change disables automatic datastore selection for HA heartbeating.

Step 4: Manually Select Heartbeat Datastores

1. After selecting Use datastores only from the specified list, click Browse.
2. Select one or more datastores to be used exclusively for HA heartbeating.

Best Practice:

    - VMware recommends selecting at least two shared datastores that are accessible by all hosts in the cluster.
3. Click OK to confirm the datastore selection.

Step 5: Save and Apply the Configuration

1. Click OK or Save to apply the cluster settings.
2. vSphere HA will automatically reconfigure the cluster.

Verification:

To confirm that automatic datastore selection is disabled:

1. Navigate to Cluster > Monitor > vSphere HA.
2. Select Heartbeat Datastores.
3. Verify that only the manually specified datastores are listed.

Result:

Automatic HA datastore selection is disabled, and vSphere HA uses only the explicitly defined datastores for heartbeating.

Summary:

By switching from automatic to manual HA datastore selection:

- Temporary datastores attached by CSI are not unintentionally used for HA heartbeating
- Datastore locks that prevent unmount or removal are avoided
- HA behavior becomes more predictable and aligned with CSI operational requirements

This configuration is essential for environments that rely on temporary datastore attachment during scanning or integrity verification workflows.

VMware vCenter – Backup and Snapshots

CyberSnap consists of two servers, each with a specific role. The CyberSnap main server will be configured with the CyberSnap Management Console, while the CyberSnap Proxy server will be responsible for scanning VMDKs from various source servers located on a NetApp volume defined in the policy.

Since certain VMware processes, such as backups and server snapshots, may be performed during the execution of the CyberSnap policy without CyberSnap being aware of them, we will provide guidelines on how to carry out these two specific tasks.

CyberSnap Console Server – Backup Application

Since the CyberSnap server will remain powered on during the backup process, the backup will be considered 'crash-consistent'. A crash consistent backup in VMware captures the state of a virtual machine (VM) at a specific point in time without shutting it down or coordinating with the applications inside. It includes all data that was in memory and on disk at the time of the snapshot, similar to a system crash or sudden power loss. While no data is lost from disk, data in memory or pending writes may not be preserved, so applications may require recovery steps on restart.

Because of “crash-consistent” nature backup can be taken during the policy running so when the server is restored by the backup application policy can be in error state. No issues are expected during the backup process, therefore, no specific measures need to be taken.

CyberSnap Console Server – VMware Snapshot

All the rules and measures mentioned in the previous paragraph are applied to the VMware Snapshot native process. We strongly suggest that before manually taking the snapshot, you validate that there are no policies or other running processes indicated in the CyberSnap console. This will help ensure the most accurate state for CyberSnap if you decide to revert the CyberSnap console server to the saved snapshot state.

CyberSnap Proxy Server – Backup Application

Since the CyberSnap Proxy server may be scanning during the backup process, this can cause the backup application to fail due to inaccessible VMDK disks that are under the control of CyberSnap.

Therefore, it is important to configure the backup application to include only the main OS disk, the disk used to set up the virtual machine and on which the ECE service is installed (typically named "Disk 0" in the VMware Console). All other disks must be excluded from the backup to avoid failures of backup and restores.

If your backup application doesn’t support this capability, you will need to define a time window during the day when no scanning processes are running on the CyberSnap Proxy Server. Then, schedule the backup to run during that time or perform a one-time manual backup while all policies on the CyberSnap Console Server are not in a 'running/scanning' state.

CyberSnap Proxy Server – VMware Snapshot

All the rules and measures mentioned in the previous paragraph also apply to the native VMware Snapshot process. We strongly recommend that, before manually taking a snapshot, you verify in the CyberSnap

console that no policies are currently running. This is necessary to ensure that no VMDK disks from scanning servers are attached to the CyberSnap Proxy server during the manual VMware snapshot creation process.

VMware vCenter – Resource Pool

As part of the best practices, we suggest creating a dedicated Resource Pool for Infra policy types. By implementing Resource Pools, you can limit the resources available to CyberSnap in the VMware vSphere environment while simultaneously allowing your production environment to utilize the maximum available resources.

Since Cyber Policy types works with VMDK disk files and this approach does not introduce additional impact to your VMware environment, except for the load on the CyberSnap server during scanning, we require configuring the Cyber Policy to the 'Target ESX' host in the policy settings and selecting the same VMware host where the Cyber Proxy server is located. If VMware DRS is enabled, ensure that VM Override rules disable DRS for the CyberSnap virtual machine.

To accommodate varying numbers of virtual machines with different RAM and CPU configurations, we suggest setting the following parameters for the CyberSnap Resource Pool:

Memory
Reservations: 20% of the total RAM limit
Limits: 50% of the total RAM

CPU
Reservation: 20% of the MAX Limit
Limits: 50% of the MAX Limit

Be aware that not all versions of VMware vSphere support Resource Pool feature, here is brief overview of versions:

- **vSphere Essentials**: Does not include the ability to create Resource Pools.
- **vSphere Essentials Plus**: Includes the ability to create Resource Pools, along with features like vMotion and High Availability.
- **vSphere Standard and above** (including vSphere Enterprise and Enterprise Plus): Also allow you to create Resource Pools and include additional features like Distributed Resource Scheduling (DRS), Storage DRS, and more.

In cases where you cannot use the Resource Pool feature due to license limitations, you will still be able to select hosts from VMware vCenter. We recommend upgrading your license to a level that supports the Resource Pool feature, as this will enable CyberSnap scans to run on a larger scale, with more servers simultaneously.

Regardless of whether you configure a Resource Pool in your environment or not, the virtual machine Overrides rule that disables DRS for the CyberSnap virtual machine must be configured if VMware DRS is enabled.

VMware vCenter – Customize Alarm Rules

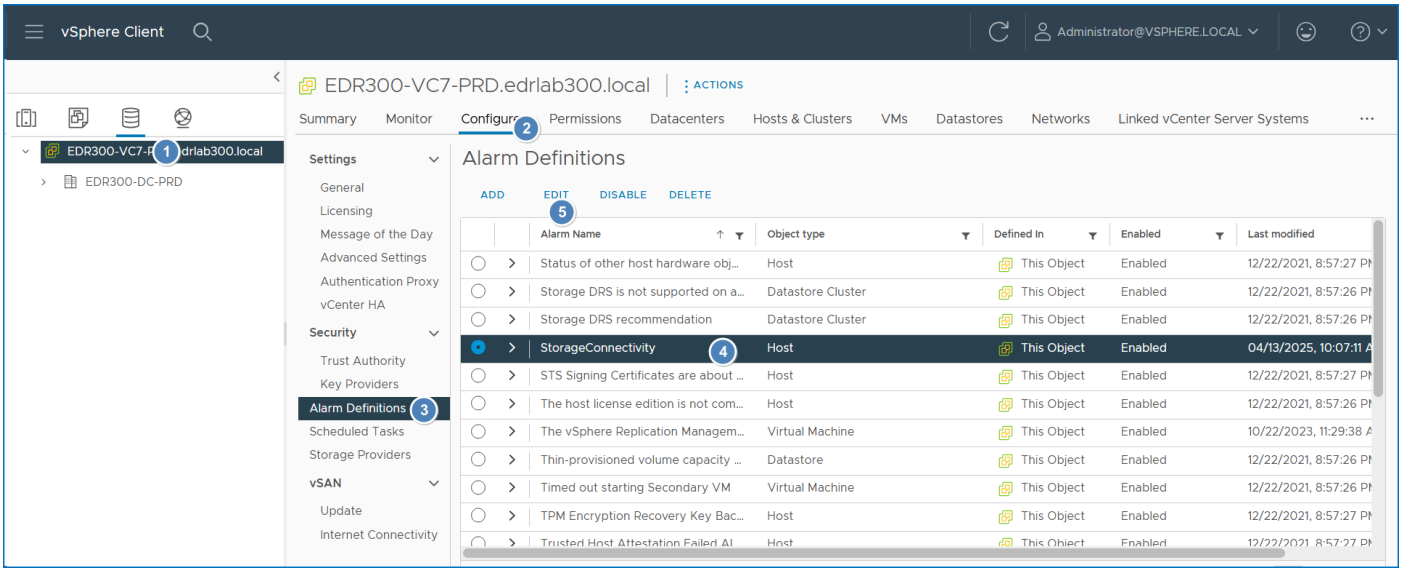
During CyberSnap operations, NetApp volumes will be connected and disconnected multiple times. If your environment includes alarms configured to trigger during this process, you may want to adjust them to prevent event generation and email notifications.

Fine tuning of Datastore Alarm definition

To avoid receiving emails when a Datastore is connected or disconnected by CyberSnap, you should add an additional filter in the current alarm definition. Once you modify the rule, it will ignore Datastore names that start with 'CSI', and no email will be sent.

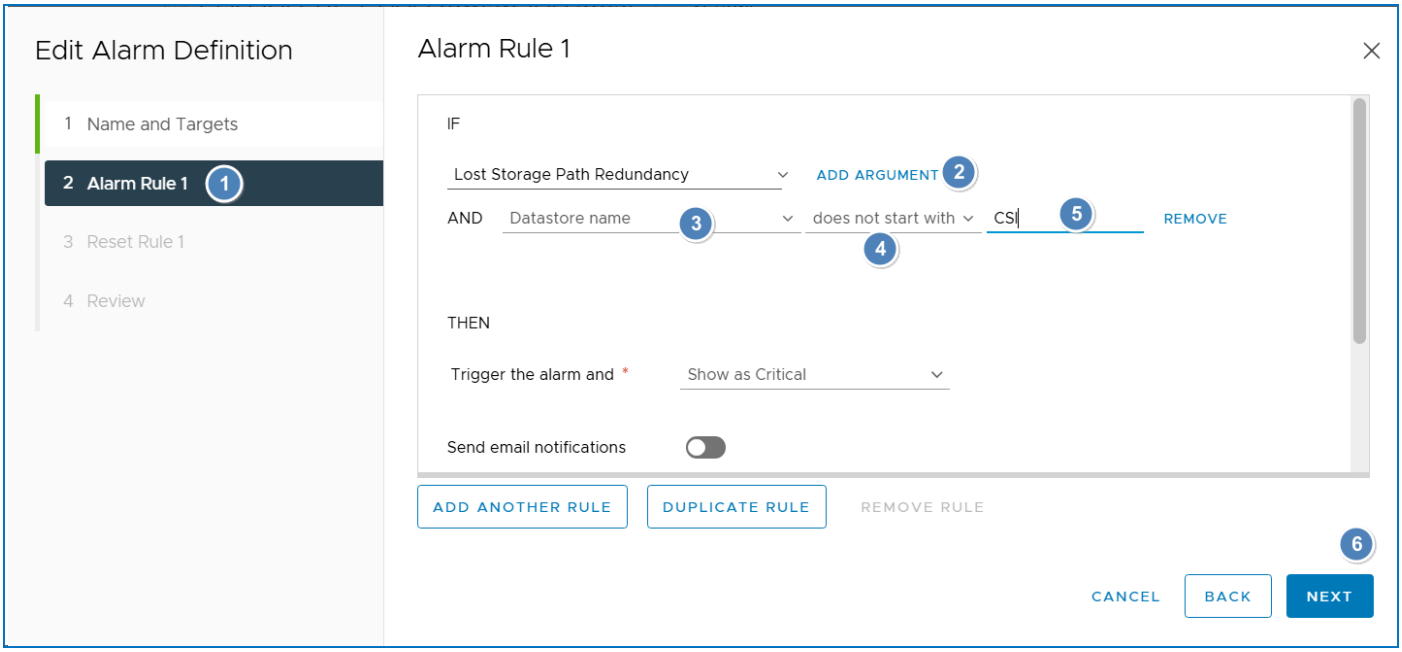
To modify an alarm definition, follow these steps:

1. Select the vCenter in the left pane.
2. In the right pane, click the Configuration tab.
3. From the list of options, select Alarm Definitions.
4. Choose the rule you previously created.
5. Click the Edit button.



When the rule is open:

1. Navigate to “Alarm Rule 1” in the Alarm Definition.
2. Click “Add Argument”. A new option will appear in the alarm definition.
3. For the filter, choose “Datastore name”.
4. Select “does not start with”.
5. Enter “CSI”.
6. Click “Next” until you reach the end of the rule definition, then click the “Save” button.

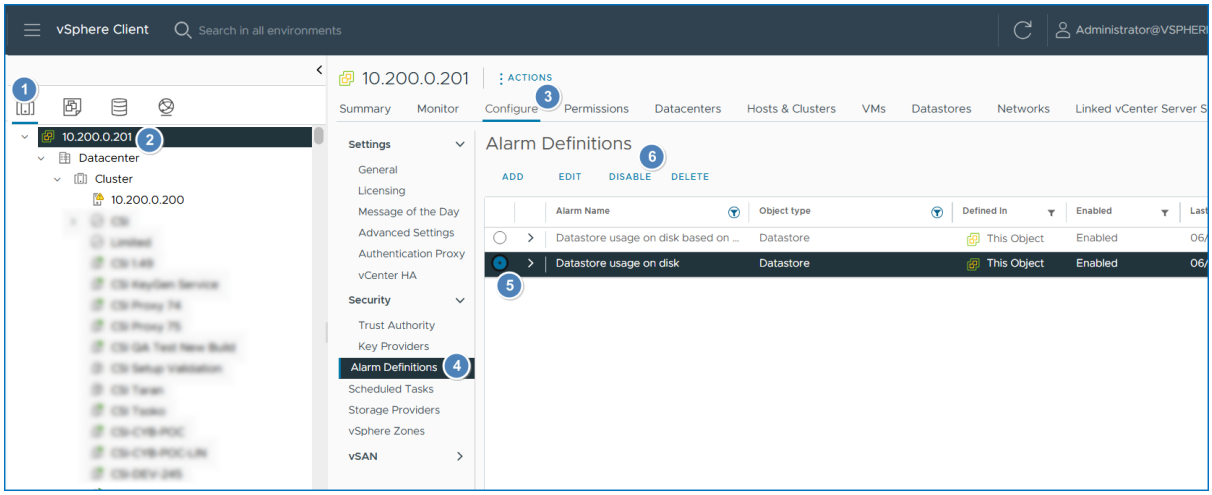


Reconfiguring Disk Usage Alarm in vSphere

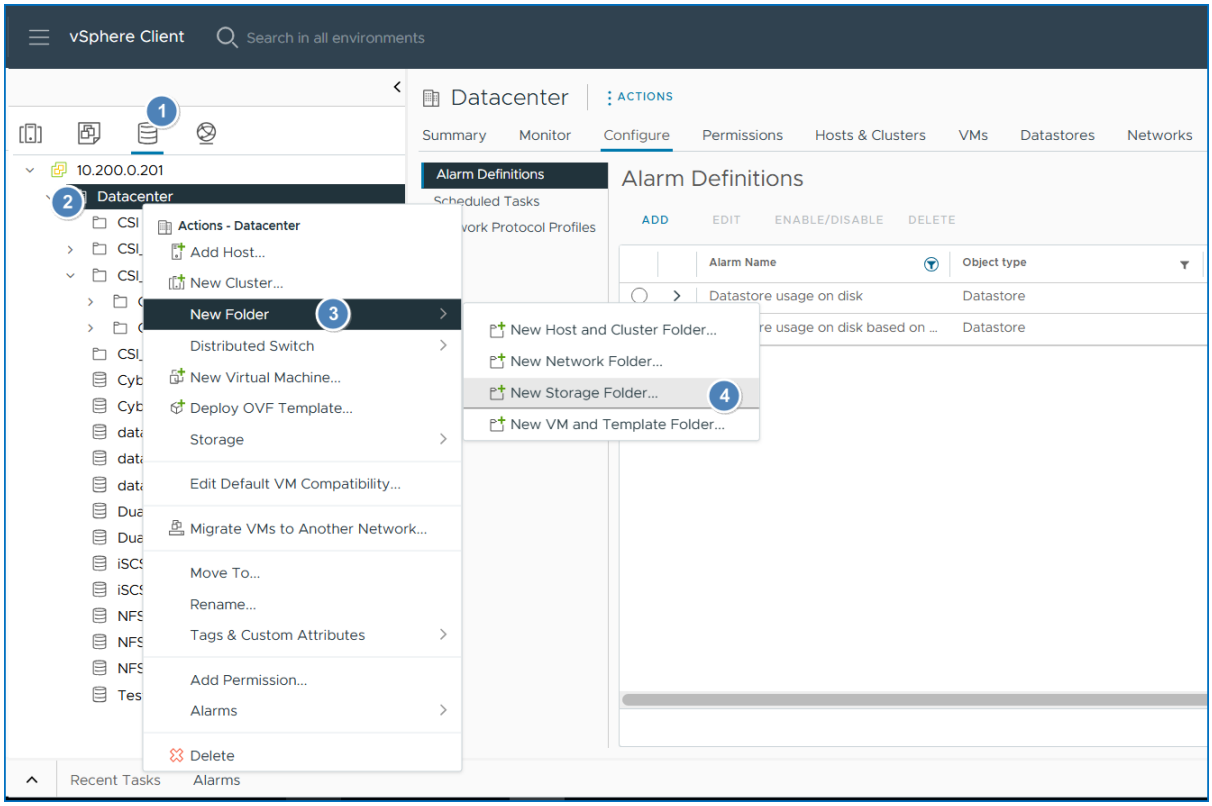
To prevent data stores created by CyberSnap from triggering the disk usage alarm, you should disable the default disk usage rule at the vCenter level and instead create a custom rule using the same metrics. This custom rule should only be applied to a specific folder, which you will need to create. Once the folder is in place and the custom rule is applied, move all production datastores into that folder.

Steps are:

- Disable the DiskUsage rule at the vSphere vCenter level

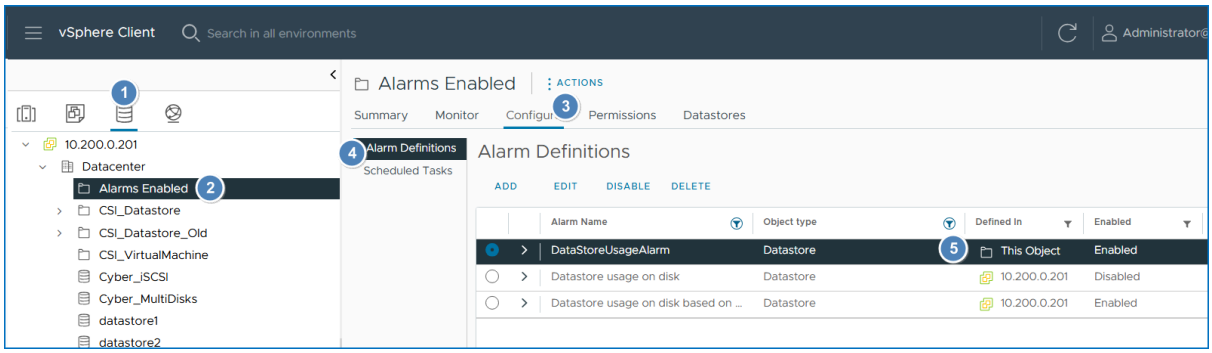


- Create folder in the datastore Inventory Tab named:
  - **Alarms Enabled**

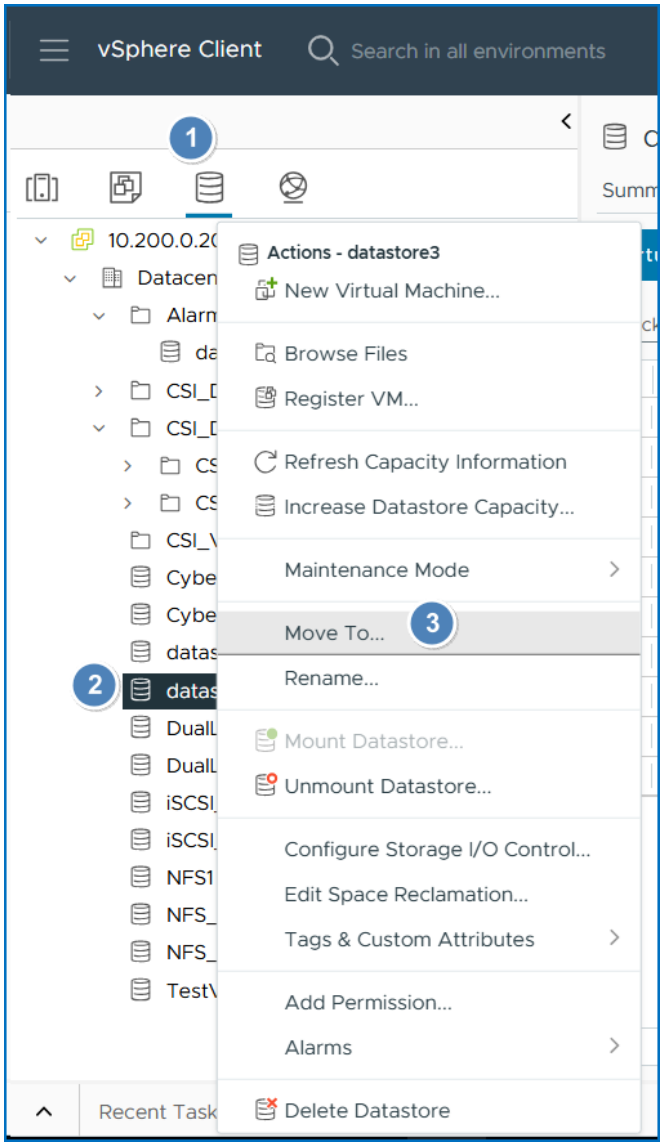


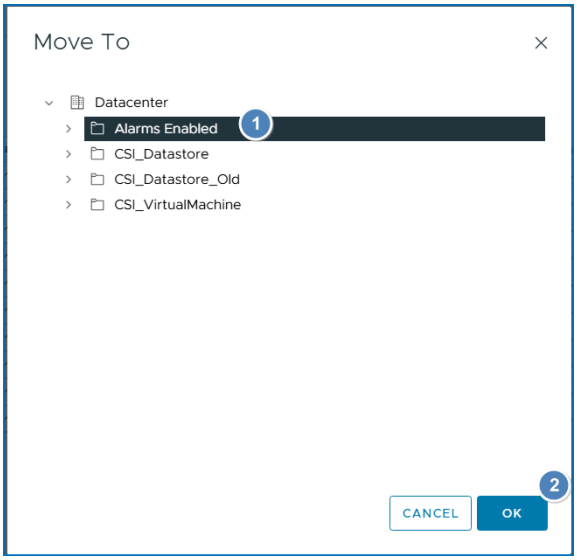
- Select the folder you created in the previous step, then create a custom rule using the same metric details as the default DiskUsage rule.

Note: “Define In” must be “This Object” (e.g. folder that you select) in point 5.



- Now that the rule has been created and applied to the 'Alarms Enabled' folder, move all production datastores that need to be monitored into this folder.


vSphere Client
Search in all environments
1
Actions - datastore3
New Virtual Machine...
Browse Files
Register VM...
Refresh Capacity Information
Increase Datastore Capacity...
Maintenance Mode
Move To...
3
Rename...
2
Mount Datastore...
Unmount Datastore...
Configure Storage I/O Control...
Edit Space Reclamation...
Tags & Custom Attributes
Add Permission...
Alarms
Delete Datastore
Recent Task

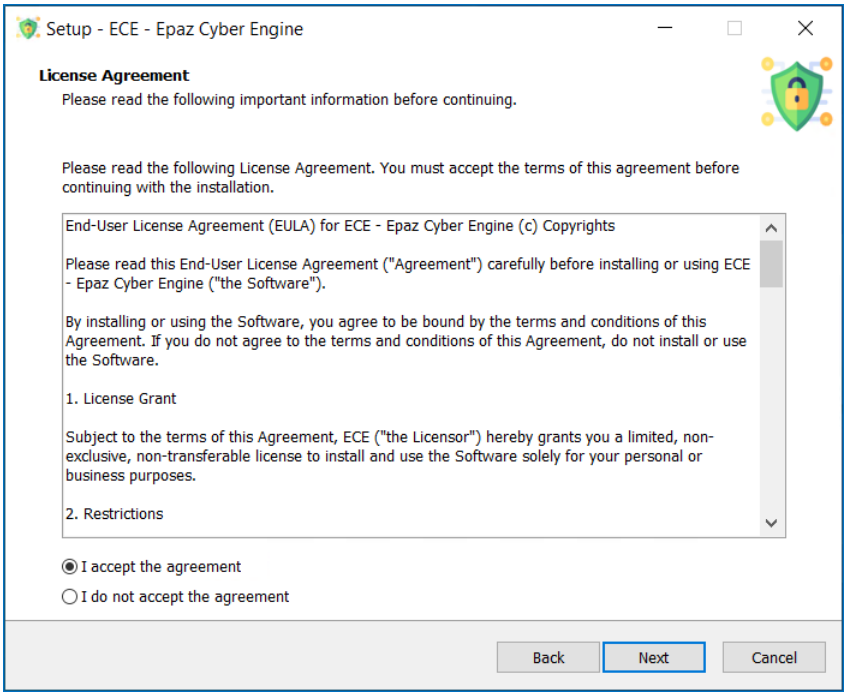

Move To
Datacenter
Alarms Enabled
1
CSI_Datastore
CSI_Datastore_Old
CSI_VirtualMachine
2
CANCEL
OK

ECE Installation

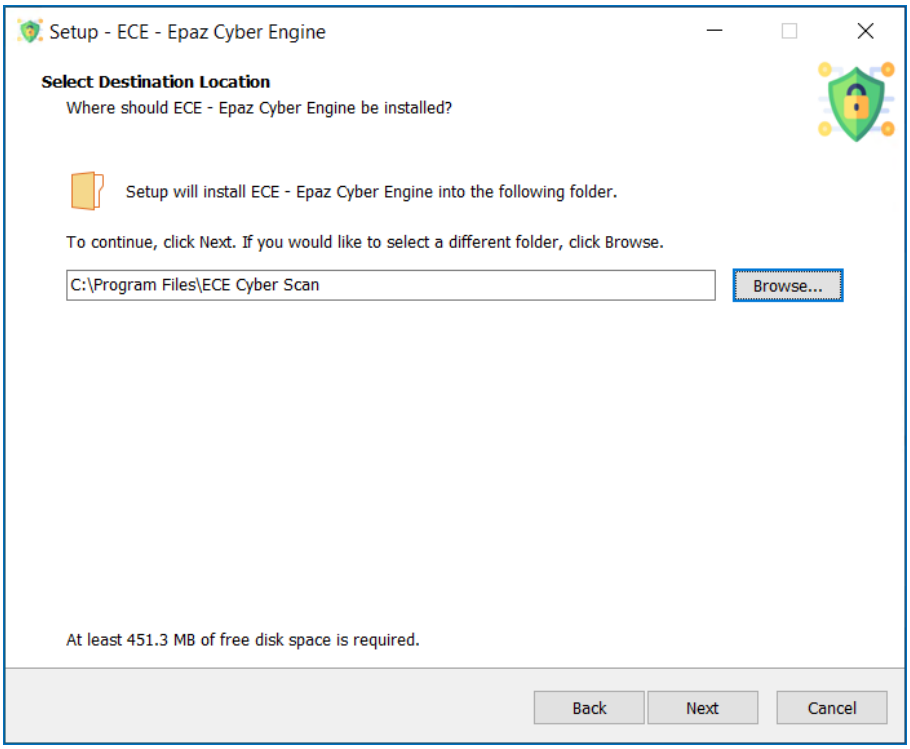
Log in to the CyberSnap Proxy server using an account with full administrative rights. Run the “ECE-Cyber-Scan-Setup.exe” executable. If a warning window appears, approve the installation. Upon doing so, a welcome screen will appear, click the 'Next' button.



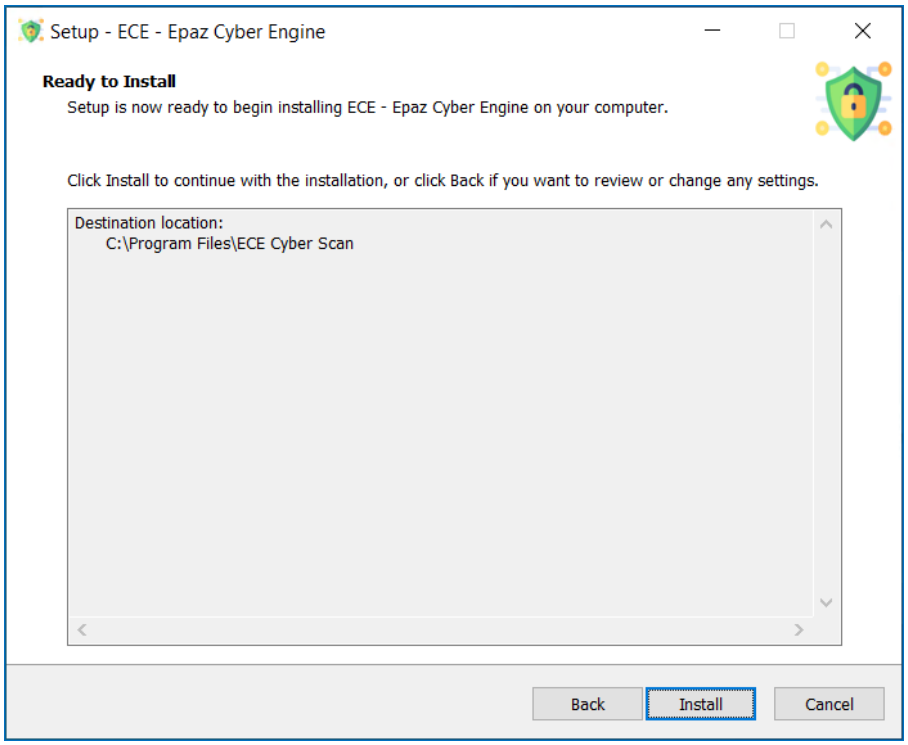
Review the License Agreement, select “I accept the agreement”, then click the 'Next' button.



In the next screen, a pre-configured path will be displayed. Customize the path if necessary, then click the ‘Next’ button to continue.



Click the ‘Install’ button and wait for the installation to complete. This may take a few minutes depending on the environment and components.



Upon completion, click the ‘Finish’ button, wait until service is started and ECE icon disappears from the task bar.

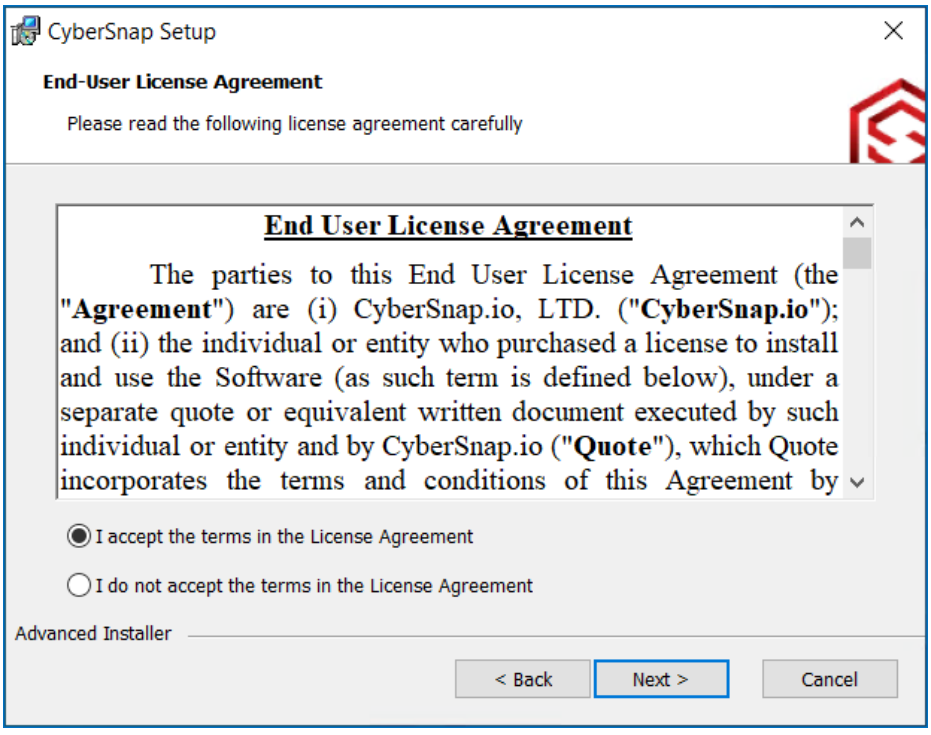


CyberSnap Installation

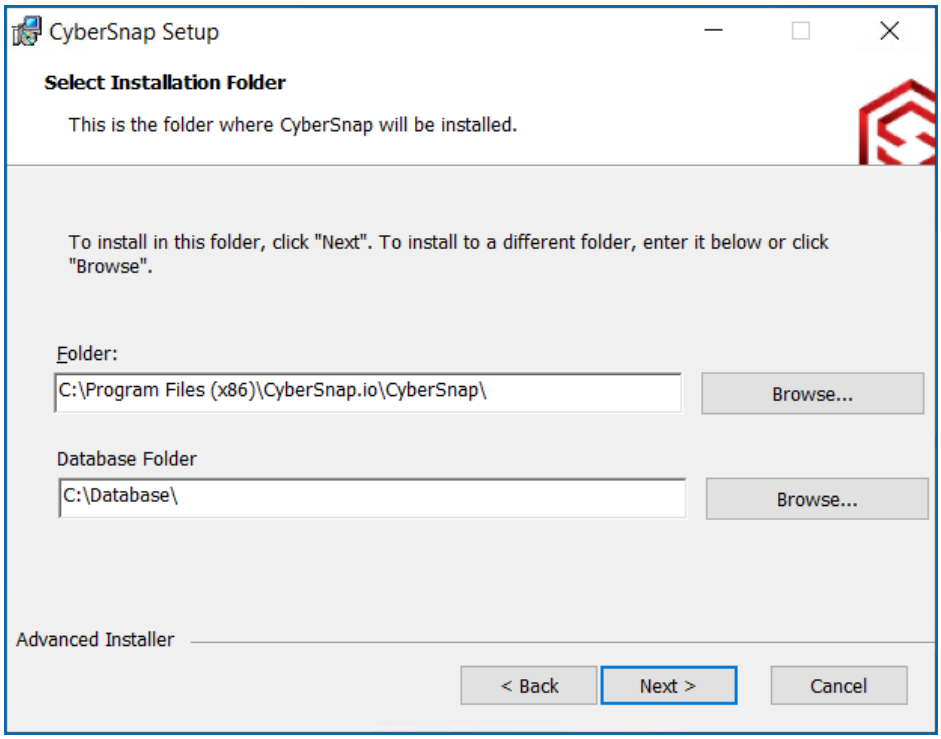
Log in to the CyberSnap server using an account with full administrative rights. Run the CyberSnap executable. If a warning window appears, click the 'Run' button. Upon doing so, a welcome screen will appear, click the 'Next' button.



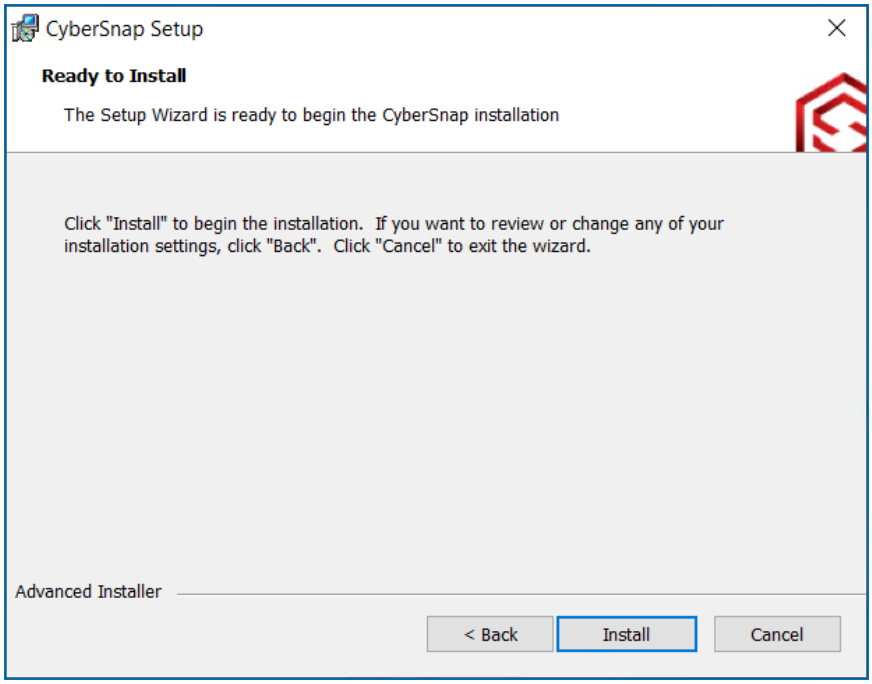
Review the License Agreement, select “I accept the terms in the License Agreement”, then click the 'Next' button.



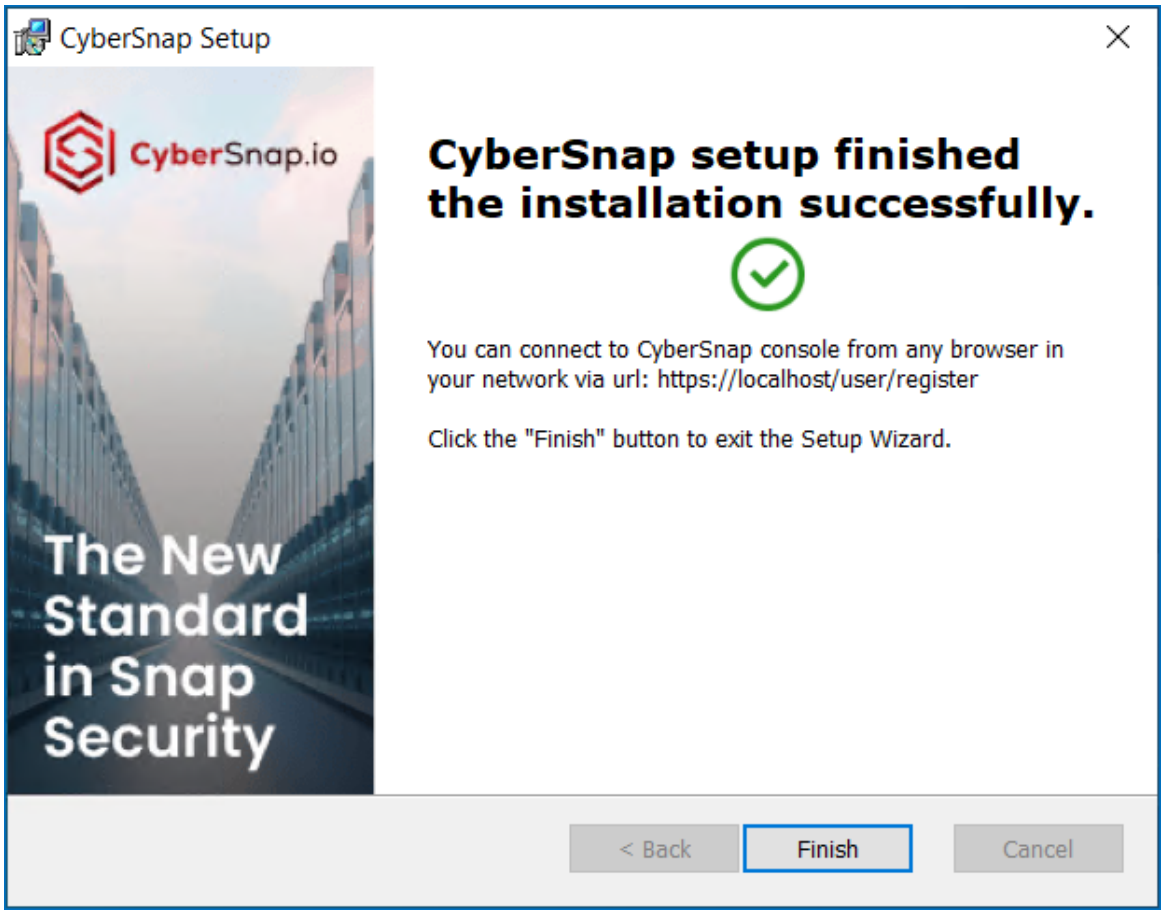
In the next screen, a pre-configured path for the CyberSnap setup and database will be displayed. Customize the path if necessary, then click the ‘Next’ button to continue.



Click the ‘Install’ button and wait for the installation to complete. This may take a few minutes depending on the environment and components.



Upon completion, click the ‘Finish’ button to conclude the setup and proceed to the CyberSnap console. The default browser will launch, opening the registration form in CyberSnap.



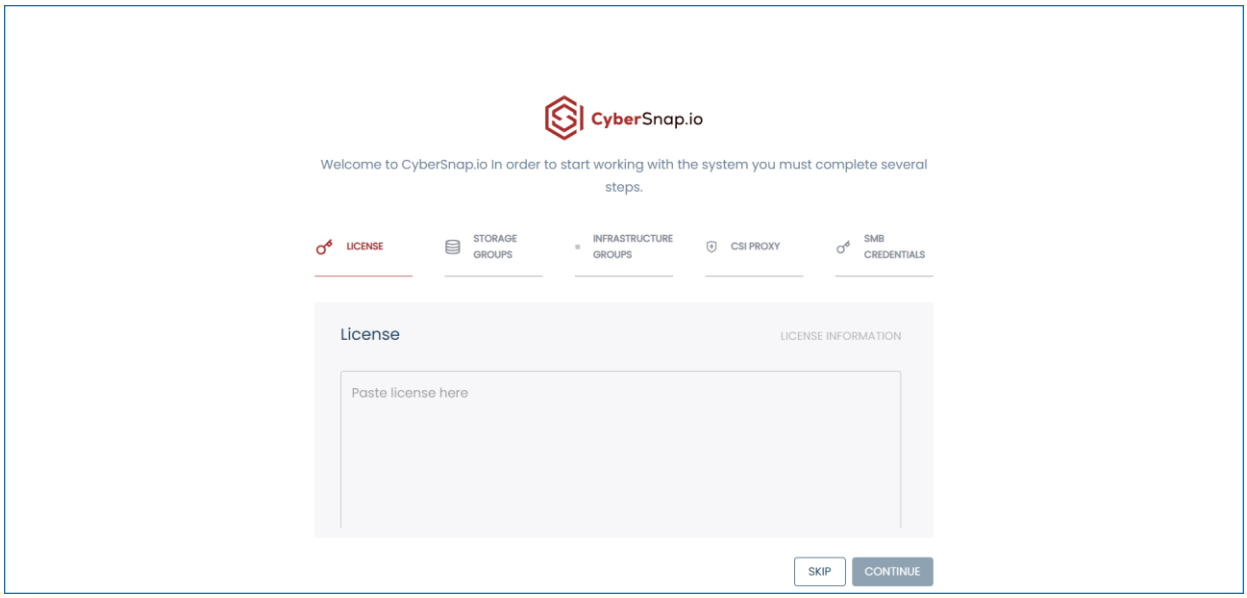
CyberSnap Initial Configuration

Enter the desired username, specify your email address, and set a password that meets the complexity requirements. Click the ‘REGISTER’ button to validate the information.

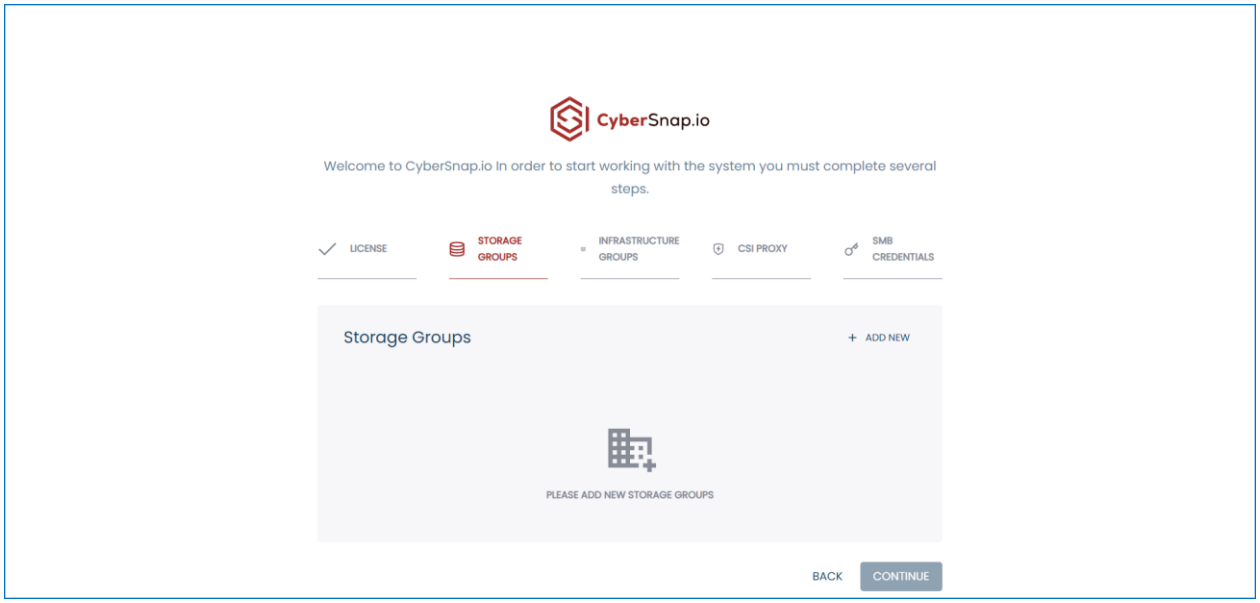


If you enter all data correctly, the CyberSnap web console opens the Welcome page. Enter the License key, and upon validation, the 'Continue' button will be enabled. Click 'Continue'.

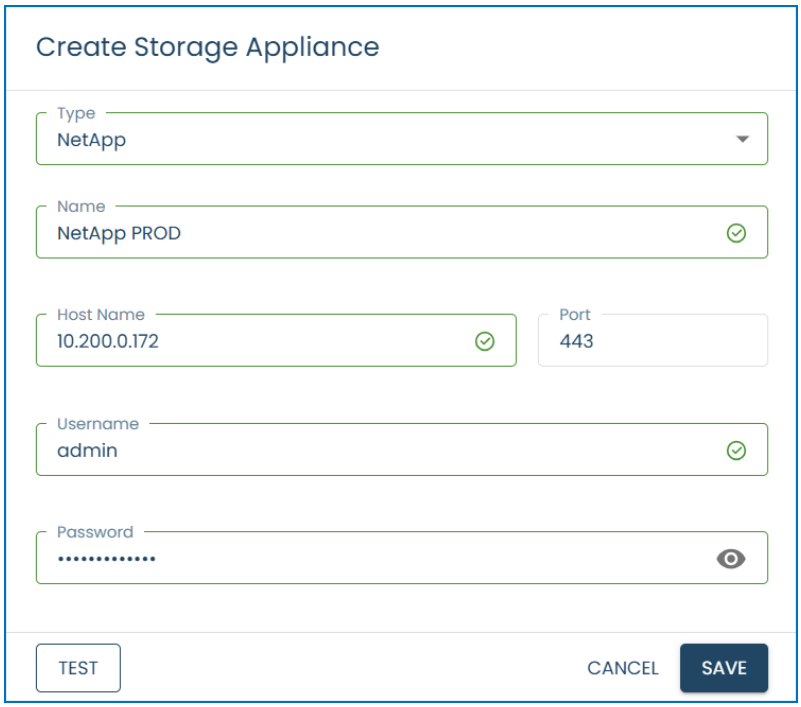
Note: If you do not have a license key, click the Skip button to start in Trial mode.

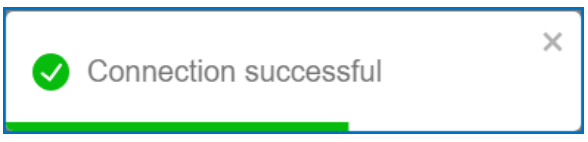


Click 'ADD NEW' to start configuring the NetApp data.

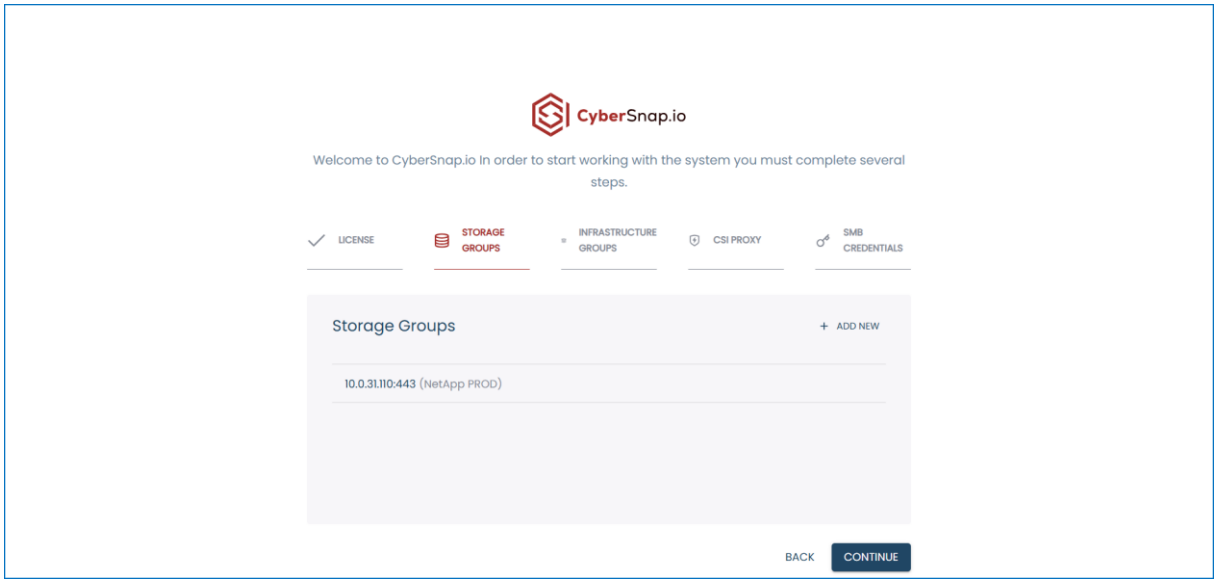


In the new window, select 'NetApp' as the Type, input a custom name, enter your NetApp storage IP address, specify port 443 (or enter a custom port number if necessary). Input the NetApp username and password, then click the 'TEST' button to validate the data. The system displays a green toast notification to confirm successful validation..

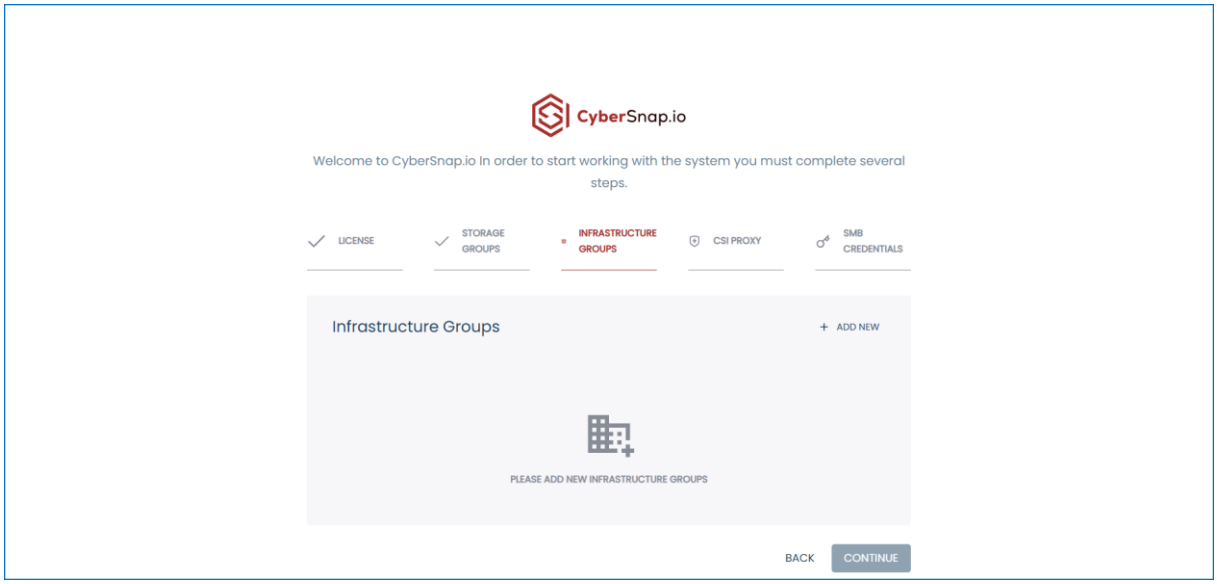




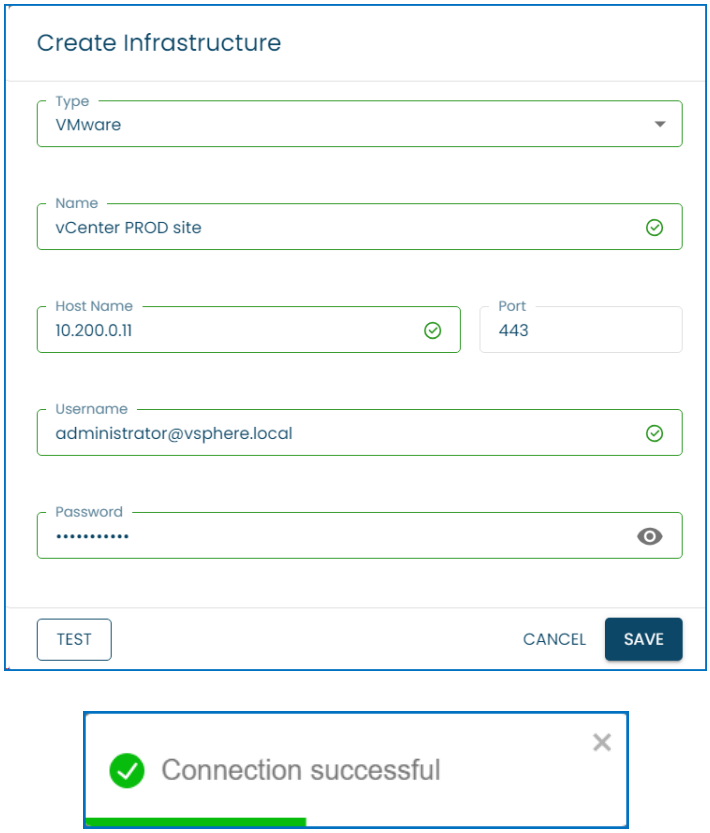
Click the 'SAVE' button. A toast notification will confirm the saved configuration. Your NetApp storage configuration will now appear in the 'STORAGE GROUPS' section of the Welcome page. Repeat these steps for additional NetApp storage configurations.



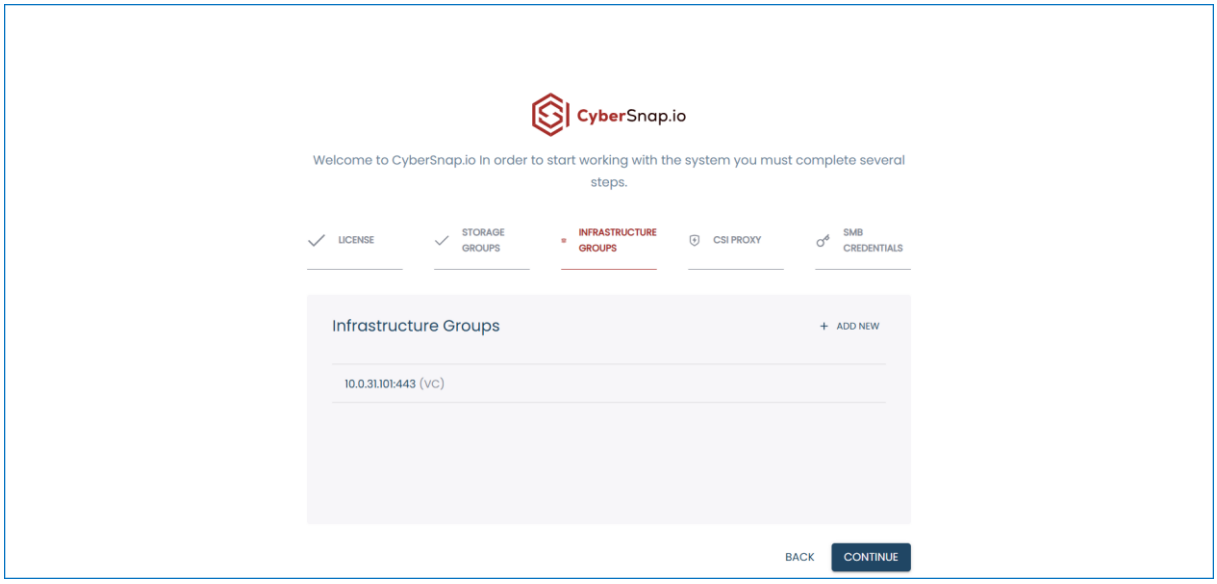
Once all NetApp storages are configured, click 'CONTINUE' to proceed to the 'INFRASTRUCTURE GROUPS' section. Click 'ADD NEW' to add infrastructure details.



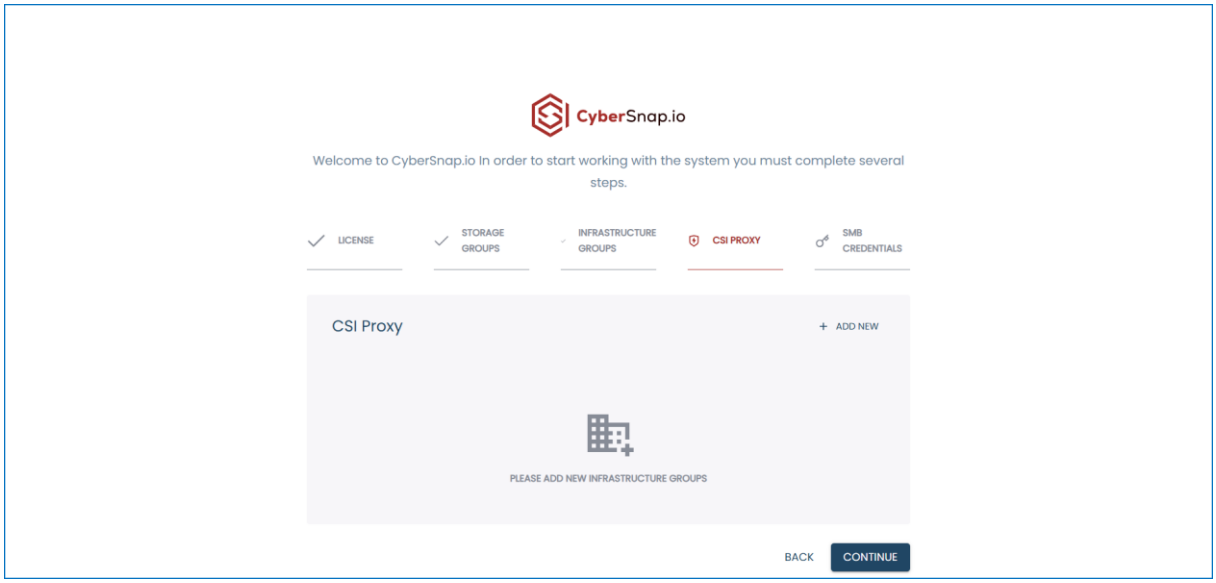
In the new window, select 'VMware' as the Type, input a custom name, enter your VMware vCenter IP address, specify port 443 (or enter a custom port number if necessary). Input the VMware username and password, then click the 'TEST' button to validate the data. The system displays a green toast notification to confirm successful validation.



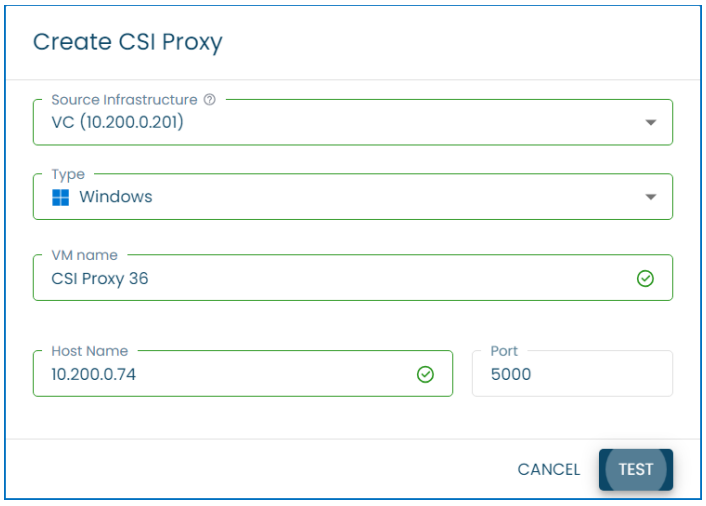
Click the 'SAVE' button. A toast notification will confirm the saved configuration. Your VMware vCenter setup will now be visible in the 'INFRASTRUCTURE GROUPS' section on the Welcome page.

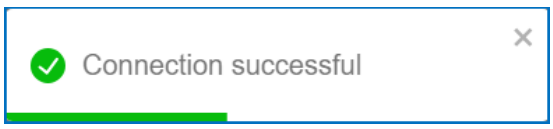


Click ‘CONTINUE' to configure the CSI Proxy , then click 'ADD NEW' to add proxy server.

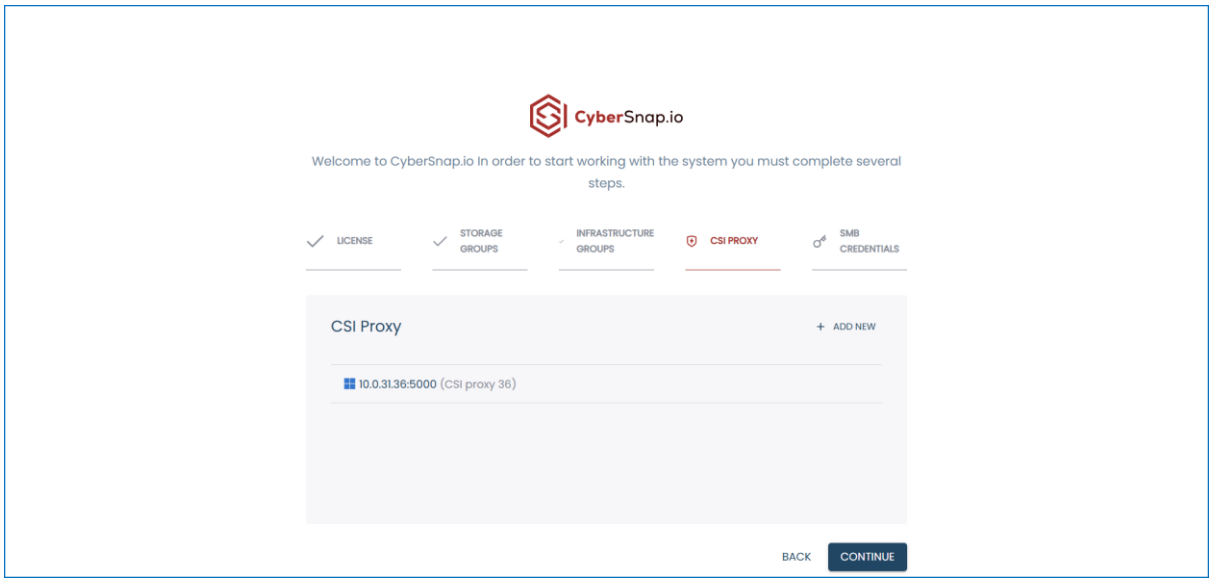


A new window will pop up, for the Source Infrastructure select VMware Virtual Center you registered in the previous step. Choose "Windows" as the Proxy type, input a VM name as specified in VMware vCenter, add the proxy server's IP address while leaving the default port set to 5000, then click the 'TEST' button to validate the data. The system displays a green toast notification to confirm successful validation.

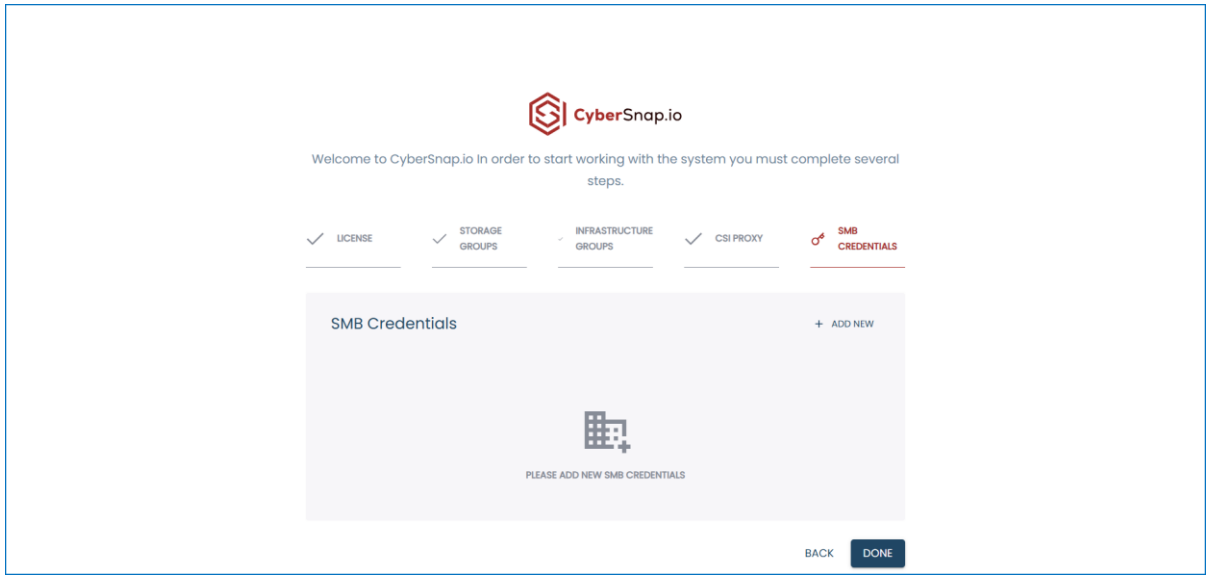




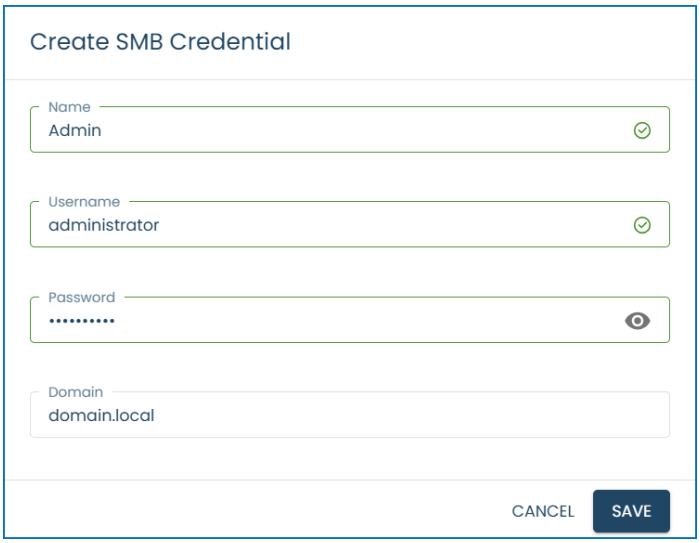
Click the 'SAVE' button. A toast notification will confirm the saved configuration. Your Proxy Server is now visible in the 'CSI PROXY' section on the Welcome page.



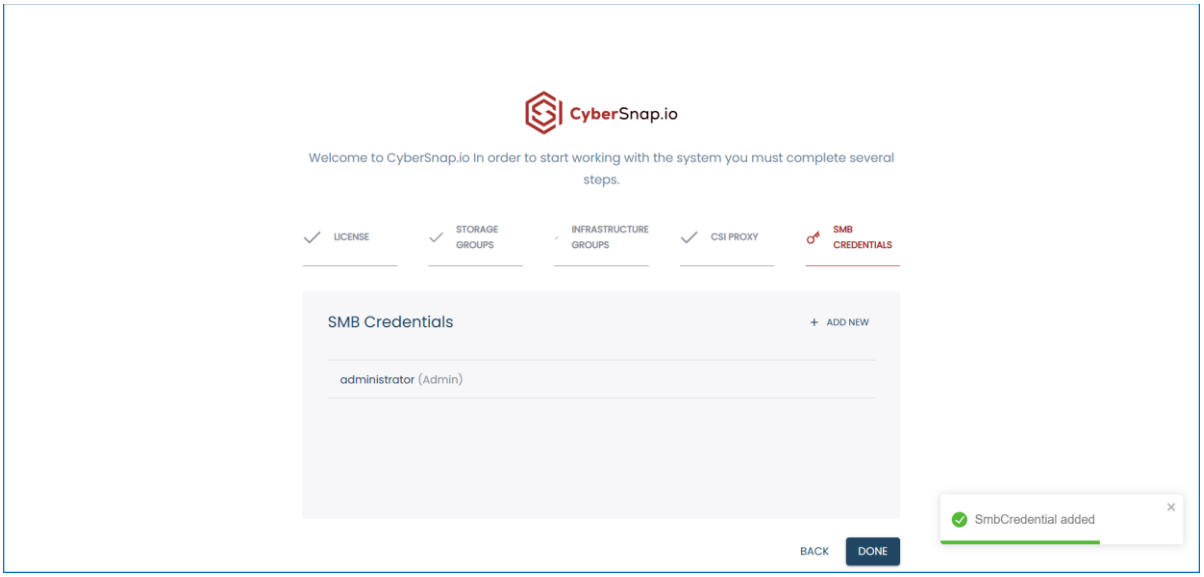
Click ‘CONTINUE’ to configure the SMB credentials, then click ‘ADD NEW’ to add new SMB credentials.



A new window will open. Enter a custom name, username, password, and domain name, then click ‘SAVE’ to save the SMB credential.

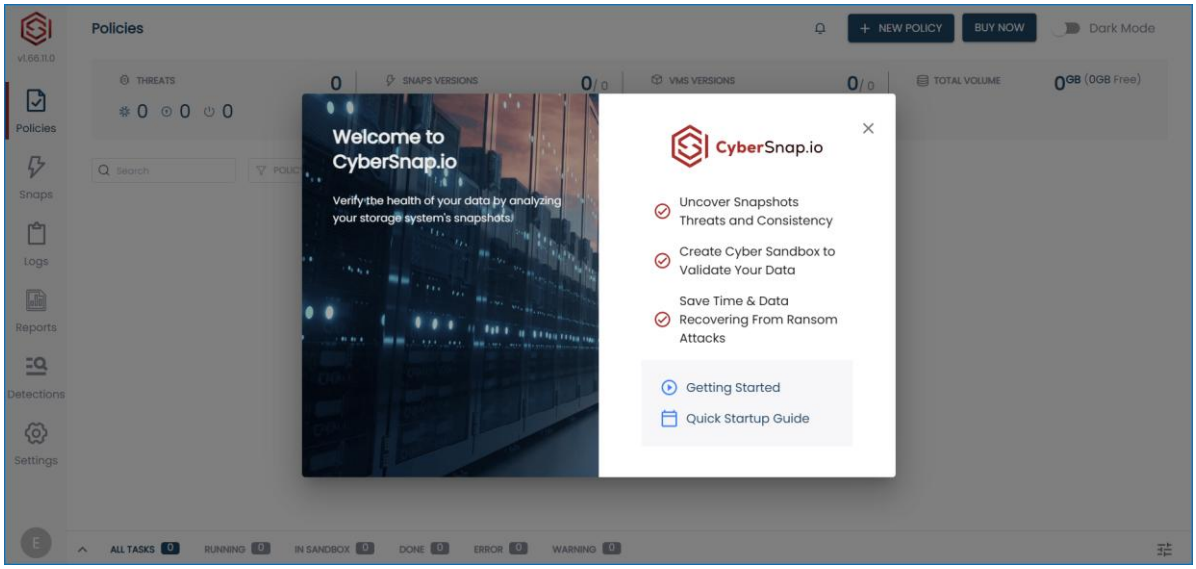


The system displays a green toast notification to confirm successful validation.



Click 'DONE' to conclude the initial setup.

After the initial setup is complete, the Welcome window will pop up. If you skip adding the license key, a notification message will appear to remind you that the trial period will end in 30 days.



From the welcome page, you can quickly access the 'Getting Started' video or the Quick Startup Guide.

Configuring CyberSnap Policy

After successfully configuring all essential data on the CyberSnap Welcome screen, you will be directed to the Policies section, where you'll need to create a policy. The CyberSnap Policy is a container that encapsulates configuration settings for CyberSnap, defining its interactions with volumes and the infrastructure. The configurations within the CyberSnap Policy guarantee consistency checks throughout the infrastructure. This engine is responsible for inspecting infrastructure compliance and identifying any anomalies that could compromise system integrity. In this container, policies are encoded as rules and checks to enforce specific checks within a defined timeframe. This automation reduces manual effort, minimizes the risk of human error, and ensures continuous compliance with organizational policies and security standards.

Each policy definition is divided into six sections:

- General Information
- CSI Proxy
- Infrastructure
- Storage
- Scan Type
- CyberSnap Policy
- Scan Configuration

General Information

In the general section you need to set a custom name for the policy.

CSI Proxy

In this section, select the proxy server to be used during the scanning process. If only one proxy server is configured, it will be selected automatically. If multiple proxy servers are available, you must manually select the server you want to use.

Infrastructure

Select the servers to include in the Infrastructure or Cyber Policy. Before proceeding, ensure that all prerequisite parameters are properly configured and entered in the policy form.

When a VMware vCenter server is selected in the right pane of the Configure Policy view, the system retrieves and displays all virtual machines from the storage selected in the Storage section that are associated with the selected vCenter server.

From the displayed list, you can select one, multiple, or all available virtual machines for inclusion in the policy.

Depending on the scenario you wish to configure, you must select either the source, the destination, or both VMware vCenter servers. The scenarios are described in the upcoming section of this user guide.

Storage

CyberSnap supports NFS/iSCSI/FC (VMFS) storage environments, enabling threat detection and integrity validation across virtualized and SMB/CIFS based infrastructures. Depending on the deployment scenario, you may be required to select the source storage, destination storage, or both. Detailed configuration requirements for each supported scenario are described in the following sections of this guide.

Cyber Policies can scan data residing on NetApp snapshots, virtual machines, and SMB/CIFS shares, providing comprehensive visibility into potential threats across primary storage and backup environments.

Scan Type

By default, the Cyber policy type is preselected to scan the volume selected in Storage section. This policy type scans the virtual machine disks. If you want to scan a shared folder hosted on your SAN, select the SMB/CIFS checkbox to specify the shared folder as the scan target.

Cyber

The CyberSnap Policy is designed to continuously monitor the organization's digital assets and ensure the integrity of its information systems by utilizing the Cyber Scanning Engine. This engine examines all virtual machines (VMs) across every snapshot to identify cybersecurity threats, including malware and ransomware. It compiles a comprehensive report that lists all VMs along with their cybersecurity statuses, providing an overview of potential vulnerabilities.

Cyber SMB/CIFS

The Cyber SMB/CIFS policy type uses the Cyber Scanning Engine to scan files and folders stored on SMB/CIFS shares instead of virtual machines. For configuration details, see “SMB/CIFS as source volume”.

CyberSnap Policy

Depending on the way the policy can be triggered, we recognize three possible configuration options:

- Manual
- Scheduled
- Sync

Manual

If 'Manual' is chosen, the policy will be activated by the end-user when scanning the volume is necessary, by selecting the 'Run Scan' option in the policy menu.

Scheduled

If you choose the scheduled option, you'll be required to specify your preferences from the options provided below. The system will then commence the scanning process according to the selected date and time settings.

Scheduler Options:

1. **Start from:** This option sets the execution time of the policy only for its first run. Specify the date and time for the policy to take effect. To activate the policy immediately, retain the suggested date and time. Note that the activation time, once set, cannot be altered in the future.

2. **Execution Frequency:** Define how often the policy should run post-activation - hourly, daily, weekly, or monthly. Each frequency option presents additional settings to refine the execution schedule:
    - **Hourly:** Specify the interval (e.g., every 1, 2, 3, hours).
    - **Daily:** Set the execution time.
    - **Weekly:** Provide the day of the week and the time.
    - **Monthly:** Specify the day of the month and the time.

Sync

When the Sync option is selected, the system will regularly scan the NetApp storage for new snapshots. Each newly detected snapshot will then be automatically processed, and the data will be available in CyberSnap.

Scan Configuration

In this section, you can configure the number of snapshots to scan during the initial scan and subsequent scans. The maximum allowed value for each field is 50. “Scan Snapshot Limit for the First Scan” sets how many snapshots are analyzed during the initial scan, and “Scan Snapshot Limit” sets how many snapshots are processed in each subsequent scan. Lower values reduce scan time, but fewer snapshots are scanned.

Scan Mode

The policy currently supports two scanning modes: Quick and Thorough.

- Quick Scan: Performs a scan without applying YARA rules, reducing the overall scanning time.
- Thorough Scan: Performs a comprehensive scan using both the built-in YARA rules included with the product and any custom YARA rules added by the user. This mode provides more extensive scanning but may require additional time to complete.

Note: For backward compatibility, CyberSnap continues to support the Infra policy type. However, this policy type is disabled by default. To enable it, you must modify the application settings configuration file, and restart services.

The Infra policy is the policy type that uses the Infrastructure Scanning Engine, which inspects your snapshots and virtual machines (VMs) for consistency. It verifies the clone-ability of snapshots, mounts them to datastores, registers each VM to ensure operability, and constructs a SnapMap© detailing all VMs and their consistency statuses.

CyberSnap Infra Policies can be configured in various scenarios, depending on the configuration and location of your infrastructure:

- Utilize the same VMware vCenter and NetApp to execute the CyberSnap Policy.
- Utilize different VMware vCenter and the same NetApp to execute the CyberSnap Policy.
- Utilize the different VMware vCenter and different NetApp to execute the CyberSnap Policy.

The first scenario enables you to execute the policy within the identical environment as your production servers, storage, and hosts. In this scenario, CyberSnap will utilize the same NetApp storage and VMware hosts as in your production environment.

In the second scenario, you can distribute workload across various VMware hosts within the same location but different VMware vCenter server. This setup utilizes the NetApp storage present in your production environment but employs different VMware hosts for scanning and sandboxing purposes.

The third scenario allows you to distribute workload across different VMware hosts and storages located in different locations, such as the DR site. In this scenario, CyberSnap will utilize the different VMware hosts and different NetApp storage. However, for this to occur, a prerequisite must be met. Your NetApp volume selected in a policy must be replicated with NetApp SnapMirror from the source NetApp on the source site to the destination NetApp on a DR site.

Regardless of the described scenarios, some prerequisites in NetApp must be completed beforehand. If you are unsure whether your NetApp environment setup is configured properly for use with CyberSnap, please review the NetApp prerequisites described in this manual. CyberSnap supports NFS and VMFS (iSCSI/FC) volumes in NetApp/VMware infrastructure.

Before proceeding to define the CyberSnap policy details, depending on your needs and infrastructure, it's essential to identify which of the described scenarios is best suited for your environment.

Example of a CyberSnap Cyber Policy

Cyber Policy supports VMware environments with NFS, iSCSI, and Fibre Channel (FC) storage configurations, including VMFS datastores, as well as SMB/CIFS shares as scan sources.

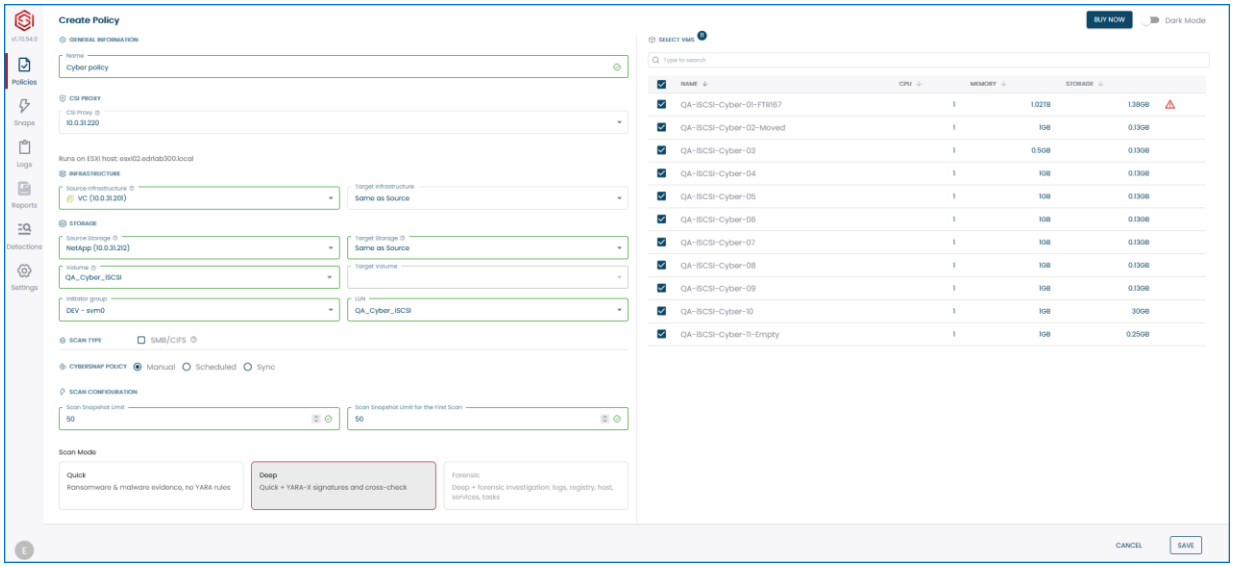
NFS/iSCSI/FC (VMFS) as source volume

Cyber Policy supports NFS, iSCSI, and Fibre Channel (FC) storage environments using VMFS datastores, as well as SMB/CIFS shares as scan sources.

Begin by entering a name for the policy and selecting the Proxy server.

If only one vCenter and one storage system were configured on the Welcome screen during the initial setup, they will be selected automatically. Otherwise, choose the appropriate vCenter and storage system from their respective drop-down lists.

Next, select a volume. The system will automatically load all virtual machines associated with the selected volume.



Finally, select one or more virtual machines to include in the policy, then click “SAVE” to save the configuration.

SMB/CIFS as source volume

For SMB/CIFS environments, CyberSnap scans files and directories stored on SMB/CIFS shares rather than virtual machines. These shares are accessed using the SMB/CIFS file-sharing protocols. CyberSnap leverages the same NetApp Snapshot technology used for VM-based scans, enabling consistent, point-in-time analysis of file data without impacting production workloads.

This example demonstrates how to configure a Cyber Policy using an SMB/CIFS share as the scan source.

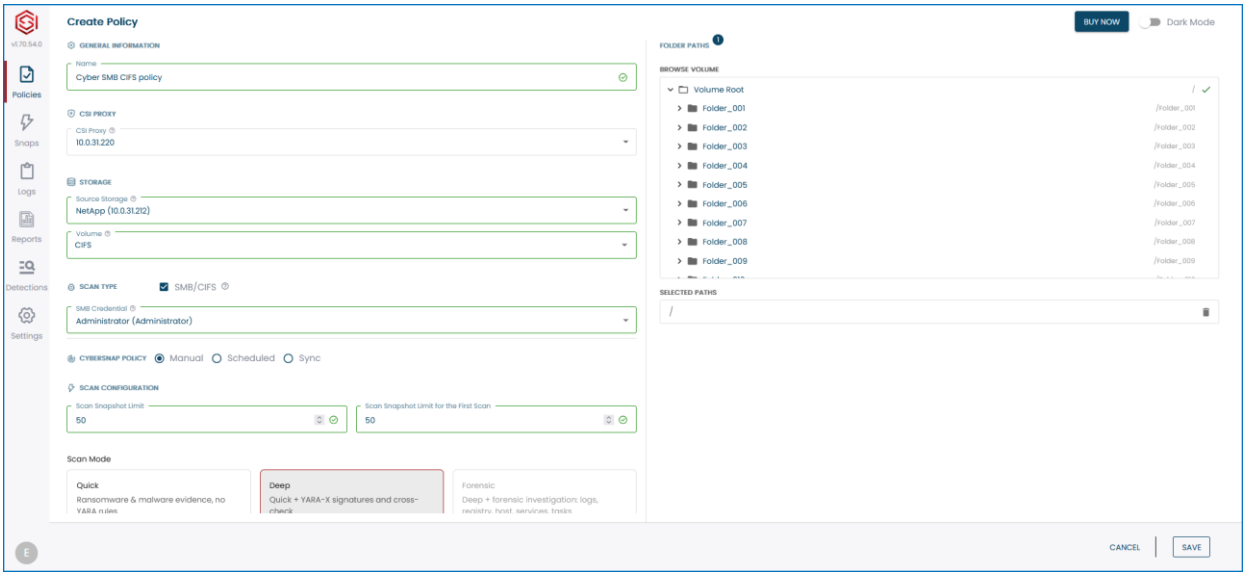
Select the scan type. In the Scan Type section, select the SMB/CIFS checkbox. The user interface automatically updates to display the configuration settings required for this scan type.

Enter a name for the policy. If only one vCenter and one Proxy or Storage system were configured on the Welcome screen during the initial setup, they are selected automatically. Otherwise, select the appropriate Proxy and Storage system from their respective drop-down lists.

Select the SMB/CIFS volume and credentials. Select the SMB/CIFS volume, then proceed to the next section to select the appropriate credentials. Once the credentials are selected, the system automatically loads the folder structure in the right-hand pane.

Select the folders to scan. In the folder tree, select either the top-level (root) folder as the starting point for the scan or one or more specific subfolders to include in the scan. Selecting specific subfolders allows the policy to focus on only the required data set.

Review and save the policy. After selecting the desired folders, review the configuration settings and save the policy.



Executing the Policy

In the chapter "Configuring CyberSnap Policy", we presented an overview of the triggering methods for defined policies. Within the CyberSnap Console, you have the flexibility to configure policies for either automatic or manual execution. The primary distinction between these two methods lies in the fact that the automatically configured policy is activated by the system, whereas the manually configured policy is activated by the end user.

Note: CyberSnap does not currently support the concurrent execution of multiple policies initiated by different CyberSnap servers against the same iSCSI/FC volume. This limitation is due to the VMware iSCSI/FC VMFS datastore attachment mechanism

Executing Policy Manually

Navigate to the Policies section, select the desired policy, and click on the three dots. From the ensuing popup menu, choose "Run Scan".

Executing Policy Automatically

Automatically executed policies can be Scheduled or Sync. Here we'll delve into further details.

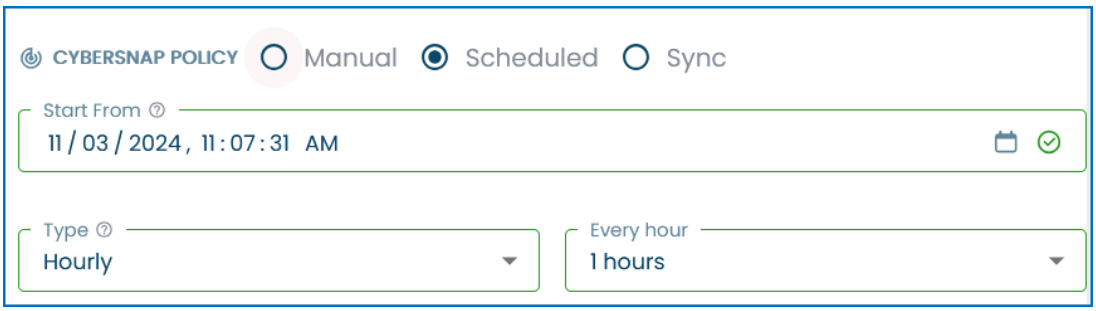
Scheduled option

Start from: The first setting to configure is the 'Start from' date and time, which specifies when the defined policy will be executed for the first time. It allows for the creation of a policy today with scheduling for future activation. If immediate activation is desired, retain the suggested date and time. Note that this is a one-time configuration for policy activation and cannot be altered in the future.

Execution Frequency: Next, define the execution frequency post-activation for the automatic scanning. The options are hourly, daily, weekly, or monthly. Here's a brief on each:

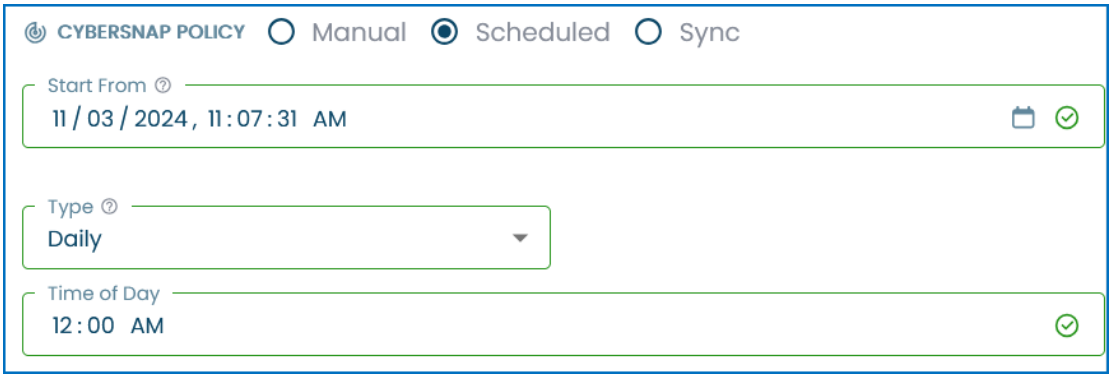
Hourly Execution

Select the 'Hourly' option and specify the repeating interval in hours. The interval range is one to twenty-three hours. You can specify the policy's initial run time, after which the policy scheduler will repeatedly execute according to the defined timeframe.



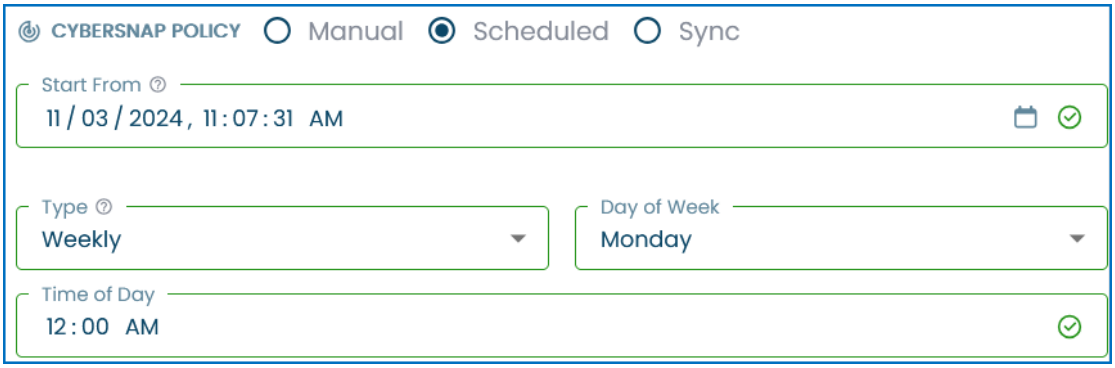
Daily Execution

With the 'Daily' option, specify the time for the scanning process. The time set pertains to the following day from when the policy is activated.



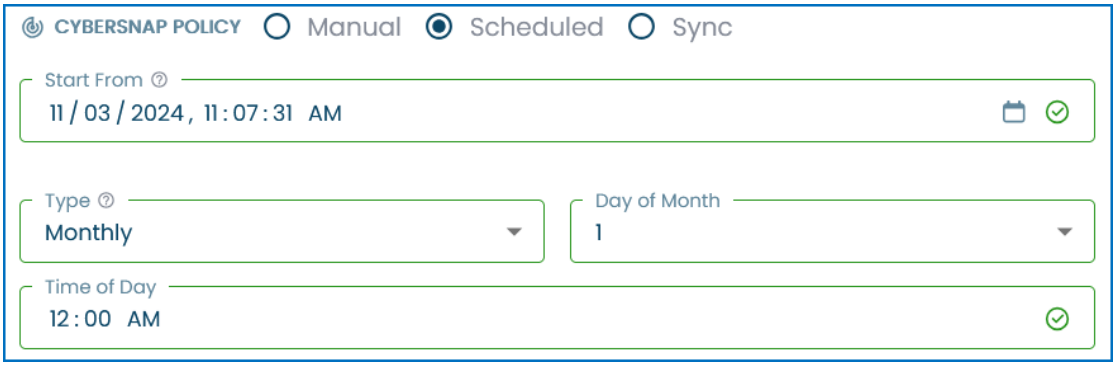
Weekly Execution

For 'Weekly' execution, indicate the day of the week and the specific time for scanning. Note that if the selected day precedes the 'Start From' day, the policy will trigger the following week.



Monthly Execution

Select the 'Monthly' option, specify the day of the month and the time for scanning. If the selected day is prior to the 'Start From' day, the policy will activate the following month.



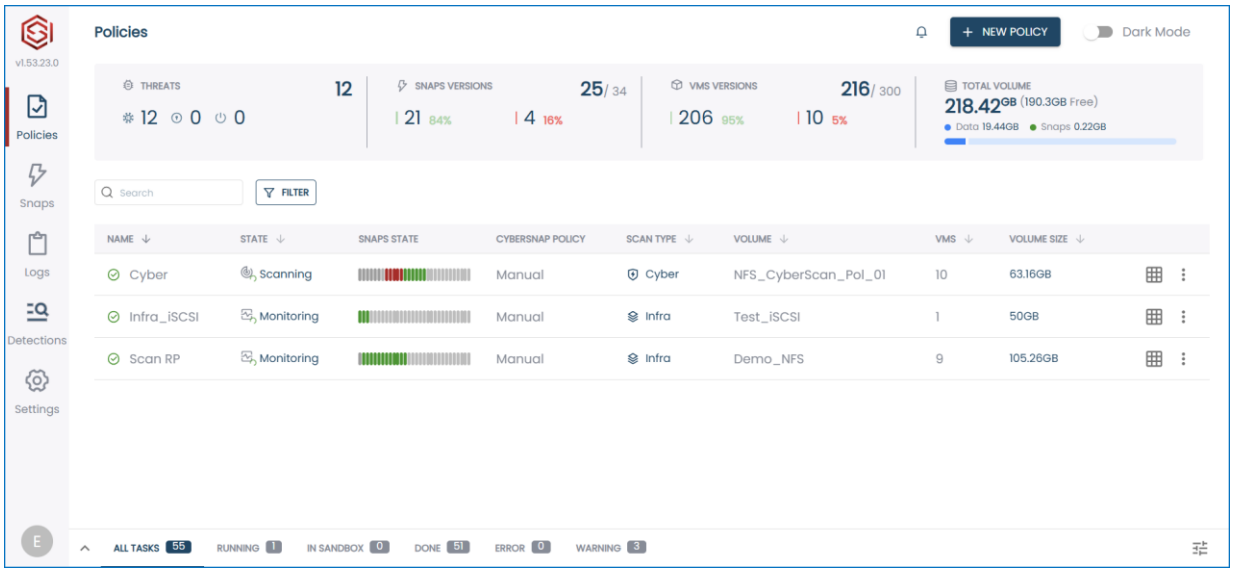
With the understanding of scheduler options in policy settings, configure the date and time that suits your needs. Post configuration, CyberSnap will initiate the policy and commence scanning at the specified times.

Sync option

For policies with the Sync option enabled, the system will periodically scan the NetApp storage for new snapshots. Once a new snapshot is detected, it will be automatically processed, and the data will become available in CyberSnap.

Policies

Upon navigating to the 'Policies' section in the CyberSnap console, the Policy details page will become available. This page allows you to review the various policies you have established. The following attributes for each policy are displayed on this page:



- **Name**: This field showcases the name you assigned to the policy during its creation phase.
- **State**: The current status of the policy is depicted here.
- **Snaps State**: Here, you will find the status of the last 30 snapshots. The color-coded indicators provide a visual cue regarding the state of virtual machines:
    - Green symbolizes that all virtual machines are in a good state.
    - Red implies that at least one virtual machine is not in a satisfactory state for the chosen snapshots.
    - Grey denotes an unknown state for selected snapshots and virtual machines.
- **CyberSnap Policy:** Represent how the system will activate the policy.
- **Scan Type:** Displays the configured threat policy type.
- **Volume**: The name of the volume as registered in NetApp is presented in this field.
- **VM**: This field displays the count of virtual machines you have selected within the specified policy.
- **Volume Size**: The capacity of the registered NetApp volume is shown here.

This organized layout facilitates a straightforward review and monitoring of your created policies, aiding in efficient management of your CyberSnap environment.

Policy ribbon

In the CyberSnap console, the Policies ribbon serves as a dashboard for overseeing the collective data across all active policies. It's segmented into four distinct sections, each providing a snapshot of different aspects of policy performance and status.

THREATS

Within the 'Threats' section, you can view the number of VMs across all policies that have cyber findings, including suspicious files.

SNAPS VERSIONS

This overview provides a high-level snapshot of all the volumes scanned across different policies within CyberSnap. It's designed to give you a quick status check of the overall system health.

- **Main Number**: At the top, you'll see the cumulative number of snapshots scanned across all policies. This aggregate figure helps you understand the breadth of your snapshot analysis.
- **Good Snaps (Green Line/Number)**: Below the main number, there's a tally of the snapshots where all VMs have passed the consistency check — meaning every VM could be registered and powered on. This is demarcated with a green line, indicating operational snapshots.
- **Bad Snaps (Red Line/Number)**: Adjacent to the good snaps count, you'll find the number of snapshots where at least one VM did not meet the consistency check. These are indicated with a red line, signaling attention may be needed for specific snapshots within this category.

This overall view is crucial for quick assessments and understanding the scope of snapshot integrity across the entire system managed by CyberSnap.

VMS VERSIONS

In the 'VMS Versions' section of the CyberSnap interface, you'll find comprehensive data concerning the state of virtual machines across all snapshots and policies:

- **Overall VM Status**: This gives you the total number of virtual machines scanned within the scope of all CyberSnap policies, offering a broad view of the virtual infrastructure being monitored.
- **Good VMs (Powered On - Green Line)**: Here, virtual machines that were successfully powered on and passed the consistency check are listed. They're considered 'good', and their count is shown with a green line, indicating operational VMs across all policies.
- **VMs with Issues (Powered Off - Red Line)**: Contrarily, VMs that couldn't be powered on, for any reason, during the scanning process are flagged. Their count is marked with a red line, and these are considered 'not in good state', signaling potential problems or areas for further investigation.

TOTAL VOLUME

The 'TOTAL VOLUME' segment of the CyberSnap interface provides a summary of storage metrics across all defined policies, offering a clear picture of how storage space is allocated and utilized within your NetApp volumes. Here's how the information is broken down:

- **Total Volume Size**: This metric showcases the sum of the capacities of all the volumes included within your policies. It's a gauge of the storage scope you're managing with CyberSnap.

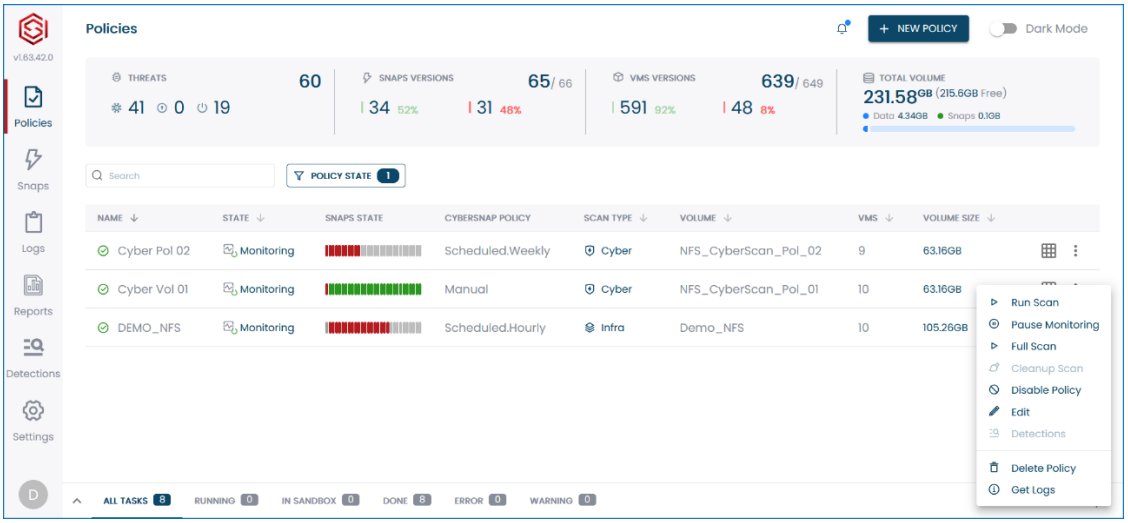
- **Storage Used**: Indicated by a blue line in the visualization, this figure denotes the actual amount of storage space currently being utilized across all volumes. It's an important measure of your existing storage footprint.
- **Snapshots Used**: Represented with a green line, this number reveals the cumulative storage space that all the snapshots are taking up. Snapshots are crucial for data protection and recovery processes, and this metric helps in understanding their impact on storage.

The combination of 'Storage Used' and 'Snapshots Used' is visually represented on a ribbon and provides a quick reference for understanding how much of your storage capacity is actively in use versus how much remains available.

- **Available Space**: The remaining storage capacity, or the 'Available' space, is visualized with a grey line. This number is the difference between your total volume size and the 'Used' space, giving you insight into the potential for additional data storage or the need for capacity planning.

Policy menu options

In CyberSnap, each policy you create comes with a set of actions that you can perform to manage and control the policy's behavior. These actions are found in a contextual menu at the end of each policy's row in the policies list, which is accessed by clicking on the three dots. Here's a description of each option available in this menu:



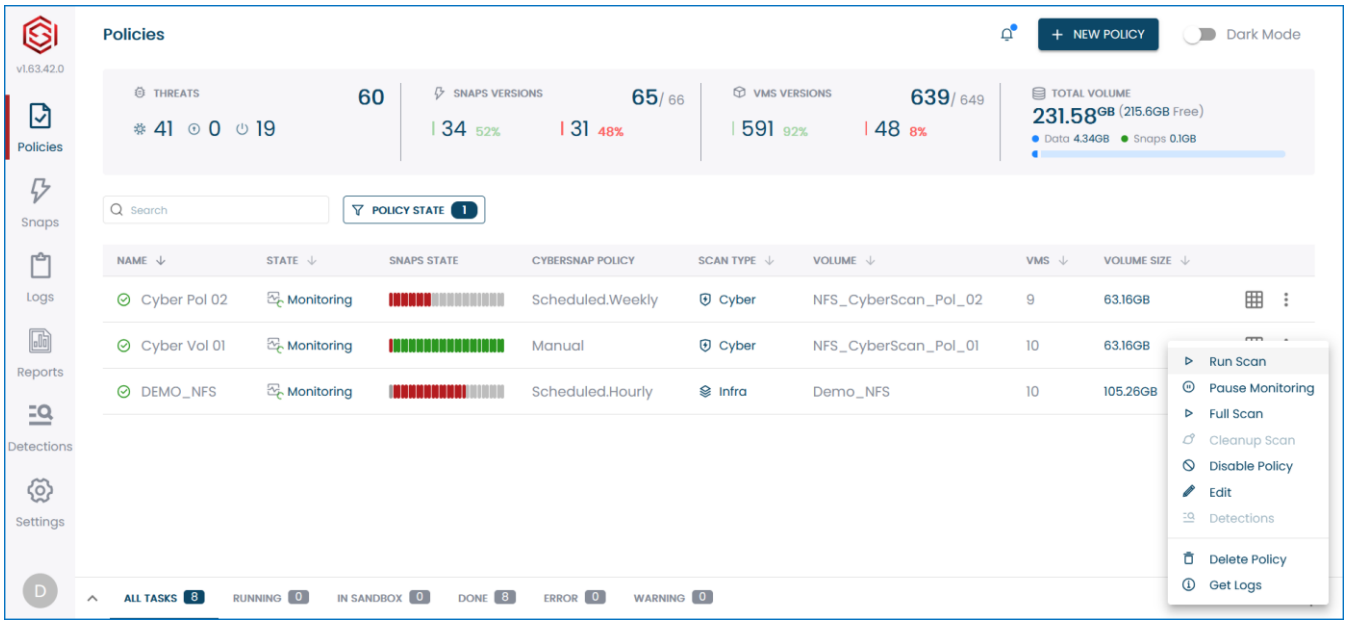
- **Run Scan**: Initiates a manual scan of the virtual machines as per the policy's parameters, allowing you to perform an immediate consistency check outside the scheduled scans.
- **Stop Scan**: Available only when a scan is actively running, this lets you halt the scan process. A confirmation step ensures you're making an intentional choice to stop the scan and begin cleanup operations.
- **Pause Monitoring**: If the policy is currently being monitored, you can pause this monitoring. It's useful for temporary suspensions without altering the policy's configuration.
- **Resume Monitoring**: Available only when Monitoring is paused. Reverses the pause action, resuming any monitoring operations that were previously active for the policy.

- **Full scan**: Initiates a complete rescan of the selected policies. All previously collected data will be discarded and re-collected from scratch. A confirmation prompt will appear, requiring approval before deleting existing data and starting the scan anew.
- **Cleanup Scan**: After a scan, you may have residual virtual machines or data that need to be cleaned up. This option automates the process to ensure your environment remains uncluttered.
- **Disable Policy**: Temporarily turns off the policy without deleting it, which means no scans or monitoring will take place until it's enabled again.
- **Enable Policy**: Available only when the Policy is disabled. Reactivates a disabled policy, returning it to active status where scans and monitoring can occur according to its configuration.
- **Edit**: Allows you to make changes to the policy's settings, such as altering the schedule, adjusting the scope of virtual machines, or changing snapshot retention rules.
- **Detections**: Allows you to navigate to the Detection view, automatically filtered by the selected policy.
- Delete Policy: Allows you to permanently delete policies that are no longer needed. Please note that deleting a policy is irreversible, and you will no longer be able to access its previous scan results.
- **Get logs**: Enables you to automatically collect logs for the desired policy.

These options provide flexibility in managing your disaster recovery and backup processes, ensuring that you can react to changes in your environment or operational requirements quickly and efficiently.

Executing Policy Scan Manually

To execute the policy scan manually, click on the three dots and select 'Run Scan' to start data collection from the Storage appliance immediately. The policy state in the CyberSnap console will change to ‘Scanning’, indicating data collection is in progress. Monitor this process in the task list at the console bottom by clicking on the ‘RUNNING’ filter in the task view.



Wait for the scanning process to complete. The duration varies based on the snapshots number and the virtual machines quantity on the selected volume. In 'Chapter SNAPS', we will detail the scanning results and the data presented in the 'SNAPS' menu of the CyberSnap console.

Scanning Process Overview

The outcome is identical whether the policy is started automatically or manually from the VMware vCenter perspective. The CyberSnap scanning process utilizes data from NetApp storage to inspect each virtual machine from all discovered snapshots and attempts to register the virtual machine in the VMware vCenter Inventory to power it up, without enabling the network adapter to avoid potential duplicate IP issues.

Note: NETAPP

During the scanning process, CyberSnap creates temporary storage objects. These temporary storages are named in the format “CSI_Scan_[VolumeName]”, indicating the volume creation by CyberSnap. After scanning, CyberSnap unmounts the datastore from VMware and deletes it from NetApp.

Note: VMware vCenter

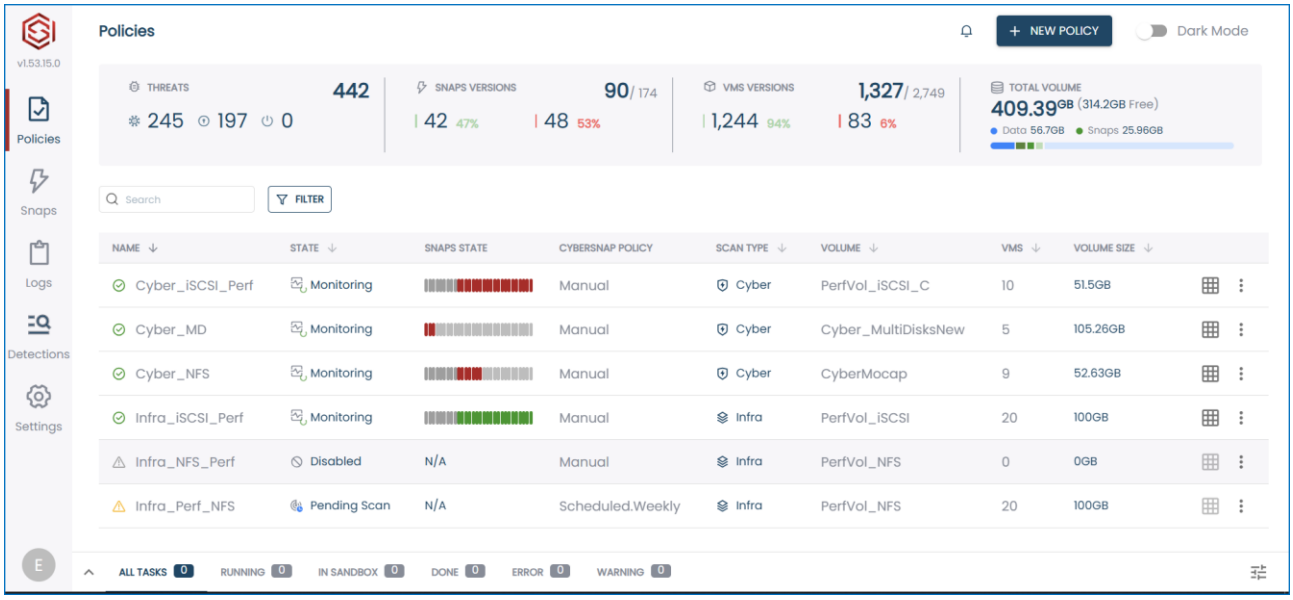
Temporary pop-ups of new datastores and virtual machines can be observed during the scanning process. Virtual machines follow the naming convention: “CSI_Scan_[ServerName]*[SnapshotName]*[Version]”, where:

- CSI_Scan is a prefix indicating the virtual machine belongs to the scanning process.
- ServerName is the server name as defined in the VMware vCenter.
- SnapshotName is the NetApp snapshot name created from two parameters: Date (in YYYYMMDD format) and Time (in HHMMSS format) representing when the snapshot was created.

Post scanning, the virtual machine and datastore will be removed from the VMware vCenter inventory.

SNAPS

After the scanning process concludes, CyberSnap updates the policy status to 'Monitoring'. This status change is reflected within the Policies section of the CyberSnap Console, where you can see a high-level summary of the scan results.



By clicking on the grid icon, which is situated next to the three-dot menu for the policy, the 'Snaps' section of the CyberSnap Console will be opened. In this section, you're presented with a more granular view of the scan's outcomes, the SnapMap©.



When you navigate to the 'Snaps' view within the CyberSnap Console, you're greeted with a detailed interface designed to provide a comprehensive understanding of the state of your virtual machines (VMs) post-scan. This interface is split into several distinct sections, each offering a different perspective on your data:

- **Virtual Machine List**: On the left side, there's a list of all the virtual machines that are included in the snapshot policy. This list may include additional options for managing each VM, such as initiating recovery or further inspection tasks.
- **Statistical Ribbon**: At the top, you'll find a ribbon that aggregates the statistical data from the scan. This includes the number of VMs that have been scanned, the status of these VMs (powered on, consistent, etc.), and any other critical metrics that are relevant to the snapshots' integrity and the VMs' viability.

- **SnapMap ©**: The main area of the 'Snaps' section features a color-coded map. This map visually conveys the results of the scanning process. Each color corresponds to a different status of the VMs within a snapshot: for instance, green may indicate VMs that are in a good state, while red may signal issues that were detected during the scan.

Virtual Machine List

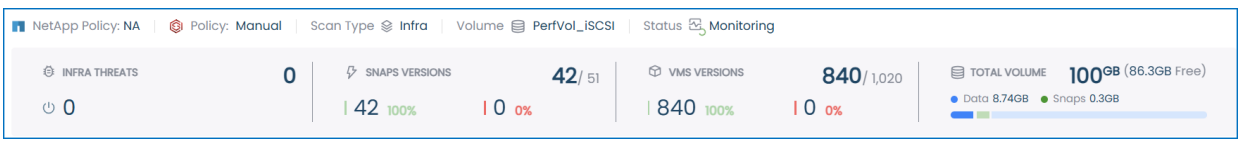
Here's what you can expect to see and do within this section:

- **Virtual Machine Listing**: This area lists all the VMs that were selected during the policy's creation or later modification. This comprehensive listing helps you keep track of all the VMs under a particular policy.
- **VM Count**: At the top of the VM list, you'll notice a tally indicating the total number of VMs included in that specific policy. This gives you a quick reference to the scope of the policy's coverage.
- **Date Picker**: A tool is available that lets you select a specific time frame for which you want to view data. This can be useful for analyzing trends over time or focusing on a particular incident window. The chosen time and date will filter the view from the present moment backward in time.
- **Visibility Toggle**: An 'Eye' icon is present, which allows you to toggle the visibility of deleted snapshots within the current map view. This can help declutter the interface and focus on the most relevant data.
- **Sandbox Recovery**: Next to each VM's name, three dots provide access to a menu where you can initiate the Sandbox recovery process for that VM. This function is crucial for testing and verification purposes in a safe environment.
- **Snapshot Management**: Along the snapshot column, three dots provide additional snapshot-specific options:
    - **Sandbox Option**: Start the VM recovery process directly from a snapshot.
    - **Keep Snapshot**: Selecting 'Keep' signals CyberSnap to instruct NetApp to prevent the chosen snapshot from being deleted, effectively protecting it. An icon will appear indicating the snapshot is protected. Later, if the protection is no longer required, you can select 'Unkeep' from the menu to remove this safeguard, and the icon will disappear, reflecting this change.

The Ribbon

The snaps ribbon serves as a dashboard for overseeing the collective data of the active policy. It's segmented into four distinct sections, each providing a snapshot of different aspects of policy performance and status.

Above the ribbon, CyberSnap will display the schedule settings for snapshot copies from both the NetApp Storage policy and the CyberSnap policy. If no schedule is configured, the ribbon will show a "Not Scheduled" alert.



INFRA THREATS

Under the ‘Infra Threats’ section, you can view the number of VMs in the selected policy that were scanned and identified as unable to Power On.

SNAPS VERSIONS

This is the detailed, policy-specific view that allows administrators to delve into the state of snapshots for a particular volume associated with a policy. It offers a focused analysis on a per-policy basis:

- **Main Number**: Displayed at the top, it shows the total number of snapshots that have been scanned within this specific policy. This detail informs you about the extent of analysis performed for this policy's volume.
- **Good Snaps (Green Line/Number)**: Directly below the main figure, the count of snapshots where all VMs within them are consistent and operational is shown with a green line. This denotes that these snapshots are reliable for restoration purposes.
- **Bad Snaps (Red Line/Number)**: This count is positioned next to the good snaps and indicates the number of snapshots within the policy where at least one VM failed the consistency checks, underscored by a red line for visibility.
-

This individual policy view is pivotal for in-depth analysis and understanding the integrity of each snapshot within a specific policy, enabling targeted action and management within CyberSnap.

VMS VERSIONS

In the 'VMS Versions' section of the CyberSnap interface, you'll find comprehensive data concerning the state of virtual machines across all snapshots of the selected policy:

- **Overall VM Status**: This gives you the total number of virtual machines scanned within the scope of all CyberSnap policy, offering a broad view of the virtual infrastructure being monitored.
- **Good VMs (Powered On - Green Line)**: Here, virtual machines that were successfully powered on and passed the consistency check are listed. They're considered 'good', and their count is shown with a green line, indicating operational VMs across all policies.
- **VMs with Issues (Powered Off - Red Line)**: Contrarily, VMs that couldn't be powered on, for any reason, during the scanning process are flagged. Their count is marked with a red line, and these are considered 'not in good state', signaling potential problems or areas for further investigation.

TOTAL VOLUME

The 'TOTAL VOLUME' segment of the CyberSnap interface provides a summary of storage metrics of a volume in the selected policy, offering a clear picture of how storage space is allocated and utilized within your NetApp volume. Here's how the information is broken down:

- **Total Volume Size**: This metric showcases the sum of the capacities of a volume included within your policy. It's a gauge of the storage scope you're managing with CyberSnap.
- **Storage Used**: Indicated by a blue line in the visualization, this figure denotes the actual amount of storage space currently being utilized across the volume. It's an important measure of your existing storage footprint.
- **Snapshots Used**: Represented with a green line, this number reveals the cumulative storage space that all the snapshots are taking up. Snapshots are crucial for data protection and recovery processes, and this metric helps in understanding their impact on storage.

The combination of 'Storage Used' and 'Snapshots Used' is visually represented on a ribbon and provides a quick reference for understanding how much of your storage capacity is actively in use versus how much remains available.

- **Available Space**: The remaining storage capacity, or the 'Available' space, is visualized with a grey line. This number is the difference between your total volume size and the 'Used' space, giving you insight into the potential for additional data storage or the need for capacity planning.

SnapMap ©

The meaning of the data shown in the SnapMap depends on the policy type. Here, we will describe the main differences between policy types.

Infra Policy

For Infra policy type SnapMap © visualizes the consistency of snapshots and virtual machines (VMs) over time, providing insights into the state of volumes and VM snapshots. The map is refreshed by two main activities: scanning and monitoring. Scanning assesses snapshot and VM consistency, using green to mark recoverable VMs and red for non-recoverable ones. Monitoring, which runs continuously in the background, syncs the state of NetApp snapshot policy with the map, adding new snapshots for scanning and removing deleted ones.

An initial scan can be executed either manually or on a set schedule, analyzing up to 50 past snapshots. Subsequent scheduled scans keep the map current with the latest snapshot and VM consistency statuses. Scan results are color-coded on the map as follows:

- Red indicates that an attempt was made to Power On the VM in the snapshot, but it was unsuccessful.
- Green indicates that the VM was successfully powered on.
- Grey signals VMs that have not been scanned, have been deleted, or migrated out of the volume, thus their state is unknown.

If all VMs in a policy are successfully powered on, the snapshot column will remain unmarked. However, if any VMs were powered off (indicating a failed power-on attempt) during the scan, a red dot will appear at the top of the snapshot column to signal that at least one unsuccessful VM was detected.



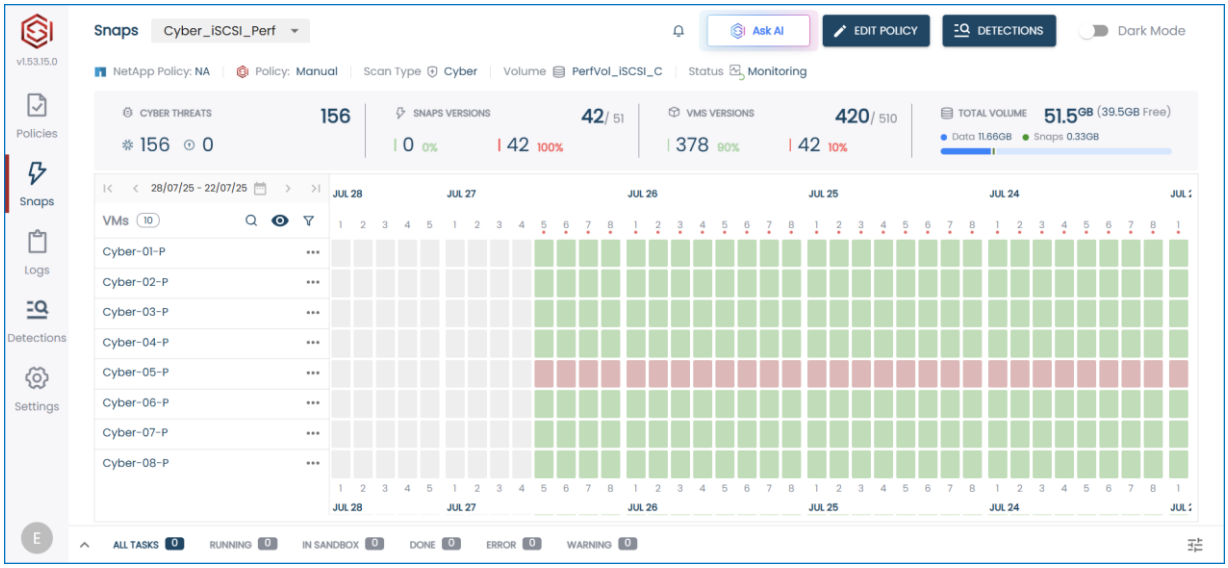
Cyber Policy

SnapMap © visualizes the cybersecurity status of snapshots and virtual machines (VMs) over time, offering visibility into the threat landscape across volumes and VM snapshots. The map is continuously updated through two core processes: scanning and monitoring. Scanning inspects snapshots and VMs for cyber threats—green indicates no malicious activity was detected, while red flags critical findings such as malware, ransomware, or similar threats. Monitoring runs persistently in the background to align the map with the current state of the NetApp snapshot policy, automatically adding new snapshots for scanning and retiring those that have been deleted.

An initial scan can be executed either manually or on a set schedule, analyzing up to 50 past snapshots. Subsequent scheduled scans keep the map current with the latest snapshot and VM consistency statuses. Scan results are color-coded on the map as follows:

- Red indicates that CyberSnap scanned all disks of all virtual machines across all snapshots and detected suspicious files.
- Green indicates that the VM was scanned, and no threats were found.
- Grey signals VMs that have not been scanned, have been deleted, or migrated out of the volume, thus their state is unknown.

If all virtual machines in a selected snapshot are marked green, the snapshot column remains unmarked. However, if any virtual machine is marked red, a red dot appears at the top of the snapshot column to indicate that at least one virtual machine is flagged.



To effectively analyze the findings in the SnapMap of a Cyber Policy, you can use the 'Ask AI' button, which generates multiple reports based on the details of the findings. To generate these reports, the CyberSnap Proxy server must have Internet access to utilize the AI agent, which provides additional insights.

CyberSnap AI reports

The following reports are generated by AI Agent when you click on the 'Ask AI' button.

Summary Report

The summary report outlines the number of snapshots and virtual machines that were analyzed. If risky files are detected, the AI estimates their impact across affected snapshots. The report also provides an overall assessment of the threat level.

Assessment Section

The report may indicate that multiple instances of malware have been detected across virtual machine snapshots. This information helps assess the potential impact on operations.

Recommendation Section

Users will see recommended actions such as isolating affected servers, reviewing detection details, and initiating recovery steps.

Severity Assessment Overview

The severity assessment provides a high-level summary of the potential impact of detected issues. Each assessment includes the following key indicators:

- Overall Severity: Indicates the criticality of the situation based on the findings. For example, a *Critical* rating suggests immediate attention is required.
- Data Loss Risk: Reflects the likelihood of permanent data loss. A *High* rating signals that important data may be at risk if not addressed promptly.
- Recovery Complexity: Describes the expected difficulty of restoring affected systems. A *Complex* rating may imply that recovery efforts will require significant coordination and resources.

- Business Impact: Summarizes potential consequences for operations. This may include service disruption, data unavailability, or financial losses, depending on the nature of the incident.

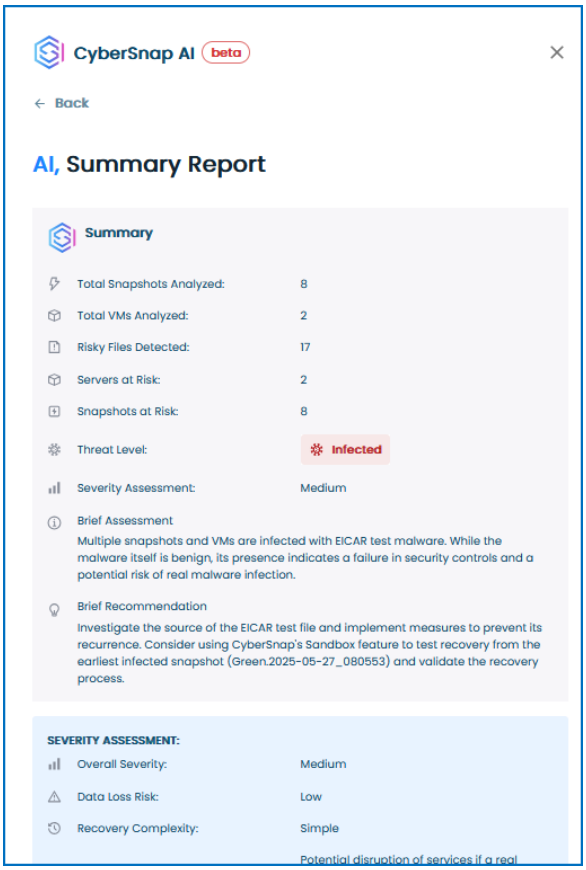
These indicators help users quickly understand the urgency and scope of a detected issue and guide appropriate response actions.

Validate Threats

The threat validation section provides detailed insight into the accuracy and reliability of the detected threats. It includes the following key metrics:

- **True Positives**: The number of confirmed malicious detections. A higher number indicates widespread presence of known threats across the scanned environment.
- **False Positives**: The number of detections mistakenly identified as threats. A value of *0* suggests a high level of detection precision.
- **Confidence Score**: A numerical value representing the system's confidence in the accuracy of the threat classification.
- **Explanation**: Provides context for why the threats were classified as true positives. This may be based on factors such as YARA rule matches, known malicious file extensions, or filenames commonly associated with ransomware.

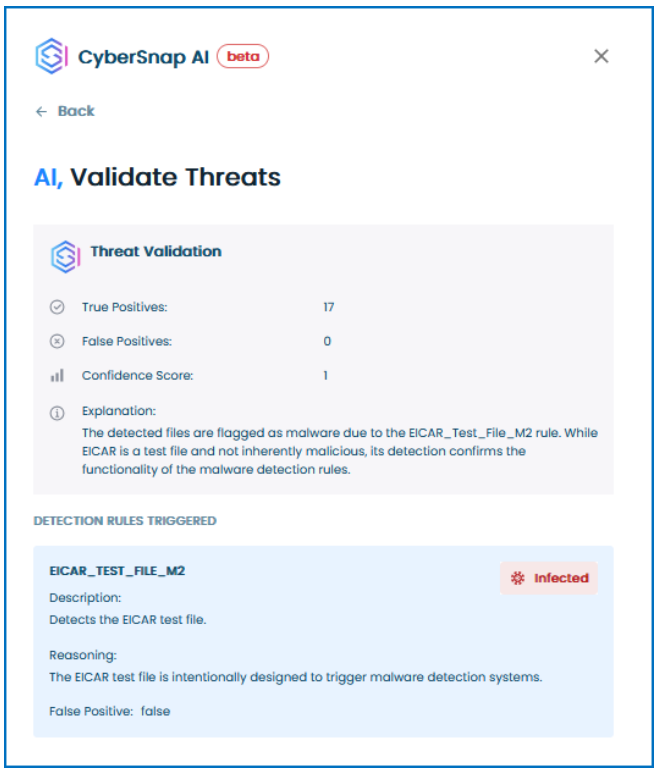
An example of the Summary Report is shown below.



Detection rules triggered

This section lists the specific detection rules activated during the scan. Each rule includes a name, description, reasoning behind the detection, and an indication of whether it is likely to be a false positive. Detections are typically based on known malware signatures, behavioral patterns, or threat intelligence, providing clear justification for each triggered rule.

An example of the Validate Threats Report is shown below.



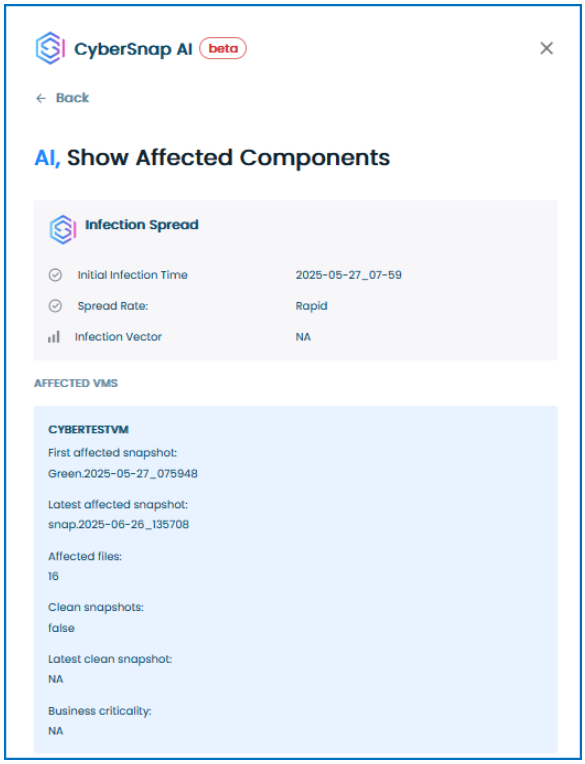
Show Affected Components

This section of the report provides an overview of the infection's progression within the environment. It highlights key details such as the initial infection timestamp, the rate at which the infection is spreading, and the infection vector if identified. For example, users can see when the infection was first detected, whether its spread rate is low, medium, or high, and any available information on how the infection propagated. If the infection vector remains unknown, that will also be indicated. This information helps users understand the scope and dynamics of the threat for informed response actions.

Affected VMs

This section lists virtual machines that have been impacted by the detected threat. For each VM, the report shows the first and latest snapshots where the infection was observed, the number of affected files found, and whether any clean snapshots are available. If no clean snapshots exist, this is noted accordingly. Business criticality information, if provided, helps prioritize response efforts based on the VM’s importance to operations. This overview enables users to quickly identify compromised VMs and assess their infection timeline and scope.

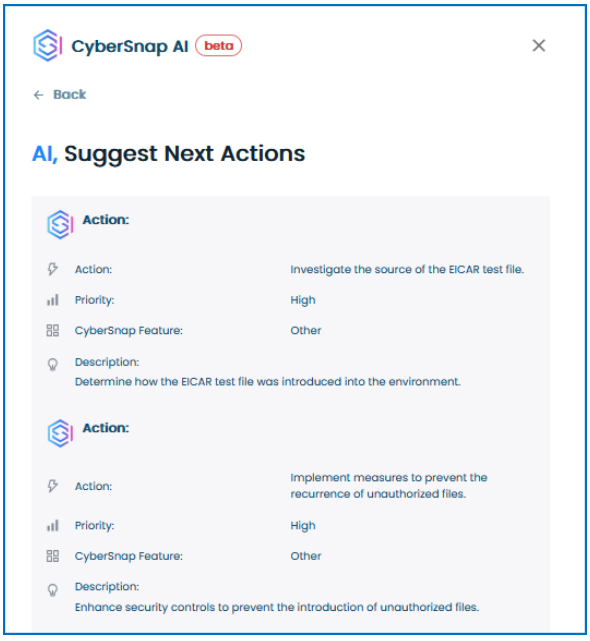
An example of the Show Affected Components Report is shown below.



Suggest Next Actions

This section outlines the recommended actions to mitigate detected threats, clearly emphasizing the priority of each step to guide timely response. Each action includes a detailed description explaining its purpose, the relevant CyberSnap feature involved, and the specific targets such as affected servers or components. Prioritizing and following these suggestions helps prevent further damage and supports effective threat containment and recovery.

An example of the Suggest Next Actions Report is shown below.

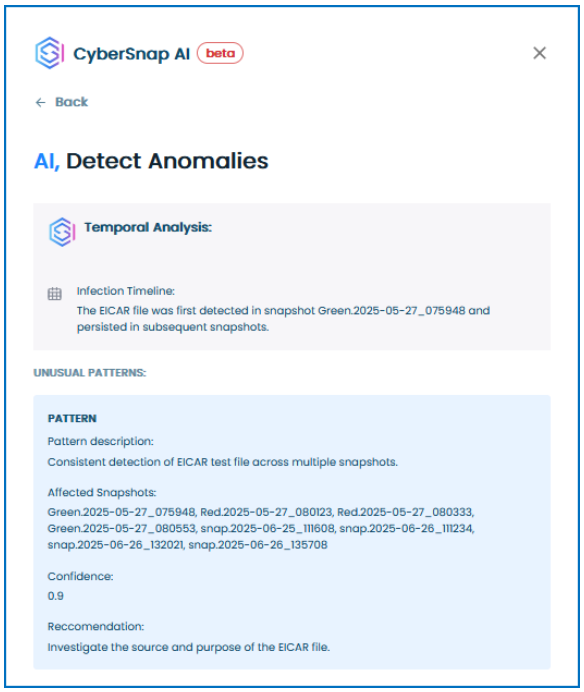


Detect Anomalies

The system performs temporal analysis of virtual machine snapshots to identify anomalous activity patterns that may indicate compromise. It reconstructs infection timelines to determine when suspicious behavior first appeared and how it evolved over time. Key indicators include spikes in file encryption, file creation, and malware detections, which help pinpoint critical events. These indicators also help correlate suspicious activity and identify potential stages of an attack.

Additionally, the system detects unusual patterns, such as a rapid increase in encrypted files across multiple snapshots. These patterns are flagged with a confidence score to help prioritize investigation. Users can review affected snapshots where anomalies were detected to better understand the scope and timing of the issue.

An example of the Detect Anomalies Report is shown below.



Analyze Threat Details

This section offers a detailed overview of identified threats through Indicators of Compromise (IoCs). It summarizes:

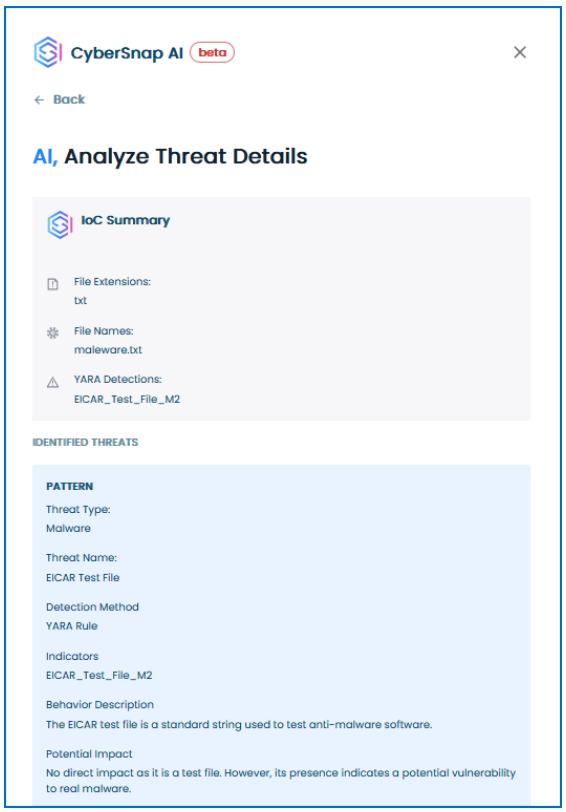
- **File Extensions:** Types of file extensions commonly associated with malicious activity.
- **File Names:** Suspicious filenames often linked to ransom notes or malware.
- **Common Patterns:** Typical behaviors observed, such as encrypted files and ransom message artifacts.
- **YARA Detections:** Specific threat signatures matched by YARA rules.

Additional information includes:

- **Threat Type:** The classification of the threat, for example, ransomware.
- **Threat Name:** The identified or unknown label of the threat.
- **Detection Method:** Techniques used to detect the threat, including file extension analysis and signature matching.
- **Indicators:** Key signs of compromise like suspicious file extensions and ransom-related filenames.
- **Behavior Description:** How the threat operates, such as encrypting files and leaving instructions for ransom.
- **Potential Impact:** Possible consequences, including data loss, system interruptions, and financial damage.

This analysis helps users comprehend the characteristics, detection, and risks of threats to support effective incident response.

An example of the Analyze Threat Details Report is shown below.



Disclaimer: The content in this *CyberSnap AI Reports* section is provided **"as is"** and may include information generated by artificial intelligence (GenAI). We reserve the right to modify or update this content at any time without prior notice.

Sandbox

CyberSnap is engineered to create a self-contained Sandbox environment, providing a secure and isolated arena for examining and analyzing the content within your virtual machines without jeopardizing your actual production system. Below are some notable applications:

1. **Cyber Investigations:**
    - Utilizing a sandbox created from snapshots, you can delve into anomalies, vulnerabilities, or incidents within a segregated environment. This facilitates the assessment of impact, comprehension of behavior, and potential identification of cyber threat sources without endangering your live environment.

2. **Forensic Analysis:**
    - The sandbox serves as a conducive space for scrutinizing the behavior of applications, files, or scripts suspected of malicious activity. It offers a secure domain where investigators can conduct thorough analyses without the risk of evidence contamination or adverse effects on the main infrastructure.

By harnessing CyberSnap's capability to map all NetApp snapshots to a VMware volume, you can effortlessly establish sandboxes for these pivotal tasks, thereby augmenting the security and robustness of the system. In the 'Snaps' menu of the CyberSnap Console, not only can you view the scanning results for the desired volume and selected virtual machine, but you can also kickstart the Sandbox process.

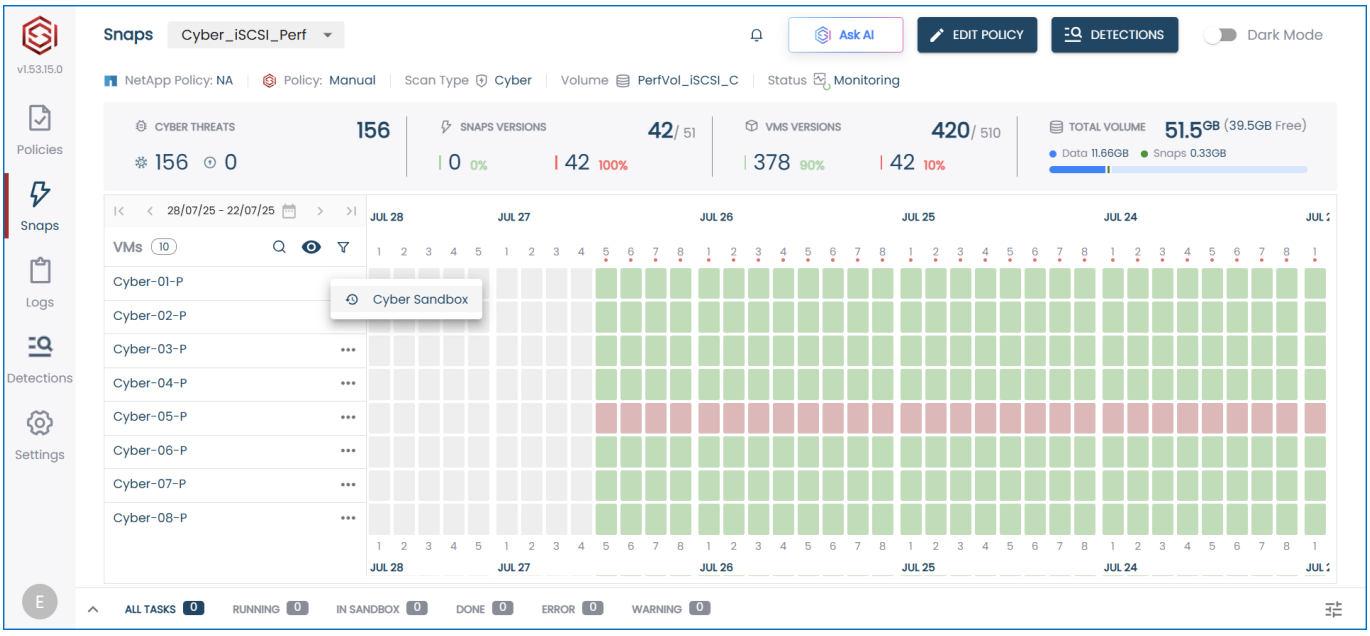
Initiating Sandbox Processes:

You have the option to initiate one of three Sandbox processes:

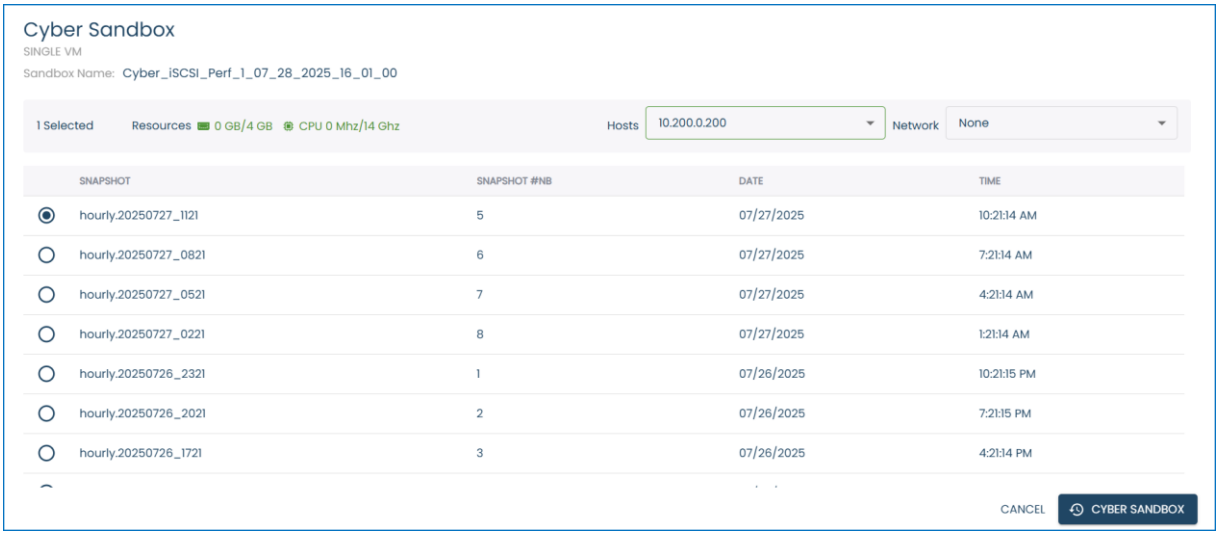
- **Sandbox of Selected Virtual Machine:** Create a sandbox environment for a specific virtual machine.
- **Sandbox of Selected Snapshot:** Establish a sandbox using a selected snapshot for a specific date and time.
- **Sandbox of Single or Multiple Virtual Machines: Customize your sandbox environment by selecting** single or multiple virtual machines based on your preference.

Single VM Sandbox

To initiate the Sandbox for a selected VM, click on the three dots on the right side of the virtual machine's name. A menu will pop up with the option 'Cyber Sandbox'.

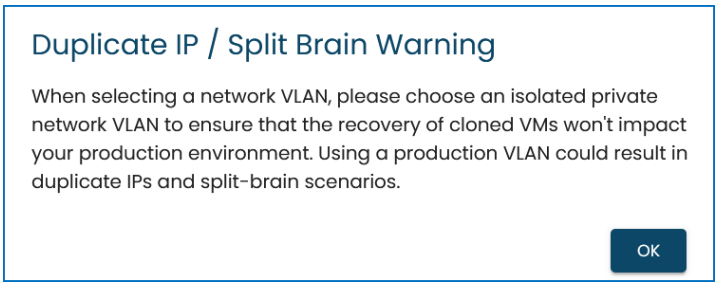


Upon clicking on the 'Cyber Sandbox' option, a new window will appear where you can select the storage snapshot policy from which you want to recover the virtual machine.



At the top of the Cyber Sandbox interface, you'll find the necessary resources for the chosen snapshot policy and selected VM. Green indicates that on the selected host(s), there are enough resources to recover all virtual machines. Red colored resources mean you should be aware that starting the Sandbox process with all virtual machines could affect resource availability on the selected ESXi host. In the hosts dropdown menu, you must choose the desired host to which you wish to recover the selected VM.

In the networking selection dropdown list, you have the option to either leave the default selection as 'None,' indicating that the recovered VM will not be connected to the network, or to choose the desired network to which you want to connect the VM after the recovery process is completed. When selecting the desired network for the recovered virtual machine, a notification window will appear to remind you of potential impacts that may occur.



Before initiating the recovery process on the selected host(s), be aware that commencing the Sandbox process without adequate resources could impact the selected ESXi host's performance.

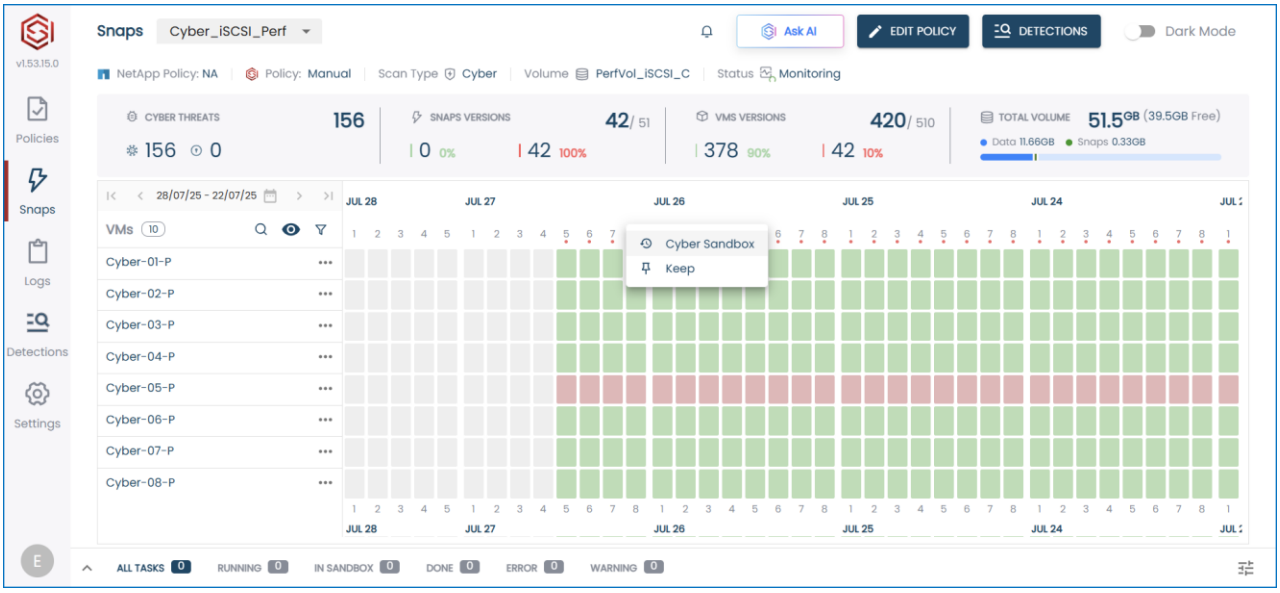
To initiate the recovery of the virtual machine and have it start without network connectivity, keep the default option as "None."

NOTE: If the preferred network is selected, ensure that there is no network connectivity between the production network and the network chosen from the drop-down menu to which the recovered virtual machine will be connected when powered on.

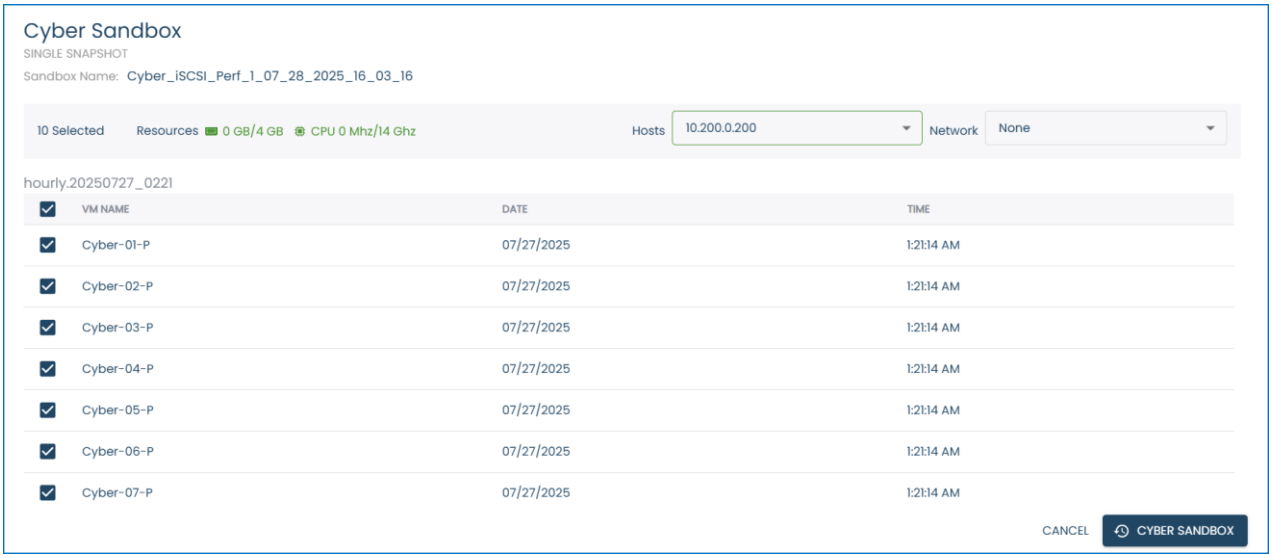
Now that you've selected the desired host and network, click on the 'CYBER SANDBOX' button located in the bottom right corner of the Cyber Sandbox window. The time needed to finish the recovery process will depend on your hardware and the availability of resources on the selected ESXi host. You can check the status of the recovery process in the task drawer. Additionally, during the recovery process, the Snaps map will display an animated view for each virtual machine undergoing recovery. Once the recovery process is complete, CyberSnap marks successfully recovered virtual machines in dark green. Otherwise, it will be marked with a dark red color to indicate an unsuccessful recovery process. After the recovery is finished, the selected job in the task drawer will be marked as “IN CYBER SANDBOX”. You can now access your restored VM from your VMware vCenter site.

Single Snapshot Sandbox

To initiate the Sandbox from the selected snapshot, click on the three dots at the top of the snapshot column. A menu will appear, click on the 'Cyber Sandbox' option in the menu.



A new window will appear, allowing you to verify if your selected host(s) have enough resources to recover all virtual machines from the selected snapshot. By default, all virtual machines will be preselected, but you have the option to deselect the ones you don't want to recover.



The guidance provided in the single sandboxing VM chapter regarding network selection also applies to scenarios involving multiple VMs. Please be aware that the chosen network will be implemented across all restored servers. If your virtual machines require different network settings, you will need to segment the recovery process into multiple sandboxes, each grouped by the specific network requirements. When you're ready, click on the “CYBER SANDBOX” button.

The duration required to complete the recovery process will depend on your hardware and the availability of resources on the selected ESXi host. You can check the status of the recovery process in the task drawer. Additionally, during the recovery process, the Snaps map will exhibit an animated view for each virtual machine undergoing recovery. Once the recovery process is complete, a successfully recovered virtual machine will be marked with a dark green color. Conversely, it will be marked with a dark red color to indicate an unsuccessful recovery process. After the recovery is completed, the selected job in the task drawer will be marked as “IN CYBER SANDBOX”. You can now access your restored VM from your VMware vCenter site.

Multi VMs Sandbox

Before diving into the Sandbox process, the first step is to decide which virtual machines you aim to recover. When you navigate to the Snaps map for the desired policy, you'll find all available virtual machines alongside their snapshots across various NetApp snapshot policies and times. Each green square on the map symbolizes a single virtual machine at a specified point in time. By clicking on a green square, you can select one or multiple virtual machines. A blue outline will appear around a green square, giving you a visual confirmation of the selected virtual machines on the map. Once you've selected the virtual machines you want to recover, click the "CYBER SANDBOX" button.



A new window will then emerge, offering a view to check if your selected host(s) have the necessary resources to recover all selected virtual machines from the chosen snapshot. If there's a resource shortfall, it will be highlighted in red; on the other hand, if the selected host has a sufficient amount of resources, they will be highlighted in green. When recovering more virtual machines than the number of hosts available in your environment select multiple hosts. This helps accelerate the recovery process and evenly distributes the workload across multiple hosts.

The guidance provided in the single sandboxing VM chapter regarding network selection also applies to scenarios involving multiple VMs. Please be aware that the chosen network will be implemented across all restored servers. If your virtual machines require different network settings, you will need to segment the recovery process into multiple sandboxes, each grouped by the specific network requirements.

Before you start the recovery process on the selected host(s), it's crucial to understand that launching the Sandbox process without enough resources could affect the performance of the selected ESXi host.

Now, to get the Sandbox process underway, click on the ‘CYBER SANDBOX’ button positioned at the bottom right corner of the Cyber Sandbox window. The duration required to wrap up the recovery process hinges on your hardware and the resource availability on the selected ESXi host. The status of the recovery process can be monitored in the task drawer. Additionally, as the recovery unfolds, the Snaps map will exhibit an animated view for each virtual machine in recovery. Upon completion, a successfully recovered virtual machine will be signified by a dark green color, while a dark red color will indicate an unsuccessful recovery process. Once the recovery phase concludes, the chosen job in the task drawer will bear the label “IN CYBER SANDBOX”. You can now access your restored VM from your VMware vCenter site.

Sandbox Result

Upon completion of the Sandbox process, CyberSnap will tag the virtual machine in the Snaps view. The tag, either dark red or dark green, serves as a visual cue for the status of the virtual machines involved in the recovery process.

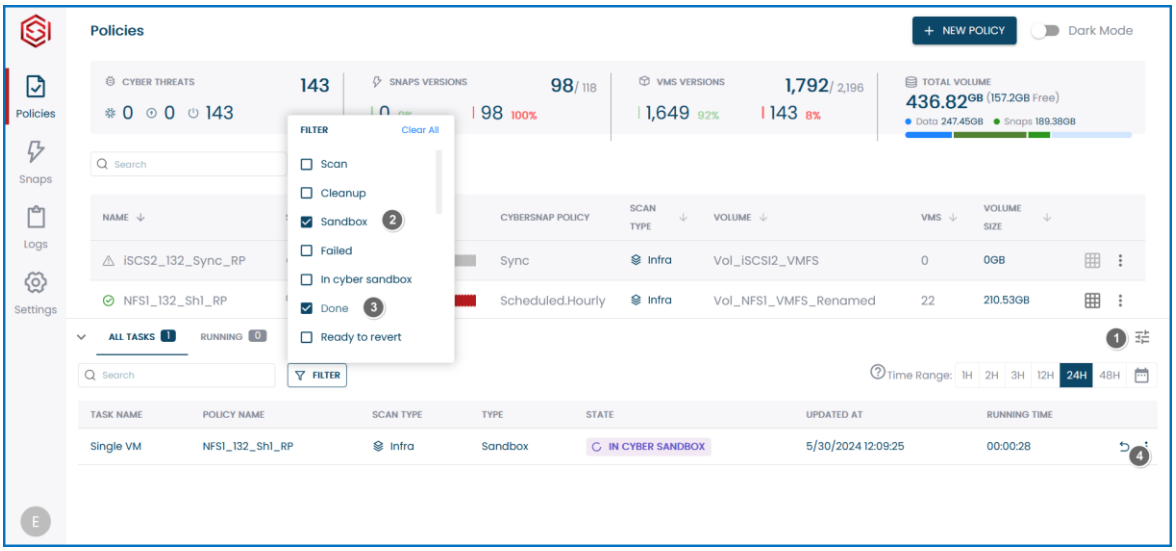
A dark green tag indicates a successful restoration of the virtual machine from the selected NetApp snapshot, with its registration and Power On status in VMware vCenter for future use, albeit without network connectivity to the virtual machine.

On the other hand, a dark red tag is indicative of an issue preventing the virtual machine from powering on within VMware vCenter. The underlying reasons for this could vary, hence, it's recommended to delve into the log for the recovery task to glean more insights into the problems hampering the Power On process of the virtual machine.

Reverting the Sandbox

Upon completion of the investigation on the virtual machine, it's necessary to initiate the reverse process to clean up the content in your VMware vCenter environment.

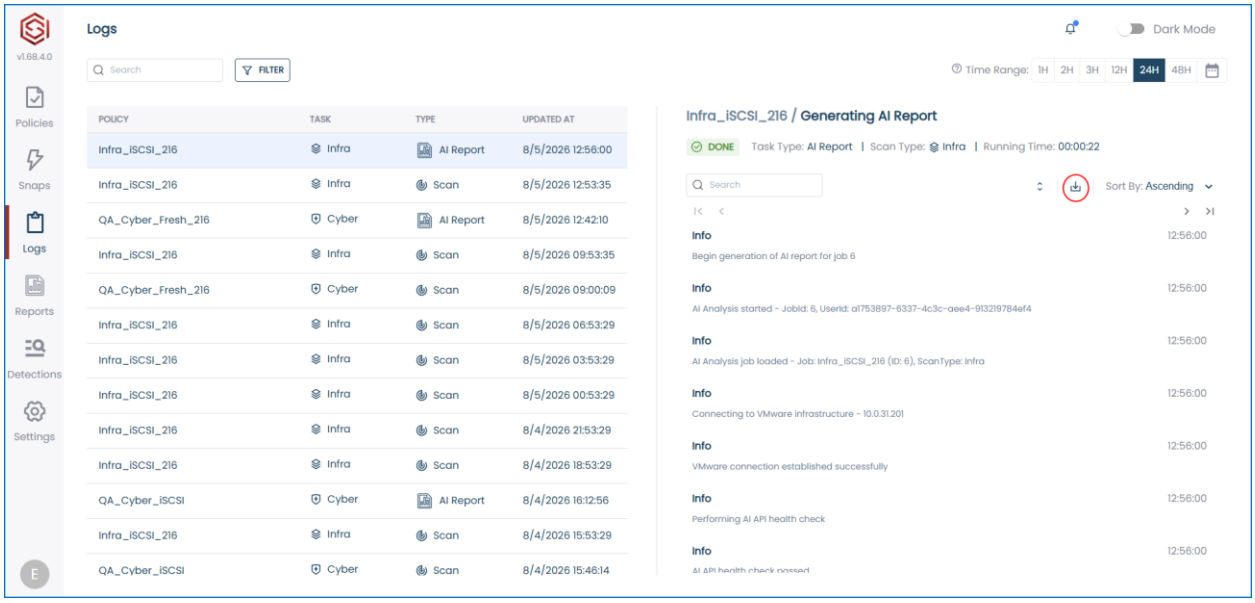
Firstly, open the task drawer and locate your recovery task which is marked as “IN CYBER SANDBOX”. To filter out the tasks, click on the filter icon (1), then click on the filter button to bring up the filtering options. From the presented filtering options, select the ‘Restore’ (2) type and State ‘Finished OK’ (3), then either click on the Undo icon adjacent to the three dots or open the task menu to choose the Undo option from the menu.



After initiating the undo process in CyberSnap, the selected virtual machines that were used in the recovery process within VMware will be powered off and subsequently unregistered from the VMware vCenter inventory. If these virtual machines were the last ones on the datastore, the datastore will then be dismounted from the VMware vCenter, and the temporary volume cloned from the selected snapshot will be removed from NetApp. This way, the content in your VMware vCenter environment is maintained post investigation.

Logs

CyberSnap maintains logs that contain all essential information about the process, enabling you to gain a comprehensive understanding regardless of whether the process is successful or not. The main screen is divided into two sections. On the left side, you will see the list of all events, while on the right side, you will find detailed information for the selected event in the left pane. To collect all event details displayed in the right pane for a specific process selected in the left pane into a single file, press the download icon marked with red circle on the picture below.

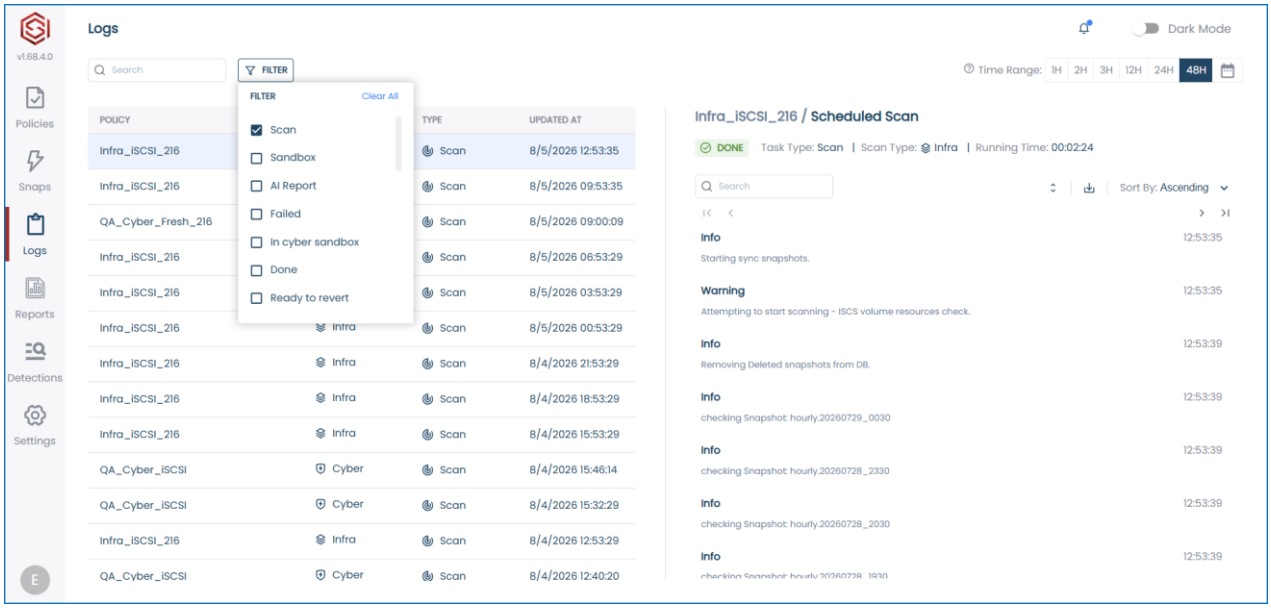


Above those sections, you will find the 'Filter' button on the left side and the 'Time Range' selector on the right side.

The 'Filter' button provides you with the ability to filter events based on type and status. To filter events, simply click on 'Status' and/or 'States'. After clicking the filter option, CyberSnap will dynamically load only those events that correspond to your selection. You can also combine multiple selections.

The 'Time Range' selector allows you to swiftly filter events based on their timestamps. For expedited access, it offers preconfigured time spans ranging from one to 48 hours back from the current time. Additionally, you have the option to pinpoint the end of events by selecting a specific day in the date picker.

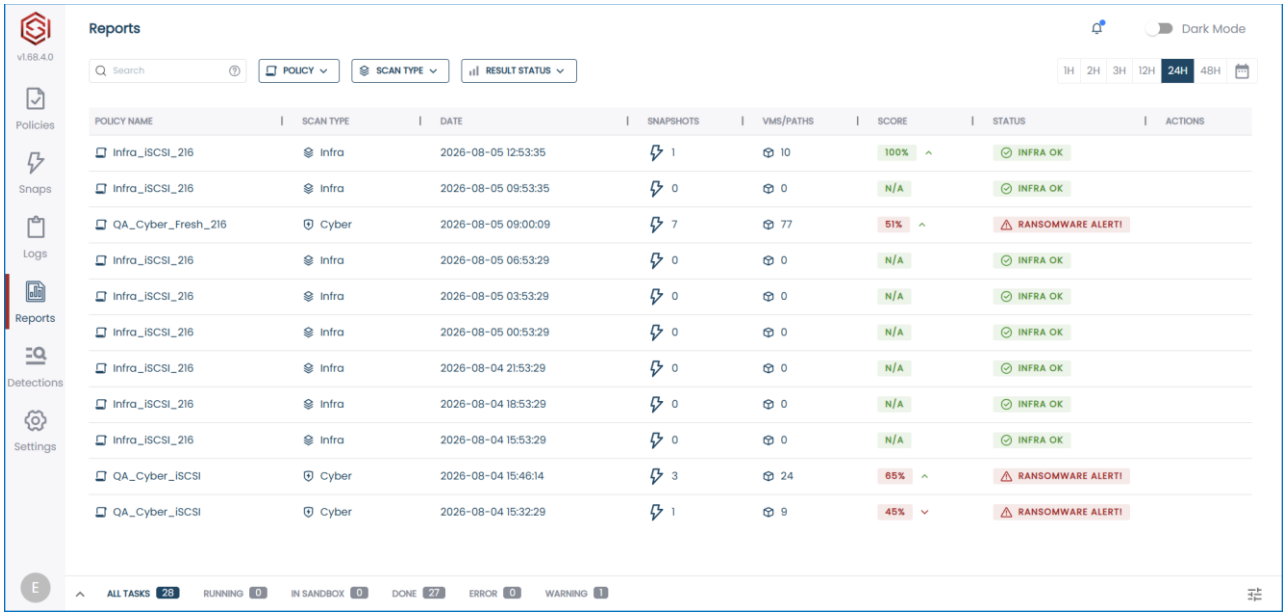
With the events provided in the logs section of the CyberSnap Console, you can easily find all events based on their status. Once the list is updated in the CyberSnap Console, you can select the desired event from the list. This will load the event details on the right side of the CyberSnap Console, where you can examine all the details related to the process. In the details pane for each step of the process, CyberSnap will provide statuses that could be either ‘Info’ or ‘Error’. The 'Info' markup signifies a process step that was executed successfully, while the 'Error' markup indicates an issue that prevented the process from completing successfully. Depending on the error message, additional steps may be required to ensure the process completes properly in the future.



Reports

The Reports page provides an overview of all completed policy executions and their scan results. Each time a policy execution is completed, a report is automatically generated and added to the Reports list.

Reports are displayed in chronological order, with the most recently completed policy execution shown at the top of the list.



Report Information

Column	Description
Policy Name	Displays the name of the policy that was executed.
Scan Type	Indicates the type of scan performed by the executed policy. The scan type can be **Infrastructure (Infra)** or **Cyber**.
Date	Displays the date and time when the policy execution was completed and the report was generated.
Snapshots	Displays the number of snapshots that were included in the scan.
VMs/Paths	Displays the number of scanned objects. For **FC, iSCSI, and NFS datastores**, this column shows the number of virtual machines (VMs) scanned. For **SMB/CIFS shares**, this column shows the number of paths scanned according to the paths configured in the policy.
Score	Displays the comparison between the current scan and the previous scan. A higher score indicates an improvement, meaning fewer issues were detected. A lower score indicates that additional issues were identified compared to the previous scan.
Status	Displays the result of the latest scan execution. If no issues are detected, the status is displayed in green with a corresponding success message. If issues are detected, the status is displayed in red and includes a message describing the detected issue.
Actions	Displays recommended actions based on the scan results. These actions provide guidance on the steps required to address detected issues.

Report Status

The report status provides a quick indication of the scan result:

- Green status – The scan completed successfully and no issues were detected.
- Red status – The scan detected issues that require attention.

Review the status message and recommended actions to determine the appropriate remediation steps.

Report Filters

The Reports page includes multiple filtering options that allow you to quickly locate and review specific reports. Filters can be used individually or combined to narrow the displayed report list based on your requirements.

Available filters include:

- Policy
- Scan Type
- Result Status
- Date Time Picker

Policy Filter

The Policy filter allows you to select a specific policy from the available list. By selecting a policy, only reports associated with the chosen policy will be displayed, making it easier to review results for a specific scan configuration.

Scan Type Filter

The Scan Type filter allows you to filter reports based on the type of scan performed:

- Infra – Displays reports generated from Infrastructure scans.
- Cyber – Displays reports generated from Cyber scans.

Selecting the appropriate scan type reduces the number of displayed reports and helps you quickly locate the required information.

Result Status Filter

The Result Status filter allows you to display reports based on their execution result or message status. This option helps identify reports with specific outcomes, such as successful scans or scans where issues were detected.

Date Time Picker Filter

The Date Time Picker allows you to limit report results to a specific time period.

You can select from predefined time ranges, including:

- 1 hour
- 2 hours
- ...
- 48 hours

Alternatively, you can define a custom date and time range to search for reports generated during a specific period.

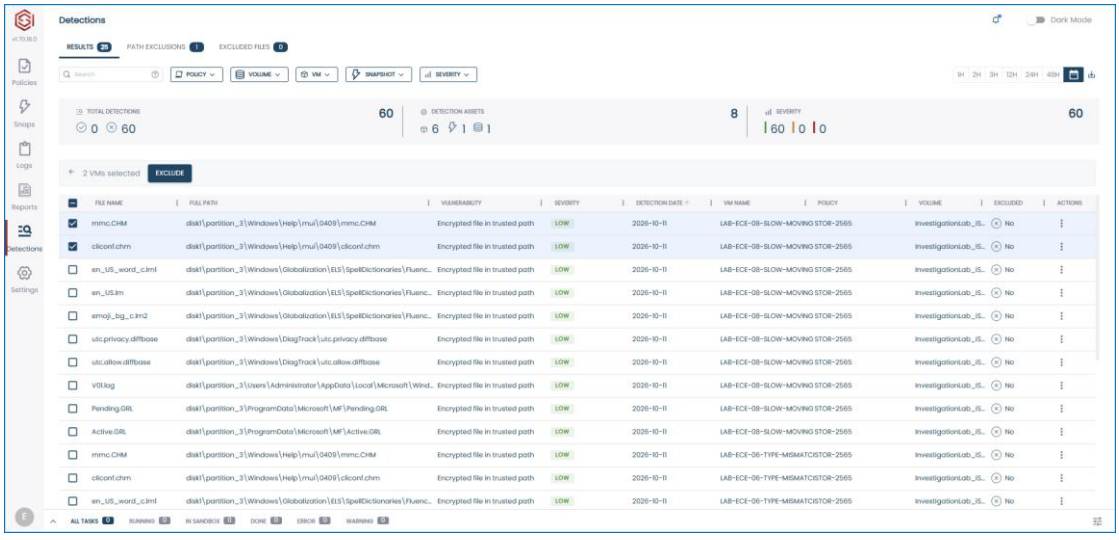
Using the Date Time Picker together with other filters provides a faster and more efficient way to locate reports from a specific policy execution period.

Detections

The Detection view provides a centralized interface for reviewing findings generated by the Cyber Policy. The system displays results in groups of 25 and loads additional findings automatically as you scroll. In addition to reviewing results, the detection panel also allows you to define exclusions, enabling you to filter out specific items from future detections and focus on those that require attention.

Detection Results

Displays the scan findings, including file name, path, detected vulnerabilities, and their severity levels.



The following are the key elements of the Result view:

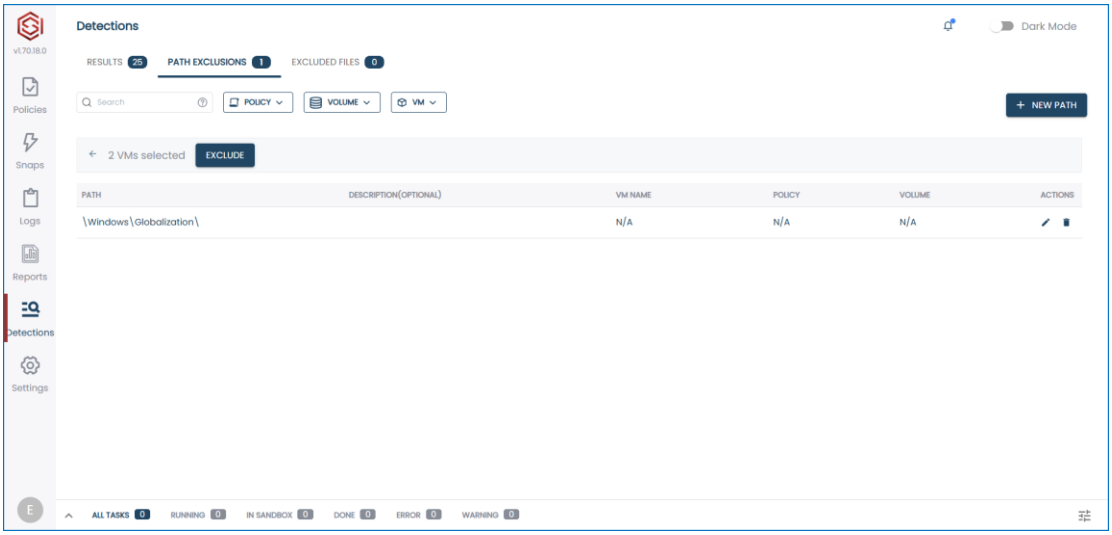
- Search box
  - The search box enables you to quickly find items in the list of reported detections.
- Policy
  - In the Policy dropdown list, you can select one or more policies to limit the scope of the examination

- Volume
  - Volume dropdown list enables you to filter detection based on NetApp volume
- VM
  - The VM dropdown list enables you to limit the output to a specific virtual machine.
- Severity
  - Based on the severity level assigned to each threat, you can filter items in the Detection panel.
- Show Excluded
  - By clicking the slider, you can see which items are excluded from Cyber Scanning.
- Date time picker
  - In the date-time range picker, you can limit the Detection view to a specific point in time, from today back to a selected date in the past.
- Exclude/UnExclude
  - This option enables you to exclude specific files from scans if they are confirmed false positives. To reinclude them in future scans, select the excluded files and click UnExclude.

Note: Exclusions take effect only for disks scanned after the exclusion is created. Scan results from disks that were previously analyzed are not affected by newly defined exclusions

Path Exclusions

Allows you to define file paths or directories to be excluded from future scans.

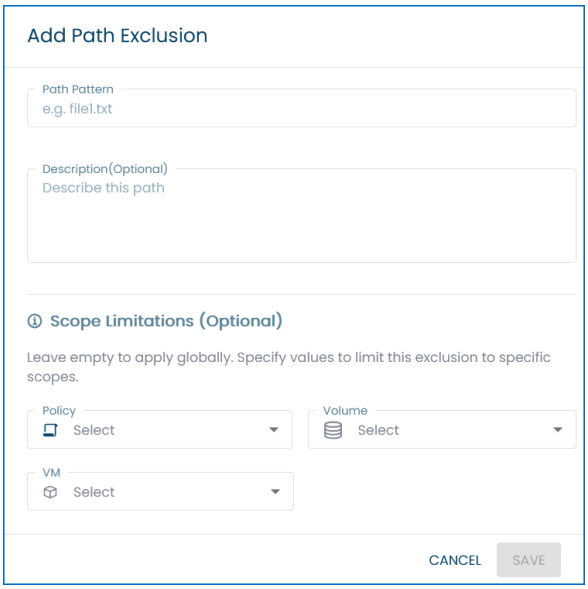


The following are the key elements of the Path Exclusions view:

- Search box
  - The search box enables you to quickly find items in the list of reported detections.
- Policy
  - In the Policy dropdown list, you can select one or more policies to limit the scope of the examination
- Volume
  - Volume dropdown list enables you to filter detection based on NetApp volume.
- VM
  - The VM dropdown list enables you to limit the output to a specific virtual machine.
- New Path
  - A button that opens a form, allowing you to define a new exclusion rule.

New Path

The New Path button opens a configuration form used to define exclusion rules. These rules allow you to specify paths that should be excluded from scanning or processing.



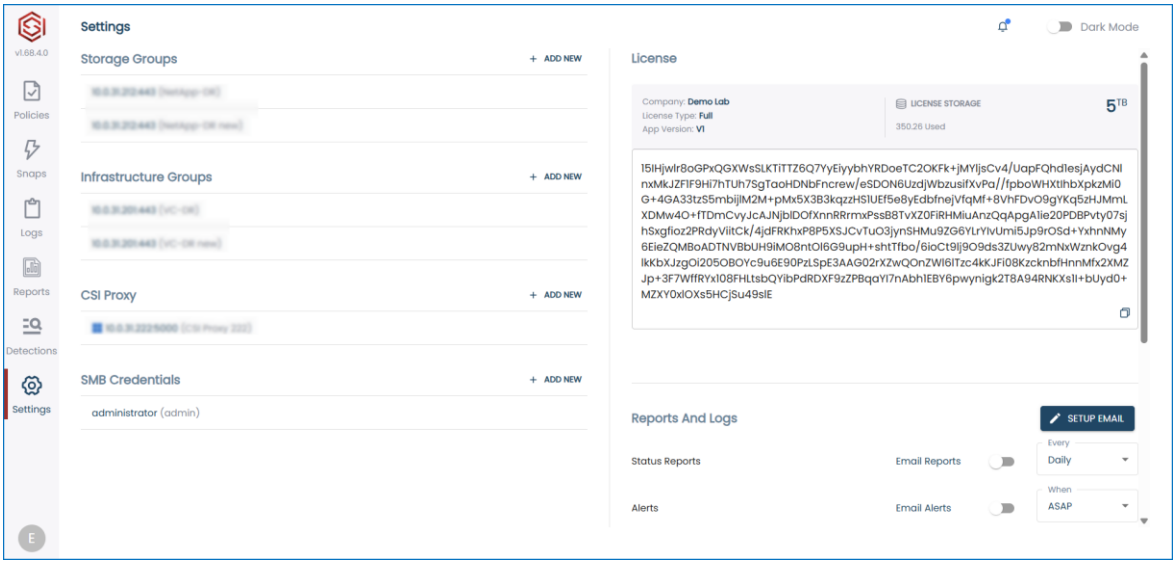
The form provides several parameters to tailor the exclusion rule to your needs:

- Path Pattern
  - Defines the file or directory path to be excluded. Enter the desired pattern in this field. Wildcards or specific directory structures may be used.
- Description
  - Provides a free-text field where you can add context for the exclusion rule. This can be useful for documenting the reason for excluding a particular file or path, aiding in long-term management and auditing.
- Scope Limitations
  - Enables you to limit the exclusion rule to a specific scope rather than applying it globally. You can narrow the exclusion to:
    - Specific policy
    - Particular volume
    - An individual virtual machine (VM)

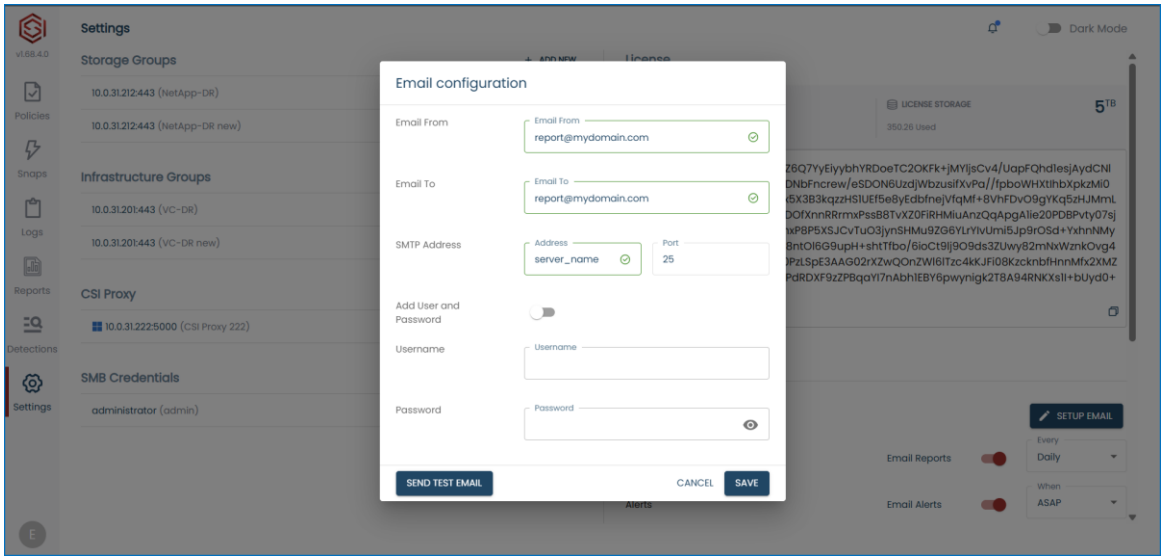
Note: Exclusions are applied only to disks scanned after the exclusion has been created. Previously scanned disks are not affected by newly defined exclusions.

Configuring Email Reporting

In CyberSnap, you can set up email reports for the "Status Report" and "Alerts." To enable these reports, navigate to the Settings panel and configure an email account.



To configure email reporting, click on the "SETUP EMAIL" button. A new popup window will appear. If the relaying option is enabled on your email server, simply provide the "Email From," "Email To," "SMTP Address," and "Port" details, then click the "Send Test Email" button to validate your input.



If the relaying option is not enabled on your email server, in addition to the previous settings, you will need to enable the "Add User and Password" slider to enter your email account credentials for authorization on the email server.

After configuring the email settings and validating them, click the "Save" button.

Now, select whether you want to automatically receive both "Status Reports" and "Alerts," or just one of them. Use the slider for each option you wish to activate, then click the "Save" button.

Licensing

CyberSnap licensing is based on the total capacity of the NetApp volumes included in its policies. The size of each registered volume must be within the available licensed capacity to maintain policy activation and access to licensed functionality. If adding a volume causes the licensed capacity to be exceeded, the most recently created policy will be deactivated until the license capacity is increased to accommodate the total volume size. A single NetApp volume can be included in multiple policies, but it is counted only once toward the licensed capacity. This ensures that usage remains within the limits of the license.

License details

In CyberSnap, the license key is initially inputted on the welcome screen. Post this step, a user can view all the pertinent licensing details by navigating to the License view under the Settings menu on the CyberSnap console. Here's a breakdown of the information available in this view:

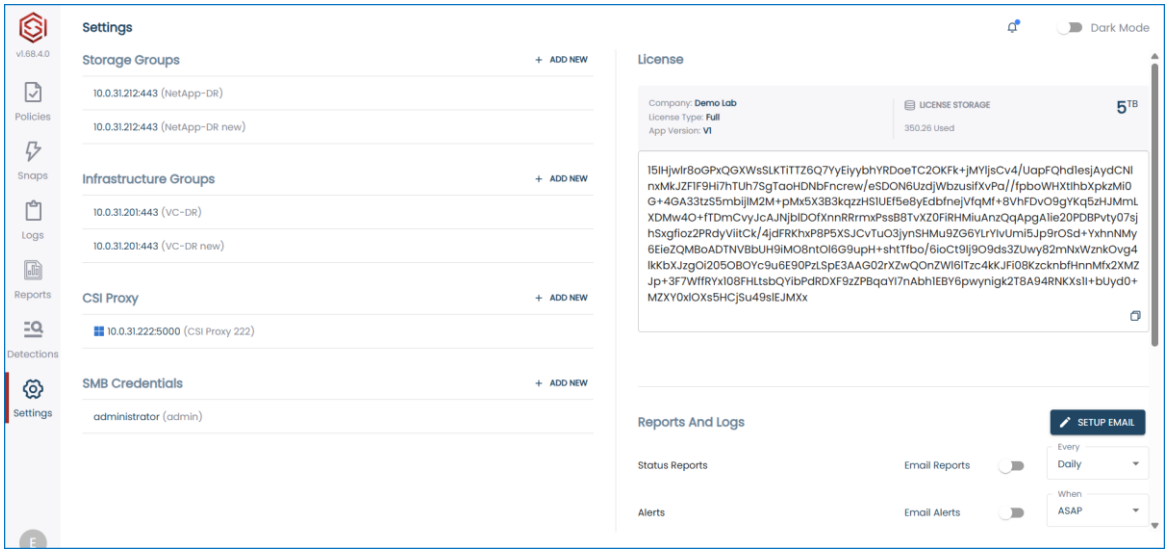
1. **Company Name**:
    - The name that was registered during the license key procurement process.
2. **License Type**:
    - There are different license types denoting the kind of access granted in CyberSnap:
        - **SaaS**: A service-based license requiring an annual renewal.
        - **Trial**: A temporary license providing full access for a specified duration.
3. **App Version**:
    - This field displays the current version of the CyberSnap application in the context of licensing.
4. **License Capacity**:
    - Indicates the maximum storage size allocated with the license key.
5. **License Key**:
    - A unique encoded string of alphanumeric characters crucial for registering and validating the user's access in CyberSnap.

Each of these details plays a pivotal role in ensuring users have the necessary information regarding their licensing status, the version of the application they are using, and the capacity available to them for utilizing CyberSnap effectively.

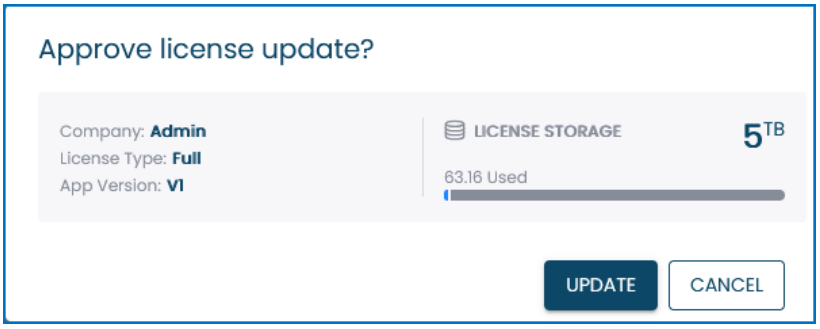
Adding new License

To accommodate more volumes in CyberSnap once the current license key has reached its capacity, you'll need to extend your license capacity. Here's a step-by-step guide on how to proceed with updating your license.

Click on the 'Settings' menu in the CyberSnap console. This will open a pane on the right showing your license details. Select the current license key displayed and delete it. Upon deleting the old key, enter your new license key in the provided field.



A button labeled ‘UPDATE LICENSE’ will pop up. Click on this button to initiate the verification process for your new license key. An approval window for the license update will pop up; click the 'UPDATE' button.



Once the new license key has been successfully registered, the updated license capacity will be reflected in the License details pane.

After license is added, you will need to reactivate any policies that may have been disabled due to previous capacity limitations. Ensure they are now in line with your updated license capacity and reactivate them as needed.

This process ensures that you can seamlessly extend your license capacity in CyberSnap and continue to manage and integrate new volumes, leveraging all the features that come with the newly added capacity.

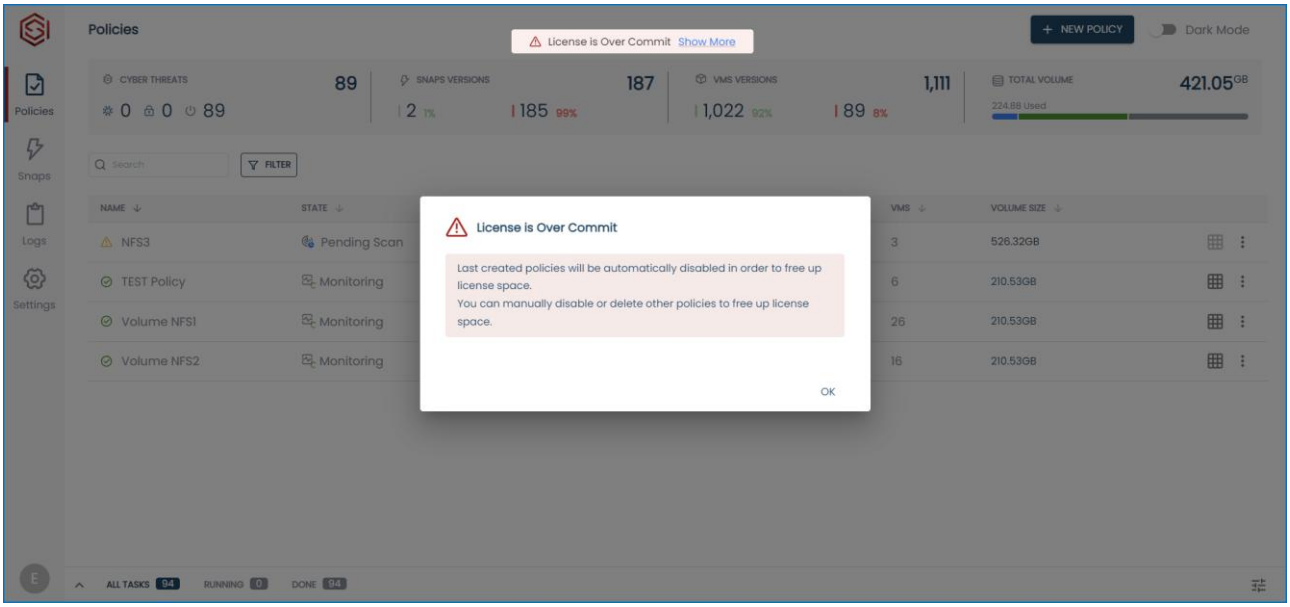
License Overcommit

In Chapter Licensing we have already explained how to add a new license and update it with a new key in case you need to extend the product's capacity support.

Here we will focus on scenarios in which you're creating a new policy using a fresh NetApp volume. In these cases, it's important to consider the total capacity of the existing policies and the potential for the new one to exceed the current license capacity.

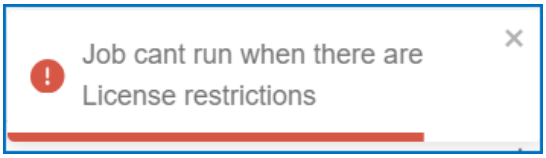
If the latest added policy exceeds the current license capacity, CyberSnap will take multiple steps to inform you about the set of measures that will be enforced when you save a new policy.

Immediately when you save a new policy in CyberSnap that exceeds the capacity, you will be notified by the system that the last added policy is overcommitting the total capacity, as shown in the picture below. Here you can click on ‘Show More’ option to get more details.



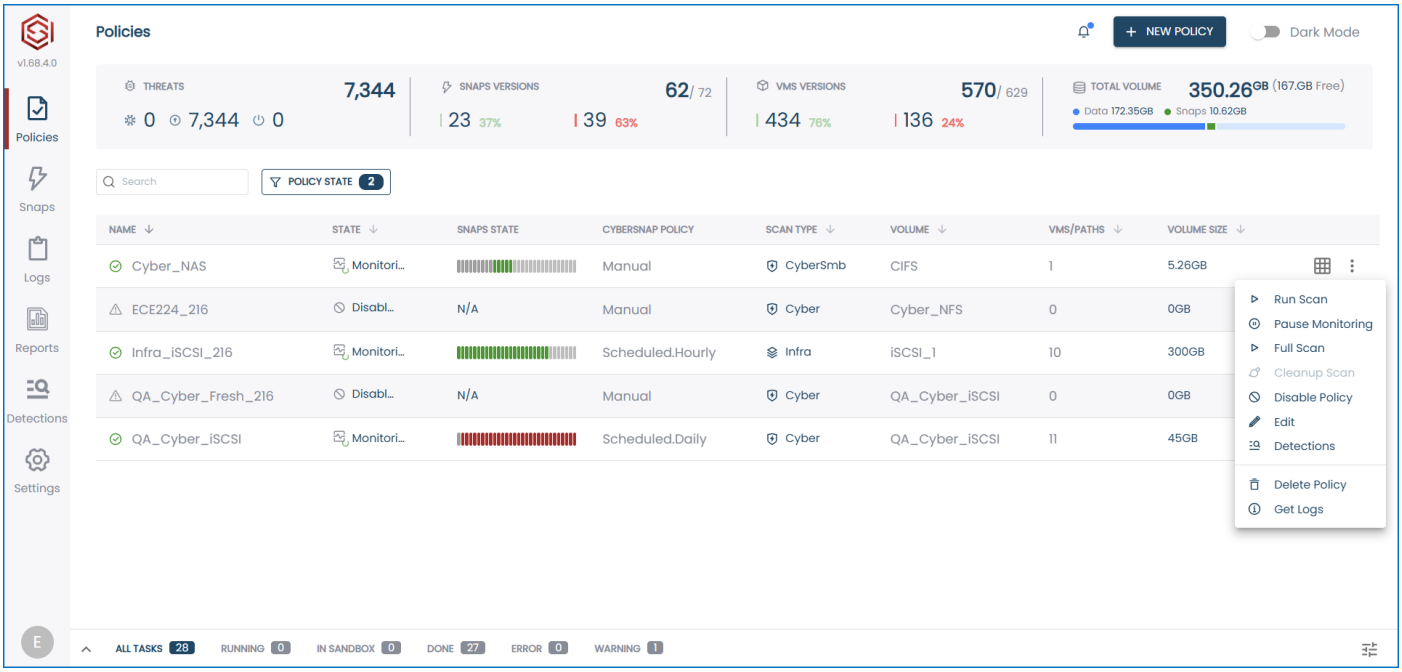
In the detailed window, you will be notified about the actions that CyberSnap will execute automatically and the steps you can also take. As outlined in the message, the policy will be disabled automatically when the background worker process is triggered by CyberSnap. Until that moment, the policy will be in the status of 'Pending Scan'. When multiple new policies are added, exceeding the current license capacity, CyberSnap will disable them in the reverse order of their addition.

If you attempt to manually execute a policy that overcommits the license capacity execution will be blocked by CyberSnap and you will be notified by the system with a toast message in the lower right corner of the CyberSnap console.



To address this overcommitment situation, you can take one of the following measures:

- Disable Policy - Selecting this option will turn off the policy, stopping the scanning process in the future. Once you click on the ‘Disable Policy’ option, a warning window will pop up. Confirm that you want to disable the policy. Once confirmed, the policy’s ‘STATE’ will change to ‘Disabled’. When you upgrade the license capacity to support your latest added needs, you can easily re-enable the policy.
- Delete Policy - Selecting this option will permanently delete the policy. Once you click on the ‘Delete Policy’ option, a warning window will pop up. Confirm that you want to delete the policy. Once confirmed, the policy will be permanently removed from CyberSnap Console.



Regardless of the solution you choose whether it's disabling or deleting the policy, the warning message will be removed from the CyberSnap Console.

Light and Dark mode

Light and Dark modes refer to different color schemes or themes used in the user interfaces of CyberSnap. These modes affect the overall color palette, text readability, and visual elements to optimize the viewing experience based on the ambient lighting conditions and user preferences.

In Light Mode, the color palettes are brighter with predominantly white backgrounds with dark text and other elements.

In Dark Mode, the color palette features dark backgrounds with light text and other elements.

You can easily switch between Light and Dark mode by clicking on the slider in the top right corner of the CyberSnap Console.



Login

To access the CyberSnap console, go to the login page. If you're on the same server where CyberSnap is installed, use:

- https://localhost/user/login

For remote access, use the server's FQDN or IP:

- https://[FQDN or IP]/user/login

Once the login page loads, enter your username and password to begin authorization. Opt for 'Remember Me' to be recognized by CyberSnap for seamless access for the next seven days. After this period, you'll need to reauthenticate your credentials.

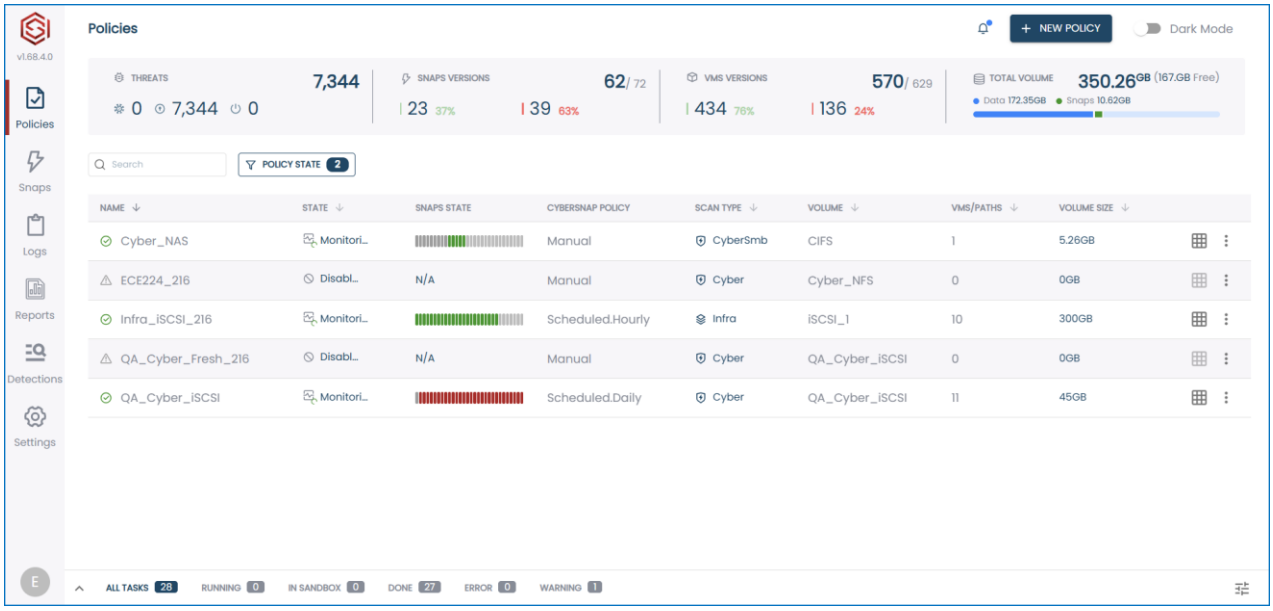


Session timeout

The idle session timeout is configured in the app settings within CyberSnap. When the configured timeout is reached, you will be automatically logged out of the CyberSnap console and will need to sign in again to resume your session.

Notification

The CyberSnap user interface includes a Notification feature (represented by the bell icon) that displays information about virtual machines that were selected during policy creation but not found during the scan. One reason virtual machines may not be located is the configuration of VMware vCenter DRS. Furthermore, customers may relocate virtual machines to different datastores during planned maintenance or infrastructure reorganization.



To provide more details about virtual machines, click on the bell icon to access additional information. The list will show a notification for every missing virtual machine associated with each snapshot. Clicking the “Mark All as Read” link allows you to acknowledge all notifications at once.



Task Drawer

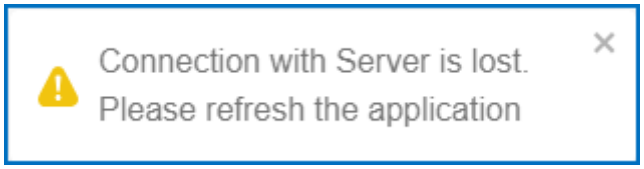
As part of the CyberSnap user interface, you have access to the task drawer. The CyberSnap task drawer provides a centralized location for managing and accessing various tasks and events. It serves as a convenient and organized way to interact with different features of the application.

The CyberSnap task drawer displays a list or overview of events, appointments, or scheduled tasks associated with your policies. This feature enables you to easily view, examine, and manage events within the application without having to navigate through multiple menus or screens.

Troubleshooting

CyberSnap Remote Service Connectivity

CyberSnap is a browser-based service that facilitates communication directly from your web browser. This operates on a client-server architecture, where the connection between your browser and the CyberSnap service is not permanent. This can lead to situations where the browser may struggle to establish communication with the remote service. While this is often due to networking issues, it may also arise from other factors. In such cases, CyberSnap will alert you with a warning message displayed in the bottom right corner, as illustrated in the accompanying image.



Automated Residual Cleanup

CyberSnap includes an automated residual cleanup feature designed to maintain the cleanliness and integrity of the virtual environment by removing residual artifacts left behind by previous operations. This feature is enabled by default and requires no manual activation or additional configuration.

This feature is designed to continuously monitor the virtual environment, identify and remove residual data, and ensure ongoing system cleanliness and integrity. The monitoring process operates within predefined time intervals, providing continuous environmental assessment while preventing any performance impact on the virtual infrastructure.

Manual Cleanup

The cleanup process should always be initiated by CyberSnap to maintain the VMware vCenter environment in the best manner. It is strongly recommended to utilize the cleanup feature in CyberSnap for this purpose. However, in cases of any kind of outage or unforeseen circumstances that could influence the recovery or undo process to not finish as designed, manual cleanup may become necessary.

Before proceeding with manual deletion of data, please ensure to double-check that you are only removing data remaining in your VMware vCenter inventory and NetApp storage that are related to the CyberSnap process and leftover as a result of an outage. Manual cleanup should only be considered as a last resort when the cleanup via CyberSnap fails. It's crucial to take this careful approach to avoid any accidental deletion of important data, ensuring the integrity and smooth operation of your systems.

Scan leftover

To manually clean up following an outage or an unsuccessful cleanup via CyberSnap, adhere to these steps while using VMware vCenter:

1. Identify all virtual machines prefixed by "CSI_Scan_".
2. Proceed to shut down or power off these identified virtual machines.
3. Once powered off, remove these virtual machines from the VMware vCenter inventory.
4. Ensure that no virtual machines remain on the datastores.
5. Collect the names of all datastores prefixed with CSI_Scan_ from which the virtual machines were previously removed to easily identify the NetApp snapshot mapped as a volume in the final step.
6. Before proceeding to delete these volumes from NetApp storage, ensure to unmount them from the VMware vCenter.
7. Delete the corresponding volumes from the NetApp storage.

These steps will help in manually cleaning up the environment post an outage, ensuring the removal of only the data and snapshots related to the CyberSnap process.

Sandbox leftover cleanup

To remove residual sandbox-related resources, perform the following steps using VMware vCenter and NetApp storage management tools.

1. Identify sandbox virtual machines. In VMware vCenter, locate all virtual machines whose names begin with the prefix CSI_Sandbox_.
2. Power off the virtual machines. Shut down the identified virtual machines gracefully where possible. If a graceful shutdown is not possible, power them off according to your operational procedures.
3. Remove the virtual machines from inventory. After confirming that the virtual machines are powered off, remove them from the VMware vCenter inventory. This action removes the inventory entries but does not necessarily delete the underlying virtual machine files or storage volumes.
4. Identify residual sandbox storage. Verify that no virtual machines with the CSI_Sandbox_ prefix remain registered in vCenter. Inspect the relevant datastores for residual sandbox-related virtual machine files and resources.
5. Record the affected datastores. List the names of all datastores associated with the sandbox resources being removed. Record the relevant datastore and volume mappings to support the storage cleanup.
6. Identify the corresponding NetApp snapshots and volumes. Using the recorded datastore information and the available storage mappings, identify the NetApp snapshots and volumes associated with the sandbox resources. Verify that each resource is no longer required and is not being used by another virtual machine or service.
7. Unmount the datastores before storage deletion. Before deleting any associated NetApp volumes, ensure that the corresponding datastores have been safely unmounted from VMware vCenter and

are no longer in use. Confirm that no active virtual machines, hosts, or other dependencies require access to these volumes.

8. Delete the obsolete storage resources. Once all dependencies have been checked and the correct resources have been identified, delete only the confirmed obsolete sandbox-related NetApp volumes or snapshots, following the applicable storage administration procedures.
9. Verify the cleanup. Confirm that the sandbox virtual machines have been removed from inventory, the obsolete sandbox resources are no longer present, and no active workloads or unrelated storage resources have been affected.

To manage a manual cleanup for sandbox-related data, follow the steps below using VMware vCenter:

1. Locate all the virtual machines with the prefix "CSI_Sandbox_".
2. Proceed to either shut down or power off these identified virtual machines.
3. After ensuring they are powered off, remove them from the VMware vCenter inventory.
4. Verify that there are no virtual machines with the prefix "CSI_Sandbox_" remaining on the datastores.
5. Gather the names of all the datastores that have the prefix "CSI_Sandbox_" from which you previously removed the virtual machines.
6. This action will aid you in the final step to easily identify the NetApp snapshot mapped as the volume.
7. Prior to deleting those volumes from the NetApp storage, make sure to unmount them from the VMware vCenter.

These steps ensure a thorough manual cleanup of the sandbox environment, removing only the data and snapshots pertaining to the CyberSnap process in the case of an unsuccessful cleanup through CyberSnap or an outage.

Understanding Your License and Support Services

As you reach the conclusion of this user guide, it's important to understand the key aspects of your agreement with CyberSnap.io and the level of support you can expect.

Software License Overview: You, the user, have a non-transferable license to use CyberSnap.io software internally, as detailed in your purchase quote. Remember, this software includes proprietary and open source components, and your use of each is governed by respective licenses.

Usage and Restrictions: Your license comes with the responsibility to use the software lawfully and within the bounds of the agreement. Unauthorized distribution, reverse engineering, and other misuses are prohibited to ensure the integrity and security of the software.

Intellectual Property: CyberSnap.io holds all rights to the software. Your valuable feedback on improving the software may be utilized by CyberSnap.io to enhance user experience.

Support and Response Times: Our commitment to you includes providing support during business hours on U.S. business days. Depending on the issue's severity, we aim to respond swiftly, with response times ranging from one to five business days.

Financial Considerations: The fees for your license are outlined in your quote and are complemented by a transparent policy regarding taxes and non-refundable payments.

Continuing Support: Your journey with CyberSnap.io is supported by our team, dedicated to providing the assistance you need as you use our software.

Contact us at: support@cybersnap.io

For a complete understanding of your rights and obligations, as well as CyberSnap.io's warranties and liability, please refer to the full End User License Agreement and Service Level Agreement.

Thank you for choosing CyberSnap.io. We look forward to supporting your success with our software.

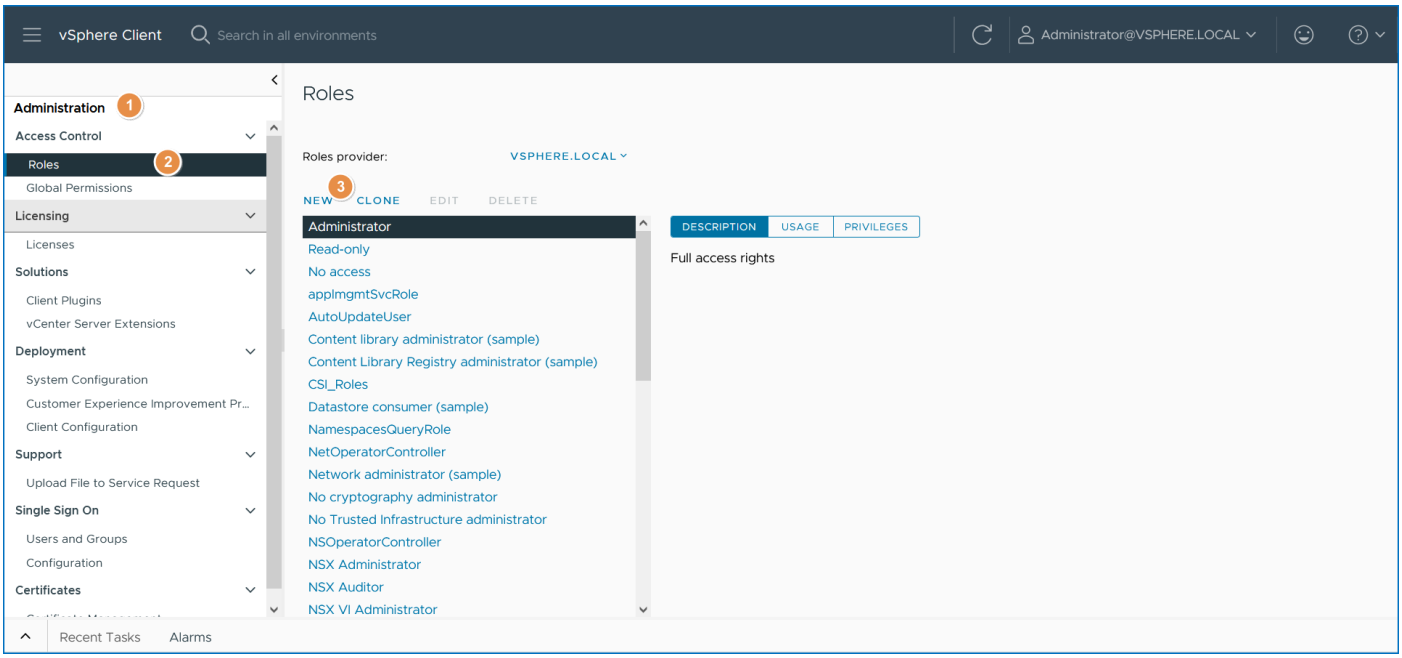
Create Custom Roles for Dedicated Accounts

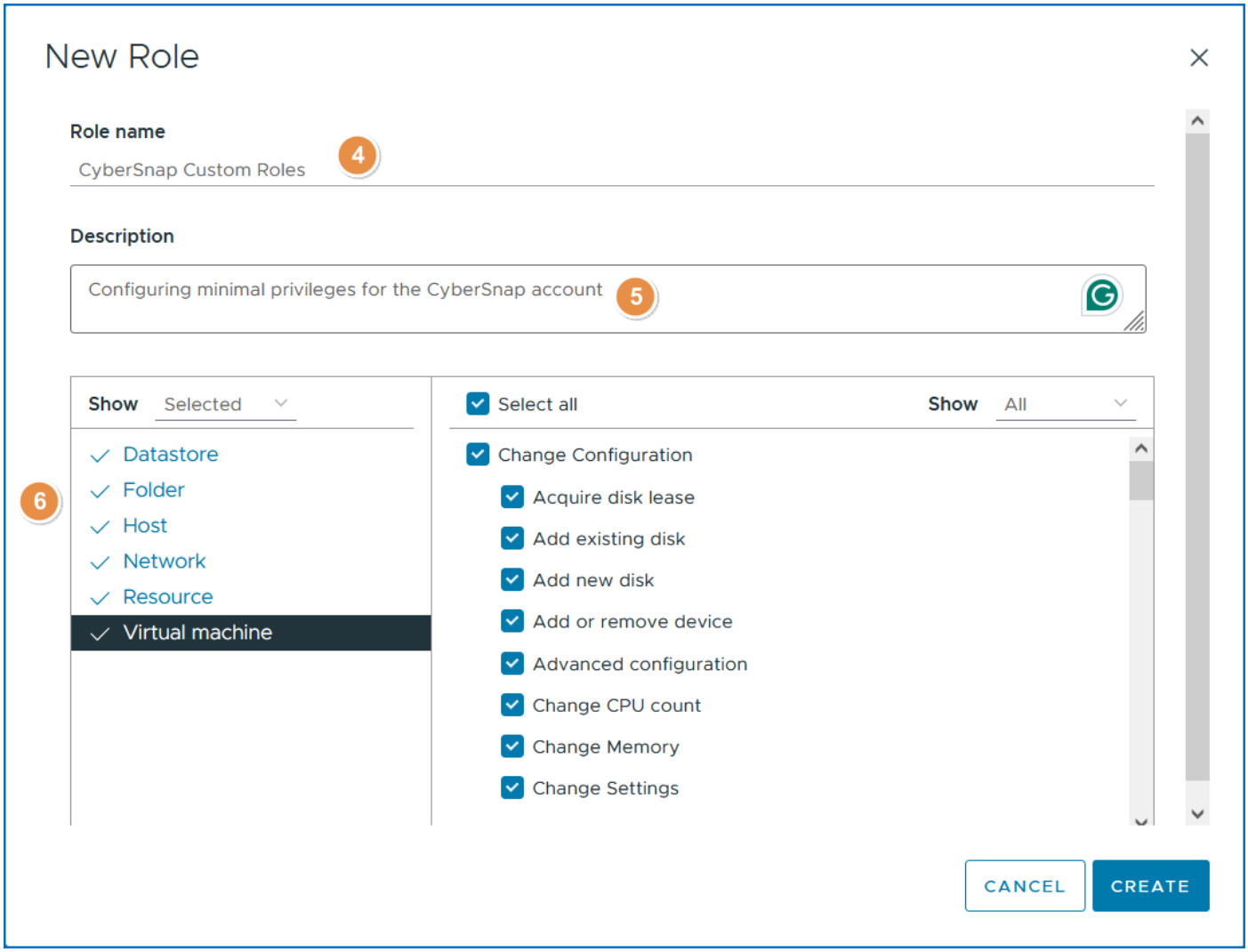
In cases where customers need to restrict account privileges, dedicated user accounts must be assigned specific and granular permissions.

Configuring limited permissions for a VMware vCenter Server account

CyberSnap requires VMware vCenter access to oversee processes within the VMware environment during scanning and recovery.
To set up the minimum required privileges for a dedicated vCenter Server user, follow these steps:

1. Log in to the vCenter Server by using the vSphere Client, select Administration.
2. Click Roles in the Access Control area.
3. Click on the New button, a new popup window will appear.
4. Provide a new name for the custom role you are creating.
5. Add a role description.
6. Choose categories and permissions from the list below the picture.





Datastore (select all)

- Allocate space
- Browse datastore
- Configure datastore
- Low level file operations
- Move datastore
- Remove datastore
- Remove file
- Rename datastore
- Update virtual machine files
- Update virtual machine metadata

Folder (select all)

- Create folder
- Delete folder
- Move folder
- Rename folder

Host (select all)

- Configuration
    - Advanced settings
    - Authentication Store
    - Change settings
    - Connection
    - GuestStore settings
    - Hyperthreading
    - Image configuration
    - Maintenance
    - Memory configuration
    - NVDIMM
    - Network configuration
    - Power
    - ProductLocker settings
    - Quarantine
    - Query patch
    - Security profile and firewall
    - Storage partition configuration
    - System Management
    - System resources
    - Virtual machine autostart configuration
- Local operations
    - Create virtual machine
    - Delete virtual machine
    - Reconfigure virtual machine
- Statistics (Settings applicable only to VMware vSphere v8 or above.)
    - Query

Network (select all)

- Assign network
- Configure
- Move network
- Remove

Resource (select all)

- Assign virtual machine to resource pool

Virtual machine (select all)

- Change Configuration
    - Acquire disk lease
    - Add existing disk
    - Add new disk
    - Add or remove device
    - Advanced configuration
    - Change CPU count
    - Change Memory
    - Change Settings
    - Change Swapfile placement
    - Change resource
    - Configure Host USB device
    - Configure Raw device
    - Configure managedBy
    - Display connection settings
    - Extend virtual disk

    - Modify device settings
    - Query Fault Tolerance compatibility
    - Query unowned files
    - Reload from path
    - Remove disk
    - Rename
    - Reset guest information
    - Set annotation
    - Toggle disk change tracking
    - Toggle fork parent
    - Upgrade virtual machine compatibility
- DataSet Operations (Settings applicable only to VMware vSphere v8 or above.)
    - Create a DataSet
    - Delete a DataSet
    - Delete an Entry from a DataSet
    - Get an Entry in a DataSet
    - List DataSets
    - List Entries in a DataSet
    - Modify the attributes of a DataSet
    - Query a DataSet
    - Set an Entry in a DataSet
- Edit Inventory
    - Create from existing
    - Create new
    - Move
    - Register
    - Remove
    - Unregister
- Guest operations
    - Guest operation alias modification
    - Guest operation alias query
    - Guest operation modifications
    - Guest operation program execution
    - Guest operation queries
- Interaction
    - Answer question
    - Backup operation on virtual machine
    - Configure CD media
    - Configure floppy media
    - Connect devices
    - Console interaction
    - Create screenshot
    - Defragment all disks
    - Drag and drop
    - Guest operating system management by VIX API
    - Inject USB HID scan codes
    - Install VMware Tools
    - Pause or Unpause
    - Perform wipe or shrink operations
    - Power off
    - Power on
    - Record session on virtual machine
    - Replay session on virtual machine
    - Reset
    - Resume Fault Tolerance

    - Suspend
    - Suspend Fault Tolerance
    - Suspend to memory
    - Test failover
    - Test restart Secondary VM
    - Turn off Fault Tolerance
    - Turn on Fault Tolerance
- Provisioning
    - Allow disk access
    - Allow file access
    - Allow read-only disk access
    - Allow virtual machine download
    - Allow virtual machine files upload
    - Clone template
    - Clone virtual machine
    - Create template from virtual machine
    - Customize guest
    - Deploy template
    - Mark as template
    - Mark as virtual machine
    - Modify customization specification
    - Promote disks
    - Read customization specifications
- Service configuration
    - Allow notifications
    - Allow polling of global event notifications
    - Manage service configurations
    - Modify service configuration
    - Query service configurations
    - Read service configuration

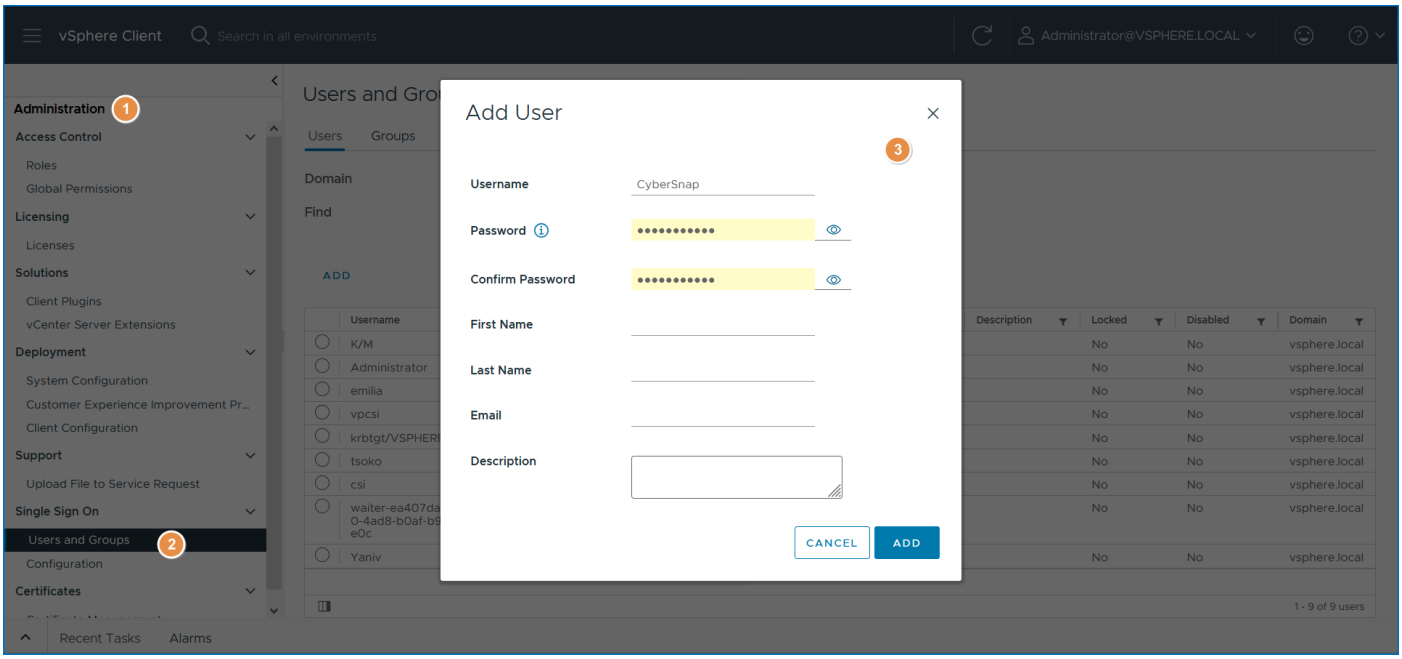
7. To save the permissions assigned to this role, click on the Create button.

Assign Roles

In order to assign new roles, a new dedicated user account must be created in VMware vCenter.

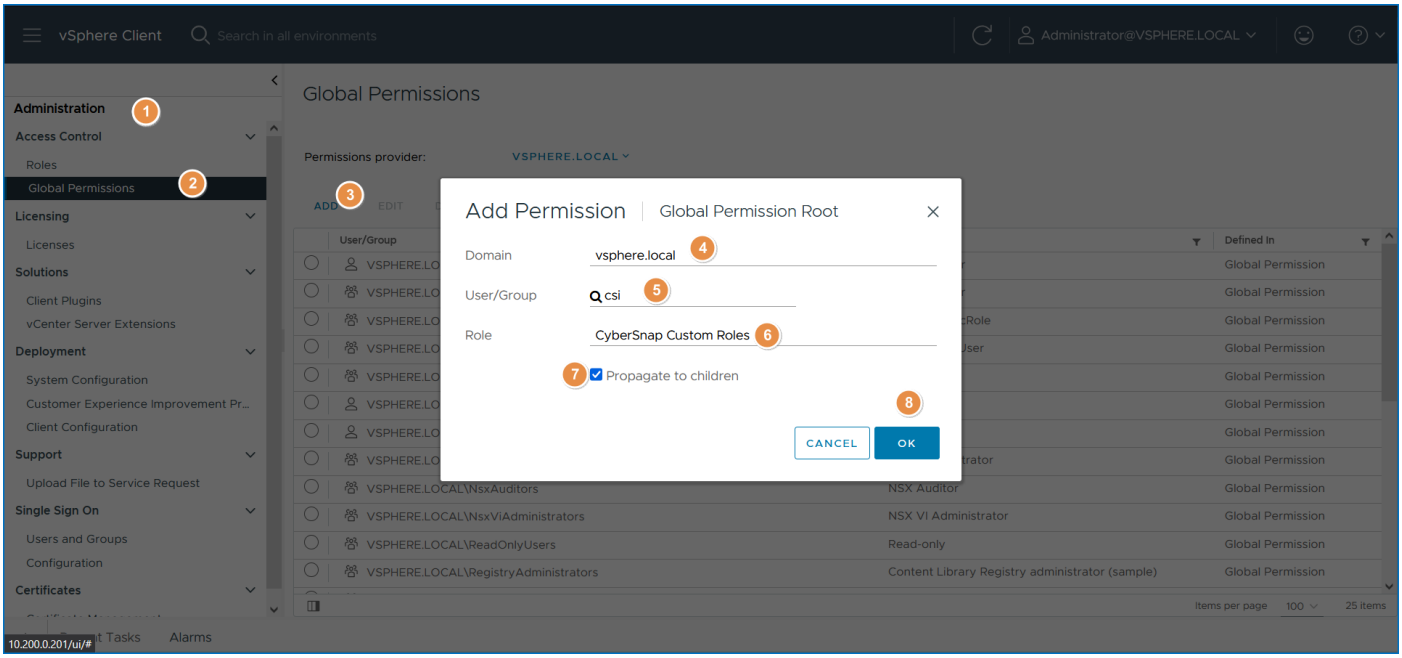
To configure dedicated user account follow these steps:

1. Log in to the vCenter Server by using the vSphere Client, select Administration.
2. Scroll down to “Single Sign On” section, select “Users and Groups”.
3. A new window will appear, enter the required information and then click the Add button.



After creating custom roles and dedicated user accounts, it's essential to establish a relationship between them. To establish relationships, follow these steps:

1. Log in to the vCenter Server by using the vSphere Client, select Administration.
2. Select “Access Control” section, select “Global Permissions”.
3. Click on the Add button, a new window will pop up.
4. Select Domain.
5. Select User.
6. Select Role.
7. Select checkbox “Propagate to children”.
8. Click on the OK button.



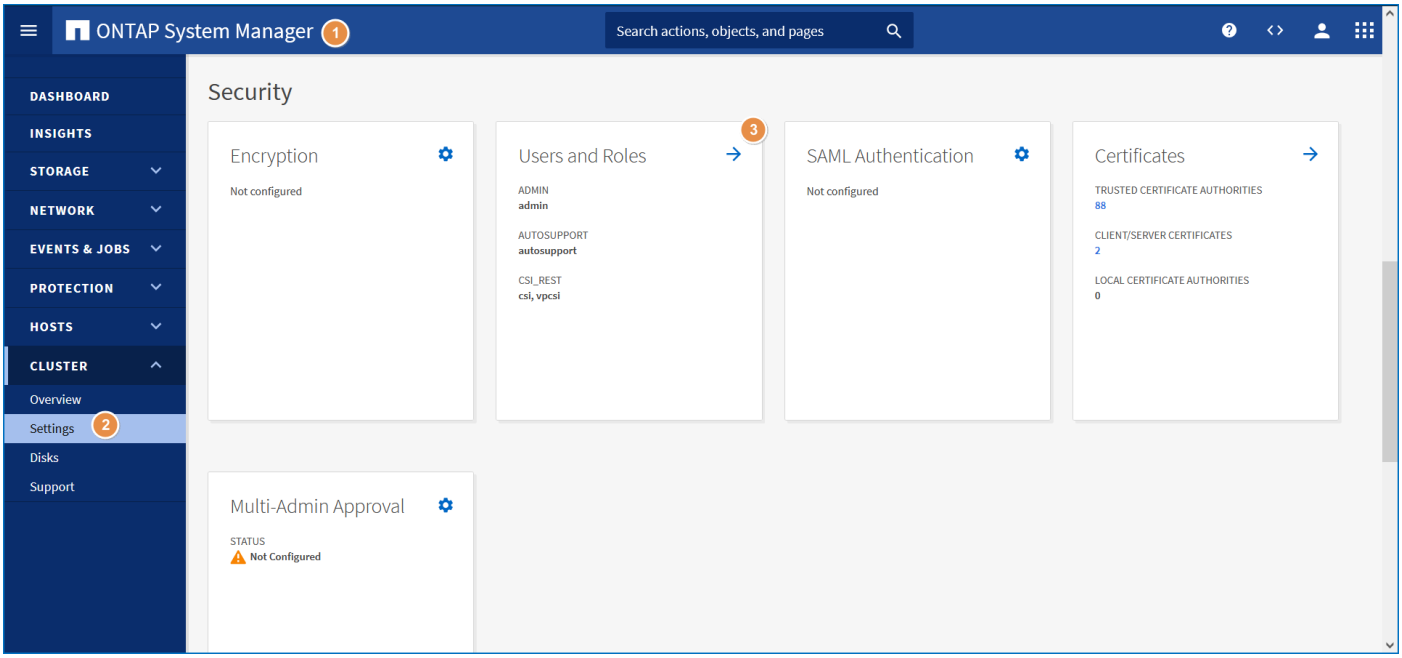
Now you have configured a dedicated VMware vSphere account with the limited privileges required for CyberSnap to operate effectively.

Configuring limited permissions for a NetApp account

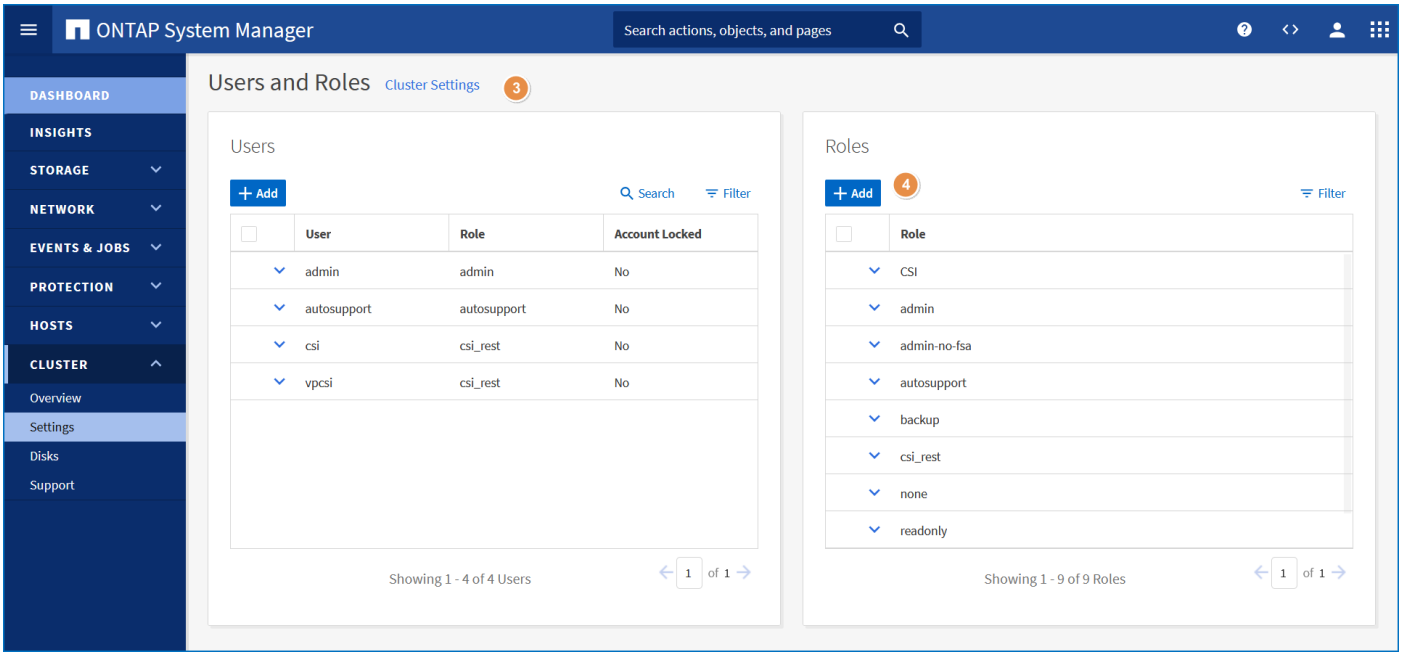
For regular functionality, CyberSnap requires access to the NetApp to oversee processes within the NetApp environment during scanning and recovery. The most efficient approach involves creating a dedicated user account with administrative privileges.

To set up the minimum required privileges for a dedicated NetApp account, follow these steps:

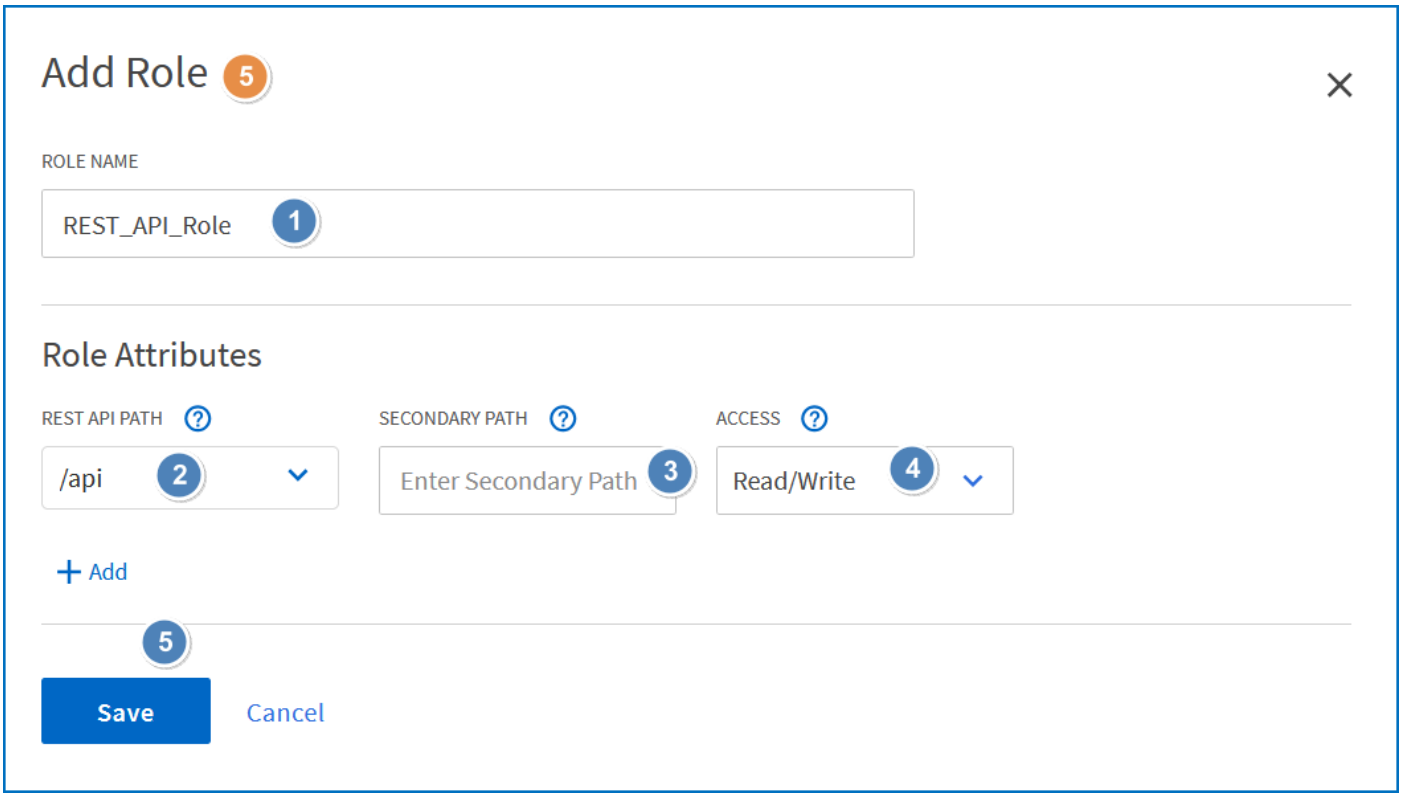
1. Log in to the NetApp system.
2. Navigate to "Cluster" and then select "Settings."



3. Within "Settings," click on "User and Roles."
4. Under "Roles," click on the "Add" button to open a new window.

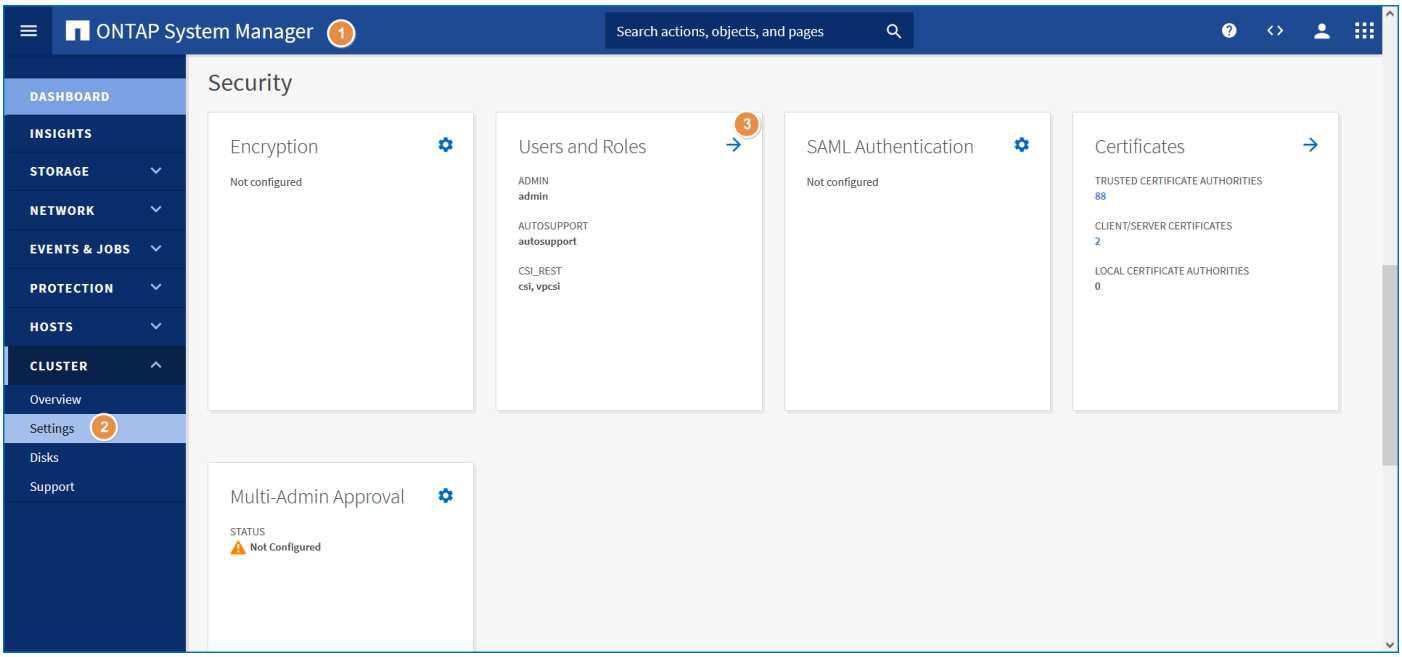


5. In the "Add Role" window:
    1. Enter the role name.
    2. Choose the REST API PATH by selecting "/api."
    3. Leave the secondary path blank.
    4. Select the access level and choose “Read/Write”.
    5. Click on the "Save" button to apply the changes.

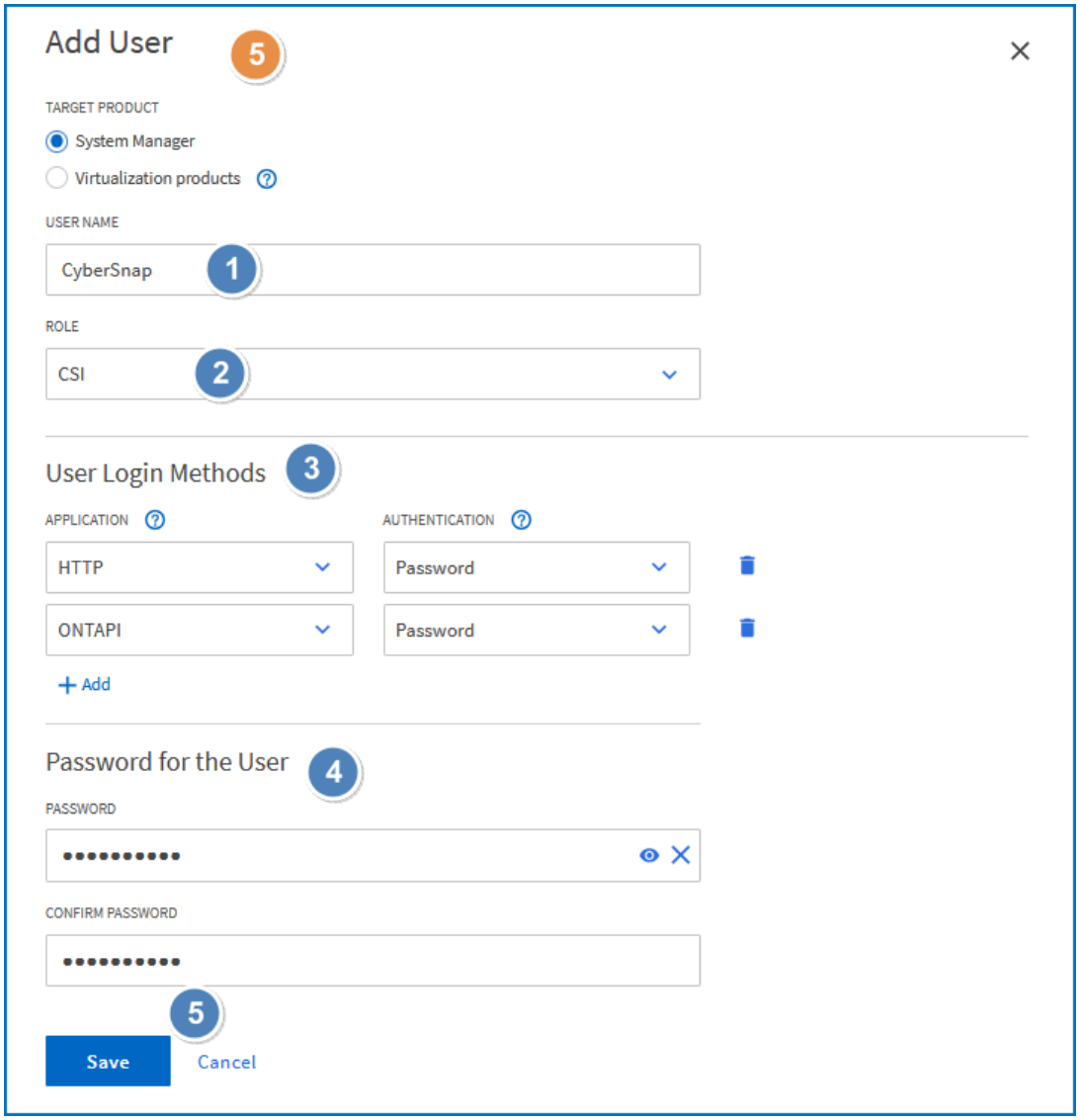


After creating a custom role, create a user and assign the newly created role to them.

1. Log in to the NetApp system.
2. Navigate to "Cluster" and then select "Settings."
3. Within "Settings," click on "User and Roles."



4. Under "Users," click on the "Add" button to open a new window.
5. In the "Add User" window:
    1. Enter the desired username.
    2. In the Role dropdown menu choose role that you created in previous step
    3. In “User Login Methods”
        - In Application
            - choose **HTTP** from dropdown menu
            - Select “Password” as “AUTHENTICATION”
            - Click on Plus sign to add new application
            - choose **ONTAPI** from dropdown menu
            - Select “Password” as “AUTHENTICATION”
    4. Configure the desired password for user
    5. Click on the Save button



Now you have configured a dedicated NetApp account with the limited privileges required for CyberSnap to operate effectively.

Upgrading to the Latest Version of CyberSnap

To successfully upgrade CyberSnap to the latest version, you must complete certain prerequisites in advance. Please note that CyberSnap officially supports upgrades only from the previous build version. If your current build version is more than one version behind, you must request support from the CyberSnap support team.

Before performing an upgrade, it is important to verify whether any CyberSnap policies are currently running or scheduled as background tasks. Review the policy status and take the following actions as appropriate:

- Policy is in the monitoring state
  - No action is required.
- Policy is in Monitoring state with a scheduler configured
  - Disable the policy to prevent it from being triggered automatically during the upgrade.
- Policy is in Scanning state
  - Disable the policy. The policy will move into a Pending Disable state.

    - Wait until the active scan completes.
    - Verify that the policy status changes to Disabled.
- Policy is not in Monitoring or Disabled state
    - Disable the policy to ensure it is not triggered by CyberSnap during the upgrade process.

All prerequisites have been met, and you can proceed with installing the new version of CyberSnap. Once the upgrade is complete, sign in to the console and re-enable the policies that were disabled at the start of the upgrade process.

Applying custom PFX certificate

This chapter describes the complete certificate replacement process, including all prerequisites and requirements that must be satisfied before replacing the out-of-the-box (self-signed) certificate with a customer-supplied domain certificate in CyberSnap.

The table below provides a concise reference of all prerequisites before proceeding with certificate replacement. Each item is described in full in the sections that follow.

Requirement	Details	Notes
PFX File (.pfx)	Certificate bundled with private key and password-protected	Password must be recorded for encryption
CyberSnapPasswordEncryptor.exe	Utility to encrypt the PFX password	Download required before configuration
File System Access	Write access to the CyberSnap web server directory	Administrator privileges required
appsettings.json Access	Ability to edit the CSI configuration file	Use a plain-text editor (e.g., Notepad++)
Service Restart Rights	Permission to stop and start the CyberSnap service	Required to apply changes after config update

PFX File

You need to generate a PFX certificate that will be used by the CyberSnap service. This document does not cover the process of creating a PFX file, as it is assumed that the necessary knowledge and infrastructure are already in place to generate the required certificate.

Copy the PFX certificate file to the following directory:

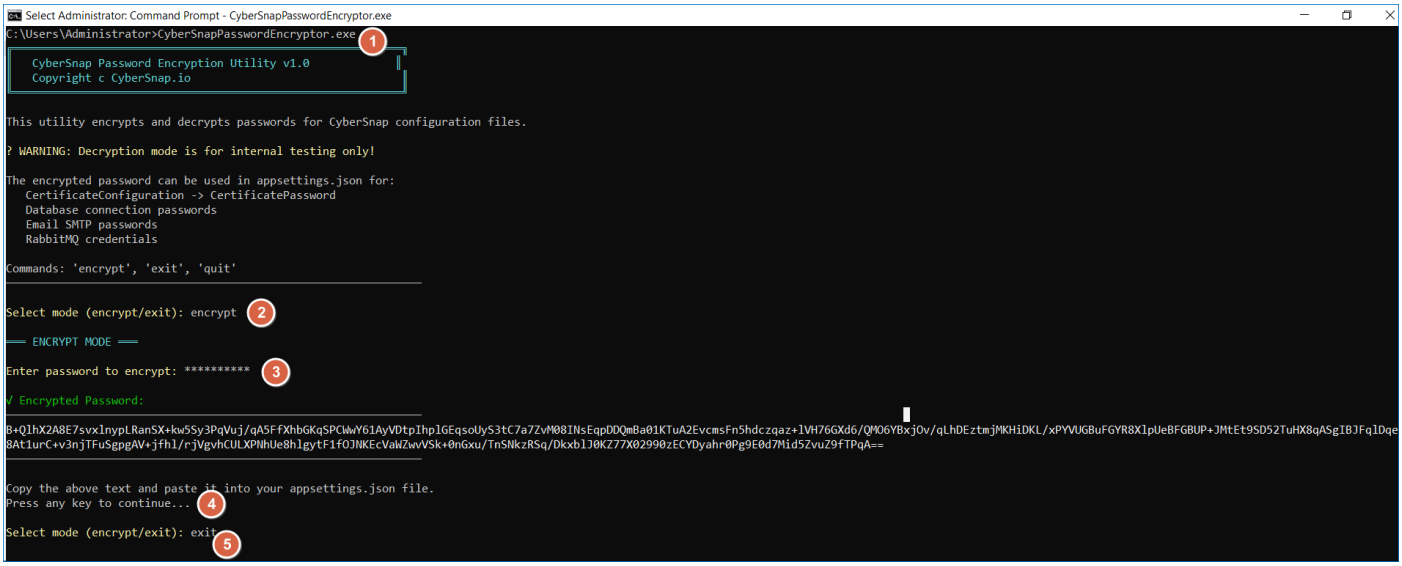
- C:\Program Files (x86)\CyberSnap.io\CyberSnap\web server\

Utility to encrypt the PFX password

Download the password encryption utility from the official CyberSnap download server before proceeding:

- https://download.cybersnap.io/LatestDownload/CyberSnapPasswordEncryptor.exe

Follow the steps below to launch the utility and generate the encrypted password string required for the appsettings.json file.



1. Double-click CyberSnapPasswordEncryptor.exe in Windows Explorer, or open a command prompt, navigate to the download location, and run CyberSnapPasswordEncryptor.exe

2. The console window opens and the application displays a command prompt, waiting for input. At the prompt, type the following command and press Enter:
   - Encrypt

   The application acknowledges the command and prompts you to enter the password to be encrypted.

   NOTE: To exit the utility at the command prompt type exit and press Enter.

3. Enter the PFX password
   - When prompted for input, type the exact password you set when creating the PFX file and press Enter.

IMPORTANT: The password is case-sensitive. Enter it exactly as specified during PFX creation. Any difference will produce an encrypted value that does not match the certificate and will cause the CyberSnap service to fail on startup.

Select the entire encrypted string in the console window, copy it (Ctrl+C or right-click → Copy), and paste it into Notepad or another plain-text editor for temporary storage. You will paste this value into appsettings.json in the next phase.

4. Exit the utility
   - After copying the encrypted key, the console displays a prompt to press any key to continue. Press any key to return to the main menu.

5. Type the following command and press Enter to close the utility:
   - exit

The password encryption process is completed.

Editing the CSI configuration file

Once the PFX certificate file has been copied to the designated folder and the password has been encrypted, all prerequisites are satisfied. The next step is to open the appsettings.json file and update the required fields.

The configuration file is located at the following path:

- C:\Program Files (x86)\CyberSnap.io\CyberSnap\web server\appsettings.json

The configuration file appsettings.json is in JSON format. The relevant section for certificate configuration is "**CertificateConfiguration**". Before making any changes please backup original appsettings.json file. The structure below illustrates the target section:

```
{
  "CertificateConfiguration": {
    "CertificateName": "<your-pfx-filename.pfx>",
    "CertificatePassword": "<encrypted-password-string>"
  }
}
```

Replace necessary values and save the appsettings.json file.

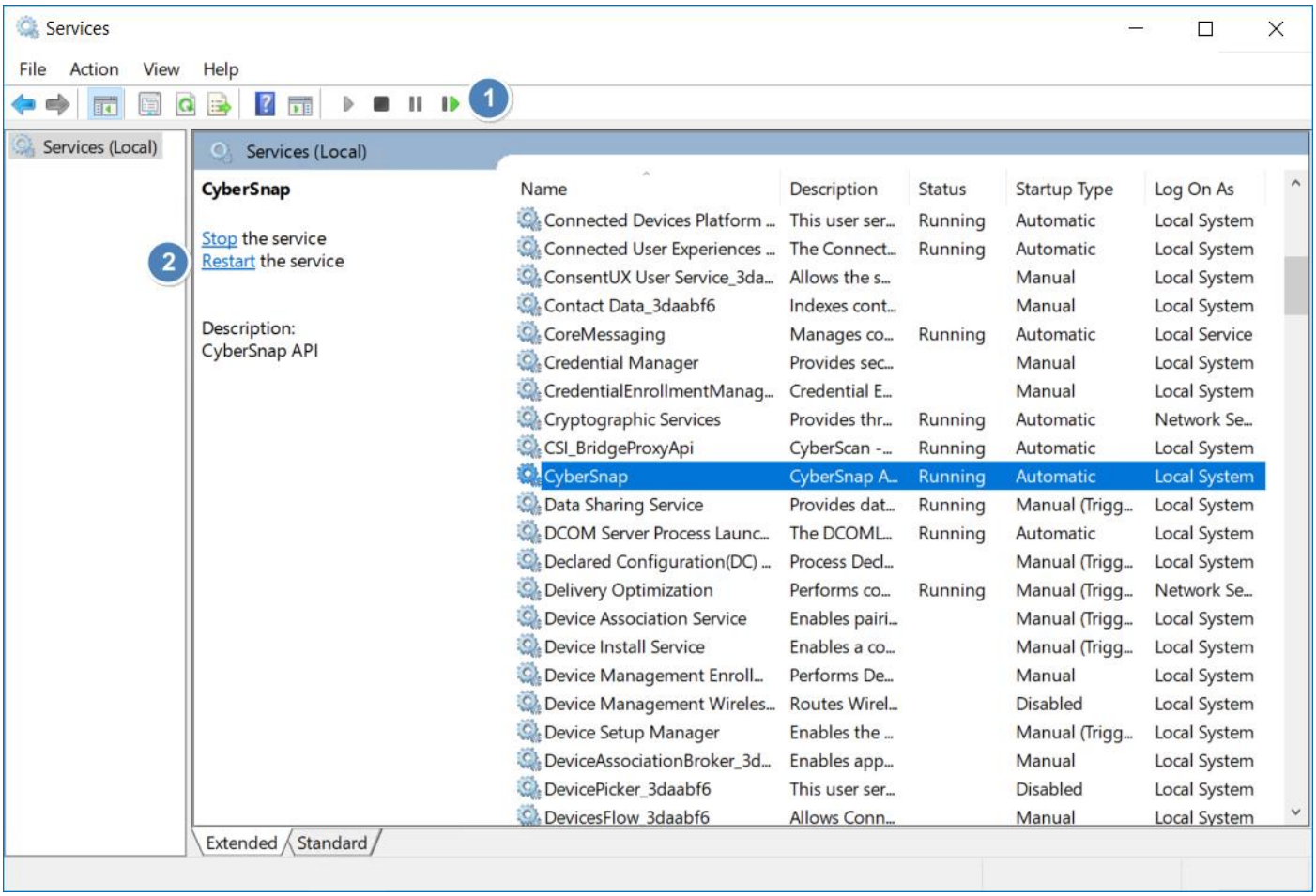
- Replace "<your-pfx-filename.pfx>" with the name of your PFX file.
- Replace "<encrypted-password-string>" with the encrypted password generated in the previous step.

Ensure the JSON is well-formed after editing. Malformed JSON (e.g. missing commas, mismatched braces, or unescaped characters) will prevent the CyberSnap service from starting.

Once all changes have been made and the file has been saved, you can proceed to restart the **CyberSnap** service.

Service Restart

To restart the service, click the **Restart** icon (1) in the service console, or select the **Restart service** option (2) from the service console menu.



If all configurations have been completed correctly, the service will restart successfully. You can then open the HTTPS URL of the CSI console to verify that the browser recognizes the certificate as valid. If the browser indicates that the URL is “Not Secure,” verify that the PFX certificate covers the specified URL (hostname). If the PFX certificate needs to be redeployed, you must repeat the entire process described in this section.