

Kaseya EndPoint Backup Guide

Release 1.30.2 | Document Version 3.06022023



Copyright Agreement

The purchase and use of all Software and Services is subject to the Agreement as defined in Kaseya's "Click-Accept" EULATOS as updated from time to time by Kaseya at <http://www.kaseya.com/legal.aspx>. If Customer does not agree with the Agreement, please do not install, use or purchase any Software and Services from Kaseya as continued use of the Software or Services indicates Customer's acceptance of the Agreement.

Contents

Chapter 1: Getting Started with Kaseya EndPoint Backup	5
Step 1: Make sure all requirements have been met	5
VSA requirements	5
Network requirements	5
Windows asset requirements	6
Port requirements	7
Step 2: Install the Kaseya EndPoint Backup TAP module	7
Step 3: Log in to Kaseya EndPoint Backup	12
Step 4: (Optional) Add a customer	14
Step 5: Install the Kaseya EndPoint Backup agent	16
Step 6: Run backups	21
Step 7: Recover files	24
Installing the VSA agent	29
Troubleshooting Kaseya EndPoint Backup agent installs	30
Chapter 2: Accessing Kaseya EndPoint Backup	35
Chapter 3: Protecting Assets with Kaseya EndPoint Backup	43
Backup considerations	43
Working with backup profiles	44
Working with backup jobs	52
Chapter 4: Recovering Files	65
Recovery considerations	65
Recovering files and folders from a backup	65
Chapter 5: Bare Metal Recovery	71
Chapter 6: Monitoring Agents, Assets, Backups, and Restores	89
Working with the Dashboard	89
Viewing backup status	91
Viewing backup history	95

BackupIQ alerts	100
Viewing restore status	100
Chapter 7: Working with Customers, Assets, and Users	103
Working with customers	103
Working with users	108
Working with assets	113
Working with your user account settings	120
Chapter 8: Working with Kaseya EndPoint Backup Settings	129
Viewing Kaseya EndPoint Backup settings	129
Working with your IT Complete integration	130
Working with your BackupIQ integration	134
Working with asset log storage	149
Chapter 9: Cooper Insights in KaseyaOne	155
Chapter 10: Upgrading to the Latest Release	159
Upgrading the Kaseya EndPoint Backup TAP module	159
Upgrading the Kaseya EndPoint Backup agent	164
Troubleshooting Kaseya EndPoint Backup agent installs	169

Chapter 1: Getting Started with Kaseya EndPoint Backup

Kaseya EndPoint Backup (formerly known as *Kaseya Direct to Cloud Backup*) protects geographically distributed Windows PCs and laptops, all without the hassle of setting up an appliance or local storage at every office location, keeping the act of data protection as simple as possible.

With Kaseya EndPoint Backup, your data is protected in the Unitrends Cloud. Data is air gapped and cannot be modified or deleted by the source. It is AES 256 encrypted in flight and at rest.

The PCs and laptops protected by Kaseya EndPoint Backup are called assets. To start protecting an asset, simply install a light-weight agent and add the asset to a backup job. Kaseya EndPoint Backup comes equipped with pre-configured backup profiles so you can start protecting your assets immediately. Follow the steps in the remainder of this chapter to start running backups using the out-of-the box profiles. See the remaining chapters in this guide to explore additional features and customize Kaseya EndPoint Backup for your environment.

- "Step 1: Make sure all requirements have been met"
- "Step 2: Install the Kaseya EndPoint Backup TAP module "
- "Step 3: Log in to Kaseya EndPoint Backup"
- "Step 4: (Optional) Add a customer"
- "Step 5: Install the Kaseya EndPoint Backup agent "
- "Step 6: Run backups"
- "Step 7: Recover files"

Step 1: Make sure all requirements have been met

Ensure that the "VSA requirements", "Network requirements", "Windows asset requirements ", and "Port requirements" have been met.

VSA requirements

Kaseya EndPoint Backup is supported on VSA instances running release 9.5 or higher. Kaseya recommends upgrading to the latest VSA release to benefit from new features and performance enhancements. If needed, upgrade your VSA instance.

Network requirements

Adhere to these best practices:

- It is highly recommended that devices are on a wired network connection for their first FULL backup.

- It is highly recommended that devices are on a wired network connection for any MANUAL FULL backups.
- Backup performance is primarily impacted by network performance. During a backup operation it is recommended to maintain at least:
 - ≤ 70 ms latency
 - $\leq 0.3\%$ packet loss
 - \geq Download speed 34 Mbps
 - \geq Upload speed 11 Mbps

These limitations apply:

- Backups are likely to begin failing under these conditions:
 - ≥ 150 ms latency
 - $\geq 7.0\%$ packet loss
 - \leq Download speed 20 Mbps
 - \leq Upload speed 11 Mbps
- In general, Kaseya EndPoint Backup requires an asset to be able to upload at least one 10MB block in a span of 15 minutes to be successful.
 - This does not guarantee a successful backup.
 - If a backup task fails, the task will attempt to back up the remaining blocks on subsequent backup tasks.
 - It is possible to obtain a full back up after a series of failed tasks as long as the connection is successfully open and data is committed to the Unitrends Cloud.

Windows asset requirements

Kaseya EndPoint Backup can be used to protect Windows PCs, laptops, and servers that meet the requirements below.

Note: Additional requirements apply for the bare metal recovery feature. See "[Bare Metal Recovery](#)" for details.

- Supported operating systems – The Windows asset must be running one of these OSs:
 - Windows 8, 64-bit
 - Windows 10, 64-bit
 - Windows 11, 64-bit
 - Windows 2008 R2, 64-bit*
 - Windows 2012, 64-bit
 - Windows 2012 R2, 64-bit

- Windows 2016, 64-bit
- Windows 2019, 64-bit
- Windows 2022, 64-bit

IMPORTANT! Kaseya EndPoint Backup is a backup solution that is ideal for workstations and laptops running Windows client operating systems. Server operating systems are supported as well, but ensure you consider the recovery requirements of the server and its applications. Kaseya Unified Backup is typically a better fit for protecting and recovering servers and is REQUIRED when protecting hosted applications, like Active Directory, SQL Server, Exchange, SharePoint, and Oracle.

- PowerShell 3.0 – PowerShell 3.0 or higher must be installed on the Windows asset. If needed, install PowerShell.
- VSA agent – The Windows asset must be running VSA agent version 9.5.0.14 or higher. If needed, install or upgrade the VSA agent as described in "[To install the VSA agent](#)".
- Unitrends agent and PCBP folder – If the asset has a Unitrends agent installed, you must uninstall the agent and delete the C:\PCBP folder. This folder will be recreated upon installing the Kaseya EndPoint Backup agent.
- *Windows 2008 R2 – The Windows asset must be running this update: Windows6.1-KB3004394-v2-x64.msu (see <https://www.microsoft.com/en-us/download/confirmation.aspx?id=45633>).

Port requirements

Port 443 (TCP) must be open outbound from each protected Windows asset to the following:

- <https://direct.backup.net>
- <https://ingest.backup.net>
- <https://storage.backup.net>

Step 2: Install the Kaseya EndPoint Backup TAP module

Use this procedure to install the TAP module. The instructions are slightly different depending on whether you have a SaaS or on-premise VSA instance:

- If you are using VSA on-premise, run all steps in the procedure.
- If you are using VSA SaaS, [step 3](#) is not needed. Skip this step in the procedure.

To install or upgrade the Kaseya EndPoint Backup TAP module

- 1 Go to https://direct.backup.net/download/kaseya_endpoint_backup.vsz and download *kaseya_endpoint_backup.vsz* to your workstation.

- 2 Log into the VSA instance.

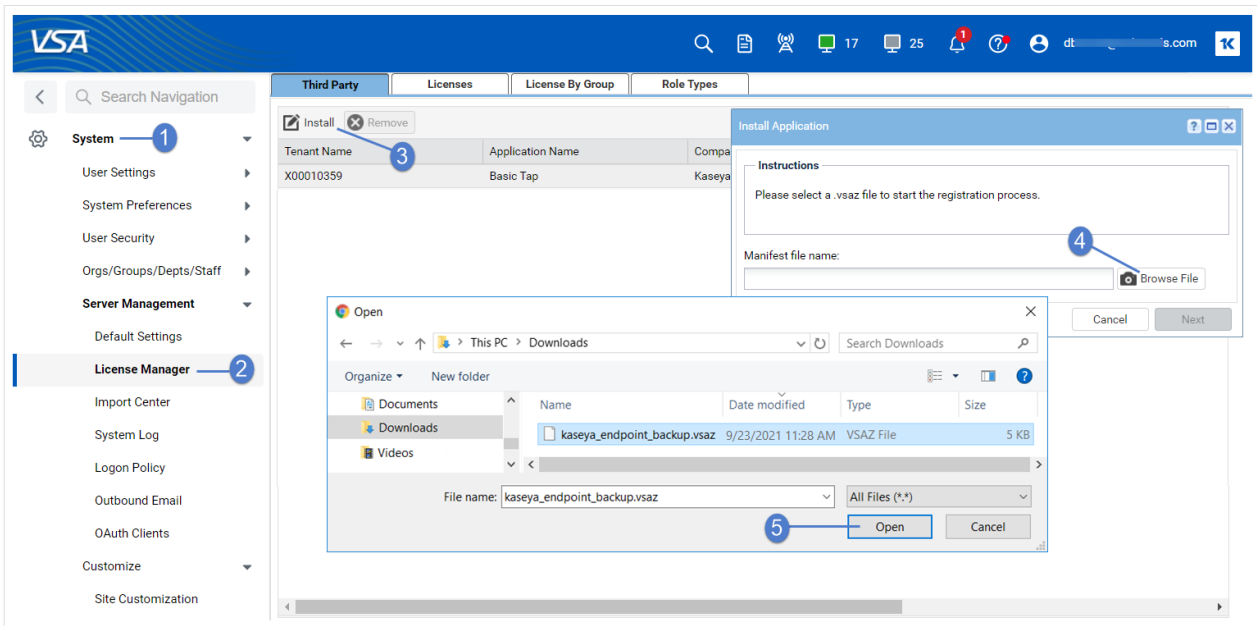
Note: Do not use a VSA URL that includes `-cdn`. Use the URL that goes directly to your VSA server instance.

- 3 On-premise instance only – Select **System > Server Management > Configure** and make sure you have checked this box: **Enable Third Party App Installation Globally**.

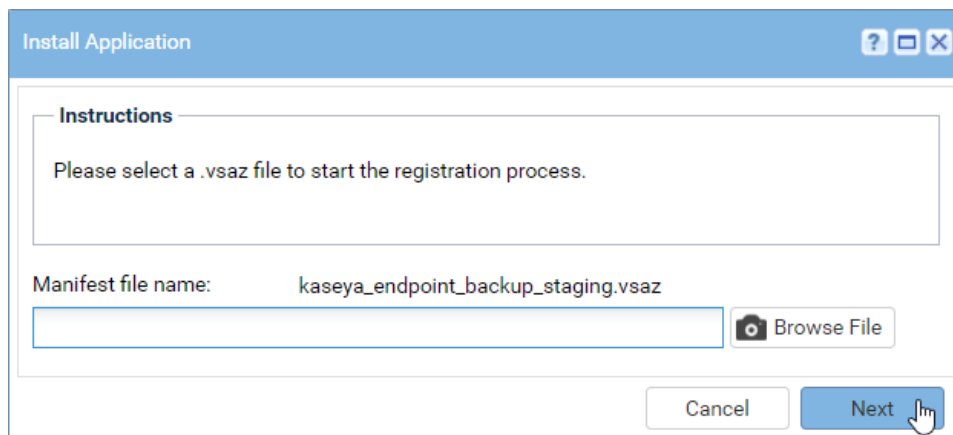
The screenshot displays the VSA web interface. The left sidebar contains a navigation menu with the following items: System (1), User Settings, System Preferences, User Security, Orgs/Groups/Depts/Staff, Server Management (2), Default Settings, License Manager, Import Center, System Log, Logon Policy, Outbound Email (3), OAuth Clients, Customize, BMS Integration, Agent, Agent Procedures, Anti-Malware, Antivirus, Audit, AuthAnvil, Backup, Cloud Backup, and Data Backup. The main content area shows the following settings:

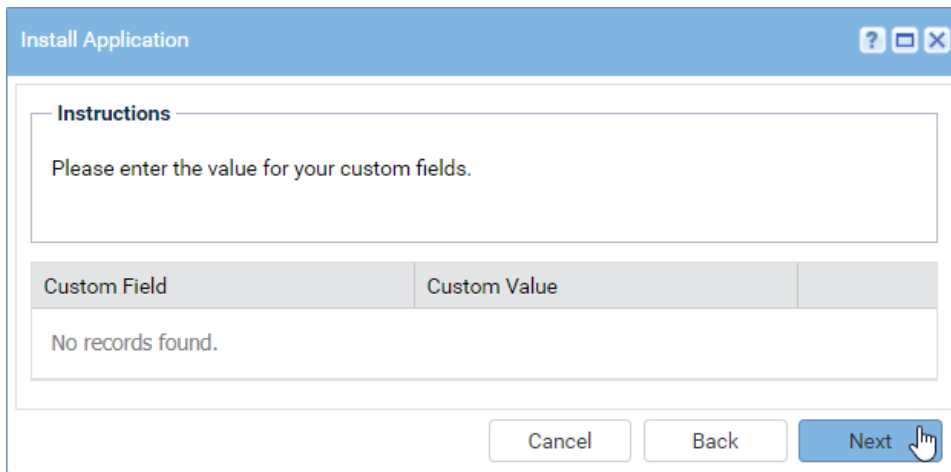
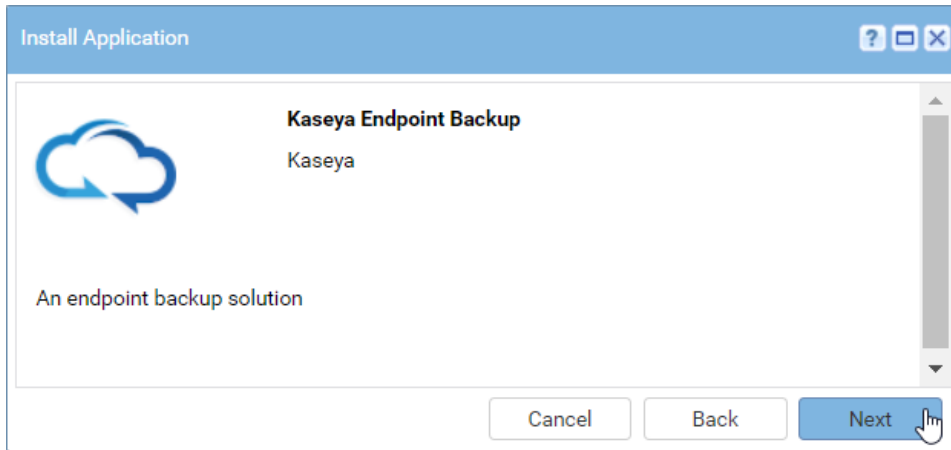
- Version Number: 9.5.0.2
- Installed Patch Level: 9.5.0.23
- Available Patch Level: 9.5.0.23
- Last Checked On: Wed Oct 2 18:28:11 EDT 2019
- Check Latest Patch Level button
- Warn if the server can not get data from <http://vsaupdate.kaseya.net> (checked)
- Warn when the license reaches the maximum number of seats (checked)
- Reload sample **scripts** with every update and database maintenance cycle (checked)
- Reload sample **event sets** with every update and database maintenance cycle (checked)
- Reload sample **monitor sets** with every update and database maintenance cycle (checked)
- Automatically redirect to HTTPS at logon page (checked)
- Enable VSA API Web Service (checked)
- Enable Third Party App Installation Globally (checked)
- Enable Invalid Patch Location Notifications (checked)
- Allow non-authenticated users to download attachments from ticket notifications (checked)
- Run database backup / maintenance every: 7 Days @ 2:00 am
- Backup folder on KWEB1: C:\Kaseya\UserProfiles\@dbBackup
- Archive and purge logs every day @ 4:00 am
- Log file archive path: C:\Kaseya\UserProfiles\@archive
- KServer Log button
- Live Connect KServer button
- Stop KServer button
- Restart MsgSys button
- Enable alarm generation. Disable during system maintenance (checked)
- Enable logging of script errors marked "Continue script if step fails" (checked)
- Enable logging of successful child script execution in agent procedure log (checked)

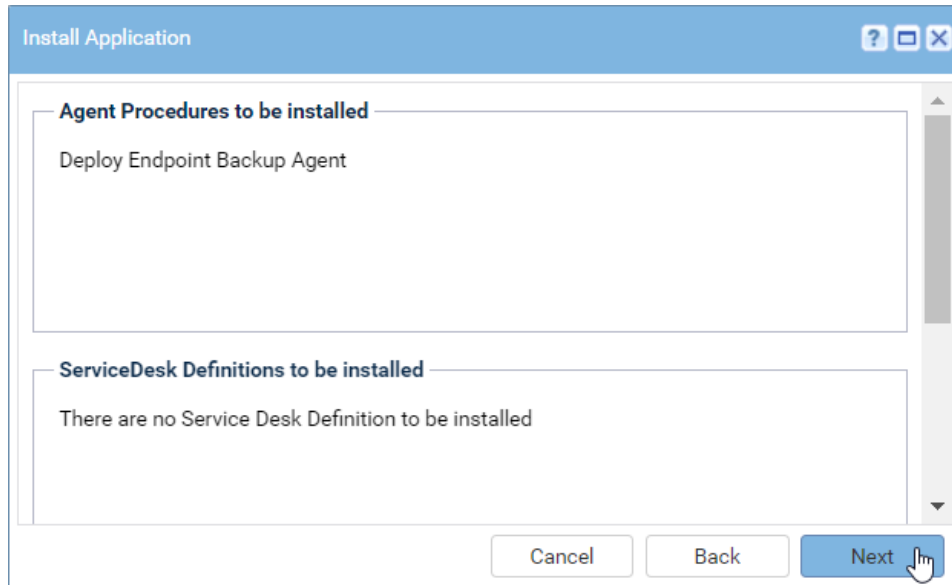
- 4 Select **System > Server Management > License Manager > Third Party > Install**.
- 5 Click **Install**. Browse to the path where you downloaded the TAP module in [step 1](#). Select `kaseya_endpoint_backup.vsz`. Click **Open**.



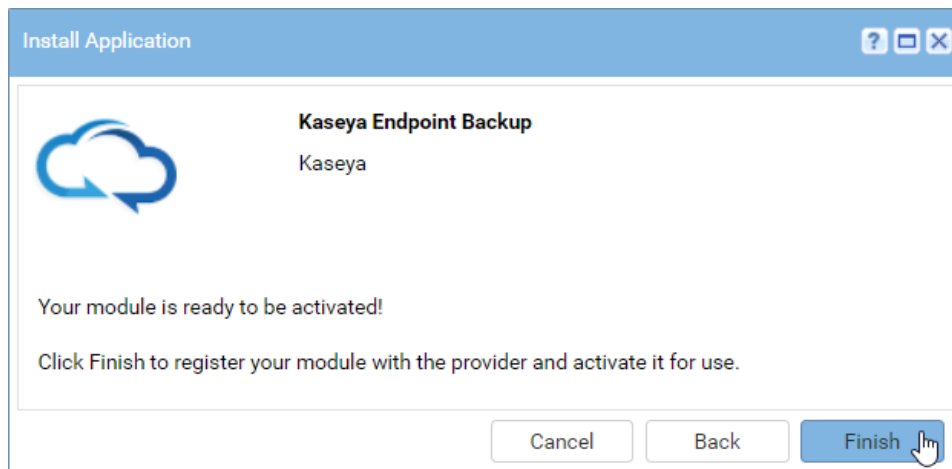
6 Click **Next** to work your way through the install wizard.

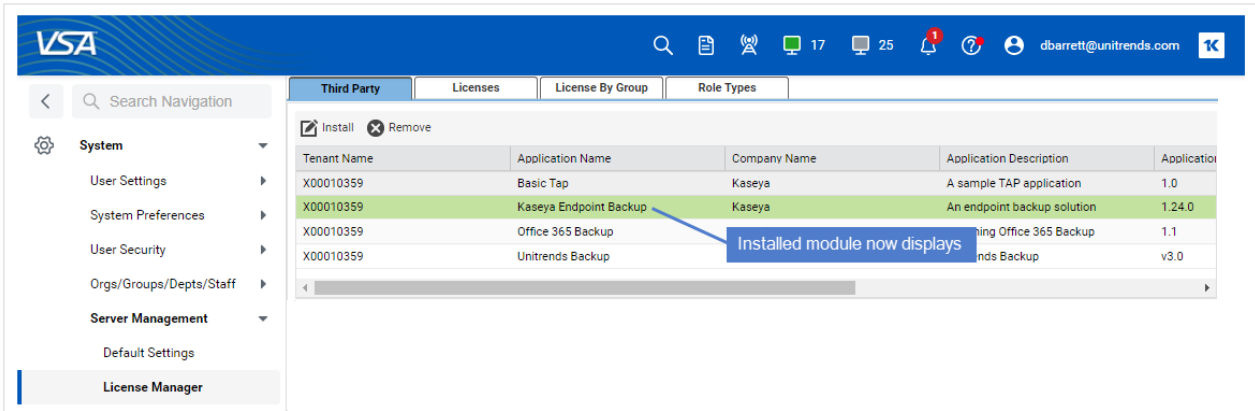






- 7 Click **Finish**. The module is installed.



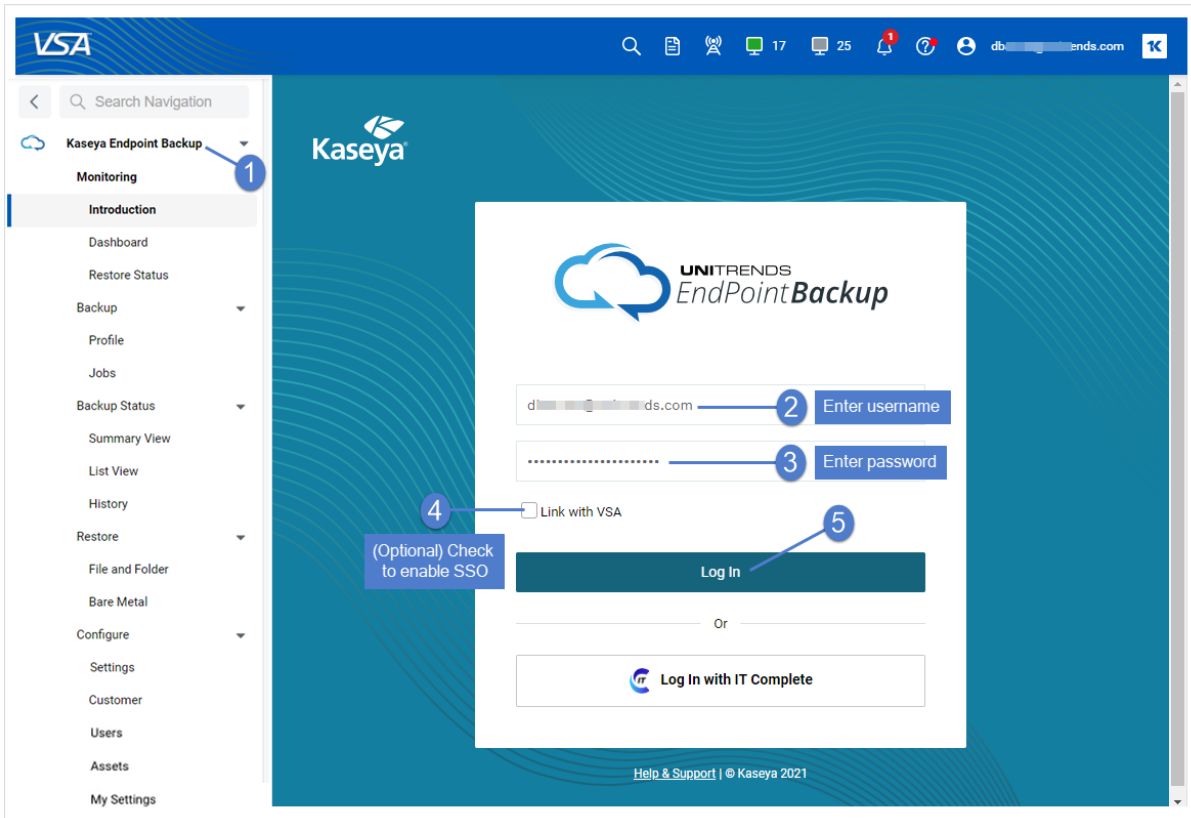


Step 3: Log in to Kaseya EndPoint Backup

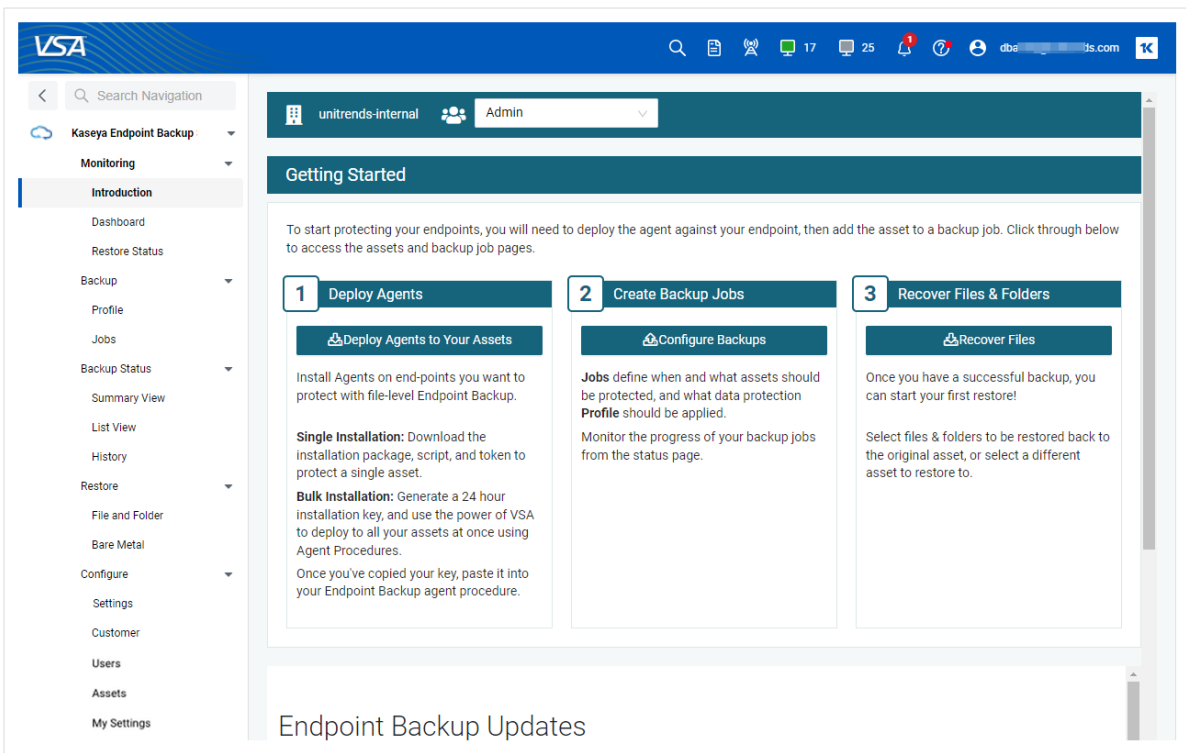
- 1 Log in to the VSA.
- 2 Select **Kaseya Endpoint Backup**.
- 3 Enter the username and password of your Kaseya EndPoint Backup account.
- 4 (Optional) Check the **Link with VSA** box to link your Kaseya EndPoint Backup and VSA accounts.

Upon logging in, your VSA account is linked and you no longer need to supply separate credentials to access the Kaseya EndPoint Backup module.

- 5 Click **Log In**.



6 The Introduction page displays.



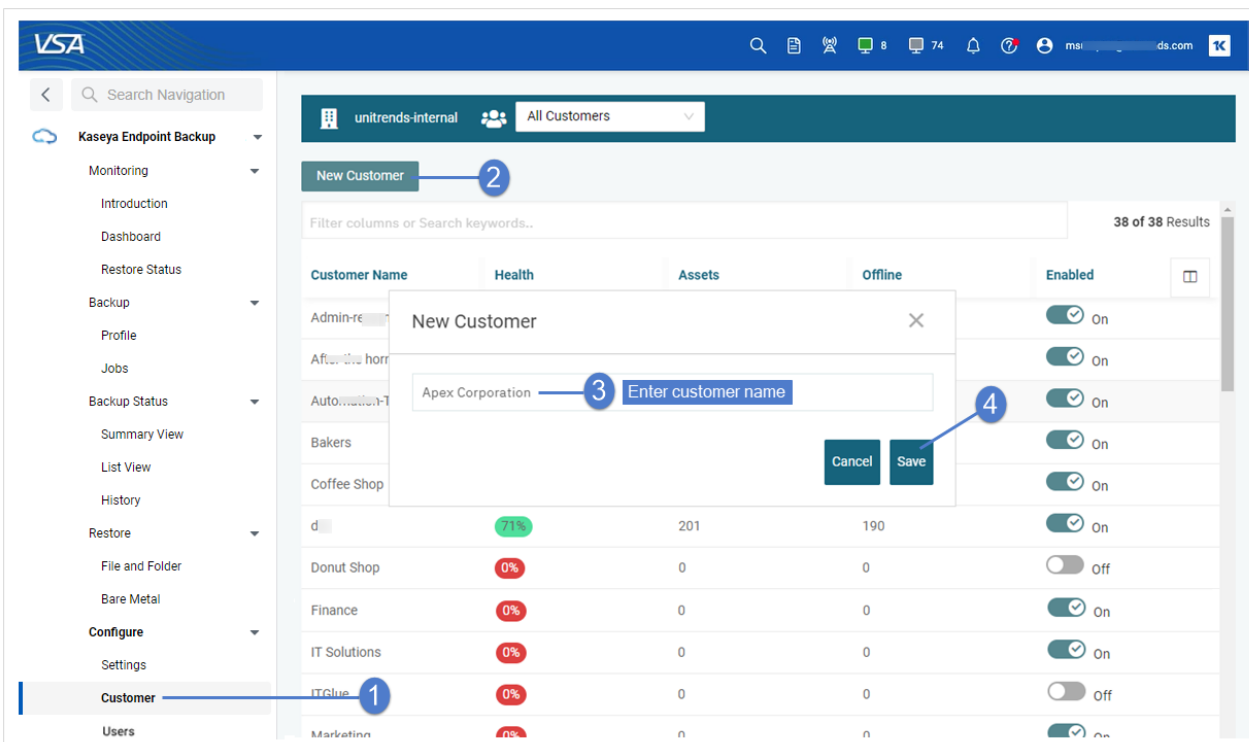
Step 4: (Optional) Add a customer

Add the customer whose assets you will back up or skip this step to use the *Default* customer.

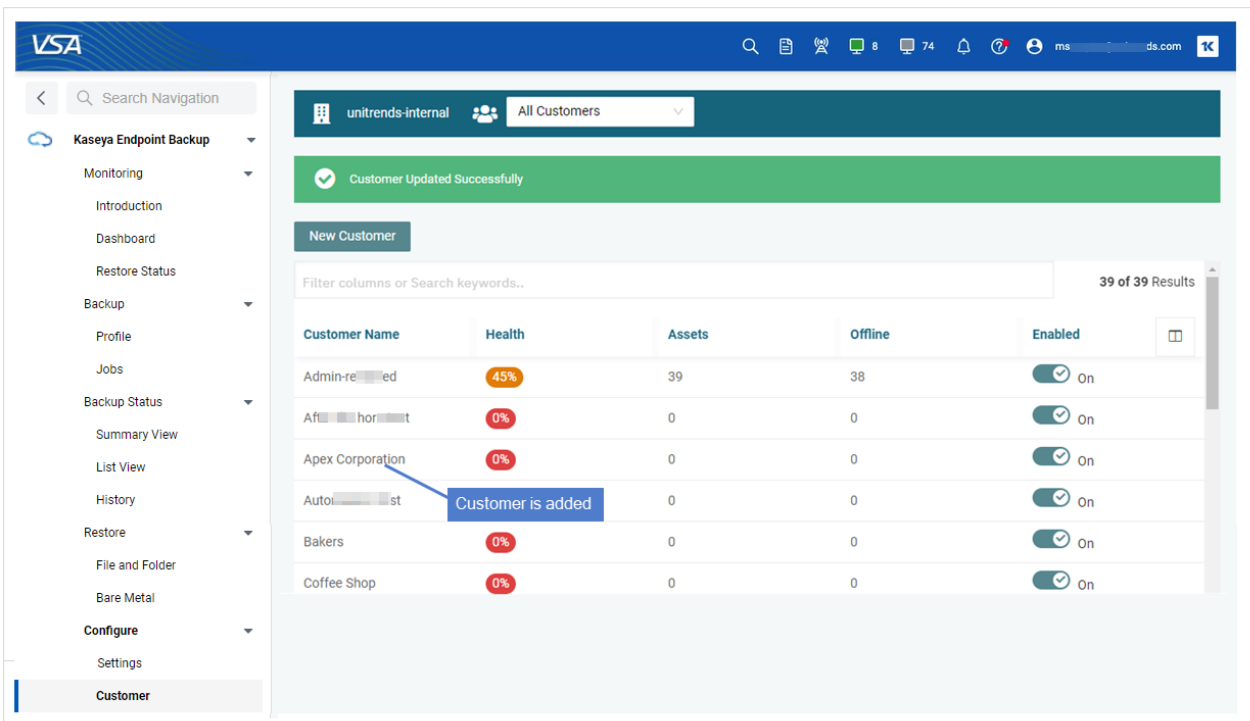
Notes:

- Kaseya EndPoint Backup comes pre-configured with a *Default* customer. You can opt to use the *Default* customer or add your own customer. If you are an MSP, you will need to add each customer that is using this Kaseya EndPoint Backup instance. If you are an SMB, you will simply create one customer for yourself or use the *Default* customer.
- The agent installer is customer-specific. The script is generated for the *Default* customer (if no other customer has been selected) or for the active customer. Be sure to add a customer if you will not be using the *Default*.

- 1 Select **Configure > Customer**.
- 2 Click **New Customer**.
- 3 Enter the customer name.
- 4 Click **Save**.



5 The customer is added.



Step 5: Install the Kaseya EndPoint Backup agent

Use these procedures to install or upgrade the agent:

- "To install or upgrade the Kaseya EndPoint Backup agent by using a VSA agent procedure"
- "To install or upgrade the agent manually on a single asset"

To install or upgrade the Kaseya EndPoint Backup agent by using a VSA agent procedure

This procedure installs the Kaseya EndPoint Backup agent to one or more machines by using a VSA agent procedure.

- 1 Select **Configure > Assets**.
- 2 Select the customer whose assets you will protect.

Note: The agent installer is specific to the selected customer. Be sure the customer whose asset you will protect displays in the customer context banner before downloading the agent.

- 3 Click **Bulk Installation** to generate a unique access key.

Note: You must run the install procedure within 30 days of generating the access key.

- 4 Copy the access key.

The screenshot shows the VSA Kaseya Endpoint Backup interface. A green notification banner at the top states: "Access key created successfully. Paste this key into your Endpoint Backup deployment procedure: 29RBZxU6T17UU8Mq". Below the banner, there are buttons for "Bulk Installation" and "Single Installation". A table lists assets with columns for Machine ID, Machine Group, Organization, Asset Name, Success Of Last 10 Tasks, Last Seen, Enabled, and Agent Version. A blue callout box labeled "3" points to the access key, and another labeled "2" points to the "Bulk Installation" button. A blue callout box labeled "1" points to the "Assets" link in the left sidebar.

Machine ID	Machine Group	Organization	Asset Name	Success Of Last 10 Tasks	Last Seen	Enabled	Agent Version
v-1-22-staging-	base	myorg	v-1-22-staging-ucb-199-250	0%	04/19/2022 10:50	ON	1.25.0
v-1-22-staging-	base	myorg	v-1-22-staging-ucb-199-250	0%	12/07/2021 17:28	ON	1.25.0
ws-ka-10168	root	propellerhead	WS-KA-10168	80%	05/20/2022 12:57	ON	1.24.0
			ucb-windows-10-	100%	10/01/2021 15:24	ON	

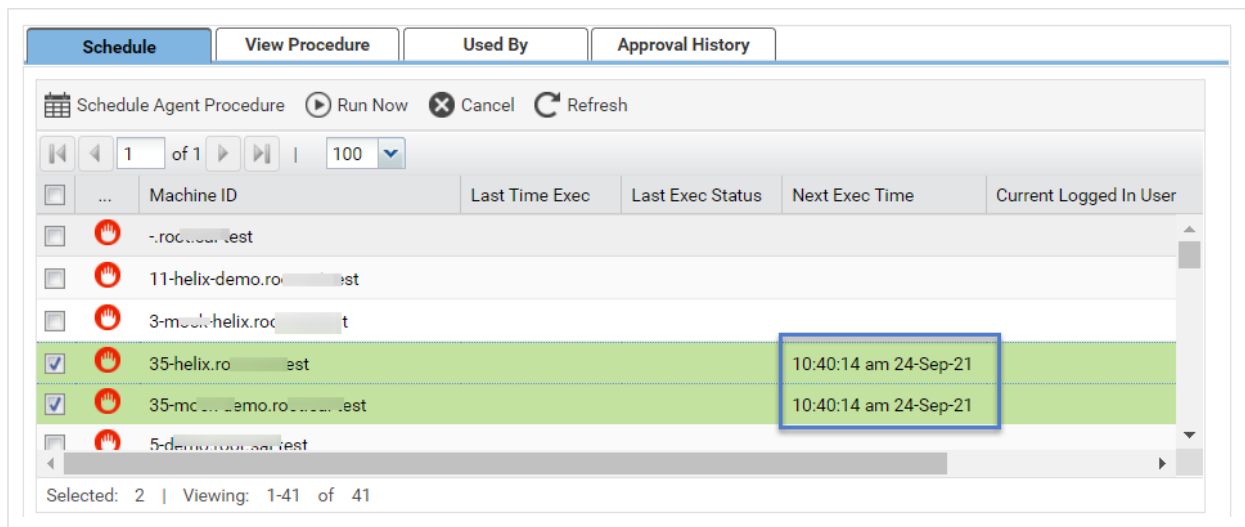
- 5 Select **Agent Procedures > Manage Procedures > Schedule/Create**.
- 6 Under **Shared procedures > Thirdparty App: Kaseya Endpoint Backup**, select **Deploy Endpoint Backup Agent**.
- 7 On the **Schedule** tab, select one or more machine IDs. Click **Run Now**.

The screenshot shows the VSA (Virus Scan Agent) interface. The left sidebar contains a navigation menu with 'Agent Procedures' selected. The main area displays the 'Deploy Endpoint Backup Agent' procedure details, including its name, modified date, and description. Below the details, there are tabs for 'Schedule', 'View Procedure', 'Used By', and 'Approval History'. The 'Schedule' tab is active, showing a table of machines to be scheduled. The table has columns for 'Machine Id', 'Last Time Exec', 'Last Exec Status', and 'Next Exec Time'. Two machines are selected, highlighted in green. A 'Run Now' button is visible above the table. Numbered callouts (1-5) indicate key UI elements: 1 points to the 'Agent Procedures' menu, 2 to the 'Schedule / Create' sub-menu, 3 to the 'Deploy Endpoint Backup Agent' procedure in the tree, 4 to the 'Select machine IDs' button, and 5 to the 'Run Now' button.

8 Enter the Access Key and click **Submit**.

The screenshot shows the 'Script Prompts' dialog box. It contains an information icon and the text 'Schedule Agent Procedure'. Below this, there is a field for 'Access Key:' with the value '1y...g...f3J' entered. A 'Submit' button is visible at the bottom right. Numbered callouts (1 and 2) indicate key UI elements: 1 points to the 'Access Key' input field, and 2 points to the 'Submit' button.

9 The install procedure is added and will run upon the next agent check-in. Look at the Next Exec Time column to see a machine's next agent check-in time:



Once the agent has been deployed, the asset displays on the **Kaseya EndPoint Backup > Configure > Assets** page. The asset name changes from *Unregistered* to the machine's host name once the agent checks in.

Note: If you do not see the asset on the **Configure > Assets** page, see "[Troubleshooting Kaseya EndPoint Backup agent installs](#)" for next steps.

To install or upgrade the agent manually on a single asset

This procedure installs the Kaseya EndPoint Backup agent to one machine by using PowerShell.

Notes:

- You can opt to install to a single asset by using a VSA agent procedure (as described in "[To install or upgrade the Kaseya EndPoint Backup agent by using a VSA agent procedure](#)"). Use this procedure if you prefer to install by using the PowerShell installer, *deploy_cloud_backup_agent.ps1*.
- You must run *deploy_cloud_backup_agent.ps1* within 30 days of downloading the file.

- 1 Select **Configure > Assets**.
- 2 Select the customer whose assets you will protect.

Note: The agent installer is specific to the selected customer. Be sure the customer whose asset you will protect displays in the customer context banner before downloading the agent.

- 3 Click **Single Installation**.
- 4 Download *deploy_cloud_backup_agent.ps1* to the Windows asset.

Note: You must run the install procedure within 30 days of downloading *deploy_cloud_backup_agent.ps1*.

The screenshot shows the VSA interface with the following elements:

- Navigation Menu (Left):** Kaseya Endpoint Backup, Monitoring, Introduction, Dashboard, Restore Status, Backup, Profile, Jobs, Backup Status, Summary View, List View, History, Restore, File and Folder, Bare Metal, Configure, Settings, Customer, Users, **Assets** (highlighted with callout 1).
- Header:** unitrends-internal, Admin (highlighted with callout 2), Select a customer.
- Notification:** Download this script to execute a bulk installation through your favorite endpoint management system. An access key is embedded. It is good for up to 30 days.
- Buttons:** Bulk Installation, Single Installation (highlighted with callout 3).
- Table:**

Machine ID	Machine Group	Organization	Asset Name	Success Of Last 10 Tasks	Last Seen	Enabled	Agent Version
v-1-22-staging-	base	myorg	v-1-22-staging-wcb-199-250	0%	04/19/2022 10:50	ON	1.25.0
v-1-22-staging-	base	myorg	v-1-22-staging-wcb-199-250	0%	12/07/2021 17:28	ON	1.25.0
ws-ka-10168	root	propellerhead	WS-KA-10168	80%	05/20/2022 12:57	ON	1.24.0
mb-windows-				100%	10/01/2021 15:24	ON	
- Warning:** This type of file can harm your computer. Do you want to keep deploy_cloud_backup...ps1 anyway? (Keep/Discard buttons, highlighted with callout 4).

- 5 Log in to the Windows asset and launch PowerShell as administrator.
- 6 Issue this command to run the agent install script, where *<FullPath>* is the full path of the location where you saved *deploy_cloud_backup_agent.ps1*: **PowerShell.exe -executionpolicy bypass -File <FullPath>\deploy_cloud_backup_agent.ps1**. Enter **Y** to confirm. Example command text is given here:

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\WINDOWS\system32> PowerShell.exe -executionpolicy bypass -File C:\users\S...m\Downloads\deploy_cloud_backup_agent.ps1
```

- 7 When you see the security warning about running downloaded scripts, press **R** and **Enter** to continue.
- 8 The agent is downloaded and deployed. When deployment is complete, you see a *cleaning up* message.

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\WINDOWS\system32> PowerShell.exe -executionpolicy bypass -File C:\users\...Downloads\deploy_cloud_backup_agent.ps1
Checking permissions
Executing as Administrator
Getting agent download location
Downloading https://ucb-.../Unitrends_Agentx64.msi
Installing cloud backup agent
Cleaning up
PS C:\WINDOWS\system32>
```

- 9 Once the agent is deployed, the asset displays on the **Configure > Assets** page.

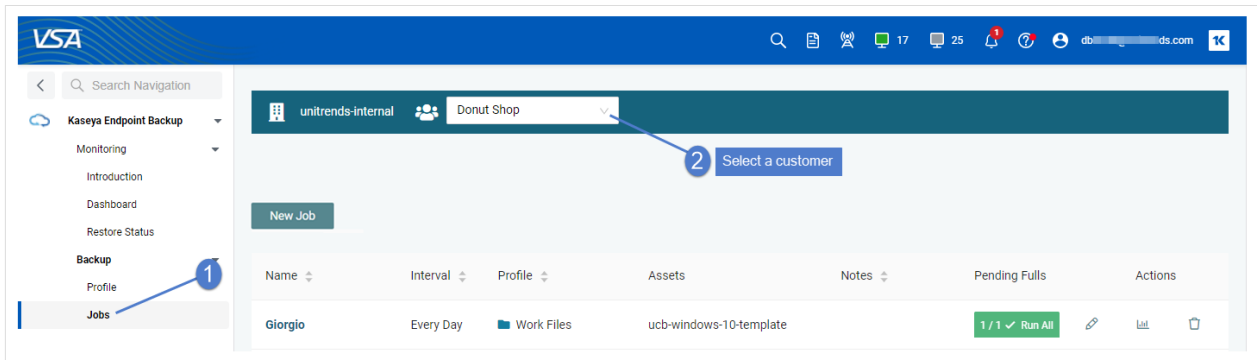
Machine ID	Machine Group	Organization	Asset Name	Success Of Last 10 Tasks	Last Seen	Enabled	Agent Version	Actions
			ws-dpinheiro-01	0%	05/20/2022 13:28	ON	1.25.0	Run Full Run Once Delete
			v15-staging-ucb-199-83	100%	07/07/2020 11:32	ON	1.25.0	Run Full Run Once Delete
			v15-staging-kdcb-199-85	100%	09/28/2020 19:37	ON	1.25.0	Run Full Run Once Delete

Step 6: Run backups

Use the "To create a backup job" procedure to start running backups.

To create a backup job

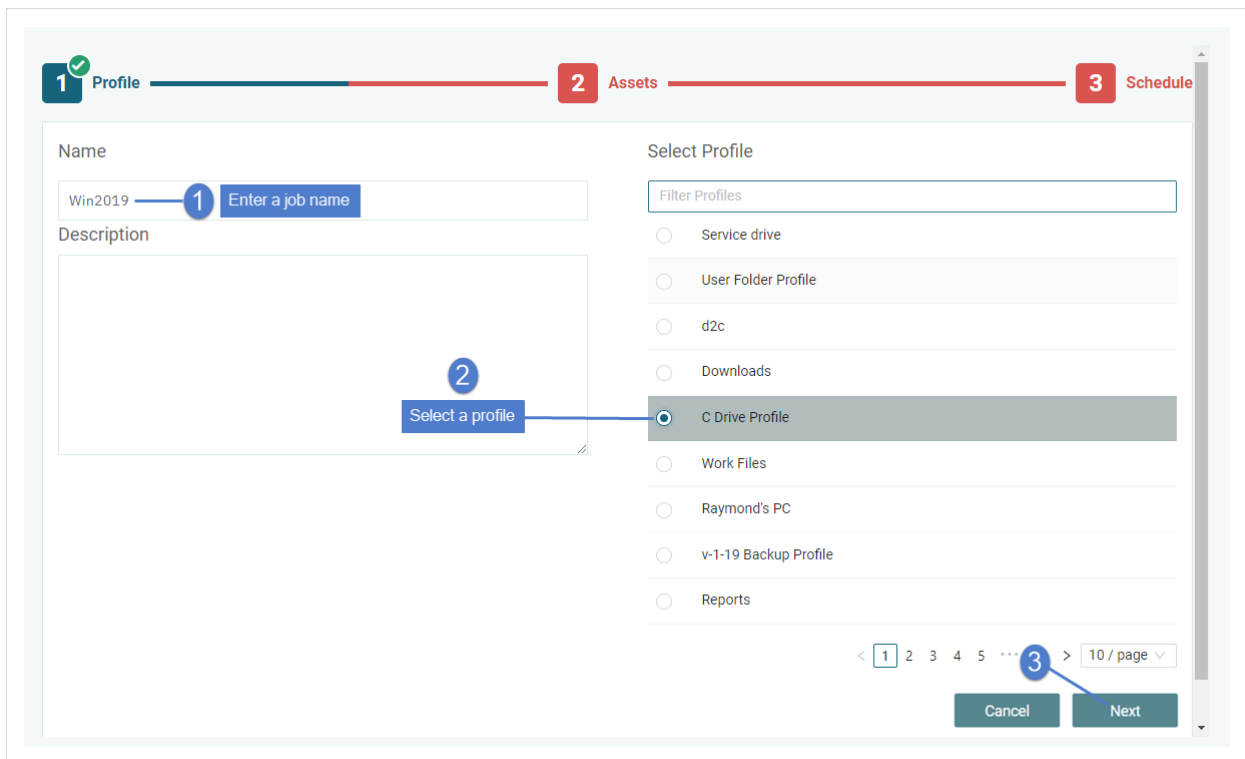
- 1 Select **Kaseya Endpoint Backup > Backup > Jobs**. Click **New Job**.
- 2 Select the customer whose assets you will protect.



3 Enter a name for the job and select a profile in the list. Click **Next**:

Notes:

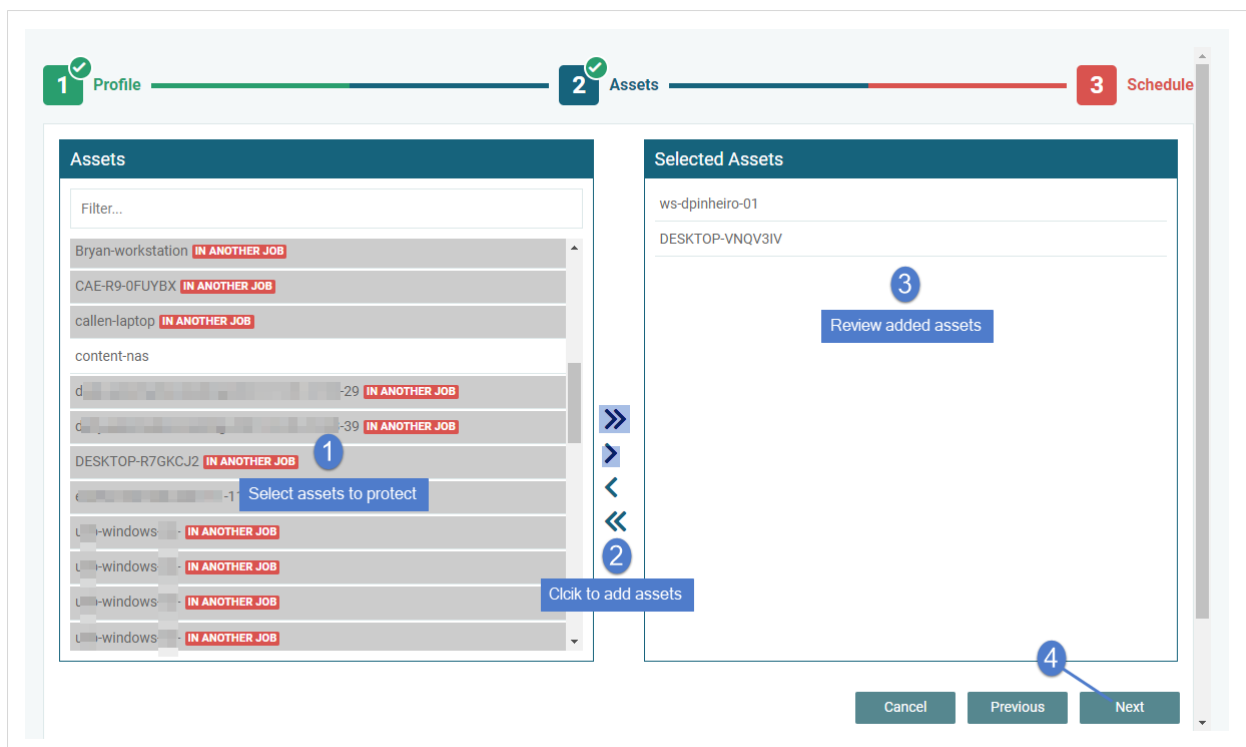
- To recover an entire asset, you must run backups with a *system state* profile (a profile whose Data Type is *System State*). Both system state and file and folder profiles support file-level recovery.
- You can opt to create your own custom profile by clicking **New** on the **Backup > Profile** page.
- For details, see "[Working with backup profiles](#)".



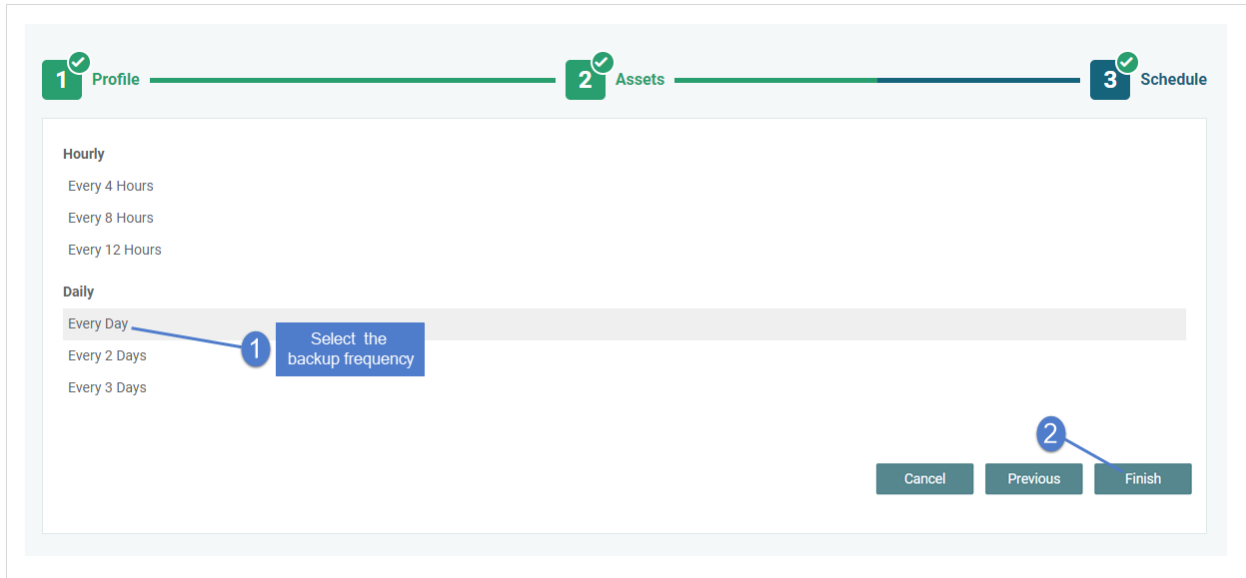
4 Select one or more Assets and click > or >> to add them to the job. Review the Selected Assets. Click **Next**:

Notes:

- The Assets list contains all registered assets for the active customer.
- Newly added assets display in the list as *Unregistered*. The asset name changes from *Unregistered* to the machine's host name once the asset checks in for the first time.
- Assets that are disabled cannot be added to the job. To add the asset to a job, you must first enable the asset (see "To enable or disable an asset").
- Assets that have already been assigned to a job cannot be added to the job. To add the asset to a different job, you must first remove it from the other job (see "Getting Started with Kaseya EndPoint Backup").

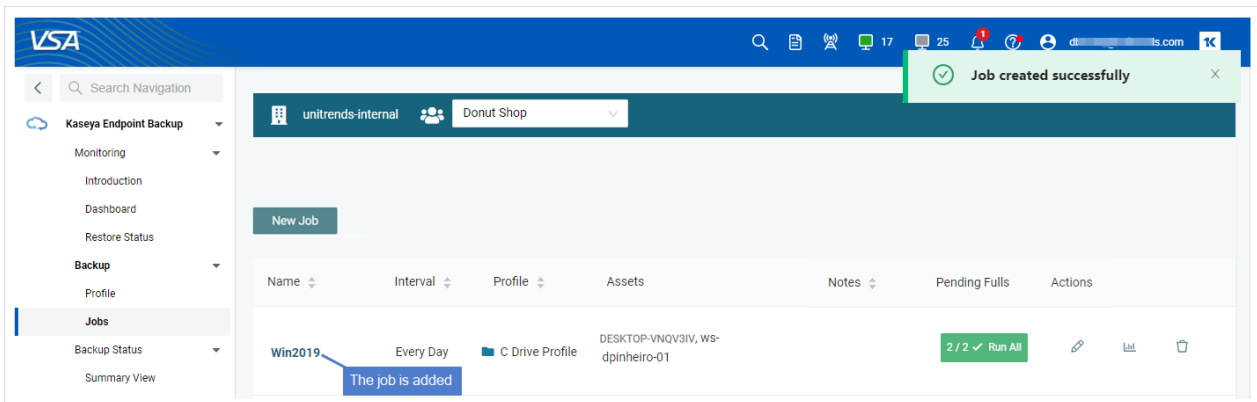


- 5 Define the backup frequency by selecting one of the following: Every 4 Hours, Every 8 Hours, Every 12 Hours, Every Day, Every 2 Days, or Every 3 Days. Click **Finish**:



6 The job is added.

- Jobs are added to the queue (one job for each asset). Select **Kaseya EndPoint Backup > Monitoring > Backup Status** to view the pending and running jobs. For details, see "[Viewing backup status](#)".
- If a job cannot run because an asset is offline, the job runs upon the next agent check-in.
- Subsequent backups will run for each asset at the specified frequency.



Step 7: Recover files

Use the "[To recover files and folders](#)" procedure to recover files. For additional considerations, see "[Recovery considerations](#)".

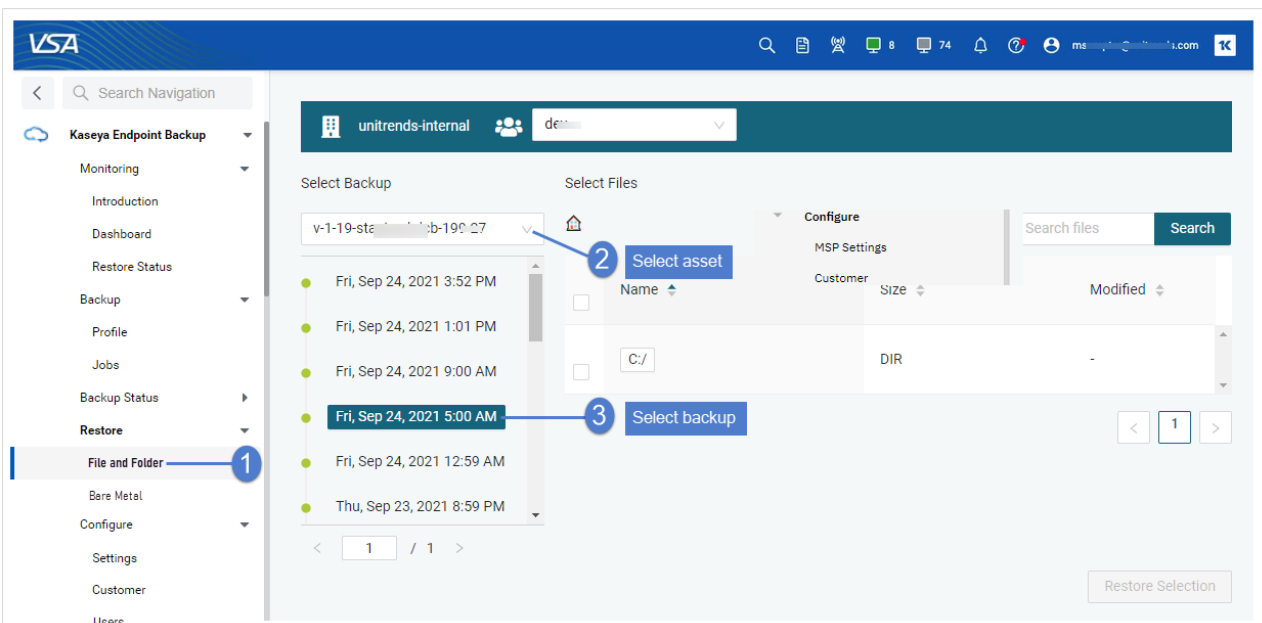
Note: To recover a failed asset from a system state backup, see "Bare Metal Recovery".

To recover files and folders

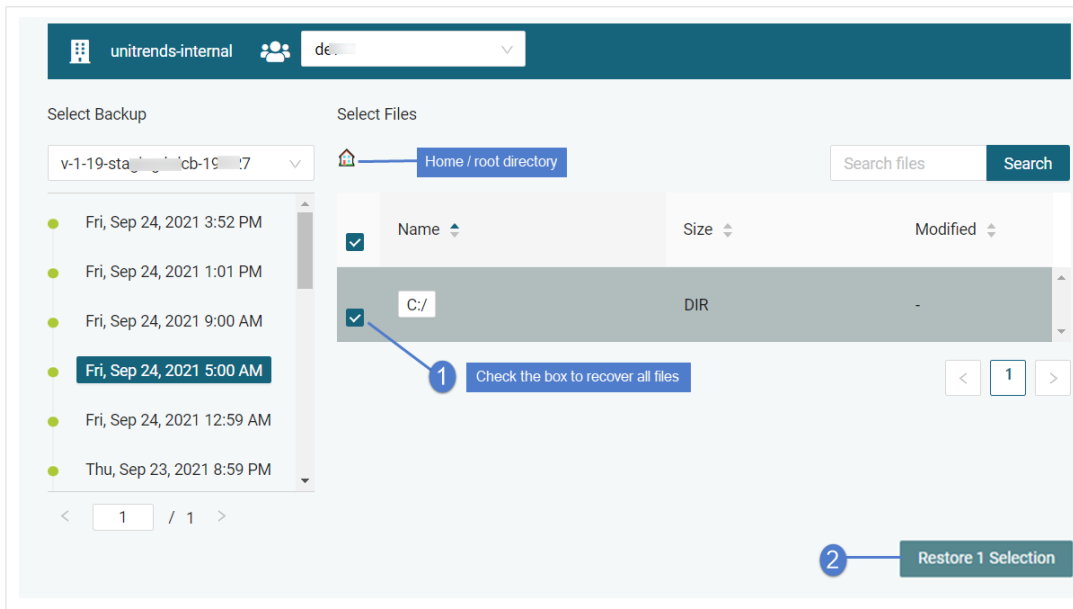
- 1 Select **Restore > File and Folder**.
- 2 Select an asset and the backup to recover:

Notes:

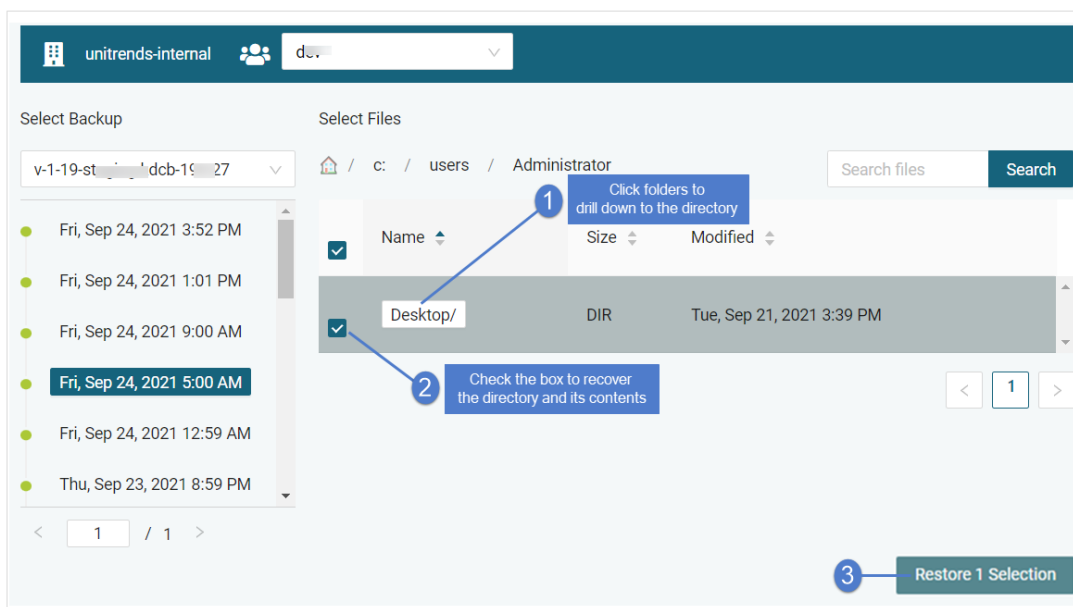
- You can filter the asset list by entering text in the Select Asset field. Only assets containing the string you entered display in the list.
- If the asset has been decommissioned, **DELETED AGENT** displays next to the asset name. You can recover backups of this asset by selecting it in the list, but you must recover the backup to another asset (one that has not been decommissioned).



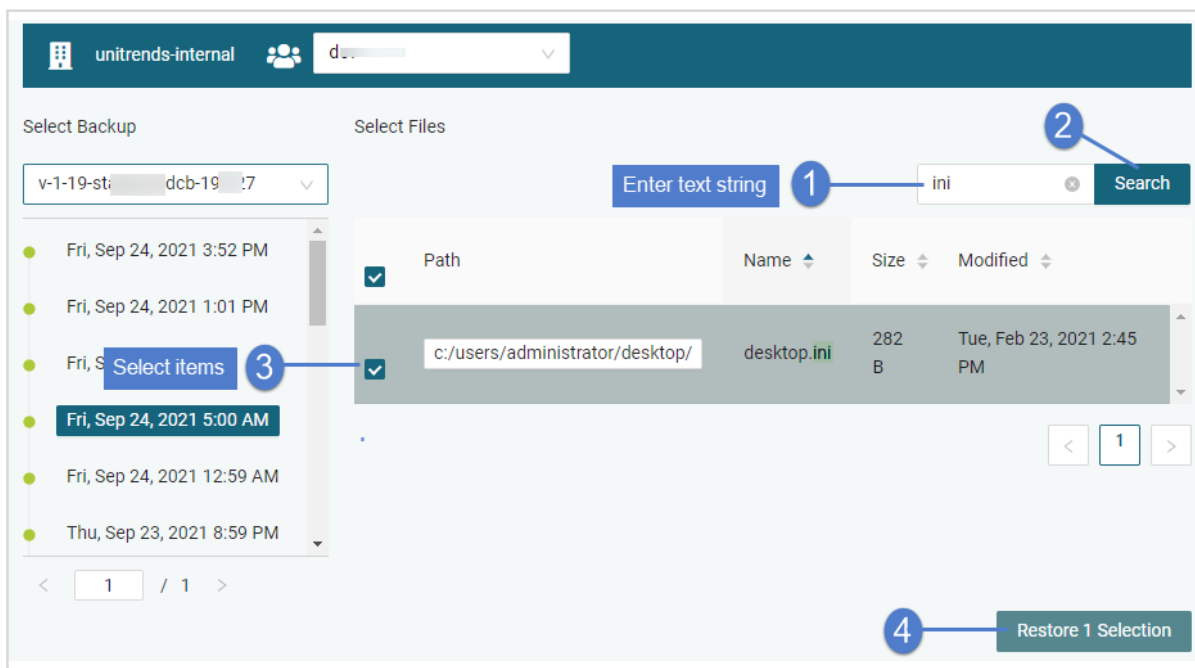
- 3 Select one or more items to recover, then click **Restore Selections**:
 - You can recover all files by selecting the root directory's checkbox.



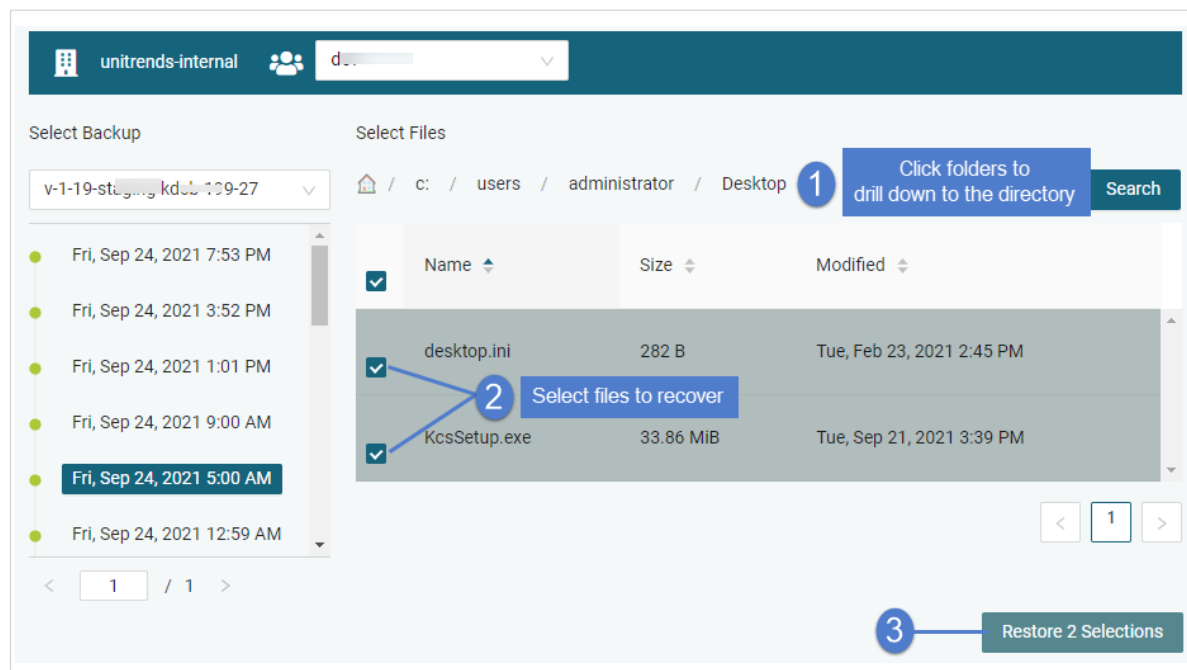
- You can recover the contents of an entire drive or folder by selecting its checkbox.



- You can search for and recover individual files/folders. Enter a text string in the Search Files field, then click **Search**. Files and directory names containing the string you entered display in a list. Check boxes to select items to recover.



- You can recover individual files by browsing the backup contents and selecting one or more files.



4 Select these Advanced Options for the recovery:

- Target Asset – Select the asset where files will be recovered.

Note: Assets that have been deleted or decommissioned are disabled in the list and cannot be used as destination assets.

- Alternate Path – Enter the recovery path on the target asset. Use the default location, `C:/recover`, or enter an alternate path.
- Conflict Resolution – Choose how to handle existing files of the same name in the target directory: select **Overwrite** to replace the file with the one you are recovering or **Preserve Newer** to keep the existing file only if it is newer than the one selected for recovery (otherwise overwrite the existing file).

Note: The Preserve Newer option is not used for files where the fully qualified file path is greater than 251 characters. In this case, the existing file is overwritten. This is a known issue that will be addressed in an upcoming release.

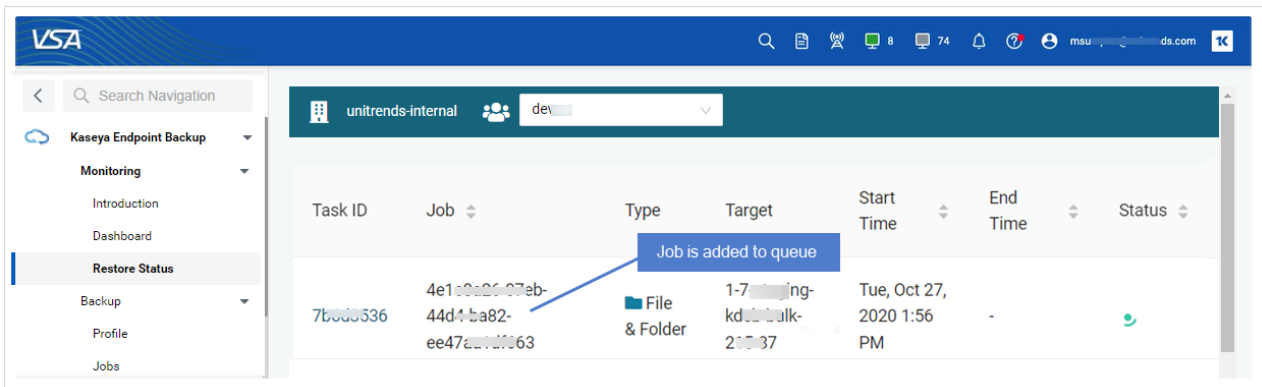
- Folder Structure – Choose **Preserve** to recover the existing folder structure under the target directory or **Flatten** to recover only the files to the target directory.

5 Click **Confirm Restore**.

The screenshot shows a dialog box titled "Selected Files and Folders" with a close button (X) in the top right corner. Inside the dialog, there is a list of files to be recovered: "c:/users/administrator/desktop/desktop.ini" and "c:/users/administrator/desktop/kcssetup.exe". A blue button labeled "List of items to recover" is positioned to the right of the file list. Below the list, there are "Advanced Options" including: "Target Asset" (1-7-s...cb-b...15-87), "* Restore Path" (C:/recover), "Conflict Resolution" (Preserve Newer), and "Folder Structure" (Preserve). At the bottom of the dialog are "Cancel" and "Confirm Restore" buttons. A blue callout box with the number "1" points to a button labeled "Select Advanced Options" which is partially obscured by the "Conflict Resolution" dropdown. Another blue callout box with the number "2" points to the "Confirm Restore" button.

6 The job is added to the queue and displays on the Restore Status page. Files are recovered to the destination asset.

- If the recovery path directory does not exist, the job creates it during the recovery.
- If the destination asset is not online, the job runs upon the next agent check-in.

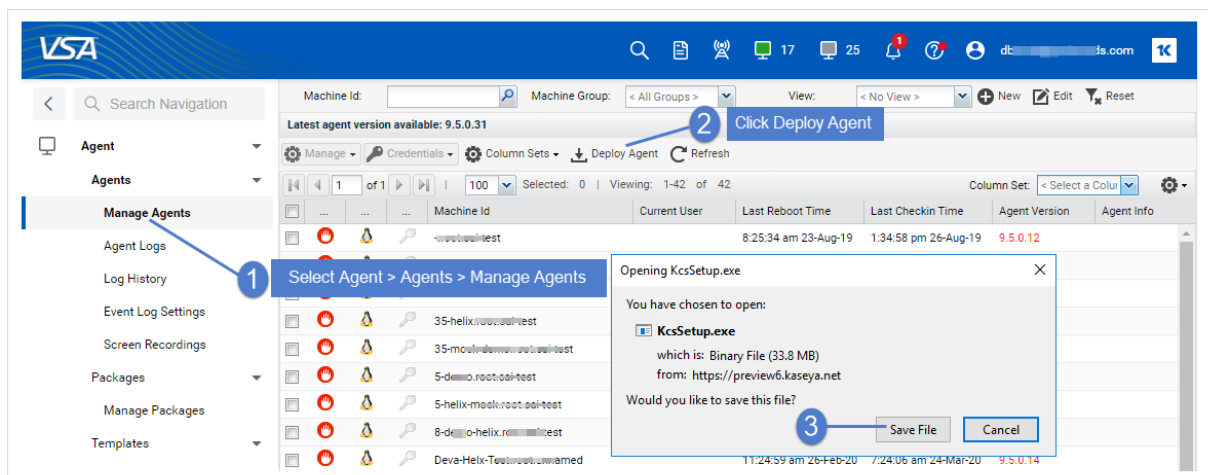


Installing the VSA agent

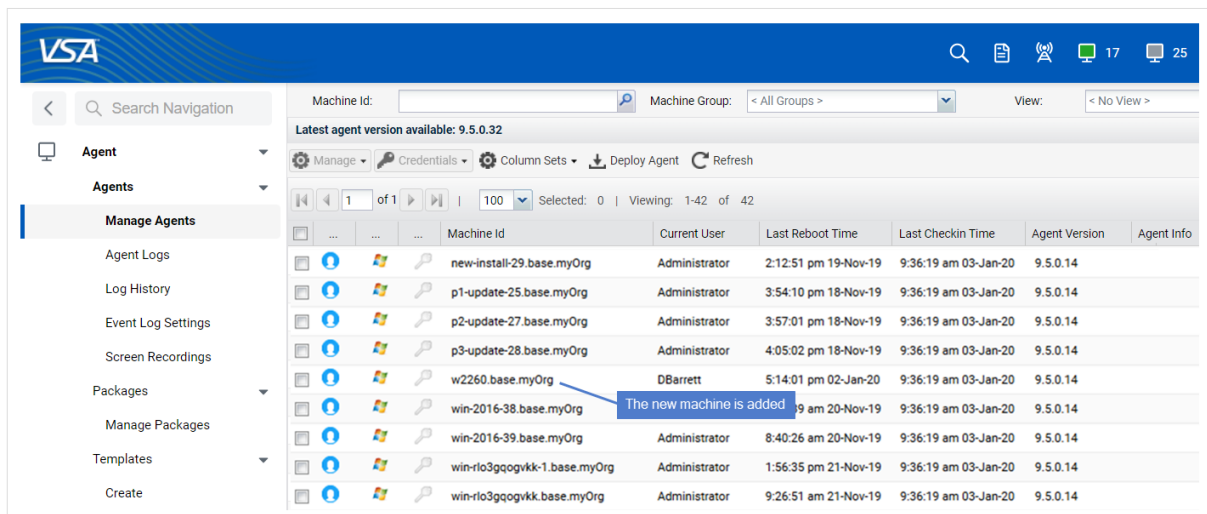
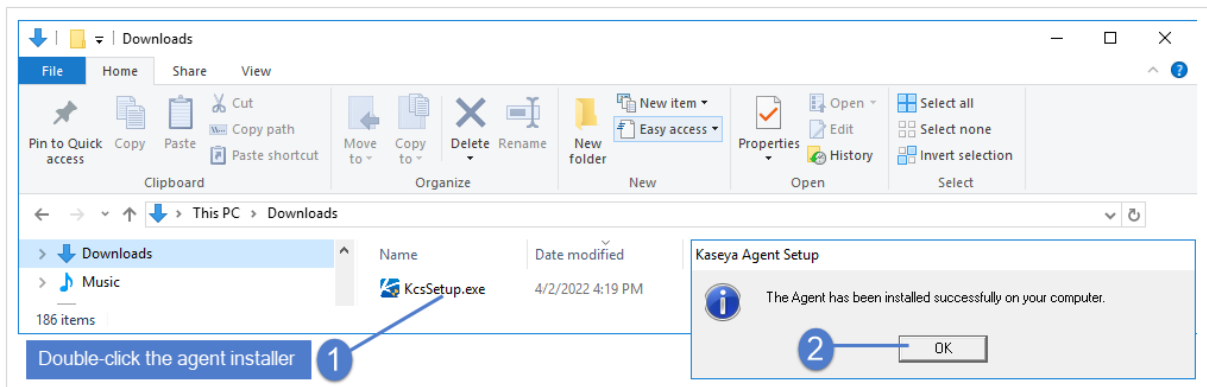
Use this procedure to install or upgrade the VSA agent.

To install the VSA agent

- 1 Log in to the Windows asset as administrator.
- 2 Open a browser and log in to the VSA.
- 3 Select **Agent > Manage Agents**.
- 4 Click **Deploy Agent**, then **Save File**.



- 5 In Windows Explorer, browse to the download location and double-click the agent installer, **KcsSetup.exe**. The VSA agent is installed.
- 6 Click **OK** to close the Kaseya Agent Setup message.



Troubleshooting Kaseya EndPoint Backup agent installs

If you have installed the Kaseya EndPoint Backup agent but the machine does not display on the **Kaseya Endpoint Backup > Configure > Assets** page, check the agent procedure log messages and address any error conditions.

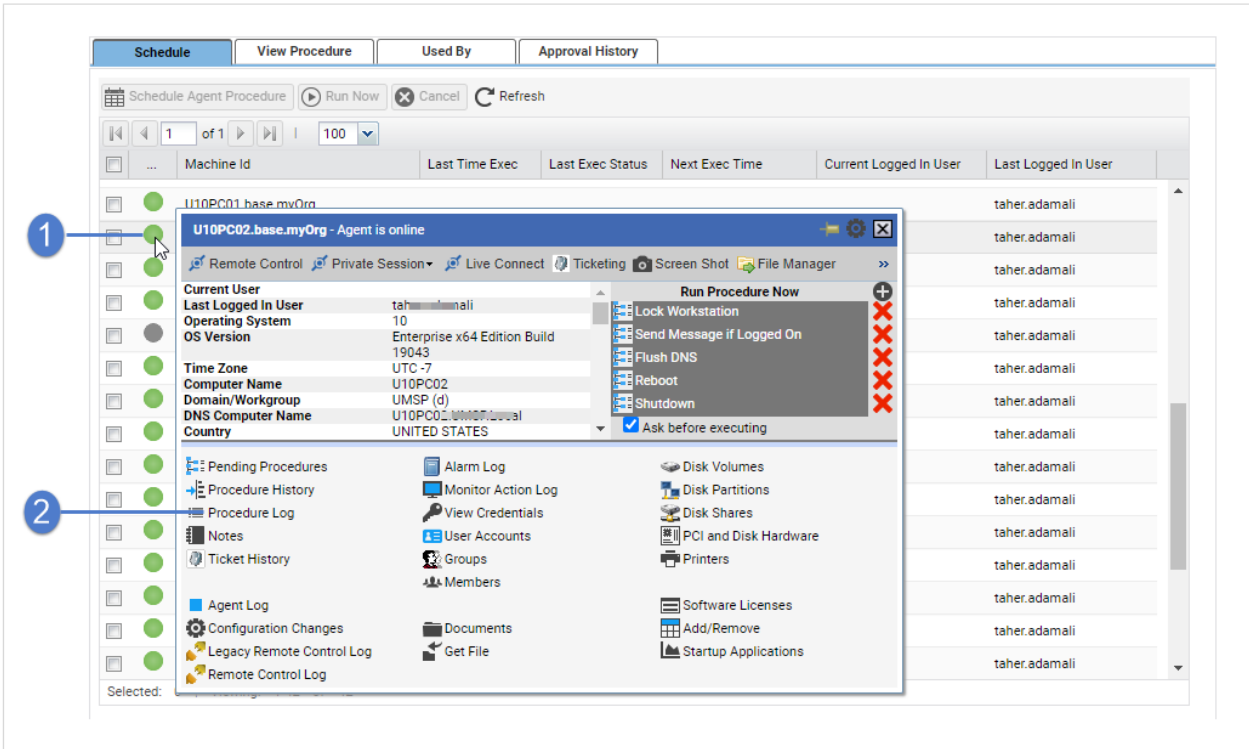
To view the agent procedure log

- 1 Select **Agent Procedures > Manage Procedures > Schedule/Create**.
- 2 Under **Shared procedures > Thirdparty App: Kaseya Endpoint Backup**, select **Deploy Endpoint Backup Agent**.

The screenshot shows the VSA interface for configuring and scheduling a procedure. The left navigation pane is expanded to 'Agent Procedures' (1) and 'Schedule / Create' (2). The main area displays the 'Deploy Endpoint Backup Agent' procedure details, including its name, modified by, date modified, approved status, and description. The 'Schedule' tab is active, showing a table of machines with columns for 'Machine Id', 'Last Time Exec', 'Last Exec Status', and 'Next Exec Time'. A blue circle '3' highlights the agent check-in icon for the machine 'U10PC01.base.myOrg'.

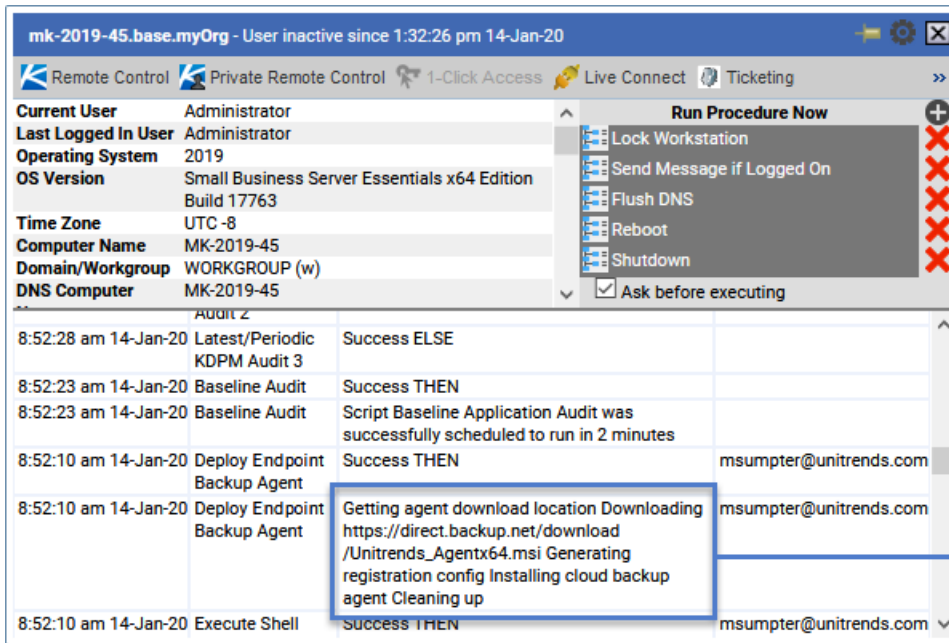
Machine Id	Last Time Exec	Last Exec Status	Next Exec Time
U10PC01.base.myOrg			
U10PC02.base.myOrg			
u10pc03.base.myOrg			
u10pc04.base.myOrg			
U16APP01.base.myOrg			
U16APP02.base.myOrg			
U19DC01.base.myOrg			

- 3 On the Schedule tab, hover over the machine's agent check-in icon to launch the agent Quick View window.
- 4 Click **Procedure Log**.



5 Check the log for Deploy EndPoint Backup Agent messages.

- Example agent install success message:



- Example agent install failure message:

The screenshot shows a remote control session for 'cae-r9-035gw1.base.myOrg'. The 'Run Procedure Now' menu is open, showing options like 'Lock Workstation', 'Send Message if Logged On', 'Flush DNS', 'Reboot', and 'Shutdown'. Below the menu is a table of recent procedures:

Time	Procedure	Description	Admin
8:11:11 am 16-Jan-20	Deploy Endpoint Backup Agent	Success THEN Endpoint	msumpter@unitrends.com
8:11:11 am 16-Jan-20	Deploy Endpoint Backup Agent	File C:\temp\deploy_cloud_backup_agent.ps1 cannot be loaded because running scripts is disabled on this system. For more information, see about_Execution_Policies at http://go.microsoft.com/fwlink/?LinkID=135170 . + CategoryInfo: SecurityError (:) [], ParentContainsErrorRecord Exception + FullyQualifiedErrorId: UnauthorizedAccess	msumpter@unitrends.com
8:11:11 am 16-Jan-20	Execute Shell command - Get Results to	Success THEN	msumpter@unitrends.com

A callout box highlights the error message in the second row of the table. A blue box on the right says 'This means agent install failed'.

This page is intentionally left blank.



Chapter 2: Accessing Kaseya EndPoint Backup

You can log in to Kaseya EndPoint Backup by using your Kaseya EndPoint Backup credentials or by using IT Complete. IT Complete links your Kaseya EndPoint Backup and KaseyaOne accounts to enable single sign-on.

Use these procedures to access Kaseya EndPoint Backup:

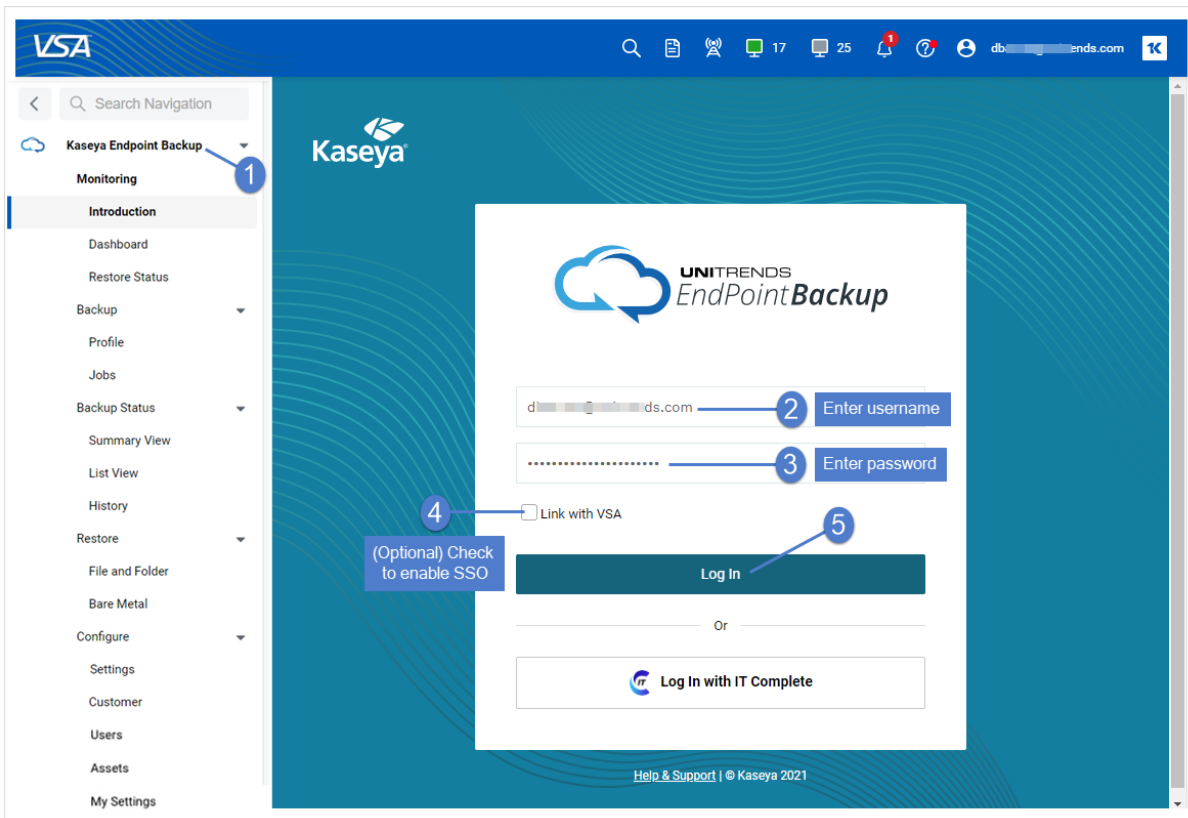
- ["To log in using Kaseya EndPoint Backup credentials"](#)
- ["To enable login with IT Complete"](#)

To log in using Kaseya EndPoint Backup credentials

- 1 Log in to the VSA.
- 2 Select **Kaseya Endpoint Backup**.
- 3 Enter the username and password of your Kaseya EndPoint Backup account.
- 4 (Optional) Check the **Link with VSA** box to link your Kaseya EndPoint Backup and VSA accounts.

Upon logging in, your VSA account is linked and you no longer need to supply separate credentials to access the Kaseya EndPoint Backup module.

- 5 Click **Log In**.



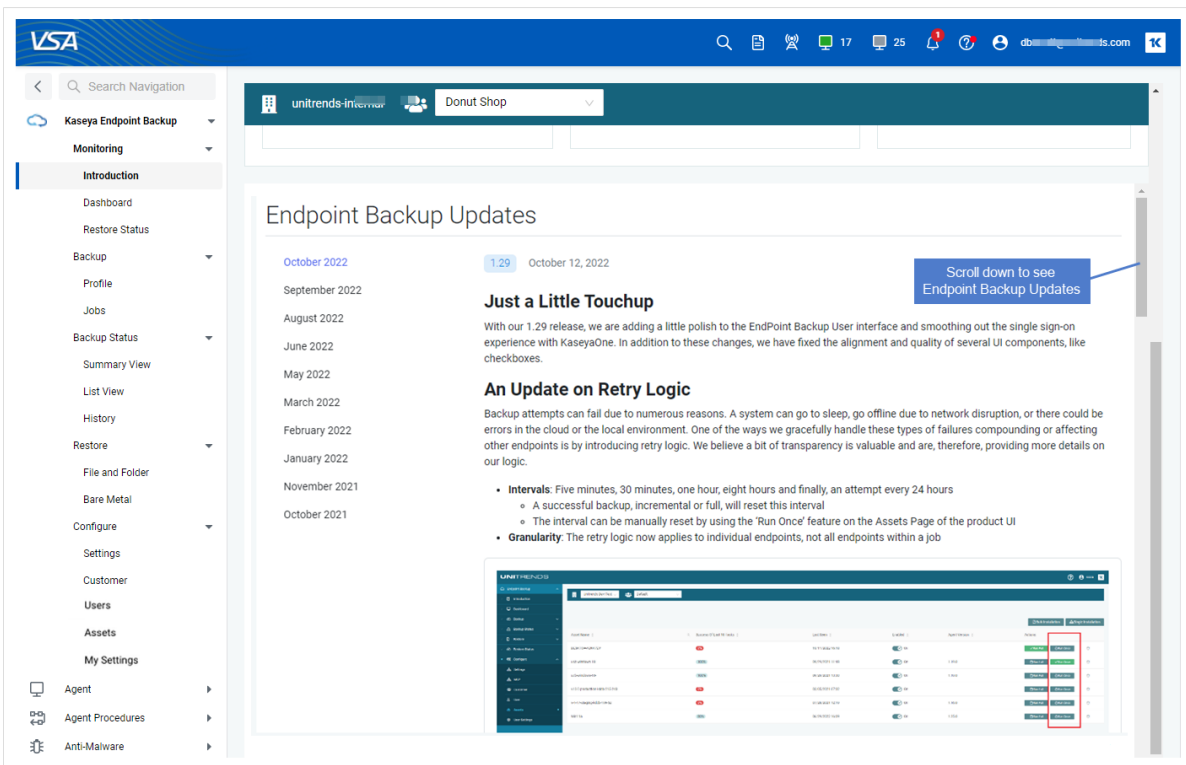
6 The Introduction page displays.

The screenshot displays the VSA Kaseya EndPoint Backup web interface. The top navigation bar includes the VSA logo, a search bar, and user information for 'unitrends-internal' and 'Admin'. The left sidebar contains a navigation menu with categories like 'Monitoring', 'Introduction', 'Backup', 'Restore', and 'Configure'. The main content area is titled 'Getting Started' and provides instructions on how to begin protecting endpoints. It features three numbered steps:

- 1 Deploy Agents**: Includes a button 'Deploy Agents to Your Assets' and instructions for 'Single Installation' (downloading the package) and 'Bulk Installation' (using a 24-hour key).
- 2 Create Backup Jobs**: Includes a button 'Configure Backups' and instructions on defining jobs and monitoring progress.
- 3 Recover Files & Folders**: Includes a button 'Recover Files' and instructions on selecting files to restore.

Below these steps, there is a section for 'Endpoint Backup Updates'.

To stay up to date on the latest releases and changes, scroll down to view EndPoint Backup Updates:

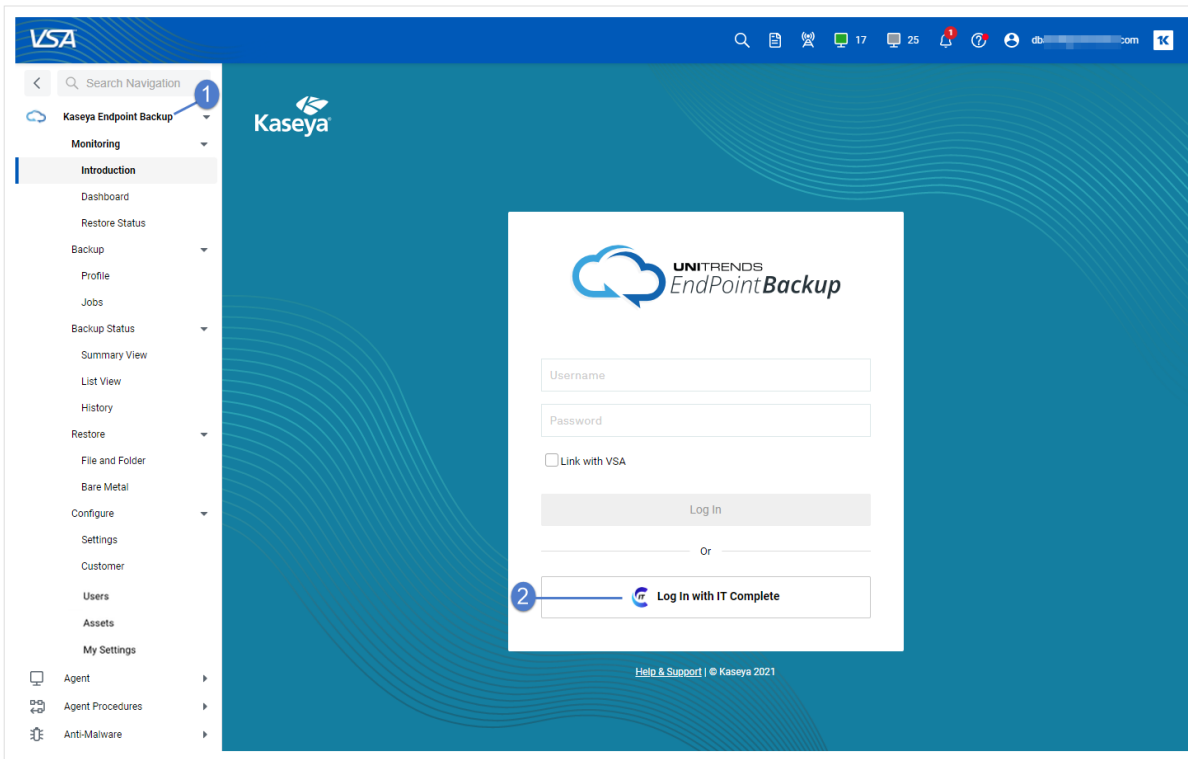


To enable login with IT Complete

[IT Complete](#) is Kaseya's integrated platform of IT and security management solutions. Use this procedure to enable single sign-on by linking your Kaseya EndPoint Backup and KaseyaOne account credentials.

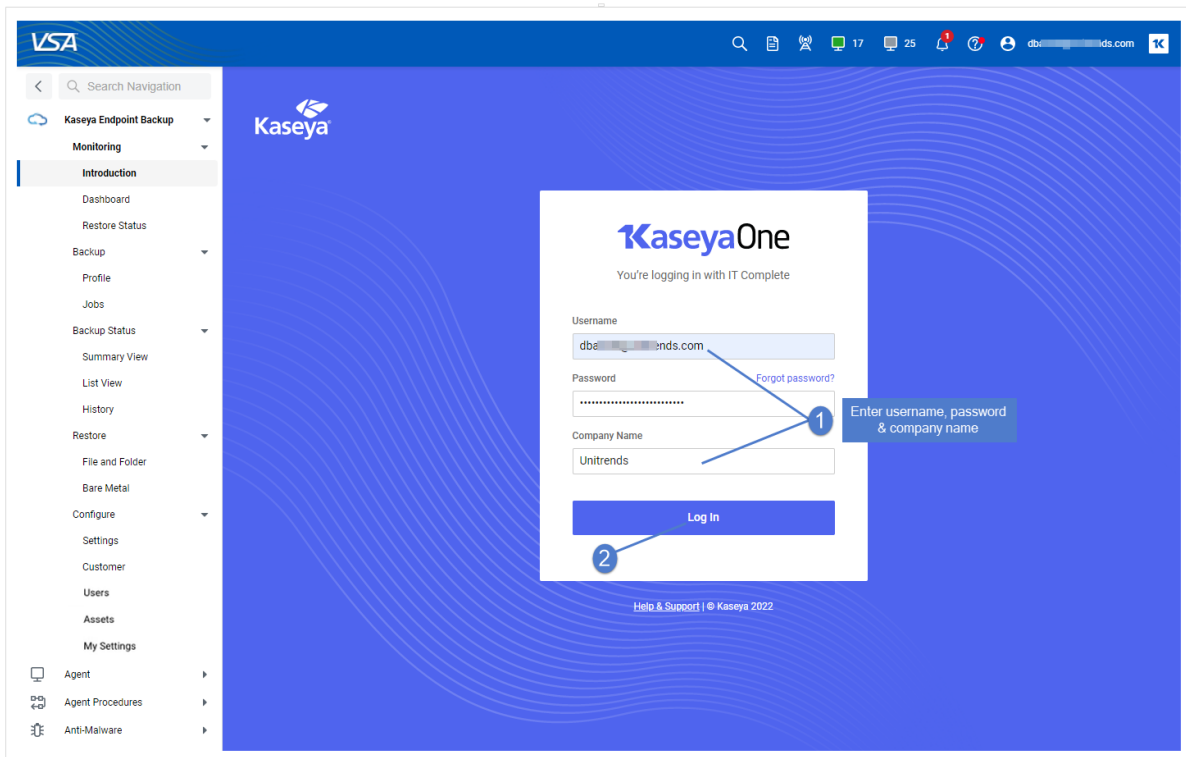
- 1 Log in to the VSA.
- 2 Select **Kaseya EndPoint Backup**.
- 3 Click **Log in with IT Complete**.

Note: If you do not see the *Log in with IT Complete* button, your organization has not been registered with IT Complete. Register your organization as described in "[Working with Kaseya EndPoint Backup Settings](#)" on [page 129](#).



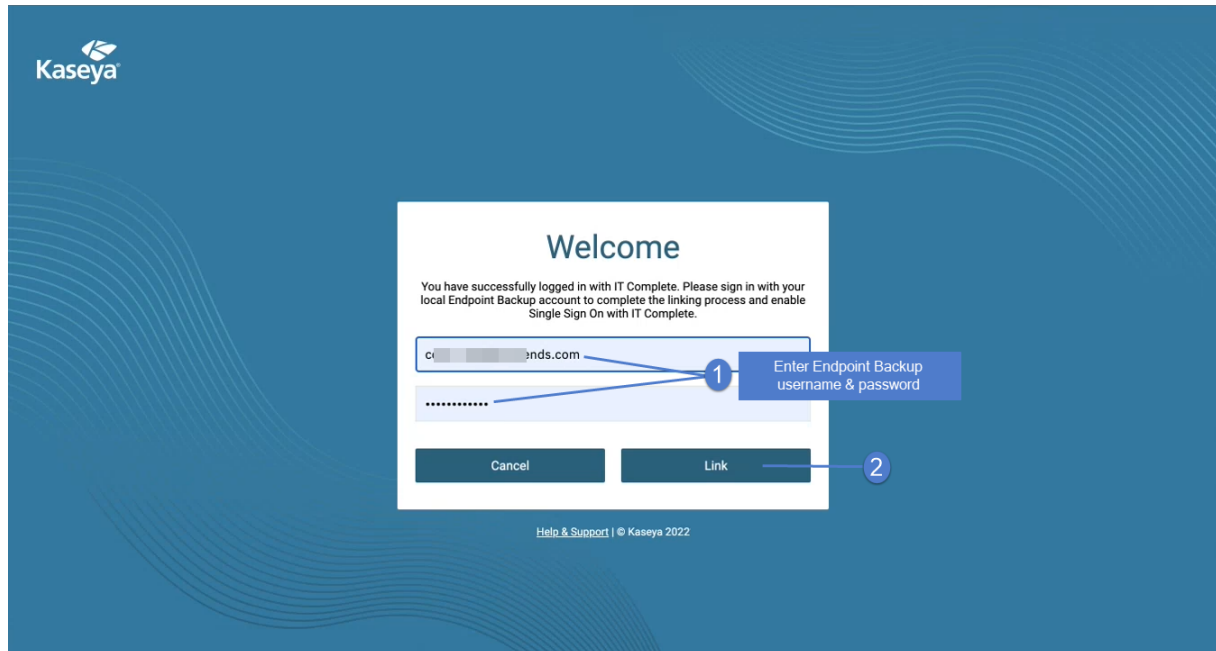
- 4 If prompted, enter your KaseyaOne username, password, and company name. Click **Log in**.

Note: If you are currently logged in to KaseyaOne, you are not prompted to enter your KaseyaOne account credentials.

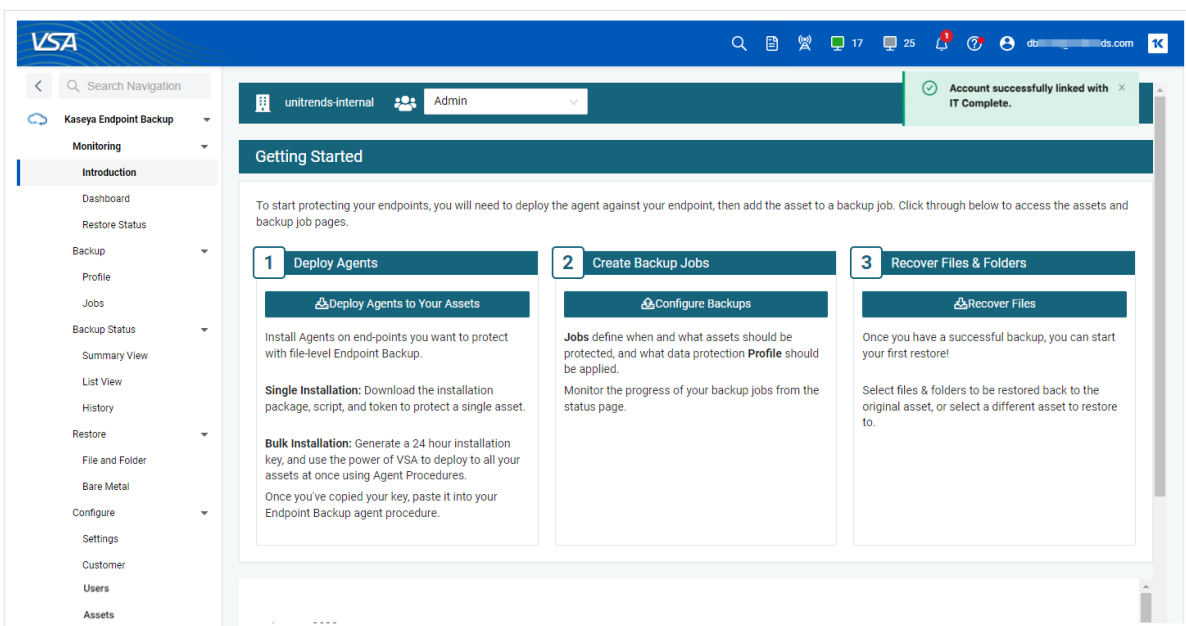


- 5 If prompted, enter your Kaseya EndPoint Backup username and password. Click **Link**.

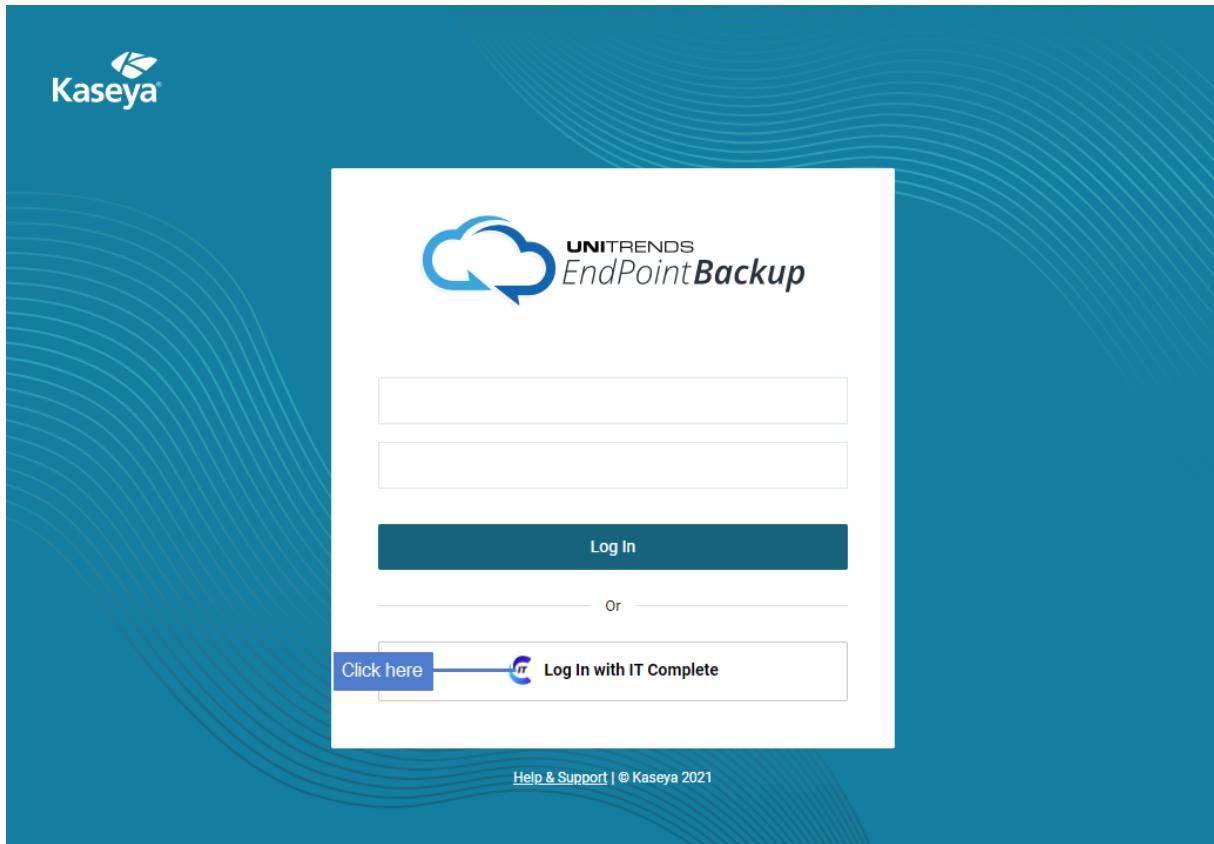
Note: This is required only if you have not yet linked your Kaseya EndPoint Backup and KaseyaOne account credentials.



- 6 You are logged in to Kaseya EndPoint Backup and the Introduction page displays.



- 7 The next time you log in, simply click **Login with IT Complete** without entering any Kaseya EndPoint Backup credentials:



Chapter 3: Protecting Assets with Kaseya EndPoint Backup

Kaseya EndPoint Backup provides protection of Windows assets. All data protection strategies begin with backups, which are duplicates of your data. Kaseya Direct to Cloud Backup utilizes the *incremental forever* protection strategy, where the first backup of an asset is a full backup that includes all specified file system data. After the first full backup completes, subsequent backups are incrementals that capture a subset of data that has changed since the last backup. Each backup functions as a recovery point for the protected asset. After you've backed up your assets, you can recover individual files or entire file systems in minutes. Or recover an entire failed asset back to the same hardware, dissimilar or virtualized.

Customize your backup strategy to meet the recovery point objectives (RPOs) required for your business continuity plan. RPOs refer to the maximum amount of data loss that you can tolerate. For example, if you can tolerate losing a day's worth of data, your RPO is one day. To meet your RPOs, use profiles and job schedules to run backups at the desired frequency.

This chapter provides instructions for creating and managing backup profiles and jobs. A *backup profile* defines the data to include in the backup. Once you have created the desired profile, you apply it to a backup job. See the following topics for details:

- ["Backup considerations"](#)
- ["Working with backup profiles"](#)
- ["Working with backup jobs"](#)

Backup considerations

Consider the following before you implement your protection strategy:

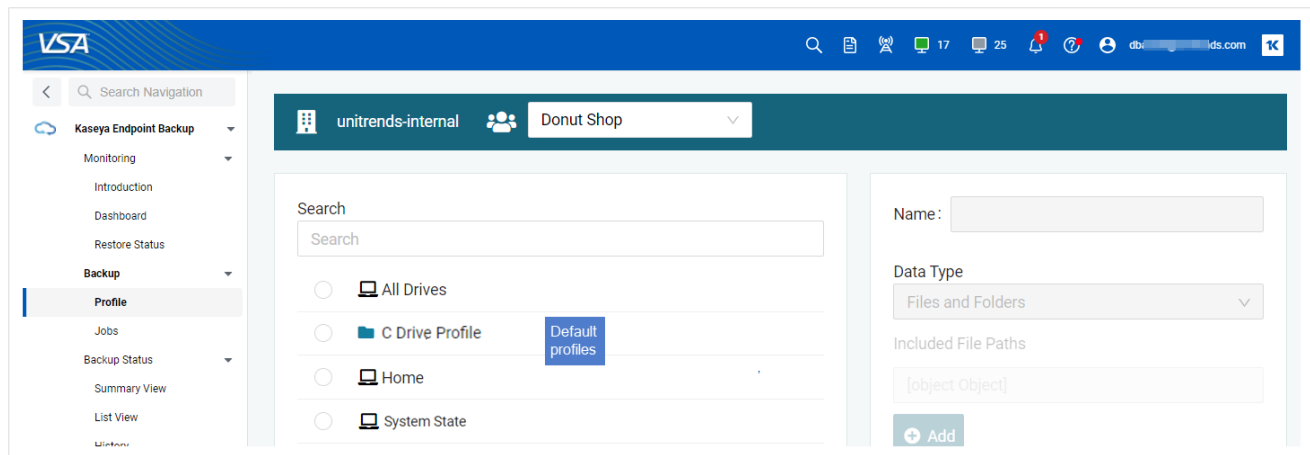
- Kaseya EndPoint Backup is ideal for workstations and laptops running Windows client operating systems. Server operating systems are supported as well, but ensure you consider the recovery requirements of the server and its applications. Kaseya Unified Backup is typically a better fit for protecting and recovering servers and is REQUIRED when protecting hosted applications, like SQL Server, Exchange, SharePoint, and Oracle.
- Kaseya EndPoint Backup protects Windows filesystems with *file and folder* backups or the entire Windows asset with *system state* backups. You can quickly recover files and folders from all backups. System state backups add the ability to recover the entire asset by using the ["Bare Metal Recovery"](#) feature.
- Unlike a file and folder backup, a system state backup includes the system state and must contain all critical volumes. System state backups are typically larger in average than targeted data backups.
- Kaseya recommends running incremental backups each day.
- The first backup of a given asset is always a full backup. Be aware that a full backup can take quite some time to complete, depending on the backup size and available bandwidth in your environment.

- Kaseya EndPoint Backup provides offsite backup storage in the Kaseya Cloud. Kaseya offers these backup retention options: 90 days, 1 year, and Infinite. Check your service level agreement to see how long your backups are retained in the Cloud.

Working with backup profiles

While creating a backup job, you apply a profile that defines the data to include in the backup. The profile's Data Type indicates the type of backup to run: *Files and Folders* or *System State*. A given profile can be applied to multiple jobs within your Kaseya EndPoint Backup environment. You can choose one of the default profiles or create a custom profile. These profiles are available by default:

- Home – Use to back up the contents of the Windows home directory, *C:\Users*, with file and folder backups.
- C Drive – Use to back up the contents of the C drive, *C:*, with file and folder backups.
- All Drives – Use to back up the contents of all drives with file and folder backups. (Removable media and synchronized drives, such as OneDrive, Google Drive, and Dropbox, are not included in the backup. These drives are automatically excluded from the job.)
- System State – Use to back up the system state and all critical volumes essential to OS functions. A system state backup can be used for both file/folder-level and bare metal recovery.





You can add, modify, and remove backup profiles. See these procedures for details:

- ["To add a backup profile for file and folder backups"](#)
- ["To add a backup profile for system state backups"](#)
- ["To view or edit a backup profile"](#)
- ["To delete a backup profile"](#)

To add a backup profile for file and folder backups

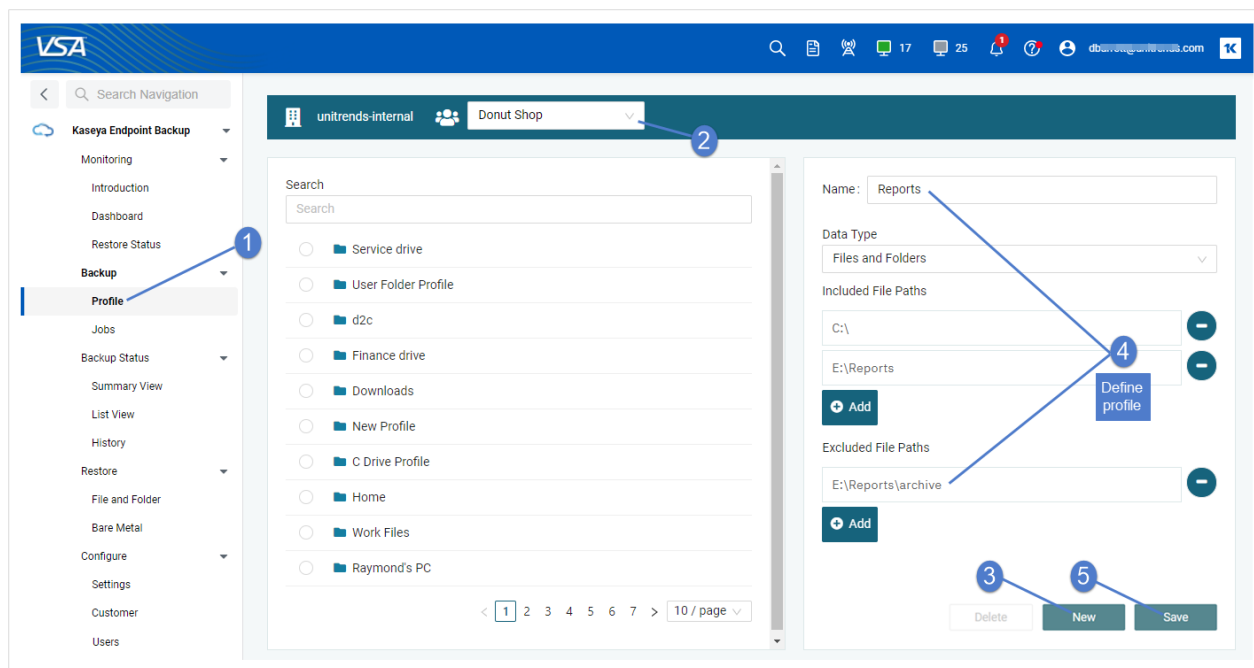
Note: A file and folder backup cannot be used for bare metal recovery (BMR) of a failed asset. For BMR, run system state backups instead.

- 1 Select **Backup > Profile**.
- 2 Select a customer.
- 3 Click **New**.
- 4 Enter a name for the profile.
- 5 Select **Files and Folders** from the Data Type list.
- 6 (Optional) In the Included File Paths field, enter a volume or folder to include in the backup:
 - Data that does not meet the criteria you specify here is NOT included in the backup.
 - Type in the volume or full folder path (e.g., *E:* or *E:\Finance*) to specify data to include. (Wildcards are not supported.)
 - Click **Add** to specify multiple file paths. (Click  to remove a file path.)
 - See "[Considerations for including and excluding files](#)" for additional information.
- 7 (Optional) In the Excluded File Paths field, enter a volume or folder to exclude from the backup:
 - Data that does not meet the criteria you specify here IS included in the backup.
 - Type in the volume or full folder path (e.g., *C:* or *C:\Finance\Customer*) to specify data to exclude. Wildcards are supported.
 - Click **Add** to specify multiple file paths. (Click  to remove a file path.)
 - See "[Considerations for including and excluding files](#)" for additional information.

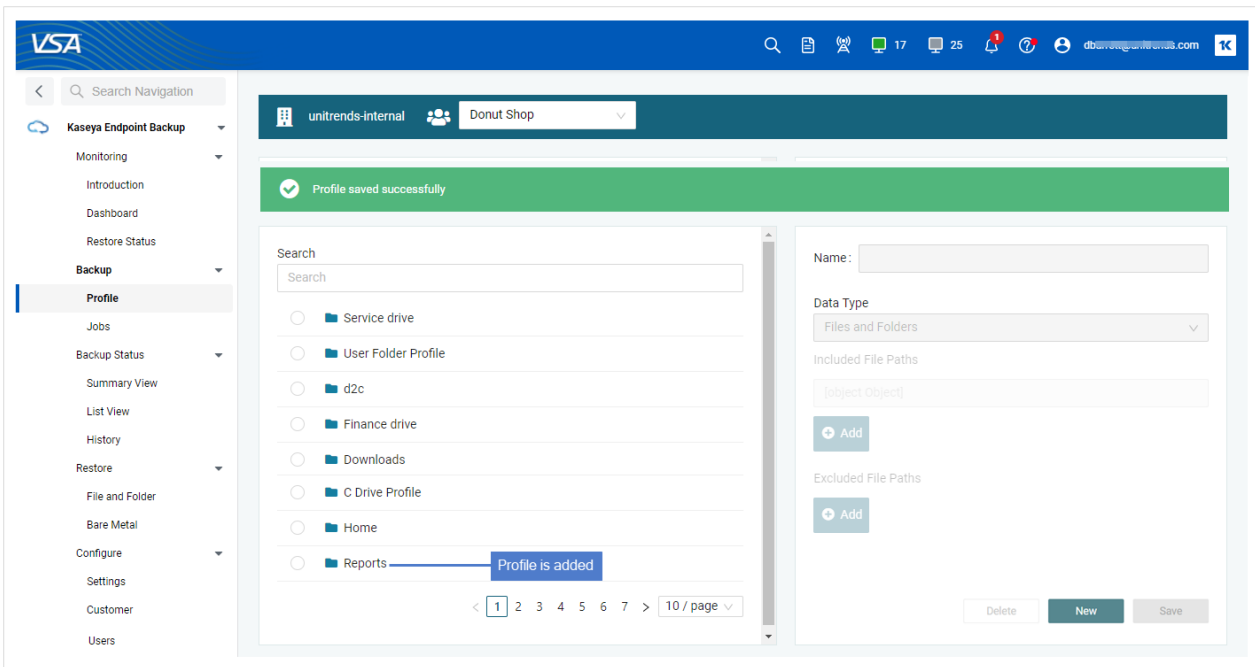
Considerations for including and excluding files

Consideration	Description
General considerations for including or excluding files from an asset's backups	<p>Review the following before specifying files to include or exclude:</p> <ul style="list-style-type: none"> • If you specify both files to include and files to exclude, the inclusion is applied first. Any exclusions are then applied to the subset of included files. • If you do not specify any files to include or exclude, the job includes all drives (other than removable media and synchronized drives, such as OneDrive, Google Drive, and Dropbox). • A new full backup is required upon adding, removing, or modifying included or excluded file paths. This is also required if you create and apply a new profile to an existing backup job and the included or excluded file paths are different from the job's original profile. If included or excluded files have changed for an incremental job schedule, the system automatically promotes the next backup of each asset to a full backup.
Wildcard * usage in Excluded File Paths	<p>An example of how to exclude all files with zero or more characters that match exclusion pattern:</p> <p style="text-align: center;">*.txt</p> <p>An example of how to exclude directories with zero or more characters and their contents within a specified path that match the exclusion pattern:</p> <p style="text-align: center;">C:/windows/sys*</p> <p>Limitations:</p> <ul style="list-style-type: none"> • *folder_abc cannot be used to exclude all folders that match <i>folder_abc</i> on the protected asset. The full path must be provided. • If an entire directory is excluded, the directory name will still appear in the backup; however, its contents will be empty. • Multiple wildcard matches like the following are not supported: <p style="text-align: center;">C:**\abc.txt</p>
Wildcard ? usage in Excluded File Paths	<p>An example of how to exclude all files within specified path that matches a single character within exclusion pattern:</p> <p style="text-align: center;">C:/PCBP/Lists.dir/pro_client?.spr</p> <p>An example of how to exclude all directories and their contents within specified path that matches a single character within exclusion pattern:</p> <p style="text-align: center;">C:/Programfiles/Case?/</p> <p>Limitation: If an entire directory is excluded, the directory name itself will still appear in the backup; however its contents will be empty.</p>

Consideration	Description
Multiple wildcards in Excluded File Paths	<p>An example that uses multiple “?” wildcards and only one * wildcard:</p> <p style="text-align: center;">C:/?Log?/*.*.logs</p> <p>Limitation: If an entire directory is excluded, the directory name itself will still appear in the backup; however its contents will be empty.</p>



The profile is added:



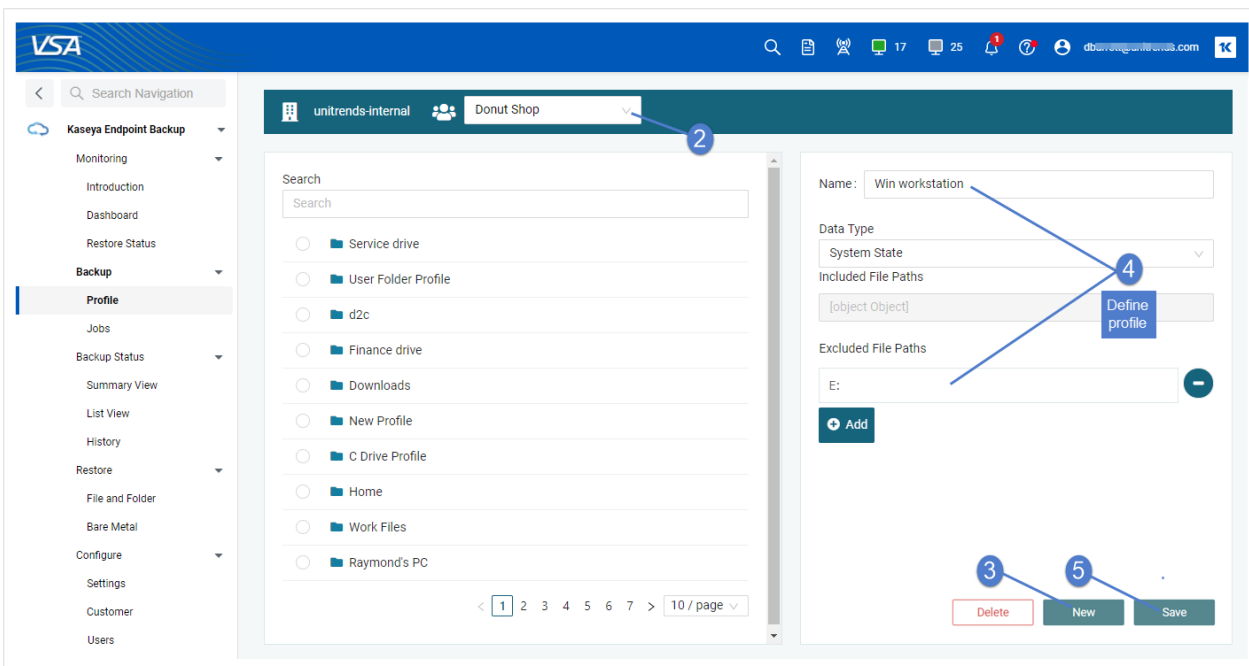
To add a backup profile for system state backups

Note: A file and folder backup cannot be used for bare metal recovery (BMR) of a failed asset. For BMR, run system state backups instead.

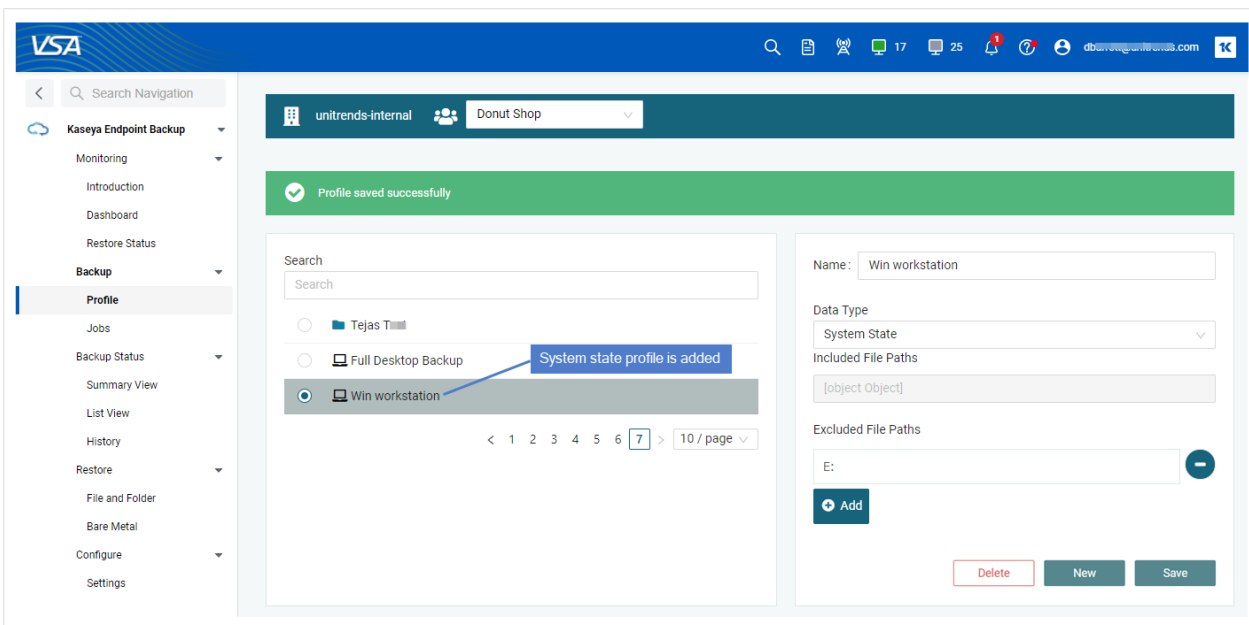
- 1 Select **Backup > Profile**.
- 2 Select a customer.
- 3 Click **New**.
- 4 Enter a name for the profile.
- 5 Select **System State** from the Data Type list.
- 6 (Optional) In the Excluded File Paths field, enter a volume or folder to exclude from the backup:

IMPORTANT! Be sure not to exclude a system critical volume. The system state and all critical volumes essential to OS functions must be included to perform a bare metal recovery.

- Data that does not meet the criteria you specify here IS included in the backup.
- Type in the volume or full folder path (e.g., C: or C:\Finance\Customer) to specify data to exclude. Wildcards are supported.
- Click **Add** to specify multiple file paths. (Click **Remove** to remove a file path.)
- See "[Considerations for including and excluding files](#)" for additional information.



The profile is added:




To view or edit a backup profile

- 1 Select **Backup > Profile**.
- 2 Select a customer.


3 Select a profile in the Search list.

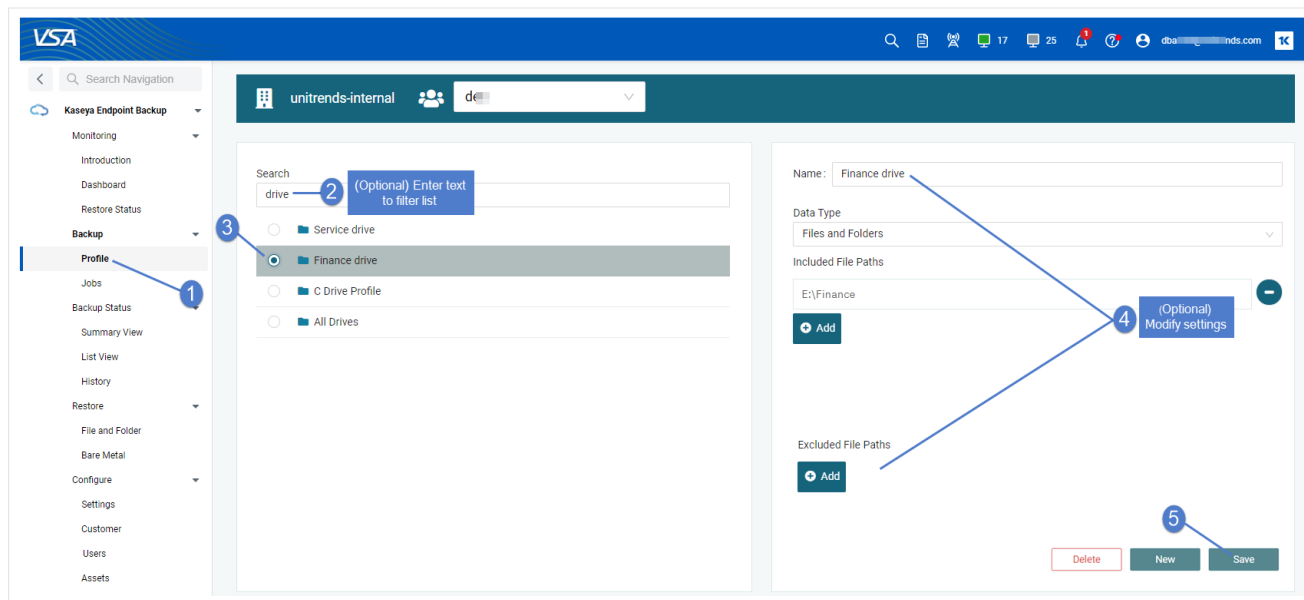
To filter the list of profiles, enter text in the Search field.

4 (Optional) Modify any of the following, then click **Save**:

- Name – Name of the profile.
- Data Type – Choose **File and Folders** to run file and folder backups or **System State** to run system state backups that enable bare metal recovery of a failed asset.
- Included File Paths (supported for file and folder profiles only) – Enter a volume or folder to include in the backup:
 - Data that does not meet the criteria you specify here is NOT included in the backup.
 - Type in the volume or full folder path (e.g., *E:* or *E:\Finance*) to specify data to include. (Wildcards are not supported.)
 - Click **Add** to specify multiple file paths. (Click  to remove a file path.)
 - See "[Considerations for including and excluding files](#)" for additional information.
- Excluded File Paths – Enter a volume or folder to exclude from the backup:

IMPORTANT! **System State profiles** – Be sure not to exclude a system critical volume. The system state and all critical volumes essential to OS functions must be included to perform a bare metal recovery.

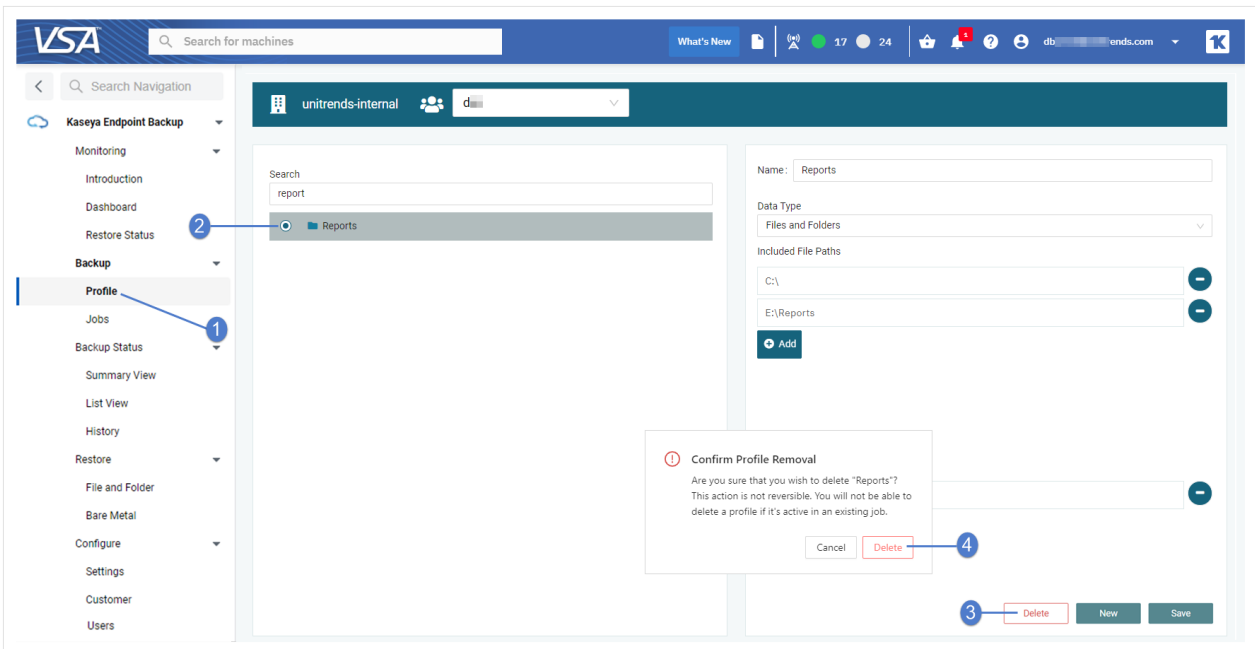
- Data that does not meet the criteria you specify here IS included in the backup.
- Type in the volume or full folder path (e.g., *C:* or *C:\Finance\Customer*) to specify data to exclude. Wildcards are supported.
- Click **Add** to specify multiple file paths. (Click  to remove a file path.)
- See "[Considerations for including and excluding files](#)" for additional information.



To delete a backup profile

Note: You cannot remove a profile that is being used by a running or scheduled job.

- 1 Select **Backup > Profile**.
- 2 Select a customer.
- 3 Select a profile in the Search list.
To filter the list of profiles, enter text in the Search field.
- 4 Click **Delete**, then **Delete** again to confirm.



Working with backup jobs

You can add, modify, and remove backup jobs. See these procedures for details:

- ["To create a backup job"](#)
- ["To view a backup job"](#)
- ["To edit a backup job"](#)
- ["To view a job's backup history"](#)
- ["To delete a backup job"](#)
- ["To run an on-demand full backup of all assets in the job"](#)

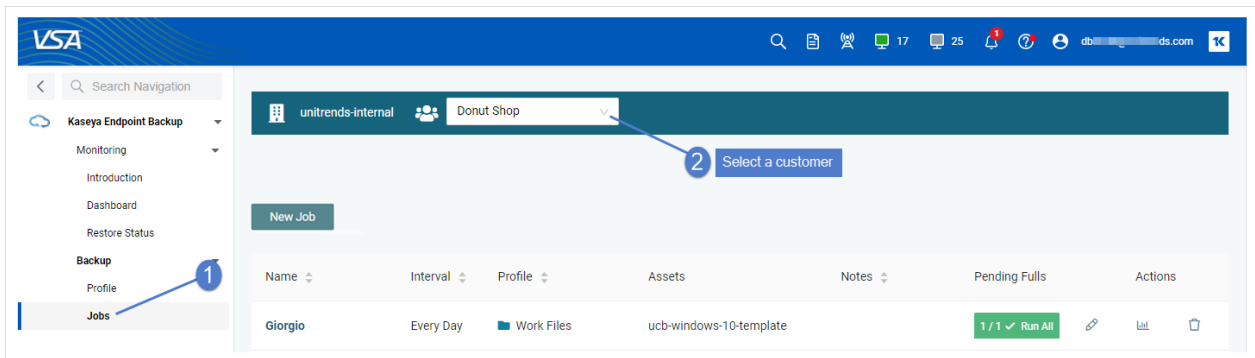
Note: To run a job by asset, see these procedures: ["To run an on-demand backup of the asset"](#) and ["To promote an asset's next backup to a full"](#).

To create a backup job

You can create a job to back up one or more assets. The job you create will run at regular intervals according to the daily or hourly option you choose. After you've created the job, you can run the job on-demand as needed (see ["To run an on-demand full backup of all assets in the job"](#)).

Note: An asset can be assigned to only one backup job schedule. To add an asset to a different schedule, remove it from the first schedule as described in ["To edit a backup job"](#).

- 1 Select **Kaseya EndPoint Backup > Backup > Jobs**. Click **New Job**.
- 2 Select the customer whose assets you will protect.



- 3 Enter a name for the job and select a profile in the list. Click **Next**:

Notes:

- To recover an entire asset, you must run backups with a *system state* profile (a profile whose Data Type is *System State*). Both system state and file and folder profiles support file-level recovery.
- You can opt to create your own custom profile by clicking **New** on the **Backup > Profile** page.
- For details, see "[Working with backup profiles](#)".

The screenshot shows the 'Assets' configuration step in the Kaseya EndPoint Backup software. At the top, there are three progress indicators: '1 Profile' (completed), '2 Assets' (current step), and '3 Schedule' (pending). The main area is divided into three sections:

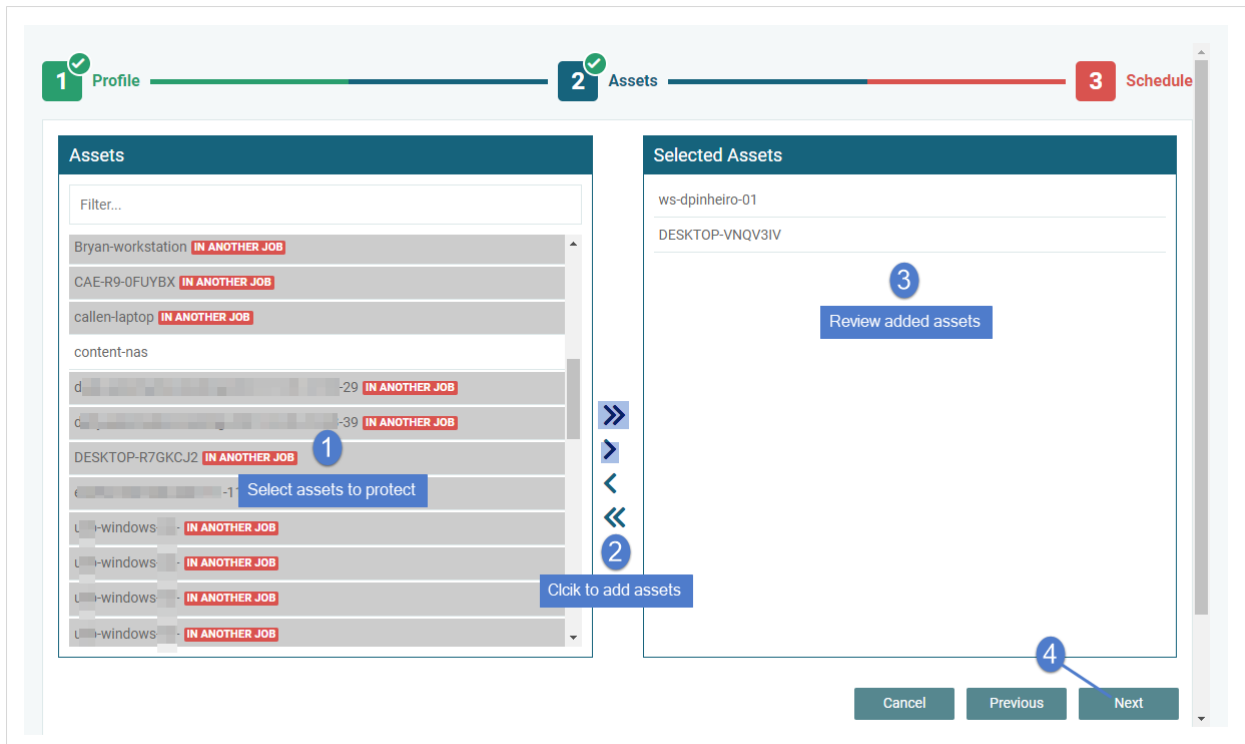
- Name:** A text input field containing 'Win2019'. A callout box with the number '1' and the text 'Enter a job name' points to this field.
- Description:** A large text area for notes. A callout box with the number '2' and the text 'Select a profile' points to the 'C Drive Profile' option in the list below.
- Select Profile:** A list of radio buttons for selecting a backup profile. The 'C Drive Profile' option is selected. Other options include 'Service drive', 'User Folder Profile', 'd2c', 'Downloads', 'Work Files', 'Raymond's PC', 'v-1-19 Backup Profile', and 'Reports'.

At the bottom right, there is a pagination control showing '< 1 2 3 4 5 ... 3 >' and a '10 / page' dropdown. Below this are 'Cancel' and 'Next' buttons.

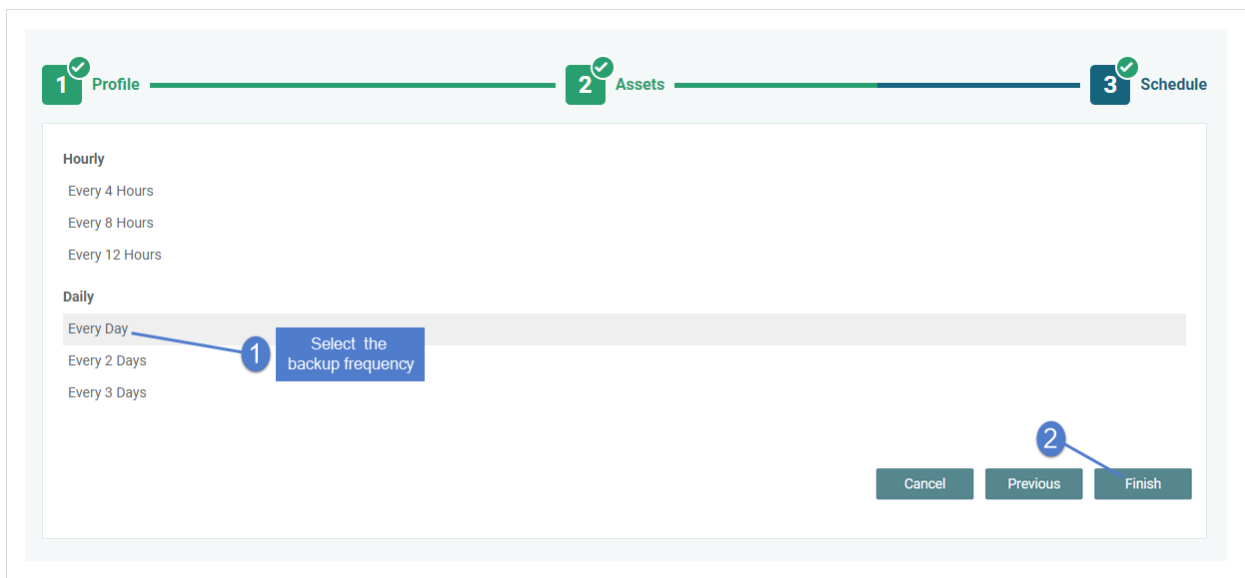
- 4 Select one or more Assets and click > or >> to add them to the job. Review the Selected Assets. Click **Next**:

Notes:

- The Assets list contains all registered assets for the active customer.
- Newly added assets display in the list as *Unregistered*. The asset name changes from *Unregistered* to the machine's host name once the asset checks in for the first time.
- Assets that are disabled cannot be added to the job. To add the asset to a job, you must first enable the asset (see ["To enable or disable an asset"](#)).
- Assets that have already been assigned to a job cannot be added to the job. To add the asset to a different job, you must first remove it from the other job (see ["Protecting Assets with Kaseya EndPoint Backup"](#)).

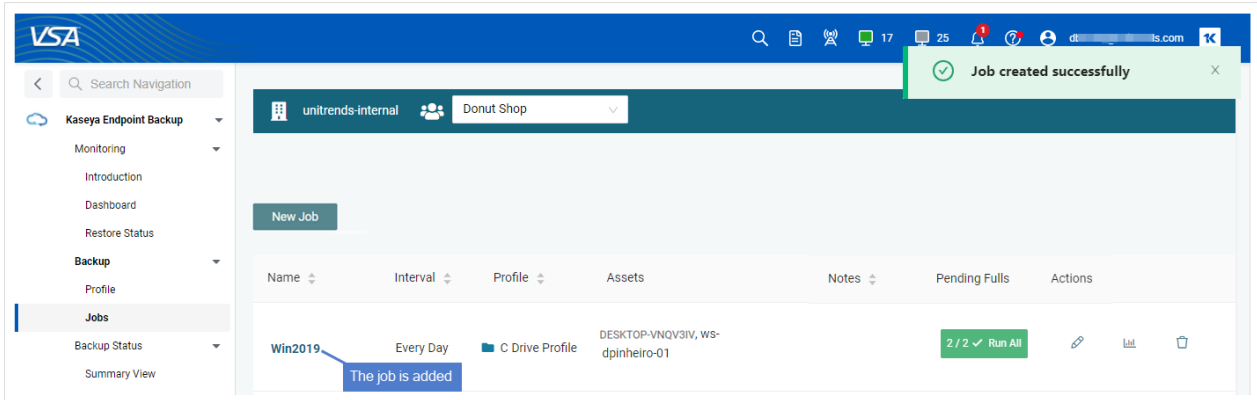


- 5 Define the backup frequency by selecting one of the following: Every 4 Hours, Every 8 Hours, Every 12 Hours, Every Day, Every 2 Days, or Every 3 Days. Click **Finish**:



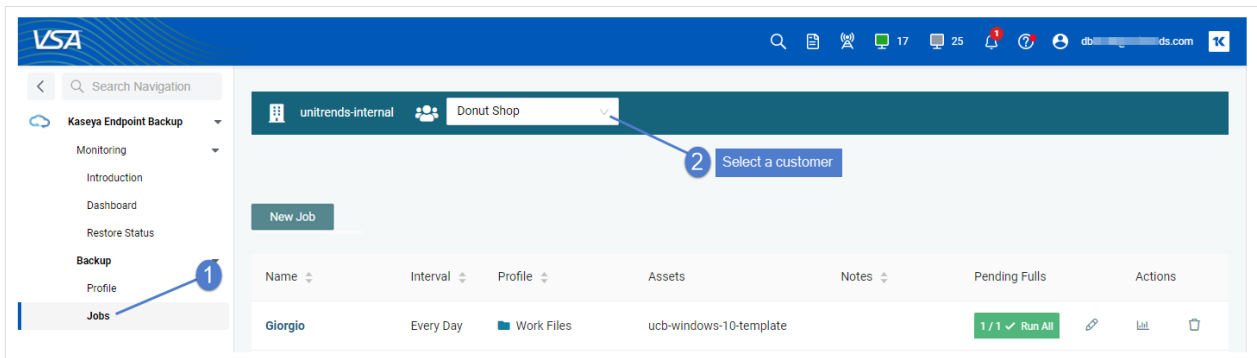
- 6 The job is added.

- Jobs are added to the queue (one job for each asset). Select **Kaseya EndPoint Backup > Monitoring > Backup Status** to view the pending and running jobs. For details, see "[Viewing backup status](#)".
- If a job cannot run because an asset is offline, the job runs upon the next agent check-in.
- Subsequent backups will run for each asset at the specified frequency.



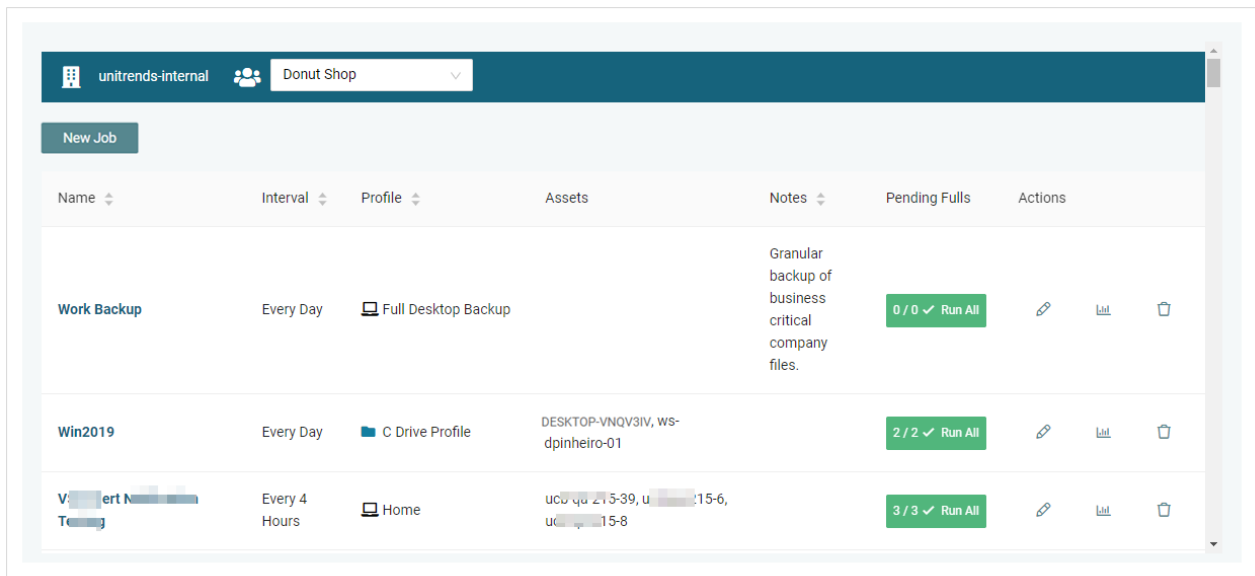
To view a backup job

- 1 Select **Backup > Jobs**.
- 2 Select the customer whose job you will view.



- 3 Locate the job in the list. If needed, filter or sort the display.
If needed, click on a column to sort alphabetically (a to z). Click the column again to reverse the order (z to a).
- 4 The following details display for the backup job:
 - Name – Name of the job.
 - Interval – Frequency of the job: Every 4 Hours, Every 8 Hours, Every 12 Hours, Every Day, Every 2 Days, or Every 3 Days.

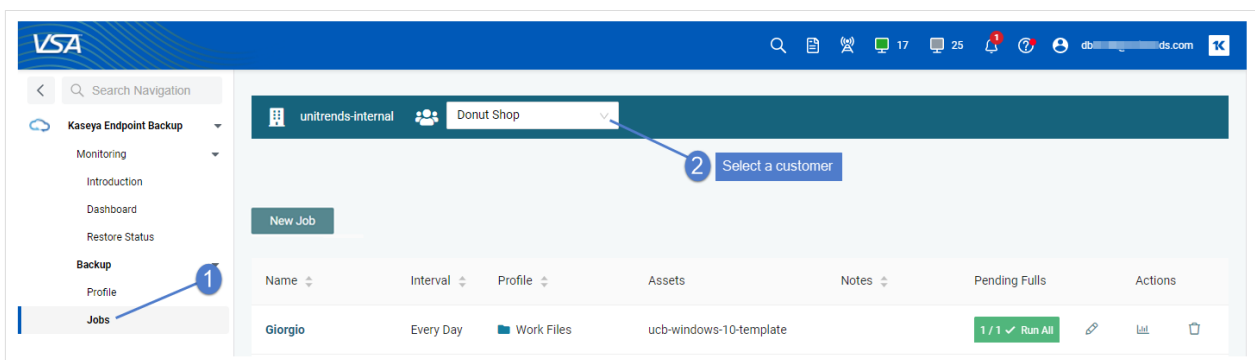
- Profile – Profile assigned to the job. (To view profile details, select **Backup > Profile**. For details, see "[To view or edit a backup profile](#)".)
- Assets – List of assets protected by the job.
- Notes – Description of the job.
- Pending Fulls – The button shows the number of pending fulls that have been queued for assets in this job. Click to run fulls of each asset. For details, see "[To run an on-demand full backup of all assets in the job](#)".



Name	Interval	Profile	Assets	Notes	Pending Fulls	Actions
Work Backup	Every Day	Full Desktop Backup		Granular backup of business critical company files.	0 / 0 ✓ Run All	[Edit] [List] [Delete]
Win2019	Every Day	C Drive Profile	DESKTOP-VN9V3IV, WS-dpinheiro-01		2 / 2 ✓ Run All	[Edit] [List] [Delete]
V. ert N... T...	Every 4 Hours	Home	ucb-qa-zv-5-39, u...:15-6, ucb-qa-zv-15-8		3 / 3 ✓ Run All	[Edit] [List] [Delete]

To edit a backup job

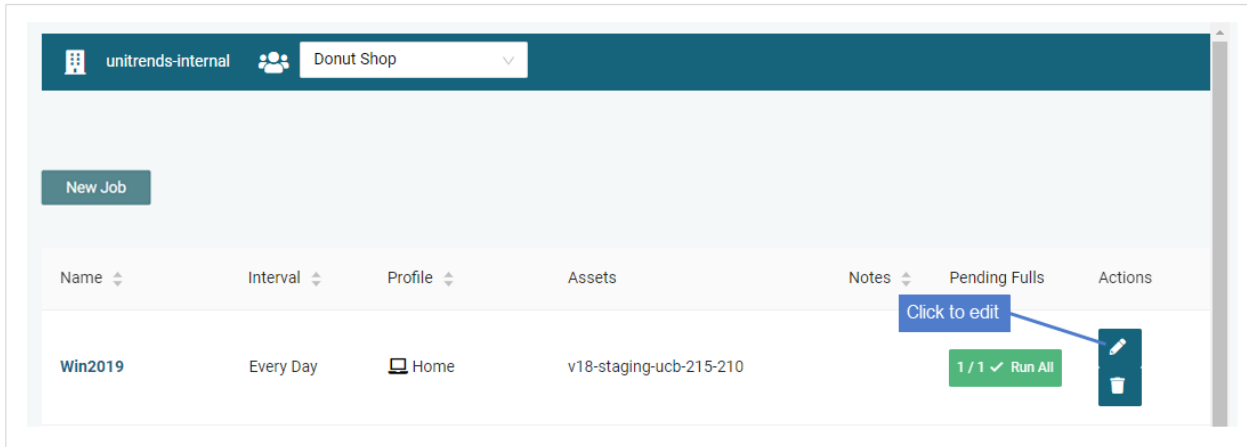
- 1 Select **Backup > Jobs**.
- 2 Select the customer whose job you will edit.



Name	Interval	Profile	Assets	Notes	Pending Fulls	Actions
Giorgio	Every Day	Work Files	ucb-windows-10-template		1 / 1 ✓ Run All	[Edit] [List] [Delete]

- 3 Locate the job in the list.
If needed, click on a column to sort alphabetically (a to z). Click the column again to reverse the order (z to a).

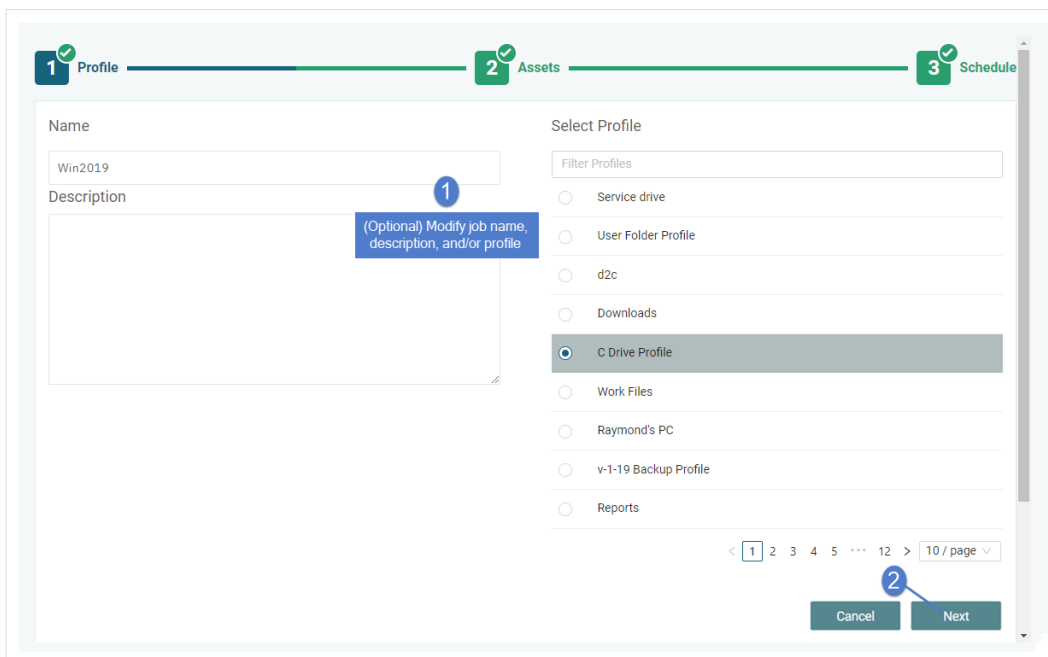
- 4 Click the job's  icon:



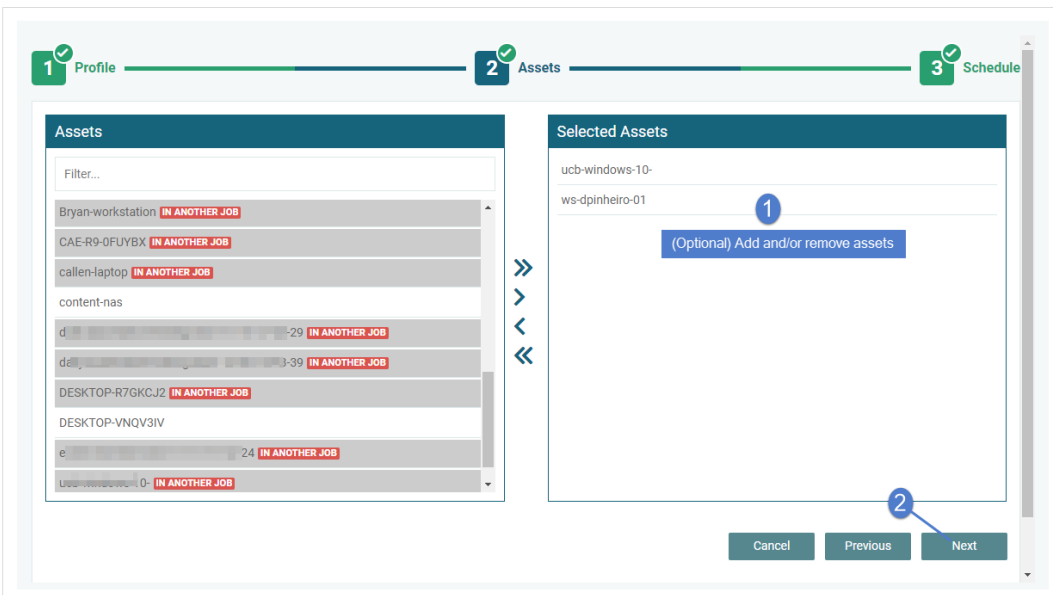
- 5 (Optional) On the Profile page, modify any of the following, then click **Next**:

- Name – Name of the backup job.
- Description – Description of the backup job.
- Select Profile – Profile assigned to the backup job.

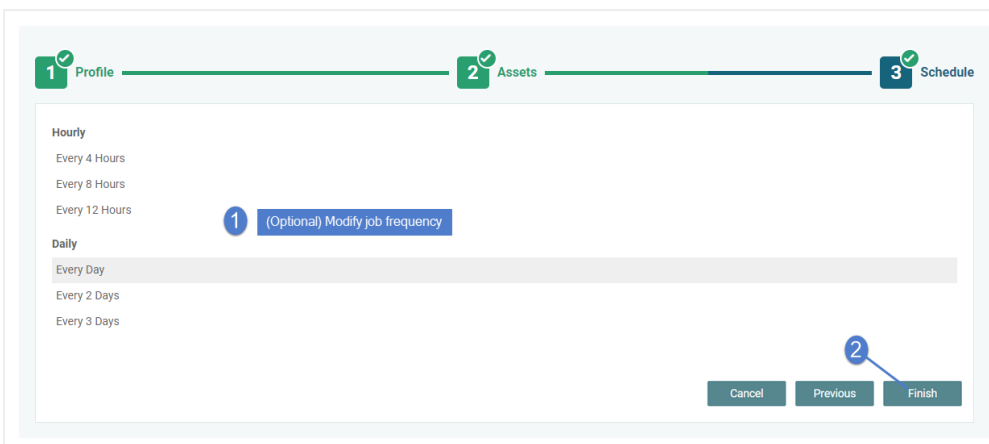
Note: If you want the option to recover the entire asset from this backup, be sure to select a system state profile (a profile whose Data Type is *System State*).



- 6 (Optional) On the Assets page, add and/or remove assets, then click **Next**:

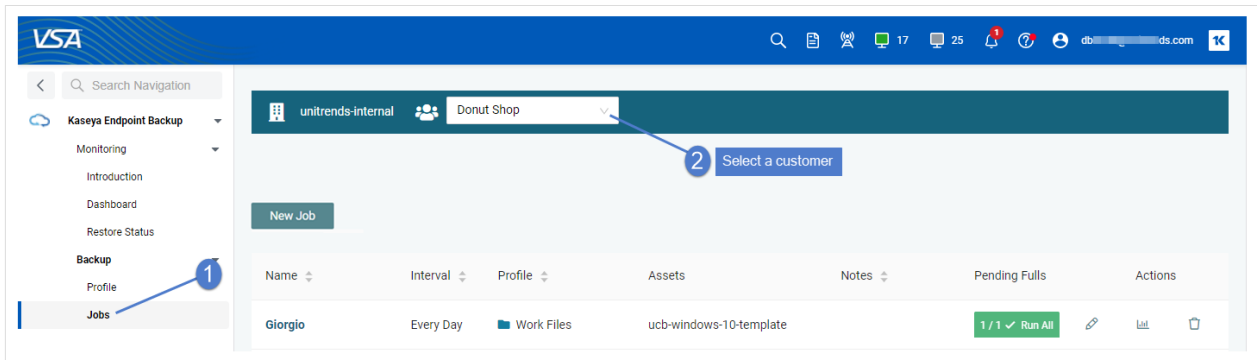


- 7 (Optional) On the Schedule page, modify the job frequency, then click **Finish**:



To view a job's backup history

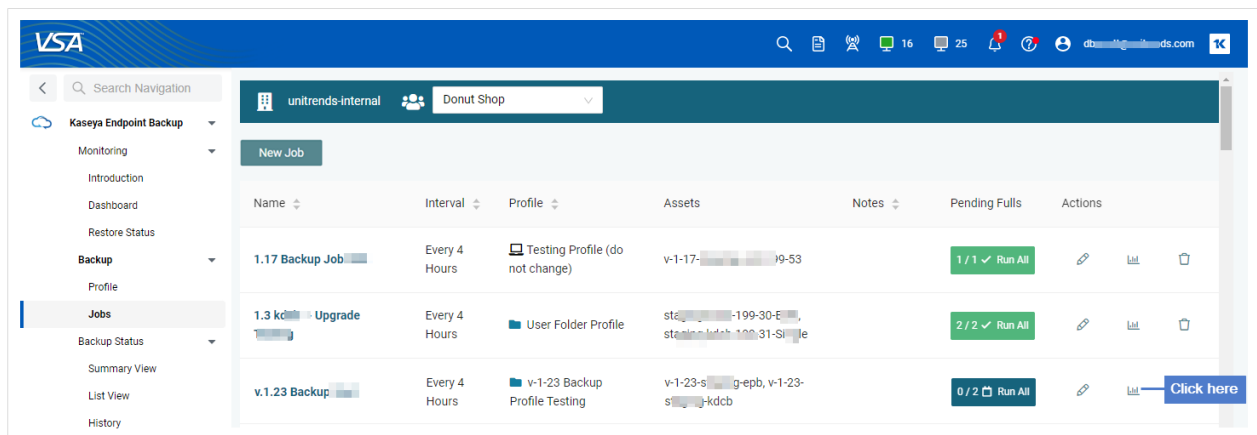
- 1 Select **Backup > Jobs**.
- 2 Select the customer whose job history you will view.



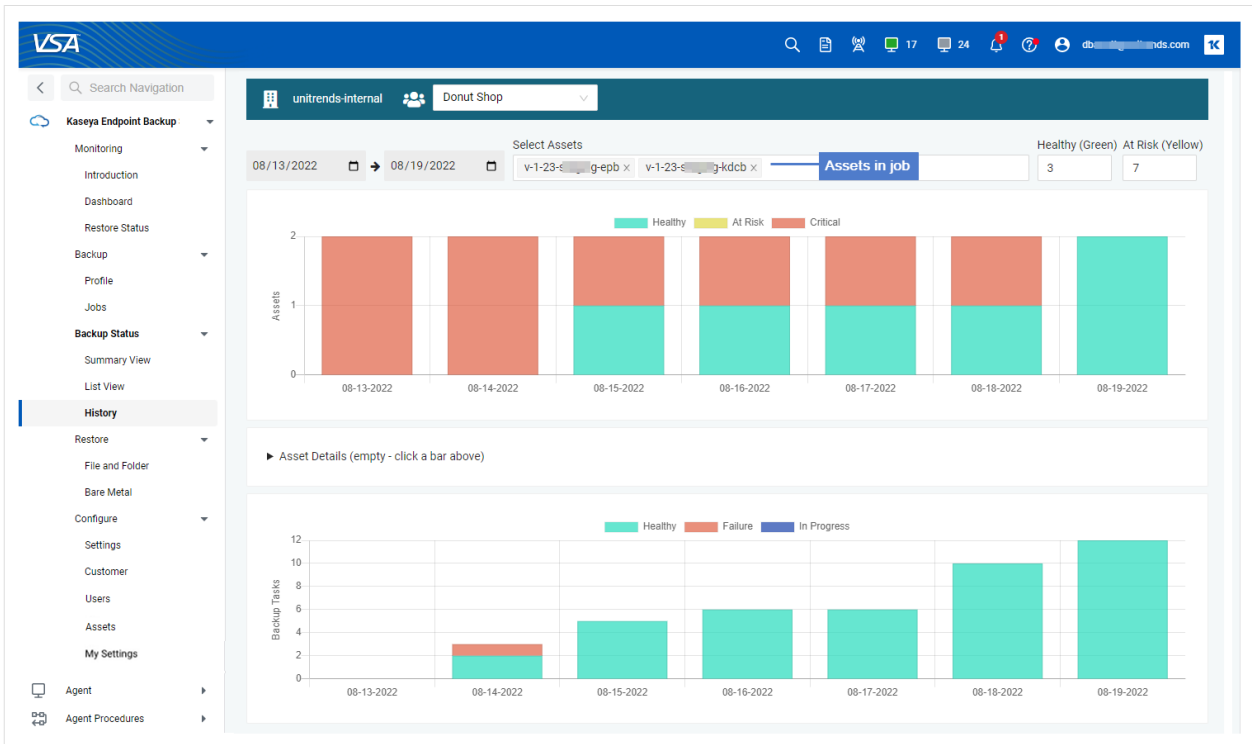
3 Locate the job in the list.

If needed, click on a column to sort alphabetically (a to z). Click the column again to reverse the order (z to a).

4 Click the job's  icon.

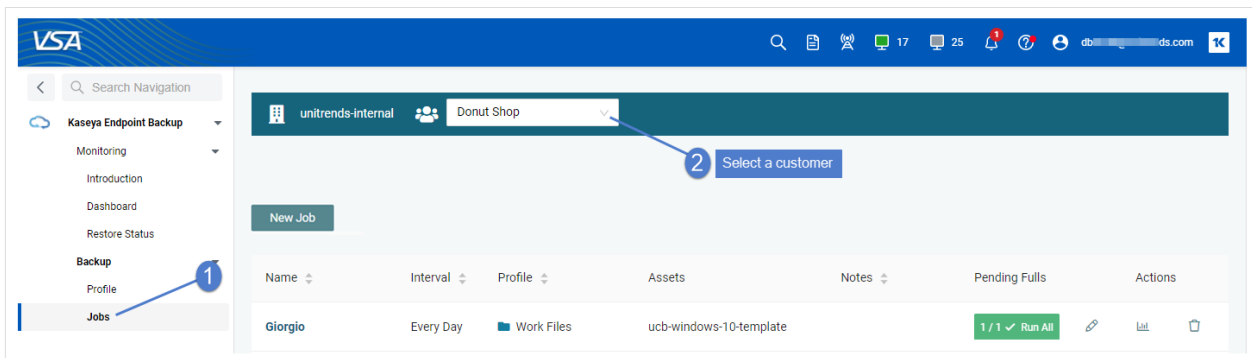



Backup history for the assets in the job displays on the History page:

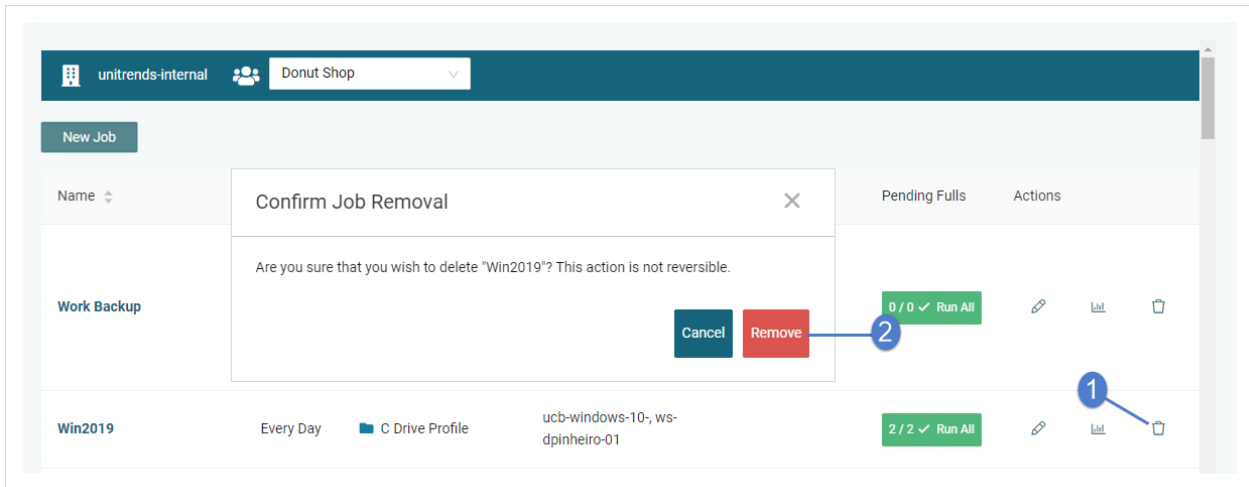


To delete a backup job

- 1 Select **Backup > Jobs**.
- 2 Select the customer whose job you will delete.



- 3 Locate the job in the list.
If needed, click on a column to sort alphabetically (a to z). Click the column again to reverse the order (z to a).
- 4 Click the job's  icon, then **Remove** to confirm. The job is deleted.



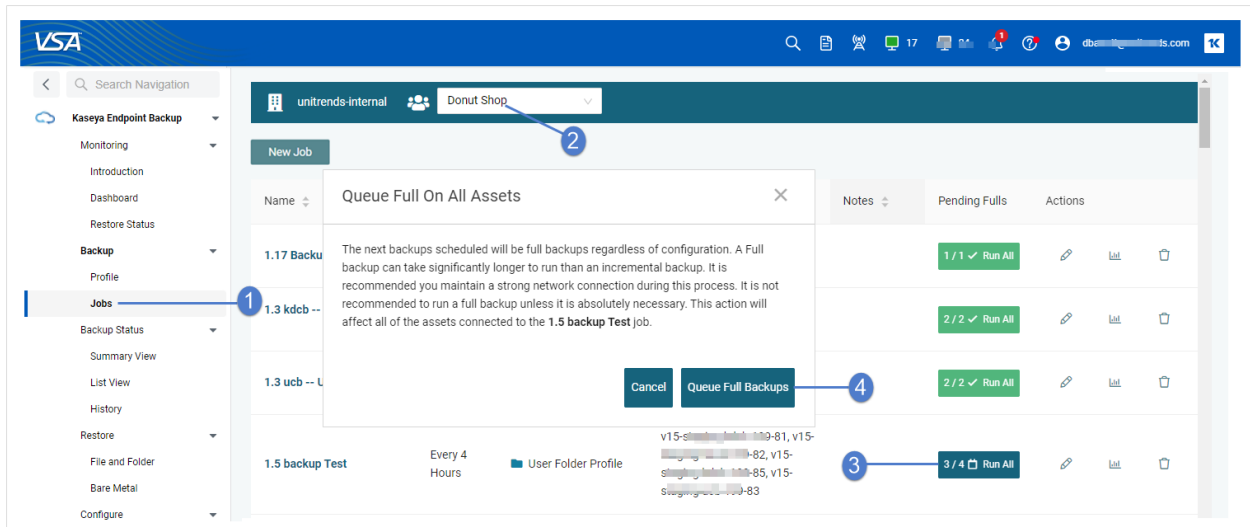
To run an on-demand full backup of all assets in the job

Use this procedure to run an on-demand full backup of each asset in the job. Jobs are queued as soon as the asset checks in and run if no other job is currently running for the asset.

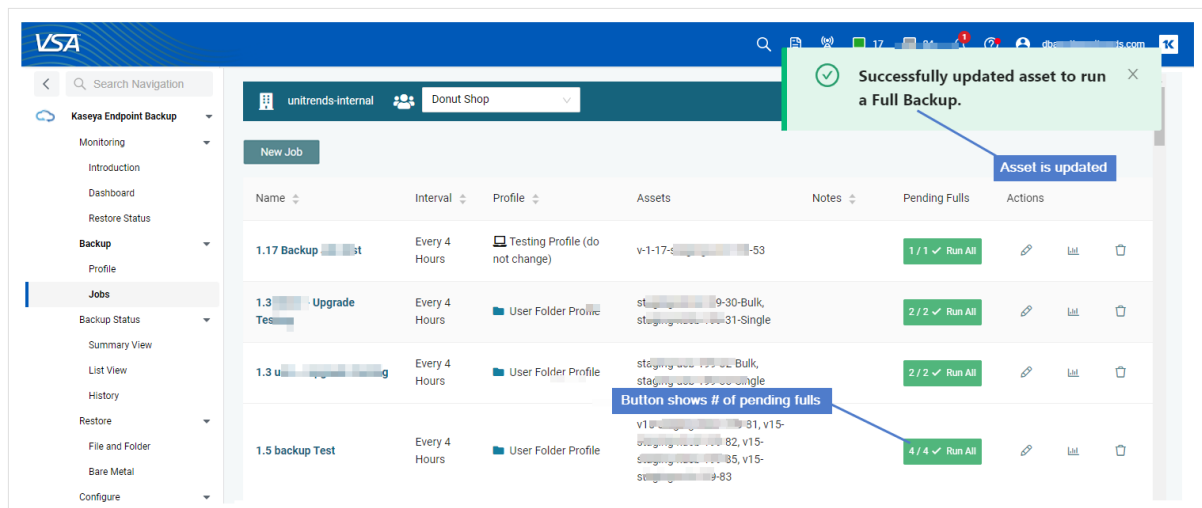
- 1 Select **Backup > Jobs**.
- 2 Select the customer whose job you will run.
- 3 Locate the job in the list.
- 4 Click the job's **Run All** button.

The Run All button shows the number of pending fulls that have already been queued for this job. In the example image below, the job contains 8 assets and 1 full has already been queued.

- 5 Click **Queue Full Backups** to confirm.



- 6 The job's Run All button changes to green and the number of pending jobs is updated, indicating that new Run All jobs are pending. Each jobs is queued as soon as the asset checks in and runs if no other job is currently running for the asset.



- 7 The button returns to blue once any pending Run All job starts. Note that you cannot initiate Run All for the job if the button is gray (all assets are disabled) or green (all Run All jobs are pending)
- 8 Select **Backup Status > List View** to view jobs.

This page is intentionally left blank.



Chapter 4: Recovering Files

This chapter provides considerations and instructions for recovering files from your backups. See the following topics for details:

- "Recovery considerations"
- "Recovering files and folders from a backup"

Note: To recover a failed asset from a system state backup, see "Bare Metal Recovery".

Recovery considerations

Consider the following before recovering files:

- You can recover files from any backup to any asset that has been added to your Kaseya EndPoint Backup environment. (To add an asset, see "Install the Kaseya EndPoint Backup agent".)
- File data is recovered. Other file attributes, such as Access Control Lists (ACLs), are not recovered.
- Recovery requires a stable connection. Recovery can resume if there is a brief disconnection. If the connection is interrupted for more than a few minutes, the recovery fails.

Recovering files and folders from a backup

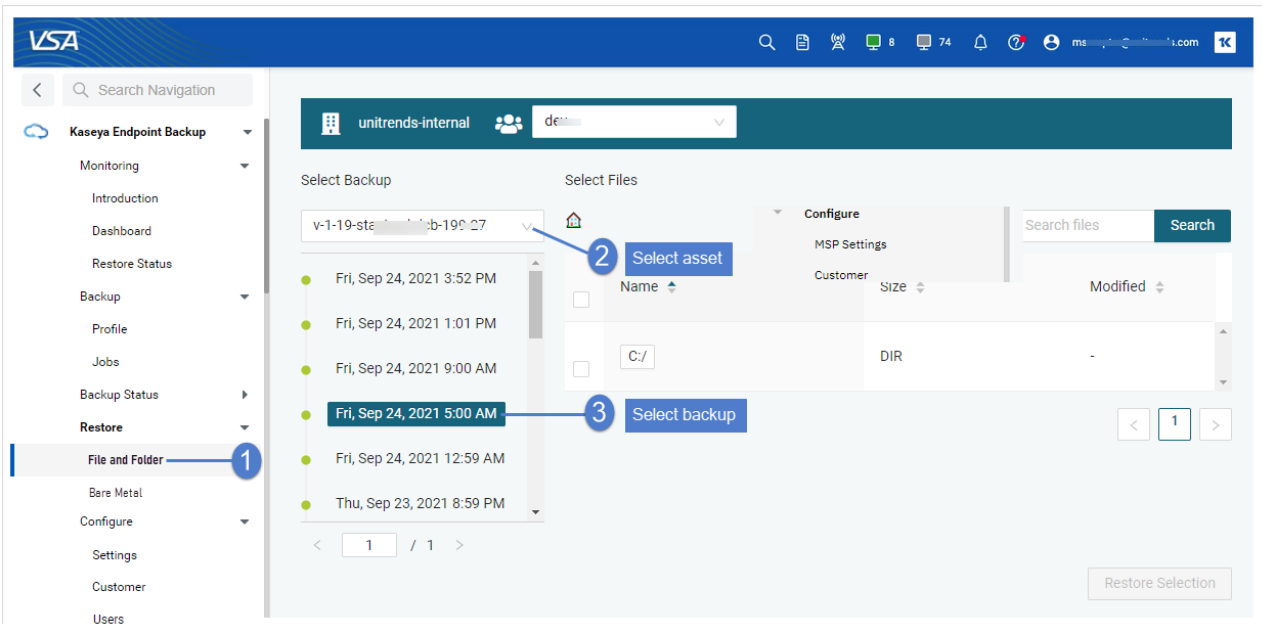
Use this procedure to recover selected files and folders from a backup.

To recover files

- 1 Select **Restore > File and Folder**.
- 2 Select an asset and the backup to recover:

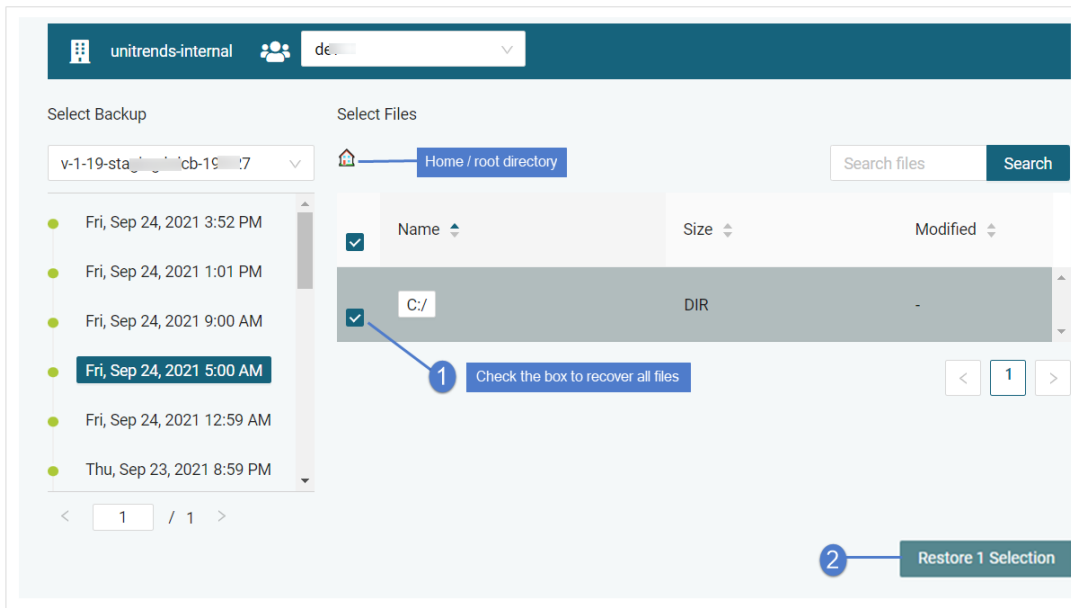
Notes:

- You can filter the asset list by entering text in the Select Asset field. Only assets containing the string you entered display in the list.
- If the asset has been decommissioned, **DELETED AGENT** displays next to the asset name. You can recover backups of this asset by selecting it in the list, but you must recover the backup to another asset (one that has not been decommissioned).

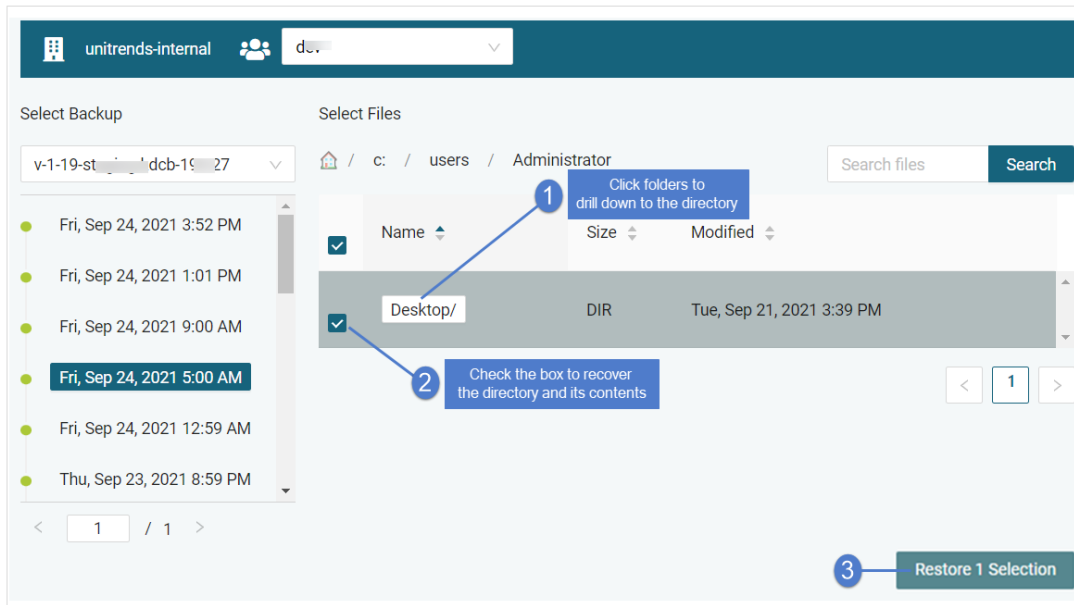


3 Select one or more items to recover, then click **Restore Selections**:

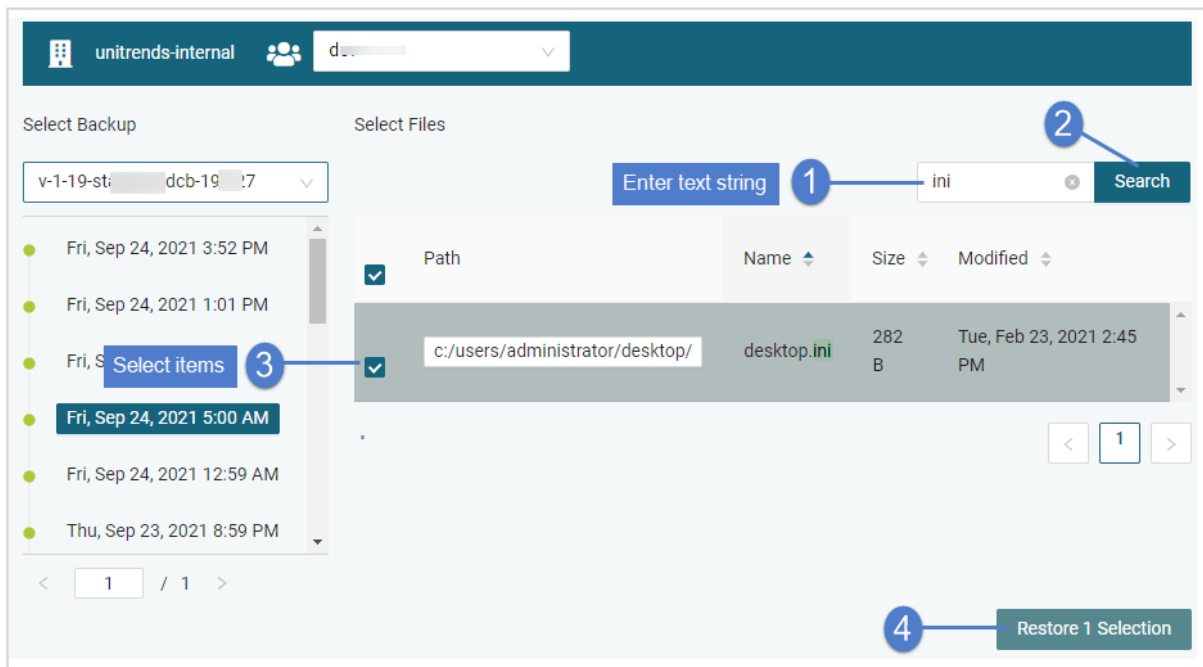
- You can recover all files by selecting the root directory's checkbox.



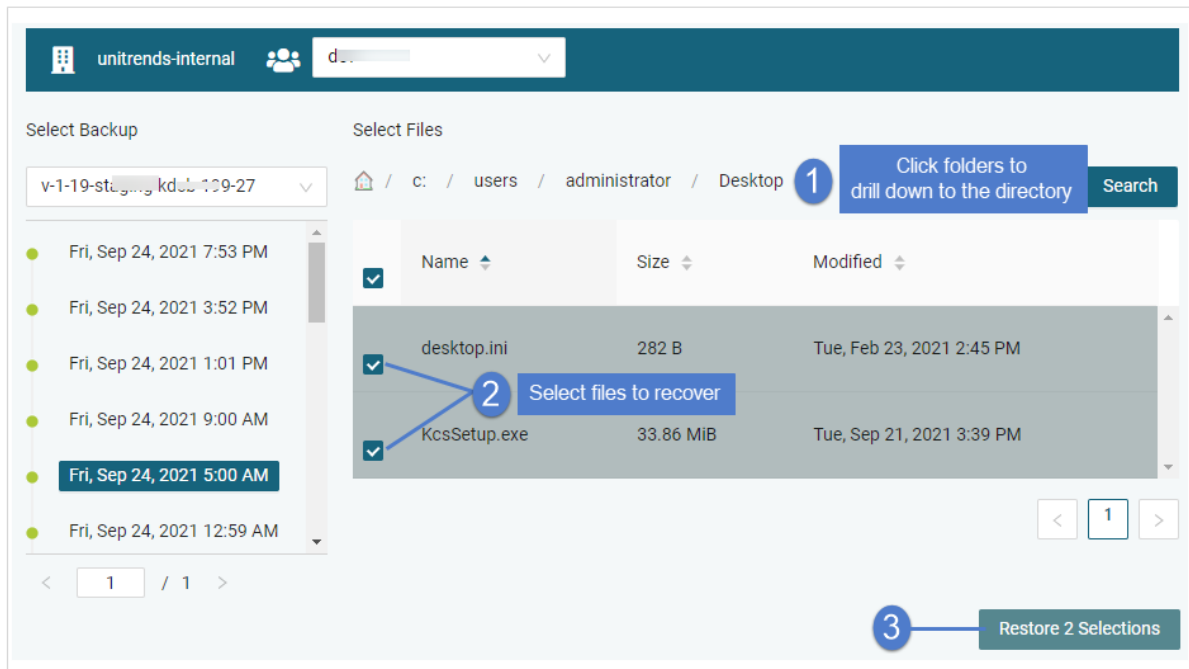
- You can recover the contents of an entire drive or folder by selecting its checkbox.



- You can search for and recover individual files/folders. Enter a text string in the Search Files field, then click **Search**. Files and directory names containing the string you entered display in a list. Check boxes to select items to recover.



- You can recover individual files by browsing the backup contents and selecting one or more files.



4 Select these Advanced Options for the recovery:

- Target Asset – Select the asset where files will be recovered.

Note: Assets that have been deleted or decommissioned are disabled in the list and cannot be used as destination assets.

- Alternate Path – Enter the recovery path on the target asset. Use the default location, `C:/recover`, or enter an alternate path.
- Conflict Resolution – Choose how to handle existing files of the same name in the target directory: select **Overwrite** to replace the file with the one you are recovering or **Preserve Newer** to keep the existing file only if it is newer than the one selected for recovery (otherwise overwrite the existing file).

Note: The Preserve Newer option is not used for files where the fully qualified file path is greater than 251 characters. In this case, the existing file is overwritten. This is a known issue that will be addressed in an upcoming release.

- Folder Structure – Choose **Preserve** to recover the existing folder structure under the target directory or **Flatten** to recover only the files to the target directory.

5 Click **Confirm Restore**.

Selected Files and Folders

c:/users/administrator/desktop/desktop.ini
c:/users/administrator/desktop/kcssetup.exe

List of items to recover

Advanced Options

Target Asset: 1-7-s...cb-b...215-87

* Restore Path: C:/recover

Conflict Resolution: Preserve Newer

Folder Structure: Preserve

1 Select Advanced Options

2

Cancel Confirm Restore

- 6 The job is added to the queue and displays on the Restore Status page. Files are recovered to the destination asset.
- If the recovery path directory does not exist, the job creates it during the recovery.
 - If the destination asset is not online, the job runs upon the next agent check-in.

VSA

unitrends-internal dev

Task ID	Job	Type	Target	Start Time	End Time	Status
7b0d0536	4e1e0e26-07eb-44d4-ba82-ee47e1d1f063	File & Folder	1-7-s...cb-b...215-87	Tue, Oct 27, 2020 1:56 PM	-	🔄

Job is added to queue

This page is intentionally left blank.



Chapter 5: Bare Metal Recovery

Bare metal recovery enables you to restore a failed asset from a system state backup to identical or dissimilar hardware. The target recovery asset can be a physical machine or a VMware virtual machine (VM). To get started, review the ["Prerequisites for bare metal recovery"](#). Next, download the recovery ISO and burn it to a DVD/USB (for recovery to a physical asset) or save it to your VMware hypervisor (for recovery to a VM). In the event that your asset fails, run the ["To perform a bare metal recovery"](#) procedure to recover a physical or VM target asset.

Prerequisites for bare metal recovery

The following requirements must be met to perform a bare metal recovery (BMR).

Requirement	Description
Operating systems	<p>Recovery to identical or dissimilar physical hardware and virtual machines is supported for the operating systems listed below.</p> <p>Supported client operating systems:</p> <ul style="list-style-type: none"> • Windows 8, 64-bit only • Windows 10, 64-bit only • Windows 11, 64-bit only <p>Supported server operating systems:</p> <ul style="list-style-type: none"> • Windows 2016, 64-bit only, support does not include Nano Server • Windows 2019, 64-bit only • Windows 2022, 64-bit only <hr/> <p>Note: Unitrends supports the most recent two Service Pack (SP) versions on all releases of Windows Server.</p> <hr/>
An eligible system state backup	<p>The backup used for recovery must meet these requirements:</p> <ul style="list-style-type: none"> • It was run using agent version 1.24 or higher (agent 1.25 or higher for Windows 11 or Windows Server 2022). • It is successful. • It is a full or incremental system state backup that contains all critical system volumes. A system state backup is run with a system state profile (a profile whose Data Type is <i>System State</i>). For details on running a system state backup, see "To add a backup profile for system state backups" and "To create a backup job".

Requirement	Description
Recovery ISO	<p>For the recovery, you must use the Kaseya EndPoint Backup BMR ISO image, <i>baremetal-recovery-media.iso</i>, provided on the Kaseya EndPoint Backup Restore > Bare Metal page. The ISO contains WinPE (a minimal version of Windows used for installations) and the BMR UI. To prepare for DR, it is recommended that you do the following:</p> <ul style="list-style-type: none"> • Create a bootable DVD or USB of the ISO and store it in a safe place, so that you can quickly recover to a physical machine target. (For details on creating bootable media, see this KB article.) • Save the ISO to your hypervisor (so you can quickly recover to a virtual machine target).
Network requirements	<p>An IP address, netmask, and gateway are assigned to the recovery target asset during bare metal recovery.</p> <p>If Dynamic Host Configuration Protocol (DHCP) is available in your environment, network settings are assigned automatically.</p> <p>If DHCP is not configured, or if you want to configure network settings for the target machine, you can manually enter the IP address, netmask, and gateway.</p>
Network adapter	Wireless network adapters cannot be used for the recovery.
Firmware interface type	Supported for BIOS- and UEFI-based assets. The firmware interface type (BIOS or UEFI) of the recovery target machine must match that of the failed asset.
Disk configuration	<ul style="list-style-type: none"> • GPT disks are supported. • Dynamic disks are not supported. • iSCSI disks are not supported. Recover the critical (non-iSCSI) volumes as described in "To perform a bare metal recovery". Once the critical volumes have been restored, recover data on the iSCSI volumes as described in "To recover files".
RAID configurations	<ul style="list-style-type: none"> • Software RAID configurations are not supported. • Hardware RAID configurations are not supported.
Additional hardware requirement	Hardware not included in the Windows 10 PE environment is not supported.

Requirement	Description
Processor features on the recovery target	These processor features must be enabled on the recovery target machine: NX, PAE, and SSE2. Ensure that these features are enabled on the target before booting from the ISO image. For instructions, see KB 360013249658 . Machines that do not have these processor features cannot be used for the recovery.
Disk space on recovery target	Make sure the target machine has enough disk space for the recovery. The recovery target can have smaller disks than the failed asset, but the recovery fails if the disks do not have enough space for the data on the critical volumes.
Supported recovery scenarios	<p>Use the "To perform a bare metal recovery" procedure for the following recovery scenarios:</p> <ul style="list-style-type: none"> Recover to the same physical hardware as the failed asset. Recover a failed physical asset to dissimilar hardware. Recover a failed physical asset to dissimilar hardware with fewer disks. Recover a failed physical asset to hardware with smaller or larger disks. Recover a failed asset BIOS/MBR configuration to a dissimilar BIOS/MBR configuration. Recover a failed asset UEFI/GPT configuration to a dissimilar UEFI/GPT configuration. Recover multi-boot configured BIOS servers. Recover a failed physical asset to a VMware virtual machine (VM). Recover a failed VM to a physical asset or to a VMware VM. <p>Notes:</p> <ul style="list-style-type: none"> IaaS VMs – BMR recovery of a failed Azure, AWS, or Google Cloud Computing (GCP) VM that was configured with IaaS roles is not supported. Recovering to a VMware VM – The virtual host must support the OS of the Windows asset you are recovering. For example, you cannot recover Windows 2016 to ESXi 5.1. See the VMware documentation for details.

To perform a bare metal recovery

Use this procedure to recover a failed asset. During this procedure, you will use the Kaseya EndPoint Backup bare metal ISO to recover the failed asset's critical disks from a backup. After the bare metal recovery completes, you will configure the recovered asset's network settings, then recover any data on non-critical volumes.

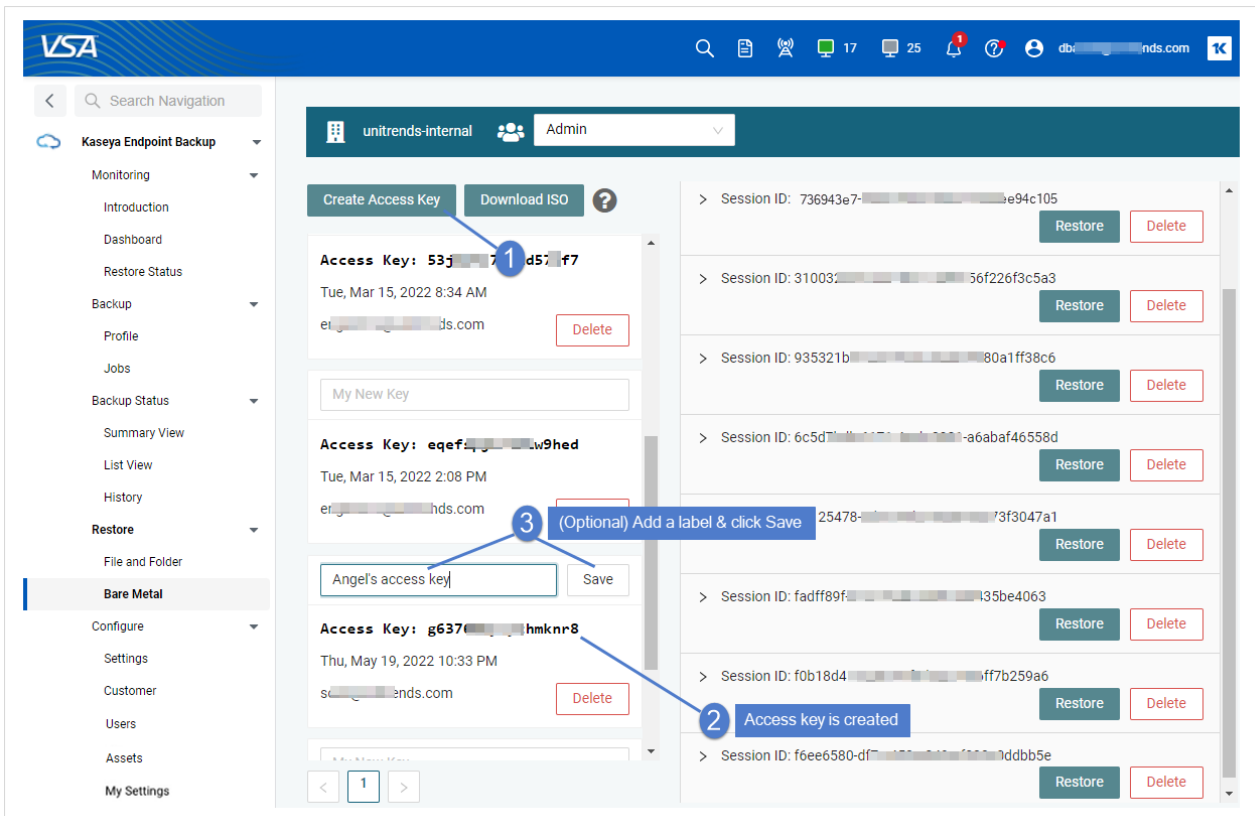
- 1 On the **Restore > Bare Metal** page, click **Download ISO**. The ISO, *baremetal_recovery_media.iso*, is downloaded.

The screenshot shows the VSA Kaseya EndPoint Backup interface. The left navigation menu includes 'Kaseya EndPoint Backup', 'Monitoring', 'Introduction', 'Dashboard', 'Restore Status', 'Backup', 'Profile', 'Jobs', 'Backup Status', 'Summary View', 'List View', 'History', 'Restore', 'File and Folder', and 'Bare Metal'. The 'Bare Metal' option is highlighted with a blue circle and the number '1'. The main content area shows the 'unitrends-internal' user interface with 'Admin' permissions. The 'Create Access Key' button is highlighted with a blue circle and the number '2'. Below this button, there are two access keys listed, each with a 'Delete' button. The 'Bare Metal Sessions' table lists several sessions with 'Restore' and 'Delete' buttons.

Session ID	Restore	Delete
> Session ID: 31dce54f-df21-4394-b347-37d208aa3aa0	Restore	Delete
> Session ID: 80d0a467-9530-4fc5-96da-f7e6b3842ab4	Restore	Delete
> Session ID: 3100329d-6123-4b17-a549-56f226f3c5a3	Restore	Delete
> Session ID: 935321b9-7257-433c-8253-4980a1ff38c6	Restore	Delete
> Session ID: 6c5d7bdb-6171-4acb-8081-a6abaf46558d	Restore	Delete
> Session ID: 87125478-ad7a-47b3-9a38-9ac73f3047a1	Restore	Delete
> Session ID: fadff89f-d7a1-42ab-bb40-aeaf4335be4063	Restore	Delete

2 Click **Create Access Key**.

The key is created and displays in the list below. For easy identification, you can click above and add a custom label.



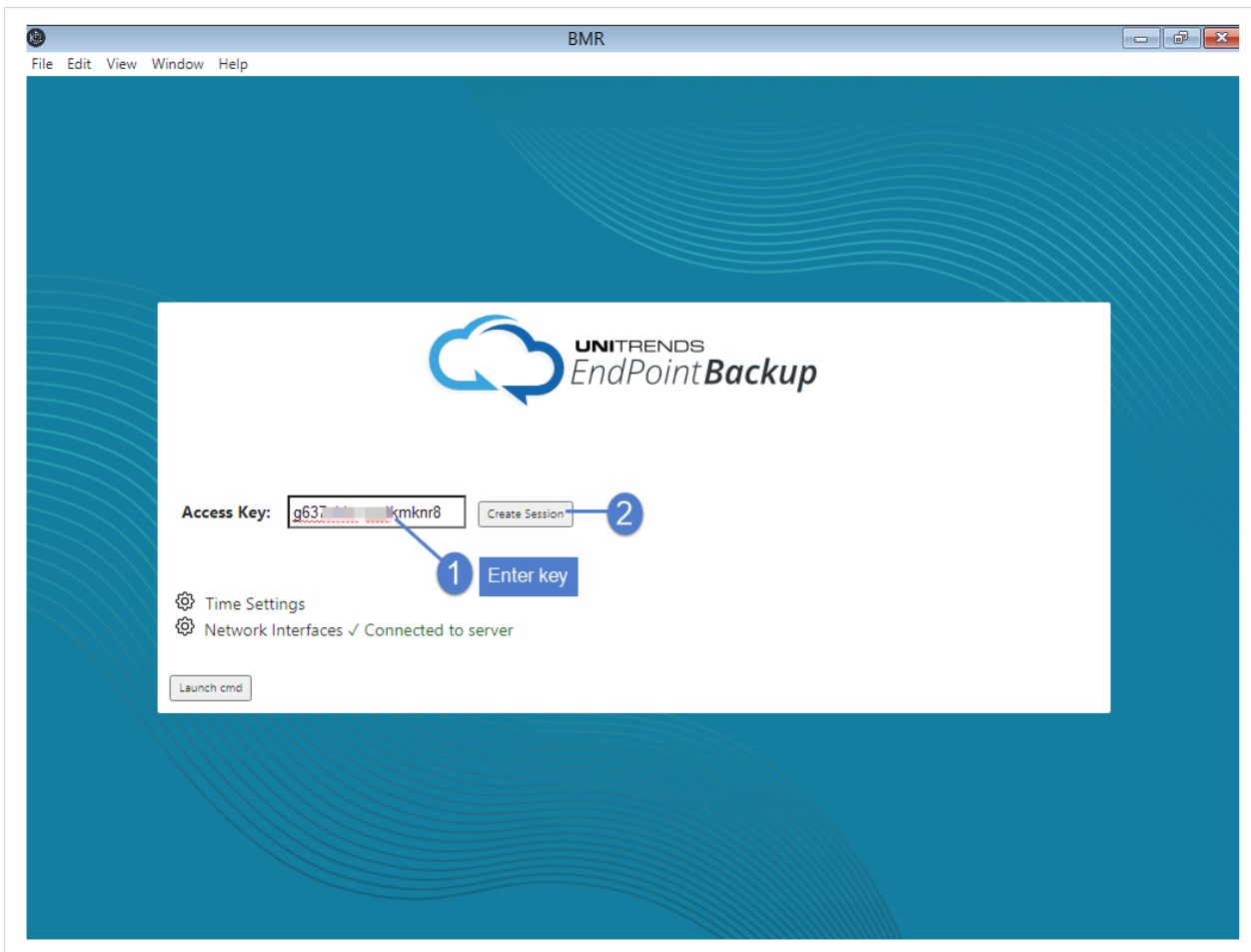
3 Prepare the recovery media:

- To recover to a VM, save the ISO in a location that you can access from your hypervisor. Power down the recovery VM and edit its settings to boot from the ISO.
- To recover to a physical machine, burn the ISO to USB or DVD (see this [KB article](#) for details). Power off the recovery machine and attach the recovery media.

4 Power on the recovery target machine. The machine boots from the ISO and the BMR interface displays.

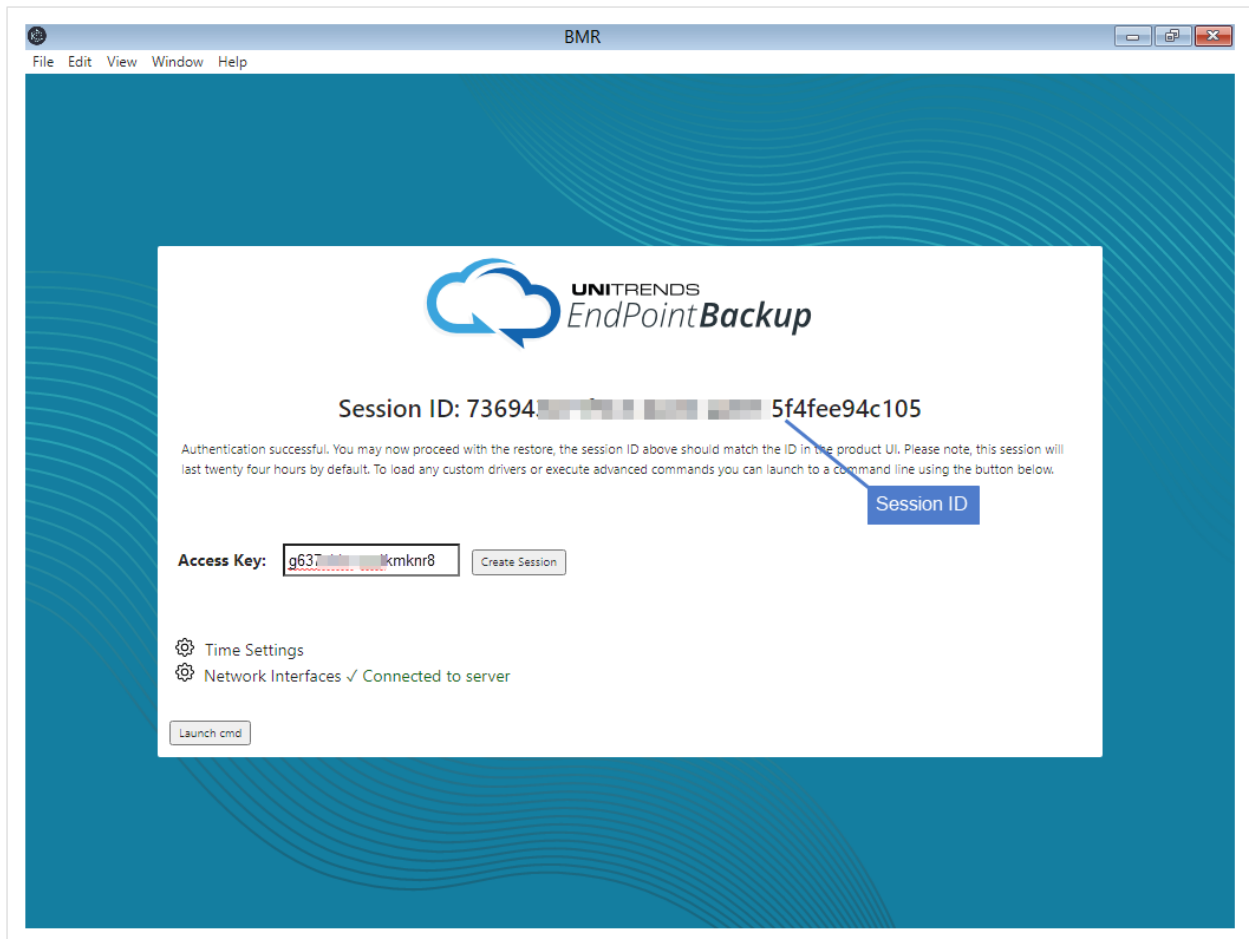
5 In the Access Key field, enter the access key you created in [step 2](#). Be sure to include the hyphen (-).

6 Click **Create Session**.



- 7 The key is saved and a secure session is created between the recovery target asset and EndPoint Backup in the Unitrends Cloud. (This may take a few minutes.)

Note the session ID as you will use it to identify your recovery session in Kaseya EndPoint Backup.

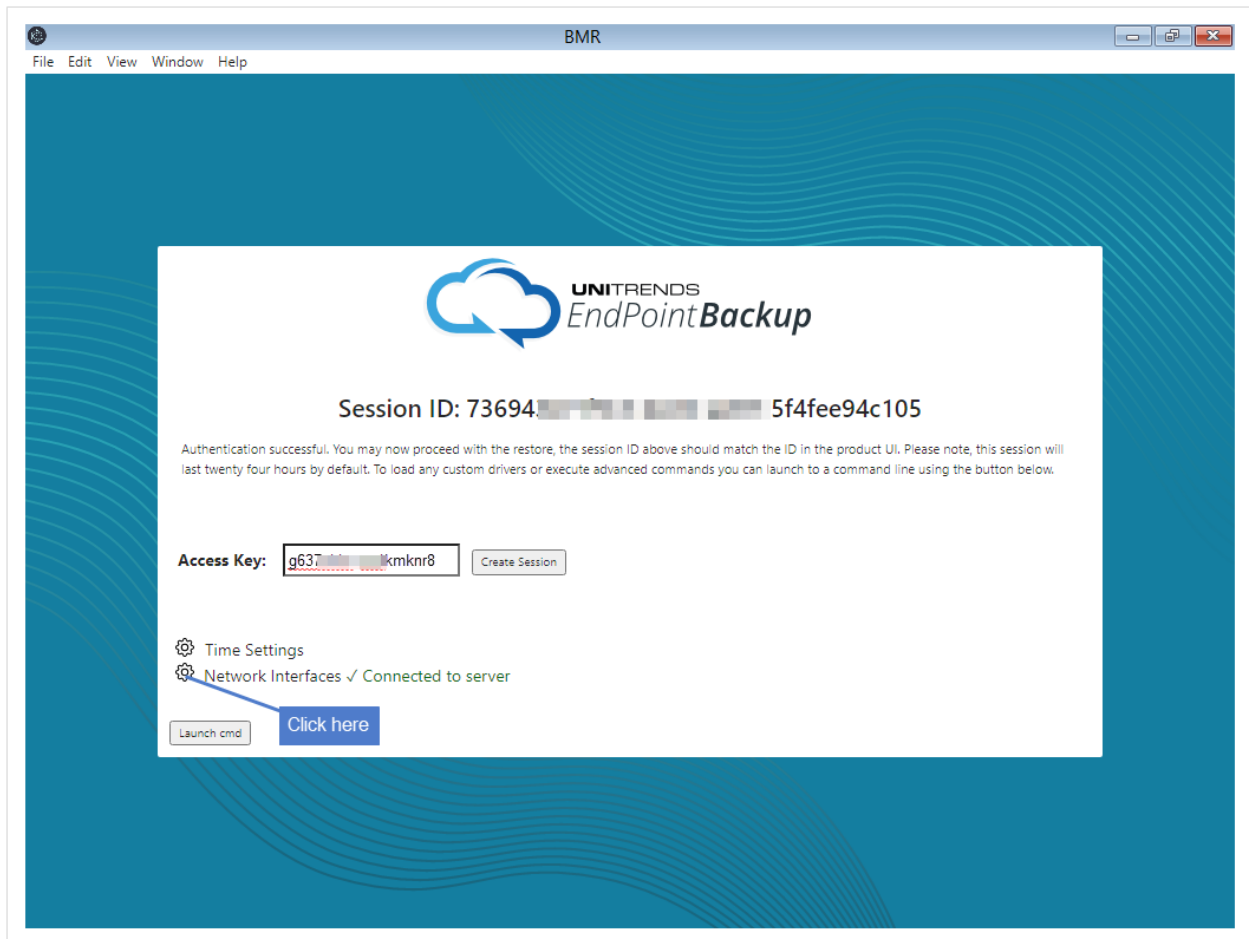


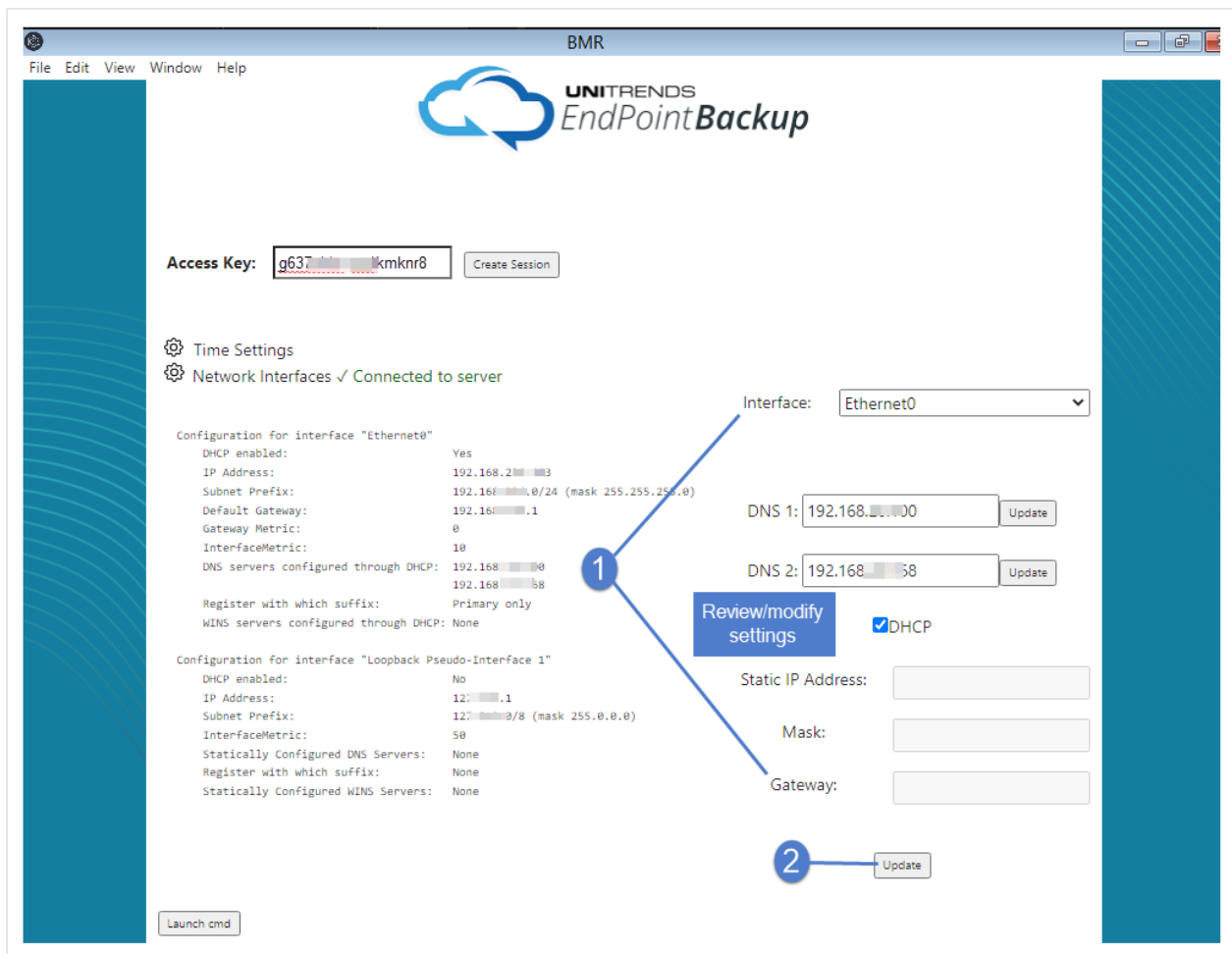
8 Review network settings and modify if needed.

- If DHCP is configured for your network, network settings are assigned automatically.
- If DHCP is not configured, or if you want to configure network settings for the target machine manually, click **Network Interfaces**. Then enter a unique IP address, the Subnet Mask, and the Gateway. Click **Update**.

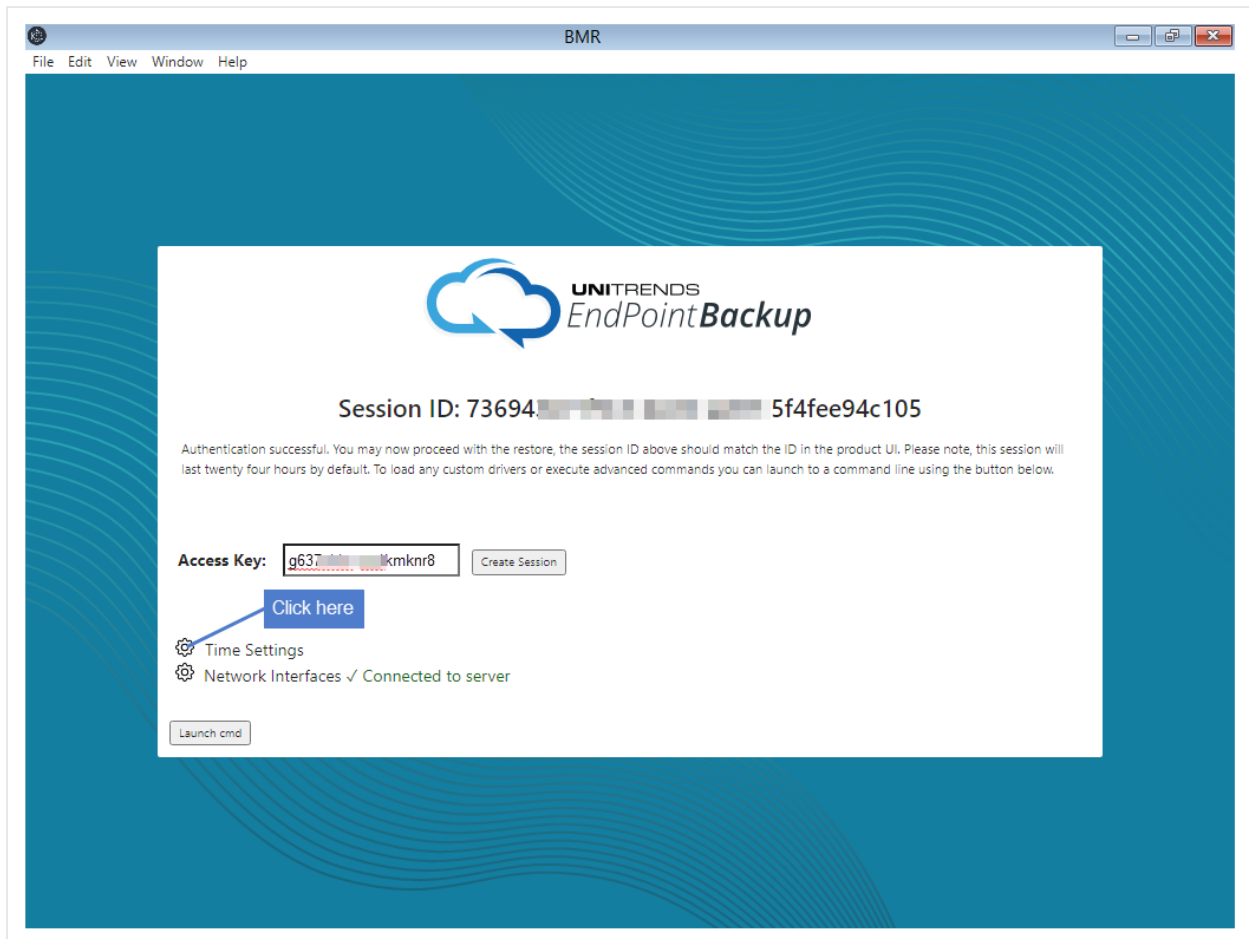
Notes:

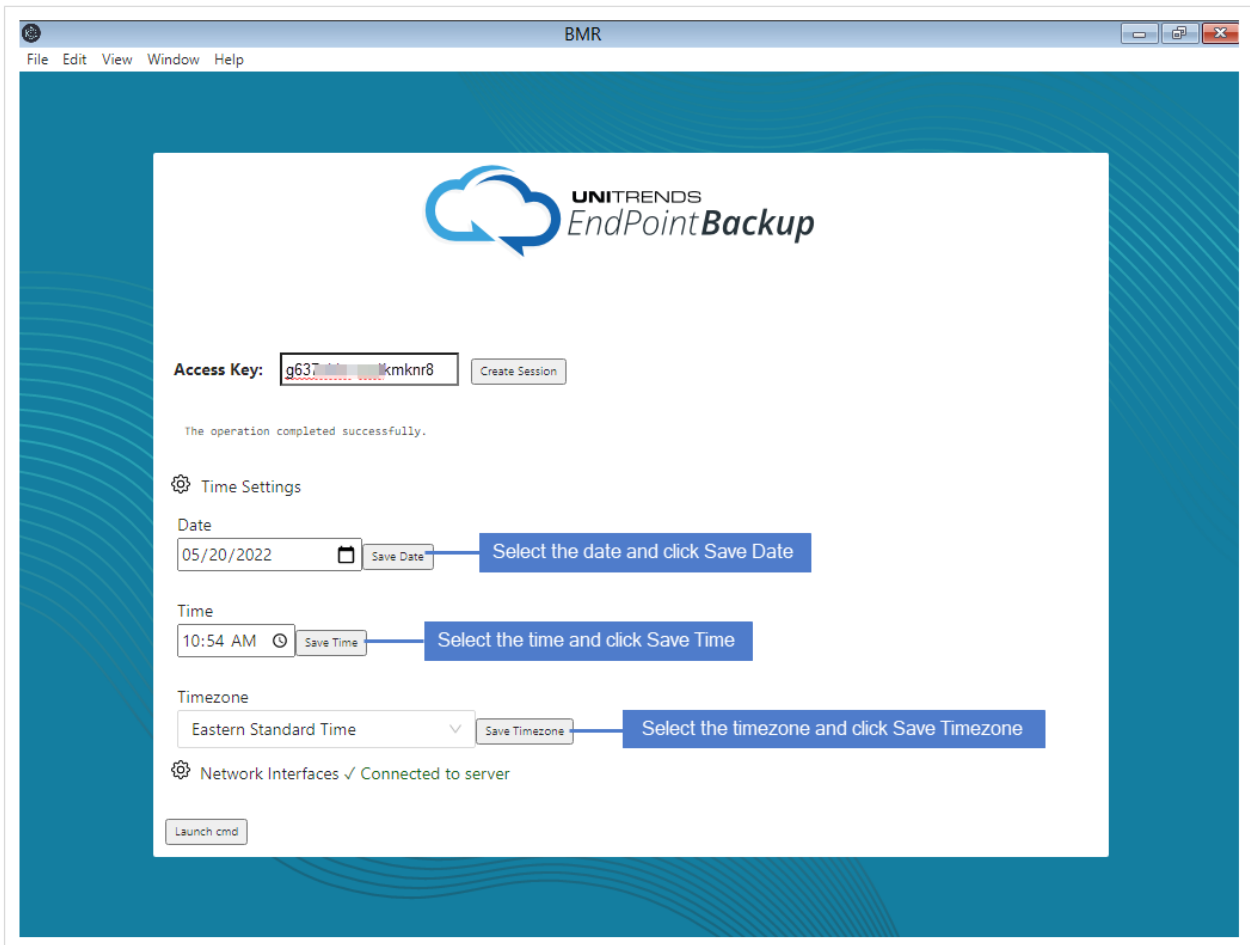
- Network settings do not need to match those of the original asset. The only requirement is that the machine can communicate with EndPoint Backup (to access the backup you will use for recovery).
- The network settings that you configure during this step are used only for the recovery. They are not applied to the network adapter when you boot into the recovered operating system. Before connecting the recovered asset to your network, you will reconfigure the asset's network settings.





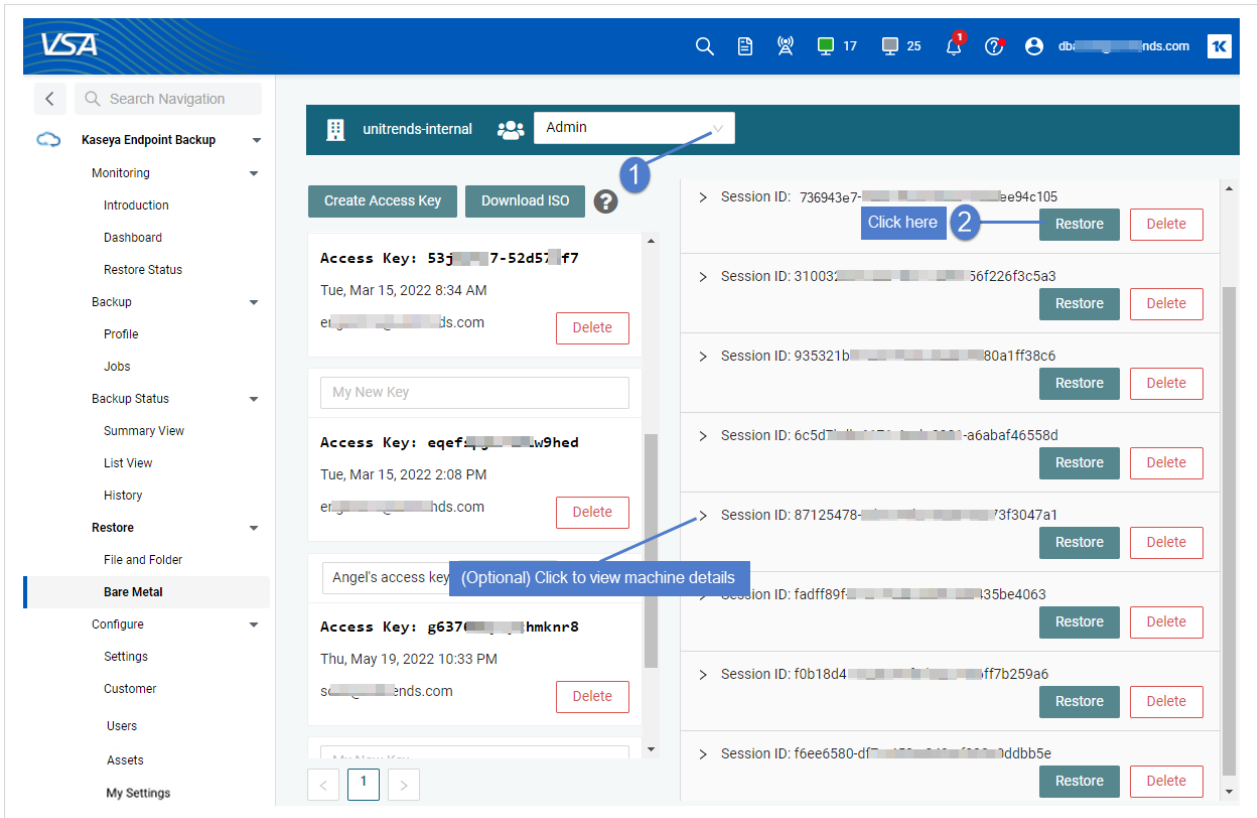
- 9 Click **Time Settings**. Select and save the date, time, and timezone of the Unitrends appliance storing the backup or hot backup copy that you will use for recovery.





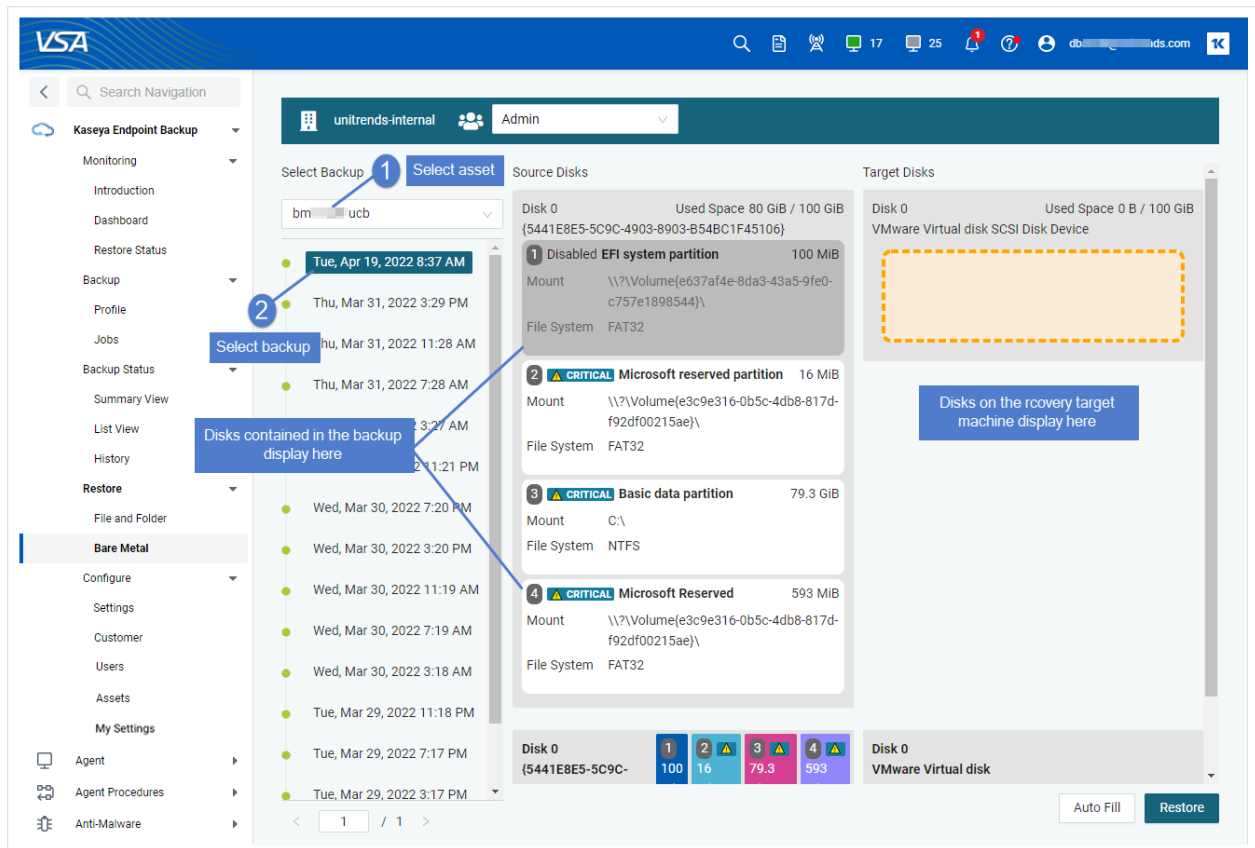
- 10 Return to the Kaseya EndPoint Backup **Restore > Bare Metal** page.
- 11 Select the customer whose backup you will recover
- 12 Locate your recovery session and click **Restore**.

Note: To view information about the machine you are recovering to, click > to expand session details.



13 Select the failed asset and the backup to recover.

Note: You can filter the asset list by entering text in the Choose Asset field. Only assets containing the string you entered display in the list.



14 Click **Auto Fill**. Source disks are mapped to disks on the target machine. In our example, source disks 2, 3, and 4 will be recovered to Disk 0 on the target machine.

15 Review the disk mapping. If needed, modify the mapping. Simply drag a disk to move it to another location on the target.

Notes:

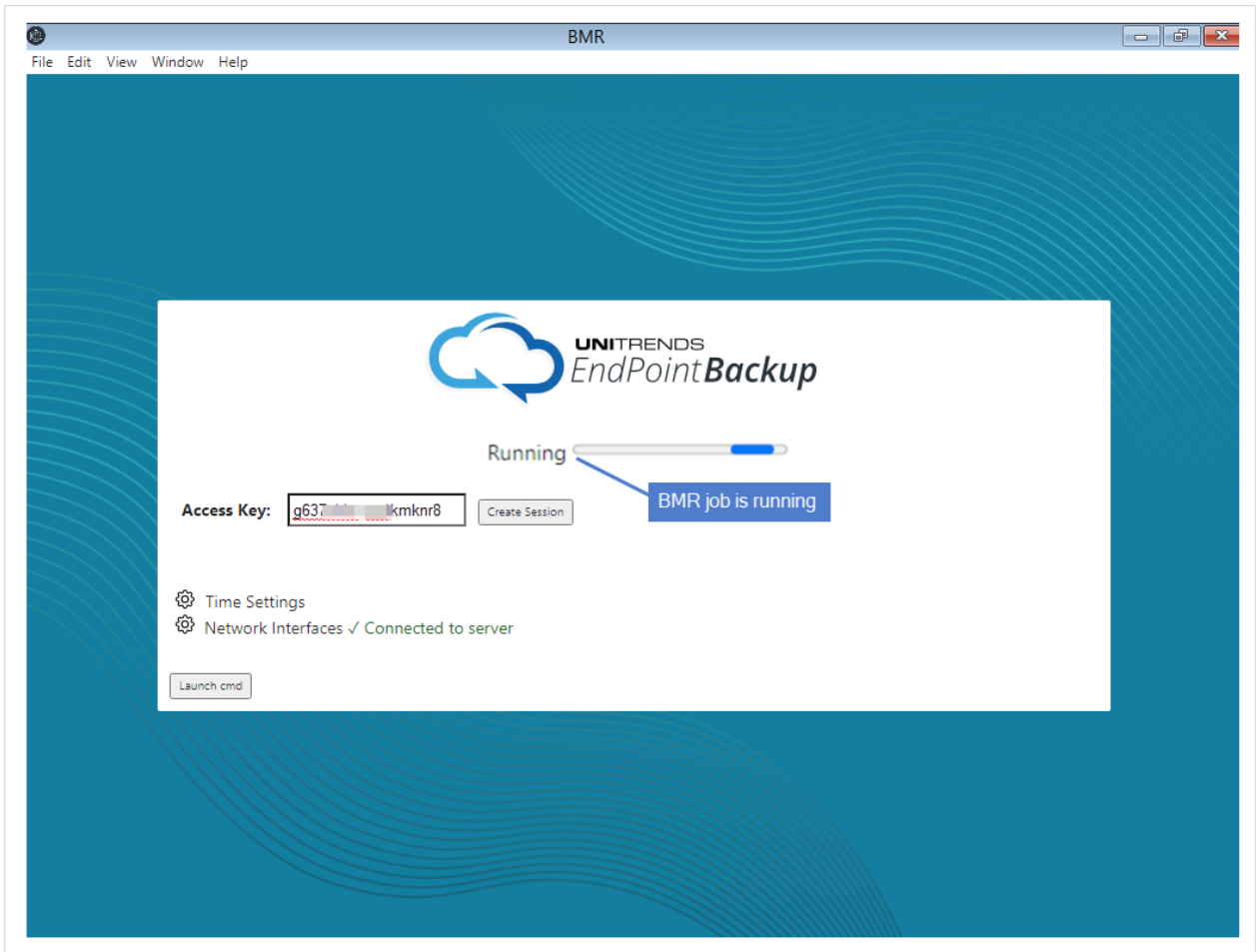
- You must recover all critical disks.
- You cannot recover non-critical disks. After performing the bare metal recovery, run the "To recover files" procedure to restore data from non-critical disks.

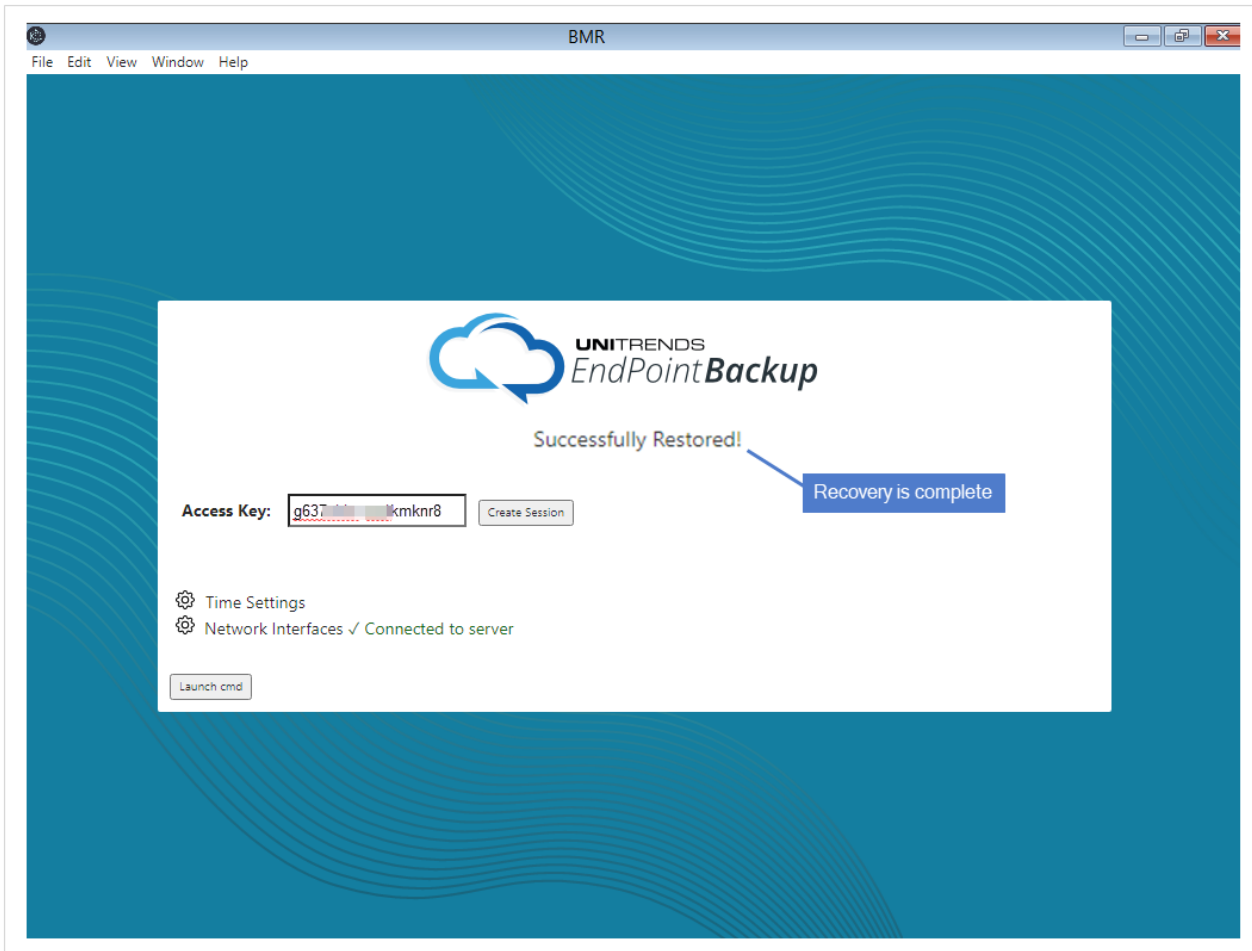
16 Click **Restore**. Click **Delete Data & Start Restore** to confirm.

The screenshot shows the Unitrends BMR interface with the following components:

- Header:** unitrends-internal | Admin
- Select Backup:** A dropdown menu showing a list of backup dates, with 'Tue, Apr 19, 2022 8:37 AM' selected.
- Source Disks:**
 - Disk 0: Used Space 100 MiB / 100 GiB. Contains a '1 Disabled EFI system partition' (100 MiB, FAT32).
- Target Disks:**
 - Disk 0: Used Space 79.9 GiB / 100 GiB. Contains:
 - '2 CRITICAL Microsoft reserved partition' (16 MiB, FAT32)
 - '3 CRITICAL Basic data partition' (79.3 GiB, NTFS)
 - '4 CRITICAL Microsoft Reserved' (593 MiB, FAT32)
- Confirm Media Recovery Dialog:**
 - Warning: All of the data on the target disks will be deleted!
 - Buttons: Cancel, Delete Data & Start Restore (highlighted with a red box and blue circle '4').
- Bottom Summary:**
 - Source Disk 0: 100 MiB EFI system partition.
 - Target Disk 0: 16 MiB Micro, 79.3 GiB Basic, 593 MiB Micro.
 - Buttons: Auto Fill (1), Restore (3).
- Callouts:**
 - '2' points to the 'Review mapping and modify if needed' button.
 - '1' points to the 'Auto Fill' button.
 - '3' points to the 'Restore' button.

17 The recovery starts. Return to the BMR interface. Recovery is complete when you see the message *Successfully Restored*.





18 When the bare metal recovery is complete, use these steps to complete the recovery:

Note: Known bare metal recovery issue – In certain cases the Windows Start button does not function on the recovered asset. This will be fixed in an upcoming release.

- Restart the machine and configure network settings for the recovered asset. The network settings that were used for the recovery are not retained after booting into the recovered operating system. Consider the following when configuring network settings:
 - If the original asset is still connected to the network, you must assign the recovered asset a unique IP address and rename it before connecting to the network to avoid conflicts.
 - If the original asset is no longer connected to the network, you can assign the recovered asset the same IP address as the failed asset.
 - If you are using DHCP and the original asset is still connected to the network, rename the recovered asset to prevent conflicts.

- (If needed) The bare metal recovery restored only the system critical volumes. If backups of the original Windows machine include other volumes, you must create and format those additional volumes.
- Install the agent on the recovered asset. For details, see ["To install or upgrade the agent manually on a single asset"](#).
- (If needed) To restore data on non-critical volumes, recover files/folders from the failed asset's last backup to the recovered asset. For details, see ["To recover files"](#).
- The recovered asset is treated as a new asset. To protect the recovered asset, add or modify job schedules. For details, see ["To create a backup job"](#) or ["To edit a backup job"](#).

This page is intentionally left blank.



Chapter 6: Monitoring Agents, Assets, Backups, and Restores

Use the Dashboard, Backup Status, and Restore Status pages to monitor your Kaseya EndPoint Backup environment. See these topics for details:

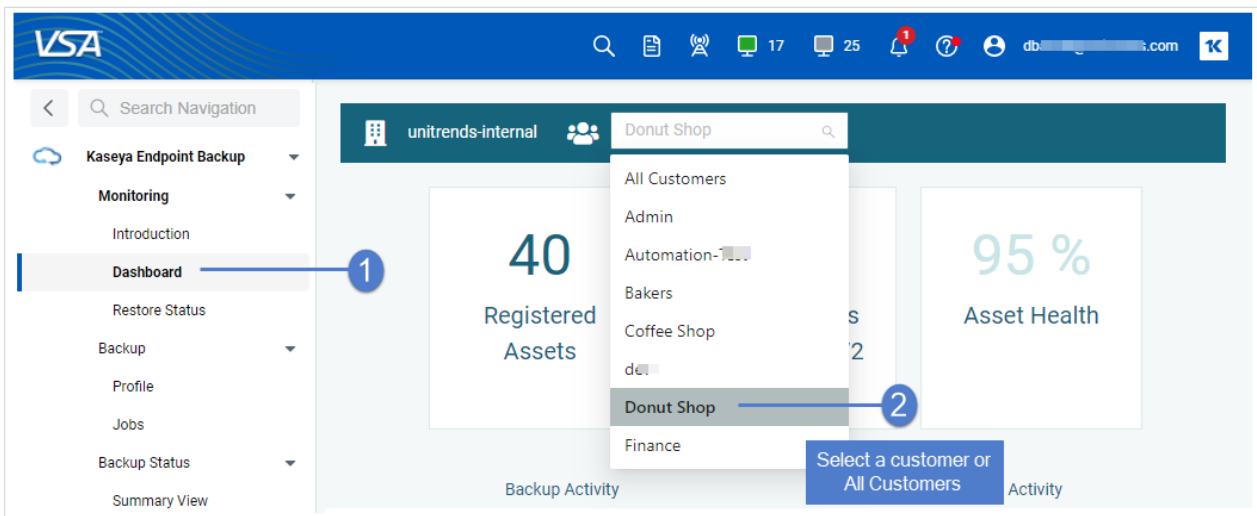
- "Working with the Dashboard"
- "Viewing backup status"
- "Viewing backup history"
- "BackupIQ alerts"
- "Viewing restore status"

Working with the Dashboard

The Dashboard provides a high-level overview of your Kaseya EndPoint Backup environment from a single pane of glass.

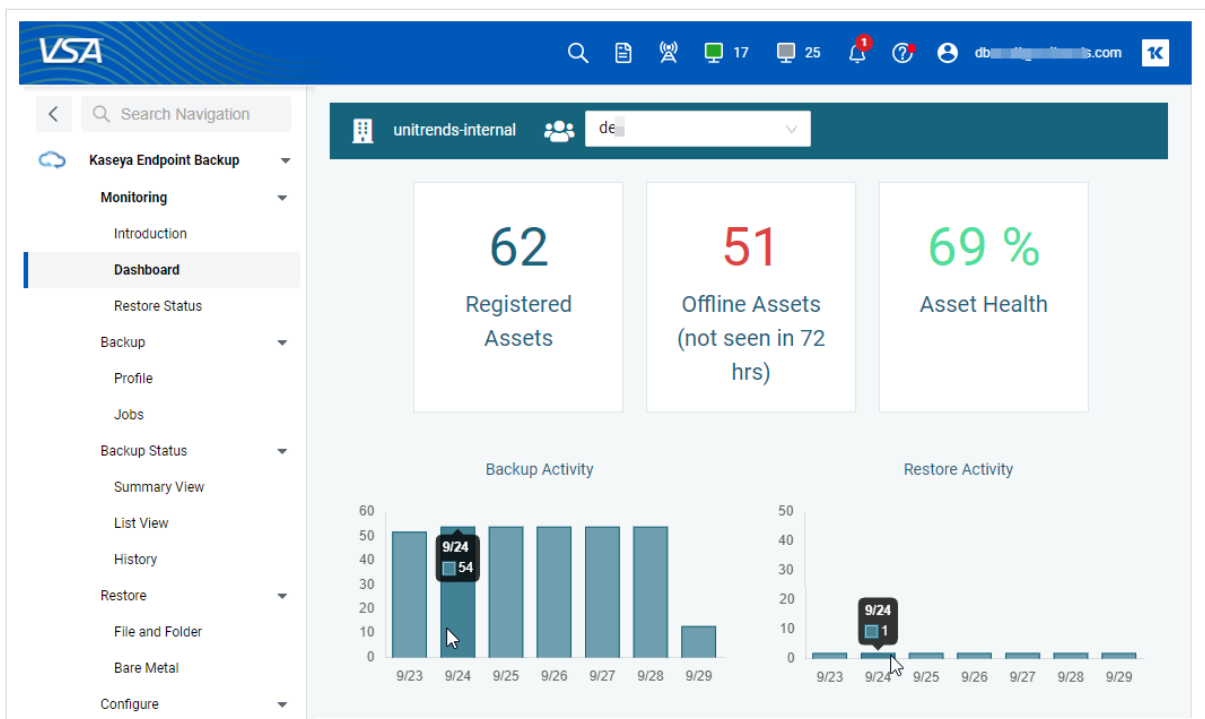
To view the Dashboard

- 1 Select **Dashboard**.
- 2 Select a customer or **All Customers** from the drop-down list in the customer context banner.
 - Select one customer for an overview of that customer's agents and assets.
 - Select **All Customers** for a quick overview of the agents and assets across your entire Kaseya EndPoint Backup environment.

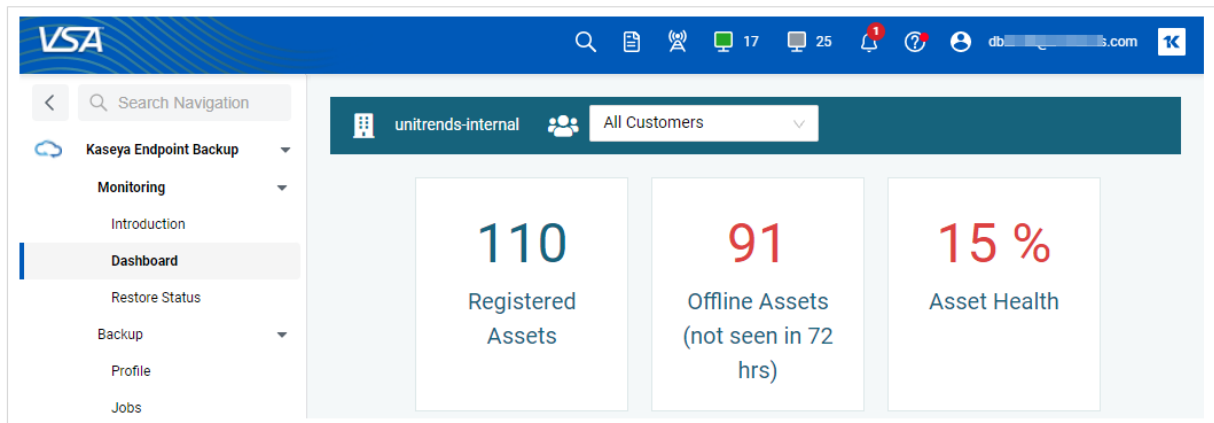


3 An overview of the customer's assets and agents displays.

- Single customer example – When one customer is selected, the following displays:
 - Registered Agents – The number of Kaseya EndPoint Backup agents that have been added.
 - Offline Agents – The number of registered agents that have not been online over the last 72 hours.
 - Asset Health – Overall asset health.
 - Backup Activity – Backup activity over the last week. Hover over a bar in the graph to see how many jobs completed on a given day.
 - Restore Activity – Restore activity over the last week. Hover over a bar in the graph to see how many jobs completed on a given day.



- When **All Customers** is selected, the following displays:
 - Registered Agents – The number of Kaseya EndPoint Backup agents that have been added.
 - Offline Agents – The number of registered agents that have not been online over the last 72 hours.
 - Asset Health – Overall asset health.

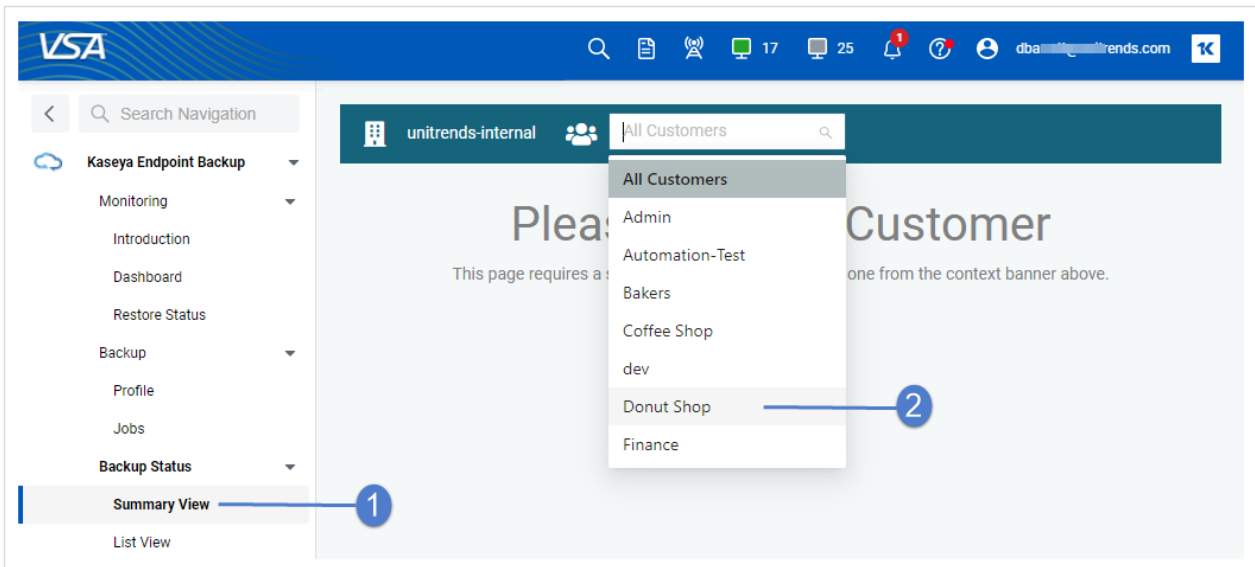


Viewing backup status

The Backup Status Summary View and List View pages show the results of backup job activity.

To view backup status

- 1 Select **Backup Status > Summary View**.
- 2 Select the customer whose jobs you will view.



- 3 The Summary View displays the following for each protected asset:

- Hostname – Name of the protected asset.

Note: If the asset has been decommissioned, **DELETED AGENT** displays next to the asset name. If a Delete All procedure is currently running for the asset, **Deleting ALL** displays next to the asset name.

- Today – Icons indicating the status of today's most recent backup jobs: ● Success, ▲ (some jobs succeeded, some jobs failed), ✖ Failed, 🔄 Running, or ● (no jobs ran).
- 1 Week Ago – Icons indicating the status of last week's backup jobs: ● Success, ▲ (some jobs succeeded, some jobs failed), ✖ Failed, 🔄 Running, or ● (no jobs ran).

Organization	Machine Group	Machine ID	Hostname	Today	1 Week Ago
myOrg	base	v-1-stag-1	v-1-stag-1	DELETED AGENT	
myOrg	base	ucb-windows-10-5	v-1-stag-1-kd-part-2	● ● ● ● ● ● ● ●	● ● ● ● ● ● ● ● ✖ ✖
myorg	base	v-1-stag-1	v-1-stag-1-kub-2022-05-17-11:00:00	● ● ● ● ● ▲ ● ●	● ● ● ● ● ● ● ● ▲ ●
myorg	base	v1-stag-k	v11-1-stag-kub-2022-05-17-11:00:00	● ● ● ● ● ● ● ●	● ● ● ● ● ● ● ●
myorg	base	v-1-stag-1	v-1-stag-1	DELETING ALL	
myorg	base	v-1-stag-1	v-1-stag-1	● ● ● ● ● ● ● ●	● ● ● ● ● ● ● ●

- (Optional) Click a status icon to view details.

Organization	Machine Group	Machine ID	Hostname	Today	1 Week Ago
myOrg	base	v-1-1-staging-1	v-1-1-staging-1 Deleted AGENT	● ● ● ● ● ● ● ●	● ● ● ● ● ● ● ●
myOrg	base	uct-windows-10-5	v-1-22-staging-kd-part-2	● ● ● ● ● ● ● ●	● ● ● ● ● ● ● ● ● ●
myorg	base	v-1-25-staging-11-11-11	v-1-25-staging-kub-2022-05-17-11-11-11	● ● ● ● ● ● ● ● ● ●	● ● ● ● ● ● ● ● ● ●
myorg	base	v1-staging-k	v11-1-staging-kub-21-75	● ● ● ● ● ● ● ●	● ● ● ● ● ● ● ● ● ●
myorg	base	v-1-21-staging-	v-1-21-staging-DELETING ALL	● ● ● ● ● ● ● ●	● ● ● ● ● ● ● ● ● ●
myorg	base	v-1-16-staging-	v-1-16-staging-uct-100-113	● ● ● ● ● ● ● ●	● ● ● ● ● ● ● ● ● ●

The List View displays backups for the asset and day you selected. The following details display on the List View page:

- Date fields – Date range of jobs displayed.
- Select Assets field – Select one or more assets to filter the jobs list.
- Asset – Name of the protected asset.
- Status icon – Job status: Running, Success, Warning, or Failed.
- Previously Successful – Time since the last successful backup.
- File Count – Number of files in the backup.
- Protected – Protected size.
- Duration – Job run time.
- Avg Transfer Rate – The job's average data transfer rate in MB/s.
- Job – Job name. *Deleted* displays if the job has been removed.
- Profile – Backup profile used by the job:
 - icon indicates the profile runs file and folder backups.
 - icon indicates the profile runs system state backups.
 - *Deleted* displays if the profile has been removed.

- Start Time – Date and time at which the backup job started.
- End Time – Date and time at which the backup job finished.
- Task – Job ID. Click to view job log.

Organization	Machine Group	Machine ID	Asset	Status	Last Backup	File Count	Protected	Duration	Avg Transfer Rate	Job	Profile	Start Time	End Time	Task
			ws-ka-10168	●	2 days	3858	1.46 GiB	15 minutes	16.6 Mbit/s	Tejas Te...	User Folder Profile	Sun, May 22, 2022 9:42 AM	Sun, May 22, 2022 9:57 AM	5f63566a
			ws-ka-10168	●	2 days	12653	3.57 GiB	21 minutes	24.86 Mbit/s	Tejas Te...	User Folder Profile	Fri, May 20, 2022 9:42 AM	Fri, May 20, 2022 10:03 AM	c2d5731f
			ws-ka-10168	●	2 days	34653	8.11 GiB	24 minutes	51.2 Mbit/s	Tejas Te...	User Folder Profile	Wed, May 18, 2022 9:41 AM	Wed, May 18, 2022 10:05 AM	58430f99
			ws-ka-10168	●	5 days	34214	7.98 GiB	18 minutes	63.26 Mbit/s	Tejas Te...	User Folder Profile	Mon, May 16, 2022 9:40 AM	Mon, May 16, 2022 9:58 AM	f07b4cf7
			ws-ka-10168	✖	4 days	8600	2.36 GiB	13 hours	424.67 Kbit/s	Tejas Te...	User Folder Profile	Sun, May 15, 2022 8:24 PM	Mon, May 16, 2022 9:40 AM	4d0df728

Click a task to view log details in the Task Details dialog.

(Optional) Click **Download Logs** to download a .zip file of the asset's recent log files. If you do not see this button, either this feature has not been enabled or the asset is running a pre-1.30 agent version. (For details, see "Working with asset log storage".)

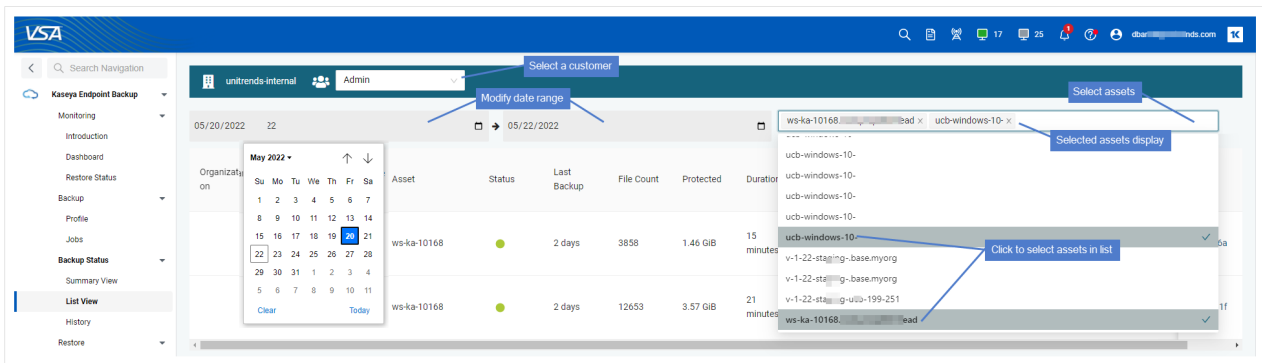
The screenshot shows the 'Task Details' dialog box for a specific backup task. The dialog contains the following information:

- asset**
- agent_version**: "10.6.1.1740"
- agent_version_cloud**: "1.24.0"
- asset_uuid**: "f6e086d2-8749-4f58-803a-3059f54e2dfc"
- compatible_profile**: true
- customer_id**: 29
- delete_state**: "NODELSTATE"
- enabled**: true
- id**: 2791
- job_uuid**: "68732d85-4728-4588-8099-335ec54c0166"
- last_known_status**: "REGISTERED"
- last_seen**: "2022-05-22T16:52:08.876Z"
- name**: "WS-KA-10168"

Callouts in the image indicate: 1. Click a task (pointing to a task ID in the list view), 2. Log details display (pointing to the dialog title), 3. Download Logs (pointing to the button), and 4. (Optional) (pointing to the dialog title).

5 (Optional) Display other jobs on the List View page by modifying any of the following:

- Selected customer – Select a different customer in the Customer list.
- Date range – Modify the date range by clicking the calendar icons and selecting new dates.
- Selected assets – Select one or more assets from the list. You can enter text to filter listed assets. Click X to clear the assets filter.



Viewing backup history

The backup history graphs provide an at-a-glance view of overall asset health and the number of successful, failed, and in-progress backups over a specified date range.

Asset health is measured by the number of days since the last successful backup. By default, assets are *healthy* (green) if there is a successful backup in the last 3 days, *at risk* (yellow) if there is a successful backup in the last 4-7 days, and *critical* (red) if there is no successful backup in over 7 days.

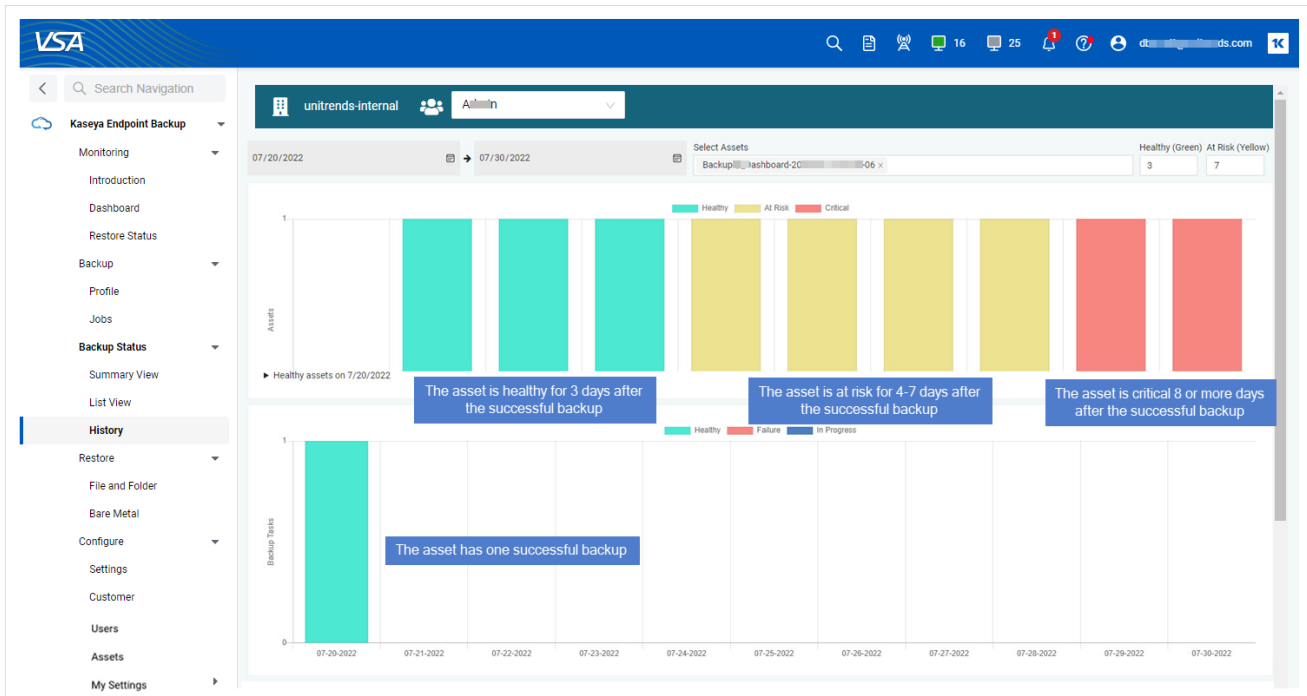
You can opt to:

- Modify the date range included in the graphs. The maximum date range is 31 days. If you attempt to enter a range of greater than 31 days, the start date or end date is automatically modified to include 31 days.
- Filter the view by selecting a customer
- Modify the number of days used to measure asset health
- Filter the view by selecting which assets to include
- View asset details by clicking a bar in the asset health graph

For details on working with the Backup History page, see the "[Asset health example](#)" and the "[To view backup history](#)" procedure.

Asset health example

In the example below we have selected a simple case. This example is one asset that was backed up on 7/20/2022. No additional backups have been taken. Setting the 3 days for Healthy and 7 days for At Risk demonstrate how the report ages out the machine. For the first 3 days the asset is considered healthy, then for 4 days it is at risk, and finally on the 8th day it is critical.

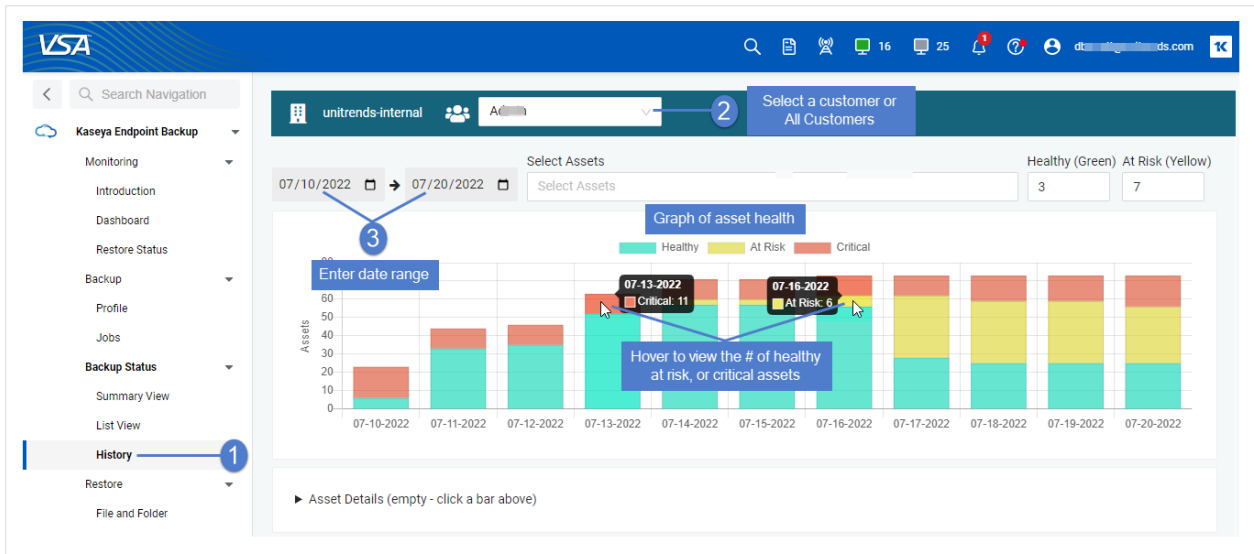


To view backup history

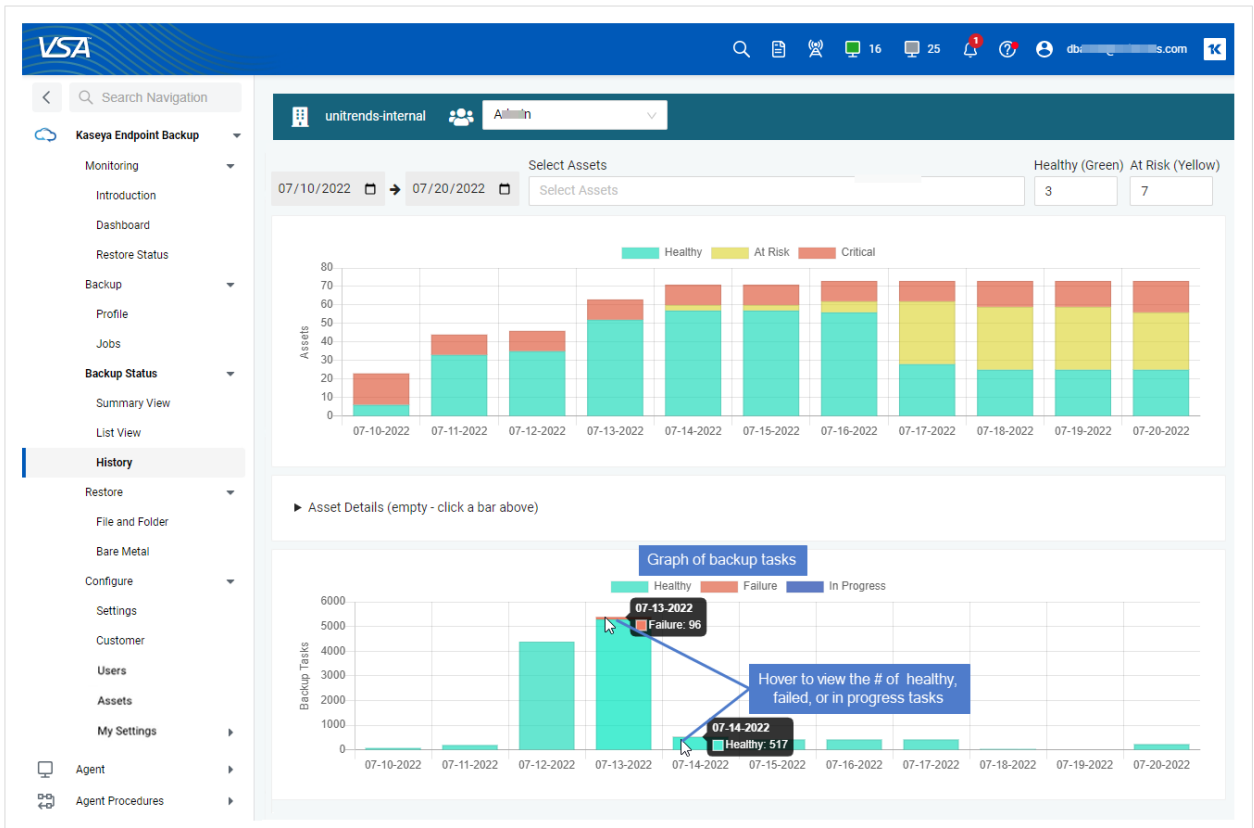
- 1 Select **Backup Status > History**.
- 2 Select a customer or **All Customers** from the drop-down list in the customer context banner.
 - Select one customer for an overview of that customer's asset health and backup tasks.
 - Select **All Customers** for a quick overview of asset health and backup tasks across your entire Kaseya EndPoint Backup environment.
- 3 (Optional) Modify the backup date range.

Note: The maximum date range is 31 days. If you attempt to enter a range of greater than 31 days, the start date or end date is automatically modified to include 31 days.

Asset health displays in the top graph. Hover over a bar in the graph to see the number of healthy, at risk, or critical assets for a given day.

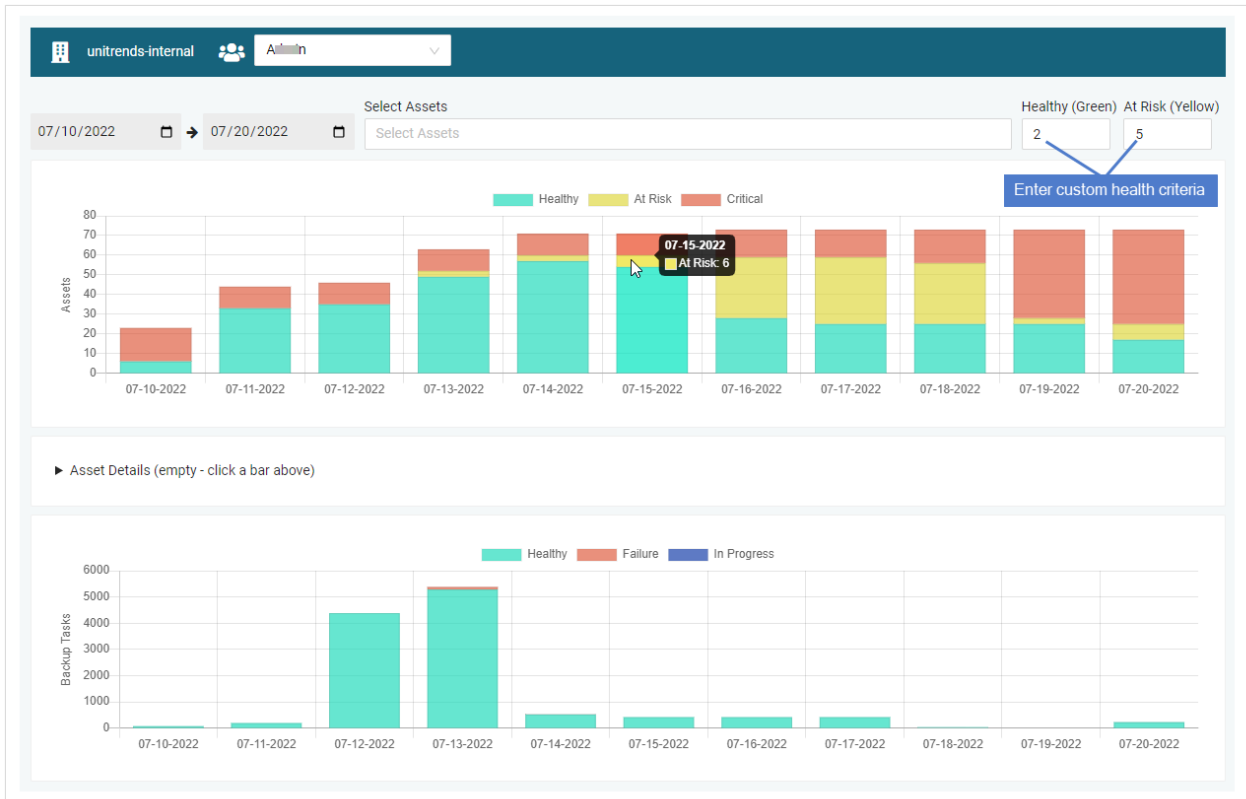


Backup tasks display in the bottom graph. Hover over a bar in the graph to see the number of *healthy* (green), *failed* (red), or *in progress* (blue) tasks for a given day.



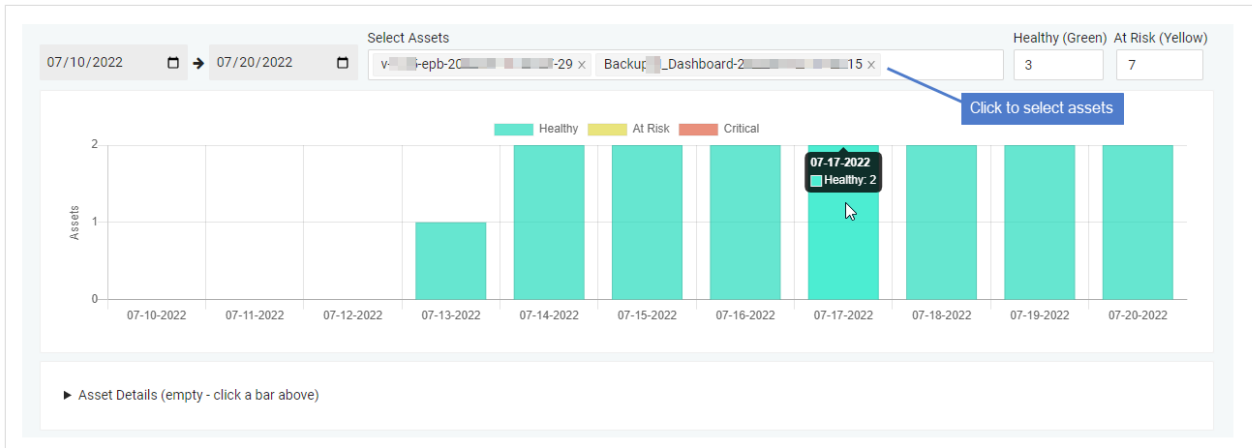
- 4 (Optional) Enter custom asset health criteria. In the following example, assets are *healthy* (green) if there is a successful backup in the last 2 days, *at risk* (yellow) if there is a successful backup in the last 3-5 days, and *critical* (red) if there is no successful backup in over 5 days:

Backup tasks display in the bottom graph. Hover over a bar in the graph to see the number of *healthy* (green), *failed* (red), or *in progress* (blue) tasks for a given day.

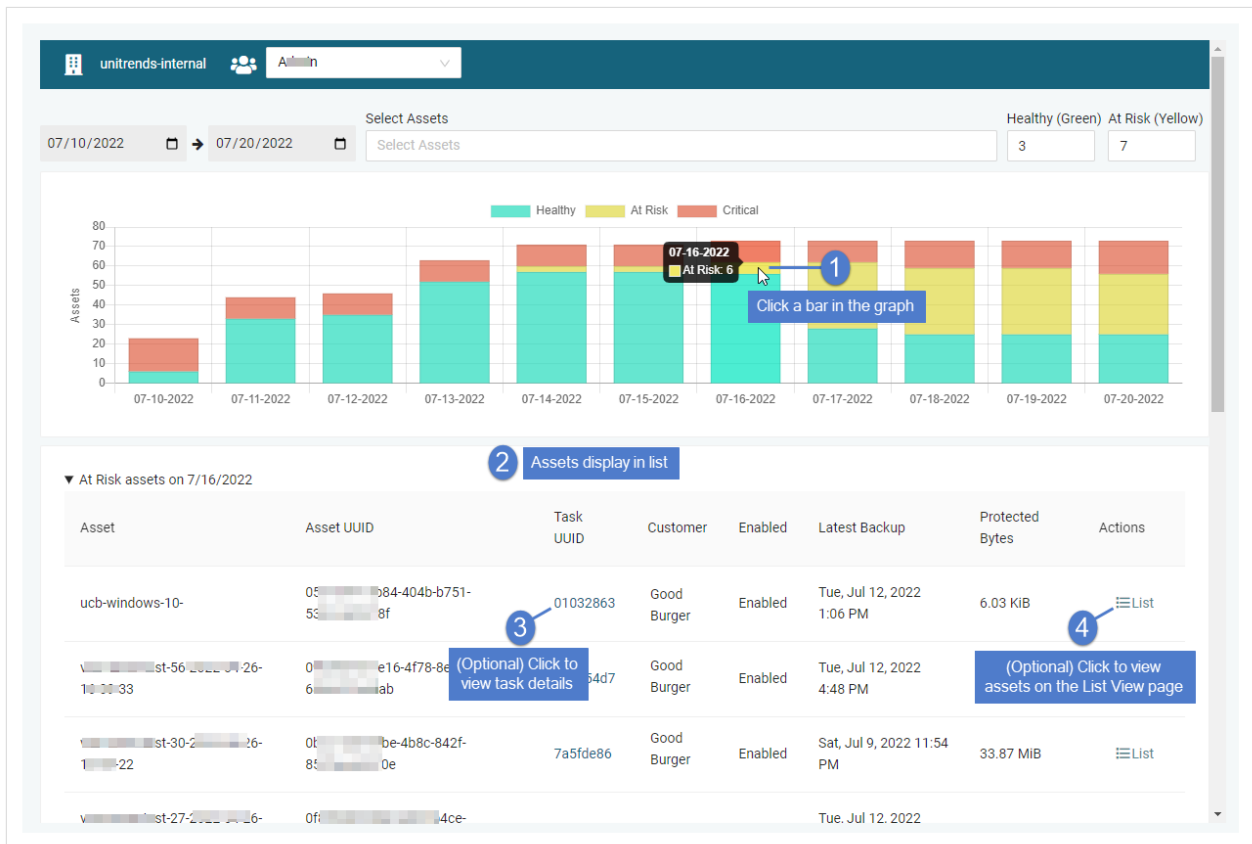


- 5 (Optional) Filter by asset:

Note: Select Assets is not available when viewing All Customers. To filter by asset, you must first select a customer.



6 (Optional) Click a bar in the asset health graph to view asset details. In our example, the at risk assets on 07/16/2022 display:



BackupIQ alerts

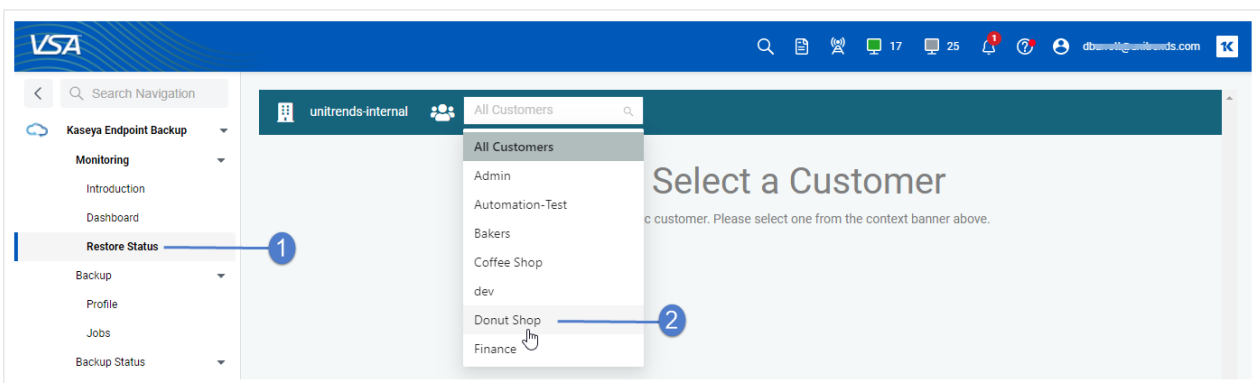
The UniView Portal (formerly known as *Unitrends Backup Portal*) has a conditional alarm feature that enables you to set a threshold for how long a machine can go without a good backup. If the threshold is exceeded, an alarm is generated and added to the Portal's BackupIQ Alerts list. You now have the option to integrate the UniView Portal module and set up backup alerting for your Kaseya EndPoint Backup job tasks. For details, see "[Working with your BackupIQ integration](#)".

Viewing restore status

The Restore Status page shows the results of restore job activity.

To view restore job status

- 1 Select **Restore > Restore Status**.
- 2 Select the customer whose jobs you will view.



- 3 The Restore Status page displays the following for each job:
 - Job – Job UUID.
 - Target Asset – Asset where files were recovered.
 - Start Time – Date and time at which the job started.
 - End Time – Date and time at which the job finished.
 - Status icon – Job status: 🔄 *Running*, ● *Success*, ▲ *Warning*, or ✖ *Failed*.

The screenshot displays the VSA Kaseya EndPoint Backup interface. The left sidebar contains navigation options: Monitoring, Introduction, Dashboard, Restore Status (selected), Backup, Profile, Jobs, Backup Status, Summary View, List View, History, Restore, File and Folder, Bare Metal, Configure, Settings, Users, Assets, and My Settings. The main area shows a table of backup jobs with columns: Target Machine ID, Machine Group, Organization, Task ID, Job, Type, Target, Start Time, End Time, and Status. Annotations include: 'Click a heading to sort by column' pointing to the Job column header; 'Click to view other pages' pointing to the page number '4' in the pagination; and 'Jobs per page' pointing to the dropdown menu showing options like 10/page, 20/page, 50/page, and 100/page.

Target Machine ID	Machine Group	Organization	Task ID	Job	Type	Target	Start Time	End Time	Status
v-1-15-staging-1	base	myOrg	450b5f8c	d25fac8-ff52-47fd-8b7a-a60a3f62cdd1	File & Folder	v-1-15-staging-kcb-199-149	Mon, May 24, 2021 2:48 PM	Mon, May 24, 2021 2:51 PM	●
			0c1b952c	d25fac8-ff52-47fd-8b7a-a60a3f62cdd1	File & Folder	v-1-15-staging-kcb-199-154	Mon, May 24, 2021 12:42 PM	Mon, May 24, 2021 12:45 PM	●
				d3d3-ec31/350/88z	Folder	kcb-199-32	PM	PM	●
v-1-13-staging-1	base	myorg	c59d68db	9366c943-73eb-40e2-b3b4-1ddd89d02726	File & Folder	v-1-13-staging-kcb-215-203	Thu, Mar 18, 2021 7:07 PM	Thu, Mar 18, 2021 9:29 PM	✖
v-1-13-staging-1	base	myorg	b5b1707f	6970070f-26d3-49fe-aca2-07d004c984b8	File & Folder	v-1-13-staging-kcb-215-203	Wed, Mar 3, 2021 6:02 PM	Wed, Mar 3, 2021 6:05 PM	●
			ba3e3e57	58a35587-56b4-4976-bf90-53a0e4a46c5c	File & Folder	v-1-13-staging-kcb-215-179	Wed, Feb 10, 2021 4:06 PM	Wed, Feb 10, 2021 4:06 PM	●

This page is intentionally left blank.



Chapter 7: Working with Customers, Assets, and Users

Use the procedures in this chapter to manage customers, assets, and users, and to modify your user account settings. See these topics for details:

- ["Working with customers"](#)
- ["Working with users"](#)
- ["Working with users"](#)
- ["Working with your user account settings"](#) – Use these procedures to change your password or enable login with IT Complete.

Working with customers

Use these procedures to manage your customers:

- ["To view customers"](#)
- ["To add a customer"](#)
- ["To enable or disable a customer"](#)

To view customers

- 1 Select **Configure > Customer**.
- 2 The Customer page displays the following for each customer:
 - **Customer Name** – Name of the customer. Click the name to edit.
 - **Health** – Overall asset health.
 - **Assets** – The number of Kaseya EndPoint Backup assets that have been added.
 - **Offline** – The number of registered assets that have not been online over the last 72 hours.
 - **Enabled** – Button indicating whether the customer is currently enabled: *On* indicates the customer is enabled, *Off* indicates the customer is disabled.

The screenshot shows the VSA interface for managing customers. The left sidebar contains a navigation menu with categories like Monitoring, Backup, Restore, and Configure. The main content area displays a table of customers with columns for Customer Name, Health, Assets, Offline, and Enabled. The 'Bakers' customer is selected, and a callout box points to its name with the text 'Click a name to edit'. Another callout box points to the 'Customer' menu item with the text 'Click here'.

Customer Name	Health	Assets	Offline	Enabled
Admin-renamed	45%	39	38	On
After the horn test	0%	0	0	On
Automation-Test	0%	0	0	On
Bakers	0%	0	0	On
Coffee Shop	0%	0	0	On
dev	71%	201	190	On
Donut Shop	0%	0	0	Off
Customer	0%	0	0	Off

3 (Optional) To modify the display, you can:

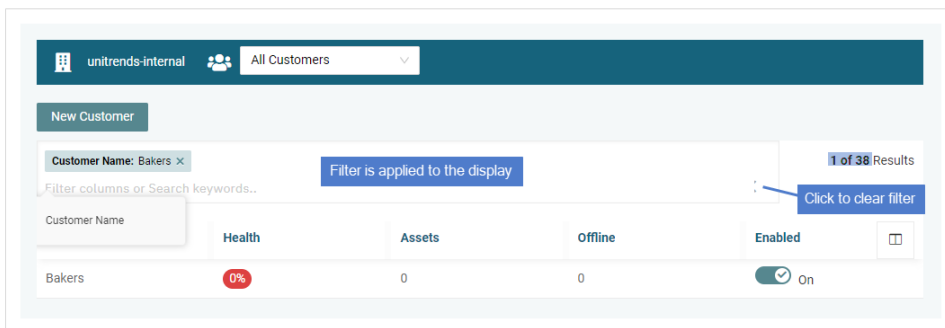
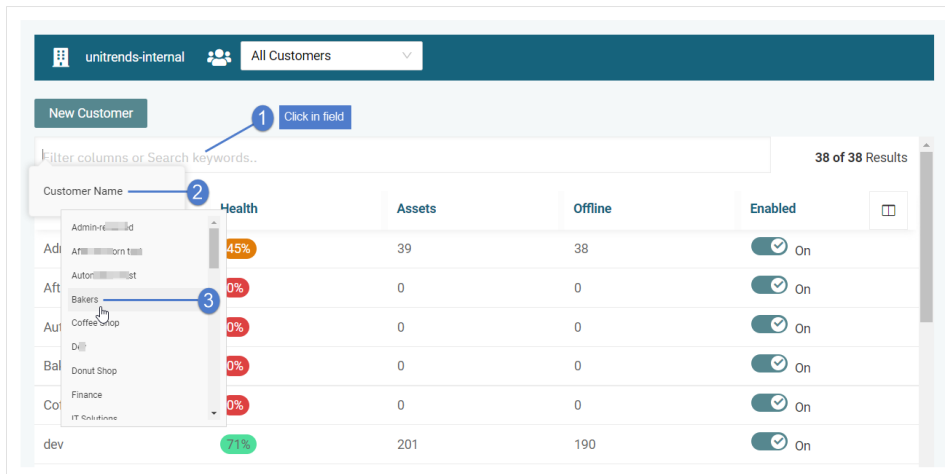
- Show, hide, and reorder columns.

The screenshot shows the VSA interface with the 'All Customers' list. A 'List View Options' dialog box is open, allowing users to customize column visibility and order. The dialog includes a 'Select All' checkbox and checkboxes for 'Customer Name', 'Health', 'Assets', 'Offline', and 'Enabled'. A callout box explains that checkboxes are used to display or hide columns, and they can be dragged to reorder. The 'Enabled' column is highlighted with a callout '1', and the 'Apply' button is highlighted with a callout '3'.

- Enter text in the *Filter columns or Search keywords* field to display only customer names that contain the string you entered.

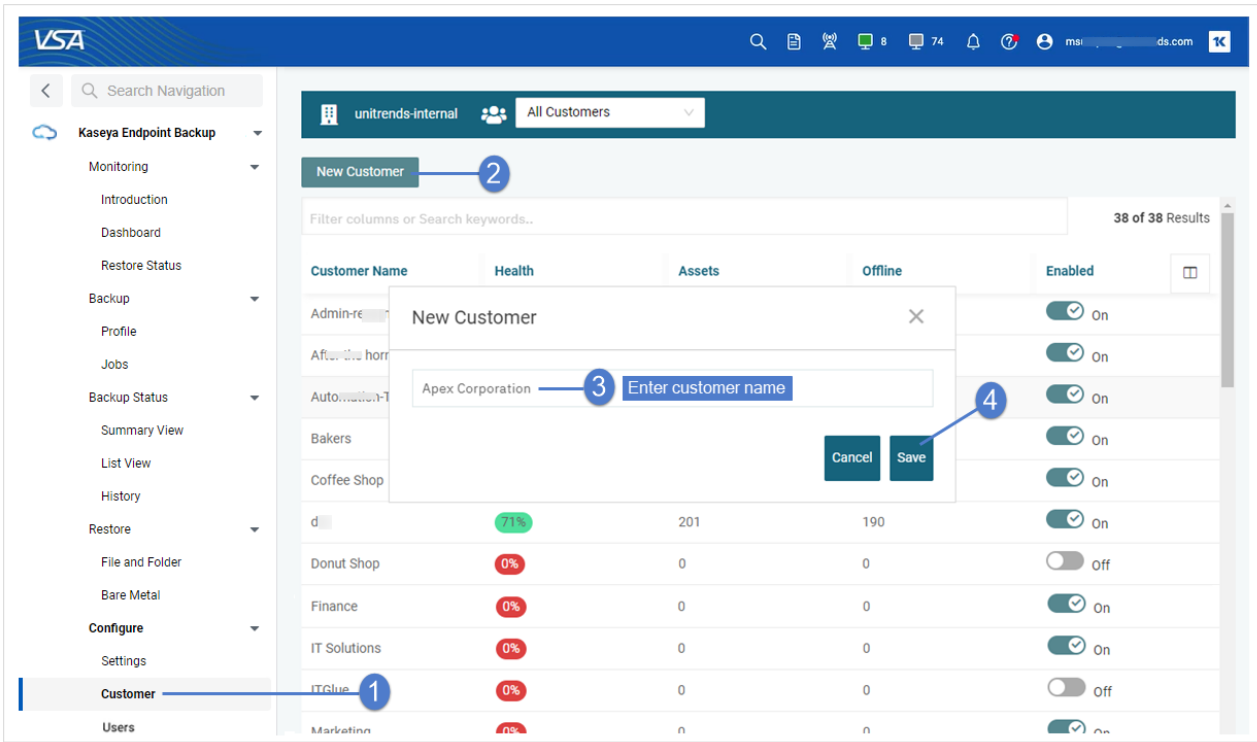
The screenshot shows the VSA interface with the 'All Customers' list filtered by the text 'store'. The 'Filter columns or Search keywords' field contains 'store' and is highlighted with a callout '1'. The results show two customers: 'Pet Store' and 'Record Store'. A callout box explains that the display is filtered to show only customers containing the string entered.

- Click in the *Filter columns or Search keywords*, click **Customer Name** and select a customer to display a single customer.

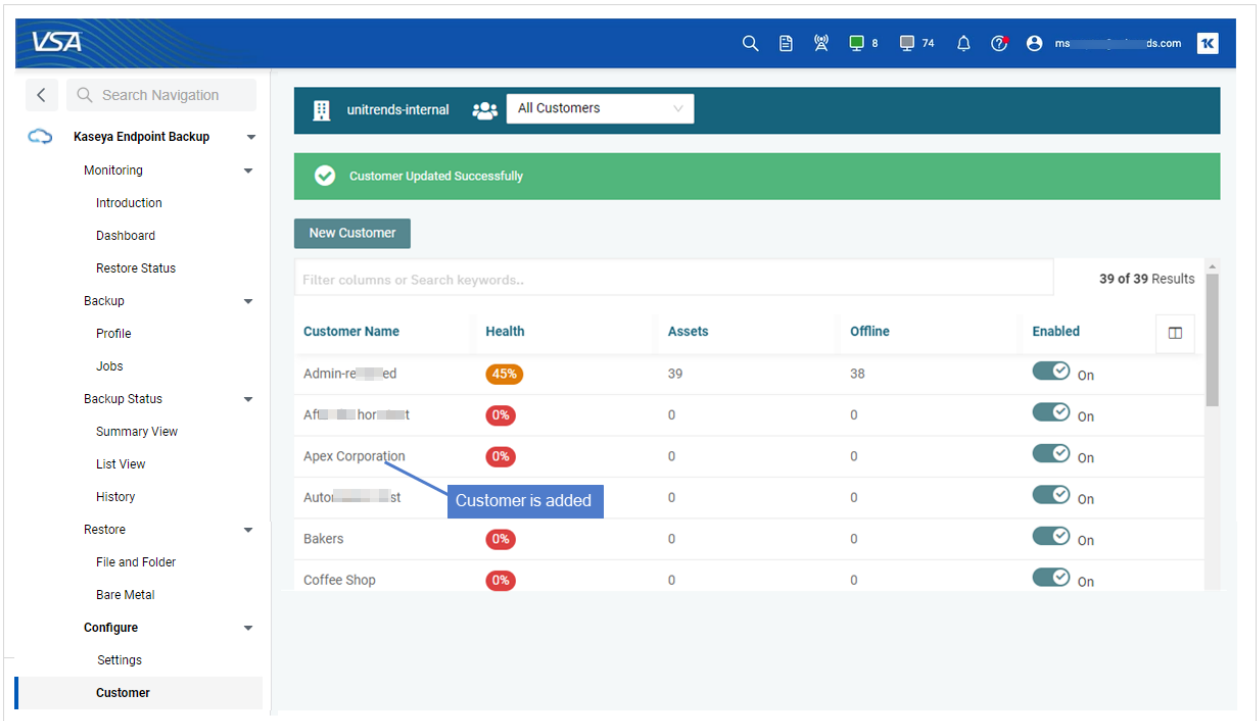


To add a customer

- 1 Select **Configure > Customer**.
- 2 Click **New Customer**.
- 3 Enter the customer name.
- 4 Click **Save**.



5 The customer is added.



To enable or disable a customer

Once a customer has been disabled, no backup jobs are run for that customer. To resume jobs for the customer, simply enable the customer.

- 1 Select **Configure > Customer**.
- 2 Locate the customer in the list.
- 3 Click the customer's Enabled button to enable or disable the customer.

Customer Name	Health	Assets	Offline	Enabled
Adm [redacted] ed	45%	39	38	On
All [redacted] on t [redacted] t	0%	0	0	Off
Apex Corporation	0%	0	0	On
Auto [redacted] st	0%	0	0	On
Bakers	0%	0	0	On
Coffee Shop	0%	0	0	On
d [redacted]	71%	203	190	On
Donut Shop	0%	0	0	Off

Working with users

Use these procedures to manage Kaseya EndPoint Backup users:






Note: If you do not see the Users page, upgrade the Kaseya EndPoint Backup TAP module to the latest version as described in "Install the Kaseya EndPoint Backup TAP module " on page 7.

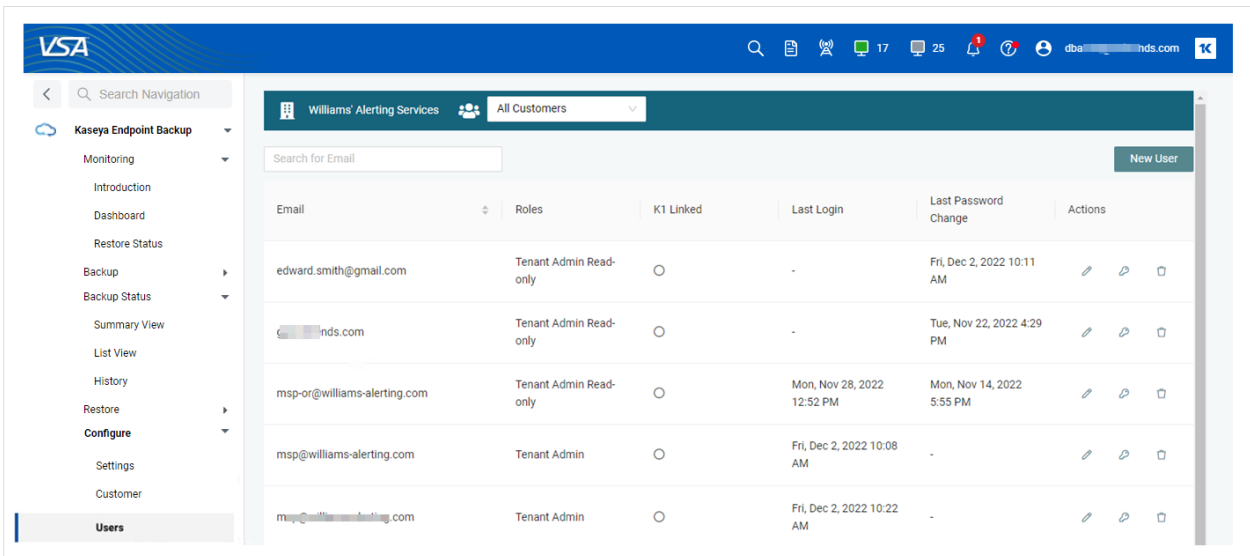
- "To view users"
- "To add a user"
- "To modify a user's role"
- "To change a user's password"
- "To delete a user"

To view users

1 Select **Configure > Users**.

2 The Users page displays the following for each user:

- Email – User's email address.
- Roles – User's role:
 - Tenant Admin – Administrator role with full access. Users with this role can perform all Kaseya EndPoint Backup tasks.
 - Tenant Admin Read-only – Administrator role with read-only access. Users with this role can view information and change their password only. These users cannot run other tasks or edit/update information.
 - System Admin – Unitrends Support role, do not use.
 - System Admin Read-only – Unitrends Support role, do not use.
- K1 Linked – Indicates whether this user account is linked to a KaseyaOne account:
 -  indicates K1 is linked, which enables the user to log in to Endpoint Backup and KaseyaOne by using single sign-on.
 -  indicates K1 is NOT linked. (The user must run the ["To enable login with IT Complete"](#) procedure to link their Endpoint Backup and KaseyaOne accounts.)
- Last Login – Date and time when the user last logged in to Kaseya EndPoint Backup.
- Last Password Change – Date and time when this user's password was last changed.
- Actions –
 - Click  to change the user's role (for details, see ["To modify a user's role"](#)).
 - Click  to change the user's password (for details, see ["To change a user's password"](#)).
 - Click  to delete the user (for details, see ["To delete a user"](#)).



To add a user

1 Select **Configure > Users**.

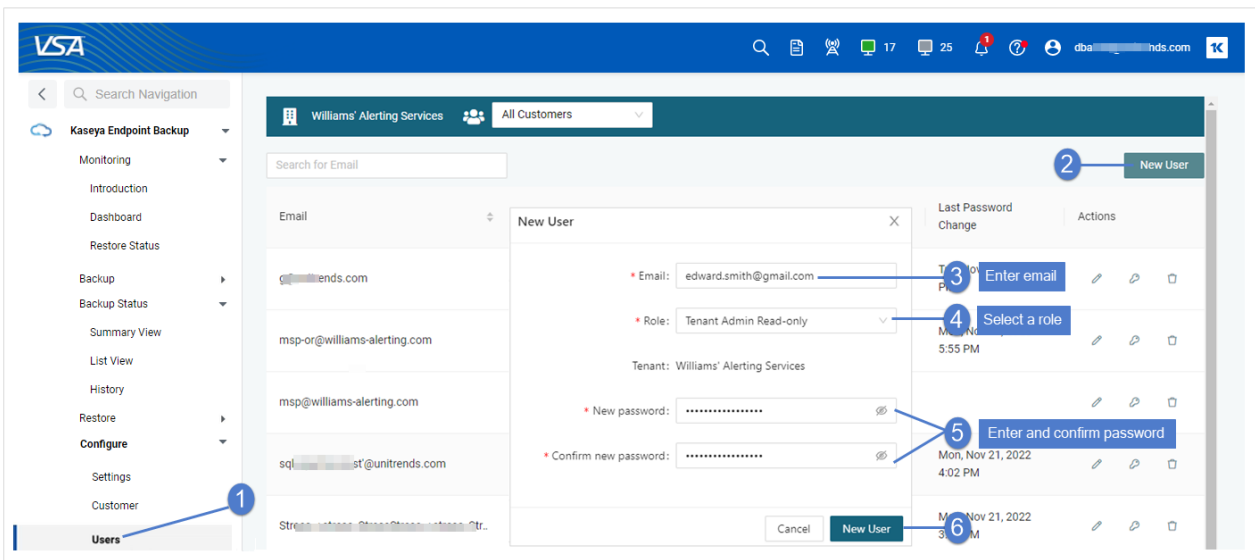
2 Click **New User**.

3 In the New User dialog:

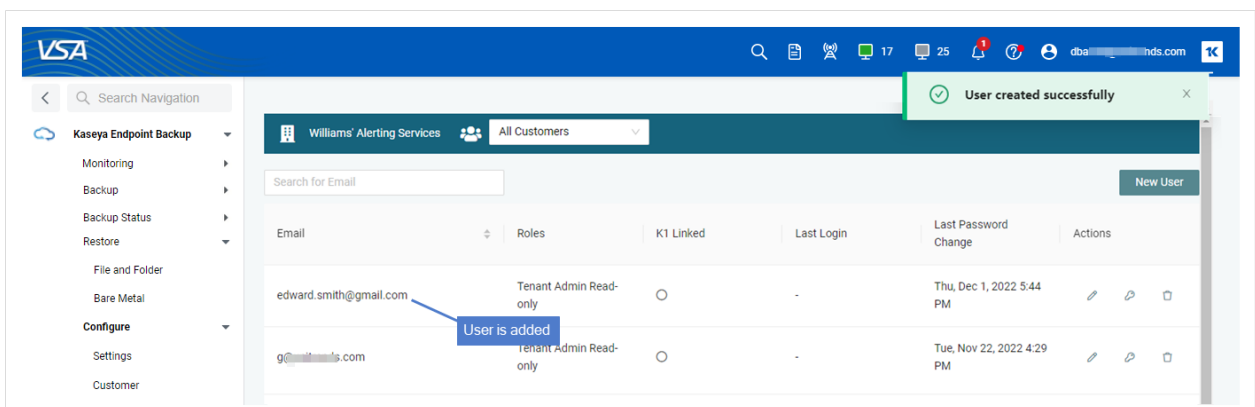
- Enter the user's email address.
- Select a role: Tenant Admin (can perform all tasks) or Tenant Admin Read-only (can view information and change their password only).

Note: Do not select the System Admin or System Admin Read-only roles. These are Unitrends Support roles.

- Enter and confirm the user's password.
- Click **New User**.



The user is added:



To modify a user's role

1 Select **Configure > Users**.

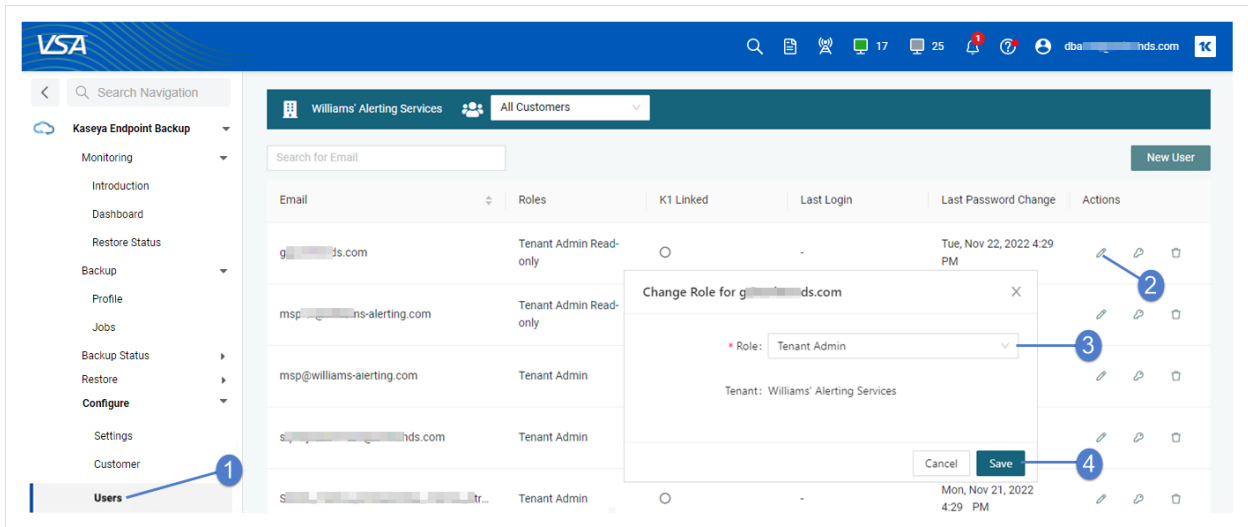
2 Locate the user and click its icon.

3 In the Change Role dialog:


- Select a new role: Tenant Admin (can perform all tasks) or Tenant Admin Read-only (can view information and change their password only).

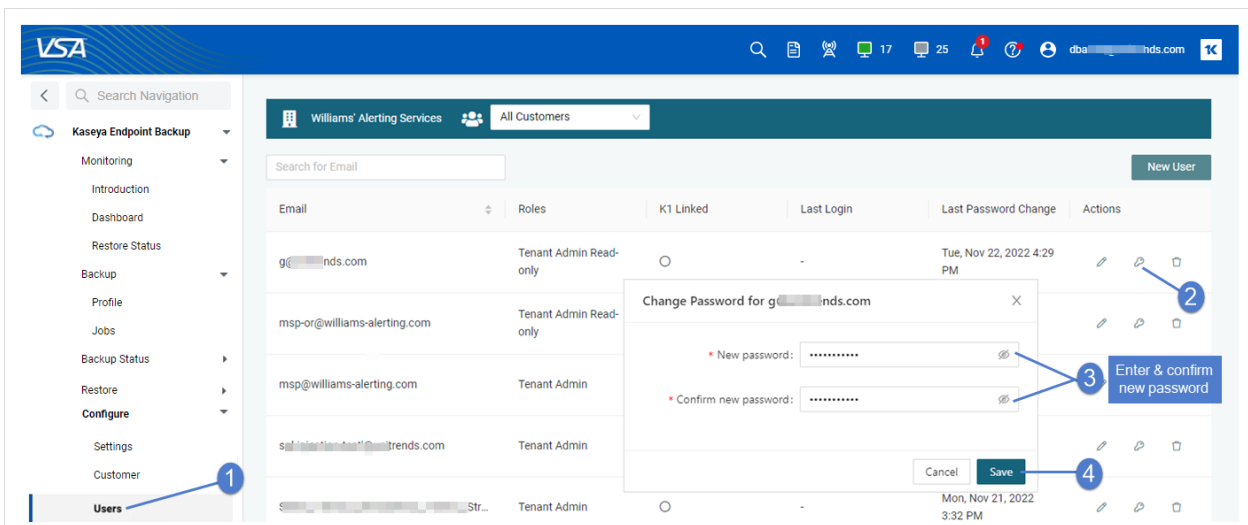
Note: Do not select the System Admin or System Admin Read-only roles. These are Unitrends Support roles.

- Click **Save**.




To change a user's password

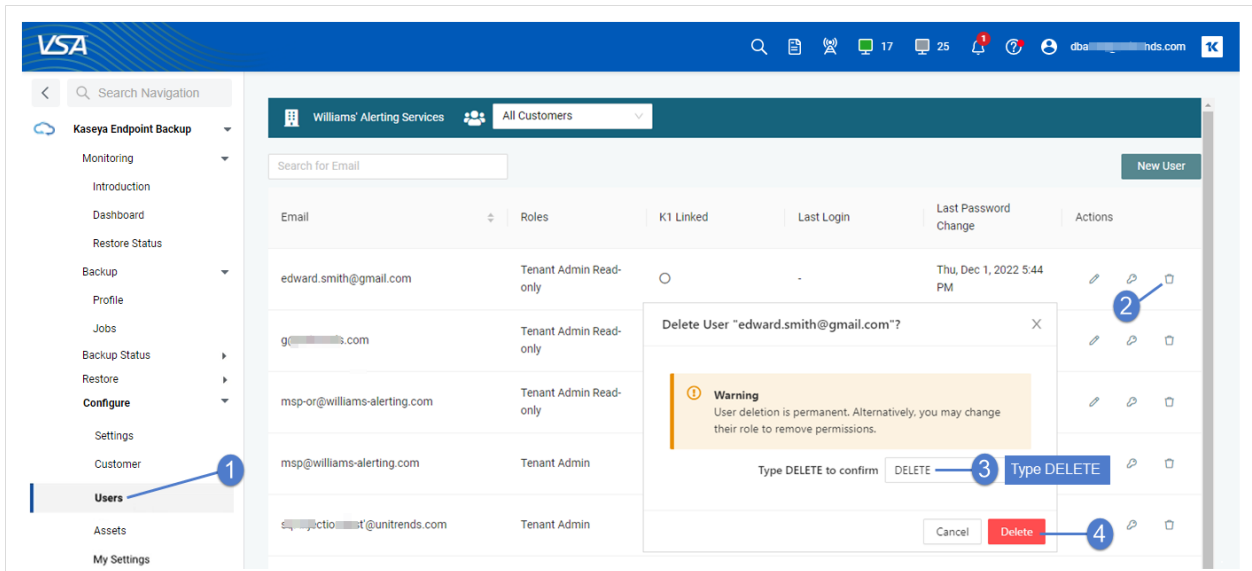
- 1 Select **Configure > Users**.
- 2 Locate the user and click its  icon.
- 3 In the Change Password dialog:
 - Enter the new password in the New Password and Confirm New Password fields.
 - Click **Save**.



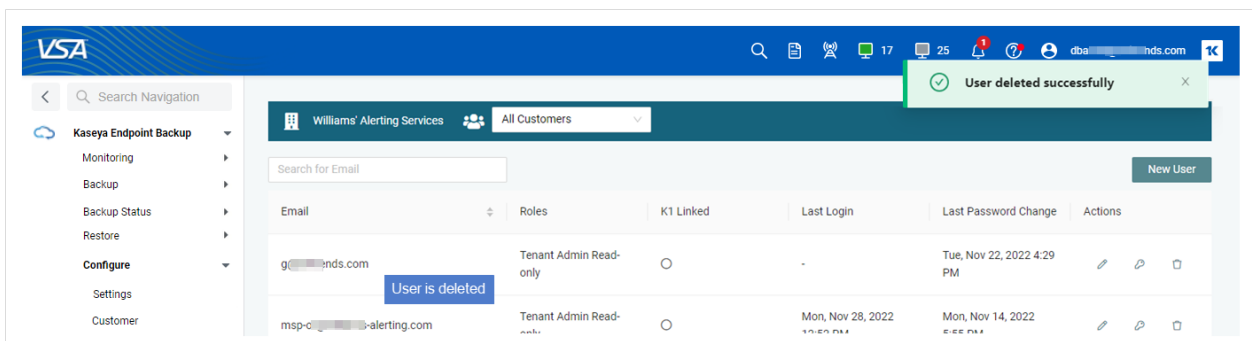
To delete a user

- 1 Select **Configure > Users**.

- 2 Locate the user and click its  icon.
- 3 In the Delete User dialog:
 - Type the word *DELETE* to confirm.
 - Click **Delete**.



The user is deleted:



Working with assets

Use these procedures to manage your assets:

- "To view assets"
- "To enable or disable an asset"
- "To delete an asset and/or an asset's backups"

- "To promote an asset's next backup to a full"
- "To run an on-demand backup of the asset"

Note: To add an asset, simply install the agent as described in "Install the Kaseya EndPoint Backup agent".

To view assets

- 1 Select **Configure > Assets**.
- 2 Select the customer whose assets you will view.
- 3 The following displays for each asset:

Note: The VSA Machine ID, Machine Group, and Organization columns contain data for assets running Kaseya EndPoint Backup agent version 1.4 or higher only.

- Machine ID – VSA machine ID.
- Machine Group – VSA machine group.
- Organization – VSA organization.
- Asset Name – Name of the protected asset.
- Success Of Last 10 Tasks – Percentage indicating how many of the last 10 jobs completed successfully.
- Last Seen – Date and time that the asset last checked in with Kaseya EndPoint Backup.
- Enabled – Button indicating whether the asset is currently enabled:
 - *On* indicates the asset is enabled.
 - *Off* indicates the asset is disabled.
 - *Deleting ALL* indicates the asset and its backups are in the process of being deleted.
 - *Deleted ALL* indicates the asset and its backups have been deleted.
 - *Deleted AGENT* indicates the asset has been decommissioned.
- Agent Version – Agent version running on the asset
- Run Full – Button used to promote the asset's next scheduled backup to a full. See "To promote an asset's next backup to a full" for details.
- Run Once – Button used to run an on-demand backup of the asset. See "To run an on-demand backup of the asset" for details.
- Delete – Button used to delete an asset and/or the asset's backups. See "To delete an asset and/or an asset's backups" for details.

The screenshot shows the Kaseya EndPoint Backup web interface. The left sidebar contains a navigation menu with categories like Monitoring, Backup, and Configure. The 'Assets' link is highlighted with a blue circle and the number '1'. At the top of the main content area, there is a search bar with the text 'unitrends-internal' and a dropdown menu showing 'Donut Shop', which is also highlighted with a blue circle and the number '2'. Below the search bar is a table of assets with columns for Machine ID, Machine Group, Organization, Asset Name, Success Of Last 10 Tasks, Last Seen, Enabled, Agent Version, and Actions. The table contains five rows of asset data.

Machine ID	Machine Group	Organization	Asset Name	Success Of Last 10 Tasks	Last Seen	Enabled	Agent Version	Actions
1-7-staging-kdc	base	myorg	1-7-staging-kdc-blob-15-87	80%	09/29/2020 15:34	Off		Run Full Run Once
pub-multi-blob	base	myorg	pub-multi-blob-112	100%	06/29/2020 21:55	On	1.27.0	Run Full Run Once
staging-kdc-199	base	myorg	staging-kdc-199-201	100%	06/15/2021 17:22	On		Run Full Run Once
staging\dcb-19-2	base	myOrg	staging\dcb-199-206	100%	07/07/2020 11:33	On		Run Full Run Once
staging\dcb-19-4	base	myOrg	staging\dcb-199-250	100%	09/29/2020 15:33	On		Run Full Run Once

4 (Optional) To modify the display you can:

- Click and enter a text string to filter by machine ID, machine group, organization, or asset name.
- Click on a column to sort alphabetically (a to z) or numerically (0-n). Click the column again to reverse the order.
- Modify the number of rows per page.

The screenshot shows the Kaseya EndPoint Backup interface. At the top, there is a header with 'unitrends-internal' and 'Donut Shop'. Below the header, there are buttons for 'Bulk Installation' and 'Single Installation'. The main area contains a table of assets with columns: Machine ID, Machine Group, Organization, Asset Name, Success Of Last 10 Tasks, Last Seen, Enabled, Agent Version, and Actions. A search box is visible over the 'Asset Name' column, with the text 'serv' entered. Annotations include: 'Click a heading to sort by column' pointing to the 'Machine ID' column header, and 'Filter by asset name' pointing to the search box. The table lists several assets, including '1-7-staging-kdc', 'pat-multi-block', 'staging-kdc-199', and 'staging-kdcb-19-2'. The 'Enabled' column shows toggle switches for each asset.

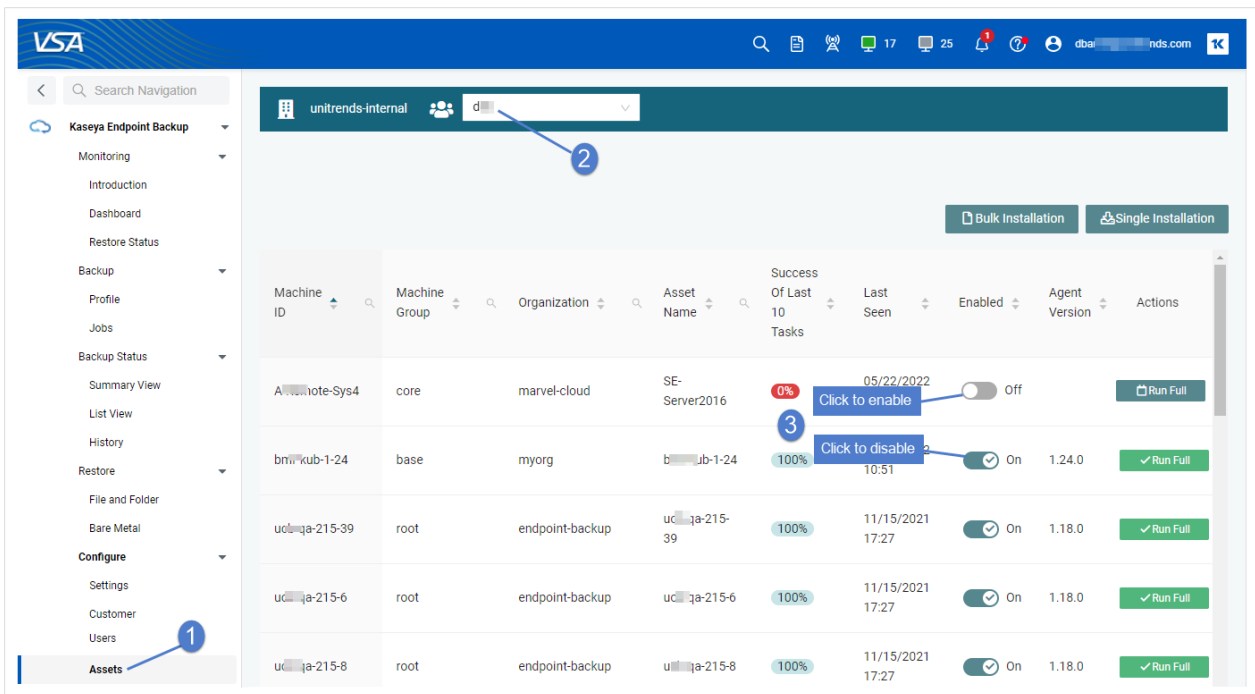
Machine ID	Machine Group	Organization	Asset Name	Success Of Last 10 Tasks	Last Seen	Enabled	Agent Version	Actions
1-7-staging-kdc	base	myorg	serv	80%	09/29/2020 15:34	Off		Run Full Run Once
pat-multi-block	base	myorg	pat-multi-block-112	100%	06/29/2020 21:55	On		Run Full Run Once
staging-kdc-199	base	myorg	staging-kdc-199-201	100%	06/15/2021 17:22	On	1.27.0	Run Full Run Once
staging-kdcb-19-2	base	myOrg	staging-kdcb-199-206	100%	07/07/2020 11:33	On		Run Full Run Once

At the bottom right, there is a pagination control with the text 'Click to view other pages' and page numbers 1, 2, 3.

To enable or disable an asset

Once an asset has been disabled, no backup jobs are run for that asset. Backups continue to run for any other enabled assets in the job. To resume jobs for the asset, simply enable the asset.

- 1 Select **Configure > Assets**.
- 2 Select the customer whose asset you will enable or disable.
- 3 Locate the asset in the list.
- 4 Click the asset's Enabled button to enable or disable the asset.



To delete an asset and/or an asset's backups

Use this procedure to delete an asset, delete the asset's backups, or delete both the asset and its backups.

- 1 Select **Configure > Assets**.
- 2 Select the customer whose asset you will delete.
- 3 Locate the asset in the list and click its **Delete** button.
- 4 Select one of the following:
 - **Decommission Endpoint** – Select to decommission the asset. Once the asset has been decommissioned, the asset is removed from jobs and you can no longer recover backups to the endpoint. (But you can recover backups of this asset to another asset.) Existing backups remain stored in the Cloud, but no new backups will run for this asset.
 - **Purge Data** – Select to delete this asset's backups from the Cloud. Data deletion may take some time depending on the size. The next backup run for this asset will be promoted to a full.
 - **Delete All** – Select to decommission the asset and delete this asset's backups from the Cloud. No new backups will run for the asset. The asset is removed from jobs and you can no longer recover files to the asset.

Note: Re-installing an agent on a decommissioned asset will register it as a new asset.

- 5 (Optional) If you selected **Decommission Endpoint** or **Delete All**, you can opt to use the **Wait For Agent Uninstallation** option to uninstall the agent on the endpoint:

- Check the **Wait For Agent Uninstallation** box to ensure that the agent has been removed from the endpoint before decommissioning the asset.

Note: Wait For Agent Uninstallation requires agent version 1.11 or later. Do not check this box if the endpoint is running an older agent or if the endpoint is no longer reachable. (You must manually uninstall older agent versions.)

- Leave the **Wait For Agent Uninstallation** box unchecked to decommission the asset without removing the agent from the endpoint.

6 Click Delete.

The screenshot shows the VSA interface with a modal dialog titled "Delete 'SE-Server2016'". The dialog has three tabs: "Agent", "Backups", and "Metadata". Under the "Agent" tab, there are three radio button options: "Decommission Endpoint", "Purge Data", and "Delete All". The "Delete All" option is selected. Below these options is a checked checkbox labeled "Wait For Agent Uninstallation". At the bottom of the dialog are "Cancel" and "Delete" buttons. The "Delete" button is highlighted in red. Numbered callouts (1-5) point to various UI elements: 1 points to the "Assets" menu item in the left sidebar, 2 points to the user dropdown menu in the top navigation bar, 3 points to the "Run Once" button in the right sidebar, 4 points to the "Delete All" option in the dialog, and 5 points to the "Delete" button in the dialog.

The Delete All or Decommission Endpoint procedure starts.

- For Delete All, the asset's Enabled column contains *Deleting ALL* while the procedure is running and *Deleted ALL* when the procedure is finished.
- For Decommission Endpoint, the asset's Enabled column contains *Deleted AGENT* when the procedure is finished.

Note: If the asset's Enabled column does not change to *Deleted AGENT*, it is possible that the system cannot connect to the agent or the endpoint is running an older agent version. Run Decommission Endpoint again without selecting the Wait For Agent Uninstallation option. After the Decommission Endpoint procedure is finished, uninstall the agent manually.

Asset Name	Success Of Last 10 Tasks	Last Seen	Enabled	Agent Version	Actions
v-1-17-staging-jcb-part-2-159706	0%		Deleted AGENT	1.24.0	Run Full Run Once
Sam-Laptop	0%		Deleting ALL	1.24.0	Run Full Run Once
v-1-16-staging-jcb-1597112	60%	07/24/2021 11:31	On	1.24.0	Run Full Run Once
v-1-16-staging-jcb-1597114	60%	07/24/2021 11:30	On	1.24.0	Run Full Run Once

To promote an asset's next backup to a full

Use this procedure to run a full backup of the asset during the next scheduled run. To use this feature, the asset must be present in a job schedule.

- 1 Select **Configure > Assets**.
- 2 Select the customer whose asset you will promote.
- 3 Locate the asset in the list.
- 4 Click the asset's **Run Full** button.
- 5 Click **Run Full** to confirm.

The screenshot shows the 'Assets' page in the Kaseya EndPoint Backup interface. A modal dialog titled "Queue Full On All Assets" is open, displaying a table of assets with 100% success. The "Run Full" button for the asset "ds-w2016-252" is highlighted with a blue circle and a number 4. The "Assets" link in the left navigation menu is highlighted with a blue circle and a number 1. The "unitrends-internal" customer is selected in the top navigation bar, highlighted with a blue circle and a number 2. The "Run Full" button for the selected asset is highlighted with a blue circle and a number 3.

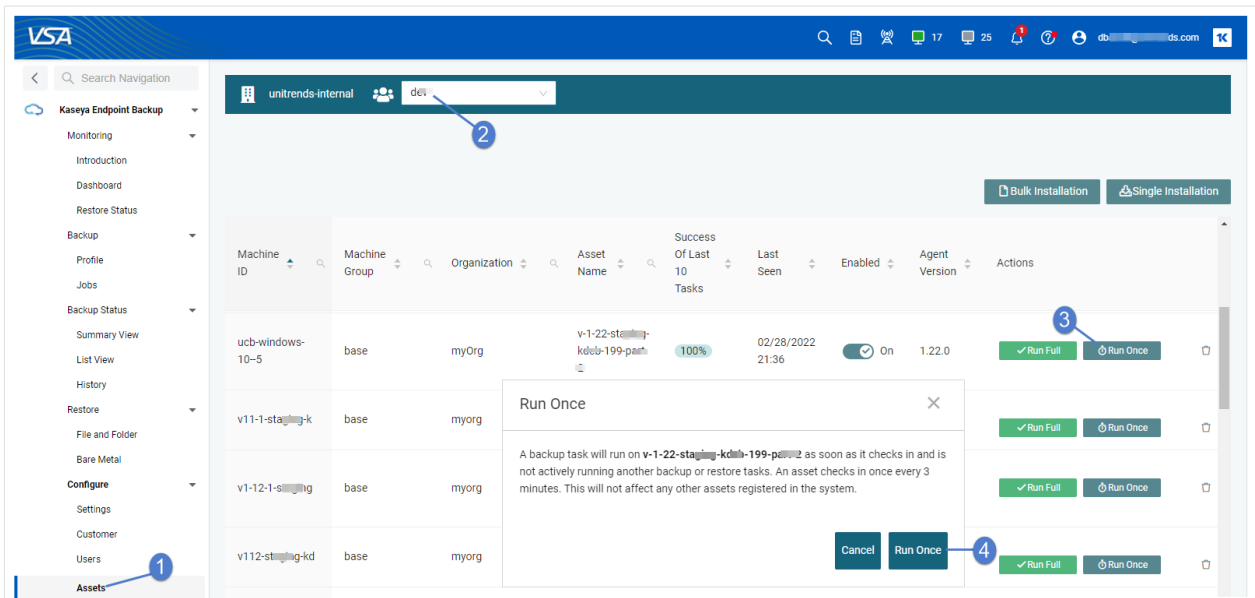
- 6 The asset's Run Full button changes to green, indicating that the Run Full job is pending. The job is queued as soon as the asset checks in and runs if no other job is currently running for this asset.

The button returns to blue once the job starts. Note that you cannot initiate Run Full for the asset if the button is gray (asset is disabled) or green (Run Full job is pending).

To run an on-demand backup of the asset

Use this procedure to run an on-demand backup of the asset. An incremental backup runs unless promotion to a full is required due to a configuration change. The job is queued as soon as the asset checks in and runs if no other job is currently running for this asset.

- 1 Select **Configure > Assets**.
- 2 Select the customer.
- 3 Locate the asset in the list.
- 4 Click the asset's **Run Once** button.
- 5 Click **Run Once** to confirm.



- 6 The asset's Run Once button changes to green, indicating that the Run Once job is pending. The job is queued as soon as the asset checks in and runs if no other job is currently running for this asset.

The button returns to blue once the job starts. Note that you cannot initiate Run Once for the asset if the button is gray (asset is disabled) or green (Run Once job is pending).

Working with your user account settings

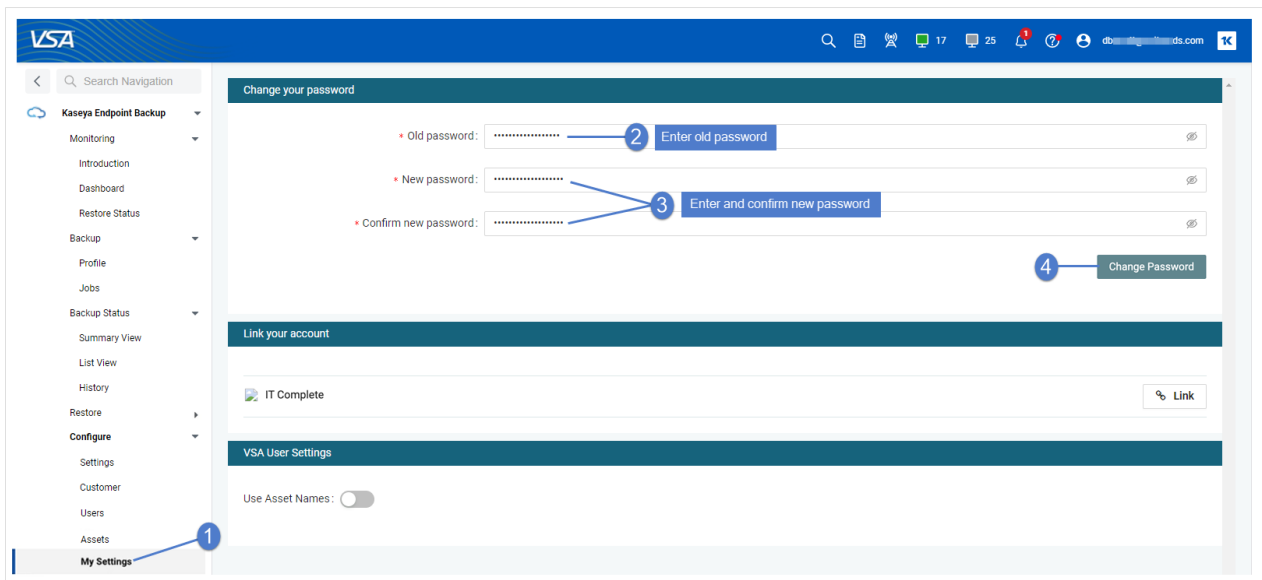
Use these procedures to change your password or enable/disable login with IT Complete:

- "To change your Kaseya EndPoint Backup password"
- "To enable login with IT Complete from the My Settings page"

- "To disable login with IT Complete"
- "To enable search by asset name"

To change your Kaseya EndPoint Backup password

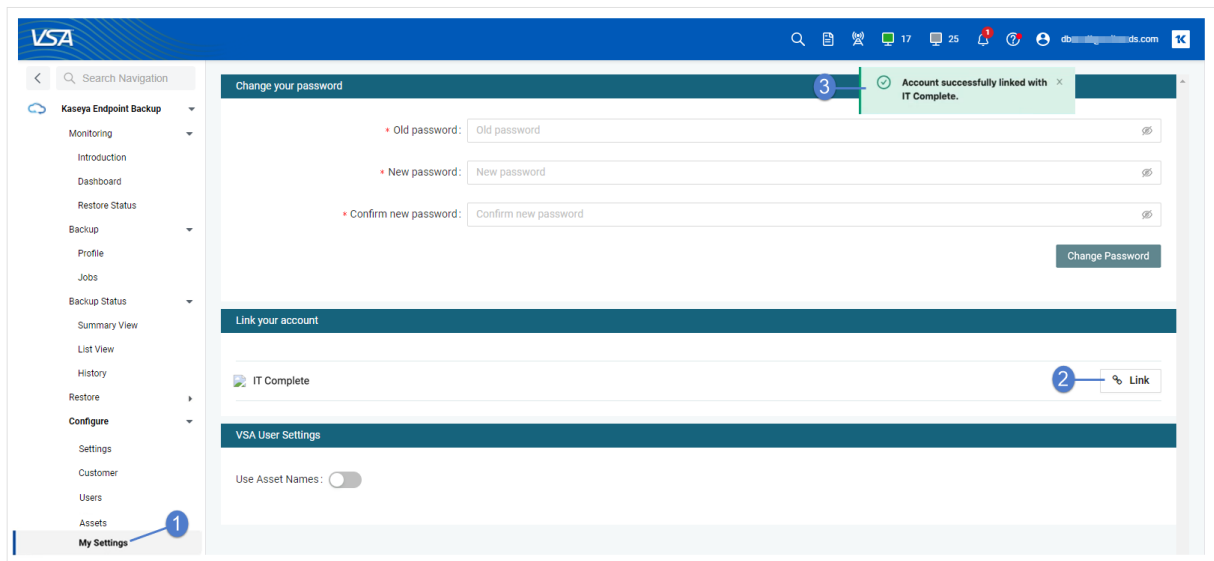
- 1 Select **Configure > My Settings**.
- 2 Enter your old password.
- 3 Enter the new password.
- 4 Enter the new password again to confirm.
- 5 Click **Change Password**.



To enable login with IT Complete from the My Settings page

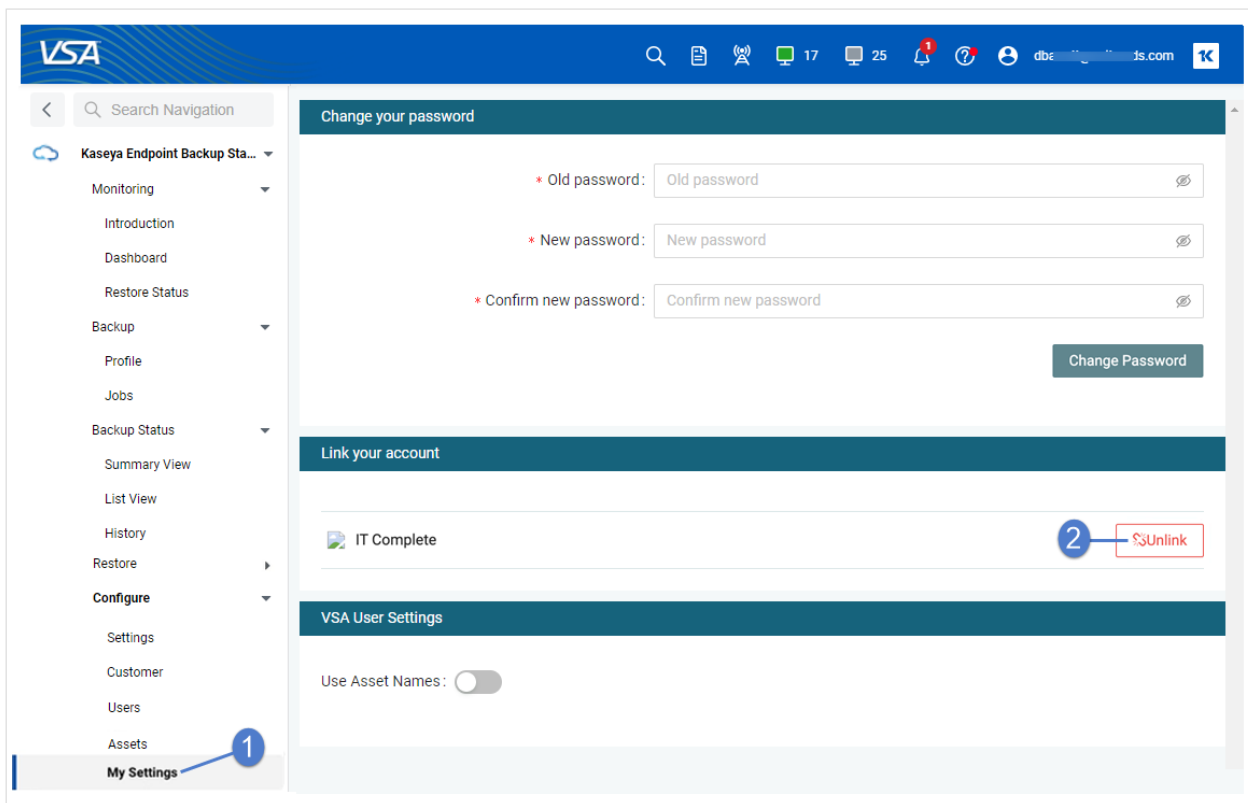
- 1 Select **Configure > My Settings**.
- 2 Click **Link**.

Note: If you do not see the IT Complete Link button, your organization has not been registered with IT Complete. Register your organization as described in "[Working with Kaseya EndPoint Backup Settings](#)" on page 129.

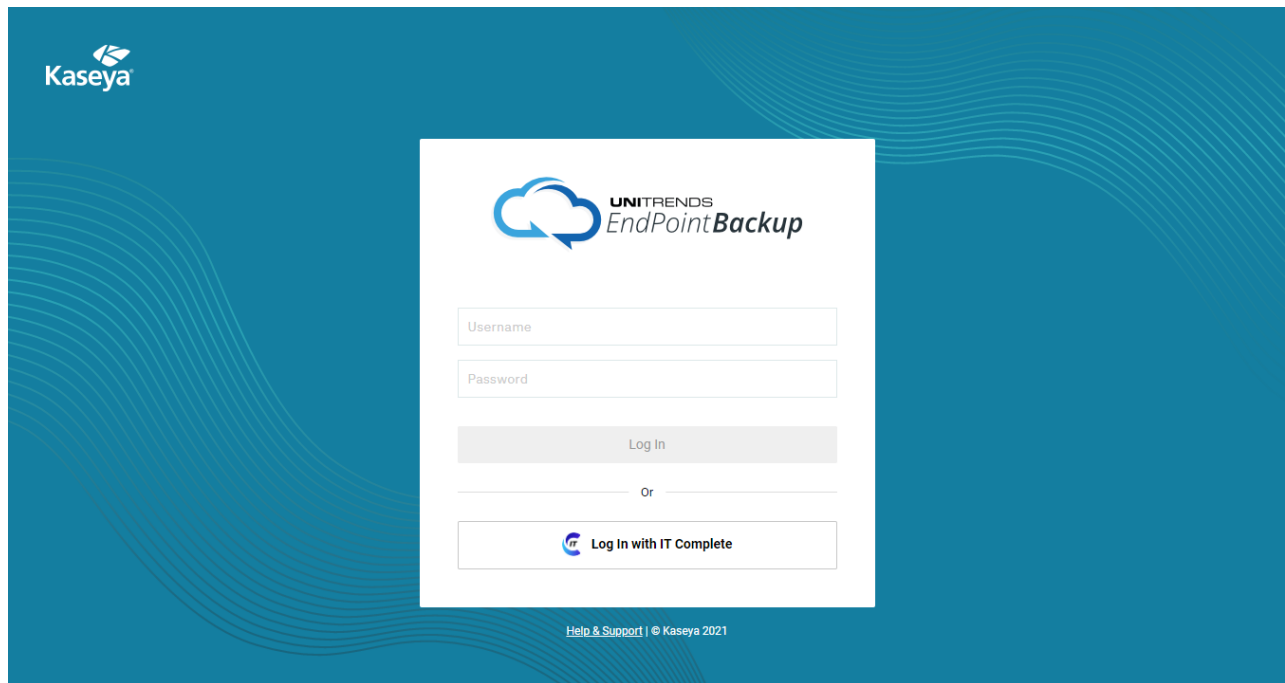


To disable login with IT Complete

- 1 Select **Configure > My Settings**.
- 2 Click **Unlink**.



The account link is removed and you are logged out of Kaseya EndPoint Backup.



To enable search by asset name

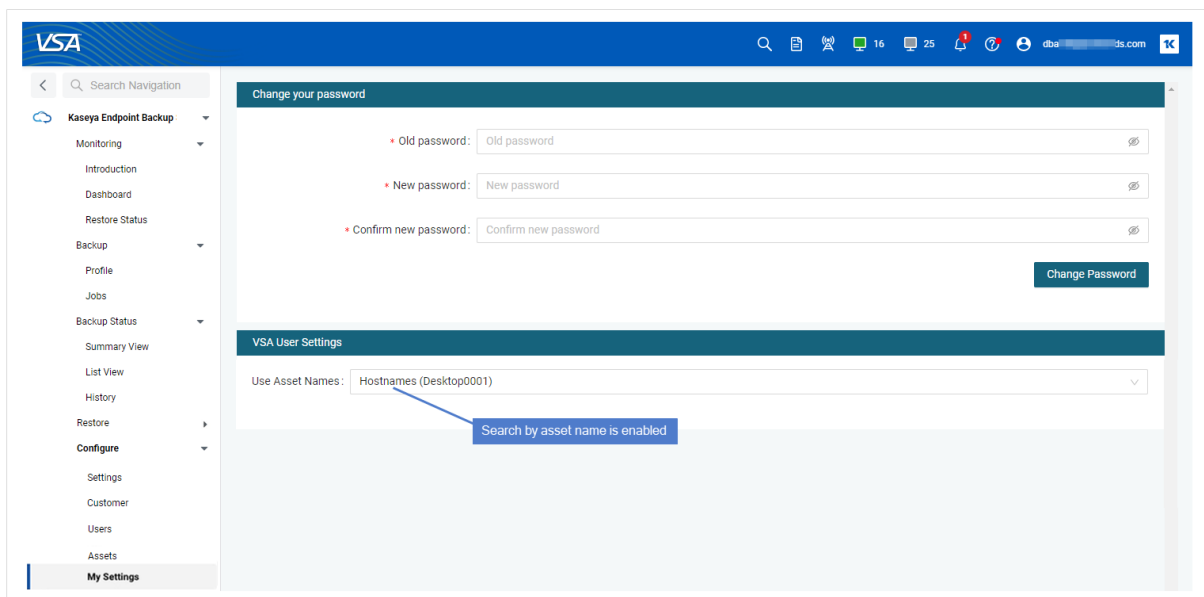
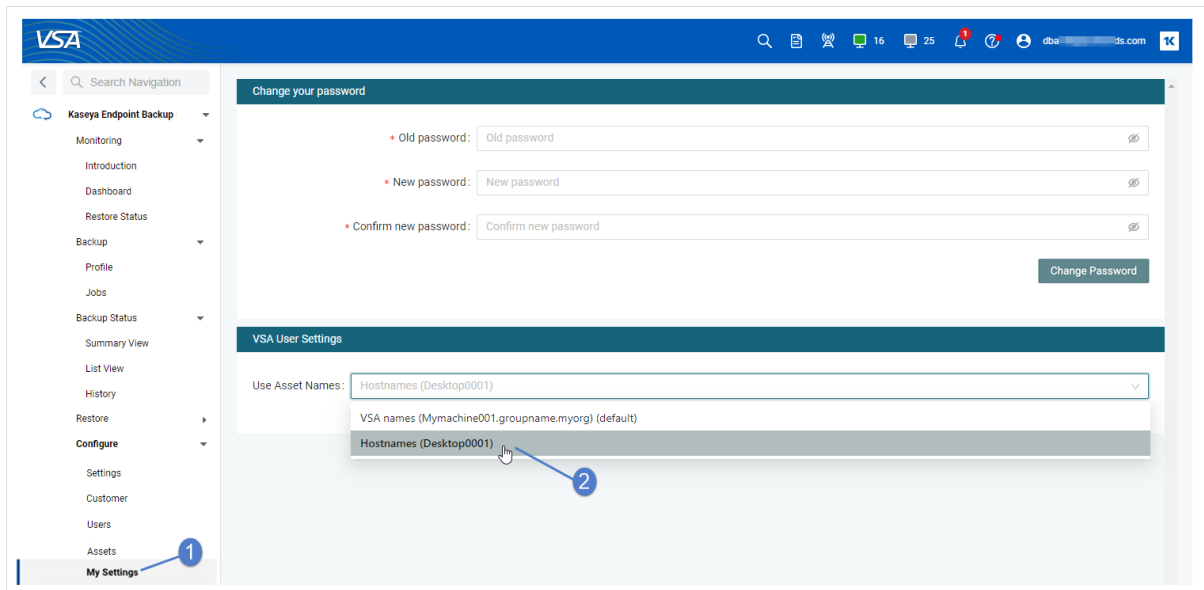
A Kaseya EndPoint Backup asset is known as a *machine ID* in the VSA:

The screenshot shows the VSA interface for configuring a procedure. The procedure name is "Deploy Endpoint Backup Agent". It is approved by the system on 03/29/2022. The procedure description is "Deploy Endpoint Backup Agent to Windows Machines". Below the description, there is a "Schedule" tab with a table of machine IDs and their execution status. A blue callout box points to the "Machine Id" column in the table, labeled "VSA machine IDs".

Machine Id	Last Time Exec	Last Exec Status	Next Exec Time
11-helix-d...			
3-multi-helix.r...			
35-helix.r...			
35-mock-dome-cent...			
5-de...			
5-helix-mo...			

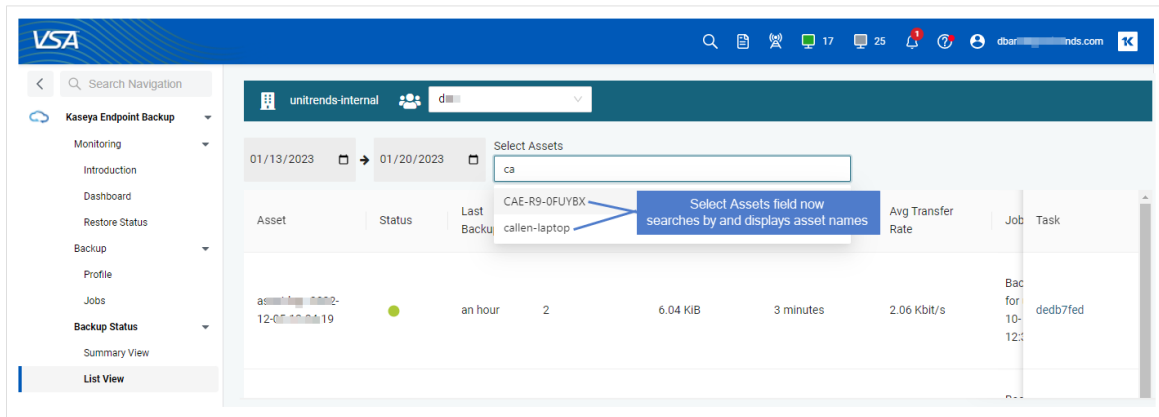
By default, the Kaseya EndPoint Backup asset filters search by VSA machine ID (e.g., *Mymachine001.groupname.myorg*). To search by asset name instead:

- 1 Select **Configure > My Settings**.
- 2 From the Use Asset Names list, select **Hostnames**:

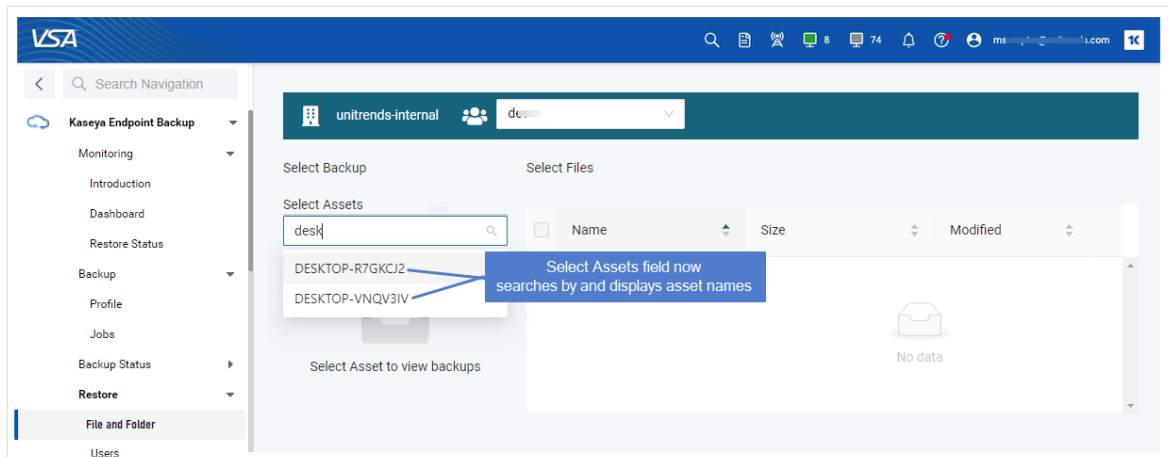


Asset filters contain asset names rather than VSA machine IDs.

- Backup Status > List View example:



- Restore > File and Folder example:



This page is intentionally left blank.



Chapter 8: Working with Kaseya EndPoint Backup Settings





Use the Settings page to view storage configuration and to manage integrations between Kaseya EndPoint Backup and Kaseya modules.

See these topics for details:

- ["Viewing Kaseya EndPoint Backup settings"](#)
- ["Working with your IT Complete integration"](#)
- ["Working with your BackupIQ integration"](#)
- ["Working with asset log storage"](#)

Viewing Kaseya EndPoint Backup settings

To view Kaseya EndPoint Backup settings, select **Configure > Settings**. These settings display:

- Storage Configuration area –
 - Region – The Kaseya Cloud region where backups are stored.
 - UUID – Unique identifier of your Kaseya EndPoint Backup instance.
 - Host Name – Cloud storage host name.
 - Alias – Cloud storage alias.
- Integrations area – Shows modules that can be integrated with your Kaseya EndPoint Backup. If you see the  button, the module is not integrated. If you see the  button, the module is integrated.
- Asset Log Storage – Enable this feature to automatically upload asset logs to the Unitrends Cloud.  indicates log storage is enabled.  indicates log storage is not enabled. For details, see ["Working with asset log storage" on page 149](#).

The screenshot displays the VSA interface for 'Williams' Alerting Services'. The left sidebar shows the navigation menu with 'Settings' highlighted. A blue callout box points to 'Settings' with the text 'Click here'. The main content area is titled 'Storage Configuration' and contains the following fields:

- Region: 102.160...71:31995
- UUID: 74021cbe...95f71f5
- Host Name: Williams Alerting Services
- Alias: Williams Alerting Services


Below this is the 'Integrations' section, which lists two modules:

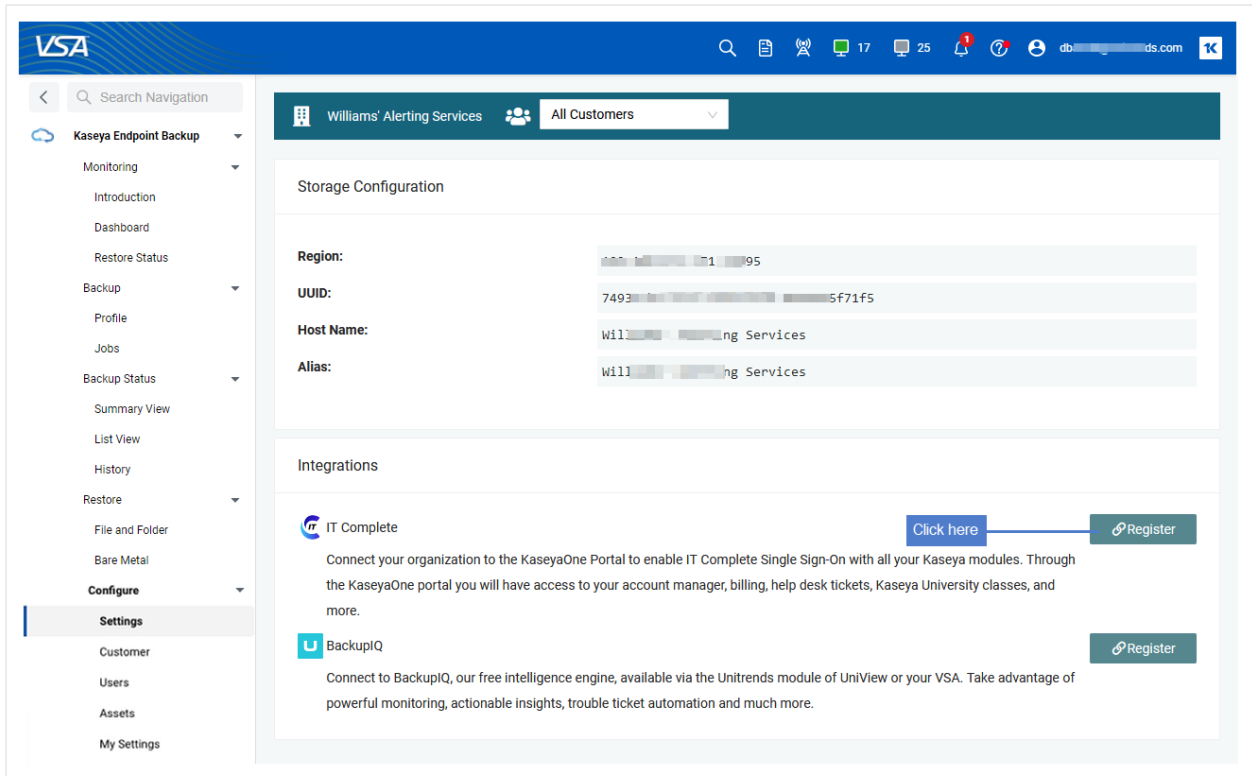
- IT Complete**: Status is 'Module is NOT integrated'. A blue callout box points to the 'Register' button.
- BackupIQ**: Status is 'Module is integrated'. A red callout box points to the 'Unregister' button.

The 'Asset Log Storage' section at the bottom has a toggle switch labeled 'Log storage is enabled' and a description: 'Allow asset logs to be stored in the cloud. This feature aids support when troubleshooting issues by uploading the relevant error logs to the Unitrends Cloud automatically.'

Working with your IT Complete integration

Once your organization is integrated with IT Complete, users can opt to link their Kaseya EndPoint Backup user account to their KaseyaOne user account to enable single sign-on. Once the account is linked, the user can simply click **Log In with IT Complete** on the Login page to access Kaseya EndPoint Backup, without entering their Kaseya EndPoint Backup credentials.

- To integrate your organization, locate the IT Complete integration and click its  button.



The screenshot displays the VSA (Veeam Service Agent) interface. The top navigation bar includes the VSA logo, search, and notification icons. A notification banner at the top right states "Registered IT Complete to Organization". The main content area is divided into two sections: "Storage Configuration" and "Integrations".

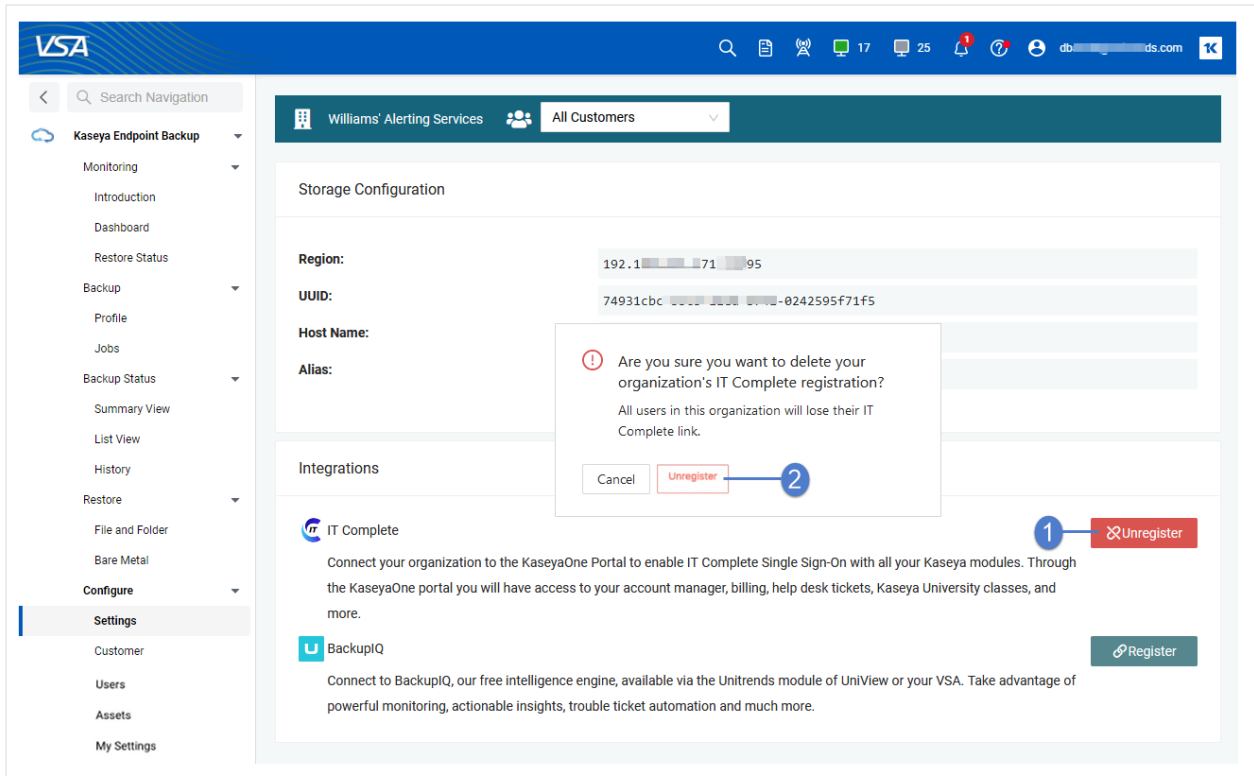
Storage Configuration:

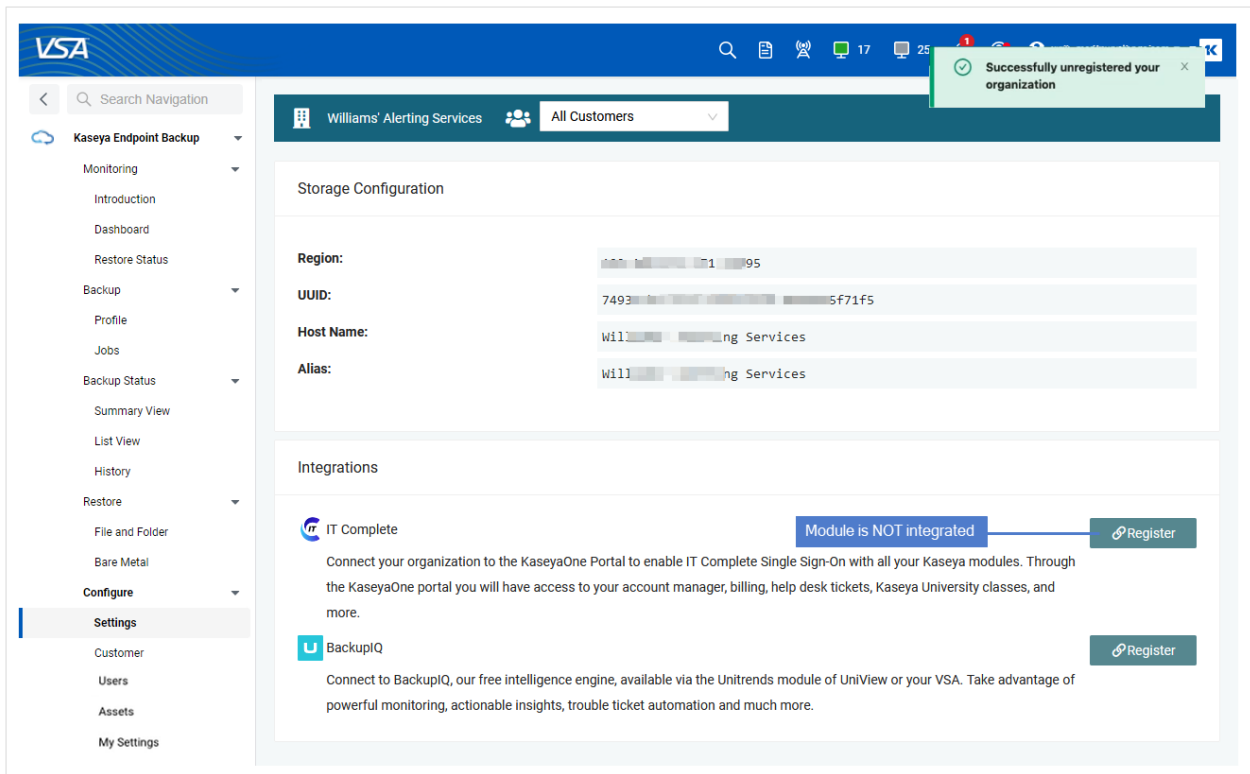
Region:	192.168.1.171
UUID:	74931cbc-9909-11e8-b742-0e42595f71f5
Host Name:	Williams' Alerting Services
Alias:	Williams' Alerting Services

Integrations:

- IT Complete:** Module is integrated. [Unregister](#)
- BackupIQ:** [Register](#)

- To remove the integration, locate the IT Complete integration and click its [Unregister](#) button. Click **Unregister** again to confirm. This removes the integration and all existing user account links to KaseyaOne.





Working with your BackupIQ integration

After you have integrated BackupIQ, you can set up alerting for your Kaseya EndPoint Backup job tasks in the UniView Portal. You use UniView Portal's conditional alarm feature to set a threshold for how long a machine can go without a good backup. If the threshold is exceeded, an alarm is generated and added to the Portal's BackupIQ Alerts list. If the UniView Portal has been integrated with a PSA system (BMS, Autotask, or ConnectWise), a ticket is also generated in the PSA. Additionally, you may opt to receive email notifications for these alerts.

See these procedures for details:


- ["To integrate BackupIQ"](#)
- ["To remove the BackupIQ integration"](#)
- ["To set up BackupIQ alerts for Kaseya EndPoint Backup"](#)
- ["To view BackupIQ alerts"](#)
- ["To set up email notification for BackupIQ alerts"](#)
- ["To dismiss BackupIQ alerts"](#)

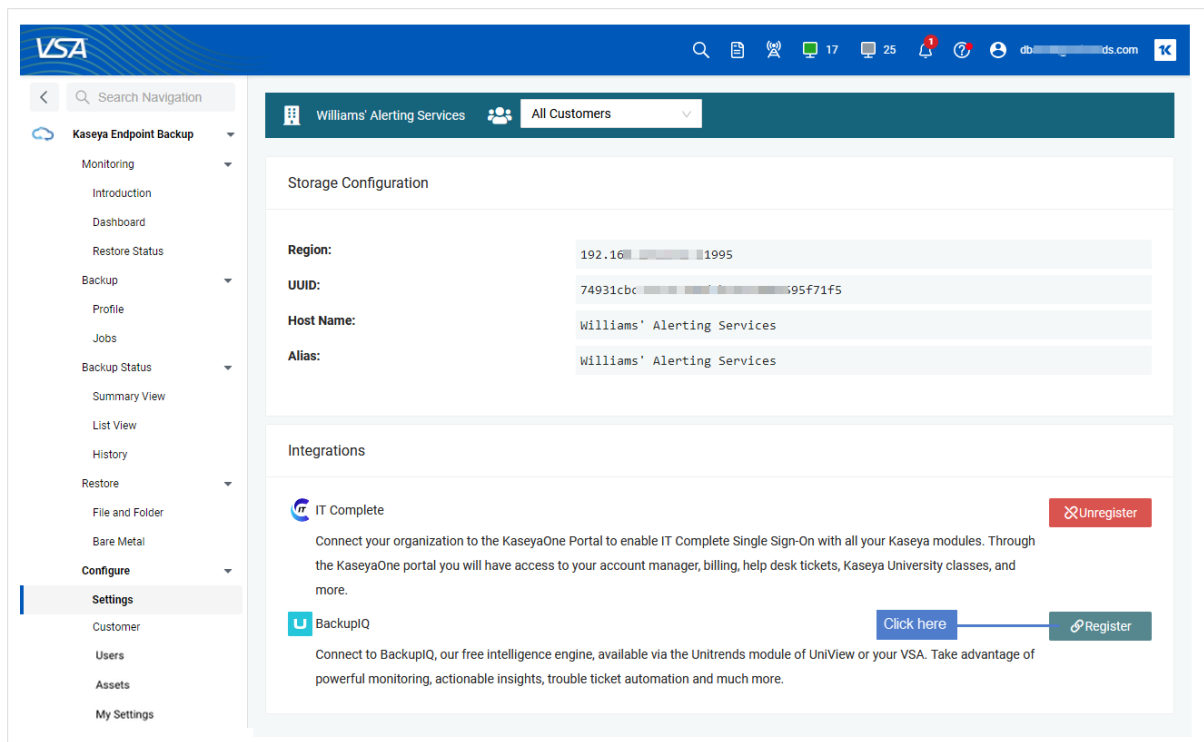
To integrate your PSA system with UniView Portal, see *Working with Integrations* in the [UniView Portal Guide](#).

To integrate BackupIQ

Notes:

- UniView Portal credentials are required for integration. If you have not received an email with credentials from the UniView Portal Onboarding team, contact your Account Manager to get started.
- A 1-to-1 UniView Portal to Kaseya EndPoint Backup relationship is enforced. (A Kaseya EndPoint Backup instance can be linked to only one UniView Portal instance. A UniView Portal instance can be linked to only one Kaseya EndPoint Backup instance.)

1. Locate the BackupIQ integration and click its  button.

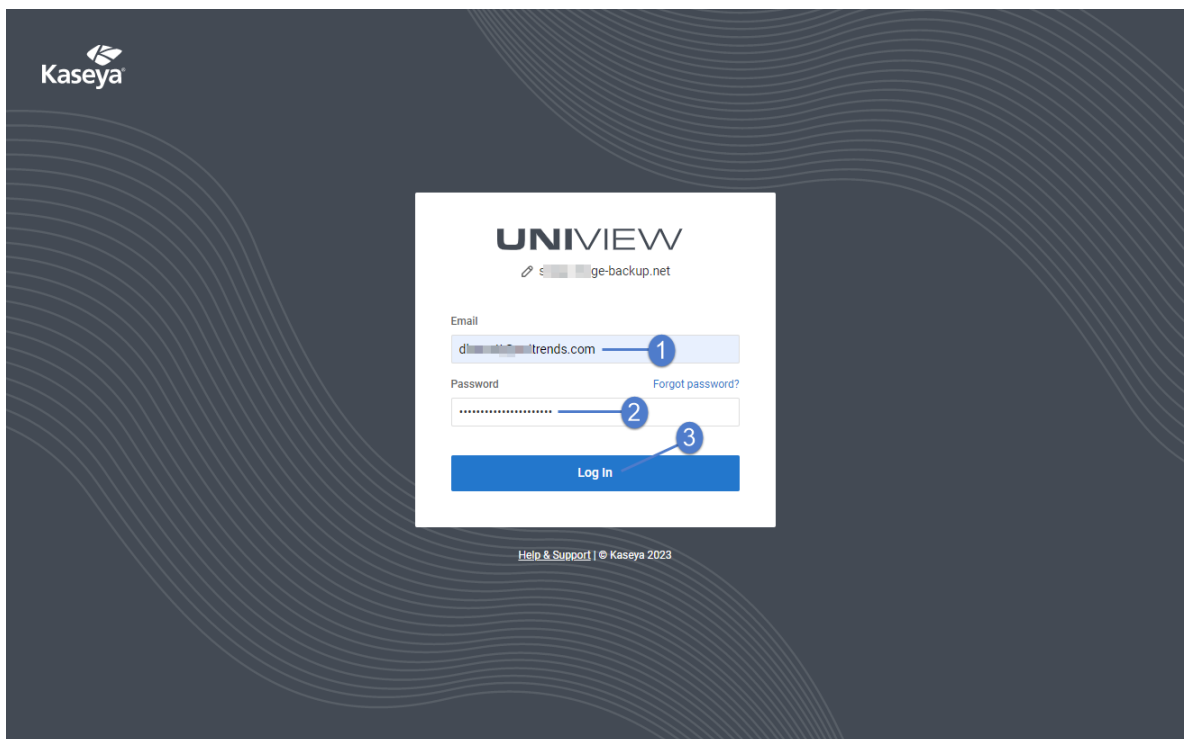


2. Log in to your UniView Portal:

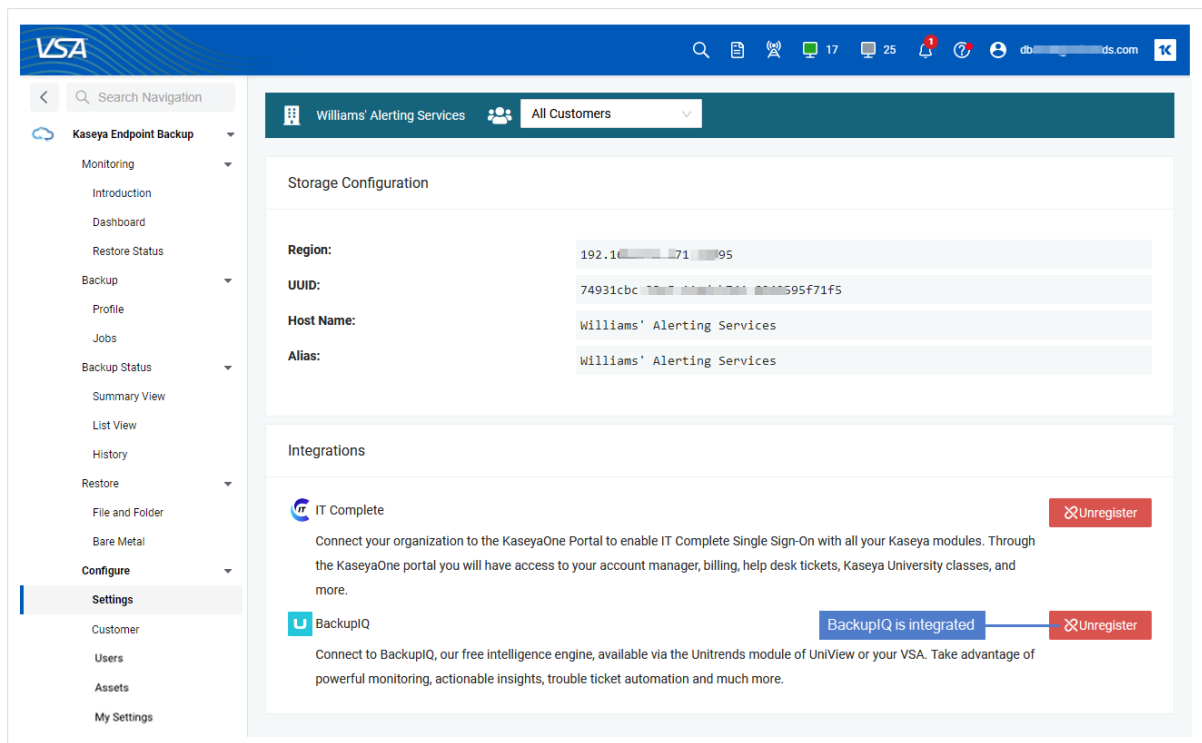
- Enter the backup.net homerealm that was provided to you by the UniView Portal Onboarding team. Click **Next**.



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



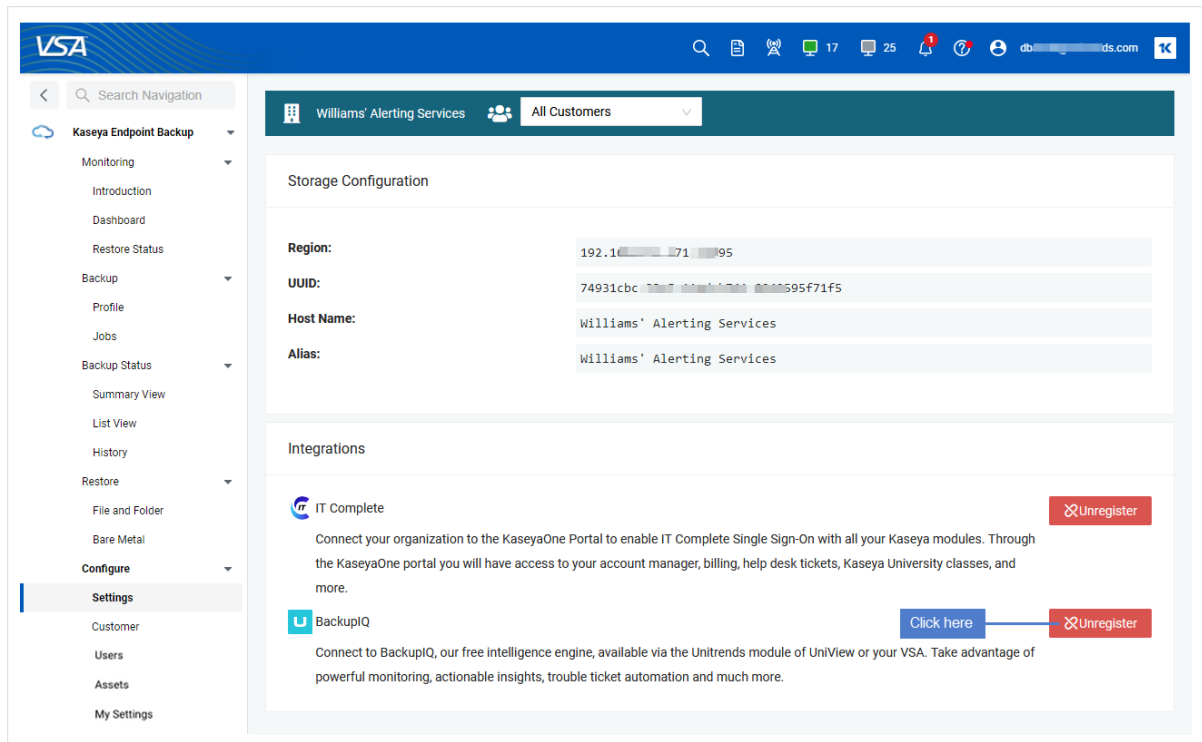
- 3 BackupIQ is integrated and the Kaseya EndPoint Backup Settings page displays:



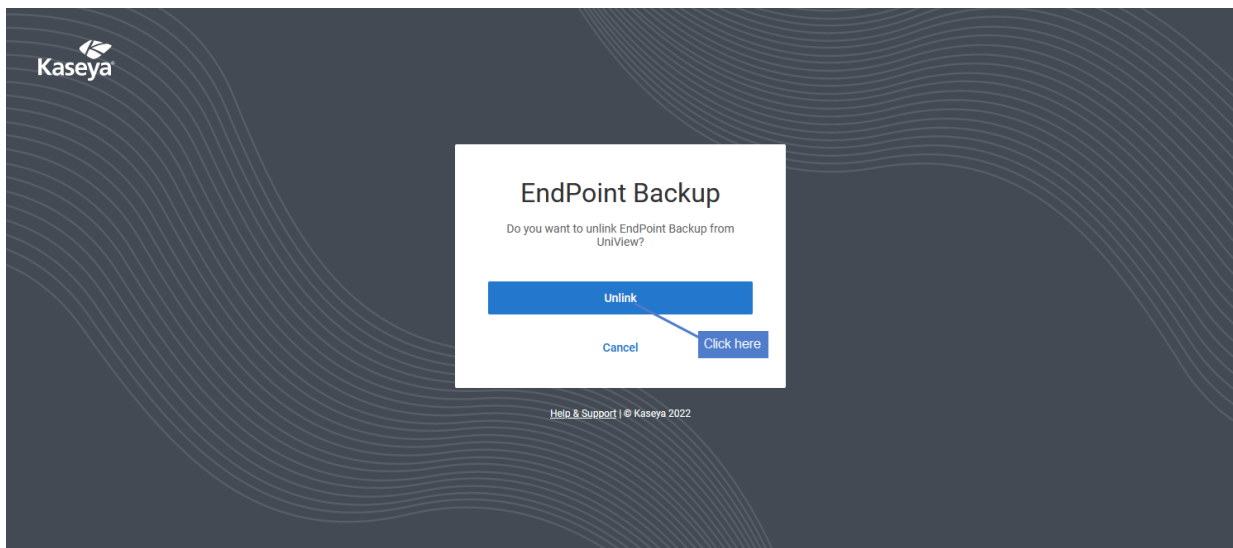
To start receiving backup alerts, proceed to "To set up BackupIQ alerts for Kaseya EndPoint Backup" on page 139.

To remove the BackupIQ integration

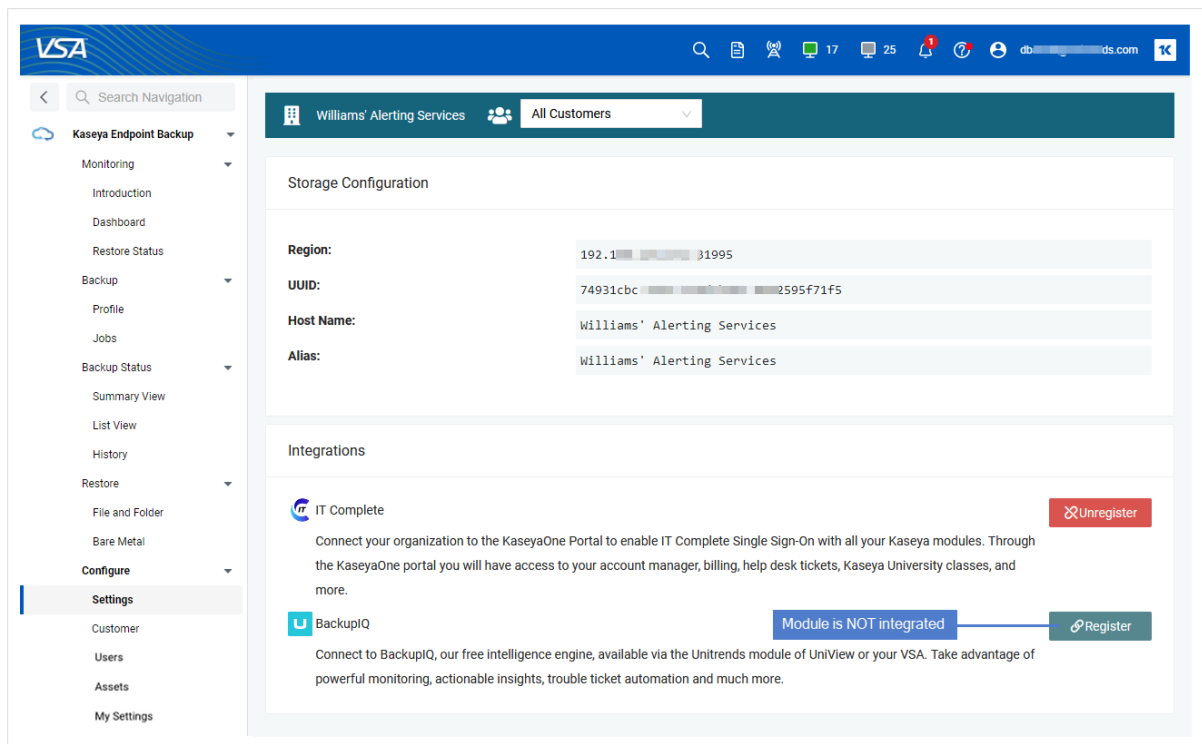
- 1 Locate the BackupIQ integration and click its [Unregister](#) button.



- 2 Click **Unlink** to confirm.



- 3 The integration is removed from Kaseya EndPoint Backup. Endpoint Backup alerts are removed from the UniView Portal.



To set up BackupIQ alerts for Kaseya EndPoint Backup

After you have integrated BackupIQ, use this procedure to set alert thresholds against the last successful backup. When a threshold is crossed, an alert is added to BackupIQ, enabling you to quickly prioritize and address alarm conditions.

Notes:

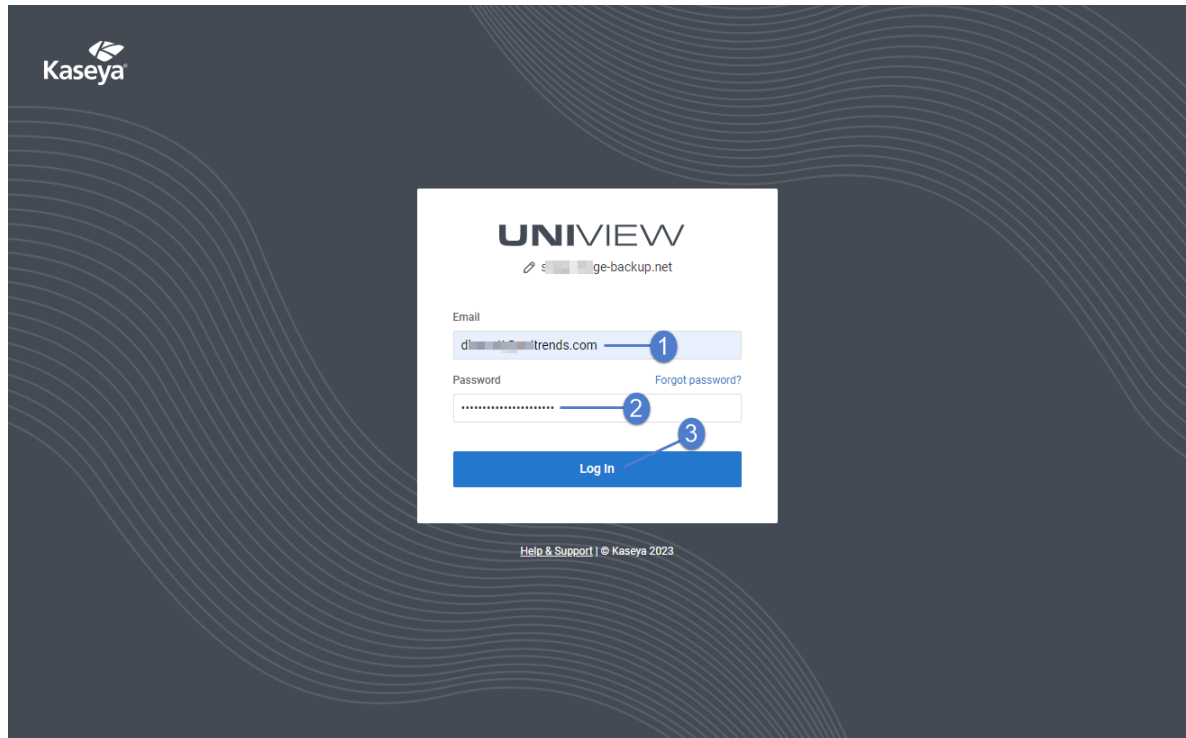
- You must integrate BackupIQ before running this procedure. For details, see "[To integrate BackupIQ](#)".
- A UniView Portal superuser account is required to run this procedure.


1 Log in to your UniView Portal as a superuser:

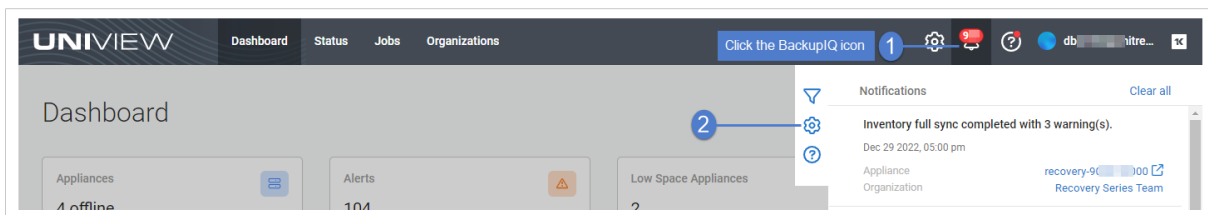
- Select the UniView module. (If you are running an older module version, select the *Unitrends Backup* module).

Note: If you have not integrated the UniView module, contact your Account Manager to get started.

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

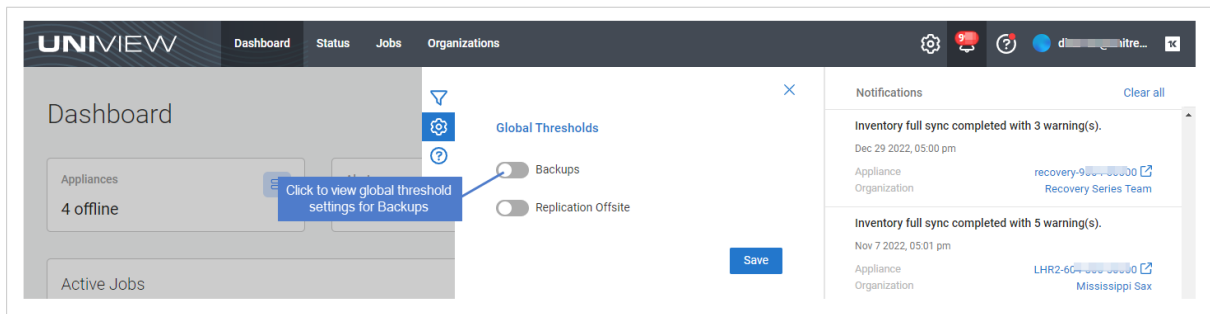


- 2 Click the BackupIQ icon in the upper-right corner.
- 3 Click the  icon.



- 4 Click to view global threshold settings for Backups.

Note: Replication Offsite thresholds do not apply to Kaseya EndPoint Backup.

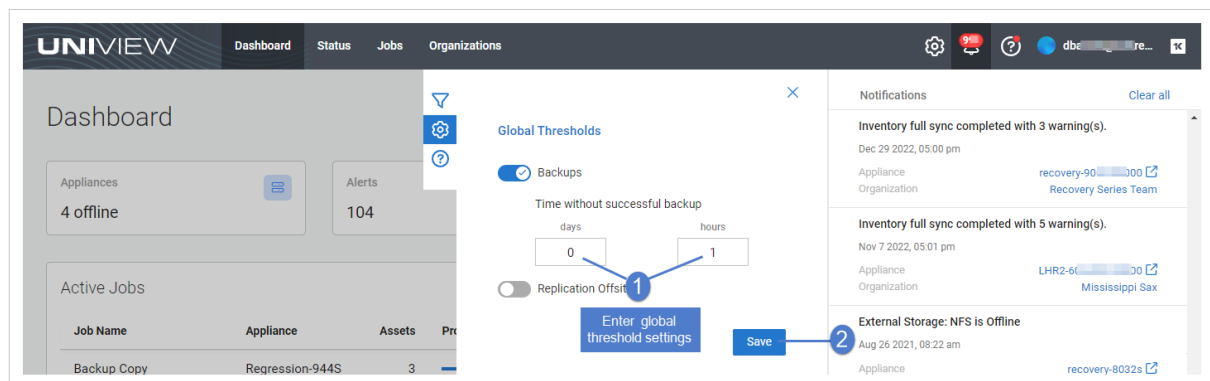


- 5 (Required) Enter global threshold settings and click **Save**.

In this 1-hour example, a backup alarm is generated if the backup does not complete successfully within 1 hour of the job's scheduled start time.

Notes:

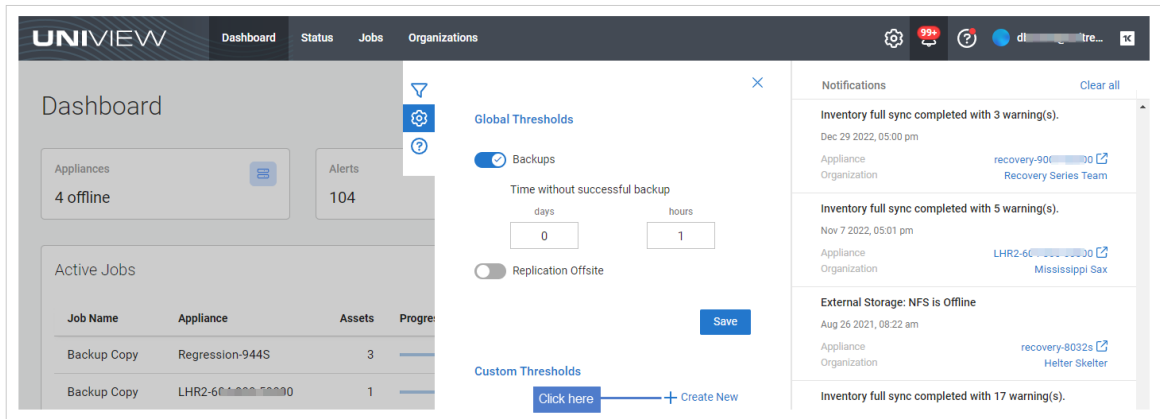
- A Kaseya EndPoint Backup *customer* is known as an *organization* in the UniView Portal.
- Global threshold settings are applied to assets that are protected by a backup schedule and do not have a custom threshold assigned. Global thresholds are applied across all organizations.



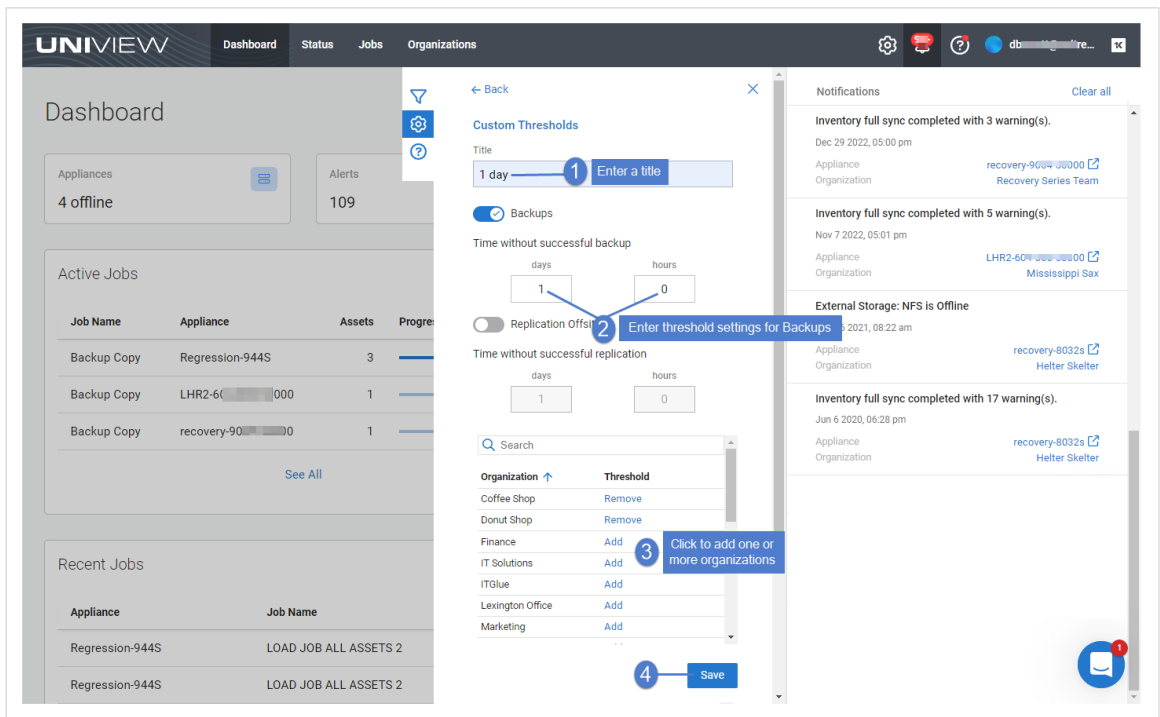
- 6 (Optional) Add a custom threshold and apply to organizations:

Note: Custom thresholds take precedence over global thresholds. Each organization can be assigned one custom threshold.

- Click **Create New**:



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



- The custom threshold is added:

The screenshot displays the UniView portal interface. The main navigation bar includes 'Dashboard', 'Status', 'Jobs', and 'Organizations'. The 'Global Thresholds' modal is open, showing settings for 'Backups'. The 'Time without successful backup' is configured as 0 days and 1 hour. A 'Replication Offsite' toggle is turned off. A 'Custom Thresholds' section shows a new threshold of '1 day' for '2 Organizations', with a confirmation message 'Custom threshold is added'. The 'Notifications' panel on the right lists several alerts, such as 'Inventory full sync completed with 3 warning(s)' and 'External Storage: NFS is Offline'.

After setting thresholds for backups, an alarm is generated if the threshold is crossed. These conditions are checked: threshold settings, last successful backup, and backup job schedule.

Notes:

- The BackupIQ integration sends last backup information to the UniView Portal. BackupIQ alerting does not begin for a given asset until the next successful backup runs (a successful backup must run after BackupIQ has been integrated to enable alerting for the asset).
- BackupIQ retains the last 90 days of backup status information received from Kaseya EndPoint Backup. Backup alerts are generated for the last 90 days of backup activity.

When alarms are generated, they are added to the alerts list in BackupIQ, as shown in ["To view BackupIQ alerts"](#).

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

To view BackupIQ alerts

- 1 In the UniView Portal, click the BackupIQ icon. Alerts display below:


The screenshot shows the UniView Portal dashboard with a notification panel on the right. The notification panel contains two alerts:

- Alert 1:** "One of the backup thresholds exceeded for one or more assets." 78 grouped. Jan 16, 01:23 am. Appliance: Regression-944S. Organization: King Bee.
- Alert 2:** "One of the backup thresholds exceeded for one or more assets." 2 grouped. Jan 13, 01:02 am. App: recovery-9000000000. Organization: Recovery Series Team.

Alerts display in list 2

Organization

Asset name bk-deb10-latest

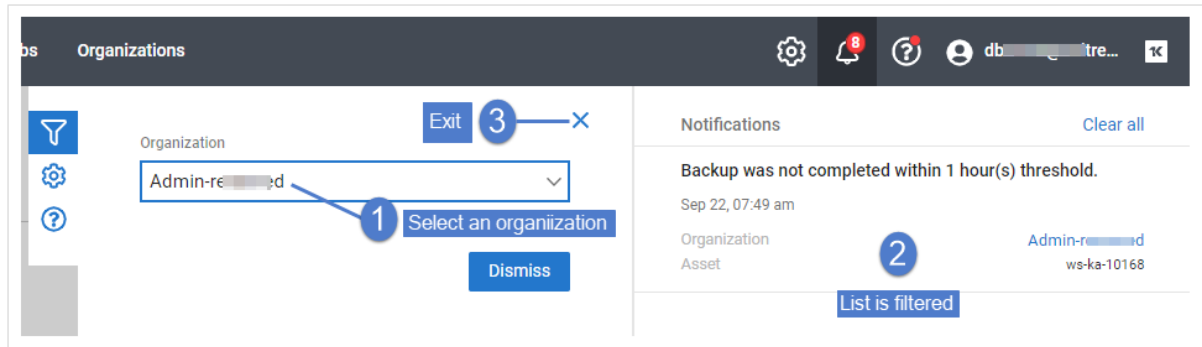
- 2 (Optional) Click  to filter the alerts list by organization:

Note: A Kaseya EndPoint Backup *customer* is known as an *organization* in UniView Portal.

The screenshot displays the 'Notifications' section of the Kaseya EndPoint Backup interface. At the top, a dark navigation bar contains icons for settings, notifications (with a red '5' badge), help, and user profile. A blue callout box with the text 'Click here' points to the notification bell icon. Below the navigation bar, the 'Notifications' section is titled and includes a 'Clear all' link. A vertical sidebar on the left contains icons for a funnel, settings, and help. The main content area shows a list of notifications, each with a title, timestamp, organization, and asset details. The notifications are as follows:

Notification Title	Timestamp	Organization	Asset
Backup was not completed within 1 hour(s) threshold.	Sep 22, 07:49 am	Admin-renamed	ws-ka-10168
Backup was not completed within 1 hour(s) threshold.	Sep 21, 03:49 pm	dev	ucb-windows-10-
Backup was not completed within 1 hour(s) threshold.	Sep 21, 03:19 pm	dev	ucb-windows-10-
Backup was not completed within 1 hour(s) threshold.	Sep 21, 02:24 pm	dev	v-1-25-staging-
Backup was not completed within 1 hour(s) threshold.	Sep 21, 02:04 pm	dev	v-1-27-alerting-release-2021-09-21-21-51
Backup was not completed within 1 hour(s) threshold.	Sep 21, 02:04 pm	dev	v-1-28-alerting-release-2021-09-21-53
Backup was not completed within 1 hour(s) threshold.			

- Select an organization from the Organization list. (To clear the filter, select **All** from the Organization list.)
- Click **X** to exit.



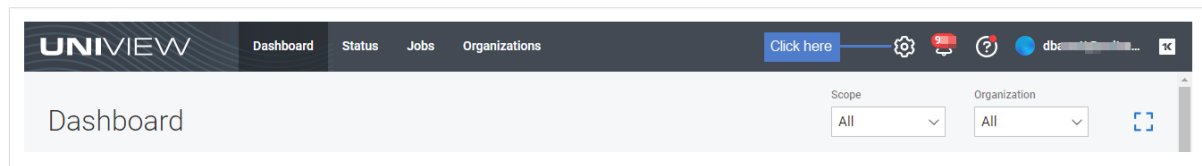
- 3 To investigate why a backup did not complete successfully within the target threshold, view the asset's last backup in Kaseya EndPoint Backup (for details see "[Viewing backup status](#)".)

To set up email notification for BackupIQ alerts

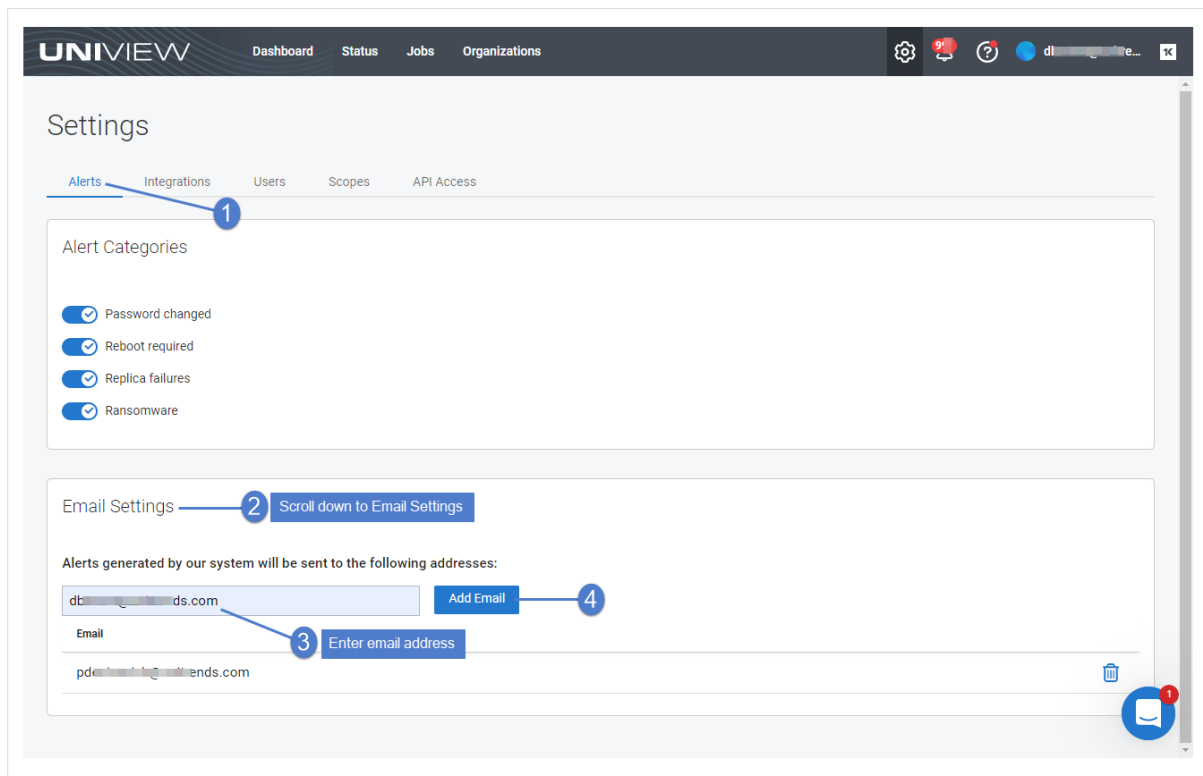
Unresolved alerts display in the BackupIQ alerts list. If you have integrated UniView Portal with a PSA system (BMS, Autotask, or ConnectWise), a ticket is also generated in your PSA. Additionally, you may opt to receive email notifications for these alerts. Use these steps to set up email notification:

Note: To integrate your PSA system with UniView Portal, see *Working with Integrations* in the [UniView Portal Guide](#).

- 1 In the UniView Portal, click **Settings**:



- 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.

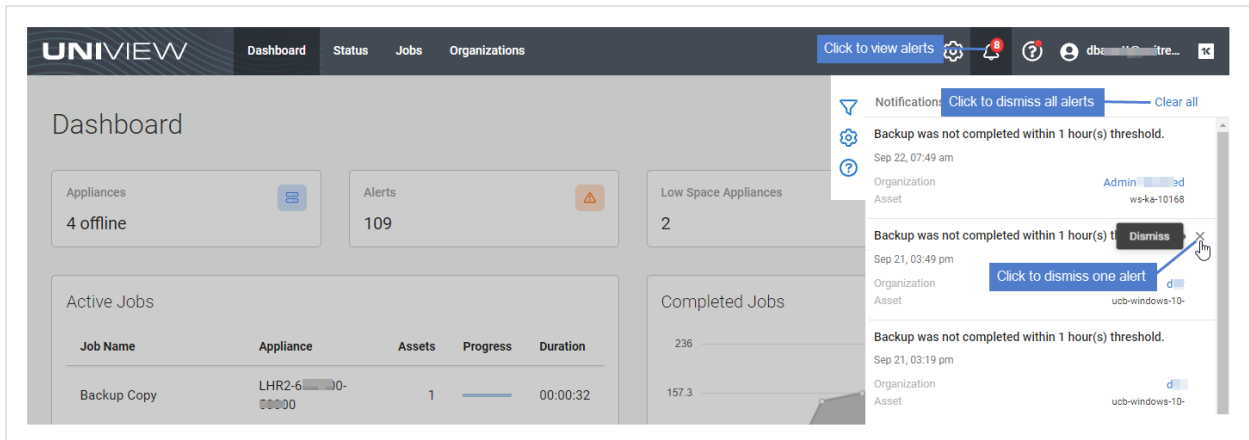
Once the alert condition has been resolved, UniView Portal automatically removes the alert from BackupIQ and emails notification that the alert has been dismissed.

To dismiss BackupIQ alerts

Once an alert condition has been resolved, UniView Portal automatically removes the alert from BackupIQ. You can opt to manually dismiss alerts by using this procedure.

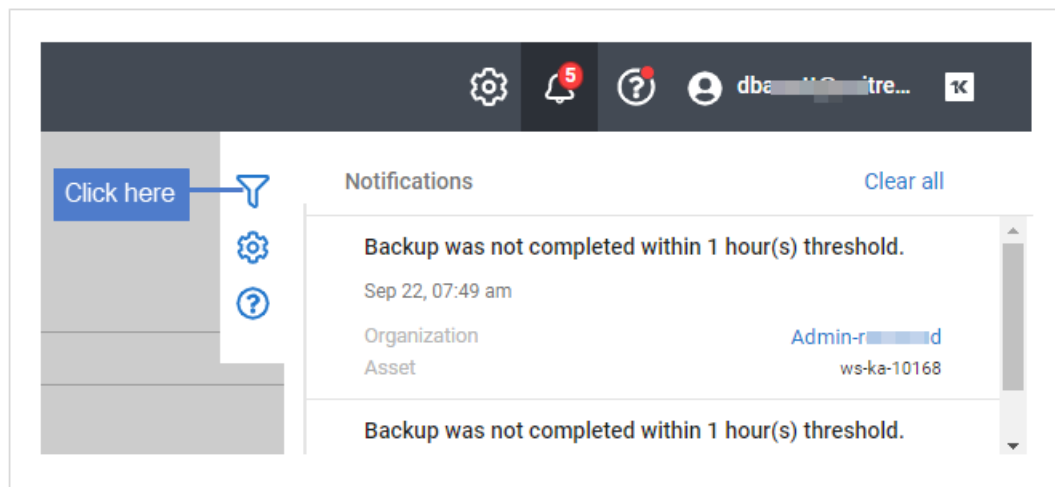
Note: Dismissing an alert does not resolve the alert condition. If the alert condition still exists, a subsequent alert will be generated.

- 1 Log in to the UniView Portal.
- 2 Click the BackupIQ icon to display alerts.
- 3 (Optional) To dismiss a single alert, click its **X** icon.
- 4 (Optional) To dismiss all alerts, click **Clear all**.

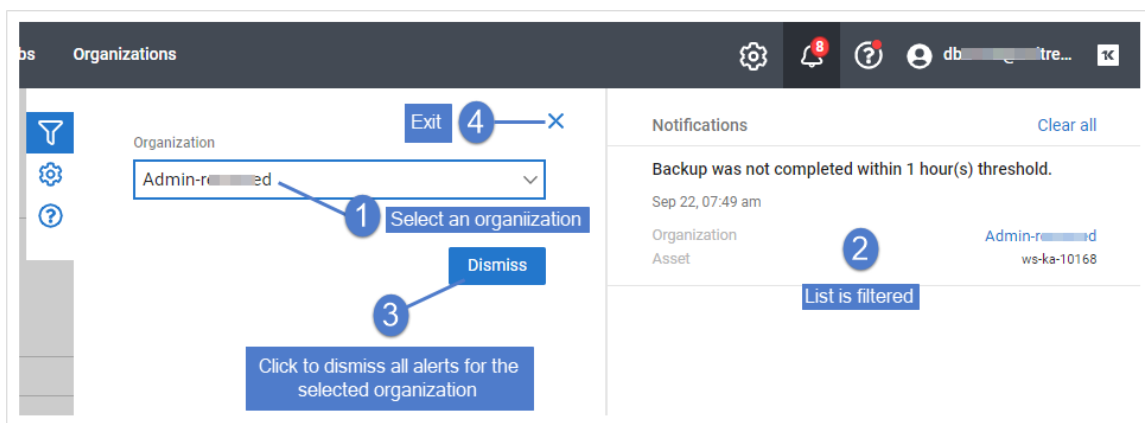


5 (Optional) To dismiss one organization's alerts:

- Click .



- Select an organization from the Organization list.
- Click **Dismiss**.



Working with asset log storage

Enable this feature to automatically upload your assets' error log files to the Unitrends Cloud. Error logs provide valuable troubleshooting information you can use to address Kaseya EndPoint Backup issues. Once logs have been uploaded, you can download and review them in just a few clicks— and easily send an error log .zip file to Unitrends Support so that issues can be resolved quickly.

The asset log feature applies to assets running Kaseya EndPoint Backup agent version 1.30 or higher. Once you have enabled the feature, logs are uploaded as tasks complete for assets running the 1.30+ agent. (To upgrade the agent on your assets, see "[Install the Kaseya EndPoint Backup agent](#)".)

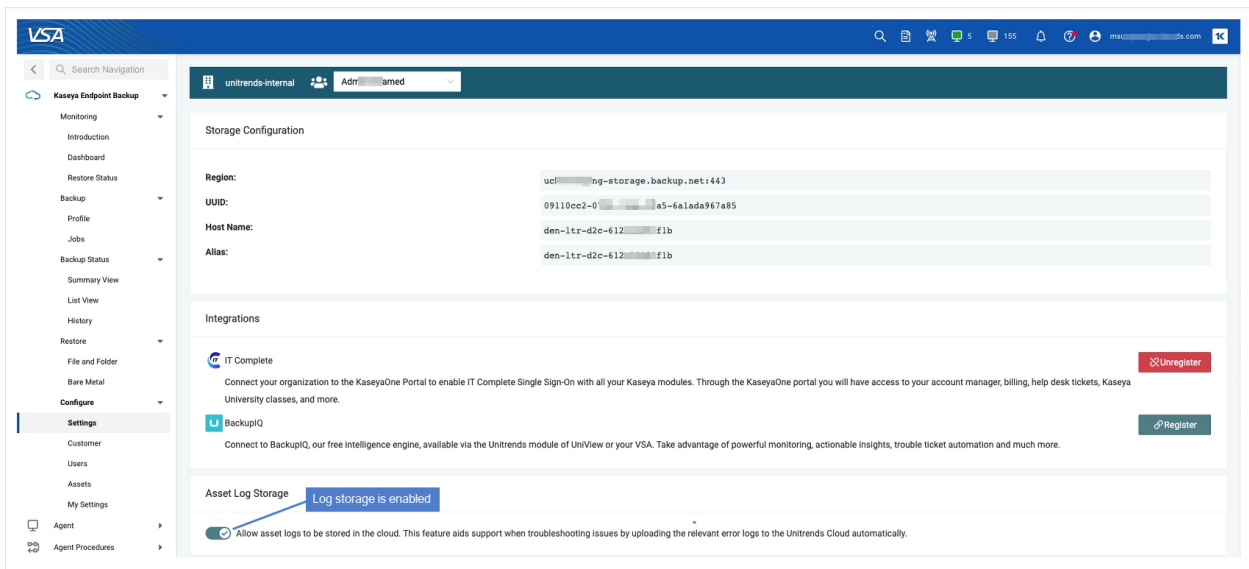
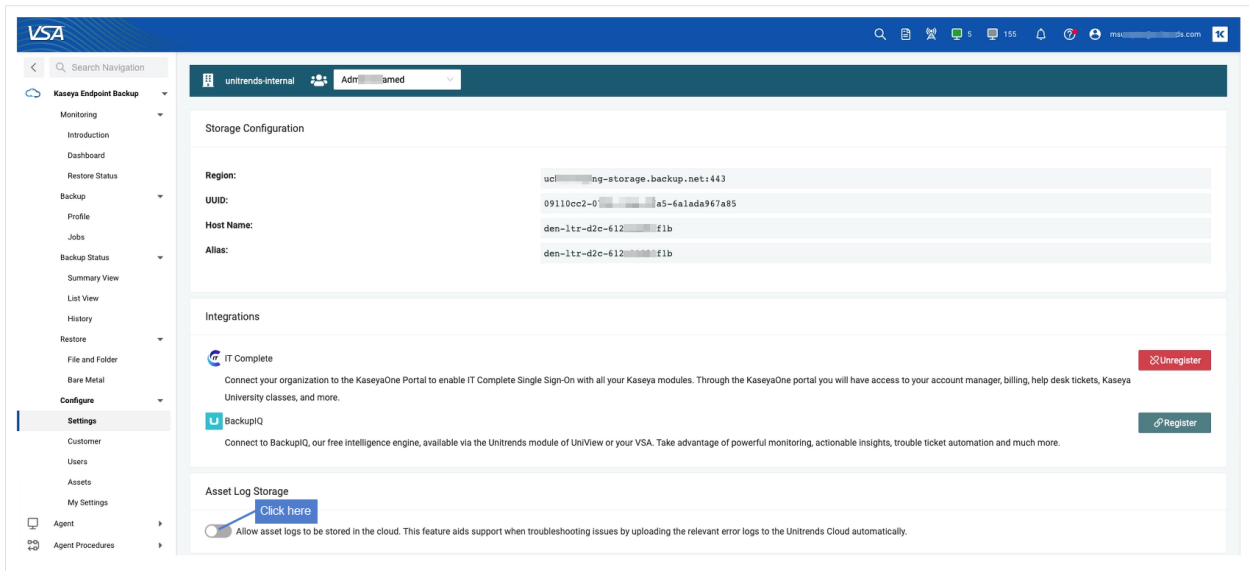
Logs are stored in the Unitrends Cloud for 60 days. Logs older than 60 days are automatically purged from Unitrends Cloud storage.

See these procedures for details:

- "[To enable asset log storage](#)"
- "[To download and view asset logs](#)"
- "[To disable asset log storage](#)"

To enable asset log storage

Locate the Asset Log Storage and click its button.

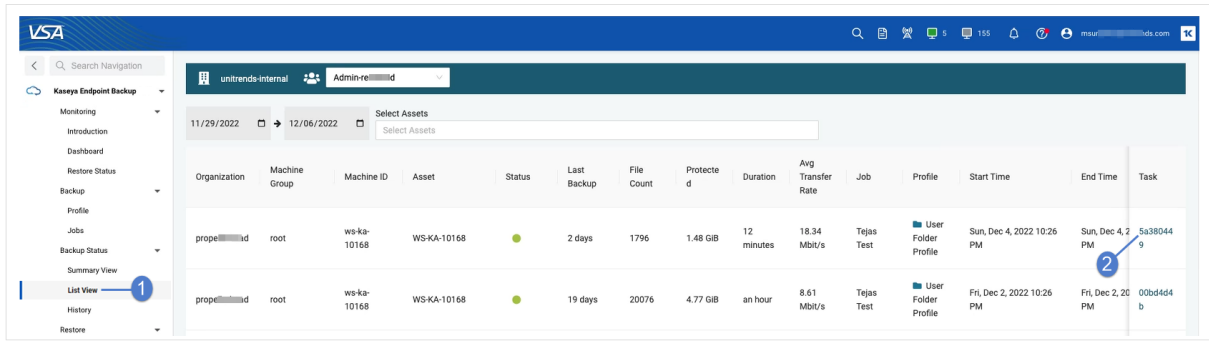


To download and view asset logs

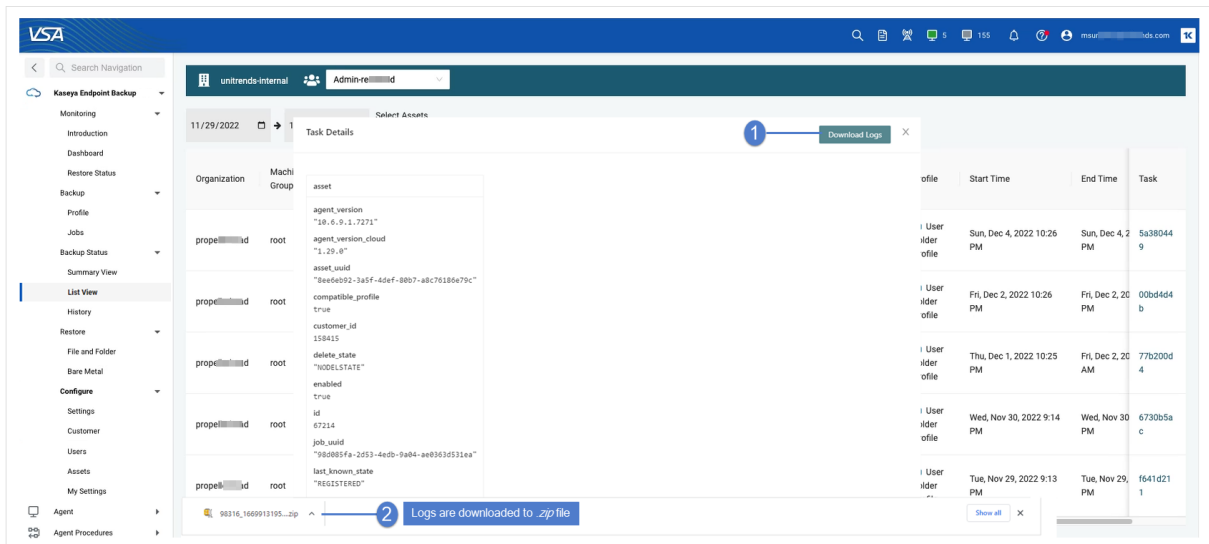
Logs are downloaded from the Task Details dialog. Access the Task Details dialog from either of these pages: Backup Status > List View or Restore Status. See "[Backup Status > List View Example](#)" or "[Restore Status Example](#)" for details.

Backup Status > List View Example

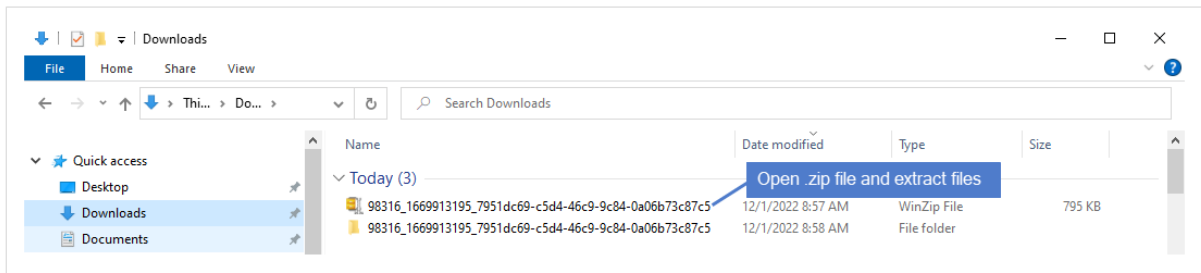
- 1 On the List View page, locate the asset and click its Task link.

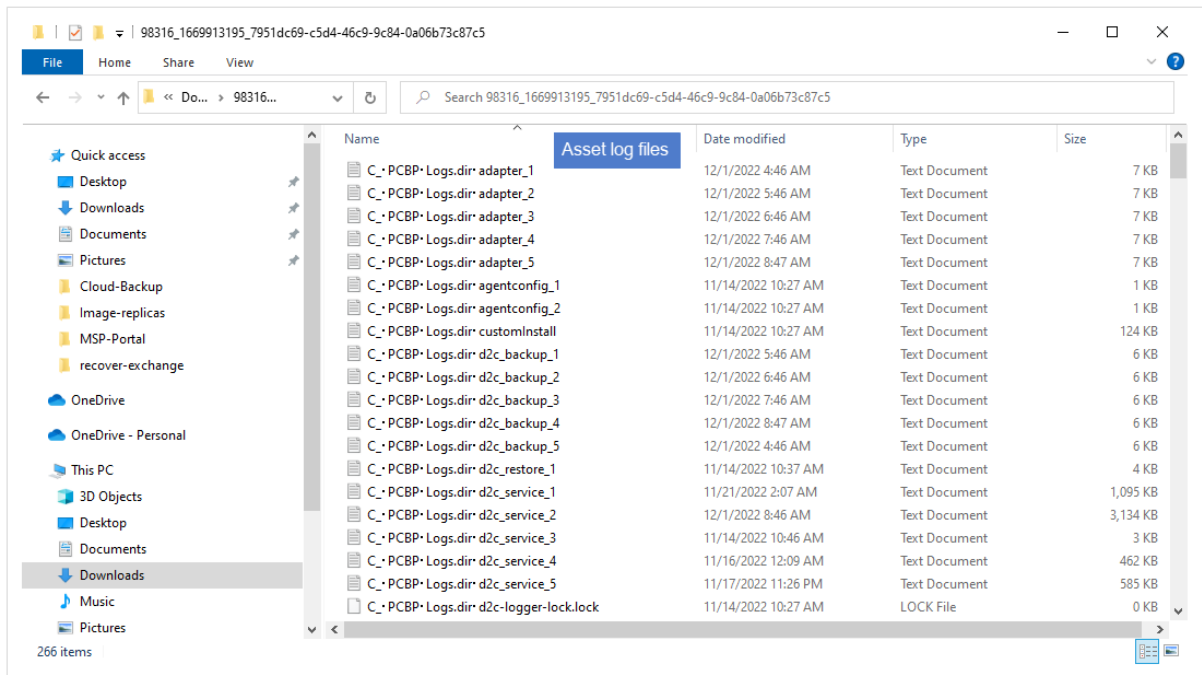


2 In the Task Details dialog, click **Download Logs**. A .zip file of the asset's recent logs is downloaded.



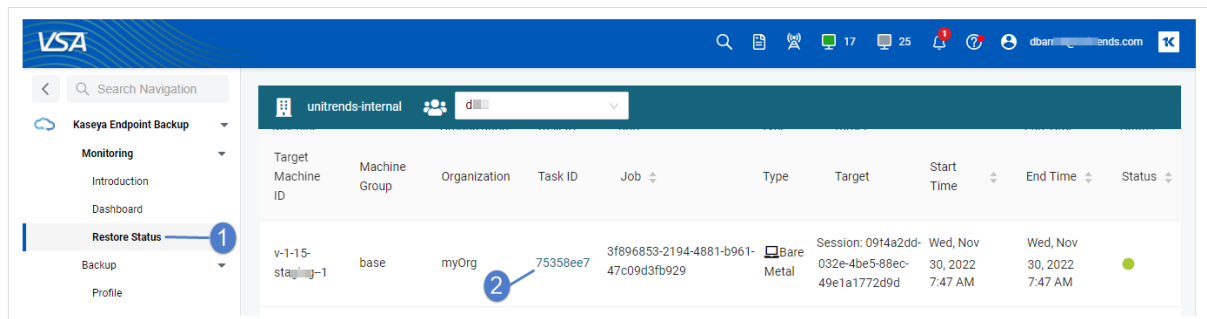
3 To view logs, open the .zip file and extract the log files.



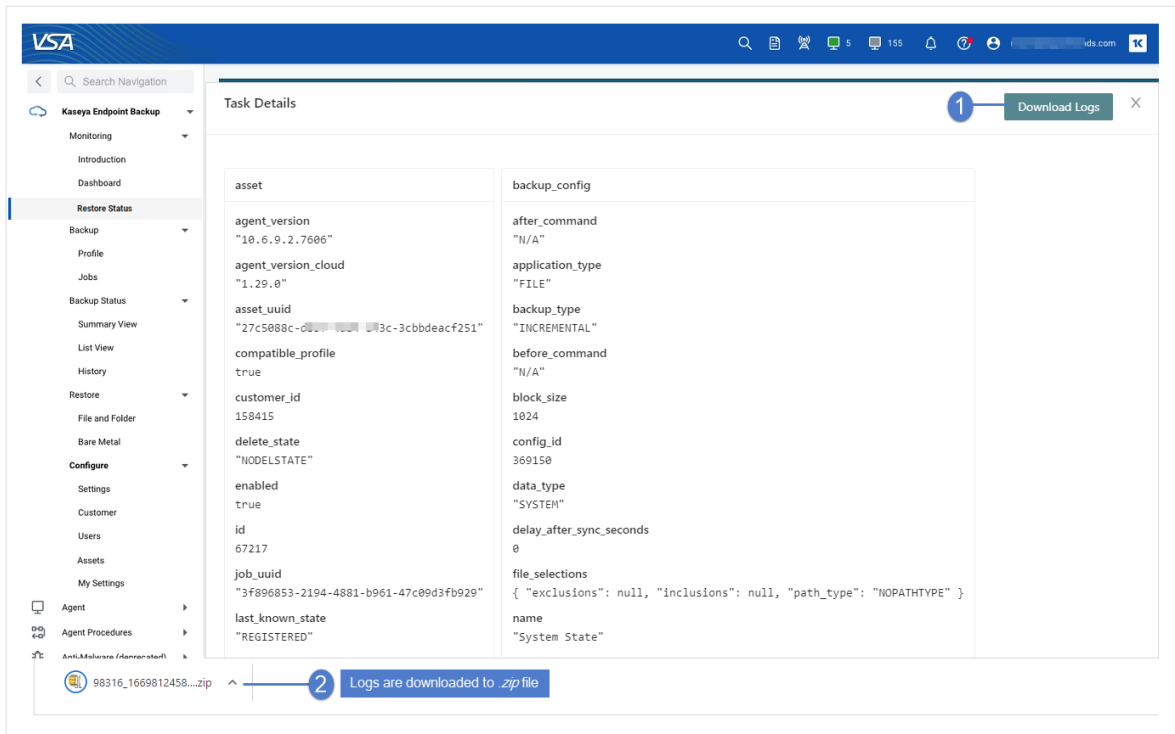


Restore Status Example

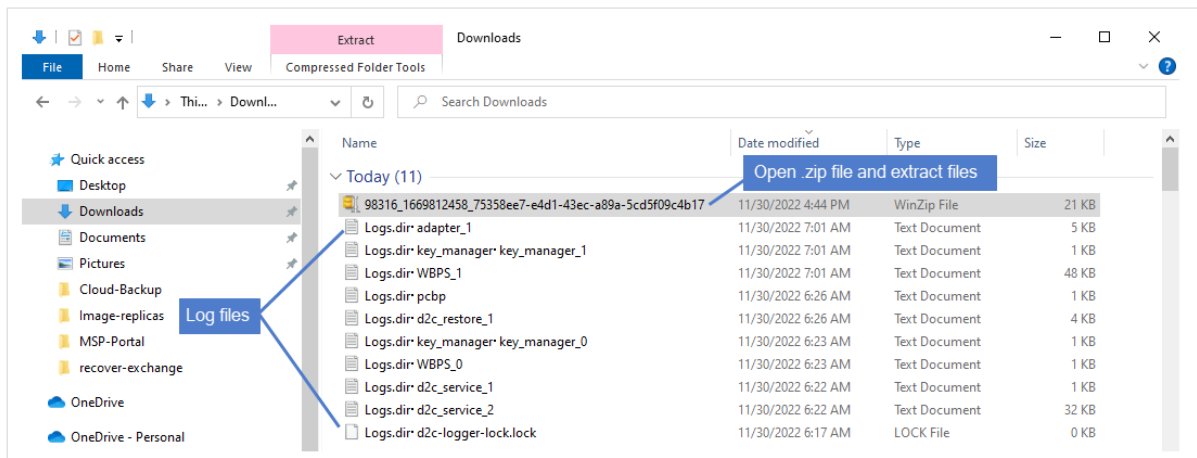
- 1 On the Restore Status page, locate the recovery task and click its Task ID link.



- 2 In the Task Details dialog, click **Download Logs**. A .zip file of the asset's recent logs is downloaded.

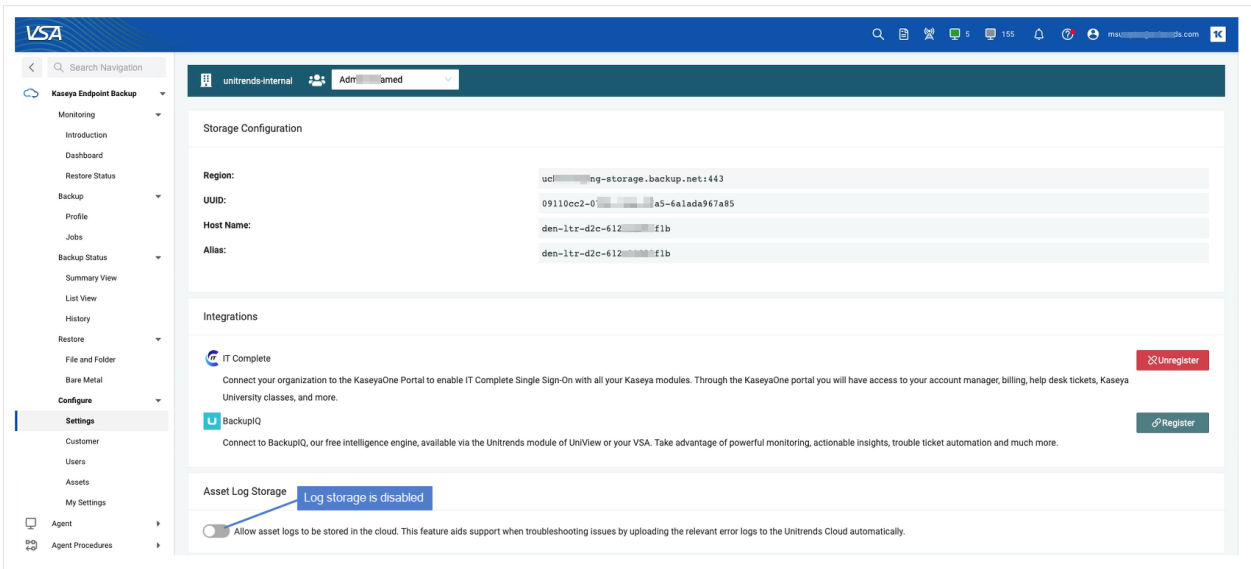
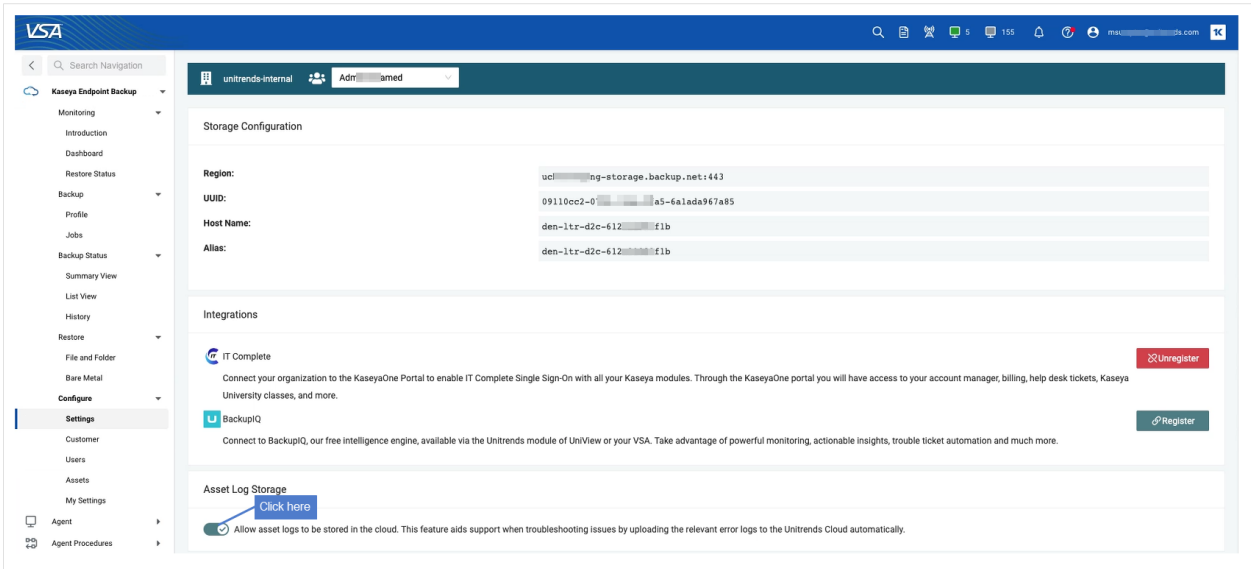


3 To view logs, open the .zip file and extract the log files.



To disable asset log storage

Locate the Asset Log Storage and click its button.



Chapter 9: 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.

To receive insights from Kaseya EndPoint Backup, your Kaseya EndPoint Backup and KaseyaOne user accounts must be linked. If you are using the *Login with IT Complete* single sign-on feature, you're all set. If not, run the "[To enable login with IT Complete](#)" procedure to set up single sign-on.

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

Kaseya EndPoint Backup includes these insights:

Insight Name	Summary	Triggers	Excludes
Recovery drills	Complete recovery testing at all your customer sites	No restores in > 90 days for a given customer	Insight does not apply to: <ul style="list-style-type: none"> • Disabled customers • Disabled assets • Systems without valid backups
Backup coverage	Ensure backups are configured and running on all systems	Asset has agent installed but is not part of a job. Not taking backups.	Insight does not apply to: <ul style="list-style-type: none"> • Disabled customers • Disabled assets • Deleted/decommissioned assets • Recently installed assets (< 7 days)

Our goal with these insights is to:

- Ensure that your assets are always protected.
- Ensure that you are adhering to industry best practices by conducting recovery tests for all the organizations you support.

These insights are just the beginning – stay tuned for more Kaseya EndPoint Backup insights in upcoming releases!

Working with Cooper Insights in KaseyaOne

To view and manage insights:

- 1 Log in to KaseyaOne and select **Cooper**.
- 2 Active insights display in the To Do list.

Module	Completed
Passly	0/2
myITprocess	0/3
Compliance Manager	5/5
Network Detective Pro	0/4
VulScan	3/4
Spanning Google Workspace	2/2
Spanning Microsoft 365	2/2
Cooper	0/4
BullPhish ID	1/2
VSA	3/4
Graphus	2/2
EndPoint Backup	0/2

- 3 Click an EndPoint Backup insight.
 - 4 Review insight details. Do one of the following:
 - Click the action button to address the insight (*Jump to the Endpoint Backup recovery page in our example*).
- OR
- Click **Skip For Now** to move the insight to the Archived list.

Notes:

- To address the recovery drills insight, run one test recovery for each of the customers listed in the insight details (*customers Good Burger and Miami Specialist Lab in our example*).
- To address the backup coverage insight, run backups for each of the assets listed in the insight details.
- You can also opt to disable customers, disable assets, or delete/decommission assets to remove them from the insight.

The screenshot displays the KaseyaOne Cooper Insights interface. On the left is a navigation sidebar with options like Home, Billing & Subscriptions, Cooper, Support, Admin Settings, and IT Complete Community. The main header shows the user's name 'Cooper' and a notification bell. Below the header, there are filters for 'To Do' (16), 'Completed' (21), and 'Archived' (2). The 'Your Insights' section contains several cards, including 'How to add and manage KaseyaOne user accounts', 'You need to test your backups!', 'Careful! Backups aren't configured to run on some of your endpoints.', and 'Maximize training engagement with 'Custom Domains''. A modal window titled 'You need to test your backups!' is open, showing a video player and a 'Skip For Now' button. Numbered callouts 1, 2, and 3 are placed on the dashboard to indicate the flow of actions.

- 5 When the insight condition is resolved, the insight moves to the Completed list.

This page is intentionally left blank.



Chapter 10: Upgrading to the Latest Release

To upgrade to the latest release:

- 1 Install the latest TAP module as described in "Upgrading the Kaseya EndPoint Backup TAP module".
- 2 Install the latest agent on all protected assets as described in "Upgrading the Kaseya EndPoint Backup agent".

Upgrading the Kaseya EndPoint Backup TAP module

Use this procedure to upgrade the TAP module. The instructions are slightly different depending on whether you have a SaaS or on-premise VSA instance:

- If you are using VSA on-premise, run all steps in the procedure.
- If you are using VSA SaaS, [step 3](#) is not needed. Skip this step in the procedure.

To install or upgrade the Kaseya EndPoint Backup TAP module

- 1 Go to https://direct.backup.net/download/kaseya_endpoint_backup.vsz and download *kaseya_endpoint_backup.vsz* to your workstation.
- 2 Log into the VSA instance.

Note: Do not use a VSA URL that includes *-cdn*. Use the URL that goes directly to your VSA server instance.

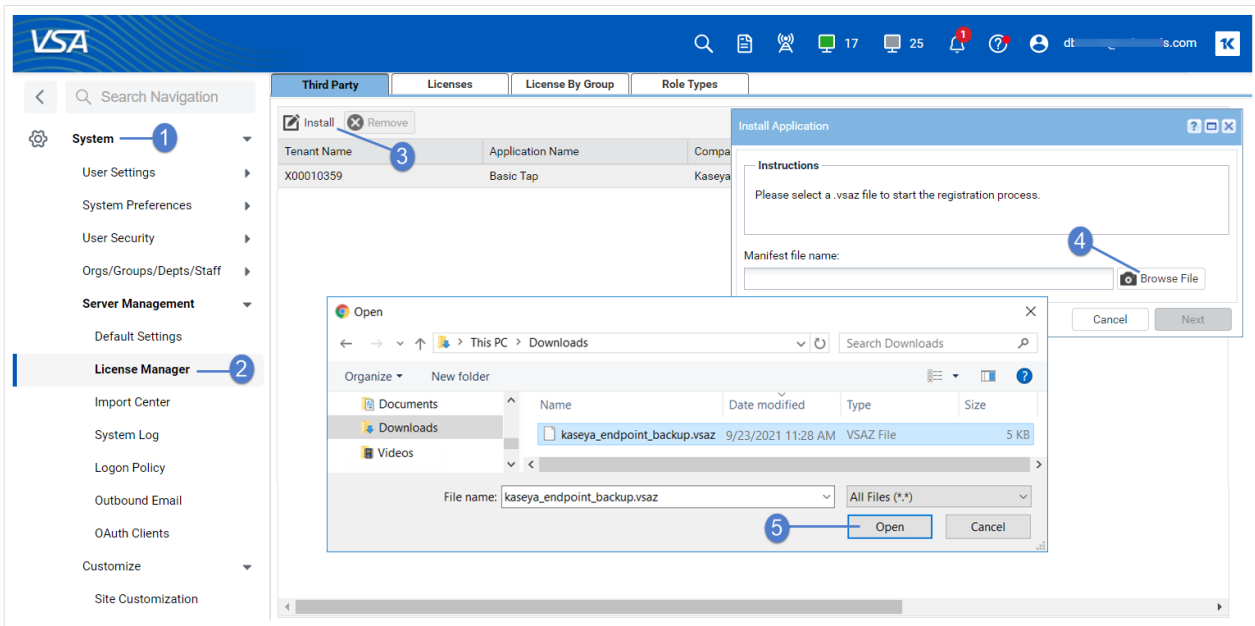
- 3 On-premise instance only – Select **System > Server Management > Configure** and make sure you have checked this box: **Enable Third Party App Installation Globally**.

The screenshot shows the VSA configuration interface. The left sidebar contains a navigation menu with the following items: System (1), User Settings, System Preferences, User Security, Orgs/Groups/Depts/Staff, Server Management, Configure (2), Default Settings, License Manager, Import Center, System Log, Logon Policy, Outbound Email (3), OAuth Clients, Customize, BMS Integration, Agent, Agent Procedures, Anti-Malware, Antivirus, Audit, AuthAnvil, Backup, Cloud Backup, and Data Backup. The main content area displays the following information:

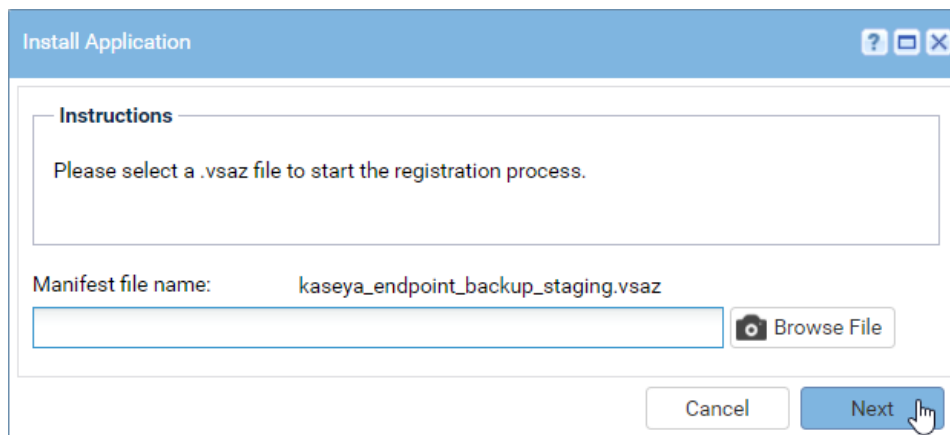
- Version Number: 9.5.0.2
- Installed Patch Level: 9.5.0.23
- Available Patch Level: 9.5.0.23
- Last Checked On: Wed Oct 2 18:28:11 EDT 2019
- Check Latest Patch Level button
- Patch Release Notes and Installation Instructions link
- Warn if the server can not get data from <http://vsaupdate.kaseya.net> (checked)
- Warn when the license reaches the maximum number of seats (checked)
- Reapply Schema and Defrag Database links
- Reload sample **scripts** with every update and database maintenance cycle (checked)
- Reload sample **event sets** with every update and database maintenance cycle (checked)
- Reload sample **monitor sets** with every update and database maintenance cycle (checked)
- Automatically redirect to HTTPS at logon page (checked)
- Enable VSA API Web Service (checked)
- Enable Third Party App Installation Globally (checked)
- Enable Invalid Patch Location Notifications (checked)
- Allow non-authenticated users to download attachments from ticket notifications (checked)
- Run database backup / maintenance every: 7 Days @ 2:00 am (Set Period button)
- Backup folder on KWEB1: C:\Kaseya\UserProfiles\@dbBackup (Change, Default buttons)
- Enter 0 to disable recurring backups. (Change DB..., Backup Now, Restore... buttons)
- Archive and purge logs every day @ 4:00 am (Set Period button)
- Log file archive path: C:\Kaseya\UserProfiles\@archive (Change, Default buttons)
- KServer Log button
- Live Connect KServer button (green dot)
- Stop KServer button
- Restart MsgSys button
- Enable alarm generation. Disable during system maintenance (checked)
- Enable logging of script errors marked "Continue script if step fails" (checked)
- Enable logging of successful child script execution in agent procedure log (checked)

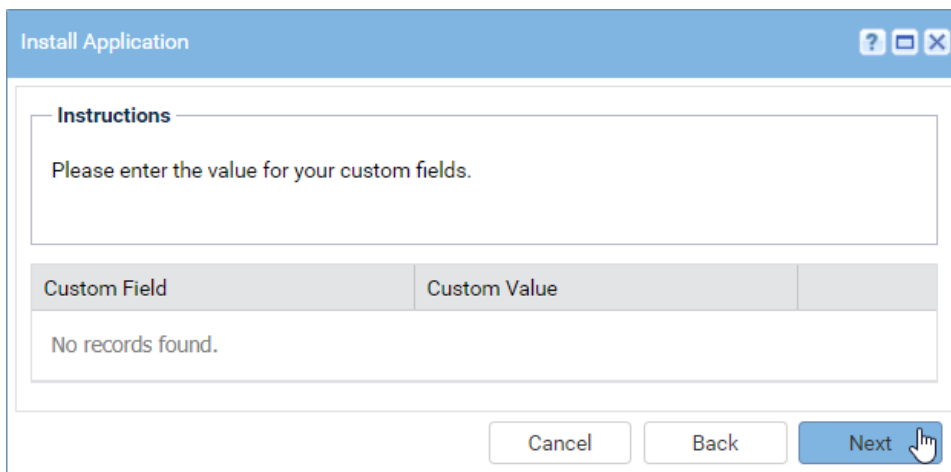
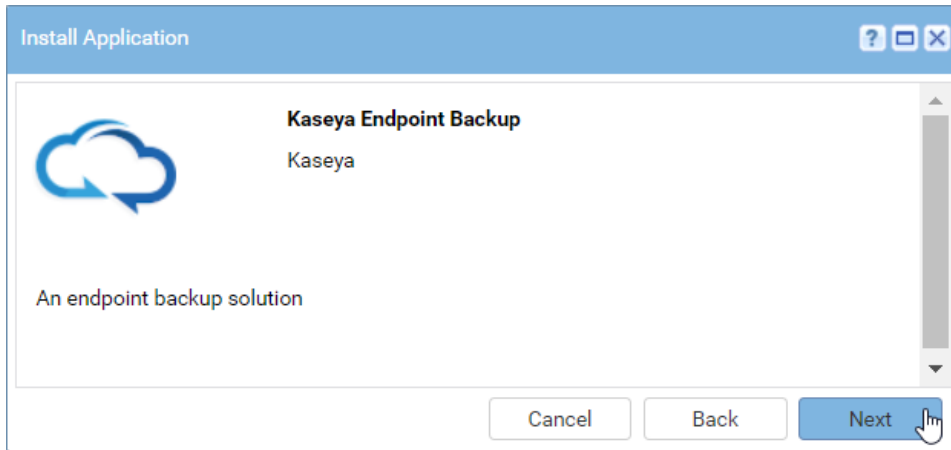
4 Select **System > Server Management > License Manager > Third Party > Install**.

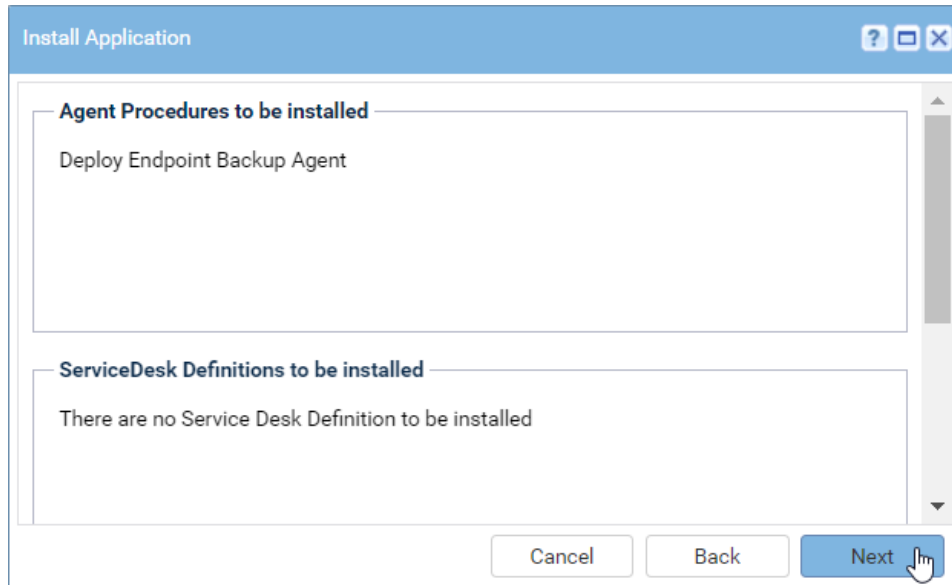
5 Click **Install**. Browse to the path where you downloaded the TAP module in [step 1](#). Select **kaseya_endpoint_backup.vsaz**. Click **Open**.



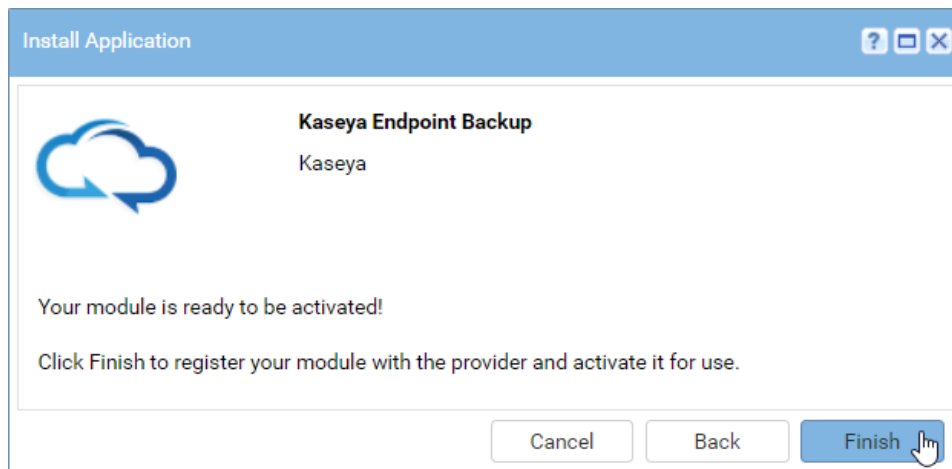
6 Click **Next** to work your way through the install wizard.

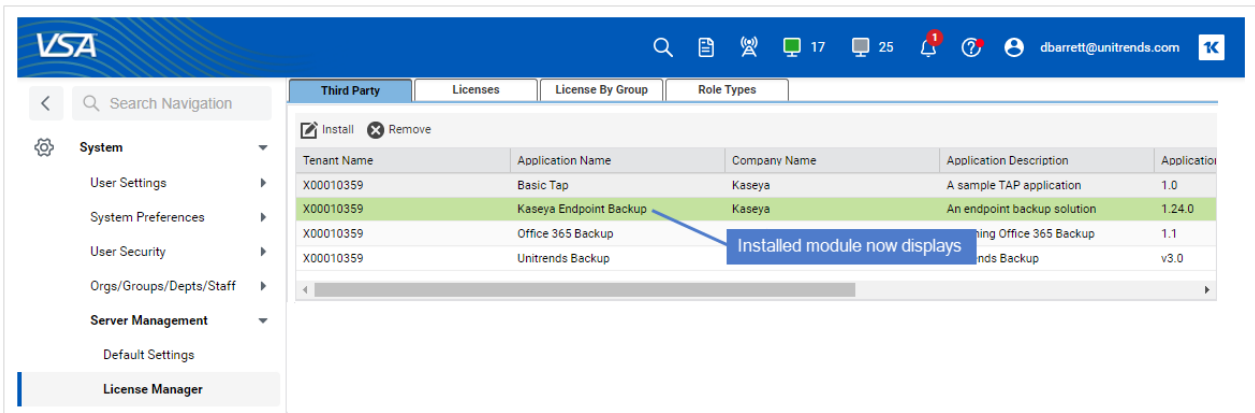






- 7 Click **Finish**. The module is installed.





Upgrading the Kaseya EndPoint Backup agent

Use these procedures to install or upgrade the agent:

- ["To install or upgrade the Kaseya EndPoint Backup agent by using a VSA agent procedure"](#)
- ["To install or upgrade the agent manually on a single asset"](#)

To install or upgrade the Kaseya EndPoint Backup agent by using a VSA agent procedure

This procedure installs the Kaseya EndPoint Backup agent to one or more machines by using a VSA agent procedure.

- 1 Select **Configure > Assets**.
- 2 Select the customer whose assets you will protect.

Note: The agent installer is specific to the selected customer. Be sure the customer whose asset you will protect displays in the customer context banner before downloading the agent.

- 3 Click **Bulk Installation** to generate a unique access key.

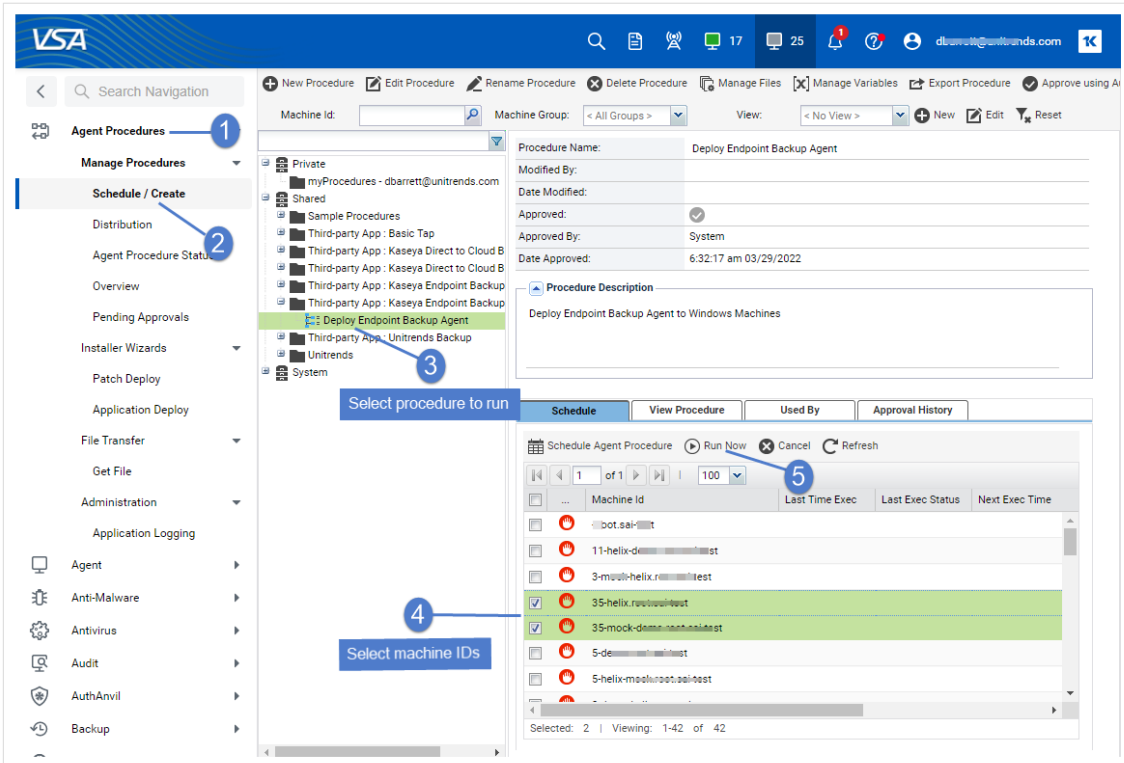
Note: You must run the install procedure within 30 days of generating the access key.

- 4 Copy the access key.

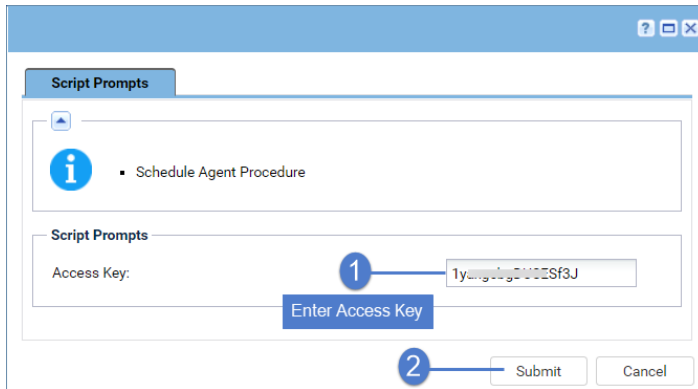
The screenshot shows the VSA Kaseya EndPoint Backup interface. A notification at the top states: "Access key created successfully. Paste this key into your Endpoint Backup deployment procedure: 29RBZxU6T17UU8Mq". Below this, there are buttons for "Bulk Installation" and "Single Installation". A table lists assets with columns for Machine ID, Machine Group, Organization, Asset Name, Success Of Last 10 Tasks, Last Seen, Enabled, and Agent Version. A "Copy the access key" button is positioned above the table. The left sidebar shows navigation options, with "Assets" highlighted and numbered 1.

Machine ID	Machine Group	Organization	Asset Name	Success Of Last 10 Tasks	Last Seen	Enabled	Agent Version
v-1-22-staging-	base	myorg	v-1-22-staging-ucb-199-250	0%	04/19/2022 10:50	ON	1.25.0
v-1-22-staging-	base	myorg	v-1-22-staging-ucb-199-250	0%	12/07/2021 17:28	ON	1.25.0
ws-ka-10168	root	propellerhead	WS-KA-10168	80%	05/20/2022 12:57	ON	1.24.0
			ucb-windows-10-	100%	10/01/2021 15:24	ON	

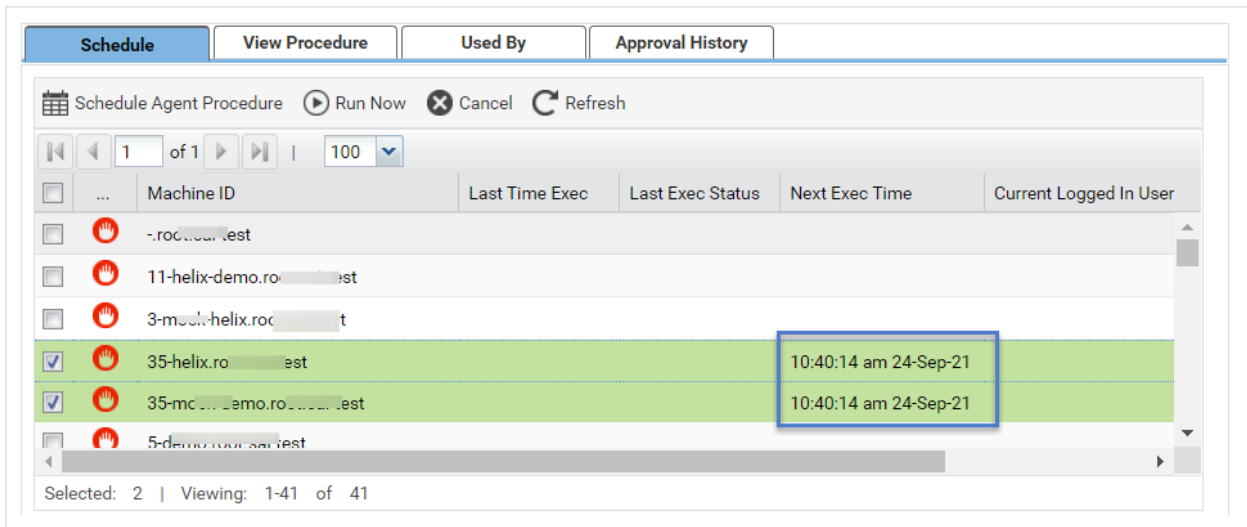
- 5 Select **Agent Procedures > Manage Procedures > Schedule/Create**.
- 6 Under **Shared procedures > Thirdparty App: Kaseya Endpoint Backup**, select **Deploy Endpoint Backup Agent**.
- 7 On the **Schedule** tab, select one or more machine IDs. Click **Run Now**.



- 8 Enter the Access Key and click **Submit**.



- 9 The install procedure is added and will run upon the next agent check-in. Look at the Next Exec Time column to see a machine's next agent check-in time:



Once the agent has been deployed, the asset displays on the **Kaseya Endpoint Backup > Configure > Assets** page. The asset name changes from *Unregistered* to the machine's host name once the agent checks in.

Note: If you do not see the asset on the **Configure > Assets** page, see "[Troubleshooting Kaseya EndPoint Backup agent installs](#)" for next steps.

To install or upgrade the agent manually on a single asset

This procedure installs the Kaseya EndPoint Backup agent to one machine by using PowerShell.

Notes:

- You can opt to install to a single asset by using a VSA agent procedure (as described in "[To install or upgrade the Kaseya EndPoint Backup agent by using a VSA agent procedure](#)"). Use this procedure if you prefer to install by using the PowerShell installer, *deploy_cloud_backup_agent.ps1*.
- You must run *deploy_cloud_backup_agent.ps1* within 30 days of downloading the file.

- 1 Select **Configure > Assets**.
- 2 Select the customer whose assets you will protect.

Note: The agent installer is specific to the selected customer. Be sure the customer whose asset you will protect displays in the customer context banner before downloading the agent.

- 3 Click **Single Installation**.
- 4 Download *deploy_cloud_backup_agent.ps1* to the Windows asset.

Note: You must run the install procedure within 30 days of downloading *deploy_cloud_backup_agent.ps1*.

The screenshot shows the VSA interface with the following elements:

- Navigation Sidebar (Left):** Includes links for Monitoring, Introduction, Dashboard, Restore Status, Backup, Profile, Jobs, Backup Status, Summary View, List View, History, Restore, File and Folder, Bare Metal, Configure, Settings, Customer, Users, and **Assets** (highlighted with callout 1).
- Header:** Shows 'unitrends-internal' and 'Admin' with a 'Select a customer' dropdown (callout 2).
- Notification:** A green banner at the top provides instructions on downloading a script for bulk installation.
- Buttons:** 'Bulk Installation' and 'Single Installation' (callout 3) buttons are located above the table.
- Table:** Contains asset information with columns: Machine ID, Machine Group, Organization, Asset Name, Success Of Last 10 Tasks, Last Seen, Enabled, and Agent Version.

Machine ID	Machine Group	Organization	Asset Name	Success Of Last 10 Tasks	Last Seen	Enabled	Agent Version
v-1-22-staging-	base	myorg	v-1-22-staging-wcb-199-250	0%	04/19/2022 10:50	ON	1.25.0
v-1-22-staging-	base	myorg	v-1-22-staging-wcb-199-250	0%	12/07/2021 17:28	ON	1.25.0
ws-ka-10168	root	propellerhead	WS-KA-10168	80%	05/20/2022 12:57	ON	1.24.0
mb-windows-				100%	10/01/2021 15:24	ON	
- Warning Dialog (Callout 4):** A red warning box at the bottom of the table asks: 'This type of file can harm your computer. Do you want to keep deploy_cloud_backup...ps1 anyway?' with 'Keep' and 'Discard' buttons.

- 5 Log in to the Windows asset and launch PowerShell as administrator.
- 6 Issue this command to run the agent install script, where *<FullPath>* is the full path of the location where you saved *deploy_cloud_backup_agent.ps1*: **PowerShell.exe -executionpolicy bypass -File <FullPath>\deploy_cloud_backup_agent.ps1**. Enter **Y** to confirm. Example command text is given here:

```

Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\WINDOWS\system32> PowerShell.exe -executionpolicy bypass -File C:\users\S\m\Downloads\deploy_cloud_backup_agent.ps1
  
```

- 7 When you see the security warning about running downloaded scripts, press **R** and **Enter** to continue.
- 8 The agent is downloaded and deployed. When deployment is complete, you see a *cleaning up* message.


```

Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\WINDOWS\system32> PowerShell.exe -executionpolicy bypass -File C:\users\...Downloads\deploy_cloud_backup_agent.ps1
Checking permissions
Executing as Administrator
Getting agent download location
Downloading https://ucb-.../Unitrends_Agentx64.msi
Installing cloud backup agent
Cleaning up
PS C:\WINDOWS\system32>

```

- 9 Once the agent is deployed, the asset displays on the **Configure > Assets** page.

Machine ID	Machine Group	Organization	Asset Name	Success Of Last 10 Tasks	Last Seen	Enabled	Agent Version	Actions
			ws-dpinheiro-01	0%	05/20/2022 13:28	ON	1.25.0	Run Full, Run Once, Delete
			v15-staging-ucb-199-83	100%	07/07/2020 11:32	ON	1.25.0	Run Full, Run Once, Delete
			v15-staging-kdcb-199-85	100%	09/28/2020 19:37	ON	1.25.0	Run Full, Run Once, Delete

Troubleshooting Kaseya EndPoint Backup agent installs

If you have installed the Kaseya EndPoint Backup agent but the machine does not display on the **Kaseya EndPoint Backup > Configure > Assets** page, check the agent procedure log messages and address any error conditions.

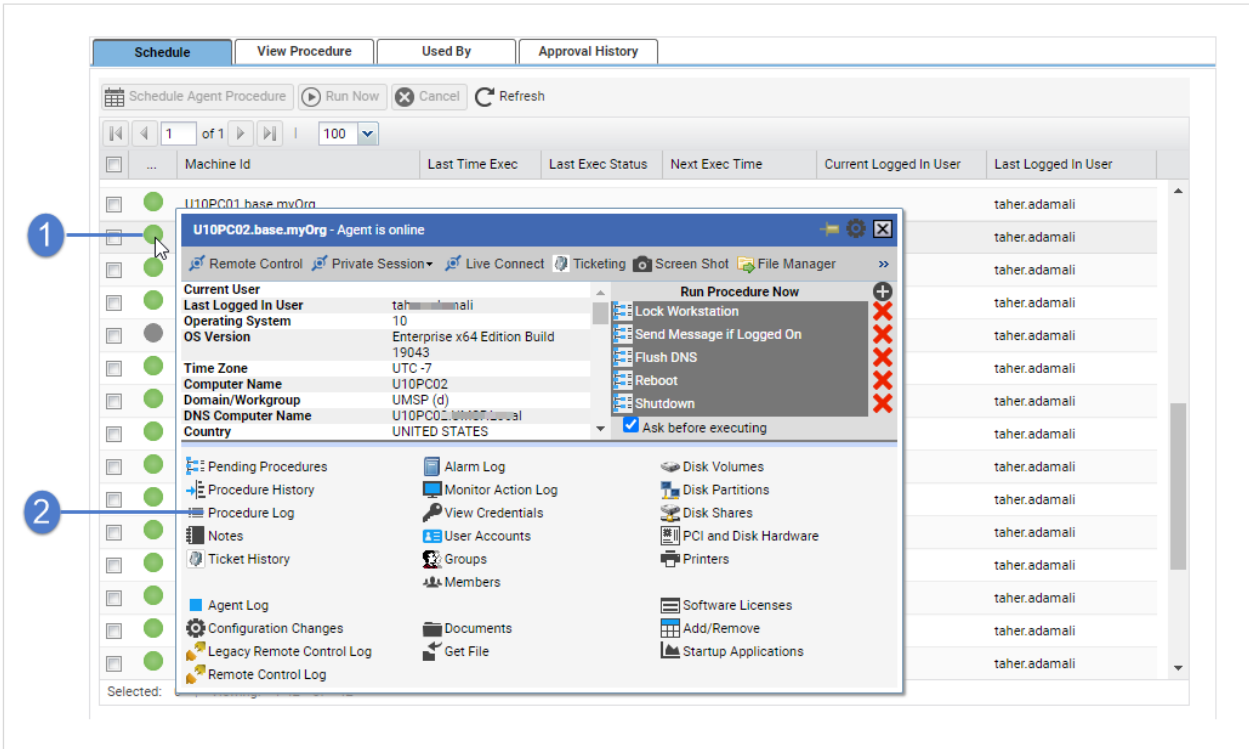
To view the agent procedure log

- 1 Select **Agent Procedures > Manage Procedures > Schedule/Create**.
- 2 Under **Shared procedures > Thirdparty App: Kaseya EndPoint Backup**, select **Deploy EndPoint Backup Agent**.

The screenshot displays the VSA (Virus Scan Agent) interface. The top navigation bar includes the VSA logo, search, and user information. The left sidebar shows 'Agent Procedures' (1) and 'Schedule / Create' (2) highlighted. The main content area shows the 'Deploy Endpoint Backup Agent' procedure details, including the procedure name, modified by, date modified, approved status, and procedure description. The 'Schedule' tab is active, showing a table of machines with columns for Machine Id, Last Time Exec, Last Exec Status, and Next Exec Time. A hover tooltip is visible over the 'Deploy Endpoint Backup Agent' procedure, showing a check-in icon (3).

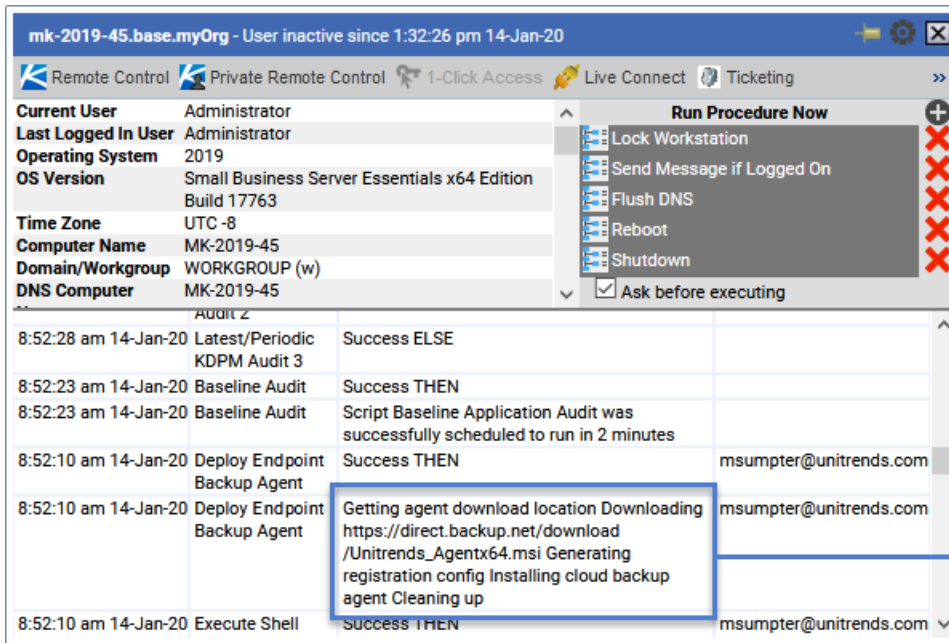
Machine Id	Last Time Exec	Last Exec Status	Next Exec Time
U10PC01.base.myOrg			
U10PC02.base.myOrg			
u10pc03.base.myOrg			
u10pc04.base.myOrg			
U16APP01.base.myOrg			
U16APP02.base.myOrg			
U19DC01.base.myOrg			

- 3 On the Schedule tab, hover over the machine's agent check-in icon to launch the agent Quick View window.
- 4 Click **Procedure Log**.



5 Check the log for Deploy EndPoint Backup Agent messages.

- Example agent install success message:



- Example agent install failure message:

The screenshot shows a remote control session for 'cae-r9-035gw1.base.myOrg'. The 'Run Procedure Now' menu is open, showing options like 'Lock Workstation', 'Send Message if Logged On', 'Flush DNS', 'Reboot', and 'Shutdown'. A log table below shows the following entries:

Time	Procedure	Description	Admin
8:11:11 am 16-Jan-20	Deploy Endpoint Backup Agent	Success THEN Endpoint	msumpter@unitrends.com
8:11:11 am 16-Jan-20	Deploy Endpoint Backup Agent	File C:\temp\deploy_cloud_backup_agent.ps1 cannot be loaded because running scripts is disabled on this system. For more information, see about_Execution_Policies at http://go.microsoft.com/fwlink/?LinkID=135170 . + CategoryInfo : SecurityError (:) [], ParentContainsErrorRecord Exception + FullyQualifiedErrorId : UnauthorizedAccess	msumpter@unitrends.com
8:11:11 am 16-Jan-20	Execute Shell command - Get Results to	Success THEN	msumpter@unitrends.com

A blue callout box points to the error message in the log, stating: "This means agent install failed".