

UniView Portal Guide

Release 2.50 | Document Version 1.04042024



Copyright

Copyright © 2024 Unitrends Incorporated. All rights reserved.

Content in this publication is copyright material and may not be copied or duplicated in any form without prior written permission from Unitrends, Inc (“Unitrends”). This information is subject to change without notice and does not represent a commitment on the part of Unitrends.

The software described in this publication is furnished under a license agreement or nondisclosure agreement. The software may be used or copied only in accordance with the terms of the license agreement. See the End User License Agreement before using the software.

The software described contains certain open source components that are copyrighted. For open source licenses, see the Unitrends Open Source Compliance section of the product Administrator Guide.

Because of the nature of this material, numerous hardware and software products are mentioned by name. In most, if not all, cases these product names are claimed as trademarks by the companies that manufacture the products. It is not our intent to claim these names or trademarks as our own.

The following applies to U.S. Government End Users: The Software and Documentation are “Commercial Items,” as that term is defined at 48 C.F.R.2.101, consisting of “Commercial Computer Software” and “Commercial Computer Software Documentation,” as such terms are used in 48 C.F.R.12.212 or 48 C.F.R.227.7202, as applicable. Consistent with 48 C.F.R.12.212 or 48 C.F.R.227.7202-1 through 227.7202-4, as applicable, the Commercial Computer Software and Commercial Computer Software Documentation are being licensed to U.S. Government end users (a) only as Commercial Items and (b) with only those rights as are granted to all other end users pursuant to the terms and conditions herein. Unpublished-rights reserved under the copyright laws of the United States. Unitrends agrees to comply with all applicable equal opportunity laws including, if appropriate, the provisions of Executive Order 11246, as amended, Section 402 of the Vietnam Era Veterans Readjustment Assistance Act of 1974 (38 USC 4212), and Section 503 of the Rehabilitation Act of 1973, as amended, and the regulations at 41 CFR Parts 60-1 through 60-60, 60-250, and 60-741. The affirmative action clause and regulations contained in the preceding sentence shall be incorporated by reference.

The following applies to all contracts and subcontracts governed by the Rights in Technical Data and Computer Software Clause of the United States Department of Defense Federal Acquisition Regulations Supplement:

RESTRICTED RIGHTS LEGEND: USE, DUPLICATION OR DISCLOSURE BY THE UNITED STATES GOVERNMENT IS SUBJECT TO RESTRICTIONS AS SET FORTH IN SUBDIVISION (C)(1)(II) OF THE RIGHTS AND TECHNICAL DATA AND COMPUTER SOFTWARE CLAUSE AT DFAR 252-227-7013. UNITRENDS CORPORATION IS THE CONTRACTOR AND IS LOCATED AT 200 WHEELER ROAD, NORTH TOWER, 2ND FLOOR, BURLINGTON, MASSACHUSETTS 01803.

Unitrends, Inc
200 Wheeler Road
North Tower, 2nd Floor
Burlington, MA 01803, USA
Phone: 1.866.359.5411

Contents

Getting Started	7
Next steps	7
Accessing the UniView Portal	8
Additional resources	31
Switching to Dark Theme view	32
Working with the Dashboard	33
Filtering the Dashboard	34
Appliances tile	34
Alerts tile	34
Low Space Appliances tile	35
Local Storage Used tile	35
Active Jobs tile	35
Completed Jobs tile	36
Recent Jobs tile	37
Working with Alerts and Conditional Alarms	39
Alerts	39
Alert conditions	39
Alerts and PSA ticketing	41
Email alerts	41
Alerts for Spanning Microsoft 365 backup	41
Alerts for Spanning Google Workspace backup	43
Alerts for Spanning Salesforce backup	45
Alerts for Datto Backup for Microsoft Azure (DBMA)	48
Managing alerts	49
Conditional alarms	61
Working with conditional alarms	61
Working with Unitrends Appliances, Assets, and Backups	85
Working with appliances	85

Adding assets to an appliance	93
Removing assets from an appliance	111
Viewing assets	127
Removing assets	132
Working with backup policies	135
Working with VSA 9 Agents	143
Working with Spanning Backup	149
Working with Microsoft 365	150
Working with Google Workspace	161
Working with Salesforce	172
Working with Datto Backup for Microsoft Azure	179
Working with Jobs	183
Working with recent jobs	183
Viewing active jobs	186
Working with scheduled jobs	189
Working with Organizations	195
Working with Users and Scopes	207
Working with users	207
Working with scopes	217
Working with Integrations	223
Integrating VSA 9	224
Integrating VSA 10	232
Integrating KaseyaOne	233
Working with your KaseyaOne integration	236
Integrating Autotask	249
Working with your Autotask Integration	258
Integrating ConnectWise Manage	270
Working with your ConnectWise Manage integration	282
Integrating Kaseya's Billing Management System (BMS) or Vorex	287
Working with your BMS or Vorex integration	292

Importing Accounts or Companies from your PSA	302
Integrating Datto Portal	306
Working with your Datto Portal integration	309
Integrating IT Glue	313
Working with your IT Glue integration	318
API Access	321

This page is intentionally left blank.



Getting Started

The UniView Portal is a SaaS-based management platform that provides UI and API integration across Unitrends best-of-breed approaches to backup and recovery: Unitrends backup appliances, Datto Backup for Microsoft Azure, and Spanning SaaS Backup for Microsoft 365, Google Workspace, and Salesforce.

UniView is the centralized management hub for Unitrends Unified Backup. Leverage UniView for time-saving automation, workflow integrations, and streamlined management of your backup and recovery environments.

With UniView, you have one screen to manage these environments in minutes per day, regardless of where your data lives.

UniView is modular in design — simply start with what you need and easily snap in additional modules as needed.

Next steps

To get started, log in to the UniView Portal (see ["Accessing the UniView Portal"](#)) and add your Unitrends Unified Backup products:

- Add each Unitrends appliance as described in ["Adding an appliance"](#).
- Add your Spanning Backup products as described in ["Integrating a Microsoft 365 tenant"](#), ["Integrating a Google Workspace domain"](#), and ["Integrating a Salesforce organization"](#).
- Add Datto Backup for Microsoft Azure as described in ["Integrating Datto Portal"](#).

Next, quickly monitor and manage your backup products from the UniView Portal:

- For Unitrends appliances, check out the Dashboard to view the status of all appliances at a glance (see ["Working with the Dashboard"](#)). To explore more features, see ["Working with Unitrends Appliances, Assets, and Backups"](#) and ["Working with Jobs"](#).
- For Spanning Backup, use the Protect page to manage your backups and licenses. For details, see ["Working with Spanning Backup"](#).
- For Datto Backup for Microsoft Azure, use the Protect page to view summary and status information about your protected assets. For details, see ["Working with Datto Backup for Microsoft Azure"](#).
- View BackupIQ alerts to quickly address issues. Set up conditional alarms and email notifications for more robust alerting. For details, see ["Working with Alerts and Conditional Alarms"](#).

Add more integrations to leverage other product features (see ["Working with Integrations"](#)). For example:

- Integrate KaseyaOne to enable users to log in to the UniView Portal with their KaseyaOne credentials.
- Integrate your PSA system (ConnectWise Manage, Autotask, BMS, or Vorex) to automatically create a ticket in the PSA for each BackupIQ alert.
- Add the Unitrends Backup module to your VSA so you can access the UniView Portal from the VSA UI. For details, see ["Integrating VSA 10"](#) or ["Integrating VSA 9"](#).
- Integrate IT Glue to synchronize your assets and appliances with Kaseya's IT Glue documentation platform.

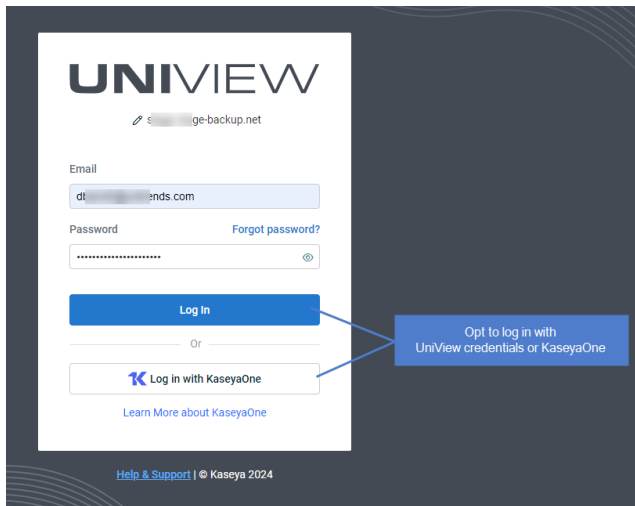
Accessing the UniView Portal

Steps required to log in vary by whether you log in with KaseyaOne or by using UniView Portal credentials. These considerations apply:

- In some environments, log in with KaseyaOne is required. In this case, if you attempt to log in by using UniView Portal credentials, you are redirected to the KaseyaOne Login page. Log in as described in "[To log in with KaseyaOne credentials](#)".

Note: This login procedure requires a KaseyaOne account. If you do not have a KaseyaOne account, request one from Support and set it up as described in this KaseyaOne article: [Set up your KaseyaOne user account](#).

- In some environments, log in with KaseyaOne is optional. You can click **Log in with KaseyaOne** or enter your UniView Portal credentials:



- In some environments, log in with KaseyaOne is not enabled. In this case, the Login page does not contain the *Log in with KaseyaOne* button and you must log in by using UniView Portal credentials. For details, see "[To activate your UniView Portal account and log in for the first time](#)" or "[To log in using UniView Portal credentials](#)".

Use these procedures to access and exit the UniView Portal:

- "[To activate your UniView Portal account and log in for the first time](#)"
- "[To log in using UniView Portal credentials](#)"
- "[To log in with KaseyaOne credentials](#)"
- "[To remove an older KaseyaOne/UniView mapping that was created with mismatched user names](#)"
- "[To log out of the UniView Portal](#)"
- "[To reset your UniView Portal password](#)"

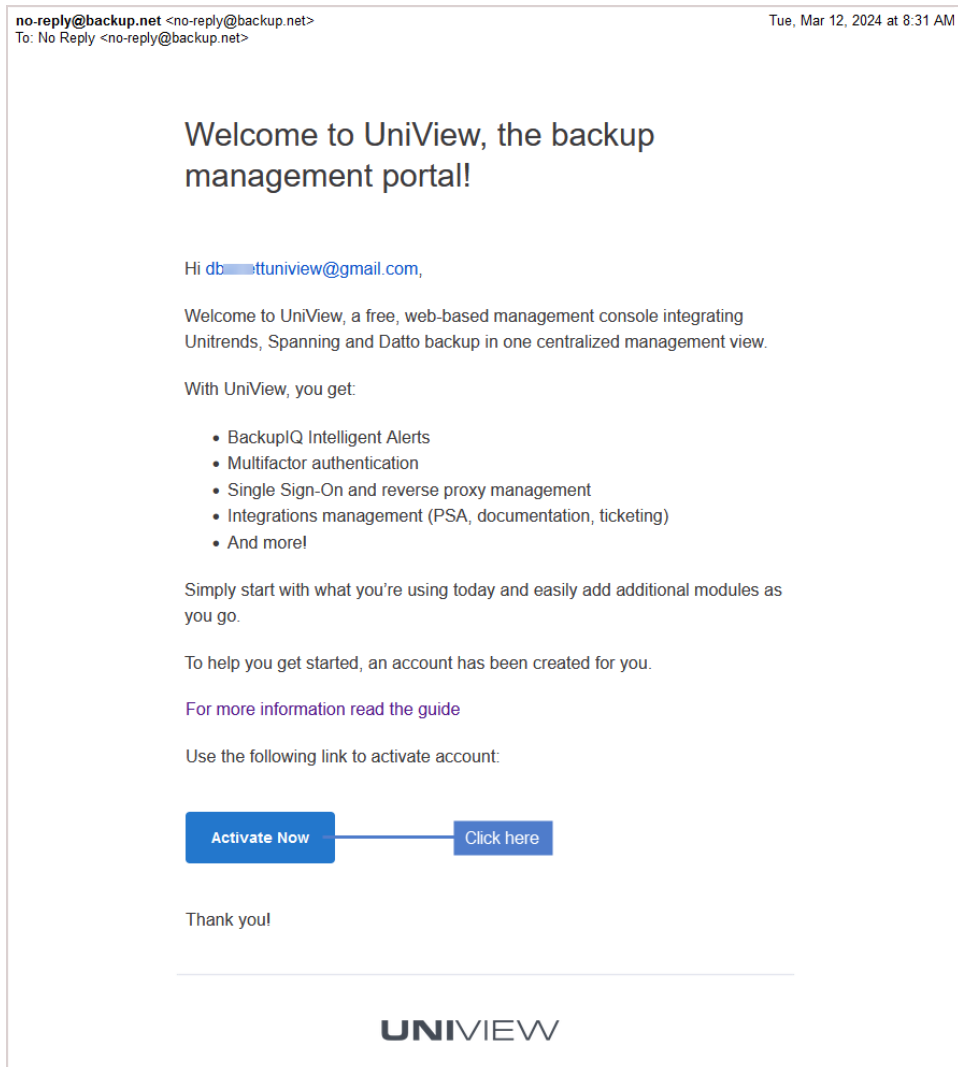
To activate your UniView Portal account and log in for the first time

When your user account is provisioned, you receive a *Welcome to UniView* email containing an activation link. You must run this procedure within 48 hours of receiving this email to activate your UniView Portal account. If your activation link has expired, contact the UniView Portal Onboarding team to obtain a new link.

Notes:

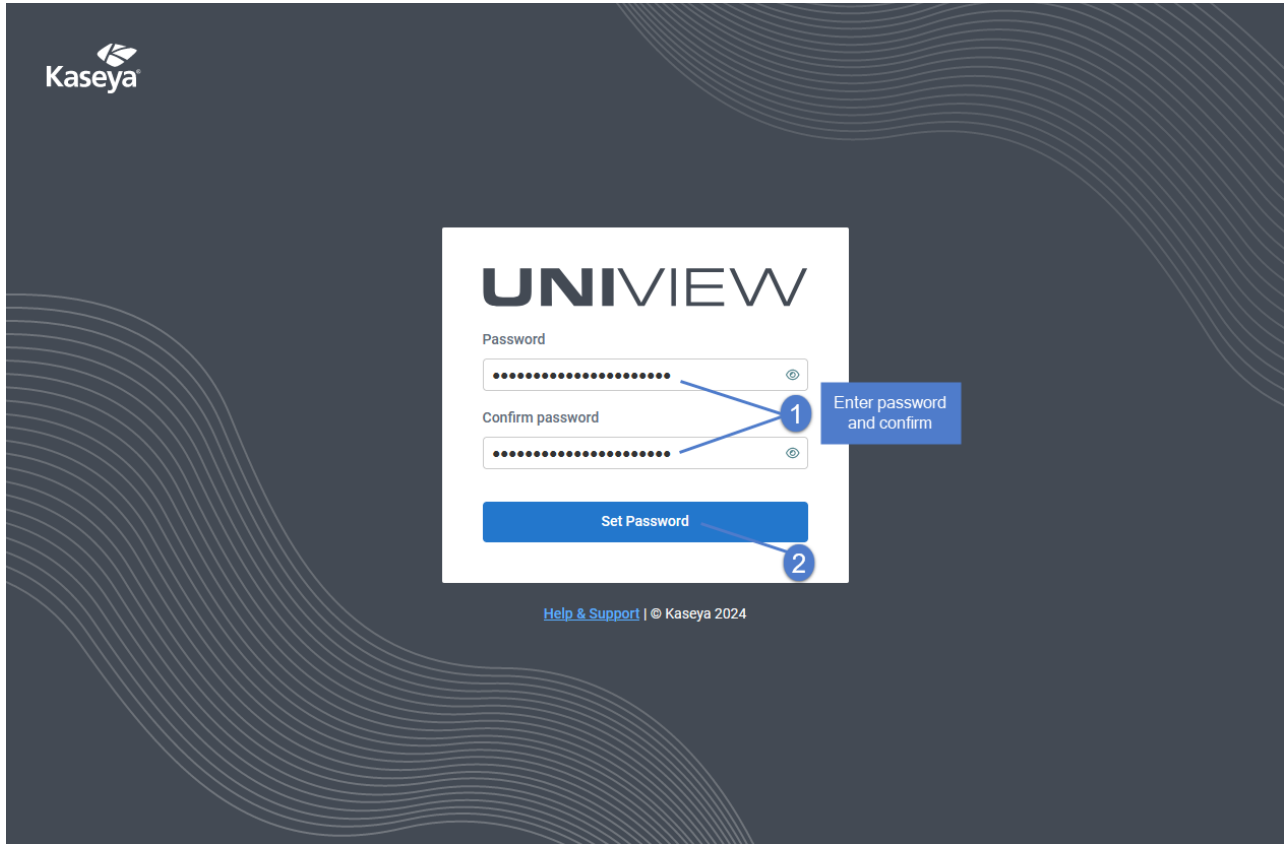
- In some environments, log in with KaseyaOne is required. In this case, a UniView account is not needed and you can log in for the first time as described in "[To log in with KaseyaOne credentials](#)". If you attempt to log in by using UniView Portal credentials, you are redirected to the KaseyaOne Login page.
- UniView Portal requires two-factor authentication (2FA) using a supported TOTP authenticator application, such as [Passly Authenticator](#). If you are not already using a supported authenticator application, you will need to download and install one to your iOS or Android device before you can log in to the UniView Portal.
- This procedure includes steps to set your password and to pair the UniView Portal with your authenticator application. These steps are required the first time you log in only.

- 1 Open the *Welcome to UniView* email that you received from no-reply@backup.net and click the **Activate Now** button.

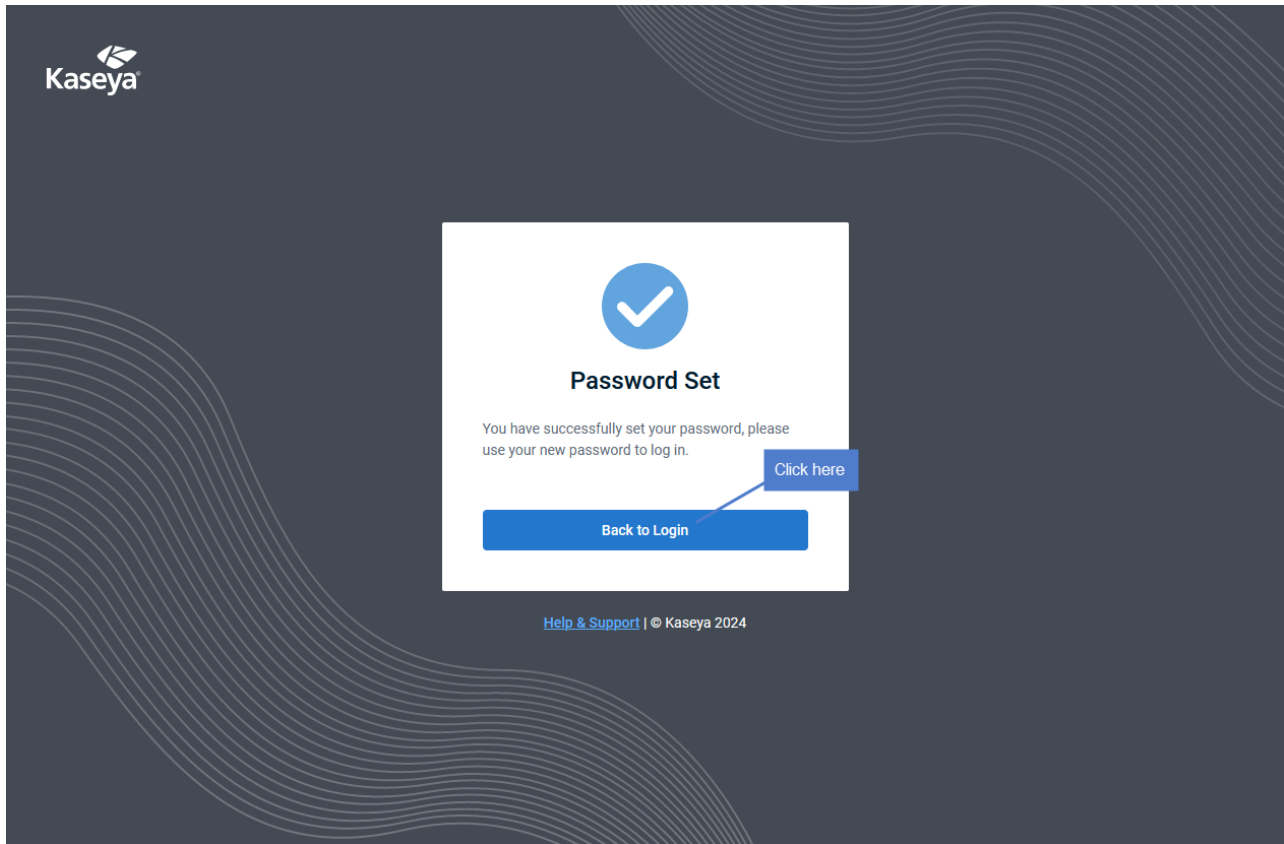


2 Create your UniView password:

- Enter the password in the Password and Confirm Password fields.
- Click **Set Password**.



- 3 Click **Back to Login**.

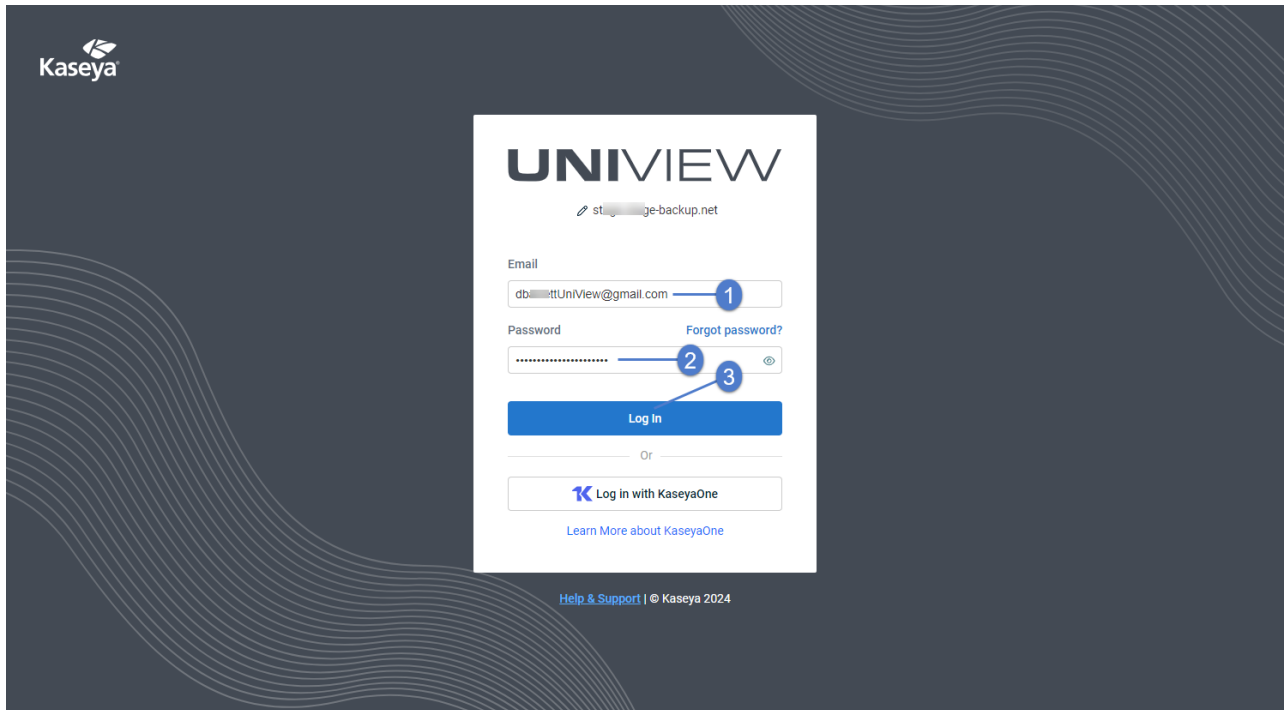


- 4 Enter the backup.net homerealm that was provided to you by the UniView Portal Onboarding team. Click **Next**.



- 5 Enter the username and password of your UniView Portal account. Click **Log In**.

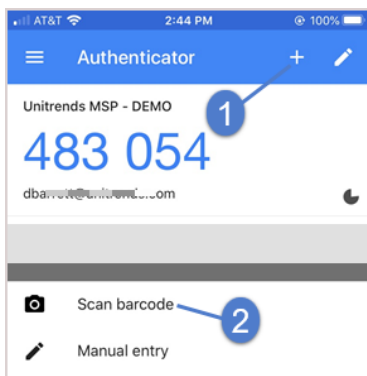
Note: If you are redirected to the KaseyaOne Login page, log in with KaseyaOne is required in your environment. Do not continue with this procedure. Instead, enter your KaseyaOne credentials (for details see "To log in with KaseyaOne credentials").



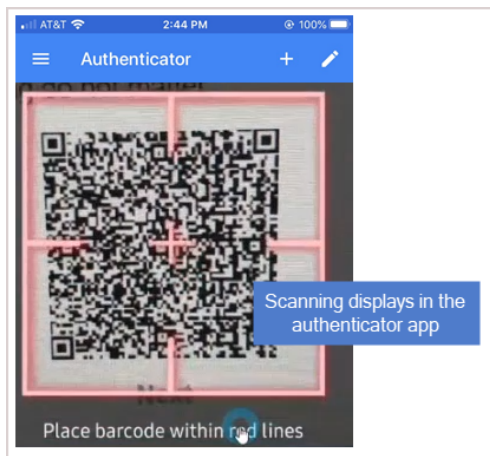
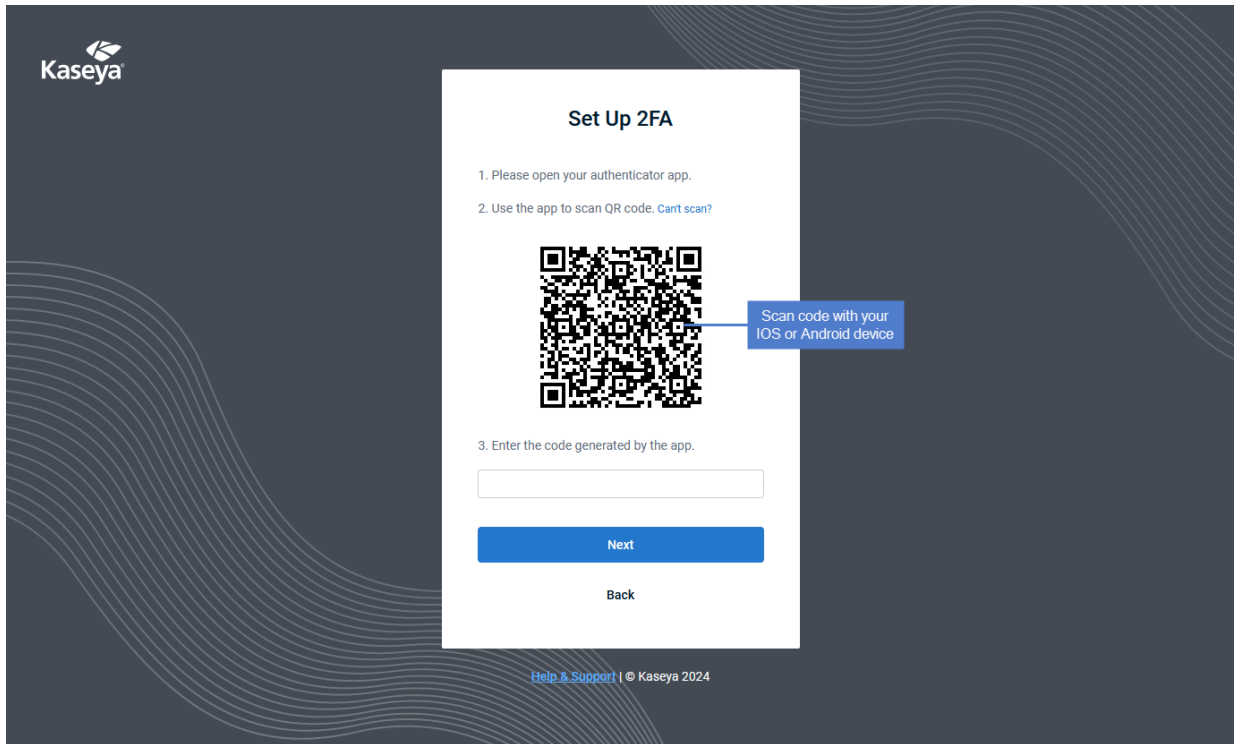
- 6 Download and install a supported TOTP authenticator application to your iOS or Android device. (Skip this step if you have already installed a supported authenticator application.)
- 7 Pair UniView Portal to your authenticator application by scanning the barcode or manually entering the QR code. Examples of both methods are given below.

Scan barcode:

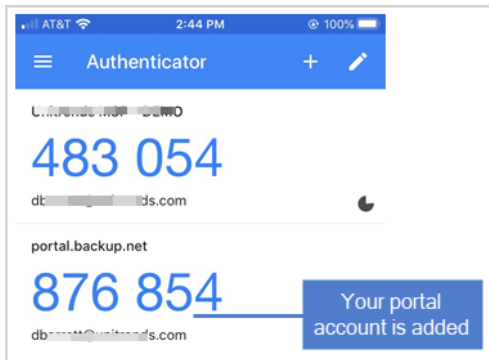
- Open your authenticator application. Select **+**, then select **Scan a barcode**.



- Use your iOS or Android device to scan the QR Code that displays on the UniView Portal Set Up 2FA page.

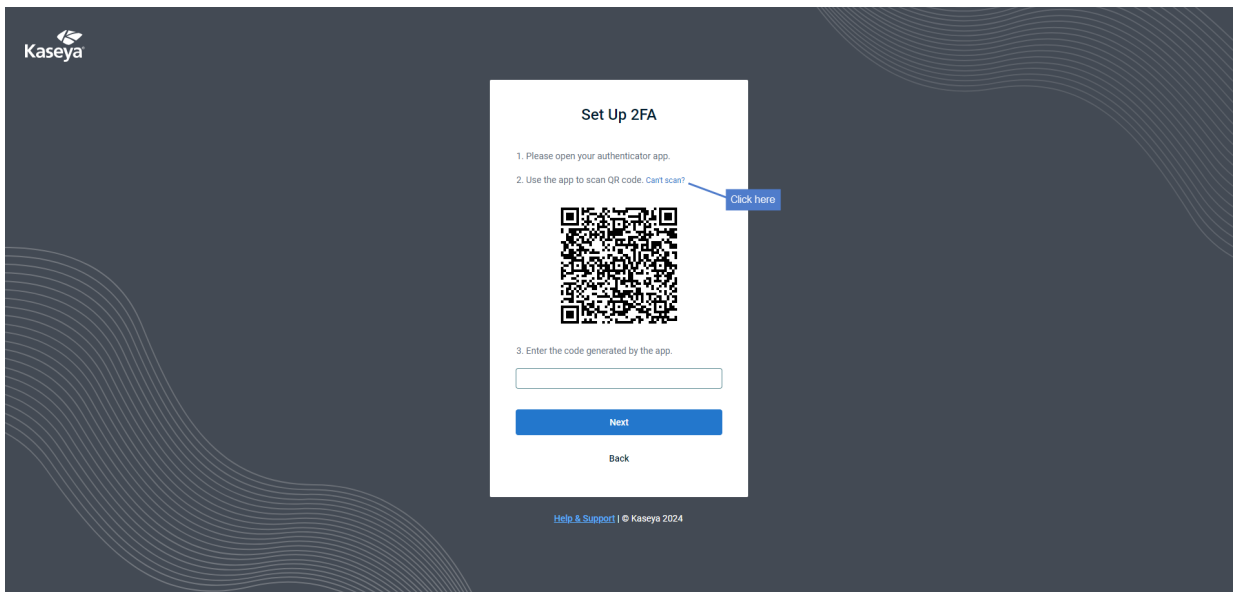


- Your UniView Portal account is added to the authenticator application.

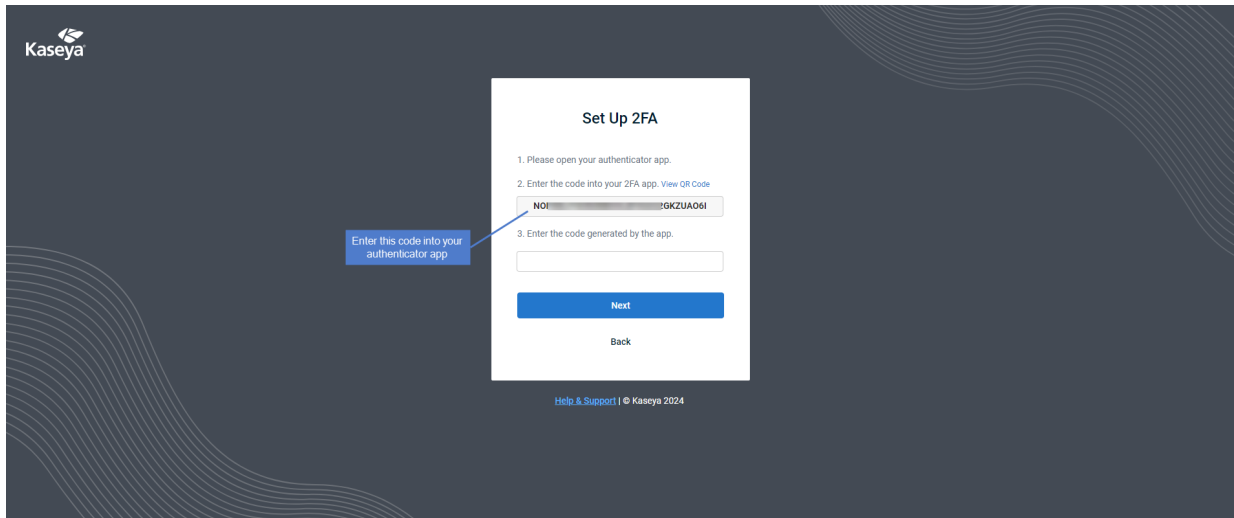


Manually enter QR code:

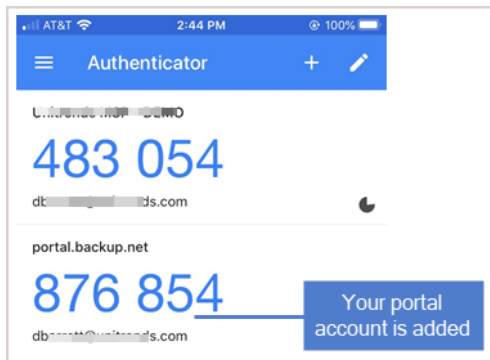
- Click **Can't Scan?**.



- The QR code displays. Enter the QR code into your authenticator app.

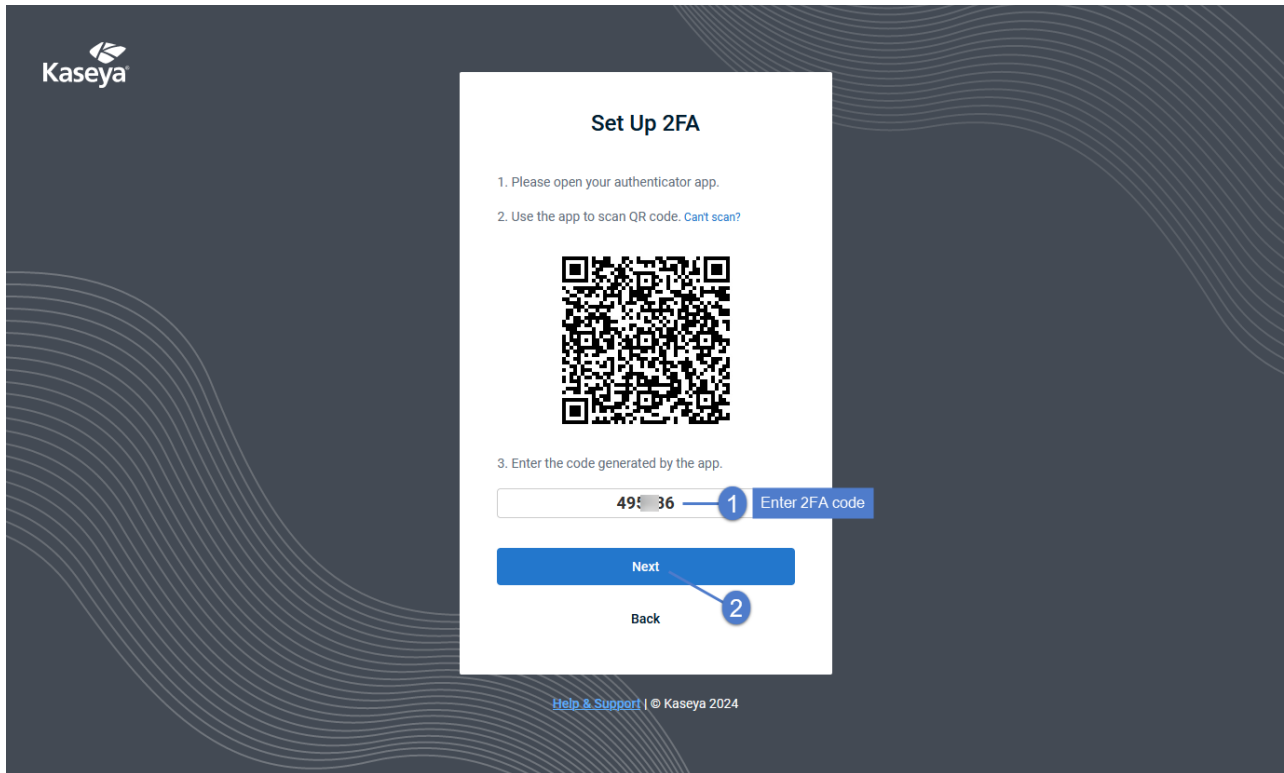


- Your UniView Portal account is added to the authenticator application.



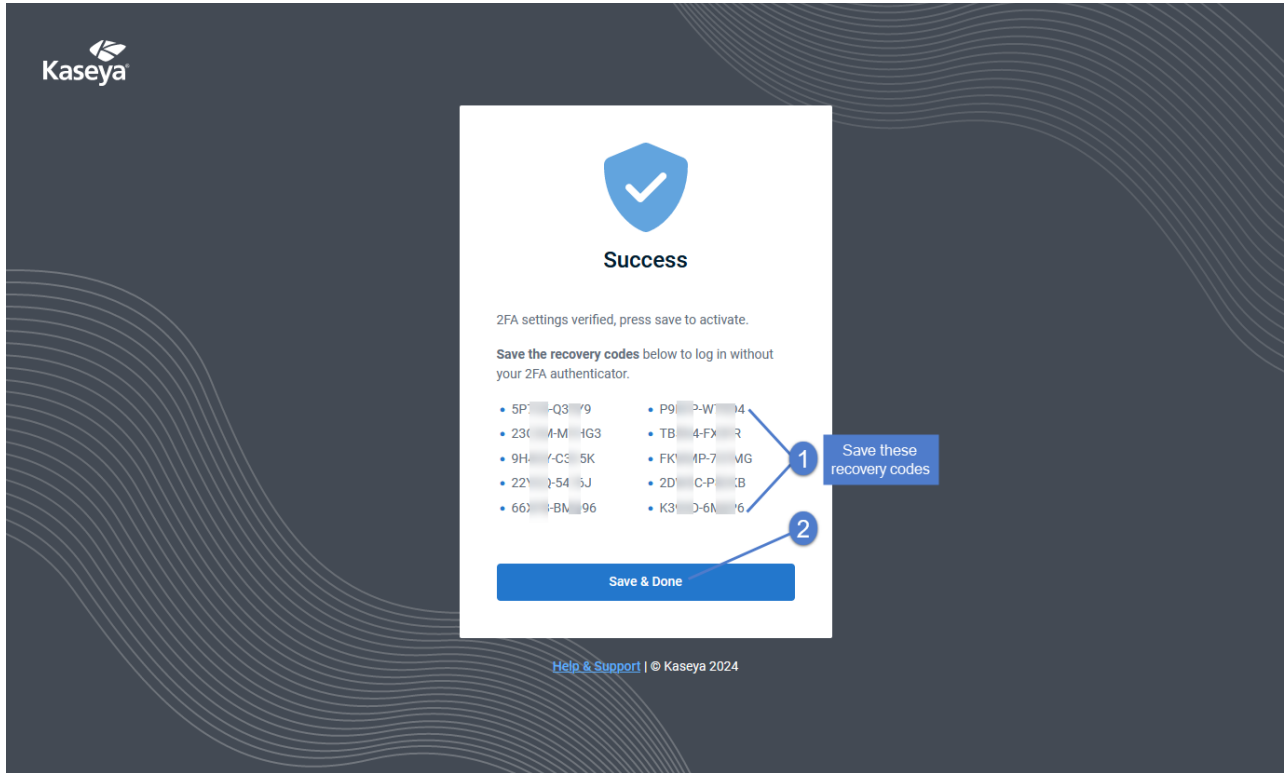
- 8 Return to the UniView Portal and enter the 2FA code supplied by the authenticator application. Click **Next**.

Note: You must enter the code within the 30-second expiration period. Otherwise, you need to enter the next non-expired code displayed in the authenticator application.

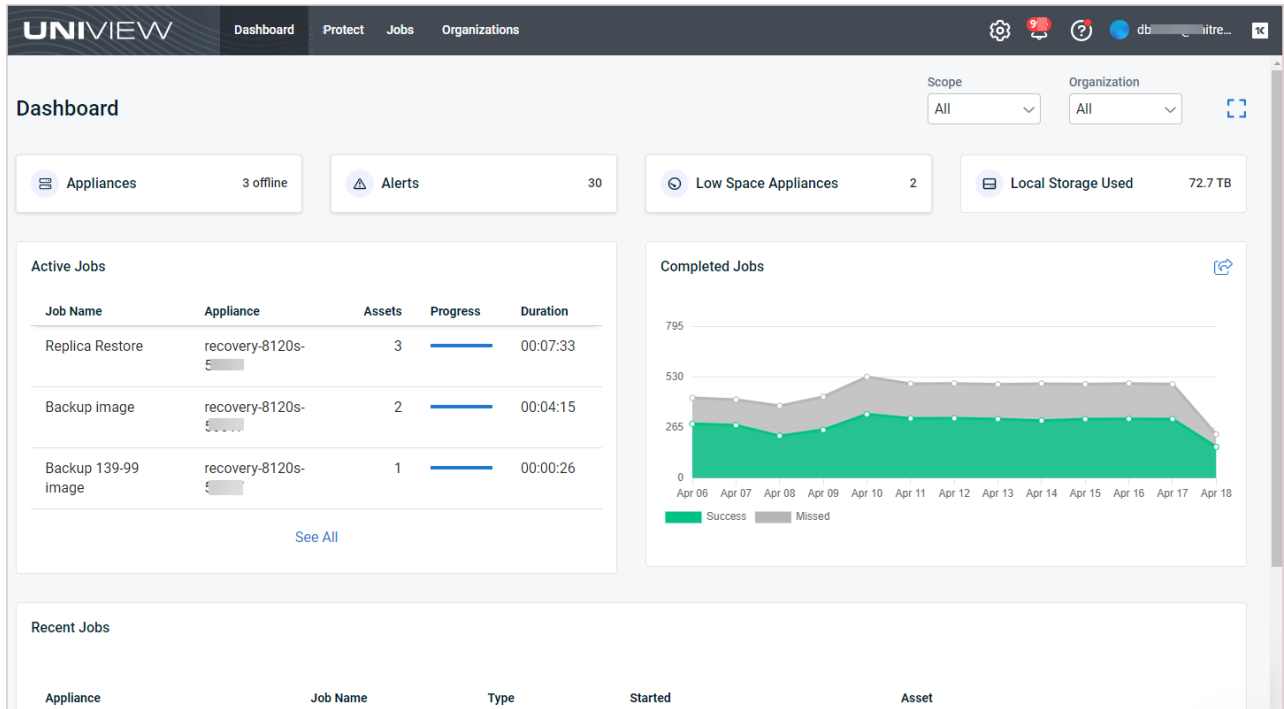


- 9 Save the recovery codes listed below. You can use them to log in without your authenticator app. Click **Save & Done**.

Note: You can quickly copy and paste the codes into a text editor (e.g., Notepad). Each recovery code listed below can be used one time only. Use these codes sparingly.



10 You are logged in to the UniView Portal.



To log in using UniView Portal credentials

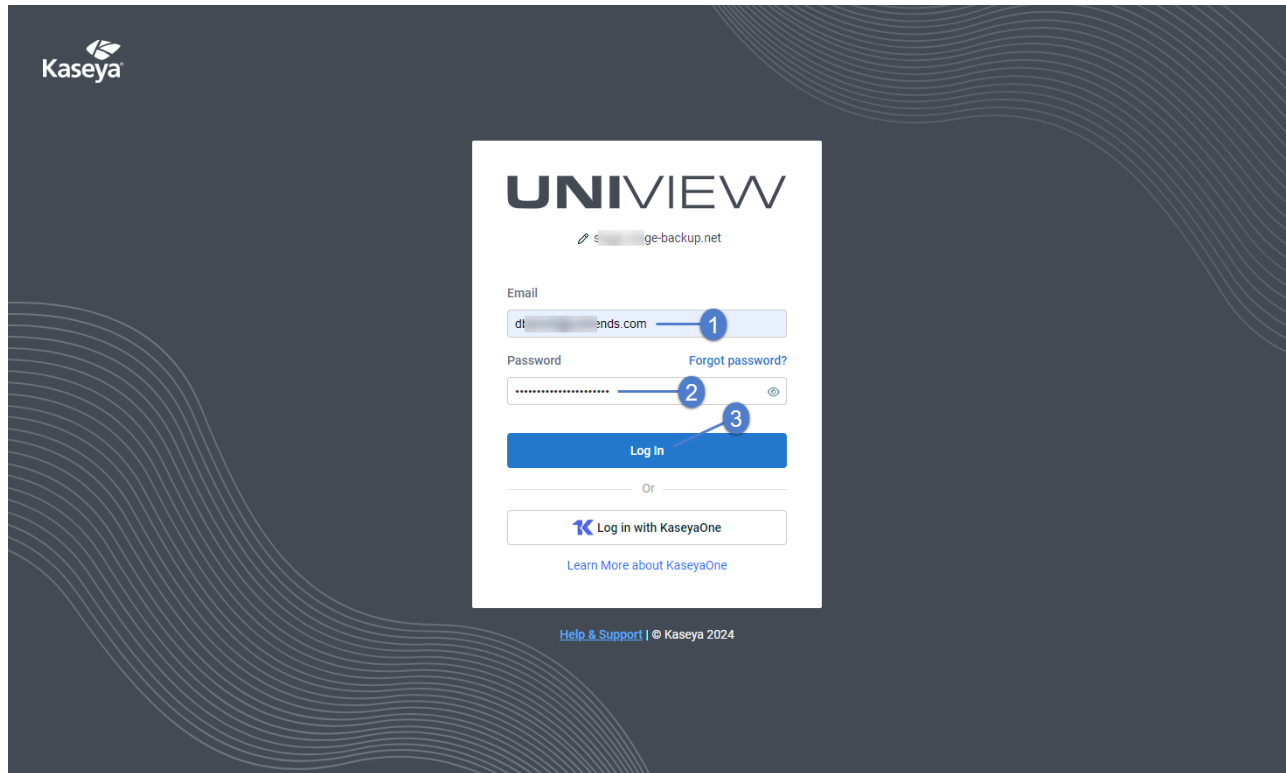
- 1 Open a Firefox or Chrome browser and enter <https://login.backup.net/> to access the Login page.



- 2 Enter the backup.net homerealm that was provided to you by the UniView Portal Onboarding team. Click **Next**.

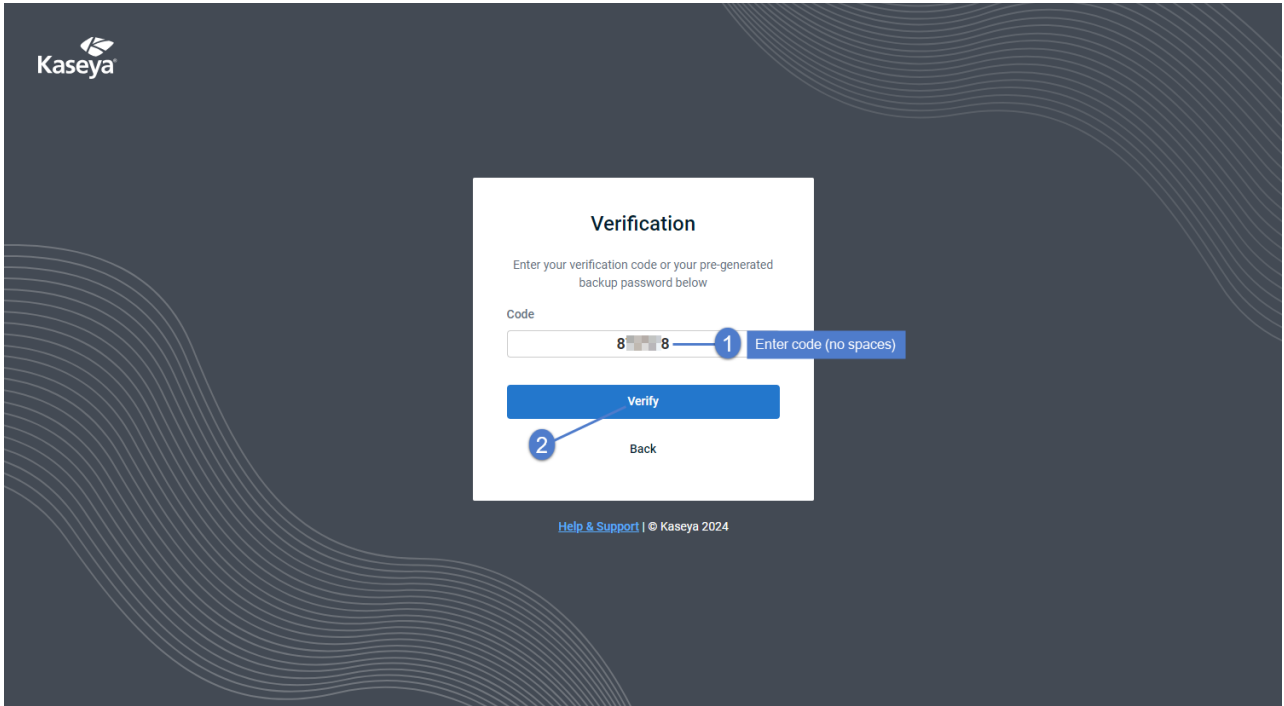


- 3 Enter the username and password of your UniView Portal account. Click **Log In**.

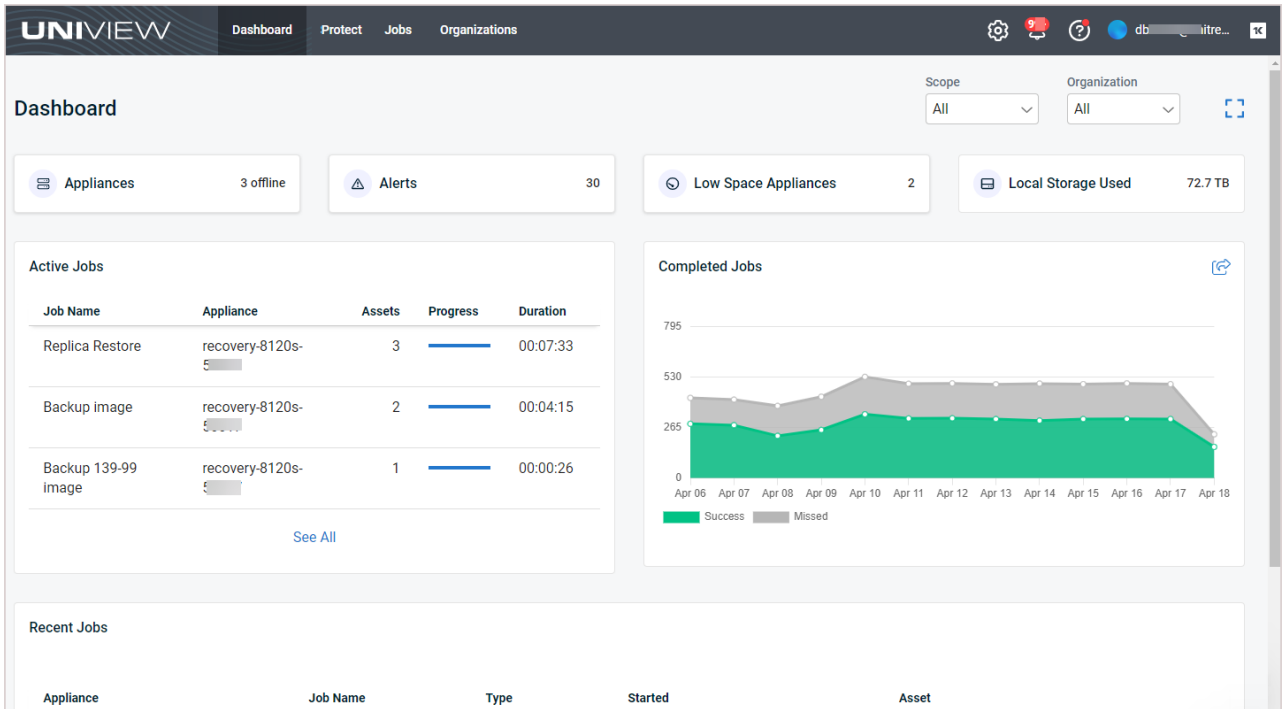


- 4 Enter your two-factor authentication (2FA) code, then click **Verify**. You can obtain the code from your authenticator app or use a recovery code.

Note: Only use a recovery code if you have lost your IOS or Android device, or cannot access your authenticator application for some other reason.



5 Upon logging in, the portal Dashboard displays.



To log in with KaseyaOne credentials

[KaseyaOne](#) is Kaseya's integrated platform of IT and security management solutions. Use this procedure to log in to the UniView Portal by using your KaseyaOne account credentials.

- 1 Open a browser and enter **<https://login.backup.net/>** to access the Login page.

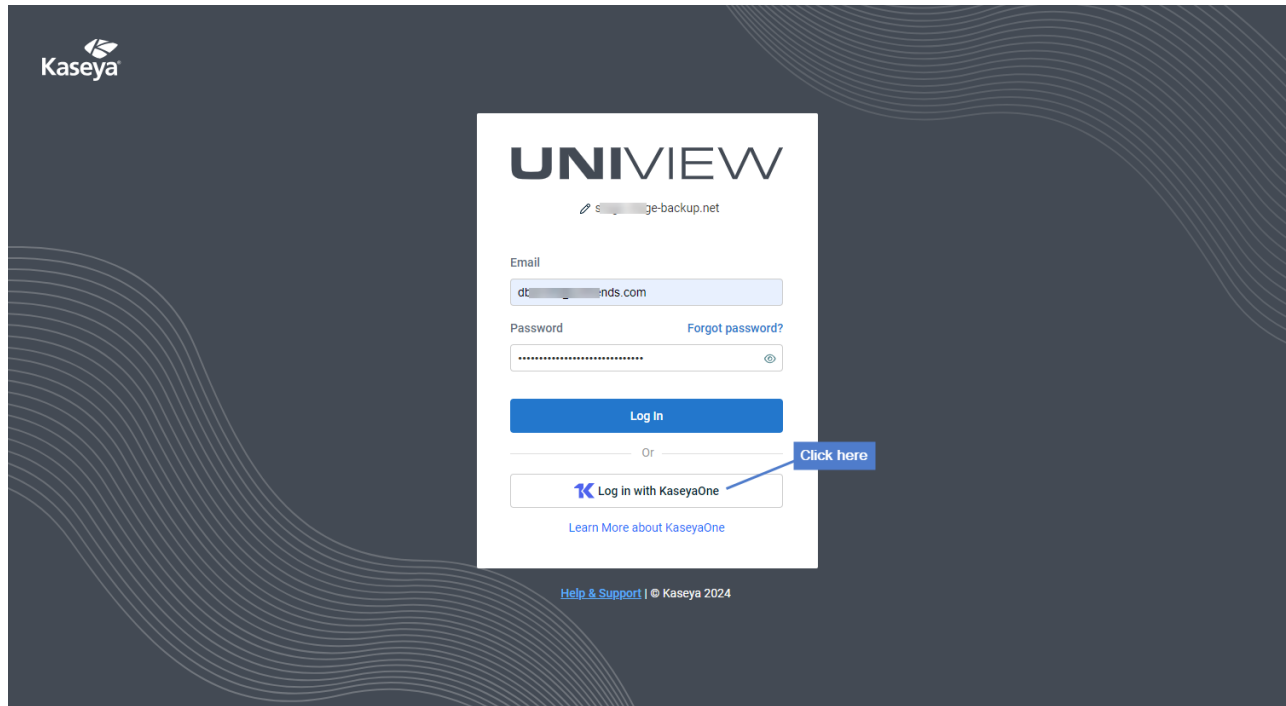


- 2 Enter the backup.net homerealm that was provided to you by the UniView Portal Onboarding team. Click **Next**.



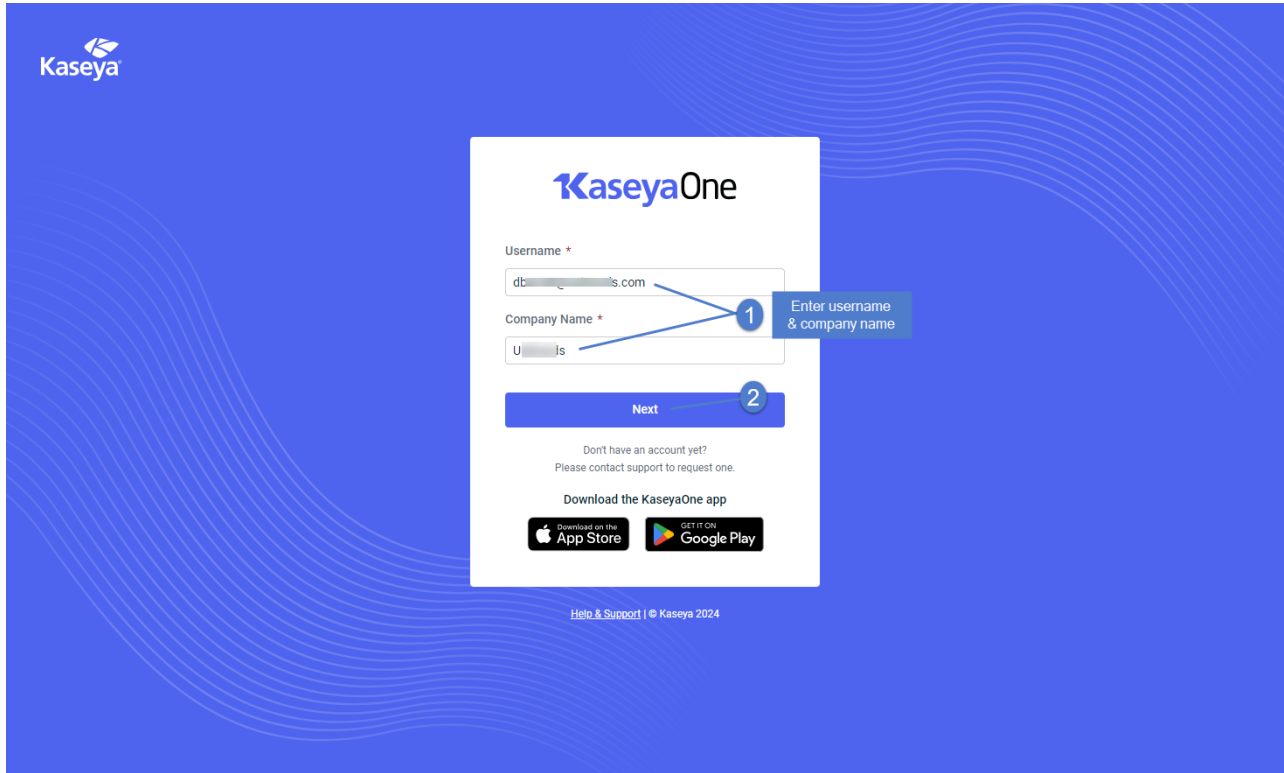
- 3 Enter your email and password. Click **Log in with KaseyaOne**.

Note: If you do not see the *Log in with KaseyaOne* button, this feature is not available in your environment.



- 4 Enter your KaseyaOne username and company name. Click **Next**.

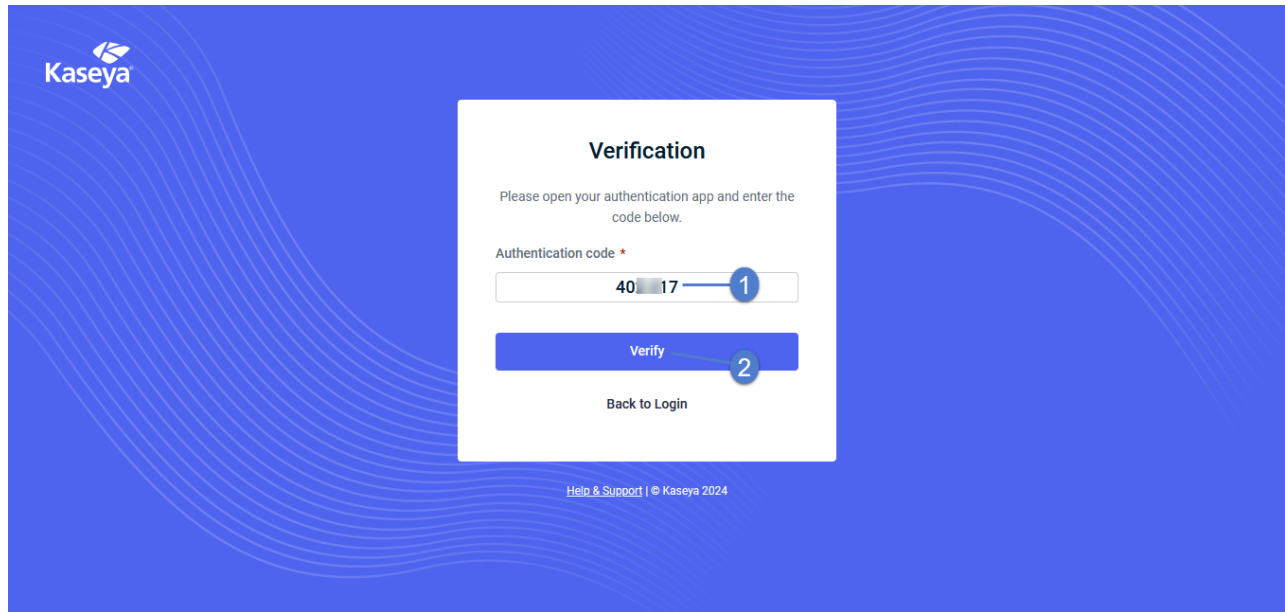
Note: If you are currently logged in to KaseyaOne, you are not prompted to enter your KaseyaOne credentials. You are automatically logged in to the UniView Portal portal without doing the remaining steps in this procedure.



5 Enter your KaseyaOne password. Click **Log In**.

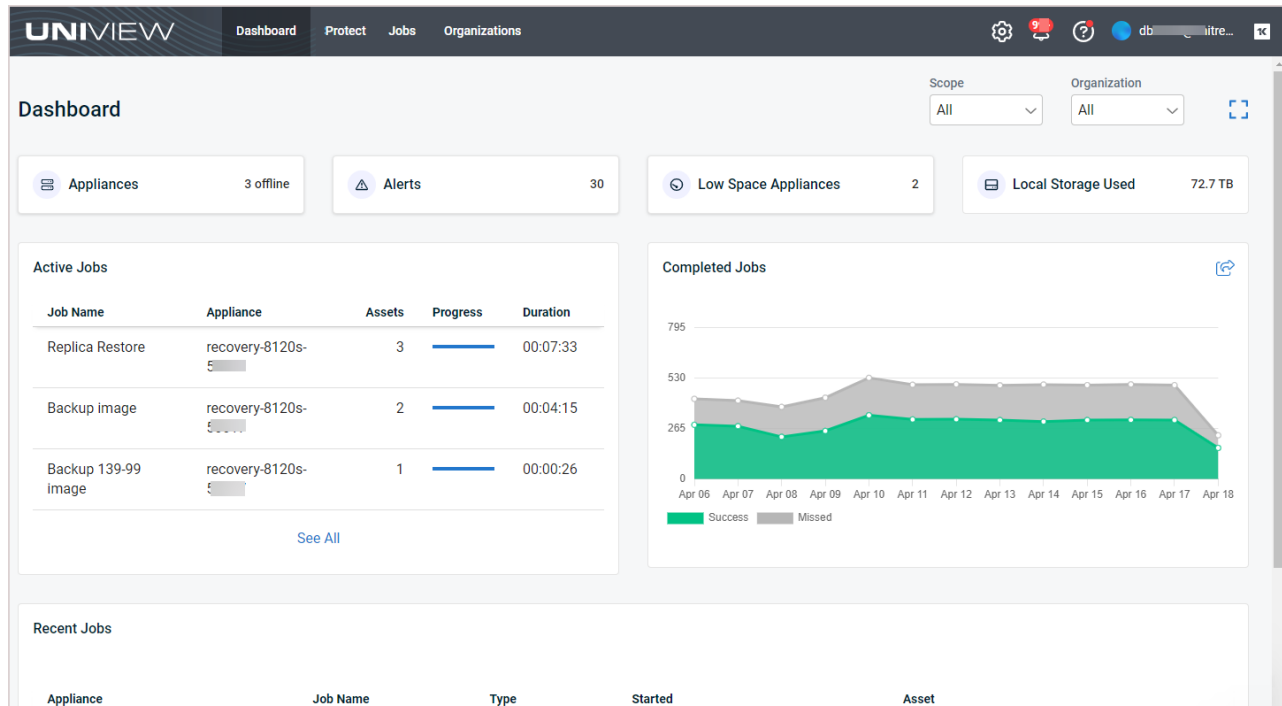


- 6 Enter your two-factor authentication (2FA) code, then click **Verify**. (You can obtain the code from your authenticator app.)



- 7 You are logged in to the UniView Portal:

Note: If you see a warning message indicating that your UniView and KaseyaOne usernames do not match, run this procedure to resolve the issue: "[To remove an older KaseyaOne/UniView mapping that was created with mismatched user names](#)".



To remove an older KaseyaOne/UniView mapping that was created with mismatched user names

Single-sign on with KaseyaOne credentials now requires matching KaseyaOne and UniView usernames. If you had enabled SSO with mismatched user names in a previous release and received a warning message when logging in with your KaseyaOne credentials, use this procedure to remove the mapping of your mismatched UniView Portal and KaseyaOne user accounts.

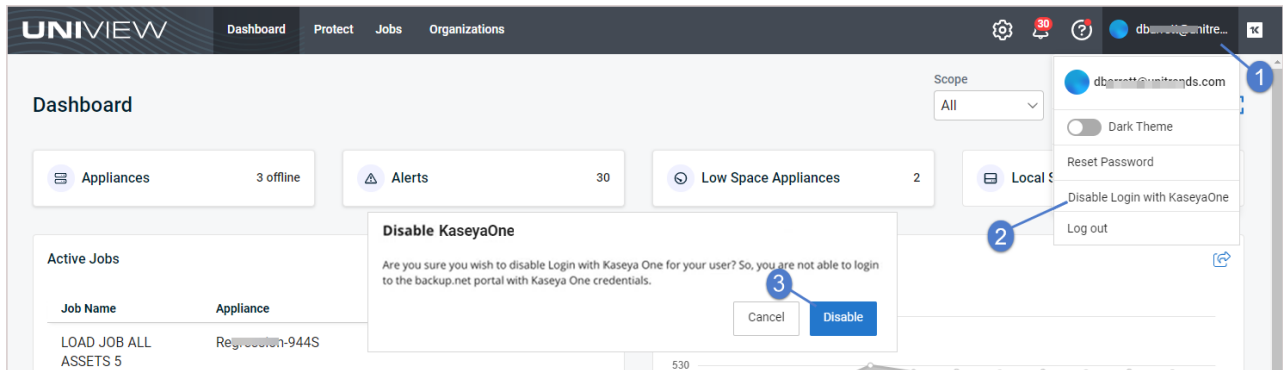
After running this procedure, simply log in using your KaseyaOne credentials (see "[To log in with KaseyaOne credentials](#)").

Note: To disable login with KaseyaOne for all UniView Portal users, see "[To disable or re-enable Login with KaseyaOne](#)".

To remove the KaseyaOne/UniView mapping:

- 1 Click your username and select **Disable Login with KaseyaOne**. Click **Disable** to confirm.

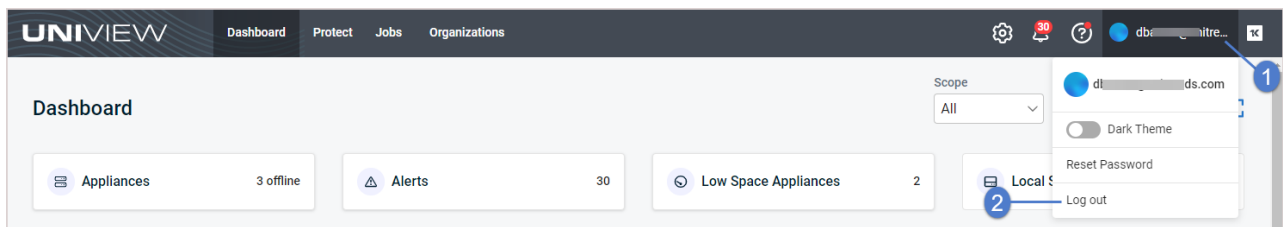
Note: If you do not see *Disable Login with KaseyaOne*, this procedure is not applicable because your KaseyaOne and UniView usernames already match (or the KaseyaOne integration has not been added to UniView Portal).



- 2 The mapping is removed. You can now log in using your KaseyaOne credentials.

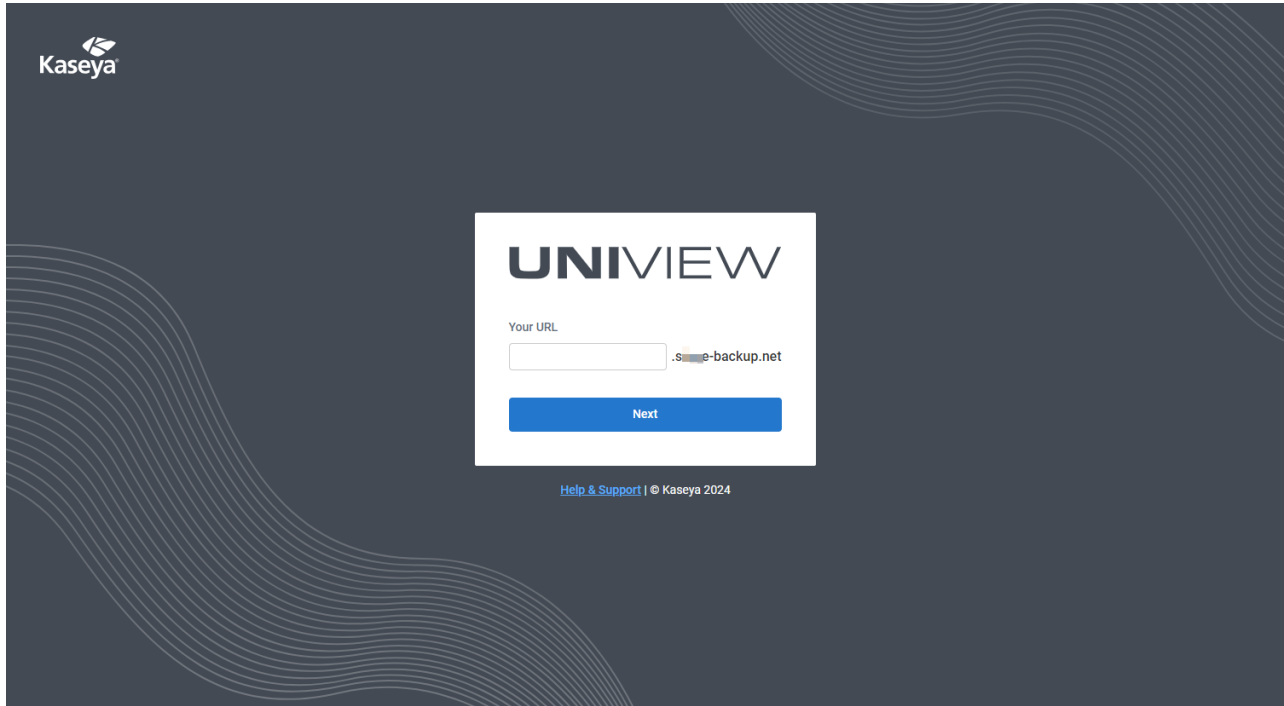
To log out of the UniView Portal

- 1 Click your username and select **Log out**.



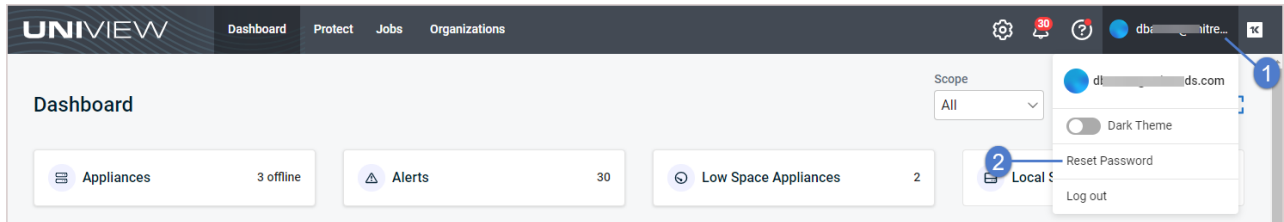
- 2 You are logged out of the portal and the Login page displays.

Note: If you had logged in by using KaseyaOne, you are also logged out of your KaseyaOne session.

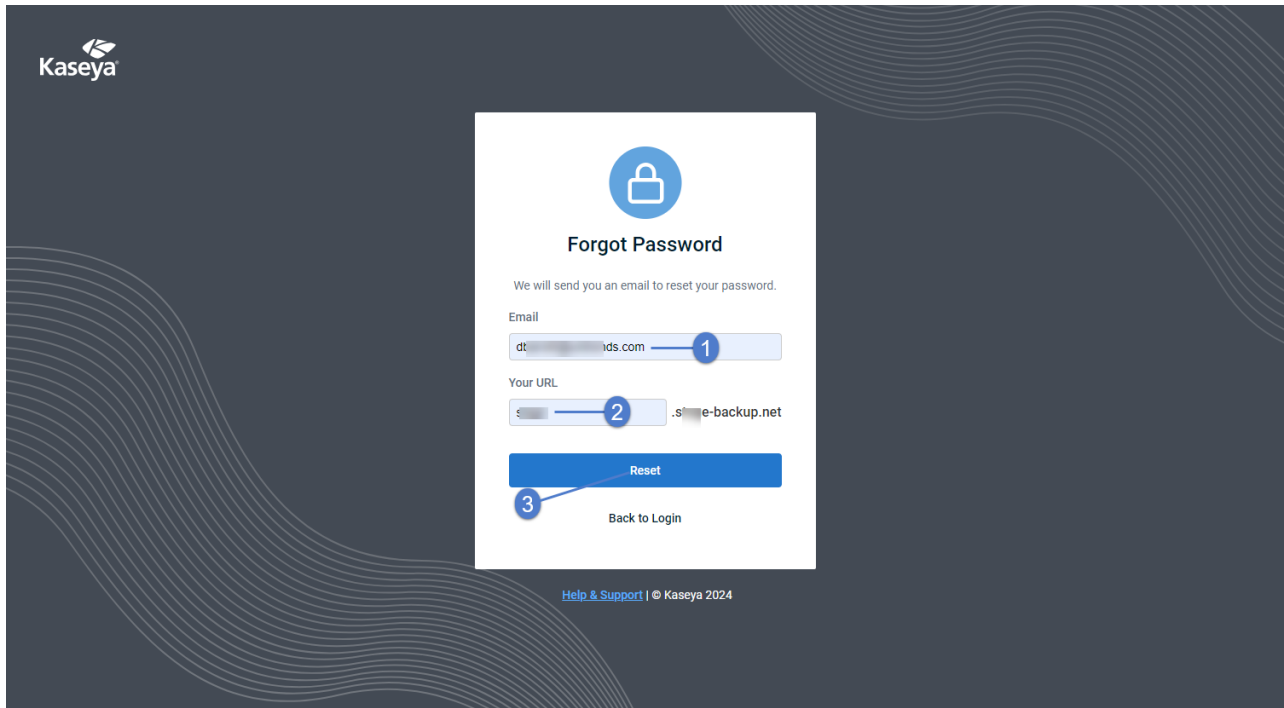


To reset your UniView Portal password

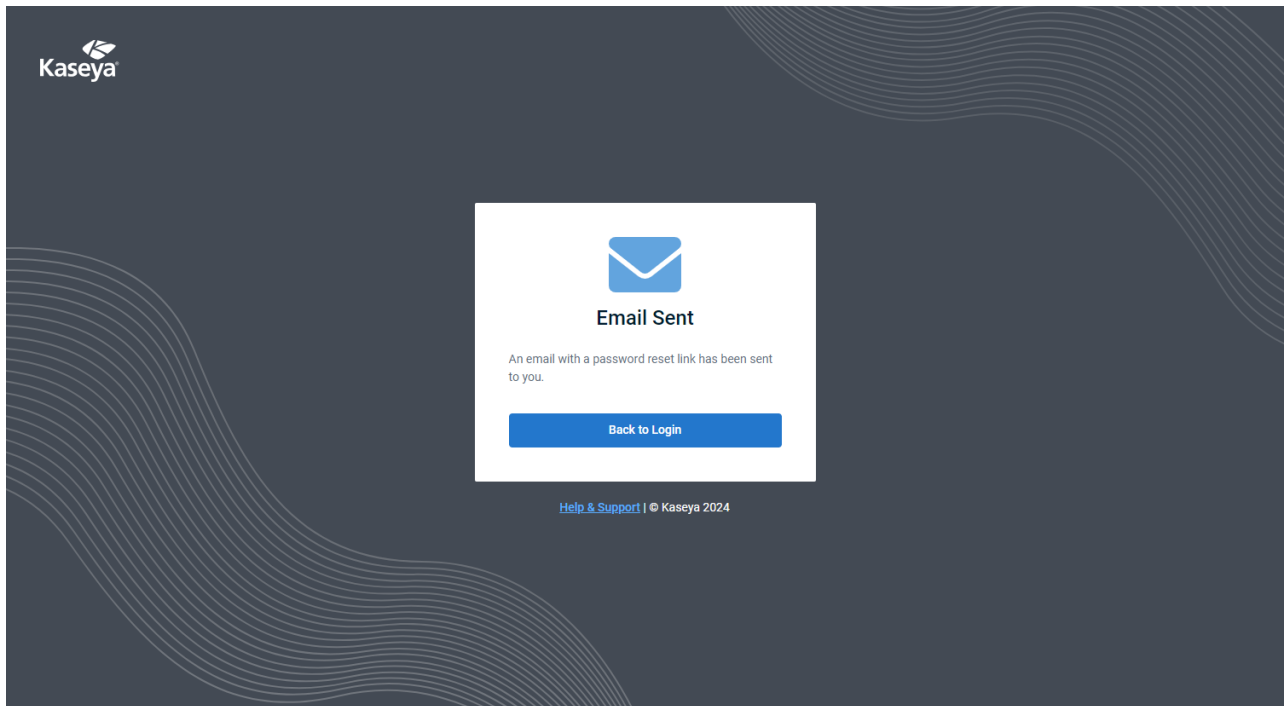
- 1 Click your username and select **Reset Password**.



- 2 On the Forgot Password page, enter the email address and homerealm associated with your portal account. Click **Reset**.

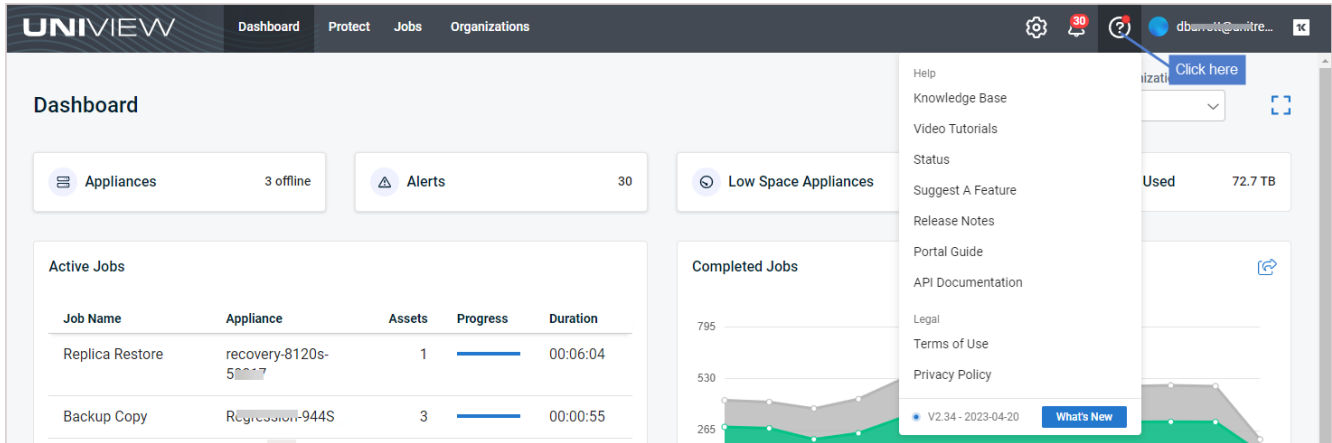



3 Check your email to reset your password.

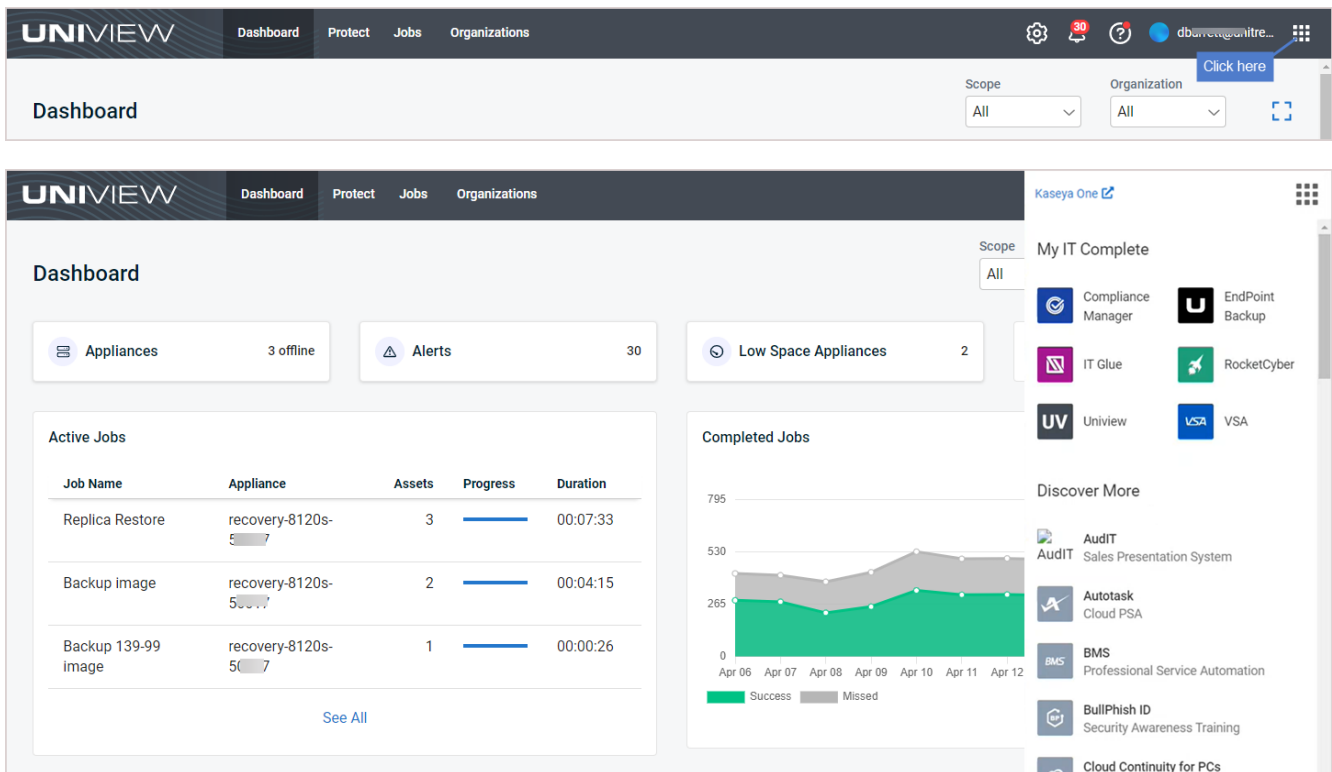


Additional resources

For additional resources, click :

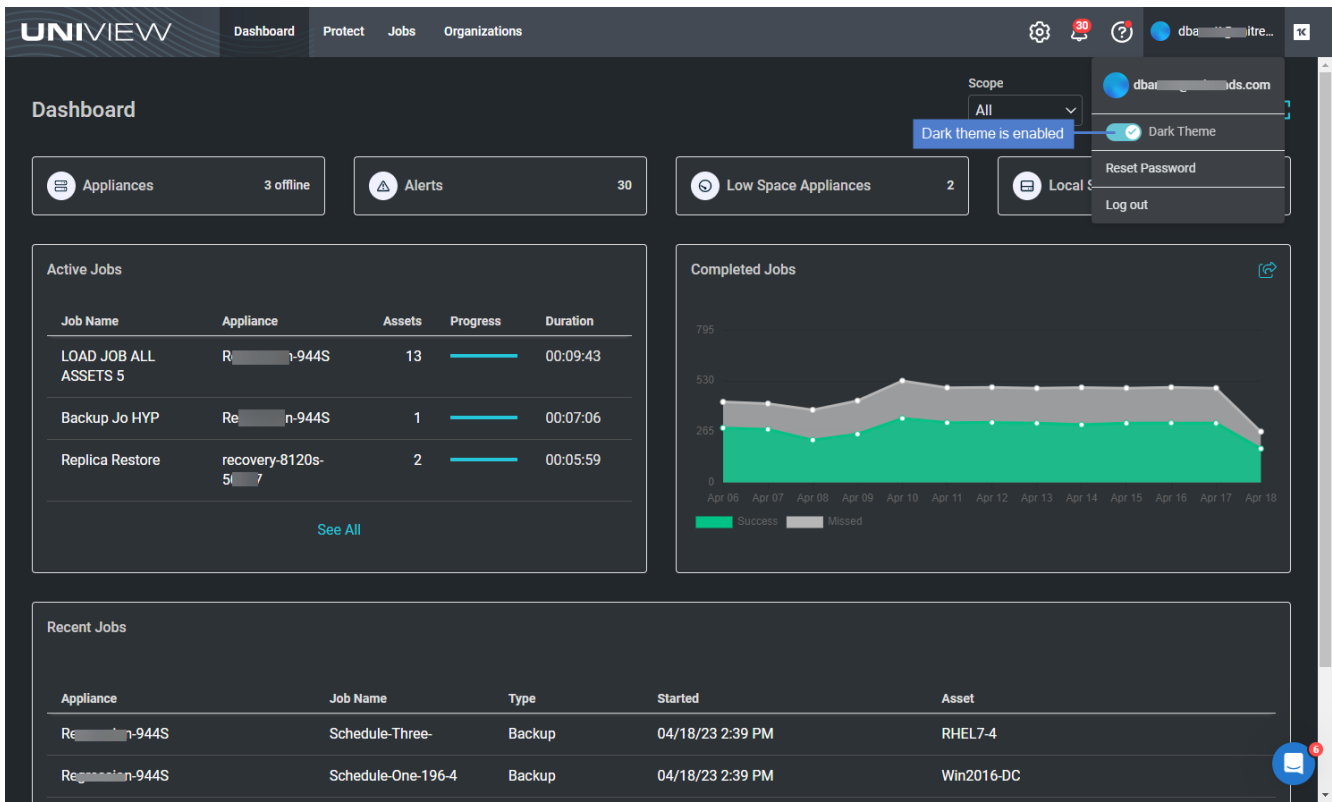
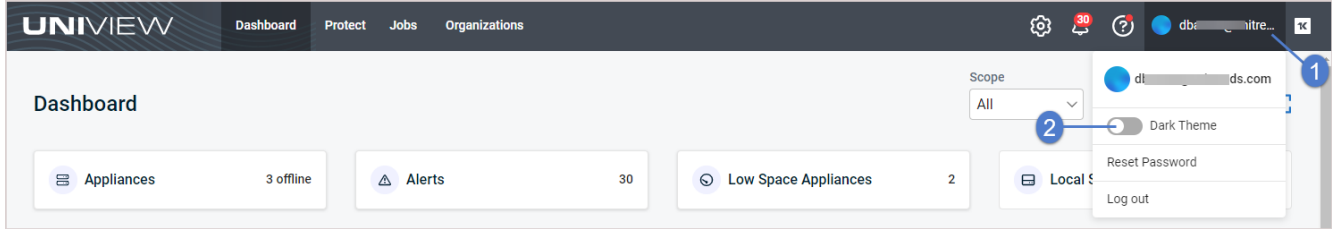


If you're logged in to KaseyaOne, click  to access the KaseyaOne application launcher:



Switching to Dark Theme view

With Dark Theme view, UI pages display with a dark background. To enable Dark Theme view, click your username and select the **Dark Theme** toggle:



Working with the Dashboard

The Dashboard provides a high-level overview of your Unitrends environments. By using the Dashboard, you can view the status of all Unitrends appliances at a glance, from a single pane of glass, and promptly address any issues. Dashboard tiles display the status of your appliances, alerts, low space appliances, storage usage, active jobs, completed jobs, and recent jobs.

See these topics for details:

- "Filtering the Dashboard"
- "Appliances tile"
- "Alerts tile"
- "Low Space Appliances tile"
- "Local Storage Used tile"
- "Active Jobs tile"
- "Completed Jobs tile"
- "Recent Jobs tile"

To access the Dashboard, click **Dashboard**:

The screenshot shows the UniView Dashboard interface. At the top, there is a navigation bar with 'Dashboard' selected, and other tabs for 'Protect', 'Jobs', and 'Organizations'. A blue arrow points to the 'Dashboard' tab with the text 'Click here'. The dashboard contains several tiles:

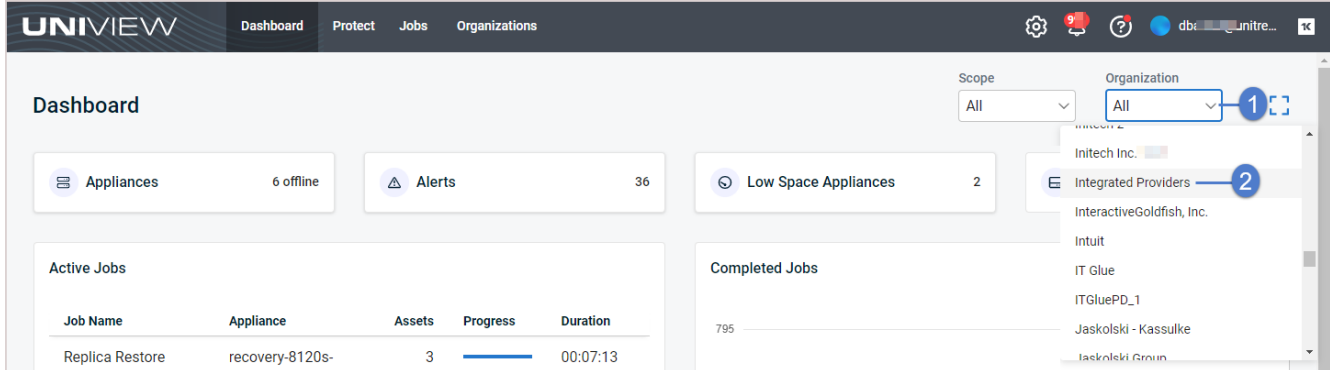
- Appliances:** 3 offline
- Alerts:** 30
- Low Space Appliances:** 2
- Local Storage Used:** 72.7 TB
- Active Jobs:** A table with columns for Job Name, Appliance, Assets, Progress, and Duration.

Job Name	Appliance	Assets	Progress	Duration
Replica Restore	recovery-8120s-50007	1	<div style="width: 100%;"></div>	00:06:04
Backup Copy	R-944S	3	<div style="width: 100%;"></div>	00:00:27
Backup Copy	LHR2-6000-5000	1	<div style="width: 100%;"></div>	00:00:25
- Completed Jobs:** A line chart showing Success (green) and Missed (grey) jobs from April 6 to April 18. The Y-axis ranges from 0 to 795. Success jobs are consistently around 250-300, while Missed jobs fluctuate between 300 and 500.
- Recent Jobs:** A table with columns for Appliance, Job Name, Type, Started, and Asset.

Appliance	Job Name	Type	Started	Asset
recovery-8120s-50007	Backup 139-99 image	Backup	04/18/23 11:32 AM	139-99
recovery-8120s-50007	Backup image	Backup	04/18/23 11:32 AM	139-216

Filtering the Dashboard

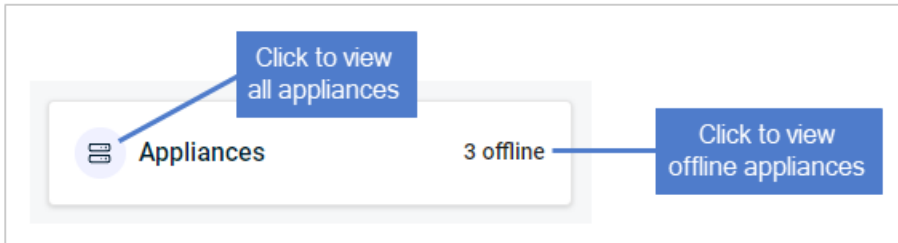
The Dashboard displays relevant information across all appliances that have been added to your backup.net instance. To filter the display, select an organization from the Organization list or a scope from the Scope list:



Appliances tile

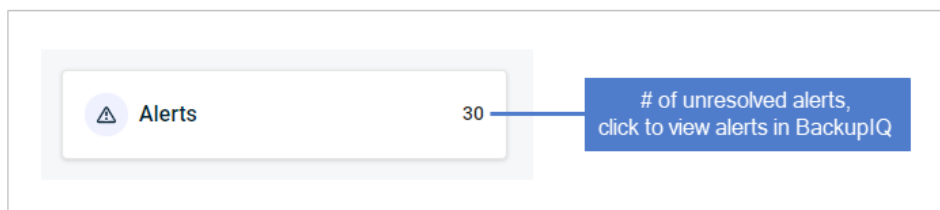
This tile shows the number of online and offline appliances.

- Appliances – Click to view all appliances on the Protect page.
- # offline – Click to view offline appliances on the Protect page.



Alerts tile

This tile shows the number of unresolved alerts across all Unitrends appliances (default view), by selected organization, or by selected scope (see ["Filtering the Dashboard"](#)). Click the tile to view alerts in BackupIQ. See ["Working with Alerts and Conditional Alarms"](#) for details about alert conditions and setting up conditional alarm thresholds.



Low Space Appliances tile

This tile shows the number of appliances whose available space is less than 30%, across all Unitrends appliances (default view), by selected organization, or by selected scope (see "[Filtering the Dashboard](#)").

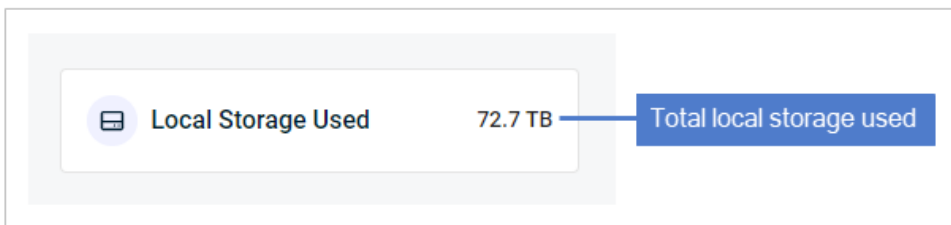
For details on managing appliance storage, see [Backup Storage](#) in the [Administrator Guide for Recovery Series, Recovery MAX, ION/ION+, and Unitrends Backup](#).



Local Storage Used tile

This tile shows the amount of local, on-appliance storage used across all Unitrends appliances (default view), by selected organization, or by selected scope (see "[Filtering the Dashboard](#)").

For details on managing appliance storage, see [Backup Storage](#) in the [Administrator Guide for Recovery Series, Recovery MAX, ION/ION+, and Unitrends Backup](#).



Active Jobs tile

This tile shows jobs currently running on all Unitrends appliances (default view), by selected organization, or by selected scope (see "[Filtering the Dashboard](#)"). The tile displays up to three active jobs (those that started most

recently).

These details are given for each job:

- Job Name – Name of the job.
- Appliance – Name of the Unitrends appliance running the job.
- Assets – Number of assets in the job.
- Progress – Bar indicating job progress.
- Duration – Time elapsed since the job started.

To view all active jobs, click **See All**. Active jobs display on the Jobs page (for details, see "[Viewing active jobs](#)").

Active Jobs				
Job Name	Appliance	Assets	Progress	Duration
Backup pr increment win32	Recovery-944S	1	<div style="width: 50%;"></div>	00:05:18
Backup image	recovery-8120s-5	2	<div style="width: 100%;"></div>	00:01:52
Backup 139-99 image	recovery-8120s-5	1	<div style="width: 100%;"></div>	00:00:41

[See All](#) Click to view all active jobs

Completed Jobs tile

This tile shows the number of successful and missed jobs over the last 13 days across all Unitrends appliances (default view), by selected organization, or by selected scope (see "[Filtering the Dashboard](#)" above):

- Hover over a point in the graph to see the number of successful and missed jobs on a given day.
- Click **Success** to hide successful jobs.
- Click **Missed** to hide missed jobs.
- For details on completed jobs, see "[Viewing job details](#)".



Recent Jobs tile

This tile shows the three most recent jobs across all Unitrends appliances (default view), by selected organization, or by selected scope (see "Filtering the Dashboard"). These details are given for each job:

- Appliance – Name of the Unitrends appliance where the job ran.
- Job Name – Name of the job.
- Type – Job type.
- Started – Date and time when the job started.
- Asset – Asset name.

To view all jobs that ran over the last 13 days, click **See All**. Jobs display on the Jobs page (for details, see "Viewing recent jobs").

Recent Jobs

Appliance	Job Name	Type	Started	Asset
recovery-8120s-500...	Backup 13... image	Backup	04/18/23 3:32 PM	13...9
recovery-8120s-500...	Backup image	Backup	04/18/23 3:30 PM	13...7
recovery-8120s-500...	Backup image	Backup	04/18/23 3:30 PM	13...6

See All — Click to view all recent jobs


This page is intentionally left blank.

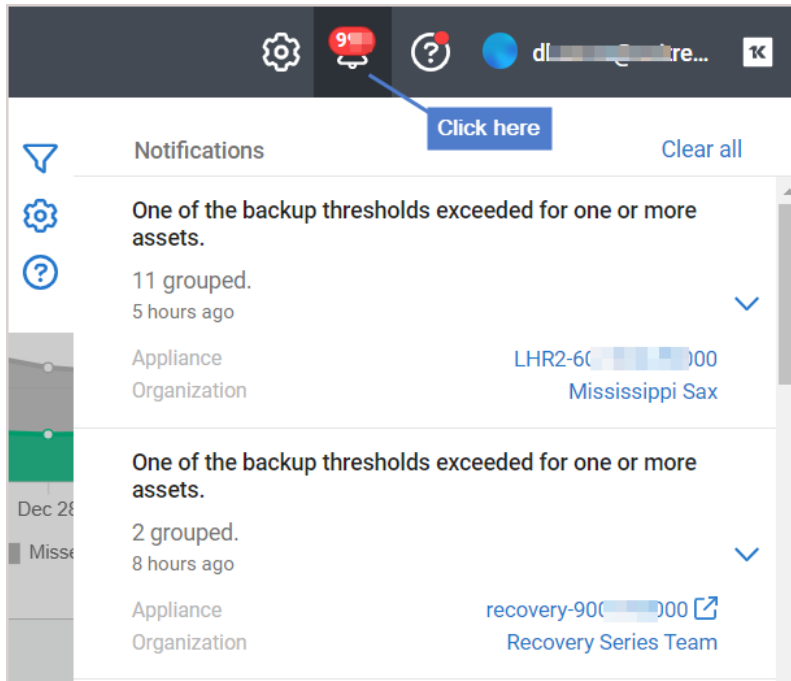


Working with Alerts and Conditional Alarms

UniView Portal includes alerts and conditional alarms to quickly notify you of issues.

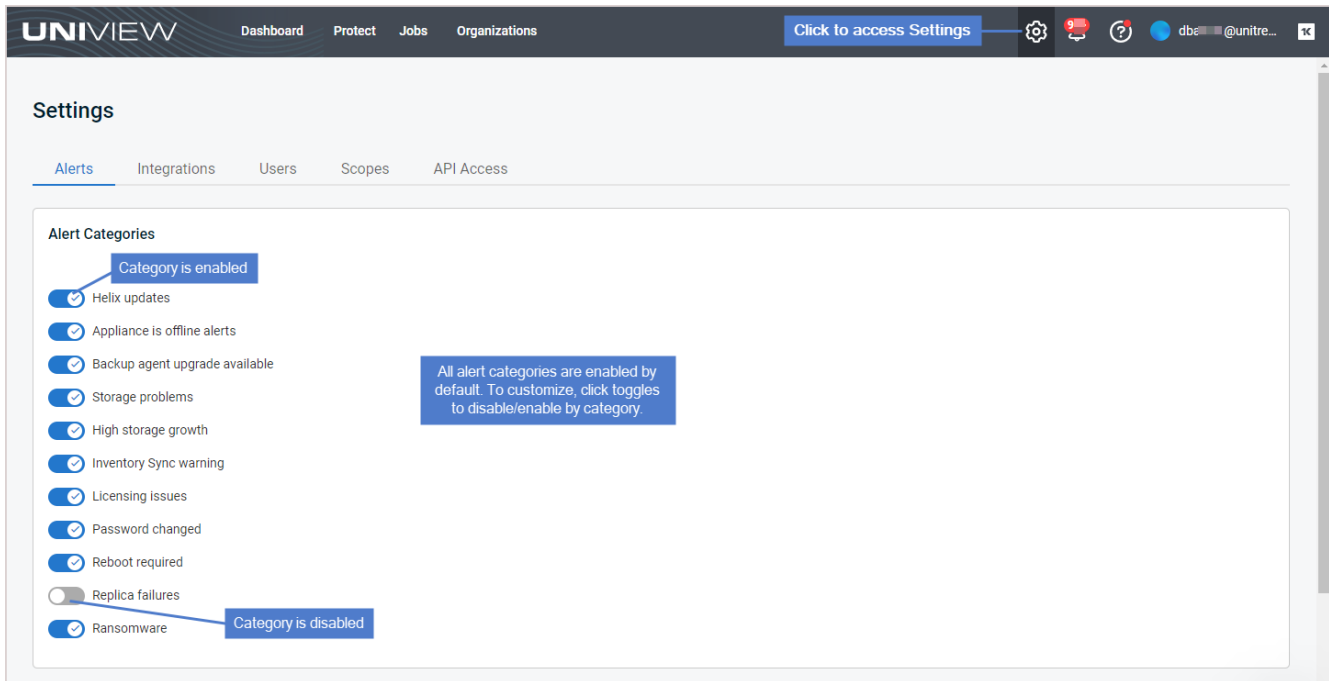
Alerts

Alerts generated across all Unitrends appliances are automatically added to BackupIQ. To access BackupIQ, click :

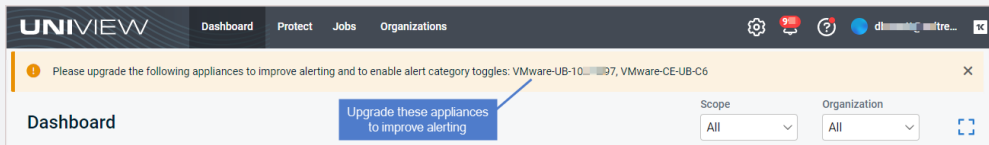


Alert conditions

By default, alerts are generated for all the categories shown below. In the Alerts view on the Settings page, you can customize the alerts you receive by clicking toggles to disable/enable alert categories:



Note: The Alert Categories feature applies to appliances running Unitrends version 10.6.1 or higher. If you have appliances running older Unitrends versions, an alert displays in the UniView Portal. Upgrade the appliances listed in the alert to improve alerting and enable alert category toggles for these older appliances.



Additional alerts

In addition to the default alerts described above, you may receive alerts for conditional alarms, Spanning Microsoft 365 backups, Spanning Google Workspace backups, Spanning Salesforce backups, or Datto Backup for Microsoft Azure (DBMA) backups:

- Conditional alarm alerts are generated if you have set up thresholds for how long a machine can go without a good backup or good hot backup copy (formerly known as *replicated backup*). For details, see "[Conditional alarms](#)".
- Spanning Microsoft 365 backup alerts are generated if you have integrated the Microsoft 365 tenant with the UniView Portal and are running Spanning Microsoft 365 backups. For details, see "[Alerts for Spanning Microsoft 365 backup](#)".
- Spanning Google Workspace backup alerts are generated if you have integrated the Google Workspace domain with the UniView Portal and are running Spanning Google Workspace backups. For details, see "[Alerts for Spanning Google Workspace backup](#)".

- Spanning Salesforce backup alerts are generated if you have integrated the Salesforce organization with the UniView Portal and are running Spanning Salesforce backups. For details, see ["Alerts for Spanning Salesforce backup"](#).
- Datto Backup for Microsoft Azure (DBMA) backup alerts are generated if you have added the Datto Portal integration to UniView Portal. To add this integration, see ["Integrating Datto Portal"](#). For details on Datto alerts, see ["Alerts for Datto Backup for Microsoft Azure \(DBMA\)"](#).

Alerts and PSA ticketing

If you have integrated your PSA system (ConnectWise Manage, Autotask, BMS, or Vorex), each alert also creates a ticket in the PSA. You can opt to automatically change the status of these tickets in PSA once the alert condition is resolved. (See ["Working with your Autotask Integration"](#), ["Working with your ConnectWise Manage integration"](#), or ["Working with your BMS or Vorex integration"](#).)

Email alerts

You can also opt to receive email notifications for alerts. For details, see ["To set up email notification for alerts"](#).

For details on viewing and managing alerts, see ["Managing alerts"](#).

Alerts for Spanning Microsoft 365 backup

If you are using Spanning Backup for Microsoft 365, you can enable BackupIQ to generate alerts for failed or partial backups. To enable these alerts, the following requirements must be met:

- Your Spanning Backup for Microsoft 365 tenant must be integrated with the UniView Portal. To add this integration, see ["Integrating a Microsoft 365 tenant"](#).
- Your Spanning Microsoft 365 tenant must be mapped to an organization in the UniView Portal. If the tenant integration was added in the UniView Portal, the tenant has been mapped to an organization. To view or modify a tenant's mapping, see ["To map Microsoft 365 tenants to organizations"](#).


Once you have enabled Spanning Microsoft 365 alerts, BackupIQ generates alerts as follows:

- BackupIQ generates alerts for tenants that have been mapped to organizations only.
- BackupIQ generates *one* alert per *tenant*.
- An alert is generated for the tenant if both of these conditions are met:
 - One or more backups over the last 7 days has either failed or was partially completed (the backup's status is Failed or Partial).
 - The Failed or Partial condition persists for 2 days.
- BackupIQ removes a Failed or Partial backup alert once the domain has had all successful backups for the last 7 days. (If a domain's Partial backup alert is followed by a Failed backup alert, BackupIQ removes the Partial backup alert and generates a Failed backup alert.)
- For each alert, BackupIQ also generates a ticket for Autotask, ConnectWise Manage, BMS, or Vorex integrations.

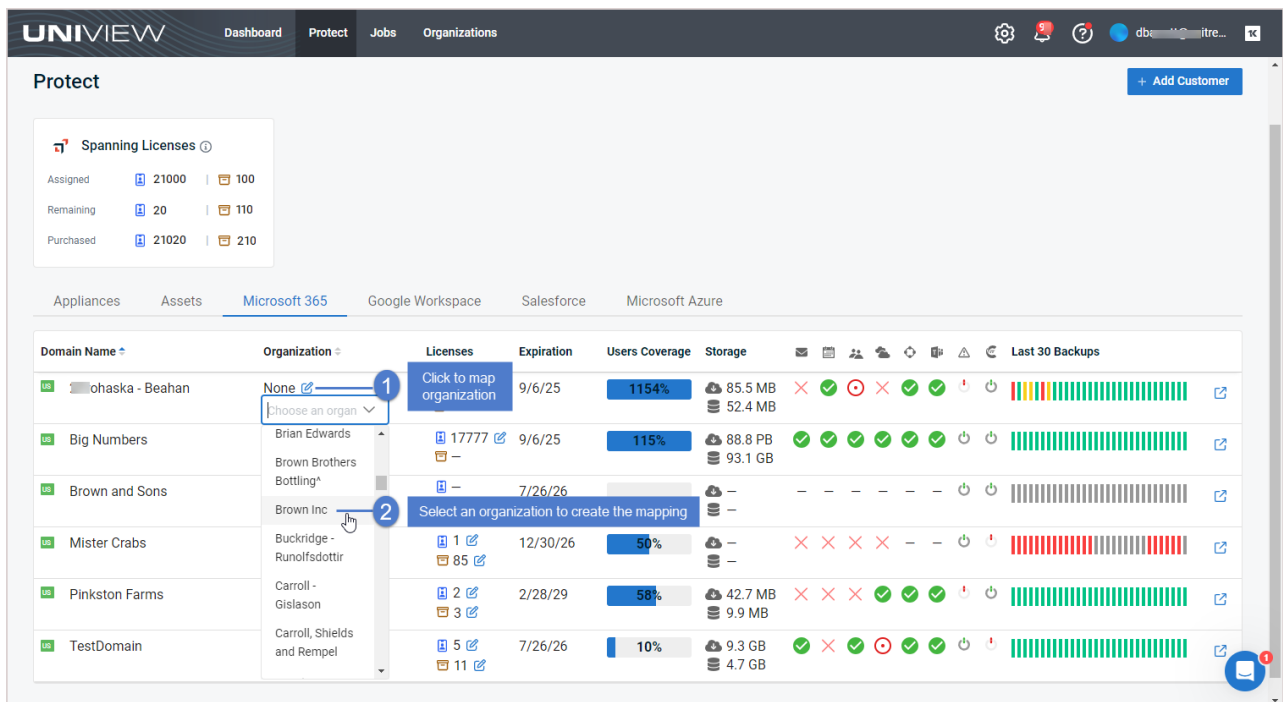
- You can also opt to receive email notifications for these alerts. To receive email notifications, run the "To set up email notification for alerts" procedure.









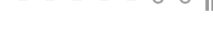






Note: For more on working with Microsoft 365 in UniView, see "Working with Microsoft 365".

To map Microsoft 365 tenants to organizations

- Log in to the UniView Portal.
- Click **Protect** and select the **Microsoft 365** view.
- To create a mapping, click  and select an organization. Repeat as needed for each tenant.

Note: Backup alerts are not generated if the tenant has not been mapped to an organization in the UniView Portal.



Domain Name	Organization	Licenses	Expiration	Users Coverage	Storage	Last 30 Backups
ohaska - Beahan	None 	Click to map organization	9/6/25	1154%	85.5 MB 52.4 MB	
Big Numbers	Brian Edwards	17777 	9/6/25	115%	88.8 PB 93.1 GB	
Brown and Sons	Brown Brothers Bottling*	—	7/26/26	—	—	
Mister Crabs	Brown Inc 	1  85 	12/30/26	50%	—	
Pinkston Farms	Buckridge - Runofsdottir	2  3 	2/28/29	58%	42.7 MB 9.9 MB	
TestDomain	Carroll - Gislason	5  11 	7/26/26	10%	9.3 GB 4.7 GB	

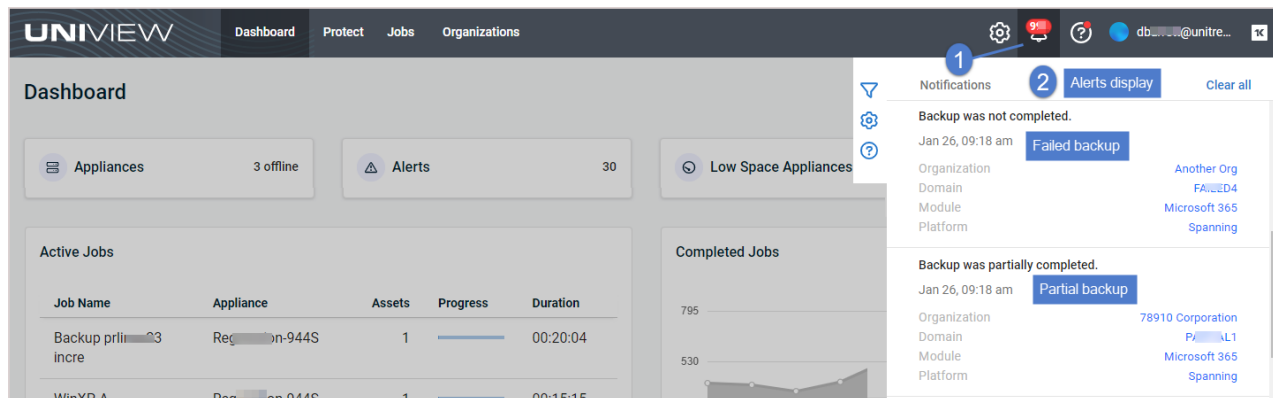
- Once mappings are created, BackupIQ generates an alert if one or more backups over the last 7 days is in Partial or Failed status, as shown below:

Note: Backup status information is received once per day from Spanning for Microsoft 365. An alert is generated if the Partial or Failed condition persists for 2 days.

- Organization link – Click to view organization details.
- Domain link – Click to view the Protect > Microsoft 365 page, which shows tenant mappings, license and storage information, and the status of each tenant's recent backups (e.g., Mail Backup, Calendar Backup,

Contact Backup, Drive Backup, SharePoint Backup, and Teams Channel Backup). For details, see ["Working with Microsoft 365"](#).

- Module link – Click to access Spanning Backup for Microsoft 365.
- Platform link – Click to access Spanning.com.



Alerts for Spanning Google Workspace backup

If you are using Spanning Backup for Google Workspace, you can enable BackupIQ to generate alerts for failed or partial backups. To enable these alerts, the following requirements must be met:


- Your Spanning Backup for Google Workspace domain must be integrated with the UniView Portal. To add this integration, see ["Integrating a Google Workspace domain"](#).
- Your Spanning Google Workspace domain must be mapped to an organization in the UniView Portal. If the domain integration was added in the UniView Portal, the domain has been mapped to an organization. To view or modify a domain's mapping, see ["To map Google Workspace domains to organizations"](#).

BackupIQ generates alerts as follows:

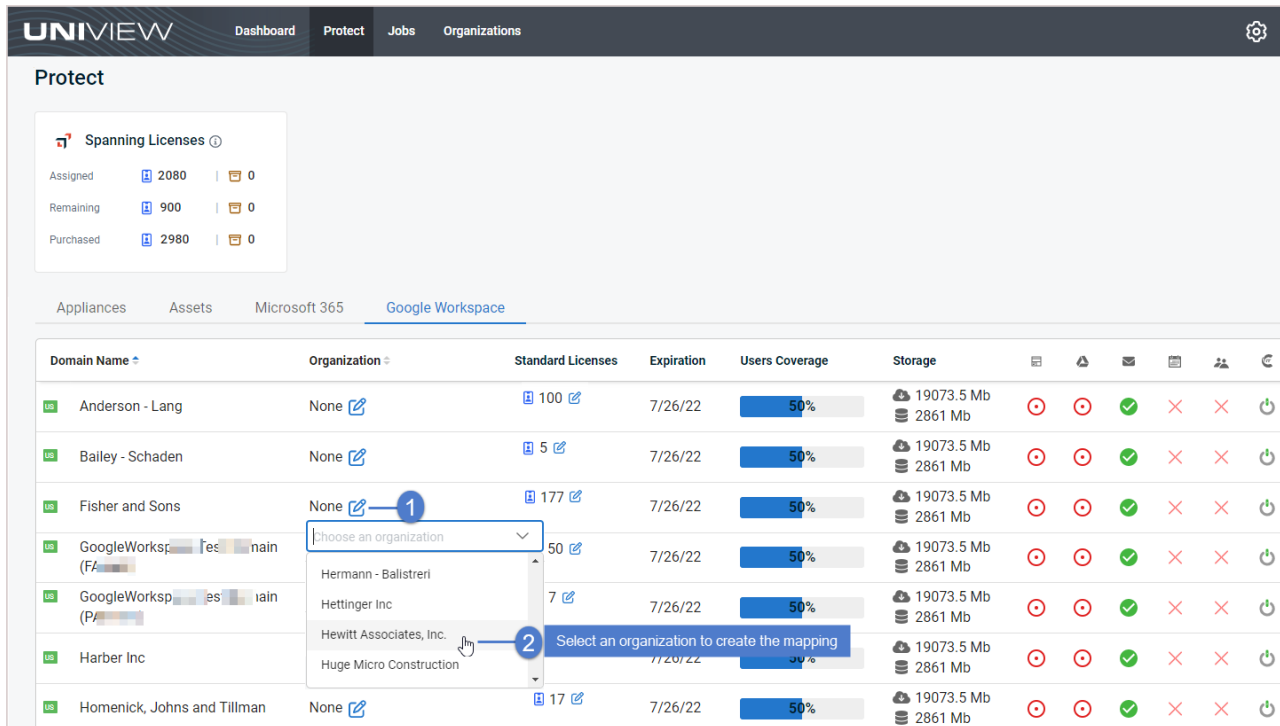
- BackupIQ generates alerts for domains that have been mapped to organizations only.
- BackupIQ generates *one* alert per *domain*.
- An alert is generated for the domain if both of these conditions are met:
 - One or more backups over the last 7 days has either failed or was partially completed (the backup's status is Failed or Partial).
 - The Failed or Partial condition persists for 2 days.
- BackupIQ removes a Failed or Partial backup alert once the domain has had all successful backups for the last 7 days. (If a domain's Partial backup alert is followed by a Failed backup alert, BackupIQ removes the Partial backup alert and generates a Failed backup alert.)
- For each alert, BackupIQ also generates a ticket for Autotask, ConnectWise Manage, BMS, or Vorex integrations.
- You can also opt to receive email notifications for these alerts. To receive email notifications, run the ["To set up email notification for alerts"](#) procedure.

Note: For more on working with Google Workspace in the UniView Portal, see "[Working with Google Workspace](#)".













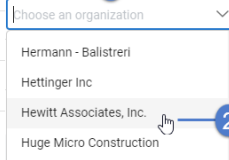













To map Google Workspace domains to organizations

- 1 Log in to the UniView Portal.
- 2 Click **Protect** and select the **Google Workspace** view.
- 3 To create a mapping, click  and select an organization. Repeat as needed for each domain.

Note: Backup alerts are not generated if the domain has not been mapped to an organization in the UniView Portal.



The screenshot shows the UniView Portal interface. At the top, there are navigation tabs: Dashboard, Protect, Jobs, and Organizations. The 'Protect' tab is active. Below the navigation, there's a 'Spanning Licenses' summary card showing Assigned (2080), Remaining (900), and Purchased (2980) licenses. Below that, there are tabs for Appliances, Assets, Microsoft 365, and Google Workspace. The Google Workspace tab is selected, displaying a table of domain mappings.

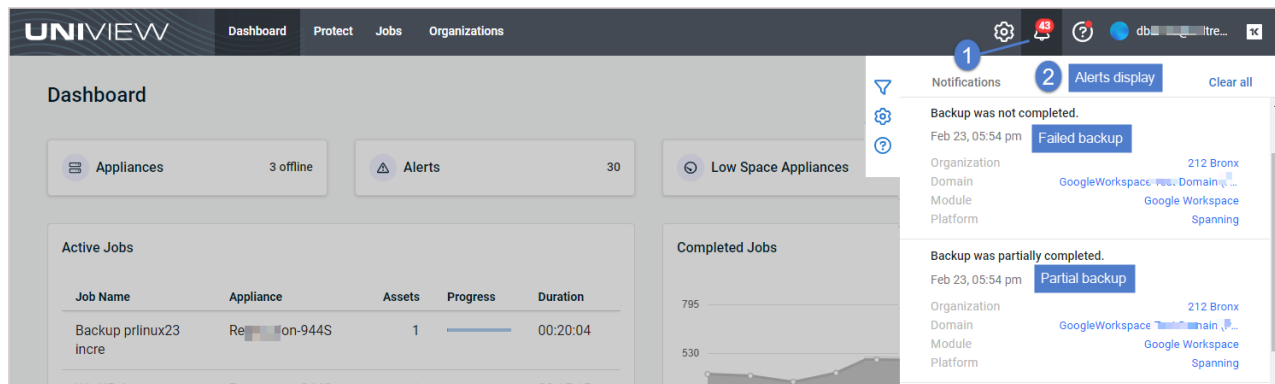
Domain Name	Organization	Standard Licenses	Expiration	Users Coverage	Storage	Alerts	Actions
Anderson - Lang	None 	100 	7/26/22	50%	19073.5 Mb 2861 Mb		
Bailey - Schaden	None 	5 	7/26/22	50%	19073.5 Mb 2861 Mb		
Fisher and Sons	None 	177 	7/26/22	50%	19073.5 Mb 2861 Mb		
GoogleWorksp... (FA...)		50 	7/26/22	50%	19073.5 Mb 2861 Mb		
GoogleWorksp... (PA...)	Hettinger Inc	7 	7/26/22	50%	19073.5 Mb 2861 Mb		
Harber Inc	Hewitt Associates, Inc.	7 	7/26/22	50%	19073.5 Mb 2861 Mb		
Homenick, Johns and Tillman	None 	17 	7/26/22	50%	19073.5 Mb 2861 Mb		

- 4 Once mappings are created, BackupIQ generates an alert if one or more backups over the last 7 days is in Partial or Failed status, as shown below:

Note: Backup status information is received once per day from Spanning for Google Workspace. An alert is generated if the Partial or Failed condition persists for 2 days.

- Organization link – Click to view organization details.
- Domain link – Click to view the Protect > Google Workspace page, which shows domain mappings, license and storage information, and the status of each domain's recent backups (e.g., Site Backup, Document Backup, Mail Backup, Calendar Backup, and Contact Backup). For details, see "[Working with Google Workspace](#)".
- Module link – Click to access Spanning Backup for Google Workspace.

- Platform link – Click to access Spanning.com.



Alerts for Spanning Salesforce backup

If you are using Spanning Backup for Salesforce, you can enable BackupIQ to generate alerts for failed backups. To enable these alerts, the following requirements must be met:

- Your Spanning Backup for Salesforce organization must be integrated with the UniView Portal. To add this integration, see ["Integrating a Salesforce organization"](#).
- Your Salesforce organization must be mapped to an organization in the UniView Portal. If the org's integration was added in the UniView Portal, the mapping has been created. To view or modify an organization's mapping, see ["To map Salesforce organizations"](#).

BackupIQ generates alerts as follows:

- BackupIQ generates alerts for Salesforce organizations that have been mapped to UniView organizations only.
- BackupIQ generates *one* alert per *organization*.
- An alert is generated for the organization if both of these conditions are met:
 - One or more backups over the last 7 days has failed (the backup's status is Failed).
 - The Failed condition persists for 2 days.
- BackupIQ removes a Failed backup alert once the organization has had all successful backups for the last 7 days.
- For each alert, BackupIQ also generates a ticket for Autotask, ConnectWise Manage, BMS, or Vorex integrations.
- You can also opt to receive email notifications for these alerts. To receive email notifications, run the ["To set up email notification for alerts"](#) procedure.

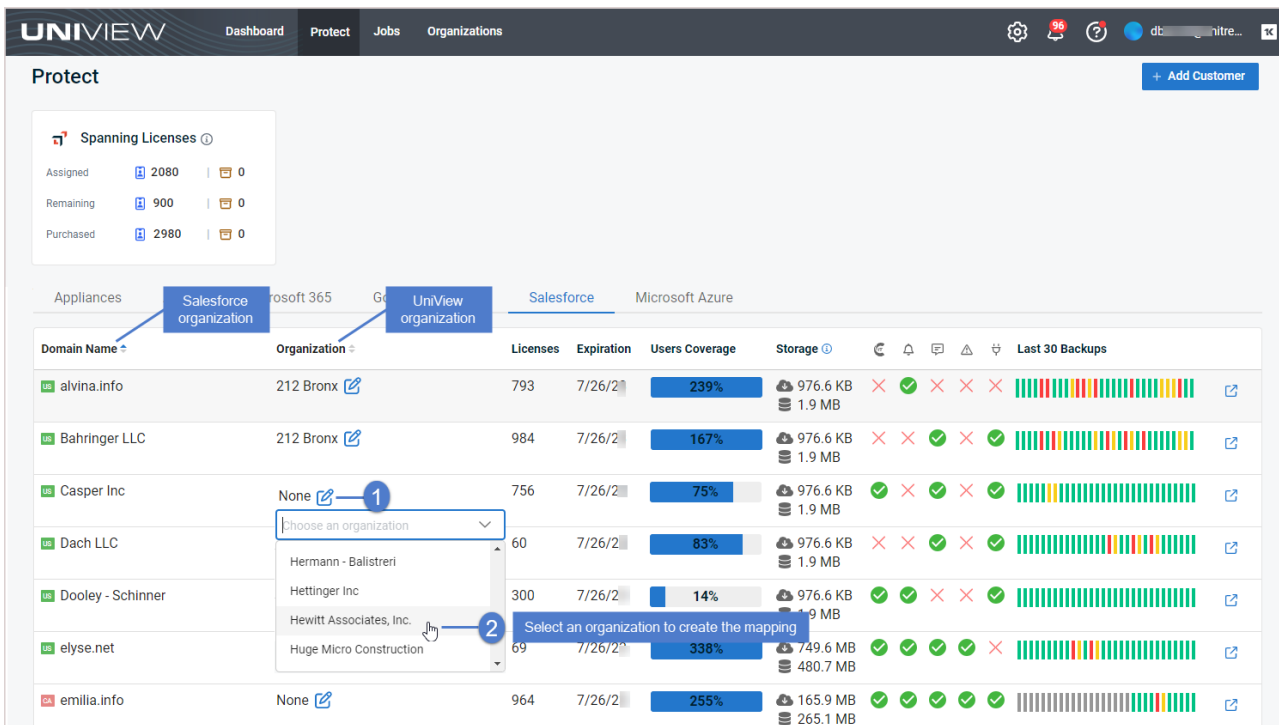
Note: For more on working with Salesforce in the UniView Portal, see ["Working with Salesforce"](#).

To map Salesforce organizations

- 1 Log in to the UniView Portal.
- 2 Click **Protect** and select the **Salesforce** view.

3 The Domain Name column lists your Salesforce organizations. To create a mapping, click [🔗](#) and select an organization. Repeat as needed for each organization.

Note: Backup alerts are not generated if the Salesforce organization has not been mapped to an organization in the UniView Portal.



4 Once mappings are created, BackupIQ generates an alert if one or more backups over the last 7 days is in Failed status, as shown below:

Note: Backup status information is received once per day from Spanning for Salesforce. An alert is generated if the Failed condition persists for 2 days.

- Organization link – Click to view organization details.
- Domain link – Click to view the Protect > Salesforce page, which shows organization mappings, license and storage information, and the status of each organization's recent backups. For details, see "Working with Salesforce".
- Module link – Click to access Spanning Backup for Salesforce.
- Platform link – Click to access Spanning.com.

The screenshot displays the UniView portal interface. At the top, there are navigation tabs: Dashboard, Protect, Jobs, and Organizations. The main content area is titled "Backup Status" and is currently filtered for "Salesforce". Below this, there are tabs for Appliances, Assets, Microsoft 365, Google Workspace, and Salesforce. A table lists the backup status for four domains: amelia.org, ava.info, jaeden.com, and karlie.biz. The table columns include Domain Name, Organization, Licenses, Expiration, Users Coverage, and Storage. The Users Coverage column shows progress bars and percentages. The Storage column shows two storage metrics for each domain. To the right of the table, a notification panel is open, showing a "Backup was not completed" alert from 18 minutes ago. The notification details include Organization (ABCD), Domain (amelia.org), Module (Salesforce), and Platform (Spanning). Below this, it shows the "Latest backup failed" alert, also from 18 minutes ago, with details for Organization (ABCD), Domain (ava.info), Module (Salesforce), and Platform (Spanning).

Domain Name	Organization	Licenses	Expiration	Users Coverage	Storage
amelia.org	ABCD	770	7/26/24	3%	869.8 MB 472.1 MB
ava.info	ABCD	888	7/26/24	157%	321.4 MB 168.8 MB
jaeden.com	ABCD	142	7/26/24	1548%	412.9 MB 135.4 MB
karlie.biz	ABCD	993	7/26/24	114%	768.7 MB 224.1 MB

Alerts for Datto Backup for Microsoft Azure (DBMA)

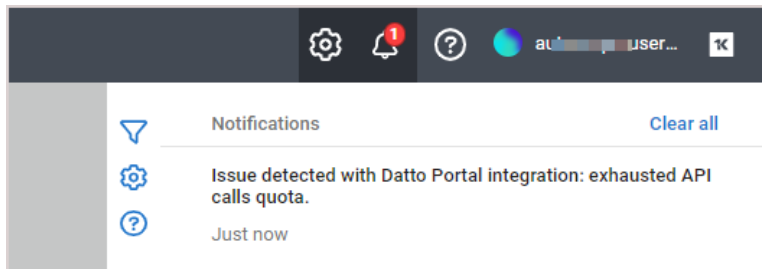
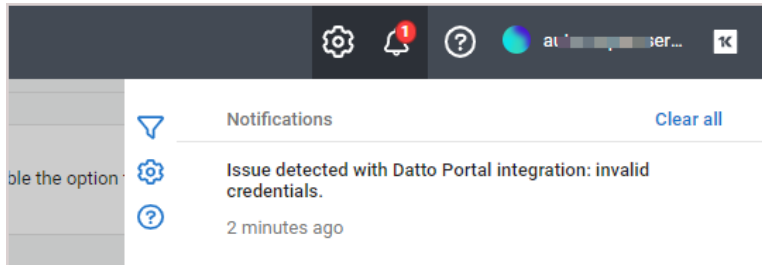
If you are using DBMA, you can enable BackupIQ to generate alerts for integration issues and failed Microsoft Azure backups. To enable these alerts, the following requirements must be met:

- The Datto Portal integration has been added to UniView Portal. (To add this integration, see "[Integrating Datto Portal](#)".)
- Your Datto clients are mapped to organizations in the UniView Portal. During integration, all clients are automatically mapped to UniView Portal organizations. (If needed, you can modify these mappings as described in "[Mapping Datto Portal clients to organizations](#)".)

Once you have enabled DBMA alerts, BackupIQ generates integration alerts and backup alerts.

- Integration alerts are generated if UniView Portal cannot connect to DBMA due to invalid credentials or if the maximum API calls quota has been reached:

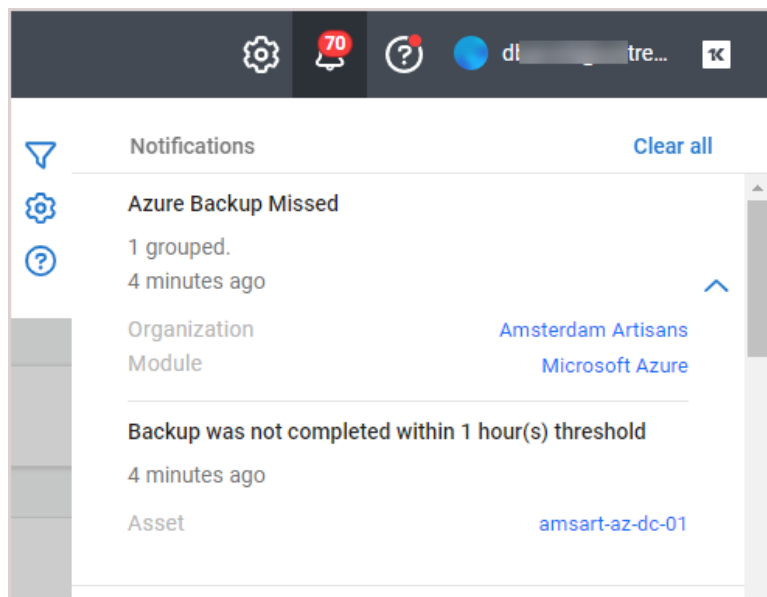
Note: PSA tickets are not generated for integration alerts.



- Microsoft Azure backup alerts are generated as follows:
 - BackupIQ generates backup alerts for assets whose Datto clients have been mapped to organizations only.
 - BackupIQ generates *one* backup alert per asset. Backup alerts are grouped by DBMA module and UniView Portal organization.
 - By default, a backup alert is generated if a successful backup has not completed for the asset within the last 24 hours. If needed, you can modify this 24-hour threshold setting (see "[Conditional alarms](#)").
 - BackupIQ removes a backup alert once the asset has had a successful backup.
 - Organization link – Click to view organization details.
 - Module link – Click to access the Datto Portal.

- Asset link – Click to view details on the Protect > Microsoft Azure page.

Microsoft Azure backup alert in BackupIQ:



Microsoft Azure backup alert for FILESERVER asset in Datto Portal:

Sengupta Technologies						
Sengupta-CSiris	Model	Client	Last Checkin	Tickets	Total Managed Disk	
SN: 0230-1900-7B3	CLDSIRIS	Sengupta Technologies	4 minutes ago	0	254 GB	⋮
Protected System	Unprotected	Latest Screenshot	Last Offsite Sync	Last Local Backup	Last 10 Backup Attempts	
FILESERVER	0 volumes	a year ago	a year ago	a year ago	●●●●●●●●●●	⋮
Sengup-vm1	0 volumes	5 hours ago	21 minutes ago	21 minutes ago	●●●●●●●●●●	⋮

[+ Protect a System](#)

- For each backup alert, BackupIQ also generates a ticket for Autotask, ConnectWise Manage, BMS, or Vorex integrations. (Tickets are NOT generated for integration alerts.)
- You can also opt to receive email notifications for these alerts. To receive email notifications, run the "To set up email notification for alerts" procedure.

Note: For more on working with DBMA in UniView, see "Working with your Datto Portal integration".

Managing alerts

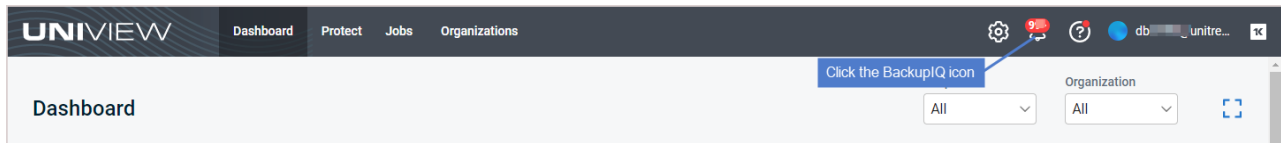
Use these procedures to view and manage alerts:

- "To view BackupIQ alerts"
- "To dismiss a group of alerts"

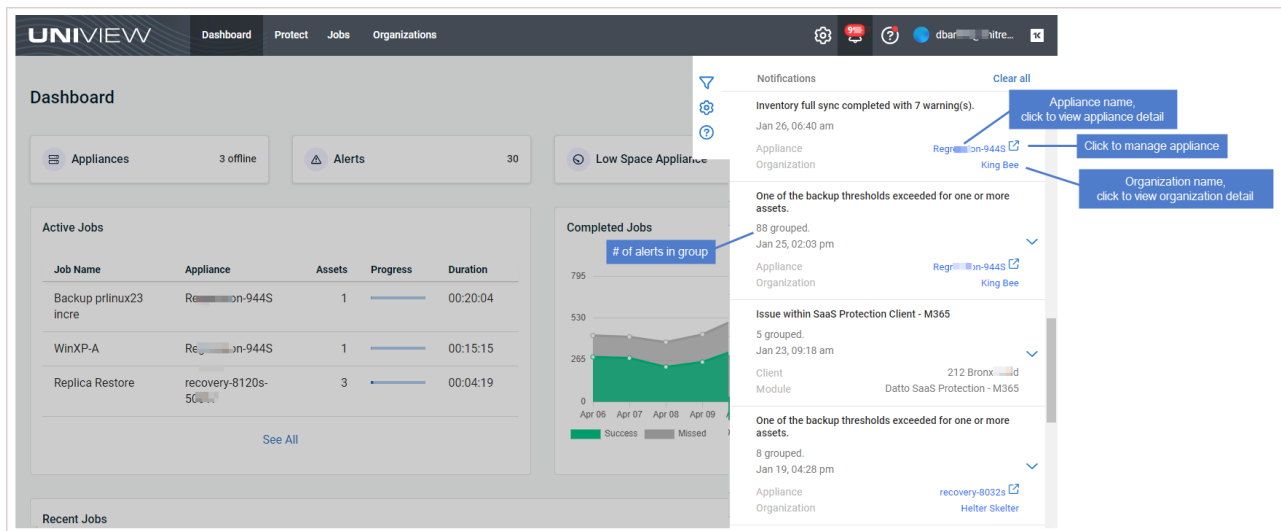
- "To dismiss BackupIQ alerts in bulk by organization or scope"
- "To dismiss all BackupIQ alerts"
- "To set up email notification for alerts"

To view BackupIQ alerts

- 1 Click the BackupIQ icon in the upper-right corner.



- 2 Alerts display:



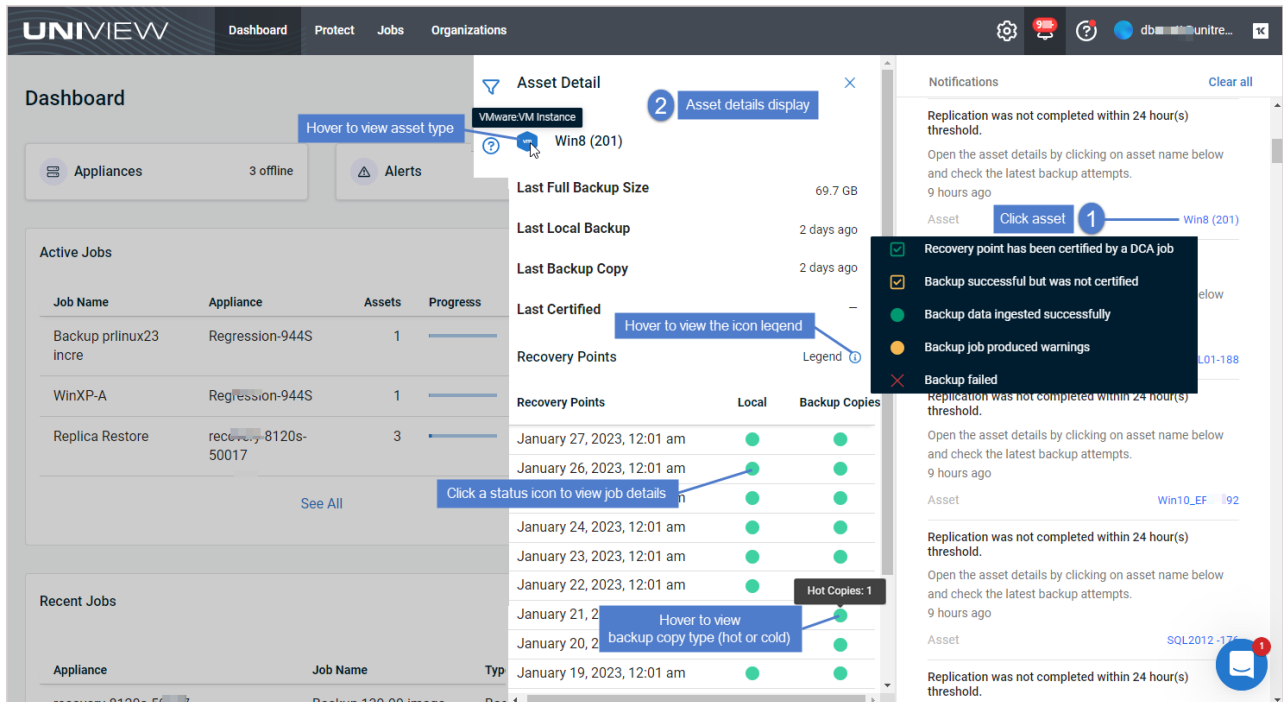
- 3 (Optional) Click an asset to display asset detail. The following information is given for each asset:

- Type icon – Indicates the asset type. Hover over the icon for type description. Asset type examples: VMware, Windows, SQL, OS (for non-Windows assets protected by installing the Unitrends agent).
- Asset name.
- Last Full Backup Size – Size of the last successful full backup.
- Last Local Backup – Number of minutes, hours, days, weeks, or months since the last backup.
- Last Backup Copy – Number of minutes, hours, days, weeks, or months since the last hot or cold backup copy. – displays if no backups have been copied.
 - *Hot backup copies* reside in the Unitrends Cloud or on a secondary appliance.
 - *Cold backup copies* reside on storage managed by other cloud storage providers (e.g., Amazon S3 or Rackspace) or on other backup copy media (e.g., a tape or NAS storage device).

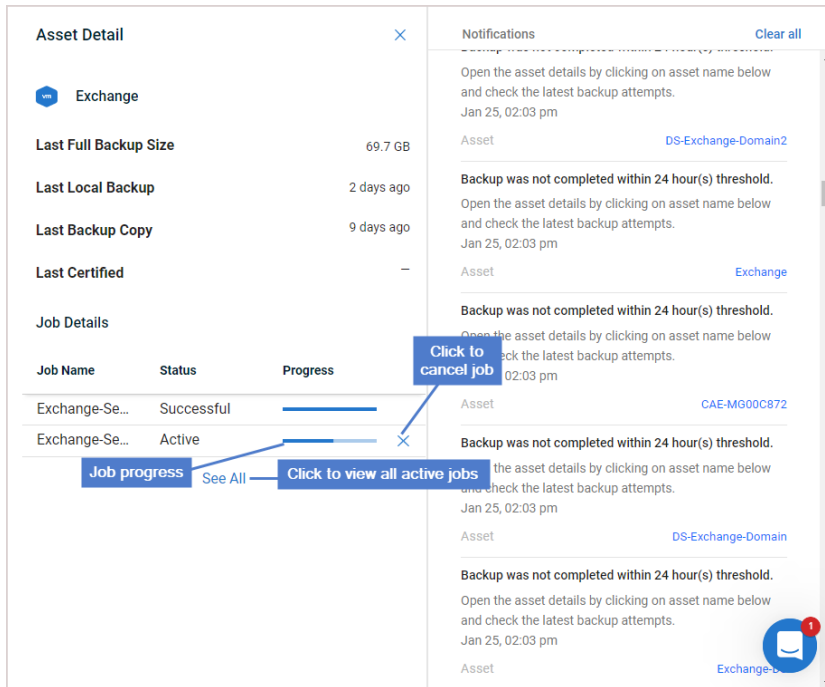
- Last Certified – Number of minutes, hours, days, weeks, or months since the last backup was certified by a data copy access (DCA) job.
- Recovery Points – Lists the asset's local backups and backup copies. Scroll to view older recovery points.

Icons display, indicating the status of each local backup and backup copy. Click a status icon to view job details. Hover over **Legend** ⓘ for a description of each status.

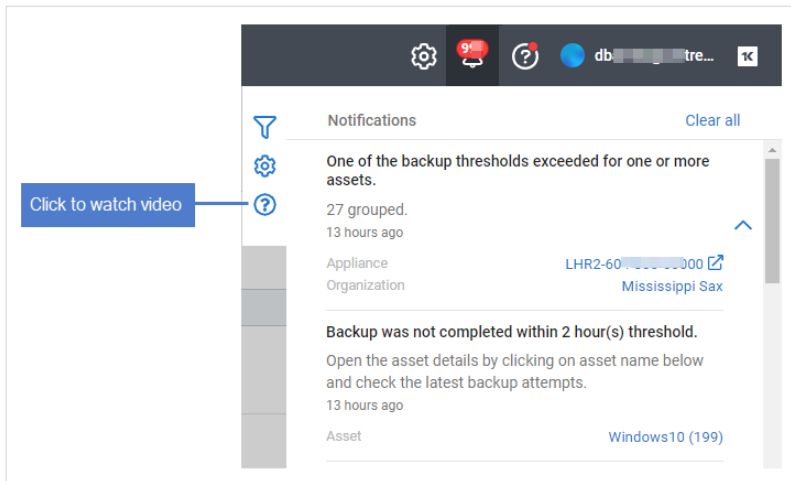
Hover over a backup copy icon to see whether it is a hot or cold copy.




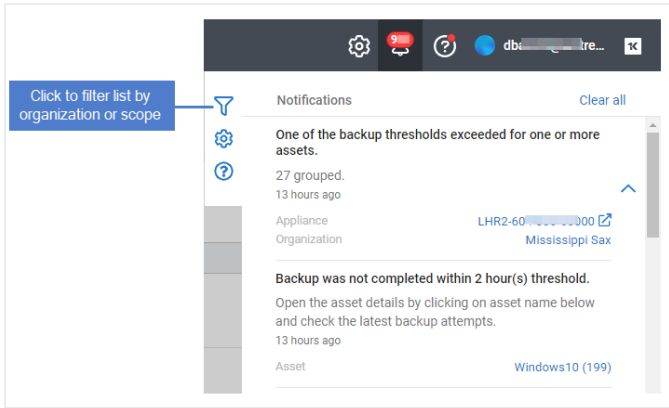
- If a job is running, job details display. Click X to cancel a running job. Click **See All** to view all active jobs.



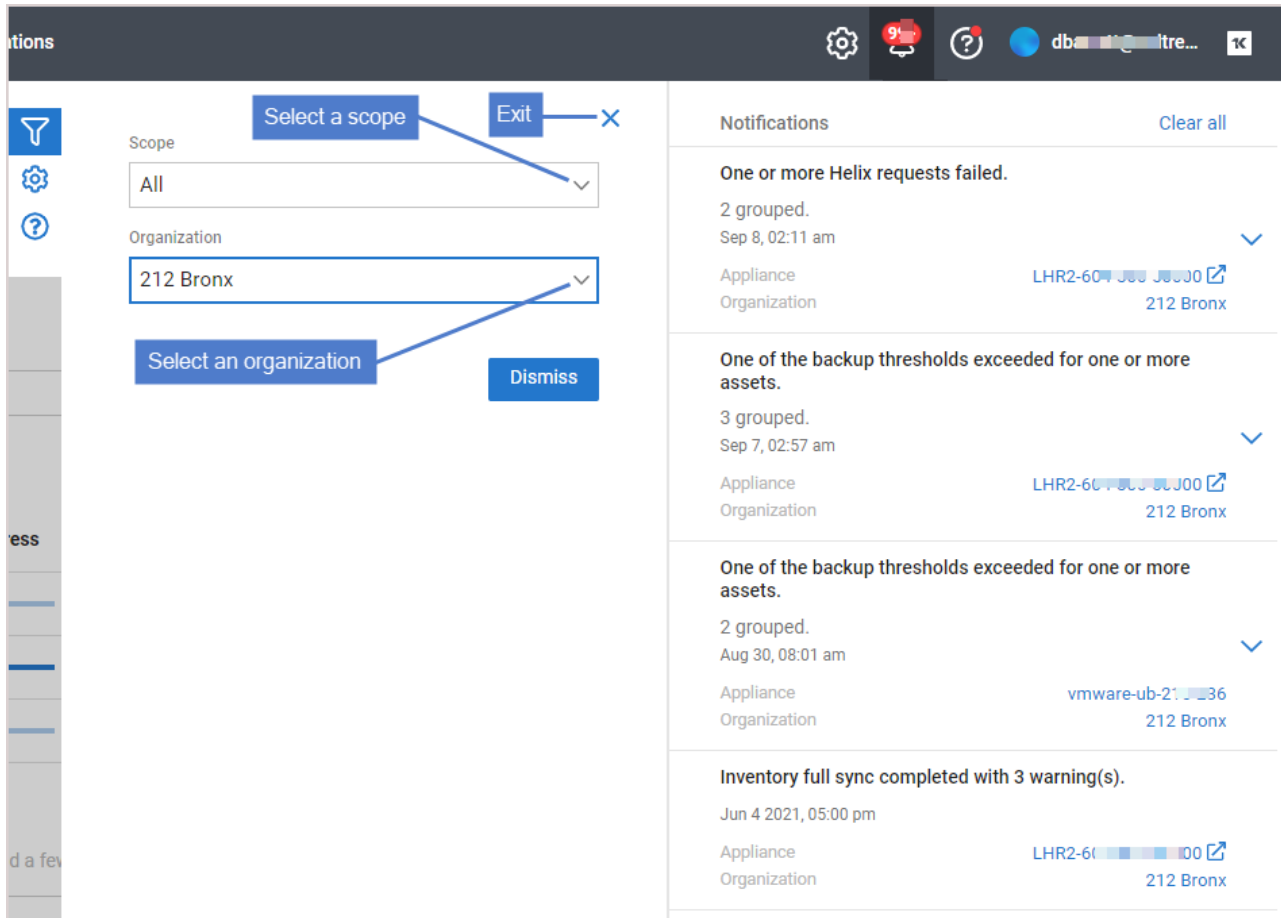
4 (Optional) Click  to watch the [Unitrends - Conditional Alarms video](#):



5 (Optional) Click  to filter the list by organization:




- Select an organization and/or scope from the Organization and Scope lists. To clear filters, select All from the Organization and Scope lists.
- Click X to exit.

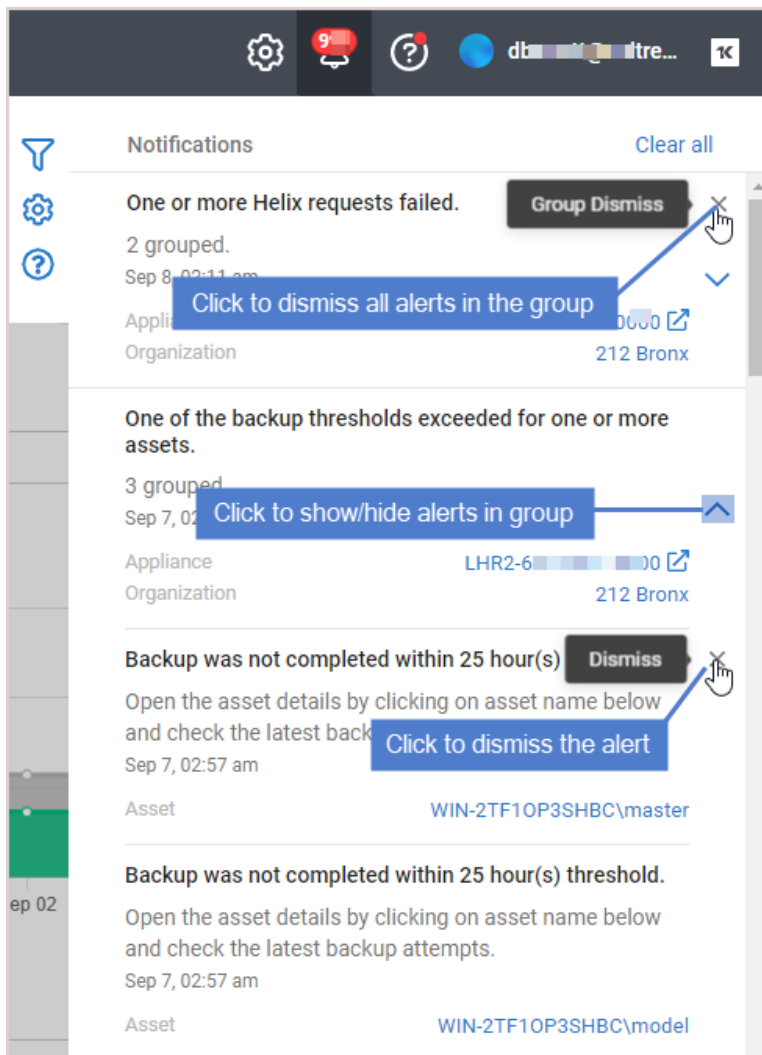


- (Optional) To view group details, click the down arrow to expand the group.

Details display for each alert in the group. Alert details include:

-  icon – Click to view related KB articles.
- Alert message (if available). Example: *In job queue (job #1216)*.
- The date and time the alert was generated.
- Asset – Name of the protected asset (if available). Click to view asset details.
- Alert's X icon – Click to dismiss the alert.

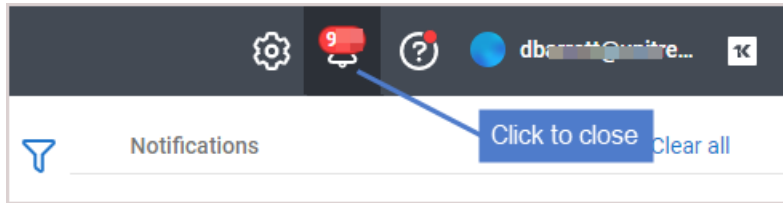
Note: The group's X icon displays above the alerts list. Clicking this icon dismisses all alerts in the group. For details, see "To dismiss a group of alerts".



The screenshot displays the Notifications section of the UniView Portal. It shows three alert groups:

- Alert 1:** "One or more Helix requests failed." (2 grouped, Sep 8, 02:11 am). It features a "Group Dismiss" button and an X icon. A callout points to the X icon with the text "Click to dismiss all alerts in the group".
- Alert 2:** "One of the backup thresholds exceeded for one or more assets." (3 grouped, Sep 7, 02:57 am). It features a collapse icon. A callout points to the collapse icon with the text "Click to show/hide alerts in group".
- Alert 3:** "Backup was not completed within 25 hour(s)" (Asset: WIN-2TF10P3SHBC\master). It features a "Dismiss" button and an X icon. A callout points to the X icon with the text "Click to dismiss the alert".

- 7 Click the BackupIQ icon to close the alerts list.

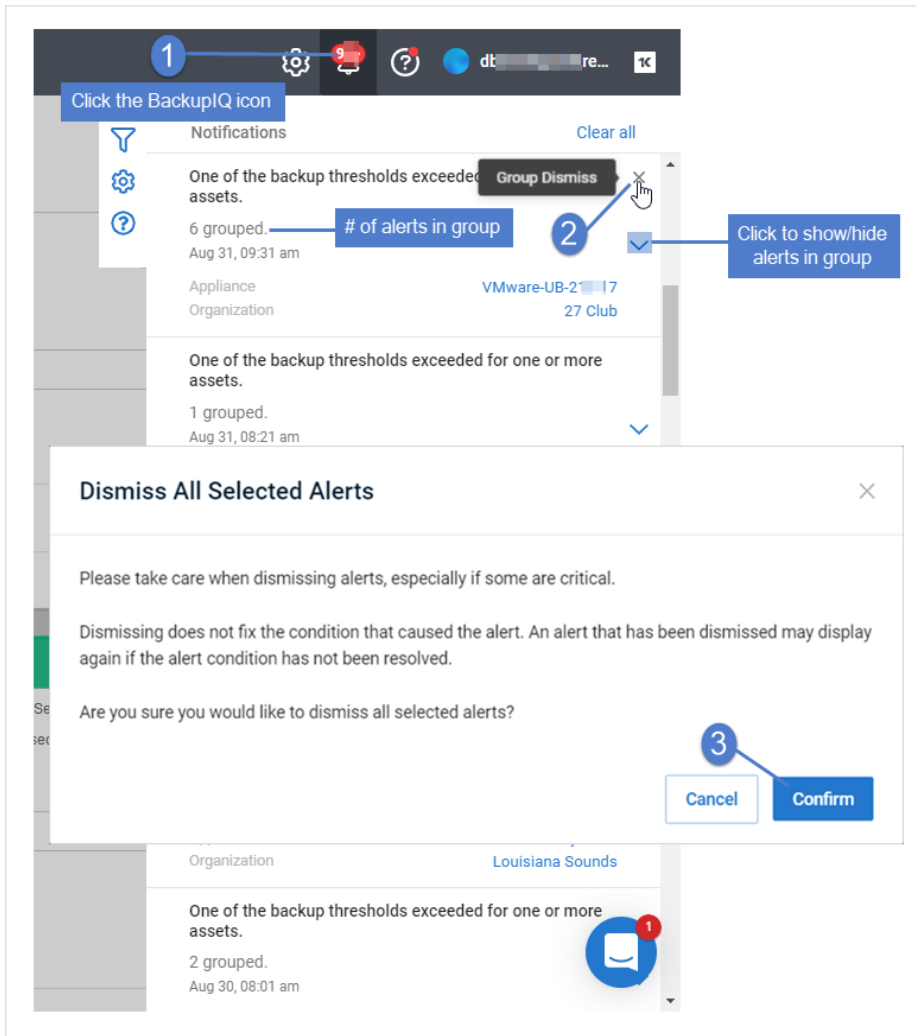


To dismiss a group of alerts

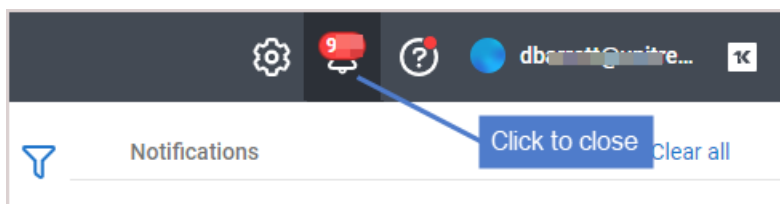
Use this procedure to dismiss a group of alerts. (To dismiss a single alert, click its **x** icon as described above in ["To view BackupIQ alerts"](#).)

- 1 Log in to the UniView Portal with an account that has the Superuser or Admin role.
- 2 Click the BackupIQ icon in the upper-right corner. Alerts display.
- 3 Locate the group in the list and click its X icon. Click **Confirm**.

Note: Clearing an alert does not resolve the alert condition. If the alert condition still exists, a subsequent alert will be generated.



- 4 Click the BackupIQ icon to close the alerts list.

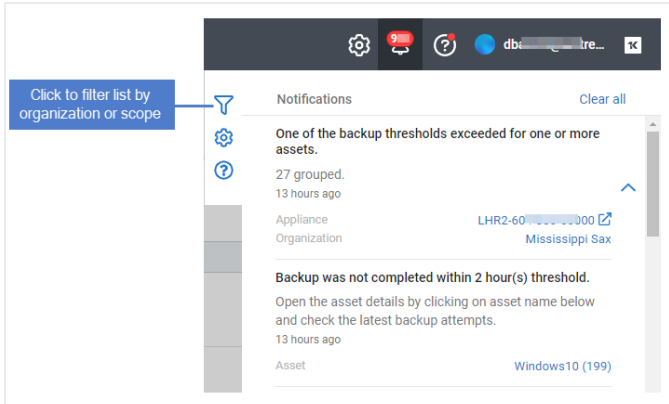


To dismiss BackupIQ alerts in bulk by organization or scope

Use this procedure to select and dismiss multiple alerts by organization and/or scope.

- 1 Log in to the UniView Portal with an account that has the Superuser role.
- 2 Click the BackupIQ icon in the upper-right corner.

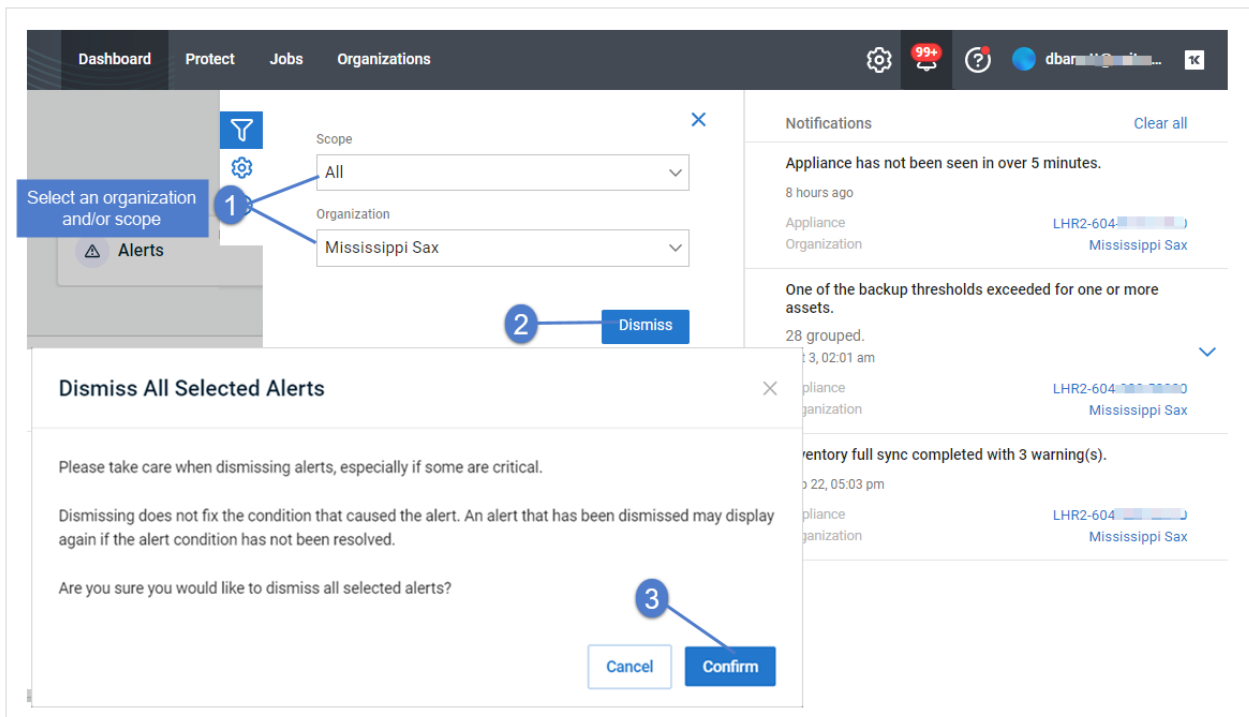
3 Click .



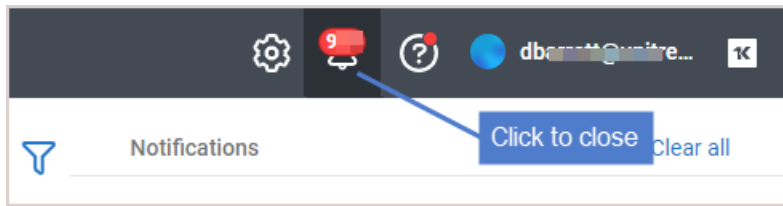
4 Select an organization from the Organization list and/or a scope from the Scope list.

5 Click **Dismiss**. Click **Confirm**.

Note: Clearing an alert does not resolve the alert condition. If the alert condition still exists, a subsequent alert will be generated.



6 Click the BackupIQ icon to close the alerts list.

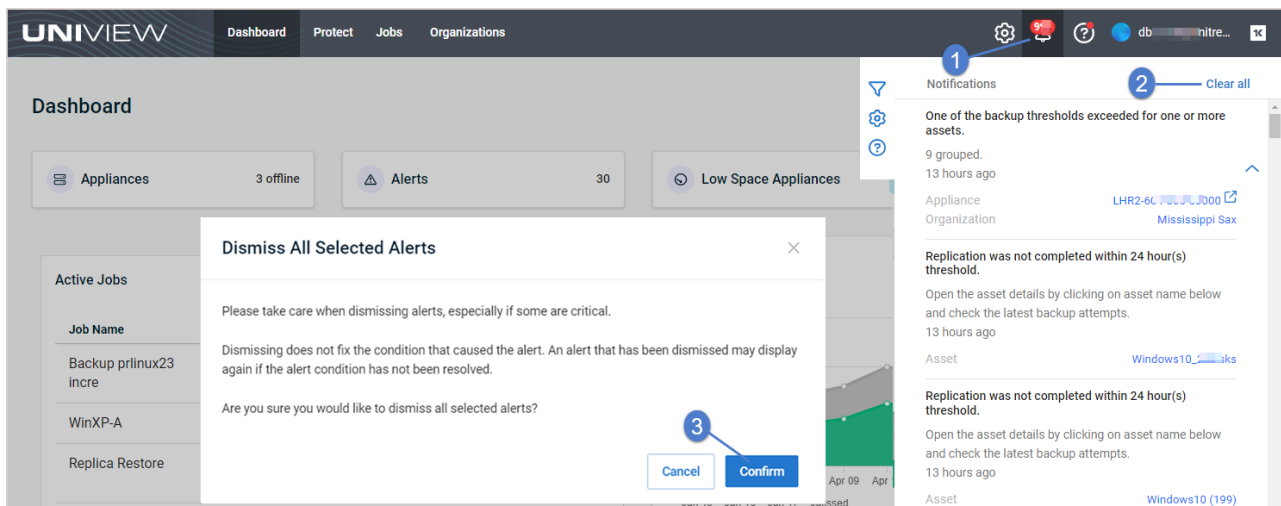


To dismiss all BackupIQ alerts

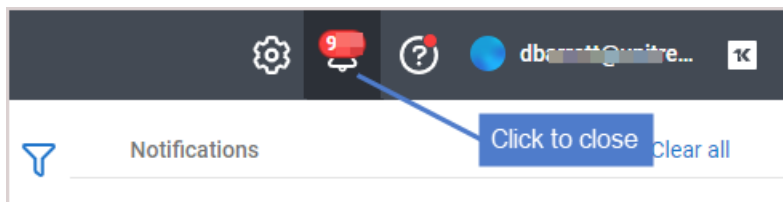
Use this procedure to dismiss all alerts. (To dismiss a single alert, click its X icon as described above in "To view BackupIQ alerts".)

- 1 Log in to the UniView Portal with an account that has the Superuser or Admin role.
- 2 Click the BackupIQ icon in the upper-right corner. Alerts display.
- 3 Click **Clear all**, then **Confirm** to dismiss all alerts.

Note: Clearing an alert does not resolve the alert condition. If the alert condition still exists, a subsequent alert will be generated.



- 4 Click the BackupIQ icon to close the alerts list.

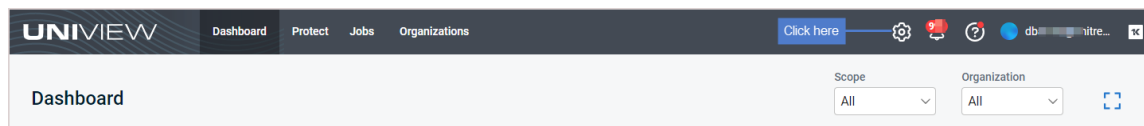


To set up email notification for alerts

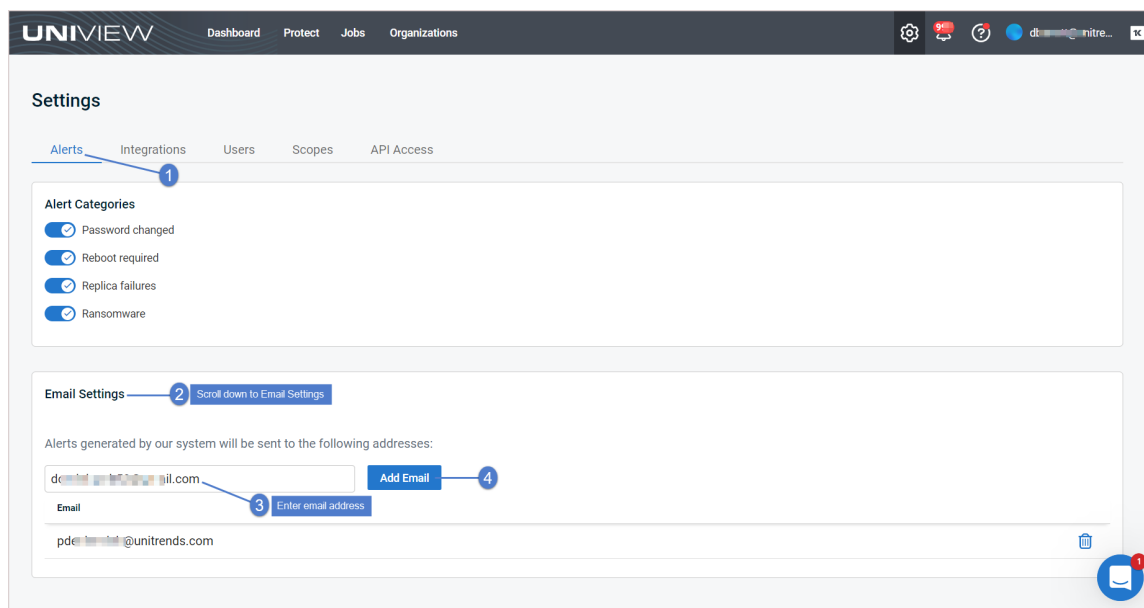
Unresolved alerts display in the BackupIQ alerts list. If you have integrated with a PSA system (BMS, Vorex, Autotask, or ConnectWise), a ticket is also generated in your PSA. Additionally, you may opt to receive email notifications for these

alerts. Use these steps to set up email notification:

- 1 Click :



- 2 On the Settings page, select the **Alerts** view.
- 3 Scroll down to Email Settings. Enter the email address and click **Add Email**. Repeat to add another address.







Upon adding one or more email addresses, alerts are emailed to the specified addresses.

Once the alert condition has been resolved, UniView Portal automatically removes the alert from BackupIQ and emails notification that the alert has been dismissed.

Sample offline and online email alerts:

BackupIQ: Conditional Alarm - Appliance recovery-9010 is offline

 No Reply <no-reply@backup.net>
To:  No Reply

[Reply](#) [Reply All](#) [Forward](#)  

UniView Portal - Alert

Appliance has not been seen in over 60 minutes.

See details below:

Alert Date: 03/10/2022 10:28 AM GMT
Organization: 212 Queens
Appliance Name: recovery-9010



[View in UniView Portal](#)



UNIVIEW

UniView
200 Summit Drive, Suite 200
Burlington MA 01803, USA

Sales: 866-359-5411
Support: 877-282-8857
UK: +44 800 048 8847
NZ: 64800995028

Re: BackupIQ: Conditional Alarm - Appliance recovery-9010 is offline

 No Reply <no-reply@backup.net>
To:  No Reply

[Reply](#) [Reply All](#) [Forward](#)  

UniView Portal - Alert

Appliance recovery-9010 is online.

[View in UniView Portal](#)

UNIVIEW

UniView
200 Summit Drive, Suite 200
Burlington MA 01803, USA

Sales: 866-359-5411
Support: 877-282-8857
UK: +44 800 048 8847
NZ: 64800995028

Conditional alarms

Use this feature to set a threshold for how long a machine can go without a good backup or good hot backup copy. If the threshold is exceeded, an alarm is generated and added to the Alerts list in BackupIQ.

To start using conditional alarms, set up thresholds as described in ["To configure conditional alarms"](#). Once you have configured this feature, alarms are added to BackupIQ. (See ["To view BackupIQ alerts"](#) to view these alarms). BackupIQ conditional alarms also generate tickets for Autotask, ConnectWise Manage, BMS, and Vorex integrations. For an overview of the conditional alarms feature, watch the [Unitrends - Conditional Alarms video](#).

You can also opt to receive email notifications for these alarms. To receive email notifications, run the ["To set up email notification for alerts"](#) procedure.

If you use Kaseya VSA 9, you can opt to add conditional alarms to your VSA (so you can view them along with your other VSA notifications) and set up VSA email alerts for these conditional alarms:

- After you've done the ["To configure conditional alarms"](#) procedure, see ["To display conditional alarms in the Kaseya VSA 9 Remote Monitoring and Management Solution"](#) to add these alarms to your VSA and ["To add VSA 9 email alerts for conditional alarms"](#).
- To manage VSA email alerts for conditional alarms, see ["To view or edit VSA 9 email alerts for conditional alarms"](#) or ["To remove VSA 9 email alerts from conditional alarms"](#).

Note: Alerts and conditional alarms are not yet supported for VSA 10 environments.

Working with conditional alarms

Use these procedures to configure and manage conditional alarms:

- ["To configure conditional alarms"](#)
- ["To view or modify conditional alarm settings"](#)
- ["To delete a custom threshold"](#)
- ["To display conditional alarms in the Kaseya VSA 9 Remote Monitoring and Management Solution"](#)
- ["To add VSA 9 email alerts for conditional alarms"](#)
- ["To view or edit VSA 9 email alerts for conditional alarms"](#)
- ["To remove VSA 9 email alerts from conditional alarms"](#)

To configure conditional alarms


Use this procedure to set alert thresholds against the last good backup and last good hot backup copy (formerly known as *replicated backup*). A good backup or hot backup copy is one that finished with status *success* or *warning*. When a threshold is crossed, an alert is added to BackupIQ, enabling you to quickly prioritize and address alarm conditions:

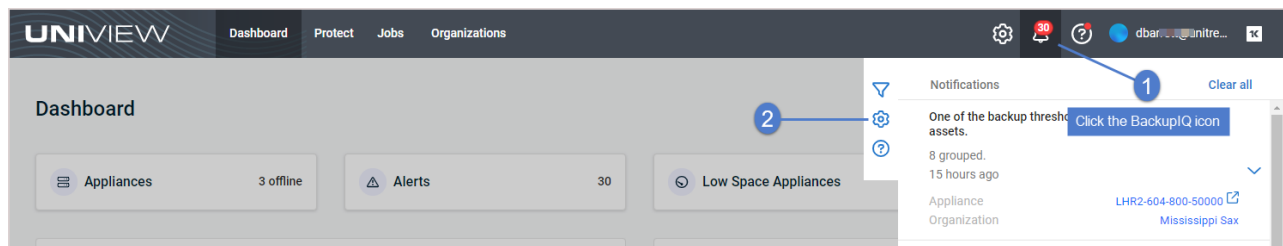
Notes:

- You must be logged in to UniView Portal as a superuser to create or modify conditional alarms.

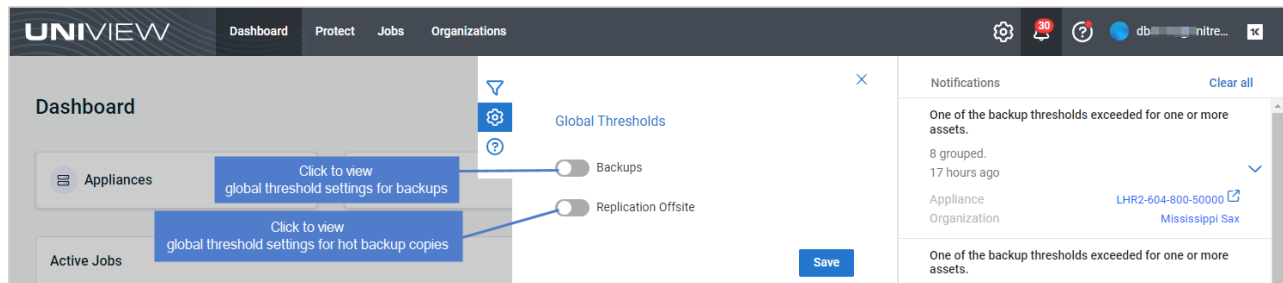
- You can also send conditional alarms to your VSA 9 environment. After configuring alarms in the UniView Portal, continue to "[To display conditional alarms in the Kaseya VSA 9 Remote Monitoring and Management Solution](#)".
- Global Thresholds (required) – Start by setting global thresholds for backups and/or hot backup copies. The global threshold settings you configure are applied to assets that are protected by a Unitrends backup schedule and do not have a custom threshold assigned. Global thresholds are applied across all organizations.
- Custom Thresholds (optional) – Create custom thresholds that you can quickly apply to one or more organizations. Custom thresholds take precedence over global thresholds.

Use these steps to configure conditional alarms:

- Click the BackupIQ icon in the upper-right corner.
- Click the  icon.

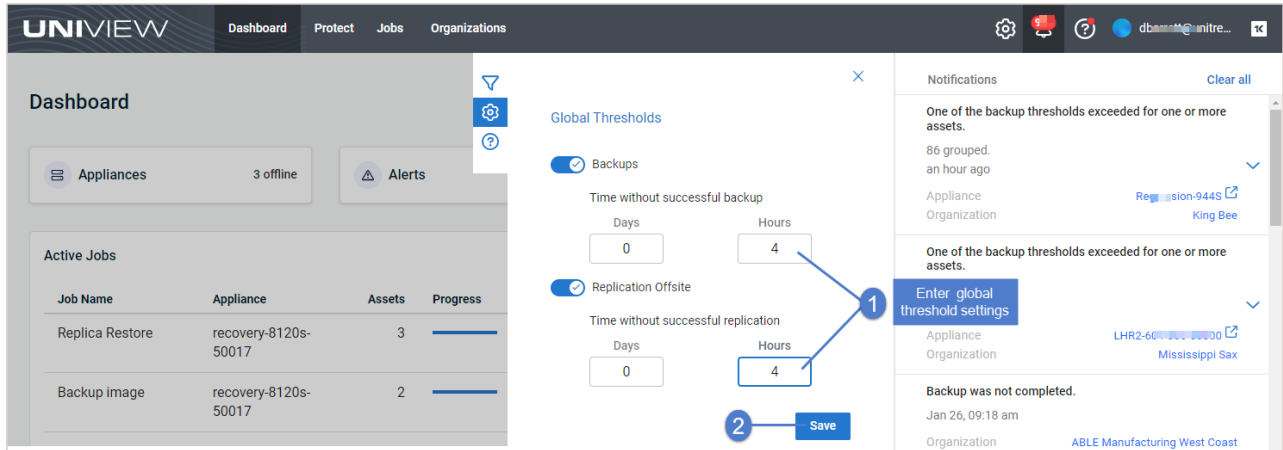


- Click to view global threshold settings for backups (Backups toggle) and hot backup copies (Replication Offsite toggle).



- (Required) Enter global threshold settings and click **Save**.

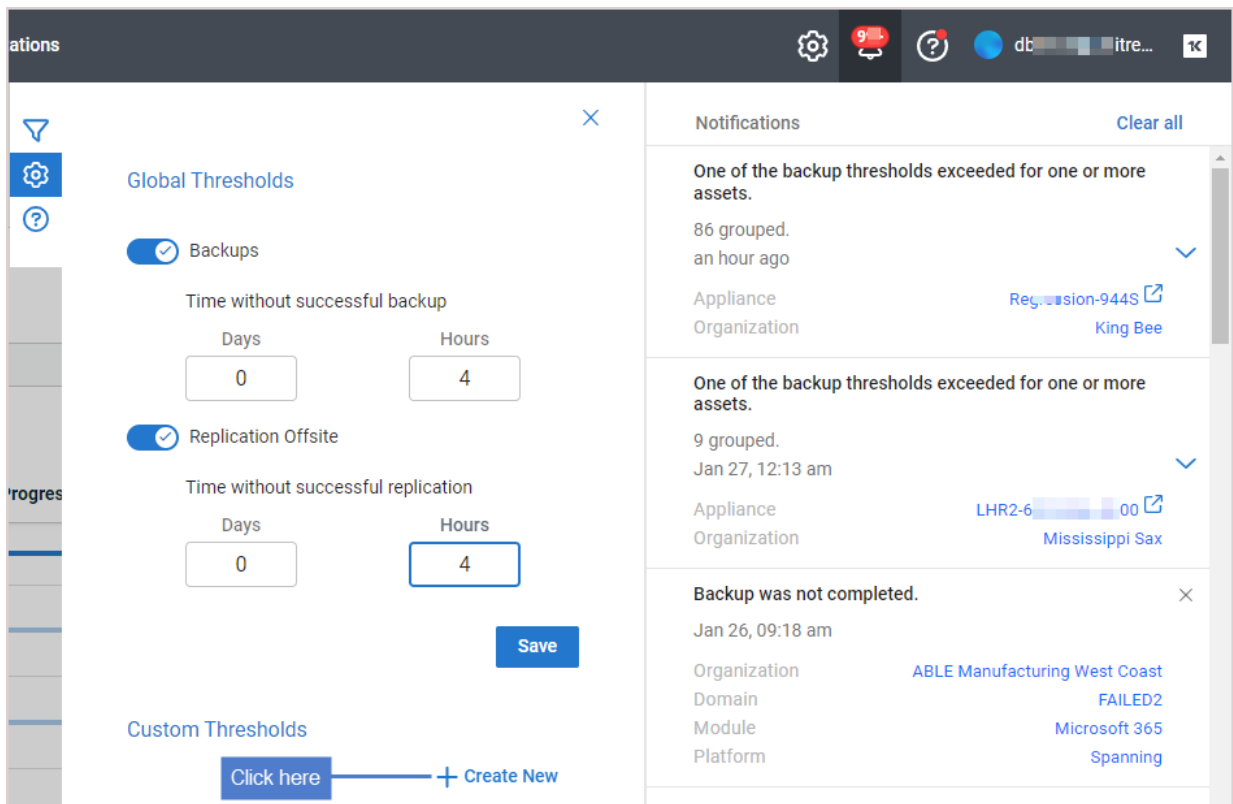
In this 4-hour example, a backup alarm is generated if a good backup does not complete within 4 hours of the job's scheduled start time. A hot backup copy alarm is generated if a good backup is not copied within 4 hours of the backup job's end time.



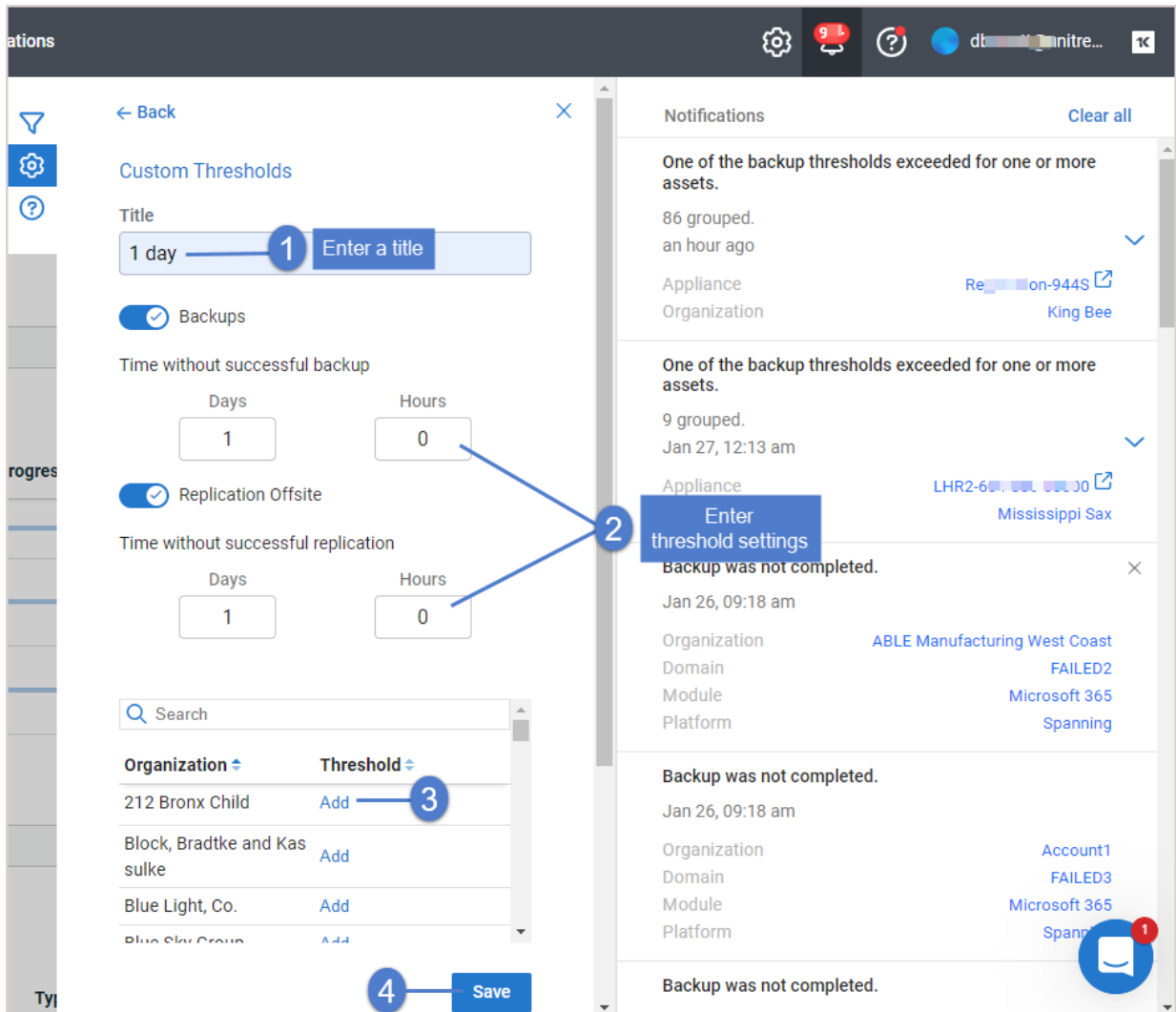
5 (Optional) Add a custom threshold and apply to organizations:

Note: Each organization can be assigned one custom threshold.

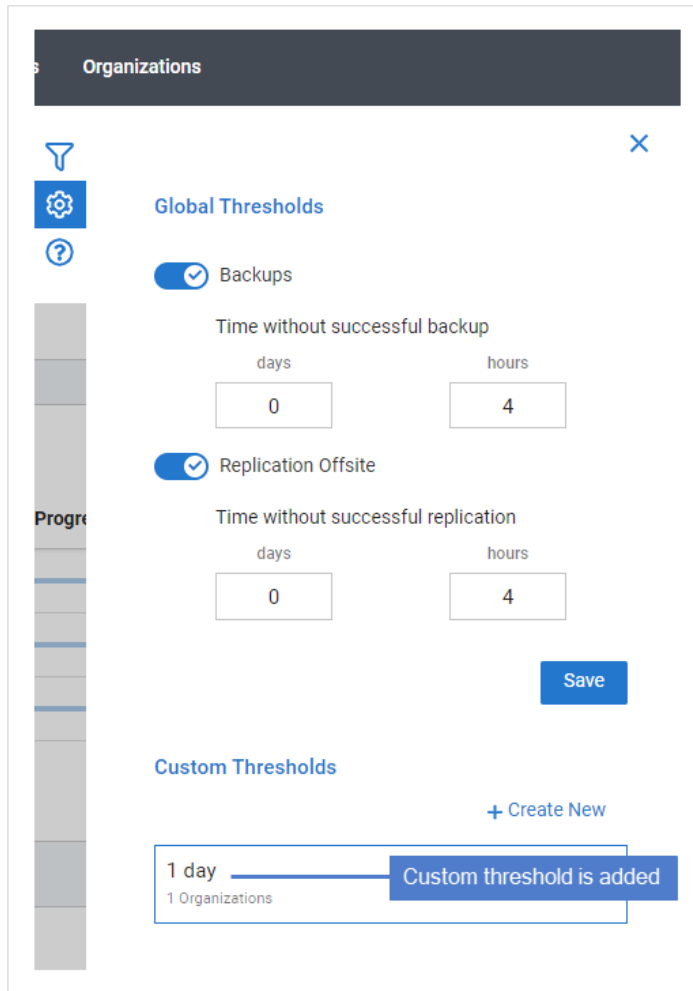
- Click **Create New**:



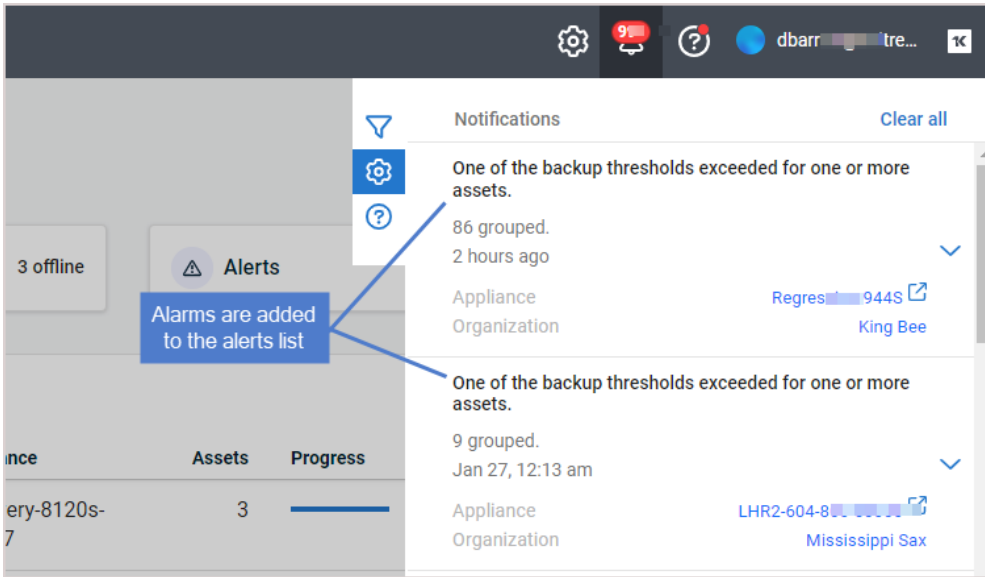
- Enter a title and threshold settings. Add one or more organizations. Click **Save**:



- The custom threshold is added:

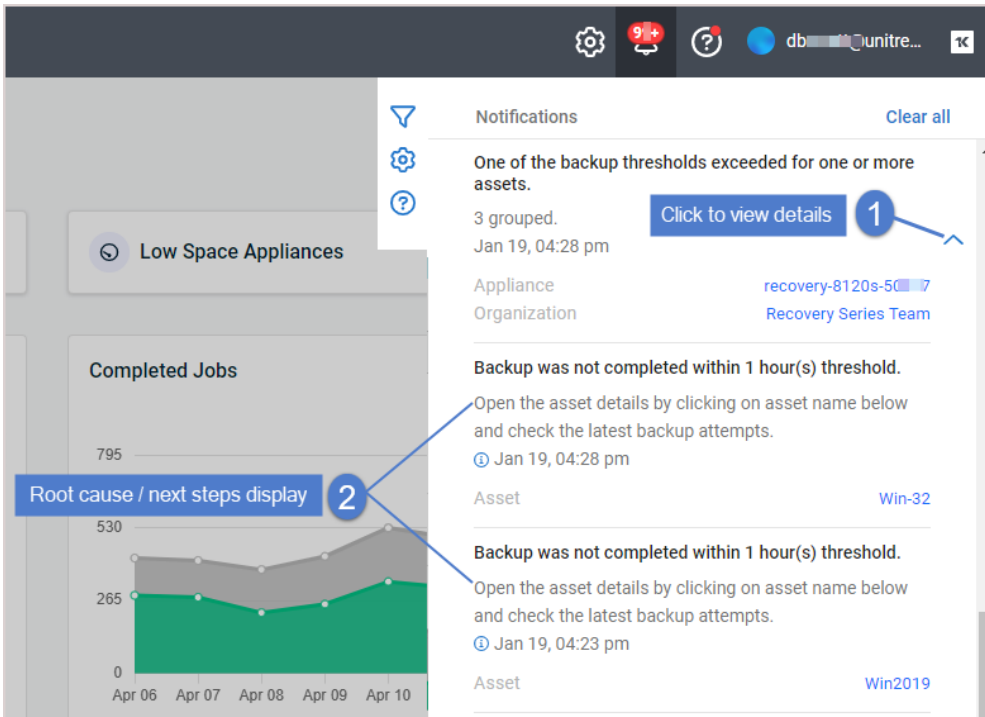


When alarms are generated, they are added to the alerts list in BackupIQ, as shown here:



View alarm details to determine root cause and next steps. These conditions are checked: appliance status, last good backup, backup job schedule, last good hot backup copy, and hot backup copy schedule. If there is an issue, an alert is generated.


Alarm details in BackupIQ Alerts list:

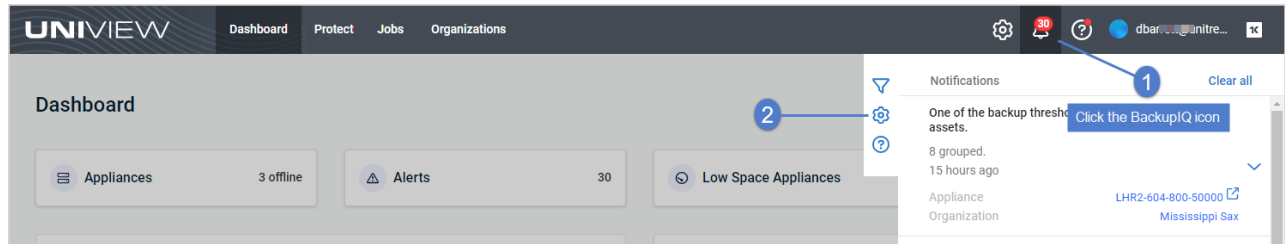


To view or modify conditional alarm settings

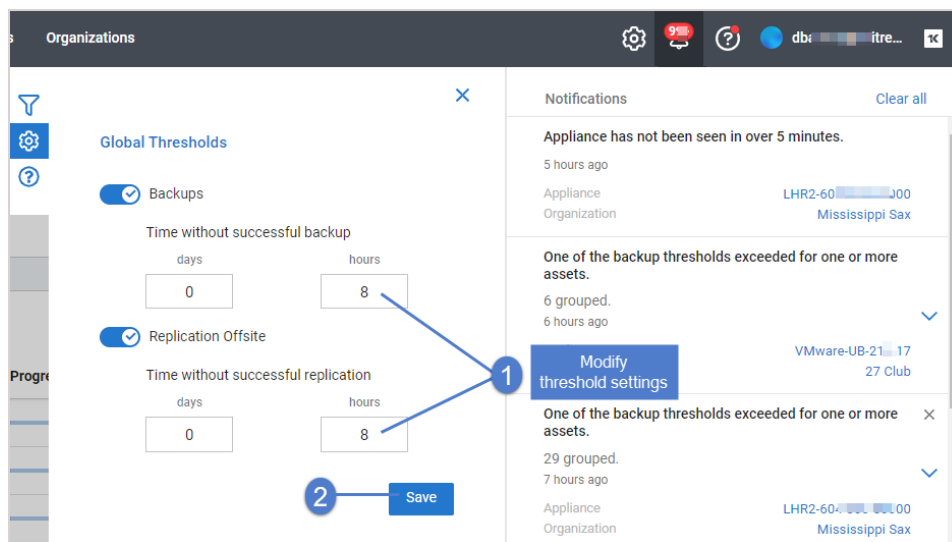
Use these steps to view or modify conditional alarms:

Note: You must be logged in to UniView Portal as a superuser to create or modify conditional alarms.

- 1 Click the BackupIQ icon in the upper-right corner.
- 2 Click the  icon.



- 3 (Optional) Modify global threshold settings and click **Save**:



- 4 (Optional) Modify custom threshold settings:
 - Select the custom threshold:

The screenshot shows the 'Organizations' settings page. On the left, under 'Global Thresholds', there are two sections: 'Backups' and 'Replication Offsite'. Each section has a toggle switch (both are checked) and two input fields for 'Time without successful backup/replication' in days and hours. The 'Backups' section has 0 days and 8 hours. The 'Replication Offsite' section has 0 days and 8 hours. A 'Save' button is located below these settings. Below the global thresholds is a 'Custom Thresholds' section with a '+ Create New' button. A callout box highlights a custom threshold of '1 day' for '1 Organizations' with the text 'Select the custom threshold'. On the right, a 'Notifications' panel shows a list of alerts. The first alert is 'Appliance has not been seen in over 5 minutes.' followed by '5 hours ago' and details for 'Appliance LHR2-60-00000000' and 'Organization Mississippi Sax'. The second and third alerts are 'One of the backup thresholds exceeded for one or more assets.' with details for '6 grouped. 6 hours ago' and '29 grouped. 7 hours ago' respectively, including appliance and organization information.


- Modify the title or threshold settings.
- Add or remove organizations.
- Click **Save**.

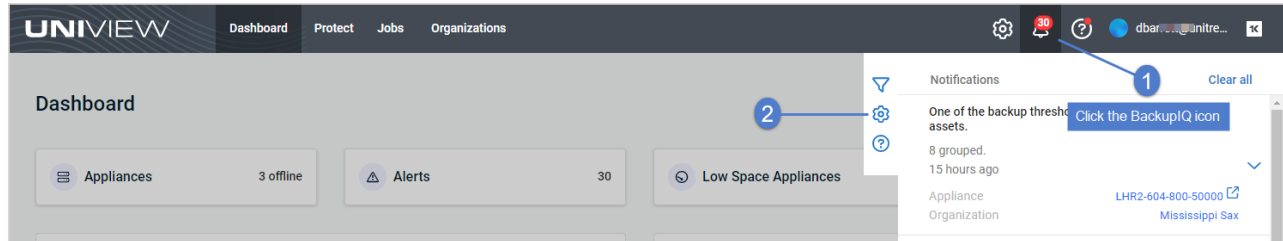
The screenshot shows the 'Organizations' settings page with a 'Modify settings' dialog box open. The dialog has a 'Back' button and a '1 Modify settings' title. It contains the same threshold settings as the previous screenshot. Below the settings is a table of organizations with a search bar. A callout box labeled '2' points to the 'Add' button for '212 Bronx 11'. A 'Delete' button and a '3 Save' button are also visible. The 'Notifications' panel on the right is identical to the previous screenshot.

Organization	Threshold
212 Bronx	Remove
27 Club	Remove
ABLE Manufacturing HQ*	Remove
212 Bronx 11	Add
Account10	Add

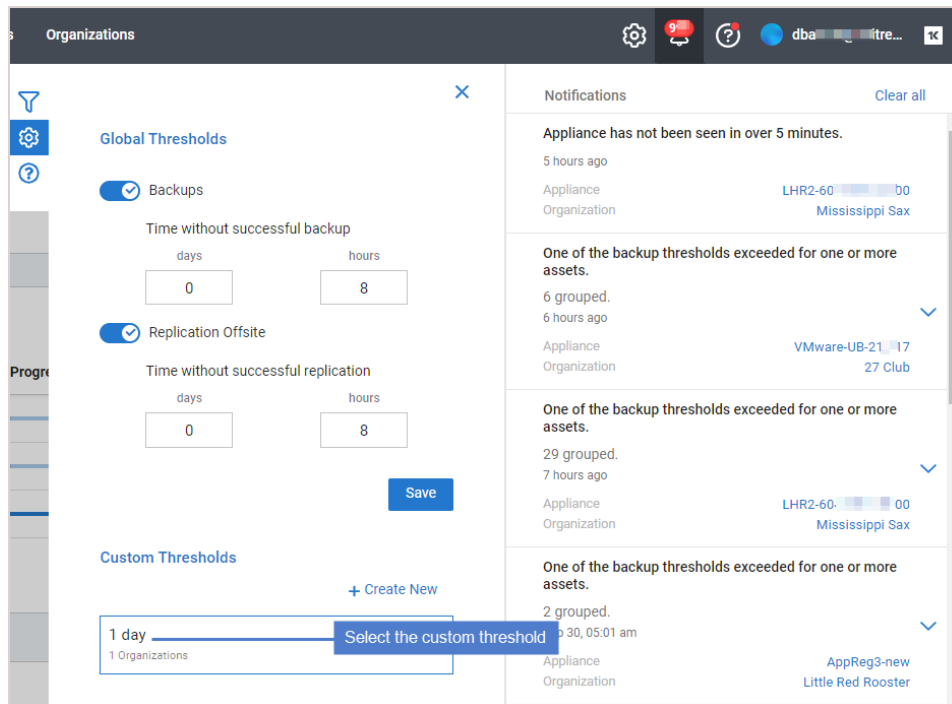
To delete a custom threshold

Note: You must be logged in to UniView Portal as a superuser to delete a custom threshold.

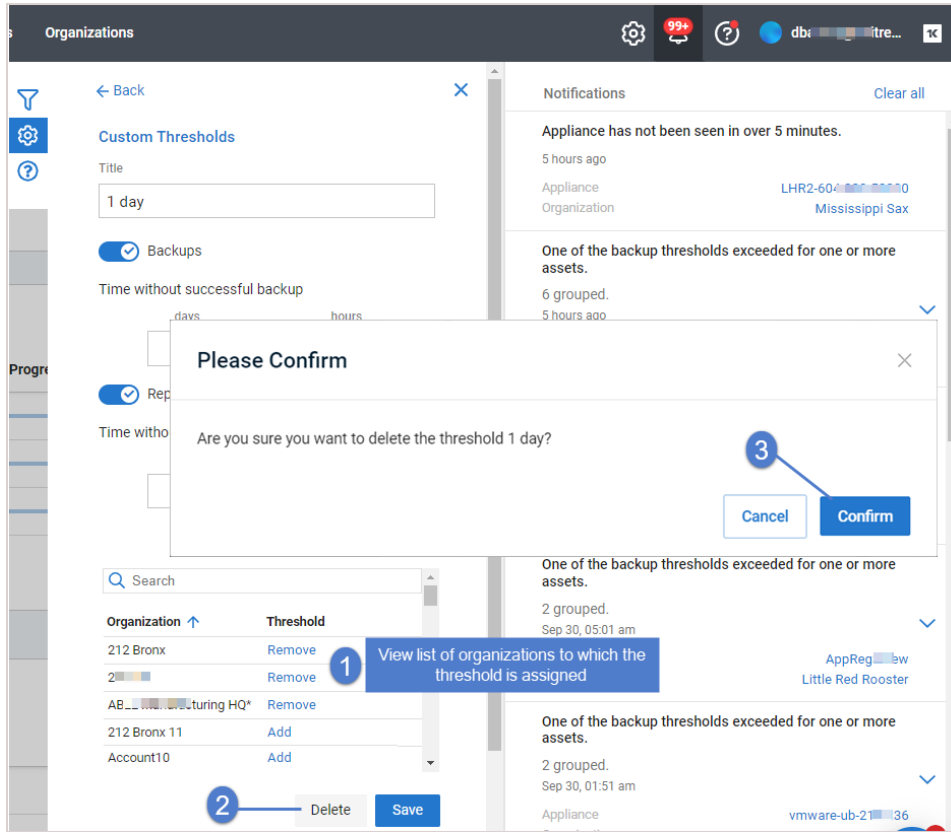
- 1 Click the BackupIQ icon in the upper-right corner.
- 2 Click the  icon.



- 3 Select the custom threshold:

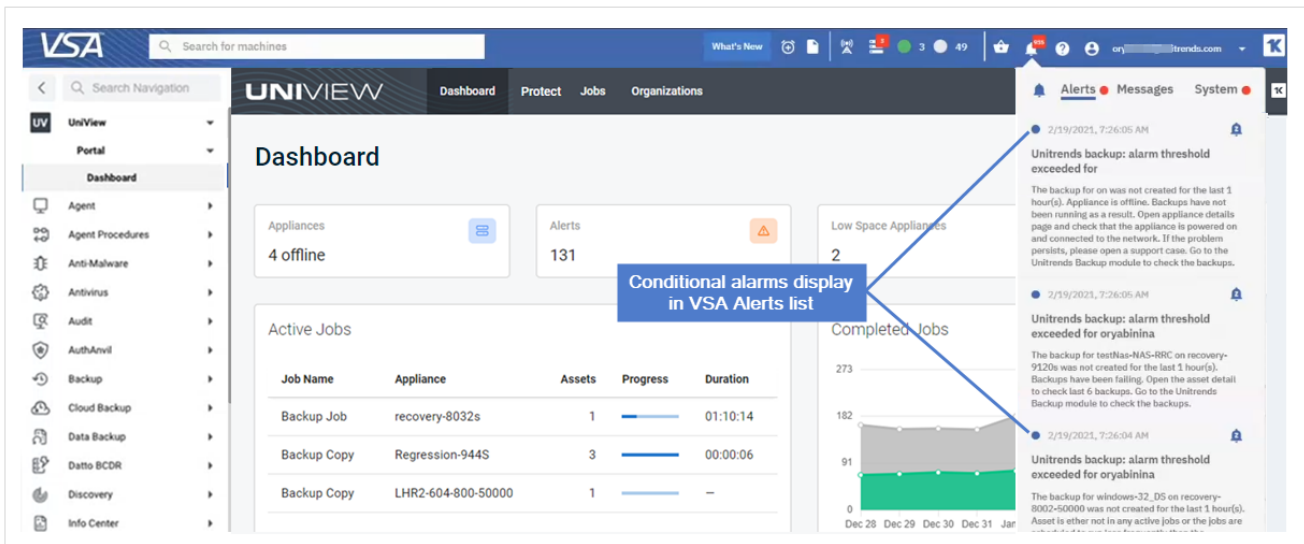


- 4 Review the organizations list. Organizations to which this custom threshold has been assigned display at the top of the list. Upon deleting the custom threshold, global thresholds are applied to any associated organizations.
- 5 Click **Delete**, then **Confirm**. The threshold is removed.



To display conditional alarms in the Kaseya VSA 9 Remote Monitoring and Management Solution

Conditional alarms can be configured to display as system alerts in your VSA 9 environment:



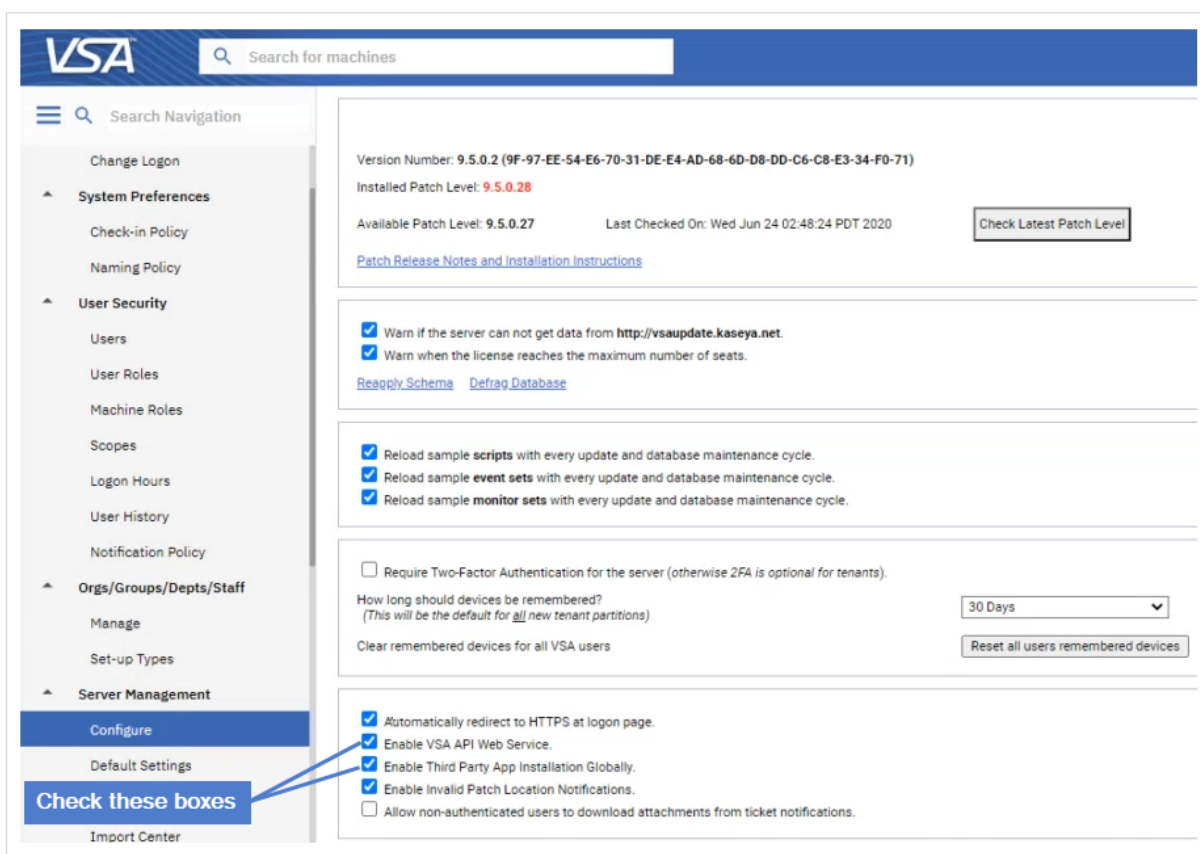
To add conditional alarms to your VSA 9 environment

1 Ensure that these requirements have been met:

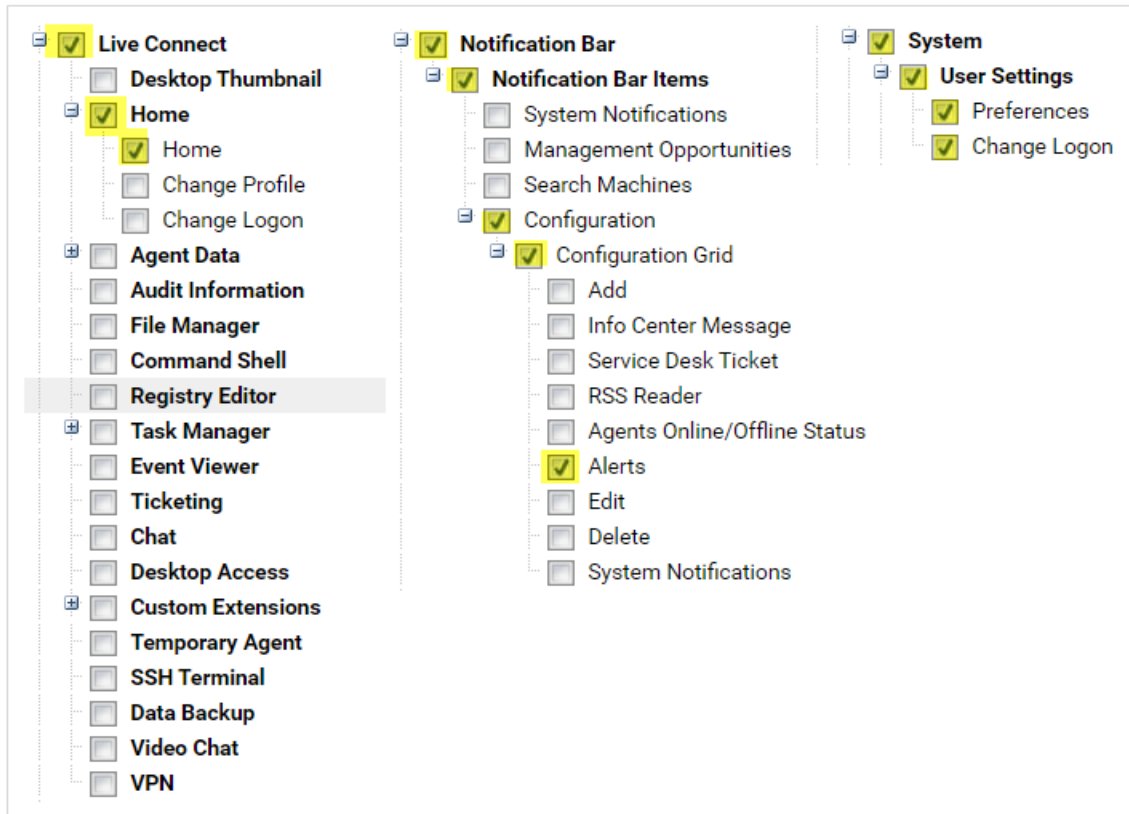
- Conditional alarms have been configured in the UniView Portal (as described in "Conditional alarms").
- VSA 9 is running release 9.5.0.28 or higher.

Note: Alerts and conditional alarms are not yet supported for VSA 10 environments.

- VSA is accessible on the Internet. If you have an on-premise VSA instance that does not have Internet access, UniView Portal cannot send conditional alarms to the VSA.
- These options are enabled in the VSA: Enable VSA API Web Service and Enable Third Party App Installation Globally. These options are located on the **System > Server Management > Configure** page:



- The roles and scopes shown below are enabled. Enable these on the VSA **System > User Security > User Roles** page.



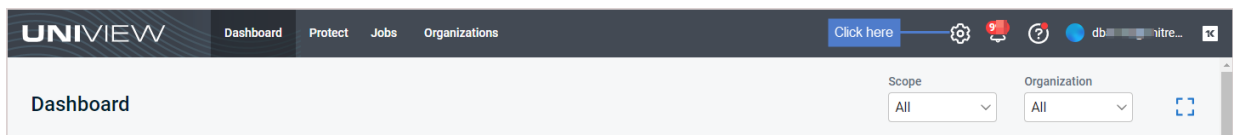
2 Add the VSA integration as described in "Integrating VSA 9".

Notes:

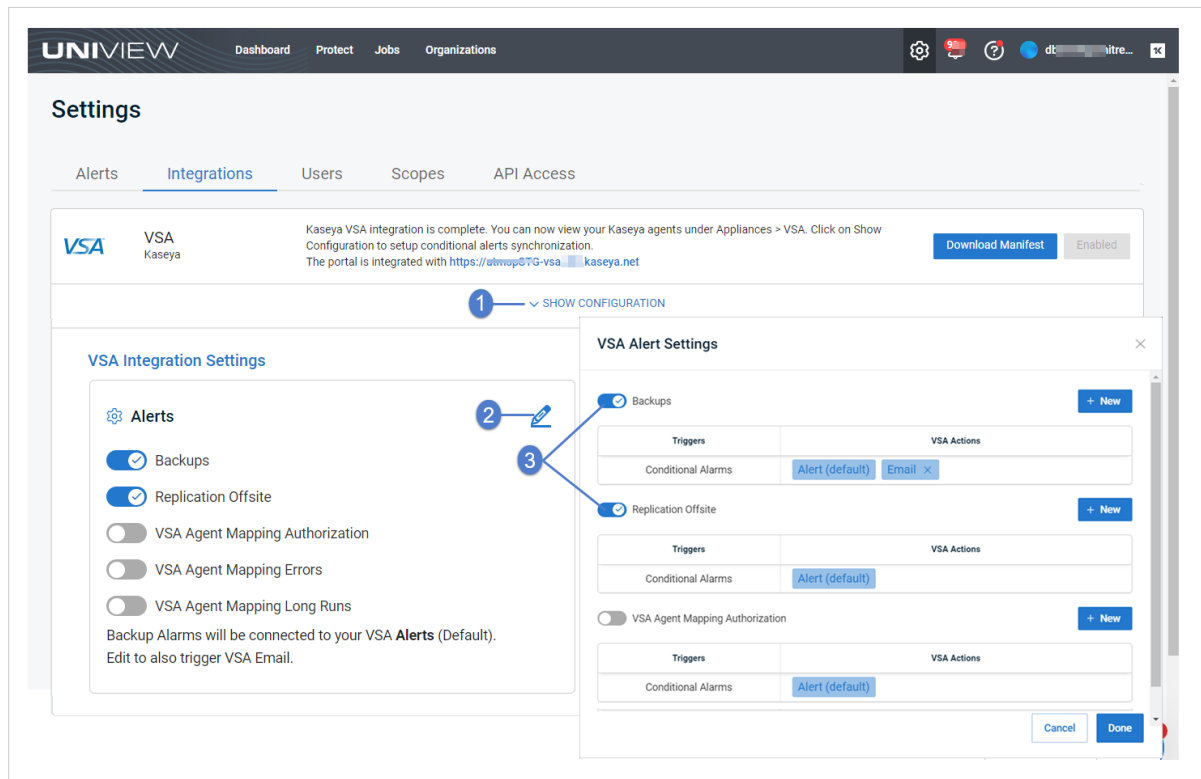
- If you have already integrated an older VSA version, you must remove this integration, then add a new one using the latest TAP module. The "Integrating VSA 9" procedure includes steps to remove the existing integration.
- If the logos and branding you see in your currently deployed VSA module do not look like this new UniView module, you may be using a prior version of the TAP module for the Unitrends Backup Portal platform. As of January 2023, module branding has been modified, but no other functional changes exist. We do not recommend customers uninstall the older module to use the newer module as this will impact existing mappings (e.g., UniView user accounts mapped to KaseyaOne accounts for single sign-on, and assets mapped to VSA IDs).

3 Enable VSA alerts in the UniView Portal:

- In the UniView Portal, click :

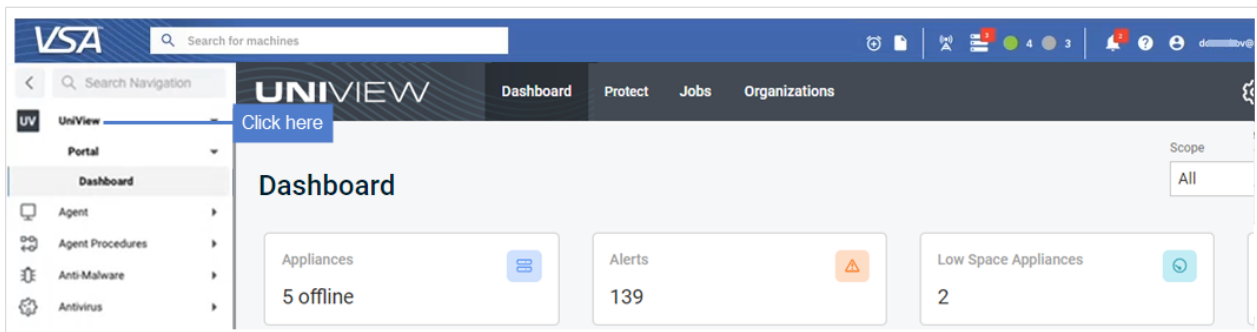


- Select the **Integrations** view.
- Locate the VSA integration and click **Show Configuration**.
- Click the toggles to enable alerts for backups (Backups toggle) and hot backup copies (Replication Offsite toggle).



- To finish the configuration, log in to the VSA and launch the UniView module.

Note: If prompted, enter your UniView Portal credentials and click **Log in**. Click **Allow** to grant UniView Portal access to the VSA instance.



To add VSA 9 email alerts for conditional alarms

Use this procedure to configure VSA email alerts for conditional alarms.

Note: Alerts and conditional alarms are not yet supported for VSA 10 environments.

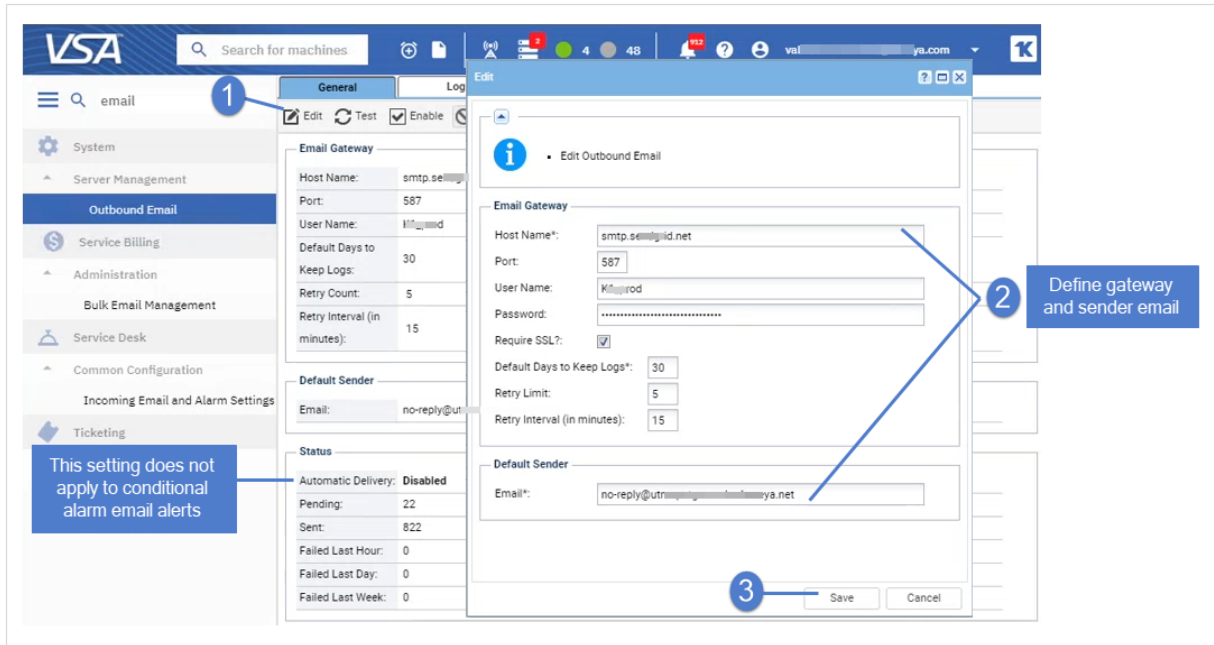
1 Ensure that these prerequisites have been met:

- Conditional alarms have been configured, as described in "[To configure conditional alarms](#)".
- Conditional alarms have been added to the VSA, as described in "[To display conditional alarms in the Kaseya VSA 9 Remote Monitoring and Management Solution](#)".
- (On-premise VSA instance only) An SMTP server has been configured on the VSA **System > Server Management > Outbound Email** page. To configure an SMTP server, click **Edit**, enter settings, then click **Save**. Outbound Email fields include:

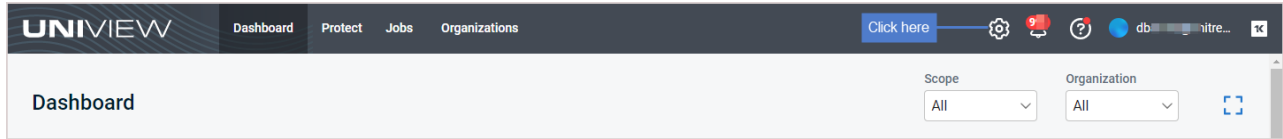
- Host Name - The name of the host email server. Example: *smtp.mycompany.com*. If no authentication or special port number is required, then only specify values for the **Default Days to Keep Logs** and **Default Sender Email** fields.


Note: Enter **localhost** in the Host Name field to use the Kaseya Server's IIS Default SMTP Virtual Server to route outbound email. The Default SMTP Virtual Server service must be installed and running in order to send email. The service must also be able to resolve DNS addresses to route email to other SMTP servers.

- Port - Typically 25, but the host email server may require a different port number. Ports 465 and 587 are typically used for connecting to an SMTP email server over SSL/TLS.
- User Name - If required for authentication, enter the username of an account authorized to use the host email server.
- Password - If required for authentication, enter the password of the account.
- Default Days to Keep Logs - Enter the number of days to keep log outbound email entries.
- Default Sender Email - Enter the default From address displayed by outbound email.



2 In the UniView Portal, click :



- 3 Select the **Integrations** view.
- 4 Locate the VSA integration and click **Show Configuration**.
- 5 Click  to edit VSA integration settings.
- 6 Click **New +** in the Backups area to configure email alerts for backups or click **New +** in the Replication Offsite area to configure email alerts for hot backup copies.

The screenshot shows the UniView Portal Settings page. The top navigation bar includes 'Dashboard', 'Protect', 'Jobs', and 'Organizations'. The main heading is 'Settings', with sub-tabs for 'Alerts', 'Integrations', 'Users', 'Scopes', and 'API Access'. The 'Integrations' tab is active, showing the 'VSA' integration status. A message states: 'Kaseya VSA integration is complete. You can now view your Kaseya agents under Appliances > VSA. Click on Show Configuration to setup conditional alerts synchronization. The portal is integrated with https://ulmosp37g-vsa.kaseya.net'. There are buttons for 'Download Manifest' and 'Enabled'. A 'SHOW CONFIGURATION' button is highlighted with a blue circle and the number '1'. Below this, the 'VSA Integration Settings' panel is visible, with an 'Alerts' section containing several toggle switches: 'Backups' (checked), 'Replication Offsite' (checked), 'VSA Agent Mapping Authorization' (unchecked), 'VSA Agent Mapping Errors' (unchecked), and 'VSA Agent Mapping Long Runs' (unchecked). A blue circle with the number '2' and a pencil icon points to the 'Alerts' section. To the right, the 'VSA Alert Settings' dialog is open, showing three sections for 'Backups', 'Replication Offsite', and 'VSA Agent Mapping Authorization'. Each section has a table with 'Triggers' and 'VSA Actions' columns. The 'Backups' section has a '+ New' button highlighted with a blue circle and the number '3'. A tooltip points to this button with the text: 'Click to configure email alerts for Backups or Replication Offsite'. The dialog also has 'Cancel' and 'Done' buttons at the bottom.

- 7 In the Create New VSA Action dialog, select **Email** from the VSA Action list.
- 8 Enter one or more recipient email addresses.
 - You can enter addresses by typing or by using copy/paste keyboard shortcuts (**Ctrl+C** and **Ctrl+V**).
 - If entering multiple addresses, you must enter a comma or space between each address.
- 9 Click **Confirm**.

Backups: Create New VSA Action [X]

Select an action to configure.

VSA Action

Email [1] Select Email [v]

Recipient

db@unitrends.com X dora@unitrends.com X mlc@unitrends.com X

[2] Enter recipient addresses

[3] [Back] [Confirm]

10 The email alert is added.

Note: VSA Actions are user specific. The email alert that you added displays for your user account only. If another user logs in to the UniView Portal, the VSA Actions that were added by your user account do not display. Because of this, it is possible that another user may create a duplicate VSA action.

VSA Alert Settings

Backups + New

Triggers	VSA Actions
Conditional Alarms	Alert (default) Email × Email alert is added

Replication Offsite + New

Triggers	VSA Actions
Conditional Alarms	Alert (default)

VSA Agent Mapping Authorization + New

Triggers	VSA Actions
Conditional Alarms	Alert (default)

VSA Agent Mapping Errors + New

Triggers	VSA Actions
Conditional Alarms	Alert (default)

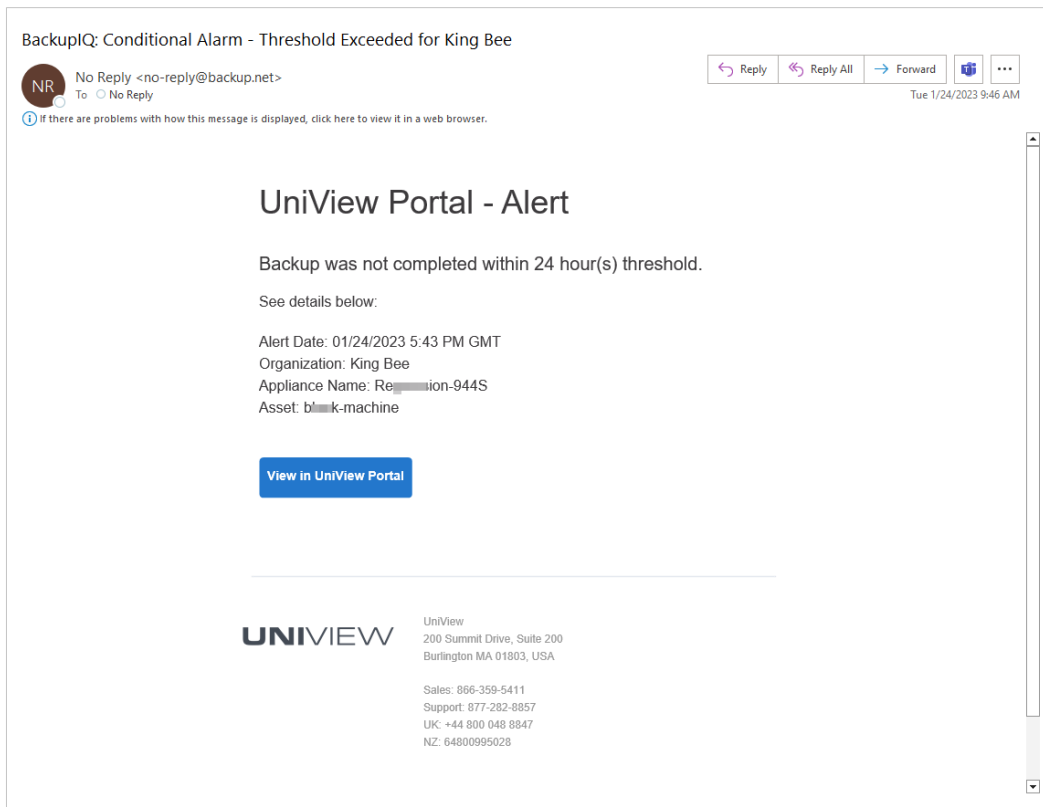
Click to exit

Cancel Done

11 (Optional) Repeat this procedure from [step 6](#) to add email alerts to the other job type.

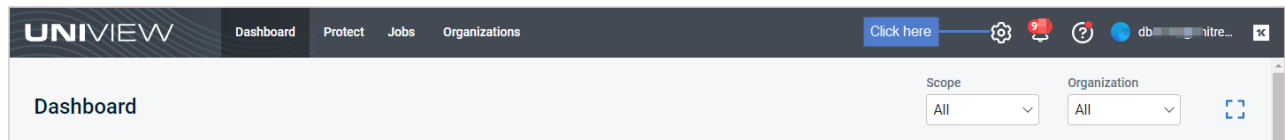
12 Click **Done** to exit.


An email alert is sent if the conditional alarm threshold is reached. Sample conditional alarm email alert:

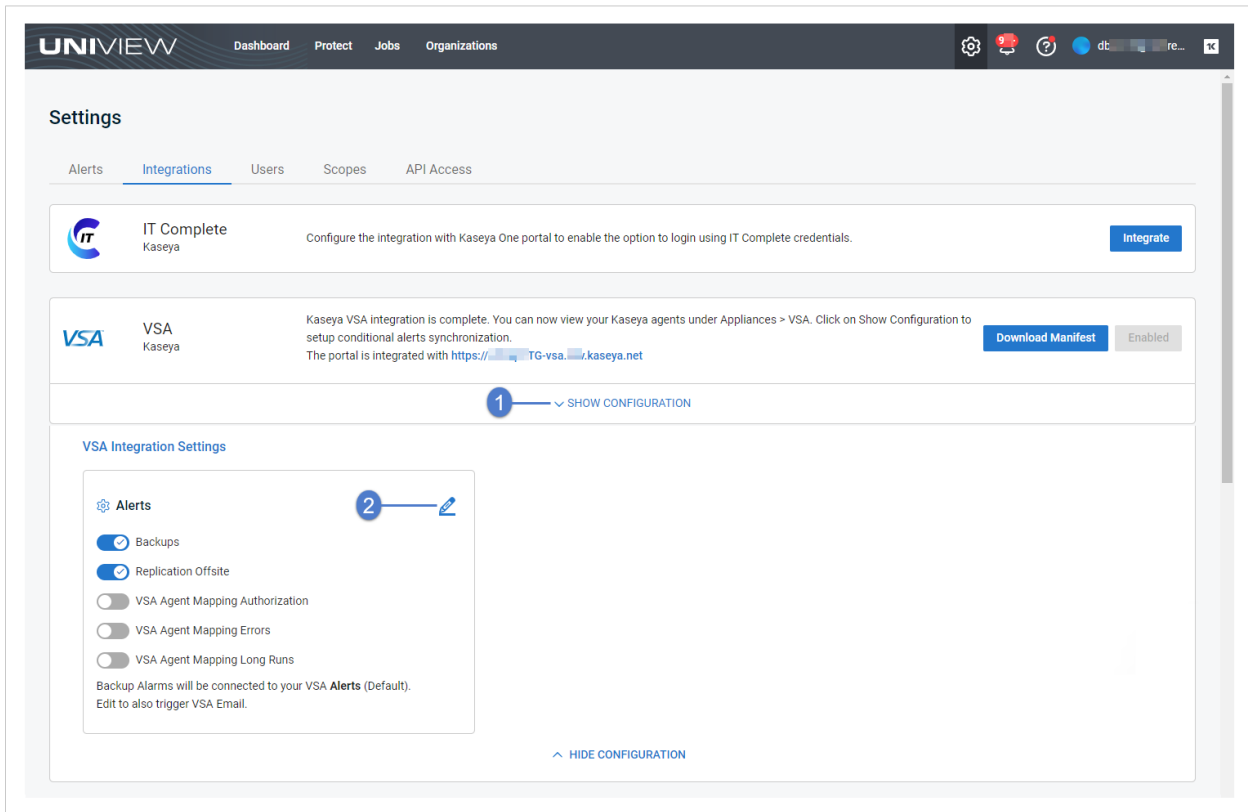


To view or edit VSA 9 email alerts for conditional alarms

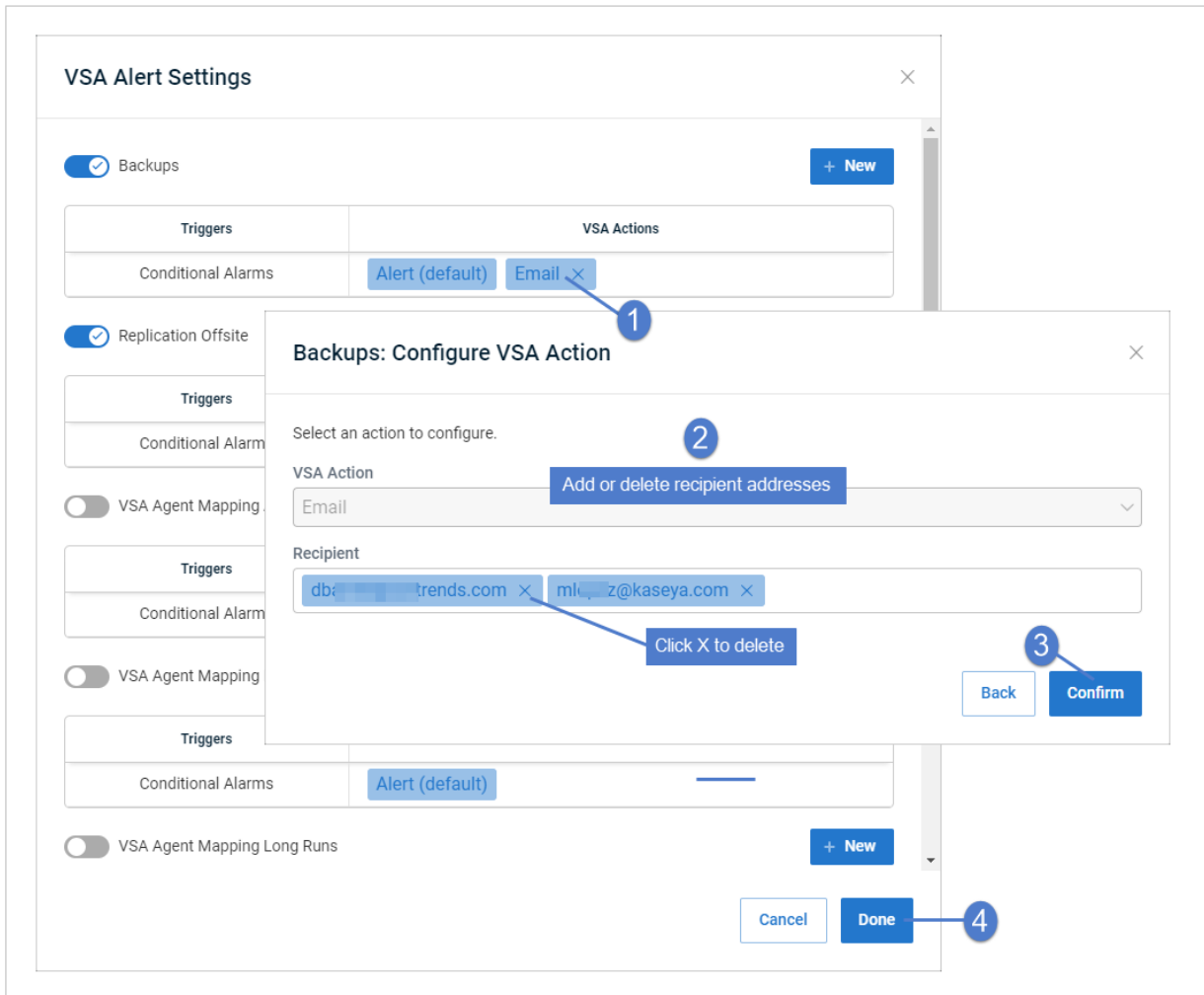
- 1 In the UniView Portal, click :



- 2 Select the **Integrations** view.
- 3 Locate the VSA integration and click **Show Configuration**.
- 4 Click  to view or edit VSA integration settings.

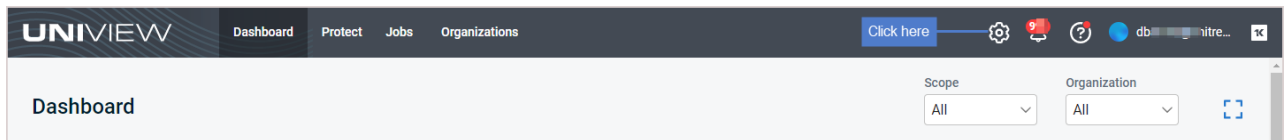



- 5 Click **Email** to view or edit the VSA action.
- 6 (Optional) Add or remove recipient email addresses, then click **Confirm**. Click **Done** to exit.
 - You can enter addresses by typing or by using copy/paste keyboard shortcuts (**Ctrl+C** and **Ctrl+V**).
 - If entering multiple addresses, you must enter a comma or space between each address.
 - To delete an email address, click its **X**.



To remove VSA 9 email alerts from conditional alarms

1 In the UniView Portal, click :



- 2 Select the **Integrations** view.
- 3 Locate the VSA integration and click **Show Configuration**.
- 4 Click  to edit VSA integration settings.

The screenshot displays the UniView Portal Settings page, specifically the Integrations tab. The page shows two integration cards: 'IT Complete' and 'VSA'. The 'VSA' card is expanded, showing 'VSA Integration Settings' with a list of alert types: Backups, Replication Offsite, VSA Agent Mapping Authorization, VSA Agent Mapping Errors, and VSA Agent Mapping Long Runs. A blue circle with the number '2' points to the 'Alerts' section header. A blue circle with the number '1' points to the 'SHOW CONFIGURATION' link above the settings panel. The 'Backups' and 'Replication Offsite' options are checked, while the others are unchecked. A note at the bottom of the settings panel states: 'Backup Alarms will be connected to your VSA Alerts (Default). Edit to also trigger VSA Email.' There is an 'Integrate' button for IT Complete and a 'Download Manifest' button for VSA. The 'Enabled' status is shown for VSA. The top navigation bar includes 'Dashboard', 'Protect', 'Jobs', and 'Organizations'.

- 5 Locate the Email conditional alarm in the Backups area or the Email conditional alarm in the Replication Offsite area for hot backup copies. Click its **X** to remove the email alert. Click **Done** to exit.

The screenshot shows the 'VSA Alert Settings' dialog box. It contains five sections, each with a toggle switch and a '+ New' button. Each section has a table with 'Triggers' and 'VSA Actions' columns. The 'Backups' and 'Replication Offsite' sections are currently active. A callout box with a blue background and white text, labeled with a circled '1', points to the 'Email' button with an 'X' icon in the 'VSA Actions' column of the 'Replication Offsite' section. The callout text reads: 'Click an X to remove email alerts from Backups or Replication Offsite (for hot backup copies)'. At the bottom of the dialog are 'Cancel' and 'Done' buttons.

Triggers	VSA Actions
Conditional Alarms	Alert (default) Email X

Triggers	VSA Actions
Conditional Alarms	Alert (default) Email X

Triggers	VSA Actions
Conditional Alarms	Alert (default)

Triggers	VSA Actions
Conditional Alarms	Alert (default)

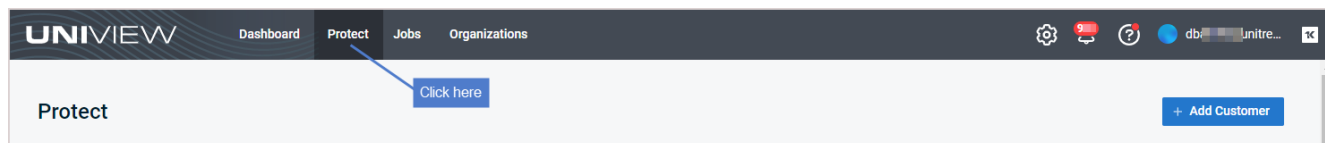
Triggers	VSA Actions
Conditional Alarms	Alert (default)

This page is intentionally left blank.



Working with Unitrends Appliances, Assets, and Backups

Use the Protect page to manage your Unitrends appliances, assets, and backups. To access the Protect page, click **Protect**:



The page contains these Unitrends views:

- Appliances (default view) – Use to:
 - View summary and status information by Unitrends appliance
 - Add appliances to the UniView Portal
 - Connect to appliances from the UniView Portal
 - Add assets to an appliance
 - Remove assets from an appliance
- Assets – Use to:
 - View status information about the assets protected by your Unitrends appliances
 - Remove assets from appliances
 - Manage backup policies for Windows image-level assets and VMware virtual machines

See these topics for details:

- ["Working with appliances"](#)
- ["Viewing assets"](#)
- ["Removing assets" on page 132](#)
- ["Working with backup policies"](#)

Working with appliances

Use the Appliances view to manage, add, and connect to appliances. See these procedures for details:

- ["Viewing appliances"](#)
- ["Filtering the Appliances view"](#)
- ["Viewing appliance details"](#)



- ["Adding assets to an appliance"](#)
- ["Removing assets from an appliance" on page 111](#)
- ["Blocking or unblocking local access to an appliance"](#)
- ["Connecting to an appliance"](#)
- ["Modifying Helix Auto Update settings"](#)
- ["Adding an appliance"](#)
- ["Deleting an appliance"](#)

Viewing appliances

The Appliances view displays all Unitrends appliances that have been added to your backup.net instance. (To filter the display, see ["Filtering the Appliances view"](#).)

The following information is given for each appliance:

Note: Appliance information is updated hourly.

- + New – Click to add an appliance. For details, see ["Adding an appliance"](#).
- Filters – Enter criteria in these fields to filter the list of appliances that display. For details, see ["Filtering the Appliances view"](#).
- Select checkbox – Check boxes to modify selected appliance's Helix settings. For details, see ["Modifying Helix Auto Update settings"](#).
- Alerts icon – Indicates whether the appliance has unresolved alerts: green for no alerts, yellow for warnings, red for critical.
- Lock icon – Indicates whether local access to the appliance has been blocked:  for blocked,  for unblocked. Once local access has been blocked, users can no longer log in directly to the appliance UI. Instead, users must connect to the appliance from UniView (as described in ["Connecting to an appliance"](#)). For more on this feature, see ["Blocking or unblocking local access to an appliance"](#).
- Name and asset tag – The appliance name and asset tag.
- Manage – Click to connect to the appliance. (The Manage button does not display for offline appliances.) For appliance procedures, see the [Administrator Guide for Recovery Series and Unitrends Backup](#).
- Last Seen – Indicates whether the appliance is online or offline. *Just Now* indicates the appliance is online. If the appliance is offline, shows the number of hours, days, months, or years since the appliance was last seen.
- Model – Appliance model. *VM* for Unitrends Backup virtual appliances. Model number for Unitrends physical appliances.
- Organization – Appliance's organization.
- Free Space – Shows the amount of free space on the appliance, in terabytes (TB) or gigabytes (GB), and as a percent of total space.

- Alerts – Number of unresolved alerts on the appliance. To address alerts, see "[Working with Alerts and Conditional Alarms](#)".
- Helix Status – Indicates whether the following have been enabled on the appliance: Helix and Helix auto updates. *On* for enabled, *Off* for disabled, or *!* for Helix status unavailable.
- Version – Unitrends version running on the appliance.

If the appliance is not running the latest release, the version number displays in yellow indicating that an update is available. Click **Manage** to log in to the appliance and install the latest Unitrends software version.
- Protected Assets – Click to view protected assets (assets that are protected by a backup schedule). Click a row in the Protected Assets table to view asset details. Click **Protected Assets** again to hide the protected assets list.
- Add Asset – Click to add an asset to the appliance. For details, see "[Adding assets to an appliance](#)".
- View Unprotected Assets – Click to see any assets that have been added to the appliance but are not protected by an enabled backup schedule. In the Unprotected Assets dialog, you can:
 - Quickly view and apply backup policies to Windows image-level assets and VMware VMs.
 - Remove selected assets from the appliance. For details, see "[Removing assets from an appliance](#)".

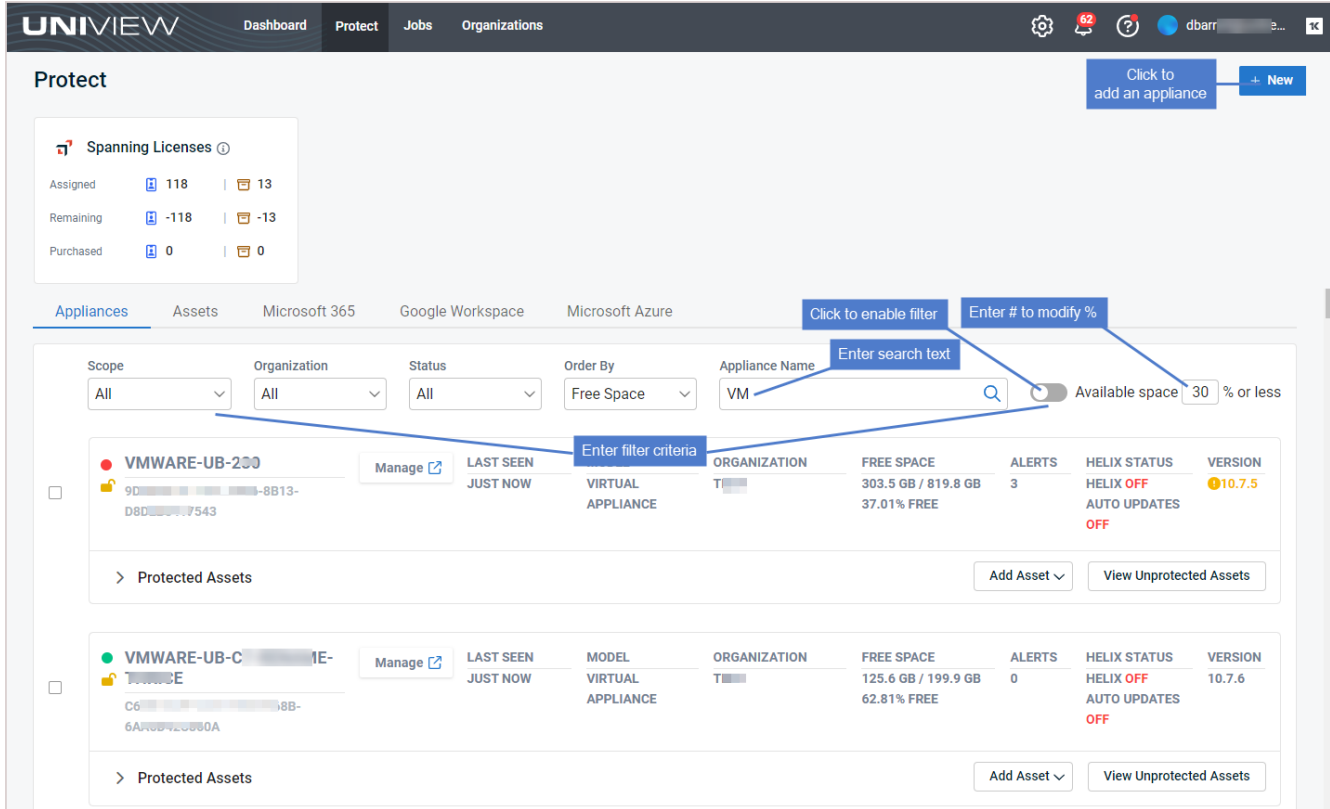
Filtering the Appliances view

The Appliances view displays all appliances that have been added to your backup.net instance.

To filter the display, enter filter criteria in any of the following:

- Scope – Select a scope from the list. (Select **All** to clear the scope filter.)
- Organization – Select an organization from the list. (Select **All** to clear the organization filter.)
- Status – Select **Online** or **Offline** to filter by appliance status. (Select **All** to clear the status filter.)
- Order By – Select **Last Time Seen**, **Name**, **Model**, **Alerts**, **Free Space**, or **Version**.

- Appliance Name field – Enter a text string, then press **Enter** to apply. Appliance names containing the text you entered display.
- Available space 30% or less – Filter by amount of free space on the appliance.



Viewing appliance details

To view appliance details:

- 1 In the Appliances view, click the appliance.

The screenshot shows the UniView Protect interface. At the top, there are navigation tabs: Dashboard, Protect, Jobs, and Organizations. A 'Protect' section is active, showing a 'Spanning Licenses' summary with 118 assigned, -118 remaining, and 0 purchased licenses. Below this, there are tabs for Appliances, Assets, Microsoft 365, Google Workspace, and Microsoft Azure. A search bar is present with filters for Scope, Organization, Status, Order By, and Appliance Name. A table lists appliances, with 'VMWARE-UB-98' selected. The table columns are: Name, Model, Organization, Free Space, Alerts, Helix Status, and Version. The selected appliance has a lock icon, a green alert icon, and a 'Manage' button. A callout box points to the appliance name with the text 'Select the appliance'.

Scope	Organization	Status	Order By	Appliance Name	Available space
All	All	All	Free Space	ub-98	30 % or less

NAME	MODEL	ORGANIZATION	FREE SPACE	ALERTS	HELIX STATUS	VERSION
VMWARE-UB-98	VIRTUAL APPLIANCE	T	172.0 GB / 199.9 GB 86.06% FREE	0	HELIX OFF AUTO UPDATES OFF	10.7.10

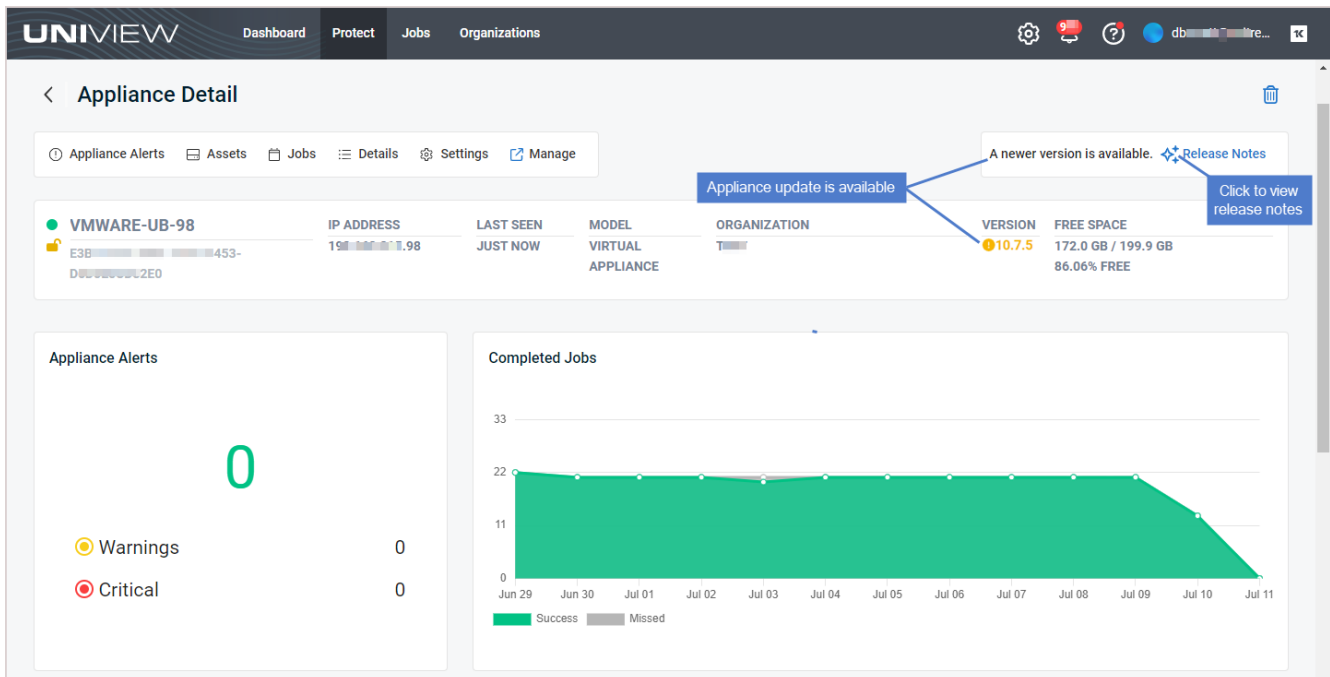
2 The following details display for the selected appliance:

- Alerts icon – Indicates whether the appliance has unresolved alerts: green for no alerts, yellow for warnings, red for critical.
- Lock icon – Indicates whether local access to the appliance has been blocked: for blocked, for unblocked. Once local access has been blocked, users can no longer log in directly to the appliance UI. Instead, users must connect to the appliance from UniView (as described in "[Connecting to an appliance](#)"). For more on this feature, see "[Blocking or unblocking local access to an appliance](#)".
- Name and asset tag – The appliance name and asset tag.
- IP Address – Appliance IP address (or *N/A* if your environment is not configured to store IP addresses).
- Last Seen – Indicates whether the appliance is online or offline. *Just Now* indicates the appliance is online. If the appliance is offline, shows the number of hours, days, months, or years since the appliance was last seen.
- Model – Appliance model. *VM* for Unitrends Backup virtual appliances. Model number for Unitrends physical appliances.
- Organization – Appliance's organization.
- Version – Unitrends version running on the appliance.

If the appliance is not running the latest release, the version number displays in yellow indicating that an update is available. Click **Release Notes** above to see details about the latest release. Click **Manage** to log in to the appliance and install the latest Unitrends software version.

Note: If you see the message *Unable to upgrade*, contact Unitrends Support or your Authorized Partner for assistance.

- Free Space – Shows the amount of free space on the appliance, in terabytes (TB) or gigabytes (GB), and as a percent of total space.
- Appliance Alerts tile – Shows the number of unresolved critical and warning alerts on the appliance.
- Completed Jobs tile – Shows the number of successful and missed jobs completed over the last 13 days. Hover over a point in the graph to see the number of successful and missed jobs completed that day. Click **Missed** to hide missed jobs. Click **Success** to hide successful jobs.
- Appliance Alerts – Lists unresolved alerts.
- Assets tile – Lists the assets protected by the appliance. For each asset, shows the Last Full backup size and the date/times when recent backups and copies were taken.
 - Click **Add Asset** to add an asset to this appliance (see "Adding assets to an appliance").
 - Click **View Unprotected Assets** to open the Unprotected Assets dialog where you can apply backup policies to assets or remove assets from the appliance (see "Removing assets from an appliance").
- Jobs – Shows active, scheduled, and recent jobs.
- Details – Shows appliance storage, backup copy targets, and network settings.
- Manage – Click to log in to the appliance (for details see "Connecting to an appliance").
- Settings – Click the toggles to block/unblock local access to the appliance or to open/close a support tunnel. For details, see "Blocking or unblocking local access to an appliance" and "Opening or closing a support tunnel".



Assets

Type: All Select to filter by asset type Enter Asset Name: Enter text to filter by asset name Click to view unprotected assets

Protected Assets Click to add an asset Add Asset View Unprotected Assets (290)

0 selected | Remove

Type	Name	Last Full	Last Backup	Recent Backups	Last Backup Copy	Recent Backup Copies	Last Certified
vm	1...D7CCC	983.8 GB	5 hours ago	MTWTFSS	5 hours ago	MTWTFSS	
vm	Windows10...ks	61.2 GB	9 hours ago	MTWTFSS	9 hours ago	MTWTFSS	
vm	Windows10...	69.7 GB	9 hours ago	MTWTFSS	9 hours ago	MTWTFSS	
vm	DS-SQLCLAD...7	21.9 GB	9 hours ago	MTWTFSS	9 hours ago	MTWTFSS	
vm	Unitrends_...	16.4 GB	10 hours ago	MTWTFSS	10 hours ago	MTWTFSS	
vm	Win8...1)	54.4 GB	10 hours ago	MTWTFSS	10 hours ago	MTWTFSS	
vm	SQL20...6		10 hours ago	MTWTFSS	10 hours ago	MTWTFSS	
vm	Win10...2	42.0 GB	10 hours ago	MTWTFSS	10 hours ago	MTWTFSS	
vm	DS-SQLCL01...8	19.1 GB	11 hours ago	MTWTFSS	11 hours ago	MTWTFSS	
vm	DS-SQLCL02...9	19.0 GB	11 hours ago	MTWTFSS	11 hours ago	MTWTFSS	
vm	sql			XXXXXXXXXX		MTWTFSS	

50 per page | 1 of 1 pages

Annotations:
 - Click to view asset details (points to SQL20...6)
 - Hover to view job details (points to Recent Backup Copies for DS-SQLCLAD...7)
 - Hover to view job details or click to view asset details (points to Recent Backups for sql)

Appliance Alerts Click to log in to appliance

Click a heading to sort by column

Date/Time	Message	Alert Source	Updated
9/22/2022 5:03 PM	Inventory full sync completed with 3 warning(s).	Process	5:04 PM

Click to dismiss alert

Jobs Click to log in to appliance

Active | Scheduled | Recent

Click a heading to sort by column

Job Name	Asset	Type	Started	Progress	Duration
Backup Copy	Windows2012R2_SB	Backup Copy (Hot)	10/7/2022 12:42 PM	<div style="width: 100%;"></div>	00:00:12
Backup Copy	Win8.1...	Backup Copy (Hot)	10/7/2022 12:42 PM	<div style="width: 100%;"></div>	00:00:12
Backup Copy	System Metadata	Backup Copy (Hot)	10/7/2022 12:20 PM	<div style="width: 100%;"></div>	-

Type	Name	Capacity	Total Size	Free Size	Status
	Internal	<div style="width: 80%;"></div>	28.1 TB	1.6 TB	Online

Adding assets to an appliance

Any physical machine, virtual machine, or application you wish to protect is an *asset*. The first step in protecting an asset is adding it to the Unitrends appliance.

You can add these asset types to your backup appliance— right from UniView:

- Windows physical machines – Adding the machine also adds any hosted applications (e.g., SQL or Exchange).
- Linux physical machines – Adding the machine also adds any hosted applications (e.g., Oracle on Linux).
- vCenter or ESXi servers – Adding the server also adds its hosted VMs.
- Hyper-V servers – Adding the server also adds its hosted VMs.

To add an asset, review the "[Prerequisites and considerations](#)", then proceed to the applicable add asset procedure below.

Prerequisites and considerations

Ensure that these prerequisites have been met before adding your asset:

- The appliance where you are adding the asset must be a Unitrends backup appliance (adding an asset to a backup copy target appliance is not supported).
- Windows physical machine – You must install the Unitrends Windows agent before adding the asset to the appliance. For details, see [Installing the Windows agent](#) in the [Administrator Guide for Recovery Series, Recovery MAX, ION/ION+, and Unitrends Backup](#).
- Linux physical machine – You must install the Unitrends Linux agent before adding the asset to the appliance. For details, see [Installing the Linux agent](#) in the [Administrator Guide for Recovery Series, Recovery MAX, ION/ION+, and Unitrends Backup](#).

- Hyper-V servers –
 - You must install the Unitrends Windows agent on the Hyper-V server before adding it to the appliance. For details, see [Installing the Windows agent](#) in the [Administrator Guide for Recovery Series, Recovery MAX, ION/ION+, and Unitrends Backup](#).
 - Hyper-V clusters are not supported.
- VMware considerations –
 - Servers running free ESXi versions are not supported and cannot be added to a Unitrends appliance.

Note: To protect a Windows or Linux VM hosted on free ESXi, you can install the Unitrends agent on the VM and add the VM to the appliance using the "[Working with Unitrends Appliances, Assets, and Backups](#)" procedure. The VM is then protected by the appliance as a physical asset.

- If a vCenter is managing your ESXi servers, Unitrends recommends that you add to the appliance each ESXi server and the vCenter server itself. Some features that you can run from the appliance UI require a vCenter server (for example, VM instant recovery). To enable these features, you must add both the ESXi host and the vCenter server to the appliance.

To add a Windows or Linux asset

Note: You must install the Unitrends Windows or Linux agent before running this procedure.

- 1 In the Appliances view, locate the appliance. Click **Add Asset**, then select **Asset**.

The screenshot shows the UniView portal interface. The top navigation bar includes 'Dashboard', 'Protect', 'Jobs', and 'Organizations'. The main content area is titled 'Protect' and features a 'Spanning Licenses' section with 'Assigned: 128', 'Remaining: -128', and 'Purchased: 0'. Below this, there are tabs for 'Appliances', 'Assets', 'Microsoft 365', 'Google Workspace', 'Salesforce', and 'Microsoft Azure'. The 'Appliances' tab is active, showing a table of appliances. The table has columns for 'Scope', 'Organization', 'Status', 'Order By', 'Appliance Name', 'Available space', 'LAST SEEN', 'MODEL', 'ORGANIZATION', 'FREE SPACE', 'ALERTS', 'HELIX STATUS', and 'VERSION'. One appliance is listed: 'UVM-S1 TGQMJJOK' with a status of '215--' and a version of '10.7.3'. The 'Add Asset' dropdown menu is open, showing options for 'Asset', 'VMware', and 'Hyper-V'. The 'Asset' option is selected.

- 2 Enter the asset's IP address. This is optional in some cases, as described here:

- DNS registration should be used for assets that obtain their network settings through DHCP. It is optional for assets with static IP addresses.
- If you do not enter a static IP address, make sure that both the asset and the appliance have DNS entries and that reverse lookup is configured.
- If you enter a static IP address, the appliance attempts to connect using this address, but if the attempt fails, it will try to add the asset using DNS.

3 Enter the asset's hostname.

4 Click **Save**.

Add Asset

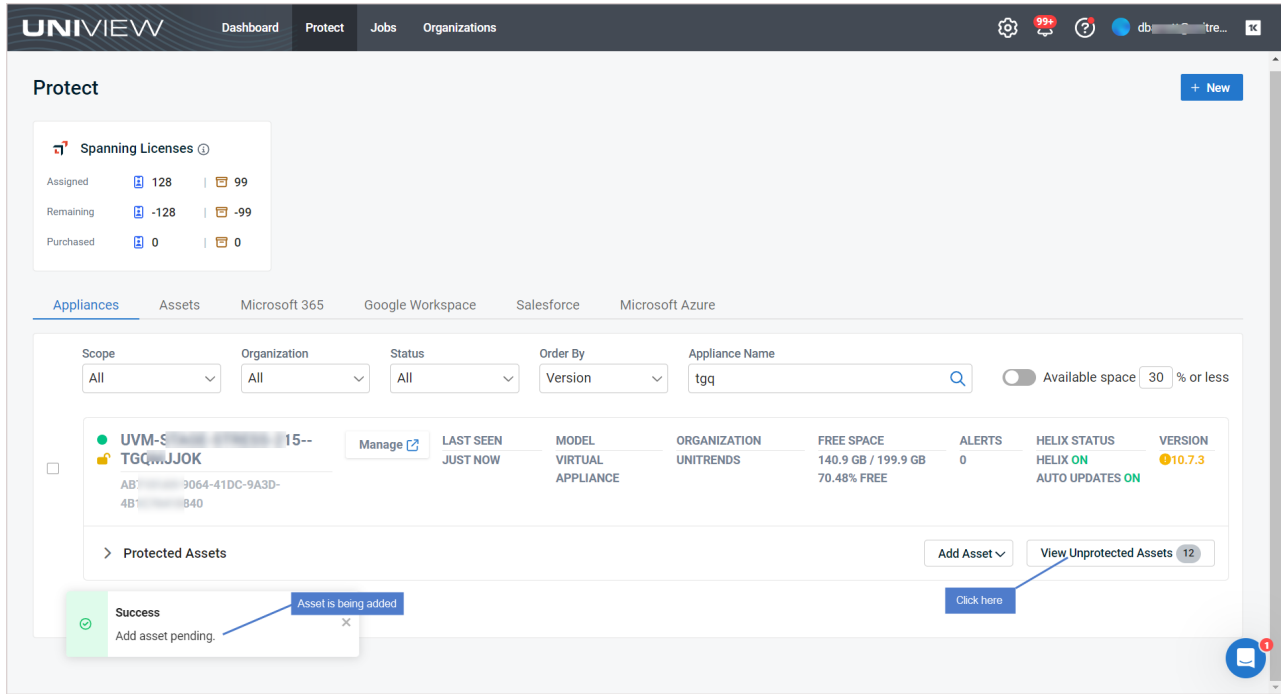
Appliance
uvm-5-tgqmjjok

IP Address
192.178 (If needed) Enter IP address

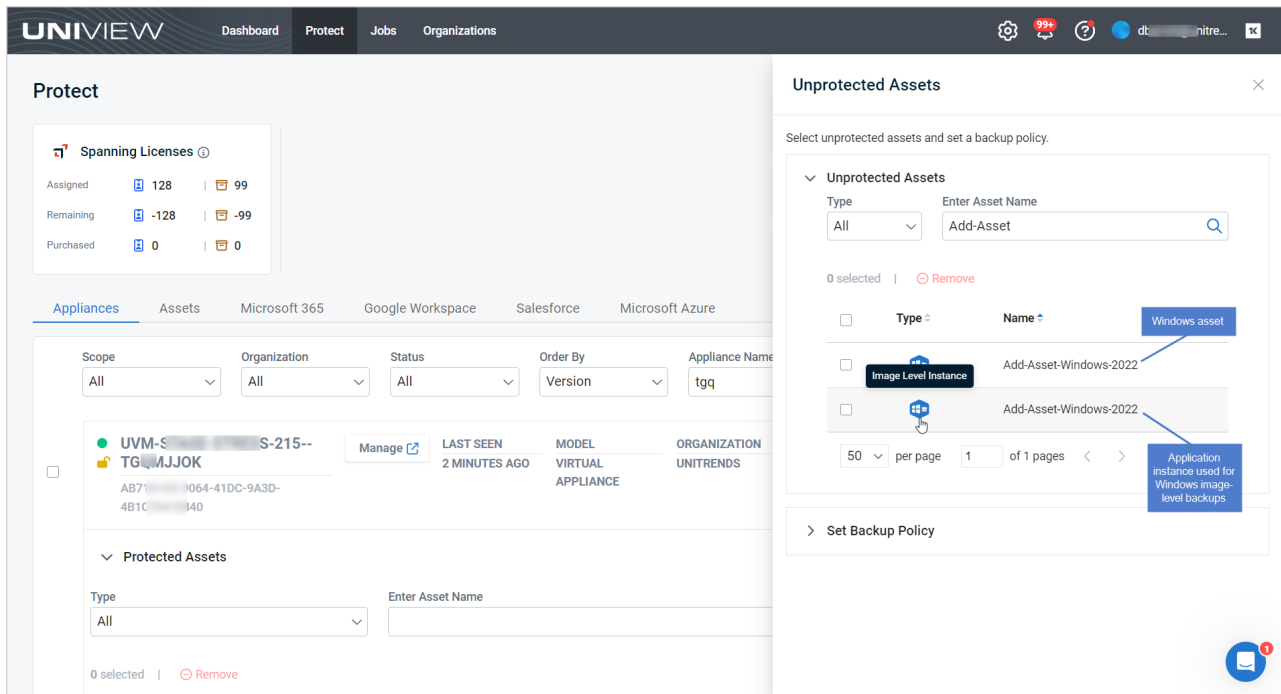
Asset Name *
Add-Asset-Windows-2022 Enter asset's hostname

Cancel Save

5 The asset is added, along with any hosted applications. Click **Unprotected Assets** to view the new asset.



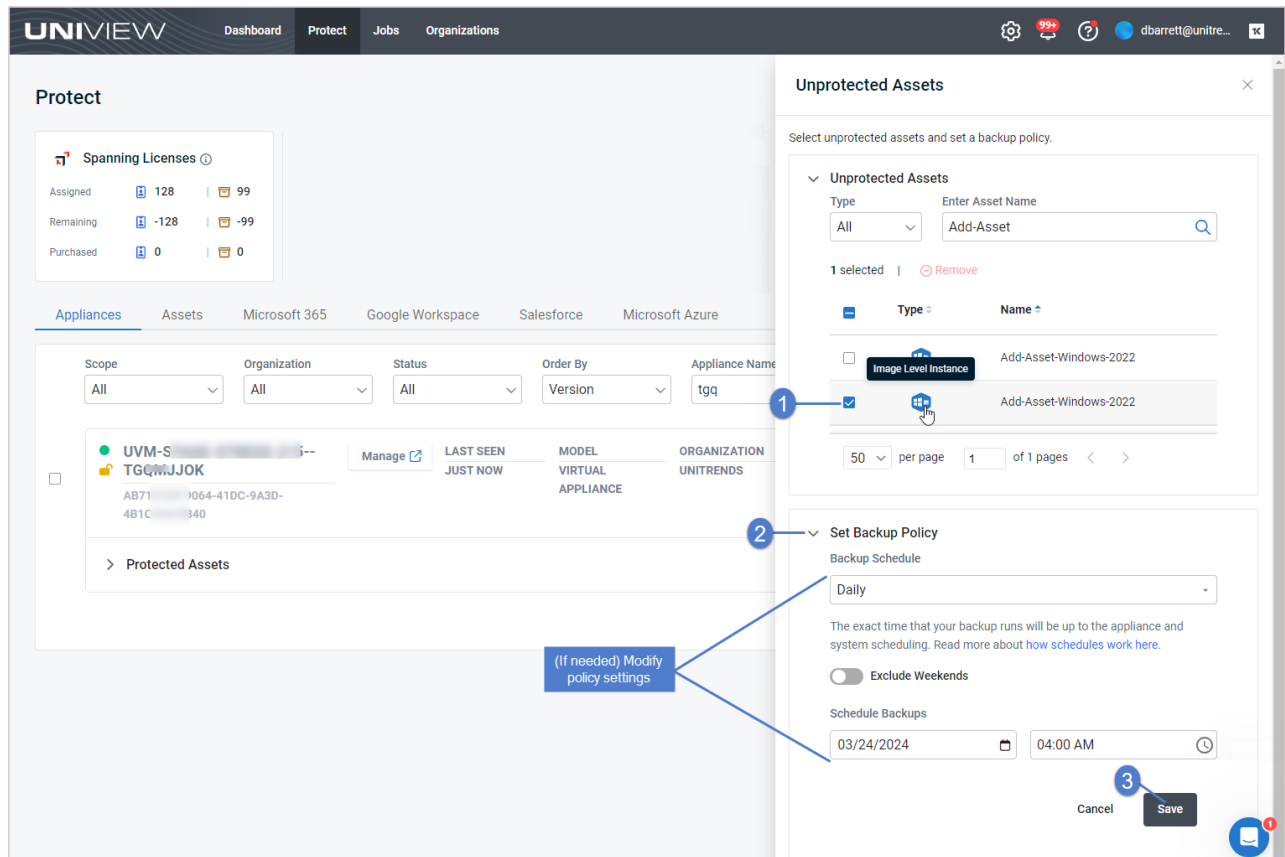
Note: The asset is still being added if you see a spinner icon by the asset in the Unprotected Assets list.



- (Optional for Windows only) Apply a backup policy to the new Image Level Instance to start running image-level backups:

Note: Backup policies are supported for Windows image-level assets and VMware VMs. Support for other asset types will be included in up-coming UniView Portal releases.

- Check the Image Level Instance box.
- Click **Set Backup Policy**.
- Modify policy settings as needed. Click **Save**.



Applying the policy can take a few minutes. Once applied, the Image Level Instance asset is listed under the appliance's Protected Assets:

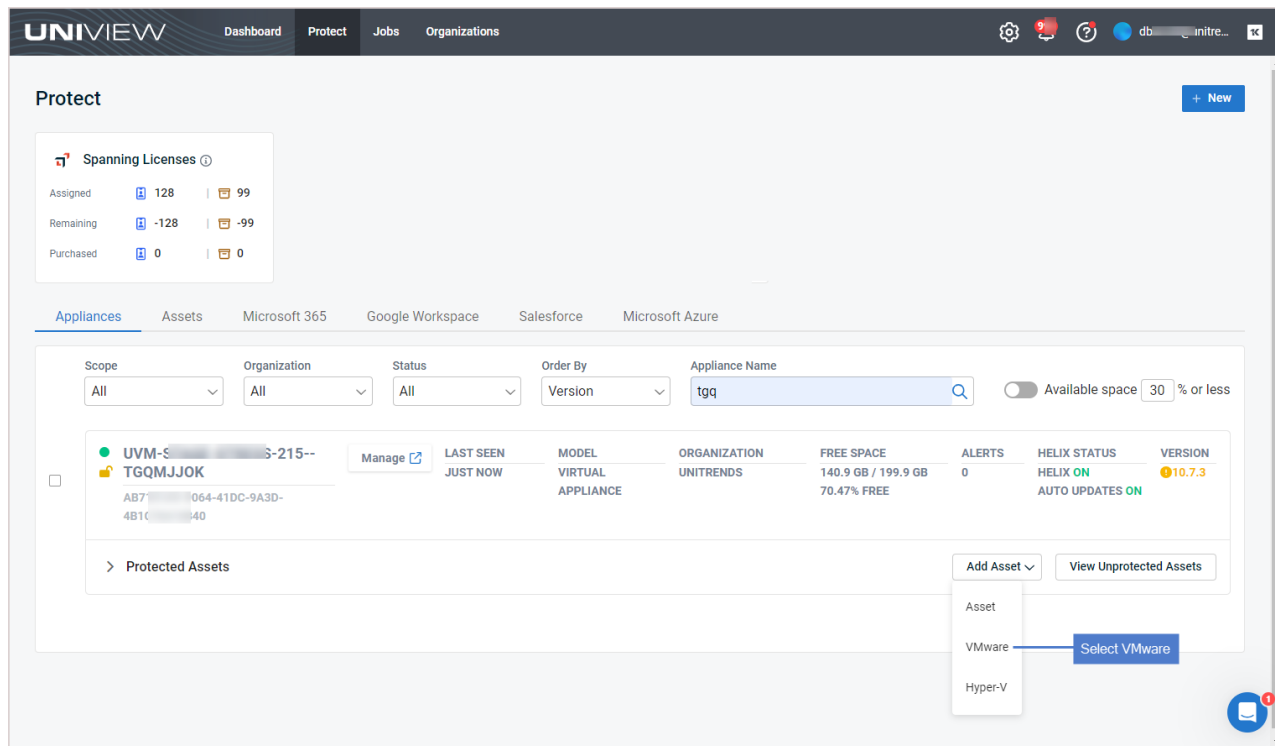
The screenshot shows the 'Assets' view in the UniView Portal. The top navigation bar includes 'Appliances', 'Assets', 'Microsoft 365', 'Google Workspace', 'Salesforce', and 'Microsoft Azure'. The 'Assets' tab is active. Below the navigation, there are filters for Scope (All), Organization (All), Status (All), Order By (Version), and Appliance Name (tgqm). A search bar and an 'Available space' toggle (30% or less) are also present. The main content area displays a table of assets. The first asset is 'UVM-S... TGQI JYOK' with a status of '5--'. Below this, there is a section for 'Protected Assets' with an 'Add Asset' button and a search bar. A table below shows a list of assets with columns for Name, Last Full, Recent Backups, Last Backup Copy, Recent Backup Copies, and Last Certified. A callout box points to the 'Last Full' column of the first row, stating 'Asset is moved to Protected Assets'.

In the Assets view, you can see the Backup Policy that was applied:

The screenshot shows the 'Assets' view in the UniView Portal, filtered to show assets with the name 'Add-Asset-Windows-2022'. The top navigation bar includes 'Appliances', 'Assets', 'Microsoft 365', 'Google Workspace', 'Salesforce', and 'Microsoft Azure'. The 'Assets' tab is active. Below the navigation, there are filters for Scope (All), Organization (All), Appliance (All), Type (All), and Asset Name (Add-Asset-Windows-2022). A search bar and a 'Recent Failures' toggle are also present. The main content area displays a table of assets. The first asset is 'Add-Asset-Windows-2022' with a status of '5--'. Below this, there is a section for 'Protected Assets' with a 'Set Backup Policy' button and a search bar. A table below shows a list of assets with columns for Name, Appliance, Backup Policy, Last Full, Last Backup, Recent Backups, Last Backup Copy, Recent Backup Copies, and Last Certified. A callout box points to the 'Backup Policy' column of the first row, stating 'Daily policy was applied'.

To add a vCenter server

- 1 In the Appliances view, locate the appliance. Click **Add Asset**, then select **VMware**.



2 In the Add VMware dialog:

- Select **Add vCenter** from the vCenter list.

Note: If the appliance is running version 10.8.1 or higher and you have already added the vCenter (through the appliance UI), you can select it in the vCenter list instead of clicking **Add vCenter**.

- Enter the vCenter IP address and credentials.
- (Recommended) For best performance and to enable certain features, we recommend that you add each ESXi host that is managed by this vCenter. Click **Add Host**, enter the host IP address and credentials, then click the checkmark to save. Repeat to add another host.
- Click **Save**.

Add VMware

vCenter Details

vCenter *
 1

Appliance IP Address * 2

vCenter Credentials

Username * Password * 2

ESXi Hosts

Please add all hosts that are connected to your vCenter.

IP Address	Username	Password	
192...1	root	*****	x
19...2	<input type="text" value="root"/>	<input type="password" value="....."/>	✓ x

3

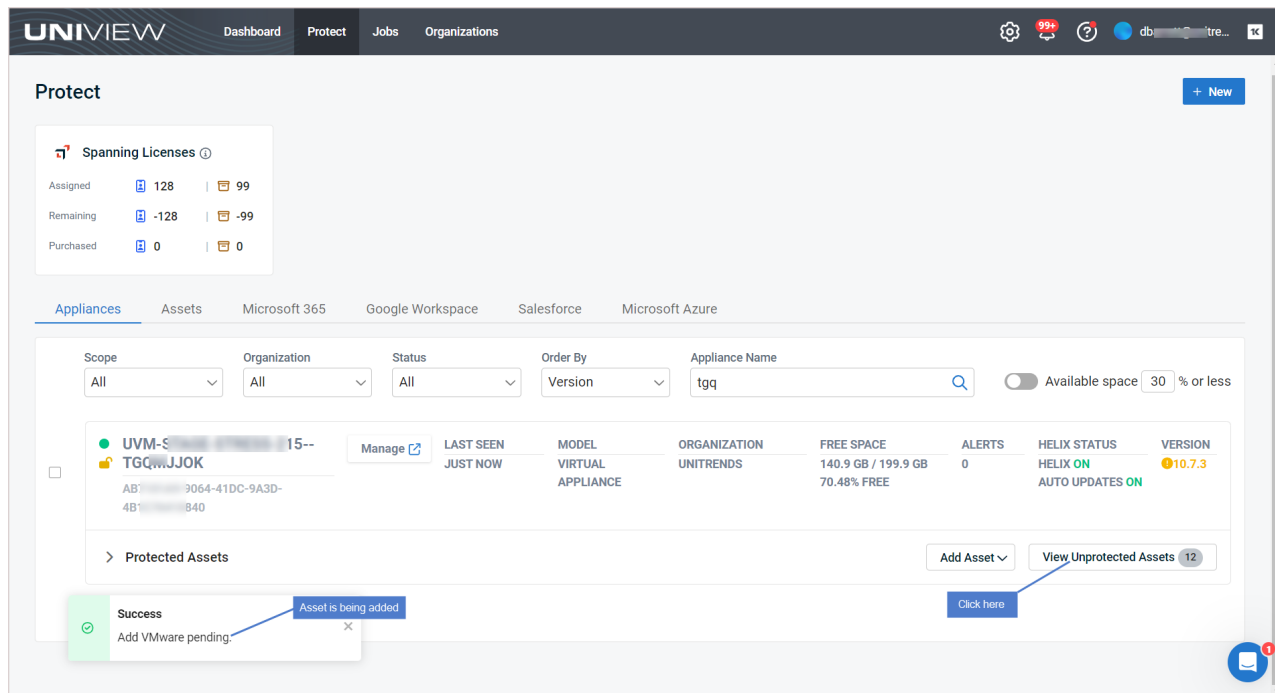
4

(Recommended) Add each ESXi host that is managed by the vCenter

3 The following assets are added:

- The vCenter server
- All VMs that reside on the ESXi hosts that this vCenter manages
- Any ESXi hosts that you added with the vCenter

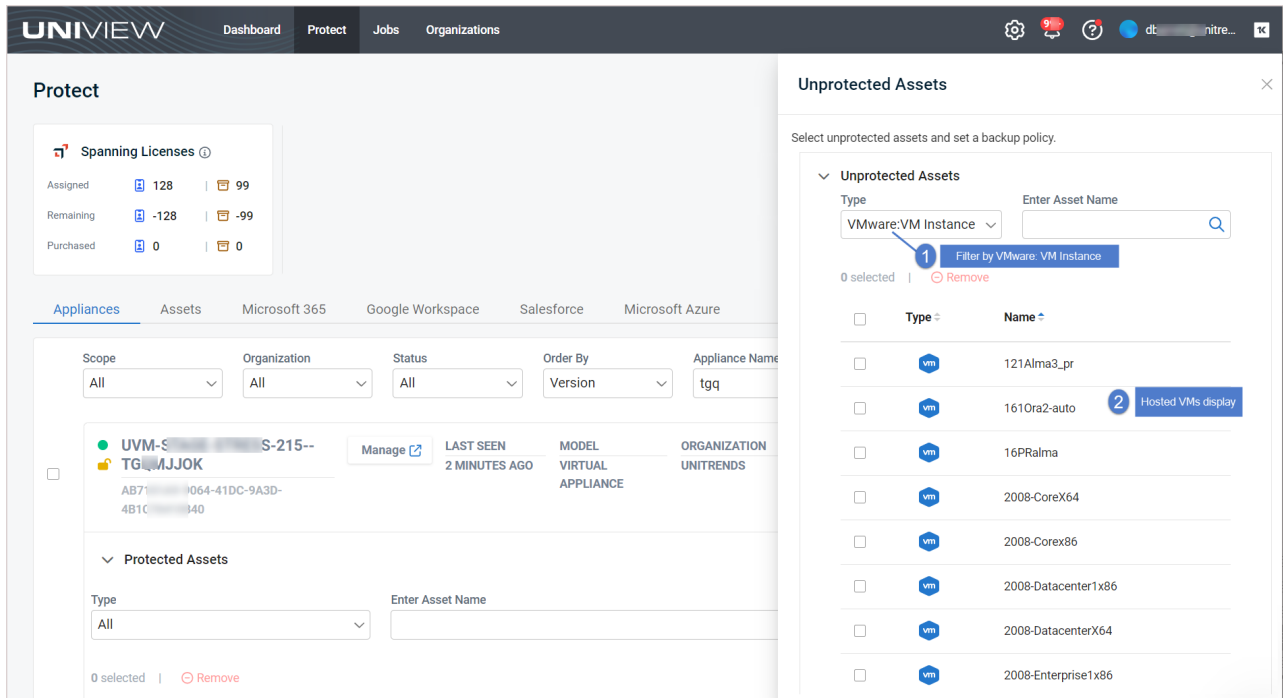
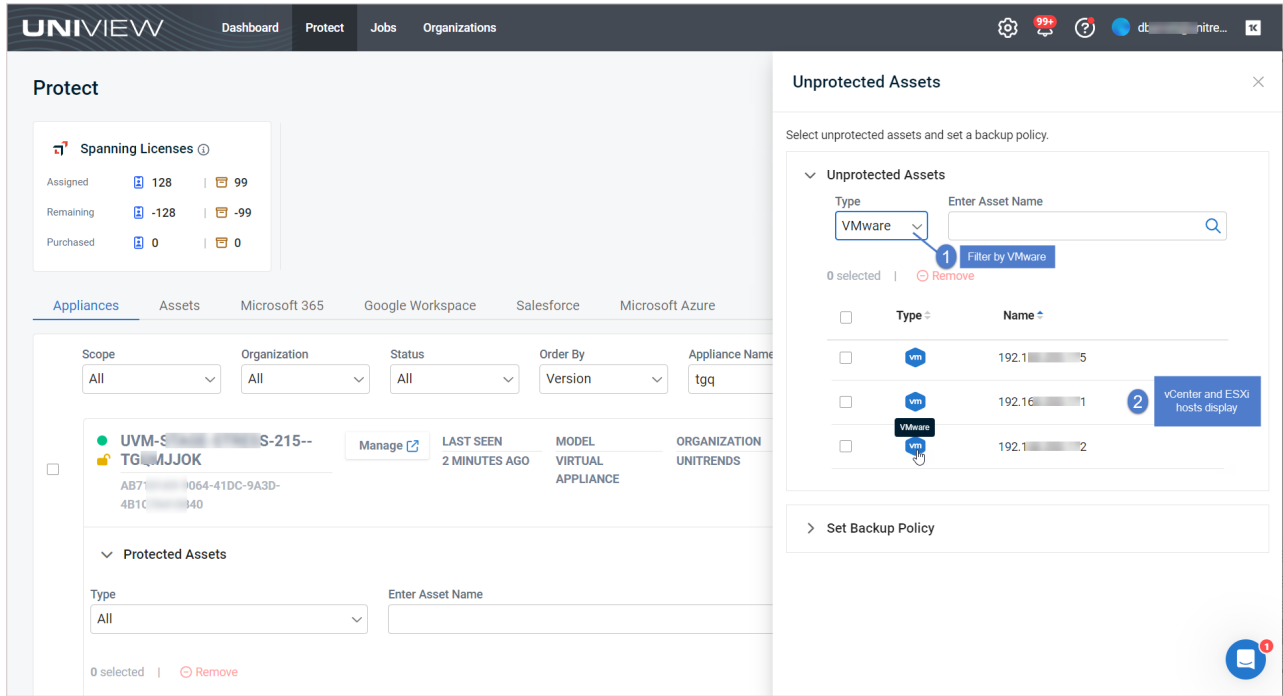
4 Click **View Unprotected Assets** to view these assets.



5 To filter the Unprotected Assets list, you can select the **VMware** Type to view the vCenter and ESXi hosts or the **VMware: VM Instance** Type to view their hosted VMs:

Notes:

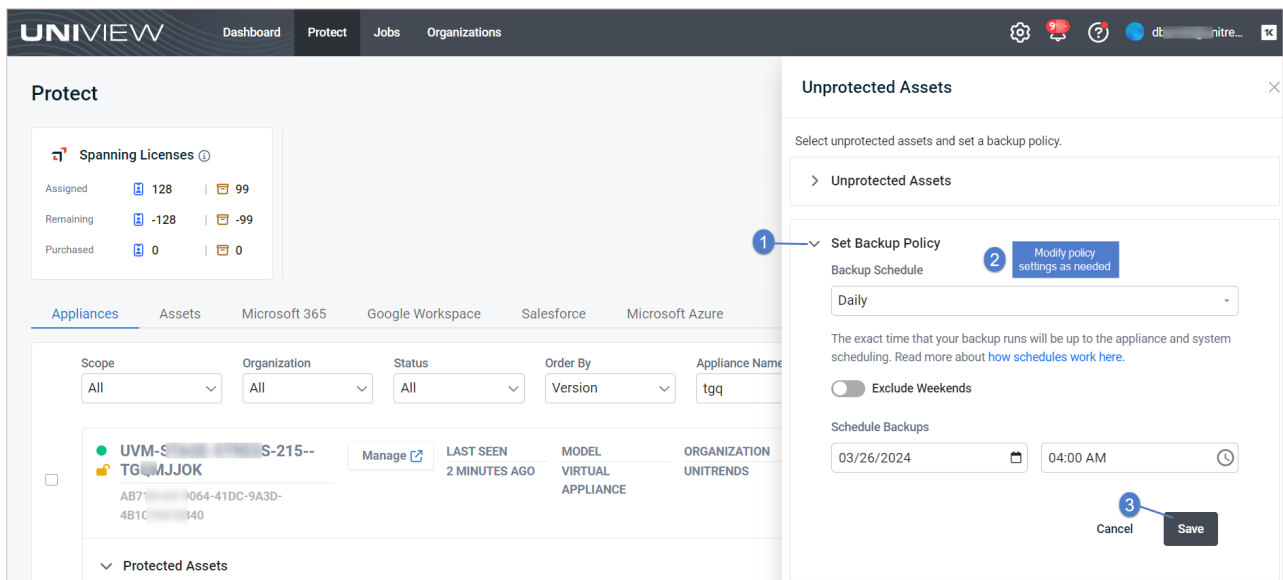
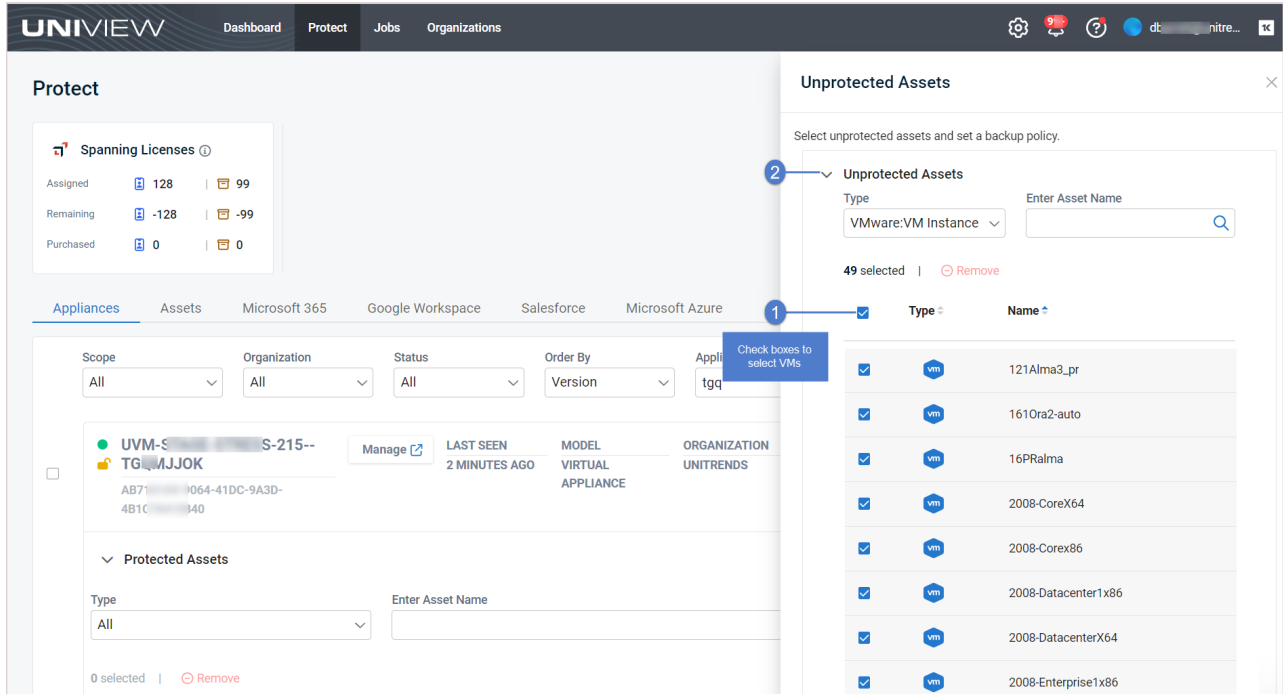
- The asset is still being added if you see a spinner icon by the asset in the Unprotected Assets list.
- For vCenter and ESXi hosts, the Name column displays the server's IP address.
- For VMs, the Name column displays the machine's hostname.



6 (Optional) Apply a backup policy to the new VMs to start running VMware host-level backups:

Note: Backup policies are supported for Windows image-level assets and VMware virtual machine assets. Support for other asset types is will be included in up-coming UniView Portal releases.

- Check boxes to select one or more VMs. In this example, we've checked the Select All box to apply a policy to all the newly added VMs.
- Click **Unprotected Assets** to hide the assets list.
- Click **Set Backup Policy**.
- Modify policy settings as needed. Click **Save**.



Applying the policy can take a few minutes. Once applied, the VMs are listed under the appliance's Protected Assets.

Switch to the Assets view to see the Backup Policy that was applied.

To add an ESXi host

Use this procedure to add a stand-alone ESXi host.

Note: If your ESXi host is being managed by a vCenter, we recommend using the "To add a vCenter server" procedure to add both the vCenter and the ESXi host.

- 1 In the Appliances view, locate the appliance. Click **Add Asset** and select **VMware**.

The screenshot displays the UniView Protect interface. At the top, there is a navigation bar with 'Dashboard', 'Protect', 'Jobs', and 'Organizations'. Below this, a 'Protect' section shows 'Spanning Licenses' with counts for Assigned (128), Remaining (-128), and Purchased (0). The main area is titled 'Appliances' and features a table with columns: Scope, Organization, Status, Order By, Appliance Name, Free Space, Alerts, Helix Status, and Version. A table entry for 'UVM-S...-215-- TGQMJJOK' is visible, showing details like 'LAST SEEN: JUST NOW', 'MODEL: VIRTUAL APPLIANCE', 'ORGANIZATION: UNITRENDS', 'FREE SPACE: 140.9 GB / 199.9 GB (70.47% FREE)', 'ALERTS: 0', 'HELIX STATUS: HELIX ON AUTO UPDATES ON', and 'VERSION: 10.7.3'. Below the table, there is a 'Protected Assets' link. On the right side, an 'Add Asset' dropdown menu is open, showing options for 'Asset', 'VMware' (which is highlighted with a blue arrow and labeled 'Select VMware'), and 'Hyper-V'. There is also a 'View Unprotected Assets' button.

- 2 In the Add VMware dialog:

- Select **None** from the vCenter list.
- Click **Add Host**. Enter the host IP address and credentials, then click the checkmark to save. Repeat to add another host.
- Click **Save**.

Add VMware

vCenter Details

vCenter * ▼

None 1

ESXi Hosts

Please add all hosts that are connected to your vCenter.

IP Address	Username	Password	
192.168.1.1	root	*****	x
192.168.1.2 3	root 👁	✓ x 4

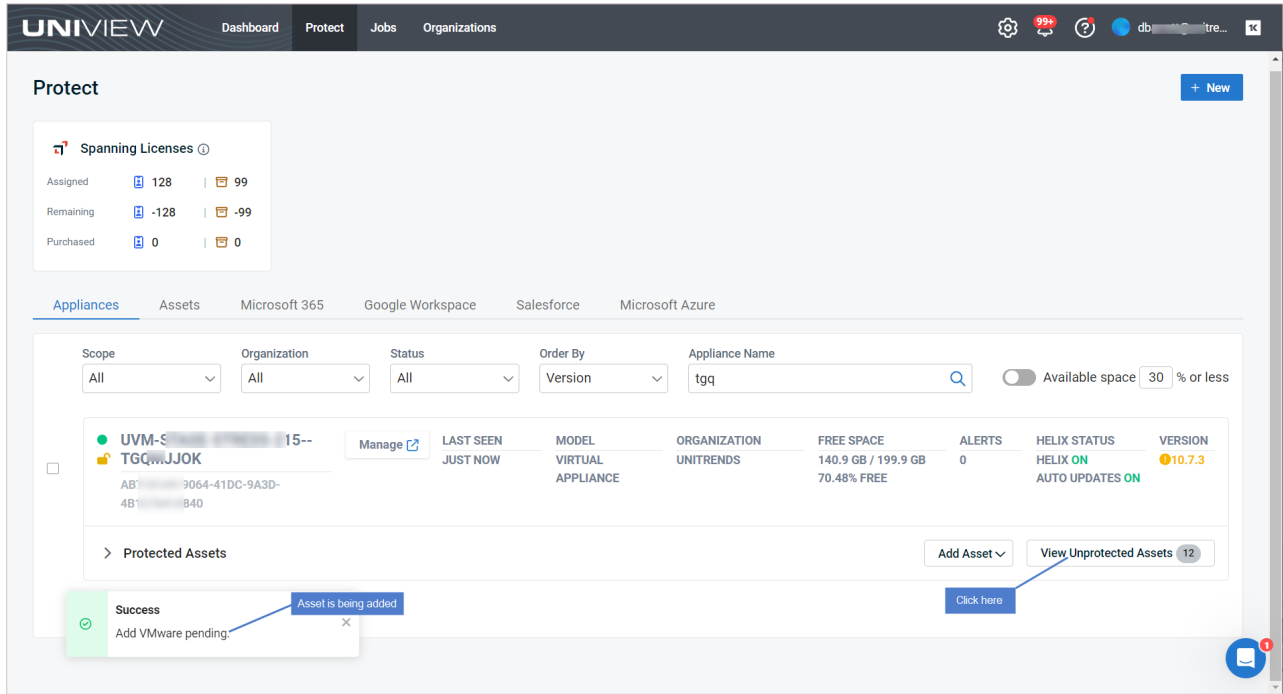
Add ESXi Host 2

Cancel 5

Save

Enter host IP address and credentials

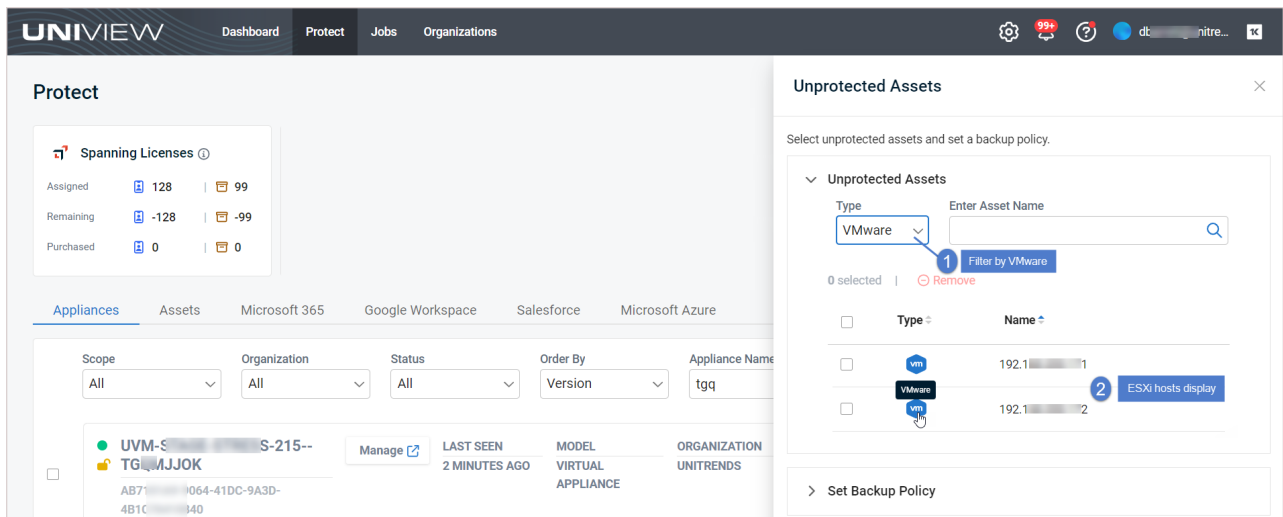
- 3 The following assets are added:
 - Each ESXi host that you added
 - All VMs that reside on the ESXi hosts that you added
- 4 Click **View Unprotected Assets** to view these assets.

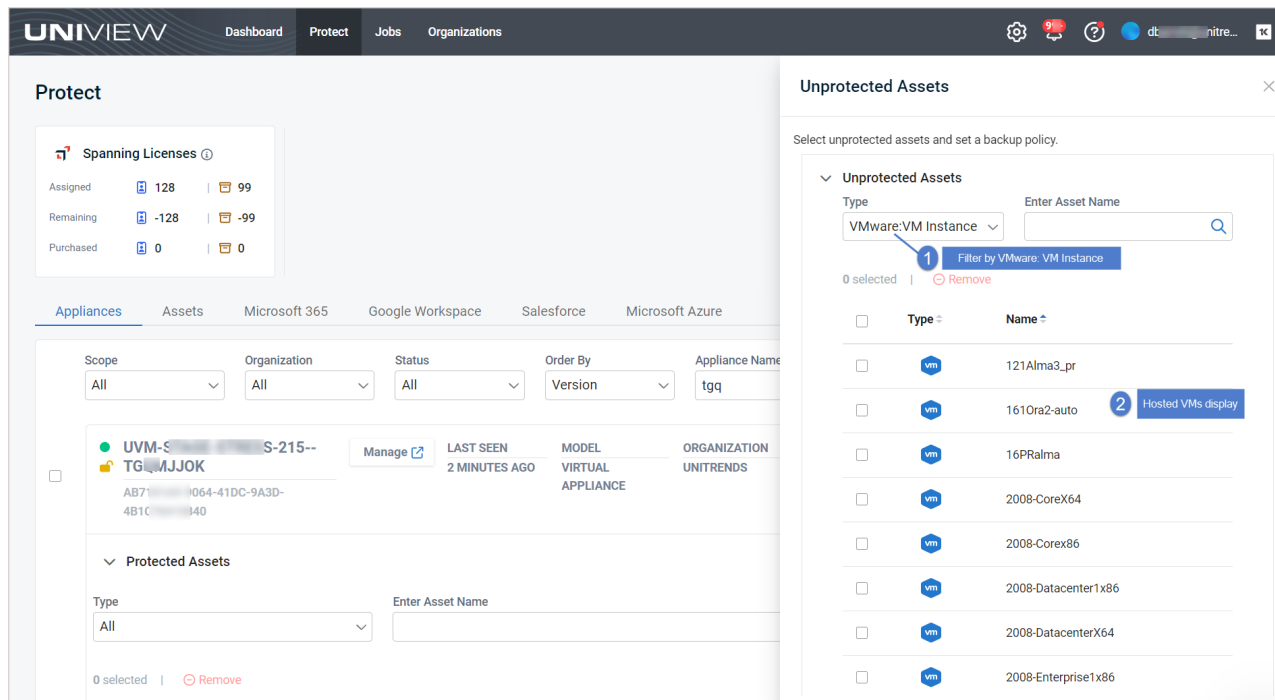


5 To filter the Unprotected Assets list, you can select the **VMware** Type to view your ESXi hosts or the **VMware: VM Instance** Type to view their hosted VMs:

Notes:

- The asset is still being added if you see a spinner icon by the asset in the Unprotected Assets list.
- When the host is first added, the Name column displays the server's IP address. The IP address is replaced by the server's hostname once the UniView Portal checks in with the Unitrends appliance.
- For VMs, the Name column displays the machine's hostname.

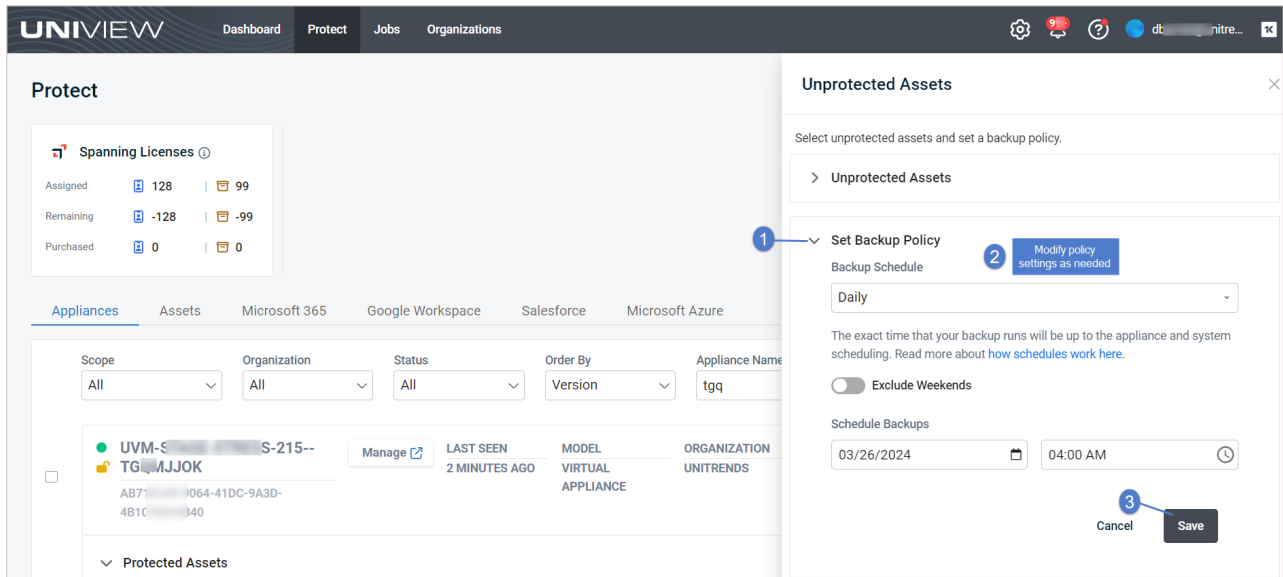
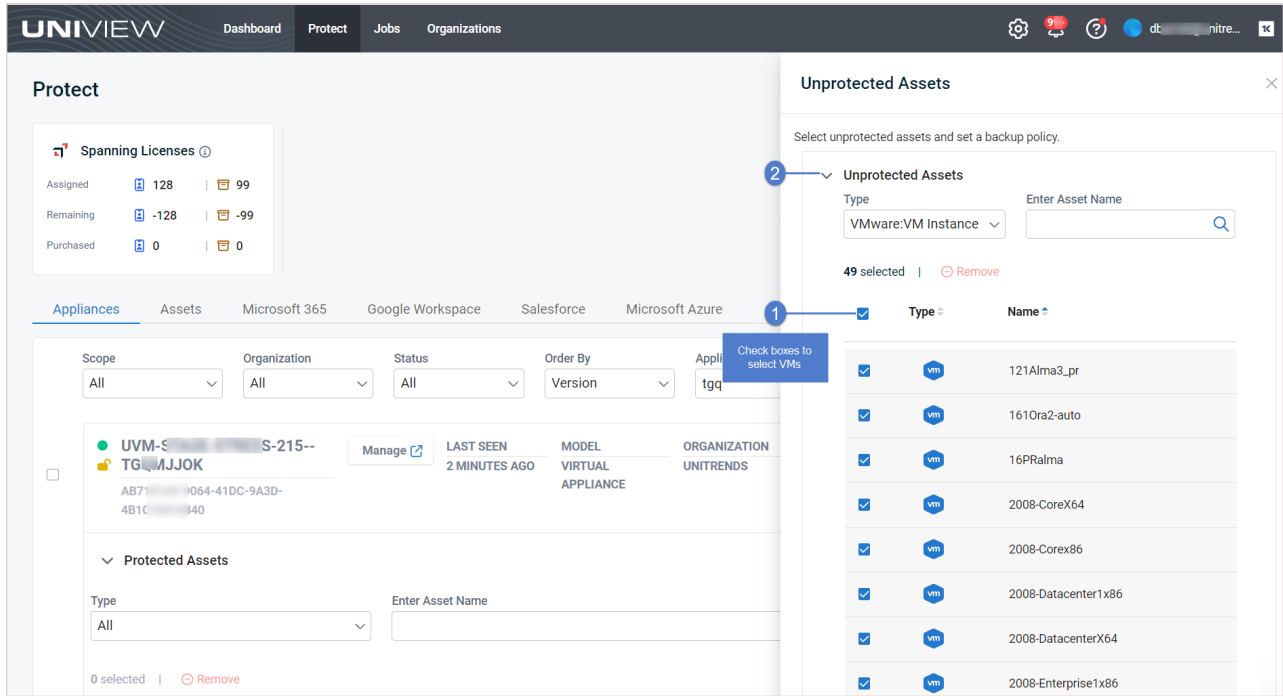




6 (Optional) Apply a backup policy to the new VMs to start running VMware host-level backups:

Note: Backup policies are supported for Windows image-level assets and VMware virtual machine assets. Support for other asset types is will be included in up-coming UniView Portal releases.

- Check boxes to select one or more VMs. In this example, we've checked the Select All box to apply a policy to all the newly added VMs.
- Click Unprotected Assets to hide the assets list.
- Click **Set Backup Policy**.
- Modify policy settings as needed. Click **Save**.



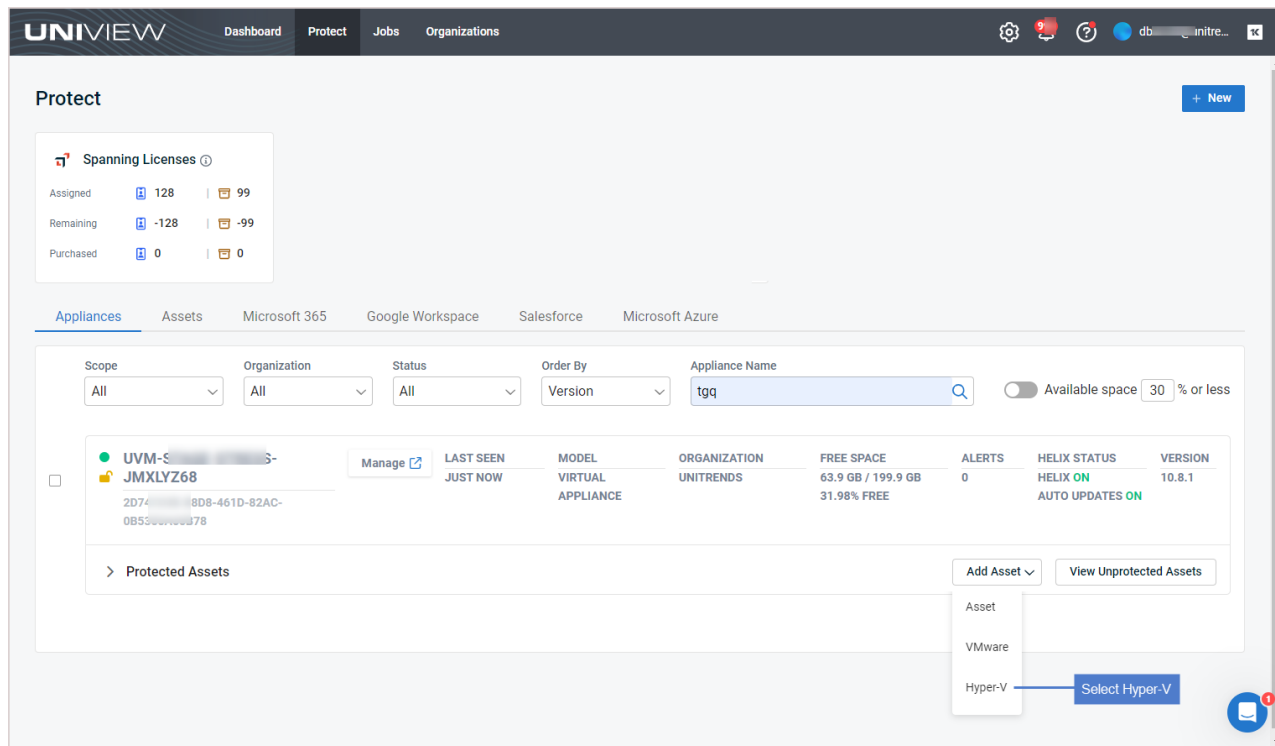
Applying the policy can take a few minutes. Once applied, the VMs are listed under the appliance's Protected Assets.

Switch to the Assets view to see the Backup Policy that was applied.

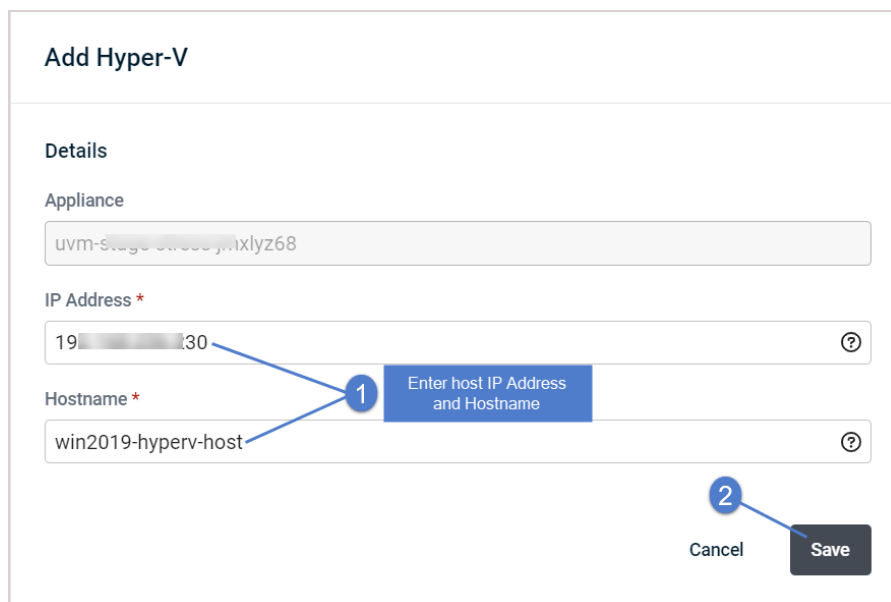
To add a Hyper-V host

Use this procedure to add a Hyper-V host.

- 1 In the Appliances view, locate the appliance. Click **Add Asset**, then select **Hyper-V**.



- 2 In the Add Hyper-V dialog:
 - Enter the host IP address and hostname.
 - Click **Save**.



- 3 The Hyper-V host and its virtual machines are added. Click **View Unprotected Assets** to view these assets.

The screenshot shows the UniView Protect interface. At the top, there's a navigation bar with 'Dashboard', 'Protect', 'Jobs', and 'Organizations'. Below that, a 'Protect' section shows 'Spanning Licenses' with counts for Assigned (128), Remaining (-128), and Purchased (0). The main area is titled 'Appliances' and contains a table of assets. A success message at the bottom left says 'Success: Add Hyper-V pending.' with a callout 'Host is being added'. A 'View Unprotected Assets' button is highlighted with a callout 'Click here'.

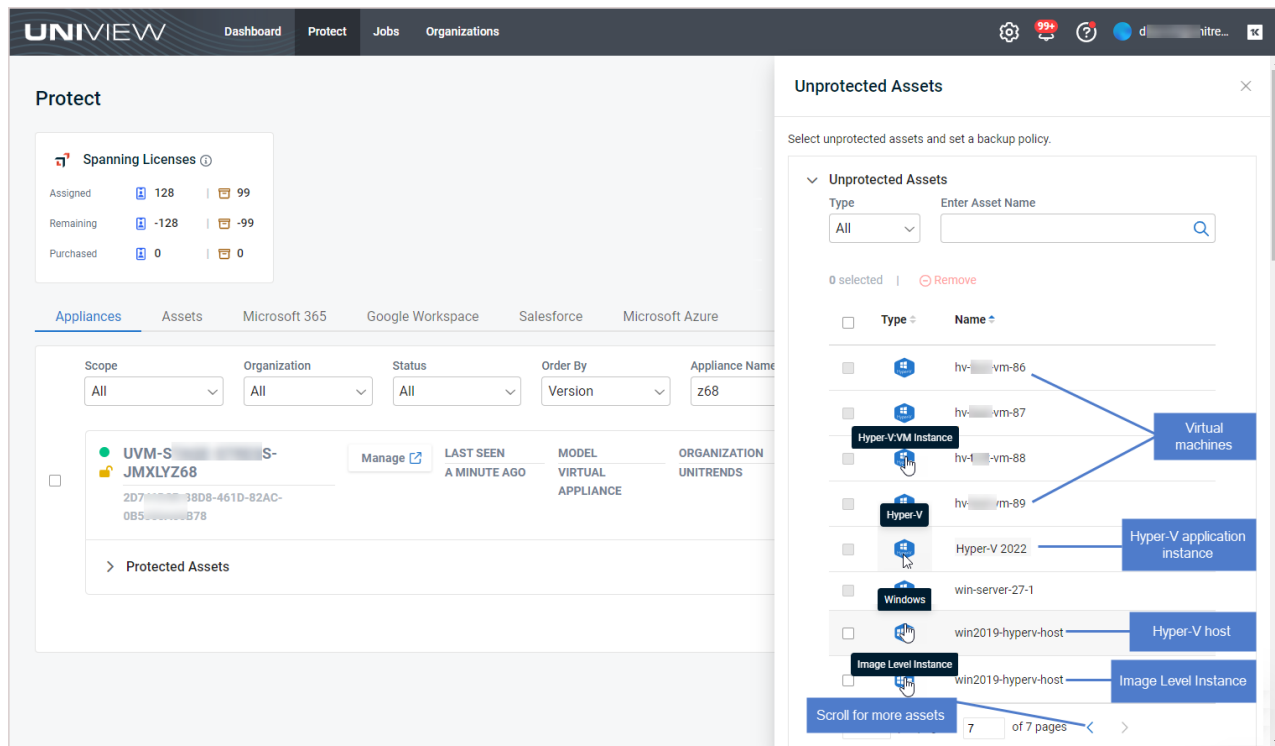
Scope	Organization	Status	Order By	Appliance Name	Available space														
All	All	All	Version	z68	30% or less														
<table border="1"> <thead> <tr> <th>Asset ID</th> <th>Model</th> <th>Organization</th> <th>Free Space</th> <th>Alerts</th> <th>Helix Status</th> <th>Version</th> </tr> </thead> <tbody> <tr> <td>UVM-S- JMXLYZ68</td> <td>VIRTUAL APPLIANCE</td> <td>UNITRENDS</td> <td>63.9 GB / 199.9 GB 31.98% FREE</td> <td>0</td> <td>HELIX ON AUTO UPDATES ON</td> <td>10.8.1</td> </tr> </tbody> </table>						Asset ID	Model	Organization	Free Space	Alerts	Helix Status	Version	UVM-S- JMXLYZ68	VIRTUAL APPLIANCE	UNITRENDS	63.9 GB / 199.9 GB 31.98% FREE	0	HELIX ON AUTO UPDATES ON	10.8.1
Asset ID	Model	Organization	Free Space	Alerts	Helix Status	Version													
UVM-S- JMXLYZ68	VIRTUAL APPLIANCE	UNITRENDS	63.9 GB / 199.9 GB 31.98% FREE	0	HELIX ON AUTO UPDATES ON	10.8.1													

- 4 These newly added assets display in the Unprotected Assets list:

- The Hyper-V host (asset type is *Windows*)
- Hosted virtual machines (asset type is *Hyper-V: VM Instance*)
- One or more Hyper-V application instances (asset type is *Hyper-V*)
- An application instance that can be used to run image-level backups of the Windows Hyper-V host server (asset type is *Image Level Instance*)

Note: The asset is still being added if you see a spinner icon by the asset in the Unprotected Assets list.

Hover over an icon to see an asset's type. You can filter the list by asset type or asset name using the fields above.



Removing assets from an appliance

You can remove these asset types from your appliance— right from UniView:

- Windows physical machines
- Linux physical machines
- vCenter or ESXi servers
- Hyper-V servers

From the Appliance page or Appliance Detail page, you can remove one or more assets in a single operation. Before removing an asset, review the ["Prerequisites and considerations for removing assets"](#). Then use the ["To remove selected assets from an appliance"](#) procedure to remove assets.

Note: You can also use the Assets page to remove assets from appliances. For details, see ["Removing assets"](#).

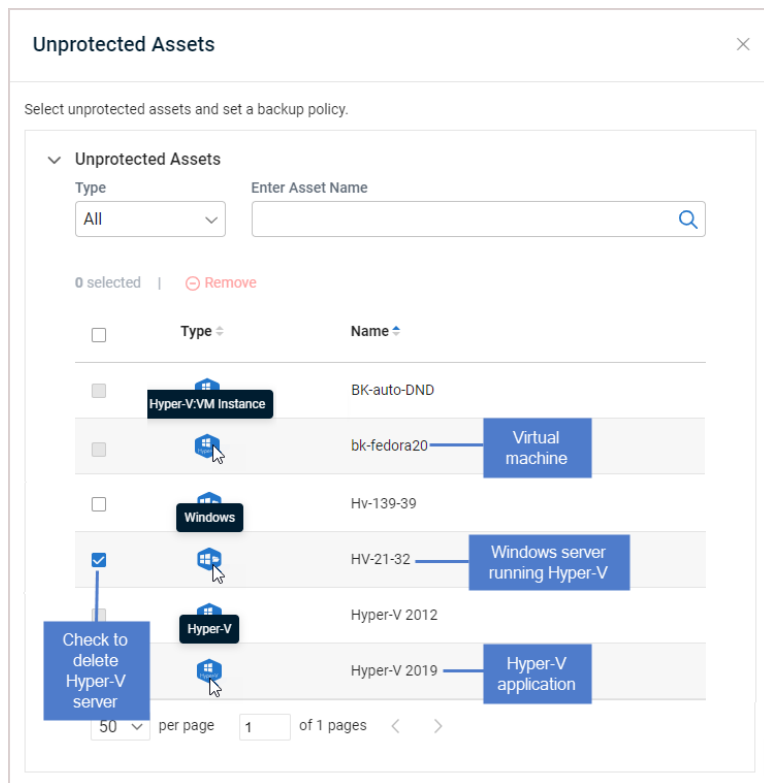
Prerequisites and considerations for removing assets

The following requirements and considerations apply:

- Before you can remove an asset, you must remove any UniView backup policy or remove the asset from any Unitrends job schedules.
- When an asset is removed, all associated backups of that asset are also deleted. Please use caution when removing an asset.

- Removing an asset also removes any associated asset instances, along with the backups of those instances. For example, removing an ESXi host removes its hosted VMs and the VM backups. Removing a Windows asset removes its image-level instance and any hosted application instances (e.g., Exchange or SQL), and backups of these instances.
- When a Hyper-V or VMware virtual host is removed, all backups of its VMs are also deleted. However, if you have added a vCenter server and the ESXi hosts it's managing, the VM backups are not deleted from the appliance if you remove only the vCenter server. The backups are not deleted unless you also remove the ESXi host servers.
- Hyper-V runs on a Windows server. When you add a Hyper-V server, the following assets are added:
 - The Hyper-V host (which is the Windows server that is running the Hyper-V application; asset type is *Windows*)
 - Hosted virtual machines (asset type is *Hyper-V: VM Instance*)
 - One or more Hyper-V application instances (asset type is *Hyper-V*)
 - An application instance that can be used to run image-level backups of the Windows Hyper-V host server (asset type is *Image Level Instance*)

To remove the Hyper-V server you must remove the Windows server asset.



- Windows agent – For Windows assets protected with a Unitrends agent:
 - Asset configuration settings are saved in the *master.ini* file, which is located in the \PCBP directory on the Windows system drive (e.g., C:\PCBP\). Deleting the asset from the Unitrends appliance also removes this file from the asset itself and any customized settings you have added are lost. Be sure to save the asset's

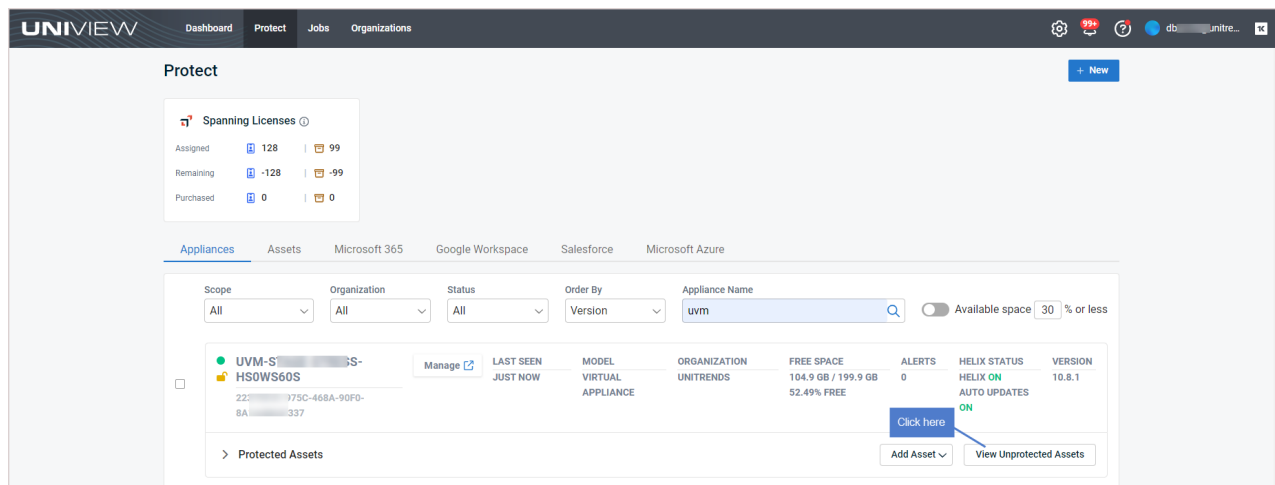
master.ini file before deleting if you think you may want to add the asset to this or another Unitrends appliance and want to use these settings. After adding the asset back to an appliance, replace the standard *master.ini* file with the one you have saved.

- If you are using Windows replicas and you remove the Windows asset while a virtual recovery is in progress, the deletion may not be instantaneous. The clean up takes time because the recovery is shut down and the virtual replica asset is removed.
- Linux agent – For Linux assets protected with a Unitrends agent, asset configuration settings are saved in the *master.ini* file (located here by default: /usr/bp/bpinit/master.ini). Deleting the asset from the Unitrends appliance also removes this file from the asset itself and any customized settings you have added are lost. Be sure to save the asset's *master.ini* file before deleting if you think you may want to add the asset to this or another Unitrends appliance and want to use these settings. After adding the asset back to an appliance, replace the standard *master.ini* file with the one you have saved.

To remove selected assets from an appliance

CAUTION! When an asset is removed, all backups of that asset are also deleted. When removing a virtual host, all backups of its VMs are also deleted. Be sure to review the "[Prerequisites and considerations for removing assets](#)" and use caution when removing an asset.

- 1 In the Appliances view, locate the appliance whose assets you will remove.
- 2 Click **Protected Assets** or **View Unprotected Assets** to view the assets you will remove. In our example, we are removing unprotected assets.



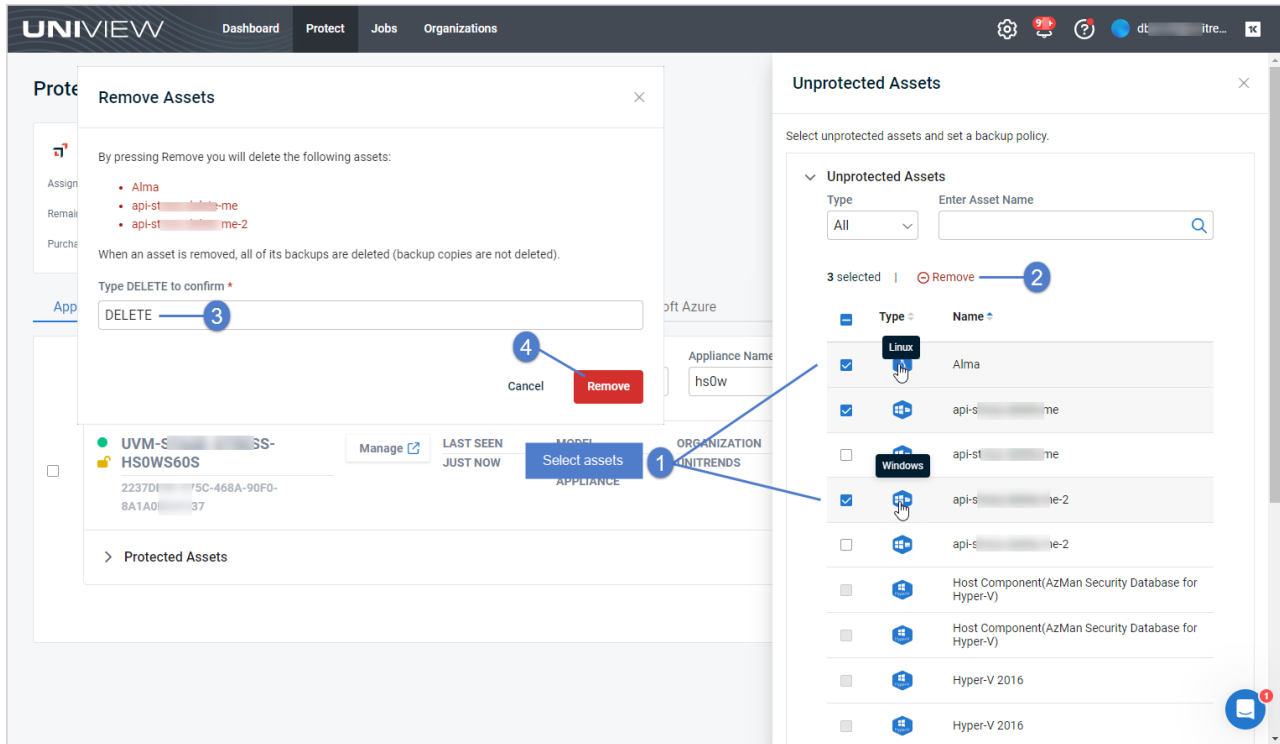
- 3 In the Unprotected Assets dialog, click to expand the assets list. Check boxes to select the assets you will remove.

You can remove these asset types (hover over the Type icon to check an asset's type):

- Windows – Use to remove a Windows asset or a Hyper-V server (for details, see "[Prerequisites and considerations for removing assets](#)")
- Linux – Use to remove a Linux asset
- VMware – Use to remove a vCenter or ESXi server

Note: Removing an asset also removes any hosted application instances and backups of those hosted instances.

- 4 Click **Remove**.
- 5 Type **DELETE** and click **Remove** to remove the assets.



Blocking or unblocking local access to an appliance

UniView enables users to restrict local access to the Unitrends appliance. The appliance UI and management functions can still be accessed through UniView. Blocking local access enforces 2FA, significantly reduces potential security exposure, and allows admins greater access controls through roles and scopes in UniView.

Once local access has been blocked, users can no longer log in directly to the appliance UI. Instead, users must connect to the appliance from UniView (as described in "[Connecting to an appliance](#)").

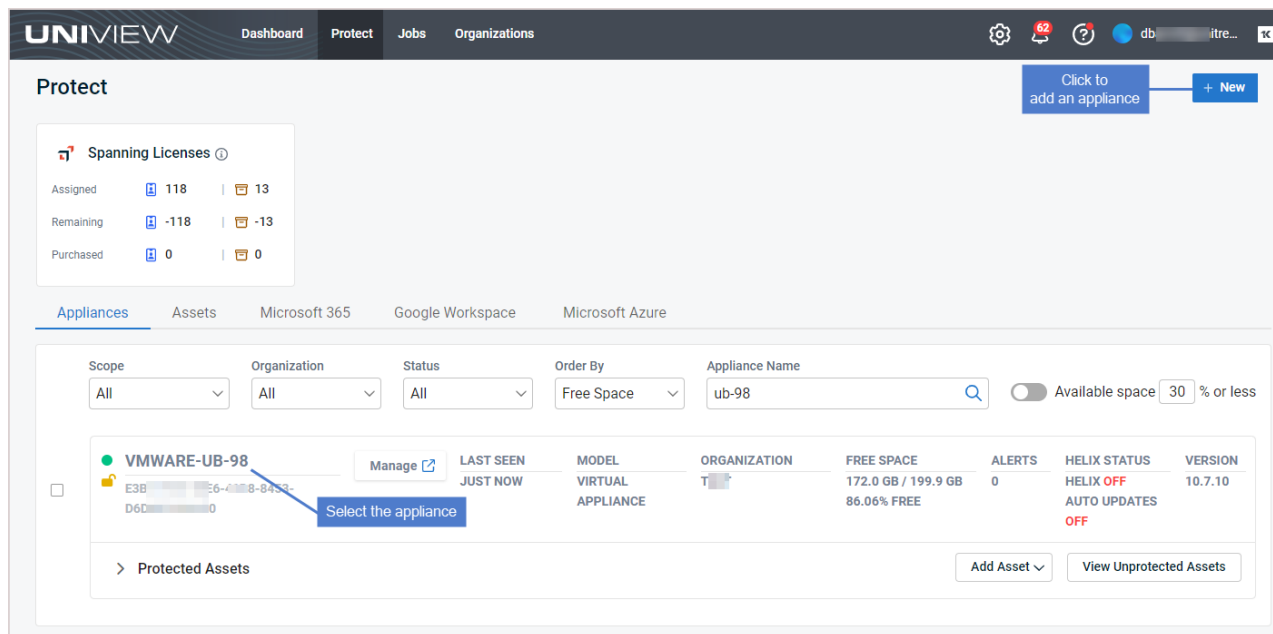
Consider the following before blocking local access:

- To block or unblock local access, you must log in to UniView as a Superuser, Admin, or Manage user. (UniView users with Monitor access cannot block or unblock local access.)
- To block or unblock local access, the Unitrends appliance must be running version 10.7.2 or higher.
- Hot backup copy to a Unitrends appliance target – To add a Unitrends appliance backup copy target to the appliance, local access must be unblocked on the backup copy target appliance. If needed, use the procedure below to unblock local access on the target appliance before adding the hot backup copy target. Once the target has been added, use the procedure below to block local access.

- iSeries protection – To protect your iSeries platform, you must log in to the appliance directly from the local network. Do NOT block local access if your appliance is protecting an iSeries environment.
- Appliance disaster recovery (DR) – Local access must be unblocked on the DR target appliance. Once you have recovered the configuration and last backups from the failed appliance, use this procedure to block local access on the target appliance.

To block or unblock local access:

- 1 In the Appliances view, click the appliance.



- 2 On the Appliance Details page, scroll down to the Settings section. In the Block Local Access tile:
 - indicates that local access is unblocked (users can access the appliance UI by entering `https://<applianceIPaddress>/ui/` in a browser on the local network).
 - indicates that local access is blocked (users must access the appliance UI by logging in to UniView and clicking the appliance's `Manage` button, as described in "Connecting to an appliance").
- 3 Do one of the following:
 - Click to block local access.
 - Click to unblock local access.

Notes:

- If the toggle is disabled () , you are using Monitor user credentials and cannot block or unblock local access.
- It may take a minute or two to block or unblock access. During this transition time, the or toggle is disabled ().

- If you see this message, you must upgrade the appliance to enable the Block Local Access feature:

Appliance version not supported
Please upgrade your appliance to enable this feature

Settings Click to log in to appliance

Block Local Access Local access is blocked. Click to unblock local access

This option will prevent local login to the appliance making it only accessible through Uniview [Read More](#)

Opening or closing a support tunnel

UniView enables you to open a secure tunnel connection to your Unitrends appliance, which Support can use to quickly troubleshoot issues. The Unitrends appliance must be running version 10.7.9 or later to use the support tunnel feature.

Use this procedure to open a support tunnel. When you're done working with Support, use this procedure to close the tunnel connection.

To open or close a support tunnel:

- In the Appliances view, click the appliance.

The screenshot shows the UniView Protect interface. At the top, there are navigation tabs: Dashboard, Protect, Jobs, and Organizations. The 'Protect' section is active, showing a 'Spanning Licenses' summary with 118 assigned, -118 remaining, and 0 purchased licenses. Below this, there are tabs for 'Appliances', 'Assets', 'Microsoft 365', 'Google Workspace', and 'Microsoft Azure'. The 'Appliances' tab is selected, displaying a table of appliances. The table has columns for Scope, Organization, Status, Order By, Appliance Name, Available space, and a table of appliance details. The appliance 'VMWARE-UB-98' is highlighted, and a blue callout box points to the 'Manage' link with the text 'Select the appliance'.

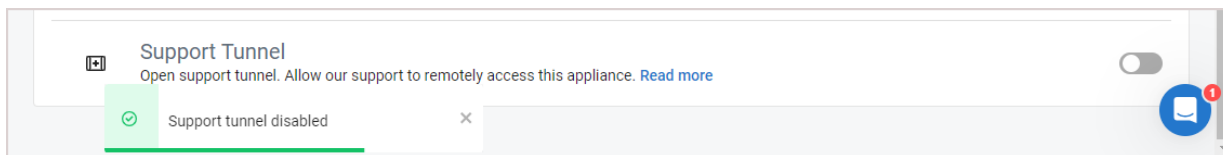
Scope	Organization	Status	Order By	Appliance Name	Available space
All	All	All	Free Space	ub-98	30 % or less


VMWARE-UB-98	Manage	LAST SEEN	MODEL	ORGANIZATION	FREE SPACE	ALERTS	HELIX STATUS	VERSION
E3B... D6D...	Select the appliance	JUST NOW	VIRTUAL APPLIANCE	T...	172.0 GB / 199.9 GB 86.06% FREE	0	HELIX OFF AUTO UPDATES OFF	10.7.10

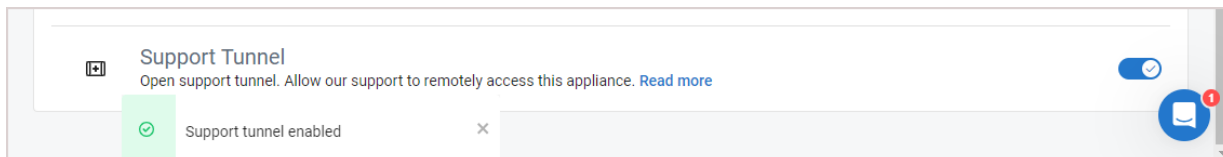
- On the Appliance Details page, scroll down to the Settings section. In the Support Tunnel tile:
 - indicates that a support tunnel is open.
 - indicates that there is no support tunnel connection to this appliance.

3 Do one of the following:


- Click  to close the support tunnel. The tunnel is closed and this message displays:



- Click  to open a support tunnel. The tunnel is opened and this message displays:



Note: If you see this message, you must upgrade the appliance to enable the Support Tunnel feature:

 **Appliance version not supported**
Please upgrade your appliance to enable this feature

Connecting to an appliance

UniView Portal supports opening multiple connections in parallel, so you can configure and manage multiple appliances from a single browser.

Use this procedure to connect to a Unitrends appliance. Repeat these steps to connect to additional appliances. Each connection opens in a separate browser tab.

To connect to an appliance:

- 1 In the Appliances view, locate the appliance and click its **Manage** button.

Protect + New

Spanning Licenses

Assigned: 118 | 13
Remaining: -118 | -13
Purchased: 0 | 0

Appliances | Assets | Microsoft 365 | Google Workspace | Microsoft Azure

Scope: All | Organization: All | Status: All | Order By: Free Space | Appliance Name: ub-98 | Available space: 30% or less

Appliance Name	LAST SEEN	MODEL	ORGANIZATION	FREE SPACE	ALERTS	HELIX STATUS	VERSION
VMWARE-UB-98	JUST NOW	VIRTUAL APPLIANCE	T	172.0 GB / 199.9 GB 86.06% FREE	0	HELIX OFF AUTO UPDATES OFF	10.7.5

Click here

Show protected assets

- 2 The appliance Login page displays in a new browser tab. Enter credentials and click **Log In**.

UniView | Login screen displays in a new tab

Kaseya

UNITRENDS

Username: root

Password: [Redacted]

Remember me

Log In

Enter credentials

1

2

Help & Support | © Kaseya 2023

Modifying Helix Auto Update settings

Helix is an intelligent SaaS remediation platform laser focused on eliminating manual tasks that IT administrators hate performing. Helix uses a SaaS delivery model to keep your Unitrends backup appliances updated, no matter where they are located.

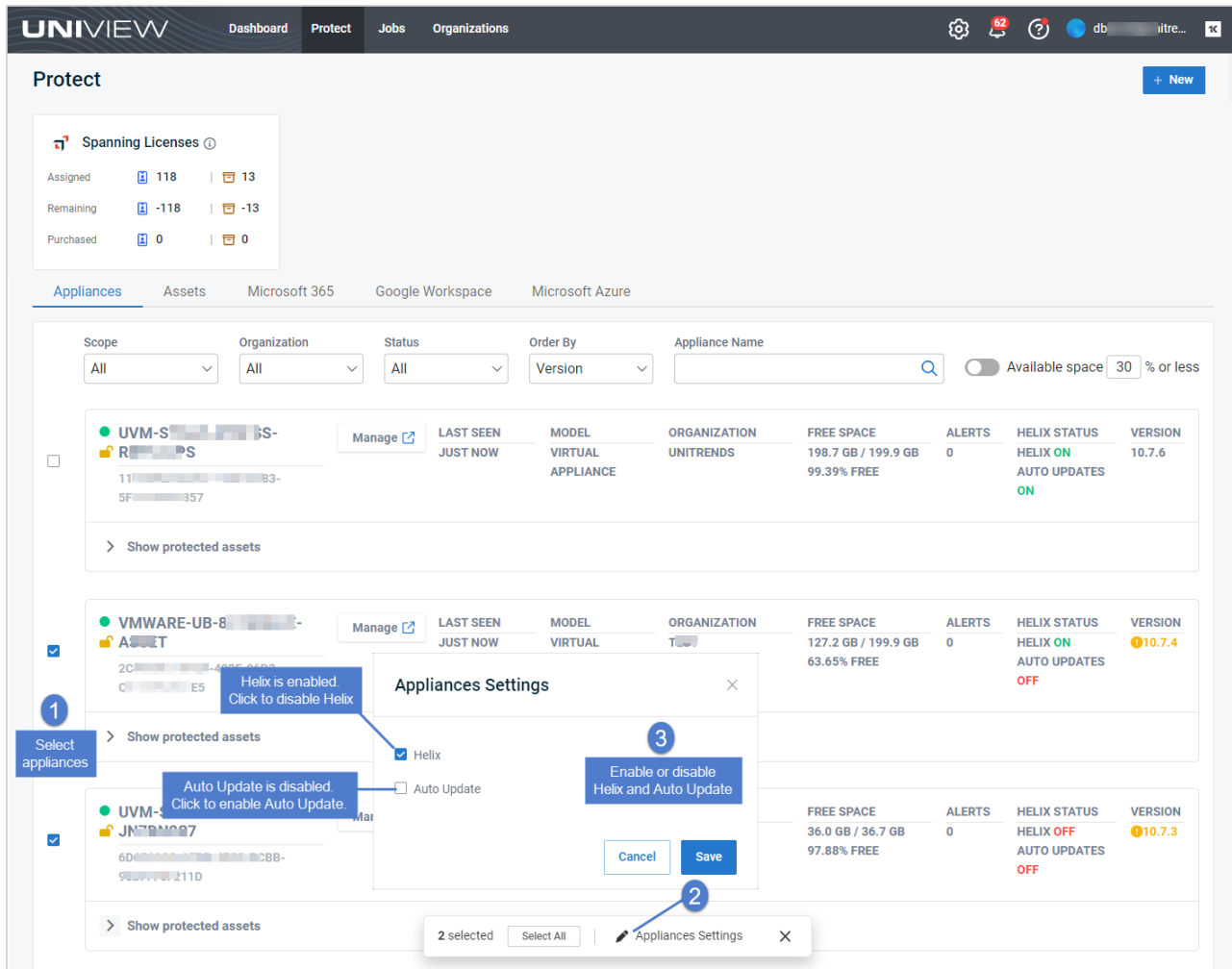
Use these steps to enable or disable Helix and the Helix Auto Update feature on one or more appliances:

- 1 In the Appliances view, check one or more boxes to select the appliances you will modify.
- 2 At the bottom of your screen, click **Appliance Settings**.
- 3 Enable or disable the Helix and Auto Update features.

Notes:

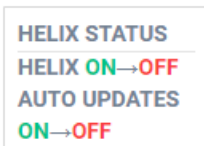
- Helix must be enabled to use the Auto Update feature. Disabling Helix also disables Auto Update.
- To use the Auto Update feature, the appliance must be running release 10.4.4 or higher and these ports must be open on the appliance:
 - 5721 outbound to IP 173.247.66.64 for the TCP and UDP protocols.
 - 443 outbound to repo.unitrends.com for the HTTPS protocol.

- 4 Click **Save**.

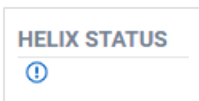


5 Helix settings are enabled or disabled for the selected appliances.

- It can take up to 20 seconds to update these settings. While updates are in progress, a transitional status displays. For example:



- If Helix is not supported on the appliance or if an error occurs, the features are not enabled. You are notified through a BackupIQ alert and this Helix status displays:



Adding an appliance

Before adding the appliance, ensure that the "Port requirements" have been met. Then use this procedure to add the appliance: "To add an appliance".

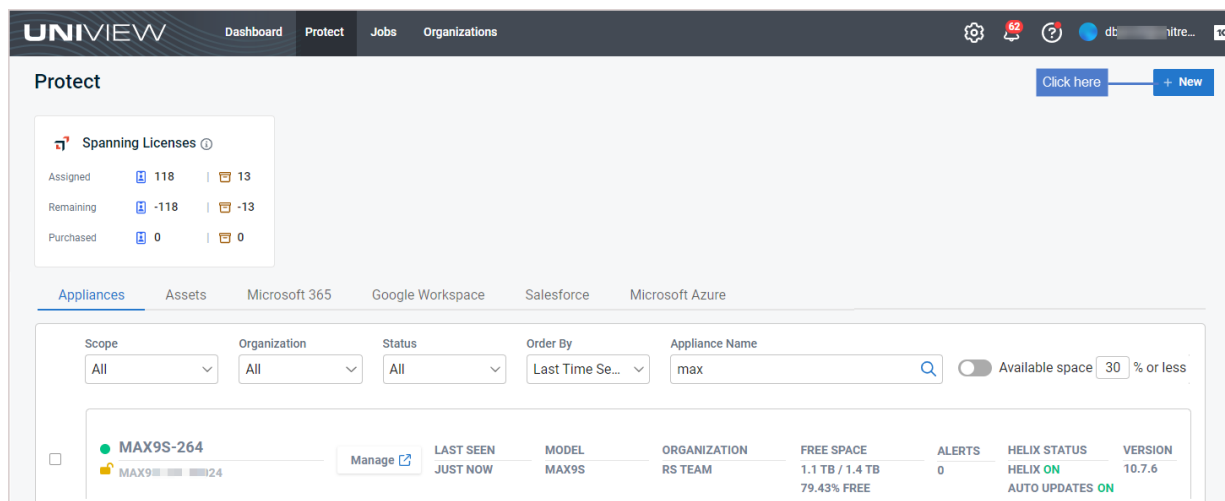
Port requirements

To enable communication between your Unitrends appliance and the UniView Portal, port 443 for the TCP and HTTPS protocols must be open outbound from the appliance to each of these locations:

- login.backup.net
- {homerealm}.backup.net
- proxy.backup.net
- api.backup.net
- download.backup.net
- index.docker.io
- hub.docker.com
- registry-1.docker.io
- production.cloudflare.docker.com
- public.ecr.aws
- *.cloudfront.net
- *.awsglobalaccelerator.com

To add an appliance

- 1 In the Appliances view, click + New.



- 2 Assign an organization to the appliance by doing one of the following:

Note: You cannot change the appliance's organization once it has been assigned. You can, however, edit the organization's name or scope at any time. To assign a different organization to an appliance, you must delete the appliance integration from UniView and the appliance UI (see "[Deleting an appliance](#)") and then add the appliance with the new organization. Backup policies must be recreated upon re-adding the appliance.

- Select an organization from the Name list.

Add A New Appliance [Close]

Choose the organization you would like to associate your new appliance with.

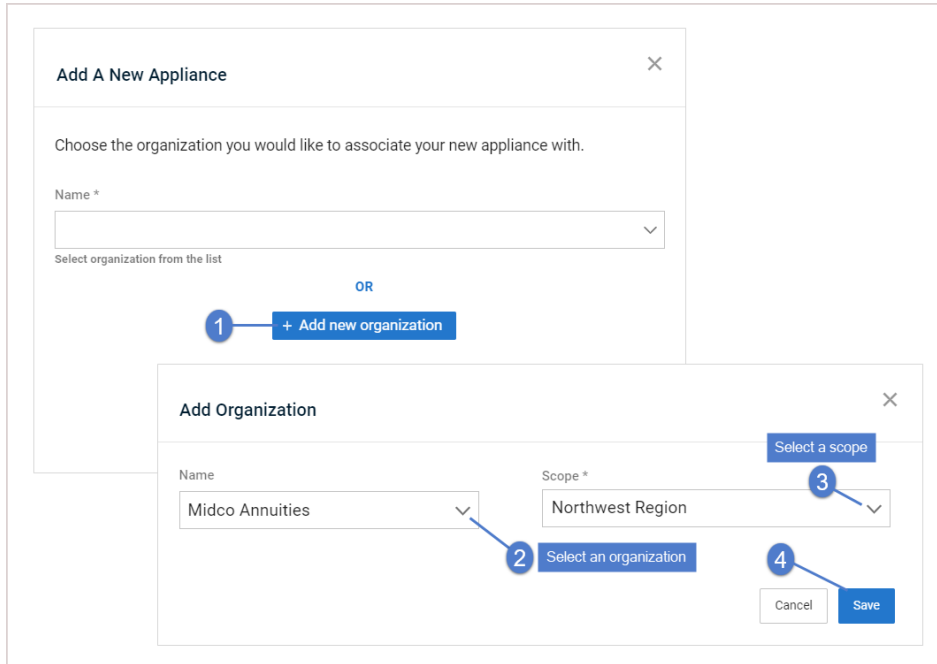
Name *

Midco Annuities
Mississippi Sax
Muddy Waters
New EBP
O'Connell - Bashirian
Old Guard Corp.
Palmers Supply
Pi t Organization

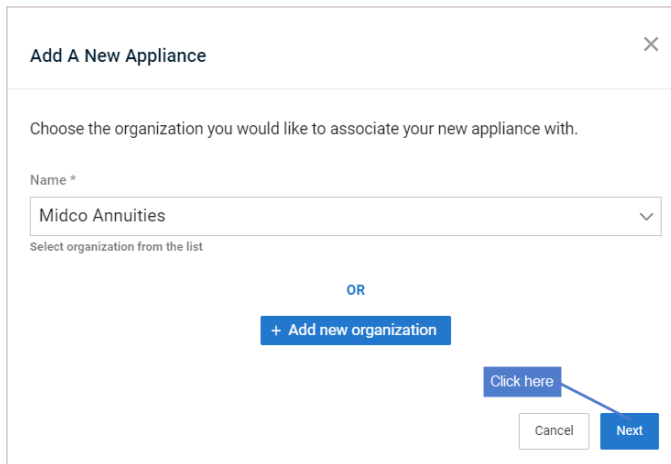
Select an organization

OR

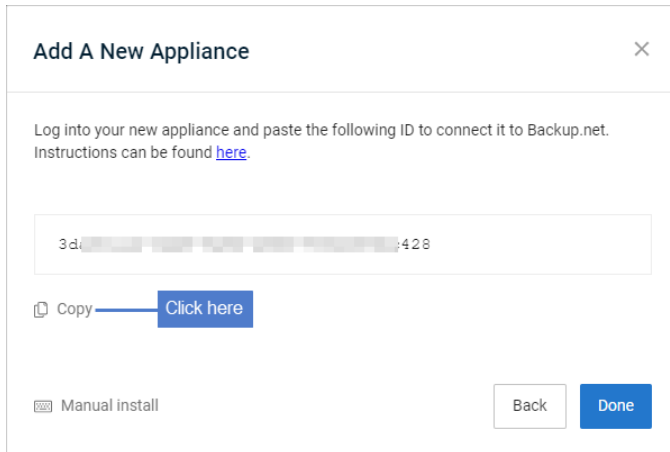
- Click **Add New Organization** and do one of the following:
 - If you have integrated your PSA system (ConnectWise Manage, Autotask, BMS, or Vorex), use the Import Organizations dialog to select an organization and scope.
 - If you have not integrated a PSA system, use the Add Organization dialog to enter the organization name, select a scope, and click **Save**.



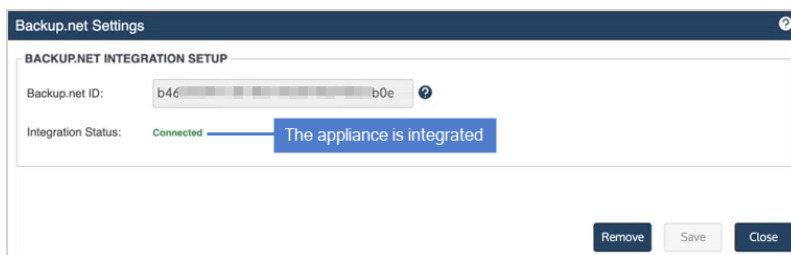
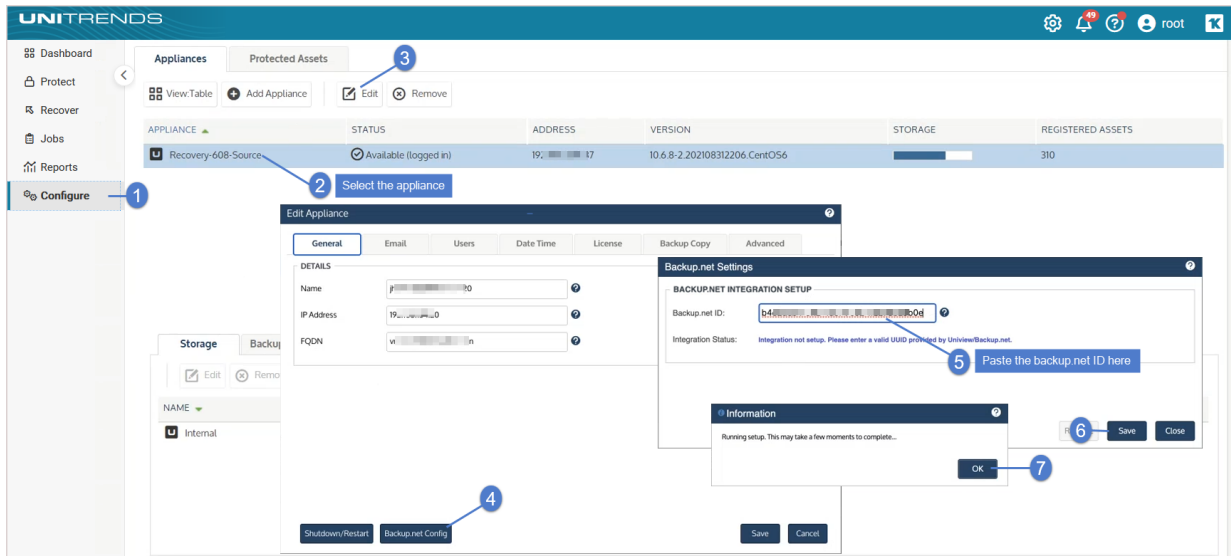
3 Click Next.



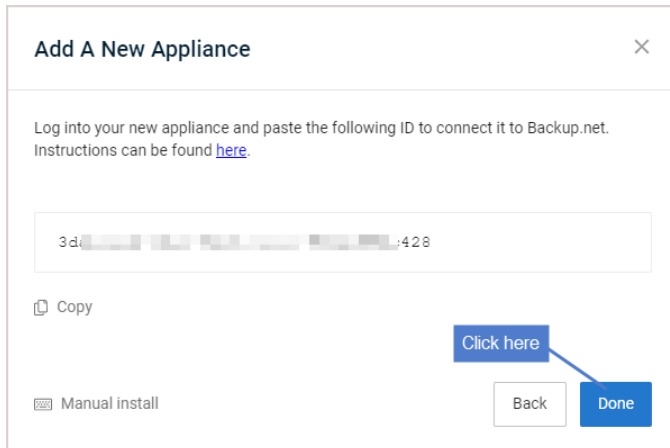
4 Copy the backup.net ID that displays. (Leave this dialog open. Do not click Done.)



- 5 Log in to the Unitrends appliance. In the Edit Appliance dialog, click **Backup.net Config**, then paste the ID into the Backup.net ID field. Click **Save**. Click **OK**.



- 6 Return to the UniView Portal. Click **Done**.



The appliance is added and displays in the Appliances list.

Notes:

- It can take a few minutes for the appliance to display in the list. If needed, refresh the page.
- For increased appliance security, the UniView Portal has a feature that blocks users from logging in directly to the appliance UI. Once local access has been blocked, users must connect to the appliance from UniView. To use this feature, see "[Blocking or unblocking local access to an appliance](#)".

Deleting an appliance

Deleting an appliance removes all of its data from the UniView Portal. Deleting the appliance does not remove or otherwise alter any of its backup data.

To delete an appliance:

IMPORTANT! Be sure to complete all steps in this procedure to ensure that the appliance integration is removed from both UniView and the appliance itself.

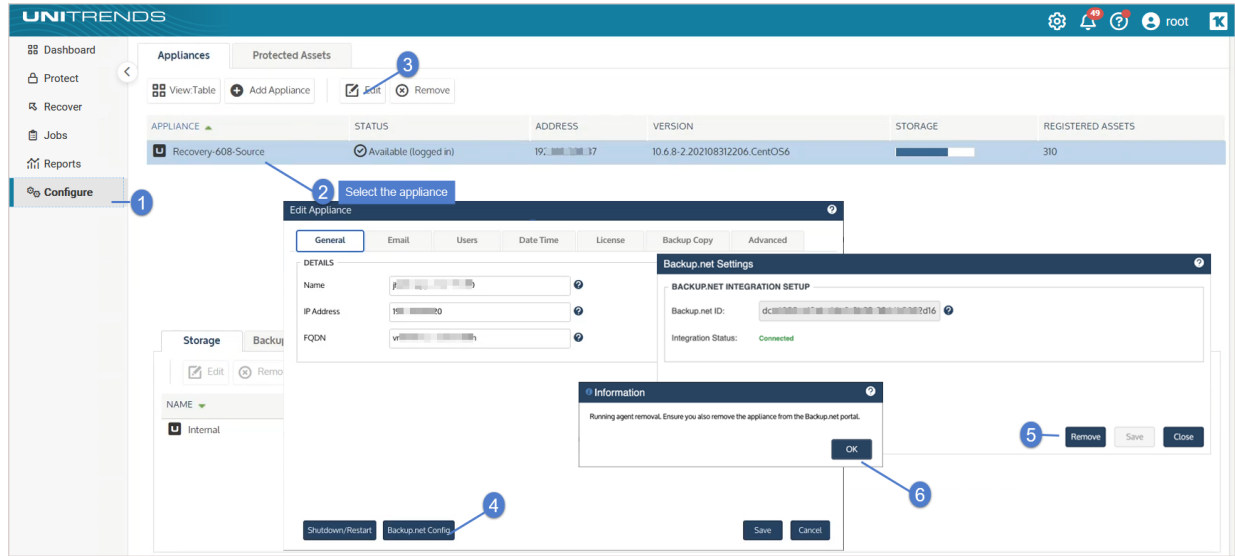
- 1 In the Appliances view, click the appliance.

The screenshot shows the UniView Protect dashboard. At the top, there are navigation tabs for Dashboard, Protect, Jobs, and Organizations. Below the navigation, there's a 'Protect' section with a '+ New' button. Underneath, there's a 'Spanning Licenses' summary showing Assigned (118), Remaining (-118), and Purchased (0). Below that, there are tabs for Appliances, Assets, Microsoft 365, Google Workspace, Salesforce, and Microsoft Azure. The 'Appliances' tab is active, showing a list of appliances with filters for Scope, Organization, Status, Order By, and Appliance Name. A search bar contains 'hv'. A table lists appliances, with the first one being 'HV-200-226'. A blue callout box points to this appliance with the text 'Click the appliance'.

- 2 On the Appliance Detail page, click . Type DELETE and click the **Delete** button.

The screenshot shows the UniView Appliance Detail page. At the top, there are navigation tabs for Dashboard, Protect, Jobs, and Organizations. Below the navigation, there's an 'Appliance Detail' section with a back arrow and a trash icon (labeled '1'). Underneath, there are tabs for Appliance Alerts, Assets, Jobs, Details, Settings, and Manage. The 'Details' tab is active, showing information for appliance 'HV-200-226', including IP address, last seen time (4 MONTHS AGO), and model. A 'Delete An Appliance' dialog box is open, showing a warning message and a confirmation prompt: 'To confirm, please type DELETE in the field below.' The input field contains 'DELETE' (labeled '2'). Below the input field, there are 'Cancel' and 'DELETE' buttons (labeled '3').

- 3 Log in to the Unitrends appliance. In the Edit Appliance dialog, click **Backup.net Config**, then click **Remove**. Click **OK**.



Viewing assets

On the Protect page, click **Assets** to switch to Assets view. The view displays the assets protected by all Unitrends appliances that have been added to your backup.net instance. Click a column heading to change the sort order of the display. To view additional pages of assets, use the scroll arrows below. (To filter the display, see "[Filtering the Assets view](#)".)

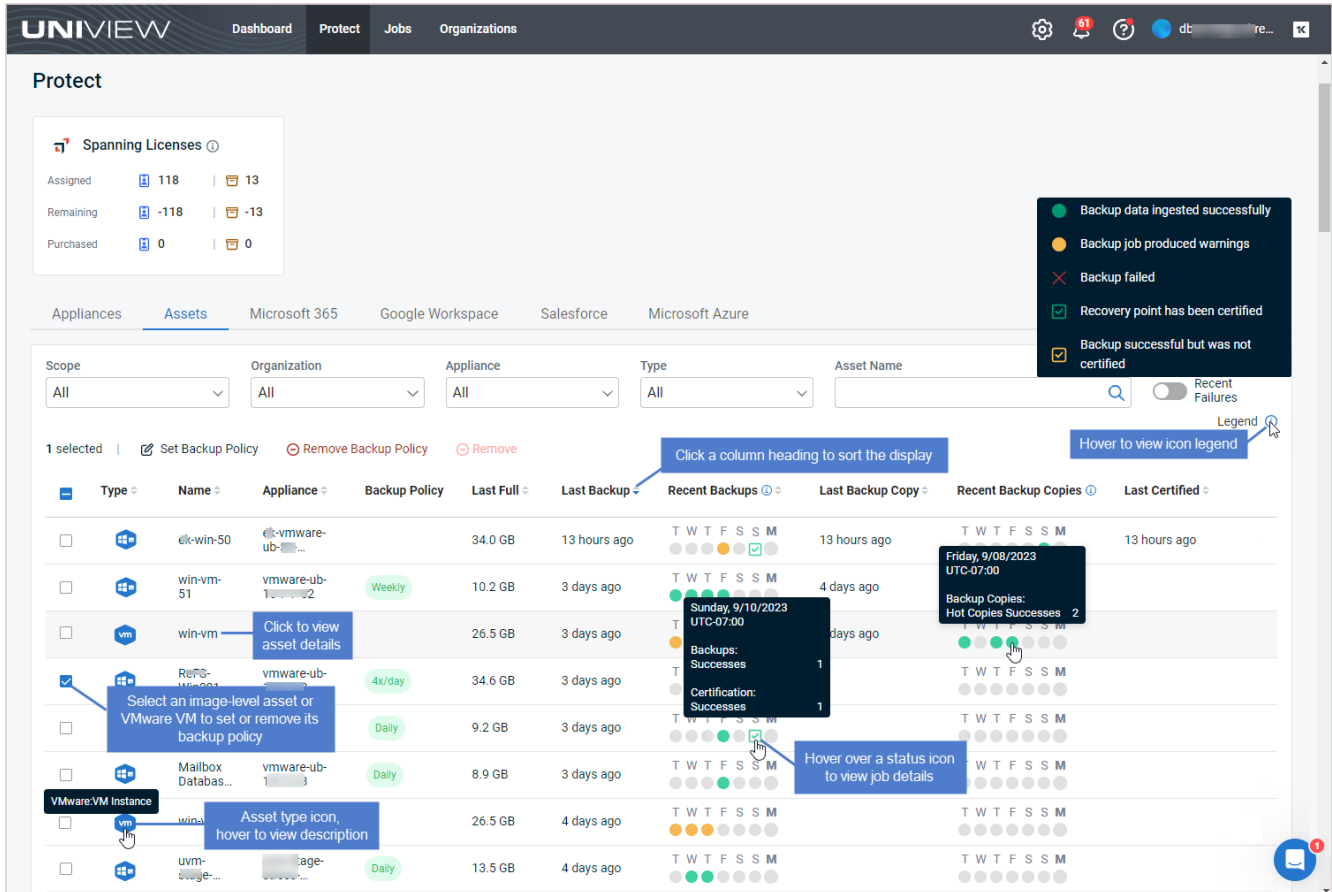
The following information is given for each asset:

- Select checkbox –
 - Use with **Set Backup Policy** or **Remove Backup Policy** to quickly modify the backup policy of one or more Windows image-level assets or VMware virtual machines. You can only select Windows image-level assets or VMware VMs that are protected by host-level backups. For details, see "[Working with backup policies](#)".
 - Use with **Remove** to quickly remove selected assets from appliances. For details, see "[Removing assets](#)".

CAUTION! When an asset is removed, all associated backups of that asset are also deleted. When removing a virtual host, all backups of its VMs are also deleted. Be sure to review the "[Prerequisites and considerations for removing assets](#)" and use caution when removing an asset.

- Type icon – Indicates the asset type. Hover over the icon for type description. Asset type examples: VMware VM Instance, Windows (file-level), Image Level Instance (Windows), Linux, SQL.
- Name – Asset name.
- Appliance – Appliance name.
- Backup Policy – Asset's backup policy: Weekly, Daily, 4x/day, Bihourly, Hourly, Custom, Appliance UI, or Error. See "[Backup policy descriptions](#)" for details.
- Last Full – Size of the last successful full backup.

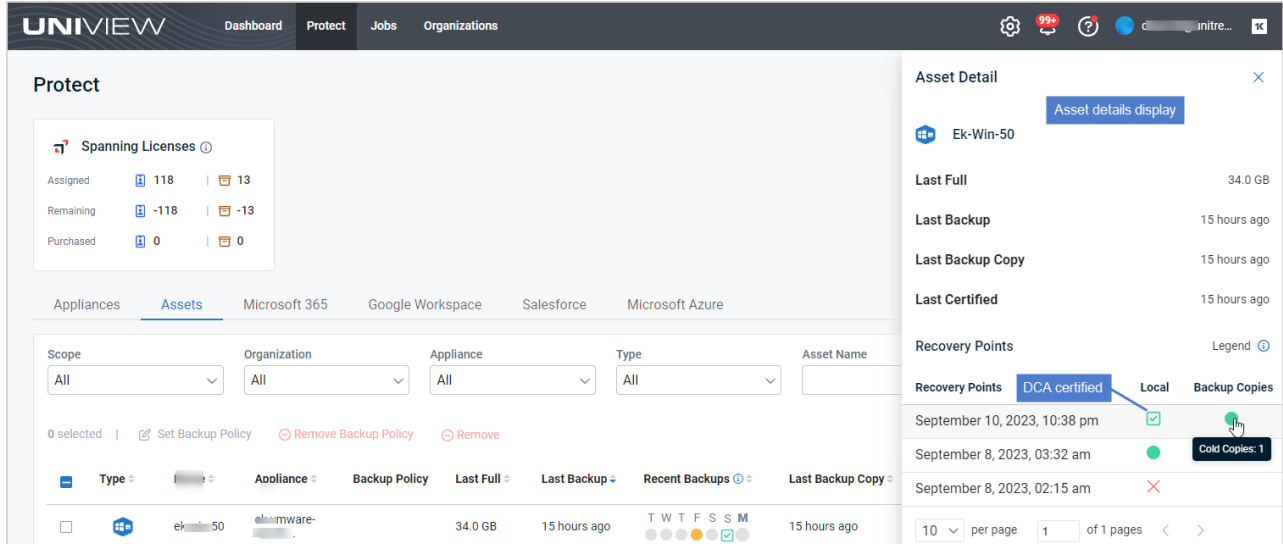
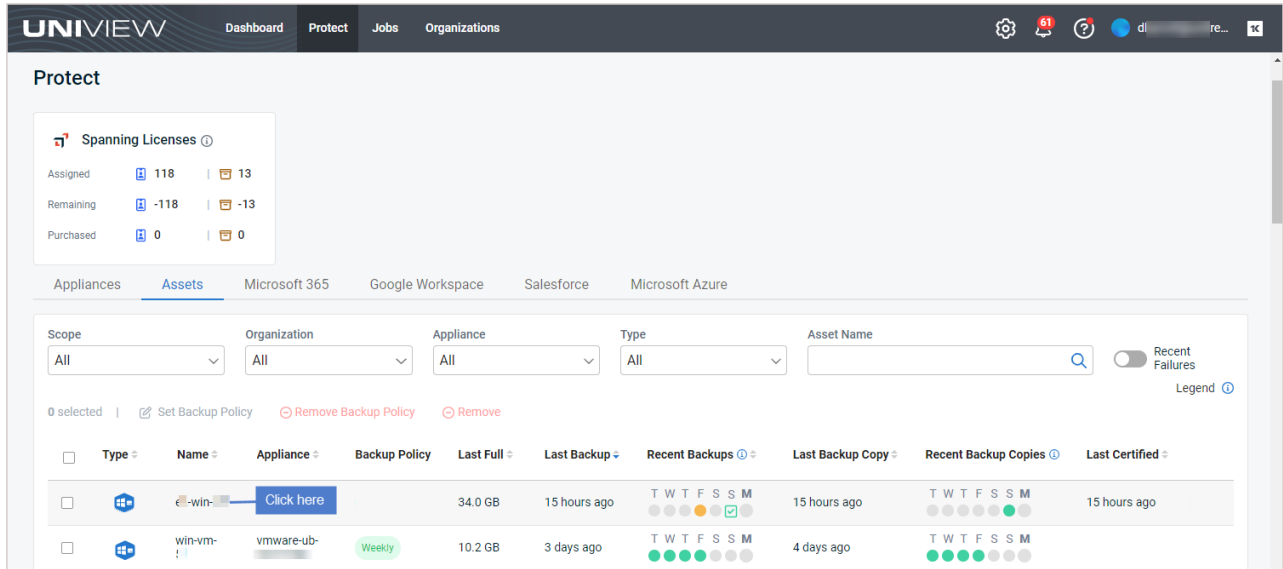
- Last Backup – Number of minutes, hours, days, weeks, or months since the last backup.
- Recent Backups – Icons indicating the status of backups over the last seven days. Hover over an icon to see job details. Click an icon to view asset details.
 - ● All backups were successful
 - ☑ Recovery point has been certified by a data copy access (DCA) job. For details, see [Recovery Assurance](#) in the [Administrator Guide for Recovery Series, Recovery MAX, ION/ION+, and Unitrends Backup](#).
 - ● One or more backups failed or ran with warnings
 - ☑ Backup was successful but was not certified
 - ✗ All backups failed
 - ● No backups were taken
- Last Backup Copy – Number of minutes, hours, days, weeks, or months since the last hot or cold backup copy.
- Recent Backup Copies – Icons indicating the status of backup copies over the last seven days. Hover over an icon to see job details (date/time and the number of hot and cold backup copies). Click an icon to view asset details.
 - ● All backup copies were successful
 - ● One or more backup copies failed or ran with warnings
 - ✗ All backup copies failed
 - ● No backup copy was taken
- Last Certified – Number of minutes, hours, days, weeks, or months since a backup has been certified by a data copy access (DCA) job.



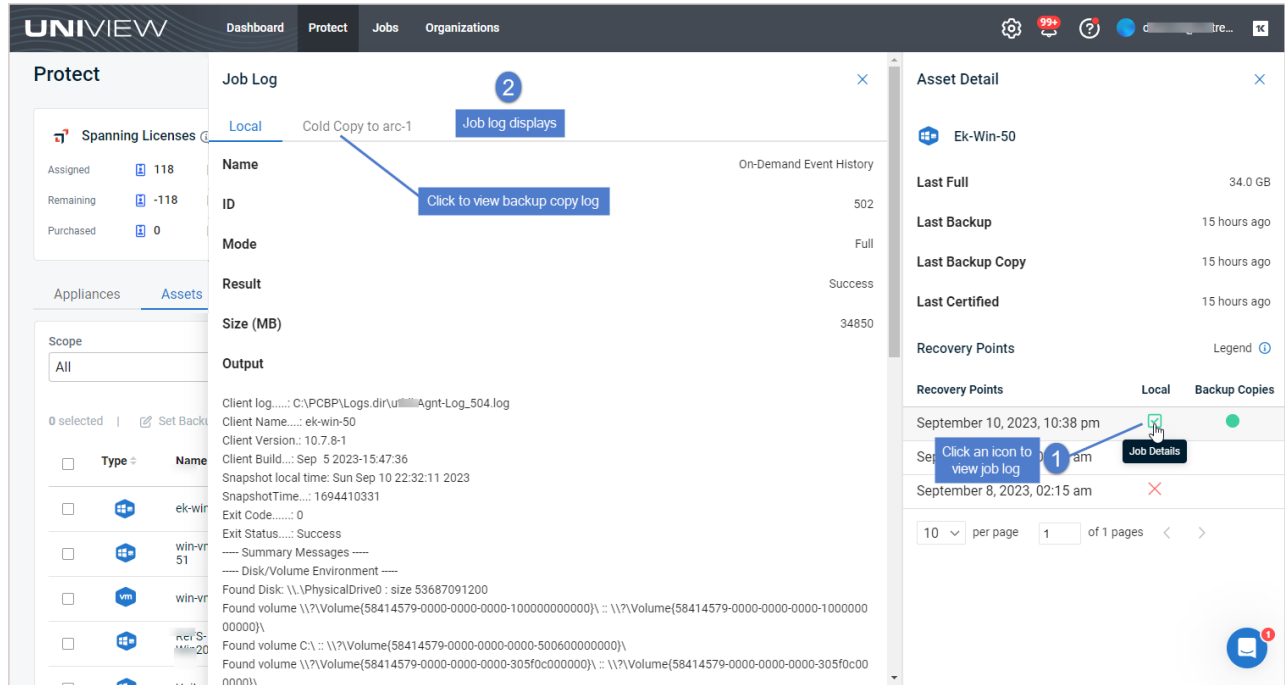
Click the asset to view these details:

- Last Full – Size of the last successful full backup.
- Last Backup – Number of minutes, hours, days, weeks, or months since the last backup.
- Last Backup Copy – Number of minutes, hours, days, weeks, or months since the last hot or cold backup copy.
- Last Certified – Number of minutes, hours, days, weeks, or months since a backup has been certified by a data copy access (DCA) job.
- Job Details – Lists jobs that are currently running or have completed in the last few minutes. Shows the job name, status, and progress bar. If a job is currently running, you may opt to click X to cancel the job. Click **See All** to view all active jobs.
- Recovery Points – Lists the asset's recovery points (local backups and backup copies) by date.
- Local – Icon indicating the status of the backup. Click an icon to view log details.
 - ● for success
 - ● for job ran with warnings
 - ● for failure

- for recovery point has been certified by a data copy access (DCA) job. For details, see [Recovery Assurance](#) in the [Administrator Guide for Recovery Series, Recovery MAX, ION/ION+, and Unitrends Backup](#).
- for DCA certification job ran with warnings.
- Backup Copies – Icon indicating whether a hot or cold backup copy was taken for the backup: ● indicates a successful copy was taken, ● indicates a copy ran with warnings, ● indicates a copy was attempted but failed, no icon indicates that no copy was taken. Hover over an icon to see the backup copy type (hot or cold).



Click a recovery point or status icon to view the job log:



Filtering the Assets view

The Assets view displays the assets protected by all Unitrends appliances that have been added to your backup.net instance.

To filter the display, enter filter criteria in any of the following:

- Scope – Select a scope from the list. (Select **All** to clear the scope filter.)
- Organization – Select an organization from the list. (Select **All** to clear the organization filter.)
- Appliance – Select an appliance from the list. (Select **All** to clear the appliance filter.)
- Type – Select one of the following to filter by asset type: AHV VM Instance, AIX, Exchange, Exchange Instance, Generic OS, Hyper-V, Hyper-V VM Instance, Image Level Instance (Windows), iSeries, Linux, Mac OS, NDMP Device, NDMP Device Instance, Novell OES, Oracle, Oracle Instance, Other OS, SCO, SharePoint, SharePoint Instance, Solaris, SQL Server, SQL Server Instance, UCS Service Profile, UCS Service Profile Instance, VMware, VMware VM Instance, Windows (file-level), Xen, or Xen VM Instance. (Select **All** to clear the filter.)
- Asset Name field – Enter a text string, then press **Enter** to apply. Asset names containing the text you entered display.
- Recent Failures – Click to slide the switch and view assets with recent failures.

Protect

Spanning Licenses

Assigned 118 | 13
Remaining -118 | -13
Purchased 0 | 0

Appliances **Assets** Microsoft 365 Google Workspace Salesforce Microsoft Azure

Scope: All Organization: All Appliance: vmware-ub-1...13 Type: All Asset Name: 20 Enter search text

0 selected | Set Backup Policy Remove Backup Policy Remove Enter filter criteria

Type	Name	Appliance	Backup Policy	Last Full	Last Backup	Recent Backups	Last Backup Copy	Recent Backup Copies	Last Certified
	EXCH2016	vmware-ub-1...13	Hourly	73.9 GB	33 minutes ago	W T F S S M T		W T F S S M T	
	RedS-Win2012R2	vmware-ub-1...13	Hourly	34.6 GB	4 days ago	W T F S S M T		W T F S S M T	
	SQL2022-WEB	vmware-ub-1...13	Daily	30.5 GB	5 days ago	W T F S S M T		W T F S S M T	
	Win-1...-200-replica	vmware-ub-1...13	Daily	41.2 GB	5 days ago	W T F S S M T		W T F S S M T	
	WIN2022-SQLSQL...	vmware-ub-1...13		17.0 MB	6 days ago	W T F S S M T		W T F S S M T	
	WIN2022-SQLSQL...	vmware-ub-1...13		48.9 GB	8 days ago	W T F S S M T		W T F S S M T	

Removing assets

UniView enables you to remove these asset types from your Unitrends appliances:

- Windows physical machines
- Linux physical machines
- vCenter or ESXi servers
- Hyper-V servers

From the Assets page, you can remove assets from multiple appliances in a single operation. Before removing an asset, review the "[Prerequisites and considerations for removing assets](#)". Then use the "[To remove assets from appliances](#)" procedure to remove assets.

Note: You can also use the Appliance page to remove assets from an appliance. For details, see "[Removing assets from an appliance](#)".

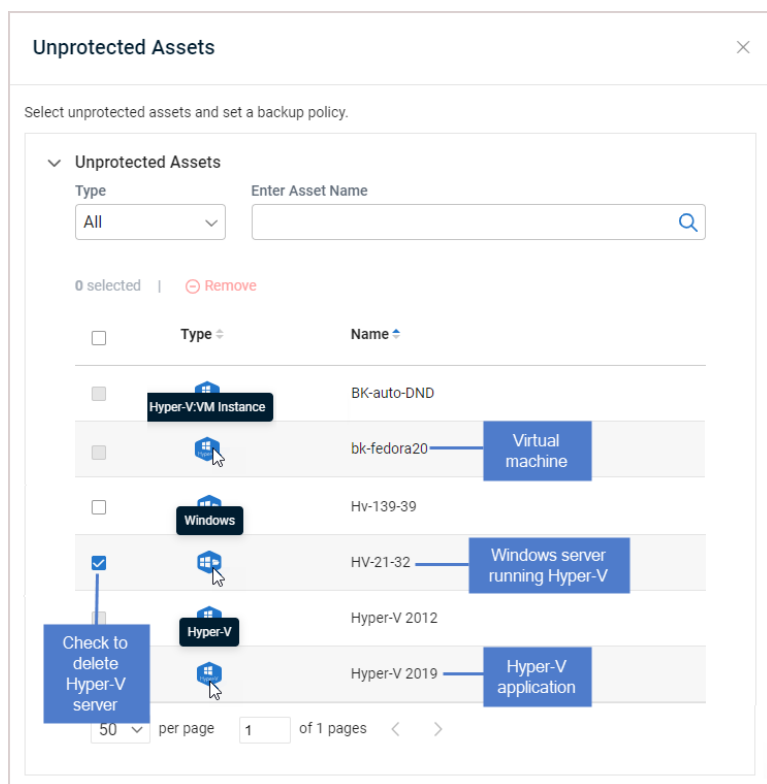
Prerequisites and considerations for removing assets

The following requirements and considerations apply:

- Before you can remove an asset, you must remove any UniView backup policy or remove the asset from any Unitrends job schedules.

- When an asset is removed, all associated backups of that asset are also deleted. Please use caution when removing an asset.
- Removing an asset also removes any associated asset instances, along with the backups of those instances. For example, removing an ESXi host removes its hosted VMs and the VM backups. Removing a Windows asset removes its image-level instance and any hosted application instances (e.g., Exchange or SQL), and backups of these instances.
- When a Hyper-V or VMware virtual host is removed, all backups of its VMs are also deleted. However, if you have added a vCenter server and the ESXi hosts it's managing, the VM backups are not deleted from the appliance if you remove only the vCenter server. The backups are not deleted unless you also remove the ESXi host servers.
- Hyper-V runs on a Windows server. When you add a Hyper-V server, the following assets are added:
 - The Hyper-V host (which is the Windows server that is running the Hyper-V application; asset type is *Windows*)
 - Hosted virtual machines (asset type is *Hyper-V: VM Instance*)
 - One or more Hyper-V application instances (asset type is *Hyper-V*)
 - An application instance that can be used to run image-level backups of the Windows Hyper-V host server (asset type is *Image Level Instance*)

To remove the Hyper-V server you must remove the Windows server asset.



- Windows agent – For Windows assets protected with a Unitrends agent:

- Asset configuration settings are saved in the *master.ini* file, which is located in the \PCBP directory on the Windows system drive (e.g., C:\PCBP\). Deleting the asset from the Unitrends appliance also removes this file from the asset itself and any customized settings you have added are lost. Be sure to save the asset's *master.ini* file before deleting if you think you may want to add the asset to this or another Unitrends appliance and want to use these settings. After adding the asset back to an appliance, replace the standard *master.ini* file with the one you have saved.
- If you are using Windows replicas and you remove the Windows asset while a virtual recovery is in progress, the deletion may not be instantaneous. The clean up takes time because the recovery is shut down and the virtual replica asset is removed.
- Linux agent – For Linux assets protected with a Unitrends agent, asset configuration settings are saved in the *master.ini* file (located here by default: /usr/bp/bpinit/master.ini). Deleting the asset from the Unitrends appliance also removes this file from the asset itself and any customized settings you have added are lost. Be sure to save the asset's *master.ini* file before deleting if you think you may want to add the asset to this or another Unitrends appliance and want to use these settings. After adding the asset back to an appliance, replace the standard *master.ini* file with the one you have saved.

To remove assets from appliances

Use this procedure to remove assets from one or more appliances.

CAUTION! When an asset is removed, all associated backups of that asset are also deleted. When removing a virtual host, all backups of its VMs are also deleted. Be sure to review the "[Prerequisites and considerations for removing assets](#)" and use caution when removing an asset.

- 1 In the Assets view, check boxes to select the assets that you will remove.

You can remove these asset types (hover over the Type icon to check an asset's type):

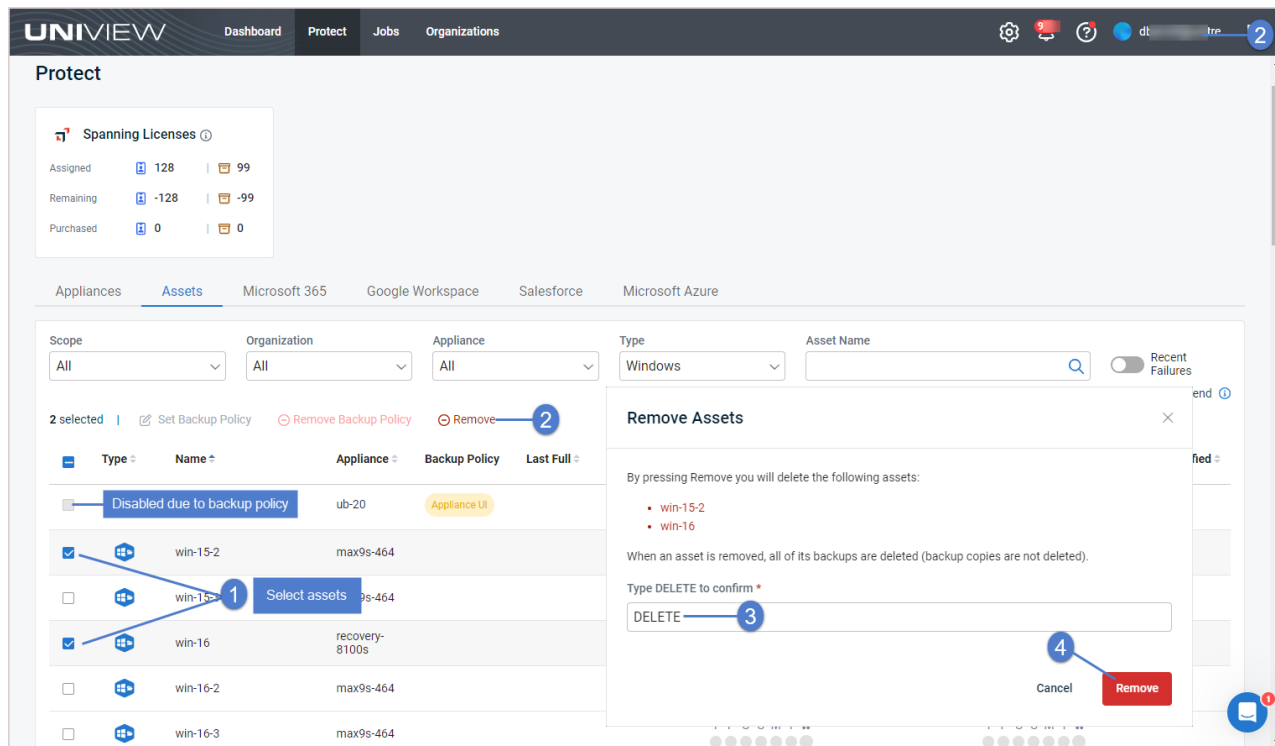
- Windows – Use to remove a Windows asset or a Hyper-V server (for details, see "[Prerequisites and considerations for removing assets](#)")
- Linux – Use to remove a Linux asset
- VMware – Use to remove a vCenter or ESXi server

Note: You can filter the assets list to quickly locate the assets to delete. In our example, we've applied a Type filter to display only Windows assets.

- 2 Click **Remove**.

Note: Removing an asset also removes any hosted application instances and backups of those hosted instances.

- 3 Type **DELETE** and click **Remove** to remove the assets.



Working with backup policies

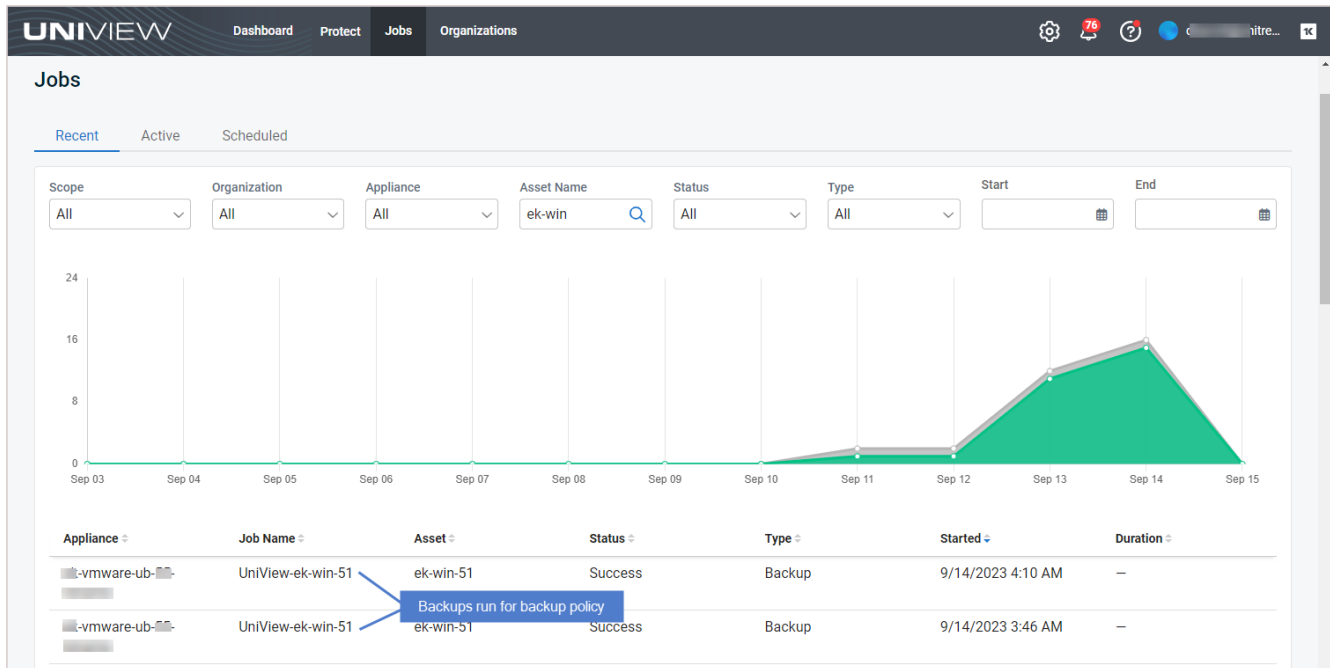
Backup policies enable you to customize your backup strategy to meet the recovery point objectives (RPOs) and recovery time objectives (RTOs) required for your business continuity plan.

From the Protect > Assets page, you can quickly view and manage the policies that define the frequency at which backups are taken for your assets—and set or remove policies for multiple assets in a single operation.

Backup policies utilize the *incremental forever* backup strategy. Once a good full backup has been taken, subsequent incrementals run to capture only the changes in the protected data since the last successful backup.

Backups initiated by a policy display on the Jobs page. They are labeled with the job name "UniView-AssetName", as shown here:

Note: For more on working with the jobs initiated by backup policies, see ["Working with Jobs"](#).



For details on working with backup policies, see these procedures:

- ["To view backup policies"](#)
- ["To select assets for backup policies"](#)
- ["To set a backup policy"](#)
- ["To remove a backup policy"](#)

To view backup policies

On the Protect page, click **Assets** to switch to Assets view. The view displays the assets protected by all Unitrends appliances that have been added to your backup.net instance. The Backup Policy column shows the asset's backup policy. Each backup policy type is described below.

Protect

Spanning Licenses ①

Assigned 118 | 13
Remaining -118 | -13
Purchased 0 | 0

Appliances Assets Microsoft 365 Google Workspace Salesforce Microsoft Azure

Scope: All Organization: All Appliance: vmware-ub-1-13 Type: All Asset Name: [Search] Recent Failures: [Toggle] Legend ①

0 selected | Set Backup Policy Remove Backup Policy Remove Backup Policy column

Type	Name	Appliance	Backup Policy	Last Full	Last Backup	Recent Backups	Last Backup Copy	Recent Backup Copies	Last Certified
EXCH2016	vmware-ub-1-13	Hourly	73.9 GB	24 minutes ago	W T F S S M T	W T F S S M T	>		
Win17-2	vmware-ub-1-13	Hourly	39.7 GB	26 minutes ago	W T F S S M T	W T F S S M T	>		
MS-Win2012R2	vmware-ub-1-13	Daily	34.6 GB	4 days ago	W T F S S M T	W T F S S M T	>		
Unitrends	vmware-ub-1-13	Daily	9.2 GB	4 days ago	W T F S S M T	W T F S S M T	>		
Mailbox Database...	vmware-ub-1-13	4x/day	8.9 GB	4 days ago	W T F S S M T	W T F S S M T	>		
SQL2022-WEB	vmware-ub-1-13	Daily	30.5 GB	5 days ago	W T F S S M T	W T F S S M T	>		
Win-1-13	vmware-ub-1-13	None	25.3 GB	5 days ago	W T F S S M T	W T F S S M T	>		
Win-1-13	vmware-ub-1-13	Weekly	25.0 GB	5 days ago	W T F S S M T	W T F S S M T	>		
Win-1-13-replica	vmware-ub-1-13		41.2 GB	5 days ago	W T F S S M T	W T F S S M T	>		

Backup policy descriptions

- Daily – A backup is taken once a day.
- Hourly – A backup is taken each hour.
- Bihourly – A backup is taken 12 times a day, at 2-hour intervals.
- 4x/day – A backup is taken 4 times a day, at 6-hour intervals.
- Weekly – A backup is taken once a week.
- Blank space – The asset is not protected by a backup policy.
- Appliance UI – The asset is protected by a backup job that was created by using the Unitrends appliance UI. You must use the appliance UI to manage the asset's backup policy (by modifying its Unitrends backup job).
- Custom – The asset is protected by a backup job that was modified by using the Unitrends appliance UI. You must use the appliance UI to manage the asset's backup policy (by modifying its Unitrends backup job).

Notes:

- Backup policies are supported only for Windows image-level assets or VMware VMs that are protected with host-level backups.
- You can use the appliance UI to remove the asset from any Unitrends jobs, then set a backup policy for the asset in UniView. Upon removing the asset from the Unitrends job, it can take some time (typically 30 minutes) to update the asset's policy in UniView. Wait until the Backup Policy changes to blank space in UniView before attempting to set a backup policy for the asset.
- For Windows image-level assets and VMware VMs, we recommend setting a policy in UniView for easier management unless you need to use advanced settings (e.g., exclusion lists and inclusion lists).

To select assets for backup policies

Checkboxes enable you to quickly set or remove backup policies for multiple Windows image-level assets and VMware virtual machines in a single operation.

Once you have selected your assets, run the "To set a backup policy" or "To remove a backup policy" procedure to set or remove the backup policy for these assets.

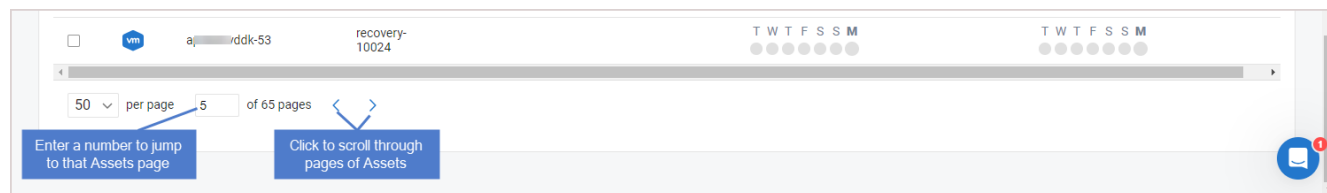
Notes:

- You can add assets from multiple pages to a single policy (use the scroll arrows below to view more pages).
- To clear your selections on all pages, reload the page.

The screenshot shows the UniView Protect interface. At the top, there are navigation tabs: Dashboard, Protect, Jobs, and Organizations. The main header is "Protect". Below it, there's a "Spanning Licenses" section with counts for Assigned (118), Remaining (-118), and Purchased (0). The main content area shows a list of assets under the "Assets" tab. The table has the following columns: Type, Name, Appliance, Backup Policy, Last Full, Last Backup, Recent Backups, Last Backup Copy, Recent Backup Copies, and Last Certified. A tooltip is visible over the "auto-centos" asset, stating "Checkbox is disabled for this AHV virtual machine".

Type	Name	Appliance	Backup Policy	Last Full	Last Backup	Recent Backups	Last Backup Copy	Recent Backup Copies	Last Certified
<input checked="" type="checkbox"/>	uvm-s-ess-rud...	uv...	Bihourly	12.9 GB	38 minutes ago	F S S M T W T		F S S M T W T	
<input type="checkbox"/>	auto-centos	ub-0		6.2 GB	an hour ago	F S S M T W T	11 days ago	F S S M T W T	
<input checked="" type="checkbox"/>	vmware-ub-9-52	vmware-ub-9-52	Daily	24.7 GB	6 hours ago	F S S M T W T	2 days ago	F S S M T W T	
<input checked="" type="checkbox"/>	VMware-VM Instance	recovery-9020s		2.3 GB	10 hours ago	F S S M T W T		F S S M T W T	
<input checked="" type="checkbox"/>	tp...	uv...	Daily	12.3 GB	11 hours ago	F S S M T W T		F S S M T W T	
<input checked="" type="checkbox"/>	Image Level Instance	uv...	Error	13.8 GB	12 hours ago	F S S M T W T		F S S M T W T	

View other pages to add more assets to the policy:



To set a backup policy

Use this procedure to create a backup policy and apply it to one or more Windows image-level assets and VMware virtual machines.

Note: If the asset already has a backup policy, this procedure updates the policy settings.



- 1 In the Protect > Assets view, check boxes to select the assets to which the policy will be applied. You can add assets from multiple pages to a single policy (use the scroll arrows below to view more pages). To clear your selections on all pages, reload the page.

Note: Backup policies are supported only for Windows image-level assets or VMware VMs that are protected with host-level backups. Do not select other asset types (see "[To select assets for backup policies](#)" above).

- 2 Click **Set Backup Policy**.
- 3 In the Set Backup Policy dialog, select the following:

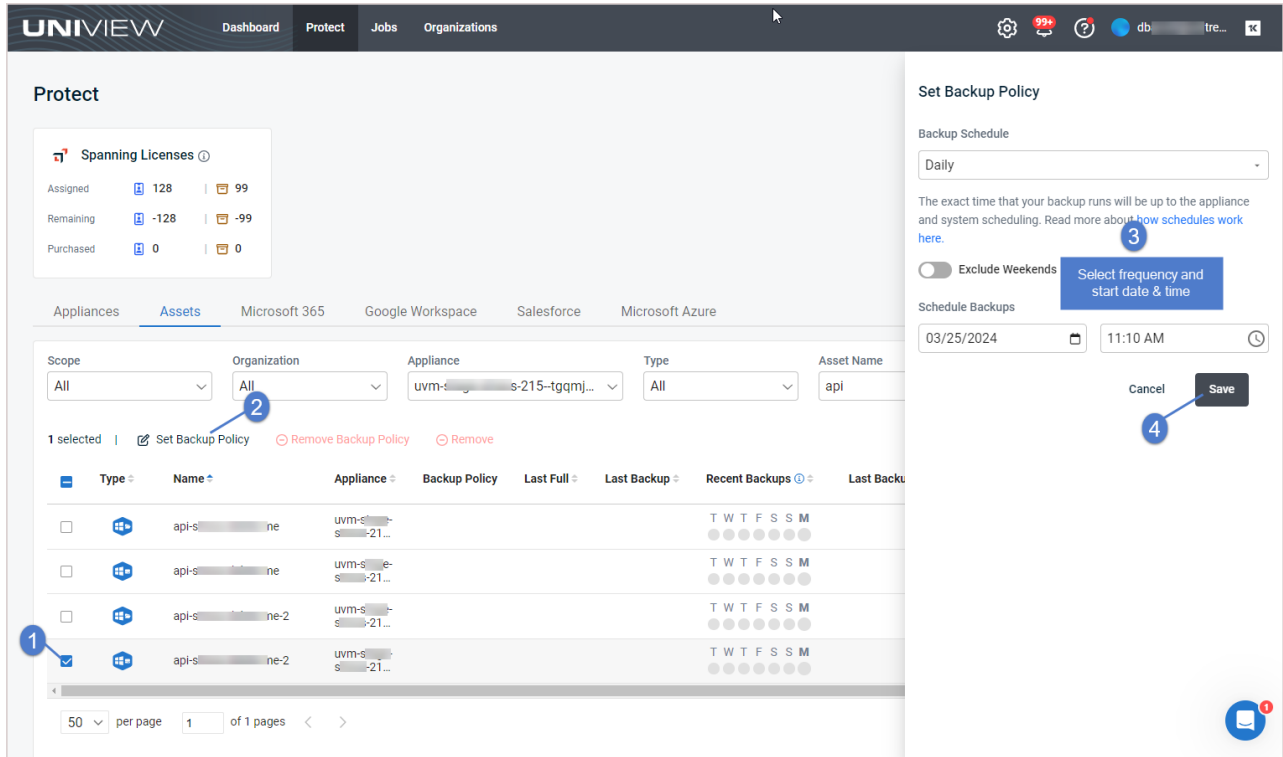
- Backup Schedule – Select a frequency from the list. (For details, see "[Backup policy descriptions](#)".)

Note: The asset's first backup is a full, which takes more time to run than subsequent incrementals. Adjust the backup frequency as needed once you have taken some incrementals.

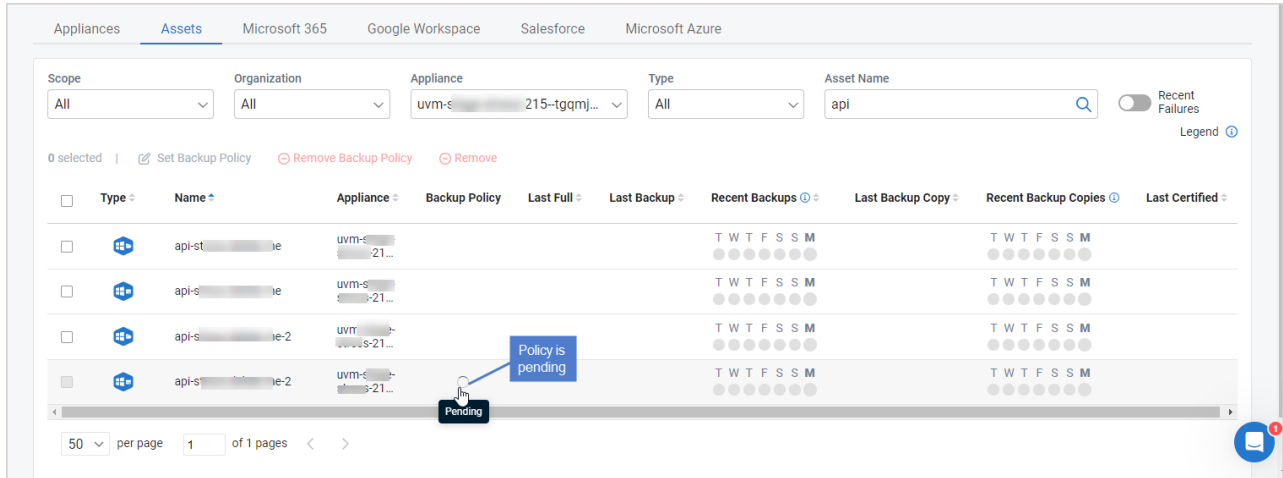
- (Optional) Exclude Weekends – Click to enable the toggle.
- Schedule Backups – Click  to select a start date, click  to select a start time.

Note: The policy's start date and time use the timezone of the Unitrends appliance.

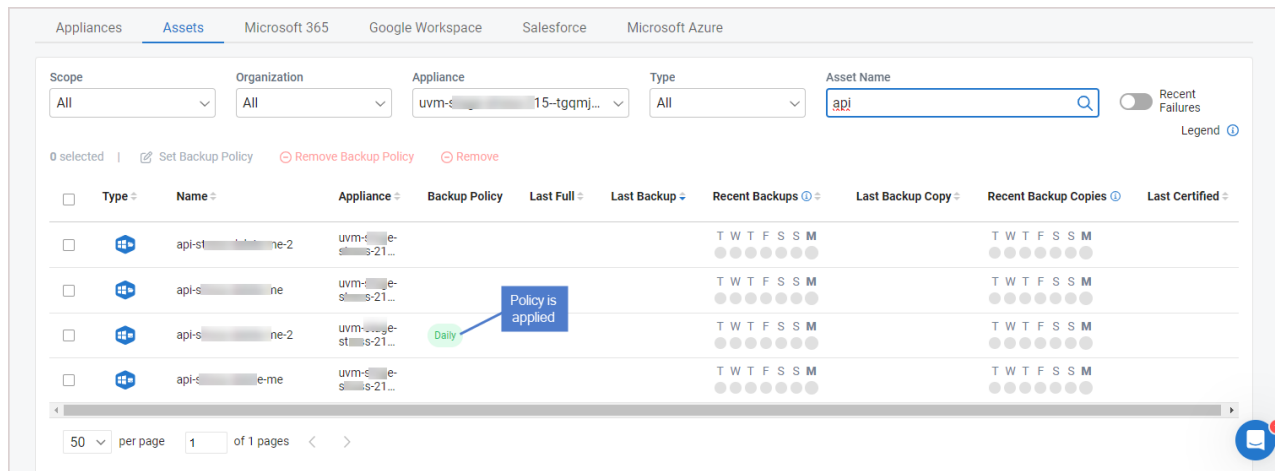
- 4 Click **Save**.



While the policy is being created, you see a spinner and the asset's checkbox is disabled. Creating the policy can take some time (typically 30 minutes).



The backup policy name displays when the policy has been applied to the asset.



To remove a backup policy

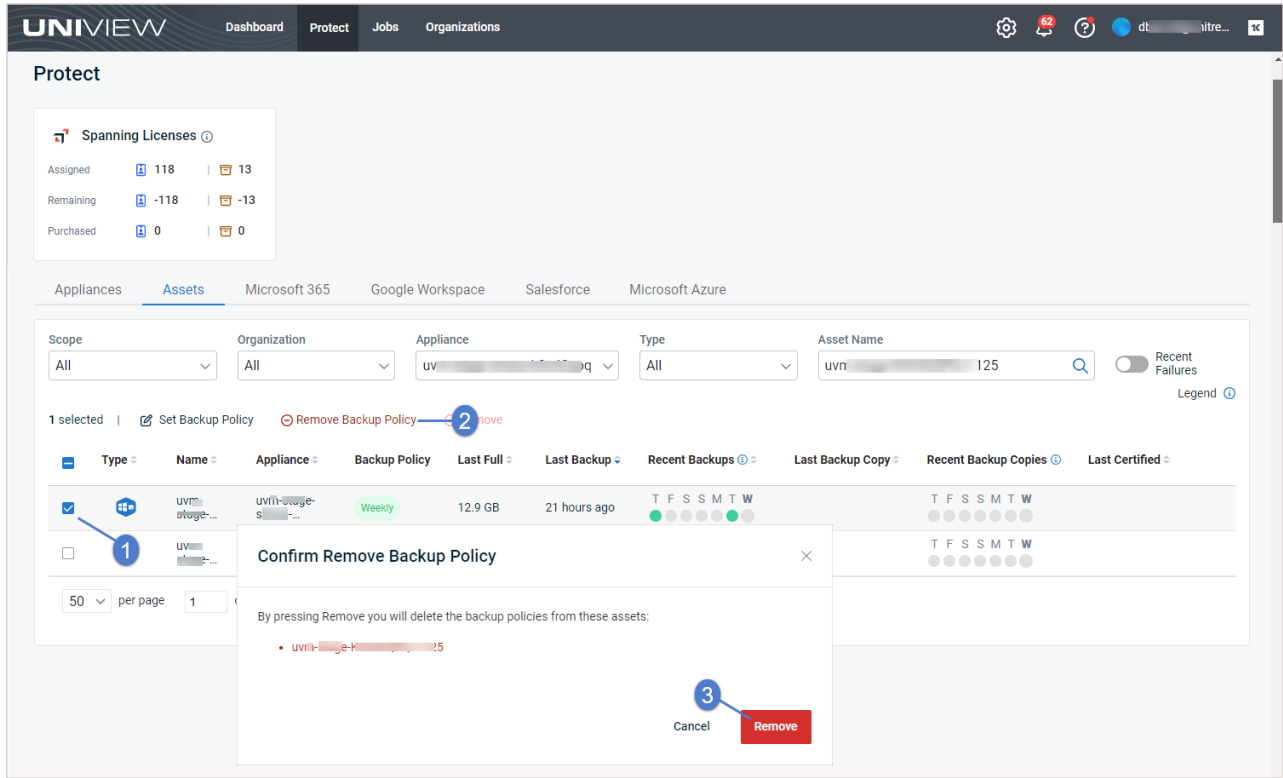
Use this procedure to remove a backup policy from one or more assets.

Note: To temporarily pause an asset's backups, see this procedure: ["Disabling or enabling a job schedule"](#).

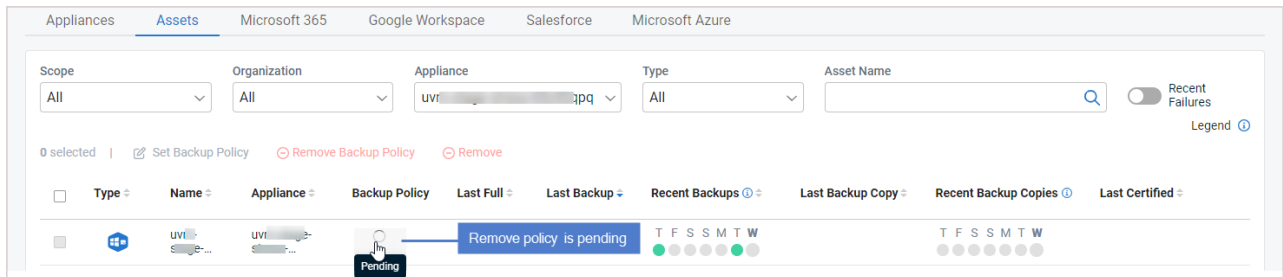
- 1 In the Protect > Assets view, check boxes to select one or more assets. You can select assets on multiple pages (use the scroll arrows below to view more pages). To clear your selections on all pages, reload the page.

Note: You cannot select an asset with the *Appliance UI* policy. The asset is protected by a backup job that was created by using the Unitrends appliance UI. You must use the appliance UI to manage the asset's backup policy (by modifying its Unitrends backup job).

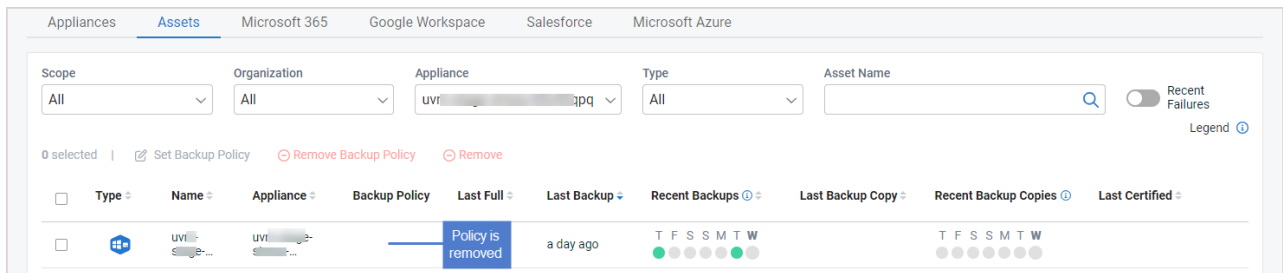
- 2 Click **Remove Backup Policy**.
- 3 Click **Remove** to confirm.



While the policy is being removed, you see a spinner and the asset's checkbox is disabled. Removing the policy can take some time (typically 30 minutes).



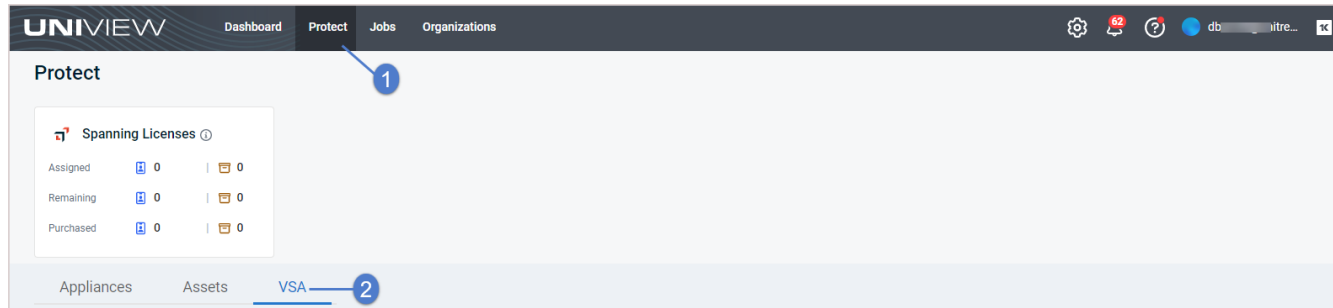
Blank space displays when the policy has been removed.



Working with VSA 9 Agents

If you have added a VSA 9 integration to your UniView Portal, VSA agent information displays in the VSA view when you launch the UniView module in the VSA interface. (The VSA view does not display when logged in directly to the stand-alone UniView Portal. For details on adding a VSA 9 integration, see ["Integrating VSA 9"](#).)

Use to view summary and status information about the VSA 9 agents installed on Unitrends appliances. To access the VSA view, click **Protect > VSA**:



See these topics for details on working in the VSA view:

Note: These procedures apply to VSA 9 only. Do not use these procedures for VSA 10.

- ["Viewing VSA 9 agents"](#)
- ["Filtering the VSA view"](#)
- ["Mapping a VSA 9 machine to a Unitrends asset"](#)
- ["Connecting to Unitrends assets with Kaseya Live Connect"](#)

Viewing VSA 9 agents

On the Protect page, click **VSA** to switch to the VSA view. This view displays the following:

- Status – VSA agent status:
 - Agent online
 - Agent online and user currently logged on
 - Agent online and user currently logged on, but user not active for 10 minutes
 - Agent is currently offline
 - Agent has never checked in
 - Agent has been suspended
- VSA Agent ID – The unique machine ID assigned to the VSA agent. The machine ID / group ID / organization ID is the account name for a managed machine in the VSA database. The agent is the client software installed on the managed machine. A one-to-one relationship exists between the agent on a managed machine and its account

name in the VSA. Tasks assigned to a machine ID by VSA users direct the agent's actions on the managed machine.

- VSA ID – Unitrends asset ID. This displays only if the VSA machine ID has been mapped to a Unitrends asset. (For details, see "[Mapping a VSA 9 machine to a Unitrends asset](#)".)
- VSA Machine Name – Name of the VSA machine where the agent is running.
- IP Addresses
- Assets

The screenshot shows the UniView Portal interface. At the top, there are navigation tabs: Dashboard, Protect, Jobs, and Organizations. The 'Protect' section is active, showing a 'Spanning Licenses' summary with 0 assigned, 0 remaining, and 0 purchased licenses. Below this, there are tabs for 'Appliances', 'Assets', and 'VSA'. The 'VSA' tab is selected, displaying a table of VSA machines. The table has columns for Status, VSA Agent ID, VSA Machine Name, IP Addresses, and Assets. There are 8 rows of data, each representing a VSA machine. The first row has a grey status icon, VSA Agent ID 861263286120167, VSA Machine Name 19...ot.kserver, IP Addresses, and Assets 0. The second row has a grey status icon, VSA Agent ID 269424728869187, VSA Machine Name 2019se...erver, IP Addresses, and Assets 0. The third row has a grey status icon, VSA Agent ID 424295965201305, VSA Machine Name desktop:...ot.kserver, IP Addresses, and Assets 0. The fourth row has a grey status icon, VSA Agent ID 284632086869212, VSA Machine Name desktop:...t.kserver, IP Addresses, and Assets 0. The fifth row has a green status icon, VSA Agent ID 761103132049688, VSA Machine Name ec2am:...ot.kserver, IP Addresses, and Assets 0. The sixth row has a grey status icon, VSA Agent ID 573415602569517, VSA Machine Name macbook:...server, IP Addresses, and Assets 0. The seventh row has a grey status icon, VSA Agent ID 134304312874031, VSA Machine Name mil:...ox.root.kserver, IP Addresses, and Assets 0. There is a search bar and dropdown menus for 'View' and 'Org/Machine Group' above the table. A chat icon is visible in the bottom right corner.

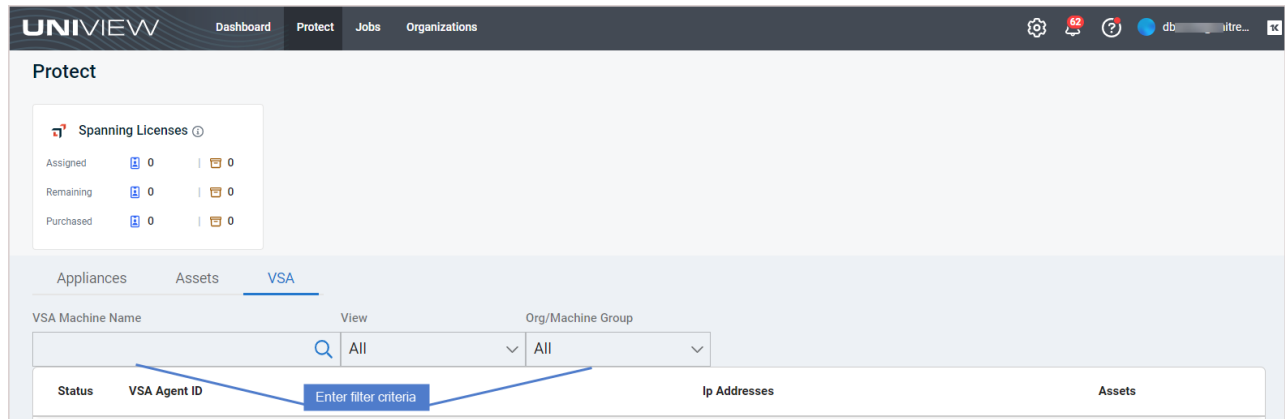
Status	VSA Agent ID	VSA Machine Name	IP Addresses	Assets
●	861263286120167	19...ot.kserver		0
●	269424728869187	2019se...erver		0
●	424295965201305	desktop:...ot.kserver		0
●	284632086869212	desktop:...t.kserver		0
●	761103132049688	ec2am:...ot.kserver		0
●	573415602569517	macbook:...server		0
●	134304312874031	mil:...ox.root.kserver		0

Filtering the VSA view

The VSA view displays all VSA 9 machines that have been added to your backup.net instance and are running the VSA agent.



To filter the display, enter filter criteria in any of the following:

- VSA Machine Name – Enter a text string, then press **Enter** to apply. VSA machine names containing the text you entered display.
- View – Select a view from the list. (Select **All** to clear the view filter.)
- Org/Machine Group– Select an organization or machine group from the list. (Select **All** to clear the filter.)



Mapping a VSA 9 machine to a Unitrends asset

You can map a VSA machine to a Unitrends asset to easily identify VSA machines in your UniView Portal environment. To create a mapping:

- 1 In the Protect > VSA view, click the machine's  and select **Map to Unitrends Asset**.
- 2 Click the asset's  and select **Map to Asset**.

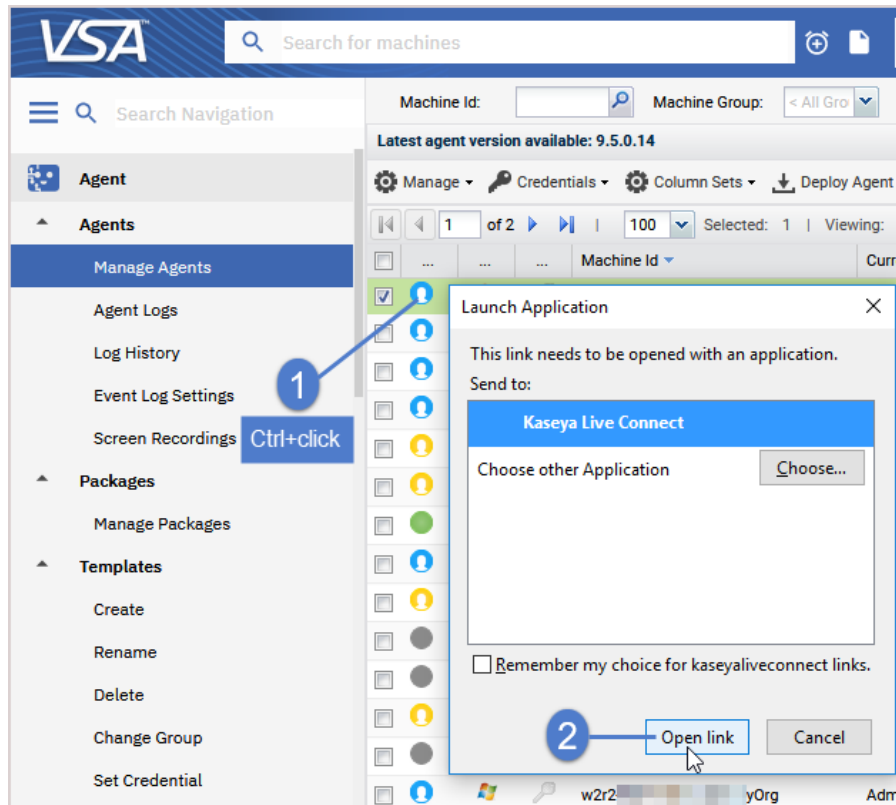
The screenshot displays the VSA interface with the following elements:


- Navigation:** 'Appliances', 'Assets', and 'VSA' tabs.
- Search and Filter:** Search bar with 'All' and 'View' dropdown with 'All' selected.
- Table:** Columns for Status, VSA Agent ID, VSA Machine Name, IP Addresses, and Assets. A row for 'kaseyavn10...helixstandard' with machine name 'Debian7_5' is highlighted.
- Modal Window:** 'Map Unitrends asset to kaseyavn10...helixstandard'. It lists assets with OS and Name columns: Debian7_5, RHEL_8, Ubuntu18, CentOS8, A_VSS_EXC-2010, NAS-NFS-NAS-RRC, A_VSS_SQL2017, and A_VSS_SQL2005.
- Callouts:**
 - 1: Clicking the menu icon for the selected agent.
 - 2: Selecting 'Map to Unitrends Asset' from the dropdown.
 - 3: Selecting 'Debian7_5' from the asset list.
 - 4: A confirmation message 'Asset is mapped' appears.

Connecting to Unitrends assets with Kaseya Live Connect

Use these steps to remote into the asset using Live Connect.

- 1 Install Live Connect on your workstation. (Skip this step if Live Connect has already been installed). To install Live Connect:
 - Log in to VSA 9 from your workstation.
 - On the Agent > Agents > Manage Agents page, **Ctrl+click** an agent icon.
 - You are prompted to download and install the Live Connect application on your local computer.



- 2 Log in to the UniView Portal.
- 3 In the Protect > VSA view, click the machine's  and select **Live Connect**.
- 4 Live Connect establishes a remote connection to the machine.

The screenshot displays the UniView Portal interface. At the top, the navigation bar includes 'Dashboard', 'Protect', 'Jobs', and 'Organizations'. The 'Protect' section is active, showing a 'Spanning Licenses' summary with 0 assigned, remaining, and purchased licenses. Below this, the 'VSA' tab is selected, displaying a table of VSA agents. The table has columns for 'Status', 'VSA Agent ID', 'VSA Machine Name', 'IP Addresses', and 'Assets'. One agent is highlighted, and a context menu is open over its IP address, with 'Live Connect' selected. A blue callout box with the number '2' points to the 'Live Connect' option, with the text 'Live Connect establishes a remote connection'. An 'Asset Info (Offline)' window is open, showing details for the selected agent, including computer name, CPU type, current user, domain, OS info, OS type, and RAM bytes.

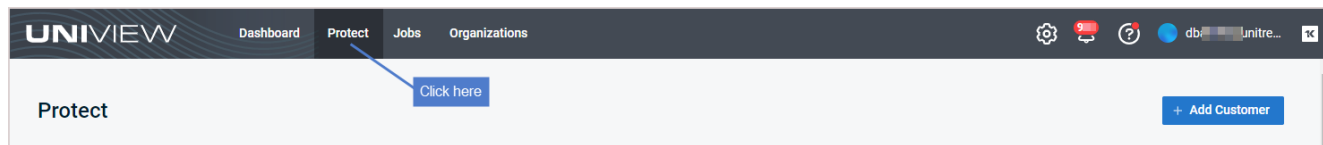
Status	VSA Agent ID	VSA Machine Name	IP Addresses	Assets
●	[Redacted]	NAS-NFS-NAS-RRC	[Redacted]-199-17	[Redacted]
●	[Redacted]	[Redacted]	[Redacted]-199-17	[Redacted]
●	[Redacted]	[Redacted]	[Redacted]	[Redacted]
●	[Redacted]	[Redacted]	[Redacted]	[Redacted]
●	[Redacted]	[Redacted]	[Redacted]	[Redacted]
●	[Redacted]	[Redacted]	[Redacted]	[Redacted]
●	[Redacted]	[Redacted]	[Redacted]	[Redacted]
●	[Redacted]	[Redacted]	[Redacted]	[Redacted]
●	[Redacted]	[Redacted]	[Redacted]	[Redacted]

Asset Info (Offline)
Computer Information

Field	Value
ComputerName	kaseyavm10
CpuType	
CurrentUser	
DomainWorkgroup	localdomain (d)
OSInfo	RecoveryOS release 7.6.1810 (Core)
OSType	Linux
RamMBytes	3881

Working with Spanning Backup

If you are running Spanning backups, you can integrate your Microsoft 365 tenants, Google Workspace domains, and Salesforce organizations to manage your backups right from the Protect page in the UniView Portal.



The Protect page includes these Spanning views:

- Microsoft 365 – Displays Spanning Backup for Microsoft 365 data for tenants that have been integrated with the UniView Portal. Use to:
 - Manage tenant/organization mappings. (Mapping a tenant to a UniView Portal organization enables BackupIQ to generate backup alerts for the domain. For details, see ["Alerts for Spanning Microsoft 365 backup"](#).)
 - Allocate licenses
 - Upgrade from a Spanning trial to a paid subscription
 - View license information, storage information, and the status of each tenant's recent backups
- Google Workspace – Displays Spanning Backup for Google Workspace data for domains that have been integrated with the UniView Portal. Use to:
 - Manage domain/organization mappings. (Mapping a domain to a UniView Portal organization enables BackupIQ to generate backup alerts for the domain. For details, see ["Alerts for Spanning Google Workspace backup"](#).)
 - Allocate licenses
 - Upgrade from a Spanning trial to a paid subscription
 - View license information, storage information, and the status of each domain's recent backups
- Salesforce – Displays Spanning Backup for Salesforce data for organizations that have been integrated with the UniView Portal. Use to manage organization mappings and to view license information, storage information, and the status of each organization's recent backups. (Mapping a Salesforce organization to a UniView organization enables BackupIQ to generate backup alerts. For details, see ["Alerts for Spanning Salesforce backup"](#).)

See these topics for details:

- ["Working with Microsoft 365"](#)
- ["Working with Google Workspace"](#)
- ["Working with Salesforce"](#)

Working with Microsoft 365

If you are using Spanning Backup for Microsoft 365, integrate your Microsoft 365 tenant to manage tenant/organization mappings, check the status of the tenant's recent backups, receive alerts for failed or partial backups, allocate licenses, upgrade from a Spanning trial to a paid subscription, and view license and storage information – right from UniView.

Start by adding the integration as described in "[Integrating a Microsoft 365 tenant](#)". Once the tenant has been added, information is synced from Spanning Backup each night. Use the Microsoft 365 view to work with this data, as described in "[Working with the Microsoft 365 view](#)".

Integrating a Microsoft 365 tenant

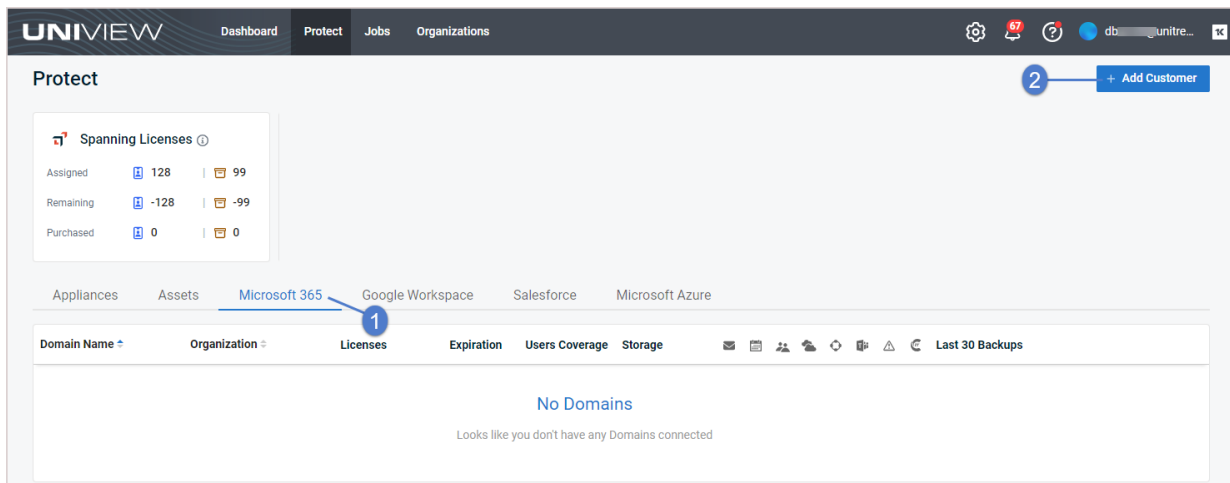
This procedure requires the following:

- A UniView account with superuser or administrator privileges
- A Microsoft 365 account with Global Admin privileges

Note: If you do not have Global Admin privileges, use this procedure to start the integration. Use the **Copy Invite Link** option to send the Global Admin a link they can use to complete the integration procedure.

To add the integration

- 1 Log in to the UniView Portal with a superuser or administrator account.
- 2 On the Protect page, click **Microsoft 365**.
- 3 Click **Add Customer**.



- 4 Select an Organization from the list.
- 5 Select the **Microsoft 365** platform.
- 6 Do one of the following:

- If you have Global Admin credentials, click **Add** and continue with this procedure to complete the integration.
- If you do not have Global Admin credentials, click **Copy Invite Link**. Then email the link to the Global Admin so that they can complete the integration.

Add Customer ×

Add a customer or provide an invite link for your customer to complete the installation process.

Organization sync is enabled. If you don't see a pre-existing organization in the list below, please make sure it exists at the source and is synced to UniView.

Organization *
212 Bronx 1

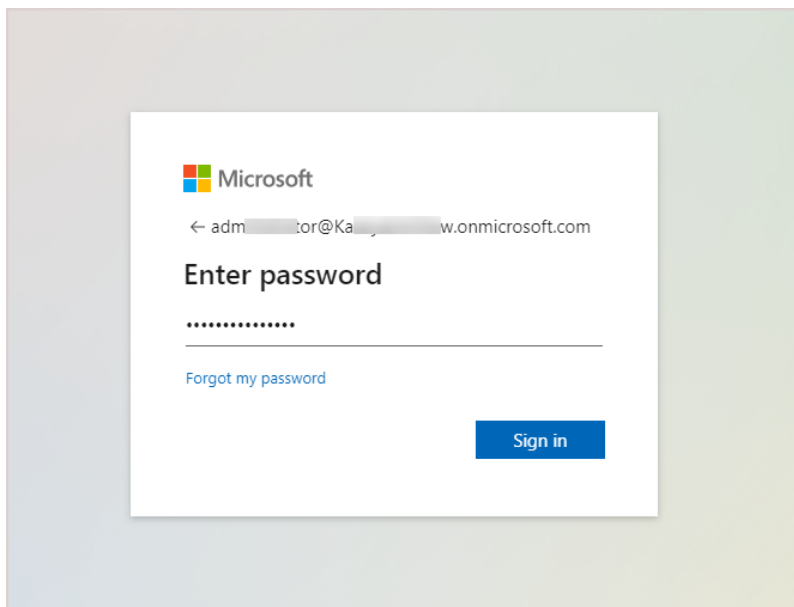
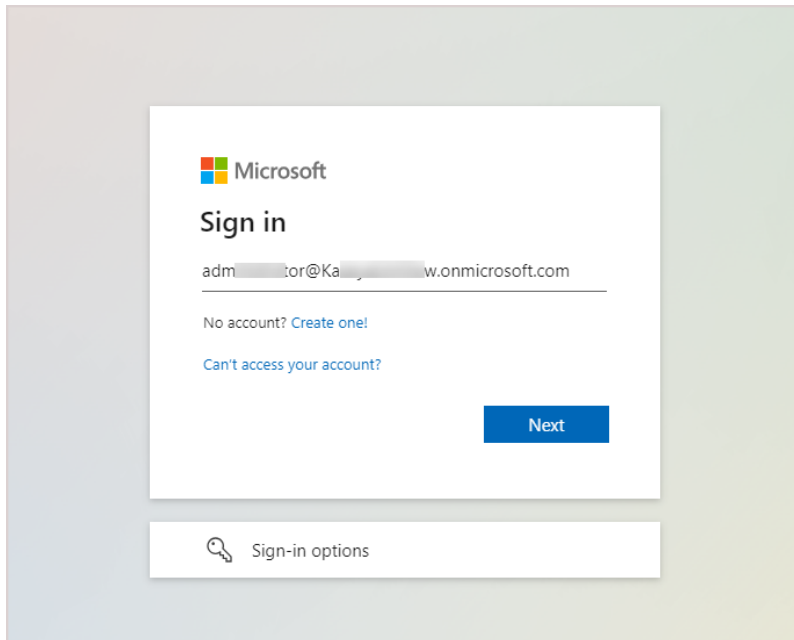
Select Platform

Microsoft 365 2
 Google Workspace
 Salesforce
 Salesforce Sandbox

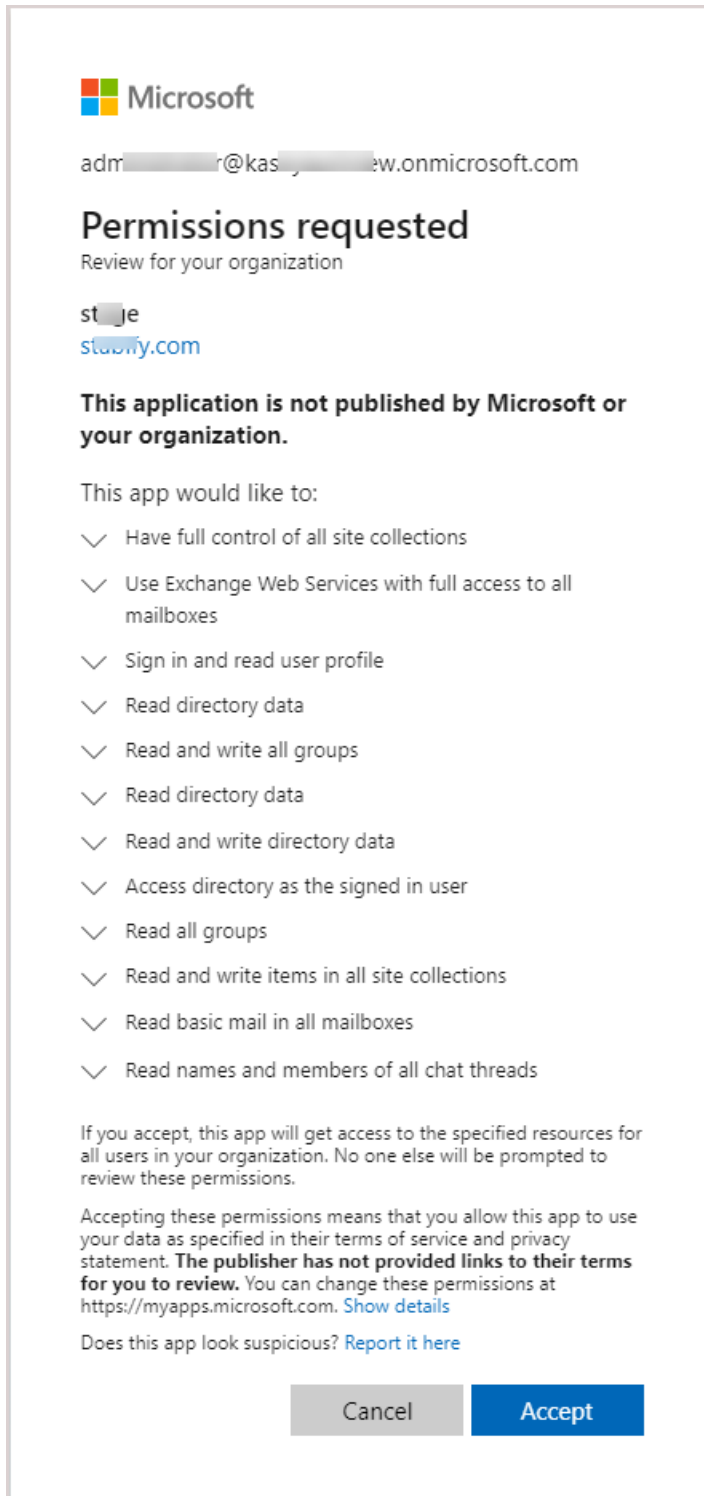
Copy Invite Link

Cancel Add 3

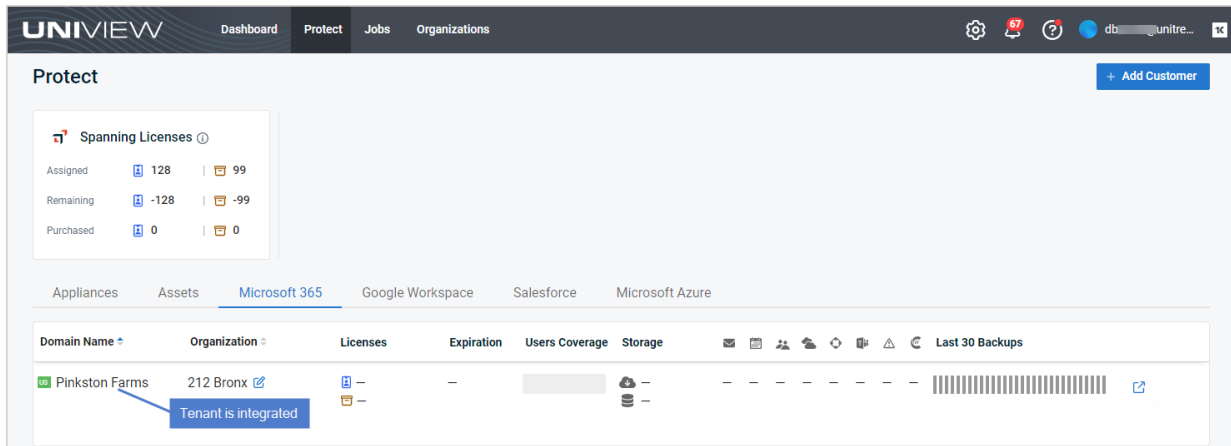
- 7 Enter your Microsoft 365 Global Admin credentials.



- 8 Click **Accept** to authorize access to your Microsoft 365 tenant.



- 9 The tenant is added and displays in the Microsoft 365 view:



- 10 Data is synced nightly from Spanning Backup to the UniView Portal. For details about this data, see ["Working with the Microsoft 365 view"](#).

Working with the Microsoft 365 view

After you have integrated your Microsoft 365 tenant, use the Protect > Microsoft 365 view to manage tenant/organization mappings, view license and storage information, allocate licenses, and check the status of a tenant's recent backups.

See these procedures for details:








- ["To view Microsoft 365 information"](#)
- ["To manage organization mappings"](#)
- ["To allocate Microsoft 365 licenses"](#)
- ["To upgrade from a Spanning Microsoft 365 trial to a paid subscription"](#)

To view Microsoft 365 information

































The following information displays in the Microsoft 365 view:






- **Spanning Licenses tile** – Shows the total number of Spanning licenses assigned, remaining, and purchased. Counts include licenses from all Spanning Backup products.
 - **Assigned** – The number of standard licenses (📄) and archived licenses (📁) that have been assigned to users.
 - **Remaining** – The number of standard licenses (📄) and archived licenses (📁) that have not yet been assigned to a user.
 - **Purchased** – The total number of Spanning Backup standard licenses (📄) and archived licenses (📁) that have been purchased.

Note: Licenses must be purchased through Spanning Backup. The UniView Portal pooled licensing feature enables you to manage how your licenses are allocated. To reallocate licenses, simply remove them from one tenant and add them to another (see ["To allocate Microsoft 365 licenses"](#)).

- Data center icon – Location of the tenant's Spanning data center. For example,  for *United States*.
- Domain Name – Name of the Microsoft 365 tenant.
- Organization – UniView Portal organization mapped to the tenant.
 - *None* indicates no organization has been mapped. To enable BackupIQ alerts for the tenant, click  and select an organization.
 - To update the mapping, simply click  and select a different organization.
 - To remove the mapping and disable BackupIQ alerts for the tenant, click  and select **X**.
- Licenses – The number of standard licenses () and archived licenses () that have been allocated to the tenant. To add or remove standard or archived licenses, modify this number by clicking  and entering a new value.

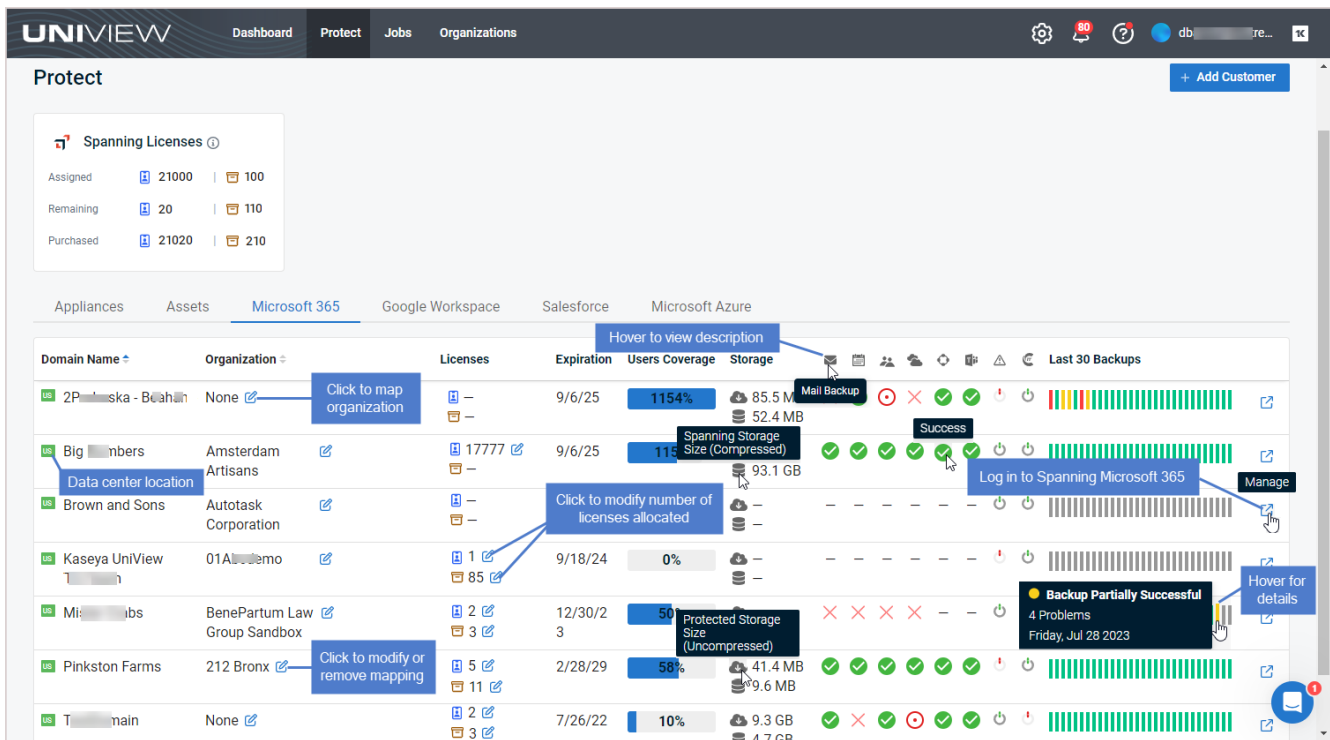
Note: When adding or removing licenses it can take some time for the new value to populate in UniView and Spanning. You cannot modify another license value until the current operation is complete.

- Expiration – License expiration date.
- User Coverage – The total number of licensed users divided by the total number of users in the domain.
- Storage – Amount of storage used.  is the amount of raw data that has been downloaded from the cloud,  is the actual amount of local storage used after compression.
-  – Status of the tenant's recent Mail Backups:  for all backups over the last 7 days were successful,  for one or more backups over the last 7 days has failed,  for one or more backups over the last 7 days was partially completed, - for no backups exist.
-  – Status of the tenant's recent Calendar Backups:  for all backups over the last 7 days were successful,  for one or more backups over the last 7 days has failed,  for one or more backups over the last 7 days was partially completed, - for no backups exist.
-  – Status of the tenant's recent Contact Backups:  for all backups over the last 7 days were successful,  for one or more backups over the last 7 days has failed,  for one or more backups over the last 7 days was partially completed, - for no backups exist.
-  – Status of the tenant's recent Drive Backups:  for all backups over the last 7 days were successful,  for one or more backups over the last 7 days has failed,  for one or more backups over the last 7 days was partially completed, - for no backups exist.
-  – Status of the tenant's recent SharePoint Backups:  for all backups over the last 7 days were successful,  for one or more backups over the last 7 days has failed,  for one or more backups over the last 7 days was partially completed, - for no backups exist.
-  – Status of the tenant's recent Teams Channel Backups:  for all backups over the last 7 days were successful,  for one or more backups over the last 7 days has failed,  for one or more backups over the last 7 days was partially completed, - for no backups exist.
-  – Error Only Email status.  indicates Error Only Email is enabled,  indicates Error Only Email is disabled.
-  – KaseyaOne status.  indicates KaseyaOne is enabled,  indicates KaseyaOne is disabled.

- Last Backups – Status of the tenant's last backup, by day. Displays status icons for the last 30 days:
 -  indicates that the last backup on this day was successful. Hover to view the date and number of problems.
 -  indicates that the last backup on this day was partially completed. Hover to view the date and number of problems.
 -  indicates that the last backup on this day failed. Hover to view the date and number of problems.
 -  indicates that there are no backups. Hover to view the date.
-  – Click to connect to Spanning Backup for Microsoft 365, where you can view error details on the Problems page. (For details, see the [Spanning Backup for Microsoft 365 Admin Guide](#).)

Notes:

- This button does not display for Monitor role users. For more on user roles, see "About UniView Portal user accounts".
- If you have Superuser, Admin, or Manage credentials and do not see this button, the feature has not been enabled in your environment.
- You can connect to only one Microsoft 365 tenant at a time.




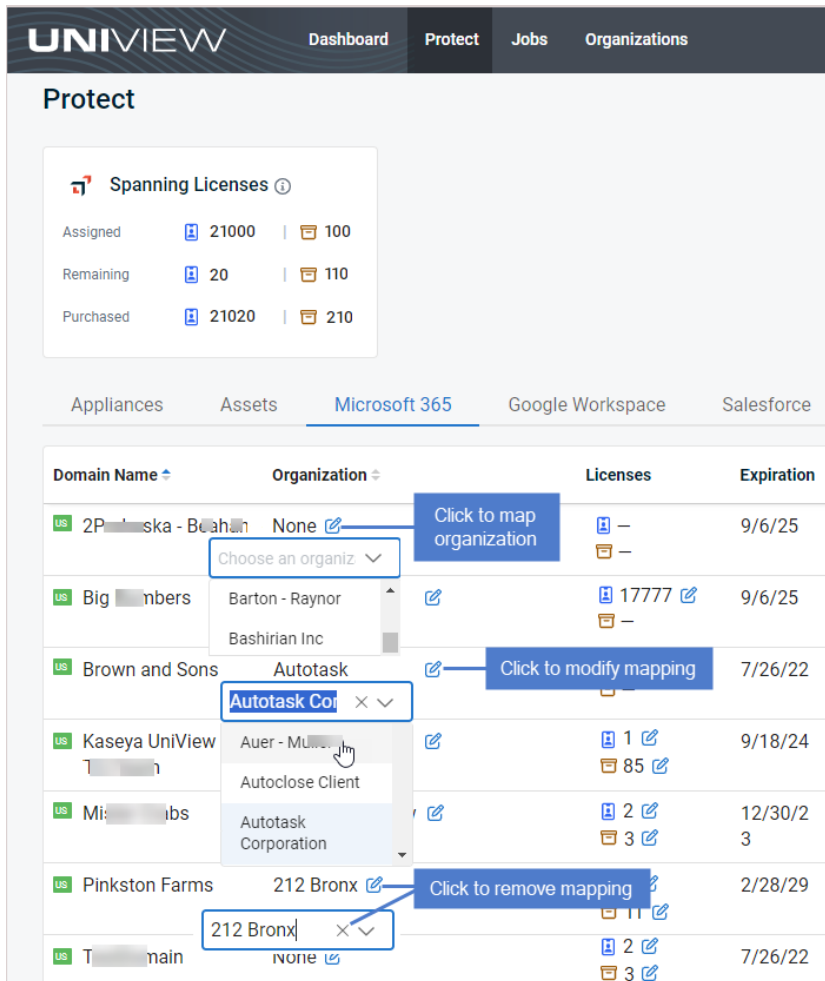
The screenshot shows the UniView Protect interface with a table of Microsoft 365 tenants. The table columns are: Domain Name, Organization, Licenses, Expiration, Users Coverage, Storage, and Last 30 Backups. Annotations include:

- Click to map organization:** Points to the organization selection icon in the Organization column.
- Hover to view description:** Points to the tooltip for the Mail Backup icon.
- Spanning Storage Size (Compressed):** Points to the storage size tooltip for the Big Members tenant.
- Log in to Spanning Microsoft 365:** Points to the external link icon in the Last 30 Backups column.
- Backup Partially Successful:** Points to a notification for the BenePartum Law Group Sandbox tenant.
- Click to modify or remove mapping:** Points to the mapping management icon in the Organization column.
- Click to modify number of licenses allocated:** Points to the license management icon in the Licenses column.
- Hover for details:** Points to the details icon in the Last 30 Backups column.

To manage organization mappings

To enable BackupIQ alerts, the tenant must be mapped to a UniView Portal organization. Use this procedure to manage these mappings.

- 1 In the Microsoft 365 view, locate the tenant whose mapping you want to add, modify, or remove.
 - The tenant name displays in the Domain column.
 - The Organization column contains either the name of the organization that has been mapped to this tenant or *None* if no organization has been mapped.
- 2 In the Organization column, click  next to the organization name and do one of the following:
 - To add a mapping and enable BackupIQ alerts for the tenant, select an organization from the list.
 - To modify the mapping, simply select a different organization from the list.
 - To remove the mapping and disable BackupIQ alerts for the tenant, select **X**.



To allocate Microsoft 365 licenses

In the Microsoft 365 view, you can easily add licenses to or remove licenses from a tenant by editing the number of Standard Licenses or Archived Licenses. You can also reallocate Spanning licenses by removing licenses from one tenant and adding them to another. The changes you make are synced to the licensing tiles in Spanning Backup for Microsoft 365.

Note: Licenses must be purchased through Spanning Backup. The UniView Portal pooled licensing feature enables you to manage how your licenses are allocated only.



The following steps show how to reallocate licenses. In our example, we will remove 5 licenses from tenant *Pinkston Farms* and add them to tenant *Mister Crabs*.

- 1 Tenant *Pinkston Farms* has 25 standard licenses. Tenant *Mister Crabs* has 3 standard licenses.

The screenshot shows the UniView Portal interface for Microsoft 365 licensing. The 'Spanning Licenses' summary shows 21000 Assigned, 20 Remaining, and 21020 Purchased licenses. The table below lists tenants and their license counts:

Domain Name	Organization	Licenses	Expiration	Users Coverage	Storage	Last 30 Backups
Mister Crabs	Crown Coffee	3 Standard, 2 Archived	12/30/23	50%	85.5 MB / 52.4 MB	Backup status icons
Pinkston Farms	212 Bronx	25 Standard, 13 Archived	2/28/29	58%	88.8 PB / 93.1 GB	Backup status icons



A callout box points to the '25' in the Licenses column for Pinkston Farms, labeled 'Current standard license allocation'.

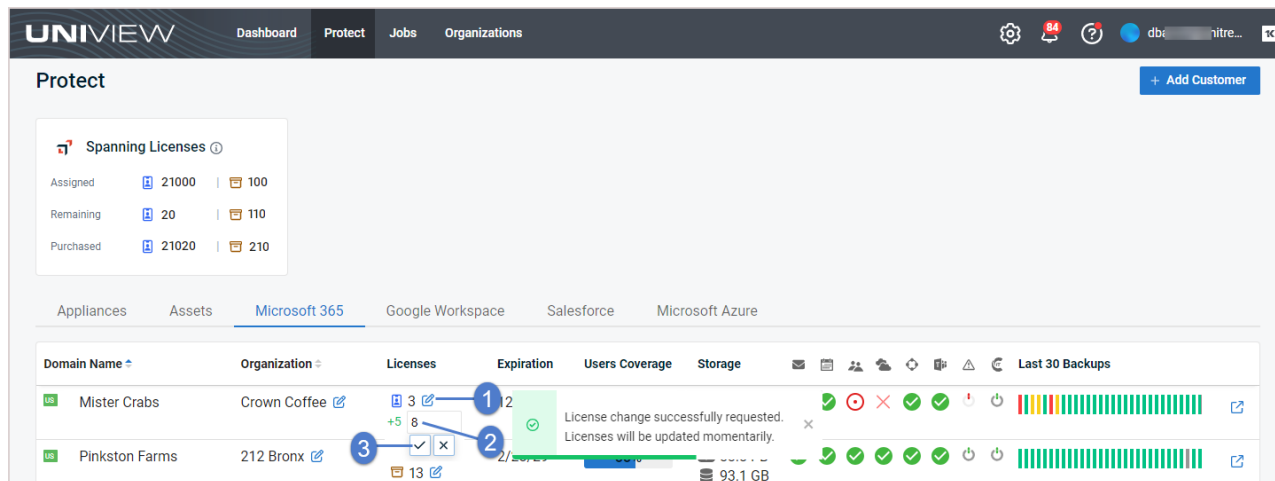
- 2 For tenant *Pinkson Farms*, click , change the number of standard licenses to 20, and click  to save.

The screenshot shows the UniView Portal interface with the license change process in progress for Pinkston Farms. The license count is updated to 20 Standard and 13 Archived. A confirmation message is displayed:

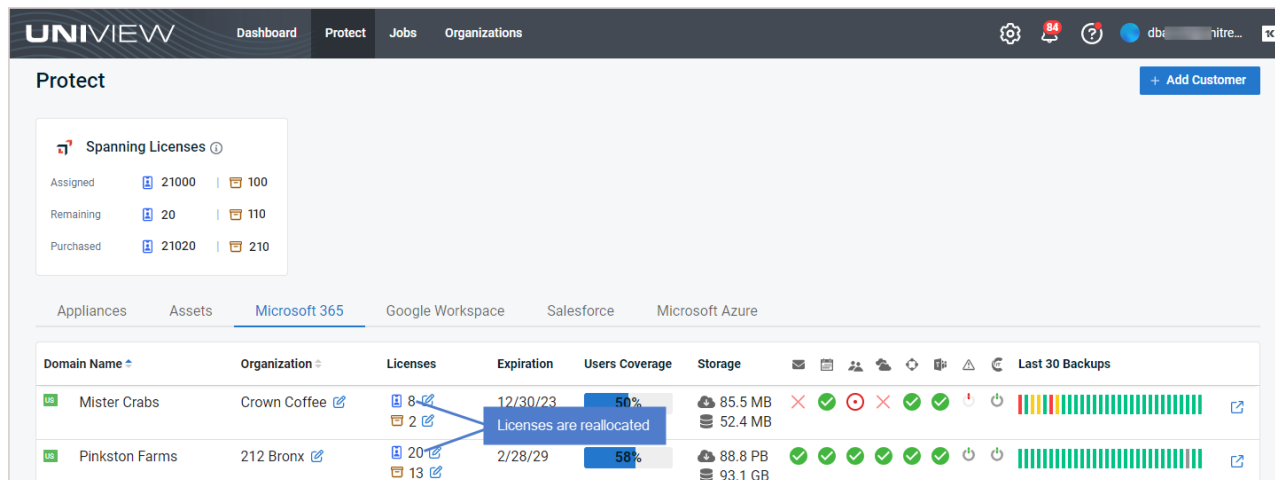
License change successfully requested. Licenses will be updated momentarily.

Numbered callouts indicate the steps: 1 points to the license count, 2 points to the save button, and 3 points to the edit button.

- 3 For tenant *Mister Crabs*, click , change the number of standard licenses to 8, and click  to save.



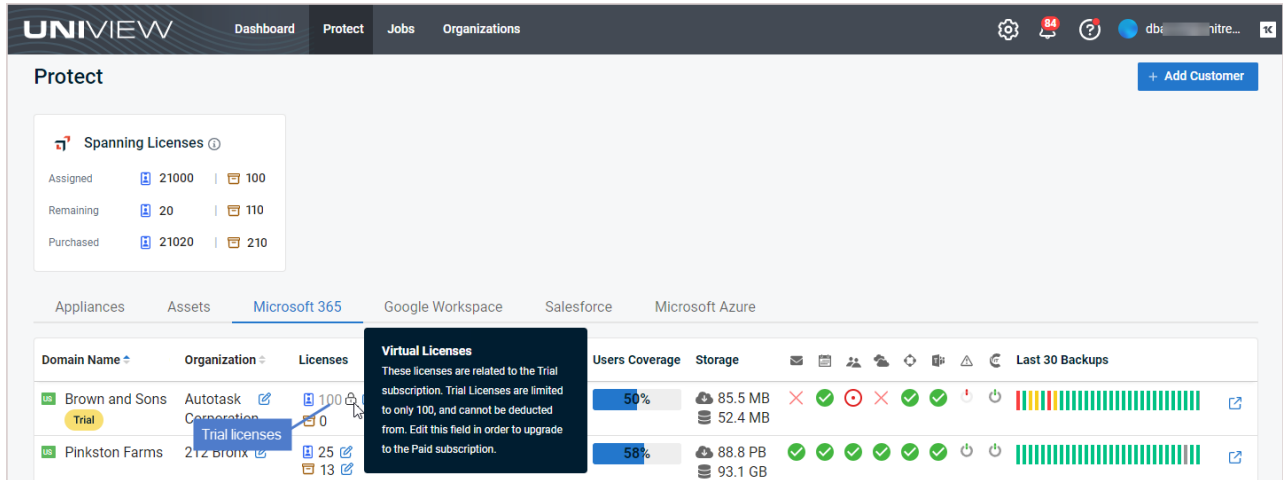
- 4 Licenses have been reallocated:






To upgrade from a Spanning Microsoft 365 trial to a paid subscription

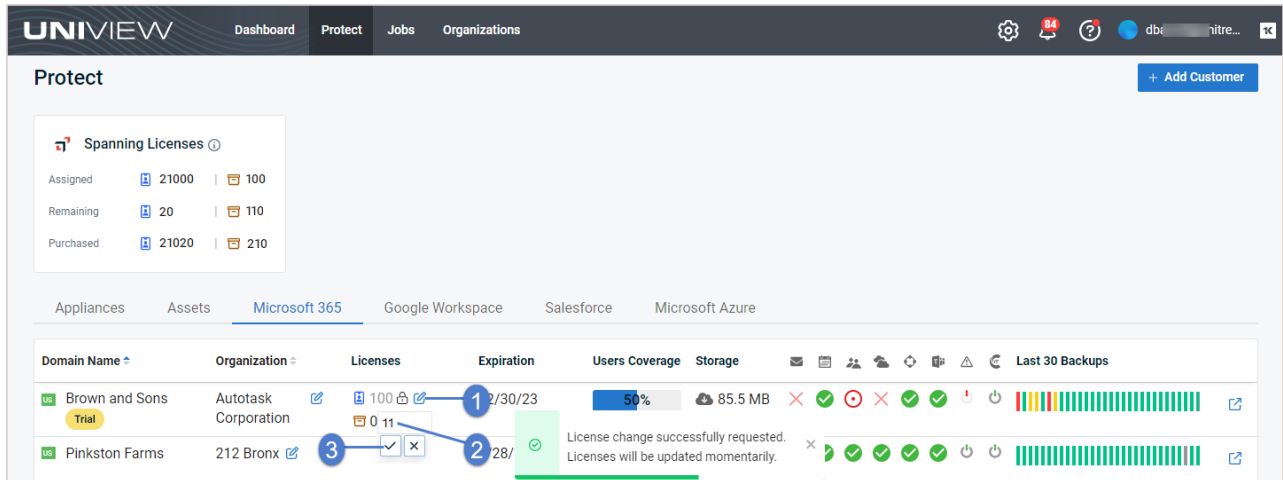
- 1 In the Microsoft 365 view, locate your trial tenant.

Note: If you don't see your trial tenant, add it to UniView by running this procedure: "Integrating a Microsoft 365 tenant".

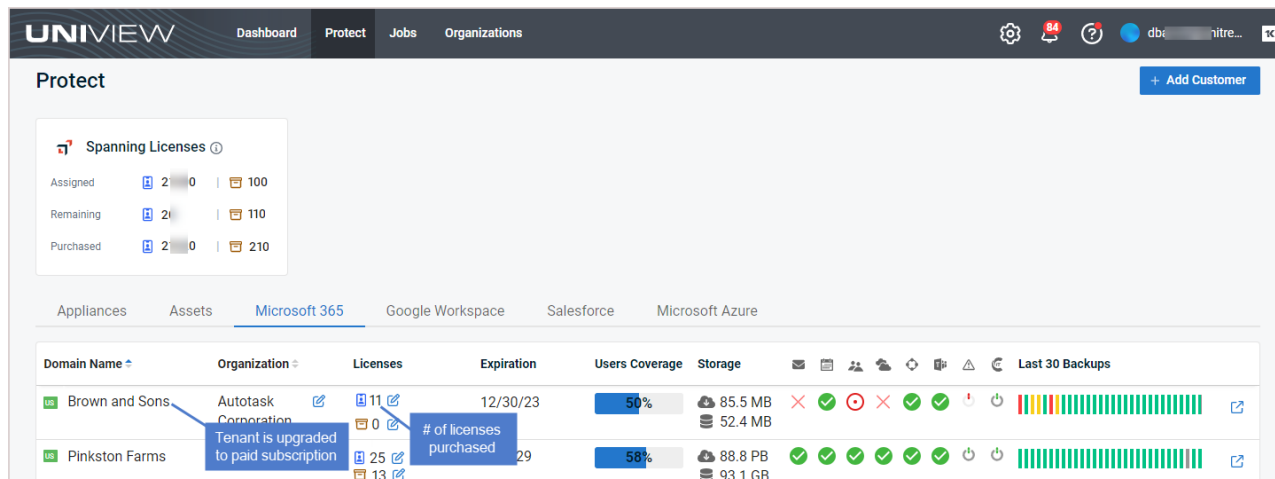


2 In the Licenses column, click , change the number of standard licenses, and click  to save.

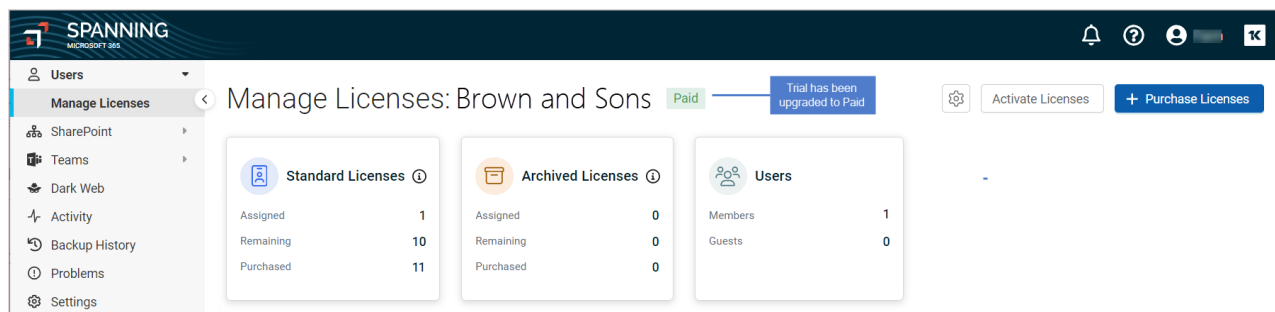
Note: When you click , the number of licenses that were assigned to users during the trial displays. You can accept this value or enter another value. Your paid subscription is created with this number of standard licenses.



3 Your trial is upgraded to a paid subscription.



On the Manage Licenses page in Spanning Backup for Microsoft 365, the tenant now displays as a paid tenant. The number of standard licenses you entered above displays in the Standard Licenses tile, in the Purchased license count:



Working with Google Workspace

If you are using Spanning Backup for Google Workspace, integrate your Google Workspace domain to manage domain/organization mappings, check the status of the domain's recent backups, receive alerts for failed or partial backups, allocate licenses, upgrade from a Spanning trial to a paid subscription, and view license and storage information — right from UniView.

Start by adding the integration as described in "[Integrating a Google Workspace domain](#)". Once the domain has been added, information is synced from Spanning Backup each night. Use the Google Workspace view to work with this data, as described in "[Working with the Google Workspace view](#)".

Integrating a Google Workspace domain

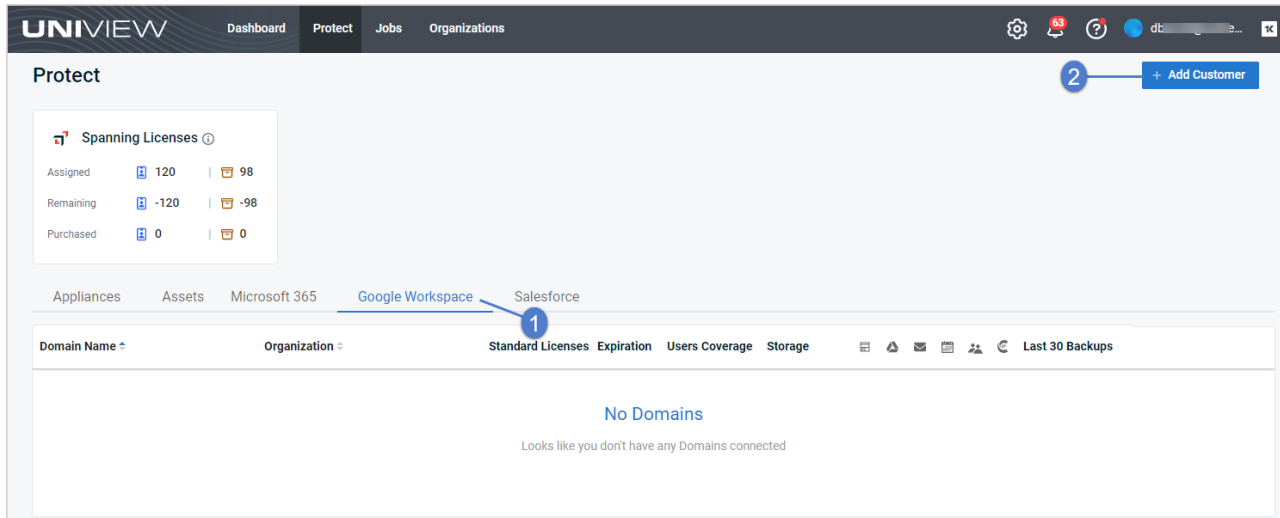
This procedure requires the following:

- A UniView account with superuser or administrator privileges
- A Google Workspace account with Global Admin privileges

Note: If you do not have Global Admin privileges, use this procedure to start the integration. Use the **Copy Invite Link** option to send the Global Admin a link they can use to complete the integration procedure.

To add the integration

- 1 Log in to the UniView Portal with a superuser or administrator account.
- 2 On the Protect page, click **Google Workspace**.
- 3 Click **Add Customer**.



- 4 Select an Organization from the list.
- 5 Select the **Google Workspace** platform.
- 6 Do one of the following:
 - If you have Global Admin credentials, click **Add** and continue with this procedure to complete the integration.
 - If you do not have Global Admin credentials, click **Copy Invite Link**. Then email the link to the Global Admin so that they can complete the integration.

Add Customer ✕

Add a **customer** or provide an **invite link** for your customer to complete the installation process.

i Organization sync is enabled. If you don't see a pre-existing organization in the list below, please make sure it exists at the source and is synced to UniView.

Organization *
212 Bronx 1 ▼

Select Platform

Microsoft 365

Google Workspace 2

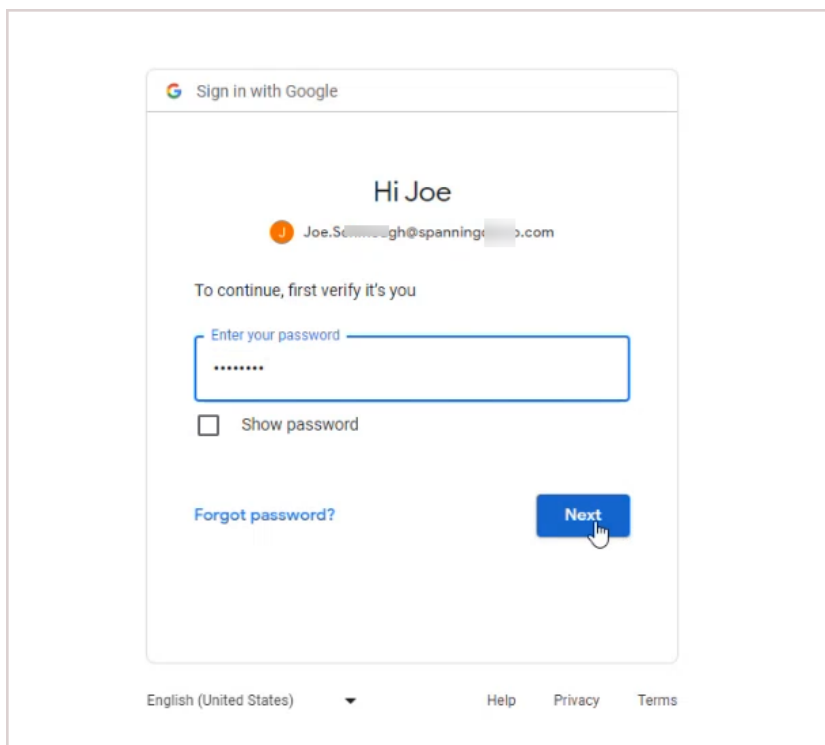
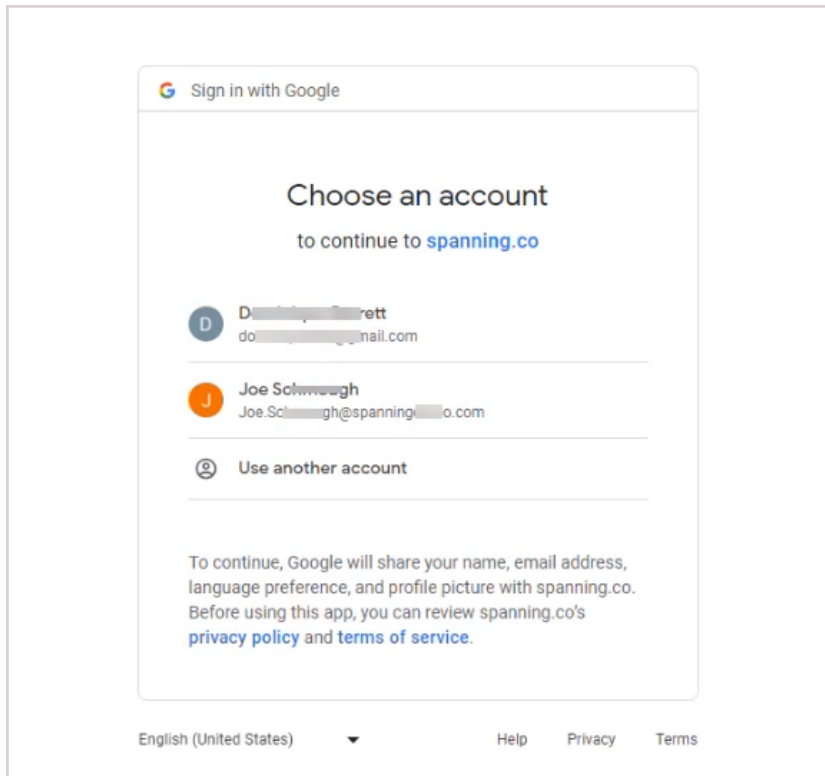
Salesforce

Salesforce Sandbox

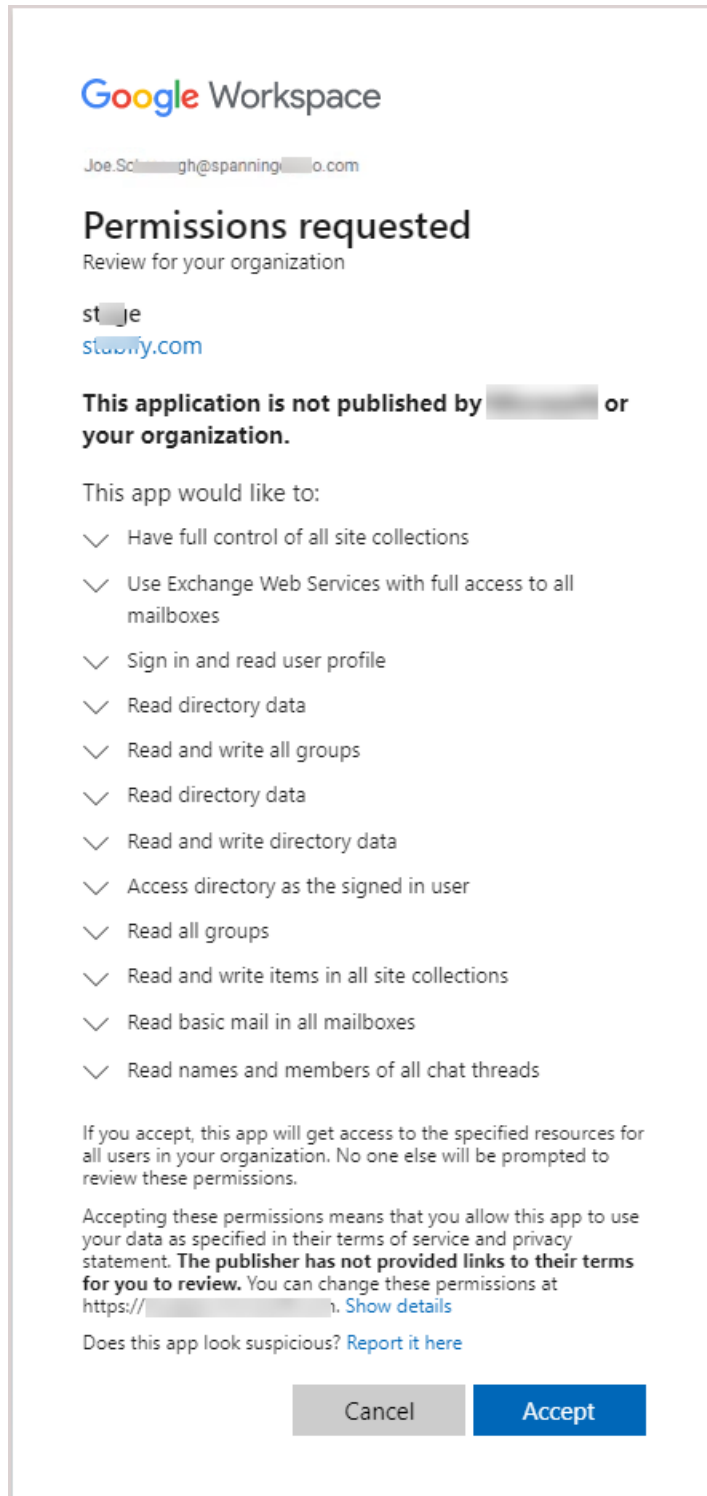
3 Cancel Add

📄 Copy Invite Link

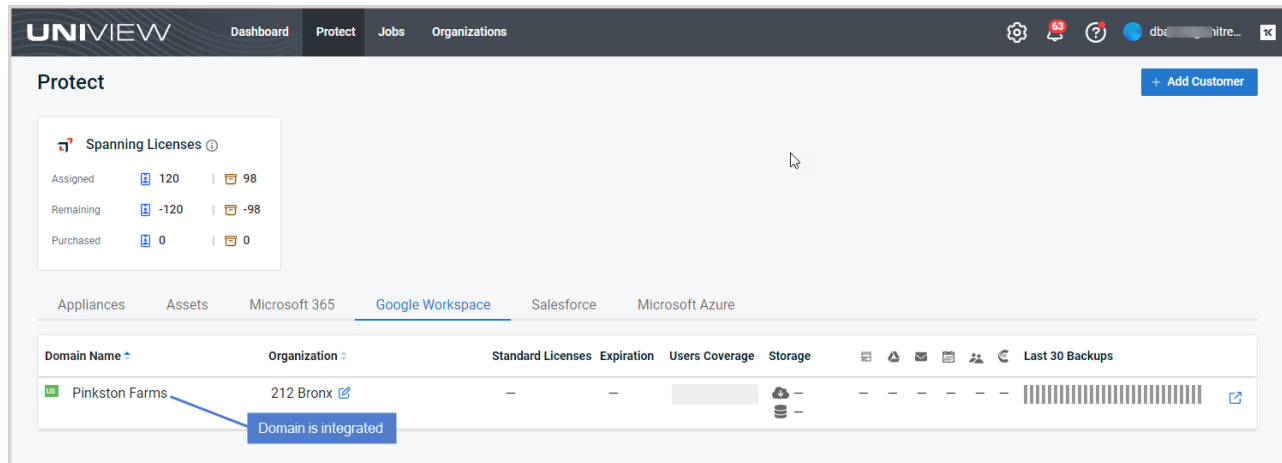
- 7 Enter your Google Workspace Global Admin credentials.



- 8 Click **Accept** to authorize access to your Google Workspace domain.



- 9 The domain is added and displays in the Google Workspace view. Data is synced nightly from Spanning Backup to the UniView Portal. For details about this data, see "[Working with the Google Workspace view](#)".



Working with the Google Workspace view

After you have integrated your Google Workspace domain, use the Protect > Google Workspace view to manage domain/organization mappings, view license and storage information, allocate licenses, upgrade from a Spanning trial to a paid subscription, and check the status of a domain's recent backups.

See these procedures for details:

- ["To view Google Workspace information"](#)
- ["To manage organization mappings"](#)
- ["To allocate Google Workspace licenses"](#)
- ["To upgrade from a Spanning Google Workspace trial to a paid subscription"](#)

To view Google Workspace information

























The following information displays in the Google Workspace view:



- Spanning Licenses tile – Shows the total number of Spanning licenses assigned, remaining, and purchased. Counts include licenses from all Spanning Backup products.

Note: Archived licenses apply only to Spanning Backup for Microsoft 365.

- Assigned – The number of standard licenses (📄) and archived licenses (📁) that have been assigned to users.
- Remaining – The number of standard licenses (📄) and archived licenses (📁) that have not yet been assigned to a user.
- Purchased – The total number of Spanning Backup standard licenses (📄) and archived licenses (📁) that have been purchased.

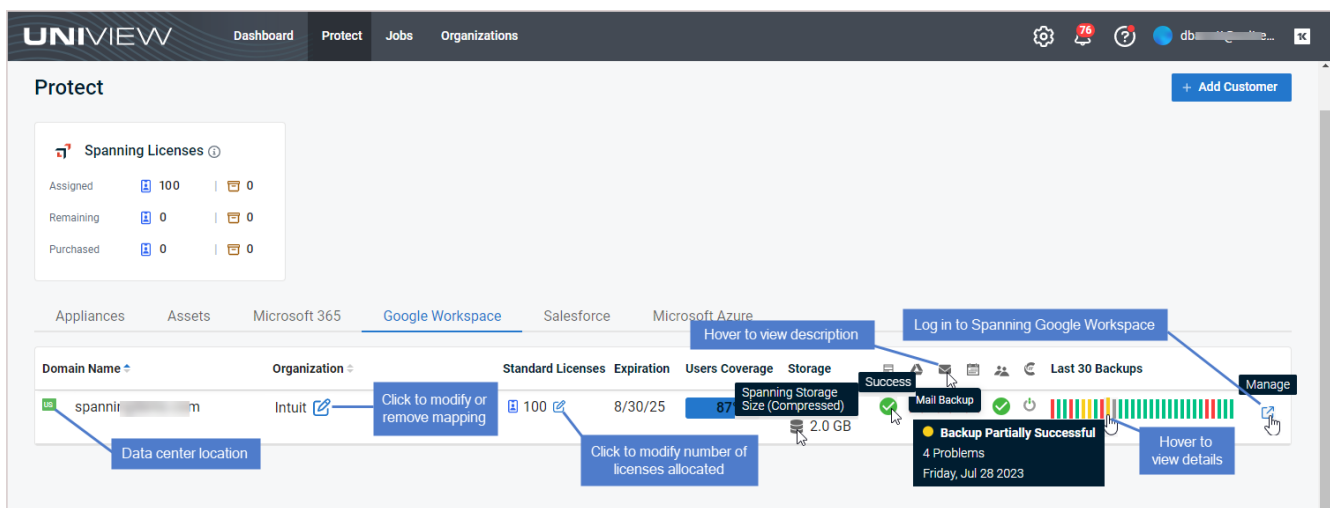
Note: Licenses must be purchased through Spanning Backup. The UniView Portal pooled licensing feature enables you to manage how your licenses are allocated. To reallocate licenses, simply remove them from one domain and add them to another (see ["To allocate Google Workspace licenses"](#)).

- Data center icon – Location of the domain's Spanning data center. For example,  for *United States*.
- Domain – Name of the Google Workspace domain.
- Organization – UniView Portal organization mapped to the domain.
 - *None* indicates that no organization has been mapped. To enable BackupIQ alerts for the domain, click  and select an organization.
 - To update the mapping, simply click  and select a different organization.
 - To remove the mapping and disable BackupIQ alerts for the domain, click  and select **X**.
- Standard Licenses – The number of standard licenses that have been allocated to the Google Workspace domain.
- Expiration – License expiration date.
- User Coverage – The total number of licensed users divided by the total number of users in the domain.
- Storage – Amount of storage used.  is the amount of raw data that has been downloaded from the cloud,  is the actual amount of local storage used after compression.
-  – Status of the domain's recent Site Backups:  for all backups over the last 7 days were successful,  for one or more backups over the last 7 days has failed,  for one or more backups over the last 7 days was partially completed, - for no backups exist.
-  – Status of the domain's recent Document Backups:  for all backups over the last 7 days were successful,  for one or more backups over the last 7 days has failed,  for one or more backups over the last 7 days was partially completed, - for no backups exist.
-  – Status of the domain's recent Mail Backups:  for all backups over the last 7 days were successful,  for one or more backups over the last 7 days has failed,  for one or more backups over the last 7 days was partially completed, - for no backups exist.
-  – Status of the domain's recent Calendar Backups:  for all backups over the last 7 days were successful,  for one or more backups over the last 7 days has failed,  for one or more backups over the last 7 days was partially completed, - for no backups exist.
-  – Status of the domain's recent Contact Backups:  for all backups over the last 7 days were successful,  for one or more backups over the last 7 days has failed,  for one or more backups over the last 7 days was partially completed, - for no backups exist.
-  – KaseyaOne status.  indicates KaseyaOne is enabled,  indicates KaseyaOne is disabled.
- Last Backups – Status of the domain's last backup, by day. Displays status icons for the last 30 days:
 -  indicates that the last backup on this day was successful. Hover to view the date and number of problems.
 -  indicates that the last backup on this day was partially completed. Hover to view the date and number of problems.
 -  indicates that the last backup on this day failed. Hover to view the date and number of problems.

-  indicates that there are no backups. Hover to view the date.
-  - Click to connect to Spanning Backup for Google Workspace, where you can view errors. (For details, see the [Spanning Backup for Google Workspace Admin Guide](#).)

Notes:


- This button does not display for Monitor role users. For more on user roles, see "[About UniView Portal user accounts](#)".
- If you have Superuser, Admin, or Manage credentials and do not see this button, the feature has not been enabled in your environment.
- You can connect to only one Google Workspace domain at a time.

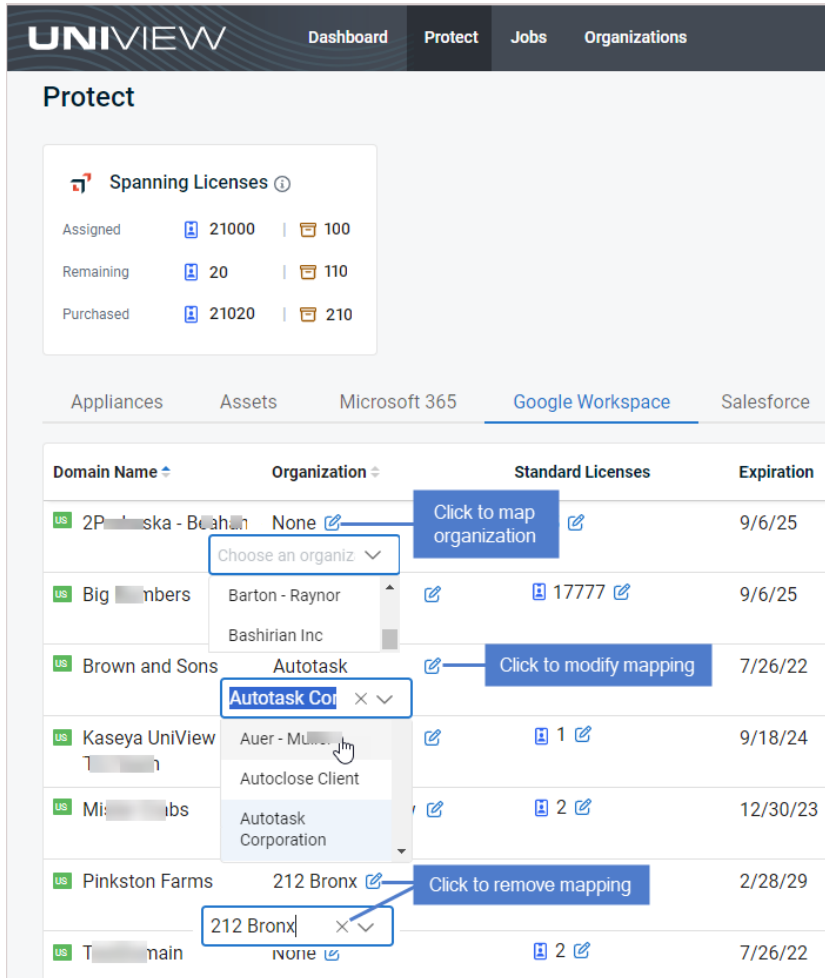


The screenshot shows the UniView Portal interface. At the top, there's a navigation bar with 'Dashboard', 'Protect', 'Jobs', and 'Organizations'. Below that, the 'Protect' section is active, showing 'Spanning Licenses' with 100 assigned, 0 remaining, and 0 purchased. The main content area is titled 'Google Workspace' and contains a table of domain mappings. The table has columns for 'Domain Name', 'Organization', 'Standard Licenses', 'Expiration', 'Users Coverage', 'Storage', 'Success', and 'Last 30 Backups'. A callout box shows a 'Backup Partially Successful' message with '4 Problems' on 'Friday, Jul 28 2023'. Other callouts point to various interactive elements like 'Log in to Spanning Google Workspace', 'Click to modify or remove mapping', and 'Hover to view details'.

To manage organization mappings

To enable BackupIQ alerts, the Google Workspace domain must be mapped to a UniView Portal organization. Use this procedure to manage these mappings.

- 1 In the Google Workspace view, locate the domain whose mapping you want to add, modify, or remove.
 - The Google Workspace domain name displays in the Domain column.
 - The Organization column contains either the name of the organization that has been mapped to this domain or *None* if no organization has been mapped.
- 2 In the Organization column, click  next to the organization name and do one of the following:
 - To add a mapping and enable BackupIQ alerts for the domain, select an organization from the list.
 - To modify the mapping, simply select a different organization from the list.
 - To remove the mapping and disable BackupIQ alerts for the domain, select X.



To allocate Google Workspace licenses

In the Google Workspace view, you can easily add licenses to or remove licenses from a domain by editing the number of Standard Licenses. You can also reallocate Spanning licenses by removing licenses from one domain and adding them to another. The changes you make are synced to the licensing tiles in Spanning Backup for Google Workspace.

Note: Licenses must be purchased through Spanning Backup. The UniView Portal pooled licensing feature enables you to manage how your licenses are allocated only.

The following steps show how to modify the number of licenses allocated to a Google Workspace domain:

- 1 The *spanning* domain has 100 standard licenses allocated.

The screenshot shows the UniView Protect interface. At the top, there are navigation tabs: Dashboard, Protect, Jobs, and Organizations. The 'Protect' tab is active. Below the navigation, there's a 'Spanning Licenses' section with 'Assigned', 'Remaining', and 'Purchased' counts, all currently at 0. Below that, there are tabs for 'Appliances', 'Assets', 'Microsoft 365', 'Google Workspace', 'Salesforce', and 'Microsoft Azure'. The 'Google Workspace' tab is selected. A table lists domain names and their associated licenses. The first row shows 'span.com' with 100 licenses, an expiration date of 8/30/25, 87% users coverage, and 6.5 GB storage. A blue callout box points to the '100' in the 'Standard Licenses' column with the text '100 licenses allocated'.

- 2 To modify the number of allocated licenses, click [✎](#), change the number, and click [✓](#) to save.

This screenshot shows the same UniView Protect interface as the previous one, but with the 'Standard Licenses' column for 'span.com' set to 100. A blue callout box highlights the '100' and the edit icon. A second callout box shows a dropdown menu with '90' selected, and a third callout box points to the checkmark icon. A green notification box at the bottom right says 'License change successfully requested. Licenses will be updated momentarily.'

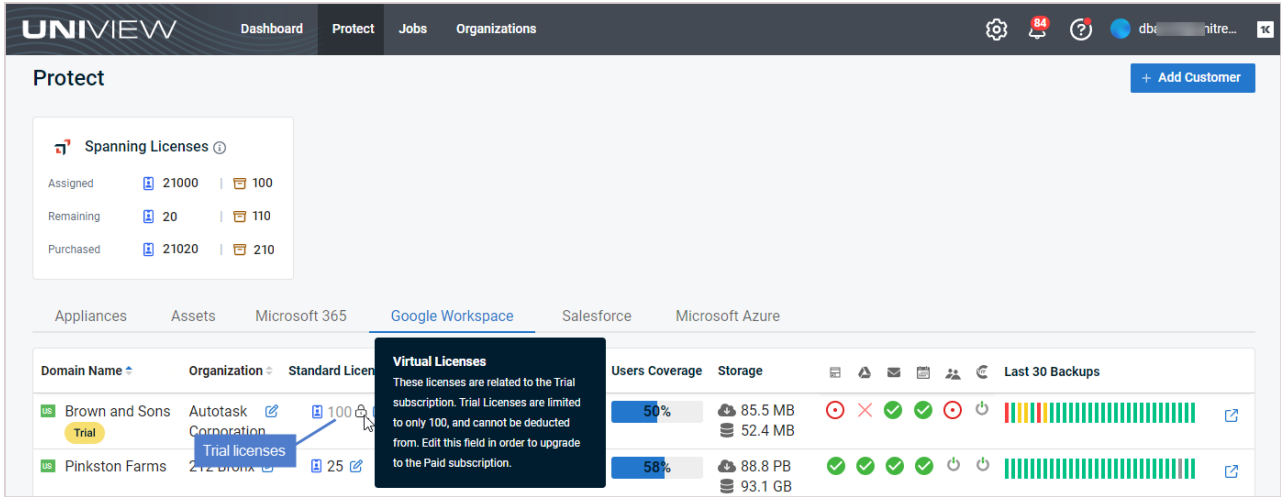
- 3 License allocation is modified:



The screenshot shows the UniView Protect interface after the license allocation has been modified. The 'Standard Licenses' column for 'span.com' now shows 90 licenses. A blue callout box points to the '90' with the text '# of allocated licenses is modified'.


To upgrade from a Spanning Google Workspace trial to a paid subscription

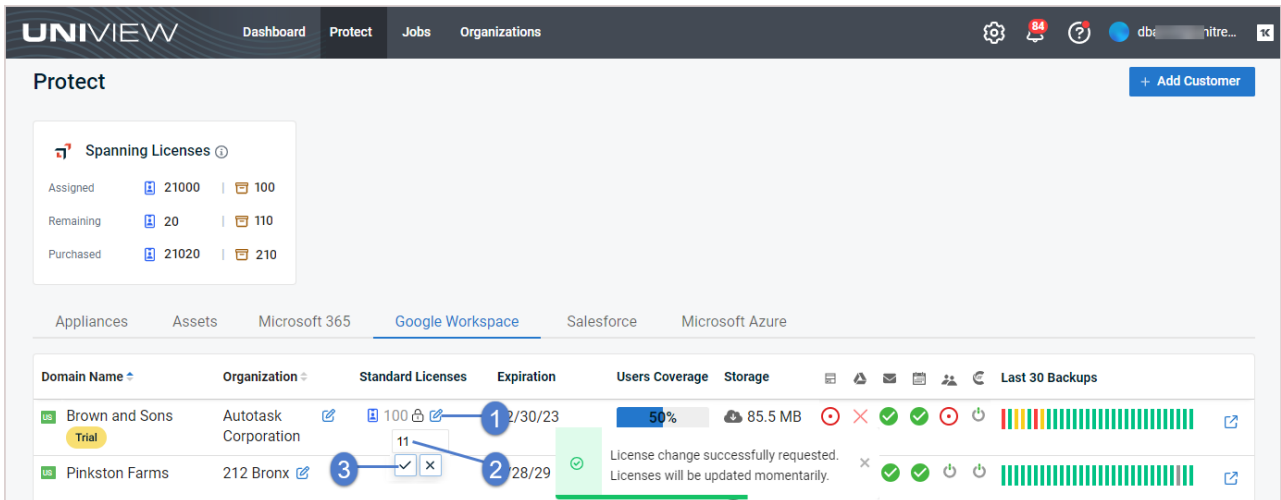
- 1 In the Google Workspace view, locate your trial domain.

Note: If you don't see your trial domain, add it to UniView by running this procedure: "[Integrating a Google Workspace domain](#)".



- 2 In the Licenses column, click , change the number of standard licenses, and click  to save.

Note: When you click , the number of licenses that were assigned to users during the trial displays. You can accept this value or enter another value. Your paid subscription is created with this number of standard licenses.



- 3 Your trial is upgraded to a paid subscription.

Spanning Licenses

Assigned: 21000 | 100
Remaining: 20 | 110
Purchased: 21020 | 210

Appliances | Assets | Microsoft 365 | **Google Workspace** | Salesforce | Microsoft Azure

Domain Name	Organization	Standard Licenses	Expiration	Users Coverage	Storage	Last 30 Backups
Brown and Sons	Autotask Corporation	11	12/30/23	50%	85.5 MB 52.4 MB	[Backup Status Icons]
Pinkston Farms		25		58%	88.8 PB 93.1 GB	[Backup Status Icons]

Domain Name: Brown and Sons
Organization: Autotask Corporation
Standard Licenses: 11
Expiration: 12/30/23
Users Coverage: 50%
Storage: 85.5 MB, 52.4 MB
Last 30 Backups: [Progress Bar]

Domain Name: Pinkston Farms
Standard Licenses: 25
Users Coverage: 58%
Storage: 88.8 PB, 93.1 GB
Last 30 Backups: [Progress Bar]

Annotations:
- Blue box: "Tenant is upgraded to paid subscription" (points to Autotask Corporation)
- Blue box: "# of licenses purchased" (points to 11)

On the Manage Licenses page in Spanning Backup for Google Workspace, the domain now displays as a paid domain. The number of standard licenses you entered above displays in the Standard Licenses tile, in the Purchased license count.

Manage Licenses: Brown and Sons Paid

Trial has been upgraded to Paid

Download CSV | Activate Licenses | Purchase Licenses

Standard Licenses	Subscription
Assigned: 54	Expires: 08/30/25
Remaining: 46	Days Remaining: 532
Purchased: 100	

Working with Salesforce

If you are using Spanning Backup for Salesforce, integrate your Salesforce organization to manage domain/organization mappings, check the status of recent backups, receive alerts for failed backups, and view license and storage information — right from UniView.

Start by adding the integration as described in "[Integrating a Salesforce organization](#)". Once the organization has been added, information is synced from Spanning Backup each night. Use the Salesforce view to work with this data, as described in "[Working with the Salesforce view](#)".

Integrating a Salesforce organization

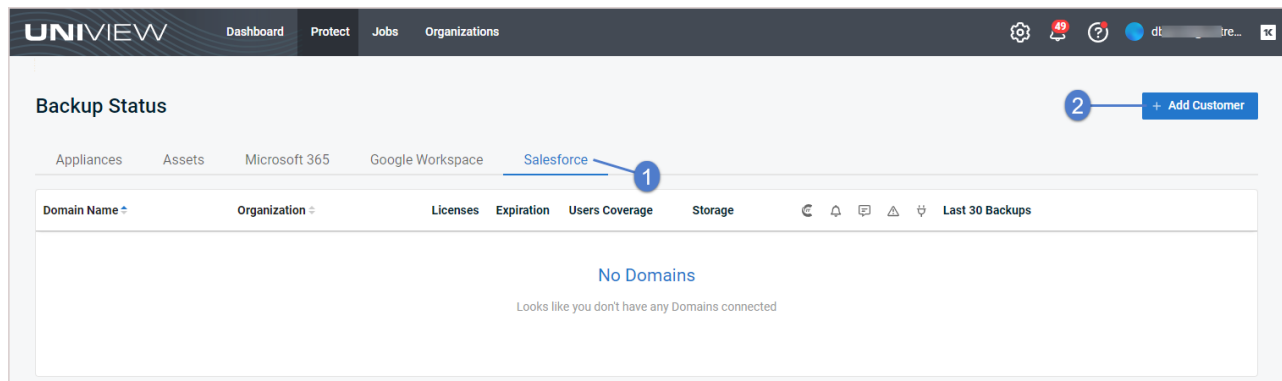
This procedure requires the following:

- A UniView account with superuser or administrator privileges
- A Spanning Administrator or Salesforce System Administrator account

Note: If you do not have a Spanning Administrator or Salesforce System Administrator account, use this procedure to start the integration. Use the **Copy Invite Link** option to send the Spanning Administrator or Salesforce System Administrator a link they can use to complete the integration procedure.

To add the integration


- 1 Log in to the UniView Portal with a superuser or administrator account.
- 2 On the Protect page, click **Salesforce**.
- 3 Click **Add Customer**.



- 4 Select an Organization from the list.
- 5 Select the **Salesforce** or **Salesforce Sandbox** platform.
- 6 Do one of the following:
 - If you have Spanning Administrator or Salesforce System Administrator credentials, click **Add** and continue with this procedure to complete the integration.
 - If you do not have Spanning Administrator or Salesforce System Administrator credentials, click **Copy Invite Link**. Then email the link to the Spanning Administrator or Salesforce System Administrator so that they can complete the integration.

Add Customer ✕

Add a **customer** or provide an **invite link** for your customer to complete the installation process.

 Organization sync is enabled. If you don't see a pre-existing organization in the list below, please make sure it exists at the source and is synced to UniView.

Organization *
212 Bronx 1 ▼


Select Platform

Microsoft 365

Google Workspace

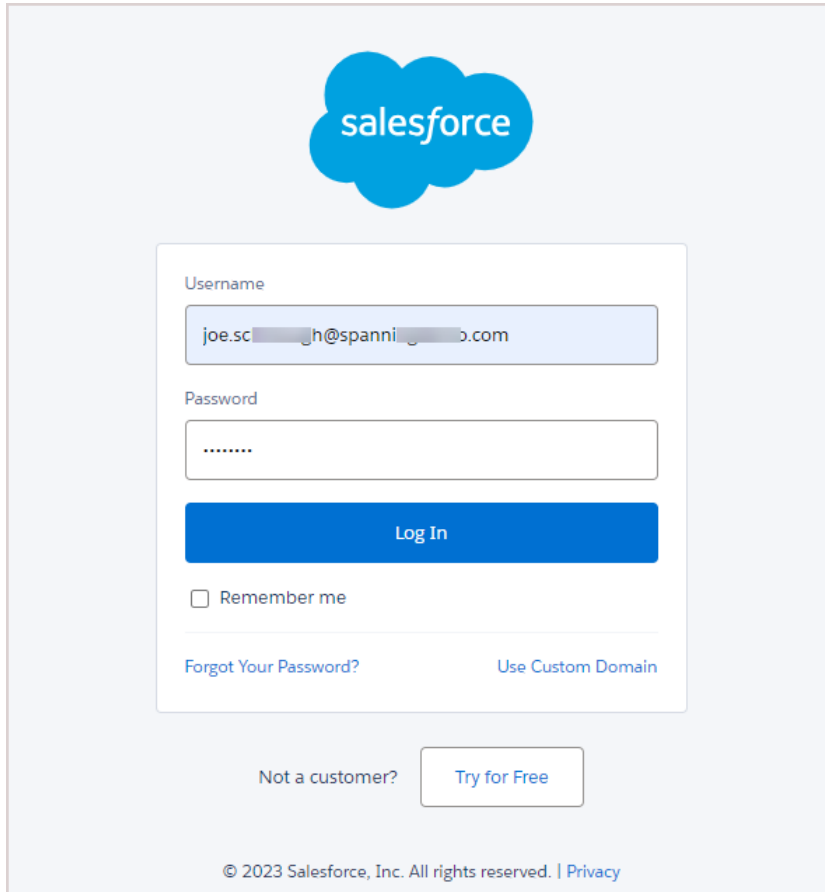
Salesforce 2

Salesforce Sandbox

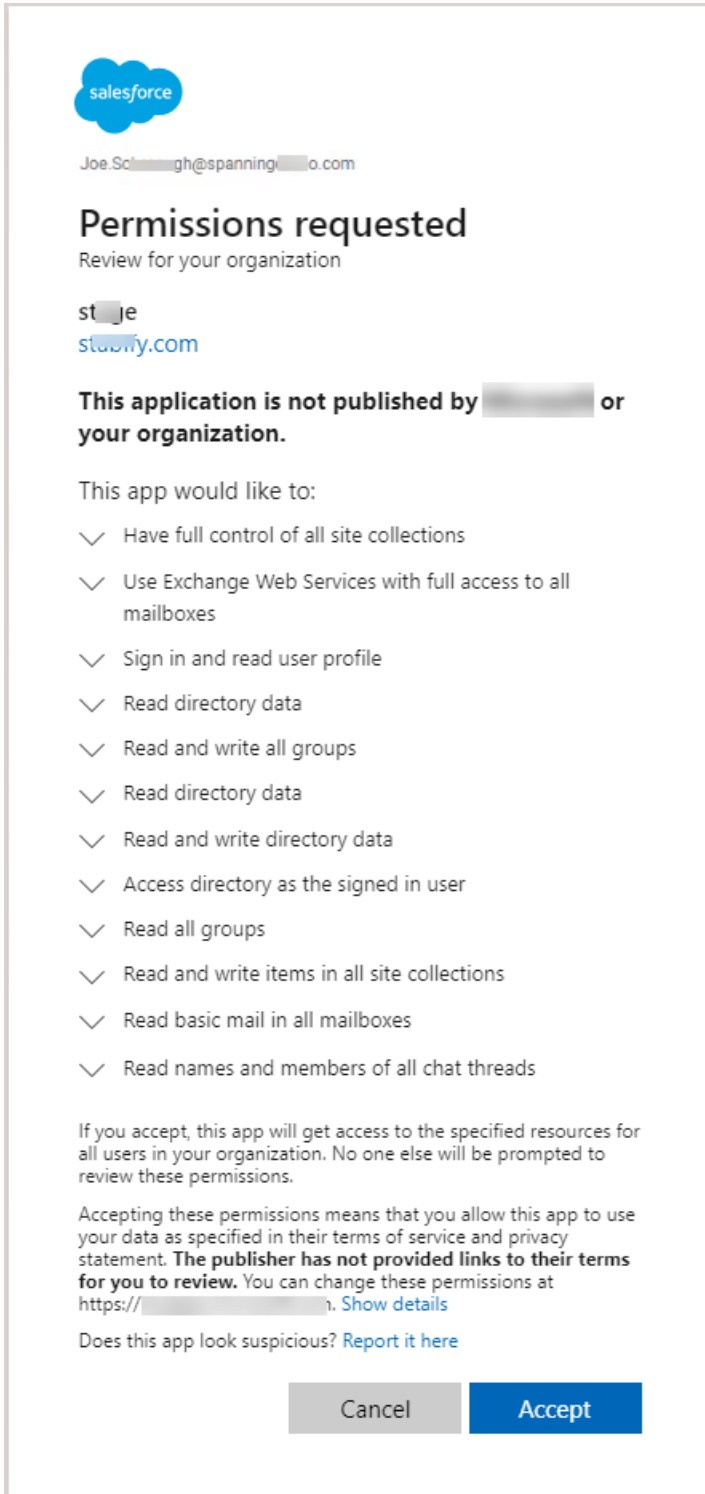
 Copy Invite Link

3 Cancel Add

- 7 Enter your Spanning Administrator or Salesforce System Administrator credentials.



- 8 Click **Accept** to authorize access to your Salesforce organization.



The image shows a Salesforce permissions request dialog box. At the top left is the Salesforce logo. Below it is the email address 'Joe.Sch...gh@spanning...o.com'. The main heading is 'Permissions requested' with the subtitle 'Review for your organization'. Below that is the name 'st...je' and the domain 'st...y.com'. A warning message states: 'This application is not published by [redacted] or your organization.' A list of permissions follows, each with a checkmark icon: 'Have full control of all site collections', 'Use Exchange Web Services with full access to all mailboxes', 'Sign in and read user profile', 'Read directory data', 'Read and write all groups', 'Read directory data', 'Read and write directory data', 'Access directory as the signed in user', 'Read all groups', 'Read and write items in all site collections', 'Read basic mail in all mailboxes', and 'Read names and members of all chat threads'. Below the list is a paragraph explaining that accepting grants access to resources for all users and that no one else will be prompted. It includes a warning: 'The publisher has not provided links to their terms for you to review.' and a link to 'Show details' at 'https://[redacted]'. At the bottom, there is a link 'Report it here' and two buttons: 'Cancel' and 'Accept'.

9 The domain is added and displays in the Salesforce view. Data is synced nightly from Spanning Backup to the UniView Portal. For details about this data, see "Working with the Salesforce view".

Working with the Salesforce view






After you have integrated your Salesforce organization, use the Protect > Salesforce view to manage organization mappings, view license and storage information, and check the status of an organization's recent backups.

The following information displays in the Salesforce view:

- Spanning Licenses tile – Shows the total number of Spanning licenses assigned, remaining, and purchased. License counts include licenses from all Spanning Backup products.

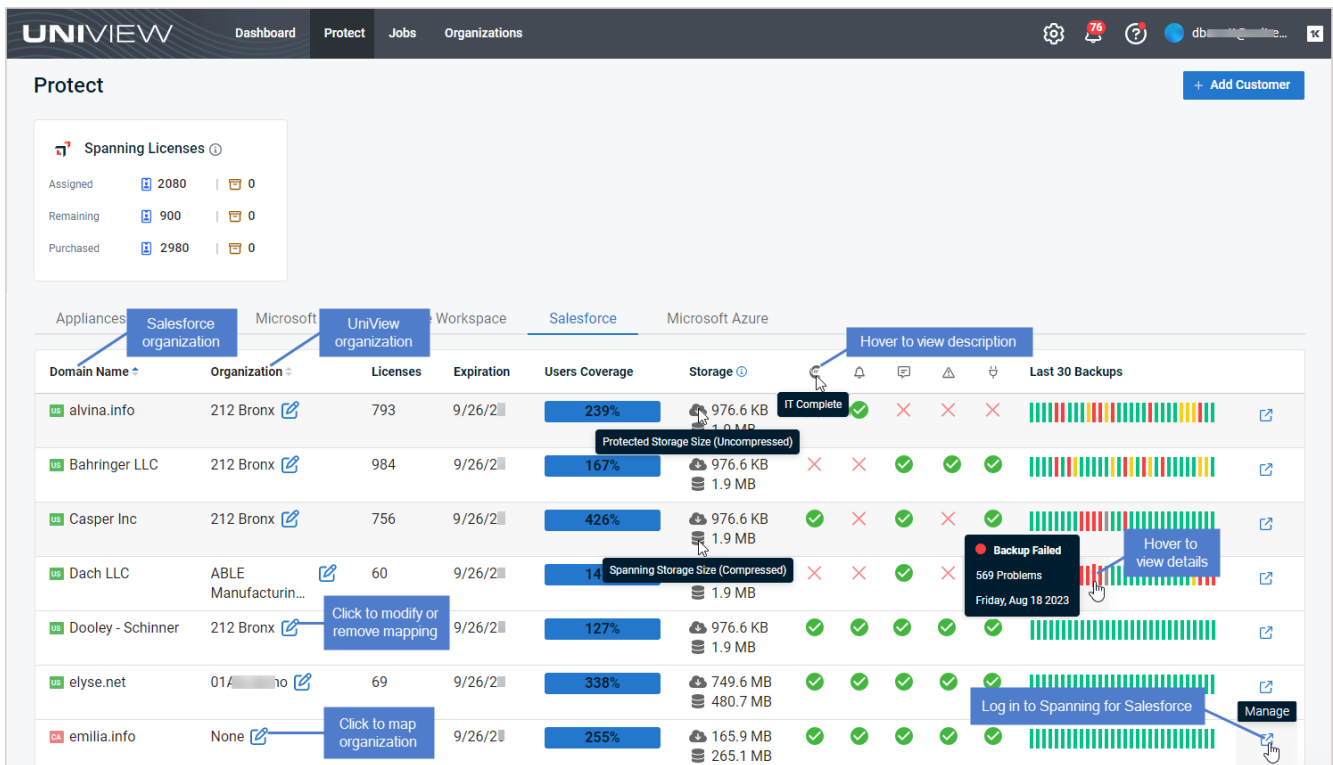
Note: Archived licenses apply only to Spanning Backup for Microsoft 365.

- Assigned – The number of standard licenses (📄) and archived licenses (📄) that have been assigned to users.
- Remaining – The number of standard licenses (📄) and archived licenses (📄) that have not yet been assigned to a user.
- Purchased – The total number of Spanning Backup standard licenses (📄) and archived licenses (📄) that have been purchased.
- Data center icon – Location of the organization's Spanning data center. For example, 🇺🇸 for *United States*.
- Domain Name – Salesforce organization.
- Organization – UniView organization mapped to the Salesforce organization.
 - *None* indicates no organization has been mapped. To enable BackupIQ alerts, click 📄 and select an organization.
 - To update the mapping, simply click 📄 and select a different organization.
 - To remove the mapping and disable BackupIQ alerts, click 📄 and select X.
- Licenses – Number of licenses that have been allocated to the organization.
- Expiration – License expiration date.
- User Coverage – The total number of licensed users divided by the total number of users in the organization.
- Storage – Amount of storage used. 📄 is the amount of raw data that has been downloaded from the cloud, 📄 is the actual amount of local storage used after compression.
- 📄 – KaseyaOne (IT Complete) status. ✅ indicates login with KaseyaOne is enabled, ❌ indicates login with KaseyaOne is disabled.
- 📄 – Daily Notifications status. ✅ indicates notifications are enabled, ❌ indicates notifications are disabled.
- 📄 – Chatter Feed status. Spanning can post status notifications for your backups, restores, and exports directly to Chatter. ✅ indicates Chatter posts are enabled, ❌ indicates Chatter posts are disabled.
- 📄 – Rule-based Alerts status. Spanning enables you to create your own rule-based alerts. These alerts are sent to the email address and Chatter feed configured for notifications. ✅ indicates rule-based alerts are enabled, ❌ indicates rule-based alerts are disabled.
- 📄 – External API status. ✅ indicates an external API is enabled, ❌ indicates external APIs are disabled.

- Last Backups – Status of the organization's last backup, by day. Displays status icons for the last 30 days:
 -  indicates that the last backup on this day was successful. Hover to view the date and number of problems.
 -  indicates that the last backup on this day was partially completed. Hover to view the date and number of problems.
 -  indicates that the last backup on this day failed. Hover to view the date and number of problems.
 -  indicates that there are no backups. Hover to view the date.
-  – Click to connect to Spanning Backup for Salesforce, where you can view errors. (For details, see the [Spanning Backup for Salesforce Admin Guide](#).)

Notes:

- This button does not display for Monitor role users. For more on user roles, see "About UniView Portal user accounts".
- If you have Superuser, Admin, or Manage credentials and do not see this button, the feature has not been enabled in your environment.
- You can connect to only one Salesforce organization at a time.

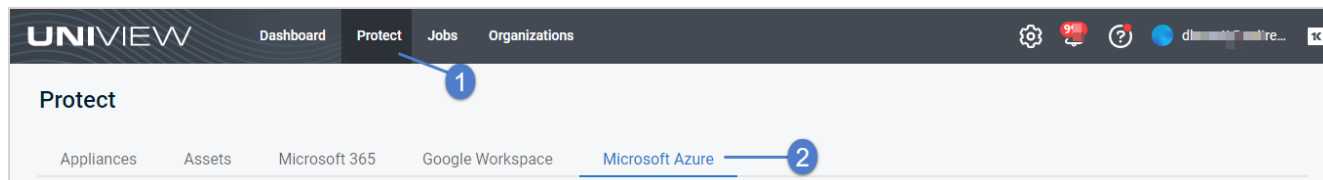


The screenshot shows the 'Protect' section of the UniView portal. At the top, there are navigation tabs for 'Dashboard', 'Protect', 'Jobs', and 'Organizations'. A 'Spanning Licenses' summary shows 2080 assigned, 900 remaining, and 2980 purchased licenses. Below this is a table of Salesforce organizations. The table columns include Domain Name, Organization, Licenses, Expiration, Users Coverage, Storage, and Last 30 Backups. Annotations highlight various features: 'Salesforce organization' link, 'Click to modify or remove mapping', 'Click to map organization', 'Hover to view description', 'Protected Storage Size (Uncompressed)', 'Spanning Storage Size (Compressed)', 'Backup Failed' notification, 'Hover to view details', 'Log in to Spanning for Salesforce', and 'Manage' button.

Domain Name	Organization	Licenses	Expiration	Users Coverage	Storage	Last 30 Backups
alvina.info	212 Bronx	793	9/26/21	239%	976.6 KB 1.9 MB	IT Complete
Bahringer LLC	212 Bronx	984	9/26/21	167%	976.6 KB 1.9 MB	Backup Failed
Casper Inc	212 Bronx	756	9/26/21	426%	976.6 KB 1.9 MB	Backup Failed
Dach LLC	ABLE Manufacturing...	60	9/26/21	14%	Spanning Storage Size (Compressed) 1.9 MB	Backup Failed
Dooley - Schinner	212 Bronx		9/26/21	127%	976.6 KB 1.9 MB	
elyse.net	01/...no	69	9/26/21	338%	749.6 MB 480.7 MB	
emilia.info	None		9/26/21	255%	165.9 MB 265.1 MB	

Working with Datto Backup for Microsoft Azure

If you are running backups with Datto Backup for Microsoft Azure (DBMA), you can integrate DBMA to manage your backups right from the UniView Portal. Start by adding the integration as described in ["Integrating Datto Portal"](#). Once the integration has been added, the Microsoft Azure view displays on the Protect page. To access this view, click **Protect > Microsoft Azure**:



The Microsoft Azure view provides summary and status information about the assets you protect with the Datto DBMA backup product. Assets that meet these criteria display on the page: the asset is a Datto CloudSIRIS model and its Datto client has been mapped to a UniView Portal organization. Datto clients were automatically mapped to organizations when the Datto Portal integration was added to UniView Portal. As clients are added to the Datto Portal, they are added to UniView Portal and automatically mapped to organizations. (If needed, you can modify organization mappings as described in ["Mapping Datto Portal clients to organizations"](#).)

Note: If you do not see the Microsoft Azure view, add the Datto Portal integration as described in ["Integrating Datto Portal"](#).

The Microsoft Azure page is shown below. To modify the display, you can sort and filter the page:

- To change the sort order of the display, click any column heading.
- To view additional pages of assets, use the scroll arrows below.
- To filter the display, do any of the following:
 - Select a **Scope**
 - Select an **Organization**
 - Enter text in the **Asset Name** field to display only asset names containing the string you entered
 - Click **Recent Failures** to display only assets that have had a recent backup failure

The following information is given for each asset:

- Type icon – Hover over the icon to see the asset type description.
- Name – Asset name.
- Organization – The asset's UniView Portal organization.
- Last Backup – Number of minutes, hours, days, weeks, or months since the last backup.

- Recent Backups – Icons indicating the status of backups over the last seven days. Hover over an icon to see job details. Click an icon to view asset details.
 - All backups were successful
 - One or more backups failed or ran with warnings
 - ✗ All backups failed
 - No backups were taken

The screenshot displays the UniView Protect interface for Microsoft Azure. It features a table of assets with columns for Type, Name, Organization, Last Backup, and Recent Backups. A legend in the top right corner defines the backup status icons: a green circle for successful backups, a yellow circle for warnings, a red 'X' for failures, and a grey circle for no backups. A tooltip for the 'Server2016' asset shows backup details for Monday, 6/12/2023, including 17 successes and 2 failures.

Type	Name	Organization	Last Backup	Recent Backups
vm	DFP	01 demo	an hour ago	T W T F S S M
vm	GermanVM	01 demo	an hour ago	T W T F S S M
vm	gen1msessio	01 demo	an hour ago	T W T F S S M
vm	CHAU-2016-03	Chau	an hour ago	T W T F S S M
Virtual Machine	Server2016	Choice Studios	an hour ago	T W T F S S M Monday, 6/12/2023 UTC-07:00 Backups: Successes 17 Failures 2
vm	Server2019	Choice Studios	an hour ago	T W T F S S M
vm	amsart-az-dc-01	Amsterdam Artisans	an hour ago	T W T F S S M
vm	amsart-az-web-0	Amsterdam Artisans	an hour ago	T W T F S S M
vm	core	01 demo	an hour ago	T W T F S S M
vm	artissessio	01 demo	an hour ago	T W T F S S M

Click an asset to view these details:

- Last Backup – Number of minutes, hours, days, weeks, or months since the last backup.
- Last Certified – Number of minutes, hours, days, weeks, or months since a backup has been certified.
- Recovery Points – Lists the asset's recovery points (local backups) by date.
- Local – Icon indicating the status of the backup. Click an icon to view log details.
 - for success
 - for job ran with warnings
 - for failure

The screenshot displays the UniView Protect interface. The top navigation bar includes 'Dashboard', 'Protect', 'Jobs', and 'Organizations'. The main content area is titled 'Protect' and has tabs for 'Appliances', 'Assets', 'Microsoft 365', 'Google Workspace', and 'Microsoft Azure'. Below these tabs are filters for 'Scope' (All), 'Organization' (All), and 'Asset Name'. A table lists various assets with columns for 'Type', 'Name', 'Organization', and 'Last Backup'. The 'Server2019' asset is highlighted with a blue circle and a '1' callout. To the right, the 'Asset Detail' panel is open for 'Server2019', showing 'Last Backup' (25 minutes ago) and 'Last Certified' (25 minutes ago) with a '2' callout. Below this is a 'Recovery Points' section with a 'Legend' icon and a list of recovery points from June 12, 2023, each with a green status icon. A '10 per page' and '1 of 2 pages' indicator is at the bottom of the panel.

Type	Name	Organization	Last Backup
vm	azurebac	Choice Studios	23 minutes ago
vm	msessio	Choice Studios	23 minutes ago
vm	gen1	Choice Studios	24 minutes ago
vm	sessio	Choice Studios	24 minutes ago
vm	Server2016	Choice Studios	25 minutes ago
vm	GermanVM	Choice Studios	25 minutes ago
vm	SRV-FTG-AZ-01	Fulton Technology Group	25 minutes ago
vm	Server2019	Choice Studios	25 minutes ago
vm	amsart-az-dc-01	Amsterdam Artisans	25 minutes ago
vm	cc-server2016	Cheng Inc	25 minutes ago

Click a recovery point or status icon to view the job log:

The screenshot displays the UniView Portal interface. The top navigation bar includes 'Dashboard', 'Protect', 'Jobs', and 'Organizations'. The main content area is split into two panels: 'Job Log' and 'Asset Detail'.

Job Log Panel:

- Appliance: Local
- Scope: All
- Job ID: 11ee0933-ea68-956a-9d68-0654aa7679e4
- Result: Success
- Type: Multiple 'vm' entries are listed.
- A blue callout '2' points to the 'Job log displays' text.

Asset Detail Panel:

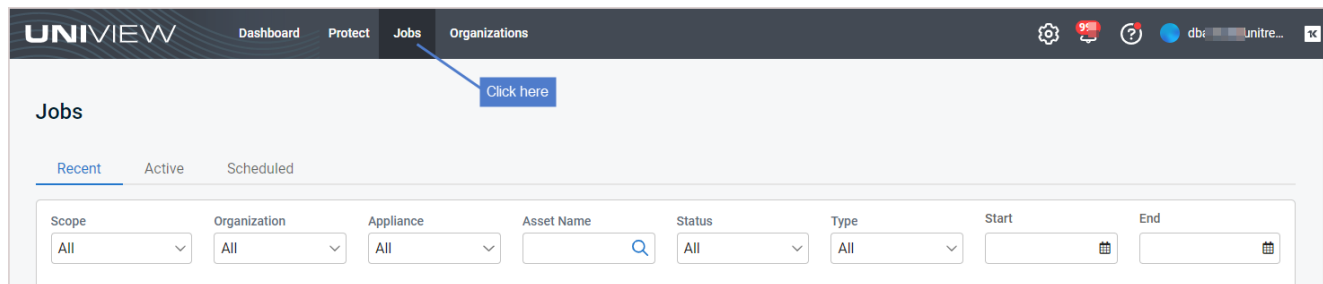
- Asset: Server2019
- Last Backup: 33 minutes ago
- Last Certified: -
- Recovery Points: Legend ⓘ
- Recovery Points Table:

Recovery Points	Local
June 12, 2023, 01:03 pm	●
June 12, 2023, 12:03 pm	●
June 12, 2023, 11:03 am	●
June 12, 2023, 10:03 am	●
June 12, 2023, 09:03 am	●
June 12, 2023, 08:03 am	●
June 12, 2023, 07:03 am	●
June 12, 2023, 06:03 am	●
June 12, 2023, 05:02 am	●
June 12, 2023, 04:02 am	●

At the bottom of the Asset Detail panel, there is a pagination control: '10 per page 1 of 2 pages'. A blue callout '1' points to the 'Job Details' link next to the 08:03 am entry. A blue callout '2' points to a notification icon in the bottom right corner.

Working with Jobs

Use the Jobs page to view information about active, scheduled, and recent jobs. To access the Jobs page, click **Jobs**:



The page contains these views:

- Recent (default view) – Provides summary and status information about recent Unitrends jobs. From this page you can also view job details. For details, see ["Working with recent jobs"](#).
- Active – Provides information about currently running jobs. For details, see ["Viewing active jobs"](#).
- Scheduled – Provides summary status information about scheduled jobs. From this page you can also view schedule details. For details, see ["Working with scheduled jobs"](#).

Working with recent jobs

Use the Recent jobs view for the following:

- ["Viewing recent jobs"](#)
- ["Filtering the Recent jobs view"](#)
- ["Viewing job details"](#)

Viewing recent jobs

The Recent jobs view displays recent jobs across all Unitrends appliances that have been added to your backup.net instance. (To filter the display, see ["Filtering the Recent jobs view"](#).)

Graph

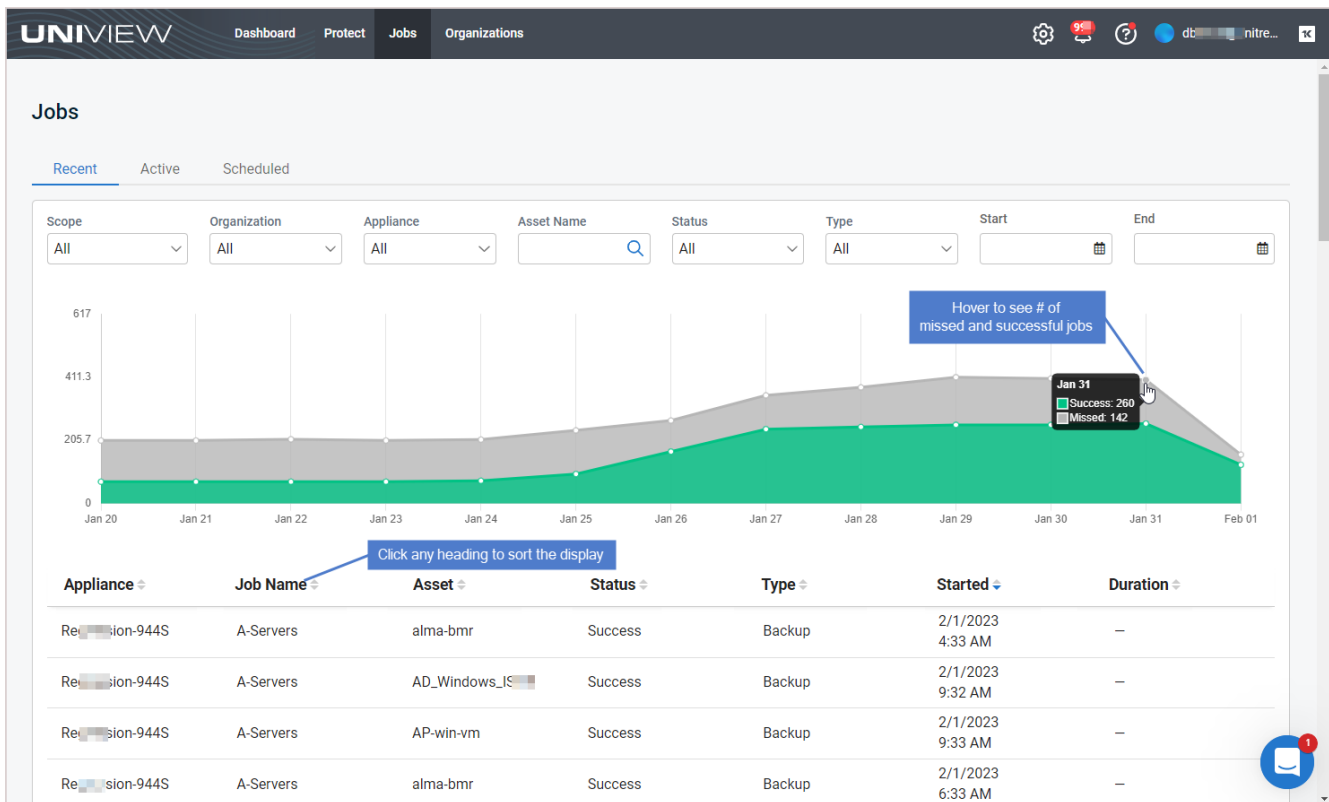
A graph shows the number of successful and missed jobs over the last 13 days.

- Hover over a point in the graph to see the number of successful and missed jobs on a given day.
- See the table below the graph for status by job.

Status by job

The following information is given for each recent job. To change the sort order of the display, click any column heading.

- Appliance – Name of the Unitrends appliance that ran the job.
- Job Name – Name of the job.
 - If initiated by a UniView backup policy, the job name is "UniView-AssetName".
 - If initiated by the Unitrends appliance, the job name is the Unitrends job name.
- Asset – Name of the Unitrends asset or '-' if the job contains multiple assets.
- Status – Job status: Success, Warning, or Error.
- Type – Job type: Backup, Backup Copy - Hot, Backup Copy - Cold, or Certification (DCA job).
- Started – Date and time at which the job started or was added to the appliance job queue.
- Duration – Amount of time that the job ran, in *hh:mm:ss* format (hours, minutes, seconds).



Filtering the Recent jobs view

The Recent jobs view displays jobs that ran in the last 90 days across all appliances that have been added to your backup.net instance.

To filter the display, enter filter criteria in any of the following:

- Scope – Select a scope from the list. (Select **All** to clear the scope filter.)
- Organization – Select an organization from the list. (Select **All** to clear the organization filter.)
- Appliance – Enter a text string, then press **Enter** to apply. Appliance names containing the text you entered display.
- Asset Name – Enter a text string, then press **Enter** to apply. Asset names containing the text you entered display.
- Status – Select a job status from the list. (Select **All** to clear the job status filter.)
- Type – Select a job type from the list. (Select **All** to clear the job type filter.)
- Start and End – Click the calendar icons to filter by date range. The date range must be within the the last 90 days.

The screenshot shows the UniView Jobs page. At the top, there are navigation tabs: Dashboard, Protect, Jobs, and Organizations. The 'Jobs' tab is active. Below the navigation, there are filter options for Scope, Organization, Appliance, Asset Name, Status, Type, Start, and End. A blue callout box points to the filter bar with the text 'Enter filter criteria'. Below the filters is a line graph showing job activity over time from Jan 23 to Feb 04. The graph has a green area representing active jobs and a grey area representing scheduled jobs. Below the graph is a table with columns: Appliance, Job Name, Asset, Status, Type, Started, and Duration. The table contains four rows of job data.

Appliance	Job Name	Asset	Status	Type	Started	Duration
max9s-264	Backup Copy Cold bk-deb10	max9s-264	Success	Backup Copy (Cold)	1/24/2023 12:00 AM	–
max9s-264	Backup Copy Cold bk-deb10	max9s-264	Success	Backup Copy (Cold)	2/1/2023 12:00 AM	–
max9s-264	Backup Copy Cold bk-deb10	max9s-264	Success	Backup Copy (Cold)	1/25/2023 12:00 AM	–
max9s-264	Backup Copy Cold bk-deb10	max9s-264	Success	Backup Copy (Cold)	1/31/2023 12:00 AM	–

Viewing job details

To view job details:

- 1 In the Recent jobs view, locate the job in the list below the graph. (If needed, sort or filter the display. See "[Filtering the Recent jobs view](#)" above.)
- 2 Click on the job. These details display in the Job Log:
 - Name – Job name.

- ID – Job ID assigned by the Unitrends appliance.
- Mode – Job mode.
 - For backups and hot backup copies: Full, Incremental, Differential, Selective, or Bare Metal (Windows only).
 - For cold backup copies: Backup Copy.
 - For certification (DCA) jobs: Test.
- Result – Job result: Success, Warning, or Error.
- Size – Size of the backup or backup copy.
- Output – Job log raw output. Review to determine why a job did not complete successfully.

3 To exit the Job Log, click the X icon.


The screenshot displays the UniView interface. On the left, the 'Jobs' section shows a table of active jobs. A callout '1' points to a job entry. The main area shows the 'Job Log' for a selected job, with callouts '2' and '3' pointing to the 'Review output to troubleshoot errors' button and the 'Click to close the log' button, respectively. The job log shows the job name 'Backup Copy Job', ID '1.1675238400.1.1', mode 'Backup Copy', and result 'Error'. The output section contains the message: 'Failed: Failed to get media size'.

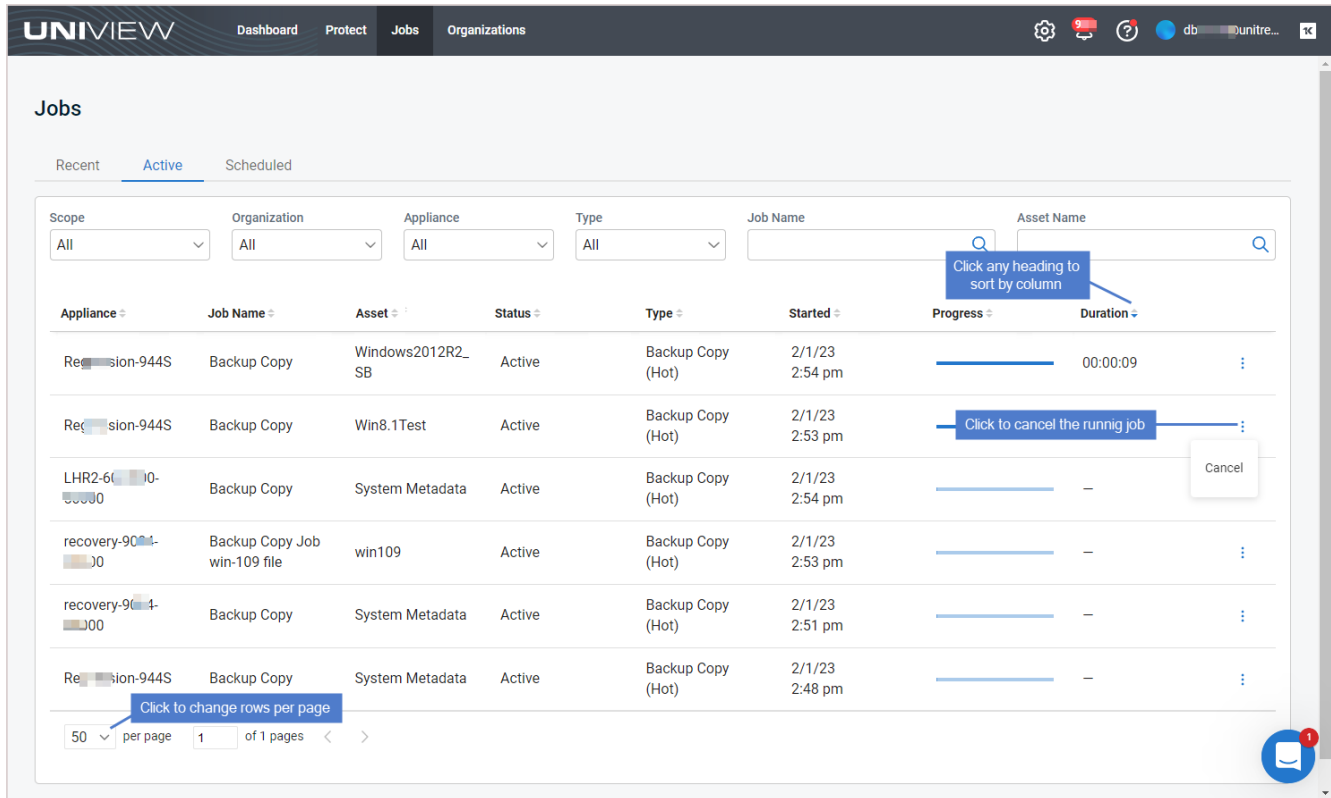
Appliance	Job Name	Asset	Status
max9s-264	Backup Copy Job	max9s-264	Error
max9s-264	Backup Copy Job	max9s-264	Error
max9s-264	Backup Copy Job	max9s-264	Error
max9s-264	Backup Copy Job	max9s-264	Error

Viewing active jobs

The Active jobs view displays all jobs that are currently running across all Unitrends appliances that have been added to your backup.net instance. To change the sort order of the display, click any column heading. (To filter the display, see "Filtering the Active jobs view".)

The following information is given for each active job:

- Appliance – Name of the appliance where the job is running.
- Job Name – Name of the job.
 - If initiated by a UniView backup policy, the job name is "UniView-AssetName".
 - If initiated by the Unitrends appliance, the job name is the Unitrends job name.
- Asset – Name of the asset.
- Status – Job status.
- Type – Job type: Backup, Backup Copy Hot, Backup Copy Cold, or Certification (DCA job).
- Started – Date and time at which the job started.
- Progress – Job progress bar.
- Duration – Amount of time that has elapsed since the job started, in *hh:mm:ss* format (hours, minutes, seconds).
-  icon – Click to cancel the job.



The screenshot shows the UniView Jobs page with the following components:

- Navigation:** Dashboard, Protect, Jobs, Organizations.
- Filters:** Scope (All), Organization (All), Appliance (All), Type (All), Job Name, Asset Name.
- Table Headers:** Appliance, Job Name, Asset, Status, Type, Started, Progress, Duration.
- Table Rows:**
 - Row 1: Re...sion-944S, Backup Copy, Windows2012R2_SB, Active, Backup Copy (Hot), 2/1/23 2:54 pm, Progress bar, 00:00:09, More options icon.
 - Row 2: Re...sion-944S, Backup Copy, Win8.1Test, Active, Backup Copy (Hot), 2/1/23 2:53 pm, Progress bar, More options icon.
 - Row 3: LHR2-6...00-...000, Backup Copy, System Metadata, Active, Backup Copy (Hot), 2/1/23 2:54 pm, Progress bar, Cancel button.
 - Row 4: recovery-90...1-...00, Backup Copy Job win-109 file, win109, Active, Backup Copy (Hot), 2/1/23 2:53 pm, Progress bar, More options icon.
 - Row 5: recovery-90...1-...00, Backup Copy, System Metadata, Active, Backup Copy (Hot), 2/1/23 2:51 pm, Progress bar, More options icon.
 - Row 6: Re...sion-944S, Backup Copy, System Metadata, Active, Backup Copy (Hot), 2/1/23 2:48 pm, Progress bar, More options icon.
- Annotations:**
 - "Click any heading to sort by column" points to the Job Name header.
 - "Click to cancel the running job" points to the More options icon in the second row.
 - "Click to change rows per page" points to the pagination control.
- Pagination:** 50 per page, 1 of 1 pages.

Click a row to view these job details:

- Name – Name of the job.
- Job ID
- Client Name – Name of the asset.

- Appliance – Name of the Unitrends appliance.
- Message – Job status message.

The screenshot shows the UniView Jobs page. The top navigation bar includes Dashboard, Protect, Jobs, and Organizations. The Jobs page has tabs for Recent, Active, and Scheduled. Below the tabs are filter dropdowns for Scope, Organization, Appliance, Type, and Job Name. A table lists jobs with columns for Appliance, Job Name, Asset, Status, Type, and Started. A blue callout '1' points to a row with the message 'Click a row'. To the right, the Job Detail panel shows information for a 'Backup Copy' job, including Job ID, Client Name, Appliance, and a Message: 'Processing (3/4)'. A blue callout '2' points to the 'Job details display' button in the Job Detail panel.

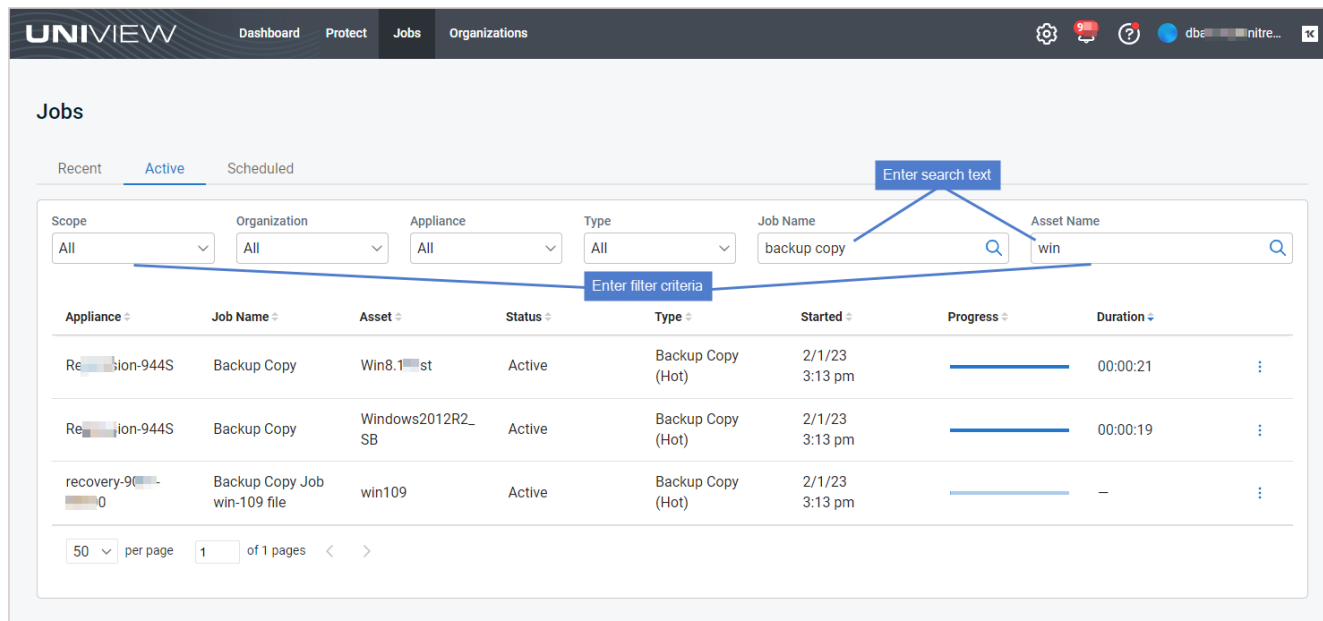
Appliance	Job Name	Asset	Status	Type	Started
Re-ion-944S	Backup Jo HYP	PC_win11-inc-live	Cancelled	Backup	2/1/23 3:01 pm
Re-ion-944S	L-ALL ASSETS 5	A	Cancelled	Backup	2/1/23 3:06 pm
Re-ion-944S	Backup Copy	Win8.1Test	Active	Backup Copy (Hot)	2/1/23 3:08 pm
Re-ion-944S	Backup Copy	Windows2012R2_SB	Active	Backup Copy (Hot)	2/1/23 3:08 pm

Filtering the Active jobs view

The Active jobs view displays all jobs that are currently running or completed in the last few minutes, across all Unitrends appliances that have been added to your backup.net instance.

To filter the display, enter filter criteria in any of the following:

- Scope – Select a scope from the list. (Select **All** to clear the scope filter.)
- Organization – Select an organization from the list. (Select **All** to clear the organization filter.)
- Appliance – Select an appliance from the list. (Select **All** to clear the appliance filter.)
- Type – Select a job type from the list. (Select **All** to clear the job type filter.)
- Job Name – Enter a text string, then press **Enter** to apply. Job names containing the text you entered display.
- Asset Name – Enter a text string, then press **Enter** to apply. Asset names containing the text you entered display.



Working with scheduled jobs

Use the Schedules view for the following:

- "Viewing scheduled jobs"
- "Filtering the Scheduled jobs view"
- "Viewing schedule details"
- "Running a scheduled job on-demand"
- "Disabling or enabling a job schedule"
- "Deleting a job schedule"

Viewing scheduled jobs


The Scheduled job view displays job schedules across all Unitrends appliances that have been added to your backup.net instance. To change the sort order of the display, click any column heading. (To filter the display, see "Filtering the Scheduled jobs view".)

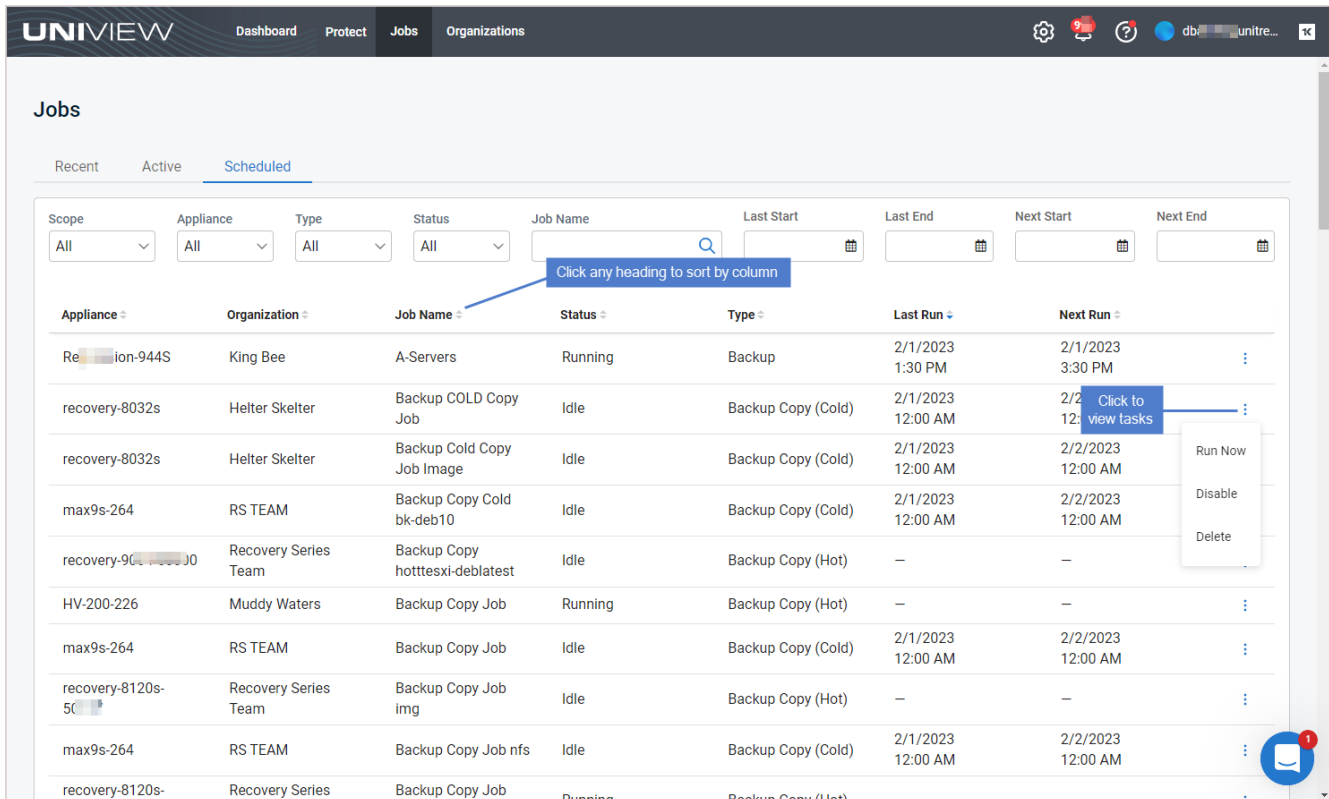
The following information is given for each schedule:

- Appliance – Name of the appliance.
- Organization – Organization name.
- Job Name – Name of the job.
 - If initiated by a UniView backup policy, the job name is "UniView-AssetName".
 - If initiated by the Unitrends appliance, the job name is the Unitrends job name.

- Status – Schedule status: Idle (no jobs are currently running) or Running (one or more jobs are currently running).
- Type – Schedule type: Backup, Backup Copy Hot, Backup Copy Cold, or Certification (DCA job).
- Last Run – Most recent date and time at which this schedule ran.
- Next Run – Next date and time at which this schedule will run.

Note: Hot copies run automatically as eligible local backups complete. Next Run time does not apply.

-  icon – Click to access additional schedule tasks (Run Now, Disable, and Delete).



The screenshot shows the UniView Jobs page with the following table of scheduled jobs:

Appliance	Organization	Job Name	Status	Type	Last Run	Next Run	
Re-ion-944S	King Bee	A-Servers	Running	Backup	2/1/2023 1:30 PM	2/1/2023 3:30 PM	⋮
recovery-8032s	Helter Skelter	Backup COLD Copy Job	Idle	Backup Copy (Cold)	2/1/2023 12:00 AM	2/2/2023 12:00 AM	⋮
recovery-8032s	Helter Skelter	Backup Cold Copy Job Image	Idle	Backup Copy (Cold)	2/1/2023 12:00 AM	2/2/2023 12:00 AM	⋮
max9s-264	RS TEAM	Backup Copy Cold bk-deb10	Idle	Backup Copy (Cold)	2/1/2023 12:00 AM	2/2/2023 12:00 AM	⋮
recovery-90-10000 J0	Recovery Series Team	Backup Copy hotttesxi-deblatest	Idle	Backup Copy (Hot)	–	–	⋮
HV-200-226	Muddy Waters	Backup Copy Job	Running	Backup Copy (Hot)	–	–	⋮
max9s-264	RS TEAM	Backup Copy Job	Idle	Backup Copy (Cold)	2/1/2023 12:00 AM	2/2/2023 12:00 AM	⋮
recovery-8120s-50	Recovery Series Team	Backup Copy Job img	Idle	Backup Copy (Hot)	–	–	⋮
max9s-264	RS TEAM	Backup Copy Job nfs	Idle	Backup Copy (Cold)	2/1/2023 12:00 AM	2/2/2023 12:00 AM	⋮
recovery-8120s-	Recovery Series	Backup Copy Job	Running	Backup Copy (Hot)	–	–	⋮

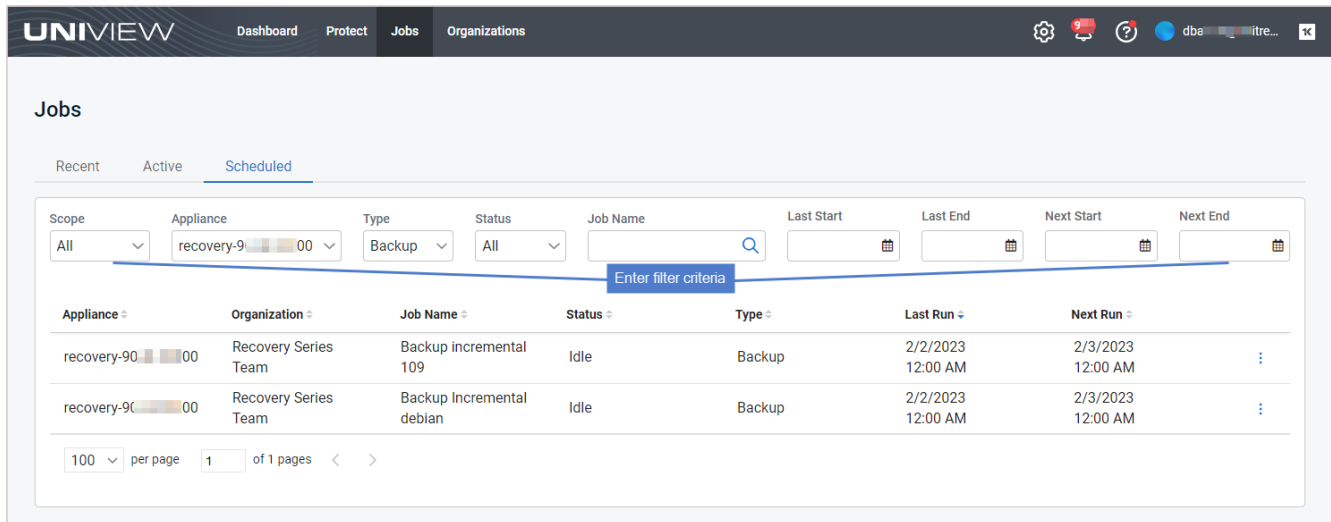
Filtering the Scheduled jobs view

The Scheduled jobs view displays job schedules across all appliances that have been added to your backup.net instance.

To filter the display, enter filter criteria in any of the following:

- Scope – Select a scope from the list. (Select **All** to clear the scope filter.)
- Appliance – Select an appliance from the list. (Select **All** to clear the appliance filter.)
- Type – Select a job type from the list. (Select **All** to clear the job type filter.)
- Status – Select Idle, Running, Failover, or InstantLab to filter by job status. (Select **All** to clear the status filter.)

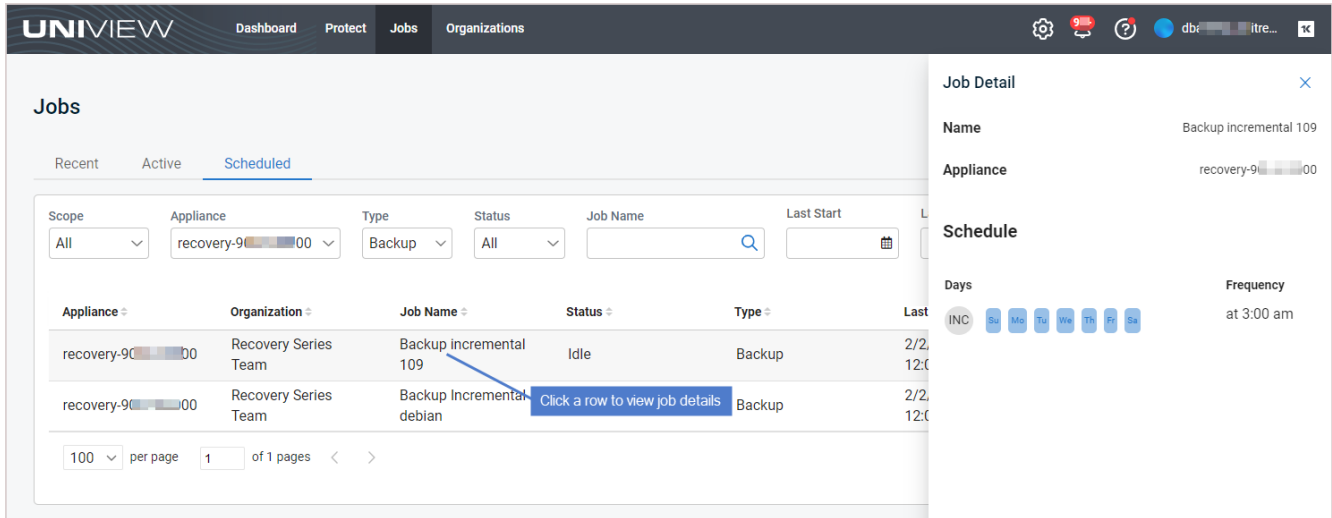
- Job Name – Enter a text string, then press **Enter** to apply. Job names containing the text you entered display.
- Last Start – Date and time at which the most recent job started.
- Last End – Date and time at which the most recent job ended.
- Next Start – Date and time at which the next job is scheduled to start.
- Next End – Date and time at which the next job will end.



Viewing schedule details

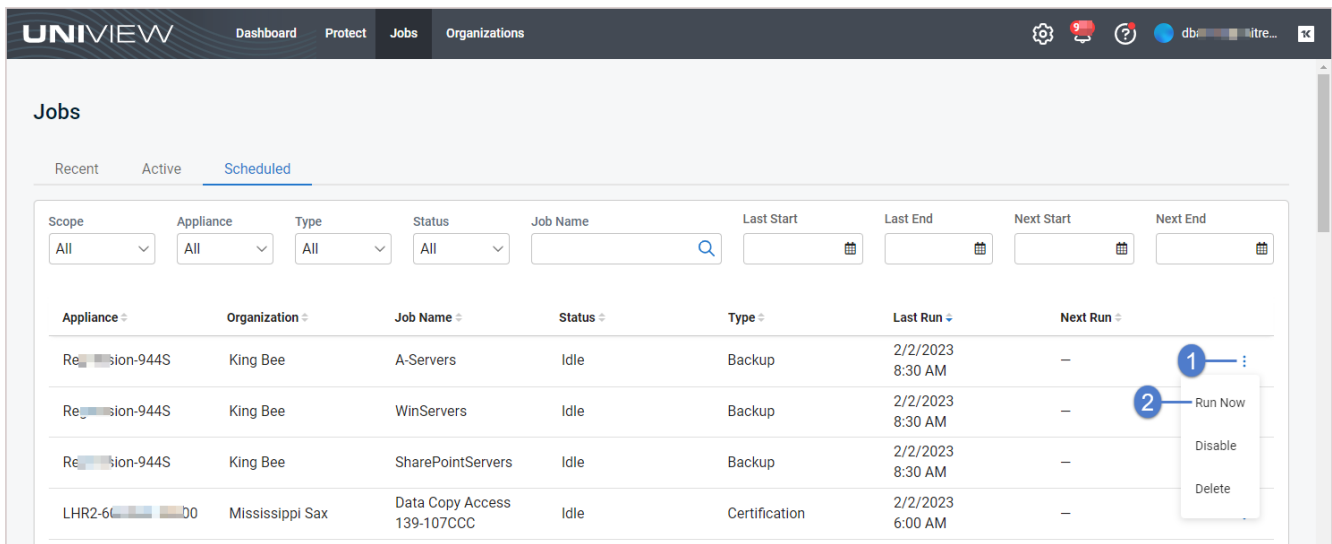
To view schedule details:

- 1 In the Scheduled jobs view, click a row in the list.
- 2 The following schedule details display:
 - Name – Job name.
 - If initiated by a UniView backup policy, the job name is "UniView-AssetName".
 - If initiated by the Unitrends appliance, the job name is the Unitrends job name.
 - Appliance – Appliance name.
 - Schedule Days – Days when the schedule runs.
 - Schedule Frequency – Time(s) at which the schedule runs each day.



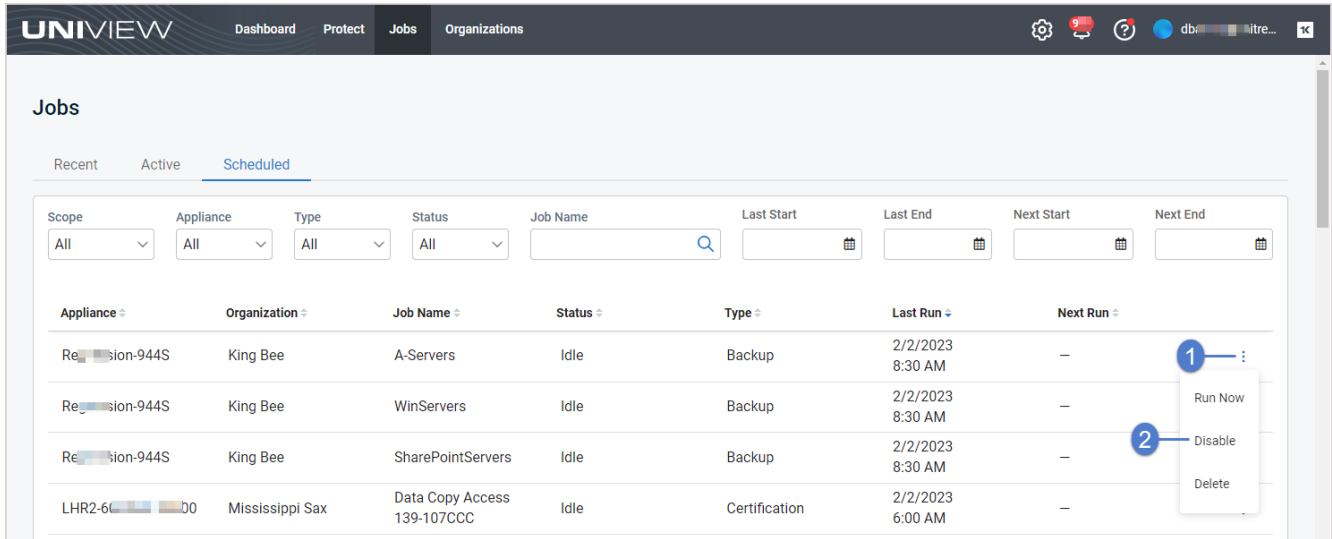
Running a scheduled job on-demand

To run a scheduled job now, click the schedule's  icon, and select **Run Now**:



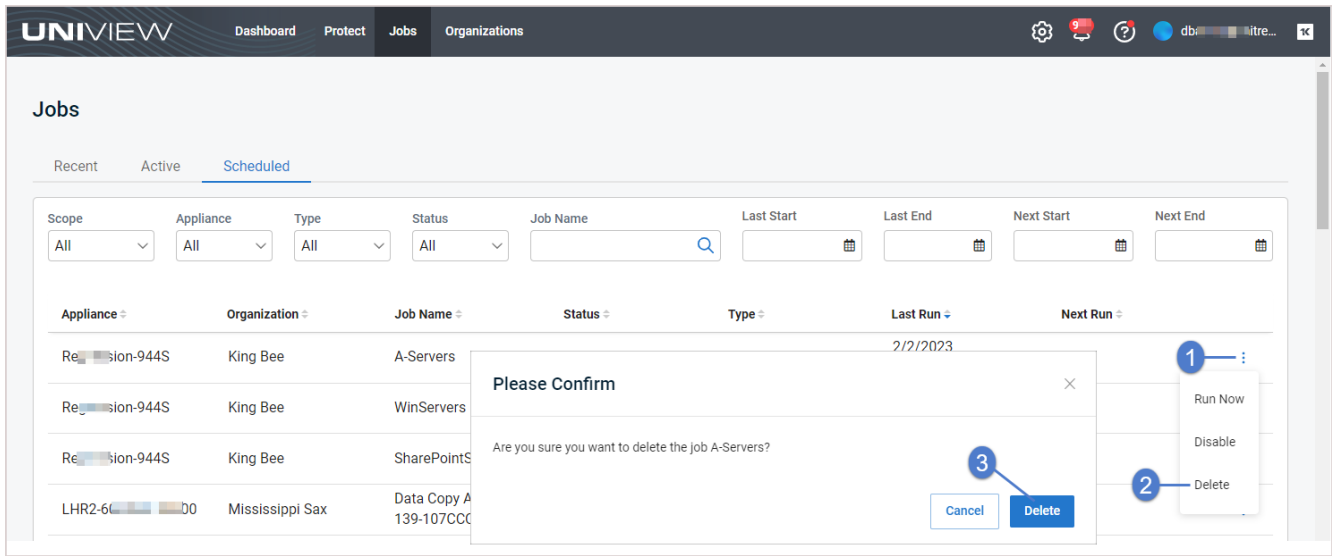
Disabling or enabling a job schedule

To disable or enable a scheduled job, click the schedule's  icon, and select **Disable** or **Enable**:



Deleting a job schedule

To delete a scheduled job, click the schedule's  icon, and select **Delete**. Click **Delete** to confirm:

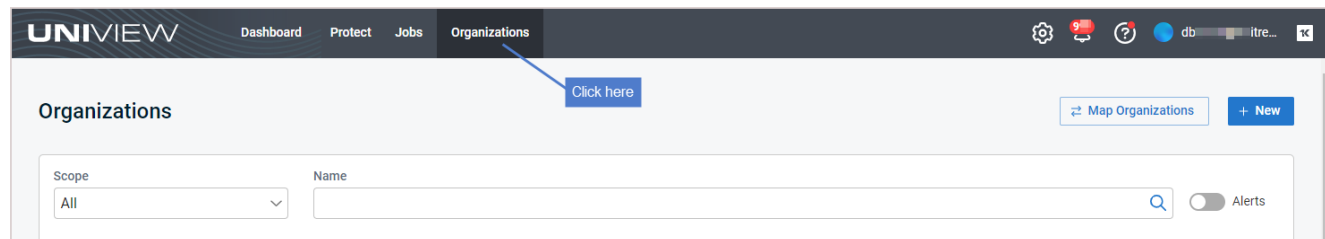


This page is intentionally left blank.



Working with Organizations

Use the Organizations page to view appliance and asset information by organization and to add or modify organizations. To access the Organizations page, click **Organizations**:



See these topics for details:

- ["Viewing appliances and assets by organization"](#)
- ["Filtering the Organizations page"](#)
- ["Adding an organization"](#)
- ["Importing organizations from Autotask, ConnectWise Manage, BMS, or Vorex"](#)
- ["Editing an organization"](#)
- ["Mapping companies and accounts to organizations"](#)
- ["Mapping Datto Portal clients to organizations"](#)
- ["Deleting an organization"](#)

Viewing appliances and assets by organization

The Organizations page displays all Unitrends organizations that have been added to your backup.net instance. To change the sort order of the display, click any column heading. (To filter the display, see ["Filtering the Organizations page"](#).)

The following information is given for each organization:

- Name – Organization name.
- Scope – Scope to which the organization is assigned.
- Appliances – Number of Unitrends appliances in the organization's environment.
- Alerts – Number of unresolved alerts across the organization's appliances.
- Free Space – The total amount of free space across the organization's appliances, shown as a percent of total appliance space.
- icon – Click to delete the organization or modify BMS, Vorex, Autotask, or ConnectWise settings. (For details, see ["Working with Integrations"](#).)

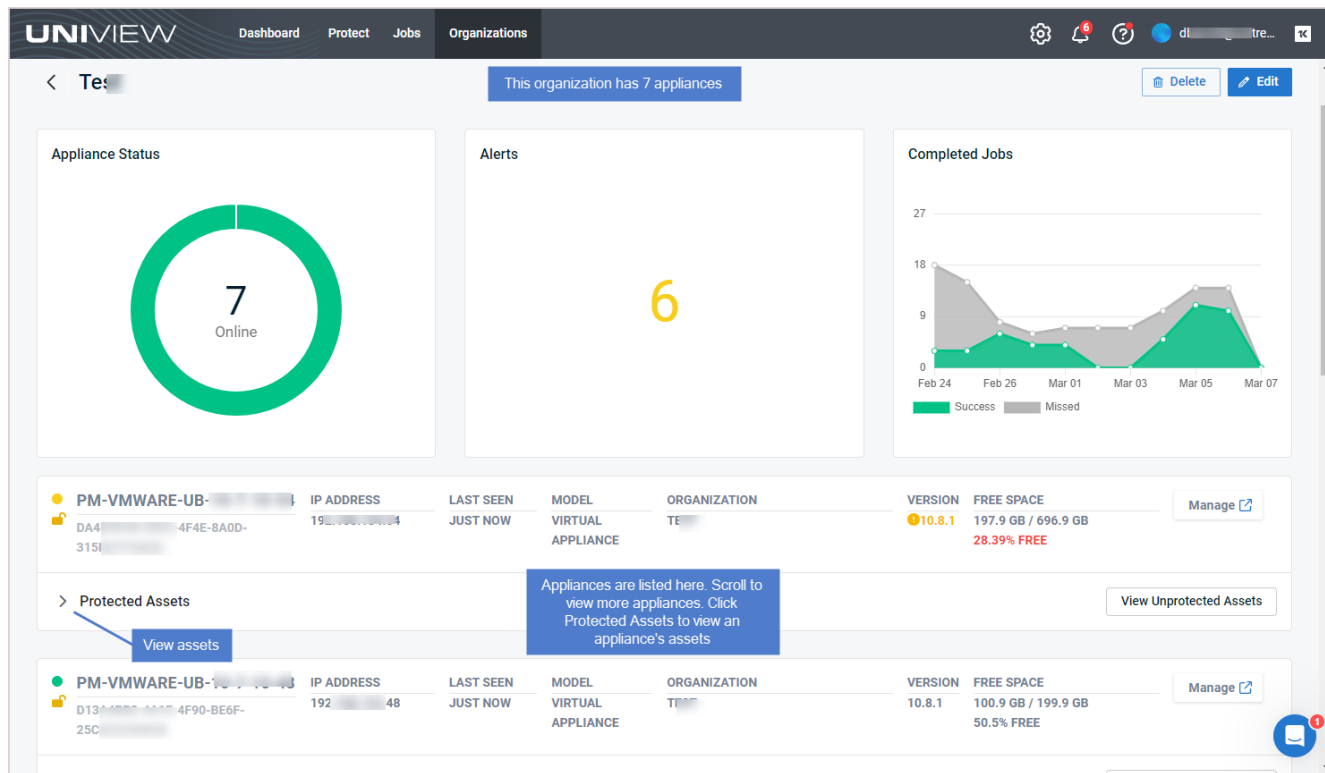
The screenshot shows the 'Organizations' page in the UniView portal. At the top, there are navigation tabs for Dashboard, Protect, Jobs, and Organizations. The main content area features a search bar with 'Scope' (set to 'All') and 'Name' fields. Below this is a table of organizations. A callout points to the column headers with the text 'Click any heading to sort by column'. Another callout points to a three-dot menu icon on the right side of the table, with the text 'Click to delete or modify PSA settings'. This menu is open, showing options for 'ConnectWise Settings', 'BMS Settings', and 'Autotask Settings'.

Name	Scope	Appliances	Alerts	Free Space
Recovery Series Team	Unitrends RS	2	1	98.41%
RS TEAM	Unitrends RS	1	0	78.35%
King Bee	My Scope	1	1	65.77%
Helter Skelter	Beat	1	2	7.82%
Mississippi Sax	My Scope	1	1	15.31%
Muddy Waters	Beat	1	0	72.62%

Click an organization in the list to view the organization's appliances and assets:

This screenshot shows the 'Organizations' page with a different set of data. A callout points to the 'Stroman - Koeppe' organization in the table with the text 'Click to view organization details'.

Name	Scope	Appliances	Alerts	Free Space
Stokes - Gerhold	Unassigned	0	0	100%
Stroman - Koeppe	Unassigned	0	0	100%
Te...	sc...	7	4	18.14%

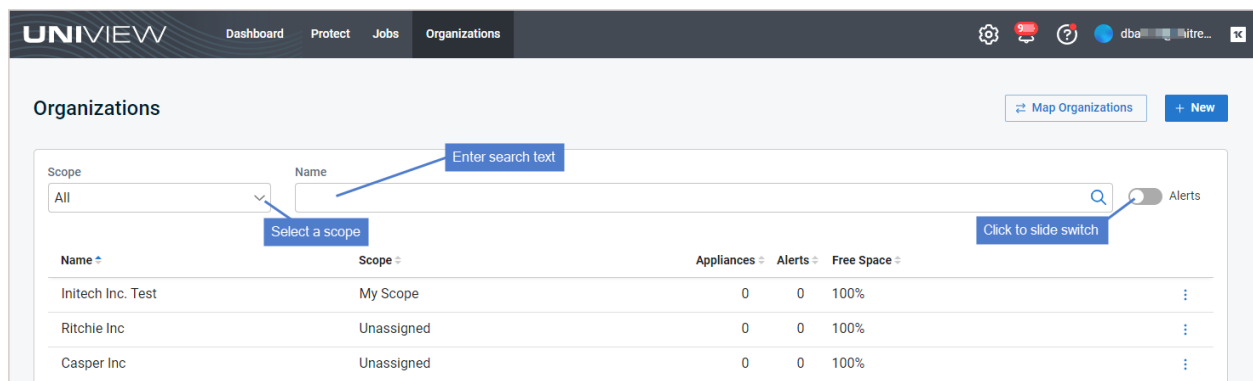


Filtering the Organizations page

The Organizations page displays all organizations that have been added to your backup.net instance.

To filter the display, enter filter criteria in any of the following:

- Scope - Select a scope from the list.
- Name field - Enter a text string, then press **Enter** to apply. Organization names containing the text you entered display.
- Alerts - Click to slide the switch. Appliances with unresolved alerts display.

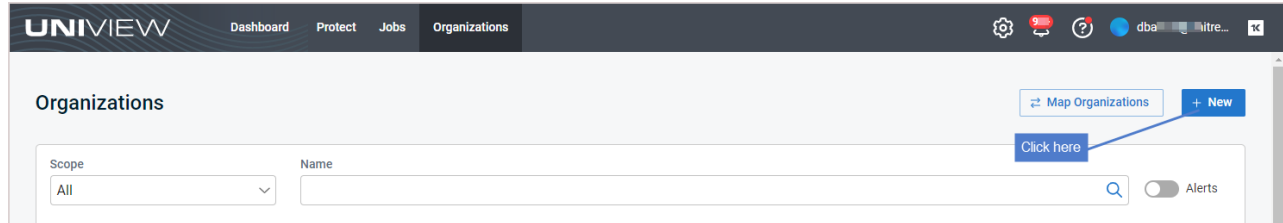


Adding an organization

Note: If you have integrated your PSA, do not use this procedure. Instead, add new accounts or companies to your PSA. Once accounts or companies have been added, import them into the UniView Portal as described in "Importing organizations from Autotask, ConnectWise Manage, BMS, or Vorex".

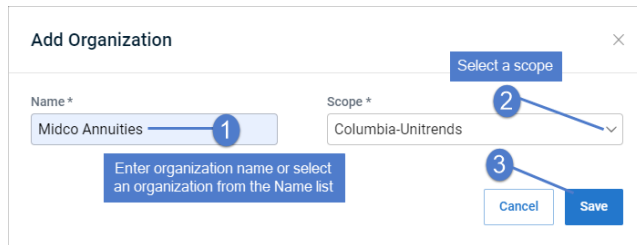
To add an organization:

- 1 On the Organizations page, click **+ New**.

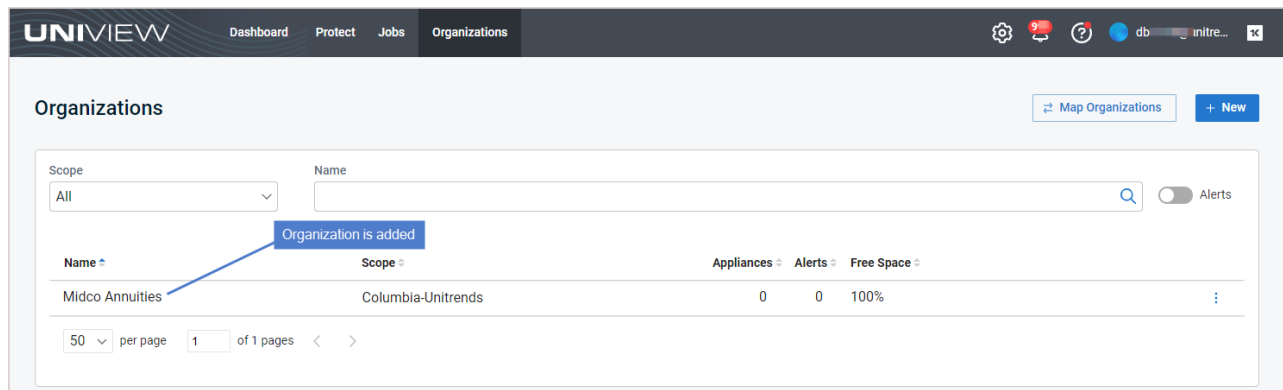


- 2 Enter the organization name.
- 3 Select a scope, and click **Save**:

Note: A user's scope determines which organizations are visible in the UniView Portal. To ensure that users can only access information about organizations specified in their scope(s), you must assign each organization to a scope.



- 4 The organization is added and displays on the Organizations page.

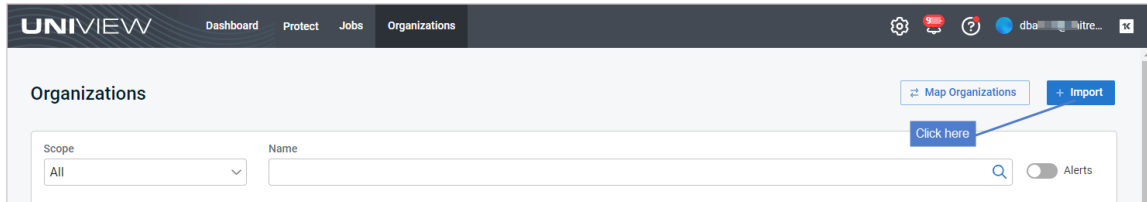


Importing organizations from Autotask, ConnectWise Manage, BMS, or Vorex

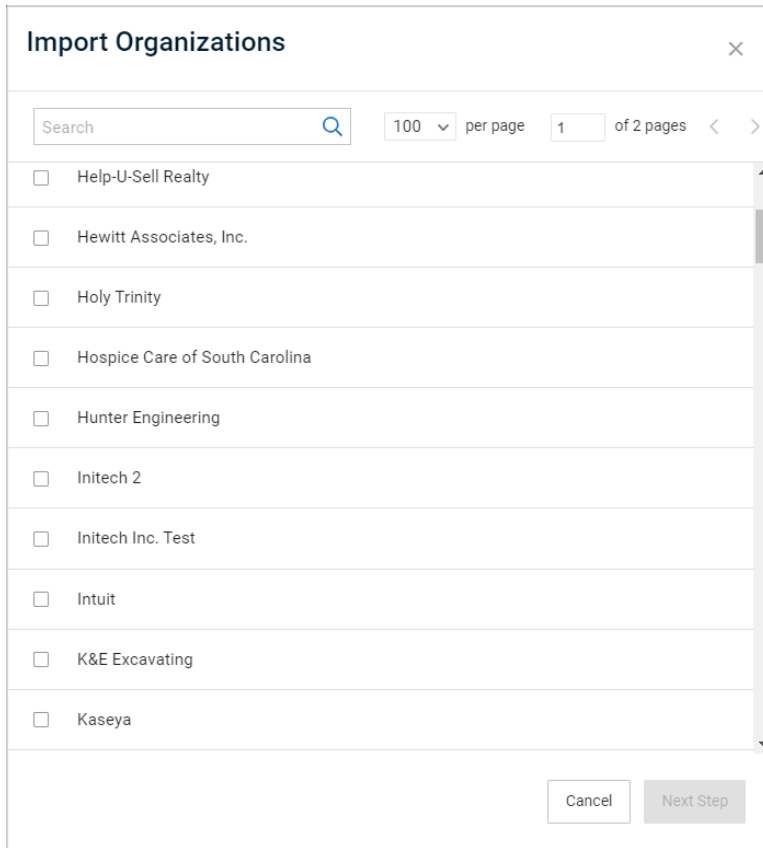
If you have integrated your PSA, add new accounts or companies to the PSA. Once accounts or companies have been added, use this procedure to import them into the UniView Portal.

To import organizations

- 1 On the Organizations page, click **Import**.



Organizations are imported:



- 2 Assign organizations to a scope:

Notes:

- A user's scope determines which organizations are visible in the UniView Portal. To ensure that users can only access information about organizations specified in their scope(s), you must assign each organization to a scope.
- In this procedure, the organizations you select are assigned to one scope. Repeat these steps to assign organizations to another scope.

- Check boxes to select organizations. Click **Next Step**.

Import Organizations [Close]

Search [Magnifying Glass] 100 per page 1 of 2 pages [Left Arrow] [Right Arrow]

<input type="checkbox"/>	Help-U-Sell Realty
<input type="checkbox"/>	Hewitt Associates, Inc.
<input type="checkbox"/>	Holy Trinity
<input type="checkbox"/>	Hospice Care of South Carolina
<input type="checkbox"/>	Hunter Engineering
<input checked="" type="checkbox"/>	Initech 2
<input checked="" type="checkbox"/>	Initech Inc. Test
<input checked="" type="checkbox"/>	Intuit
<input checked="" type="checkbox"/>	K&E Excavating
<input type="checkbox"/>	Kaseya

[Cancel] [Next Step]

- Select a scope from the list. Click **Save**.

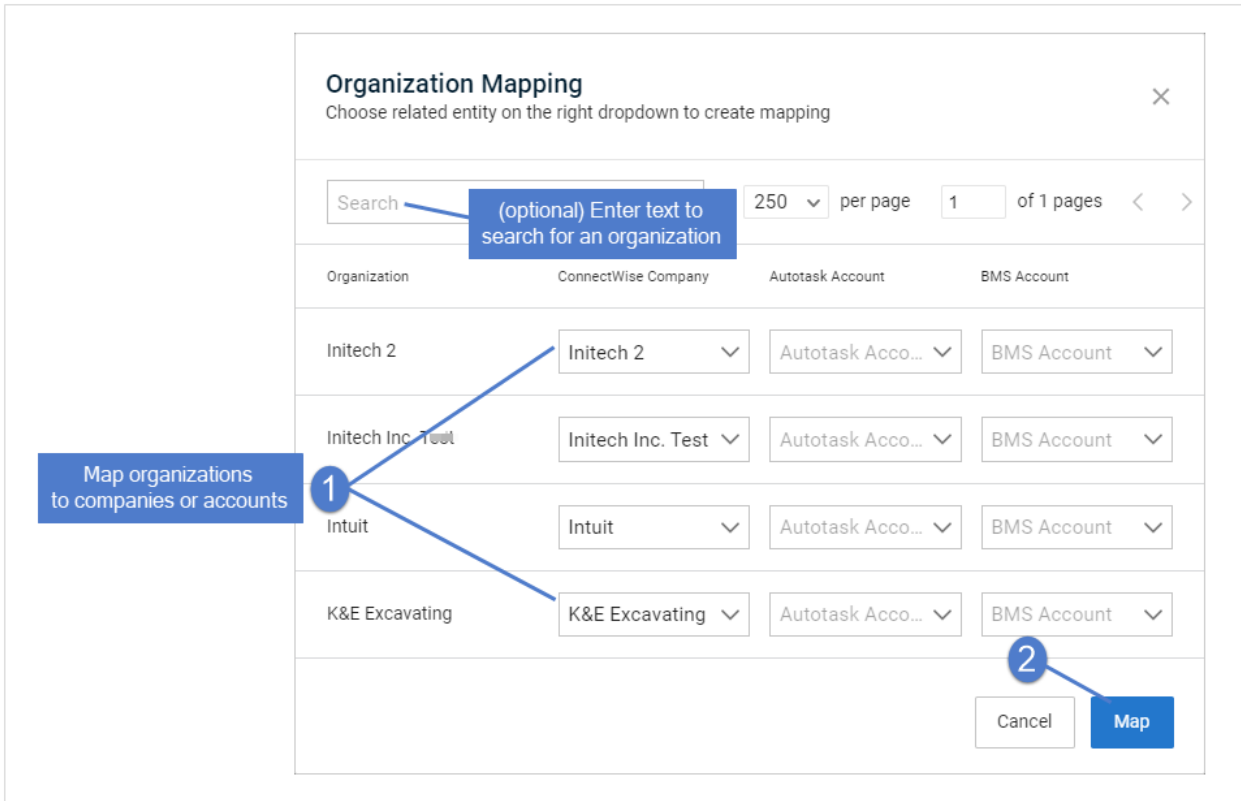
← Import Organizations [Close]

Scope *

My Scope [Down Arrow]

[Cancel] [Save]

- 3 Map organizations to companies or accounts. Click **Map**.

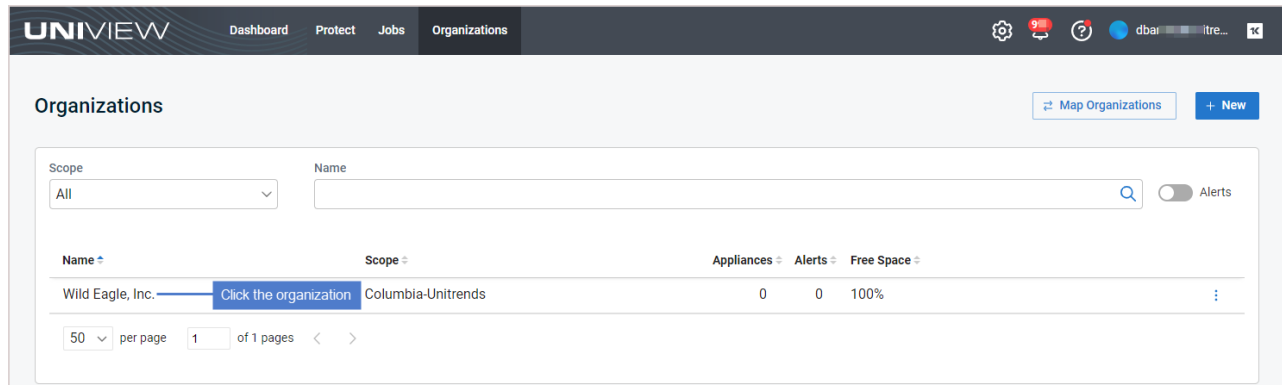


Editing an organization

Note: If ConnectWise Manage, Autotask, BMS, Vorex, or IT Glue has been integrated, you can run additional procedures on the Organizations page. For details, see ["To view or modify one organization's ConnectWise Manage settings"](#), ["To view or modify one organization's Autotask settings"](#), ["To view or modify one organization's BMS or Vorex integration settings"](#), ["To view or modify IT Glue credentials settings"](#), and ["Working with Integrations"](#).

To edit an organization

- 1 On the Organizations page, click the organization row in the list.



2 Click Edit.



3 Modify the organization name and/or scope, and click Save:

Notes:

- A user's scope determines which organizations are visible in the UniView Portal. To ensure that users can only access information about organizations specified in their scope(s), you must assign each organization to a scope.
- You cannot modify the name of a VSA, Autotask, ConnectWise Manage, BMS, Vorex, or IT Glue organization.

Mapping companies and accounts to organizations

By default, the integration's company or account is applied to all of its organizations. Use this procedure to quickly apply different companies or accounts to multiple organizations.

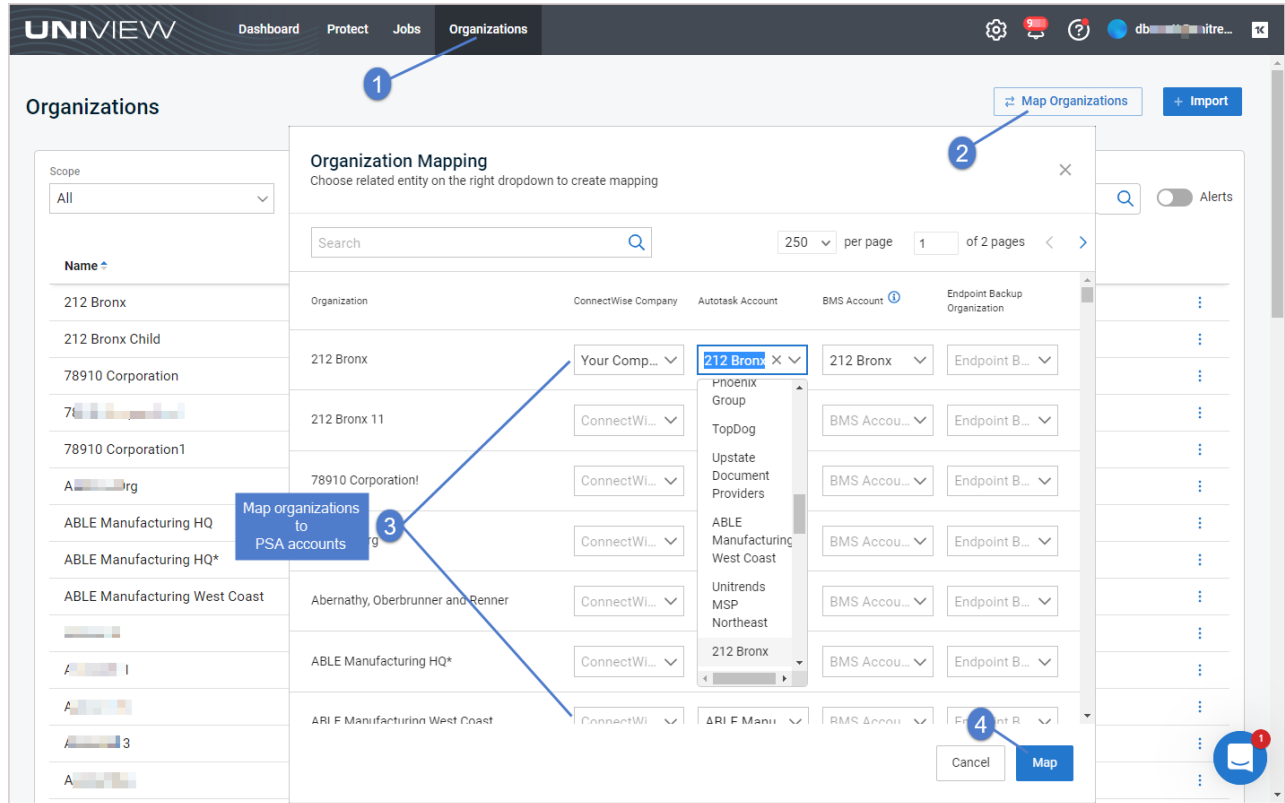
To map companies and accounts to organizations

- 1 Log in to the UniView Portal.
- 2 Select **Organizations**.

- 3 Click **Map Organizations**.
- 4 (Optional) Filter the organization list by entering a text string in the Search field.
- 5 Select a different company or account for one or more organizations.

Note: In the figure below, ConnectWise, Autotask, BMS, and Endpoint Backup integrations have been configured for this UniView Portal instance. If you do not see an integration, it has not been added to your UniView Portal instance.

- 6 Click **Map**.

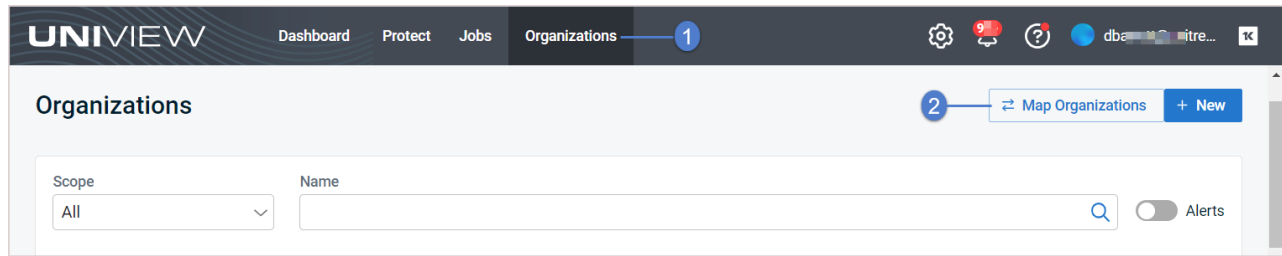


Mapping Datto Portal clients to organizations

When the Datto Portal integration was added, UniView Portal automatically created a mapping for each Datto client. As new clients are added to Datto Portal, they are automatically added to UniView and mapped to a UniView organization. If needed, you can use this procedure to quickly modify mappings for multiple organizations.

To map Datto clients to organizations

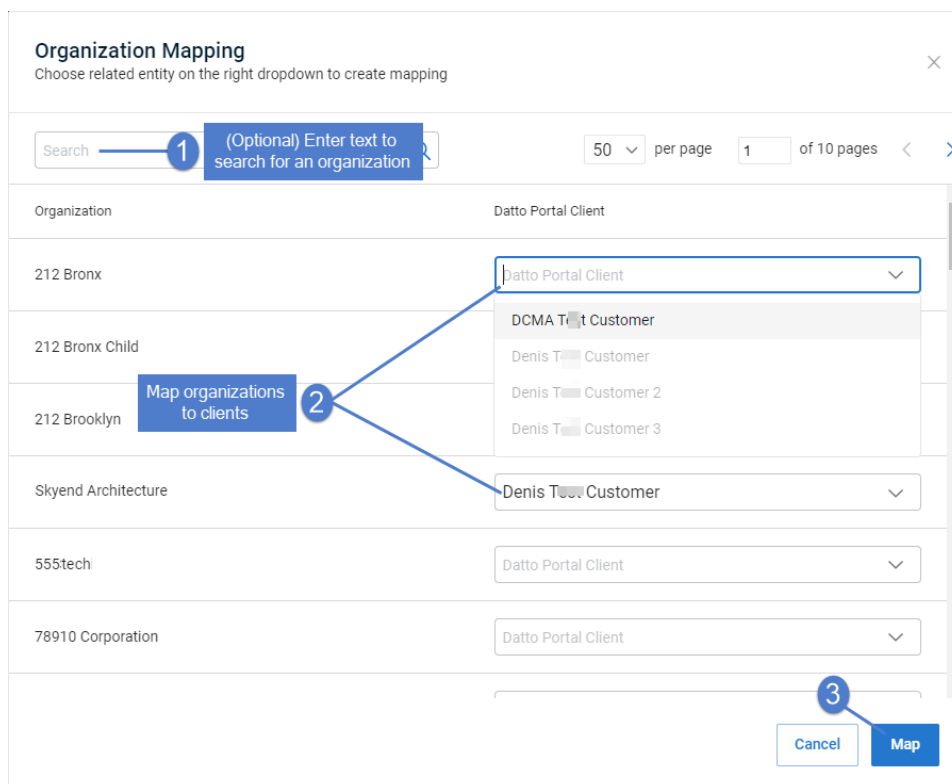
- 1 Log in to the UniView Portal.
- 2 Select **Organizations**.
- 3 Click **Map Organizations**.



- 4 (Optional) Filter the organization list by entering a text string in the Search field.
- 5 In the Datto Portal Client column, select a different client for one or more organizations.

Note: If you do not see a Datto Portal Client column, the Datto integration has not been added to your UniView Portal instance. To add this integration, see "[Integrating Datto Portal](#)".

- 6 Click **Map**.



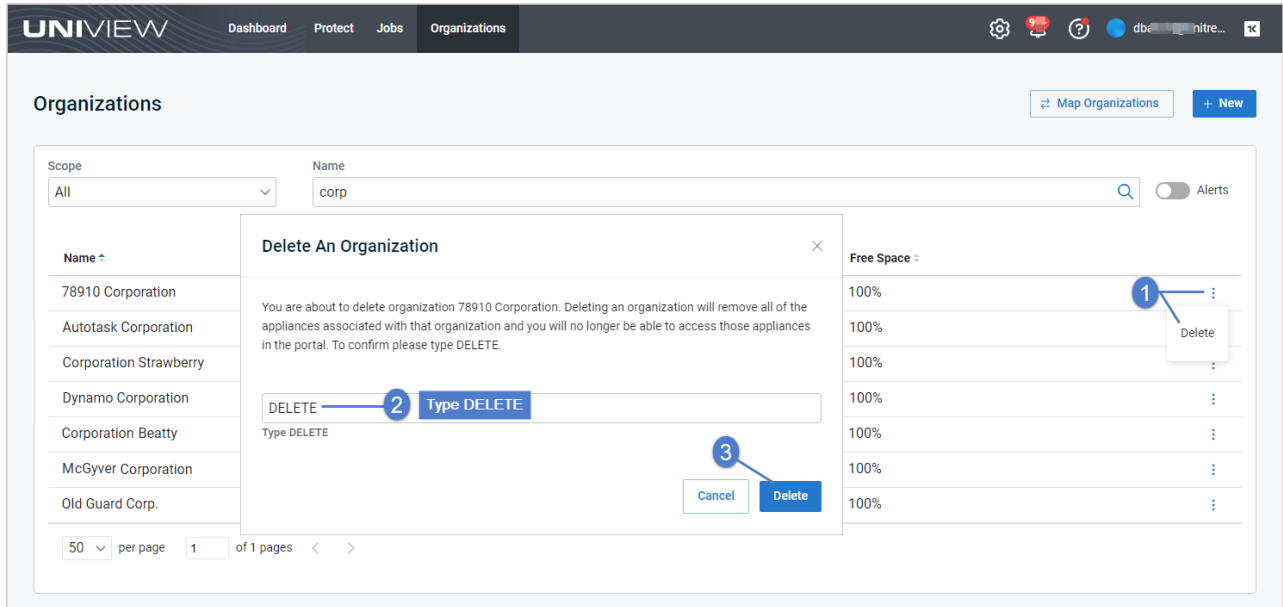
Deleting an organization

Deleting an organization removes the organization and all of the appliances associated with that organization. Upon deleting an organization, you can no longer access those appliances in the UniView Portal.

To delete an organization

- 1 On the Organizations page, click the organization's  icon and select **Delete**.

- 2 To confirm, type DELETE and click **Delete**.



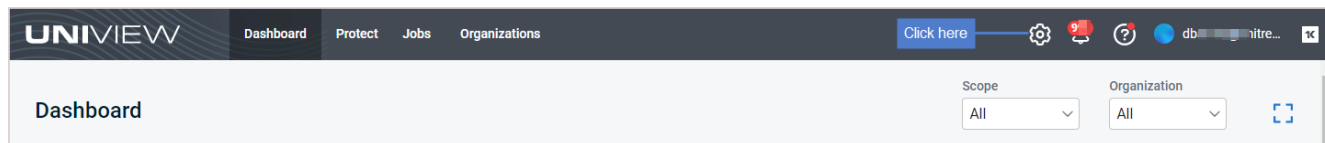
This page is intentionally left blank.



Working with Users and Scopes

Use the procedures in this chapter to view and add portal users, and to add and apply scopes that define which organizations a user can access in the UniView Portal.

Users and scopes are managed from the Settings page. To access the Settings page, click :



Working with users

Use these procedures to manage portal users:

- ["About UniView Portal user accounts"](#)
- ["Viewing users"](#)
- ["Adding a user"](#)
- ["Editing a user"](#)
- ["Enabling a user"](#)
- ["Disabling a user"](#)
- ["Resetting 2FA"](#)
- ["Resending an activation email"](#)

About UniView Portal user accounts

Access to data and features is determined by the *role* and *scope(s)* of the UniView Portal account that the MSP, SMB, or organization uses to log in to the portal. A user's role defines the functions they can perform. The assigned scopes determine the data they can see. Membership in a role and membership in a scope are independent of each other.

- The scope defines which organizations are visible to the user in the UniView Portal. For details, see ["Working with scopes"](#).
- The role defines which features and procedures the user can run:


Role	Description
Superuser	This role can perform all operations for all organizations, including creating and modifying other Superuser accounts, and adding or modifying integrations. Superusers are assigned all scopes and have access to all organizations.

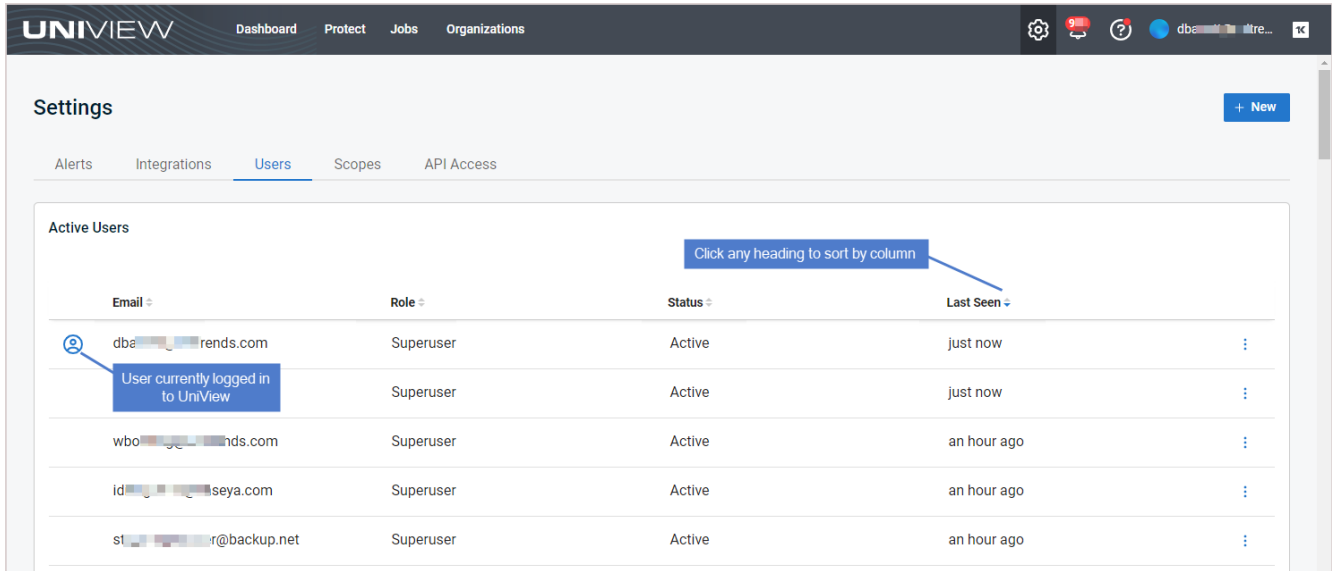
Role	Description
Admin	This role can perform most operations, including appliance configuration, backup job configuration and management, and user creation. Admin users cannot create or modify Superuser accounts, cannot create scopes, and cannot add or modify integrations. Admins can only view and perform operations for certain organizations, based on the scopes assigned to their user account.
Manage	This role has Monitor access and can start backup jobs and modify retention settings.
Monitor	This role has read-only access to the user interface and reports.

Viewing users

The Users view displays all portal users in the scope(s) that are visible in the current UniView Portal session. To change the sort order of the display, click any column heading.

The following information is given for each user:

- Email – Email address used to create the user.
- Role – Role that determines which features and procedures the user can run: Monitor, Manage, Admin, or Superuser. (See "[About UniView Portal user accounts](#)" for details.)
- Status – User status: active, pending activation, or disabled.
- Last seen – Number of days since last login.
-  icon –
 - For active users, click to edit or disable the user account, or to reset the user's two-factor authentication (2FA).
 - For disabled users, click to enable the user account.
 - For users in *pending activation* status, click to resend the *Welcome to UniView* email with an updated **Activate Now** link. (New users must click **Activate Now** to set their password and log in to UniView within 48 hours of receiving the Welcome to UniView email. Resending the email provides a new link with a fresh 48-hour activation window.)



Adding a user

Note: If two-factor authorization (2FA) has been enabled for your UniView Portal instance, new users are automatically prompted to configure the 2FA application when they log in for the first time.

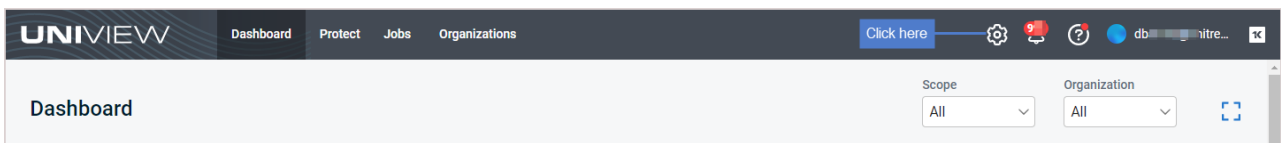
To add a user:

- 1 Log in to the UniView Portal with an account that has the Admin or Superuser role.

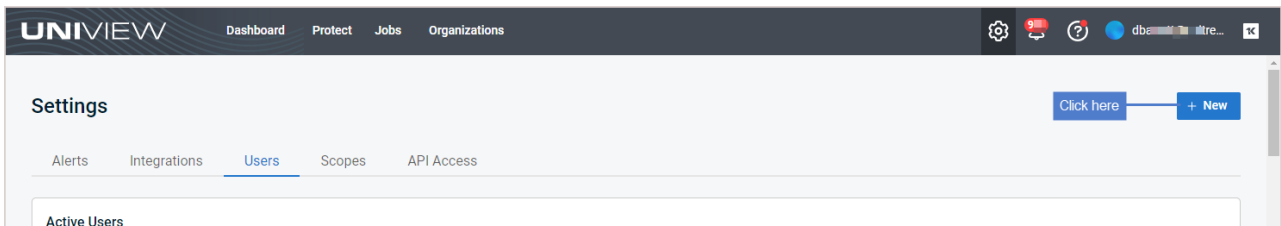
Notes:

- As Admin, you can add a user account and assign it any role other than Superuser.
- As Superuser, you can add a user and assign it any role, including that of Superuser.

- 2 Click :



- 3 In the Users view, click **+ New**.




- 4 Enter the user's email and role.

The role you select determines which features and procedures the user can run. (See ["About UniView Portal user accounts"](#) for details.)

- (If needed) Check the **Add to User Exception List for KaseyaOne Unified Login** box if you require login with KaseyaOne but would like to create an exception for this user. For details, see ["To enable or disable Require Login with KaseyaOne"](#).

Note: This banner displays at the top of the page if Require KaseyaOne Login is enabled:

 Require Log In with KaseyaOne is enabled. If this user does not have a KaseyaOne user account, they will be prevented from logging in. To allow this user to login with local module credentials, add this user to the User Exception list under Require Log In with KaseyaOne.

- Add one or more scopes:
 - To manually assign scopes, click **+ Add another scope**. In the Scopes dialog, check boxes and click **Select** to assign selected scopes to the user.
 - To add access to all scopes, click to enable the **Global Scope** toggle.

Note: The scopes option does not display for the Superuser role as all scopes are accessible to Superuser accounts. You must assign at least one scope to non-Superuser accounts.

- Click **Save**.

The screenshot shows the 'Add User' dialog box with the following elements:

- 1**: Email input field containing 'dbawattuniview@gmail.com'.
- 2**: Role dropdown menu set to 'Manage'.
- 3**: 'Global Scope' toggle (currently off) and '+ Add another scope' button.
- 4**: 'Save' button.


A blue callout box states: "Add scopes: Click **Global Scope** to add all scopes OR Click **+ Add another scope** to select scopes in the Scopes dialog."

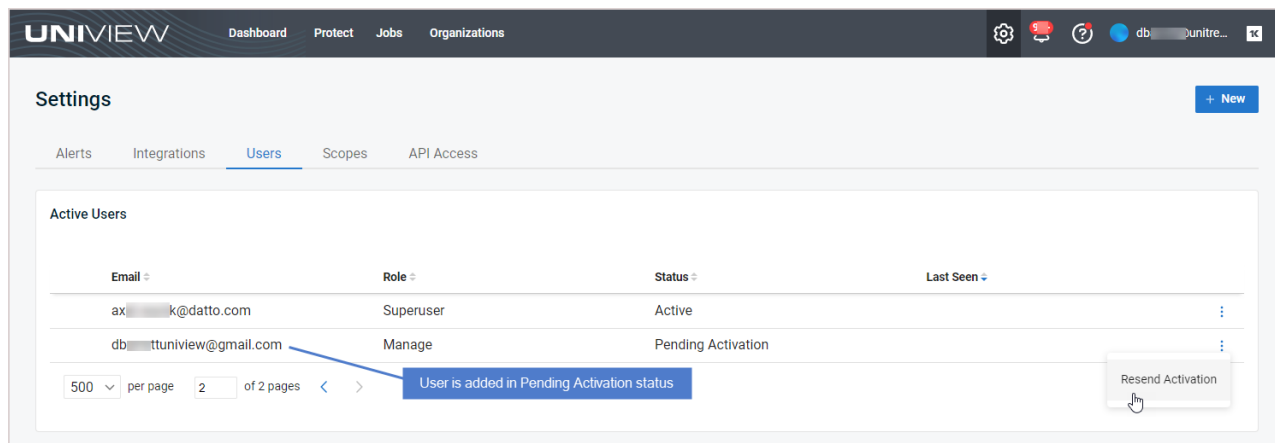
The 'Scopes' dialog box shows a list of scopes with checkboxes:

- Columbia-Unitrends
- Crossroads
- Delta Blues
- Ellada

Buttons 'Cancel' and 'Select' are at the bottom of the 'Scopes' dialog.

- The user is added in *pending activation* status and a *Welcome to UniView* email is sent to the user. The user must click the **Activate Now** button in that email within 48 hours to activate their account. When activated, the user's status changes to *active* on the Users page.

Note: If the user's activation link expires, you can click the user's  icon and select **Resend Activation** to send the user a new link.



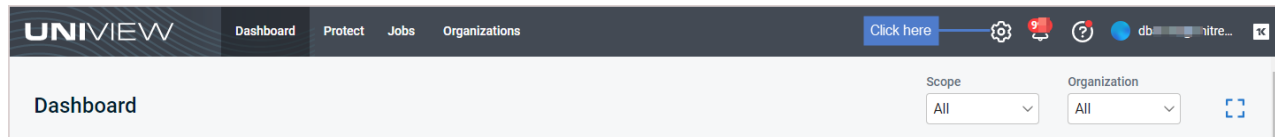
Editing a user

Use these steps to modify the user's role, scopes, and whether the user has an exception for KaseyaOne Unified Login:

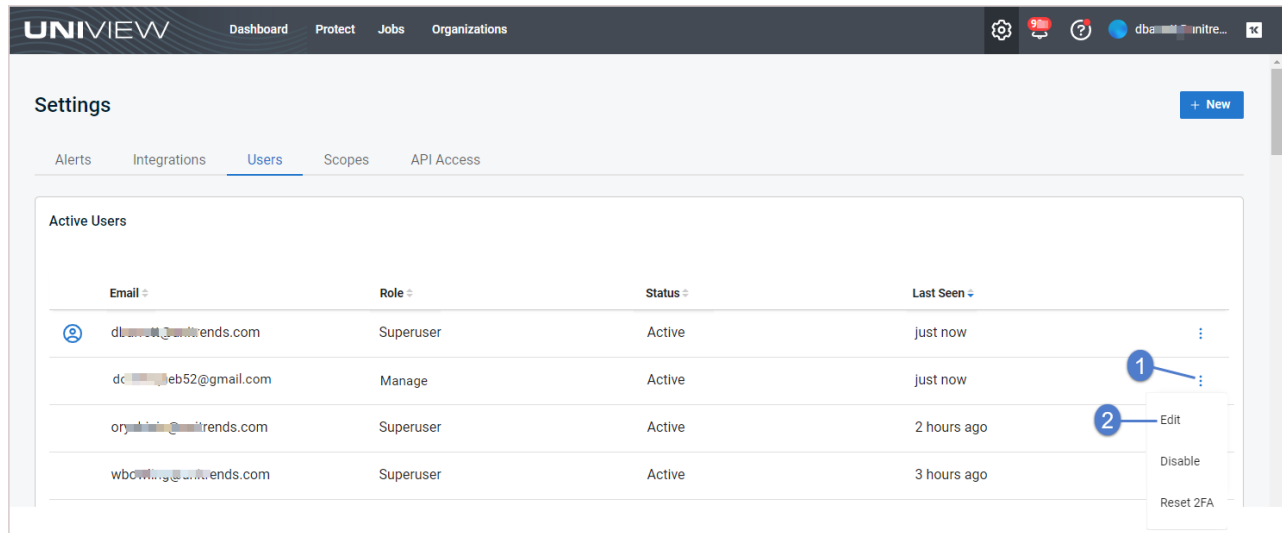
- 1 Log in to the UniView Portal with an account that has the Admin or Superuser role.

Note: As Admin, you cannot modify a superuser account or assign the superuser role to a user account.

- 2 Click :

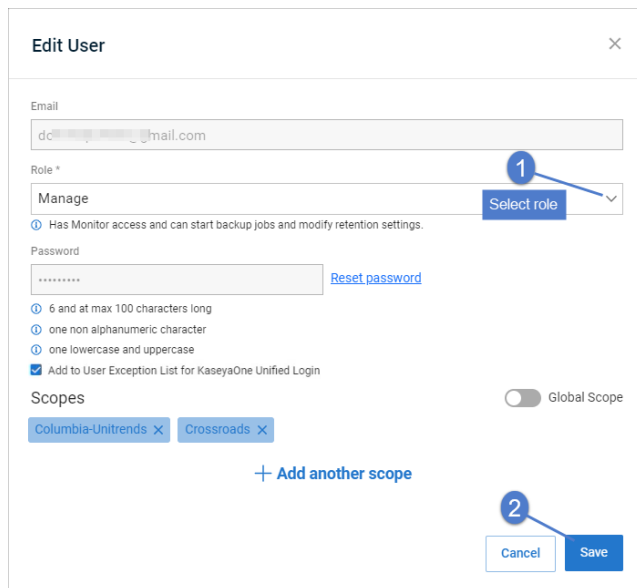


- 3 In the Users view, locate the user, click its  icon, and select **Edit**.



- 4 (Optional) Apply a different role. Select a role, then click **Save**.

The role determines which features and procedures the user can run. (See ["About UniView Portal user accounts"](#) for details.)



- 5 (Optional) Modify the user's *Add to User Exception List for KaseyaOne Unified Login* setting.

- Check the **Add to User Exception List for KaseyaOne Unified Login** box if you require login with KaseyaOne but would like to create an exception for this user.
- Clear the **Add to User Exception List for KaseyaOne Unified Login** box to remove the exception from this user.

Note: This banner displays at the top of the page if Require KaseyaOne Login is enabled:

Require Log In with KaseyaOne is enabled. If this user does not have a **KaseyaOne user account**, they will be prevented from logging in. To allow this user to login with local module credentials, **add this user to the User Exception list** under Require Log In with KaseyaOne.

- (Optional) Modify scope assignment. You can add or remove scopes, or click **Global Scope** to add access to all scopes. Click **Save**.

Note: The scopes option does not display for the Superuser role as all scopes are accessible to Superuser accounts. You must assign at least one scope to non-Superuser accounts.

Edit User

Email
do...@...il.com

Role *
Manage

Has Monitor access and can start backup jobs and modify retention settings.

Password
..... [Reset password](#)

6 and at max 100 characters long
one non alphanumeric character
one lowercase and uppercase
 Add to User Exception List for K... We

Scopes
Columbia-Unitrends X Crossroads X

+ Add another scope

Global Scope

Cancel Save

Scopes

Columbia-Unitrends
 Crossroads
 Delta Blues
 Ellada

Cancel Select

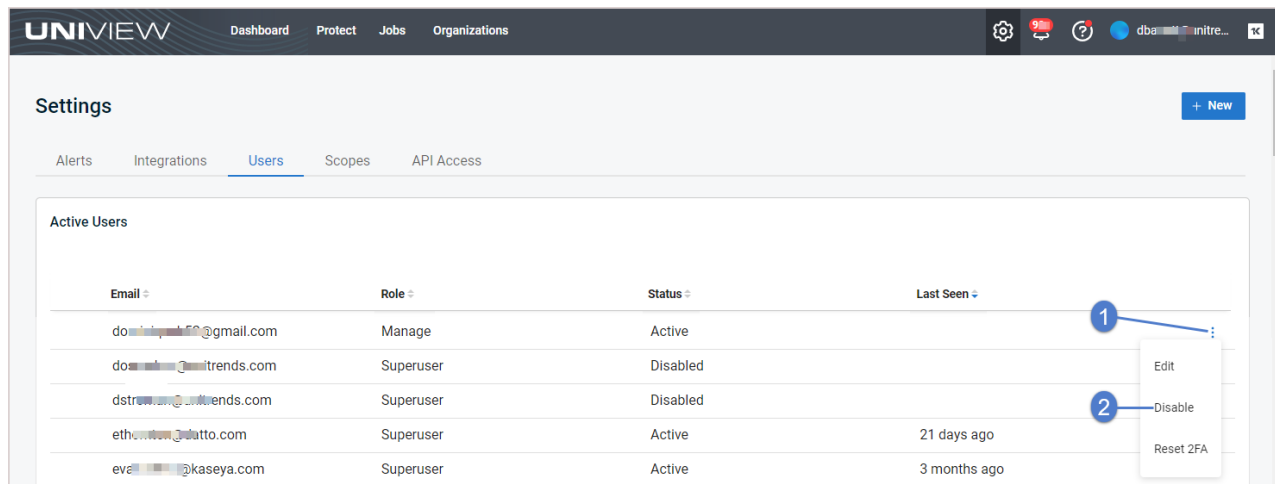
7 (Optional) Reset the user's password:

- Click **Reset Password**.
- Enter and confirm the new password.
- Click **Save**.

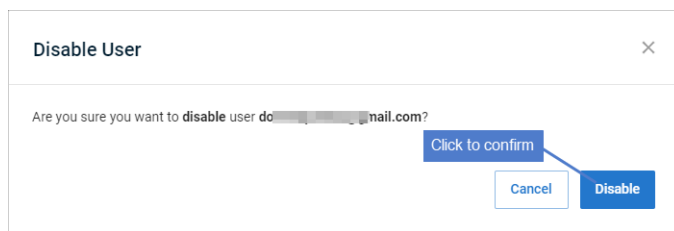
Disabling a user

To disable a user:

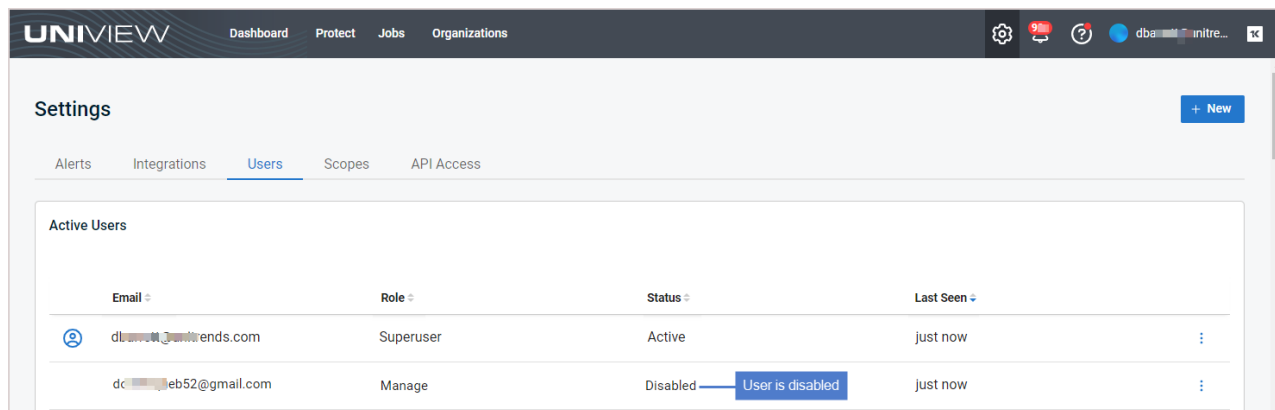
- 1 In the Users view, locate the user, click its **⋮** icon, and select **Disable**.



2 Click **Disable** to confirm.



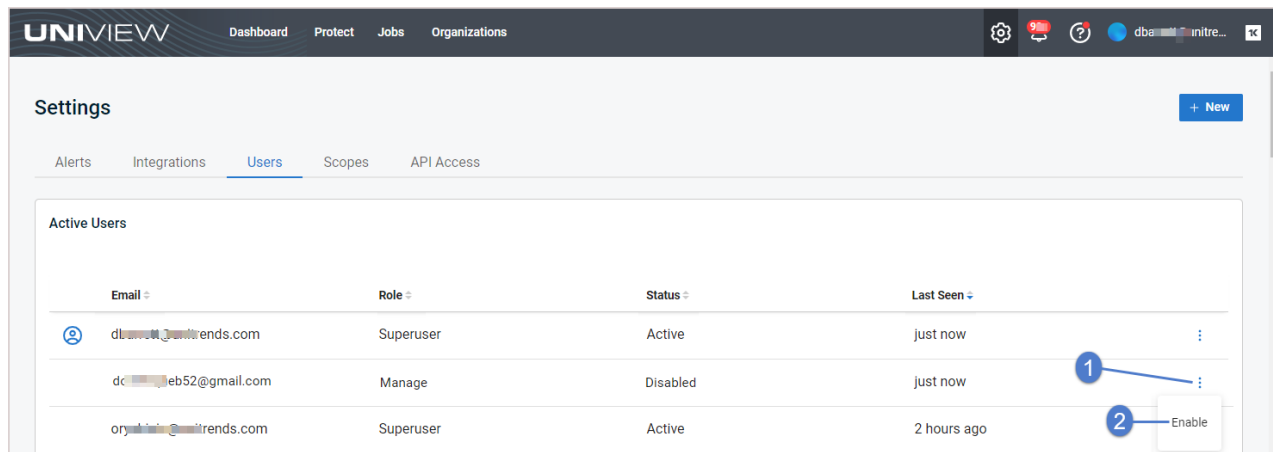
3 The user is disabled.



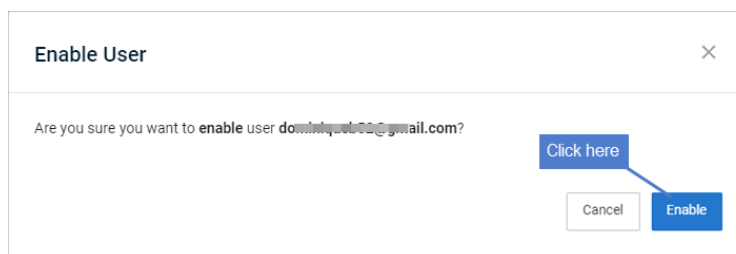
Enabling a user

To enable a user:

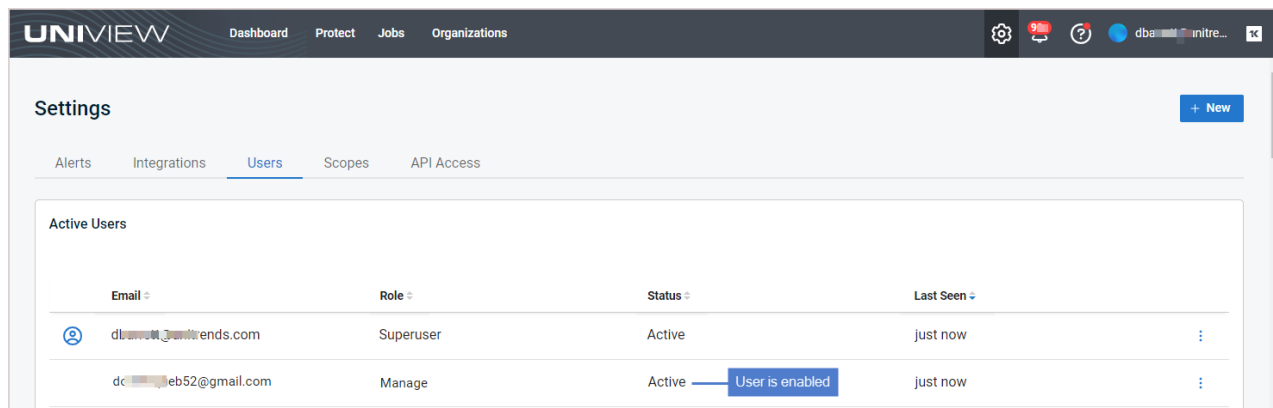
1 In the Users view, locate the user, click its **:** icon, and select **Enable**.



- 2 Click **Enable** to confirm.



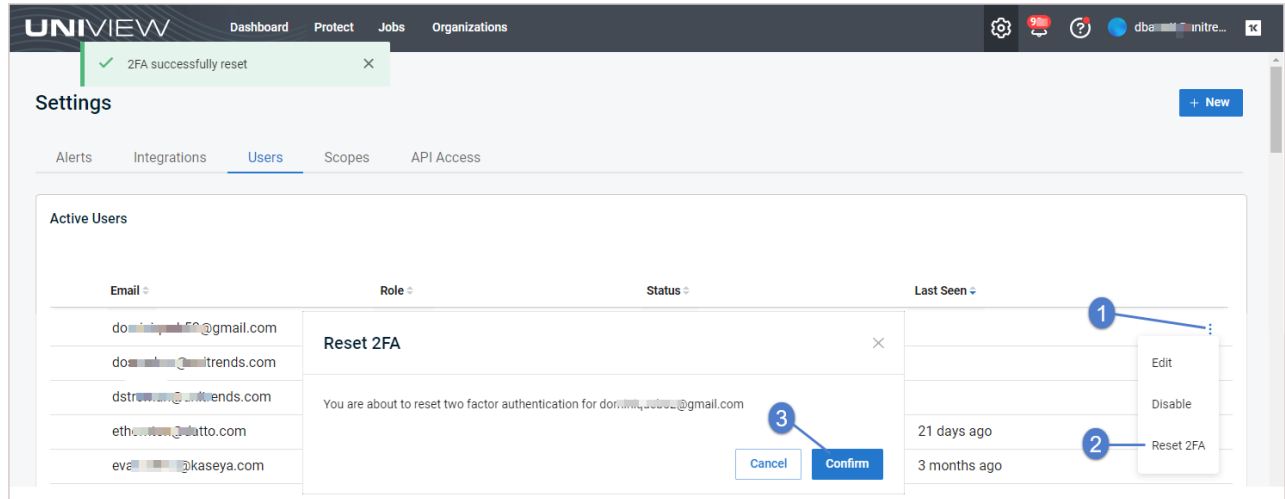
- 3 The user is enabled.



Resetting 2FA


Use this procedure to remove a user's two-factor authentication (2FA). Use this option if the user has lost their device. Once 2FA has been reset, the user will be prompted to configure 2FA on their new device. Any recovery codes from the previous configuration are no longer valid.

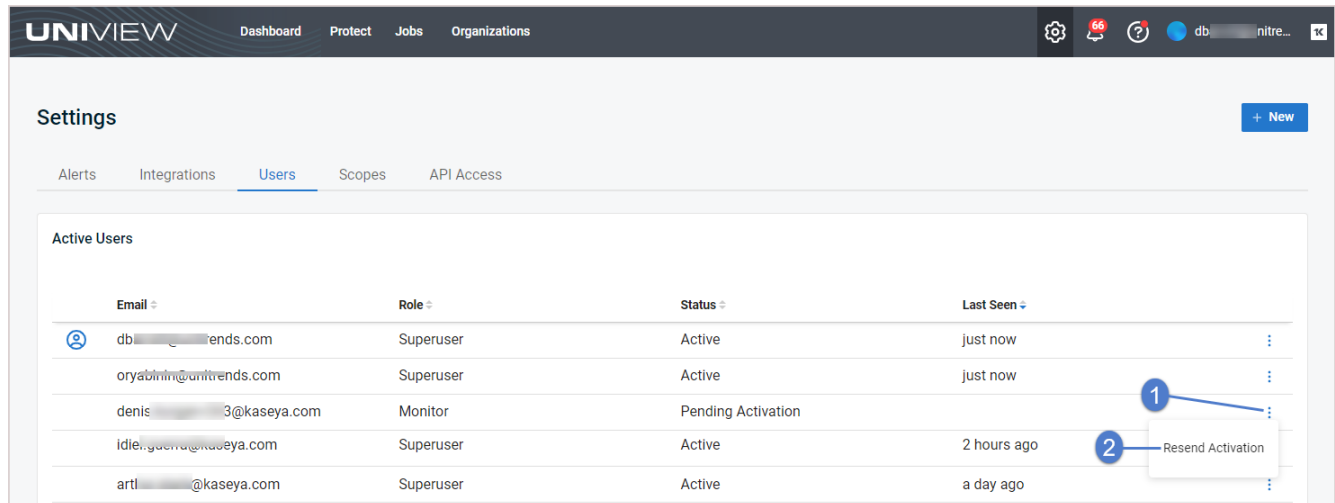
- 1 In the Users view, locate the user, click its **⋮** icon, and select **Reset 2FA**.
- 2 Click **Confirm**.



Resending an activation email

When the user was added, a *Welcome to UniView* email was sent to the user. The activation link in this email expires in 48 hours.

To send a new activation link to a pending user, click the user's  icon and select **Resend Activation**. The user must activate their UniView account within 48 hours of receiving this email.



Working with scopes

To control access to organization data in the UniView Portal:

- Each organization is assigned to one scope.
- Each portal user account is configured with one or more scopes. A user's scope determines which organizations are visible throughout the UniView Portal.

- The scopes option does not display for the Superuser role as all scopes are accessible to Superuser accounts. You must assign at least one scope to non-Superuser accounts.

Note: A user logs on with both an assigned role (the functions they can perform) and an assigned scope (the data they can see). Membership in a role and membership in a scope are independent of each other.


Use the Scopes view to manage scopes. See these procedures for details:

Note: To view and manage scopes, the feature must be enabled for your UniView Portal user account. If needed, contact your administrator to enable this feature.

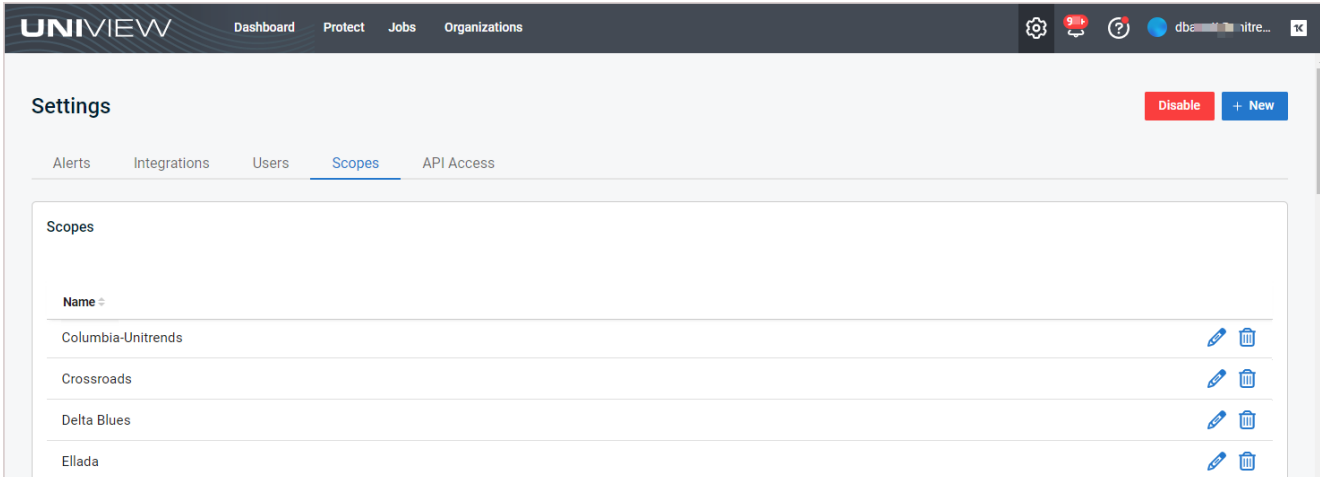
- "Viewing scopes"
- "Adding a scope"
- "Editing a scope"
- "Disabling or enabling the scopes feature"

Viewing scopes









The Scopes view displays all scopes that have been added to your backup.net instance. The following information is given for each scope:

- Name – Name of the scope.
- Pencil icon – Click to edit the scope name. (Displays for superusers only.)
-  icon – Click to delete the scope. (Displays for superusers only.)

Note: You must remove all users and organizations from the scope before it can be deleted. Use Edit Organization to assign a different scope to applicable organizations (see "Editing an organization"). Use Edit User to remove the scope from applicable users (see "Editing a user").



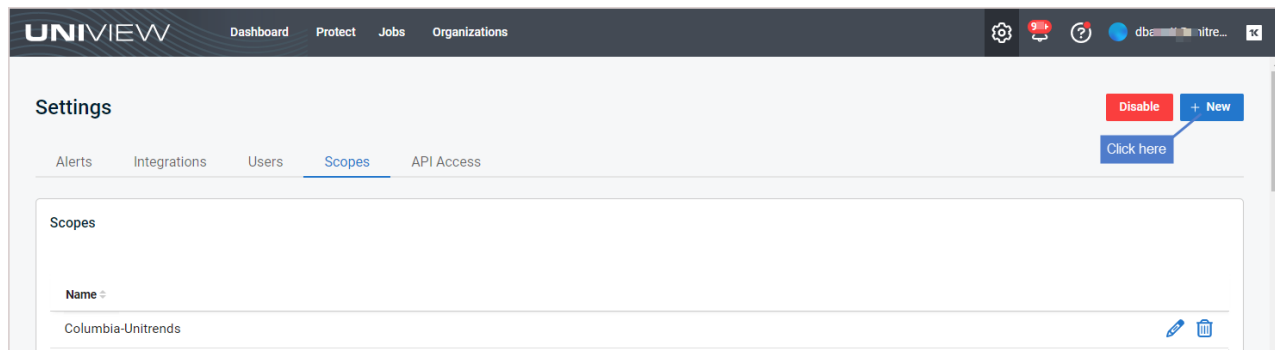
The screenshot shows the UniView Portal interface. At the top, there is a navigation bar with 'UNIVIEW' and menu items: 'Dashboard', 'Protect', 'Jobs', and 'Organizations'. On the right side of the navigation bar, there are icons for settings, a notification bell with '9', a help icon, and a user profile 'dba... nitre...'. Below the navigation bar, the 'Settings' page is displayed. The 'Settings' page has a 'Disable' button and a '+ New' button. The 'Scopes' tab is selected, showing a list of scopes. The list has the following entries:

Name	Actions
Columbia-Unitrends	 
Crossroads	 
Delta Blues	 
Ellada	 

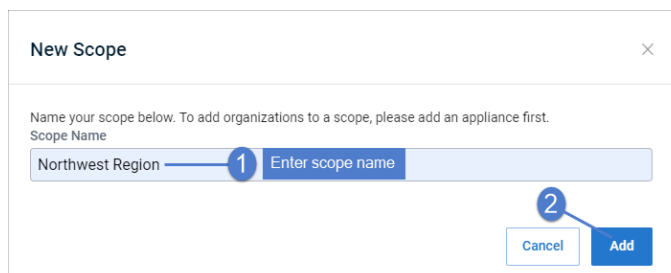
Adding a scope

To add a scope:

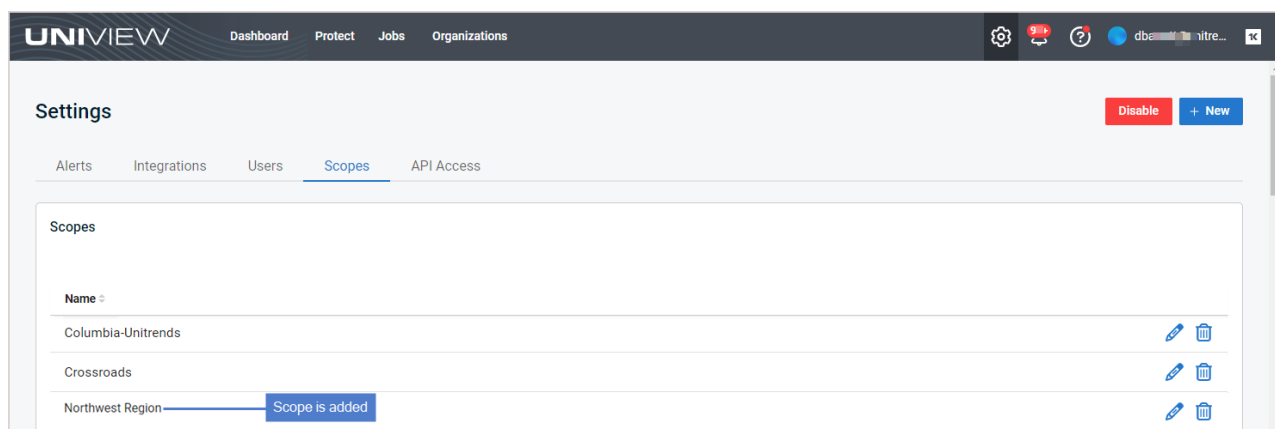
- 1 Log in to the UniView Portal with an account that has the superuser role.
- 2 In the Scopes view, click **+ New**.



- 3 Enter the scope name. Click **Add**.



- 4 The scope is added and displays in the list.

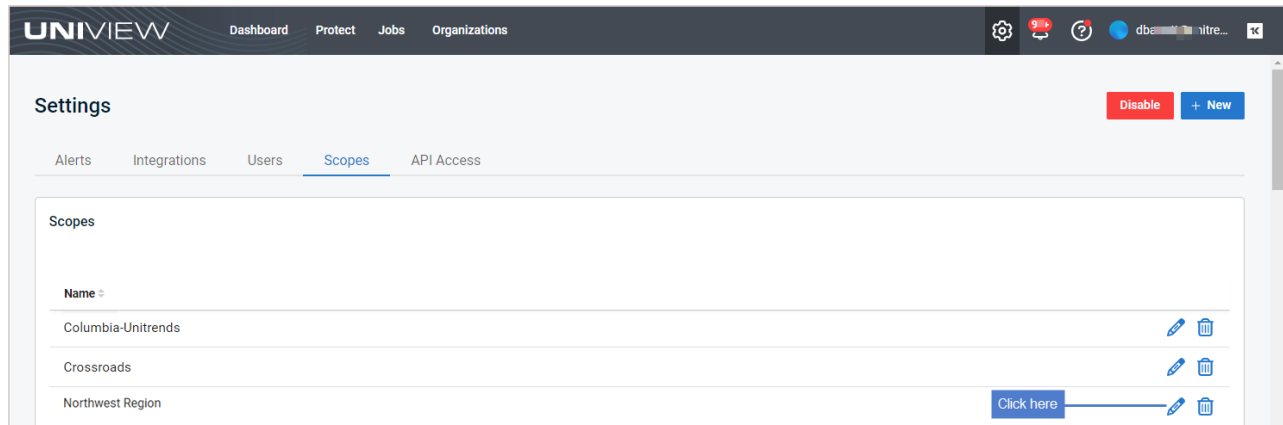


Editing a scope

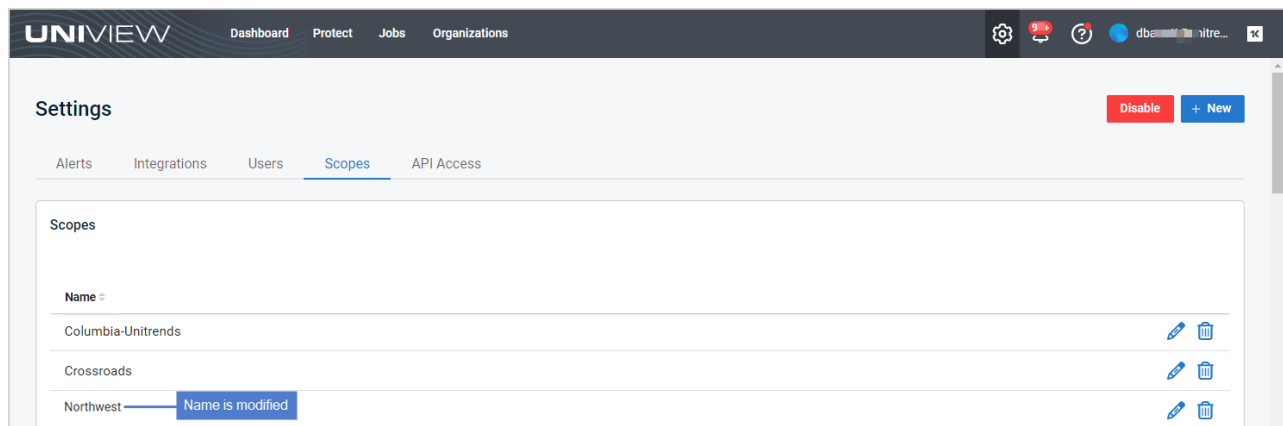
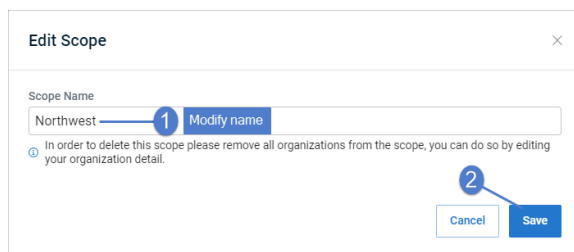
Use these steps to modify a scope name:

- 1 Log in to the UniView Portal with an account that has the superuser role.

- In the Scopes view, locate the scope and click its pencil icon.



- Modify the scope name, then click **Save**.

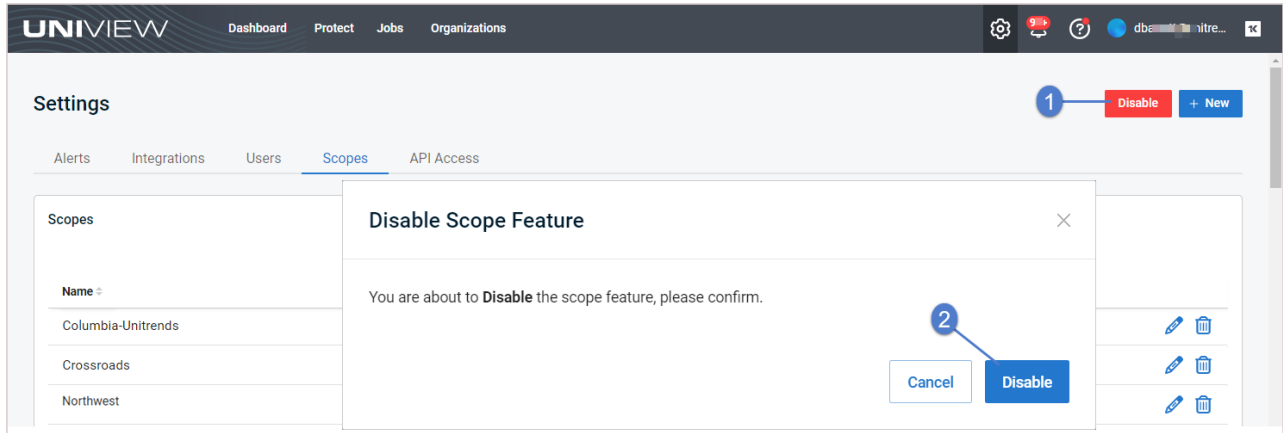


Disabling or enabling the scopes feature

Use this procedure to disable or enable the scopes feature for a UniView Portal user.

- Log in to the UniView Portal as the user whose scopes feature will be disabled or enabled by this procedure.
- In the Scopes view, click **Disable** or **Enable**, then click **Disable** or **Enable** to confirm.

Note: If scopes are enabled for the user, the Disable button displays. If scopes are disabled for the user, the Enable button displays.



This page is intentionally left blank.



Working with Integrations

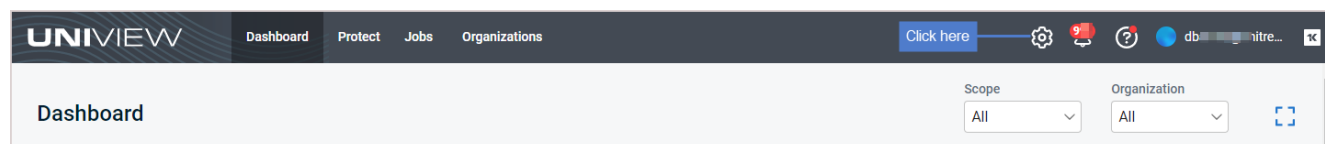
To customize your UniView Portal environment, you can integrate Kaseya modules. Once you've integrated a module, you can perform various tasks right from UniView, rather than logging in to a separate system.

Use the Settings > Integrations view (described below in "[Viewing integrations](#)") to manage your integrations. For details on adding and working with integrations, see these topics:

- "[Integrating VSA 9](#)"
- "[Integrating VSA 10](#)"
- "[Integrating KaseyaOne](#)"
- "[Working with your KaseyaOne integration](#)"
- "[Integrating Autotask](#)"
- "[Working with your Autotask Integration](#)"
- "[Integrating ConnectWise Manage](#)"
- "[Working with your ConnectWise Manage integration](#)"
- "[Integrating Kaseya's Billing Management System \(BMS\) or Vorex](#)"
- "[Working with your BMS or Vorex integration](#)"
- "[Importing Accounts or Companies from your PSA](#)"
- "[Integrating Datto Portal](#)"
- "[Working with your Datto Portal integration](#)"
- "[Integrating IT Glue](#)"
- "[Working with your IT Glue integration](#)"

Viewing integrations

Integrations are managed from the Settings page. To access the Settings page, click  :



The Integrations view displays Kaseya modules that are available for integration with your UniView Portal. The following information is given for each integration:

- Module icon and name.
- A description of the module.
- An action button indicating the next step needed to start using the integration.

The screenshot shows the UniView Portal Settings page with the Integrations tab selected. The page lists several integrations:

- KaseyaOne**: Configure the integration with Kaseya One portal to enable the option to login using KaseyaOne credentials. Action buttons: Integrate.
- VSA**: Kaseya VSA Integration is complete. You can now view your Kaseya agents under Appliances > VSA. Click on Show Configuration to setup conditional alerts synchronization. The portal is integrated with <https://u...TG-vsa...kaseya.net>. Action buttons: Download Manifest, Enabled.
- BMS**: Create tickets in Kaseya BMS based on alerts and warnings issued by BackupIQ. Action buttons: Integrate.
- IT Glue**: Synchronize data with Kaseya IT Glue documentation tool. Action buttons: Integrate.
- Autotask**: Create tickets in Autotask PSA based on alerts and warnings issued by BackupIQ. Action buttons: Integrate.

Integrating VSA 9

Use these procedures to integrate your VSA 9 SaaS or on-premise instance with the UniView Portal.

Notes:

- SaaS instance managed by Kaseya – If you are using a SaaS VSA instance that is managed by Kaseya, do not run these VSA integration procedures. Instead, work with Support or your Evaluation Engineer to perform the VSA integration.
- These integration procedures apply to VSA 9 only. Do not use these procedures for VSA 10.
- Conditional alarms for an on-premise instance that is not accessible on the Internet – UniView Portal requires Internet access to push alarms to the VSA. If your VSA is not connected to the Internet, you cannot add UniView Portal conditional alarms to the VSA instance.

- " Step 1: (If needed) Remove the existing VSA 9 integration"
- " Step 2: Install the latest TAP module"
- " Step 3: Complete the integration"

Step 1: (If needed) Remove the existing VSA 9 integration

If you have already integrated VSA 9, use these steps to remove the UniView TAP module from your VSA instance.

Notes:

- You must remove the existing TAP module before installing the latest UniView TAP module.
- If the logos and branding you see in your currently deployed VSA module do not look like this new UniView module, you may be using a prior version of the TAP module for the Unitrends Backup Portal platform. As of January 2023, module branding has been modified, but no other functional changes exist. We do not recommend customers uninstall the older module to use the newer module as this will impact existing mappings (e.g., UniView user accounts mapped to KaseyaOne accounts for single sign-on, and assets mapped to VSA IDs).

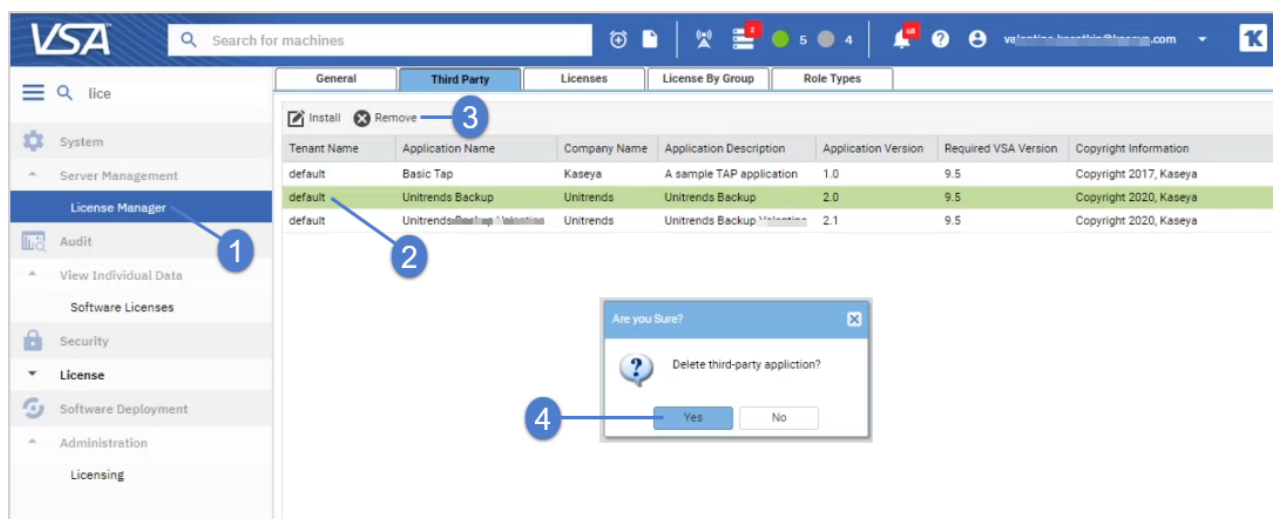
1 Log in to the VSA UI.

Note: Do not use a VSA URL that includes `-cdn`. Use the URL that goes directly to your VSA server instance.

2 Select **System > Server Management > License Manager > Third Party**.

3 Select the row containing *UniView*, *Unitrends Backup* (older versions), or *Unitrends MSP* (older versions).

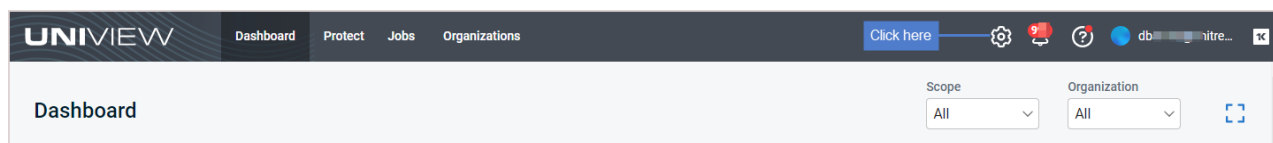
4 Click **Remove**, then **Yes** to confirm.



Step 2: Install the latest TAP module

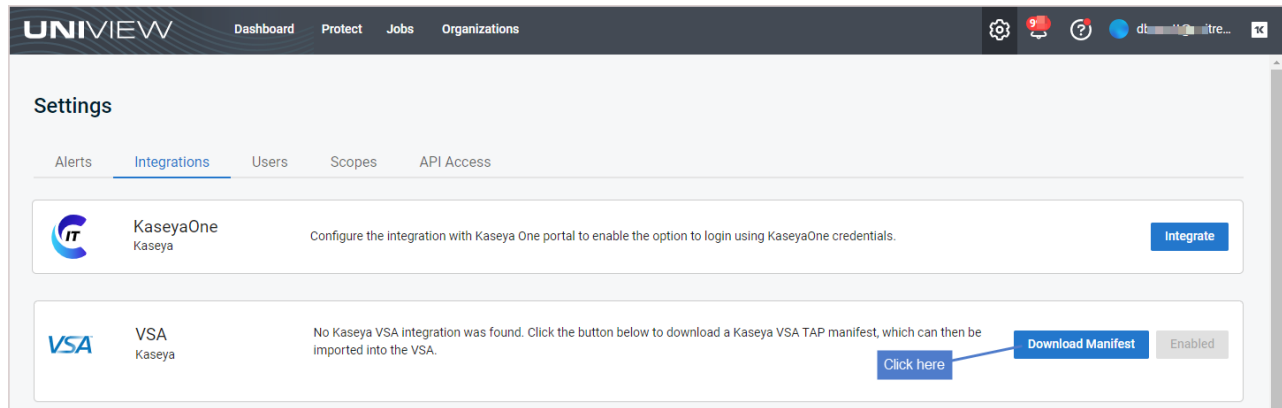
1 Log in to the UniView Portal as a superuser.

2 Click :



3 Select the **Integrations** view.

4 Locate the VSA integration and click **Download Manifest**. The UniView TAP module, *UniView.vsaz*, is downloaded.



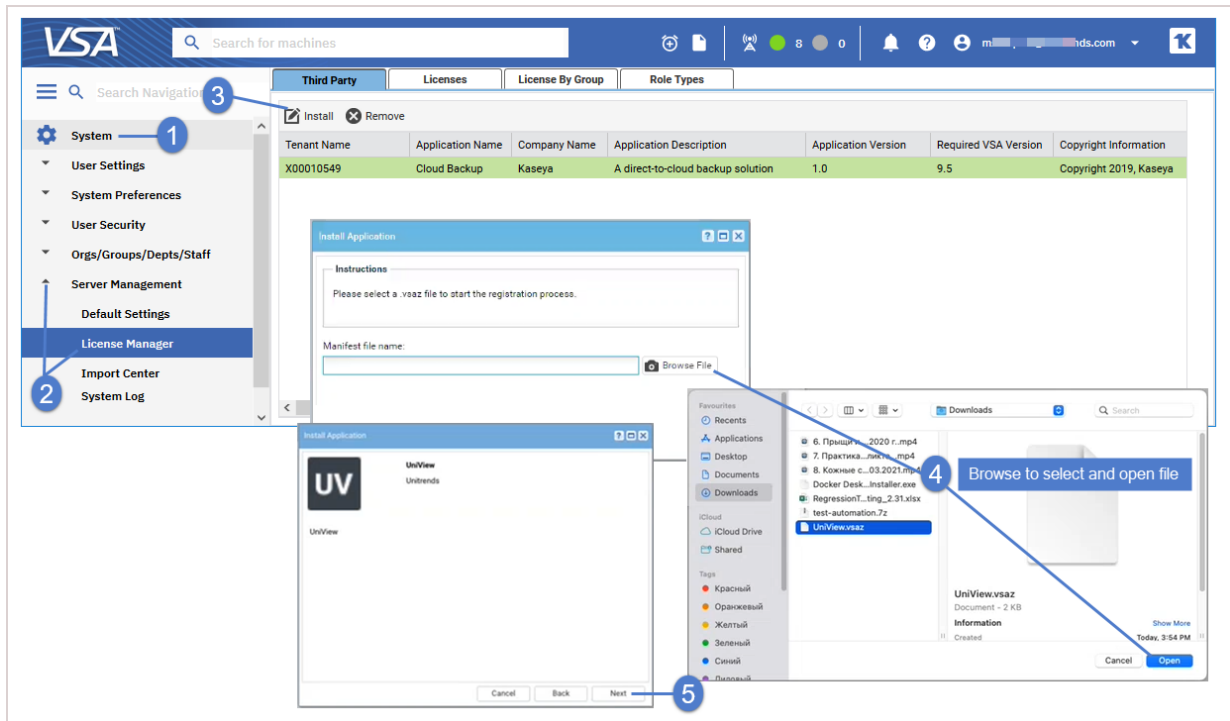
5 Use these steps to add the UniView TAP module to the VSA:

- Log in to the VSA UI.

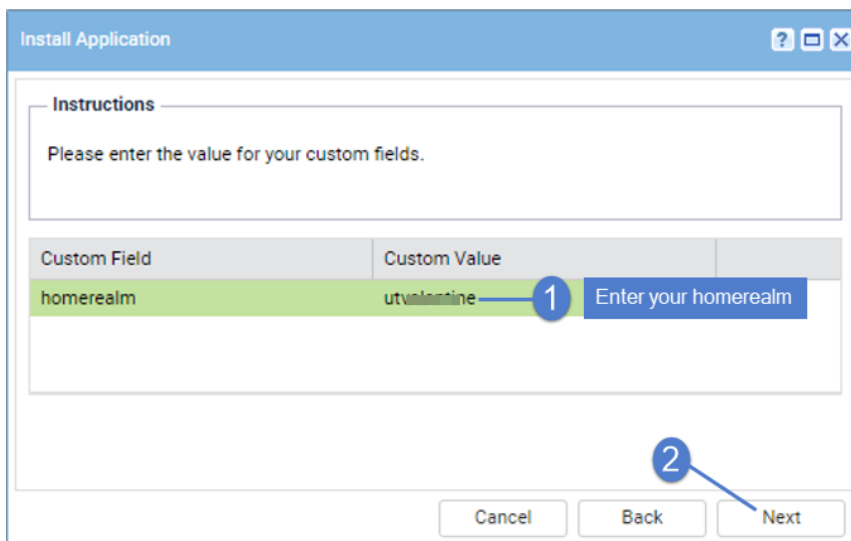
Note: Do not use a VSA URL that includes *-cdn*. Use the URL that goes directly to your VSA server instance.

- On-premise instance only – Select **System > Server Management > Configure** and make sure you have checked this box: **Enable Third Party App Installation Globally**. (Skip this step if you have a SaaS VSA instance.)

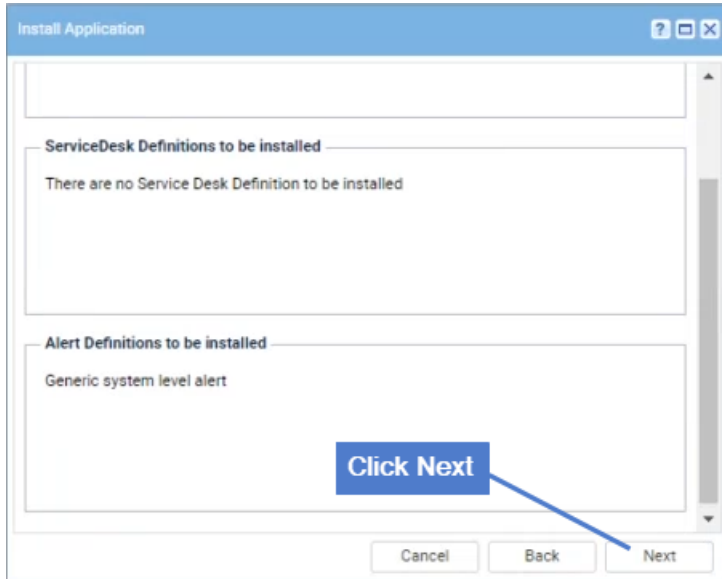
- Select **System > Server Management > License Manager > Third Party > Install**.
- Click **Install**. Browse to the path where you downloaded the TAP module. Select **UniView.vsaz**. Click **Open**. Click **Next**.



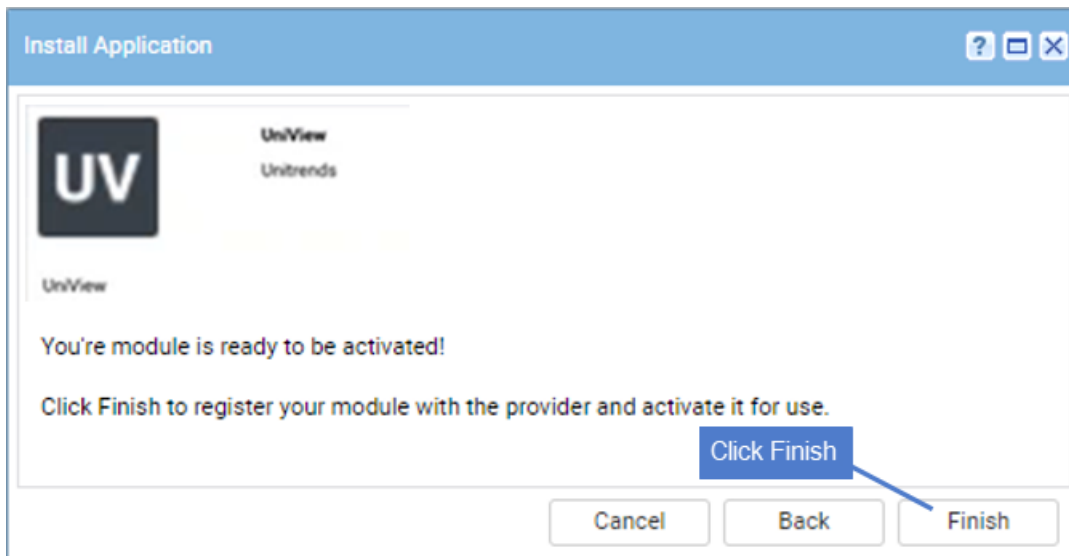
- Enter your homerealm in the *homerealm* Custom Value field. Click **Next**.



- Click **Next**.



- Click **Finish**. The module is installed and activated.



Step 3: Complete the integration

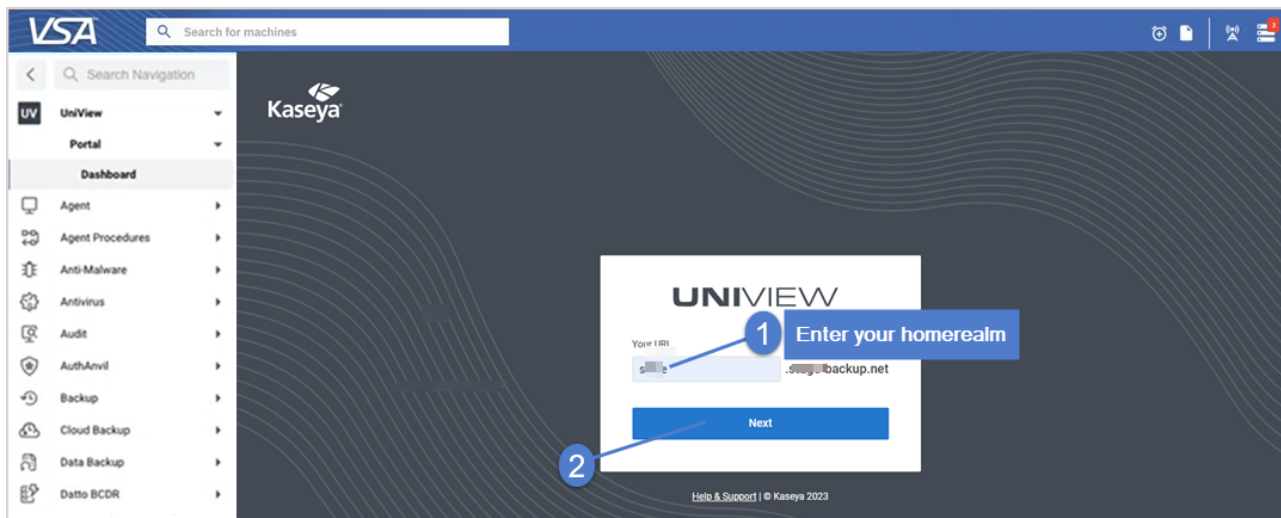
Run this procedure to link your VSA and UniView Portal credentials, enabling single sign-on (SSO) access to the UniView module from your VSA session.

Notes:

- You must run this procedure from the VSA. Authorizing UniView Portal access to the VSA by logging in directly to backup.net is not supported.

- If you must access the VSA from the local network by IP address or DNS alias, SSO is not supported. Do not run this "Step 3: Complete the integration" procedure. Instead, you must enter your UniView Portal credentials to access the UniView module from your VSA session.
- This procedure uses third-party cookies for authentication and to help you sign up for our services. If prompted, click to allow third-party cookies in your browser.
- A 1-to-1 VSA to UniView Portal account ratio is now enforced. (A VSA user account can be linked to only one UniView Portal user account. A UniView Portal user can be linked to only one VSA user account.) If needed, administrators can create additional accounts to meet this requirement.

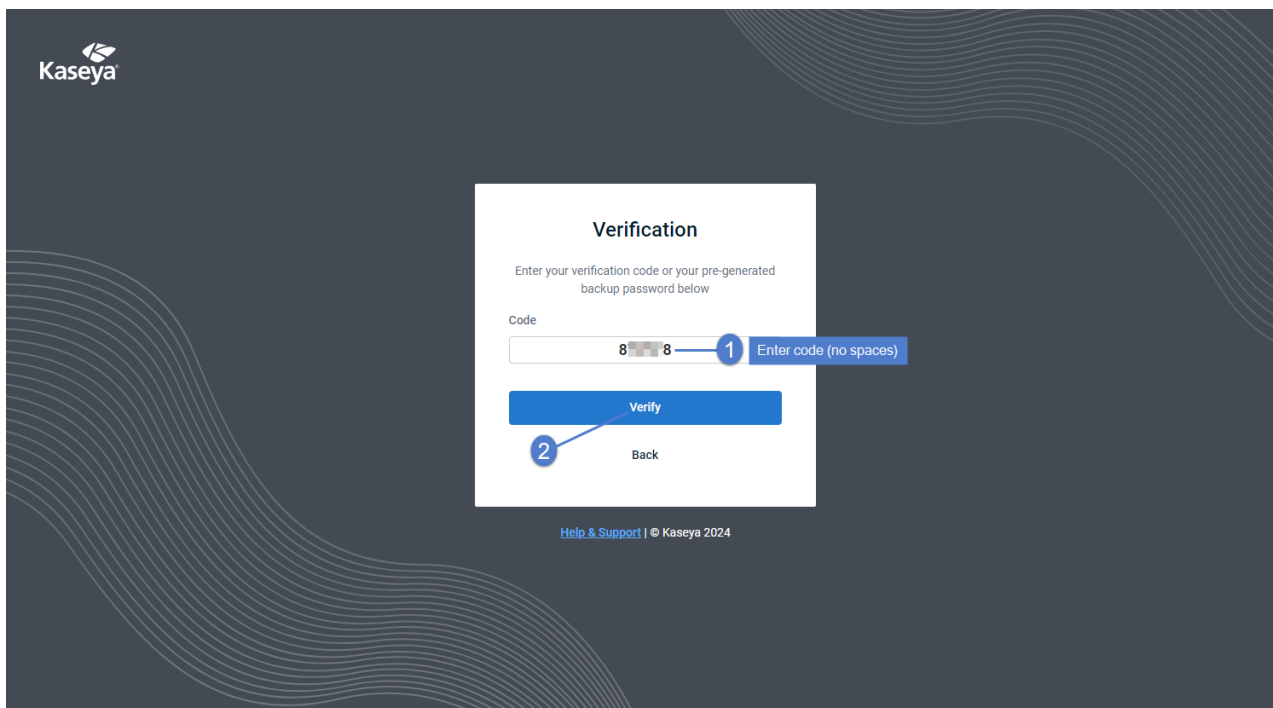
- 1 In the VSA, select the **UniView** module.
- 2 Enter the backup.net homerealm. Click **Next**.



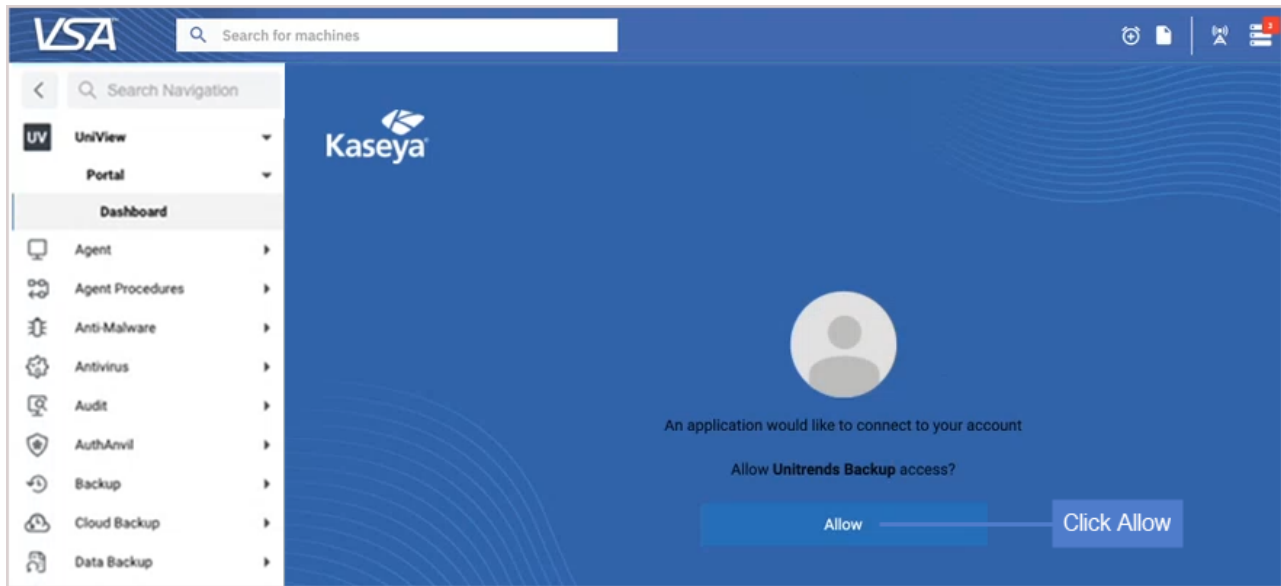
- 3 Log in to UniView Portal as a superuser.
 - Enter your UniView Portal username and password.
 - Click **Log in**.



- 4 Enter your two-factor authentication (2FA) code, then click **Verify**. (You can obtain the code from your authenticator app or use a recovery code.)



- 5 Click **Allow** to grant UniView Portal access to the VSA instance.

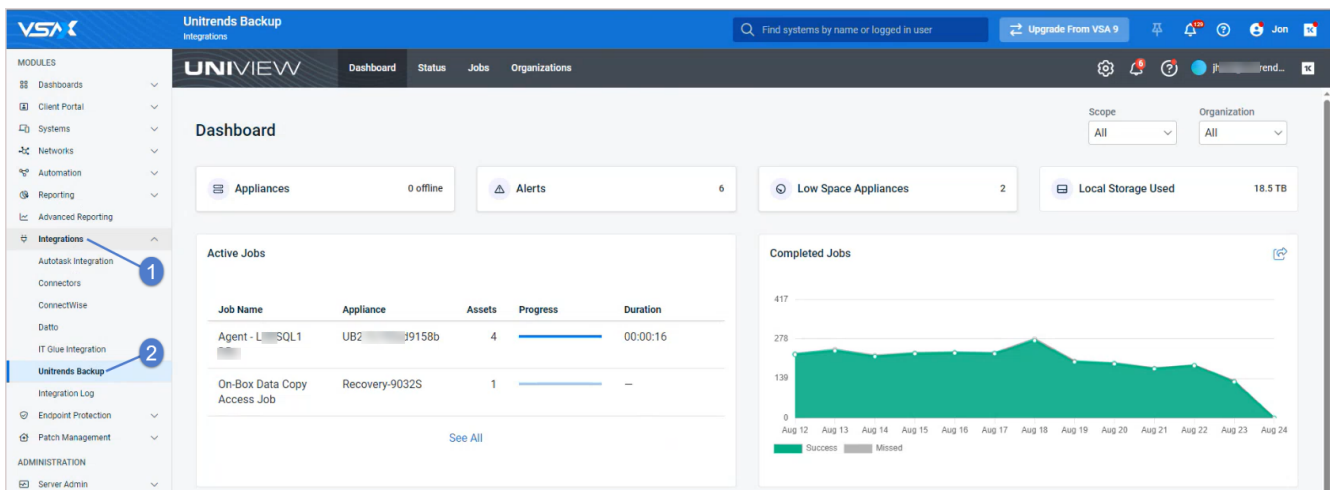


The UniView Portal Dashboard displays.

Integrating VSA 10

The UniView Portal provides UI and API integration across these backup and recovery solutions: Unitrends backup appliances, Spanning SaaS backup for Microsoft 365, Google Workspace and Salesforce, and backup for public cloud workloads. Add the UniView Portal module to VSA 10 so that you can manage your backup and recovery environments from a single interface.

Contact your Account Manager or Customer Support to add the UniView Portal module to your VSA 10 instance. Once the module is added, you can quickly access the UniView Portal right from your VSA by selecting **Integrations > Unitrends Backup**:




Integrating KaseyaOne

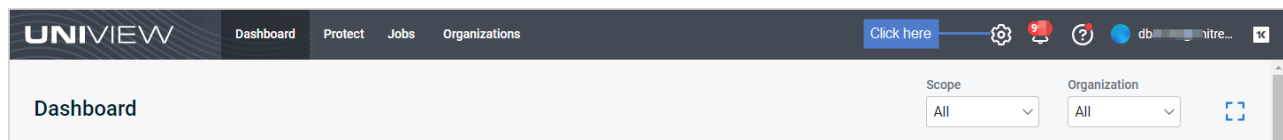
KaseyaOne is its own identity provider (IdP) and you can use your KaseyaOne account to log in to all of your other Kaseya modules. Use this procedure to integrate KaseyaOne. Integration enables users to log in to UniView Portal by using KaseyaOne credentials and provides the option to automatically create UniView Portal users for each KaseyaOne user. For details, see "[Working with your KaseyaOne integration](#)".

Note: KaseyaOne also supports third-party IdP integrations, such as Okta, Microsoft EntraID, and Passly. If you have integrated your third-party IdP with KaseyaOne, simply add the KaseyaOne integration and enable Require Login with KaseyaOne to manage your UniView users with this IdP provider. (To add an IdP integration to KaseyaOne, see this article: [Set up third-party IdP integrations](#).)

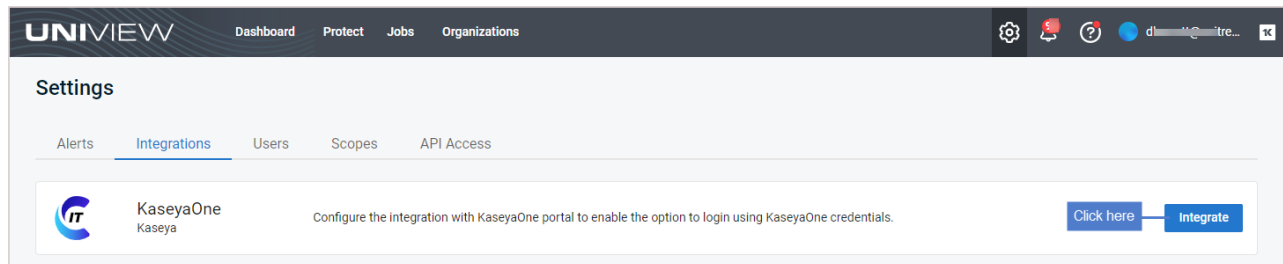
To integrate the KaseyaOne portal

Note: To perform this procedure, you must log in to UniView Portal as a superuser and log in to KaseyaOne as a master role user.

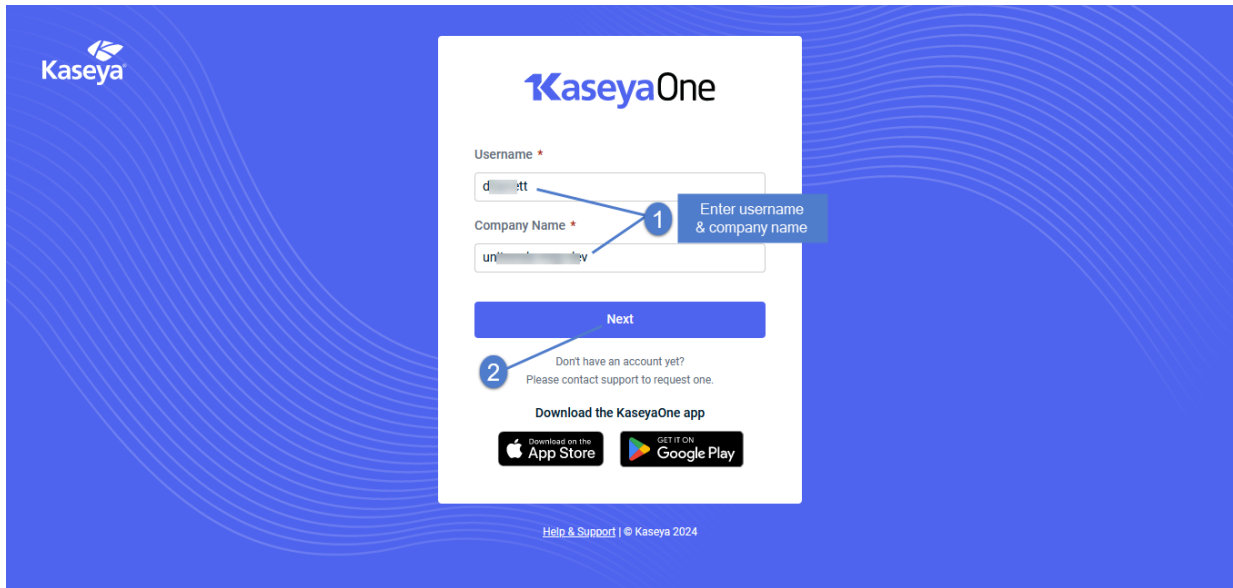
- 1 Log in to the UniView Portal as a superuser.
- 2 Click :



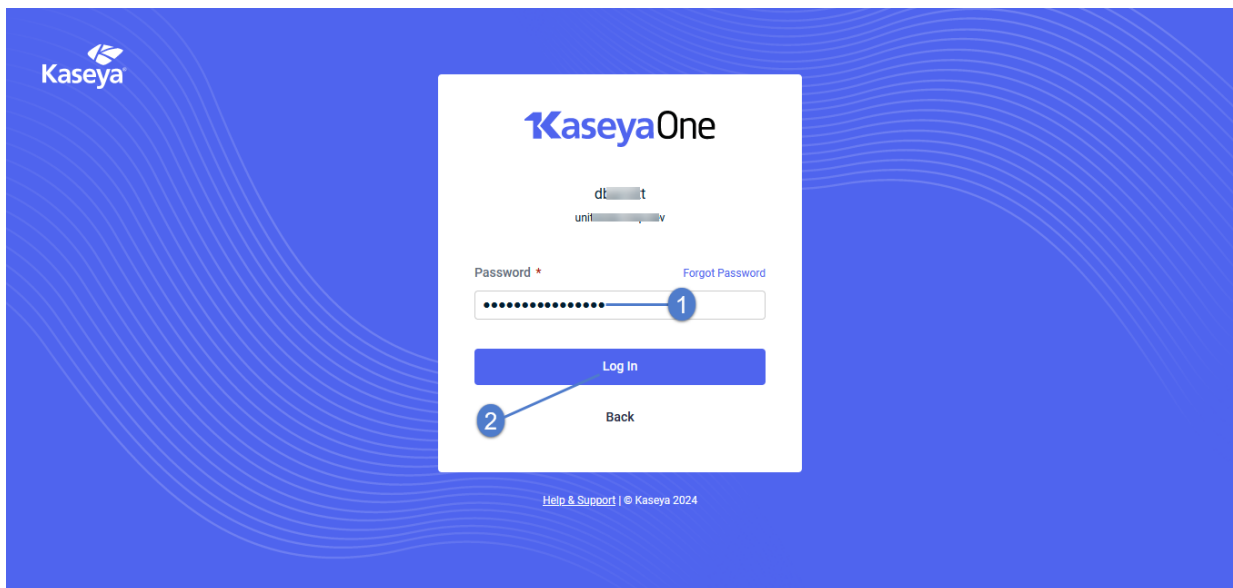
- 3 Select the **Integrations** view.
- 4 Locate the KaseyaOne integration and click **Integrate**.



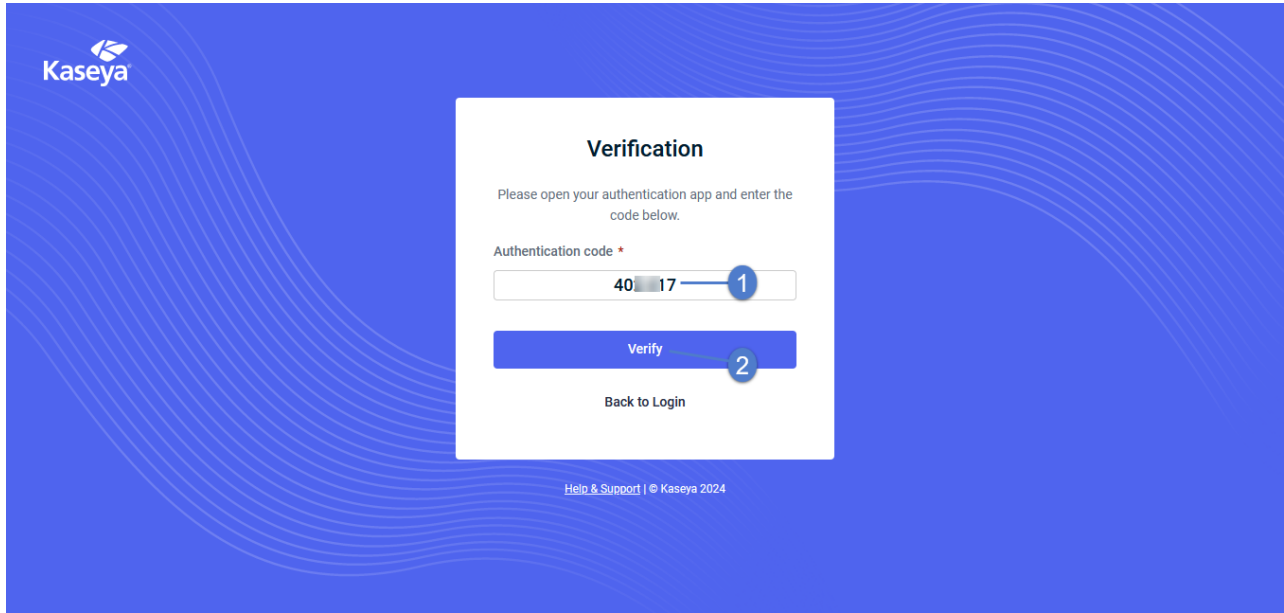
- 5 Log in to the KaseyaOne portal as a master role user. (If your KaseyaOne account does not have the master role, you receive an *Access denied* message.)
 - Enter your username and company name. Click **Next**.



- Enter your password. Click **Log In**.

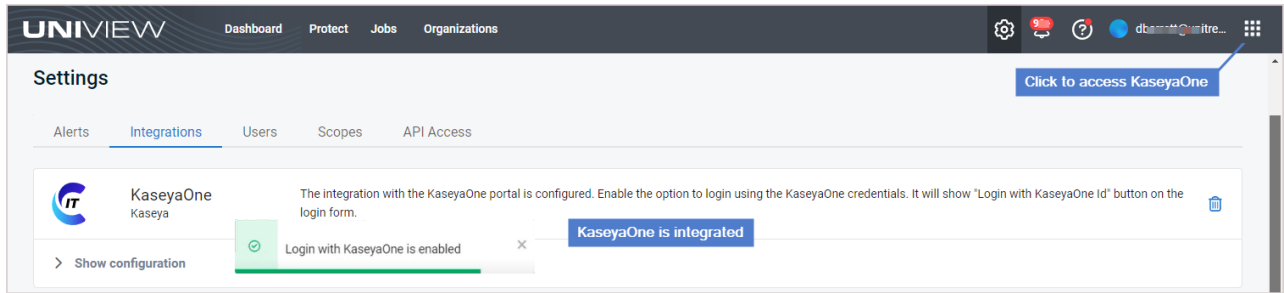


- 6 Enter your two-factor authentication (2FA) code, then click **Verify**. (You can obtain the code from your authenticator app.)

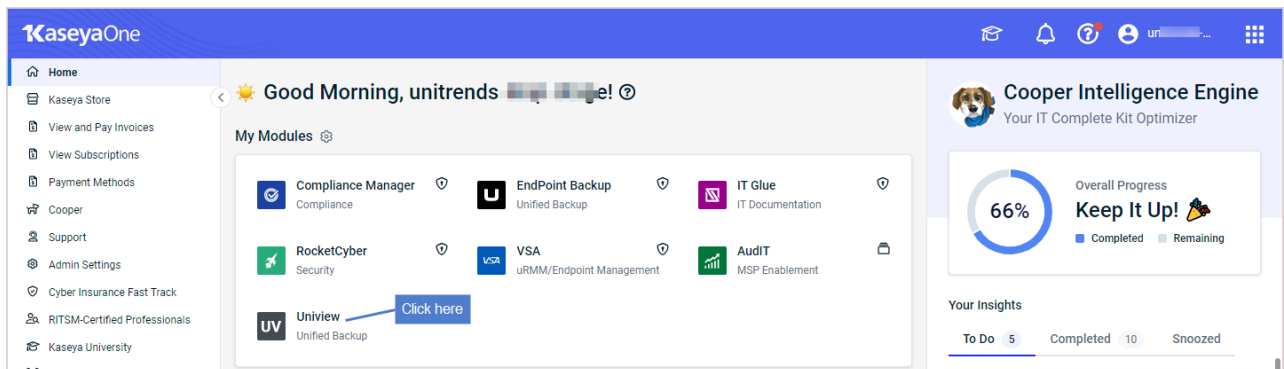


7 The integration is configured and login with KaseyaOne is enabled.

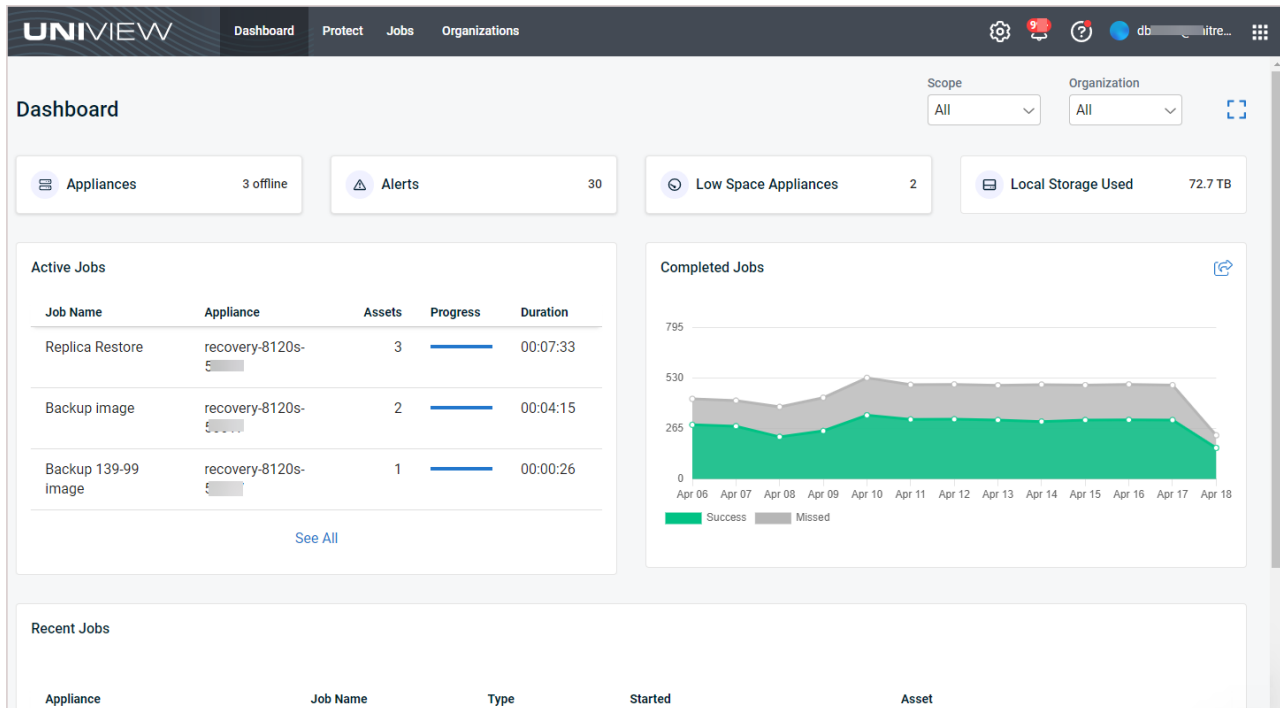
8 To access KaseyaOne, click .



9 You can see that the UniView module has been added to KaseyaOne. To connect to UniView from KaseyaOne, click the **UniView** module:



The Dashboard displays:



Working with your KaseyaOne integration


Once you've integrated KaseyaOne, use these procedures as needed:

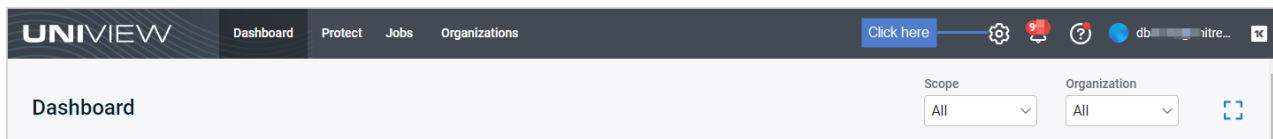
- ["To disable or re-enable Login with KaseyaOne"](#)
- ["To enable or disable Require Login with KaseyaOne"](#)
- ["To enable or disable automatic user creation"](#)
- ["To reset the KaseyaOne integration"](#)
- ["Working with Cooper Insights in KaseyaOne"](#)

To disable or re-enable Login with KaseyaOne

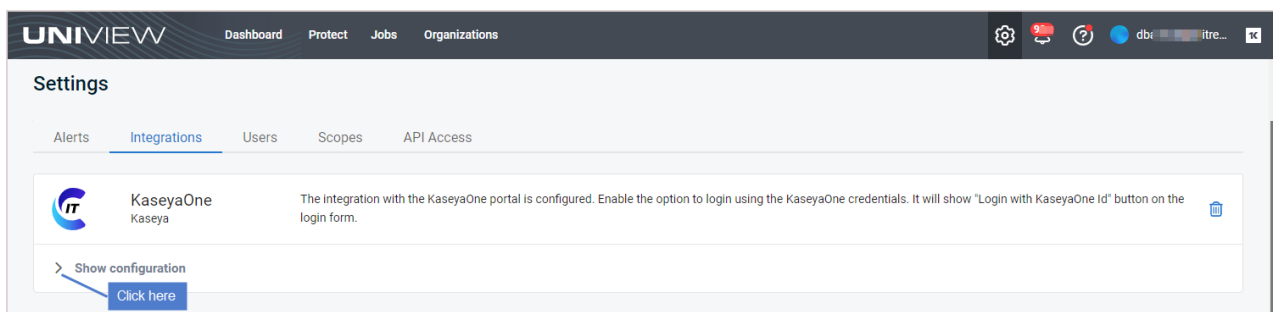
Disabling the Enable Login with KaseyaOne toggle prevents all UniView Portal users from logging in by using KaseyaOne credentials but does NOT remove any user mappings.

Run this procedure to temporarily disallow KaseyaOne login for all users. You can then re-enable the Login with KaseyaOne toggle so that users can resume using their KaseyaOne credentials for the UniView Portal.

- 1 Log in to the UniView Portal as a superuser.
- 2 Click :

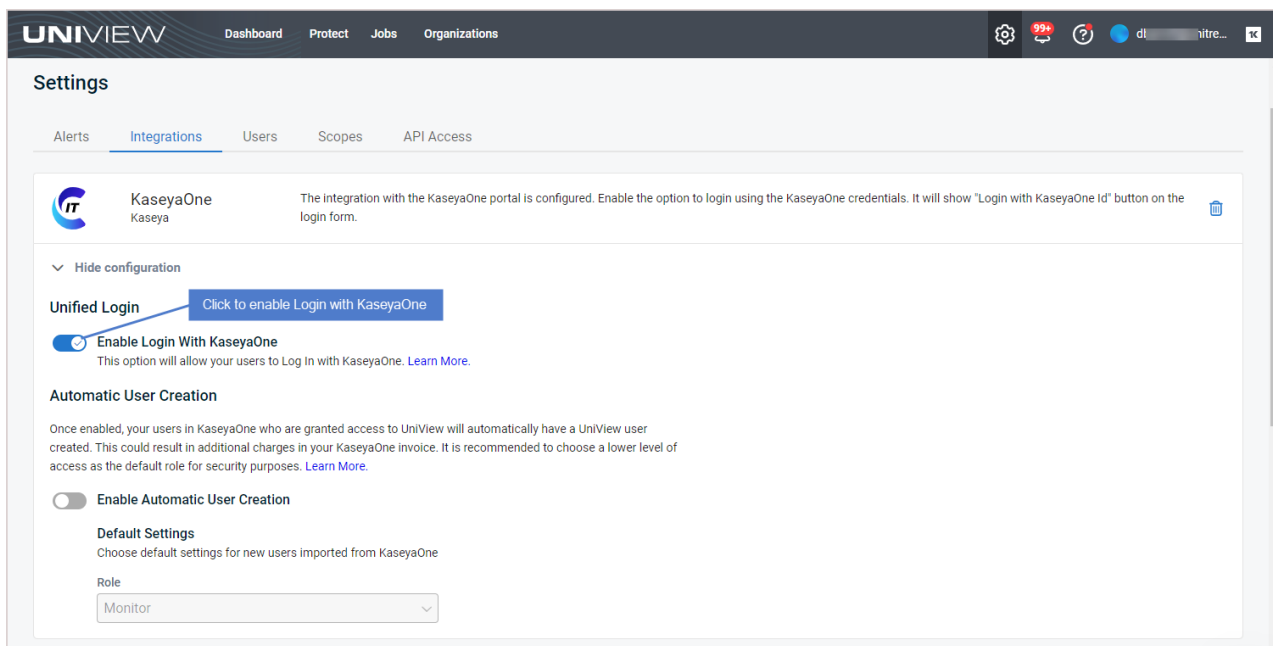


- 3 Select the **Integrations** view.
- 4 Locate the KaseyaOne integration and click **Show configuration**:




- 5 Under Unified Login, click to disable or to enable log in with KaseyaOne.

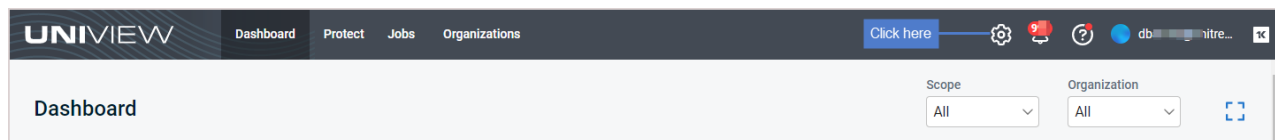
Note: This toggle must be enabled to use the Require Log In With KaseyaOne feature. Disabling this toggle also disables the Require Log In With KaseyaOne feature.



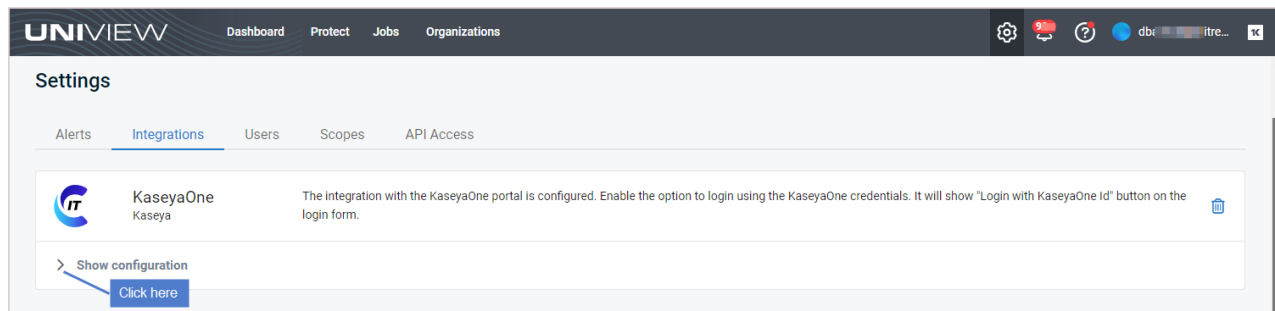
To enable or disable Require Login with KaseyaOne

If enabled, the Require Login with KaseyaOne toggle forces users to log in to the UniView Portal with their KaseyaOne Unified Login credentials. When enabling this feature, you are able to grant exceptions to specified users so that these users are still able to log in using their UniView Portal credentials.

- 1 Log in to the UniView Portal as a superuser.
- 2 Click :



- 3 Select the **Integrations** view.
- 4 Locate the KaseyaOne integration and click **Show configuration**:



- 5 Under Require Log In With KaseyaOne, click to disable or to enable Require Log In with KaseyaOne.
- 6 (If needed) If you are enabling the Require Log In With KaseyaOne feature, ensure that the Enable Login with KaseyaOne toggle is also enabled so that users can log in via KaseyaOne.

Note: If you've enabled Require Log In With KaseyaOne, it is best to also enable automatic user creation.

UNIVIEW Dashboard Protect Jobs Organizations

Hide configuration

Unified Login (If needed) Enable this toggle

Enable Login With KaseyaOne
This option will allow your users to Log In with KaseyaOne. [Learn More.](#)

Automatic User Creation

Once enabled, your users in KaseyaOne who are granted access to UniView will automatically have a UniView user created. This could result in additional charges in your KaseyaOne invoice. It is recommended to choose a lower level of access as the default role for security purposes. [Learn More.](#)

Enable Automatic User Creation (Recommended) Enable if using Require Log In With KaseyaOne

Default Settings
Choose default settings for new users imported from KaseyaOne

Role
Monitor

Require Log In With KaseyaOne

This option will prevent users from logging in directly and only allow them to authenticate via KaseyaOne. [Learn More.](#)

Require Log In With KaseyaOne

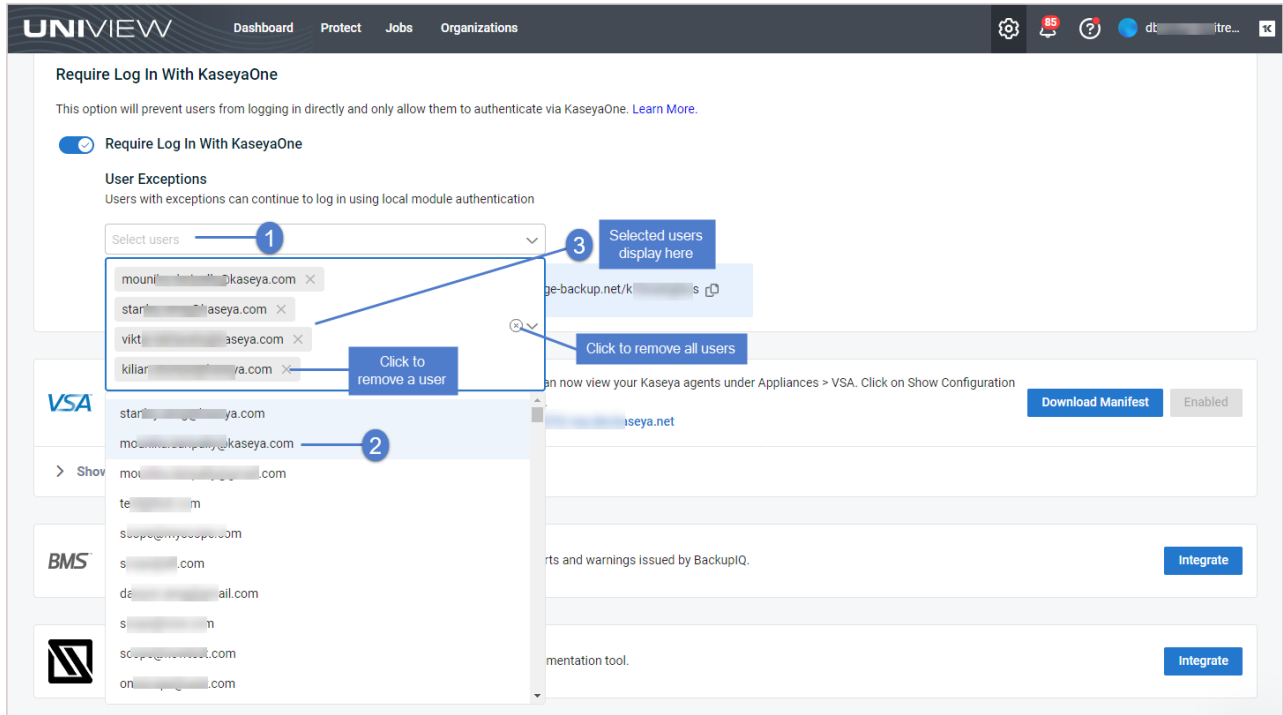
User Exceptions
Users with exceptions can continue to log in using local module authentication

Select users

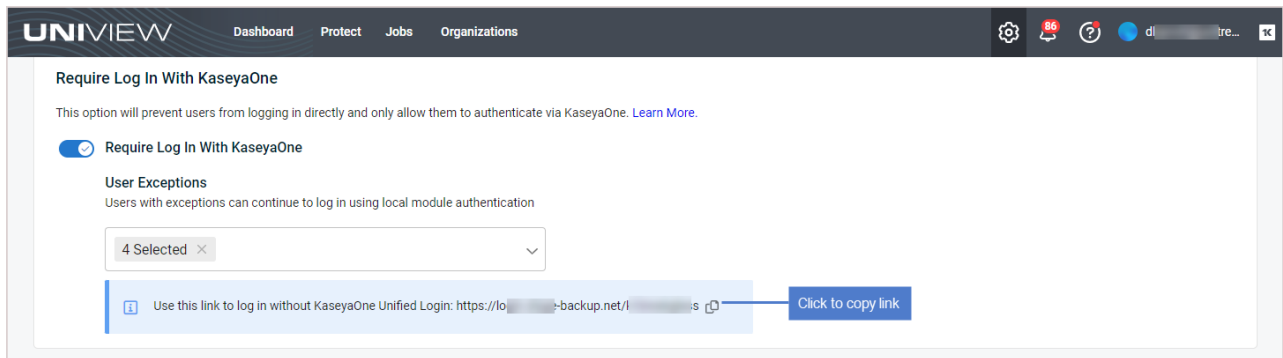
Use this link to log in without KaseyaOne Unified Login: [https://log\[redacted\]-backup.net/k\[redacted\]](https://log[redacted]-backup.net/k[redacted])

7 (Optional) Allow specified users to log in with UniView Portal credentials by granting exceptions to these users:

- Click **Select users**.
- Click users to add them to the exceptions list.



- 8 (Optional) To enable a user to log in with UniView Portal credentials without granting an explicit exception, send the user the log-in link shown here:




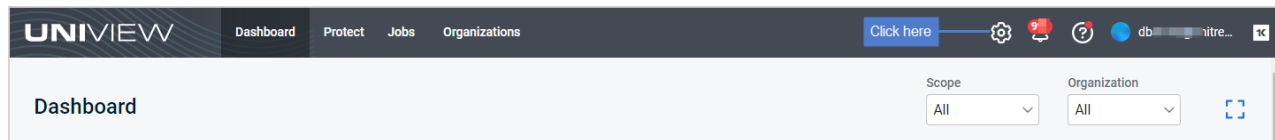
To enable or disable automatic user creation

The KaseyaOne integration has an Automatic User Creation setting that you can enable to automatically create a UniView Portal user for each KaseyaOne user. Once enabled, your users in KaseyaOne who are granted access to the UniView Portal module will automatically have a UniView Portal user created. UniView Portal users are created with the default role you select for the Automatic User Creation setting (described in the procedure below). It is recommended to choose a lower level of access as the default role for security purposes.

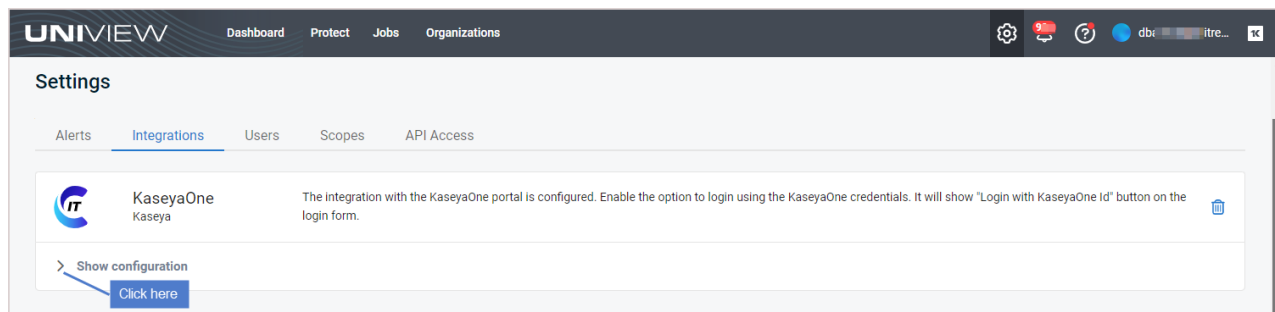
Note: Creating additional users could result in additional charges in your KaseyaOne invoice.



Run this procedure to enable or disable automatic user creation:

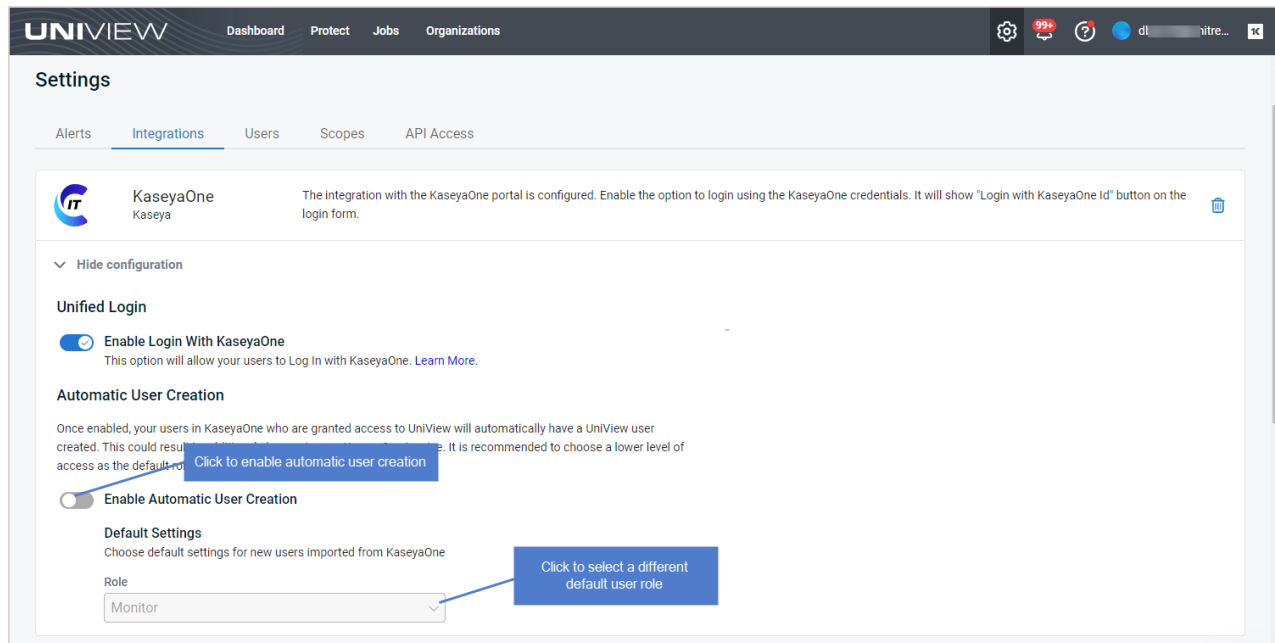
- 1 Log in to the UniView Portal as a superuser.
- 2 Click :



- 3 Select the **Integrations** view.
- 4 Locate the KaseyaOne integration and click **Show configuration**:




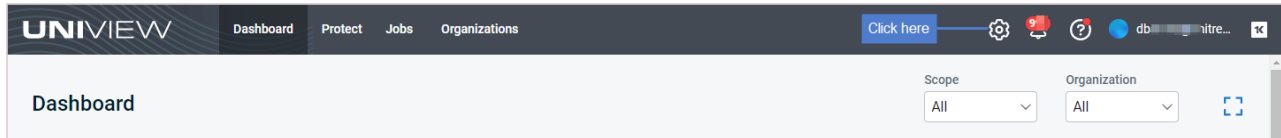
- 5 Under Automatic User Creation, click  to disable or  to enable automatic user creation.
- 6 (Optional) Under Default Settings, modify the default role assigned to the newly created users: Monitor, Manage, Admin, or Superuser (see "[About UniView Portal user accounts](#)" for details).




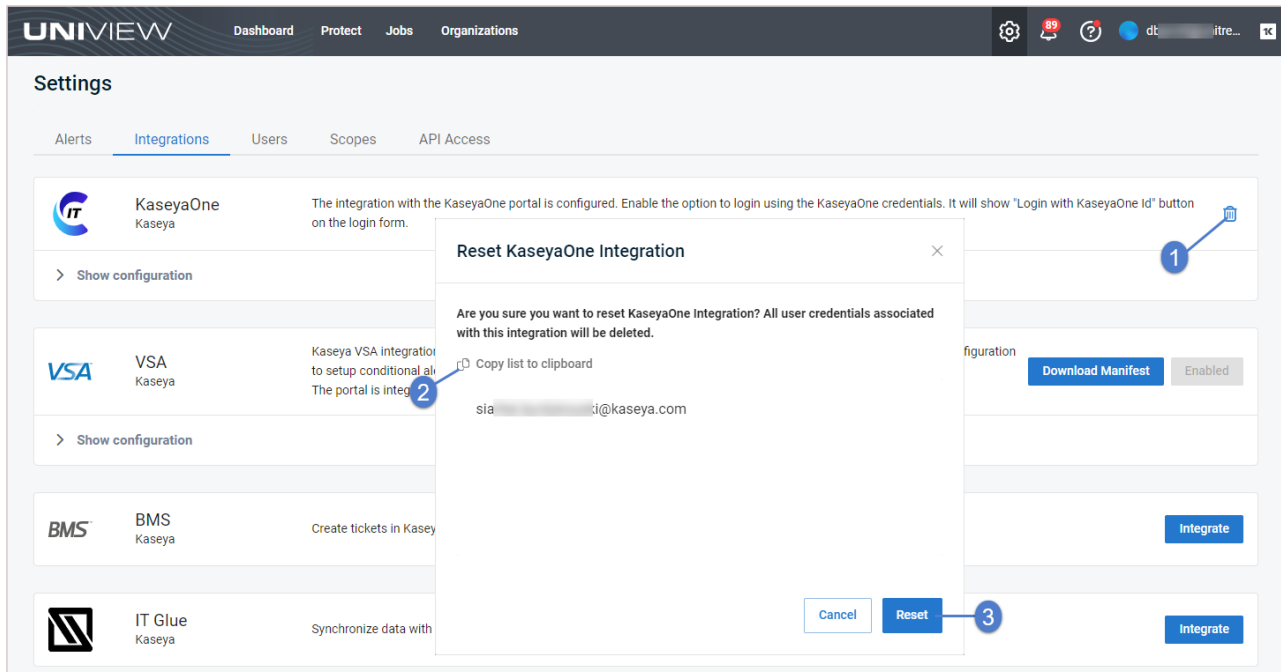
To reset the KaseyaOne integration

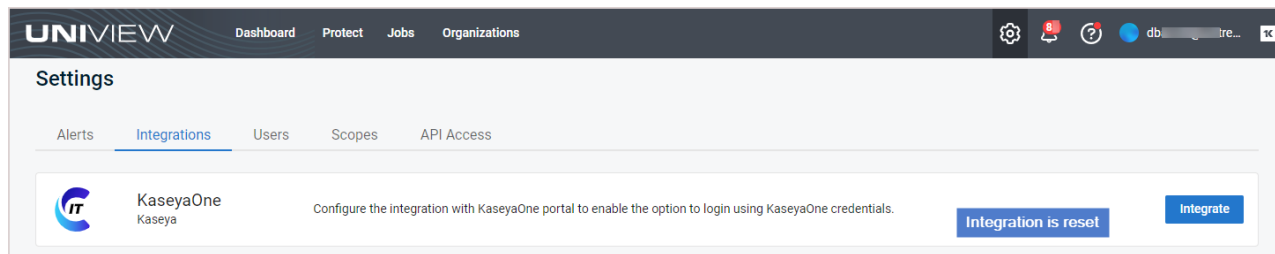
Use this procedure to reset the KaseyaOne integration. This procedure removes the integration and all associated user mappings from UniView, and removes the UniView module from KaseyaOne. (To temporarily disable login via KaseyaOne without removing the user mappings, see "To disable or re-enable Login with KaseyaOne".)

- 1 Log in to the UniView Portal as a superuser.
- 2 Click :



- 3 Select the **Integrations** view.
- 4 Locate the KaseyaOne integration and click .
- 5 (Optional) In the Reset KaseyaOne Integration dialog, click **Copy list to clipboard** to copy and save a list of the integration's users. (You may need to refer to this list as the reset removes these users.)
- 6 Click **Reset** to confirm that this will remove the integration and all of its user mappings.





Working with Cooper Insights in KaseyaOne

The Cooper Intelligence Engine provides insights based on telemetry gathered from your module usage. These insights are designed to help you get the most out of your Kaseya modules. Insights let you know about features that drive the most value for your business and guide you toward following industry leading best practices.

Once you have integrated KaseyaOne, Unitrends insights are enabled and added to Cooper if trigger conditions are met. See these topics for details:

- ["Insight details"](#) for a description of each Unitrends insight
- ["To view and manage insights"](#) for steps used to review and resolve insights

For more on KaseyaOne and Cooper Insights, see [KaseyaOne](#) and [FAQs - Cooper Intelligence Engine](#).

Haven't used KaseyaOne? It's free! Contact Support to get started.

Insight details

UniView Portal includes these Unitrends insights:

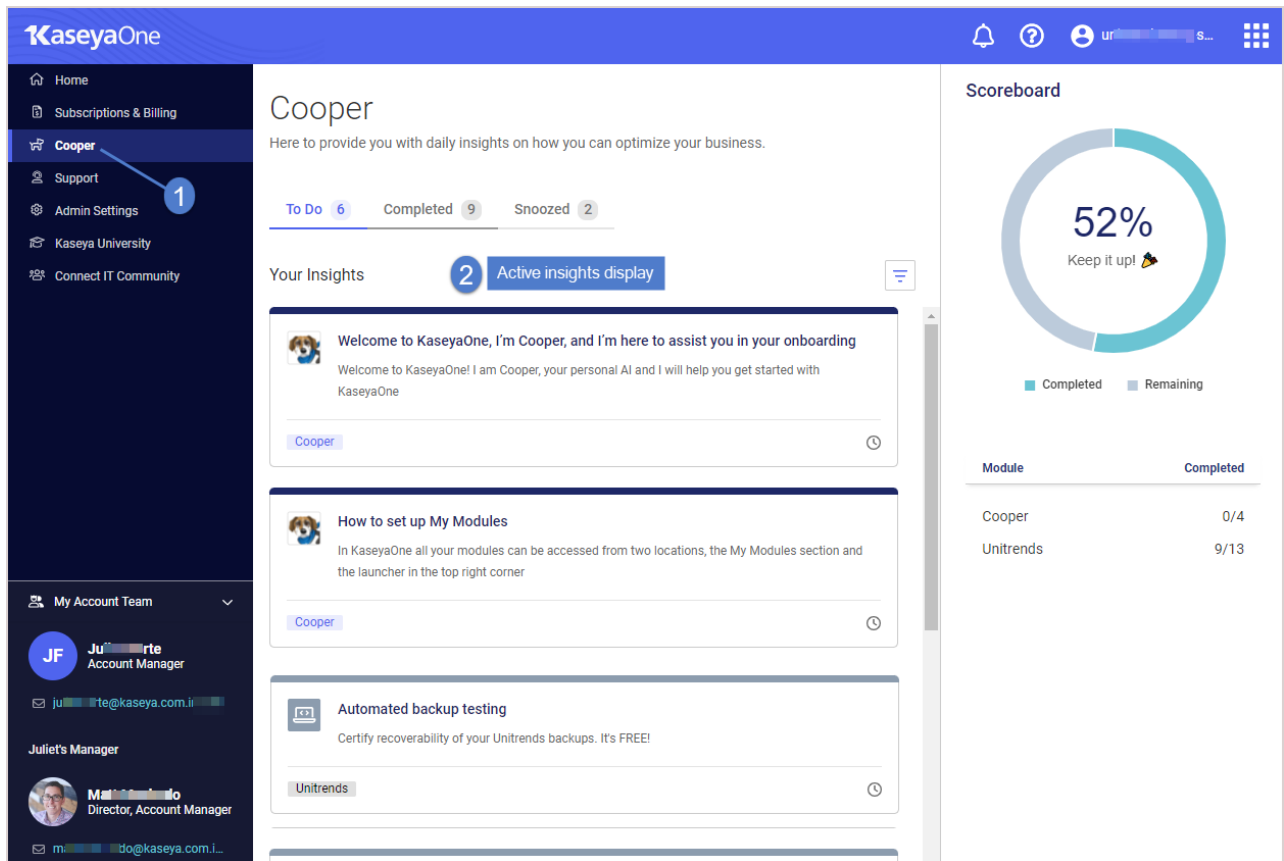
Component & Insight Name	Summary	Triggers	Excludes
Appliance updates			
You could be missing out on critical updates	Enable Helix auto updates to keep your appliances updated to the latest release.	Send if Helix auto updates have not been enabled on any appliance in the UniView Portal.	<ul style="list-style-type: none"> • Tenant was added < 7 days ago. • A Unitrends appliance with at least one protected asset has not been added to the UniView Portal
Backup			


Component & Insight Name	Summary	Triggers	Excludes
Automated backup testing	Certify recoverability of your backups by running Unitrends Data Copy Access (DCA) jobs. It's FREE!	Send if there are no scheduled DCA jobs.	<ul style="list-style-type: none"> Tenant was added < 7 days ago.
You haven't set up backup alerting yet	Set a threshold for how long machines can go without a good backup and receive alerts if this threshold is exceeded.	Send if backup alerting has not been set up in the UniView Portal.	<ul style="list-style-type: none"> Tenant was added < 7 days ago.
Backup copy			
You are one incident away from total data loss!	Prevent data loss by setting up a backup copy job on the Unitrends appliance to store copies of your backups off-site.	Send if there are no scheduled backup copy jobs.	<ul style="list-style-type: none"> Tenant was added < 7 days ago. A Unitrends appliance with at least one protected asset has not been added to the UniView Portal
You haven't set up replication alerting yet	Set a threshold for how long machines can go without a good offsite replication and receive alerts if this threshold is exceeded.	Send if replication alerting has not been set up in the UniView Portal.	<ul style="list-style-type: none"> Tenant was added < 7 days ago.
PSA integration			
You're losing time without PSA ticketing integration	Integrate your PSA system (ConnectWise Manage, Autotask, BMS, or Vorex) so that each BackupIQ alert also creates a ticket in the PSA.	Send if no PSA system has been integrated.	<ul style="list-style-type: none"> Tenant was added < 7 days ago.
Your tickets could be going to the wrong inbox	Map your UniView Portal organizations to PSA companies or accounts to ensure tickets are assigned to the correct queue.	Send if no organizations have been mapped to your PSA accounts or companies.	<ul style="list-style-type: none"> Tenant was added < 7 days ago. PSA integration was added < 7 days ago.

Component & Insight Name	Summary	Triggers	Excludes
You could be saving more time with automated ticketing updates!	Use your UniView Portal PSA integration to automatically close tickets.	Send if your PSA integration settings have not been configured to automatically close tickets by status.	<ul style="list-style-type: none"> Tenant was added < 7 days ago. No PSA system has been integrated with UniView Portal.

To view and manage insights

- 1 Log in to KaseyaOne and select **Cooper**.
- 2 Active insights display in the To Do list.



- 3 (Optional) Filter the To Do list to display only Unitrends insights: click , check the Unitrends Module box, and click **Apply**.

The screenshot displays the KaseyaOne UniView Portal interface. On the left is a dark sidebar with navigation links: Home, Subscriptions & Billing, Cooper (selected), Support, Admin Settings, Kaseya University, and Connect IT Community. The main content area is titled 'Cooper' and includes a sub-header 'Here to provide you with daily insights on how you can optimize your business.' Below this are tabs for 'To Do' (6), 'Completed' (9), and 'Snoozed' (2). A 'Your Insights' section shows a list of insights, with a filter menu open over the first one. The filter menu has 'Unitrends' selected under 'Module' and 'Apply' highlighted. A 'Scoreboard' section on the right features a circular progress indicator at 52% with the text 'Keep it up! 🏆' and a legend for 'Completed' (teal) and 'Remaining' (grey). Below the scoreboard is a table:

Module	Completed
Cooper	0/4
Unitrends	9/13

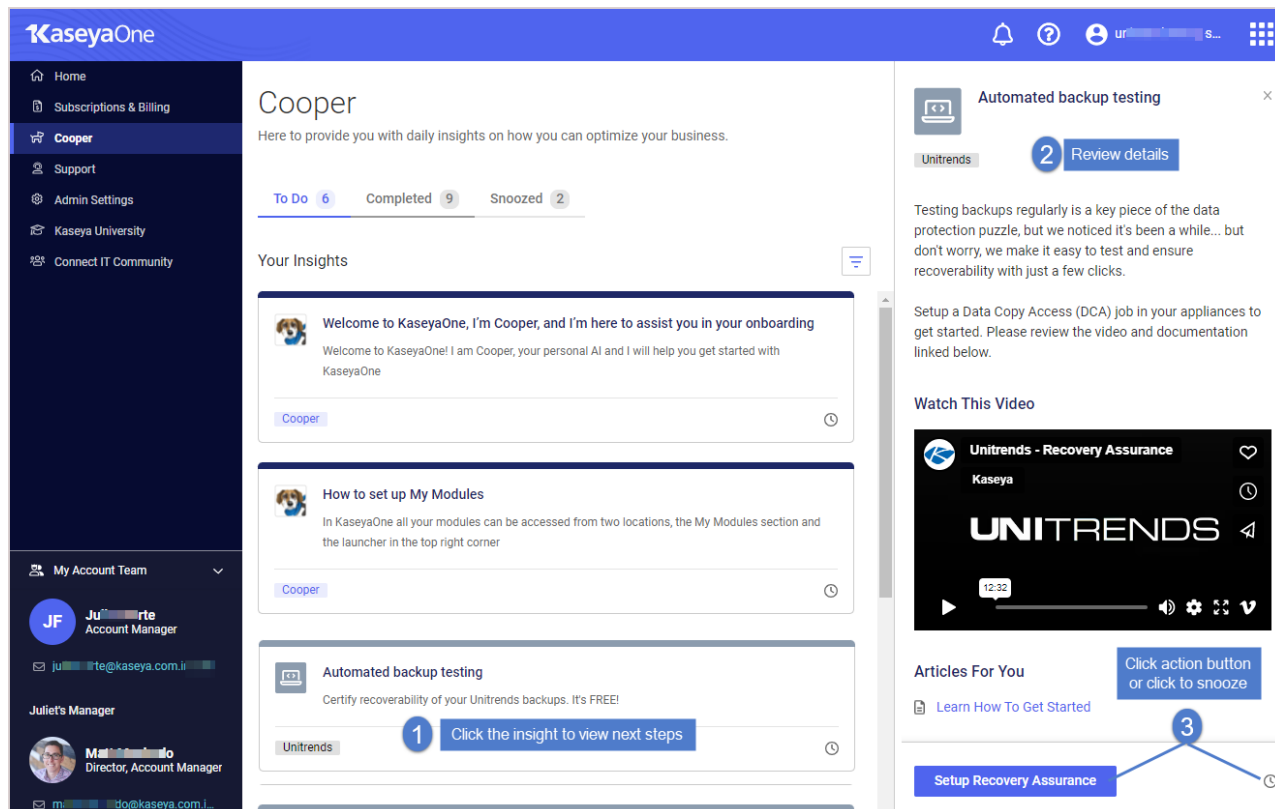
4 Click a Unitrends insight.

5 Review insight details. Do one of the following:

- Click the action button to address the insight (*Setup Recovery Assurance* in our example). For details, see "[Resolving insights](#)" below.

OR

- Click ⌚ to move the insight to the Snoozed list.



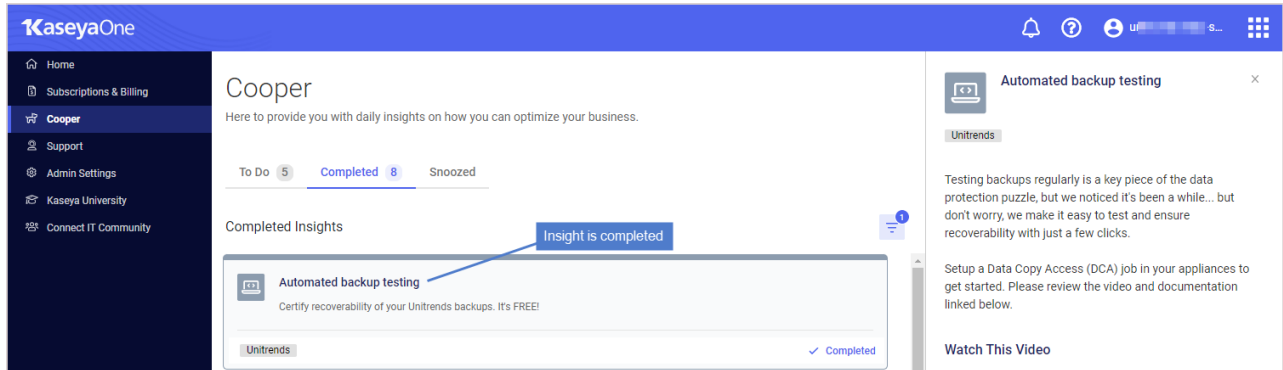
Resolving insights

Find your insight in this table for next steps:

Component	Insight	Steps to resolve
Appliance updates	You could be missing out on critical updates	Enable Helix auto updates for an appliance. See " Modifying Helix Auto Update settings " for details.
Backup	Automated backup testing	Create a DCA job on a Unitrends appliance. See Recovery Assurance in the Administrator Guide for Recovery Series, Recovery MAX, ION/ION+, and Unitrends Backup for details.
Backup	You haven't set up backup alerting yet	Set up conditional alarm thresholds for backups. See " Conditional alarms " for details.

Component	Insight	Steps to resolve
Backup copy	You are one incident away from total data loss!	<p><i>Backup copies</i> are duplicates of your backups that are stored off-site. You can copy your backups to the following types of targets: Unitrends Cloud, a secondary Unitrends appliance, cloud storage (managed by Amazon, AWS, Google, or Rackspace), disks, NAS devices, and other media.</p> <p>To resolve this insight, add a backup copy target to a Unitrends appliance and create a backup copy job to copy backups to the target. See these topics in the Administrator Guide for Recovery Series, Recovery MAX, ION/ION+, and Unitrends Backup for details:</p> <ul style="list-style-type: none"> • Backup copy targets • Creating backup copy jobs
Backup copy	You haven't set up replication alerting yet	Set up conditional alarm thresholds for offsite replications. See " Conditional alarms " for details.
PSA integration	You're losing time without PSA ticketing integration	Integrate your PSA with the UniView Portal to enable BackupIQ to create PSA tickets for your alerts. See the following for details: " Integrating Autotask ", " Integrating ConnectWise Manage ", or " Integrating Kaseya's Billing Management System (BMS) or Vorex ".
PSA integration	Your tickets could be going to the wrong inbox	Map your PSA's accounts or companies to UniView Portal organizations to ensure tickets are sent to the correct PSA queue. See " Mapping companies and accounts to organizations " for details.
PSA integration	You could be saving more time with automated ticketing updates!	Edit your PSA's integration settings to automatically close tickets by selecting a status in the Close Ticket Status field. See the following for details: " To view or modify Autotask integration settings ", " To view or modify ConnectWise Manage integration settings ", or " To view or modify BMS or Vorex integration settings ".

- 6 When the insight condition is resolved, the insight moves to the Completed list.



Integrating Autotask

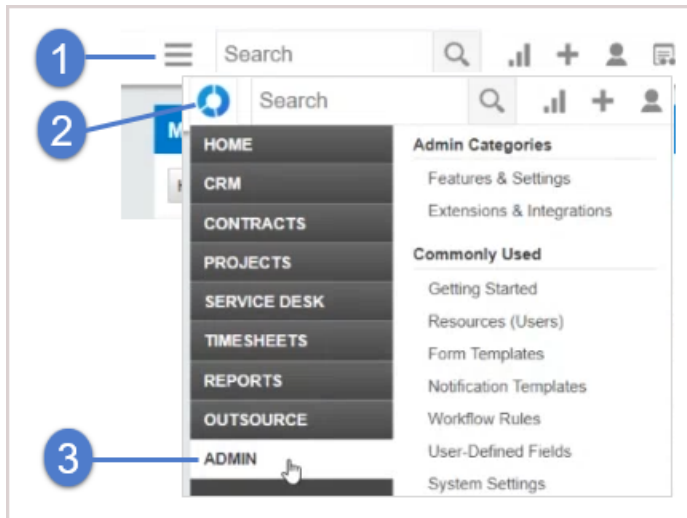
Use the procedures below to integrate Autotask PSA with the UniView Portal. Once you have configured the integration, Autotask creates tickets based on alerts and warnings issued by BackupIQ.

- " Step1: Create a UniView Portal API user in Autotask"
- " Step 2: Add the Autotask integration in the UniView Portal"

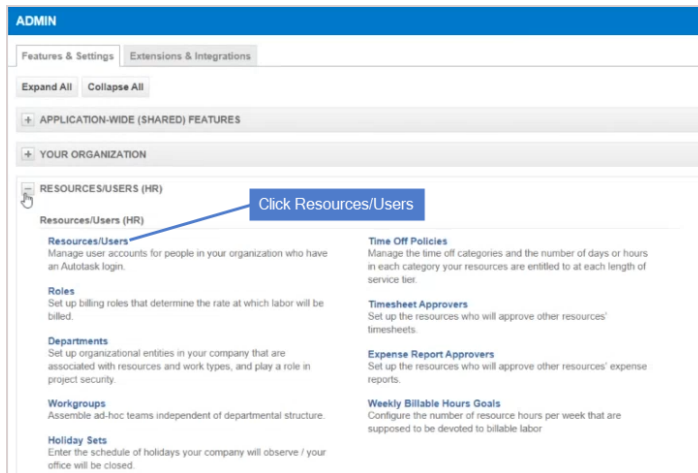
Step1: Create a UniView Portal API user in Autotask

Use this procedure to create an API user that Autotask will use for the UniView Portal integration.

- 1 Log in to Autotask.
- 2 Select > > Admin.



- 3 Expand Resources/Users (HR) and click Resources/Users.

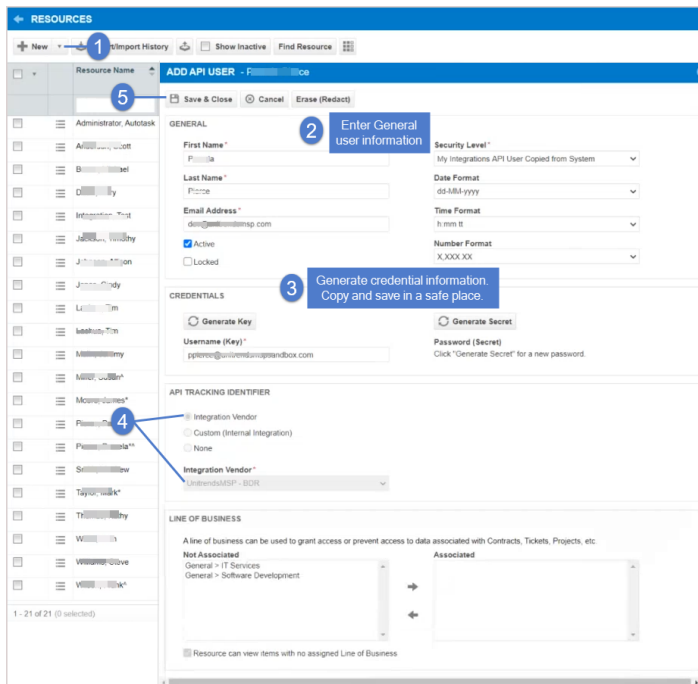


4 Click **New**.

5 Enter user information.

- Be sure to select the following in the API Tracker Identifier area: the **Integration Vendor** option and **UnitrendsMSP-BDR** from the Integration Vendor list.
- Save the username and password of the API user in a safe place. You will need these credentials to complete the integration.

6 Click **Save & Close**.

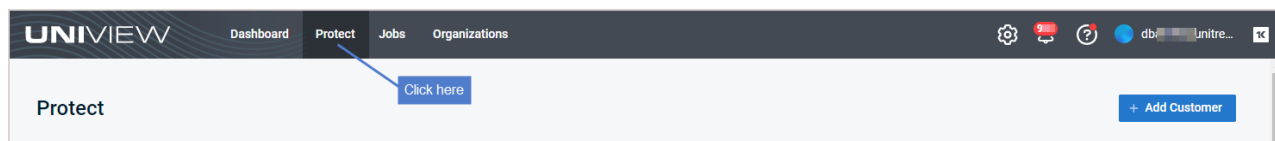


Step 2: Add the Autotask integration in the UniView Portal

Use this procedure to add the integration to the UniView Portal.

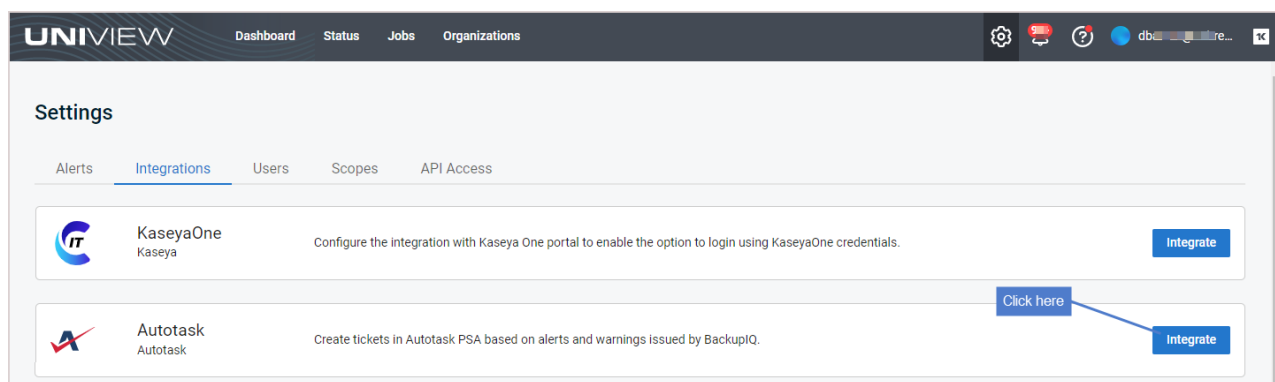
1 Log in to the UniView Portal with a superuser account.

2 Click :



3 Select the **Integrations** view.

4 Locate the Autotask integration and click **Integrate**:



5 Enter the **Username** and **Password** of the API user.

6 (Recommended) Click **Test Credentials** to verify that UniView Portal can connect to Autotask.

7 Click **Next Step**.

Autotask Integration ✕

Please fill out your credentials below

Username
PP@unitrends.com 1

Password
..... 👁

Test Credentials 2

Cancel Next Step 3

8 Select an Autotask account from the Account list.

By default, the account you select here is applied to all Autotask organizations. The list contains all Autotask accounts that have been mapped to a UniView Portal organization. If you don't see your account in the list, use the ["Mapping companies and accounts to organizations"](#) procedure to add the account to the list. Later in this procedure you can map different accounts to other organizations as needed.

9 Select an Autotask ticketing queue from the list.

- The queue you select is the location where BackupIQ tickets will be created in Autotask.
- Only one Autotask ticketing queue can be used for BackupIQ tickets.
- This list contains all Autotask queues assigned to the Unitrends MSP account. (If needed, you can use Autotask to create a new queue to use for BackupIQ tickets.)
- You can switch to another queue at any time by editing this setting (see ["To view or modify Autotask integration settings"](#).)

10 (Optional) BackupIQ dismisses offline appliance alerts and conditional alarms automatically when the alert condition has been resolved. You can opt to automatically close corresponding Autotask tickets by selecting a status from the Close Ticket Status list. Or select *Do not close automatically*.

11 Select a priority level for alerts. Choose from these levels: Do not sync, High, Medium, Low, or Critical.

Autotask Integration Settings ✕

Account

Unitrends MSP 1 Select an account ▼

Queue

Client Portal 2 Select a ticketing queue ▼

Close Ticket Status

Complete 3 (Optional) To automatically close tickets, select a status from the list ▼

Select priority for alerts

Alerts

High 4 Select priority level for alerts ▼

Reset For All Organizations Create Test Ticket Cancel Save

12 (Recommended) Click **Create Test Ticket**. Go to Autotask to view the test ticket.

Autotask Integration Settings ✕

Account
Unitrends MSP ▼

Queue
Client Portal ▼

Close Ticket Status
Complete ▼

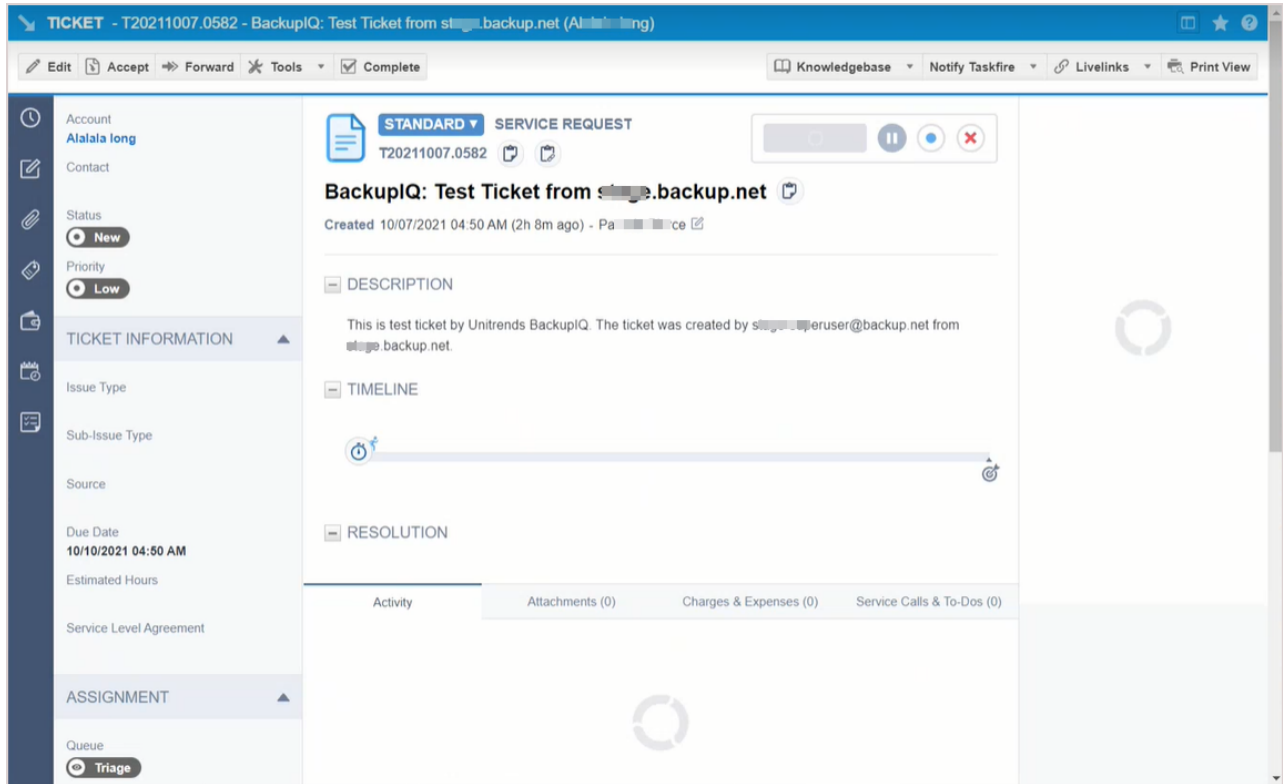
Select priority for alerts

Alerts
High ▼

Reset For All Organizations Create Test Ticket

(Recommended)
Click to create a test ticket

Sample test ticket in Autotask:



13 Click **Save**.

Autotask Integration Settings ✕

Account
Unitrends MSP ▼

Queue
Client Portal ▼

Close Ticket Status
Complete ▼

Select priority for alerts

Alerts
High ▼

[Click here](#)

[Reset For All Organizations](#) [✓ Create Test Ticket](#) [Cancel](#) [Save](#)

14 Map organizations to Autotask accounts.

By default, all organizations are mapped to the account you selected above in [step 8](#). If needed, assign organizations to other Autotask accounts as shown here. Once you've completed your account selections, click **Map**:

Notes:

If there are no Autotask accounts in the Organization Mapping dialog, or if you do not see all accounts in the drop-down lists:

- 1 Click **Map** to add the integration and exit the dialog.
- 2 Import organizations from Autotask as described in "[Importing Accounts or Companies from your PSA](#)".

Organization Mapping

Choose related entity on the right dropdown to create mapping

Search 250 per page 1 of 2 pages < >

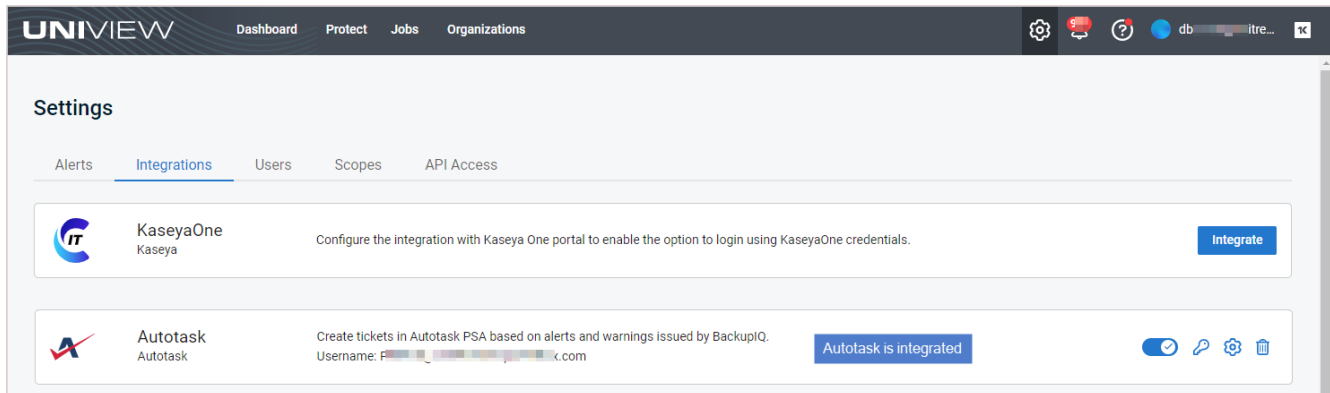
(optional) Enter text to search for an organization

Organization	Autotask Account
212 Bronx	ABLE Ma... ▾
212 Bronx Child	Autotask Acco... ▾
212 Brooklyn	Autotask Accour ▾
78910 Corporation	Upstate Document Providers
78 [blurred]	ABLE Manufacturing West Coast
[blurred]	Unitrends MSP Northeast
	212 Bronx

1 Map organizations to Autotask accounts

2 Cancel Map

The integration is added.



- 3 After you have completed the step above, tickets are added to the Autotask queue as new BackupIQ alerts. To view these tickets, see ["Integrating Autotask"](#).

Note: Autotask tickets are created for all BackupIQ alerts unless you selected *Do not sync* in the Autotask Integration Settings Alerts field.

Working with your Autotask Integration

Once you've integrated Autotask, use these procedures as needed:

- ["To view BackupIQ tickets in Autotask"](#)
- ["To view or modify one organization's Autotask settings"](#)
- ["Working with your Autotask Integration"](#)

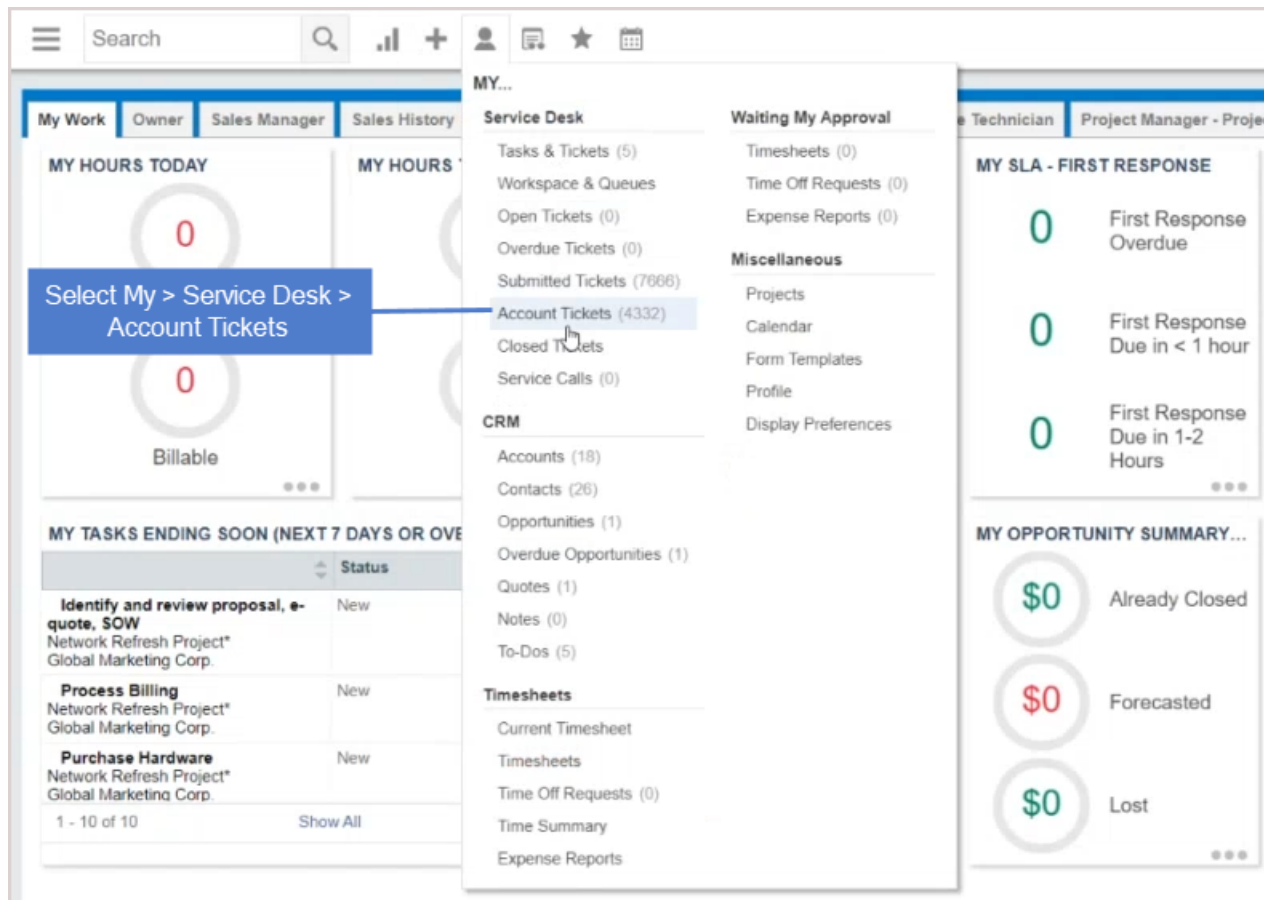
Note: The procedures below can be run only by users that have the superuser role.

- ["To view or modify Autotask integration settings"](#)
- ["To set up integrated customer billing for Spanning Microsoft 365 and Spanning Google Workspace"](#)
- ["To remove the Autotask integration"](#)

To view BackupIQ tickets in Autotask

After you have integrated Autotask with the UniView Portal, tickets are automatically created for BackupIQ alerts generated in your UniView Portal environment. Use these steps to view these tickets in Autotask.

- 1 Log in to Autotask.
- 2 Select **My > Service Desk > Account Tickets**.



3 Enter the following:

- Account Name – Select **Unitrends MSP**.
- Status – Select **All**.
- From and To – Select the date range of tickets to view.

4 Click **Generate**. Tickets generated in the specified date range display. Click a ticket to view details.

MY ACCOUNT TICKETS

Hide Report Criteria Save Report as HTML

REPORT CRITERIA

Account Name: prodtest, qalest, TopDog, Troy Wire and Cable, **Unitrends MSP**

Status: **All**, All Open, New, Waiting Dispatch, Scheduled

Sort By: Date & Time

From: 03/01/2020 To: 06/17/2020

Generate

My Account Tickets
From 02/29/2020 To 06/17/2020 06/17/20 05:08M

Ticket #	Title	Account	State	Queue	Status	Priority	Alloc	Created	Due
T20200304.0001	Alert - QA_Test - AppReg1	Unitrends MSP	Massachusetts	IT.Level I	New	High		03/04/2020	01/12/2020
T20200304.0002	Alert - QA_Test - AppReg1	Unitrends MSP	Massachusetts	IT.Level I	New	High		03/04/2020	01/12/2020
T20200304.0003	Job Failure - QA_Test - AppReg1	Unitrends MSP	Massachusetts	IT.Level I	New	High		03/04/2020	02/29/2020
T20200304.0004	Job Failure - QA_Test - AppReg1	Unitrends MSP	Massachusetts	IT.Level I	New	High		03/04/2020	03/01/2020
T20200304.0005	Job Failure - QA_Test - AppReg1	Unitrends MSP	Massachusetts	IT.Level I	New	High		03/04/2020	03/02/2020
T20200304.0006	Job Failure - QA_Test - AppReg1	Unitrends MSP	Massachusetts	IT.Level I	New	High		03/04/2020	03/03/2020
T20200304.0007	Job Failure - QA_Test - AppReg1	Unitrends MSP	Massachusetts	IT.Level I	New	High		03/04/2020	03/04/2020
T20200304.0008	Job Failure - QA_Test - AppReg1	Unitrends MSP	Massachusetts	IT.Level I	New	High		03/04/2020	03/05/2020
T20200304.0009	Job Failure - QA_Test - AppReg1	Unitrends MSP	Massachusetts	IT.Level I	New	High		03/04/2020	03/06/2020
T20200331.0002	Alert - Afourtech - tp-207	Unitrends MSP	Massachusetts	IT.Level I	New	High		03/31/2020	04/03/2020
T20200331.0006	Alert - Afourtech - tp-207	Unitrends MSP	Massachusetts	IT.Level I	New	High		03/31/2020	04/03/2020
T20200331.0007	Alert - Afourtech - tp-207	Unitrends MSP	Massachusetts	IT.Level I	New	High		03/31/2020	04/03/2020
T20200331.0008	Alert - Afourtech - tp-207	Unitrends MSP	Massachusetts	IT.Level I	New	High		03/31/2020	04/03/2020
T20200331.0009	Alert - Afourtech - tp-207	Unitrends MSP	Massachusetts	IT.Level I	New	High		03/31/2020	04/03/2020

Tickets display. Click a ticket to view details.

TICKET - T20200331.0009 - Alert - Afourtech - tp-207 (Unitrends MSP)

Edit Accept Forward Tools Complete Knowledgebase Notify Taskflr

Account: Unitrends MSP

Contact

Status: **New**

Priority: **High**

TICKET INFORMATION

Issue Type

Sub-Issue Type

Source

Due Date: **04/03/2020 09:54 AM**

Estimated Hours

Service Level Agreement

ASSIGNMENT

Queue

STANDARD SERVICE REQUEST
T20200331.0009

Alert - Afourtech - tp-207
Created 03/31/2020 09:55 AM (77d 19h 14m ago) - Pamela Pierce

DESCRIPTION

Alert details Created: Tue, 31 Mar 2020 16:54:00 +0000 Due: Fri, 03 Apr 2020 16:54:00 +0000 Severity: critical Appliance: tp-207 Message: The VM replica tp-Centos-minimal_replica758503 has been invalidated. The replica has entered live mode. Please delete the replica and start over.

TIMELINE

RESOLUTION

Activity Charges & Expenses (0) Service Calls & To-Dos (0)


New Time Entry New Note New Attachment

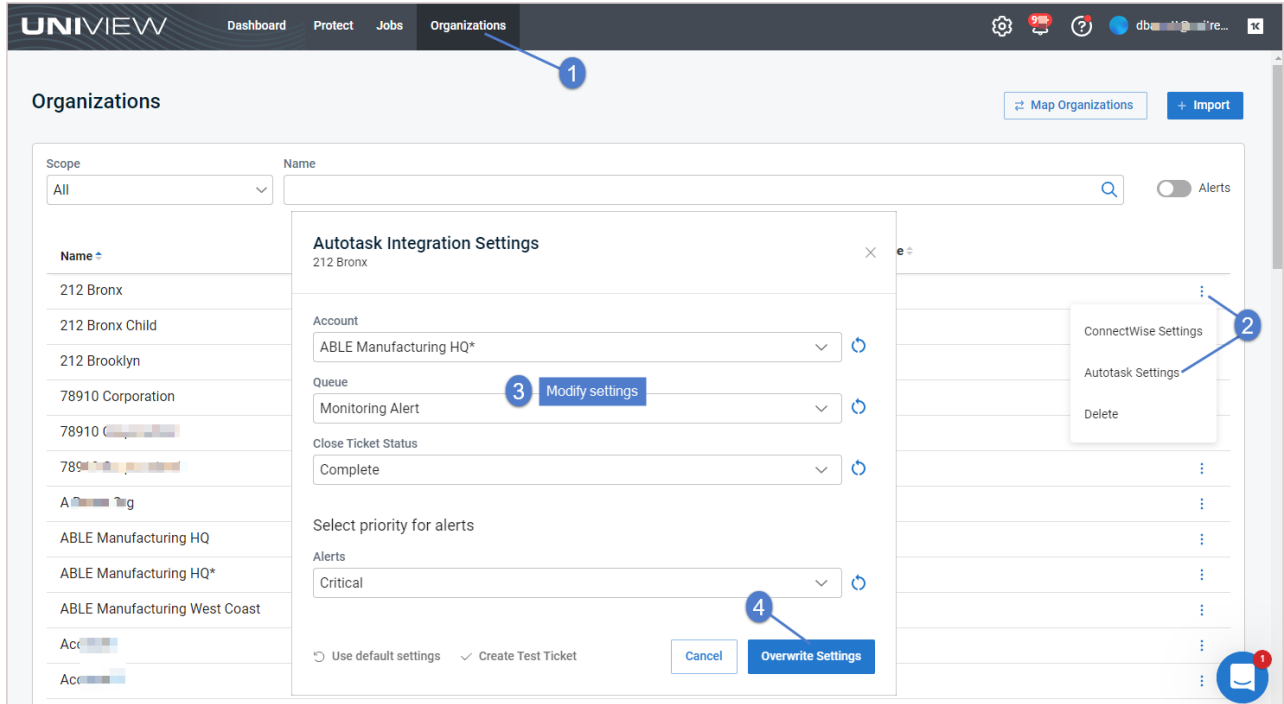
Add a note...

To view or modify one organization's Autotask settings


By default, the integration's account, queue, close ticket status, and alert priority settings are applied to all organizations. If needed, you can use this procedure to apply different settings to an organization or to re-apply the default settings to an organization whose settings you have modified.

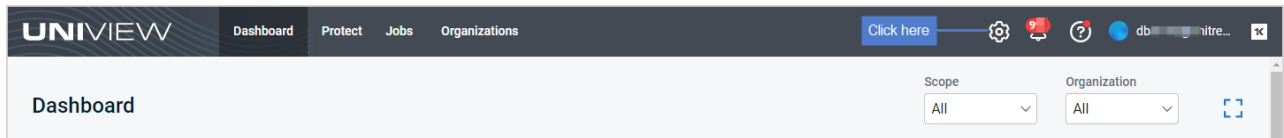
- 1 Log in to the UniView Portal.
- 2 Select **Organizations**.


- 3 Locate the organization. Click  and select **Autotask Settings**.
- 4 (Optional) Do one of the following:
 - Modify settings and click **Overwrite Settings** to apply your changes.
 - To re-apply the defaults to this organization, click **Use Default Settings**, then click **Overwrite Settings** to apply your changes.

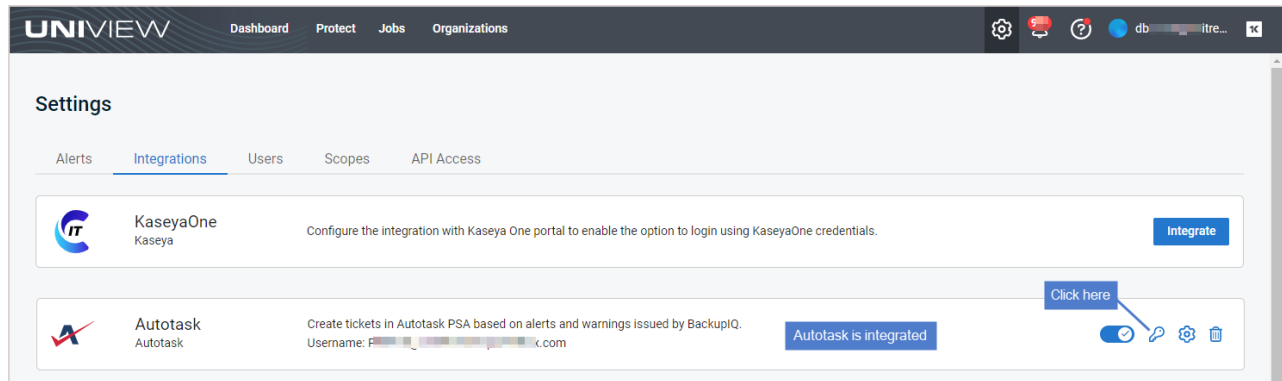



To view or modify Autotask integration settings

- 1 Log in to the UniView Portal with a superuser account.
- 2 Click :



- 3 Select the **Integrations** view.
- 4 Locate the Autotask integration and click .



- 5 (Optional) To view the Password, click the  icon.
- 6 (Optional) Modify credentials settings. Click **Test Credentials** to verify that UniView Portal can connect to Autotask.
- 7 Click **Next Step**.

Autotask Integration ×

Please fill out your credentials below

Username

PP@...@...k.com

Password

.....

Test Credentials

Cancel

Next Step

- 8 (Optional) Modify integration settings.
- 9 (Optional) Click **Reset For All Organizations** to apply changes to all Autotask organizations.
- 10 Click **Save**.

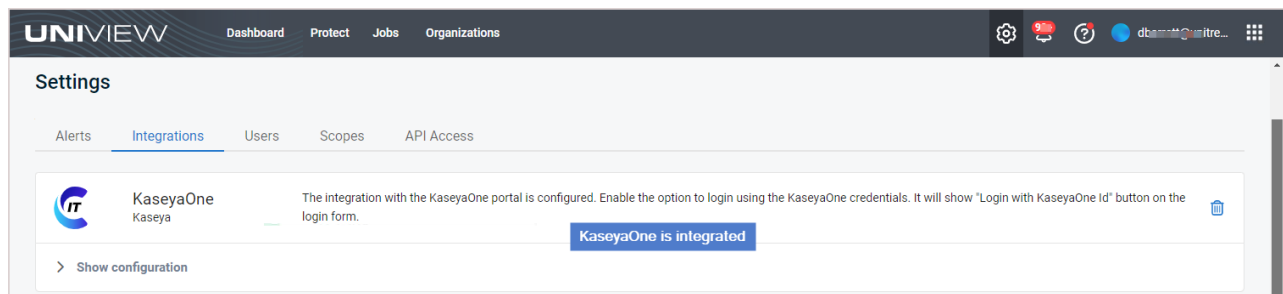
To set up integrated customer billing for Spanning Microsoft 365 and Spanning Google Workspace

Use these procedures to set up Autotask integrated customer billing for Spanning Backup for Microsoft 365 and/or Spanning Backup for Google Workspace. These procedures enable the following license information to be posted to Autotask each night: number of Standard Licenses in Use and number of Archived Licenses, by Spanning tenant or domain. This license data is then used by Autotask when generating invoices.

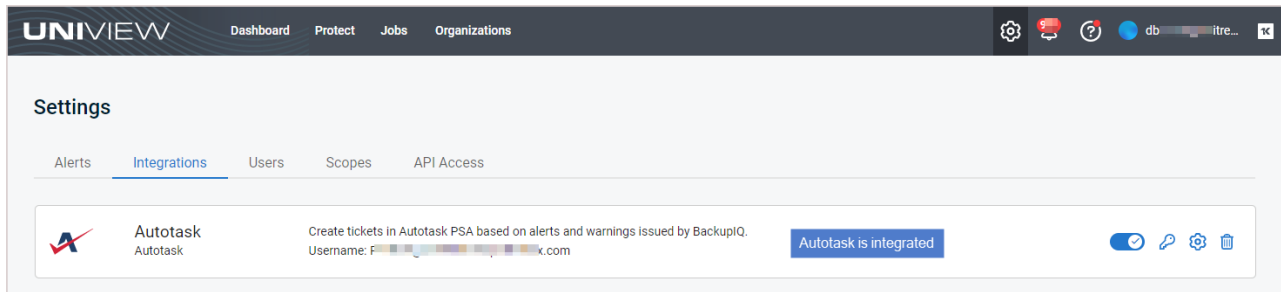
Prerequisites

Ensure that these prerequisites have been met before running the procedures below:

- UniView Portal has been integrated with KaseyaOne. (To add the integration, see "[Integrating KaseyaOne](#)".)



- UniView Portal has been integrated with Autotask. (To add the integration, see "[Integrating Autotask](#)".)



- Your Spanning Backup for Microsoft 365 tenants and/or Google Workspace domains have been integrated with the UniView Portal.
 - To integrated a Microsoft 365 tenant, see "[Integrating a Microsoft 365 tenant](#)".
 - To integrate a Google Workspace domain, see "[Integrating a Google Workspace domain](#)".

Use these procedures to set up integrated customer billing for Spanning Backup Microsoft 365 and Google Workspace domains:

- "[Step 1: Set up organization mapping in UniView](#)"
- "[Step 2: Verify that corresponding mappings have been created in Autotask](#)"
- "[Step 3: Set up service mapping in Autotask](#)"

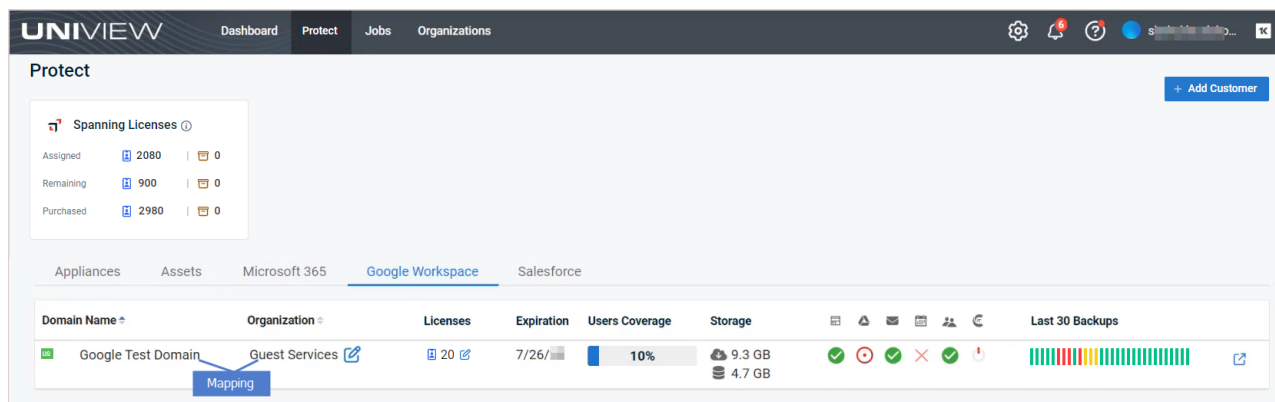
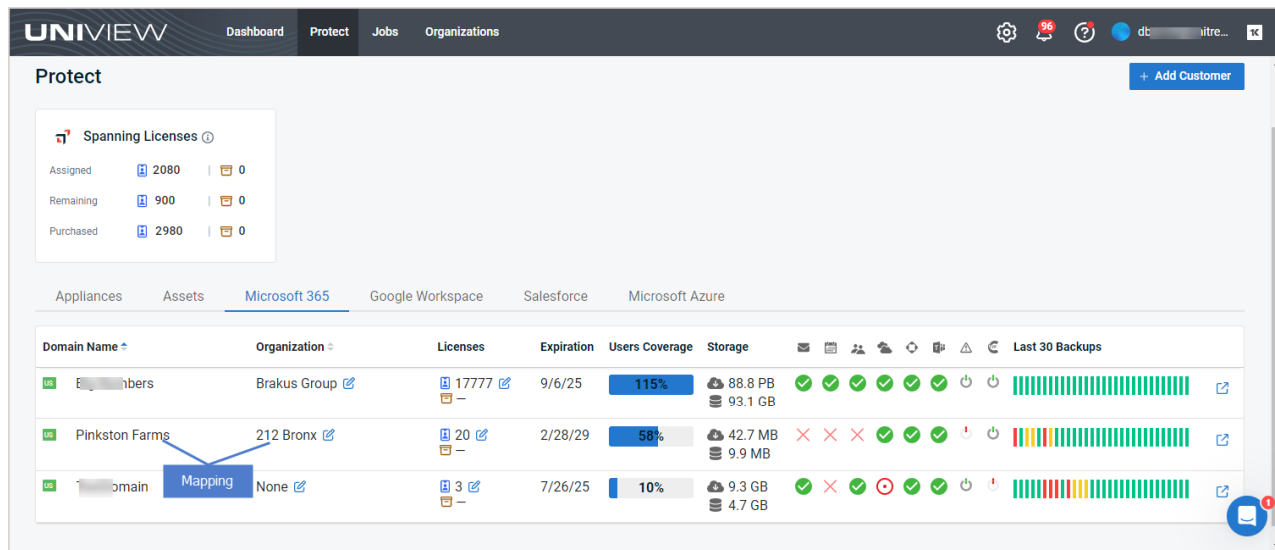
Step 1: Set up organization mapping in UniView

- 1 Log in to the UniView Portal.
- 2 In the Protect > Microsoft 365 or Protect > Google Workspace view, ensure that the Spanning Backup tenants and domains for which you will use integrated customer billing have been mapped to UniView organizations.

Notes: See these procedures to view and modify mappings:

- "[To map Microsoft 365 tenants to organizations](#)"
- "[To map Google Workspace domains to organizations](#)"

In our example, the Microsoft 365 tenant *Pinkston Farms* has been mapped to the UniView organization *212 Bronx*, and the Google Workspace domain *Google Test Domain* has been mapped to the UniView *Guest Services* organization:

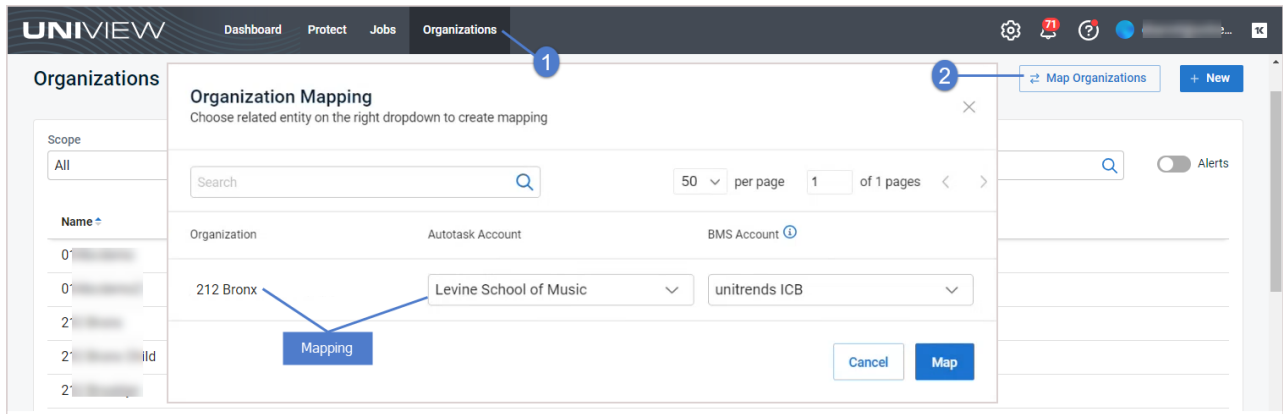


3 On the Organizations page, click **Map Organizations** and ensure that the UniView organizations that were mapped to the Spanning domains in [step 2](#) have also been mapped to Autotask accounts.

Notes:

- These conditions must be met to post a Spanning domain's license information to Autotask:
 - The Spanning domain is mapped to a UniView organization (in UniView on the Protect > Microsoft 365 or Google Workspace page).
 - The UniView organization that has been mapped to the Spanning domain is also mapped to an Autotask account in UniView (under Organizations > Map Organizations).
- If you don't see your Autotask accounts, import accounts from Autotask as described in "[Importing Accounts or Companies from your PSA](#)".

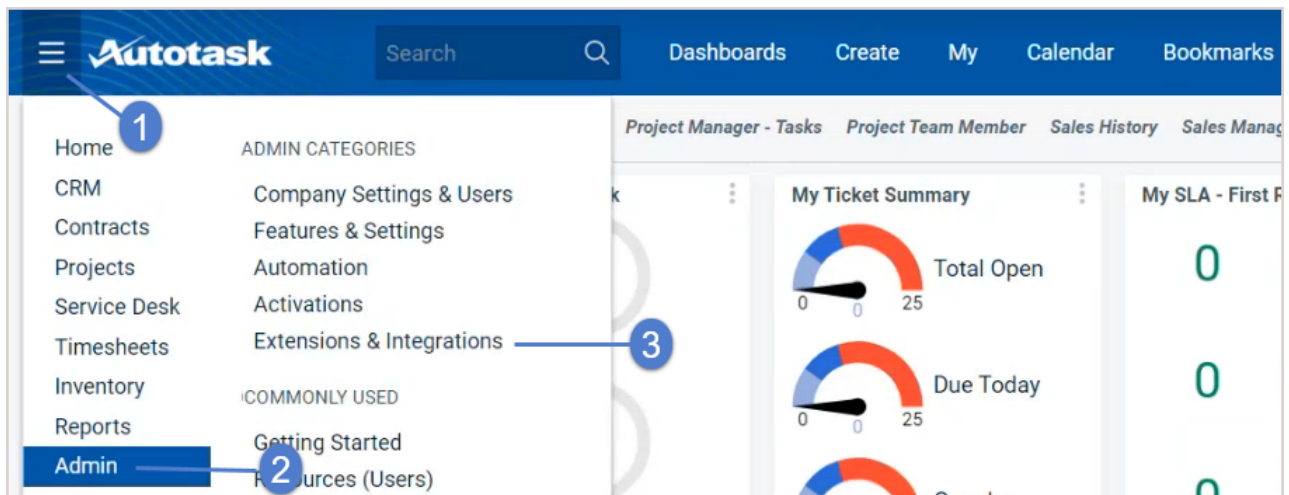
In our example, the UniView organization *212 Bronx* has been mapped to the Autotask *Levine School of Music* account:



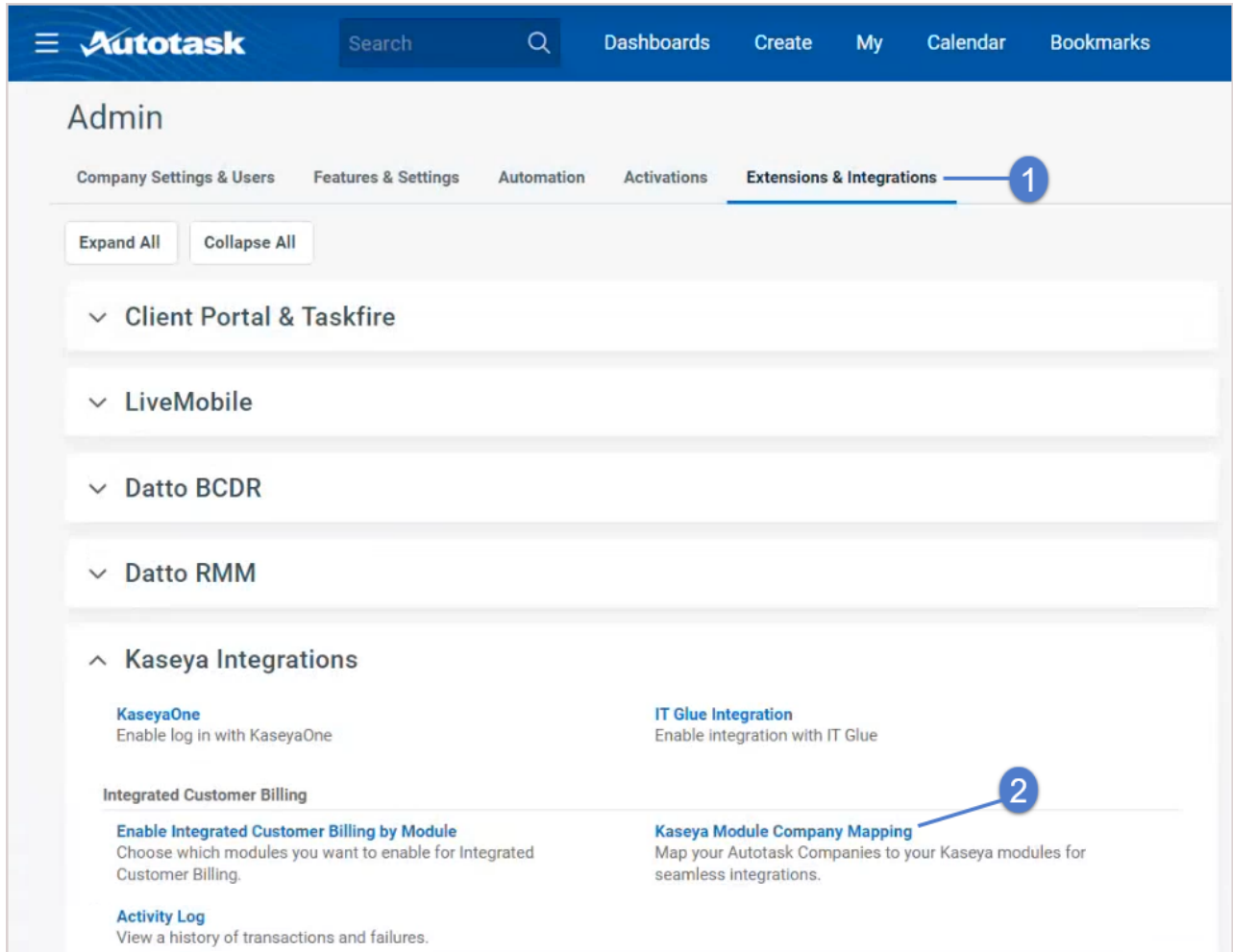
- 4 After the Spanning domain and Autotask organization mappings have been added in UniView, corresponding mappings are automatically created in Autotask.

Step 2: Verify that corresponding mappings have been created in Autotask

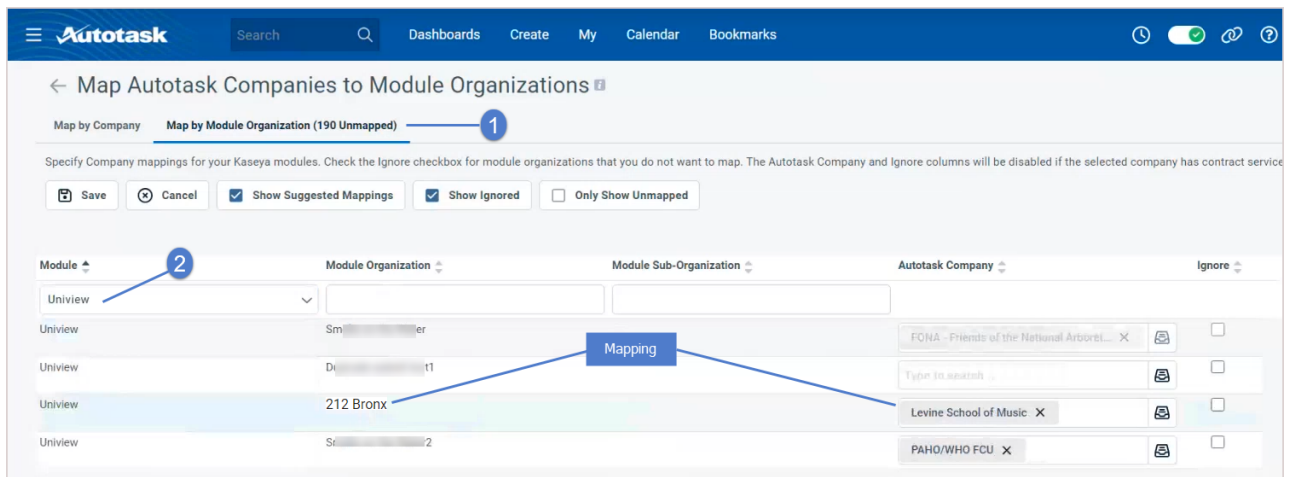
- 1 Log in to Autotask.
- 2 Select  > Admin > Extensions & Integrations.



- 3 On the **Extensions & Integrations** tab, click **Kaseya Integrations > Kaseya Module Company Mapping**:

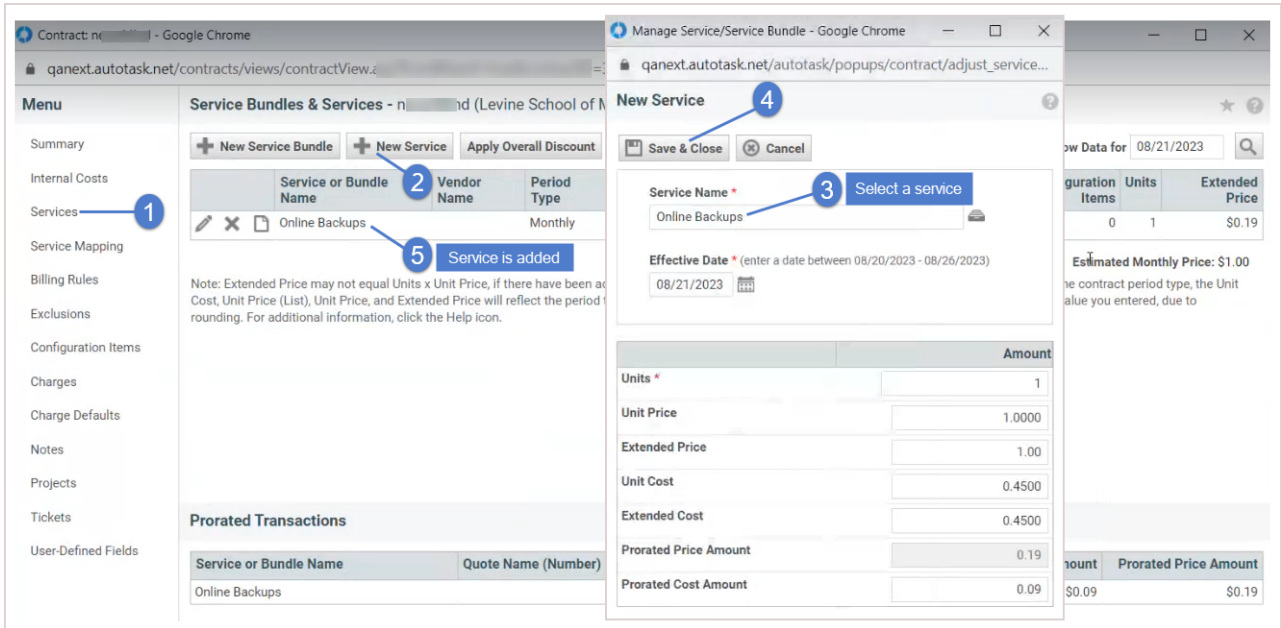


- 4 Click **Map by Module Organization** and select the **UniView** module. UniView mappings display. Our mapping was created automatically:

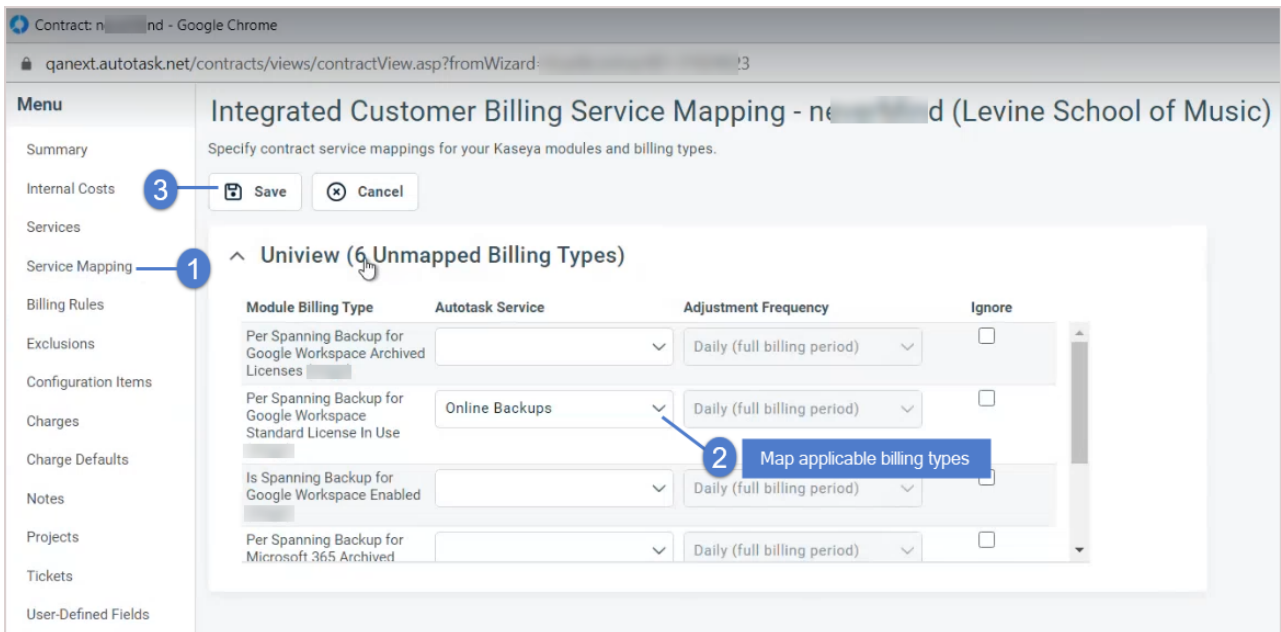


Step 3: Set up service mapping in Autotask

- 1 In Autotask, open the company's contract and select **Services**.
- 2 Click **New Service** and add the applicable billing service (*Online Backups* in our example):



- 3 Select **Service Mapping** and map the applicable Spanning Microsoft 365 and Google Workspace billing types to the service you added above (*Online Backups* in our example). Click **Save**.



The contract is updated:


Service or Bundle Name	Vendor Name	Period Type	Unit Cost	Unit Price (List)	Discount	Unit Price (this Period)	Configuration Items	Units	Extended Price
Online Backups	ICB	Monthly	\$0.10	\$1.00	77.42%	\$0.051	0	6	\$0.45

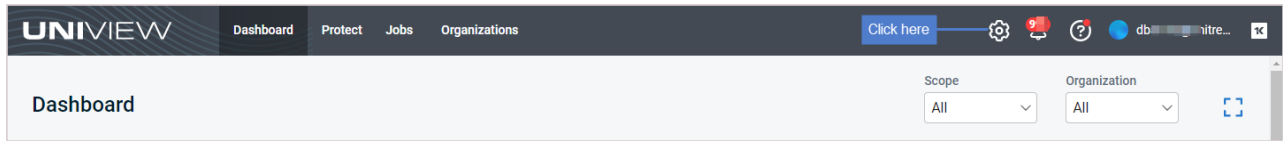
Service or Bundle Name	Quote Name (Number)	Unit Change	Effective Date	Prorated Cost Amount	Prorated Price Amount
Online Backups		1	08/21/2023	\$0.09	\$0.19

Integrated customer billing is set up and Autotask will begin receiving updated Spanning license information each night.

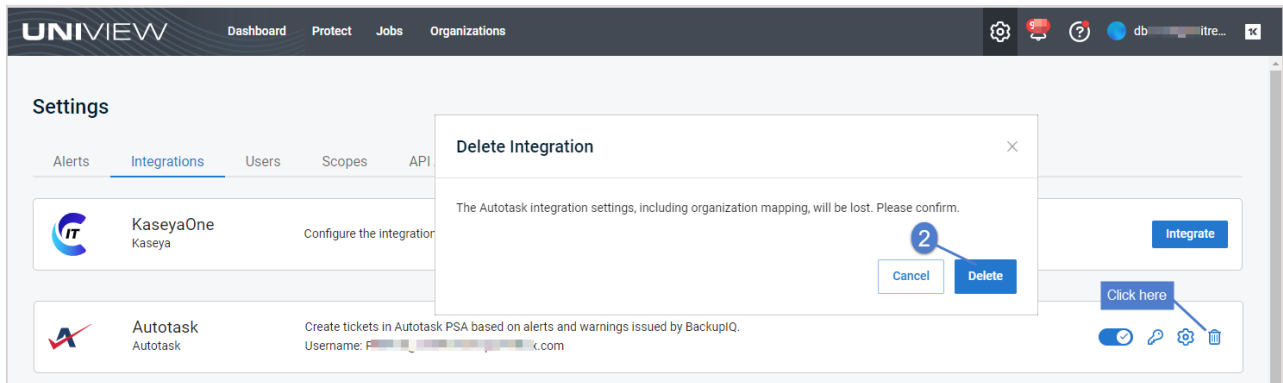
To remove the Autotask integration

Use this procedure to remove the Autotask integration from the UniView Portal.

- 1 Log in to the UniView Portal with a superuser account.
- 2 Click :



- 3 Select the **Integrations** view.
- 4 Locate the Autotask integration and click . Click **Delete**. The integration is removed.



Integrating ConnectWise Manage

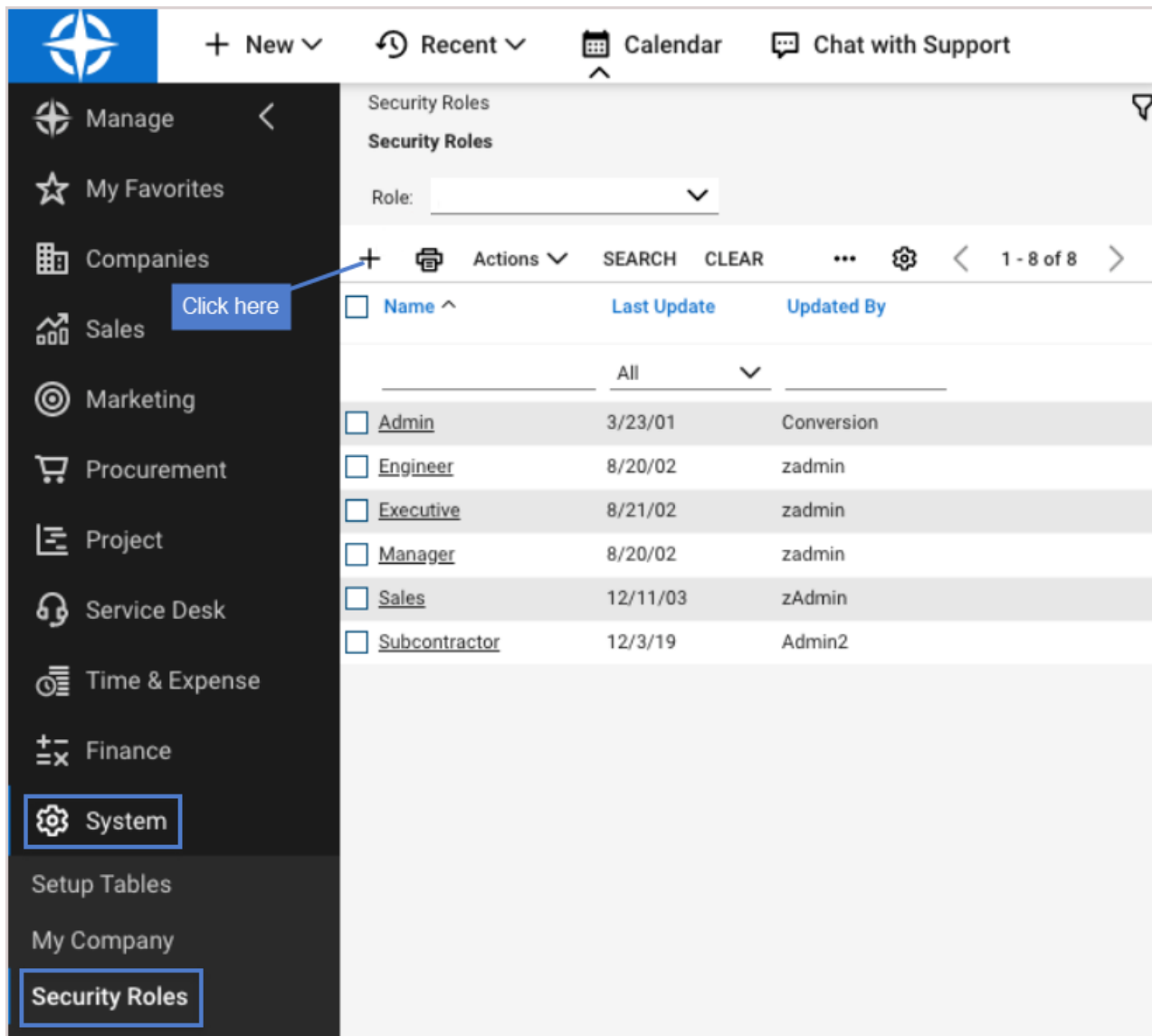
Use these procedures to integrate ConnectWise Manage PSA with the UniView Portal. Once you have configured the integration, ConnectWise Manage creates tickets based on alerts and warnings issued by BackupIQ.

- ["Step 1: Add a security role to ConnectWise"](#)
- ["Step 2: Add the ConnectWise Manage integration"](#)

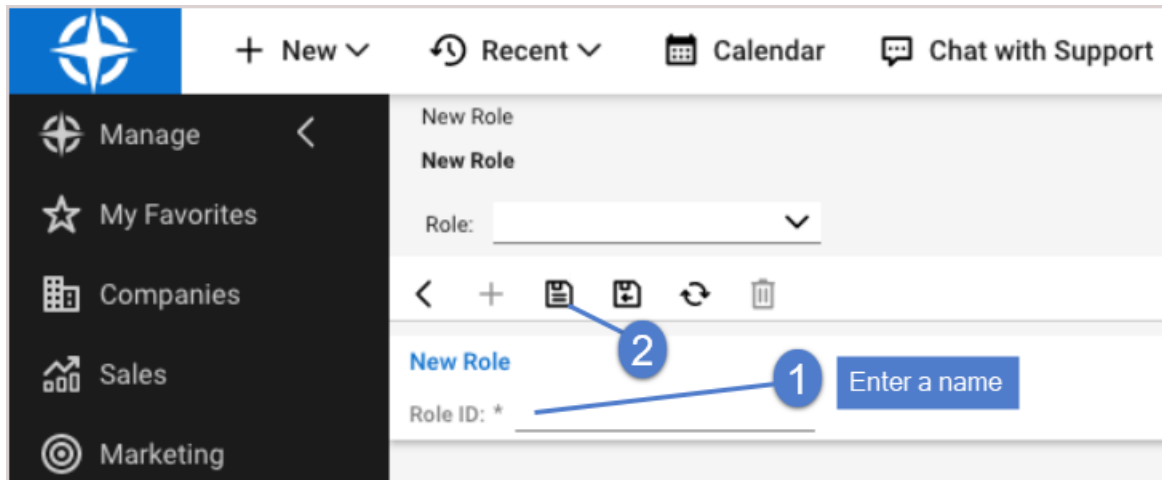
Step 1: Add a security role to ConnectWise

Use this procedure to create a new security role to be used for obtaining the REST API credentials needed for integration with the UniView Portal.

- 1 Log in to ConnectWise Manage with an administrator account.
- 2 Navigate to **System > Security Roles**.
- 3 Click the plus icon (+) at the top of the screen.



- 4 In the Role ID field, enter a name for your new security role (e.g., *UniView Portal API Integration*). Click the **Save** icon.



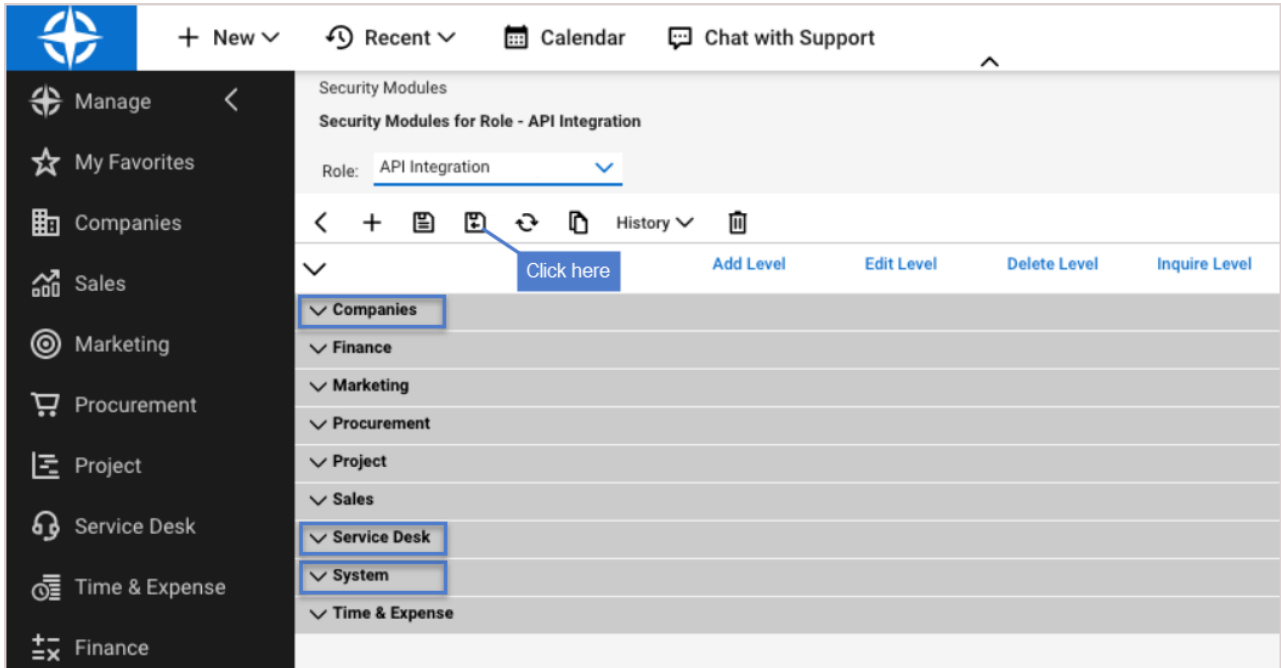
- 5 On the Security Modules screen, click the down arrows beside the Companies, Service Desk, and System headings to expand each section.
- 6 In all three sections, replicate the permission parameters exactly as shown in the tables below. To do so, click the down arrows to change the permissions from None (default) to All. The tables below only show the rows that require editing.

Companies	Add Level	Edit Level	Delete Level	Inquire Level
Company Maintenance	None	None	None	All
Company / Contact Group Maintenance	None	None	None	All

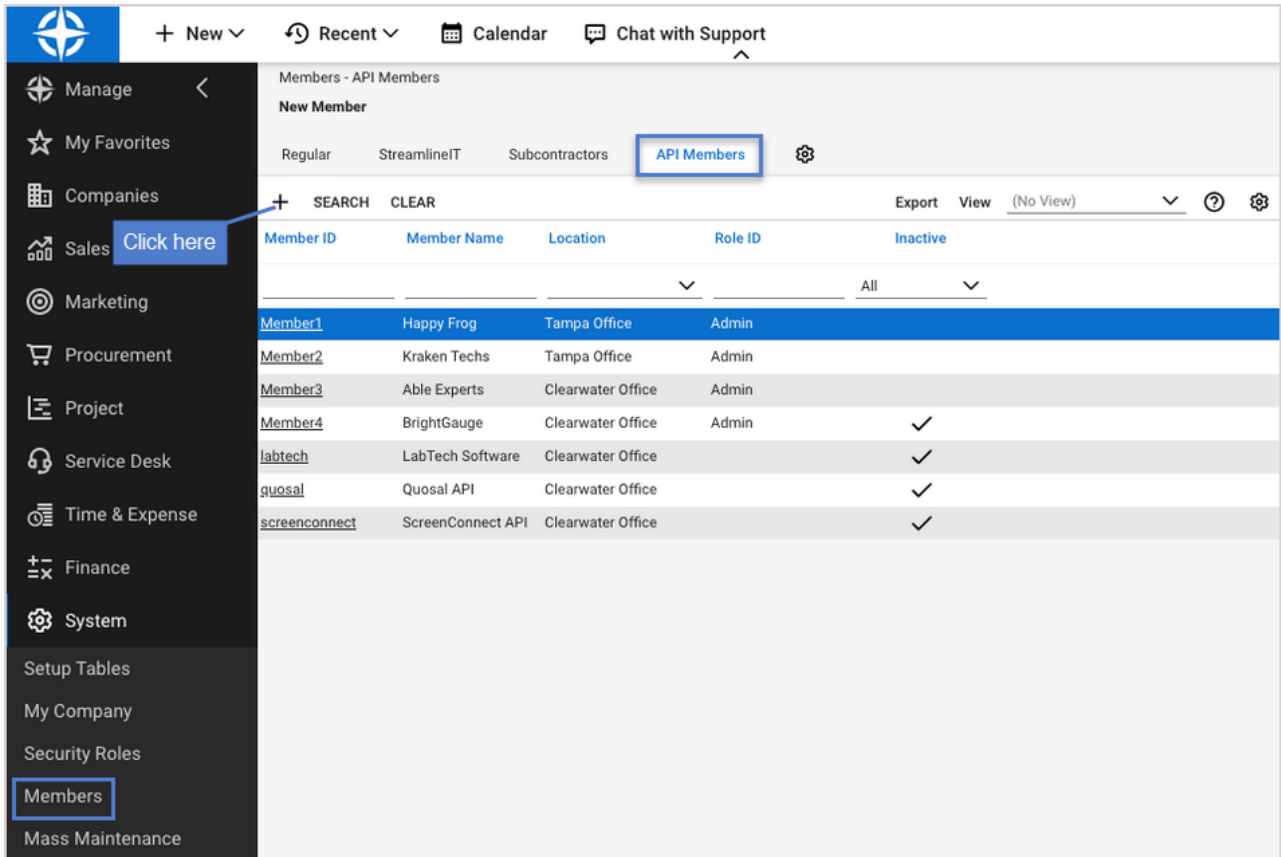
Service Desk	Add Level	Edit Level	Delete Level	Inquire Level
Close Service Tickets	All	All	None	All
Merge Tickets	All	All	None	All
Service Tickets - Dependencies	All	All	None	All
Service Tickets	All	All	None	All
Service Tickets - Finance	All	All	None	All

System	Add Level	Edit Level	Delete Level	Inquire Level
Table Setup	None	None	None	All

- 7 Click the **Save and Close** icon.



8 Navigate to **System > Members > API Members** tab. Click the plus icon (+).



9 On the next Details screen, complete the following fields in each section:

- Profile section –
 - Member ID – Enter the username of the member (e.g., *Uni Portal*). The maximum number of characters allowed is 15.
 - Time Zone – Select a time zone for the internal company.
 - Member Name – Enter the member's first and last name.
- System section –
 - Role ID – The security Role ID controls the level of access to the ConnectWise Manage application by limiting access to functionality. Select the new security role that you created in [step 4](#) (e.g., *UniView Portal API Integration*).
 - Location – Select the default location for the company. Any new record created by the member will default to the location set here.
 - Level – Select the level of access that the member will have in the application. The member will be able to search for companies at the specified level and the ones below it. The restriction here applies to tickets for companies outside the location, as well as members.

IMPORTANT! We strongly recommend that you select the highest level of access (e.g., *Level 1*) to ensure that all companies will sync to the UniView Portal without issue. Selecting a lower level of access may result in some companies not syncing to the UniView Portal.

- Business Unit – Select the member's business unit.
- Name – This field corresponds to the Level field above. After selecting a Level, select a specific name associated with the structure level.
- Default Territory – Select the member's default territory.

Members - API Members > Detail
New Member

< + [Save] [Refresh] [History] [Delete]

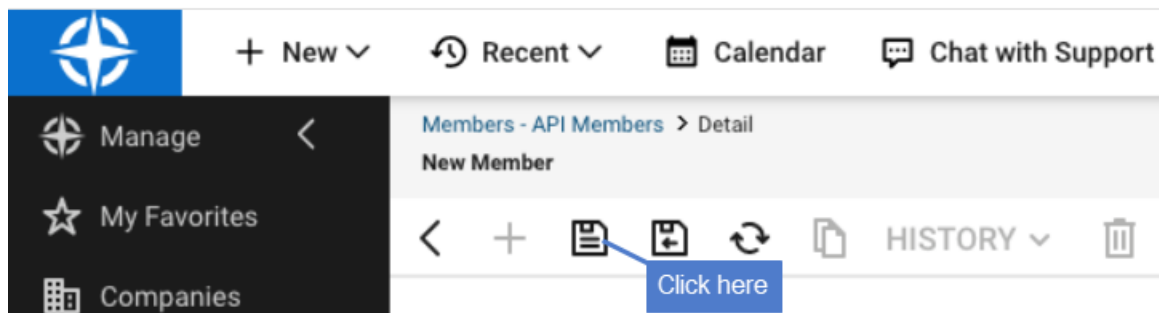
Profile

Member ID* Time Zone*
Member Name* Email

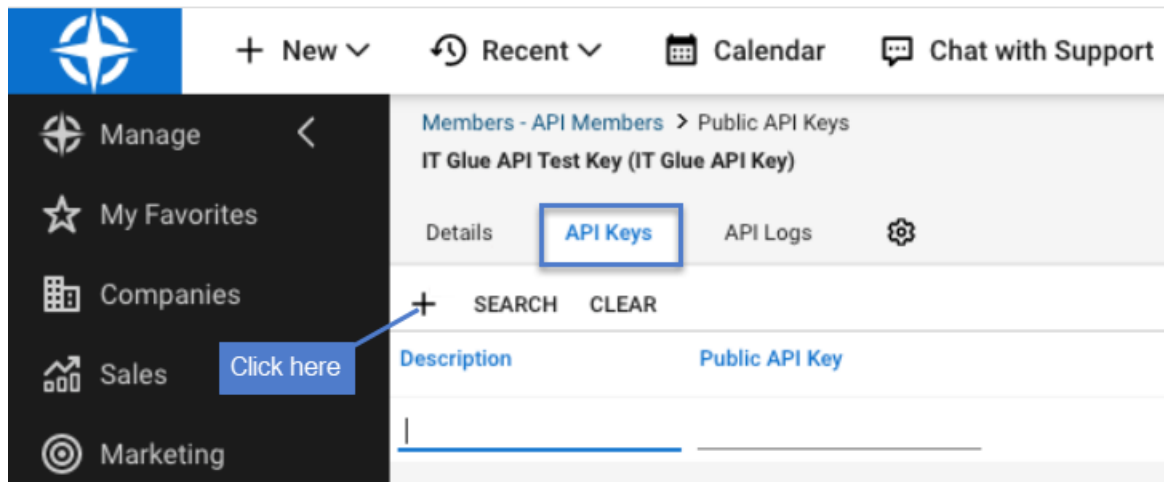
System

Role ID* Location*
Level* Business Unit*
Name* Default Territory*

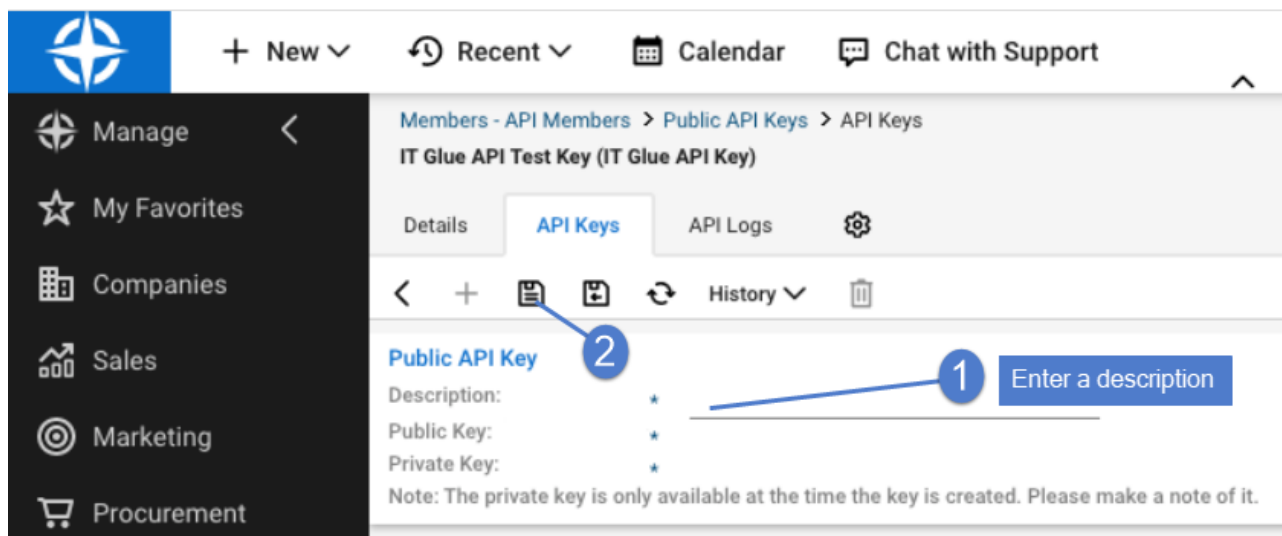
10 In the top menu bar, click the **Save** icon.



11 Click the **API Keys** tab and then on the plus icon (+).

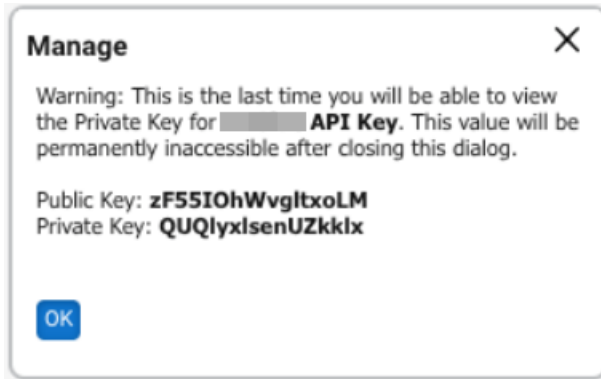


- 12 Enter a description of the key (e.g., *UniView Portal*) and click the **Save** icon.




The public and private keys are generated. Note the Public and Private Keys. You will enter these in the "[Step 2: Add the ConnectWise Manage integration](#)" procedure.

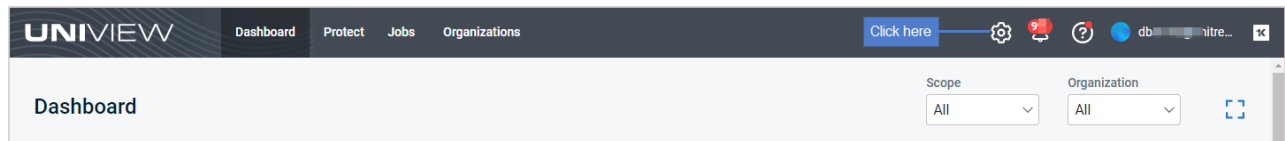
IMPORTANT! Keep the private key in a secure location. The key will not be visible again after closing the window.



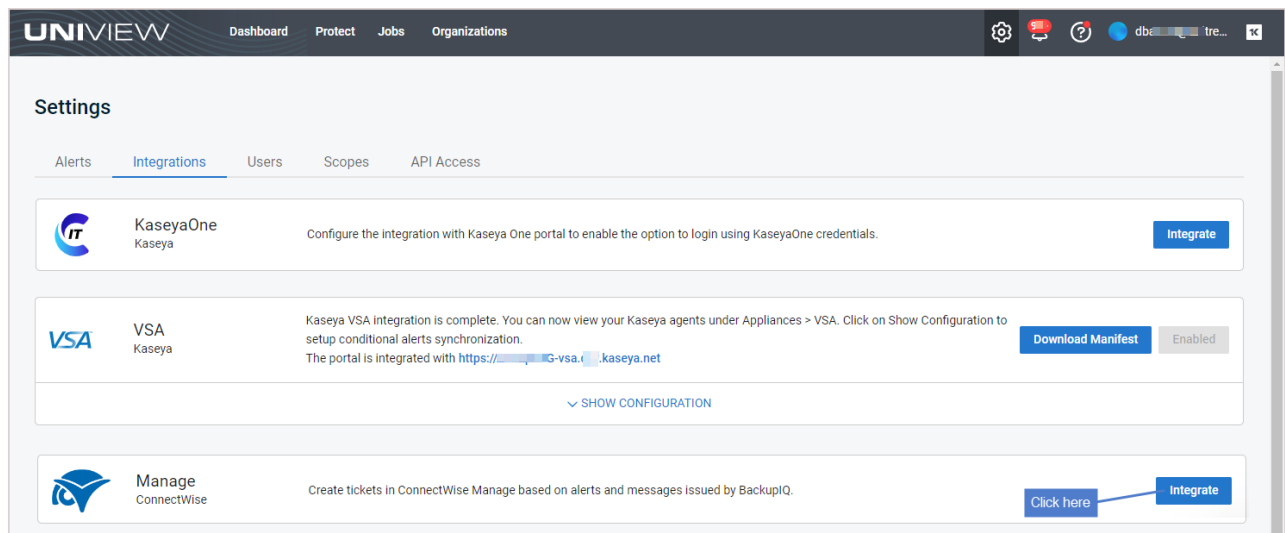
Step 2: Add the ConnectWise Manage integration

Note: During this procedure you will select a company, service board, and priority level for alerts. These selections are applied to all ConnectWise organizations by default. If needed, you can modify these settings. (For details, see "Integrating ConnectWise Manage" for details.)

- 1 Log in to the UniView Portal with a superuser account.
- 2 Click :

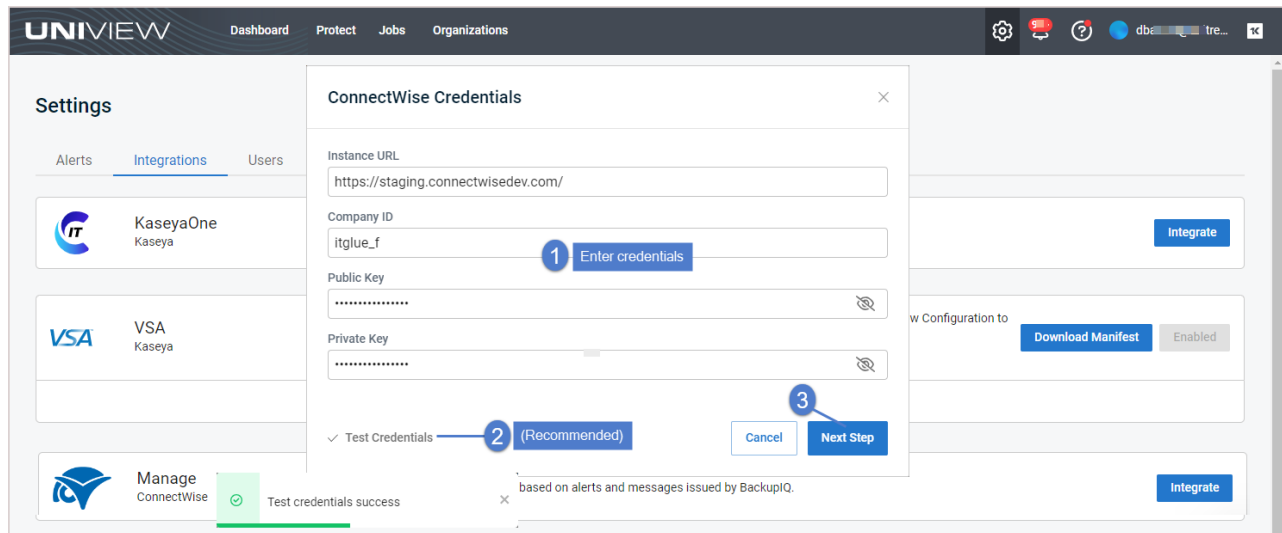


- 3 Select the **Integrations** view.
- 4 Locate the ConnectWise Manage integration and click **Integrate**:



- 5 Enter the ConnectWise **Instance URL** and **Company ID**. Enter the **Public Key** and **Private Key** that you generated in the "Step 1: Add a security role to ConnectWise" procedure above.

- 6 (Recommended) Click **Test Credentials** to verify that UniView Portal can connect to ConnectWise Manage.
- 7 Click **Next Step**.



- 8 Select a company and service board.
 - The service board you select is the location where BackupIQ tickets will be created in ConnectWise Manage.
 - The drop-down lists contain all companies and service boards assigned to the UniView Portal account. (If needed, you can use ConnectWise Manage to add a new company and service board to use for BackupIQ tickets.)
 - You can switch to another service board or company at any time by editing these settings (see "[Integrating ConnectWise Manage](#)").
- 9 (Optional) BackupIQ dismisses offline appliance alerts and conditional alarms automatically when the alert condition has been resolved. You can opt to automatically close corresponding ConnectWise tickets by selecting a status from the Close Ticket Status list. Or select *Do not close automatically*.
- 10 Select a priority level for alerts. Choose from these levels:
 - Do not sync – No ticket is created in ConnectWise Manage
 - Priority 1 – Emergency Response
 - Priority 2 – Quick Response
 - Priority 3 – Normal Response
 - Priority 4 – Scheduled Maintenance

ConnectWise Integration Settings [Close]

Company: Your Company [v]

Service Board: Professional Services [v]

Close Ticket Status: Closed (resolved) [v]

Select priority for alerts

Alerts: Priority 1 - Emergency Response [v]

Reset For All Organizations Create Test Ticket

Cancel Save

1 Select a company & service board

2 (Optional) To automatically close tickets, select a status from the list

3 Select priority level for alerts

11 (Recommended) Click **Create Test Ticket**. Go to ConnectWise Manage to view the test ticket.

ConnectWise Integration Settings [Close]

Company: Your Company [v]

Service Board: Professional Services [v]

Close Ticket Status: Closed (resolved) [v]

Select priority for alerts

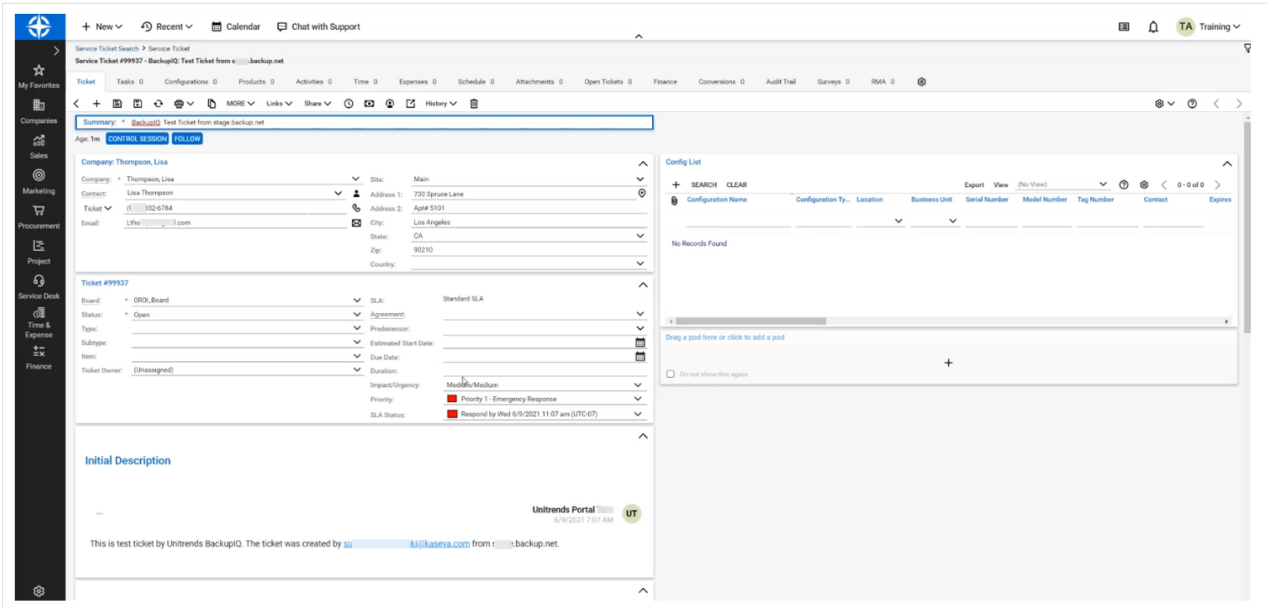
Alerts: Priority 1 - Emergency Response [v]

Reset For All Organizations Create Test Ticket

Cancel Save

(Recommended)
Click to create a test ticket

Sample test ticket in ConnectWise Manage:



12 Click Save.

ConnectWise Integration Settings ✕

Company

Service Board

Close Ticket Status

Select priority for alerts

Alerts

Reset For All Organizations Create Test Ticket

Cancel
Save

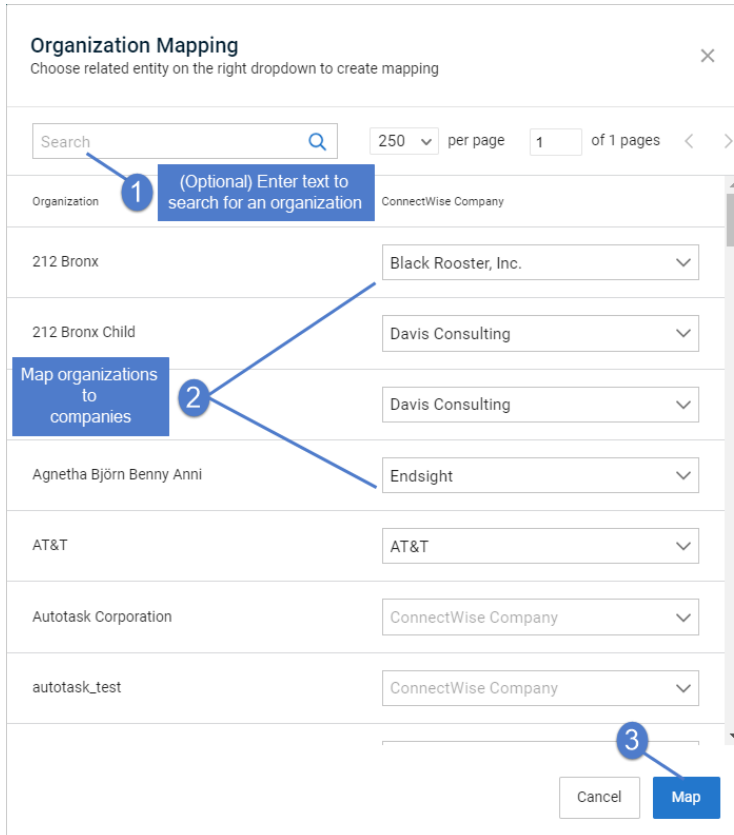
13 Map organizations to ConnectWise companies.

By default, all organizations are mapped to the company you selected above in [step 8](#). If needed, assign organizations to other ConnectWise companies as shown here. Once you've completed your company selections, click **Map**:

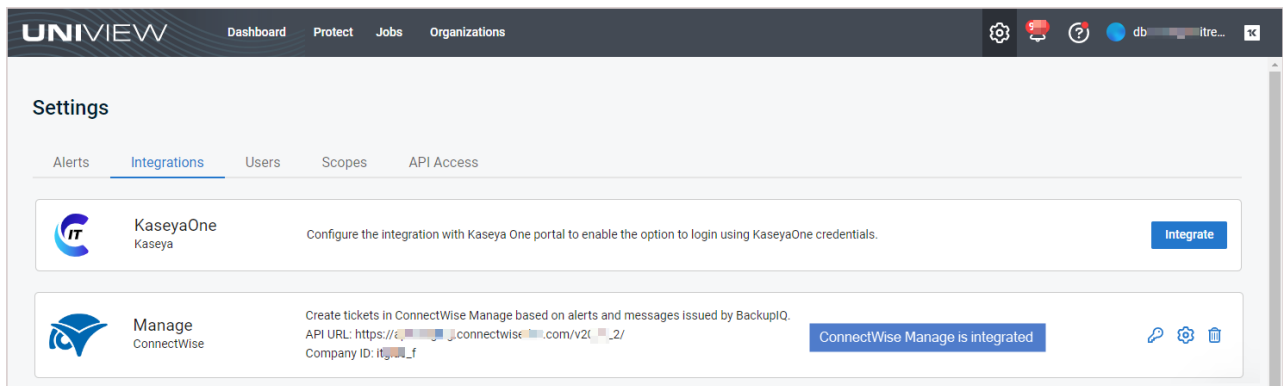
Notes:

If there are no ConnectWise companies in the Organization Mapping dialog, or if you do not see all companies in the drop-down lists:

- 1 Click **Map** to add the integration and exit the dialog.
- 2 Import organizations from ConnectWise as described in "[Integrating ConnectWise Manage](#)".



The integration is added.



Note: ConnectWise tickets are created for all BackupIQ alerts unless you selected *Do not sync* in the ConnectWise Integration Settings Alerts field.

Working with your ConnectWise Manage integration

Working with your ConnectWise Manage integration

Once you've integrated ConnectWise Manage, use these procedures as needed:

- ["To view or modify one organization's ConnectWise Manage settings"](#)
- ["Mapping companies and accounts to organizations"](#)

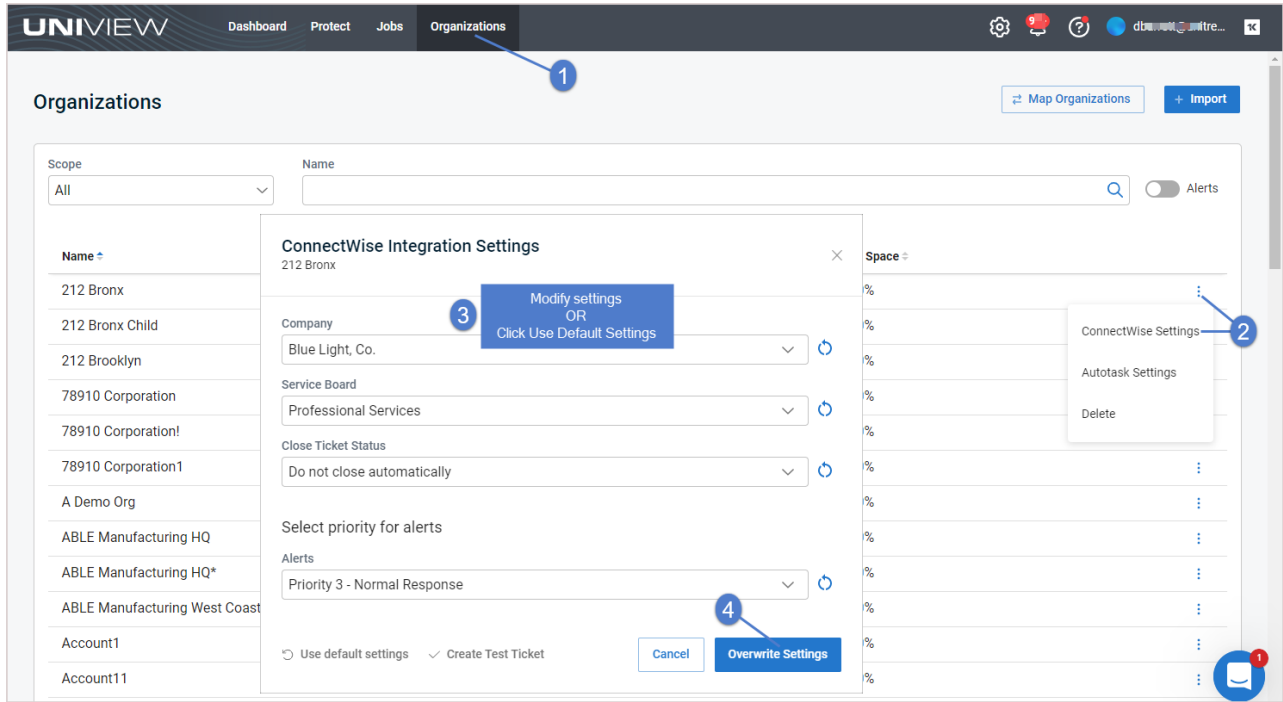
Note: The procedures below can be run only by users that have the superuser role.

- ["To view or modify ConnectWise Manage integration settings"](#)
- ["To apply default integration settings to all ConnectWise organizations"](#)
- ["To remove the ConnectWise Manage integration"](#)


To view or modify one organization's ConnectWise Manage settings

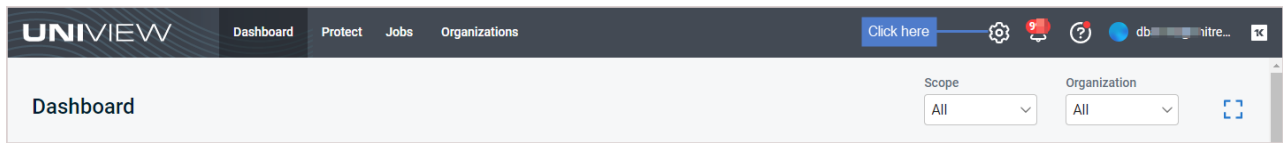
By default, the integration's company, service board, close ticket status, and alert priority settings are applied to all ConnectWise Manage organizations. If needed, you can use this procedure to apply different settings to an organization or to re-apply the default settings to an organization whose settings you have modified.



- 1 Log in to the UniView Portal.
- 2 Select **Organizations**.
- 3 Locate the organization. Click **:** and select **ConnectWise Settings**.
- 4 (Optional) Do one of the following:
 - Modify settings and click **Overwrite Settings** to apply your changes.
 - To re-apply the defaults to this organization, click **Use Default Settings**, then click **Overwrite Settings** to apply your changes.

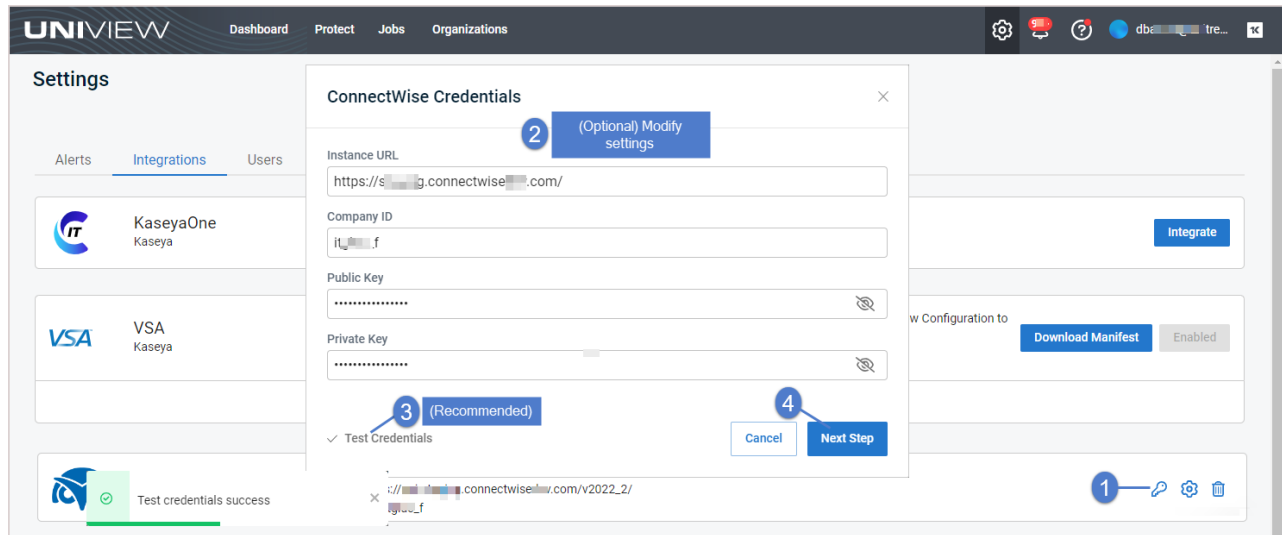


To view or modify ConnectWise Manage integration settings

- 1 Log in to the UniView Portal with a superuser account.
- 2 Click :

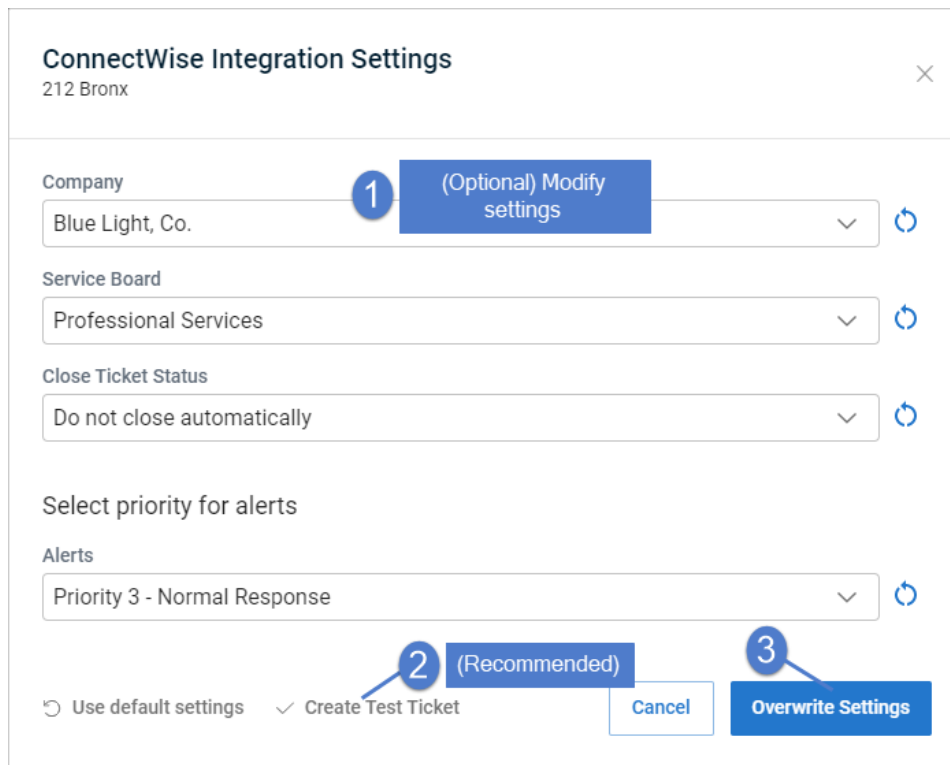


- 3 Select the **Integrations** view.
- 4 Locate the ConnectWise Manage integration and click .
- 5 (Optional) To view the Public and Private keys, click the  icons.
- 6 (Optional) Modify credentials settings. Click **Test Credentials** to verify that UniView Portal can connect to ConnectWise Manage.
- 7 Click **Next Step**.

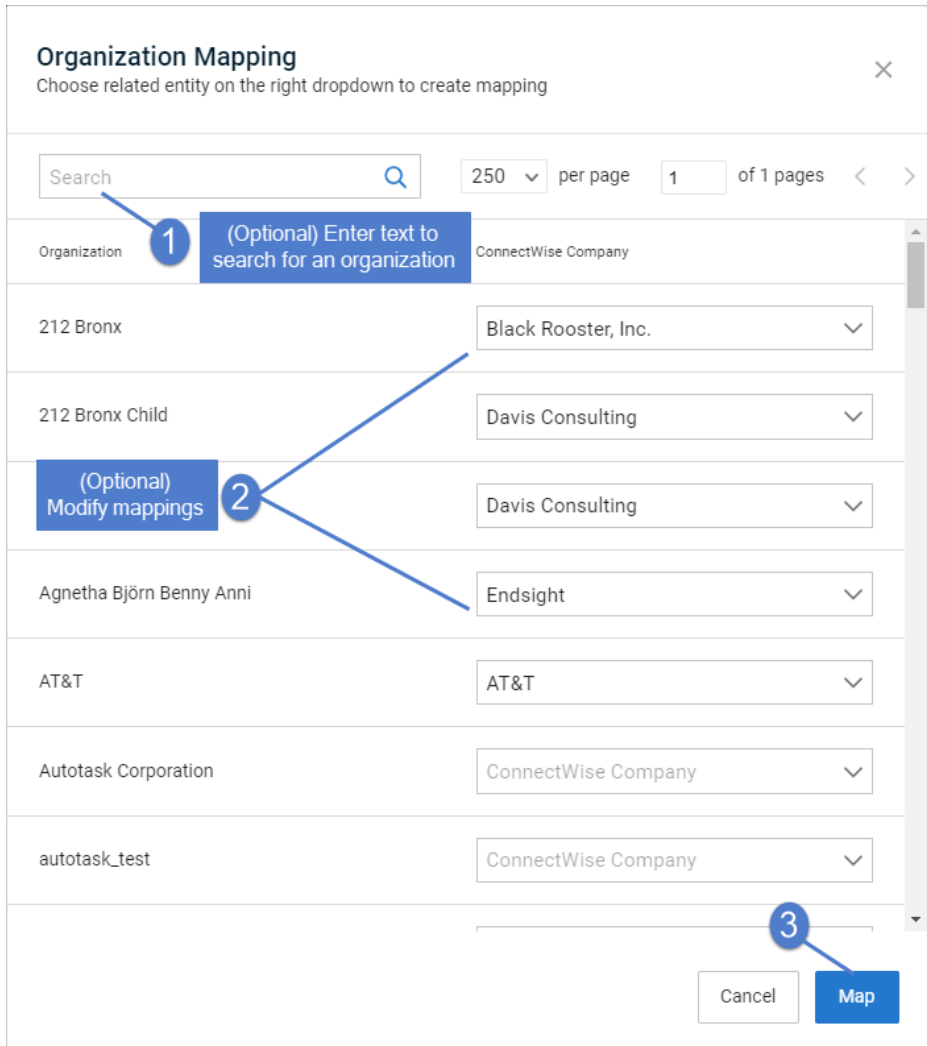


8 (Optional) Modify integration settings.

9 Click **Overwrite Settings**.




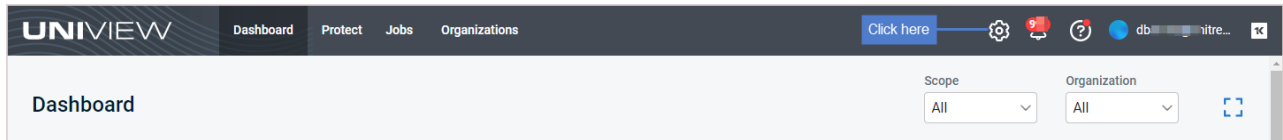
10 (Optional) Modify mappings and click **Map**.




To apply default integration settings to all ConnectWise organizations

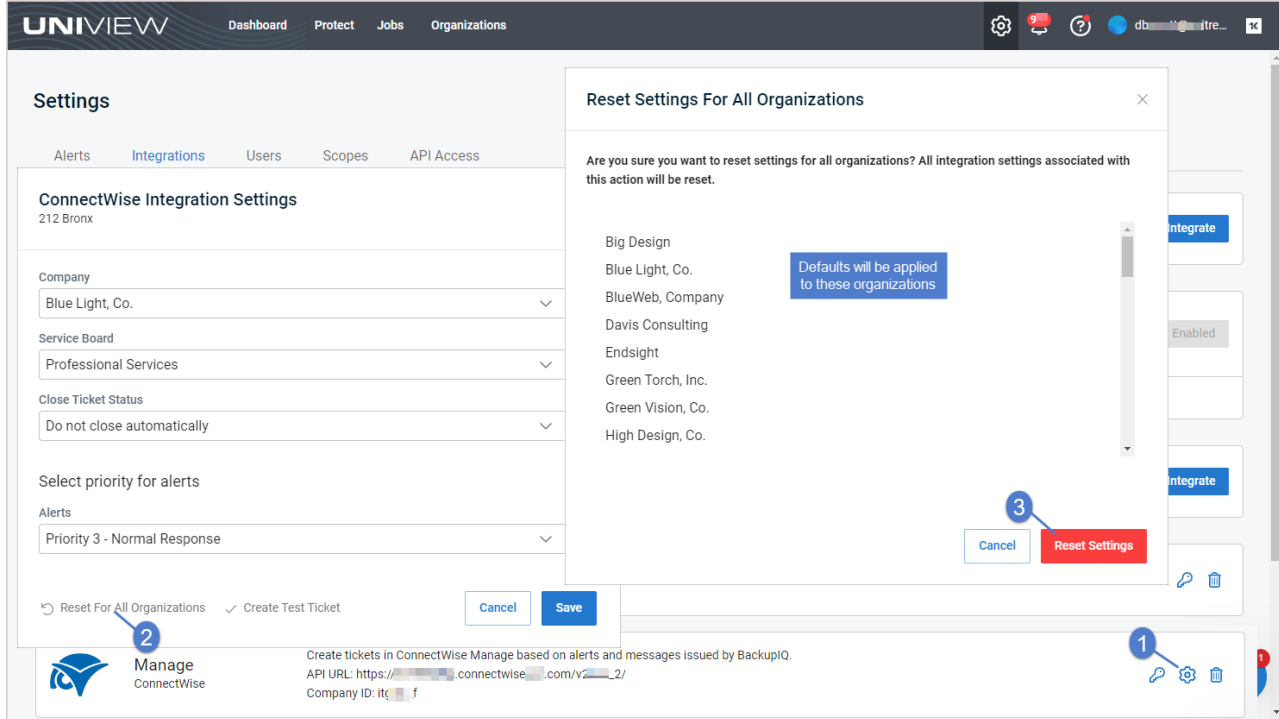
By default, the integration's company, service board, and alert priority settings are applied to all organizations. If you have applied custom settings to organizations (as described in "To view or modify one organization's ConnectWise Manage settings"), you can use this procedure to re-apply the integration's default settings to all organizations.

- 1 Log in to the UniView Portal with a superuser account.
- 2 Click :



- 3 Select the **Integrations** view.


- 4 Locate the ConnectWise Manage integration and click .
- 5 Click **Reset for All Organizations**.
- 6 Review the list of organizations whose settings will be reset. Click **Reset Settings**.

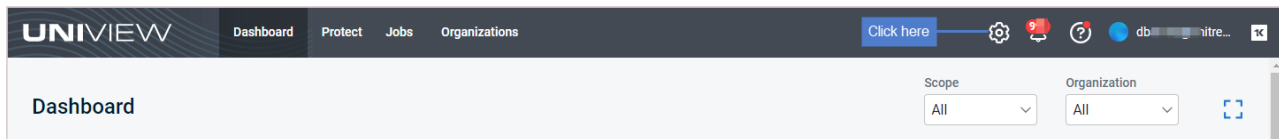


The screenshot shows the UniView Portal interface. The main content area is titled "Settings" and has tabs for Alerts, Integrations, Users, Scopes, and API Access. The "Integrations" tab is active, showing "ConnectWise Integration Settings" for "212 Bronx". The settings include fields for Company (Blue Light, Co.), Service Board (Professional Services), Close Ticket Status (Do not close automatically), and Select priority for alerts (Priority 3 - Normal Response). At the bottom of the settings, there are checkboxes for "Reset For All Organizations" (checked) and "Create Test Ticket". A "Save" button is visible. A modal dialog titled "Reset Settings For All Organizations" is open, asking for confirmation to reset settings for all organizations. The dialog lists several organizations: Big Design, Blue Light, Co., BlueWeb, Company, Davis Consulting, Endsight, Green Torch, Inc., Green Vision, Co., and High Design, Co. A blue box indicates "Defaults will be applied to these organizations". The dialog has "Cancel" and "Reset Settings" buttons. A red "Reset Settings" button is highlighted with a blue circle and the number 3. A blue circle with the number 1 points to the gear icon in the top right corner of the settings page. A blue circle with the number 2 points to the "Reset For All Organizations" checkbox.


To remove the ConnectWise Manage integration

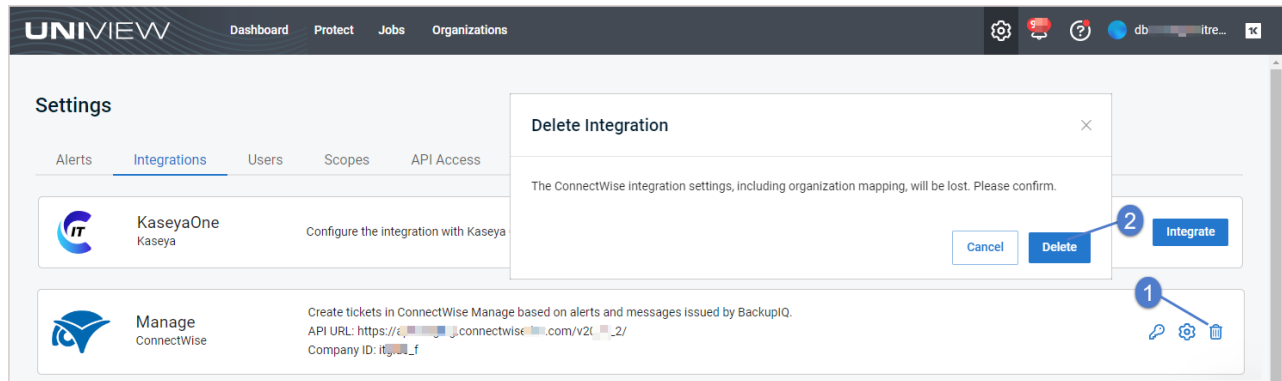
Use this procedure to remove the ConnectWise Manage integration from the UniView Portal.

- 1 Log in to the UniView Portal with a superuser account.
- 2 Click :



The screenshot shows the UniView Portal Dashboard. The top navigation bar includes "Dashboard", "Protect", "Jobs", and "Organizations". A "Click here" button is visible next to the gear icon. The main content area is titled "Dashboard" and has dropdown menus for "Scope" (All) and "Organization" (All). A blue circle with the number 1 points to the gear icon in the top right corner of the dashboard.

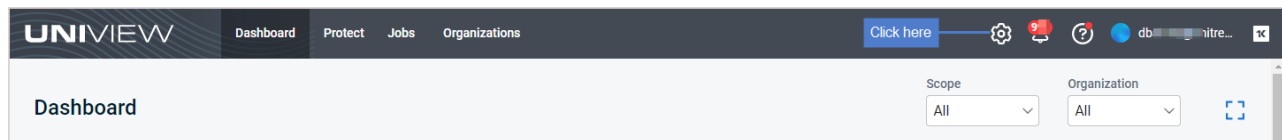
- 3 Select the **Integrations** view.
- 4 Locate the ConnectWise Manage integration and click .
- 5 Click **Delete**. The integration and any organization mappings are removed.



Integrating Kaseya's Billing Management System (BMS) or Vorex

Use this procedure to integrate BMS or Vorex with the UniView Portal. Once you have configured the integration, BMS or Vorex creates tickets based on alerts and warnings issued by BackupIQ.

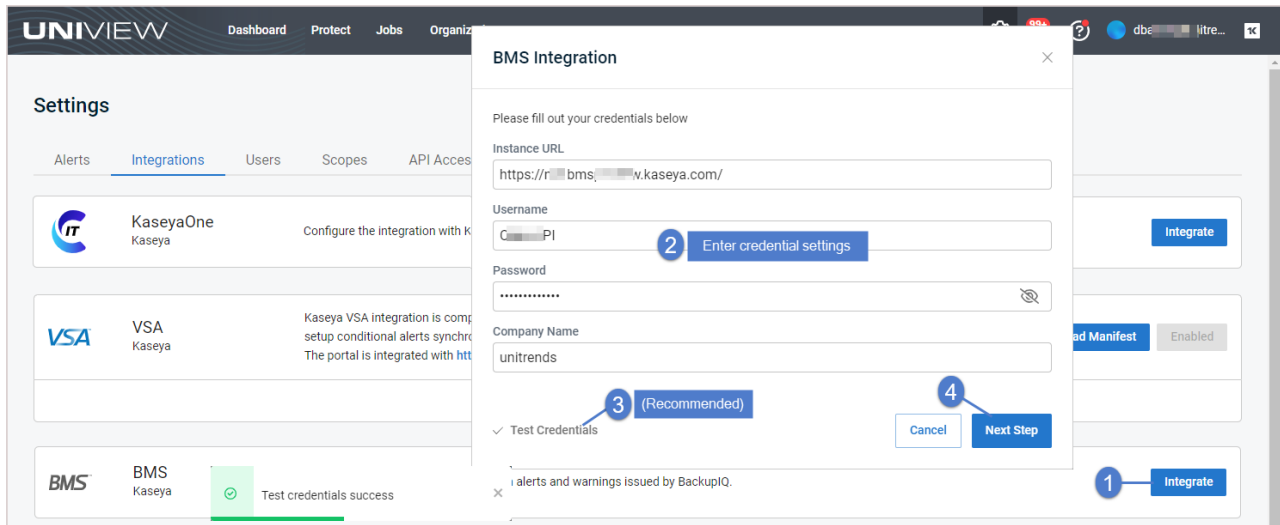
- 1 Log in to the UniView Portal with a superuser account.
- 2 Click your user name and select **My Settings**:



- 3 Select the **Integrations** view.
- 4 Locate the BMS or Vorex integration and click **Integrate**.
- 5 Enter the URL of your BMS or Vorex instance.
- 6 Enter the **Username** and **Password** of a BMS or Vorex Administrator account or the BMS or Vorex API user account.

IMPORTANT! If two-factor authentication is enabled in your environment, you must enter the username and password of the BMS or Vorex API user account.

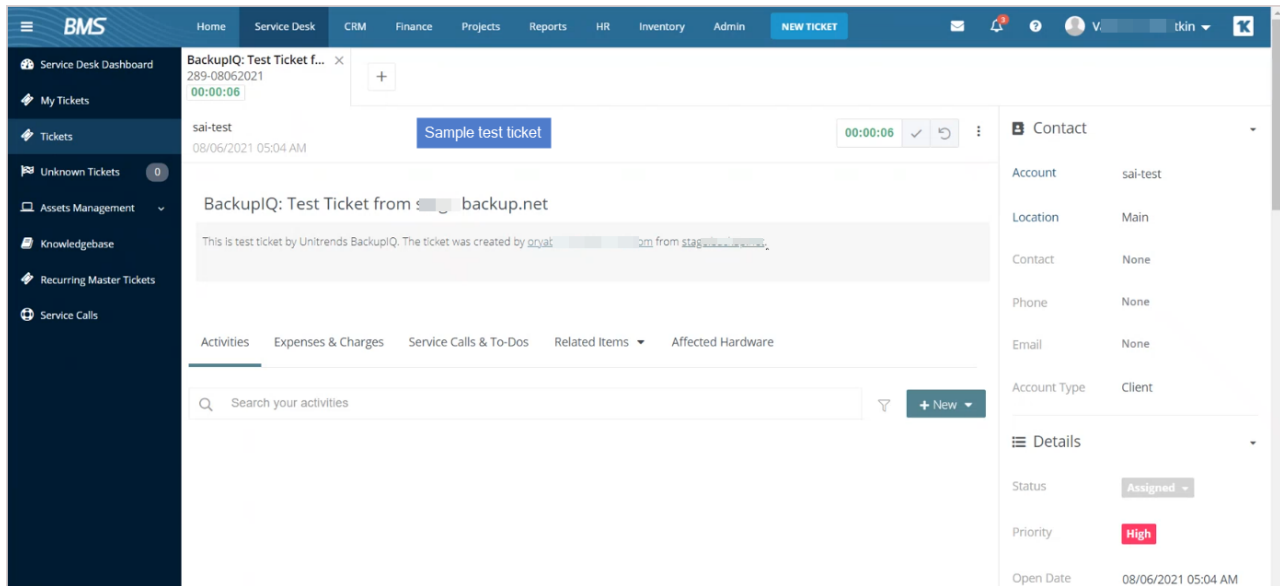
- 7 Enter a company name.
- 8 Click **Test Credentials** to verify the credentials you entered.
- 9 Click **Next Step**.



- 10 Configure integration settings by selecting an Account, Location, Queue, Status, Type, and Source.
- 11 (Optional) BackupIQ dismisses offline appliance alerts and conditional alarms automatically when the alert condition has been resolved. You can opt to automatically close corresponding BMS or Vorex tickets by selecting a status from the Close Ticket Status list. Or select *Do not close automatically*.
- 12 Select a priority level for alerts. Choose from these levels:
 - Do not sync – No ticket is created in BMS or Vorex
 - High
 - Low
 - Medium
 - Very High
- 13 (Optional) Click **Create Test Ticket**. View the test ticket in BMS or Vorex under **Tickets > Service Desk** (see "Sample BMS test ticket:" below).
- 14 Click **Save**.

The screenshot shows the 'BMS Integration Settings' form. It contains several dropdown menus: Account (212 Bronx), Location (Main), Queue (Level Four Support), Status (Assigned), Type (Change Request), Source (Chat), Close Ticket Status (Completed), and Alerts (High). At the bottom, there are checkboxes for 'Reset For All Organizations' and 'Create Test Ticket' (with a blue callout '2' and '(Optional)') and 'Cancel' and 'Save' buttons (with a blue callout '3'). A blue callout '1' points to the 'Type' dropdown menu.

Sample BMS test ticket:



15 Map organizations to BMS or Vorex accounts.

By default, all organizations are mapped to the account you selected above in [step 10](#). If needed, assign organizations to other BMS or Vorex accounts as shown here. Once you've completed your account selections, click **Map**:

Notes:

If there are no BMS or Vorex accounts in the Organization Mapping dialog, or if you do not see all accounts in the drop-down lists:

- 1 Click **Map** to add the integration and exit the dialog.
- 2 Import organizations from BMS or Vorex as described in "[Importing organizations from Autotask, ConnectWise Manage, BMS, or Vorex](#)".

Organization Mapping ✕
Choose related entity on the right dropdown to create mapping

Search 250 per page 1 of 1 pages < >

Organization	BMS Account
212 Bronx	212 Bronx
212 Bronx Child	212 bronx child
Map organizations to BMS accounts 1	BMS Account
Agnetha Björn Benny Anni	BMS to VSA
AT&T	Kaseya
Autotask Corporation	BMS Account
autotask_test	BMS Account


2

The integration is added.


UNIVIEW Dashboard Protect Jobs Organizations ⚙️ 9:10 🔄 🔍 db: inire... 🗑️

Settings

Alerts Integrations Users Scopes API Access


 **KaseyaOne**
Kaseya

Configure the integration with Kaseya One portal to enable the option to login using KaseyaOne credentials.

 **VSA**
Kaseya

Kaseya VSA integration is complete. You can now view your Kaseya agents under Appliances > VSA. Click on Show Configuration to setup conditional alerts synchronization.
The portal is integrated with [https://\[redacted\]-vsa.c\[redacted\].kaseya.net](https://[redacted]-vsa.c[redacted].kaseya.net)

[SHOW CONFIGURATION](#)

 **BMS**
Kaseya

Create tickets in Kaseya BMS based on alerts and warnings issued by BackupIQ.
API URL: [https://ne\[redacted\]bms\[redacted\].kaseya.com/](https://ne[redacted]bms[redacted].kaseya.com/)
Username:
Company Name: unitrends

- 3 After you have completed the step above, tickets are added to the BMS or Vorex queue as new BackupIQ alerts are generated.

Note: BMS or Vorex tickets are created for all BackupIQ alerts unless you selected *Do not sync* in the Integration Settings Alerts field.

Working with your BMS or Vorex integration

Once you've integrated BMS or Vorex, use these procedures as needed:

- ["To view or modify one organization's BMS or Vorex integration settings"](#)
- ["Mapping companies and accounts to organizations"](#)

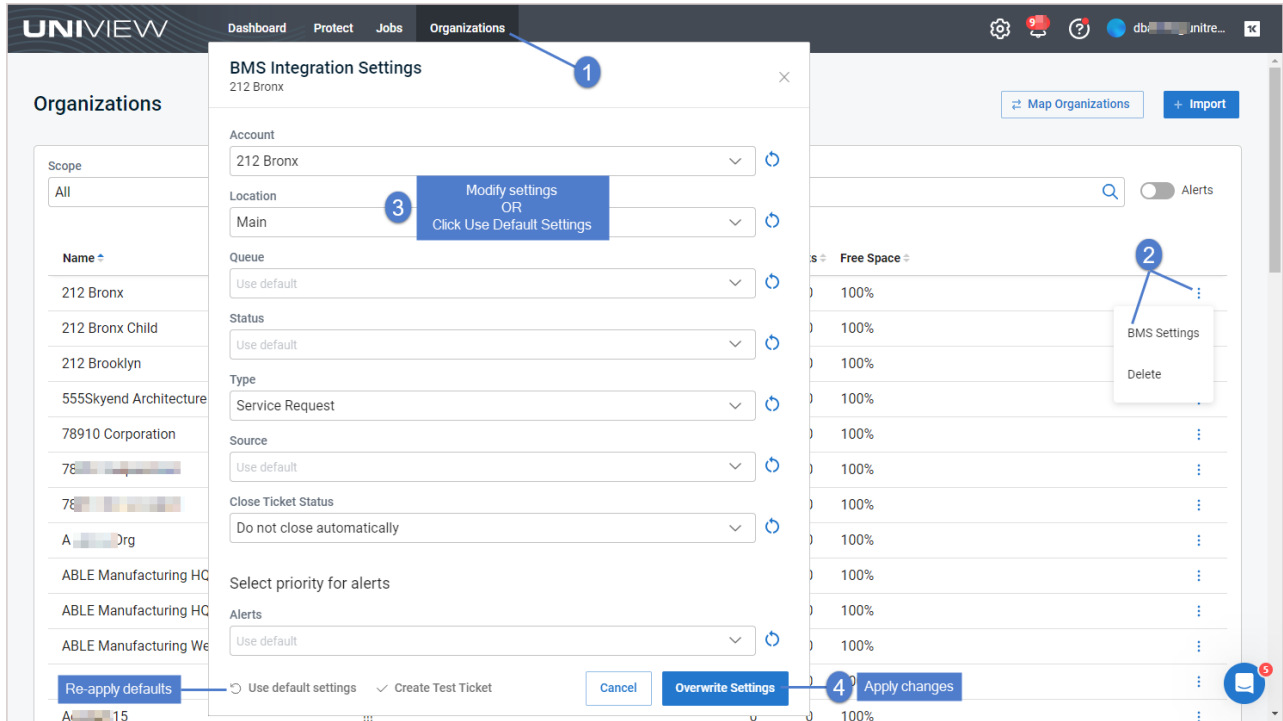
Note: The procedures below can be run only by users that have the superuser role.

- ["To view or modify BMS or Vorex integration settings"](#)
- ["Working with your BMS or Vorex integration"](#)
- ["To set up integrated customer billing for Spanning Microsoft 365 and Spanning Google Workspace"](#)
- ["To remove the BMS or Vorex integration"](#)


To view or modify one organization's BMS or Vorex integration settings

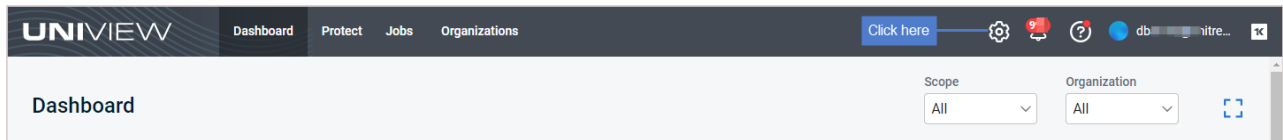
By default, the integration's account, location, queue, status, type, source, and alert priority settings are applied to all organizations. If needed, you can use this procedure to apply different settings to an organization or to re-apply the default settings to an organization whose settings you have modified.



- 1 Log in to the UniView Portal.
- 2 Select **Organizations**.
- 3 Locate the organization. Click **:** and select **BMS Settings** or **Vorex Settings**.
- 4 (Optional) Do one of the following:
 - Modify settings and click **Overwrite Settings** to apply your changes.
 - To re-apply the defaults to this organization, click **Use Default Settings**, then click **Overwrite Settings** to apply your changes.

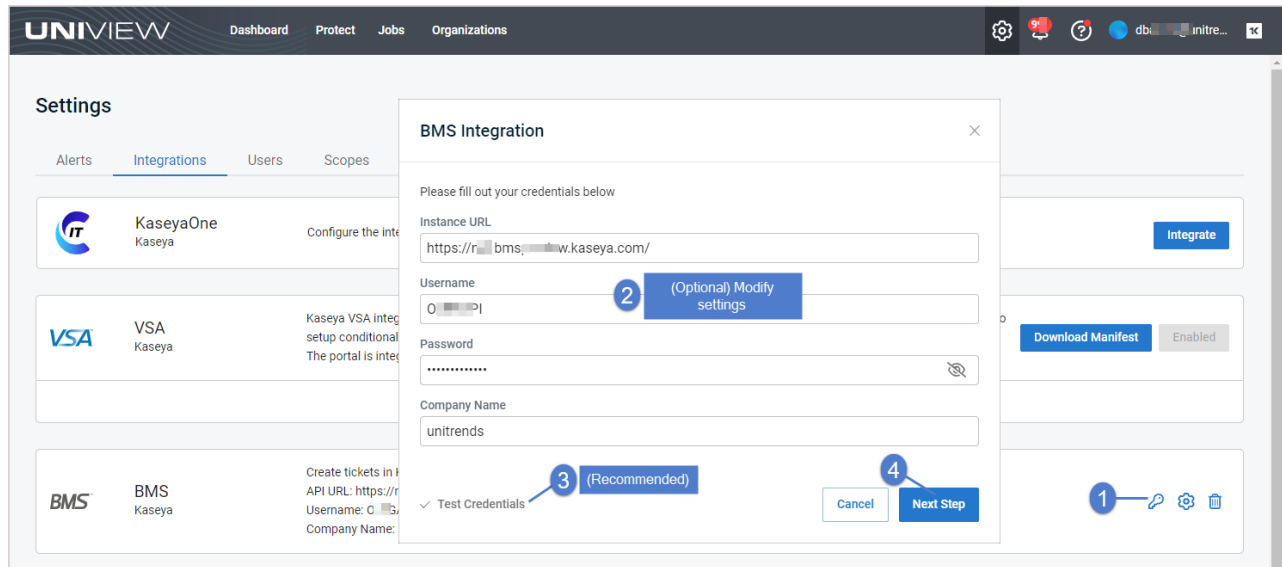


To view or modify BMS or Vorex integration settings

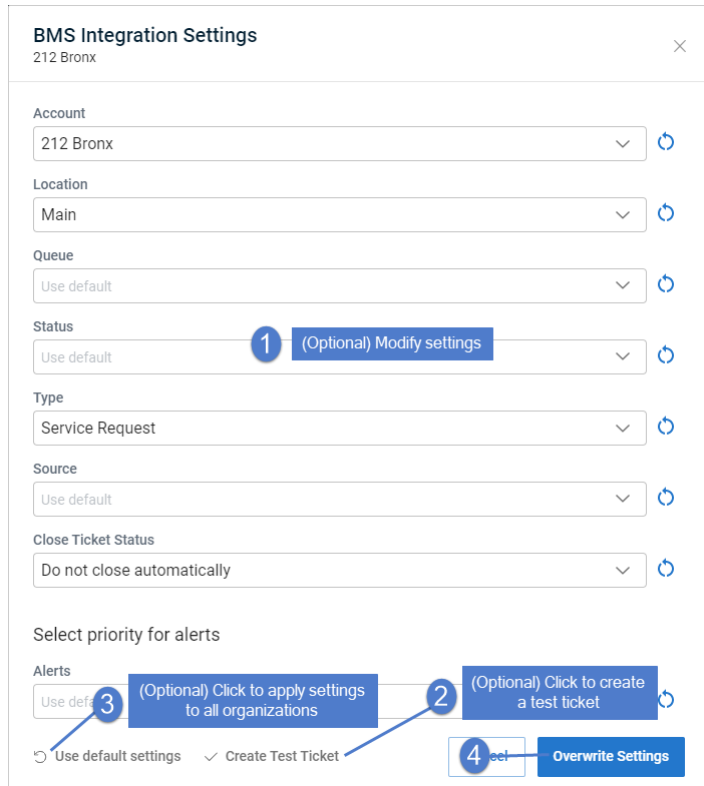
- 1 Log in to the UniView Portal with a superuser account.
- 2 Click :



- 3 Select the **Integrations** view.
- 4 Locate the BMS or Vorex integration and click .
- 5 (Optional) To view the Password, click the .
- 6 (Optional) Modify credentials and URL settings. Click **Test Credentials** to verify that UniView Portal can connect to BMS or Vorex.
- 7 Click **Next Step**.



- 8 (Optional) Modify integration settings.
- 9 (Optional) Click **Create Test Ticket**. View the test ticket in BMS or Vorex under **Tickets > Service Desk**.
- 10 (Optional) To apply these settings to all organizations, click **Reset for All Organizations**. Review the list of organizations whose settings will be reset. Click **Reset Settings**.
- 11 Click **Save**.



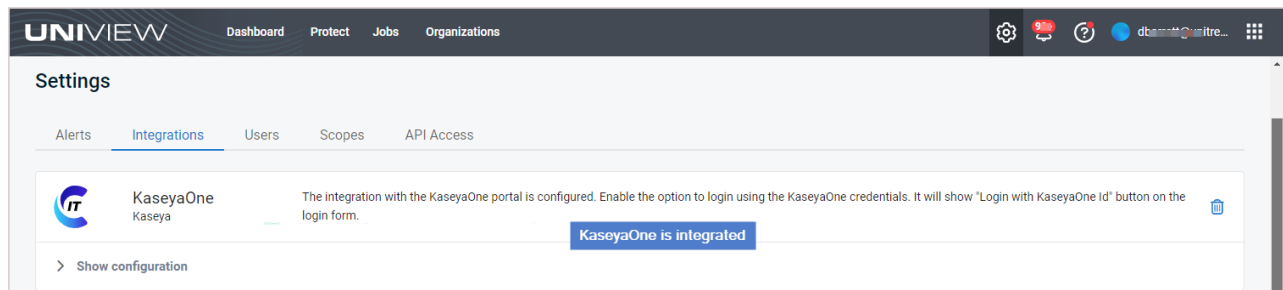
To set up integrated customer billing for Spanning Microsoft 365 and Spanning Google Workspace

Use these procedures to set up integrated customer billing for Spanning Backup for Microsoft 365 and/or Spanning Backup for Google Workspace. These procedures enable you to post the following license information to BMS or Vorex: number of Standard Licenses in Use and number of Archived Licenses, by Spanning tenant or domain. This license data can then be used by BMS or Vorex when generating invoices.

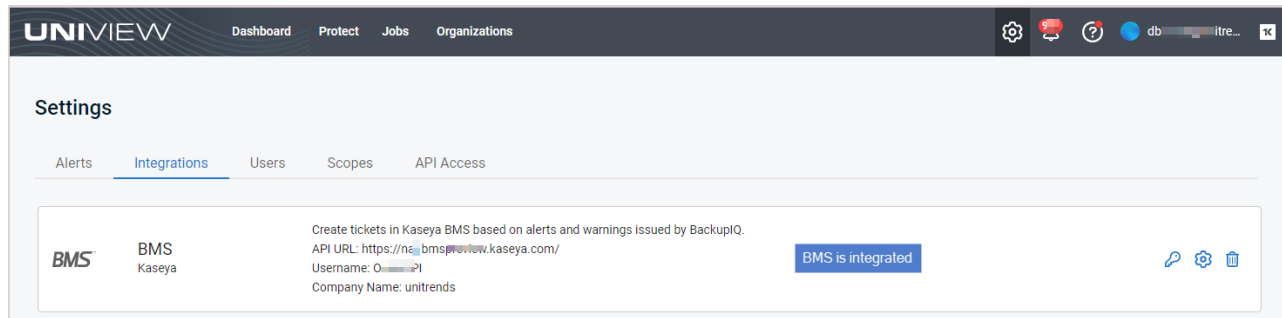
Prerequisites

Ensure that these prerequisites have been met before running the procedures below:

- UniView Portal has been integrated with KaseyaOne. (To add the integration, see "[Integrating KaseyaOne](#)".)



- UniView Portal has been integrated with BMS or Vorex. (To add the integration, see "[Integrating Kaseya's Billing Management System \(BMS\) or Vorex](#)".)



- Your Spanning Backup for Microsoft 365 tenants and/or Google Workspace domains have been integrated with the UniView Portal.
 - To integrated a Microsoft 365 tenant, see "[Integrating a Microsoft 365 tenant](#)".
 - To integrate a Google Workspace domain, see "[Integrating a Google Workspace domain](#)".

Use these procedures to set up integrated customer billing for Spanning Backup Microsoft 365 and Google Workspace domains:

- "[Step 1: Set up organization mapping in UniView](#)"
- "[Step 2: Map the account to the UniView organization in BMS or Vorex](#)"
- "[Step 3: Set up services in BMS or Vorex](#)"

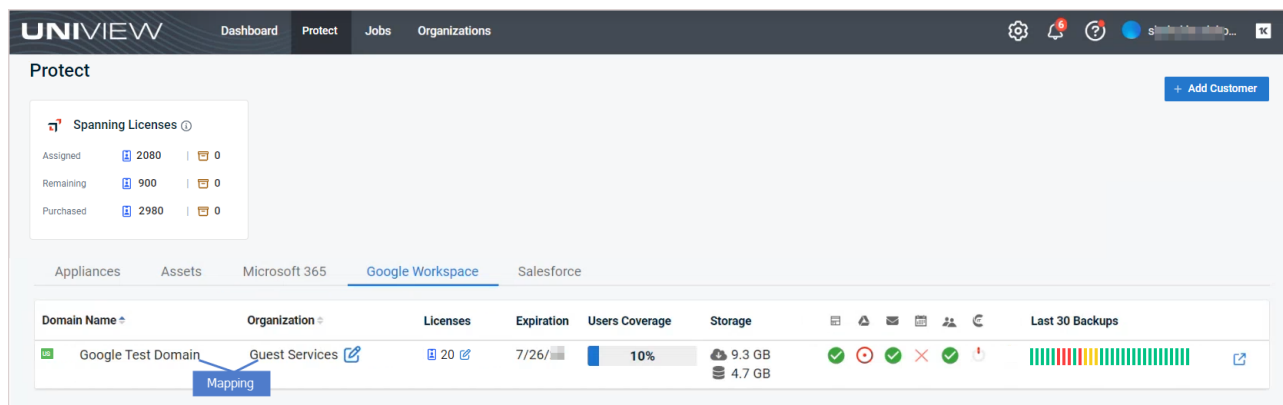
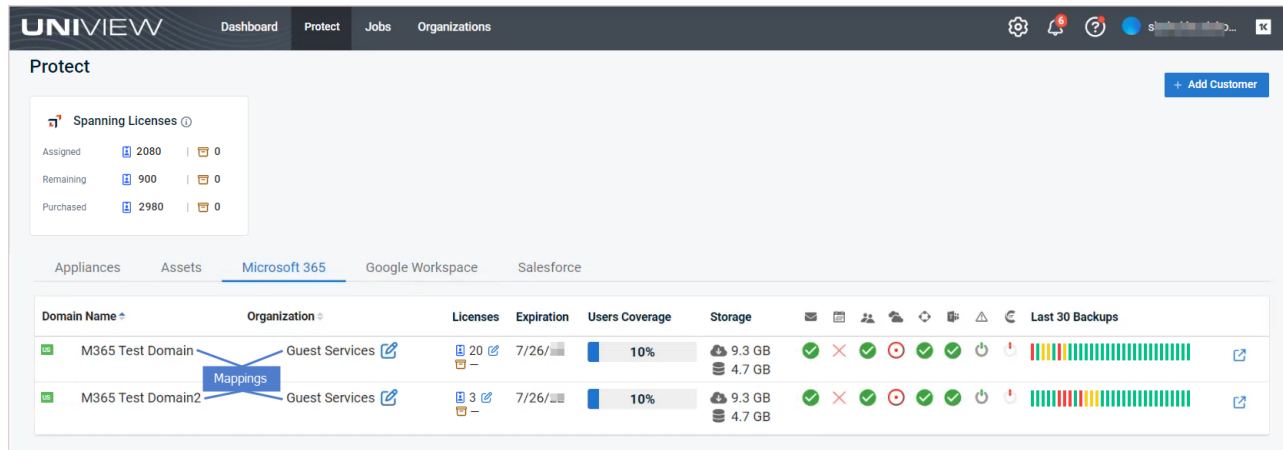
Step 1: Set up organization mapping in UniView

- 1 Log in to the UniView Portal.
- 2 In the Protect > Microsoft 365 or Protect > Google Workspace view, ensure that the Spanning Backup tenants or domains for which you will use integrated customer billing have been mapped to UniView organizations.

Notes: See these procedures to view and modify mappings:

- "[To map Microsoft 365 tenants to organizations](#)"
- "[To map Google Workspace domains to organizations](#)"

In our example, the Microsoft 365 tenants *M365 Test Domain* and *M365 Test Domain2* have been mapped to the UniView *Guest Services* organization, and the Google Workspace domain *Google Test Domain* has been mapped to the UniView *Guest Services* organization:

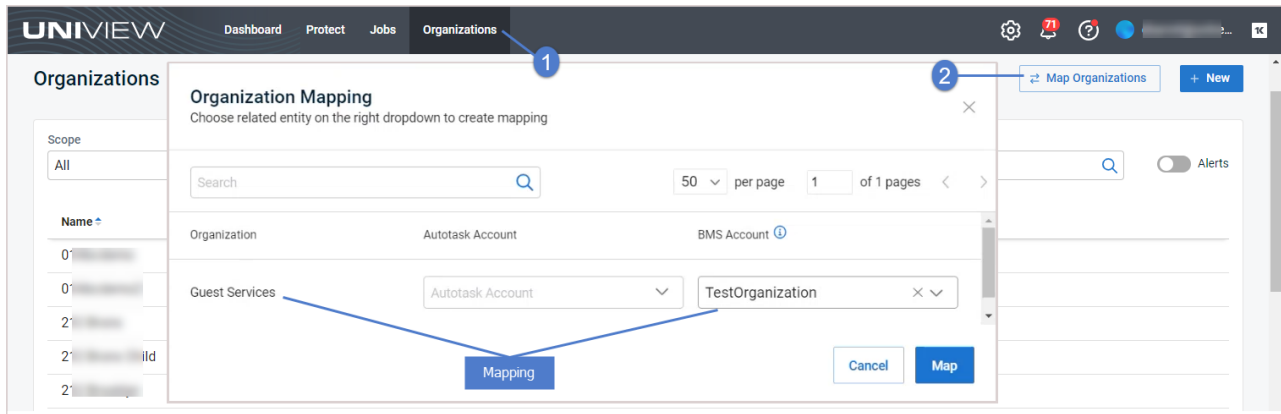


- On the Organizations page, click **Map Organizations** and ensure that the UniView organizations that were mapped to the Spanning tenants or domains in [step 2](#) have also been mapped to BMS or Vorex accounts.

Notes:

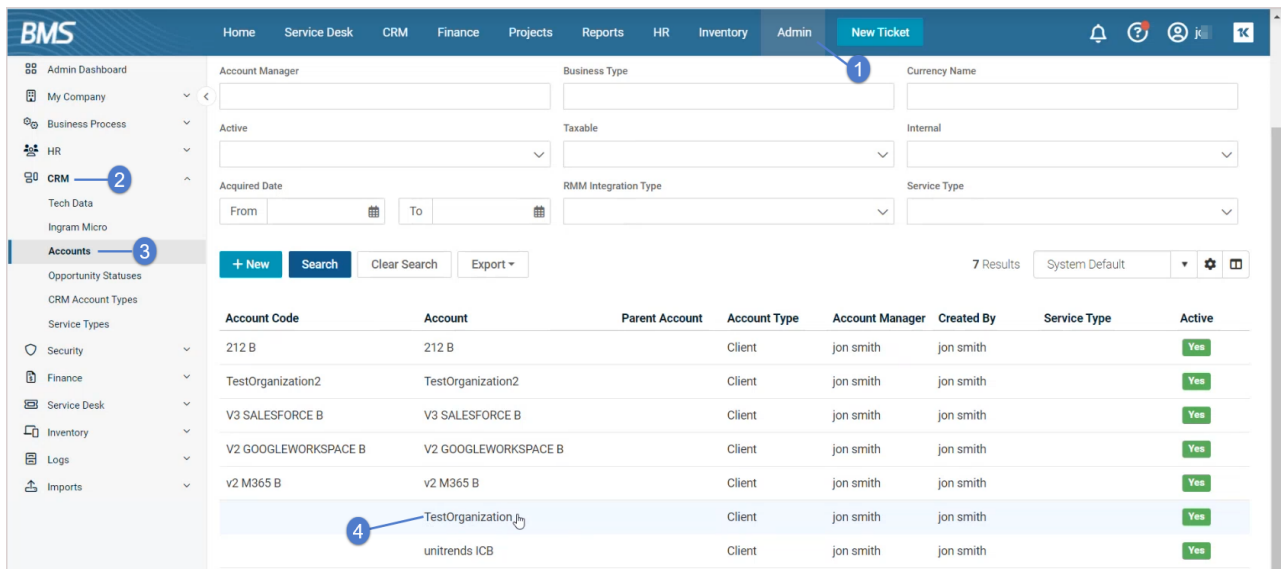
- These conditions must be met to post a Spanning domain's license information to BMS or Vorex: The Spanning tenant or domain is mapped to a UniView organization (in UniView on the Protect > Microsoft 365 or Google Workspace page).
 - The UniView organization that has been mapped to the Spanning domain is also mapped to a BMS or Vorex account in UniView (under Organizations > Map Organizations).
- If you don't see your accounts, import accounts from BMS or Vorex as described in ["Importing Accounts or Companies from your PSA"](#).

In our example, the UniView *Guest Services* organization has been mapped to the BMS *TestOrganization* account:

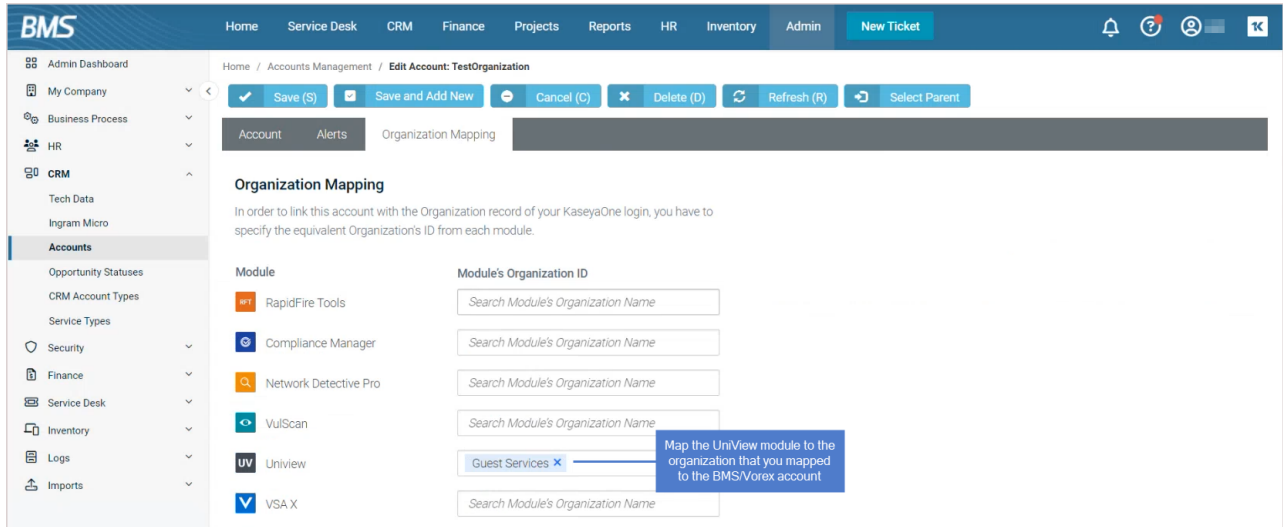


Step 2: Map the account to the UniView organization in BMS or Vorex

- 1 Log in to BMS or Vorex.
- 2 Select **Admin > CRM > Accounts**.
- 3 Scroll down to the accounts list and select the BMS/Vorex account that you mapped in UniView above (*TestOrganization* in our example).

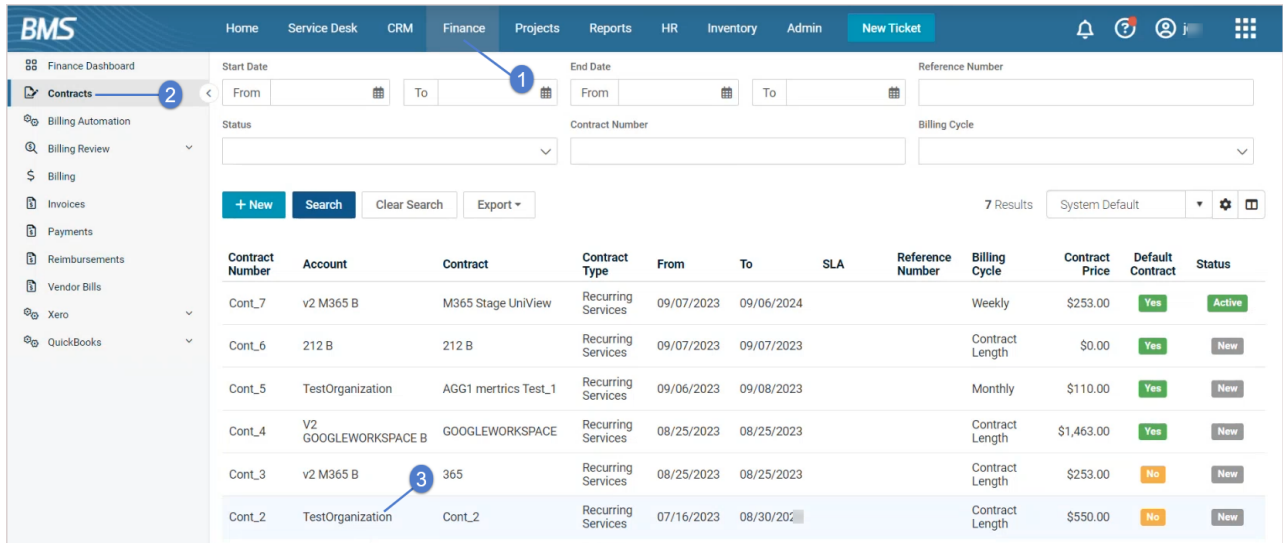


- 4 On the **Organization Mapping** tab, locate the UniView module and map it to the UniView organization that you mapped to BMS/Vorex above (*Guest Services* in our example):



Step 3: Set up services in BMS or Vorex

- 1 In BMS or Vorex, select **Finance > Contracts** and select the contract for the BMS/Vorex account (*Cont_2* for the *TestOrganization* account in our example).




- 2 Scroll down to Billing Information and click **Add**.

The screenshot shows the 'Contracts' configuration page in the BMS UniView Portal. The page is divided into several sections:

- Navigation:** A top navigation bar with tabs for Home, Service Desk, CRM, Finance, Projects, Reports, HR, Inventory, Admin, and New Ticket. A left sidebar menu lists various modules like Finance Dashboard, Contracts, Billing Automation, Billing Review, Billing, Invoices, Payments, Reimbursements, Vendor Bills, Xero, and QuickBooks.
- Contract Details:** A form with fields for Contract Number (Cont_2), Contract Name (Recurring Services), Account (TestOrganization), Start Date (07/16/2023), End Date (08/30/2023), SLA, Billing Cycle, Reference Number, and Billing Information (Contract History, Exclusions, Custom Fields, Attachments, Notifications).
- Contract Billing Price:** A field showing \$550.00.
- Contract Billing Table:** A table with columns: SERVICE NAME, DESCRIPTION, EFFECTIVE DATE, UNITS, DEFAULT UNIT COST, UNIT COST, TOTAL COST, DEFAULT UNIT PRICE, UNIT PRICE, TOTAL PRICE, and SORT ORDER. The table contains one row with ServiceName, ServisDescr, 07/16/2023, 50, \$11.00, \$11.00, \$550.00, \$11.00, \$11.00, \$550.00, and 1.


3 Add the applicable billing service:

- Click **Integrated Customer Billing**.
- Select the **Uniview** Module.
- Select a Billing Type from the list, then click  to load the latest licensing data.
- Modify other options as needed, then click **Save**.

In our example, we selected the *Per Spanning Backup for Microsoft 365 Archived License* service. The archived license total for the Spanning Microsoft 365 domains we mapped to the *TestOrganization* is 200.


4 Repeat step 3 to add other integrated customer billing services.

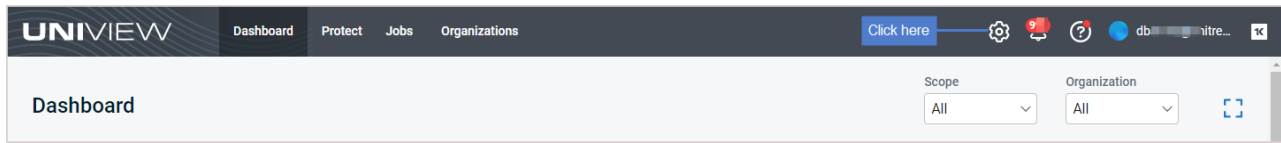
Integrated customer billing is set up for the BMS or Vorex account.


IMPORTANT! Spanning license information is updated nightly. To update Spanning license information in BMS or Vorex, you must open the Add Service or Edit Service dialog and click the  icon next to the Billing Type field.

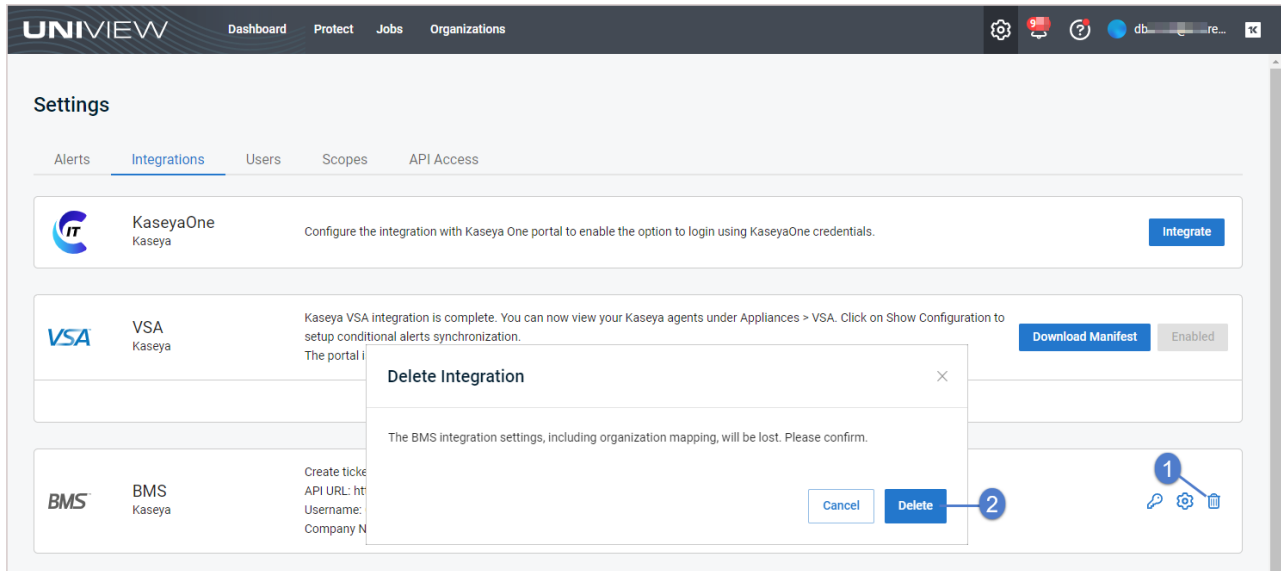
To remove the BMS or Vorex integration

Use this procedure to remove the BMS or Vorex integration from the UniView Portal.

- 1 Log in to the UniView Portal with a superuser account.
- 2 Click :



- 3 Select the **Integrations** view.
- 4 Locate the BMS or Vorex integration and click .
- 5 Click **Delete**. The integration and any organization mappings are removed.



Importing Accounts or Companies from your PSA

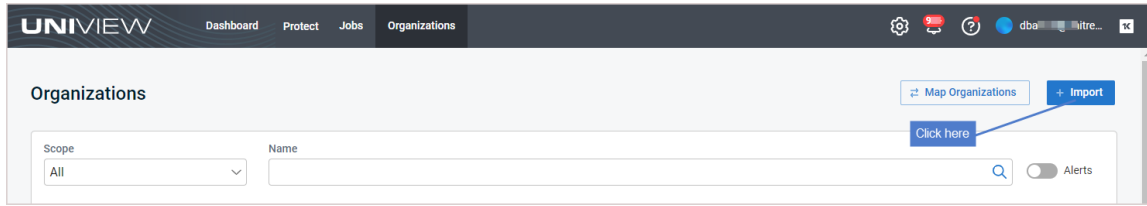
When the PSA integration was added to UniView Portal, existing companies or accounts were automatically imported. As you add new PSA companies or accounts, you will need to manually import them into UniView Portal. To import new accounts or companies, see ["Importing organizations from Autotask, ConnectWise Manage, BMS, or Vorex"](#). To map newly imported companies or accounts to UniView Portal organizations, see ["Mapping companies and accounts to organizations"](#).

Importing organizations from Autotask, ConnectWise Manage, BMS, or Vorex

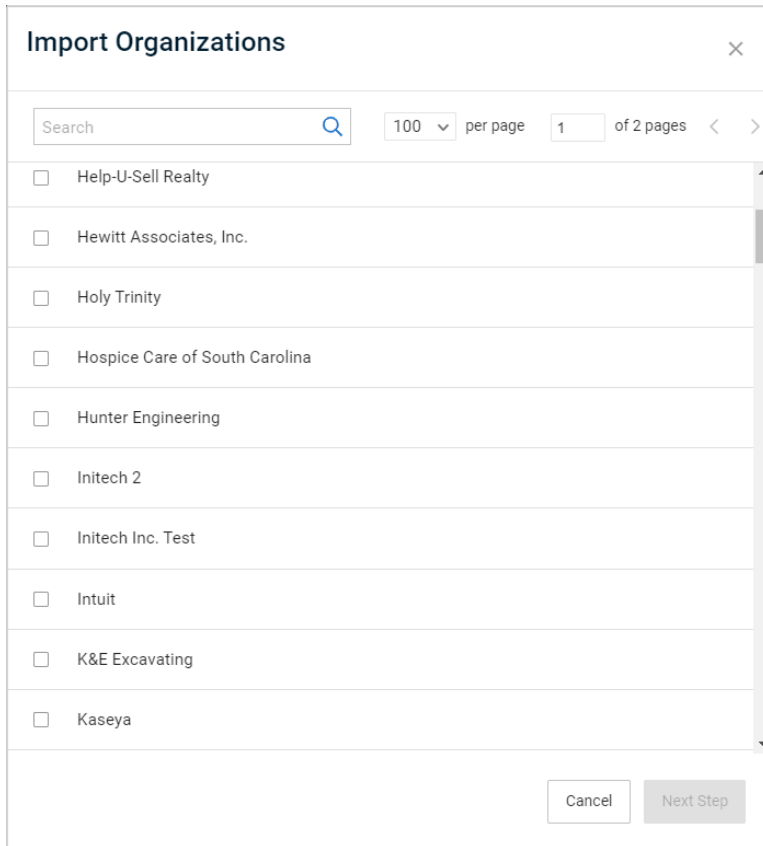
Once accounts or companies have been added to your PSA, use this procedure to import them into the UniView Portal.

To import organizations

- 1 On the Organizations page, click **Import**.



Organizations are imported:



2 Assign organizations to a scope:

Notes:

- A user's scope determines which organizations are visible in the UniView Portal. To ensure that users can only access information about organizations specified in their scope(s), you must assign each organization to a scope.
- In this procedure, the organizations you select are assigned to one scope. Repeat these steps to assign organizations to another scope.

- Check boxes to select organizations. Click **Next Step**.

Import Organizations [Close]

Search [Magnifying Glass] 100 per page 1 of 2 pages [Previous] [Next]

<input type="checkbox"/>	Help-U-Sell Realty
<input type="checkbox"/>	Hewitt Associates, Inc.
<input type="checkbox"/>	Holy Trinity
<input type="checkbox"/>	Hospice Care of South Carolina
<input type="checkbox"/>	Hunter Engineering
<input checked="" type="checkbox"/>	Initech 2
<input checked="" type="checkbox"/>	Initech Inc. Test
<input checked="" type="checkbox"/>	Intuit
<input checked="" type="checkbox"/>	K&E Excavating
<input type="checkbox"/>	Kaseya

[Cancel] [Next Step]

- Select a scope from the list. Click **Save**.

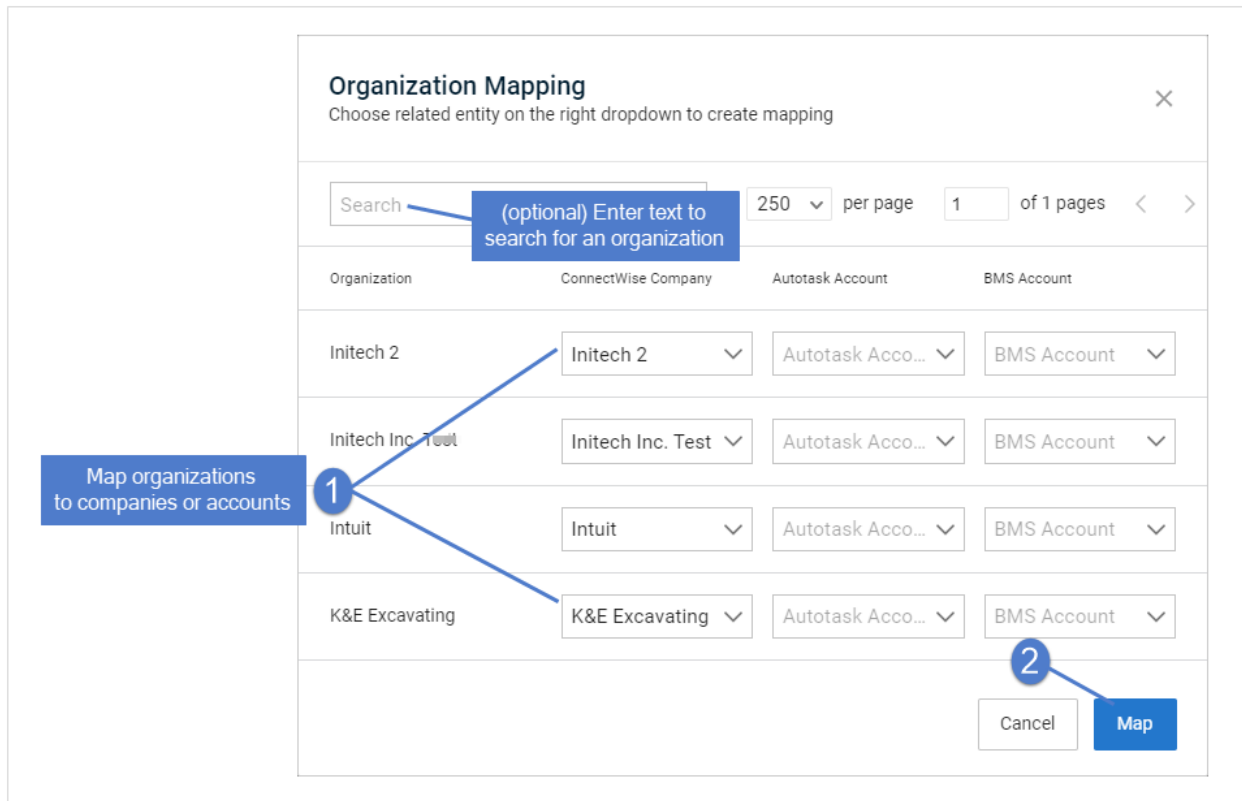
← Import Organizations [Close]

Scope *

My Scope [Down Arrow]

[Cancel] [Save]

- 3 Map organizations to companies or accounts. Click **Map**.



Mapping companies and accounts to organizations

By default, the integration's company or account is applied to all of its organizations. Use this procedure to quickly apply different companies or accounts to multiple organizations.

To map companies and accounts to organizations

- 1 Log in to the UniView Portal.
- 2 Select **Organizations**.
- 3 Click **Map Organizations**.
- 4 (Optional) Filter the organization list by entering a text string in the Search field.
- 5 Select a different company or account for one or more organizations.

Note: In the figure below, ConnectWise, Autotask, BMS, and Endpoint Backup integrations have been configured for this UniView Portal instance. If you do not see an integration, it has not been added to your UniView Portal instance.

- 6 Click **Map**.

The screenshot shows the UniView Portal interface with the 'Organizations' tab selected. A modal window titled 'Organization Mapping' is open, displaying a table for mapping UniView organizations to external systems. The table has columns for 'Organization', 'ConnectWise Company', 'Autotask Account', 'BMS Account', and 'Endpoint Backup Organization'. A callout box with the text 'Map organizations to PSA accounts' points to a button in the left sidebar of the modal. Other callouts (1, 2, 3, 4) highlight the 'Map Organizations' button, the search bar, the dropdown menu for '212 Bronx', and the 'Map' button respectively.

Integrating Datto Portal

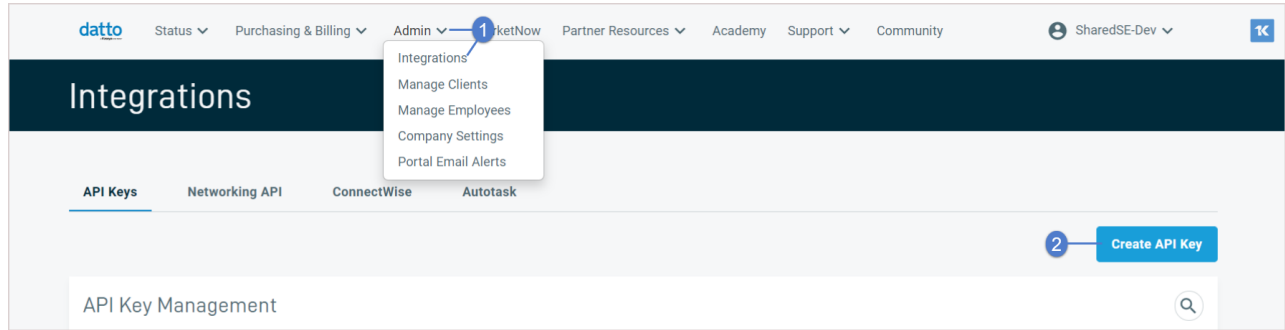
Use this procedure to integrate the Datto Portal DBMA backup tool. After the integration is added, Datta Portal data is synchronized with UniView Portal so that you can receive backup alerts and manage issues right from UniView.

Note: Use this procedure to add the Datto Portal integration if you are using the Datto Backup for Microsoft Azure (DBMA) backup product. If you are using Datto SaaS Protection, you must add the UniView integration through the Datto Portal only. For details, see this article: [Integrating SaaS Protection with Autotask and BMS](#).

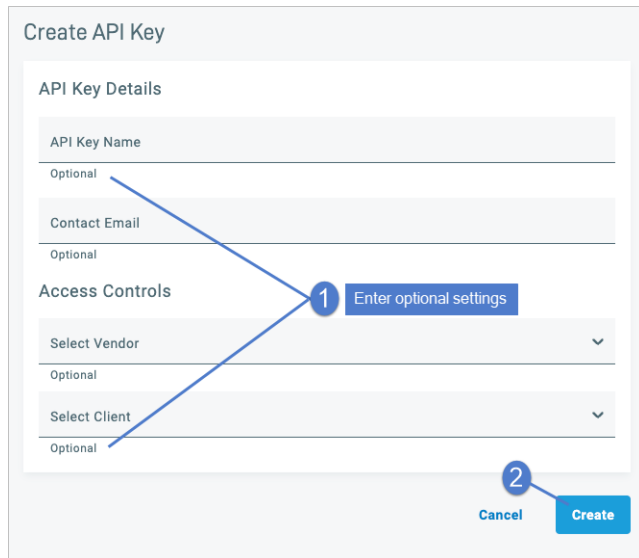
If you have integrated your PSA system with UniView Portal, backup alerts also generate tickets in your PSA (Autotask, BMS, Vorex, or ConnectWise Manage).


To integrate Datto Portal

- 1 In the Datto Portal, select **Admin > Integrations**.
- 2 Click **Create API Key**.

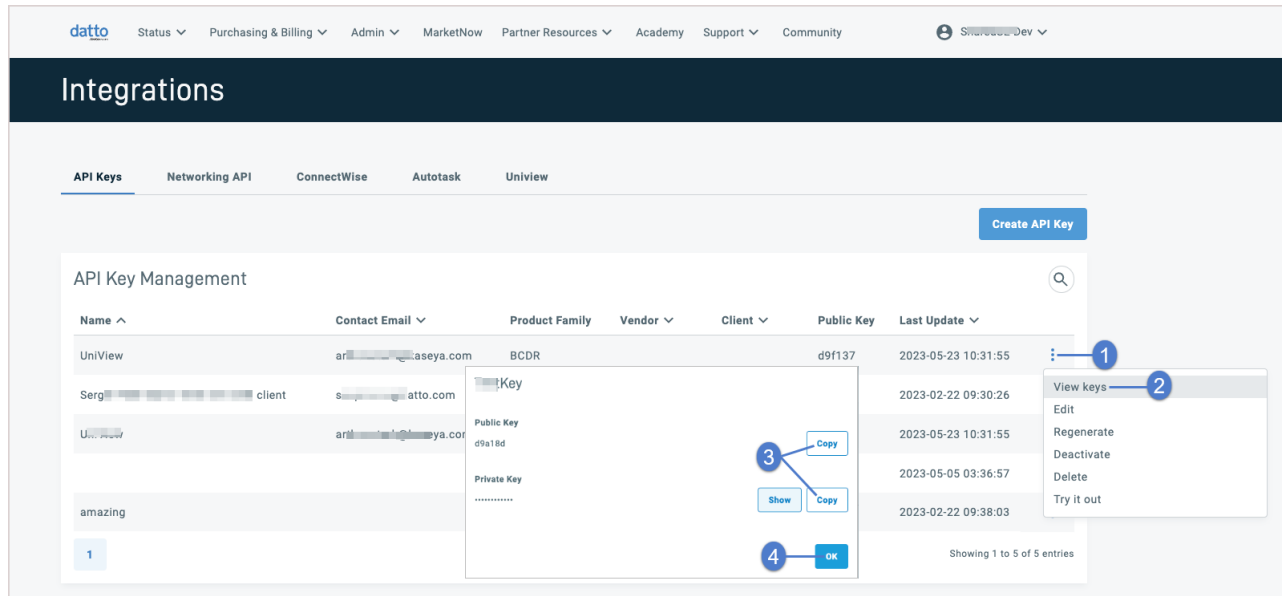


3 Enter optional information and click **Create**.



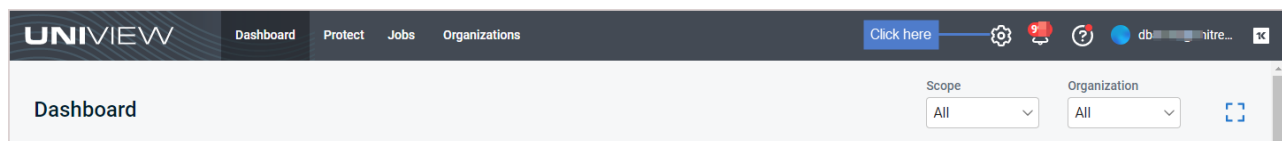
4 Locate the newly generated UniView key entry in the API Key Management table. Click its  icon and select **View Keys**.

5 In the Key dialog, copy and save the public and private keys (you will enter these later in this procedure).



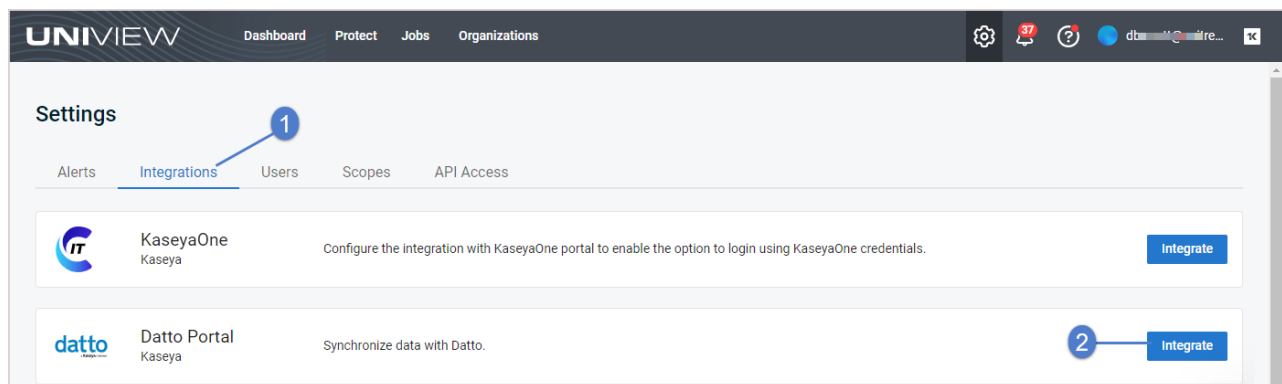
6 Log in to the UniView Portal with a superuser account.

7 Click :



8 Select the **Integrations** view.

9 Locate the Datto Portal integration and click **Integrate**:

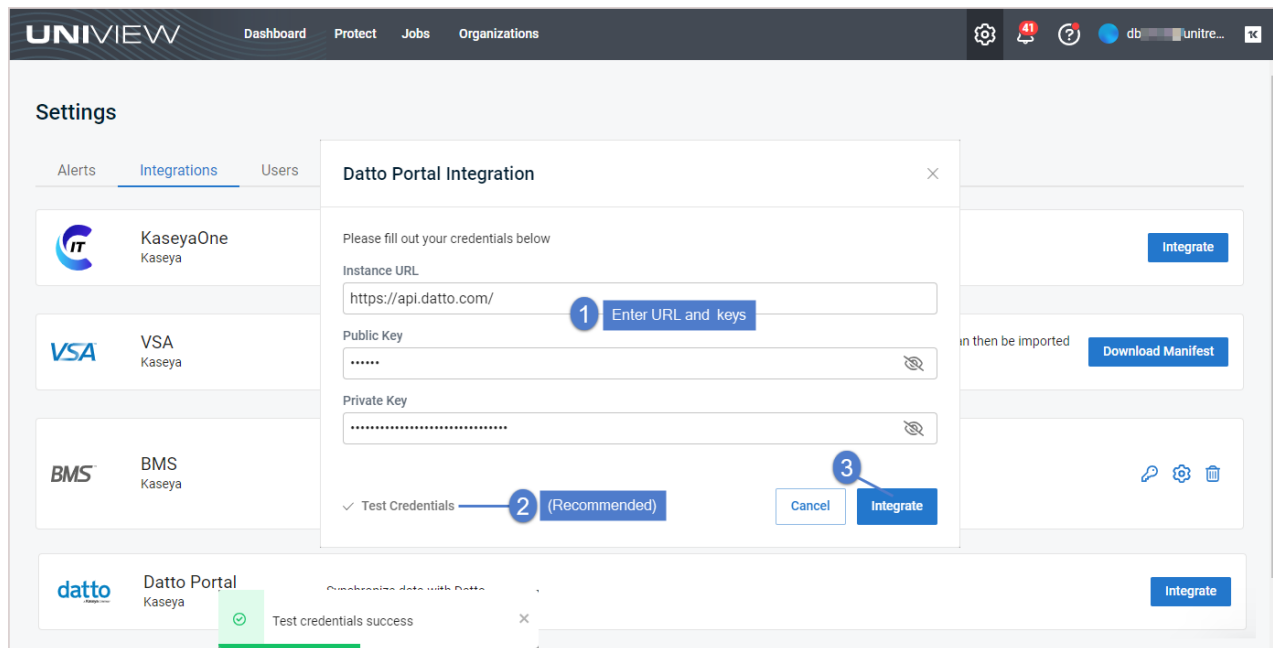


10 Enter the following:

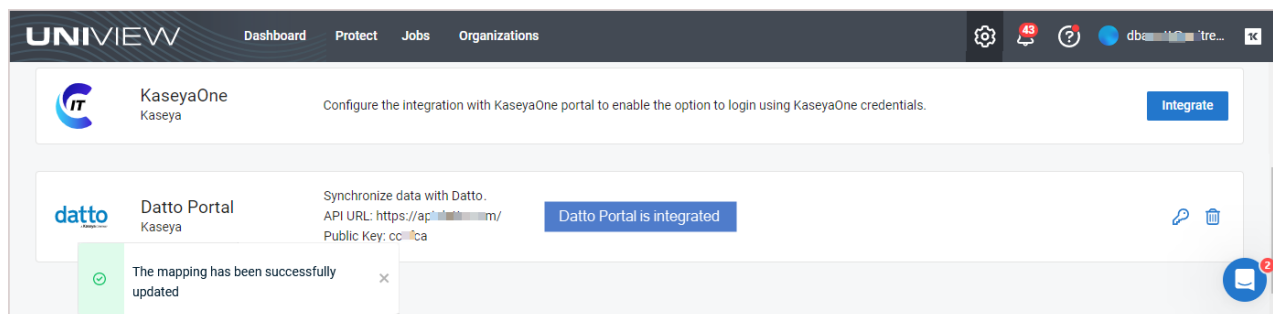
- In the Instance URL field, enter <https://api.datto.com/>.
- In the Public Key and Private Key fields, enter the public and private keys you saved in [step 5](#).

11 (Recommended) Click **Test Credentials** to verify that UniView Portal can connect to Datto Portal.

12 Click Integrate.



UniView Portal automatically maps all Datto clients to UniView organizations and adds the integration.



Working with your Datto Portal integration

Once you've integrated Datto Portal, use these procedures as needed:

- "Mapping Datto Portal clients to organizations"

Note: The procedures below can be run only by users that have the superuser role.

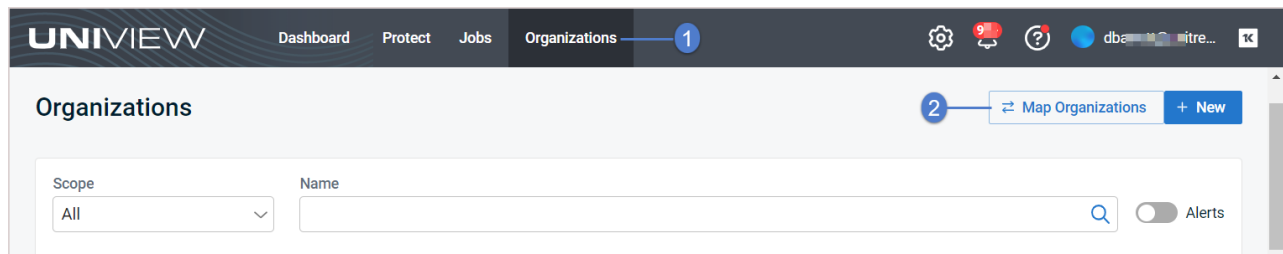
- "To view or modify Datto Portal integration settings"
- "To remove the Datto Portal integration"

Mapping Datto Portal clients to organizations

When the Datto Portal integration was added, UniView Portal automatically created a mapping for each Datto client. As new clients are added to Datto Portal, they are automatically added to UniView and mapped to a UniView organization. If needed, you can use this procedure to quickly modify mappings for multiple organizations.

To map Datto clients to organizations

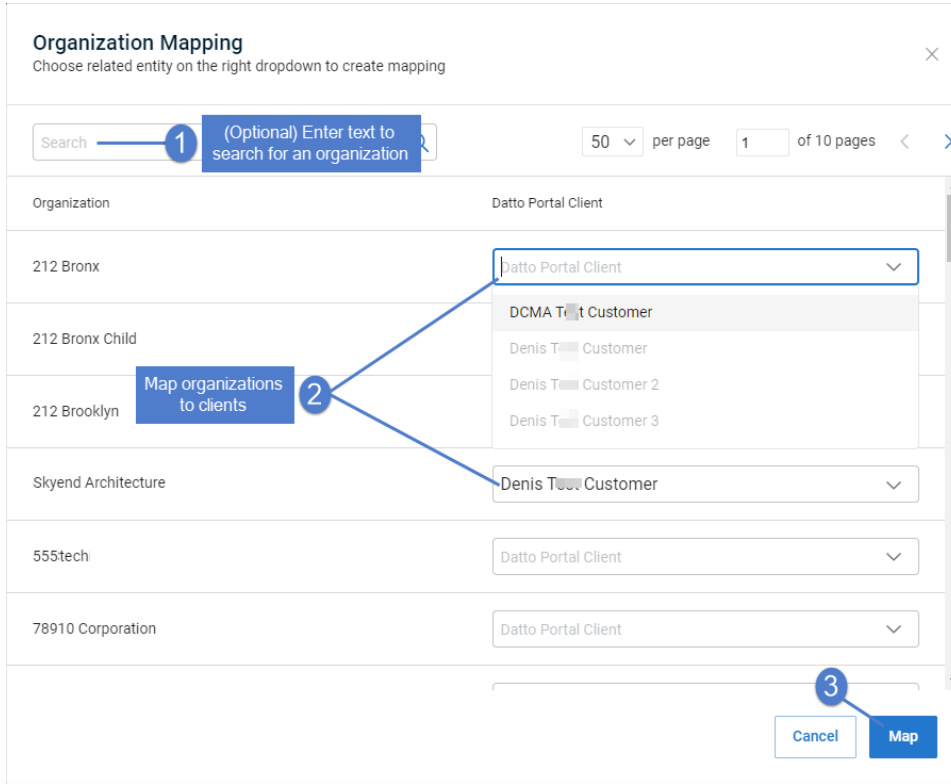
- 1 Log in to the UniView Portal.
- 2 Select **Organizations**.
- 3 Click **Map Organizations**.




- 4 (Optional) Filter the organization list by entering a text string in the Search field.
- 5 In the Datto Portal Client column, select a different client for one or more organizations.

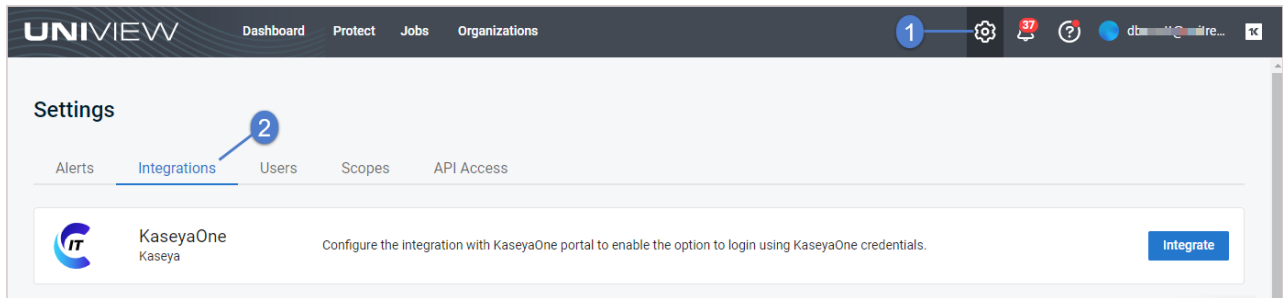
Note: If you do not see a Datto Portal Client column, the Datto integration has not been added to your UniView Portal instance. To add this integration, see "[Integrating Datto Portal](#)".



- 6 Click **Map**.



To view or modify Datto Portal integration settings

- 1 Log in to the UniView Portal with a superuser account.
- 2 Click .
- 3 Select the **Integrations** view.



- 4 Locate the Datto Portal integration and click .
- 5 (Optional) To view the Public and Private keys, click the  icons.
- 6 (Optional) Modify the Instance URL.
- 7 (Optional) Modify credentials settings. Click **Test Credentials** to verify that UniView Portal can connect to the Datto Portal.


8 Click **Integrate**.

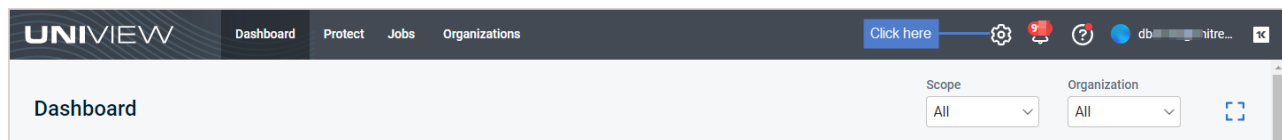
The screenshot shows the 'Datto Portal Integration' configuration window in the UniView Portal. The window contains the following elements:


- Instance URL:** A text input field containing 'https://api.datto.com/'.
- Public Key:** A text input field with masked characters '.....' and a 'Show/Hide' icon.
- Private Key:** A text input field with masked characters '.....' and a 'Show/Hide' icon.
- Test Credentials:** A checked checkbox labeled 'Recommended'.
- Buttons:** 'Cancel', 'Integrate', and 'Integrate' (in a larger blue box).
- Additional UI:** A 'Download Manifest' button in the top right, and a 'Save your changes' callout pointing to the 'Integrate' button.

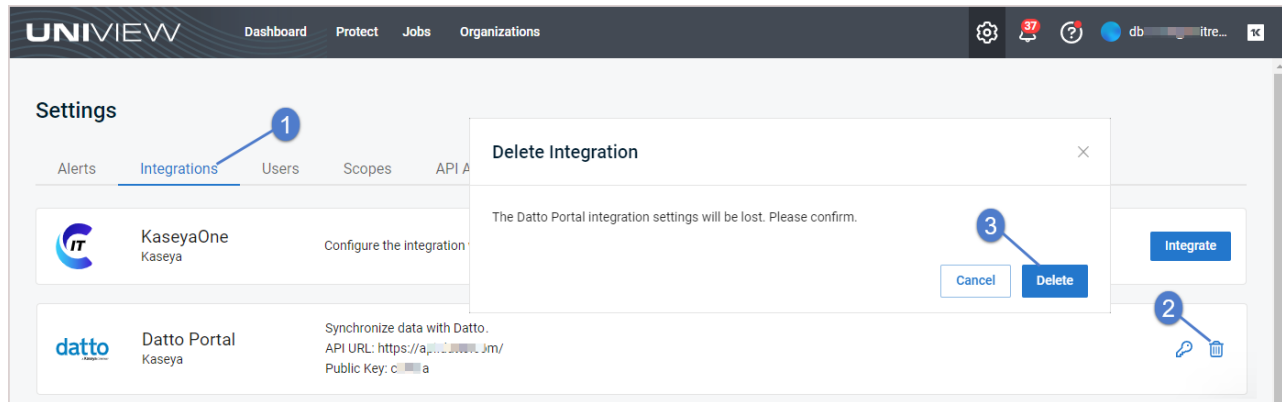
To remove the Datto Portal integration

Use this procedure to remove the Datto Portal integration from the UniView Portal.

- 1 Log in to the UniView Portal with a superuser account.
- 2 Click :



- 3 Select the **Integrations** view.
- 4 Locate the Datto Portal integration and click .
- 5 Click **Delete**. The integration and any organization mappings are removed.



Integrating IT Glue

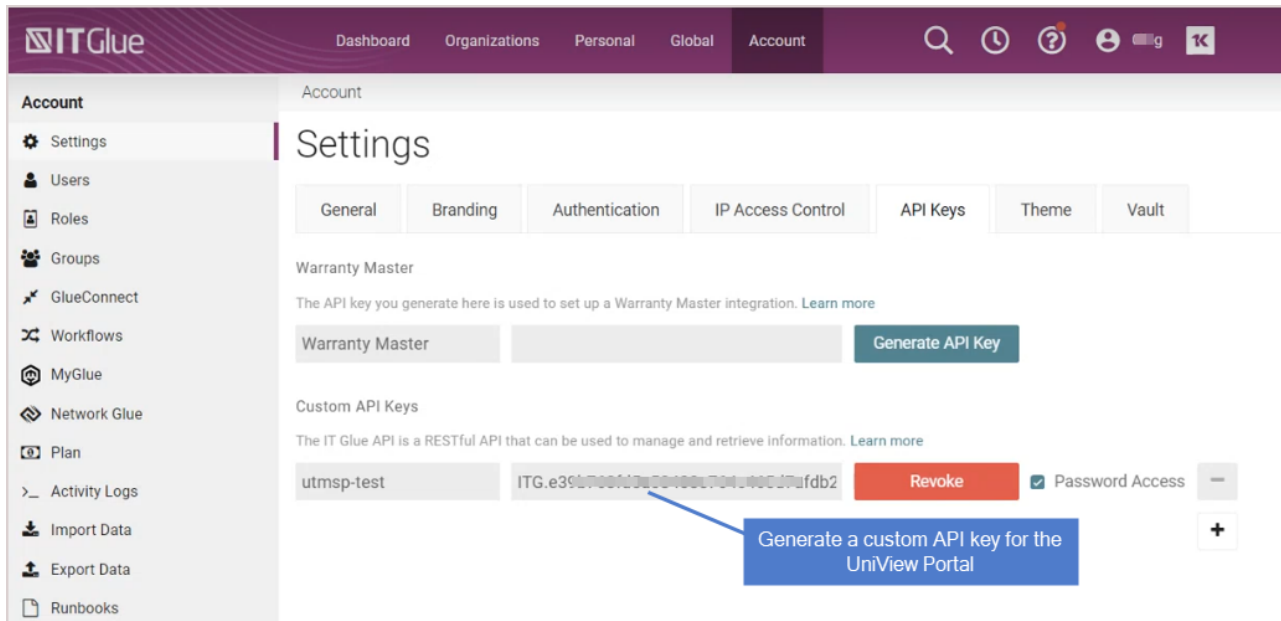
You can now synchronize your assets and appliances with Kaseya's IT Glue documentation platform. This enables IT Glue users to:


- View backup configuration information from the UniView Portal.
- Display backup status, last backup time, and storage for endpoints in IT Glue.
- Ensure organizations and assets from the UniView Portal are automatically mapped to IT Glue organizations and configurations.

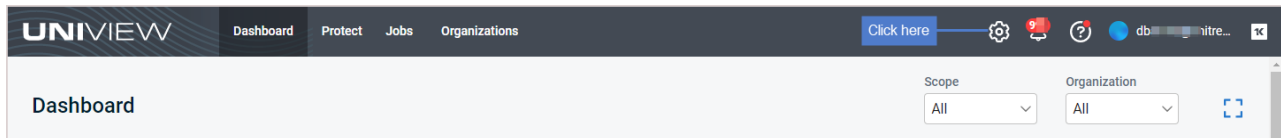
To integrate IT Glue

Use this procedure to integrate IT Glue with the UniView Portal.

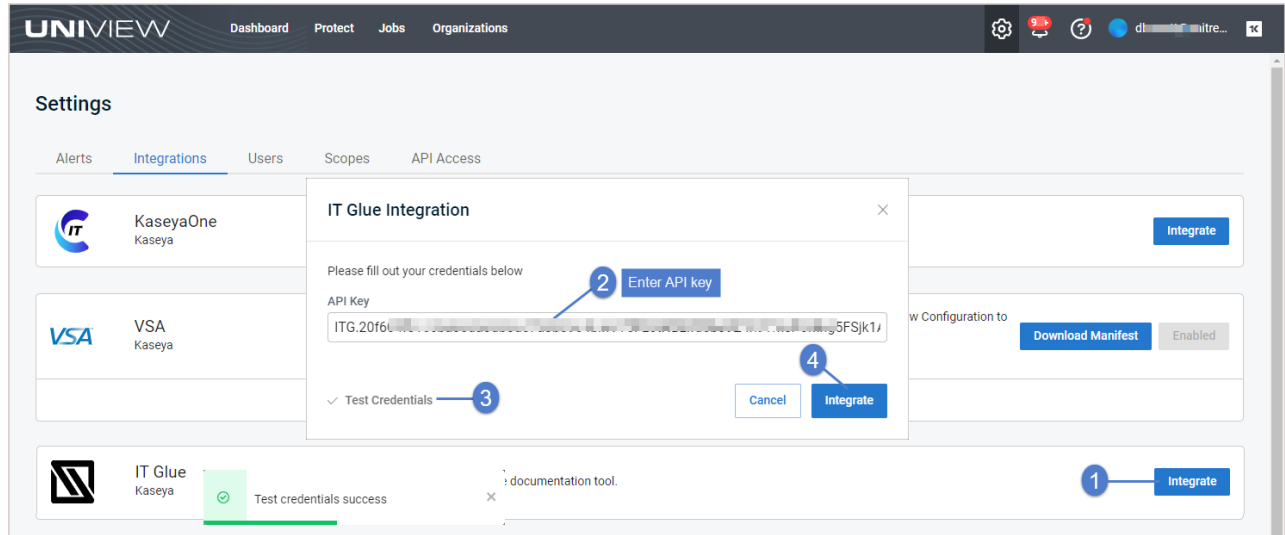
- 1 Log in to IT Glue with a Manager or Administrator account.
- 2 On the **Account > API Keys** tab, generate a custom key for the UniView Portal.



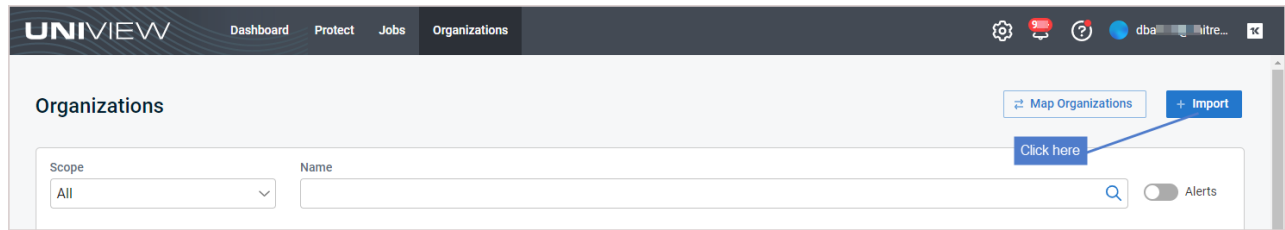
- 3 Log in to the UniView Portal as a superuser.
- 4 Click :



- 5 Select the **Integrations** view.
- 6 Locate the IT Glue integration and click **Integrate**.
- 7 Enter the API Key you generated above in [step 2](#).
- 8 Click **Test Credentials** to verify the API key you entered.
- 9 Click **Integrate**.



10 On the Organizations page, click **Import**:



Organizations are imported:

Import Organizations ×

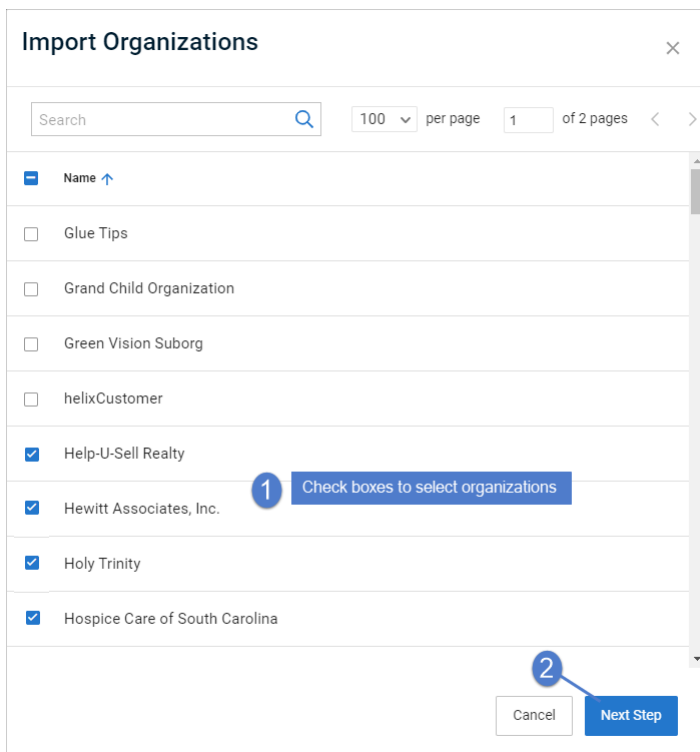
Search 100 per page 1 of 2 pages < >

<input type="checkbox"/>	Name ↑
<input type="checkbox"/>	Glue Tips
<input type="checkbox"/>	Grand Child Organization
<input type="checkbox"/>	Green Vision Suborg
<input type="checkbox"/>	helixCustomer
<input type="checkbox"/>	Help-U-Sell Realty
<input type="checkbox"/>	Hewitt Associates, Inc.
<input type="checkbox"/>	Holy Trinity
<input type="checkbox"/>	Hospice Care of South Carolina

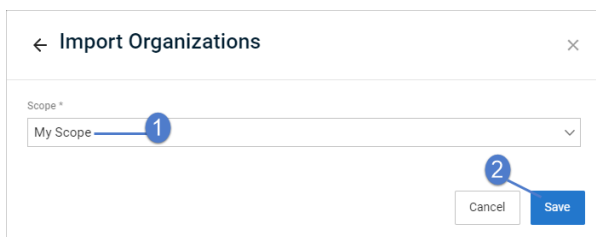
11 Assign organizations to a scope:

Notes:

- A user's scope determines which organizations are visible in the UniView Portal. To ensure that users can only access information about organizations specified in their scope(s), you must assign each organization to a scope.
- In this procedure, the organizations you select are assigned to one scope. Repeat these steps to assign organizations to another scope.
- Check boxes to select organizations. Click **Next Step**.

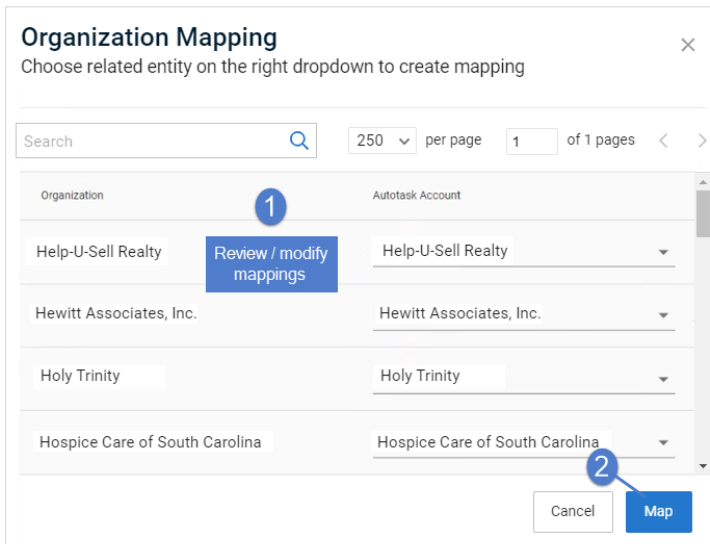


- Select a scope from the list. Click **Save**.



- If you have integrated UniView Portal with your PSA (Autotask, ConnectWise Manage, BMS, or Vorex), the Organization Mapping dialog displays. UniView Portal automatically maps PSA accounts/companies to IT Glue organizations based on name. If no suggested match can be found, the organization remains unmapped.

Review the mappings and make changes if needed. Then click **Map**.




- Repeat these steps to assign organizations to another scope.

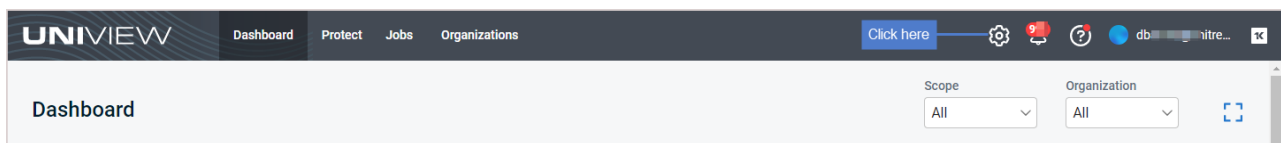
Working with your IT Glue integration

Use these procedure to view/modify IT Glue credentials or remove the IT Glue integration:

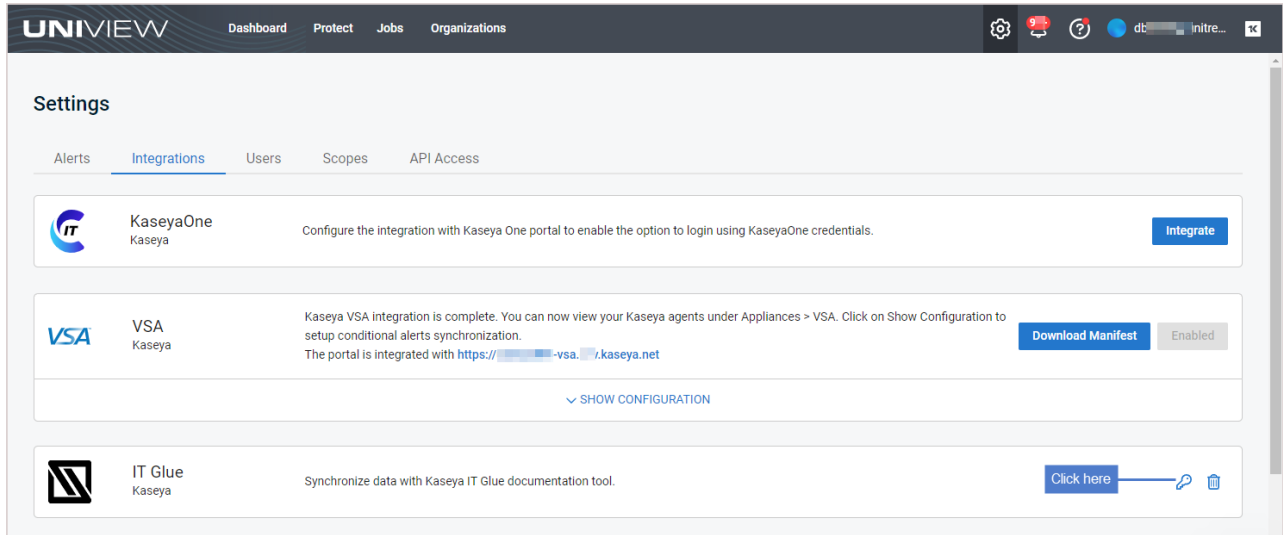
- "To view or modify IT Glue credentials settings"
- "To remove the IT Glue integration"

To view or modify IT Glue credentials settings

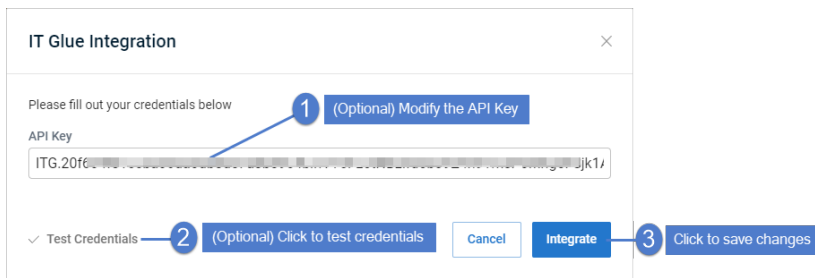
- 1 Log in to the UniView Portal with a superuser account.
- 2 Click :



- 3 Select the **Integrations** view.
- 4 Locate the IT Glue integration and click .




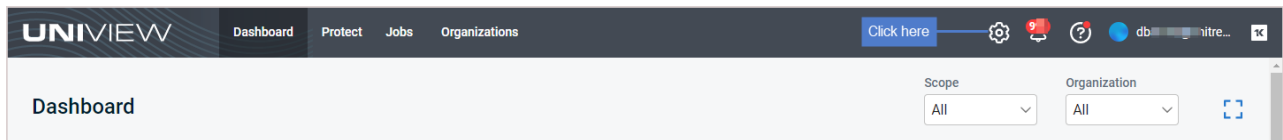
- (Optional) Modify the API Key. Click **Test Credentials** to verify that UniView Portal can connect to IT Glue. Click **Integrate**.



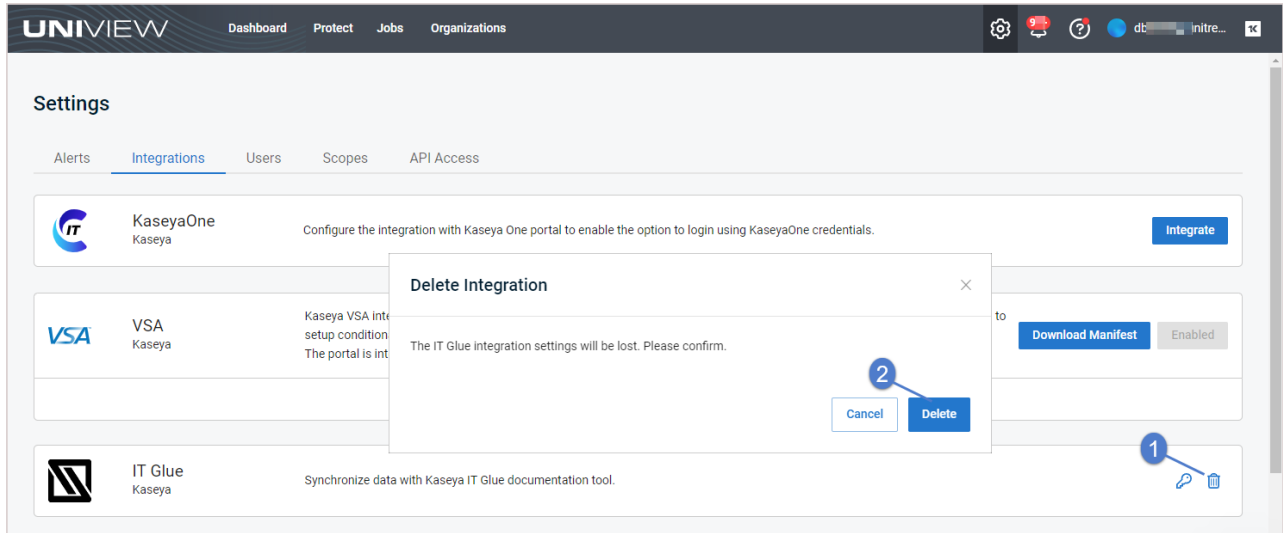
To remove the IT Glue integration

Use this procedure to remove the IT Glue integration from the UniView Portal.

- Log in to the UniView Portal with a superuser account.
- Click :



- Select the **Integrations** view.
- Locate the IT Glue integration and click . Click **Delete**. The integration is removed.




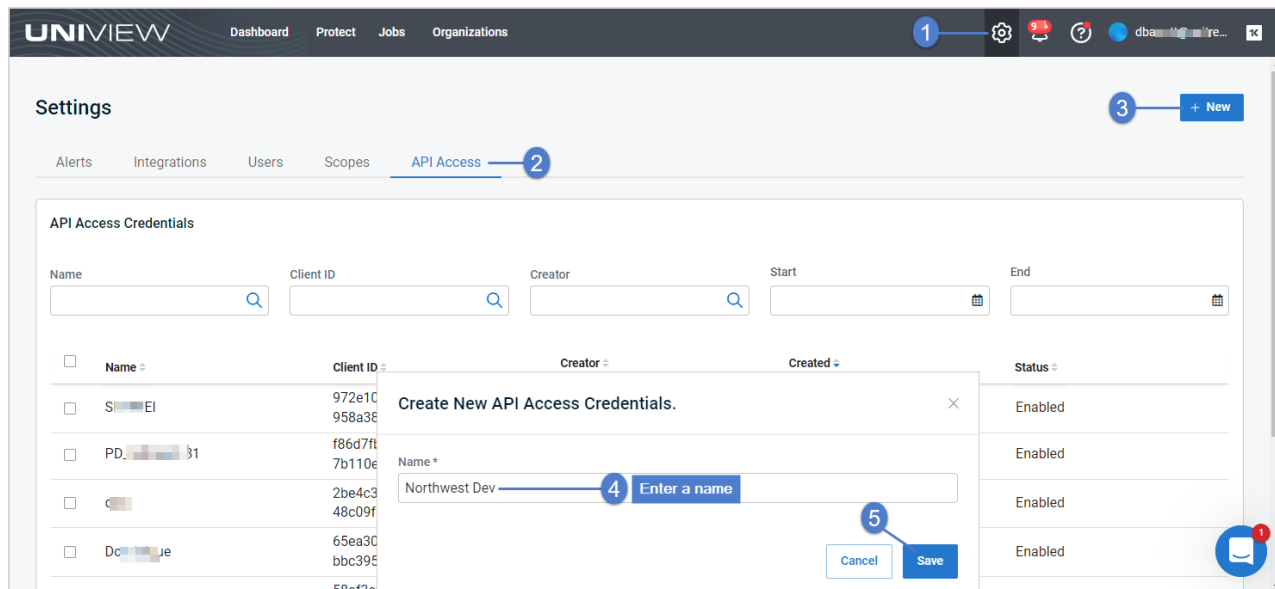
API Access

UniView Portal provides public APIs that customers can use to develop their own tools to access their Portal data. Our public API uses the [OAuth 2.0 client credentials flow](#), but we generally support OIDC protocol. Auth-related endpoints can be discovered through <https://login.backup.net/.well-known/openid-configuration>.

To get started, create public API credentials as described below. For an example request, see ["Get public API access_token example"](#). For a description of each public API, see UniView Portal's [Public API](#).

To create public API credentials

- 1 In the UniView Portal, click .
- 2 In the API Access view, click **+ New**.
- 3 Enter a name for the credentials. Click **Save**.



- 4 Copy and save the Client ID and Client Secret.

IMPORTANT! Be sure to save the Client Secret in a safe place. You will not be able to access the Client Secret after you close this dialog.

- 5 Click **Close**.

New API Access Credentials Were Successfully Created!

Name: Northwest Dev

Client ID: 983...i6c1cc

Client Secret:

1 Copy and save the Client ID and Client Secret

2 Close

Copy Client ID and Secret and store them in a secure place.
COPY THE CLIENT SECRET NOW. IT WILL NOT BE SHOWN AGAIN AND YOU WILL NOT BE ABLE TO COPY IT LATER.

6 Credentials are added to the Public API Credentials page.

UNIVIEW Dashboard Protect Jobs Organizations

Settings + New

Alerts Integrations Users Scopes API Access

API Access Credentials

Name Client ID Creator Start End

Name	Client ID	Creator	Created	Status
Northwest Dev	983...i6c1cc	d Barrett@unitrends.com	2/6/23 10:46 am	Enabled
SIADMEI	97...ea53	superuser@yopmail.com	1/10/23 4:59 am	Enabled
PD...	f86d...bec27b110e	pd@yopmail.com	1/3/23 1:37 am	Enabled
...	2be4c3...0ee	superuser@yopmail.com	11/1/22 7:10 am	Enabled
...	65ea309a77744d0696b734312		10/13/22	

Get public API *access_token* example

Send the following request to get the public API *access_token*, where *<token>* is Base64 of your UniView Portal *client_id:client_secret* string:

```
POST https://login.backup.net/connect/token
Content-Type: application/x-www-form-urlencoded
Authorization: Basic <token>
Accept: */*
Cache-Control: no-cache
Host: login.backup.net
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Content-Length: 36
grant_type: client_credentials
```