

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?

- <u>Aranda Security Compliance ASEC Getting Started Guide</u>
- 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.



• 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 <u>Define compliance policies</u>.

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.

🗱 🔐 Aranda Securi	ity Compliance	WB
Resumen	Políticas Resumen de políticas aplicadas a los dispositivos. Para crear una nueva política haga clic en el botón en la parte superior.	
Politicos	C Buscar	NUEVO
Uispositivos	C Política · Cumplimiento de la política · Dispositivos alcanzados · Fecha de creación	n 🗸 Descripción de la política
Vunerabiliadues	• •	4 am Prueba Filtro
	● F Filtr3 ● NO CUMPLE 18/06/2024 12:02:4	0 pm Filro 3
	• F2 Filtro 2 07/06/2024 1:32:48 07/06/2024 1:32:48	i pm Filtro 2
	FL Filtro 5 - Linux O NO CUMPLE 19/06/2024 5:08:58	pm Prueba Filro 5 - Linux
	□ • N <u>new1</u>	lam asd
	□ • N3 <u>New 3</u> O NO CUMPLE 28/12/2023 8:33:44	am asd
	• N4 <u>new 4</u> 2 8/12/2023 9:00:24	am asd
	● N5 new 5 O CUMPLE 28/12/2023 9:01:30	am asd
	• N6 <u>new 6</u> 29/12/2023 10:09:21	5 am asd
Onfiguración		Mostrando 1 al 20 de 67 registros

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:

w	Windows
L	Linux
M	MacOS

Política - Nueva Política Detalles y configuración de la política Nombre de la política Tlempo de monitoreo 🗎 X 🔺 NP Nueva Politica 1 Minutos Sistema operativo Linux Descripción Nueva Politica ESTADO Deshabilitado Criterios de políticas Seleccione uno o agregue criterio para la politica VPN Client \sim ۵ VPN VPN CLIENT El programa debe ser Seleccione un programa \sim

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.

The second second

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



and choose a program from the existing listing.

Google Chrome		_
El programa debe ser	🗌 Verificar instalación	
Google Chrome	~	
🗌 Validar versión mínima	🗌 Validar protección de antiphishing	
🗌 Validar navegador predeterminado		

P 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. <u>View validations by configuration criteria</u>

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





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

P 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.

🗱 📲 Aranda Security C	ompliance	w
Resumen	Politica - Politica Vulnerabilidad Detalles y configuración de la política	
Políticas	PV Nombre de la política Política Vulnerabilidad	Tlempo de monitoreo
Dispositivos	Sistema operativo Windows Descripción	
	Prueba de Política con Vulnerabilidad	ESTADO CIVO
	Criterios de políticas Grupos	
	Asocie grupos a las políticas Escriba el nombre del grupo que desea asociar	+
	Grupos asociados a las políticas	🔘 Desasociar
	C Grupo	Dispositivos del grupo
	GV Grupo Vulnerabilidad	P2 (2)
Orfiguración	<	1 > Mostrando 1 al 1 de 1 registros

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 th**(++)** 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

	Criterio	s de po	líticas	Grupos		
Asocie gruț	pos a las po	oliticas	grupo		+	
Gruposo	asociado	os a las	🗌 grupo 2			Desasociar
		Grupo	🖌 grupo 3			
0	NN	Nuevo	🗹 grupo 4			
			🗌 grupo 5	 		
	AA	Autom			Agregar	

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.

Criterios de po	olíticas	Grupos		
Asocie grupos a las politicas	Escriba el nombre del	grupo que desea asociar	+	
Grupos asociados a	las políticas			🖯 Desasociar
Grupo V			Dispositivos del grupo 💛	
GG Grupo1			₽ 2	

Delete Policies

12. To delete policies, log in to the Aranda Security console with administrator role, in the sectior**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**.

Aranda Secur	ity Compliance			<u>v</u>
Resumen	Políticas Resumen de políticas aplicadas a los dispositivo	os. Para crear una nueva política haga clic en el botón en la parte superior.		
😨 Politicas				
Dispositivos				
Vulaarabilidadaa	Política	Cumplimiento de la política \vee Dispositivos alcanzados \vee	Fecha de creación 🔗	Descripción de la política
	CN change name		30/05/2024 7:07:24 am	Prueba Filtro
	F <u>Filtr3</u>		18/06/2024 12:02:40 pm	Filro 3
	F2 Filtro 2		07/06/2024 1:32:48 pm	Filtro 2
	FL Filtro 5 - Linux		19/06/2024 5:06:58 pm	Prueba Filro 5 -Linux
	I I NI <u>new 1</u>		29/12/2023 8:30:02 am	asd
	□ • N3 <u>New 3</u>		29/12/2023 8:33:44 am	asd
	• N4 <u>new 4</u>		29/12/2023 9:00:24 am	asd
	• N5 <u>new 5</u>		29/12/2023 9:01:30 am	asd
	□ • N6 <u>new 6</u>		29/12/2023 10:09:25 am	asd
🛞 Configuración	Estado 🖸 • ACTIVO 🗋 • INACTIVO			Mostrando 1 al 20 de 67 registr

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

Mensaje de confirmación
Está seguro que desea eliminar las políticas?
RECUERDA: AL ACEPTAR se eliminará de manera permanente
Cancelar Aceptar

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**.

🗱 🚘 Arand	la Security	Com	pliance	9							WB
Resumen	٢	P	olíticas	s de polí	ticas aplicadas a los dis	positivos. Para crear una pueva polític	a haaa clic e	en el botón en la parte superior			
Politicas			2 Q B	luscar						NUEVO	ELIMINAR
Dispositivos					Política 🖂	Cumplimiento de la p	política 🗸	Dispositivos alcanzados 🛛 🗠	Fecha de creación 🔗	Descripción de la político	1
			•	NI	new policy FE 1		UMPLE		26/01/2024 9:55:56 am	asd	
			•	PA	Politica - ASEC	🕑 cut	MPLE	6	08/11/2023 10:46:10 am	Politica Basica	
			•	P4	Politica - Walter 4		UMPLE		23/11/2023 2:35:53 pm	prueba de políticas	
			•	P4	Politica 4		UMPLE		19/06/2024 2:29:33 pm	Politica	
			•	PA	Politica Agente		UMPLE		27/12/2023 12:17:01 pm	Testing Agent	
			•	Ρ	Politica Bug		UMPLE		18/10/2024 7:21:18 am	Politica Bug	
			•	PC	Politica Chrome		UMPLE		04/04/2024 9:50:22 am	Politica Chrome	
			•	PF	Politica Fecha		UMPLE		10/07/2024 10:02:19 am	Politica FEcha	
			•	PL	Politica LInux		UMPLE		04/01/2024 3:20:14 pm	Prueba Politica Linux	-
Ô Configuración		E	stado	•			I			Mostrando 1 al 20 d	de 67 registros

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.

E	1 € -	⊘∓		Policy (2)	.xlsx - Excel				Herramienta	de tab	ola			Walter Jose	ef Berdugo C	olon E	3 – Ø	×
Arcl	nivo In	icio Inse	rtar Diseño de pág	jina Fórmulas	Datos	Revisar	vista .	Ayuda	Diseñ	0	Ç ¿Qu	é desea hacer?					A. Compa	artir
Peg	■	Calibri N K S	• 11 • A		≫ ð	🦻 Ajustar text 🗄 Combinar y	o centrar	Gene	eral % 000 58	-\$,0	Formato condicional •	Dar formato como tabla *	Estilos de celda *	Insertar Eliminar Formato	∑ Autosur ↓ Rellenar ◆ Borrar ▼	ma • A - Z Ord filt	enar y Buscar y rar * seleccionar *	
Porta	papeles 🖪	i l	Fuente	G.	Alineac	ión		5	Número	Es		Estilos		Celdas		Edici	ón	^
A1		· : :	× √ f _x A	ctive														~
	А		в	с			D				Е	F		G		н	1	-
1	Active 💌	Complian	ceState 💌 Creatior	nDate 🔻	Descriptio	n				▼ De	vicesReach	ed 🔻 Id	Name	2	🔻 Plat	formId 🔻	PlatformName	
2	True	False	1/1/000	1 5:00:00 AM	TEST					4		69	001 b	ackup vm22	Win	dows	001 backup vm22	
3	True	False	6/29/20	23 4:33:49 PM	detalle							41	002 b	rowser vm 1	Win	dows	002 browser vm 1	
4	True	True	7/11/20	23 9:07:15 PM	Comodo fi	rewall				1		71	003 f	irewall vm3	Win	dows	003 firewall vm3	
5	True	False	7/11/20	23 8:56:32 PM						1		70	004 b	kp,browser,firewall vm4	Win	dows	004 bkp,browser,f	irev
6	True	False	7/26/20	23 4:40:25 PM								85	005 L	OCAL ANTIPISHING	Win	dows	005 LOCAL ANTIPIS	SHIP
7	True	False	10/9/20	23 12:00:00 AM	DETALLE							122	DEM	D ENTREGA	Win	dows	DEMO ENTREGA	
8	True	False	10/3/203	23 12:00:00 AM	DEMO TES	т				2		114	DEMO	D TEST	Win	dows	DEMO TEST	
9	True	False	7/5/202	3 7:19:11 PM	testDev					6		48	DEV I	DEVICES	Win	dows	DEV DEVICES	
10	True	False	1/4/2024	4 3:33:23 AM	OSDEV					10		134	MacO)SDev	Mac		MacOSDev	
11	True	False	10/30/20	023 9:09:34 PM	Política mí	nima de ver	ificación			1		130	Politi	ica - Walter 1	Win	dows	Politica - Walter 1	
12	True	False	11/15/20	023 1:24:37 PM	Prueba de	la hora al m	omento	de guar	dar la polític	а		132	Políti	ca 3	Win	dows	Política 3	
13	True	False	9/5/202	3 2:16:08 PM	FirewallEd	lgeChrome		-				111	Politi	ica BR	Win	dows	Politica BR	
14	True	False	4/4/2024	4 7:17:35 PM	Politica Ch	rome						140	Politi	ica Chrome	Win	dows	Politica Chrome	
15	True	False	10/30/20	023 7:11:37 PM	Política de	cumplimier	nto de W	/alter				129	Políti	ca de cumplimiento de W	alter Win	dows	Política de cumplir	mie
16	True	False	10/6/20	23 12:00:00 AM	detalle po	litica firewa	II					121	politi	ica firewall	Win	dows	politica firewall	
17	True	True	10/10/2	023 12:00:00 AM	Descripcio	n				1		128	Politi	ica FW	Win	dows	Politica FW	
18	True	False	2/8/2024	4 8:04:56 PM	Políticas In	nágenes						137	Políti	ca Imagen	Win	dows	Política Imagen	
19	True	False	2/19/20	24 1:19:49 PM	test politio	ces user						138	Polit	ica Usuario	Linu	x	Politica Usuario	
20	True	False	10/3/20	23 12:00:00 AM	TEST					6		113	POLI	FICA VM AZURE	Win	dows	POLITICA VM AZUF	RE
21	True	False	6/24/20	24 3:23:34 PM	Prueba de	Politica con	Vulnera	bilidad		2		151	Politi	ica Vulnerabilidad	Win	dows	Politica Vulnerabil	lida
22	True	False	11/7/20	23 9:02:24 PM	prueba1							131	Politi	ica1	Win	dows	Politica1	
		Balliev	(1)															
		Policy	Ð									: •					-	
Listo																끤 -	+	100%

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.

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

Policies					
Devices	Q Search				NEW DEL
Vulnerabilities	P. Key Over lines	Policy Compliance 🔍	Devices reached \sim	Creation date 🗸	Description policy
		NON-COMPLIANT	2	01/01/0001 12:03:44 am	TEST
	COMPLIANT	NON-COMPLIANT		29/08/2023 11:33:49 am	detalle
	Windows Using	ONDN-COMPLIANT		11/07/2023 4:07:15 pm	Comodo firewall
	MacOS	O NON-COMPLIANT		11/07/2023 3:58:32 pm	
	Devices	NON-COMPLIANT		28/07/2023 11:40:25 am	
	Without devices	NON-COMPLIANT		08/10/20237:00:00 pm	DETALLE
	Apply filters (0)	NON-COMPLIANT	2	02/10/2023 7:00:00 pm	DEMO TEST
	DO <u>DEV DEVICES</u>	NON-COMPLIANT	5	05/07/2023 2:19:11 pm	testDev
		NON-COMPLIANT	9	03/01/2024 10:33:23 pm	OSDEV
	MacOSDev				
		NON-COMPLIANT	1	30/10/2023 4:09:34 pm	Politica minima de verifi
Jettings	H NocCODex Politica-Water1 Politica3 Status ACTIVE MACTIVE	NON-COMPLIANT		30/10/2023 4:09:34 pm 16/11/2023 8:24:37 am	Politica minima de verifi Prueba de la hora al mo Showing 1 to 20 of 28 m
Dettings	Image: Market Status Image: Market Status Image: Market Status Image: Market Status Image: Market Status Image: Market Status	NON-COMPLIANT		30/10/2023 4:09:34 pm 16/11/2023 8:24:37 am	Politica minima de verifi Prueba de la hora al ma Showing 1 to 20 of 29 m
Settings	ty Compliance	NON-COMPLIANT		30/10/2023 4:09:34 pm 16/11/2023 8:24:37 am	Politioa minima de verifi Prueba de la hora al mo Showing 1 to 20 of 28 m
Settings	ty Compliance Policies Support of colicies product to devices. To receive a page	NON-COMPLIANT NON-COMPLIANT		30/10/2023 4:00-34 pm 18/11/2023 8:24:37 am	Politica minima de verifi Prueba de la hora al mo Showing 1 to 20 of 29 m
Settings	H MacGBay Patrice - Water Patrice -	NON-COMPLIANT NON-COMPLIANT NON-COMPLIANT		30/10/2023 4:00-34 pm 18/11/2023 8:24:37 am	Politica minima de verifi Prueba de la hora al mo Showing 1 to 20 of 23 m
Dettings	ty Compliance Policies Summary of policies applied to devices. To create a na Summary of policies applied to devices. To create a na To create a na Compliance Summary of policies applied to devices. To create a na To create a na	w policy click the button at the top.		30/10/2023 4:00-34 pm 16/11/2023 8:24:37 am	Politica minima de verifi Prueba de la hora al mo Showing 1 to 20 of 23 m Showing 1 to 20 of 23 m
Eettings	ty Compliance Compliance Constant of policies applied to devices. To create a new Constant of policies applied to devices. To create a new Compliance X Operating system platform X	NON-COMPLIANT NON-COMPLIANT w policy click the button at the top.		30/10/2023 4:00-34 pm 18/11/2023 8:24:37 am	Politica minima de verif Prueba de la hora at ma Ohowing 1 to 20 of 23 m New Example Survey Remove fitters 2
Dettings Dettings Caranda Secur Dummary Devices Jevices Vulnerobilities	Image: Participation	NON-COMPLIANT NON-COMPLIANT NON-COMPLIANT	I I	30/10/2023 4:00:34 pm 19/11/2023 8:24:37 cm	Politica minima de vertif Prueba de la hara al ma Showing 1 to 20 of 28 m Showing 1 to 20 of 28 m United Showing 1 to 20 of 28 m Description policy
Bettings Bettings Bummary Policies Devices Vulnerabilities		NON-COMPLIANT NON-COMPLIANT NON-COMPLIANT NON-COMPLIANT	Image: Contract of the second of the seco	30/10/2023 4:08:34 pm 18/11/2023 8:24:37 am Creation date ~ 24/08/2024 10:23:34 am	Politica minima de verifi Prueba de la hora al ma Showing 1 to 20 of 25 m Network 1 to 20 of 25 m Remove Tutera 2 Description policy Prueba de Politica con Y
Settings		NON-COMPLIANT NON-COMPLIANT NON-COMPLIANT NON-COMPLIANT Policy click the button at the top. Policy Compliance COMPLIANT COMPLIANT COMPLIANT	Image: Control of the second of the secon	30/10/2023 4:04:34 pm 18/11/2023 8:24:37 cm	Politica minima de verifi Prueba de la hora al ma Showing 1 to 20 of 28 m Showing 1 to 20 of 28 m El control de la bora al ma Remove filters 2 Description policy Prueba de Politica con V

O Settings	Settings			Showing I to 3 of 3 m
----------------	----------	--	--	-----------------------

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:



P 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 <u>How to View the List of Security Applications</u>.

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 vo defau	alidated on the workstation if the Microsoft Edge is set as It.	



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 enab	validated that the software Kaspersky Endpoint Security have real-time protection oled.



3. Validate Execution Status

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



le 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:





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 Valida enabl	ate that the software Windows Firewall have FIREWALL protection ed.



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.		If the software has Anti-Phishing protection enabled.	
NOT COMPLIANT		If the software does NOT have Anti-Pishing protection enabled or if the software installed.	e is NOT
Example	Valida active	ate that the software Google Chrome have Anti-Phishing protection e.	

BROWSER Google Chrome	Ē
Establecer versión minima	Validar protección de antiphishing
🗌 Validar navegador predeterminado	🗌 Validar instalación
El programa debe ser	
Google Chrome	

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 Valido 1.0.1	ate that the version of AVG internet security installed on the workstation is greater than or equal to version

<u>ش</u>
Validar estado de protección en tiempo real
Validar protección de antiphishing
El programa debe ser
AVG Internet Security

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

🖌 Establecer versión minima	Validar protección de antiphishing
1.0.1	
Requerido	Ulidar instalación
Si ingresa una versión válida, se verifica que la versión instalada en el equipo sea igual o mayor, de lo contrario se verifica que la versión sea la misma.	
Validar navegador predeterminado	

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 .	ates that the backup status of the software can be obtained Avast Business Cloud Backup

BACKUP Avast Business Cloud Backup			<u>ش</u>
El programa debe ser			
Avast Business Cloud Backup	~		
🗌 Verificar instalación		✓ Obtener Estado de Copia de Seguridad	

View Security Application Listing

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

- 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.

eleccione el sistema operativo Windows				
Q google				
Nombre del producto	Nombre del proveedor	Nombre de la firma	Versión del producto	í
Google Apps Sync for Microsoft Outlook	Google Inc.	Google Apps Sync for Microsoft Outlook	3.5.385.1020	
Google Chrome	Google Inc.	Google Chrome	110.0.5481.104	
Google Chrome	Google Inc.	Google Chrome	110.0.5481.178	
Google Chrome	Google Inc.	Google Chrome	111.0.5563.111	
Google Chrome	Google Inc.	Google Chrome	111.0.5563.147	
Google Chrome	Google Inc.	Google Chrome	111.0.5563.65	
Google Chrome	Google Inc.	Google Chrome	112.0.5615.138	

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 <u>Validations or methods</u> that it endures.

eleccione el sistema operativo Windows			
		CC Google Chrome	Lista de métodos
Q google		GC Google Chirome	
Nombre del producto	Nombre del proveedor	Nombre del produc Google Chrome	 DetectProduct Ejecutor
Google Apps Sync for Microsoft Outlook	Google Inc.	Nombre del provee Google Inc.	 Establecer versión mínima Validar navegador predeterminado
Google Chrome	Google Inc.	Versión del produc 110.0.5481.178	Validar protección de antiphishing
Google Chrome	Google Inc.	Nombre de la firma: Google Chrome	
Google Chrome	Google Inc.	Categorias	
Google Chrome	Google Inc.	🚱 ANTIPHISHING	
Google Chrome	Google Inc.	BROWSER	
Google Chrome	Google Inc.		

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 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.

	-	
	ANTIPHISHING	
С	riterio	n

anline security and privacy. Examples include McAfee WebAdvisor and K7SecureWeb. Description

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

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.



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 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.

0
ENDPOINT

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 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

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 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.





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 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.



Description 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.

Aranda		
Todo Aplicaciones Documentos	Web M	ás ▼ ···· ×
Mejor coincidencia		
Windows PowerShell Aplicación		\geq
Aplicaciones		Windows PowerShell
Fotos	>	Aplicación
Windows PowerShell ISE	>	
Windows Media Player	>	다 Abrir
Configuración		😕 Ejecutar como administrador
Configuración de Windows Update	>	🖉 Ejecutar ISE como administrador
C Buscar actualizaciones	>	Windows PowerShell ISE
Seguridad de Windows	>	
Buscar en el trabajo y en Internet		
vindo - Ver resultados del trabajo y de Internet	>	
P windows 11	>	
, ∕⊂ windows 10	>	

2. The command copied from the screen <u>Deploy Agent</u> 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.

😕 Administrador: Windows PowerShell	-		×
indows PowerShell opyright (C) Microsoft Corporation. Todos los derechos reservados.			^
rueba la nueva tecnología PowerShell multiplataforma https://aka.ms/pscore6			
S C:\Windows\system32> \$installerPath="\$Env:ProgramData\Aranda"; \$installerFile="\$installerPath\setup.exe"; if (-not erPath)){ New-Item \$installerPath -ItemType Directory; }Invoke-WebRequest -Uri 'https://download.arandasoft.com/aes/a tFile \$installerFile; & cmd.exe /c "\$installerFile /S /V`"/qn APIURL=https://releaseqa3.arandasoft.com"" S C:\Windows\system32>	(Test-F agent/se	'ath \$ir tup.exe	stal ' -O

ASEC Agent Deployment by Domain Policy

Create Execution Files

1. After copying the ASEC agent execution command, during the <u>Agent Deployment</u> 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.

🔐 C:\Users\luis.orjuela\Downloads\ArandaTest\runAgent.bat - Notepad++	-	٥	\times
<u>A</u> rchivo <u>E</u> ditar <u>B</u> uscar <u>V</u> ista <u>C</u> odificación Lenguaje C <u>o</u> nfiguración <u>H</u> erramientas <u>M</u> acro Ejecutar Complementos Pestañas <u>?</u>		+	• ×
🔚 nso_ara_proceso_comercial_suitelet js 🔀 🔚 nso_ara_proceso_comercial_userevent js 🗵 🔚 nso_ara_prc 🗵 🔚 nso_ara_valdar_tasa_cambio_userevents 🗵 🔚 nno	Agent bat	×	• •
1 PowerShell.exe -Command "\\Domain\netlogon\ASC\agente.psl"			
hand the first second sec	CRUD	LITE O	INC
satch file length : 58 lines : 1 Windows (CKLF)	UIF-8	INS

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.

	1						
Administración de directivas de grupo	Objetos de directiva de grupo en INTERSEQ.LOCAL						
▲ Bosque: INTERSEQLOCAL ▼ ■ Domininios ▼ ■ Domininios ▼ ■ Domininios ▼ ■ Domininios > ■ INTERSEQLOCAL ■ Default Domain Policy > ■ Domain Controllers > ■ Domain Controllers > ■ Domain Controllers > ■ Domain Controllers > ■ Objector da Graetina da nume ■ Act ■ Act ■ Act ■ Act ■ Def ■ Objector da fractina desde aquí ○ Dic ■ Objector da f	Contenido Delegación Nombre Actualizaciones WSUS Aranda Walpaper Defauit Domain Contro Defauit Domain Policy Log Off Terminal Server Old - Agente V8 Old - Agente V8 Old - Agente V8 Old - Agente V8 Old - Agente Rolicy Old - Instal_ADM Old - Instal_ADM Old - Instal_ADM Old - Instal_ADM	Estado de GPO Habitado Habitado Habitado Habitado Habitado Todos los valores de configuración deshabitados Todos los valores de configuración deshabitados	Filtre WMI Ninguno Ninguno Ninguno Ninguno Ninguno Ninguno Ninguno Ninguno Ninguno Ninguno	Modificado 6/10/2016 5:34:56 p. m. 9/05/2023 1:9:26 p. m. 1/07/2022 7:23:38 a. m. 9/05/2023 1:28:54 p. m. 4/08/2021 11:40:32 a. m. 26/12/2016 2:27:46 p. m. 26/12/2016 2:27:46 p. m. 27/02/2023 1:18:12 p. m. 27/02/2023 1:18:12 p. m. 27/02/2019 3:16:28 p. m. 21/01/2021 3:16:38 p. m. 1/07/2022 7:19:44 a. m.	Propietario Domain Admine (INTERSEQI-Domain Admin Domain Admine (INTERSEQI-Domain Admin		

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

V B Dominios					
V III INTERSEQLOCAL		Ampto Detalles Configuración Delegación Esta	0		
		Vinculos			
Default Domain Policy		Mostrar vínculos en esta ubicación: INTERSEQ.LO	AL		~
> 🛋 Aranda		Los siguientes sitios, dominios y unidades organizativas	están vinculados a este GPO:		
> 🛋 Domain Controllers		10.0			
> Microsoft Exchange Security Gro	ps	Ubicación	xigido Vinculo habilitado	Puta	
> 🛋 Prueba					
Objetos de directiva de grupo					
Actualizaciones WSUS					
Aranda Wallpaper					
ASC EANN					
A CINE					
Estado de GPO	,				
Hacer copia de seg	dad				
OI Restaurar desde cor	de seguridad				
I OI Importar configura					
I OI Guardas informa					
OI Guardar Informe		Filtrado de securidad			
Ol Ver	>	La configuración en este GPO solo se puede aplicar a	s grupos, usuarios y equipos s	siguientes:	
Pr Nueva ventana desa	aquí	Nombre			
> 🚔 Filtros Copiar		& Authenticated Users			
> 😭 GPO c Eliminar					
> Sitios Cambiar nombre					
Modelado de Actualizar					
Resultados d					
Ayuda					

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.



Editor de administración de directivas de grupo			-	×
<u>A</u> rchivo A <u>c</u> ción <u>V</u> er Ay <u>u</u> da				
🕨 🔿 🚾 🖾 📾 🛛 🖬				
 Directiva ASC [DOMAIN.INTERSEQ.LOCAL] Configuración del equipo Configuración de software Configuración de Windows Directiva de resolución de nombres Scripts (inicio o apagado) Empresoras implementadas Configuración de seguridad QoS basada en directiva Preferencias Configuración de usuario Directivas Preferencias Preferencias 	Scripts (inicio o apagado) Inicio Mostrar propiedades. Descripción: Contiene scripts de inicio de equipo.	Nombre inicio Apagado		
< > >	Extendido Estándar			

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

Propiedades de Inicio	?	\times
Scripts Scripts de PowerShell		
Inicio scripts para ASC		
Nombre Parámetros	<u>A</u> mba A <u>b</u> ajo	
	Agr <u>e</u> gar Edi <u>t</u> ar.	r
	Q <u>u</u> itar	r
Para mostrar los scripts guardados en este objeto de direct de grupo, presione el botón de abajo. <u>M</u> ostrar archivos	iva	
Aceptar Cancelar	Apl	i <u>c</u> ar

🛛 📘 🛨		A	dministrar	Startup				– 🗆 ×
Archivo Inicio	Compartir Vista	Herramie	ntas de aplicació	n				^ (
Anclar al acceso rápido	Pegar Pegar actor	ita de acceso ceso directo	Mover a •	¥ Eliminar ▼ ■ Cambiar nombre rganizar	Nueva carpeta Nuevo	Propiedades Abrir	•	Seleccionar todo No seleccionar ninguno Invertir selección Seleccionar
← → ~ ↑	« Machine > Scri	ipts > Startup	0			5 v	,○ B	uscar en Startup
Dropbox	^	Nombre	^	Fec	ha de modificac	ión Tipo		Tamaño
📀 OneDrive - Ara	nda Software	💿 runAgent		24/0	08/2023 8:17 a. n	n. Archiv	o por lo	otes 1 KB
💻 Este equipo								





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**.

Nombre del script:		
run Agent bat	Examin	ar
Parámetros de script:		
Parâmetros de script:		
Parámetros de script:		

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 ink an existing GPO.

Administración de directivas de grupo A Bosque: INTERSEQLOCAL Sogue: INTERSEQUE:		ASC Ambito D	Detalles Configuración Delegación Estado		
		AS0 Dato Gene	C s recopilados el: 24/08/2023 8:19:56 a.m. sral Netalles		mostrar todo ocutar
v 🎲 Objetc	Crear un GPO en este dominio y vincularlo aquí	V	linculos		CLOBER .
J Ac	Vincular un GPO existente				mostar
Ar.	Bloquear herencia	B	itrado de seguridad		mostrar
AS Az	Actualización de directiva de grupo	D	lelegación		
De De	Asistente para modelado de directivas de grupo Nueva unidad organizativa Nueva ventana desde aquí		iguración del equipo (habilitada)		etostar ocutar
Oh Oh			ectivas		ooter
I Ok	Eliminar	0	onfiguración de Windows		ooter
- Ok	Cambiar nombre		Scripts		ocultar
Oh	Actualizar		Inicio		ocultar
Pri	Propiedades		For this GPO, Script order: No configurado		
> 📑 Filtros	Ayuda		Nombre	Parámetros	
> 📑 GPO dewe	n n		run Agent bat		
Resultados de dire	ectivas de grupo ectivas de grupo	Confi	iguración del usuario (habilitada)		on dar
			Configuración no definida.		

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

 \triangleright 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.

🗱 Aranda Security	Compliance		wc
Resumen Politicas Dispositivos Vulnerabilidades	Resumen D5 de Julio de 2024 7:53 a.m. AGENTE INSTALADOS 55 DISPOSITIVOS 53 CON POLÍTICA (* 2 SIN POLÍTICA	CUMPLIMENTO DE POLÍTICA POR DISPOSITIVOS 53 DISPOSITIVOS 7 CUMPLEN 1 100000000000000000000000000000000000	ESTADO DE POLÍTICAS 27 activas 3 CUMPLEN TRADUCTOR
	TOP ESTADO DE POLÍTICAS POR GRUPOS	Cantidad da diagonitiuna	Percentrio de sumplimiente %
	prueba linux MACOSDEV	14 Dispositivos	• 7%
	DevGroup VMAZURE	6 Dispositivos 6 Dispositivos	16%
Configuración	<u>Grupo Release</u>	4 Dispositivos	0%

\bowtie 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.

000 000 000	Aranda Security Comp	pliance							wc
	K O5 de Julio de 2024 7:53 a.	AGENTE INSTALADOS 55 DISPOSITIVOS 53 CON POLITICA	2 SIN POLLITICA	CUMPLIMENTO D DISPOSITIVOS 53 DISPOSITIVO 7 CUMPLEN	E POLÍTICA POR S ↑ 46 INCUMPLEN	ESTADO DE PO 27 activas 3 cumplen	DLÍTICAS	24 INCOMPLEN ¥	
	TOP ESTADO DE POLÍTI	ICAS POR GRUPOS)						
	Grupo		Can	tidad de dispositivos		Porcentaje	de cump	limiento %	
	<u>prueba linux</u>		1	14 Dispositivos					7%
	MACOSDEV			10 Dispositivos					10%
	DevGroup			6 Dispositivos					16%
	VMAZURE			6 Dispositivos					0%
Ô	<u>Grupo Release</u>			4 Dispositivos					0%

Dispositivos - DevGroup				×
Q Buscar	NIVEL D	DE CUMPLIMIENTO DE LA POLÍTICA EN EL GRU	JPO 6%	REMEDIACIÓN
Dispositivo \vee	Sistema operativo 🛛 🗸	IP 🗸	Fecha de ejecución	Acción \vee
BG-D-JPEDRAZA01	Microsoft Windows 10 Pro	192.168.224.1; 192.168.1	05/07/2024 7:42:15 am	REMEDIACIÓN
BG-D-WPENA01	Microsoft Windows 10 Pro	192.168.0.147; fe80::fd26		REMEDIACIÓN
DESKTOP-CBTU791	Microsoft Windows 11 En	172.17.48.1; 192.168.50.15	28/12/2023 3:20:28 am	REMEDIACIÓN
<u>JCTREJOSI</u>	Microsoft Windows 11 Ho	192.168.56.1; 192.168.1.5;	24/04/2024 8:11:47 pm	REMEDIACIÓN
LAPTOP-RIKFNOA1	Microsoft Windows 10 Pro	192.168.56.1; 192.168.0.9		REMEDIACIÓN
• <u>MIGUEL-PC</u>	Microsoft Windows 10 Pro	192.168.1.6; fe80::fee9:2		REMEDIACIÓN
ESTADO OCUMPLEN O INCU	JMPLEN 🔲 NO APLICADO	< 1	>	Mostrando 1 al 6 de 6 registros

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.

Política - Política-Release Detalles y configuración de la política		
P Nombre de la política Política-Release Sistema operativo Windows	Tiempo de monitoreo	₿ × ^
Descripción Pruebas Release	ESTADO CON	
Criterios de políticas Grupos Asocie grupos a las políticas Escriba el nombre del grupo que desea asociar	+	
Grupos asociados a las políticas) Desasociar
Grupo V	Dispositivos del grupo 🛛 🗠	
CR Grupo Release	두 🕢	
		Mostrando 1 al 1 de 1 registros

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.

Buscor 25% <th <t<="" <th="" th=""><th></th><th></th><th>NIVEL DE CUMPLIMIENTO DE LA POLÍTICA EN E</th><th>L GRUPO</th><th></th></th>	<th></th> <th></th> <th>NIVEL DE CUMPLIMIENTO DE LA POLÍTICA EN E</th> <th>L GRUPO</th> <th></th>			NIVEL DE CUMPLIMIENTO DE LA POLÍTICA EN E	L GRUPO	
Dispositivo Sistema operativo IP Fecha de ejecución Acción IZ2 Red Hat Enterprise Linux 172.27.99.253; fe80::215 © REMEDIACIÓN B6-D-BCARBON001 Microsoft Windows 11 Pro 192.168.0.62; 172.17.176.1 06/02/2024 2:27.03 pm © REMEDIACIÓN B6-D-WEERDUS001 Microsoft Windows 10 Pro 192.168.56.1; 192.168.1.13 © REMEDIACIÓN	Buscar			25%	🔮 REMEDIACIÓN 🖓 EXPO	
Instrume Red Hat Enterprise Linux 172.27.99.253 ; fe80::215 Image: Red Hat Enterprise Linux	Dispositivo 🗸	Sistema operativo 🛛 🗸	IP V	Fecha de ejecución	Acción \vee	
BGE-D-BGARBON001 Microsoft Windows 11 Pro 192.188.0.62; 172.17.176.1 06/02/2024 2:27:03 pm C REMEDIACIÓN BGE-D-WBERDUG001 Microsoft Windows 10 Pro 192.188.56.1; 192.186.1.13 06/02/2024 2:27:03 pm C REMEDIACIÓN	<u>172</u>	Red Hat Enterprise Linux	172.27.99.253 ; fe80::215		REMEDIACIÓN	
BG-D-WBERDUG001 Microsoft Windows 10 Pro 192.168.58.1; 192.168.1.13	BG-D-BCARBON001	Microsoft Windows 11 Pro	192.168.0.62 ; 172.17.176.1	06/02/2024 2:27:03 pm	REMEDIACIÓN	
	BG-D-WBERDUG001	Microsoft Windows 10 Pro	192.168.56.1; 192.168.1.13		REMEDIACIÓN	
MUBC-RELEASE2 Microsoft Windows 11 Pro 10.0.0.10; fe80::294d:48 Image: Comparison of the state of	WJBC-RELEASE2	Microsoft Windows 11 Pro	10.0.0.10; fe80::294d:48		V REMEDIACIÓN	

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.

Dispositivo 192	× Politica del dispositivo MacOSDev
Fecha de escaneo: 02/12/2024 08:11:29	Detalle política Esta política tiene los siguientes criterios:
IP:; 192.168.0.6; fe80::c6b:4ea3:3e8a:fe9f%5; fe80::9c92:32ff:feda:3ff3%10; fe80::33e7:ebe3:f5c:d378%11; fe80::31de:2477:c753:8213%12 DIspositivo; macOS Catalina	 Browser Safari DetectProduct Validar protección de antiphishing
Grupo Este dispositivo pertence al siguiente grupo MACOSDEV	Remote_control AnyDesk DetectProduct VER
Cambiar de grupo	

 \triangleright Note: In the device detail select the Change Group to modify the existing group association.

Asociar Grupos A continuación podrá seleccionar o verificar el grupo asociado	
Seleccione un grupo Este dispositivo pertenece al siguiente grupo:	
MACOSDEV Usuarios del grupo: 1 usuarios	

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.

Dispositivos - Grupo Demo			🔁 Acciones de remediación	Seleccionar todo		×
Q Buscar		NIVEL DE CUMPLIMIENT	CC Google Chrome	Z Ejecutar		
Dispositivo \vee	Sistema operativo 🛛 🗸	IP 🗸		SetAntiphisingState		
BG-D-WBERDUG001	Microsoft Windows 10 Pro	192.168.56.1; 192				
LAPTOP-0J5MVA0B	Microsoft Windows 11 Ho	192.168.1.7 ; fe80				
WJBC0A	Microsoft Windows 10 Pro	10.0.0.4 ; fe80::4				
ESTADO LA POLÍTICA	FALLIDO NO APLICADO				CANCELAR ENV	IAR

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

P 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.

Acciones de remediación	Seleccionar todo	×
GC Google Chrome	Ejecutar Definir estado del antiphishing	Î
KS Kaspersky Internet Security	 Ejecutar Actualizar configuración Activar protección en tiempo real Escaneo Activar firewall Contraseña 	

▷ **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.

000 000 000	Aranda Security Compliance							
E I	Resumen	٢	Administrador de dispositivos Listado de tados los dispositivos. Puede cambiar el arupo del dispositivo dando cilo sobre el nombre del dispositivo.					
0	Politicas		R Q Buscor	ELIMINAR				
_			Q Buscar	W ELIMINAR				

	🗆 🗸 Dispositivo 🗸	Sistema operativo 🖂	Vulnerabilidades	Versión del agente 🔗	IP V	Último reporte 🗸 📩
Vulnerabiliadaes	• 1	Microsoft Windows 11 Pro	IN ESCANEAR	0.0.0.205	192.168.1.16 ; 172.30.128.1	10/10/2024 3:01:55 pm
	BG-D-BCARBON001	Microsoft Windows 11 Pro	🕏 2 🕏 29 😎 24	0.0.0.205	192.168.1.16 ; 172.30.128.1	10/10/2024 3:01:55 pm
	BG-D-WBERDUG001	Microsoft Windows 11 Pro	😎 16 😎 9 😎 1	9.4.2.1	192.168.1.4 ; 172.23.192.1	31/10/2024 8:09:01 am
	• <u>D2</u>	Microsoft Windows 11 Pro	SIN ESCANEAR	0.0.0.205	192.168.1.16 ; 172.30.128.1	10/10/2024 3:01:55 pm
	• <u>D3</u>	Microsoft Windows 11 Pro	SIN ESCANEAR	0.0.0.205	192.168.1.16 ; 172.30.128.1	10/10/2024 3:01:55 pm
	• <u>D4</u>	Ubuntu 23.10	SIN ESCANEAR	0.0.0.205	192.168.1.16 ; 172.30.128.1	10/10/2024 3:01:55 pm
	• <u>D5</u>	Ubuntu 23.10	SIN ESCANEAR	0.0.0.205	192.168.1.16 ; 172.30.128.1	10/10/2024 3:01:55 pm
	LinuxUbuntu	Ubuntu 20.04.6 LTS	SIN ESCANEAR	9.4.2.1	10.0.0.7; fe80::6245:bdf	
	LinuxUbuntu	Ubuntu 20.04.6 LTS	SIN ESCANEAR	9.4.2.1	10.0.0.7; fe80::6245:bdf	
Orfiguración	Cumplimiento de la OND APLICADO política OCUMPLEN	• NO CUMPLEN	II < 1 ∶			Mostrando 1 al 12 de 12 registros

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.

oliticas	Q Buscar					I EL
spositivos	Filtrar por Vulnerabilidad	ma operativo 🛛 🗸	Vulnerabilidades	Versión del agente 🔗	IP V	Último reporte 🔗 🗸
nerabilidades	Seleccione los CVEs 🗸 🗸	soft Windows 11 Pro	IN ESCANEAR	0.0.0.205	192.168.1.16 ; 172.30.128.1	10/10/2024 3:01:55 pm
	Plataforma del sistema operativo	soft Windows 11 Pro	🛡 2 🔍 29 🔍 24	0.0.0.205	192.168.1.16 ; 172.30.128.1	10/10/2024 3:01:55 pm
	Linux MacOS	soft Windows 11 Pro	IN ESCANEAR	0.0.0.205	192.168.1.16 ; 172.30.128.1	10/10/2024 3:01:55 pm
	Estado de la vulnerabilidad	soft Windows 11 Pro	SIN ESCANEAR	0.0.0.205	192.168.1.16 ; 172.30.128.1	10/10/2024 3:01:55 pm
	Sin escanear	tu 23.10	SIN ESCANEAR	0.0.0.205	192.168.1.16 ; 172.30.128.1	10/10/2024 3:01:55 pm
	Baja Mederada	tu 23.10	SIN ESCANEAR	0.0.0.205	192.168.1.16 ; 172.30.128.1	10/10/2024 3:01:55 pm

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.

Q						
	Dispositivo \vee	Sistema operativo 🛛 🗸	Vulnerabilidades	Versión del agente 💎	IP \vee	Último reporte 💚
	<u>43</u>	macOS Sonoma	♥1 ♥5 ♥2		172.86.43.25;fe80::b3:f	
	BG-D-BCARBON001	Ubuntu 22.04.2 LTS	IN ESCANEAR		172.22.211.90 ; fe80::215:	
	BG-D-BCARBON001	Ubuntu 22.04.2 LTS	IN ESCANEAR		172.22.211.90 ; fe80::215:	
	BG-D-BCARBON001	Ubuntu 22.04.4 LTS	IN ESCANEAR		172.22.211.90 ; fe80::215:	
•	BG-D-BCARBON001	Microsoft Windows 11 Pro	♥2 ♥6 ♥10	1.0.0.0	172.18.176.1 ; 192.168.1.16	26/08/2024 11:38:27 am
	<u>bg-d-fvasquezmac</u>	macOS Catalina	IN ESCANEAR		192.168.0.11 ; fe80::36:8a	
•	BG-D-WBERDUG001	Microsoft Windows 11 Pro	♥1	9.4.0.7	172.19.144.1; 192.168.1.6;	27/08/2024 9:15:43 am
•	DemoW11	Microsoft Windows 11 Pro	♥1 ♥9 ♥32 ♥1	9.4.0.7	10.0.0.6; fe80::8b85:483	

Remove Devices

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

000 000 000	👷 Aranda Secur	rity C	ompliance						WB
E	Resumen	>	Administra Listado de toc	idor de dispositivos dos los dispositivos. Puede cami	biar el grupo del dispositivo dar	ido clic sobre el nombre del dispos	itivo.		
Q L	Politicas								ELIMINAR
	Uispositivos Vulnerabilidades			Dispositivo \vee	Sistema operativo 🔗	Vulnerabilidades	Versión del agente 🔗	IP V	Último reporte \vee
				<u>43</u>	macOS Sonoma	♥ 1 ♥ 5 ♥ 2		172.86.43.25; fe80::b3:f	
				MacBookAir-Intel-FVFX	macOS Sonoma	Q 2 Q 5 Q 2		192.168.110.3; fe80::aed	
				• <u>ubuntu23-10-1-7-0</u>	Ubuntu 23.10	SIN ESCANEAR	0.0.0.131	172.17.51.214 ; fe80::215:	09/10/2024 8:02:35 am
Q	Configuración		Cumplimiento de la política	○ ● NO APLICADO ● NO		< 🕦 >	,		Mostrando 1 al 3 de 3 registros

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 th Export.

Resumen	< Adminis	strador de dispositivos	oiar el aruno del dispositivo dando clic s	obre el nombre del dispositivo.			
Politicas	T	Buscar					🗇 ELIMINAR 🔂 EXPORTAR
Vulnerabilidades		∨ Dispositivo ∨	Sistema operativo 🔍	Vulnerabilidades	Versión del agente 🖂	IP V	Último reporte 🛛 🗠
		1	Microsoft Windows 11 Pro	SIN ESCANEAR	0.0.0.205	192.168.1.16 ; 172.30.128.1	
		• <u>192</u>	macOS Catalina	265 < 250 < 8	9.4.2.2	192.168.0.8; fe80::1883:	12/12/2024 8:44:10 am
		BG-D-BCARBON001	Microsoft Windows 11 Pro	Q 2 Q 29 Q 24	0.0.205	192.168.1.16 ; 172.30.128.1	
		<u>D2</u>	Microsoft Windows 11 Pro	SIN ESCANEAR	0.0.205	192.168.1.16 ; 172.30.128.1	
		<u>D3</u>	Microsoft Windows 11 Pro	SIN ESCANEAR	0.0.205	192.168.1.16 ; 172.30.128.1	
		<u>JK</u>	Microsoft Windows 11 Pro	3 7	9.4.2.2	192.168.56.1; 192.168.20	
		<u>LinuxUbuntu</u>	Ubuntu 20.04.8 LTS	SIN ESCANEAR	9.4.2.1	10.0.0.7;fe80::8245:bdf	
		LinuxUbuntu	Ubuntu 20.04.8 LTS	SIN ESCANEAR	9.4.2.1	10.0.0.7; fe80::8245:bdf	
		<u>MACMINI-INTEL-ADM</u>	macOS Sonoma	0 13 0 9	9.4.2.2	192.168.1.91 ; 172.88.43.1	11/12/2024 1:57:18 pm
		• <u>ubuntu23-10-1-7-0</u>	Ubuntu 23.10	SIN ESCANEAR	9.4.2.2	172.28.102.140 ; fe80::21	11/12/2024 1:57:17 pm
		WALTER	Microsoft Windows 11 Ho	♥ 21 ♥ 43 ♥ 5	9.4.2.2	10.2.254.215 ; 192.168.1.7	03/12/2024 9:18:25 am

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.

	ਜ਼ • • ∂	~ .					Devices (5)	.xlsx - Excel		Walter Jos	ef Berdugo Colon 🛛 🖻	- 0	×
Ar	chivo Inicio	Insertar Di	seño de página	Fórmulas Dato	os Revisar Vista	a Ayuda	Acrobat	♀ ¿Qué desea hacer				P₄ Comp	artir
Pe	egar 💉 I	Calibri • N <u>K S</u> • III • Fuente	11 • A A • <u>></u> • <u>A</u> •	≡ = s>. ≡ ≡ ≡ • = •	ab C- General → \$ → % 0 Γ ₂ Núme	• • • • • • • • •	Formato condicional	Dar formato Estilos d como tabla × celda × Estilos	e Insertar • Eliminar • Formato • Celdas	∑ · A ↓ Ordenar y filtrar * seleccionar * Edición	Crear Crear un PDF y un PDF compartir vínculo Adobe Acrobat		^
G	18 🔻	: × 🗸	f_x										×
1	A AgentVersio	B Id	C Ip	D LastUpdated 💌	E Name 💌	F PlatformNa	ame 💌 Vuln	G erabilityCritical 💌 V	H /ulnerabilityImpor	l tan <mark>▼</mark> VulnerabilityLow ▼	J VulnerabilityModerate	ĸ	L *
2 3 4	0.0.0.205 9.4.2.2 0.0.0.205	4c4c4544-0036 d4239794-4ffe 4c4c4544-0036	- 192.168.1.16 - 192.168.0.8 ; - 192.168.1.16	; f <mark>. 12/12/2024 1:44:</mark> ;	1 192 BG-D-BCARBONO01	Windows MacOS Windows	0	6	5	8 0	50 24		
5 6 7	0.0.0.205 0.0.0.205 9.4.2.2	4c4c4544-0036 4c4c4544-0036 1bc3a50c-dad	5- 192.168.1.16 5- 192.168.1.16 a- 192.168.56.1	;	D2 D3 JK	Windows Windows Windows	6	3		0	7		
8 9	9.4.2.1 9.4.2.1	9dbcdc47-9e0 9dbcdc47-9e0	c- 10.0.0.7 ; fe80 c- 10.0.0.7 ; fe80	D D	LinuxUbuntu LinuxUbuntu	Linux Linux MacOS		4	2		6		
10 11 12	9.4.2.2 9.4.2.2 9.4.2.2	af6545ff-0b2d cf0703cc-f3d8	-(172.26.102.14 -(172.254.215)	; 12/11/2024 6:57: (12/11/2024 6:57: ; 12/3/2024 2:18:2	ubuntu23-10-1-7-0 WALTER	Linux Windows	0	2	1	5	43		
13 14 15													
16 17													
18 19 20													
21 22													
List	:0	Devices (+)								▦ ▣ ▣ -	+	 100%

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

🗱 Aranda Securit	y Compliance				WB
Resumen	Resumen de vulnerabilidades por estado				
Politicas					
Dispositivos	VULNERABILIDADES	VULNERABILIDADES	VULNERABILIDADES MODERADAS	VULNERABILIDADES BAJAS	
🖄 Vulnerabilidades	2	115	115	14	
	R Buscar				
	Vulnerabilidad $$	Aplicación \vee	Fabricante 🗸	Dispositivos 🗸	^
	<u>CVE-2007-4559</u>	Python 3.1184-bit	Python Software Founda	1	
	• <u>CVE-2019-17067</u>	PuTTY (x84)	PuTTY	1	
	• <u>CVE-2019-17068</u>	PuTTY (x84)	PuTTY	1	
	<u>CVE-2019-17089</u>	PuTTY (x84)	PuTTY	1	
	<u>CVE-2019-9894</u>	PuTTY (x84)	PuTTY	1	
	• <u>CVE-2019-9895</u>	PuTTY (x84)	PuTTY	1	
	• <u>CVE-2019-8898</u>	PuTTY(x64)	PuTTY	1	
	<u>CVE-2019-9897</u>	PuTTY (x84)	PuTTY	1	
Onfiguración	Severidad • CRITICA • MPORTANTE • MODERADA •	• BAJA	7 > H	Mostrando 1 al 2	:0 de 127 registros

P 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.

Vulnerabilidad: CVE-20 Fecha última actualizaci Fecha de publicación: 20	022-32868 ón: v/09/2022			×
Descripción: A logic issue was addressed with improved stat CVSS 3.0 CVSS 2	e management. This issue is fixed in Safari 18, iOS 18, iOS 15.7 .0	and iPadOS 15.7. A website may be able to tra	Severidad: 👽 BAJA indice: 39 Dispositivos con est	a vulnerabilidad: 🔚 1
Gravedad base: Puntuación base: Vector: Puntuación de impacto: Puntuación de explotabilidad:	MEDIO 43 CVS3:3:1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N 14 2:8	Vector de ataque: Complejidad del ataque: Privilegios requeridos: Alcance: Impacto en la confidencialidad: Impacto en la integridad: Impacto en la disponibilidad:	Red BAJA N/A Sin cambios BAJA N/A N/A	
Referencias a avisos, soluciones y herramie https://support.opole.com/en-us/H1213442 https://support.opole.com/en-us/H1213445 http://support.opole.com/en-us/H1213446 http://seclists.org/fulldisclosure/2022/0ct/39 http://seclists.org/fulldisclosure/2022/0ct/50	ntas:		Resolución: Update to version greater than or equal to 16.0	
Software afectados: Safari 15.8.1 (15813.3.9.1.18)				

Export Vulnerabilities

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

🗱 🕂 Aranda Securi	ty Compliance					WB
Resumen	Resumen de vulnerabi 13 de Diciembre de 2024 7:31	lidades por estado a. m.				
Politicas						
Dispositivos			VULNERABILIDADES IMPORTANTES	VULNERABILIDADES MODERADAS	VULNERABILIDADES BAJAS	
🖄 Vulnerabilidades		2	118	124	13	
	👔 🔍 Buscar					EXPORTAR
	Vulne	rabilidad 🖂	Aplicación \vee	Fabricante 💛	Dispositivos 🔗	A
	• <u>CVE-2</u>	007-4559	Python 3.10 84-bit	Python Software Founda	1	
	• <u>CVE-2</u>	007-4559	Python 3.11 84-bit	Python Software Founda	1	
	• <u>CVE-2</u>	015-20107	Python 3.10 84-bit	Python Software Founda	1	
	• <u>CVE-2</u>	019-17067	PuTTY (x84)	PuTTY	1	
	• <u>CVE-2</u>	019-17068	PuTTY (x84)	PuTTY	1	
	• <u>CVE-2</u>	019-17069	PuTTY (x84)	PuTTY	1	
	• <u>CVE-2</u>	019-9894	PuTTY (x84)	PuTTY	1	
	• <u>CVE-2</u>	019-9895	PuTTY (x84)	PuTTY	1	
O Configuración	Severidad CRITICA	IMPORTANTE MODERADA BA	AL AL	1 12 > ▶]	Mostrando I al :	20 de 257 registros

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.

ਜ਼ੁ ਙਾ ∂ਾ ∓	Vulnerabilitie	s (4).xlsx - Excel			Herramientas de tabla				Walter Jo	sef Berdu	go Colon	ħ	- 0	×
Archivo Inicio Insertar Diseño de página F	órmulas Da	tos Revisar V	sta Ayuda	Acrobat	Diseño	Ç ¿Qué des	ea hacer?						A Com	partir
$\begin{array}{c c} & & \\ & & \\ & & \\ & \\ Pegar \\ & \\ & \\ & \\ & \\ & \\ & \\ & \\ & \\ & \\ $	= = ≫. = = = = •	ab General Image: state S → %	000 ¢,00 000	Formato condicional	Dar formato Estilos de	Eliminar	· ∑ · · ♥ ·	A Z Ordenar y filtrar *	Buscar y seleccionar +	Crear un PDF	Crear un	P PDF y vínculo		
Portapapeles 🖙 Fuente 🕞	Alineación	ra Nú	mero r	ā l	Estilos	Celdas		Edicio	ón	A	dobe Acroba	at		^
A1 • : × ✓ f _x Cve														~
A B C	D	E	F	G	н	I.	J	к	L	м	N	0	Р	
1 Cve Cveld DevicesCount 💌	Productid	ProductName	Severity 💌	VendorId	VendorName 💌 Ve	ersion 💌								
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	Satari	Moderate	100011	Apple Inc.									
< → Vulnerabilities ↔														Þ
Listo										Ħ	E		-	+ 100%

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.

Nor Sist Ver: IP: 1	nbre del dispositivo: WALTE ema operativo: Microsoft Win sión del agente: 9.4.1.2 192.168.1.3 ; fe80::9234:638e:	ER ndows 11 Home Single La 88f6:dd2c%11	nguage			×
Resumen	Políticas	Grupos	Vulnerabilidades			
Politica Vulnerabilidad Este dispositivo tiene los	siguientes criterios:			Último escaneo;	28/8/2024, 4:23:55 p.m.	REMEDIACIÓN
NAVEGADOR WEE Microsoft Edge	APLICADO					

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.

000	Aranda Secu	Recurity Compilance	wc
	Summary Policies	Operating system: HiGrosoft Windows 11 Pro Agent Version: 9: 42.3 Agent Version: 9: 42.3 IP: 192.188.18.49; 172.17.240.1; 172.18.80.1; fe80::4aed.be01:5fb1:bf66%9; fe80::fd59:62d2:fl5d:478c%24; fe80::6a87.f649:58dd:66eo%29	×
0	Vulnerabilities	Summary Policies Groups Vulnerabilities Remediation Activity Groups This device belongs to the following group: This device belongs to the following group: This device belongs to the following group:	Change group
		Release 9.5.0 Windows	



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.

000	🔐 Aranda Secu	rity Compliance							wc
	Summary Policies		Device name: WALTER Operating system: Microsoft Win Agent Version: 8.4.2.3 Last report date: 12/27/2024 IP: 10.2.254.224 ; 192.168.1.18 ; fe	ndows 11 Home Single Languag 80: :cf7b:7c4b:f473:d482%6 ;	je fe80::9234:638e:88f6:dd2	lc%11			×
	Vulnerabilities	Summar	ry Policies	Groups	Vulnerabilities	Remediation Act	ivity		
		Q Search						Last so	an: 27/12/2024, 10:05:23 a.m.
			Vulnerability \vee	A	pplication \vee		Version \vee	Vendor \vee	A.
		•	<u>CVE-2007-4559</u>	Pj	ython 3.11 84-bit		3.11.3	Python Software Founda	
		•	CVE-2022-40682	Fo	ortiClient		7.0.7.0345	Fortinet Inc.	_
		•	CVE-2022-42470	Fo	ortiClient		7.0.7.0345	Fortinet Inc.	
		•	CVE-2022-43948	Fo	ortiClient		7.0.7.0345	Fortinet Inc.	_
		•	CVE-2023-24329	Pj	ython 3.11 64-bit		3.11.3	Python Software Founda	
		•	<u>CVE-2023-33304</u>	Fo	ortiClient		7.0.7.0345	Fortinet Inc.	
			CVE-2023-36038	Vi	isual Studio Communit		17.7.4	Microsoft Corporation	
		•	CVE-2023-38042	Vi	isual Studio Communit		17.7.4	Microsoft Corporation	
			CVE-2023-38049	Vi	isual Studio Communit		17.7.4	Microsoft Corporation	-
Ô	Settings	Ceverity 🔲 🖷	CRITICAL . IMPORTANT	IODERATE DU		I4 < 1 3	> M		Showing 1 to 20 of 43 records

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.

P 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.

000	Aranda Security	Complie	ance										WB
E R	esumen (Ð	Nombre del o Sistema ope Versión del o Fecha del últ IP; 172.26.96	dispositivo: BG-D-WBI rativo: Microsoft Window agente: 9.4.2.2 timo reporte2024-12-09T k1 ; 192.168.1.5 ; fe80::cda	ERDUGOO1 /s 11 Pro 13:00:44.380/ 2:c18a:99b9:e	4967 e713%70;fe8	0::bab8:5954:20ef;	a8ff%11				×
2 V	ulnerabilidades	72	Resumen Q Buscar		Políticas	Grupos		Vulnerabilidade	S	Actividad de reme	ediación		
		Ţ	Fecha de cr 20/11/2024 o	eación 🖂	Usuario 🗸	NIST	Acción 🗸		Aplicación V Google Chrome	Fe 20	cha última actualización 💚 m 2024 8:24:46 pm	Mensaje de error 🔗	•
		•	28/11/2024 3 28/11/2024 7	:25:09 pm :53:40 pm	APPLICATION ADMI	NIST	Run		Kaspersky Endpo	oint Sec 28	/11/2024 3:25:19 pm		
		•	28/11/2024 7	:53:40 pm			Run		Kaspersky Endpo	pint Sec 28	/11/2024 7:53:53 pm		
		•	28/11/2024 7 28/11/2024 7	:54:29 pm :54:29 pm			Run		Google Chrome Kaspersky Endpo	28. pint Sec 28.	/11/2024 7:54:38 pm /11/2024 7:54:38 pm		
		Sever	28/11/20247 ridad 🗌 🖲 🖲	Ejecutado	• Pendiente 🗌 • Error		Run	I4 < 1	Coorde Chrome	28	/11/2024 7·55·20 nm	Mostrando 1 al 20 de 2	▼ 7 registros
(\$) c	onfiguración												

Aranda Securit	y Compliance							WB
Resumen Politicas	Nombr Sistem Verslör Fecha (IP; 172.)	e del dispositivo; BG-D-V a operativo; Microsoft Win a del agente; 9.4.2.2 del último reporte2024-12-1 26.96.1; 192.168.1.5; fe80;::	VBERDUGO01 dows 11 Pro 09T13:00:44.380496 cda2:c18a:99b9:e713	7 5%70;fe80::bab8:5954:20ef:	a8ff%11			×
Vulnerabilidades	Resumen	Políticas	Grupos	Vulnerabilidade	s Actividad d	e remediación		
	Filtrar por		A	cción 🗸	Aplicación 🗸	Fecha última actualización 🔗	Mensaje de error 🛛 🗸	*
	Usuarios APPLICATION ADMINISTRAT	OR X	R	un nableRTP	Kaspersky Endpoint Sec Kaspersky Endpoint Sec	13/11/2024 2:33:58 pm 13/11/2024 2:33:58 pm		1
	Acciones de remediación		U	pdateDefinitions	Kaspersky Endpoint Sec	27/11/2024 2:19:14 pm		
	Run Scan SetAntiphishingState	1	R	un	Kaspersky Endpoint Sec Google Chrome	27/11/2024 2:19:14 pm 27/11/2024 2:19:14 pm		
		Aplicar filtros(0)	R	un	Kaspersky Endpoint Sec	27/11/2024 2:19:14 pm	Mastanda 1 al 20 da 22	-
	Severidad 🗌 🖲 Ejecutado	Pendiente 🗌 🖷 Err	ror	14 < 1	2 >		Mostrando 1 al 20 de 27	registros

Onfiguración



ASEC Configuration

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.

Regresar CONFIGURACIÓN Windows Linux MacOS
CONFIGURACIÓN Windows Linux MacOS
Deselerar agente
Agente Agente
Grupos de chimodra de la contractica de la contr
Configuración general Ejecute este comando en una terminal con privilegios de administrador. Copiar comando
2 Usuarios
💭 Grupos de usuario
Siga los pasos que se presentan a continuación para el despliegue del
Licenciamiento
Autenticación externa
📧 Servicios de directorio

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

	1 Seleccione un sistema operat	ivo	
	Windows	Linux	MacOS
Agente	sudo sh -c 'curl -o asecagent.pkg "ht -target / && asec-configuration -d h	tps://download.arandasoft.com/as ttps://releaseqa3.arandasoft.com'	ec/agent/setup.pkg* && installer -pkg as
··· ≻-	Ejecute este comando en un	a terminal con privilegios	de administrador.
los pasos que se presentan a inuación para el despliegue del ite.			

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 sectionConfiguration from the main menu, select theCompliance Groups. In the information view, you can view the list of available groups and sort the information by name of groups and devices.

🝀 📲 Aranda Security C	Compliar	ice						wc
✓ Regresar > Ø CONFIGURACIÓN	Grup Para g	os asoci estionar lo	i <mark>ados a las políticas</mark> Is grupos que se asocian en las políticas y	y crear nuevos grupos				
Desplegar agente	Q	Buscar]			NUEVO	ELIMINAR
Grupos de cumplimiento			Grupo 💛		Disp	ositivos del grupo 💛		<u>^</u>
Configuración general		OB	<u>001 backup</u>			₽ 2		
2 Usuarios		OB	002 browser			₽ 0		_
Servicios de email		OF	003 firewall			P2 🕦		
Licenciamiento		OF	004 bkp,browser, firewall			₽ ()		
Autenticación externa		AC	ASEC CHROME			聖 🕦		
Servicios de directorio		DG	<u>Default group</u>			₽ 🕕		
		D	DEMO			旦 🕕		
		DT	DEMO TESTS			聖 🕕		
			DauOraus			G 👝		•
				< 🚺	2 >		Mostrando I	l al 20 de 31 registros

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

P 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.

🝀 ୁନ୍ଦିର୍ Aranda Security	y Con	nplianc	e					wc
✓ Regresar Ø CONFIGURACIÓN		Grupos Para ges	s asocio tionar los	ados a las políticas s grupos que se asocian en las políticas y	r crear nuevos grupos			
Desplegar agente	l	Q, BI	uscar]		NUEVO	ELIMINAR
cumplimiento				Grupo \vee		Dispositivos del grupo 🔗		
Configuración general			OB	<u>001 backup</u>		<u>⊭</u> 2		
2 Usuarios			OB	002 browser				
Servicios de email			OF	<u>003 firewall</u>		12 1		
Licenciamiento			OF	<u>004 bkp,browser, firewall</u>		12 1		
Autenticación externa			AC	ASEC CHROME		12 1		
directorio			DG	<u>Default_group</u>				
		_	D	DEMO		<u>⊭</u> 0		
			DT	DEMO TESTS		Pa 🚺		
		r 1	0	DevOraus			Mastrondo	1 el 20 de 31 registras



Remove from Groups

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

	📲 Aranda Secur	ity Con	nplianc	e					wc
R ب ©	egresar CONFIGURACIÓN Desplegar agente) ا	Grupos Para ges Q Bi	s asoci stionar lo uscar	ados a las políticas s grupos que se asocian en las políticas :	y crear nuevos grupos			NUEVO 🗃 ELIMINAR
R	Grupos de cumplimiento				Grupo 🗸			Dispositivos del grupo 🛛 🗸	Â
Со	nfiguración general			OB	<u>001 backup</u>			陸 (2)	
2	Usuarios			OB	002 browser			두 🕕	
	Servicios de email			OF	003 firewall			🚘 🕕	
E	Licenciamiento			OF	004 bkp,browser, firewall			🖳 🚺	
	Autenticación externa			AC	ASEC CHROME			🖳 🕦	
	Servicios de directorio			DG	<u>Default group</u>			₽ 0	
				D	DEMO			₽ <u>0</u>	
				DT	DEMO TESTS			R 🔁 🕦	
					DauOraun			С. 👝	-
							< 🕦 2 >		Mostrando 1 al 20 de 31 registros

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

Mensaje de confirmación
Está seguro que desea eliminar los grupos?
RECUERDA: AL ACEPTAR se eliminará de manera permanente
Cancelar Aceptar

P 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**.

DD Nombre del grupo				a ×
Q Buscar			Sociar dispositivos	O DESASOCIAR DISPOSITIVO
Dispositivo V	Sistema operativo 🛛 🗸	IP V	Fecha de ejecución	
				Obsuine O to O of O

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.

Nombre del grupo				
) Buscar			ASOCIAR DISPOSITIVOS	O DESASOCIAR DISPOSITIVO
Dispositivo 🗸	Sistema operativo 🔗	IP 👳	Fecha de eje	cución
BG-D-JPEDRAZA01	Microsoft Windows 10 Pro	172.22.112.1 ; 192.168.1.53	23/10/2023 8	32:37 am
BG-D-WPENA01	Microsoft Windows 10 Pro	192.168.0.147; fe80::fd26	23/10/2023 4	23:15 pm
D е реактор-свтитя	Microsoft Windows 11 En	172.27.208.1 : 192.168.50	10/10/2023 11	42:25 pm
	Microsoft Windows 11 Ho	192.168.1.2 ; fe80::8527:3	23/10/2023 6	22:43 am

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 <u>User Management </u>

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 Active Directory

For more information, see the <u>Management Directory ↔ Services</u>.

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 <u>Authentication Provider \hookrightarrow Management</u>.