Aranda Security Compliance

It is a monitoring solution that allows companies to define compliance policies based on the security standards established by the company, detect and make visible the security risks in endpoint devices, as well as control applications, firewalls and browsers found.

The implemented policies are automatically executed on the devices where the agent is deployed, facilitating an active evaluation of the device through the validation of compliance with the established policies and the subsequent remediation of non-compliance.

The Aranda Security administrator will be able to know first-hand the status of the endpoint, about compliance with the implemented policies; assessing vulnerability and security risks at the endpoint.

Begin with

An Aranda Security user must consider three essential stages for the management and monitoring of compliance policies.

The first stage The administrator is responsible for defining the compliance policies that are required to be implemented and associating them with a group of devices.

The second stage the deployment or distribution of the Aranda Security agent in charge of establishing communication with the devices is carried out.

The third stage It is the process of monitoring devices to identify and track compliance with policies.

Who is this manual for?

This manual is designed for an administrator who can define policies, associate groups, configure users, query and track policies, and set corrective tasks.

This manual is designed for a specialist who can define policies, associate groups, consult and follow up on defined policies.

What is the value of Aranda Security?

- It is the ideal complement to the security solutions that work in the company's infrastructure, integrating regulatory requirements into compliance policies.
- Identify vulnerabilities in monitored devices, reducing security gaps and mitigating risks.
- High demand for Security-oriented Solutions

What is our documentation?

- Aranda Security Compliance ASEC Getting Started Guide
- User Manual Aranda Security Compliance ASEC

Policy Definition

ASEC Policy Definition

A policy is an entity that defines the rules and conditions associated with security components, which are applied to a program under criteria that comply with regulatory frameworks for information protection.

The definition and configuration of security policies allow the establishment of mechanisms for diagnosis, control and protection of information at different levels.

Who Sets the Policies

The Administrator and Specialist are the roles established in ASEC that will be able to define the criteria for compliance with policies.

Policy structure

A policy at Aranda Security is composed of the following criteria

- **Basic Facts**: Basic policy information such as name, status, description, and monitoring time.
- **Configuration criteria**: Each policy in Aranda Security groups the required security applications or components on a workstation, into categories according to their function. The Enabled criteria in ASEC they are: ANTIMAWARE, ANTIPISHING, BACKUP, CLOUD STORAGE, COMMUNICATIONS TOOLS, DATA LOSS

PREVENTION, ENDPOINT ENCRYPTION, FIREWALL, HEALTH AGENT, REMOTE CONTROL, VIRTUAL MACHINE, VPN CLIENT and WEB BROWSER.

|**Note**:|To understand the scope of the validations by each of the security programs that group the ASEC policy criteria, according to the operating system (Windows, Linux and Mac), know [How to View the Security Application Listing](#section-01a)

- **Validations**: These are the parameters responsible for verifying, according to the program chosen by configuration criteria, compliance with security policies in each of the workstations. Validations by configuration criteria.

- **Device Groups**: Grouping of devices linked to the ASEC agent, to be associated with the compliance policy. In the Policies section of the Aranda Security Compliance console, you will be able to Define compliance policies.

What does a policy do on a device?

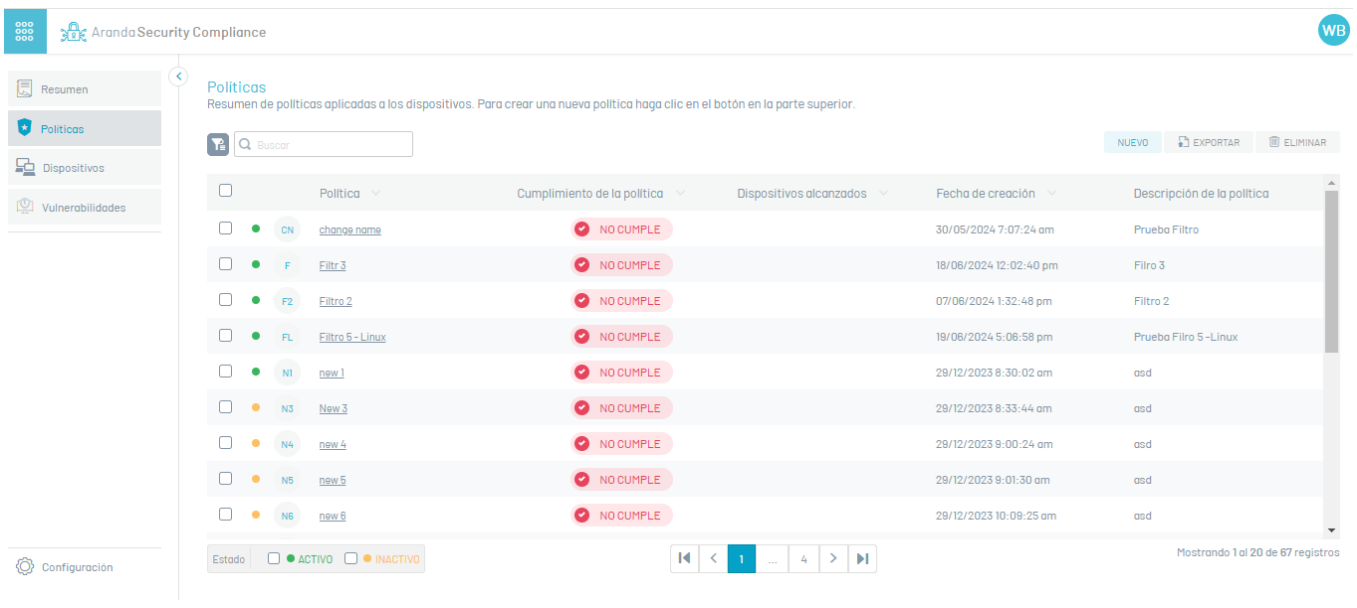
Establishes security guidelines to detect and respond to potential vulnerabilities

Manage Policies

In the process of managing and administering compliance policies in the Aranda Security application, you will be able to view, create, edit, and delete security policies.

View Policies

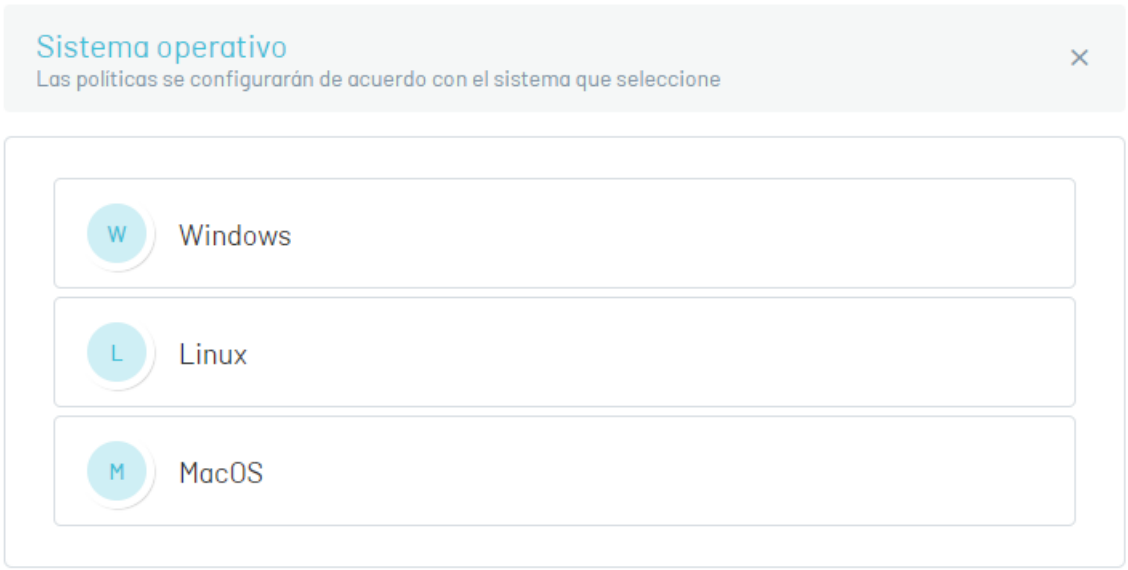
1. Enter the Aranda Security Compliance console with administrator role, select the option **Policies** from the main menu. In the information view, you can view the list of available policies and sort the information grouped by name, devices reached (associated with the policy) and date of creation.

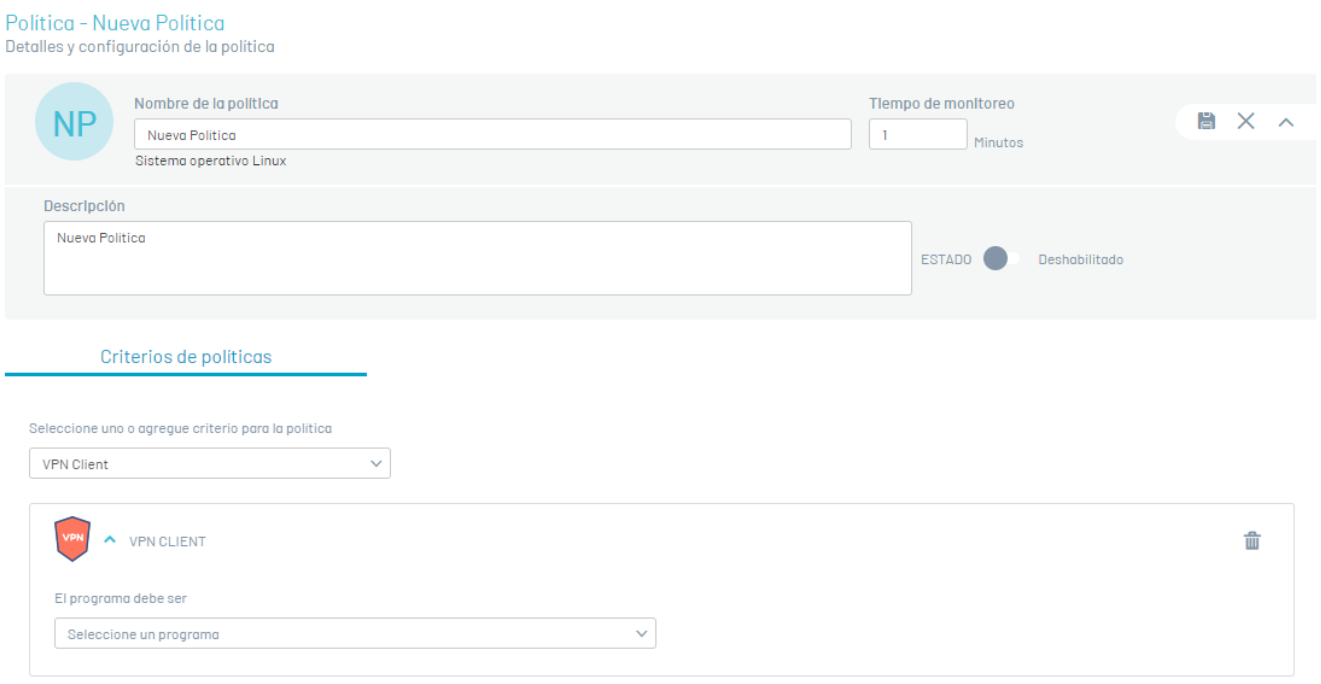


2. In the information view of the policies, you will have information management and organization actions available Information View in ASEC Web Environment

Policy Creation

1. To create a policy, log in to the Aranda Security console with the administrator or specialist role, in the **Policies** from the main menu. In the information view, select the **New**; window is enabled **Operating system**, select an Operating System to proceed to the form where you need to enter the basic policy information:



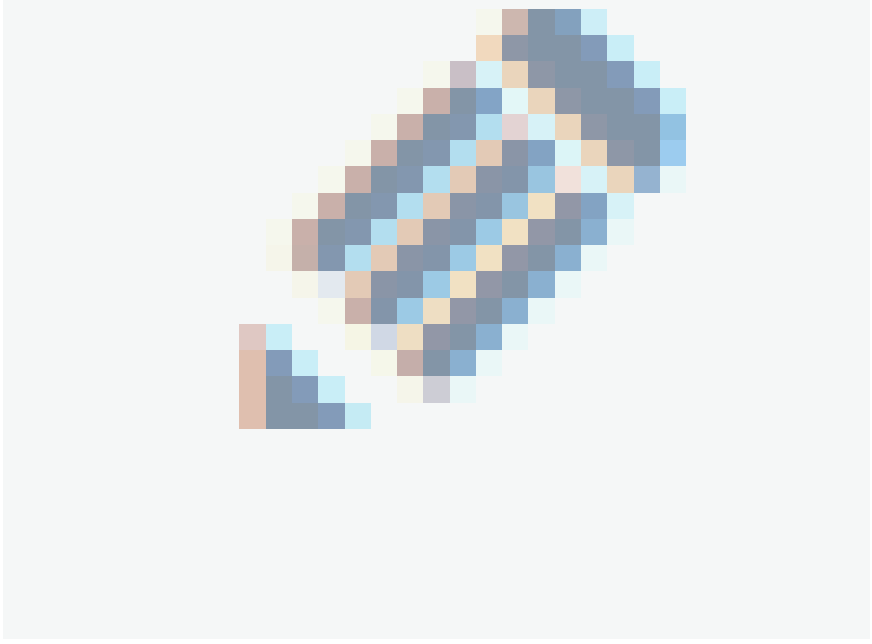


Field	Description
Policy Name	Name that identifies the policy.
Description	Policy description.
State	Policy status indicates whether you will start Active immediately, or start Inactive.
Monitoring Time	Time interval where agents will be reporting compliance with the policy.

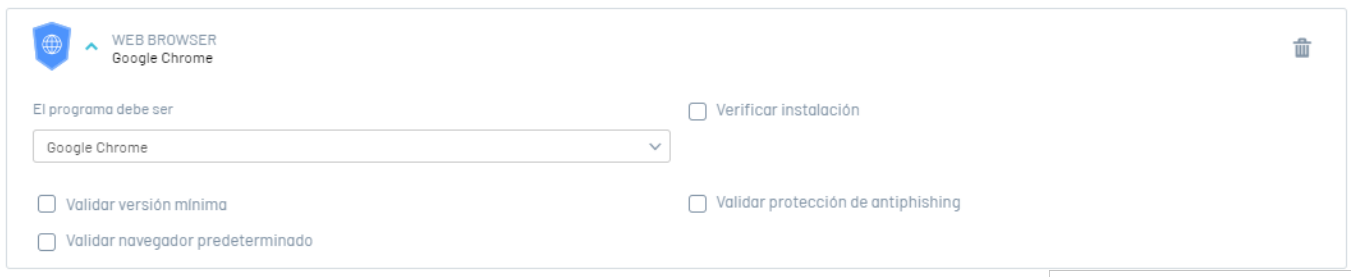
Policy Criteria

2. In the information view for the new policy, select the**Policy criteria** and choose a configuration software criterion from the list. The**Enabled criteria** in ASEC they are: ANTIMAWARE, ANTIPISHING, BACKUP, CLOUD STORAGE, COMMUNICATIONS TOOLS, DATA LOSS PREVENTION, ENDPOINT ENCRYPTION, FIREWALL, HEALTH AGENT, REMOTE CONTROL, VIRTUAL MACHINE, VPN CLIENT and WEB BROWSER.

3. When selecting the software criterion (Antimalware, browser, firewall), click the**Edit**

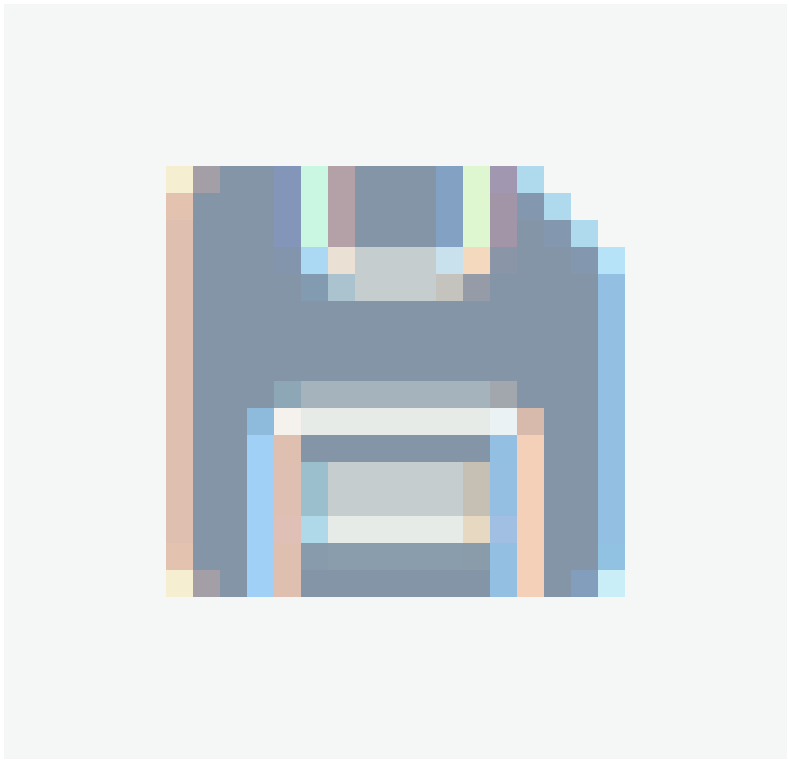


and choose a program from the existing listing.



⚐ **Note:** Selecting a program from the policy criteria triggers the methods or validations corresponding to the defined program. For each program, different validation options will be activated. View validations by configuration criteria

4. Select the enabled validation items to determine the compliance levels for that instance of the security policy, and click the **Save**



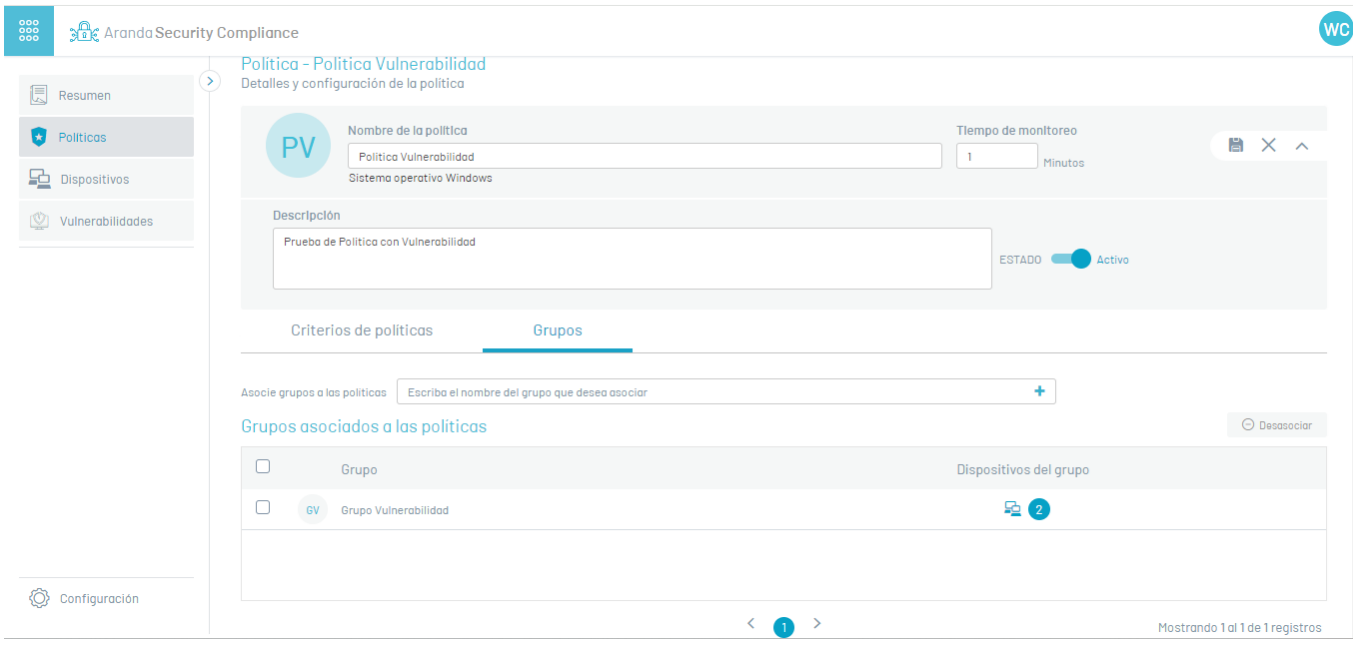
, to confirm the changes made. These criteria are what are evaluated and determine whether a policy is complied with or not.

⚐ **Note:** To remove the details of the software criterion, at any time, click the respective icon to clear the settings.

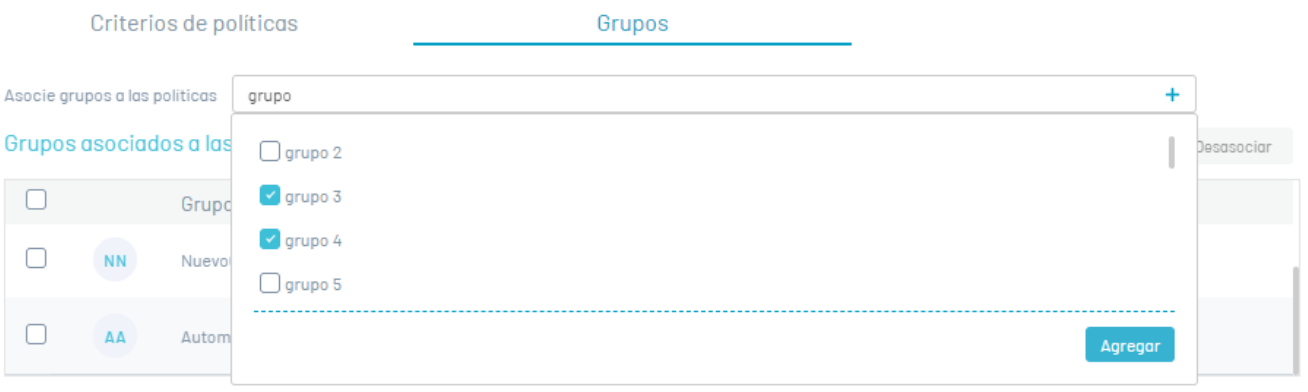
5. After a policy is created, the tab is enabled to associate device groups with the defined policy.

Associate Groups

6. When you finish configuring the basic information of the policy, enter the Aranda Security console again and select the policy created; In the information view, the **Groups** where you can associate device groups to the defined policy.



7. In the field **Associate Groups** Enter a name to search for a group, or type in a name to create a new group. Click the **(+)** to create a new group. Each policy may contain many groups. 8. To associate a created group with the policy, select a group from the available list and click the **Add**

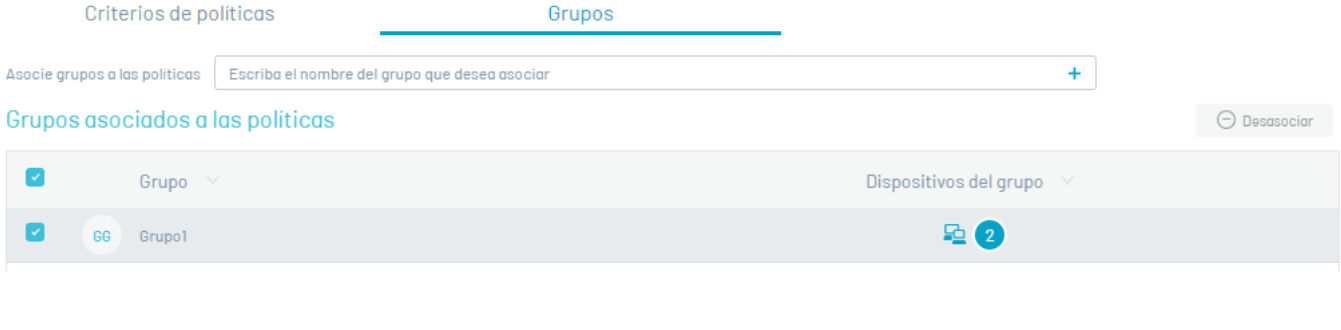


9. In the list of associated groups, select the name of the group with linked devices, to access the Device Compliance Detail.

Disassociate Groups

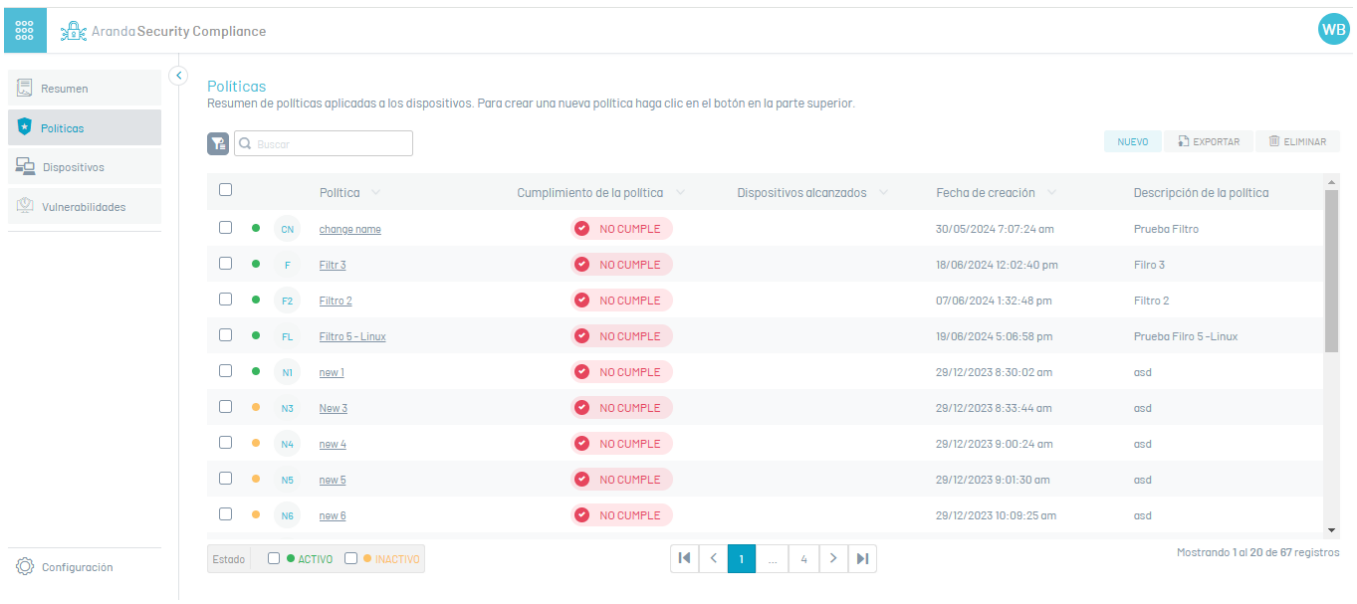
10. To delete one or more groups, in the policy information view, on the **Groups**, select a record from the created groups, and click the **Disassociate** to clear the associated information.

11. When defining the groups for the policy, click the **Save**, to confirm the changes made.



Delete Policies

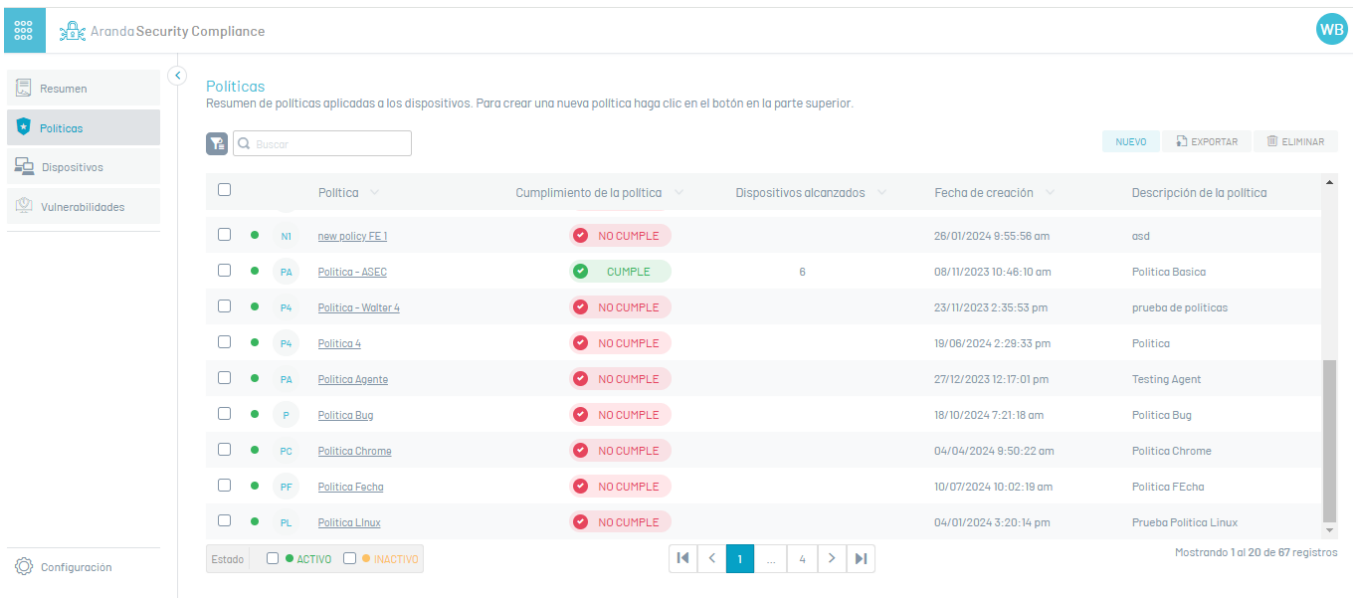
12. To delete policies, log in to the Aranda Security console with administrator role, in the section **Policies** from the main menu. In the information view, you will be able to view the list of available policies; Select one or more records and click the **Delete Policies**.



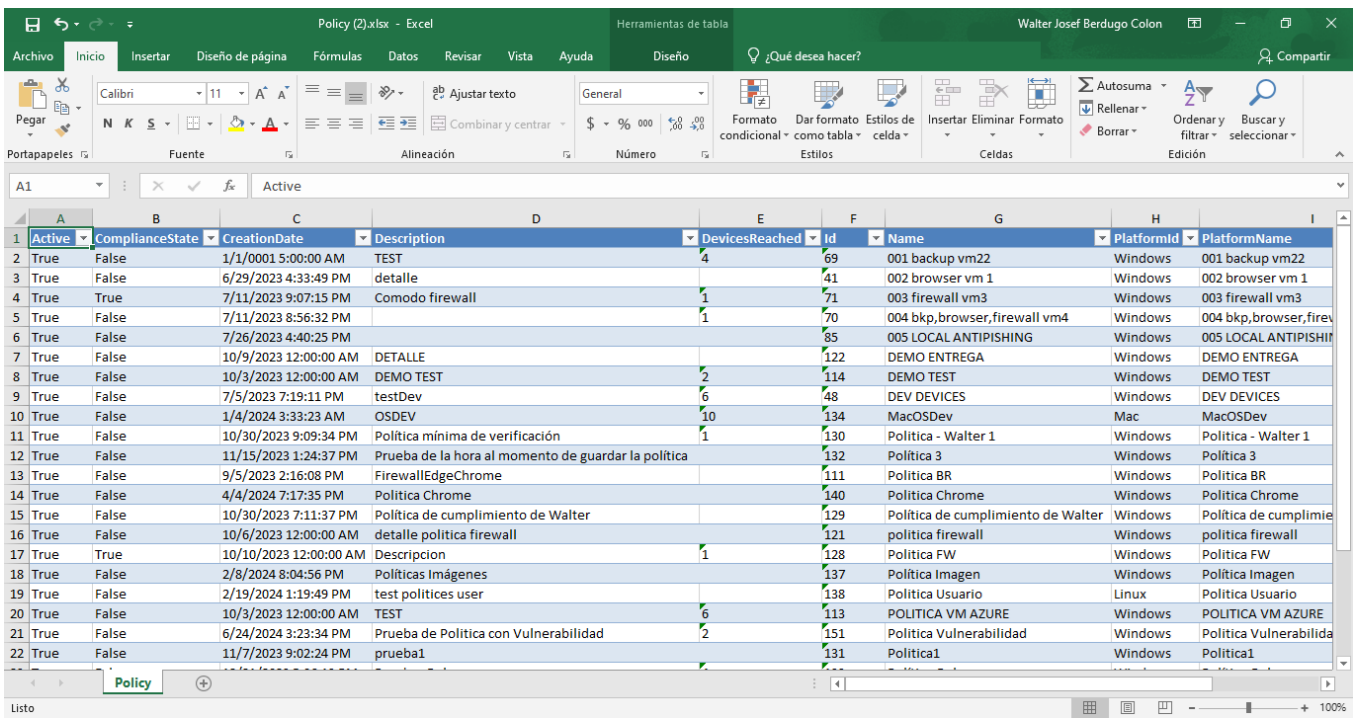
13. A warning message is enabled where you must confirm the deletion of the policy.

Export Policies

1. To export the policy information, log in to the Aranda Security console with administrator role, in the **Policies** from the main menu. In the information view, the list of available policies can be viewed; Filter one or more records in the field **To find** and click the **Export**.



2. In the Aranda Security Management Console header menu, the option to **Downloads** where you can view the generated format of the list of policies in Excel format
3. Click the file to download the policy information. The downloaded file includes all the fields in the policy.

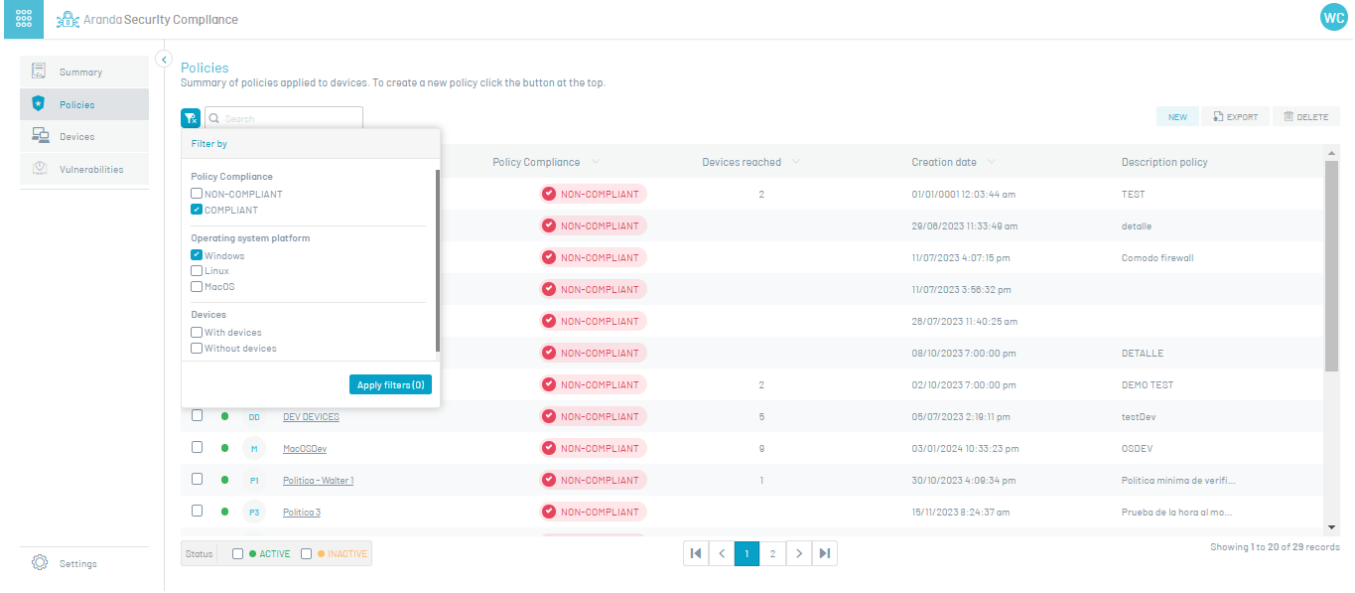


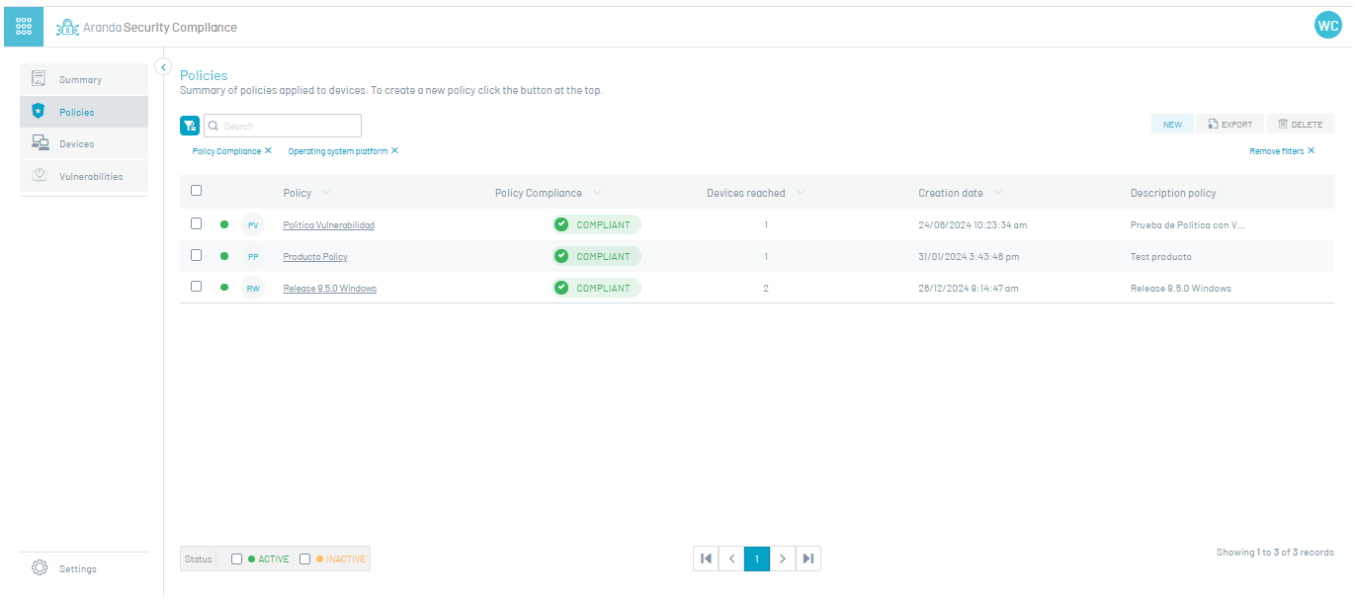
Filter Policies

1. In the Policy information view, select the Policy Filter (icon) and enable query criteria such as Policy Compliance, Operating System Platform, and Devices. When finished, click on the **Apply Filters**.

2. Additionally, you can combine the query, using the filter by policy status to have a more detailed and personalized view.

⚐ **Note:** Applying the policy filters and filter by states allows you to identify devices or systems that require tracking, corrective actions, or priority attention.





Validations by Criteria

The policies configured in Aranda Security evaluate the compliance levels of security applications on different workstations. This diagnosis is possible due to the validations that are applied for the different policy criteria programs

For each security program, different validation options will be activated. Each validation may be used in the Policy criteria Available.

The validation options available in Aranda Security are:

⚐ **Note:** To understand the scope of the validations by each of the security programs that group the ASEC policy criteria, according to the operating system (Windows, Linux and Mac), know How to View the List of Security Applications.

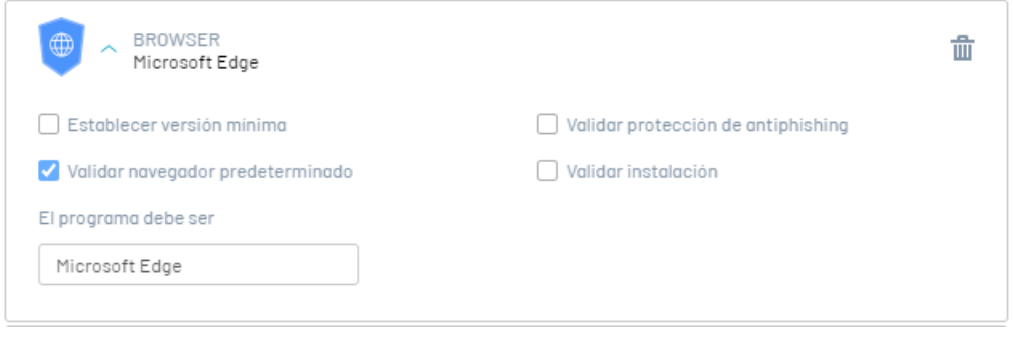
Here are some scenarios for configuring policy criteria and validations:

1. Validate default browser

This option validates that the selected browser is set as the default browser on the workstation. The validation response options are:

Return	Description
MEETS	If the browser is set as default on the workstation.
NOT COMPLIANT	If the browser is not set as default or if it is not installed

Example	It is validated on the workstation if the**Microsoft Edge** is set as default.

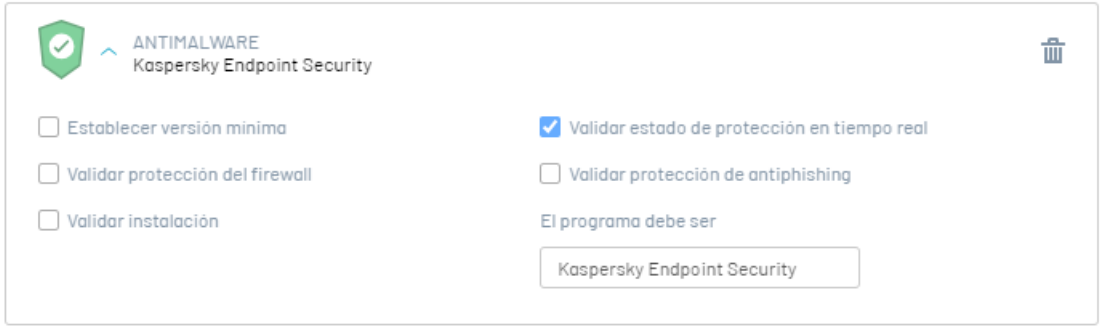


2. Validate Protection Status in Real-Time

This option validates that the software has real-time protection enabled. The validation response options are:

Return	Description
MEETS	Whether the software has real-time protection enabled.
NOT COMPLIANT	If the software does NOT have real-time protection enabled or if it is not installed.

Example	It is validated that the software**Kaspersky Endpoint Security** have real-time protection enabled.

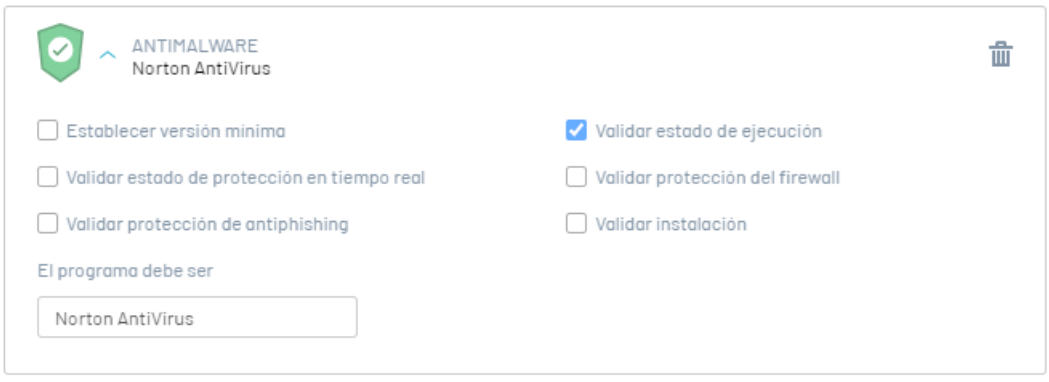


3. Validate Execution Status

This option validates whether the software is running on the workstation. The validation response options are:

Return	Description
MEETS	If the software is running.
NOT COMPLIANT	if the software is NOT running or if it is not installed.

Example	It is validated if the**Software Norton Antivirus** is running.

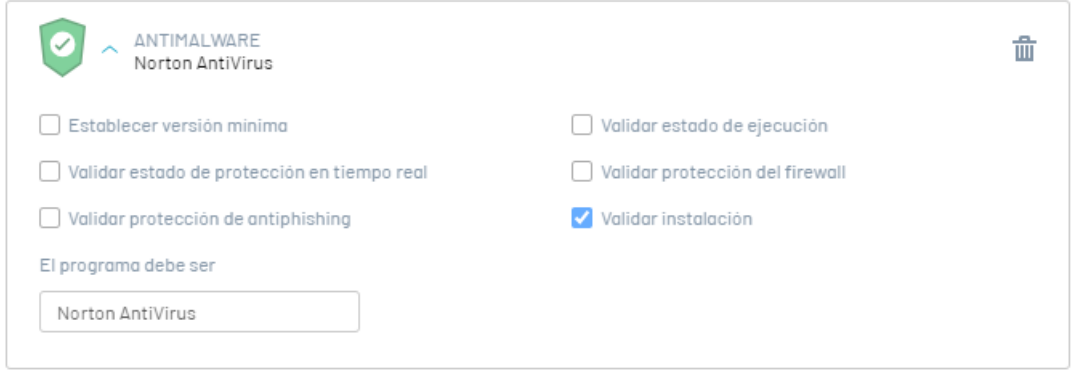


4. Validate Installation

This option is valid if the software is installed on the workstation. The validation response options are:

Return	Description
MEETS	If the software is installed.
NOT COMPLIANT	if the software is NOT installed.

Example	It is validated if the**Software Norton Antivirus** It is installed on the workstation.



5. Validate Firewall Protection

This option is valid if the software has FIREWALL protection enabled. The validation response options are:

Return	Description
MEETS	If the software has FIREWALL protection enabled.
NOT COMPLIANT	If the software does NOT have FIREWALL protection enabled or if it is NOT installed.

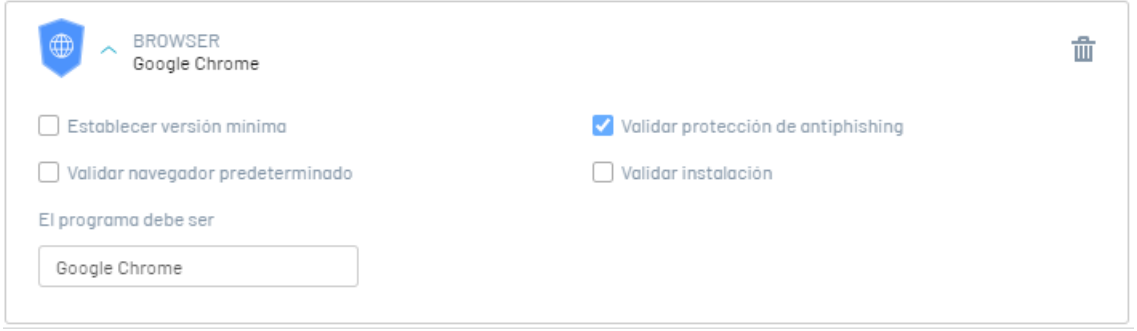
Example	Validate that the software**Windows Firewall** have FIREWALL protection enabled.

6. Validate Anti-Phishing Protection

This option is valid if the software has Anti-Phishing protection enabled. The validation response options are:

Return	Description
MEETS	If the software has Anti-Phishing protection enabled.
NOT COMPLIANT	If the software does NOT have Anti-Pishing protection enabled or if the software is NOT installed.

Example	Validate that the software**Google Chrome** have Anti-Phishing protection active.



7. Set Minimum Version

This option sets a minimum version to later validate against the version installed on the workstation. The validation response options are:

Return	Description
MEETS	This criterion is met when a full version is specified or when the version is greater than a partial version
NOT COMPLIANT	The criterion is not met when the installed software has a different or lesser version, depending on the case.

Example	Validate that the version of**AVG internet security** installed on the workstation is greater than or equal to version 1.0.1

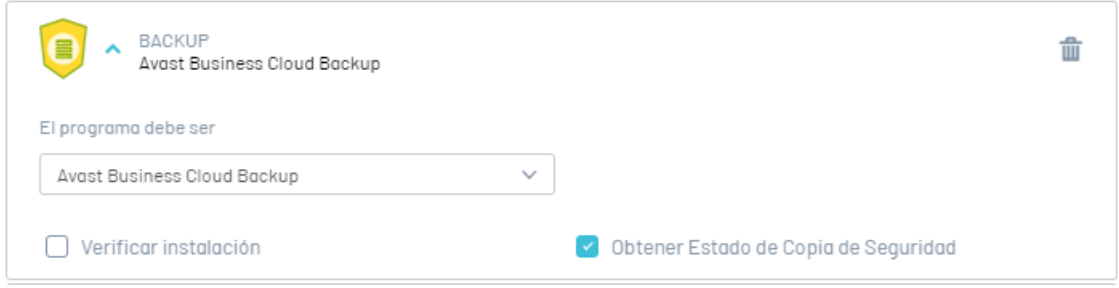
|**Example**|Validate that the version of**Sea Monkey** installed on the workstation is greater than or equal to version 1.0.1

8. Validate Backup Status

This option validates the status of the software backup. The validation response options are:

Return	Description
MEETS	If the software has the option to get the backup status enabled.
NOT COMPLIANT	If the software does NOT have the option to get the backup status enabled.

Example	Validates that the backup status of the software can be obtained**Avast Business Cloud Backup** .

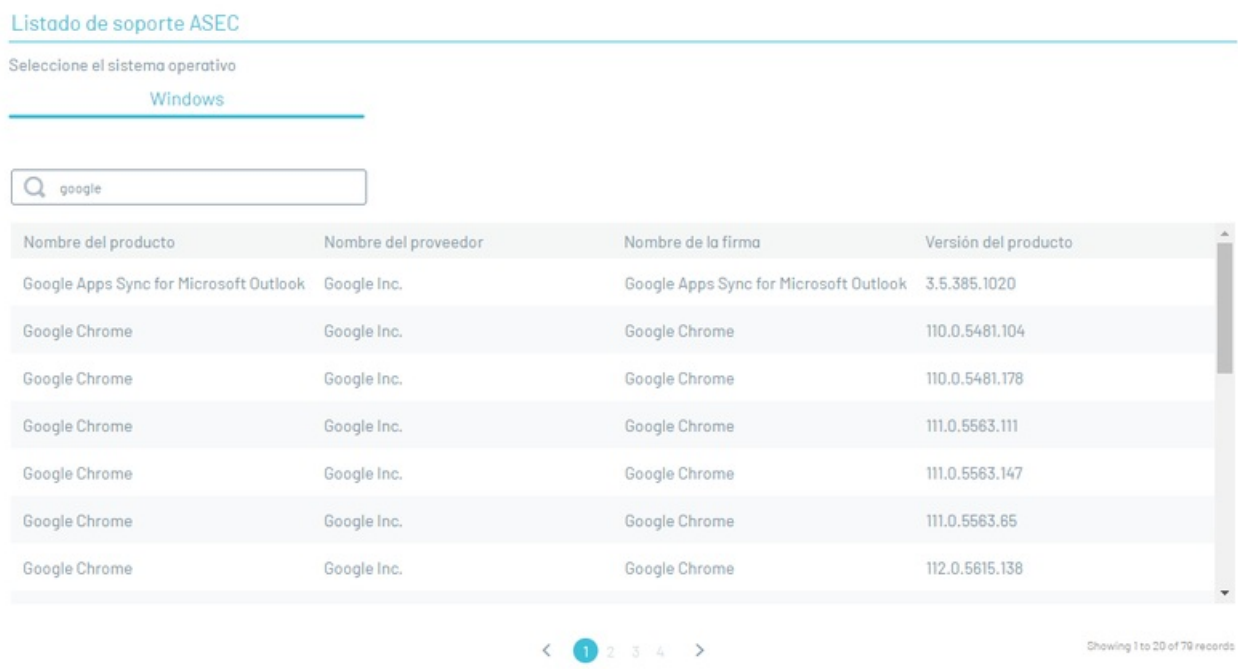


View Security Application Listing

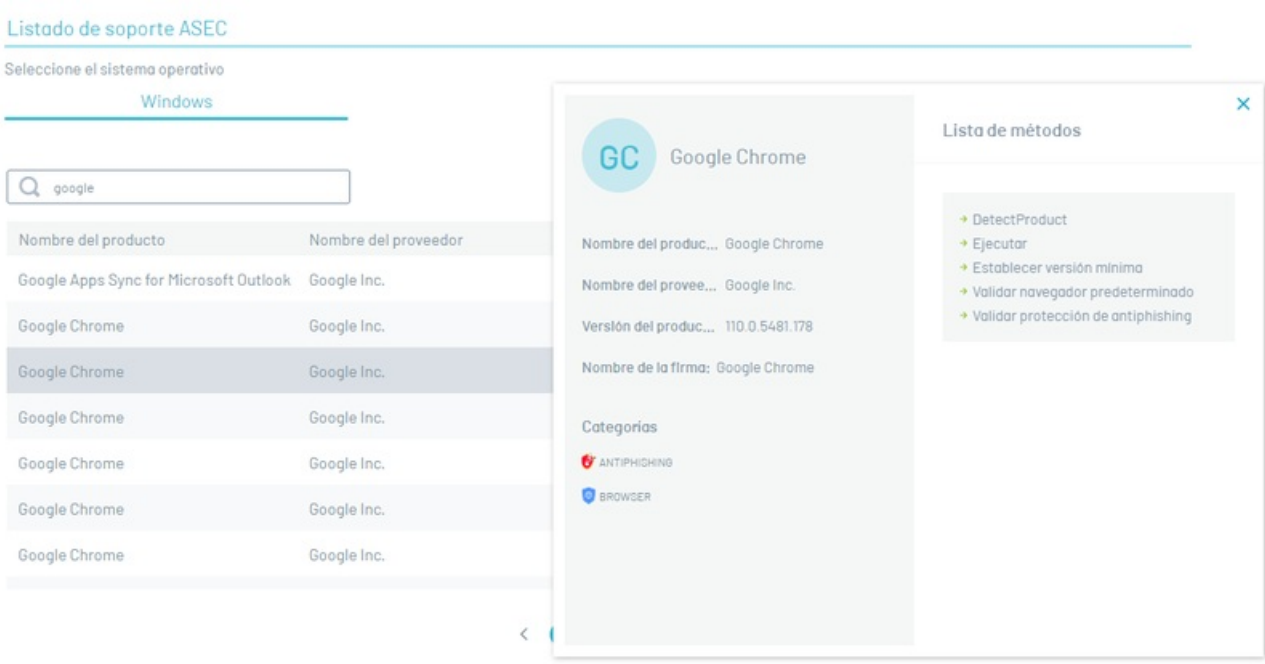
1. Enter the ASEC support list: https://docs.arandasoft.com/asec/supportchart

2. In the information view, you will be able to view the list of security applications and supported versions to manage ASEC compliance policies.

3. In the search engine you can consult the security applications and supported versions, entering the name of the program.



4. By selecting a record from the list of security applications, you will be able to view related information such as product name, vendor name, configuration criteria to which it belongs (ANTIMAWARE, ANTIPISHING, BACKUP, CLOUD STORAGE, COMMUNICATIONS TOOLS, DATA LOSS PREVENTION, ENDPOINT ENCRYPTION, FIREWALL, HEALTH AGENT, REMOTE CONTROL, VIRTUAL MACHINE, VPN CLIENT and WEB BROWSER.) and the Validations or methods that it endures.



Policy Criteria

The Policy Criteria are organized into categories that determine the classification of programs according to their functionalities. Each program has different validation options and may belong to different Criteria.

Criterion	Description
ANTIMALWARE	Antimalware programs are applications designed to detect, prevent, and remove malicious software from computer devices. They help protect against viruses, trojans, spyware, and other online threats, being a critical part of digital security. Examples include Windows Defender and Kaspersky Anti-Virus.
	Anti-phishing programs are tools that protect users against phishing attacks, which attempt to trick them into revealing sensitive information. These programs detect and block fake emails, messages, or websites that attempt to steal personal or financial data. They help maintain

Criterion	Description
	online security and privacy. Examples include McAfee WebAdvisor and K7SecureWeb.
BACKUP	Backup applications help organizations maintain the immortality of their data, which in turn improves business continuity and strengthens disaster recovery capabilities. Examples include IDrive and MEGAsync.
CLOUD STORAGE	Cloud Storage programs are tools that allow you to store, manage, and access data remotely over the Internet. They facilitate file synchronization between devices, file sharing, and data security, being used by both individual users and businesses for online storage and collaboration. Examples include Dropbox, Google Drive, and Microsoft OneDrive.
COMUNICATION TOOLS	Communication Tools programs are digital tools that facilitate communication between individuals and teams through various means, such as instant messaging, video conferencing, and project management. Examples include Slack and Zoom enabling effective collaboration and remote teamwork.
DATA LOSSPREVENTION	Data Loss Prevention (DLP) programs are tools that prevent the loss or leakage of an organization's sensitive data. They monitor, detect, and control the flow of information in and out of the enterprise network to protect sensitive data, such as financial or personal information, trade secrets, and intellectual property. Examples include Wave Data Protection Agent and Dr.Web Security Space.
ENDPOINT ENCRIPTION	Endpoint Encryption programs are tools that encrypt data stored on end devices such as laptops and mobile phones. They help protect sensitive information in the event of loss or theft of the device, keeping it inaccessible without the proper decryption key. Examples include CipherShed and CryptoExpert.
FIREWALL	Firewall programs are applications or devices designed to protect computer networks by controlling and filtering the data traffic in and out of them. They function as a security barrier, examining each data packet and deciding whether to allow it to pass through or block it according to predefined rules. They are critical to preventing unauthorized intrusions, protecting sensitive data, and maintaining the integrity of computer systems. Examples include Smart Heal Total Security and SpyShelter Firewall.
HEALTH AGENT	Health Agent programs are part of endpoint security suites that are centrally managed. These agents enforce policies and perform client-side tasks, such as deploying, configuring, and updating other components of the security suite. These additional components can range from the personal firewall and anti-malware engine, to anti-phishing protection, data loss prevention agent, disk encryption agent, and network access control agent, among other forms of endpoint protection offered by various security vendors in their products. Examples include HP Support Assistant and Windows Security Health Agent.
REMOTE CONTROL	Remote Control programs are tools that allow users to control and access devices remotely over a network connection, such as the internet. They are used to display the screen, interact and troubleshoot on devices located in different geographical locations. They are useful for technical support, systems administration, telecommuting, and team collaboration. Examples include TeamViewer, AnyDesk, and Microsoft Remote Desktop.
VIRTUAL MACHINE	Software that enables virtualization in computer systems. They create and manage virtual machines, isolated environments that run operating systems and applications independently. Examples include VirtualBox and VMware Workstation.
VPN CLIENT	VPN Client programs are applications that allow users to establish secure connections to a virtual private network (VPN) from their devices. These encrypted connections ensure the privacy and security of communication, especially on public Wi-Fi networks. Examples include Cisco AnyConnect, and ExpressVPN.

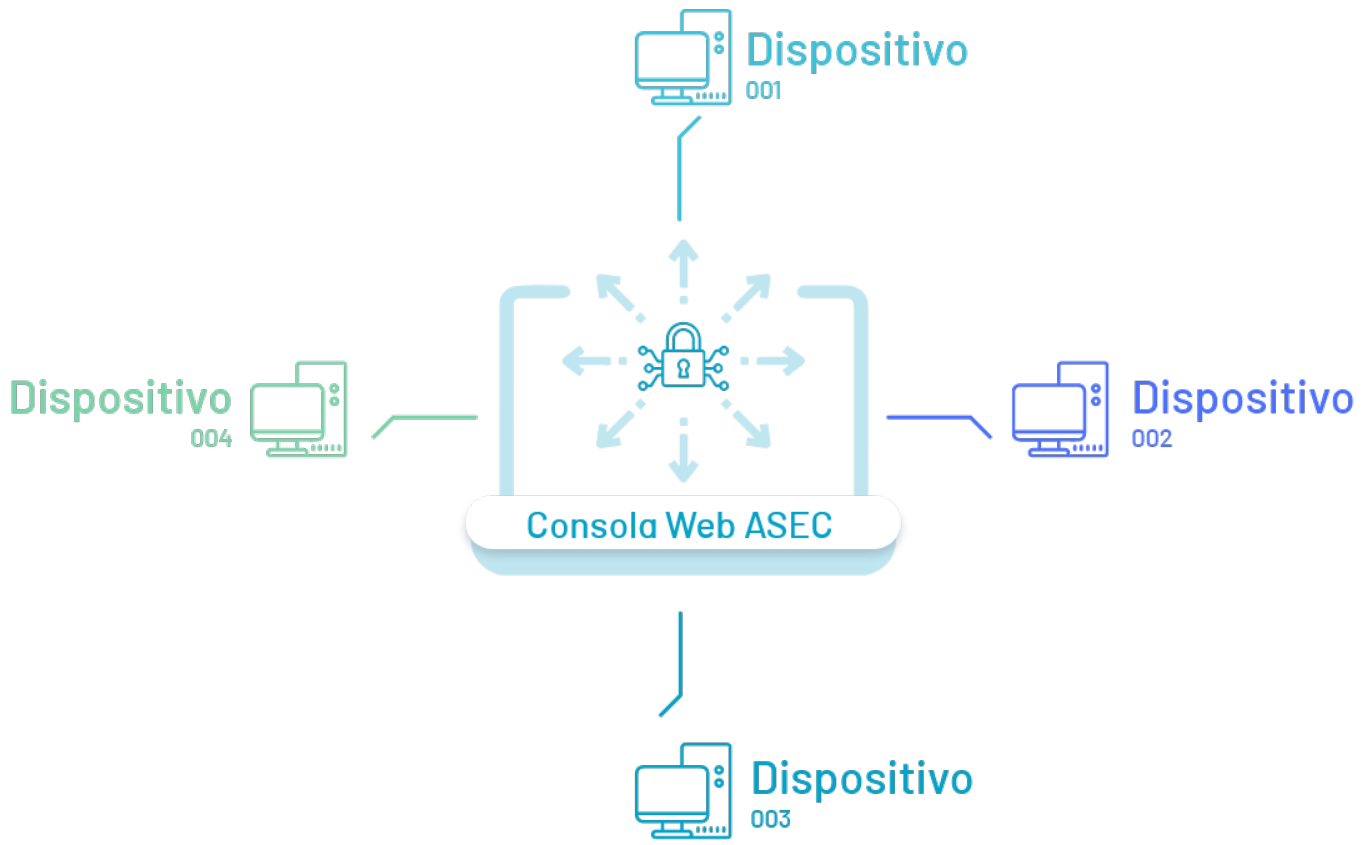
Criterion	Description
WEB BROWSER	Web Browser programs, or web browsers, are applications that allow users to access and browse web pages on the Internet. They offer features such as opening multiple tabs, managing bookmarks, and searching the web. Popular examples include Google Chrome, Mozilla Firefox, Microsoft Edge, Safari, and Opera. They are critical to the internet browsing experience.

Deployment and Installation

Aranda Security Agent

The agent in ASEC is the component in charge of validating that the security policies implemented on the devices meet the proposed objective.

After being installed on the devices, the ASEC agent reads compliance with the defined policies and generates alerts that can be viewed by the administrator through the web console.



In the Aranda Security web console, the general administrator will be in charge of performing the following task:

Agent Deployment

Agent deployment is the process of distributing this component to the devices that need to be monitored. From the ASEC web console, the generated command will be copied for subsequent installation in each disopsitive.

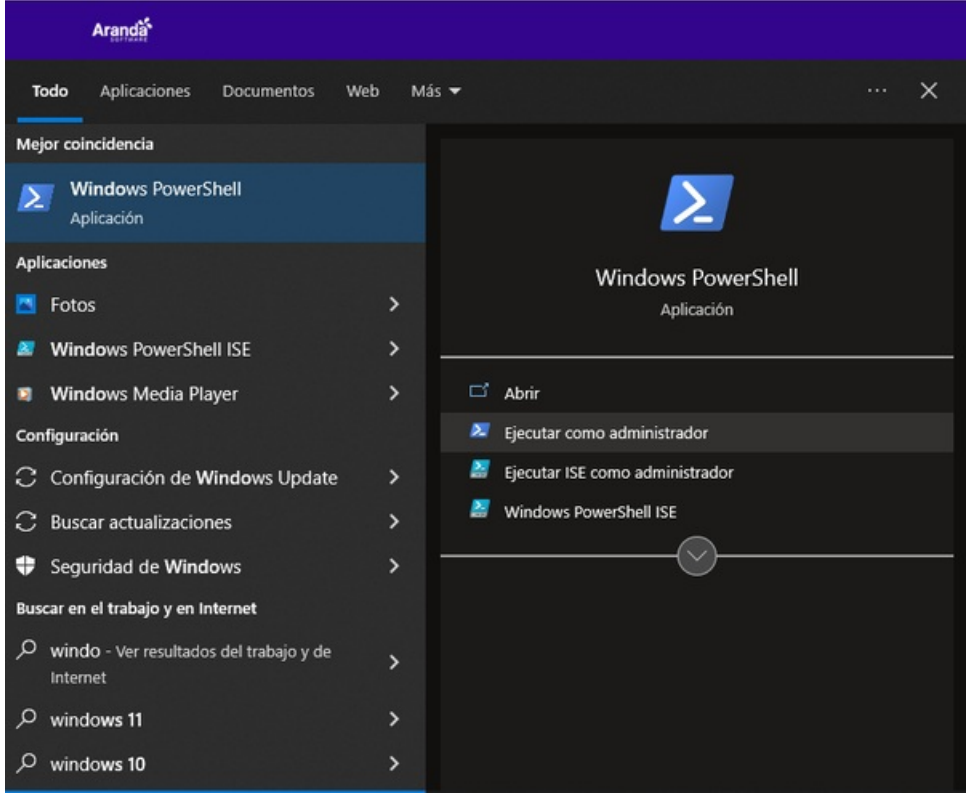
The deployment of the agent in ASEC can be carried out in three ways:

- **Deployment by devices**: Through the Aranda Security web console you can deploy and subsequently install the ASEC agent on the devices.
- **Deployment by Domain Policy**: The installation of the agent can be done through the domain policy.
- **Deploy with ADM**: Using Aranda Device Management ADM you will be able to upload the ASEC agent package and start the process of distributing the ASEC agent to the devices.

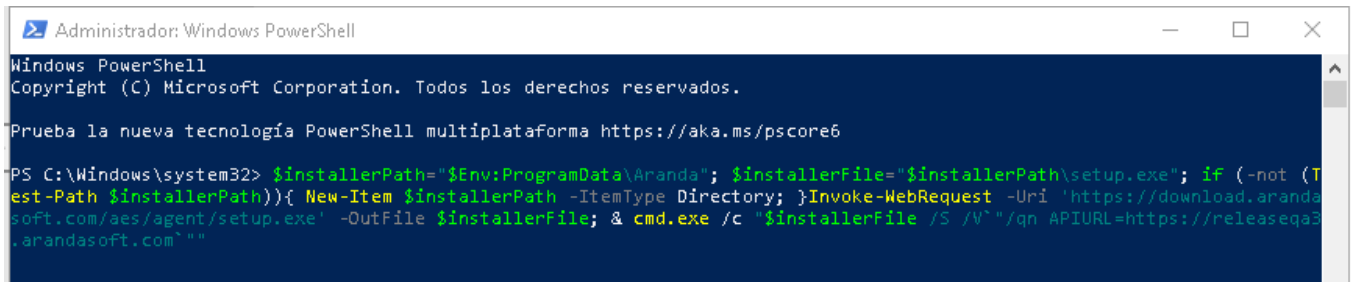
Deploy and Install Agent by Devices

Agent installation requires administrator permissions on the device.

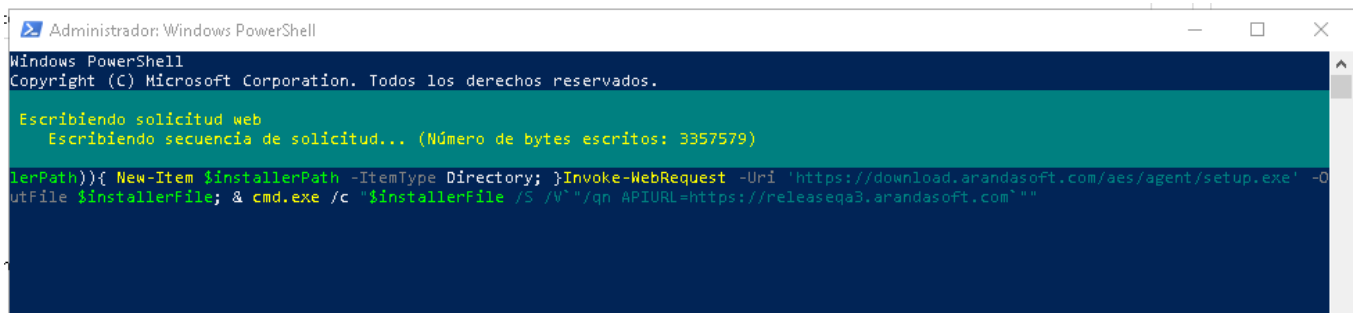
1. Open Windows PowerShell and run the program as an administrator.



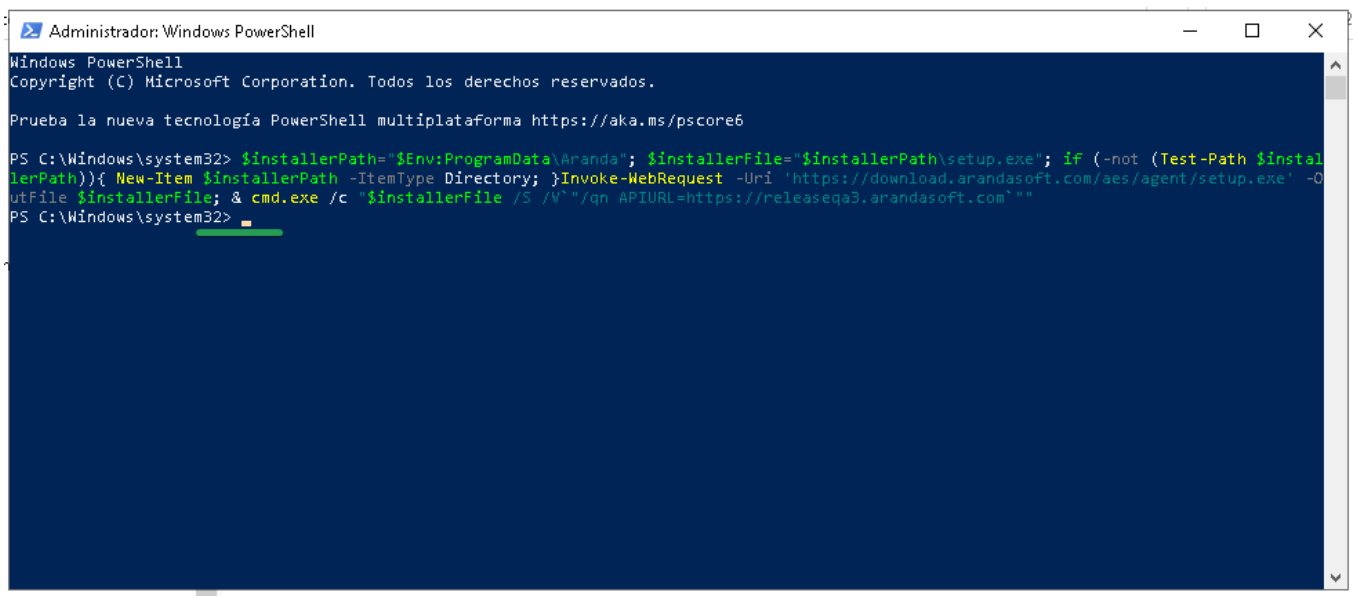
2. The command copied from the screen[Deploy Agent](#) in the ASEC web console, paste it into the PowerShell and**Enter**. The installation of the agent on the device will begin.



3. Starts a byte counter that represents the download and installation of the agent on the device



4. Once the installation process is complete, the cursor over the PowerShell console will be presented again and from that moment the agent will start the verification of the policies.

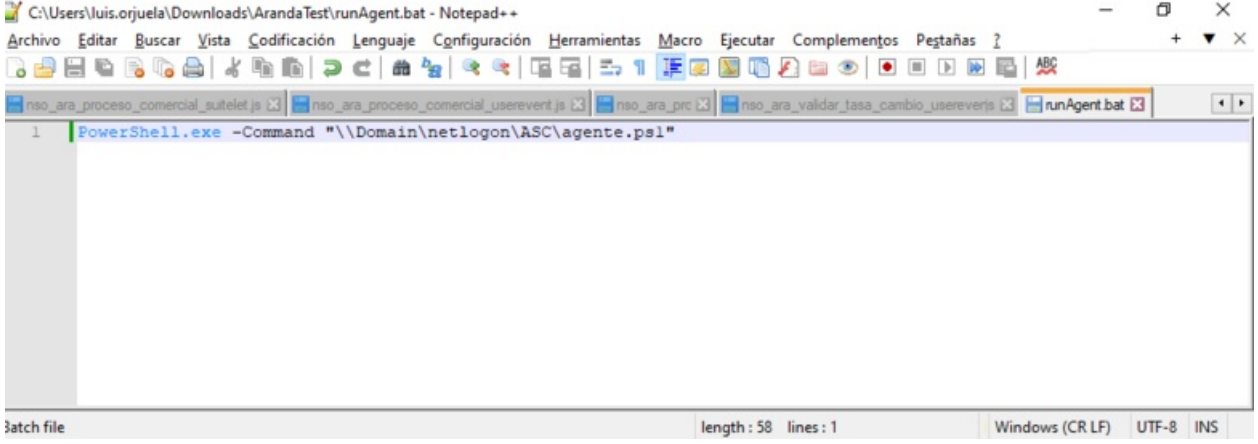


ASEC Agent Deployment by Domain Policy

Create Execution Files

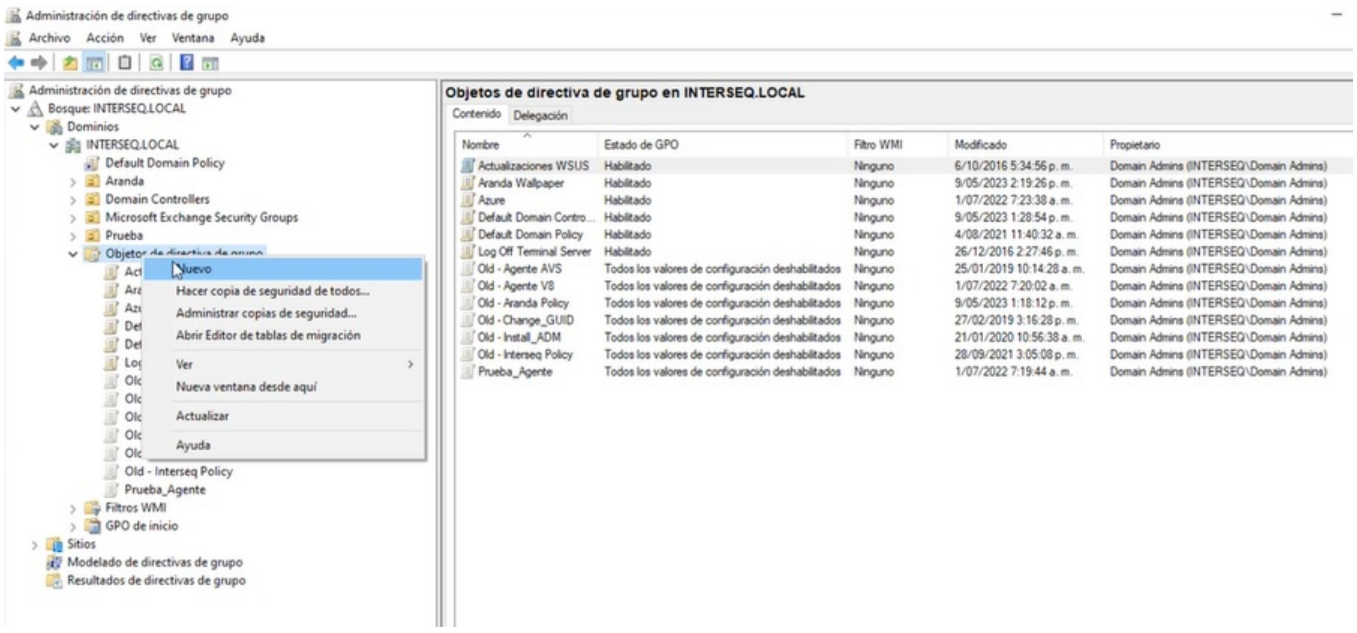
1. After copying the ASEC agent execution command, during the [Agent Deployment](#) in the ASEC web console, generate a file with**PS1 extension** including the copied command, to later execute it in the required domain.

2. Define a .bat file with the path of the required domain.

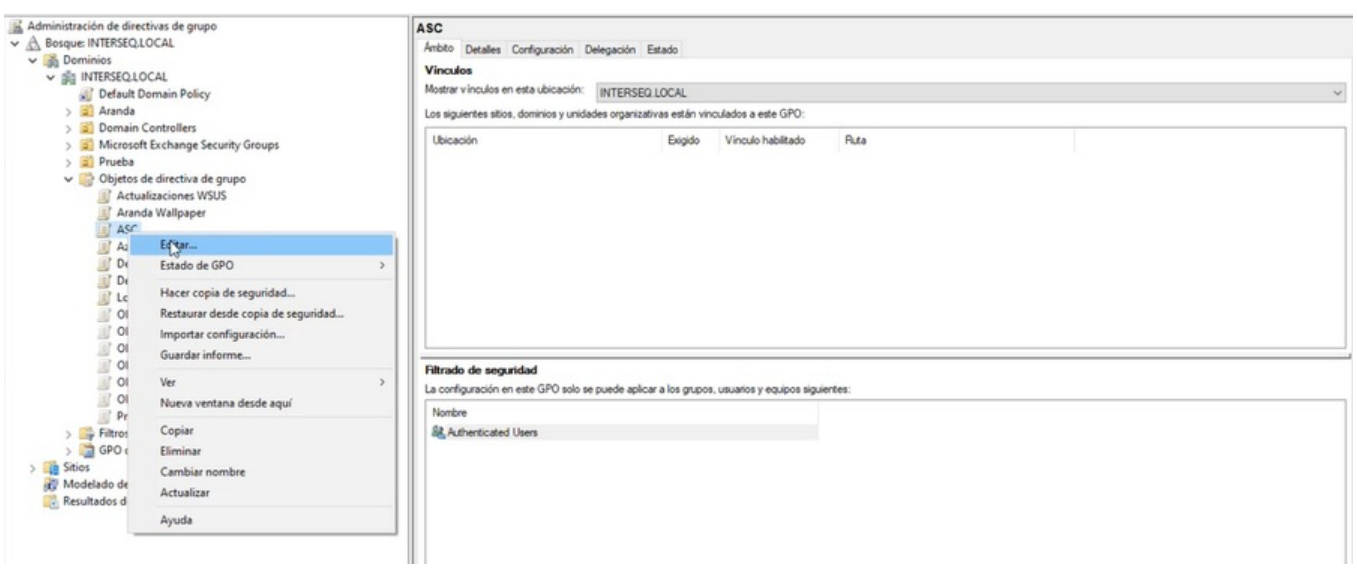


Create Group Policies

1. Enter the option of **Group Policy Management**, in the local domain, select the **Group Policy Objects** and click on the **New**.

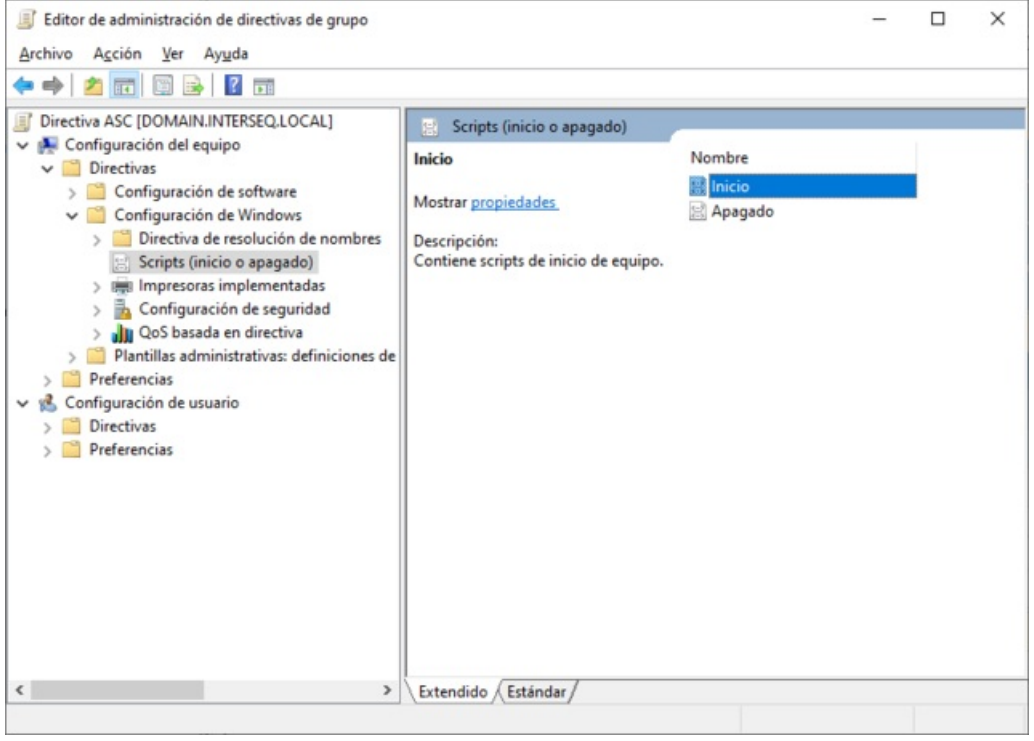


2. In the window **New GPO** Enter a name of the new policy. Example: ASC.3. Select the newly created policy and click the option **Edit**.

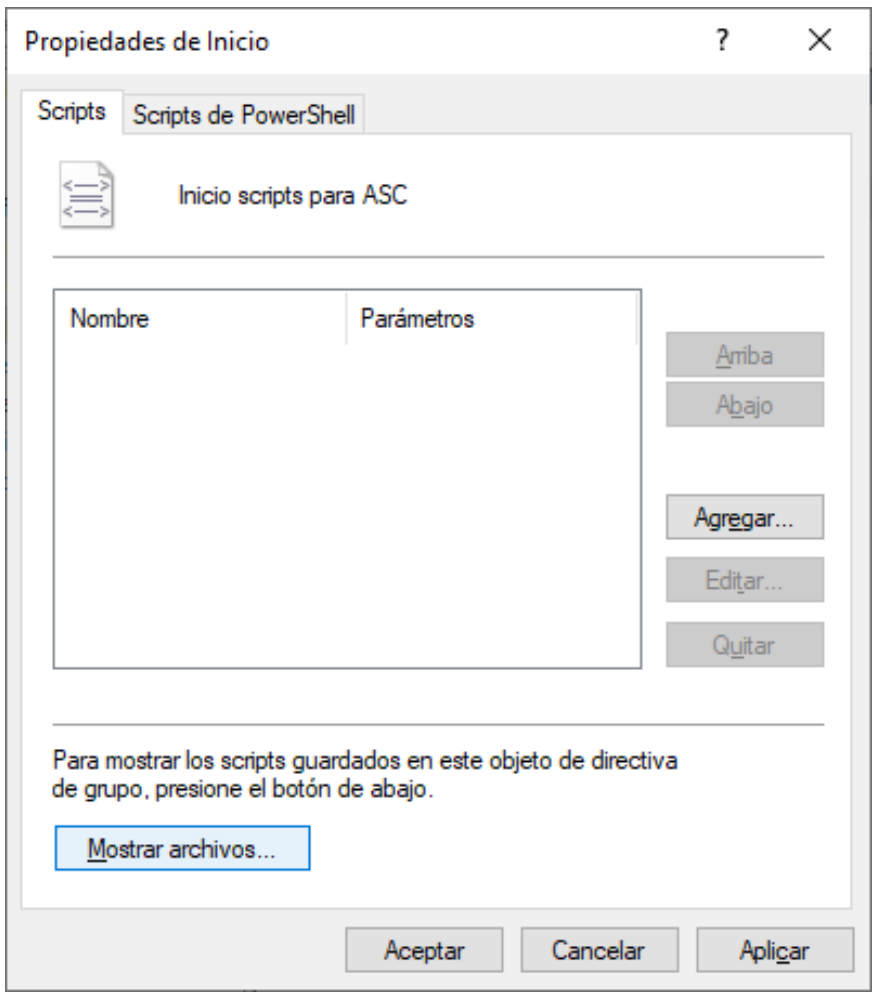


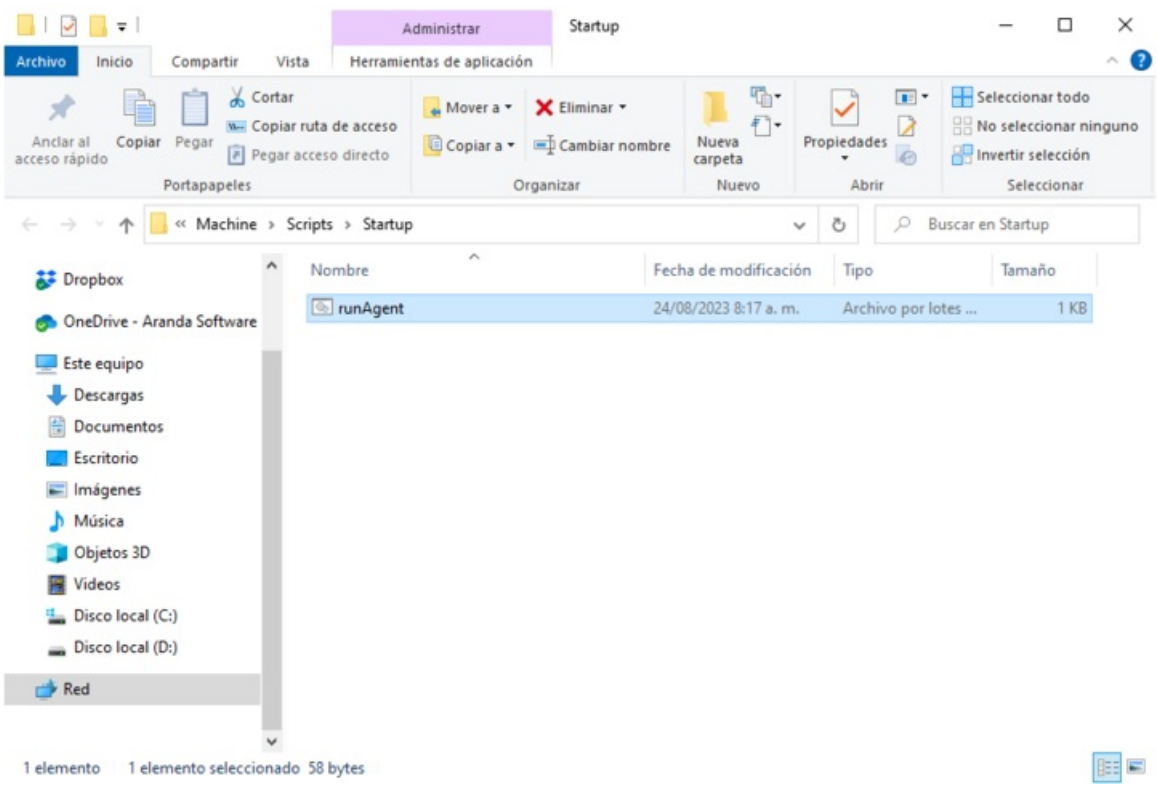
4. In the **Group Policy Management Editor**, select the Computer Configuration, Policies, Windows Settings option, and select the **Scripts**. In the information view, select the **Beginning** .

> ⚐ **Note:** Configure the startup policy allows the ASEC agent to run at logon time.

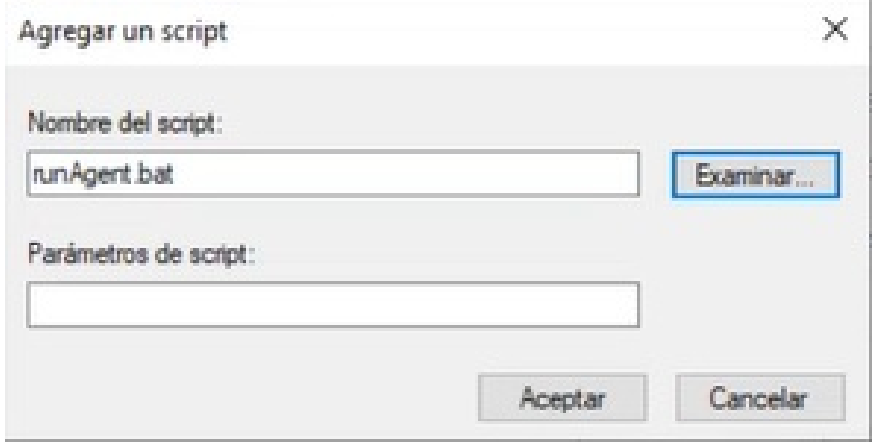


5. In the window **Startup properties**, select the **Show Files** to paste the file **.bat** of the ASEC agent.



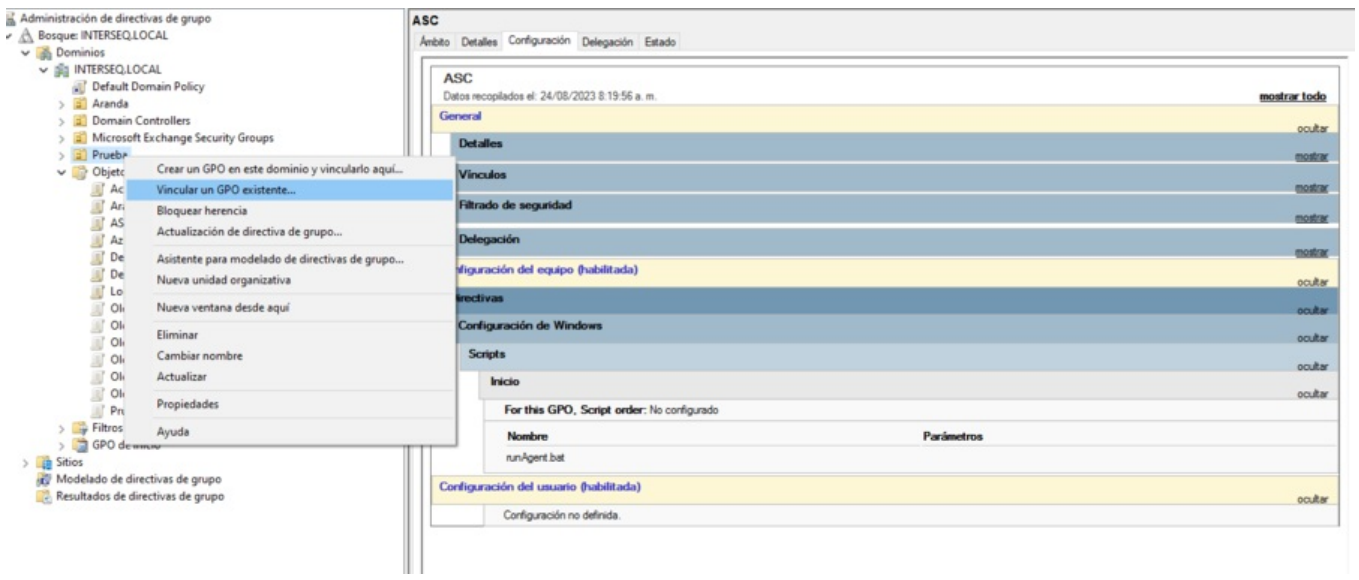


6. In the window **Startup properties**, select the **Add** and in the window **Add a Script** Select the **Examine** to select the **.bat file** on the ASEC agent, when finished click **Accept**.



Associating the Policy with the Organizational Unit

1. Enter the option of **Group Policy Management**, in the local domain, select the organizational unit to which you are linking the created GPO, and click the **Link an existing GPO**.



2. In the window that is enabled, select the policy of the created policy.

> ⚐ **Note:** In the information view, select the **configuration** to validate that the policy configured with the ASEC agent is enabled.

Policy Monitoring

Policy Compliance Monitoring

Monitoring is the process of monitoring and validating the levels of compliance with the policies implemented.

The administrator and specialist will be able to consult and verify the results generated after the analysis carried out by the agent on each of the devices, taking into account the following statements:

1. Policy Brief

Refer to the analysis generated by Aranda Security to determine the levels of compliance with security policies on different devices.

2. Devices

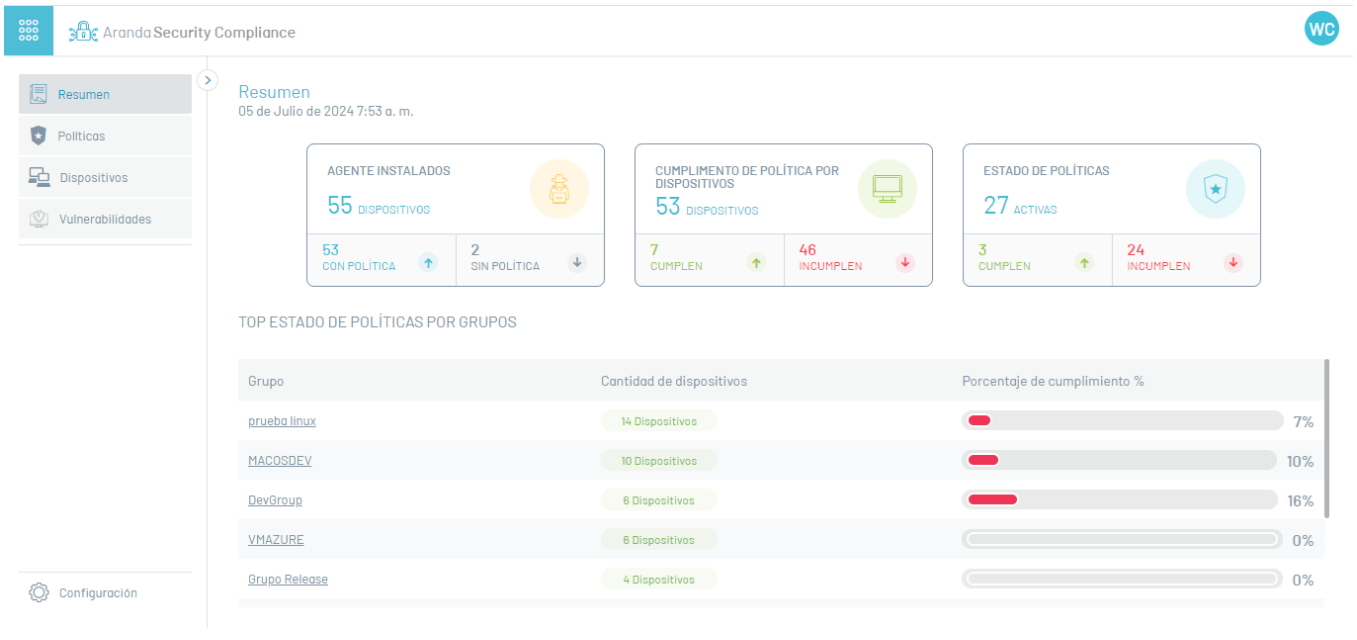
See the list of registered devices with details about their association with compliance groups and the vulnerabilities detected.

3. Vulnerabilities

View the vulnerabilities reported by each registered device, showing criticality levels to support the implementation of plans and policies.

Policy Summary

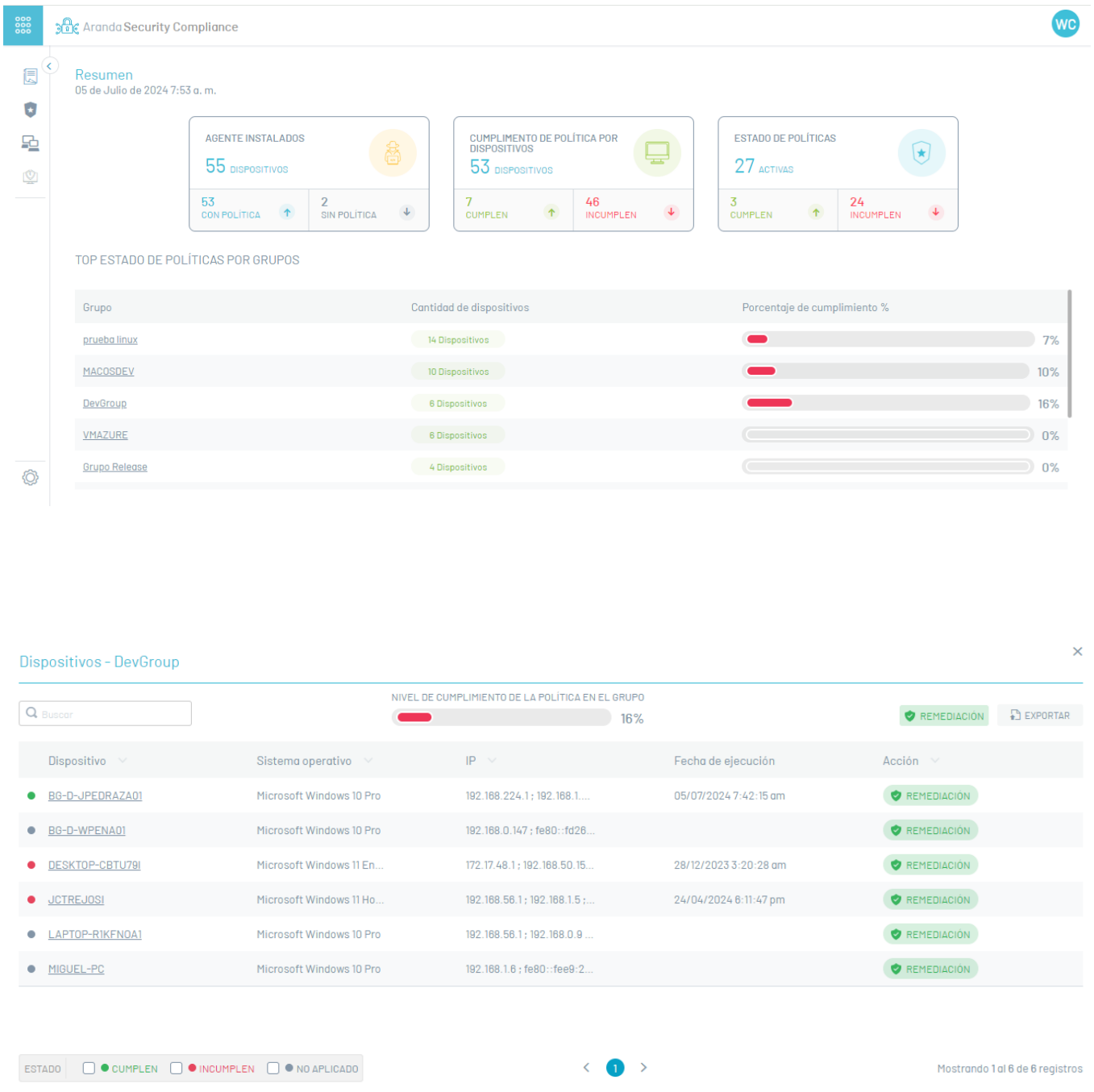
1. Enter the Aranda Security Compliance console with administrator role, select the option**Summary** from the main menu. In the information view, you can view the results of the security policy compliance analysis on the linked devices. The information generated is grouped by compliance levels, installed agents, policy status, and the top policy status by groups.



⚐ Note:

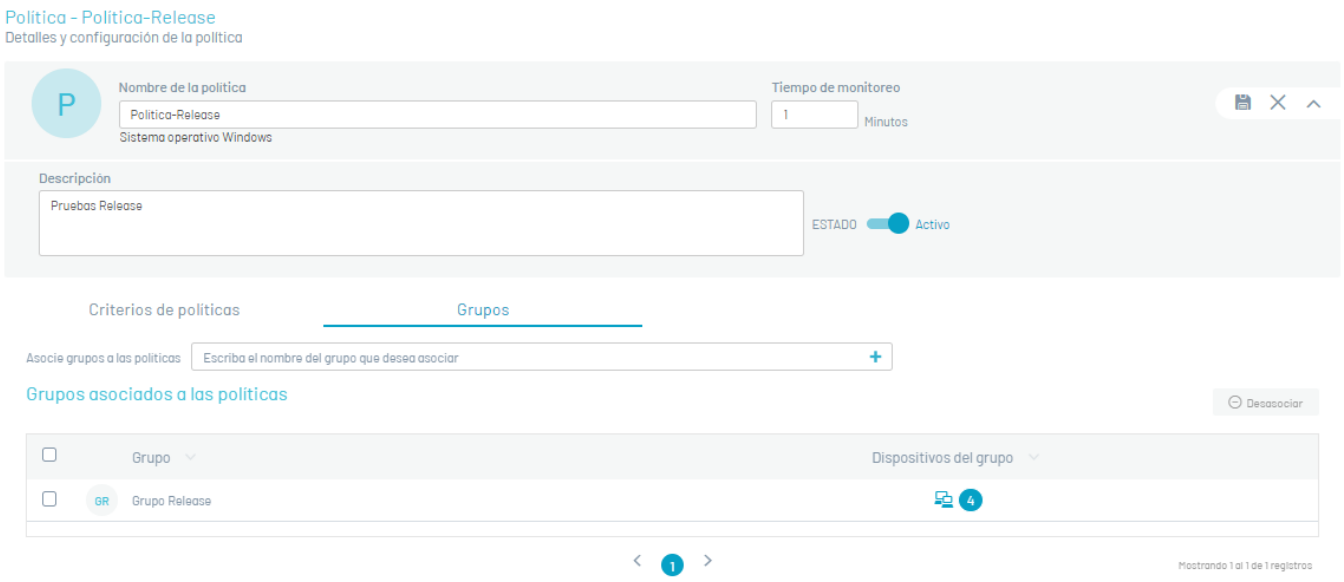
1. The consolidated report of compliance levels presents a global view of the status of the devices in relation to the security policies applied.
2. In the generated summary, only the information of the last 10 device records linked to the ASEC agent can be displayed.

2. In the Summary view, when you select a group from the top policy status, you will be able to access the[Device Compliance Detail](#) associated with the group.

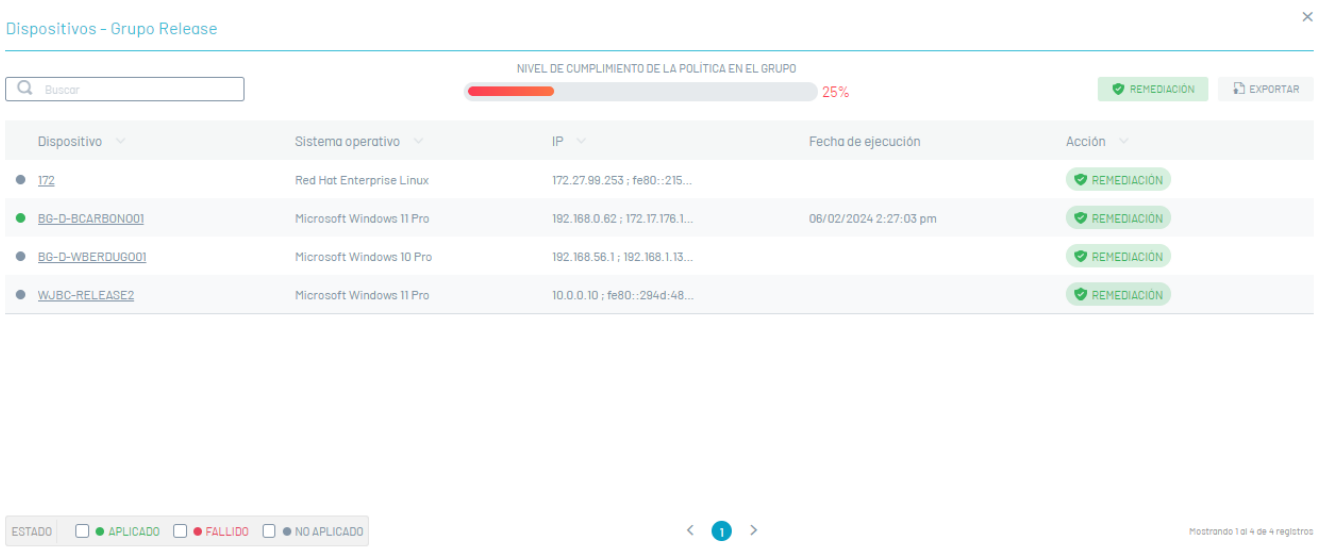


Device Compliance Detail

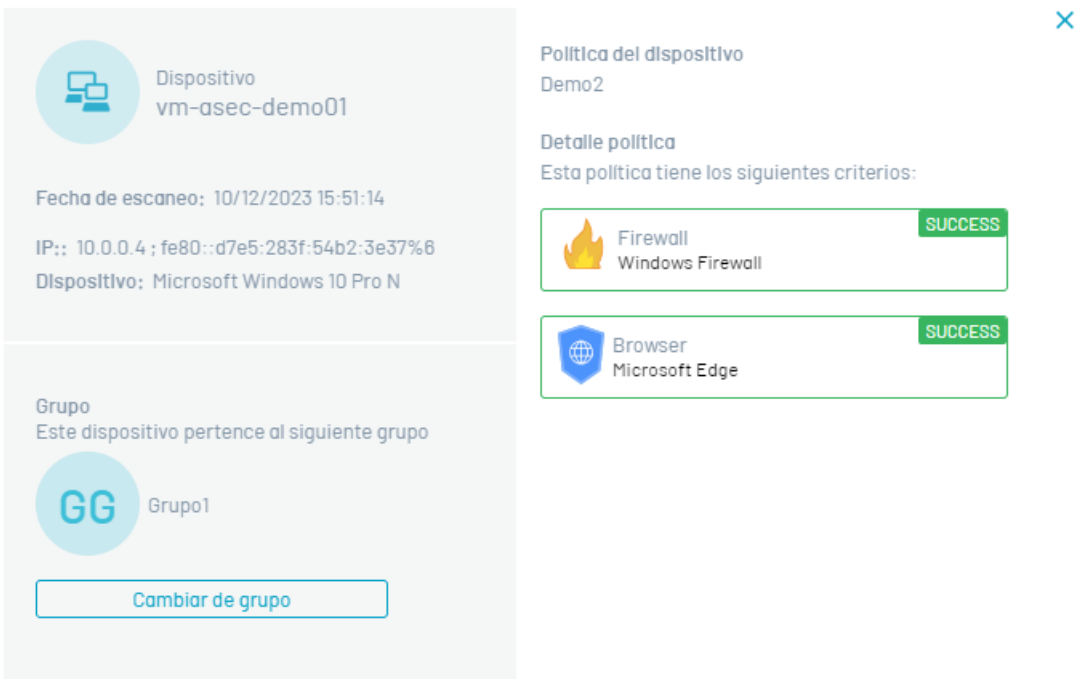
1. In the Policy information view in Aranda Security Compliance, on the**Groups** You will be able to view the list of groups associated with the policies. Selecting a group with associated devices will allow you to display the **Devices** with the detail of compliance of the devices.



2. In the window **Devices** You will be able to view the related information of the devices associated with a group. This data is organized by name, operating system, IP, start date, and remediation action to be executed of the group's compliance level.

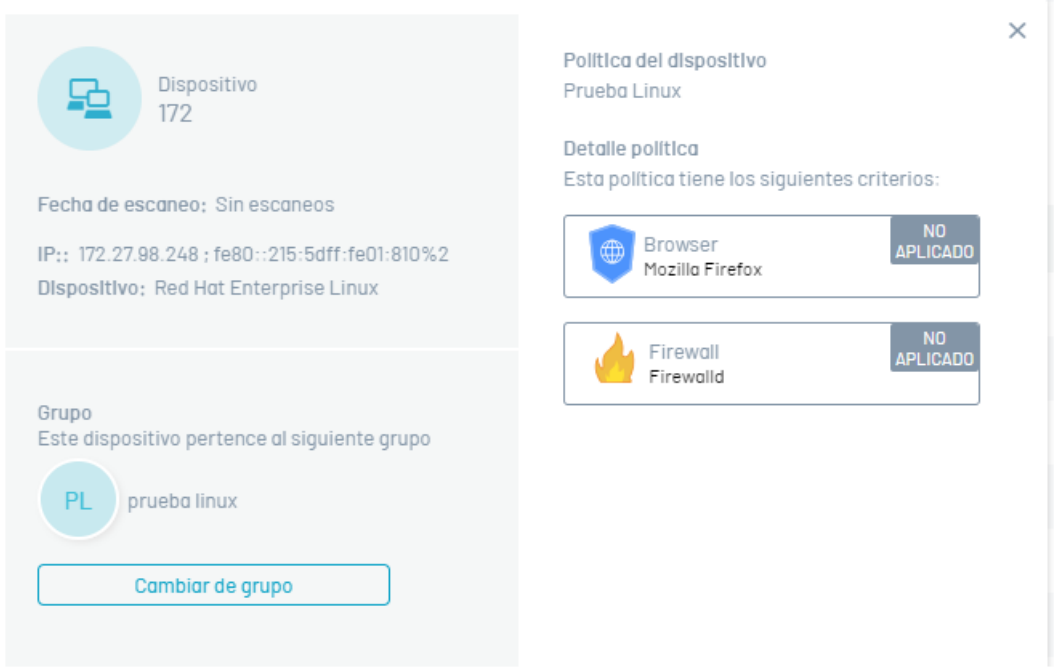


3. By selecting the device name, you can view in detail relevant information such as device name, policy name, the date of the scan, group to which it belongs, and applied policy criteria.

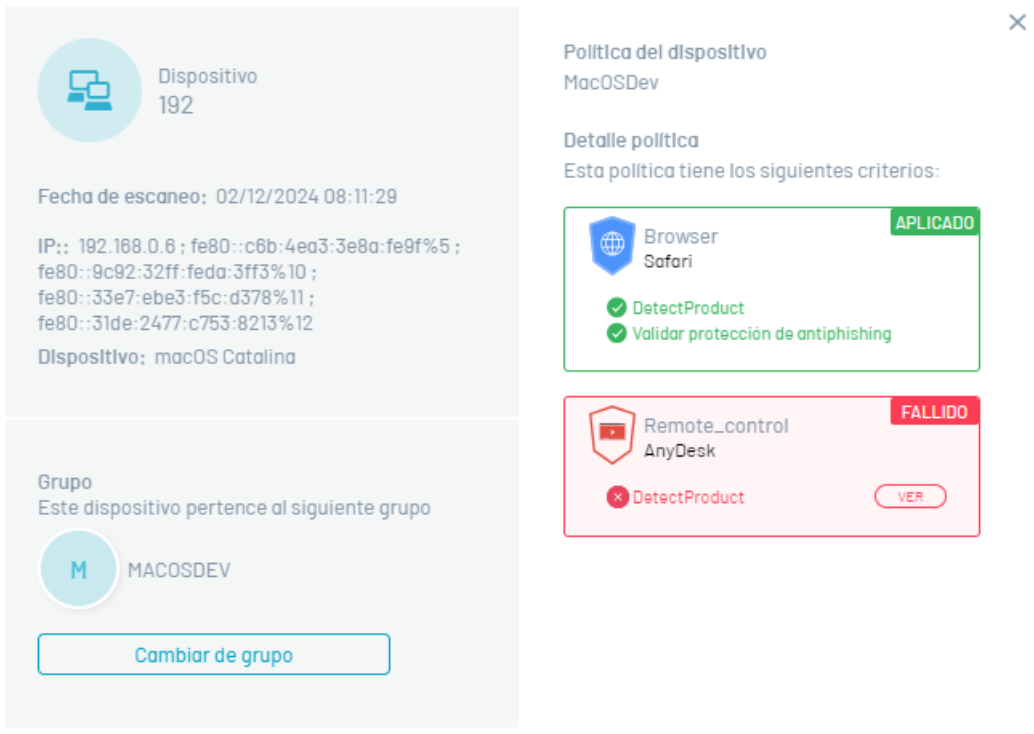


4. The detail of the policy applied to the device will be able to visualize the level of compliance with the criteria of the implemented policies, through the referenced States:

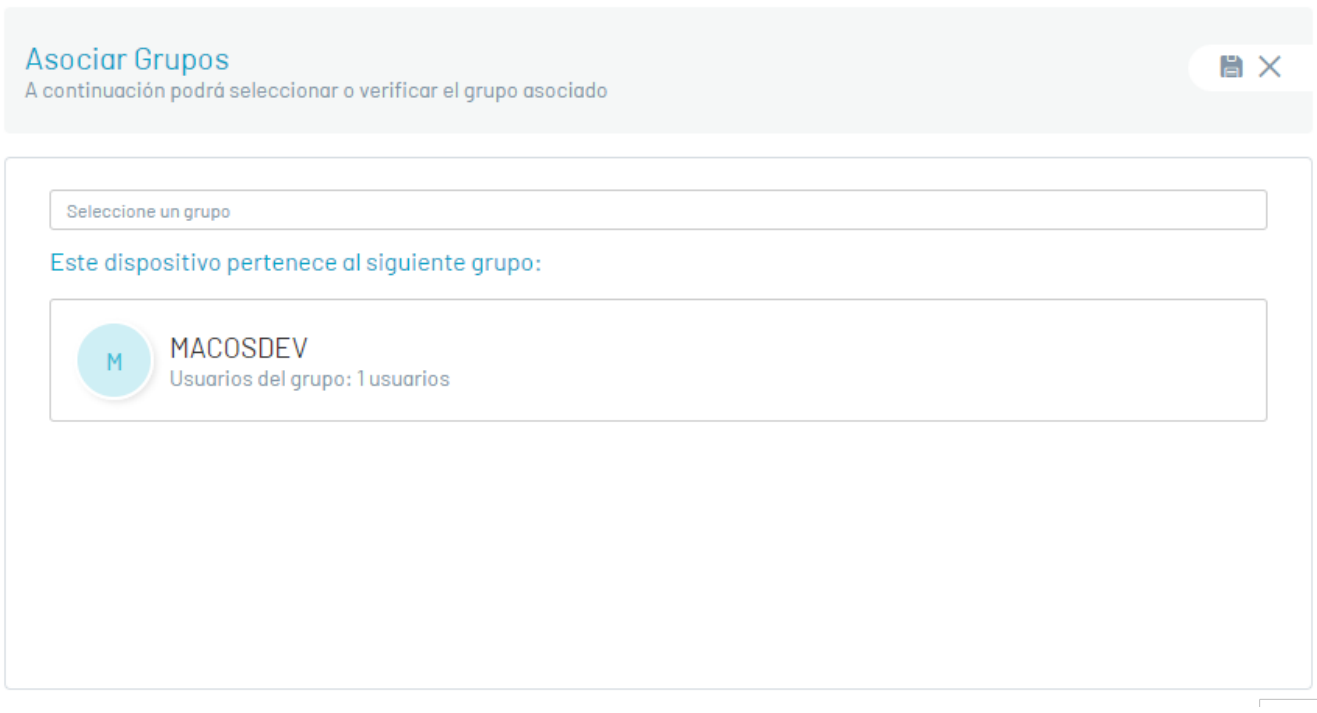
States	Description
SUCCESS	The Successful status is displayed when the policy criterion is met, applied to the device.
FAILED	The failed status is displayed when the policy criterion, applied to the device, is NOT met
NOT APPLIED	The Not Applicable status is displayed when the device has not been scanned.



5. In the policy detail, selecting the generated state displays the case validations.

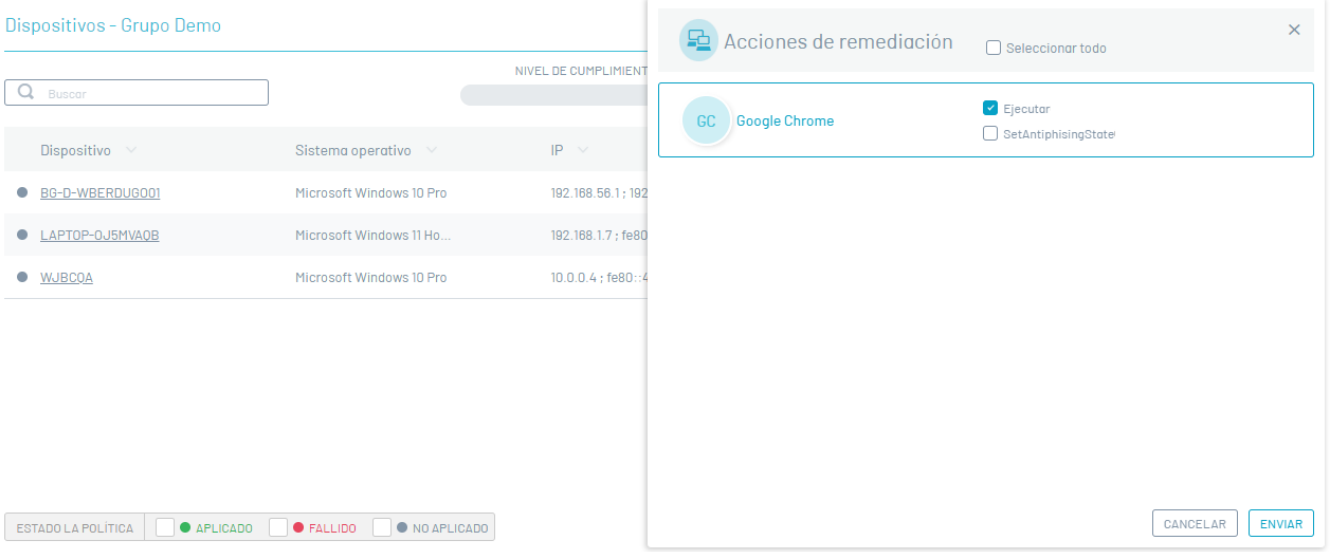


⚐ **Note:** In the device detail select the**Change Group** to modify the existing group association.



Remediation Actions

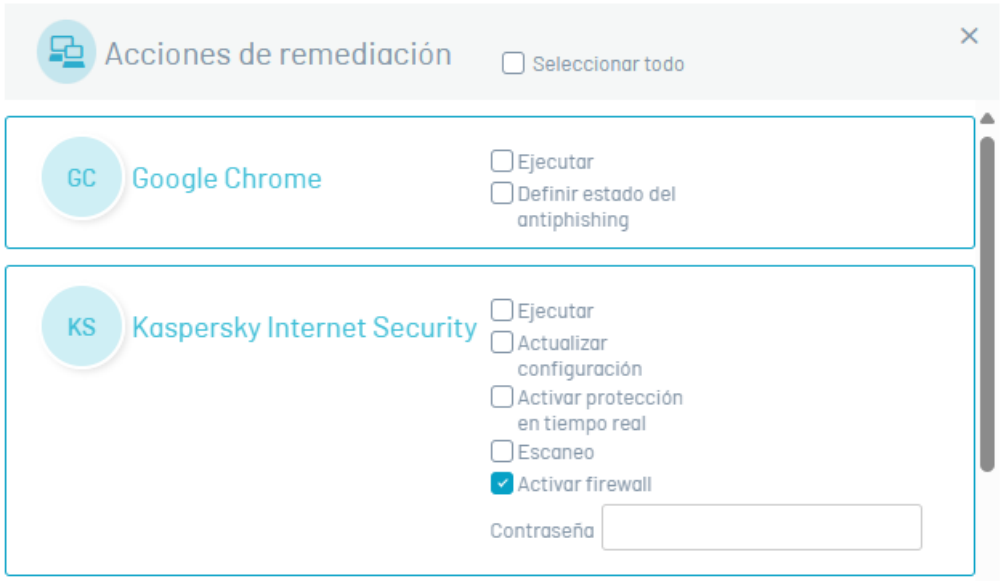
6. Regardless of the status generated (Successful, Failed, or Not Applicable) during the policy compliance analysis on the devices, you will be able to execute the required remediation actions. Select the **Remediation** to execute the actions enabled for the implemented security criterion.



⚐ **Note:** When you select the**Send** The chosen remediation actions will be implemented.

⚐ **Note:** By selecting the menu option **Compliance Groups** in the list, only the remediations are performed in the options in the**Group devices**

7. Remediation actions that require a password require the management product key. These keys are required to access the advanced settings of the software. The countryside **Password** It is not required and can be left blank, unless the product requires an administration key to make modifications.

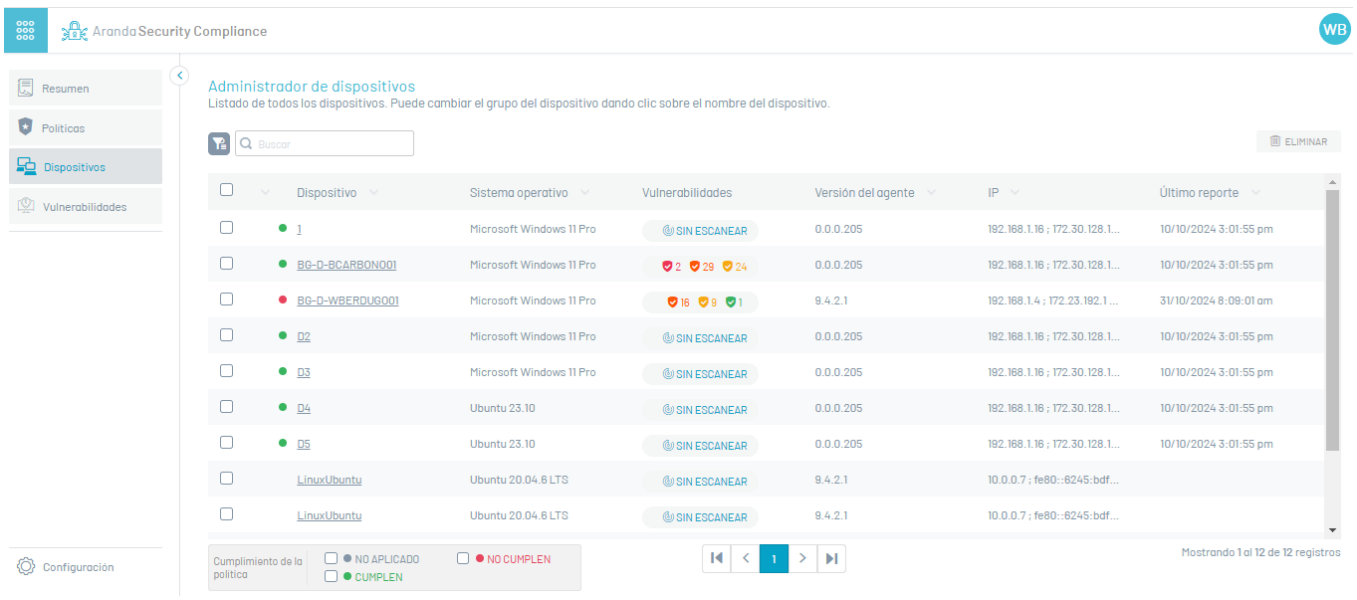


⚐ **Note:** Administration or Change Keys:

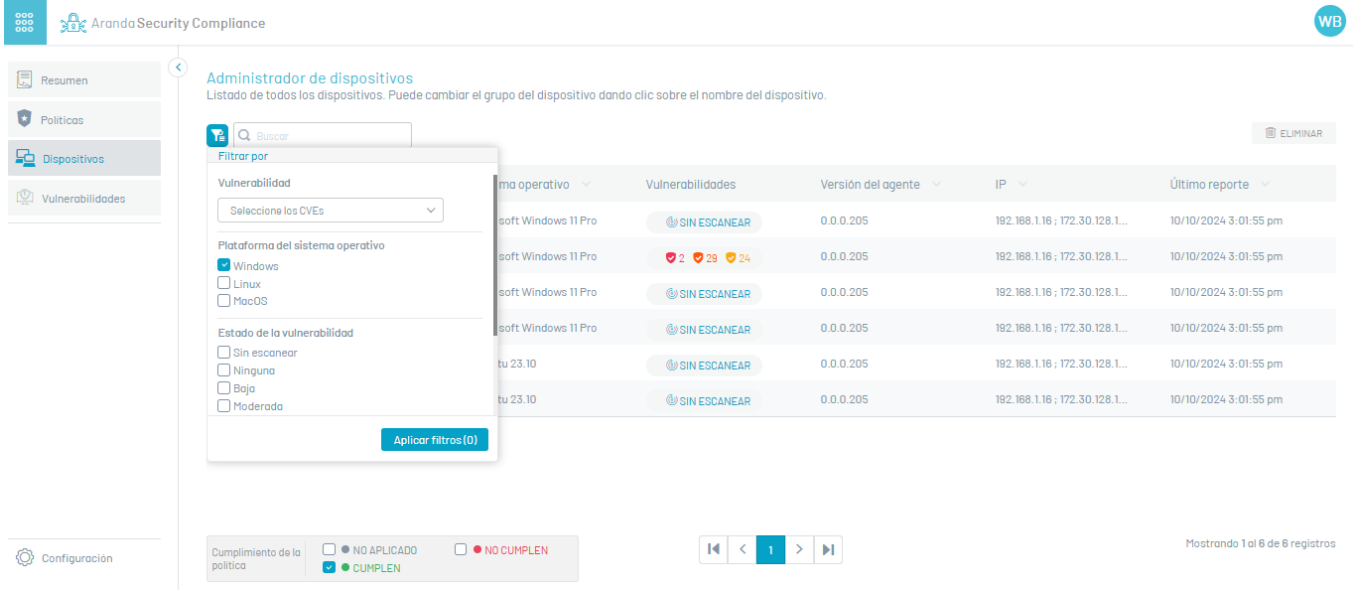
- 1. Required to make significant changes to software configuration or management.
- 2. They prevent unauthorized access and unwanted modifications.
- 3. Examples: Administrator keys in operating systems, root keys in Android mobile devices, keys to access advanced settings in security systems or business software.

Devices

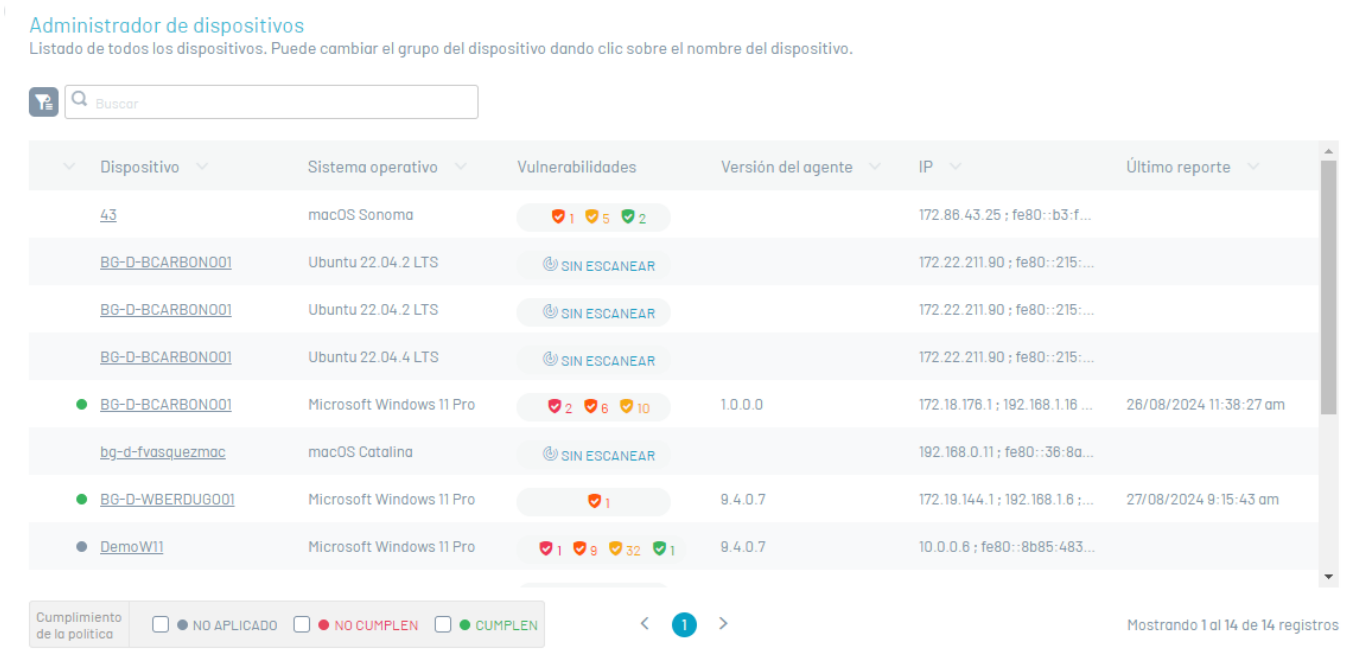
1. Enter the Aranda Security Compliance console with administrator role, select the option**Devices** from the main menu. In the information view, you can view the list of devices registered through the Agent, showing the name, operating system, vulnerabilities, and the latest policy report.



2. In the Devices view, the filter option is enabled in the upper left, divided by the sections of**Vulnerability**,**Operating System Platform**,**Vulnerability status**. This filter allows users to refine the list of devices displayed, making it easier to identify those that meet specific criteria based on their security status, device type, and most recent evaluation status.

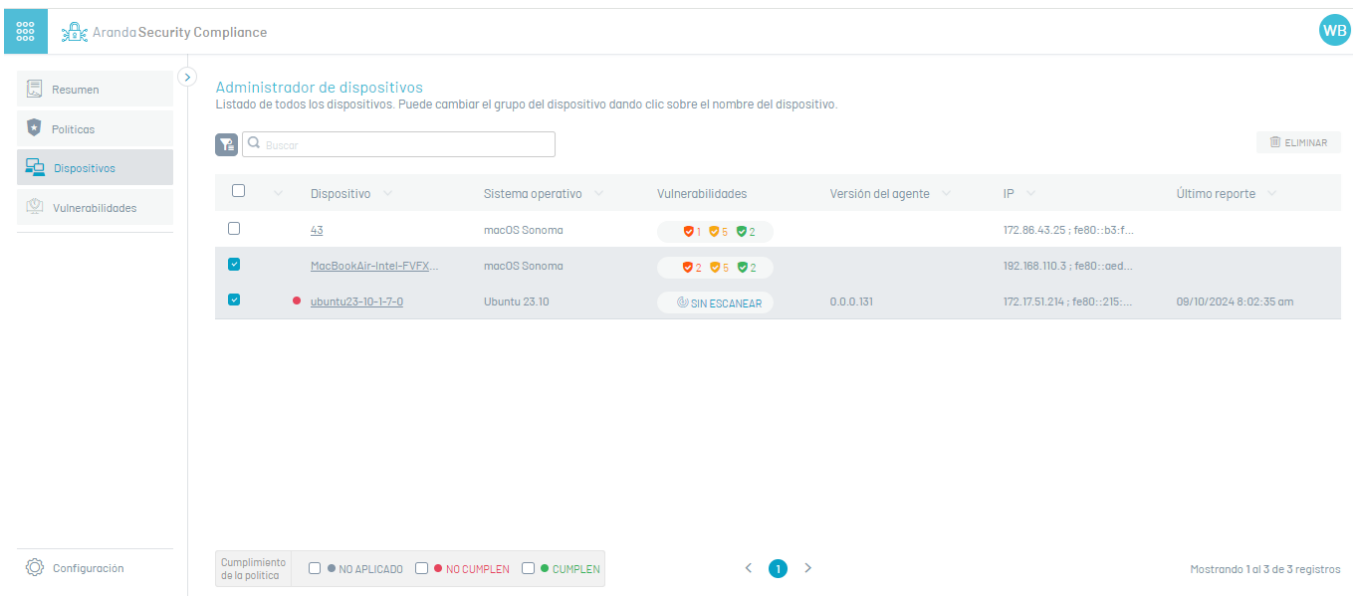


3. The Policy Compliance Filter, located in the footer, is designed to filter devices based on their alignment with established security policies. By enabling this filter, users can only view devices that meet or do not meet the requirements of these policies, making it easy to quickly identify equipment that requires corrective action or that is in compliance with established standards. This allows for more efficient management of compliance status across the device environment.

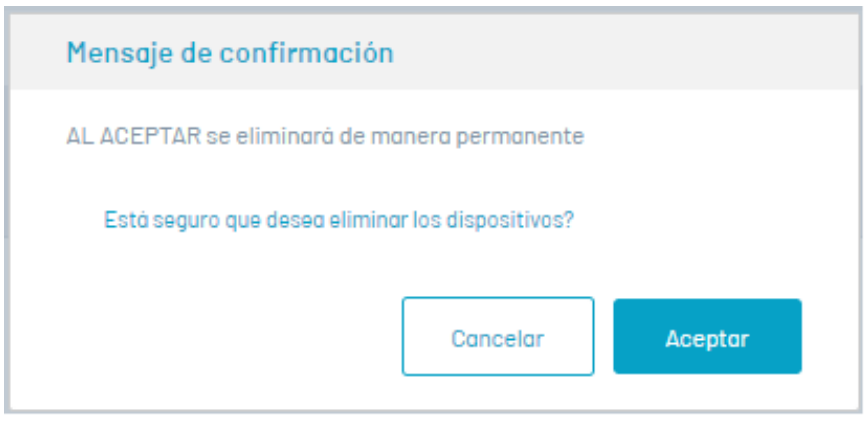


Remove Devices

4. To remove devices, select one or more records and click the **Eliminate**.

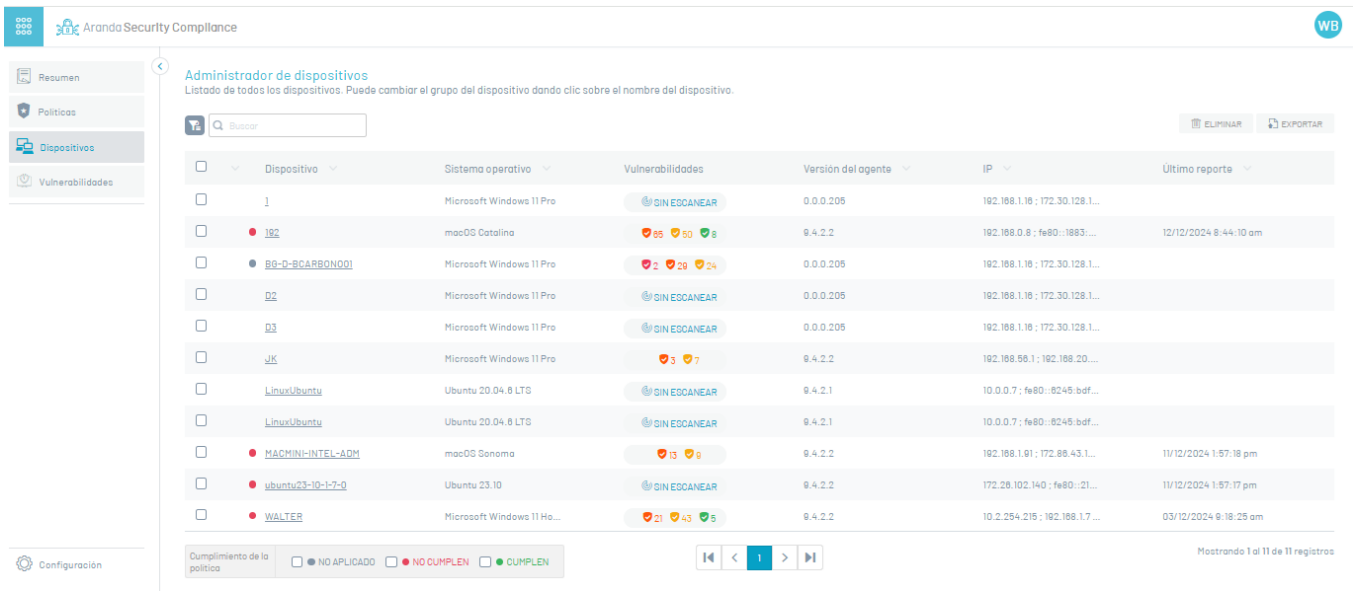


5. A warning message is enabled where you must confirm the wiping of the device.

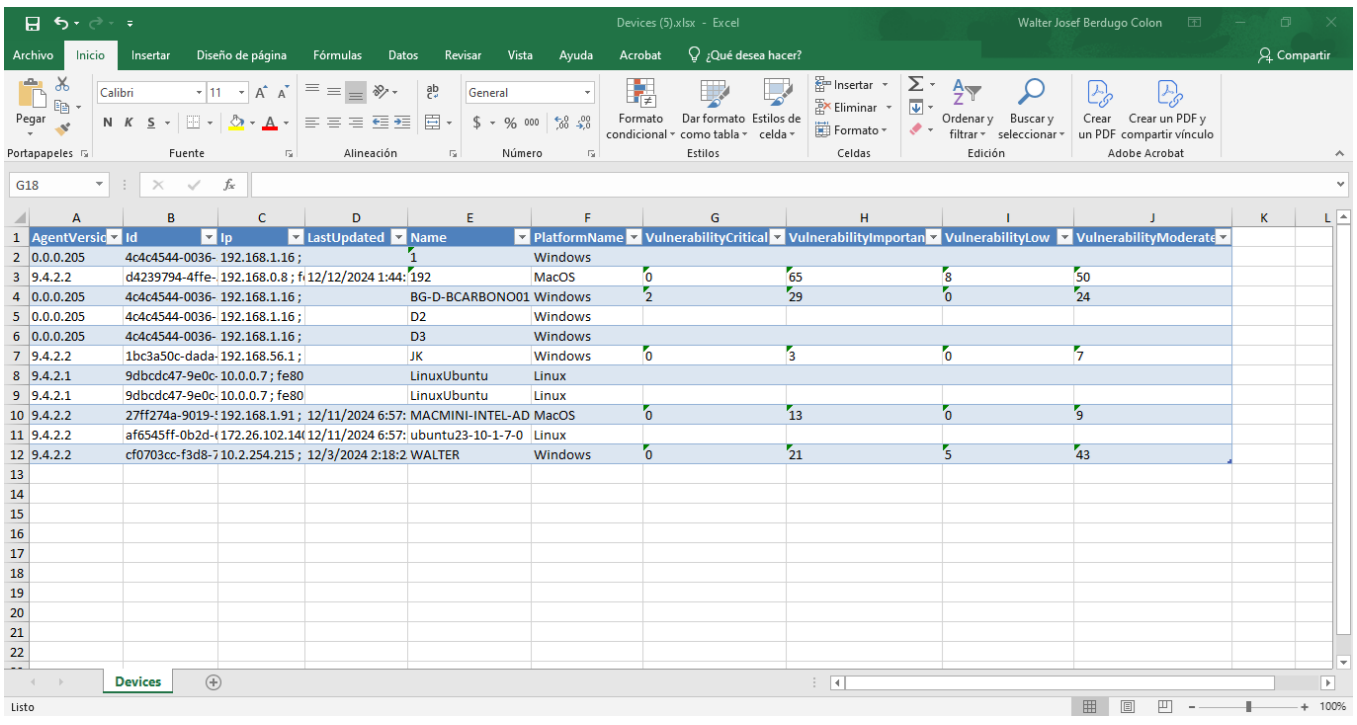


Export Devices

1. In the Devices information view, after filtering the respective data and getting the list of available devices, click the **Export**.

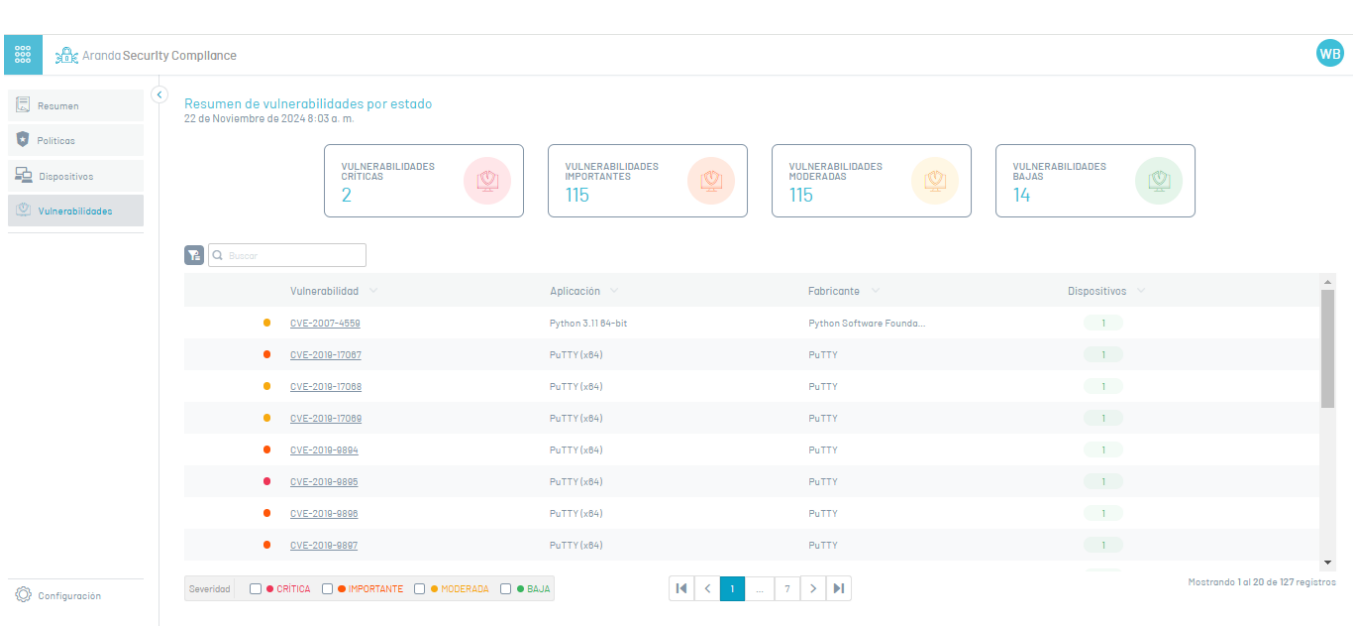


2. In the Aranda Security Management Console header menu, the option to **Downloads** where you can view the generated format of the list of devices in Excel format
3. Click on the file to download the device information. The downloaded file includes all the fields on the device.



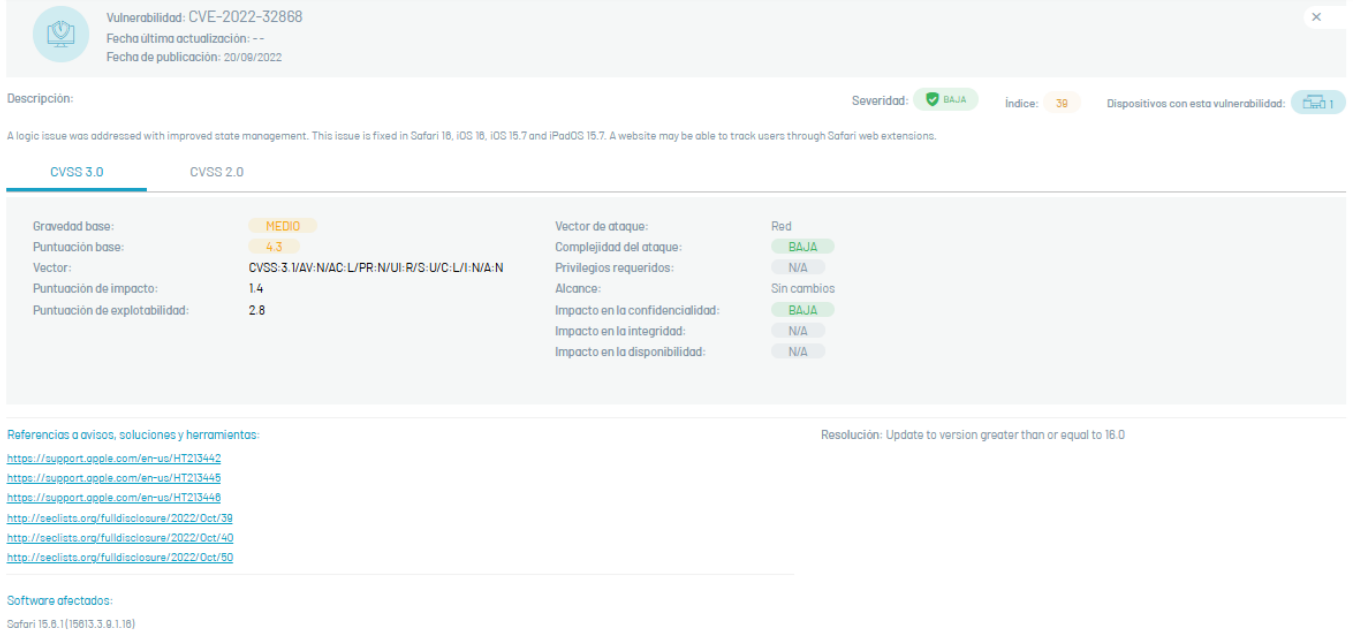
Vulnerabilities

1. Enter the Aranda Security Compliance console, select the option **Vulnerabilities** from the main menu. In the summary view, you will be able to view the results of the analysis of the list of vulnerabilities classified by severity and grouped by devices



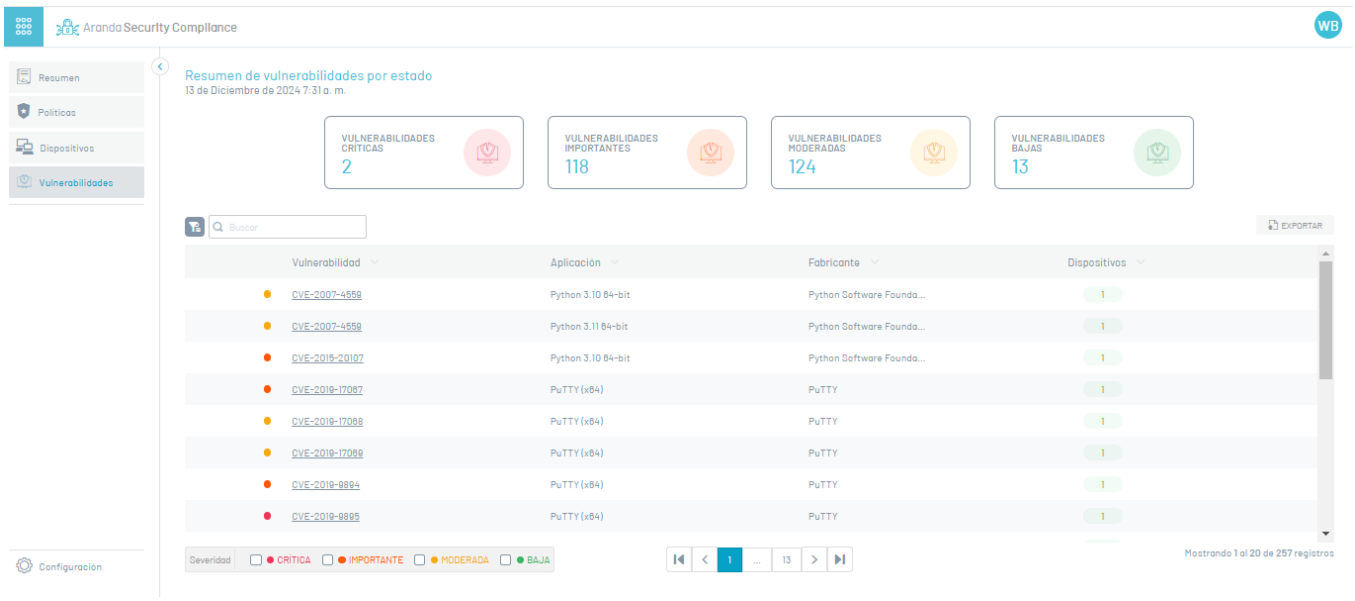
⚐ **Note:** The report generated from the vulnerability scan performed by the agents is only available for Windows and MacOS operating systems. If you are using a different operating system, you will not be able to access this report.

2. In the Vulnerabilities view, when selecting the name of a vulnerability, a new view is displayed showing the name, description, date of last update, date of publication, severity, affected software and the number of devices that register it with access to filter the devices.

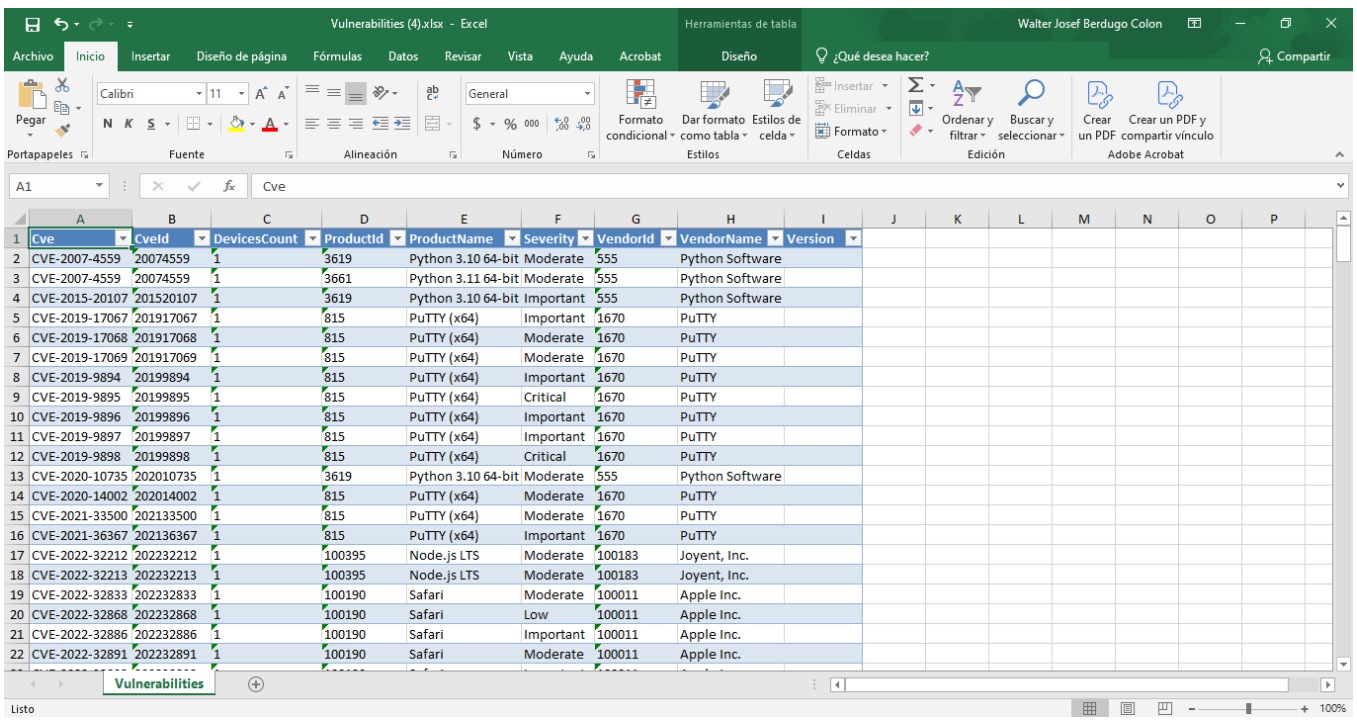


Export Vulnerabilities

1. In the Vulnerabilities information view, after filtering the respective data and getting the list of vulnerabilities associated with devices, click the**Export**.



2. In the Aranda Security Management Console header menu, the option to**Downloads** where you can view the generated format of the list of vulnerabilities in Excel format 3. Click on the file to download the vulnerability information. The downloaded file includes all the fields of the vulnerability.



	Cve	CveId	DevicesCount	ProductId	ProductName	Severity	VendorId	VendorName	Version
2	CVE-2007-4559	20074559	1	3619	Python 3.10 64-bit	Moderate	555	Python Software	
3	CVE-2007-4559	20074559	1	3661	Python 3.11 64-bit	Moderate	555	Python Software	
4	CVE-2015-20107	201520107	1	3619	Python 3.10 64-bit	Important	555	Python Software	
5	CVE-2019-17067	201917067	1	815	PuTTY (x64)	Important	1670	PuTTY	
6	CVE-2019-17068	201917068	1	815	PuTTY (x64)	Moderate	1670	PuTTY	
7	CVE-2019-17069	201917069	1	815	PuTTY (x64)	Moderate	1670	PuTTY	
8	CVE-2019-9894	20199894	1	815	PuTTY (x64)	Important	1670	PuTTY	
9	CVE-2019-9895	20199895	1	815	PuTTY (x64)	Critical	1670	PuTTY	
10	CVE-2019-9896	20199896	1	815	PuTTY (x64)	Important	1670	PuTTY	
11	CVE-2019-9897	20199897	1	815	PuTTY (x64)	Important	1670	PuTTY	
12	CVE-2019-9898	20199898	1	815	PuTTY (x64)	Critical	1670	PuTTY	
13	CVE-2020-10735	202010735	1	3619	Python 3.10 64-bit	Moderate	555	Python Software	
14	CVE-2020-14002	202014002	1	815	PuTTY (x64)	Moderate	1670	PuTTY	
15	CVE-2021-33500	202133500	1	815	PuTTY (x64)	Moderate	1670	PuTTY	
16	CVE-2021-36367	202136367	1	815	PuTTY (x64)	Important	1670	PuTTY	
17	CVE-2022-32212	202232212	1	100395	Node.js LTS	Moderate	100183	Joyent, Inc.	
18	CVE-2022-32213	202232213	1	100395	Node.js LTS	Moderate	100183	Joyent, Inc.	
19	CVE-2022-32833	202232833	1	100190	Safari	Moderate	100011	Apple Inc.	
20	CVE-2022-32868	202232868	1	100190	Safari	Low	100011	Apple Inc.	
21	CVE-2022-32886	202232886	1	100190	Safari	Important	100011	Apple Inc.	
22	CVE-2022-32891	202232891	1	100190	Safari	Moderate	100011	Apple Inc.	

Device Detail

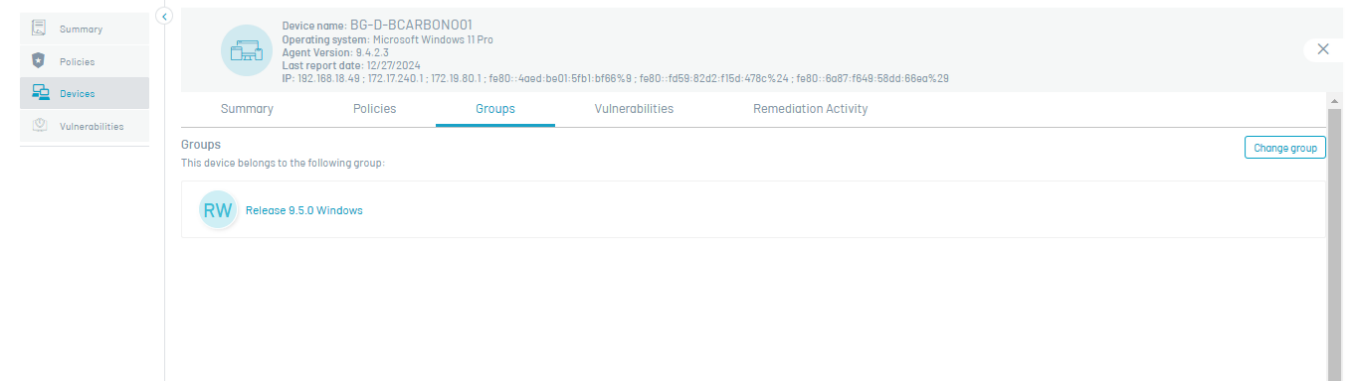
From the view of the list of Devices, you will be able to access a detail where the summary of vulnerabilities, the list of vulnerabilities and the group with its associated policy will be displayed.

Summary Vulnerabilities

When you select the**Summary** a summary of the vulnerabilities registered in the Device will be displayed, the total number of vulnerabilities by severity and the top 5 applications with the most vulnerabilities will be indicated.

Policies

When you select the**Policies**, the criteria associated with the device will be displayed, along with the policy name. The remediation options and the date of the last scan will also be displayed, allowing the most recent changes to be identified.

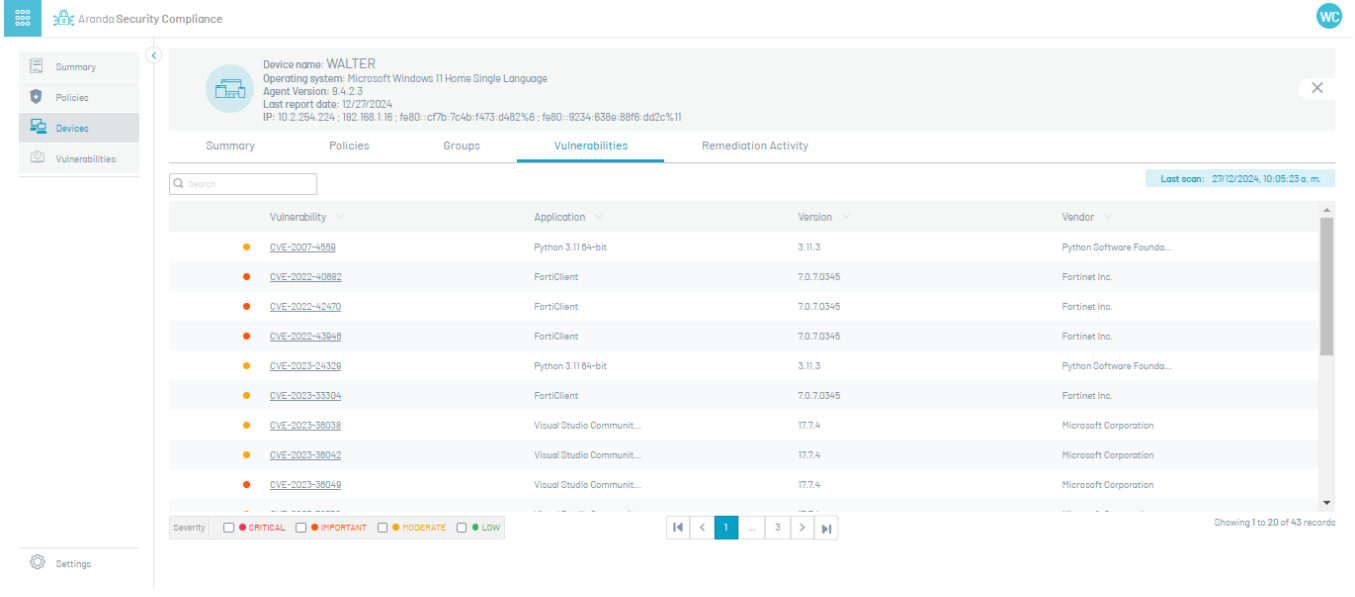


Groups

When accessing the**Groups**, the name of the only group that the device is associated with will be displayed. This functionality allows the relationship between the device and its corresponding group to be quickly and accurately identified, facilitating its management within the platform.

Vulnerabilities

When you select the**Vulnerabilities**, a detailed list of detected vulnerabilities that are associated with the device will be displayed. In addition, the tool offers severity filtering options, making it easy to prioritize those most critical vulnerabilities that require immediate attention.

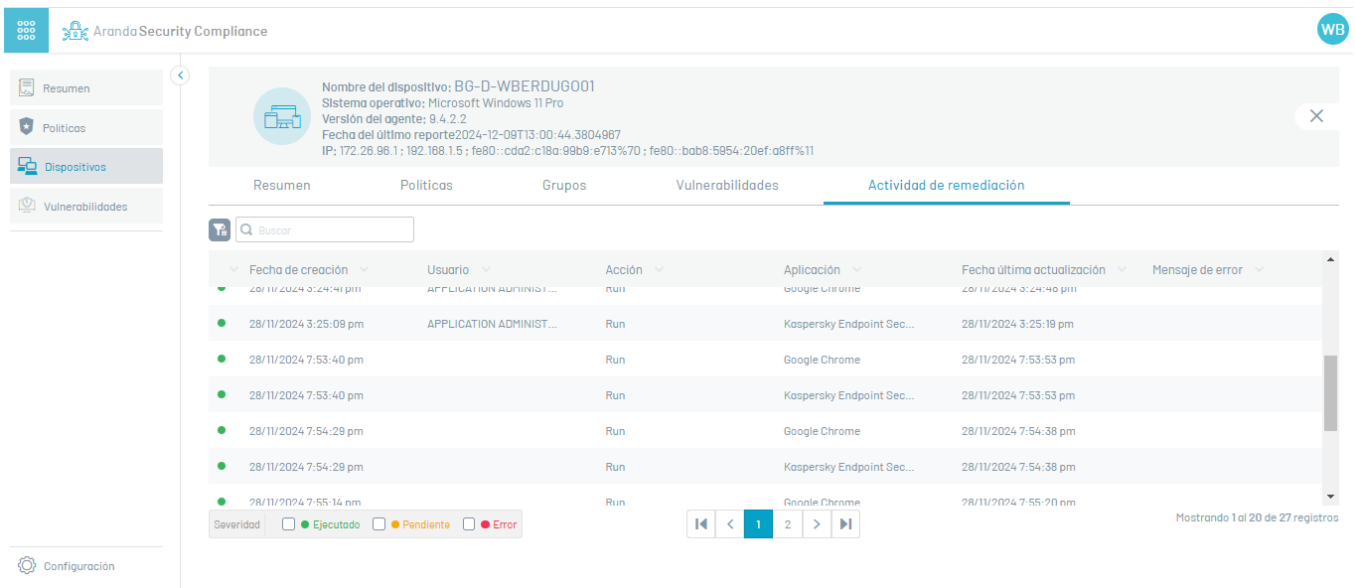


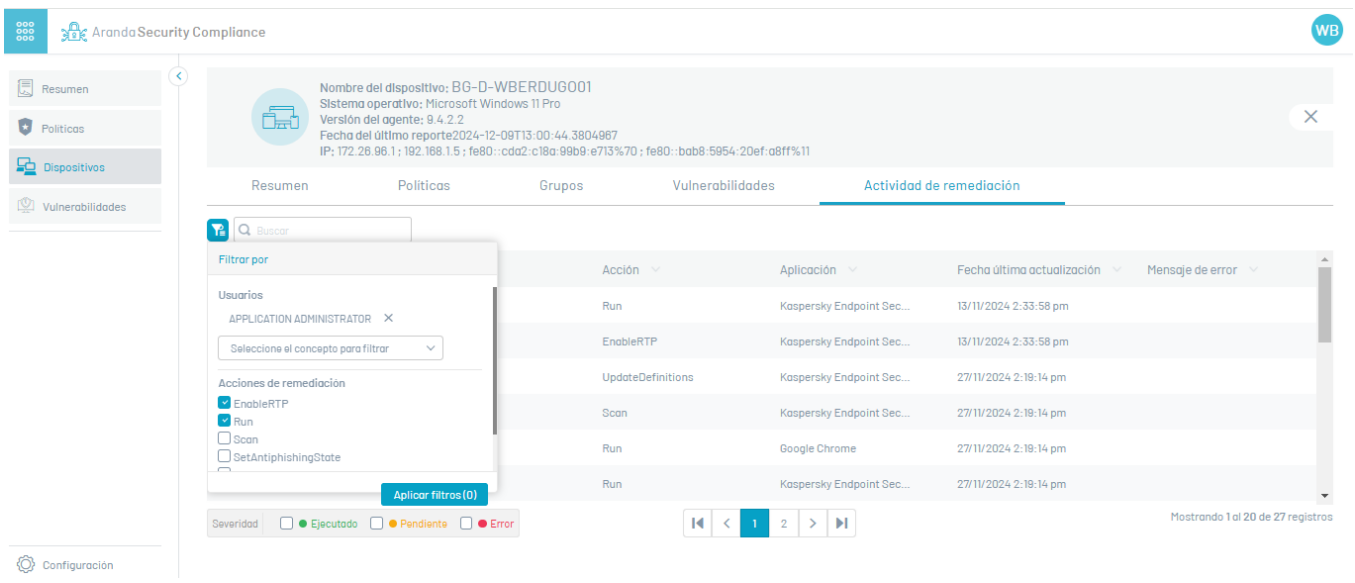
Remediation Activity

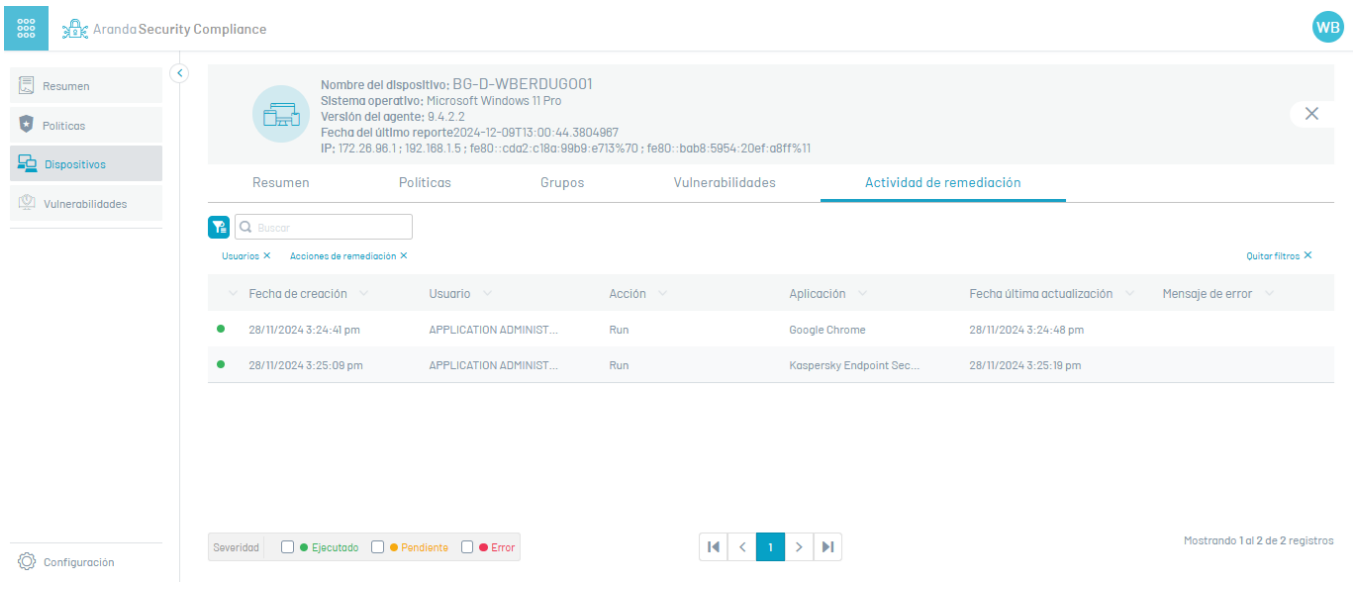
When you select the**Remediation Activity**, you will be able to view the list of actions carried out on the device, allowing detailed monitoring according to their status of evolution (Executed, Pending or Error) and facilitating the supervision and management of remediations.

⚐ **Note:** In this section you will be able to Apply the advanced filters to search for user-specific actions and/or remediation actions and/or Use the filters by status to identify devices or systems that require tracking, corrective actions, or priority attention.

This management speeds up the location of interventions and ensures quick access to the information necessary for analysis and decision-making.







ASEC Configuration

The general administrator from the ASEC Web console will be able to perform the following configuration tasks:

1. Deploy Agent

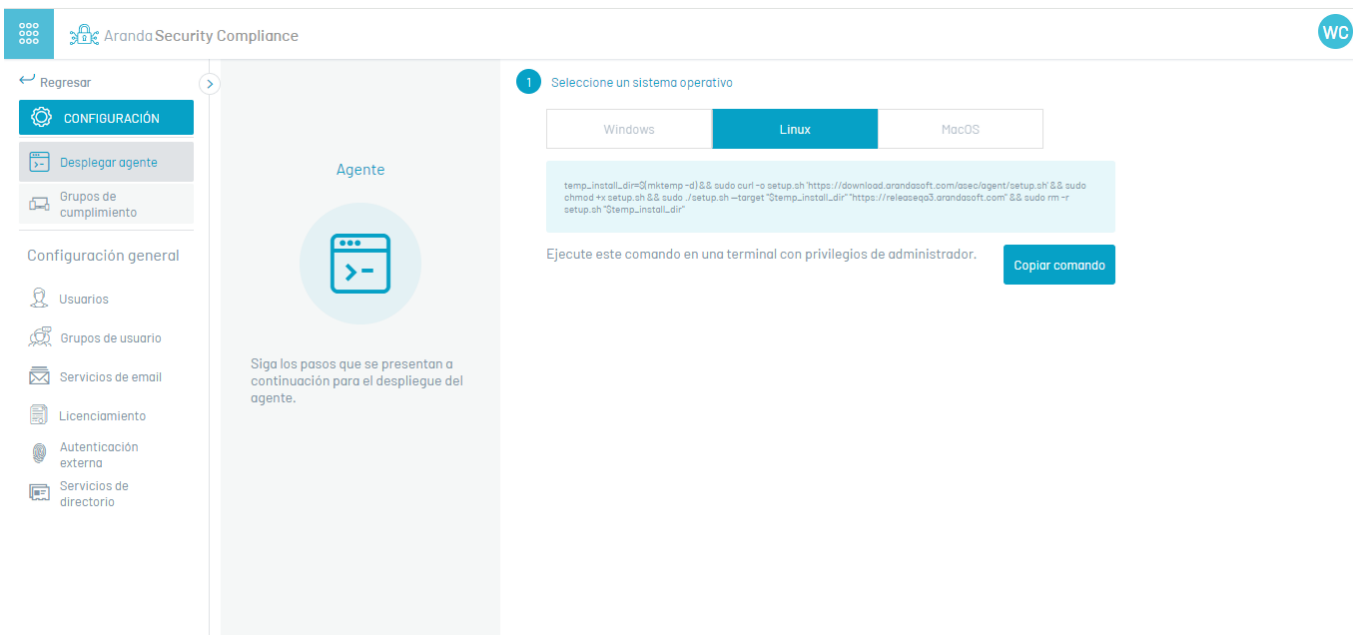
Distribute the Aranda Security agent on the different devices that require the evaluation of compliance with security policies.

2. Policy Groups

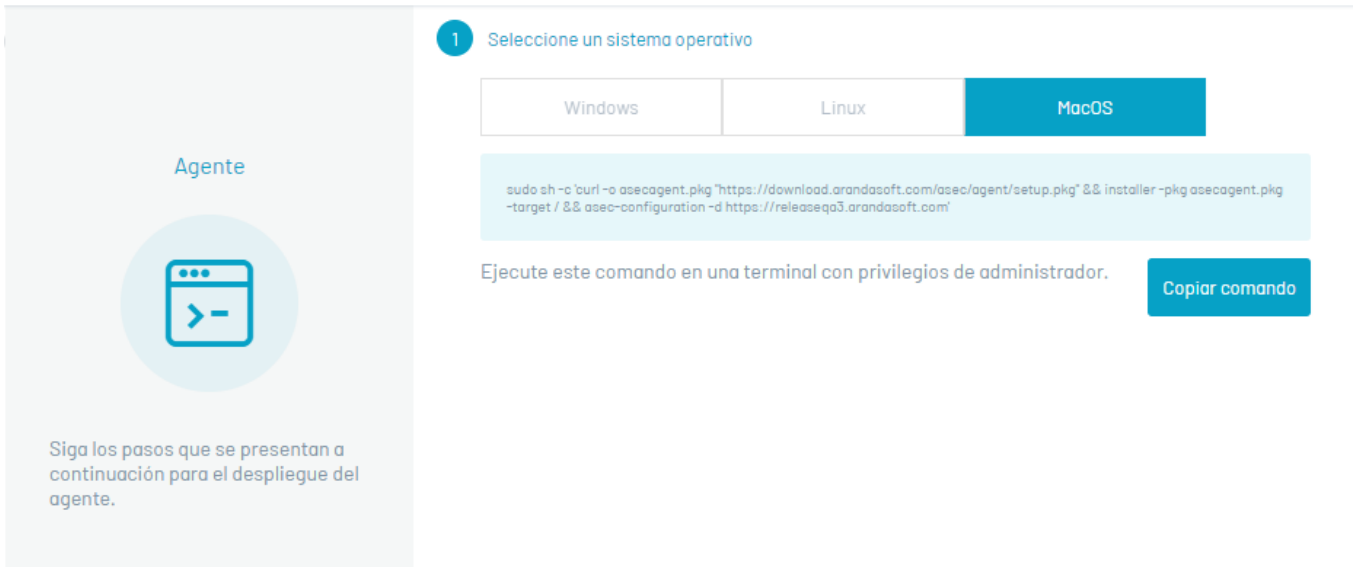
Manage the groups associated with compliance policies and include the provisions for each group.

Deploy Agent

1. To deploy the agent, log in to the Aranda Security Compliance console as an administrator, in the **Configuration** from the main menu, select the **Deploy Agent**. In the information view, you will be able to see the steps to deploy the agent on the devices.



2. In the agent deployment information view, select an operating system (Wndows, Linux, Mac).



3. Selecting the operating system enables the script to install and enroll the agent. Click the **Copy Command**; This information will be saved to the clipboard.
4. Copy the execution command and continue the ASEC agent distribution and installation process, according to the defined deployment type:

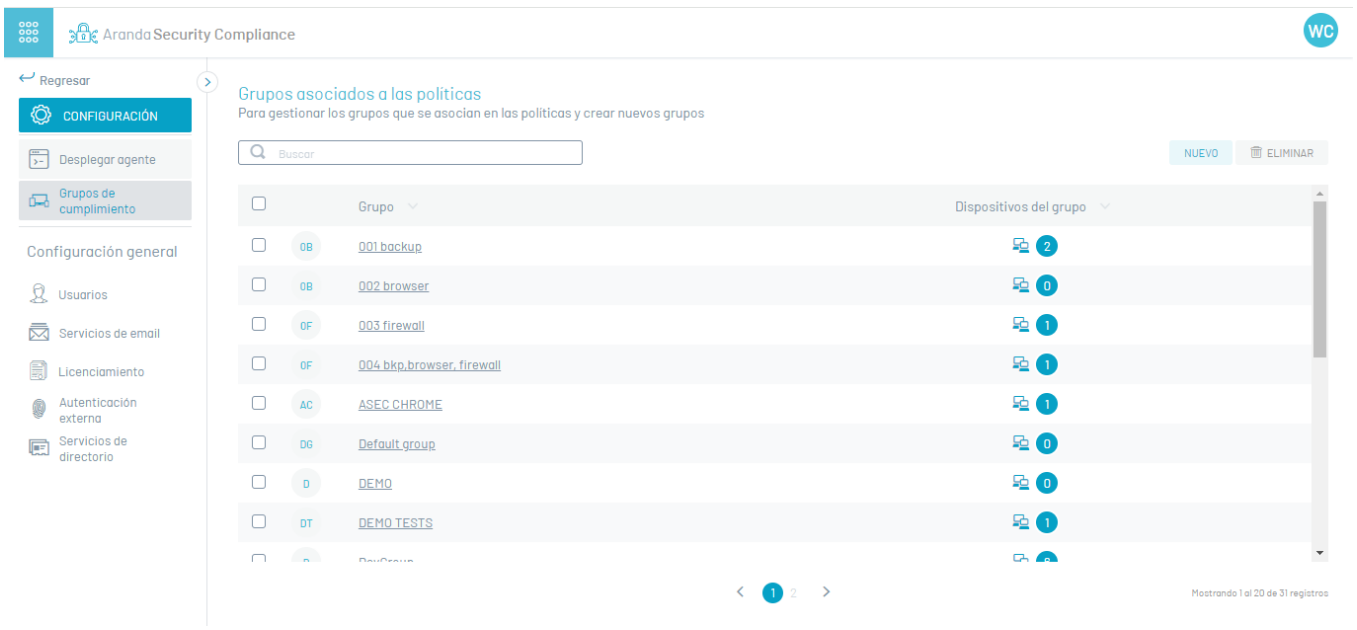
- Installation by Devices ↪
- Installation by Domain Policy ↪
- Installation and distribution with Aranda Device Management ADM ↪

Policy Groups

In the section you will find the groups that are created from the Aranda Security Compliance console.

View Groups and Devices

1. Enter the Aranda Security Compliance console with administrator role, in the section **Configuration** from the main menu, select the **Compliance Groups**. In the information view, you can view the list of available groups and sort the information by name of groups and devices.



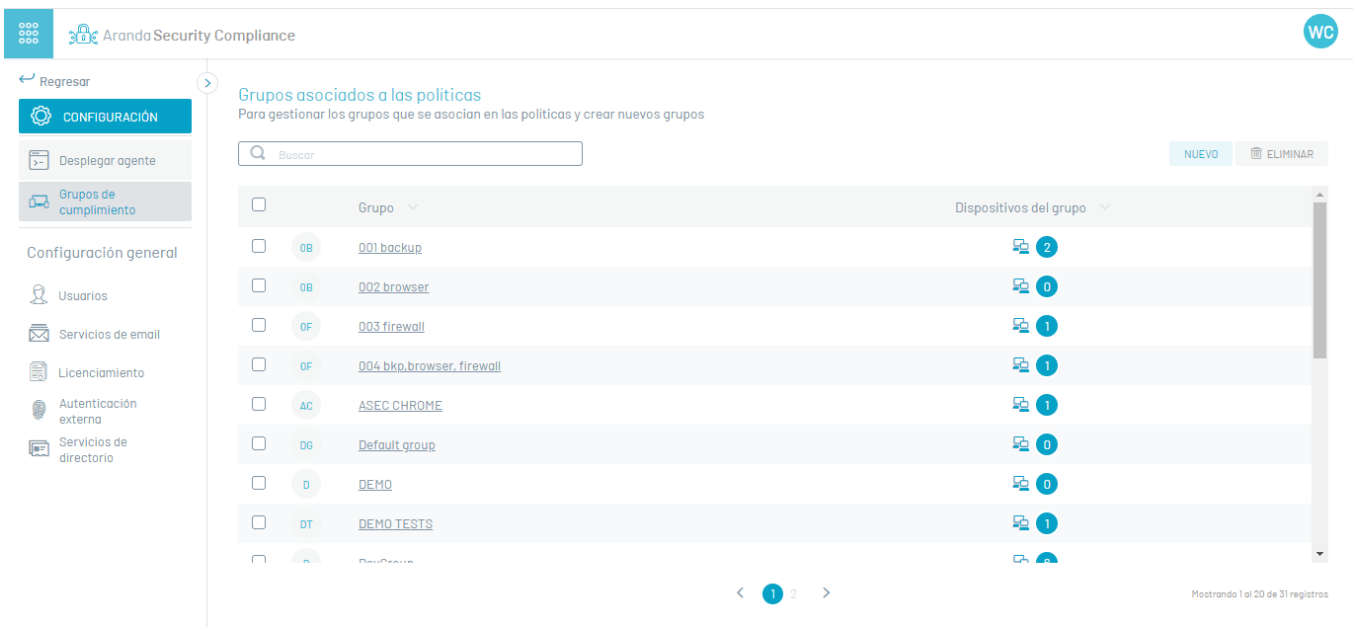
2. En la vista de información de grupos también podrá visualizar el listado de dispositivos que pertenecen a cada grupo.

> ⚐ **Note:** If the group has an associated policy, it will present the device status and the respective remediation actions that can be applied.

Group Creation

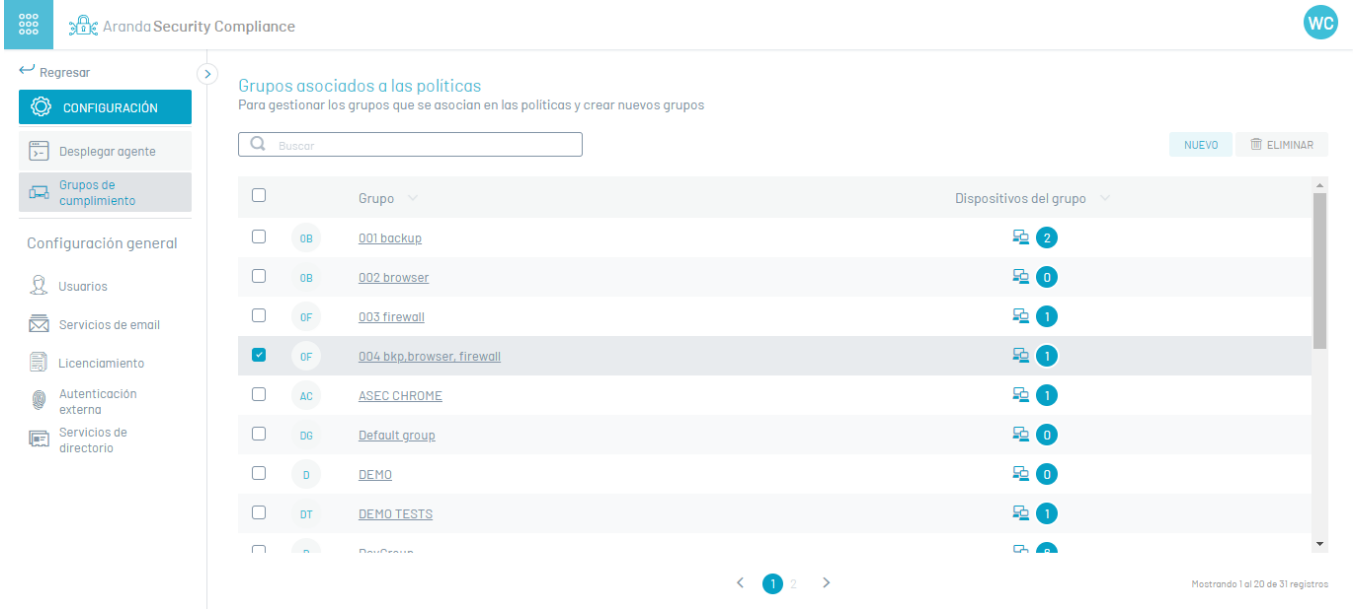
3. To create policy groups, in the group information view, select the **New**; window is enabled **Devices** where you can enter the name of the group.

When you enter the created group again, you will have the options to associate and disassociate devices enabled.



Remove from Groups

4. To delete groups, in the group information view, select a record from the list and click the **Eliminate**.

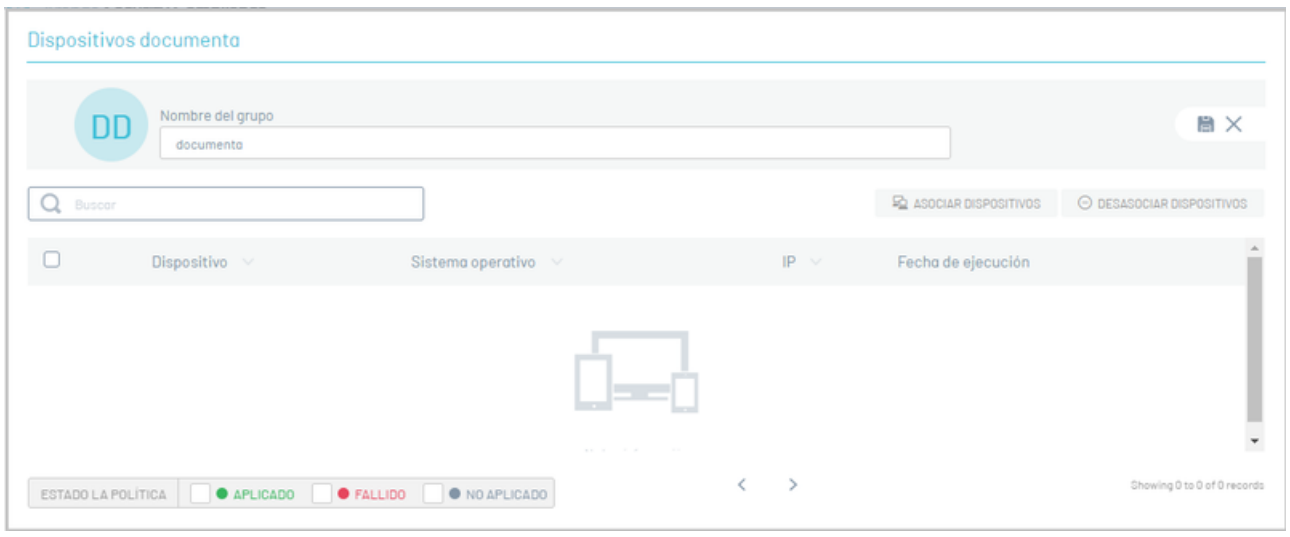


En la ventana que se habilita podrá confirmar o denegar la acción de eliminar el grupo.

⚐ **Note:** If the group has devices associated with it, at the time of confirmation, the devices will be available to be associated with another group.

Associate devices

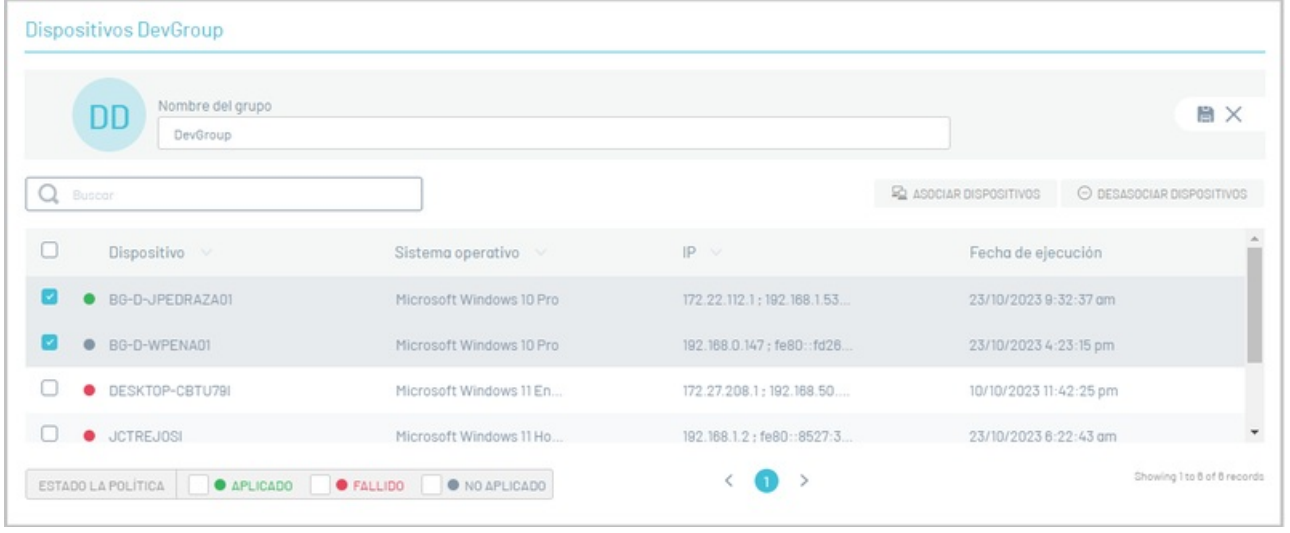
5. To associate devices, in the group information view, enter a record of a created group, and in the **Devices** Click the **Associate Devices**.



En el listado de dispositivos seleccione un registro y haga clic en el botón **Asociar Dispositivos** , para asociar el dispositivo al grupo.

Disassociate devices

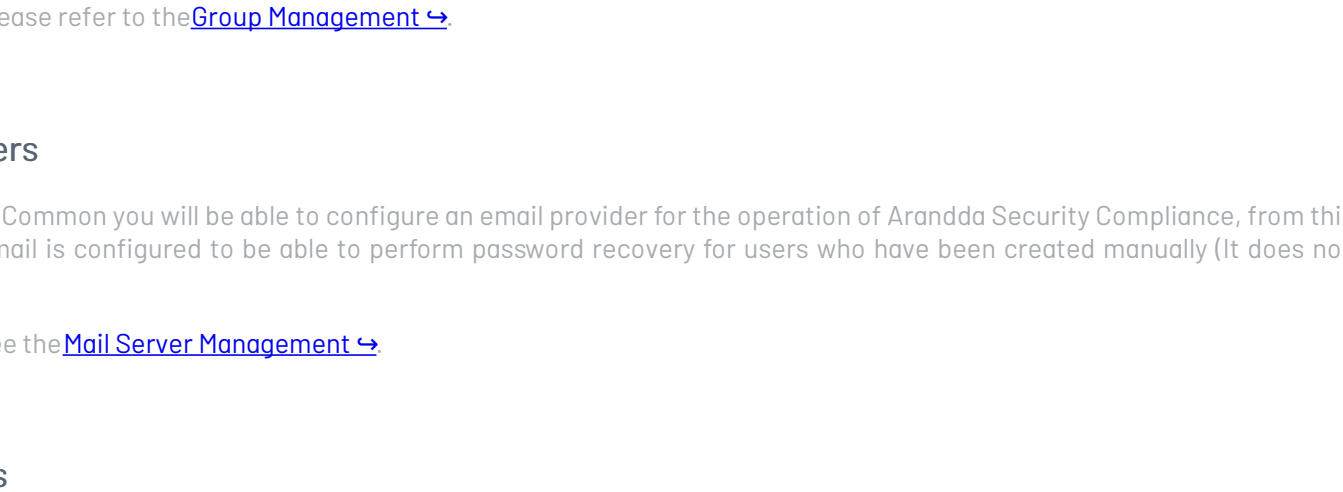
6.To detach devices, in the Devices window, select a record and click the Unassociate Devices button.



General Settings

General Settings

The general administrator from the ASEC Web console will be able to configure the following transversal modules:



1. Users

In this module of Aranda Common you can configure the users in charge of managing security policies. These configurations can only be made by a user with an administrator role. Additionally, you can assign the roles Administrator and Specialist.

For more information, please refer to the User Management ↪.

2. User groups

In this module of Aranda Common you will be able to configure and manage user groups to perform the assignment of roles in a more efficient way.

For more information, please refer to the Group Management ↪.

3. Set Up Mail Servers

In this module of Aranda Common you will be able to configure an email provider for the operation of Arandda Security Compliance, from this server notifications will be sent to users. The email is configured to be able to perform password recovery for users who have been created manually (It does not apply to those who are imported).

For more information, see the Mail Server Management ↪.

3. Manage Licenses

Aranda Security Compliance allows you to manage the licenses acquired and associate them with the devices required to carry out an adequate management of security policies.

For more information, see the License Management ↪.

4. Directory Services

In this Aranda Common module, you can configure the directory services that can be used in the Aranda Security application, such as the lightweight directory access protocol **LDAP**, which allows you to configure the connection to other business directories or the directory service **Azure Active Directory**

For more information, see the Management Directory ↪ Services.

5. Configure Authentication Providers

In this Aranda Common module you can define the external authentication providers, which follow the SAML (Security Assertion Markup Language) standard to perform user authentication in the application.

For more information, see the Authentication Provider ↪ Management.