



BlueXP ransomware protection documentation

BlueXP ransomware protection

NetApp
March 22, 2024

Table of Contents

- BlueXP ransomware protection documentation 1
- Release notes: What’s new with BlueXP ransomware protection preview 2
 - 5 March 2024 2
 - 6 October 2023 2
- Get started 3
 - Learn about BlueXP ransomware protection preview 3
 - BlueXP ransomware protection prerequisites 7
 - Quick start for BlueXP ransomware protection 7
 - Set up BlueXP ransomware protection 8
 - Access BlueXP ransomware protection 9
 - Discover workloads in BlueXP ransomware protection 10
 - Configure BlueXP ransomware protection settings 11
 - Frequently asked questions for BlueXP ransomware protection 16
- Use BlueXP ransomware protection 18
 - Use BlueXP ransomware protection 18
 - View workload health at a glance using the Dashboard 18
 - Protect workloads against ransomware attacks 21
 - Respond to a detected ransomware alert 27
 - Recover from a ransomware attack (after incidents are neutralized) 29
- Knowledge and support 36
 - Register for support 36
 - Get help 40
- Legal notices 46
 - Copyright 46
 - Trademarks 46
 - Patents 46
 - Privacy policy 46
 - Open source 46

BlueXP ransomware protection documentation

Release notes: What's new with BlueXP ransomware protection preview

Learn what's new in BlueXP ransomware protection preview.

5 March 2024

This preview release of BlueXP ransomware protection includes the following updates:

- **Protection policy management:** In addition to using predefined policies, you can now create, change, and delete policies. [Learn more about managing policies.](#)
- **Immutability on secondary storage (DataLock):** You can now make the backup immutable in secondary storage using NetApp DataLock technology in the object store. [Learn more about creating protection policies.](#)
- **Automatic backup to NetApp StorageGRID:** In addition to using AWS, you can now choose StorageGRID as your backup destination. [Learn more about configuring backup destinations.](#)
- **Additional features to investigate potential attacks:** You can now view more forensic details to investigate the detected potential attack. [Learn more about responding to a detected ransomware alert.](#)
- **Recovery process.** The recovery process was enhanced. Now, you can recovery volume by volume, all volumes for a workload, or even a few files from the volume all in a single workflow. [Learn more about recovering from a ransomware attack \(after incidents have been neutralized\).](#)

[Learn about BlueXP ransomware protection.](#)

6 October 2023

The BlueXP ransomware protection service is a SaaS solution for protecting data, detecting potential attacks, and recovering data from a ransomware attack.

For the preview version, the service protects application-based workloads of Oracle, MySQL, VM datastores, and file shares on on-premises NAS storage as well as Cloud Volumes ONTAP on AWS (using the NFS protocol) across BlueXP accounts individually and backs up data to Amazon Web Services cloud storage.

The BlueXP ransomware protection service provides full use of several NetApp technologies so that your data security administrator or security operations engineer can accomplish the following goals:

- View ransomware protection on all your workloads at a glance.
- Gain insight into ransomware protection recommendations
- Improve protection posture based on BlueXP ransomware protection recommendations.
- Assign ransomware protection policies to protect your top workloads and high-risk data against ransomware attacks.
- Monitor the health of your workloads against ransomware attacks looking for data anomalies.
- Quickly assess the impact of ransomware incidents on your workload.
- Recover from ransomware incidents intelligently by restoring data and ensuring that reinfection from stored data does not occur.

[Learn about BlueXP ransomware protection.](#)

Get started

Learn about BlueXP ransomware protection preview

Ransomware attacks can block access to your systems and data and attackers can ask for ransom in exchange for the release of data or decryption. According to the IDC, it is not uncommon for victims of ransomware to experience multiple ransomware attacks. The attack can disrupt access to your data between one day and several weeks.

BlueXP ransomware protection is an orchestration service for ransomware protection, detection, and recovery. For the preview version, the service protects application-based workloads of Oracle, MySQL, VM datastores, and file shares on on-premises NAS storage as well as Cloud Volumes ONTAP in Amazon Web Services (using the NFS protocol) across BlueXP accounts and backs up data to Amazon Web Services cloud storage or NetApp StorageGRID.



THIS DOCUMENTATION IS PROVIDED AS A TECHNOLOGY PREVIEW. With this preview offering, NetApp reserves the right to modify offering details, contents, and timeline before General Availability.

What you can do with BlueXP ransomware protection

The BlueXP ransomware protection service provides full use of several NetApp technologies so that your storage administrator, data security administrator, or security operations engineer can accomplish the following goals:

- **Identify** all application-based, file-share, or VMware-managed workloads in NetApp on-premises NAS with NFS working environments in BlueXP, across BlueXP accounts, workspaces, and BlueXP Connectors. The service then categorizes the data priority and provides recommendations to you for ransomware protection improvements.
- **Protect** your workloads by enabling backups and Snapshot copies on your data.
- **Detect** anomalies that might be ransomware attacks.
- **Respond** to potential ransomware attacks by automatically initiating a NetApp ONTAP Snapshot copy.
- **Recover** your workloads that help accelerate workload uptime by orchestrating several NetApp technologies. You can choose to recover volumes, folders, or specific files. The service provides recommendations on the best options.

Benefits of using BlueXP ransomware protection

BlueXP ransomware protection offers the following benefits:

- Discovers workloads and datasets, analyzes the priority based on usage index, and ranks their relative importance.
- Evaluates your ransomware protection posture and displays it in an easy-to-understand dashboard.
- Provides recommendations on next steps based on discovery and protection posture analysis.
- Applies AI/ML-driven data protection recommendations with one-click access.

- Protects data in top application-based workloads, such as MySQL, Oracle, VMware datastores and file-shares.
- Detects ransomware attacks on data in real time on primary storage using AI technology.
- Initiates automated actions in response to detected potential attacks by creating Snapshot copies and initiating alerts about abnormal activity.
- Applies curated recovery to meet RPO policies. BlueXP ransomware protection orchestrates recovery from ransomware incidents by using several NetApp recovery services, including BlueXP backup and recovery (formerly Cloud Backup).

Cost

NetApp doesn't charge you for using the preview version of BlueXP ransomware protection.

Licensing

The BlueXP ransomware protection preview itself does not require any special licensing. All preview licenses are Evaluation licenses.



For the preview version, NetApp helps to set up the evaluation and any required licenses.

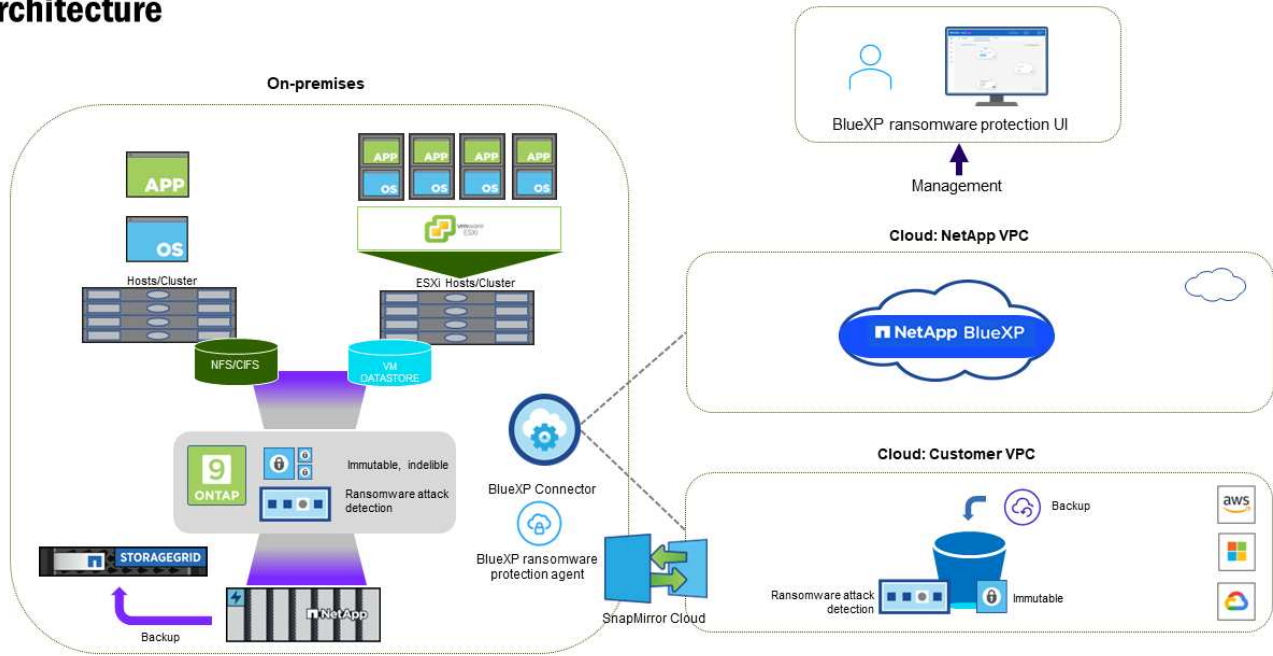
The BlueXP ransomware protection preview requires the following licenses:

- ONTAP
- NetApp Autonomous Ransomware Protection technology. Refer to [Autonomous Ransomware Protection overview](#) for details.
- BlueXP backup and recovery service

How BlueXP ransomware protection works

At a high-level, BlueXP ransomware protection works like this.

Architecture



Feature	Description
IDENTIFY	<ul style="list-style-type: none"> Finds all customer on-premises NAS (NFS mounts) data connected to BlueXP. Identifies customer data from ONTAP service APIs and associates it with workloads. Learn more about ONTAP and SnapCenter Software. Discovers each volume's current protection level of NetApp Snapshot copies and backup policies as well as any on-box detection capabilities. The service then associates this protection posture with the workloads by using BlueXP backup and recovery, BlueXP digital advisor, and ONTAP services and NetApp technologies such as Autonomous Ransomware Protection, FPolicy, Backup policies, and Snapshot policies. Learn more about Autonomous Ransomware Protection and BlueXP backup and recovery, BlueXP Digital Advisor, and ONTAP FPolicy. Assigns a business priority to each workload based on automatically discovered protection levels and recommends protection policies for workloads based on their business priority. Ransomware protection also learns the policy associations and recommends your custom policies to similar workloads.
PROTECT	<ul style="list-style-type: none"> Actively monitors workloads and orchestrates the use of BlueXP backup and recovery and ONTAP APIs by applying policies to each of the identified workloads.

Feature	Description
DETECT	<ul style="list-style-type: none"> • Detects potential attacks with an integrated machine learning (ML) model that detects potentially anomalous encryption and activity. • Provides dual-layer detection that starts with detecting potential ransomware attacks in the primary storage and responding to abnormal activities by taking additional automated Snapshot copies to create the nearest data restore points. The service provides the ability to dig deeper to identify potential attacks with greater precision without impacting the performance of the primary workloads. • Determines the specific suspect files and maps that attack to the associated workloads, using ONTAP, Autonomous Ransomware Protection and FPolicy technologies.
RESPOND	<ul style="list-style-type: none"> • Shows relevant data, such as file activity, user activity, and entropy, to help you complete forensic reviews about the attack. • Initiates quick Snapshot copies by using NetApp technologies and products such as ONTAP, Autonomous Ransomware Protection and FPolicy.
RECOVER	<ul style="list-style-type: none"> • Determines the best Snapshot or backup and recommends the best recovery point actual (RPA) by using BlueXP backup and recovery, ONTAP, Autonomous Ransomware Protection and FPolicy technologies and services. • Orchestrates the recovery of workloads including VMs, file shares, and databases with application consistency.

Supported backup targets, working environments, and data sources

Use BlueXP ransomware protection preview to see how resilient your data is to a cyber attack on the following types of backup targets, working environments, and data sources:

Backup targets supported

- Amazon Web Services (AWS) S3
- NetApp StorageGRID

Supported working environments

- On-premises ONTAP NAS (using NFS protocol)
- ONTAP Select
- Cloud Volumes ONTAP in AWS (using NFS protocol)

Data sources

For the preview version, the service protects the following application-based workloads:

- NetApp file shares
- VMware datastores
- Databases (For the preview version, Oracle and MySQL)

Terms that might help you with ransomware protection

You might benefit by understanding some terminology related to ransomware protection.

- **Protection:** Protection in BlueXP ransomware protection means ensuring that Snapshots and immutable backups occur on a regular basis to a different security domain using protection policies.
- **Workload:** A workload in BlueXP ransomware protection preview can include MySQL or Oracle databases, VMware datastores, or file shares.

BlueXP ransomware protection prerequisites

Get started with BlueXP ransomware protection by verifying the readiness of your operational environment, login, network access, and web browser.

To use BlueXP ransomware protection preview version, you'll need these prerequisites:

- An account in NetApp StorageGRID or AWS S3 for backup targets and the access permissions set

Refer to the [AWS permissions list](#) for details.

- ONTAP 9.11.1 and later
 - Cluster admin ONTAP permissions
 - A license for NetApp Autonomous Ransomware Protection, used by BlueXP ransomware protection, enabled on the on-premises ONTAP instance, depending on the version of ONTAP you are using. Refer to [Autonomous Ransomware Protection overview](#).

For more licensing details, refer to [Learn about BlueXP ransomware protection](#).

- In BlueXP:
 - A BlueXP Connector per each Virtual Private Cloud (VPC) or on an on-premises region must be set up in BlueXP. Refer to [BlueXP documentation to configure the Connector](#).



If you have multiple BlueXP Connectors, the service will scan data across all Connectors beyond the one that currently shows in the BlueXP UI.

- The BlueXP backup and recovery service with backup enabled on the working environment
- A BlueXP working environment with NetApp NAS on-premises storage
- A BlueXP account with at least one active Connector connecting to on-premises ONTAP clusters. All source and working environments must be on the same BlueXP account.
- A BlueXP user account with Account Admin privileges for discovering resources
- [Standard BlueXP requirements](#)

Quick start for BlueXP ransomware protection

Here's an overview of the steps needed to get started with BlueXP ransomware protection. The links within each step take you to a page that provides more details.

1

Review prerequisites

Ensure your environment meets these requirements.

2

Set up the ransomware protection service

- [Prepare NetApp StorageGRID or Amazon Web Services as a backup destination.](#)
- [Configure a Connector in BlueXP.](#)
- [Configure backup destinations.](#)
- [Discover workloads in BlueXP.](#)

3

What's next?

After you set up the service, here's what you might do next.

- [View workload protection health on the Dashboard.](#)
- [Protect workloads.](#)
- [Respond to detection of potential ransomware attacks.](#)
- [Recover from an attack \(after incidents are neutralized\).](#)

Set up BlueXP ransomware protection

To use BlueXP ransomware protection, perform a few steps to set it up.

Before you begin, review [prerequisites](#) to ensure that your environment is ready.

Prepare the backup destination

Prepare one of the following backup destinations:

- NetApp StorageGRID
- Amazon Web Services

After you configure options in the backup destination itself, you will later configure it as a backup destination in the BlueXP ransomware protection service.

Prepare StorageGRID to become a backup destination

If you want to use StorageGRID as your backup destination, refer to [StorageGRID documentation](#) for details about StorageGRID.

Prepare AWS to become a backup destination

- Set up an account in AWS.
- Configure [AWS permissions](#) in AWS.

For details about managing your AWS storage in BlueXP, refer to [Manage your Amazon S3 buckets](#).

Set up BlueXP

The next step is to set up BlueXP and the BlueXP ransomware protection service.

Review [standard BlueXP requirements](#).

Create a Connector in BlueXP

You should reach out to your NetApp Sales Rep to try out this service. Then, when you use the BlueXP Connector, it will include the appropriate capabilities for the ransomware protection service.

To create a Connector in BlueXP before using the service, refer to the BlueXP documentation that describes [how to create a BlueXP Connector](#).



If you have multiple BlueXP Connectors, the service will scan data across all Connectors beyond the one that currently shows in the BlueXP UI. This service discovers all workspaces and all Connectors associated with this account.

Access BlueXP ransomware protection

You use NetApp BlueXP to log in to the BlueXP ransomware protection service. From the BlueXP left navigation, select **Protection > Ransomware protection**.

For details, refer to [Access BlueXP ransomware protection](#).

Configure backup destinations in BlueXP ransomware protection

Use the BlueXP ransomware protection backup destinations option to configure backup destinations. For details, refer to [Configure settings options](#).

Access BlueXP ransomware protection

You use NetApp BlueXP to log in to the BlueXP ransomware protection service.

To log in to BlueXP, you can use your NetApp Support Site credentials or you can sign up for a NetApp cloud login using your email and a password. [Learn more about logging in](#).

Steps

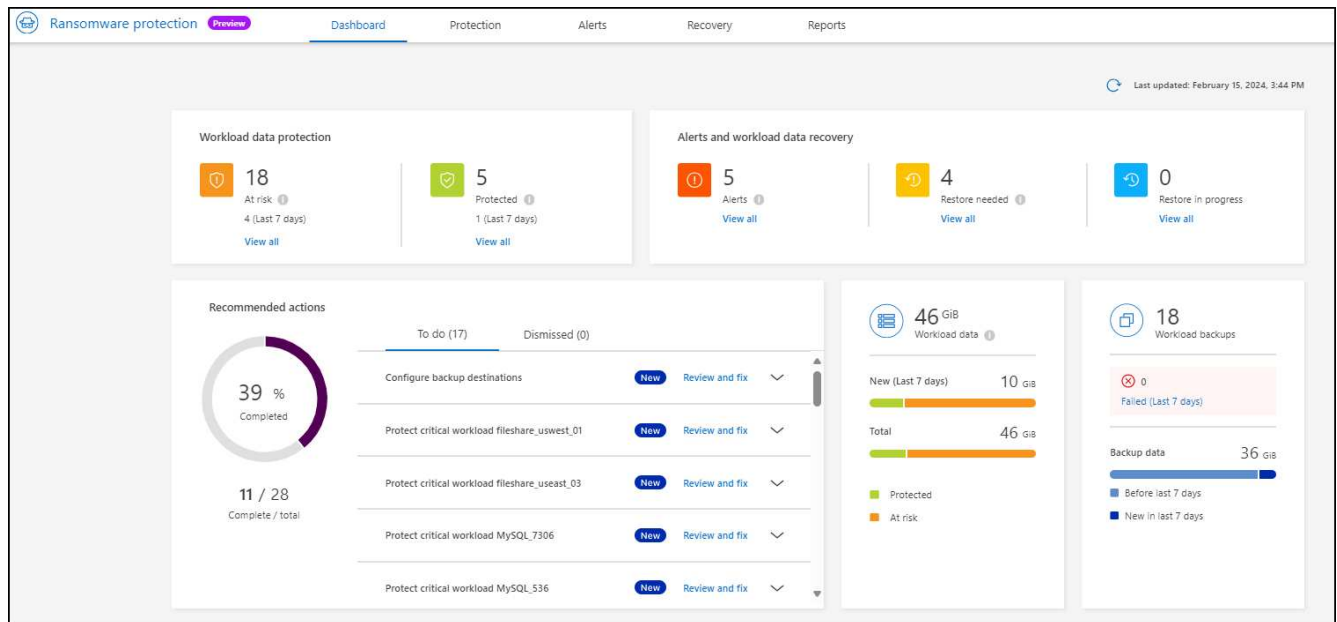
1. Open a web browser and go to the [BlueXP console](#).

The NetApp BlueXP login page appears.

2. Log in to BlueXP.
3. From the BlueXP left navigation, select **Protection > Ransomware protection**.

If this is your first time logging in to this service, the landing page appears.

Otherwise, the BlueXP ransomware protection Dashboard appears.



4. Start using the service.

- If you don't have a BlueXP Connector or it's not the one for this preview, you might need to contact NetApp Support or follow messages to sign up for this preview.
- If you are new to BlueXP and haven't used any Connector, when you select "**Ransomware protection**", a message appears about signing up. Go ahead and submit the form. NetApp will contact you about your evaluation request.
- If you are a BlueXP user with an existing Connector, when you select "**Ransomware protection**", a message appears about signing up.
- If you are already participating in the preview, when you select "**Ransomware protection**", you can proceed with the service. If you haven't done so already, you should select the **Discover workloads** option.

Discover workloads in BlueXP ransomware protection

To use BlueXP ransomware protection, the service needs to first discover data. During discovery, BlueXP ransomware protection analyzes all volumes and files in working environments across all BlueXP Connectors and workspaces within an account.



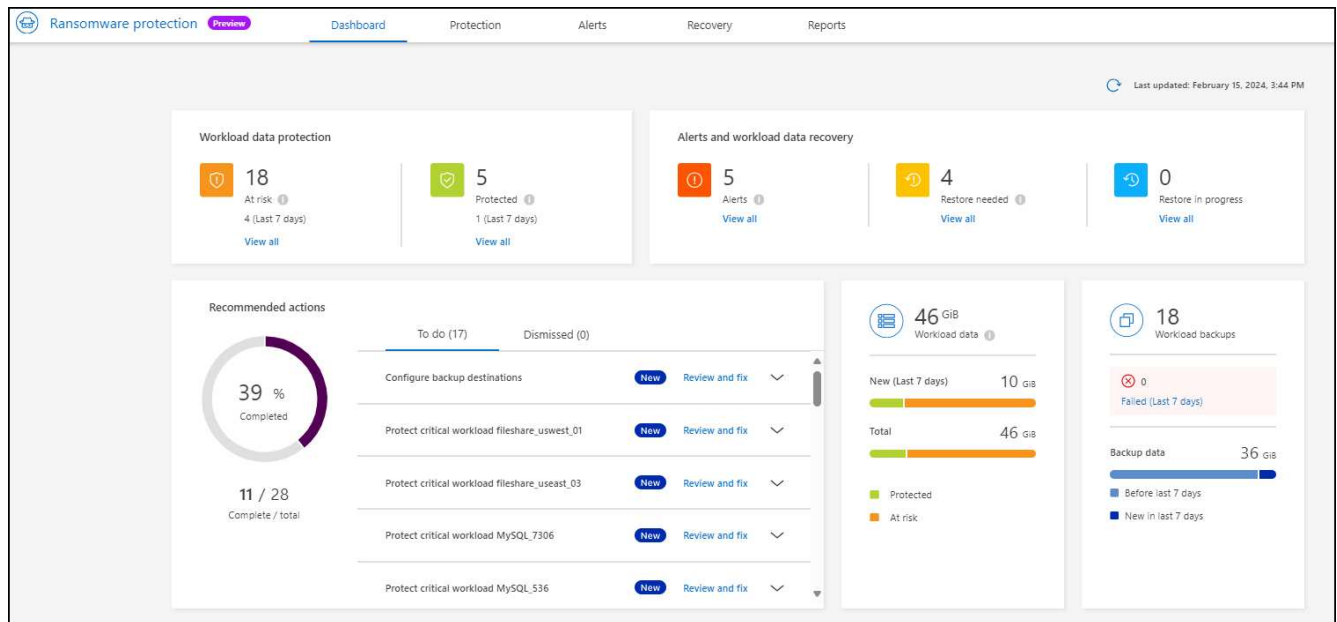
For the preview version, BlueXP ransomware protection assesses MySQL applications, Oracle applications, VMware datastores, and file shares.

The service assesses the existing protection level including the current backup protection, Snapshot copies, and NetApp Autonomous Ransomware Protection options. Based on the assessment, the service then recommends how to improve your ransomware protection.

Steps

1. From the BlueXP left navigation, select **Protection > Ransomware protection**.
2. Select **Discover workloads** from the initial landing page.

The service discovers workload data and shows the health of data protection in the Dashboard.



Configure BlueXP ransomware protection settings

You can configure a backup destination by reviewing recommendations on the Dashboard.

Add a backup destination

BlueXP ransomware protection can identify workloads that do not have any backups yet and also workloads that do not have any backup destinations assigned yet.

To protect those workloads, you should add a backup destination. You can choose one of the following backup destinations:

- NetApp StorageGRID
- Amazon Web Services (AWS)

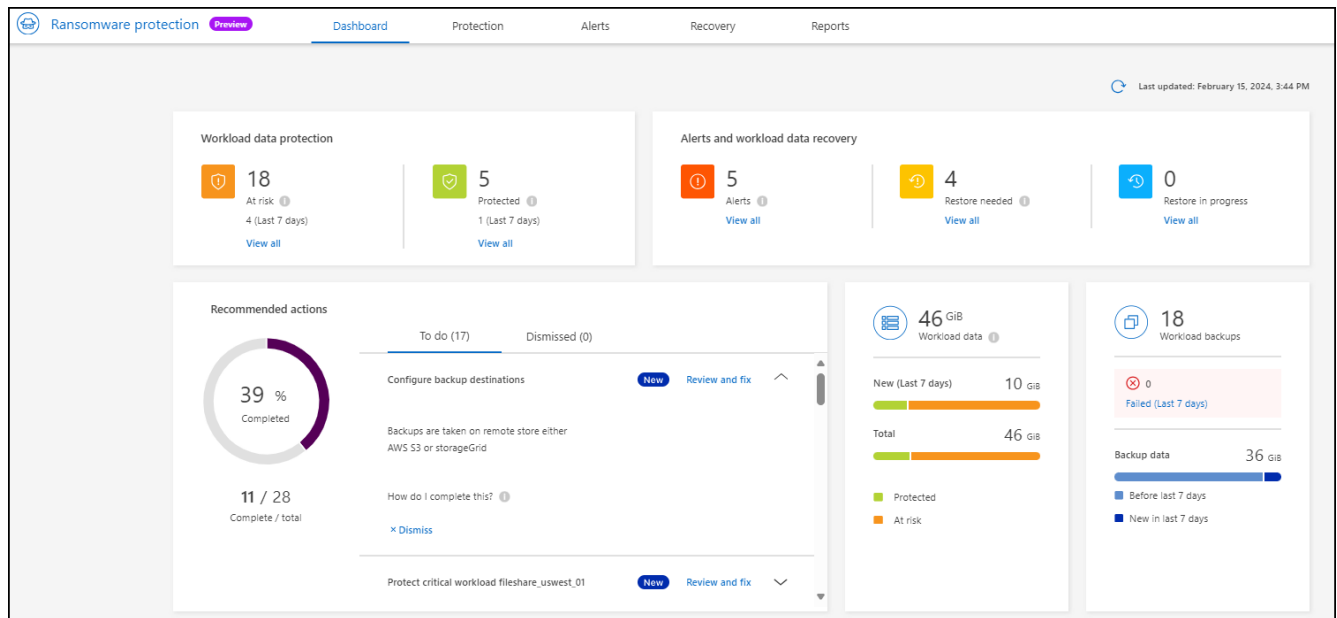
You can add a backup destination based on a recommended action from the Dashboard.

Access Backup Destination options from the Dashboard's recommended actions

The Dashboard provides many recommendations. One recommendation might be to configure a backup destination.

Steps

1. From the BlueXP left navigation, select **Protection > Ransomware protection**.
2. Review the Dashboard's Recommended actions pane.





3. From the Dashboard, select **Review and fix** for the recommendation of "Configure backup destinations."
4. Continue with instructions depending on the backup provider.

Add StorageGRID as a backup destination

To set up NetApp StorageGRID as a backup destination, enter the following information.

1. In the **Settings > Backup destinations** page, select **Add**.
2. Enter a name for the backup destination.

Add backup destination

Name	backup-dest1	▼
Provider	i Action required	▲
Select a provider to back up to the cloud.		
<div style="display: flex; justify-content: space-around; gap: 20px;"> <div style="text-align: center;">  <p>Amazon Web Services</p> </div> <div style="text-align: center;">  <p>StorageGRID</p> </div> </div>		
Provider settings	Defined by provider selection	▼
Networking	Defined by provider selection	▼
Backup lock	Defined by provider selection	▼

Cancel
Add

3. Select **StorageGRID**.

4. Select the Down arrow next to each setting and enter or select values:

- **Provider settings:**
 - Create a new bucket or bring your own bucket that will store the backups.
 - StorageGRID gateway node fully qualified domain name, port, StorageGRID access key and secret key credentials.
- **Networking:** Choose the IPspace.
 - The IPspace is the cluster where the volumes you want to back up reside. The intercluster LIFs for this IPspace must have outbound internet access.
- **Backup lock:** Choose whether you want the service to protect backups from being modified or deleted. This option uses the NetApp DataLock technology. Each backup will be locked during the retention period, or for a minimum of 30 days, plus a buffer period of up to 14 days.



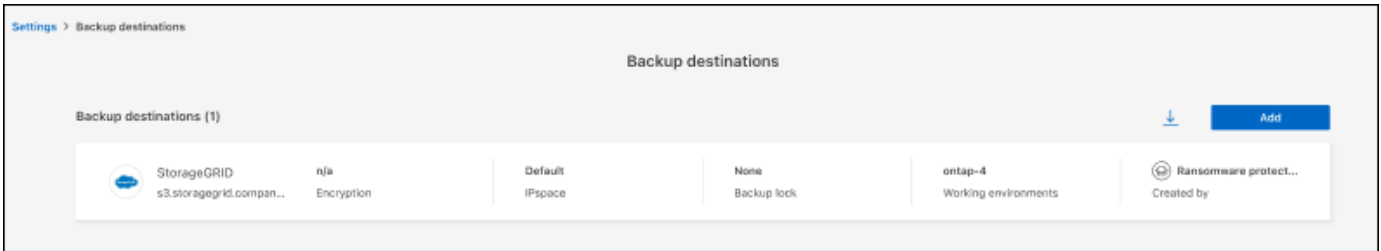
If you configure the backup lock setting now, you cannot change the setting later after the backup destination is configured.

- **Compliance mode:** Users cannot overwrite or delete protected backup files during the retention period.

5. Select **Add**.

Result

The new backup destination is added to the list of backup destinations.

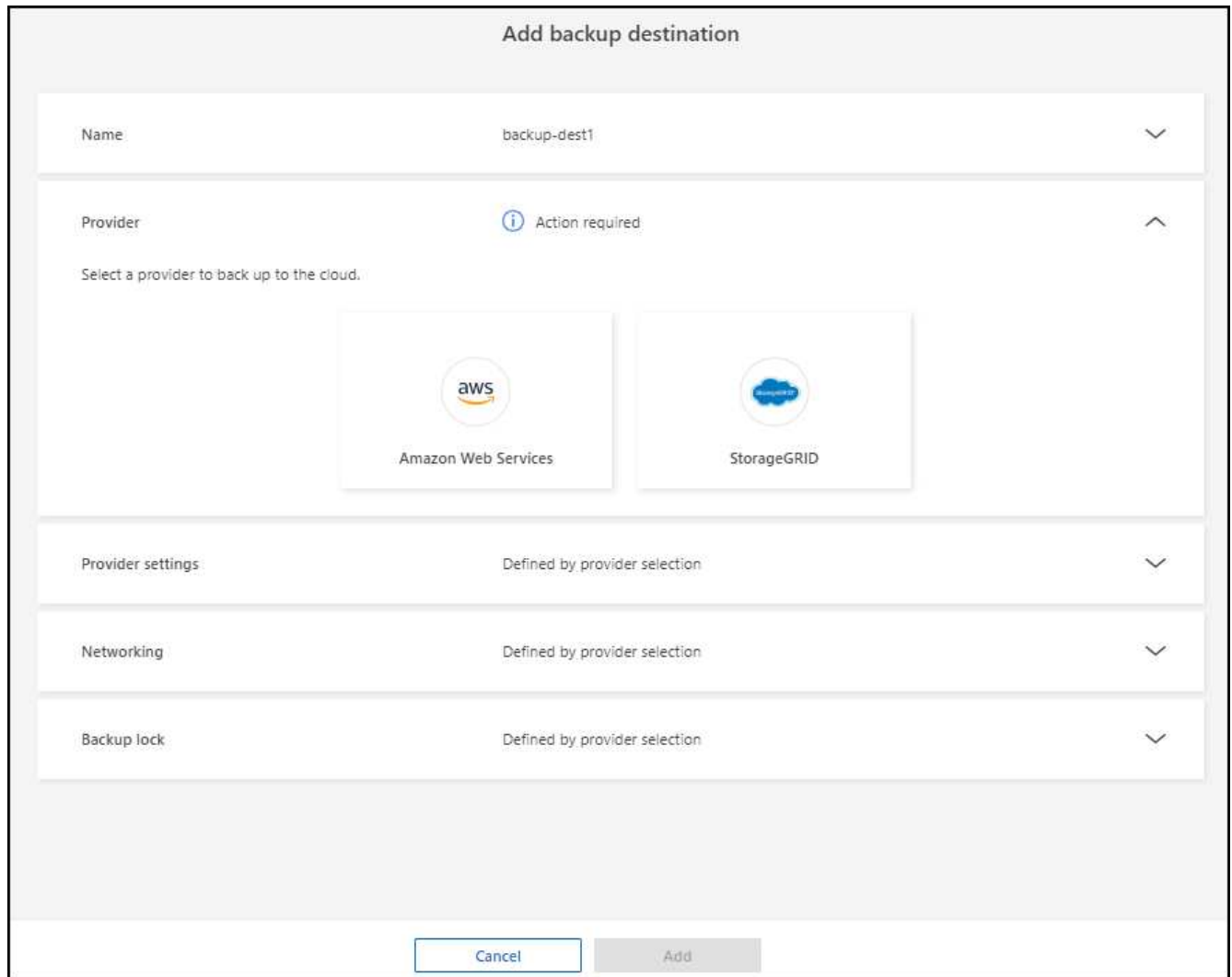


Add Amazon Web Services as a backup destination

To set up AWS as a backup destination, enter the following information.

For details about managing your AWS storage in BlueXP, refer to [Manage your Amazon S3 buckets](#).

1. In the **Settings > Backup destinations** page, select **Add**.
2. Enter a name for the backup destination.



3. Select **Amazon Web Services**.

4. Select the Down arrow next to each setting and enter or select values:

◦ **Provider settings:**

- Create a new bucket, select an existing bucket if one already exists in BlueXP, or bring your own bucket that will store the backups.
- AWS account, region, access key and secret key for AWS credentials

If you want to bring your own bucket, refer to [Add S3 buckets](#).

- **Encryption:** If you are creating a new S3 bucket, enter encryption key information given to you from the provider. If you chose an existing bucket, encryption information is already available.

Data in the bucket is encrypted with AWS-managed keys by default. You can continue to use AWS-managed keys, or you can manage the encryption of your data using your own keys.

- **Networking:** Choose the IPspace and whether you'll be using a Private Endpoint.

- The IPspace is the cluster where the volumes you want to back up reside. The intercluster LIFs for this IPspace must have outbound internet access.
- Optionally, choose whether you'll use an AWS private endpoint (PrivateLink) that you previously configured.

If you want to use AWS PrivateLink, refer to [AWS PrivateLink for Amazon S3](#).

- **Backup lock:** Choose whether you want the service to protect backups from being modified or deleted. This option uses the NetApp DataLock technology. Each backup will be locked during the retention period, or for a minimum of 30 days, plus a buffer period of up to 14 days.



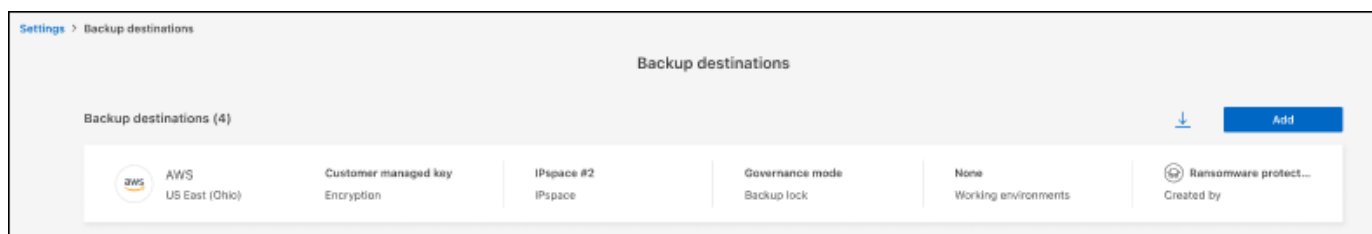
If you configure the backup lock setting now, you cannot change the setting later after the backup destination is configured.

- **Governance mode:** Specific users (with s3:BypassGovernanceRetention permission) can overwrite or delete protected files during the retention period.
- **Compliance mode:** Users cannot overwrite or delete protected backup files during the retention period.

5. Select **Add**.

Result

The new backup destination is added to the list of backup destinations.



Frequently asked questions for BlueXP ransomware protection

This FAQ can help if you're just looking for a quick answer to a question.

Access

What's the BlueXP ransomware protection URL?

For the URL, in a browser, enter: <https://console.bluexp.netapp.com/> to access the BlueXP console.

Do you need a license to use BlueXP ransomware protection?

A NetApp License File (NLF) is not required. The BlueXP ransomware protection preview itself does not require any special licensing. All preview licenses are Evaluation licenses.

The preview version of this service requires a BlueXP backup and recovery service license.



For the preview version, NetApp helps to set up the evaluation and any required licenses.

How do you enable BlueXP ransomware protection?

BlueXP ransomware protection does not require any enablement. The ransomware protection option is automatically enabled on the BlueXP left navigation.

For the preview version, you need to sign up or reach out to your NetApp Sales rep to try out this service. Then, when you use the BlueXP Connector, it will include the appropriate capabilities for the service.

Does BlueXP ransomware protection available in standard, restricted, and private modes?

At this time, BlueXP ransomware protection is available only in standard mode. Stay tuned for more.

For an explanation about these modes across all BlueXP services, refer to [BlueXP deployment modes](#).

How are access permissions handled?

Only account admins have the ability to initiate the service and discover workloads (because this involves committing to usage of a resource). Subsequent interactions can be done by any role.

What device resolution is best?

The recommended device resolution for BlueXP ransomware protection is 1920x1080 or better.

Which browser should I use?

Any modern browser will work.

Interaction with other services

Is BlueXP ransomware protection aware of protection settings made in NetApp ONTAP?

Yes, BlueXP ransomware protection discovers Snapshot schedules set in ONTAP.

If you set a policy using BlueXP ransomware protection, do you have to make future changes only in this service?

We recommend that you make policy changes from the BlueXP ransomware protection service.

Workloads

What makes up a workload?

A workload includes all volumes that are used by a single application instance. For example, an Oracle DB instance deployed on ora3.host.com can have vol1 and vol2 for its data and logs, respectively. Those volumes together constitute the workload for that specific instance of the Oracle DB instance.

How does BlueXP ransomware protection prioritize workload data?

Data priority for the Preview version is determined by the Snapshot copies made and backups that are scheduled.

The workload priority is determined by the following Snapshot frequencies:

- **Critical:** Snapshot copies taken less than 1 per hour (highly aggressive protection schedule)
- **Important:** Snapshot copies taken less than 1 per day but greater than 1 per hour
- **Standard:** Snapshot copies taken more than 1 per day

New volume added, but doesn't appear yet

If you added a new volume to your environment, initiate discovery again and apply protection policies to protect that new volume.

The Dashboard doesn't show all my workloads. What might be wrong?

Currently, only NFS volumes are supported. iSCSI volumes, CIFS volumes and other non-supported configurations are filtered out and do not appear on the Dashboard.

Protection policies

Do BlueXP ransomware policies co-exist with the other kinds of workload policies?

At this time, BlueXP backup and recovery (Cloud Backup) supports one backup policy per volume. So, BlueXP backup and recovery and BlueXP ransomware protection share backup policies.

Snapshot copies are not limited and can be added separately from each service.

Use BlueXP ransomware protection

Use BlueXP ransomware protection

Using BlueXP ransomware protection, you can view workload health and protect workloads.

- [Discover workloads in BlueXP ransomware protection.](#)
- [View protection and workload health from the Dashboard.](#)
 - Review and act on ransomware protection recommendations.
- [Protect workloads:](#)
 - Assign a ransomware protection policy to workloads.
 - Increase application protection to prevent future ransomware attacks.
 - Create, change, or delete a protection policy.
- [Respond to detection of potential ransomware attacks.](#)
- [Recover from an attack](#) (after incidents are neutralized).
- [Configure protection settings.](#)

View workload health at a glance using the Dashboard

The BlueXP ransomware protection Dashboard provides at-a-glance information about the protection health of your workloads. You can quickly determine workloads that are at risk or protected, identify workloads impacted by an incident or in recovery, and gauge the extent of protection by looking at how much storage is protected or at risk.

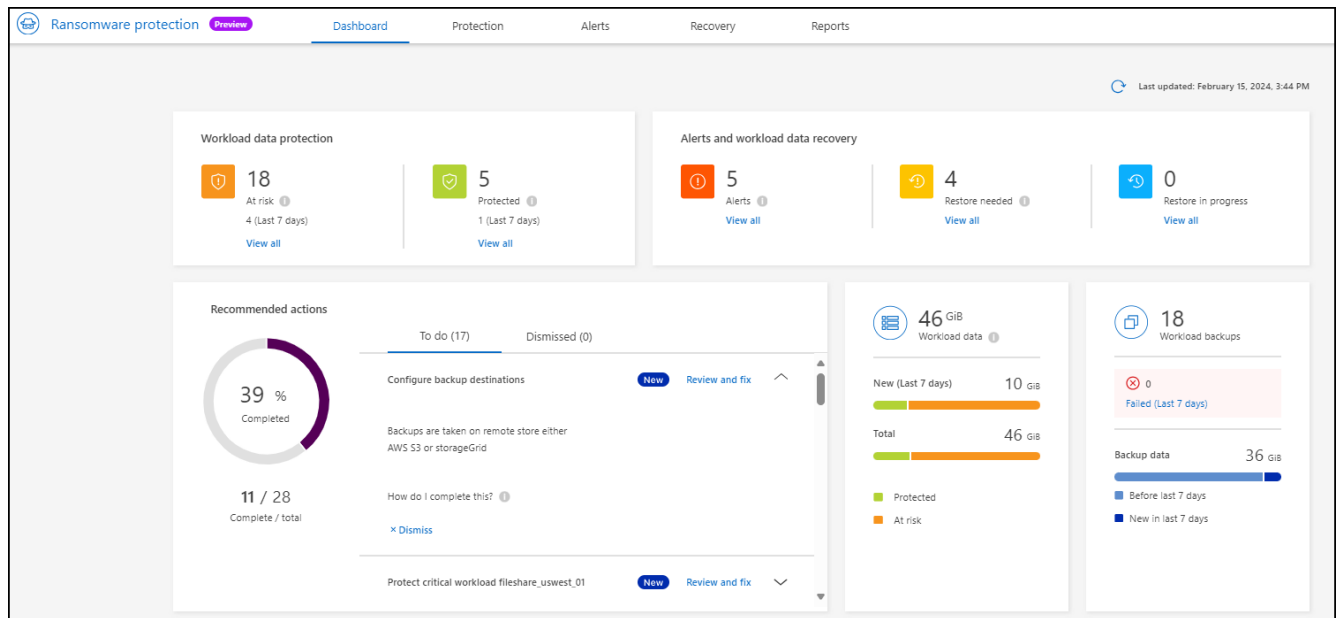
You can also use the Dashboard to review and act on protection recommendations.

Review workload health using the Dashboard

Steps

1. From the BlueXP left navigation, select **Protection > Ransomware protection**.

After discovery, the Dashboard shows you the health of workload data protection.



2. From the Dashboard, you can view and do any of the following in each of the panes:

- **Workload data protection:** Click **View all** to see all workloads that are at risk or protected on the Protection page. Workloads are at risk when protection levels don't match a protection policy. Refer to [Protect workloads](#).
- **Alerts and workload data recovery:** Click **View all** to see active incidents that have impacted your workload, are ready for recovery after incidents are neutralized, or are in recovery. Refer to [Respond to a detected alert](#).

An incident is categorized in one of the following states:

- Impacted (shows on Alerts page)
- Ready for recovery (shows on Recovery page)
- Recovering (shows on Recovery page)
- Recovery failed (shows on Recovery page)
- Recovered (shows on Recovery page)
- **Recommended actions:** To increase protection, review each recommendation and click **Review and fix**.

Refer to [Review protection recommendations on the Dashboard](#) or [Protect workloads](#).

Any recommendations that were added since you last visited the Dashboard are indicated with "New" for at least 24 hours. Actions are listed in priority order with the most important at the top. You can review and act on each one or dismiss it.

The total number of actions does not include dismissed actions.

- **Workload data:** Monitor changes in protection coverage over the last 7 days.
- **Workload backups:** Monitor changes in workload backups created by the service that failed or completed successfully in the last 7 days.

Review protection recommendations on the Dashboard

BlueXP ransomware protection assesses the protection on your workloads and recommends actions to improve that protection.

You can review a recommendation and act on it, which changes the recommendation status to Complete. Or, if you want to act on it later, you can dismiss it. Dismissing an action moves the recommendation to a list of dismissed actions, which you can review later.

Here is a sampling of the recommendations that the service offers.

Recommendation	Description	How to resolve
Add a ransomware protection policy	The workload is currently not protected.	Assign a policy to the workload. Refer to Protect workloads against ransomware attacks .
Configure backup destinations	The workload does not currently have any backup destinations.	Add backup destinations to this workload to protect it. Refer to Configure protection settings .
Make a policy stronger.	Some workloads might not have enough protection. Strengthen protection on workloads with a policy.	Increase retention, add backups, enforce immutable backups, block suspicious file extensions, enable detection on secondary storage and more. Refer to Protect workloads against ransomware attacks .
Protect critical or important application workloads against ransomware.	The Protect page displays critical or important (based on the Priority level assigned) application workloads that are not protected.	Assign a policy to these workloads. Refer to Protect workloads against ransomware attacks .
Protect critical or important file share workloads against ransomware.	The Protection page displays critical or important workloads of the type File Share or Datastore that are not protected.	Assign a policy to each of the workloads. Refer to Protect workloads against ransomware attacks .
Review new alerts	New alerts exist.	Review the new alerts. Refer to Respond to a detected ransomware alert .

Steps

1. From the BlueXP left navigation, select **Protection > Ransomware protection**.
2. From the Recommended actions pane, select a recommendation and select **Review and fix**.
3. To dismiss the action until later, select **Dismiss**.

The recommendation clears from the To Do list and appears on the Dismissed list.



You can later change a dismissed item to a To Do item. When you mark an item completed or you change a dismissed item to a To Do action, the Total actions increases by 1.

4. To review information on how to act on the recommendations, select the **information** icon.

Protect workloads against ransomware attacks

You can protect workloads against ransomware attacks by completing the following actions using BlueXP ransomware protection.

- View existing workload protection.
- Assign a policy to a workload.
 - Increase application protection to prevent future RW attacks.
 - Change the protection for a workload that was previously protected in the RW service.
- Manage policies (only the ones that you created).

BlueXP ransomware protection assigns a priority to each workload during discovery. The workload priority is determined by the following Snapshot frequencies:

- **Critical:** Snapshot copies taken less than 1 per hour (highly aggressive protection schedule)
- **Important:** Snapshot copies taken less than 1 per day but greater than 1 per hour
- **Standard:** Snapshot copies taken more than 1 per day

Protection status: A workload can show one of the following protection statuses to indicate whether a policy is applied or not:

- **Protected:** A policy is applied.
- **At risk:** No policy is applied.
- **In progress:** A policy is being applied but not completed yet.
- **Failed:** A policy is applied but is not working.

Protection health: A workload can have one of the following protection health statuses:

- **Healthy:** The workload has protection enabled and backups and Snapshot copies have been completed.
- **In progress:** Backups or Snapshot copies are in progress.
- **Failed:** Backups or Snapshot copies have not completed successfully.
- **N/A:** Protection is not enabled or sufficient on the workload.

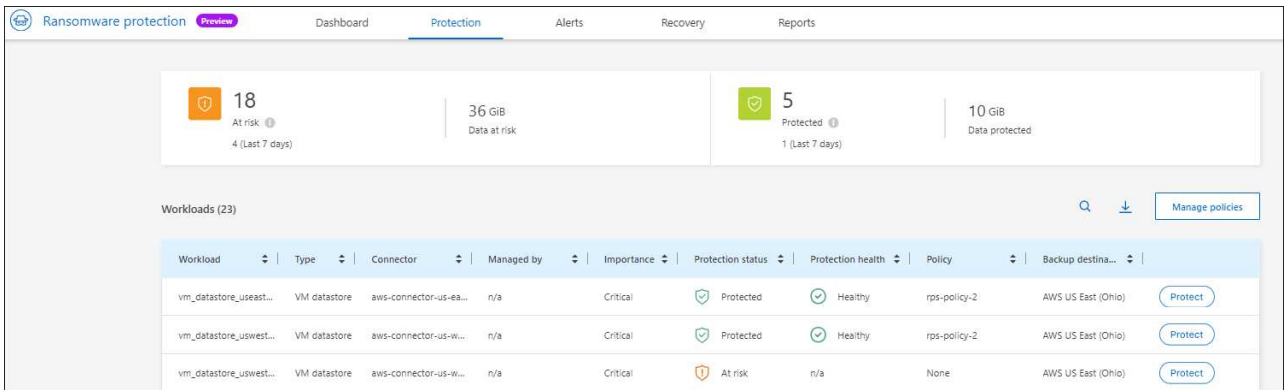
View workload ransomware protection

One of the first steps in protecting workloads is viewing your current workloads and their protection status. You can see the following types of workloads:

- VM workloads
- File share workloads

Steps

1. From the BlueXP left navigation, select **Protection > Ransomware protection**.
2. Do one of the following:
 - From the Dashboard Data Protection pane, select **View all**.
 - From the menu, select **Protection**.



3. From this page, you can assign a policy to a workload.

Assign a predefined protection policy to workloads

To help protect your data, you can assign an existing ransomware protection policy to one or more workloads. You can also assign a different policy to a workload that already has a policy.

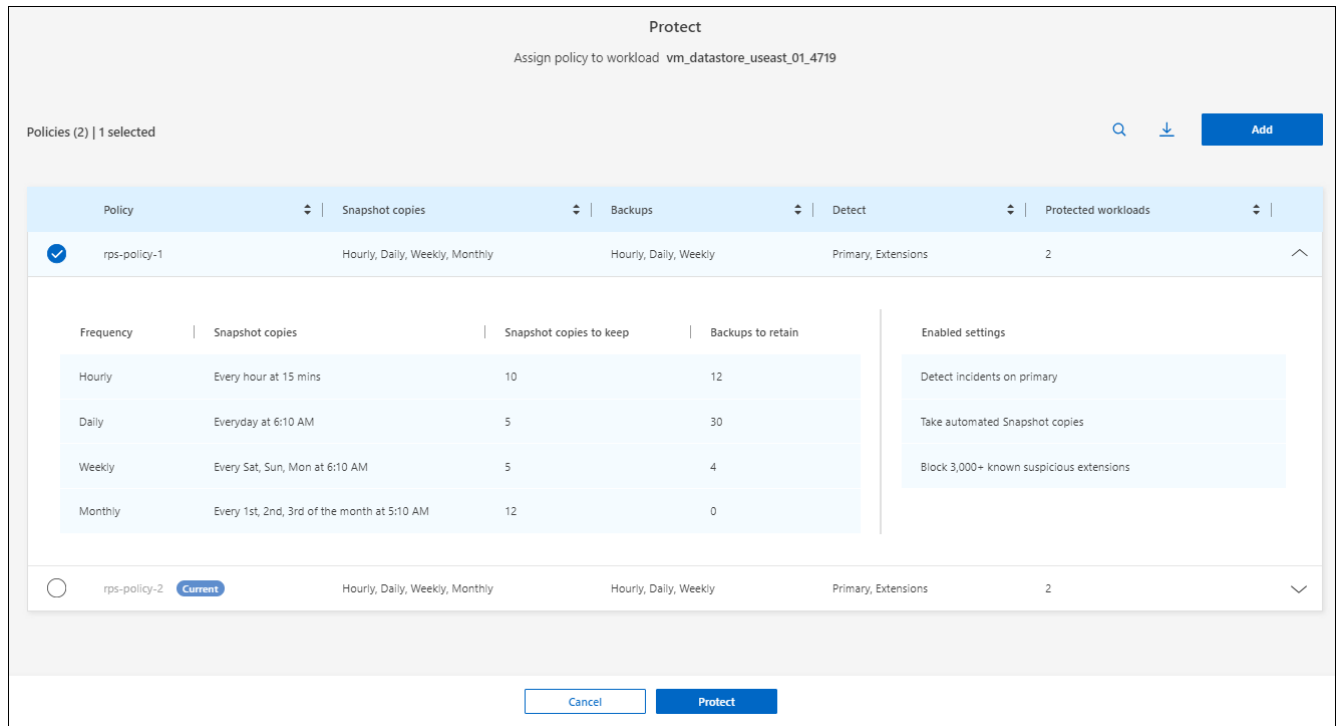
BlueXP ransomware protection includes the following predefined policies that are aligned with workload priority:

Policy level	Snapshot	Frequency	Retention (Days)	# of Snapshot copies	Total Max # of Snapshot copies
Critical workload policy	Quarter hourly	Every 15 min	3	288	309
	Daily	Every 1 day	14	14	309
	Weekly	Every 1 week	35	5	309
	Monthly	Every 30 days	60	2	309
Important workload policy	Quarter hourly	Every 30 mins	3	144	165
	Daily	Every 1 day	14	14	165
	Weekly	Every 1 week	35	5	165
	Monthly	Every 30 days	60	2	165
Standard workload policy	Quarter hourly	Every 60 min	3	72	93
	Daily	Every 1 day	14	14	93
	Weekly	Every 1 week	35	5	93
	Monthly	Every 30 days	60	2	93

Steps

1. From BlueXP ransomware protection, do one of the following:
 - From the Dashboard Data Protection pane, select **View all**.
 - From the Dashboard Recommendation pane, select a recommendation about assigning a policy and select **Review and fix**.
 - From the menu, select **Protection**.
2. From the Protection page, review the workloads and select **Protect** next to the workload.

A list of policies appears.



3. To see details, click on the down arrow on a policy.
4. Select a policy to assign to the workload.
5. Select **Protect**.
6. Review the Dashboard Recommended actions pane, which shows the action as "Completed."

Create a protection policy

If the existing policies do not meet your business needs, you can create a new protection policy. You can create your own from scratch or use an existing policy and modify its settings.

You can create policies that govern primary and secondary storage and treat primary and secondary storage the same or differently.

You can create a policy when you are managing them or during the process of assigning a policy to a workload.

Steps to create a policy during policy management

1. From the BlueXP ransomware protection menu, select **Protection**.

The dashboard shows 18 items at risk (4 in the last 7 days), 36 GiB of data at risk, 5 items protected (1 in the last 7 days), and 10 GiB of data protected. Below this, there are 23 workloads. A table lists the first three workloads:

Workload	Type	Connector	Managed by	Importance	Protection status	Protection health	Policy	Backup destina...	
vm_datastore_useast...	VM datastore	aws-connector-us-aa...	n/a	Critical	Protected	Healthy	RPS-Policy-Importatnt	AWS US East (Ohio)	Protect
vm_datastore_uswest...	VM datastore	aws-connector-us-w...	n/a	Critical	Protected	Healthy	RPS-Policy-Importatnt	AWS US East (Ohio)	Protect
vm_datastore_uswest...	VM datastore	aws-connector-us-w...	n/a	Critical	At risk	n/a	None	AWS US East (Ohio)	Protect

2. From the Protection page, select **Manage policies**.

The 'Manage policies' page shows 3 policies. A table lists the existing policies:

Policy	Snapshot copies	Backups	Detect	Protected workloads	
RPS-Policy-Critical	Hourly, daily, weekly, monthly	Hourly, daily, weekly, monthly	Primary, extensions	2	⌵ ...
RPS-Policy-Importatnt	Hourly, daily, weekly, monthly	Hourly, daily, weekly, monthly	Primary, extensions	2	⌵ ...
RPS-Policy-Standard	Hourly, daily, weekly, monthly	Hourly, daily, weekly, monthly	Primary, extensions	0	⌵ ...

3. From the Manage policies page, select **Add**.

The 'Add policy' form includes the following fields and options:

- Policy name:** test-policy
- Copy from existing policy:** No policy selected (with a Select button)
- Primary storage:**
 - Snapshot copy schedules: Weekly
 - Primary detection: Disable
 - Block file extensions: Disable
- Secondary storage:**
 - Backup schedules: Weekly
 - Secondary detection: Disable

Buttons for 'Cancel' and 'Add' are at the bottom.

4. Enter a new policy name, or enter an existing policy name to copy it. If you enter an existing policy name, choose which policy to copy.



If you choose to copy and modify an existing policy, you must change at least one setting to make it unique.

5. For each item, select the Down arrow.

◦ **Primary storage:**

- **Snapshot copy schedules:** Choose schedule options, the number of Snapshot copies to keep, and select to enable the schedule.
- **Primary detection:** Enable the service to detect ransomware incidents on primary storage.
- **Block file extensions:** Enable this to have the service block known suspicious file extensions. The service takes automated Snapshot copies when Primary detection is enabled.

◦ **Secondary storage:**

- **Backup schedules:** Choose schedule options for secondary storage and enable the schedule.
- **Secondary detection:** Enable the service to detect ransomware incidents on secondary storage.
- **Lock backups:** Choose this to prevent backups on secondary storage from being modified or deleted for a certain period of time. This is also called *immutable storage*.

This option uses NetApp DataLock technology, which locks backups on secondary storage. The period of time that the backup file is locked (and retained) is called the DataLock Retention Period. It is based on the backup policy schedule and retention setting that you defined, plus a 14-day buffer. Any DataLock retention policy that is less than 30 days is rounded up to 30 days minimum.

6. Select **Add**.

Steps to create a policy during protection policy assignment

1. From the BlueXP ransomware protection menu, select **Protection**.

The screenshot displays the BlueXP ransomware protection dashboard. At the top, there are two summary cards: one for 'At risk' data (18 items, 36 GiB) and one for 'Protected' data (5 items, 10 GiB). Below these is a table of 23 workloads. The table has columns for Workload, Type, Connector, Managed by, Importance, Protection status, Protection health, Policy, and Backup destination. Each row includes a 'Protect' button.

Workload	Type	Connector	Managed by	Importance	Protection status	Protection health	Policy	Backup destina...	
vm_datastore_useast...	VM datastore	aws-connector-us-ear...	n/a	Critical	Protected	Healthy	RPS-Policy-Importatnt	AWS US East (Ohio)	Protect
vm_datastore_uswest...	VM datastore	aws-connector-us-w...	n/a	Critical	Protected	Healthy	RPS-Policy-Importatnt	AWS US East (Ohio)	Protect
vm_datastore_uswest...	VM datastore	aws-connector-us-w...	n/a	Critical	At risk	n/a	None	AWS US East (Ohio)	Protect

2. From the Protection page, select **Protect**.

3. From the Protect page, select **Add**.

Protection > Manage policies > Add policy

Add policy

Policy name

Copy from existing policy Select

Primary storage

Snapshot copy schedules	Weekly	▼
Primary detection	Disable	▼
Block file extensions	Disable	▼

Secondary storage

Backup schedules	Weekly	▼
Secondary detection	Disable	▼

4. Complete the process, which is the same as creating a policy from the Manage policies page.

Assign a different protection policy

You can choose a different protection policy for a workload.

You might want to increase the protection to prevent future ransomware attacks by changing the protection policy.

Steps

1. From the BlueXP ransomware protection menu, select **Protection**.
2. From the Protect page, select a workload, and select **Protect**.
3. In the Protect page, select a different policy for the workload.
4. To change any details for the policy, select the down arrow on the right and change the details.
5. Select **Save** to finish the change.

Edit an existing policy

You can change the details of a policy only when the policy is not associated with a workload.

Steps

1. From the BlueXP ransomware protection menu, select **Protection**.
2. From the Protection page, select **Manage policies**.
3. In the Manage policies page, select the **Actions** option for the policy you want to change.
4. From the Actions menu, select **Edit policy**.
5. Change the details.
6. Select **Save** to finish the change.

Delete a policy

You can delete a protection policy that is not currently associated with any workloads.

Steps

1. From the BlueXP ransomware protection menu, select **Protection**.
2. From the Protection page, select **Manage policies**.
3. In the Manage policies page, select the **Actions** option for the policy you want to delete.
4. From the Actions menu, select **Delete policy**.

Respond to a detected ransomware alert

If BlueXP ransomware protection detects a possible attack, an alert appears on the BlueXP ransomware protection Dashboard and in the BlueXP Notifications in the upper right indicating a potential ransomware attack. The service also immediately initiates taking a Snapshot copy. At this point, you should look at the potential risk in the BlueXP ransomware protection **Alerts** tab.

To begin to recover your data, mark the alert as ready for recovery so that your storage administrator can begin the recovery process.

Each alert could have multiple incidents on different volumes with different statuses, so be sure to look at all incidents.

The service provides information called *evidence* about what caused the alert to be issued, such as the following:

- File extensions were created or changed
- File creation occurred and increased by a listed percentage
- File deletion occurred and increased by a listed percentage

An alert is based on the following types of behavior:

- **Potential attack:** An alert occurs when Autonomous Ransomware Protection detects a new extension and the occurrence is repeated more than 20 times in the last 24 hours (default behavior).
- **Warning:** A warning occurs based on the following behaviors:
 - Detection of a new extension has not been identified before and the same behavior does not repeat enough times to declare it as an attack.
 - High entropy is observed.
 - File read/write/rename/delete operations incurred a 100% surge in activity beyond the baseline.

Evidence is based on information from Autonomous Ransomware Protection in ONTAP. For details, refer to [Autonomous Ransomware Protection overview](#).

View alerts

You can access alerts from BlueXP ransomware protection Dashboard or from the **Alerts** tab.

Steps

1. In the BlueXP ransomware protection Dashboard, review the Alerts pane.
2. Select **View all** under one of the statuses.
3. Click on an alert to review all incidents on each volume for each alert.
4. To review additional alerts, click on **Alert** in the breadcrumbs at the upper left.
5. Review the alerts on the Alerts page.

Alert ID	Workload	Location	Type	Connector	Incidents	Impacted data	First detected
Alert9314	fileshare_uswest_02_3223	svm_cvoawswest01rpsdemosandbox02aws	File share	aws-connector-us-west-1-account-LXtf4Xh-e298	1	2 GiB	4 months ago
Alert8727	Oracle_8821	10.0.1.193	Oracle	aws-connector-us-east-1-account-LXtf4Xh-105d	2	2 GiB	4 months ago
Alert3932	MySQL_9294	10.0.1.10	MySQL	aws-connector-us-east-1-account-LXtf4Xh-105d	2	2 GiB	4 months ago
Alert7918	vm_datastore_202_7359	10.195.52.126	VM datastore	onprem-connector-account-LXtf4Xh	1	2 GiB	4 months ago
Alert5319	vm_datastore_uswest_01_6699	10.0.1.215	VM datastore	aws-connector-us-west-1-account-LXtf4Xh-e298	1	2 GiB	4 months ago

6. Continue with [Mark ransomware incidents as ready for recovery \(after incidents are neutralized\)](#).

Mark ransomware incidents as ready for recovery (after incidents are neutralized)

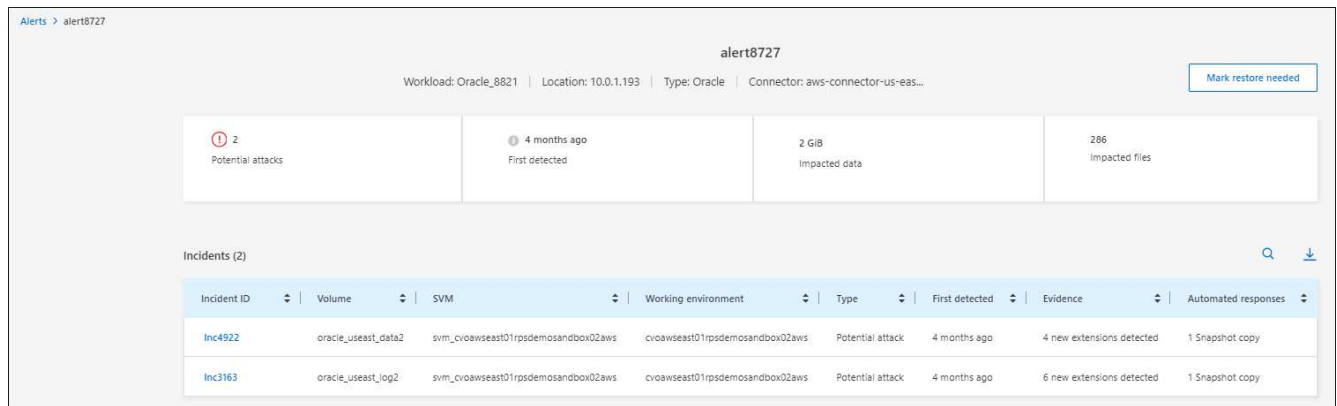
After you have mitigated the attack and are ready to recover workloads, you should communicate with your storage admin team that the data is ready for recovery so that they can start the recovery process.

Steps

1. From the BlueXP ransomware protection menu, select **Alerts**.

Alert ID	Workload	Location	Type	Connector	Incidents	Impacted data	First detected
Alert9314	fileshare_uswest_02_3223	svm_cvoawswest01rpsdemosandbox02aws	File share	aws-connector-us-west-1-account-LXtf4Xh-e298	1	2 GiB	4 months ago
Alert8727	Oracle_8821	10.0.1.193	Oracle	aws-connector-us-east-1-account-LXtf4Xh-105d	2	2 GiB	4 months ago
Alert3932	MySQL_9294	10.0.1.10	MySQL	aws-connector-us-east-1-account-LXtf4Xh-105d	2	2 GiB	4 months ago
Alert7918	vm_datastore_202_7359	10.195.52.126	VM datastore	onprem-connector-account-LXtf4Xh	1	2 GiB	4 months ago
Alert5319	vm_datastore_uswest_01_6699	10.0.1.215	VM datastore	aws-connector-us-west-1-account-LXtf4Xh-e298	1	2 GiB	4 months ago

2. In the Alerts page, select the alert.
3. Review the incidents in the alert.



- If you determine that the incidents are ready for recovery, select **Mark restore needed**.
- Confirm the action and select **Mark restore needed**.
- To initiate the workload recovery, select **Recover** workload in the message or select the **Recovery** tab.

Result

After the alert is marked for recovery, the alert moves from the Alerts tab to the Recovery tab.

Recover from a ransomware attack (after incidents are neutralized)

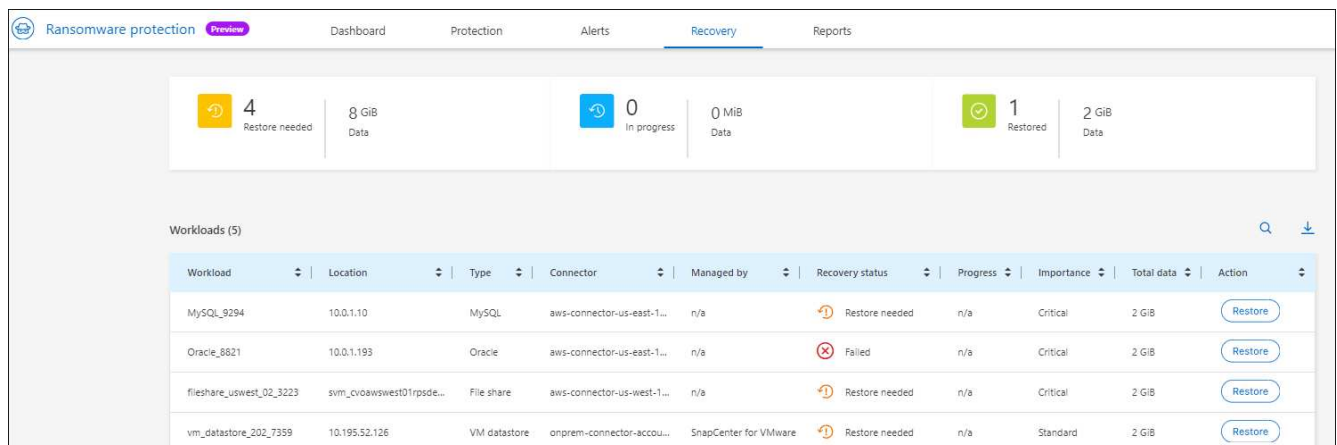
After workloads have been marked "Ready for recovery", BlueXP ransomware protection recommends a recovery point actual (RPA) and orchestrates the workflow for a crash-resistant recovery.

View workloads that are ready to be restored

Review the workloads that are in the "Restore needed" recovery status.

Steps

- Do one of the following:
 - From the Dashboard, review the "Restore needed" totals in the Alerts pane and select **View all**.
 - From the menu, select **Recovery**.
- Review the workload information in the **Recovery** page.



Recover a workload

Using BlueXP ransomware protection, the storage administrator can determine how best to recover workloads either from the recommended restore point or their preferred restore point.

The security storage admin can recover data at different levels:

- Recovery all volumes
- Recover an application at the volume level or file and folder level.
- Recover a file share at the volume level, directory, or file/folder level.
- Recover from a datastore at a VM level.

The process differs slightly depending on the workload type.

Steps

1. From the BlueXP ransomware protection menu, select **Recovery**.
2. Review the workload information in the **Recovery** page.
3. Select a workload that is in the “Restore needed” state.
4. To restore, select **Restore**.
5. **Restore scope:** Select the type of restore you want to complete:
 - All volumes
 - By volume
 - By file: You can specify a folder or single files to restore.

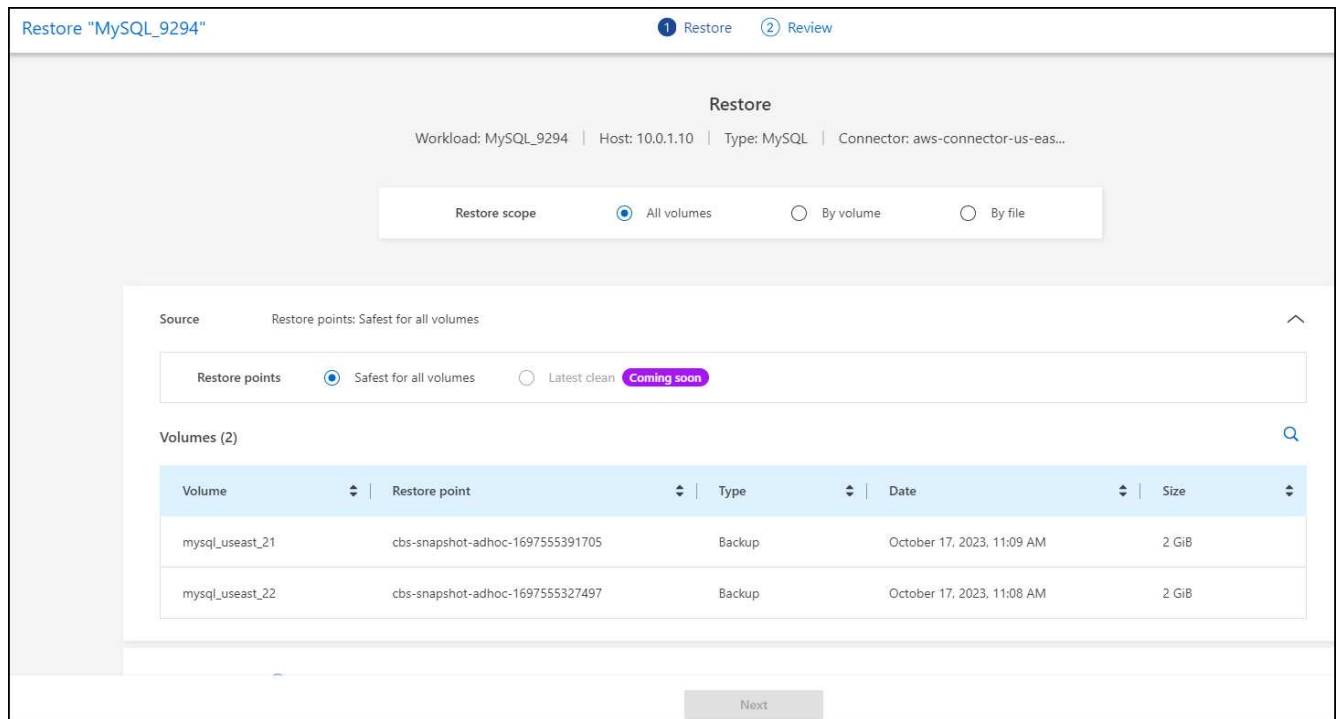


You can select up to 100 files or a single folder.

6. Continue with one of the following procedures depending on whether you chose application, volume, or file.

Restore all volumes

1. On the Restore page, in the Restore scope, select **All volumes**.



2. **Source:** Select the down arrow next to Source to see details.
 - a. Select the restore point that you want to use to restore the data.



BlueXP ransomware protection identifies the best restore point as the latest backup just before the incident and shows a “Safest for all volumes” indication. This means that all volumes will be restored to a copy prior to the first attack on the first volume detected.

3. **Destination:** Select the down arrow next to Destination to see details.
 - a. Select the working environment.
 - b. Select the Storage VM.
 - c. Select the aggregate.
 - d. Change the volume prefix that will be prepended to all new volumes.

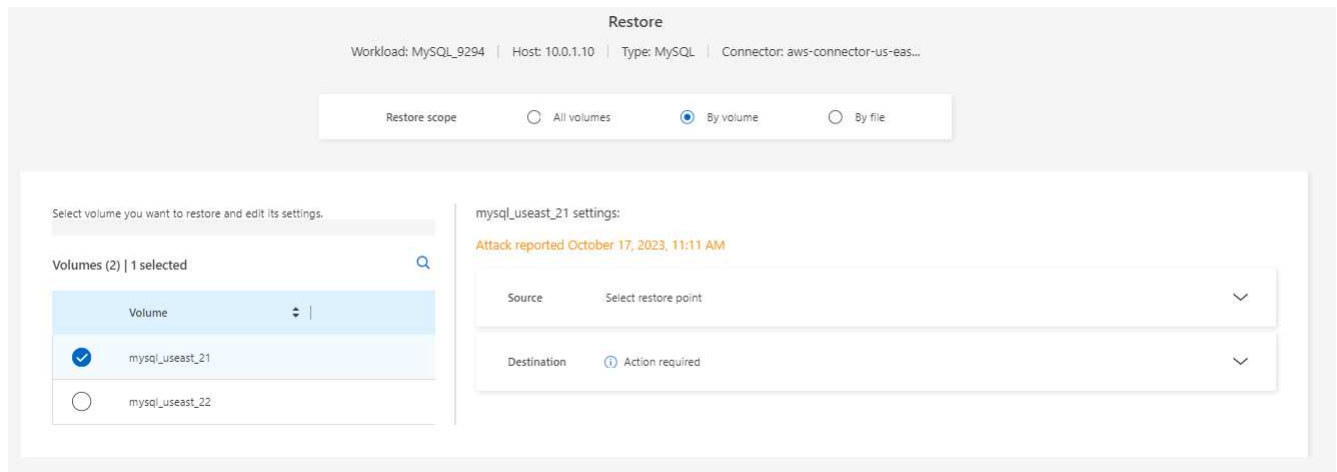


The new volume name appears as prefix + original volume name + backup name + backup date.

4. Select **Save**.
5. Select **Next**.
6. Review your selections.
7. Select **Restore**.
8. From the top menu, select **Recovery** to review the workload on the Recovery page where the status of the operation moves through the states.

Restore an application workload at the volume level

1. On the Restore page, in the Restore scope, select **By volume**.



2. On the list of volumes, select the volume you want to restore.
3. **Source:** Select the down arrow next to Source to see details.
 - a. Select the restore point that you want to use to restore the data.



BlueXP ransomware protection identifies the best restore point as the latest backup just before the incident and shows a “Recommended” indication.

4. **Destination:** Select the down arrow next to Destination to see details.
 - a. Select the working environment.
 - b. Select the Storage VM.
 - c. Select the aggregate.
 - d. Review the new volume name.



The new volume name appears as the original volume name + backup name + backup date.

5. Select **Save**.
6. Select **Next**.
7. Review your selections.
8. Select **Restore**.
9. From the top menu, select **Recovery** to review the workload on the Recovery page where the status of the operation moves through the states.

Restore an application workload at the file level

1. On the Restore page, in the Restore scope, select **By file**.
2. On the list of volumes, select the volume you want to restore.
3. **Source:** Select the down arrow next to Source to see details.
 - a. Select the restore point that you want to use to restore the data.



BlueXP ransomware protection identifies the best restore point as the latest backup just before the incident and shows a “Recommended” indication.

b. Select up to 100 files or a single folder to restore.

4. **Destination:** Select the down arrow next to Destination to see details.

a. Choose where to restore the data: original source location or an alternate location that you can specify.



While the original files or directory will be overwritten by the restored data, the original file and folder names will remain the same unless you specify new names.

b. Select the working environment.

c. Select the Storage VM.

d. Optionally, enter the path.



If you don't specify a path for the restore, the files will be restored to a new volume at the top-level directory.

e. Select whether you want the names of the restored files or directory to be the same names as the current location or different names.

5. Select **Save**.

6. Select **Next**.

7. Review your selections.

8. Select **Restore**.

9. From the top menu, select **Recovery** to review the workload on the Recovery page where the status of the operation moves through the states.

Restore a file share or datastore at the volume or file level

1. After selecting a file share or datastore to restore, on the Restore page, in the Restore scope, select **By volume** or **By file**.

2. On the list of volumes, select the volume you want to restore.
3. **Source:** Select the down arrow next to Source to see details.
 - a. Select the restore point that you want to use to restore the data.



BlueXP ransomware protection identifies the best restore point as the latest backup just before the incident and shows a “Recommended” indication.

4. **Destination:** Select the down arrow next to Destination to see details.
 - a. Choose where to restore the data: original source location or an alternate location that you can specify.



While the original files or directory will be overwritten by the restored data, the original file and folder names will remain the same unless you specify new names.

- b. Select the working environment.
- c. Select the Storage VM.
- d. Optionally, enter the path.



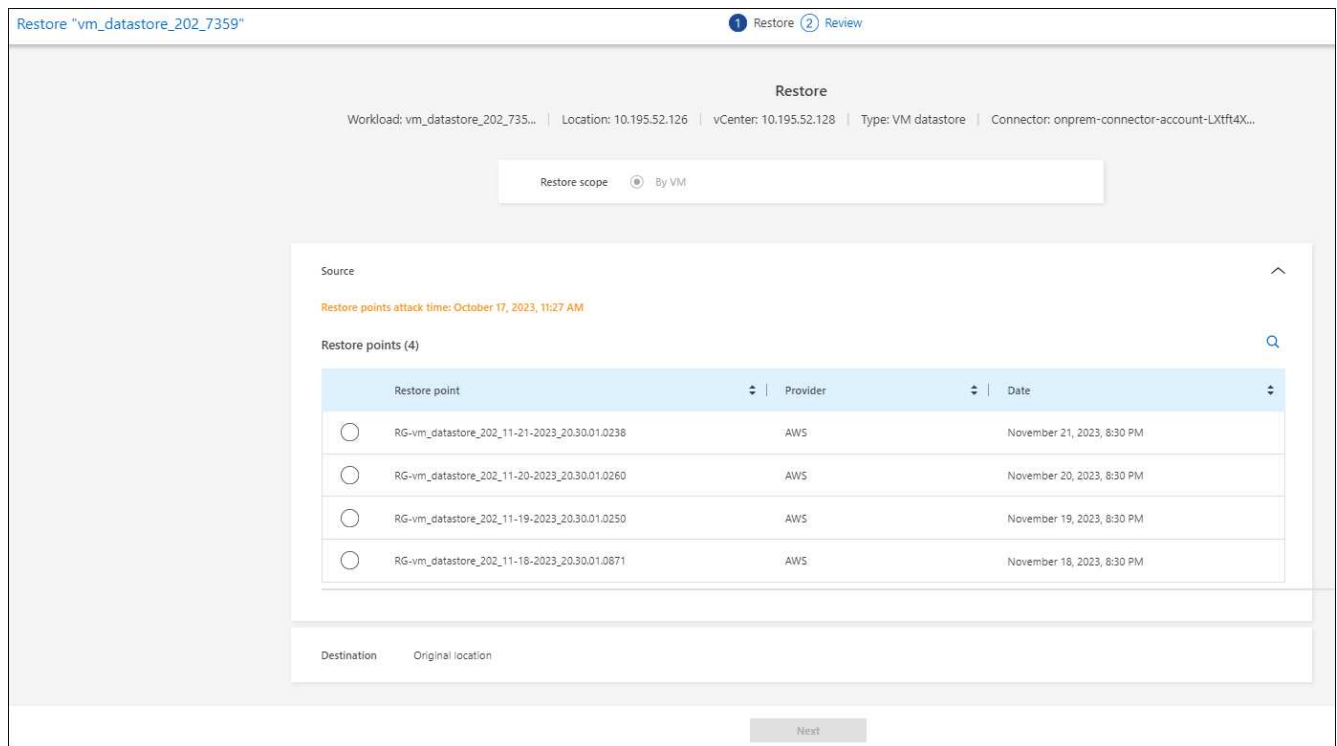
If you don't specify a path for the restore, the files will be restored to a new volume at the top-level directory.

5. Select **Save**.
6. Review your selections.
7. Select **Restore**.
8. From the menu, select **Recovery** to review the workload on the Recovery page where the status of the operation moves through the states.

Restore a VM file share at the VM level

On the Recovery page after you selected a VM to restore, continue with these steps.

1. **Source:** Select the down arrow next to Source to see details.



2. Select the restore point that you want to use to restore the data.
3. **Destination:** To original location.
4. Select **Next**.
5. Review your selections.
6. Select **Restore**.
7. From the menu, select **Recovery** to review the workload on the Recovery page where the status of the operation moves through the states.

Knowledge and support

Register for support

Support registration is required to receive technical support specific to BlueXP and its storage solutions and services. Support registration is also required to enable key workflows for Cloud Volumes ONTAP systems.

Registering for support does not enable NetApp support for a cloud provider file service. For technical support related to a cloud provider file service, its infrastructure, or any solution using the service, refer to "Getting help" in the BlueXP documentation for that product.

- [Amazon FSx for ONTAP](#)
- [Azure NetApp Files](#)
- [Cloud Volumes Service for Google Cloud](#)

Support registration overview

There are two forms of registration to activate support entitlement:

- Registering your BlueXP account ID support subscription (your 20 digit 960xxxxxxx serial number located on the Support Resources page in BlueXP).

This serves as your single support subscription ID for any service within BlueXP. Each BlueXP account-level support subscription must be registered.

- Registering the Cloud Volumes ONTAP serial numbers associated with a subscription in your cloud provider's marketplace (these are 20 digit 909201xxxxxxx serial numbers).

These serial numbers are commonly referred to as *PAYGO serial numbers* and get generated by BlueXP at the time of Cloud Volumes ONTAP deployment.

Registering both types of serial numbers enables capabilities like opening support tickets and automatic case generation. Registration is completed by adding NetApp Support Site (NSS) accounts to BlueXP as described below.

Register your BlueXP account for NetApp support

To register for support and activate support entitlement, one user in your BlueXP account must associate a NetApp Support Site account with their BlueXP login. How you register for NetApp support depends on whether you already have a NetApp Support Site (NSS) account.

Existing customer with an NSS account

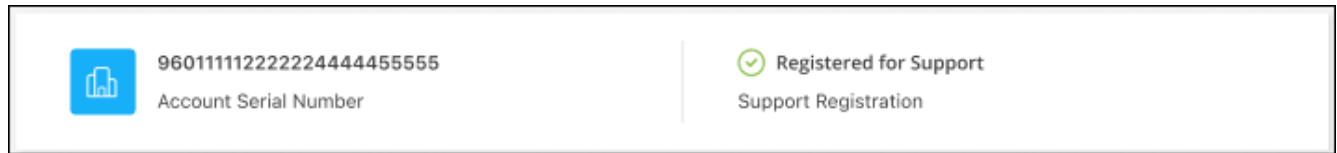
If you're a NetApp customer with an NSS account, you simply need to register for support through BlueXP.

Steps

1. In the upper right of the BlueXP console, select the Settings icon, and select **Credentials**.
2. Select **User Credentials**.

3. Select **Add NSS credentials** and follow the NetApp Support Site (NSS) Authentication prompt.
4. To confirm that the registration process was successful, select the Help icon, and select **Support**.

The **Resources** page should show that your account is registered for support.



Note that other BlueXP users will not see this same support registration status if they have not associated a NetApp Support Site account with their BlueXP login. However, that doesn't mean that your BlueXP account is not registered for support. As long as one user in the account has followed these steps, then your account has been registered.

Existing customer but no NSS account

If you're an existing NetApp customer with existing licenses and serial numbers but *no* NSS account, you need to create an NSS account and associate it with your BlueXP login.

Steps

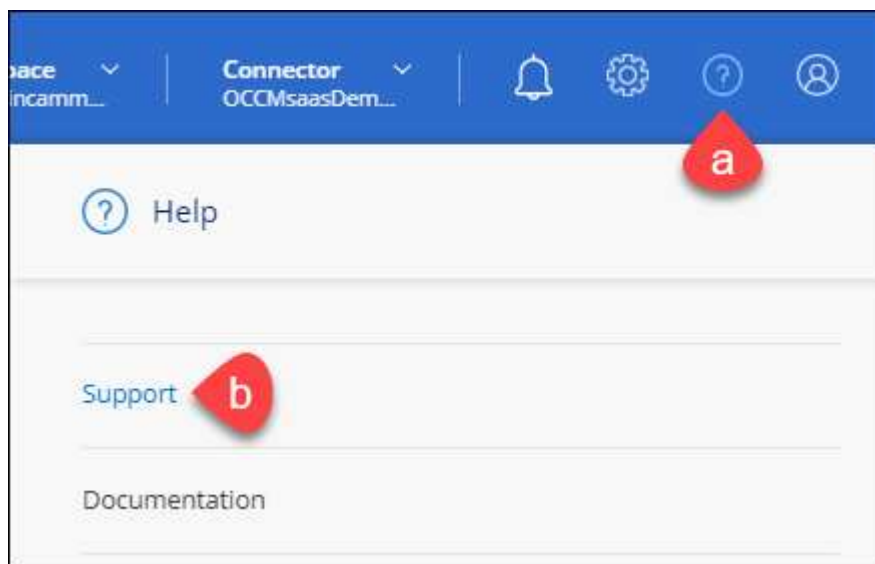
1. Create a NetApp Support Site account by completing the [NetApp Support Site User Registration form](#)
 - a. Be sure to select the appropriate User Level, which is typically **NetApp Customer/End User**.
 - b. Be sure to copy the BlueXP account serial number (960xxxx) used above for the serial number field. This will speed up the account processing.
2. Associate your new NSS account with your BlueXP login by completing the steps under [Existing customer with an NSS account](#).

Brand new to NetApp

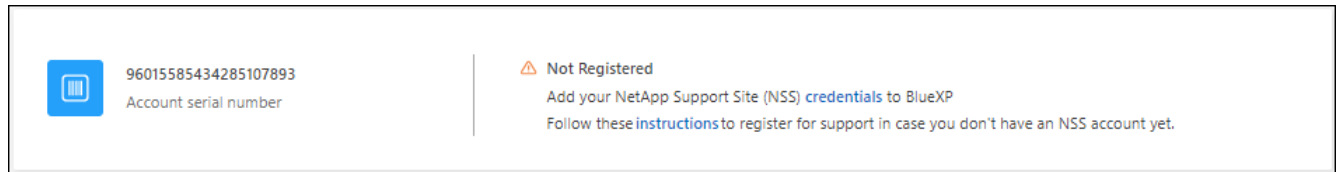
If you are brand new to NetApp and you don't have an NSS account, follow each step below.

Steps

1. In the upper right of the BlueXP console, select the Help icon, and select **Support**.



2. Locate your account ID serial number from the Support Registration page.



3. Navigate to [NetApp's support registration site](#) and select **I am not a registered NetApp Customer**.
4. Fill out the mandatory fields (those with red asterisks).
5. In the **Product Line** field, select **Cloud Manager** and then select your applicable billing provider.
6. Copy your account serial number from step 2 above, complete the security check, and then confirm that you read NetApp's Global Data Privacy Policy.

An email is immediately sent to the mailbox provided to finalize this secure transaction. Be sure to check your spam folders if the validation email doesn't arrive in few minutes.

7. Confirm the action from within the email.

Confirming submits your request to NetApp and recommends that you create a NetApp Support Site account.

8. Create a NetApp Support Site account by completing the [NetApp Support Site User Registration form](#)
 - a. Be sure to select the appropriate User Level, which is typically **NetApp Customer/End User**.
 - b. Be sure to copy the account serial number (960xxxx) used above for the serial number field. This will speed up the account processing.

After you finish

NetApp should reach out to you during this process. This is a one-time onboarding exercise for new users.

Once you have your NetApp Support Site account, associate the account with your BlueXP login by completing the steps under [Existing customer with an NSS account](#).

Associate NSS credentials for Cloud Volumes ONTAP support

Associating NetApp Support Site credentials with your BlueXP account is required to enable the following key workflows for Cloud Volumes ONTAP:

- Registering pay-as-you-go Cloud Volumes ONTAP systems for support

Providing your NSS account is required to activate support for your system and to gain access to NetApp technical support resources.

- Deploying Cloud Volumes ONTAP when you bring your own license (BYOL)

Providing your NSS account is required so that BlueXP can upload your license key and to enable the subscription for the term that you purchased. This includes automatic updates for term renewals.

- Upgrading Cloud Volumes ONTAP software to the latest release

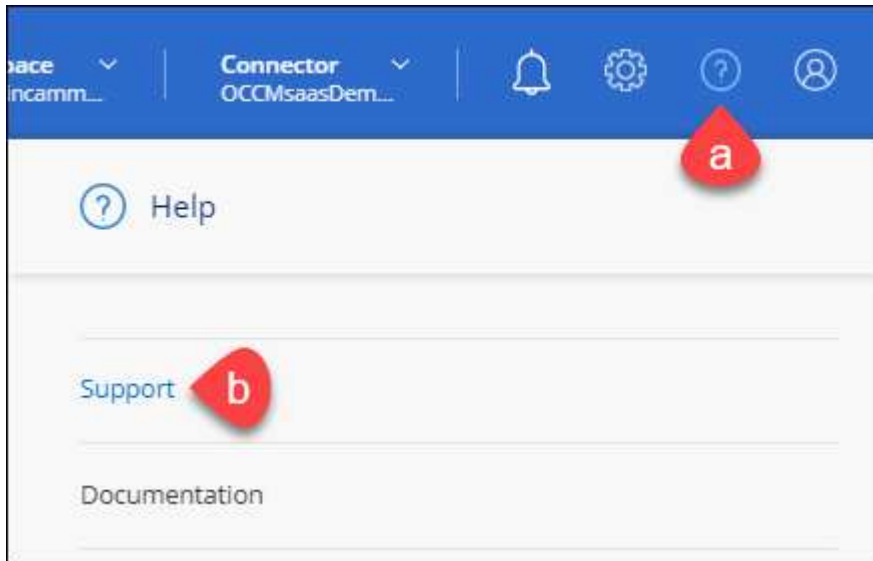
Associating NSS credentials with your BlueXP account is different than the NSS account that is associated with a BlueXP user login.

These NSS credentials are associated with your specific BlueXP account ID. Users who belong to the BlueXP account can access these credentials from **Support > NSS Management**.

- If you have a customer-level account, you can add one or more NSS accounts.
- If you have a partner or reseller account, you can add one or more NSS accounts, but they can't be added alongside customer-level accounts.

Steps

1. In the upper right of the BlueXP console, select the Help icon, and select **Support**.



2. Select **NSS Management > Add NSS Account**.
3. When you're prompted, select **Continue** to be redirected to a Microsoft login page.

NetApp uses Microsoft Entra ID as the identity provider for authentication services specific to support and licensing.

4. At the login page, provide your NetApp Support Site registered email address and password to perform the authentication process.

These actions enable BlueXP to use your NSS account for things like license downloads, software upgrade verification, and future support registrations.

Note the following:

- The NSS account must be a customer-level account (not a guest or temp account). You can have multiple customer-level NSS accounts.
- There can be only one NSS account if that account is a partner-level account. If you try to add customer-level NSS accounts and a partner-level account exists, you'll get the following error message:

"The NSS customer type is not allowed for this account as there are already NSS Users of different type."

The same is true if you have pre-existing customer-level NSS accounts and try to add a partner-level account.

- Upon successful login, NetApp will store the NSS user name.

This is a system-generated ID that maps to your email. On the **NSS Management** page, you can display your email from the **☰** menu.

- If you ever need to refresh your login credential tokens, there is also an **Update Credentials** option in the **☰** menu.

Using this option prompts you to log in again. Note that the token for these accounts expire after 90 days. A notification will be posted to alert you of this.

Get help

NetApp provides support for BlueXP and its cloud services in a variety of ways. Extensive free self-support options are available 24x7, such as knowledgebase (KB) articles and a community forum. Your support registration includes remote technical support via web ticketing.

Get support for a cloud provider file service

For technical support related to a cloud provider file service, its infrastructure, or any solution using the service, refer to "Getting help" in the BlueXP documentation for that product.

- [Amazon FSx for ONTAP](#)
- [Azure NetApp Files](#)
- [Cloud Volumes Service for Google Cloud](#)

To receive technical support specific to BlueXP and its storage solutions and services, use the support options described below.

Use self-support options

These options are available for free, 24 hours a day, 7 days a week:

- **Documentation**

The BlueXP documentation that you're currently viewing.

- [Knowledge base](#)

Search through the BlueXP knowledge base to find helpful articles to troubleshoot issues.

- [Communities](#)

Join the BlueXP community to follow ongoing discussions or create new ones.

Create a case with NetApp support

In addition to the self-support options above, you can work with a NetApp Support specialist to resolve any issues after you activate support.

Before you get started

- To use the **Create a Case** capability, you must first associate your NetApp Support Site credentials with your BlueXP login. [Learn how to manage credentials associated with your BlueXP login.](#)
- If you're opening a case for an ONTAP system that has a serial number, then your NSS account must be associated with the serial number for that system.

Steps

1. In BlueXP, select **Help > Support**.
2. On the **Resources** page, choose one of the available options under Technical Support:
 - a. Select **Call Us** if you'd like to speak with someone on the phone. You'll be directed to a page on netapp.com that lists the phone numbers that you can call.
 - b. Select **Create a Case** to open a ticket with a NetApp Support specialist:
 - **Service:** Select the service that the issue is associated with. For example, BlueXP when specific to a technical support issue with workflows or functionality within the service.
 - **Working Environment:** If applicable to storage, select **Cloud Volumes ONTAP** or **On-Prem** and then the associated working environment.


The list of working environments are within scope of the BlueXP account, workspace, and Connector you have selected in the top banner of the service.

- **Case Priority:** Choose the priority for the case, which can be Low, Medium, High, or Critical.

To learn more details about these priorities, hover your mouse over the information icon next to the field name.


- **Issue Description:** Provide a detailed description of your problem, including any applicable error messages or troubleshooting steps that you performed.
- **Additional Email Addresses:** Enter additional email addresses if you'd like to make someone else aware of this issue.
- **Attachment (Optional):** Upload up to five attachments, one at a time.

Attachments are limited to 25 MB per file. The following file extensions are supported: txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx, and csv.

ntapitdemo 
NetApp Support Site Account

Service Working Environment


Select Select

Case Priority 


Low - General guidance



Issue Description

Provide detailed description of problem, applicable error messages and troubleshooting steps taken.

Additional Email Addresses (Optional) 

Type here

Attachment (Optional) Upload 

No files selected  

After you finish

A pop-up will appear with your support case number. A NetApp Support specialist will review your case and get back to you soon.

For a history of your support cases, you can select **Settings > Timeline** and look for actions named "create support case." A button to the far right lets you expand the action to see details.

It's possible that you might encounter the following error message when trying to create a case:

"You are not authorized to Create a Case against the selected service"

This error could mean that the NSS account and the company of record it's associated with is not the same company of record for the BlueXP account serial number (ie. 960xxxx) or the working environment serial number. You can seek assistance using one of the following options:

- Use the in-product chat
- Submit a non-technical case at <https://mysupport.netapp.com/site/help>

Manage your support cases (Preview)

You can view and manage active and resolved support cases directly from BlueXP. You can manage the cases associated with your NSS account and with your company.

Case management is available as a Preview. We plan to refine this experience and add enhancements in upcoming releases. Please send us feedback by using the in-product chat.

Note the following:

- The case management dashboard at the top of the page offers two views:
 - The view on the left shows the total cases opened in the past 3 months by the user NSS account you provided.
 - The view on the right shows the total cases opened in the past 3 months at your company level based on your user NSS account.

The results in the table reflect the cases related to the view that you selected.

- You can add or remove columns of interest and you can filter the contents of columns like Priority and Status. Other columns provide just sorting capabilities.

View the steps below for more details.

- At a per-case level, we offer the ability to update case notes or close a case that is not already in Closed or Pending Closed status.

Steps

1. In BlueXP, select **Help > Support**.
2. Select **Case Management** and if you're prompted, add your NSS account to BlueXP.

The **Case management** page shows open cases related to the NSS account that is associated with your BlueXP user account. This is the same NSS account that appears at the top of the **NSS management** page.

3. Optionally modify the information that displays in the table:
 - Under **Organization's cases**, select **View** to view all cases associated with your company.
 - Modify the date range by choosing an exact date range or by choosing a different time frame.

Search: Cases opened on the last 3 months ▼ Create a case

Date created	Last updated	Priority	Status (5)	
December 22, 2022	December 29, 2022	Medium (P3)	Assigned	...
December 21, 2022	December 28, 2022	Medium (P3)	Active	...
December 15, 2022	December 27, 2022	Medium (P3)	Pending customer	...
December 14, 2022	December 26, 2022	Low (P4)	Solution proposed	...

- Filter the contents of the columns.

Search: Cases opened on the last 3 months ▼ Create a case

Last updated	Priority	Status (5)	
December 29, 2022	Critical (P1)	<input checked="" type="checkbox"/> Active <input checked="" type="checkbox"/> Pending customer	...
December 28, 2022	High (P2)	<input checked="" type="checkbox"/> Solution proposed <input checked="" type="checkbox"/> Pending closed	...
December 27, 2022	Medium (P3)	<input type="checkbox"/> Closed	...
December 26, 2022	Low (P4)	Apply Reset	...

- Change the columns that appear in the table by selecting + and then choosing the columns that you'd like to display.

Search: Cases opened on the last 3 months ▼ Create a case

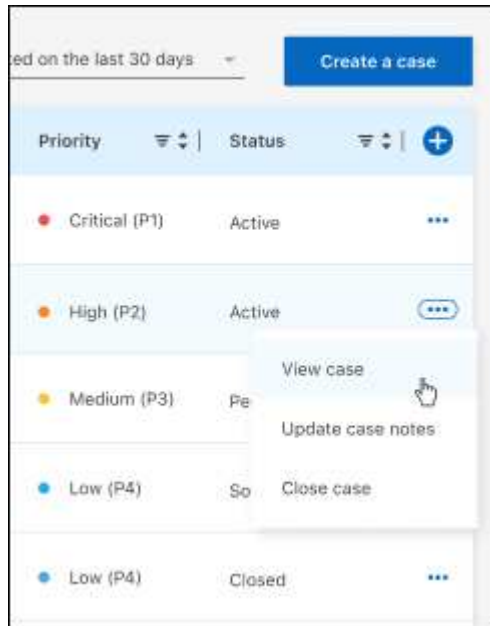
Last updated	Priority	Status (5)	
December 29, 2022	Critical (P1)	<input checked="" type="checkbox"/> Last updated <input checked="" type="checkbox"/> Priority	...
December 28, 2022	High (P2)	<input checked="" type="checkbox"/> Cluster name	...
December 27, 2022	Medium (P3)	<input type="checkbox"/> Case owner <input type="checkbox"/> Opened by	...
December 26, 2022	Low (P4)	Apply Reset	...

4. Manage an existing case by selecting **...** and selecting one of the available options:

- **View case:** View full details about a specific case.
- **Update case notes:** Provide additional details about your problem or select **Upload files** to attach up to a maximum of five files.

Attachments are limited to 25 MB per file. The following file extensions are supported: txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx, and csv.

- **Close case:** Provide details about why you're closing the case and select **Close case**.



Legal notices

Legal notices provide access to copyright statements, trademarks, patents, and more.

Copyright

<https://www.netapp.com/company/legal/copyright/>

Trademarks

NETAPP, the NETAPP logo, and the marks listed on the NetApp Trademarks page are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.

<https://www.netapp.com/company/legal/trademarks/>

Patents

A current list of NetApp owned patents can be found at:

<https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf>

Privacy policy

<https://www.netapp.com/company/legal/privacy-policy/>

Open source

Notice files provide information about third-party copyright and licenses used in NetApp software.

- [Notice for BlueXP](#)

Copyright information

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.