



Aranda Security Compliance

ASEC is a monitoring solution that allows companies to define compliance policies based on security standards.

Knowledge of the basic and transversal elements of ASEC gives the user context to later access the processes of configuration, management and monitoring of policies. The guidelines to be taken into account are:



1. Access

Learn how to log in to the client console and identify application usage requirements.

2. ASEC Operation

Learn how Aranda Security and its components work.

3. Environment

Identify the ASEC web interface with which you are going to interact in the different political management processes and get to know the different sections that make it up.

4. Roles

Learn about the roles defined in ASEC and their scope in the management of the different remote support processes.

Who is this guide for?

This guide is designed to familiarize the user with the elements necessary to interact with the functionality at a first level.

What is our documentation?

- [Aranda Security Compliance ASEC Starter Guide](#)
- [Aranda Security Compliance ASEC User Manual](#)

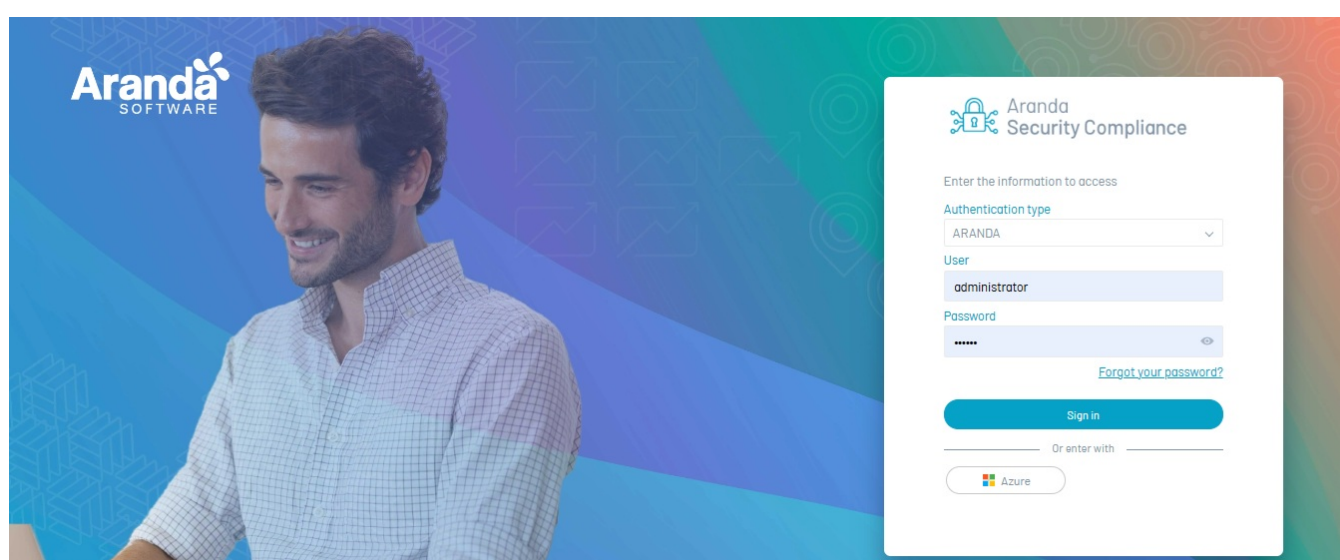
ASEC Access

ASEC Access

The authentication process to the ASEC web console will be executed according to the role defined by the organization to develop the different tasks of compliance policy management. The two instances of authentication are:

Login

1. Enter the url of the Aranda Security Compliance ASEC web console.
2. To log in to the ASEC application, enter the username and password assigned to you, taking into account the [Field Specifications](#).



Logout

1. When a user is in an active session within the web console and needs to end the session and exit the application, in the console header menu select the user icon and click **sign out**.



2. Once the session is closed, the user returns to the home screen and the user can enter the console again.

reCAPTCHA

1. To improve the safety in the use of the platform, it is possible to activate the reCAPTCHA functionality. This tool helps protect the site against unwanted or automated access.

If you want to enable this option, you can head over to the following link to learn more and set up reCAPTCHA [reCAPTCHA configuration](#)

Usage Requirement

Supported Browsers

The supported browsers are as follows:

Browser	Version
Edge	Version >= 88
Google Chrome	Version >= 97.0.4692.71
Mozilla	Version >= 96.0.2

Supported Windows versions

Windows	Version
Microsoft Windows	10 & 11
Microsoft Windows Server	2008 R2, 2012, 2012 R2, 2016, 2019

Supported Linux versions

Linux	Version
Ubuntu	16, 18, 20, 22, 23
Fedora	39
Red Hat Enterprise (Oracle)	7, 8, 9
OpenSUSE	15

Supported MacOS versions

MacOS	Version
Sonoma MacOS	14
MacOS Catalina	10
MacOS Monterey	12
MacOS Ventura	13

ASEC Required Ports

The following are the communication ports used by Aranda Security Compliance (ASEC). The network needs to be configured to allow communications over these ports.

Communication Ports

Agent		
Port	Protocol	Description
5671	TCP AMPQ	Connection to the Notification Hub.
443	TCP HTTPS	Connection to the application server.

Required Exclusions in Antivirus for Windows

Process	Description	Route
wa_3rd_party_host_32.exe	Utility for Delivery Methods	C:\Program Files\Aranda Software\Aranda Security Compliance Agent
wa_3rd_party_host_64.exe	Utility for Delivery Methods	C:\Program Files\Aranda Software\Aranda Security Compliance Agent
wa_3rd_party_host_ARM64.exe	Utility for Delivery Methods	C:\Program Files\Aranda Software\Aranda Security Compliance Agent
Aranda.EndpointSecurity.Agent.exe	Compliance Agent	C:\Program Files\Aranda Software\Aranda Security Compliance Agent

Required Permissions

It is required that the Aranda Windows User with whom the installation and deployment of Agents will be carried out has Installation permissions, preferably administrator of the corresponding machines.

A relay account is required for notifications that are sent via email.

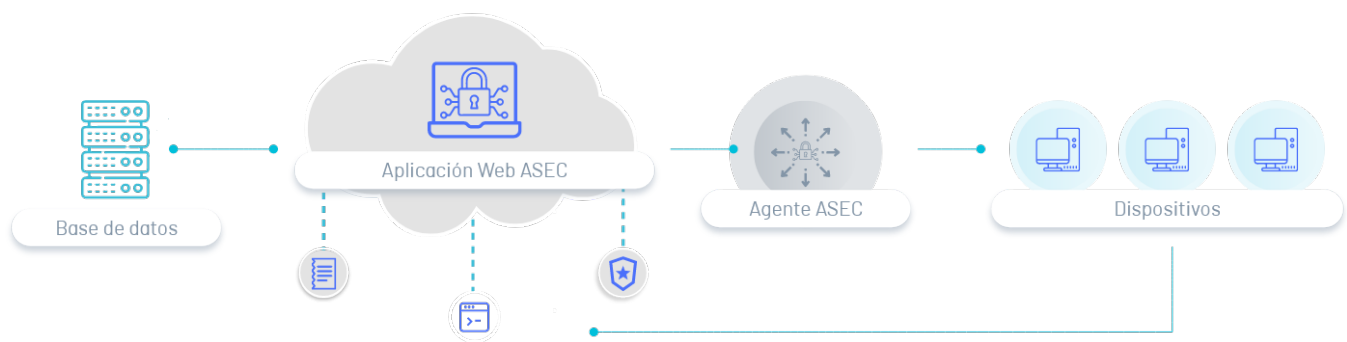
ASEC Operation

ASEC Operation

The process of managing compliance policies and the configuration tasks of the tool is carried out from the Aranda Security Web console. From ASEC's web environment, an administrator or specialist processes the information sent by the linked agents on the customer's devices, carrying out policy compliance verifications, generating the corresponding notifications to replicate the remediation actions on the devices.

Compliance policy management information is stored in a database.

For the operation of Aranda Security you must take into account the following components and their scope:



Web Console

Through a web environment, the user, according to the established role, will be able to manage the different processes of definition, follow-up and monitoring of compliance policies on security issues in the different workstations.

Agent

The Aranda Security agent is the component installed on the client's devices, which allows the specialist to detect the security components and monitor the implemented security policies from the ASEC web console.

Devices

The devices or workstations in ASEC correspond to the desktops and servers where the state of security software will be evaluated.

ASEC Environment









Aranda Security Web Console

The management and monitoring of compliance policies and the different configurations are carried out from the Aranda Security Compliance ASEC web environment.

After logging in, log in to the Aranda Security web console with the role set (administrator, specialist, users). You will be able to access a web console with the following features:

Main Menu

It groups the different categories associated with the main ASEC management concepts; the management modules in Aranda Security are:

Modules	Description	icon
Policies	This module defines compliance policies	
Summary	This module presents the results of compliance policies	
Deploy Agent	This configuration module makes it easy to distribute the agent across devices	
Users	This configuration module manages users and defines ASEC roles.	
Mail server	This configuration module manages mail servers.	
Licensing	This configuration module queries the purchased licenses.	
Directory Services	In this configuration module they manage the directory services that can be used by ASEC.	
External Authentication	This configuration module manages external authentication providers.	

Selecting a module from the main menu enables the information view with the custom information.



Info View

In this view, the information related to the concept chosen in the main menu is displayed and administrative tasks (consultation, creation, editing and deletion) of ASEC management are carried out.

In the information view, you can also find cross-cutting actions that complement management tasks, such as:

- **Data List:** This section groups the information of the records found by category or selected concept. The information presented is grouped into columns with the data entered.

By selecting the record from the available list, you will be able to view and edit the associated data, or delete the record.
- **See Pagination:** The numeric consecutive sorts the records on different pages.
- **Search engine:** This field allows you to perform a data query for the selected category. (searchable by the name of the fields defined for each ASEC concept)
- **New:** This button defines the action to create a record for ASEC management concepts such as policies, users, mail servers, and directory services. Activating this action enables a window to fill in the related information.
- **Delete:** This button defines the action for deleting an already created record in ASEC management processes for policies, users, mail servers, and directory services.

Aranda Security Compliance

AA

Regresar

CONFIGURACIÓN

Desplegar agente

Grupos de políticas

Usuarios

Servidor de correo

Licenciamiento

Servicios de directorio

Autenticación externa

Usuarios

Ahora puede crear el perfil de usuario y asociar roles a este.

Buscar

NUEVO

ELIMINAR

	Nombre	Usuario	Rol	Teléfono	E-mail	Fecha de creación
<input type="checkbox"/>	AA abraham pinelo	abraham.pinelo				21/09/2023 15:13:29
<input type="checkbox"/>	AA academy	academy				21/09/2023 15:13:35
<input type="checkbox"/>	AA Academy	academy			academy@arandasoft.c...	21/09/2023 15:39:48
<input type="checkbox"/>	AA Academy	academy			academy@arandasoft.c...	25/09/2023 10:48:38
<input type="checkbox"/>	AA Academy	academy			academy@arandasoft.c...	25/09/2023 11:11:52
<input type="checkbox"/>	AD ADM DESA	admdesa				21/09/2023 15:39:48
<input type="checkbox"/>	AD ADM DESA	admdesa				25/09/2023 10:48:38
<input type="checkbox"/>	AD ADM DESA	admdesa				25/09/2023 11:11:52
<input type="checkbox"/>	AA admdesa	admdesa				21/09/2023 15:13:26

ESTADO ☐ ACTIVO ☐ INACTIVO

< 1 2 3 4 5 6 7 8 9 >

20 of 2597 records

Detail View

This view presents detailed information on management concepts in ASEC. Example: User Details, Policy Summary, License Detail.

AD

ADM DESA

ACTIVO

Nombre completo: ADM DESA

Usuario: admdesa

Contraseña: *****

E-mail:

Teléfono:

Fecha de creación: 2023-09-25T16:11:52.41+00:00

ELIMINAR

Tipo de acceso a la consola

AD

ADM DESA

ACTIVO

*Nombre completo

ADM DESA

*Usuario

admdesa

*Contraseña

E-mail

Teléfono

Estado

Activo

Tipo de acceso a la consola

☐ Administrador

Administrador

☐ Especialista

Ver y modificar informes, tableros y pivotes

☐ Usuario

Ver informes, tableros y pivotes

Roles ASEC

Roles ASEC

Aranda Security Compliance ASEC has designed specialized user roles to carry out different tasks to implement compliance policies on devices according to the needs of the organization.



General Administrator Role

The general administrator is the role in charge of managing, monitoring and following up on compliance policies in security guidelines on workstations. It is also responsible for defining configuration items. In ASEC, the general administrator is in charge of the following functionalities:

- Create, update, delete, export, and monitor policies.
- Configure and manage users.
- Assign the roles of administrator, specialist, and user.
- Set up mail servers and manage licenses.
- Deploy the agent.
- Manage the licenses purchased.
- Consult the summary of the evaluation of compliance policies.

Rol	Módulos	Permisos

Specialist role

The specialist in Aranda Security Compliance will be able to define and manage security policies. ASEC specialist is responsible for the following functionalities:

- Create, update, delete, export, and monitor policies.
- Configure and manage users.
- Assign the roles of administrator, specialist, and user.
- Set up mail servers and manage licenses.
- Deploy the agent.
- Consult the summary of the evaluation of compliance policies.

