
Aranda Data Safe

Welcome to the Aranda Datasafe Introductory Tutorial. If you're new to Aranda Datasafe, this is the perfect place to learn how to:

- Discover your devices and data.
- Configure your Active Directory computers, repositories, and connector.
- Create policies to configure Backup and Data Loss Prevention options.
- Run backups and restores.
- Learn how to use Data Loss Prevention features, such as Local Encryption, Remote Wipe and Geolocation.
- Learn how to use the full remote migration feature.

The tutorial is divided into a series of steps. You need to complete them in sequence, starting with Step 1 -Administrator Account Activation

Starting Data Safe

System Requirements

Hardware Requirements

Hardware Requirements for Storage Vault

The hardware requirements for Storage Vault can vary depending on the number of devices you need to protect. The following tables show our recommendations.

Specification	1-250 Users	251-500 Users	500-800 Users
Operating System	- Windows Server 2016 - 2019 - CentOS 6.x – 9.x - Debian 6.x – 11.x – Ubuntu 22.04 or later	- Windows Server 2016 - 2019 - CentOS 6.x – 9.x - Debian 6.x – 11.x – Ubuntu 22.04 or later	- Windows Server 2016 – 2019 – CentOS 6.x – 9.x - Debian 6.x – 11.x – Ubuntu 22.04 or later
CPU	CPU 4 Cores	6 Cores / vCPUs	8 Cores / vCPUs
Memory	6 GB	8 GB	16 GB
Storage - Vault(~20 GB per user)	5 TB	10 TB	16 TB +
Storage – Vault Index	N/A	50GB SSD	50GB SSD

Agent Requirements

Here are the recommended system requirements for devices to successfully run Aranda Agent:

Specification	Description
Operating System	Windows 10/11 Pro or Enterprise
CPU	Intel i3, i5, i7 or AMD equivalent
RAM	384 MB available to the agent
Storage	500MB free *Solid state drive for better performance.

Network Requirements

Request	Description
Resolve EPC Tenant DNS Name	nslookup endpointcloud.com
Allow Internet Access to the Tenant	The firewall and proxy must allow communication with: .endpointcloud.com Allow outbound communication on port 443.
The Firewall must allow communication from the client devices to the storage vault server.	Incoming and outgoing via port 9000 on the storage vault server.

Active Directory Connector Requirements

The AD Connector will be able to be installed on the same hardware as the Storage Vault. If you don't have an On-Premises/On-premises Vault, then you'll need the following minimum hardware specifications for AD Connector installation:

Request	Description
Operating System	Windows Server 2016 - 2019
CPU	4 Cores / vCPUs
RAM	4 GB (OS requirement included)
Storage	500MB free.

Active Directory and Access Requirements

The following requirements must be met to provide access:

Requirements	Description
AD Domain for User Authentication	AD domain for user authentication For AD integration, an AD domain is required. Domain is not required for workgroup deployment.
The AD Connector must be installed on a server joined to the active directory domain.	It must be the same AD domain that is used to authenticate the user.
The Windows Server administrator account must have sufficient permissions.	You must have permissions to: Install software and services. Register an SPN record in the domain. Access https://endpointcloud.com
Firewalls must allow customer devices to communicate with the Storage Vault.	Port 9000 inbound and outbound.

Activate your Administrator Account

To get started, activate your administrator account so you can log in and set up Aranda Datasafe.

⚐ > Note: When your organization registers with Aranda Datasafe, an account administrator will send you an email invitation. If you do not receive the email, please check your spam folders. If you still can't find the email, contact Aranda reportedecasos@arandasoft.com customer service. Once you have the email, click on **Activate Account**. Your browser opens the activation web page. The first time you access Aranda Datasafe, you need to enter a password and then re-enter it to confirm. Click **Activate** to log in. If you are the first administrator to log in, you will automatically be assigned the role of **Security Officer**. If it is not the first, it is assigned a role of **administrator**. (This can be changed later if needed.) The Security Officer role is the highest-ranking role and allows you to download and register the AD connector that is used for user authentication.

Install Discovery Agent

You can use the free Discovery Agent app to have Aranda Datasafe detect your users' devices automatically.

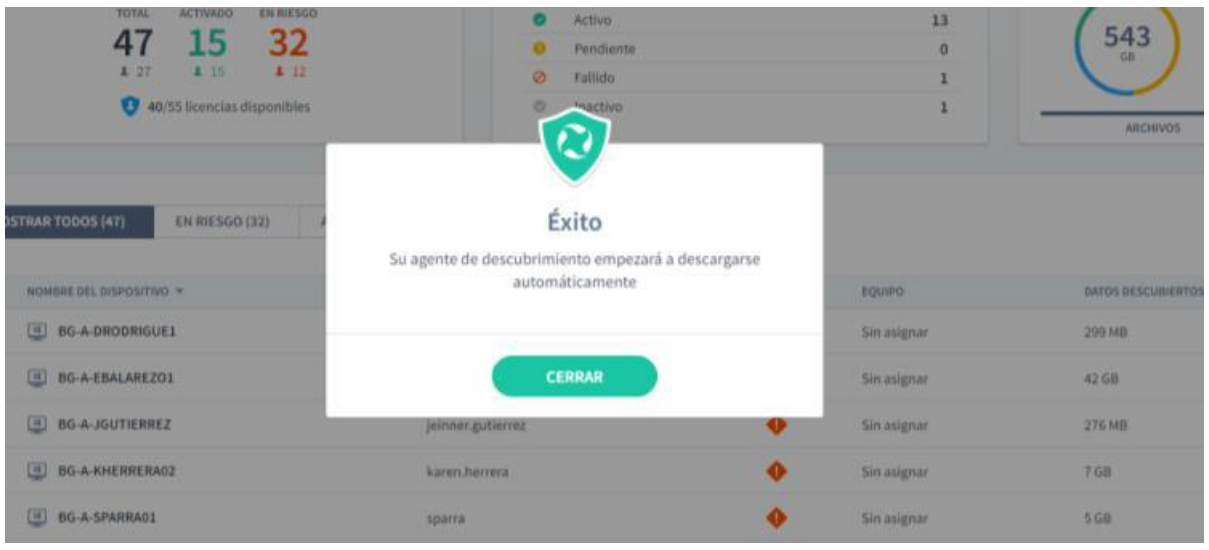
To configure Discovery Agent, download it and then install it on each end-user device. Do not install it on your server.

Download Discovery Agent

You can download Discovery Agent from your Aranda Datasafe Console:

1. Log in as an administrator. When you log in as an administrator for the first time, Inventory is selected by default. At this stage, Aranda Datasafe has not discovered any devices.

2. Click Download Discovery Agent. The Discovery Agent MSI package is downloaded to your browser. Discovery Agent is specific to your Aranda Datasafe instance.



Install Discovery Agent on your user devices

Install the MSI Discovery Agent package on each user device (desktop, laptop, etc.). The discovery agent will perform an inventory of devices and data, and then securely upload the information to Aranda Datasafe.

Prerequisites

- The user's devices must have access to the internet as the Discovery Agent needs to connect to Aranda Datasafe.
- The user's devices must use a Windows, Windows 7, or later operating system. A Mac version will be available soon.
- Firewalls and proxy servers must allow connections. You may need to whitelist endpointcloud.com and the full path to the Aranda Datasafe tenant URL. Example: https://arandasoftware.endpointcloud.com where "arandasoftware" is replaced with your organization's name.

You can install Discovery Agent manually or remotely on each device.

Manual Agent Installation

Discovery Agent can be installed by running the MSI package on each user device.

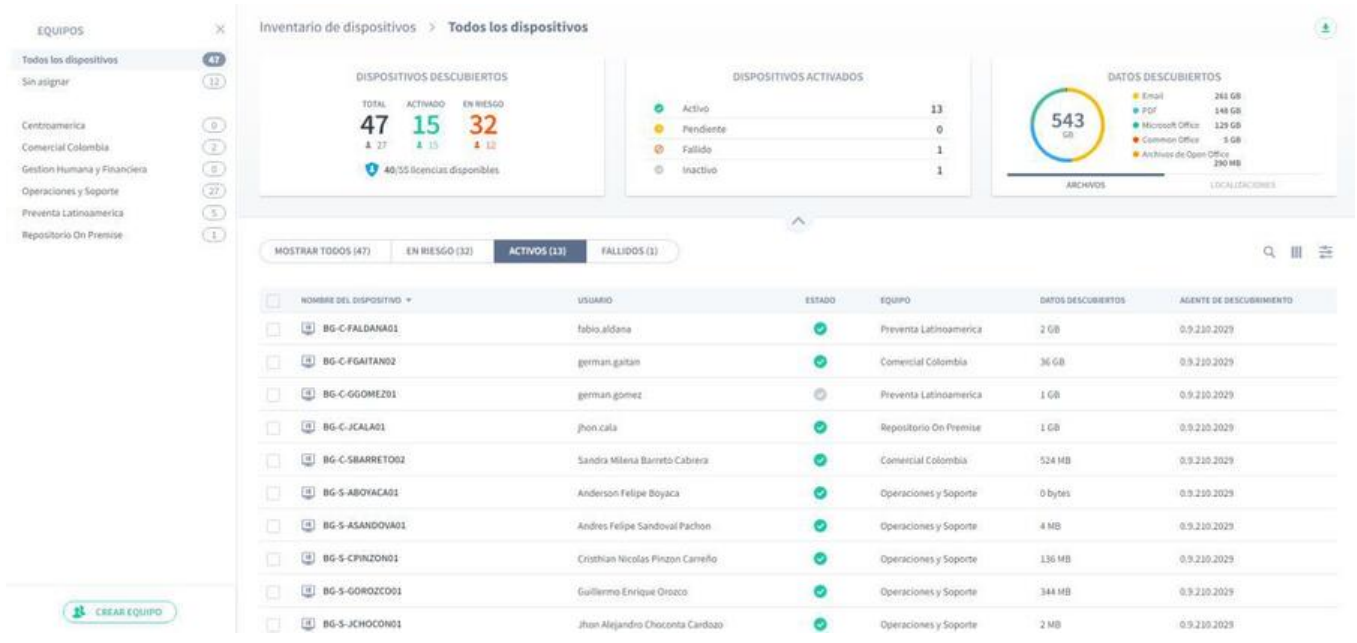
You may want to move the MSI package to a shared folder that can be accessed by all devices. Alternatively, you can put the MSI package on a memory card and transfer it between devices that way.

Remote Agent Installation

You can install the MSI package on devices remotely, using the Active Directory Group Policy feature or a third-party application. For more details, please contact Aranda Support (reportedecasos@arandasoft.com).

Inventory

When their devices have Discovery Agent installed, they will report to their Aranda Datasafe tenant. You'll see devices appear in the Inventory list, and the dashboard populates with data.



View the information for each of the sections.

1. **Discovered devices**: how many devices have been discovered, how many have been activated for protection, and how many are still at risk.

2. **Activated devices**: Useful once we start activating devices. It shows us how many devices are pending activation and how many have failed.

3. **Data discovered**: the amount of data discovered. You can see the amount based on file types or file locations.

There is also a device list that shows all the devices that Discovery Agent has discovered. There is a brief summary of the device, including the device's user account and the amount of data discovered.

You can access more detailed information for each device.

1. Click a device in the list of devices. A sliding panel appears that contains a more detailed summary of the device and the user account associated with it.

2. Click on the profile icon to display the full details of the device.

3. Click the back arrow next to the username at the top of the screen to return to the Inventory.

You may have noticed that on the left side of the Inventory is a list of**Equipment**. You'll use it to create new teams and organize your devices in the next step.

Organizing Devices into Teams

When your devices connect to Aranda Datasafe for the first time, they are "unassigned". This means that they are not on a team. You can create teams and use them to organize your devices into meaningful groups.

With Teams, you can:

- Assign a policy to control backup and protection settings for a group of devices.
- Assign a repository where the team will make backups.
- Filter the information by a team so you can see information about the devices that are used in the same area of your business, for example, you could have a team that shows all the devices used for marketing.

We'll show you how it works.[Create your own team](him) [Assign devices](and then you can) [Visualize the information](on the devices on that computer.)

Create a Team

To create a team:

1. Click on**Inventory**.

2. Click**Create Team**(bottom left corner of the Inventory screen).

3. Enter a name for the new team.

4. Ignore the Assign a Policy and Assign a Repository settings for now. You'll return to them after you've created a Policy and repository.

5. Click Save Computer.

Assign a device to a team

Once you've set up your teams, you can use them to organize your discovered devices:

1. Hover over a device in the list of devices.

2. Click on the radio button on the device (...).

3. Click Assign Team.

4. Assign the device to a team in the list.

5. Click Assign.

The page will automatically refresh and the device will be assigned to your selected team. You can now use Inventory to view information about all devices, unassigned devices, or devices on each of your computers.

View a Team's devices

When you have your devices organized into computers, you can filter the inventory so that it only shows information about the devices on a particular computer.

1. Click Inventory.

2. In the Teams section, click:

- **All devices** to display information about all devices on all devices
- **Unassigned** to display information only for those devices that are not yet assigned to a team
- **** to display information about devices on a specific team. Select multiple devices by holding down the CTRL key and clicking on the computers.

Install Repository

You need to set up a repository to which your devices will be backed up.

A repository is a storage area that can be installed on a server on your premises or on a remote server in a data center. Securely stores backup data from your activated devices.

Note: Private Cloud Vault software is available for Windows Server 2019 64-bit.

Download and install the Private Cloud Vault Package - Windows

To register a repository, you will need to have the email address and password of an Aranda Datasafe user account with the role of administrator or security officer.

To download and install the Private Cloud Vault package:

1. Click Repository.

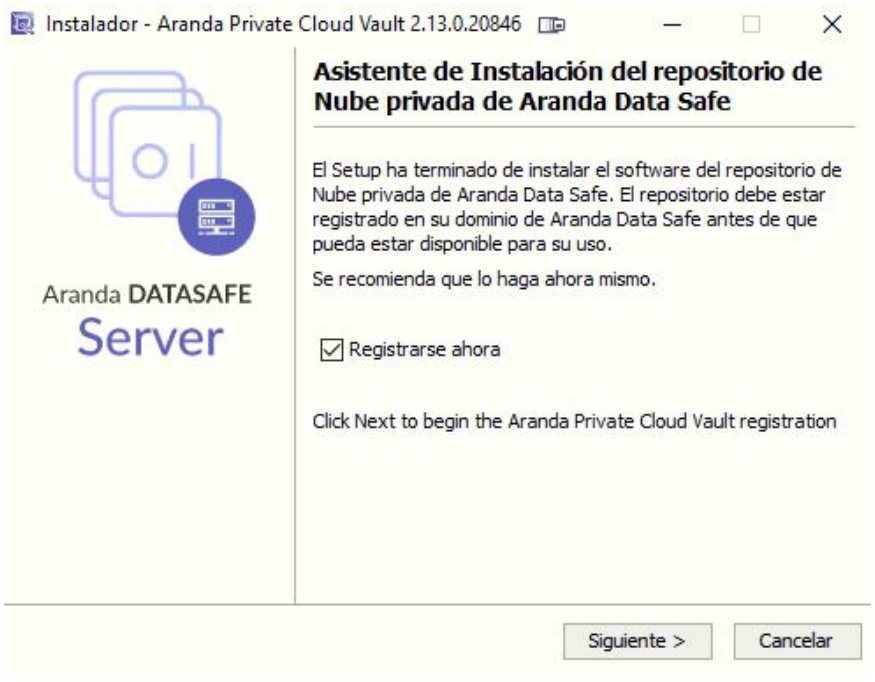
2. Click Download Private Cloud Vault.

3. When the Private Cloud Vault package is downloaded, search for it on your computer and copy it to your server.

4. On the server, install the Private Cloud Vault software. You can install it in the default location or choose another location if you prefer.

Follow the steps in the installation wizard.

When you have installed the software, make sure that**Register Now** is checked and then click**Next**.



5. Enter the registration details:

-

Field	Description
Domain	The name of your Aranda Datasafe tenant. This is usually the name of your organization and is the first part of your Aranda Datasafe address.
Username	Enter the email address of an Aranda Datasafe account that has the role of Administrator or Security Officer. Only these user accounts have permission to register a repository.
Password	Enter the password for the Aranda Datasafe account.
Hostname / IP	Enter the name or IP address of the server that has the repository software installed. If the server is at an internet address, enter the URL instead.
Port	9000. (You can select the port of your choice, but we recommend using 9000.)
Alias	Enter the name of the repository as it will appear in Aranda Datasafe.

⚠ >**Important:** Discovery agents and protection agents must be able to communicate on port 9000.

6. Click Sign Up and Finish.

Install Active Directory Connector

The Active Directory Connector (AD Connector) is an application that Aranda Datasafe uses to authenticate your user accounts, so that your encrypted data is only available to authorized users.

You must install AD Connector on a domain-joined Windows server that is on-premises in your company.

To download, install, and register the AD Connector software:

1. Click on **Settings**.

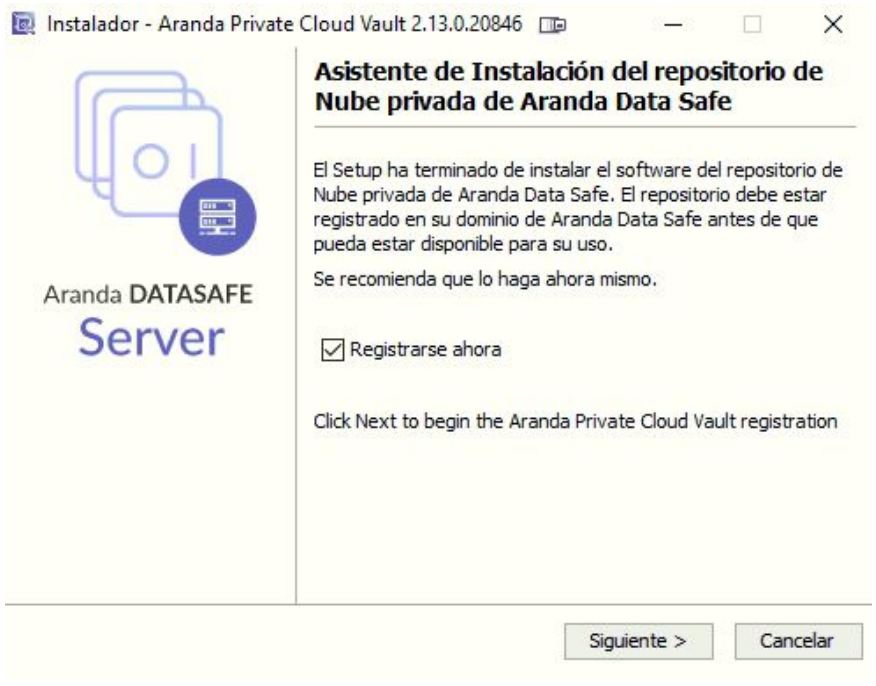
2. Click on **Active Directory**.

3. Click Connect **Ad** to download the adconnector executable file. You will need to copy this file to your local server.

4. Log in to the server on which the AD Connector will run. You must log on through a domain administrator user account that has permission to register a service principal name (SPN) for Kerberos authentication.

5. Copy the adconnector executable file to the server and then run it.

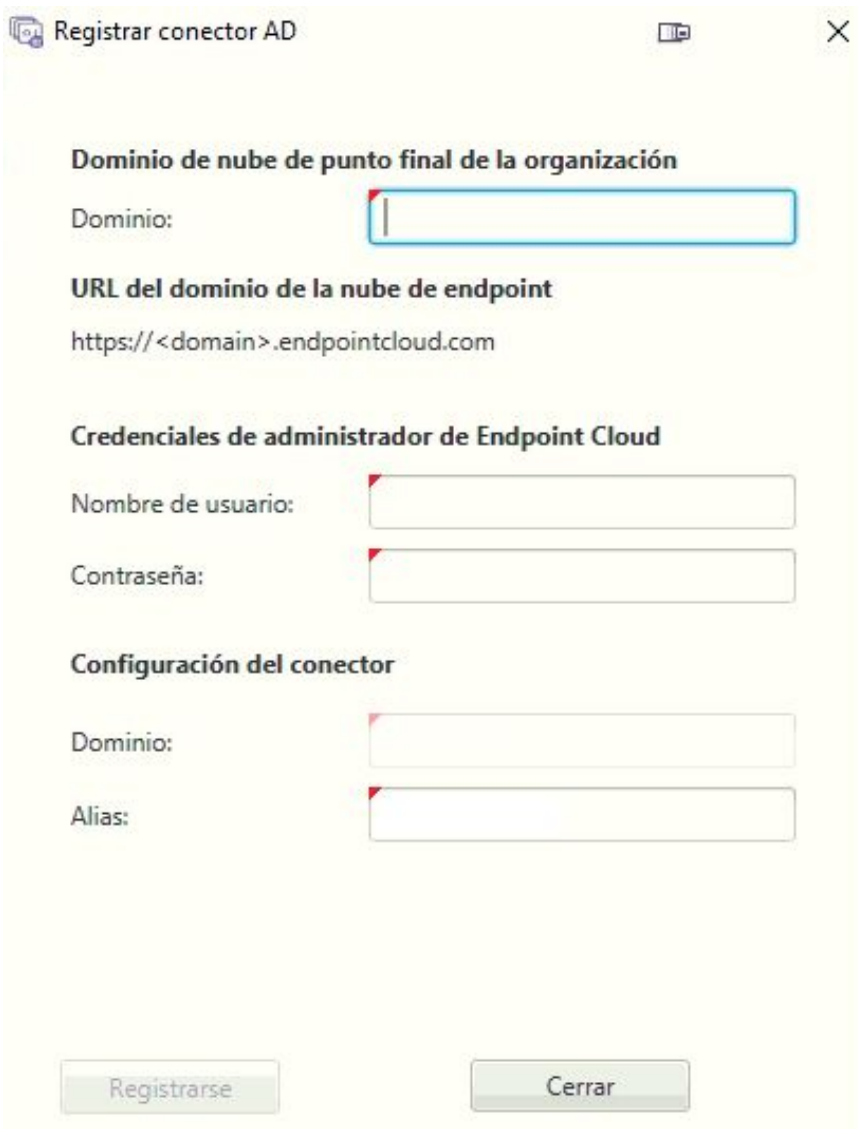
6. Follow the on-screen instructions to install it.



You can install it in any directory (the default location is C drive).

When you complete the installation steps, the files begin to be extracted and installed. When the files are installed, the installation wizard asks if you want to register.

7. Make sure Register is now checked, and then click Next.



8. Enter the registration details:

Field	Description
Domain	The name of your Aranda Datasafe tenant. This is usually the name of your organization and is the first part of your Aranda Datasafe address.
Username	Enter the email address of an Aranda Datasafe account that has the Security Officer role. Only Security Officer user accounts are allowed to register an AD Connector.
Domain	Enter the domain name of the organization
Password	Enter the password for the Aranda Datasafe account.
Alias	Enter the name of the AD connector as it will appear in Aranda Datasafe.

9. . Click **Register** and **finish**.

Create a Policy

A policy is a set of rules that define:

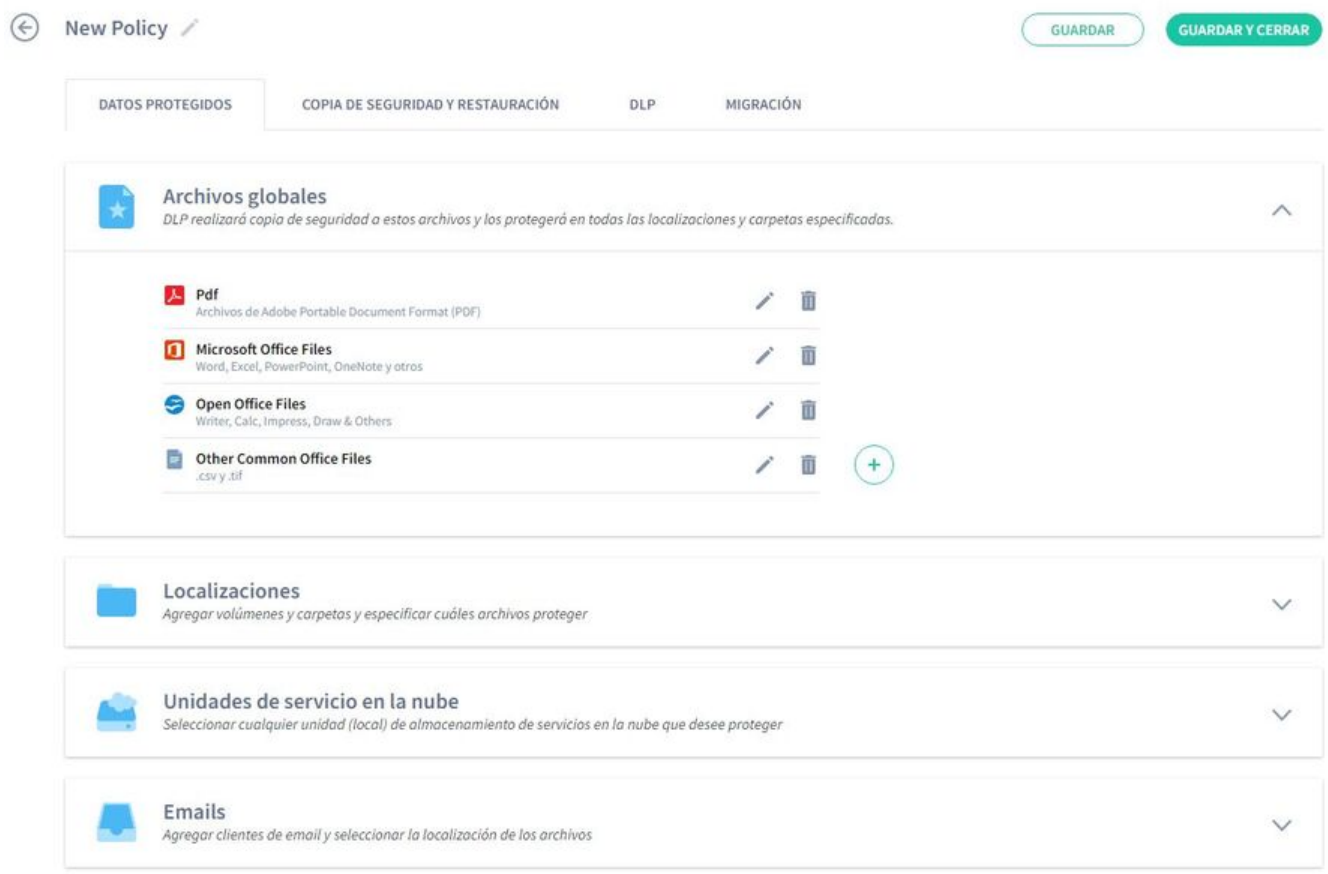
- What data is protected and backed up
- How often backups occur
- If any data loss prevention features are used to protect your data in the event of a device being lost or stolen
- If Windows user profile settings are backed up.

You can create as many policies as you need. You can have one Policy for everyone, or you can have different Policies for each team.

Create a new policy

1. Click Policies.

If you don't have a policy in Aranda Datasafe, click Add a Policy. Aranda Datasafe creates a new Policy and opens it, ready for you to define its configuration.



2. Enter a name to the Policy. Click the edit icon next to the default name, and then enter the new name.

Their new Policy has default settings, and many Aranda Datasafe administrators find these settings to be suitable for their needs. If you have different requirements, you can change the settings in the following sections:

Field	Description
Protected Data	It is used to define what data is selected for protection.
Backup & Restore	It is used to choose how often backups are performed.
DLP	It is used to choose data loss prevention measures for policy.
Migration	It is used to choose whether to back up settings related to Windows user profiles.

Visualize the choices you can make in the sections Protected data, Backup and restore , DLP and Migration.

Protected Data

Use the Protected Data settings to choose which files will be protected and backed up (according to the rules defined in the policy). The policy settings define:

- What data is backed up and protected
- Whether encryption is applied to files on the local device.
- Whether access to the data can be automatically revoked.
- Whether protected data can be wiped from a device remotely

Visualize the different sections.

Global Archives

Global files are collections of file types. For example, there is a collection of Microsoft Office files, for files saved in Word, Excel, PowerPoint, etc. By default, Aranda Datasafe will back up these 'global' files, regardless of where they are stored on devices using the policy.

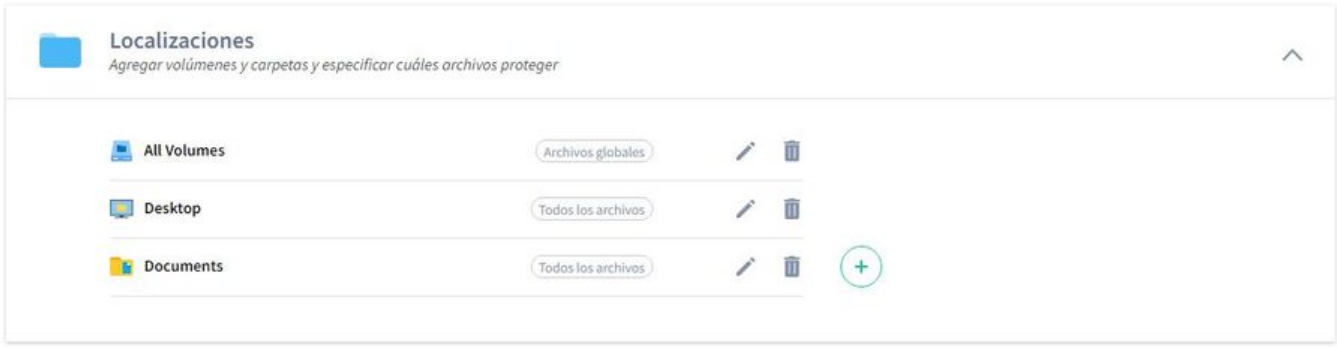
You can use the Global Files settings to:

- Add or remove file types from different collections
- Create a new collection for different file types. For example, you might want to create a new collection that contains the file types for your proprietary software.

Locations

You can configure Aranda Datasafe to back up and protect files in specific locations on a computer (local drives only, by default). Some common locations are included by default, including All Volumes, Desktop, and Documents, and you can add other locations if needed.

For each location, you can choose which files will be backed up and protected: all files, only global files, or a set of files that you choose manually.



Cloud Drives

The Cloud Drives section works the same way as Locations, except it applies to cloud storage locations, such as One Drive.

Choose the cloud drive you want Aranda Datasafe to back up and protect, and then choose to include all files, global files, and/or a custom file selection.

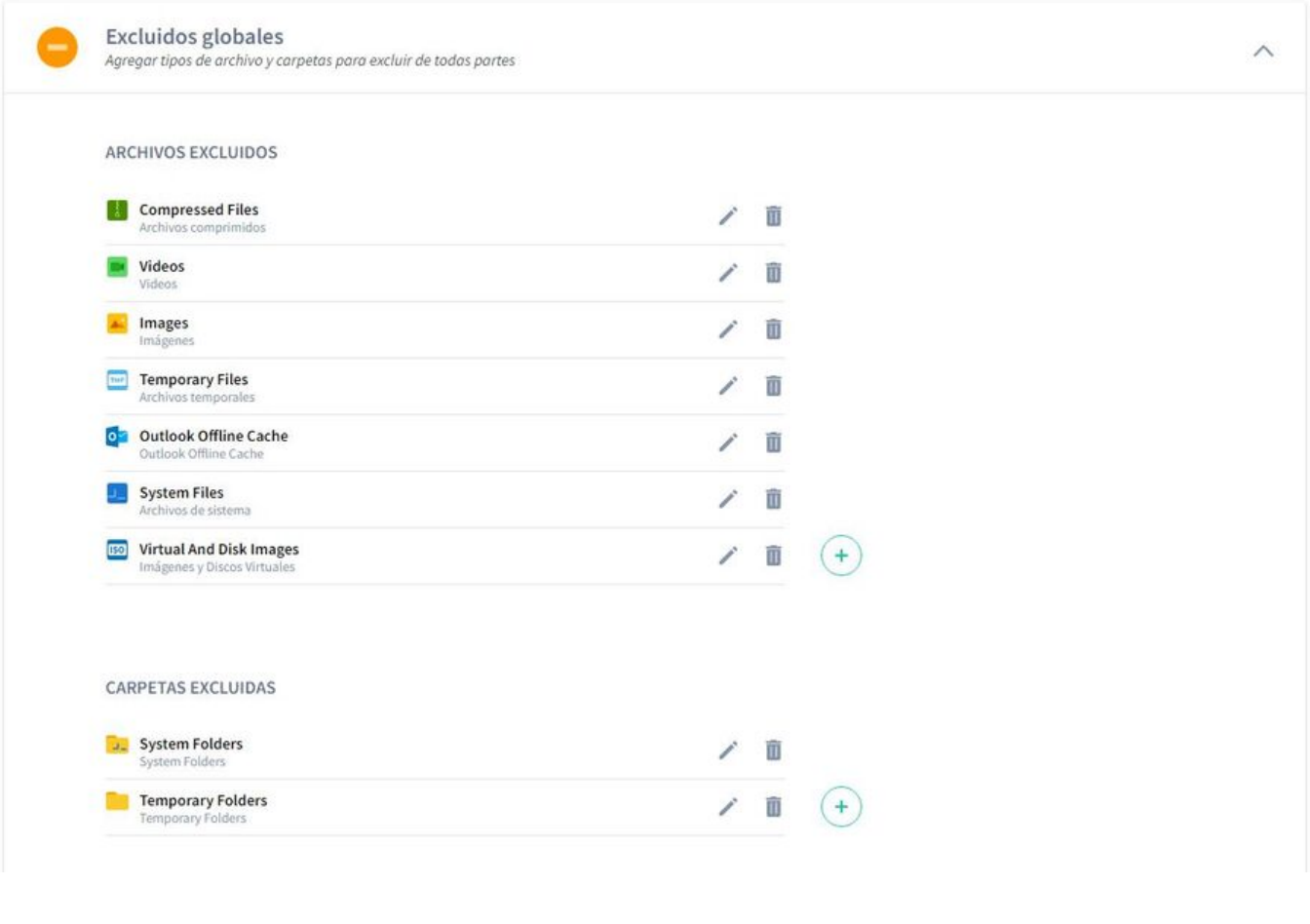
Emails

Use the Emails section to configure Aranda Datasafe to back up and protect your email client files. For example, you can add Microsoft Outlook as an email client and then configure Aranda Datasafe to back up and protect all Outlook PST files or only those PST files that are active in the Outlook profile.

Global Exclusions

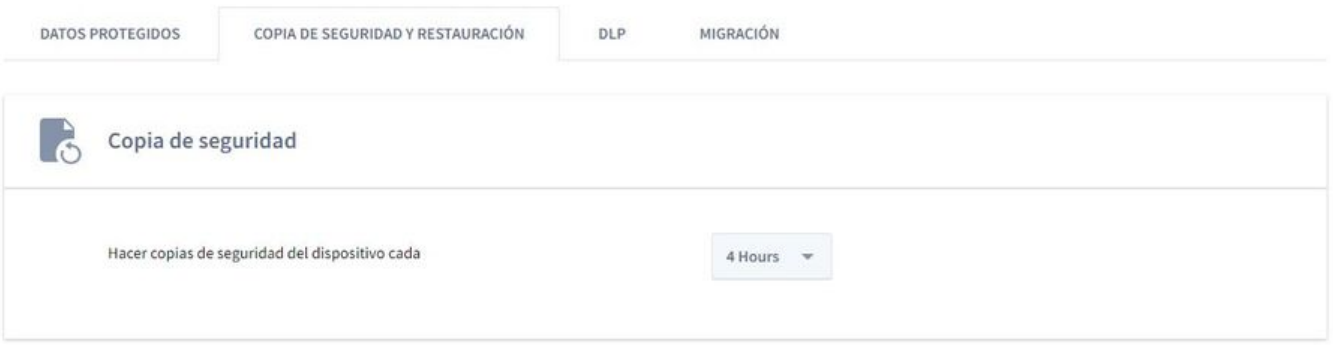
Use the Global exclusions section to specify which types of files and folders should not be backed up or protected. Note that if a folder or file type is included in

Global Files and Global Excluded Files, it will not be backed up or protected (global excluded files take precedence over global files).



Backup & Restore

Use the Backup and Restore tab to set the schedule for backing up devices (that use the policy) on a regular basis.



DLP

The Data Loss Prevention (DLP) tab is where you control settings to protect data locally on devices. These settings are designed to protect your data when a device (that uses this policy) is lost or stolen.

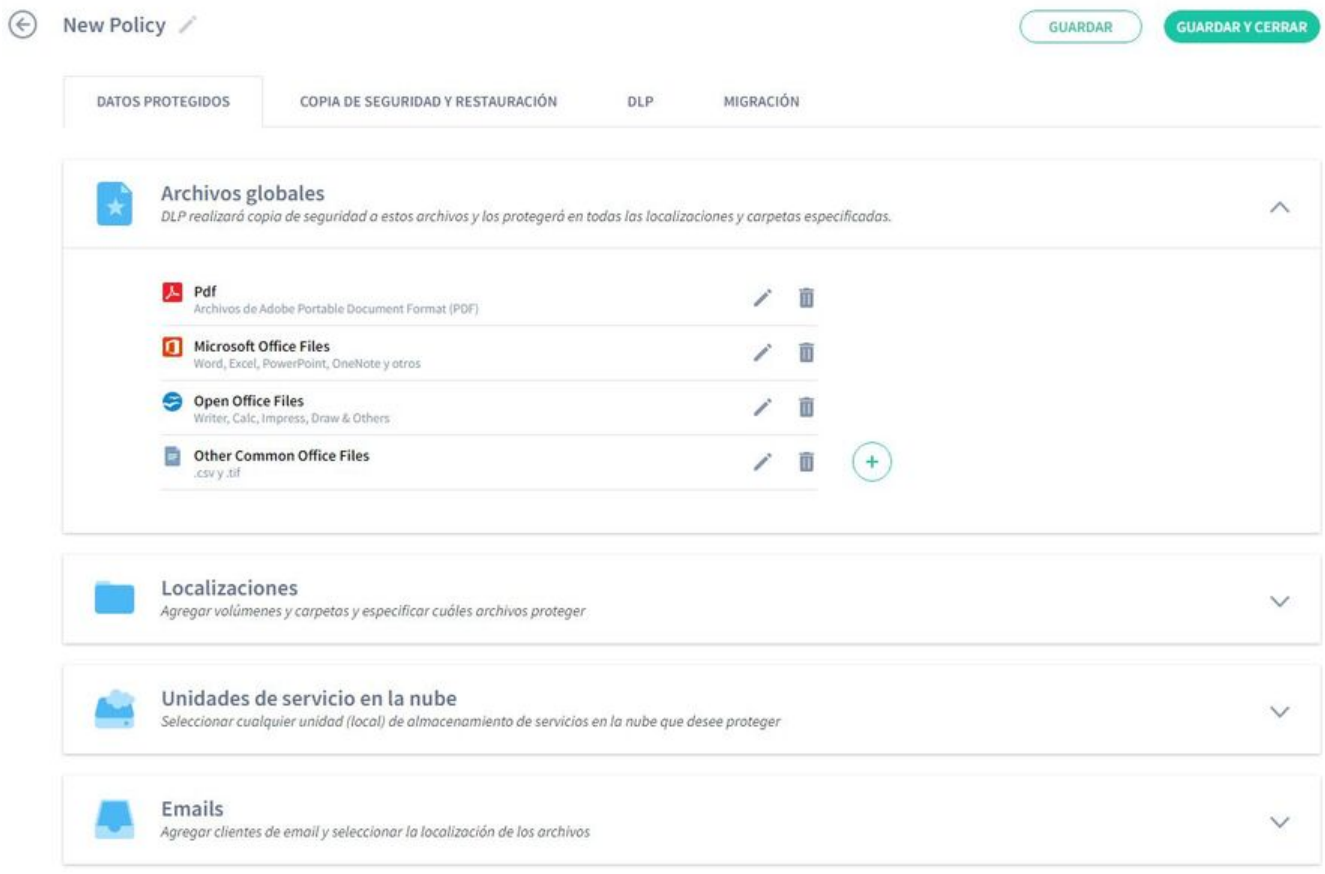
You can choose:

1. Enable local file encryption on the machine. This works by loading a user encryption certificate onto the device. Files can only be accessed if the certificate is available.
2. Prevent access to files if the device does not connect to Aranda Datasafe within a set period of time. The agent automatically revokes the user's encryption certificate, so the files cannot be accessed.
3. Use geolocation to find the last known location of the device.

Migration

Use the Migration settings to control whether Aranda Datasafe backs up Windows user profile settings. This type of data includes accessibility settings, mouse and keyboard settings, favorites, and many other user-specific settings.

You can enable or disable migration as needed.



Assign Policies and Repositories to Your Teams

You can assign a policy and repository to each of your teams. These tell Aranda Datasafe which devices should be backed up and protected, how often backups should be made, and where data should be stored.

To assign a policy and repository, you must edit the team.

1. Click on **Inventory**.

2. In the **Teams** bar, hover over the team to which you are going to assign a repository and/or Policy.

3. Click on the Team radio button (...).

4. Click **Edit**.

5. Choose a policy from the list.

6. Choose a repository from the list.

7. Click Save Computer.

The team is now associated with the policy and repository you selected. Each device assigned to that team will be backed up and protected according to the details of the selected Policy. The data from the team's devices will be encrypted and stored in the selected repository.

Activate Devices

Once you've set up your teams, repositories, and policies, you can **activate** your devices.

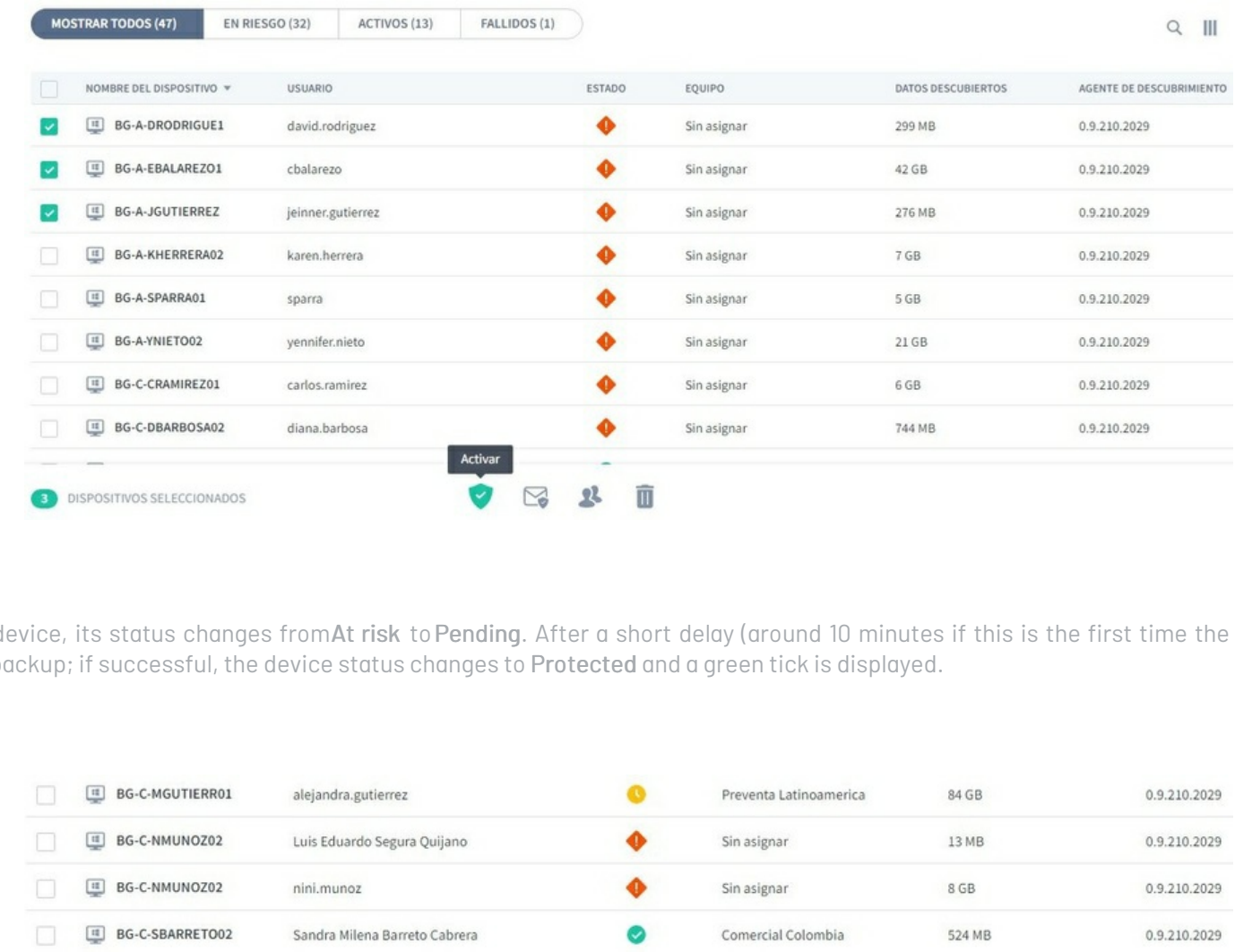
When you activate a device, you create a request for that device to be protected and backed up. If the activation request is successful, the device will be protected **when the next backup is scheduled** (as defined in the Policy settings).

To activate a device:

Click on **Inventory**. Find the device you want to activate in the list of devices.

To activate a single device, you can click on its radio button (...) and then click on **Activate**.

To activate multiple devices, select the checkboxes for the devices you want to activate. Then click on the **Activate** icon in the pop-up bar at the bottom.



When you activate a device, its status changes from **At risk** to **Pending**. After a short delay (around 10 minutes if this is the first time the device is activated), the device will perform a backup; if successful, the device status changes to **Protected** and a green tick is displayed.

If the device can't be protected, a red shield icon is displayed. You will need to investigate why activation failed. It may be because the user is not signed in to the device or there was a connection-related issue.

Backup

When you have activated devices in Aranda Datasafe, your data is automatically backed up:

- Approximately 10 minutes after initial activation or after the agent is started
- Regularly, in accordance with the backup schedule (defined in the Policy).

After the initial automatic backup is done, you can also back up a device manually. The backup is initiated from Aranda Datasafe or by using the Protection Agent locally on the device.

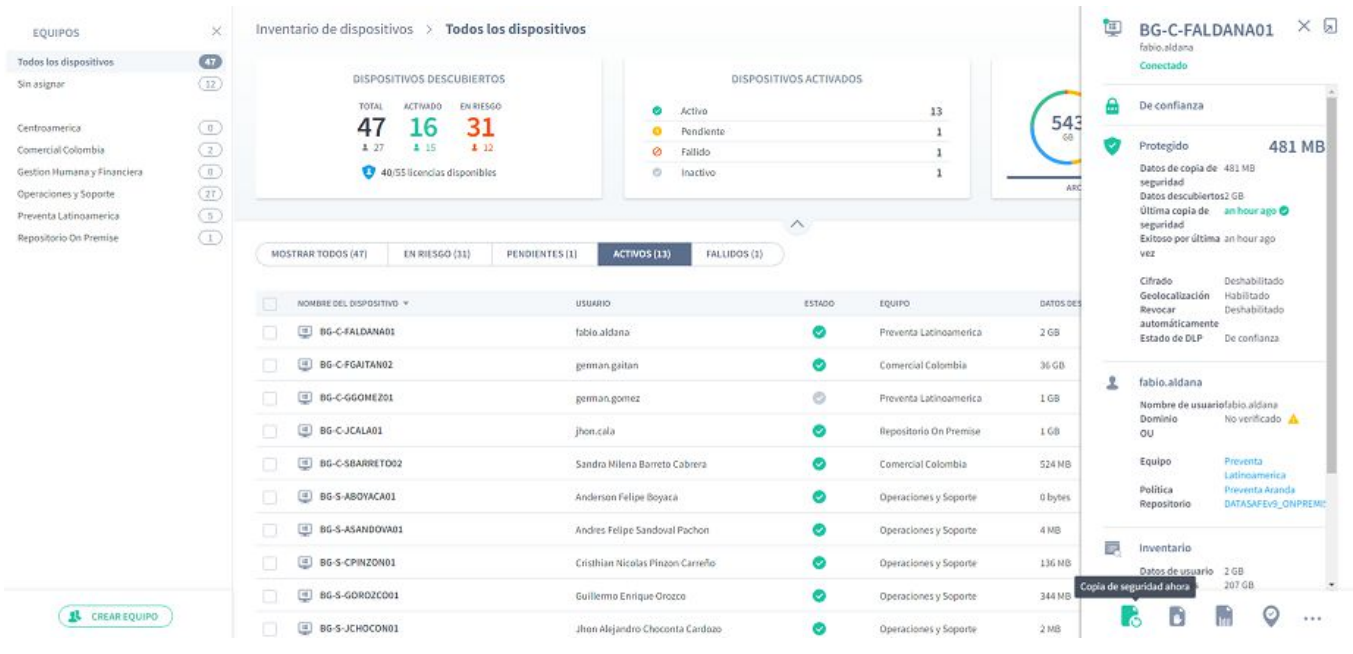
In this step, you will learn how to start a backup from Aranda Datasafe and then you will see detailed information about the backup.

1. Click Inventory.

2. In the list of devices, click on the device you want to backup. Their details appear in a slide-out panel.

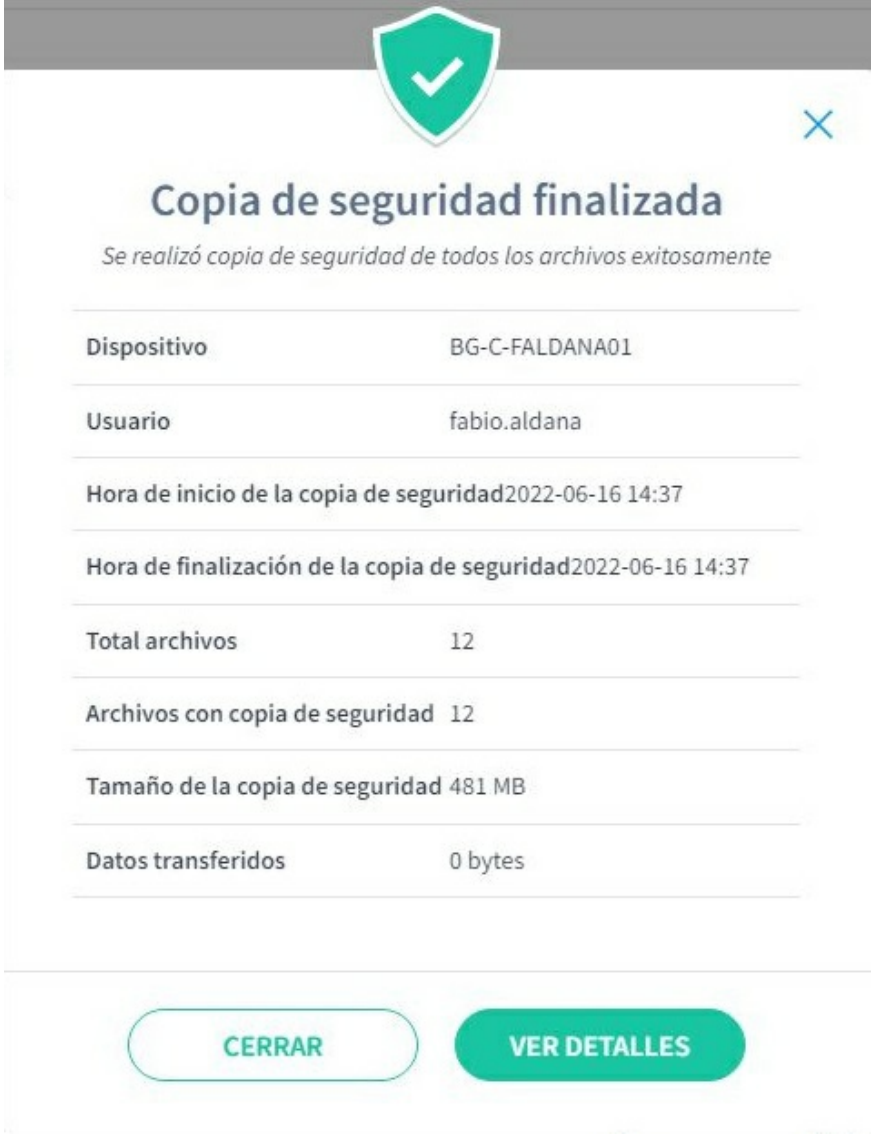
3. Click the Back Up Now icon at the bottom of the slider panel.

A confirmation message appears at the bottom of the screen to let you know that the backup request was successful.



The Protection Agent software (on the user's device) uses deduplication to ensure that only single data is backed up to the repository. The amount of time it takes to back up a device will vary, depending on the amount of data that needs to be indexed and backed up.

4. In the sliding panel, click the link next to the Last Backup entry to display a summary of the backup.



5. For more detailed information about the backup, click View Details. You can then view the details of the backup, the device, the files that could not be backed up, and the error logs.

Restore to Device

Aranda Datasafe stores backups of protected data on your activated devices. If the data is accidentally deleted on the device, you can restore it by downloading it from Aranda Datasafe. You can also restore backups from an old device to a new device.

To **restore** files on a device:

1. Log in to the device that will receive the backup of the data from Aranda Datasafe.

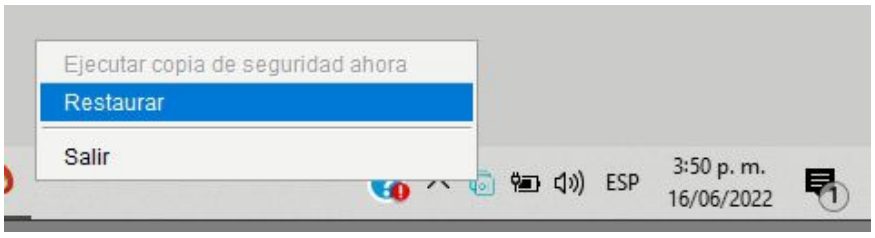
2. If your device already has Discovery Agent installed, ignore steps 2 and 3 and continue from step 4.

3. If you need to restore data to a new device or a device that has not been protected by Aranda Datasafe before, you need to install Discovery Agent. Continue from step 2.

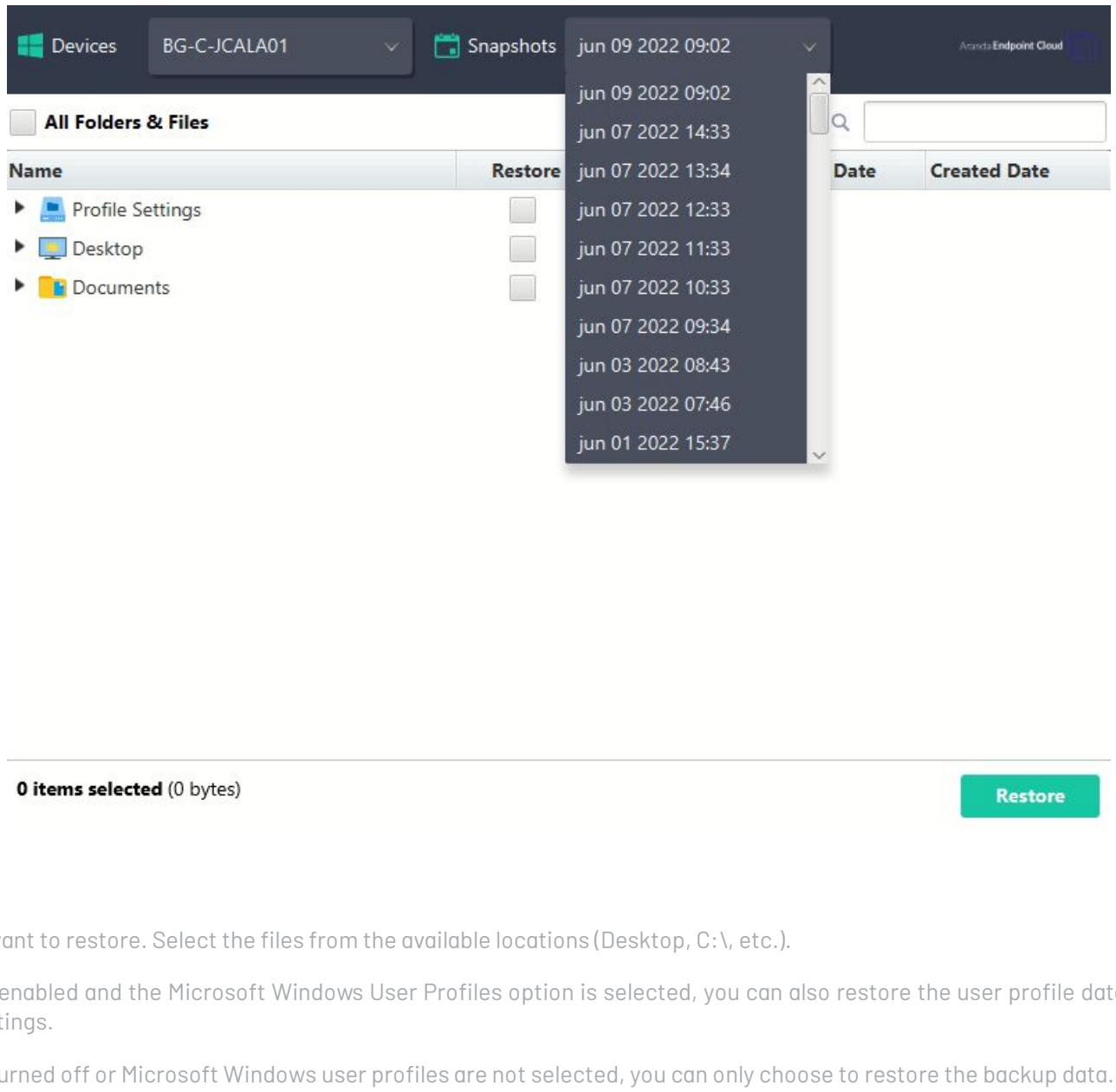
4. Install Discovery Agent on the device, so that Aranda Datasafe can detect it.

5. In Aranda Datasafe, activate the new device.

6. On the Windows taskbar, right-click the Protection Agent icon and select Restore.



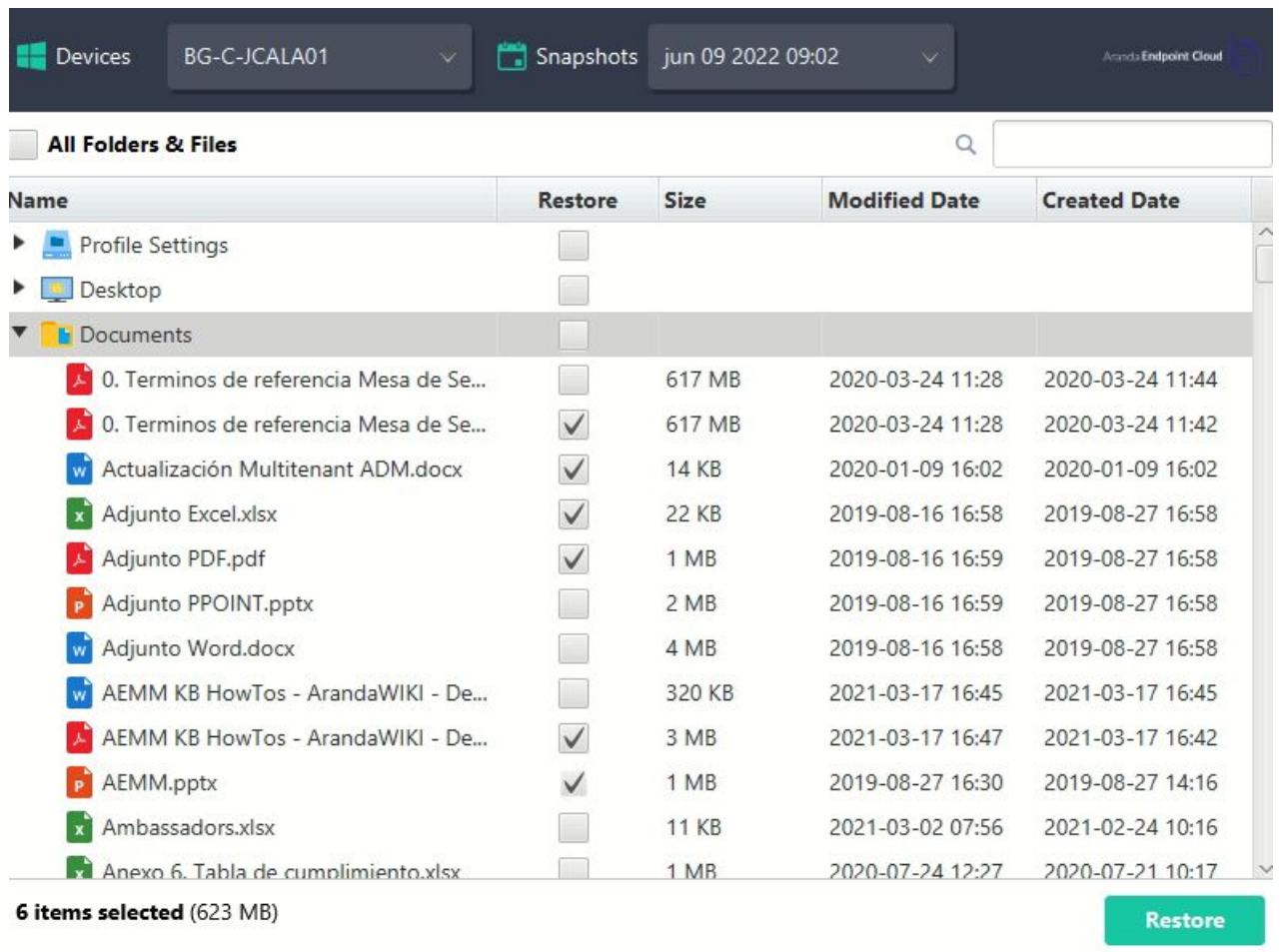
7. At the top of the Datasafe Aranda Agent, choose the device that contained the data you want to restore. Then, choose the appropriate snapshot. A snapshot is a record of a device's data at a specific point in time, and you can choose from any of the times shown in the list.



8. Choose which files you want to restore. Select the files from the available locations (Desktop, C:\, etc.).

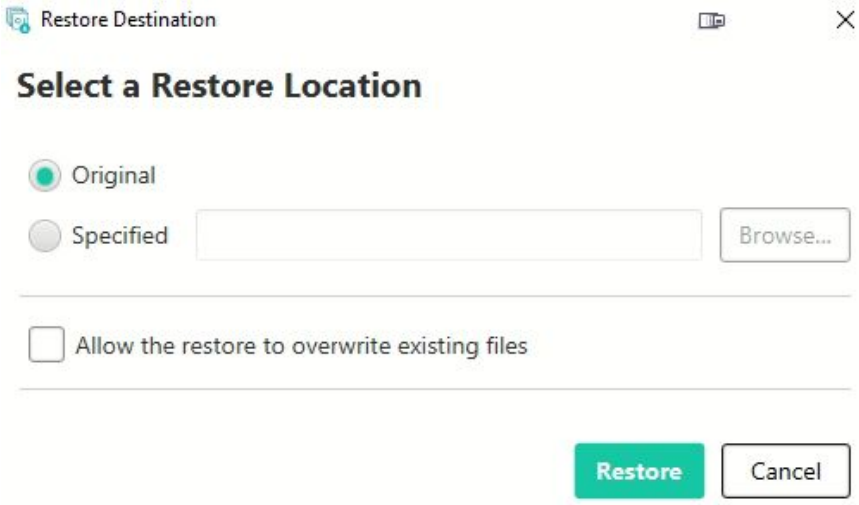
If the policy has migration enabled and the Microsoft Windows User Profiles option is selected, you can also restore the user profile data. Select the **Profile Settings** option to restore these settings.

If the migration feature is turned off or Microsoft Windows user profiles are not selected, you can only choose to restore the backup data.



9. Select **Restore**.

10. . Choose the location for the restore files. This is where they will be restored to your new device. If you choose **Original**, the files will be recovered to the same location they had on the previous device. Or you can choose a different **specified** location if you prefer.



Select **Restore**.

The selected data is restored from the repository to your device. If you've chosen desktop files, you'll see them appear on the desktop.

If you are restoring backup data and user profile settings, the restore will be completed in two separate phases.

Data Loss Prevention

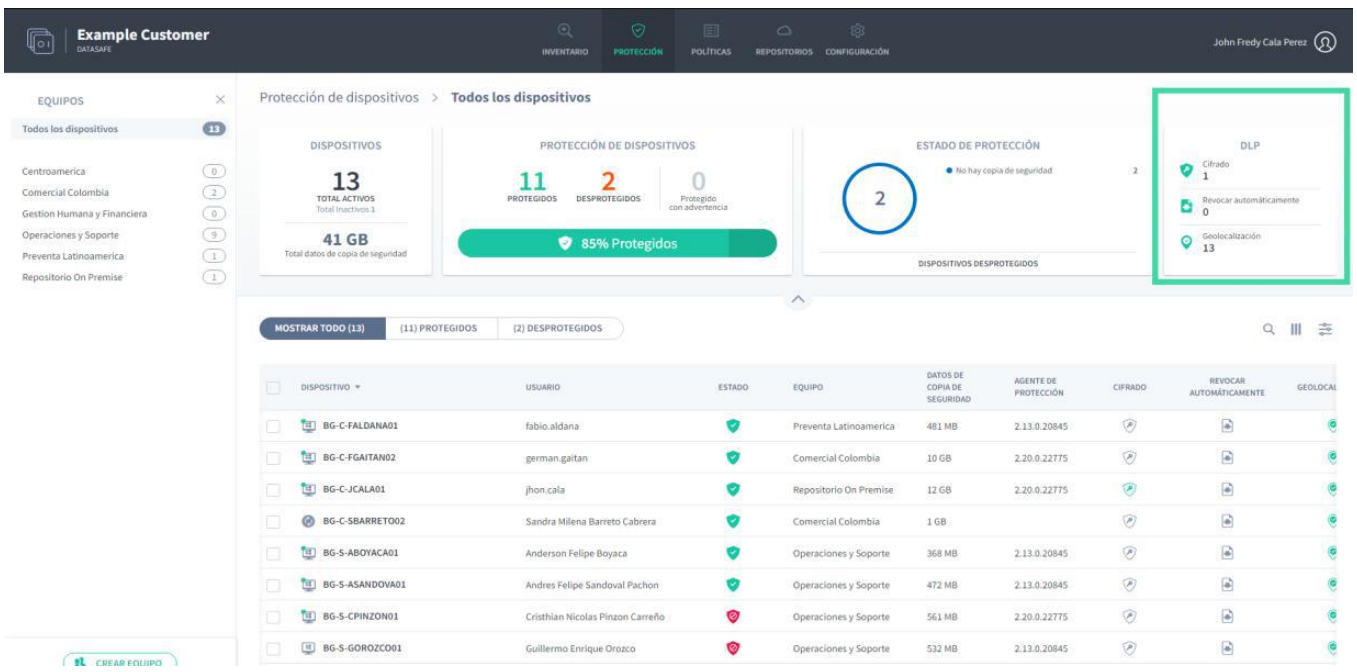
Aranda Datasafe has data loss prevention (DLP) features that mitigate your risk in the event of a lost or stolen protected device. Features are enabled in the Policy [see Create a Policy](#) and they can protect their data with:

- Encryption of local data on your devices
- Automatic prevention of access to protected data if a device does not connect within a specific number of days (automatic revocation)
- Provide you with the last known location of the device (geolocation)
- Allow you to remotely wipe backed up data on a device

Let's look at how you can view and use DLP features.

View DLP status

You can view the status of DLP on the Protection page. Shows the number of devices that have local encryption, auto-revocation, and geolocation features enabled (in the policy).



The DLP status is also displayed in the list of devices at the bottom of the Protection section.

Revoke a device

If a policy has local encryption enabled, each device receives an encryption certificate that is stored locally on each machine. Encrypted data can only be accessed by the registered user if the certificate is in place.

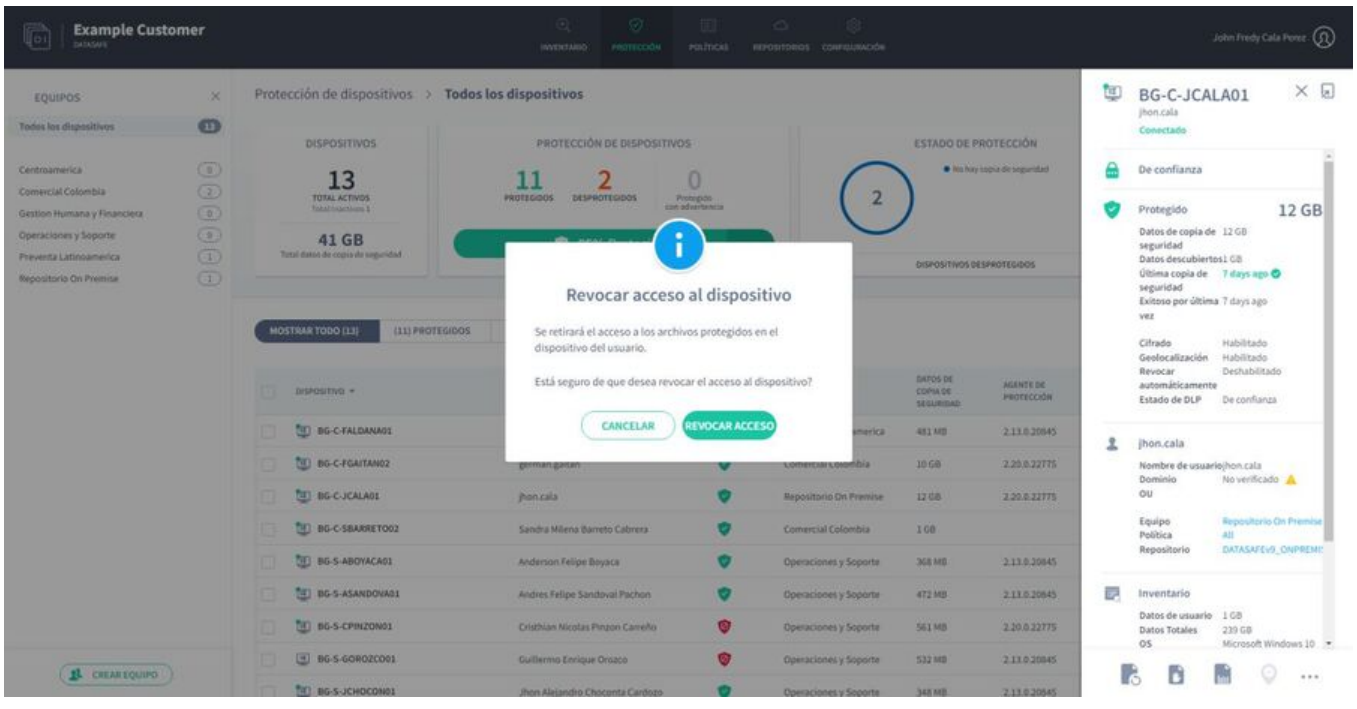
When you revoke a device, you remove the certificate so that the encrypted data cannot be accessed.

1. Click on **Protection**.

2. Click on the device you want to revoke.

3. Click on the **Revoke Device** icon.

4. Click **Revoke** to confirm.



⚐ > Note: If auto-revocation is enabled in a policy, Aranda Datasafe will automatically revoke the certificate of any protected device that does not connect to Aranda Datasafe within a specified number of days. (You can change the automatic revocation time period in the policy settings.)

Erase a device

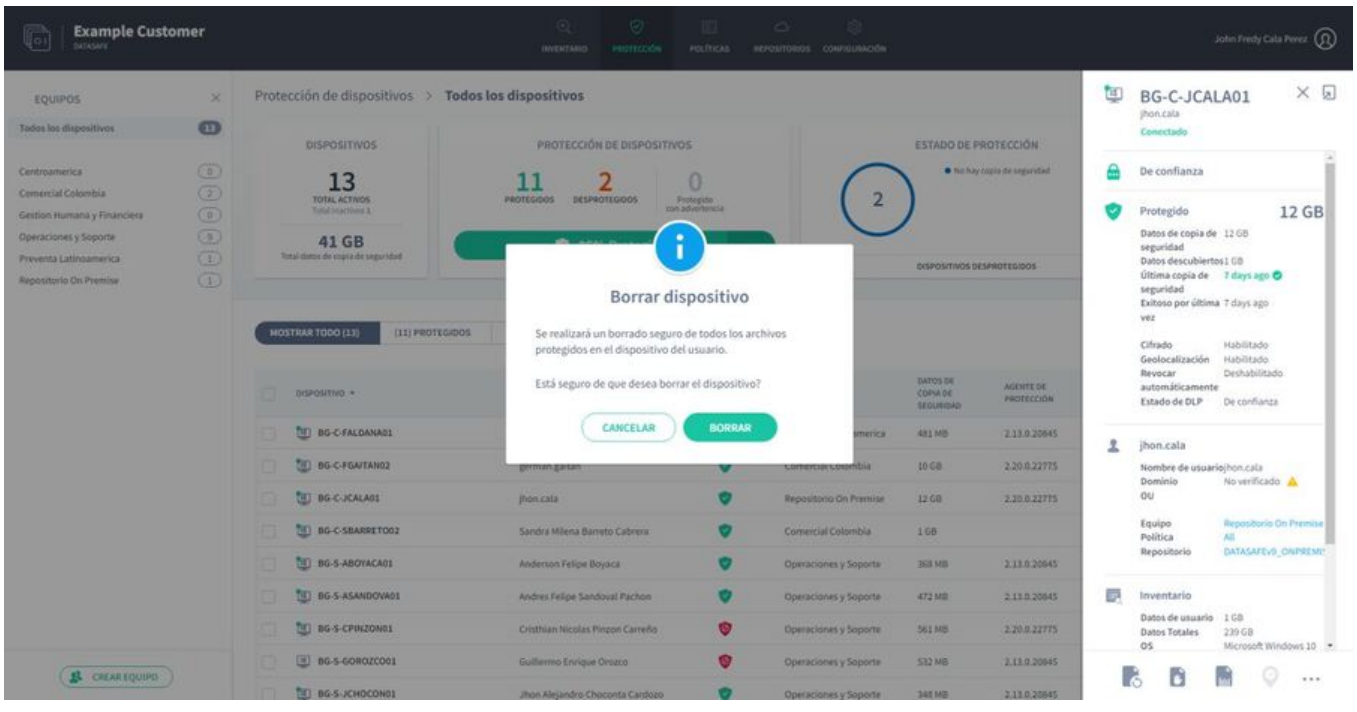
You can remotely wipe the protected files on your devices. With a wipe, the protected files are deleted and Aranda Datasafe also performs a "forensic erase" to remove any traces of the files on the device.

1. Click on **Protection**.

2. Click on the device you want to erase.

3. Click on the **delete** icon.

4. . Click Clear to confirm.



Locate a device

If a policy has geolocation enabled, it can see the last known location of a protected device (the device must have Wi-Fi enabled).

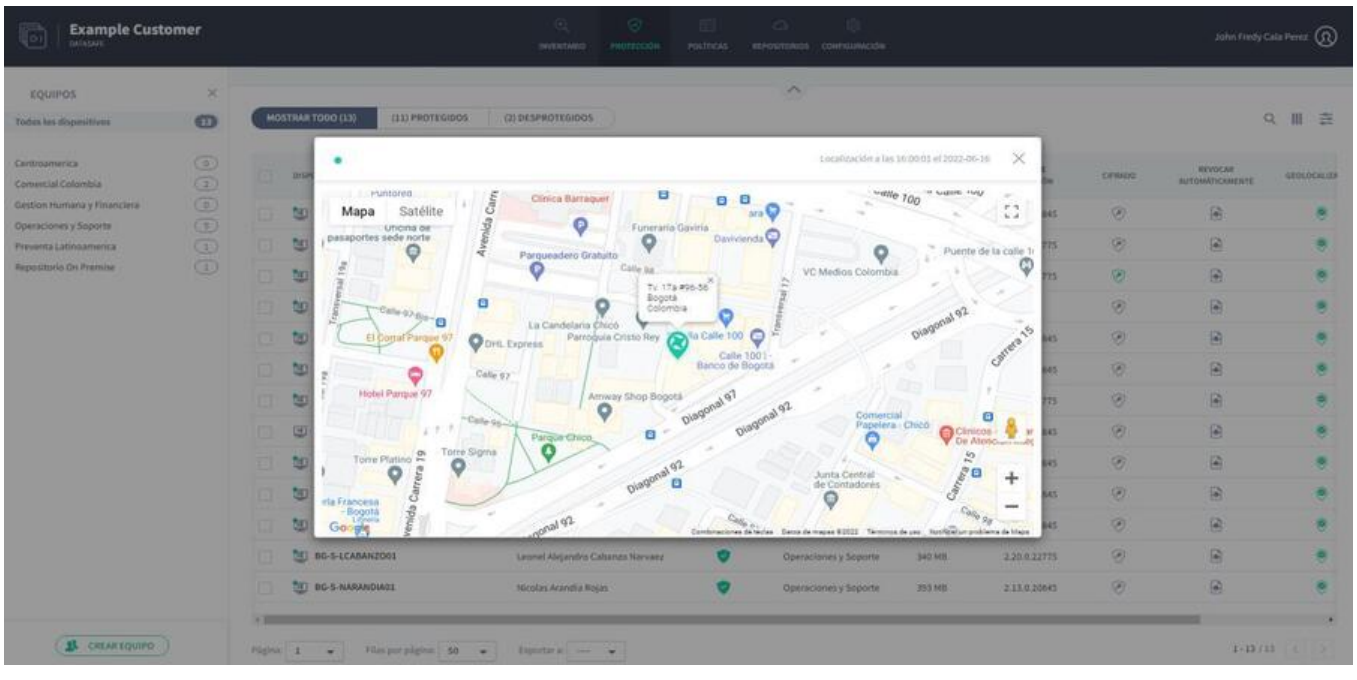
To use geolocation to find a device:

1. Click on **Protection**.

2. Click on the device you want to locate.

3. Click the Geolocate icon.

The last known location is shown on a Google map. You can zoom in, zoom out, and show the satellite view.



Configuration Migration

At some point, you will most likely need to replace one of your protected devices. For example, an older device may need to be upgraded to a newer model, or a protected device may be lost or stolen. To make it easier and faster to set up a new device, Aranda Datasafe has a migration feature.

With the migration feature, you can configure Aranda Datasafe to perform monthly backups of Windows user profile settings on protected devices. Then, when you need to replace a protected device, you can migrate your Aranda Datasafe configuration to the new replacement device.

To use the migration feature, you must enable it in the relevant policies.

Enable user profile migration

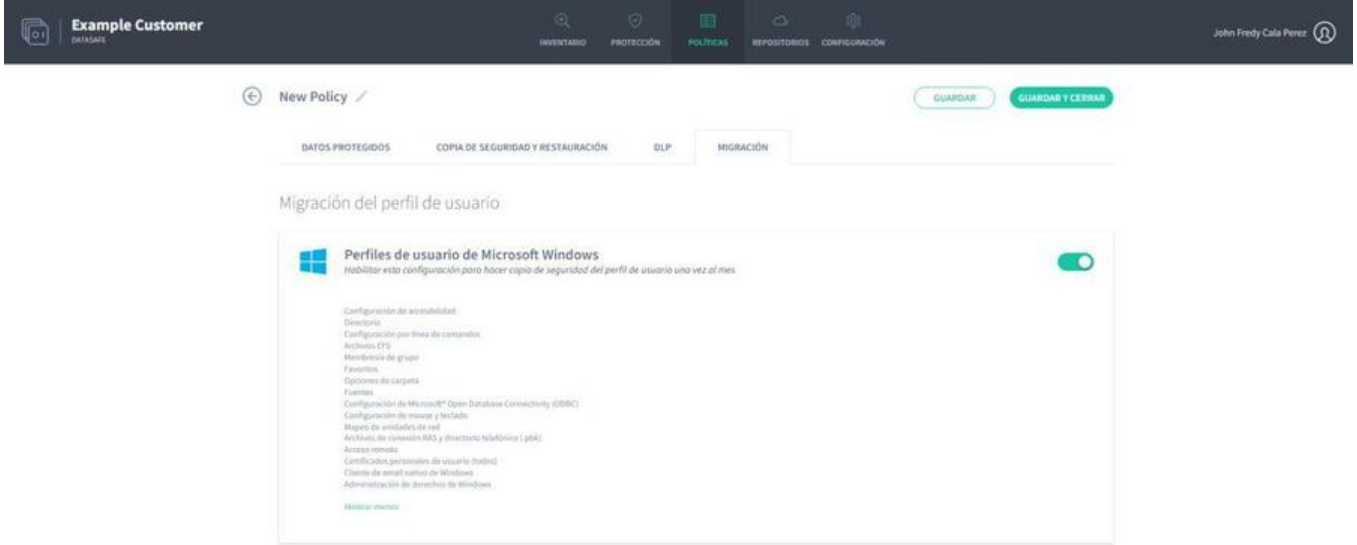
To enable the migration feature of user profile settings:

1. In Aranda Datasafe, click on**Policies**.

2. Edit the Policy associated with the device equipment.

3. Click on**Migration**.

4. Enable profile migration for Microsoft Windows user profiles.



5. Click the **Show More** link to see a complete list of Windows user profile information that will be backed up. It includes taskbar layout, mapped network drives, folder options, email accounts, previously attached pst files, and email signatures.

6. Click **Save & Close**.

User data and profiles will be backed up to the protected devices when the next data backup is made (as scheduled in the policy).

When a backup has been made, you can migrate the settings to a new device.

Migrate settings to a new device

If you have enabled migration in a policy, you can use Restore to transfer Windows user profile data (and backup data) from an old device to a new device (via Aranda Datasafe).

To restore files to a device:

1. Sign in to the new device.

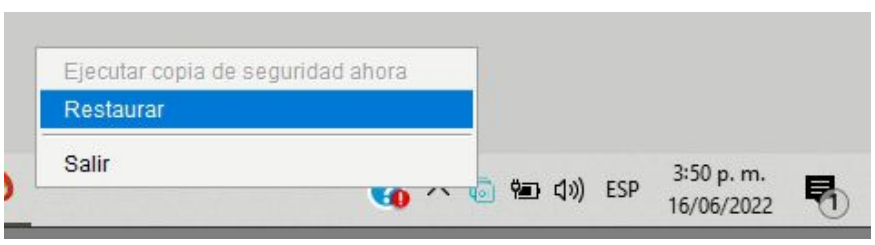
If your device already has Discovery Agent installed, ignore steps 2 and 3 and continue from step 4.

If you need to restore data to a new device or a device that has not been protected by Aranda Datasafe before, you need to install Discovery Agent. Continue from step 2.

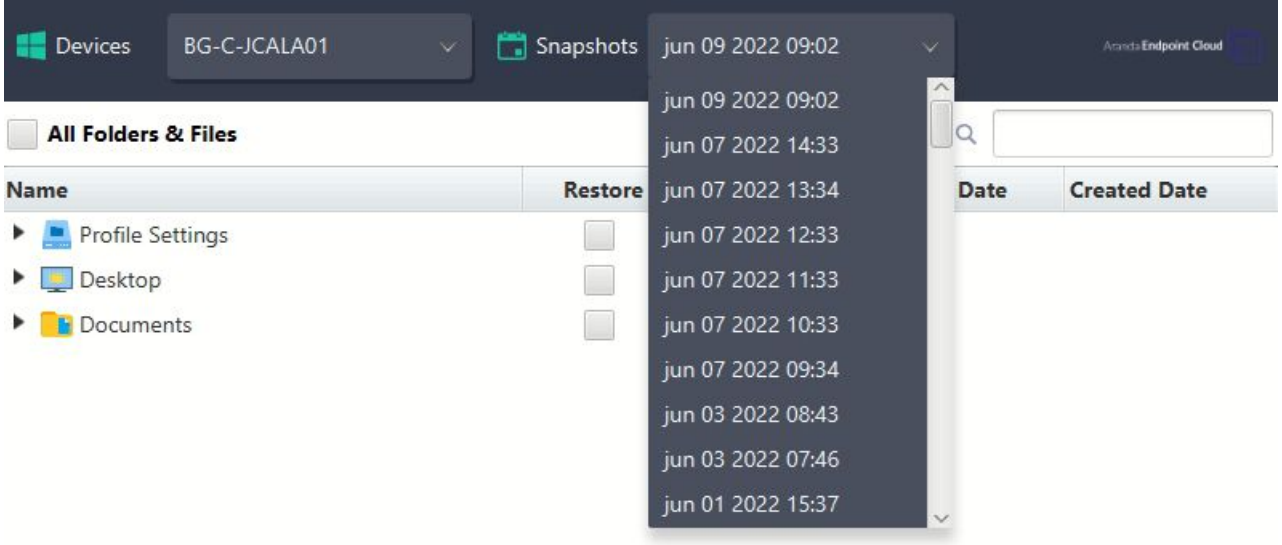
2. Install Discovery Agent on the device, so that Aranda Datasafe can detect it.

3. In Aranda Datasafe, activate the new device.

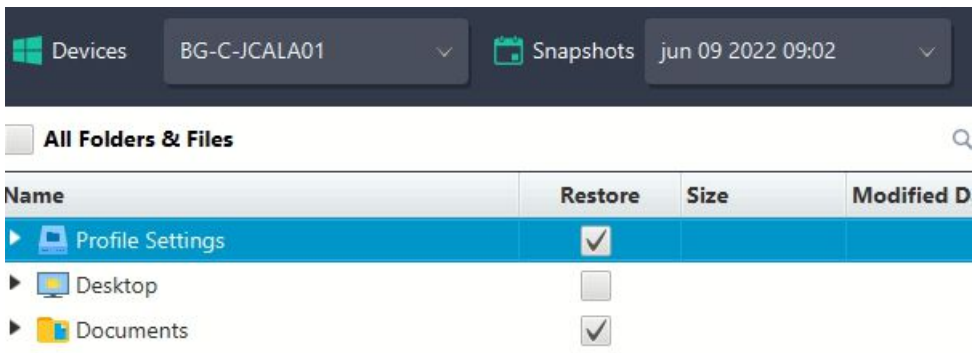
4. In the Windows system tray, right-click the Protection Agent icon and select **Restore**.



5. At the top of the Aranda Datasafe Agent, choose the device and then the snapshot you want to migrate to the new device. The snapshot is a record of a device's data at a specific point in time, and you can choose from any of the times shown in the list.

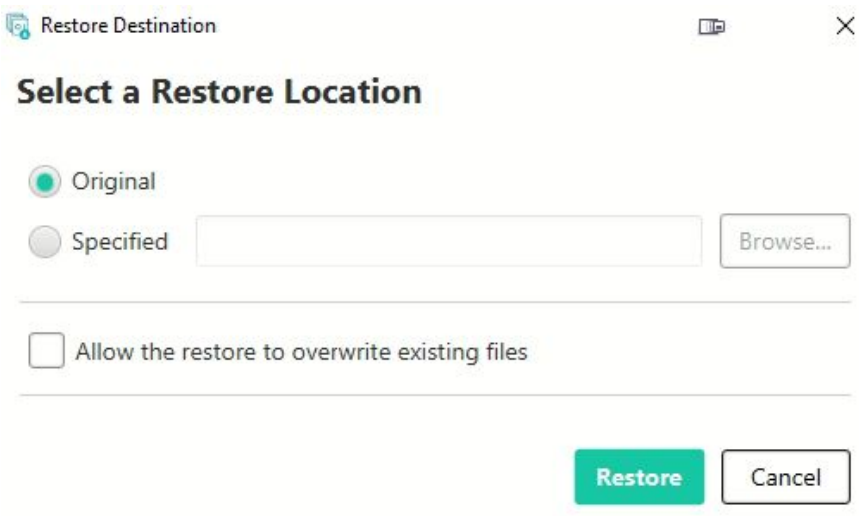


6. Choose which files you want to restore. You can choose**All folders and files**, all desktop files, all documents, or all files on volumes (drives). Alternatively, you can select individual files.



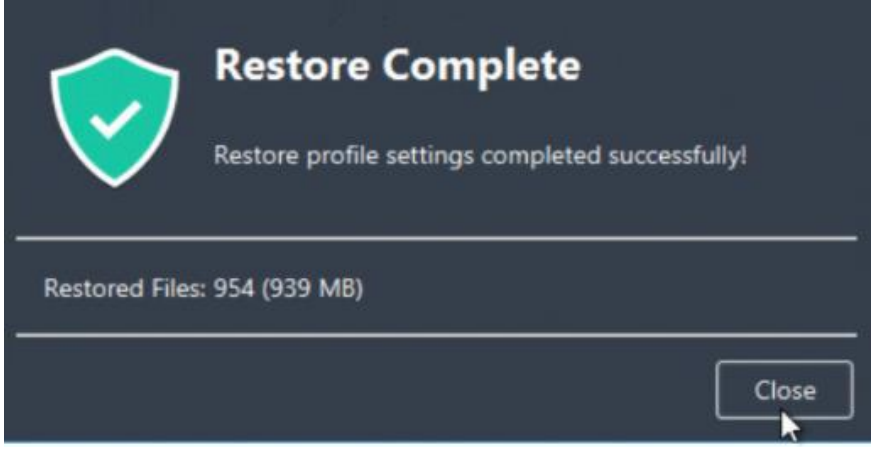
7. Select **Restore**.

8. Choose the location of the migrated files. If you choose**Original**, the files will be uploaded to the same location they had on the previous device. Or you can choose a different **specific** location if you prefer.



9. Select **Restore**.

The selected user data and profile information are downloaded from Aranda Datasafe to your new device. If you've chosen desktop files, you'll see them appear on the desktop.



Discovery and Inventory

Discovery and Inventory

Aranda Datasafe can give you an overview of your devices and data on a global scale. You can use this information to determine what types of data your organization has, what data is at risk, and how much storage space is required to back it up to Aranda Datasafe.

For an overview, install the Discovery Agent app on each of your business devices (but don't install it on your server).

Discovery Agent allows Aranda Datasafe to detect your users' devices automatically.

What is Discovery Agent?

The Discovery Agent is a lightweight, free app that you can deploy to an unlimited number of devices in your organization. It gives you an instant view of your endpoint devices and data, so you can plan your storage and start protecting your devices, all from within Aranda Datasafe.

When you run Discovery Agent, it analyzes your devices and data and creates an inventory. Aranda Datasafe uses inventory to give you a wealth of information about your devices and data, including details of:

- The hardware components that make up the device
- Installed applications, drivers, services, and updates
- Device data, automatically categorized into commercial and non-commercial data
- Activation status. You can see which devices are at risk and which are enabled for protection.

You can access all this information from the Aranda Datasafe Inventory page.

Discovery Agent Installation and Deployment

You can use Aranda Datasafe's Discovery Agent to identify:

- The amount of your company's data that is at risk.
- How much storage space you'll need to back up and protect your devices.

Discovery Agent is free and gives you an overview of your devices and data. You need to install it on all the devices that you would like to backup and protect with Aranda Datasafe.

Download Discovery Agent

You can download and install the Discovery Agent on all the devices that you want to be included in the Aranda Datasafe inventory. **Do not install Discovery Agent on**

your on-premises servers or cloud servers.

On a device you want to be discovered:

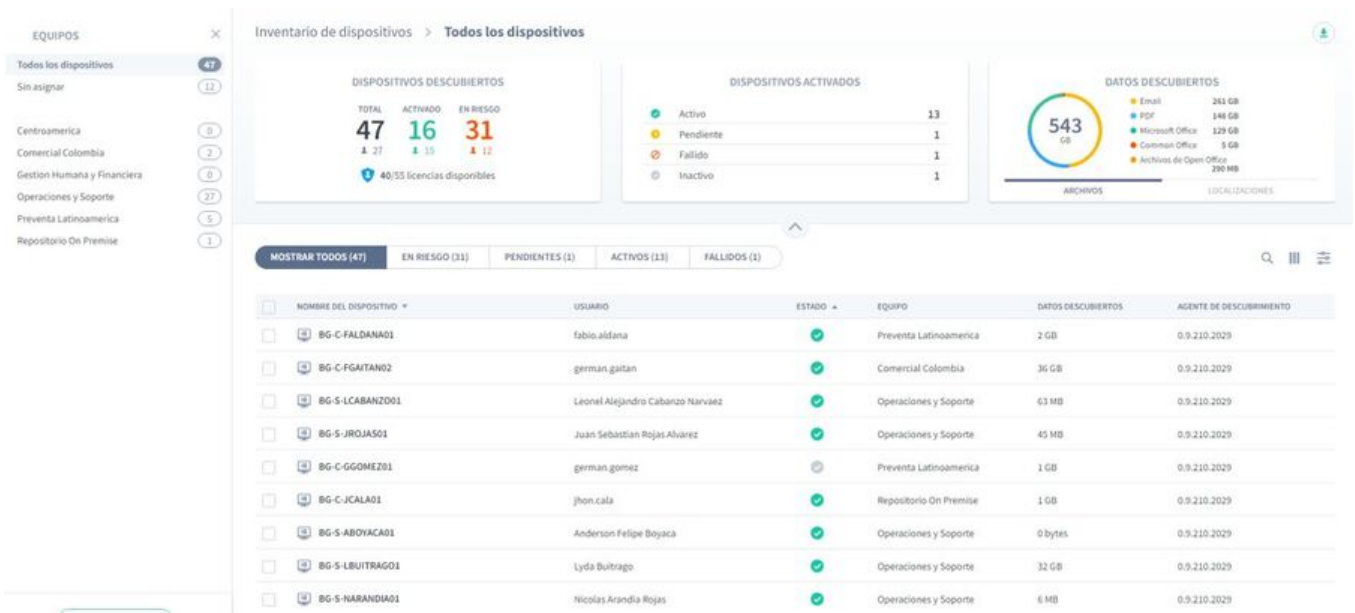
1. Log in to Aranda Datasafe as an administrator.

If Aranda Datasafe has not yet discovered any devices, the Inventory page does not contain information about the device and advises you to download the discovery agent.

If Aranda Datasafe has discovered devices, the Inventory page displays information about those devices.

2. If Aranda Datasafe has not discovered any devices, click Download Discovery Agent to begin downloading a Discovery Agent that is specific to your Aranda Datasafe Tenant. (The MSI Discovery Agent package is downloaded to your browser.)

If Aranda Datasafe has previously discovered devices, click on the download icon in the top right, above the **Data discovered## panel.** Discovery Agent will begin downloading to your browser.



Install Discovery Agent on your end-user devices

Install the MSI Discovery Agent package on each user device (desktop, laptop, etc.). The discovery agent will perform an inventory of devices and data, and then securely upload the information to Aranda Datasafe.

Prerequisites

- The user's devices must have **Internet access** since Discovery Agent needs to connect to Aranda Datasafe.
- The user's devices must use a **Windows operating system**, Windows 7 or later. A Mac version will be available soon.
- **Firewalls and proxy servers must allow connections**. You may need to whitelist endpointcloud.com and the full path to the Aranda Datasafe tenant URL. Example: https://arandasoftware.endpointcloud.com where **"arandasoftware"** is replaced with your organization's name.

You can install Discovery Agent manually or remotely on each device.

Manual Agent Installation

Discovery Agent can be installed by running the MSI package on each user device.

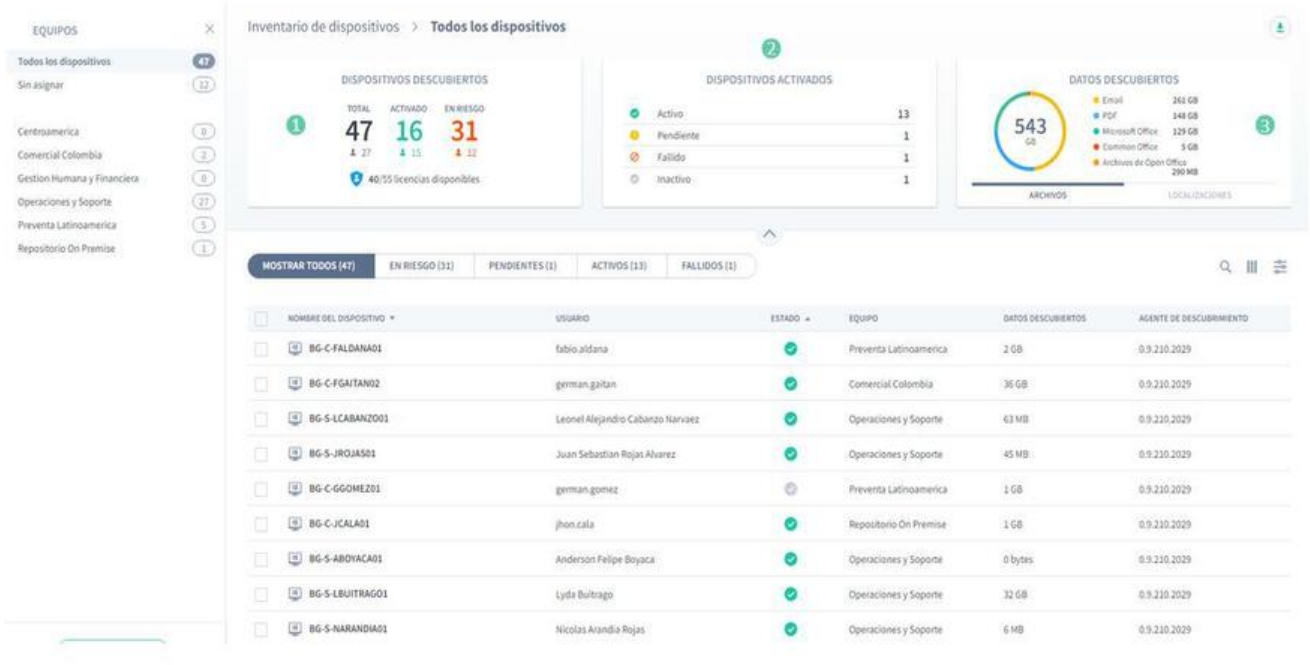
You may want to move the MSI package to a shared folder that can be accessed by all devices. Alternatively, you can put the MSI package on a memory card and transfer it between devices that way.

Remote Agent Installation

You can install the MSI package on devices remotely, using the Active Directory Group Policy feature or a third-party application. For more details, please contact Aranda Support (reportedecasos@arandasoft.com).

Device Inventory

The Inventory page displays information about the devices that Aranda Datasafe has discovered. This information includes details about each device, the amount of data discovered, and the protection status of each device.



Discovered Devices

The Discovered Devices pane provides a summary of the devices that have been discovered.

Field	Description
Total	The total number of devices that have been discovered (activated devices + compromised devices). Below the total number is the number of users. In the image above, Aranda Datasafe has discovered 47 devices and 27 users.
Assets	The number of discovered devices that have been activated. Devices that are activated are either being backed up and protected or are waiting to be backed up and protected. When you first wake a device, its status is set to On, but activation doesn't start until the next backup is made. Below the activated number is the number of users who have activated their devices.
At Risk	The number of discovered devices that have not been activated and therefore are not protected or supported by Aranda Datasafe.
Available Licenses	The number of licenses that are currently in use and the total number of licenses that are available to you.

Activated devices

The Activated Devices pane provides information about the devices that have been activated (configured to be backed up and protected).

Field	Description
Assets	The total number of devices that have been activated and are currently backed up and protected by Aranda Datasafe.
Pending	The number of discovered devices that have been activated but are not yet backed up and protected by Aranda Datasafe. They will be activated when the protection agent is successfully authenticated.
Failed	The number of discovered devices that could not be activated. An activation may fail if the Protection Agent was not downloaded and installed or if the user is not authenticated with Active Directory.
Inactive	The number of discovered devices that have not connected to Aranda Datasafe in the last 30 days.

Data Discovered

The Discovered Data dashboard provides a summary of the types of business data that Aranda Datasafe has encountered on your devices. By default, it displays files with a summary of file types and the amount of storage space required to back up.

If you click Locations, the dashboard provides a summary of the various places where the data is located on your devices. It also provides details of the storage space required to back up each location.

Teams sidebar

On the left side of the Inventory page is the Equipment sidebar. This displays a list of the devices that are configured in Aranda Datasafe (plus All Devices and Unassigned, which are integrated).

If you click a computer, the inventory panes and list are updated so that it only shows information for the devices on the selected computer. You can click All Devices to configure Inventory to display data for each device.

Device List

The bottom section of the Inventory displays the list of devices, which contains a summary of the devices that Aranda Datasafe has discovered.

NOMBRE DEL DISPOSITIVO	USUARIO	ESTADO	EQUIPO	DATOS DESCUBIERTOS	AGENTE DE DESCUBRIMIENTO
BG-C-FALDANA01	fabio.aldana		Preventa Latinoamerica	2 GB	0.9.210.2029
BG-C-FGAITAN02	german.gaitan		Comercial Colombia	36 GB	0.9.210.2029
BG-S-LCABANZO01	Leonel Alejandro Cabanzo Narvaez		Operaciones y Soporte	63 MB	0.9.210.2029
BG-S-JROJAS01	Juan Sebastian Rojas Alvarez		Operaciones y Soporte	45 MB	0.9.210.2029
BG-C-GGOMEZ01	german.gomez		Preventa Latinoamerica	1 GB	0.9.210.2029
BG-C-JCALA01	jhon.cala		Repositorio On Premise	1 GB	0.9.210.2029

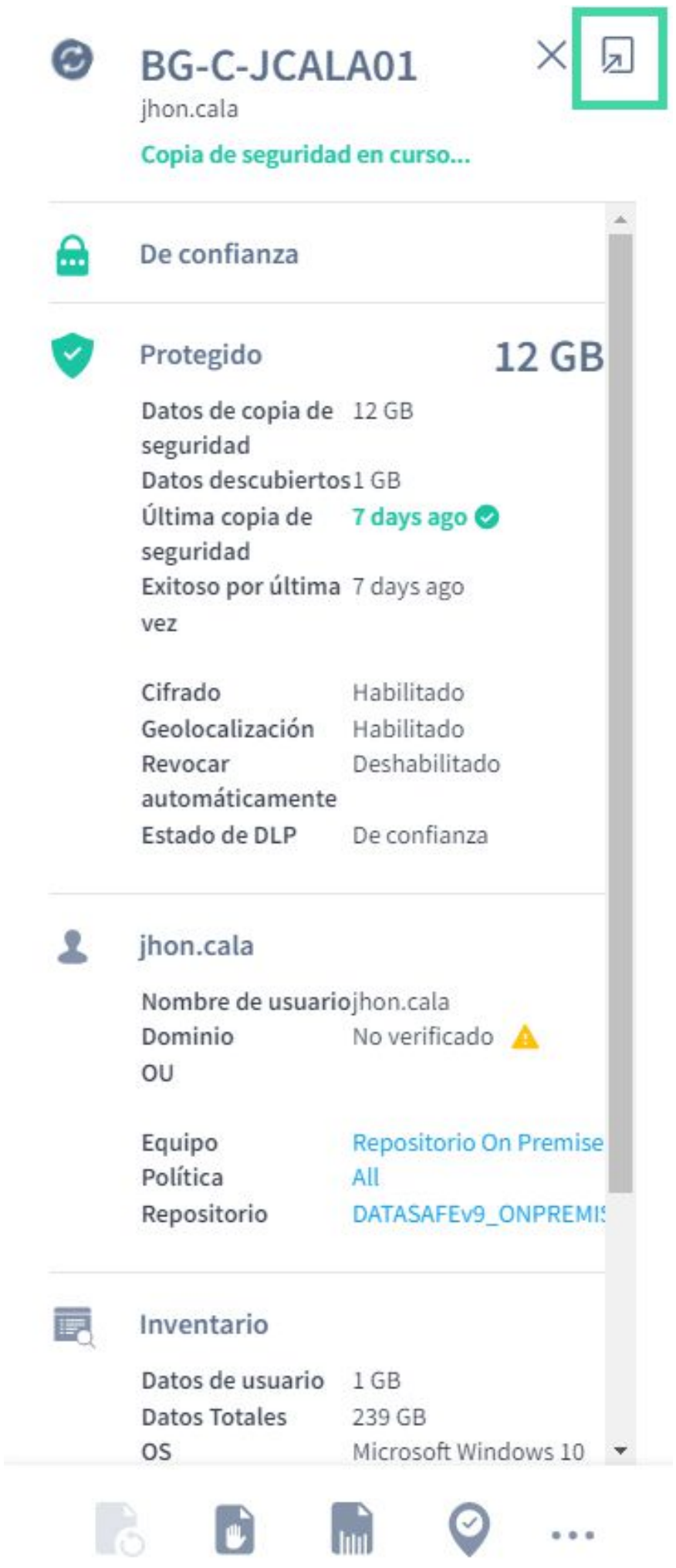
Field	Description
Name	The device name Device
User	The username associated with the device
Status	Displays device status: - Active (Green Check Icon) - Pending Activation (Yellow Watch Icon) - At Risk (Red Warning Icon) - Failed (Red Failed Icon)
Team	The computer to which the device is assigned
Data Discovered	The amount of business data discovered
Discovery Agent	The version number of the Discovery Agent software that was used to discover the device.

If you highlight a device in the list, a radio button (...) appears to the right of the device name. Click the radio button to display a context menu with these options:

Field	Description
View	Displays the Device page, which contains details about the device, including its hardware and software.
Activate	Use it to activate the device so that Aranda Datasafe begins to back it up and protect it. You can only activate a device if it's assigned to a team and the team is assigned to a repository and policy.
Assign Team	Use it to assign the device to a team. Aranda Datasafe can only backup and protect devices that are assigned to computers, as computers must be associated with a repository and a policy.
Delete	Use it to remove a device.

Device sidebar

If you click a device in the list of devices, the device's sidebar appears. Displays additional information about the selected device. If you click on the View icon in the top corner, Aranda Datasafe displays the Device page, which contains a more detailed view of the device, including its hardware and software.

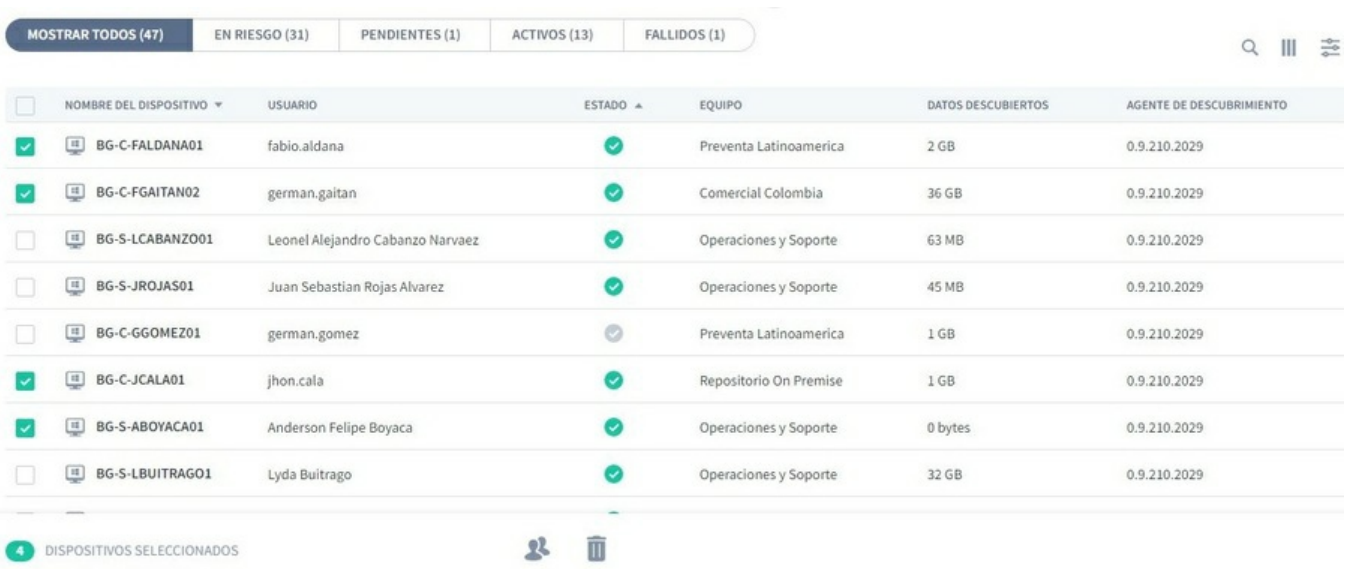


At the bottom of the device's sidebar, there are icons to manually back up the device, revoke it, erase it, and use geolocation to discover it.

Multi-device actions

You can use the device list to apply a single action to multiple devices. For example, you can assign multiple devices to the same computer.

Use the check box to the left of each row of devices to select a device. When you select the check boxes, the action options appear at the bottom of the list. These work the same way as for individual devices, except that the action will apply to all the devices you selected.



Devices

Aranda Datasafe provides a device page for each device it discovers. The Device page provides detailed information about the device's health, data, hardware, and software.

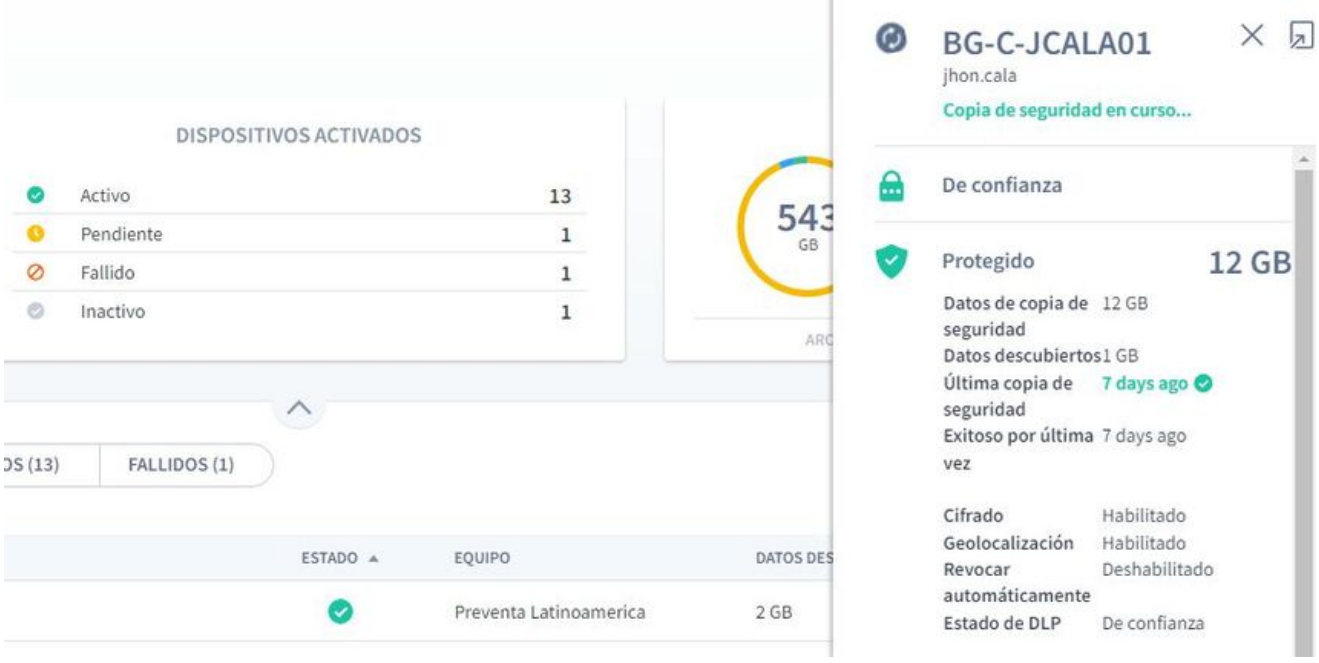
To access a device's **Device** page:

1. Click on **Inventory** or **Protection**.

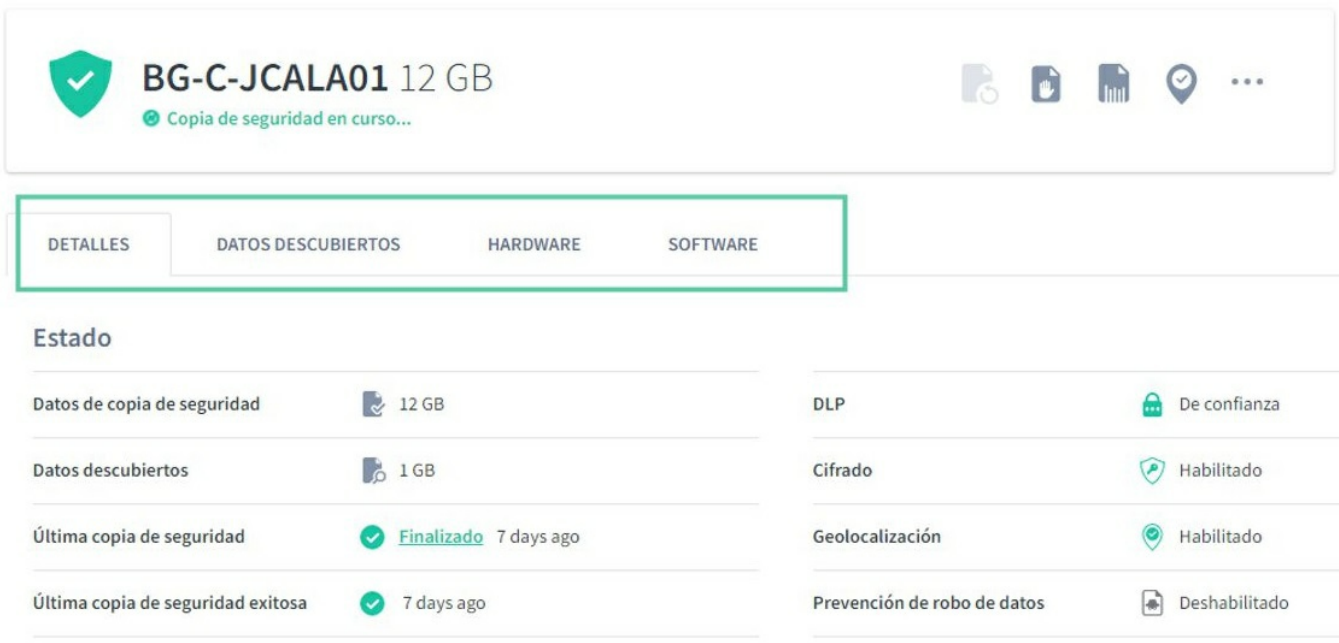
2. Click the options button (...) of the device in the list of devices.

3. Click **View**.

Alternatively, you can click on the device in the list of devices and then select the **View** icon at the top of the sliding panel.

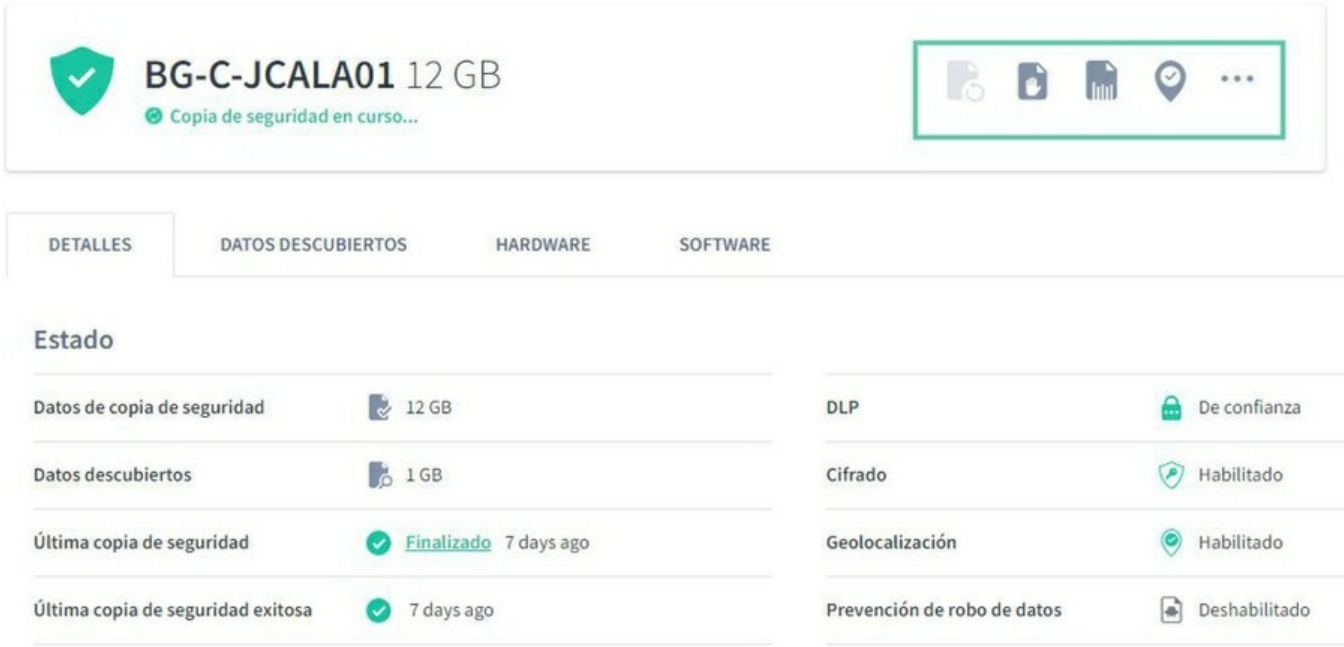


The Device page has an action pane at the top and information tabs below. The**Details** tab is displayed by default and you can select**Discovered Data, Hardware and Software**.



Actions

The name and status banner at the top of the Device page contains several action icons. Icon availability varies depending on which features are enabled in the Policy and whether Protection Agent has been enabled.

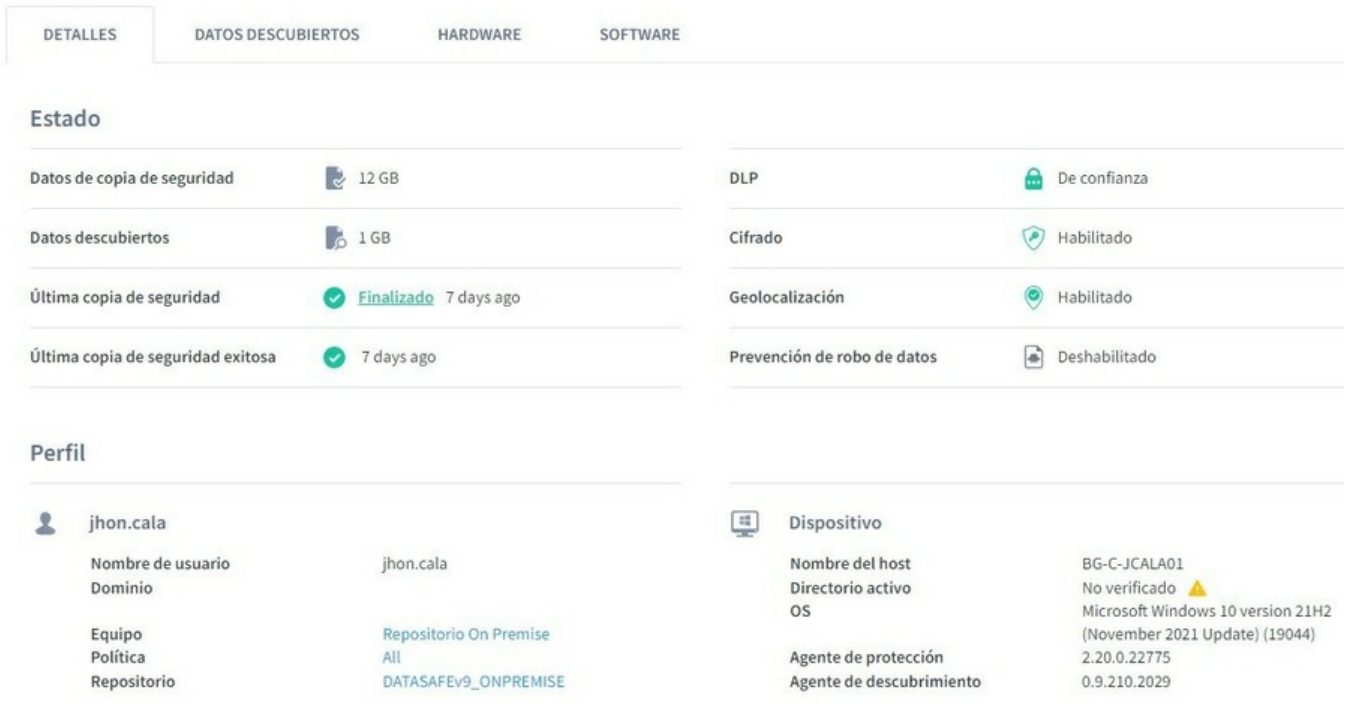


You can use the action icons only after the Protection Agent has been activated:

- Back up a device manually
- Revoke a device.
- Clean a device.
- Locate a device.

Details

The Details tab is displayed by default and provides information about the Aranda Datasafe device view.



The Status section includes the size of the backup data, the amount of data discovered, the time and status of the most recent backup, and whether DLP features are enabled.

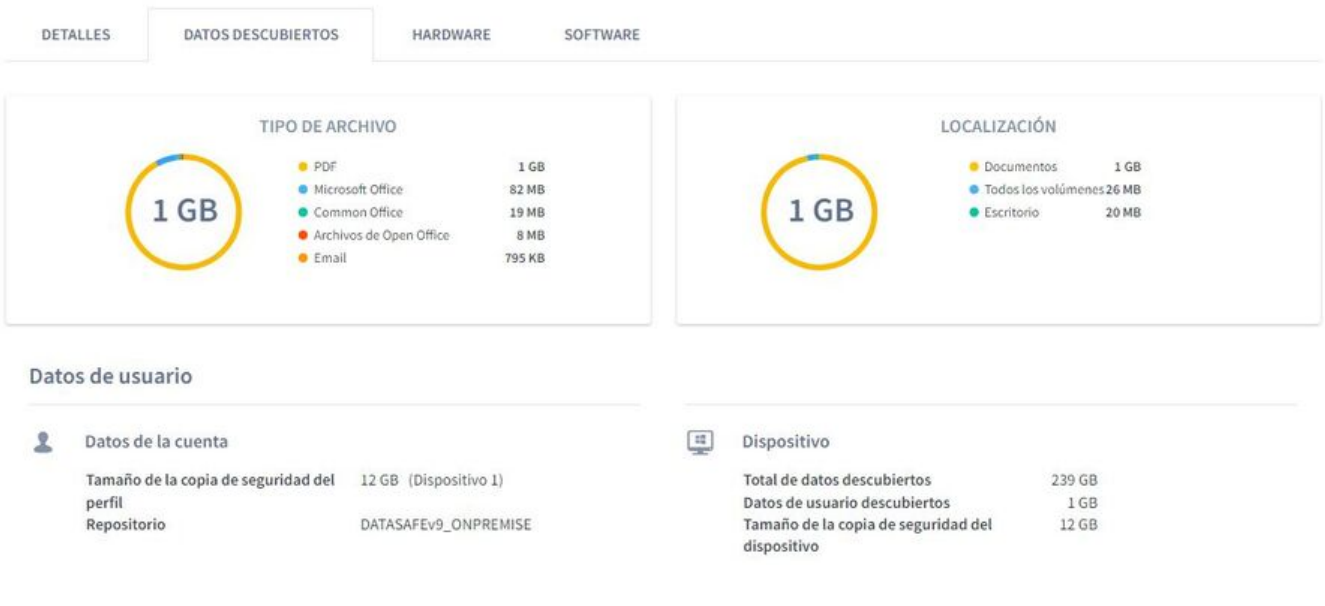
The Profile section displays the credentials for the user profile and the computer, policy, and repository with which the device is associated.

The Device section displays information about the operating system and agents running on the device. It also displays the network connection details.

Data Discovered

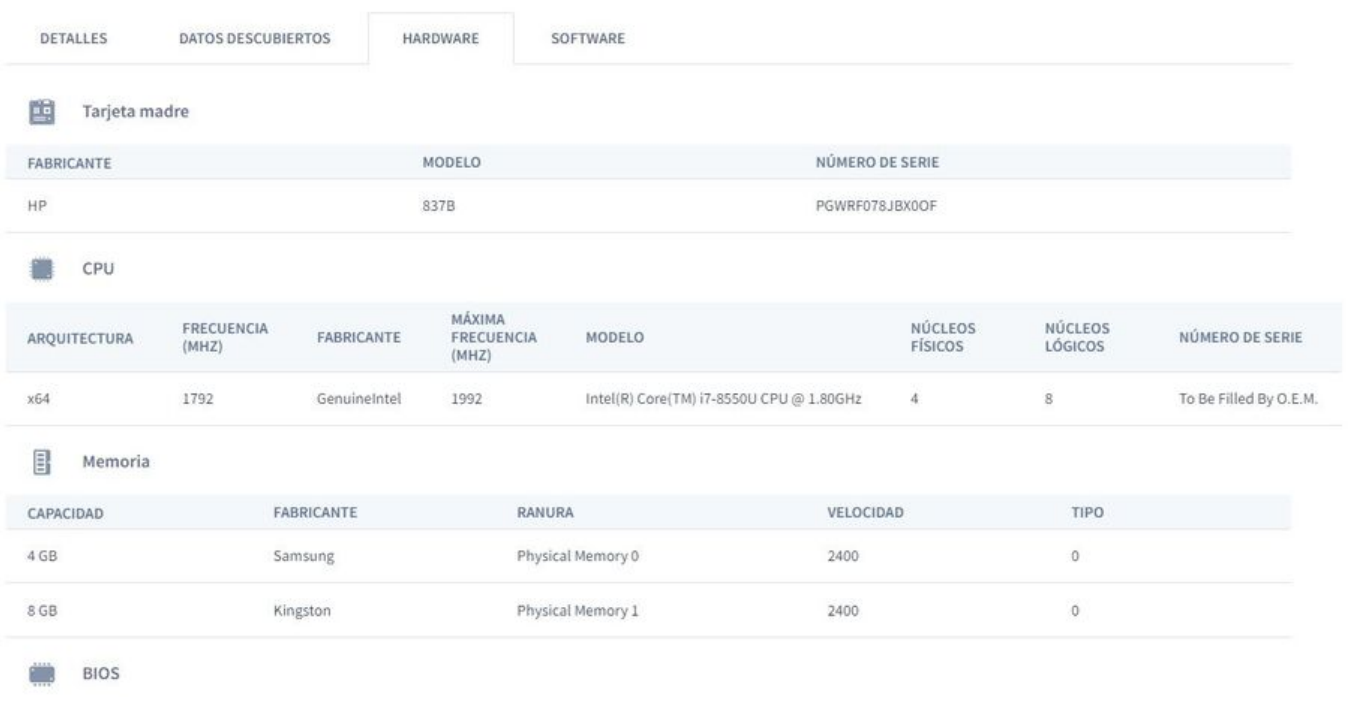
The Discovered Data tab provides information about the data that Aranda Datasafe has discovered on the device.

There is information about the file types that Aranda Datasafe has discovered and also the locations where the data was found.



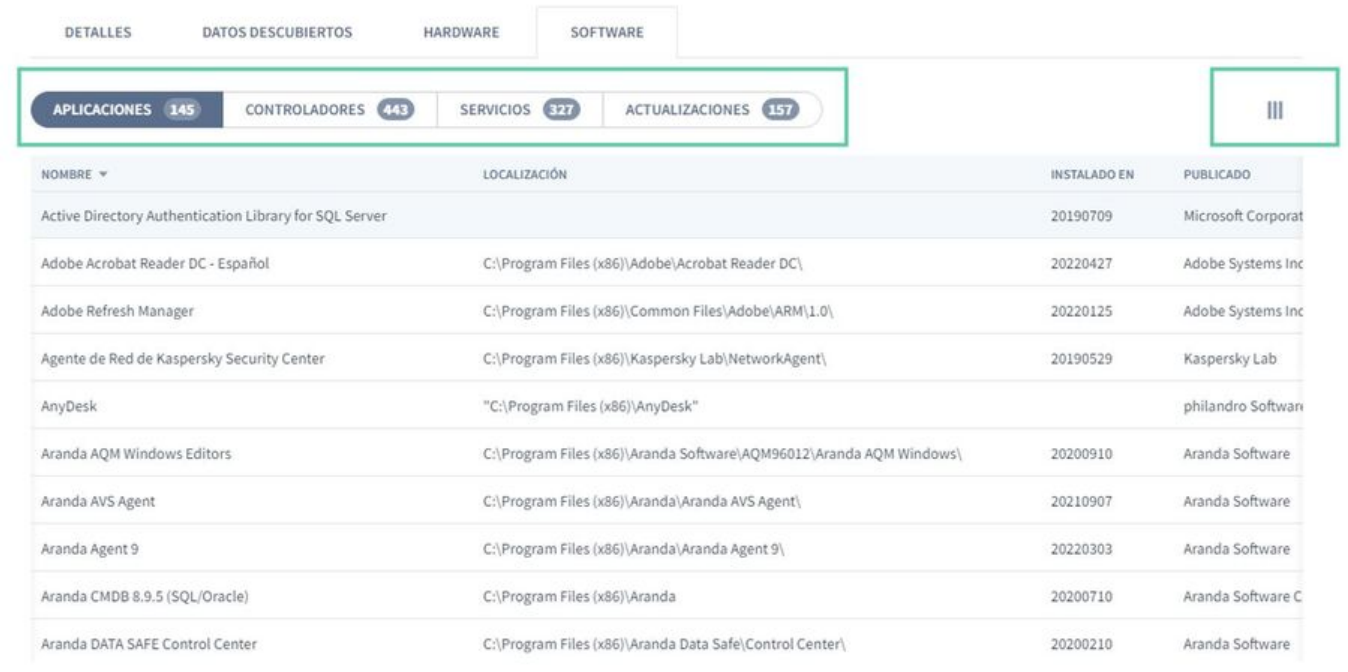
Hardware

The Hardware tab provides information about the device and its components, including the type of motherboard and processor, and the amount of memory.



Software

The software tab contains a list of software applications, drivers, services, and updates that are installed on your device.



By default, the list shows the **apps**. You can click the buttons above the list to configure it to display **Drivers, Services, or Updates**.

You can use the search function to configure the software list to only display information about applications, drivers, services, or updates that have a particular name (or part of a name).

You can also choose to hide columns in the software list. For example, you may not be interested in the **installation date** or **publisher** in the Apps view, so you can hide those columns.

To show/hide columns, click the Columns icon and then choose which columns to include or exclude.

Activating Your Devices

Aranda Datasafe will only back up and protect devices that have been activated. Data from any device that isn't activated is potentially at risk.

When you activate a device, you create a request for that device to be protected and backed up. If the activation request is successful, the device will be protected when the next backup is scheduled (as defined in the Policy settings).

Prerequisites

In this article, we explain how to activate your devices. Before you can activate a device, you must have the following in place:

- A policy that defines what data will be backed up, how often it will be backed up, and what protection settings will be used. see Policies.
- A repository that defines the storage area that will be used to store the device's backup data. For more information about repositories See repositories.
- A team. The policy and repository must be assigned to the team. The device you're activating must also be assigned to the Team. For more information see Equipment.

When these settings are in place, you can activate your **"at risk"** devices.

Activate a device

To activate a "compromised" device:

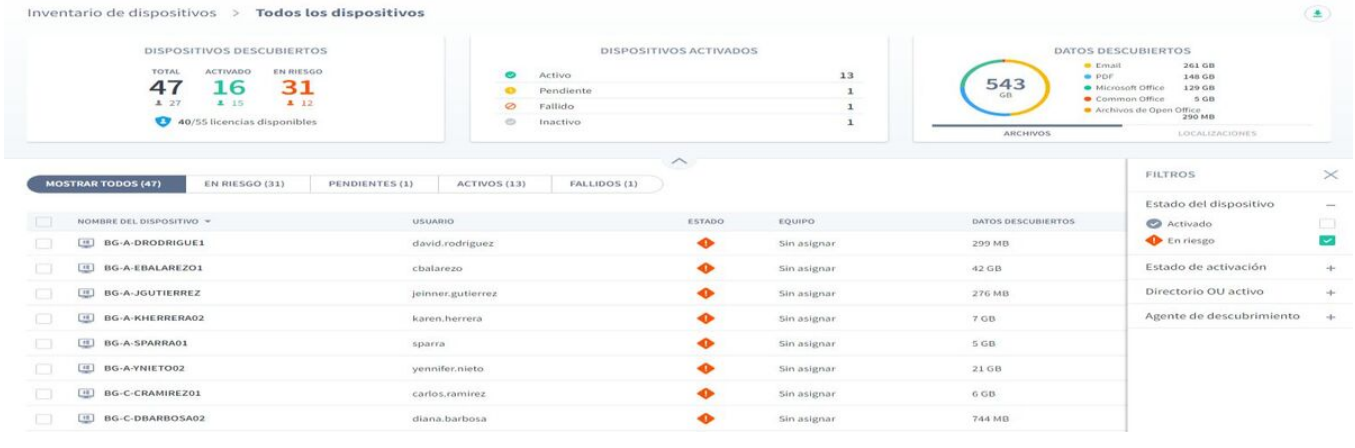
1. Click on **Inventory**.

2. Click on the filter icon above the list of devices.

3. Choose **Device Status** and select **At Risk**.

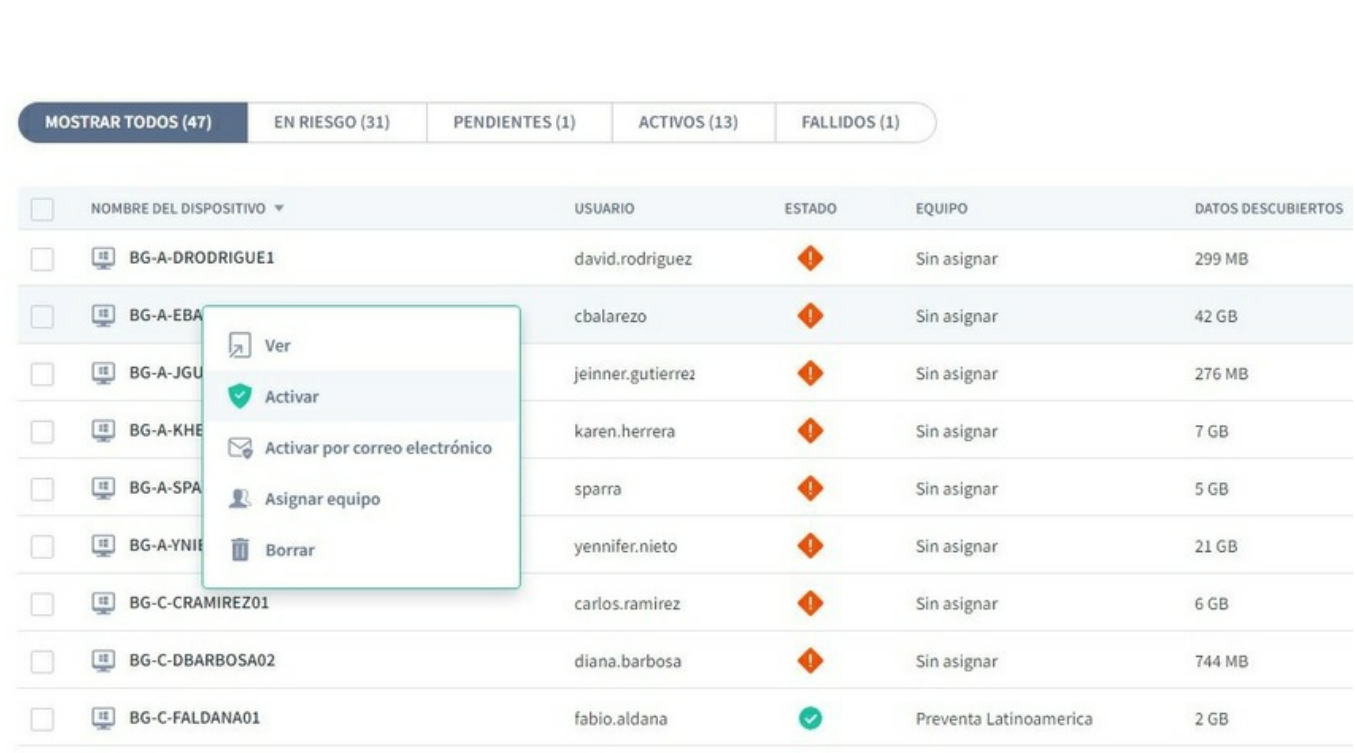
4. Click **Apply**.

The list of devices is now filtered to only show those devices that are “at risk.”

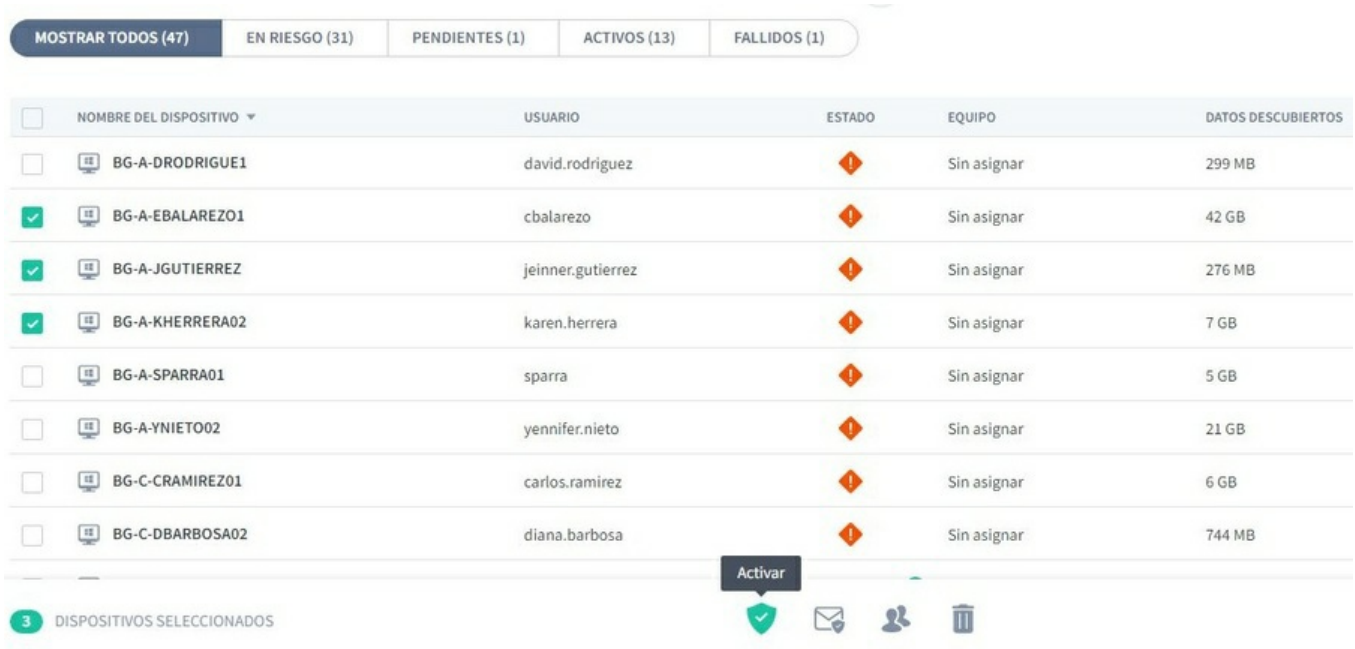


5. There are several ways to activate devices.

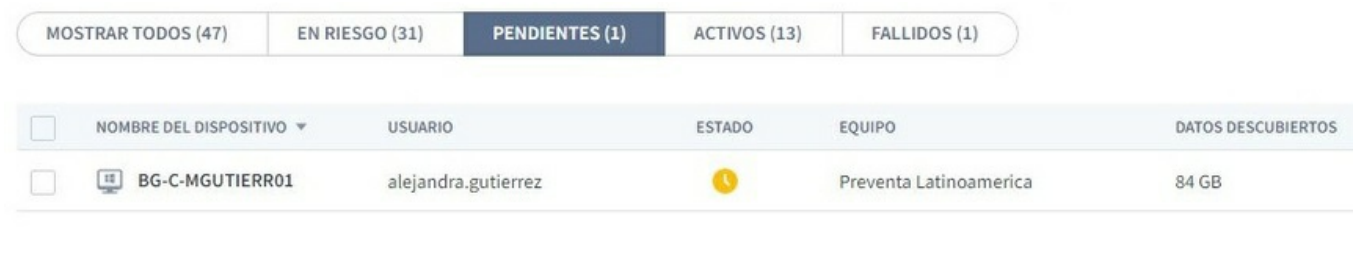
To activate a single device, you can click on its radio button and then click on**Activate**. Or you can select your checkbox and click the**Activate** icon in the pop-up bar at the bottom.



To activate multiple devices, select the checkboxes for the devices you want to activate. Then click the Activate icon in the pop-up bar at the bottom.



When you activate a device, its status changes from At Risk to Pending. After a short delay, the device status changes to Active and a green check icon is displayed.



If the device can't be activated, a red error icon is displayed. You will need to investigate why activation failed. It may be because the user is not logged in to the device or there was a connection issue.

6. To find out which devices are protected by Aranda Datasafe, click Protection.The Protection Page displays details of devices that currently have data encrypted and backed up by Aranda Datasafe.

Inventory Page Filtering

By default, the Inventory page displays information for all computers and devices. But, if necessary, you can filter the Inventory page to only show information that meets certain criteria. For example, you can filter the Inventory page to only show information for devices on a particular computer.

There are several ways to filter the Inventory page (or parts of the Inventory page):

Filter by team

Use a search to filter the list of devices

Filter the list of devices by selected criteria

Show or hide columns in the device list.

Filter by Team

You can use the Computers sidebar to filter the Inventory page so that it only shows information about the devices on certain Computers. For example, you can configure the Inventory page to only display information for a "Finance" team and an "HR" team.

Note

If you use the Teams sidebar to filter the Inventory page, all information panels and the list of devices are filtered.

1. Click on **Inventory**.

2. In the **Equipment** section, click:

- **All Devices** to display information about all devices on all computers (this is the equivalent of removing the computer filter)
- **Unassigned** to display information only for those devices that are not yet assigned to a team
- **** to display information about devices on a specific team.

When you select a Device or Devices, the Inventory page refreshes and the information screens and device list are filtered. They only show information about the devices on the selected teams.

Click **All Devices** in the **Teams** sidebar to remove the filter.

Use a search to filter the list of devices

You can use the search function to filter the list of devices so that it only includes devices that have certain values. For example, you can use search to filter the list so that it only shows devices with a particular name (or prefix to a name). This is useful if you have a consistent device naming scheme and only want to see particular devices. For example, you may have devices that start with names that start with ERL, so you can search for ERL.

You can use search to filter the list of devices by any text value, including device name, user name, and computer name.

To apply a search filter:

1. Click on the search icon above the list of devices.

2. Enter the first few characters of the text value you want to use as a filter. Aranda Datasafe applies the filter as you type, so you can do partial matches OR you can enter the full-text value to be more specific.

Filter the list of devices by selected criteria

You can filter the device list to only show devices that match your chosen criteria.

To filter the list of devices:

1. Click on the filter icon

to display the Sliding Filters options.

2. Expand Filter Categories and select the filter criteria you want to apply. The device list will only show devices that match all the criteria you select.

3. Click **Apply**.

You can choose any of these filter options:

Filter	Description	Options
Device Status	Filter devices based on their activation status.	Activated (selected for activation) At risk (not yet selected for activation)
Activation Status	Filter the list to only show devices with a particular activation status.	Pending The activation process is scheduled to begin. -active. Device has been successfully activated Failed - The activation process was unsuccessful.
Active Directory OU	Filter by an Active Directory organizational unit of devices. This OU data comes from the discovery agent on the user's device.	List of available OUs
Agent of Discovery	Filter the list to only show devices that use a particular version of the Discovery Agent software.	List of Available Discovery Agents

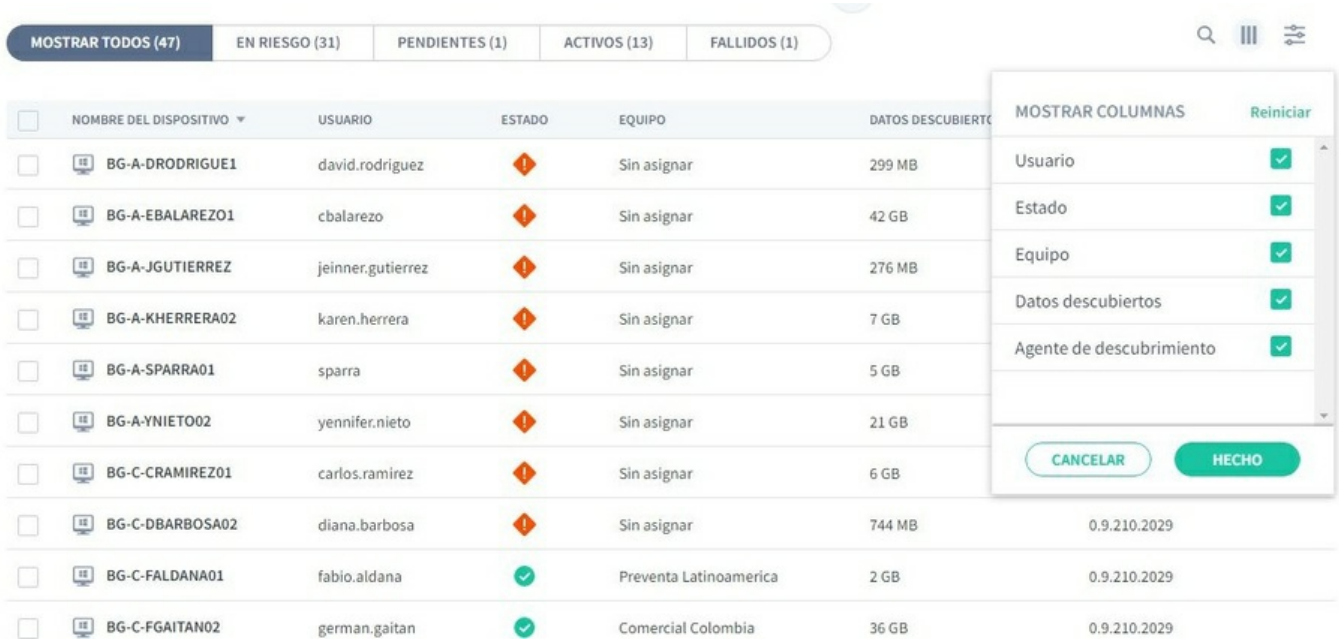
To remove the filters, click the Filter icon and click **Reset** (or uncheck each of the filter boxes).

Show or hide columns in the device list

You can choose to show or hide columns in the device list. For example, you might not care which version of Discovery Agent was used to discover a device, so you

can hide it from view.

To show/hide columns, click the Columns icon and then choose which columns to include. For a description of each column, see the Inventory Page.



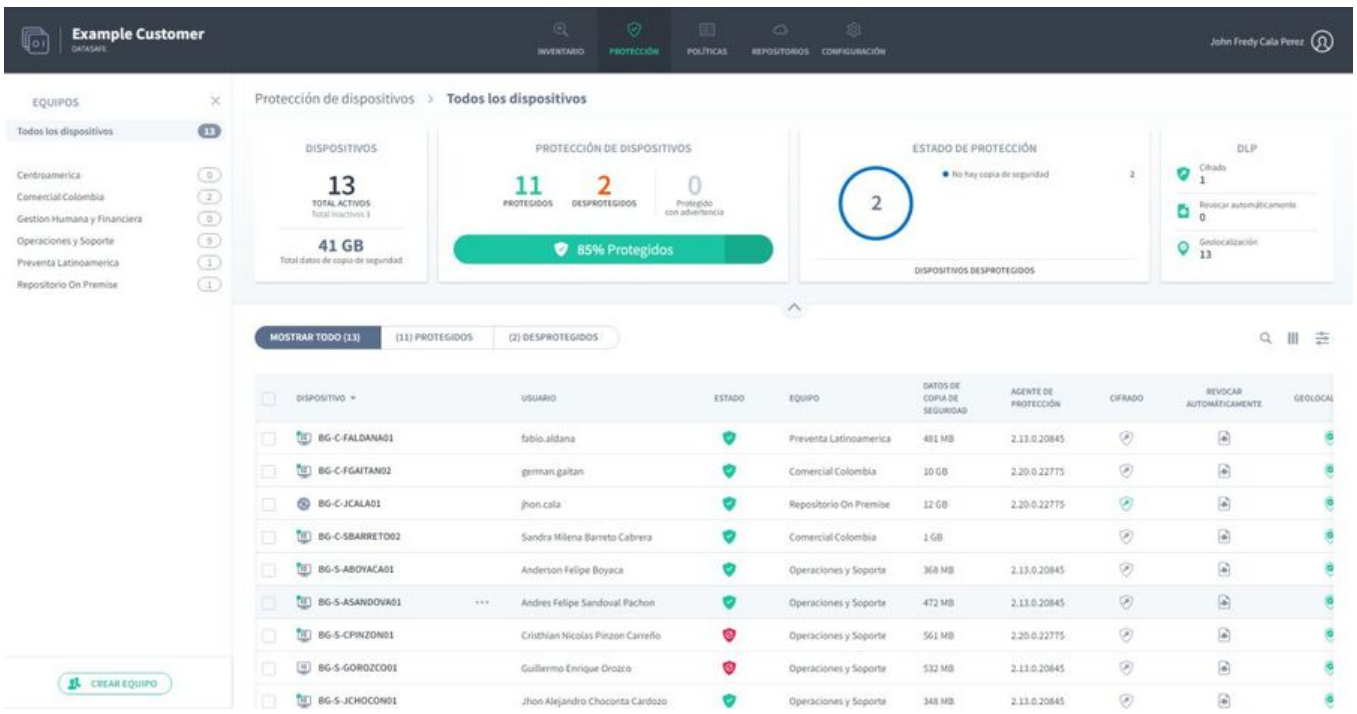
Protection

Aranda Datasafe protects your company's data by automatically performing encrypted backups of your company's data. It also has data loss prevention (DLP) features that you can turn on or off, depending on your requirements.

You can use the Protection page to view the protection status of all your activated devices. Please note that the Protection page It doesn't show data for devices that haven't been activated yet.

Device protection

The **Protection** page provides information about activated devices and their current protection status. You can use it to find out which devices are currently protected, unprotected, or protected with warning.



Protection Status	Description
Protected	The device has been activated, has the Protection Agent software installed, and its data is backed up by Aranda Datasafe.
Unprotected	The device has been activated, has the Protection Agent software installed, but has not been successfully backed up in the last 5 days. (5 days is the default protection range) Until a successful backup is made, the data on an unprotected device is at risk. The first backup of the device usually happens around 10 minutes after the device is activated. But it may take longer, depending on how long it takes for the Protection Agent software to index the files.
Protected with Warning	The device has been activated and has the Protection Agent software installed. The device performed a successful backup within the last 5 days, but Warning failed the last backup attempt.

The Protection page only displays devices that are successfully detected and activated. If the Protection page is empty, your devices have not been discovered or have been discovered, but not activated.

⚐ >**Note:** In the Inventory page , we use the term "At risk" to describe a device that has been discovered, but not activated. The "Unprotected" devices on the Protection page have been activated, but they have not been backed up in the protection range. Both "at risk" and "unprotected" devices contain data that is vulnerable.

Devices

The Devices dashboard provides a summary of:

- Number of active and inactive devices
- Amount of backup data across all devices.

Backup data shows the sum of all data included in the Policy across all devices at a specific point in time. This number is not the information stored in the repository.

An active device is a device that has been activated and connected to Aranda Datasafe in the last 30 days.

Field	Description
Total Assets	The total number of devices that are active. These devices have been activated and are**protected, protected with warning, or unprotected** (see Device Protection). Active devices are not necessarily protected or backed up.
Total Inactive	The total number of devices that have been activated but have not connected to Aranda Datasafe in the last 30 days (and are therefore not backed up for that time period).
Total Data Backed Up	The amount of data on all devices that are included in backup policies at a specific point in time. You can use this as an indication of how much storage space is needed. But keep in mind that the backup data cipher will change whenever the Policy changes or when users add/remove backup data on their devices.

Device Protection

The Device Protection dashboard provides information about the number of devices that have been backed up and protected in the last 5 days. Sample:

Field	Description
Protected	The total number of devices that have been successfully backed up in the last 5 days.
Unprotected	The total number of devices that have not been successfully backed up in the last 5 days.
Protected with Warning	The total number of devices that have been successfully backed up in the last 5 days, but the most recent backup failed.

Protected Status

The Protection Status pane provides a summary of the number of devices that are currently protected, protected with warnings, or unprotected.

If some of your devices are in the unprotected or unprotected with warning status, the Protection Status panel has two tabs **Unprotected** and **Protected** with warning (shown at the bottom of the panel).

The **Unprotected** tab shows:

Field	Description
No Backrest	The number of devices that are unprotected and have no backup data in Aranda Datasafe.
Offline	The number of devices that are unprotected and do not have a connection to Aranda Datasafe.
Lost Connection	The number of devices that are unprotected and have lost their connection to Aranda Datasafe
Agent Error	The number of devices that have an agent error that the server cannot recognize. If you have agent error messages, please contact our technical support team for assistance.
Server Connection Limit	The number of devices that try to connect to Aranda Datasafe when the server's connection limit has already been reached. Aranda Datasafe allows a certain number of simultaneous connections (60 by default) and once this limit is reached, no additional connections can be made. Devices will try again in a few minutes to check if a connection is available and back it up.
Other	The number of errors that are not categorized. If you have other errors, please contact our technical support team for assistance. (reportedecasos@arandasoft.com)

The **Protected with warning** tab shows the number of devices that are protected with a warning. If there are warnings, statistics are provided for the warnings (as shown below):

Field	Description
Agent Error	The number of devices that are protected, but have an agent error that the server can't recognize. If you have agent error messages, please contact our technical support team for assistance.
Locked Files	The number of devices that are protected, but have locked files (files that were open on the device when the backup was made). Aranda Datasafe can back up locked files, but the success of the backup depends on the Windows VSS service working properly. If you have blocked file warnings, we recommend that you filter the Device List on the Protected page to show only devices with the "protected with warning" status. Then, display the device's backup log to determine which files were locked. You can then decide whether you want to close the files on the devices and back up the devices manually or leave them until the next scheduled backup.

DLP

The DLP dashboard displays a summary of the number of devices using Data Loss Prevention features (encryption, auto-revocation, and geolocation). DLP features are enabled and disabled in the policy settings.

Teams sidebar

On the left side of the Protection page is the Teams sidebar. This displays a list of the devices that are configured on your Datasafe Aranda (plus All Devices and Unassigned, which are integrated).

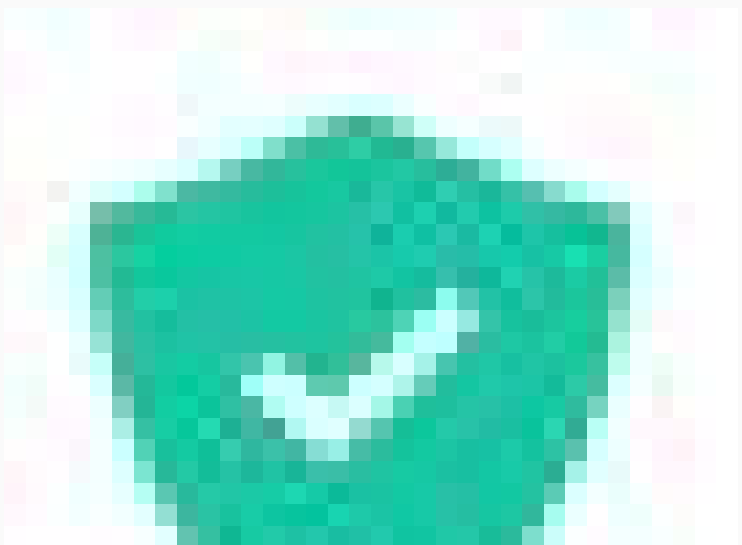
If you click a computer, the protection panels and device list are updated so that it only displays information for the devices on the selected computer. You can click **All Devices** to set the Inventory to display data for each device.

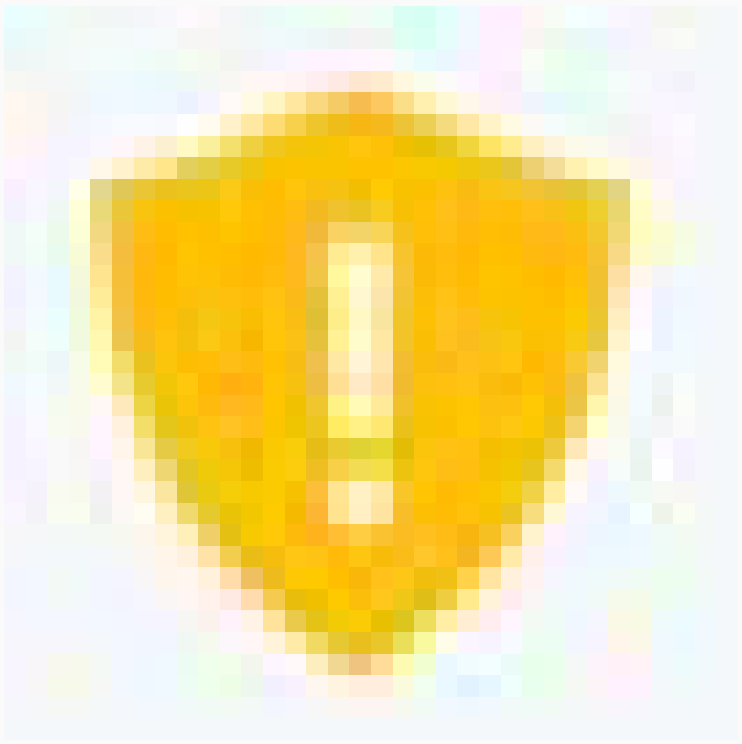
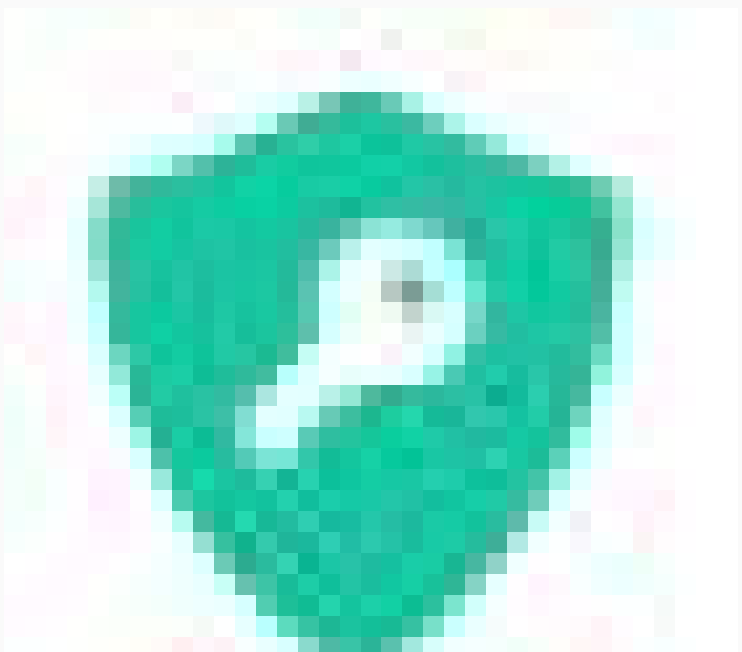
Admin users can use a keyboard shortcut to select computers to report on. Press the CTRL key and then select the equipment you want to include.

Device Protection List

The bottom Protection section displays the Device Protection List, which contains a summary of the devices that Aranda Datasafe has discovered and their protection status.

Field	Description
Device	The name of the device.
User	The name of the user associated with the device.
	Displays protection status: Protected



Field	Description
	Protected with Warning
Status	
	Unprotected
	
Team	The computer to which the device is assigned.
Backed Data	Aranda Datasafe backs up a certain amount of data on the device (in accordance with a Policy). The quantity is displayed in the Backup Data column.
Protection Agent	The version of the Protection Agent software that is currently installed on the device.
	Shows if the local encryption feature is enabled for the device. You can enable and disable local encryption in the Policy that is associated with the Computer (of which the device is a member). A green icon means it's enabled, a gray icon means it's disabled.
Encryption	

Field	Description
Automatic Revocation	<p>Shows if the auto-revocation feature is enabled for the device. You can enable and disable automatic revocation in the Policy that is associated with the Team (of which the device is a member). A green icon means it's enabled, a gray icon means it's disabled.
Geolocation	Shows if the geolocation feature is enabled for the device. You can enable and disable geolocation in the Policy that is associated with the Team (of which the device is a member). A green icon means it's enabled, a gray icon means it's disabled.
DLP Status	Displays the data loss prevention status. This can be: **Trusted**: The device has been authenticated and can connect to Aranda Datasafe. **Revoked**: The device has been revoked, so unauthorized users cannot access the encrypted data on the device. It is not trusted and no further backups or restores will be performed. **Erased**: The device has been erased. It is not trusted and no further backups or restores will be performed.

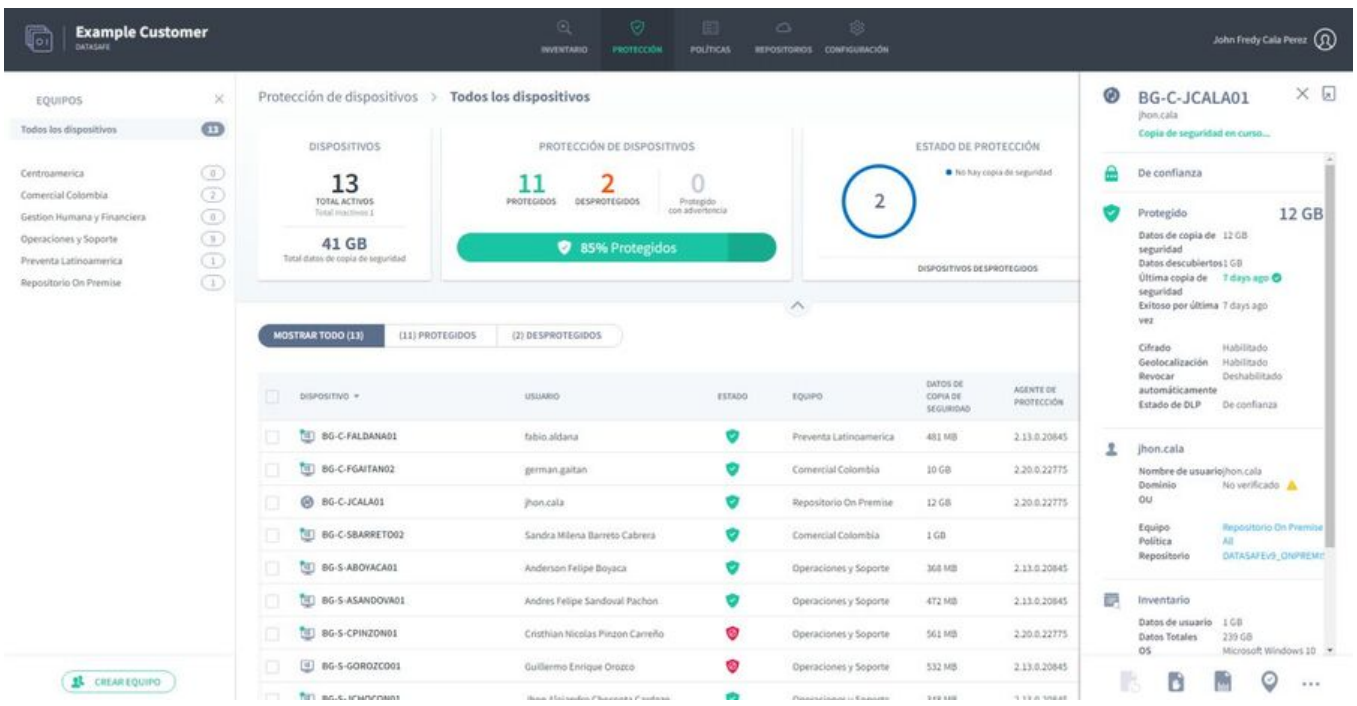
By default, the device list displays information for all devices (**Show All** filter). If you prefer, you can click on one of the other filter options. There are three other possible filter options, one for each state: **protected, protected with warning, unprotected**. Filter options are only available if there are devices in that particular state.

If you highlight a device in the list, a radio button (...) appears to the right of the device name. Click the radio button to display a context menu with these options:

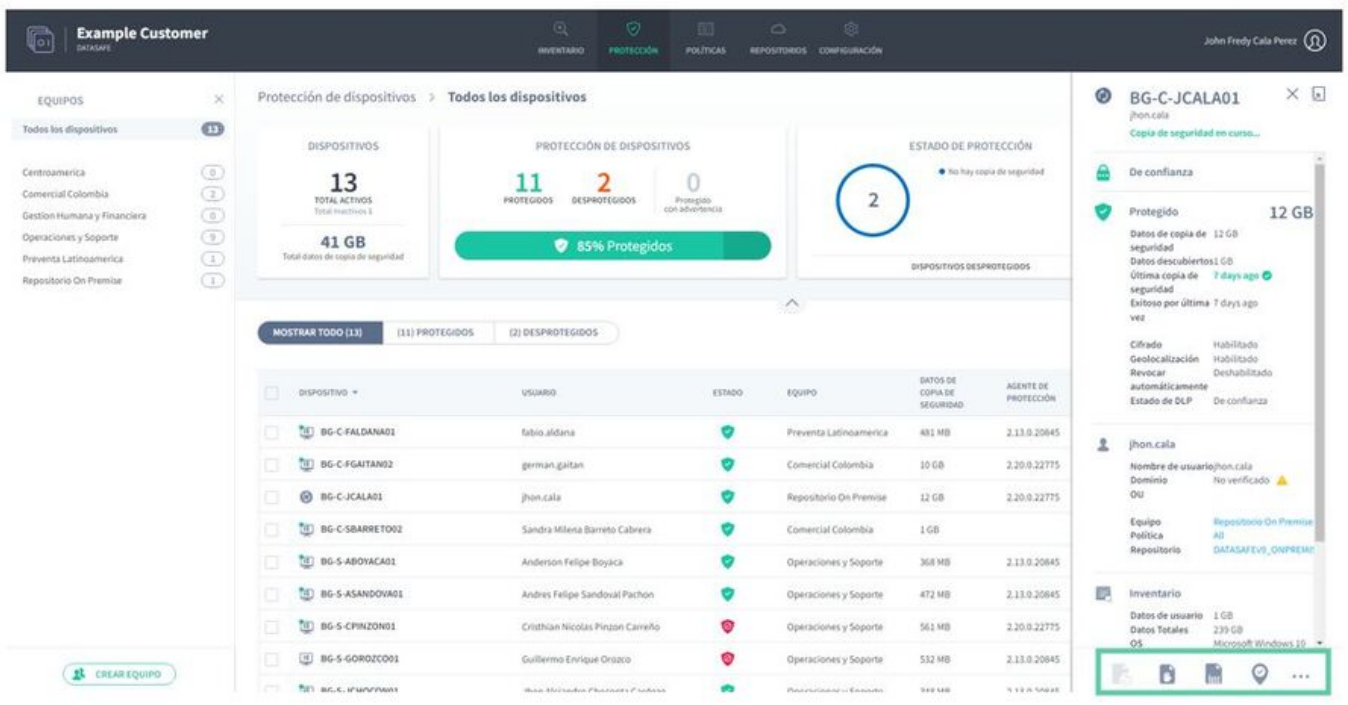
Field	Description
View	Displays the Device page, which contains details about the device, including its hardware and software.
Assign Team	Use it to assign the device to a team. Aranda Datasafe can only backup and protect devices that are assigned to computers, as computers must be associated with a repository and a policy.
Remove	Use it to remove a device. If you delete a user's last remaining device, a license will be released and available for use by other users.

Device sidebar

If you click a device in the list of devices, the device's sidebar appears. Displays additional information about the selected device. If you click on the View icon in the top corner, Aranda Datasafe displays the Device page, which contains a more detailed view of the device, including its hardware and software.



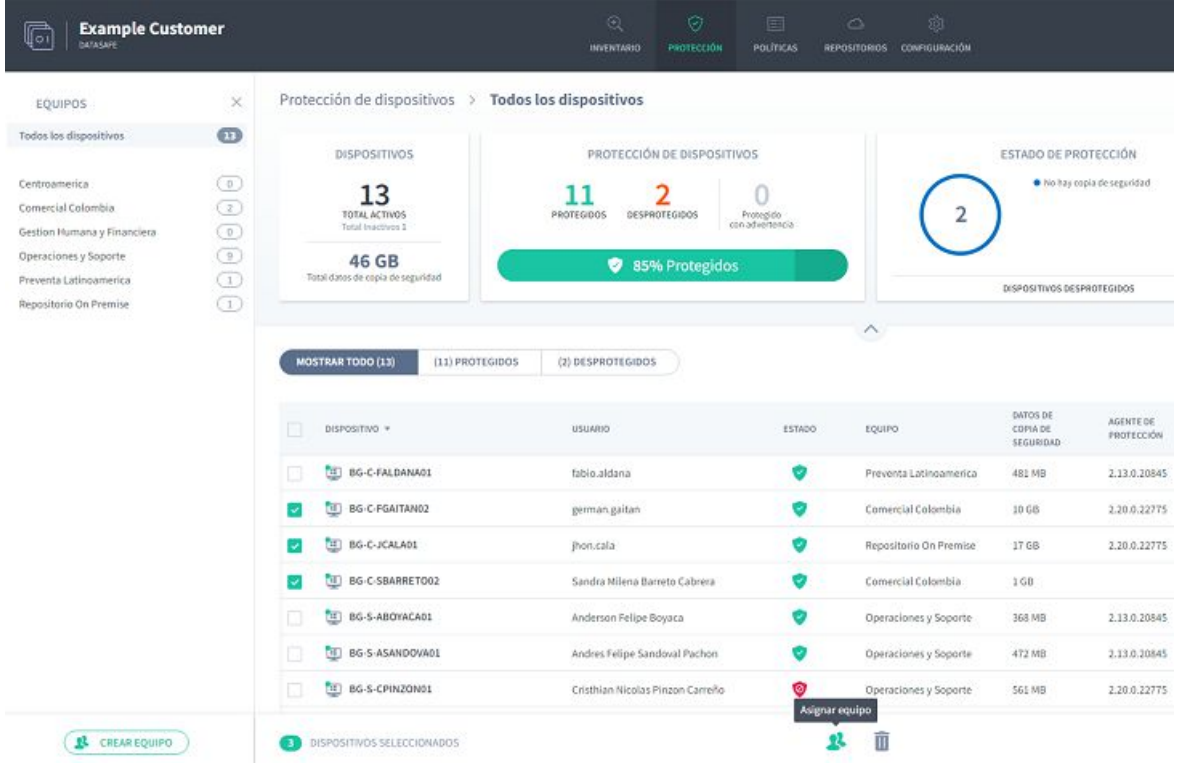
At the bottom of the device's sidebar, there are icons to manually back up the device, revoke it, erase it, and use geolocation to discover it. The same icons are also available on the Device page.



Multi-device actions

You can use the device list to apply a single action to multiple devices. For example, you can assign multiple devices to the same computer.

Use the check box to the left of each row of devices to select a device. When you select the check boxes, the action options appear at the bottom of the list. These work the same way as for individual devices, except that the action will apply to all the devices you selected.



Filtering Protection

By default, the Protection page displays information for all computers and devices. But, if necessary, you can filter the Protection page to only show information that meets certain criteria. For example, you can filter the Protection page to only show information about the devices on a particular computer.

There are several ways to filter the Protection page (or parts of the Protection page):

Filter by team

Use a search to filter the list of devices

Filter the list of devices by selected criteria

Show or hide columns in the device list

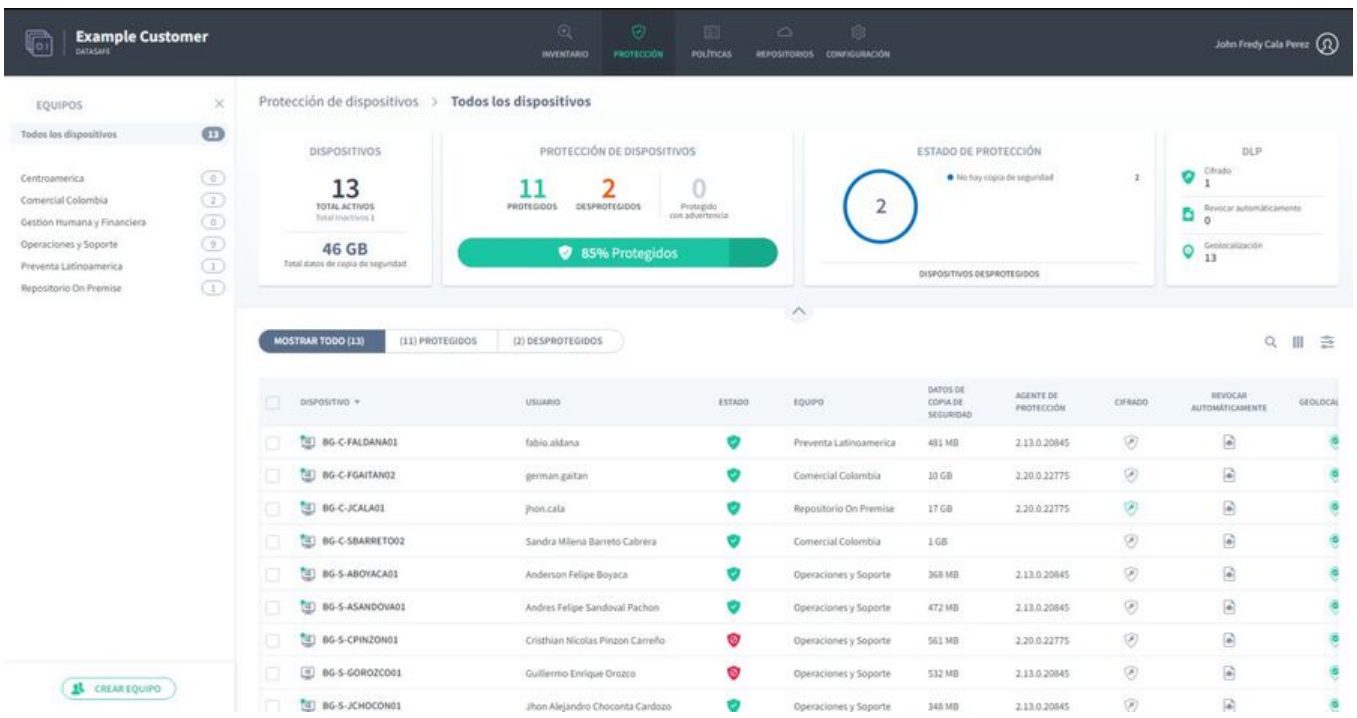
Filter by Team

You can use the **Devices** sidebar to filter the **Protection** page so that it only shows information about devices on certain **Devices**. For example, you can configure the Protection page to only display information for a "Finance" team and a "Human resources" team.

1. Click on **Protection**.

2. In the **Equipment** section, click:

- **All Devices** to display information about all devices on all computers (this is the equivalent of removing the computer filter)
- **Unassigned** to display information only for those devices that are not yet assigned to a team
- **** to display information about devices on a specific team.



When you select a device or devices, the **Protection** page refreshes and filters the information screens and device list. They only show information about the devices on the selected teams.

Click **All Devices** in the **Teams** sidebar to remove the filter.

Use a search to filter the list of devices

You can use the **search** function to filter the list of devices so that it only includes devices that have certain values. For example, you can use search to filter the list so that it only shows devices with a particular name (or prefix to a name). This is useful if you have a consistent device naming scheme and only want to see particular devices. For example, you may have devices that start with names that start with ERL, so you can search for ERL.

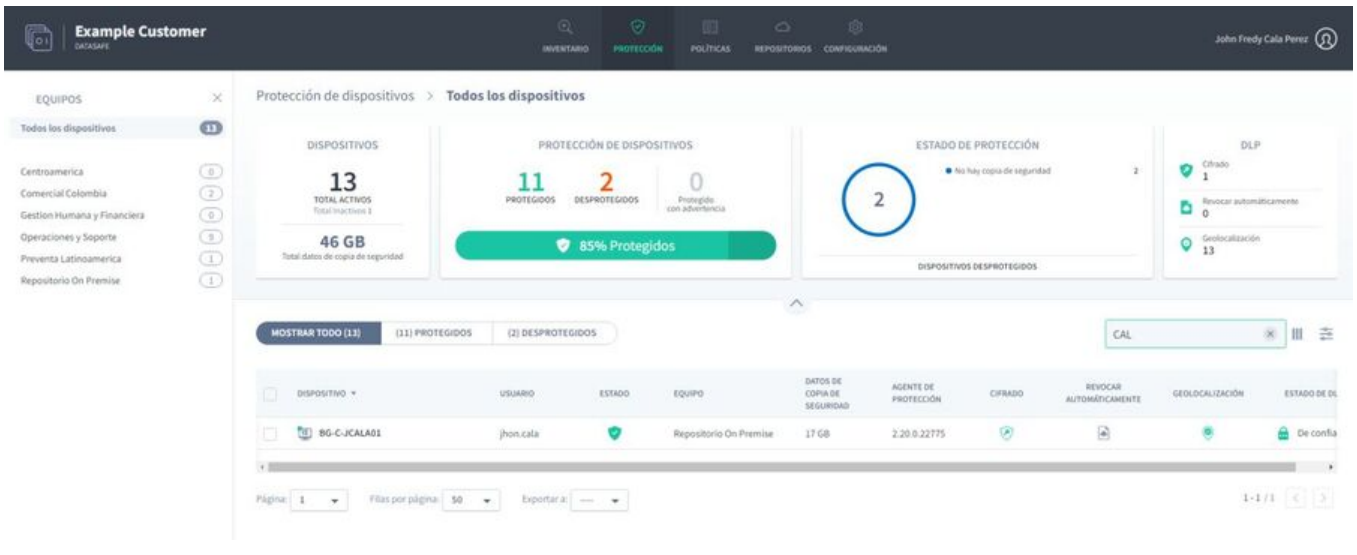
You can use the search to filter the list of devices by any text value, including the **device** name, **user** name, and **computer** name.

To apply a search filter:

1. Click on the search icon above the list of devices.

2. Enter the first few characters of the text value you want to use as a filter. Aranda Datasafe applies the filter as you type, so you can do partial matches or you can enter the full-text value to be more specific.

You can search for the device name, username, or computer name.



Filter the list of devices by selected criteria

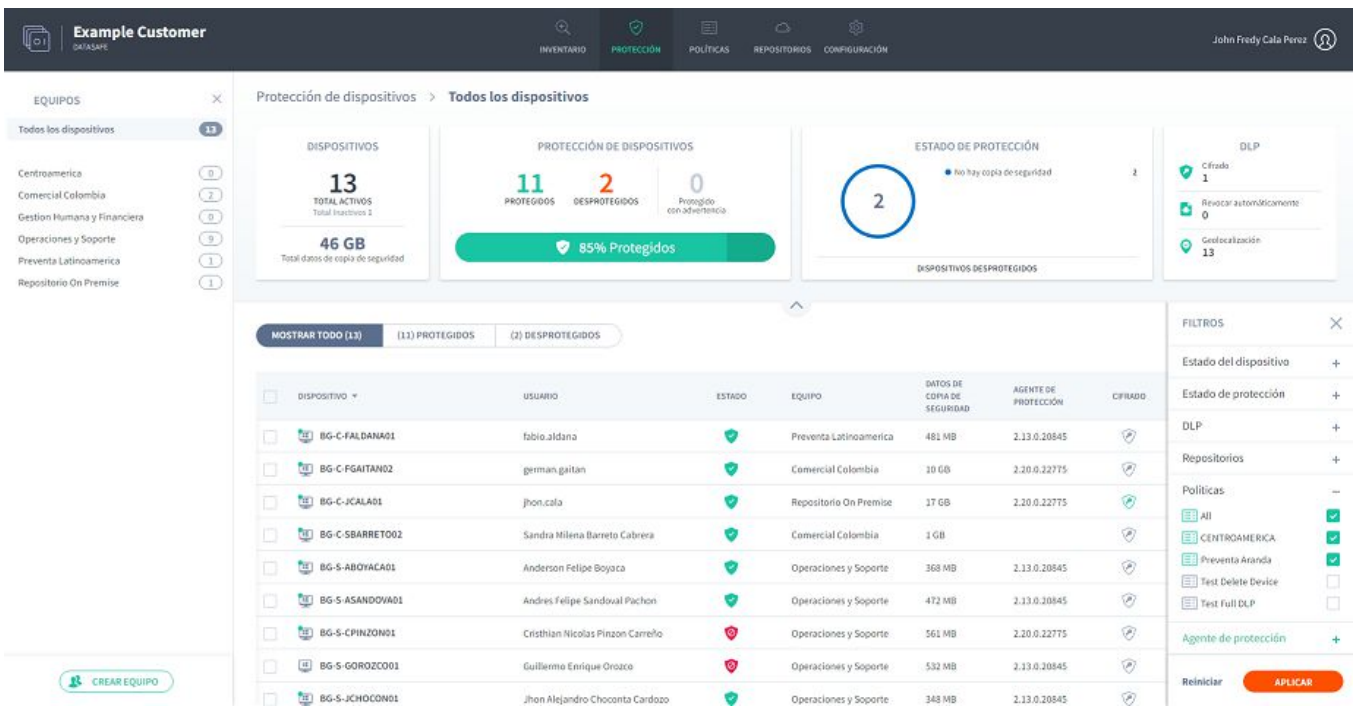
You can filter the device list to only show devices that match your chosen criteria.

To filter the list of devices:

1. Click on the filter icon to display the slide-out filter options.

2. Expand Filter Categories and select the filter criteria you want to apply. The device list will only show devices that match all the criteria you select.

3. Click Apply.



You can choose any of these filter options:

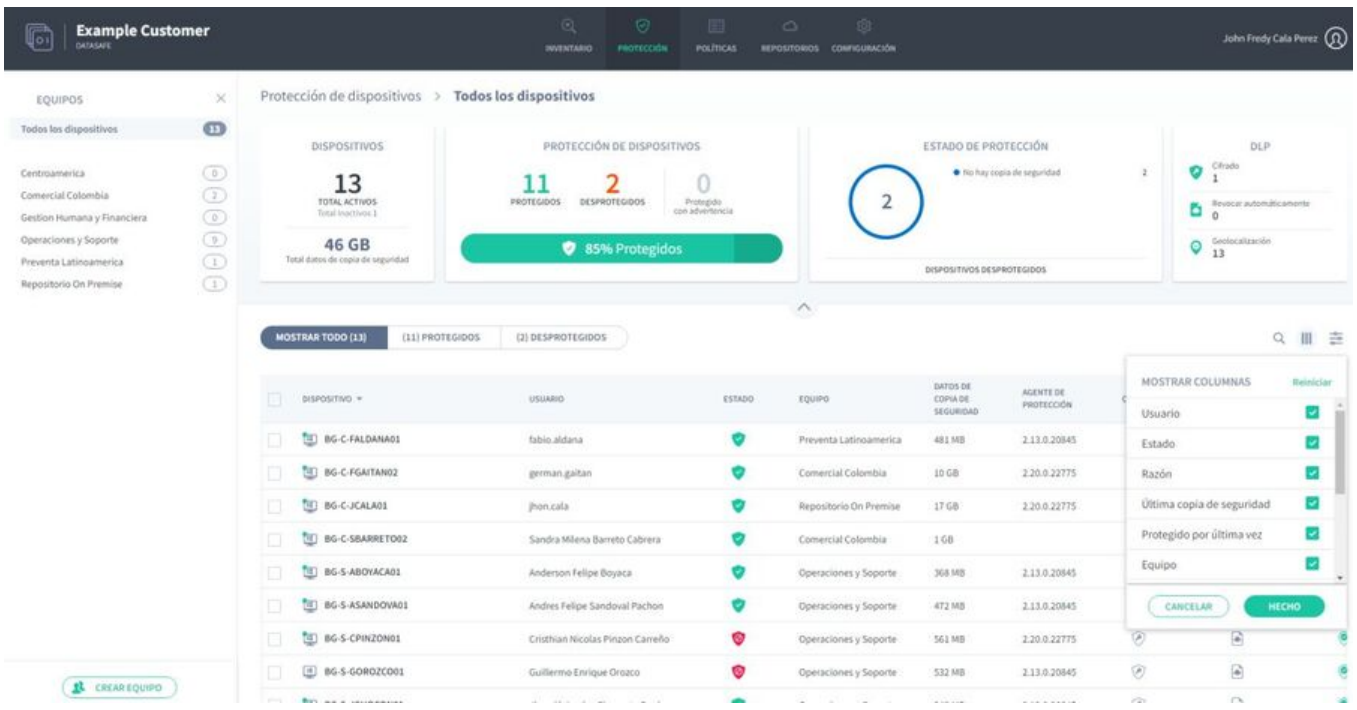
Filter	Description	Options
Device Status	Filter devices based on their activation status.	- Active - Inactive
Protected Status	Filter the list to only show devices with a particular protection status.	- Protected – Protected with warning (device has been protected in the last 5 days, but the most recent backup failed) – Unprotected. - Offline (Aranda Datasafe discovered the device, but it can't connect).
DLP	Filter devices by DLP status.	- Trusted: The device has been authenticated - Revoked: The device's security certificate has been removed* - Erased: The device's protected data has been deleted. Devices are usually revoked or erased when they are missing, stolen, or have not been connected to Aranda Datasafe within a set period of time.
Repositories	Filter the list to only show devices associated with a particular repository.	List of available repositories
Policies	Filter the list to only show devices associated with a particular policy.	List of Available Policies
Protection Agent	Filter the list to only show devices that use a particular version of the Protection Agent software.	List of Available Protection Agent Versions

To remove the filters, click the Filter icon and click **Reset** (or uncheck each of the filter boxes).

Show or hide columns in the device list

You can choose to show or hide columns in the device list. For example, you might not care which version of the protection agent was used to discover a device, so you can hide it from view.

To show/hide columns, click the Columns icon and then choose which columns to include. For a description of each column, see the Protection page.



Policies Description

Policies Overview

Aranda Datasafe needs to know which files it wants to protect and back up. Provide these instructions by setting up a Policy.

A policy is a set of rules that define:

- Protected data: What data is selected for protection and backup.
- Backup and restore options: How often backups are performed.
- DLP: If any data loss prevention features are used to protect your data in the event of a device being lost or stolen. These include local encryption, data theft prevention, and geolocation.
- Migration: Whether Windows user profile settings can be backed up for migration to other devices.

You can create as many policies as you need. You can have one Policy for everyone, or you could have different Policies for each department in your organization.

To view, create, and edit policies, you'll use the Policy Page and the Policy Editor Page.

Policies

The Policies page provides access to the Policies in Aranda Datasafe. You can use it to:

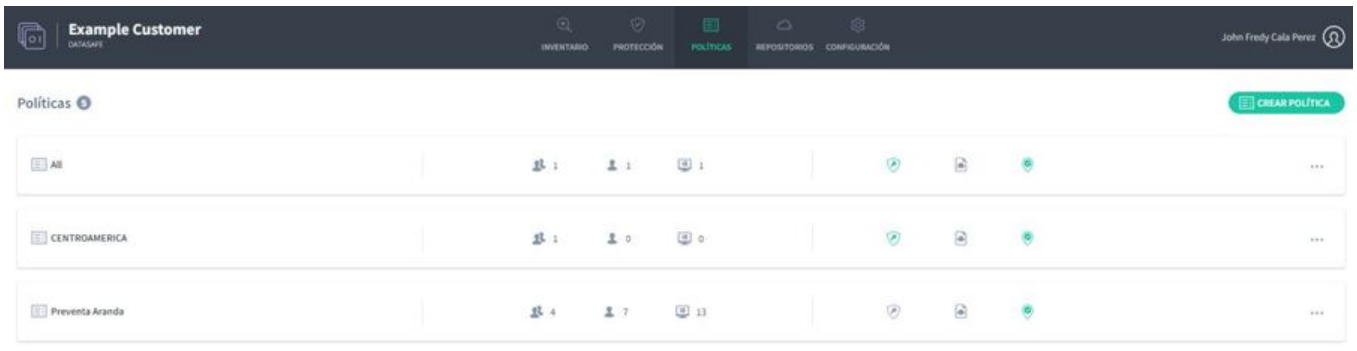
- View a list of policies
- View or edit a policy
- Create a policy
- Delete a policy

Click **Policies** to display the Policies page.

Policy List

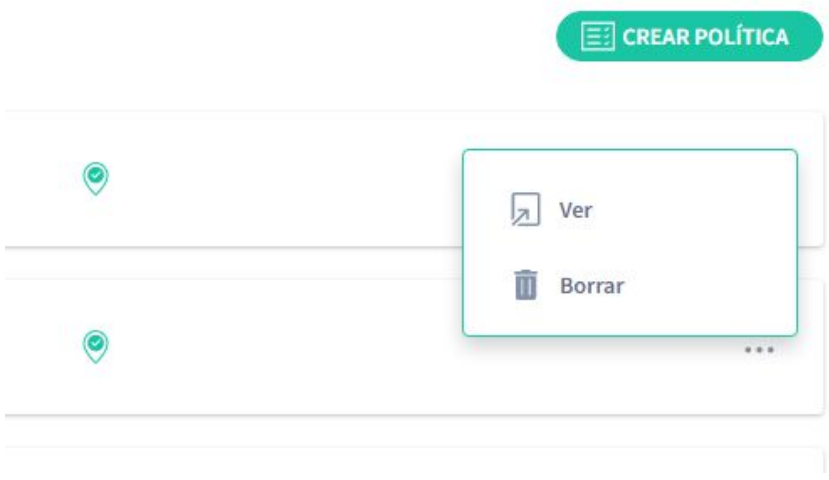
When you display the Policies page, it presents you with a list of the Policies that are currently in Aranda Datasafe.

The name of the Politics is shown on the left and there are a number of icons.



Icon	Description
	Number of teams using the policy.
	Number of user accounts associated with the Policy.
	Number of devices associated with the Policy.
	The status of the encryption function (green = local encryption on, gray = local encryption disabled)
	The status of the auto-revoke function (green = on, gray = off).
	The status of the geolocation function (green = on, gray = off).

On the right side of the row, there is a context menu (...). If you click on it, you can choose to view the policy or delete it.



View or edit a policy

To view or edit a policy, click the policy name or use the View option in the context menu.

When you view or edit a policy, its details are displayed on the policy editor page.

Policy Editor

Use the policy editor page to view and edit various settings for a policy, including:

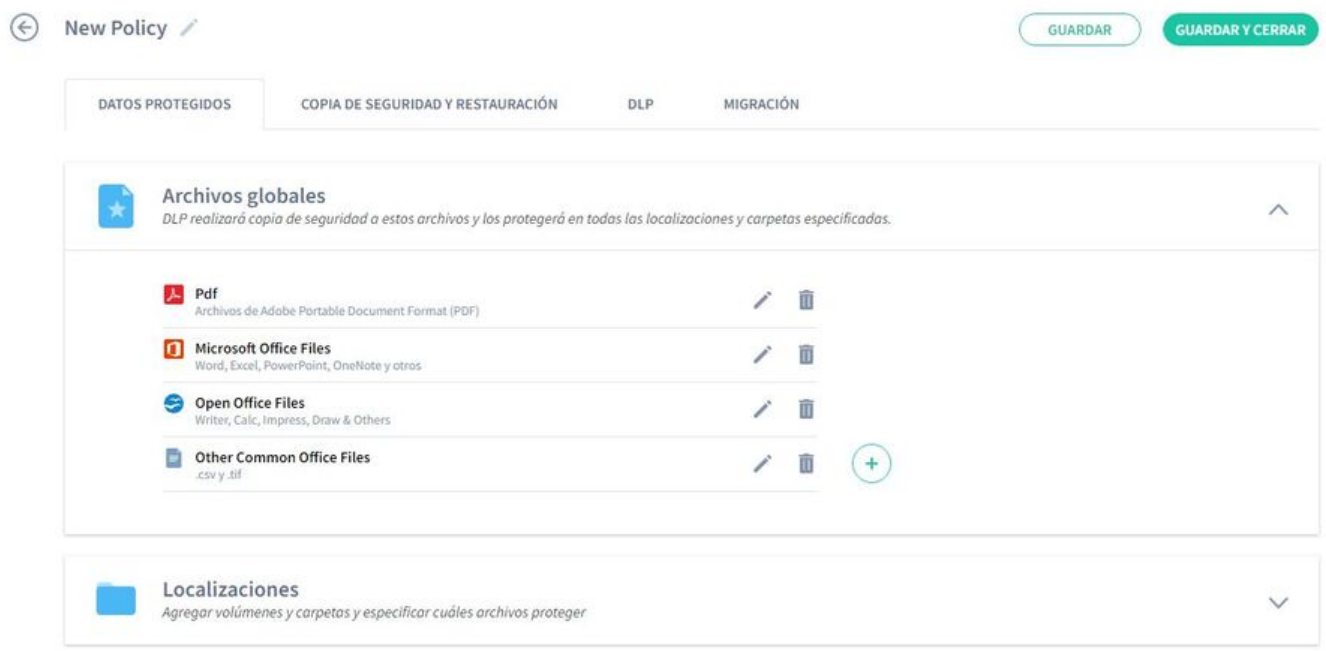
- What types of data are backed up and protected
- Which locations are protected and supported
- Which email is protected and backed up
- What data is not protected or backed up
- When automatic backups will be performed
- What data loss prevention features are used
- What data migration features are used.

To display the policy editor page, click**Policies**.

- Protected data
- Restore backup
- DLP (Data Loss Prevention)-Migration.

Protected Data

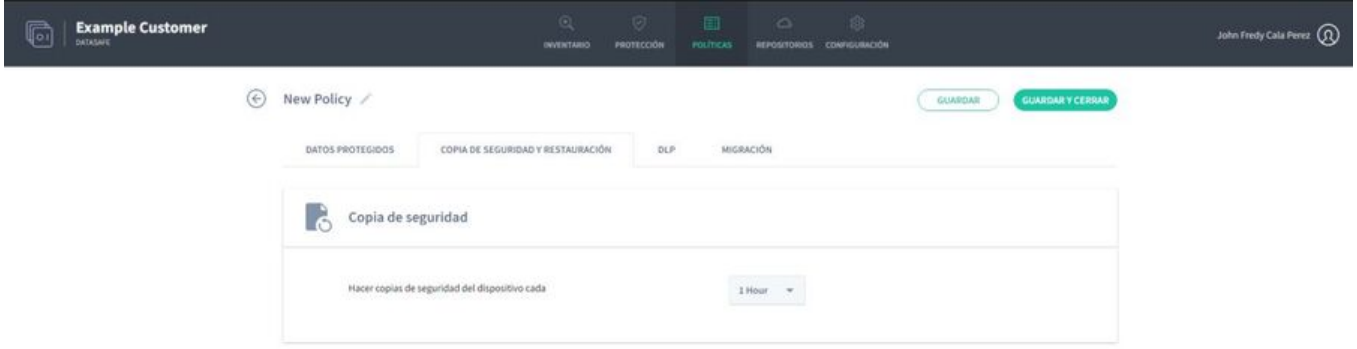
Use the Protected Data settings to choose which file types and file locations will be backed up or excluded from your backups.



Settings	Description	View Article
Global Archives	Global files are groups of file types, for example, there is a global file group for Microsoft Office files. You can add, edit, or delete groups of global file types.	Choose which file types are "global files"
Locations	Choose which volumes and folders Aranda Datasafe will backup and protect. For each location, you can choose which files are backed up (all, global, and custom	Choose which locations are protected
Cloud Drives	Choose which cloud drives Aranda Datasafe will backup and protect. For each cloud drive, you can choose which files are backed up (all, global, and custom).	Choose which cloud drives are protected
Emails	Choose which email files Aranda Datasafe will backup and protect.	Email backup and protection
Global Exclusions	Use it to define any file type or location that Aranda Datasafe should not back up or protect.	Exclude files and folders from backup and protection

Backup and Restore

Use the Backup & Restore settings to schedule automatic backups.

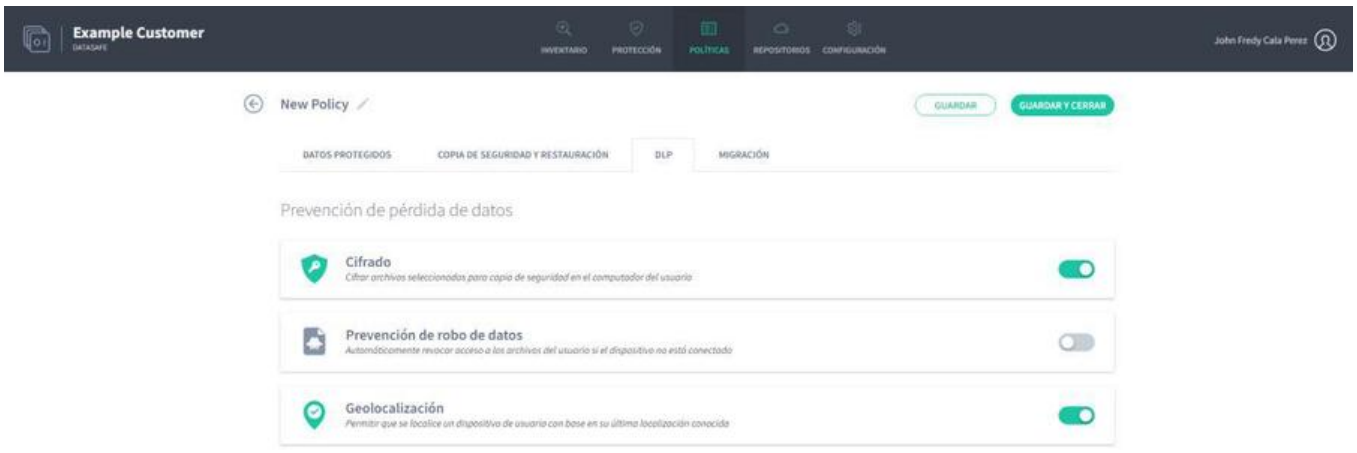


You can choose to run backups every:

- 1 hour
- 2 hours
- 4 hours
- 8 hours.

DLP (Data Loss Prevention)

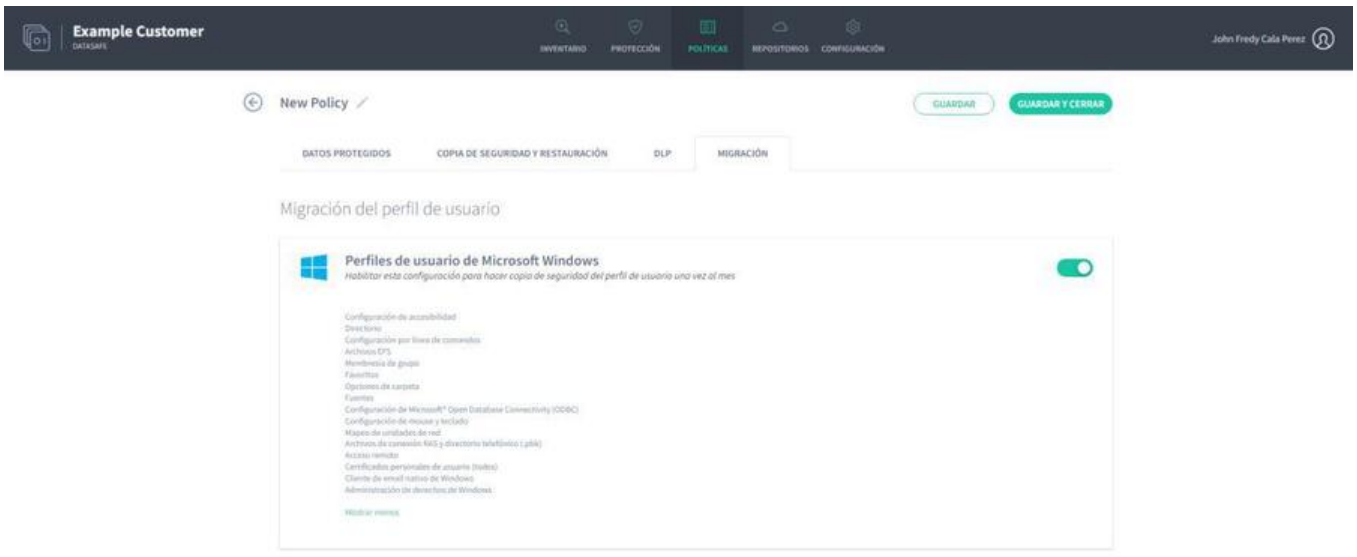
Use the DLP settings to choose which data loss prevention features you want the Policy to use.



Settings	Description	View Article
Encryption	You can enable local encryption to encrypt data on each device. Unauthorized users will not be able to view the encrypted files.	Enable local encryption
Information Theft Prevention	<p>If a device does not connect to Aranda Datasafe within a certain period of time, Aranda Datasafe may revoke access to the files on the device. While revoked, the user cannot access the protected data. Use Data Theft Prevention to turn this feature on or off.	Enable data theft prevention.
Geolocation	You can enable geolocation for devices. If you enable geolocation, you can use Aranda Datasafe to view a map of a device's last known location.	Enable geolocation

Migration

Use migration settings to enable or disable migration of user profile settings for a policy



The User Profile Migration feature is designed to be used when you are replacing a device. Instead of setting up your new device from scratch, you can use Restore to load it with another device's user profile and settings.

Create Policies

A policy is a set of rules that define:

- What data is protected and backed up
- How often backups occur
- If any data loss prevention features are used to protect your data in the event of a device being lost or stolen
- If the Windows profile configuration information is backed up.

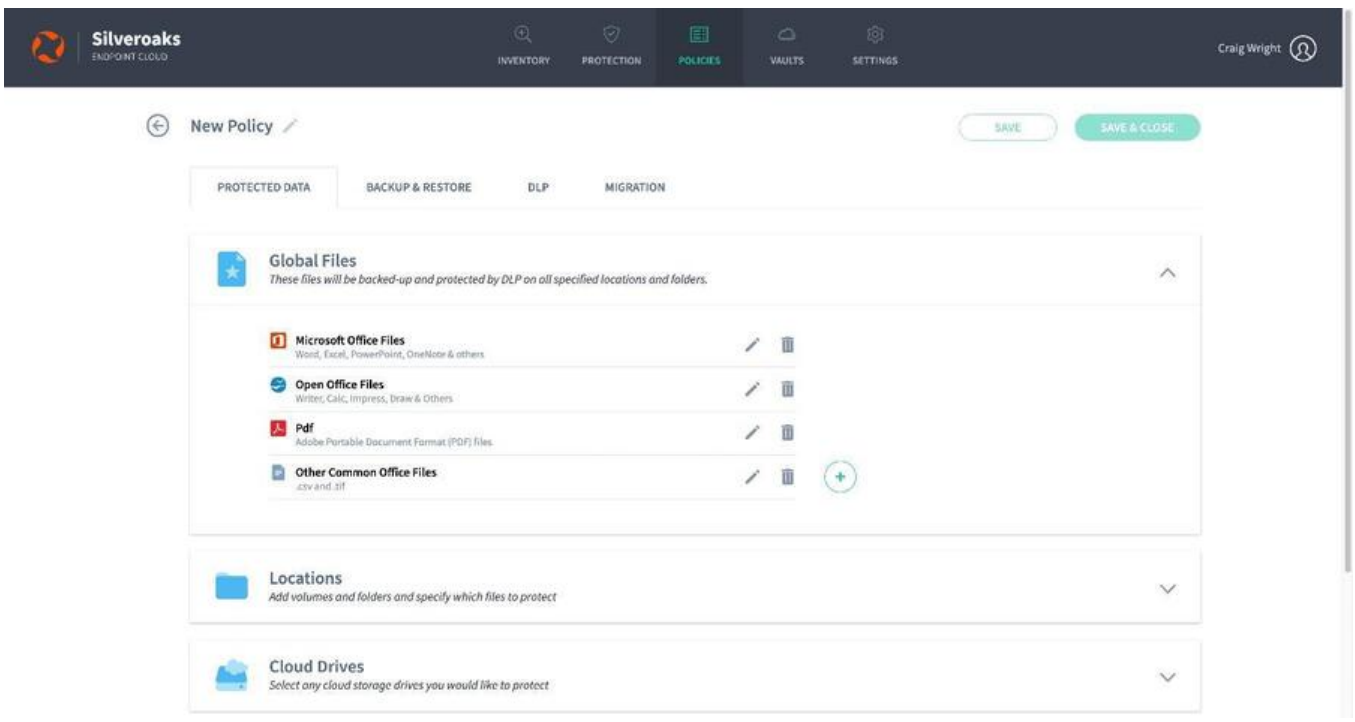
You can create as many policies as you need. You can have one Policy for everyone, or you can have different Policies for each team.

To create a new policy:

1. Click on **Policies**.

If you don't have any policies in Aranda Datasafe, click **Add a Policy**. If you already have some policies, click **Create Policy**.

Aranda Datasafe creates a new Policy and opens it, ready for you to define its configuration.



2. Give a name to the Policy. Click the edit icon next to the default name, and then enter the new name.

Their new Policy has default settings, and many Aranda Datasafe administrators find these settings to be suitable for their needs. If you have different requirements, you can change the settings in the following sections:

- **Protected data**: Used to define what data is encrypted and backed up.
- **Backup & Restore**: Used to choose how often backups are made.
- **DLP**: Used to choose data loss prevention measures for the policy.
- **Migration**: Used to choose whether to back up settings related to Windows user profiles.

Edit Policies

If you want to make changes to an existing policy:

1. Click on **Policies**.

2. Click on the Policy you want to change.

Aranda Datasafe opens the policy editor page, which you can use to change the policy settings.

You can change the settings in the following sections:

- **Protected data**: Used to define what data is encrypted and backed up.
- **Backup & Restore**: Used to choose how often backups are made.
- **DLP**: Used to choose data loss prevention measures for the policy.
- **Migration**: Used to choose whether to back up settings related to Windows user profiles.

Delete Policies

If you no longer need a Policy or have created a Policy by mistake, you can delete it.

Caution: If you delete a policy that is associated with computers and devices, those computers and devices will no longer have a policy assigned to them. This means that they won't be backed up automatically, and other features, such as geolocation, won't be available.

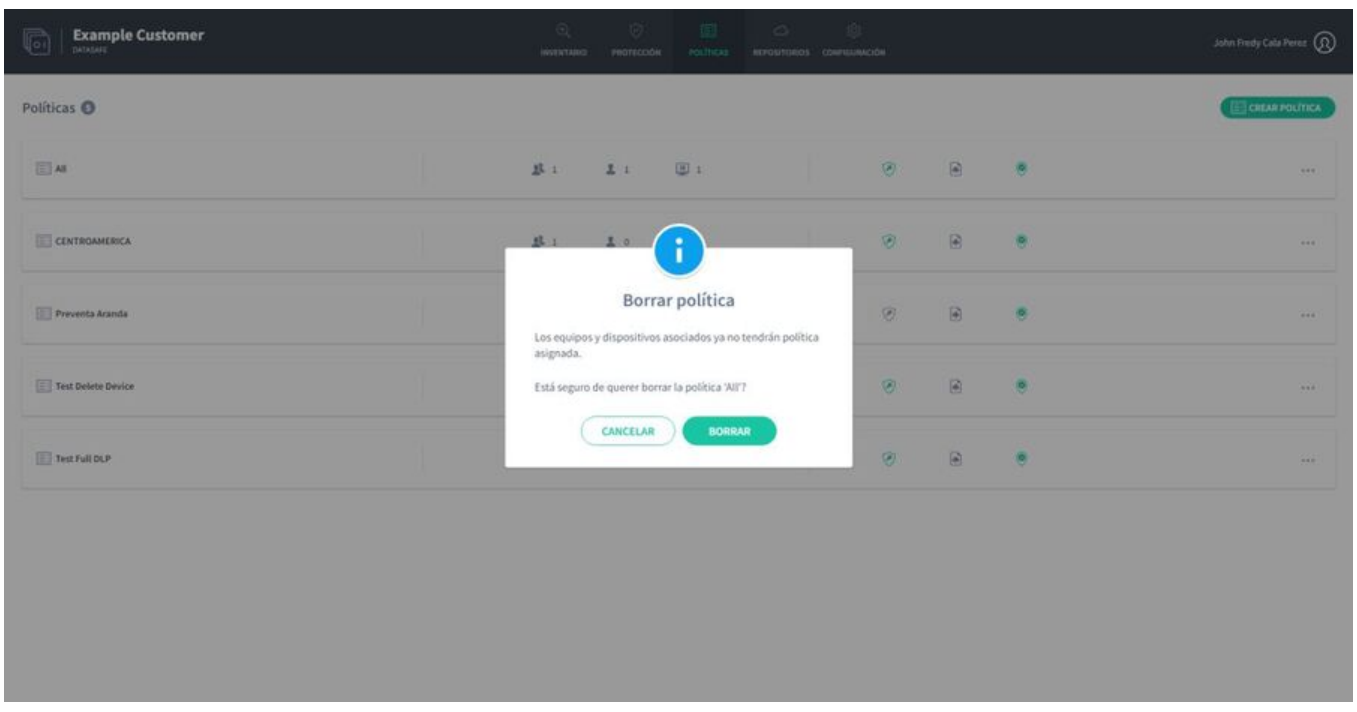
To delete a policy:

1. Click Policies to display the Policies page . 2. In the Policies list, find the Policy you want to delete.

3. Click on the radio button (...) of the Policy.

4. Click Delete.

5. When prompted, click Delete to confirm.



Global Archives

You can use the **Global Files** feature to create collections of file types. It makes it much faster to choose which files are backed up, because instead of having to choose each file type separately for each location, you can choose a collection of Global Files.

For example, by default, each policy has a collection of Microsoft Office files from global files. This collection includes files saved in Word, Excel, PowerPoint, etc. When you choose which file types should be backed up, you can choose the Global Files collection instead of having to select each MS Office file type separately.

You can use the Global Files setting in a policy to:

- Add or remove file types from the different global file collections
- Create a new collection for different file types. For example, you might want to create a new collection that contains the file types for your proprietary software.

Change an existing collection of global files

To make changes to an existing collection of global files:

1. Open the Policy Editor for the Policy you want to change (click **Policies** and then click Policy).

2. Make sure the **Protected Data** tab is displayed.

3. In the list of **Global Files**, find the collection of Global Files you want to change and click on the Edit icon (pencil).

4. Use the **Edit File Type Name** field to rename the global file collection, if necessary.

5. Use the **Add or Remove Extensions** box to add or remove file extensions.

To add a file extension, click an empty part of the box and enter the characters of the file extension. Press Enter and a blue block will appear for your new extension type. Click **Save Changes** to confirm.

To remove a type of file extension, click the X in the corresponding blue block. Click **Save Changes** to confirm.

Add a new global file collection

To add a new global file collection:

1. Open the Policy Editor for the Policy you want to change (click **Policies** and then click **Policy**).

2. Make sure the **Protected Data** tab is displayed.

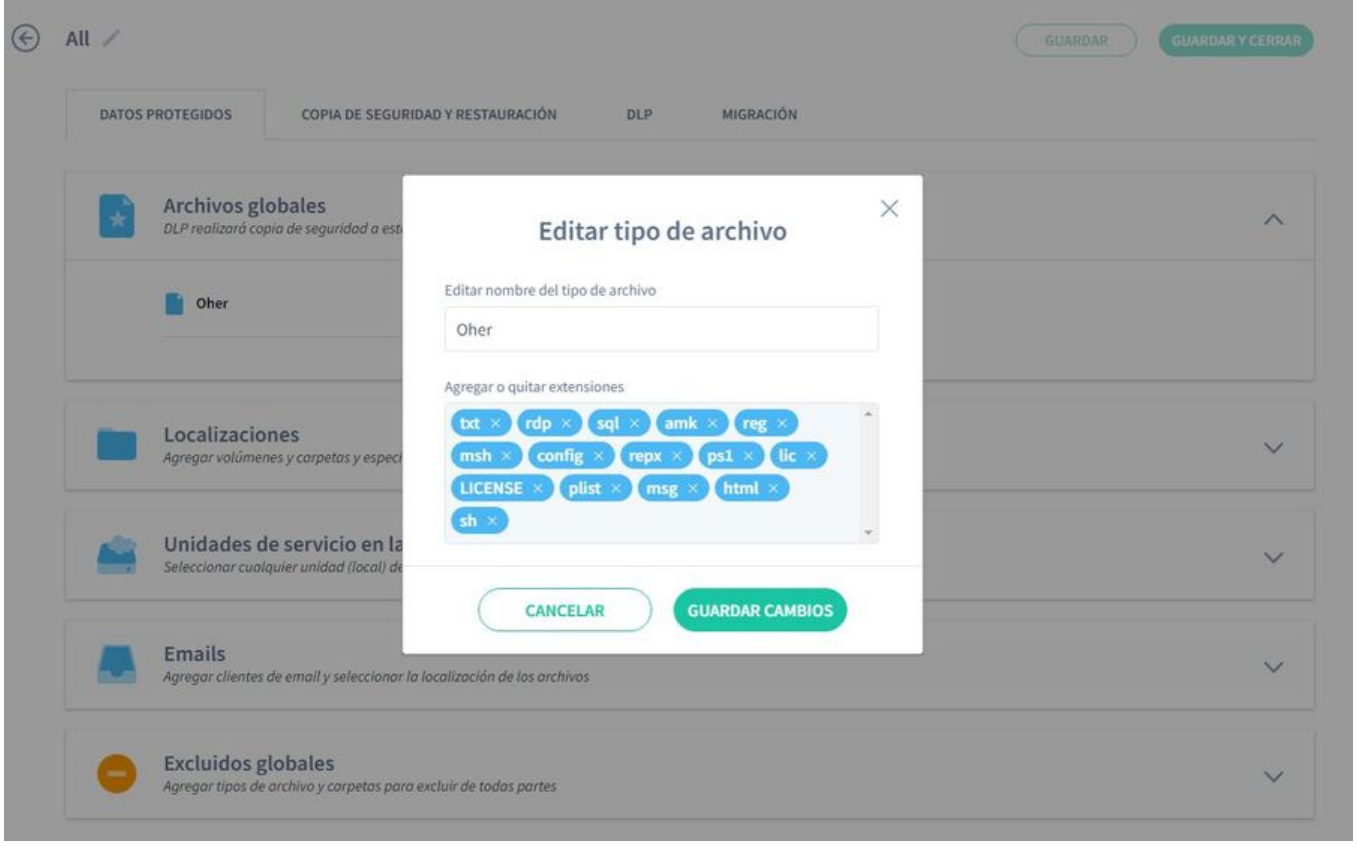
3. In the Global Files section of the **Protected Data** tab, click the plus (+) icon to display the Add File Type dialog box.

4. Use the **Select a file type** option to set the name of your new global file collection. You can choose from the list of available file types, or you can select Add New File Type.

5. If you selected **Add New File Type** in step 2, enter the name of the new global file collection in the **Edit File Type Name** field. If you choose an existing file type, you can edit the name or leave it as is.

6. Use the **Add or Remove Extensions** box to add or remove file extensions from the new global file collection. This works in the same way as when editing a collection of global files (see above).

7. Click **Save Changes**.



Delete a collection of global files

To delete a collection of Global Files from Aranda Datasafe:

1.Open the Policy Editor for the Policy you want to change (click**Policies** and then click Policy).

2. Make sure the**Protected Data** tab is displayed.

3.In the list of**Global Files**, find the collection of Global Files you want to delete and click on its trash can icon.

Protected Locations

You can configure Aranda Datasafe to back up and protect files in specific locations on a computer (local drives only, by default). Some common locations are included by default, including All Volumes, Desktop, and Documents, and you can add other locations if needed.

To choose the locations to protect, use the**Locations** setting in a Policy. For each location, you can choose which files are backed up and protected:

- All files
- global files only
- files that you choose manually.

You can use the Locations section to:

Add a location.

Edit a location.

Delete a location.

Add Location

1. Open the Policy Editor for the Policy you want to change (click Policies, and then click Policy).

2. In the**Protected Data** tab, expand the**Locations** settings.

3. Click the plus (+) icon to display a context menu. The context menu has options for some commonly protected locations, including Downloads and Videos. To add your own location, click **Add New Location**.

4. Enter a meaningful location name so that other people understand where this location is.

5. In the **Path** field, enter the folder location of the files you want to protect.

6. If you want to include multiple folders, click the plus (+) icon to **Add another path**. This creates another path field.

7. Click **Save Changes** to confirm.

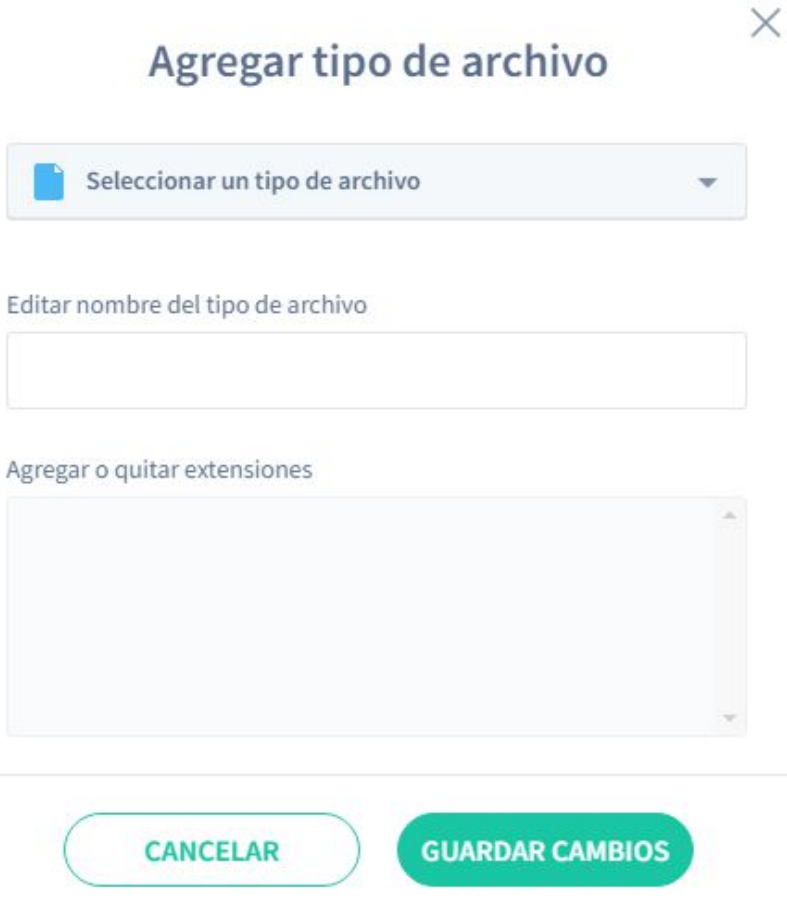
8. Choose whether you want to protect **All files**.

If you enable this feature, all files in the location will be protected, with the exception of any excluded file type (global file excludes or custom file selection excludes). If you turn it off, you can choose which files to protect.

9. Choose whether you want to protect the **global sources** for this location. If you enable this feature, all global types will be backed up and protected. If you turn it off, global file types won't be included (unless you add them as custom file sections in the next step).

10. . Use Custom File Selection to include or exclude any particular file type for this location. If you enable this feature, you can use the Includes and Exclude section (see the steps below). For example, you can choose to include a collection of global files instead of all global file types.

In the **Includes** section, click on **Add File Type**.



11. Use the Add File Type dialog box to choose the file types you want to protect for this location. You can choose any of your global file collections and then **Add or Remove Extensions** to specify which file types will be backed up.

Alternatively, you can click **Add New File Type** to create your own custom selection (enter the name in the **Edit File Type Name** field and use **Add or Remove Extensions** to choose file types). Click **Save Changes** to confirm.

12. In the Exclusions section, use **Add File Type** to Exclude to choose any file type that should not be protected for this location. For example, if you want Aranda Datasafe to protect all global files except PDFs, the fastest way is to enable Global Files for the location and then exclude PDFs.

Use the Add File Type dialog box to choose the file types that you don't want to be protected for this location.

You can choose any of your global file collections, and then add or remove extensions to specify which file types to exclude. Alternatively, you can add a new file extension to exclude it. Click Save Changes to confirm.

13. In the **Exclusions** section, use **Add a folder to exclude** to choose specific folders that should not be protected for this location. Click Add a folder to exclude to display a context menu. You can then choose System Folders, Temporary Folders, or Add a New Folder. If you add a new folder, the Add Folder dialog box appears, and you can set the folder name and path(s).

Click Save Changes to confirm that the folders will not be protected.

14. Click on **Save Change**.

edit location

To make changes to an existing location:

1. Open the Policy Editor for the Policy you want to change (click **Policies** and then click Policy).

2. In the **Protected Data** tab, expand the **Locations** settings.

3. Click the Edit icon (pencil) for the Location you want to change.

4. Use the settings of **All Files, Global Files, and Custom File Selection** to make the changes. These work in the same way as when you add a location (see above).

5. Click **Save Changes**.

delete location

To remove a location from a policy:

1. Open the Policy Editor for the Policy you want to change (click **Policies** and then click Policy).

2. **On the Protected Data tab, expand the Locations settings**

3. Click on the trash can icon of the location you want to delete.

Protected Cloud Drives

You can configure Aranda Datasafe to back up and protect files on cloud storage services, such as One Drive, Google Drive, and Dropbox.

To choose which cloud services to protect, use the **Cloud Drives** setting in a Policy. For each cloud drive, you can choose which files are backed up and protected:

- All files
- global files only
- files that you choose manually.

Add a cloud drive

To add a cloud drive to a policy so that it is protected:

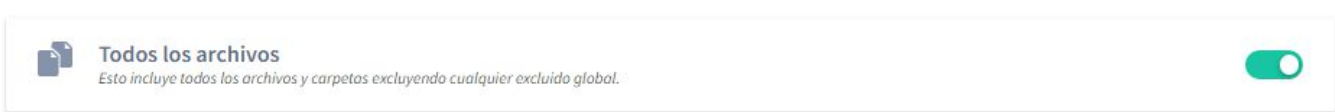
1. Open the Policy Editor for the Policy you want to change (click **Policies** and then click Policy).

2. In the **Protected Data** tab, expand the **Cloud Drives** settings.

3. Click the plus (+) icon to display a context menu.

4. Choose the cloud drive you want to add, for example, One Drive.

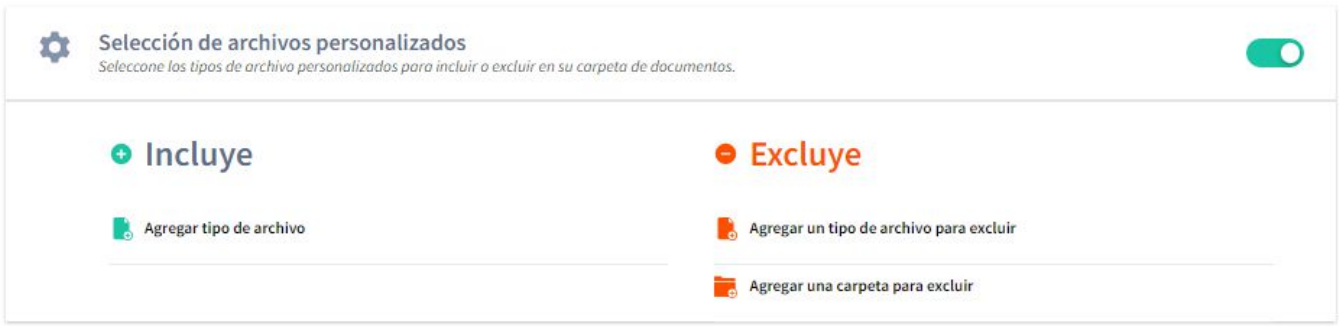
5. Choose whether you want to protect **All files**.



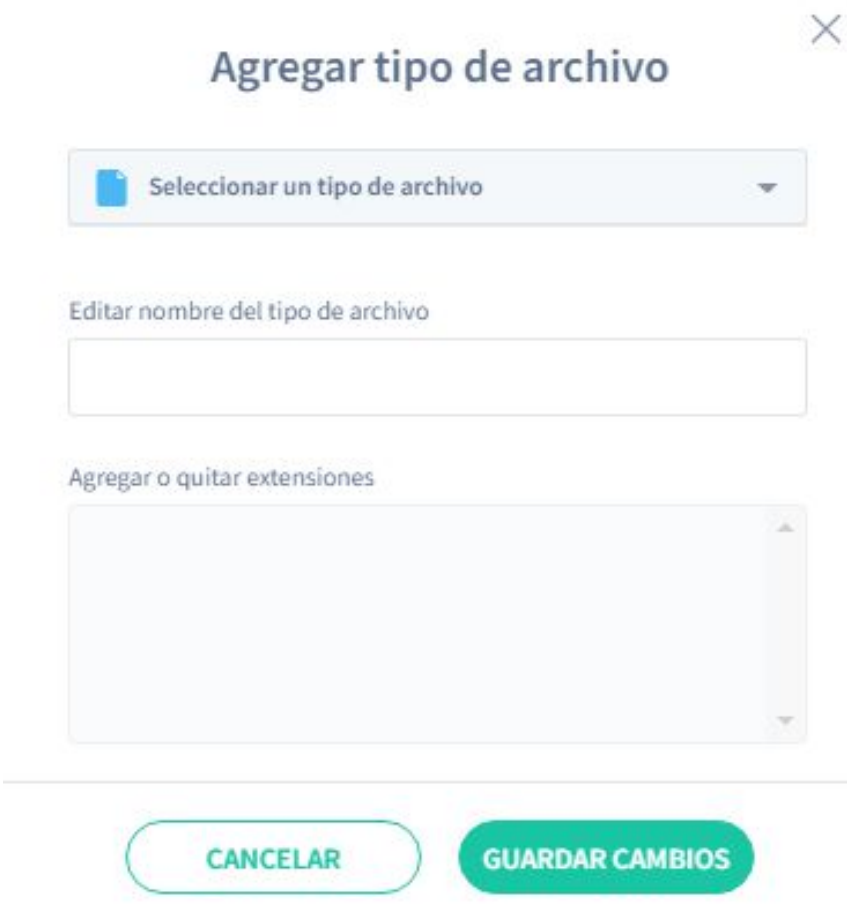
If you enable this feature, all files on the cloud drive will be protected, with the exception of any excluded file type (global file excludes or custom file selection excludes). If you turn it off, you can choose which files to protect.

6. Choose whether you want the **global files** to be protected for this cloud drive. If you enable this feature, all global types will be backed up and protected. If you turn it off, global file types won't be included (unless you add them as custom file sections in the next step).

7. Use the **custom files** selection to include or exclude any particular file type for this cloud drive. If you enable this feature, you can use the **Inclusions and Exclusions** section (see next steps). For example, you can choose to include a collection of global files instead of all global file types.



8. In the **Inclusions** section, click on **Add File Type**.



Use the Add File Type dialog box to choose the file types you want to protect for this cloud drive. You can choose any of your global file collections and then **Add or Remove Extensions** to specify which file types will be backed up.

Alternatively, you can click **Add New File Type** to create your own custom selection (enter the name in the **Edit File Type Name** field and use **Add or Remove Extensions** to choose file types). Click **Save Changes** to confirm.

9. In the **Exclusions** section, use **Add File Type** to Exclude to choose any file type that should not be protected for this cloud drive. For example, if you want Aranda Datasafe to protect all global files except PDFs, the fastest way is to enable Global Files for the cloud drive and then exclude PDFs.

Use the **Add File Type** dialog box to choose the file types that you don't want to be protected for this cloud drive.

You can choose any of your global file collections, and then add or remove extensions to specify which file types to exclude. Alternatively, you can add a new file extension to exclude it. Click **Save Changes** to confirm.

10. In the **Exclusions** section, use **Add a folder** to exclude to choose specific folders that should not be protected for this cloud drive. Click Add a folder to exclude to display a context menu. You can then choose System Folders, Temporary Folders, or Add a New Folder. If you add a new folder, the Add Folder dialog box appears, and you can set the folder name and path(s).

Click **Save Changes** to confirm that the folders will not be protected

Edit a cloud drive

To make changes to an existing cloud drive:

1. . Open the Policy Editor for the Policy you want to change (click **Policies** and then click Policy).

2. In the **Protected Data** tab, expand the **Cloud Drives** settings.

3. Click the Edit icon (pencil) of the cloud drive you want to change.

4. Use the settings of **All Files, Global Files, and Custom File Selection** to make the changes. These work in the same way as when you add a cloud drive (see above).

5. Click **Done**.

Delete a cloud drive

To remove a cloud drive from a policy:

1. Find the Policy you want to change in the Policy Editor (click **Policies** and then click Policy).

2. In the **Protected Data** tab, expand the **Cloud Drives** settings.

3. Click the trash can icon of the cloud drive you want to delete.

Email Protection and Backup

You can configure Aranda Datasafe to back up and protect your email client files. For example, you can add Microsoft Outlook as an email client and then configure Aranda Datasafe to back up and protect all Outlook PST files or only those PST files that are active.

The email settings are in the policy that is used to back up your device.

Add an email client for backup

To add an email client:

1. Open the Policy Editor for the Policy you want to change (click Policies, and then click Policy).

⚐ > Note: The policy editor is automatically displayed when you create a new policy.

2. Make sure the **Protected Data** tab is displayed.

3. Expand the **Emails** section.

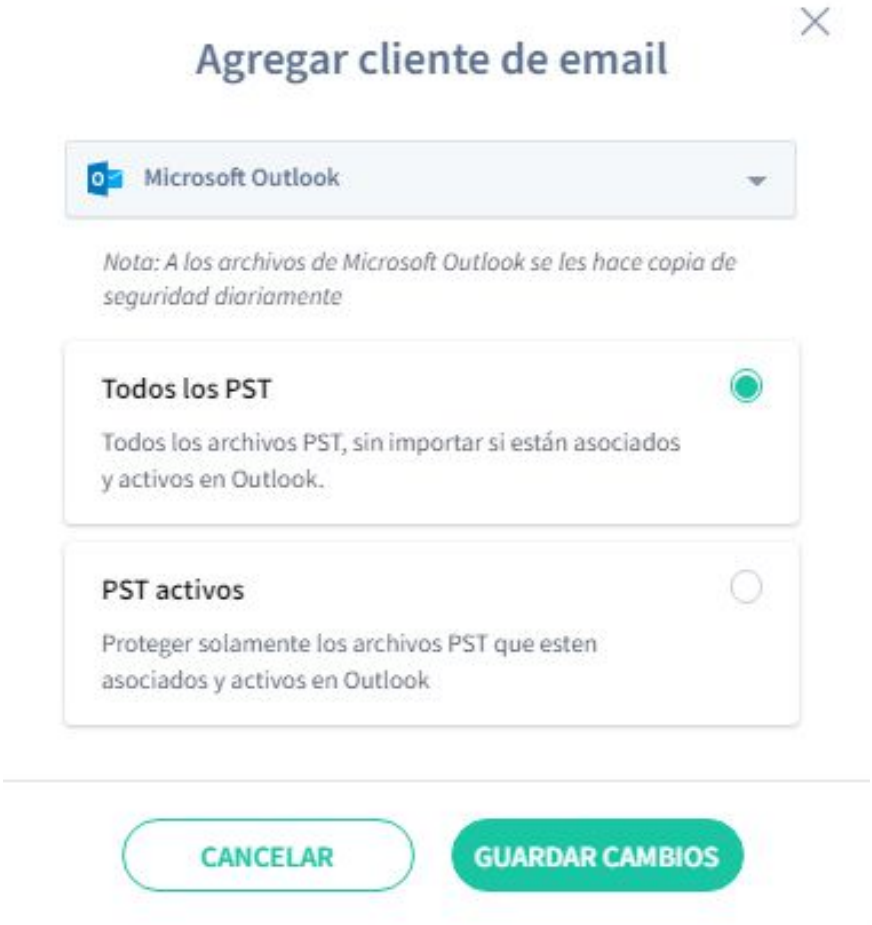
4. Click the plus (+) icon.

5. Select the email client, for example, Microsoft Outlook.

6. Choose which PST files you want to backup:

- All PST files: Aranda Datasafe will back up all PST files, even if they are inactive or not associated with the email client.
- Active PST: Aranda Datasafe will only back up PST files that are associated with the email client and are currently active in the Outlook profile.

7. Click **Save Changes**.



Edit an email client

To make changes to an existing email client:

1. Open the Policy Editor for the Policy you want to change (click **Policies** and then click Policy).

2. Make sure the **Protected Data** tab is displayed.

3. Expand the **Emails** section.

4. Click the Edit icon (pencil) of the email client you want to change.

5. Use the Edit Email Client dialog box to choose which files are backed up:

- **All PST files**: Aranda Datasafe will back up all PST files, even if they are inactive or not associated with the email client.
- **Active PST**: Aranda Datasafe will only back up PST files that are associated with the email client and are currently active.

6. Click **Save Changes**.

Delete an email client

To delete an email client:

1. Open the Policy Editor for the Policy you want to change (click Policies, and then click Policy).

2. Make sure the Protected Data tab is displayed.

3. Expand the Emails section.

4. Click the Trash icon of the email client you want to delete.

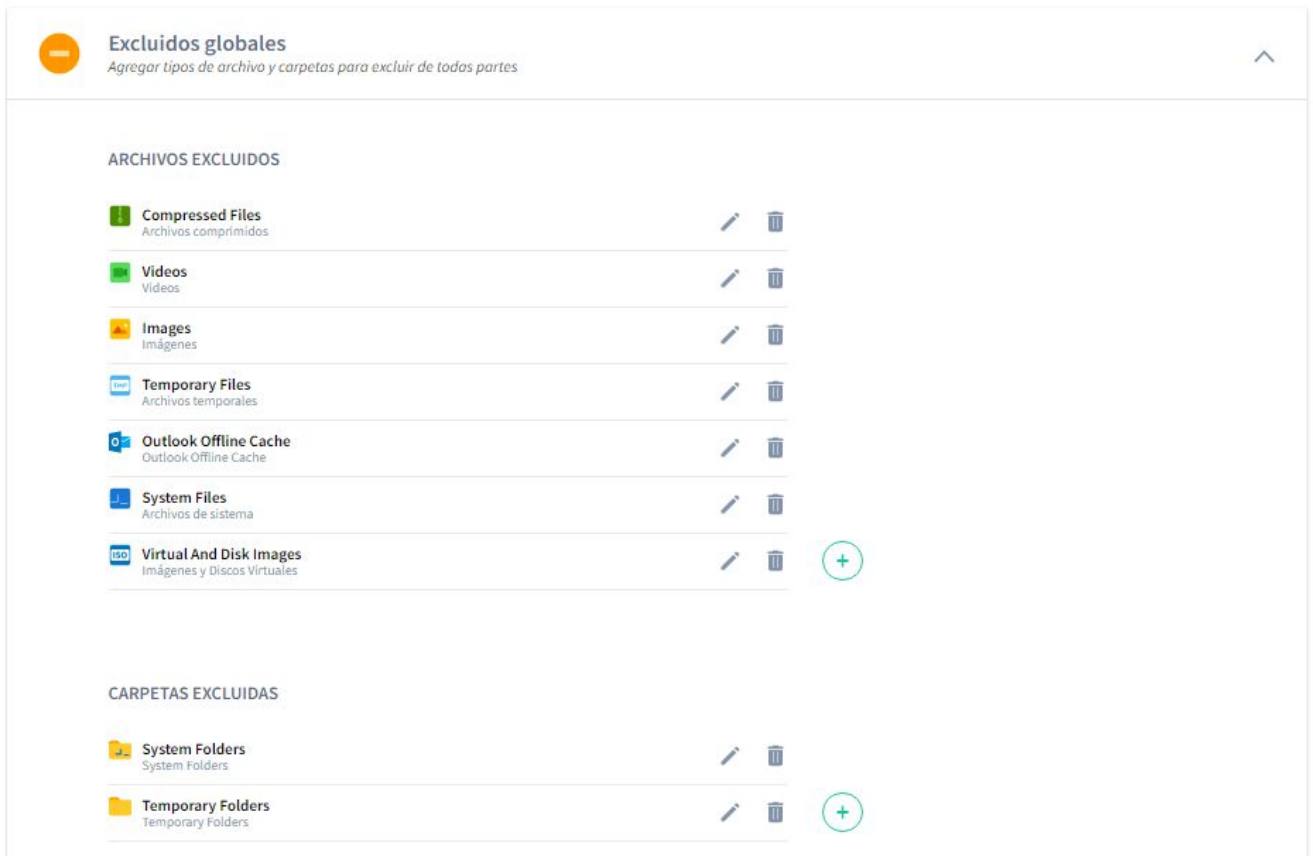
Exclude files and folders from backup and protection

You may want to exclude certain types of files from Aranda Datasafe backup and protection. For example, you can exclude image files, videos, and music. You can also exclude certain folders.

There are two ways to exclude files and folders:

- You can exclude for a specific location
- You can exclude for all locations.

In this article, we explain how to use the Global Exclusions feature to exclude files and folders from all locations. The Global Exclusions feature is useful when you know that there are certain file types that you never want to be protected for any one location. Allows you to create a group of file types that you can exclude for all locations in a single action.



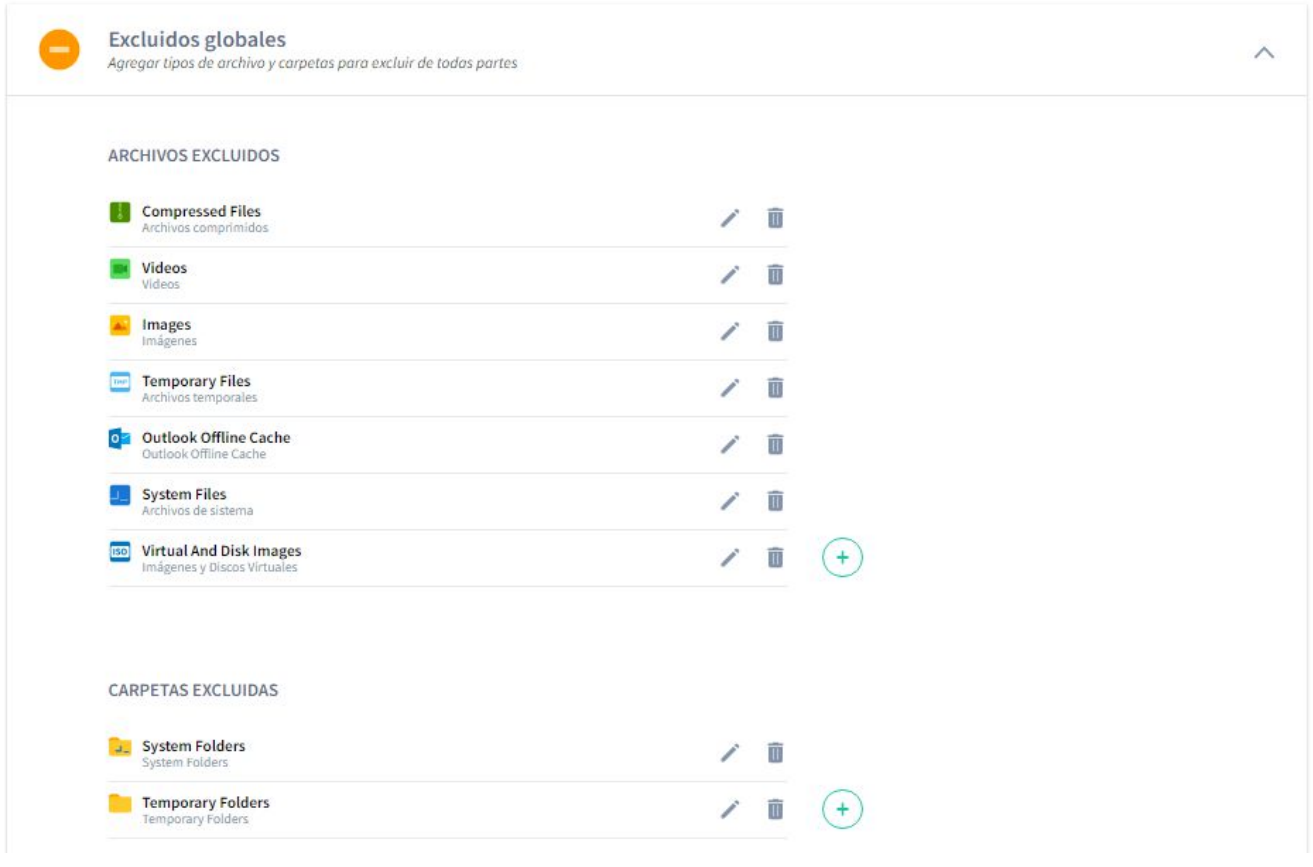
To learn how to exclude files for a specific location, see [Choose which files and folders] are protected.

Exclude files from protection for all locations

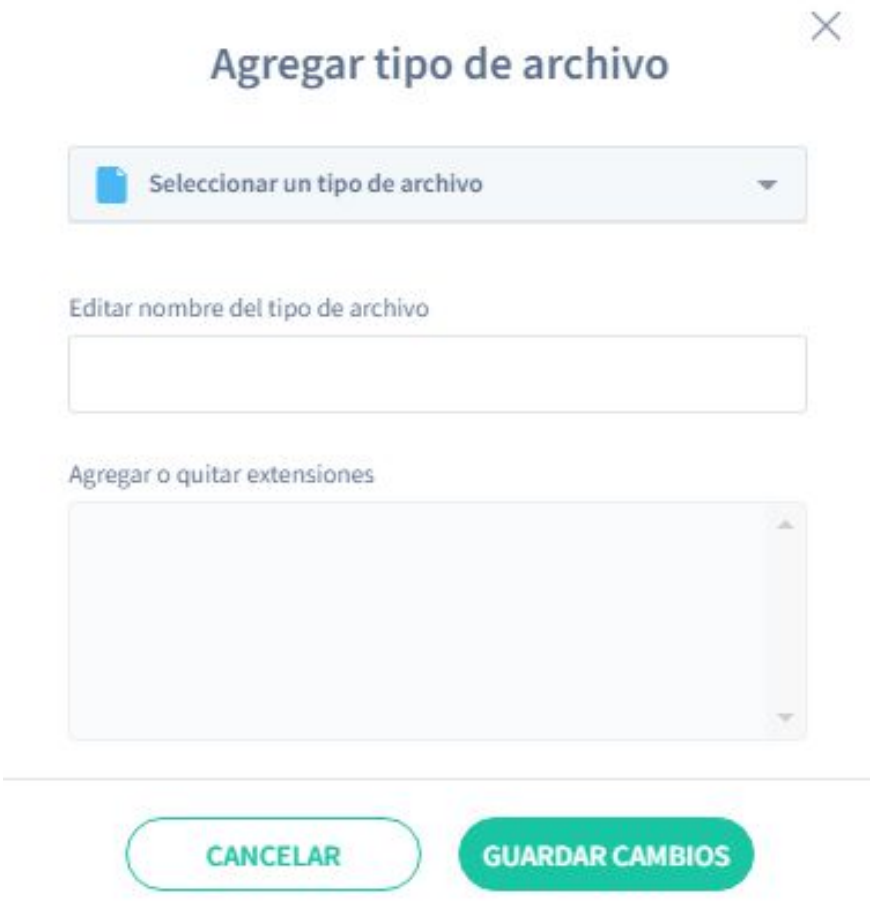
To prevent certain file types from being backed up and protected for all locations:

1. Open the Policy Editor for the Policy you want to change (click **Policies** and then click Policy).

2. In the **Protected Data** tab, expand the **Global Exclusion** settings.



3. In the Excluded Files section, click the plus (+) icon to display the Add File Type dialog box.



4. Use the **Select a file type** option to set the name of your new global filegroup. You can choose from the list of available file types or you can select **Add new file type**.

5. If you selected **Add New File Type** in step 4, enter the name of the new Global Files group in the **Edit File Type Name** field. If you choose an existing file type, you can edit the name or leave it as is.

6. Use the **Add or Remove Extensions** box to add or remove file extensions from the new Global Files group. File extensions that you add to the box will be excluded; Aranda Datasafe will not protect these file types for devices that use this Policy.

7. Click **Save Changes**.

Edit global file exclusion rules

To change the files that are included in global exclusions:

1. Open the Policy Editor for the Policy you want to change (click **Policies** and then click Policy).

2. Make sure the **Protected Data** tab is displayed.

3. In the list of **global exclusions**, find the group you want to change and click on the **Edit** icon (pencil).

4. Use the **Edit File Type Name** field to rename the group, if necessary.

5. Use the **Add or Remove Extensions** box to add or remove file extensions.

To add a file extension, click an empty part of the box and enter the characters of the file extension. Press Enter and a blue block will appear for your new extension type. Click **Save Changes** to confirm.

To remove a type of file extension, click the X in the corresponding blue block. Click **Save Changes** to confirm.

Exclude folders from protection for all locations

You can exclude folders from Aranda Datasafe protection. For example, your users may have personal data folders where they store non-business data, and you don't want this information backed up.

To exclude folders from all locations:

1. Open the Policy Editor for the Policy you want to change (click **Policies** and then click Policy).

2. Make sure the **Protected Data** tab is displayed.

3. In the **Global exclusions** section, click on the plus (+) icon.

4. You can choose System Folders or Temporary Folders, or click Add New Folder to choose a specific folder. If you add a new folder, the Add Folder dialog box appears, and you can set the folder name and path(s).

5. Click **Save Changes**.

Edit the excluded folders

If you have set Excluded Folders in Global Exclusions for a policy, you can edit them to:

- Rename the folder
- Change the path
- Add additional routes.

To edit global exclusion folders:

1. Open the Policy Editor for the Policy you want to change (click **Policies** and then click Policy).

2. Make sure the **Protected Data** tab is displayed.

3. In the **Global Exclusions** section, click the Edit icon (pencil) of the global exclusion group you want to change.

4. Use the **Folder Name** field to change the name of the group.

5. Use the **Path** fields to change folder locations.

6. Click **Save Changes**.

Remove files or folders from global exclusions

To remove files or folders from a policy's global exclusions:

1. Open the Policy Editor for the Policy you want to change (click **Policies** and then click Policy).

2. Make sure the **Protected Data** tab is displayed.

3. In the Global Exclusions section, click the trash can icon for the global exclusion group or folder you want to delete.

When you delete a group of files or folders from global exclusions in a policy, they are no longer excluded from Aranda Datasafe protection. (Unless they're also excluded in the Location settings.)

Schedule Automatic Backups

Aranda Datasafe will automatically back up devices that use a Policy. The first backup is done about 10 minutes after a device is first activated, and after that, backups run on a regular schedule.

You can set the schedule in the **Backup & Restore** settings for a Policy.

Set the schedule for automatic backups

1. Open the Policy Editor for the Policy you want to change (click **Policies** and then click Policy).

2. Click on the **Backup & Restore** tab.

3. Use the Run device backups option in all options to choose how often automatic backups will be performed. You can choose:

- 1 hour
- 2 hours
- 4 hours
- 48 hours
- Click **Save** or **Save & Close** to confirm.

Example: If you have a 'Finance' policy and have set it to back up every 2 hours. It also has a 'Finance' team and has been assigned the 'Finance' policy.

The Finance team's devices will have their data backed up automatically every 2 hours (since that's the schedule defined in the policy used by their team).

For devices on other computers, the backup schedule might be different, as your computers may use a different policy that is configured to back up at a different time, such as every 8 hours.

Enable Local Encryption

Prerequisites: Before enabling DLP features, make sure that Active Directory Certificate Services have been configured.

You can configure the policy to enable encryption of files that are on the user's devices. We call this "local file encryption".

Once enabled, each device that uses the Policy will receive a certificate (also known as a key) and local encryption will be applied. Only authenticated users can access data on a device if the certificate is available.

The certificate is used to control access to data on a device. By revoking the certificate in Aranda Datasafe, you delete it from the device and the data on the device becomes inaccessible.

If you enable the **Data Theft Prevention** feature, the certificate is automatically revoked on devices that do not connect to Aranda Datasafe within a certain period of time (see Enabling Data Theft Prevention).

To enable or disable local file encryption in a policy:

1. Open the Policy Editor for the Policy you want to change (click **Policies** and then click Policy).

2. Click on the **DLP** tab.

3. Use the **Encryption** slider to enable or disable local file encryption (green is enabled, gray is disabled).

4. Click **Save or Save & Close** to confirm.

Enable Data Theft Prevention

With Aranda Datasafe's **data theft prevention** feature, you can configure devices to revoke file access if they don't connect with Aranda Datasafe within a certain period of time. To revoke a device, Aranda Datasafe removes the device's encryption certificate.

While a device is being revoked, it cannot be used to access protected data.

You can enable or disable the data theft prevention feature in a policy. When Data Theft Prevention is enabled, all devices using the Policy will need to connect to Aranda Datasafe regularly or they will be revoked.

Prerequisites: Before enabling DLP features, make sure that Active Directory Certificate Services are configured.
The data theft prevention feature is only available if the local file encryption feature is enabled for policy. (It uses the encryption certificate that is generated when using local file encryption.)

To enable or disable data theft prevention:

1. Open the Policy Editor for the Policy you want to change (click **Policies** and then click Policy).

2. Click on the **DLP** tab.

3. Use the slider of **Data Theft Prevention** to enable or disable Data Theft Prevention (green is enabled, gray is disabled).

A message appears reminding you to configure Active Directory Certificate Services (AD CS). We recommend that you configure AD CS before enabling DLP. Click **OK** to close the message.

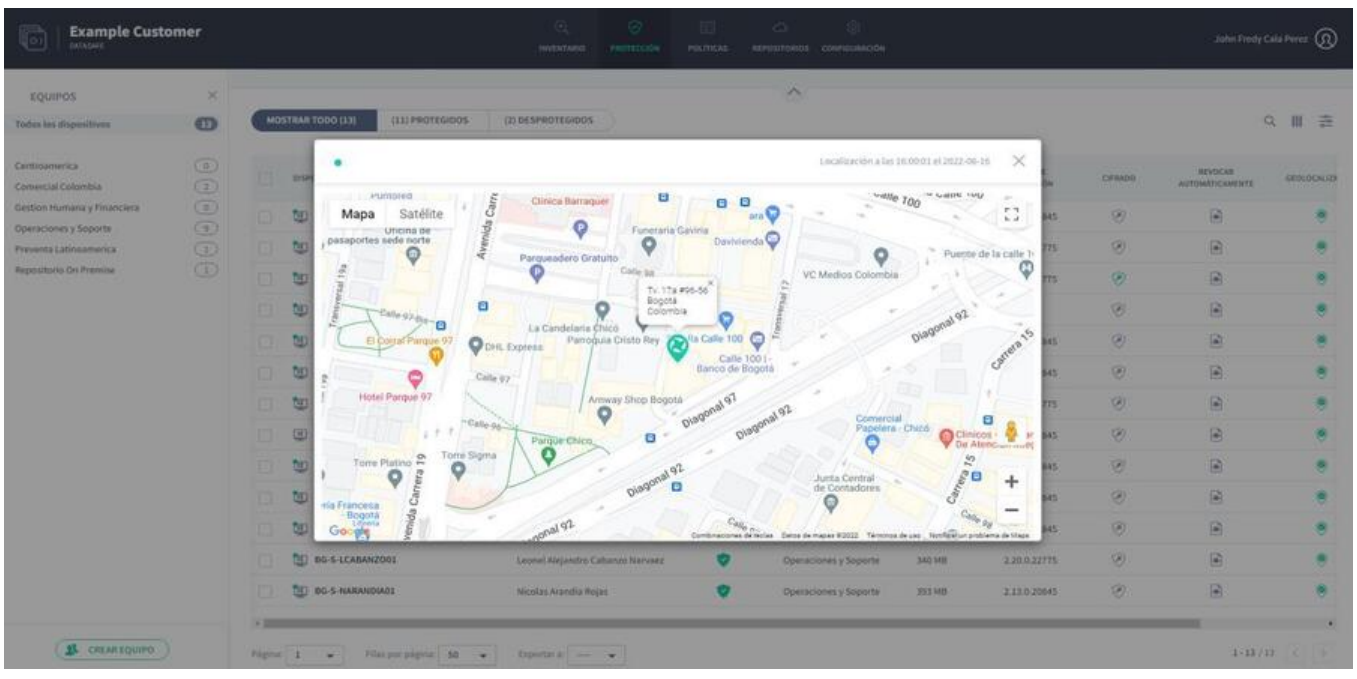
4. Use the **Revoke if device disconnects for days** option to define how long Aranda Datasafe will wait before locking a device.

5. Click **Save or Save & Close** to confirm.

Enable Geolocation

Prerequisites: Before enabling DLP features, make sure that Active Directory Certificate Services are configured.
You can use the geolocation feature to find the last known location of your protected devices. It can be used with any device that has wi-fi enabled.

When geolocation is enabled, you can use Aranda Datasafe to locate a device and it will display the last known location on an embedded Google map.



You can enable or disable the **geolocation** feature in a policy. If enabled, all devices that use that Policy and have Wi-Fi enabled can be located **using Locate Device** in Aranda Datasafe.

To enable or disable geolocation in a policy:

1. Open the Policy Editor for the Policy you want to change (click Policies, and then click Policy).

2. Click on the **DLP** tab.

3. Use the **Geolocation** slider to enable or disable local encryption (green is enabled, gray is disabled).

4. Click **Save** or **Save & Close** to confirm.

Enable user profile migration

The **migration** feature is designed to help you migrate Windows user profile settings from one protected device to another. This type of data includes accessibility settings, mouse and keyboard settings, favorites, and many other user-specific settings.

For example, let's say you have a laptop backed up and protected by Aranda Datasafe. You decide to replace the laptop with a newer, higher-spec laptop. By using the migration feature, you can transfer Windows user profile settings from the old laptop to the new one. This is much faster and easier than setting up the new laptop from scratch.

You can enable or disable the migration feature for each policy.

1. Open the Policy Editor for the Policy you want to change (click **Policies** and then click Policy).
2. Click on the **Migration** tab.
3. Use the slider to enable or disable Microsoft Windows user profiles (green is enabled, gray is disabled).
4. Click **Save** or **Save & Close** to confirm.

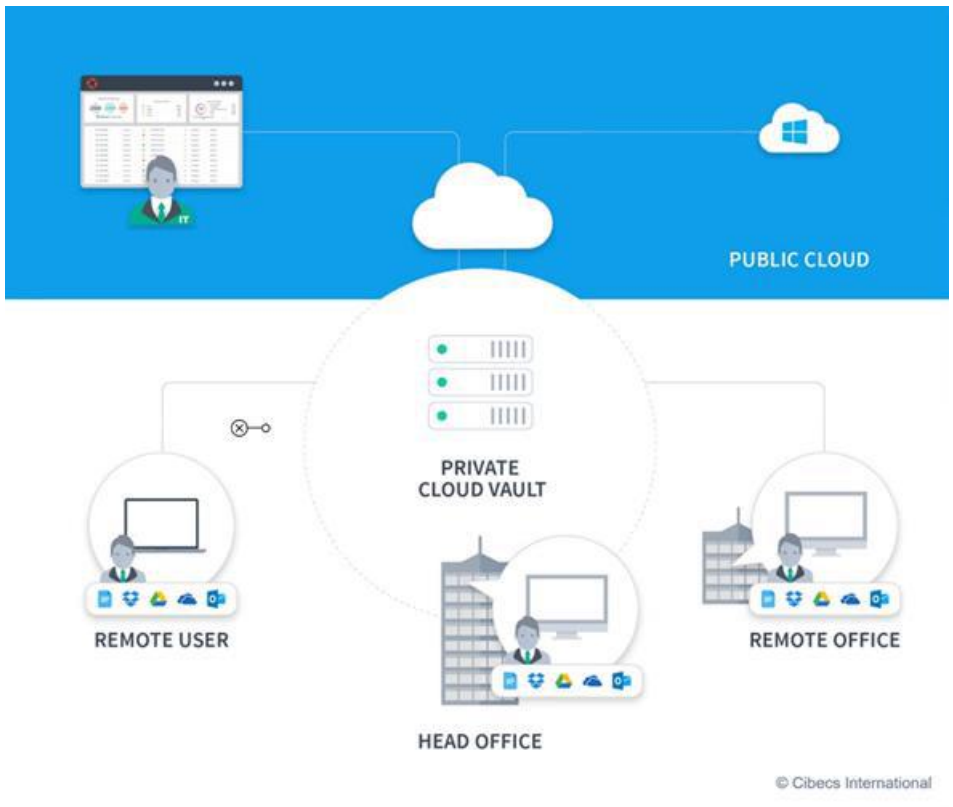
To transfer Windows user profile settings from one machine to another, you can manually back up the device to be replaced. Then sign in to the new device and perform a restore and choose which profile and data settings to use. For more information, see Migrate user profile data to a new device.

Repositories

Repositories Overview

A repository is a storage area that can be installed on a server on your premises or on a remotely accessible server. It stores encrypted backup data from your activated devices.

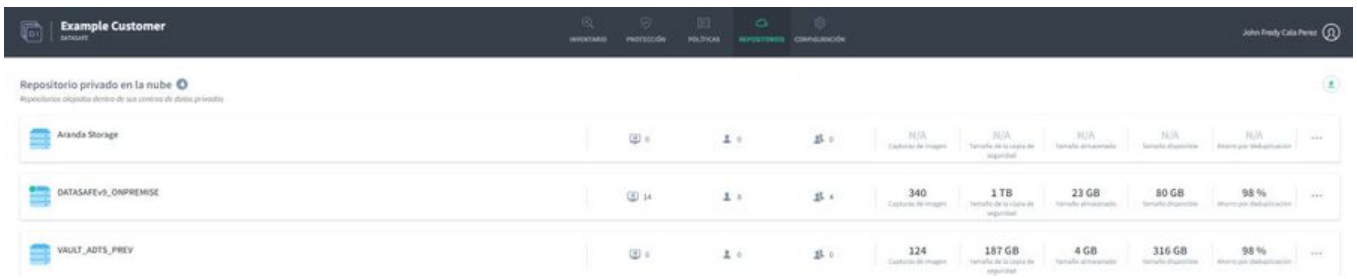
For maximum efficiency, Aranda Datasafe uses source-side block-level deduplication to ensure that only data that is new or has changed is uploaded to the repository. The unchanged data already exists in the repository, so it doesn't need to be reloaded.



Repositories

You can use the Repositories page to view information about your repositories, which are storage areas for your backups.

To display the Repositories page, click Repositories in the top banner.



The repositories page provides a list of your repositories. You can search the list of repositories by name, and you can also download the repository installer and Disconnect a repository .

List of repositories

Field	Description
Online Status	- Online: green icon - Offline: gray icon
Repository Aliases	The name given to the repository when it was created. It is usually a descriptive name that makes the repository easy to identify.
Repository Hostname	The repository FQDN (Fully Qualified Domain Name). This hostname will be used to connect to a repository.
Devices	The number of devices that are associated with the repository by the Computer to which they belong. These devices will back up to the associated repository.
Users	The number of devices that are associated with the repository by the Computer to which they belong. These users will have their data backed up in the associated repository.
Equipment	The number of computers assigned to the repository.
Snapshot	The number of backups that have been made for a repository. A snapshot is a backup made at a particular point in time.
Backrest Size	The size of the backup data before deduplication has been applied.
Backup Almacenado	The amount of storage space used to store the backup data.
Deduplication Savings	The amount of storage space saved by using deduplication, which is displayed as a percentage. Instead of backing up each file every time, Aranda Datasafe only backs up files that have changed since the last backup. This is called deduplication and means that less space is required for your backups and the backup process is more efficient.

Install and configure a repository

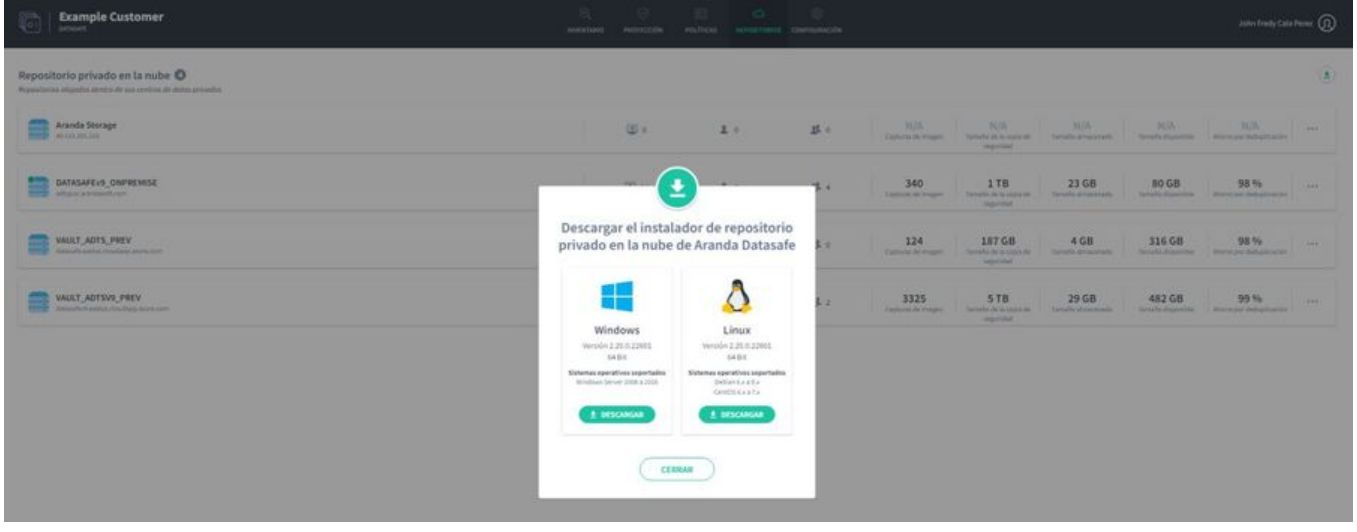
To add a new repository for storage, you must first download the repository installer. You can then run it on your server and register it to connect to Aranda Datasafe.

⚐ >**Note:** To register a repository, you will need to have the email address and password of an Aranda Datasafe user account with the role of**Administrator or Security Officer**.

To download and install the Private Cloud Vault package:

1. Click on**repositories**.

2. Click Download**Private Cloud Vault**.



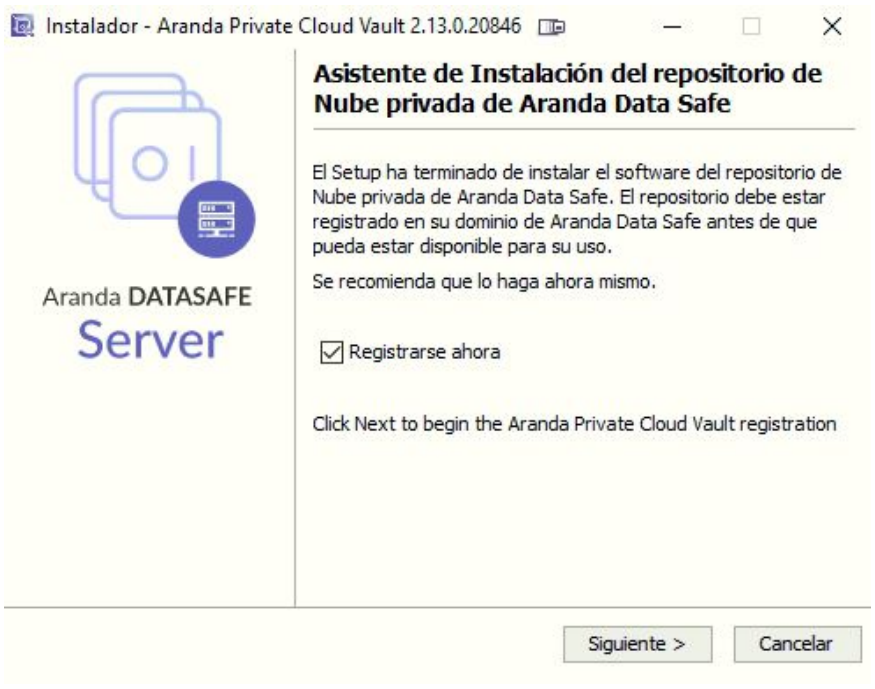
3. When the Private Cloud Vault package is downloaded, search for it on your computer and copy it to your server.

4. On the server, install the Private Cloud Vault software. You can install it in the default location or choose another location if you prefer.

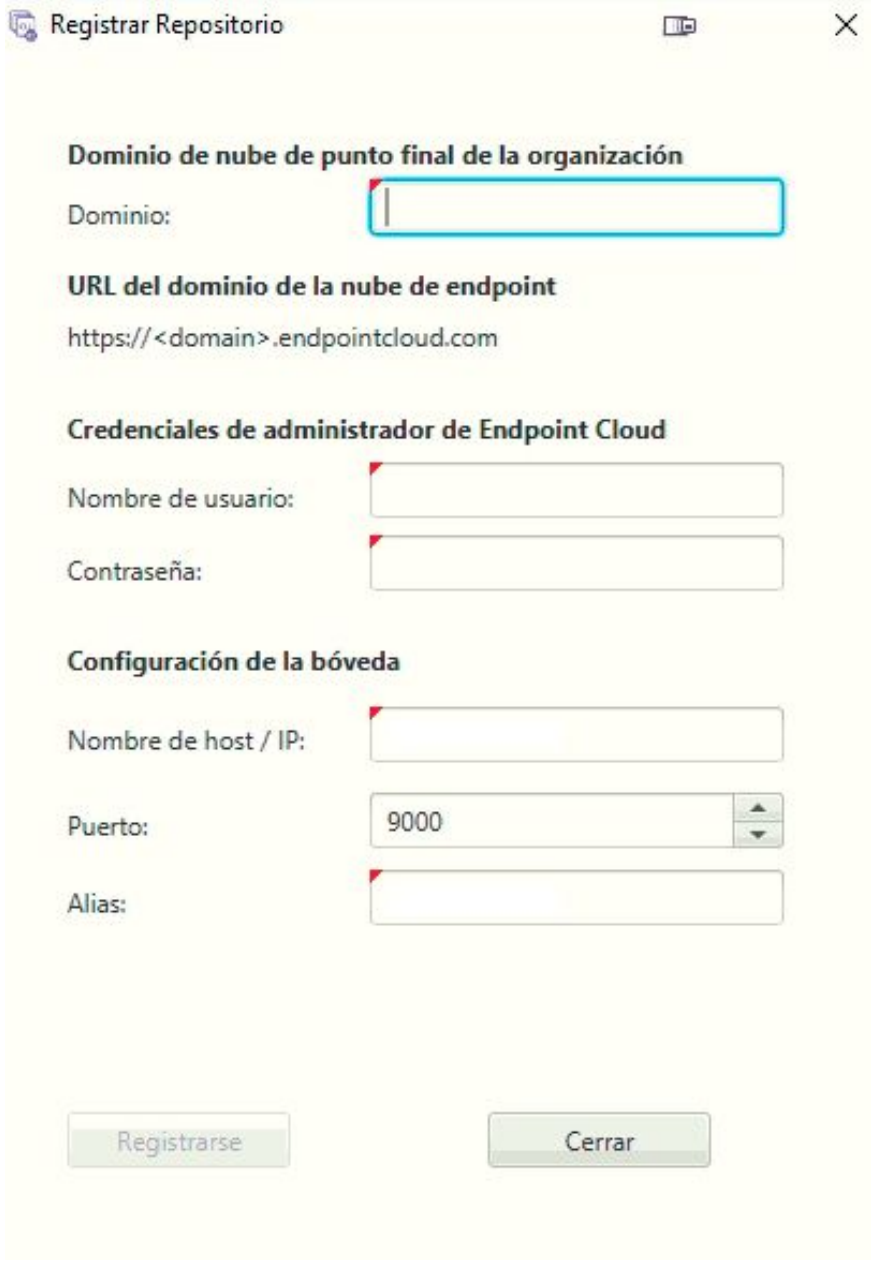
Important: You should choose a location that has an adequate amount of storage space for your data. We generally recommend 20 GB per user, but this can vary depending on the type and amount of data your organization uses.

Follow the steps in the installation wizard.

When you have installed the software, make sure that Sign Up Now is checked, and then click Next.



5. Enter the registration details:



Field	Description
Domain	The name of your Aranda Datasafe tenant. This is usually the name of your organization and is the first part of your Aranda Datasafe address.
Username	Enter the username of an Aranda Datasafe account that has the role of Administrator or Security Officer. Only these user accounts have permission to register a repository.
Password	Enter the password for the Aranda Datasafe account.
Hostname / IP	Enter the name or IP address of the server that has the repository software installed. If the server is at an internet address, enter the URL instead.
Port	9000. (The port must be set at 9000).
Alias	Enter the name of the repository as it will appear in Aranda Datasafe.

Important: Discovery agents and protection agents must be able to communicate with the repository over port 9000.

6. Click **Sign Up**.

Delete a repository

If you no longer need a repository, you can remove it from Aranda Datasafe by "separating" it. When you delete a repository:

- You can no longer restore devices from the deleted repository
- The repository cannot be assigned to any Team (if you have Teams using the deleted repository, you will need to assign them a different repository, otherwise their devices will not be backed up).

To delete a repository:

1. Click on **repositories**.

2. Locate the repository you want to delete.

3. Select the radio button (...) of the repository and click on **Delete repository**.

4. To confirm that you want to delete the repository, enter DETACH in uppercase letters in the dialog box.

5. Click Disconnect to delete the repository.

Administrators

Administrators Overview

Aranda Datasafe has a secure login to prevent unauthorized access. To log in, you will need to have d[Manager Account](#) or a [Security Officer Account](#) .

To get an account, [must be invited to Aranda Datasafe by another administrator](#) . You'll receive the invitation via email, and you can follow the link to set up your account.

When you log in, the features that are available to you will depend on the role assigned to your account. But all administrators and security officers can use Aranda Datasafe

to monitor, manage, and configure the backup and protection of your organization's data.

Administrators Settings

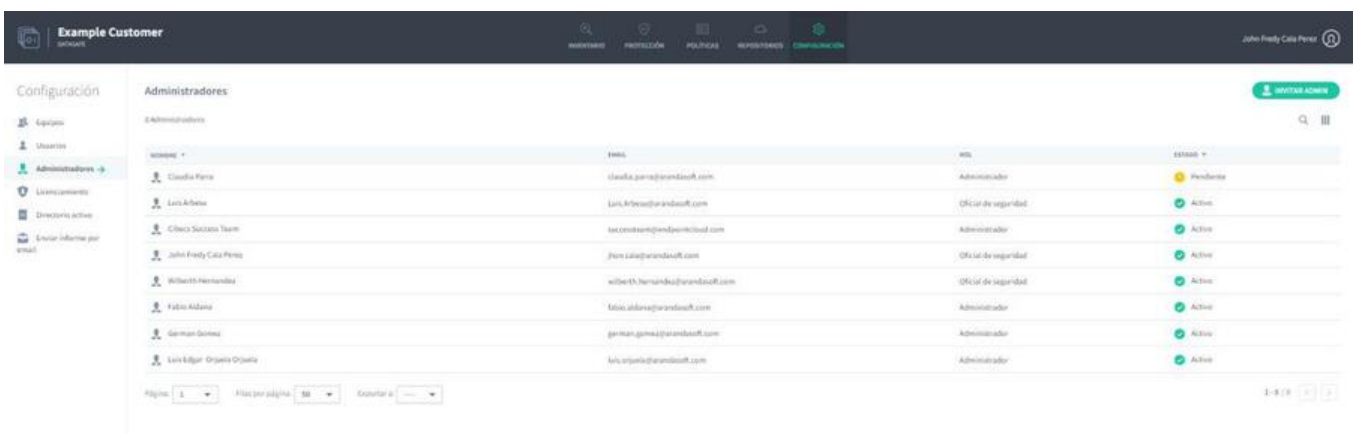
The settings page has an administrators section that you can use to:

- View the name and email address of each admin.
- See if someone is an administrator or a security officer of Aranda Datasafe
- Invite someone to become an administrator of Aranda Datasafe
- Remove an administrator or security officer.

To display the Administrators section:

1. Click on **Settings**.

2. In the side panel, click on **Admins**.



For each admin, you can view the:

Field	Description
Name	The name of the administrator.
Email	The email address used to invite the administrator to Aranda Datasafe.
Role	The administrator's role affects the features that are available to them. Possible roles are: Security Officer: Has full administrator permissions and can also download and register AD Connector, and can change the role of administrators. The security officer holds the key to the organization's backup data. It is recommended that at least two security officers be deployed per customer tenant. **Administrator**: Has access to all Aranda Datasafe features, but cannot download or register AD Connector or change the role of administrators.
Status	Shows whether the admin has activated their account (Active) or hasn't yet responded to the email invitation (Pending).

If you hover over an administrator, you can select their context menu (...). From here you can:

- Assign Security Officer Permissions to an Active Administrator. The Assign Security Officer option is only available if you sign in as a Security Officer.
- Remove an administrator.

Invite Admin

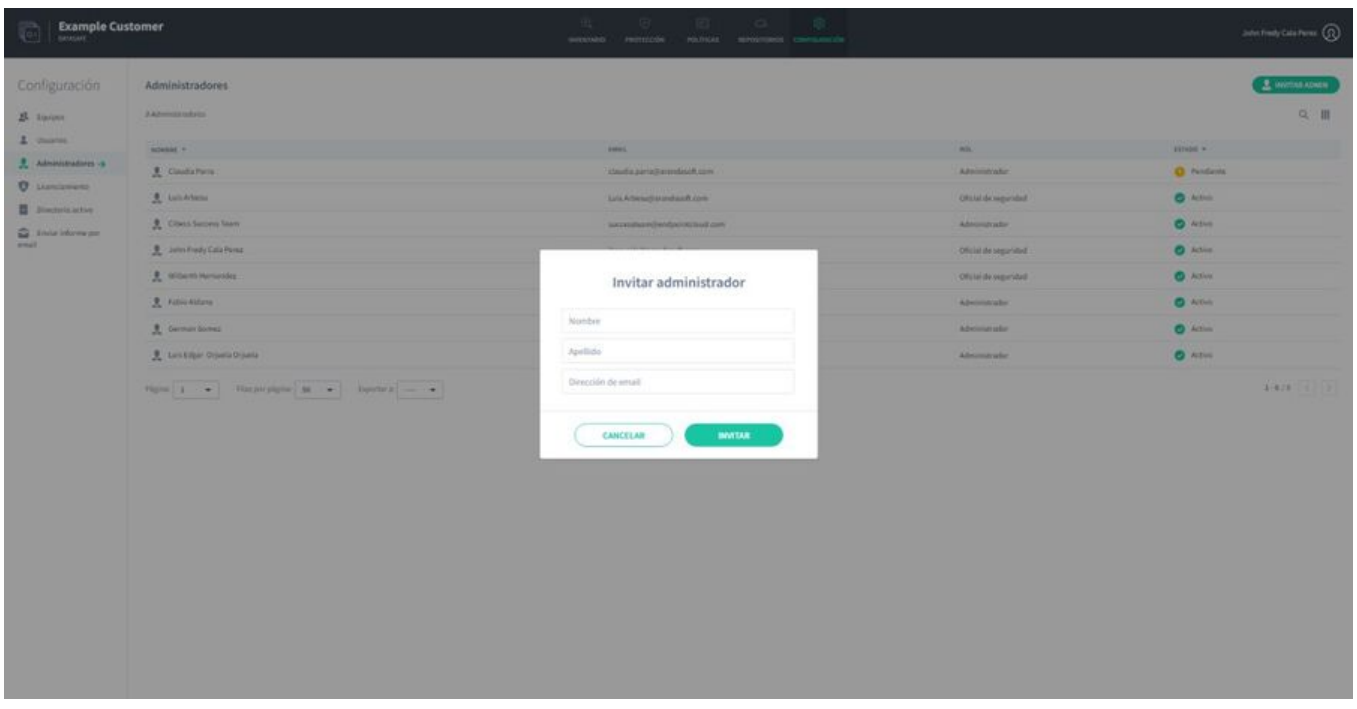
If you want to give someone access to Aranda Datasafe, you can invite them to join as an administrator. When you send the invitation, Aranda Datasafe creates a new administrator-level user automatically and sends an email to the new user. They can use email to activate their account.

To invite a new administrator:

1. Click on **Settings**.
2. Click on **Admins**.
3. Click **Invite Admin**.
4. In the Invite Admin dialog box, enter the first name, last name, and email address of the user you want to add as an admin.
5. Click **Invite**.

The user will receive an email invitation. When they receive the email, they can use it to activate their account. Once activated, they will be able to log in to Aranda Datasafe and access the administrator-level features.

For more information about the email invitation, see Activate your account.



Activate Account

If you are going to use Aranda Datasafe, you should receive an email inviting you to activate your account.

If you do not receive the email, please check your spam and junk mail folders. If you still can't find the email, contact Aranda support.

Once you have the email, click on **Activate Account**. Your browser opens the activation web page. The first time you access Aranda Datasafe, you need to enter a password and then re-enter it to confirm. Click **Activate** to log in.

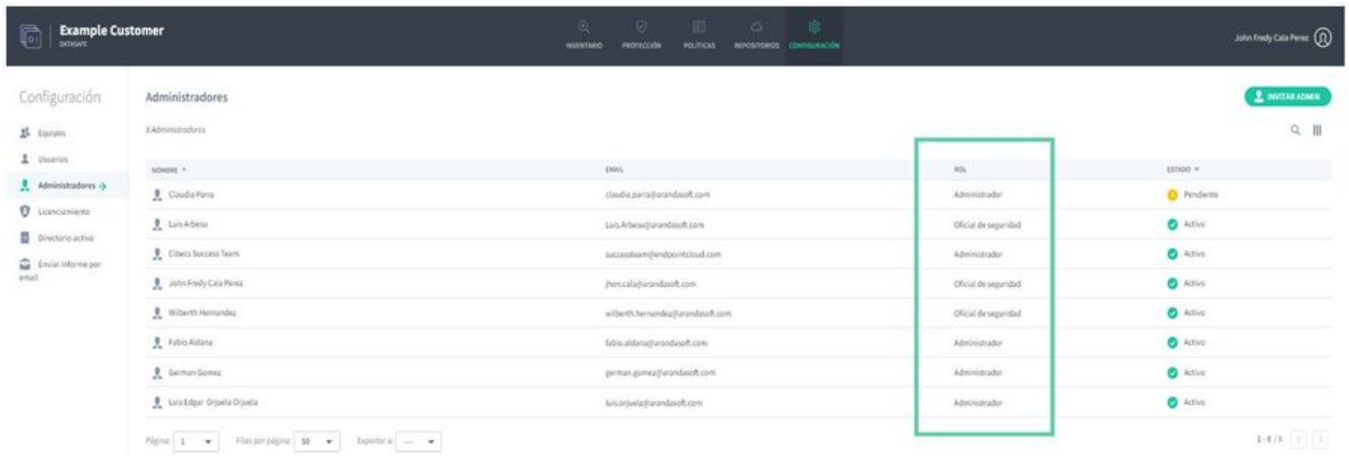
Administrator Role

When you activate an invitation to join Aranda Datasafe, you are automatically given an account. The account has a role, either as an**administrator** or as a**security officer**.

If you are granted an administrator account, you can access all the features of Aranda Datasafe, but you cannot download and register the AD Connector.

Only people with the Security Officer role can download and register AD Connector.

You can see their role in the**Admins** section on the**Settings** page (see Administrators - Settings Page).



Official Security Role

The role of**Security Officer** is the highest-ranking role. Users with this role have access to a wider range of features in Aranda Datasafe than other users, so you should be careful when assigning this role.

Security officers are the only users who can:

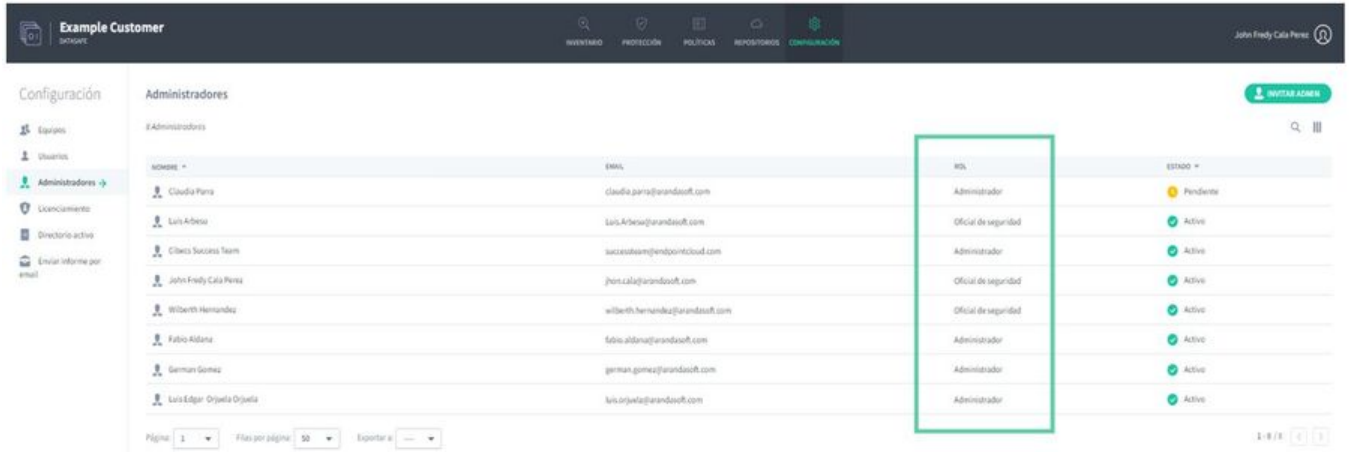
- Download and register the AD connector. This is necessary to allow Aranda Datasafe to protect your devices and data.
- Allow access to encrypted data, which is needed to restore a user's data.

Aranda Datasafe must have at least one user with the role of**Security Officer**.

To check if your user account has the role of**Security Officer**:

1. Click on**Settings**.

2. Click on**Admins**.



3. Find your user account in the list and see if you have the role of **Security Officer**.

Only users with the **Security Officer** role can change the role of a user account.

Change Account Role

If you sign in as a security officer, you can change the role of an administrator account. This is useful when you want to upgrade an administrator to security officer, so you can register the AD connector and restore user data.

To change an account's role:

1. Log in as a security officer.

2. . Click on **Settings**.

3. Click on **Admins**.

4. Click the context button (...) of the administrator you want to change.

5. Click **Assign Security Officer**.

6. Enter your password to confirm the change.

Remove an administrator or security officer

If you log in to Aranda Datasafe as a security officer, you can delete other administrator and security officer accounts. It will usually only delete accounts that are no longer in use, for example, if a staff member has left the organization.

Caution: If you delete an account, the user of that account will not be able to log in to Aranda Datasafe.

To remove an administrator or security officer:

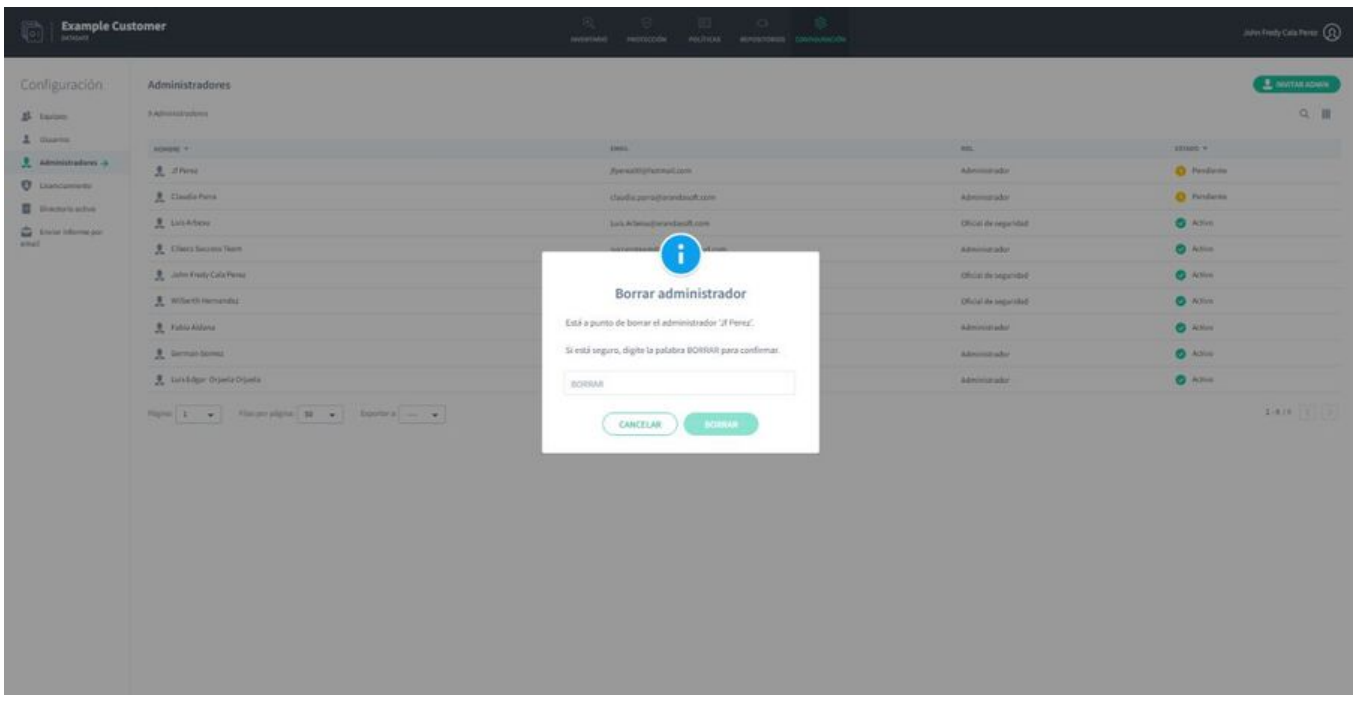
1. Click on **Settings**.

2. Click on **Admins**.

3. Click the context button (...) of the administrator or security officer you want to remove.

4. Click **Delete**.

5. Type Delete in the dialog box to confirm, and then click **Delete**.



Equipment

Equipment

In Aranda Datasafe, you need to organize your devices into teams. Typically, Aranda Datasafe users create teams for significant groups, such as departments in a company or the geographic locations of different facilities. But there are no limitations: you can create teams for any grouping you want.

When Aranda Datasafe first discovers your devices, they are "unassigned." This means that they are not on a team.

You need to create your own teams to be able to:

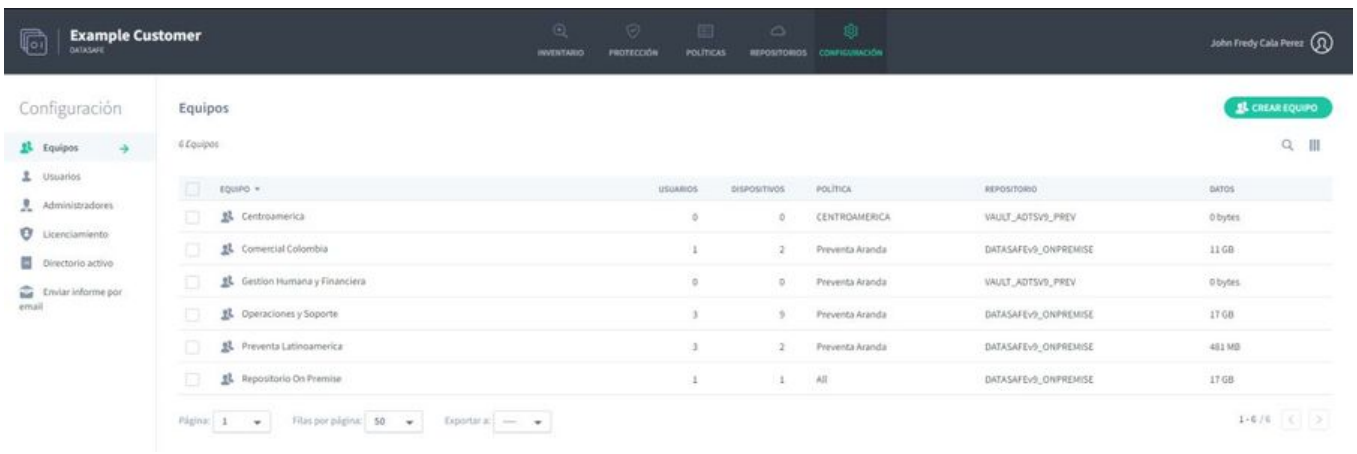
- Assign a **policy** to the team. A policy is a set of rules that define:
    - What data is protected and backed up
    - How often backups occur
    - If any **data loss prevention** feature is used to protect your data in the event of loss or theft of a device. These include local encryption, data theft prevention, and geolocation.
    - Whether Windows user profile data can be backed up to **migrate** it to other devices.
- Assign a storage area **(repository)**. The repository is a storage area on a server and is used by Aranda Datasafe when backing up devices on your Computer.
- View and filter information about devices on specific computers.

To create, edit, and view equipment, you can use the **Inventory** page, the **Protection** page, or the **Settings** page (which has a **Equipment** section).

Equipment Configuration

You can use the **Teams** section on the **Settings** page to view, edit, and delete your Teams.

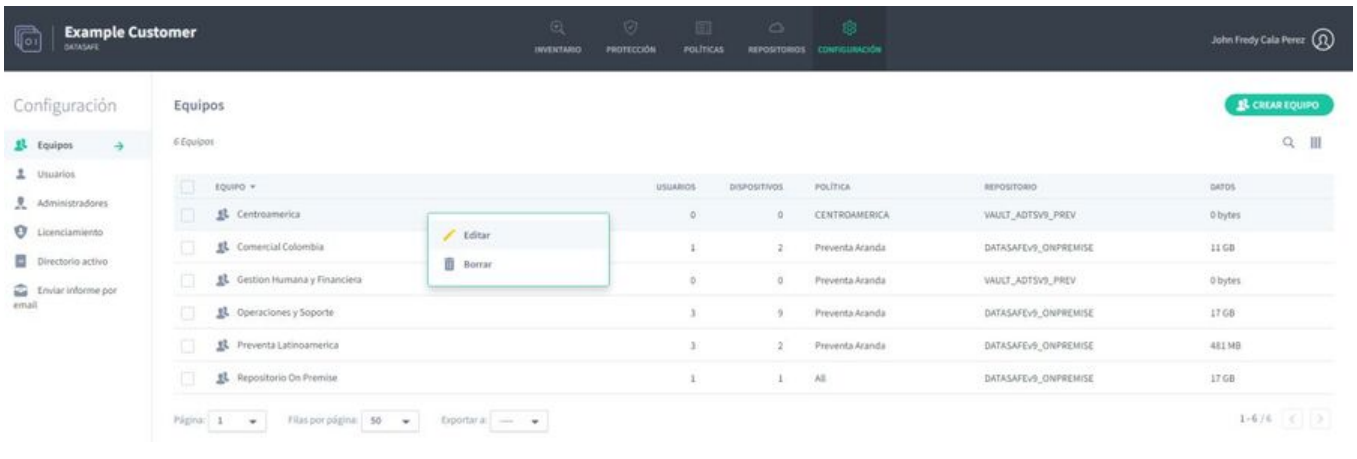
To display the **Computers** section, click Settings. The Teams section is displayed by default (if necessary, you can display it by clicking Teams in the sidebar).



For each team, you can see:

Field	Description
Users	The number of users on the team
Devices	The number of devices assigned to the team.
Politics	The Policy that is assigned to the Team. A policy is a set of rules that define: - What data is protected and backed up - How often backups occur - Whether any **data loss prevention** features are used to protect your data in the event of a lost or stolen device. These include local encryption, data theft prevention, and geolocation. - Whether Windows user profile data can be backed up to **migrate** to other devices.
Repository	The repository assigned to the team. The repository is a storage area on a server, and is used by Aranda Datasafe when backing up devices on your computer.
Data	The amount of storage space used to back up data on your computer.

If you hover over a computer, you can select its context menu (...). From here, you can edit the team or delete it.



Equipment Filtering Configuration

By default, the **Computers** section on the **Settings** page displays information for all computers and devices. But, if necessary, you can filter the **Teams** section to only show information that meets certain criteria. For example, you can use search to filter the Computers section so that it only shows information from the devices of a particular **computer**.

There are several ways to filter the Teams section:

Use a search to filter the list of computers

Show or hide columns in the team list

Use a search to filter the list of computers

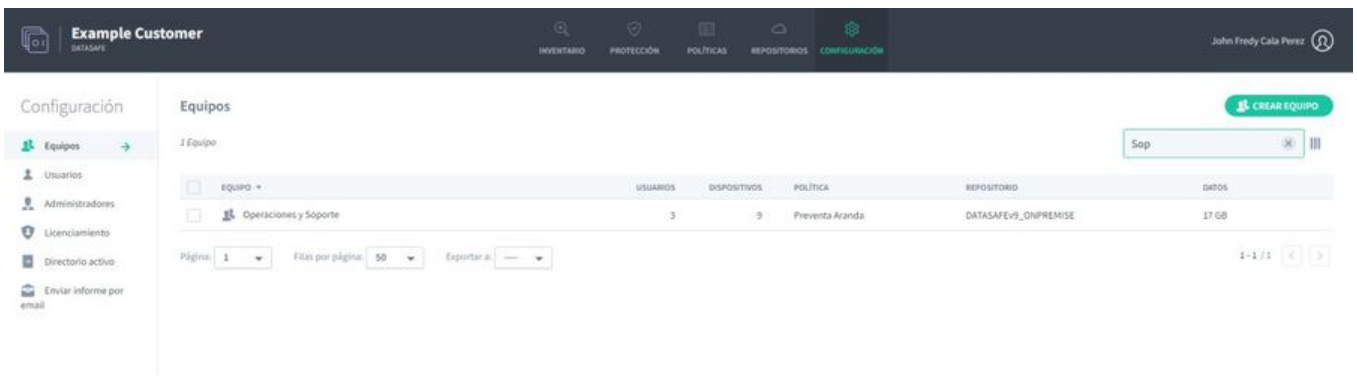
You can use the **search** function to filter the list of computers so that it only includes computers that have certain values. For example, you can use search to filter the list so that it only shows computers that are associated with a particular repository.

You can use search to filter the list of **teams** by any text value, including the **team** name, **policy** name, and **repository** name.

To apply a search filter:

1. Click on the search icon above the list of equipment.

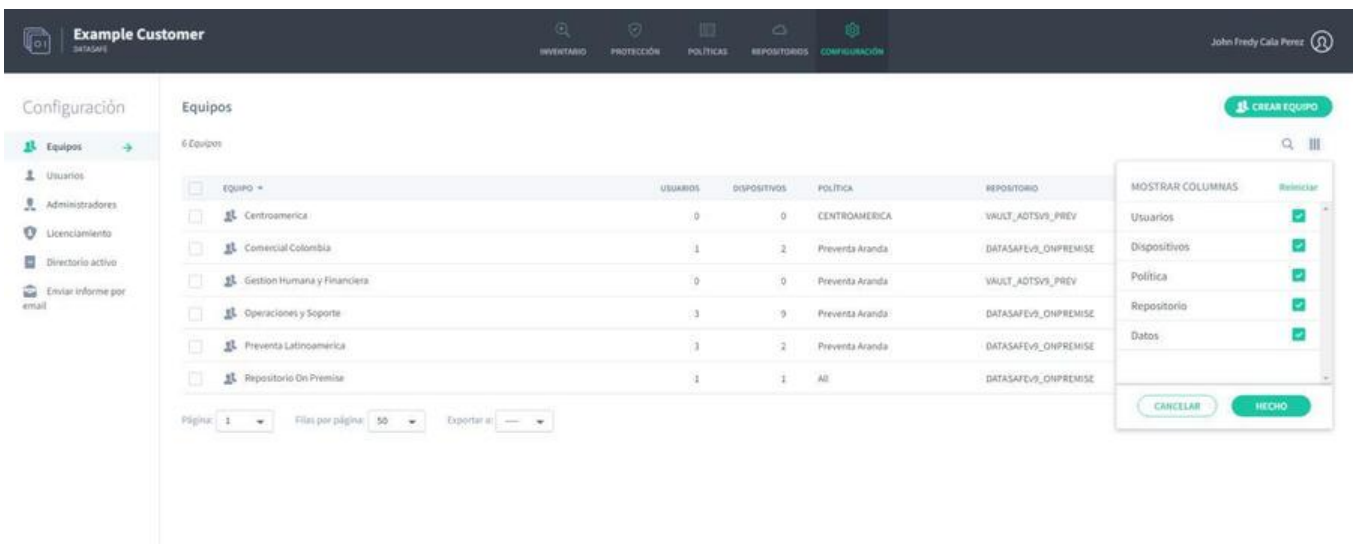
2. Enter the first few characters of the text value you want to use as a filter. Aranda Datasafe applies the filter as you type, so you can do partial matches or you can enter the full-text value to be more specific.



Show or hide columns in the equipment list

You can choose to show or hide columns in the team list. For example, you might not care which repository each team uses, so you can hide the repository column.

To show/hide columns, click the Columns icon and then choose which columns to include.



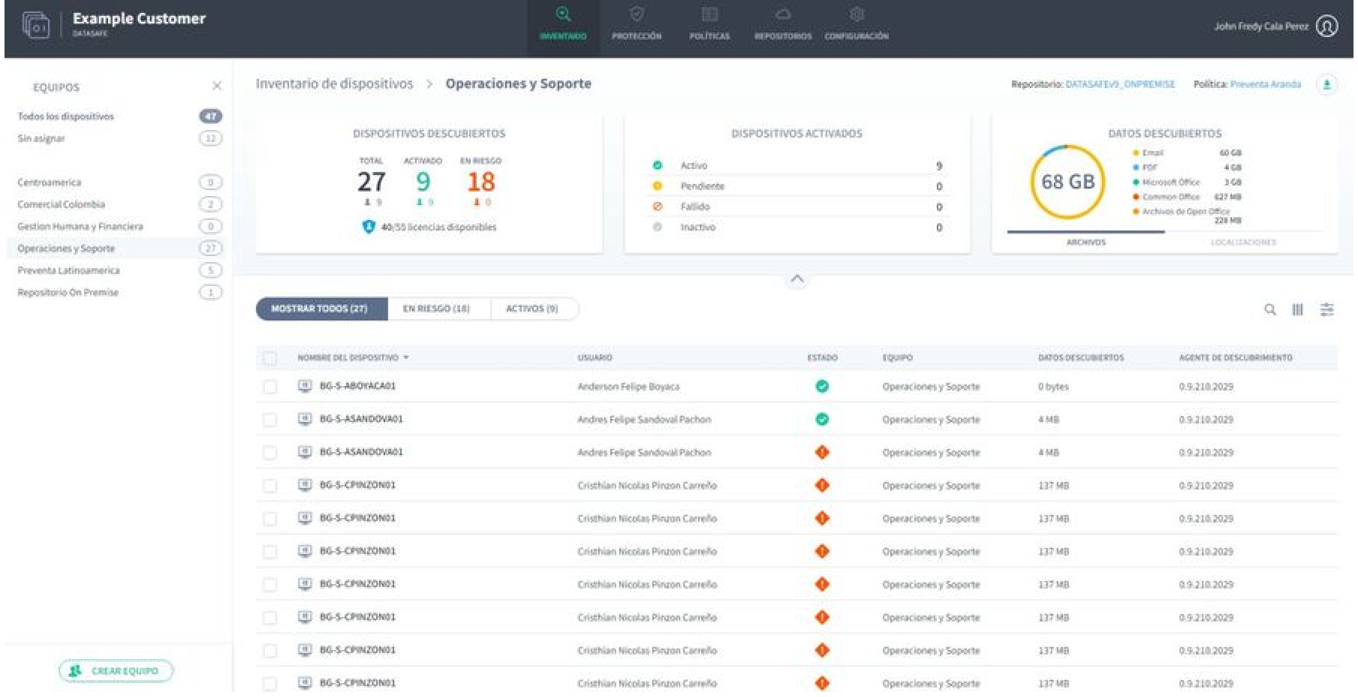
View devices in a team

You can use the **Inventory** or **Protection** pages to view information about the devices on any Computer.

1. Click Inventory or Protection.

2. In the Teams section, click:

- **All devices** to display information about all devices on all devices
- **Unassigned** to display information only for those devices that are not yet assigned to a team
- to display information about devices on a specific computer.



When you click on a Team option, the **Inventory** or **Protection** page refreshes and the dashboard and list screens are filtered to show only information about the devices on the selected Device.

Click **All Devices** in the **Teams** sidebar to remove the filter.

Create a Team

Aranda Datasafe uses Teams to organize its devices into groups.

Each team has one:

- **Policy**: Defines when devices on your computer will be backed up, as well as what migration and data loss prevention settings the devices will use.
- **Repository**: Defines where backup data for your team's devices will be stored.

When you create a team, you choose a policy and a repository. You can also edit a Team to rename it or associate it with a different Policy or repository.

Create a team

You can create a new team and then assign it a policy and repository. When your computer is set up, you can assign it to your devices.

You should create a new team if:

- There are no teams in Aranda Datasafe
- Existing computers don't meet your requirements, for example, they don't use data theft prevention, but you need it for your devices.
- Existing teams back up to a repository that isn't suitable for their devices.

To create a team:

1. There are three ways to create a team: from the **Inventory** page, the **Protection** page, or from the **Teams** section on the Settings page. Then you can:

Click on **Inventory**.

or:

Click on **Protection**.

or:

Click on **Settings** and use the **Computers** section.

2. Click Create Equipment (lower-left corner of the Inventory or Protection screen, upper-right corner on the Computers - Settings page).

3. Enter a name for the new team.

4. Use the **Assign a Policy** combo box to choose the Policy for the team. All devices on your Computer will use the settings defined in the Policy (backup scheduling, data loss prevention settings, etc.).

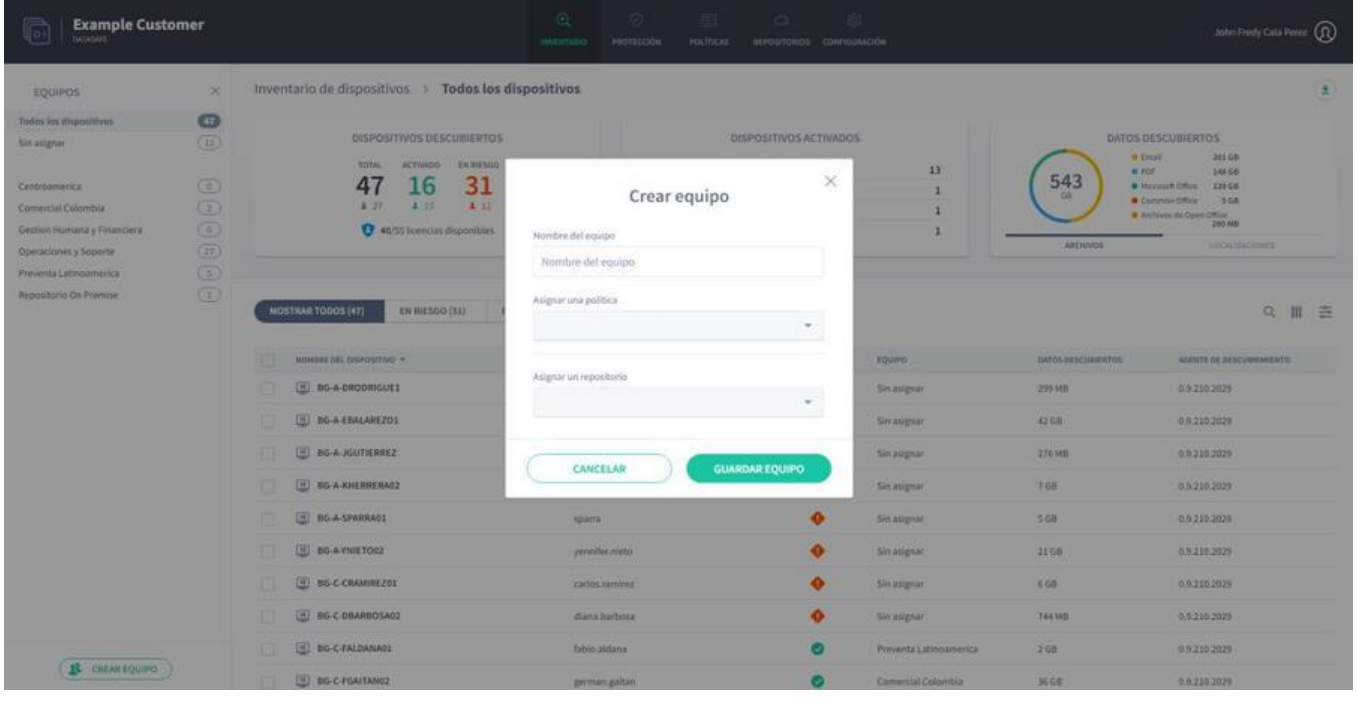
5. Use the **Assign a repository** combo box to choose the storage area that will be used to store backup data for devices on your computer.

6. Click **Save Equipment**.

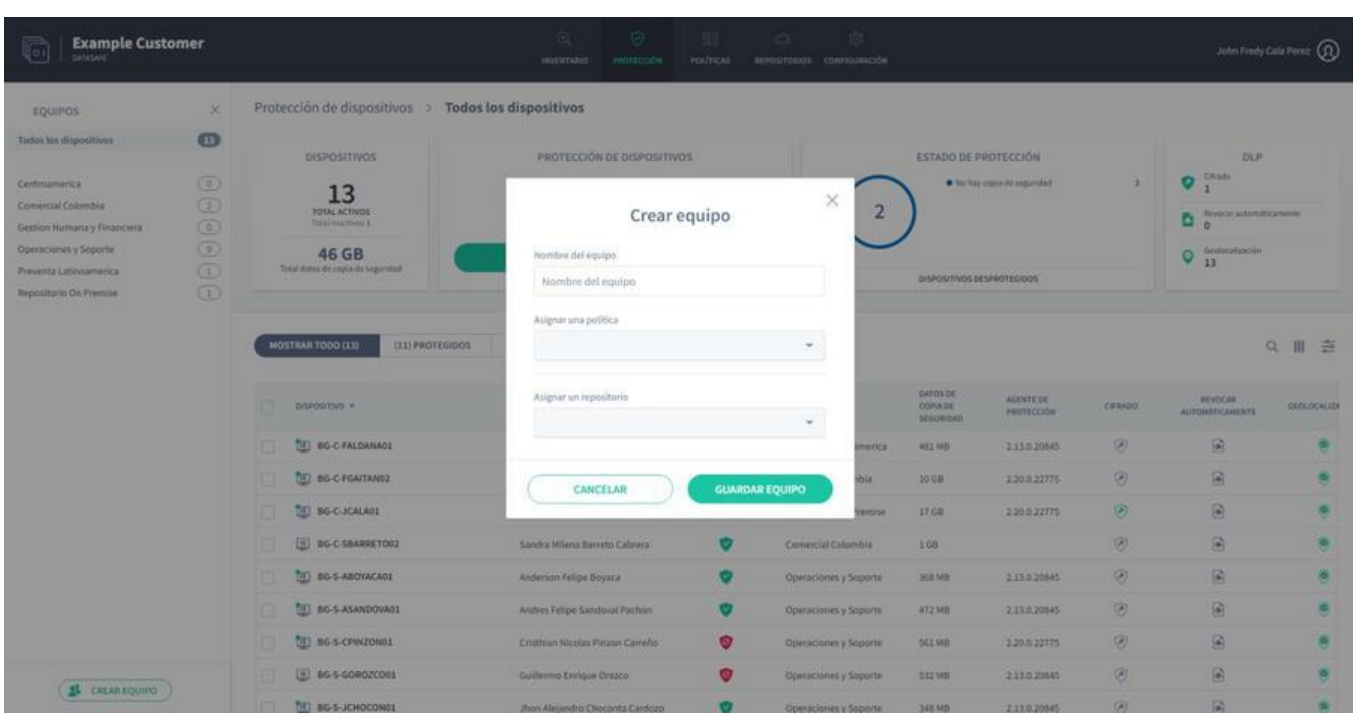
Your new equipment appears in the **Equipment** section of the **Inventory** page and the Protection page. It also appears in the list of **devices** on the **Settings** page).

7. Repeat steps 2 through 6 inclusive to create as many new computers as you need.

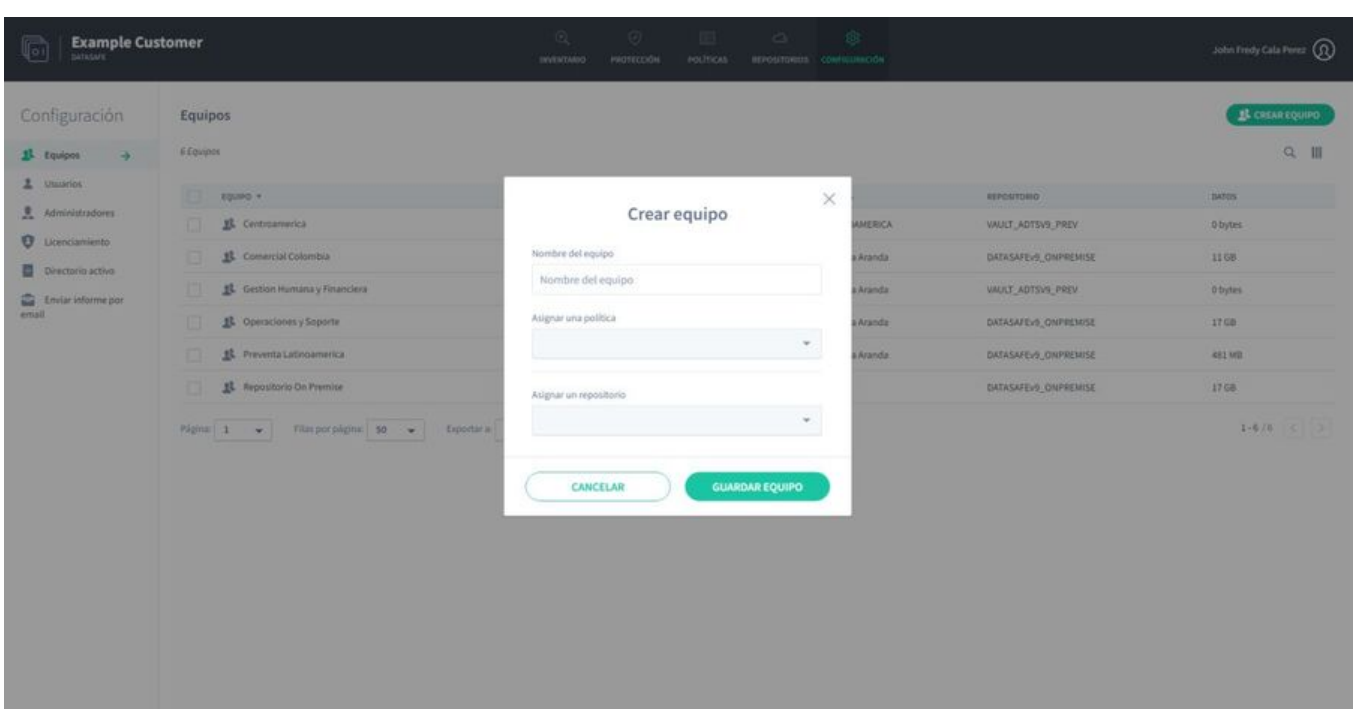
Creating a team from inventory:



Creating a team from the Protection page:



Creating a team from the Settings page:



Edit a Team

If you want to make changes to an existing computer:

1. There are three ways to edit a device: from the**Inventory** page, the **Protection** page, or from the**Equipment** section on the**Settings** page. Then you can:

Click on **Inventory**.

or:

Click on **Protection**.

or:

Click on **Settings** and use the **Computers** section.

2. Hover over the equipment you want to edit and then click on its radio button (...).

3. Click **Edit**.

4. Use the **Team Name** field to change the team name, if necessary.

5. Use the **Assign a Policy** combo box to choose the Policy for the team. All devices on your Computer will use the settings defined in the Policy (backup scheduling, data loss prevention settings, etc.).

6. Use the **Assign a repository** combo box to choose the storage area that will be used to store backup data for devices on your PC.

7. Click **Save Equipment**.

Assign Policies to Teams

You can assign a policy to each of your teams. A policy is a set of rules that define:

- What data is protected and backed up
- How often backups occur
- If any **data loss prevention** feature is used to protect your data in the event of loss or theft of a device. These **include local encryption, data theft prevention, and geolocation**.
- Whether Windows User Profile data can be backed up for migration to other devices.

Typically, you assign a policy to a team when you first create the team. But you can also edit a team to use a different policy:

1. Click on **Inventory** or **Protection**.

2. Hover over the team name and then click on the radio button (...).

3. Click **Edit**.

4. Use the **Assign a Policy** combo box to change the team's policy.

5. Click **Save Equipment**.

Assign Repository to a Team

You can assign a repository to each of your teams. A repository is a storage area on a server, and it's where Aranda Datasafe will store backup data for all devices on a computer.

Typically, you assign a repository to a team when you first create the team. But you can also edit a team to use a different repository:

1. Click on **Inventory** or **Protection**.

2. Hover over the team name and then click on the radio button (...).

3. Click **Edit**.

4. Use the **Assign a repository** combo box to change the team's repository.

5. Click **Save Equipment**.

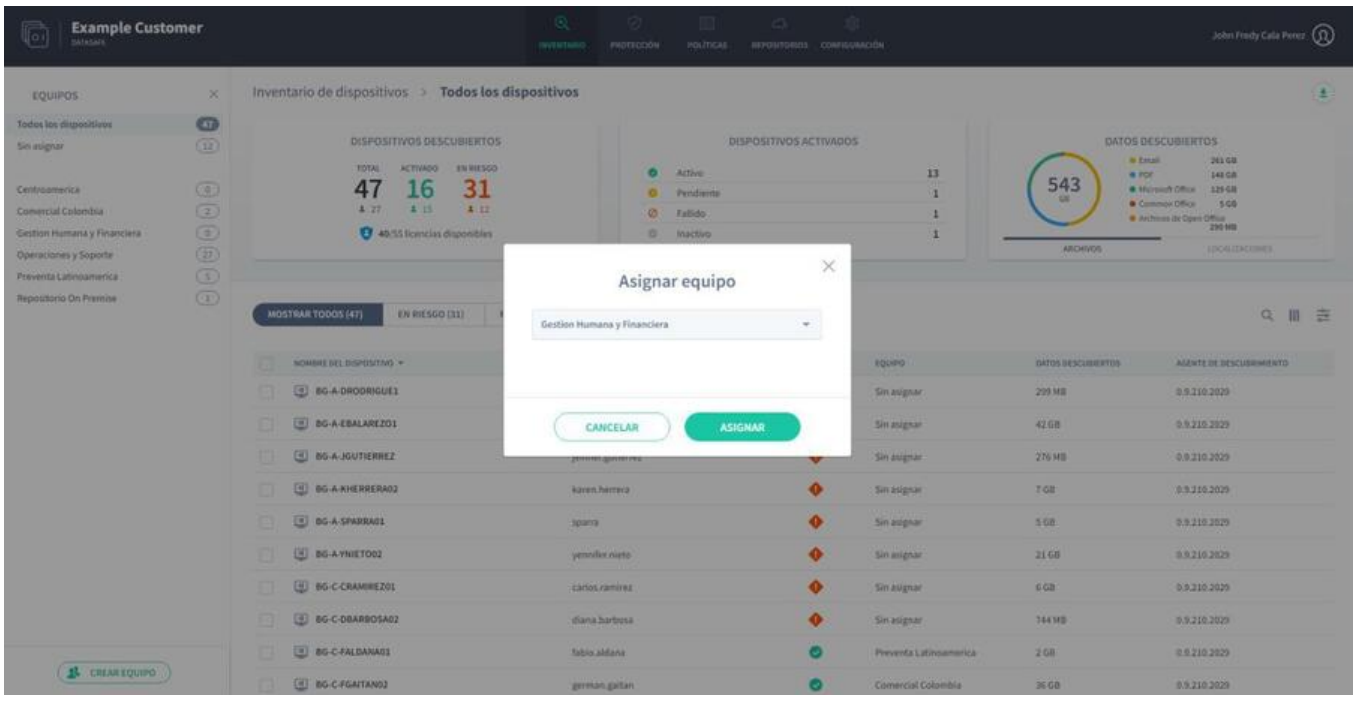
Assign Device to a Team

To use Aranda Datasafe to back up and protect a device, the device must be assigned to a Team. The team is associated with a policy and repository, and these define:

- When devices are backed up
- What Data Loss Prevention settings are used
- What migration configurations are used
- Where the backup data is stored.

All devices on that computer use the computer settings. To assign a device to a team:

1. Click on **Inventory** or **Protection**.
2. Hover over a device in the list of devices.
3. Click on the radio button on the device (...).
4. Click **Assign Team**.
5. Assign the device to a team from the list.
6. Click **Assign**.



The page will automatically refresh, and after a short pause, the device will be assigned to their selected team. You can now use the **Inventory** or **Protection** page to view Information on:

- All devices
- Unassigned devices
- Devices on each of your computers.

Delete Equipment

There may be times when you need to remove a computer from Aranda Datasafe. For example, it is You may want to delete a Team if your organization has been restructured, or some Teams in Aranda Datasafe no longer exists in your business or has merged with other Teams.

If you no longer need a piece of equipment, you can remove it from your Datasafe Washer. When you delete a computer, Aranda Datasafe:

- Remove the equipment
- Delete all devices assigned to the team.

Important: If you want to keep the devices, you must assign them to a different team before you perform the deletion.

To delete a team:

1. Click on **Inventory** or **Protection**.
2. Hover over the Equipment you want to delete and then click on its radio button (...).
3. Click **Delete**.
4. Enter DELETE in capital letters and then click **Delete** to confirm that you want to delete the Equipment

Users

When Aranda Datasafe discovers your devices, it automatically creates information about users' accounts and devices. This information is displayed on several screens, including the Inventory page, the Protection page, and the Settings page.

User accounts and device information are displayed as:

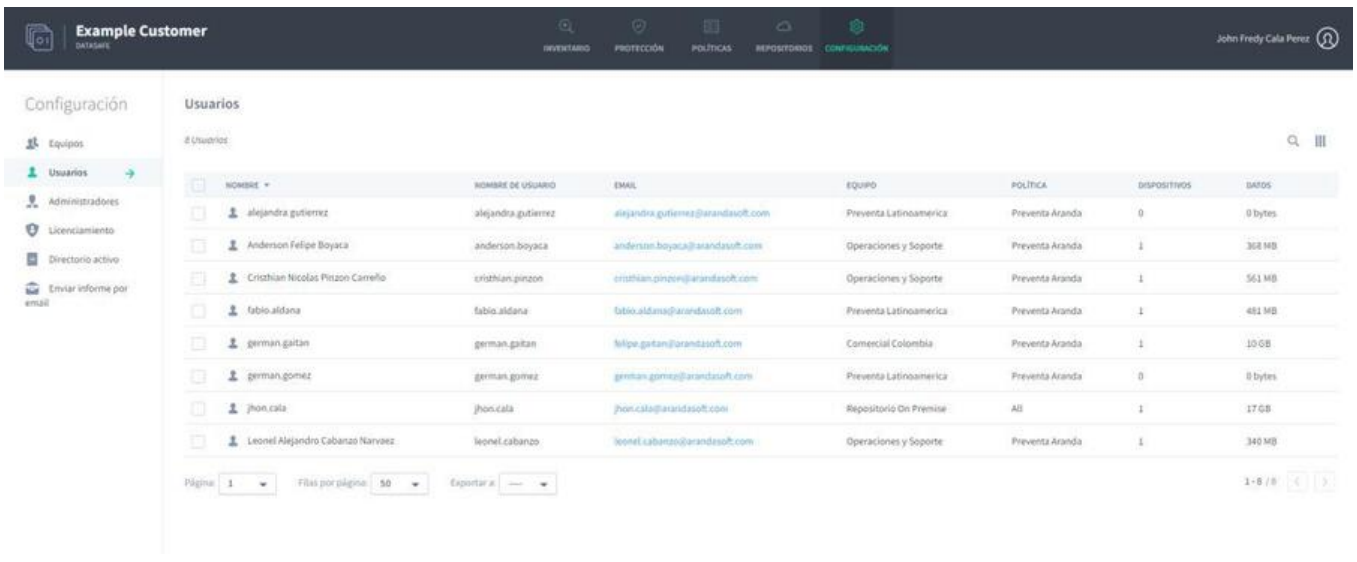
- **User**: A user represents a Microsoft Windows user profile. During the discovery process, Aranda Datasafe connects with the devices that are configured to be protected and retrieves the user's profile information. Create one user for each Windows user profile (typically, this means one user per person).
- **Device Name**: Each user has one or more user devices. For example, a user might have a desktop computer and a laptop. Aranda Datasafe uses Microsoft Windows user profile information to match each device to a specific user.

Users Settings

You can view the details of your Aranda Datasafe users on the Users page.

1. Click on **Settings**.

2. In the sidebar, click **Users**.



The Users page displays a list of users and provides this information:

Field	Description
Name	The user's full name.
User	The username used to log in to the user's device.
Email	The user's email address.
Team	The computer to which the user's device is assigned. If a user has multiple devices, they must all be assigned to the same team.
Politics	The policy assigned to the computer that uses the user's device. It is this Policy that defines when the user's device is backed up, what data is backed up and protected, and what protection and migration features are enabled.
Equipment	The number of computers assigned to the repository.
Devices	The number of devices that the user has backed up and protected by Aranda Datasafe.
Data	The amount of data that Aranda Datasafe has backed up for this user's devices.

User Filtering Settings

By default, the **Users** section on the **Settings** page displays information for all Aranda Datasafe users (who are based on Microsoft Windows user profiles). But, if necessary, you can filter the **Users** section to only show information that meets certain criteria. For example, you can filter the **Users** section to only show information about a particular User.

There are several ways to filter the User section:

Use a search to filter the list of users

Show or hide columns in the user list.

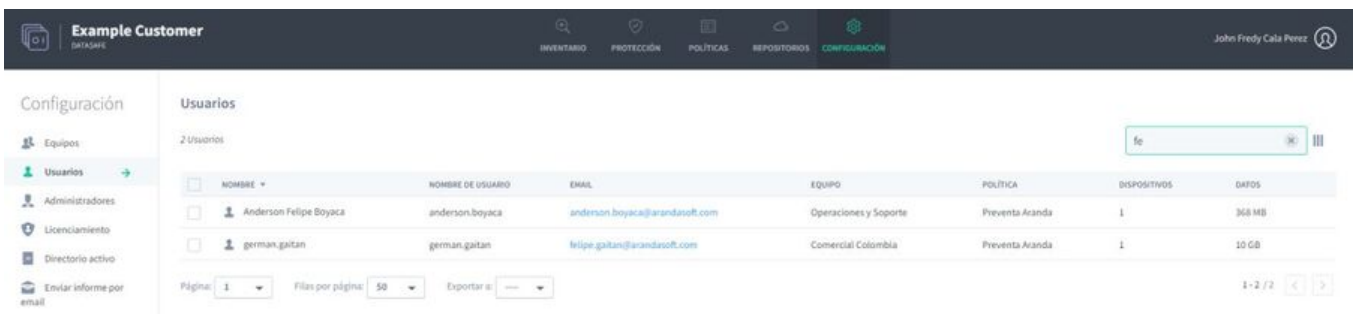
Use a search to filter the list of users

You can use the **search** function to filter the list of users so that it only includes users who have a particular name (or a partial name).

To apply a search filter:

1. Click on the search icon above the list of users.

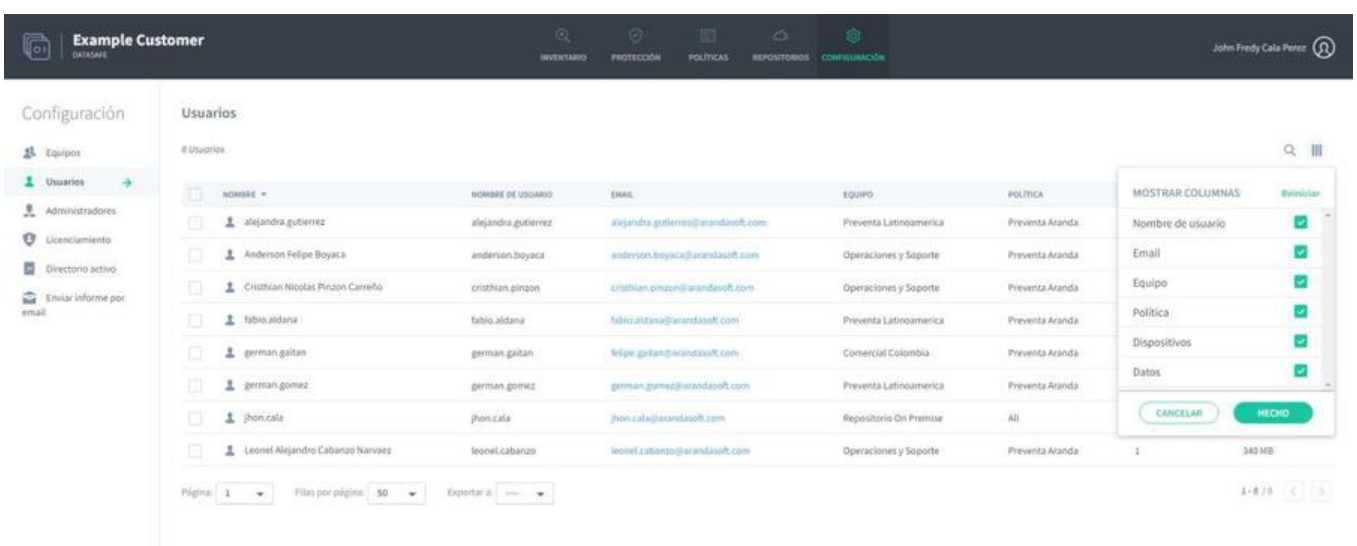
2. Enter the first few characters of the text value you want to use as a filter. Aranda Datasafe applies the filter as you type, so you can do partial matches or you can enter the full-text value to be more specific.



Show or hide columns in the user list

You can choose to show or hide columns in the list of users. For example, you might not care about each user's email address, so you can hide the Email column.

To show/hide columns, click the Columns icon and then choose which columns to include



Create New User

Aranda Datasafe automatically creates new users as part of the discovery process. There is no need to create users manually.

If you have a new staff member and need Aranda Datasafe to back up and protect their devices, install Discovery Agent on the devices. Aranda Datasafe will then be able to discover the devices and connect to them.

When Aranda Datasafe connects to a device, it creates a User automatically, based on the device's Microsoft Windows user profile.

Delete User

If you want to remove a**user** from Aranda Datasafe, you must delete all of that user's devices. When Aranda Datasafe does not have devices for a User:

- Delete that user automatically
- Remove the user's license and make it available for use.

To remove a user's devices (and also the user):

1. The first step is to find all of the user's devices in a list of devices. To do this, you can use the list of devices on the**Inventory** page or the**Protection** page.

Click on**Inventory**. or:

Click on**Protection**.

2. In the device list section, click the**Search** icon.

3. Enter the user's name in the search box. Aranda Datasafe filters the list so that it only shows the devices of that User.

4. Click the checkbox at the top of the list to have all of the user's devices selected.

5. Click on the**Remove Device** icon at the bottom of the device list.

6. Enter DELETE in all caps and then click**Delete** to confirm.

Active Directory Connector

Active Directory Connector

The Active Directory Connector (AD Connector) is an application that Aranda Datasafe uses to authenticate its user accounts. It connects to your Microsoft Active Directory and allows Aranda Datasafe to:

- Identify each Microsoft user account
- Identify the devices that are associated with each Microsoft user account.
- Automatically create matching users and devices in Aranda Datasafe
- Authenticate device connections to Aranda Datasafe.

You must install AD Connector on a domain-joined Windows server that is on-premises in your company. You must also register the AD connector so that it can connect to Aranda Datasafe.

Install and Register Active Directory Connector

The Active Directory Connector (AD Connector) is an application that Aranda Datasafe uses to authenticate its user accounts. Your encrypted data is only available to authorized users.

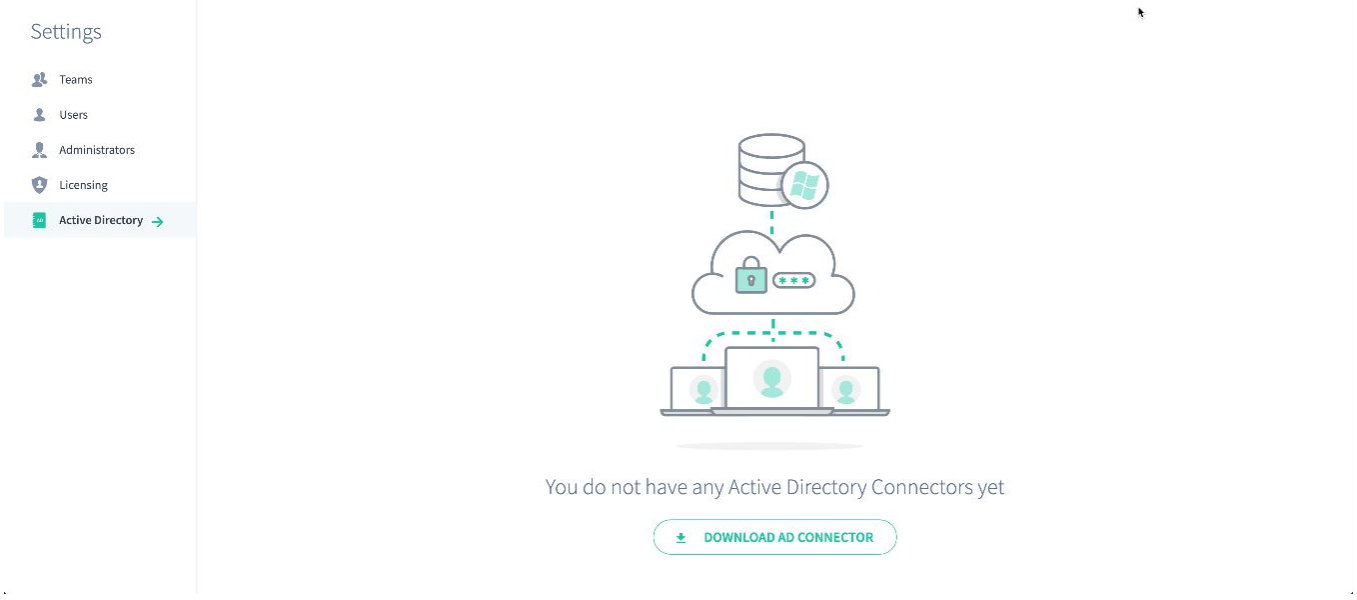
You must install AD Connector on a domain-joined Windows server that is on-premises in your company. You must also register the AD connector so that it can connect to Aranda Datasafe.

To download, install, and register the AD Connector software:

1. Click on**Settings**.

2. Click on**Active Directory**.

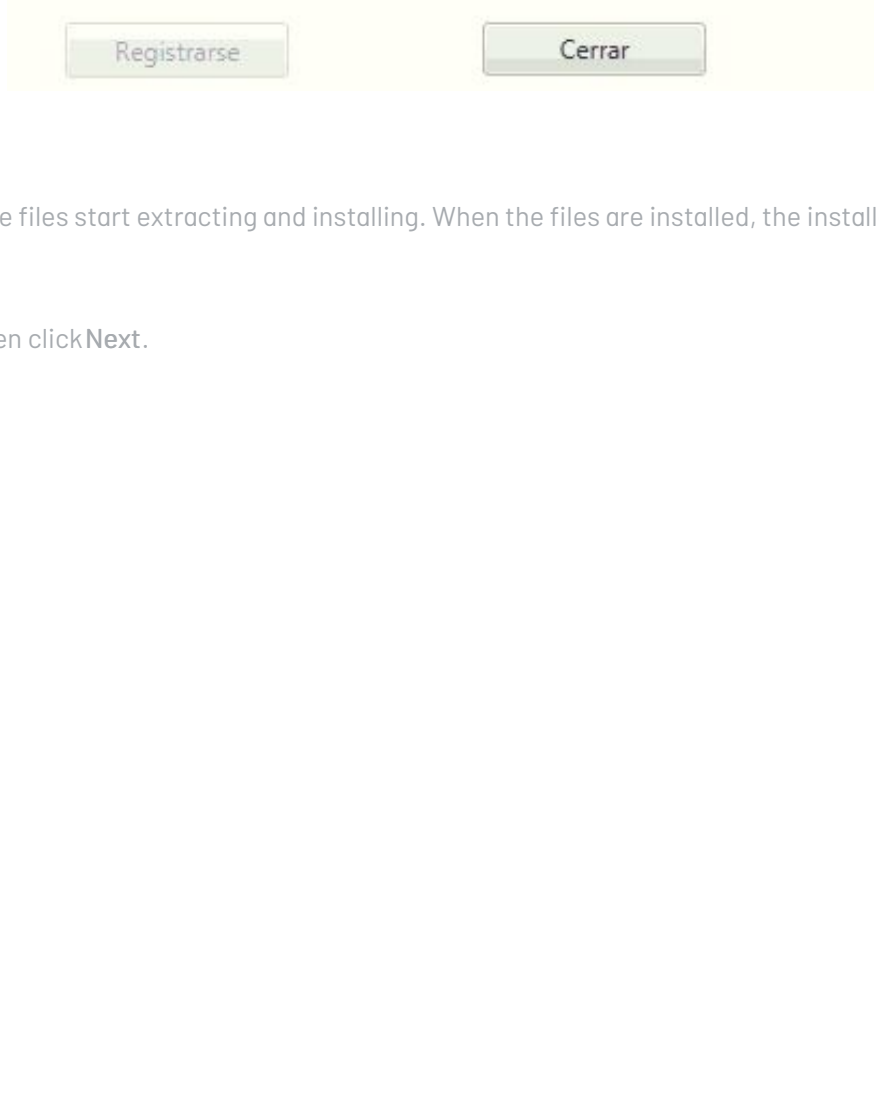
3. Click **Download Ad Connector** to download the adconnector executable file. Copy this file to your local server.



4. Log in to your local server (the server on which the AD Connector will run). You must log in through a domain administrator user account that has permission to register a Principal Service Name (SPN) for Kerberos connections.

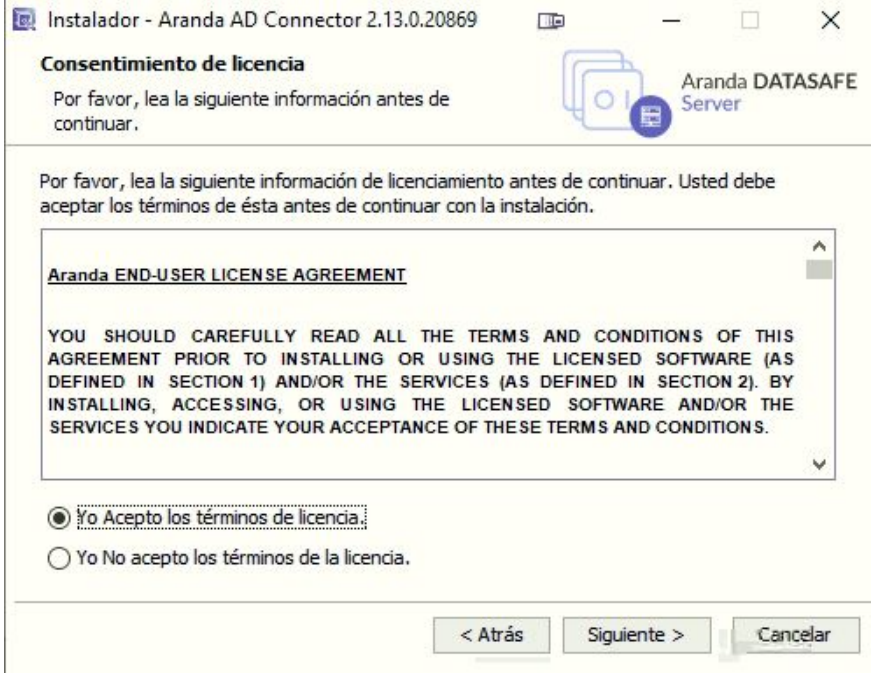
5. Copy the adconnector executable file to the server and then run it.

6. Follow the on-screen instructions to install the AD connector. You can install it in any directory (the default location is C drive).



When you complete the installation steps, the files start extracting and installing. When the files are installed, the installer asks you if you want to register.

7. Make sure **Register Now** is checked and then click **Next**.



8. Enter the registration details:

Field	Description
Domain	The name of your Aranda Datasafe tenant. This is usually the name of your organization and is the first part of your Aranda Datasafe tenant's address.
Username	Enter the username of an Aranda Datasafe account that has the Security Officer role. Only Security Officer user accounts have permission to register a repository.
Password	Enter the password for the Aranda Datasafe account.
Domain	Enter the name or IP address of the server that has the AD software installed.
Alias	Enter the name of the AD connector as it will appear in Aranda Datasafe. We recommend that you give it a descriptive name that your Aranda Datasafe users recognize.

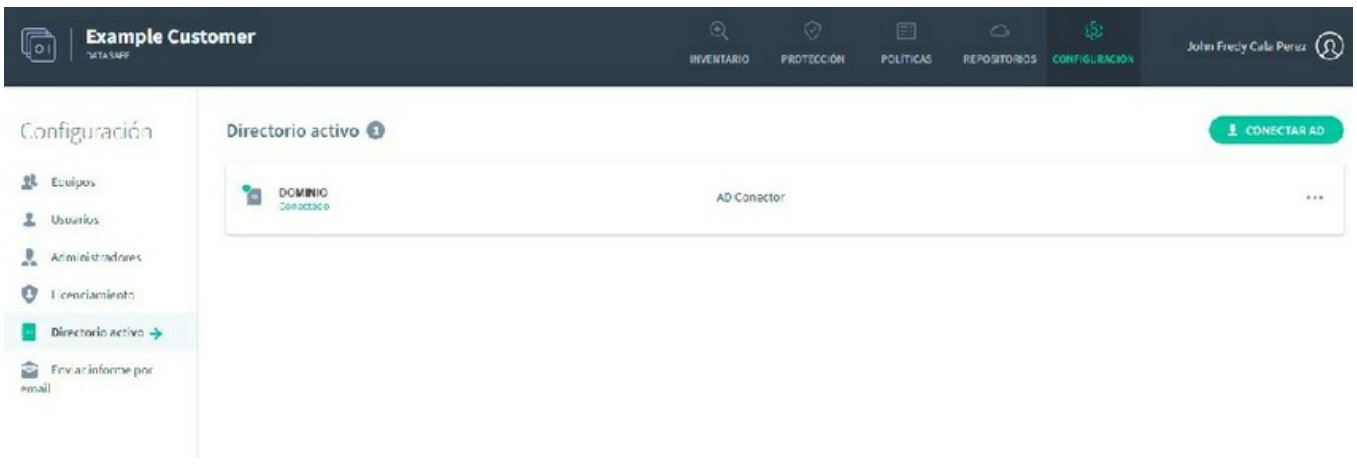
9. Click **Register**.

Remove Active Directory Connector

To remove an AD connector:

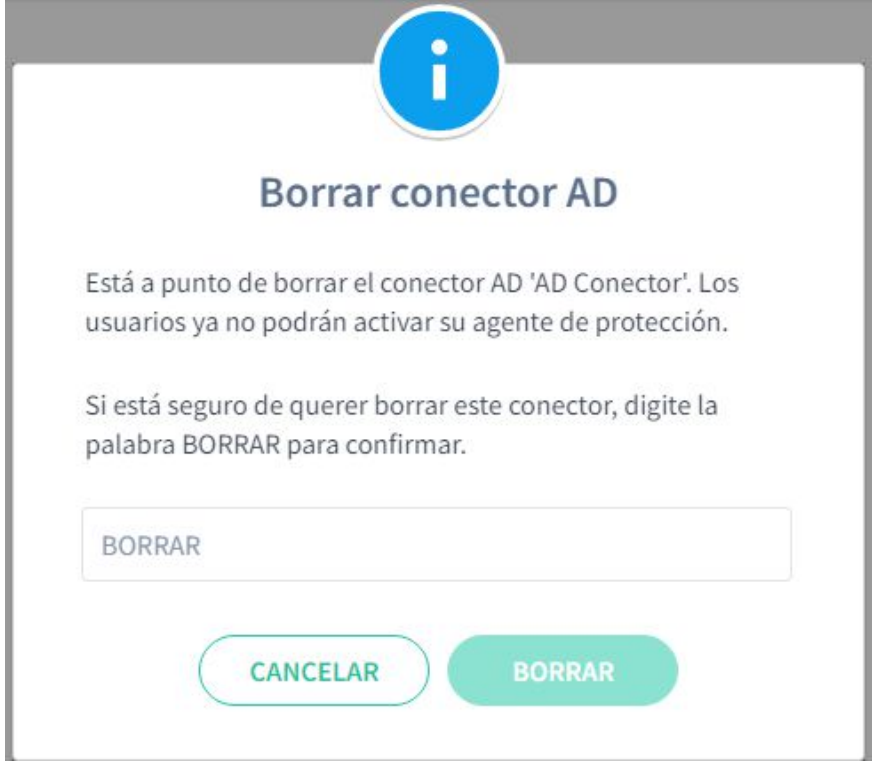
1. Click on **Settings**.

2. Click on **Active Directory** in the sidebar.



3. Find the Active Directory you want to delete and then click its radio button (...) and click **Delete**.

4. Enter CLEAR in uppercase letters in the dialog box to confirm.



5. Click **Delete**.

Licences

Licences

Aranda Datasafe requires you to have licenses for your users. When you purchase a commercial plan, you are assigned a number of licenses based on your requirements. If these requirements change, you can purchase more licenses and add them to your plan.

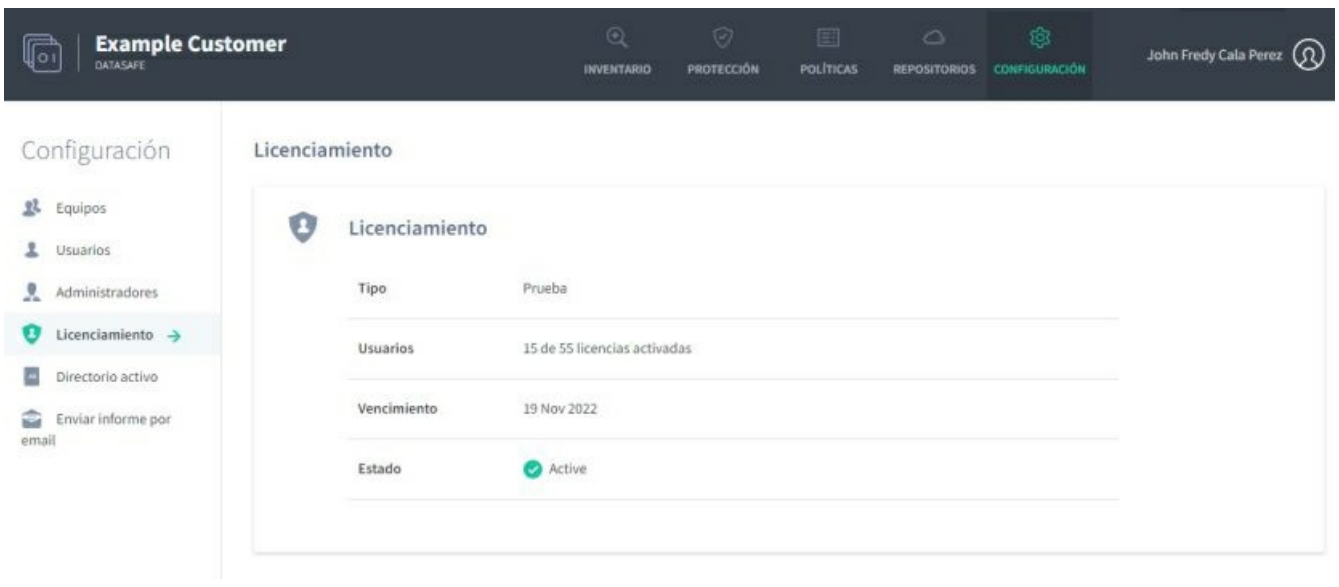
You can view information about your licenses in the Licensing page. Shows the number of licenses you have available and the status of your Aranda Datasafe subscription.

Licensing configuration

You can view information about your plan and available licenses on the Licensing page.

1. Click on **Settings**.

2. Click Licenses in the sidebar.



The Licensing page displays:

Field	Description
Type	Your Aranda Datasafe plan. Commercial: On the commercial plan, you can use Aranda Datasafe to back up and protect your devices for the duration of your subscription.
Users	The number of licenses that are currently in use and the number of remaining licenses available.
Expiration*	The date and time of the end of your Aranda Datasafe subscription.
Status	Shows whether your Aranda Datasafe subscription is active or expired. If your subscription expires, your devices are no longer backed up or protected and therefore at risk. To resubscribe, please contact your account manager.

Backup & Restore

Backup & Restore

Aranda Datasafe backs up your activated devices automatically, at scheduled times. Data is deduplicated and encrypted prior to transfer and remains encrypted during transfer and when stored in the repository.

What happens before the backup occurs?

To start backing up a device, you'll need to activate the device for protection. During activation, the protection agent will be downloaded and installed on the device. The protection agent will go through an authentication process before indexing and backups can begin.

Before the backup begins, the agent indexes the file system. The index is created once and is updated in real time as files are added, modified, or deleted from the file system. Real-time indexing **ensures that a time- and resource-consuming scan is not necessary at backup time.

What happens during a backup?

During a backup, the index is referenced for new and changed business data; A VSS snapshot is created and the data is deduplicated to ensure that only unique data blocks are encrypted and transferred from the user's device to the repository (storage area on your server).

Automatic Backup

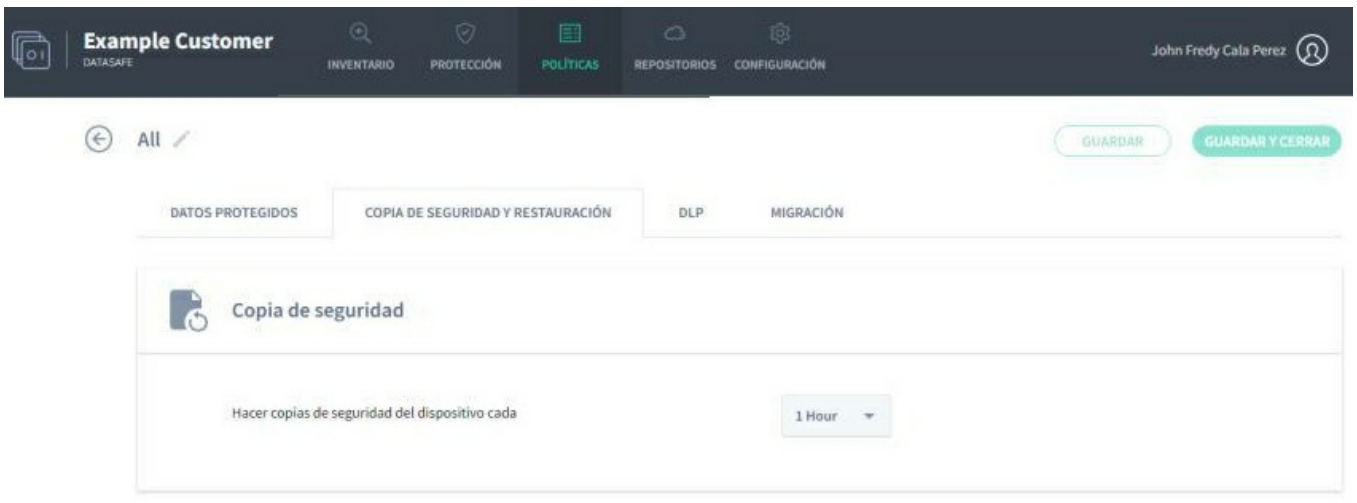
Aranda Datasafe automatically backs up business data to your devices, provided that:

- The device is activated
- The device is associated with a computer
- The team is associated with a policy and a repository.

The **repository** defines where the backup data is stored.

The **Politics** defines:

- What trading data is backed up
- When backups are made.
- Which Data Loss Prevention features are enabled.
- Whether user profile settings are backed up for computer migrations.



Your devices are automatically backed up and protected:

- **Shortly after they are activated for the first time** This is usually about 10 minutes, but it can take longer, as the backup can only happen after the Protection Agent has finished indexing.
- **Regularly** in accordance with the scheduled intervals set forth in the Policies.

Available options: **Every 1 hour	2 Hours	4 hours	8 hours**.

You can also make a Backup manually if you wish.

Running Aranda Data Safe Backup

When you have devices activated in Aranda Datasafe, your business data is automatically protected:

- Approximately 10 minutes after initial activation
- Regularly, in accordance with the backup schedule (as defined in the Policy).

You can also back up a device manually, either to Aranda Datasafe or by using the Protection Agent locally on the device. This is useful if you need to back up a device right away and the next scheduled backup shouldn't be done for some time.

Below, we explain the various ways you can **run a remote backup to Aranda Datasafe**:

Run a remote backup from the protection page .

Run a remote backup from the device page.

Run a remote backup from the protection page

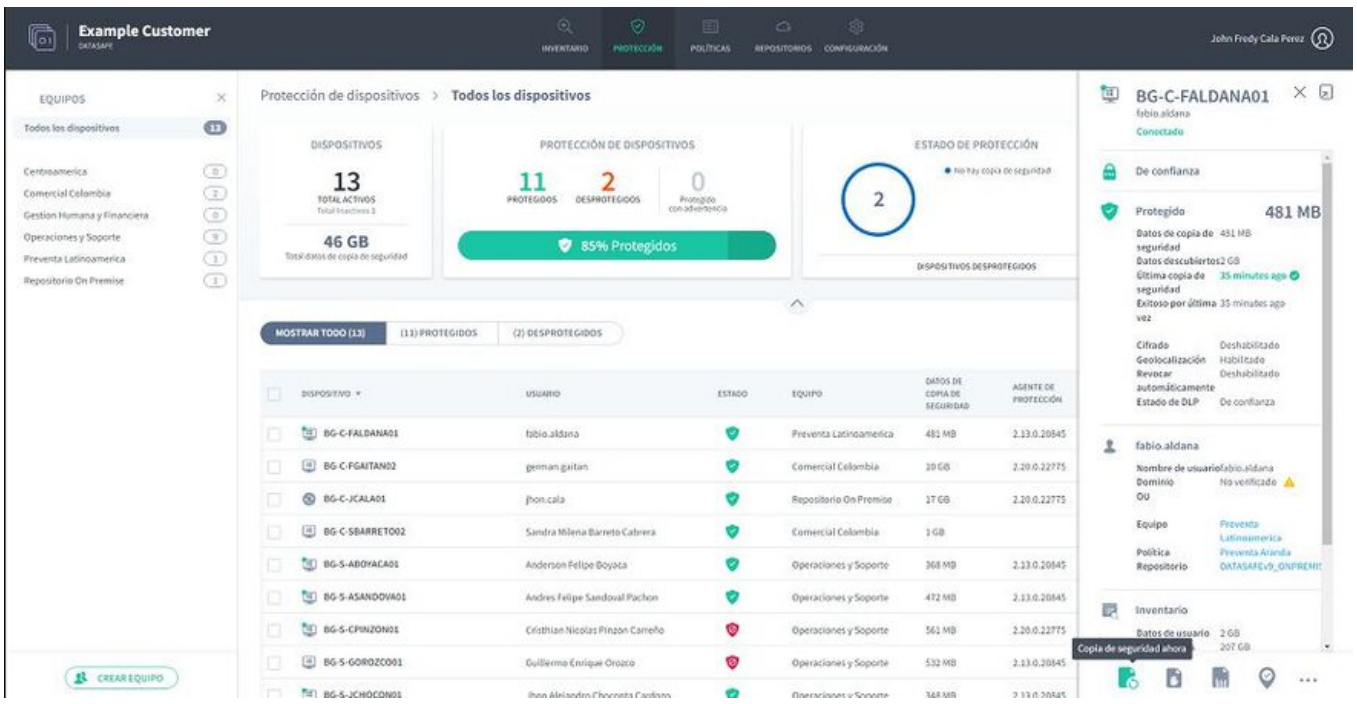
To run a backup from the Aranda Datasafe **Protection** page:

1. Click on **Protection**.

2. In the list of devices, click on the device you want to backup. Its details appear in a side panel.

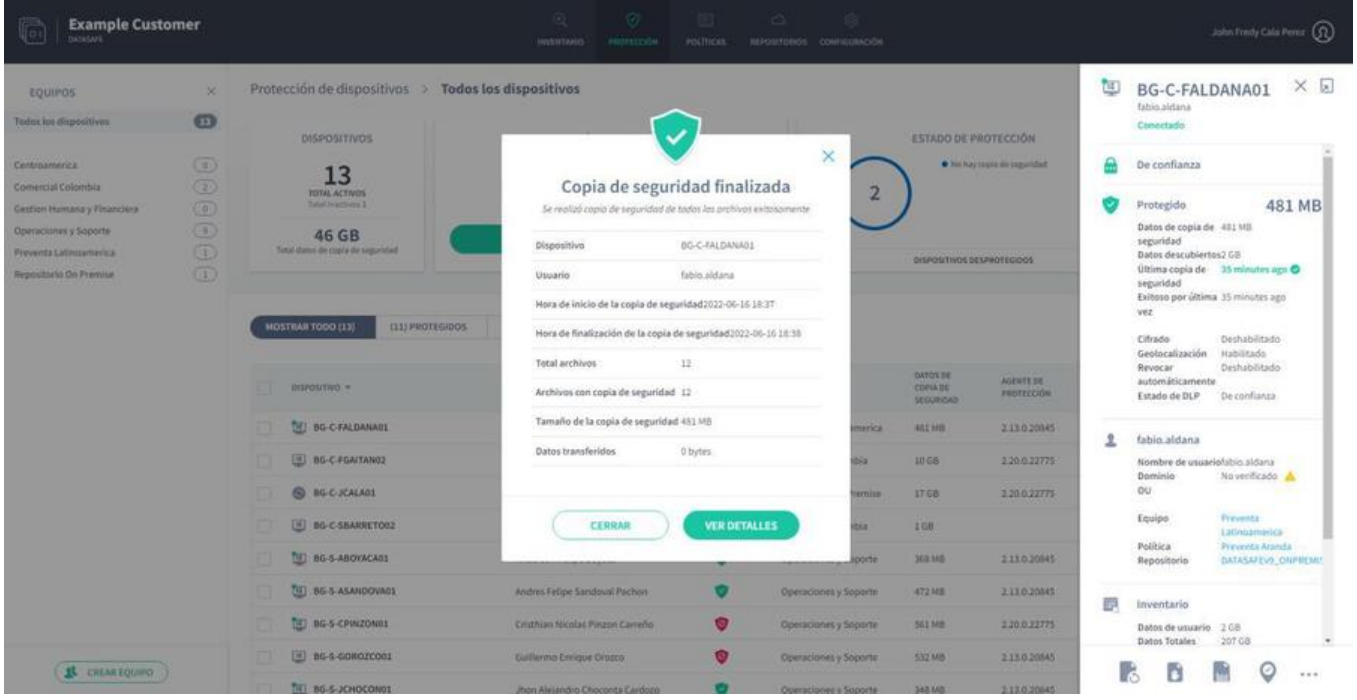
3. Click the **Back Up Now** icon at the bottom of the panel.

4. A message appears at the bottom of the screen to let you know that the backup request was successful.

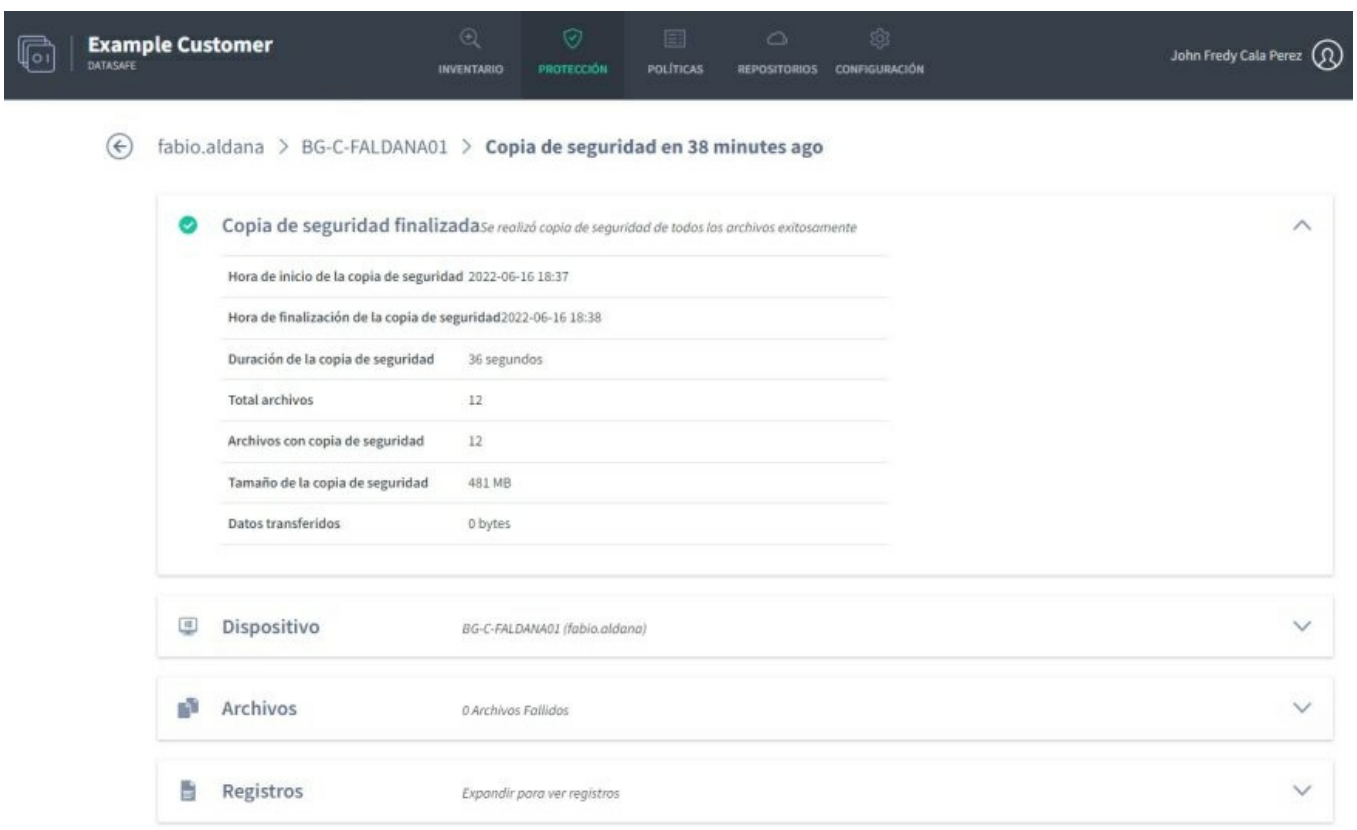


The Protection Agent software (on the user's device) uses deduplication to ensure that only new or changed data is backed up in the repository. The amount of time it takes to back up a device will vary, depending on the amount of data that needs to be indexed and backed up.

5. In the side panel, click the link next to the **Last Backup** entry to display a summary of the backup.



6. For more detailed information about the backup, click **View Details**. You can then view the details of the backup, the device, the files that could not be backed up, and the log data.



Run a remote backup from the device profile page

To run a backup from the device profile page:

1. The first step is to access the list of devices on the **Inventory** page or on the **Protection** page.

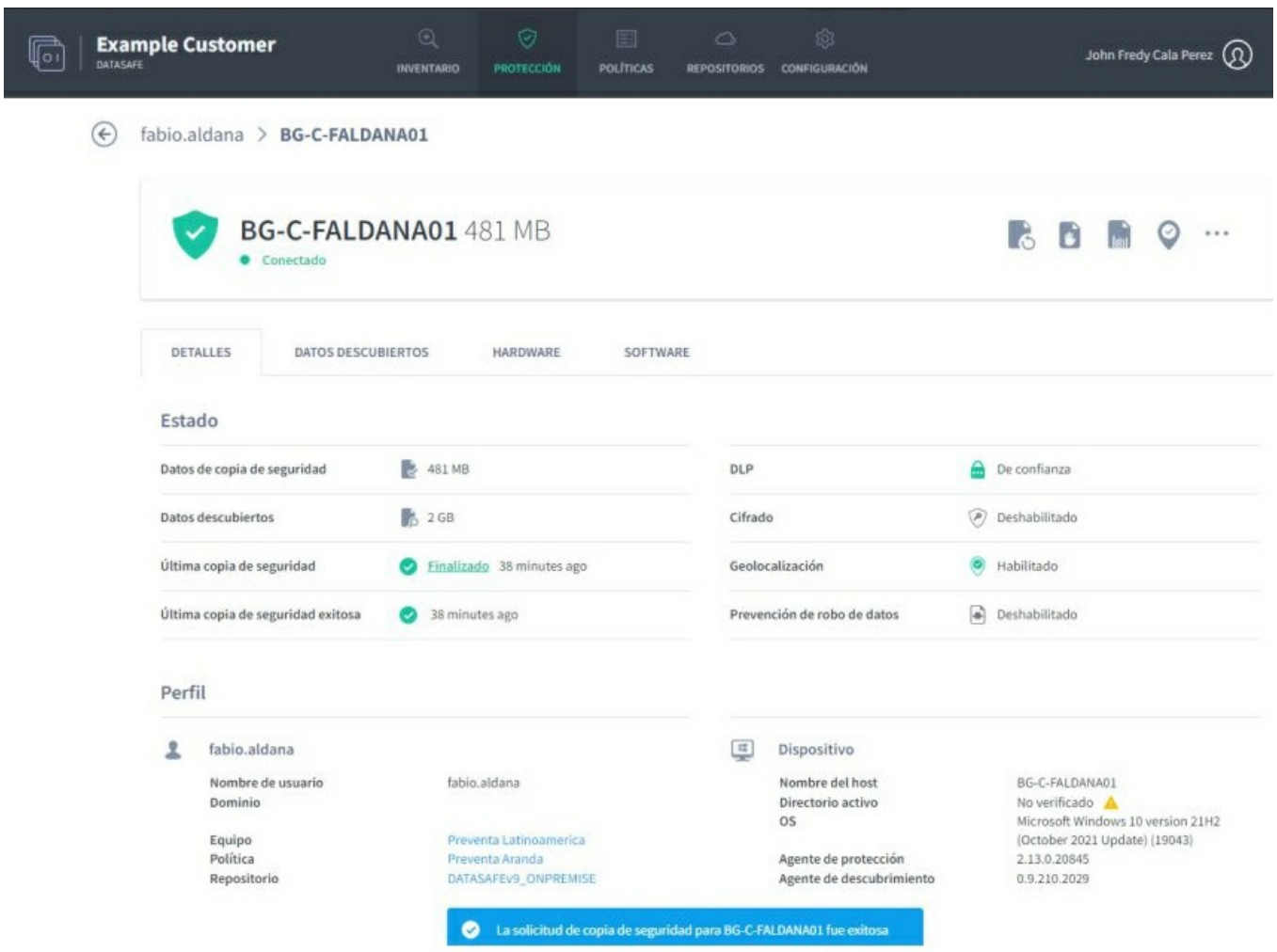
Click on **Inventory**. Or:

Click on **Protection**.

2. In the list, click on the device you want to back up. A side panel appears that shows information about the device you selected.

3. Click the Details icon in the top corner of the side panel to display the device's profile page.

4. On the device profile page, click the**Back Up Now** icon.

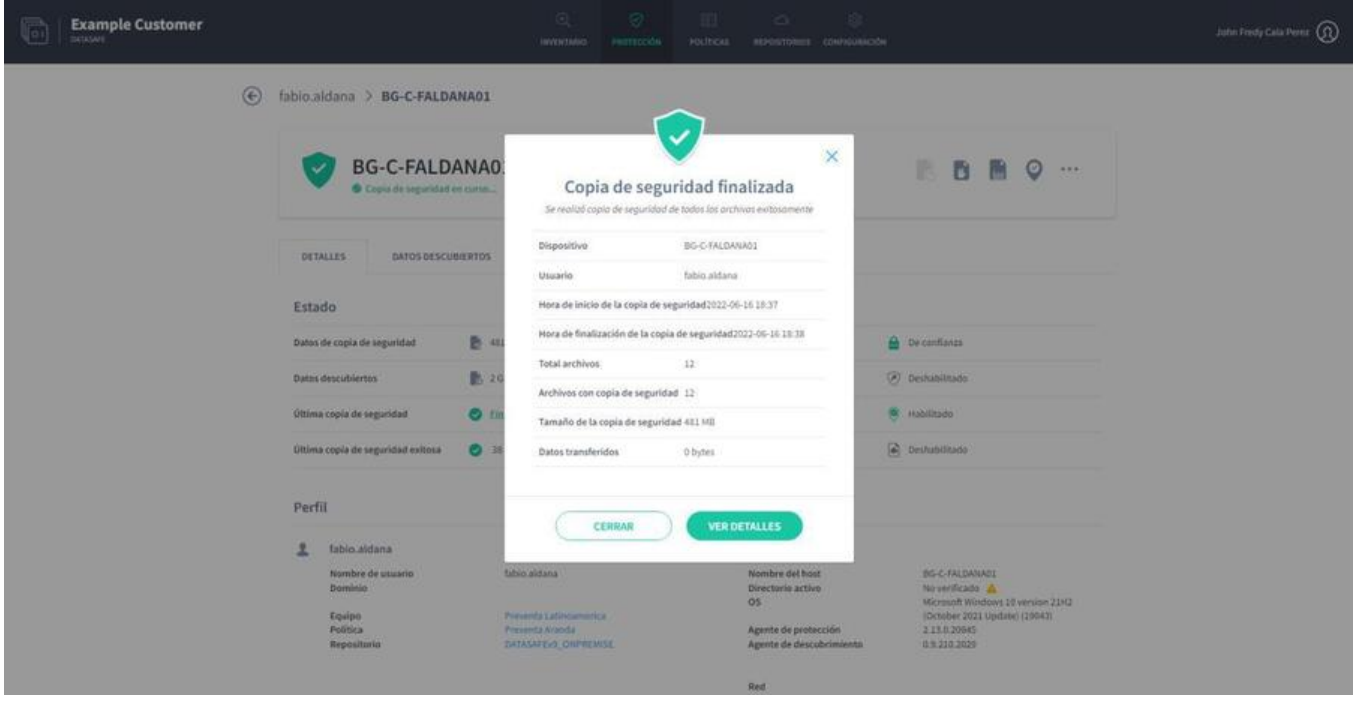


A message appears at the bottom of the screen to let you know that the backup request was successful.

The Protection Agent software (on the user's device) uses deduplication to ensure that only new or changed data is backed up in the repository. The amount of time it takes to back up a device will vary, depending on the amount of data that needs to be indexed and backed up.

5. When the backup is complete, click the link in the Last Backup entry in the Details tab of the device profile page. Aranda Datasafe displays a summary of the backup.

6. For more detailed information about the backup, click **View Details**. You can then view the details of the backup, the device, the files that could not be backed up, and the log data.



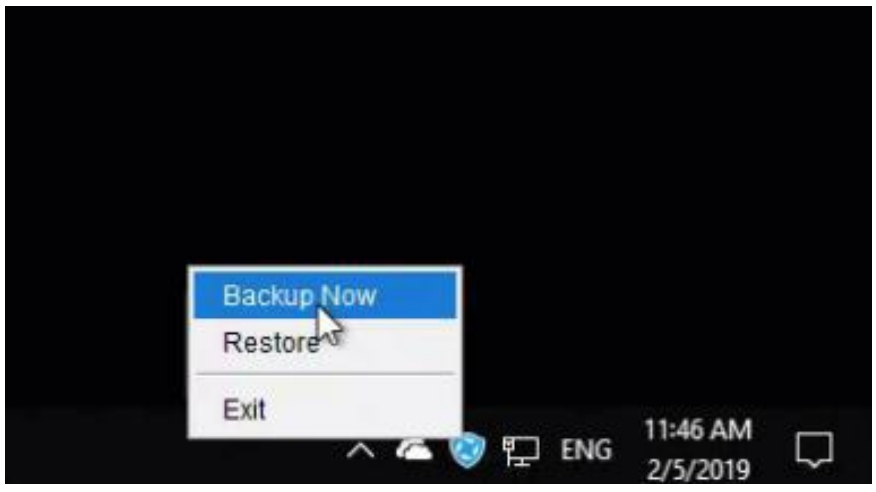
Running Agent Backup

There are three ways to back up your data to Aranda Datasafe:

1. Aranda Datasafe backs up your activated devices automatically, at the intervals defined in the Policies for your devices (see Schedule automatic backups).
2. You can start a manual backup remotely from Aranda Datasafe (see Run a Remote Backup from Aranda Datasafe).
3. You can initiate a manual backup from an activated local device (see below).

Each activated device must have the Protection Agent software installed. This agent is required if you are going to perform a manual backup from a local device.

1. Right-click the Protection Agent icon in the Windows system tray.
2. Click Back Up Now to start a backup.



Backup Details and Logs

If the Protection page shows that you have unprotected devices or devices that are protected with a warning, you can find more information in the last device backup event log. Aranda Datasafe keeps a record of the last backup attempt for each connected device.

To view a device's backup history and logs:

1. Click on **Protection**.
2. In the Devices list, click on a device to display the device details in a slide-out panel.
3. Click the View icon in the top corner of the slider panel to display the device's profile page.
4. On the Device page, click the link in the **Last Backup** entry (on the Details tab).
5. In the backup summary dialog box, click **View Details** to display the device backup log.
6. Expand the backup log sections to view the details of the last backup.

Restore Device

Important: You can only restore user data and profile information if the user's data has been backed up to Aranda Datasafe.

If Aranda Datasafe has backups of data on protected machines, you can restore them at any time. Normally, you would use the restore feature if:

- You have accidentally deleted a protected file and want to add it back to your device
- You have a new device and want to download the protected data that was previously on a different device. For example, if you are replacing an old laptop, you can use **Restore** to add the protected files from the old laptop to the new laptop.

If the policy has **migration** enabled and the **Microsoft Windows User Profiles** option is selected, you can also restore the user profile settings.

To **restore** files on a device:

1. Log in to the device that will receive the backup of the data from Aranda Datasafe.

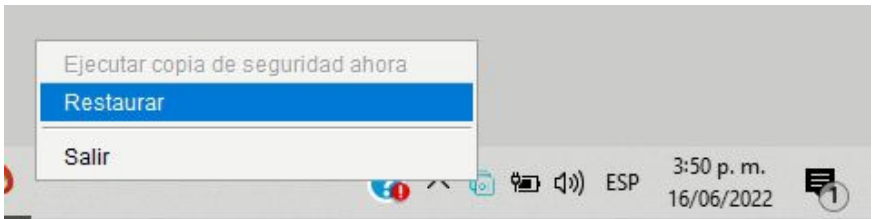
If your device already has Discovery Agent installed, ignore steps 2 and 3 and continue from step 4.

If you need to restore data to a new device or a device that has not been protected by Aranda Datasafe before, you need to install Discovery Agent. Continue from step 2.

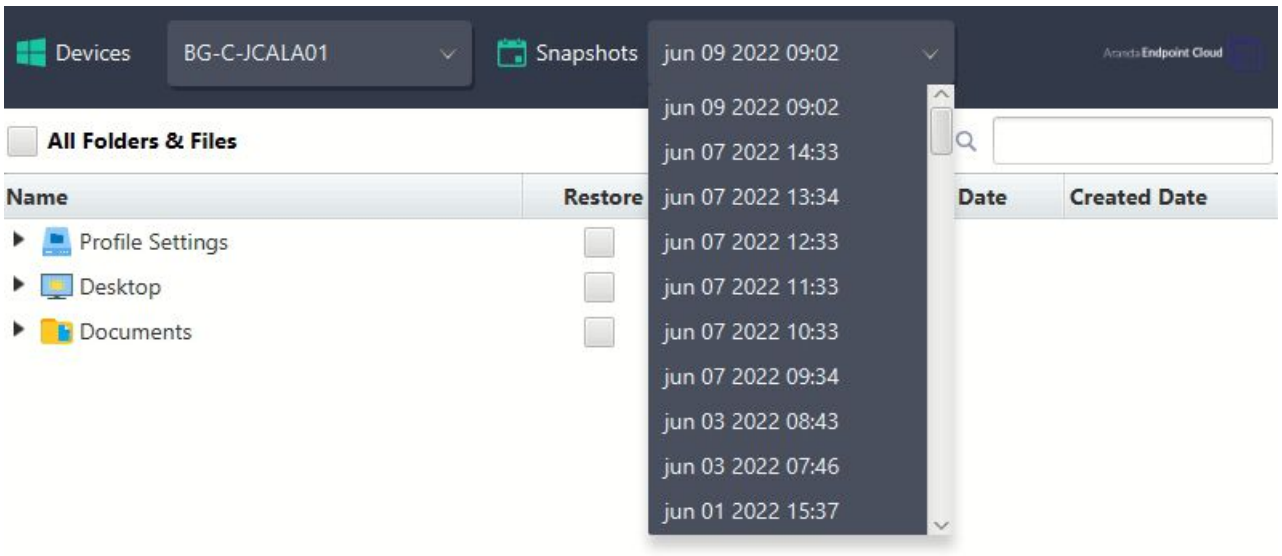
2. Install Discovery Agent on the device, so that Aranda Datasafe can detect it. For more information, see Discovery Agent Installation and Deployment.

3. In Aranda Datasafe, activate the new device. For more information, see Activating Your Devices.

4. In the Windows system tray, right-click the Protection Agent icon and select **Restore**.



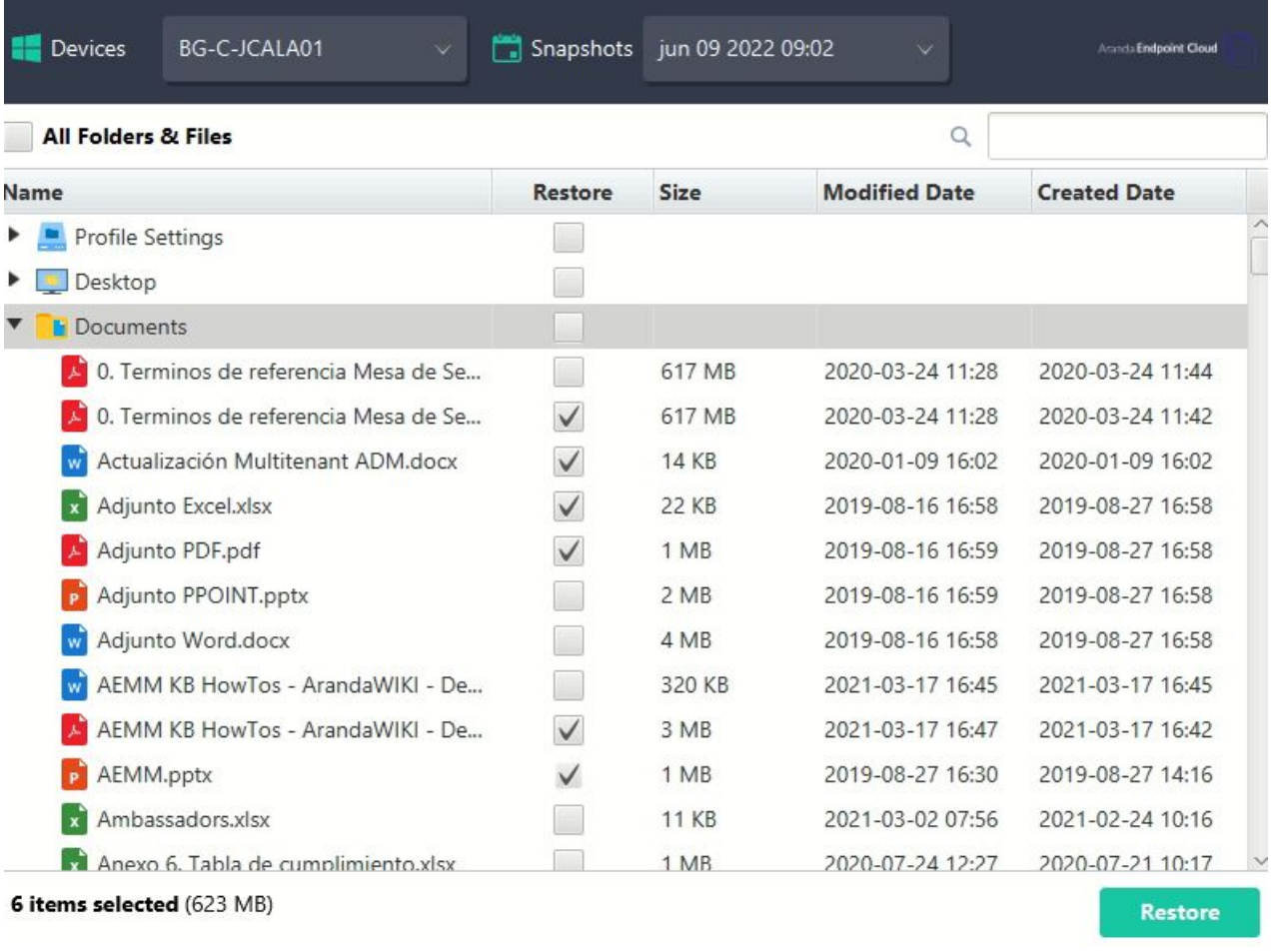
5. At the top of the Aranda Agent, choose the device and associated snapshot that you want to migrate to the new device. The snapshot is a record of a device's data at a specific point in time, and you can choose from any of the times shown in the list.



6. Choose which files you want to restore. You can choose **All folders and files**, all **desktop files**, all documents** or all files in volumes (drives). Alternatively, you can select individual files.

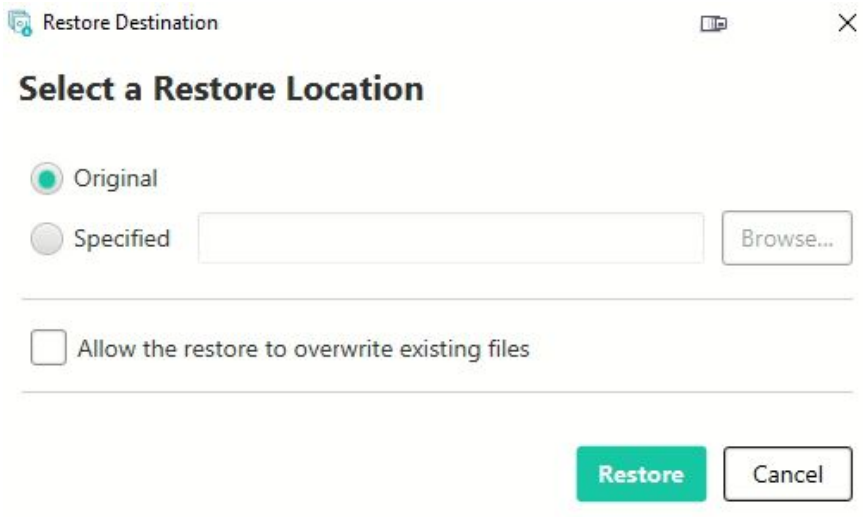
If the policy has **migration** enabled and the **Microsoft Windows User Profiles** option is selected, you can also restore the user profile data. Select the **Profile Settings** option to restore these settings.

If the **migration** feature is disabled or the **Microsoft Windows user profiles** are not selected, you can only choose to restore the backup data.



7. Select **Restore**.

8. Choose the restore location of the files. If you choose **Original**, the files will be uploaded to the same location they had on the previous device. Or you can choose a different **specified** location if you prefer.



9. Select **Restore**.

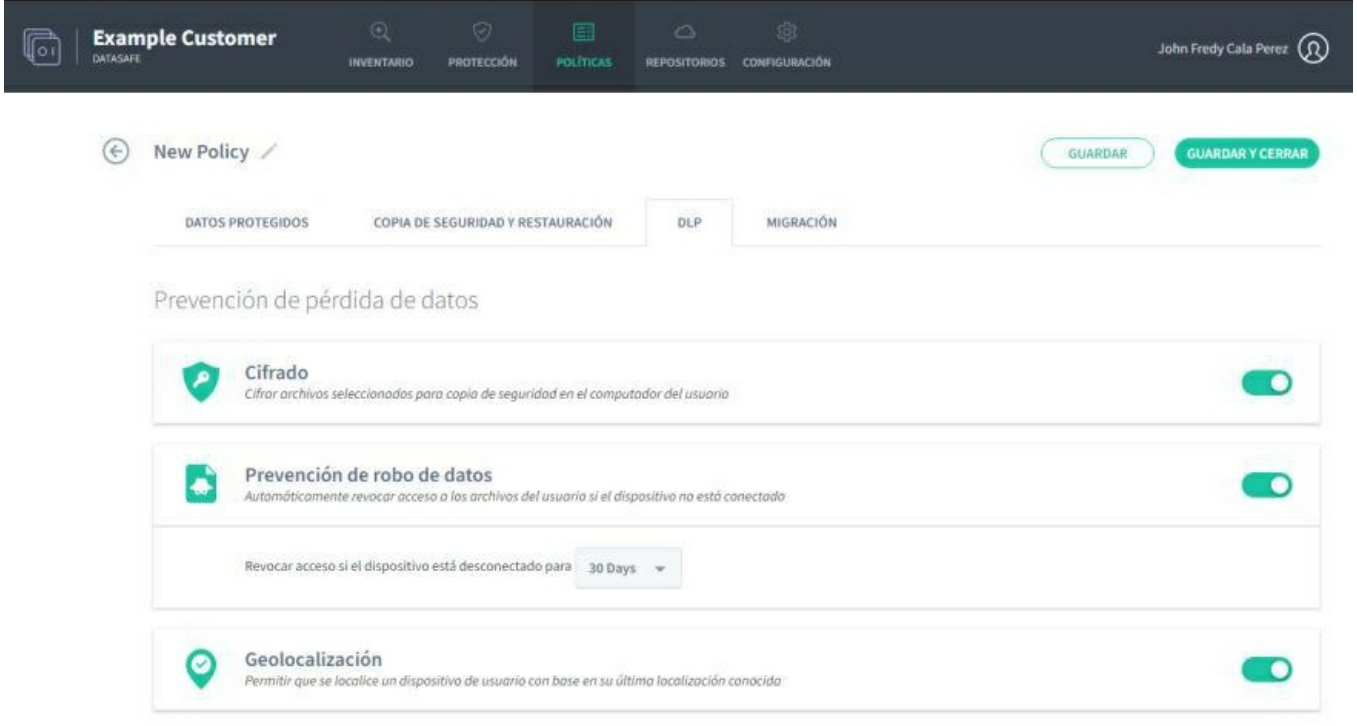
The selected data is downloaded from Aranda Datasafe to your device. If you've chosen desktop files, you'll see them appear on the desktop.

If you are restoring backup data and user profile settings, the restore will be completed in two separate phases.

Data Loss Prevention

Data Loss Prevention

Aranda Datasafe has many Data Loss Prevention (DLP) features that are designed to protect your company's data if one of your devices is lost or stolen.



DLP features allow you to:

- Enable local file encryption. This encrypts the data on your user devices to ensure that security and access to data are controlled. For more information, see Enable local encryption.
- Have automatic data theft prevention. If a device is disconnected from Aranda Datasafe for a certain period of time, the Aranda Agent will prevent access to the encrypted data on the device. (This only applies when local encryption is enabled) For more information, see Enable data theft prevention).
- Use geolocation to find the last known location of the device, based on its wi-fi signal (see Find devices with geolocation).
- Use Aranda Datasafe to Securely erase a device so that your data no longer exists on the device.
- Use Aranda Datasafe to Revoke access to encrypted data on the online device (only applies when local encryption is enabled). When a device is revoked, its encrypted data is not available, but it can be Cancel if you want to make your data available again.

You can turn DLP features on or off for each policy (see Turn on data loss prevention features).

If one of your devices is missing or stolen, see If a device is lost or stolen.

Lost or Stolen Device

If a device protected by Aranda Datasafe is lost or stolen, you can:

Find the device

If the Device Policy has Geolocation enabled, you can use Aranda Datasafe to find the last known location of the device. The location is shown in Aranda Datasafe on an embedded Google map. This feature uses the device's Wi-Fi connections to identify the last known location and therefore requires the device to be Wi-Fi enabled.

For more information on geolocation, see Find devices with geolocation.

Revoke the device*

If your device policy has local encryption enabled, you can revoke the device. This can be a good option if you suspect that a device has been lost, rather than stolen.

With a revocation, you tell Aranda Datasafe to remotely remove the encryption certificate from the device. As soon as the agent receives the instruction, the certificate is deleted, and the encrypted data on the device cannot be accessed or used. Therefore, anyone using the device will not be able to access your data.

You have the option to override the revocation later. Revocation will put the encryption certificate back on the device to make the encrypted data available again.

For more information, see:

- Revoke a device
- Revoke a device

Device wipe

You can use Aranda Datasafe to perform a "forensic wipe" of the device. Erasing securely deletes data from your device. It involves a revocation of the encryption certificate and a series of deletions that delete the data and then wipe it again to remove any traces of your data.

For more information, see Clean a device remotely.

⚐ >**Note:** You can configure Aranda Datasafe to automatically revoke a device if the device does not connect to Aranda Datasafe within a certain period of time.

Enable Prevention Features

You can edit a policy and turn each of the DLP (Data Loss Prevention) features on or off as needed. But keep in mind that the Policy settings apply to all computers that use the Policy.

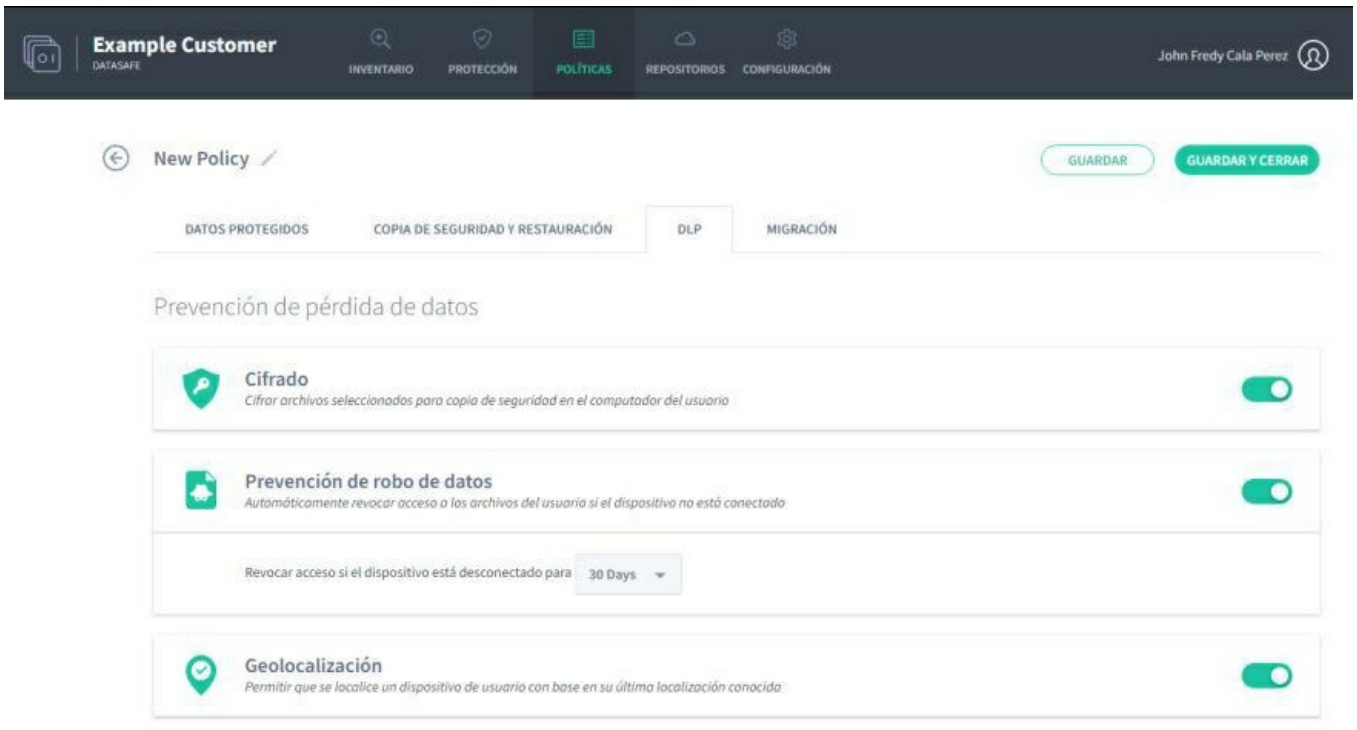
1. Click on **Policies**.

2. Click on the Policy you want to edit.

3. Click on the **DLP** tab.

4. Use the sliders to enable or disable each DLP feature (green is enabled, gray is disabled).

5. Click on **Save** or **Save and close**.



Find Devices with Geolocation

You can use geolocation to find the last known location of a device, provided that:

- The device has WI-FI enabled
- The **geolocation** feature is enabled in the policy (used by the device team).

To discover the last known location, Aranda Datasafe connects to Google Maps. The location is estimated based on:

- The coordinates of the last WI-FI access points that your device located
- The signal strength of your device to the access point.

The location is estimated based on the WI-FI signal, no GPS is needed.

To use Aranda Datasafe's geolocation to find a device:

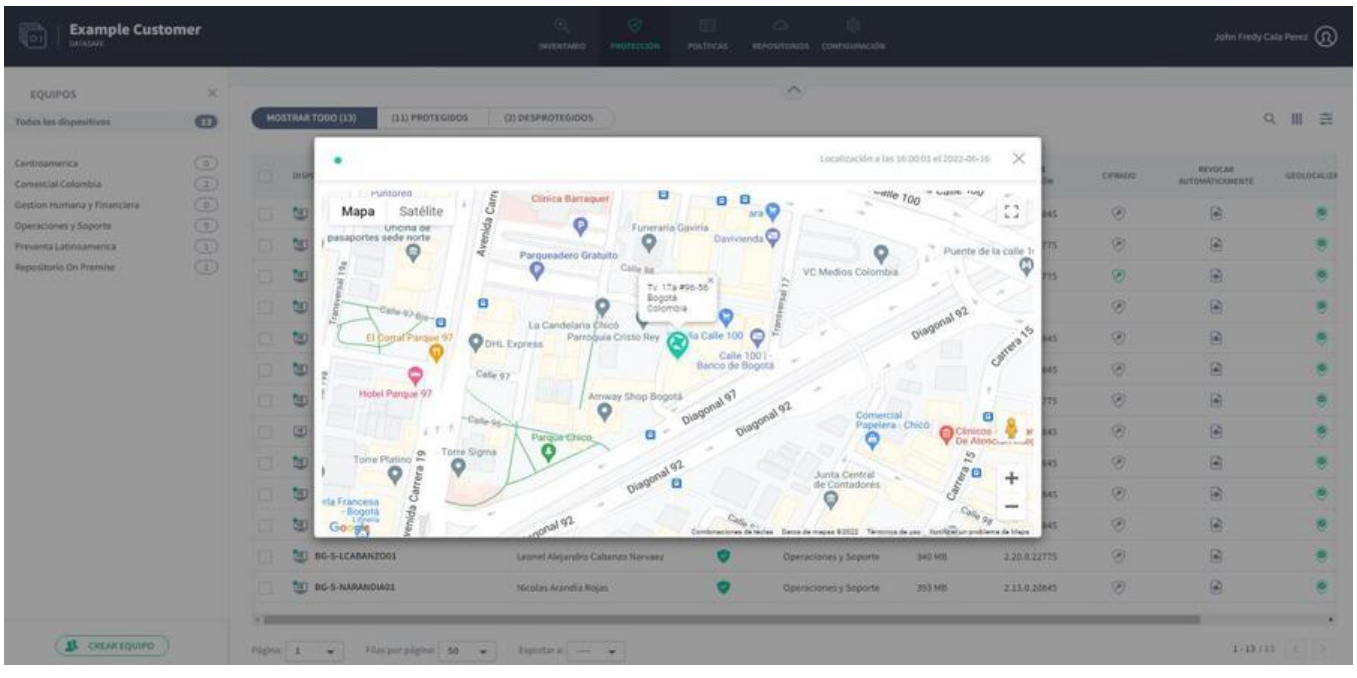
1. Click on **Inventory** or **Protection**.

2. In the list of devices, click on the device you want to locate. Its slide-out panel appears.

3. Click on the **Geolocate** icon.

The last known location is shown on a Google map. You can zoom in, zoom out, and show the satellite view.

⚐ >Note:** The geolocation icon is also available on the device profile page (from the Inventory or Protection page, display the device slider panel, then click the view details icon to display the device profile page).



Revoke Device Access

If you enable local encryption on a policy, each device that uses that policy receives an encryption certificate. When a user logs on to a device, they can only access the encrypted data if the certificate is in place.

If a device is lost or stolen, you can use Aranda Datasafe to remotely wipe the device's certificate. Once the certificate is deleted, anyone, including the logged-in user, will not be able to access the encrypted data on the device (since the certificate is not on the device).

Using Aranda Datasafe to delete a certificate is known as "revoking a device."

To revoke a device:

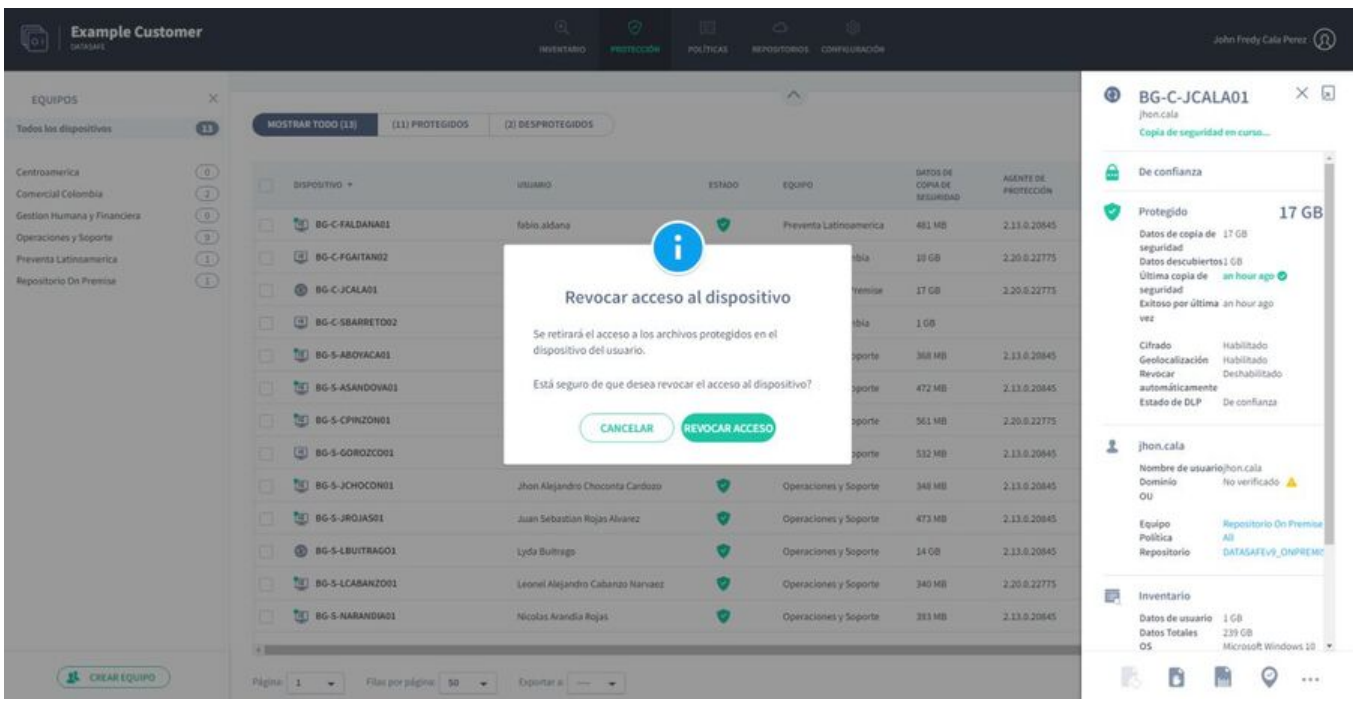
1. Click on **Inventory** or **Protection**.

2. In the list of devices, click on the device you want to revoke. The slide-out panel on your device appears.

3. Click on the **Revoke Device** icon.

⚐ > Note: The Revoke Device icon is also available on the device's profile page (on the Inventory or Protection page, display the device's side panel, and then click the view details icon to display the device's profile page).

4. Click Revoke to confirm. The request to revoke the device is made. You can cancel the revocation request if necessary (display the device slider panel or device page, and then click the Cancel Revocation icon).



⚐ > Note: If Auto Revoke is enabled in a Policy, Aranda Datasafe will automatically revoke the certificate of any protected device that does not connect to Aranda Datasafe within a period of 30 days. (You can change the automatic revocation time period in the policy settings.)

Remote wipe to device

If you want to delete files from a device that is missing or stolen, you can use the **Erase** feature. This completely removes the protected files from the device (unlike Revoke, which leaves the files in place but makes them inaccessible).

With a cleanup, use Aranda Datasafe to perform a remote "forensic erase," which removes protected files on the device. As part of the "forensic erase", Aranda Datasafe removes the encryption certificate and performs a series of additional deletions to completely remove any traces of the protected data from the device.

To erase a device:

1. Click on **Inventory** or **Protection**.

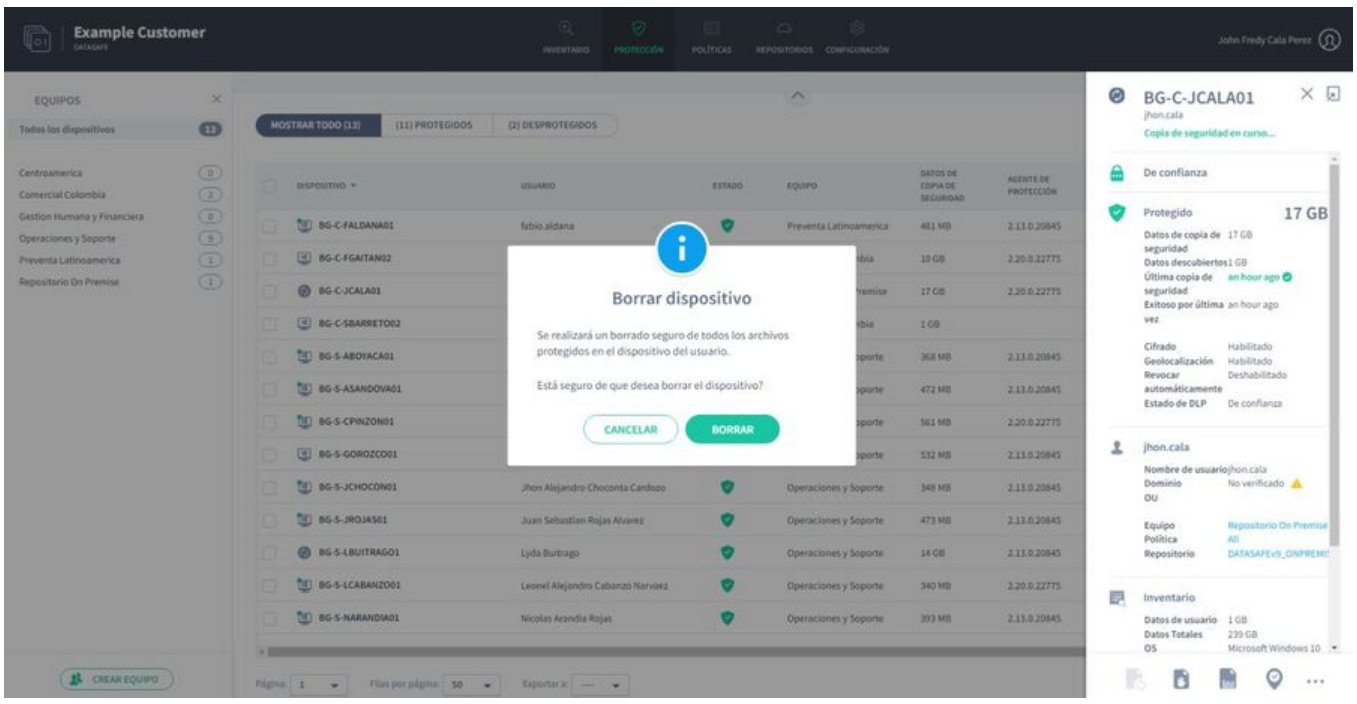
2. In the list of devices, click on the device you want to erase.

3. Click on the **Delete** icon.

4. Click **Delete** to confirm. Cleaning is set as pending, and after a short delay, cleaning begins. While the cleanup is pending, you can cancel it (click the **Cancel Erase** icon in the device slider panel or on the Device page). When the cleaning has started, it cannot be canceled.

The amount of time it takes to complete the erase varies, depending on the size and speed of the disk.

⚐ > Note: The wipe icon is also available on the device's profile page (from the Inventory or Protection page, display the device's slider panel, and then click the view details icon to display the device's profile page).



Override Device Revocation

In Aranda Datasafe, you can revoke a device so that its protected files become inaccessible. This is to keep your data safe in case a device is lost or stolen. If the device is found, you can make the data accessible again using **Override**.

With a revocation override, Aranda Datasafe places the encryption certificate back on the revoked device. Once the certificate is on the device, it cannot be revoked and its protected data can be accessed.

To revoke a device:

1. Click on **Inventory** or **Protection**.

2. In the list of devices, click the device that you want to revoke. The slide-out panel on your device appears.

3. Click the **Unrevoke Device** icon.

4. Click **Unrevoke** to confirm. The request to revoke the device is made and the revocation is pending. When Aranda Datasafe completes the application, the revocation is complete.

While the revocation is pending, you can cancel the revocation request if necessary (display the device slider panel or device page, and then click the **Cancel Revocation Cancel**) icon).

Data Loss Prevention Status

You can view the status of **DLP** in the **Protection** section. Shows the number of devices that have local encryption, auto-revocation, and geolocation features enabled (in the Policy).

The DLP status is also displayed in the list of devices at the bottom of the **Protection** section.

Remote Migration

Remote Migration

Our remote device migration solution transfers all user data and profile settings to the new machine, while the user works. The data transfer is completely secure and you don't risk losing any user files.

IT staff can manage it remotely and users can simply start using the new machine with all its settings and files exactly as they were on their old computer.

- Remotely activate and monitor multiple migrations from Aranda Datasafe
- Device-to-device migration (no need for additional repository storage)
- Better network path discovery
- Automatically open/close Windows firewall
- Live migrations (full initial and updates for the following)
- Connection retry capability
- Compression and encryption
- Migrate all data (including business and personal)
- Migration of direct access to new locations
- Migrate cloud drive locations (not configuration)

- Profile migration
    - Taskbar settings, Windows folder options, network drives
    - Microsoft Outlook: All email accounts, PST files, email signature.

Remote Migration Preparation

Before you can migrate, the following checks are needed:

Origin and destination machines must be prepared

- Both machines must be in **Active** status and visible in the **Protection** window in Aranda Datasafe.
- The relevant user must log in to both machines.
- The target machine must have Windows and applications installed prior to migration. Many customers use a standard company image for their machines.

Preparing the target device

- There should be sufficient disk size on the target device.
- It is important that the disk configuration or partition is the same on both devices. If the source device has a C:\&D://volume, for example, and the destination device only has a C:\ volume, migrating the data into D:\ will fail.
- Make sure that applications such as MS Office, Antivirus, and other company applications are installed before running the migration. The **Inventory** information in Aranda Datasafe will show all the applications that are installed on the **Source** device.
- Discover and activate the target device in Aranda Datasafe if it is not already active and visible in the Protection window.

What can I expect from migration?

The full remote migration feature will copy all user data and profile settings to the target device.

What will be included in the profile settings?

- Email profile for Microsoft Outlook
- Email signatures
- Email storage files (PST files)
- Mapped unit locations
- Network printers
- Custom folder views
- Taskbar preferences

What will be excluded from migration?

-Applications

- Built-in file excludes as executables, system files, and temporary files
- Locked files will be excluded
- Disks and volumes that do not exist on the target device
- Migration will fail if the target disk size is smaller
- Locally connected printers will not be included
- Desktop background will not be migrated

Performing Remote Migration

Start a migration from Aranda Datasafe

1. Navigate to Protection in Aranda Datasafe.

2. Use the search function in the device list panel and search for the user you would like to migrate.

3. The search must result in at least two devices for the user. The current device and the new device

4. Click on the target device to open the side panel.

5. Click on the 3 dots at the bottom right of the side panel and select Migrate.

6. Select the device to migrate from from the drop-down menu and continue.

7. The migration will begin and show the progress.

Monitoring

After starting the migration, the administrator can continue to monitor the progress from Aranda Datasafe. The window may close while other management tasks are being performed.

The admin can check the migration progress at any time, by clicking on any of the devices involved in the migration and opening the event details from the side panel.

Perform an upgrade migration

Once the initial full remote migration has been completed, there are a few more steps before handing over the target device to the user:

- In the event that a user was working on the source machine while the migration was running, some files might be locked. This will be visible in the details of the migration event.
- It is important that the user closes all applications during the upgrade migration (later).
- In Aranda Datasafe you can start another migration. This will migrate any data that was in use by the user at the time of the initial migration execution.
- Once the upgrade migration is successfully completed, you can perform a logout/login to apply the profile settings to the new device.
- Be sure to apply other settings that are not covered by the full remote migration feature.
- Give the new device to the user and confirm with them that everything has been migrated.

Event Details

When the full remote migration is complete, you will be able to view the results and details of the migration event. Select the target device in Aranda Datasafe and click on the device name next to Migrated from.

The following information will be displayed:

- Start and end times
- Number of files migrated
- Size of the migration
- Successful vs failed files with failure reasons

Migration

Migration

Aranda Datasafe's migration feature makes it easy to transfer user profile settings from one device to another. Using the migration feature can save you a lot of time and effort when you need to upgrade or replace your devices.

Migrating Profile Settings

With the profile settings migration feature, you can back up user data and profile settings to a device in Aranda Datasafe. Then, you can restore them to another device. This makes it easier and faster to transfer common user data, such as desktop shortcuts, desktop files, documents, etc.

To use the migration feature, you must [enable it in the Policy] that the device you want to replace uses.

When migration is enabled, Aranda Datasafe will back up user data and profile settings. This takes place at the same time as the next business data backup (as defined in the Policy).

When the user's data and profile settings have been backed up, you can restore them to a new device.

Example: Let's say you have a laptop backed up and protected by Aranda Datasafe. The laptop will be replaced with a newer model.
Use the migration feature to back up the user data and profile settings of the current laptop.

When the new laptop arrives, you'll discover and activate the device in Aranda Datasafe. Then, use the Restore feature to transfer the user data and profile settings of the old laptop from Aranda Datasafe to the new laptop.

Your new laptop is updated with user data and profile settings (Outlook profile and signatures, mapped network drives, and various folder and taskbar settings, etc.).

Enable User Profile Migration Feature

You can use the user profile migration feature in Aranda Datasafe to back up Windows user profile information to a device. You can then transfer the information to a different device by performing a restore.

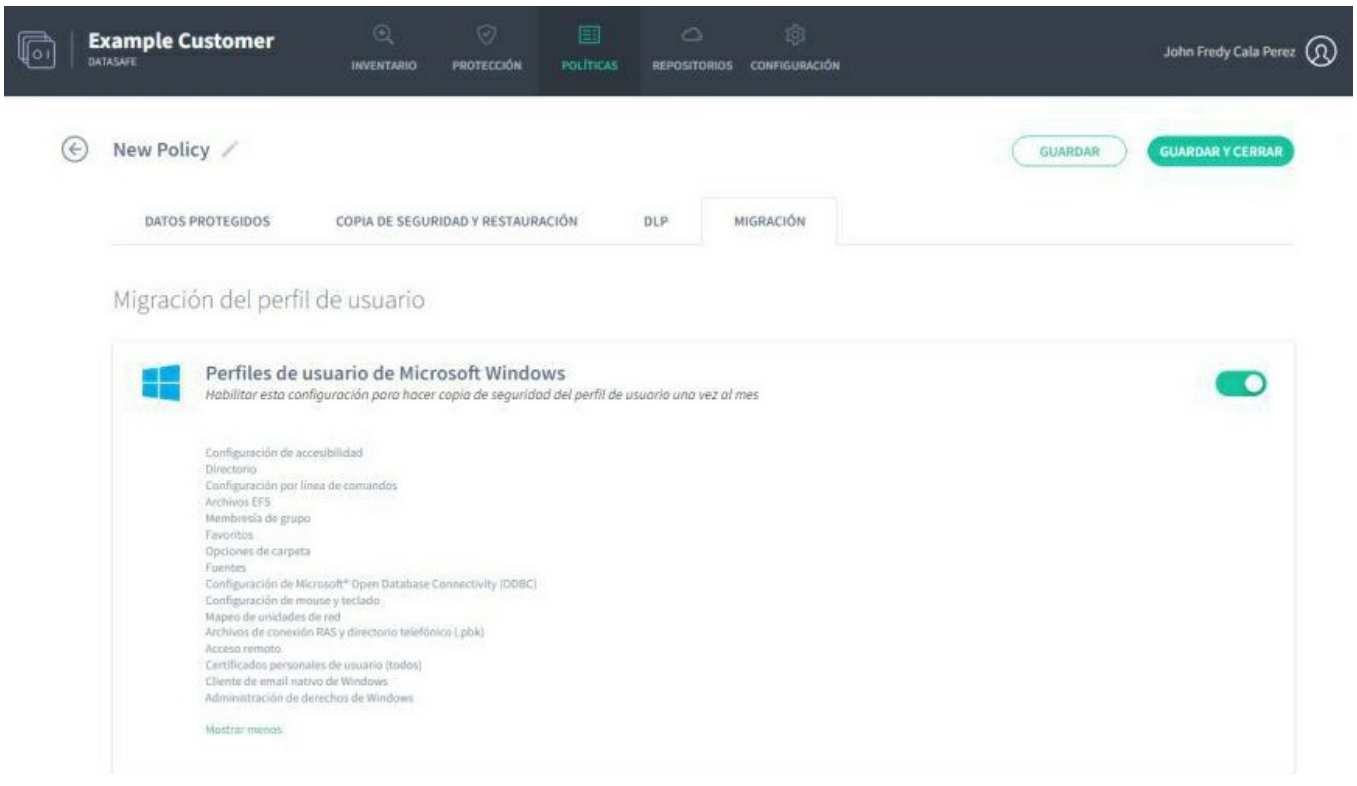
To use profile migration, enable it in the Policy used by the device you want to backup:

1. Click on **Policies**.

2. Edit the Policy associated with the Computer to which the device belongs.

3. Click on **Migration**.

4. Use the slider to enable **profile migration for Microsoft** Windows user profiles. (Green is enabled, gray is disabled.)



4. Click the **Show More** link to see a complete list of Windows user profile information that will be backed up. It includes taskbar layout, mapped network drives, folder options, email accounts, previously attached pst files, and email signatures.

5. Click **Save & Close**.

Aranda Datasafe will back up user data and profile settings on all devices associated with this Policy. The profile backup will be performed when the next backup of business data is made (as scheduled in the Policy). It will run once every 30 days to ensure it is updated regularly.

When a backup has been made, you can migrate the Setting up to a new device.

Disable User Profile Migration Feature

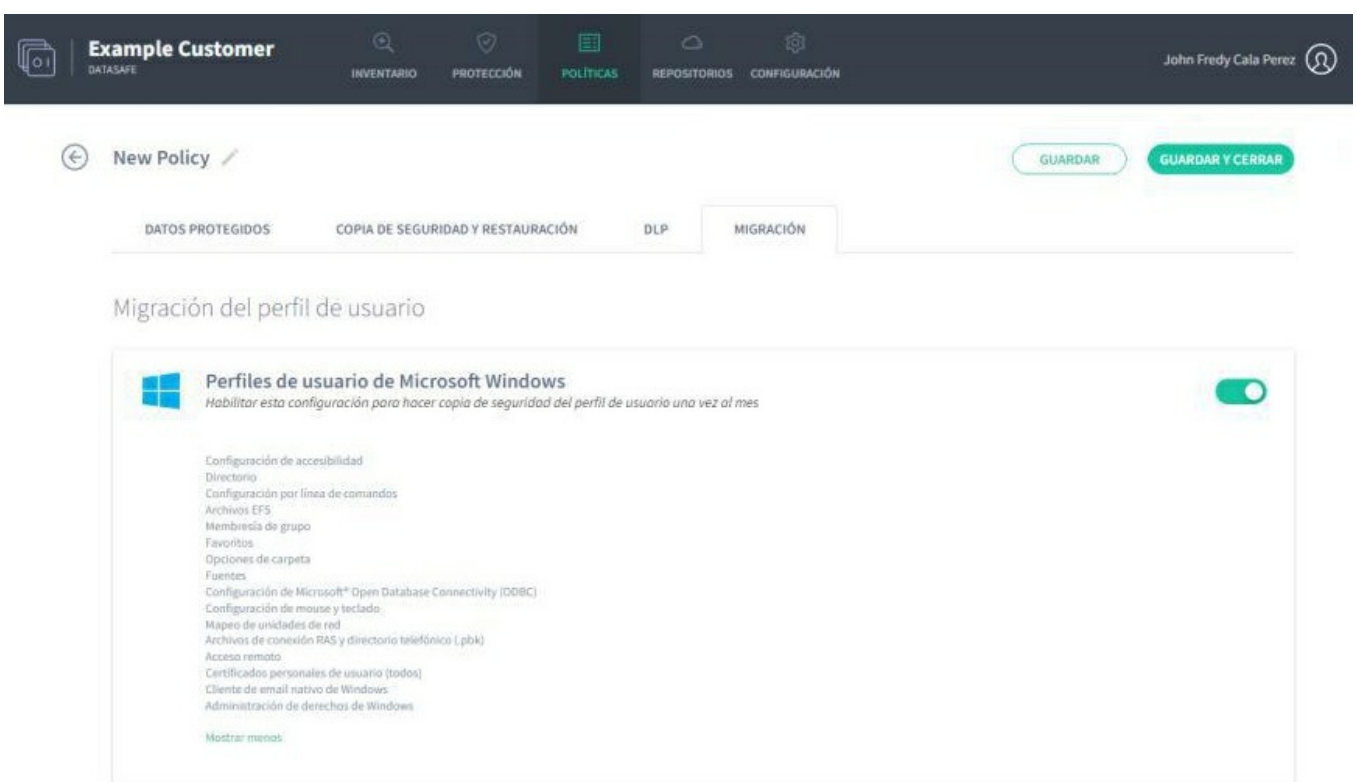
To disable the user profile migration feature so that Aranda Datasafe does not back up Windows user profile data:

1. Click on **Policies**.

2. Edit the Policy associated with the Computer to which the device belongs.

3. Click on **Migration**.

4. Use the slider to disable profile migration for Microsoft Windows user profiles. (Gray is off, green is off.)



5. Click **Save & Close**.

Aranda Datasafe will **not** back up user data and profiles on all devices associated with this Policy.

Migrate User Profile Data to Device

If you have enabled migration in a Policy, you can use Restore to transfer Windows user profile data (and backup data) from an old device to a new device (via Aranda Datasafe).

⚐ > Note: You can only restore user profile data from another device if migration is enabled and the "old" device has been backed up. To learn how to enable the migration feature, see Enable the migration feature.

To **restore** files on a device:

1. Sign in to the new device.

If your device already has Discovery Agent installed, ignore steps 2 and 3 and continue from step 4.

If you need to restore data to a new device or a device that has not been protected by Aranda Datasafe before, you need to install Discovery Agent. Continue from step 2.

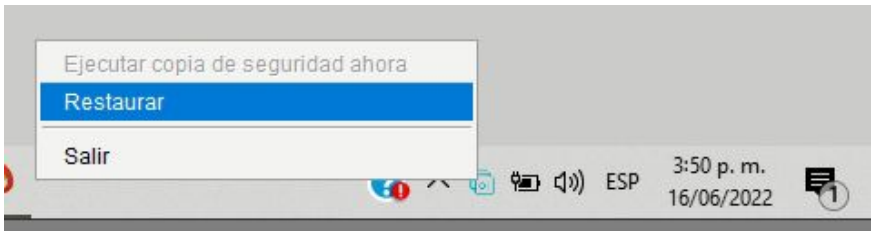
2. Install Discovery Agent on the device, so that Aranda Datasafe can detect it. For more information, see Discovery Agent Installation and Deployment.

3. At Aranda Datasafe, Activate the new device.

For more information, see Activating your devices.

⚐ > Note: Aranda Datasafe uses the Windows user account on the new device to identify which old device is being replaced. Automatically assigns the new device to the same team and profile as the old device.

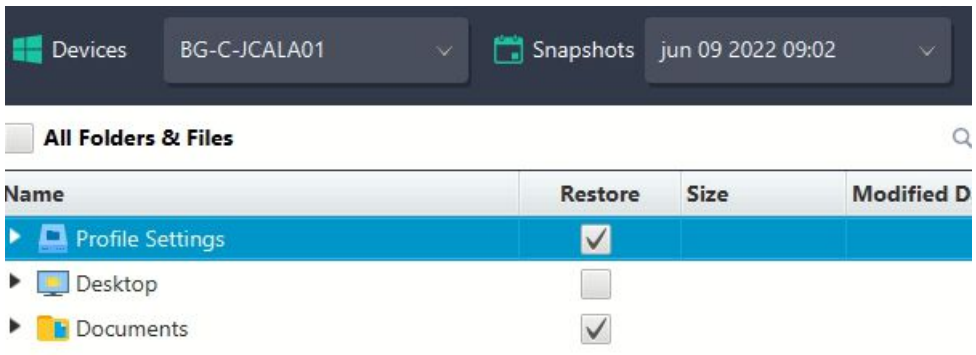
4. On the Windows taskbar, right-click the Protection Agent icon and select Restore.

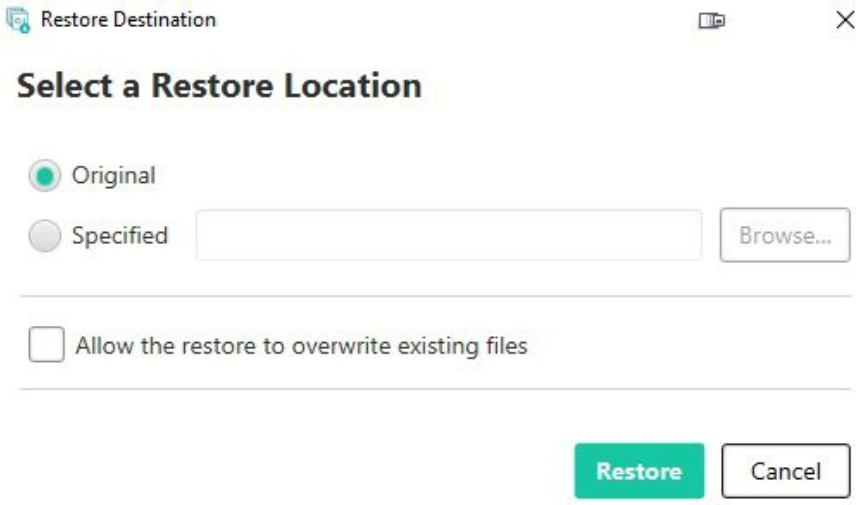


⚐ > Note: If the Protection Agent icon is not displayed, find the Agent of Protection app on your device and then launch it.

5. Choose the data you want to migrate and the location of the migrated data.

- Use the Devices option to choose the "old" device that has the data you want to migrate to the "new" device.
- Use the Snapshots option to choose the snapshot you want to migrate to the new device. A snapshot is a record of a device's data at a specific point in time. In most cases, you'll want to select the most recent snapshot.
- Use the Restore checkboxes to choose the data to migrate. Select all the data you want to restore and also the Profile Settings (Windows User Profile).
- Click Restore.
- Choose Restore Location for the migrated data on the new device. You can choose Original to migrate the data to the same location you had on your previous device, or choose Specified to set a different location.





1. Click Restore.

The selected user data and profile information are downloaded from Aranda Datasafe to your new device. If you've chosen desktop files, you'll see them appear on the desktop.