GUÍA DEL ADMINISTRADOR

Prólogo

GRACIAS!

Estimado Cliente,

Gracias por elegir Aranda 360 Security Suite de Aranda Software.

Nuestra reconocida y galardonada suite de seguridad ofrece una consistente y potente protección de 360 grados, a través de un único agente instalado en las estaciones de trabajo de los usuarios y administrado desde una consola central.

Con tan sólo un agente, Aranda 360 permite a las empresas proteger las estaciones de trabajo y equipos móviles de cualquier ataque o robo de información crítica, sin interrumpir la actividad del usuario.

A QUIEN ESTA DIRIGIDO ESTE DOCUMENTO?

Este documento está dirigida a los administradores del sistema que van a implementar y administrar la solución Aranda 360.

Contiene toda la información técnica necesaria para instalar y utilizar el producto en su sistema y entorno de red.

Este documento técnico incluye notas de la versión para la versión de Aranda 360 que está utilizando.

¿COMO ESTA ORGANIZADO ESTE DOCUMENTO?

CONVENCIONES DE ESCRITURA

FORMATOS

Las convenciones de escritura son descritas en la siguiente tabla:

CONVENTION	MEANING
Actualización/Licencia	Etiquetas de control, Etiquetas de menú, etc.
Actualización/Licencia	Etiquetas de control, Etiquetas de menú. En información o advertencias
notepad.exe	Nombre de archivos, rutas, etc.
notepad.exe	Nombre de archivos, rutas, etc. En notas o alertas
"paquetes"	Enlaces.
"paquetes"	Enlaces en notas o alertas.

Tabla 1.1: Convenciones de escritura

ICONOS

Descripción de los íconos:

Informativo — Información importante o consejo

Advertencia — Información crítica

Capítulo 1- GENERALIDADES DE ARANDA 360

ACERCA DE ESTE CAPÍTULO:

Este capítulo ofrece una introducción general a Aranda 360. A continuación un resumen del producto:

Valor agregado de Aranda 360:

- Concepto 1: Seguridad integrada.
- Concepto 2: Protección proactiva.
- Concepto 3: Control adaptativo.
- Concepto 4: Control de políticas flexibles.
- Concepto 5: Retroalimentación.
- Concepto 6: Cifrado de datos.

Mecanismos de protección de Aranda 360:

- Protección basada en reglas.
- Protección automática.
- Protección basada en perfiles.

Arquitectura de Aranda 360:

Conceptos:

- Comunicación entre componentes.
- Protección de estaciones de trabajo.
- Escalabilidad y alta disponibilidad.

Componentes de Aranda:

- Servidor Aranda 360.
- Servidor de Base de Datos SQL.
- Consola de administración Aranda.
- Agente Aranda 360.

Paquetes, opciones y licencias:

Paquetes:

- Aranda 360 Professional Edition.
- Aranda 360 Secure Edition.
- Aranda 360 Server-Side Protection.

Licencias:

- Actualizando la licencia.
- Aplicando una licencia a una ambiente.
- Información sobre licencias.

VALOR AGREGADO DE ARANDA 360

En un mundo cada vez más interconectado, las organizaciones de TI necesitan introducir medidas de seguridad más complejas ante las amenazas que se van presentando.

En la actualidad, existen pocas soluciones de seguridad realmente satisfactorias implementadas en estaciones de trabajo. La mayoría de los proveedores de servicios de seguridad ofrecen soluciones especializadas (cifrado de disco duro, antivirus, firewall personal).

Por ejemplo, consideremos un software antivirus y firewall, que han demostrado ser muy eficaces contra las amenazas externas. Sin embargo, su fortaleza es limitada cuando se instalan en laptops situados fuera de la organización. Las fallas de seguridad también puede ser aprovechadas cuando el análisis y filtrado de redes no identifican las amenazas en contra.

Enfoque Aranda Systems abarca seis conceptos básicos para compensar estas deficiencias.

CONCEPTO 1: SEGURIDAD INTEGRADA

Este concepto ofrece, a través de un agente, políticas de seguridad consistentes que abarcan:

- Control de usuario.
- Niveles de seguridad.
- Protección de información.
- Conectividad de red

CONCEPTO 2: PROTECCIÓN PROACTIVA

Este concepto proporciona una combinación de políticas inteligentes basadas en el comportamiento (amenazas desconocidas), firmas (amenazas conocidas) y protecciones. Esto elimina la necesidad de que los equipos de TI de revisar y actualizar periódicamente las PCs para el cumplimiento y eliminar aplicaciones no autorizadas.

Por desgracia, nuevos tipos de ataques son lanzados cada día. Las medidas de seguridad basadas en firmas deben conocer la amenaza antes de su identificación y prevención, proporcionando poca protección contra las nuevas variantes de virus o de software malicioso.

Además, un antivirus no tiene la capacidad de bloquear un ataque dirigido a una organización específica. Estos ataques nunca sigilo programado llevar a una firma que se emitió desde los proveedores de antivirus de soluciones siguen sin ser conscientes de ellos.

Si un virus se instala exitosamente en una estación de trabajo, su funcionamiento será neutralizado por Aranda 360 hasta el momento en que el antivirus tenga disponible la firma del virus para limpiar completamente la estación de trabajo…

CONCEPTO 3: CONTROL ADAPTATIVO

Este concepto ofrece políticas de control seguridad y seguridad de usuario que cambian dinámicamente en función del nivel de riesgo asociado a la forma en que los endpoints (estación de trabajo, portátil, PDA, etc.) son usados.

Por ejemplo, las aplicaciones instaladas directamente por los usuarios para uso personal pueden presentar tanto una amenaza de seguridad como una pérdida de productividad. Aranda 360 proporciona las herramientas necesarias para aplicar diferentes niveles de control sobre cualquier persona o grupo al utilizar las estaciones de trabajo.

CONCEPTO 4: CONTROL DE POLÍTICAS FLEXIBLES

Este concepto da la capacidad al IT de asegurar endpoints a través de una protección automática de rápida implementación, integrada en la suite de seguridad con configuraciones personalizadas que se adaptan a las políticas de seguridad de la organización.

CONCEPTO 5: RETROALIMENTACIÓN

Aranda 360 ofrece una amplia gama de información sobre operaciones maliciosas o sospechosas que afectan las estaciones de trabajo. Esta información constituye un complemento esencial a la información de los sistemas de monitoreo de redes para la protección de todos los sistemas de TI.

CONCEPT 6: CIFRADO DE DATOS

Para ayudar a proteger los sistemas y la información, Aranda 360 ofrece un cifrado de todo el disco antes del arranque y un cifrado de archivos después del arranque.

La información estará protegida en todo momento, independientemente de la estación de trabajo. Las políticas de cifrado que se administran desde una consola centralizada, se puede aplicar a:

- Cualquier usuario.
- Cualquier estación de trabajo.
- Todo el disco duro.
- Dispositivos extraíbles.
- Archivos / carpetas específicas.

MECANISMOS DE PROTECCIÓN DE ARANDA 360

Aranda 360 incluye tres mecanismos de protección para proporcionar el nivel más alto de seguridad en las estaciones de trabajo:

- Protección basada en reglas.
- Protección automática.
- Protección basada en perfiles.

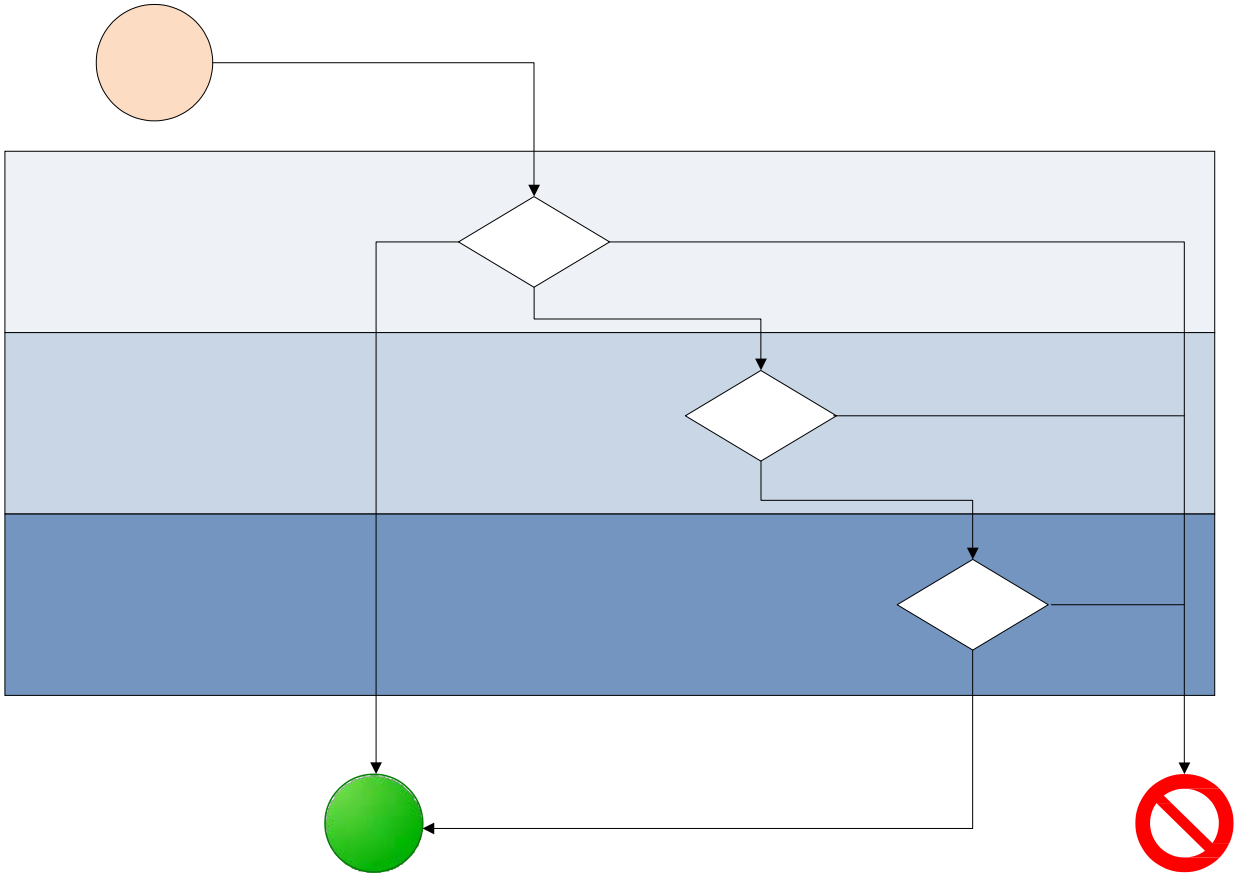


Fig. 1.1: Aranda 360 en su infraestructura de seguridad

PROTECCIÓN BASADA EN REGLAS

La Protección basada en reglas es utilizada para definir y garantizar la aplicación de políticas de seguridad en puntos donde el cliente lo considere. Las políticas de seguridad contienen una serie de reglas para permitir o denegar el acceso a:

- Ejecución de aplicaciones.
- Reglas de Firewall.
- Normas de uso de los recursos (red, archivos, registro base) para cada aplicación.
- Permisos sobre tipos de archivo (Dependiendo de su extensión).
- Derechos sobre dispositivos de almacenamiento.

Aplicaciones de confianza (La cual puede sobrescribir parte o la totalidad de las restricciones de Aranda 360). Una política de seguridad explícita puede aplicar a diferentes grupos de estaciones de trabajo.

Aranda 360 suministra reglas predefinidas para que las políticas puedan ser aplicadas inmediatamente por el administrador. Estas reglas por defecto pueden ser modificadas en cualquier momento para adaptar políticas a las necesidades de la empresa.

PROTECCIÓN AUTOMÁTICA

La protección automática está diseñada para detectar y bloquear código malicioso, ya sea conocido o desconocido, mediante identificación de patrones de ataque, y no por identificación de código

La protección automática no requiere ninguna configuración por el administrador. Sin embargo el administrador puede configurar los niveles de como Aranda 360 reaccionara a diferentes eventos. Para obtener más información, ver “Configuración para protección automática”, página 234.

Existen dos categorías principales de mecanismos de protección automática en Aranda 360:

- La primera categoría comprende las actividades de las aplicaciones y del sistema.

  Su función es proteger las estaciones de trabajo de intentos de corrupción de archivos ejecutables y acceso no autorizado a servicios del sistema o información sensible.

- La segunda categoría comprende un sistema de detección de intrusiones (IDS) para que las estaciones de trabajo puedan protegerse de ataques en la red.

  Los mecanismos aplicados para detectar ataques al sistema o red por parte del sistema de protección automática permanecen activos de forma permanente. El tratamiento de estos eventos puede ser controlado por el administrador. Dependiendo del tipo de evento que se produzca, el sistema enviará una alerta o aplicará medidas automáticas definidas por el administrador.

PROTECCIÓN BASADA EN PERFILES

La Protección basada en perfiles está basada en la capacidad avanzada de monitorear las llamadas al sistema realizadas por cada aplicación. Durante una fase de aprendizaje, el comportamiento de la aplicación es monitoreado.

La fase de aprendizaje es usada para recopilar información esencial sobre las acciones realizadas por las aplicaciones mientras se están ejecutando en su estación de trabajo. Las llamadas al sistema son memorizadas para crear un perfil estándar de la aplicación. Después de esta fase, las acciones realizadas por la aplicación son comparadas con el perfil estándar, a fin de detectar posibles comportamientos indebidos que puedan ocurrir. La exclusiva tecnología de Aranda 360 permite que dichos comportamientos se puedan manejar de forma inteligente por correlación y prioridad.

Aranda 360 detectará cualquier comportamiento de la aplicación diferente al de su perfil estándar y reaccionará de acuerdo a los parámetros establecidos por el administrador.

La Protección basada en perfiles constituye una tercera línea de defensa, que es especialmente adecuado para los ataques dirigidos a nuevos gusanos y de rápida propagación. Cualquier intento de ataque basado en corrupción de aplicaciones o servicios del sistema operativo será bloqueado, incluso si no se existe la definición de la firma u otro mecanismo para proteger el sistema.

ARQUITECTURA DE ARANDA 360

Aranda 360 es un sistema de protección distribuida que cubre todas las estaciones de trabajo pertenecientes a la organización.

Su arquitectura está basada en un modelo multi-capa que permiten ser rápidamente integradas e implementadas en la red de la organización.

CONCEPTOS

Comunicación entre componentes

Las Comunicación entre todos los componentes es autenticada y cifrada utilizando certificados SSL v3 and X509 v3. Autenticación mutua es usada por cada componente para reforzar la seguridad.

Protección en estaciones de trabajo

La protección en las estaciones de trabajo es manejada por el módulo agente Aranda 360.

El agente se comunica con el servidor de implementación, cuya función es distribuir las políticas de seguridad a cada agente y recoger información con respecto a la seguridad de éstas.

Esta información es almacenada por el servidor en una base de datos dedicada, la cual se puede acceder a través de la consola de administración.

Escalabilidad y alta disponibilidad

Aranda 360 está preparada para los entornos empresariales más exigentes.

La alta disponibilidad está basada en mecanismo de balanceo de carga y tolerancia a fallos, distribuidos en varios servidores de implementación.

El agente requiere al menos un servidor de implementación, denominado servidor principal. Los servidores secundarios pueden ser agregados al servidor principal.

El servidor principal es el único servidor que se comunica directamente con la consola de administración.

El servidor principal comparte las políticas de seguridad y descripciones de los "Grupos de agentes" con los servidores secundarios.

COMPONENTES DE ARANDA 360

Aranda 360 está compuesta por:

- Servidor Aranda 360.
- Base datos SQL.
- Consola de Administración Aranda 360.
- Agente Aranda 360.

Fig. 1.2: Arquitectura de Aranda 360

Servidor Aranda 360

Servidor Principal

El servidor principal es utilizado para distribuir las políticas de seguridad y los logs.

El agente requiere al menos un servidor de implementación, denominado servidor principal.

Debe existir al menos un servidor principal por sitio.

Los servidores secundarios son opcionales. Pueden ser utilizados como contingencia ante posibles fallas y para balanceo de carga.

Servidores Secundarios

Los servidores secundarios pueden ser agregados al servidor principal. El servidor principal comparte las políticas de seguridad y descripciones de los "Grupos de agentes" con los servidores secundarios.

La consola de administración se comunica con los servidores disponibles. Si un servidor no está disponible cuando la consola envía una configuración, el servidor actualizará su configuración con los demás servidores cuando vuelva a estar en línea.

Servidor de balanceo de carga

En el Editor de configuración, se puede definir una lista de servidores (principal y secundario) para balancear la carga. También Es posible dar prioridad a los servidores.

Cada vez que se implementa una configuración, los agentes reciben la dirección del servidor principal y secundario que están autorizados, en el orden en el que se accedieron. Cuando el agente intenta conectarse a un servidor para determinar si una nueva configuración está disponible, se conecta de forma predeterminada al último servidor conectado. Si éste se encuentra sobrecargado, un mensaje es enviado al agente para que éste se conecte a otro servidor.

La lista de servidores se utiliza para definir una prioridad basada en localización de agentes.

Respaldo del servidor secundario

Si el servidor principal no está disponible, el siguiente servidor secundario definido en la lista de prioridades toma el rol de servidor principal. Los agentes se comunican con el nuevo servidor principal y el administrador es notificado de este cambio.

Cuando el servidor original está disponible de nuevo, automáticamente toma su función principal y el servidor secundario que realizó temporalmente su función retorna a su rol.

Base de datos SQL

La base de datos SQL es utilizada para almacenar la siguiente información:

- Logs.
- Políticas de seguridad.
- Información recuperada.

Una sola base de datos puede ser asignada a varias consolas de administración (si es necesario).

Consola de Administración Aranda 360

La consola de administración es utilizada para:

- Definir políticas de seguridad.
- Administración de usuarios.
- Logs de monitoreo.

Las características de la consola de administración dependerán del paquete de Aranda 360 seleccionado.

Agente Aranda 360

Los agentes instalados en las estaciones de trabajo tienen la función de aplicar políticas de seguridad y enviar logs al servidor Aranda 360.

PAQUETES, OPCIONES Y LICENCIAS

PAQUETES

Aranda 360 está disponible en tres paquetes, cada una adaptada a sus necesidades:

- Aranda 360 Professional Edition.
- Aranda 360 Secure Edition.
- Aranda 360 Server-Side Protection.

Los paquetes de Aranda 360 están disponibles para las siguientes versiones:

Paquetes de Aranda 360	Versión 32-bit	Versión 64-bit
Professional Edition		
Secure Edition		
Server-Side Edition		

Tabla 1.1: versiones de Aranda 360

Cada paquete esta licenciado para usar en un ambiente específico.

CARACTERÍSTICAS DE ARANDA 360	Professional Edition (32 bits)	Professional Edition (64 bits)	Secure Edition (32 bits)	Secure Edition (64 bits)	Server-Side Protection (64 bits)
Políticas de seguridad					
Configuración general: • Control de comportamiento del sistema.	✓	✓	✓	✓	✓
• Control de comportamiento de procesos.	✓	✓	✓	✓	✓
• Control de dispositivos.	✓	✓	✓	✓	✓
• Autenticación y cifrado Wi-Fi.	✓	✓	✓	✓	✓
• Control de actividad de red.	✓	✓	✓	✓	✓
• Firewall.	✓	✓	✓	✓	✓
• Reglas de aplicación.	✓	✓	✓	✓	✓
• Reglas de Extensión.	✓	✓	✓	✓	✓
• Componentes del Kernel.	✓	X	✓	X	X
• Trusted Rules.	✓	✓	✓	✓	✓
• Puntos de acceso Wi-Fi.	✓	✓	✓	✓	✓
• Dispositivos Extraíbles.	✓	✓	✓	✓	✓
Configuraciones					
• Configuración del agente.	•	•	•	•	•
• Acceso temporal web.	•	•	•	•	•
• Aprendizaje.	•	•	•	•	•

Tabla 1.2: Características de los Paquetes de Aranda 360 (Parte 1 de 2)

CARACTERÍSTICAS DE ARANDA 360	Professional Edition (32 bits)	Professional Edition (64 bits)	Secure Edition (32 bits)	Secure Edition (64 bits)	Server-Side Protection (64 bits)
Scripts					
• Pruebas	✓	✓	✓	✓	✓
• Acciones	✓	✓	✓	✓	✓
• Procesos por lotes	✓	✓	✓	✓	✓
Políticas de Cifrado					
• Configuración general	✗	✗	✓	✓	✗
• Parámetros de cifrado de archivos	✗	✗	✓	✗	✗
• Parámetros de cifrado de todo el disco	✗	✗	✓	✓	✗
La opción AVP está disponible en todo los paquetes					

Aranda 360 Professional Edition

El paquete "Professional Edition" incluye tres características:

- Políticas de seguridad.
- Configuraciones.
- Scripts.

Característica "Políticas de seguridad"

Esta característica permite al administrador aplicar controles específicos a los agentes (a través del servidor).

Característica "Configuraciones"

Esta característica permite al administrador aplicar políticas y configuraciones que cambian dinámicamente.

Característica "Scripts"

Esta característica permite al administrador escribir scripts personalizados para ejecutar pruebas, aplicar políticas y configuraciones.

Aranda 360 Secure Edition

El paquete "Secure Edition" incluye además de las tres características del paquete "Professional Edition", la funcionalidad de "políticas de cifrado".

Característica " políticas de cifrado "

Esta funcionalidad adicional permite al administrador crear políticas de cifrado para discos duros y archivos.

Aranda 360 Server-Side Protection

El paquete de "Aranda 360 Server-Side Edition" es utilizado por servidores con el sistema operativo Microsoft Windows Server 2008 R2 (versión 64-bi).

- El servidor Aranda 360 y el agente no pueden ser instalados en la misma máquina.

El paquete de "Server-Side Edition" incluye las características de la edición "64-bit Professional Edition's.

- El paquete "Server-Side Edition" no es compatible con la opción "Server Core installation" en Windows Server 2008 R2.

LICENCIAS

Actualizando la licencia

Una licencia es adquirida para un entorno específico. Si se está utilizando una versión de Aranda inferior a 6.0, es necesario actualizar la licencia.

Si el proceso de actualización falla, un mensaje aparecerá en pantalla.

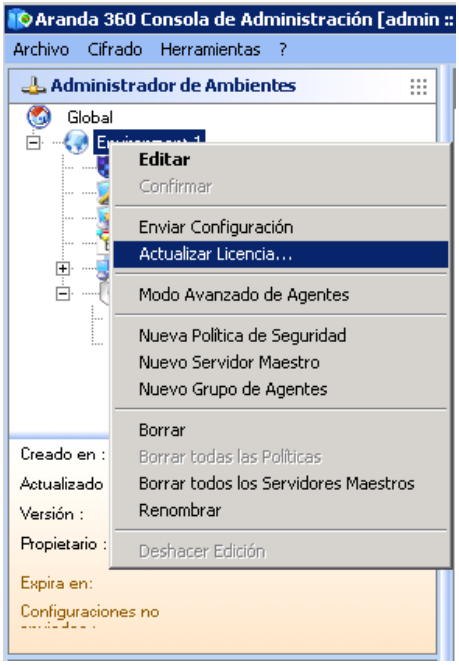
El nuevo archivo mostrara el número de licencias total y por opción.

Ejemplos:

Aplicando la licencia en un ambiente

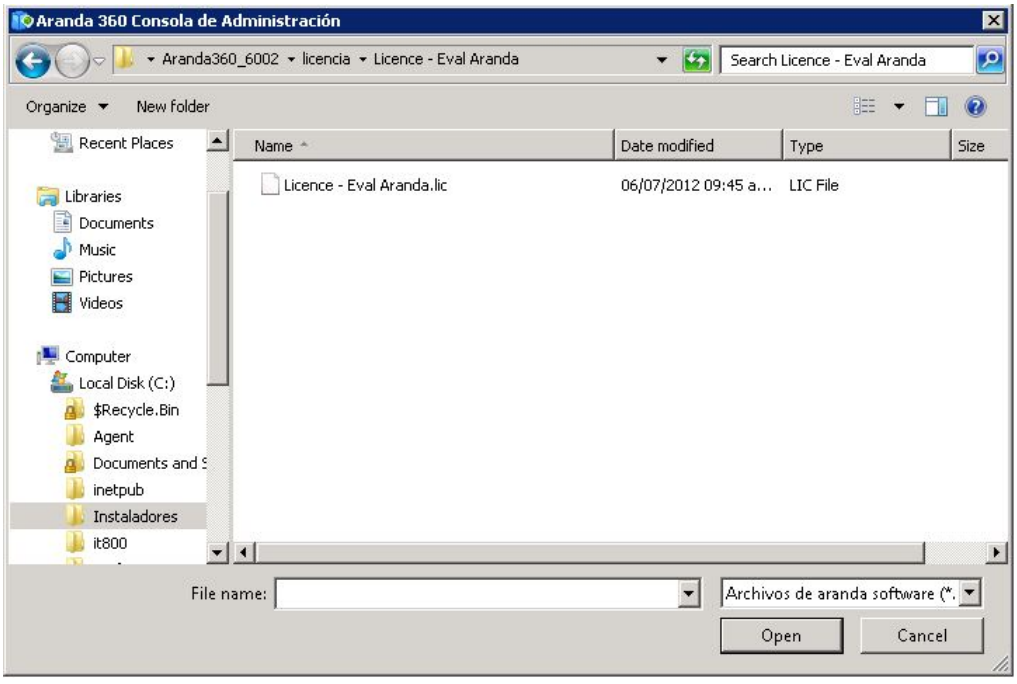
Para actualizar y aplicar la licencia a un entorno, siga los siguientes pasos:

1 Clic derecho en ambientes y seleccione Actualizar/Licencia desde el menú.

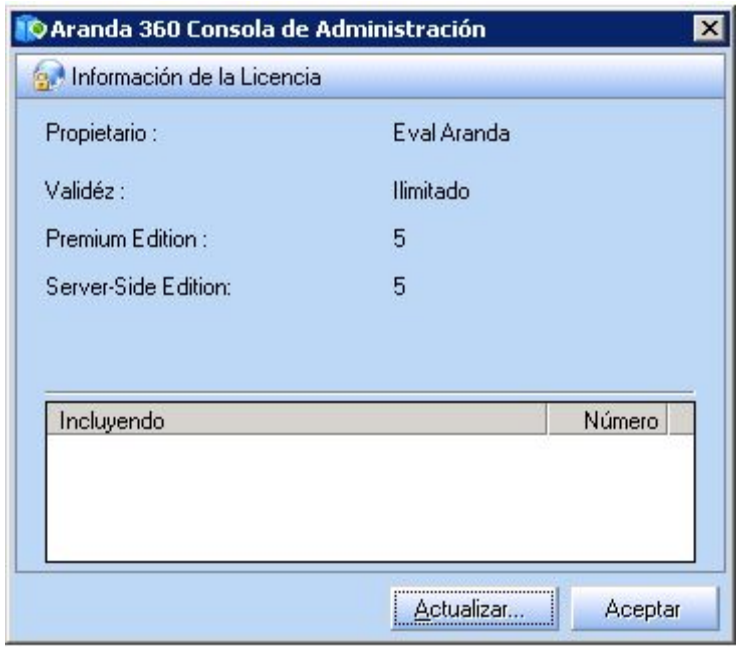


2 Para actualizar la licencia de Aranda 360, seleccione Actualizar.

3 Seleccione el archivo de licencia de Aranda 360 y haga clic en Abrir.



- Si la licencia actualizada no es compatible con algunas funcionalidades de la anterior licencia, Aranda 360 alertará la posibilidad de pérdida de información.



Si tiene una licencia con fines de evaluación, tendrá una versión de demostración de la consola de administración. La fecha de expiración será mostrada en la parte inferior al hacer clic en el ambiente creado.

Información sobre licencias

Para obtener información sobre las licencias, siga los siguientes pasos:

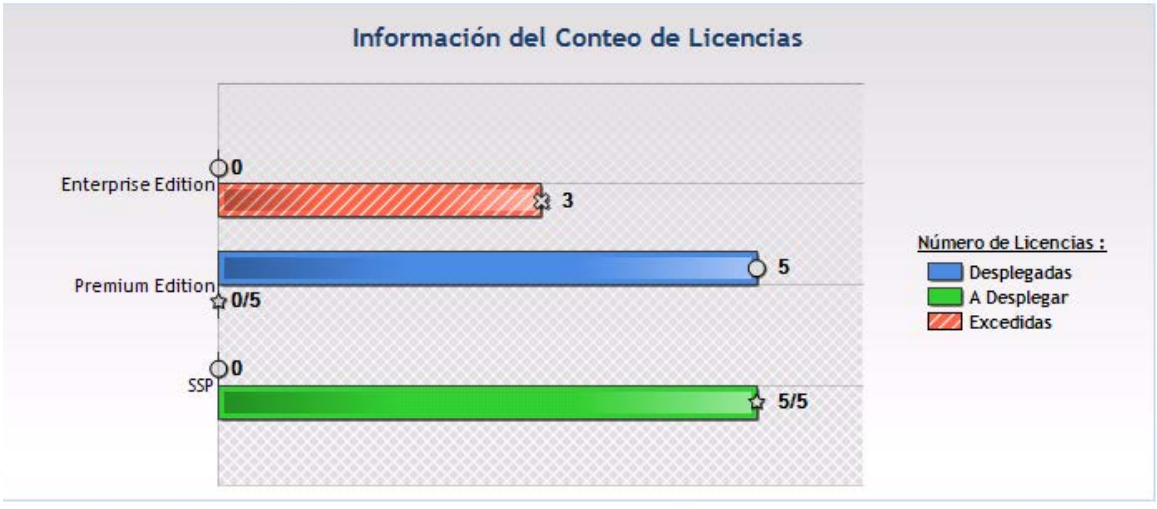
1. Haga clic en licencias en el panel de administración y monitoreo.

Se abrirá un reporte con:

- La fecha de la licencia.

- La implementación del agente y el número de licencias disponibles.

- Información sobre el número de licencias:
  - Desplegado.
  - Disponible.
  - Excedido.



2. Utilice la barra de desplazamiento para mostrar toda la información.
3. Si desea guardar el reporte, Haga clic sobre el ícono

El reporte se guardará en la ruta especificada, en formato .png.

Capítulo 2 - INSTALACIÓN, ACTUALIZACIÓN Y DESINSTALACIÓN DE ARANDA 360

ACERCA DE ESTE CAPÍTULO

Este capítulo contiene:

Requisitos para Aranda 360 bajo Windows:

- Requisitos para el servidor Aranda 360
- .Requisitos para la base de datos:
  - Con una base de datos existente.
  - Con una base de datos embebida.
- Requisitos para la consola de administración.
- Requisitos para el agente.

Herramientas de instalación:

- Requisitos.
- Configuración.
- Procedimiento:
  - Asistente de instalación Aranda 360.
  - Asistente de instalación de la base de datos.
  - Asistente de configuración de ambiente.
  - Asistente para la implementación del agente.

Instalación Manual de Aranda 360:

- Requisitos.
- Procedimiento:
  - Instalando el servidor principal.
  - Instalando servidores secundarios.
  - Instalando la consola de administración.
  - Instalando la base de datos.
  - Configurando el ambiente.
  - Instalando el agente.

Descarga de certificados:

- Periodo de Validez del certificado.
- Inicio de sesión y contraseña para descargar certificados.
- Compatibilidad con herramientas de clonación.

Pruebas posteriores a la instalación.

Actualizando componentes.

Posibles cambios:

- Cambiando la dirección IP del servidor Aranda.
- Cambiando los puertos TCP del servidor para servicios HTTP y SSL.

Desinstalando componentes:

- Desinstalando el servidor y la consola.
- Desinstalando el agente.
- Removiendo la base de datos.

REQUISITOS PARA ARANDA 360 BAJO WINDOWS

REQUISITOS PARA EL SERVIDOR ARANDA 360

Para la instalación de Aranda 360 Versión 6.0 bajo Windows, el servidor debe cumplir con los siguientes requisitos:

- Procesador: 1 GHz mínimo.
- Memoria RAM: 1 GB mínimo.
- Disco Duro: 1 GB libre mínimo.
- Disco Duro (para un servidor con antivirus): 1.5 GB libre mínimo.
- Sistema operativo:

Sistema operativo	Versión 32-bit	Versión 64-bit
Windows Server 2003 SP2		
Windows Server 2003 R2		
Windows Server 2008 SP2		
Windows Server 2008 R2	-	

Una dirección IP estática para el servidor.

Comunicación entrante (Servidor Aranda 360):

- Puerto TCP 16003.
- Puerto TCP 16005.
- Puerto TCP 16006.
- Puerto TCP 16007.

Comunicación saliente (Servidor Aranda 360):

- Puerto TCP 16003.
- Puerto TCP 16006.

Comunicación entrante (Servidor Web):

- Puerto TCP 80.
- Puerto TCP 443.

Se deberán escoger otros puertos si éstos ya están siendo utilizados por un servidor Web instalado en el servidor.

Los puertos TCP 80 y 443 serán usados por el servidor web para desplegar los agentes instalados.

REQUISITOS PARA EL SERVIDOR ARANDA 360

La base de datos debe cumplir con los siguientes requisitos:

- Cualquier versión de Windows compatible con MS SQL Server 2005.
- Comunicación con el Servidor Aranda 360 y la consola:
    - Puerto TCP dinámico definido en:
      SQL Server 2005 Configuración de red > Protocolos para [instancia de la base de datos] > TCP/IP > Propiedades > Dirección IP > IPAll > puerto dinámico TCP.

      Para obtener más información, ver " Como cambiar el puerto para S Q L Server 2005 ".
    - Puerto UDP 1434.
- Disco duro: 10 MB libres para la base de datos inicializada (excluyendo el motor SQL), y un espacio adicional para las configuraciones y número de alertas.

  Espacio adicional es requerido para:

  - Log de la base de datos: 30 MB por agente por cada año.
  - Identificación de la base de datos: 1 MB por agente.
  - Cifrado de claves de la base de datos: 1 MB por agente.

  Esta información es solo un estimado para requerimientos de disco. Esto depende de las políticas de seguridad implementas y las configuraciones del log.

MS SQL Server 2005 Express Edition es suministrado con Aranda 360 y puede ser directamente instalado con las herramientas de instalación de Aranda 360.

En la instalación de la base de datos, use el modo de autenticación mixto.

Se deben usar las intercalaciones no sensibles a mayúsculas y minúsculas, o de otra forma los scripts necesarios para la instalación la base de datos no serán soportados.

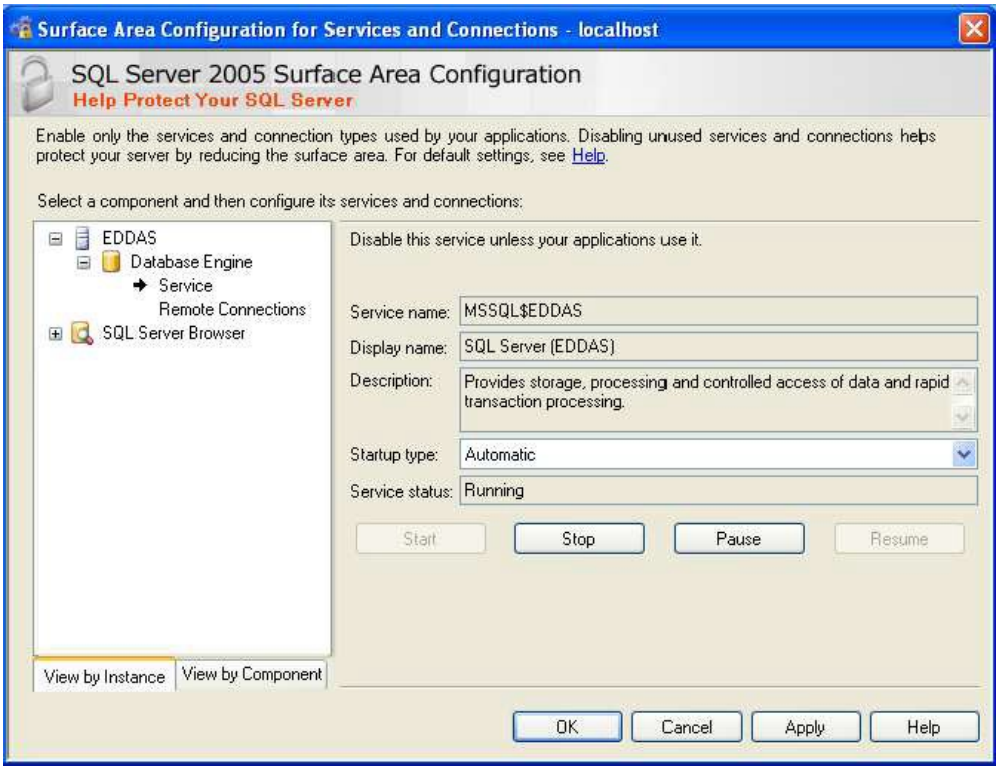
Utilizando una base de datos existente

El modo de autenticación mixta (NT y SQL) y conectividad TCP son requeridos.

Como cambiar los parámetros de conexión a SQL Server 2005

Para cambiar los parámetros de conexión (acceso remoto o local) a SQL Server 2005, utilice la configuración de Área para servicios y conexiones. Esta herramienta mostrará información sobre:

- Servicio de SQL Server (EDDAS):



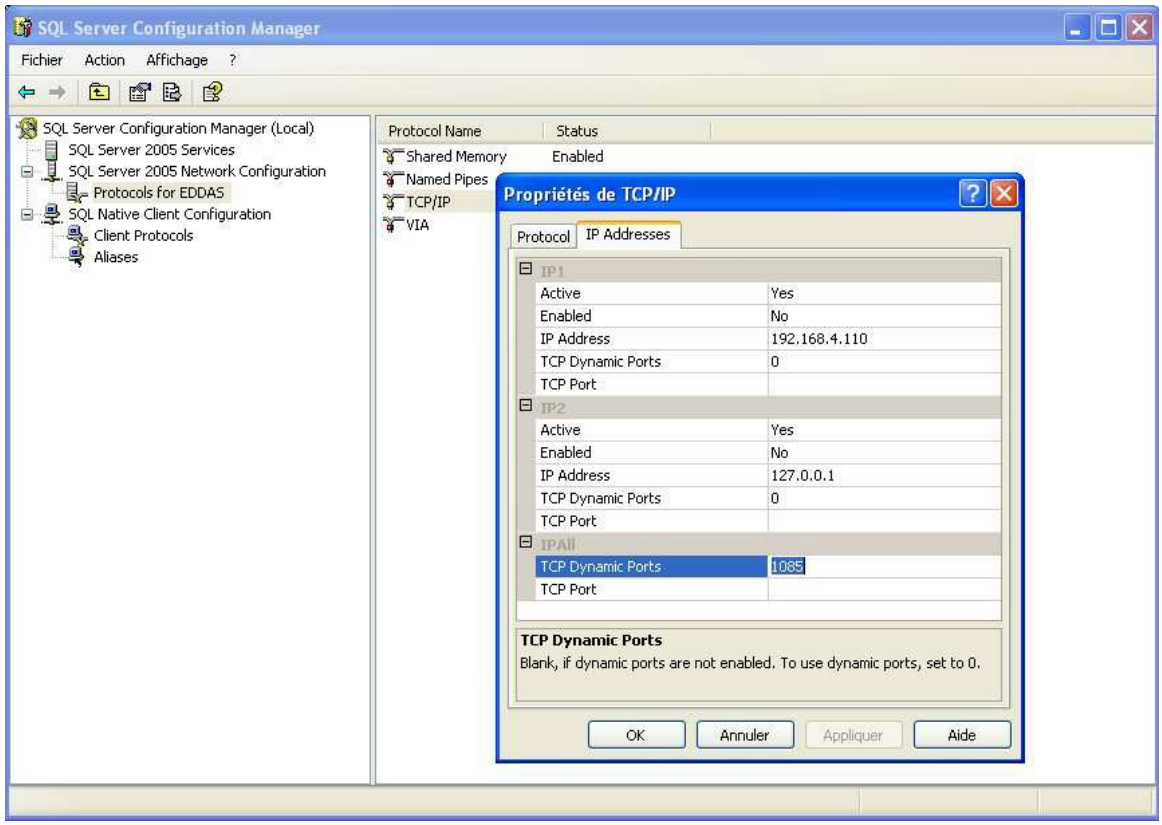
- Conexiones locales y remotas:

Como cambiar el puerto TCP para SQL Server 2005

Para cambiar el número del puerto TCP asignado a la instancia de la base de datos, utilice el Administrador de configuración de SQL Server en:

> SQL Server 2005 Configuración de red > Protocolos para [instancia de la base de datos] > TCP/IP > Propiedades > Dirección IP > IPAll > puerto dinámico TCP.

Utilizando una base de datos embebida



Compruebe en el equipo de destino que no hay ninguna instancia de base de datos con el mismo nombre que la base de datos a instalar (EDDAS). Para ello, asegúrese que la lista de servicios en el panel de control no incluye el servicio SQL SERVER (EDDAS).

.

REQUISITOS PARA LA CONSOLA DE ADMINSTRACIÓN

Los Requisitos para la consola de administración son:

- Pentium III: ~800 MHz (recomendado).
- Memoria RAM: 512 MB (recomendado).
- Disco duro: 50 MB libres.
- Sistema operativo:

Sistema operativo	versión 32-bit	Versión 64-bit
Windows XP SP1		
Windows XP SP2		
Windows XP SP3		-
Windows Server 2003 SP1		
Windows Server 2003 SP2		
Windows Server 2008 SP1		
Windows Server 2008 SP2		
Windows Vista SP1		
Windows Vista SP2		
Windows 7		

- Framework .Net 2.0.
- Paquete redistribuible Microsoft Visual C++ 2008.
- Dirección IP estática de la máquina donde vaya a ser instalado el primer servidor principal.
- Dirección IP o nombre de la máquina donde vaya a ser instalada la base de datos.
- Comunicación saliente:
    - Puerto TCP 16007.
    - Puerto TCP 1434.
- Contraseña de la cuenta de administrador de la base de datos.

REQUISITOS PARA EL AGENTE

Los Requisitos para el agente son:

- Pentium IV: 3 GHz.
- Memoria RAM: 512 MB (mínimo), 1 GB (recomendado).
- Espacio en disco: 25 MB libres (90 MB con logs de agentes).
- Espacio requerido para un servidor con antivirus: 350 GB.
- Sistema operativo:

Sistema Operativo	versión 32-bit	versión 64-bit
Windows XP SP3		-
Windows Vista SP2		
Windows 7		
Windows Server 2008 R2	-	

- GINA (Autenticación e identificación Gráfica): Si en la organización se utiliza un sistema de autenticación fuerte basado en la DLL gina, es necesario instalar éste producto antes de la instalación de Aranda 360.
  En caso de que se desinstale el producto de autenticación, se debe desinstalar primero Aranda 360. La suite guarda la ruta de la actual DLL gina.dll hasta la instalación, y la restaurará hasta la desinstalación.

  Este comentario sobre la DLL `gina` es aplicable solo a ambientes XP.

- Comunicación entrante: Puerto TCP 16006.
- Comunicación saliente:
  - Puerto TCP 16005.
  - Puerto TCP 16006.
  - Puerto TCP 443 (configurable).
  - Puerto TCP 80 (configurable).
  - Puerto TCP 7080.
- Bucle local:
  - Puerto TCP 16010.
  - Puerto TCP 16011
  - Puerto TCP 16012.

HERRAMIENTAS DE INSTALACIÓN

REQUISITOS

Antes de instalar Aranda 360 utilizando las herramientas de instalación, verifique que los siguientes archivos y carpetas estén presentes:

- La carpeta bin con los siguientes archivos:
  - Server.exe
  - Console.exe

- La carpeta resources_x86 (32 bits) o resources_x64 (64 bits) con los siguientes archivos:
  - dotnetfx.exe (Microsoft .Net Framework).
  - MSXML6.msi (Microsoft MSXML 6.0 Parser).
  - SQLEXPR.exe (Microsoft SQL Server 2005 Express Edition).
  - SSMSEE.msi (Advanced Services for SQL Server 2005 Express Edition).
  - vcredist.exe (Microsoft Visual C++ 2008 Redistributable).
  - WindowsInstaller.exe (Microsoft Windows Installer 4.5).

- El archivo setup.exe (Aranda 360).

CONFIGURACIÓN

Al comenzar el proceso de instalación, el administrador puede definir la siguiente configuración:

- Tipo de instalación:
  - Instalación completa.
  - Instalación sencilla (sin asistente).
  - Solo servidor (servidor secundario).
  - Solo consola (consola remota).
  - Instalación personalizada.
- Componentes:
  - Servidor.
    - Generación de certificados.
  - SQL Server 2005 Express Edition.
    - SQL Server Management Studio Express.
  - Consola.
- Herramientas de Administración:
  - Instalación de la base de datos.
  - Configuración de consola.
  - Implementación del agente.
- Carpeta de instalación.

PROCEDIMIENTO

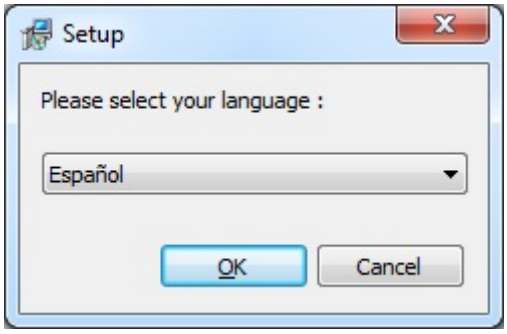
Aranda 360 puede ser instalada en cuatro escenarios utilizando las características mostradas en la ventana de instalación:

1. Asistente de instalación de Aranda 360.
2. Asistente de instalación de la base de datos.
3. Asistente de configuración de ambientes.
4. Asistente de implementación del agente.

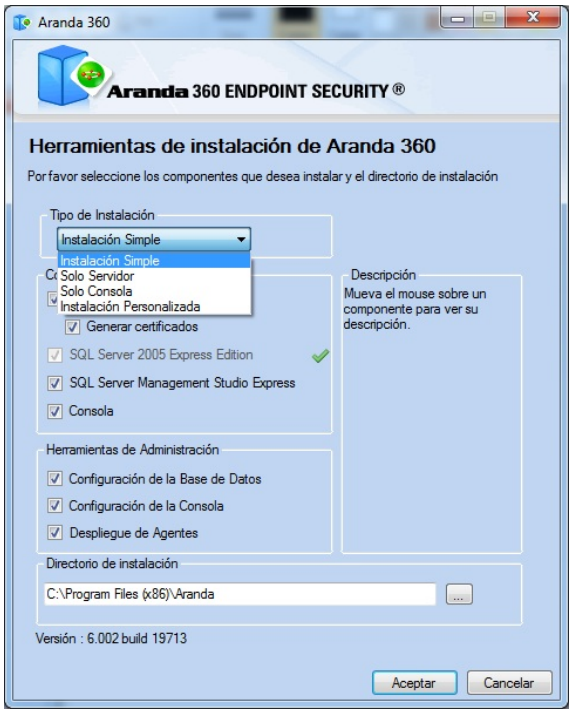
Aranda 360 asistente de instalación

Para instalar Aranda 360, siga los siguientes pasos:

1. Doble clic en setup.exe.
2. Seleccione un idioma.



3. Escoja la configuración.



- El tipo de instalación que desea iniciar:
  - Instalación completa.
  - Instalación básica (sin asistente).
  - Solo servidor (servidor secundario).
  - Solo Consola (consola remota).
  - Instalación personalizada.

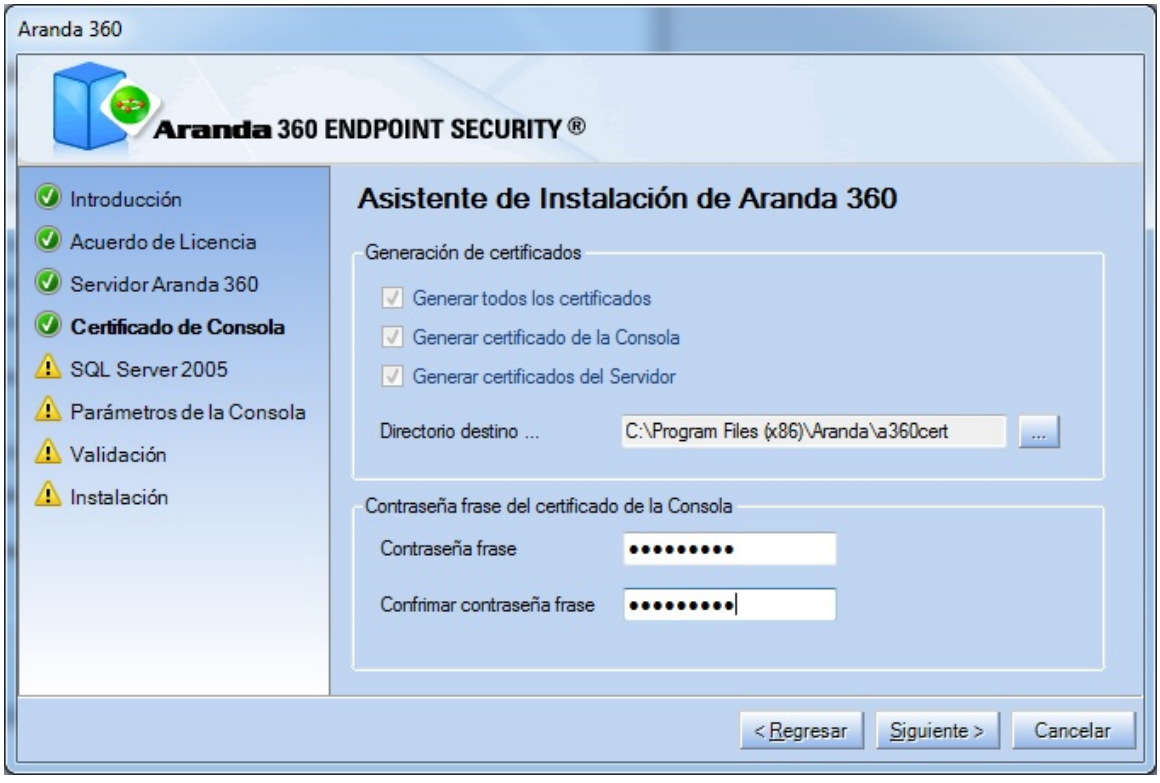
- Los componentes de Aranda 360 que desea instalar (si escoge una instalación diferente a la completa):
  - Servidor Aranda 360 (y su certificado).
  - Servidor SQL.
  - Consola de administración Aranda.
- Las herramientas de administración que desea utilizar para instalar Aranda 360:
  - Instalación de la base de datos (Asistente de instalación de Aranda 360).
  - Configuración de consola (Asistente de configuración de ambientes).
  - Implementación de agente (Asistente de implementación del agente).
- La carpeta de instalación de Aranda 360.

Haga clic en OK para validar la configuración.

4. Para comenzar el proceso de instalación de Aranda 360, haga clic en Siguiente.

5. Digite la dirección IP del servidor, y haga clic en siguiente.

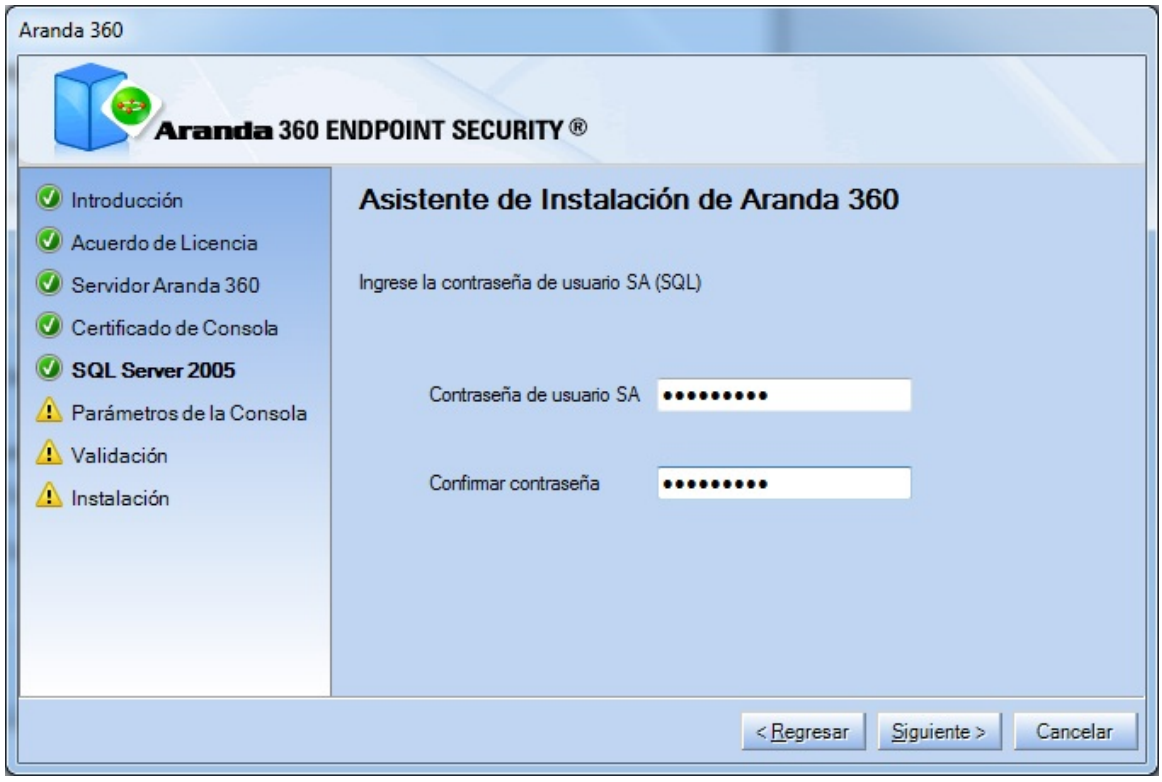
6. Digite y confirme la nueva contraseña del certificado.
Haga Clic en siguiente.



- Si ha marcado las opciones Servidor y Generar certificados en la sección Componentes.

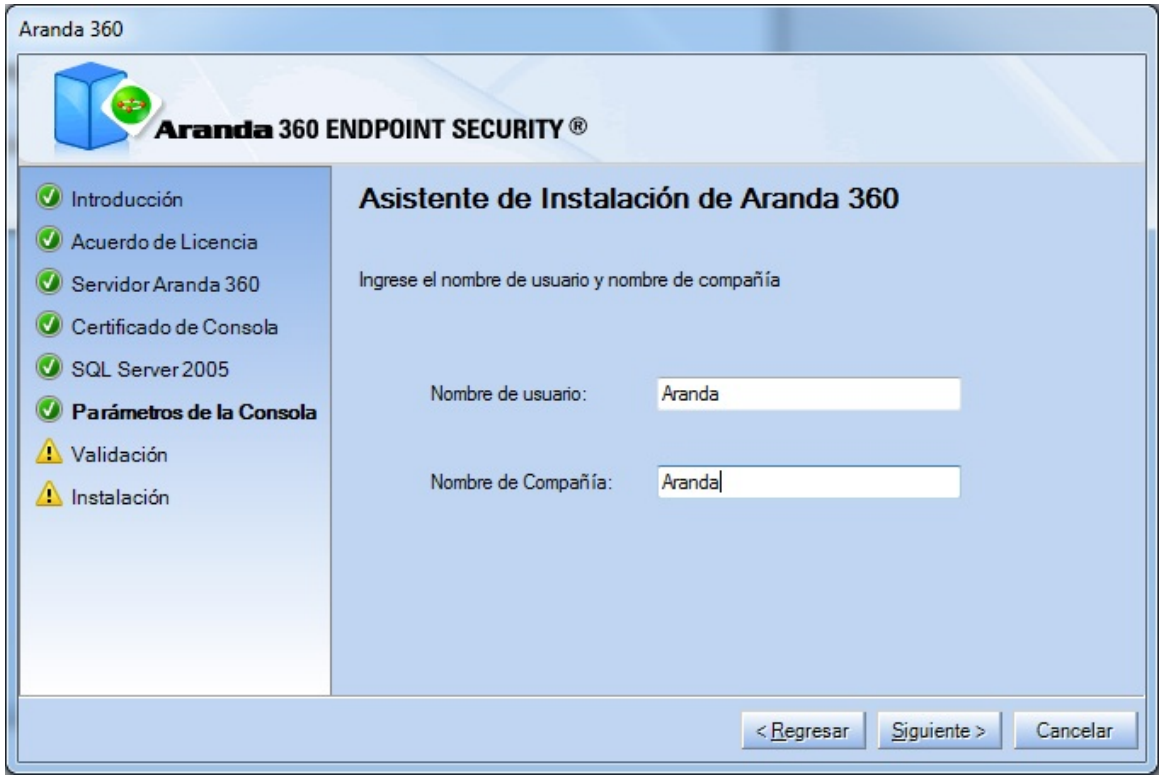
7. Digite y confirme la nueva contraseña de la base de datos.

   Haga Clic en siguiente.



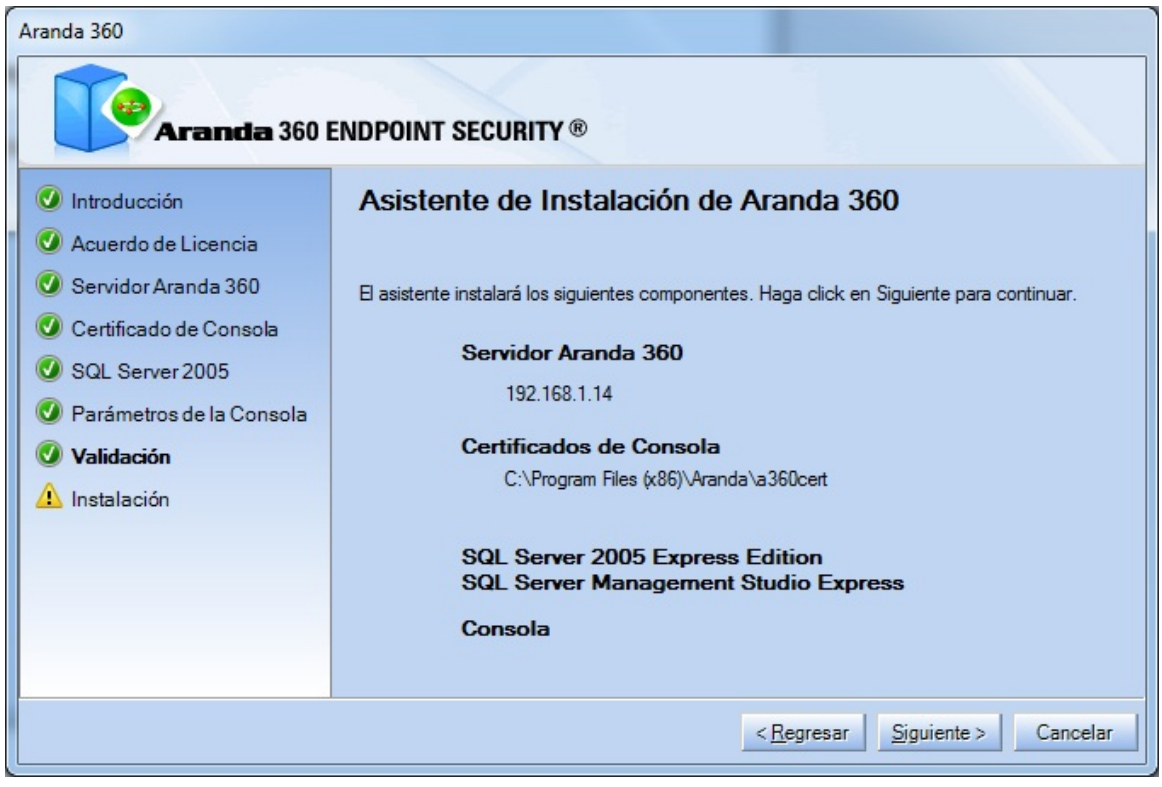
8. Digite el nombre de usuario y de la compañía para instalar la consola de administración.

   Haga Clic en siguiente.

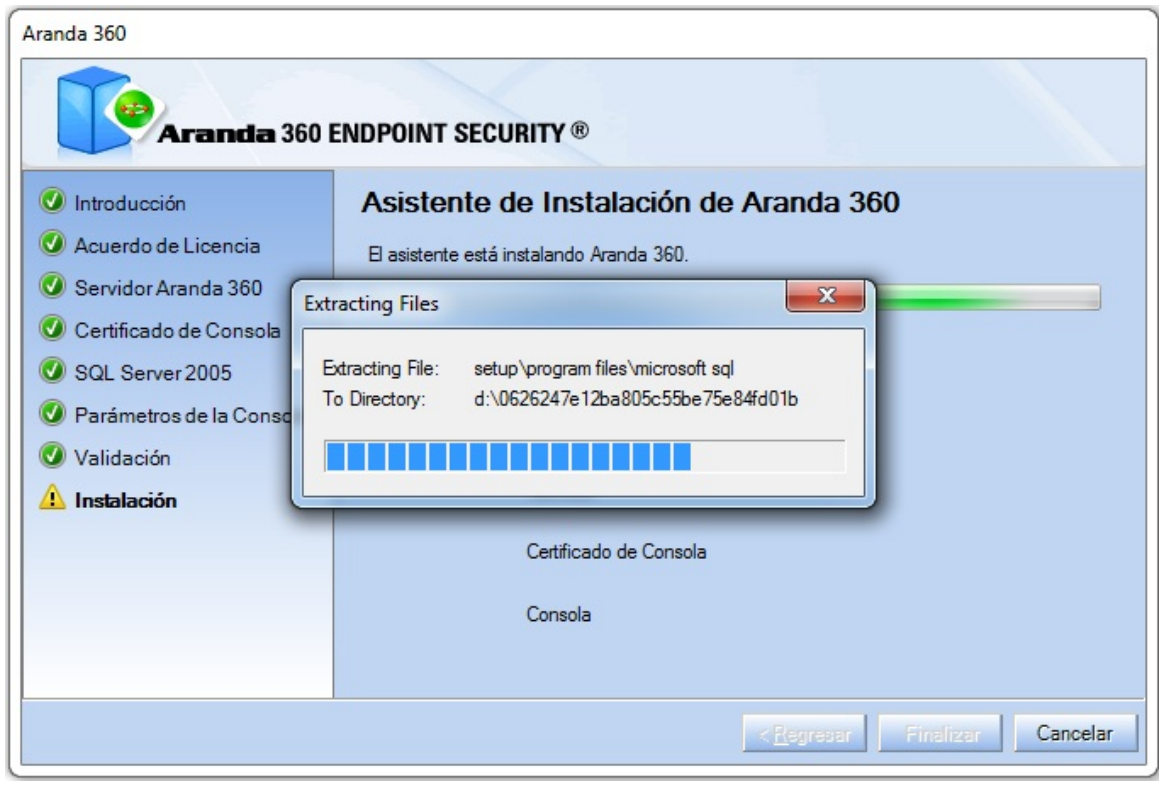


9. La siguiente ventana muestra un resumen de toda la configuración definida.

Haga clic en siguiente para validar la configuración.

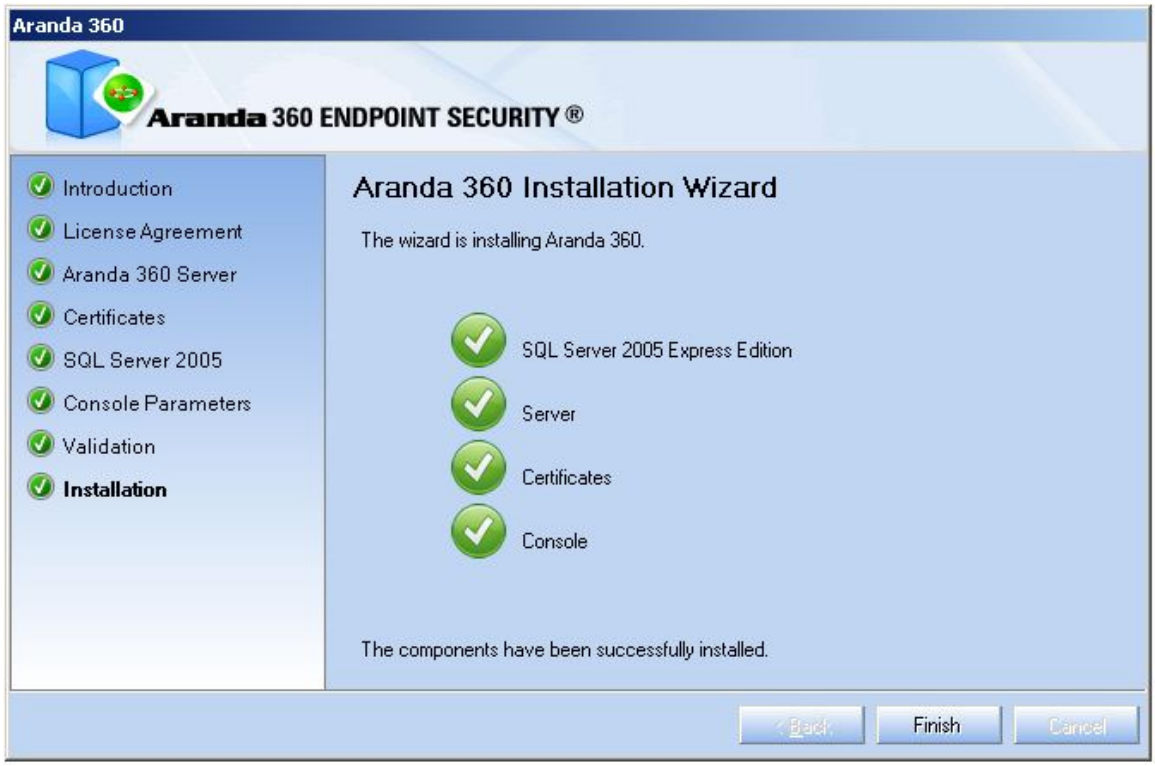


10. Espere hasta que el proceso de instalación de Aranda 360 haya finalizado.



11. La siguiente ventana que componente han sido instalados correctamente.

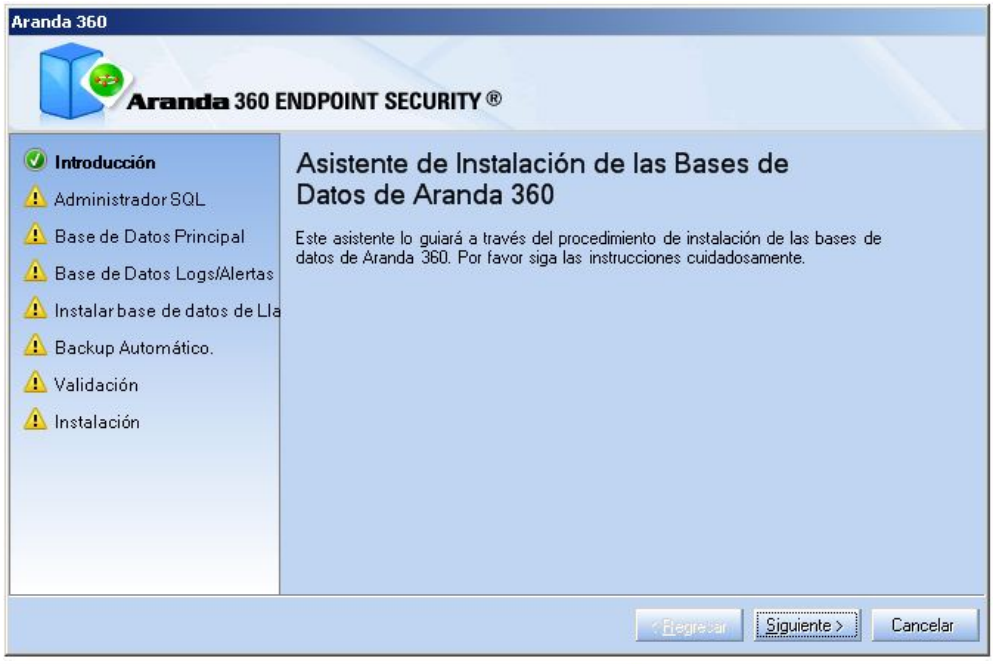
    Haga Clic en el botón finalizar para completar la instalación de Aranda 360.



Asistente de instalación de la base de datos

Para la instalación de la base de datos, siga los siguientes pasos:

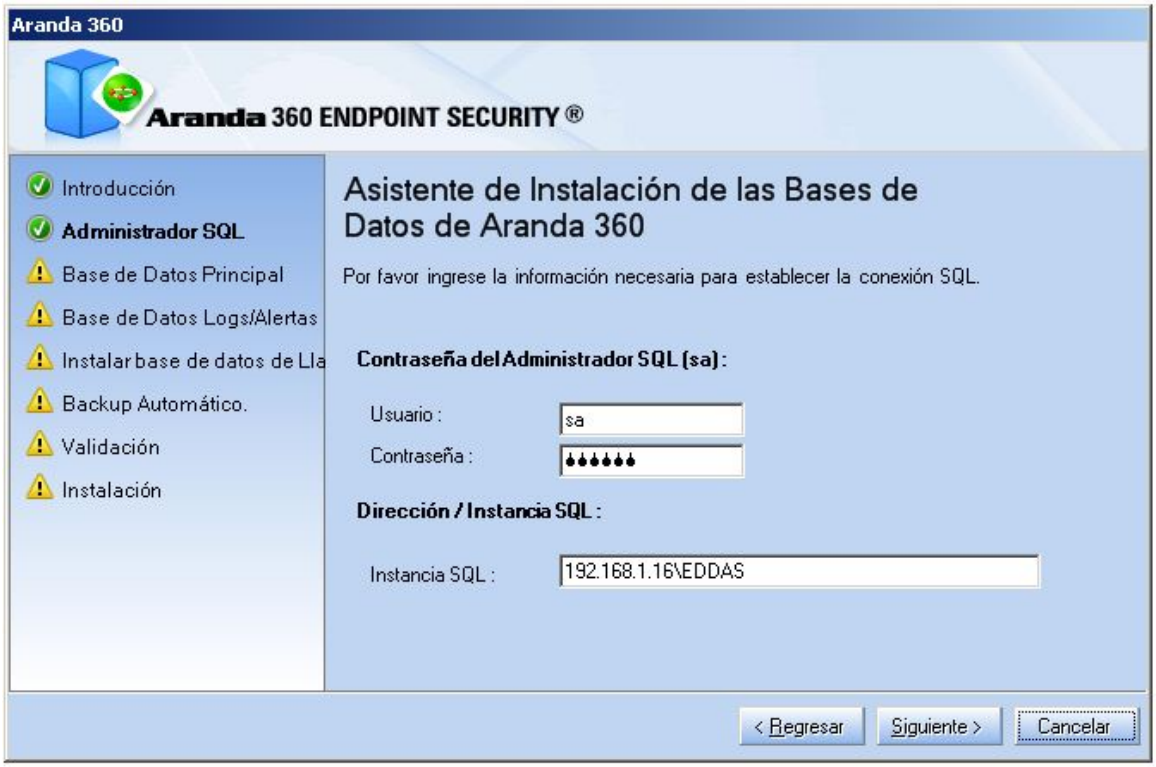
1. Después de instalar Aranda 360, el asistente de la base de datos se abrirá. Haga Clic en siguiente.



2. Para conectarse a la base de datos, digite:

- La cuenta de usuario del administrador.
- La contraseña de la cuenta.
- La instancia de la base de datos.

Haga Clic en siguiente.



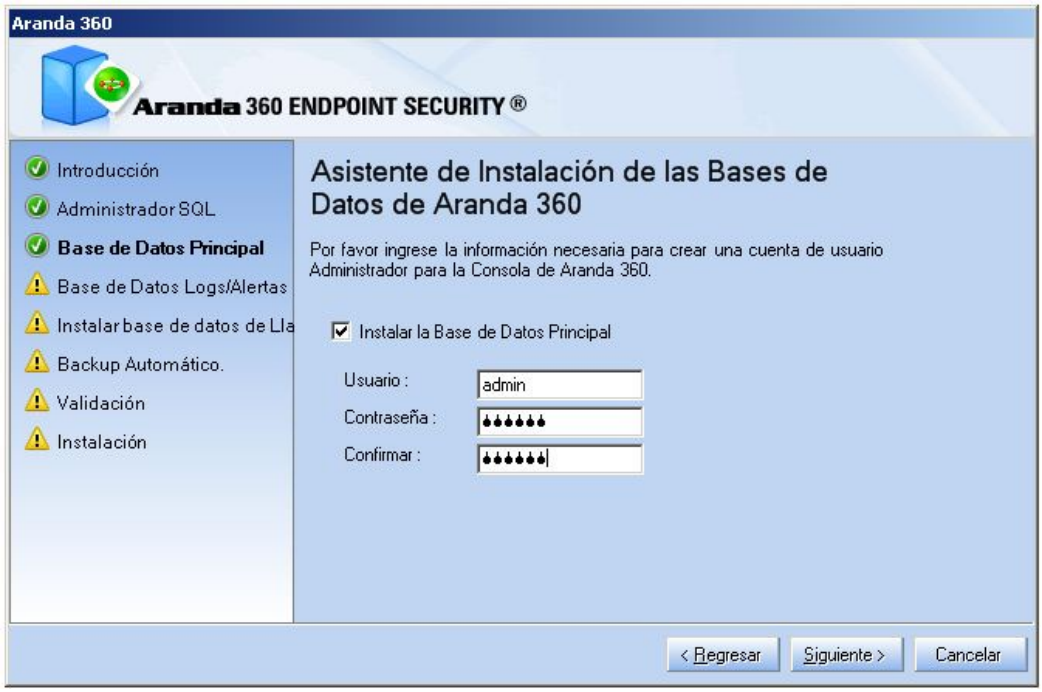
Para definir la instancia de la base de datos, existen dos métodos:

- **Método 1:**
  Si el servidor SQL utiliza un Puerto fijo (ejemplo: 1433), defina el puerto SQL en el campo instancia con cualquiera de las siguientes formas:
  - SqlServer,1433
  - 192.168.1.1,1433
- **Método 2:**
  Si el servidor SQL utiliza un Puerto fijo, defina la instancia SQL con cualquiera de las siguientes formas:
  - SqlServer\EDDAS
  - 192.168.1.1\EDDAS

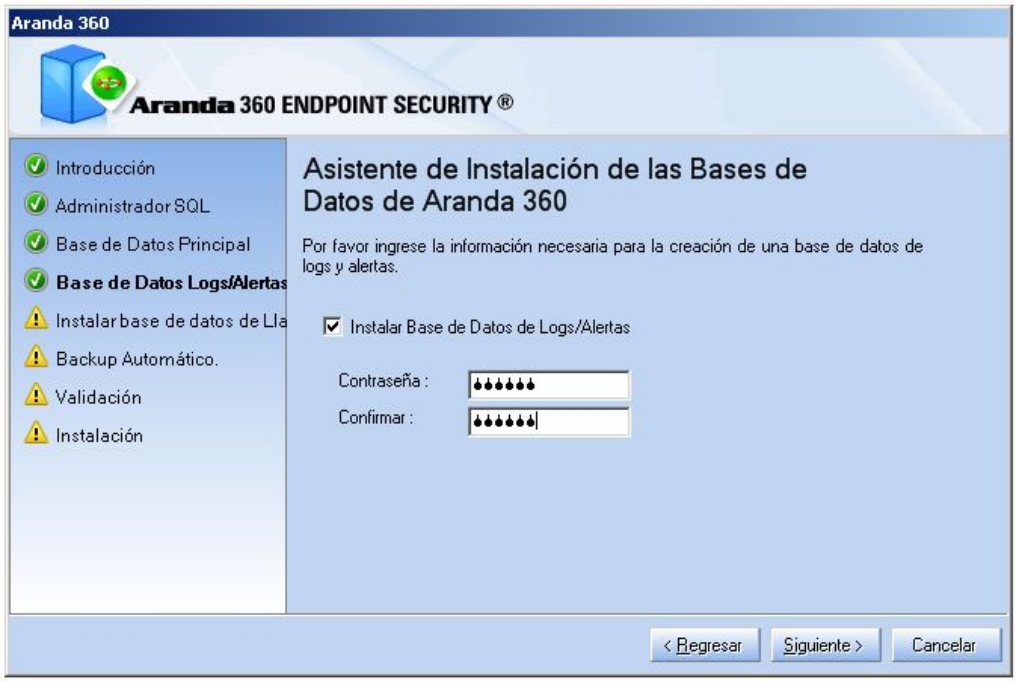
  Método 2 aplica también cuando el servidor SQL utiliza un puerto fijo. Pero, declarando una instancia requiere instalar el servicio SQL Browser.

3. Para crear una cuenta de Administrador dedicada a la base de datos principal:

- Marque la casilla Instalar base de datos principal.
- Digite la contraseña.
- Confirme la contraseña.
- Haga clic en siguiente.

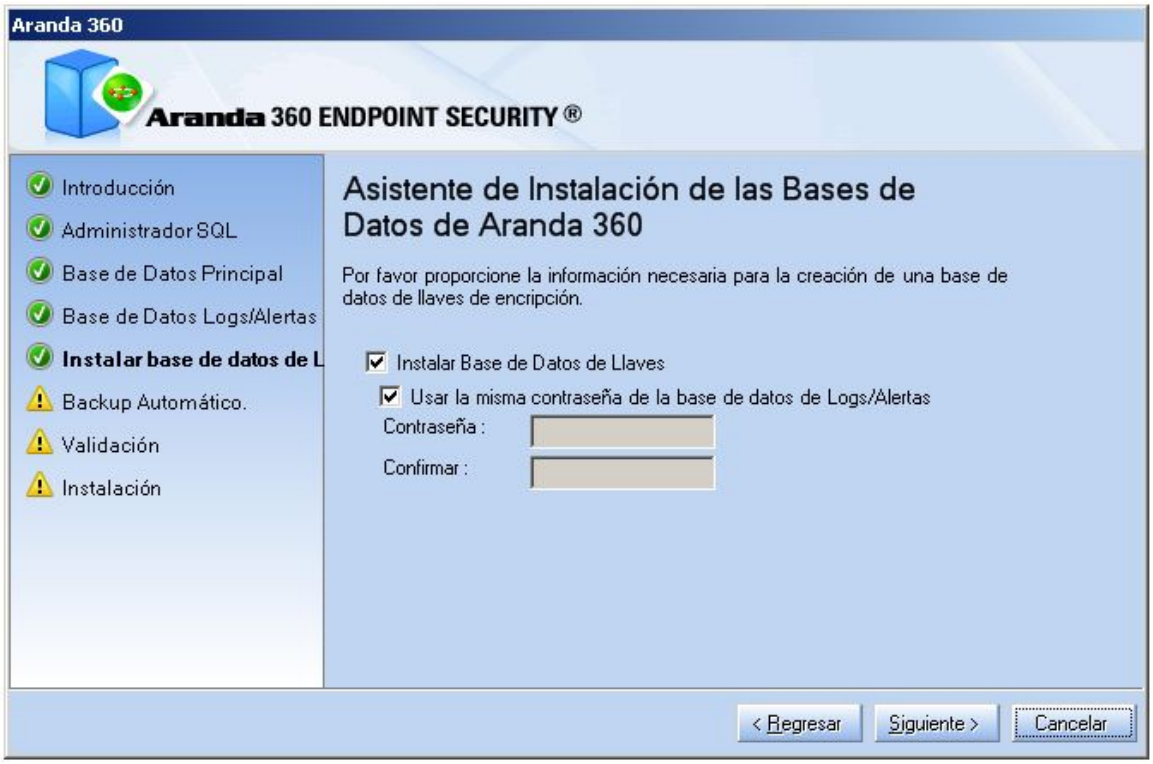


4. Para habilitar el reporte de alertas:
    - Marque la casilla Instalar Alertas de la base de datos.
    - Digite la contraseña.
    - Confirme la contraseña.
    - Haga clic en siguiente.



5. Para habilitar la cuenta de la base de datos:

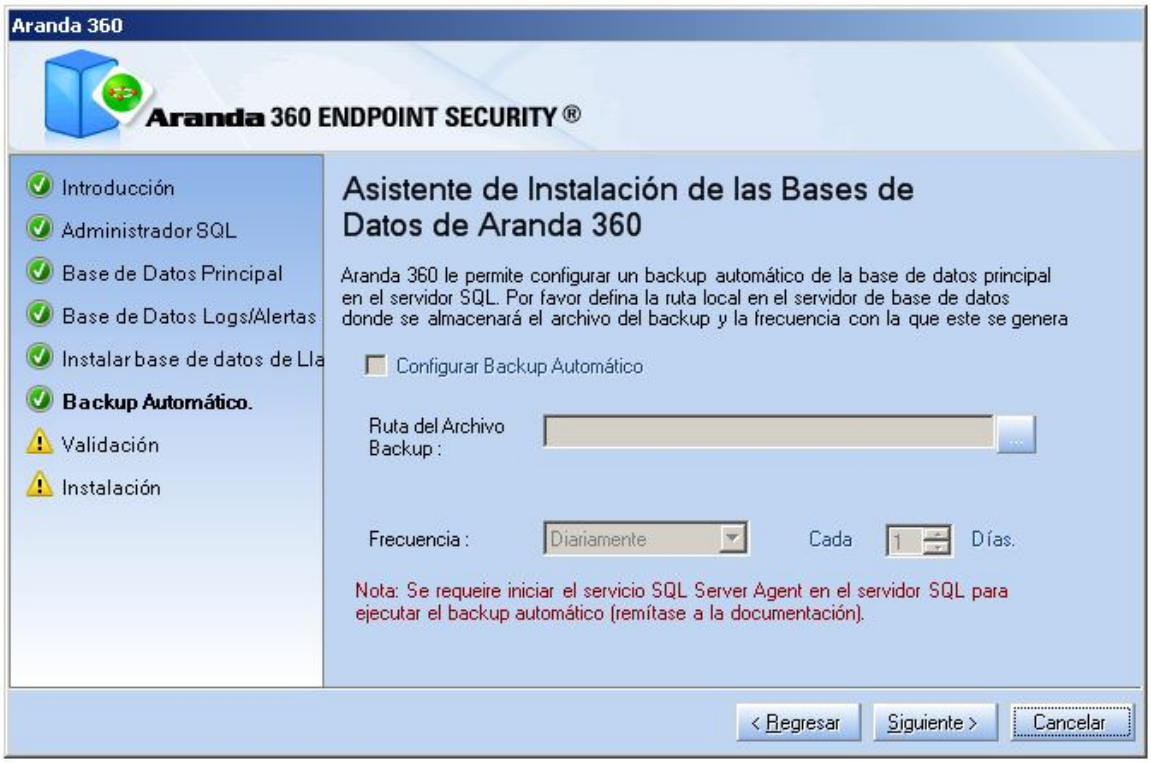
- Marque la casilla Instalar Clave.
- Marque la casilla usar la misma contraseña para la cuenta de alertas
- Haga clic en siguiente.



- En caso de ser necesario, es posible seleccionar una contraseña diferente para la clave de la base de datos. Para ello, desmarque Usar la misma contraseña para la cuenta de alertas.

6. Para guardar automáticamente la base de datos principal del Servidor, siga los siguientes pasos:

   - Marque la casilla Copia de seguridad automática de la base de datos
   - Digite la ruta del archivo de la copia de seguridad.
   - Seleccione la frecuencia de la copia de seguridad.
   - Haga clic en siguiente.



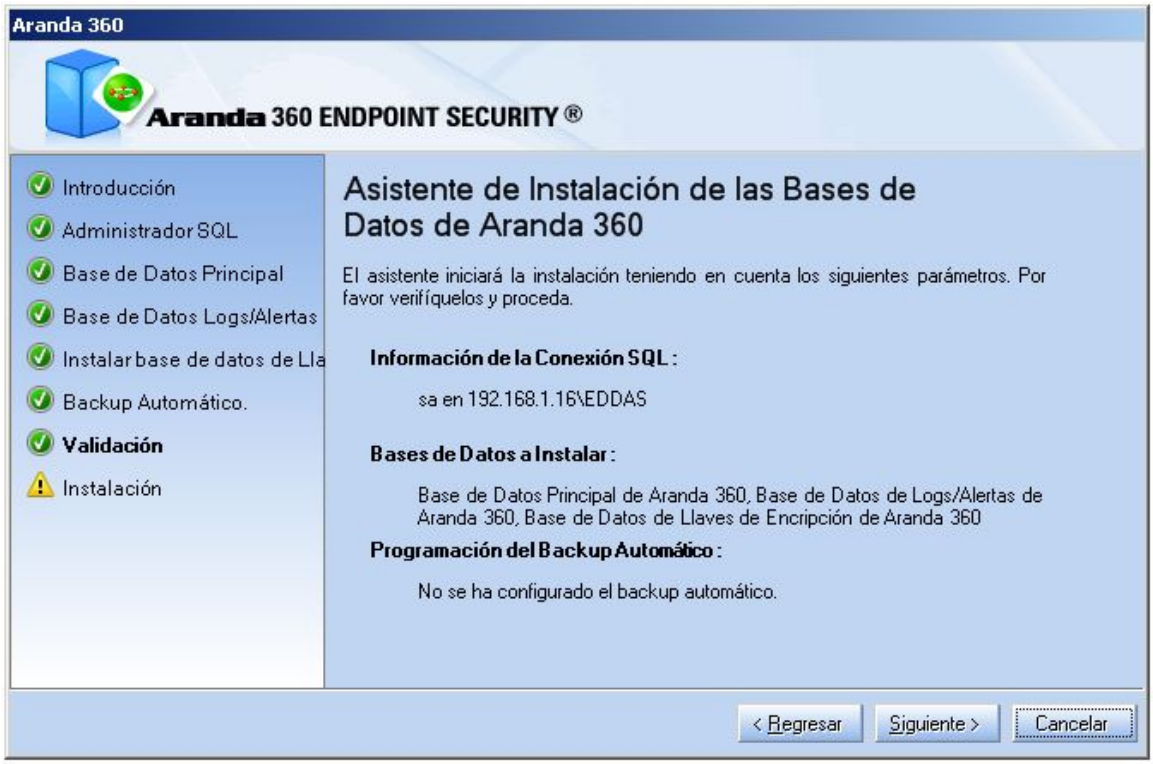
- Esta característica está disponible si se tiene acceso al servicio SQL SERVER AGENT [EDDAS.

Para realizar copia de seguridad automática, es necesario lanzar el servicio SQL SERVER AGENT antes de finalizar este paso.

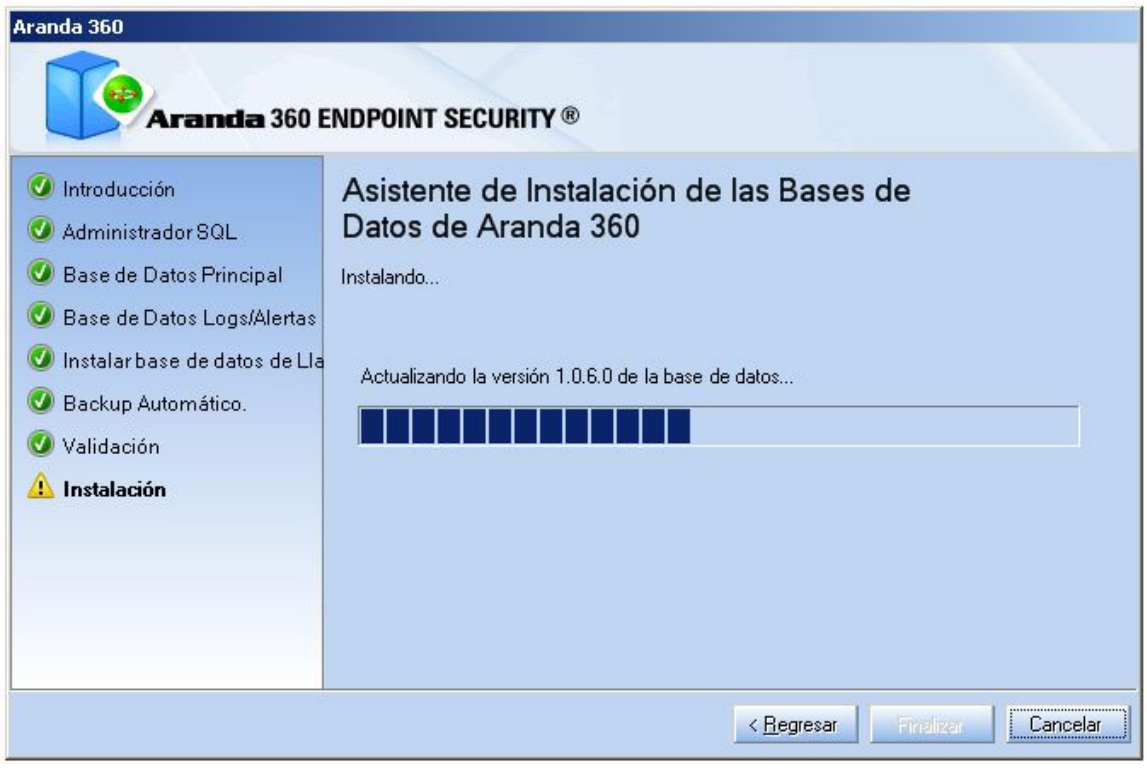
- Para realizar la copia de seguridad de la base de datos en otro directorio diferente al que está por defecto.
  (ejemplo: .\Mssql\Backup), asigne privilegios de lectura/escritura al grupo de seguridad SQLServer2005MSSQLUser$ServerName$SQLInstance.

7. La siguiente ventana muestra un resumen de toda la configuración definida.

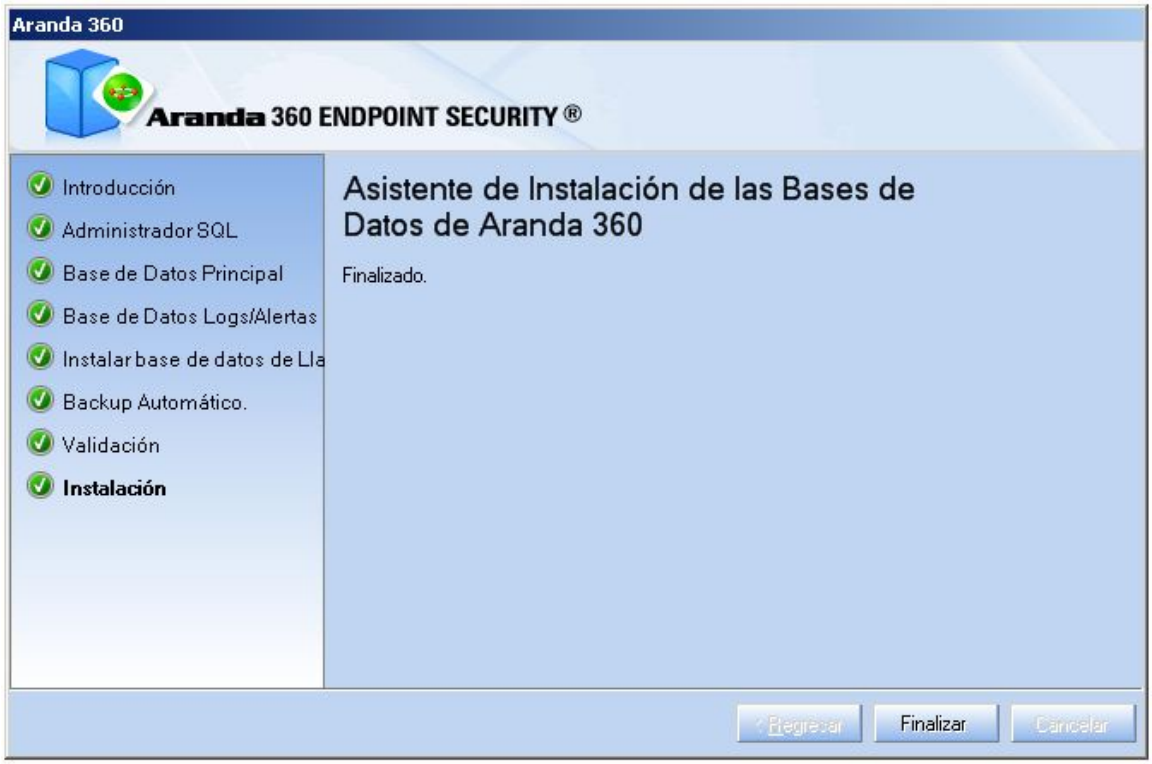
Haga clic en siguiente para validar la configuración.



8. Espere un hasta que el proceso de instalación haya finalizado.



9. Haga clic en finalizar para terminar la instalación.

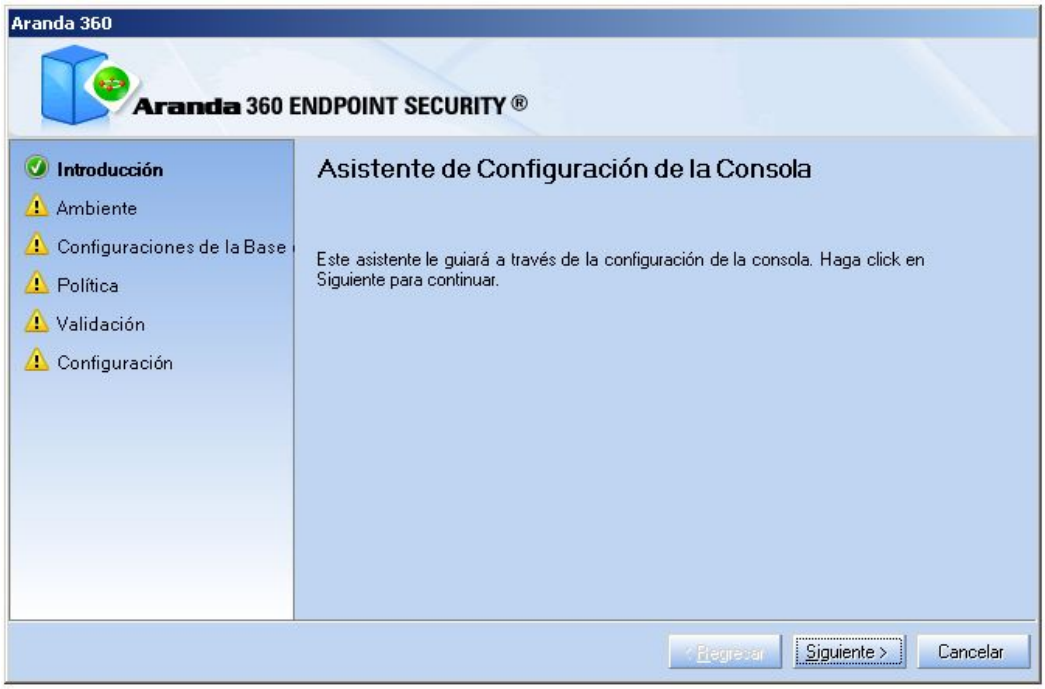


Asistente de configuración de ambientes

Para configurar la consola de administración y crear un ambiente operativo, siga los siguientes pasos:

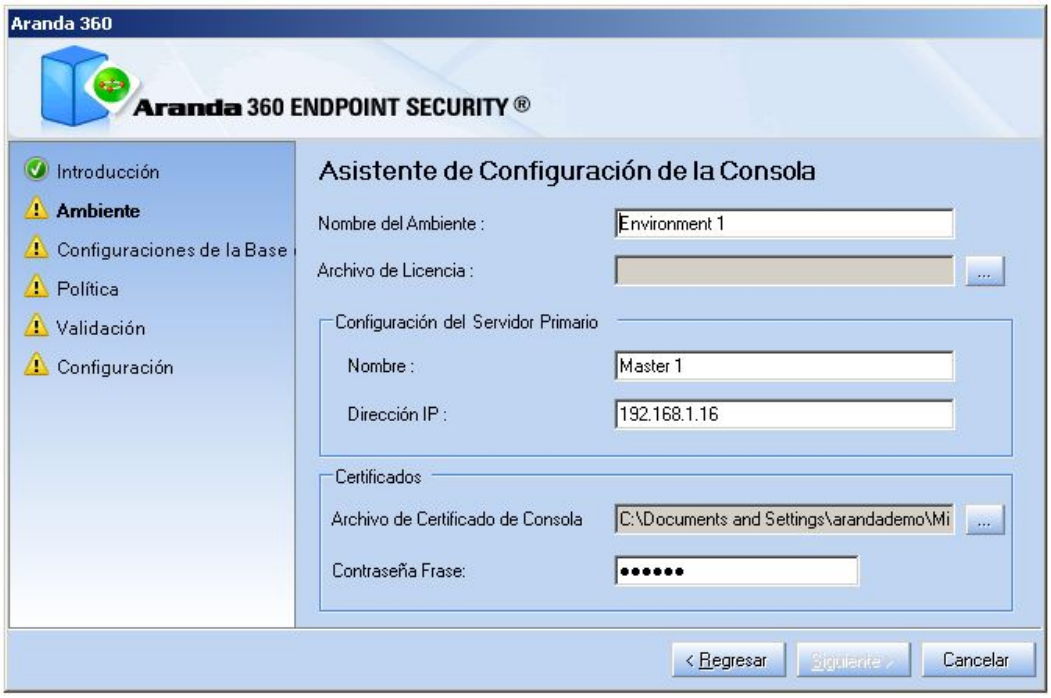
1. Después de instalar la Base de datos, el asistente de configuración se abrirá.

Haga clic en siguiente.

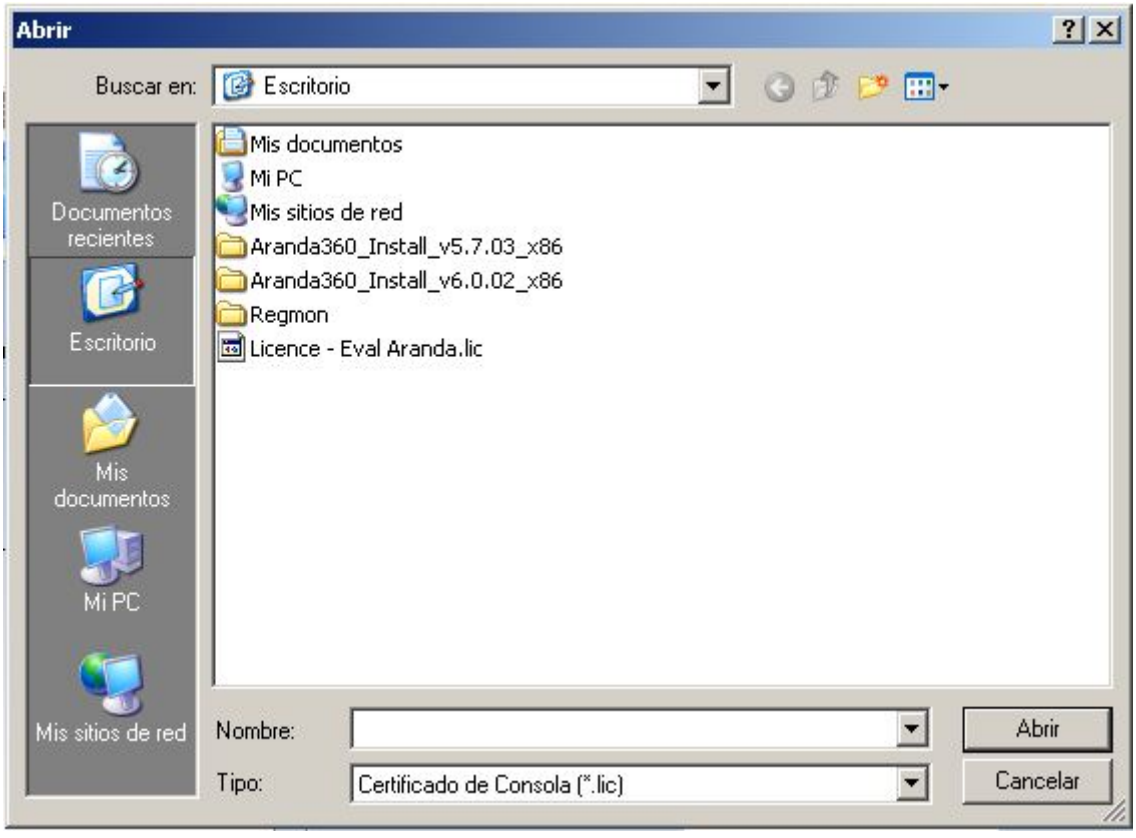


2. Para definir el ambiente, digite la siguiente información y haga clic en siguiente:

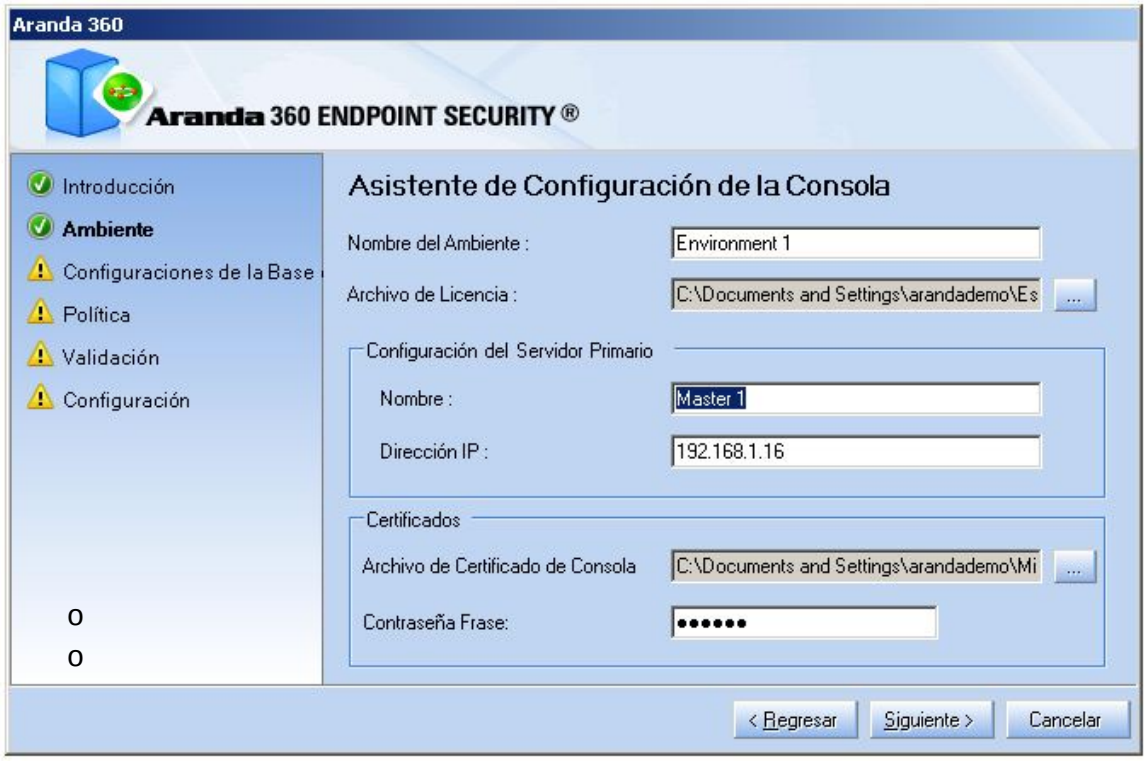
- Digite el nombre del ambiente.



- Seleccione la licencia a usar

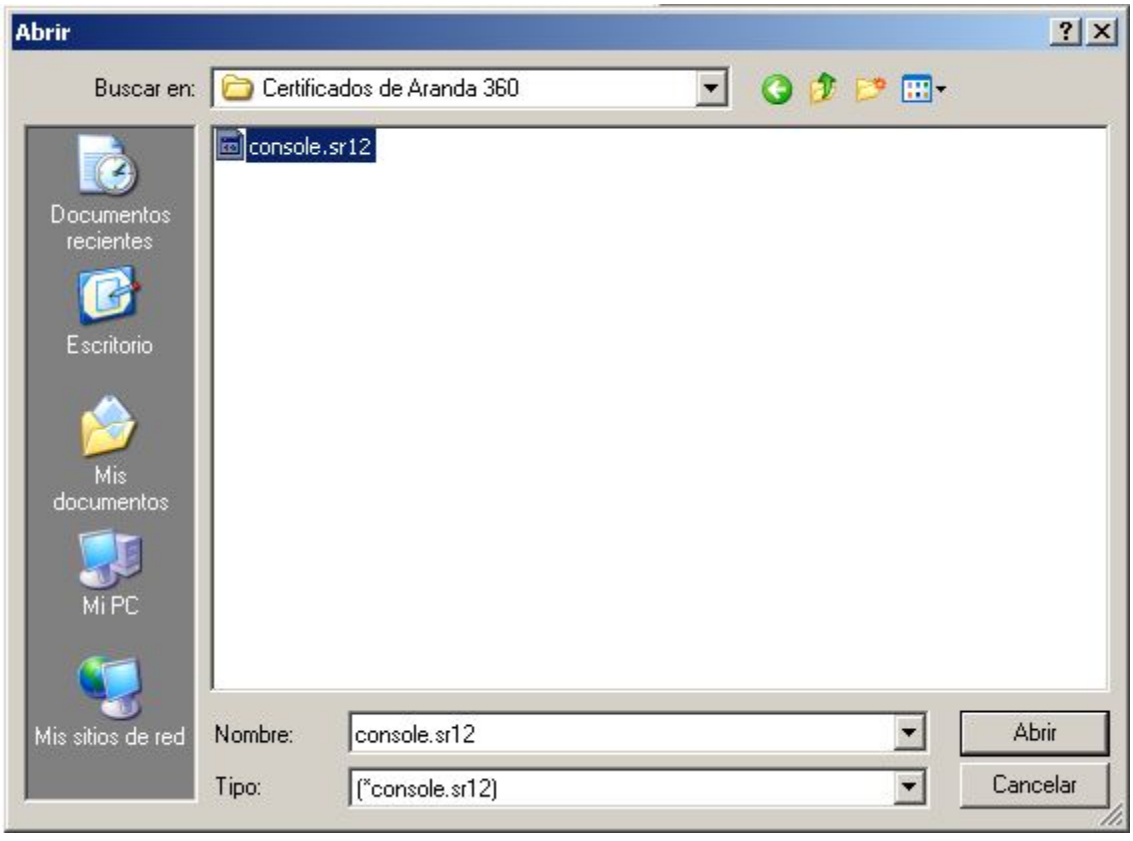


- Digite el nombre del servidor principal
- Digite la dirección IP del servidor maestro. .



- o
- o

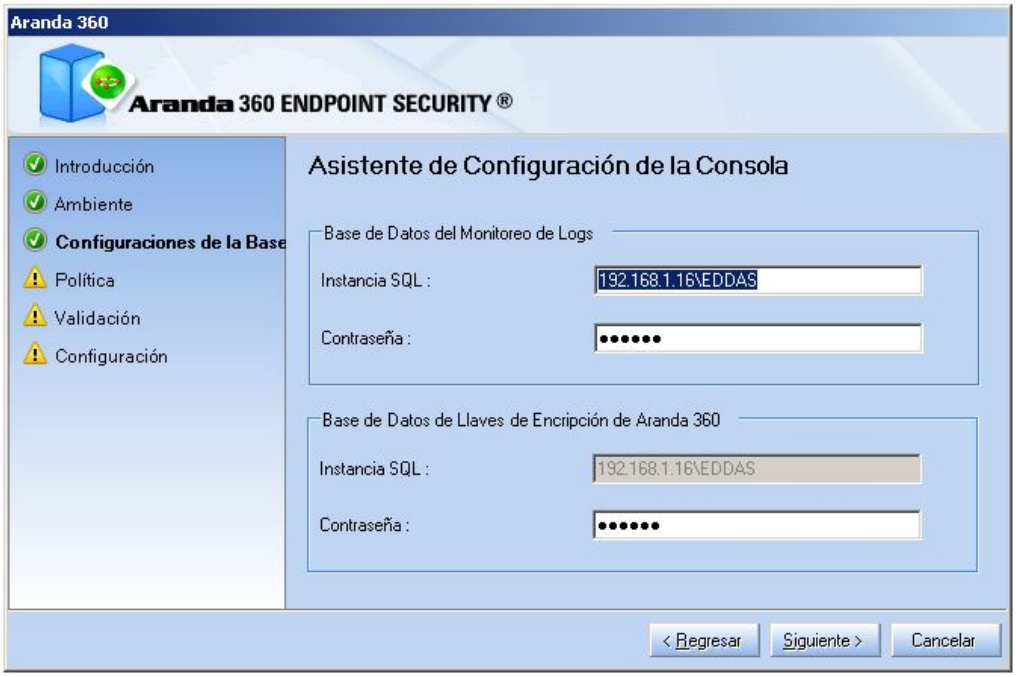
- o Seleccione el directorio de salida para los certificados de la consola



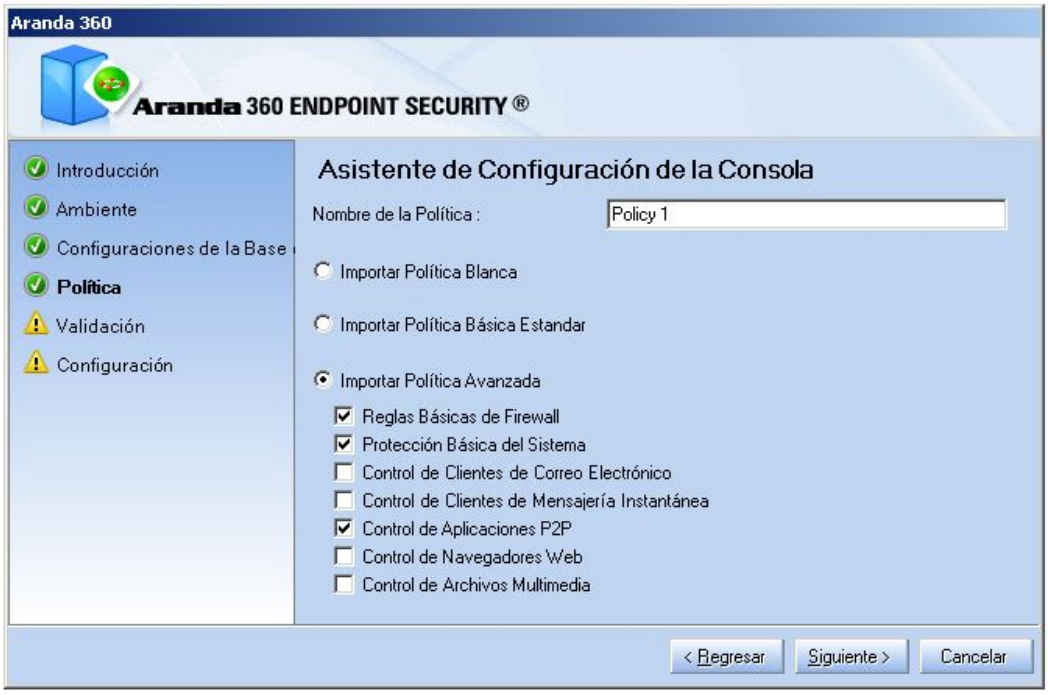
- o Digite la frase de contraseña asociada al certificado de la(s) consola(s) generado al instalar Aranda 360.

3. Para configurar la conexión entre la base de datos y la consola, digite la contraseña de la base de datos que definió al instalar Aranda 360:
   - Alerta de la base de datos.
   - Clave de la base de datos.

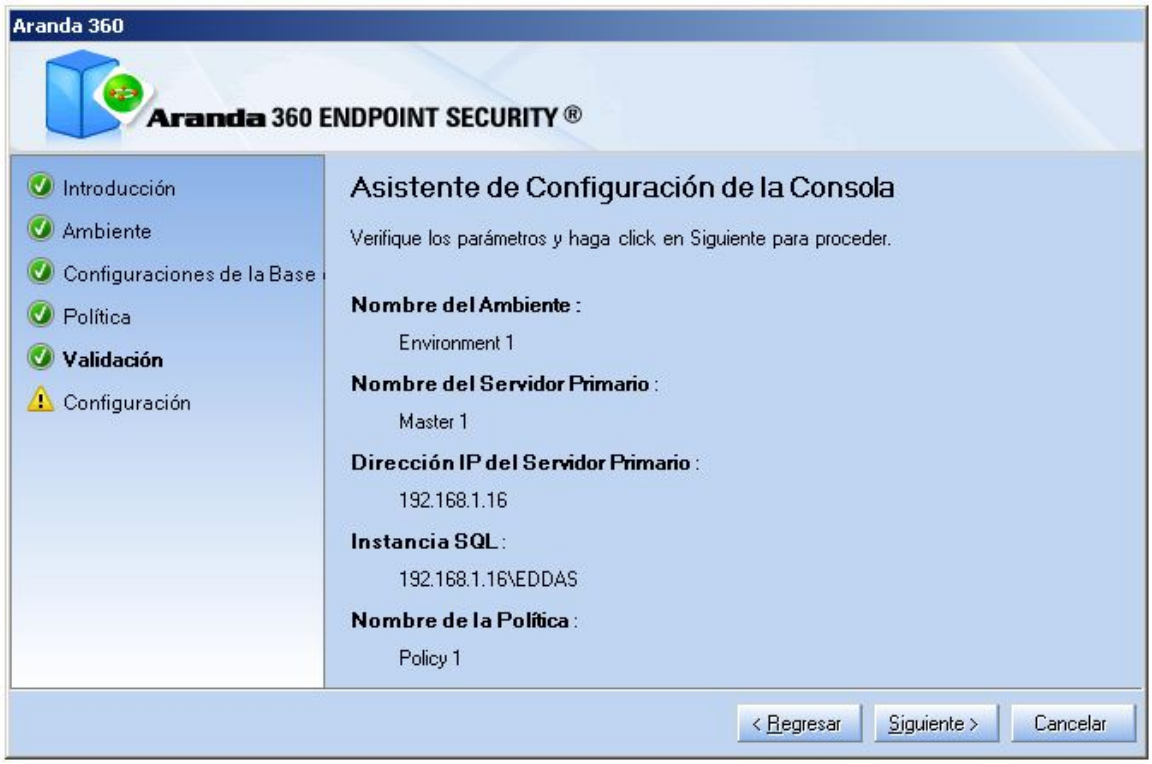
   Haga clic en siguiente.



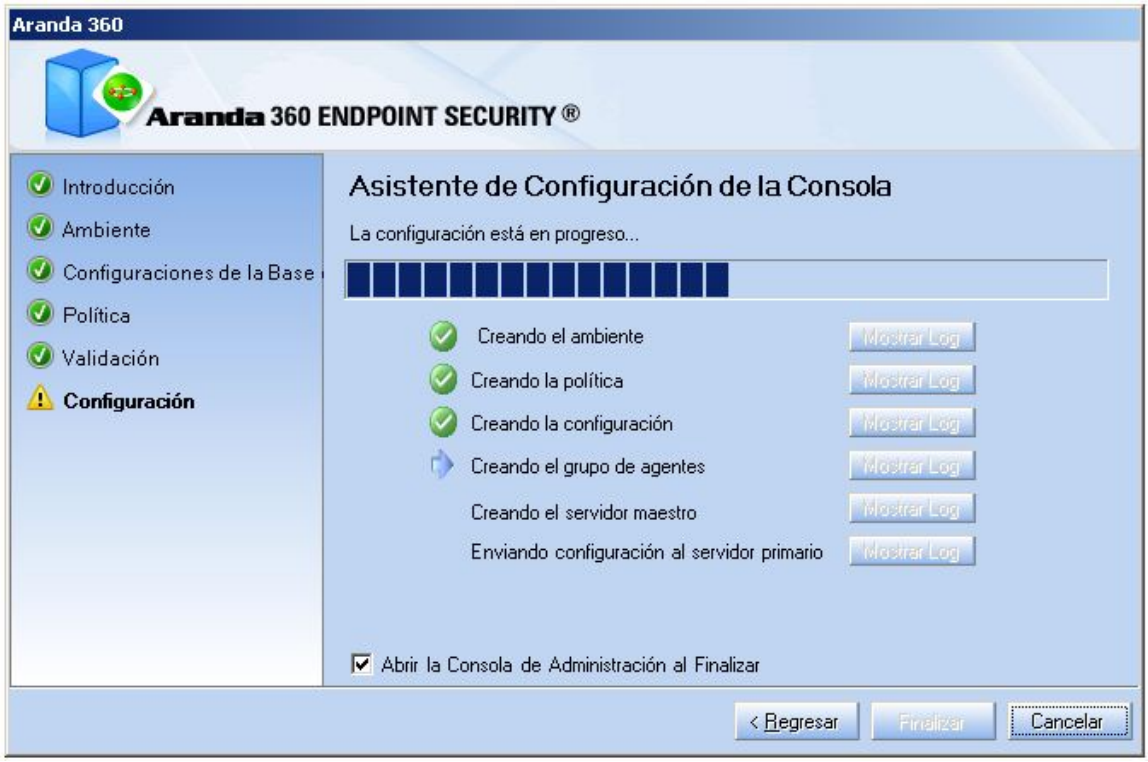
4. Para definir las políticas de seguridad, marque las opciones requeridas.
   Haga clic en siguiente.



5. La siguiente ventana muestra un resumen de toda la configuración definida. Haga clic en siguiente para validar la configuración.



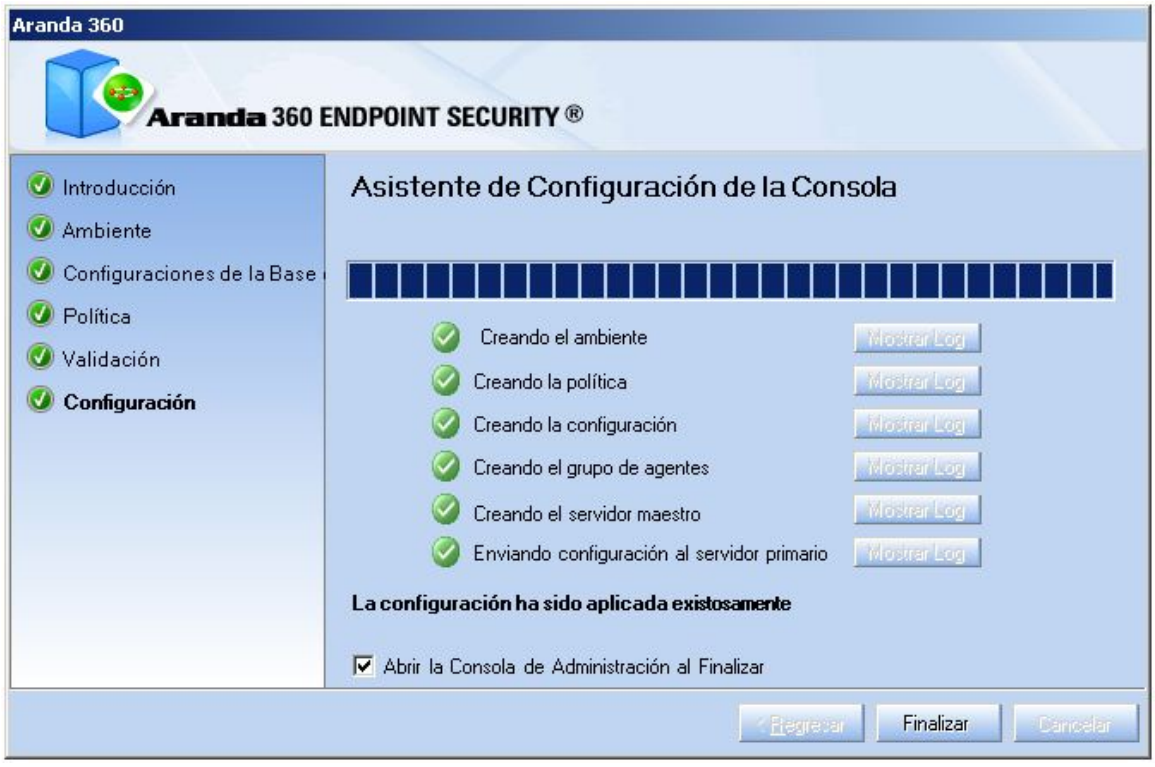
6. La siguiente ventana muestra que la configuración está en progreso



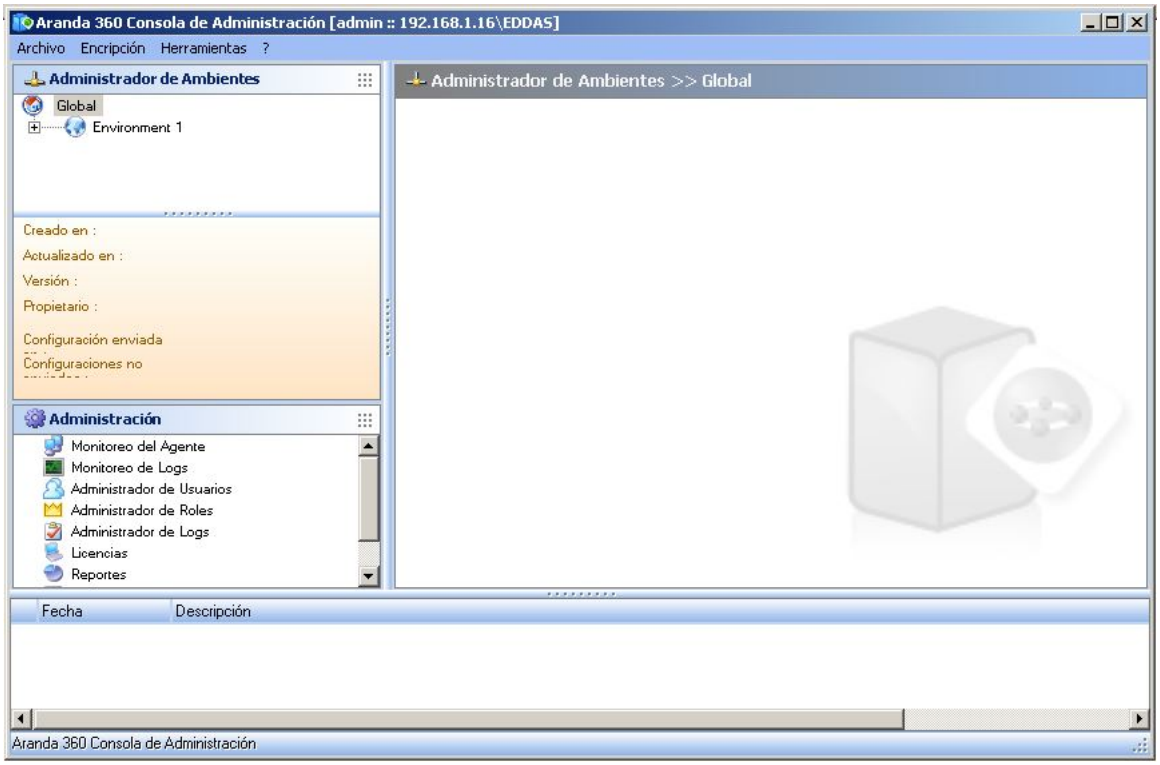
- La casilla Abrir la consola al finalizar está marcada por defecto. Si no desea abrir la consola, desmarque esta opción.

7. Haga clic en sí, si desea instalar el certificado.

8. La siguiente ventana muestra que el ambiente fue instalado correctamente.



9. La siguiente ventana aparecerá si previamente se seleccionó la opción de abrir la consola al finalizar la instalación.



Asistente de distribución del agente

Para la implementación de los agentes, siga los siguientes pasos:

1. Después de configurar el ambiente, aparecerá la siguiente ventana. Haga clic en siguiente.

2. Digite los parámetros de conexión:

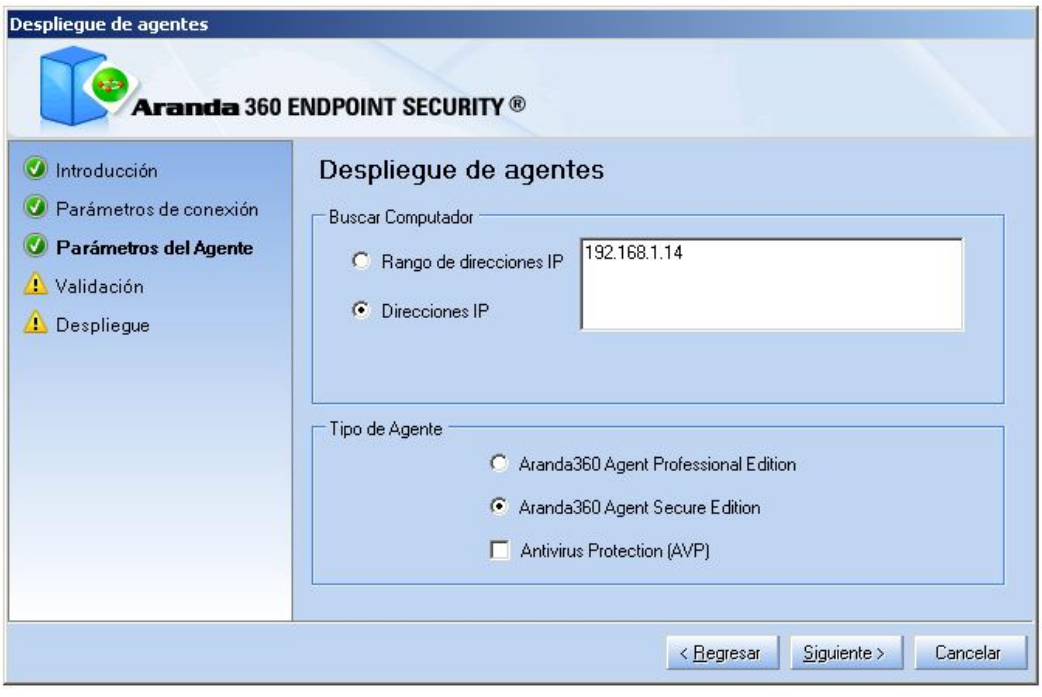
- Nombre del dominio (o grupo de trabajo
- Nombre de usuario.
- Contraseña.
- Dirección IP del servidor.
- Número del puerto del servidor Web instalado con el servidor Aranda 360.

- La cuenta debe tener privilegios de Administrador en la estación de trabajo.

Haga clic en siguiente.

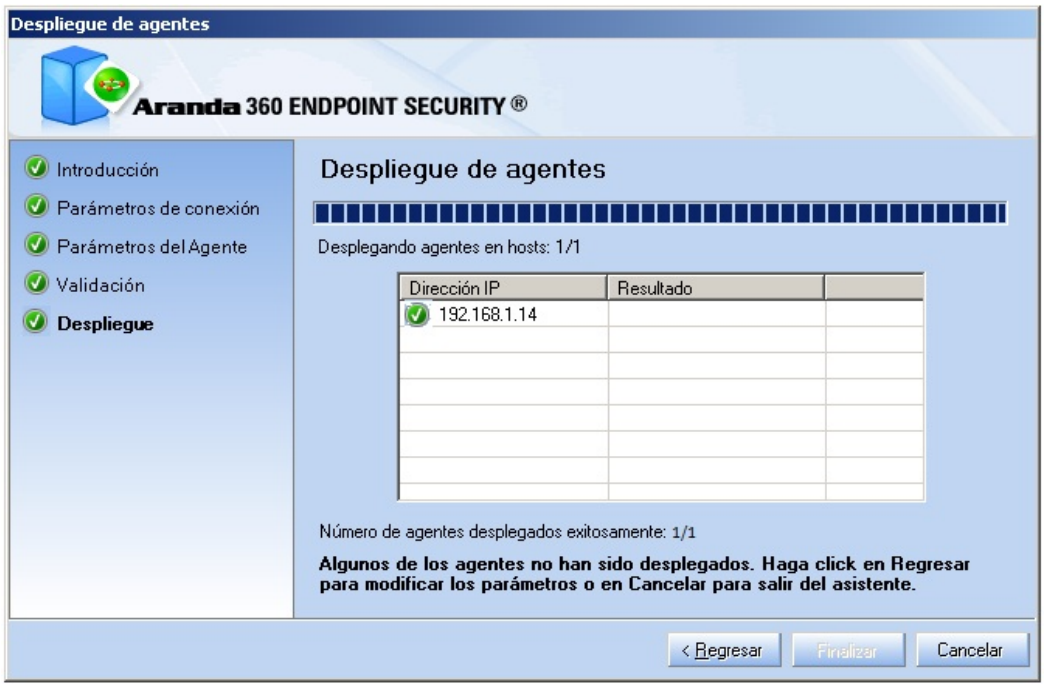
3. Configure los parámetros del agente:

- Defina la lista en las cuales va instalar el agente, por:
  - Rango de direcciones IP.
  - Dirección IP.
- Seleccione el paquete de Aranda 360 a instalar:
  - Aranda 360 Agent Professional Edition.
  - Aranda 360 Agent Secure Edition.
- Haga clic en siguiente



4. La siguiente ventana muestra un resumen de toda la configuración.
   Clic en siguiente para validar la configuración.

5. Aparecerá la siguiente ventana
   Espere hasta que la implementación del agente se complete.
   Haga Clic en finalizar.



- Para utilizar el asistente de implementación del agente, asegúrese de:

- Las máquinas donde se va a implementar el agente puedan acceder al servicio Web de Aranda 360.
- Las estaciones de trabajo puedan acceder a Herramientas administrativas.

Si otra aplicación o un usuario ya tienen acceso a Herramientas administrativas en una máquina en la que va ser distribuido el agente, la implementación fallará.

En caso de algún problema, verifique que el acceso no está siendo bloqueado por un firewall y este deshabilitado Uso Compartido Simple de Archivos.

INSTALACIÓN MANUAL DE ARANDA 360

REQUERIMIENTOS

Cabe señalar:

- D el firewall de Microsoft XP debe ser deshabilitado antes de instalar el agente.
- el puerto TCP 16006 debe ser abierto para permitir conexiones al Servidor Aranda 360.

PROCEDIMIENTO

La instalación manual de Aranda 360 se compone de seis pasos:

1. Instalando el servidor principal.
2. Instalando el servidor secundario.

   - Los servidores secundarios pueden ser instalados en cualquier momento después de instalar el servidor principal.

3. Instalando la consola.
4. Instalando la base de datos
5. Configurar el ambiente (consola).
6. Instalando los agentes.

Instalando el servidor principal

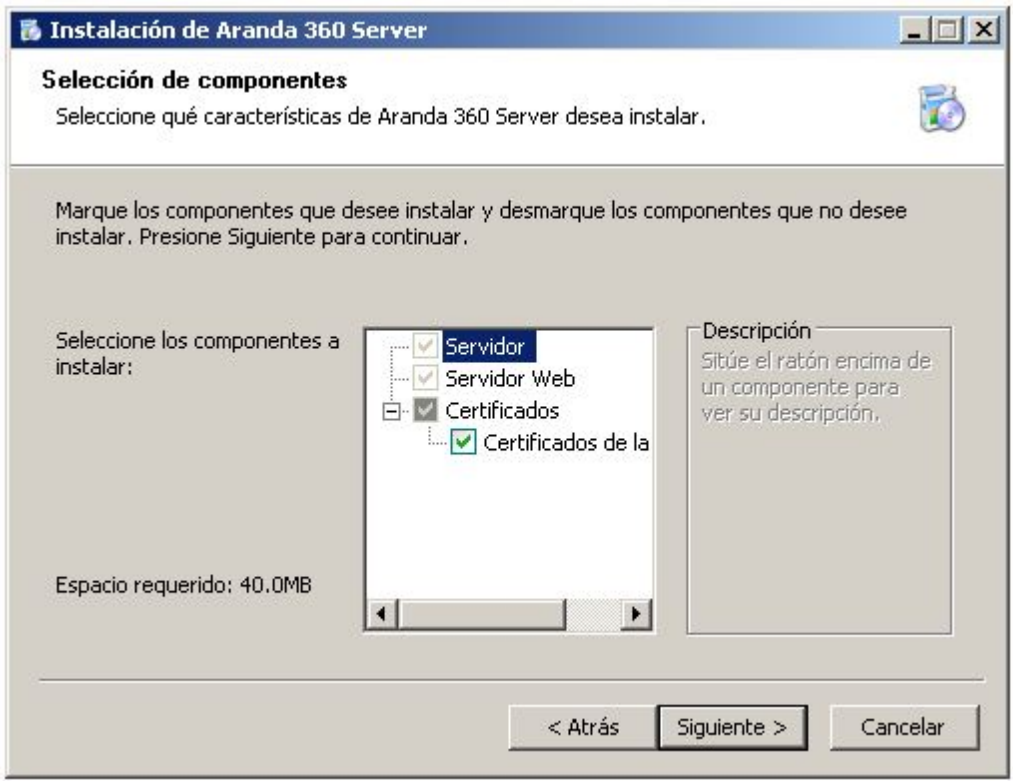
- Si tiene la opción Protección Antivirus (AVP), debe usar el instalador server.exe, el cual incluye ésta opción.

Para instalar el servidor principal con el instalador, siga los siguientes pasos:

1. Vaya a la carpeta de bin y haga doble clic en el archivo server.exe.
   El instalador del servidor Aranda 360 arrancará.

2. Seleccione el idioma de instalación.

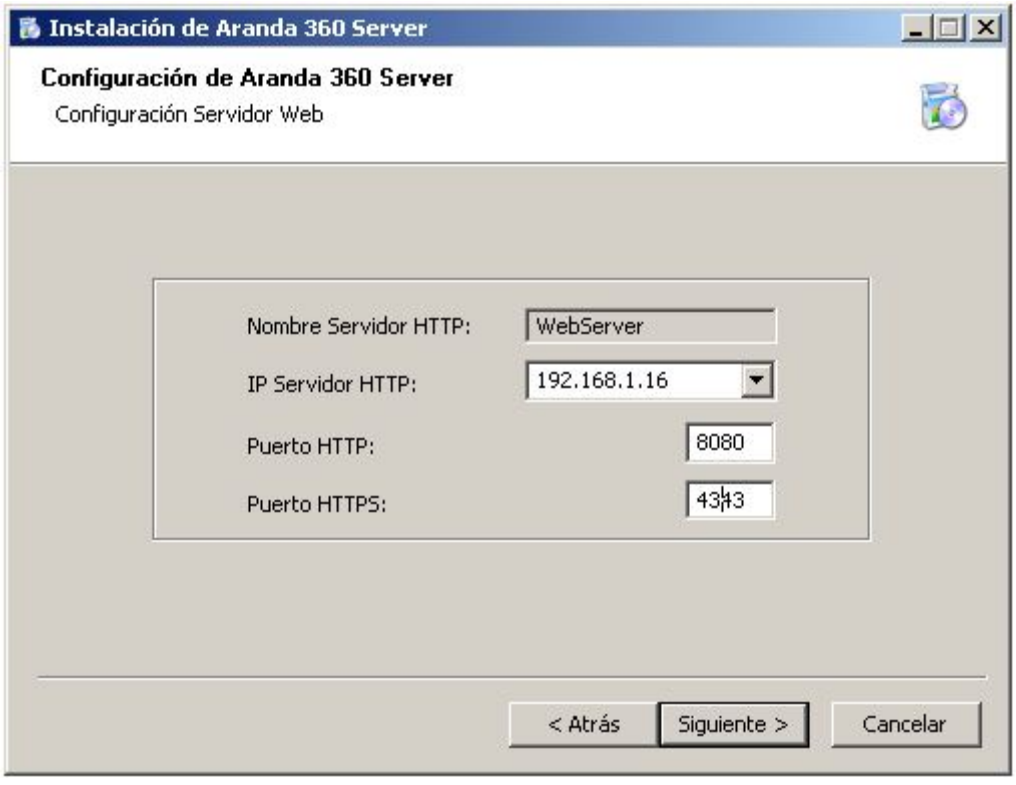
3. Seleccione los componentes a instalar.



Puede elegir lo siguiente:

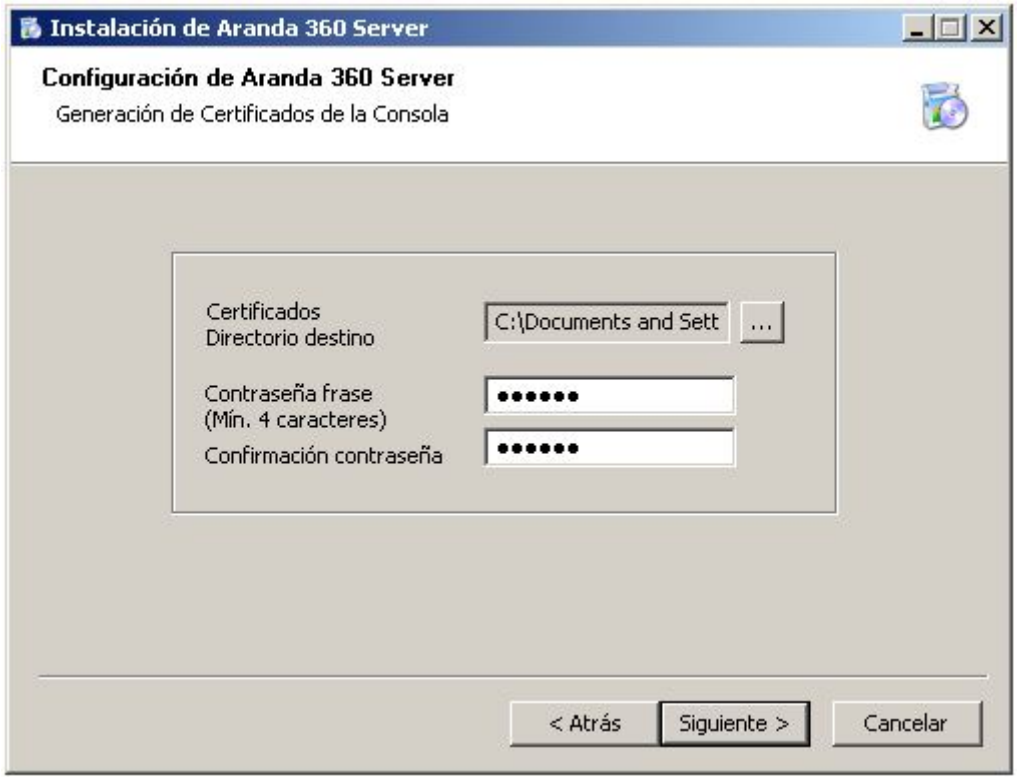
- El servidor Aranda 360 y el servidor web están marcados por defecto y deshabilitados para edición.
- El certificado de la consola.
- La base de datos MS SQL Server 2005 (Express Edition).
  La opción de la base de datos MS SQL Server 2005 puede ser desmarcada si prefiere hacer su instalación en una máquina diferente o si un servidor MS-SQL ya ha sido instalado para utilizarlo con Aranda 360.

4. Haga clic en siguiente para generar el certificado del servidor.
5. Digite la dirección IP y los puertos utilizados servidor Web embebido.
   El instalador le solicitará esta información si la opción de servidor web fue marcada.



Por defecto, los puertos 80 y 443 son utilizados. Estos valores deben cambiarse si el servidor web ya está usando dichos puertos.

6. Digite los parámetros para generar el certificado.



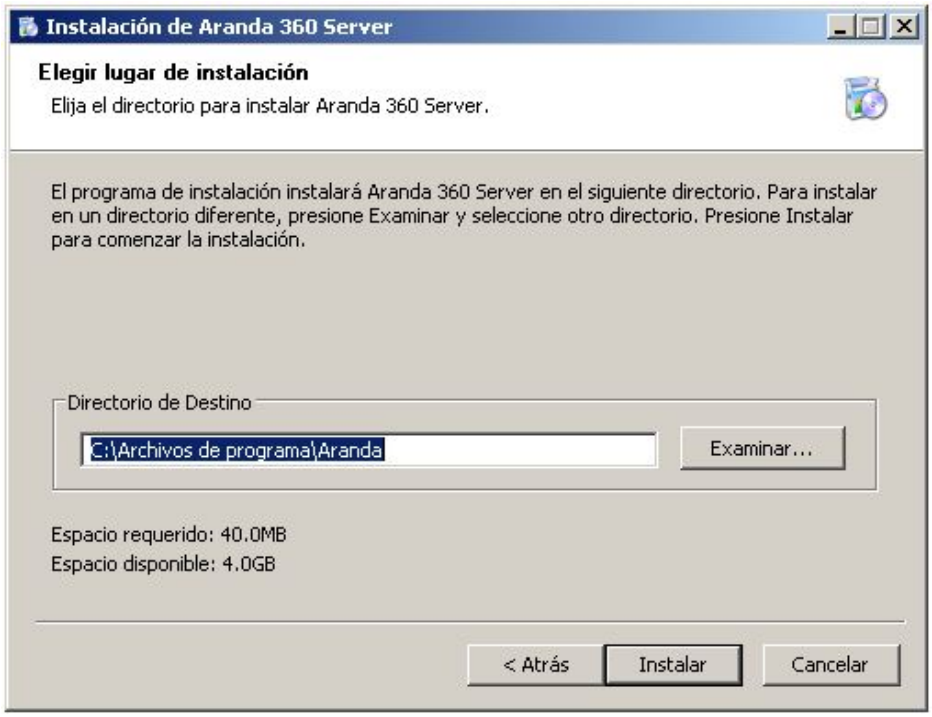
Esta opción aparecerá solo si la casilla de certificado de consola fue seleccionada.

Si es así, debe especificar el directorio de destino donde se crearán los certificados, así como la contraseña.

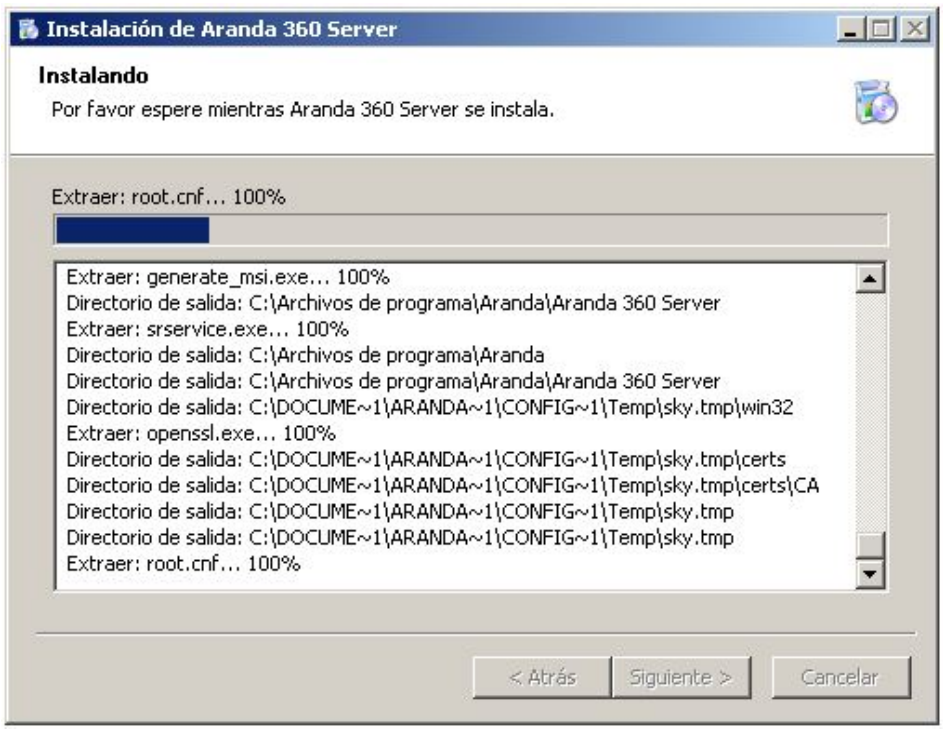
Se debe asegurar que éste directorio es accesible desde la máquina donde se va a instalar la consola, o si prefiere puede copiarlos en otro lugar donde la consola pueda acceder.

La contraseña es sensible a mayúsculas y minúsculas. Debe contener al menos cuatro caracteres alfanuméricos. Ésta también es requerida para acceder a la consola de administración.

7. Digite la contraseña de la cuenta de administrador de la base de datos.
   Esta opción aparecerá solo si la casilla de base de datos fue seleccionada.
8. Digite la ruta de instalación del servidor Aranda 360 server.
   Haga clic en instalar.

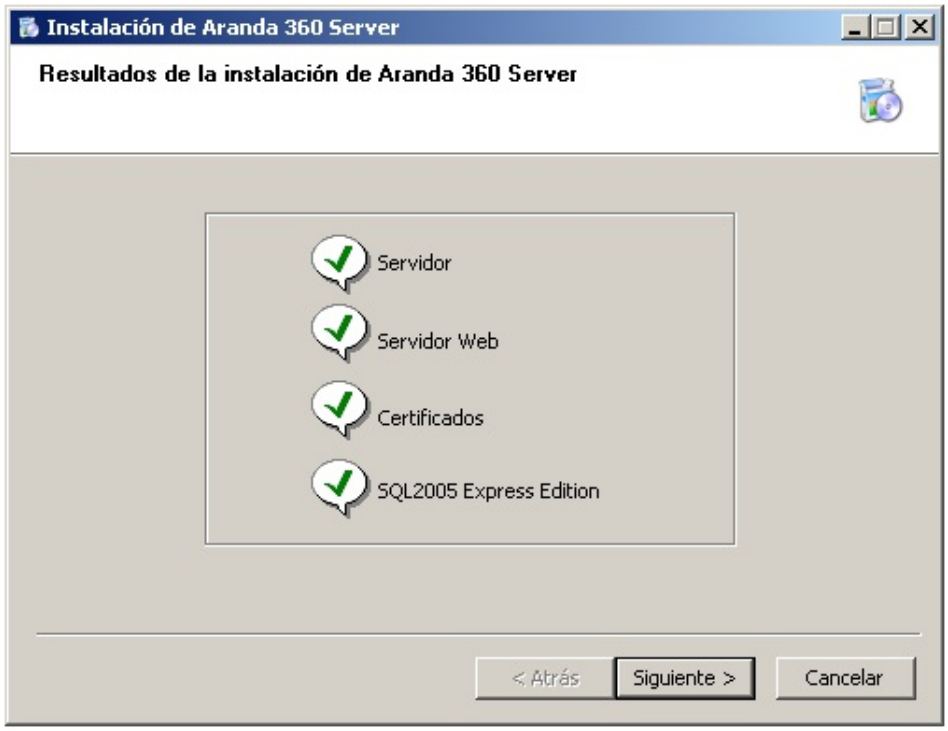


9. Espere un momento hasta que el proceso de instalación haya finalizado.

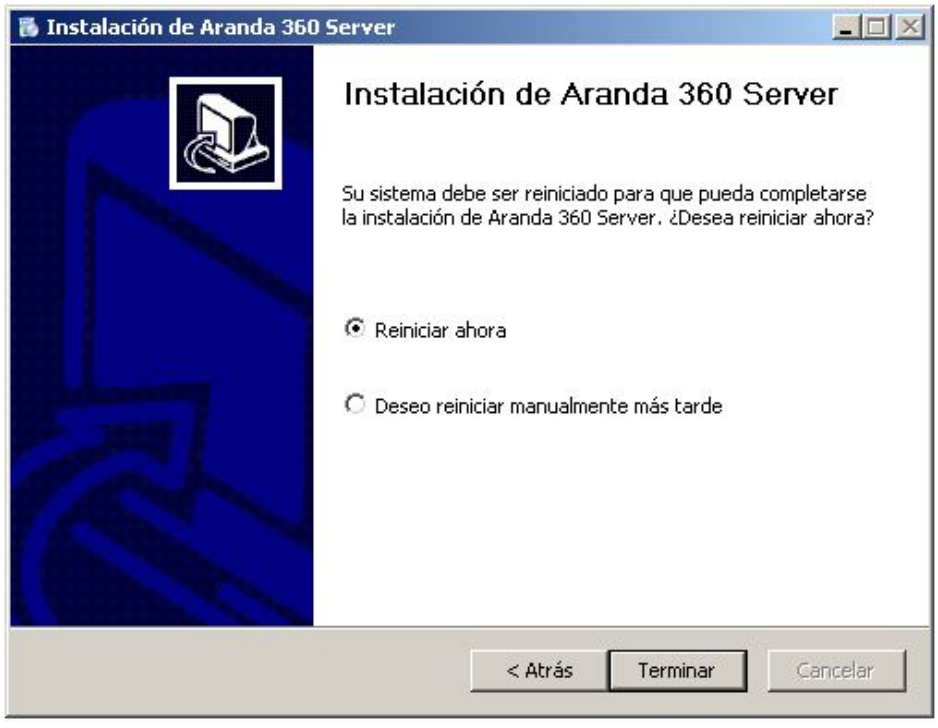


10. Verifique el reporte de instalación.

Este reporte mostrará el estado de instalación de los componentes seleccionados.



11. Reinicie la máquina para iniciar el servidor.



Instalando servidores secundarios

La instalación de servidores secundarios es opcional. Se utilizan para distribución de carga de las solicitudes entre agentes y servidores.

Además, aseguran una alta disponibilidad a nivel de implementación del servidor, en la medida que el servidor secundario automáticamente toma el rol del servidor principal en caso de que éste se detenga accidentalmente.

Número de servidores secundarios

El número de servidores secundarios depende de:

- Número de agentes distribuidos.
- Velocidad de la red.
- Tamaño de la configuración.
- Número de alertas y logs retornados.

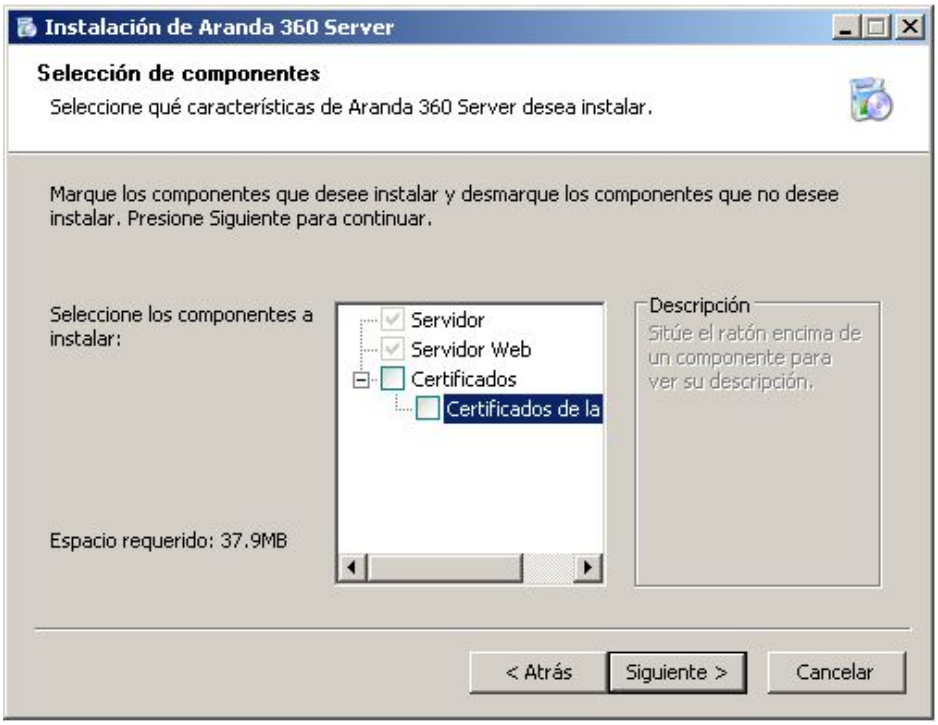
Procedimiento

La instalación del servidor secundario se realiza con el mismo instalador del servidor principal, para ello siga los siguientes pasos:

1. Vaya a la carpeta bin y haga doble clic sobre el archivo server.exe.
2. Seleccione el idioma de instalación.
   Haga Clic en OK.

3. Aparecerá una ventana con los siguientes componentes seleccionados por defecto y deshabilitados para edición:
   - El servidor Aranda 360.
   - El servidor Web (Apache), el cual es utilizado para la implementación los agentes en modo de descarga.
4. Desmarque la opción de Certificados, ya que éstos se generaron cuando el servidor principal fue instalado.

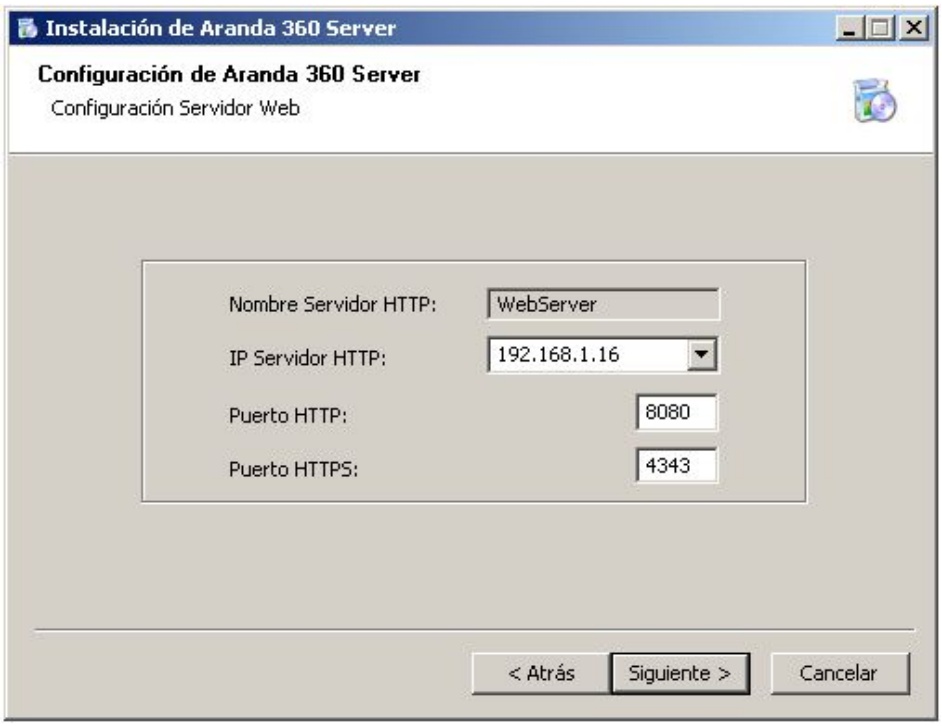
5. Desmarque la opción de base de datos MS SQL Server 2005 para consolidar toda la información retornada por los agentes en la misma base de datos del servidor principal.



6. Especifique la ruta de acceso de los dos archivos que contiene el certificado del servidor principal:
   - root.pem (Autoridad de certificación).
   - rootcert.pem (certificado).

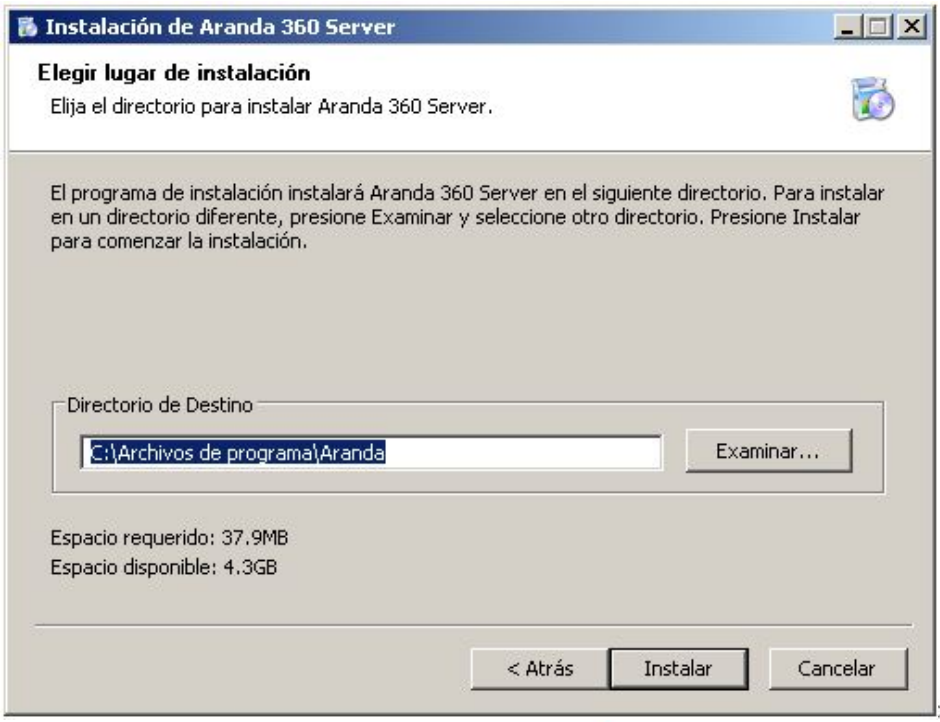
   Estos archivos fueron puestos en el director de instalación del servidor principal.

7. Digite la dirección IP del servidor principal y los puertos usados por el servidor Web.

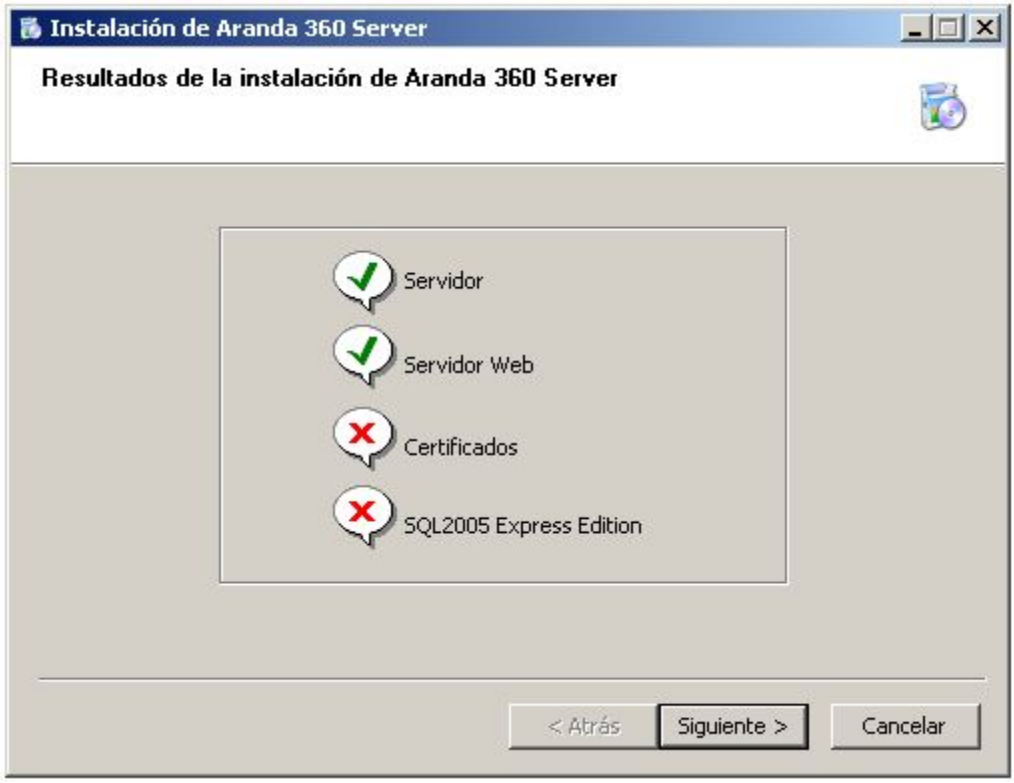


Por defecto, los puertos 80 y 443 son utilizados. Estos valores deben cambiarse si el servidor web ya está usando dichos puertos.

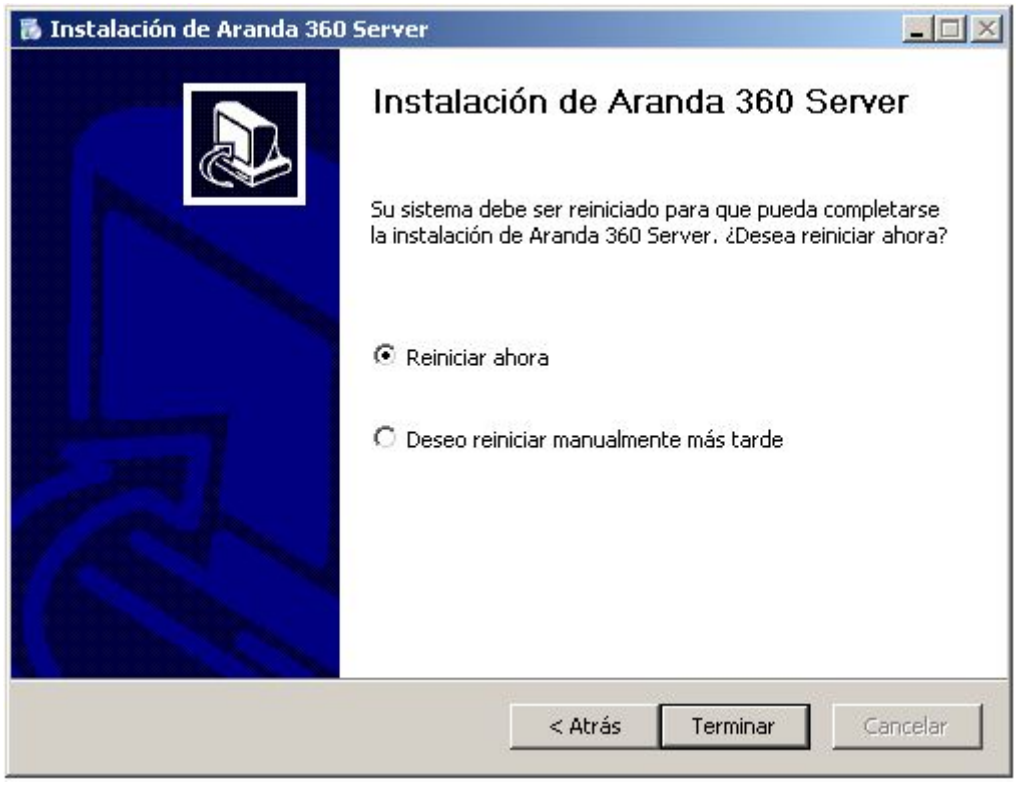
8. Defina la ruta de instalación del servidor Aranda 360.
Haga clic en instalar.



9. Verifique el reporte de instalación.
   Este reporte muestra el estado de instalación de los componentes seleccionados.



10. Reinicie la máquina para iniciar el servidor.

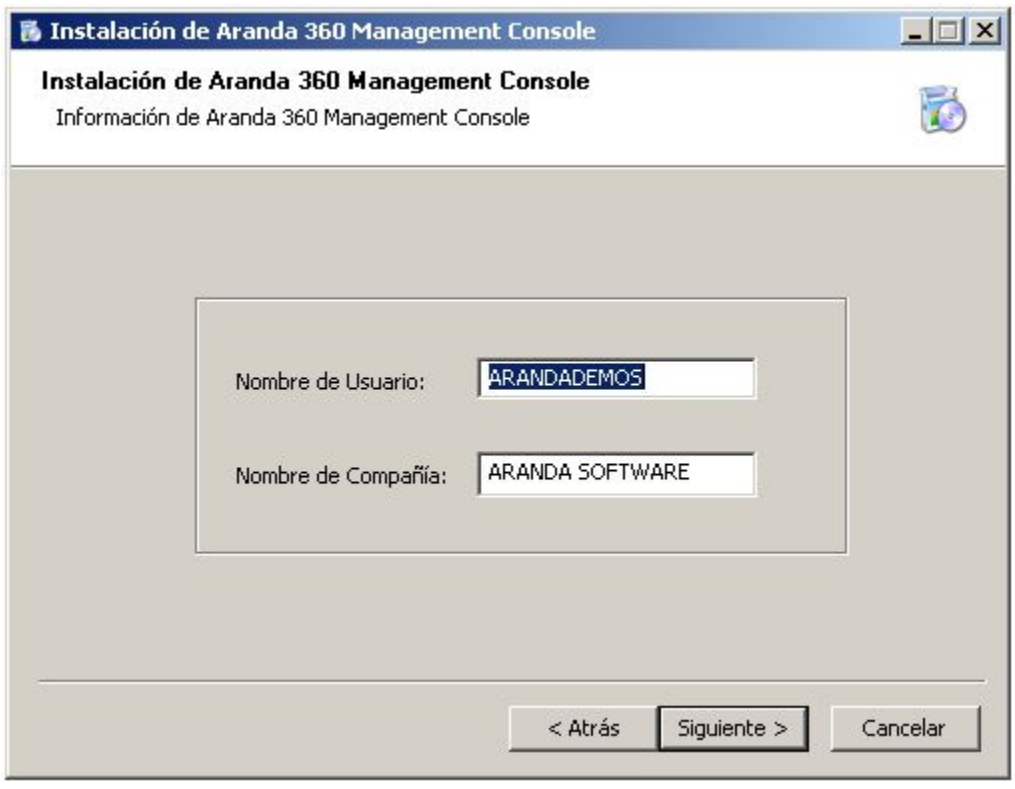


Instalando la consola de administración

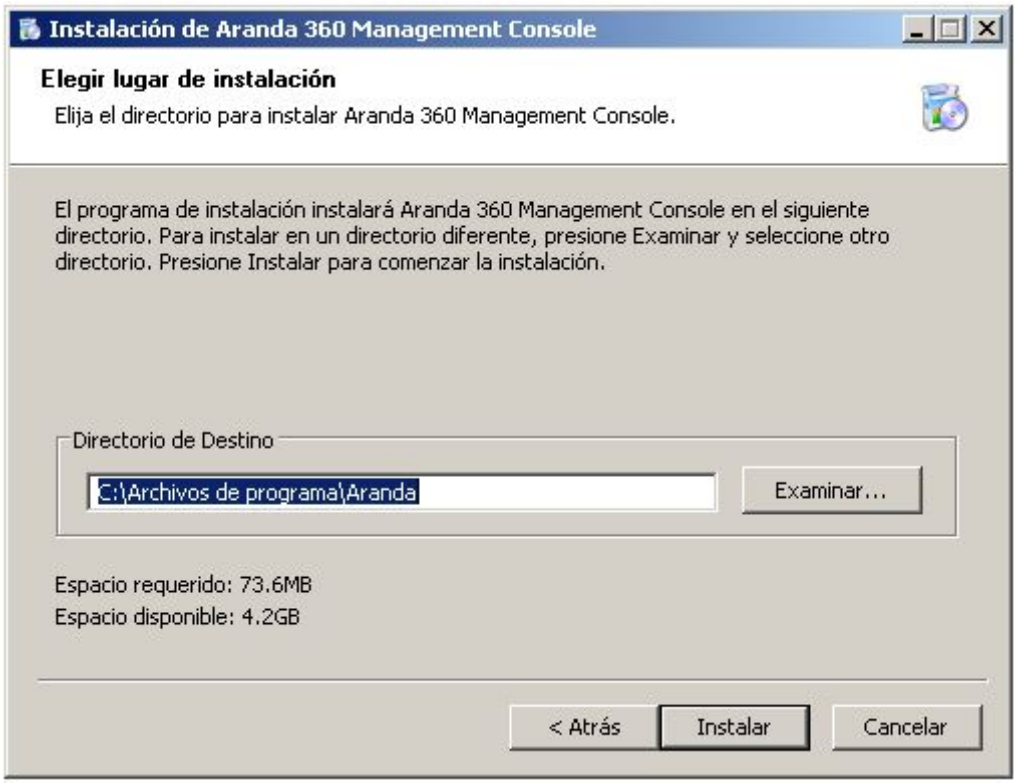
Para la instalación de la consola se debe usar el instalador proporcionado, para ello siga los siguientes pasos:

1. Vaya a la carpeta bin y haga doble clic sobre el archivo console.exe.
   Esta operación inicia el instalador de Microsoft.NET Framework (Si no está instalado en el equipo).
2. Seleccione el idioma de instalación.

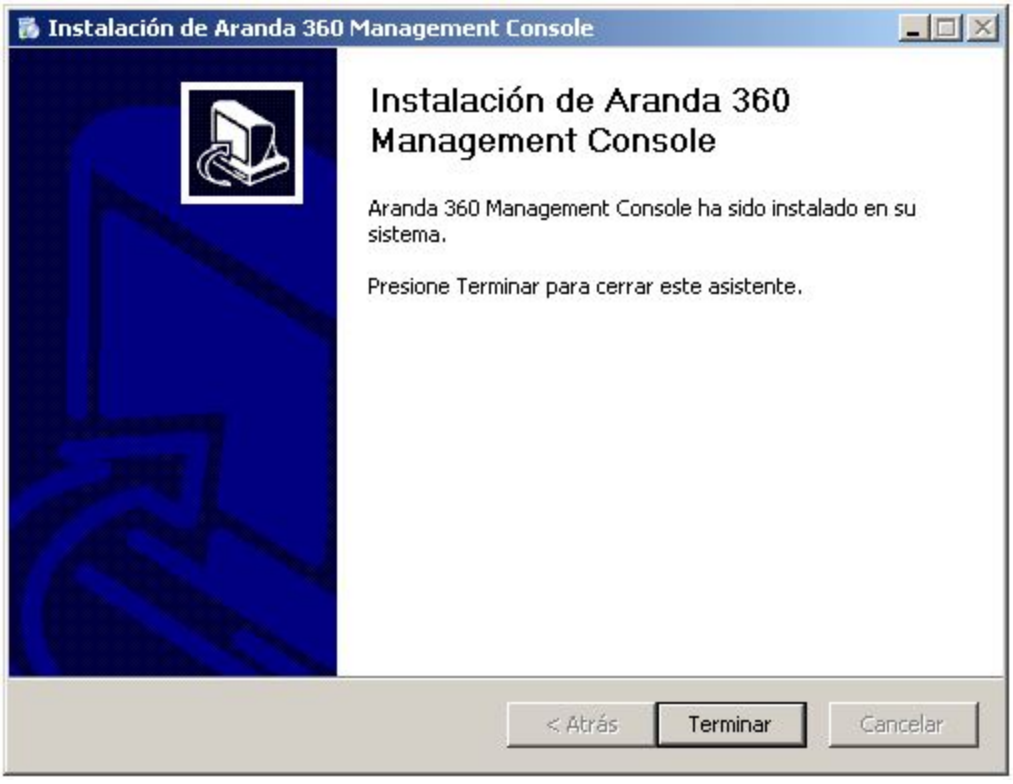
3. Digite el nombre de usuario y de la organización.



4. Haga clic en instalar.



5. Haga clic en finalizar para completar la instalación de la consola.



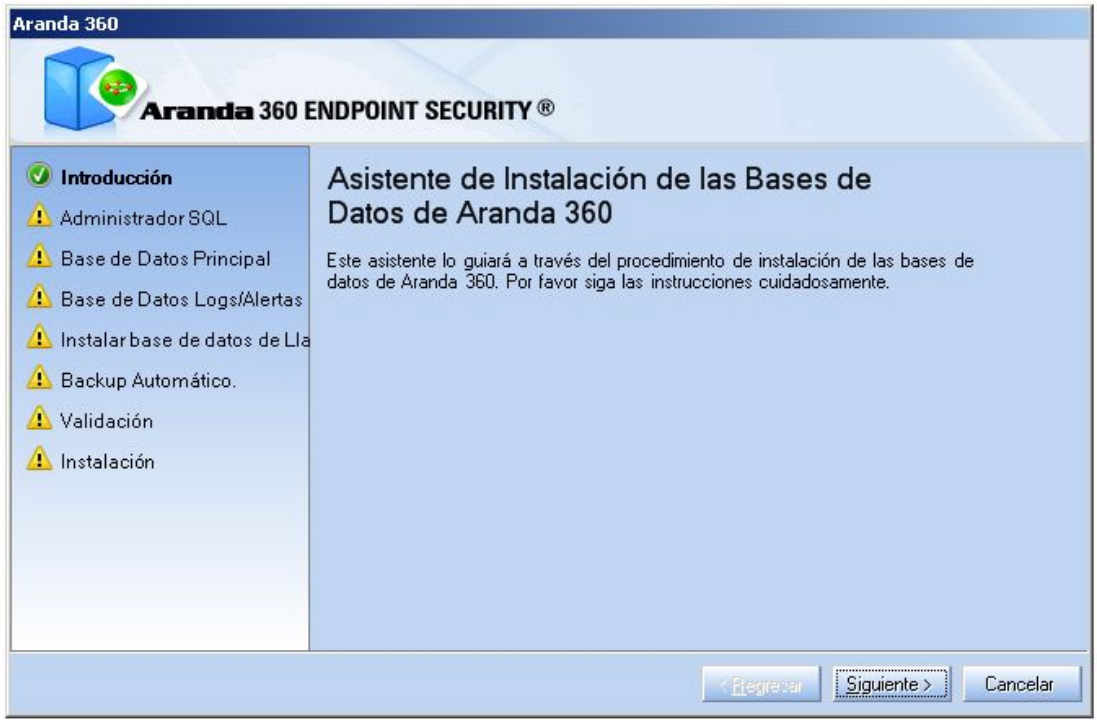
Instalando la base de datos

Para la instalación de la base de datos se debe usar el instalador proporcionado, para ello siga los siguientes pasos:

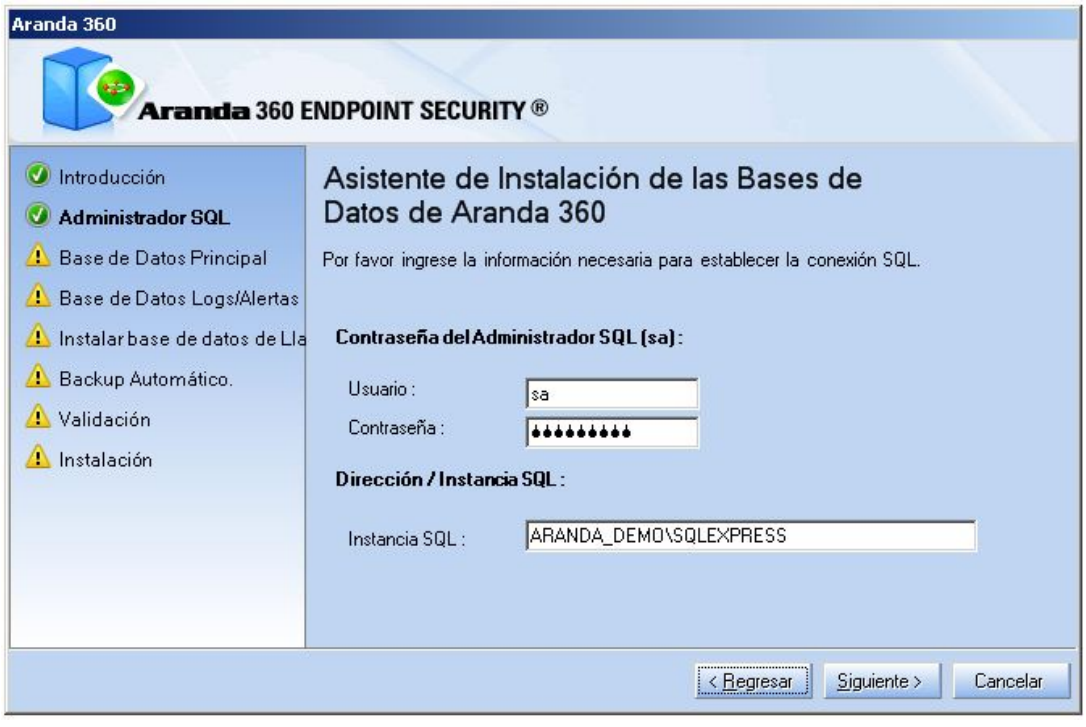
1. Inicie el programa de instalación de la base de datos, llamado DBInstaller, representado por el ícono :
   Inicio\Programas\Aranda\DBInstaller

   Aparecerá la siguiente ventana. Seleccione Instalar base de datos Aranda 360.

2. Instale la base de datos utilizando el asistente de configuración.



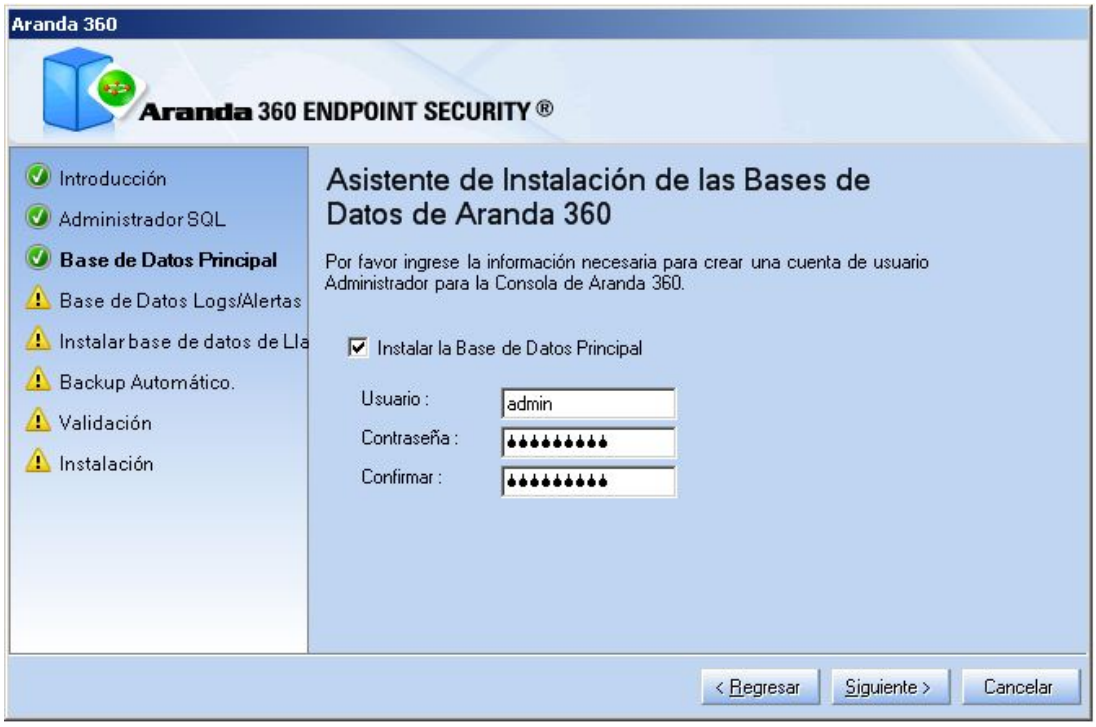
3. Defina los parámetros requeridos para crear la base de datos:
   - El nombre y contraseña de la cuenta de administrador (sa).
   - La dirección IP del servidor de base de datos MS SQL Server 2005.
   - Opcionalmente, el puerto utilizado para acceder a la base de datos.



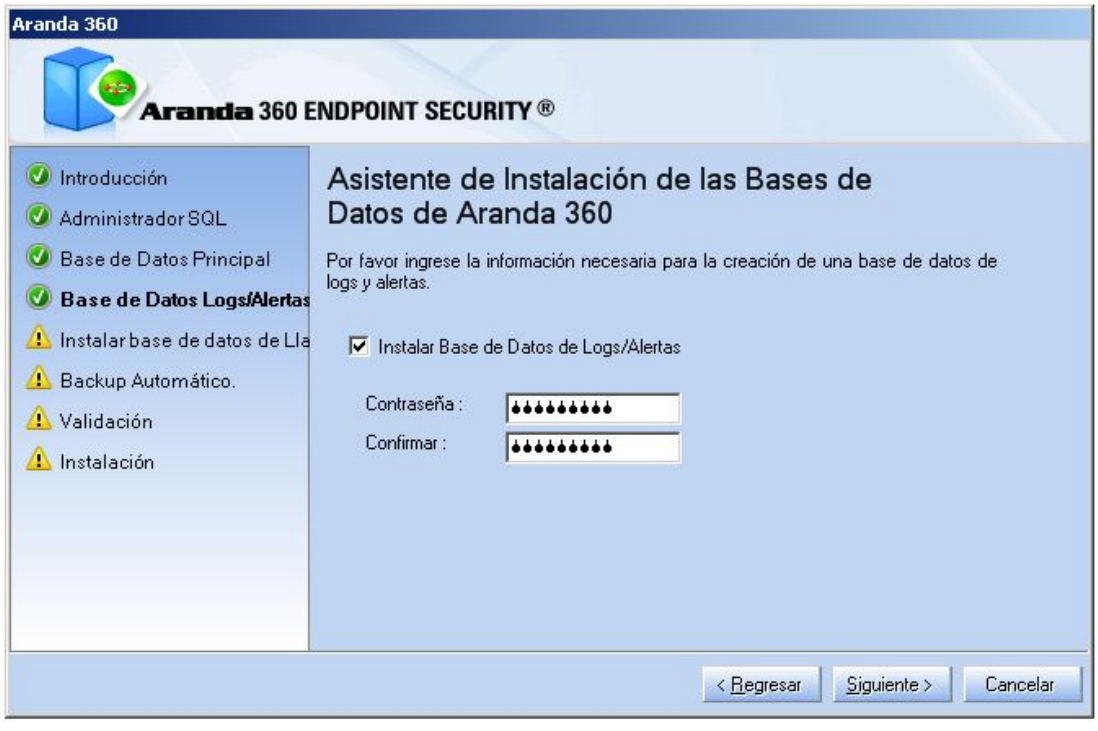
- La cuenta es únicamente usada para crear las cuentas de usuario de la base de datos, el servidor y la

consola.

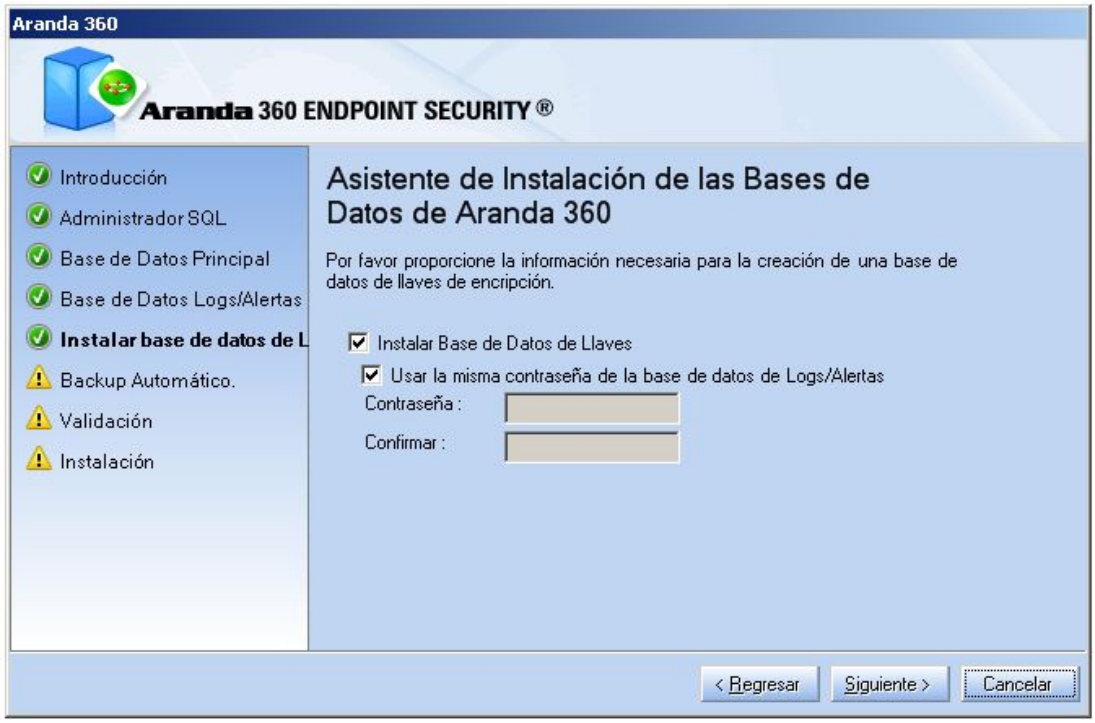
4. Instale la base de datos principal
   Se debe definir la contraseña que utilizará la cuenta de administrador de Aranda 360 (admin).



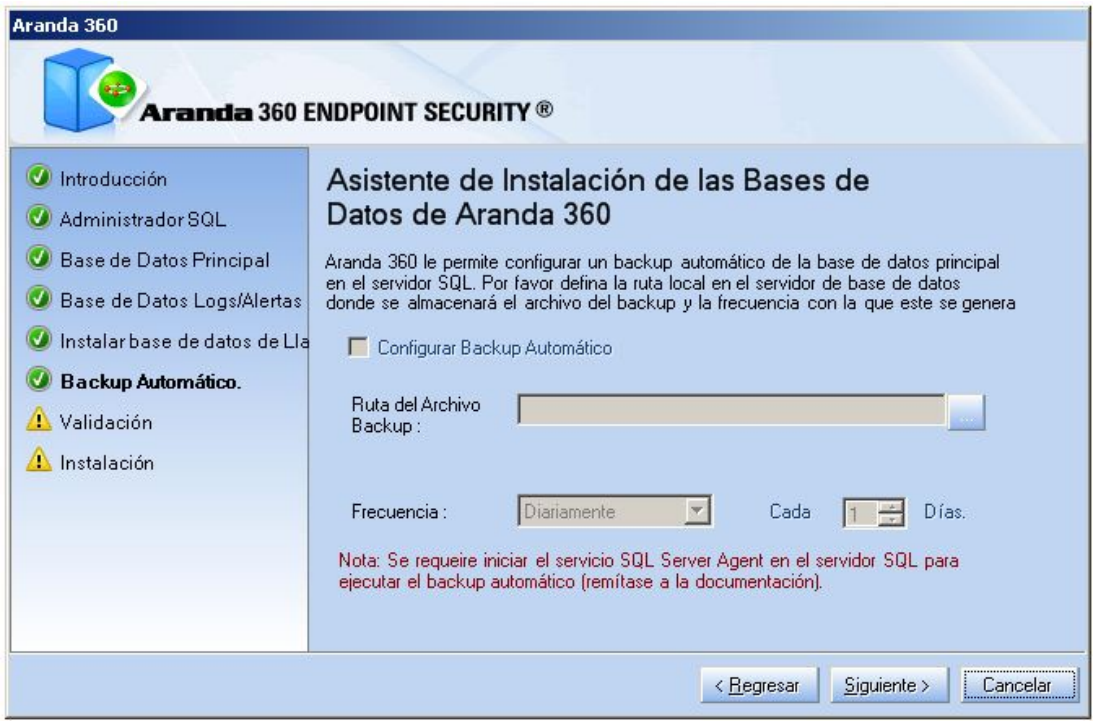
5. Instalar base de datos de alertas.
   Se debe definir una contraseña que utilizará el servidor de Aranda 360 para escribir en la base de datos.



6. Instalando la base de datos de claves.
   Se debe definir una contraseña para el servidor Aranda 360 para manejar el cifrado de claves en la base de datos.

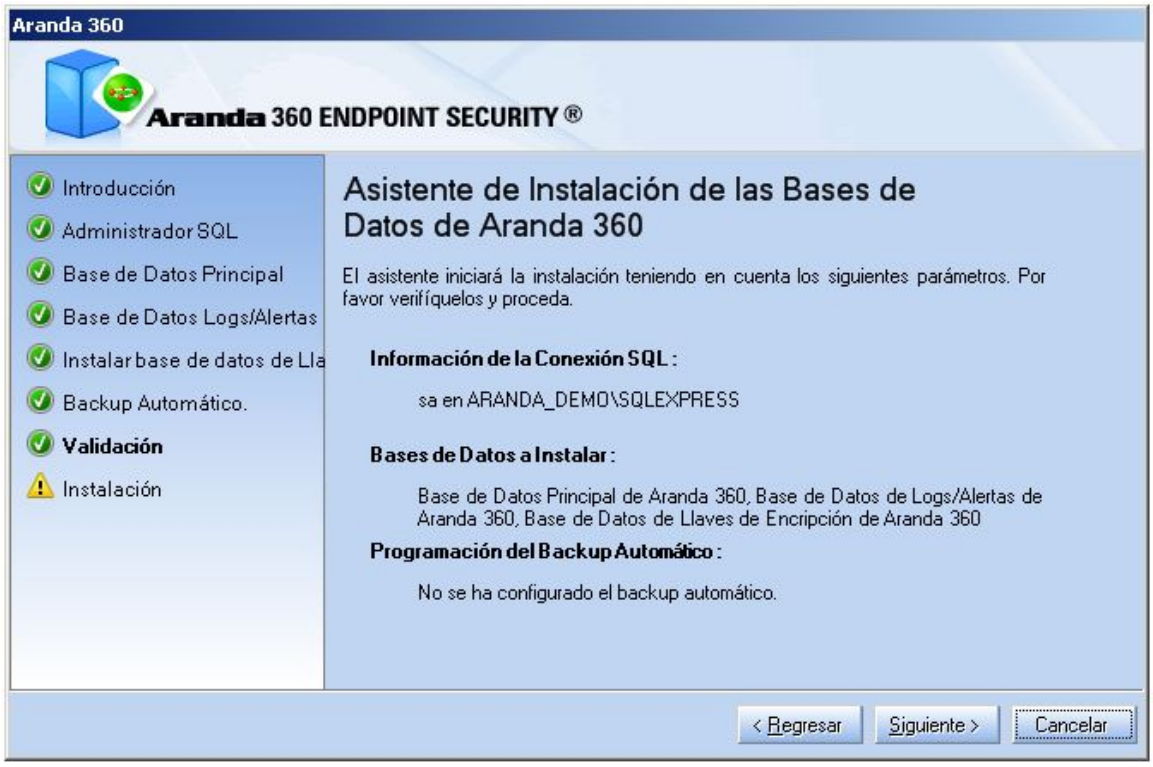


7. Opcional: creando una tarea.
   Para realizarlo, inicie el servicio del AGENTE SQL SERVER.
   Haga clic en siguiente.

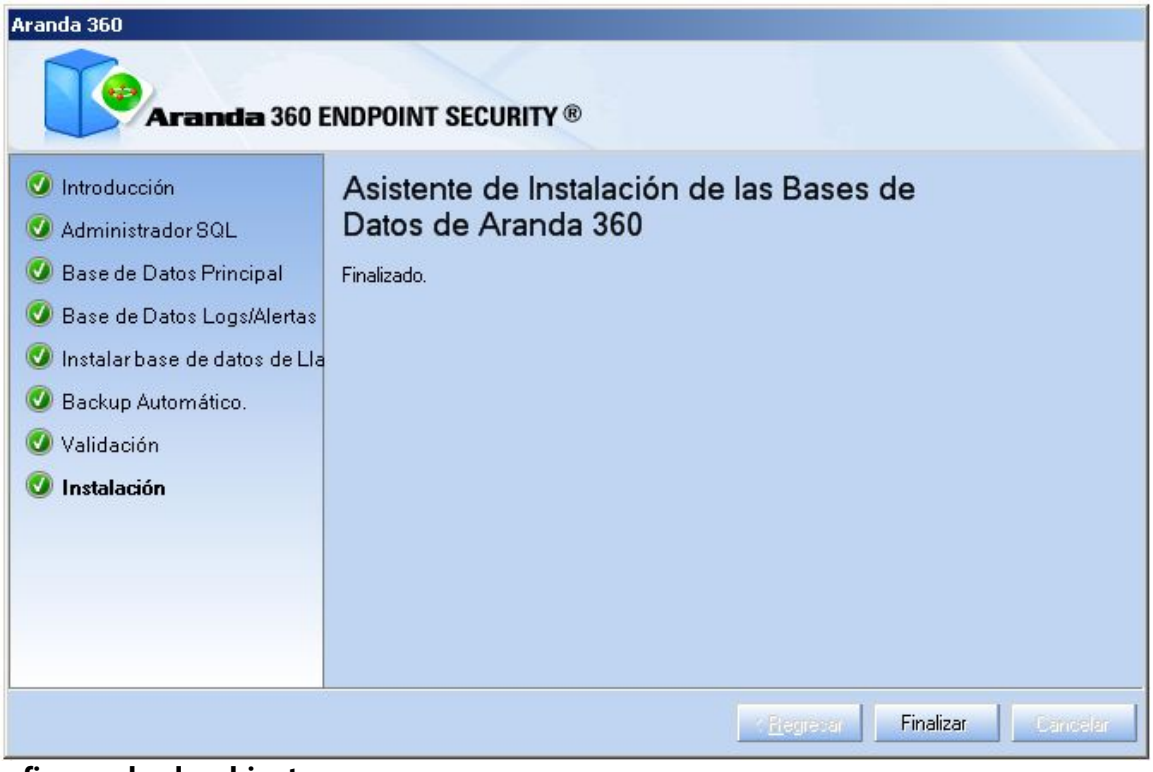


- Para realizar una copia de la base de datos en un directorio diferente al que viene por defecto (ejemplo: .\Mssql\Backup), asigne permisos Lectura/Escritura al grupo de seguridad SQLServer2005MSSQLUser$ServerName$SQLInstance.

8. Aparecerá la siguiente ventana con el resumen de toda la configuración definida.
   Haga clic en siguiente.



9. Aparecerá la siguiente ventana. Haga clic en finalizar.



Configurando el ambiente

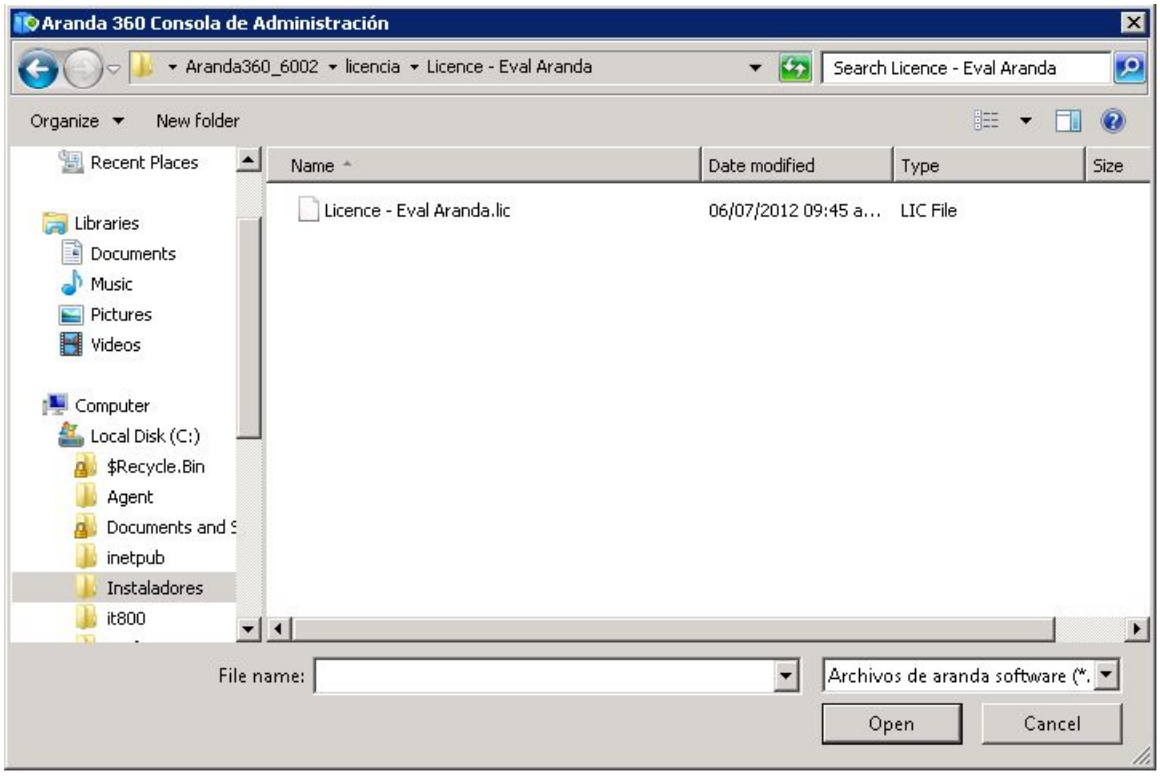
Para configurar el ambiente en la consola de administración, siga los siguientes pasos:

1. Haga clic en el icono de Aranda 360para abrir la consola.
2. Digite la cuenta de usuario y contraseña definida en la instalación de la base de datos.

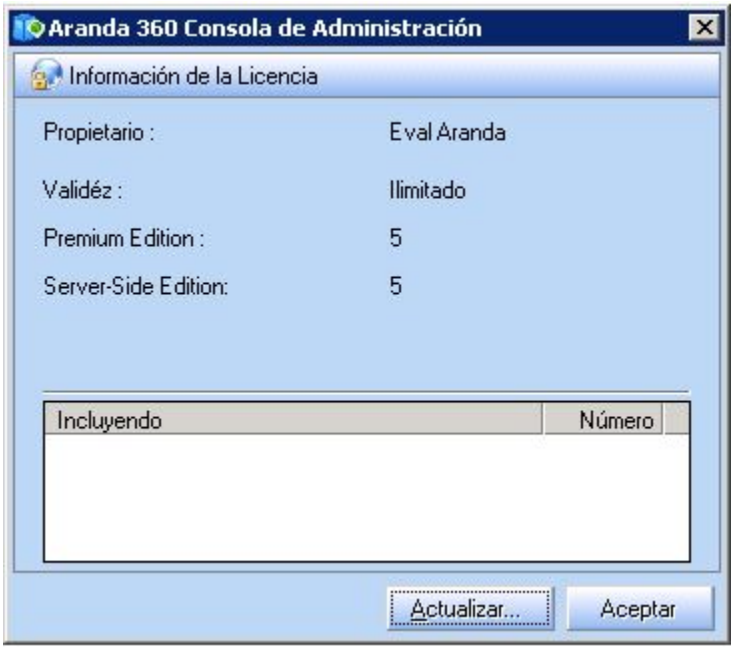
3. Para configurar un nuevo ambiente, siga los siguientes pasos:
   - Haga clic derecho para desplegar el menú contextual.
   - Clic en nuevo ambiente.

4. Haga clic en actualizar y seleccione el archivo de la licencia.

5. Para habilitar la licencia de Aranda 360, haga clic en abrir.

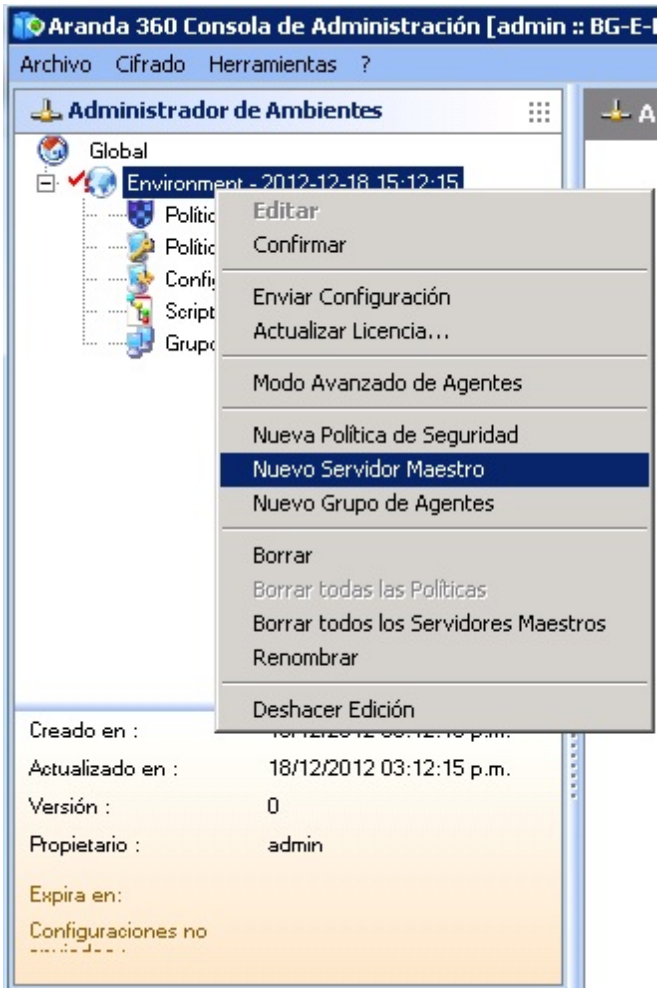


6. Haga clic en OK



El ambiente que se ha creado aparecerá de la siguiente forma:

7. Ahora agregue un nuevo servidor principal:
   - Haga clic Nuevo Servidor Principal.



- Digite la dirección IP del servidor y haga clic en OK.

El servidor principal que se ha creado aparecerá de la siguiente forma:

Instalando el agente

Descargando el agente desde el servidor Web

Descargando el agente desde el servidor Web server es el modo de distribución por defecto cuando no existe una herramienta de distribución remota.

En este modo, el instalador del agente es descargado y ejecutado manualmente en cada estación de trabajo.

La dirección de acceso para esta página es la dirección IP que fue configurada al instalar el servidor. Si el puerto 80 (por defecto) ha sido cambiado, es necesario especificar el Puerto asignado como sufijo de la dirección IP en el campo de dirección del navegador.

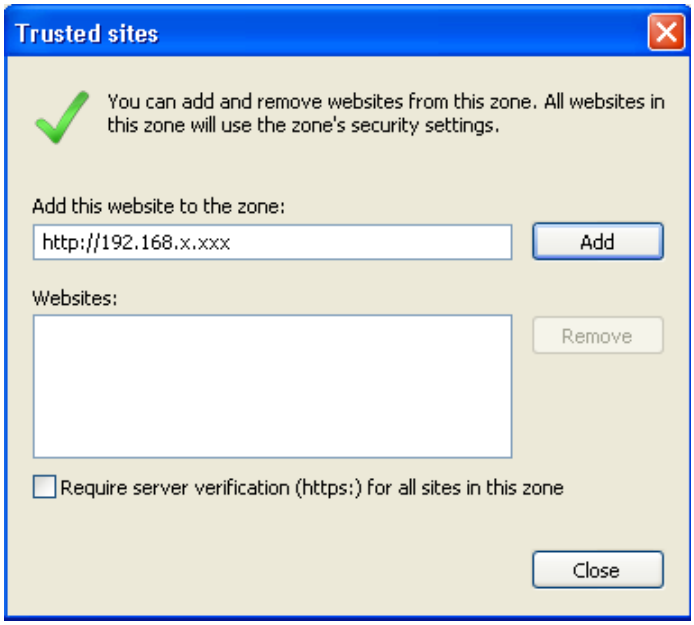
- Antes de instalar el agente, el administrador debe tener:
  - Haber creado al menos un grupo de agentes.
  - Haber aplicado una configuración y una política de seguridad al grupo.
  - Haber asociado el grupo con el Servidor principal.
  - Haber realizado una sincronización.

Instalación

El instalador del agente puede ser ejecutado directamente desde la página web o almacenado localmente para una posterior instalación

Este es un procedimiento desatendido, por lo tanto, no se solicitará información particular durante la instalación.

- Al utilizar Aranda 360 Server-Side Edition, por favor adicione el sitio web de Aranda en sus Sitios de Confianza para completar la instalación del agente.



Aparecerá un mensaje en una ventana emergente encima de la bandeja del sistema cuando la instalación es completada. La máquina debe ser reiniciada para activar el agente.

Dado que este método de instalación hay que repetirlo en cada estación de trabajo, es frecuentemente usado en ambientes de prueba y piloto.

- Debe utilizarse la cuenta de Administrador para instalar el agente. Si se instala el agente con otra cuenta, la instalación inicia pero no finaliza.

Directorio de instalación del agente

El agente puede ser instalado en otro directorio al que viene por defecto, en este caso es:

C:\Archivos de Programa\Aranda\Aranda 360 Agent\

Cambiando la ruta de instalación del agente de Aranda 360

Para cambiar la ruta de instalación del agente, siga los siguientes pasos:

1. En el servidor, abra el siguiente archivo:
   [Archivos de Programa]\Aranda\Aranda 360 Server\Apache\cgi-bin\msi.nsi
   Busque la siguiente línea:
   ;;WriteINIStr '$TEMP\sky.tmp\sky.cnf' Agent Install_path
   'C:\Archivos de Programa\company'

2. Remueva los comentarios (;;)
   Remplace C:\ Archivos de Programa\company por la ruta de instalación de destino [ruta personalizada].

   - Si la línea es comentada, el valor por defecto %archivo de programa%\Aranda será utilizado.

3. Guarde el archivo.

4. Ejecute [archivos de programa]\Aranda\Aranda 360 Server\generate_msi.exe. El agente se instalará en la ruta personalizada. Éste debe tener la siguiente forma [ruta personalizada]\Aranda 360 agent\.

Utilizando GPO para implementar los agentes

Las directivas de grupo (GPO) del directorio activo® son usadas para distribuir aplicaciones usando el servicio Microsoft Windows Installer. Este es un proceso desatendido dado que no se requiere información por parte del usuario durante la instalación.

Implementación remota usando GPO requiere un formato específico llamado MSI. Este tipo de archivos pueden ser utilizados para ejecutar instalaciones remotas sin intervención del usuario.

El archivo MSI se encuentra en el subcarpeta files del directorio de instalación del servidor que está por defecto:

c:\Archivos de Programa\Aranda\Aranda 360 Server\Apache\cgi-bin\files

- Las herramientas de clonación no son compatibles con los agentes de Aranda 360 Secure Edition.

Antes de instalar la imagen principal, verifique que no exista el certificado (agent.srn) en el directorio de instalación del agente Aranda 360.

DESCARGANDO CERTIFICADOS

Para una comunicación segura entre los componentes de Aranda 360 (consola, servidor y agente), éstos utilizan su propio certificado.

Cuando un agente ha sido instalado en una estación de trabajo, ningún certificado es proporcionado por alguna instancia de éste. Es necesario obtener el certificado antes de establecer una comunicación con el servidor.

Para ello, un servidor de certificados está instalado en el servidor Aranda 360, el cual se puede acceder por defecto por el puerto TCP 443.

- Para obtener más información de cómo configurar, desinstalar o desactivar el agente.

PERIODO DE VALIDEZ DEL CERTIFICADO

Por razones de seguridad, la descarga de certificados deben ser restringidos a un periodo limitado de tiempo, generalmente el tiempo necesario para la implementación de los agentes en la red.

El periodo de tiempo del certificado puede ser configurado en la consola de administración seleccionando un servidor principal en el árbol de administrador de ambientes.

Las opciones de configuración aparecerán en el panel interactivo de la parte derecha. El parámetro validar certificado (día(s)) está en ADMINISTRADOR de ambientes > Servidor Principal > Servicio de Autenticación.

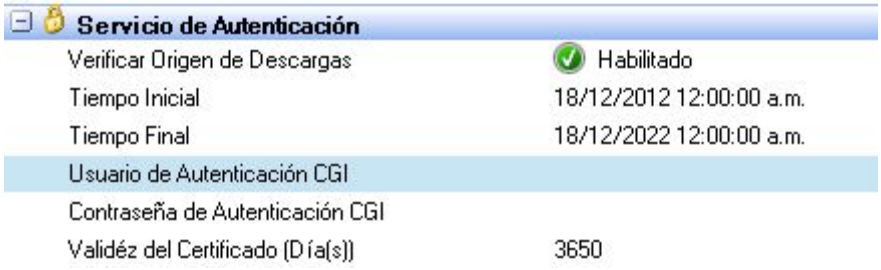
Por defecto, el periodo de tiempo está limitado a 10 años desde la fecha de instalación de la consola.

Modifique el valor de la disponibilidad del certificado Fecha de Terminación si prefiere un periodo más corto.

NOMBRE DE USUARIO Y CONTRASEÑA PARA DESCARGAR CERTIFICADOS

Es posible definir un nombre de usuario y una contraseña para permitir a un administrador descargar los certificados del sitio web.

Para ello, utilice los campos respectivos para autenticación CGI y de contraseña CGI.



Para descargar un certificado, vaya a la siguiente dirección:

https://<Dirección IP del servidor>/ssl/cgi

En la página de autenticación del certificado, digite el nombre de usuario y la contraseña.

Si la autenticación es exitosa, se abrirá una ventana para descargar el archivo del certificado con nombre agent.srn. Teste archivo debe ser copiado dentro del directorio de instalación del agente.

Compatibilidad con herramientas de clonación

El agente es compatible con herramientas de clonación.

- Las herramientas de clonación no son compatibles con el paquete Aranda 360 Secure Edition.

Para crear el disco principal de un sistema que contiene una agente, instale el agente en el sistema principal.

Cada agente requiere un certificado único. La instalación de una agente en la estación de trabajo principal no debe incluir el certificado de éste.

Para prevenir esto, antes de la instalación, cambie el periodo de autenticación a una fecha inválida en la consola de administración colocando una fecha anterior a la de creación de la estación de trabajo principal.

Antes de crear la imagen maestra, se debe verificar que no exista:

- El archivo agent.srn
- El archivo host_guid.sro
- Archivos en la carpeta vfs que se encuentra en el directorio de instalación del agente.

Si se da alguno(s) de los anteriores casos se deben esos archivos.

Los parámetros del servicio de autenticación están disponibles en el administrador de ambientes > [Servidor Principal] en los parámetros de configuración del servidor.

Cuando los sistemas clonados son distribuidos, restablezca el periodo de disponibilidad del servicio de autenticación para permitir que cada agente recupere su propio certificado.

PRUEBAS POSTERIORES A LA INSTALACIÓN

PRUEBA DE COMPONENTES

Es recomendable probar todos los componentes de Aranda 360 después de su instalación. Siga los siguientes pasos para probar toda la secuencia operativa de Aranda 360:

1. Identificar la máquina destino a través de la descripción de la red.
2. Defina una configuración simple y fácil de probar.
3. Una configuración simple, es por ejemplo, eliminarle la opción al bloc de notas de abrir cualquier archivo de texto con extensión .txt.
   Para obtener más información, ver "Protección basada en reglas "
4. Enviar la configuración (e implementar el agente en la máquina, si aún no se realizado).
5. Verifique que la regla es aplicada en la máquina destino.
6. Verifique accesos a los eventos almacenados en la base de datos. En caso de que surja algún problema.

ACTUALIZANDO COMPONENTES

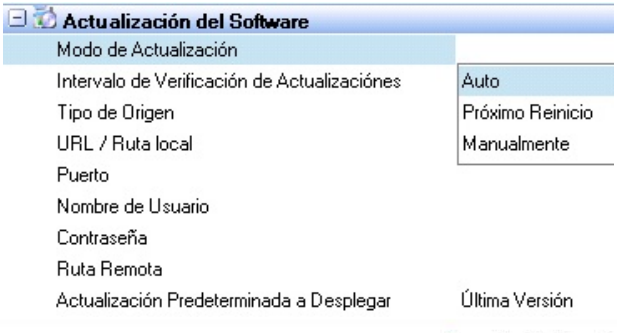
INTERFAZ GRÁFICA

Aranda 360 ofrece varias formas de obtener y aplicar las actualizaciones de software.

Las actualizaciones puede ser configuradas desde la consola de administración y el servidor principal a través de Administrador de Ambientes > [Nombre del Servidor Principal] > Configuración de Actualizaciones de Software.

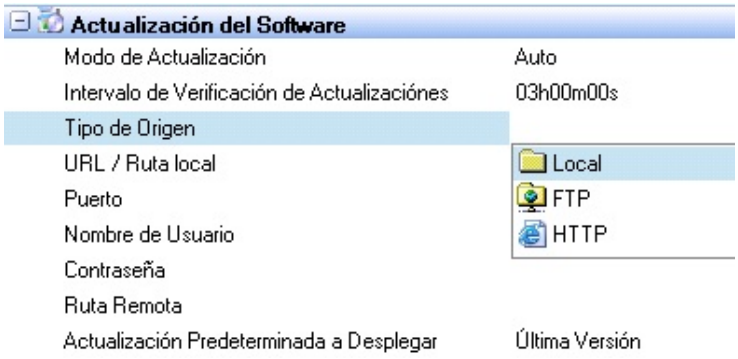
Los parámetros para actualizar los componentes de Aranda 360 son:

- Modos de actualización:
  El software puede ser actualizado:
  - Automáticamente.
  - Manualmente.
  - Aplicado en el siguiente reinicio.



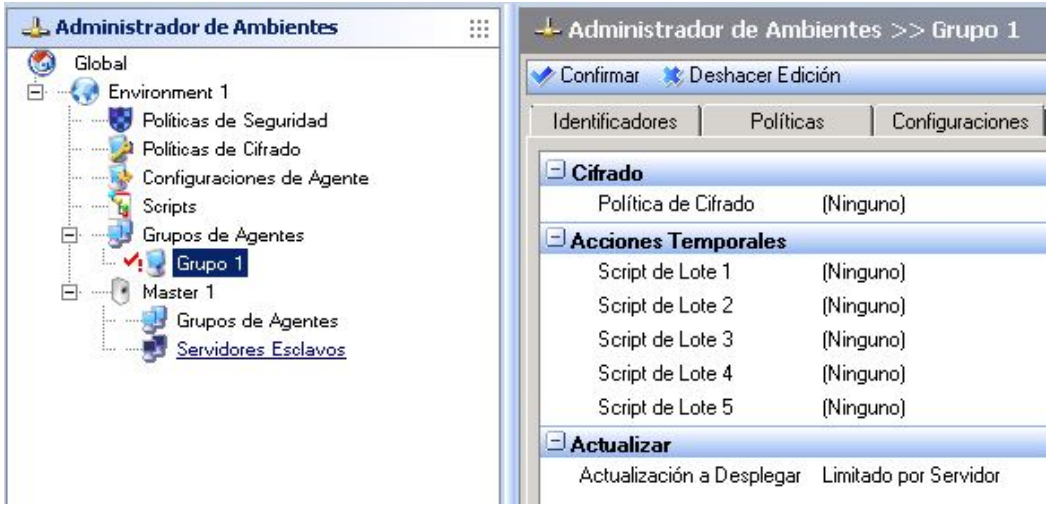
- Verifique el intervalo de actualización
  Este es el intervalo de tiempo (ejemplo: 03h00m00s) para verificar si existen nuevas actualizaciones para el servidor o la consola.

- Fuente:
  Los tipos de fuente son:
  - Local.
  - HTTP.
  - FTP.



- Ruta URL/Local:
  Esta es la ruta o dirección donde las actualizaciones son almacenadas.
- Puerto
- Nombre de usuario.
- Contraseña.
- Ruta remota.
- Actualización por defecto a distribuir (ex.: 5.700):
  Este es el número máximo de versión de Aranda 360 aplicada a los agentes.
  Si no se desea utilizar esta opción, aplique la última versión. El grupo de agentes serán automáticamente actualizados a la última versión aplicada al servidor.
  Si se requiere una versión específica, el grupo de agentes no serán actualizados a una versión superior definida en la actualización por defecto (ejemplo.: 4.806).

Ejemplo : La versión limitada que está asignada al grupo de agentes Grupo 1 es 4.806.



Modos de Actualización

Los modos de actualización para los componentes del servidor y del agente son:

- Automático.
- Siguiente reinicio.
- Manualmente.

Estos modos se relacionan con los parches de la aplicación y las descargas automáticas de los componentes.

Tipo de Fuente

El servidor recupera las actualizaciones y los parches. La consola de administración define como los archivos deben ser accedidos:

- Local.
- FTP.
- HTTP.

Local

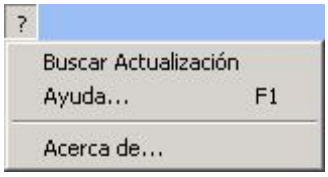
El modo local es usado para las actualizaciones manuales. Se pueden obtener los parches por vía mail, CD-ROM u otro medio extraíble, entonces son puestos en un directorio cuya ruta está configurada en la consola de administración.

FTP y HTTP

Los modos FTP and HTTP son usados para descargar automáticamente las actualizaciones.

Actualizaciones por demanda

La consola puede ser actualizada por demanda usando la opción en el menú, > **Verificar Actualización.**



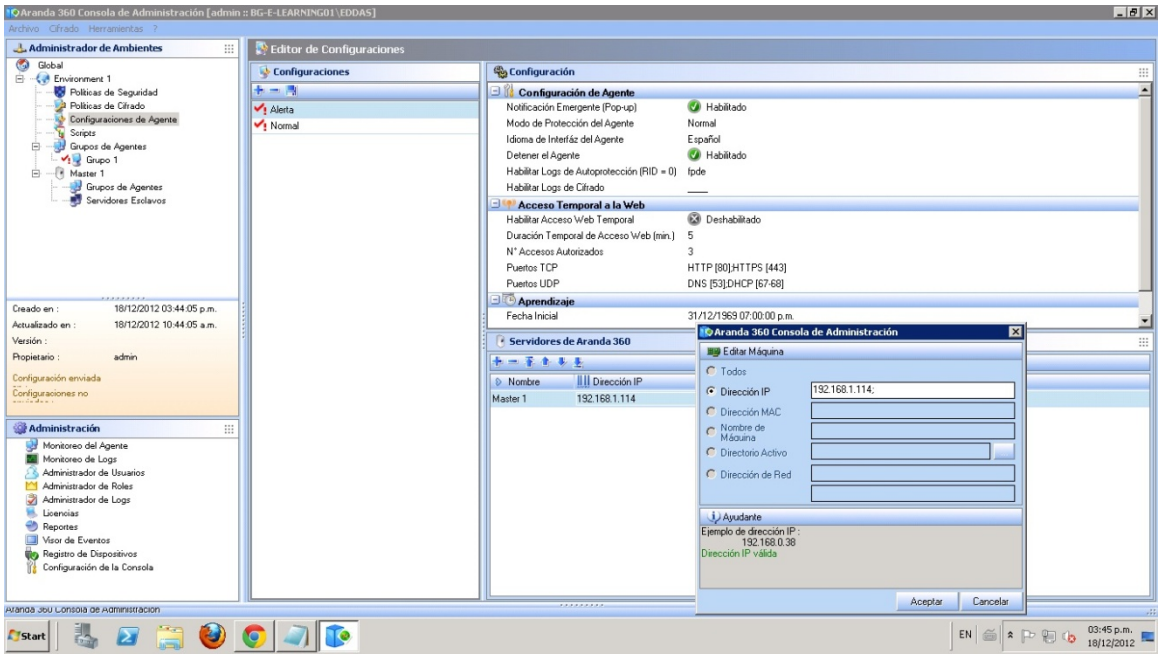
POSIBLES MODIFICACIONES

MODIFICANDOLA DIRECCIÓN IP DEL SERVIDOR ARANDA 360

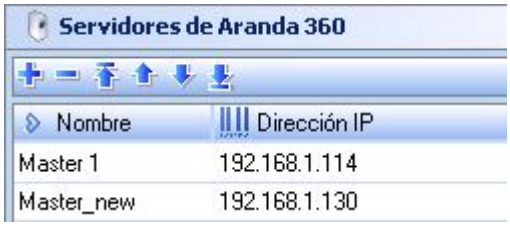
Después de instalar y configurar Aranda 360, es posible que en algún momento necesite cambiar la dirección IP del servidor principal , y en consecuencia, actualizar los agentes.

Para cambiar la dirección IP del servidor principal, siga los siguientes pasos:

1. Edite todas las configuraciones del agente en el Editor de Configuración:
    - Haga clic en configuración en el Administrador de Ambientes.
    - Haga clic en el panel de servidores Aranda 360.

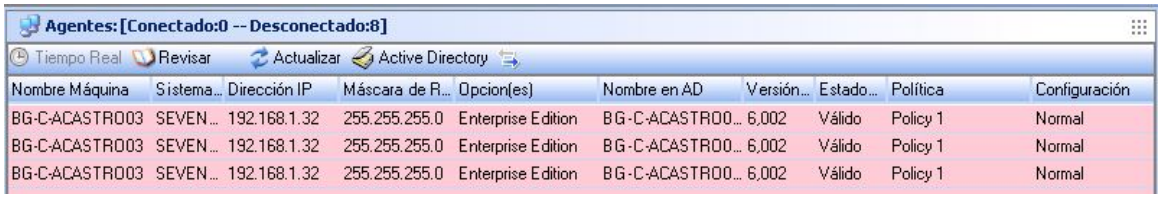


- Agregue una nueva dirección IP.



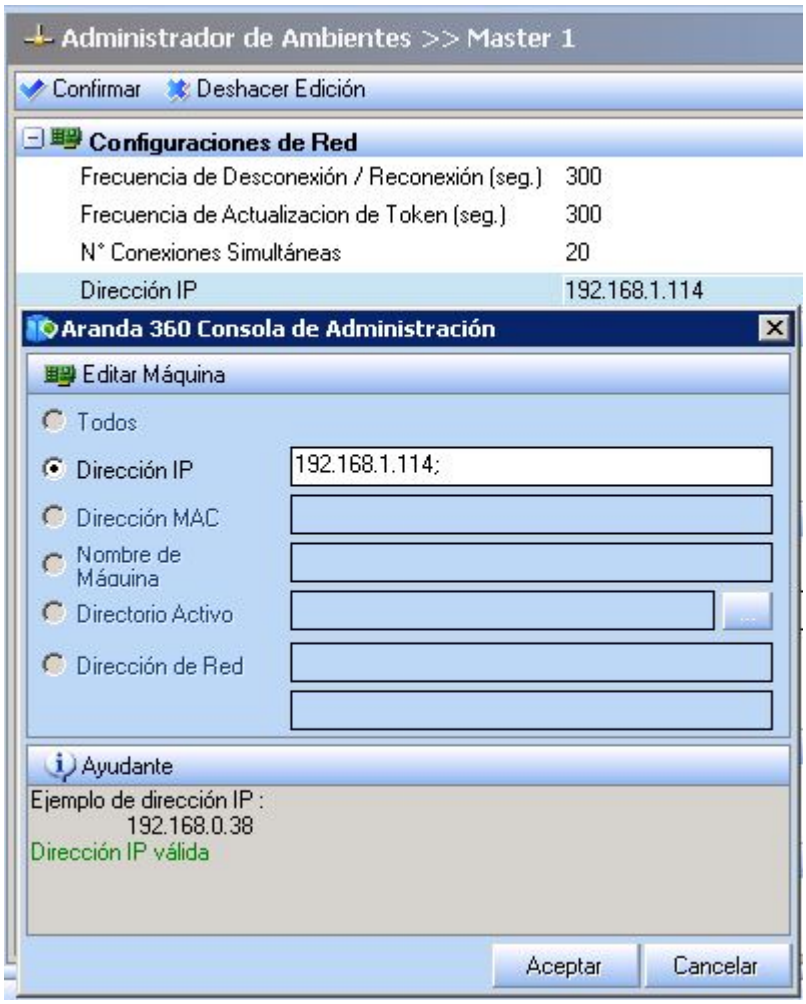
2. Envié la nueva configuración para actualizar los agentes con la nueva dirección IP del servidor principal.
   Para enviar una nueva configuración, Haga clic derecho en el servidor y seleccione la opción Sincronizar.

3. Verifique en el monitor del agente que la nueva configuración fue aplicada correctamente (Ejemplo: Config. Update).



Nombre Máquina	Sistema...	Dirección IP	Máscara de R...	Opcion(es)	Nombre en AD	Versión...	Estado...	Política	Configuración
BG-C-ACASTRO03	SEVEN...	192.168.1.32	255.255.255.0	Enterprise Edition	BG-C-ACASTRO0...	6,002	Válido	Policy 1	Normal
BG-C-ACASTRO03	SEVEN...	192.168.1.32	255.255.255.0	Enterprise Edition	BG-C-ACASTRO0...	6,002	Válido	Policy 1	Normal
BG-C-ACASTRO03	SEVEN...	192.168.1.32	255.255.255.0	Enterprise Edition	BG-C-ACASTRO0...	6,002	Válido	Policy 1	Normal

4. Después que se hayan actualizados los agentes:
   - Eliminar la dirección IP anterior por cada configuración en el Editor.
   - Remplace la anterior dirección IP por la nueva en ADMINISTRADOR de Ambientes >Servidor Principal > Configuración de Red.

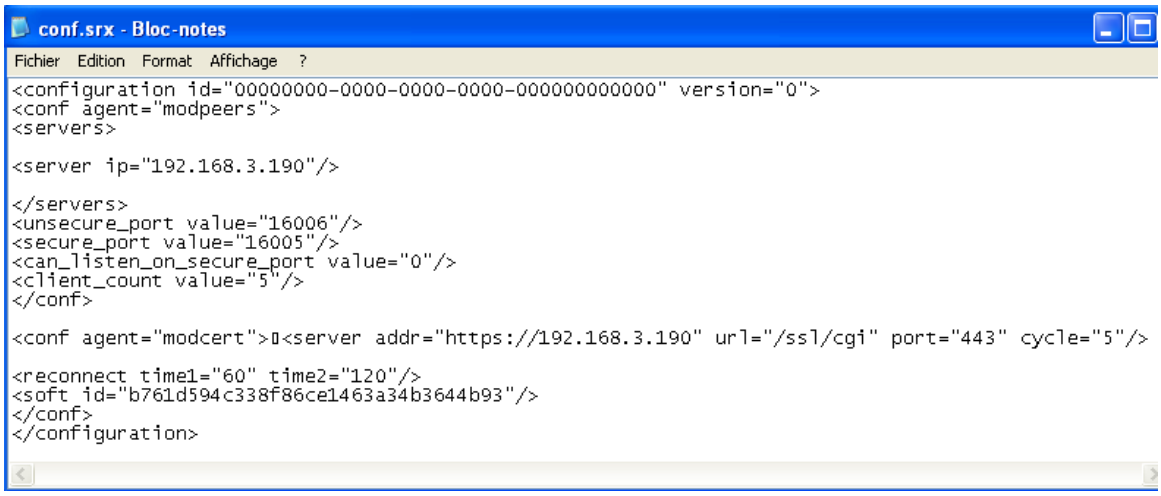


5. Cambie la dirección IP del servidor en la tarjeta de red..
6. Envié esta configuración desde el servidor principal para actualizar los agentes con la nueva dirección IP, y remover la dirección antigua.
7. Si un servidor MS SQL es instalado, es necesario reiniciar el servidor inmediatamente.

Después de actualizar el servidor principal y las direcciones IP de los agentes, es necesario actualizar el instalador del agente para que puedan tomar la nueva dirección IP los nuevos agentes.

Para ello, Siga los siguientes pasos:

1. Vaya al directorio de instalación del servidor principal.
2. Actualice todas las referencias a la dirección IP en el siguiente archivo:
   [directorio de instalación]\Apache\cgi-bin\conf.srx



3. Haga doble clic en el siguiente archivo:
   [directorio de instalación]\Generate_msi.exe
   El instalador ha sido actualizado, ahora es posible descargar los nuevos agentes desde el servidor web.

MODIFICANDO LOS PUERTOS TCP DEL SERVIDOR PARA SERVICIOS HTTP Y SSL

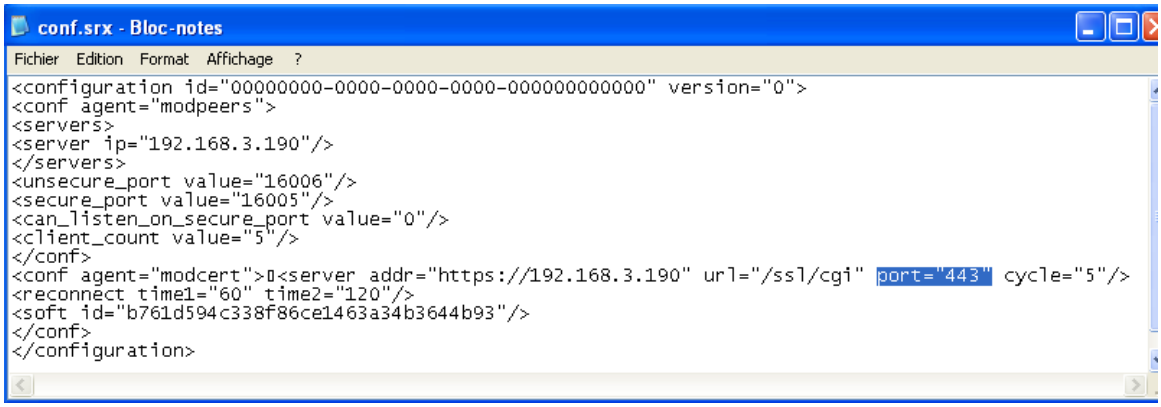
Para modificar los puertos TCP para servicios HTTP and SSL (después de la instalación), siga los siguientes pasos:

1. Después de instalar el servidor, es posible cambiar los dos puertos TCP utilizados por el servidor HTTP/ SSL server editando los siguientes archivos:
   C:\Archivos de Programa\Aranda\Aranda 360Server\Apache\conf\httpd.conf
   C:\ Archivos de Programa \Aranda\Aranda 360 Server\Apache\conf\ssl.conf
2. Para httpd.conf, cambie el puerto asignado al servidor Web (por defecto 80).
3. Para ssl.conf, cambie el puerto asignado al servidor Web y host virtual (por defecto 443).
4. Reinicie el servidor

.

Ahora, debe actualizar el instalador del agente para que tome los cambios de los nuevos valores de los puertos TCP del servidor.

1. Vaya al directorio del instalador del servidor principal:
   C:\Archivos de Programa\Aranda\Aranda 360Server\Apache\cgi-bin\
2. En el archivo conf.srx, cambie el valor del puerto (Por defecto 443).



3. Haga doble clic en el siguiente archivo:
   [directorio de instalación]\Generate_msi.exe
   El instalador ha sido actualizado, ahora puede descargar nuevos agentes desde el servidor Web.

DESINSTALANDO COMPONENTES

DESINSTALANDO EL SERVIDOR Y LA CONSOLA

La consola de administración y los servidores de Aranda 360 pueden ser desinstalados utilizando la herramienta de desinstalación, la cual es accesible desde:

- En el menú Inicio en los sistemas que alojan estos componentes.
- La opción Agregar / Quitar Programas en el panel de control.

DESINSTALANDO EL AGENTE

El agente puede ser desinstalado utilizando el programa SRend.exe ubicado en el directorio de instalación.

La ruta predeterminada del programa para la desinstalación es:

C:\Program Files\Aranda\Aranda 360 Agent\SRend.exe

Este es un procedimiento desatendido, sin intervención del usuario. Cada estación de trabajo debe ser reiniciada después de la eliminación de los archivos.

Si el agente fue instalado remotamente utilizando GPO, puede también utilizar esta misma herramienta para eliminar el agente desatendidamente.

- Tiene que ser un administrador de la máquina para poder desinstalar el agente. Detener el Agente debe estar habilitado en Configuración del agente para realizar la desinstalación.

Si adquirió la versión Aranda 360 Secure Edition, el usuario debe reiniciar el sistema dos veces con el fin de:

- Descifrar archivos.
  Descifrando los datos en la desinstalación y la fecha de Inicio/Fin de inicio de permitir desinstalaciones, debe estar configurada en los parámetros del servidor principal

- Desinstalando Aranda 360 después de que todos los archivos fueron descifrados.

REMOVIENDO LA BASE DE DATOS

Para desinstalar la base de datos MS SQL Server 2005 se debe utilizar la herramienta de Windows Agregar/Quitar programas o el instalador de la base de datos.

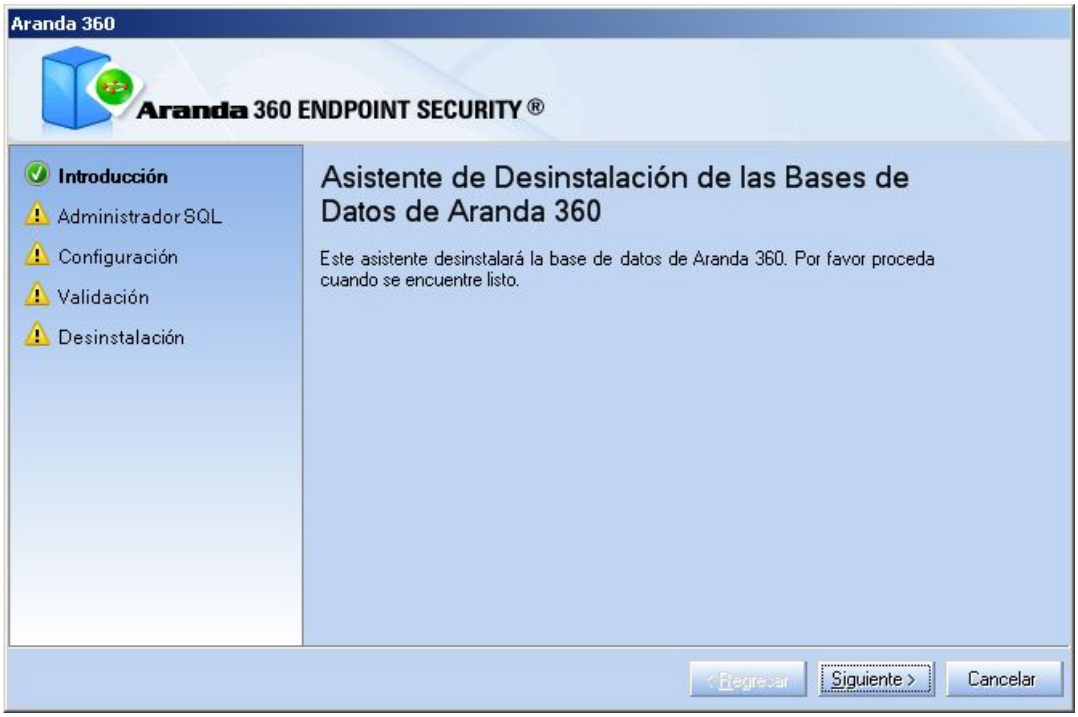
- La base de datos debe ser removida antes de desinstalar la consola.

  Si se desinstala la consola antes de remover la base de datos, el instalador DB será desinstalado y no será posible remover la base de datos.

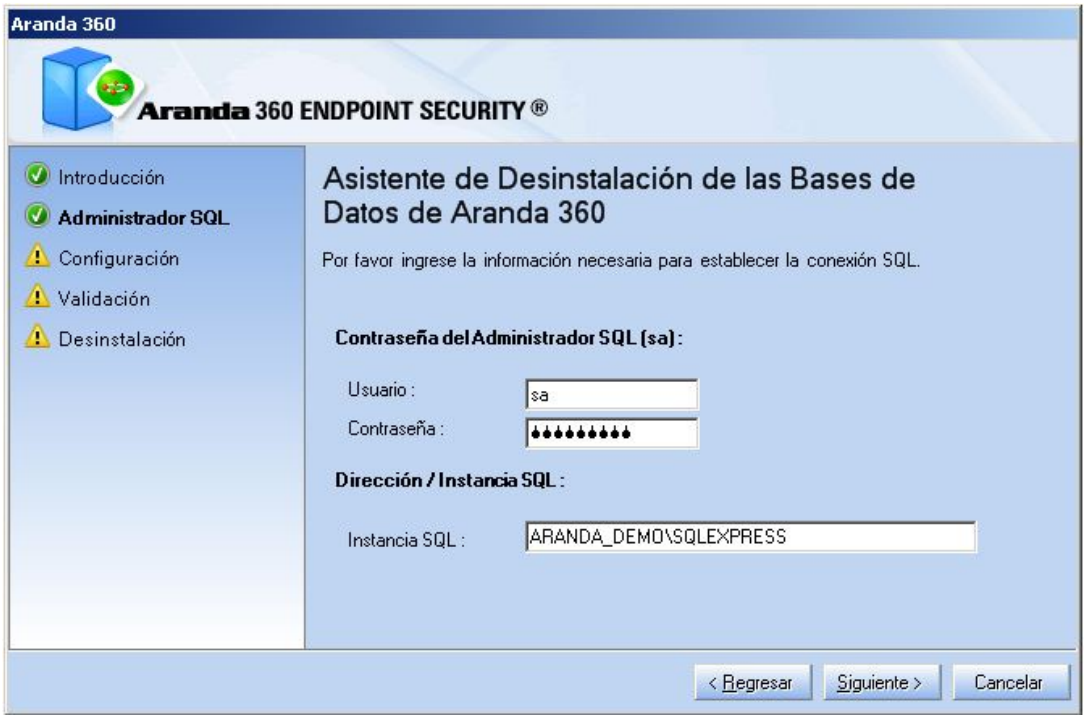
Para remover la base de datos, siga los siguientes pasos:

1. Vaya a Inicio>Todos los programas>Aranda>DB Installer. La ventana de herramienta de administración de base de datos se abrirá.
2. Haga clic en desinstalar base de datos Aranda 360.

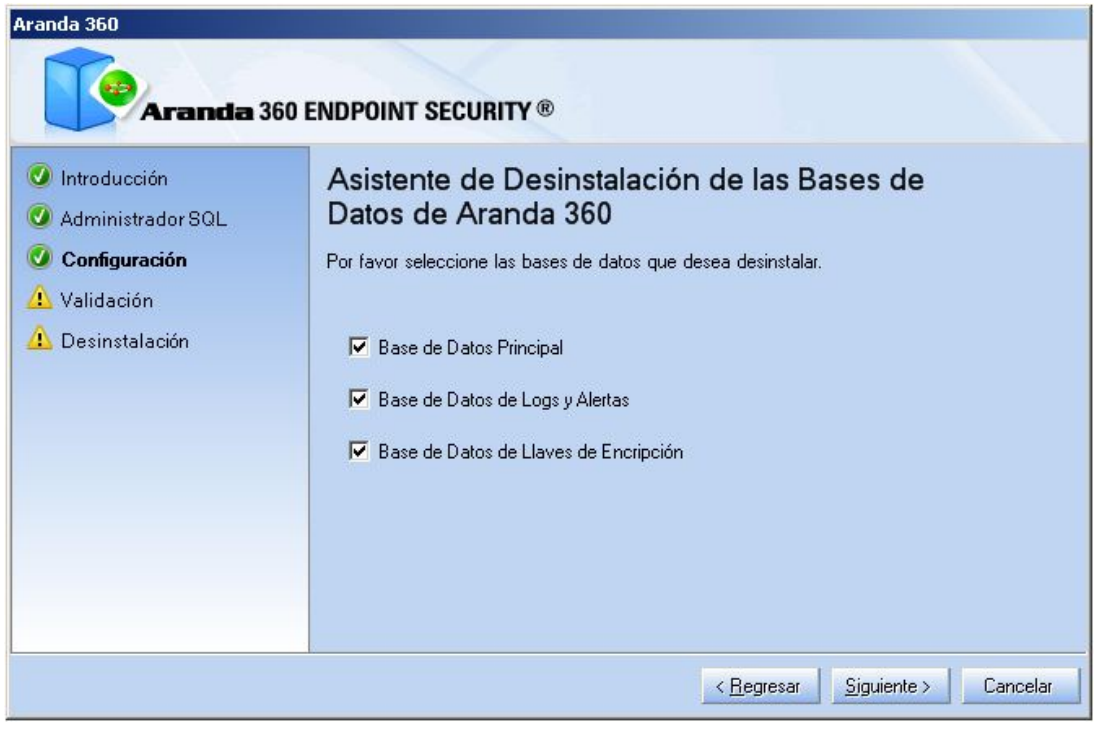
3. Aparecerá la siguiente ventana.
   Haga clic en siguiente.



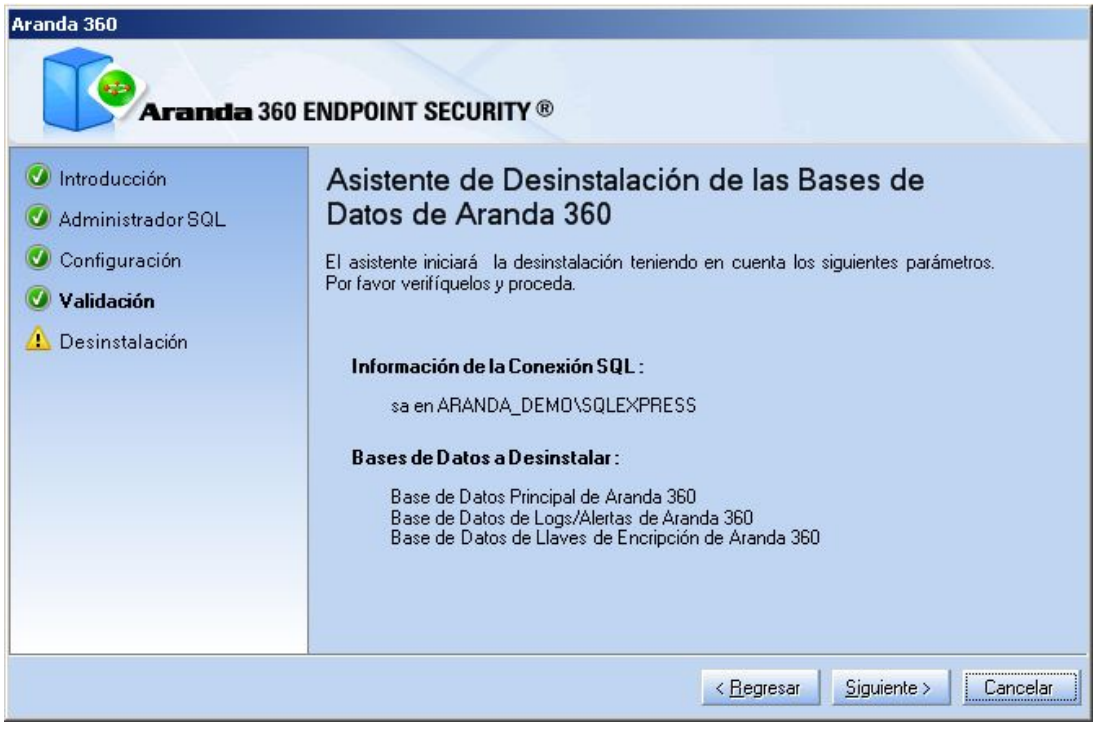
4. Digite la información de administrador para conectarse a la base de datos:
   - La cuenta de usuario del administrador.
   - La contraseña de la cuenta (por defecto sa).
   - La ruta de la base de datos.
     Haga clic en siguiente.



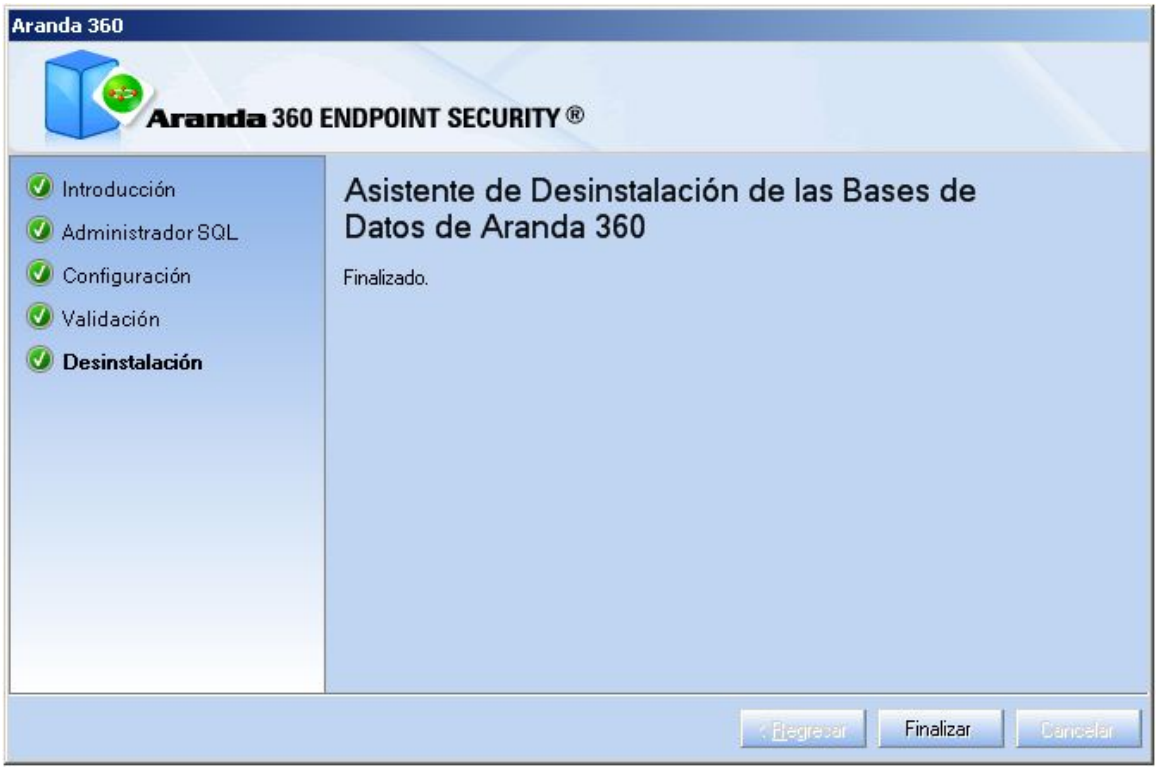
5. Seleccione la base de datos a desinstalar.
   Haga clic en siguiente.



6. Antes de comenzar el proceso de desinstalación, verifique la información mostrada.
   Haga clic en siguiente.



7. El proceso de desinstalación ha finalizado.



Capítulo 3 - ACTUALIZANDO ARANDA 360

ACERCA DE ESTE CAPÍTULO

Éste capítulo describe el proceso de actualización de Aranda 360:

- Con MS SQL Server 2000 en la estación de trabajo:
  - Recomendaciones.
  - Procedimiento.

- Con MS SQL Server 2005 en la estación de trabajo:
  - Requisitos.
  - Procedimiento.

CON MS SQL SERVER 2000

RECOMENDACIONES

Si el servidor donde está alojada la base de datos es MS SQL Server 2005 o MS SQL Server 2005 Express Edition.

- Es altamente recomendable respaldar la base de datos antes de actualizar Aranda 360.

Si el servidor donde está alojada la base de datos es MSDE o SQL Server 2000, debe primero respaldar la base de datos. Luego, Podrá desinstalar la base de datos y migrarla a MS SQL Server 2005 o MS SQL Server 2005 Express Edition.

- En la versión 5.2, la base de datos Aranda 360 está compuesta por:
  - La base de datos de la consola.
  - La base de datos de alertas.
  - La base de datos de claves.

- Solo es posible actualizar a versión 6.0 desde una versión 5.2.x.
  Para actualizar Aranda 360 desde una versión anterior, se debe actualizar primero a versión V4.8.

Para actualizar Aranda 360 desde una versión anterior a 6.0, debe salvar primero la base de datos.

Luego, podrá desinstalar el servidor de base de datos.

PROCEDIMIENTO

- Cuando se tiene una versión anterior a 4.5.10, ver procedimiento de actualización (versión 5.2) en nuestro sitio de extranet.

Guardando la base de Datos Aranda 360

Para guardar la Base de Datos de la consola

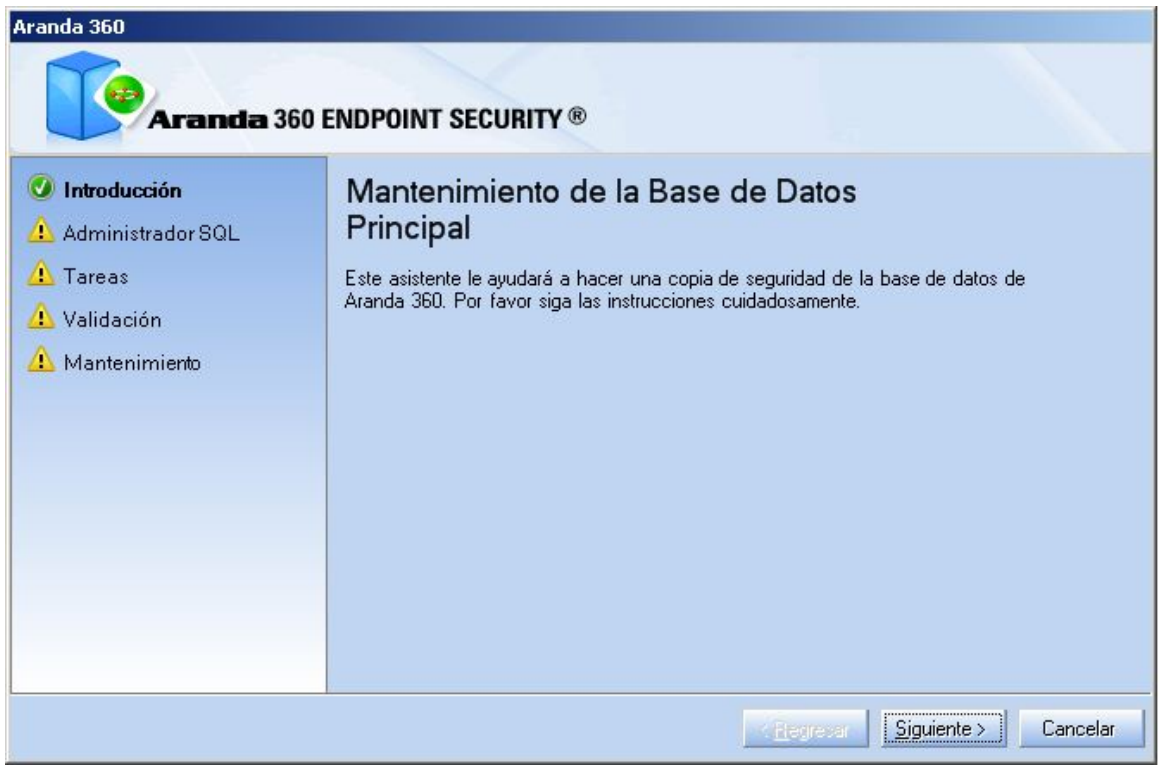
Para guardar la Base de Datos de la consola, siga los siguientes pasos:

1. Cierre la consola de administración.
2. Ejecute el archivo DbInstaller.exe que se encuentra por defecto en:
   C:\Archivos de Programa\Aranda\Aranda Management Console\DBInstall
   DbInstaller.exe se puede acceder desde el menú inicio.
   DbInstaller.exe está representado por el ícono .
   Esto iniciará la herramienta de administración de la base de datos.

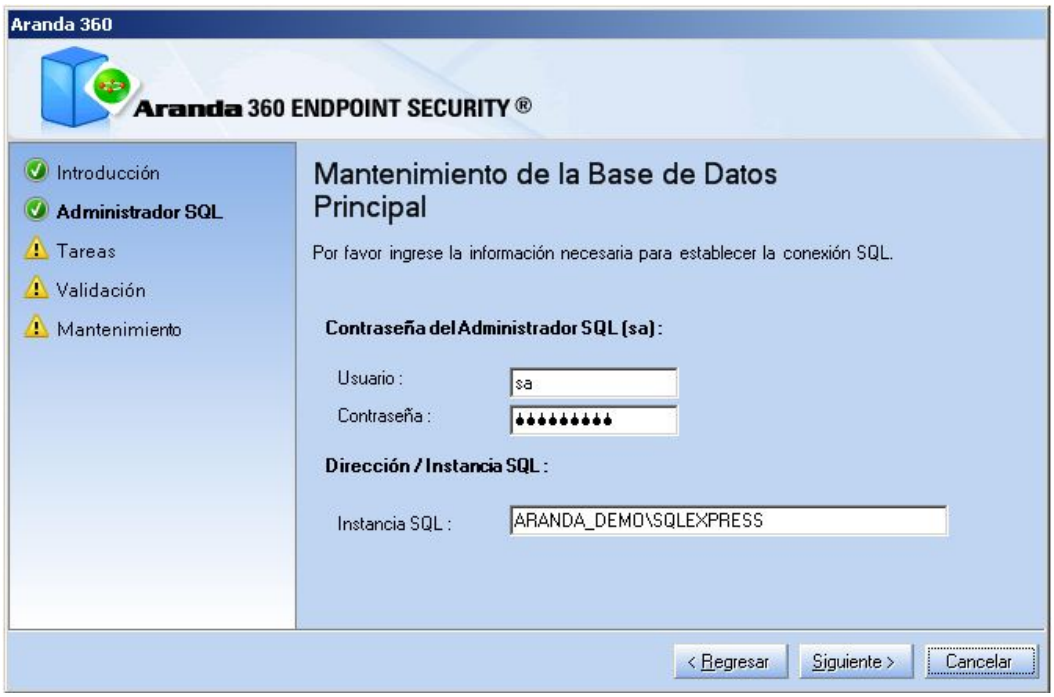
3. Seleccione mantenimiento de la base de datos de la consola.

Esta imagen corresponde a la versión 6.002 de Aranda 360.

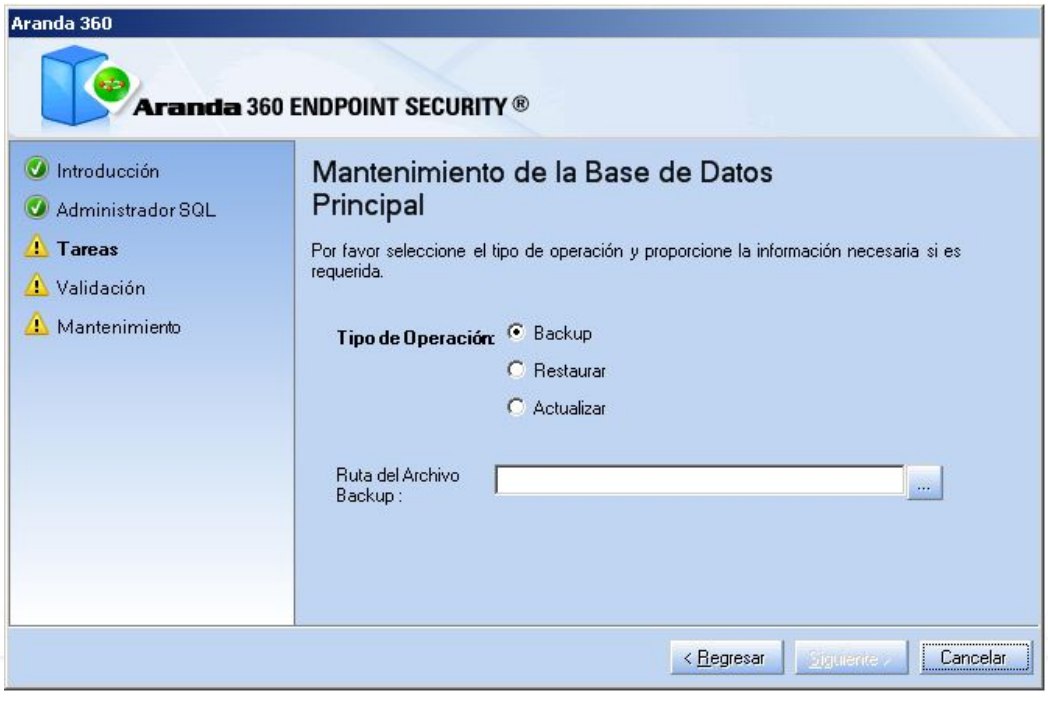
4. Haga clic en siguiente para abrir la ventana que establece la conexión a la base de datos.



5. Digite:
    - La cuenta de usuario y contraseña del administrador para establecer conexión a la base de datos (cuenta sa).
    - La instancia de la base de datos.
    - Haga clic en siguiente.

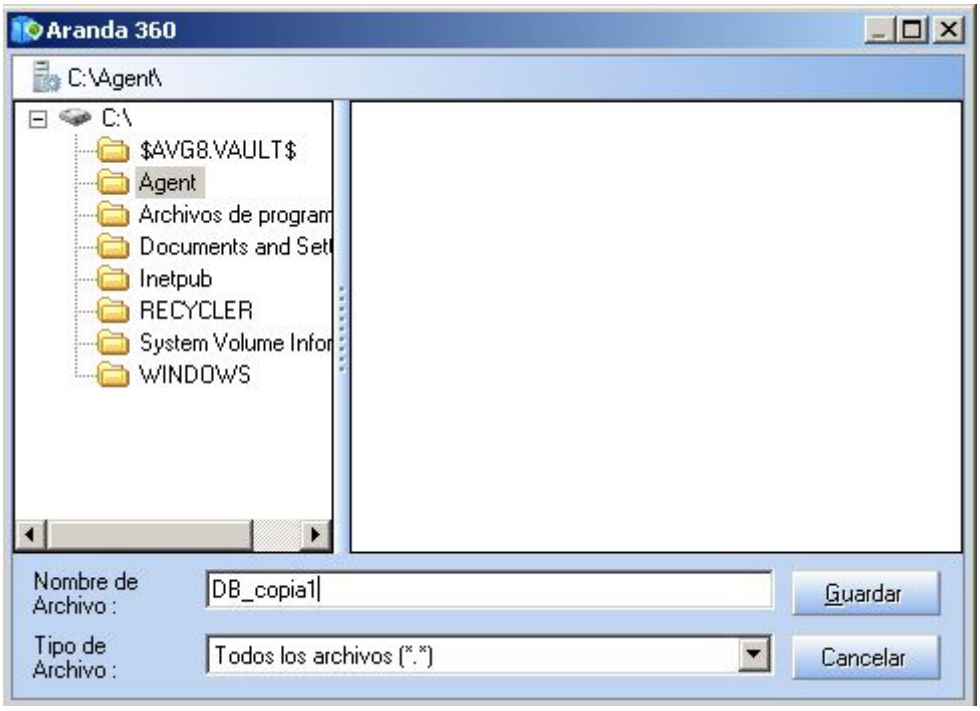


6. Debajo de tipo de operación, haga clic en la opción de copia de seguridad.

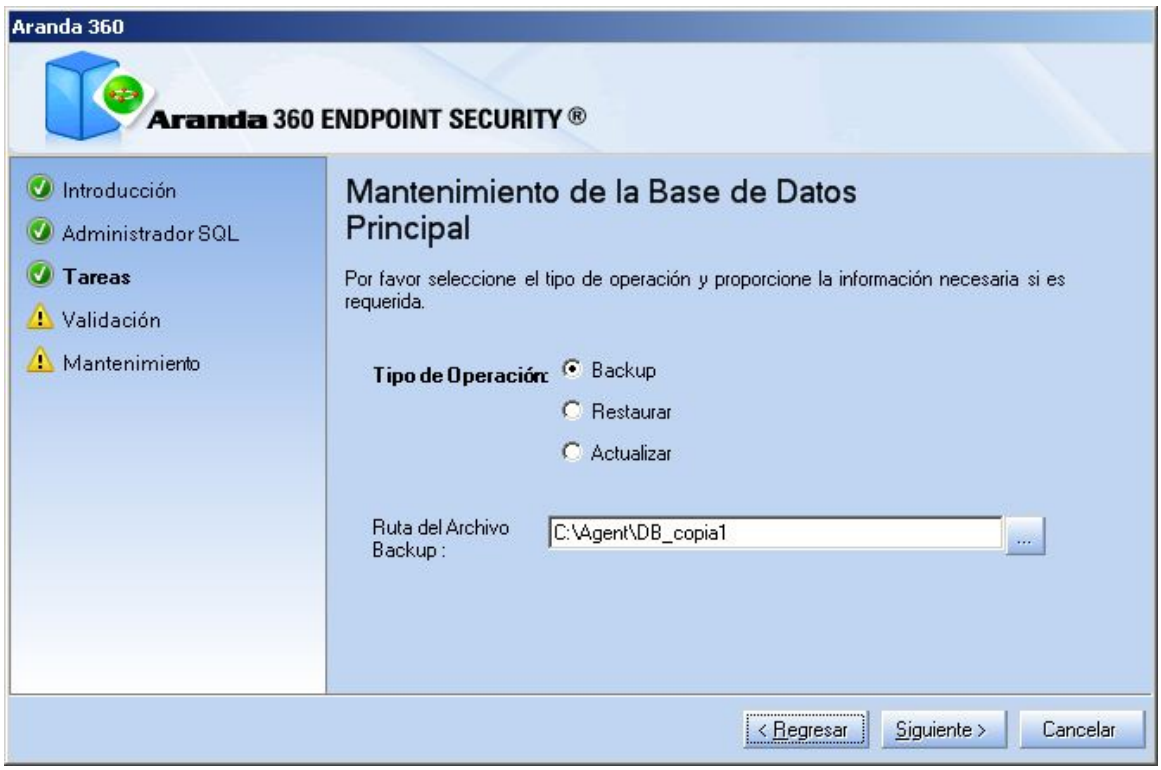


7. Clic ... en para seleccionar la ruta donde se guardara la copia de seguridad. Digite un nombre para el archivo.

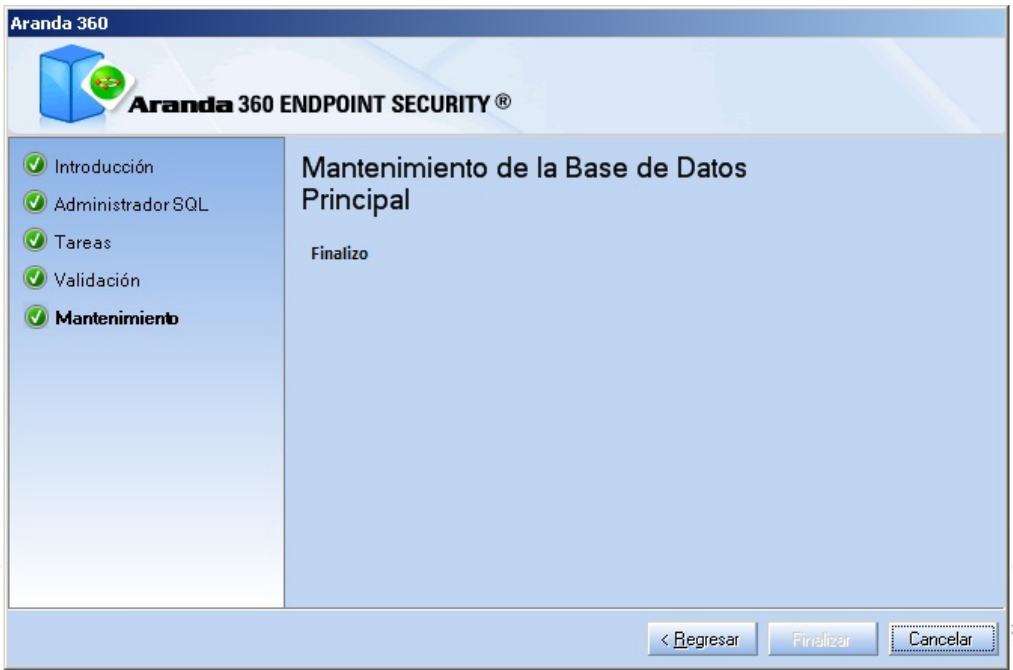
   Haga clic en guardar.
   La copia de seguridad se guardara en la máquina donde se encuentra la base de datos.



8. Haga clic en siguiente.



9. Un resumen es presentado.
   Haga clic en siguiente.



10. Haga clic en finalizar

para completar la instalación.

Guardando la base de datos de claves

Para guardar la base de datos de las claves, siga los siguientes pasos:

1. Ejecute DbInstaller.
2. Haga clic en Mantenimiento de la Base de Datos de claves.
3. Repita los pasos del 1 al 9 en " Guardando la base de datos de la consola " .

Guardando la base de datos de Alertas (logs)

Esta operación es opcional. Requiere la herramienta de administración de SQL Server.

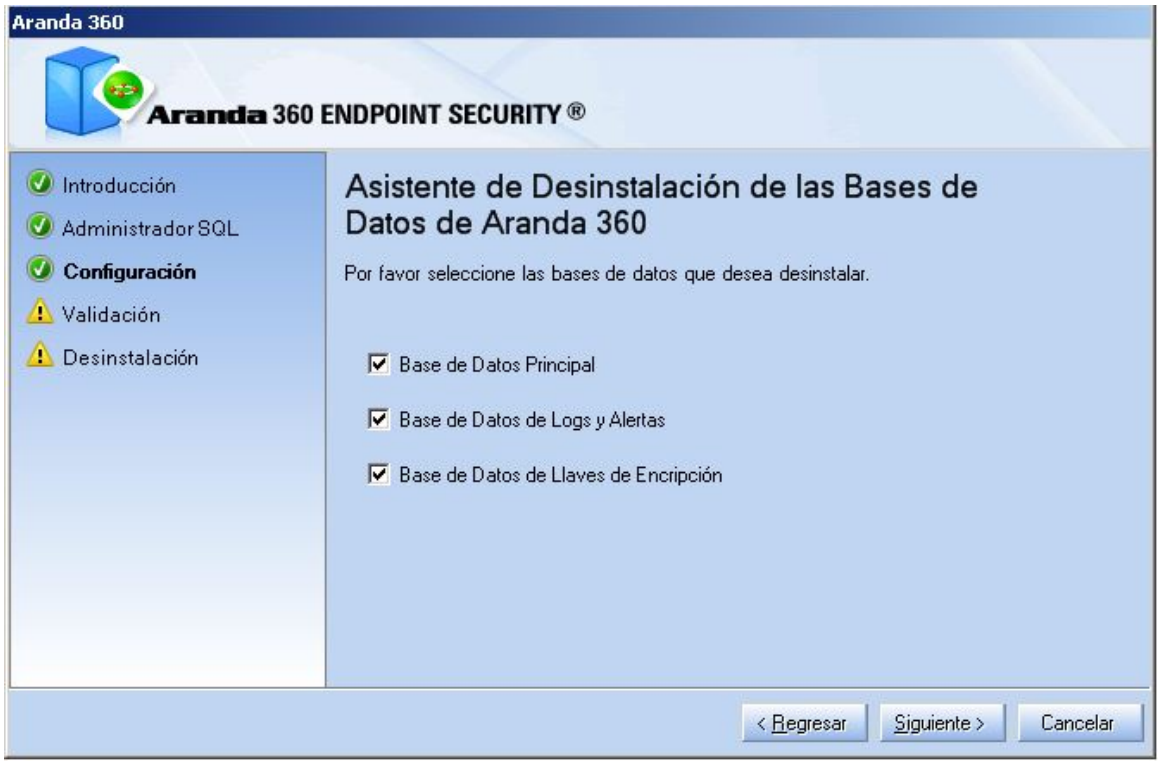
Para obtener más información, contacte al Administrador de la base de datos o nuestro servicio Profesional en support@Aranda.com.

Desinstalando la base de datos

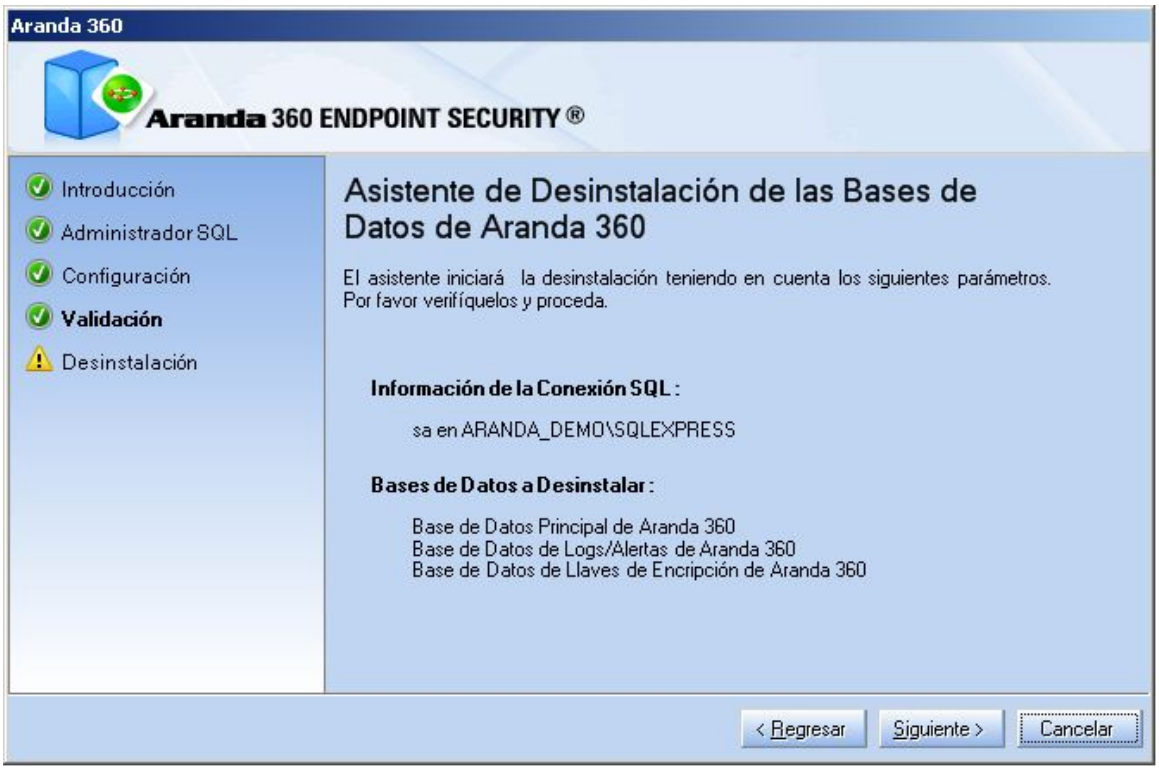
Para desinstalar la base de datos de las claves, siga los siguientes pasos::

1. Ejecute DbInstaller.
2. Haga clic en Desinstalar Base de Datos Aranda 360.
3. Seleccione la base de datos que desea desinstalar.

Haga clic en siguiente.



4. Un resumen es presentado.
   Haga clic en siguiente.



5. Haga clic en finalizar para completar el proceso de desinstalación.

Desinstalando la base de datos

Para desinstalar el servidor de base de datos (MSDE o SQL Server 2000), utilice la herramienta de desinstalación ubicada en:

- Menú Inicio.
- Agregar o Remover programas dentro del Panel de Control.

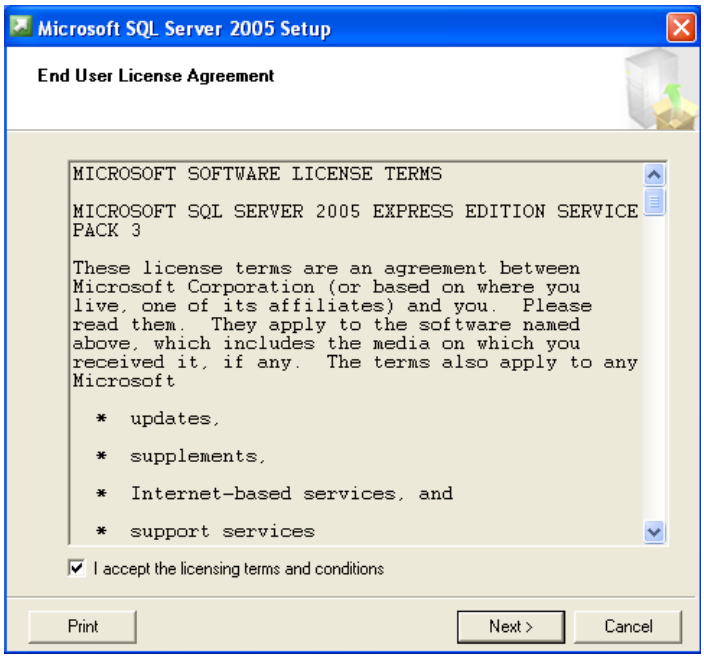
Instalando el nuevo servidor de base de datos

Primero que todo, verifique que el archivo SQLEXPR.exe (MS SQL Server 2005 Express Edition) y si es requerido, el archivo SSMSEE.msi (Servicios avanzados para MS SQL Server 2005

Express Edition) están presentes en la estación de trabajo.

Para instalar MS SQL Server 2005, siga los siguientes pasos:

1. Haga clic en SQLEXPR.exe.
2. Aparecerá la siguiente ventana.



3. Defina la configuración para el nuevo servidor de base de datos

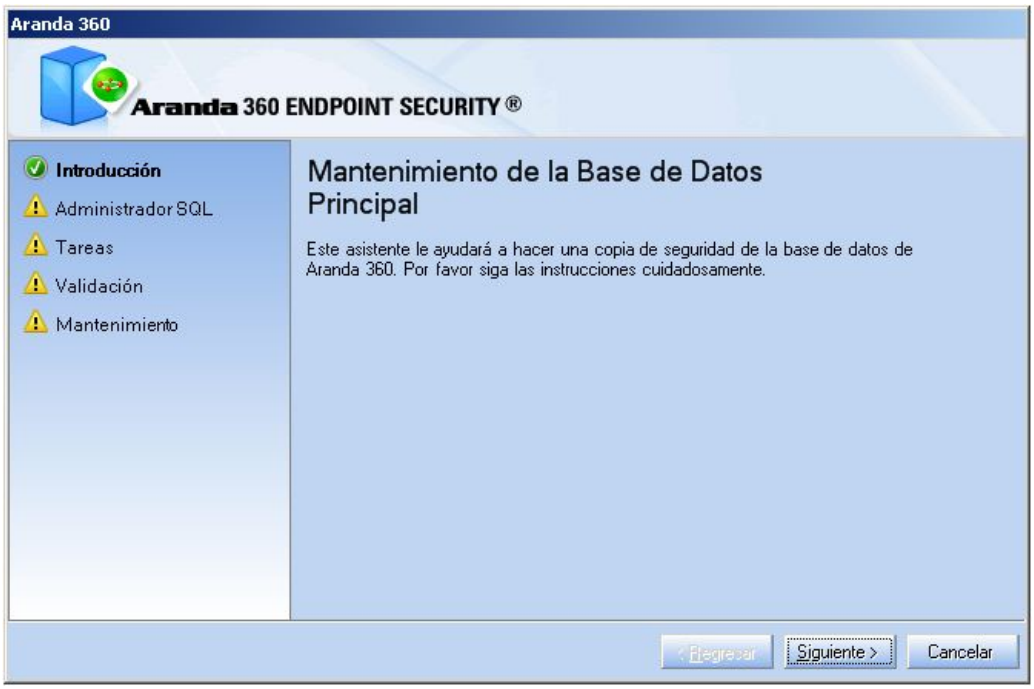
- Cuando instale la base de datos, utilice autenticación Modo Mixto.

Restaurando la base de datos

Restaurando la base de datos de la consola

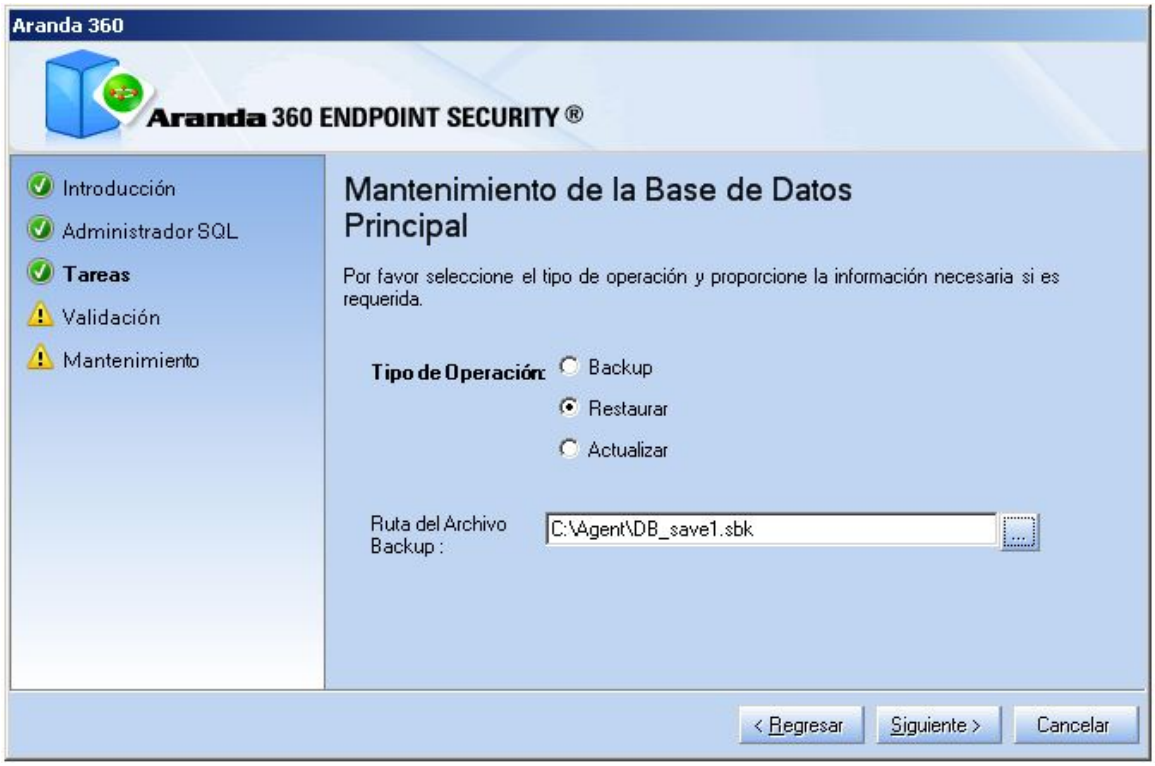
Para restaurar la base de datos de la consola, siga los siguientes pasos:

1. Ejecute DbInstaller.
2. Haga clic en Mantenimiento de la Base de Datos de la Consola.
3. Haga clic en siguiente.

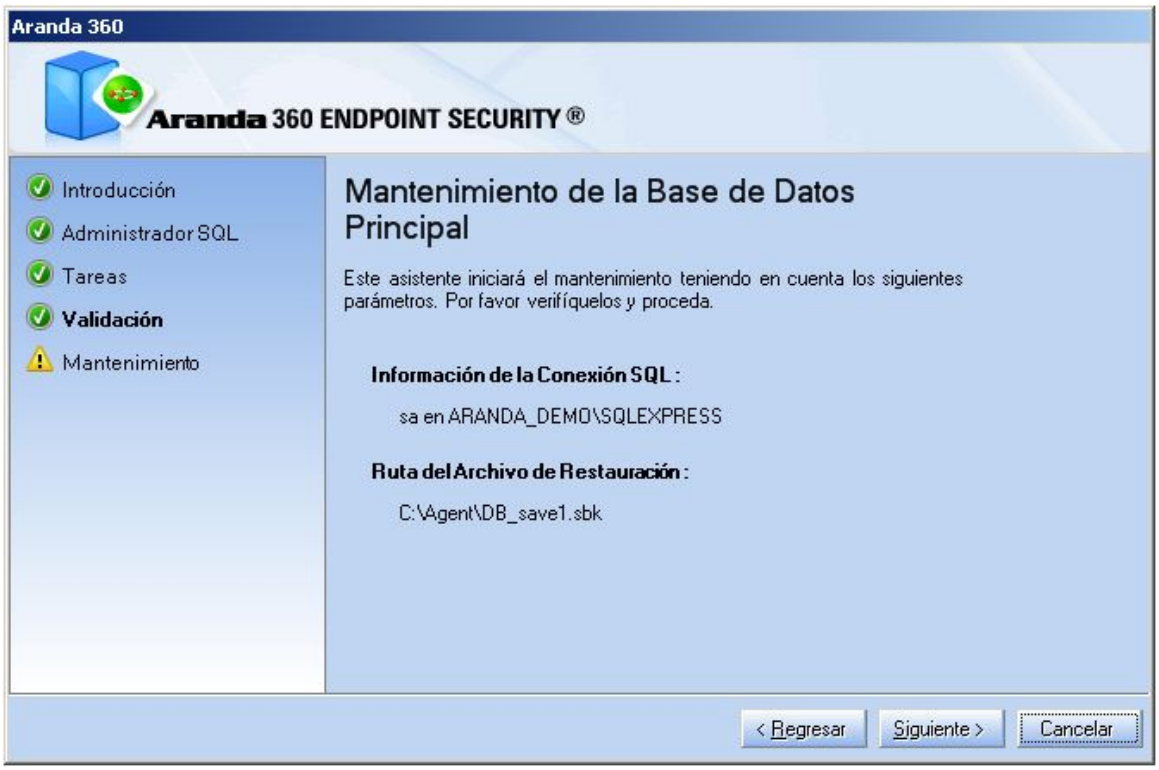


4. Diligencie la información requerida y haga clic en siguiente

5. Debajo de tipo de operación, haga clic en la opción de Restaurar.
   Haga Clic para seleccionar la ruta y el archivo para la restauración.



6. Verifique la información mostrada.
   Haga clic en siguiente.



7. Haga clic en finalizar para completar el proceso de restauración.

Restaurando la base de datos de claves

Para restaurar la base de datos de claves, siga los siguientes pasos:

1. Ejecute DbInstaller.
2. Haga clic en mantenimiento de base de datos de claves.
3. Haga clic en siguiente.
4. Diligencie la información requerida y haga clic en siguiente.
5. Debajo de tipo de operación, haga clic en la opción de Restaurar.
   Haga clic para seleccionar la ruta y el archivo para la restauración.
6. Verifique la información.
   Haga clic en siguiente..
7. Haga clic en finalizar para completar el proceso de restauración.

Restaurando la base de datos de alertas

Esta operación es opcional.

Verificando los cambios

Para verificar que la base de datos ha sido restaurada correctamente y que MS SQL Server 2005 opera adecuadamente, conéctese al ADMINISTRADOR de la consola (versión 5.2).

Descargando nuevos parches

Antes de actualizar Aranda 360, primero deben descargarse los parches utilizando el enlace suministrador por Aranda Systems.

- Si desea actualizar únicamente el servidor Aranda 360, solo descargue el parche para éste.

Antes de actualizar Aranda 360 a una nueva versión, existen seis parches para ser descargados:

- Servidor:
  - Aranda 360server_win32_5.2xx.srh
  - Aranda 360server_win32_5.2xx.sru
- Consola:
  - Arandaconsole_win32_5.2xx.srh
  - Arandaconsole_win32_5.2xx.sru
- Agente:
  - Aranda 360agent_win32_5.2xx.srh
  - Aranda 360agent_win32_5.2xx.sru

- Aclaraciones:
  - El símbolo xx corresponde al número de versión de la actualización.
  - Archivos con la extensión .srh son encabezados de los parches.
  - Archivos con extensión .sru son parches.
  - Los encabezados son usados para la autenticación de los parches.Aclaraciones:

  - El símbolo xx corresponde al número de versión de la actualización.
  - Archivos con la extensión .srh son encabezados de los parches.
  - Archivos con extensión .sru son parches.
  - Los encabezados son usados para la autenticación de los parches.

Reiniciando el servicio del servidor Aranda 360

Reinicie el servicio (srservice.exe) para forzar el proceso de actualización.
Para obtener más información, ver “Actualizando el servidor Aranda 360”

Actualizando la Licencia

Después de actualizar la consola de administración a la versión 6.0, actualice su licencia.

Para obtener más información, ver:

- Actualizando la consola de administración ”
- ” Aplicando una licencia a un ambiente ”

Una licencia es requerida por ambiente.

CON MS SQL SERVER 2005

REQUISITOS

Guardando la base de datos

- En la versión 6.0, la base de datos incluye:
  - La base de datos de la consola.
  - La base de datos de alertas.
  - La base de datos de claves.

- Para guardar la base de datos en un directorio diferente al que viene por defecto (ejemplo: .\Mssql\Backup), asigne permisos de Lectura/Escritura al grupo de seguridad SQLServer2005MSSQLUser$ServerName$SQLInstance.

Guardando la base de datos de la Consola

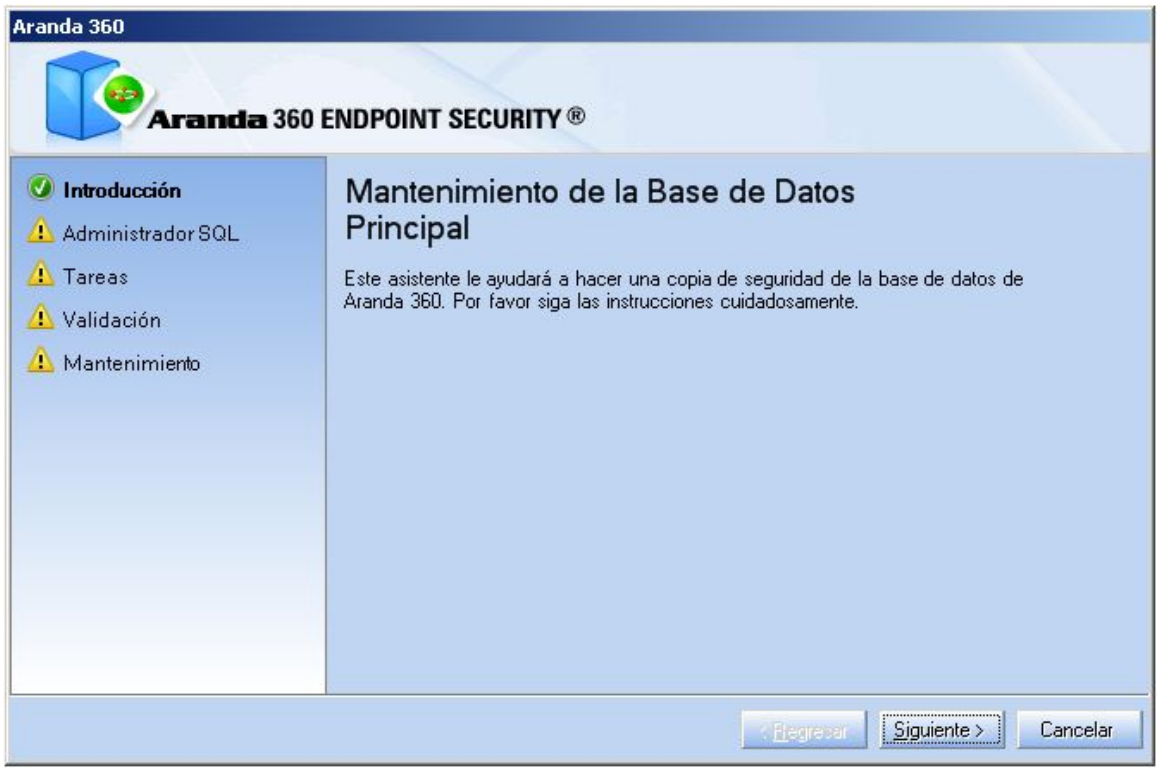
Para guardar la base de datos de la consola, siga los siguientes pasos:

1. Cierre la consola de administración.
2. Ejecute el archivo DbInstaller.exe que se encuentra por defecto en:
   C:\ Archivos de Programa\Aranda\Aranda Management Console\DBInstall

   DbInstaller.exe se puede acceder desde el menú inicio.
   Esto iniciará la herramienta de administración de la base de datos.

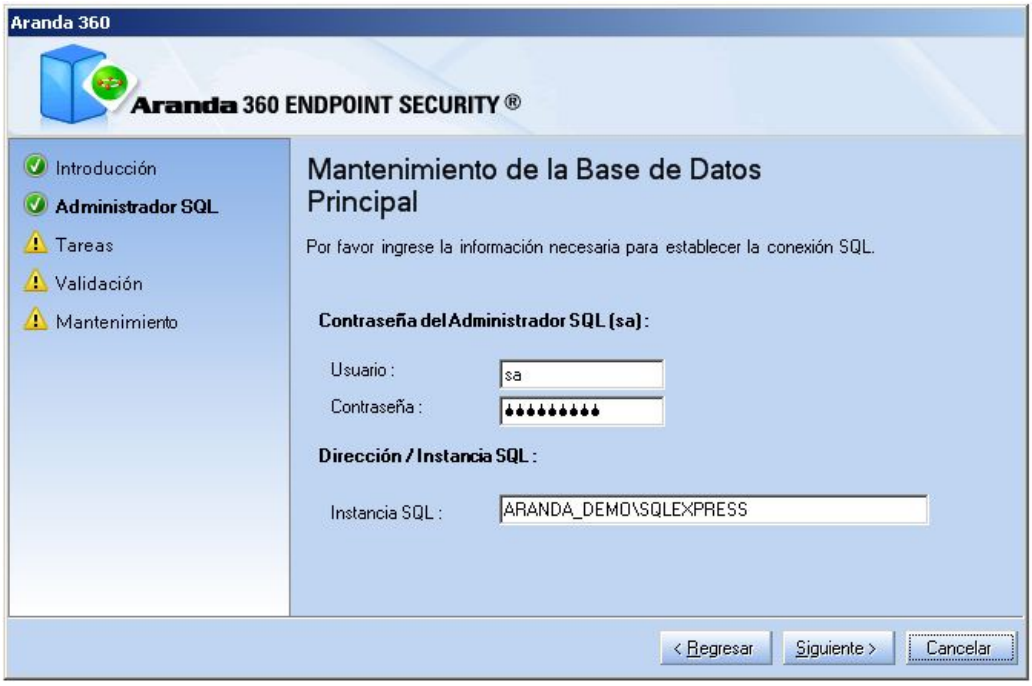
3. Seleccione mantenimiento de la base de datos de la consola.

4. Haga clic en siguiente para abrir la ventana que establece la conexión a la base de datos.



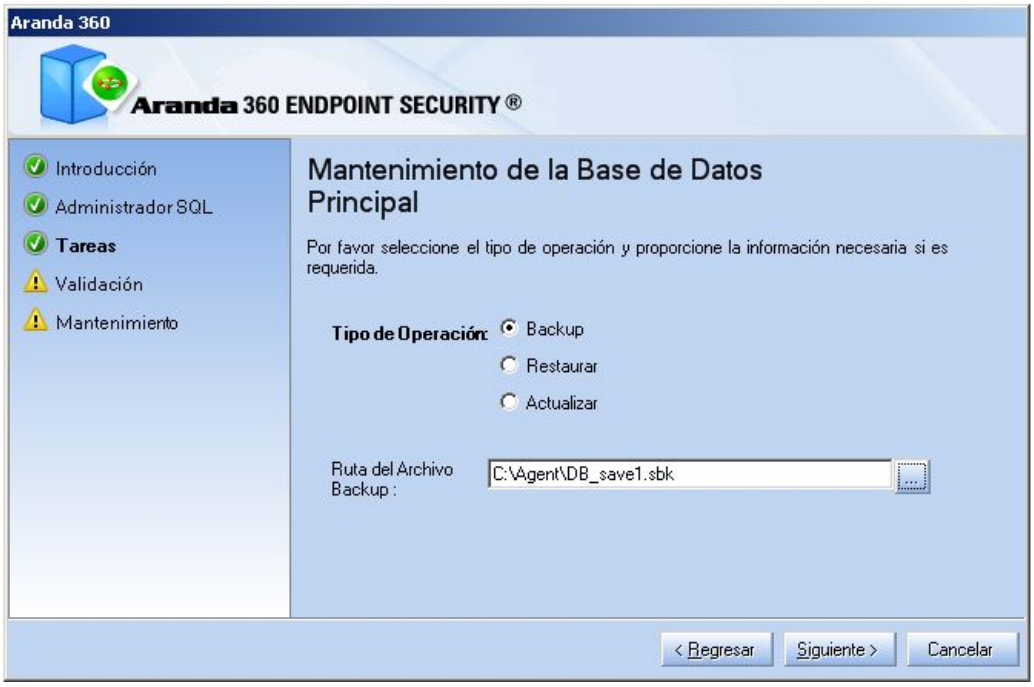
5. Introduzca:

   - La cuenta de usuario y contraseña del administrador para establecer conexión a la base de datos (cuenta sa).
   - La dirección IP o el nombre de la netbios del servidor de base de datos. Si algunas instancias son instaladas, éstas pueden ser especificadas.
     Ejemplo: [database IP instance]\EDDAS.
   - Haga clic en siguiente.

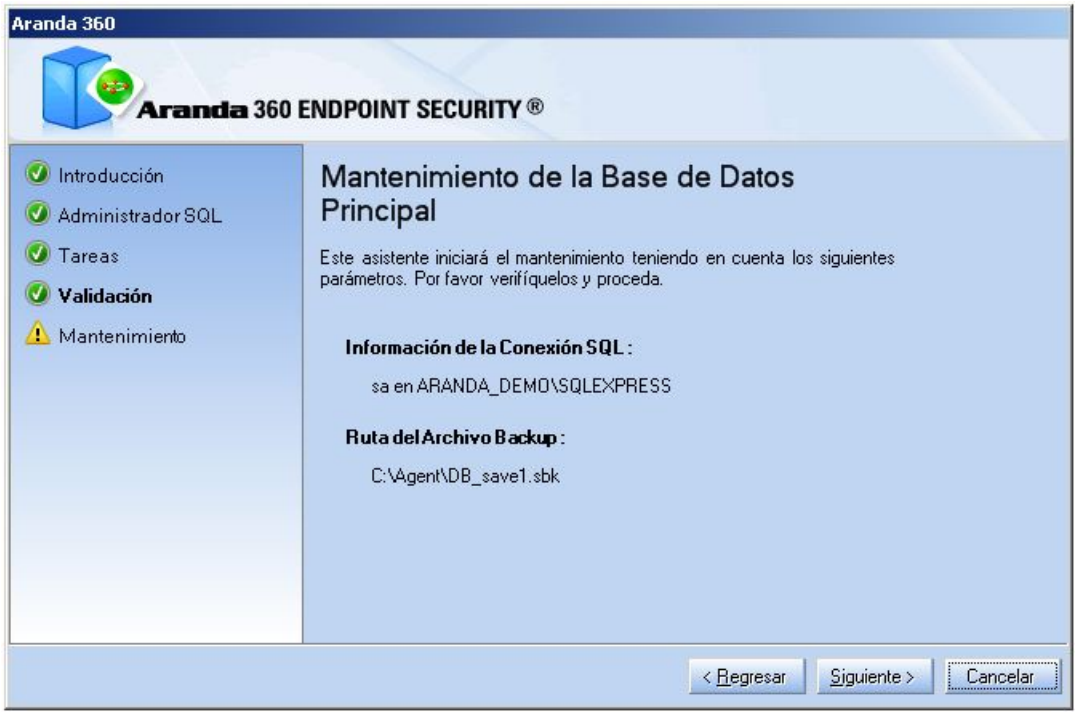


6. Debajo de tipo de operación, seleccione la opción salvar.

7. Haga clic -• para seleccionar la ruta de la copia de seguridad y digitar el nombre del archivo.
   Haga clic en Guardar.
   La copia de seguridad será guardada en la máquina donde está instalada la base de datos.



8. Un resumen es presentado.
   Haga clic en siguiente.



9. Haga clic en finalizar para completar la copia de seguridad.

Guardando la base de datos de claves

Repita el procedimiento "Guardando la base de datos de la consola".

Guardando la base de datos de alertas

Repita el procedimiento "Guardando la base de datos de la consola".

Descargando Parches

Antes de actualizar Aranda 360, primero deben descargarse los parches utilizando el enlace suministrador por Aranda Systems.

- Si desea actualizar únicamente el servidor Aranda 360, solo descargue el parche para éste.
- Si desea definir por separado los parámetros de actualización para el servidor y los agentes, utilice Implementar Actualización por defecto (por ejemplo 5.700) en [servidor Principal]> Actualizaciones de software

Antes de actualizar Aranda 360 a una nueva versión, existen seis parches para ser descargados:

- Servidor:
  - stormshieldserver_win32_6.0xx.srh
  - stormshieldserver_win32_6.0xx.sru
- Consola:
  - skyreconconsole_win32_6.0xx.srh
  - skyreconconsole_win32_6.0xx.sru
- Agente:
  - stormshieldagent_win32_6.0xx.srh
  - stormshieldagent_win32_6.0xx.sru

- Aclaraciones:
  - El símbolo xx corresponde al número de versión de la actualización.
  - Archivos con la extensión .srh son encabezados de los parches.
  - Archivos con extensión .sru son parches.
  - Los encabezados son usados para la autenticación de los parches

PROCEDIMIENTO

Actualizando el agente

Existen dos formas para actualizar el agente:

- Actualización automática.
- Actualización manual.

Actualización automática

Copie los archivos de actualización del agente en la carpeta patchs, que se encuentra por defecto en la siguiente ruta:

C:\Archivos de programa\Aranda\Aranda 360 Server

- Si un agente se conecta a un servidor secundario, éste descargará los parches desde el servidor principal para distribuirlos a los agentes conectados.

Los agentes descargarán la actualización y la instalarán automáticamente (sin intervención del usuario).
La actualización después de que el agente ha sido reiniciado. Sin embargo, Aranda 360 continuara protegiendo la máquina.

Actualización Manual

- Tel agente debe estar habilitado para conectarse al servidor para ser actualizado manualmente

Para actualizar el agente manualmente, siga los siguientes pasos:

1. Verifique la versión del agente abriendo el archivo version.sro, el cual está localizado en: C:\Archivos de Programa\Aranda\Aranda 360 Agent\conf

2. Renombre el parche con el número de versión que tenga actualmente el agente instalado. Por ejemplo, si está actualizando desde la versión 5.2 a la 6.0, renombre el parche:

    - Aranda 360agent_win32_5.7.srh en Aranda 360agent_win32_5.2.srh
    - Aranda 360agent_win32_5.7.sru en Aranda 360agent_win32_5.2.sru

3. Para la actualización, copie los archivos de parches del agente en la carpeta patchs, que se encuentra por defecto en la siguiente ruta:
   C:\Archivos de Programa\Aranda\Aranda 360 Agent\

4. Para actualizar inmediatamente, fuerce la conexión entre la agente y el servidor:
    - Haga clic derecho en el icono del Monitor Aranda 360 localizado en la bandeja del sistema.
    - Vaya a Otras operaciones > reconectar al servidor.

Cuando el agente inicia el proceso de actualización, el archivo updater.sro es creado en la carpeta patchs.
Los cambios realizados al agente serán aplicados después de reiniciar.

5. Reinicie la máquina una vez haya recibido está notificación al completar el proceso de actualización.

- A diferencia de procedimiento para actualizar el servidor, el archivo updater.sro es borrado después del reinicio.

Actualización el servidor Aranda 360

Para actualizar el servidor , siga los siguientes pasos:

1. Copie los archivos de actualización del servidor en la carpeta patchs, que se encuentra por defecto en la siguiente ruta: C:\Program Files\Aranda\Aranda 360 Server
2. El servidor será actualizado de acuerdo a las configuraciones definidas en el servidor principal.
3. Cuando el servidor inicia el proceso de actualización automático, el archivo updater.sro aparecerá en la carpeta patchs.
   La actualización se ejecuta en segundo plano y toma alrededor de cinco minutos. Una vez se haya completa la actualización:
   - El archivo updater.sro es removido.
   - El archivo log.txt es creado en la carpeta Log, ésta se encuentra en la raíz del servidor.
   - El servidor principal también envía actualizaciones a los servidores secundarios.
     Los servidores secundarios tiene el mismo proceso de actualización del servidor principal.
4. Reinicie el servidor donde están instalados los parches. Es posible posponer el reinicio pero se requiere actualizar el servicio (srservice.exe).

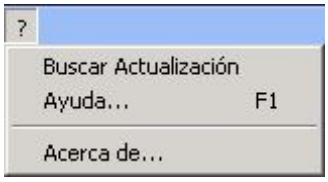
- Actualizando el servidor Aranda 360 no implica la actualización del servidor Apache. Puede manualmente aplicar actualizaciones ejecutando «skyapache.exe --update» localizado en Archivos de Programa\Aranda\Aranda 360 Server\ Apache\conf desde la línea de comandos. Los archivos antiguos son renombrados a httpd.conf.old y ssl.conf.old. Reinicie el servidor para que los cambios sean aplicados

Actualizando la consola de administración

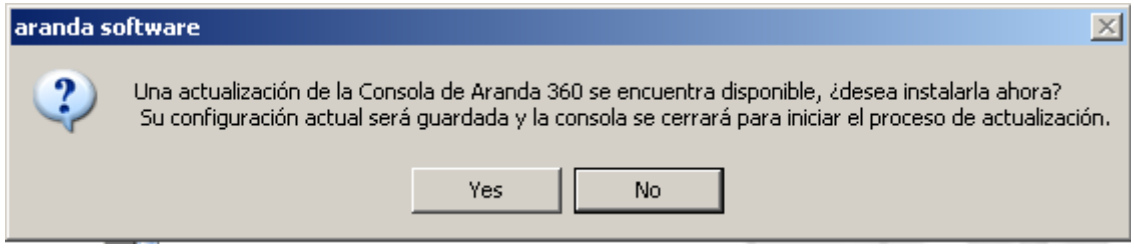
Para actualizar la consola de administración, siga los siguientes pasos:

1. Copie los archivos de actualización de la consola en la carpeta patchs, que se encuentra por defecto en la siguiente ruta: C:\Program Files\Aranda\Aranda 360 Server

2. En la consola, haga clic en y seleccione verificar actualización.

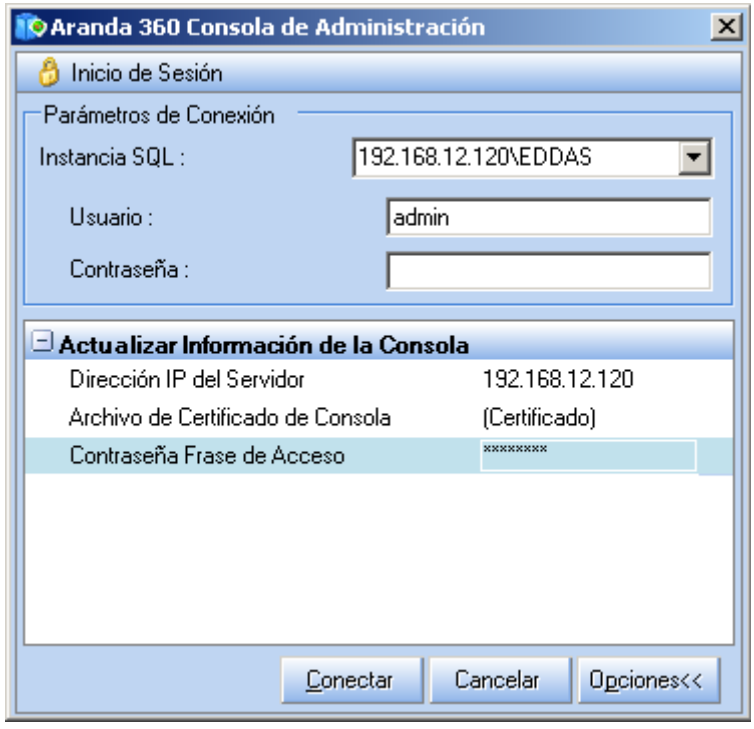


3. Se abrirá un cuadro de dialogo informando que la actualización está disponible.



Haga clic en Sí.

4. Para actualizar otras consolas, diligencie la información requerida para establecer conexión entre la(s) consola(s) y el servidor:
   - Haga clic en Opciones.



- Actualice la información de la consola utilizando:
  - Dirección IP del servidor.
  - Certificado de la consola:
    Especifique la ruta del donde se encuentra el certificado. Este archivo protege las comunicaciones entre el servidor principal y la consola.
  - Contraseña:
    Establezca la contraseña al instalar el servidor para prevenir el uso indebido de los certificados.

5. Haga clic en Conectar.
   La consola de administración se abrirá.

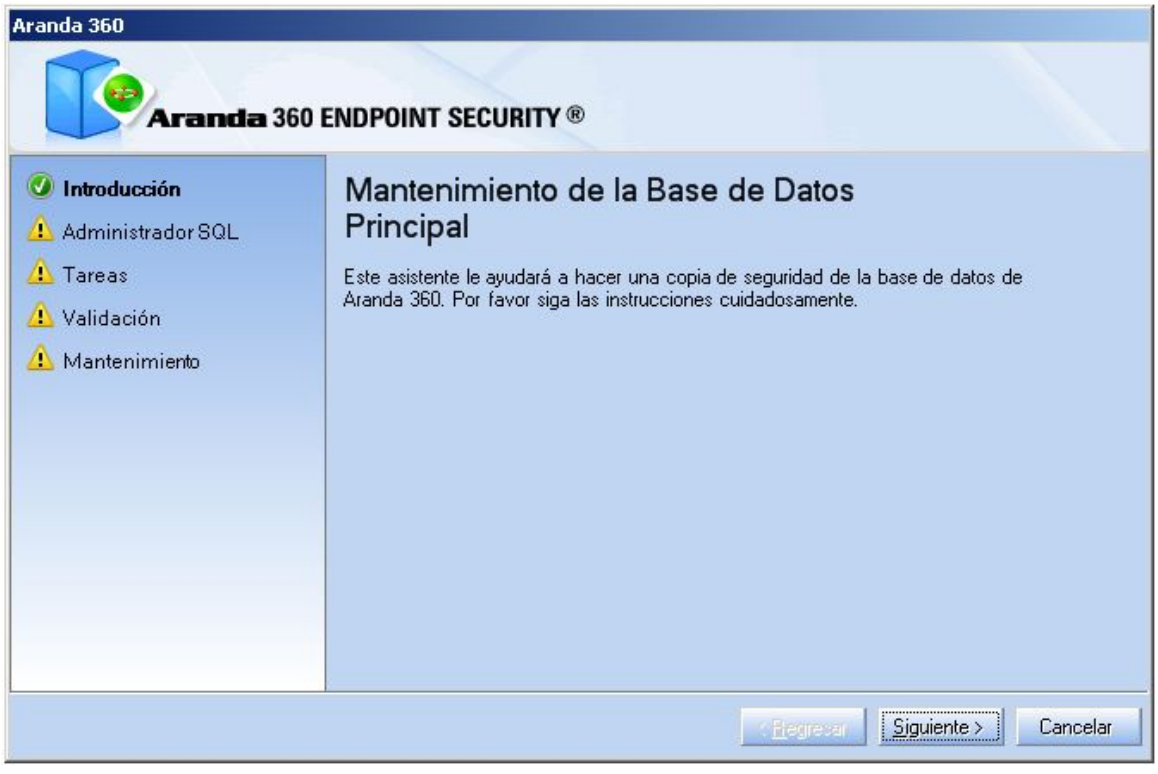
Ahora, debe actualizar las bases de datos (base de datos de la consola, alertas y claves) para que las versiones de la consola y las bases de datos estén sincronizadas.

Actualizando la base de datos

Actualizando la base de datos de la consola

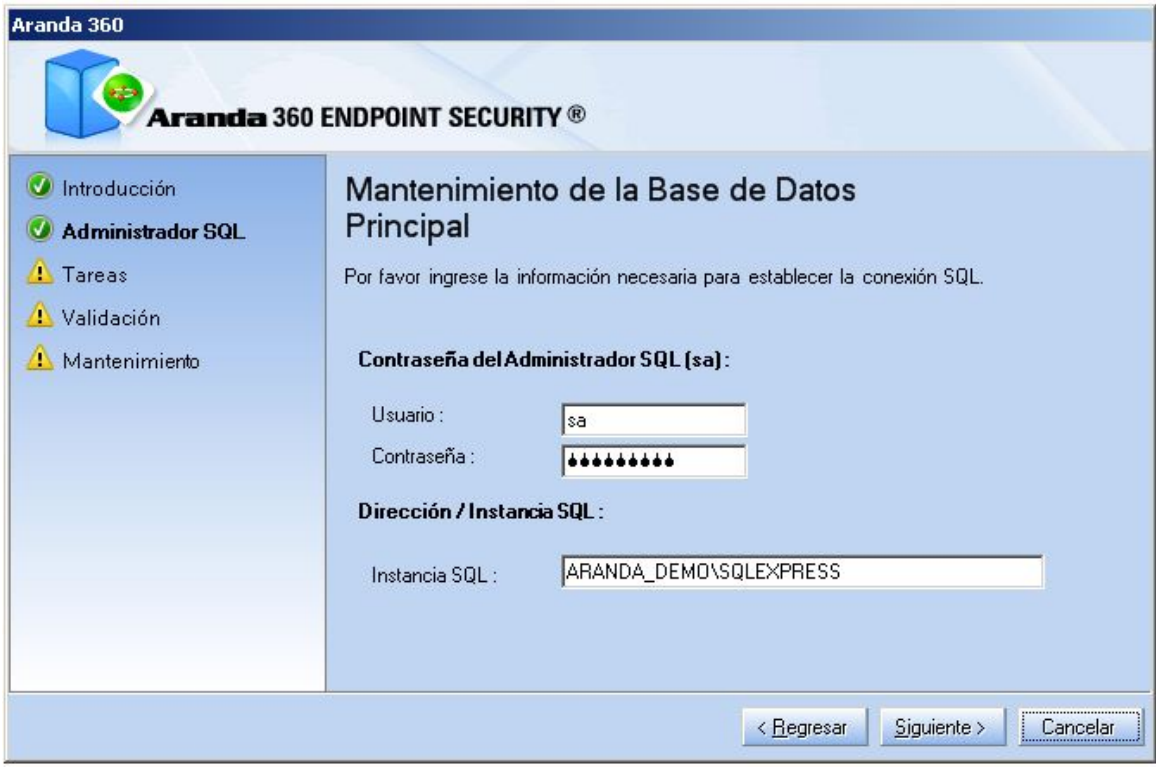
Para actualizar la base de datos de la consola, ejecute la utilidad DBInstaller , el cual puede ser localizado en el menú inicio.

1. Ejecute DBinstaller.exe.
2. Aparecerá lo siguiente ventana.

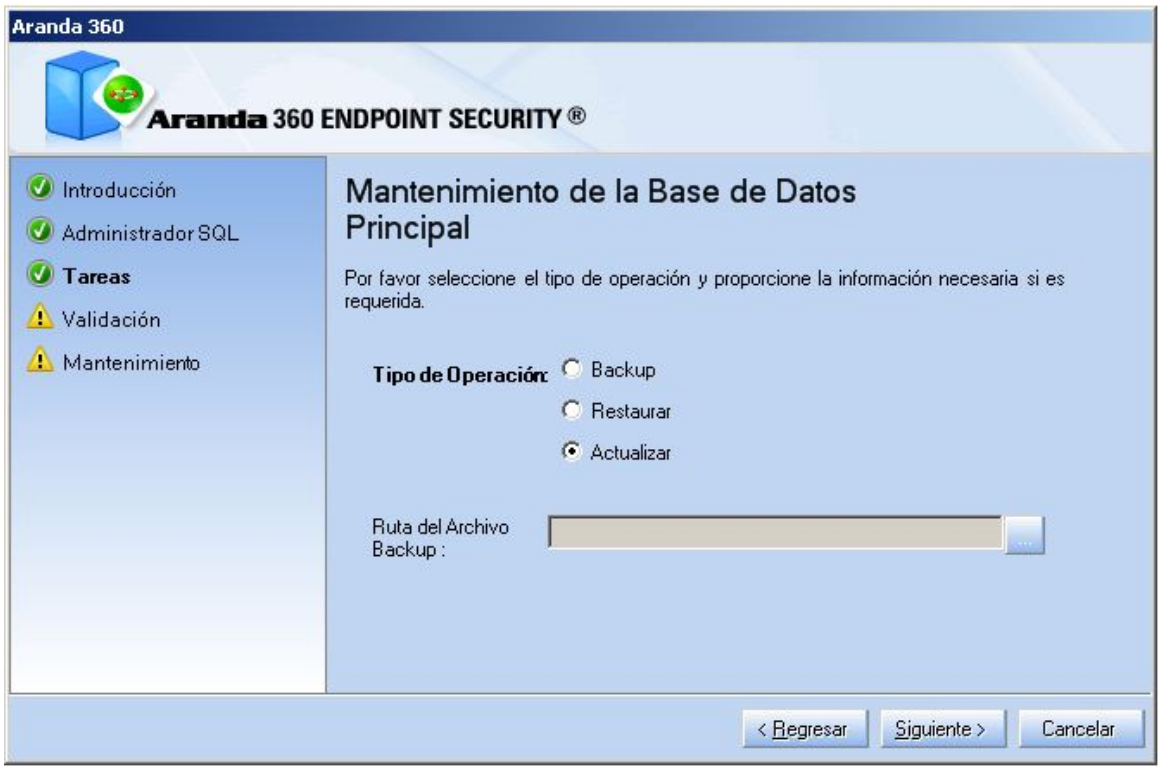


Haga clic en siguiente.

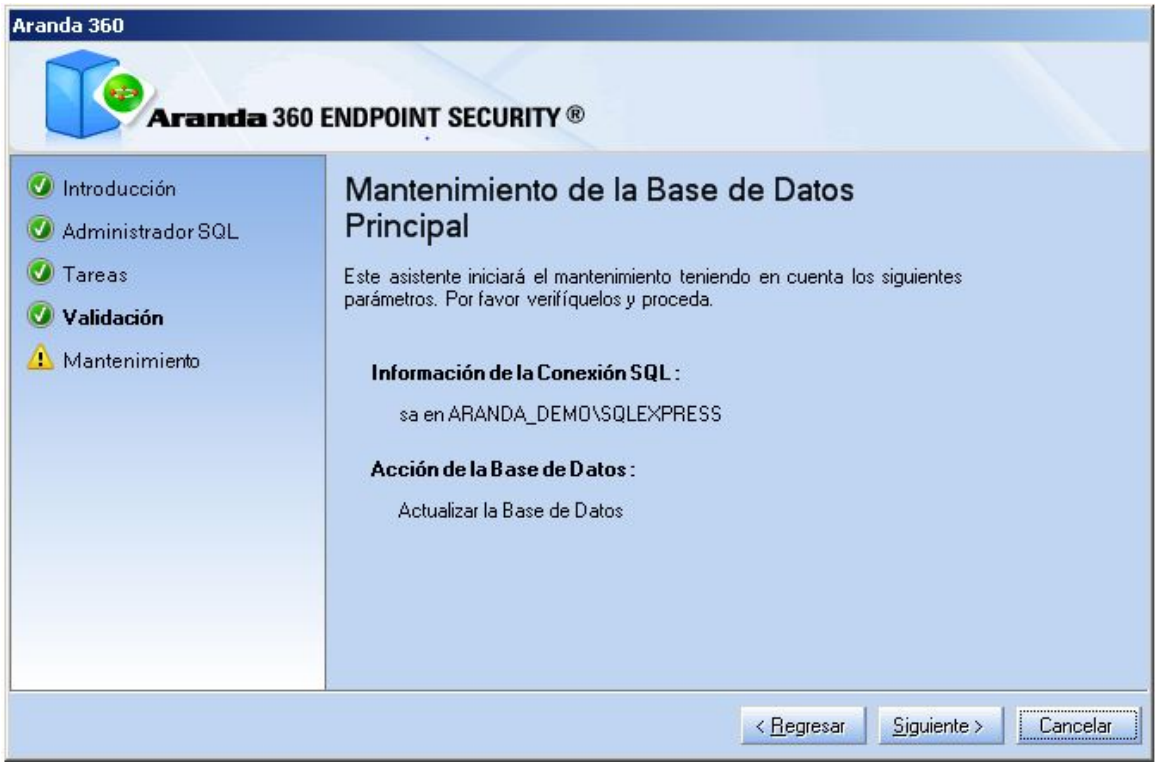
3. Diligencie la información requerida.



4. Seleccione Actualizar.
   Haga clic en siguiente.



5. Verifique la información.
   Haga clic en siguiente.



6. Espere hasta que el proceso de actualización haya terminado.
   Haga clic en Finalizar.

Actualizando la base de datos de alertas

1. Ejecute DBInstaller.exe.
2. Seleccione Mantenimiento de la Base de Datos de alertas.
3. Repita los mismos pasos de “Actualizando la base de datos de la consola". En caso de tener el paquete Professional Edition, el proceso de actualización está terminado.
   Si está ejecutando el paquete Secure Edition, vaya a “Actualizando la base de datos de claves”.

Actualizando la base de datos de claves

Si está ejecutando el paquete Secure Edition, siga los siguientes pasos:

1. Ejecute el archivo DBInstaller.exe.
2. Seleccione Mantenimiento de la Base de Datos de claves.
3. Repita los mismos pasos de “Actualizando la base de datos de la consola ”

El proceso de actualización está terminado. Ahora, puede usar la consola de Administración. Continúe con el proceso de actualización del servidor Aranda 360 y los agentes.

Capítulo 4 - CONFIGURACIÓN DE LA CONSOLA DE ADMINISTRACIÓN

ACERCA DE ESTE CAPÍTULO

Éste capítulo presenta la consola de administración de Aranda y la configuración por parte del administrador

Contiene lo siguiente:

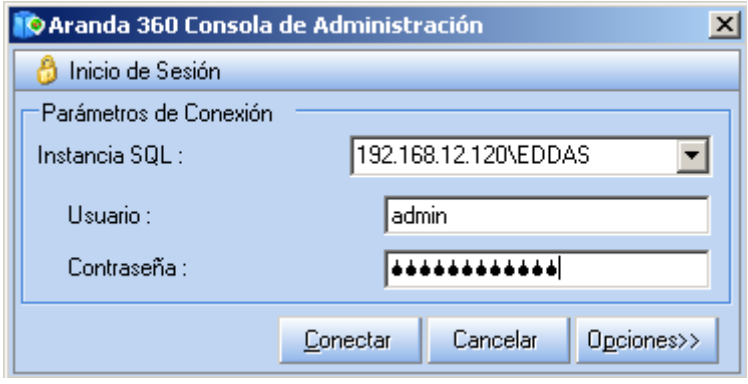
- Primeros pasos con la consola.
- Generalidades de la consola:
  - Administrador de ambientes.
  - Herramienta de administración y monitoreo.
  - Panel de configuración.

PRIMEROS PASOS

La consola de administración puede ser iniciada de dos formas:

- Desde el menú inicio, seleccione:
  Programas > Aranda > Aranda Management Console

- Desde el escritorio::
  - Haga doble clic en el ícono de la consola de administración
  - Digite el usuario y contraseña.
  - Haga clic en Conectar (o presione la tecla Enter) para acceder a la consola de administración.



- Si es la primera vez que utiliza la consola.

GENERALIDADES DE LA CONSOLA

La interfaz de la consola de administración aparecerá de esta forma:

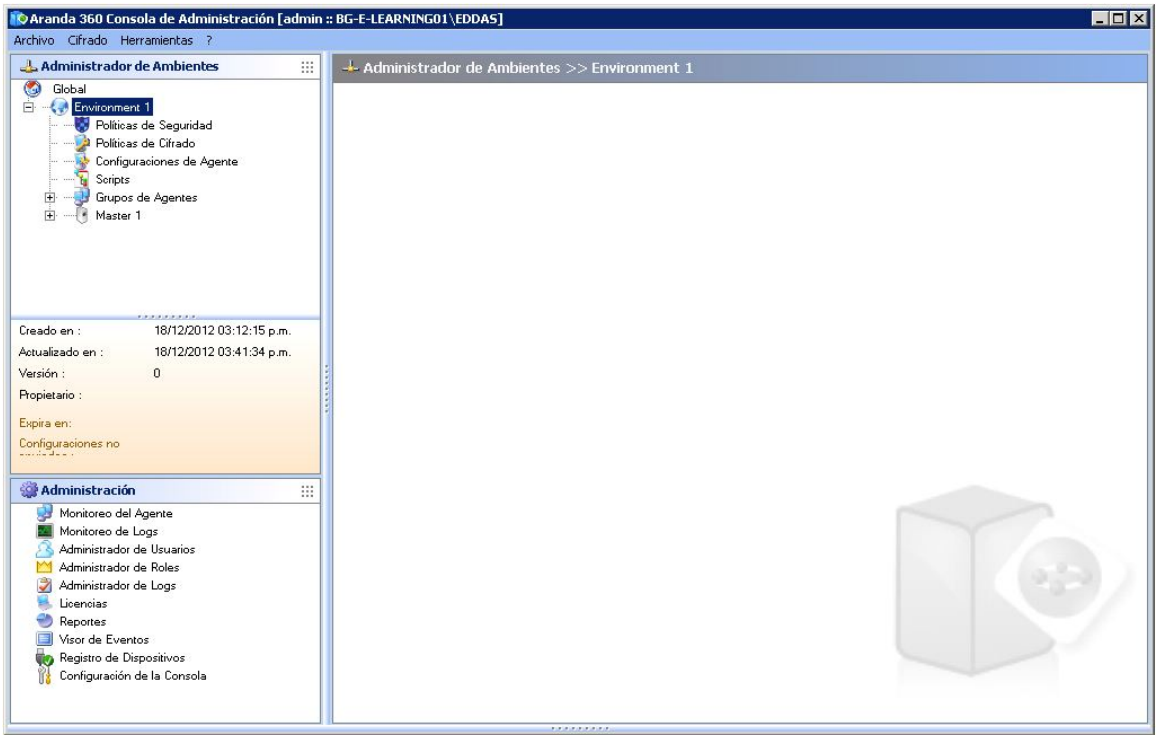
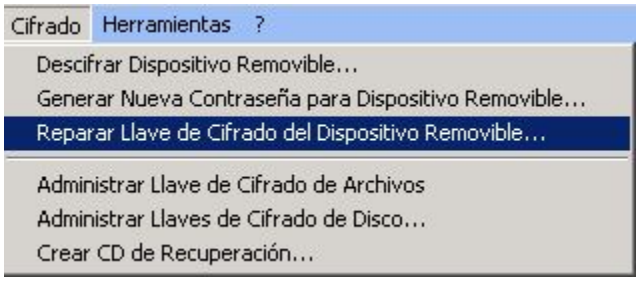


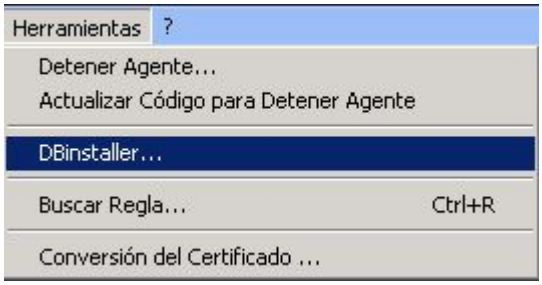
Fig. 4.1: Interfaz de la consola de administración

- Menú:
  Este es el menú estándar de Windows, el cual brinda el acceso a varias características de la consola:
  - Archivo:

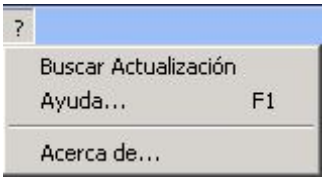
- Cifrado:



- Herramientas:



- ? :



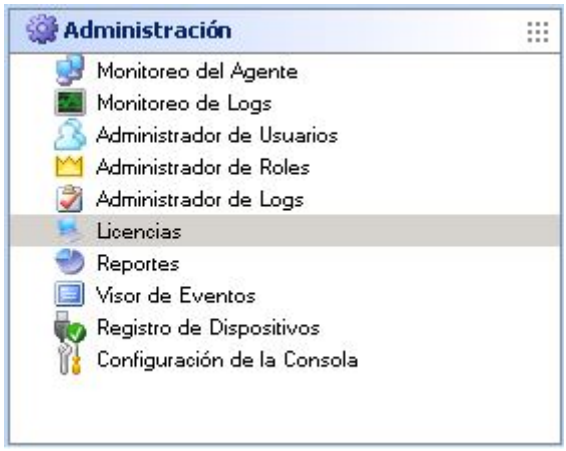
- Administrador:
  En esta parte se manejan:
  - Políticas (seguridad, cifrado, antivirus).
  - Configuraciones.
  - Scripts.
  - Grupo de agentes (asignado a varios servidores principales).
  - Servidores (principal y secundario).

- Detalles de la versión:

Aquí se explica:

- Fecha de creación de la consola.
- Fecha de actualización de la consola.
- Versión (Ejemplo: Política 1, versión 2).
- Dueño (admin).
- Fecha de expiración de la consola (Cualquiera).
- La fecha de la última configuración enviada.
- Número de sincronizaciones.

- Herramientas de Administración y Monitoreo:



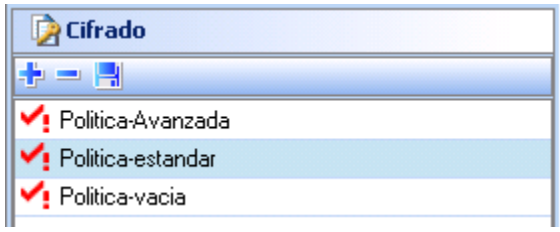
En esta sección se visualiza y se modifica:

- Agentes.
- Logs.
- Usuarios.
- Roles.
- Licencias.
- Reportes.
- Eventos.
- Consola.

ADMINISTRADOR DE AMBIENTES

El administrador de ambiente, valga la redundancia, es donde se crean los ambientes

- Para aplicar políticas de seguridad a un grupo de agentes, verifique que la opción Versión Preliminar, que se encuentra en el menú emergente del administrador de ambientes (clic derecho) se encuentra desmarcado.
  La versión preliminar previene que un administrador aplique una política de seguridad a un grupo de agentes, sin ésta haber sido validada.
  Los nombres de las políticas de seguridad son editadas en rojo cuando la versión preliminar está habilitada.
  Cuando una política de seguridad está siendo editada por el administrador, un bloqueo es mostrado a los demás administradores que estén usando la consola. Ellos no estarán habilitados para mostrar la versión preliminar de la política de seguridad.



Ambiente

El primer nivel corresponde al ambiente.

Aquí se manejan:

- Políticas (seguridad, cifrado, antivirus).
- Configuraciones.
- Scripts.
- Grupo de agentes.
- Servidores.

Cada ambiente es asociado con cualquier número de servidores principales y un ilimitado número de servidores secundaros.

Las estaciones de trabajo para ser protegidas son asignadas a un único ambiente. Pueden ser reunidos en grupos de agentes que son homogéneos desde el punto de vista de seguridad.

La formación de grupos de agentes pueden estar basados en:

- Direccionamiento IP.
- Nombre de la máquina.
- Directorio Activo.

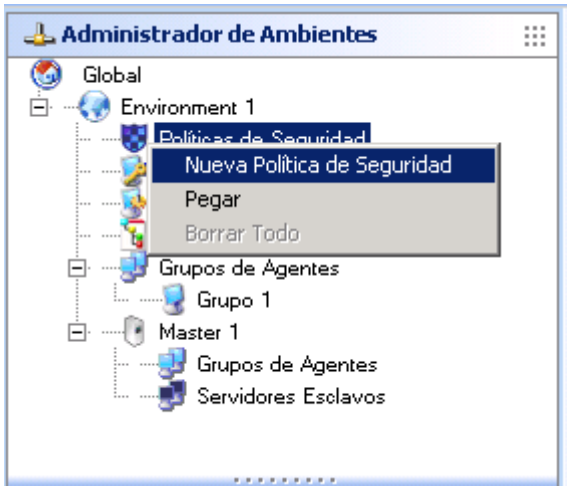
Cuando el direccionamiento IP es utilizado, una simple o lista de direcciones IP, o una dirección de subred puede ser especificada.

Cuando Directorio Activo es utilizado, es posible apuntar el nombre o grupo de máquinas declaradas en el directorio (ejemplo: en forma de una unidad organizacional (OU)).

Políticas

Las Políticas son manejadas bajo tres escenarios:

1. Creación de políticas:
   Las políticas son creadas en el administrador de ambientes.

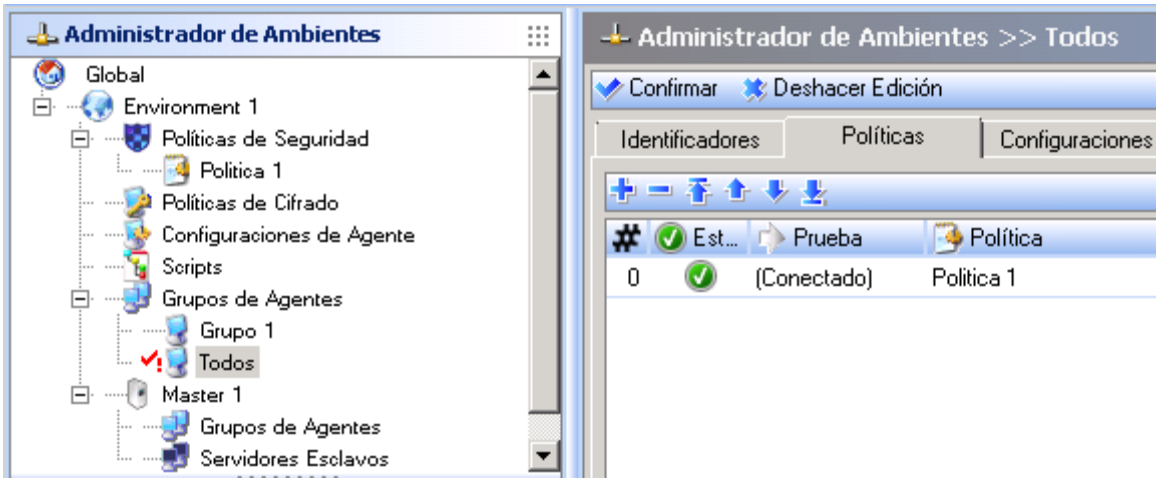


2. Configuración de políticas:
   Las políticas son configuradas en el Editor de Políticas de Seguridad.

El editor de Políticas de Seguridad es utilizado para crear y nombrar las políticas, las cuales pueden contener una combinación de:

- Reglas de protección automática.
- Reglas de Firewall.
- Permisos de acceso a la aplicación.
- Protección de los componentes del núcleo.
- Comportamiento de la aplicación.
- Permisos sobre los dispositivos.

3. Asignación de políticas:
   Las políticas son asignadas a grupos de agentes a través del ADMINISTRADOR de ambientes en la etiqueta de Políticas.



Grupos de Agentes

Los grupos de agentes son manejados en modo estándar o en modo avanzado

Modo estándar

El modo estándar es manejado de la siguiente forma:

- Generalidades del grupo de agentes.
- Asignación de grupos de agentes a servidores principales.
- Implementación de políticas para grupos de agentes y recopilación de logs.

Generalidades

Los grupos de agentes se pueden encontrar en al árbol del primer nivel del administrador de ambientes.

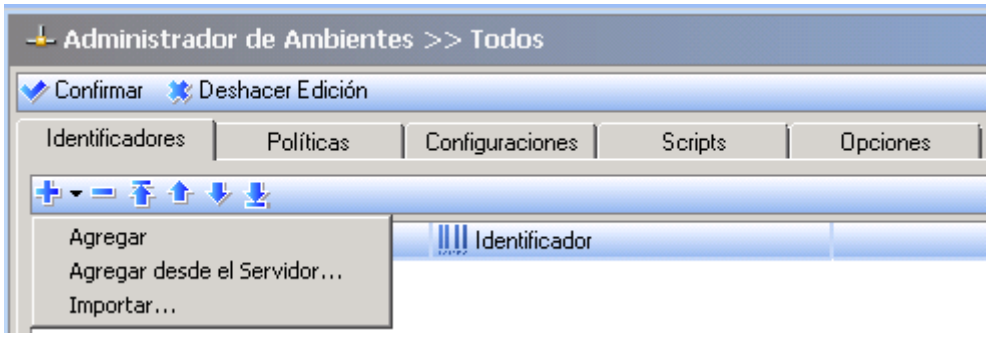
Fig. 4.2. Grupos de agentes en una estructura de árbol

La implementación de los agentes y políticas de seguridad requieren una operación preliminar. Los agentes deben ser identificados para acceder a las estaciones de trabajo para ser protegidas.

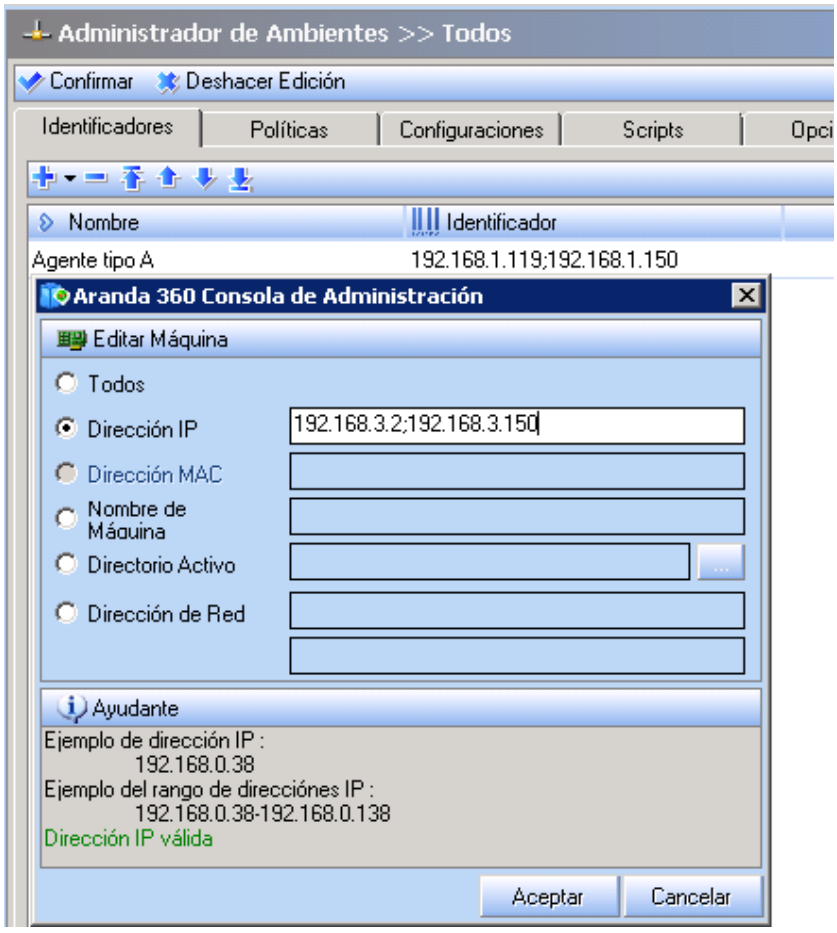
- Por defecto, al crear un ambiente, la opción Grupos de Agentes está vacía pero disponible.

Para identificar los grupos de agentes, siga los siguientes pasos:

1. Vaya al nivel Grupos de Agentes en el Administrador de Ambientes.
2. Edite el grupo a ser identificado.
3. Agregue y defina los identificadores de los agentes a través de la barra de herramientas y ..., Para agregar un identificador, hay tres opciones disponibles:



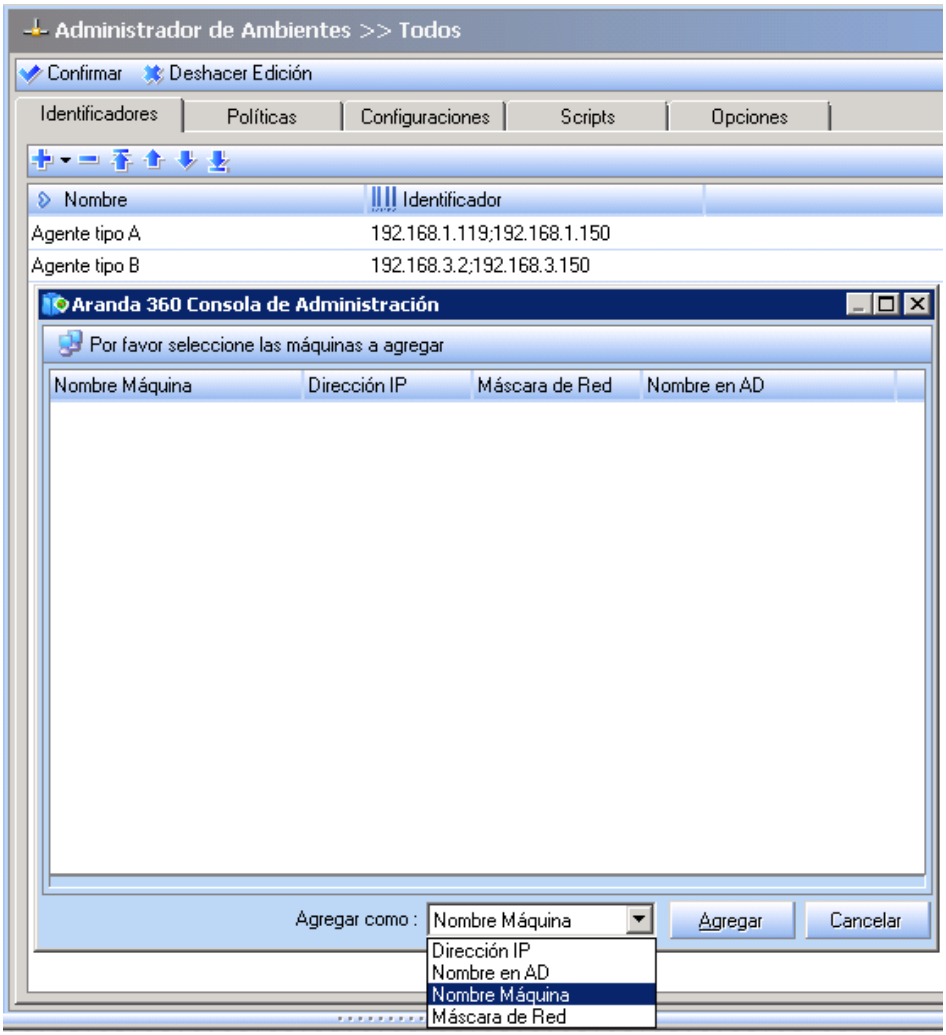
- Agregar



Esta opción es utilizada para agregar un identificador a través de las siguientes opciones:

- Todos:
  Todos los agentes serán agregados al grupo.
- Dirección IP:
  Los agentes que coincidan con la dirección IP serán agregados al grupo.
- Nombre de Host:
  Los agentes que coincidan con el nombre del host serán agregados al grupo. Es posible utilizar el comodín (*).
  Ejemplo: Workstation*.
- Directorio Activo:
  Los agentes que coincidan con el nombre AD u OU serán agregados al grupo.
- Dirección de subred:
  Los agentes que pertenezcan a la dirección de la subred especificada serán agregados al grupo.

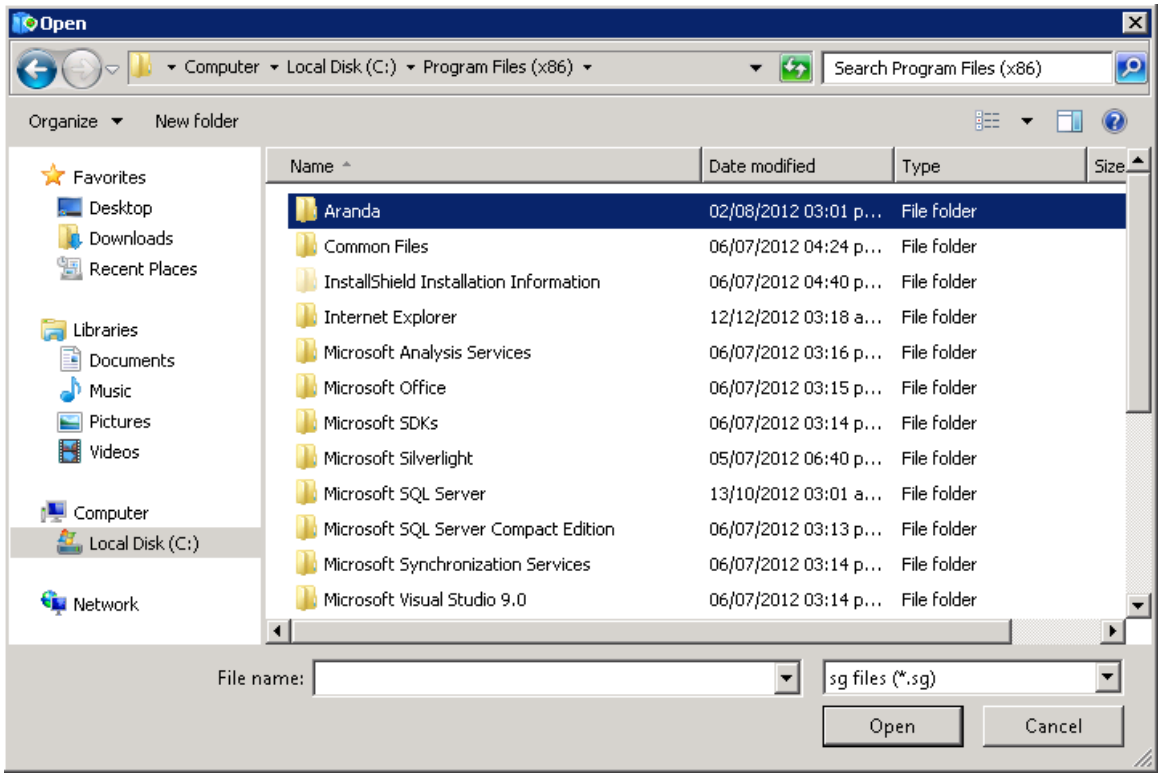
- Importe desde el servidor.



Esta opción es utilizada para agregar un identificador a través de las siguientes opciones:

- Nombre maquina.
- Dirección IP.
- Nombre en AD.
- Máscara de Red.

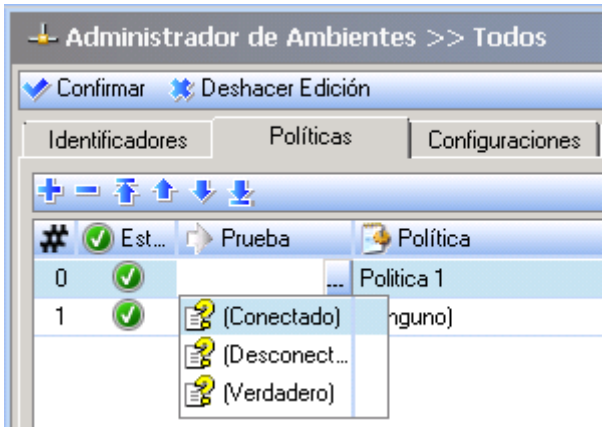
- Importar
  Esta opción es utilizada para agregar un identificador a través de la siguiente ventana:



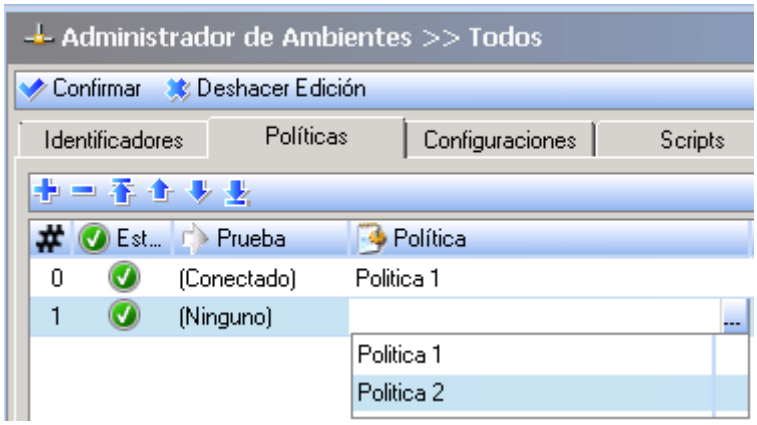
4. Agregue y defina las políticas a través de la barra de herramientas y ...

   - Verifique el estado.

   - Seleccione la prueba a ser aplicada.

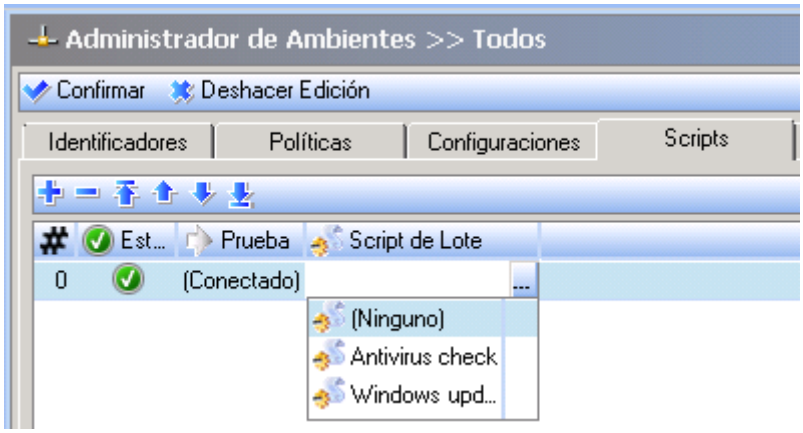


- Seleccione la política de seguridad.

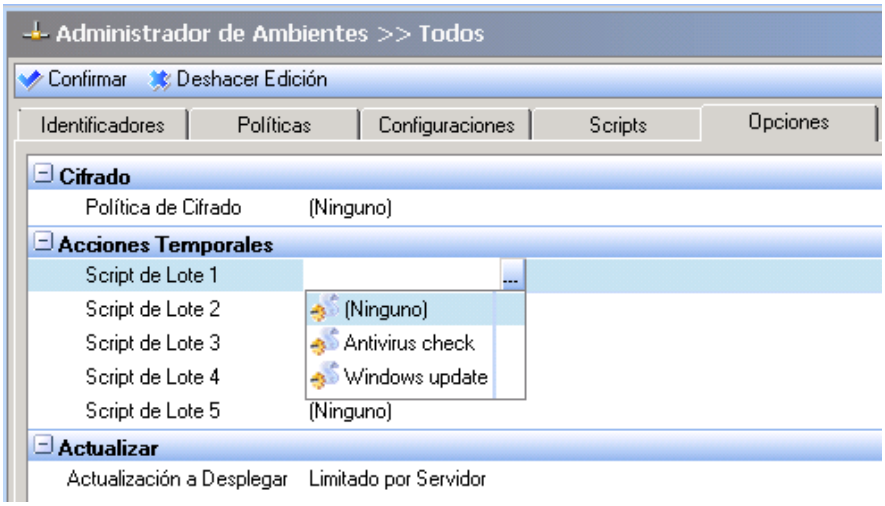


5. Agregue y defina la configuración a través de la barra de herramientas y ...

6. Agregue y defina los scripts a través de la barra de herramientas y ...



7. Agregue y defina las opciones a través de la barra de herramientas y ....



8. Haga clic para validar los parámetros.

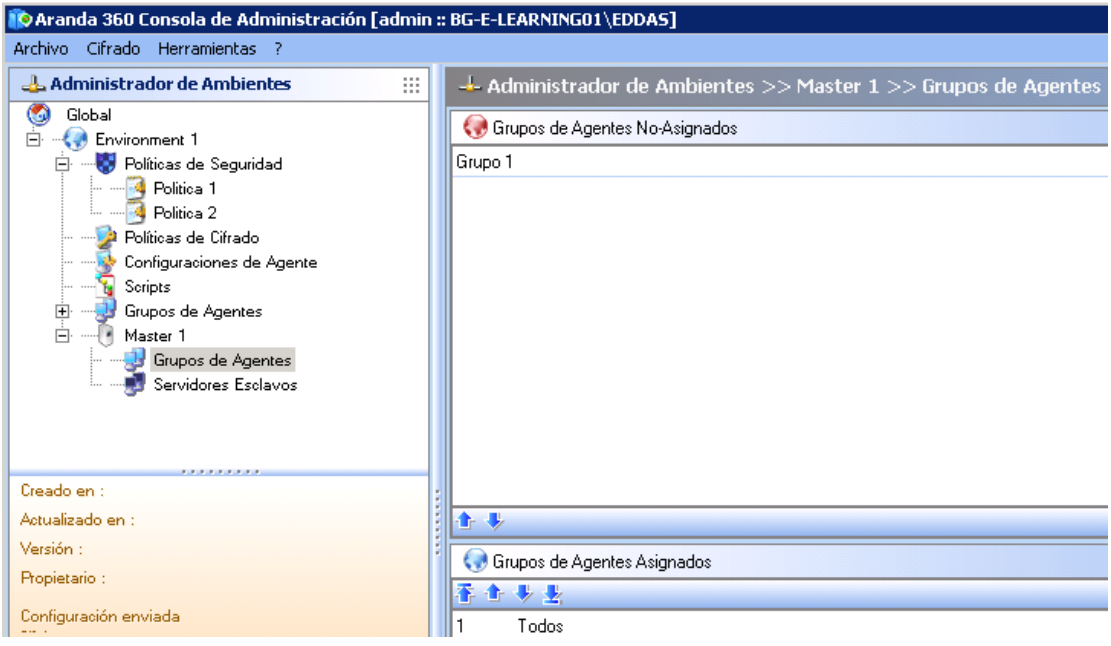
Asignado grupos de agentes a los servidores principales

Después de crear un grupo de agentes, éstos no son asignados a cualquier servidor principal. Esta operación debe ser hecha manualmente para cada servidor.

- Un grupo de agentes puede ser asignado a varios servidores principales

Para asignar grupos de agentes, siga los siguientes pasos:

1. Haga clic en grupos de agentes bajo el servidor principal.



2. Mueva los grupos de agentes no asignados al panel de grupos usando las flechas.

El orden de los grupos de agentes es importante ya que la primera regla encontrada es usada para la configuración al conectarse un agente al servidor.

Implementando las políticas y recopilación de logs

Las políticas de seguridad son implementadas y la información de las actividades de los agentes es recopilada por medio de tokens.

Por intervalos regulares de tiempo definidos por el administrador, el servidor notifica a los agentes por medio de tokens. Éstos son enviados de una máquina a otra y regresados al servidor.

Este modelo de comunicación protege la red de un ataque de denegación de servicios causado por un gran número de agentes intentándose conectar simultáneamente al servidor.

Al recibir el token, cada agente realiza alguna acción como actualizar políticas de seguridad o trasmitir logs al servidor.

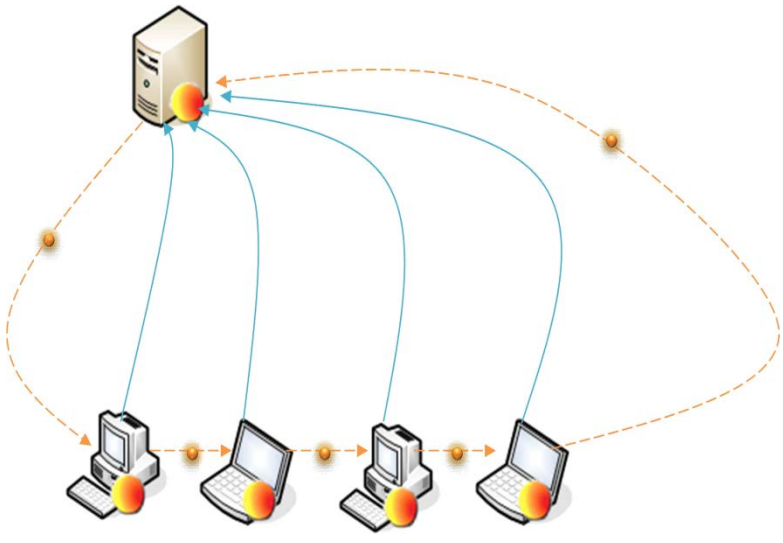


Fig. 4.3. Implementación de políticas por medio de tokens

El periodo de rotación del token (también llamado tiempo de refresco) es configurable por el administrador para optimizar la asignación del ancho de banda para Aranda 360.

Número DE AGENTES POR SERVIDOR	NUMERO DE CONEXIONES SIMULTANEAS	TIEMPO DE REFRESCO DEL TOKEN	RTEIEMPO DE RECONEXIÓN AL SERVIDOR PRINCIPAL (EN SEGUNDOS)
1 a 500	100 a 50	60 a 600	60 a 300
500 a 2000	70 a 20	600 a 1800	300 a 600
2000 a 4000	50 a 10	1800 a 3600	600 tao 1200
+ 4000	30 a 10	3600 a 7200	600 a 1200

El número máximo de agentes es: 5000.

Estos detalles son basados en nuestras observaciones con diferentes configuraciones.

Con menor frecuencia el token es enviado, la menor parte de las conexiones del agente. Esto implica que la distribución de carga a través de la red y la tasa de ocupación de los servidores disminuirán de manera significativa.

Por otra parte, el refresco del log y el intervalo de tiempo de implementación de políticas son significativamente afectadas por un pequeño número de tokens en circulación.

Modo Avanzado

El modo avanzado se maneja de la siguiente forma:

- Propósito.
- Habilitando el modo avanzado.
- Definiendo colecciones de agentes.

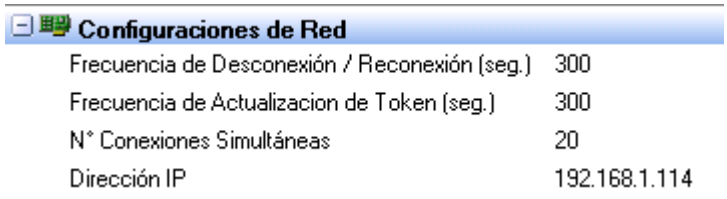
Propósito

El modo avanzado es utilizado para crear colecciones de agentes.

Las colecciones de agentes son grupos que han sido previamente creados por el administrador. Éste puede agregar una o varias colecciones a grupos de agentes.

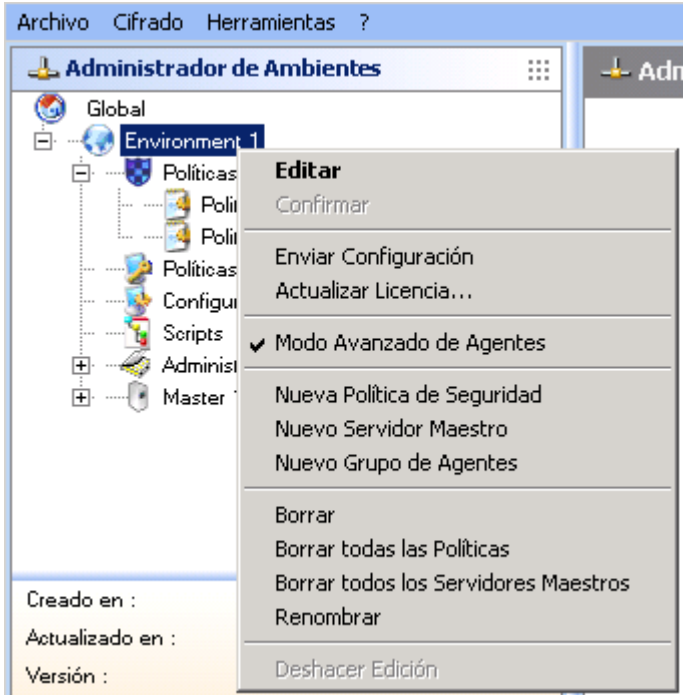
Esto hace más fácil manejar un gran número de agentes.

La colección de agentes debe ser asignado al servidor principal Administrador de Ambientes > [Nombre del Servidor] > Configuración de red.

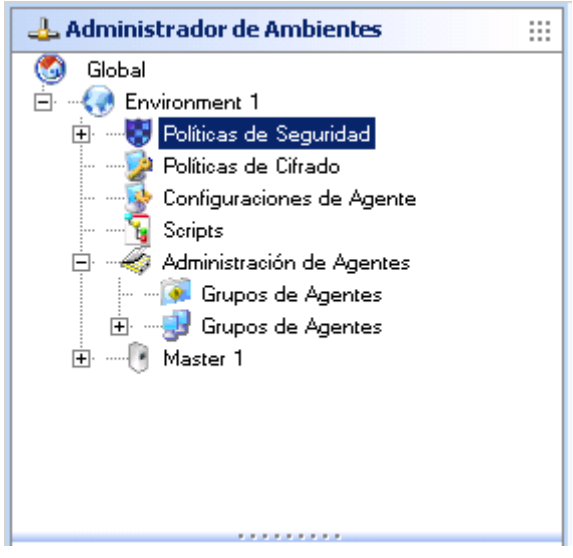


Habilitando el modo avanzado

Para habilitar el modo avanzado, haga clic derecho en el nombre del ambiente y seleccione Modo Avanzado del Agente.



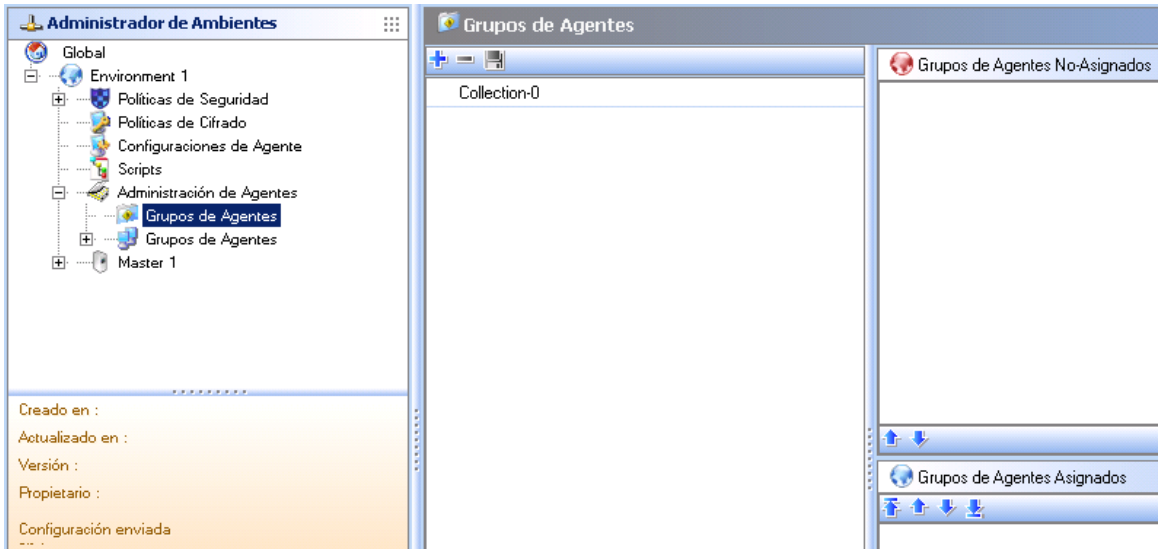
La interfaz gráfica cambia en la sección del agente.



Definiendo colecciones de agentes

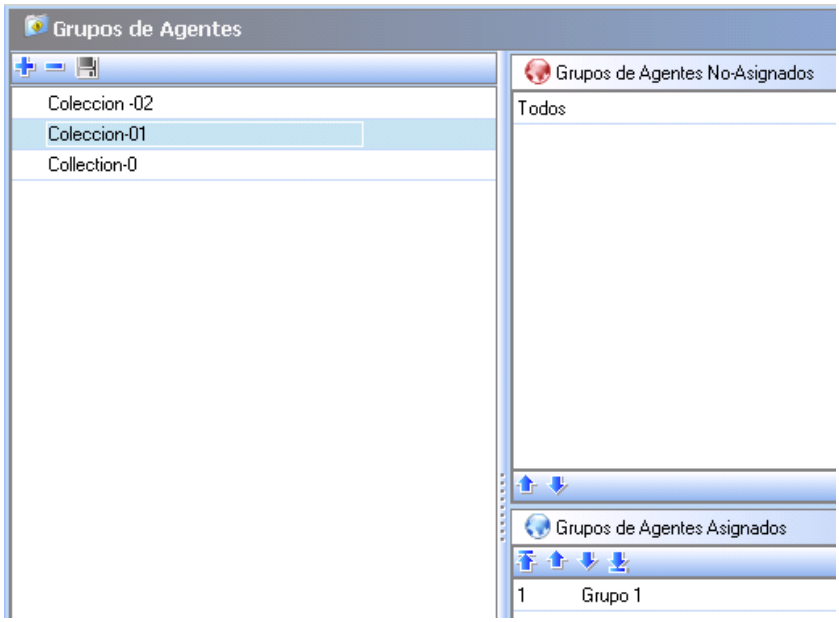
Para crear una colección de agentes, siga los siguientes pasos:

1. Haga clic en .

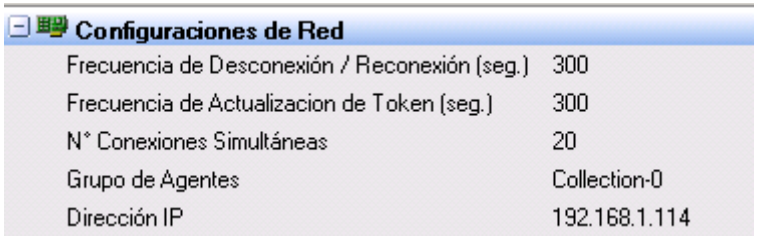


2. Renombre la colección.

3. Mueva los grupos de agentes para la configuración de las colecciones usando las flechas.



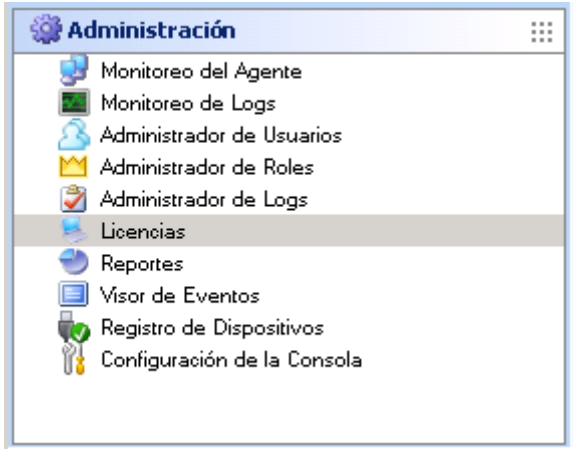
4. Asigne la colección al servidor principal en Administrador de Ambientes > [Nombre del Servidor] > Configuración de Red.



5. Valide el ambiente y los parámetros del servidor principal.
6. Sincronice los agentes.

HERRAMIENTAS DE ADMINISTRACIÓN Y MONITOREO

El panel de herramientas de administración y monitoreo está localizado en la parte inferior de consola de administración:



Este panel es usado para administrar y monitorear los siguientes elementos:

Monitoreo del agente

Ofrece al administrador una perspectiva clara y global del estado del agente para verificar las versiones de las configuraciones y de los agentes.

Monitoreo del log

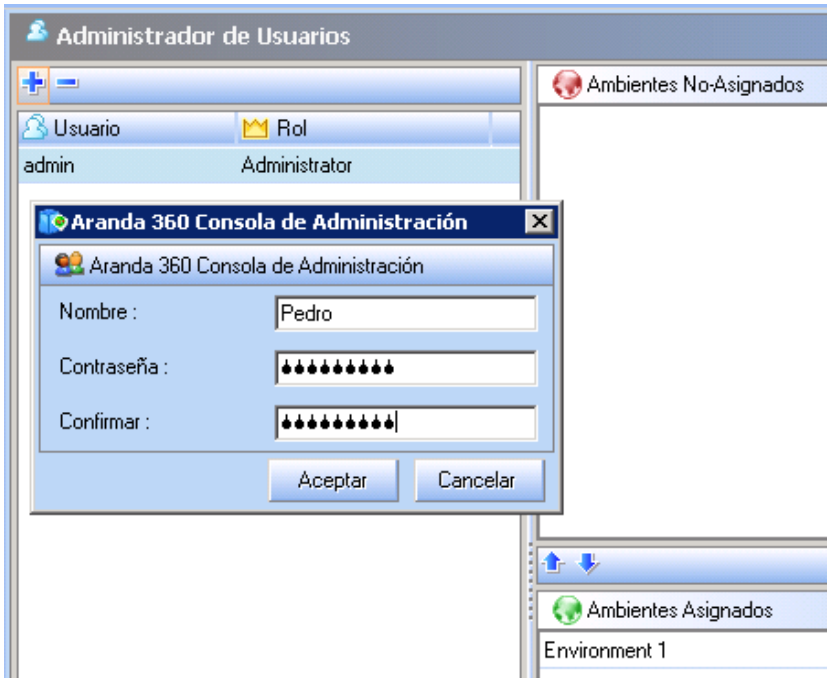
Registra cualquier actividad sospechosa en las estaciones de trabajo y la respectiva reacción del agente.

Administración de usuarios

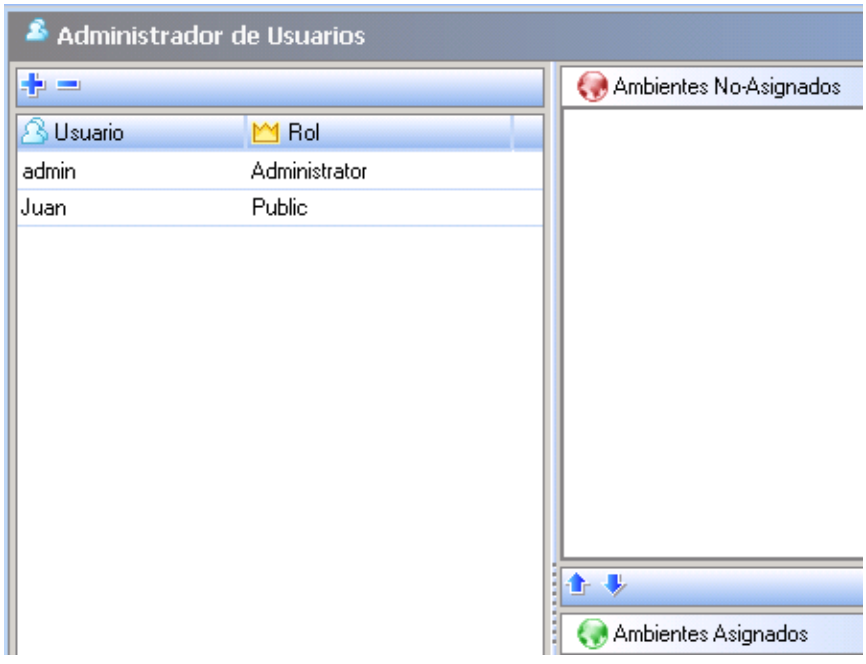
En esta sección se definen los usuarios que pueden acceder a la consola de administración, así como de la asignación de roles.

Para agregar un usuario, siga los siguientes pasos:

1. Haga clic en Administrador de Usuarios.
2. Haga clic en .
3. Diligencie los tres campos que se muestran y valide.



4. Seleccione el rol que se le va asignar al usuario en la respectiva columna.
5. Seleccione el ambiente que se le va asignar al usuario (si es necesario) con la flecha.



6. Verifique las modificaciones.

Administrador de roles

En esta sección se crean los roles asignado a los usuarios de la consola. Esto se realiza a través del Administrador de Usuarios.

Los roles por defecto son los siguientes:

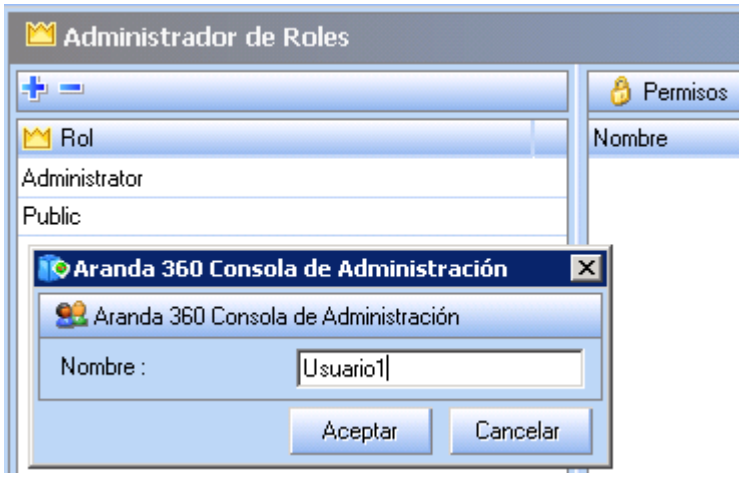
- Administrador:
  Permisos para todas las operaciones de la consola.

- Público:
  Permisos de solo lectura para la configuración de la consola, administrador de ambientes y las herramientas de administración y monitoreo.

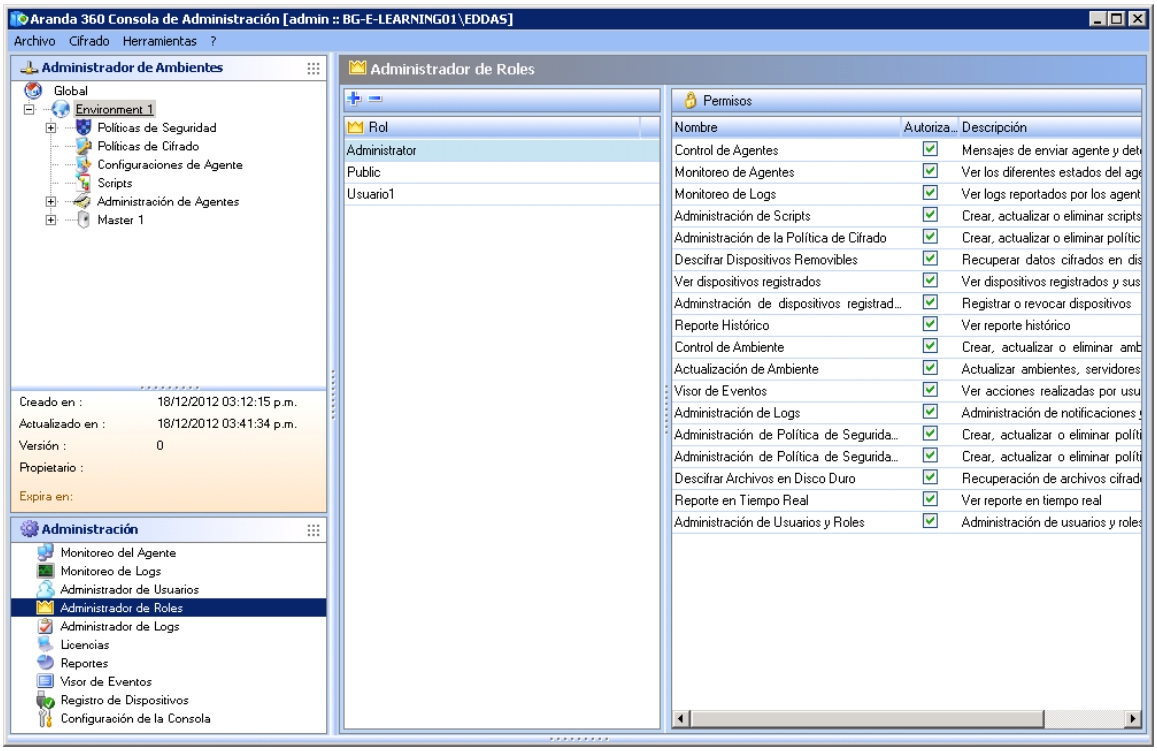
El administrador de roles se utiliza para crear y personalizar roles para la respectiva asignación de usuarios.

Para agregar un rol, siga los siguientes pasos:

1. Haga clic en Administrador de Roles.
2. Haga clic en .
3. Digite el nombre del nuevo rol y valide



4. Haga clic en el rol creado en la respectiva columna y configure las respectivas opciones.



5. Verifique las modificaciones.

Administrador del log

En esta sección se personalizan los mensajes de log y notificaciones del agente.

Es utilizado para seleccionar como los logs serán reportados y almacenados:

- En una base de datos.
- A través de otras aplicaciones.

Los logs son sistemáticamente escritos en un archivo local. La columna de interfaz de usuario es utilizada para habilitar o deshabilitar el monitoreo sobre el agente.

Licencias

Muestra información acerca de:

- Número de agentes implementados (tomando en cuenta el paquete de Aranda 360 que fue instalado).
- El número de licencias que están aún disponibles.

Generador de reportes

Muestra informes en tiempo real e histórico. Son usados para mostrar información acerca de:

- Agentes.
- Servidores.
- Políticas.
- Configuraciones.
- Dispositivos extraíbles.

Visor de Eventos

Muestra las acciones llevadas a cabo por el administrador de la consola.

Acciones como:

- Envío de configuraciones al servidor.
- Renombrando grupos de agentes.
- Actualizando políticas de cifrado.

Configuración de la consola

Para modificar y configurar la consola de administración.

PANEL DE CONFIGURACIÓN DE LA CONSOLA

Para configurar los parámetros de la consola de administración, haga clic en el panel de herramientas de administración y monitoreo.

El panel incluye dos áreas: Opciones y conexiones seguras.

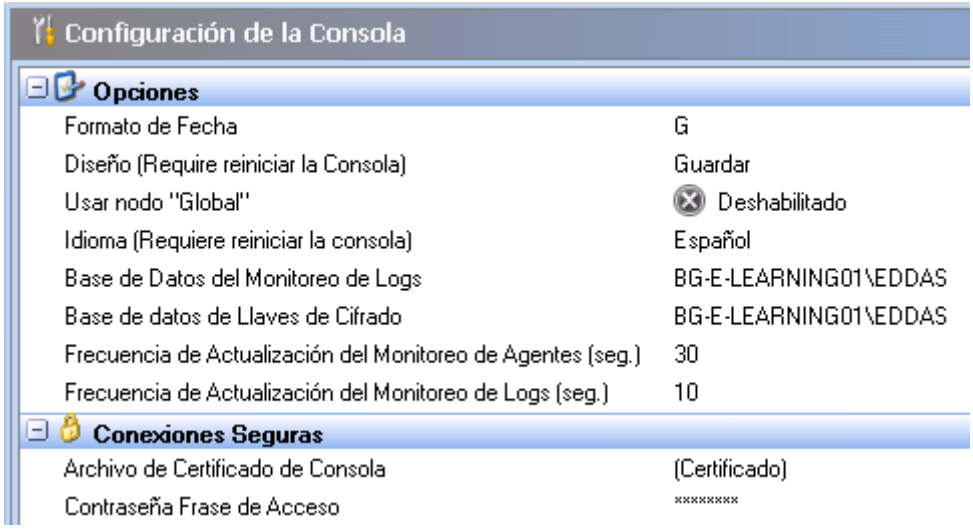


Fig. 4.4: Panel de Configuración

Opciones

En Opciones, el administrador puede modificar:

- Formato de fecha
  Puede cambiar el formato de la fecha para toda la consola. Pueden usarse los siguientes formatos:
  - Dddd/MM/yyyy.
  - dd/MM/yy.
  - dd/MM/yyyy.
- Diseño
  Es posible ajustar el tamaño de las columnas y paneles, guardando las modificaciones

  - Debe reiniciar la consola para que el nuevo diseño sea aplicado

- Idioma
  Puede cambiar el idioma de la consola utilizando uno de los siguientes métodos:
  - Haga doble clic en la columna de la derecha hasta que el idioma requerido aparezca.
  - Haga clic en la columna de la derecha y en el botón . Seleccione el idioma requerido en la lista.
  - Debe reiniciar la máquina para que los cambios tengan efecto.
- Base de datos para monitoreo del log
  Seleccione la instancia de SQL server que quiere utilizar para monitorear los logs.

- Base de datos para cifrado de claves
  Seleccione la instancia de SQL server que quiere utilizar para cifrado de claves.

- Tiempo de refresco del monitor del agente
  Digite el tiempo en segundos que se usará para el monitoreo del log (Intervalo de tiempo entre cada actualización).

- Tiempo de refresco del monitor del log
  Digite el tiempo en segundos que se usará para el monitoreo del agente (Intervalo de tiempo entre cada actualización).

Conexiones Seguras

En esta sección puede modificar:

- La ruta de los certificados para la protección de la comunicación entre la consola y el servidor.
- La contraseña que se configuró al instalar el servidor para prevenir cualquier uso ilegal de los certificados.

Capítulo 5 - CONFIGURACIÓN DEL SERVIDOR ARANDA 360

ACERCA DE ESTE CAPÍTULO

Este capítulo presenta el servidor Aranda 360 server y su editor de configuración.

EDITOR DE CONFIGURACIÓN

El editor de configuración del servidor incluye las siguientes áreas:

- Roles del servidor.
- Configuración de red.
- Configuración del monitor del log.
- Cifrado.
- Actualización del Antivirus.
- Configuración del clúster.
- Configuración de actualizaciones.
- Servicio de autenticación.

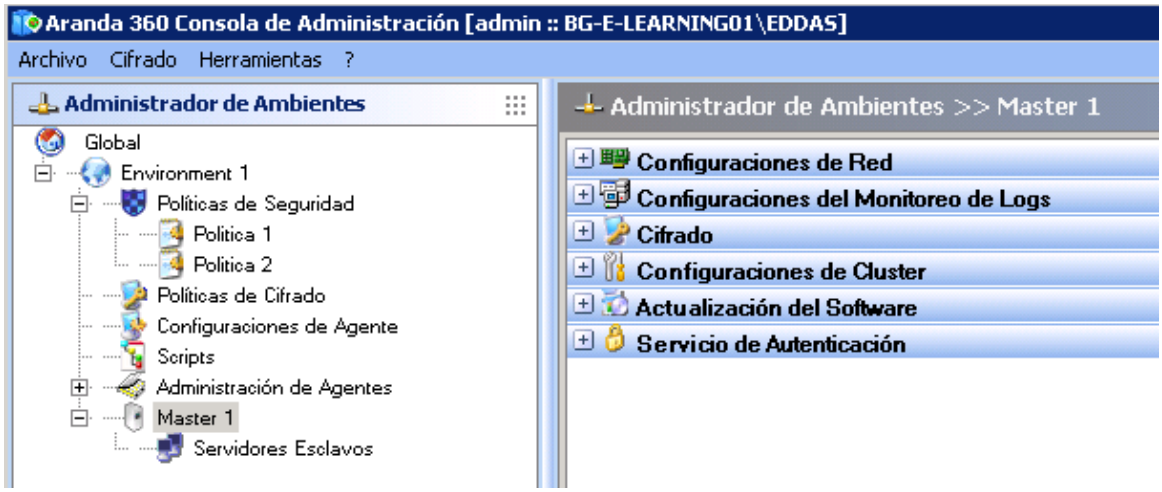


Fig. 5.1: Editor de configuración del servidor

ROLES DEL SERVIDOR

La Interfaz gráfica de esta funcionalidad se muestra a continuación:

- Servidor Aranda 360:
  Esta función se puede habilitar o deshabilitar.

  Si la función es deshabilitada, las siguientes opciones también lo estarán:
  - Cifrado.
  - Configuración del Clúster.
  - Servicio de autenticación.

CONFIGURACIONES DE RED

La Interfaz gráfica de esta funcionalidad se muestra a continuación:

Fig. 5.3: Servidor Principal: Configuración de red

- Tiempo de reconexión (ser):
  Este es el intervalo de tiempo de cada intento de reconexión con el servidor, realizada por los agentes.
- Tiempo de refresco del Token (seg.):
  Este es el intervalo de tiempo entre cada transmisión del token realizada por el servidor a los agentes.
- Número de conexiones simultaneas:
  Este es el número de agentes que pueden conectarse simultáneamente al servidor.
- Dirección IP:
  Esta es la dirección IP del servidor.

CONFIGURACIÓN DEL MONITOR DEL LOG

La interfaz gráfica de la configuración del monitor del log es la siguiente:

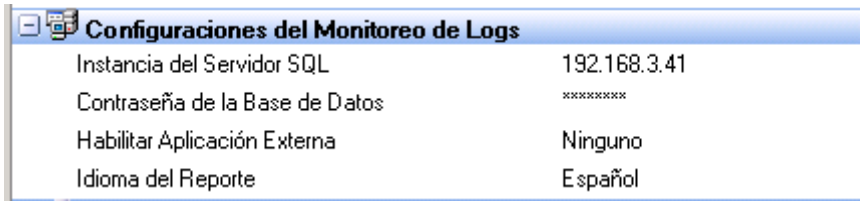
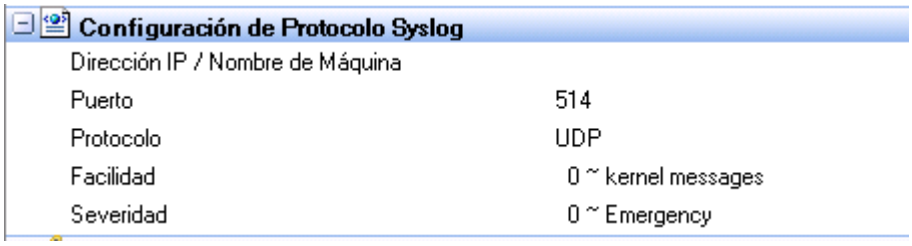
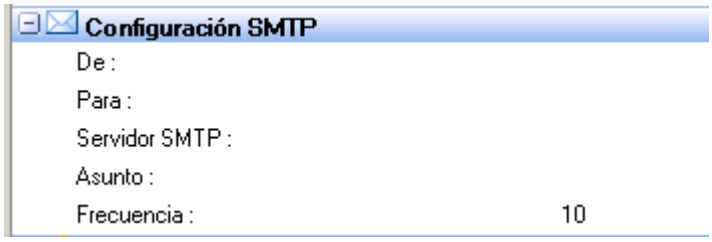


Fig. 5.4. Servidor principal: Configuración del monitor del log

- Instancia de SQL server:
  Digite la dirección IP de la instancia del servidor utilizado para la base de datos del log.
- Contraseña de la base de datos:
  Esta es la contraseña usada para la cuenta de la base de datos del log. Ésta fue definida al instalar la base de datos Aranda.
- Aplicación externa para generar reportes:
  Y puede seleccionar una aplicación para generar logs:
  - Ninguna.
    Si escoge Ninguna, el editor de configuración del servidor principal no será modificado.
  - Syslog.
    Si escoge Syslog, el editor de configuración del servidor principal mostrará la siguiente información:



  - SMTP.
    Si escoge SMTP, el editor de configuración del servidor principal mostrará la siguiente información.



  - Idioma del generador de reportes:
    Este es el idioma usado para el generador de reportes del log.

CIFRADO

La interfaz gráfica de la función de cifrado es la siguiente:

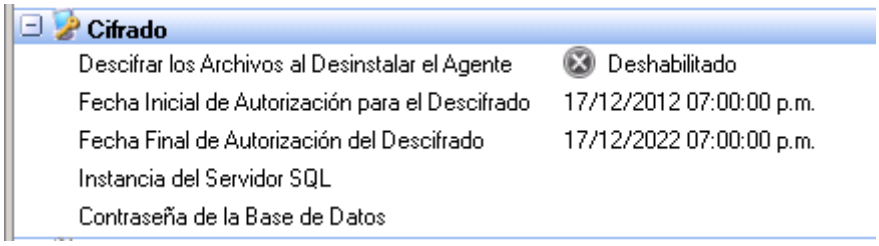


Fig. 5.5: Servidor Principal: Cifrado

- Descifrado los Archivos al desinstalar el agente:
  La información cifrada en la máquina del agente será descifrada al desinstalar Aranda 360.
  Solo los archivos cifrados con una clave pueden ser descifrados automáticamente.

- Fecha inicial de autorización para el descifrado:
  Define la fecha y hora para comenzar la desinstalación de los agentes.

- Fecha Final de autorización del desinstalación:
  Define la fecha y hora para terminar la desinstalación de los agentes.

- Instancia del servidor SQL:
  Digite la dirección IP de la instancia del servidor SQL server utilizado para la base de datos de las claves.

- Contraseña de la base de datos:
  Digite la contraseña para la base de datos de las claves.

CONFIGURACIÓN DEL CLUSTER

La interfaz gráfica para la configuración del clúster es la siguiente:

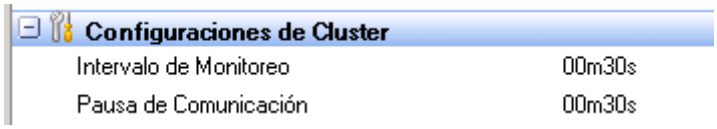


Fig. 5.7: Servidor principal: Configuración del clúster

- Intervalo de monitoreo:
  El servidor principal comienza comunicándose con los servidores secundarios y realiza verificaciones.
- Pausa de comunicación:
  Es el tiempo de espera (30 segundos) en el que un servidor secundario se considera no disponible.

CONFIGURACIÓN DE ACTUALIZACIONES

La interfaz gráfica para la configuración de las actualizaciones es la siguiente:

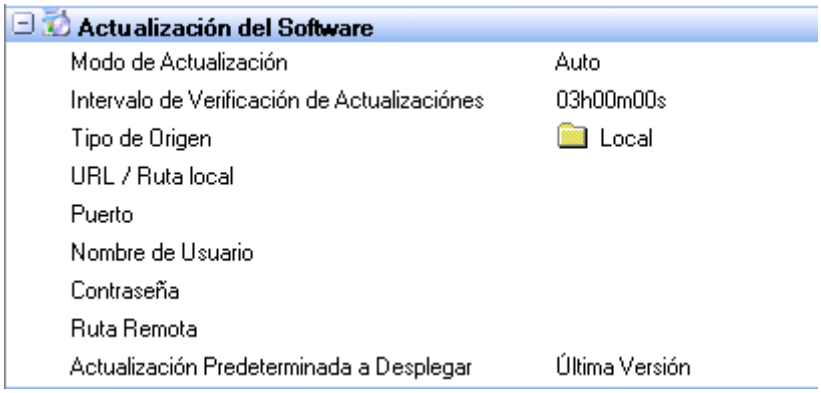


Fig. 5.8. Servidor principal: Configuración de actualizaciones

- Modo Actualización:
  - Auto.
  - Manual.
  - Próximo Reinicio.
- Verificación de intervalo de actualización.
- Fuente:
  - Local.
  - FTP.
  - HTTP.
- Ruta URL/Local.
- Puerto.
- Nombre de usuario.

- Contraseña.
- Ruta remota.

SERVICIO DE AUTENTICACIÓN

La interfaz gráfica el servicio de autenticación es la siguiente:

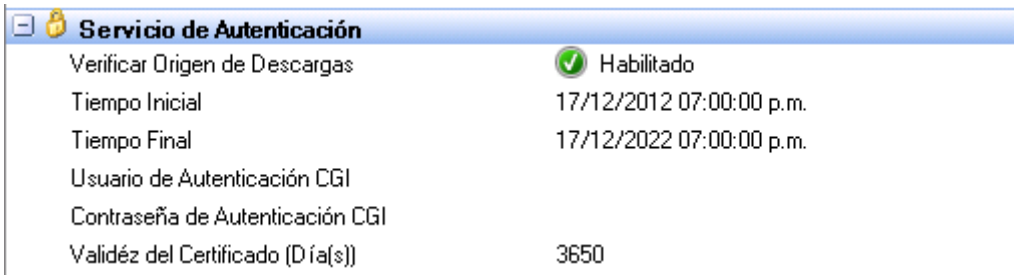


Fig. 5.9: Servidor principal: Servicio de Autenticación

- Verificar origen de descargas:
  Cuando se habilita esta opción, solo los agentes distribuidos en el servidor serán autorizados para conectarse en este ambiente.
  Cuando se deshabilita esta opción, cualquier agente puede conectarse al servidor.
- Tiempo Inicial:
  Es la fecha para iniciar la distribución del certificado.
- Tiempo Final:
  Es la fecha para finalizar la distribución del certificado.
- Usuario de autenticación CGI:
  Este es el nombre de usuario de la cuenta para descargar un certificado del agente desde la siguiente dirección http://[server IP]/ssl/cgi.
- Contraseña de autenticación CGI:
  Este es la contraseña de usuario de la cuenta para descargar un certificado del agente desde la siguiente dirección http://[server IP]/ssl/cgi.
- Validez del certificado (día(s)):
  Puede modificar el periodo de validez de los certificados de los agentes (por defecto 10 años).

Capítulo 6 - CONFIGURACIÓN DEL AGENTE

ACERCA DE ESTE CAPÍTULO

Este capítulo presenta la configuración del agente a través del editor de configuración, esto incluye:

- Configuración del puerto.
- Editor de configuración:
    - Configuración del agente.
        - Notificación (ventana emergente).
        - Modo de protección del agente.
        - Interfaz de usuario.
        - Detener Agente.
        - Habilitar logs.
    - Acceso web temporal.
        - Configuración desde la consola.
        - Configuración desde el agente.
        - Enviando información de interface de red.
    - Aprendizaje.

- Aplicando una configuración a un grupo de agentes.

CONFIGURACIÓN DEL PUERTO DEL AGENTE

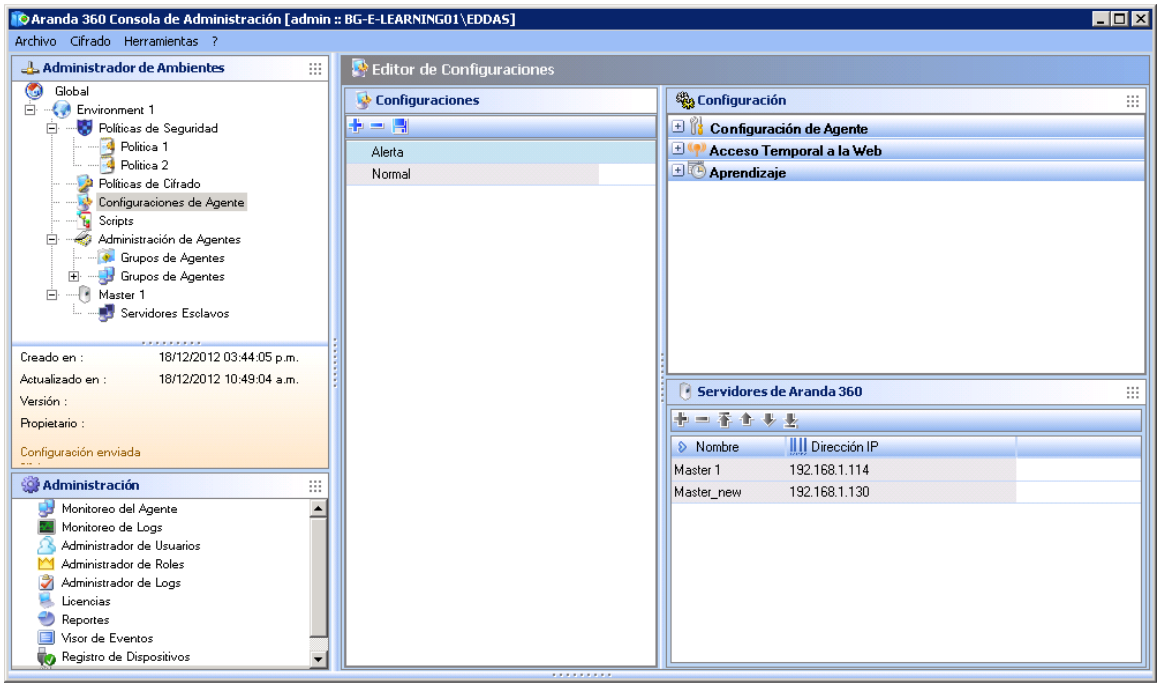
Los puertos TCP 16005 y 16006 son reservados para el agente.

Al probar la comunicación agente/servidor, el agente bloqueara cualquier comunicación que utilice esos puertos (ejemplo: telnet).

EDITOR DE CONFIGURACIÓN

El editor de configuración incluye cuatro áreas:

1. Configuración del agente.
2. Acceso Web temporal.
3. Aprendizaje.



AGENT CONFIGURATION

La interfaz gráfica de la configuración del agente es la siguiente:

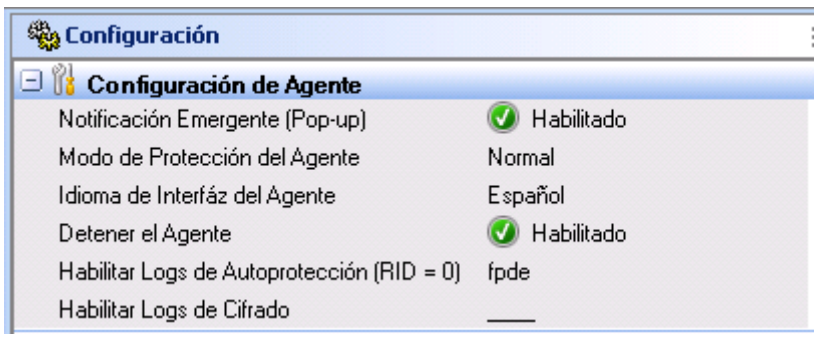


Fig. 6.1. Configuración del Agente

Notificación (ventana emergente)

Esta opción habilita/deshabilita la ventanas emergentes mostradas sobre el agente.

Modos de protección del agente

La interfaz gráfica de modos de protección del agente es la siguiente:

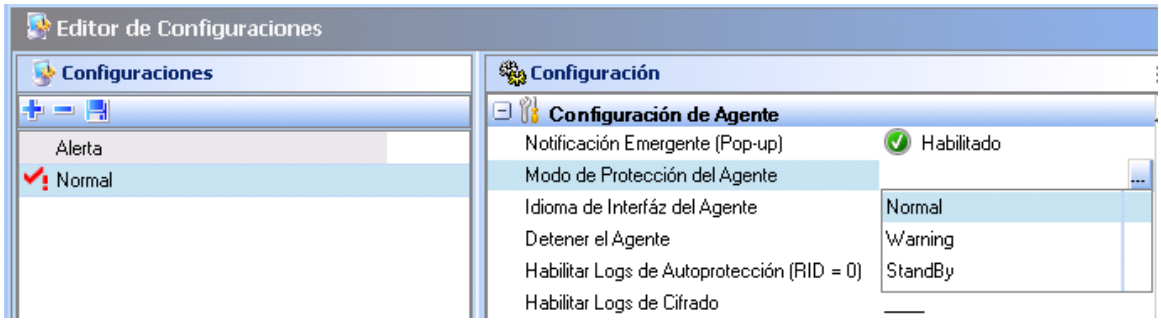


Fig. 6.2: Configuración del agente: Modos de protección

Existen tres modos de protección:

- Normal:
  El agente aplica las políticas.
  Este modo bloquea y registra.
- Advertencia:
  El agente no aplica las políticas, sino que proporciona una advertencia en donde se muestra que se está bloqueando.
  Esta opción es utilizada para verificar las acciones de la política y modificarla después en caso de ser necesario. Esta opción puede ser usada para simulación.
  Este modo no bloquea pero registra.
- Modo de Espera:
  El agente no aplica políticas y guarda registros de advertencia.
  Esto actúa como un modo "detenido" que puede ser usado cuando no se desee aplicar una política específica (ejemplo: durante la instalación del servidor).
  Este modo no bloquea, y tampoco registra.

Interfaz de Usuario

Esta opción es utilizada para seleccionar el idioma de la interfaz de usuario del agente.

Deteniendo el agente

La opción detener el agente se maneja en cinco etapas:

1. Configuración de consola.
2. Si la opción detener el agente está habilitada.
3. Si la opción detener el agente está habilitada.
   - Procedimiento del usuario.
   - Procedimiento del Administrador.
4. Si el usuario quiere desinstalar el agente.
5. Si el usuario quiere detener una acción temporal en progreso.

Configuración de consola

En el editor de configuración, el administrador puede habilitar o deshabilitar la opción de detener el agente.

- Si esta opción está habilitada, un usuario con privilegios de administrador puede detener el agente ejecutando stopagent.exe.

  - Después que el agente está instalado y antes de descargar los certificados, la opción de detener el agente está habilitada por defecto.

- Si esta opción está deshabilitada, el usuario puede solicitarle al administrador detener temporalmente el agente.
  El usuario y el administrador utilizarán el procedimiento de impugnación.

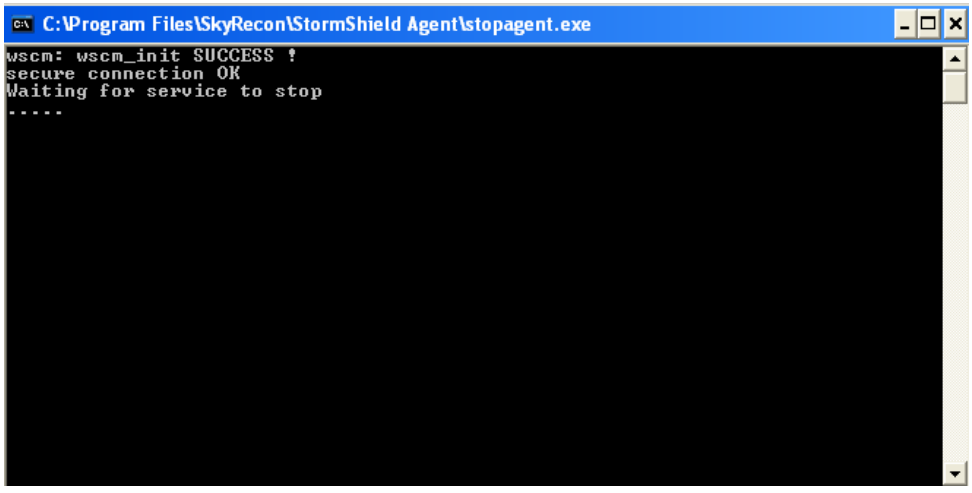
Detener el agente es un proceso que debe ser usado cuidadosamente, ya que esto hace vulnerable la estación de trabajo de ataques de virus o capturadores de teclado (keylogging), el cual es el proceso de capturar eventos para robar contraseñas e información confidencial

Sin embargo, este procedimiento es útil en un ambiente de pruebas.

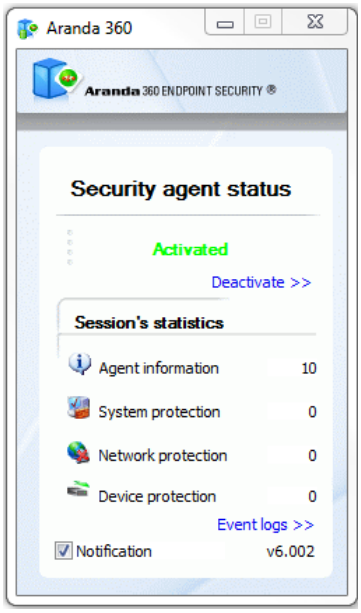
Si la opción Detener el Agente está habilitada

Para detener el agente, siga los siguientes pasos:

1. Vaya al directorio:
   [Archivos de Programa]\Aranda\Aranda 360 Agent
2. Haga doble clic en el archivo stopagent.exe.
3. Espere hasta que la ventana se cierre:



4. Haga clic derecho en el icono y seleccione estado para verificar que el agente efectivamente fue detenido.



5. Para habilitar de nuevo el agente, haga clic en Activar en la ventana de estado.
   Si la opción Detener el Agente está deshabilitada

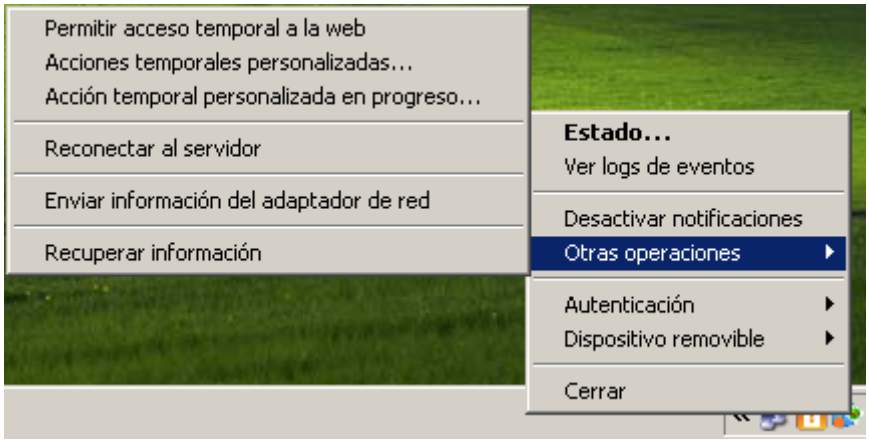
Si la opción Detener el Agente está deshabilitada

Para detener el agente, el usuario debe solicitarle al administrador desactivar el agente temporalmente

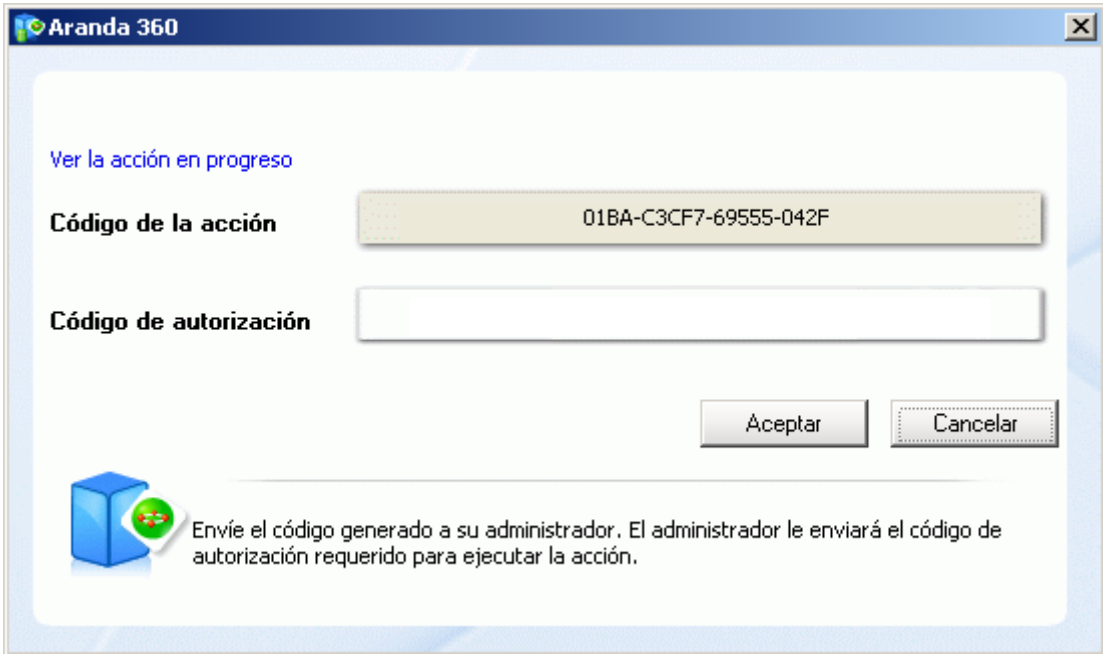
Procedimiento del Usuario

El usuario debe seguir los siguientes pasos:

1. Haga clic en el ícono y seleccione Otras operaciones > acciones personalizadas temporales.

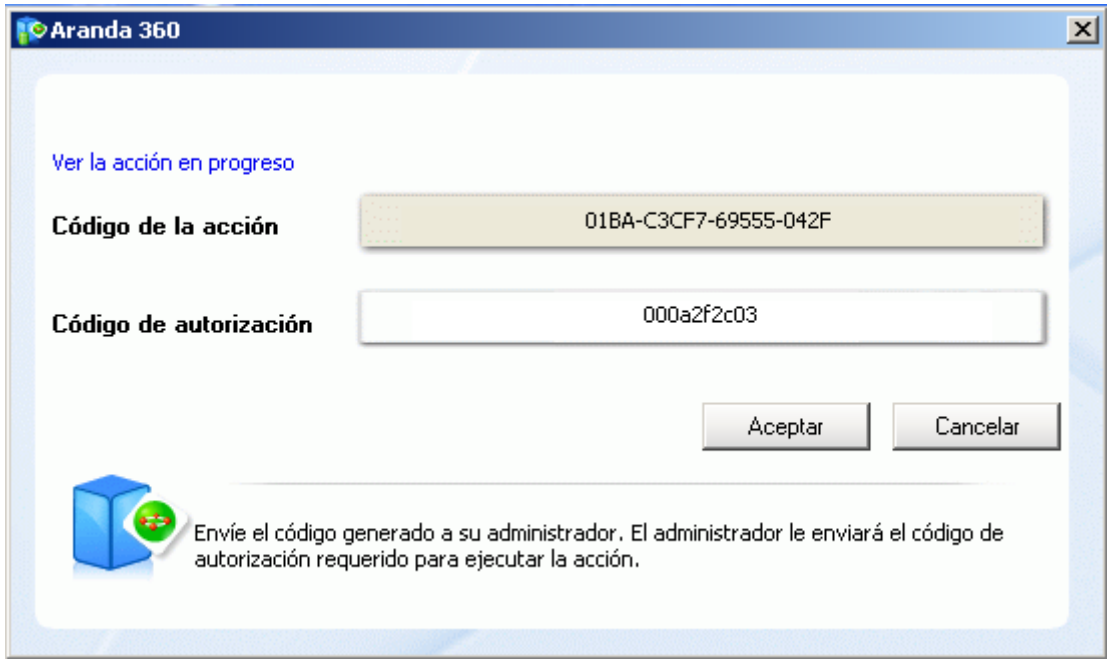


2. Envíe el código de acción, el cual es visualizado por el administrador.



El administrador enviará el código de autorización, el cual es visualizado en la consola.

3. En el campo de autorización, digite el código dado por el administrador.

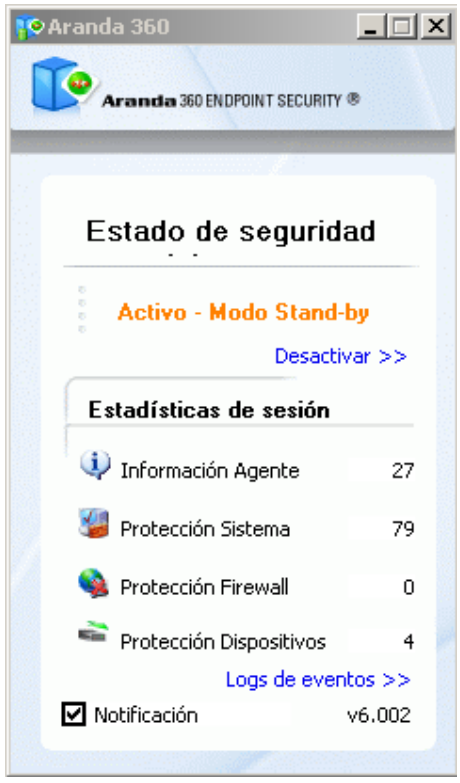


4. Haga clic en OK.

   El agente será deshabilitado temporalmente por el tiempo configurado por el administrador.

   - Si la acción seleccionada es Deshabilitar Protecciones, debe esperar al menos 30 segundos antes de que la protección del agente sea detenida. En otros casos, la acción tendrá efecto inmediatamente.

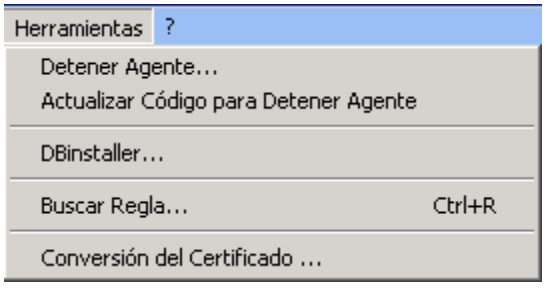
5. Haga clic derecho sobre el icono y seleccione Estado para verificar que el agente efectivamente fue detenido.



Procedimiento del Administrador

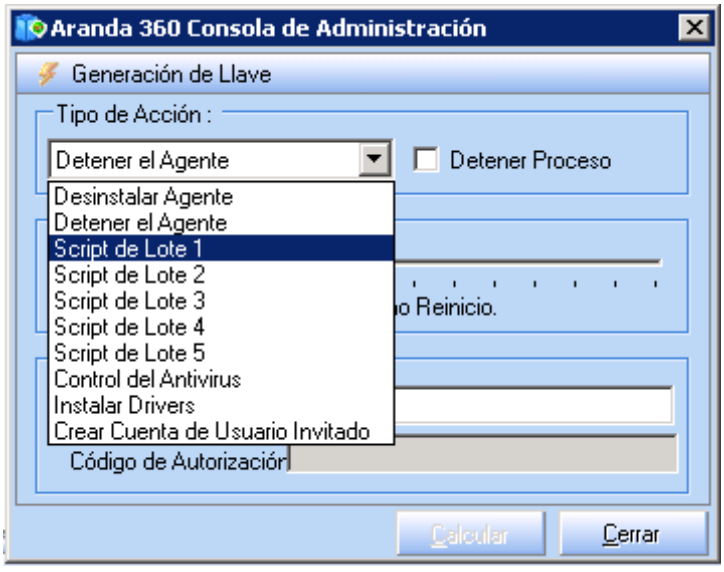
Para responder a una solicitud de un usuario que quiere desactivar temporalmente el agente, se debe seguir los siguientes pasos:

1. En la consola de administración, seleccione Herramientas > Administrar Impugnaciones.

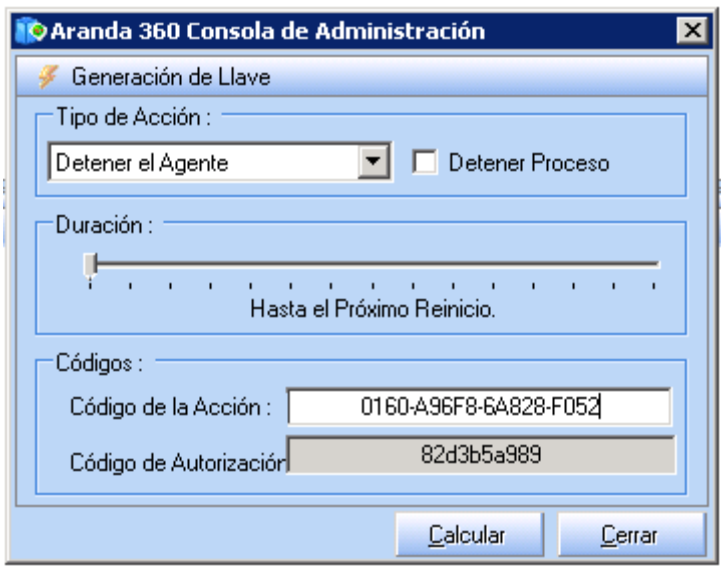


2. Defina los siguientes parámetros:

- En la sección Tipo de Acción utilice para mostrar la lista de acciones temporales.
  Si marca la opción Detener Completamente, el agente se detendrá y no será posible cambiar al modo Activado – Modo Espera.
  Por lo tanto, no se enviarán logs, ni se aplicarán políticas.
- Deslice el cursor sobre la línea de tiempo para configurar la duración de la acción temporal.
- Digite el código de acción enviado por el usuario.

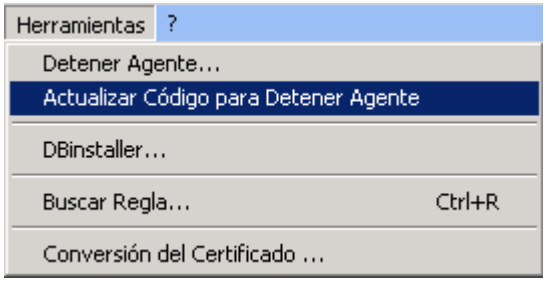


3. Haga clic en Calcular para obtener el código de autorización.



4. Envíe el código al usuario.

- Si el administrador quiere renovar la clave de impugnación, haga clic en: **Herramientas > Renovar clave de impugnación.** Se recomienda renovar la clave cada quince días si se están usando impugnaciones regularmente.



Si el usuario desea desinstalar el agente

En caso de que un usuario con privilegios de administrador y la opción de detener el agente esté habilitado, puede desinstalar el agente ejecutando el archivo Srend.exe.

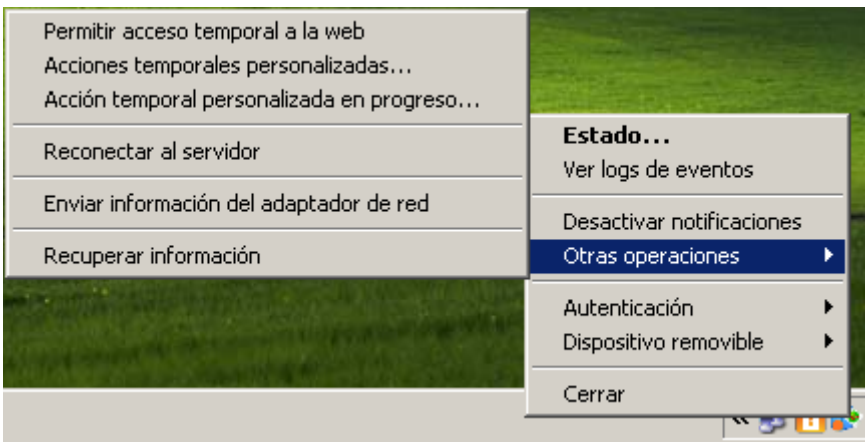
Para desinstalar el agente, el usuario debe seguir los siguientes pasos:

1. Vaya a [Archivos de Programa]\Aranda\Aranda 360Agent.
2. Haga doble clic en el archivo Srend.exe.
3. Reinicie la máquina para completar el procedimiento de desinstalación.

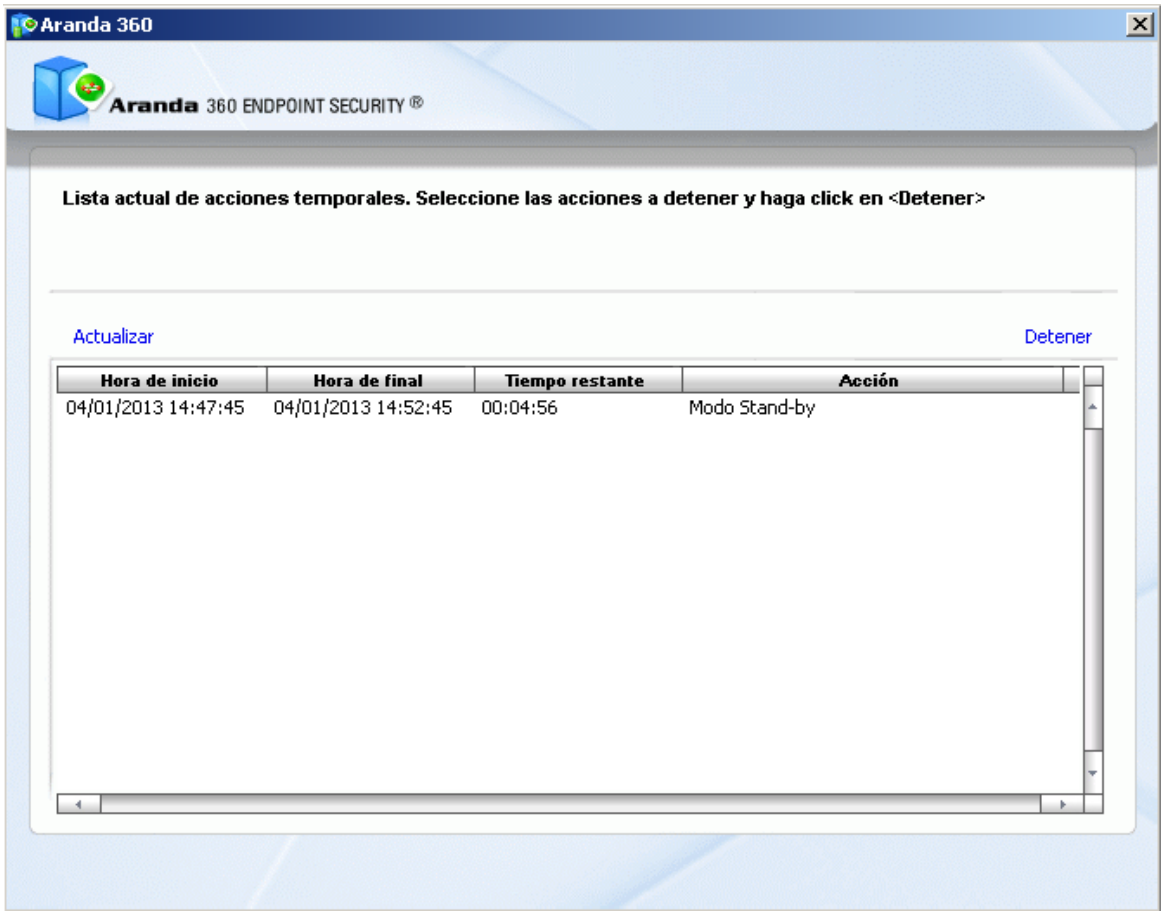
Si el usuario desea detener temporalmente una acción en progreso

Para detener una acción temporal que está en progreso, el usuario debe seguir los siguientes pasos:

1. Haga clic derecho sobre el icono y seleccione Otras operaciones > Acción personalizada en progreso.



2. La lista de acciones temporales que están en progreso serán visualizadas. Haga clic sobre la acción para ser interrumpida.



3. Haga clic en Detener.

Habilitando logs

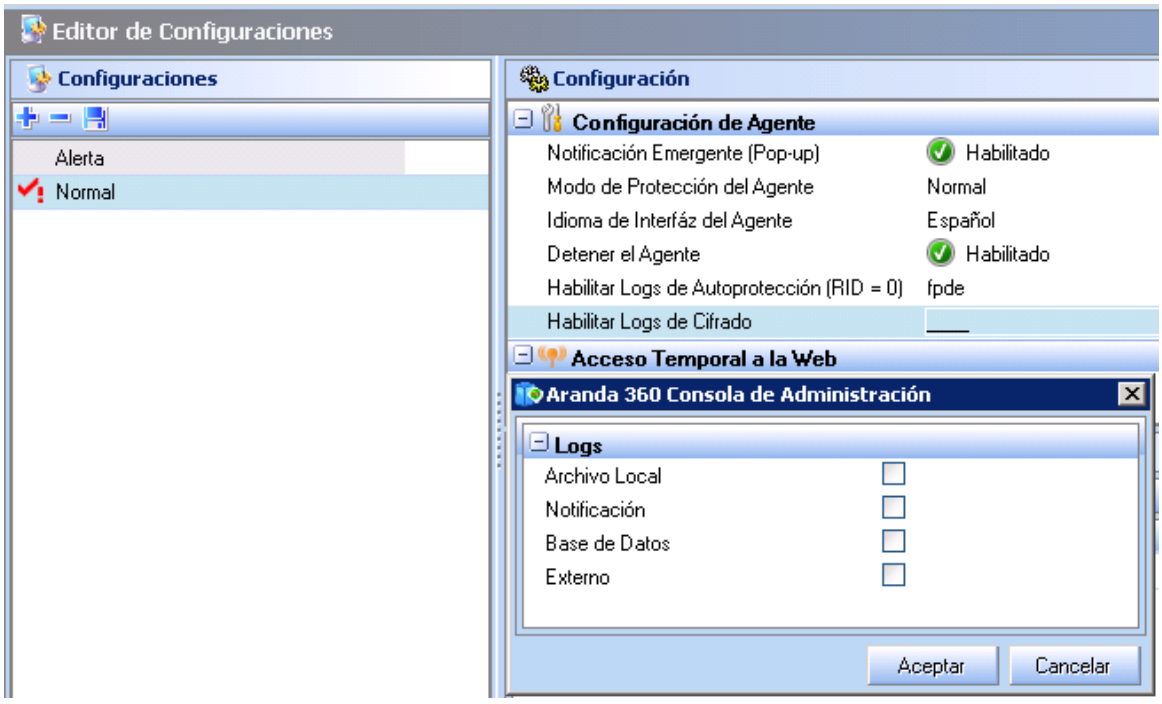
Generalidades

Existen dos tipos de opciones para habilitar logs en el editor de configuración:

- Habilitar logs de autoprotección:
  Cubre los logs generados con RID=0.

- Habilitar logs de cifrado:
  Cubre todos los logs de errores de cifrado.

Ambas opciones permiten decidir cuales logs son visualizados y (Panel de herramientas de administración y monitoreo).



Cada opción contiene los siguientes parámetros para guardar y consultar:

- Interfaz de usuario:
  Logs son mostrados en la interfaz de usuario.

- Ventana emergente:
  Logs son mostrados en una ventana emergente.

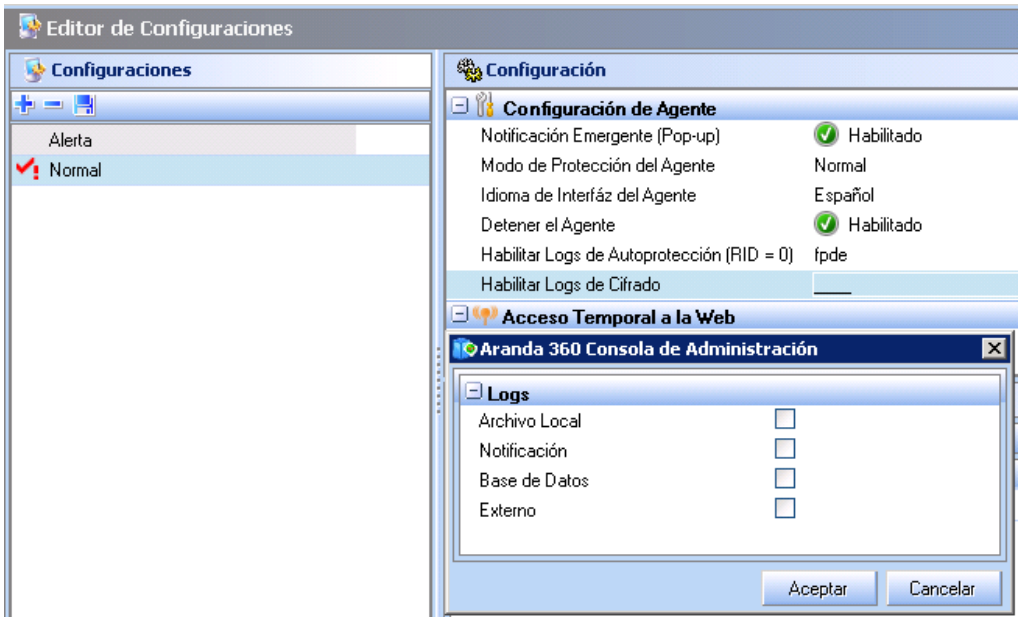
- Base de Datos:
  Logs son enviados a la base de datos.
- Aplicación externa:
  Logs son enviados a un sistema externo (ejemplo: syslog o servidor SMTP).

La configuración por defecto es [vacía].

Configuración de logs de autoprotección y cifrado del sistema

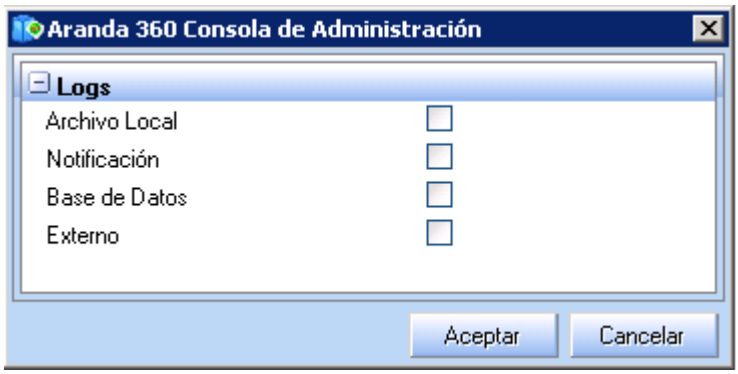
Para aplicar configuraciones a los logs, el administrador debe seguir los siguientes pasos:

1. En el panel de Configuración del Agente, haga clic en la segunda columna sobre las opciones de Habilitar Logs de Autoprotección o Habilitar logs de Autoprotección.



Se abrirá una ventana emergente con las opciones de:

- Interfaz de usuario (F/f).
- Ventana Emergente (P/p).
- Base de Datos (D/d).
- Aplicación Externa (E/e).



2. Seleccione las opciones para ser habilitadas o deshabilitadas.
3. Haga clic en OK.

Estado del log

Los ajustes aplicados por el administrador para los estados del log pueden ser consultados y modificados en el Editor de Políticas de Seguridad (columna Log) y en el administrador del log.

Dependiendo de los ajustes en Configuraciones > Configuración del agente, los estados del log serán visibles en el Editor de Políticas de seguridad y en el Administrador del log.

Existen tres estados del log disponibles:

- Habilitado:
  La casilla de verificación aparecerá marcada
  En cada campo del log, éstos serán mostrados en mayúsculas (ejemplos: F, P, D, E).
  Éstos son visibles en el Administrador del Log.

- Deshabilitado:
  La casilla de verificación aparecerá marcada de color rojo.
  En cada campo del log, éstos serán mostrados en minúsculas en caso de estar deshabilitados (por ejemplo: f, p, d, e).
  Éstos no son visibles en el Administrador del Log.

- Vacío:

  Si la casilla de verificación está vacía, el administrador puede seleccionar un log para ser mostrado en el Administrador del log.
  En cada campo del log, una línea subrayada es mostrada
  (por ejemplo: _pde).
  Si el log está vacío, el comportamiento será definido en el Administrador del log.

ACCESO TEMPORAL WEB

Cuando el acceso a Wi-Fi es denegado, Permite al agente establecer conexiones HTTP o HTTPS.

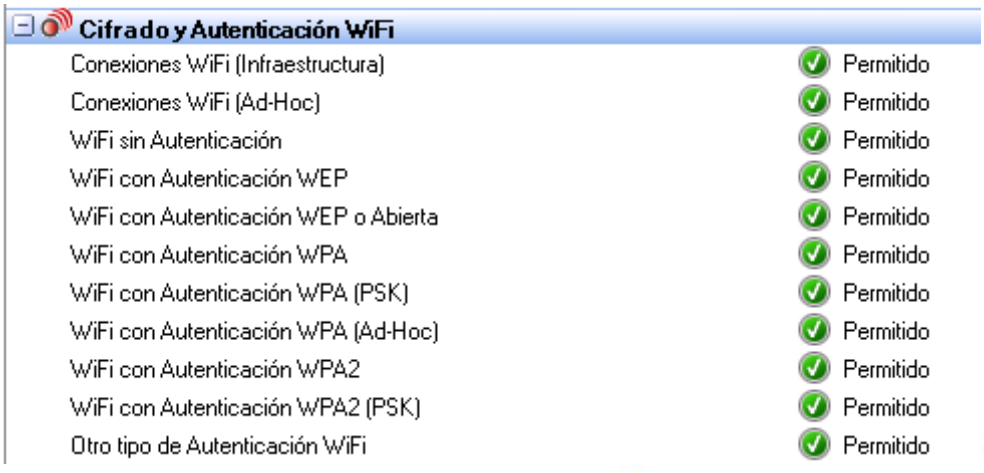
Puede configurar los puertos para ello.

Ejemplo: Un usuario puede trabajar fuera de la organización utilizando un punto de acceso Wi-Fi para conectarse a un servidor VPN SSL de la empresa.

Configuración desde la consola

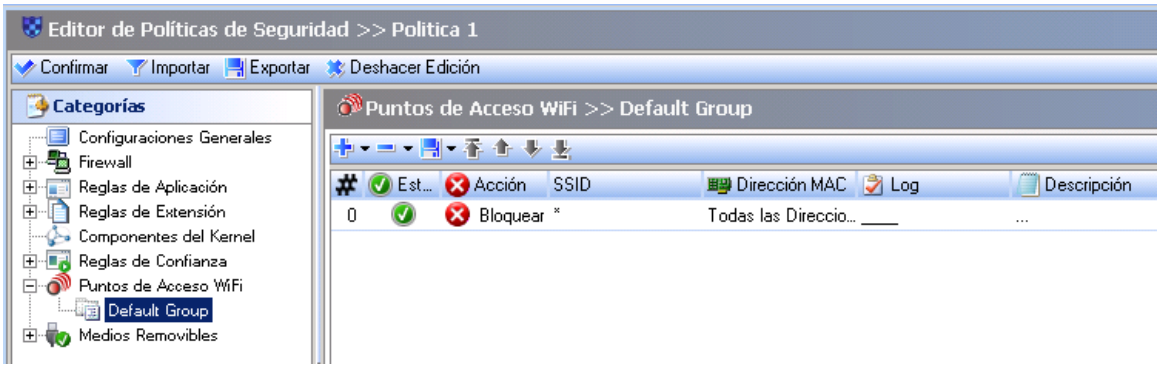
Para denegar acceso a Wi-Fi y permitir el uso de punto de acceso, el administrador debe configurar las políticas de seguridad:

1. En Editor de Políticas de Seguridad, vaya a Categorías > Configuración General > Cifrado y Autenticación Wi-Fi.
2. Configure las conexiones Wi-Fi y Wi-Fi adhoc que serán permitidas.



3. Bajo Puntos de acceso Wi-Fi, bloquee el acceso creando una regla.
   Para ello siga los siguientes pasos:

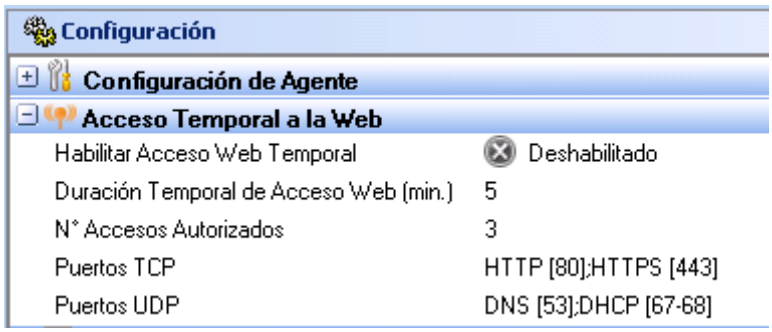
- Edité las políticas de seguridad.
- Agregue una regla haciendo clic en el botón con el signo más.
- Digite los siguientes parámetros:
  - SSID : *.
  - Acción: Bloquear



El administrador puede incluir una lista blanca de puntos de acceso permitidos. Cabe señalar, que las reglas para los puntos de acceso Wi-Fi reglas deben ser configurados de la siguiente manera:

- Reglas con el parámetro Acción en Aceptar son listadas primero.
- Una regla final (Acción con el valor Bloqueado and SSID con *) está en la parte final de la lista.

4. En el editor de configuración, vaya a Acceso Temporal y habilite la opción Acceso Temporal.



5. Establezca la duración en minutos del acceso.

   Por defecto, la duración es de 5 minutos, lo cual es un tiempo suficiente para que el usuario realice la conexión. El tiempo máximo de duración es de 30 minutos.

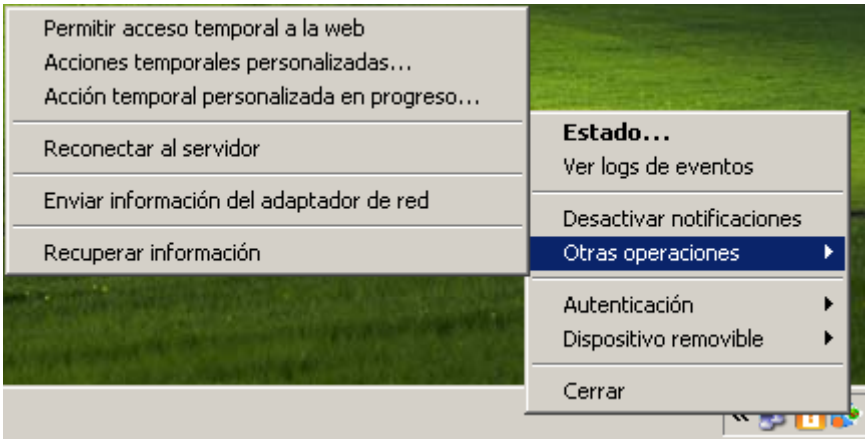
6. Digite el número de acceso autorizado.
   Por defecto, con valor 3.

7. Si es necesario, cambie o agregue puertos TCP Y UDP en los respectivos campos.
   Si se incluye un comentario, se debe incluir el número del puerto entre corchetes (ejemplo: HTTP [80]).

Configuración desde el agente

Para configurar el Acceso temporal Web desde el agente, se deben seguir los siguientes pasos:

1. Haga clic derecho sobre el ícono .
2. Seleccione Otras operaciones y clic en Conceder Acceso Temporal Web.



3. Cuando se le solicite, haga clic en Sí.

   Ahora puede acceder al navegador Web por la cantidad de tiempo especificada por el Administrador.
   El tiempo de duración es normalmente suficiente para registrase en el punto de acceso o conectarse al servidor VPN SSL de la organización.

4. Se abrirá una ventana indicando que el acceso Web temporal ha expirado.

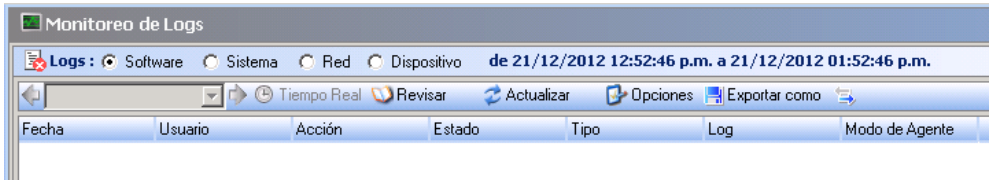
Enviando información de Interfaz de Red

Para recuperar el identificador de la interfaz de red del agente para un uso posterior siga los siguientes pasos:

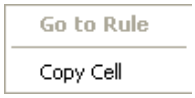
1. Tome un agente que pertenezca a la red para enviar información de interfaz al log del servidor:

- Haga clic derecho sobre el ícono
- Seleccione Otras operaciones > Enviar Información de Interfaz de Red.

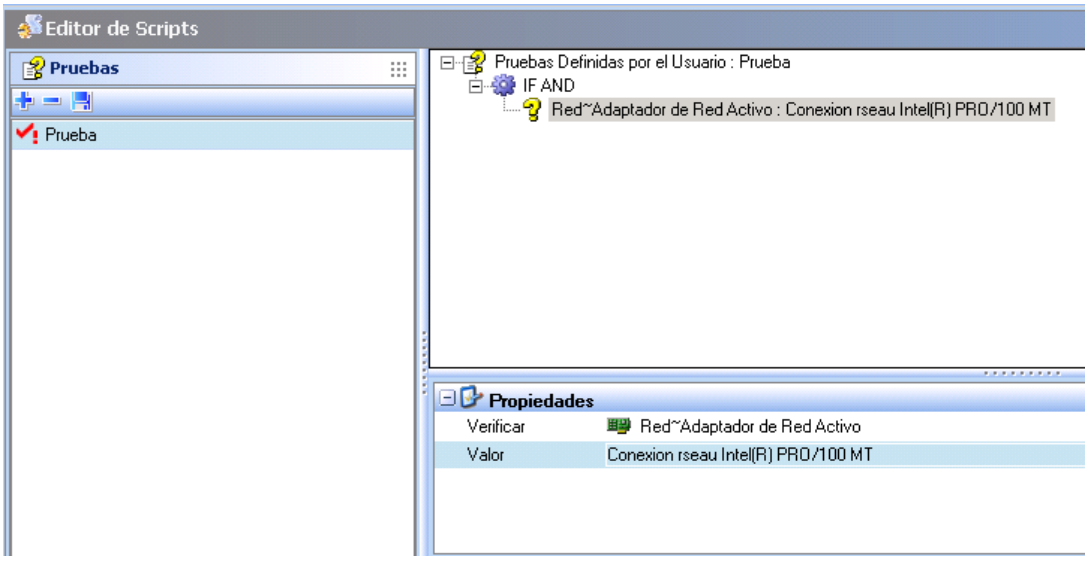
2. Sobre la consola de administración, seleccione Monitor de Log.
3. Haga clic en la opción Software.
4. Busque la entrada del log para el ID de la interfaz de red.
   La entrada mostrará la siguiente información:
   - Fecha.
   - Nombre de Usuario: Administrador.
   - Acción: INFO.
   - Estado: NET-INT.
   - Tipo: Agente.
   - Mod. Nombre: MODENFORCEMENT.
   - Log: ID de la Interfaz de Red.
   - Modo Agente.



5. Haga clic derecho en Entrada de Log



6. Copie el ID de la interfaz de red.
7. Copie el ID en el campo valor en el panel Propiedades de Interfaz de Red.



APRENDIZAJE

La interfaz gráfica de la función Aprendizaje es la siguiente:

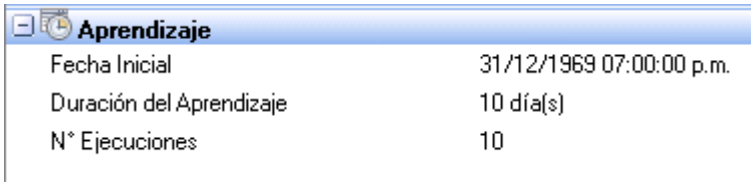


Fig. 6.3. Configuración: Aprendizaje

La función Aprendizaje tiene las siguientes opciones:

1. Fecha Inicio.
   Para establecer el periodo inicial de Aprendizaje.
   Haga clic en ... . Para establecer la fecha al periodo actual.

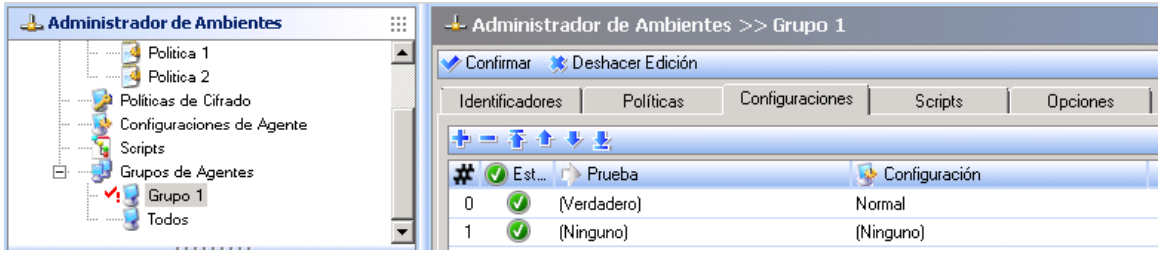
2. Duración del Aprendizaje.
   Para definir el tiempo de aprendizaje en días, haga clic sobre el campo y digite el valor.
3. Número de ejecuciones.
   Para definir el número de ejecuciones por proceso para crear una aplicación basada en perfiles, haga clic sobre el campo y digite el valor

APLICANDO UNA CONFIGURACIÓN A UN GRUPO DE AGENTES

Las configuraciones son asignadas a grupos de agentes.

Para realizar esta asignación, siga los siguientes pasos:

1. Haga clic en Grupos de Agentes en el Administrador de Ambientes.
2. Haga clic sobre la etiqueta Configuraciones para visualizar la configuración aplicada al grupo.



3. Para modificar la configuración, Haga clic en la columna Configuración y en el botón ...

Aparecerá una lista de las configuraciones disponibles.

4. Seleccione la configuración que se le aplicará al grupo.
5. Verifique los cambios.
6. Envíe la nueva configuración a los grupos de agentes.

Capítulo 7- PROTECCIÓN DEL SISTEMA

ACERCA DE ESTE CAPÍTULO

Este capítulo describe los mecanismos de protección que ofrece Aranda 360:

- Mecanismo de protección:
  - Protección basada en perfiles.
  - Protección automática.
  - Protección basada en reglas.
  - Orden utilizado para aplicar los mecanismos de protección.
  - Interfaz Gráfica.
- Protección basada en perfiles:
  - Principios.
  - Asignación automática de nivel de confianza.
  - Correlación y ponderación.
  - Aprendizaje.
  - Protección basada en perfiles.

- Protección automática:
  - Principios.
  - Accediendo a os parámetros de protección automática
  - Configuración de protección automática:
    - Control de comportamiento del sistema.
    - Control de comportamiento de procesos.
    - Control de dispositivos.
    - Cifrado y autenticación Wi-Fi.
    - Control de actividad de red.

- Protección basada en reglas:
  - Listas blancas y negras.
  - Combinando listas blancas y negras.

MECANISMOS DE PROTECCIÓN

Para una protección óptima, Aranda 360 utiliza varios métodos de protección que funcionan de una manera coherente y complementaria.

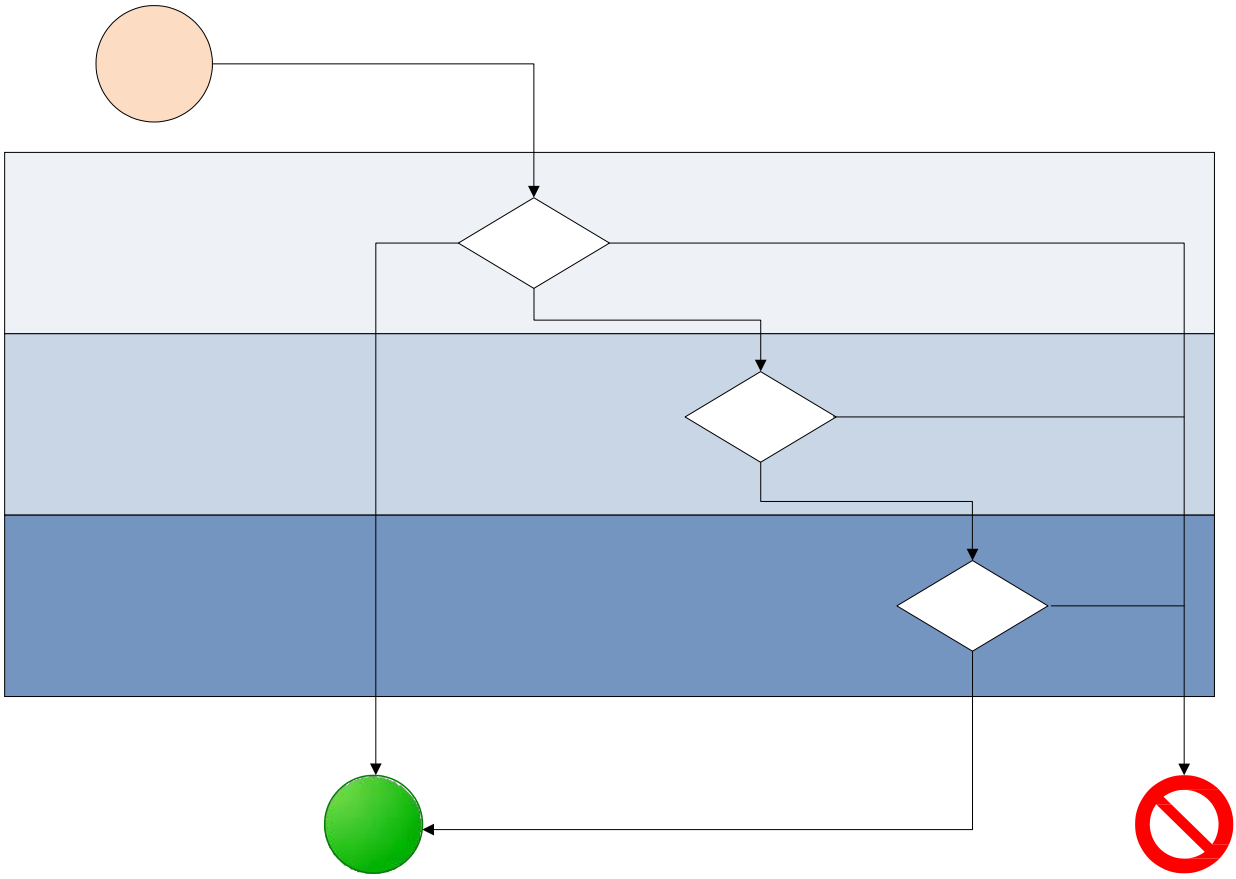


Fig. 7.1. Aranda 360 y sus tres mecanismos de protección.

PROTECCIÓN BASADA EN PERFILES

Protección basada en perfiles:

- Monitorear las aplicaciones que se están ejecutando.
- Alertar y bloquear cualquier proceso cuyo comportamiento difiera del perfil configurado.

PROTECCIÓN AUTOMÁTICA

La Protección automática cubre actividades del sistema y de red en las estaciones de trabajo. No requieren ninguna configuración por parte del administrador. Cabe señalar que el administrador puede deshabilitar estas protecciones parcial o totalmente.

PROTECCIÓN BASADA EN REGLAS

Protección basada en reglas es usada para definir y aplicar políticas específicas de usuario en la organización. El encargado de aplicar éstas políticas es el Administrador para dar o denegar permisos sobre los recursos de las máquinas.

ORDEN UTILIZADO PARA APLICAR LOS MECANISMO DE PROTECCIÓN

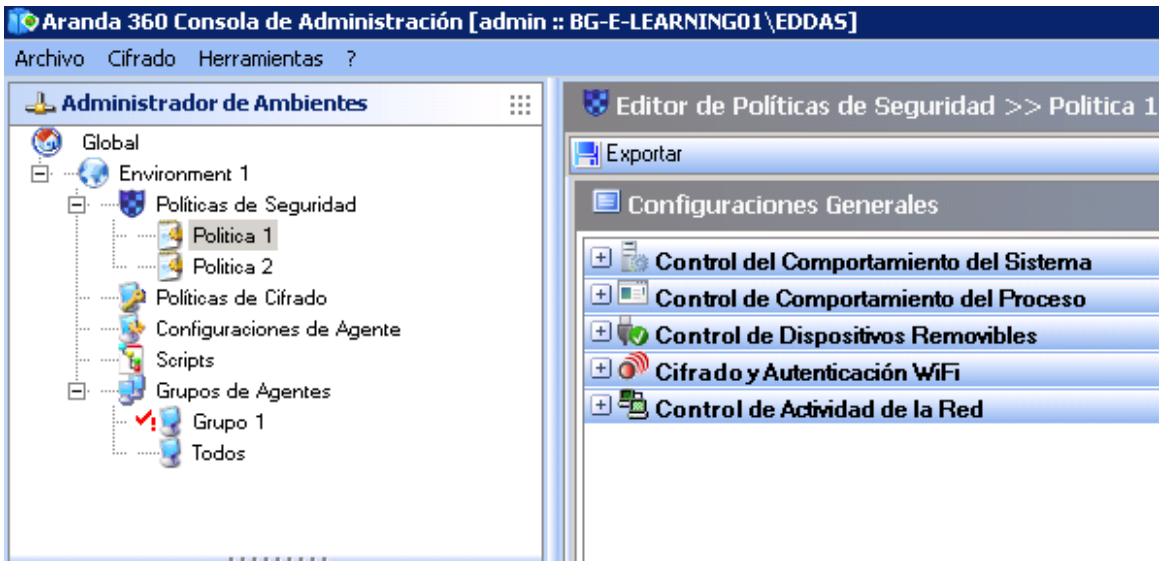
Los tres mecanismos de protección son aplicados en un orden específico:

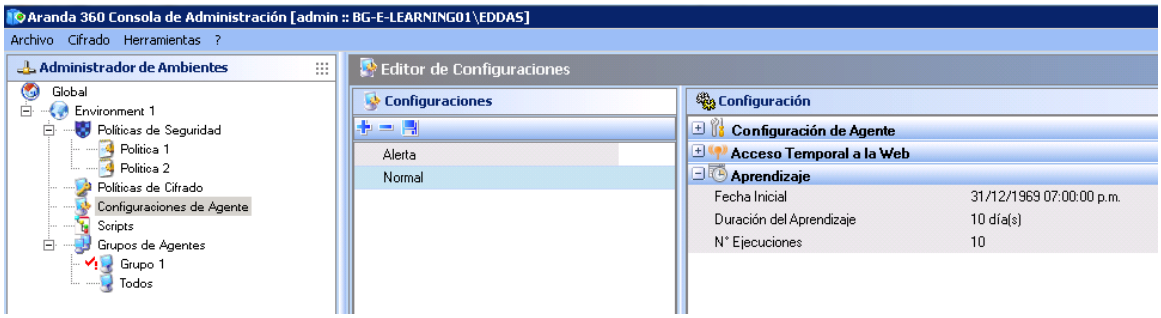
1. Protección basada en reglas.
2. protección automática.
3. Protección basada en perfiles.

Este orden de precedencia da prioridad a las políticas explícitamente definidas por el administrador (Protección basada en reglas). En consecuencia, cualquier rechazo o autorización expresada por el administrador siempre será aplicada. El Control humano siempre tendrá prioridad sobre el automático.

INTERFAZ GRÁFICA

La Protección de Aranda 360 es visualizada en la consola de administración:





PROTECCIÓN BASADA EN PERFILES

PRINCIPIOS

Protección basada en perfiles realiza un análisis del comportamiento de la aplicación comparándolo con un perfil de referencia. Éste análisis está basado en monitorear las llamadas realizadas por la aplicación al sistema.

Aquí están unos ejemplos:

- Abriendo puertos.
- Accediendo a la memoria compartida.
- Cargando librerías.
- Leyendo claves del registro,
- Etc.

Durante el periodo de aprendizaje, estas llamadas son memorizadas para crear un perfil estándar. Después de esta fase, las acciones ejecutadas por las aplicaciones son comparadas con dicho perfil para detector cualquier anomalía.

Aprendizaje es automáticamente reiniciado después de:

- Cualquier modificación autorizada por una aplicación.
- Cambiando el periodo de aprendizaje (fecha seleccionada en el futuro).

ASIGNACIÓN AUTOMÁTICA DE NIVEL DE CONFIANZA

Cuando un proceso es iniciado, un nivel de confianza es automáticamente asignado. Este nivel cambia con el tiempo, dependiendo de las diferencias observadas entre el perfil estándar y la actividad real.

CORRELACIÓN Y PONDERACIÓN

Una simple diferencia entre el perfil estándar y la actividad real de una aplicación no es suficiente para clasificar un código como malicioso. Por esta razón la protección basada en perfiles también recurren al mecanismo de correlación y ponderación.

Correlación es utilizada para comparar algunas desviaciones (pertenecientes a diferentes categorías) de manera que pueda cambiarse el nivel de confianza. Por ejemplo, inyectando un proceso desconocido correlacionado con la apertura de un nuevo puerto, indicará un alto riesgo de ataque.

La ponderación es utilizada para tener en cuenta el nivel definido por el administrador en los parámetros de la protección automática. Como resultado, un nivel crítico en combinado con inyecciones de procesos, bloquearán cualquier aplicación que intente ejecutar esta operación (a excepción de aplicaciones de confianza en esta categoría), independientemente del nivel de confianza asignado al proceso.

APRENDIZAJE

La consola de administración es usada para lanzar el proceso de aprendizaje utilizando parámetros que pueden accederse desde el editor de configuración.

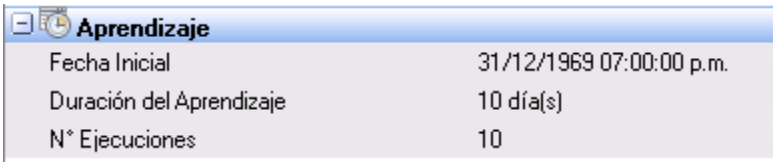


Fig. 7.2. Parámetros de aprendizaje

La fecha indica cuando el proceso de aprendizaje iniciará en todas las estaciones de trabajo asignadas al servidor.

La duración y/o número de ejecuciones de cada proceso son utilizadas para establecer los parámetros de la fase de aprendizaje. Si la duración de esta fase es completada pero el número de ejecuciones es inferior al definido por el administrador. El proceso de aprendizaje continúa.

PARÁMETROS DE LA PROTECCIÓN BASADA EN PERFILES

Los parámetros generales para la protección del sistema que se presentan en el Control de Comportamiento de Procesos son también utilizados para la protección basada en perfiles.

Estos parámetros pueden accederse en el panel de Configuración General de cada política de seguridad:

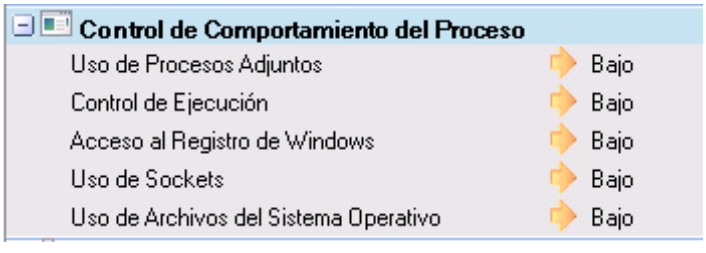


Fig. 7.3: protección basada en perfiles: Control de Comportamiento de Procesos

PROTECCIÓN AUTOMÁTICA

PRINCIPIOS

Protección automática en Aranda 360:

- Detección de anomalías.
- Bloqueo de anomalías.
- No requiere configuración por parte del administrador.

Sin embargo, el administrador puede ajustar las respuestas a diferente tipo de eventos. Dependiendo de la configuración del administrador, Aranda 360:

- Ignora los eventos.
- Genera una alerta.
- Bloquea una acción en progreso.

ACCEDIENDO A LOS PARÁMETROS DE PROTECCIÓN AUTOMÁTICA

Los parámetros de protección automática se encuentran en el panel de Configuración General en el Editor de Políticas de Seguridad:

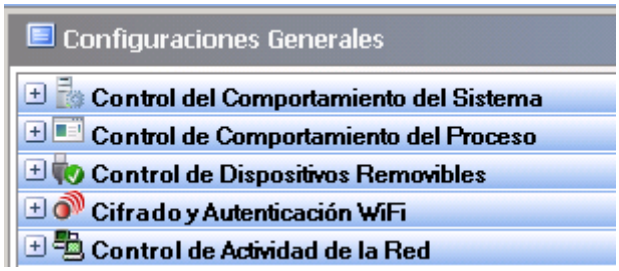


Fig. 7.4. Configuración General: Protección automática

CONFIGURACIÓN DE PROTECCIÓN AUTOMÁTICAS

Aranda 360 realiza un monitoreo de las actividades de las aplicaciones y del sistema. La información recopilada es utilizada para proteger las estaciones de trabajo de:

- Intentos de corrupción de archivos ejecutables.
- Intentos de acceso a ciertos servicios o información sensible.

Dependiendo del tipo de anomalía detectada y el nivel de respuesta definido por el administrador, Aranda 360 puede reaccionar en tiempo real para proteger el sistema.

La Protección consiste en rechazar llamadas maliciosas al sistema, mientras la aplicación sigue ejecutándose.

La protección automática puede ser ajustada por cada política de seguridad. El administrador puede:

- Activar o desactivar la protección.
- Establecer el nivel de protección.

Estos parámetros pueden ser encontrados en Configuración General:

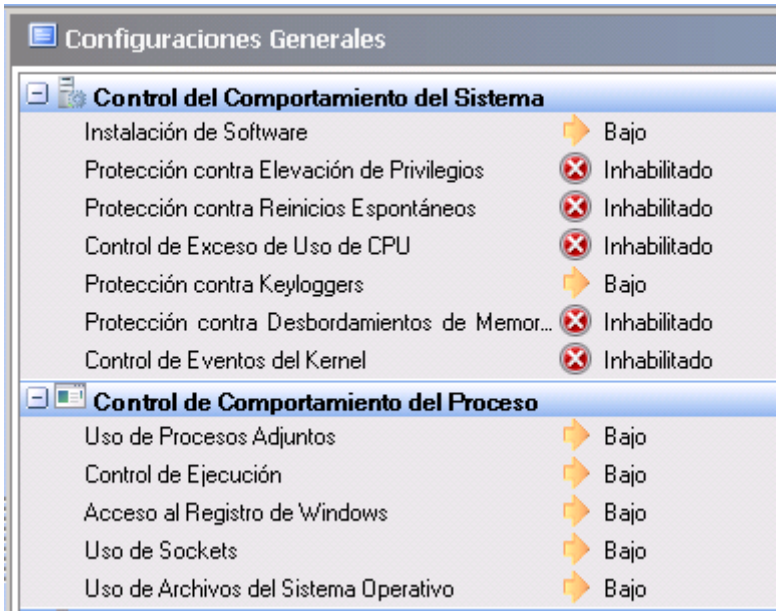


Fig. 7.5. Ejemplo parcial de parámetros de protección automática

Control de comportamiento de proceso

Los parámetros del control de comportamiento del sistema pueden ser configurados para:

- Habilitado/Deshabilitado.
- Alto/Bajo/Crítico/Avanzado.

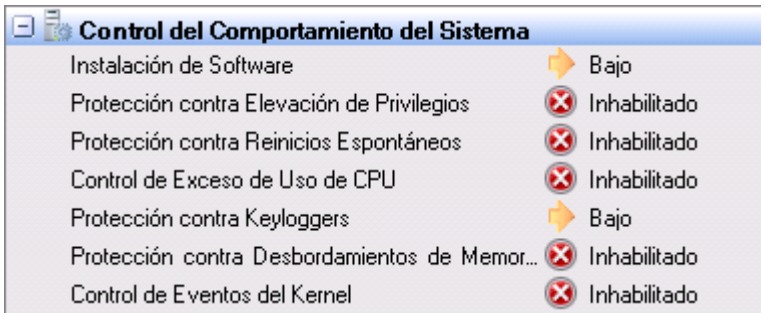


Fig. 7.6. Configuración General: Control de comportamiento del sistema

- Creación de archivos ejecutables:
  Una posible configuración puede ser la siguiente:
  - Bajo:
    Por defecto, Este parámetro es establecido a bajo. En realidad está deshabilitado.
  - Alto:
    Previene la creación de los siguientes archivos ejecutables:

com	dll	exe	msi	mst	scr

  - Critico:

    Previene la creación de los siguientes archivos ejecutables:

bat	com	exe	mst	scr	vbs
cmd	dll	inf	pif	sys	ws
chm	drv	msi	reg	vbe	wsm

    Puede utilizar las listas blancas y negras para permitir o no la instalación de aplicaciones específicas.

- Protección en contra de escalamiento de privilegios: Los posibles valores son Habilitado o Deshabilitado.
  Cuando se habilita, previene que las aplicaciones eleven los permisos de administrador o del sistema.
  Los privilegios solicitados por las aplicaciones son guardados en el log del sistema.

- Protección en contra de reinicios espontáneos: Los posibles valores son Habilitado o Deshabilitado.
  Sucede cuando un usuario quiere iniciar el sistema pero algún código malicioso puede lanzar reinicios espontáneos para:
  - Provoca una denegación de servicios.
  - No permitir la descarga de parches.
  - No permitir la descarga de firmas del antivirus.
- Este parámetro previene o permite que las aplicaciones tengan privilegios que permitan reiniciar la máquina.
  Los privilegios requeridos por las aplicaciones son guardadas en el log del sistema.

- Protección contra sobrecarga de CPU:
  Los posibles valores son Habilitado o Deshabilitado.
  Algunos ataques tienden a utilizar todos los recursos de la CPU con el fin de:
  - Provoca una denegación de servicios.
  - No permitir la descarga de parches.
  - No permitir la descarga de firmas del antivirus.

  Este parámetro previene o permite que las aplicaciones realicen un uso intensivo de los recursos de la de la CPU. Estas aplicaciones son detenidas por Aranda 360.

- Protección contra capturadores de teclado (keyloggers):
  El cuál es el proceso de capturar eventos para robar contraseñas e información confidencial, etc.
  Posibles configuraciones:
  - Baja:
    No bloquea, ni registra.

  - Alta:
    Capturador de teclado (Keylogging) es bloqueado.

  - Critico:
    Recomendado para cuelgue de interfaz gráfica (cualquier evento relacionado con la interfaz gráfica es capturado).

- Protección contra desbordamiento de memoria:
  El desbordamiento de memoria ocurre cuando algún programa intenta escribir en memoria más allá de la asignada. Estos bytes extras
  Estos bytes extras remplazan información valida, y son ejecutados como parte de código del programa.

  Posibles configuraciones:
  - Deshabilitado:
    Sin protección.

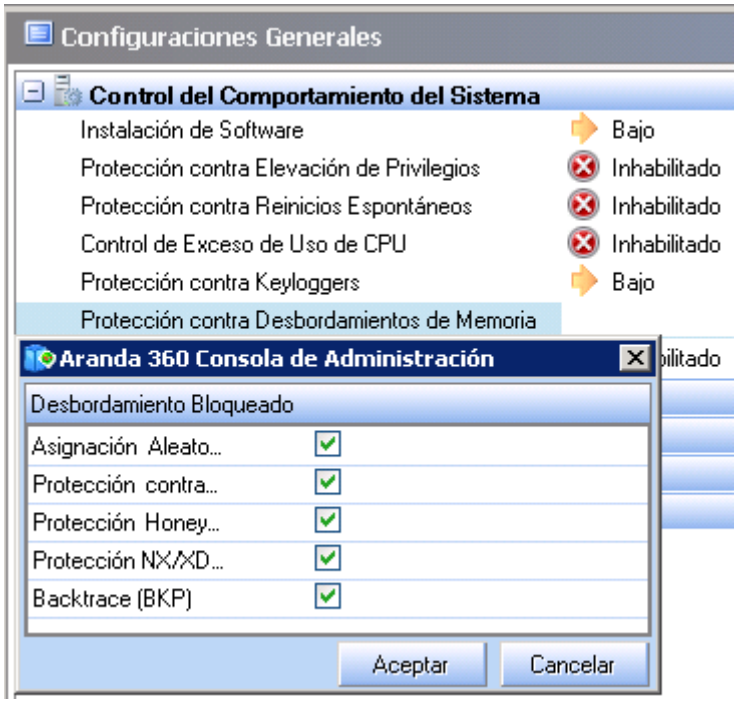
  - Baja:
    KRP+RCP+HPP.

  - Alto:
    Bajo+NXP o BKP aplicado a los procesos de red.

  - Crítico:
    Alto+BKP aplicado a los procesos de red si NXP está habilitado
    O
    Alto +BKP aplicado a todos los procesos si NXP esta deshabilitado.

- Avanzado:
  El administrador puede deshabilitar una o varias técnicas de protección en caso de alguna incompatibilidad.

  Posibles opciones:



- ASLR (KRP):
  Esta opción se utiliza para establecer aleatoriamente la dirección base de kernel32.dll cuando es asignada a memoria (bajo XP) en cada reinicio.

  Reinicie la máquina para activación/desactivación ASLR (KRP) para ser tenido en cuenta.

- Ret-Lib-C (RCP):
  Esta opción bloquea ataques return-into-lib(c).

- Honeypot (HPP):
  Esta opción genera un señuelo que será utilizado por código malicioso para encontrar kernel32.dll.

- NX/XD (NXP):

  En primer lugar, se necesita activar esta característica en la BIOS (Basic Input / Output System) de su máquina, así como el DEP (Data Execution Prevention) de Windows.
  Esta opción de Aranda 360 bloquea la ejecución de procesos basados en direccionamiento de memoria pero no termina el proceso en curso. Hay un alto riesgo de “falsos positivos”, sin embargo.

Puede desactivar esta opción para no bloquear el proceso en curso. Puede resultar útil cuando un proceso legítimo ejecuta código en el espacio de direccionamiento de memoria.

- Backtrace (BKP):
  Esta opción realiza un seguimiento de las operaciones que llevaron a cabo la ejecución de código no confiable.
  Esta opción puede ralentizar el rendimiento de la máquina. Si es necesario, puede desactivarse.

  - En caso de incompatibilidad entre una aplicación y la protección de desbordamiento de la memoria, se recomienda verificar que la aplicación se ejecuta apropiadamente mediante la desactivación de las opciones de protección NX/XP (NXP) y traza inversa (BKP).
    Si el problema persiste, agregue una regla en Reglas de Confianza.

  - Algunas aplicaciones legítimamente utilizar mecanismos verificados por Protección automática.
    Por ejemplo, la función de depuración en una herramienta de desarrollo de software puede utilizar inyecciones de procesos mientras que una herramienta de control remoto puede realizar capturas de eventos del teclado.
    Esta es la razón por Aranda 360 tiene la capacidad de confiar en estas aplicaciones.

PROTECCIÓN	ASLR	RET-LIB-C	HONEYPOT	NX/XD	BACKTRACE
Deshabilitada	off	off	off	off	off
Baja	on	on	on	off	off
Alta	on	on	on	on	off
Crítico	on	on	on	on	on
Avanzado	on/off	on/off	on/off	on/off	on/off

Tabla 7.1:
Resumen de la protección de desbordamiento de memoria

  - NX/XD y Backtrace:
    - Cuando la opción NX/XD esta deshabilitada o no está presente en la máquina, la opción traza inversa es habilitada.
    - La opción traza inversa esta siempre habilitada cuando la protección contra desbordamiento de memoria es establecida como Crítica.

- Protección de componentes del núcleo:
  Este parámetro permite al administrador activar o desactivar la detección de descargas de controladores.

Un período de aprendizaje permite la protección de los componentes del núcleo para establecer una lista de controladores legítimos. Después de que el periodo de aprendizaje ha terminado, los nuevos y sospechosos controladores serán bloqueados de acuerdo al nivel de protección seleccionado (Deshabilitado, Bajo, Alto o Crítico).

Las posibles configuraciones son:

- Deshabilitado:
  La detección del controlador del núcleo es deshabilitado. No se crea log en el Servidor.

- Baja:
  Nuevos y sospechosos controladores serán detectados pero no bloqueados. Los controladores cuyas descargas no están permitidas por políticas de seguridad serán bloqueadas.

- Alta:
  Nuevos y sospechosos controladores serán bloqueados en el siguiente reinicio. Los controladores instalados por Windows Update son automáticamente puestos como confiables.

- Crítica:
  Desconocidos controladores serán bloqueados en el siguiente reinicio. Los controladores instalados por Windows Update son automáticamente puestos como confiables.

Control de Comportamiento de Procesos

Los parámetros de control de comportamientos de procesos pueden ser configurados a Bajo, Alto o Crítico.

El nivel de protección seleccionado por el administrador puede tener un impacto directo en el comportamiento del agente y la protección basada en perfiles.

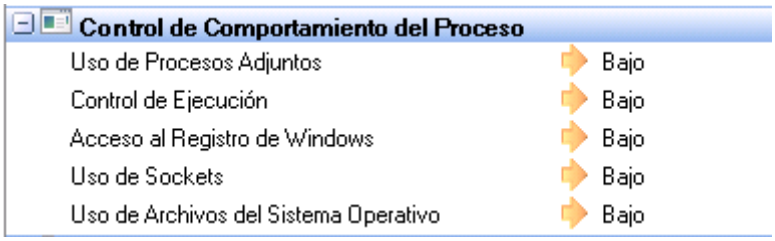


Fig. 7.7. Configuración General: Control de Comportamiento de Procesos

- Acceso de procesos:
  El mecanismo de inyección de procesos es utilizado por programas maliciosos para:
  - Bloquear otro proceso en ejecución.
  - Corromper los procesos que están ejecutándose.
  - Tomar control sobre los procesos que están ejecutándose.

  Las posibles configuraciones son:
  - Baja:
    No bloquea, ni registra (el nivel de confianza cambia marginalmente).
  - Alta:
    El nivel de confianza asignado a la aplicación es afectado por cualquier inyección de procesos inusuales. Sólo las inyecciones de procesos guardados en el perfil de la aplicación durante el período de aprendizaje están autorizadas.
  - Crítica:
    Todas las inyecciones de procesos son bloqueadas y la protección basada en perfiles es usada.

- Control de ejecución:
  Este mecanismo controla la ejecución de las aplicaciones instaladas en la estación de trabajo ya que código malicioso puede estar oculto en aplicaciones autorizadas.

  Las posibles configuraciones son:

- Baja:
  No bloquea.

- Alta:
  Detecta errores de verificación de consistencia (checksum) de las aplicaciones cargadas en memoria.

- Crítica:
  Permite la ejecución de archivos binarios que se encuentren dentro del directorio del sistema de Windows.

  Las extensiones para dichos archivos binarios son:

com	dat	dll	drv	exe	msi
nls	scr	sra	srn	sro	sys
ocx					

- Acceso al registro:
  Este parámetro, que permite la escritura en la base del registro, desactiva Protección Automática y se inicia automáticamente como cualquier otro programa al reiniciar el sistema.

  Las posibles configuraciones son:

  - Baja:
    No bloquea (el nivel de confianza cambia marginalmente).

  - High:
    El nivel de confianza asignado a la aplicación es afectado por cualquier operación inusual en la base del registro.

  - Crítico:
    El nivel de confianza asignado a la aplicación es severamente afectado por cualquier operación inusual en la base del registro.

- Acceso a Socket:

  Las posibles configuraciones son:

  - Baja: Política de lista negra.
    No hay bloqueo de red, excepto cuando una existe una prohibición explícita.
    La protección basada en perfiles no se aplica: la no deviación en el uso de socket afectara el nivel de confianza de la aplicación.
    Todas las conexiones de red de las aplicaciones que no hayan sido explícitamente autorizadas por el administrador (Reglas de Aplicación o Reglas de confianza) se registrarán con la palabra clave [WARN].

  - Alta: Políticas flexibles de lista blanca.

Sólo los accesos de red definidos explícitamente por el administrador y aquellos detectados durante el período de aprendizaje serán autorizados.

- Crítica: Políticas de lista blanca.
  No se permite el acceso a la red a menos que haya sido explícitamente declarada. Los datos recolectados durante el período de aprendizaje no se tienen en cuenta.

- Acceso a Archivos:
  Este parámetro se utiliza para prevenir la corrupción y modificación de nombres archivos ejecutables. Cualquier aplicación declarada en protección basada en reglas queda automáticamente protegida contra cambios de nombre del archivo.
  Las posibles configuraciones son:

  - Baja:
    No bloquea, no registra (el nivel de confianza cambia marginalmente).

  - Alta:
    El nivel de confianza es afectado por cualquier acceso a un tipo de archivo

  - Crítica:
    El nivel de confianza es severamente afectado por cualquier acceso a un tipo de archivo inusual.
    Cualquier intento por cambiar el archivo ejecutable es bloqueado.

  Estableciendo el valor como Crítica es una herramienta ponderosa pero también restrictiva
  La actualización de una aplicación requiere que primero se deshabilite la protección o se inicie otro período de aprendizaje.
  Es altamente recomendable utilizar el modo Advertencia para ajustar una política.

Control de Dispositivos

El control de dispositivos puede ser permitido o denegado:

Fig. 7.8. Configuración General: Control de dispositivos

El control de dispositivos cubre los siguientes elementos:

- Módems (ejemplo: RTC, 3G).
- Bluetooth.
- Puertos IrDA (Asociación De datos por Infrarrojo).
- Puertos LPT (paralelos).
- Puertos Comm.
- Tarjetas inteligentes USB.
- Unidades de disquete (interno o externo).
- CD/DVD/Blu-Ray.
- Quemador CD/DVD/Blu-Ray.
- Tarjetas CMCIA.
- Tarjetas de audio USB
- Dispositivos USB HID (Dispositivos de interfaz humana) teclado o dispositivos apuntadores (ejemplo: mouse, tabletas gráficas, etc.).
- Dispositivos de imagen USB (ejemplo: cámaras, scanners, etc.).
- Impresoras USB.
- Característica U3:
  Bloquea la ejecución automática (autorun) sobre memorias USB y lectores de CD-ROM
- Almacenamiento masivo USB/FW:
  Dispositivos como memorias y discos duros USB, FireWire, etc.

- Recuperación de Almacenamiento masivo:
  Permite al usuario descifrar dispositivos de almacenamiento masivo, los cuales han sido cifrados con Aranda 360.
- Seguridad obligatoria de contraseña:
  Este valor es establecido en 2 por defecto
  Es utilizado para cifrar dispositivos de almacenamiento masivo con Aranda 360.

  - El administrador puede crear políticas aplicadas a grupos de agentes que utilizan dispositivos extraíbles

Los dispositivos cuyo acceso es establecido como No Permitido son bloqueados. Esta información se almacena en los logs de dispositivos y el usuario recibirá una alerta.

Cifrado y Autenticación Wi-Fi
Cifrado y Autenticación Wi-Fi puede ser establecido como Permitir y No Permitir:

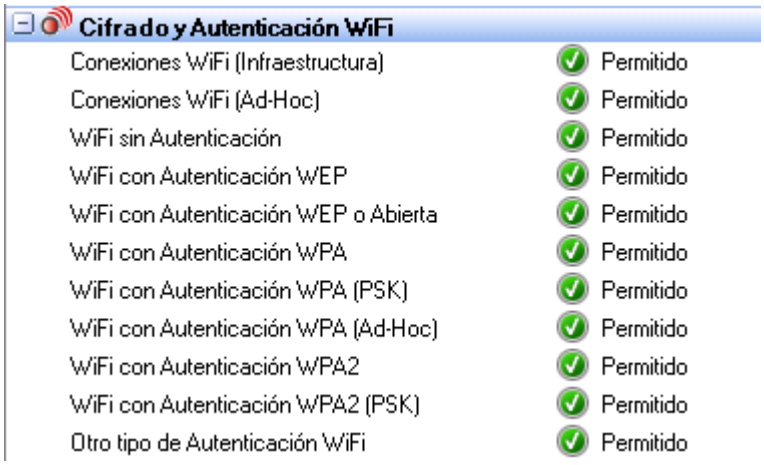


Fig. 7.9. Configuración General: Cifrado y Autenticación Wi-Fi

Los parámetros de Cifrado y Autenticación Wi-Fi son los siguientes:

- Conexiones Wi-Fi:
  Cuando es establecido como Permitido, este parámetro permite el uso de Wi-Fi.
  Cuando es establecido como No Permitido, la interfaz de red permanece activa pero las comunicaciones son bloqueadas.
- Conexiones Wi-Fi adhoc:
  Este parámetro permite o impide el uso de Wi-Fi ad hoc.
  Este tipo de conexión no requiere una estación de trabajo base y está limitada al tiempo de duración de la sesión
- Tipo de autenticación abierto:
  Cuando es establecido como Permitido, no se realizan comprobaciones durante autenticación abierta IEEE 802.11.
- Tipo de autenticación WEP :

Cuando es establecido como Permitido, este modo utiliza la autenticación de claves compartidas IEEE 802.11. Este modo requiere el uso de una clave "privacidad equivalente a cableado" (WEP) para la autenticación 802.11.

- Tipo de autenticación abierto o WEP:

  Cuando es establecido como Permitido, habilita el modo auto-selección. Cuando se utiliza dicho modo, el dispositivo intenta utilizar la autenticación de clave compartida IEEE 802.11.
  Si la autenticación de clave compartida falla, el dispositivo intentará utilizar autenticación abierta IEEE 802.11

- Tipo de autenticación WPA:
  Cuando es establecido como Permitido, habilita el uso de la versión del modo de seguridad WPA versión 1. La autenticación se lleva a cabo entre los servidores solicitantes, autenticadores y de autenticación mediante IEEE 802.1X.
  Las claves de cifrado son dinámicas y son obtenidas a través del proceso de autenticación. En el modo de autenticación, el dispositivo sólo se asociará con un punto de acceso cuyo modelo o detección de respuesta contiene un conjunto de autenticaciones de tipo 2 (clave previamente compartida) de tipo 1 dentro del elemento de información WPA.

- Tipo de autenticación WPA (PSK):
  Cuando es establecido como Permitido, habilita el uso del modo de seguridad WPA versión 1. La autenticación se lleva a cabo entre los servidores solicitantes, autenticadores y de autenticación mediante IEEE 802.1X.
  Las claves de cifrado son dinámicas y son obtenidas a través de una clave pre-compartida utilizada por el solicitante y el autenticador.
  En este modo, el dispositivo sólo se asociará con un punto de acceso cuyo modelo o detección de respuesta contiene un conjunto de autenticaciones de tipo 2 (clave previamente compartida) dentro del elemento de información WPA.

- Modo de autenticación WPA (ADHOC):
  Cuando es establecido como Permitido, habilita el uso del modo de seguridad WPA (ADHOC) versión 1. Esta configuración especifica el uso de una clave previamente compartida sin autenticación IEEE 802.1X.
  Las claves de cifrado son estáticas y provienen de la clave previamente compartida.

- Tipo de autenticación WPA2:
  Cuando es establecido como Permitido, habilita el uso del modo de seguridad WPA versión 2. La autenticación se lleva a cabo entre los servidores solicitantes, autenticadores y de autenticación mediante IEEE 802.1X.
  Las claves de cifrado son dinámicas y provienen del proceso de autenticación.

En este modo, el dispositivo sólo se asociará con un punto de acceso cuyo modelo o detección de respuesta contiene un conjunto de autenticaciones de tipo 1 (802.1X) dentro del elemento de información RSN.

- Tipo de autenticación WPA2 (PSK):

  Cuando es establecido como Permitido, habilita el uso del modo de seguridad WPA versión 2.
  La autenticación se lleva a cabo entre los servidores solicitantes y autenticadores IEEE 802.1X.
  Las claves de cifrado son dinámicas y provienen del proceso de llaves previamente compartidas usadas por el solicitante y el autenticador.
  En este modo, el dispositivo sólo se asociará con un punto de acceso cuyo modelo o detección de respuesta contiene un conjunto de autenticaciones de tipo 2 (llave previamente compartida dentro del elemento de información RSN.

- Otros tipos de autenticación:

  Cuando es establecido como Permitido, habilita el uso de otras autenticaciones.

Control de Actividad de red

Aranda 360 protege la actividad de red a través de un sistema de detección de intrusiones (IDS) y de prevención de intrusiones.

El interés de IDS es múltiple:

- El IDS integrado proporciona a la estación de trabajo la capacidad de protección de red de la Empresa.
- El IDS retorna alertas que identifican con precisión ataques reconocidos.

IDS está integrado con firewall contenido en Aranda 360 para formar un Sistema de prevención de intrusiones (IPS).

El IPS alerta al administrador y bloquea los ataques en tiempo real del tráfico entrante.

Dependiendo de la sensibilidad de IDS definido por el administrador, las alertas generadas pueden lanzar la aplicación dinámica de una regla filtrada por el firewall para interrumpir temporalmente el acceso de red en el puerto afectado y en niveles de protocolo.

El control de actividad de red es utilizado para bloquear las comunicaciones de red en función de la gravedad de la alerta.

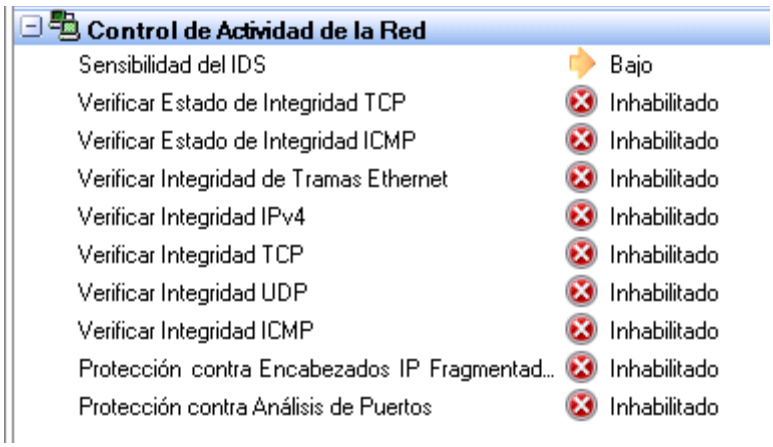


Fig. 7.10: Configuración General: Control De Actividad de Red

Los parámetros de configuración del Control de Actividad de Red son:

- Sensibilidad IDS:
  Las posibles opciones son:
  - o Baja:
    Cualquier actividad de red sospechosa es registrada.
  - o Alta:
    Cualquier actividad de red ilegal es registrada.
  - o Crítico:
    Cualquier actividad de red ilegal es bloqueada.

Cuando está habilitada esta opción, es utilizada durante el análisis caché ARP para bloquear el robo de identidad.

Correlación entre IDS e IPS

El ajuste de sensibilidad permite activar/desactivar las siguientes funciones:

- Protección contra desbordamiento.
- Protección contra escaneo de puertos.
- Protección contra "Envenenamiento de Cache ARP" (ARP cache poisoning.)

A. Protección contra desbordamiento

Protege las conexiones utilizando el protocolo TCP contra desbordamientos. Se efectuará un seguimiento de las conexiones entrantes y eliminara conexiones que permanecen demasiado tiempo en el estado SYN_RCVD o FIN_WAIT (~ 10 segundos). Si la opción de IDS está establecido como Alta, y más de 20 conexiones están bloqueadas en el estado SYN_RCVD orFIN_WAIT, se eliminarán dichas conexiones.

Fragmentos de Log:

[FLOOD]ÿ[CONNECTION_CLOSED]ÿ[(SYN_RCVD;16006;1533)]ÿ[192.168.42.1
21]ÿ[0]ÿ[0]ÿ[0]ÿ[0]ÿ[HOSTNAMEl]ÿ[20]ÿ[0]
[FLOOD]ÿ[CONNECTION_CLOSED]ÿ[(FIN_WAIT1;80;6218)]ÿ[192.168.42.122
]ÿ[0]ÿ[0]ÿ[0]ÿ[0]ÿ[HOSTNAME]ÿ[20]ÿ[0]

Si la opción de IDS está establecida como Crítica, y más de 10 conexiones están bloqueadas en el estado SYN_RCVD o FIN_WAIT, se eliminarán dichas conexiones y el firewall genera una regla para bloquear las conexiones que vienen de la dirección IP de origen.

Fragmentos de Log

[FLOOD]ÿ[IP_BLOCKED]ÿ[0]ÿ[192.168.42.122]ÿ[0]ÿ[0]ÿ[0]ÿ[0]ÿ[HOSTNAM E]ÿ[20]ÿ[0]

El número de conexiones en el estado SYN_RCVD por servicios es limitado (puerto).

NIVEL IDS	PROTECCIÓN CONTRA DESBORDAMIENTO
Bajo	Deshabilitada
Alto	Las conexiones se elimina cuando son mayor a 20
Crítico	• Las conexiones se elimina cuando son mayor a 10 • Fuente de la dirección IP es bloqueada.

B. Protección contra escaneo de puertos

- Para usar esta característica debe habilitar la Protección contra escaneo de puertos en Configuración General > Control de Actividad de Red.

Consiste en la filtración de:

- Paquetes RST_ACK de puertos TCP cerrados.
- Paquetes ICMP de puertos TCP cerrados.

Una dirección IP es reconocida como un escáner cuando un número de paquetes filtrados es alcanzado:

- Aproximadamente 3 paquetes para escaneos rápidos
- Aproximadamente 3 paquetes para los análisis lentos

Si el IDS está establecido como Bajo, el agente detecta escaneos de puertos, pero no se tomarán acciones para bloquear la dirección IP asociada con el escaneo detectado.

Fragmentos de Log cuando IDS es establecido en Bajo:

[PORTSCAN]ÿ[SCAN_IN]ÿ[CHECKSCAN_MAX_QUICK_SUSPICIOUS_REACHED 4: (TCP;8080)(TCP;8081)(TCP;8082)(TCP;8083)]ÿ[192.168.42.117]ÿ[0]ÿ[0] ÿ[0]ÿ[0]ÿ[HOSTNAME]ÿ[0]ÿ[61710]

Si el IDS está establecido como Alto o Crítico, el agente bloqueará la dirección IP asociado al escáner detectado.

Fragmentos de Log indicando que los escaneos entrantes son bloqueados, cuando IDS es establecido en Alto:

[PORTSCAN]ÿ[SCAN_IN]ÿ[CHECKSCAN_MAX_QUICK_SUSPICIOUS_REACHED 4: (TCP;49154)(TCP;49157)(TCP;34313)(TCP;37792) (Blocked until

20h06m33s)]ÿ[192.168.42.117]ÿ[0]ÿ[0]ÿ[0]ÿ[0]ÿ[HOSTNAME]ÿ[777]ÿ[0]

Logs SCAN_OUT son mostrados si el equipo que ejecuta el agente actúa como un escáner:

[PORTSCAN]ÿ[SCAN_OUT]ÿ[CHECKSCAN_MAX_QUICK_SUSPICIOUS_REACHED 4: (TCP;8080)(TCP;8081)(TCP;8082)(TCP;8083)]ÿ[192.168.42.1]ÿ[0]ÿ[0]ÿ[

0]ÿ[0]ÿ[HOSTNAME]ÿ[0]ÿ[61710]

IDS LEVEL	PROTECTION AGAINST PORT SCAN
Bajo	Filtros de escaneo de puertos
Alto	• Filtros • Bloqueos
Crítico	• Filtros • Bloqueos

C. Protección contra "Envenenamiento de cache ARP" (cache poisoning ARP)

Esta protección detecta:

- Cuando la máquina que está ejecutando el agente intenta robar la identidad de otra máquina en la red.
- Cuando cualquier máquina en la red intenta robar la identidad de otra máquina.

Esta protección incluye:

- Una inspección de estado ARP para filtrar respuestas que no corresponden a solicitudes ARP.
- Protección para paquetes innecesarios (gratuitos ARP) que son enviadas cuando el agente detecta que una máquina ha robado la identidad del host del agente. Las solicitudes innecesarias (gratuitos ARP) se utilizan para corregir entradas en la caché ARP de las máquinas que no dispongan de Aranda 360.

IDS LEVEL	PROTECTION AGAINST PORT SCAN
Bajo	Filtros de escaneo de puertos
Alto	• Filtros • Bloqueos
Crítico	• Filtros • Bloqueos

Fragmento de log:

[ARP_DELETE 00000005]ÿ[IN]ÿ[Request EthSrc=00:20:20:20:20:20 EthDst=00:16:17:2d:26:99 ArpHwSrc=00:20:20:20:20:20 ArpIpSrc=192.168.42.254 ArpHwDst=00:00:00:00:00:00 ArpIpDst=192.168.42.254]ÿ[192.168.42.254]ÿ[PORTSRC]ÿ[PORTDST]ÿ[PROTO1]ÿ[PROTO2]ÿ[]ÿ[0]ÿ[61710]

IDS	IPS		
	PROTECTION CONTRA	PROTECTION CONTRA	PROTECTION CONTRA
Bajo	Deshabilitado	Filtros de escaneo	Inspección de estado
Alto	Conexiones son eliminadas cuando > 20	• Filtros • Bloqueos	• Inspección de estado • "Gratuitos ARP" bloqueada
Crítico	• Conexiones son eliminadas cuando > 10 • Dirección IP fuente bloqueada	• Filtros • Bloqueos	• Inspección de estado • Gratuitos ARP bloqueada • Protección contra robo de identidad

Tabla 7.2: Resumen de la correlación entre IDP y IPS

- Verificación de integridad de estado TCP:
  Este parámetro puede ser establecido como Habilitado o Deshabilitado. Se verifica el cumplimiento con el protocolo RFC 793.

- Verificación de integridad de estado IMCP:
  Este parámetro puede ser establecido como Habilitado o Deshabilitado. Se verifica el cumplimiento con el protocolo RFC 792.

- Verificación de integridad de tramas Ethernet:
  Este parámetro puede ser establecido como Habilitado o Deshabilitado. Se verifica el cumplimiento con el protocolo RFC 894.

- Verificación de integridad IPv4:
  Este parámetro puede ser establecido como Habilitado o Deshabilitado. Se verifica el cumplimiento con el protocolo RFC 791.

- Verificación de integridad TCP:
  Este parámetro puede ser establecido como Habilitado o Deshabilitado. Se verifica el cumplimiento con el protocolo RFC 793.

- Verificación de integridad UDP:
  Este parámetro puede ser establecido como Habilitado o Deshabilitado. Se verifica el cumplimiento con el protocolo RFC 768.

- Verificación de integridad ICMP:
  Este parámetro puede ser establecido como Habilitado o Deshabilitado. Se verifica el cumplimiento con el protocolo RFC 792.

- Protección contra fragmentación de cabeceras:
  Este parámetro puede ser establecido como Habilitado o Deshabilitado.
  Protege contra ataques de red mediante la fragmentación de cabeceras como una manera de saltarse las reglas del firewall.

- Protección contra escaneo de puertos:
  Este parámetro puede ser establecido como Habilitado o Deshabilitado.
  Bloquea los paquetes entrantes desde la dirección origen, si un escaneo de puertos es detectado.

PROTECCIÓN BASADA EN REGLAS

Permite al administrador definir qué acciones están autorizadas o prohibidas a nivel de sistema y de red (ejemplos: acceso a archivos, base de registro o protocolos de red).

Las Reglas representan la granularidad más sofisticada de las políticas de seguridad definidas por el administrador. Están organizados por categorías en el Editor de Políticas de Seguridad

Estas categorías son:

- Firewall.
- Reglas de Aplicación.
- Reglas de Extensión.
- Componentes del Núcleo.
- Reglas de Confianza.
- Puntos de acceso Wi-Fi.
- Dispositivos Extraíbles.

LISTAS BLANCAS Y NEGRAS

Basado en reglas de protección puede utilizarse en un enfoque de listas blancas o negras.

Una aproximación al concepto de lista blanca consiste en la prohibición de todo lo que no esté expresamente autorizado.

Un enfoque de lista negra consiste en autorizar todo lo que no está expresamente prohibido.

COMBINANDO LISTAS BLANCAS Y NEGRAS

Éstas pueden combinarse en función del entorno en el que se aplican las reglas.

Es posible utilizar una lista blanca para todo lo relativo al acceso de red y una lista negra cuando se trata de aplicaciones que los usuarios pueden utilizar legítimamente.

Capítulo 8 - PROTECCIÓN BASADA EN REGLAS

ACERCA DE ESTE CAPÍTULO

Este capítulo explica en detalle la configuración de la protección basada en reglas en el firewall de red y del sistema.

Contiene lo siguiente:

- La relación entre los componentes de las políticas de seguridad:
  - Reglas.
  - Grupo de reglas.
  - Categoría de reglas.

- Tipos de Políticas de Seguridad:
  - Políticas vacías.
  - Políticas estándar.
  - Políticas avanzadas.

- Editor de Políticas de Seguridad.

- Categorías de Reglas:
  - Firewall.
  - Reglas de aplicación.
  - Reglas de Extensión.
  - Componentes del núcleo.
  - Reglas de Confianza.
  - Puntos de Acceso Wi-Fi.
  - Dispositivos Extraíbles.

- Administración de reglas:
  - Adicionando una regla.
  - Importando una regla.
  - Importando un grupo de reglas.
  - Eliminando una regla.
  - Estableciendo un orden de prioridad para las reglas.
  - Habilitando/Deshabilitando un grupo de reglas.
  - Mostrando más detalles sobre las reglas.

- Manejando conflictos en las reglas:
  - Orden de prioridad para la regla.
  - Ejemplos.

- Convenciones de escritura:
  - Aplicación del formato de entrada.
  - Variables de ambiente.

- Configuración de plantillas:
  - Generalidades.
  - Grupos predefinidos y configuración de reglas.

RELACIÓN ENTRE LOS COMPONENTES DE LAS POLÍTICAS DE SEGURIDAD

En la siguiente figura se examina la relación entre:

- Reglas.
- Grupo de reglas.
- Categoría de reglas.

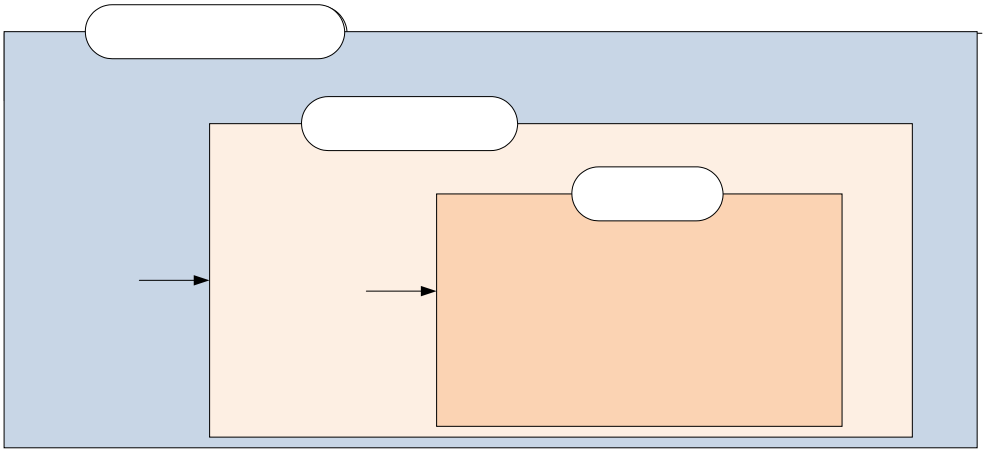


Fig. 8.1. Relación entre los componentes de las políticas de seguridad

Fig. 8.2. Componentes de políticas de seguridad: Categorías, Grupos y Reglas.

REGLAS

Protección basada en reglas permite al administrador definir y asegurar la aplicación de políticas de seguridad explícitas. Una política de seguridad está definida por reglas formales establecidas para permitir o prohibir el acceso a determinados servicios o información

Las Reglas representan la representan la granularidad más sofisticada de más de las políticas definidas por el administrador. Ellas están organizan en el Editor de Políticas de seguridad.

GRUPO DE REGLAS

Las reglas son puestas en grupos en para facilitar su uso por parte del administrador.

Estos son algunos ejemplos de grupos de reglas que figuran dentro de los archivos proporcionados por Aranda Systems.

Estos grupos de reglas se generan al importar el archivo de Aranda Systems ", o al crear una política de seguridad avanzada después de la verificación de los grupos adecuados:

- Grupo por defecto.
- Sistema Base.
- Red Base.
- Navegadores Web.
- Cliente de Correo.
- P2P.
- Mensajería Instantánea.
- Multimedia.

CATEGORÍAS DE LAS REGLAS

Los Grupos de reglas son puestos en categorías.

Éstas son listadas a continuación:

- Configuración general.
- Firewall.
- Reglas de aplicación.
- Reglas de Extensión.
- Componentes.
- Reglas de confianza.
- Puntos de acceso Wi-Fi.
- Dispositivos Extraíbles.

TIPOS DE POLÍTICAS DE SEGURIDAD

Cuando se adiciona una nueva política de seguridad, el administrador tiene la opción de elegir entre tres tipos de políticas:

- Políticas Vacía.
- Políticas Estándar.
- Políticas Avanzada.

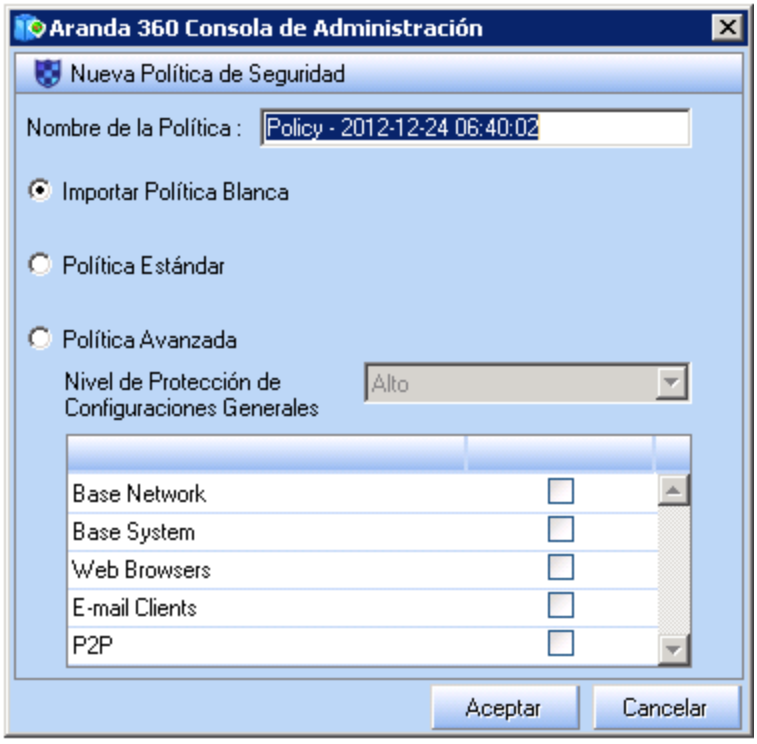


Fig. 8.3. Tipos de Políticas de Seguridad

POLÍTICAS VACIA

Una política de seguridad vacía contiene el grupo de reglas por defecto que puede ser configurado por el administrador.

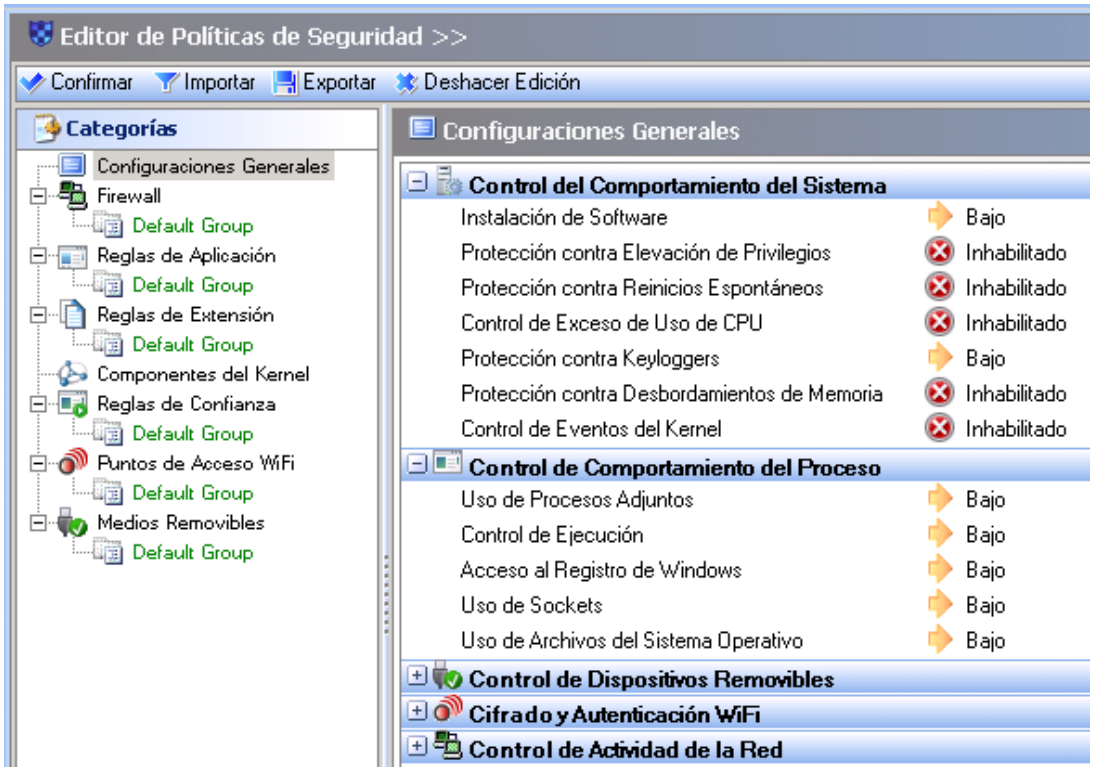


Fig. 8.4. Editor de Políticas de Seguridad: Ejemplo de Políticas Vacía

POLÍTICAS ESTANDAR

Además de contar con los grupos de reglas predeterminadas, una política de seguridad estándar contiene los siguientes grupos de reglas:

- Red Base:
  Este es un conjunto de reglas del firewall utilizadas para servicios estándar en estaciones de trabajo.

- Sistema Base:
  Este es un conjunto de reglas del sistema utilizadas para servicios estándar en estaciones de trabajo.

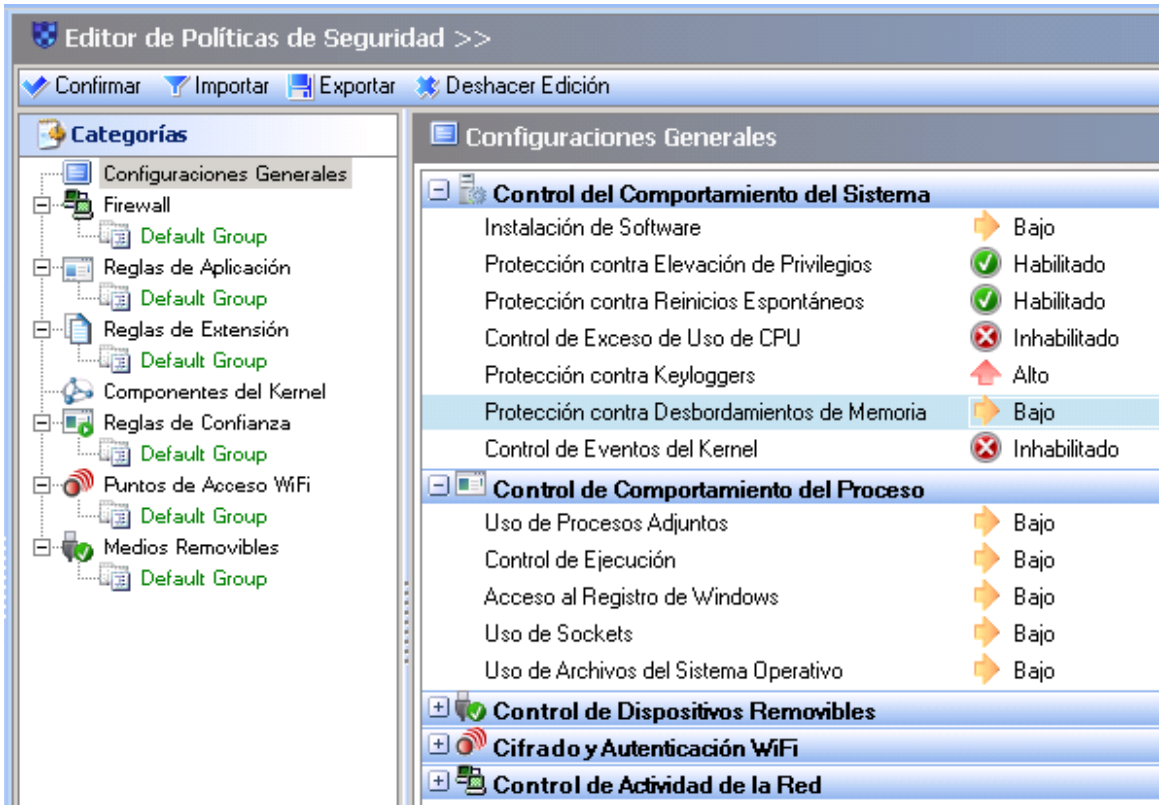


Fig. 8.5.

Editor de Políticas de Seguridad: Ejemplo de Políticas Estándar

POLÍTICAS AVANZADAS

Al crear una política de seguridad avanzada, el administrador puede optar por adicionar otros grupos de reglas para los grupos de reglas predeterminados.

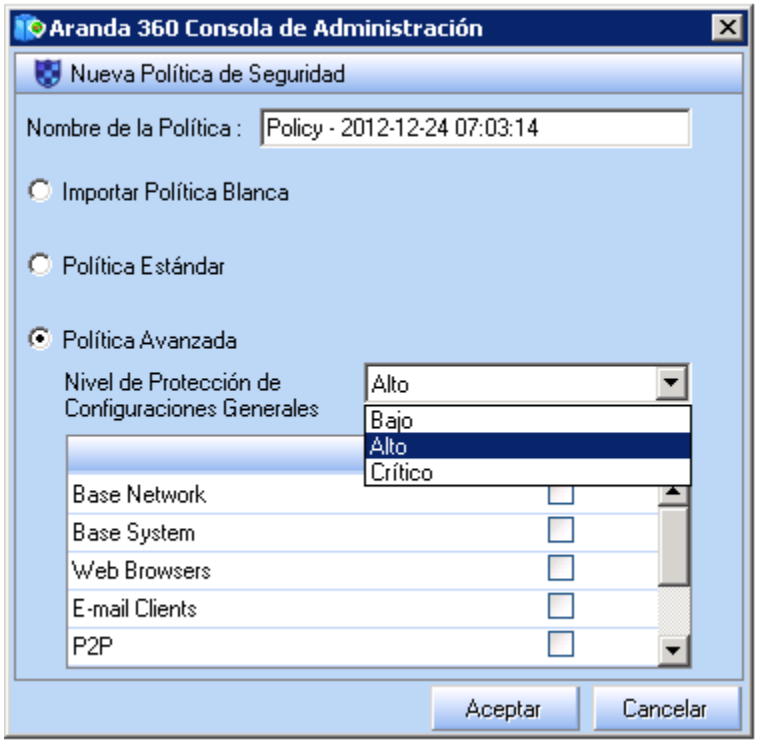


Fig. 8.6. Opciones de Políticas de Seguridad Avanzada

El administrador puede elegir entre siete grupos de reglas:

- Red Base:
  Grupo de reglas para controlar DNS, netbios y la administración de la máquina.

- Navegador Web:
  Grupo de reglas para controlar o restringir el navegador Web estándar.

- Clientes de Correo Electrónico:
  Grupo de reglas restrictivas para los clientes de correo electrónico estándar que controla el acceso a POP3, SMTP y HTTP. También se restringe el acceso a VBS y exe.

- Sistema Base:
  Grupo de reglas de los principales servicios y programas de Windows y programas como svchost, explorer y rundll.

- P2P:
  Grupo de reglas restrictivas para denegar el acceso a las aplicaciones punto a punto (peer-to-peer - P2P).

- Mensajería Instantánea:
  Grupo de reglas restrictivas para los clientes de mensajería instantánea (restricciones de red para el servidor y archivos compartidos).

- Multimedia:
  Grupo de reglas restrictivas para los reproductores multimedia y formatos de archivos.

EDITOR DE POLÍTICAS DE SEGURIDAD

Las políticas de seguridad incluyen reglas que el administrador puede configurar en el Editor Políticas de Seguridad sobre la consola de administración.

El panel del editor incluye las siguientes categorías en modo de visualización de árbol.

Fig. 8.7. Políticas de seguridad en modo de visualización de árbol, la cual incluye categorías (en negro) y grupos de reglas (en verde)

CATEGORÍAS DE REGLAS

Para abrir una categoría de reglas, haga clic en el nodo de Categorías. Existen ocho categorías:

- Configuración General:
  Esta categoría se encuentra en el primer nivel. Estos ajustes determinan la protección automática.
- Firewall:
  Esta categoría permite un control estático y dinámico del firewall.

- Reglas de Aplicación:
  Esta categoría contiene:
  - Todas las reglas relacionadas con las aplicaciones en ejecución.
  - Todas las reglas relacionadas con la modificación de aplicaciones.
  - Aplicaciones con permisos sobre la red, archivos y registros.

- Reglas De Extensión:
  Esta categoría es utilizada para definir reglas de acuerdo al tipo de archivo, independientemente de la aplicación que tenga acceso.

- Componentes del Núcleo:
  Esta categoría ofrece una protección al núcleo, habilitando el control sobre la carga y detección de controladores sospechosos.

- Reglas de Confianza:
  Esta categoría es utilizada para liberar a ciertas aplicaciones de cualquier verificación para evitar bloqueos.

- Puntos de Acceso Wi-Fi:
  Esta categoría ofrece protección de red, habilitando el control sobre los puntos de acceso Wi-Fi accedidos por las estaciones de trabajo.

- Dispositivos Extraíbles:
  Esta categoría proporciona protección a los dispositivos extraíbles, permitiendo el control sobre los dispositivos que pueden ser utilizados por las estaciones de trabajo.

Para remover el acceso a dispositivos extraíbles, conexiones Wi-Fi y/o Wi-Fi adhoc, vaya a Configuración General > Cifrado y Autenticación Wi-Fi

FIREWALL

Aranda 360 está integrado con un firewall, el cual es controlado:

- Estáticamente (por reglas del administrador).
- Dinámicamente (mediante la reacción de alertas IDS embebidas).

Las operaciones estáticas del firewall están definidas por reglas.

Las operaciones estáticas del firewall están definidas por la sensibilidad y la gravedad de las alertas IDS.

Las reglas son mostradas en formato tabular:

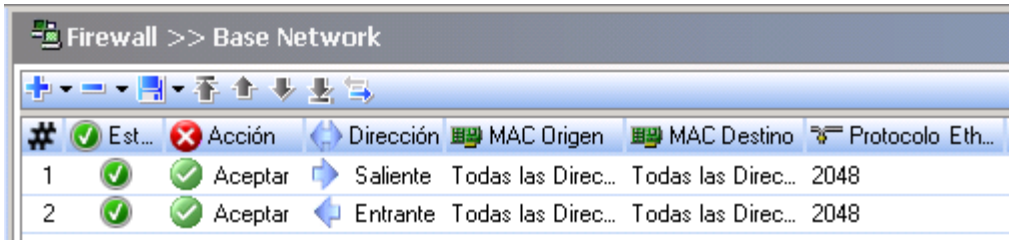


Fig. 8.8. Reglas del Firewall

Las Interfaces de red en modo puente (bridge) sobre las máquinas virtuales no son filtradas por el firewall.

Atributos

Los atributos de las reglas de red son las siguientes:

- #:
  Este atributo es utilizado para definir el orden en que las reglas serán evaluadas con el fin de evitar conflictos entre ellas.

  El firewall utiliza la primera regla que coincide.

- Estado:

  Este atributo puede ser establecido como Habilitado o Deshabilitado.

  Una regla deshabilitada, aunque es guardada en la configuración no se evalúa cuando sucede el evento.

  El ícono de habilitado es:

  El ícono de deshabilitado es:

- Acción:
  Bloquea o acepta el flujo de información.

  El ícono de Aceptar es .

  El ícono de Bloquear es .

- Dirección:

  Define si el flujo de información se filtra en la entrada o en la salida.

  Las reglas sobre tráfico TCP, ICMP y UDP son de estado. Esto significa que sólo la dirección del primer paquete necesita ser definido. Una regla para permitir una respuesta a un flujo se generado de forma dinámica por el firewall. En otros casos (sin estado), el administrador debe definir dos reglas: una regla para la entrada y otra para la salida.

- IP Remota:

  Es atributo es utilizado para restringir el flujo de información de la dirección de destino. Esta dirección puede ser:

  - Una dirección IP.
  - Una lista de direcciones IP.
  - Un rango de direcciones IP.

  Por defecto, no se especifica el equipo host. Esto significa que la regla se aplica a todas las direcciones.

- Sobre IP:

  Este atributo define a cual protocolo IP se aplicará la regla.

- Con Estado:

  Este atributo permite activar/desactivar el procesamiento de flujos con estado TCP, UDP o ICMP.

  Las Reglas con estado mantendrán el estado de la sesión, mientras que el firewall automáticamente genera la regla requerida por el flujo de respuesta.

- Puerto Local:

  Este atributo define número del puerto del host local (para TCP y UDP) o el código (para ICMP).

  El administrador puede definir:

  - Número de puerto.
  - Lista de puertos.
  - Rango de puertos.

- Puerto Remoto:

Este atributo define número del puerto del host remoto (para TCP y UDP) o el código (para ICMP). El administrador puede definir:

- Número de puerto.
- Lista de puertos.
- Rengo de puertos.

- Log:
  Este atributo es utilizado para guardar archivos del log.

- Descripción:
  Añade comentaros a la regla.

- Grupo:
  Este atributo indica el grupo al que pertenece la regla. Esto sólo es visible en él la raíz de cada categoría.

Atributos Adicionales

El administrador tiene acceso más opciones haciendo clic sobre la barra de herramientas del firewall. Se visualizarán más columnas.

Los atributos adicionales son:

- MAC Local:
  Restringe el flujo de datos de la dirección origen.
  Estas direcciones pueden ser:
  - Dirección MAC.
  - Lista de direcciones MAC.
  - Lista de rangos MAC.

  Por defecto, ningún host es especificado. Esto significa que la regla se aplica a todas las direcciones.

- MAC Remoto:
  Restringe el flujo de datos de la dirección destino.
  Estas direcciones pueden ser:
  - Dirección MAC.
  - Lista de direcciones MAC.
  - Lista de rangos MAC.

  Por defecto, ningún host es especificado. Esto significa que la regla se aplica a todas las direcciones.

- Sobre Ethernet:
  Este atributo define el protocolo sobre Ethernet, en la cual es aplicada la regla.

- IP Local:
  Restringe el flujo de datos de la dirección fuente.
  Estas direcciones pueden ser una dirección IP o una lista de direcciones.
  Por defecto, ningún host es especificado. Esto significa que la regla se aplica a todas las direcciones.

  Atributos de MAC locales y remotos se tienen en cuenta sólo bajo Windows XP.

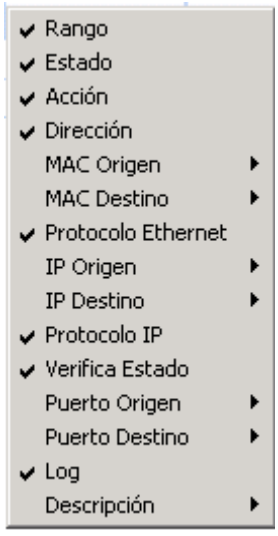
Configuración de atributos

Interfaz Gráfica

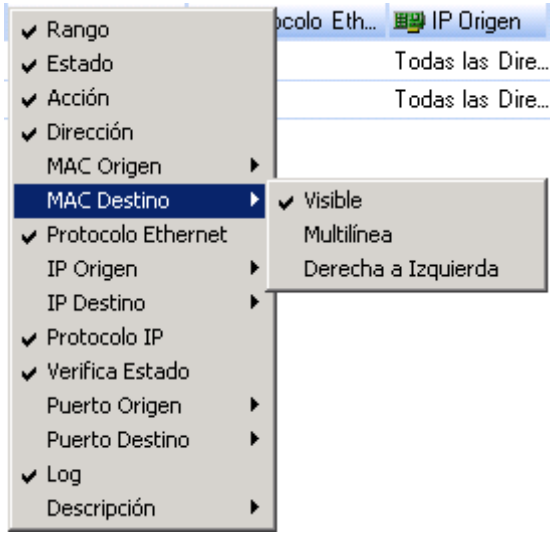
Por defecto, la configuración del Firewall está establecida a “Todos” y el estado como “Aceptar”.

Puede seleccionar las columnas que se muestran haciendo clic derecho en cualquier cabecera.

Escoja las cabeceras que quiera mostrar en la lista.

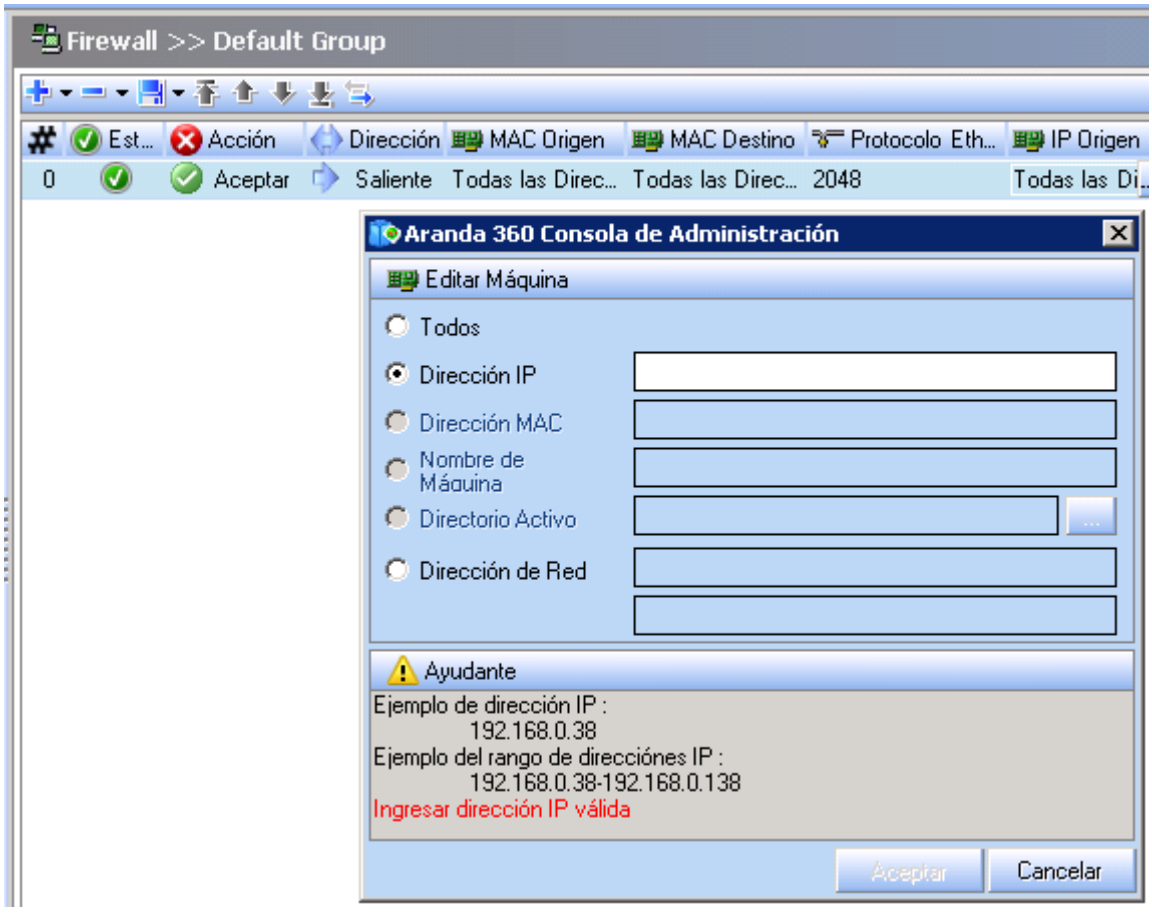


Puede personalizar la visualización de algunos atributos para facilitar la lectura:



IP Remota

Para modificar la configuración, Haga clic en ... para visualizar la siguiente pantalla y realizar las respectivas modificaciones:

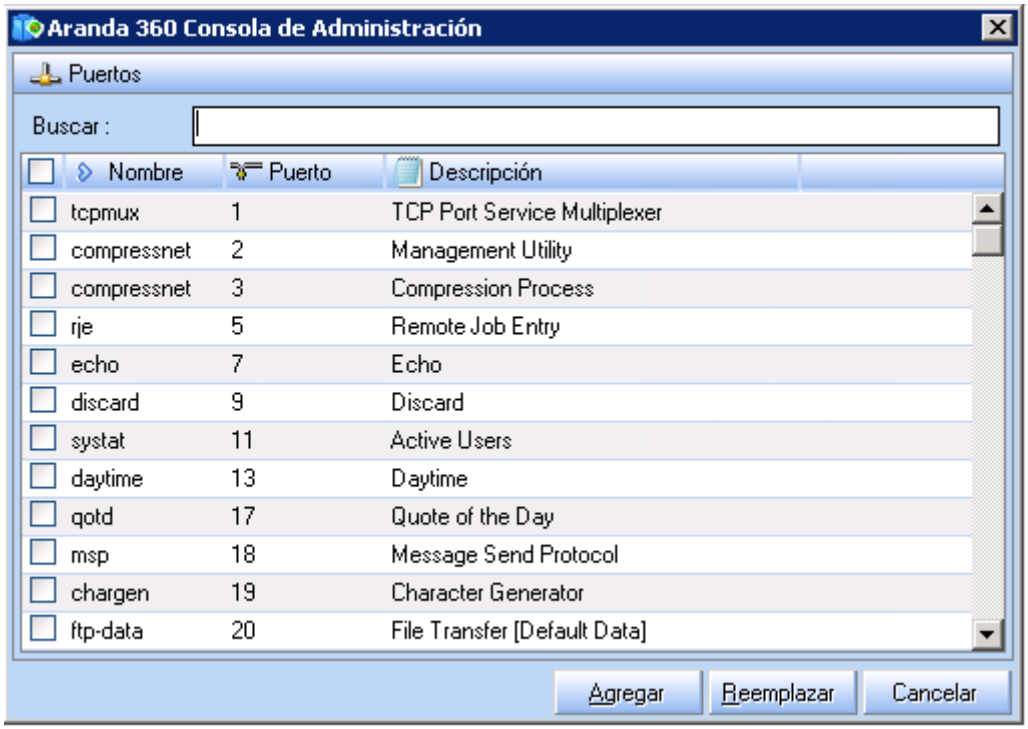


Sobre IP

Para modificar la configuración, Haga clic en para visualizar la siguiente pantalla y realizar las respectivas modificaciones:

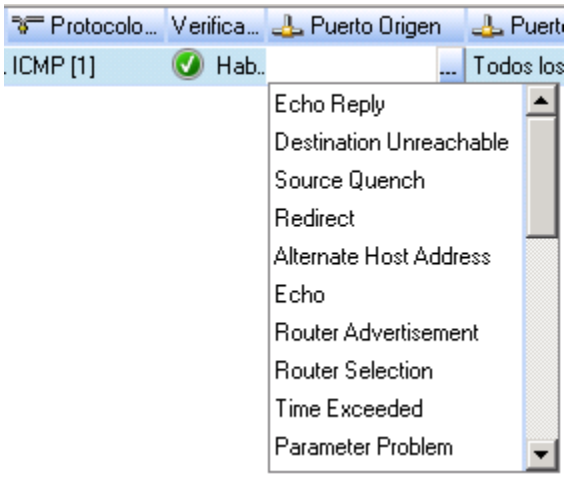
Puerto Local

Para modificar la configuración, Haga clic en ... para visualizar la siguiente pantalla y realizar las respectivas modificaciones:



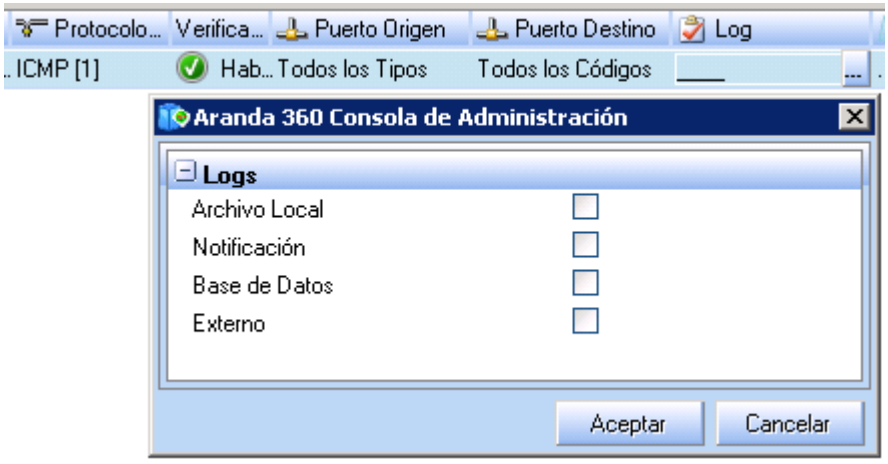
1. Seleccione los servicios necesarios haciendo clic en las casillas respectivas.
2. Introduzca los caracteres en el campo de búsqueda para reducir el desplazamiento en la lista.
3. Haga clic en adicionar después de realizar la selección.

Para modificar la configuración, Haga clic en ... para visualizar la siguiente pantalla y realizar las respectivas modificaciones:



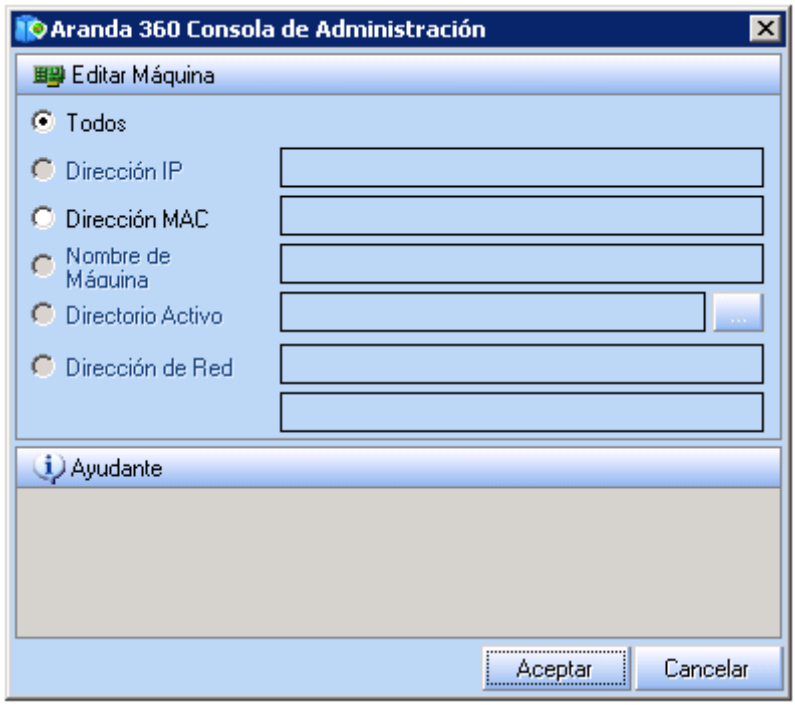
Log

Para modificar la configuración, Haga clic en ... para visualizar la siguiente pantalla y realizar las respectivas modificaciones



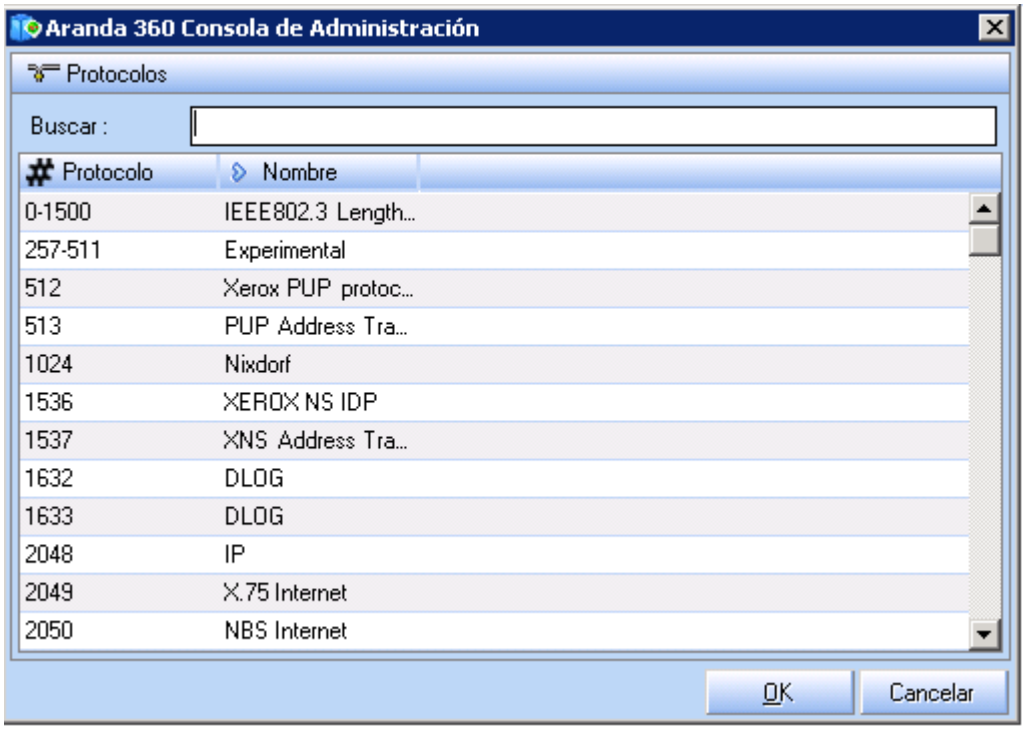
MAC Local

Para modificar la configuración, Haga clic en •- para visualizar la siguiente pantalla y realizar las respectivas modificaciones:



Sobre Ethernet

P ara modificar la configuración, Haga clic en para visualizar la siguiente pantalla y realizar las respectivas modificaciones:



1. Introduzca los caracteres en el campo de búsqueda para reducir el desplazamiento en la lista.
2. Seleccione el protocolo apropiado.
3. Haga clic en OK.

REGLAS DE APLICACIÓN

Aquí se muestra un ejemplo de reglas de aplicación:

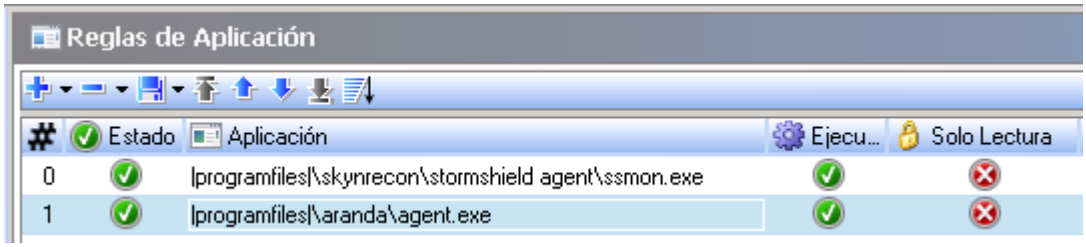


Fig. 8.9. Reglas de Aplicación

Atributos

Los atributos de las reglas de aplicación son:

- Estado:
  Este atributo define el estado de las reglas que puede ser establecido como Habilitado o Deshabilitado.
  Una regla deshabilitada, aunque es guardada en la configuración no se evalúa cuando sucede el evento.
  El ícono de habilitado es .
  El ícono de deshabilitado es .

- Aplicación:
  Este atributo define la aplicación a la que se le aplicará la regla. El uso de un comodín al final de la ruta de acceso permite establecer una regla que cubra todos los programas ejecutables en una ruta determinada.
  Ejemplo: |archivosdeprograma|\Internet Explorer*

- Ejecución:
  Este atributo permite o deniega el acceso a la aplicación.

- Solo Lectura:
  Este atributo protege la aplicación. Cuando se establece como Habilitado, no es posible:

  - Modificar
  - Mover
  - Renombrar
  - Eliminar la aplicación.

- Archivos:
  Este atributo muestra los permisos de acceso a los archivos:

  - Solo Lectura (ejecutar).
  - Acceso Denegado.
  - Permitir (ejecutar).
  - Creación Denegada.
  - Ejecución Denegada.

- Red:
  Este atributo controla los permisos de acceso a la red.

- Registro:
  Este atributo controla los permisos de acceso al registro.

- Copiar/Pegar:
  Este atributo controla la función copiar/pegar en las aplicaciones.

- Log:

Este atributo define la configuración para guardar y ver archivos del log.

- Descripción:

Para definir comentarios.

- Grupo:

Este atributo indica el grupo al que pertenece la regla. Esta indicación sólo es visible en la raíz de cada categoría.

Barra de Herramientas

La barra de herramientas (En la parte superior de la ventana) es utilizada para:

- Adicionar
- Importar
- Guardar
- Eliminar
- Ordenar reglas.

El campo buscar es utilizado para reducir desplazamiento en la lista.

Configuración de atributos

Red

Haga doble clic en la columna Red para abrir la ventana de Acceso a Red.

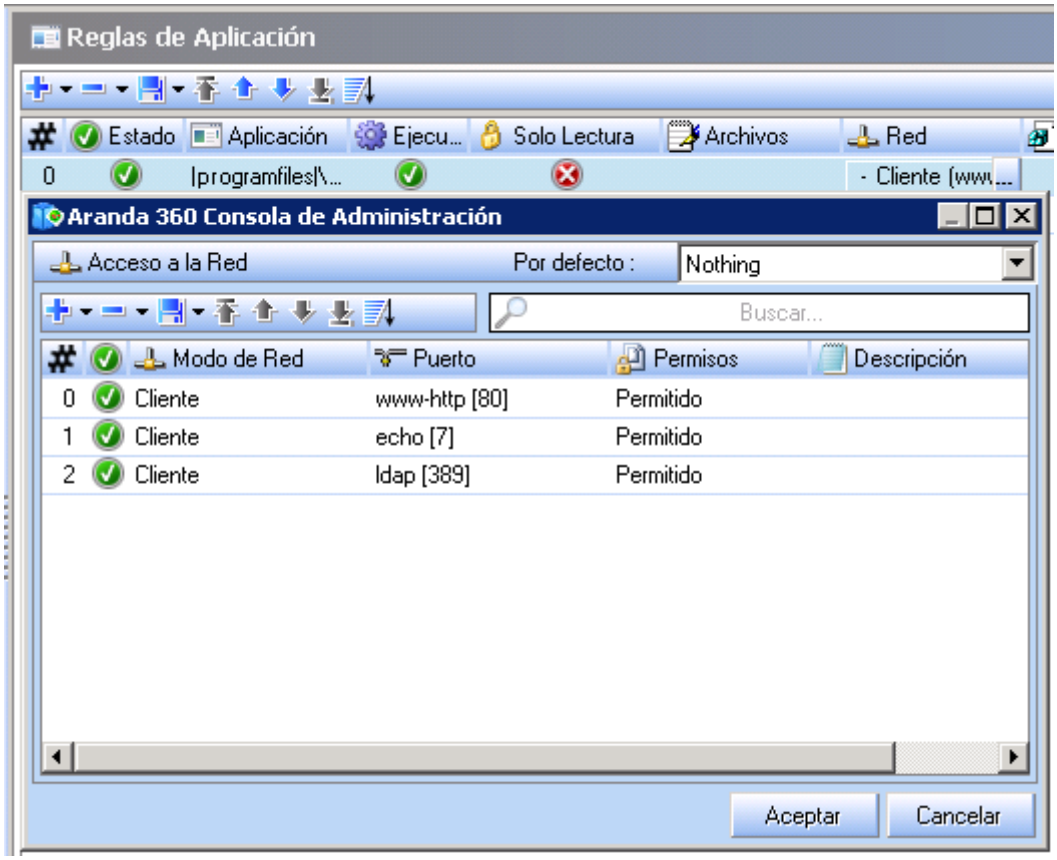
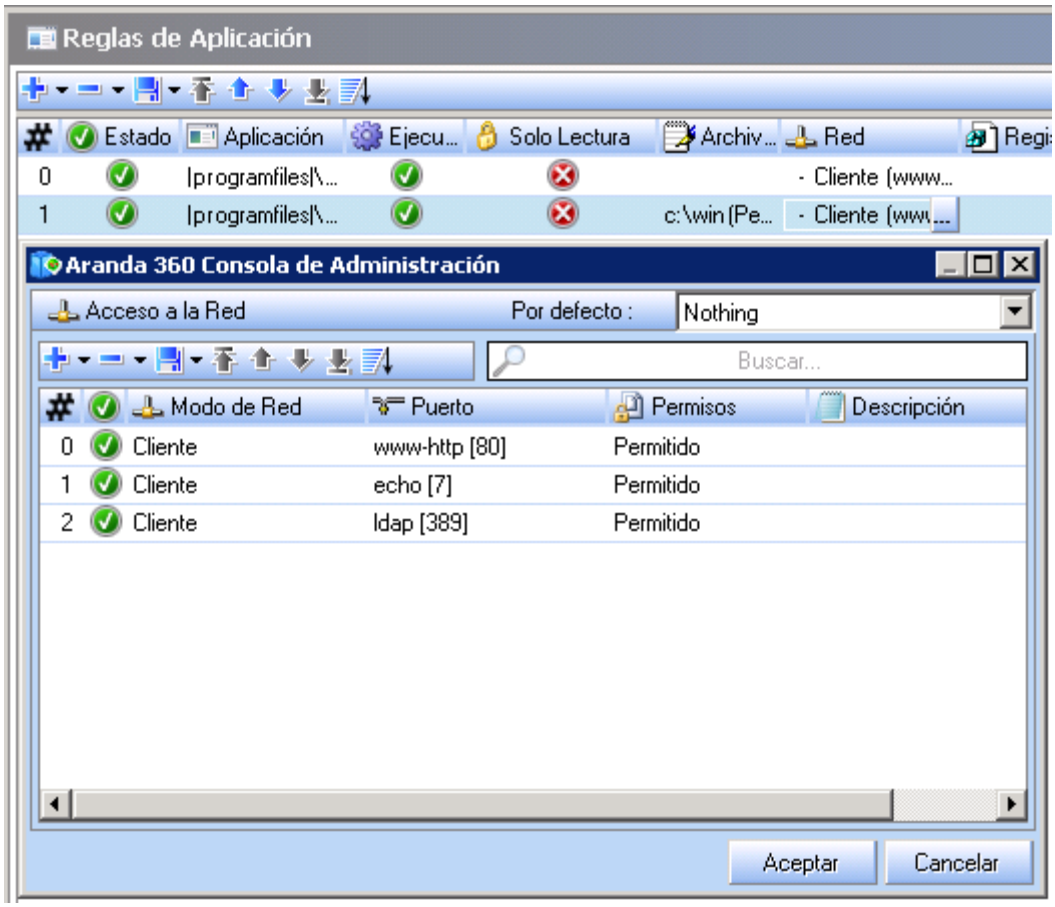


Fig. 8.10: Ventana de Acceso a Red

Administración general de permisos sobre la red

Los permisos de una aplicación se gestionan con carácter general y de forma detallada.

Los permisos son definidos en el campo Por Defecto. Este campo se utiliza para restringir las comunicaciones.



Cuatro opciones están disponibles:

- Denegar solo Servidor:
  La aplicación no puede escuchar ningún puerto. Sólo puede operar en modo de Cliente, lo cual significa que sólo la aplicación puede iniciar una conexión a un servicio dado.

- Denegar solo Cliente:
  La aplicación sólo puede funcionar en modo Servidor. Sólo puede responder a las conexiones iniciadas por clientes.

- Denegar Todo:
  No se le permite a la aplicación conectarse a la red.

- [Vacía]:
  No se aplica el comportamiento por defecto, excepto para el nivel de seguridad global (alto, bajo o crítico) y las reglas asociadas.

  - Sockets locales no son controlados por las reglas de acceso a red.

Administración detallada de permisos sobre la red

Los atributos de acceso a red son los siguientes:

- Estado:
  Este atributo puede ser establecido como Habilitado o Deshabilitado.
  Al igual que otras opciones que requieren activación, un permiso de acceso deshabilitado es almacenado en la configuración, pero no es evaluado al procesar el evento.

- Modo Red:
  Los posibles valores son:
  - Cliente.
  - Servidor.
  - Cliente y Servidor.
  - [Ninguna]: No se aplica el comportamiento por defecto.

- Puerto:
  Utilice el botón de selección para elegir de una lista predefinida de servicios. Puede definir una lista de puertos y rangos.

- Permisos:
  Pude ser establecido como Permitido y No Permitido.

- Descripción:
  Este atributo es un comentario para facilitar su identificación.

Archivos

Haga doble clic en la columna de archivos para abrir la ventana de acceso:

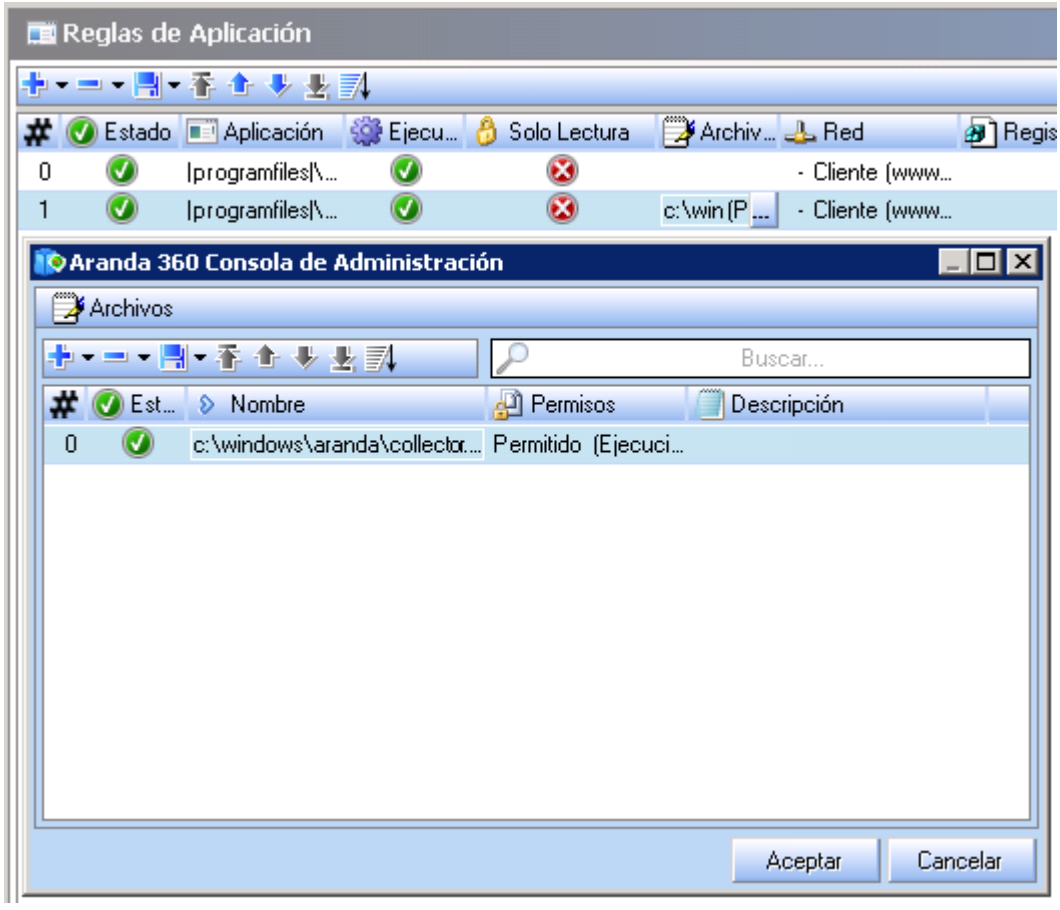
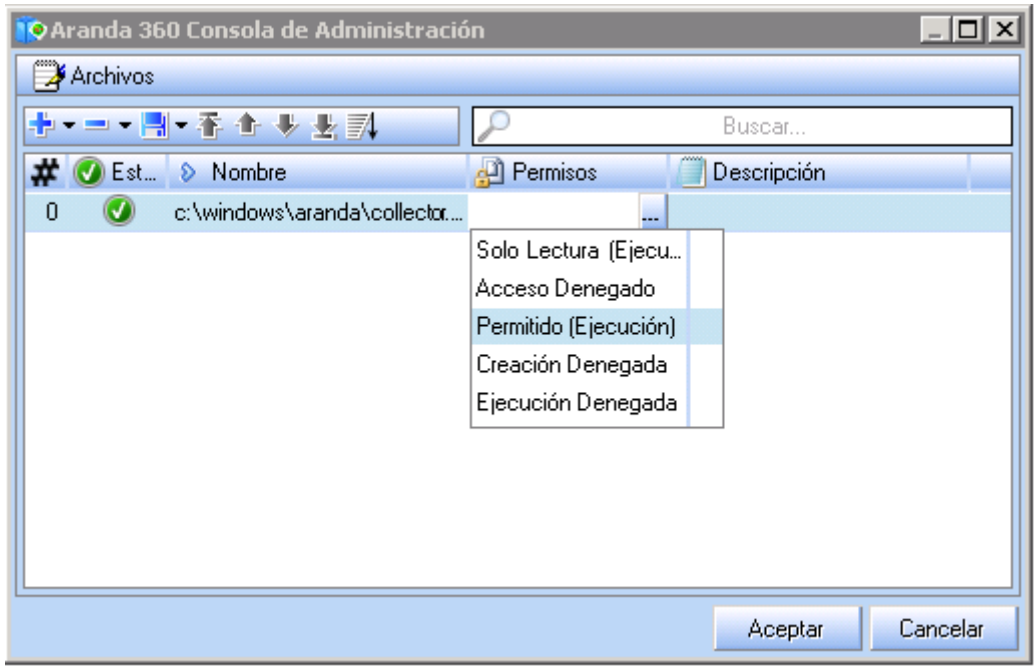


Fig. 8.11: Ventana de Acceso a Archivos

Los atributos son los siguientes:

- Estado:
  Este atributo puede ser establecido como Habilitado o Deshabilitado.
  Al igual que otras opciones que requieren activación, un permiso de acceso deshabilitado es almacenado en la configuración, pero no es evaluado al procesar el evento.
- Nombre:
  Este atributo es el nombre de archivo que puede incluir uno o varios comodines *.

- Permisos:
  Los valores posibles son:



- Descripción:
  Este atributo es un comentario para facilitar su identificación

Registro

Haga doble clic en la columna Registro para abrir la ventana de acceso:

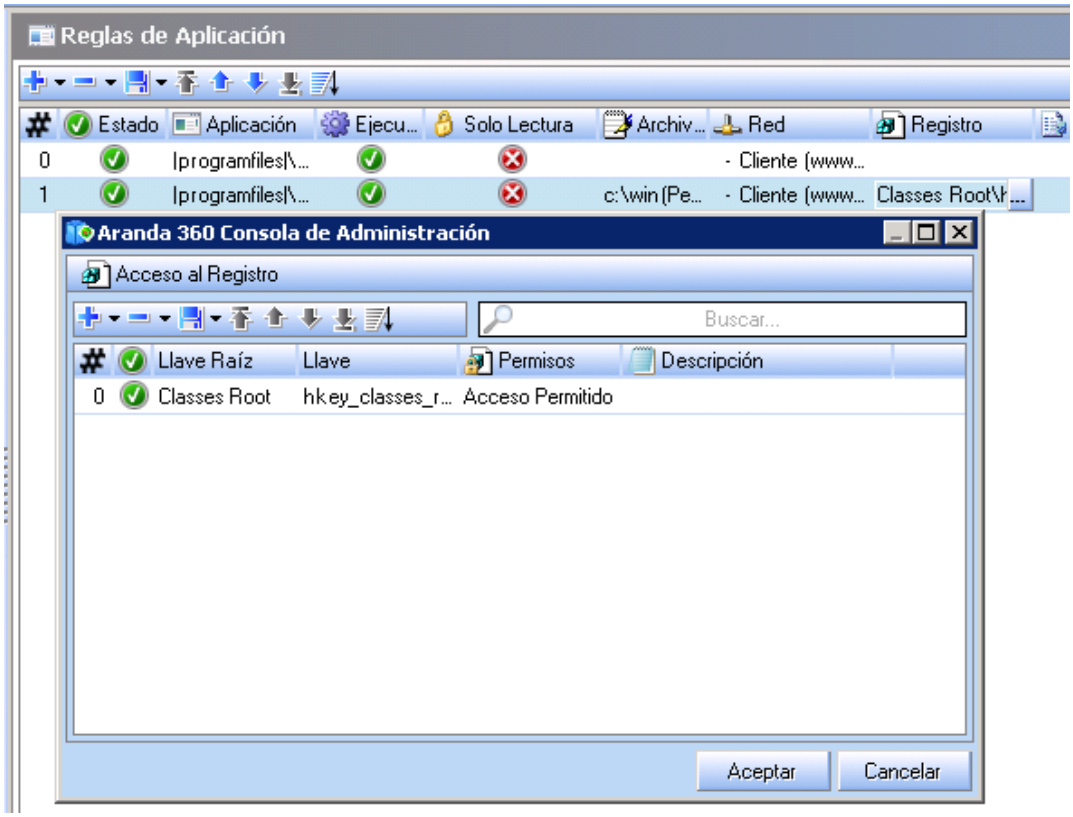
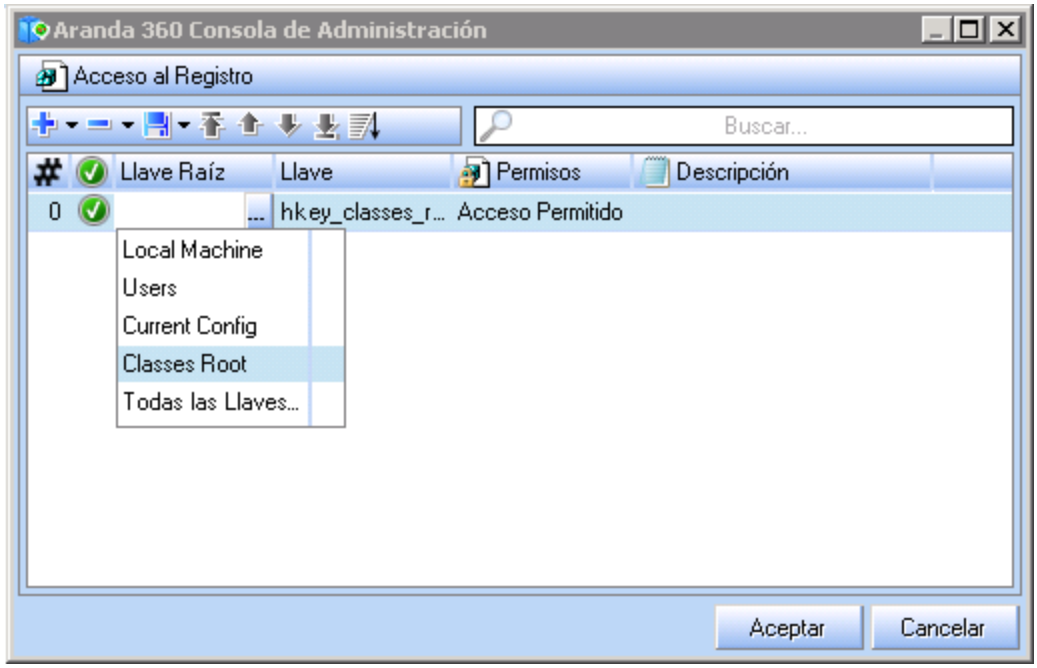


Fig. 8.12: Ventana de Acceso al Registro

Los atributos son los siguientes:

- Estado:
  Este atributo puede ser establecido como Habilitado o Deshabilitado.
  Al igual que otras opciones que requieren activación, un permiso de acceso deshabilitado es almacenado en la configuración, pero no es evaluado al procesar el evento.

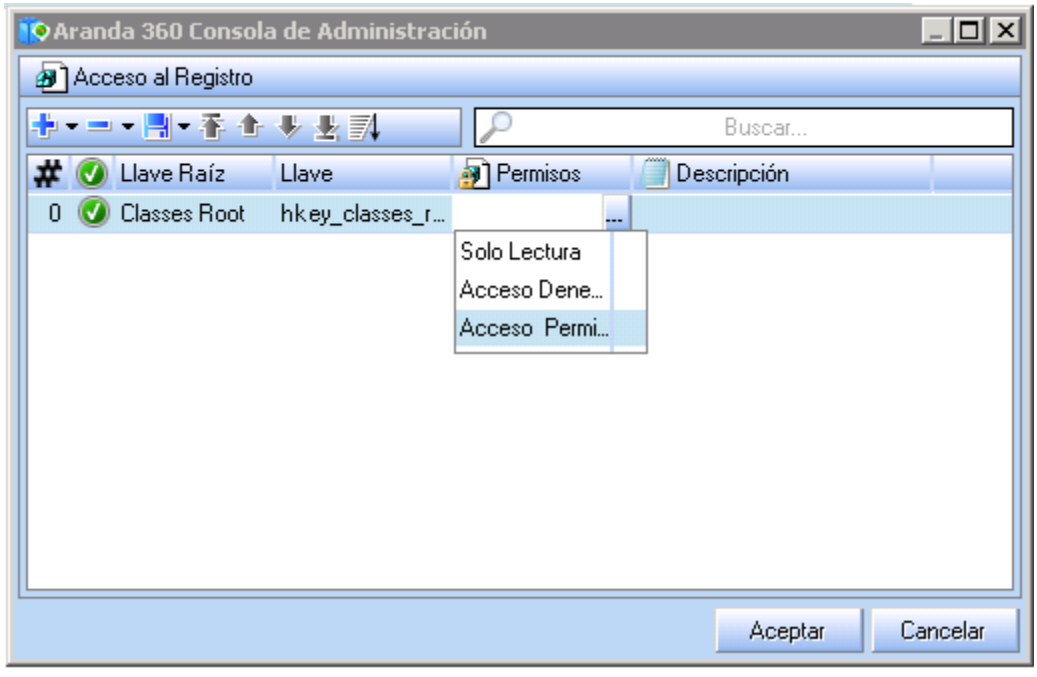
- Llave Raíz:
  Los posibles valores son:
  - Máquina Local.
  - Usuarios.
  - Configuración actual.
  - Clases (CLASSES ROOT).
  - Todas las claves (ROOT KEYS).



- Llave:
  Este atributo es el nombre de la clave para el acceso al registro

- Permisos:
  Los posibles valores son:

  - Acceso denegado.
  - Acceso permitido.
  - Solo Lectura.

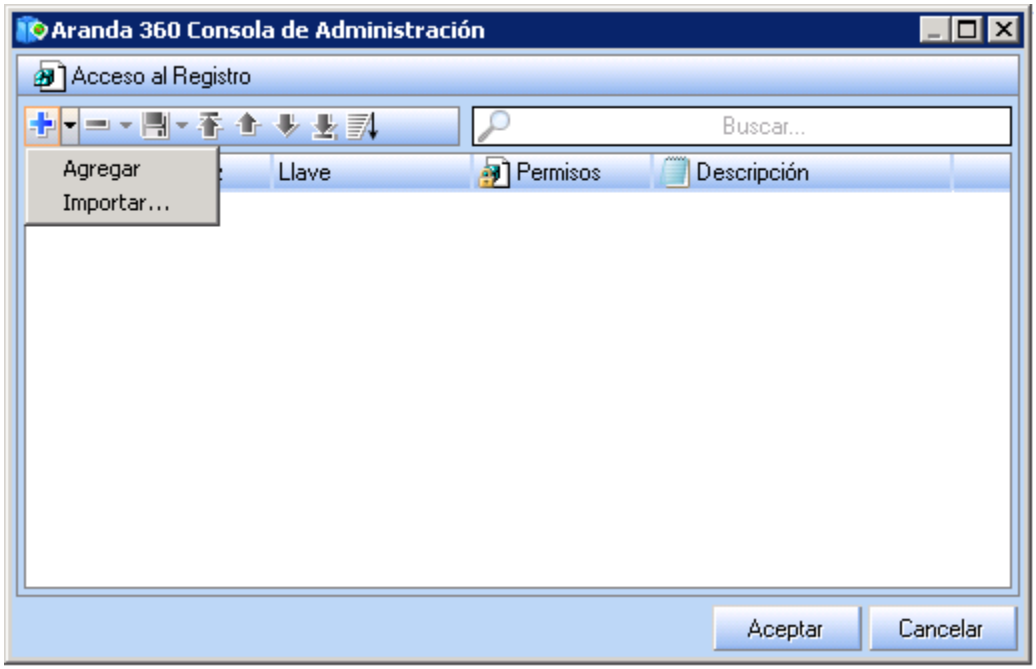


- Descripción:
  Describe el tipo de llave utilizada para acceder al registro para facilitar su identificación

Lista de permisos predefinidos para el acceso al registro

Para facilitar la definición de políticas de seguridad, Aranda 360 tiene una lista de permisos predefinidos para el acceso al registro.

Para importar esta lista predefinida, Haga clic en seguido de Importar. Una ventana de búsqueda se abrirá para escoger el archive a ser importado.



El archive registry_protection.srxml es un archivo de sólo lectura que lista las claves del registro. Los programas maliciosos pueden utilizar estas claves para su instalación en las estaciones de trabajo.

Una vez que la lista es cargada, se puede realizar los siguientes cambios:

- Adicionando líneas.
- Eliminando líneas.
- Cambiando permisos de acceso.

Estas modificaciones no serán reflejadas en el archivo hasta que guarde sus cambios, utilizando .

REGLAS DE EXTENSIÓN

Las reglas de extensión son utilizadas para crear una lista blanca y especificar las aplicaciones que pueden usar dichas extensiones de archivos.

Por cada extensión de archivo especificada, es necesario definir las aplicaciones que pueden acceder a ellos. Por defecto, la definición de una regla para una extensión bloqueará todas las aplicaciones que accedan al correspondiente tipo de archivo

Las Reglas son presentadas en forma tabular:

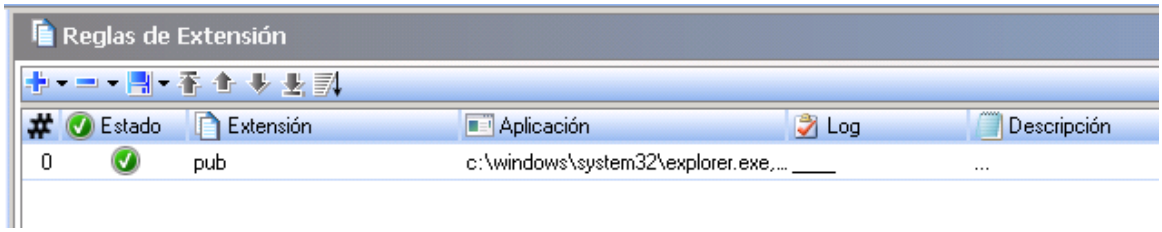


Fig. 8.13: Reglas de Extensión

Atributos

Los atributos de las reglas de extensión son:

- Estado:
  Este atributo puede ser establecido como Habilitado o Deshabilitado.
  Al igual que otras opciones que requieren activación, un permiso de acceso deshabilitado es almacenado en la configuración, pero no es evaluado al procesar el evento.

  - Estado no tiene ningún efecto en si la aplicación puede acceder o no a los archivos con la extensión especificada en la columna respectiva.
    Cuando Estado es establecido como Deshabilitado, la solicitud no será tratada como parte de la lista blanca hasta que el Estado se vuelva a habilitar.

- Extensión:
  Este atributo define la extensión a la que se aplicará la regla. Sólo la extensión se debe introducir. No hay necesidad de introducir un punto o un comodín *.

- Aplicación:
  Este atributo indica qué aplicaciones pueden acceder a los archivos que correspondan con la extensión especificada.
  Por ejemplo, en la Fig. 8.13. “Reglas de Extensión”, tiene acceso a los archivos cuya extensión es. Wab. Ninguna otra aplicación puede acceder a estos archivos a menos que hayan sido incluidas en las reglas de extensión.

- Si no se incluye |systemroot|\explorer.exe en la lista de programas, no se podrán acceder a los archivos a través el explorador

- Log:
  Este atributo indica el log donde los mensajes son guardados cuando una aplicación no especificada en la lista blanca intenta acceder a un archivo cubierto por la regla de extensión. Los mensajes del log serán guardados o visualizados en:

  - La interfaz de usuario.
  - Ventana Emergente.
  - Base de datos.
  - Sistema externo.

- Descripción:
  Este atributo es un comentario para facilitar su identificación.

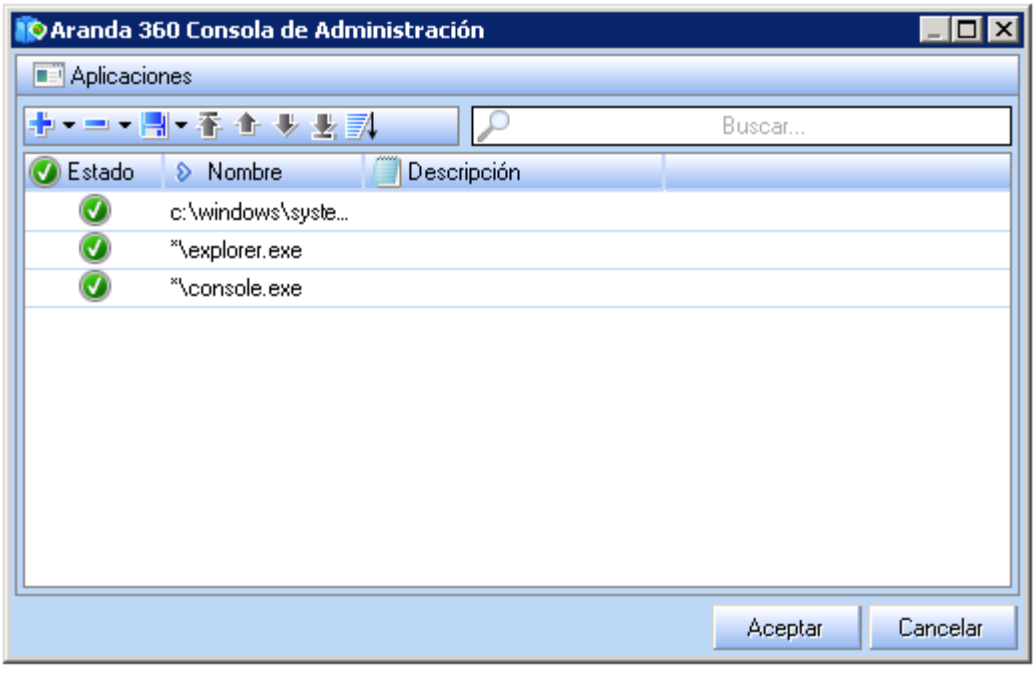
- Grupo:
  Este atributo indica el grupo al que pertenece la regla. Esto sólo es visible en la raíz de cada categoría.

Configuración de Atributos

Aplicaciones

Haga doble clic en la columna Aplicaciones para abrir un cuadro de dialogo.

Esta ventana permite especificar las aplicaciones que tienen permisos sobre los archivos de acuerdo a su extensión.



- Para remover temporalmente una aplicación de las reglas de extensión, haga doble clic en el campo Estado para deshabilitarlo.

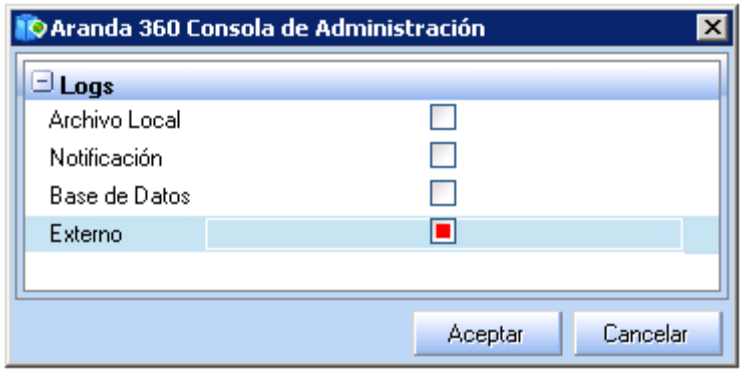
- Si no se especifica una aplicación, la regla aplicará a todas las aplicaciones. Por lo tanto, ésta no será capaz de acceder a los archivos con la extensión especificada.

Logs

Siempre que una regla de extensión es ejecutada, una entrada de registro se agrega al log del sistema.

Para especificar dónde guardar las entradas de registro cuando una regla de extensión es aplicada:

- Haga clic en el campo Log asociado a cada extensión para visualizar la ventana de Logs.
- Marque los log(s) que quiera utilizar.



COMPONENTES DEL NÚCLEO

Atributos

Esta categoría habilita el control sobre la carga de controladores, así como la detección de controladores sospechosos.

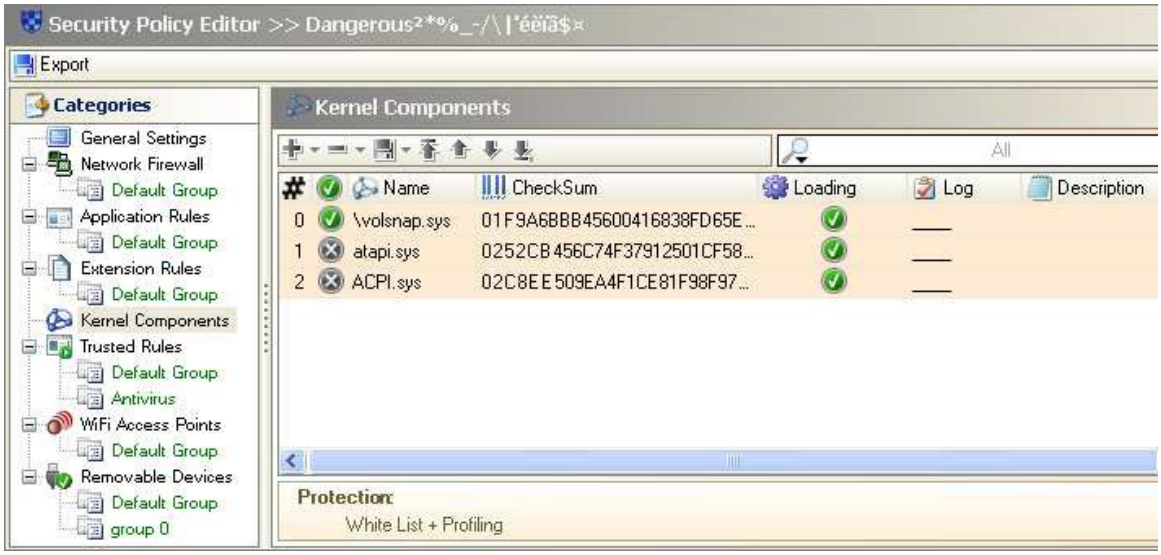


Fig. 8.14: Componentes del Núcleo

Los atributos de los componentes del núcleo son:

- Estado:
  Este atributo puede ser establecido como Habilitado o Deshabilitado.

- Nombre:
  Este atributo es el nombre del driver.

- Verificación de Consistencia (CheckSum):
  Este atributo es el hash del controlador.
  La lista no puede incluir dos veces el mismo hash pero dos controladores pueden tener el mismo nombre con un hash diferente.

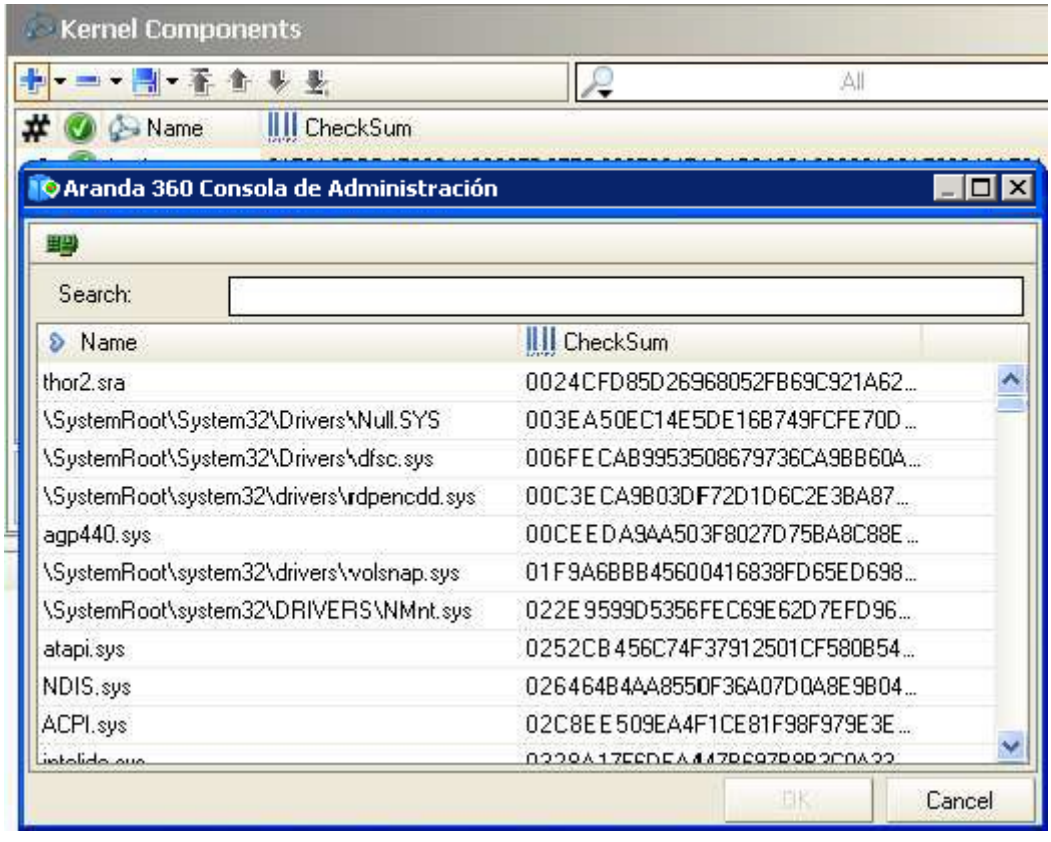
- Carga:
  Este atributo puede ser habilitado o deshabilitado.

- Log:
  Este atributo define la configuración para guardar y ver los archivos del log.

- Descripción:
  Este atributo es un comentario para facilitar su identificación.

Configuración de Atributos

Para adicionar un controlador a la lista de los componentes del núcleo, Haga clic en la barra de herramientas. Se visualizará la siguiente ventana:



La lista de los componentes del núcleo es automáticamente generada a partir de los controladores cargados en las estaciones de trabajo, en donde se ha instalado el agente.

La protección debe estar en un nivel Bajo para que los controladores cargados puedan ser listados.

Puede utilizar el campo de búsqueda para asegurar que el driver o su hash no están ya presente en la lista.

REGLAS DE CONFIANZA

Definiendo las aplicaciones en la categoría de Reglas de Confianza, se liberan estas aplicaciones de ciertas verificaciones, para que puedan continuar ejecutando acciones bloqueadas por estas verificaciones

Por ejemplo:

- Una aplicación de control remoto podría legítimamente usar funciones de captura de teclado (keylogging) si la casilla respectiva es marcada.
- Una herramienta de depuración debe ser capaz de adherir procesos, si la casilla Asociar está marcada.

Atributos

Las Reglas de Confianza son visualizadas en forma tabular

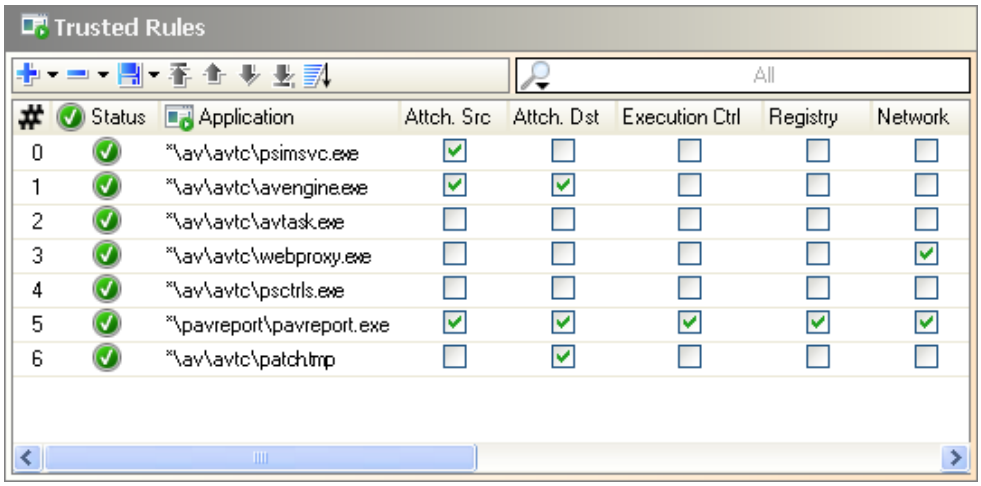


Fig. 8.15: Reglas de confianza

Los atributos de las reglas de confianza son:

- Estado:
  Este atributo puede ser establecido como Habilitado o Deshabilitado.
  Al igual que otras opciones que requieren activación, un permiso de acceso deshabilitado es almacenado en la configuración, pero no es evaluado al procesar el evento.

- Aplicación:
  Este atributo define la aplicación a la que se le aplicará la regla.

- Dominios:
  Este atributo especifica los dominios en los cuales la aplicación es de confianza
  Cuando la casilla de verificación está marcada, significa que la aplicación es de confianza en el respectivo dominio. Todas las acciones relacionadas a este dominio que son normalmente bloqueados, o señaladas por Protección Automática o basada en perfiles, serán consideradas legítimas o protección basada en el perfil será, en este caso, se considera legítima.
  Cuando la casilla de verificación está desmarcada, significa que la aplicación no es de confianza en el respectivo dominio.

- Descripción:
  Este atributo es un comentario para facilitar su identificación.

- Grupo:
  Este atributo indica el grupo al que pertenece la regla. Esto sólo es visible en la raíz de cada categoría.

Dominios de Confianza

Los dominios de confianza son:

- Attach.Src (asociación fuente):
  Si la opción está marcada, la aplicación puede asociar uno o más procesos.

- Attach.Dst (asociación destino):
  Si la opción está marcada, otros procesos pueden asociarse a la aplicación.

- Ctrl Ejecución:
  Si la opción está marcada, el acceso a archivos binarios es permitido.

- Registro:
  Si la opción está marcada, la aplicación puede acceder al registro

- Red:
  Si la opción está marcada, la aplicación puede utilizar sockets.

- Privilegios:
  Si la opción está marcada, la aplicación permite subir los privilegios.

- Archivos:
  Si la opción está marcada, la aplicación puede acceder a los archivos protegidos.

- Captura de teclado (Keylogging):
  Si la opción está marcada, la aplicación puede capturar eventos de teclado.

- Desbordamiento:
  Si la opción está marcada, la aplicación es protegida contra desbordamiento de memoria.

  - Prevención de ejecución de datos (DEP) debe estar habilitado para limitar falsos positivos.

- Reinicio:
  Si la opción está marcada, la aplicación puede reiniciar la estación de trabajo.

- Control de CPU:
  Si la opción está marcada, la aplicación puede sobrecargar la CPU.

Los dominios de confianza corresponden a los ajustes generales definidos para la protección automática y basada en perfiles.

PUNTOS DE ACCESO WI-FI

Generalidades

Las reglas para la conexión Wi-Fi permiten bloquear o aceptar puntos de acceso

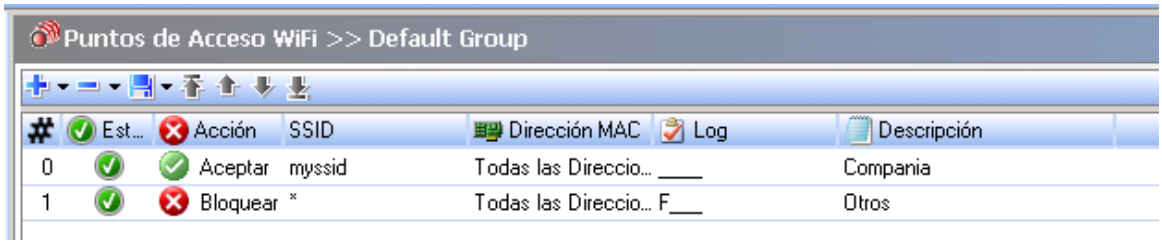


Fig. 8.16: Puntos de acceso Wi-Fi

Las acciones bloqueadas sobre puntos de acceso Wi-Fi son almacenadas en el log de dispositivos.

Las reglas para la conexión Wi-Fi definen una lista blanca de puntos de acceso, en la cual Aranda 360 protege a las estaciones de trabajo

Para crear una lista blanca, se debe crear o modificar una directiva para que incluya:

1. En Configuración general, configure la opción conexiones Wi-Fi como Habilitada (Debajo de la opción Autenticación y Cifrado WI-FI).
2. Seleccione Las reglas de los puntos de acceso Wi-Fi puntos de acceso con los nombres de los SSID permitidos y establezca la opción Acción en Aceptar.
3. Agregue una regla final estableciendo SSID en * y Acción como Bloqueado.

Las reglas Wi-Fi deben ser ordenadas, de esta manera:

- Las reglas con el parámetro Acción establecido como Aceptar serán listadas primero.
- Una regla final con el parámetro Acción establecido como Bloquear y SSID en * son colocados al final de la lista.

Atributos

Los atributos para acceso Wi-Fi son:

- Estado:
  Es el estado de las reglas (Habilitado o deshabilitado).

- Acción:
  Puede tener los siguientes valores: Aceptar o Bloquear.

- SSID:
  Identificador del Conjunto de Servicios.

- Dirección MAC:
  Dirección MAC del punto de acceso.

- Log:
  Define la configuración para guardar y ver los archivos del log.

- Descripción:
  Es solo una explicación libre.

- Grupo:
  Grupo en el cual es aplicada la regla. Es visible solo en la raíz de Puntos de Acceso Wi-Fi.

Barra de Herramientas

Es utilizada para:

Adicionar

- Importar
- Eliminar
- Guardar
- Ordenar Reglas.

DISPOSITIVOS EXTRAIBLES

El uso de grupos de dispositivos extraíbles fortalece la seguridad de la información.

Puede configurar los grupos de dispositivos extraíbles para garantizar el cumplimiento de las políticas de uso de dispositivos extraíbles de la compañía. Por ejemplo, puede crear grupos separados de dispositivos basados en los requerimientos de trabajo de los empleados, cargo en la compañía, etc.

Un grupo de dispositivos extraíbles para ingenieros R&D podrían tener menos restricciones que un grupo administrativo.

Generalidades

Varias reglas de Dispositivos Extraíbles pueden formar un grupo:

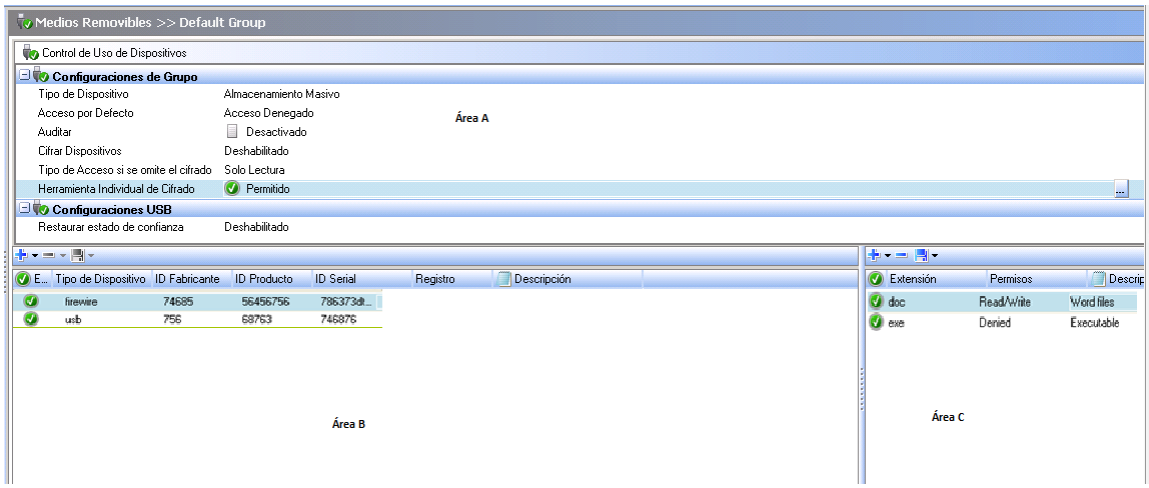


Fig. 8.17: Dispositivos Extraíbles

El panel de dispositivos extraíbles incluye tres áreas:

- Área A: Configuración de Grupos
  Esta configuración es aplicable a todos los dispositivos extraíbles en el grupo.

- Área B: Configuración de Dispositivos Individuales
  Esta es la lista de los dispositivos que constituyen el grupo.

- Área C: Excepciones por extensiones de archivo

Para dispositivos extraíbles de almacenamiento masivo (USB o FireWire), puede especificar las excepciones a las reglas por defecto, de acuerdo a la extensión del archivo.

Ejemplo: Puede configurar la regla de acceso por defecto como Denegada para un determinado dispositivo, pero puede permitir acceso de solo lectura a archivos Excel o Word.

Configuración de Grupos

La configuración a todos los dispositivos extraíbles en el grupo.

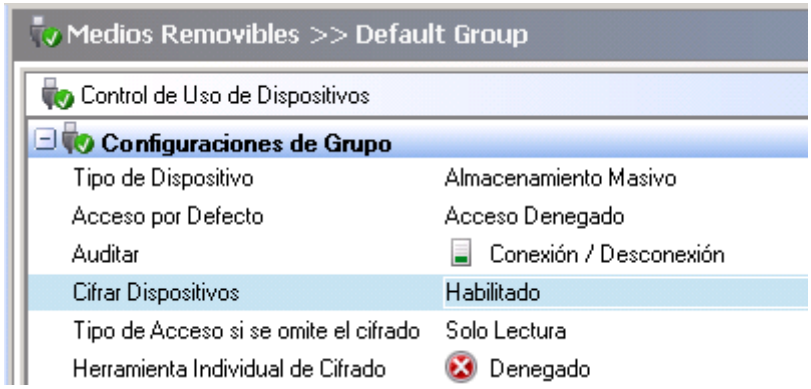


Fig. 8.18: Dispositivos Extraíbles: Configuración de Grupos

La configuración de grupos incluye seis opciones:

- Tipo de dispositivo.
- Por defecto (acceso).
- Auditoria.
- Cifrado de archivos.
- Permisos de acceso si el cifrado es cancelado.
- Herramienta de cifrado Stand-alone (SURT).

Tipo de Dispositivos

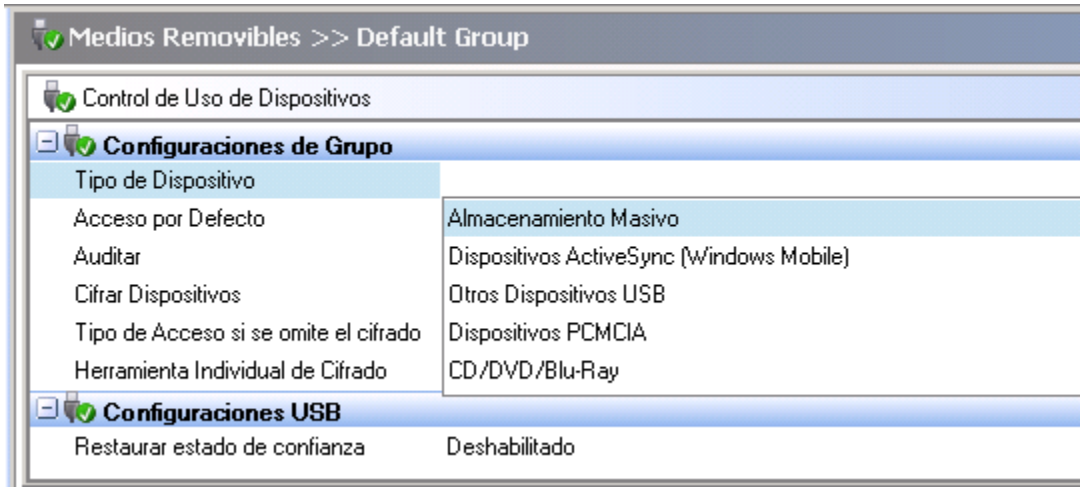


Fig. 8.19: Dispositivos Extraíbles: Tipo de Dispositivos

Este parámetro define el tipo de dispositivo. Puede tomar los siguientes valores:

- Almacenamiento masivo.
- ActiveSync (USB):
  Sincronización con teléfonos móviles (Windows).
- Otros dispositivos USB:
  Es utilizado para todos los tipos de dispositivos USB.
- PCMCIA:
  Permite al usuario insertar tarjetas PCMCIA para facilitar la transferencia y el intercambio de información.
- CD/DVD/Blu-Ray.

Después de seleccionar un tipo de dispositivo, la información relacionada a este valor es actualizada y establecida por defecto. La Actualización de datos consiste en:

- Por Defecto:
  Para obtener más información, ver "Por Defecto (acceso) ".

- Auditoría:
  Para obtener más información, ver "Auditoría".

- Cifrado:
  Para obtener más información, ver "Cifrado de Archivos".

Por defecto (acceso)

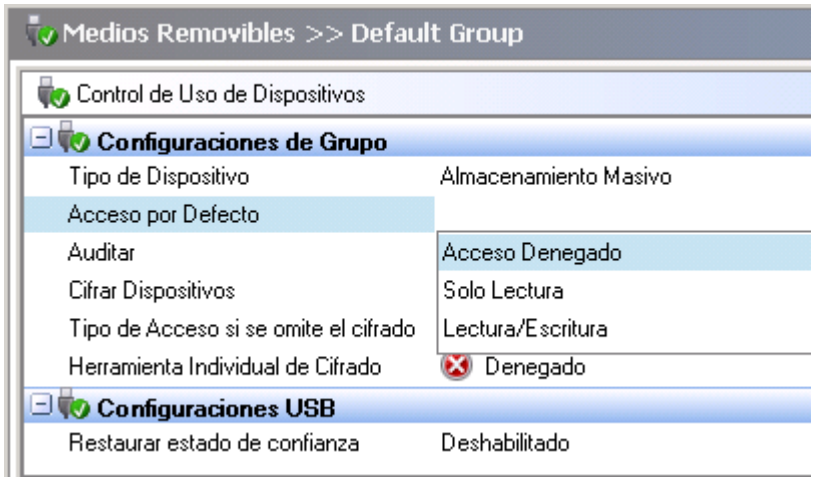


Fig. 8.20: Dispositivos extraíbles: Defecto (acceso)

Este parámetro puede tomar los siguientes valores:

- Denegado:
  Por defecto, el usuario no tiene permisos de acceso a los dispositivos de la lista.
  Si el acceso por defecto para el grupo de dispositivos es establecido como denegado, cuando el usuario vaya a intentar leer o escribir en un dispositivo de dicho grupo, la acción será bloqueada y el evento será registrado en el log de dispositivos.

- Lectura:
  Por defecto, el usuario tiene permisos de lectura a los dispositivos de la lista.
  Si el usuario intenta escribir en algún dispositivo de la lista, la acción será bloqueada y el evento será registrado en el log de dispositivos.

- Lectura/Escritura:
  Por defecto, el usuario tiene permisos de lectura y escritura de todos los dispositivos de la lista.

Puede agregar una lista de archivos que serán exceptuados de la de Access por Defecto.
Esta lista está definida en el Área C llamada Excepciones por extensión de archivo.

Diferencia entre Acceso Denegado desde la Configuración General y de Dispositivos Extraíbles

Cuando el acceso a un dispositivo extraíble es denegado por la política de seguridad en "Configuración general> Control de dispositivos", la unidad aparece en la máquina, pero no su contenido.

Cuando el acceso a un dispositivo extraíble es denegado por la categoría de dispositivos extraíbles en "Dispositivos extraíbles> Configuración de Grupos> Predeterminado, la unidad aparece la máquina.

Además, se pueden listar los archivos y carpetas de la unidad, incluso si el acceso es denegado. La creación de carpetas vacías también es posible, pero no la de archivos nuevos.

Auditoria

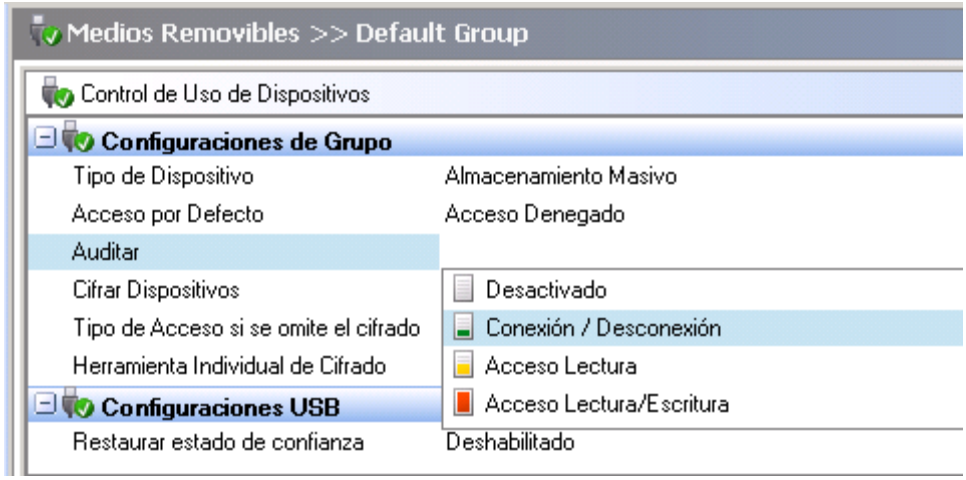


Fig. 8.21: Dispositivos Extraíbles: Auditoría

Este parámetro es utilizado para habilitar la auditoría para un grupo específico de dispositivos de almacenamiento masivo.

Este parámetro le permite monitorear el uso de dispositivos sin bloquear acciones. Puede recopilar información de cómo los dispositivos están siendo utilizados. Cada vez que la auditoría está habilitada, es registrada en el log de dispositivos.

El agente no notifica al usuario cuando la auditoria es lanzada. Sin embargo, el usuario puede ver la actividad de la auditoría en Monitoreo del Log > Dispositivos > Información.

Puede tener los siguientes valores:

- Desactivado:
  Auditoria es deshabilitada.
- Conectar/Desconectar:
  Un registro es escrito en el log de dispositivos, cuando es conectado o desconectado de la máquina un dispositivo de la lista.
  Esta entrada incluye la capacidad de almacenamiento del dispositivo.
- Acceso a Archivos:
  Un registro de la auditoría se genera en el log de dispositivos cuando:
  - Un dispositivo de la lista es conectado o desconectado de la máquina.
  - Un archivo en el dispositivo es creado, renombrado o eliminado.
- Acceso de Escritura:
  Un registro de la auditoría se genera en el log de dispositivos cuando:
  - Un dispositivo de la lista es conectado o desconectado de la máquina.
  - Un archivo en el dispositivo es creado, renombrado o eliminado.

- La auditoría registra acciones en el log de dispositivos. No bloquea acciones no autorizadas. El bloqueo de acciones no autorizadas está controlado por la configuración de acceso Predeterminada y la lista de excepciones en dispositivos extraíbles> Excepciones por extensión de archivo.

Cifrado de Archivos

Este parámetro permite el cifrado de archivos almacenados en un dispositivo USB o FireWire. Puede ser establecido como Activado o Desactivado.

Permisos de Acceso si el cifrado es cancelado

Este parámetro puede tomar los siguientes valores:

- Denegado
- Solo lectura
- Lectura/Escritura (acceso),

  Sucede cuando el usuario decide no cifrar el dispositivo cuando se le solicita crear una contraseña para el cifrado.

Herramienta de Descifrado Stand-alone (SURT)

Este parámetro permite o bloquea el uso de la herramienta de descifrado SURT para habilitar el descifrado de archivos en dispositivos extraíbles, para sistemas que no están ejecutando Aranda 360.

Si esta opción está activada, la aplicación SURT será copiada en los dispositivos extraíbles cifrados por Aranda 360.

Parámetros USB

Los parámetros USB aplican a los dispositivos del grupo.

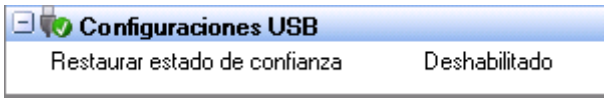


Fig. 8.22: Ventana de definición de parámetros USB

Los parámetros incluyen los siguientes elementos:

- Aplicación del estado de confianza

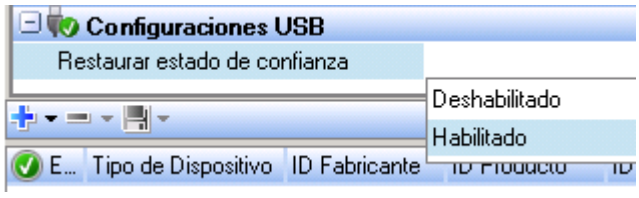


Fig. 8.23: Activación del estado de confianza

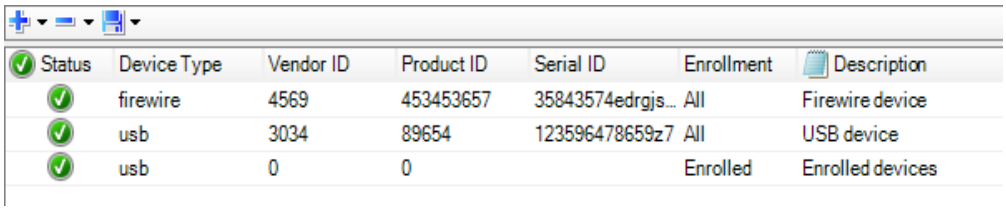
Este parámetro aplica sólo si el dispositivo está registrado.

Cuando esta opción está habilitada y existe un antivirus instalado en el equipo, los archivos agregados o modificados fuera del ambiente controlado por Aranda 360 son verificados por el antivirus con el fin de verificar que no exista riesgo en el contenido.

Adicionando dispositivos a un grupo

Generalidades

Puede crear un grupo de dispositivos con sus respectivos parámetros.



Status	Device Type	Vendor ID	Product ID	Serial ID	Enrollment	Description
✓	firewire	4569	453453657	35843574edrgjs...	All	Firewire device
✓	usb	3034	89654	123596478659z7	All	USB device
✓	usb	0	0		Enrolled	Enrolled devices

Fig. 8.24: Dispositivos Extraíbles: Parámetros

Los dispositivos incluyen detalles específicos (tipos, identificador de proveedores, etc.).

Los dispositivos adicionados en la lista deben incluir toda o parte de la siguiente

información:

- Estado:
  Indica si el estado de la regla está habilitado o deshabilitado (campo obligatorio).

- Tipo de Dispositivo:
  Puede tener los valores USB o FireWire.

- ID del Proveedor:
  Es el número de identificación del proveedor del dispositivo.

- ID del Producto:
  Código de producto del dispositivo.

- Serial:
  Número del serial del dispositivo. Digite este número si desea asignar los parámetros a un dispositivo, de lo contrario deje el campo en blanco.

- Registro:
  Este parámetro está disponible solo para dispositivos USB. Los posibles valores son:

- Todo: La regla aplica para todos los dispositivos
- Registrado: La regla aplica solo para dispositivos registrados por un administrador.
- De Confianza: La regla aplica solo para dispositivos registrados por un administrador y que no han sido modificados desde una máquina no protegida por Aranda 360.

- Descripción:
  Puede añadir un comentario sobre el dispositivo (opcional).

  Puede utilizar un comodín para crear una regla que incluya cualquier dispositivo USB o FireWire.
  Para ello, en la ventana del dispositivo (área B), configure todos los campos con el valor * excepto el ID del Serial , el cual debe dejarse en blanco.

  Esta información puede ser agregada manualmente o mediante la detección automática de dispositivos.

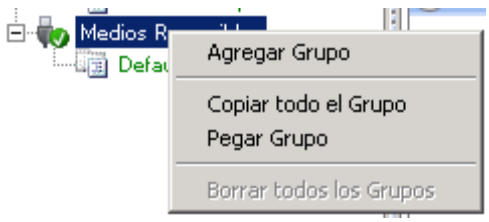
Procedimiento

Existen dos formas de controlar los dispositivos extraíbles en la consola:

- Desde Configuración General > Control de Dispositivos en el Editor de Políticas de Seguridad.
- Desde Categoría de Dispositivos Extraíbles mediante la creación de un grupo de dispositivos.

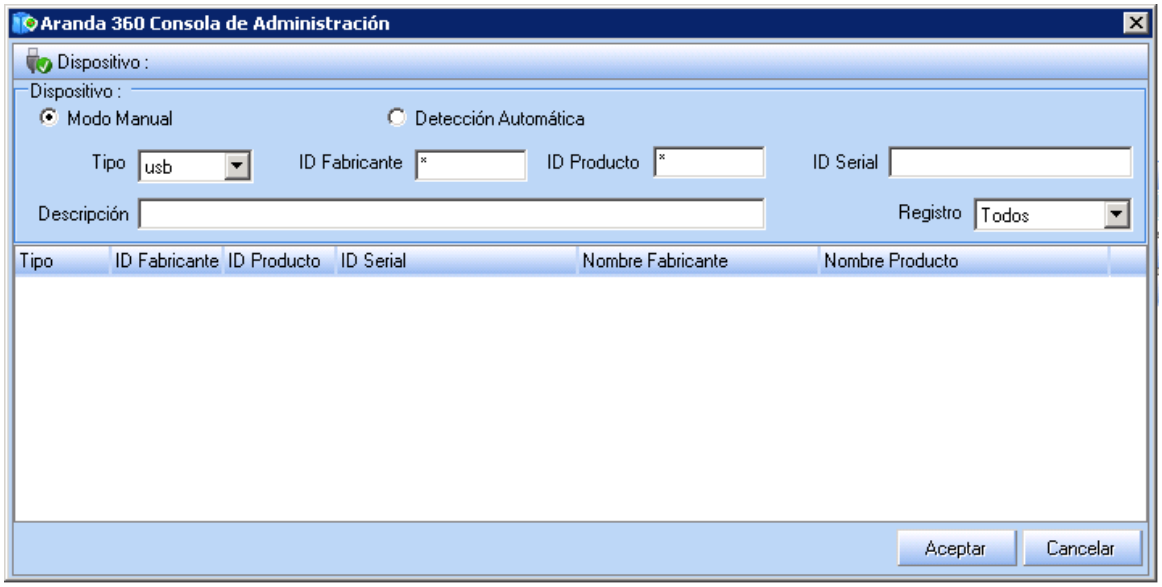
Para controlar el uso de dispositivos extraíbles mediante la creación de un grupo, siga los siguientes pasos:

1. En Categorías, haga clic derecho en Dispositivos Extraíbles y clic en Adicionar Grupo.



   Para cambiar el nombre del grupo por defecto:
   - Seleccione el nombre.
   - Presione F2.
   - Introduzca un nuevo nombre

2. En Configuración de grupos, seleccione la Auditoría y configuración de acceso que desea aplicar a todo el grupo de dispositivos.
3. Haga + clic en. Se visualizará la ventana de Dispositivos:

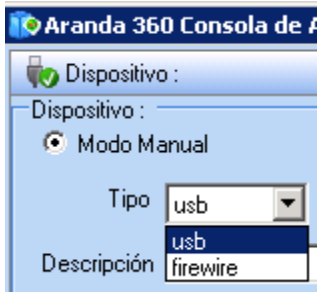


4. Agregue un dispositivo a la lista de forma manual o automática. Para ello, haga clic en la opción de preferencia Modo Manual o Detección Automática. Repita la operación con cada dispositivo.

   Si seleccionó Detección automática, tiene que conectar cada dispositivo que desee agregar.

   - Dependiendo de cómo quiere utilizar el grupo de dispositivos, es posible que no quiera proporcionar información específica por cada categoría.
     Por ejemplo, es posible que desee incluir todos los dispositivos a partir de un único proveedor.
     En ese caso, no se incluirá el ID del Serial.

- Si escogió el modo manual, siga los siguientes pasos:
  - En el campo Tipo, seleccione USB o FireWire en el menú desplegable



- Introduzca la siguiente información según sea el caso:
  - ID del proveedor.
  - ID del producto.
  - Serial.
  - Descripción.

- Registro.

- Si escogió Detección Automática, seleccione USB o FireWire en el menú desplegable.
  Aranda 360 detectará cualquier dispositivo que esté conectado al puerto USB y lo agregará al grupo.
  La ventana de dispositivos se actualizará automáticamente mostrando la nueva información.
  El nuevo dispositivo es seleccionado automáticamente. Puede quitar la selección haciendo clic en él.
  Si es necesario, puede eliminar cualquier dispositivo del grupo.
  5. Introduzca una descripción (opcional).
  6. Haga clic en OK.
     El dispositivo extraíble se agregará al grupo..
  7. Edite la información del dispositivo, si es necesario..
  8. Cree una lista de excepciones de archivos (opcional).

Excepciones por extensión de archivo

Generalidades

Puede especificar excepciones a la configuración predeterminada del grupo. Estas excepciones se basan en las extensiones de los archivos

Por ejemplo, los permisos de acceso por defecto de los grupos se puede configurar como Denegado, pero puede permitir que los archivos con extensión txt, rtf, jpg, etc. puedan tener permisos de solo lectura en Excepciones (área C) configurando el respectivo campo.

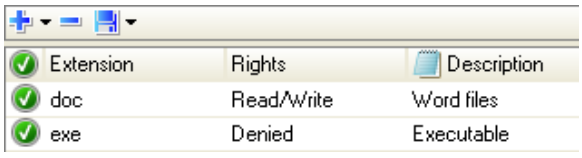


Fig. 8.25: Dispositivos Extraíbles: Excepciones por Extensión

Este parámetro puede tomar los siguientes valores:

- Denegado:
  Si un usuario intenta leer o escribir en un archivo cuyo acceso está denegado (el cual está almacenado en un dispositivo correspondiente al grupo), la acción será bloqueada, incluso si los permisos de acceso del grupo están establecidos como Lectura/Escritura o solo lectura.

- Lectura:
  El usuario puede leer archivos "excluidos" de los dispositivos, incluso si los permisos de accesos están establecidos como Denegado.

- Lectura/Escritura:
  El usuario puede leer y escribir archivos "excluidos" de los dispositivos, incluso si los permisos de accesos están establecidos como Denegado.

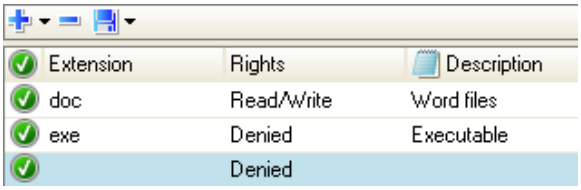
    - Las excepciones por extensión de archivos aplican para todos los dispositivos en el grupo.

Procedimiento

Para crear una lista de excepciones por extensión de archivo, siga los siguientes pasos:

1. En Dispositivos Extraíbles, Haga clic en para agregar una regla.

   Por defecto, Los permisos están denegados.



2. Haga doble clic en la columna Extensión.
3. Digite una extensión de archivo (ejemplo: doc.).

   Para agregar una extensión, sólo tiene que introducir los caracteres que lo indiquen. No es necesario el uso de comodines. Por ejemplo, no es necesario introducir *. doc, doc es suficiente.
4. En la columna Permisos, seleccione los permisos asignados a la extensión del archivo.
5. Escriba una Descripción (opcional).

Ejemplos

Los siguientes ejemplos ilustran cómo pueden utilizarse las políticas de los grupos de dispositivos para aplicar los estándares de la compañía.

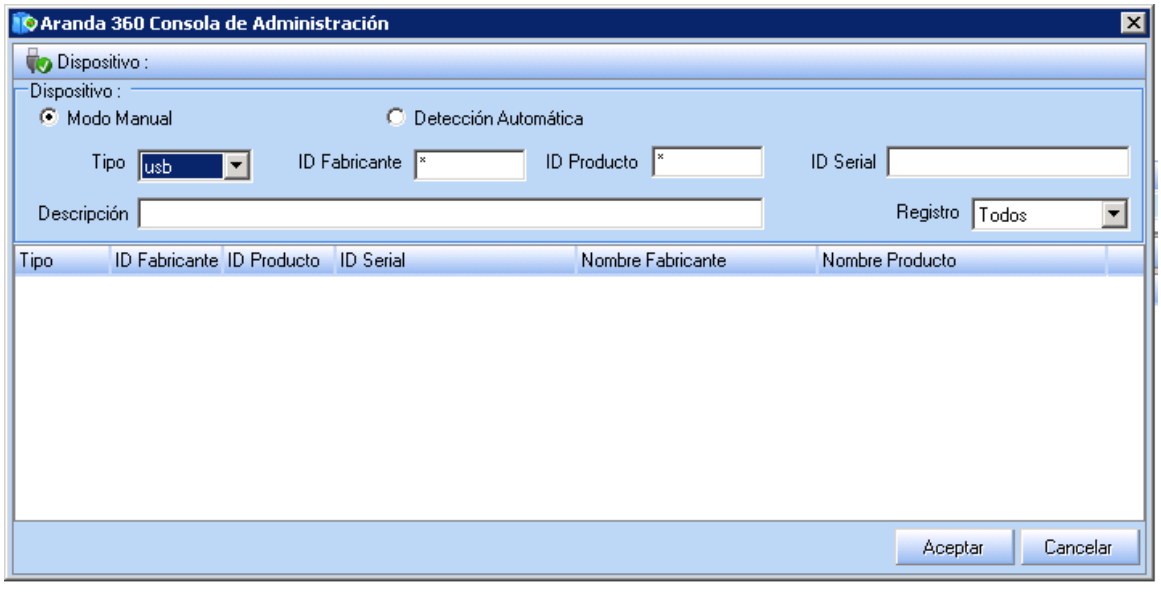
Ejemplo 1

En este ejemplo, una regla "Acceso Mínimo " es creada para controlar cualquier dispositivo que no está especificado en otra regla.

El Ejemplo 1 es el más restrictivo.

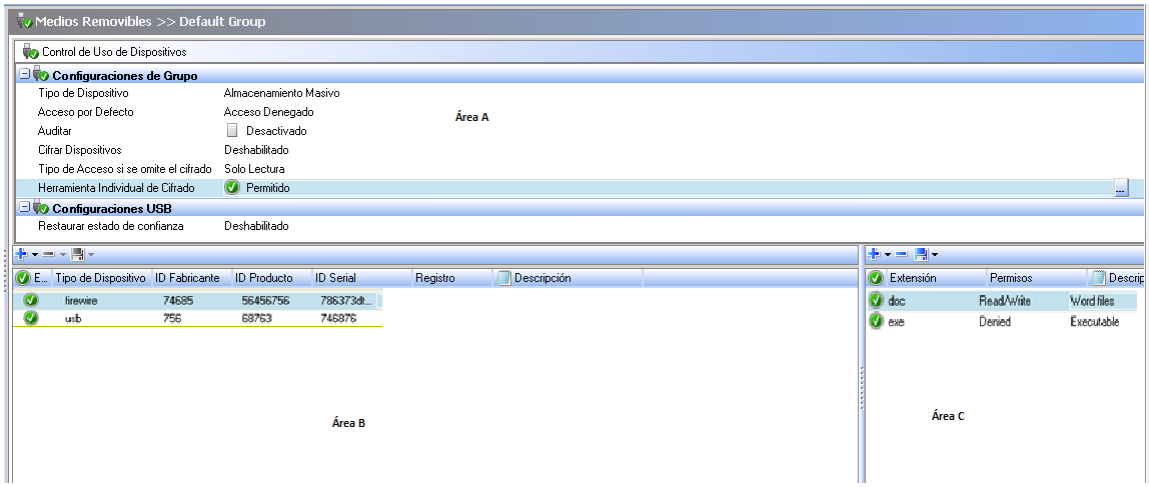
Este grupo no permite el acceso a todos los dispositivos mientras que las excepciones de los archivos permiten acceso de Lectura/Escritura a Microsoft Word, Excel y PowerPoint.

1. Configure el acceso al grupo a Denegado.
2. Haga clic en para añadir una regla.
3. En la ventana de Dispositivos, Cree un grupo de dispositivos USB:
    - Seleccione el modo manual.
    - Establezca Tipo en USB.
    - Digite 0 en el ID del proveedor y del producto.
    - Deje el Serial en blanco. Actúa como un comodín.
    - El resultado final es que todos los dispositivos estarán bloqueados por defecto.
    - Introduzca una Descripción (opcional).
    - Haga clic en OK.



4. Repita el paso 3 para crear un grupo de dispositivos FireWire.
5. Establecer los permisos para los archivos "excluidos" archivos (doc, xls and ppt).

6. La configuración debe ser similar a este ejemplo.



Ejemplo 2

En este ejemplo, un grupo "VIP" es creado para manejar ciertos dispositivos utilizados por funcionarios de alto rango en la empresa.
El acceso es restringido, pero los dispositivos son especificados individualmente.
ID de Proveedores, productos y seriales se incluyen para que sólo los dispositivos identificados puedan ser utilizados. El serial es muy importante para especificar un dispositivo único.

- Un dispositivo no identificado será manejado en el grupo " Acceso Mínimo " creado en el Ejemplo 1

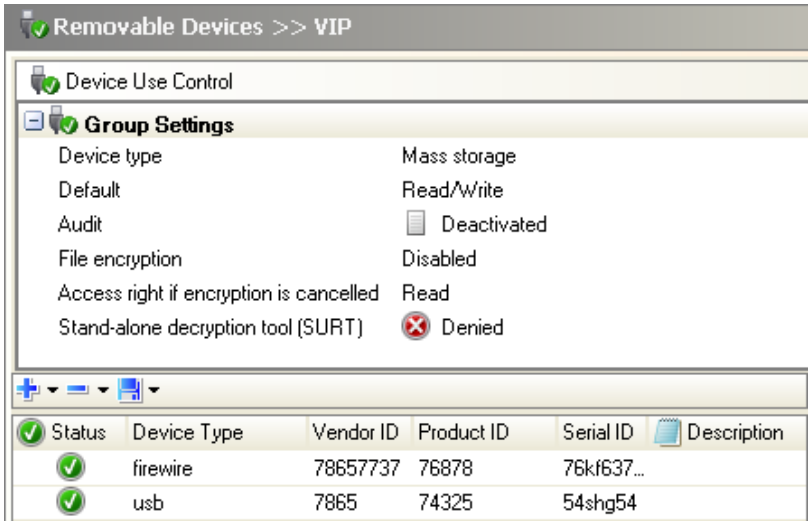
Para realizar este ejemplo, siga los siguientes pasos:

1. Configure el acceso a Lectura/Escritura.
2. Haga clic en para agregar una regla a los dispositivos USB.
   - Defina la configuración para:
     - Tipo.
     - ID del proveedor.
     - ID del Producto.
     - Serial.
     - Descripción (opcional).
   - Haga clic en OK.

3. Repita el paso 2 para agregar una regla a dispositivos FireWire.

- En este ejemplo, se dan permisos de lectura / escritura a todos los dispositivos Esa es la razón por la que es muy recomendable diligenciar los campos informativos - en especial el campo serial -

4. La configuración debe ser similar a esta:



Ejemplo 3

En este ejemplo, se crea el grupo “Empleado”.

El acceso es:

- Menos restringido que en el grupo "Acceso Mínimo" del Ejemplo 1.
- Más restringido que en el grupo “VIP” del Ejemplo 2.

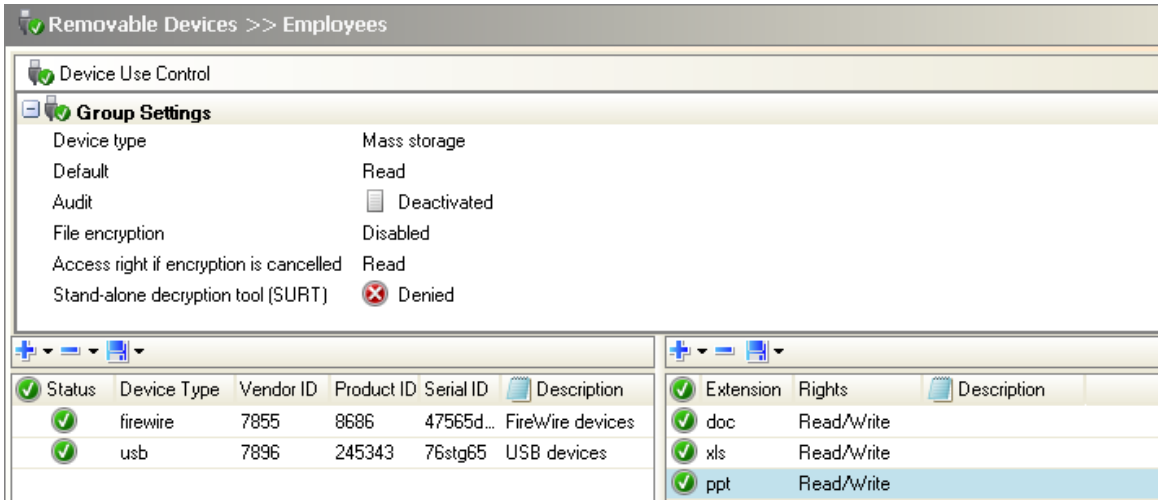
El grupo "Empleado" no muestra los dispositivos individualmente sino por grupos. Esto es de gran utilidad para restringir los dispositivos que usan un particular ID de proveedor y producto.

El acceso por defecto, la configuración de la auditoría, y las excepciones a los archivos aplicarán a cualquier dispositivo que coincida con el ID del proveedor y producto de alguno de los dispositivos registrados.

Para realizar este ejemplo, siga los siguientes pasos:

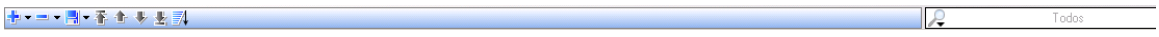
1. Define acceso de solo lectura.
2. Haga clic en +para adicionar una regla.
3. En la ventana de dispositivos, cree un grupo:
   - Seleccione el modo de detección: Modo Manual
   - Detección Automática.Seleccione el tipo de dispositivo: USB o FireWire.
   - Configure los siguientes parámetros:
     - Tipo de Dispositivo.
     - ID del proveedor.
     - ID del producto.
     - Descripción es opcional.
   - Dejar el serial en blanco.
   - Haga clic OK.

4. La configuración debe ser similar a esta:



ADMINISTRADOR DE REGLAS

La barra de herramientas es utilizada para:



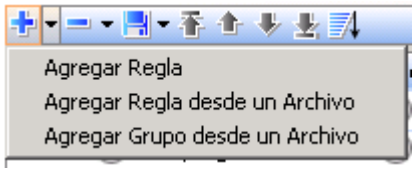
- Adicionar
- Importar
- Eliminar
- Guardar
- Ordenar reglas.

El campo de búsqueda es utilizado para reducir desplazamiento en la lista

ADICIONANDO UNA REGLA

Para adicionar una regla, siga los siguientes pasos:

- Haga clic en o Para mostrar el menú desplegable.
- En segundo lugar, Haga clic en Adicionar Regla.



- Defina la configuración de la regla.

IMPORTANDO UNA REGLA

Para importar una regla, siga los siguientes pasos:

- Haga  clic en para mostrar el menú desplegable
- Seleccione Importar Regla.
  Se abrirá una ventana de búsqueda para seleccionar el archivo de la regla.

IMPORTANDO UN GRUPO DE REGLAS

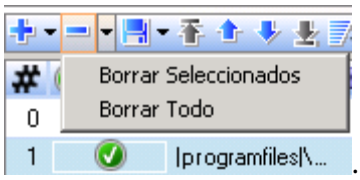
Para adicionar un grupo, siga los siguientes pasos:

- Haga  clic en para mostrar el menú desplegable.
- Seleccione Importar Grupo.
  Se abrirá una ventana de búsqueda para seleccionar el archivo del grupo.

ELIMINANDO UNA REGLA

Para eliminar una regla, siga los siguientes pasos:

- Seleccione la regla a eliminar.
- Haga clic en para eliminar la regla directamente o clic en para mostrar el menú desplegable



- En segundo lugar, haga clic en Eliminar Selección o Eliminar Todo para remover todos los grupos

> Para eliminar más de una regla al tiempo, presione la tecla Ctrl mientas hace clic en las reglas seleccionadas.

CONFIGURANDO UN ORDEN DE PRIORIDAD PARA LAS REGLAS

Existen tres botones para configurar el orden de las reglas:

- Haga clic en o en para cambiar el rango de la regla seleccionado.
- Haga clic en o en para establecer el orden de la regla en la lista.
- Haga clic en para ordenar automáticamente las reglas, de acuerdo a:
  - Ruta completa.
  - Ruta completa incluyendo variables de ambiente.
  - Ruta completa sin variables de ambiente, finalizando con un *.
  - Ruta completa incluyendo variables de ambiente, finalizando con un *.
  - Ruta comenzando con un *.

> Es recomendable utilizar cuando existe una gran cantidad de reglas a ser ordenadas.

HABILITANDO/DESHABILITANDO UN GRUPO DE REGLAS

Para habilitar o deshabilitar un grupo, siga los siguientes pasos:

- Haga clic derecho en el grupo seleccionado
- Seleccione Deshabilitar/Habilitar en el menú desplegable.

Para deshabilitar un grupo de reglas, que está guardado en la configuración, sin perder su aplicación, haga clic en el grupo y seleccione Deshabilitar. Para deshabilitar una regla, haga doble clic sobre la regla en la respectiva columna.

MOSTRANDO MAS DETALLES DE LAS REGLAS

Esta opción sólo aplica para la barra de herramientas del firewall. Se puede acceder a los atributos adicionales hacienda clic en .

MANEJANDO CONFLICTOS ENTRE REGLAS

ORDEN DE PRIORIDAD PARA LAS REGLAS

El orden para evaluar reglas depende de la definición realizada por el Administrador, la categoría de norma y su foco de acción.

La secuencia de verificación para las categorías es la siguiente:

1. Reglas de confianza.
2. Reglas de extensión.
3. Reglas de aplicación.

- Simplemente definiendo una regla para una aplicación en particular, se libera de las demás reglas aplicables a un conjunto de aplicaciones, en cuanto a:
  - Entorno de red.
  - Archivos.
  - Registros.

EJEMPLOS

A continuación, tres ejemplos de cómo los conflictos entre las reglas son manejados.

Ejemplo 1

Consideremos la siguiente situación:

- Ninguna aplicación (*.exe) está autorizada para acceder a archivos (*.txt).
- Windows Notepad (*\notepad.exe) está autorizado para acceder a archivos (*.txt)

En este caso, la segunda regla tiene la mayor prioridad, ya que es la más específica. Por lo tanto, es posible abrir un archivo de texto usando el Bloc de notas.

Ejemplo 2

Consideremos la siguiente situación:

- Ninguna aplicación (*.exe) está autorizada para acceder a archivos (*.txt).
- Internet Explorer está autorizada para acceder a la red utilizando ciertos puertos.

La regla de Internet Explorer toma procedencia sobre la regla genérica. No existe conflicto, ya que el campo de acción de las dos reglas es diferente:

- La primera regla aplica para archivos.
- La segunda regla aplica para acceso a red.

Ejemplo 3

Consideremos la siguiente situación

- Ninguna aplicación (*.exe) está autorizada para acceder a archivos (*.txt).
- Internet Explorer no está autorizado para acceder a archivos MP3 (*.mp3).

La regla de Internet Explorer toma procedencia sobre la regla genérica, esta aplicación tiene permisos para abrir archivos de texto.

Para evitar este comportamiento, es necesario especificar ambas reglas de acción (.txt y .mp3) para esta aplicación.

CONVENCIONES DE ESCRITURA

APPLICATION ENTRY FORMAT

La ruta completa de la aplicación puede ser especificada. Uno o varios comodines * también pueden ser usados.

Ejemplo 1

Un ejemplo de una aplicación identificada por la ruta completa:

C:\program files\Internet Explorer\iexplore.exe

Ejemplo 2

En este ejemplo muestra cómo identificar una aplicación independientemente de la unidad donde se encuentra o su ruta de acceso:

*:\program files\Internet Explorer\iexplore.exe

*\iexplore.exe

VARIABLES DE AMBIENTE

Existen tres variables de ambiente utilizadas para especificar las reglas independientemente de las diferencias de nomenclatura y organización correspondiente a los directorios del sistema de Windows.

Estas variables se definen mediante separadores (|), al principio o al final de la cadena:

|programfiles|

Este es el directorio de instalación predeterminado para las aplicaciones. Normalmente es:

c:\program files

|systemdrive|

Esta es la raíz de la unidad donde está instalado el sistema. Normalmente es:

c:\

|systemroot|

Este es el directorio principal del sistema operativo. Para Windows XP, normalmente es:

c:\windows

PLANTILLAS DE CONFIGURACIÓN

GENERALDADES

Aranda 360 incluye plantillas básicas de políticas y un conjunto de paquetes predefinidos que pueden ser usados para agilizar la implementación de políticas.

Estas plantillas están diseñadas para ser mejorada con el tiempo. Por lo tanto, sólo proporcionará referencias a algunas configuraciones básicas.

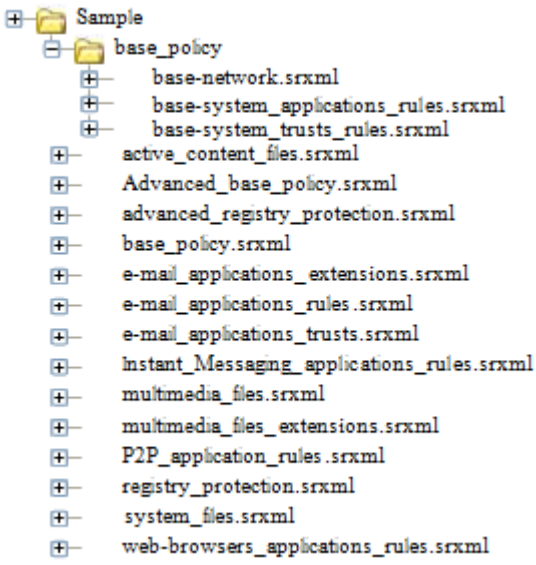
Antes de implementar estas configuraciones, consulte con su distribuidor o en la extranet de Aranda Systems (http://extranet.Aranda.fr) para obtener nuevas plantillas.

GRUPOS PREDEFINIDOS Y REGLAS DE CONFIGURACIÓN

Los siguientes son algunos de los grupos y reglas de configuración predefinidas suministrado con Aranda 360 6,0 (además de los ya incluidos en la configuración base).

Son instalados de forma predeterminada en la carpeta Sample en:

C:\Program Files\Aranda\Aranda Management Console\



Políticas Base

Aranda 360 incluye varias plantillas de políticas base. Éstas son utilizadas como una plantilla de inicio rápido para la construcción de propias políticas.

Las políticas base incluyen varias reglas de red y del sistema para prevenir bloqueos de operaciones básicas de Windows.

Cuando la configuración de las reglas está completa, se debe aumentar los niveles de seguridad de Protección Automática en Configuración General.

Las políticas base están compuestas por los siguientes archivos:

- base_policy.srxml:
  Ejemplo de una política base para una estación de trabajo estándar.

- advanced_base_policy.srxml:
  Ejemplo de una política base reforzada para una estación de trabajo estándar.

La carpeta Sample también contiene una carpeta base_policy, la cual incluye tres archivos:

- base-network.srxml:
  Ejemplo de reglas de firewall para una estación de trabajo estándar.

- base-system_applications_rules.srxml:
  Ejemplo de reglas de aplicación para una estación de trabajo estándar.

- base-system_trusts_rules.srxml:
  Ejemplo de reglas de confianza para una estación de trabajo estándar.

Reglas de Aplicación

Las reglas de aplicaciones predefinidas son:

- Reglas para la protección de Outlook, Outlook Express y Thunderbird (previniendo la ejecución de código anormal, filtrado de red, protección de las libretas de direcciones
  - e-mail_applications_rules.srxml: Reglas de Aplicación.
  - e-mail_applications_extensions.srxml: Reglas de extensión.
  - e-mail_applications_trusts.srxml: Reglas de confianza.

- Reglas para la protección de Internet Explorer y Firefox (filtro de red, Bloqueo de apertura de archivos ejecutables):
  - web-browsers_application_rules.srxml: Reglas de aplicación.

- Grupo de reglas para el bloqueo de aplicaciones P2P (listas negras):
  - P2P_application_rules.srxml:
    Reglas de Aplicación

- Grupo de reglas para el bloqueo de aplicaciones de mensajería instantánea(blacklist):
  - Instant_Messaging_applications_rules.srxml: Reglas de Aplicación.

- Grupo de reglas para el bloqueo de archivos multimedia en el sistema:
  - multimedia_files_extensions.srxml: Reglas de Extensión.

- Reglas para la protección del usuario y el registro de la máquina:
  - registry_protection.srxml:
    Lista de claves de registro para reglas de aplicación.
- advanced_registry_protection.srxml:
  Lista de claves de registro avanzadas para reglas de aplicación.
- Reglas para archivos protegidos del sistema:
  - system_files.srxml.

Lista de objetos predefinidos

Aranda 360 ofrece dos listas de tipos de archivos que son útiles para las listas negras. Estas listas son incluidas en los siguientes archivos:

- multimedia_files.srxml:
  Lista de las principales extensiones de archivos multimedia, audio y video.
- active_content_files.srxml
- Lista de las principales extensiones de archivos ejecutables.

Capítulo 9 - ADMINISTRACIÓN DE DISPOSITIVOS EXTRAIBLES

ACERCA DE ESTE CAPÍTULO

Este capítulo describe la administración y registro de dispositivos extraíbles.

Contiene lo siguiente:

- Generalidades
- Preparación para el registro del dispositivo extraíble
- Delegación de la administración e dispositivos extraíbles
    - Generalidades
    - Permisos
    - Consulta de dispositivos registrados
        - Selección de dispositivos
        - Directorio
        - Historial de eventos
- Registro de dispositivos y revocación

GENERALIDADES

Aranda 360 permite registrar dispositivos extraíbles utilizados en las estaciones de trabajo de la organización con el fin de controlarlos. Garantiza la seguridad en la máquina, a la cual está conectado el dispositivo y facilita la administración de los dispositivos.

Un dispositivo extraíble registrado es identificado como único y es configurado por la herramienta de administración de dispositivos. Debe estar asociado a un único usuario, quien es el propietario.

Un dispositivo registrado es “de confianza”, siempre y cuando su contenido no ha sido modificado fuera del entorno de la organización. Se puede utilizar en cualquier estación de trabajo del entorno de seguridad. Si alguna modificación es detectada, es posible configurar un control de antivirus en el dispositivo para ser considerado “de confianza” de nuevo.

Un agente de control instalado en cada estación de trabajo y en el servidor permite sólo el acceso a dispositivos extraíbles registrados que cumplan con los controles definidos en las políticas de seguridad.

- Un dispositivo registrado no puede ser cifrado.

PREPARACIÓN DEL REGISTRO DE DISPOSTIVOS EXTRAIBLES

Llave	Valor
enrollment-organizationGuid	El valor de esta propiedad debe ser específico a la organización. El formato del identificador es xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxx donde x es un dígito hexadecimal.
enrollment-IdapGuidAttribute	Esta propiedad contiene el nombre del atributo LDAP incluyendo los usuarios GUID. El valor por defecto es objectguid.
enrollment-IdapBaseDN	Esta propiedad define la ramificación del directorio donde los usuarios están buscando. De forma predeterminada, es la raíz del Directorio Activo.
enrollment-IdapServer	Esta propiedad contiene la dirección y el puerto del servidor LDAP El Directorio Activo actual es utilizado por defecto.
enrollment- IdapUser	El inicio de sesión es utilizado para autenticar y buscar usuarios en el directorio. Esta propiedad puede estar vacía cuando una conexión de directorio activo o anónimo es usada.
enrollment- IdapPwd	Esta propiedad contiene la contraseña de conexión al directorio. Esta propiedad contiene la contraseña de conexión al directorio.
enrollment-IdapAuthType	Los posibles valores para esta propiedad son Anónimo para una conexión anónima, Básica o implícita para un directorio LDAP clásico, y Acordar para un directorio activo
enrollment-IdapUserFilter	Esta propiedad contiene el filtro LDAP para listar los usuarios del directorio. El filtro por defecto corresponde a los usuarios habilitados del Directorio Activo. (&(!(useraccountcontrol:1.2.840.113556.1.4.803:=2))(objectcategory=person)) para un directorio LDAP clásico, el filtro puede ser (objectclass=inetorgperson).

Llave	Valor
enrollment-ldapAutoComplet eFilter	El filtro LDAP es usado cuando se completa automáticamente el nombre de un usuario. El valor por defecto es (cn={0}*). El atributo utilizado como usuarios RDN debe ser usado. Este filtro puede ser sustituido por (uid={0}*) por ejemplo.
enrollment-ldapAdministratorFilter	Esta propiedad contiene el filtro LDAP habilitado para encontrar la cuenta LDAP del administrador conectado a la consola desde su identificador Aranda 360. El valor por defecto es (&(userprincipalname={0}@*)(objectcategory=person)). Se recomienda nombrar los usuarios Aranda 360 con el mismo nombre de cuenta del directorio. En algunos repositorios LDAP repositorios, el valor puede ser (&(uid={0})(objectclass=inetorgperson)).
enrollment-ldapSearchUserFilter	Esta propiedad contiene el filtro LDAP utilizado por la consola para búsqueda avanzada de nombres. Puede ser aplicado a todos los atributos que contengan una parte del nombre del usuario buscado. El valor por defecto es (l(cn=*{0}*)(displayname=*{0}*)(mail=*{0}*)).
enrollment-ldapSearchDepartmentFilter	Esta propiedad es utilizada como un filtro LDAP por la consola para búsqueda avanzada de nombres. Puede ser aplicado a todos los atributos que contengan una parte del servicio o sitio del usuario buscado.. El valor por defecto es (l(ou=*{0}*)(department=*{0}*)(l=*{0}*)).

Para modificar estas propiedades, debe editar la tabla [db_properties] de la configuración de Aranda 360 con la ayuda de un cliente SQL Server como sqlcmd o SQL Management Studio.

DELEGACIÓN DE LA ADMINISTRACIÓN DE DISPOSITIVOS EXTRAIBLES

GENERALIDADES

Si una política de seguridad es aplicada a varios dispositivos, puede ser tedioso estar agregando nuevos dispositivos. Es necesario implementar una nueva configuración al modificar la lista de dispositivos.

Con el fin de simplificar estos escenarios, las reglas de las políticas de seguridad se basan en registro del dispositivo. El estado es uno de los valores de configuración de las reglas.

La consola permite asignar un estado a un dispositivo. La configuración de los agentes no depende del estado de los dispositivos. Las ventajas son las siguientes:

- Los administradores de Aranda 360 que tienen funciones de administración de registro no tiene que ser los mismos que modifican la configuración del agente.
  El número de administradores de registro puede ser mucho mayor que el número de administradores de los agentes.

- El estado de un mismo dispositivo puede cambiar. Un dispositivo se considera de confianza, si sólo se utiliza en la red de la organización. Se puede perder esta condición si se modifica en una estación de trabajo que no esté en la red.

- El propietario sabe cuándo registrar el dispositivo. Los registros generados por el agente mencionan el nombre del propietario.

La instalación de Aranda 360 puede ser personalizada como se describe en la sección “preparación del registro del dispositivo extraíble ” , página 321 para usar la función de registro..

La delegación de administración de dispositivos es detallada en las siguientes secciones.

PERMISOS DE ADMINISTRACIÓN DE DISPOSITIVOS

La administración de dispositivos se divide en dos opciones. Cada una es controlado por un permiso especifico en la ventana de administración de roles.

View enrolled devices	☑	View enrolled devices and their owners
Enrolled devices management	☑	Enroll or revoke devices

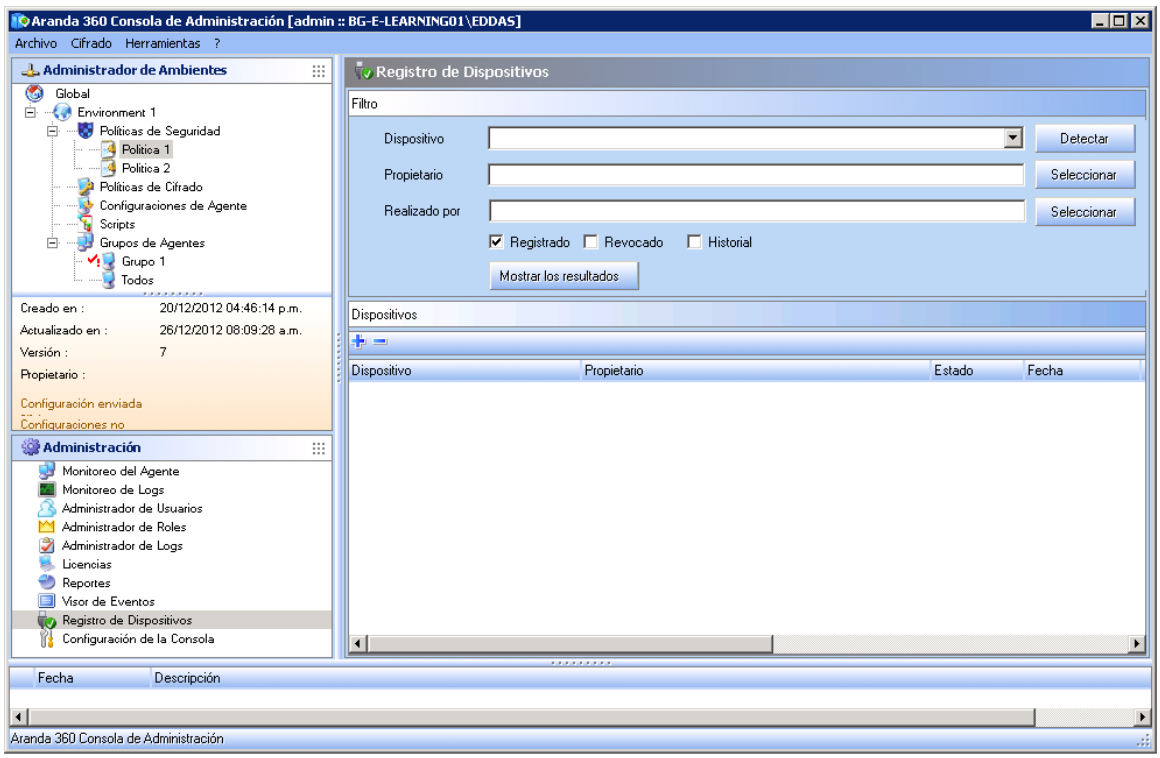
La opción Ver dispositivos registrados es obligatoria para todos los administradores de dispositivos. Se permite consultar el estado de registro actual, para encontrar los dispositivos asociados a una persona y ver el historial de las acciones realizadas. Es un acceso de sólo lectura.

La opción Administración de Dispositivos Registrados permite a los administradores inscribir o revocar un dispositivo. El alcance de los administradores incluye todos los dispositivos y propietarios.

No es posible limitar la administración de los dispositivos registrados para un segmento de la organización. Sin embargo, todas las acciones de administración son monitoreadas y es posible auditar las operaciones del administrador.

CONSULTA DE DISPOSITIVOS REGISTRADOS

Todas las funciones de administración de dispositivos se encuentran en la ventana de Registro de Dispositivos.

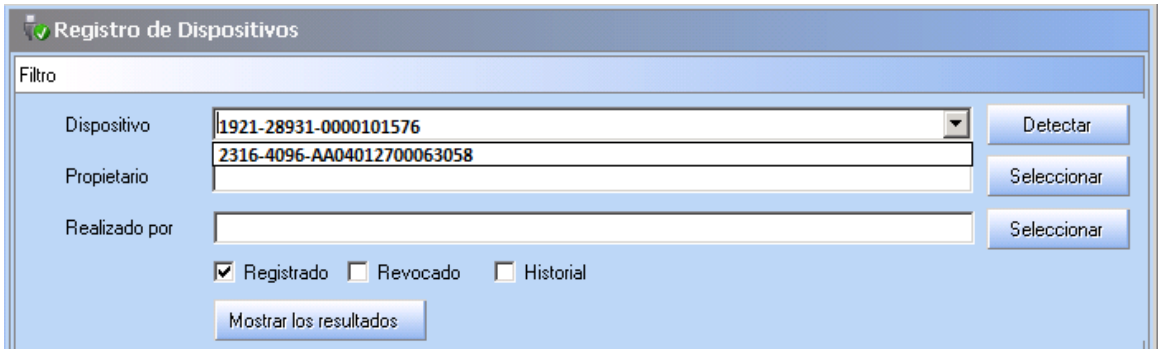


El panel Filtro permite filtrar la lista de dispositivos para consultar el estado de un registro de un dispositivo especifico, una persona en particular, o conocer la lista de operaciones de registro ejecutadas por un administrador de consola.

La lista de dispositivos en el panel inferior detalla los registro y en particular el nombre del administrador, quien registró o revocó el dispositivo.

Selección de Dispositivos

Las ventanas de administración detectan automáticamente los dispositivos conectados a la estación de trabajo.

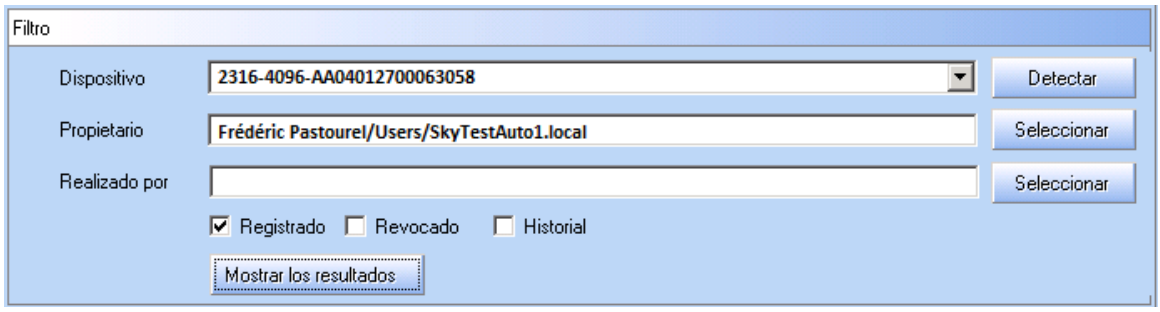


Haga clic en el botón Detectar para mostrar los identificadores de los dispositivos en la lista desplegable respectiva.

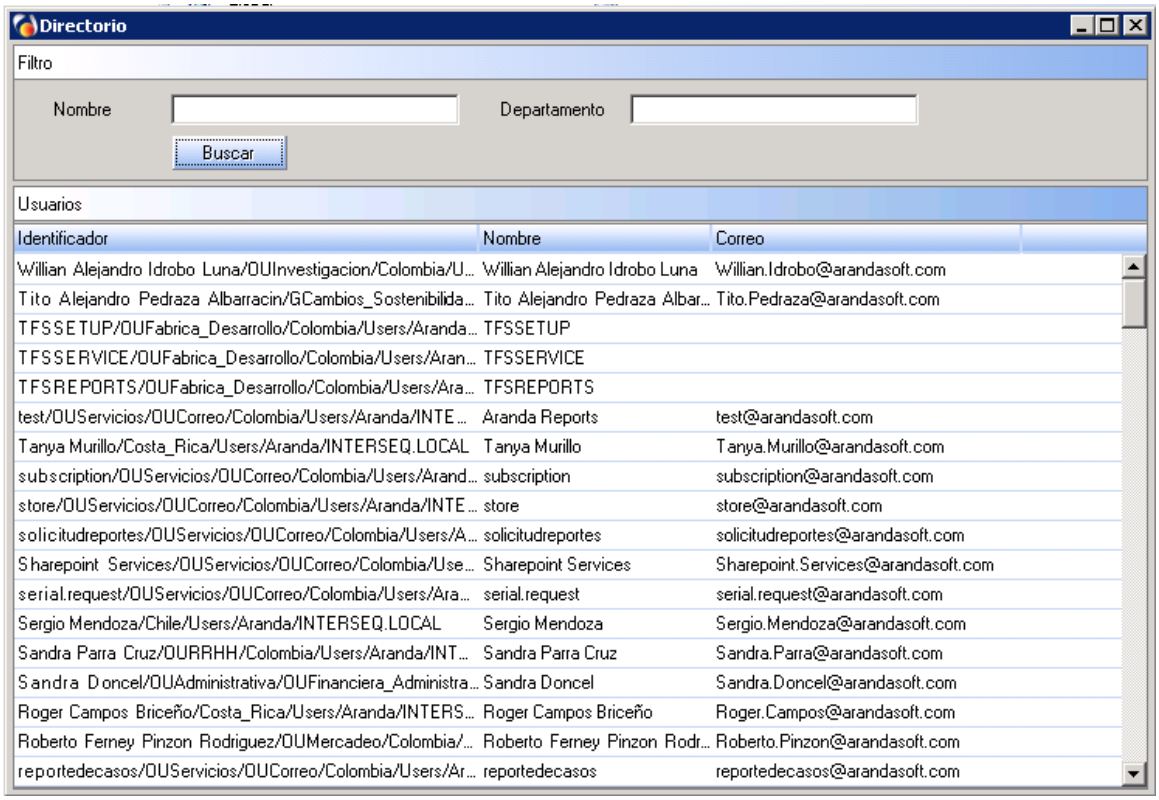
Directorio

En los campos Propietario y Ejecutada por, seleccione el propietario del dispositivo o el administrador, quien ejecutó la operación de registro.

Completando automáticamente los nombres basados en las primeras letras permite una selección rápida.



Si no es posible buscar a una persona por su nombre, haga clic en el botón Seleccionar para abrir el formulario de búsqueda avanzada. Introduzca cualquier carácter del nombre, ubicación o el departamento al que pertenece el empleado para filtrar la lista de usuarios.



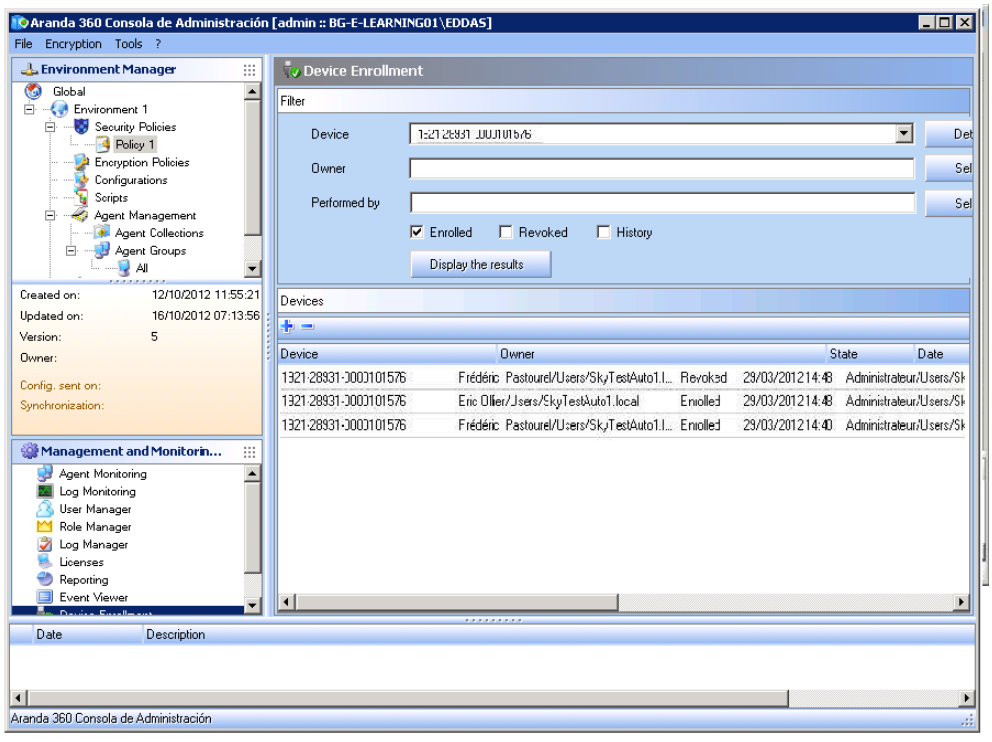
Historial de eventos

Completando automáticamente los nombres basados en las primeras letras permite una selección rápida.

Si no es posible buscar a una persona por su nombre, haga clic en el botón Seleccionar para abrir el formulario de búsqueda avanzada. Introduzca cualquier carácter del nombre, ubicación o el departamento al que pertenece el empleado para filtrar la lista de usuarios.

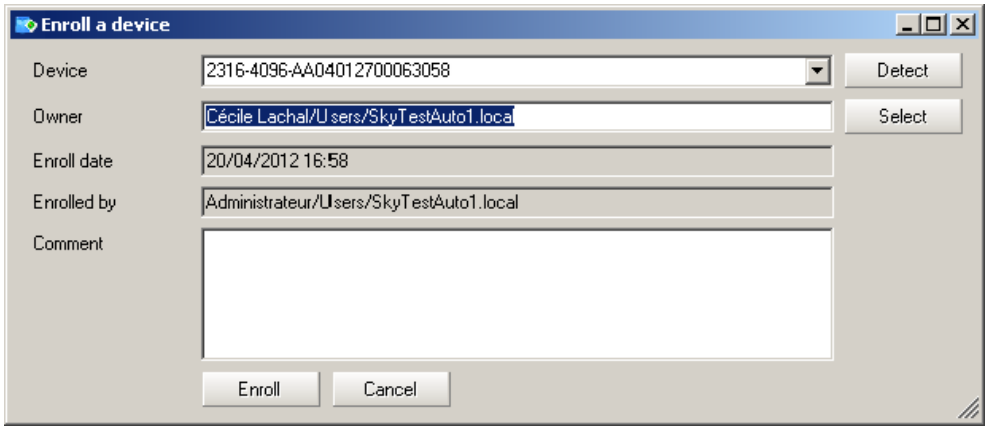
En el panel de Filtro, si la casilla Historial no está marcada, la lista de dispositivos sólo mostrará el estado actual del dispositivo o de la persona seleccionada en el filtro.

Si esta es marcada, listará también los eventos antiguos.

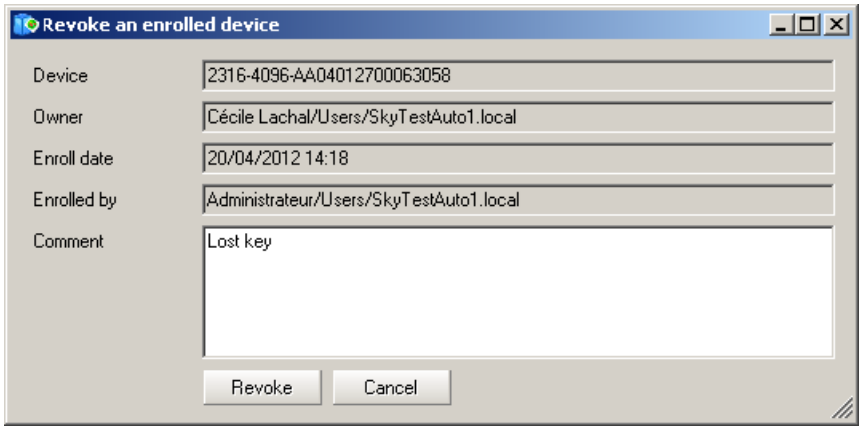


REGISTRO Y REVOCACIÓN DE DISPOSITIVOS

Un administrador puede registrar un dispositivo, para ello haga clic en el icono en el panel principal. Aparecerá una ventana para registrar dispositivos. Puede seleccionar el dispositivo, propietario y escribir un comentario.



Cuando un dispositivo registrado es mostrado en el panel principal, el administrador puede revocarlo, para ello selecciónelo de la lista y haga clic en . Se abrirá una ventana de revocación. Puede ver los detalles del dispositivo y adicionar un comentario acerca de la revocación.



Los eventos de administración son sistemáticamente monitoreados en la base de Aranda 360 y puede ser visto en el historial.

Capítulo 10 - CIFRADO DE DISPOSITIVOS EXTRAIBLES

ACERCA DE ESTE CAPÍTULO

Este capítulo describe el cifrado/descifrado de dispositivos extraíbles. Contiene lo siguiente:

- Generalidades:
    1. Propósito.
    2. Características:
        - Estándar de Cifrado Avanzada.
        - Protección de contraseña.
        - Contraseña de cifrado.
        - Eliminación segura.
    3. Sistemas operativos soportados.
    4. Que puede ser cifrado.
    5. Particiones no cifradas.
    6. Clave de cifrado.
    7. Sincronización.
    8. Simbología.

- Creando una política de cifrado para ser aplicada a un grupo de dispositivos:
    1. Configuración de segundo nivel:
        - Dispositivos extraíbles.
        - Configuración general.

- Conectando un dispositivo extraíble:
    1. Contraseña.
    2. Sincronización.
    3. Acceso al dispositivo sin contraseña.
    4. Acceso a la información cifrada.
    5. Comportamiento al modificar las políticas de cifrado.
    6. Utilizando dispositivos cifrados en otras máquinas:
        - Compartiendo archivos cifrados.
        - Sistemas sin Aranda 360.
        - Otros sistemas ejecutando Aranda 360.
    7. Removiendo tarjetas SD.

- Descifrando un dispositivo extraíble:
    1. Lado administrador.
    2. Lado Agente.

- Contraseñas:
    1. Lado Administrador.
    2. Lado Usuario.

- Reparando una clave cifrada.

GENERALIDADES

PROPÓSITO

Cifrado de dispositivos extraíbles ofrece un nivel adicional de protección mediante cifrado de información almacenada en dispositivos USB o FireWire con una clave protegida por contraseña.

- El cifrado de dispositivos extraíbles no está relacionado con la función de cifrado de Aranda 360.
- Un dispositivo registrado no es posible cifrarlo

Características

Estándar de Cifrado Avanzado

El cifrado proporcionado por Aranda 360 (para dispositivos USB y FireWire) está basado en el estándar de cifrado avanzado (AES).

Este es un sistema de cifrado simétrico que ha sido aprobado por el Gobierno de los EE.UU. para utilizarlo en documentos clasificados y no clasificados.

El tamaño de las claves de cifrado del dispositivo está limitado a 128 bits.

Protección de contraseña

Al proteger con contraseña la información cifrada, la cual esta almacenada en estos dispositivos, la información sensibles de la compañía está protegida contra robos.

Cifrado de contraseña

La contraseña utilizada para abrir los archivos cifrados también está cifrada. Por lo tanto, es tan seguro como el cifrado aplicado en los archivos.

Eliminación Segura

Al cifrar un dispositivo que ya contiene archivos, Aranda 360 genera en primer lugar, una copia cifrada de la información antigua antes de realizar la eliminación. Cuando se crean nuevos archivos en el dispositivo cifrado por Aranda 360, esta operación no es requerida.

Por esta razón, el cifrar un dispositivo que ya contiene archivos tarda más tiempo que la copia de la misma cantidad de información en un dispositivo ya encriptado. El número de pasos necesarios para una eliminación segura depende del tipo de dispositivo: magnético (disco duro externo) o de memoria flash (memoria USB).

SISTEMAS OPERTAIVOS SOPORTADOS

Cifrado USB y FireWire es soportada por

- Windows XP SP3 32bits.
- Windows Vista SP2 32bits.
- Windows 7 32bits.

Los menús relacionados al cifrado de dispositivos están ocultos en los agentes que se instalan en computadores ejecutando sistemas operativos no soportados.

QUE PUEDE SER CIFRADO

Puede optar por cifrar automáticamente todos los dispositivos USB y FireWire.

Para obtener más información, ver " Creando una política de cifrado para ser aplicada a un grupo de dispositivos .

La política de cifrado se aplica a todo el grupo de dispositivos.
La Lista de control de acceso (ACL) definido en Configuración General es aplicada como parte de la política.

PARTICIONES NO CIFRADAS

Para los dispositivos con particiones, es posible omitir una partición para la política de cifrado, tal como discos duros externos, después de que el primer plug-in.

No se solicitará contraseña para una partición no cifrada.

Las Particiones deben ser creadas antes de cifrar..

CLAVE DE CIFRADO

La clave de cifrado se almacena en un archivo llamado SR_ID. en el directorio raíz de claves.

Hay un archivo SR_ID.

Por cada partición. Cada partición puede estar protegida por una contraseña diferente.

El servidor Aranda 360 contiene una copia de la información almacenada en el archivo SR_ID. Si este archivo está dañado en el dispositivo de almacenamiento, una copia de la información es descargada automáticamente desde el servidor con el fin de restaurar el archivo. Esta operación es transparente para el usuario.

Sin embargo, si el servidor no está disponible, el usuario recibirá un mensaje indicando que:

- sr_id. esta corrupto.
- Los archivos cifrados son inaccesibles.

El usuario puede solicitar una nueva clave de cifrado al administrador o reemplazar el SR_ID. El archivo con una copia de seguridad (en caso de que el usuario haya hecho una).

- Para mayor seguridad, el usuario debería realizar una copia de seguridad de la clave de cifrada utilizando la función de exportar en el menú del agente.

SINCRONIZACIÓN

La primera vez que un dispositivo es conectado después de una política de cifrado es aplicada, y se realiza un proceso de sincronización, cifrando todo el dispositivo

Una barra de progreso muestra el estado de la operación.

SIMBOLOGÍA

Una figura de un candado naranja es mostrado en el nivel "Mi PC > Dispositivos con almacenamiento extraíble" indicando que hay al menos un archivo cifrado en el dispositivo.

CREANDO AN POLÍTICAS DE CIFRADO PARA SE APLICADAS A UN GRUPO DE DISPOSITIVOS

CONFIGURACIÓN DE SEGUNDO NIVEL

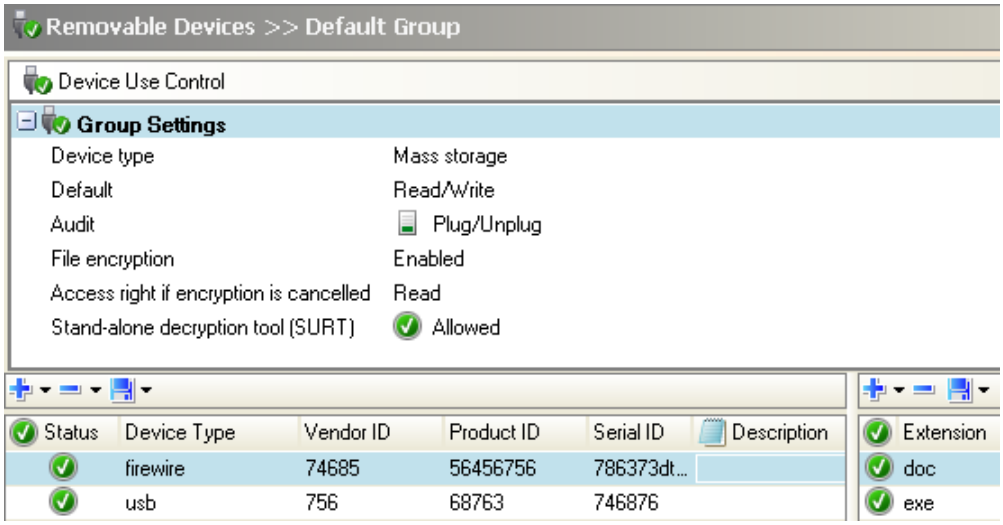
Puede definir el cifrado de dispositivos extraíbles en 2 niveles:

- Dispositivos Extraíbles.
  Para obtener más información, ver " Dispositivos Extraíbles" , página 2 9 4 .

- Configuración General.
- Para obtener más información, ver " Control de Dispositivos ".

Dispositivos Extraíbles

La configuración de cifrado está en Dispositivos Extraíbles> Control de Uso de dispositivos> Configuración del grupo:



- Cifrado de Archivos:
  - Deshabilitado:
    Ningún archivo cifrado.
  - Habilitado:
    Cifra el dispositivo entero o una partición.

- Permisos si el cifrado es cancelado:
  Esta opción habilita:
  - Solo lectura,
  - Lectura/Escritura,
  - Acceso denegado,
    para archivos no cifrados, si el usuario decidió no cifrar el dispositivo cuando se le solicite crear una contraseña de cifrado.

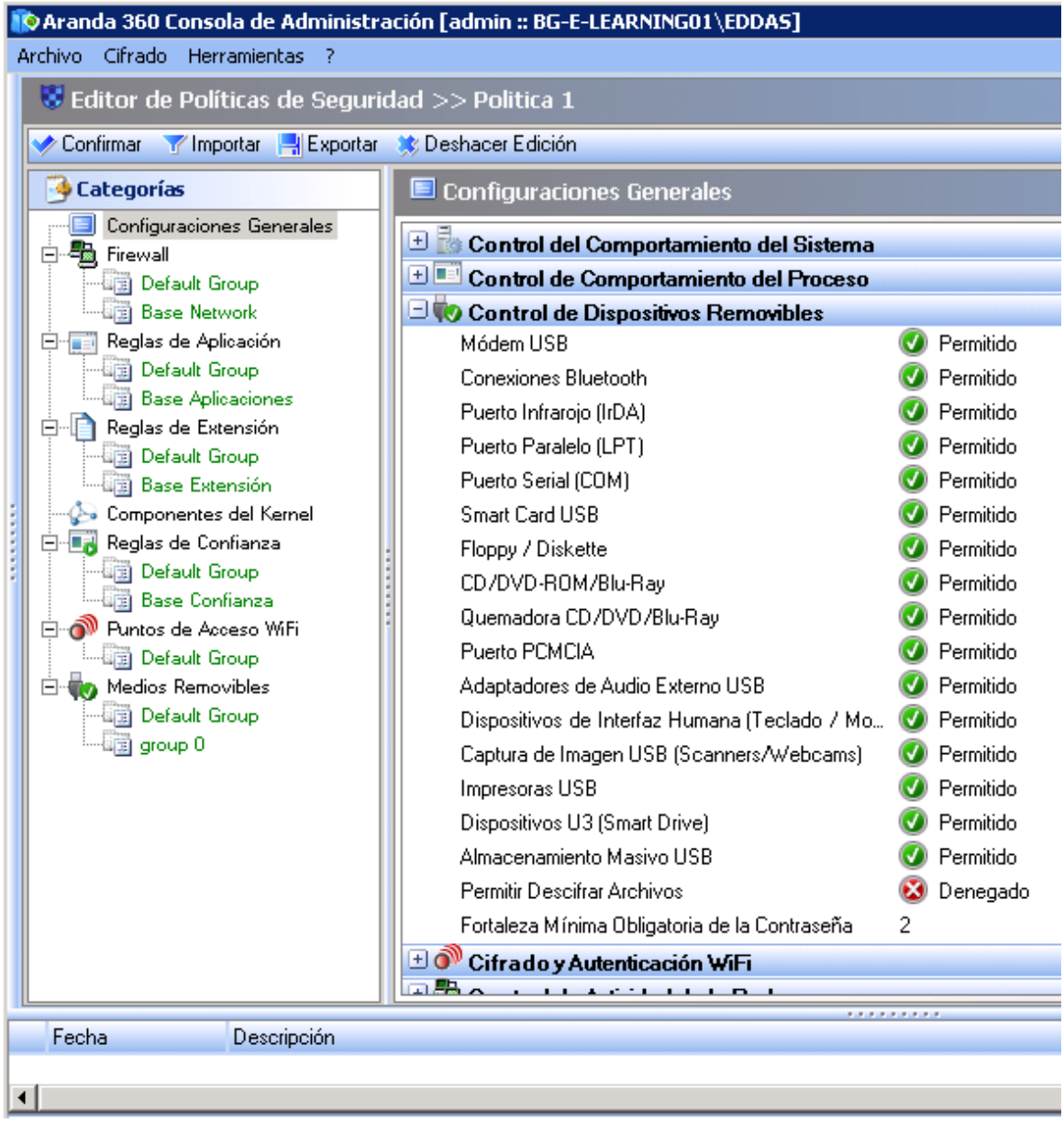
- Herramienta de cifrado stand-alone (SURT):
  Esta opción permite o deniega el uso de la herramienta de cifrado SURT para permitir el descifrado de archivos en sistemas que no usan Aranda 360.

La configuración de cifrado aplica para todos los dispositivos del grupo.

Si el acceso por Defecto al grupo del dispositivo es establecido como Denegado, el dispositivo no será capaz de acceder a la estación de trabajo en la que se encuentra instalado el agente.
El Acceso denegado permanecerá si las políticas de cifrado aplican a los dispositivos.

Configuración General

La configuración del cifrado del dispositivo se encuentra en Configuración General > Control de dispositivos:



- Recuperación de Almacenamiento Masivo
  Esta opción permite o deniega al usuario para descifrar el dispositivo extraíble.

- Seguridad de la contraseña:
  Esta opción define la seguridad de la contraseña utilizada para el cifrado del dispositivo. El valor es establecido en 2 por defecto.

CONUN DISPOSITIVO EXTRAIBLE

CONTRASEÑA

La primera vez que un usuario conecta un dispositivo con una política de cifrado, una ventana, una ventana:

- Se abre.
- Solicitar digitar una nueva contraseña.
- Confirmar la contraseña.

Si un dispositivo USB o FireWire utiliza una política de cifrado, aparecerá una ventana emergente solicitando la contraseña cada vez que se conecta el dispositivo .

La seguridad obligatoria para la contraseña es establecida por el administrador en Configuración General

> Control de Dispositivos.

SINCRONIZACIÓN

La primera vez que un dispositivo con una política de cifrado es conectado, un proceso de sincronización es llevado a cabo para cifrar el dispositivo.

- Durante el proceso de sincronización, el usuario no debe dejar el computador por un periodo largo de tiempo.
  Si el equipo se bloquea automáticamente o entra en modo de Stand-by, el proceso de sincronización se detendrá.
  Entonces, el usuario tendrá que introducir la contraseña de cifrado del dispositivo para relanzar el proceso.

  El Control de acceso de forma predeterminada se omite. Esto significa que todos los archivos en el dispositivo se cifran incluso si el acceso por defecto está establecido en denegado o de sólo lectura.

ACCESO AL DISPOSITIVO SIN CONTRASEÑA

Si al solicitar introducir una contraseña, el usuario hace clic en Cancelar, el dispositivo será bloqueado para evitar que la información no cifrada se escriba en el dispositivo.

En este caso, los permisos dependerán si el cifrado es cancelado en:

Dispositivos Extraíbles > Control de Dispositivos > Configuración de Grupos. Los permisos pueden tener los siguientes valores:

- Solo Lectura.
- Lectura/Escritura.
- Denegado.

Cabe señalar que el acceso predeterminado y excepciones por extensión de archivo también aplican al grupo de dispositivos.
Por lo tanto, si el acceso por defecto para el dispositivo está configurado como Denegado el usuario no podrá acceder al dispositivo.

Si el usuario intenta acceder a un archivo cifrado sin establecer la contraseña, la información contenida en el archivo se mostrará como texto cifrado.

El modo de sólo lectura sólo es válido para esta sesión. La próxima vez que el usuario conecta el dispositivo, la solicitud de contraseña se mostrará de nuevo.

ACCESO A INFORMACIÓN CIFRADA

Mientras la contraseña correcta es entrada, no hay diferencia para el usuario entre la lectura de los datos cifrados y sin cifrar.

La información es cifrada cada vez que se escribe en un dispositivo con cifrado activo. Si un archivo se copia, se crea o se modifica en el dispositivo, sus datos serán cifrados.

COMPORTAMIENTO AL MODIFICAR LA REGLAS DE CIFRADO

Cuando existan cambios en las políticas de cifrado, éste no surtirá efecto hasta la próxima vez que se conecte el dispositivo.

La próxima vez que el dispositivo se conecte:

- Los nuevos archivos serán cifrados.
- El dispositivo cifrado permanecerá de esa forma.
  En este caso, el usuario debe descifrar manualmente el dispositivo que permanecerá sin cifrar en concordancia con la nueva política de cifrado.

UTILIZANDO DISPOSITIVOS CIFRADOS EN OTROS COMPUTADORES

Compartiendo archivos cifrados

Los archivos cifrados en un dispositivo puede ser compartidos en condición de:

- El dispositivo está conectado a otro equipo con un agente de Aranda 360.
- La política de cifrado en el ordenador incluye accesos de lectura o de lectura / escritura.
- El usuario conoce la contraseña del dispositivo encriptado.

Sistemas sin ejecutar Aranda 360

Si un dispositivo cifrado está conectado a un equipo que no se está ejecutando un agente:

- Los archivos cifrados se pueden abrir, pero su contenido se mostrará como texto cifrado.
  Si el dispositivo contiene una partición cifrada con archivos, estos archivos se pueden utilizar con normalidad.

- Se pueden añadir nuevos archivos al dispositivo. No serán encriptados.
- Los archivos pueden ser copiados desde el dispositivo, pero permanecerán cifrados.
- Si las herramientas de cifrado SURT están habilitadas en Administración de Políticas de Seguridad, el usuario puede cifrar y descifrar archivos con solo arrastrarlo.
  La herramienta de cifrado standalone pueden ser también descargadas del sitio Web.

Otros sistemas ejecutando Aranda 360

Si un dispositivo cifrado está conectado a un equipo distinto del agente

- El dispositivo cifrado no será afectado .
- El usuario tendrá que introducir la contraseña del dispositivo cifrado con el fin de acceder a los archivos.
- Las políticas de acceso y auditoria se aplicarán al dispositivo

REMOVIENDO TARJETAS SD

Al extraer una tarjeta SD del lector, odin (Controlador de Dispositivo extraíble) no es notificado

Al extraer una tarjeta SD del lector, el sistema no detectará la acción y la etiqueta de volumen de la tarjeta seguirá apareciendo en el Explorador de Windows.

Como consecuencia de ello, si instala una nueva tarjeta SD, no se le solicitará que introduzca una contraseña.

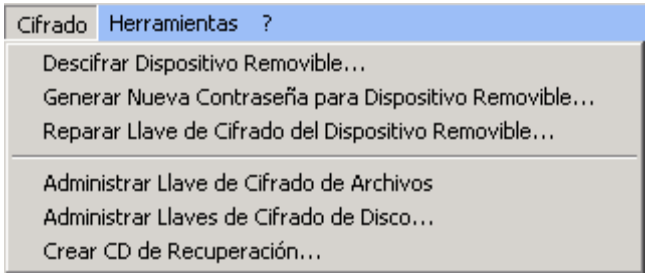
En lugar de eso, Aranda 360 utilizará la contraseña previa de la tarjeta SD. El usuario no podrá acceder a los archivos existentes, porque la clave utilizada para descifrar ellos no es correcta y los nuevos archivos se cifrarán con una clave errónea.

Antes de extraer una tarjeta SD, es imperativo el uso de la función de expulsión en Windows (sólo haga clic derecho en el lector y clic en extraer).

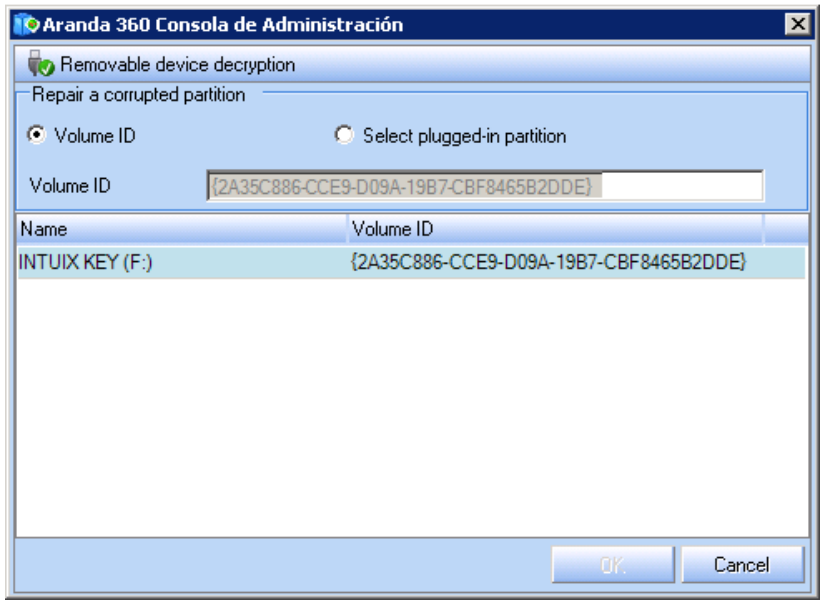
DESCIFRANDO UN DISPOSITVO EXTRAIBLE

LADO ADMINISTRATOR

Para descifrar un dispositivo, el administrador debe seguir los siguientes pasos:



1. Conecte el dispositivo extraíble al equipo donde está instalada la consola.
2. Haga clic en el menú Cifrado.
3. Seleccione Descifrar Dispositivo Extraíble.
4. Digite la contraseña del certificado de la consola.
5. Seleccione un dispositivo de la lista.



LADO AGENTE

Cualquier usuario agente puede descifrar un dispositivo en Configuración General > Control de Dispositivos > Recuperación de Almacenamiento Masivo, establecer Políticas de Seguridad en Permitido.

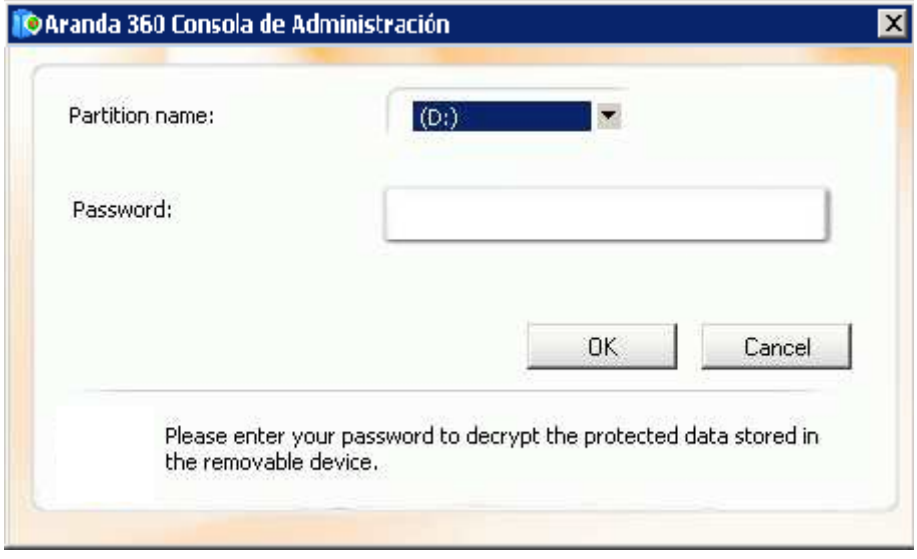
- Durante el proceso de sincronización, el usuario no debe dejar el computador sin actividad durante un largo periodo de tiempo.
  Si el equipo se bloquea automáticamente o entra en el modo de stand-by, el proceso de sincronización se detendrá.

Para descifrar un dispositivo, el usuario debe seguir los siguientes pasos:

1. Haga clic derecho sobre el icono del Monitor Aranda 360 Monitor para visualizar el siguiente menú

2. Haga clic Dispositivo Extraíble seguido de Descifrar un dispositivo extraíble.

   Se visualizará la ventana de Descifrado de información protegida.



3. Seleccione el dispositivo (o partición) de la lista.
4. Digite la contraseña de cifrado del dispositivo.
5. Haga clic en OK.

CONTRASEÑAS

Si un usuario olvida la contraseña de cifrado, una nueva puede ser proporcionada por el administrador.

- El procedimiento requiere la acción del usuario y el administrador.

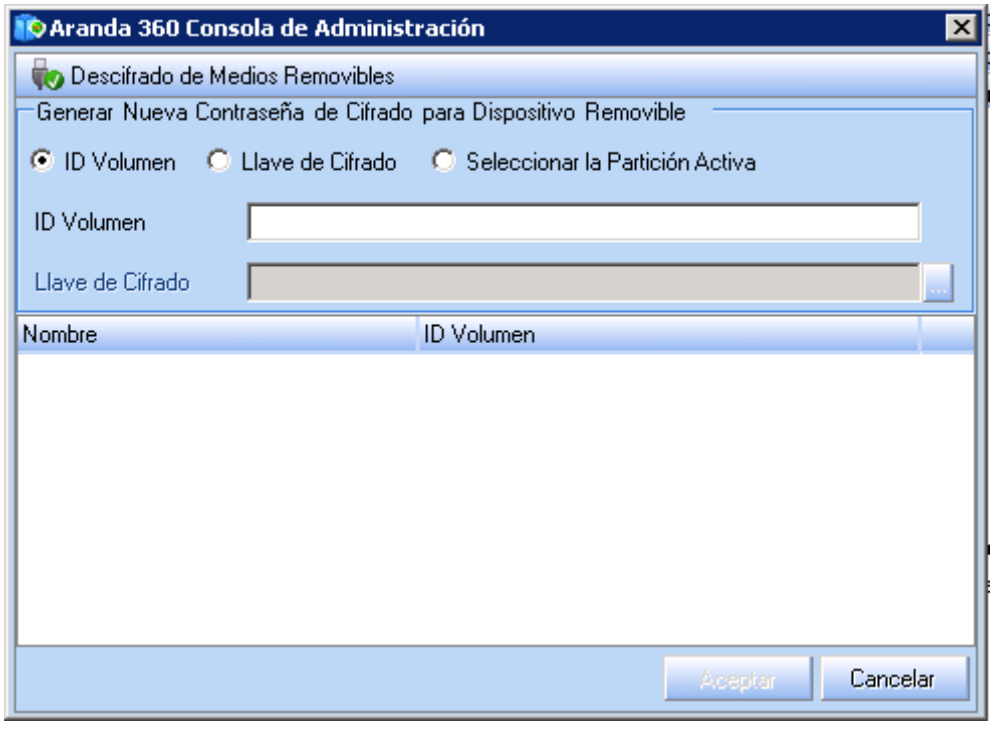
LADO ADMINISTRADOR

Cambiar una contraseña perdida

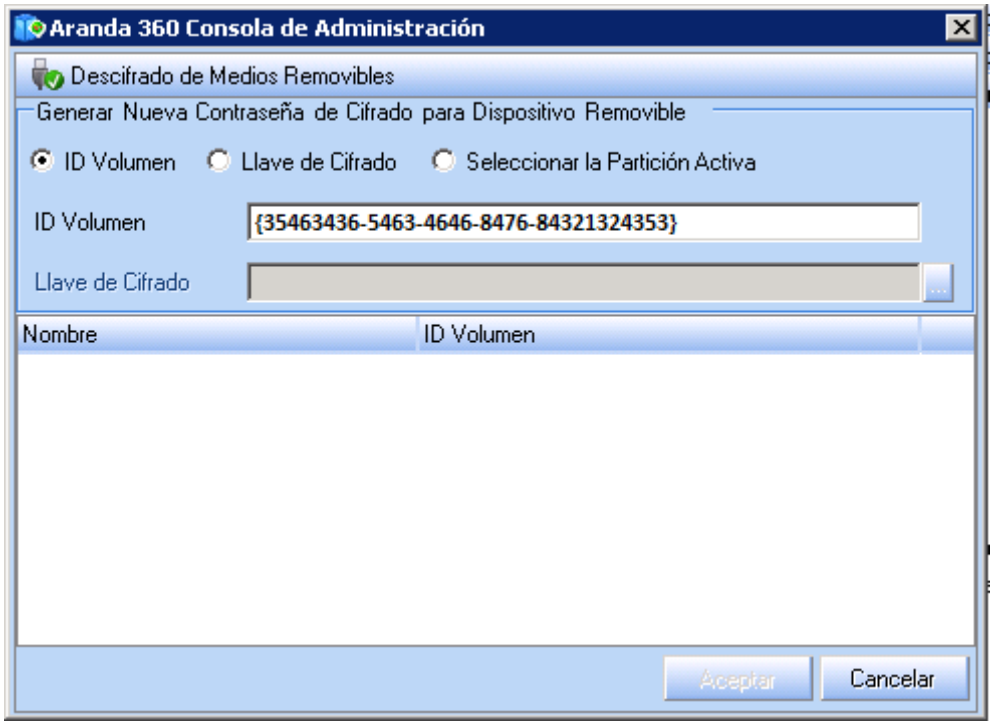
Para cambiar una contraseña, el administrador debe realizar los siguientes pasos:

1. Haga clic en cifrado > Generar nueva contraseña para dispositivo extraíble.
2. Escriba la contraseña del certificado consola.

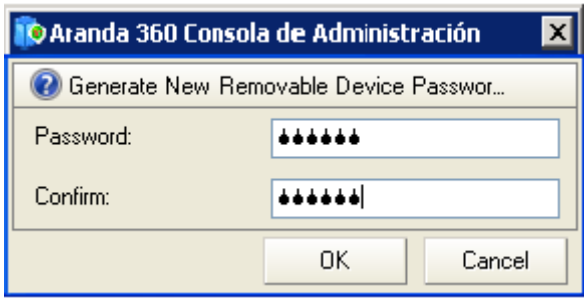
3. Seleccione la forma de generar una nueva contraseña:



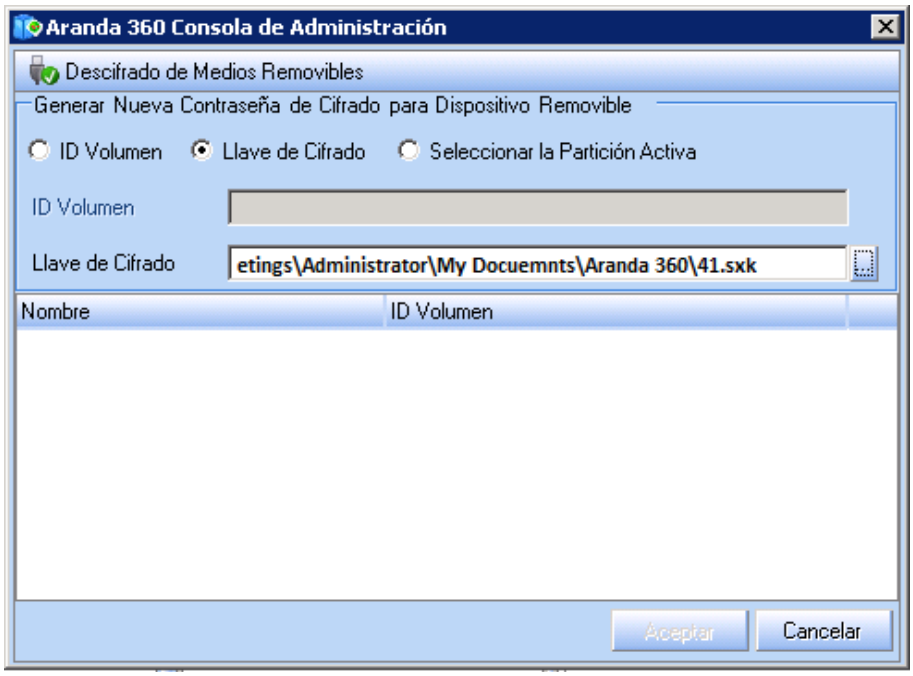
- Por ID del volumen:
  - Haga clic en la opción ID del Volumen.
  - Digite el ID de volumen enviado por el usuario y haga clic en OK.
    El botón OK es activado tan pronto el ID del volumen es reconocido.



- Digite la nueva contraseña.
- Confirme la contraseña.
- Haga clic en OK.

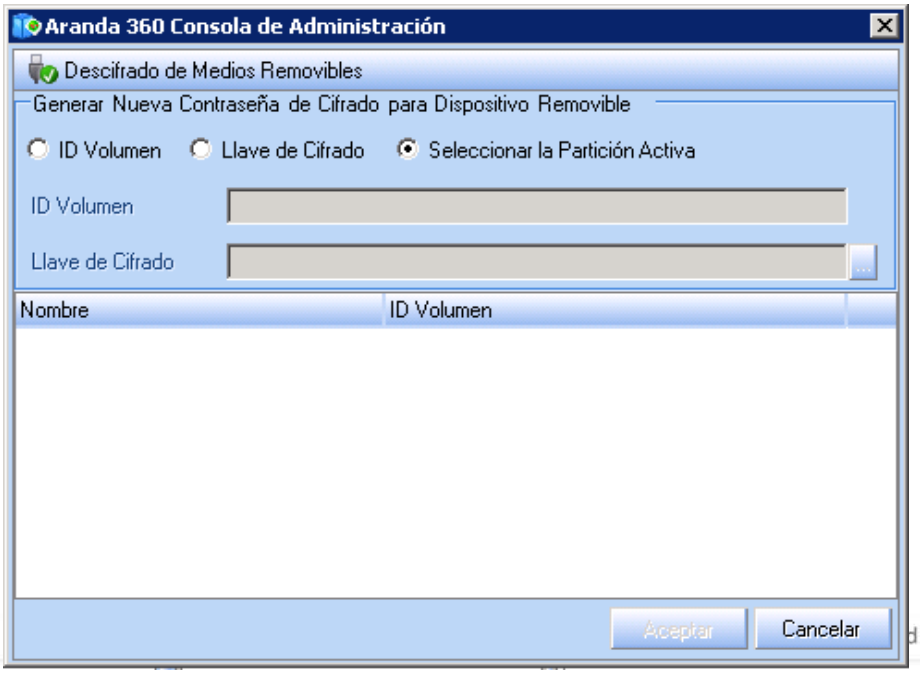


- Por clave cifrada:
  - Haga clic en la opción Clave cifrada.
  - Seleccione el archivo de la clave de cifrado en el sistema, haciendo clic en el botón buscar ... .



  - Haga clic en OK.
  - Cambie la contraseña.
  - Confirme la contraseña.
  - Haga clic en OK.

- Por Selección de partición conectada:
  - Haga en la opción Selección de partición conectada.
  - Seleccione la partición del dispositivo extraíble.



- Cambie la contraseña.
- Confirme la contraseña.
- Haga clic en OK.

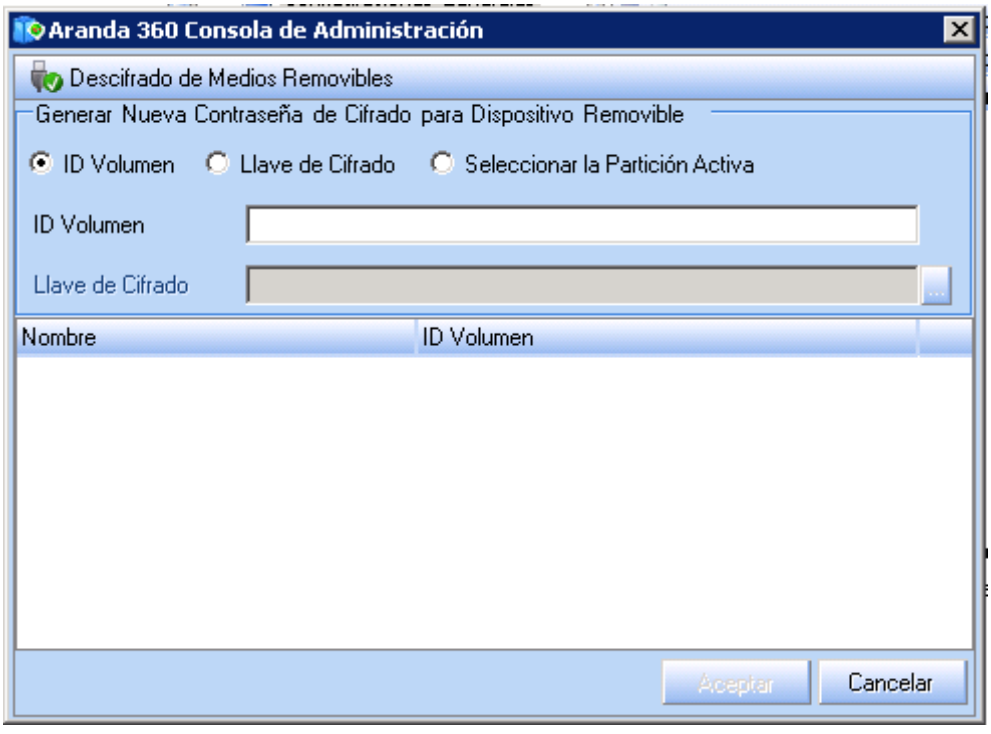
Si la acción seleccionada no logra generar la clave, pruebe con otra.

Exportando una llave cifrada

Después de generar una nueva contraseña para el usuario, el administrador podrá exportar la clave de cifrado. Para ello, siga los siguientes pasos:

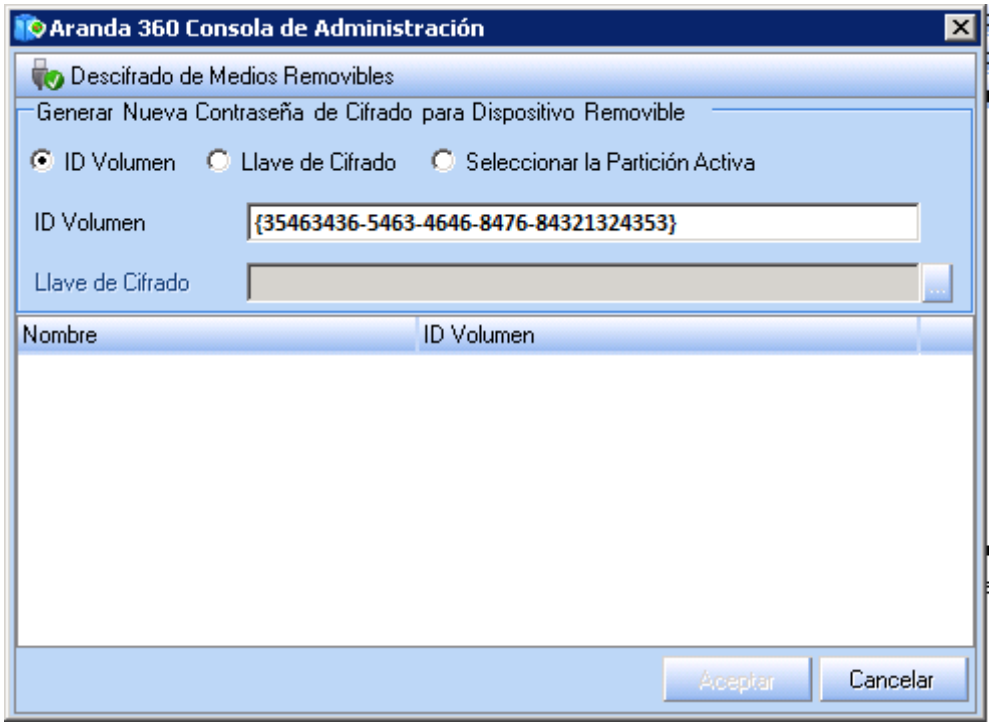
1. Haga clic en Cifrado > Generar nueva contraseña de Dispositivo Extraíble.
2. Digite la contraseña del certificado de la consola.

3. Seleccione la forma de generar una nueva contraseña

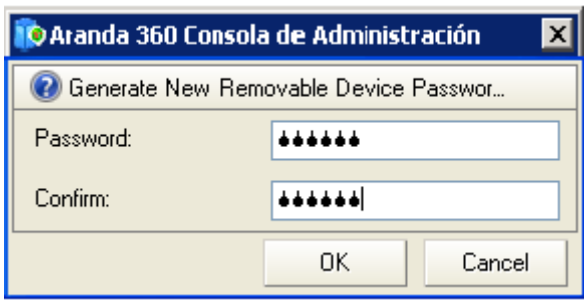


- Por ID del Volumen:
    - Haga clic en la opción ID del Volumen.
    - Digite el ID de volumen enviado por el usuario y haga clic en OK.

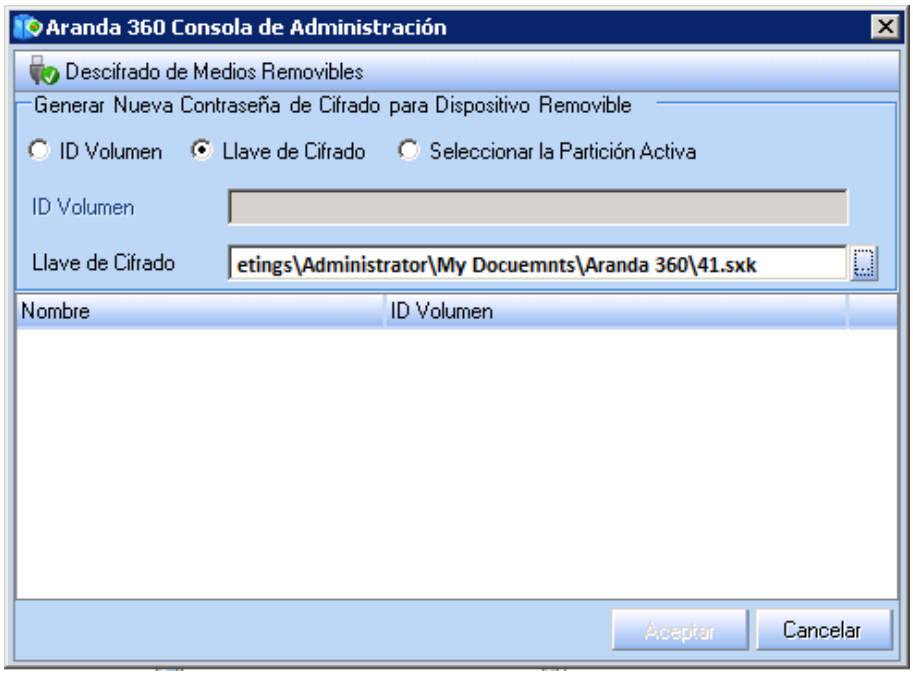
El botón OK es activado tan pronto el ID del volumen es reconocido.



- Digite la nueva contraseña.
- Confirme la contraseña.
- Haga clic en OK.

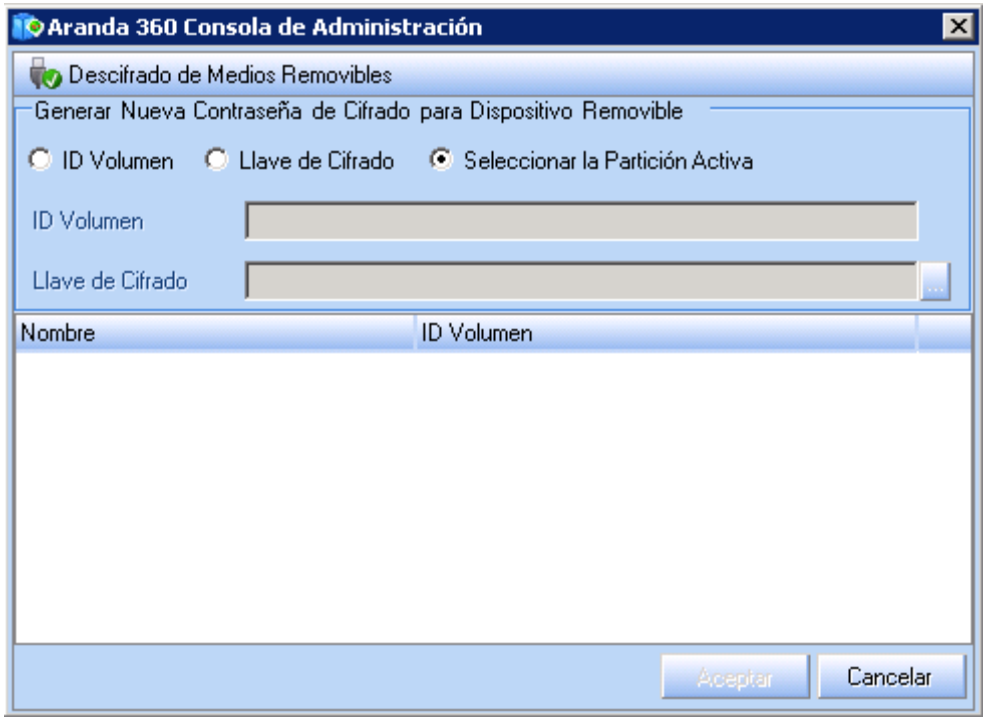


- Por clave cifrada:
  - Haga clic en la opción Clave cifrada.
  - Seleccione el archivo de la clave de cifrado en el sistema, haciendo clic en el botón buscar ... .



  - Haga clic en OK.
  - Digite la nueva contraseña.
  - Confirme la contraseña.
  - Haga clic en OK.

- Por Selección de partición conectada:
    - Haga en la opción Selección de partición conectada.
    - Seleccione la partición del dispositivo extraíble.



    - Cambie la contraseña.
    - Confirme la contraseña.
    - Haga clic en OK.
      Si escoge esta opción, el archive de la clave de cifrado ExportKey.sxk será exportado directamente al dispositivo conectado.
4. Después de introducir la nueva contraseña, guarde el archivo ExportKey.sxk.
5. Notifique al usuario de la ubicación de la nueva clave. El usuario puede importar la nueva clave.

LADO USUARIO

Creando una contraseña

Para crear una contraseña, el usuario debe realizar el siguiente procedimiento:

1. Con el dispositivo conectado, haga clic derecho en el icono de monitor de clic Aranda 360 y clic en Dispositivo Extraíble > Crear Contraseña.

Aparecerá una ventana que solicitara la contraseña para acceder a los datos protegidos.

2. Seleccione el volumen de la lista.
3. Digite la información requerida.
4. Haga clic en OK.

Cambiando una contraseña

Los usuarios pueden cambiar su propia contraseña, para ello siga los siguientes pasos:

1. Haga clic derecho en el icono de monitor de clic Aranda 360 y clic en Dispositivos Extraíbles >Cambiar su Contraseña.

Aparecerá una ventana que le solicitara la contraseña para acceder a los datos protegidos.

2. Seleccione el volumen de la lista.
3. Diligencia la información requerida.
4. Haga clic en OK.

Contraseña Perdida

Para obtener una nueva contraseña del administrador, los usuarios deben seguir los siguientes pasos:

1. Con el dispositivo conectado, Haga clic derecho en el icono de monitor de clic Aranda 360 y clic en Dispositivos Extraíbles
2. Haga clic en Contraseña perdida.

Un nombre de volumen y un número (ID de la clave) son visualizados.

3. Envíe el número del volumen para el administrador (por correo electrónico o copiándolo al servidor, etc.)

4. Si el administrador le envía la clave de cifrado, siga los siguientes pasos:
   - Haga clic para importar la clave de cifrado de:
   - Introduzca la ruta y el nombre del archivo (o haga clic en para localizar el archivo).
   - Haga clic en OK para importar el archivo.

Exportando una clave de cifrado

Los usuarios de Aranda 360 pueden exportar una copia de la clave de cifrado para propósitos de respaldo. Exportar una clave de cifrado puede ser útil cuando no hay acceso a la red.

Para exportar una clave cifrada, el usuario debe ejecutar los siguientes pasos:

1. Con el dispositivo conectado, clic derecho en el icono del monitor Aranda 360 y clic en dispositivos extraíbles.
2. Clic en exportar una llave cifrada

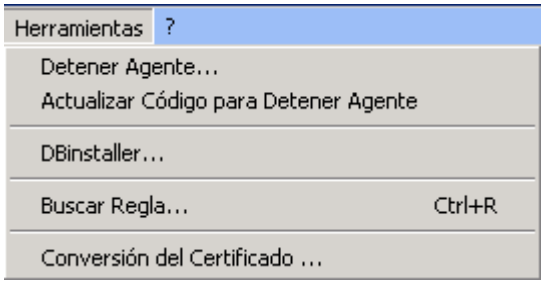
La ventana de exportar clave cifrada será visualizada.

3. Haga clic en exportar la clave cifrada: campo.
4. Introduzca la ruta del archivo de la llave cifrada (o clic en el botón buscar
5. Clic en OK para exportar el archivo.

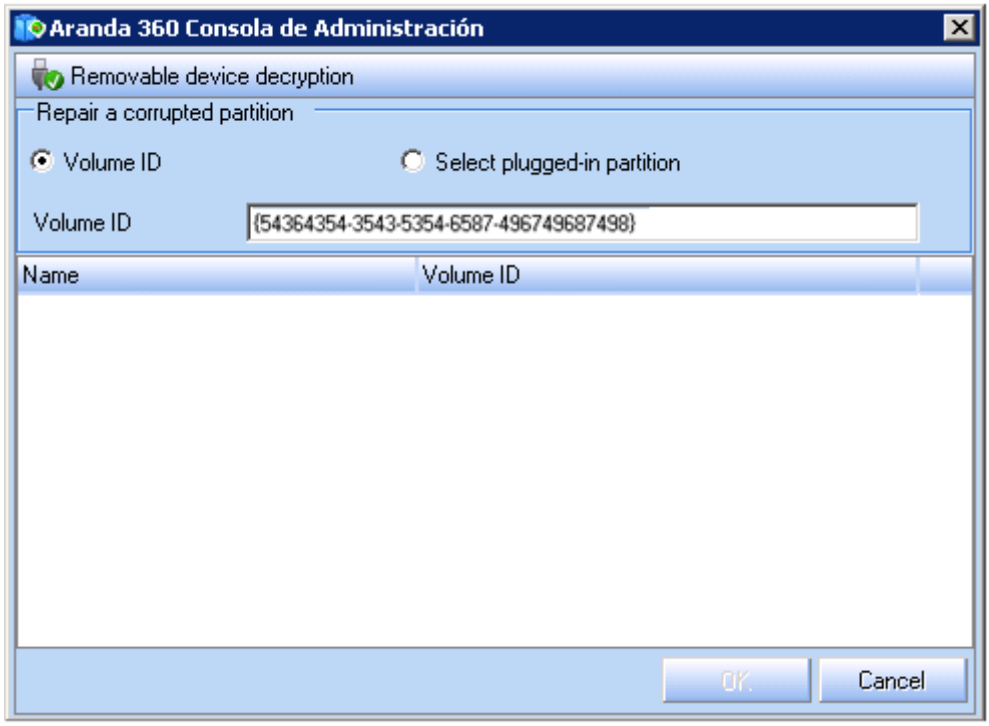
REPARANDO UNA CLAVE CIFRADA CORRUPTA

Para reparar una llave cifrada, el administrador debe seguir los siguientes pasos:

1. Seleccione Cifrado > Reparar llave de cifrado de dispositivos extraíbles



2. Seleccione la forma de reparar la llave de cifrado.



   - Si usted elige la opción Identificación del volumen, escriba el ID de volumen en el campo de texto.
   - Si usted elige la opción Seleccionar Partición Conectada, seleccione el volumen apropiado

3. Haga clic en OK.

   El botón OK se activa sólo si el ID de volumen es correcto o si el dispositivo extraíble es detectado.
4. Guarde la nueva clave de cifrado.

Capitulo 11 – SCRIPTS

ACERCA DE ESTE CAPITULO

En este capítulo se describe la funcionalidad para Scripts incluida en Aranda 360, además como se pueden crear e implementar scripts propios.

Se incluye:

- Generalidades:
  - La funcionalidad scripts.
  - Tipos de Scripts:
    - Scripts de Pruebas.
    - Scripts de acciones.
    - Scripts para procesos lotes.

- Editor de Scripts.

- Scripts de pruebas:
  - Generalidades.
  - Declaraciones.
  - Pruebas predefinidas.
  - Pruebas definidas por el usuario.
  - Creando Scripts de pruebas.

- Scripts de acciones:
  - Generalidades.
  - Acciones predefinidas.
  - Acciones definidas por el usuario.
  - Creando un scripts de acciones.

- Scripts para procesos por lotes:
  - Generalidades.
  - Resultados Verdaderos/Falsos.
  - Creando un script por lotes.

- Scripts de acciones temporales.
- Cargando archivos del servidor principal.

GENERALIDADES

CARACTERÍSTICAS DE LOS SCRIPTS

Aranda 360 se puede utilizar para crear scripts que controlen la reconfiguración automática y autónoma de agentes.

El uso de scripts permite al administrador definir las condiciones para la aplicación de políticas y configuraciones basadas en:

- El estado de la estación de trabajo.
- La conexión utilizada.
- La identidad del usuario.

El cumplimiento de políticas dinámicas permite modificar las políticas de seguridad en tiempo real y exigir el cumplimiento de estas en una estación de trabajo. Esto último es muy importante antes de permitir el acceso para una estación de trabajo a la red corporativa.

TIPOS DE SCRIPTS

Los tres tipos de scripts son:

1. Scripts de pruebas.
2. Scripts de acciones.
3. Scripts para procesos por lotes.

Los tipos de scripts son detallados a continuación.

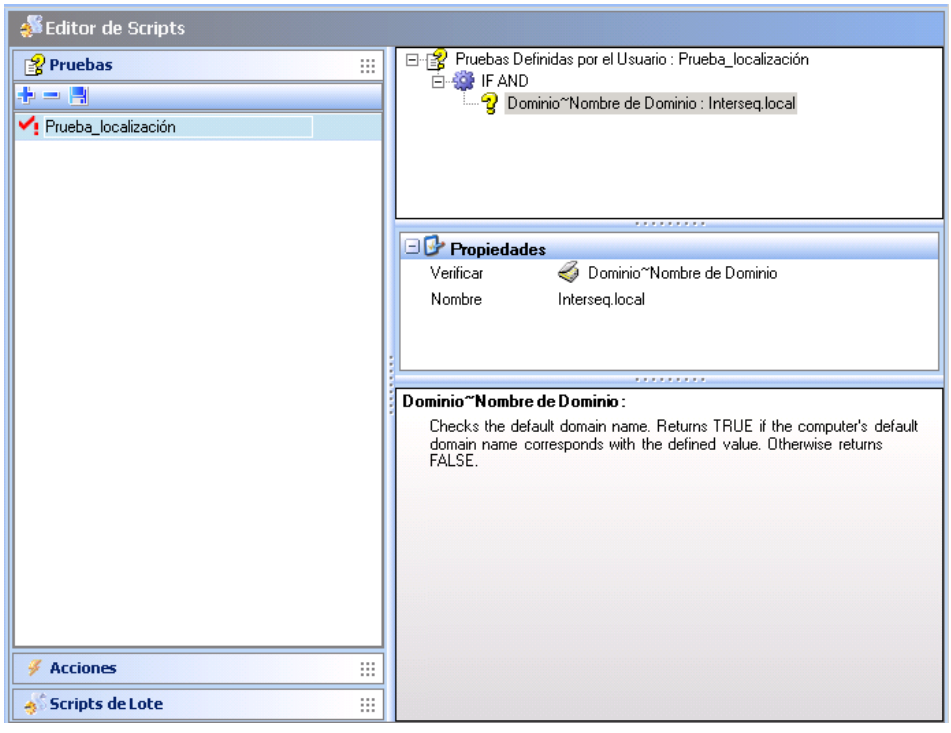
Scripts de prueba

Los Scripts de pruebas pueden incluir:

- Pruebas predefinidas.
- Pruebas definidas por usuarios.
- Operadores lógicos boléanos.

El icono de un script de prueba es  .

Este es un ejemplo de un script de prueba en donde se incluye una prueba definida por el usuario basada en un nombre de dominio:



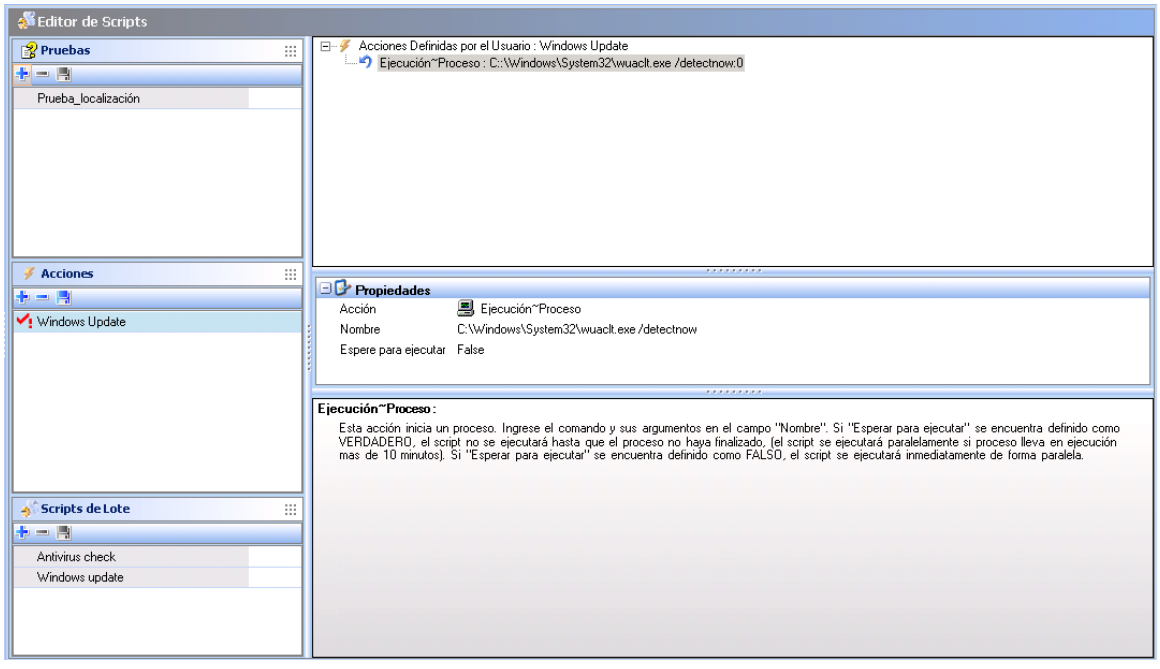
Scripts de acciones

Los scripts de acciones pueden incluir:

- Acciones predefinidas.
- Acciones definidas por usuarios.

El icono para un script de acciones es .

Este es un ejemplo de un script de acción que incluye una acción definida por el usuario:



Scripts para procesos por lotes

Los scripts para procesos por lotes pueden incluir:

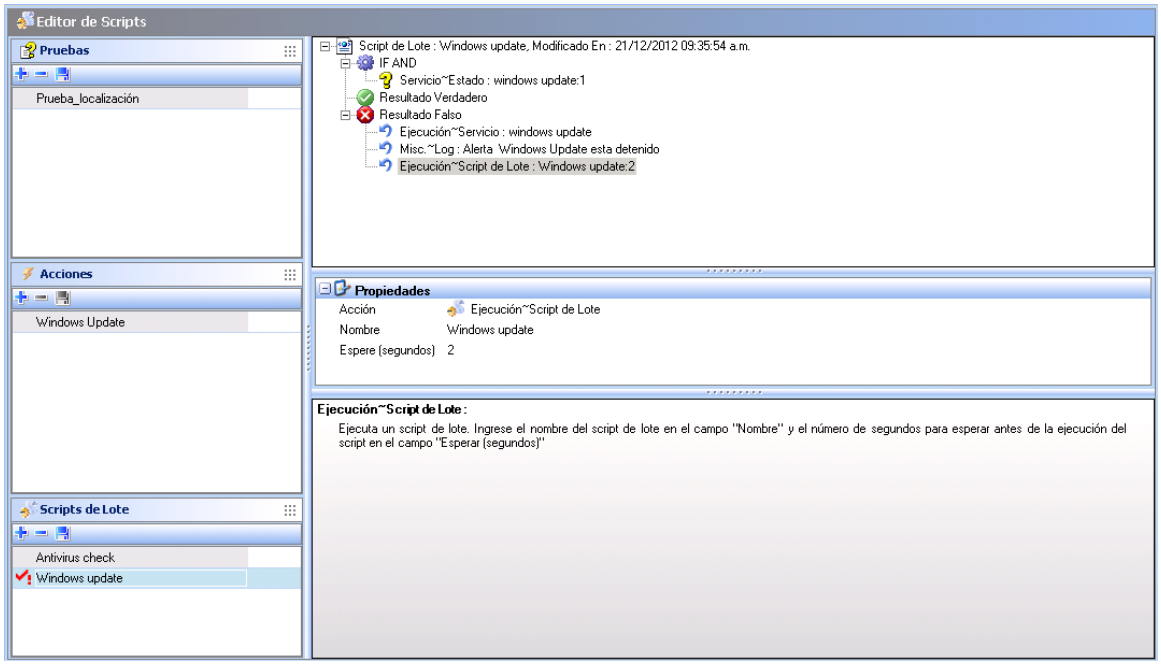
- Scripts de pruebas.
- Scripts de acciones.
- Operadores lógicos boléanos.
- Resultados.

El icono para un script de procesos por lotes es .

El icono para un Resultado verdadero es .

El icono para un Resultado falso es .

Este es un ejemplo de un script de proceso por lotes que consiste en la verificación de la ejecución del Servicio Windows Update. Si el servicio no está activo, este será ejecutado nuevamente:

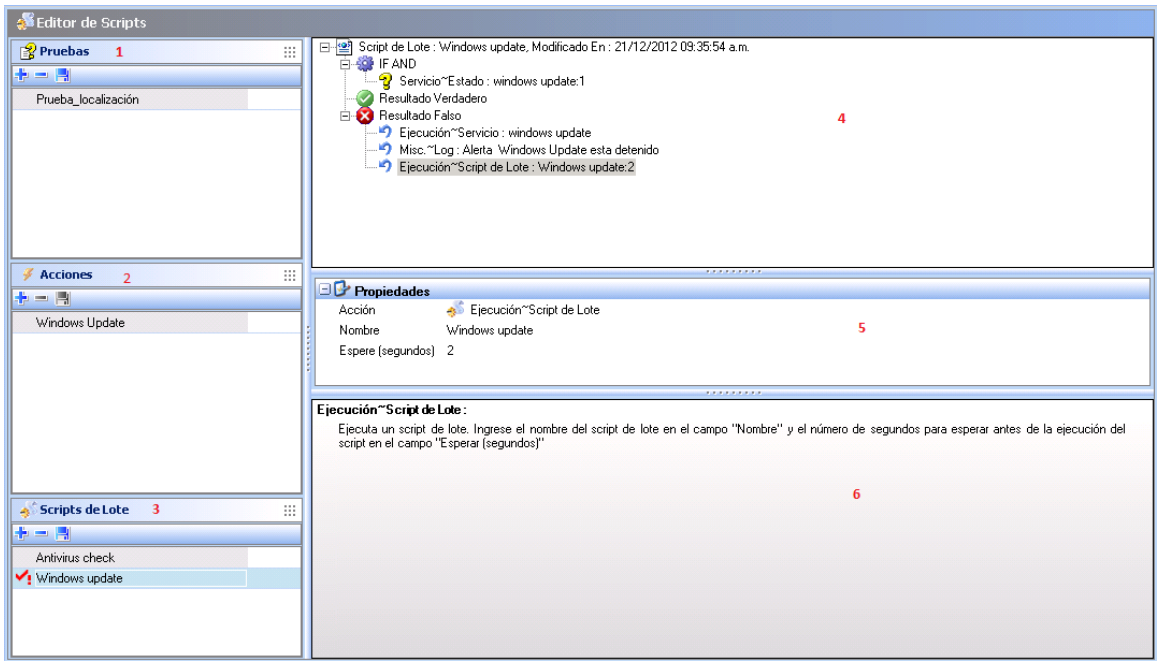


- Usted encontrará en este capítulo, una sección llamada “Scripts de acciones temporales”.
  Los scripts de acciones temporales no pertenecen a la categoría de scripts simples. Estos scripts cumplen una función específica a petición del usuario quien decide lo que se va a ejecutar:
  - Scripts de soporte
  - Scripts de acción
  - Scripts para procesos por lote

  Estos scripts se configuran en la consola de administración de Aranda.

EDITOR DE SCRIPTS

El Editor de scripts es donde se pueden construir los scripts.



1. De prueba:

   En esta área se muestran las pruebas disponibles

   Usted puede agregar una así:

   - Clic-derecho en esta área y seleccionar Adicionar del menú desplegable.
   - Clic directamente en .

   También puede verificar pruebas existentes.

2. De Acciones:
   En esta área se muestran las acciones disponibles.
   Usted puede agregar acciones de la lista.
   También puede verificar acciones existentes.

3. De Procesos por lotes:
   En esta área se muestran los procesos por lotes disponibles.
   Usted puede agregar procesos por lotes de la lista.
   También puede verificar los existentes.

4. Área de trabajo:
   Esta área muestra el contenido del script seleccionado. Aquí es donde realmente se construyen o editan los scripts.

5. Propiedades:
   Esta área muestra las propiedades asociadas a una prueba o una acción. Puede hacer doble clic en el campo que está junto a la propiedad en cuestión para cambiarla.

6. Área de mensajes:
   Esta área muestra una descripción de la prueba o acción seleccionada.

   - Al crear o modificar scripts, puede mover los elementos (ejemplos:
     Declaraciones, pruebas predefinidas o pruebas definidas por el usuario) con un simple arrastrar y soltar.

SCRIPTS DE PRUEBA

GENERALIDADES

Un script de prueba se compone de:

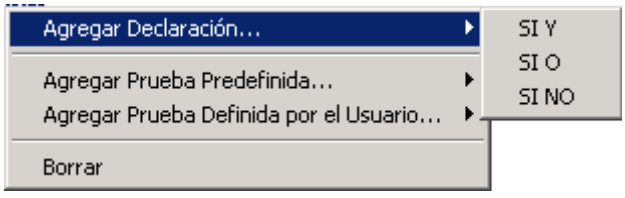
- Declaraciones:
  Operadores lógicos boléanos (ejemplo: SI Y).

- Pruebas predefinidas:
  Pruebas prediseñadas (ejemplo: el usuario verifica la ejecución de un proceso).

- Pruebas definidas por el usuario:
  Pruebas que usted u otro administrador han creado previamente.

DECLARACIONES

Las declaraciones usan los operadores lógicos boléanos SI Y, SI O and SI NO.



Definición de declaraciones

Las declaraciones devuelven VERDADERO o FALSO dependiendo de los resultados de las pruebas.

DECLARACIONES	VALORES DEVUELTOS...
SI Y	- VERDADERO si todas las pruebas devuelve VERDADERO. - FALSO si alguna prueba retorna FALSO.
SI O	- VERDADERO si al menos una prueba devuelve VERDADERO - FALSO si todas las pruebas devuelven FALSO.
SI NO	- VERDADERO si todas las pruebas devuelven FALSO. - FALSO si alguna prueba devuelve VERDADERO.

Tabla 11.3: Definición para declaraciones

Ejemplo de pruebas usando operadores lógicos

Este es un ejemplo de los componentes que constituyen una prueba simple:

IF NOT

\

IF AND

\

mytest1

|

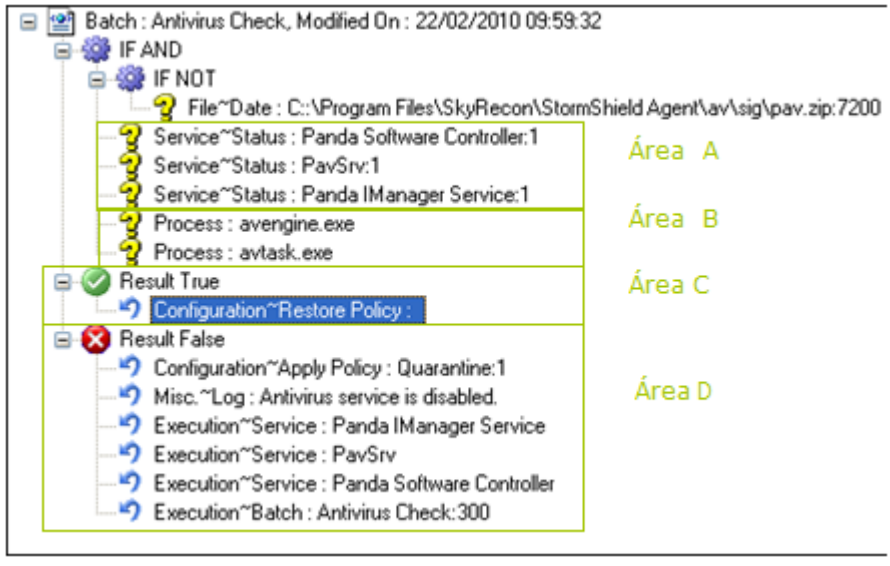
mytest2

- SI miprueba1 Y miprueba2 devuelven ambas VERDADERO:
  - Declaración SI Y retorna VERDADERO.
  - Declaración SI NO retorna FALSO.

- SI miprueba1 devuelve VERDADERO Y miprueba2 devuelve FALSO:
  - Declaración SI Y retorna FALSO.
  - Declaración SI NO retorna VERDADERO.

Declaraciones anidadas

Puede anidar declaraciones para formar pruebas más poderosas y complejas. Este es un ejemplo de una prueba por lotes incluyendo declaraciones anidadas:



El propósito de este ejemplo es probar si el servicio de antivirus se está ejecutando en una estación de trabajo.

El agente comprobará si:

- Los tres servicios se han puesto en marcha (Zona A).
- Los dos archivos ejecutables están presentes en la estación de trabajo (Área B).

Si la prueba devuelve VERDADERO, el agente va a restaurar la anterior política permanentemente en la estación de trabajo (zona C).

Si la prueba devuelve FALSO (Zona D):

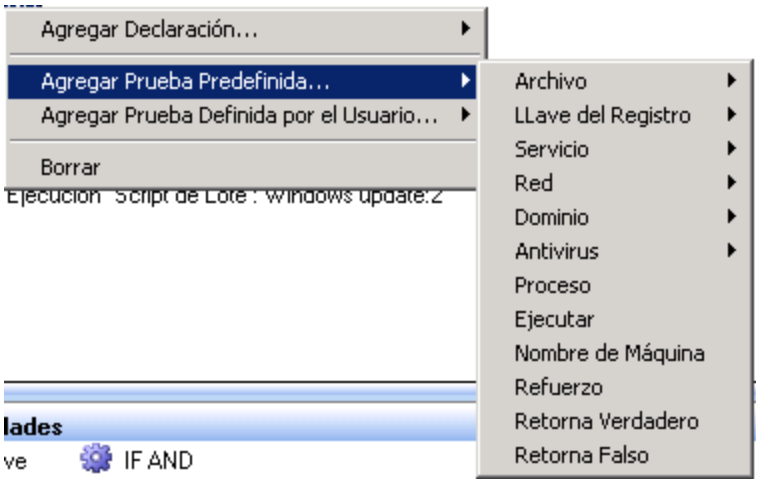
- Una política de cuarentena se aplicara temporalmente para evitar cualquier riesgo y estará vigente siempre y cuando el servicio del antivirus este deshabilitado.
- Un log se enviará indicando que el servicio del antivirus está deshabilitado.
- Los tres servicios se lanzaran nuevamente.
- El proceso por lotes se volverá a ejecutar después de 300 segundos.

PRUEBAS PREDEFINIDAS

Una prueba predefinida es una prueba prediseñada que puede ser usada en su script.

Primer nivel

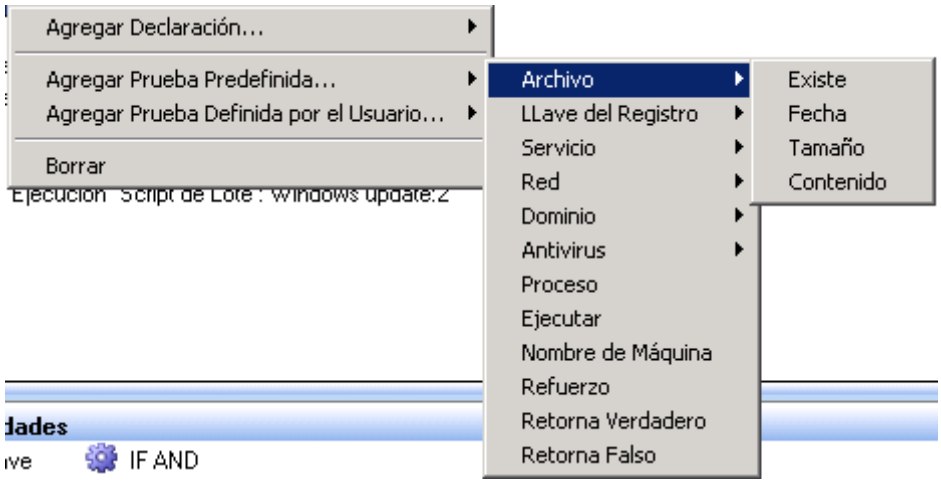
Esta es la lista de pruebas predefinidas de primer nivel disponibles en Aranda 360:



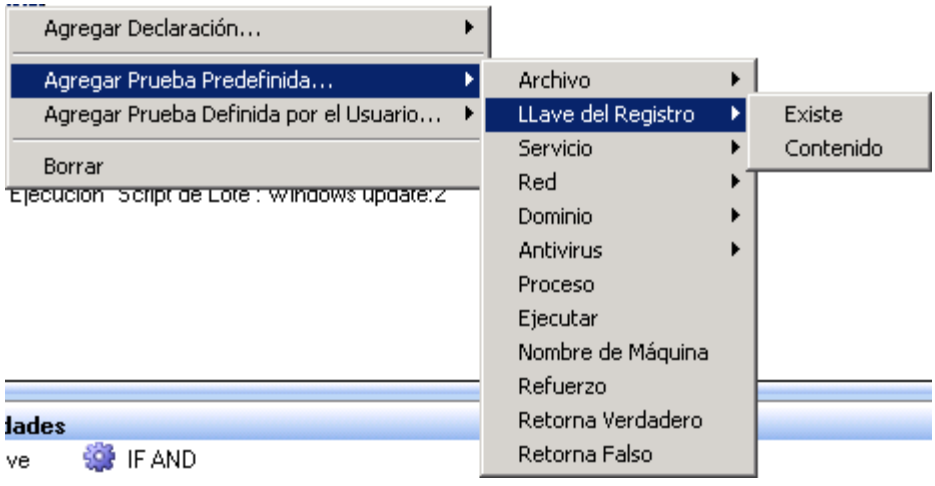
Segundo nivel

Esta es la lista de pruebas predefinidas de segundo nivel disponibles en Aranda 360:

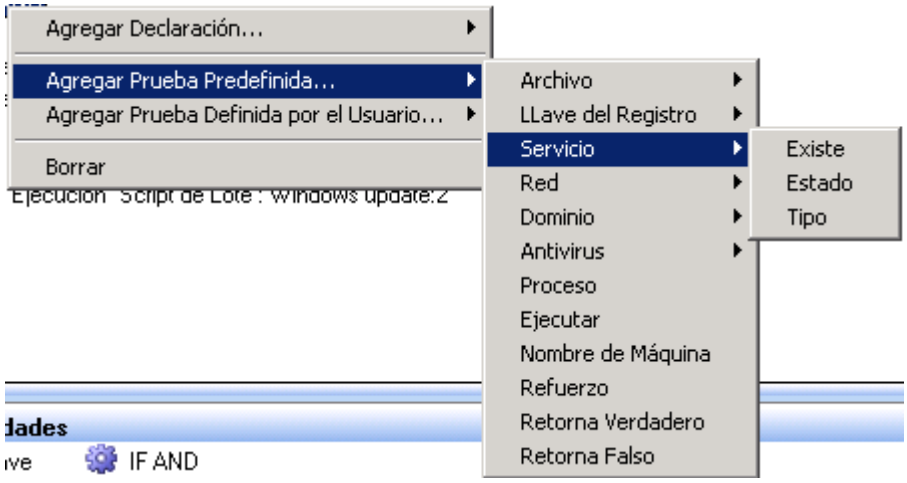
- En el submenú Archivo, se encuentran las siguientes pruebas predefinidas:



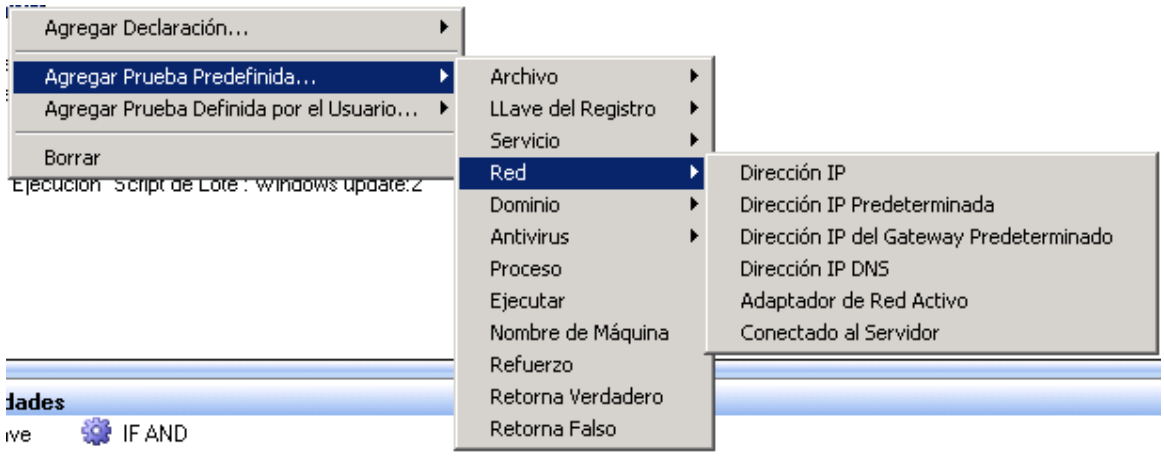
- En el submenú Clave del Registro, se encuentran las siguientes pruebas predefinidas:



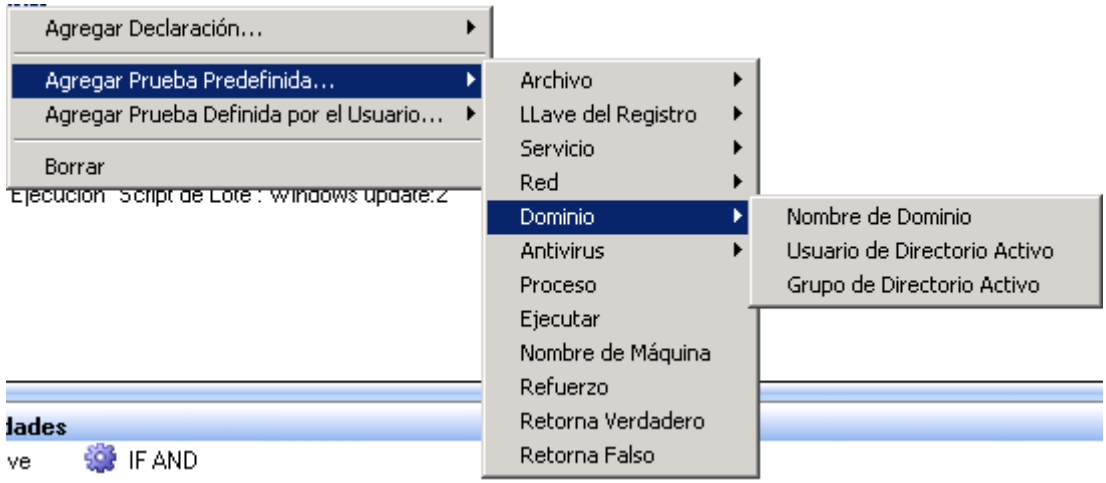
- En el submenú Servicio, se encuentran las siguientes pruebas predefinidas:



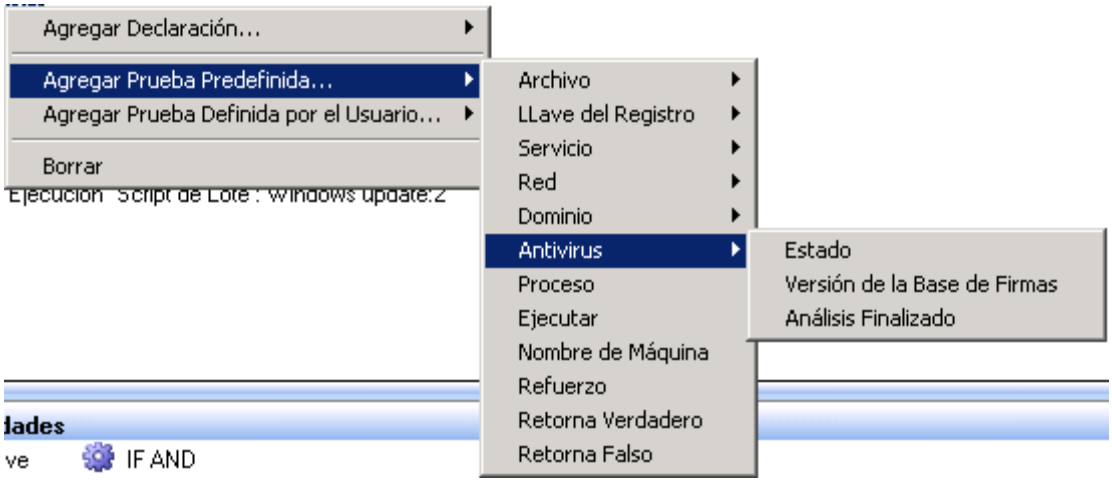
- En el submenú RED, se encuentran las siguientes pruebas predefinidas:



- En el submenú DOMINIO, se encuentran las siguientes pruebas predefinidas



- En el submenú Antivirus, se encuentran las siguientes pruebas predefinidas:



Definición de pruebas predefinidas

Una prueba predefinida usualmente es usada para que se ejecute como parte de un script

PRUEBA	DESCRIPCIÓN	PROPIEDADES
Archivo > Existe	El agente comprueba si el archivo especificado existe en el sistema. Devuelve VERDADERO si el archivo especificado existe. De lo contrario, devolverá FALSO.	Ingrese el nombre y la ruta del archivo: o Nombre: c:\programs\acme software\ acme software update.exe
Archivo > Fecha	El agente verifica la última fecha de modificación del archivo especificado en el sistema, y la fecha de creación. Devuelve FALSO: o si la fecha de modificación y el tiempo de existencia del archivo es mayor que o igual a la fecha actual, o o si el archivo especificado no existe. De otro modo, devolverá VERDADERO.	Ingrese el nombre y la ruta del archivo: o Nombre: c:\Programs\antivirus\ update.exe Ingrese el tiempo que se adicionara a la ultima fecha de modificación para determinar el tiempo en el que se basara la prueba: o Tiempo (sec.): 120
Archivo > Tamaño	El agente verifica el tamaño del archivo especificado. Devuelve FALSO: o Si el tamaño del archivo es diferente del tamaño especificado, o o si el archivo especificado no existe. De otro modo, devolverá VERDADERO.	Ingrese el nombre y la ruta del archivo: o Nombre: c:\test\file.png Especifique el tamaño del archivo en bytes: o Tamaño (bytes): 20

Tabla 11.4: Definición de pruebas predefinidas (Hoja 1 de 5)

PRUEBAS	DESCRIPCIÓN	PROPIEDA DES
Archivo > Contenido	Comprobar el contenido del archivo especificado. Devuelve VERDADERO si el archivo contiene la cadena de caracteres especificada. Devuelve FALSO: - si el archivo especificado no existe, - o si la cadena de caracteres no se encuentra, - o si el tamaño del archivo supera los 5 MB.	Ingrese el nombre y la ruta del archivo: - Nombre: c:\test\file.txt Defina la cadena de caracteres a buscar: - Contenido: antivirus test log
Clave de registro > Existe	Busca la clave de registro en la base de datos de registros. Devuelve VERDADERO si la clave de registro existe. De lo contrario, devuelve FALSO.	Seleccione la ruta del registro: - Ruta raíz: HKEY_LOCAL_MACHINE Ingrese la ruta de la clave de registro: - Ruta: Software\Microsoft Office 11.0
Clave de registro > Contenido	Comprueba el contenido de la clave de registro especificada en la base de datos de registros. Devuelve VERDADERO si la clave contiene la cadena de caracteres especificada. De lo contrario, devuelve FALSO.	Ingrese la ruta del registro: - Ruta raíz de la clave: HKEY_CLASSES_ROOT - clave: SYSTEM\CurrentControlSet\ Services\TCPip\Parameters - Nombre: [Hostname] - Tipo de contenido: REG_DWORD - Contenido: COMPUTER1
Servicio > Existe	Verifica la existencia de un servicio. Devuelve VERDADERO si el servicio existe. De lo contrario devuelve FALSO.	Siga los siguientes pasos: - Ingrese services.msc en Inicio > Ejecutar o por símbolo del sistema. - Seleccione el servicio. - Haga clic-derecho en el servicio. - Clic en Propiedades para ver el nombre del servicio (Mayúsculas/Minúsculas). - Ingrese el nombre exacto en la prueba predefinida (observe el cuadro):  - Nombre: Dhcp

Tabla 11.4: Definición de pruebas predefinidas (Hoja 2 de 5)

PRUEBAS	DESCRIPCIÓN	PROPIEDADES
Servicio > Estado	Verifica el estado del servicio. Devuelve VERDADERO si el estado del servicio coincide con el especificado en las propiedades. De lo contrario, devuelve FALSO.	Ingrese el nombre del servicio: • Nombre: Dhcp Defina el estado del servicio: • Estado: SERVICE_RUNNING
Servicio > Tipo	Verifica el tipo del servicio. Devuelve VERDADERO si el tipo coincide con el especificado en las propiedades. De lo contrario, devuelve FALSO.	Ingrese el nombre del servicio: • Nombre: Dhcp Ingrese el tipo del servicio: • Tipo: SERVICE_AUTO_START
Red > Dirección IP	Verifica la dirección ip de un equipo host. Devuelve VERDADERO si la dirección ip está configurada en el equipo host. De lo contrario, devuelve FALSO.	Ingrese la dirección ip y la máscara de red: • IP/mascara: 172.16.36.21/32
Red > Dirección IP por defecto	Verifica la dirección IP por defecto. Devuelve VERDADERO si la dirección Ip está configurada en el equipo host. De lo contrario, devuelve FALSO.	Ingrese la dirección ip y la máscara de red: • IP/mascara: 172.16.36.21/32
Red > Dirección IP de la puerta de enlace por defecto	Verifica la dirección ip por defecto para la puerta de enlace. Devuelve VERDADERO si la dirección ip está configurada en el equipo host. De lo contrario, devuelve FALSO.	Ingrese la dirección ip y la máscara de red: • P/mascara: 172.16.36.254/32
Red > Dirección IP del servidor DNS	Verifica que la dirección del servidor DNS este configurada en el equipo. Devuelve VERDADERO si la dirección Ip coincide con la dirección ip del servidor DNS. De lo contrario, devuelve FALSO.	Ingrese la dirección ip y la máscara de red: • IP/mascara: 172.16.36.254/32
Red > Interfaz de red activa	Verifica la interfaz de red especificada. Devuelve VERDADERO si la interfaz de red active coincide con una especificada. De lo contrario, devuelve FALSO.	Después de hacer clic en el área de Propiedades, seleccione las interfaces de red activas de la lista que se muestra en el cuadro de diálogo desplegado
Red > Conexión al servidor	Verifica que el agente pueda conectarse al servidor de Aranda 360.	
Dominio > Nombre de Dominio	Verifica el nombre de dominio por defecto. Devuelve VERDADERO si el nombre de dominio del equipo host coincide con el registrado en el servidor DNS. De lo contrario, devuelve FALSO.	Ingrese el nombre de dominio a verificar: o Nombre: domain.com

Tabla 11.4: Definición de pruebas predefinidas (Hoja 3 de 5)

PRUEBAS	DESCRIPCIÓN	PROPIEDADES
Dominio > Usuario en el directorio activo	Verifica que el usuario tenga una sesión vigente en el directorio activo. Devuelve VERDADERO si el usuario tiene una sesión vigente que corresponde con uno usuario en el directorio activo especificado. De lo contrario, devuelve FALSO.	Ingrese el nombre distintivo del usuario (DN): • Nombre: CN=john, OU=Users,DC=Aranda,DC=fr Observación: Esta prueba predefinida solo funciona en modo conectado.
Dominio > Grupo del directorio activo	Comprueba si un determinado usuario pertenece a un grupo del Directorio activo. El primer parámetro es el nombre de dominio en formato NETBIOS. El segundo parámetro es el nombre del grupo. Devuelve VERDADERO si el usuario pertenece al grupo especificado. De lo contrario, devuelve FALSO.	Ingrese el nombre del dominio en formato NETBIOS: • Dominio: Aranda Ingrese el nombre del grupo del directorio activo: o Nombre: users Observación: Esta prueba predefinida solo funciona en modo conectado.
Antivirus > Estado	Verifica el estado del antivirus. Devuelve VERDADERO si el antivirus esta activo. De lo contrario, devuelve FALSO.	Sólo si se ha instalado la opción de AVP.
Antivirus > Versión de la base de datos de virus	Verifica la vigencia de la base de datos de virus del antivirus. Devuelve VERDADERO si la vigencia de la base de datos de virus del antivirus coincide con un número de días especificado. De lo contrario, devuelve FALSO.	Sólo si se ha instalado la opción de AVP. La base de datos de virus de un antivirus se considera obsoleta cuando es mayor a 3 días. Usted puede aumentar este valor.
Antivirus > Fin del escaneo	Verifica que el antivirus termine de explorar en búsqueda de virus. Devuelve VERDADERO si el escaneo del antivirus ha terminado. De lo contrario, devuelve FALSO.	Sólo si se ha instalado la opción de AVP.
Procesos	Verifica que un proceso se esté ejecutando. Devuelve VERDADERO si el proceso está corriendo . De lo contrario, devuelve FALSO.	Ingrese el nombre del proceso: • Nombre: update.exe

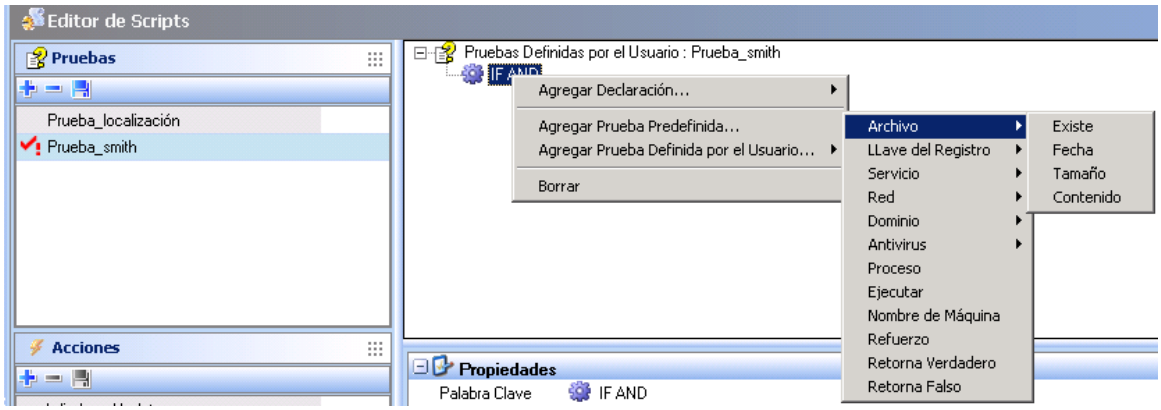
Tabla 11.4: Definición de pruebas predefinidas (parte 4 de 5)

PRUEBAS	DESCRIPCIÓN	PROPIE DADES
Ejecución de procesos	Lanza y comprueba la ejecución de un proceso. Si la Espera por la ejecución se establece en VERDADERO, el script esperará a que termine la ejecución del proceso antes de ejecutar otra acción. Si la ejecución del proceso excede los 10 minutos, el script ejecutara acciones en paralelo. Si la Espera por la ejecución se establece en FALSO, el script seguirá con ejecuciones de otras acciones en paralelo. Devuelve TRUE si el proceso finaliza correctamente. De lo contrario, devuelve FALSO.	Ingrese el nombre y loa ruta del proceso: • Nombre: c:\program files\antivirus\ update.exe Active/Desactive la espera por la ejecución: • Espera por ejecución: Falso
Nombre del Host	Verifica el nombre de un host. Devuelve VERDADERO si el nombre del host corresponde con uno especificado. De lo contrario, devuelve FALSO.	Ingrese el nombre del host: • Nombre: Computer1
Control de Red	Asigna un valor a la variable "Control de Red". Puede ser usado por clientes TNC (Trusted Network Connect) como clientes de acceso Odyssey en redes Juniper (R).	Establezca un estado de control de red a cualquiera de las siguientes opciones: • Permitir, • Aislar, • No permitir acceso, • No hay recomendaciones.
	Para más información de UAC (user acces control) de Juniper, vea ¿"Como instalar el modulo de usuarios con control de acceso?	
Devuelve verdadero	Siempre devuelve verdadero.	
Devuelve falso	Siempre devuelve falso.	

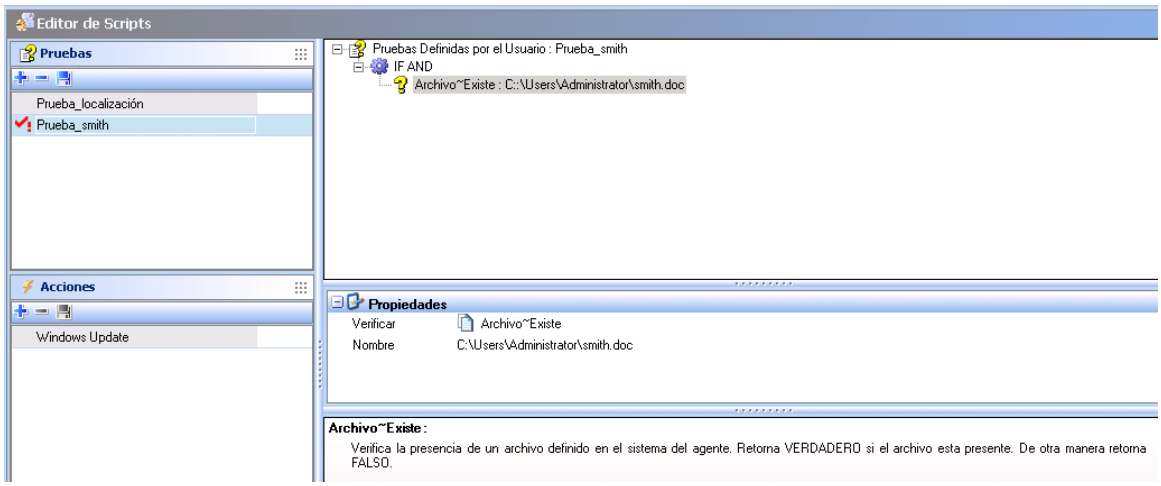
Tabla 11.4: Definición de pruebas predefinidas (Hoja 5 de 5)

Ejemplo de pruebas predefinidas

Este es un ejemplo de una prueba predefinida (Archivo>Existe) que está diseñada para verificar el archivo Smith.doc en la estación de trabajo donde está instalado un agente:



También se puede especificar la ruta del archivo. Si el archivo existe, la prueba devolverá VERDADERO.



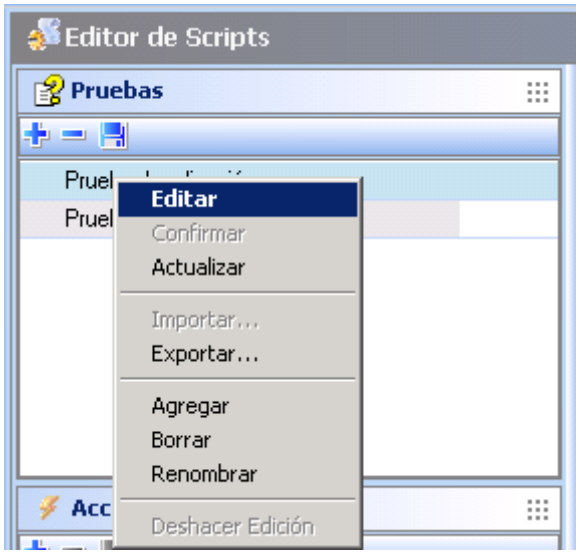
PRUEBAS DEFINIDAS POR EL USUARIO

Una prueba definida por usuario es una prueba que usted u otro administrador ha creado. Puede incluir pruebas definidas por usuario en sus scripts.

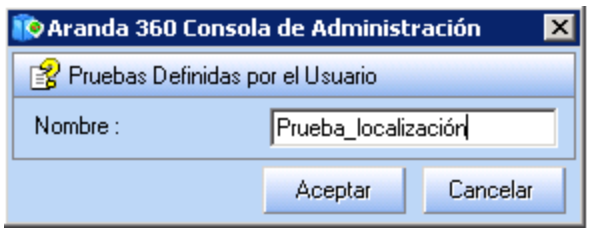
CREANDO UN SCRIPT DE PRUEBA

Para crear un script de prueba, siga los siguientes pasos:

1. En el área de pruebas del Editor de Scripts:
   - Clic derecho en el área.
   - Seleccione Adicionar del menú desplegable o haga clic directamente en el icono de la barra de herramientas.

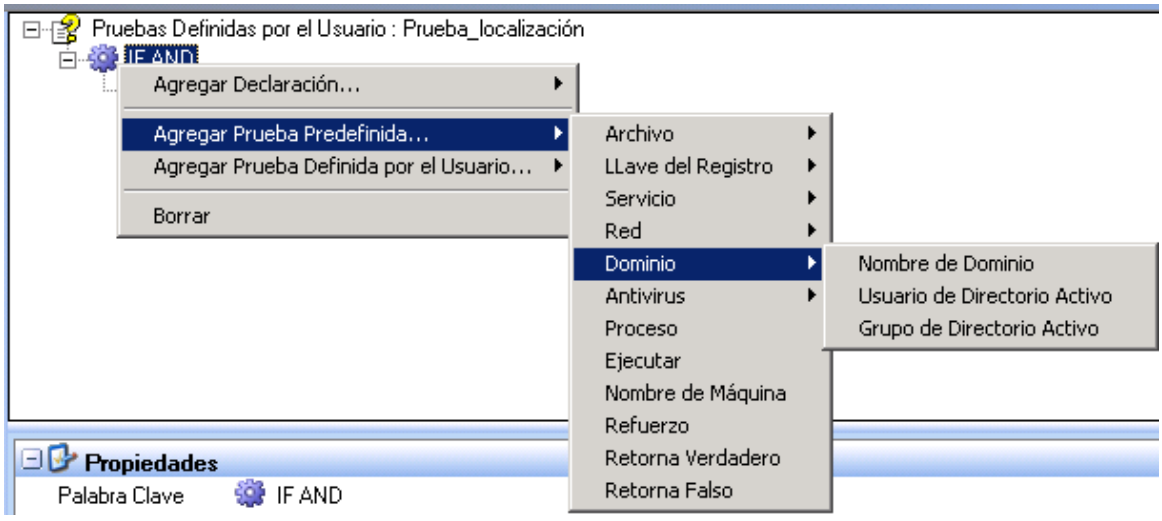


- Nombre el script de prueba definida por usuario.



2. clic-derecho en la declaración mostrada por defecto (SI Y) y haga clic en alguno de las siguientes opciones:

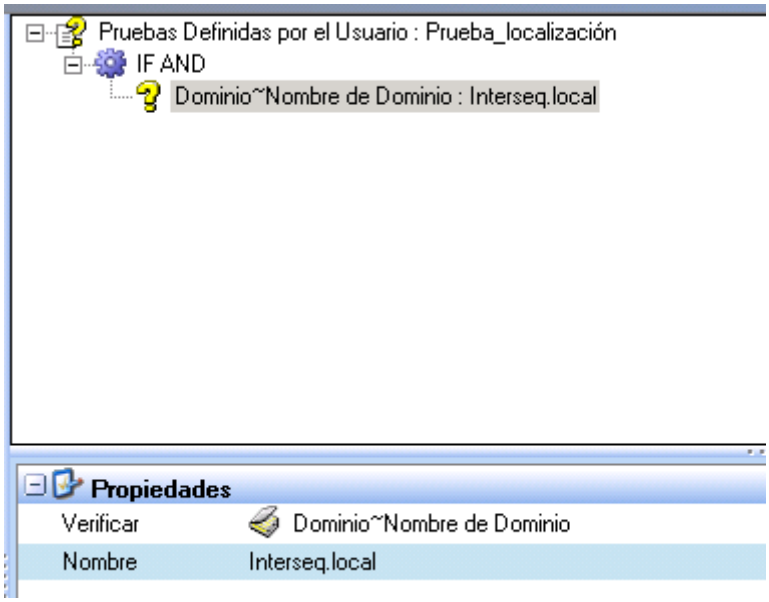
- Agregar Declaración.
- Agregar Prueba predefinida.
- Agregar Prueba definida por usuario.



3. Cuando agregue una prueba, especifique sus propiedades.

   Para ver y configurar el panel de propiedades:

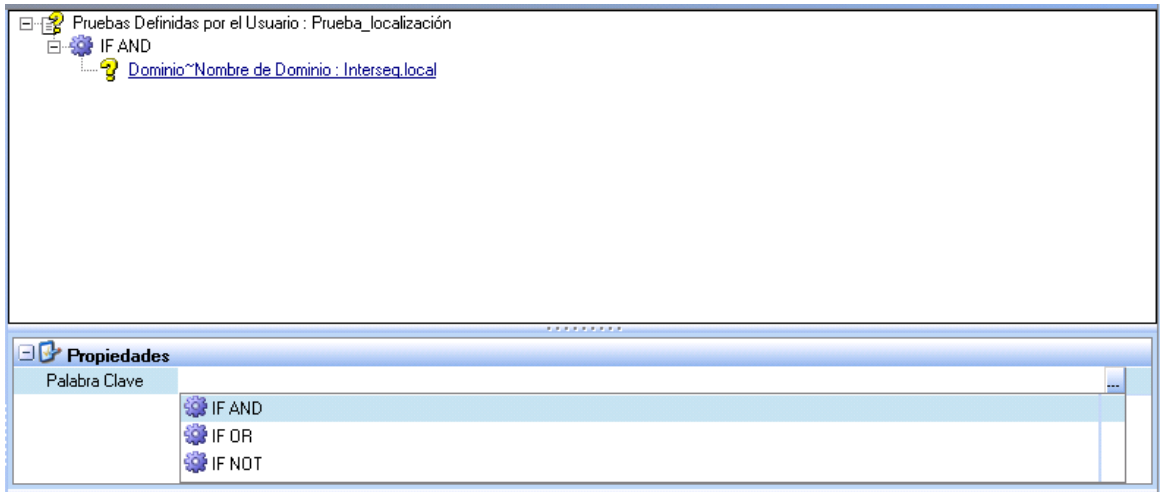
   - Clic en la nueva prueba creada.
   - Escriba el nombre del dominio en el campo nombre.



4. Para cambiar la declaración por defecto (SI Y) o agregar otra:

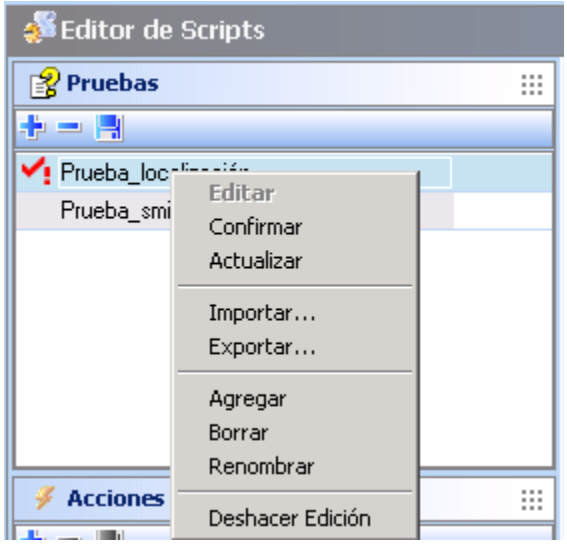
   - Clic en la declaración SI Y en el panel superior.
   - Clic en la declaración en el panel de propiedades.
   - Clic ... para examinar la lista de declaraciones.

   - Seleccione la declaración del menú desplegable.



- Si varias pruebas se incluyen en el script de prueba, tiene que entrar y/o seleccionar la información deseada con el botón Examinar ...

5. Cuando haya terminado de crear el script de prueba:
   - Clic-derecho al script de prueba en el panel de pruebas.
   - Seleccione Registrar.



SCRIPTS DE ACCIONES

GENERALIDADES

Un script de acciones puede incluir dos tipos de acciones:

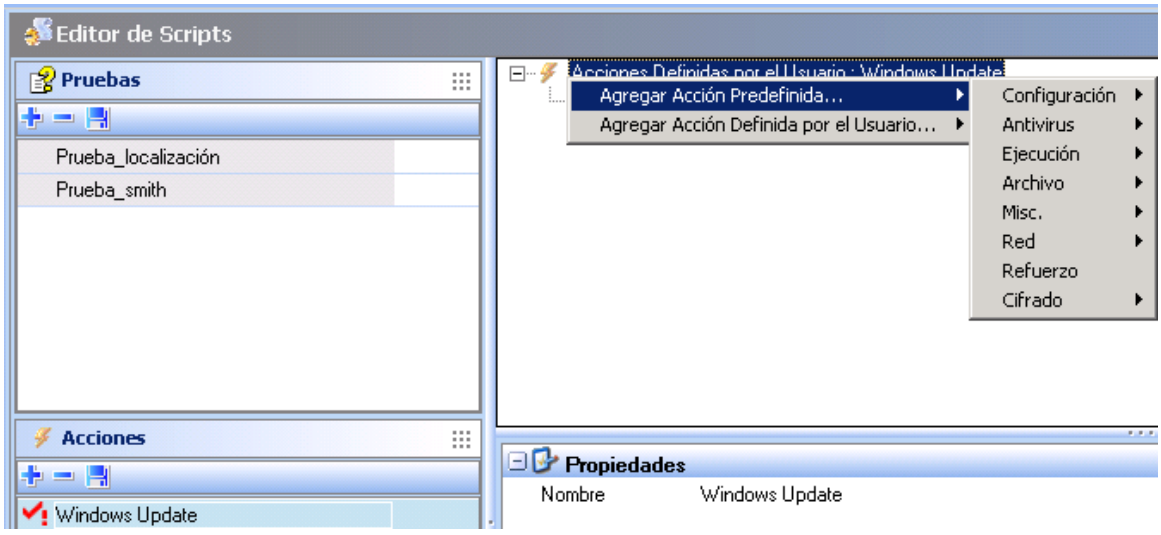
- Acciones predefinidas:
  Estas acciones son acciones ya definidas e incluidas con Aranda 360.
- Acciones definidas por usuario:
  Son acciones creadas por usted u otro administrador.

ACCIONES PREDEFINIDAS

Una acción predefinida es una acción prediseñada usada en sus scripts. Usted puede agregar varias acciones de este tipo a sus scripts.

Primer Nivel

Este es un ejemplo pruebas predefinidas disponibles en Aranda 360 de primer nivel:

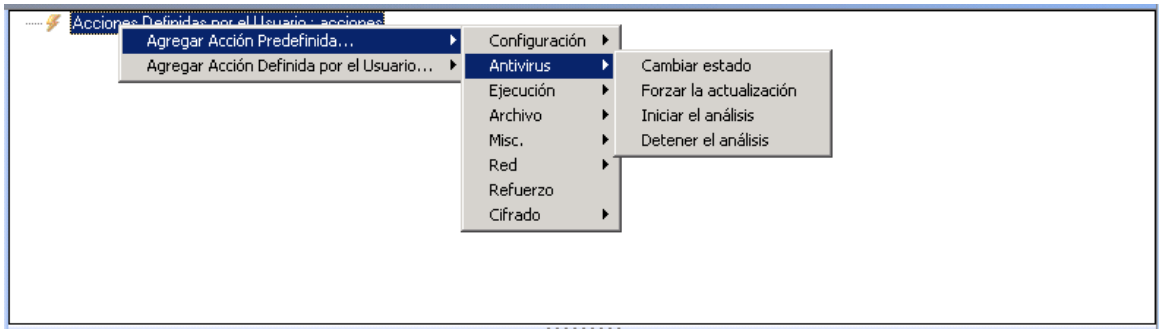


Segundo nivel

Este es un ejemplo pruebas predefinidas disponibles en Aranda 360 de segundo nivel:

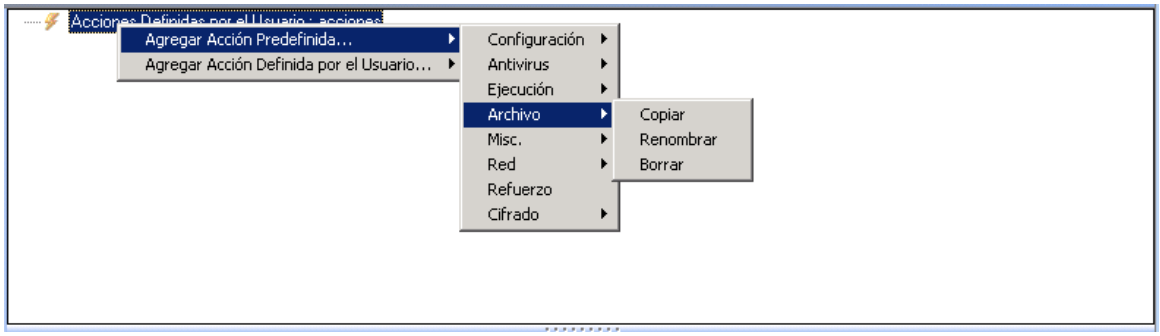
- En el submenú Configuración, encontrará las siguientes acciones predefinidas:
- En el submenú Antivirus, encontrará las siguientes acciones predefinidas:

- En el submenú Antivirus, encontrará las siguientes acciones predefinidas:

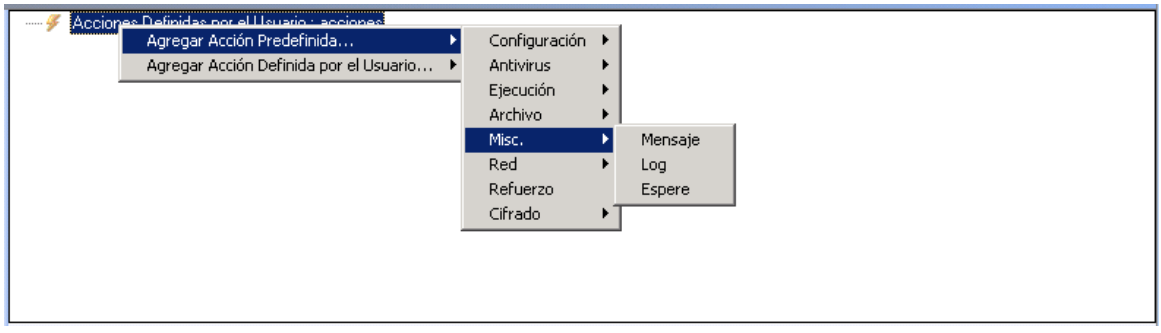


- En el submenú Ejecución, encontrará las siguientes acciones predefinidas:

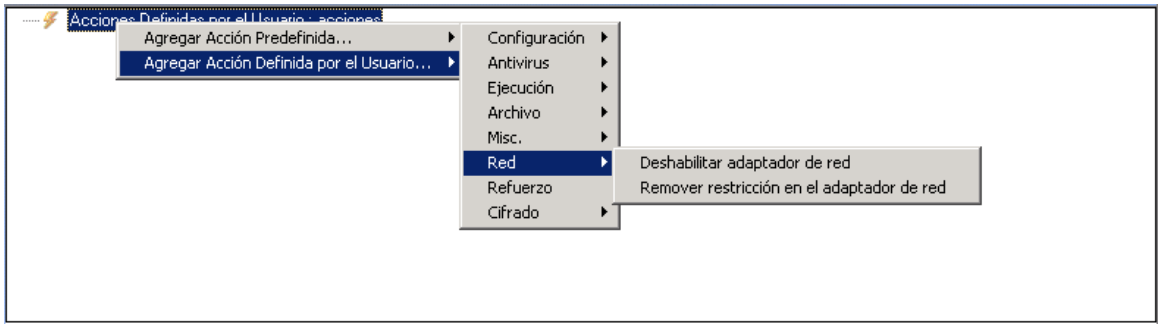
- En el submenú Archivo, encontrará las siguientes acciones predefinidas:



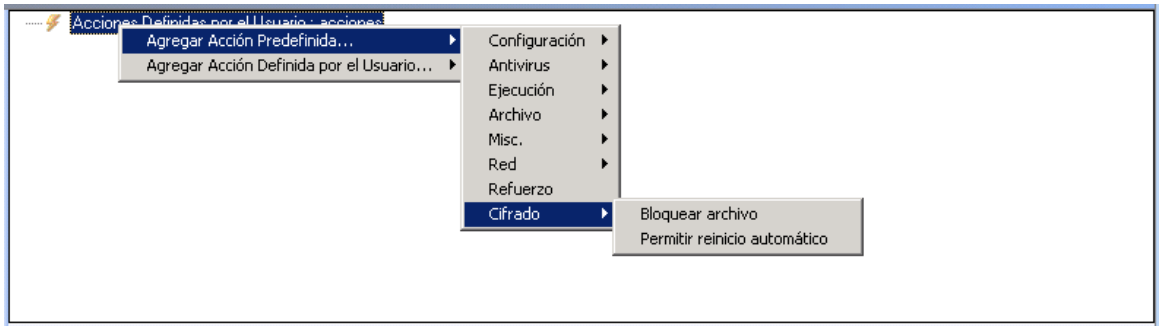
- En el submenú Misc., encontrará las siguientes acciones predefinidas:



- En el submenú Red, encontrará las siguientes acciones predefinidas:



- En el submenú Cifrado, encontrará las siguientes acciones predefinidas:



Definición de acciones predefinidas

Una prueba predefinida de acciones usualmente es usada para que se ejecute como parte de sus propias pruebas, scripts ó de scripts para ejecutar procesos

ACCIÓN	DESCRIPCIÓN	PROPIEDADES
Configuración> Aplicar Política	Aplica una política de seguridad.	Seleccione una política de seguridad: • Nombre: Policy 1 • Tipo: o Temporalidad: Si usted aplica la acción "Restaurar política", la política se restaurara permanentemente. o Permanencia: Si usted aplica la acción "Restaurar política", la política de seguridad será
Configuración> Restaurar Política	Restaura la última política de seguridad vigente. La política restaurada debe estar definida a nivel de grupo para los	
Configuración > Aplicar Configuración	Aplica una configuración.	Ingrese el nombre de la configuración. • Nombre: Paris Office • Tipo: o Temporalidad: Si usted aplica "Restaurar Configuración" esta será restaurada permanentemente. o Permanencia: Si usted aplica la acción "Restaurar configuración", la
Configuración > Restaurar Configuración	Restaura la última Configuración vigente. La Configuración restaurada debe estar definida a nivel de grupo para los agentes.	
Antivirus > Cambiar el estado	Activa/Desactiva el antivirus.	
Antivirus > Forzar la actualización	Obliga la actualización del antivirus.	
Antivirus > Iniciar escaneo	Activa/Desactiva el escaneo del antivirus.	
Antivirus > Detener escaneo	Detiene el escaneo del antivirus.	

Tabla 11.5: Definición de acciones predefinidas (hoja 1 de 3)

ACCIÓN	DESCRIPCIÓN	PROPIEDADES
Ejecución > Procesos	Ejecuta aplicaciones o procesos.	Ingrese el nombre y la ubicación del proceso, y el parámetro de espera (Si aplica): - Nombre: c:\Programs\antivirus\update.exe - espera para la ejecución: - Verdadero: El script no terminara hasta que el proceso termine. - Falso: El script seguirá su ejecución en segundo plano. Para ejecutar el proceso se deben contar con permisos de usuario en el sistema.
Ejecución > Servicio	Ejecuta un servicio.	Ingrese el nombre del servicio: - Nombre: wuauserv
Ejecución > proceso por lotes	Ejecuta un proceso por lotes.	Ingrese el nombre del proceso por lotes: - Nombre: Antivirus Check Ingrese cuanto se debe esperar, en segundos, para iniciar la ejecución del proceso por lotes : - Espera (segundos): 30
Archivo > Copiar	Copia un archivo.	Ingrese el nombre y la ruta del archivo a copiar: - Nombre: c:\Account1 Ingrese el nombre y la ruta en donde se copiará el archivo : Nombre: c:\Account2
Archivo > cambiar nombre	Cambia el nombre de un archivo.	Ingrese el nombre y la ruta del archivo original: - Nombre: c:\programs\acme software\ myfile1.txt Ingrese el nombre y la ruta del nuevo archivo: - Nuevo Nombre: c:\programs\acme software\ myfile2.txt
Archivo > Borrar	Borra un archivo.	Ingrese el nombre y la ruta del archivo: - Name: c:\document.txt
Miscelánea > Mensaje	Muestra un mensaje en una ventana emergente de Aranda 360.	Ingrese el mensaje que se mostrará en la ventana emergente. Mensaje: Usted debe actualizar el antivirus.
Miscelánea > Log	Genera nueva información para registrarla en el log generado por el agente. Este log se puede ver en: Software, bajo la opción MONITOREO DE LOG (en el panel de administración) en la consola. El nombre del log	Ingrese el mensaje que se mostrará en el log.

Tabla 11.5: Definición de acciones predefinidas (hoja 2 de 3

ACCIÓN	DESCRIPCIÓN	PROPIEDADES
Miscelánea > Esperar	Detiene la ejecución de un script.	Ingrese en segundos el tiempo que debe esperar un script para reanudar su ejecución.
Red > Desactivar Interfaces de Red	Desactiva las interfaces de red para un agente.	Seleccione como se desactivarán las interfaces de red para un agente: - Tipo: - lista blanca: Todas las interfaces de red estarán deshabilitadas a excepción de las mencionadas en la lista. Esta acción se mantiene activa hasta que se realice una revisión completa de un proceso por lotes, ejecutada por un agente, ó con una llamada explícita desde un archivo de lotes a las "Restricciones NIC Flush". - lista negra: Solo se desactivan las interfaces mencionadas en la lista. - Valores: Tarjeta de red. Para deshabilitar todas las interfaces de red en la lista blanca, debe ser ingresado un valor del tipo 0:000000000. Tras hacer clic en Valores en el panel de Propiedades, selecciónelo del cuadro de dialogo. Las Interfaces de red pueden ser añadidas por el administrador o importadas de la base de datos.
Red > Restricciones Flush NIC	Cancela la acción "Desactivar interfaces de red". Las interfaces de red no se activan automáticamente.	
Control de Red	Asigne un valor a la variable "Control de Red". Puede ser usado por clientes TNC (Trusted Network Connect) como clientes de acceso Odyssey en redes Juniper (R).	Establezca un estado de control de red a cualquiera de las siguientes opciones: - Permitir, - Aislar, - No permitir acceso, - No hay recomendaciones.
	Para más información de UAC (user acces control) de Juniper, vea ¿"Como instalar el modulo de usuarios con control de acceso?	
Cifrado > Bloquear descarga de archivo	Activa/Desactiva descarga de archivos. Cuando la descarga de archivos está bloqueada, el usuario no tendrá acceso a ellos (incluso autenticado).	
Cifrado > Permitir reinicio automático	Activa / Desactiva el reinicio automático (sin obligar el ingreso de contraseña) para el cifrado de todo el disco.	

Tabla 11.5: Definición de acciones predefinidas (hoja 3 de 3)

ACCIONES DEFINIDAS POR EL USARIO

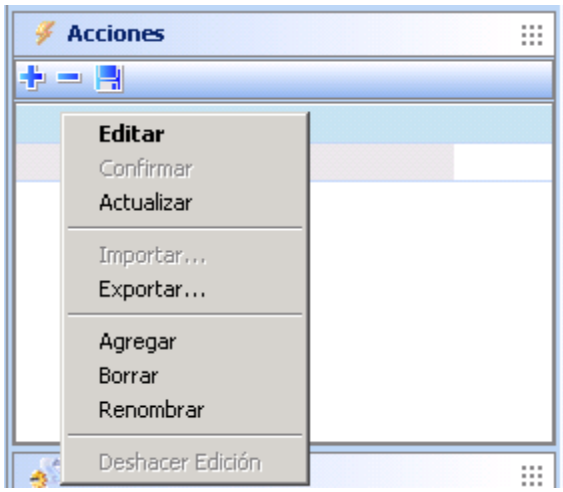
Las acciones definidas por el usuario son acciones previamente creadas por usted u otro administrador.

Las acciones definidas por un usuario pueden ser incluidas en los scripts de pruebas y en los de procesos por lotes.

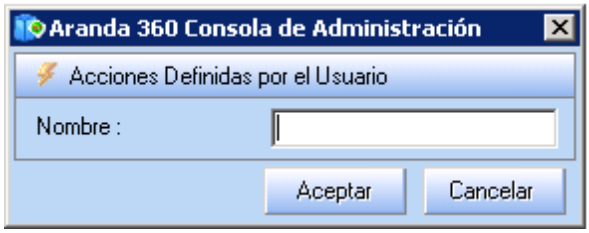
CREANDO UN SCRIPT DE ACCIONES

Para crear un script de acción, siga los siguientes pasos:

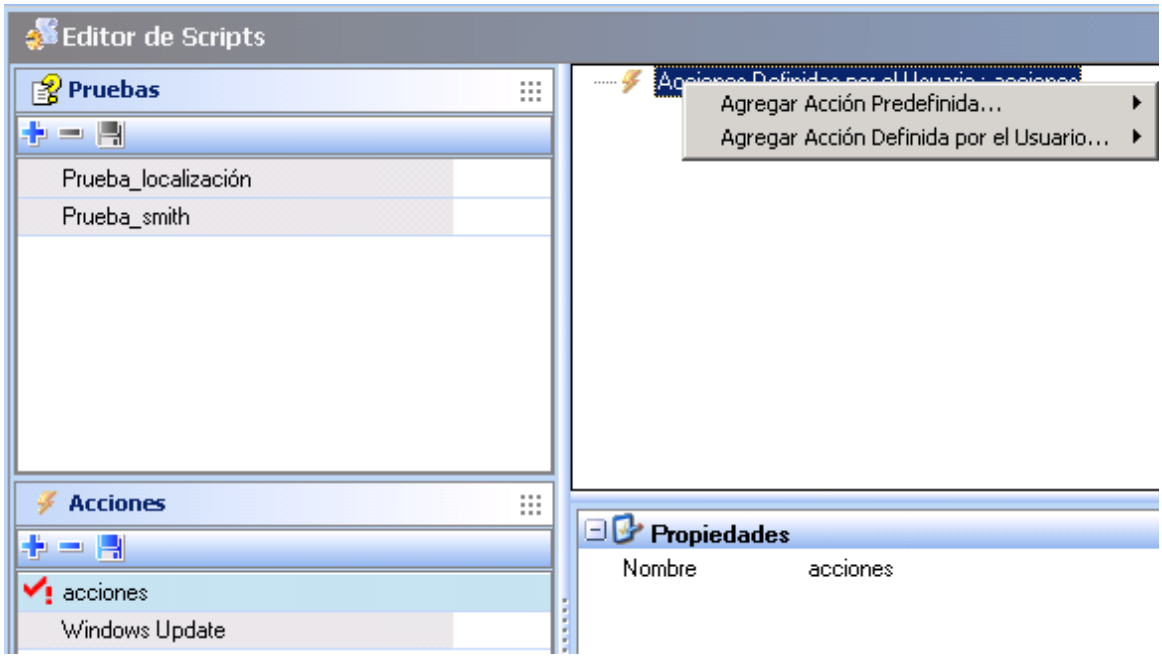
1. En el área de acciones del editor de scripts.
   - Clic-derecho sobre cualquier parte dentro del área.
   - Seleccione Adicionar del menú desplegable o directamente en l icono de la barra de herramientas.



   - Nombre el script de acciones.



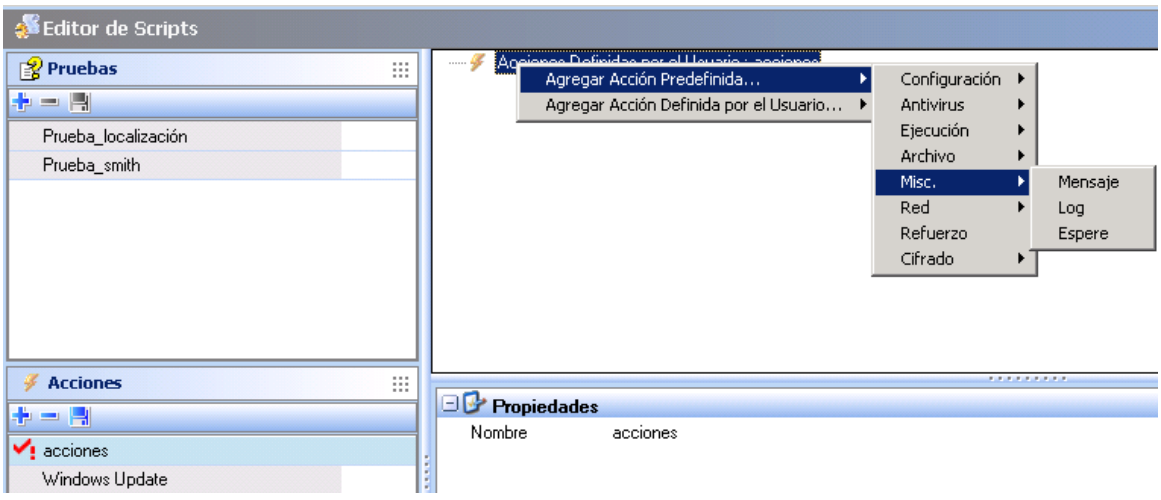
2. En el área de trabajo, haga clic-derecho en el icono para mostrar el menú desplegable Adicionar.



3. Para visualizar las acciones de primer nivel que están disponibles, seleccione una de las siguientes opciones:

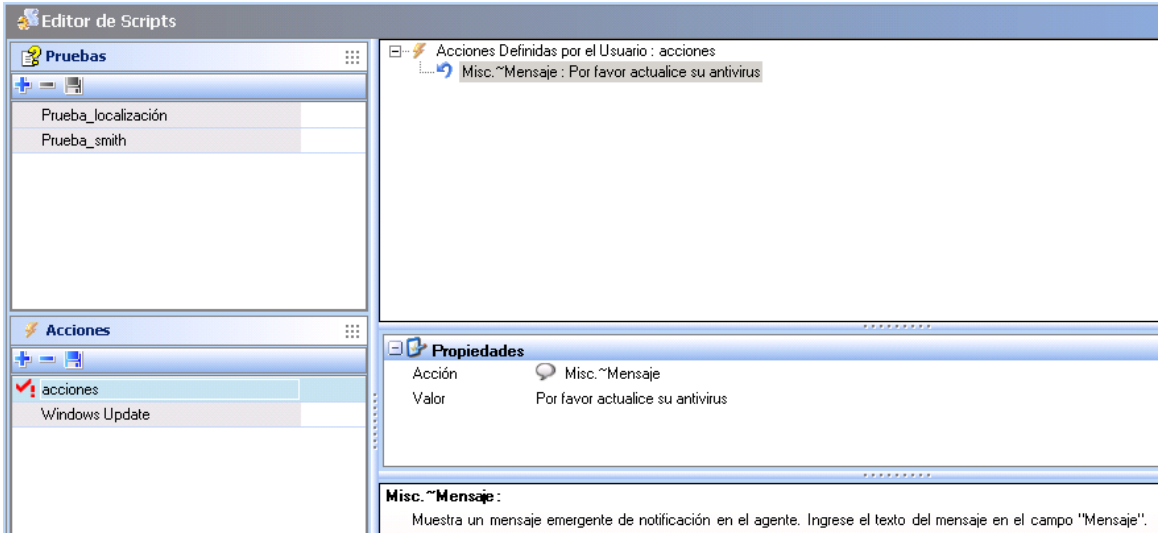
   - Adicionar acción predefinida.
   - Adicionar acciones definidas por el usuario.

4. Seleccione una acción de Segundo nivel (Ejemplo: Miscelánea. > Mensaje).



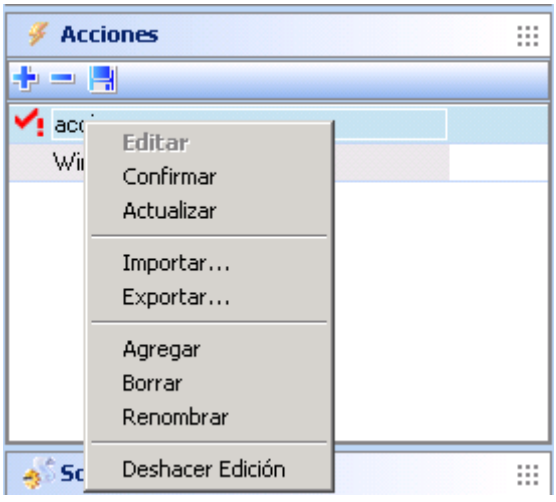
La acción se agregará al script. Ahora debe especificar las propiedades.

5. Clic en la acción para mostrar sus propiedades. Ingrese y/o la información requerida usando el botón ... .



6. Cuando haya terminado de crear el script de acción:

- Haga clic-derecho en el script de acción ubicado en el Panel de acciones.
- Seleccione Registrar.



SCRIPTS PARA PROCESOS POR LOTES

GENERALIDADES

Los Procesos por lotes le permiten combinar pruebas y acciones con el fin de crear scripts más complejos y potentes, los cuales se pueden aplicar a políticas de red y configuraciones.

Los scripts de Procesos por lotes incluyen:

- Declaraciones:
  Las declaraciones utilizan operadores lógicos booleanos SI Y, SI O y SI NO.

- Pruebas predefinidas:
  Las pruebas predefinidas se utilizan usualmente en las pruebas suministradas por Aranda 360 (Ejemplo: "Proceso" el usuario verifica la ejecución de un proceso).

- Pruebas definidas por usuario:
  Las pruebas definidas por usuario son pruebas creadas por usted u otro administrador.
  Consisten en:
  - Declaraciones.
  - Pruebas predefinidas.
  - Pruebas definidas por otros usuarios.

- Acciones predefinidas:
  Una acción predefinida se utiliza usualmente en las acciones suministradas por Aranda 360 (Ejemplo: "Ejecución de Proceso" para iniciar un proceso).

- Acciones definidas por el usuario:
  Las acciones definidas por un usuario son acciones creadas por usted u otro administrador.
  Consisten en:
  - Declaraciones.
  - Acciones predefinidas.
  - Acciones definidas por otros usuarios.

RESULTADOS VERDADERO/FALSO

Cuando se adiciona un nuevo proceso por lotes, automáticamente se añaden las acciones que se ejecutaran según los resultados, ya sean Verdaderos o Falsos.

Otras acciones que se deseen ejecutar según los resultados obtenidos deben ser adicionadas.

Puede crear un archivo por lotes para comprobar que cualquier estación de trabajo ha tratado de conectarse teniendo instalado un antivirus. Si no cumple con esto, el proceso por lotes será configurado para denegar el acceso de red.

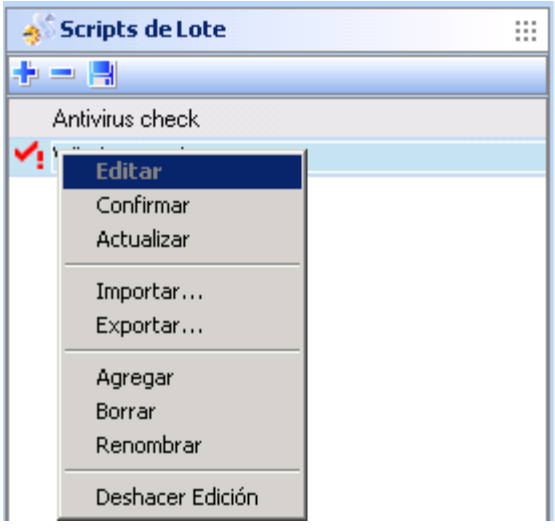
El proceso por lotes contiene pruebas y acciones que se ejecutarán según los resultados obtenidos.

- El administrador no puede eliminar un script (prueba, acción o proceso por lotes) utilizado por otro script

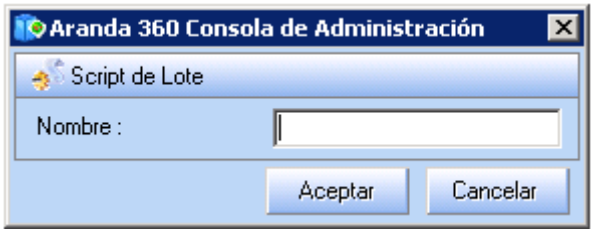
CREANDO UN SCRIPT PARA PROCESOS POR LOTES

Para crear un script de procesos por lotes, siga los siguientes pasos:

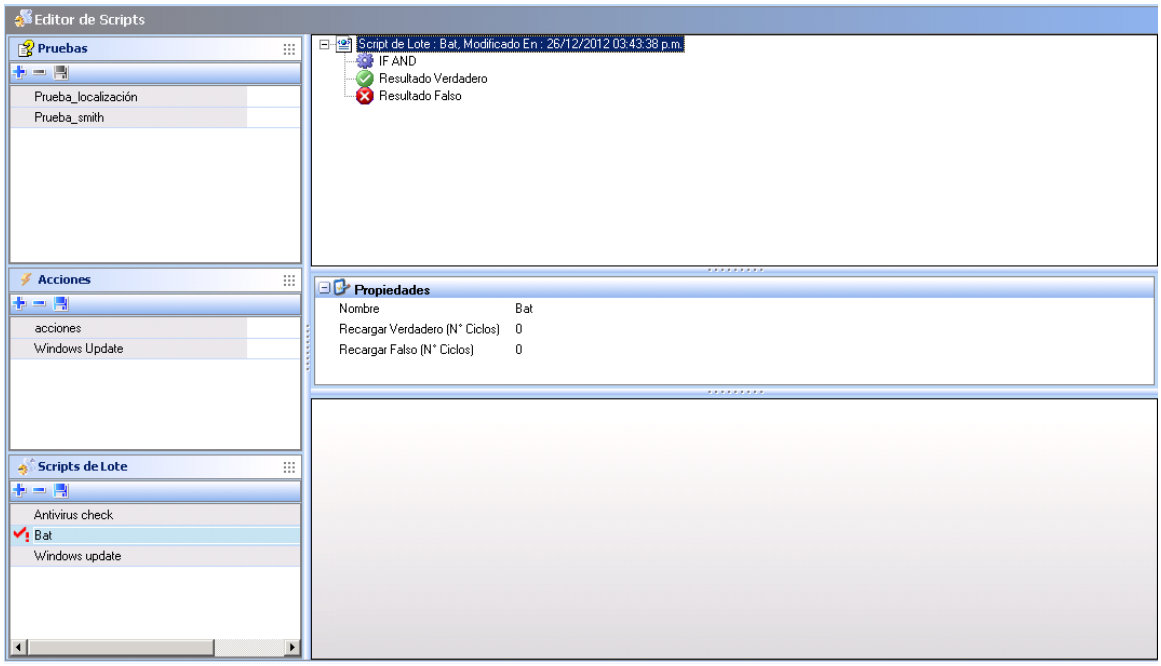
1. En el panel de procesos por lotes del Editor de scripts:
   - Clic-derecho en el área de los procesos por lotes.
   - Seleccione Adicionar del menú desplegable o haga clic directamente en el icono de la barra de herramientas.



   - Ingrese el nombre del proceso por lotes.

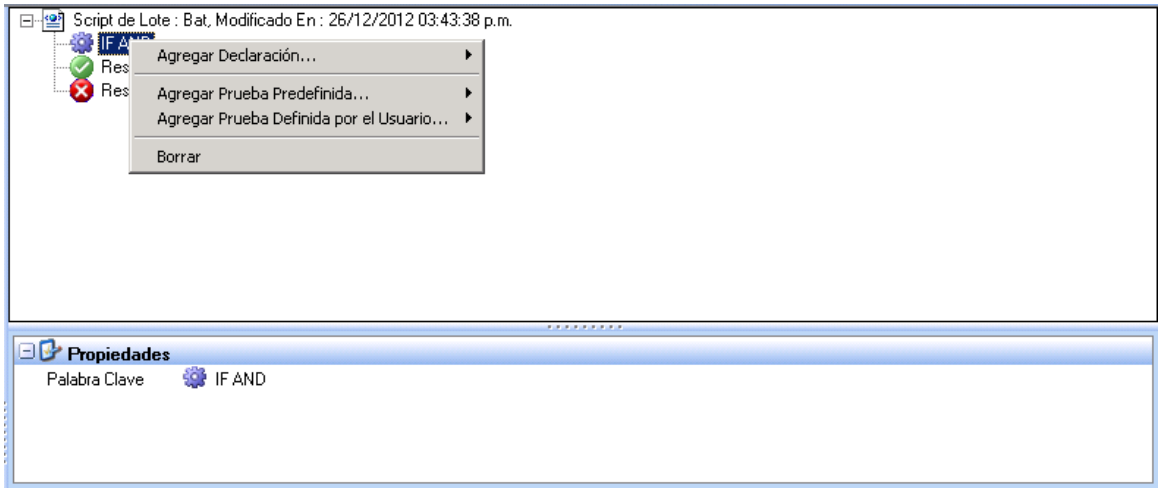


   - Puede modificar el nombre del lote, haga doble clic en el campo Nombre del panel de propiedades.



2. Clic-derecho en la declaración mostrada por defecto (SI Y) y haga clic en alguna de las siguientes opciones:

   - Adicionar declaración.
   - Adicionar prueba predefinida.
   - Adicionar prueba definida por usuario.



3. Para cambiar la declaración por defecto (SI Y) o adicionar una nueva:
   - Clic en la declaración SI Y en el panel superior.
   - Clic en la declaración en el panel de propiedades.
   - Clic en el botón ... para explorar la lista de declaraciones.
   - Seleccione la declaración deseada del menú desplegable.

4. Si ha adicionado una prueba, especifique sus propiedades.
5. Clic-derecho en el icono de resultado verdadero o en el de Resultado falso para mostrar la lista de acciones asociadas a estos resultados.
   Ambos iconos son generados por defecto cuando se crea un proceso por lotes
6. Adicione las acciones requeridas, pruebas y declaraciones en su script de procesos por lotes (Ejemplo: Actualización de Windows.)
7. Para aplicar el script de procesos por lotes a un grupo de agentes:
   - Diríjase a Grupos de agentes en el Administrador de ambientes.
   - Edite el grupo de agentes asociado al proceso por lotes.
   - Clic en la pestaña de scripts.
   - Seleccione la prueba que se desea asociar al grupo de agentes (conectado, desconectado el valor verdadero es el valor por defecto).
   - Seleccione el proceso por lotes para aplicarlo a un grupo de agentes.

   - Verifique sus cambios.

Ejemplo 1

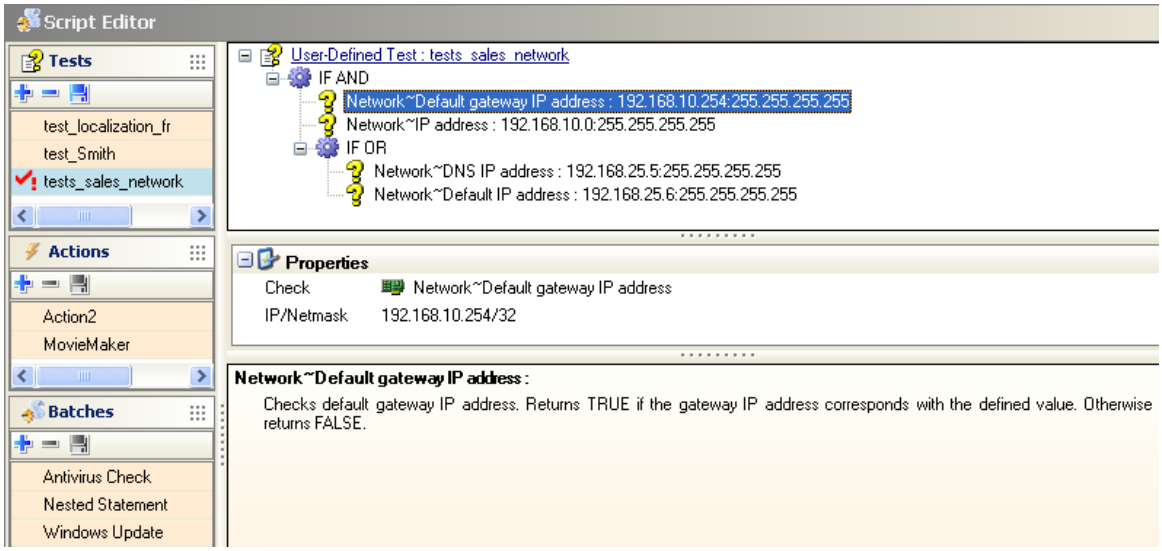
Realizando pruebas para verificar que una estación de trabajo este en red

Para verificar que una estación de trabajo está en red, siga los siguientes pasos:

1. Cree un script para pruebas llamado "test_sales_network" para comprobar si el computador esta en red:

   - Adicione una declaración SI Y.
   - Adicione la prueba predefinida Dirección IP por defecto del Gateway (puerta de enlace).

- En las propiedades, especifique:
  - La dirección ip del Gateway (puerta de enlace).
  - La dirección Ip asignada en la red.

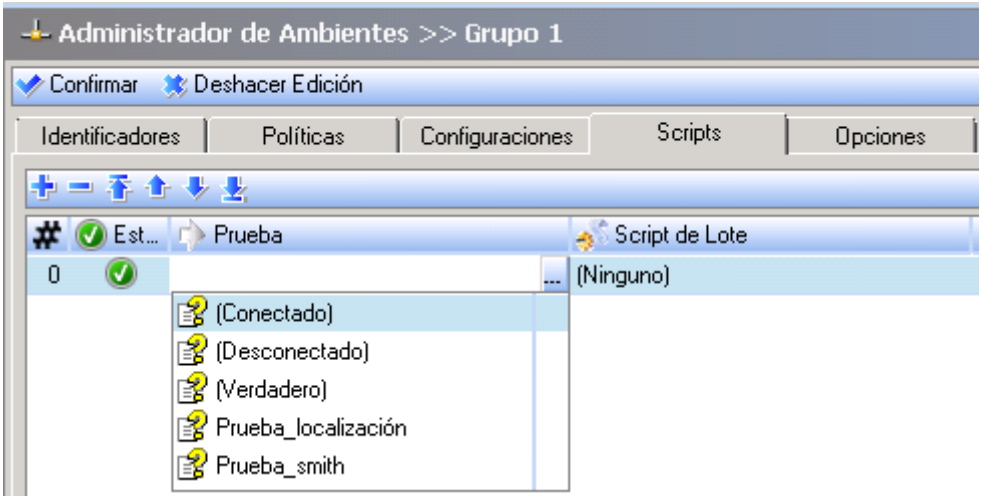


- Adicione una declaración SI O.
- Adicione la prueba predefinida DIRECCIÓN IP DEL SERVIDOR DNS.
- Adicione otra prueba predefinida DIRECCIÓN IP EN EL SERVIDOR DNS.
- En las propiedades para cada uno de los servidores DNS, especifique:
  - La dirección Ip del servidor.
  - La máscara de red.

2. Para aplicar la prueba a un grupo de agentes:

   - Diríjase al administrador de ambientes.
   - Seleccione y edite el grupo que será probado.
   - Clic en la pestaña scripts:
     - Clic en .

- En la columna pruebas, seleccione que será aplicada al grupo de agentes.



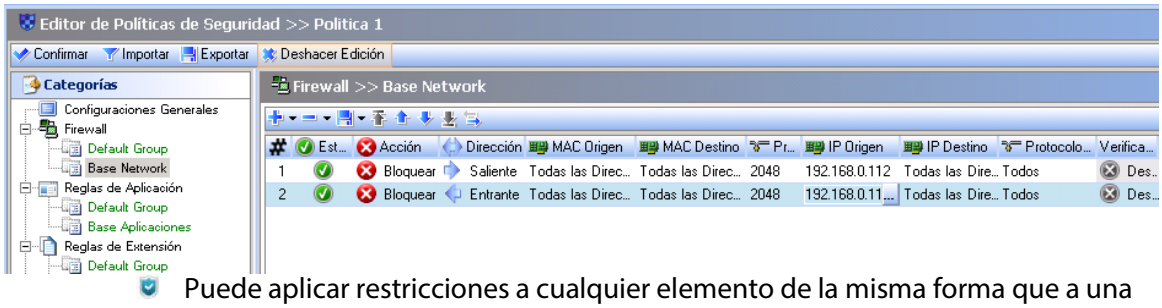
- Verifique sus cambios.

Ejemplo 2

Aplicando una política de cuarentena

Para aplicar una política de cuarentena, si el antivirus ha dejado de funcionar, siga los siguientes pasos:

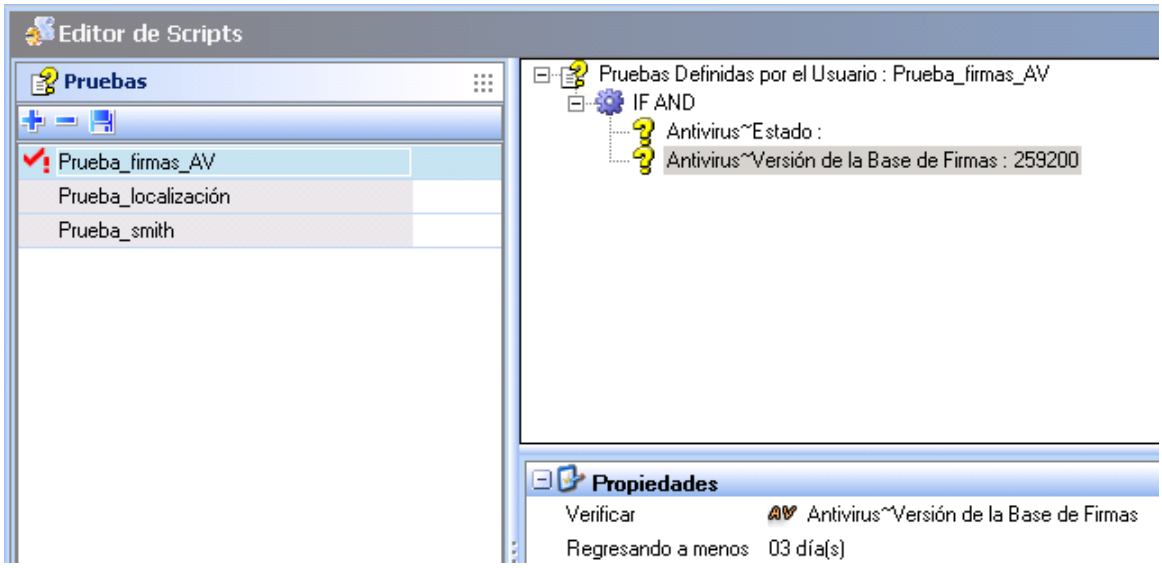
1. En el editor de políticas > Categorías > Firewall de Red, cree una política de cuarentena para restringir el acceso del servidor del antivirus a la red y además prohibir el acceso los servidores sensibles.



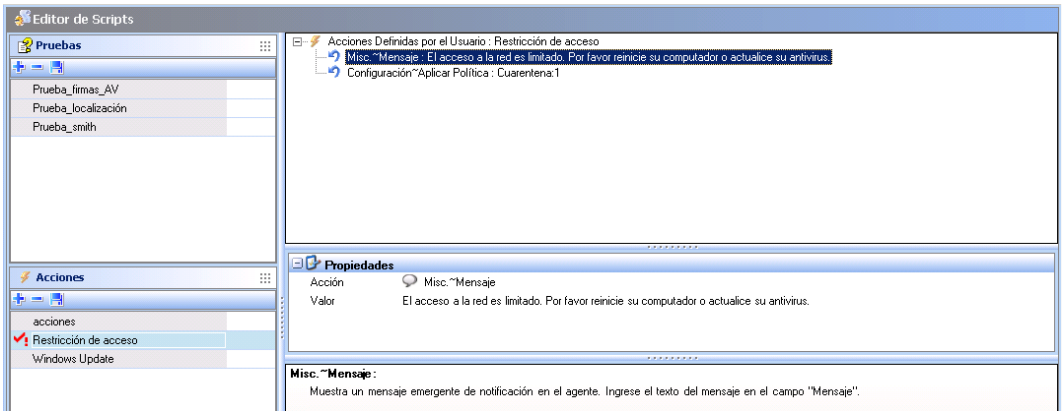
- Puede aplicar restricciones a cualquier elemento de la misma forma que a una política de seguridad (Ejemplo: prohibir la ejecución de programas específicos).

2. Crear una prueba llamada "test_antivirus" para comprobar que cuando un host se conecte al servidor de la empresa:

   - El antivirus este ejecutándose.
   - La versión de la base de datos de virus no sea mayor a 2 días



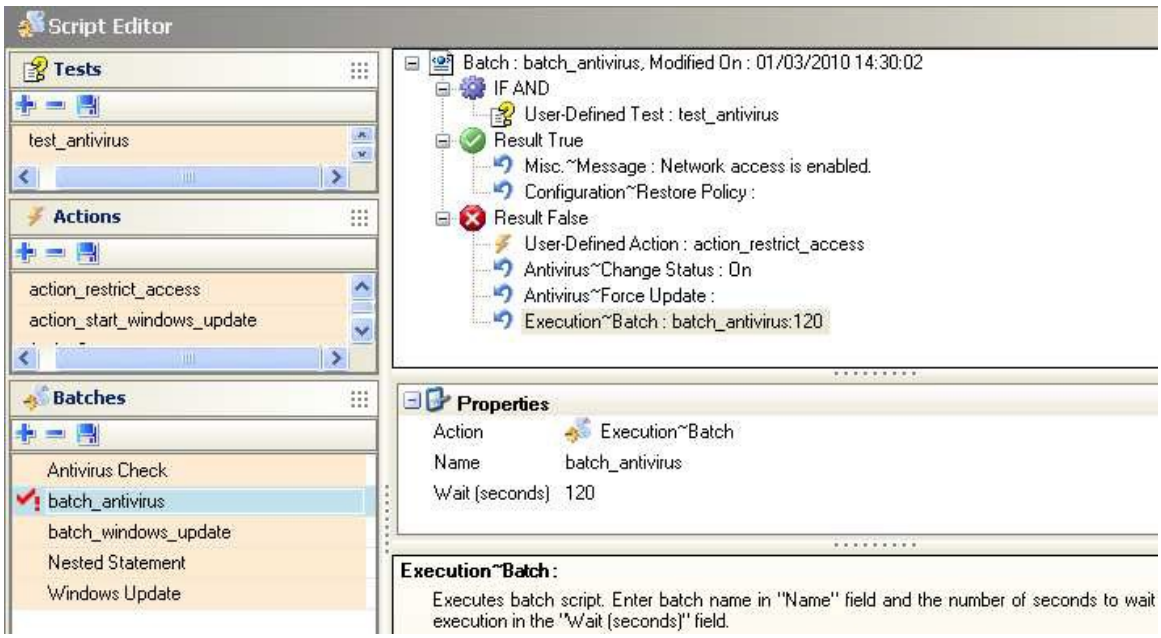
3. En la opción Editor Scripts > Pruebas, siga los siguientes pasos:
   - Adicione una declaración SI Y.
   - Dentro de la declaración, adicione las dos pruebas siguientes:
     - Antivirus > Estado:
       Con el fin de comprobar el estado del antivirus (Activo/Desactivo)
     - Antivirus > Versión de la base de datos de virus:
       En el panel de propiedades, introduzca la duración tras la cual se considera que el antivirus es obsoleto. En este ejemplo, 3 días se han convertido en segundos (259200 segundos en la sección superior de pruebas definidas por el usuario).
4. En la opción Editor Script > Acciones, cree una nueva acción llamada "action_restrict_access".
   Usted aplicara esta acción para usarla en la política de cuarentena.



5. En las acciones definidas por el usuario "aación_restricción_de_acceso", siga los siguientes pasos:

   - Adicione una acción del tipo Miscelánea > Mensaje para informar al usuario.
   - Adicione una acción del tipo Configuración > Aplicar política:
     - Seleccione la política de cuarentena que se creó en el primer paso.
     - Seleccione la Temporalidad.
       Si el computador se desconecta, la política de seguridad permanente será aplicada nuevamente.

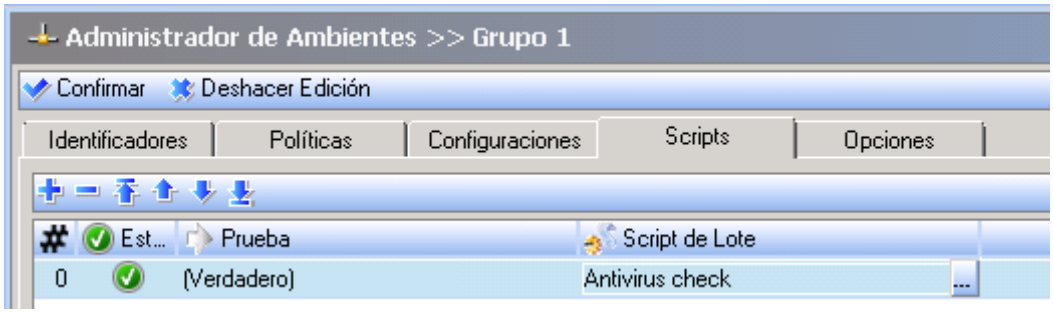
6. En la opción Editor Scripts> Procesos por lotes, cree un proceso por lotes para asociarlo con las acciones necesarias de la prueba:



   - Adicione una declaración del tipo SI Y.
   - Adicione la prueba definida por usuario "prueba_antivirus" que se creó en el paso dos
   - Adiciones en los resultados VERDADEROS las acciones que tendrán que ser ejecutadas si el resultado de la prueba es VERDADERO:
     - Una acción de tipo Miscelánea > Mensaje indicara que el acceso a la red es permitido.
     - Una acción de tipo Configuración > Restaurar Política restaurar la política permanentemente.
   - Adicione en los resultados Falsos:
     - La acción definida por usuario "acción_restrngir_acceso" para aplicar una política de cuarentena.
     - La acción predefinida Antivirus > Cambio de estado. Indicando que debe estar activado en el panel de propiedades.
     - La acción predefinida Antivirus > Forzar Actualización.

- Una acción del tipo Ejecución > procesos por lotes para ejecutar la prueba cada 2 minutos (120 s).

7. Para aplicar el proceso por lotes a un grupo de agentes, siga los siguientes pasos:
   - Diríjase al administrador de ambientes.
   - Seleccione y edite un grupo de agentes.
   - Haga clic en la pestaña Scripts:
     - En la columna de pruebas, seleccione (VERDADERO).
     - En La columna de procesos por lotes, seleccione el proceso por lotes que será aplicado al grupo de agentes.



   - Verifique sus cambios.

Ejemplo 3

Verificando que el servicio de Actualización de Windows se esté ejecutando

Para poder verificar que el servicio de actualización de Windows se está ejecutando, usted necesitara crear los siguientes scripts:

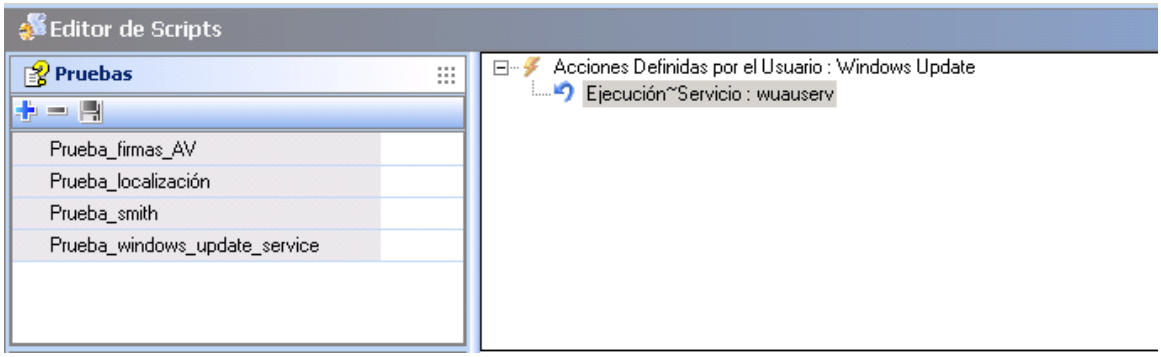
- Un script de pruebas
- Un script de acciones
- Un script para procesos por lotes.

Podrá incluir una acción para forzar la ejecución del servicio en caso de que el servicio no se esté ejecutando.

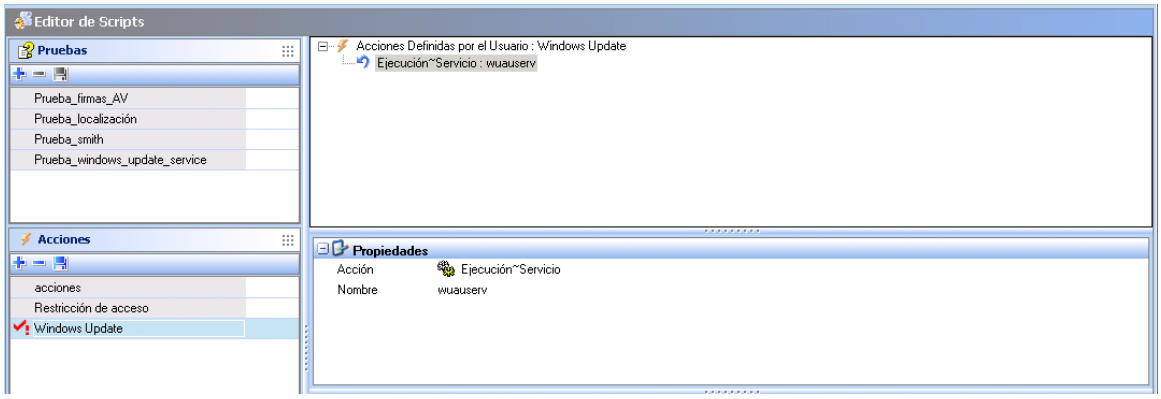
Para verificar que el servicio de actualización de Windows se está actualizando, siga estos pasos:

1. En el Editor de Scripts > Pruebas, cree una prueba llamada "test_windows_update_service".
   - Adicione una declaración SI Y.
   - Dentro de la declaración:
     - Adicione la acción Servicio > Probar estado.
     - Ingrese el nombre del servicio de actualización de Windows: wuauserv.

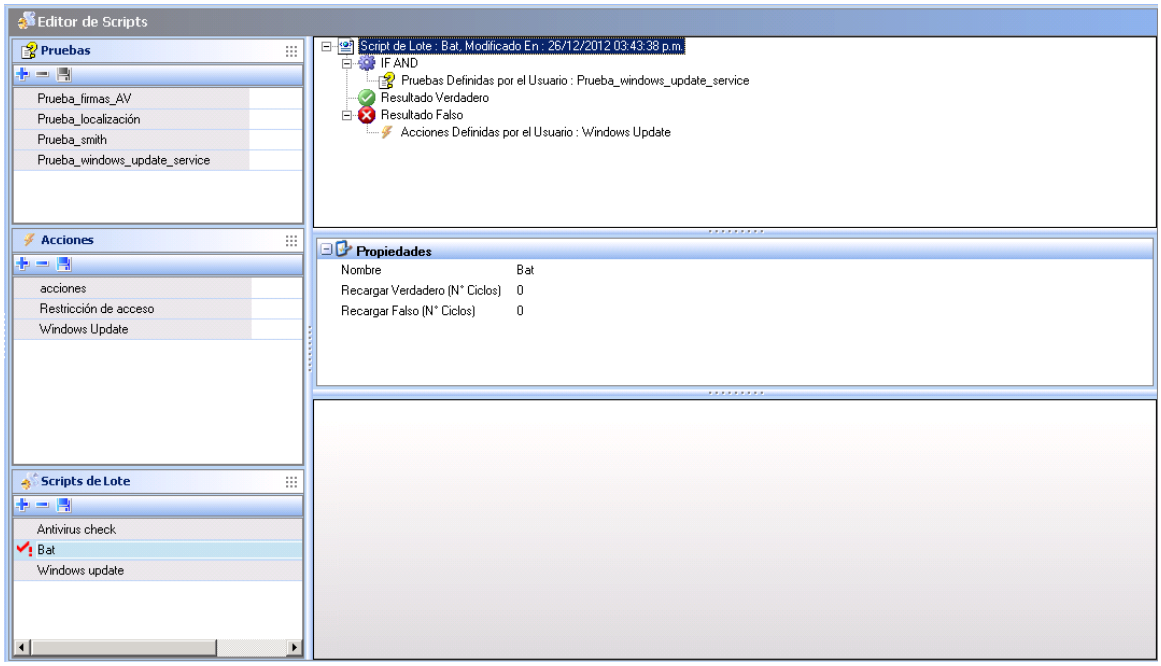
La prueba devolverá falso si el servicio no está ejecutándose.



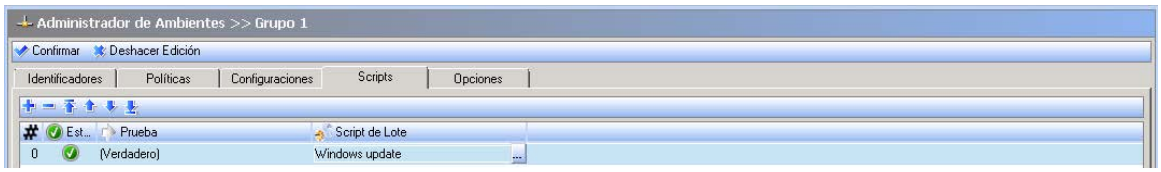
2. En el Editor de Script > Acciones, cree una nueva acción llamada "action_start_windows_update_service".
    - Adicione Ejecución > Acción de Servicio.
    - Ingres el nombre del servicio de actualización de Windows: wuauserv.



3. En el Editor de Scripts > Procesos por lotes, cree un Nuevo proceso por lotes:
    - Adicione una declaración SI Y.
    - Dentro de la declaración, adicione la prueba definida por usuario "test_windows_update_service" que se creó en el paso 1.
    - Para los resultados falsos, adicione la acción definida por usuario "action_start_windows_update_service" que fue creada en el paso 2.



4. Para aplicar el proceso por lotes a un grupo de agentes:
    - Diríjase al administrador de ambientes.
    - Selección y edite el grupo que estará relacionado con el proceso por lotes.
    - Haga clic en la pestaña Scripts:
        - En la columna pruebas, seleccione (Verdadero).
        - En la columna de procesos por lotes, seleccione el proceso por lotes que se le aplicara al grupo de agentes.



- Verifique sus cambios.

SCRIPTS DE ACCIÓN TEMPORAL

GENERALIDADES

Los scripts de acciones temporales son scripts configurados en la consola de administración de Aranda. Una acción temporal se aplica a un agente de Aranda 360 temporalmente.

Los usuarios solicitan la ejecución de acciones temporales a través de solicitudes.

El administrador gestiona estas solicitudes por medio de la consola de administración de Aranda.

La aplicación de una acción de carácter temporal de ninguna manera remplazará la aplicación convencional de una política, una configuración ó procesos por lotes definidos por el administrador y dedicados a un entorno específico.

Una política definida a un escenario específico no se puede restaurar utilizando un script de acción temporal.

Los scripts para procesos por lotes y scripts de acciones temporales son iniciados por el administrador. El usuario solo puede solicitarlos.

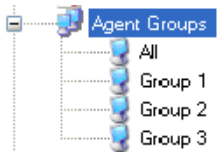
Los Scripts temporales de acción se detallan en esta sección de acuerdo a un orden cronológico:

- El administrador aplica una medida temporal a un grupo de agentes.
- El usuario envía una solicitud de acción temporal para el administrador.
- El administrador gestiona las solicitudes de acción temporales enviadas por el usuario.
- El usuario revisa las acciones temporales en curso.
- El usuario detiene una acción temporal en curso.

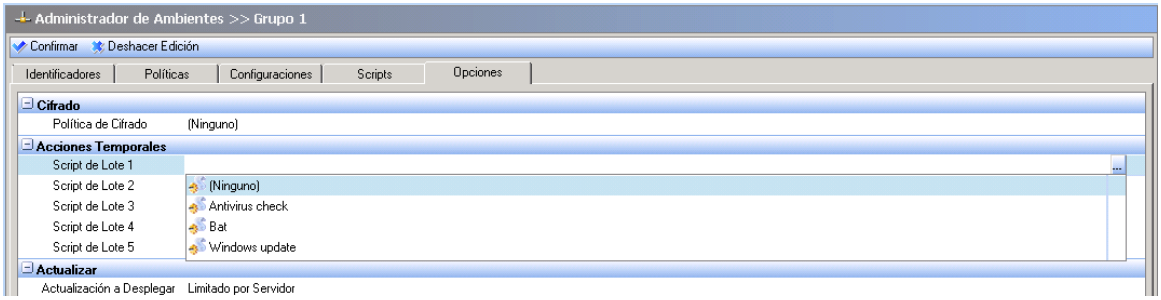
Aplicando una acción temporal a un grupo de agentes por parte del Administrador

Para aplicar una acción temporal a un grupo de agentes, el administrador debe seguir los pasos descritos a continuación:

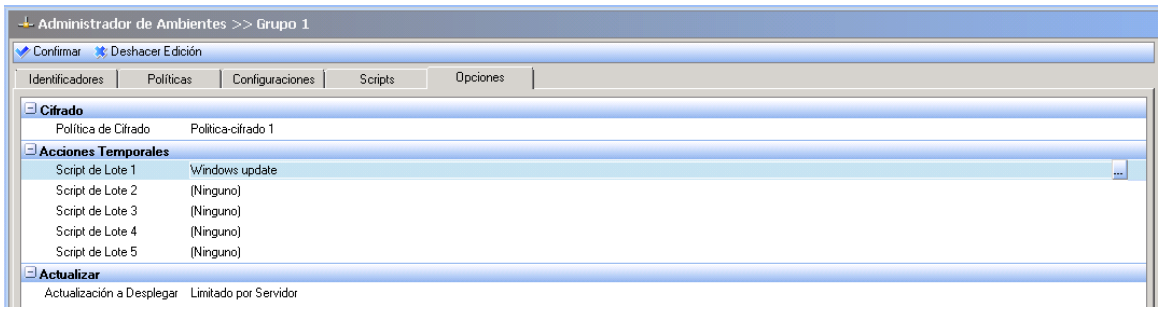
1. En el administrador de ambientes, haga clic en el grupo de agentes al que se le asociará la acción temporal.



2. Haga clic en la pestaña de Opciones.
   Una lista de los procesos por lotes numerados, sin parámetros, se muestra por defecto.



3. Haga clic sobre cualquier proceso por lotes para ver el botón ... .
   El administrador podrá accede a la lista.
4. Para usar un script de procesos por lotes como una acción temporal, selecciónelo del menú desplegable.
   El proceso por lotes se asociara al grupo que está siendo editado.



Los scripts usados como acciones temporales son creados en el EDITOR de Scripts

Usuario realizando una petición de acción temporal al administrador por parte del usuario

Recordatorio

Antes de aplicar una acción temporal, el usuario debe solicitar los permisos necesarios al administrador. Esto se realiza con una solicitud de acción temporal.

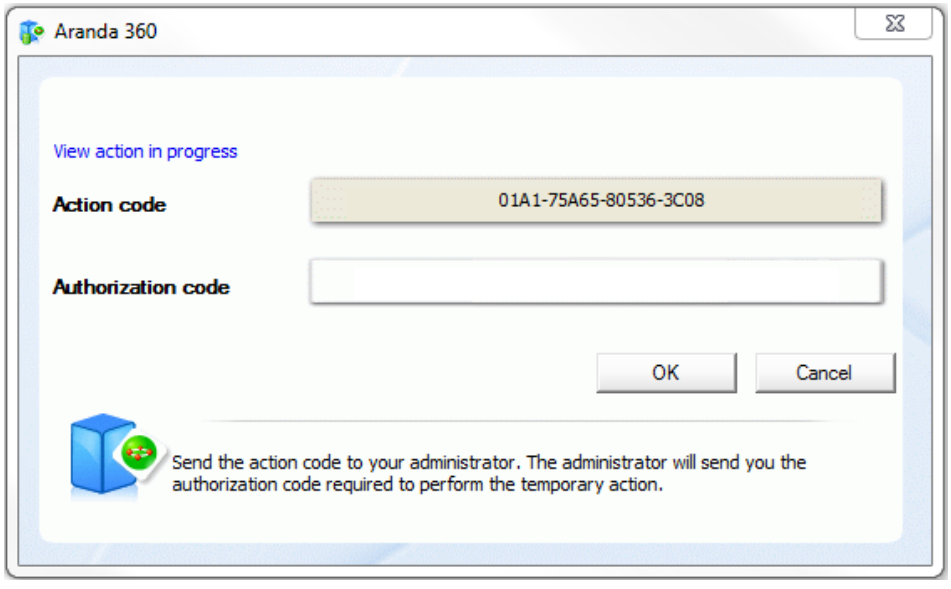
El administrador es el encargado de seleccionar el tipo de acción temporal y el tiempo durante el cual se aplicara. El administrador escogerá la acción y el tiempo que permanecerá activa a través de la consola de administración.

Procedimiento

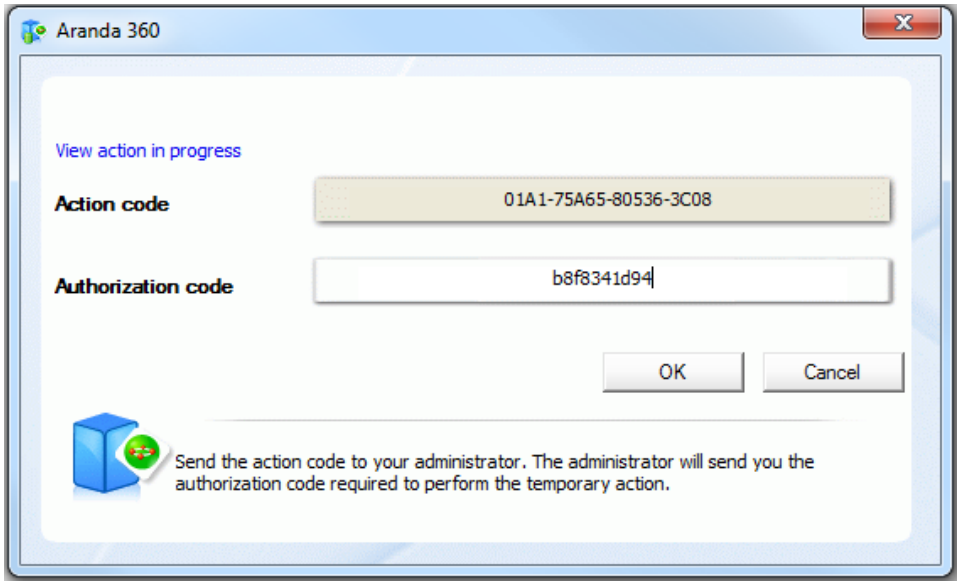
Para enviar una solicitud de acción temporal, el usuario debe seguir el siguiente procedimiento:

1. Hacer clic-derecho en el icono del monitor de Aranda 360 and hacer clic en el submenú Otras operaciones >Acciones temporales Personalizadas.

2. Enviar el código para la Acción que verá el administrador.
   A cambio, el administrador le hará llegar un código de autorización.



3. En el campo del Código de autorización, ingrese le código suministrado por el administrador.



4. Haga clic en OK.

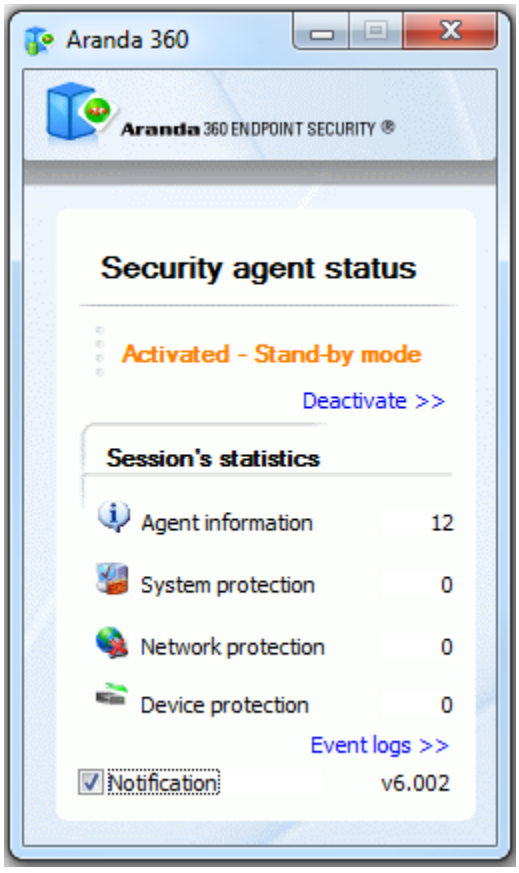
La acción temporal seleccionada por el administrador se activara desde la consola con el tiempo especificado por este.

- Si el administrador selecciona Desactivar Protecciones, el usuario tendrá que esperar por lo menos 30 segundos para permitir que el proceso de protección del agente sea detenido. De otra forma, la acción será ejecutada inmediatamente.

5. Para verificar que la acción temporal está en proceso:

   - Haga clic-derecho en el icono del monitor de Aranda 360.
   - Seleccione Estado o Ver eventos del log.

   Esta es la ventana de Estado que muestra las protecciones desactivadas para una acción temporal (Modo stand-by):



Administrador manejando los requerimientos de acción temporal enviados por el usuario (retos)

Recordatorio

Escenario 1: El usuario envía una solicitud para una acción temporal. El administrador recibe el código generado para la acción (una clave para el agente).

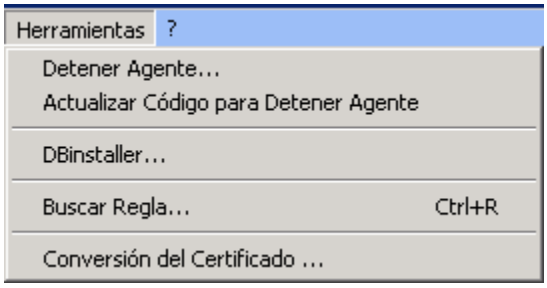
Escenario 2: El administrador genera un código de autorización para la acción temporal.

Escenario 3: El usuario ingresa el código de autorización para dar inicio a la acción temporal en su estación de trabajo.

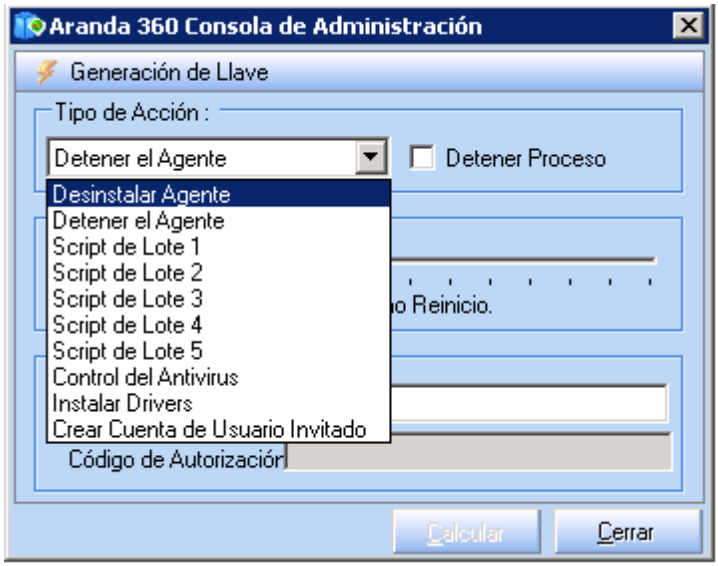
Procedimiento

Para dar respuesta a una petición de un usuario para una acción temporal, el administrador debe seguir estos pasos:

1. En la consola de administración, seleccione Herramientas > Administración de solicitudes.

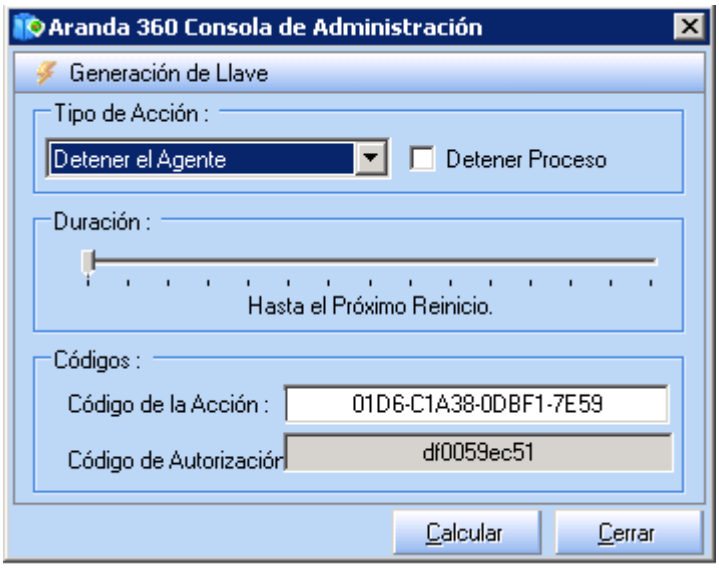


2. Defina los siguientes parámetros:

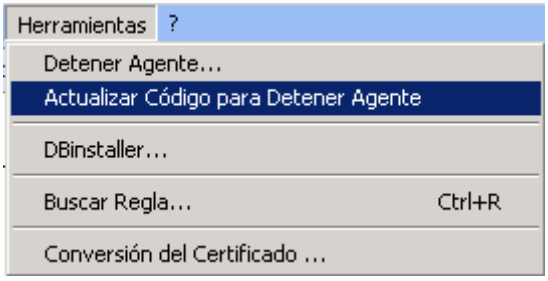


- Tipo de acción usando para mostrar la lista de las acciones temporales.
  Si marca la casilla delante de Protecciones desactivadas, DETENCIÓN TOTAL, el agente se detendrá completamente y no se cambiara de modo de espera a Activado. Por lo tanto no se registrara el log ni se aplicara la política.
- Duración de la acción temporal deslizando el cursor por la línea de tiempo.
- Ingresar el código de la acción enviado por el usuario.

3. Clic en Calcular para obtener el código de autorización.



4. Enviar el código al usuario.
    - Si el administrador quiere generar nuevamente un código, debe hacer clic directamente en Herramientas > Obtener nuevamente clave de solicitud.



Desplegando acciones temporales en progreso por parte del usuario

El usuario puede consultar que acciones temporales se están ejecutando en su estación de trabajo haciendo clic en Otras operaciones > Acciones temporales personalizadas en progreso.

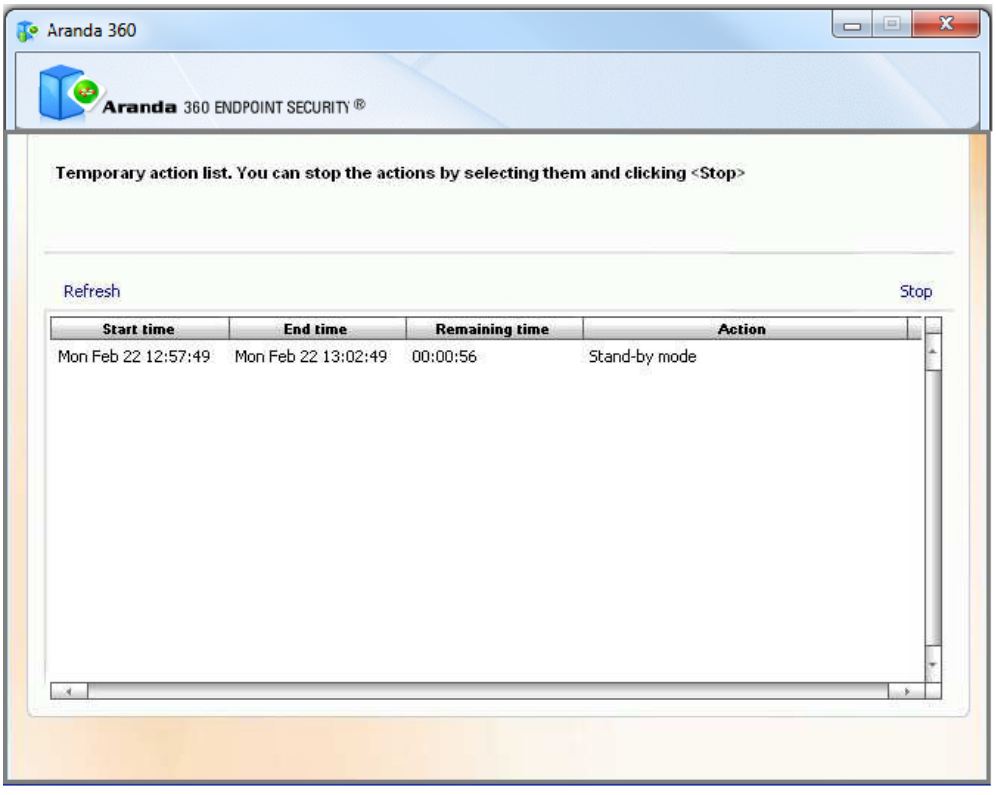
La información que se mostrara para las acciones temporales en progreso es:

- Tiempo de inicio:
  Es el tiempo cuando el agente aplica la acción.

- Tiempo de finalización:
  Es el tiempo cuando la acción temporal se detiene.

- Tiempo restante:
  Es el tiempo que resta para que la acción se detenga.

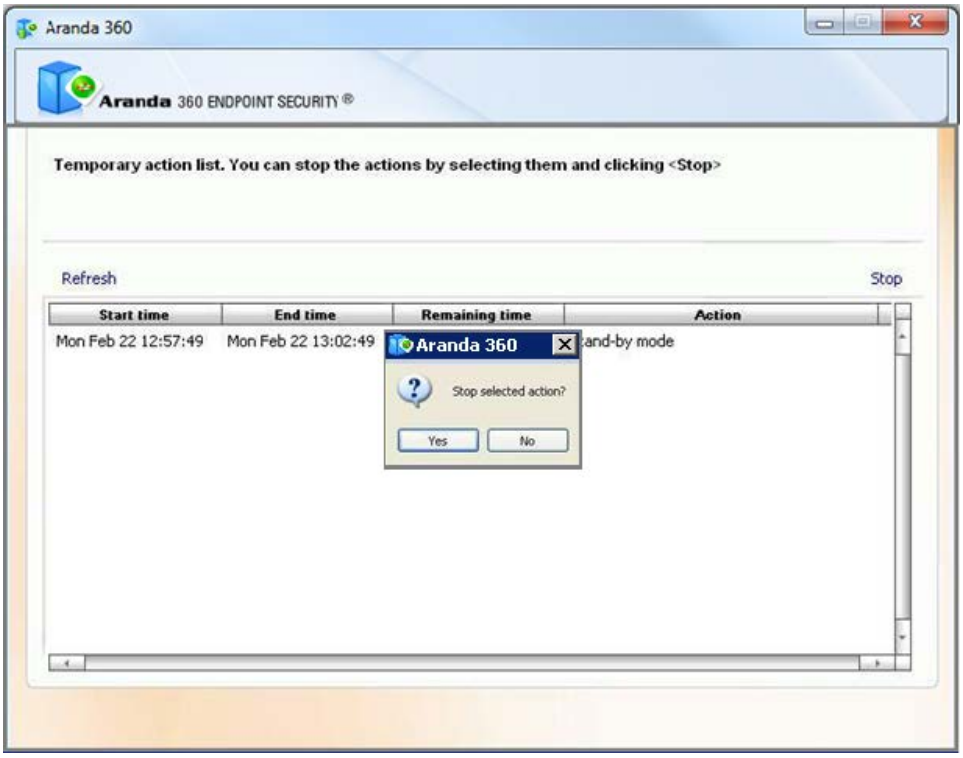
- Acción:
  Es el tipo de acción temporal que es aplicada por el agente.



Deteniendo acciones temporales en progreso por parte del usuario

Para detener una acción temporal en progreso el usuario debe:

1. Hacer clic-derecho en el icono del monitor de Aranda 360 .
   - o Seleccione Otras operaciones > Acciones temporales personalizadas en progreso. Se mostrara la lista de acciones temporales en progreso.
2. Seleccione la acción temporal que va a detener.
3. Haga clic en Detener y luego SI.



4. El resultado aparecerá en la ventana

CARGANDO ARCHIVOS DESDE EL SERVIDOR PRINCIPAL

Generalidades

El administrador puede utilizar la consola de administración de Aranda con el fin de:

- Subir archivos desde el servidor principal.
- Distribuir archivos a los agentes.
- Distribuir esos archivos a servidores secundarios.

Por ejemplo, se pueden subir y distribuir archivos con scripts para ser aplicados a los agentes.

Cabe señalar que sólo un archivo se puede cargar y desplegar a la vez.

Sus características deben ser las siguientes:

- El tamaño máximo del archivo no puede exceder un 1 MB.
- El archivo cargado será renombrado automáticamente por Aranda 360 con el nombre upload_file.srn.
- El Archivo distribuido entre los agentes quedara copiado en la ruta: [Aranda 360 Agent install dir]\batch].
- El archivo distribuido entre los servidores quedara copiado en la ruta: [Aranda 360 Server install dir\batch].

La extensión del archivo upload_file.srn implica que:

- Si la casilla de verificación en las REGLAS DE CONFIANZA no está marcada, no se permitirá el acceso al archivo.
- Sera denegado el acceso al archivo a todo aquello que no sea ejecutado por Aranda 360.

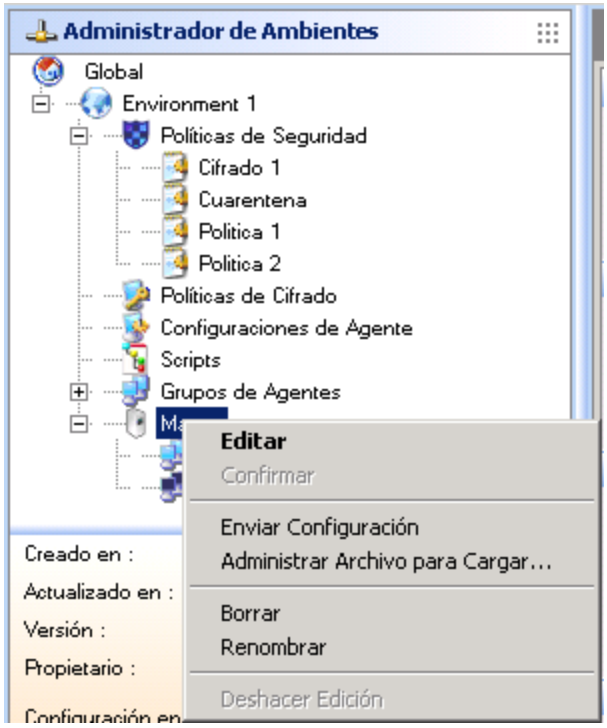
Cargando un archivo desde el servidor principal a los agentes

Procedimiento

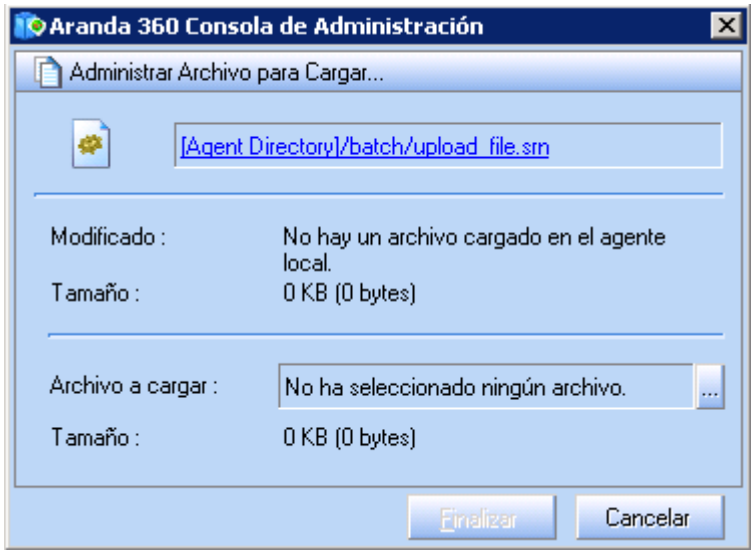
Para cargar un archivo desde el servidor principal a los agentes, el administrador debe ejecutar los siguientes pasos:

1. En el administrador de ambientes, hacer clic-derecho [Servidor principal].

El siguiente menú desplegable aparecerá:



2. Del menú desplegable, seleccionar Administrar archivo para cargar.
   Se mostrará la siguiente pantalla:



3. Hacer Clic en el botón de exploración junto al campo ARCHIVO A SUBIR.
   Se mostrará el explorador de Windows.
4. Seleccionar el archivo que se cagara.
   Si el archivo ha sido subido previamente, se mostrará una notificación indicándolo.

   - Si se intenta subir un archivo ya cargado, sin modificaciones, la carga será rechazada.

5. Hacer clic en Enviar.
   - El archivo será distribuido a los agentes.
   - Los servidores secundarios serán sincronizados.
   - El archivo será renombrado a upload_file.srn.
   - El archivo distribuido quedara en los agentes copiado en la ruta: [Aranda 360 Agent install dir]\batch].
   - El archivo distribuido quedara en los servidores copiado en la ruta: [Aranda 360 Server install dir\batch].

Ejemplo

El administrador puede distribuir un script a los agentes hacienda distinción entre estaciones de trabajo y portátiles. El script probará la presencia de baterías.

- El Script no está incluido con Aranda 360.

El Script debe escribirse de la siguiente manera:

- Si una bacteria es detectada, el script devolverá VERDADERO retornando al agente un valor de "1".
  Si el valor es retornado por un script en VBScript puede usarse la función "Wscript.quit(1)".
- De lo contrario, el script retornara FALSO al agente enviando un valor de "0".

Si el valor es retornado por un script en VBScript puede usarse la función "Wscript.quit(0)".

Para usar el script en una prueba o en un proceso por lotes, el administrador deberá usar la función EJECUTAR e ingresar la siguiente información:

Cscript.exe/E:Vbscript"c:\program files\Aranda\Aranda 360 Agent\ Batch\upload_file.srn"

/E:Vbscript se utiliza para indicar el formato de archivo (upload_file.srn) si la extensión no es .VBS.

- El administrador no debe usar el intérprete Wscript.

Si el Script Vbs permite el uso de argumentos, el administrador usara la función EJECUTAR declarando los argumentos como se muestra a continuación:

Cscript.exe/E:Vbscript"c:\program files\Aranda\Aranda 360 Agent\ Batch\upload_file.srn" Argumento1

o

Cscript.exe/E:Vbscript"c:\program files\Aranda\Aranda 360 Agent\ Batch\upload_file.srn" Argumento1 Argumento2

Capitulo 12 - CIFRADO DE DATOS

ACERCA DE ESTE CAPÍTULO

En este capítulo se describe cómo utilizar la característica de cifrado de datos para aumentar la seguridad de los datos que están en el disco duro y de los enviados a través de internet.

Esto incluye:

- Generalidades:
  - Propósito.
  - Características.
  - Sistemas soportados, hardware y software.

- Tipos de Cifrado:
  - Cifrado de archivos.
  - Cifrado del disco completo.

- Creando una política de cifrado:
  - Interfaz gráfica.
  - Procedimiento.

- Características de cifrado de archivos:
  - Seguridad multi-usuario.
  - Seguridad de información eliminada.
  - Opciones de cifrado de archivos.
  - Creación de contraseñas e inicios de sesión.
  - Sincronización.
  - Sincronización con múltiples usuarios.

- Parámetros de Cifrado:
  - Configuración general.
  - Parámetros de cifrado de archivos.
  - Parámetros de cifrado del disco completo.

- Aplicando una política de cifrado a un grupo de agentes.

- Recuperación de:
  - Recuperación de la contraseña para el cifrado de archivos.
  - Recuperación de datos de archivos cifrados (descifrado).
  - Recuperación de la contraseña para el cifrado del disco completo.
  - Recuperación de datos de cifrado de disco complete usando un CD de recuperación.

- Desinstalando agentes de Aranda 360:
  - Descifrado antes de la desinstalación.
  - Cambiando la cuenta de usuario en una máquina.

GENERALIDADES

Propósito

El Cifrado de datos ofrece una capa más de protección además de la contraseña de usuario.

Sus datos pueden ser:

- Guardados en disco duro.
- O enviados a usuarios que están tanto dentro como afuera de la red corporativa.

Al proteger los datos con el uso de contraseñas o cifrándolos en los discos duros,

los datos confidenciales están protegidos en caso de robo de computadora (ejemplo: ordenadores portátiles robados durante los viajes de negocios).

El cifrado de datos también protege los datos confidenciales de la empresa enviados por los usuarios a través de Internet.
Esta función generará una contraseña que el receptor deberá tener para poder abrir sus archivos. No es necesario que el receptor tenga Aranda 360 instalado.

Características

Estándar de cifrado avanzado

La característica de cifrado de Aranda 360 está basada en el estándar de cifrado de archivos, en ingles Advanced Encryption Standard (AES). Este es un sistema de cifrado simétrico el cual permite escoger claves con longitudes de 128, 192 o 256-bit para ser usadas en el ciframiento.

El estándar ha sido aprobado por el gobierno de los Estados Unidos para ser usado tanto en documentos clasificados como no clasificados.

Aranda 360 ha obtenido la certificación de cifrado Federal Information Processing Standard (FIPS) 140-2.

- Dos modos de CBC (Cipher Block Chaining) están disponibles en Cifrado de datos.

Ocultamiento

Una vez el administrador ha configurado las opciones de cifrado, el computador comenzara el proceso de sincronización. Los agentes del computador comenzaran a cifrar cada archivo o cada disco de la maquina (dependiendo de la política de cifrado aplicada).

- El cifrado de datos consiste en cifrar archivos o discos completos.
  El cifrado por archivos no excluye el cifrado por discos completos. Ambas opciones pueden ser ejecutadas al mismo tiempo.

Después del despliegue o distribución de la política de cifrado, los usuarios de Aranda 360 no notaran la ejecución del proceso de cifrado mientras trabajan en la computadora.

Sin embargo, existen algunos casos donde una barra de progreso será visible durante el cifrado (también llamado sincronización):

- Cambio de la política de cifrado.
- Transferencias de archivos de zonas sin cifrar a zonas cifradas.
- Recuperaciones

Para evitar que estos indicadores sean mostrados, el administrador puede activar

Modo invisible bajo la opción parámetros de cifrado de archivos.

El candado indica el cifrado ha sido aplicado a un archivo. Los archivos cifrados no se mostraran.

- Si el modo invisible esta desactivado, el administrador necesitara establecer una sesión con autentificación de Windows.

HARDWARE Y SOFTWARE SOPORTADO

Los sistemas operativos soportados son:

- Windows XP SP3 32bits.
- Windows Vista SP2 32bits.
- Windows 7 32bits.

El hardware y software que nos soportados son:

- Software RAID y discos dinámicos.
- Administración de particiones y herramientas para clonaciones de discos.
- Discos duros con tamaños de sectores diferentes a 512 bytes.
- Las particiones extendidas no son soportadas para el cifrado de disco completo. Solo los discos con particiones principales pueden ser cifrados.
- Multiarranque (varios sistemas operativos en una partición o en particiones separadas) no está soportado en el cifrado de disco completo.
- Gestores de arranque diferentes a el gestor de arranque de Microsoft Windows no está soportado en el cifrado de disco complete.

El Cifrado de datos es usado para cifrar discos duros. No es posible cifrar dispositivos extraíbles como memorias USB.

Por otra parte, el cifrado de dispositivos extraíbles, puede realizarse con la característica Cifrado de dispositivo extraíble disponible en Aranda 360.

- Antes de usar la característica de ciframiento, guarde todos sus datos.

- Si el disco duro cifrado incluye uno o varios sectores defectuosos, el cifrado podría ser interrumpido y todos los datos que hayan sido cifrados se descifraran nuevamente.
  Se recomienda realizar un escaneo del disco a detalle y reparar los sectores defectuosos antes de aplicar el cifrado de disco completo.

Justo después de aplicar la política de cifrado de disco completo, el desempeño puede verse afectado al comenzar una sesión de inicio.

Esto es absolutamente normal debido al hecho de que el cifrado se inicia antes de la pantalla de inicio.

Además, el agente tiene que conectarse al servidor Aranda 360 con el fin de implementar el cifrado del disco completo.

El cifrado o descifrado de disco complete no puede ser detenido una vez comience.

TIPO DE CIFRADOS

Estos son los dos tipos de cifrados que existen en Aranda 360:

- Cifrado de archivos.
- Cifrado del disco completo.

Cifrado de archivos
Sus características son:

- Solamente el contenido del archivo es cifrado.
- La lista de archivos es definida por el administrador.
- El sistema y los programas permanecen sin cifrar.

Las ventajas del cifrado de archivos son:

- Cada archivo normalmente se cifra con una clave de cifrado independiente.
- Administración individual de cada archivo cifrado.
- El administrador puede modificar los archivos que desea cifrar.
- Cuando una estación de trabajo está en modo multiusuario, cada usuario tiene una contraseña única para la autenticación.

Las desventajas del cifrado de archivos son:

- El Administrador puede olvidarse de seleccionar los datos importantes que necesitan ser encriptados.
- Los usuarios pueden guardar datos en carpetas que no están cifradas.
- Perdida de desempeño cuando todo el disco está cifrado.

Cifrado del disco completo

El cifrado de disco completo se utiliza para cifrar todo el disco en una partición específica.

- En la definición o escribiendo la contraseña de cifrado, siga estas pautas:
  - No utilizar la tecla de bloqueo de mayúsculas (Shift).
  - No utilice el teclado numérico (utilizar los números en la parte superior del teclado).

Las ventajas del cifrado del disco complete son:

- Todo es cifrado, incluso la configuración del equipo.
  Esta es la mejor ventaja cuando el administrador olvida cifrar algunos archivos. Esto se vuelve aún más importante cuando el administrador desea cifrar archivos de configuración sensibles o datos que están almacenados directamente por algún software en los directorios del programa.

- El despliegue del cifrado completo del disco es más fácil que el despliegue de cifrado de archivos.

Las desventajas son:

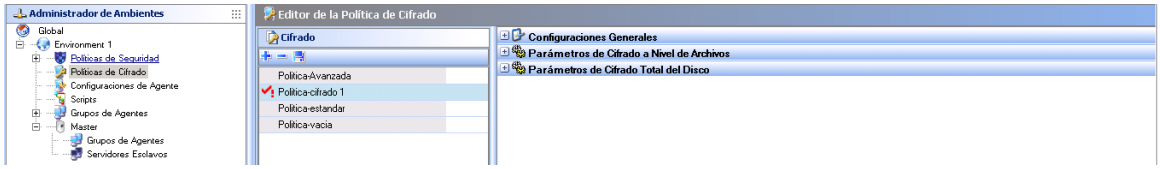
- Sólo hay una contraseña de encriptación compartida por todos los usuarios del ordenador.
- El despliegue del cifrado completo del disco puede tardar más que el despliegue de cifrado de archivos dependiendo del tamaño del disco.
- Sólo el disco duro en el que se ha instalado el sistema podrá ser cifrado. Si desea cifrar los documentos presentes en otro disco duro, usted tiene que utilizar el cifrado de disco completo y el cifrado de archivos (en Configuración general> Modo de protección).
  El cifrado de archivos sólo se aplicará al disco duro secundario.

CREANDO POLÍTICAS DE CIFRADO

Interfaz Gráfica

Las políticas de cifrado se encuentran en el panel del administrador de ambientes. Al igual que para otras políticas usted puede crear políticas de cifrado:

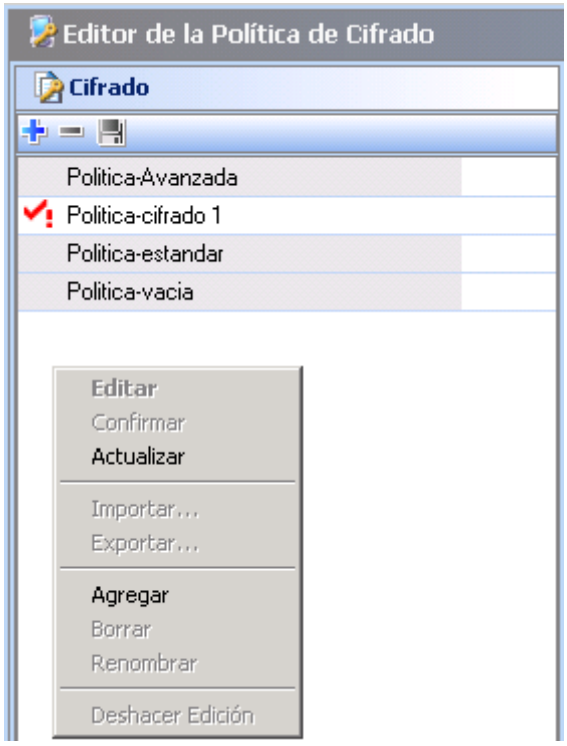
- A nivel global, que son políticas de cifrado aplicables a cualquier ambiente.
- A nivel local, que son políticas de cifrado dedicadas a un único ambiente.



Procedimiento

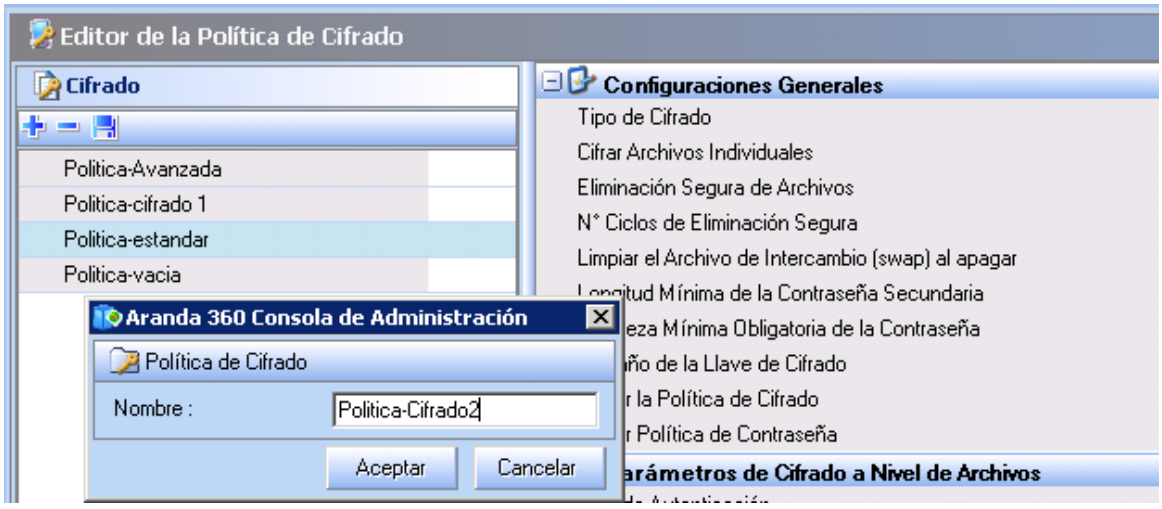
Para crear una política de cifrado, ejecute los siguientes pasos:

1. En el editor de políticas de cifrado, haga clic-derecho en la columna de cifrado.



2. Seleccione Adicionar del menú desplegable o clic directamente en el icono de adicionar en la barra de herramientas.

3. Ingrese el nombre de la política y haga clic en OK.



4. Especifique los parámetros de cifrado.
5. Aplique la política de cifrado a un grupo de agentes.
6. Envié la configuración al servidor.

- Cuando usted aplica una nueva política de cifrado a un grupo de agentes, la política no se ejecutara hasta el próximo reinicio de la maquina donde se encuentra el agente.

CARACTERÍSTICAS DEL CIFRADO DE ARCHIVOS

Seguridad multiusuario

Aranda 360 usa dos tipos de claves de cifrado: una calve para el computador y otra clave de usuario. Cada máquina tiene una sola clave de computador pero múltiples claves de usuario. esto permite a los usuarios compartir los ordenadores y aun así mantener la privacidad y confidencialidad de los datos.

Clave de cifrado de maquina

Las carpetas y archivos que son cifrados con la clave del computador pueden ser abiertos por cualquier usuario autorizado.

Clave de cifrado de usuario

Después de aplicar las políticas de cifrado, las carpetas y archivos cifrados con una clave de usuario de cifrado solamente pueden ser abiertos por el primer usuario que creo o accedió al archivo o carpeta.

Seguridad de información eliminada

Proporcionar el borrado seguro de archivos implica sobrescribir los archivos borrados para impedir la recuperación de datos (especialmente de los usuarios no autorizados). Esto es muy importante cuando un ordenador portátil ha sido robado o ha cambiado de usuario.

Es posible seleccionar el número de sobrescribe que se deben realizar para el borrado seguro.

- Los profesionales pueden recuperar información desde casi cualquier soporte magnético, incluso los dañados.
  Para eliminar un archivo de forma permanente, el proceso de borrado de datos seguro realiza una serie de datos aleatorios que se sobrescribirán donde se almacenaba el archivo eliminado.
  El borrado de datos seguro utiliza métodos de trituración para eliminar archivos de forma permanente.
  La Trituración es actualmente el único método válido para borrar datos de forma segura en su disco.
  Esto hace que sea casi imposible de recuperar datos a través de remanencia magnética.

Opciones de cifrado de archivos

Hay dos opciones de cifrado de archivos:

- Cifrar archivos por su extensión.
- Cifrar carpetas.

El administrador puede cifra archivos por su extensión o con un comodín *.

Estos son algunos ejemplos del uso del comodín:

- c:*
- *\crypt*
- c:*.txt
- c:\fichier.txt
- |userprofile|*

También puede excluir archivos y / o carpetas del cifrado.

Creación de contraseña e inicio de sesión

Creación de contraseña

La primera vez que un usuario inicia sesión en una maquina a la que se le ha aplicado una política de seguridad, se le solicitará que cree una contraseña de autenticación o un código PIN, dependiendo del tipo de autenticación seleccionado (Windows, secundario o Tarjeta inteligente).

Esta contraseña de autenticación se convierte en la clave de cifrado para acceder a los datos protegidos en la estación de trabajo.

Si un usuario está en el proceso de creación de una nueva contraseña y el agente pierde su conexión con el servidor antes de que la contraseña sea confirmada, se mostrara el siguiente mensaje de error:

Usted no está conectado al servidor

- Si usted aplica la política del cifrado de archivos justo después de instalar el agente de Aranda 360, una ventana emergente pedirá al usuario crear la contraseña.
  Un mensaje de error aparecerá si la maquina del agente no es reiniciada antes de crear la contraseña de usuario.
  Reinicie el equipo con el fin de solucionar el problema y crear la contraseña de usuario.

Creación de alerta de contraseña

La ventana de contraseñas para los usuarios nuevos y para los usuarios que ya tienen contraseñas.

Esto se debe a que un usuario que ya tenga una contraseña de cifrado puede existir en otro equipo.

Otra situación puede ser que una contraseña de cifrado que ya existe para el usuario y el agente de Aranda 360 ha sido desinstalado y reinstalado en la maquina.

- Si el usuario ya tiene una contraseña de cifrado, esta contraseña debe introducirse tanto en las casillas de Nueva contraseña y Confirmar contraseña.

Conexión

Si un usuario intenta iniciar sesión con una contraseña incorrecta, aparecerá un mensaje de error. Después de cinco intentos fallidos de inicio de sesión, el usuario será bloqueado y tendrá que esperar 30 segundos para volver a intentarlo.

Si el intento de inicio de sesión por primera vez, después de la espera de 30 segundos falla, el usuario se bloqueará automáticamente y deberá esperar nuevamente 30 segundos más.

SINCRONIZACIÓN

Una sincronización con el disco duro se realiza cuando un usuario inicia una sesión por primera vez después de aplicar una política de cifrado.

La próxima vez que este usuario inicie la sesión, la sincronización se producirá sólo si la lista de zonas cifradas se modifica.

La sincronización se produce cuando un usuario mueve una carpeta o varios archivos desde una zona sin cifrar a una zona de cifrado.

La desincronización se produce cuando un usuario mueve una carpeta o varios ficheros de una zona cifrada a una zona sin cifrar.

Si un usuario no autenticado ha creado archivos en una zona de cifrado, los archivos permanecerán sin cifrar hasta que el usuario realice una autenticación o realice una sincronización manual de la zona de cifrado.

Para autentificarse, el usuario debe hacer clic-derecho en el icono del monitor Aranda 360 y seleccionar Autentificación > Acceso a Datos Protegidos.

La primera vez que el usuario inicia sesión, encontrará los siguientes campos:

Los archivos sin encriptar se cifrarán en el siguiente acceso autenticado o al realizar una sincronización manual de la zona de cifrado mediante el uso de una política de re sincronización de cifrado.

Desincronización

Durante la desincronización, el disco duro se restaura a su estado original y todos los archivos serán des encriptados.

La desincronización ocurre cuando:

- Una carpeta se elimina de la lista de zonas cifradas.
- El agente de Aranda 360 se actualiza al actualizar las versiones 4.5, 4.6, 4.7 a la versión 4.8.
- El tipo de clave de cifrado asociado con una zona se modifica.
- El agente de Aranda 360 está desinstalándose y Descifrar datos con la instalación esta activado. Solamente los archivos cifrados con una maquina de maquina son descifrados. Los archivos cifrados con una clave de usuario deben ser descifrados manualmente.

    - Cuando una política de cifrado se modifica, las carpetas cifradas que no están asociadas a una aérea de cifrado son de sincronizadas mientras que las carpetas que se definen en la nueva política de cifrado si serán sincronizadas.

Sincronización después de actualizar

La primera vez que el usuario inicia sesión después de una actualización de Aranda 360, se ejecutará un proceso de desincronización.

Todos los archivos son descifrados antes de que se aplicara una nueva política de cifrado. El proceso de sincronización continuará normalmente.

- La desincronización sucede cuando se actualizan versiones 4.5, 4.6 o 4.7 a versiones 4.8.
  Para los agentes, es necesario actualizar primero 4.5, 4.6 y 4.7 a versiones 4.8 antes de realizar actualizaciones a versiones mayores.
- Bajo el administrador de ambientes > [Servidor Principal] > Cifrado, asegúrese de:
  - La fecha permitida para iniciar la desinstalación,
  - La fecha permitida para terminar la desinstalación,

  En el panel del administrador de ambientes para indicar el tiempo indicado, de otro modo la desincronización no sucederá.

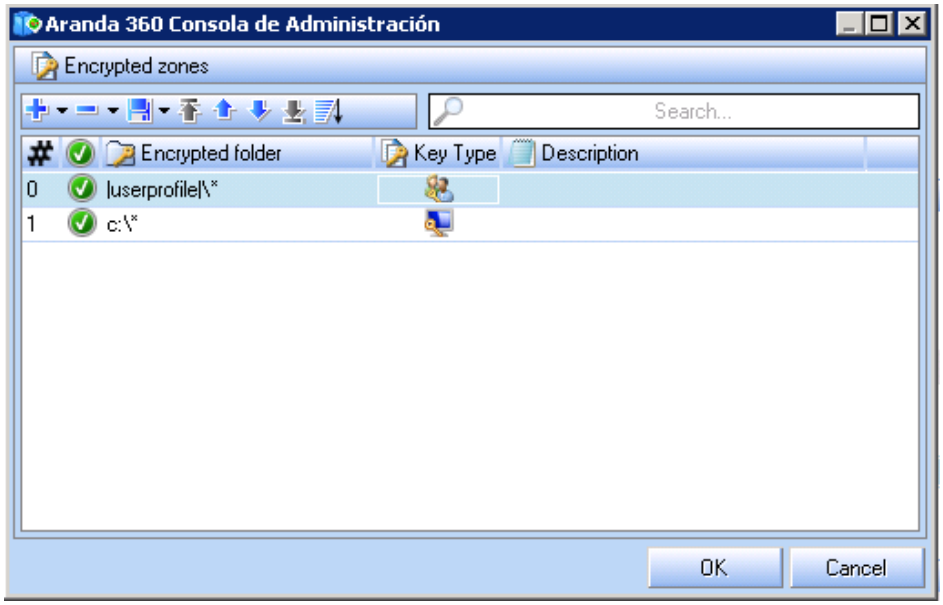
Sincronización con múltiples usuarios

Si un equipo tiene varios usuarios, los archivos cifrados se vuelven a sincronizar cada vez que un nuevo usuario inicia sesión por primera vez.

Los archivos cifrados se vuelven a sincronizar con el tipo de clave de cifrado asociado a cada nuevo usuario.

Para ilustrar esto, consideremos el siguiente ejemplo. Dos usuarios compartir el mismo equipo. Cada usuario tiene un perfil de usuario específico.

Para ver la siguiente ventana, diríjase a Políticas de cifrado > Parámetros para cifrado de archivos> Zonas cifradas.



La política de cifrado se define como:

- La clave de cifrado de usuario es aplicada a la carpeta |userprofile|*
- La clave de cifrado de maquina es aplicada a C:*

La zona de cifrado con la ruta de acceso genérica deberá aparecer siempre en la última zona de cifrado.
La aplicación de Las políticas y las reglas de cifrado tendrán prioridad sobre las zonas sin cifrado.

Primera sincronización

Por ejemplo, Craig es el primer usuario que inicie la sesión. Su perfil de usuario es:

Perfil de usuario = c:\Documents and Settings\craig

El proceso de sincronización cifra:

- Con la calve de usuario de Craig todos los archivos guardados en: c:\Documents and Settings\craig

- Con la clave de maquina todos los archivos guardados en C:\ excepto:
  - Las carpetas definidas en las zonas son cifrar (si existen).
  - c:\Documents and Settings\craig

Sincronizaciones posteriores

Un Nuevo usuario, Lucy, inicia sesión. Su perfil de usuario es: Perfildeusuario = c:\Documents and Settings\lucy

Un Nuevo proceso de sincronización será ejecutado.

Los archivos guardados en c:\Documents and Settings\lucy fueron cifrados previamente con la clave de maquina en la primera sincronización.

El nuevo proceso de sincronización removerá la clave de máquina y cifrara de nuevo los archivos con la clave de lucia.

- Inclusive si algunos usuarios permiten que otro usuario acceda a sus archivos guardados en sistemas con New Technology File System (NTFS),y cifrados con clave de usuario, el acceso será denegado.

PARÁMETROS DE CIFRADO

Configuración general

La configuración general permiten establecer una serie de comandos y opciones como:

- Modo de protección.
- Autorizar la creación de archivos cifrados.
- Autorizar el borrado seguro de archivos.
- Número de ciclos de borrado seguro.
- Borrado del archivo swap cuando una maquina es detenida.
- Caracteres mínimos exigidos para la contraseña de autenticación.
- Obligatoriedad del uso de contraseñas seguras.
- Tamaño de la clave de cifrado.
- Forzar la política de cifrado.
- Obligar el cambio de contraseña.

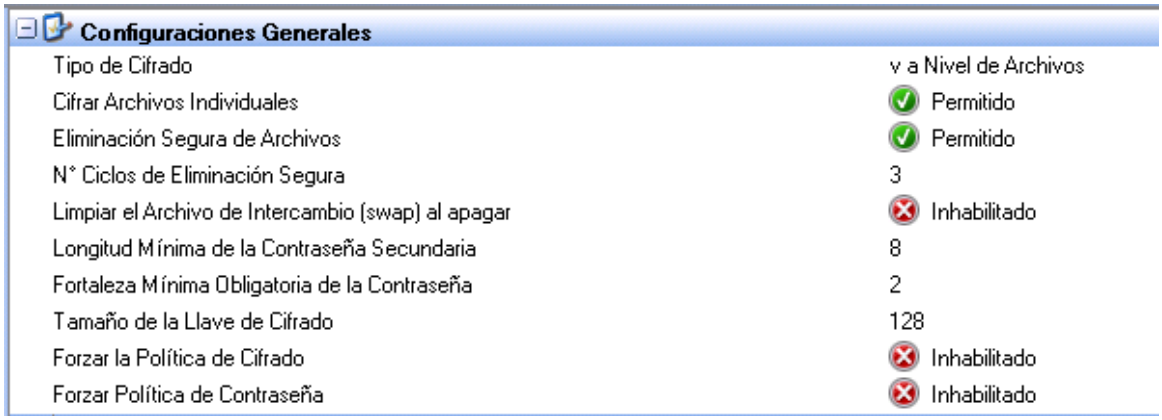


Fig. 12.1: Cifrado: Configuración general

Modo de protección

El modo de protección se puede ajustar a:

- Cifrado de archivos.
- Cifrado de disco completo.
- Cifrado de archivos y de disco completo.

Cifrado de archivos

Si el modo de protección es ajustado a cifrado de archivos:

- Los parámetros de cifrado de disco completo son desactivados.

- La opción Ignorar la partición del sistema (en los parámetros para cifrado de archivos) será desactivada.

Cifrado del disco completo

Si el modo de protección está configurado para el cifrado de disco completo, los parámetros de cifrado serán estarán desactivados.

Cifrado del disco completo y de archivos

Si el modo de protección está establecido para ambas opciones, todas las características y parámetros estarán disponibles y podrán ser modificados.

- El administrador no puede cambiar directamente el modo de protección de cifrado de archivo a cifrado de disco completo.
  El usuario primero debe descifrar todos los archivos cifrados.
  Esto se puede lograr mediante el uso de:
  - Por un proceso de recuperación.
  - O una política de cifrado de archivos sin datos cifrados o zonas que obligarían una desincronización.

Permitir la creación de archivos cifrados

Esta opción permite a los agentes de Aranda 360 crear sus propios archivos cifrados los cuales pueden ser guardados y enviados por correo electrónico a otros usuarios, dentro y fuera de la red corporativa, sin el riesgo de que pudiesen ser leídos mientras transitan por internet.

En el editor de políticas de cifrado, cuando AUTIRIZAR CREACIÓN DE ARCHIVOS CIFRADOS está configurada como PERMITIDO, el usuario agente puede hacer clic-derecho en el archivo o carpeta para mostrar las opciones de cifrado en el menú emergente.

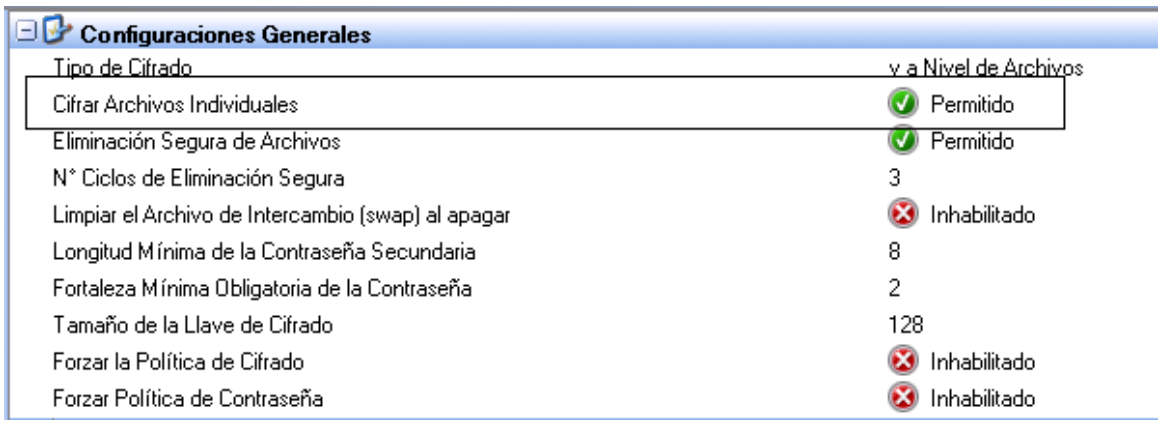


Fig. 12.2: Autorización para creación de archivos cifrados

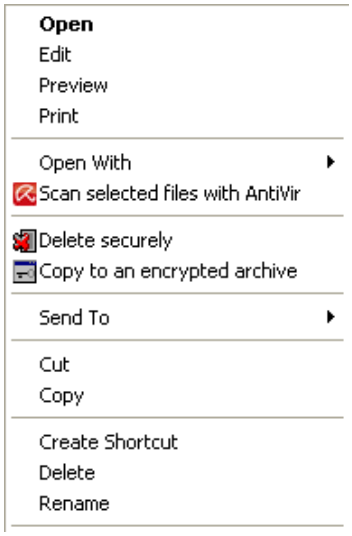


Fig. 12.3: Menú del agente para cifrar un archivo/carpeta (estación de trabajo)

Permitir la eliminación segura de archivos

Cuando esta opción es activada, los usuarios agentes de Aranda 360 pueden borrar archivos de forma segura. Los archivos son sobrescritos el número de veces indicado en número de ciclos para el borrado seguro en las configuraciones generales.

Cuando esta opción es desactivada, ya no se mostrará en el menú la opción de Borrado seguro. El usuario no podrá seleccionarla.

Número de ciclos de eliminación segura

Esta opción indica el número de ciclos de borrado que se llevará a cabo para eliminar de forma segura archivos y carpetas.

Los archivos marcados como eliminados se sobrescriben el número de veces especificado en número de ciclos para el borrado seguro en las configuraciones generales.

Por defecto, el valor es 3.

- Puede establecer un número mayor para los ciclos pero aumentará el tiempo necesario para borrar archivos ó carpetas de forma segura, lo que puede ocasionar problemas con archivos o carpetas de gran tamaño.

Eliminar archivo swap cuando la maquina es detenida

Esta opción asegura el borrado del archivo swap cuando la maquina se detiene.

Caracteres mínimos permitidos en la contraseña en la segunda autenticación

Este es el número de caracteres mínimo requerido para crear una contraseña de protección para datos cifrados y descifrados.

Por defecto, el valor es 8.

- Esta opción solo está disponible cuando el tipo de autentificación está establecida como Secundario.

Seguridad de contraseña obligatoria

El administrador puede definir el mínimo de caracteres para determinar su una contraseña es segura. Una contraseña segura puede variar de 1 a 5 (siendo 5 el nivel máximo).

Cuando el usuario define su contraseña, Aranda 360 realiza una evaluación en tiempo real de la seguridad de la contraseña que acaba de ser introducida.

Si la seguridad es menor que la definida por el administrador, se rechazara la contraseña.

La evaluación de la contraseña se basa en un coeficiente de entropía para los caracteres utilizados.

Se utiliza la siguiente fórmula:

Coeficiente = (log base 2 (rango de caracteres usados) * (tamaño de la contraseña)

Se aplica al coeficiente de entropía si cualquier repetición que se detecta en la contraseña introducida.

- Cuando se usa el cifrado de disco completo, el número de intentos de introducción de contraseña en el inicio de sesión del equipo están limitados a 10.
  Cuando se excede de 10 intentos, es necesario reiniciar el ordenador.

Tamaño de clave de cifrado

El administrador puede establecer el tamaño de la clave de cifrado:

- 128 bits.
- 192 bits.
- 256 bits.

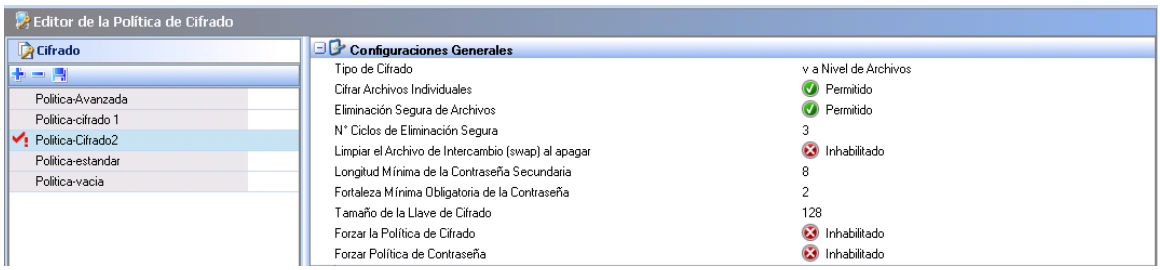
Cumpliendo las políticas de cifrado

La opción es establecida por defecto en Desactivada. Si el administrador activa la opción, evitará que el usuario cierre la ventana de ingreso de la contraseña al abrir la sesión.

Cumpliendo las políticas de contraseña

Esta opción está definida por defecto en Desactivada. Si el administrador habilita la opción, se recomienda al usuario cambiar la contraseña, la antigua contraseña permanecerá valida.

Cuando esta opción es habilitada, el campo Edad máxima de la contraseña se mostrará.



PARÁMETROS PARA CIFRADO DE ARCHIVOS

Los parámetros de cifrado de archivos permiten controlar los siguientes:

- Tipo de autentificación.
- Proveedores de servicios de cifrado (CSP).
- Autorización para detener sincronización.
- Autentificación después de desbloquear sesión.
- Ignorar la partición del sistema (ya se ha cifrado a nivel de disco).
- Autentificación de usuario obligatoria.
- Modo silencioso.
- Zonas cifradas.
- Tipo archivos cifrados.
- Zonas no cifradas.

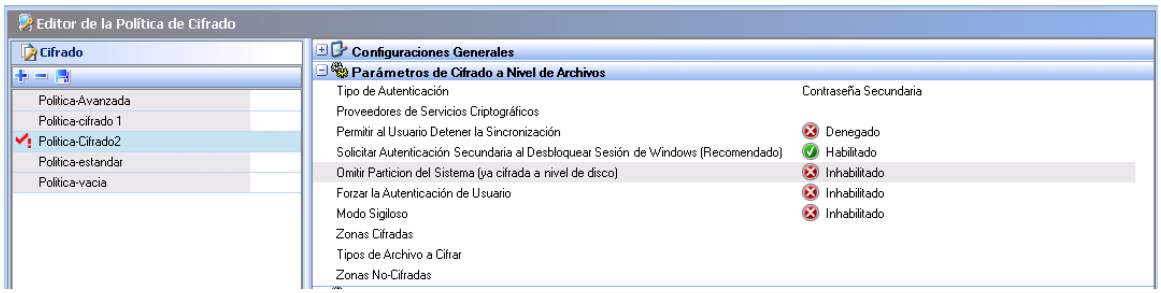


Fig. 12.4: Parámetros de cifrado de archivos

Tipo de autenticación

Un tipo de autenticación es definido para cada política de cifrado. Diferentes tipos de autenticación pueden ser aplicados a diferentes grupos de agentes.

Sólo hay un tipo de autenticación por política de cifrado.

- Después del despliegue del agente, los tipos de autenticación no se pueden modificar. Las modificaciones deben ser realizadas manualmente por el administrador de cada usuario.

Los tres tipos de autenticación son las siguientes:

- Windows.
- Secundaria.
- Tarjeta inteligente.

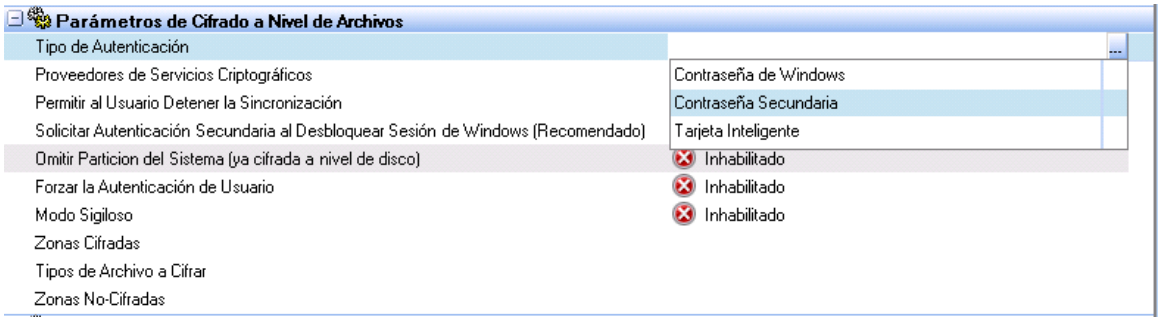


Fig. 12.5: Parámetros de cifrado de archivos: Tipo de autenticación

Autenticación Windows

Este tipo de autenticación está basado en la autenticación de Windows. Esta autenticación no es tan segura como la secundaria o la tarjeta inteligente.

El usuario puede acceder fácilmente a los archivos cifrados a través de este tipo de autentificación simplemente iniciando sesión con una contraseña y usuario de Windows.

Autenticación secundaria

Cuando se inicia por primera vez la maquina después de haber aplicado una política de cifrado, se le pedirá al usuario que cree una contraseña de autenticación secundaria.

Además de introducir la contraseña de inicio de sesión de Windows durante el arranque, el usuario también debe introducir una contraseña para acceder a los datos cifrados almacenados en el disco duro.

Fig. 12.6: Contraseña de autenticación secundaria

- Se recomienda crear una contraseña de autenticación secundaria.

Autenticación de tarjeta inteligente

La tarjeta inteligente y el lector de tarjetas deben estar conectados a la computadora con el fin de acceder a los datos codificados en el sistema.

Después de iniciar Windows, se pide al usuario que introduzca una contraseña para abrir los archivos cifrados almacenados en el disco duro.

Por lo general, la contraseña utilizada para este tipo de autenticación es el código PIN suministrado por el proveedor de servicios de las tarjetas inteligentes.

Proveedores de servicio de criptografía (CSP)

Los proveedores de servicios criptográficos son los fabricantes de tarjetas inteligentes. Las tarjetas inteligentes proporcionadas por el CSP incluyen un software que se debe instalar en el equipo del Agente para permitir el uso de la autenticación de tarjetas inteligentes.

Para propósitos de fácil manejo, se recomienda instalar el CSP en el equipo donde ha sido instalada la consola de administración de Aranda para configurar las tareas administrativas de tarjetas inteligentes (ejemplo: cambiar el usuario de las tarjetas inteligentes con sólo elegir en el menú desplegable el parámetro CSP en el Editor de políticas de cifrado).

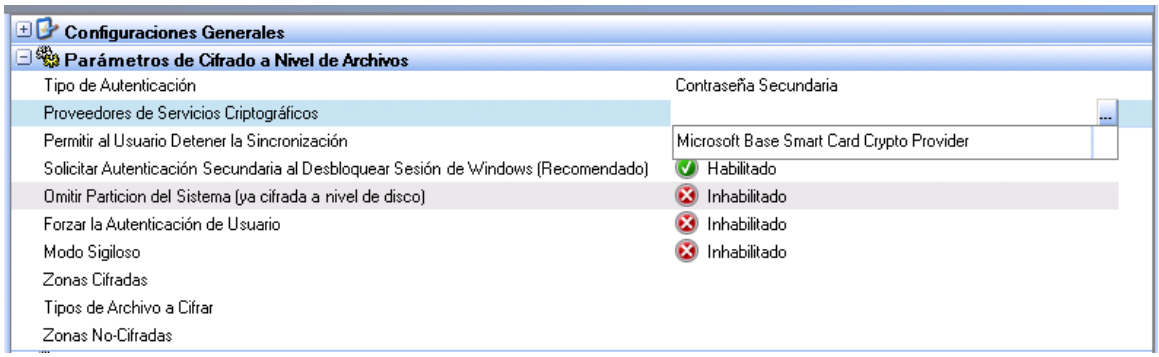


Fig. 12.7: Proveedores de servicio de criptografía (CSP)

Si el CSP no está instalado en el servidor de Aranda 360, pero en la computadora del agente, el administrador debe introducir el nombre exacto de la CSP haciendo doble clic en el campo de la derecha.

- Esta opción sólo se puede establecer cuando el tipo de autenticación es Tarjeta inteligente. Los nombres de los CSP instalados se encuentran bajo el registro: HKLM \ Software \ Microsoft \ Cryptography \ defecto \ Provider El nombre del CSP debe ser exactamente el mismo en la consola y en las estaciones de trabajo del cliente.

- Los tres siguientes carpetas se añaden por defecto a los archivos / carpetas exentas de cifrado:
  - |userprofile|\application data\microsoft\crypto*
  - |userprofile|\application data\microsoft\
  - systemcertificates*
  - |userprofile|\application data\microsoft\protect*

  Dependiendo del CSP utilizado, estas carpetas pueden incluir datos de caché para certificados de tarjetas inteligentes que deben ser legibles por el sistema.

Autorización para detener la sincronización

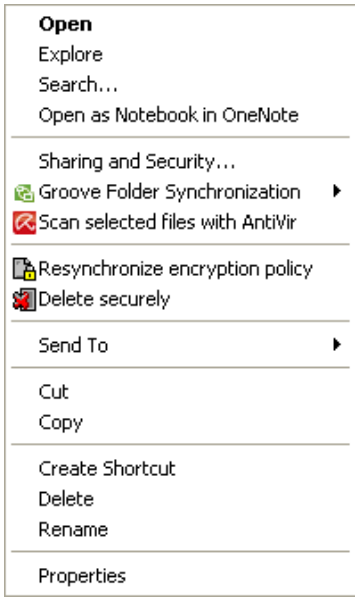
Si los datos se actualizan en:

- Zonas cifradas,
- Tipo de archivos cifrados,
- Zonas sin cifrar,

la sincronización será ejecutada nuevamente.

Por defecto, este parámetro se establece como Denegado. Cuando se cambia a permitido, el usuario puede detener el proceso de sincronizado.

Para ejecutar manualmente una re sincronización, haga clic derecho en las opciones de la carpeta a re sincronizar en la maquina del agente.



Autenticación después de desbloquear la sesión

Cuando esta opción es establecida como Activada, se previene que se pierdan las claves de cifrado cuando la sesión de usuario este bloqueada.

Es útil para evitar bloqueos entre el software que acceda a los archivos cifrados, mientras que la sesión de usuario está bloqueada.

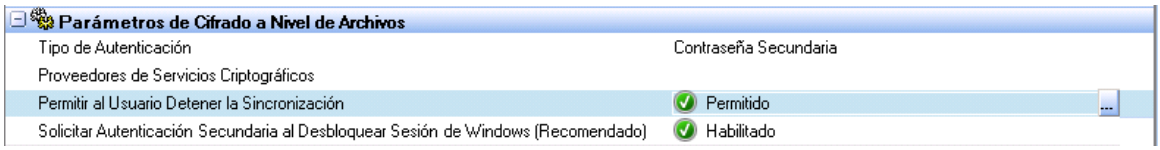


Fig. 12.8: Autenticación después de desbloquear la sesión

Por otra parte, si desea desactivar esta opción, piénselo dos veces. De hecho, hay algunos inconvenientes graves asociados esta acción. Por ejemplo, un hacker podría robar las claves de cifrado de usuario contenidos en el archivo hiberfil.sys mediante el uso de la función de hibernación en el sistema operativo.

Si un hacker rompe el inicio de sesión, los archivos cifrados se podrán acceder sin autenticación (ya que las claves de cifrado no han sido eliminadas).

Ignorar partición del sistema (ya cifrado a nivel de disco)

Esta opción se activa solamente cuando Modo de protección es establecido para cifrado de archivos y cifrado de disco completo.

Si la opción es activada, la ruta |systemdrive| será cifrada por cifrado de disco completo pero no estará protegida por cifrado de archivos.

Si la opción esta desactivada, la ruta |systemdrive| será protegida por cifrado de disco completo.

Si la ruta también está incluida en las zonas cifradas, entonces será cifrada dos veces: por cifrado de archivos y cifrado completo de disco.

- Las reglas de las zonas Sin cifrar tendrán prioridad sobre otras reglas de cifrados.

Autenticación de usuario obligatoria

Cuando esta opción es establecida como activa, al usuario se le pedirá autentificarse cuando inicie sesión con el fin de evitar la creación de archivos sin cifrar.

Modo silencioso

Cuando esta opción esta activada, el cifrado de archivos se aplica a las estaciones de trabajo, pero sus usuarios no notarán la ejecución del proceso.

El agente dejara de mostrar aspectos al usuario como:

- Clic-derecho en la ventana de cifrado de archivos.
- Barra de progreso de cifrado.
- Clic-derecho en el menú (Copiar un archivo cifrado).
- El icono de bloqueo en archivos cifrados.

Si el modo silencioso esta activo, el administrador necesitará autentificarse en modo Windows.

Zonas cifradas

Esta opción es usada para cifrar todos los archivos de una carpeta. El administrador tiene que definir las carpetas donde los usuarios almacenarán los archivos.

El Administrador deberá informar a los usuarios donde pueden almacenar sus archivos.

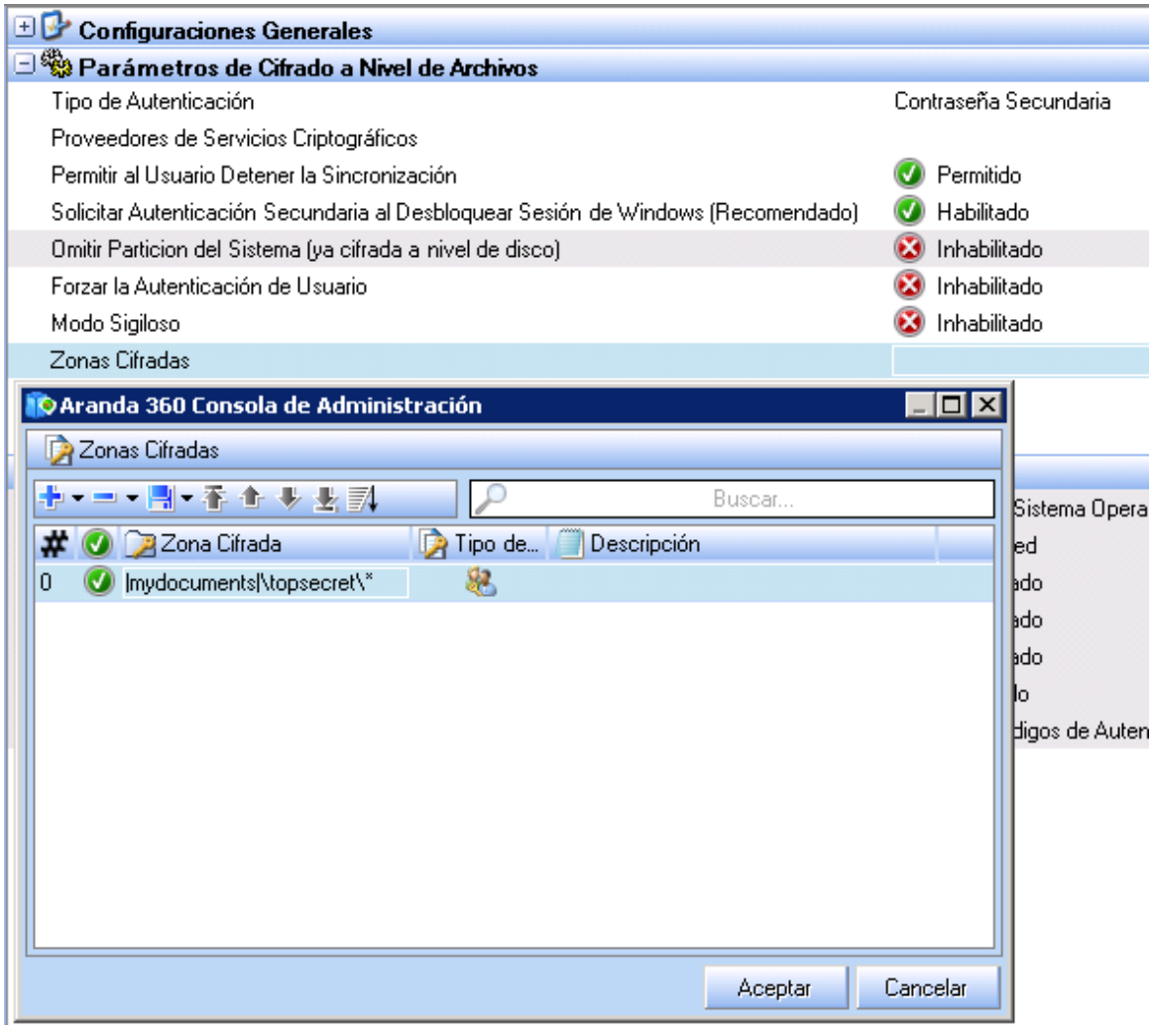


Fig. 12.9: Zonas cifradas

- La zona de cifrado con la ruta de acceso genérica deberá aparecer siempre
  En la última zona de cifrado
  La aplicación de Las políticas y las reglas de cifrado tendrán prioridad sobre las zonas sin cifrado.

Variables de entorno

Las variables de entorno hacen que sea más fácil configurar zonas cifradas.

Por ejemplo, puede introducir | userprofile | para especificar todas las carpetas de usuario individuales, en lugar de entrar en cada carpeta individual.

Las variables de entorno soportadas son:

- |username|
- |systemroot|
- |systemdrive|
- |programfiles|
- |userprofile|
- |mydocuments|

- Las variables de entorno, en particular |username| y |userprofile|, son dinámicas. Ellas cambian con cada inicio de sesión de usuario.
  Consideremos la siguiente situación:
  - usuario1 inicia sesión.
    La zona que será cifrada según las definiciones de la política es:
    c:\documents and settings\ usuario1
    (la variable de entorno se reemplaza por su valor).
  - usuario2 inicia sesión después del usuario1 en la misma computadora.
    La zona que será cifrada según las definiciones de las políticas es:
    c:\documents and settings\ usuario2
    y la sincronización se ejecutará.
    Si el usuario2 tiene permitido el acceso a c:\documents and settings\usuario1 (siempre que los permisos del sistema sean concedidos y los archivos sean cifrados con una clave de maquina), el descifrado se ejecutará.
    Para evitar esto, el administrador debe definir una clave de usuario para este tipo de carpetas.

Tipo de claves de cifrado

Existen dos tipos de claves de cifrado:

- Llave de cifrado de máquina.
- Llave de cifrado de usuario.

Llave de cifrado de maquina

La llave de cifrado de maquina está disponible para cualquier usuario que tenga una contraseña de cifrado para ese equipo en particular.

Esto significa que los datos encriptados están protegidos contra el robo y el acceso de usuarios no autorizados.

Cada equipo tiene sólo una clave de máquina. La clave de maquina es cambiada con cada instalación del Agente de Aranda 360 para que cada equipo tenga una clave de cifrado de maquina única.

Clave de cifrado de usuario

La llave de cifrado de usuario es única para cada usuario.

Esto significa que si un archivo es cifrado por un usuario "A", solo el usuario "A" puede acceder al archivo. Cuando el usuario inicia sesión por primera vez con una contraseña, Aranda 360 crea una única calve de usuario. La clave de usuario es una combinación de la clave de máquina y la clave de usuario con la contraseña del usuario.

A continuación se describen tres situaciones típicas:

- Archivos cifrados por una clave
  Un archivo puede ser únicamente cifrado por una clave: una única clave de usuario o de máquina.

- El usuario accede a la clave de maquina
  Cada usuario es capaz de acceder a la clave de maquina con su propia contraseña. En realidad, la contraseña del usuario se utiliza para las claves de cifrado de máquina y usuario. Esto es transparente para el usuario.
- Acceso denegado a los archivos
  El acceso denegado a un archivo cifrado se da cuando:
  - El archivo ha sido cifrado con la clave de usuario de otro usuario.
  - No se ha ingresado la contraseña de autentificación.
  - Hay varias sesiones de usuario en un equipo con Windows Vista.
  - El agente de Aranda 360 ha sido detenido.
  - El administrador ha desactivado la política de cifrado mientras los archivos son cifrados.

Tipo de archivos cifrados

Esta opción se utiliza para especificar qué archivos se cifran según sus extensiones.

Ejemplo: Para proteger y cifrar archivos de documentos de Word, archivos de texto y archivos Excel, podría ingresar: .doc.; .txt; .rtf; .xls.

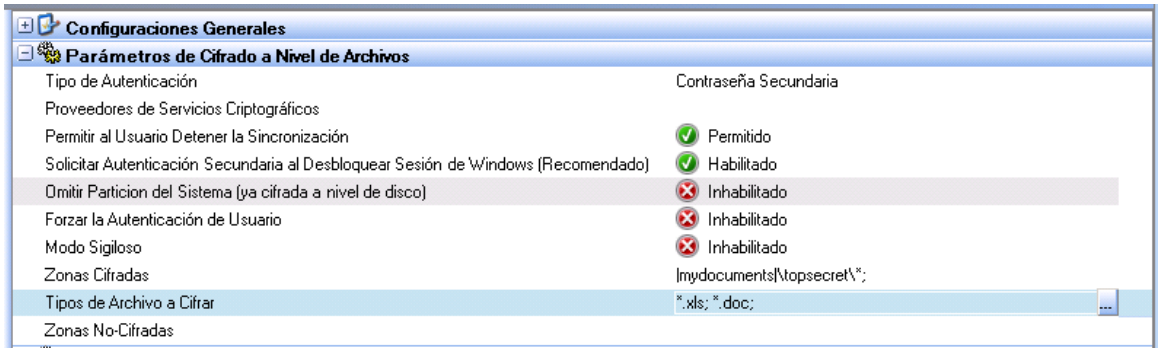
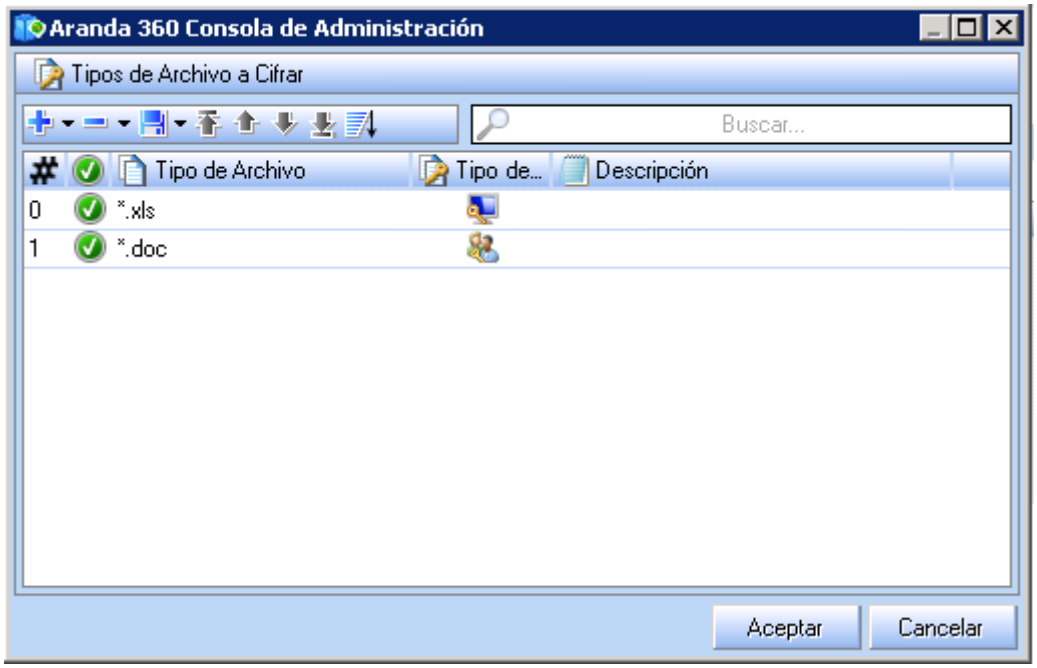


Fig. 12.10: Tipo de archivos cifrados

Los Tipos de archivos cifrados deben estar asociados a una clave de maquina o a una clave de usuario.



Zonas sin cifrar

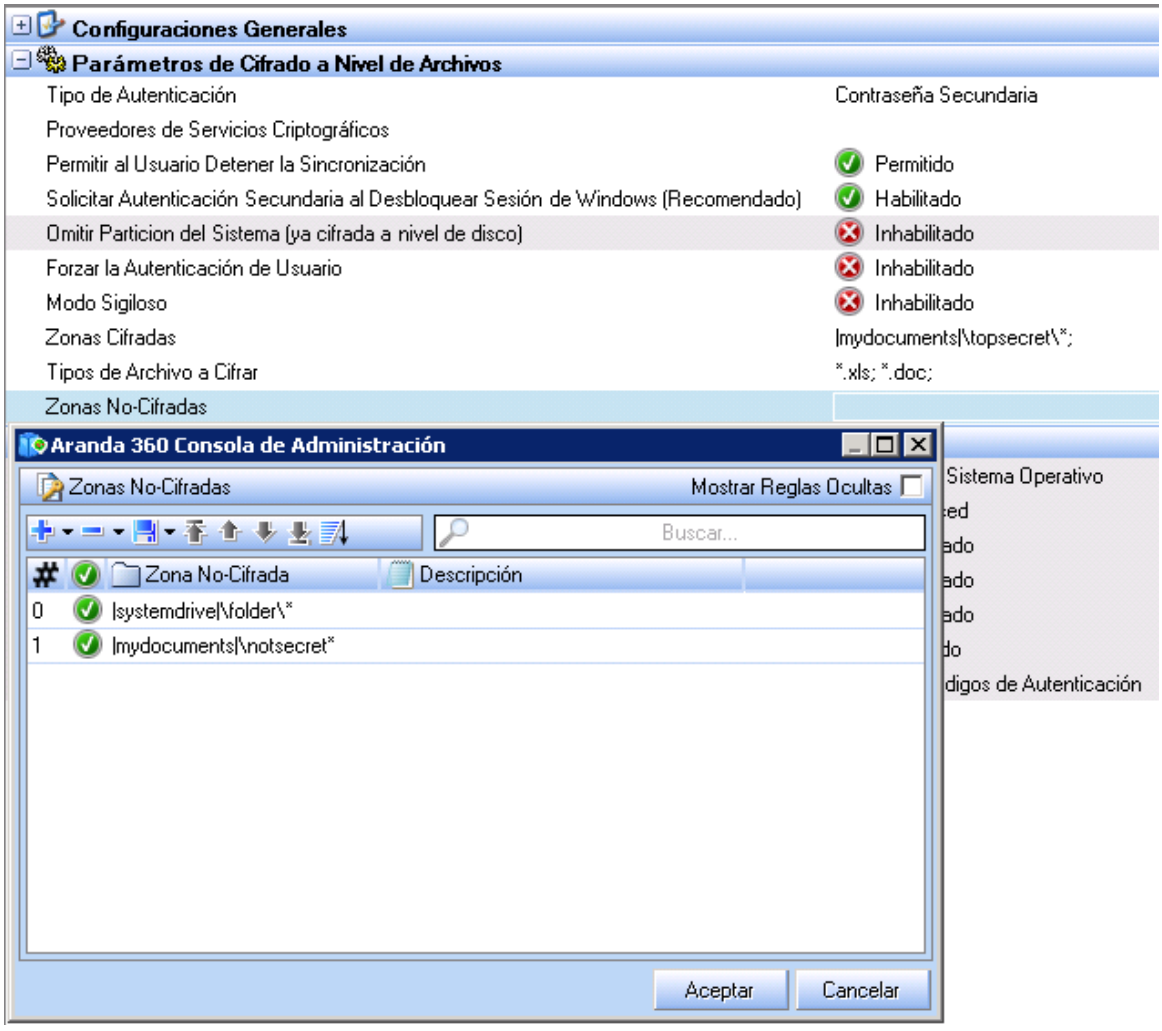


Fig. 12.11: Zonas sin cifrar

Archivos sin cifrar

Para cada zona sin cifrar, ingrese la ruta y el nombre de la carpeta teniendo en cuenta que los archivos contenidos allí no serán cifrados.

Si marca la casilla Mostrar reglas ocultas en la ventana emergente, se mostrará un listado de reglas predefinidas.

Archivos no cifrables

Aplicaciones importantes que se inicializan al mismo tiempo que el equipo no se cifran, es decir:

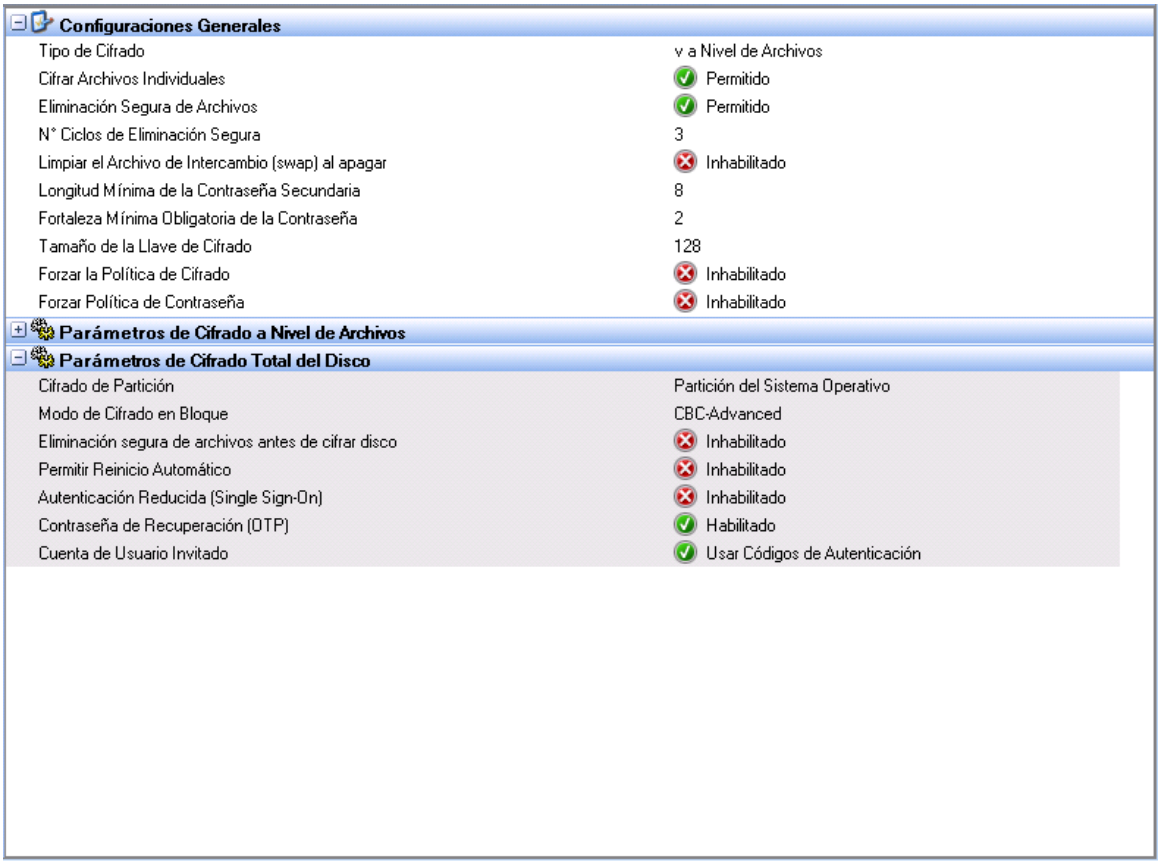
- Archivos del sistema operativo Windows.
- Información del sistema de la unidad.
- Aranda 360.

- En los siguientes escenarios los archivos también deben estar exentos de cifrado:
  - Cualquier sistema de archivos cargados durante el inicio de Windows.
    Puesto que los archivos se pueden descifrar sólo cuando el usuario inicia sesión, todos los archivos utilizados durante la secuencia de arranque de los servicios, controladores o del sistema operativo no deben ser cifrados. Esto incluye el gestor de archivos de escritorio.
  - Perfiles movibles.
    El acceso a los archivos cifrados es denegado hasta después de la autenticación con la contraseña de cifrado. Puesto que la sincronización de Windows se produce antes de la autenticación, el perfil móvil seguiría siendo cifrado y la sincronización de Windows no se llevaría a cabo.

Parámetros de cifrado del disco completo

os parámetros de Cifrado de disco completo permiten modificar los siguientes aspectos:

- Cifrado de particiones.
- Modo de operaciones Block-cipher.
- Eliminación segura antes de cifrado.
- Número de ciclos para borrados seguros.
- Permitir el reinicio automático.
- Registro sencillo (SSO).
- Recuperación de contraseña por una vez.
- Uso de cuenta de invitado.



Cifrado de partición

Esta opción incluye:

- Partición del sistema
  Sólo la partición del sistema donde está instalado el sistema operativo es cifrada.
- Todas las particiones
  Todas las particiones en el disco duro en el que está instalado Aranda 360 serán cifradas. Sólo están soportadas las particiones principales o conocidas como maestras.

Modo de operación Block-cipher

Esta opción se ejecuta en bloques con una longitud fija de 128 bits.

Puesto que los mensajes pueden ser de cualquier longitud y el cifrado del texto claro con la misma clave, por lo general genera la misma salida, varios modos de operación han sido creados.

Estos modos de operación permiten que el cifrado por bloques garantice la confidencialidad de los mensajes independientemente de su longitud.

Esta opción puede establecerse en:

- CBC (Cipher Block Chaining)
  CBC es el modo más usado. Su principal inconveniente es que el cifrado es secuencial (la salida de cifrado de bloque anterior se transmite al siguiente bloque) sin capacidad para el procesamiento paralelo. Por lo tanto, el tamaño del mensaje crecerá a un múltiplo del tamaño de bloque de cifrado.
  Aranda 360 usa CBC con bloques de 128-bit por cada sector del disco de 512-bit.
- CBC Avanzado
  Es el mismo modo CBC excepto por la inclusión de reglas algorítmicas como los niveles de complejidad. Por cada bloque cifrado, una clave (AES) es dinámicamente generada para prevenir criptoanálisis.

Eliminación segura antes de cifrado

Cuando esta acción esta activada, el disco se borrara de forma segura antes de un proceso de cifrado.

Número de ciclos para borrados seguros

Esta opción indica el número de ciclos de borrado efectuados para garantizar una eliminación completa. Los bloques en el disco son sobrescritos el número de veces establecido, con datos aleatorios antes de cifrarlos.

Cuanto más sea el número de ciclos de borrado, más largo el número de sincronizaciones.

Permitir reinicio automático

Consola

Esta opción permite el reinicio automático para el mantenimiento a distancia sin necesidad de utilizar contraseñas de cifrado.

Después de desactivar el gestor de arranque de Aranda 360, el administrador debe reiniciar manualmente o por medio de script la consola.

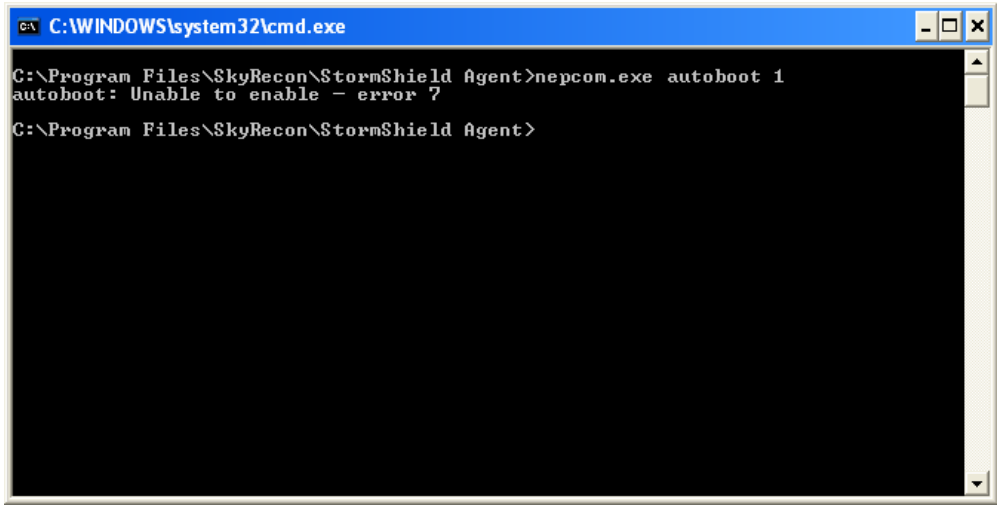
Agente

En el agente de Aranda 360, el administrador puede permitir a un número predefinido de reinicios automáticos a través del proceso nepcom.exe.

Requerimientos

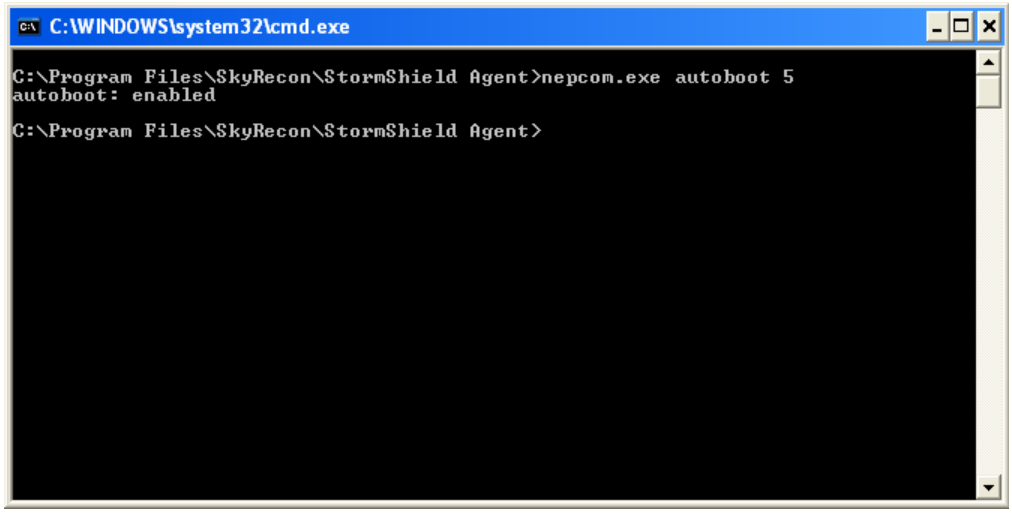
Para permitir el reinicio automático en el Agente de Aranda 360, debe activar Permitir reinicio automático en la consola.

De lo contrario, usted no será capaz de utilizar nepcom.exe y el mensaje "No se puede permitir que" se mostrará.



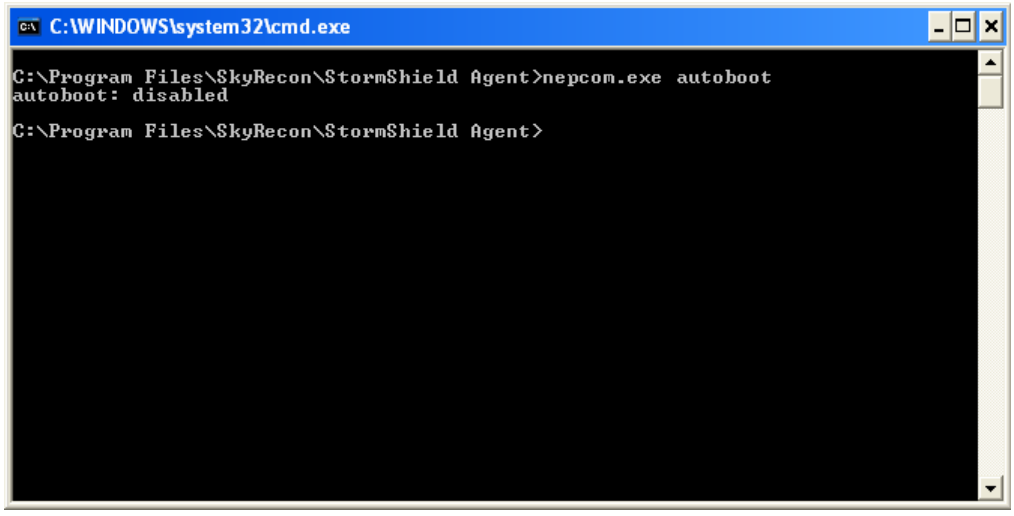
Procedimiento

Para permitir los reinicios automáticos en el Agente de Aranda 360, siga los siguientes pasos:



1. Abra una ventana de símbolo del sistema.
2. Diríjase al directorio del agente de Aranda 360.
3. Ingrese el siguiente comando:
   nepcom.exe autoboot [numero de reinicios automáticos permitidos]
   Verifique que el comando ha sido activado, el mensaje "Activado" será mostrado.

Para no permitir los reinicios automáticos en el Agente de Aranda 360, siga los siguientes pasos:



1. Abra una ventana de símbolo del sistema.
2. Diríjase al directorio del agente de Aranda 360.
3. Ingrese el siguiente comando:
   nepcom.exe autoboot
   Verifique que el comando ha sido desactivado, el mensaje "desactivado" será mostrado.

.

Registro sencillo (SSO)

Esta opción es usada para combinar dos tipos de autentificación (Cifrado+Windows) para un usuario principal.

Cuando el usuario se autentica por primera vez con su contraseña e identificador de sesión de Windows a través del servicio de autentificación de Aranda 360, la información de autenticación del usuario se cifra con la clave de cifrado y se almacena en el agente.

A partir de ahora, el usuario ya no tendrá que iniciar sesión con el usuario ni la contraseña de Windows, ya que el agente ha descifrado y enviado esta información al servicio de autenticación de Aranda 360. El servicio se encargara automáticamente de proporcionar los detalles de autenticación para la cuenta Windows.

Si el usuario cambia su contraseña de Windows, se deberán ejecutar los siguientes pasos:

- El usuario procederá como de costumbre para cambiar su contraseña en Windows.
- El usuario reiniciara la maquina
- El usuario ingresara su nueva contraseña de Windows al abrir una nueva sesión con el fin de que el agente de Aranda 360 cifre y almacene la nueva contraseña y usuario.

Si el usuario hace clic directamente en OK (o ingresa la contraseña anterior), el proceso de autentificación se detendrá. La ventana indicara que el usuario debe ingresar su nueva contraseña.

En la siguiente sesión, el usuario ya no tendrá que ingresar ni su usuario ni la contraseña de Windows.

Recuperación de contraseña por una vez

Cuando el usuario se autentica con una contraseña recuperada, esta opción genera una contraseña nueva de recuperación en el próximo inicio de sesión.

Uso de cuenta de invitado

Esta opción esta activada por defecto. Está diseñada para crear una cuenta temporal de invitado. la cuenta de invitado permitirá que se puedan autenticar usuario en la estación de trabajo sin usar la cuenta de un usuario principal

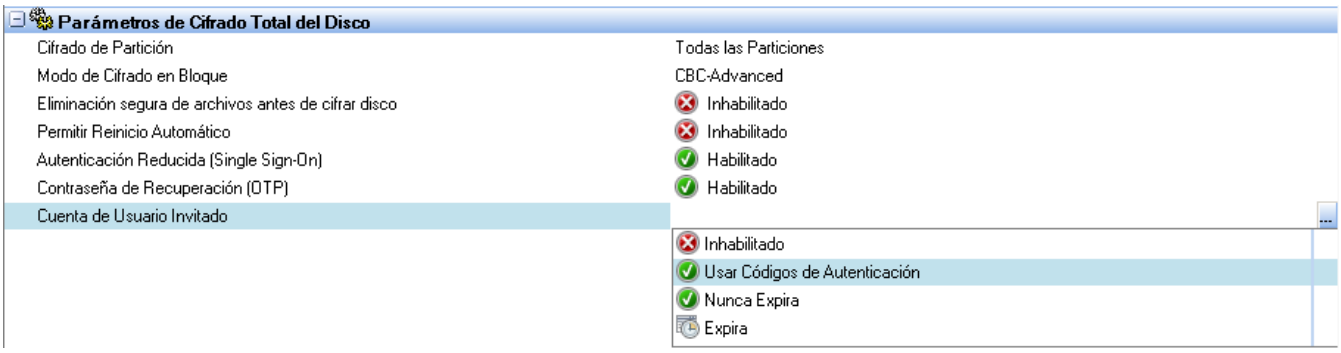


Fig. 12.13: Uso de la cuenta de invitado

Las opciones disponibles para esto son:

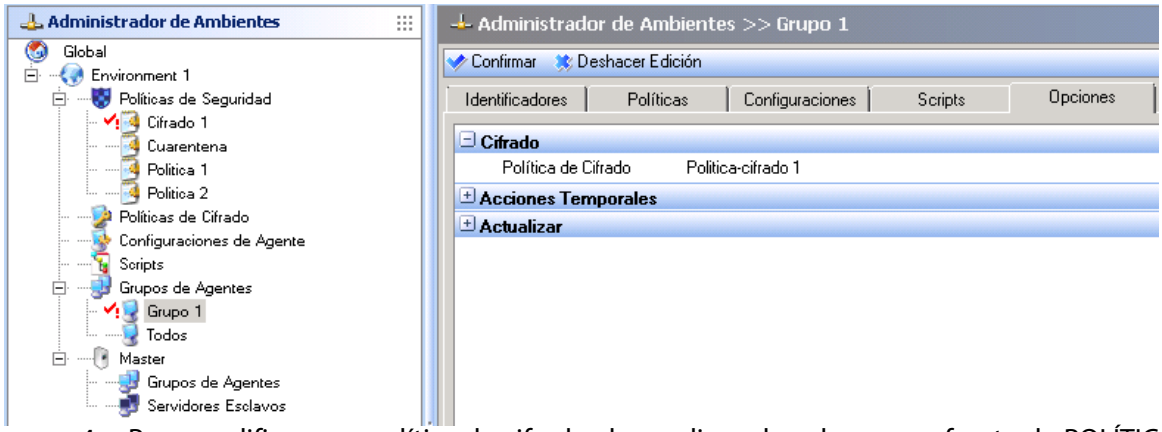
- Desactivado
- Usar solicitudes de cambio.
- Nunca caduca.
- Expira con una fecha.
  En este caso el admnistrador deberá indicar La edadmaxima para unna cuenta de invitado.

APLICANDO POLÍTICAS DE CIFRADO A UN GRUPO DE AGENTES

Las políticas de cifrado son aplicadas a grupos de agentes.

Para aplicar una política de cifrado a un grupo de agentes, siga las siguientes instrucciones:

1. Clic en Grupo de agentes en el panel de administrador de ambiente.
2. Edite el grupo de agentes que aplicaran o modificarán la política de cifrado.
3. Clic en la pestaña Opciones para mostrar la política de cifrado aplicada al grupo de gentes.



4. Para modificar una política de cifrado, haga clic en la columna en frente de POLÍTICA DE CIFRADO y haga clic en el botón de exploración ... .
   La lista del menú desplegable mostrará las políticas de cifrado existentes.

5. Seleccione la política de cifrado que se aplicará al grupo de agentes.
6. Verifique sus cambios.
7. Realice una sincronización.

RECUPERACIÓN

Recuperación de contraseña cuando se usa cifrado de archivos

Desde el Agente

Generalidades

Cuando el usuario crea una contraseña, una contraseña de copia de seguridad se genera automáticamente.

Para cambiar una contraseña perdida, el usuario puede ponerse en contacto con el administrador. El administrador localizará la contraseña de seguridad y la enviará al usuario.

Una vez que el administrador encuentra la contraseña de seguridad, puede copiarla, pegarla y enviarla por correo electrónico al usuario. El usuario puede copiar y pegar directamente la contraseña en el campo indicado.

La contraseña de seguridad funciona de la misma manera como la contraseña habitual.

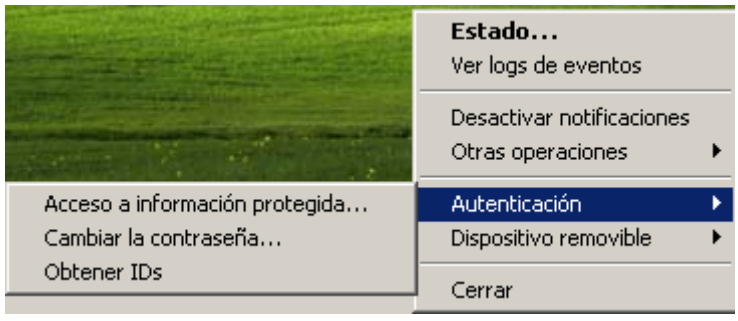
Para ayudar al administrador a localizar una contraseña de seguridad se usa el ID de usuario en lugar del nombre de usuario, el usuario puede proceder como se describe más adelante en " Obtener Id ".

- Si no se usa el Directorio Activo, los usuarios que trabajan en estaciones de trabajo diferentes pueden tener el mismo Nombre de usuario (ejemplo: una cuanta de administrador), pero no el mismo ID de usuario.
  Para encontrar un usuario por su ID, póngase en contacto con el administrador.
  La columna Dominio sólo contiene nombres de máquina.

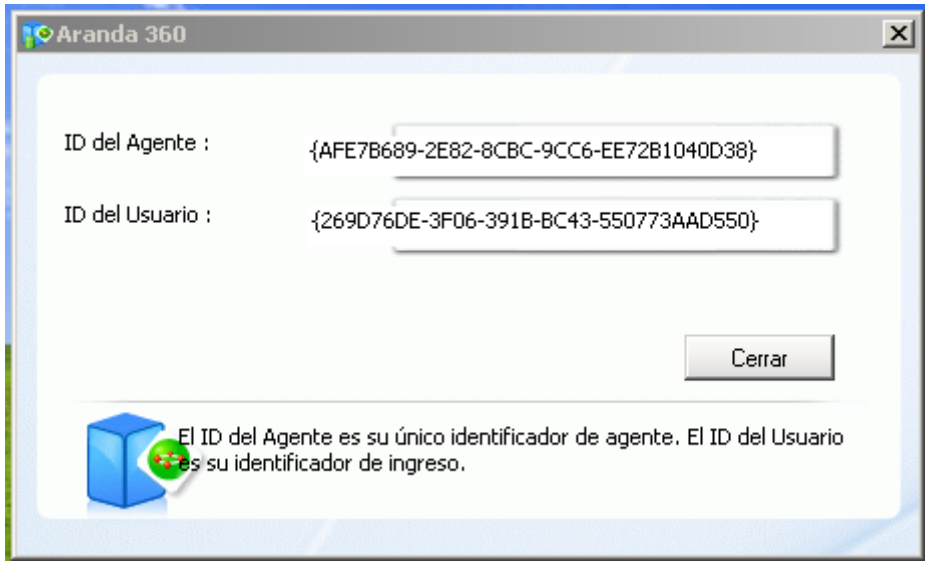
Obtener IDs

Para obtener el ID de un usuario, el usuario debe ejecutar los siguientes pasos:

1. Clic derecho en el icono del monitor  de Aranda 360.
2. Seleccione Autenticación > Obtener Id.

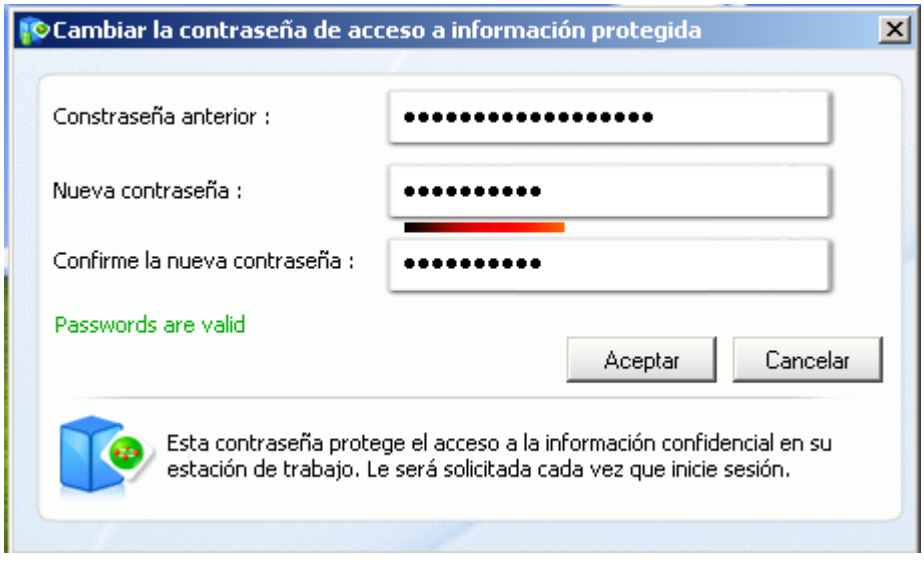


3. El ID del usuario se mostrará.
   Copiar el número Id del usuario y enviarlo por mail al administrador.



- El usuario debe cambiar su contraseña de copia de respaldo tan pronto como sea posible con el fin de que quede como una contraseña anterior.

4. Pegar la contraseña de respaldo enviada por el administrador en el campo de Contraseña anterior.
   Escribir y confirmar una nueva contraseña.



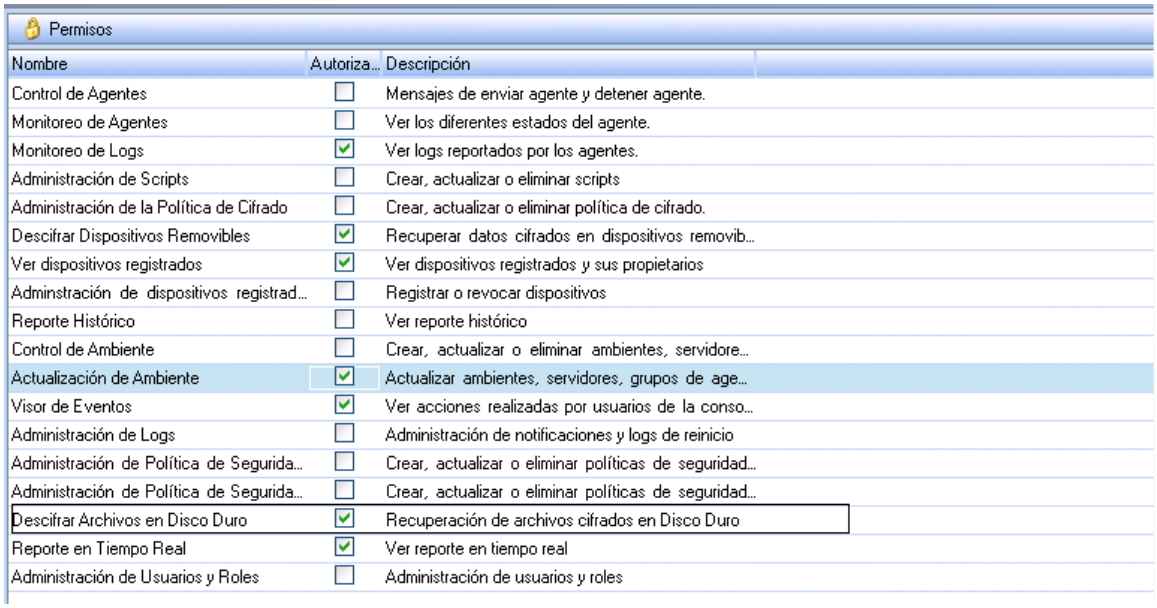
- Si el usuario crea una nueva contraseña en un equipo y va a otro equipo con la misma cuenta, el usuario debe introducir la nueva contraseña y no la contraseña de respaldo.

Desde el Administrador

Requerimientos

Con el fin de que el administrador pueda buscar contraseñas de respaldo, Administrar Roles > Permisos > Descifrar datos en disco duro debe ser establecida como Autorizada.

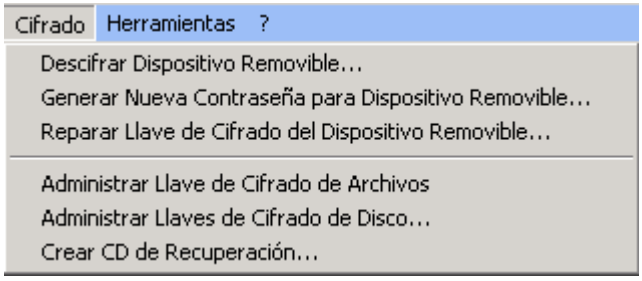
- El administrador de roles se utiliza para crear roles asignados a usuarios de la consola de administración de Aranda.



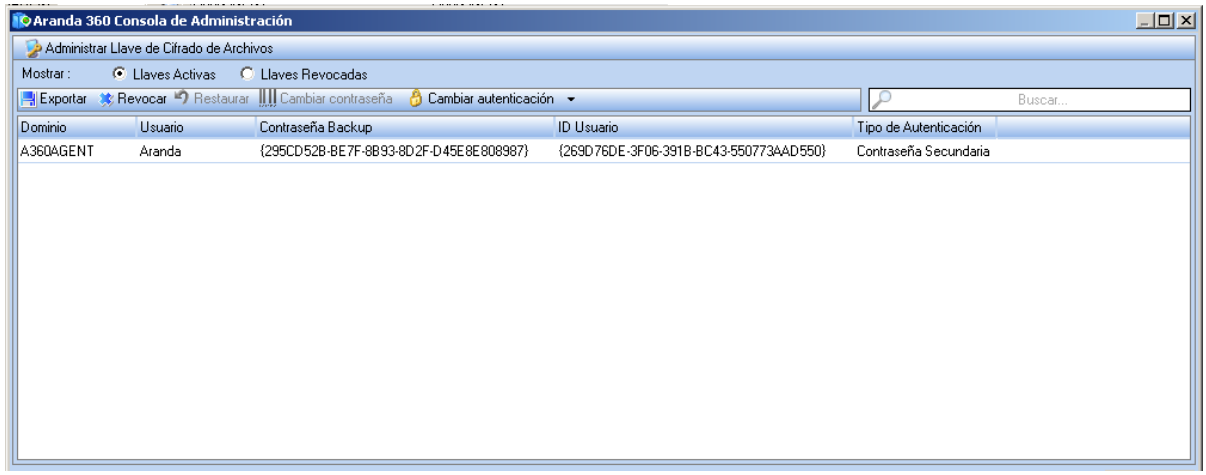
Recuperación de contraseña

Para recuperar una copia de respaldo de la contraseña, el administrador debe:

1. Seleccionar Cifrado > Administrar la información de cifrado de archivos.



2. Introducir la contraseña para el certificado de la consola.
   La ventana de Administrar la información de cifrado de archivos se mostrará.



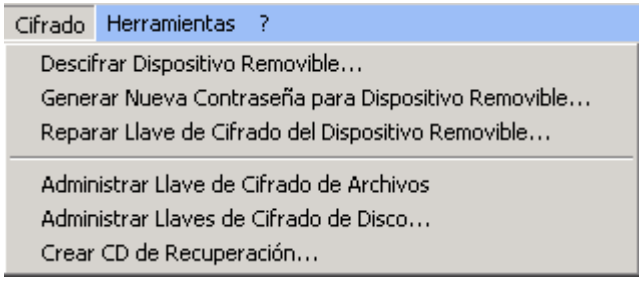
   - Si recibe un mensaje de error, la consola no se ha configurado correctamente. Compruebe que las rutas del certificado de la consola son correctas.

3. Buscar el nombre de usuario en la lista de claves activas.
   Para listas largas, puede ser utilizado el campo de búsqueda para localizar rápidamente el nombre de usuario.
4. Enviar la contraseña de respaldo para el usuario.

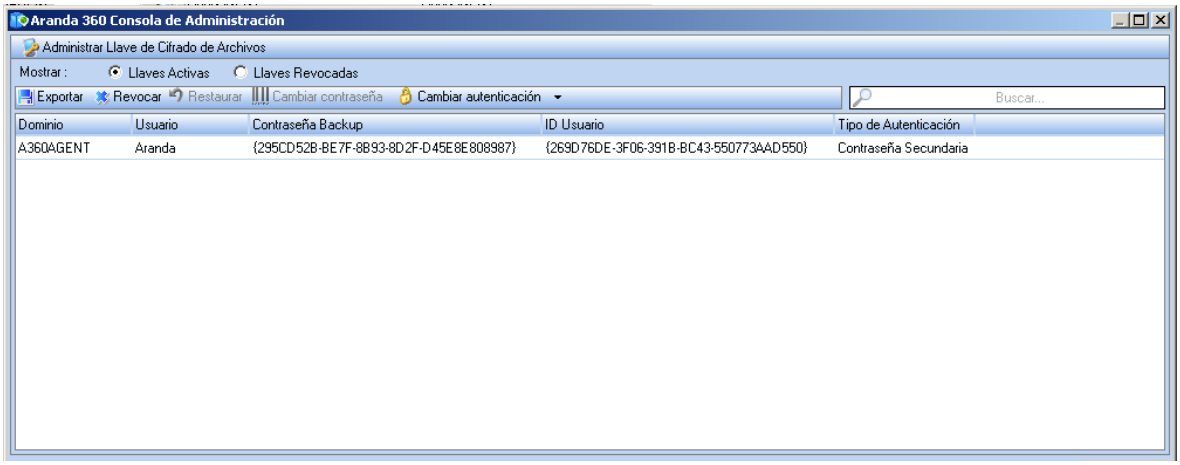
Cambiando la segunda contraseña de autenticación

Para cambiar la contraseña secundaria de un usuario utilizada para el cifrado, el administrador debe tener en cuenta los siguientes pasos:

1. Seleccionar Cambio de Contraseña bajo la opción Cifrado > Administrar la información de cifrado de archivos.



2. Introducir la contraseña para el certificado de la consola.
   La ventana de Administrar la información de cifrado de archivos se mostrará.



3. Seleccionar Cambio de contraseña.
4. Ingresar y confirmar la nueva contraseña.

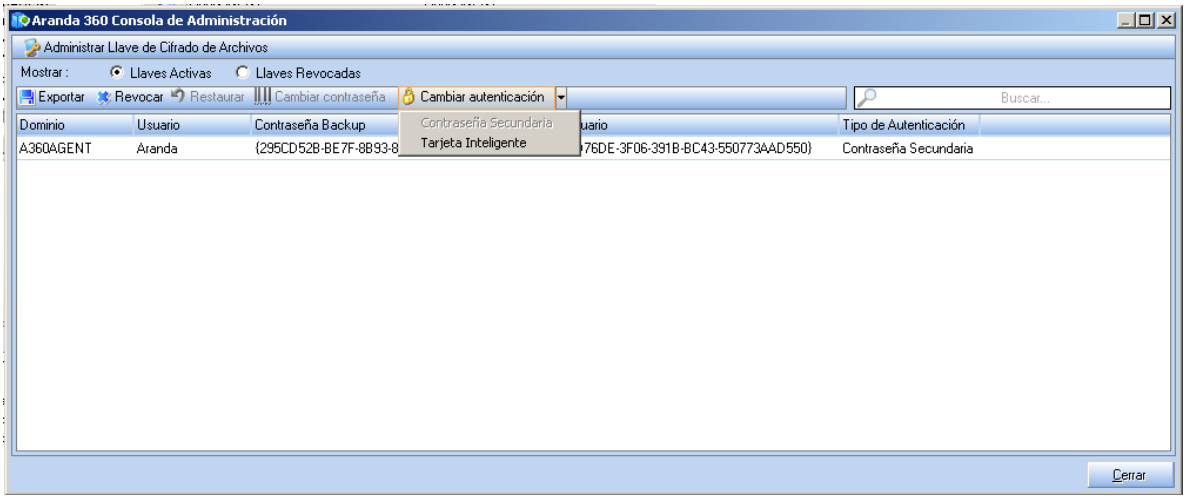
5. Clic en OK.

Para activar la nueva contraseña, el usuario debe cerrar la sesión en el sistema y luego iniciar sesión.
Para que el proceso de cifrado entre en vigencia, el usuario debe introducir la nueva contraseña de autenticación secundaria después del inicio de Windows.
El agente de Aranda 360 debe estar conectado.

Cambiando el tipo de autenticación

Para cambiar el tipo de autenticación del agente, el administrador debe seguir los siguientes pasos:

1. Hacer clic en el nombre de usuario para resaltarlo.
2. Hacer clic en Cambiar autenticación y seleccionar el tipo de autenticación en el menú desplegable.



- La política de cifrado asignada al agente debe estar configurada para que tenga el mismo tipo de autenticación que el definido para el usuario.

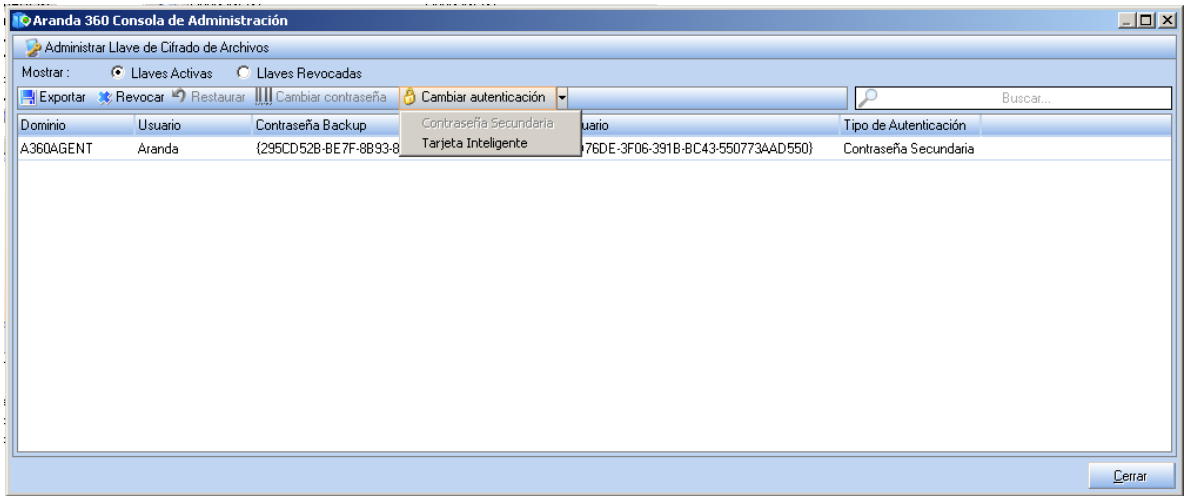
3. Ingresar la información requerida.
4. Validar sus modificaciones.
5. Sincronizar.

- Después de que el agente de Aranda 360 vuelve a conectar al servidor y recibe nueva información, el usuario debe cerrar la sesión y volver ha iniciarla para poder aplicar el nuevo el tipo de autenticación.

Cambiando la autenticación tarjeta inteligente

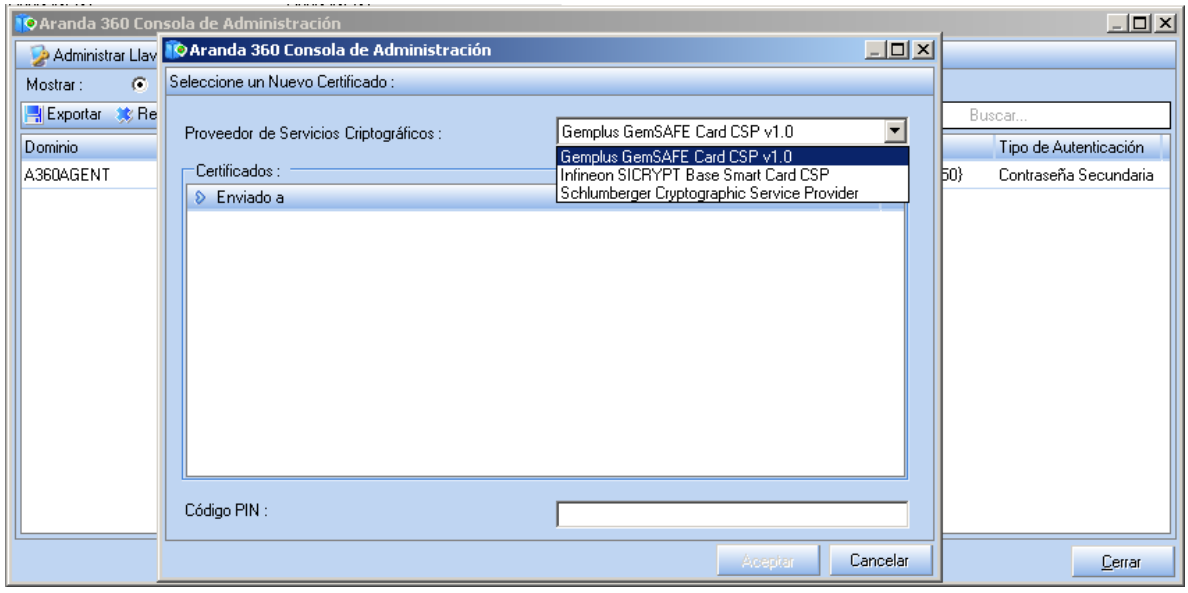
Para cambiar a la autenticación de tarjetas inteligentes, el administrador debe seguir los siguientes pasos:

1. Hacer clic en el nombre de usuario para resaltarlo.
2. Hacer clic en Cambiar autenticación y seleccionar el tipo tarjetas inteligentes en el menú desplegable.



3. Indicar la siguiente información:

    - Seleccionar el CSP.
    - Seleccionar el certificado.



4. Clic en OK.
5. Sincronizar.

- Después de que el agente de Aranda 360 vuelve a conectarse al servidor y recibe nueva información, el usuario debe cerrar la sesión y volver a iniciarla para aplicar el nuevo el tipo de autenticación.
  Al inicio de sesión, Aranda 360 solicitara al usuario que inserte la tarjeta inteligente e introduzca el código PIN (proporcionado por el CSP).

Revocando y restaurando las claves de usuario

Hay dos tipos de claves de usuario en Administrar Información del cifrado de archivo:

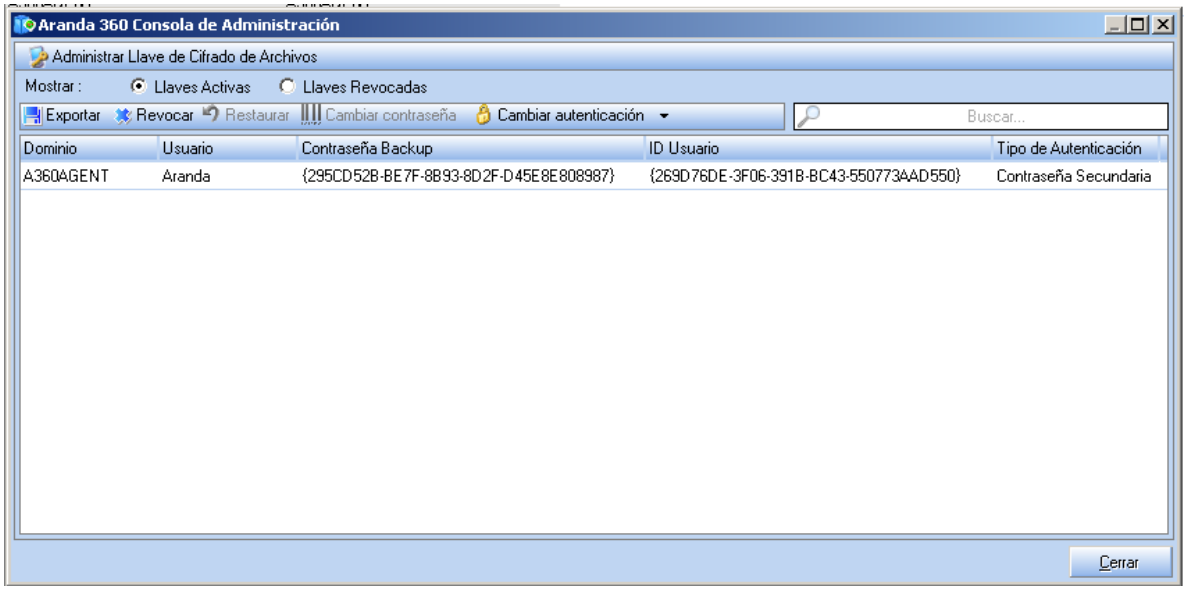
- Claves activas
  Son las claves que pertenecen a usuarios activos que pueden autenticarse.

- Claves revocadas
  Son las claves que pertenecen a usuarios revocados. El administrador puede activar claves revocadas.

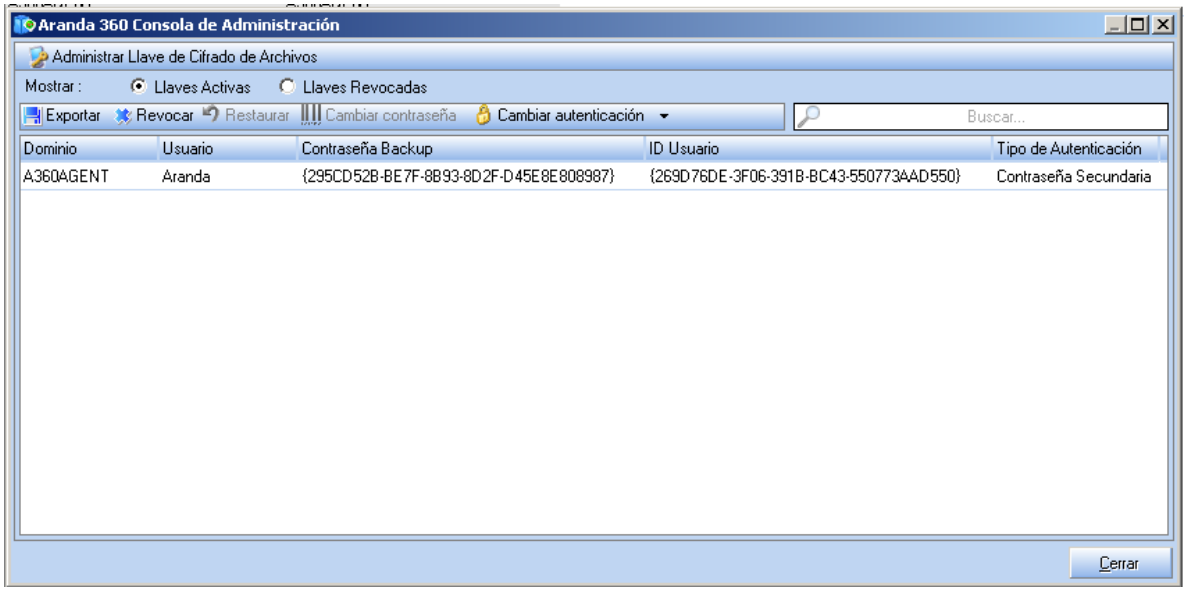
- Un usuario con una clave revocada no será capaz de acceder a los archivos cifrados. La autenticación será rechazada.

Para restaurar o revocar una calve de usuario, el administrador debe ejecutar los siguientes pasos:

1. Buscar un usuario utilizando el campo de búsqueda y hacer clic en Revocar.



2. El usuario es eliminado de la lista de claves activas. Por otra parte, su nombre aparecerá en la lista de claves revocados.
Para comprobar esto, haga clic en el botón de radio de claves revocadas.



3. Varias acciones están disponibles en la barra de herramientas:

- Exportar la clave de usuario como un archivo RecoveryKey.srk.
- Eliminar la clave de usuario.
- Restaurar la clave de usuario (Clave Revocada > Clave Activa).
- Cambio de contraseña de usuario.
- Cambio de autenticación de usuario.

Recuperación de información desde archivos cifrados (descifrado)

El administrador puede tener que decodificar algunos o todos los datos en un disco duro.

Ejemplos:

- Cuando un usuario deja la empresa.
- Cuando los datos se recuperan de un disco duro dañado.

Conjunto de llaves de recuperación

Si el administrador tiene que descifrar más de un disco duro, puede crear un conjunto de claves de recuperación.

El conjunto de claves de recuperación es un archivo que se puede copiar en una memoria USB y que puede ser usado para descifrar manualmente cada equipo individualmente.

En el paso 3 del procedimiento de descifrado de datos manual, el administrador selecciona los nombres de usuario que quiere incluir en el conjunto de claves de recuperación.

A continuación, puede cambiar el nombre del archivo (si es necesario), y exportarlo a un dispositivo USB.

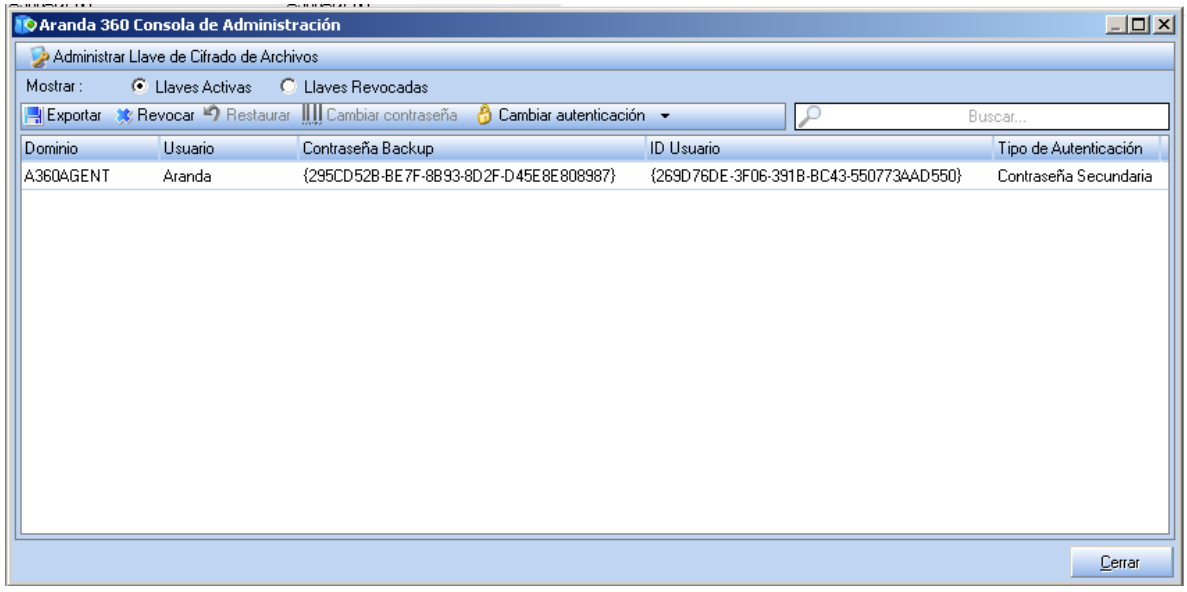
- El conjunto de claves de recuperación incluye todas las claves de maquina utilizadas por los usuarios seleccionados.

Descifrado de datos manualmente

Desde el administrador

Para descifrar los datos manualmente, el administrador debe seguir las siguientes instrucciones:

1. Seleccione Cifrado > Administrar la información de cifrado de archivos.
2. Introduzca la contraseña para el certificado de la consola.
   La ventana para Administrar la información de cifrado de archivos se mostrará.

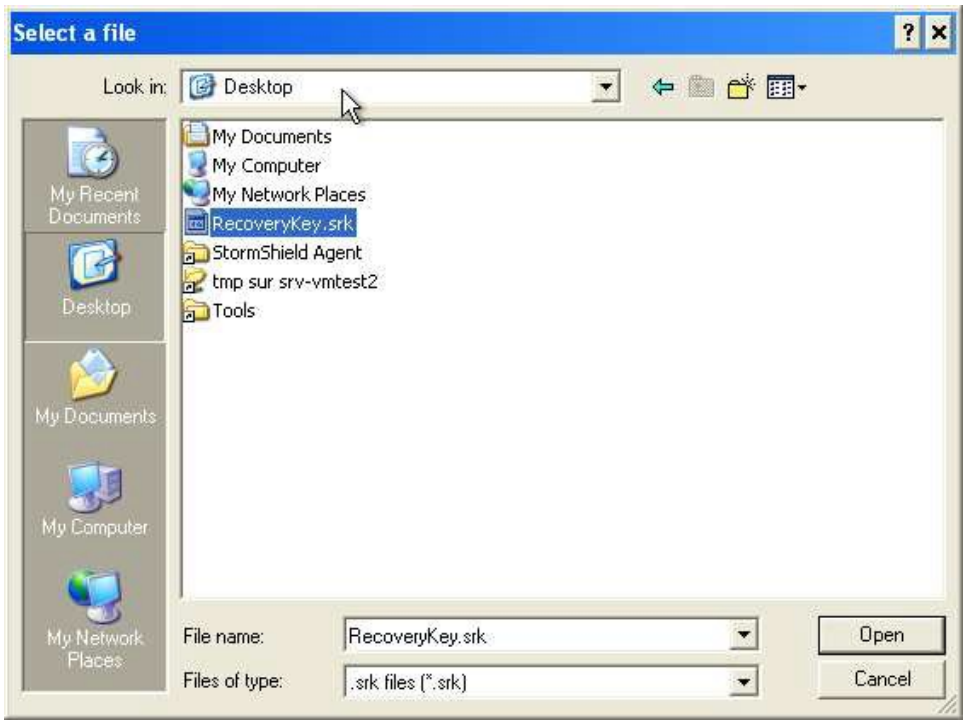


- Si recibe un mensaje de error, la consola no se ha configurado correctamente.

3. Busque el nombre de usuario en la lista.
   Para listas largas, puede utilizar el campo de búsqueda para localizar el nombre de usuario rápidamente. Puede seleccionar varios nombres de usuario para crear un conjunto de claves.

- Si el Directorio Activo no se utiliza, los usuarios que trabajan en estaciones de trabajo diferentes pueden tener el mismo nombre de usuario (ejemplo: una cuenta administrador), pero no el mismo ID de usuario. Para localizar a un usuario con su nombre de usuario, solicítelo al administrador por correo electrónico..

4. Después de seleccionar el nombre de usuario (o ID de usuario), haga clic en Exportar.
5. Seleccione la ruta y nombre de archivo.
   El archivo se guarda como un archivo [RecoveryKey]. Srk que contiene las claves utilizadas para la recuperación de archivos.
   Los archivos SRK pueden ser exportados de la consola y usados por el agente de Aranda 360.



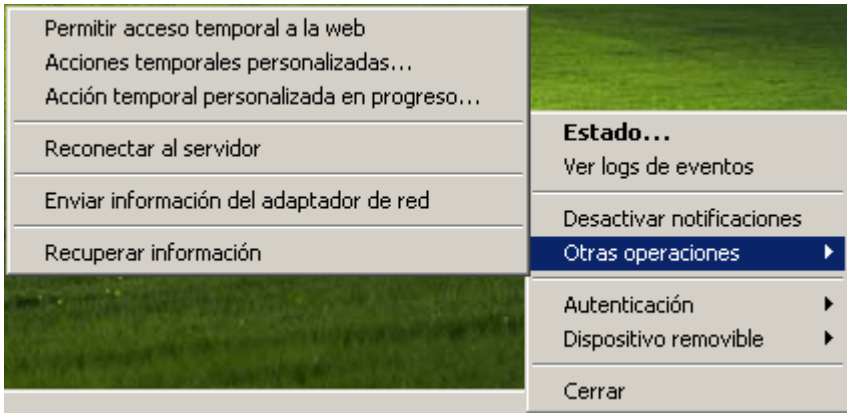
El archivo SRK puede guardarse en una memoria USB o en otro servidor.

- Es altamente recomendable que el archivo SRK sea almacenado en un lugar seguro, cuyo acceso debe ser reservada para personal Autorizado (administradores).

Desde el agente

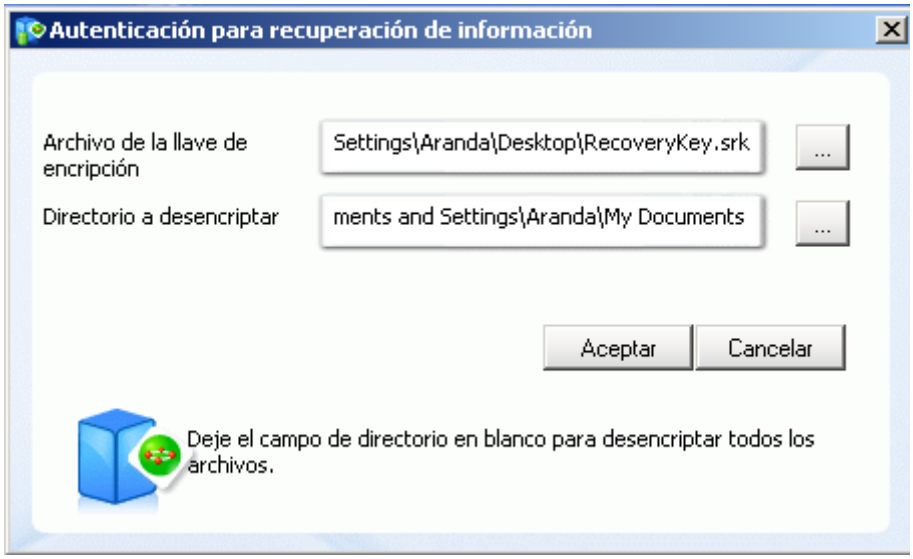
Para descifrar los datos de forma manual, el usuario debe proceder con los siguientes pasos:

1. Haga clic en el icono del Monitor de Aranda 360



2. Seleccione Otras operaciones> Ejecución de proceso de recuperación de datos.

3. En el campo para la clave de Cifrado de archivo, escriba la ruta y el nombre de la clave de recuperación o haga clic directamente en el botón Examinar.



Utilice el campo Carpeta para descifrar si usted necesita para descifrar una carpeta a la vez (por ejemplo: si realiza la recuperación de datos en un disco duro diferente al disco de la maquina)

4. Reinicie la maquina.
El proceso de descifrado se inicia al reiniciar el equipo.

Si la política de cifrado no se removió con anterioridad, esta se aplicara una vez más al reiniciar el agente, con el fin de cifrar los archivos nuevamente.
El usuario puede seguir trabajando durante el proceso de recuperación. El descifrado continúa incluso cuando el ordenador está bloqueado.

Si repite el paso 1 para iniciar el proceso de recuperación de datos antes de que el agente haya reiniciado, se le preguntará si desea cancelar la recuperación de datos o realizar otro proceso de recuperación.

Descifrado automático

Para lograr un proceso exitoso de descifrado automático:

1. El agente de Aranda 360 debe ser capaz de conectarse con el servidor Aranda 360.
2. En el Editor de Configuración bajo Configuración de agente, la opción Permitido detención de agente debe estar activada.
3. En el Administrador de Ambientes bajo la opción Servidor Principal > Cifrado:
    - Descifrado de datos durante la desinstalación se debe establecerse en Activado.
    - La fecha de desinstalación deberá estar comprendida entre la fecha de inicio de desinstalación permitida y la fecha permitida de finalización de la desinstalación.

- Sólo los archivos cifrados con una clave de maquina pueden ser recuperados durante un descifrado automático.
  Para los archivos cifrados con una clave de usuario, el administrador debe realizar una de las siguientes acciones:
    - Llevar a cabo una recuperación manual.
    - Volver a instalar el agente de Aranda 360.Transferir los archivos cifrados con una clave de usuario a una carpeta cifrada con una clave de máquina.
    - Utilice SURT para descifrar los archivos después de desinstalar Aranda 360 si el usuario no desea instalar el agente de Aranda 360 de nuevo.

Si el parámetro Descifrar datos durante la desinstalación es activado en la política de cifrado, el proceso de descifrado iniciara automáticamente cuando el usuario ejecute el proceso Srend.exe para desactivar un agente de Aranda 360.

Durante el descifrado automático, no es necesario que reinicie el equipo si ningún usuario ha iniciado sesión previamente (por ejemplo: cuando se desístala con una política de Directorio Activo GPO).

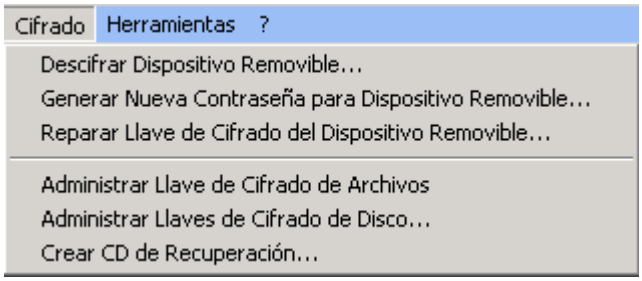
De cualquier modo, si el usuario ha iniciado o inicia sesión (sin reiniciar), el equipo debe ser reiniciado. Al usuario se le pedirá que reinicie el ordenador.

Recuperación de contraseña cuando se usa cifrado de disco completo

Procedimiento de recuperación

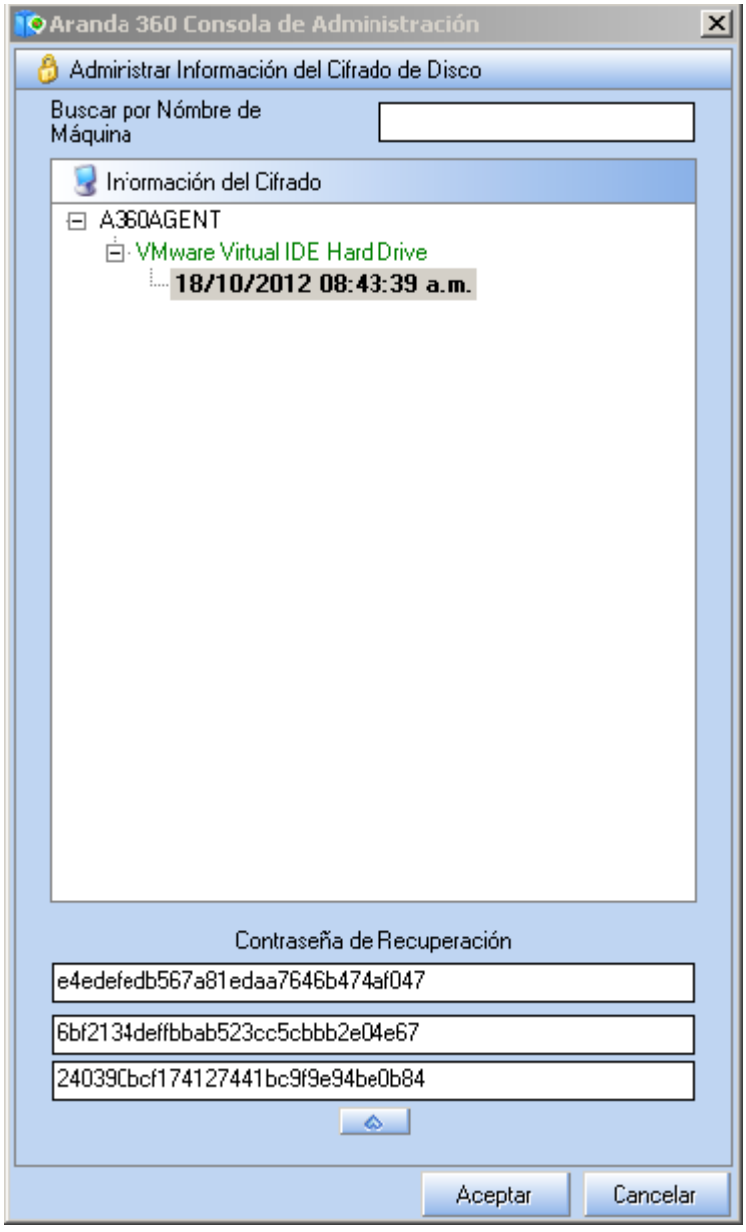
Para acceder a la recuperación de la contraseña cuando se utiliza cifrado de disco completo, el administrador debe seguir estos pasos:

1. Diríjase a Cifrado > Administrar información de disco cifrado.



2. Ingrese la contraseña para el certificado de consola.

3. Los discos cifrados del agente se detectan automáticamente y aparecen listados en una estructura de árbol en la ventana.
   Para localizar un disco o un sistema de cifrado, utilice la barra de búsqueda por el nombre de host.



4. Haga clic en la fecha bajo el nombre del disco. La contraseña será mostrada en el campo Recuperación de contraseña.
   Esta clave se envía al agente por teléfono o correo electrónico con el fin de recuperar los datos cifrados del disco.

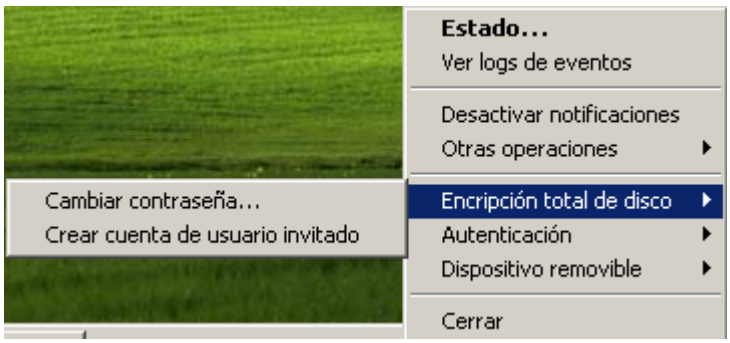
- Si varias fechas están asociadas con un disco dado, se recomienda utilizar la contraseña de recuperación situada debajo de la fecha más reciente.
  Las fechas de recuperación anteriores se mantienen en la lista de referencia en la eventualidad de que surgiera un problema.

- Si el administrador ha habilitado recuperación de la contraseña por una vez en la política de cifrado (en los parámetros de cifrado de disco completo), y si el usuario
  No se puede conectar al servidor Aranda 360, la recuperación de la contraseña no será actualizada automáticamente.
  El administrador enviará al usuario una contraseña anterior que seguirá siendo válida hasta la próxima conexión al servidor server.

Cambiando la contraseña

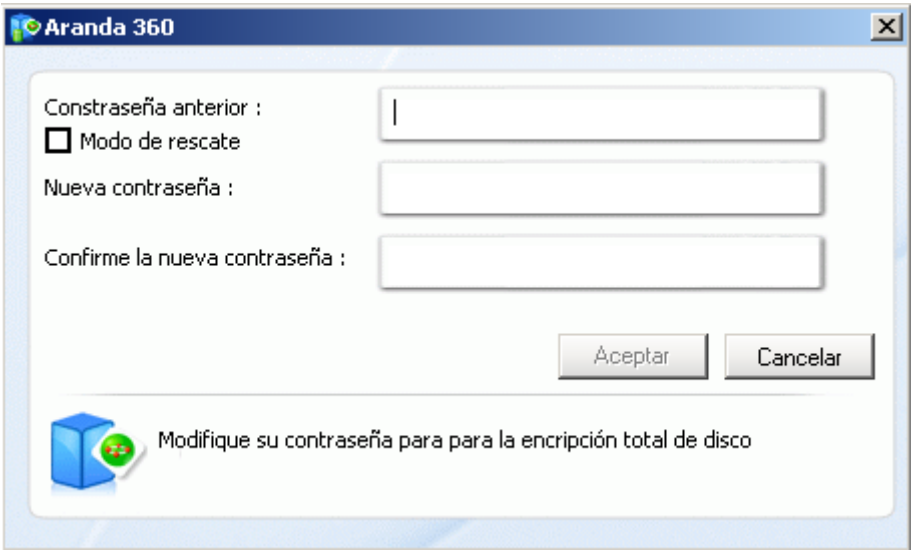
Cambiando la contraseña a través del agente Aranda 360

1. En la maquina del agente:
   - Haga clic-derecho en el icono del monitor de Aranda.
   - Seleccione Cifrado de disco completo > Cambiar su contraseña.



2. En la ventana, ingrese la contraseña anterior.
   Si no recuerda su contraseña anterior, ingrese la contraseña recuperada que le envió su administrador.
   Si usted marca la casilla Contraseña recuperada la contraseña se mostrara en texto claro.
   Si no marca la casilla, la contraseña será convertida automáticamente al modo QWERTY.

Pegue la contraseña recuperada enviada por el administrador en el campo Contraseña anterior.



3. Ingrese y confirme la nueva contraseña.
4. Haga clic en OK.

- Si el usuario recuerda la contraseña anterior, puede introducir la contraseña de usuario anterior en lugar de la contraseña recuperada.

Cambiando la contraseña hasta el arranque

Si no recuerda su contraseña de usuario, puede iniciar el equipo utilizando la contraseña recuperada (Admin).

Para ello, ejecute los siguientes pasos:

1. Presione F2 (admin).
2. Ingrese la contraseña recuperada en la ventana de notificación.
3. resione Enter.

Recuperación de información de un cifrado total de disco a través de un CD

El administrador realiza una recuperación de datos de un cifrado de disco completo a través de un CD si el disco cifrado no se ha iniciado correctamente.

La recuperación se utiliza principalmente para el descifrado de disco y cuando la máquina no se puede iniciar en condiciones normales. Ejemplos: Contraseña Perdida o caída del sistema, incluso cuando se arranca en modo seguro.

El CD-ROM permitirá a los usuarios:

- Descifrar información del disco duro.
- Cambiar contraseñas.
- Descifrar y eliminar el gestor de arranque.

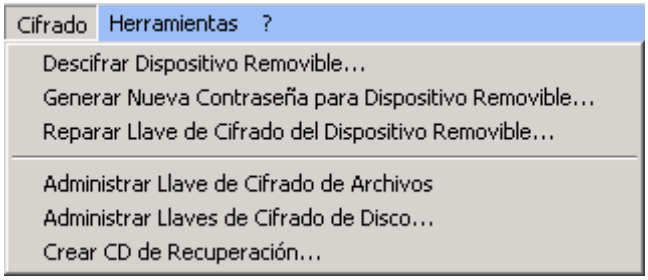
Crear un CD para recuperación de datos

En la consola de administración de Aranda, el administrador puede crear un CD-ROM con el fin de:

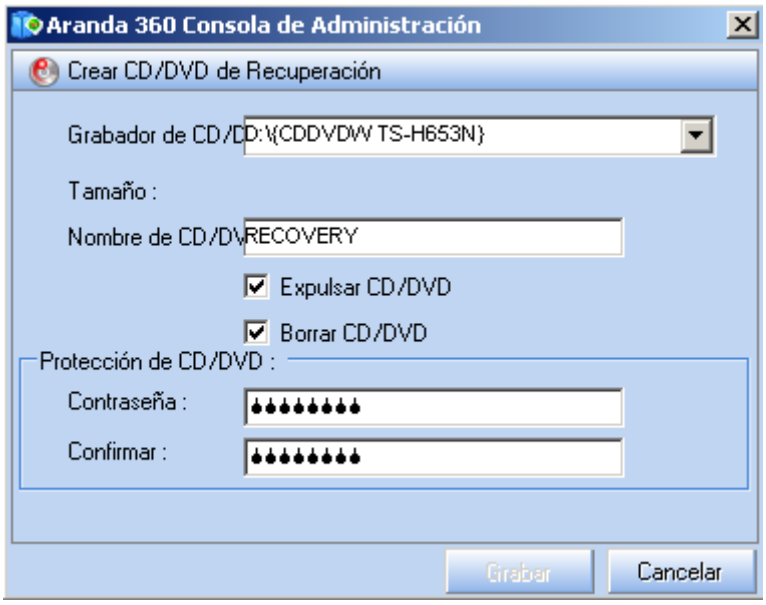
- Poner en marcha una recuperación del disco en el equipo del agente.
- Descifrar todos los datos cifrados.

Para recuperar el disco cifrado a través de un CD, el administrador debe:

1. Ir a Cifrado > Crear CD de Recuperación.



2. Especificar la siguiente información:



- Seleccionar el grabador de CD.
- Cambiar el nombre del CD de recuperación.
  - Marcar la casilla Expulsar disco para iniciar el disco después de la grabación.
  - Marcar la casilla Borrado de disco para formatear el CD antes de escribir en el. Esto funciona si el CD es re escribible.
- Ingrese y confirme una Contraseña para proteger el CD.

Si es necesario defina una contraseña para proteger el CD. En efecto, el CD puede ser usado para recuperar todos los datos guardados en la maquina del agente que tenga discos cifrados.

- El CD puede ser utilizado para acceder a todos los datos de la compañía. Las personas no autorizadas pueden acceder a este CD y utilizarlo para robar información.
  Por tanto, es esencial que se tomen medidas de seguridad extremas con el CD.

3. Clic en grabar para iniciar el proceso.

Recuperando el equipo (vía CD)

Se recomienda descifrar archivos con la herramienta de recuperación de Aranda.

Si el cifrado falla.

El proceso de cifrado puede fallar debido a un bloque dañado

Para reparar una maquina, el usuario debe:

1. Ingresar un CD grabado.

   - Aranda 360 proporciona todas las herramientas necesarias para la recuperación.

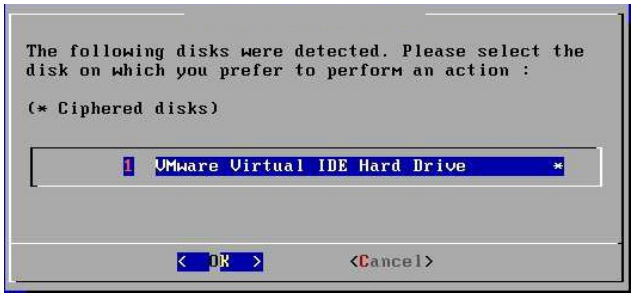
2. En el inicio, escriba la contraseña del CD.

3. Seleccione Reparar la maquina.

4. Seleccione el tipo de proceso y haga clic en OK.

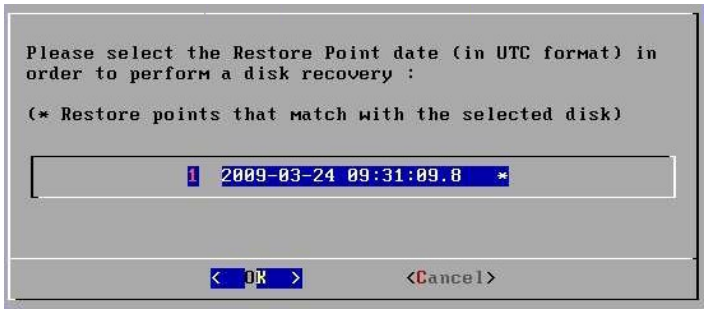
   - Si Usted escoge Selección automática de disco, por favor proceda al paso

   - Si usted escoge Selección manual de disco, seleccione los discos cifrados que son detectados por el sistema.



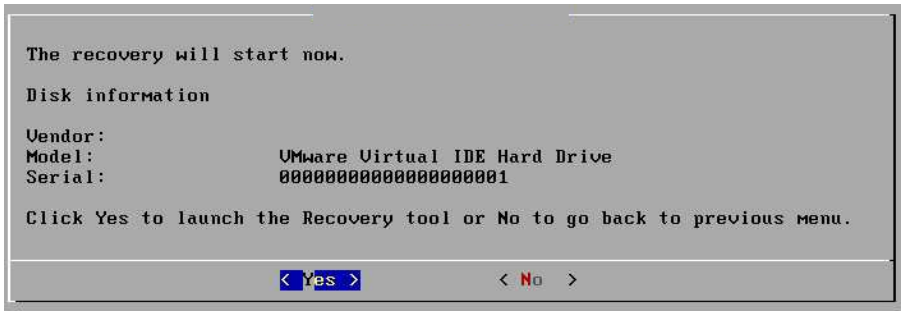
5. La ventana de información del disco duro aparecerá.
   Seleccione Sí para continuar.

6. Seleccione la fecha del punto de restauración para realizar la recuperación del disco.



- El punto de restauración incluye todas las claves necesarias para recuperar los datos del sistema.
  La fecha y las marcas de tiempo permiten utilizar claves antiguas como copias de seguridad, en caso de que surja un problema con la fecha del punto de restauración más reciente.

7. Si se selecciona Selección de Disco automática, se le solicitará que inicie la recuperación inmediatamente.
   Seleccione Si para proceder.



8. El proceso de recuperación comenzará.

Recuperación en modo Windows

El usuario puede realizar este tipo de recuperación sólo en discos duros adicionales que no se ejecutan en el sistema.

Ejemplo:

Si el usuario no tiene una unidad de CD-ROM a su disposición, puede extraer el disco duro de su ordenador y conectarlo de forma externa a otro ordenador que si tenga una unidad de CD-ROM para llevar a cabo el proceso de recuperación.

Para ejecutar la recuperación en modo Windows, el usuario debe seguir los pasos a continuación:

1. Ingrese el Cd de recuperación.
   Seleccione OK para proceder.

2. Ingrese la contraseña.
   Seleccione OK para continuar.

3. Seleccione Reparar su máquina.
   Seleccione Continuar.

4. Seleccione el tipo de proceso.
   Continúe con OK.

5. Una vez que el proceso de recuperación se ha completado, salga del asistente.
   Seleccione Sí para continuar

Cambiando la contraseña

Si el usuario olvida la contraseña de cifrado, Aranda 360 ofrece una opción para guiar al usuario a través del proceso de cambio de contraseña.

Este proceso aplica parar recuperaciones usando un CD de recuperación y recuperaciones modo Windows.

Para cambiar la contraseña de cifrado, el usuario debe:

1. Seleccione Cambiar la contraseña de usuario.
2. Ingrese la nueva contraseña de cifrado.
3. Confirme la contraseña.

El usuario recibe una notificación de cambio de contraseña si este fue exitoso.

DESINSTALANDO LOS AGENTES ARANDA 360

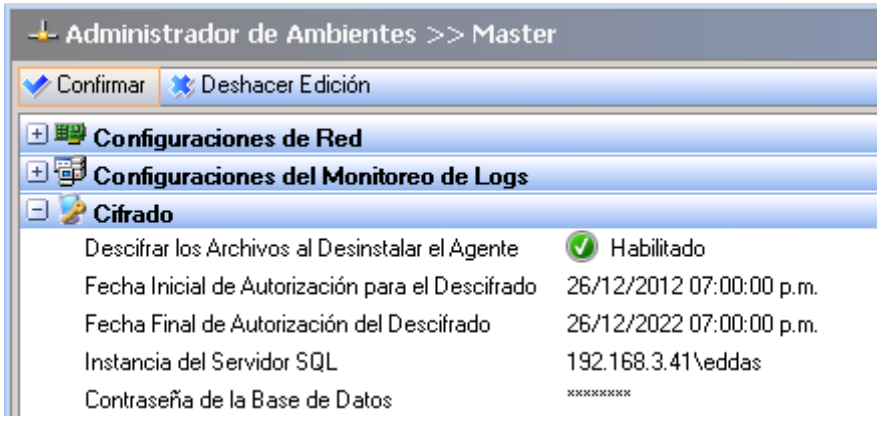
Descifrado previo a desinstalación

Cuando los agentes se desinstalan, Aranda 360 debe descifrar las carpetas y ficheros almacenados en el disco duro del agente, de modo que los usuarios pueden acceder a sus datos después de la eliminación de software.

Varios agentes se pueden desinstalar al mismo tiempo mediante directivas de grupo por el directorio activo (GPO), sin necesidad de intervención del usuario.

Sin embargo, con el fin de utilizar los GPO en el panel del Administrador Ambientes, los parámetros deben configurarse de la siguiente manera:

- El agente debe estar conectado al servidor.
- La opción Descifrar en la desinstalación debe ser activada.



- La Fecha de inicio permitida de desinstalación y Fecha de finalización permitida de desinstalación deben ser especificadas.
  Durante este período, los agentes pueden solicitar la clave de cifrado al servidor la cual permite que Aranda 360 pueda descifrar el disco duro sin la necesidad realizar la autenticación del usuario.

Sólo los archivos cifrados con la clave de maquina son recuperados con un descifrado automático.

Para recuperar los archivos cifrados con una clave de usuario, el administrador debe realizar una de las siguientes acciones:

- Realizar una recuperación manual.
- Vuelve a instalar el agente de Aranda 360.
- Transferir los archivos cifrados con una clave de usuario a una carpeta cifrada con una clave de máquina.

- Utilice SURT para descifrar los archivos después de desinstalar Aranda 360 en caso de que el usuario no dese instalar el agente de Aranda.

Si el proceso de descifrado automático es ejecutado y procedimiento de recuperación falla, el agente de Aranda 360 se desinstalara de todas formas. Sera necesario descifrar los archivos manualmente.

Cambiando una cuenta de usuario sobre una maquina

Después de cambiar una cuenta de usuario en un equipo, compruebe que la fecha permitida para iniciar una desinstalación y la fecha permitida para terminar una desinstalación cubren el período de tiempo hasta que el usuario inicia sesión por primera vez.

Esto asegurará que:

- El agente podrá solicitar la clave de cifrado al servidor.
- El usuario será capaz de acceder a las funciones de cifrado.

Para mantener la seguridad del cifrado, se debe establecer el tiempo permitido de desinstalación al mínimo.

Capítulo 13 - SURT

ACERCA DE ESTE CAPÍTULO

Este capítulo describe cómo usar SURT y su interfaz grafica. Se incluye:

- Generalidades.
- Cifrando un archivo.
- Descifrando y cifrando archivos:
  - Procedimiento.
  - Barra de progreso.
- Referencia del menú:
  - Interfaz grafica.
  - Opciones.
- Cifrado de dispositivos extraíbles y SURT:
  - Conjunto de configuraciones para dispositivos extraíbles.
  - Configuraciones SURT.
- Recuperación de datos cifrados a través de la función de cifrado de datos:
  - Requerimientos.
  - Procedimiento.

GENERALIDADES

- Un usuario que no tenga Aranda 360 instalado en su ordenador puede descargar gratis la herramienta SURT de cifrado de Aranda 360 en el sitio web de Aranda Systems "http://www.Aranda.com/Downloads".

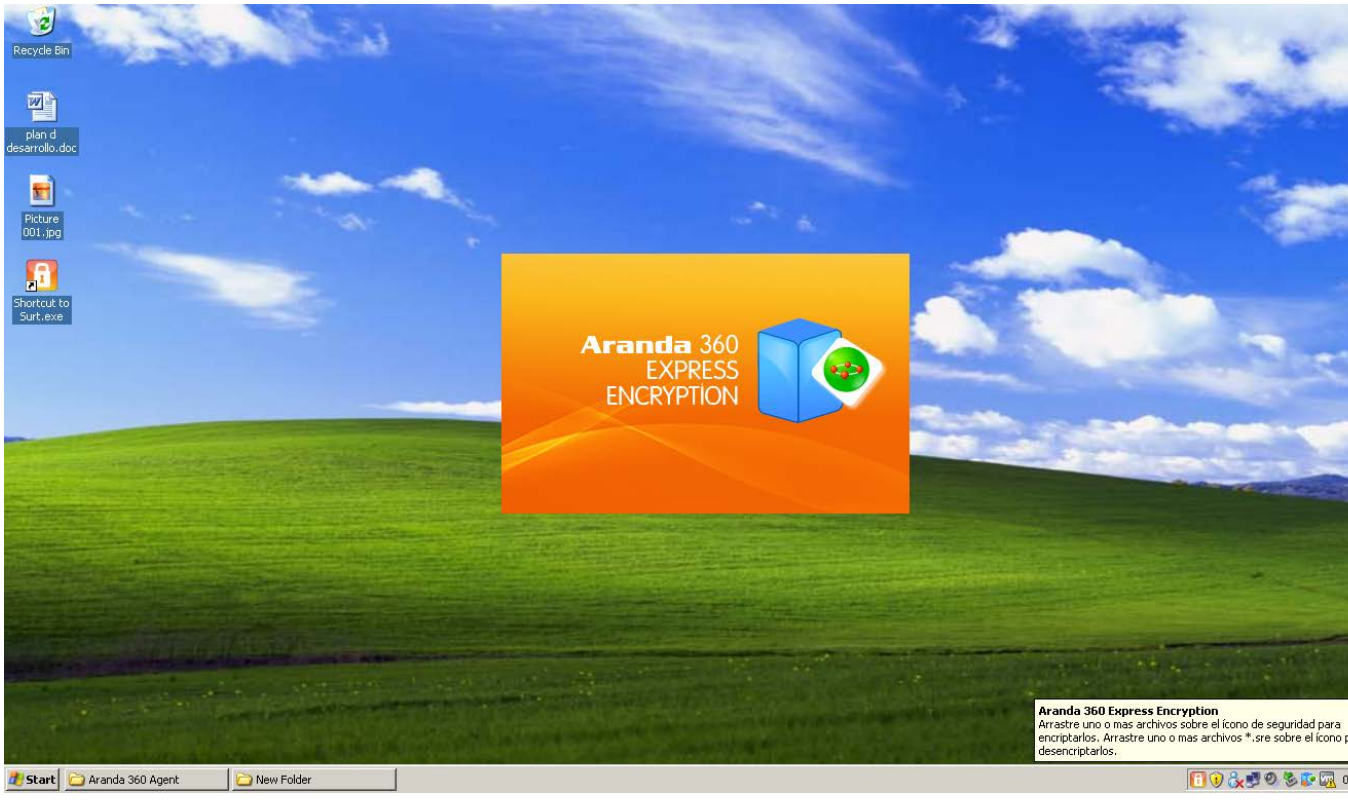
SURT (también llamado Aranda 360 Express Encryption) es un software portable sin tener que ser instalado en su computador.

SURT está asociado con la extensión de archivo .sre. Por lo tanto, cuando se copia a la maquina, se muestra como Surt.exe.

Si hace doble clic en SURT, la siguiente ventana aparecerá incluyendo los iconos de abajo:

- Icono de la bandeja del sistema: .
- Superposición de escritorio: .
- Icono del ejecutable: 

.



CIFRANDO UN ARCHIVO

Procedimiento

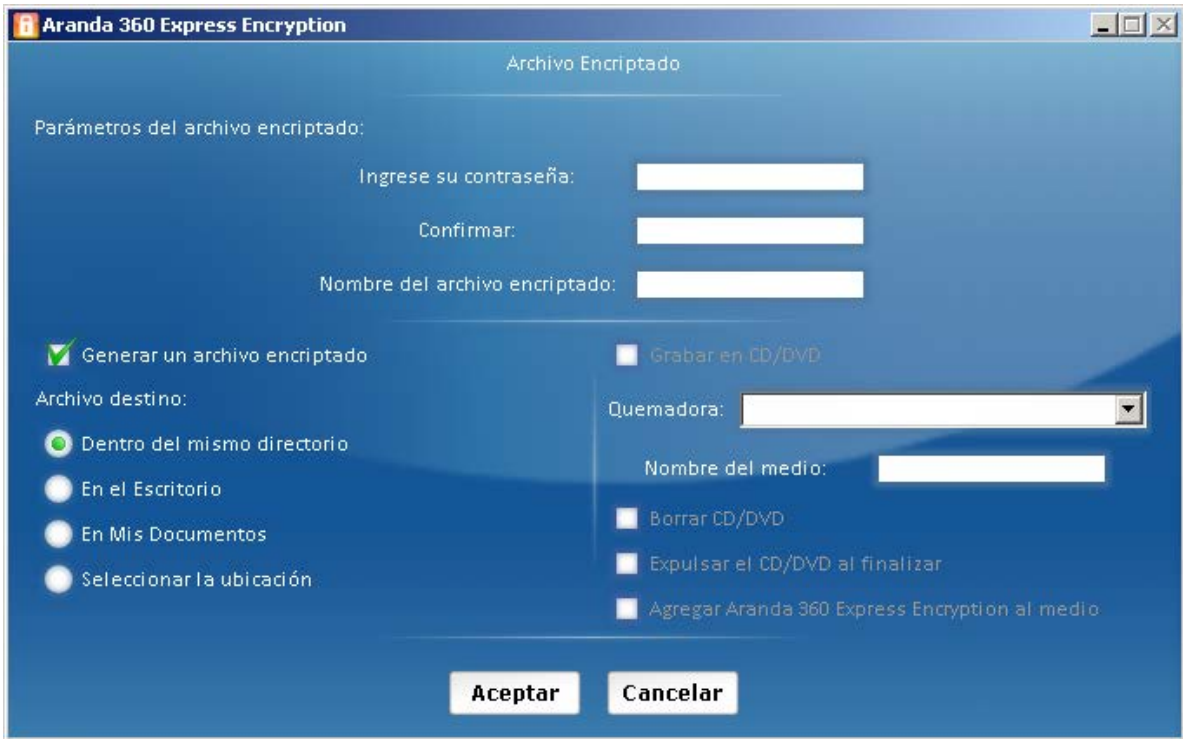
Para descifrar un archivo:

1. Haga doble-clic en el icono de surt.exe en su escritorio o donde estén ubicados los archivos de SURT.
   Una pantalla de inicio se mostrará y el icono aparecerá en la esquina inferior derecha de su escritorio.
2. Arrastre el archivo deseado hasta el icono .
3. Especifique los siguientes ajustes de cifrado:
   - Contraseña de acceso al archivo cifrado.
   - Confirme la contraseña.
   - El nombre del archivo cifrado.
   - Destino del archivo:
     - Dentro de la misma carpeta.
     - En mi escritorio.
     - En mis documentos.
     - Examinar para escoger una ubicación.

   La casilla Generar un archivo cifrado está marcada por defecto.

4. Debe escribir directamente el archivo cifrado en el CD-ROM.
   Para esto, marque la casilla Escribir a un CD/DVD y especifique las siguientes configuraciones:
   - Nombre del dispositivo grabador.
   - Nombre del medio.
   - Otras opciones como:
     - Borrar CD/DVD.
     - Expulsar CD/DVD después de la grabación.
     - Adicionar Aranda 360 Express Encryption al medio.

5. Hacer clic en OK.



6. Si usted tiene marcada la casilla Escribir en CD/DVD, el proceso de grabación comenzará inmediatamente.

7. Cuando el proceso haya terminado, una nueva ventana se mostrará. Haga Clic en OK.

CIFRANDO O DESCIFRANDO UN ARCHIVO

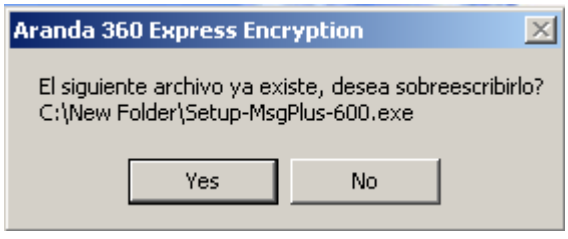
Procedimiento

Para descifrar un archivo, el usuario debe:

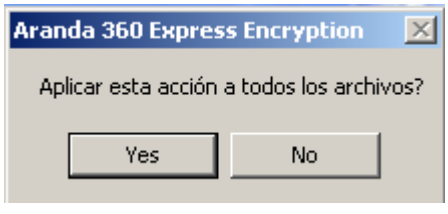
1. Arrastrar y soltar el archivo a descifrar en el icono  .
   Se mostrará la siguiente

2. Ingrese la contraseña del archivo cifrado.
3. Especifique la ruta del archivo descifrado.
4. Haga clic en OK.

- Si usted quiere sobre escribir un archivo existente en la misma ubicación, haga clic en Sí.



El siguiente mensaje se mostrará para aplicar la sobre escritura a todos los archivos.



Barra de progreso

La barra de progreso durante el cifrado del archivo solamente cuando:

- El usuario arrastre y suelte más de un archivo a la vez.
- El archivo que el usuario está cifrando es muy grande.

Fig. 13.1: Aranda 360 Express Encryption: barra de progreso

MENÚ DE REFERENCIA

Interfaz Gráfica

El menú de referencia de Aranda 360 Express Encryption se muestra cuando el usuario hace clic en el icono de la bandeja del sistema .

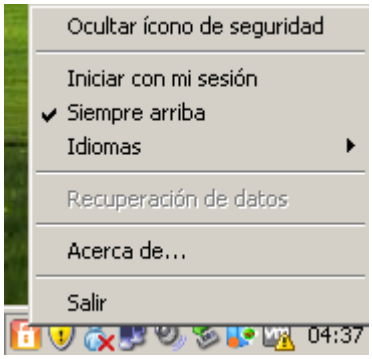


Fig. 13.2: Aranda 360 Express Encryption: menú de referencia

Opciones

Las opciones del menú de referencia son las siguientes:

- Ocultar/Mostrar arrastrar al icono:
  Si Ocultar arrastre al icono esta activado, el icono sólo se muestra en la bandeja del sistema.
  Si Mostrar arrastre al icono esta activado, el icono sólo se muestra en el escritorio del sistema.

- Iniciar con mi sesión:
  Esta opción inicia automáticamente SURT durante el inicio de sesión de Windows.

- Siempre visible:
  Esta opción mantiene el icono en la parte superior de todas las aplicaciones en ejecución.

- Idiomas:
  Esta opción establece el idioma utilizado para SURT (francés, inglés, español o portugués).

- Recuperación de datos:
  Esta opción recupera archivos cifrados creados con la característica Cifrado de datos en la consola de administración de Aranda.

- Para recuperar los archivos cifrados que se crearon con la función de cifrado de datos en la consola de administración de Aranda, el usuario debe iniciar su computador en modo seguro.
  Si el usuario desea estar en modo NORMAL, el agente de Aranda 360 debe ser desinstalado.

  - Acerca de:
    Esta opción muestra la versión del software y los derechos de autor.

  - Salir:
    Esta opción cierra la aplicación.

CIFRADO DE DISPOSITIVOS EXTRAÍBLES Y SURT

Configuración de dispositivos extraíbles

En la consola de administración de Aranda, SURT puede ser Permitido o Denegado en el Editor de políticas de seguridad, bajo la categoría de dispositivos extraíbles.

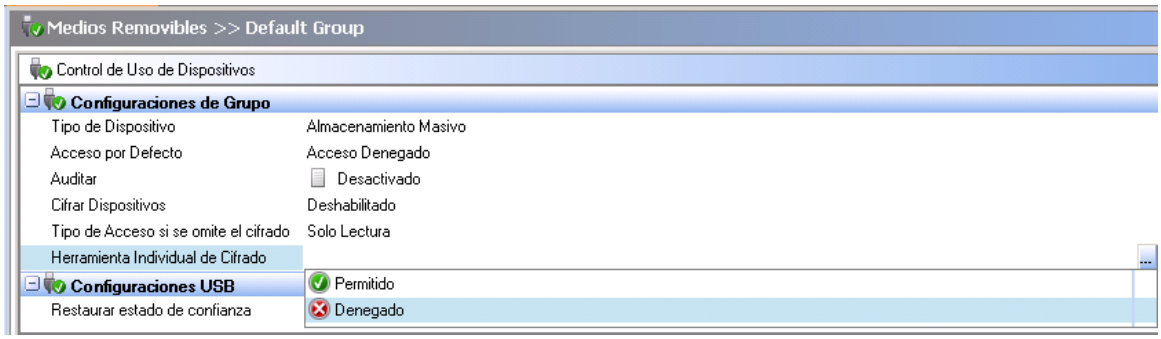


Fig. 13.3: Configuración SURT en la consola de administración Aranda

Configuración de SURT

Las opciones de SURT son:

- Permitido:
  Cuando se establece como permitido, El usuario puede cifrar o descifrar datos en dispositivos extraíbles.
  El archivo ejecutable SURT.exe será copiado automáticamente dentro de una memoria USB.
  De esta manera, cualquier intento de remplazar SURT.exe por un archivo SURT hackeado será contrarrestado y el archivo SURT.exe sobrescribirá el archivo hackeado.

- Denegado:
  Cuando se establece como denegado, el usuario no podrá usar SURT para cifrar o descifrar datos de un dispositivo extraíble.

RECUPERANDO INFORMACIÓN CIFRADA USANDO LA FUNCION CIFRADO DE DATOS

Requerimientos

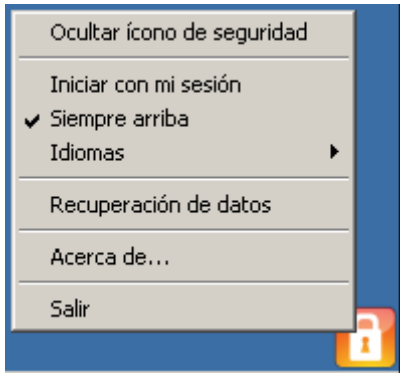
Para recuperar los archivos cifrados que se crearon mediante la función de cifrado de datos en la consola de administración de Aranda, el usuario tiene que iniciar su estación de trabajo en modo seguro.

- Si el usuario desea estar en modo NORMAL, el agente de Aranda 360 debe ser desinstalado.

Procedimiento

Para recuperar los datos cifrados a través de la función de cifrado de datos, siga los siguientes pasos:

1. Haga clic derecho en el icono y seleccione Recuperación de datos.



2. Se mostrará la siguiente ventana.

Especifique la configuración utilizando el botón Examinar .

- El nombre y la ruta de la carpeta a descifrar.
- La ruta del archivo con la clave de acceso de recuperación enviada por el administrador.

3. Haga Clic en OK.
   Iniciará el descifrado de la carpeta.

4. Después de descifrar, una ventana le mostrara al usuario que el proceso ha terminado.

5. Reinicie en modo normal.

Capítulo 14 - ARANDA 360 GENERADOR DE REPORTES

ACERCA DE ESTE CAPÍTULO

En este capítulo se describen los informes disponibles en Aranda 360 y la forma de acceder a ellos.

Este capítulo incluye:

- Administrador de reportes:
  - Administrador de Segundo nivel:
    - A Nivel de reporte.
    - A Nivel de administración de roles.
  - Ruta del reporte
    .
- Descripción del reporte:
  - Categorías.
  - Tipos.
- Interfaz gráfica:
  - Menú.
  - Ajustes de pantalla:
    - Opciones.
    - Filtros.
- Reportes en tiempo real:
  - Servidores y agentes.
  - Integridad de la estación de trabajo.
  - Seguridad del sistema.
  - Dispositivos extraíbles.
- Reportes de Históricos:
  - Servidores y agentes.
  - Dispositivos extraíbles.
  - Integridad de la estación de trabajo

ADMINISTRADOR DE REPORTES

Los informes de Aranda 360 se administran en dos niveles por medio de la consola de administración de Aranda:

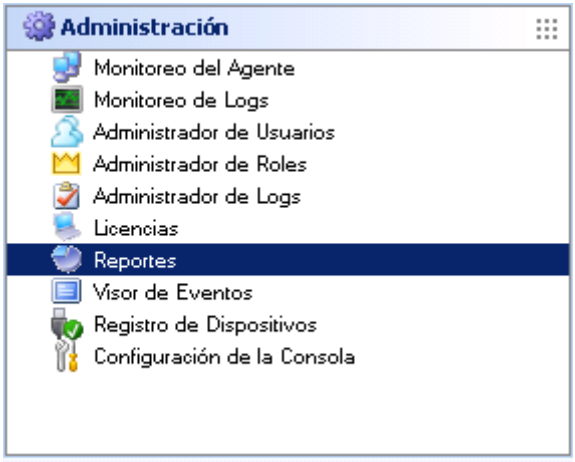
- A Nivel de reportes.
- A nivel de administración de roles.

Ambos niveles son accesibles desde el panel de Herramientas de administración y monitoreo.

Administrador de Segundo nivel

A Nivel de reportes

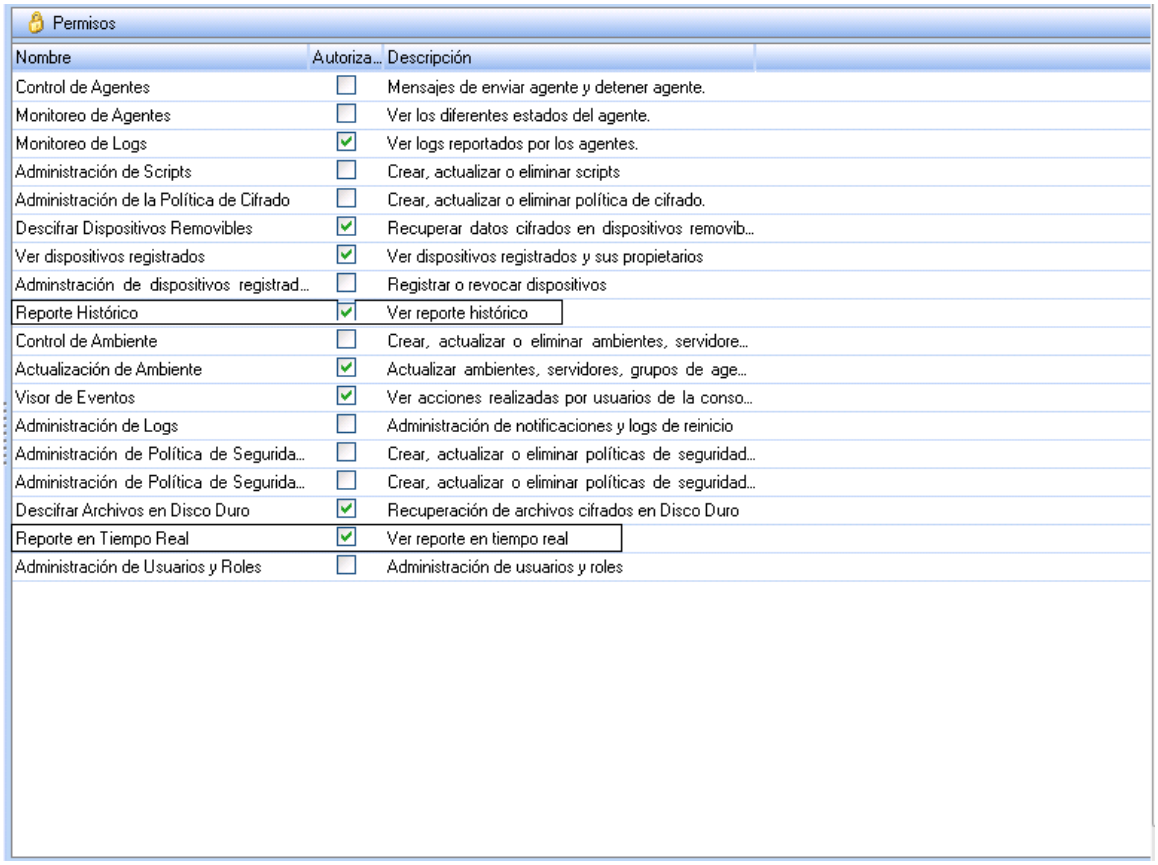
Para generar y ver informes, el administrador deberá hacer clic en Informes en Herramientas de administración y monitoreo en la consola de administración de Aranda.



A Nivel de Administración de roles

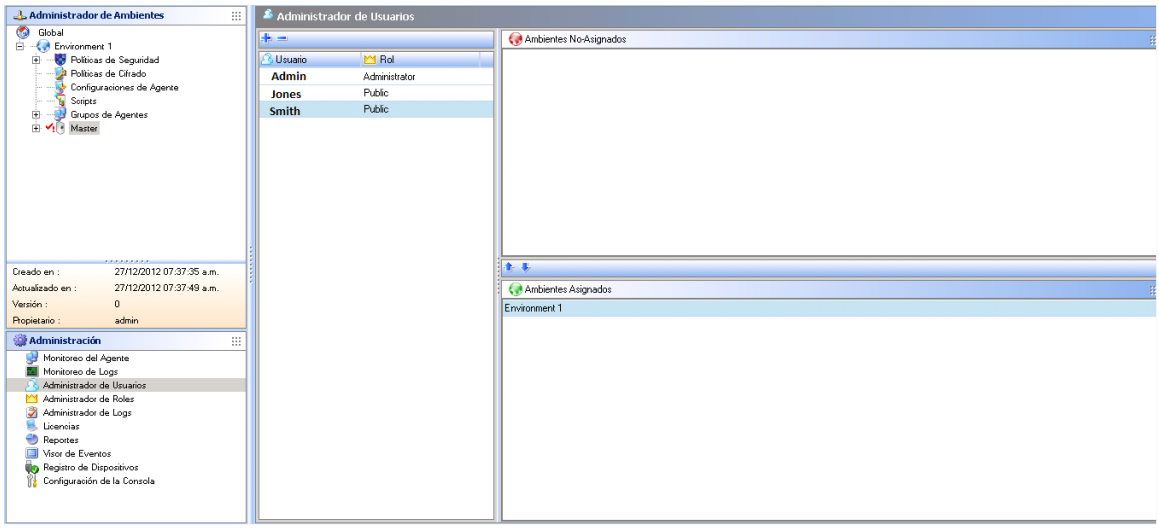
Para generar y ver informes, el usuario de la consola debe tener los permisos adecuados. Los Permisos se otorgan al usuario por el administrador a través de la Función Herramientas de administración y monitoreo.
El administrador determina quién tiene los derechos de acceso a los informes, marcando las casillas apropiadas en el panel del administrador.

Ejemplo: User1 se le permite ver informes históricos y en tiempo real, informes marcados en las casillas).



- Los roles administrador y Público son creados por defecto. No pueden ser modificados

Los roles son asignados a los usuarios de la consola a través de herramientas de administración y monitoreo.



Ruta para reportes

El camino recorrido por la información utilizada para generar informes se describe a continuación:

1. Los informes se basan en los registros enviados por los agentes al servidor Aranda 360.
2. El servidor envía estos registros a la base de datos SQL Aranda 360.
3. La base de datos almacena estos registros.

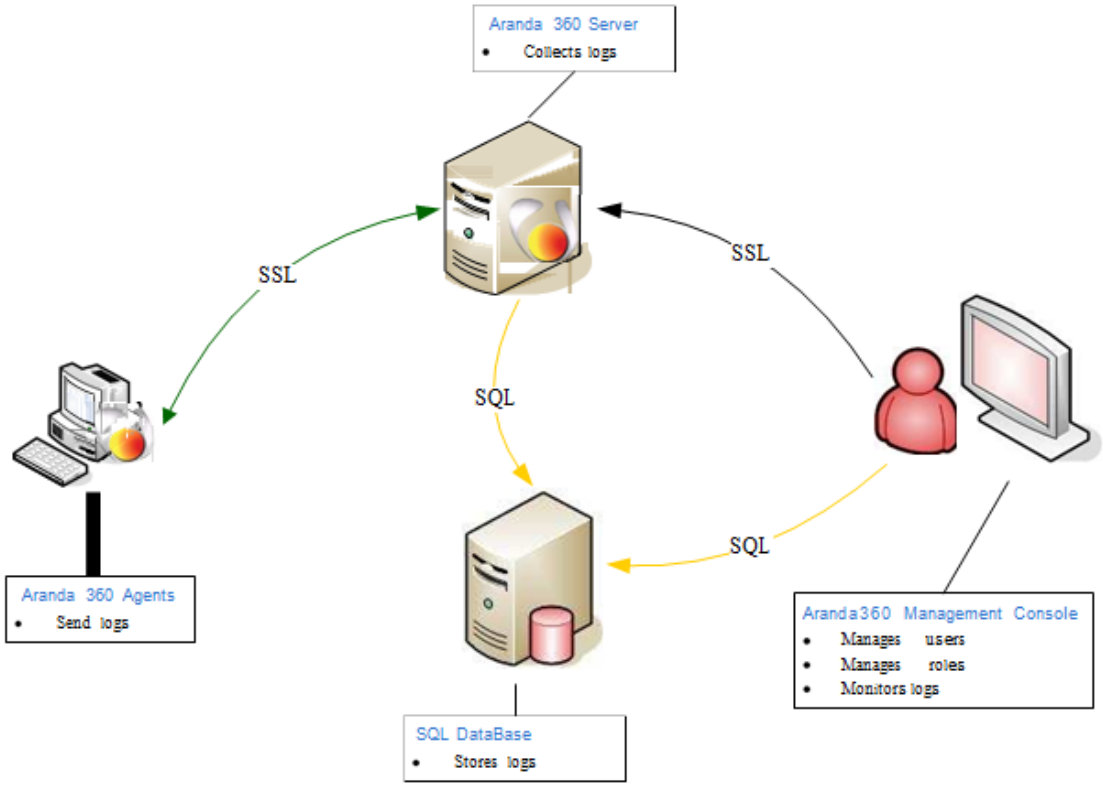


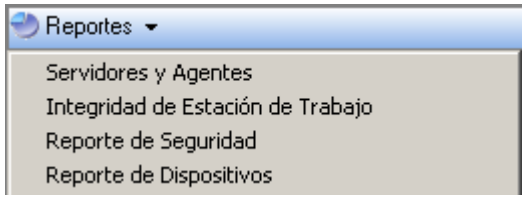
Fig. 15.1: Administrador de reportes Aranda 360

Descripción para reportes

Categorías

Hay cinco categorías de informes Aranda 360:

- Servidor y agentes.
- Integridad de la estación de trabajo.
- Seguridad del sistema.
- Dispositivos extraíbles.



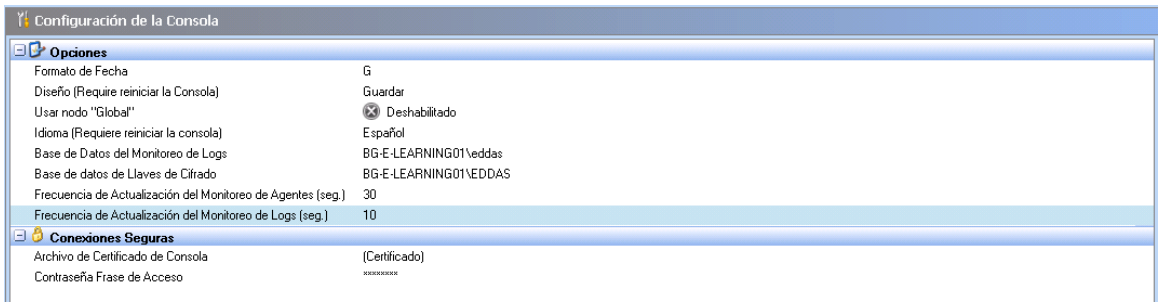
Tipos

Las categorías se dividen en dos tipos de informe:

- Reportes en tiempo real.
- Reportes de históricos.

El tipo de informe de tiempo real brinda la última información.

Esta información es actualizada automáticamente dependiendo del número de segundos establecidos en Tiempo para refrescar EL monitoreo Del log (sec.) bajo Configuración de consola.



También puede forzar la actualización de los reportes haciendo clic en Actualizar Reportes.

.; Servers and Agents
Worl<station Integrity
System Security
Removable Deviees
Antivirus

Servers and Agents
192.168.4.109\Eddas

Date
21241201O 3:44:16 PM

INTERFAZ GRÁFICA

Menú

El menú se muestra así:

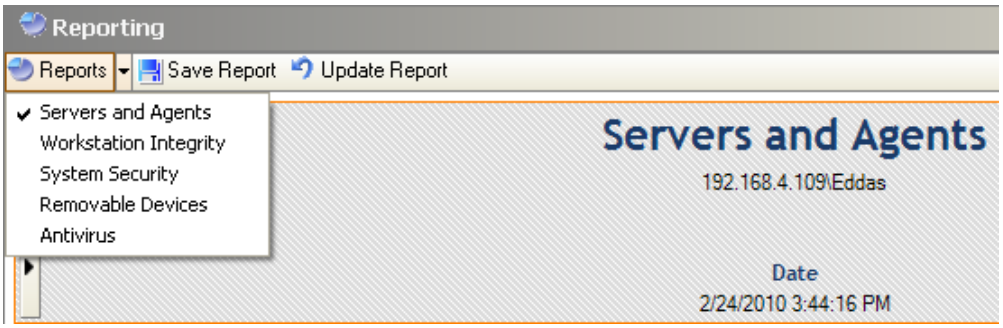


Fig. 15.1 : Generador de reportes: Menú

El menú contiene las siguientes acciones:

- Reportes :
  Esta opción es usada para seleccionar la categoría del reporte a generar.

- Guardar reportes:
  Esta acción es usada para salvar reportes en una ubicación específica, con el formato .png o .csv.

- Actualizar Reportes:
  Con esta acción se actualizan los reportes.

Configuración

Opciones

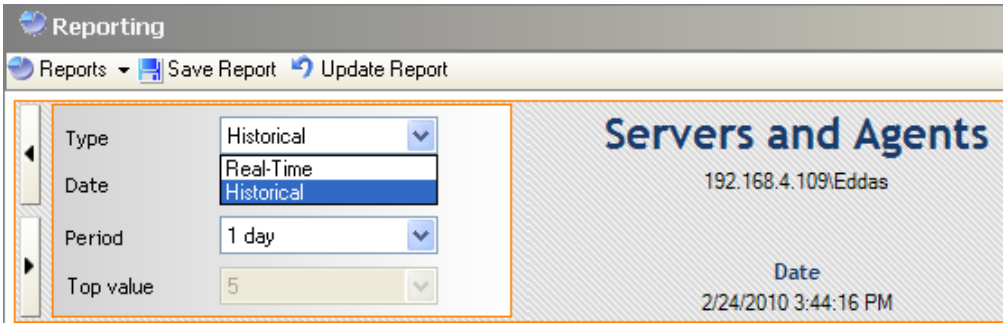
Dependiendo de la categoría seleccionada, el reporte puede incluir las siguientes opciones:

- Tipo.
- Fecha.
- Periodo.
- Valor máximo.

Las opciones no disponibles aparecen en gris.

Tipo

Esta opción se utiliza para seleccionar el tipo de informe, histórico o en tiempo real.

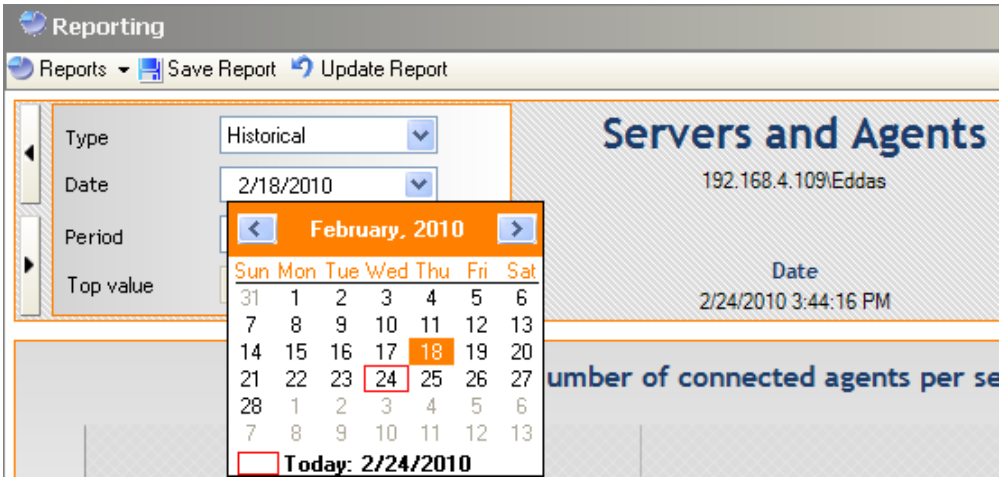


Si se selecciona en tiempo real, la información que se muestra es la más reciente.

Si selecciona Histórico, la información que se muestra cubre el intervalo de tiempo especificado por el administrador.

Fecha

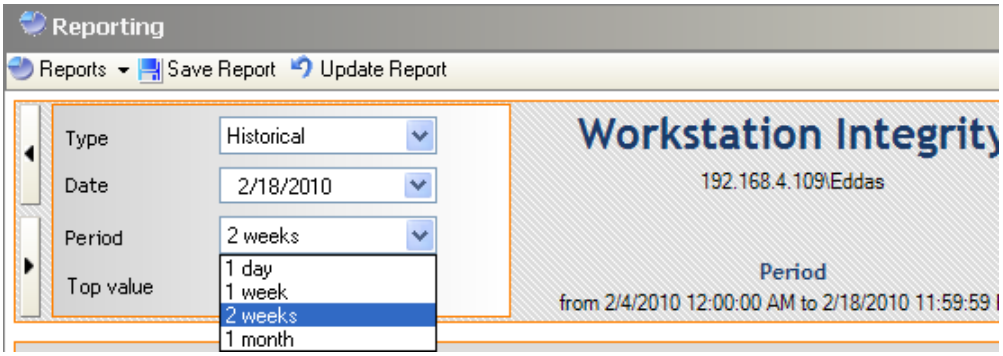
Esta opción se utiliza para seleccionar la fecha de inicio para generar un informe histórico. La fecha actual está seleccionada por defecto.



Periodo

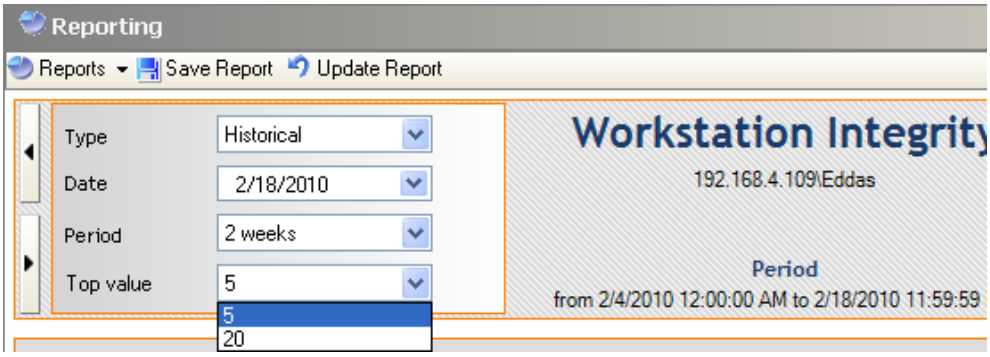
Esta opción se usa para definir el intervalo de tiempo requerido para generar un informe histórico:

- 1 día.
- 1 semana.
- 2 semanas.
- 1 mes.



Valor tope

Esta opción se utiliza para seleccionar el valor superior (5 o 20) necesario para generar un informe.

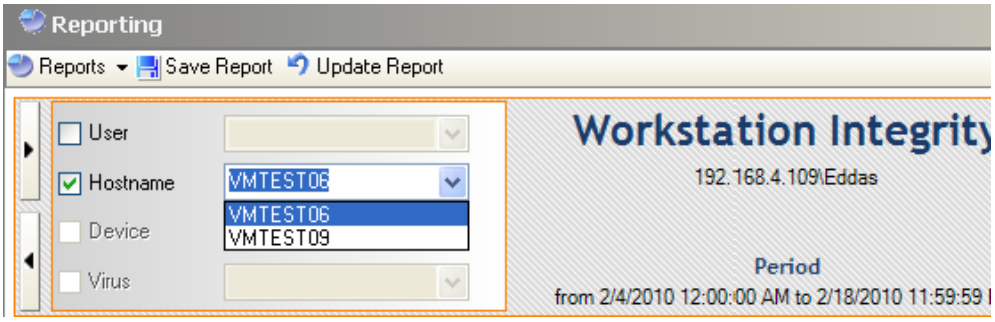


Filtros

En función de la categoría seleccionada, el informe puede ser generado mediante la aplicación de los siguientes filtros :

- Usuario.
- Nombre del host.
- Dispositivo.

Los Filtros disponibles aparecen en gris.

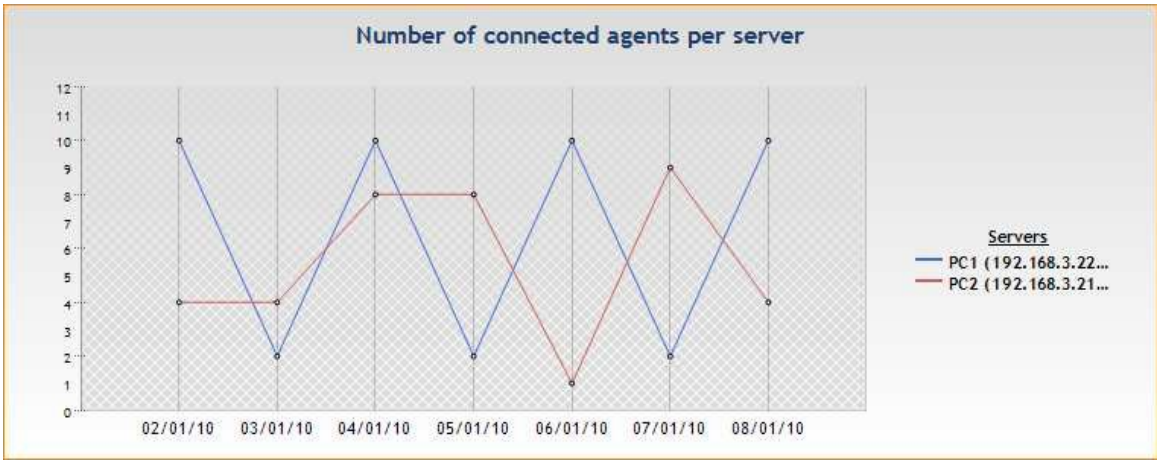


REPORTES EN TIEMPO REAL

Servidores y Agentes

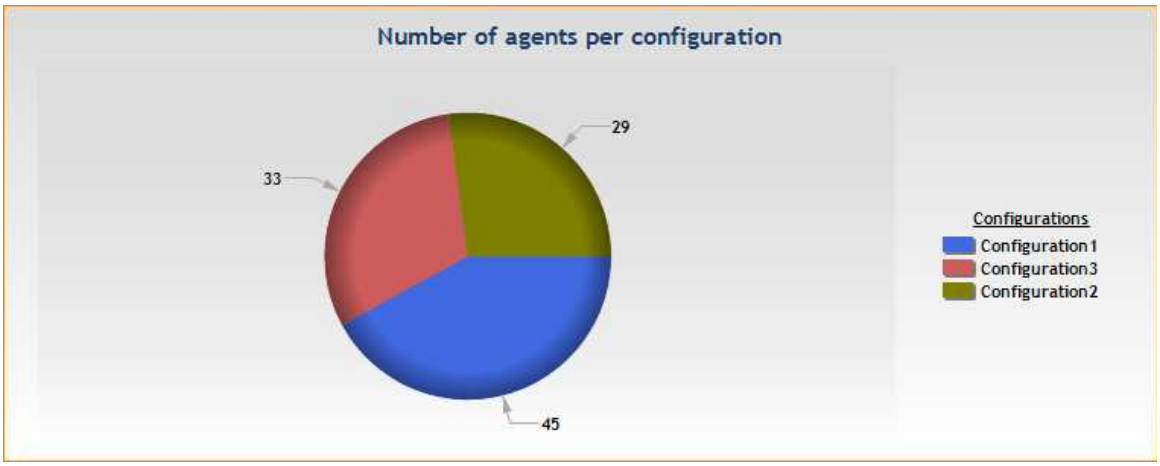
Los informes de servidores y agentes proporcionan datos de los servidores de Aranda 360:

- Número de agentes conectados al servidor:



- Número de agentes por versión:
  Muestra todas las versiones de Aranda 360 en uso y el número de agentes por cada versión.

- Número de agentes por la política:
  Se muestra las políticas por su nombre y el número de agentes que utilizan esta política.

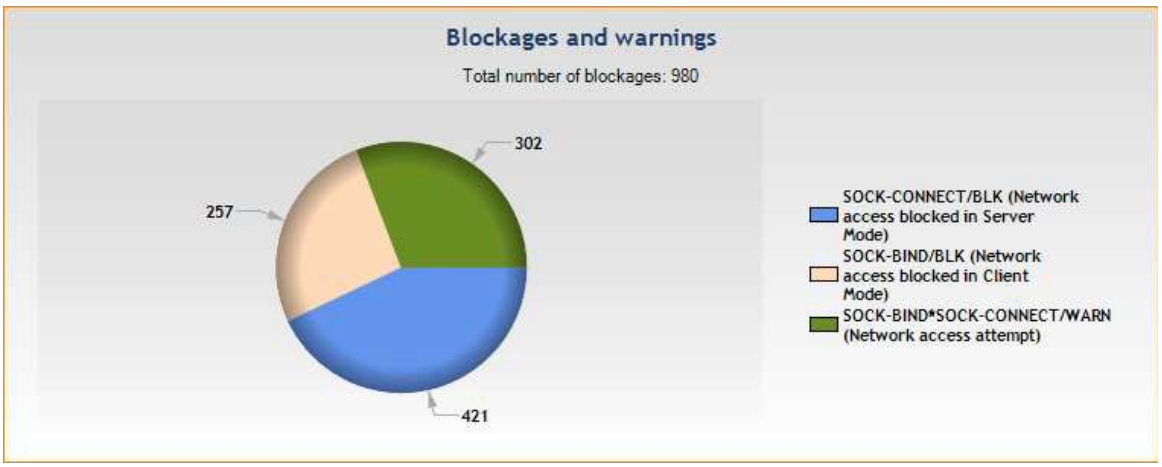


- Los títulos mostrados a la derecha de los gráficos son interactivos. Los Gráficos cambian cuando se pasa el mouse sobre los títulos.

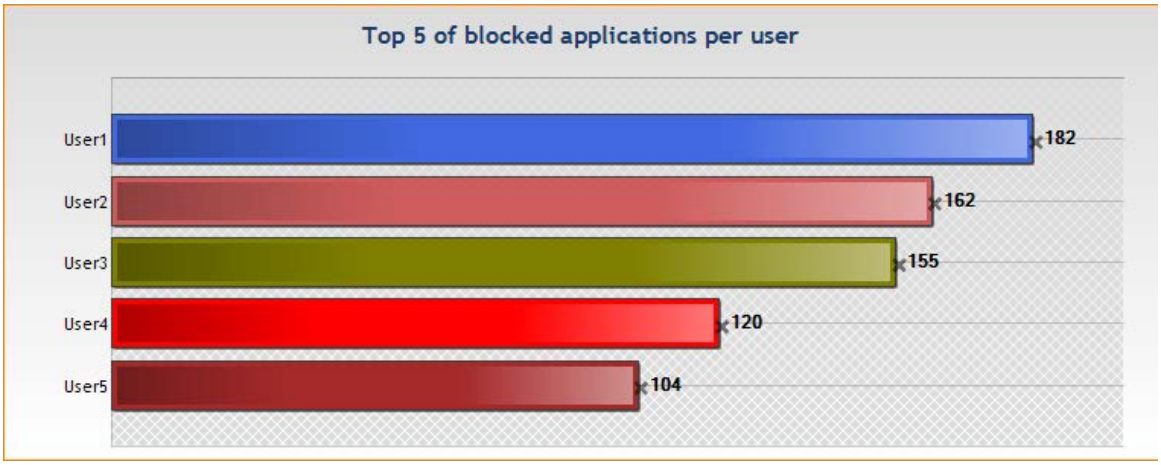
Integridad de las estaciones de trabajo

El informe de Integridad de la estación de trabajo proporciona la siguiente información:

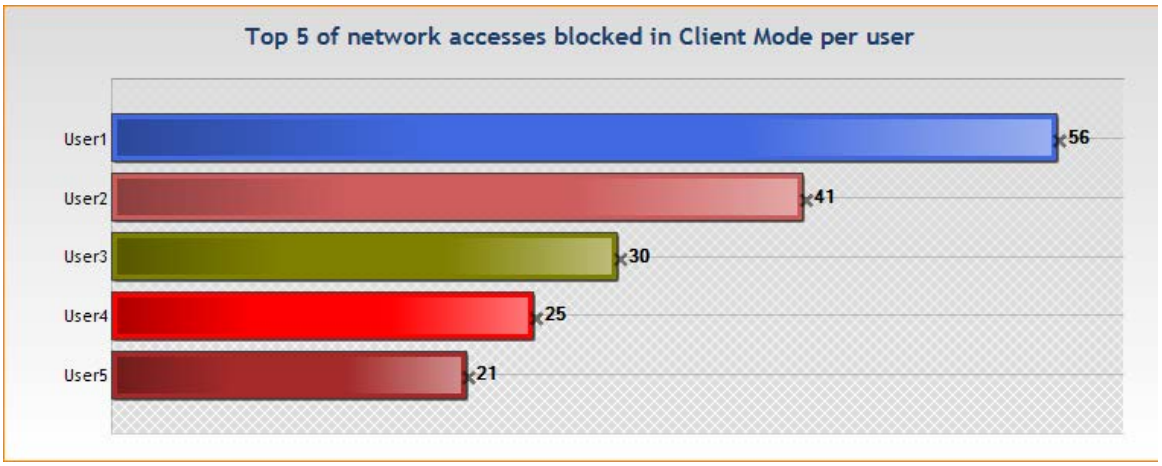
- Bloqueos y las advertencias:



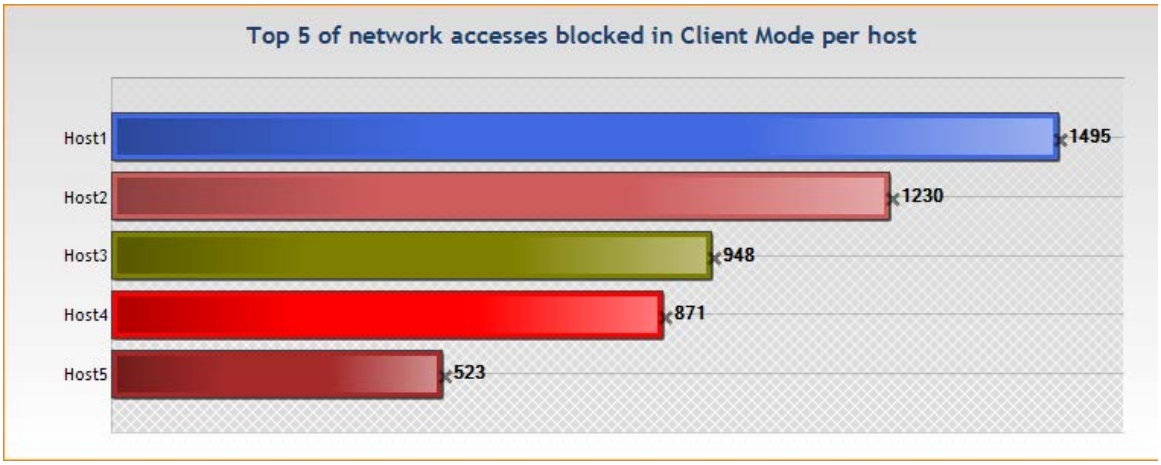
o El Top [5] de aplicaciones bloqueadas por usuario



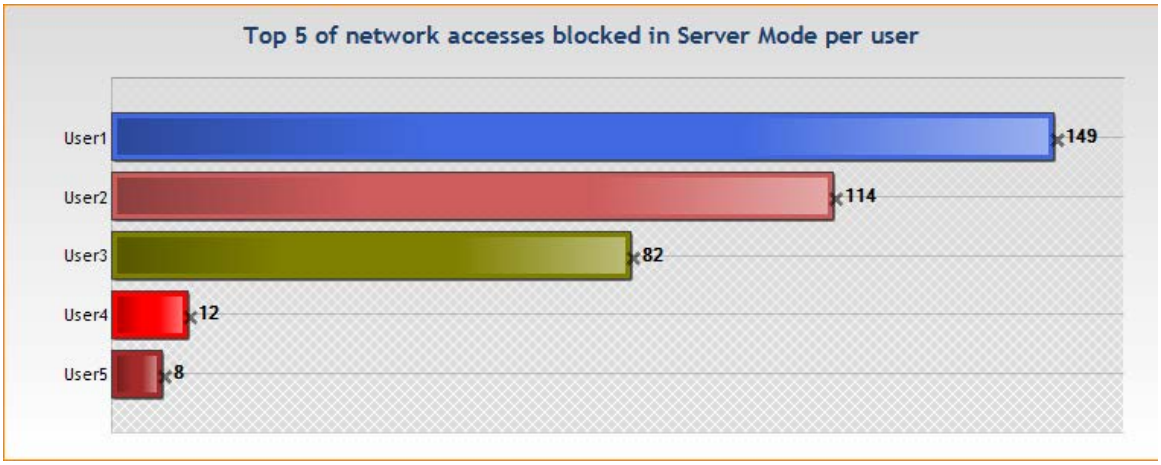
• El Top [5] de accesos a la red bloqueados en modo cliente por usuario:



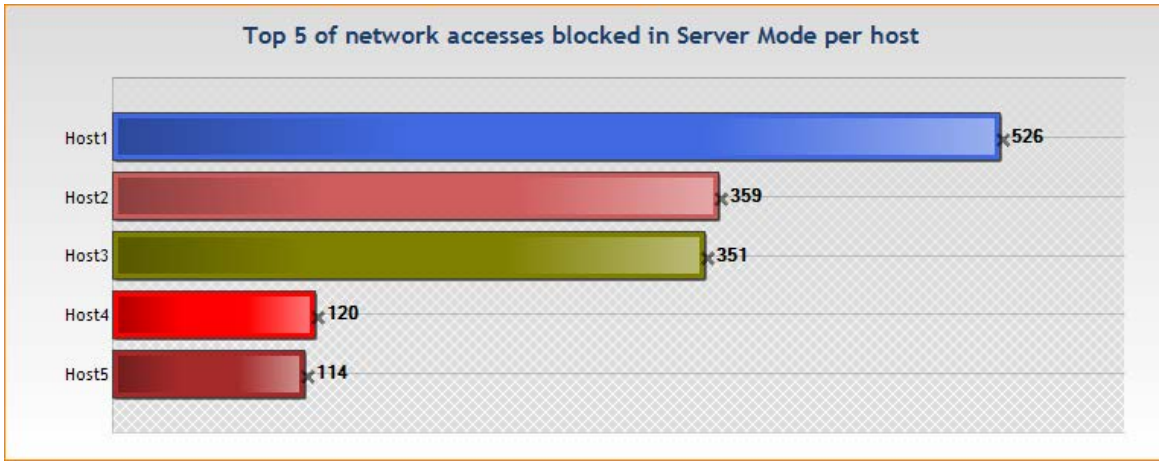
- El Top [5] de accesos a la red bloqueados en modo cliente por host:



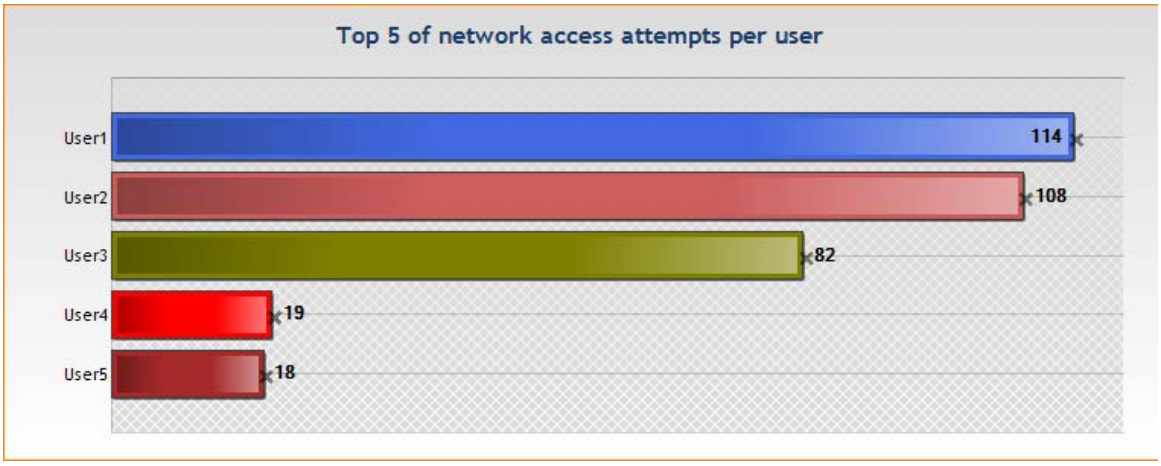
- El Top [5] de accesos a la red bloqueados en modo servidor por usuario:



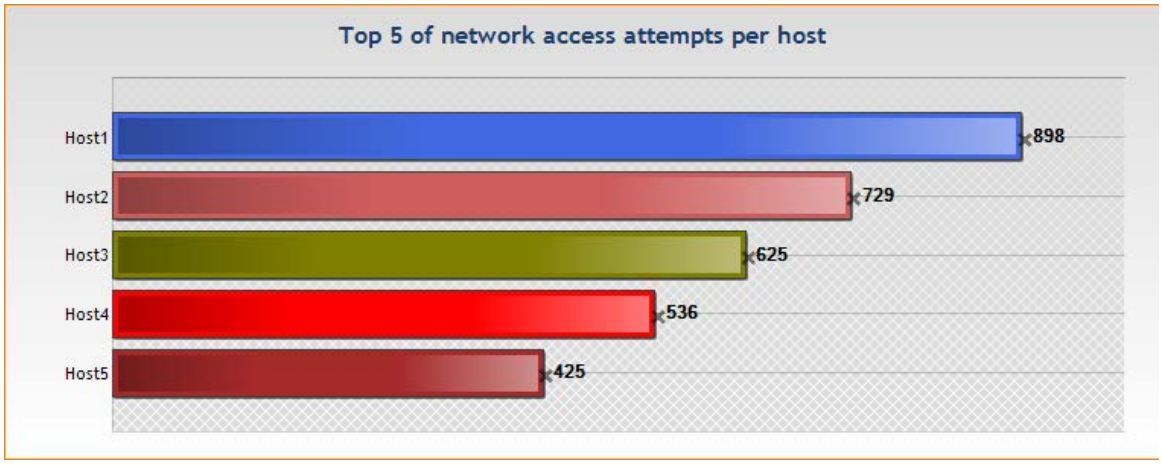
- El Top [5] de accesos a la red bloqueados en modo servidor por host:



- El Top [5] de los intentos de acceso a la red por usuario:



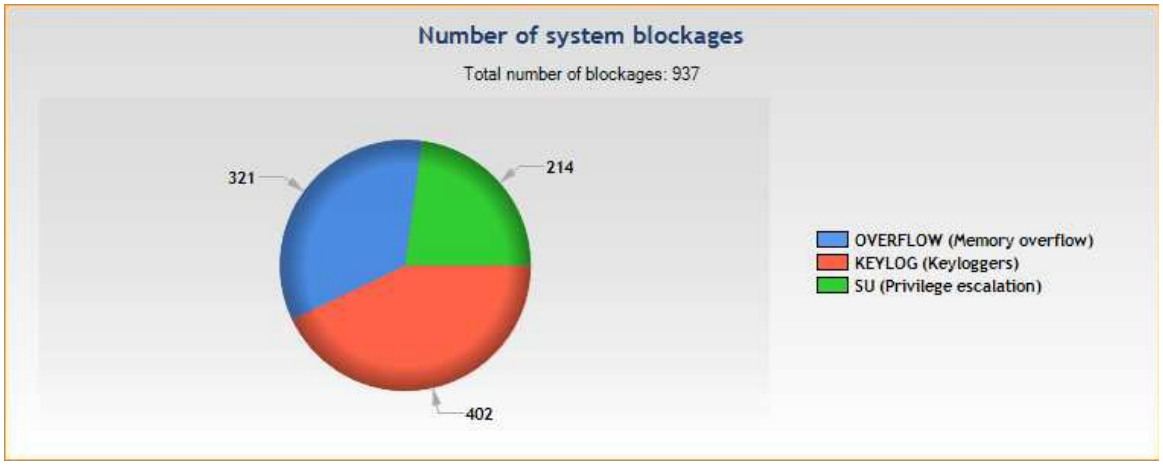
- El Top [5] de accesos a la red permitidos por host:



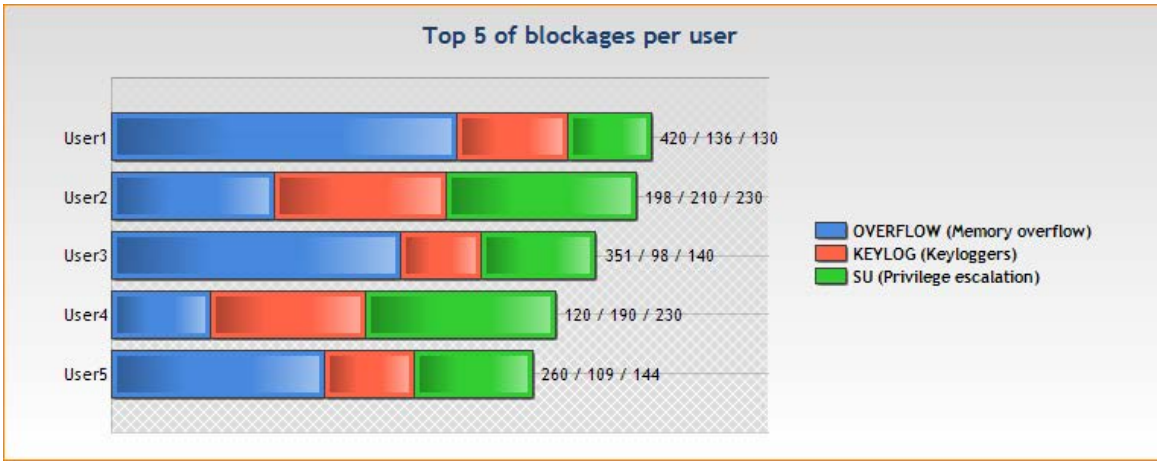
Seguridad del sistema

El reporte de la seguridad del sistema provee la siguiente información:

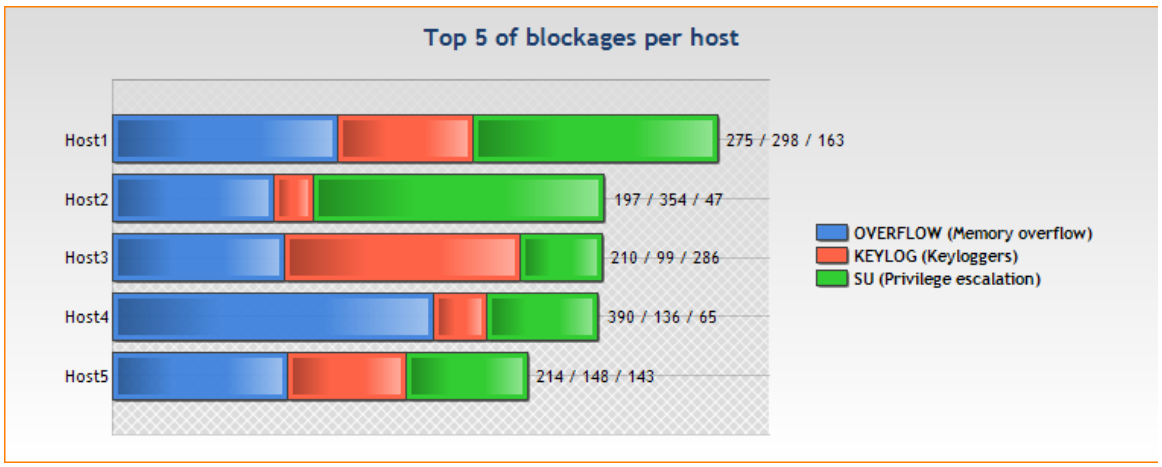
- Numero de bloqueos en el sistema:



- El Top [5] de bloqueos por usuario:



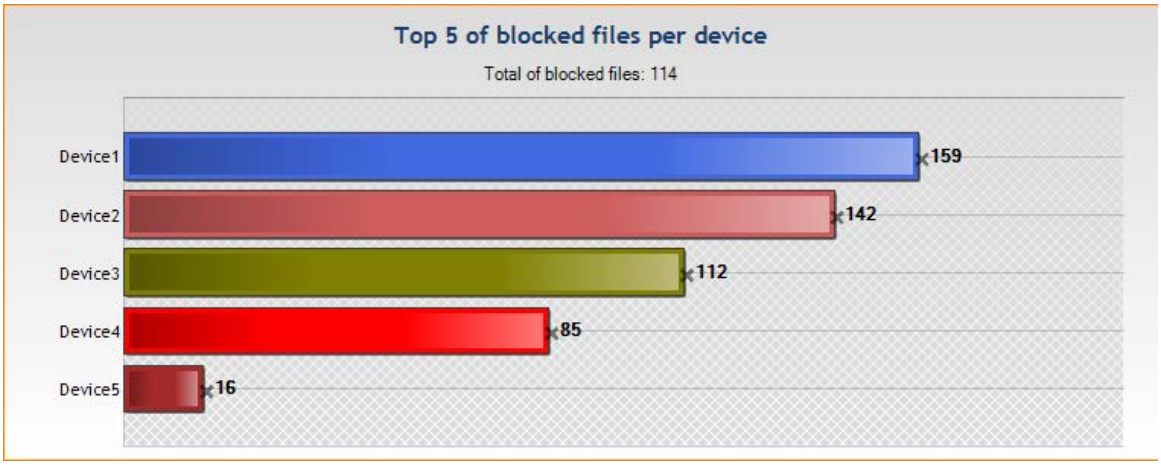
- El Top [5] de bloqueos por host:



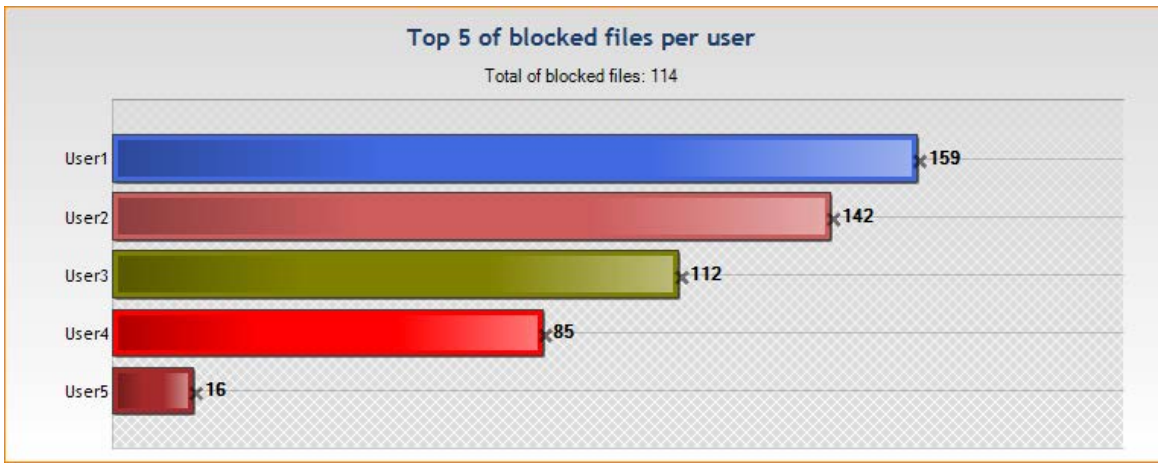
Dispositivos extraíbles

El reporte de dispositivos extraíbles contiene la siguiente información:

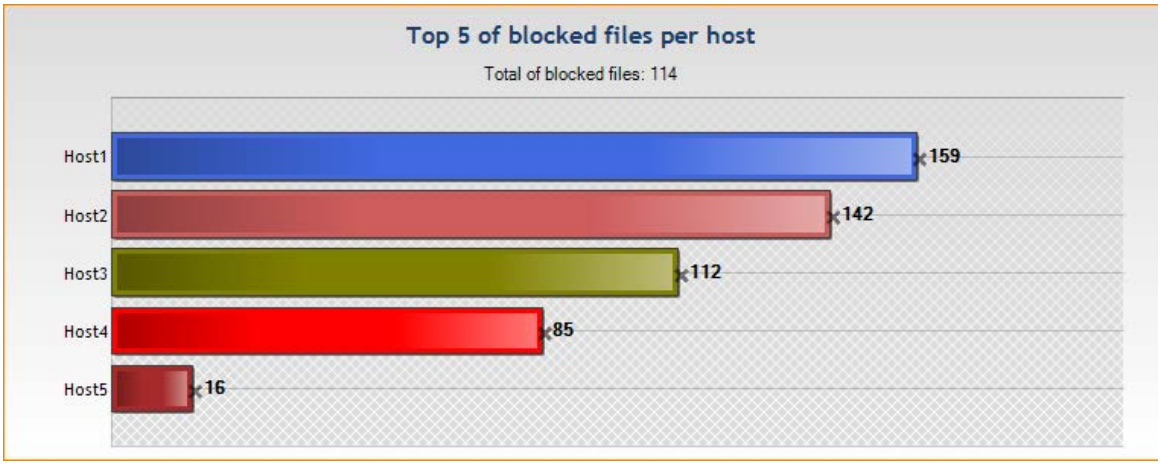
- El Top [5] de bloqueos de archivos por dispositivo:



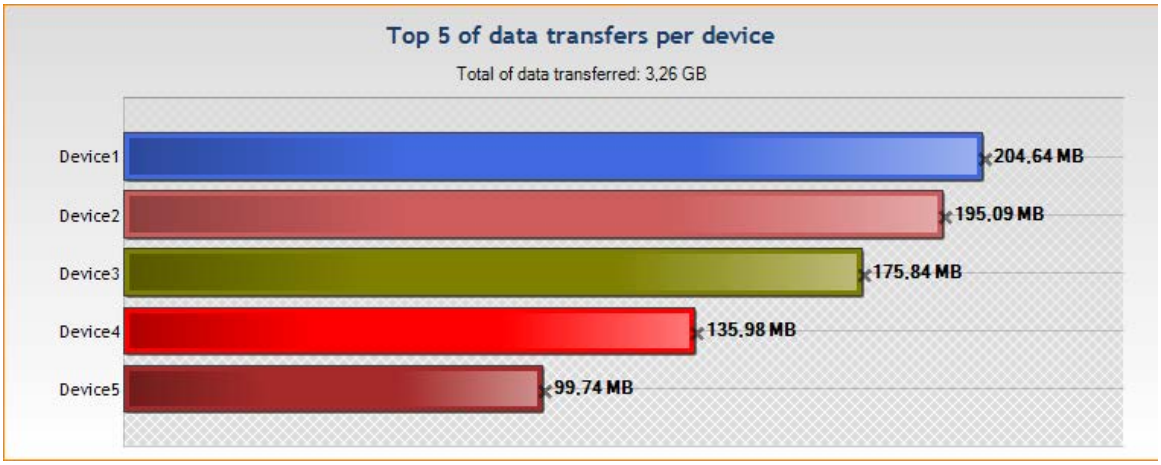
- El Top [5] de bloqueos de archivos por usuario:



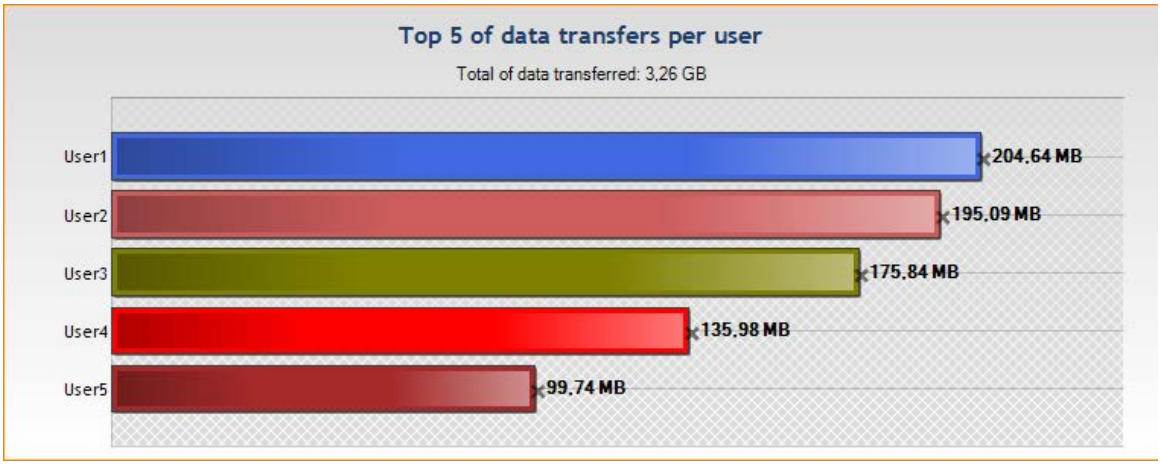
- El Top [5] de bloqueo de archivos por host:



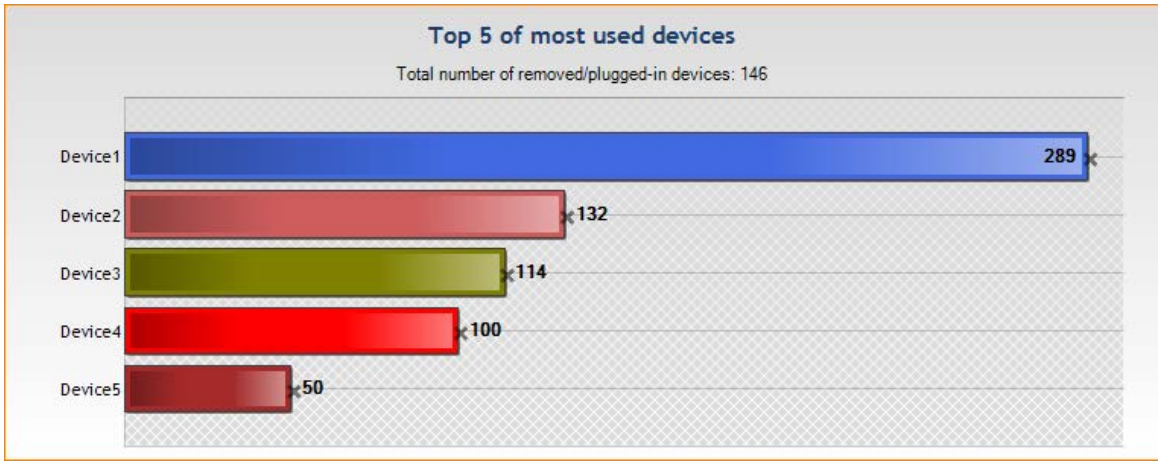
- El Top [5] de transferencia de datos por dispositivo



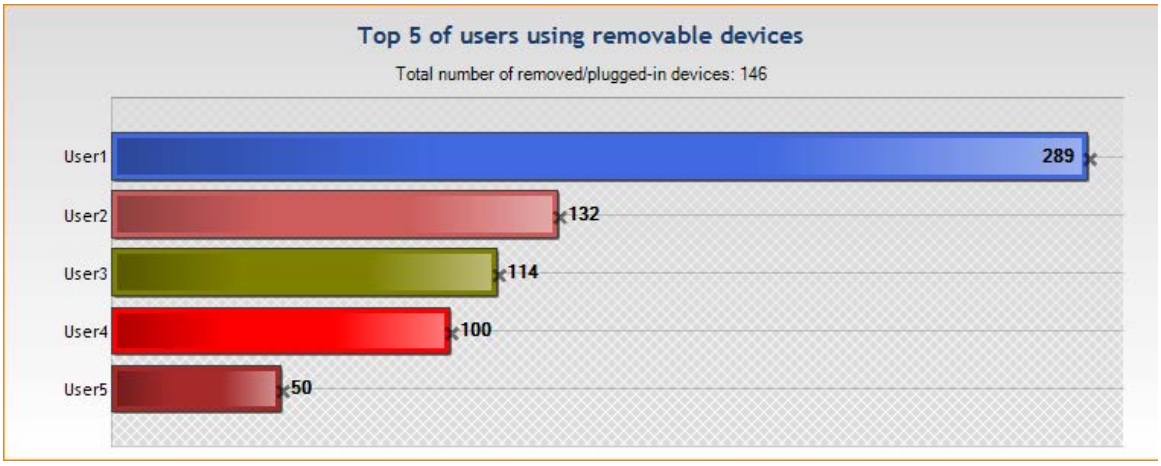
- El Top [5] de transferencia de datos por usuario:



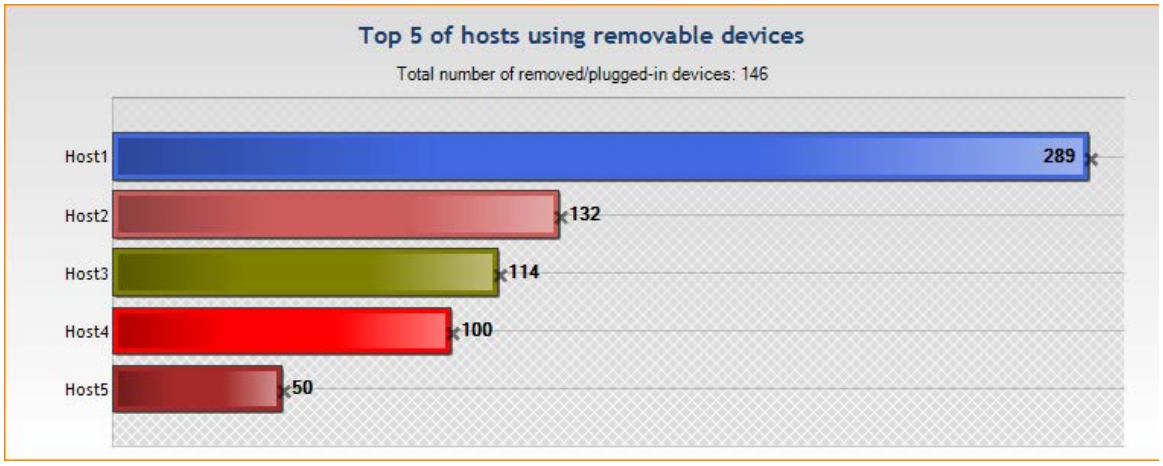
- El Top [5] de dispositivos más usados:



- El Top [5] de usuarios dispositivos removibles:



- El Top [5] de host usando dispositivos removibles

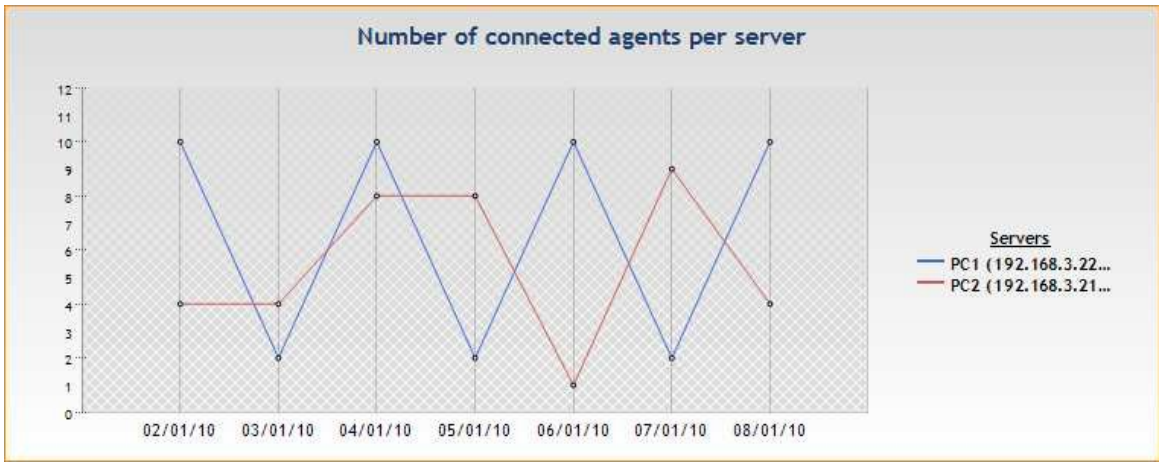


REPORTES HISTÓRICOS

Servidores y Agentes

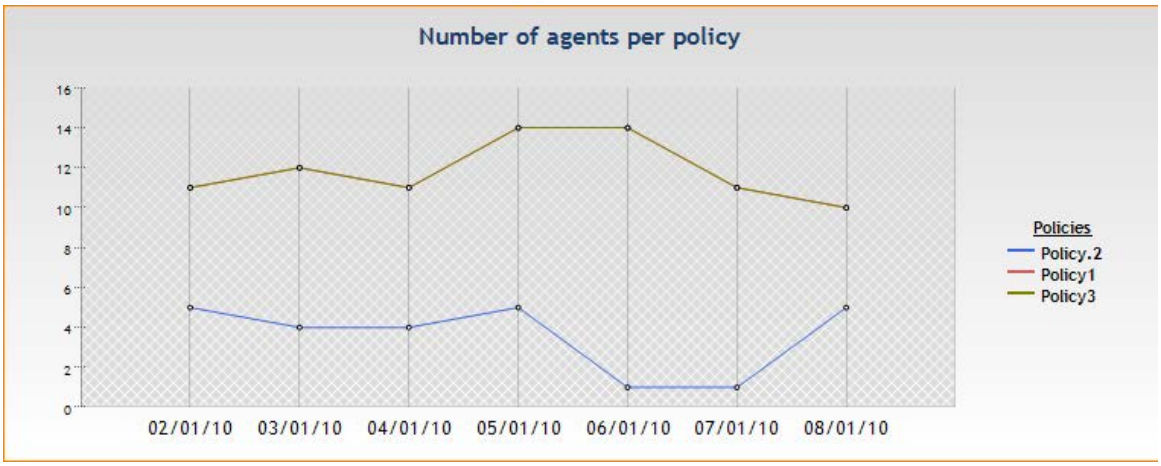
Los reportes de servidores y agentes proporcionan la siguiente información de los servidores de Aranda 360 servers:

- Número de agentes conectados por servidor:
  Muestra el número de gentes conectadas al servidor por un periodo de tiempo seleccionado.

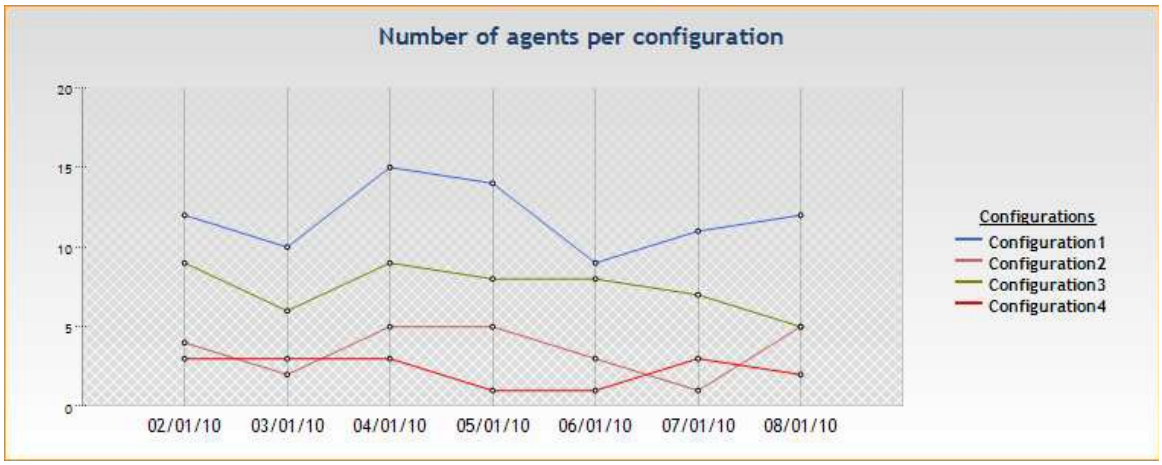


- Número de agentes por versión:
  Muestra todas las versiones de Aranda 360 en uso y el número de agentes por versión en el período seleccionado.

- Número de agentes por política:
  Esto muestra las políticas por nombre, y el número de políticas usadas por agentes en un periodo seleccionado.



- Número de agentes por configuración :
  Esto muestra las configuraciones por nombre, y el número de agentes que están usando las configuraciones en un periodo de tiempo seleccionado.



Los siguientes reportes están en formato de Excel:

- Estado del agente:
  Esto muestra la fecha de la última conexión, el último usuario y la versión de cada agente.

- Modificación de configuraciones de Aranda 360:
  Esto muestra todas las modificaciones realizadas en la configuración con los nombres de los administradores y políticas implicadas.

- Agentes detenidos:
  Esto muestra toda la lista de agentes detenidos en un periodo de tiempo en particular.

- Configuración de agentes:
  Esto muestra la fecha y la versión de configuraciones usadas por cada agente.

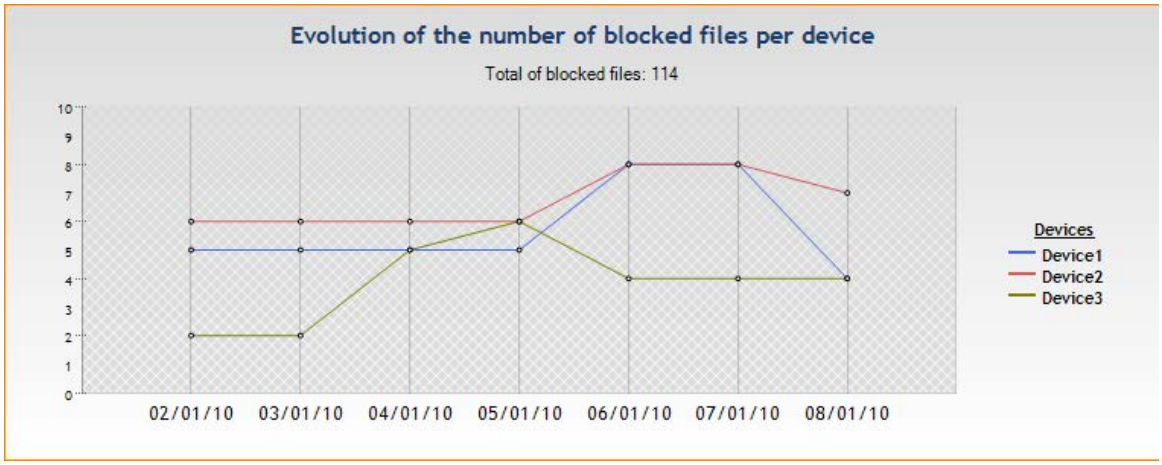
- Políticas de agentes:
  Esto muestra la fecha y la versión de políticas usadas por cada agente.

- Directivas para grupos de:
  Muestra las directivas disponibles para cada grupo de agentes.

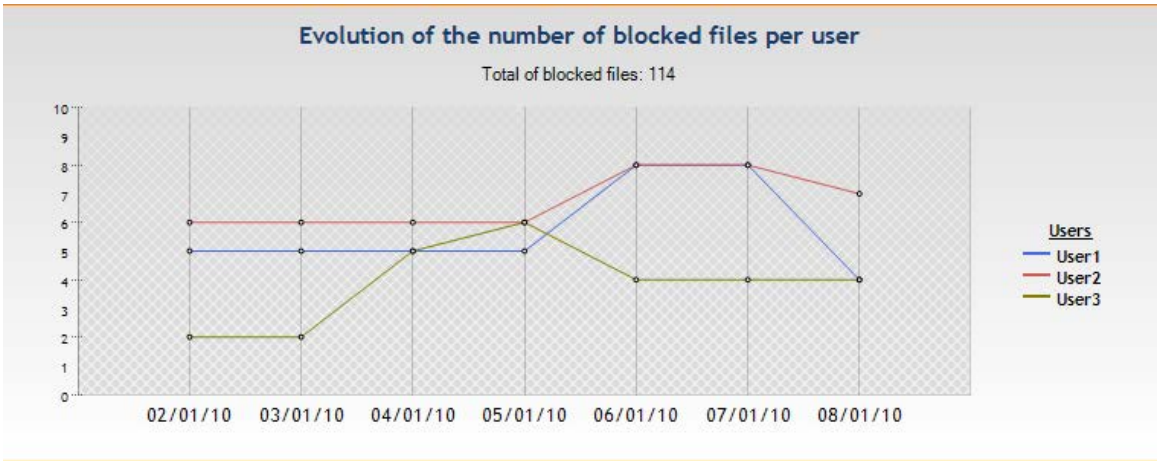
Dispositivos extraíbles

El reporte de los dispositivos extraíbles muestra la siguiente información:

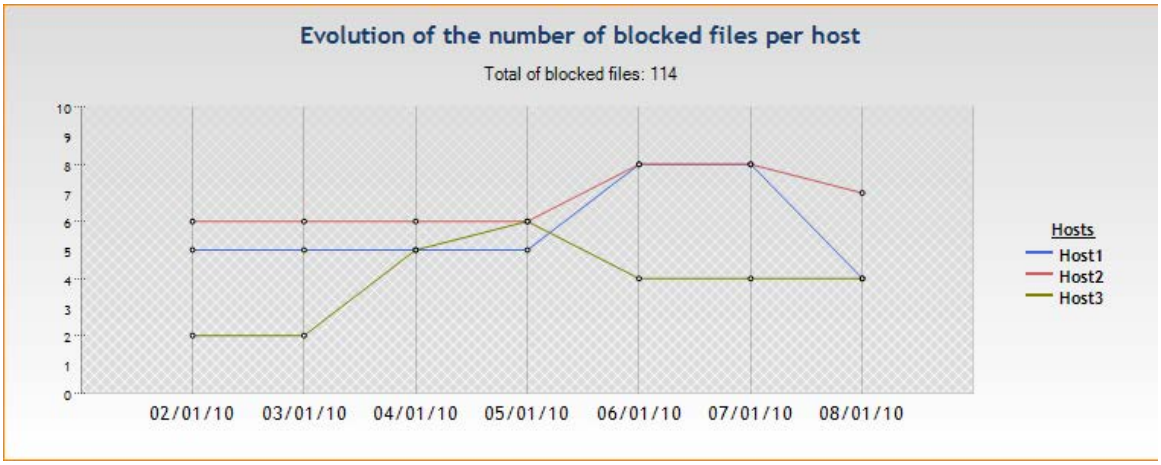
- Evolución del número de archivos bloqueados por dispositivos:



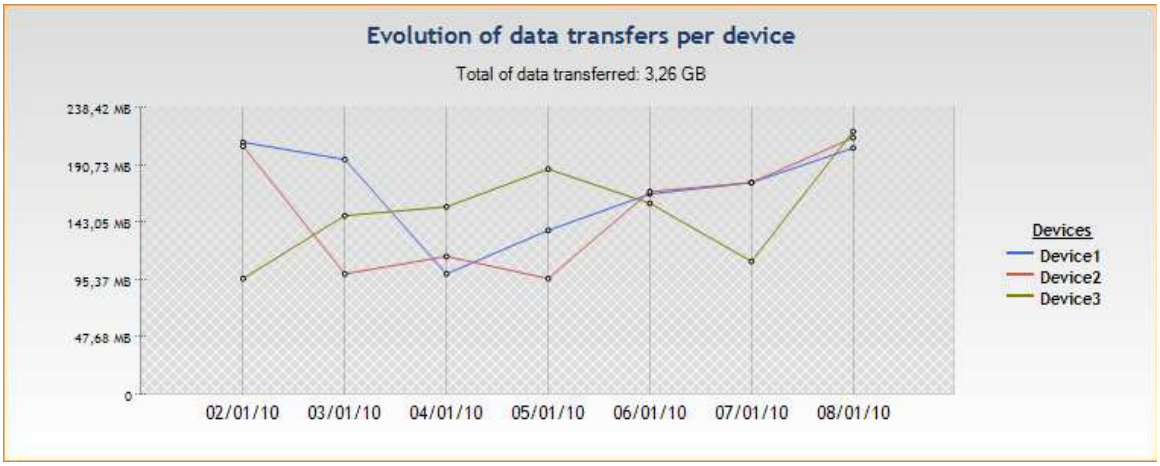
- Evolución del número de archivos bloqueados por usuario:



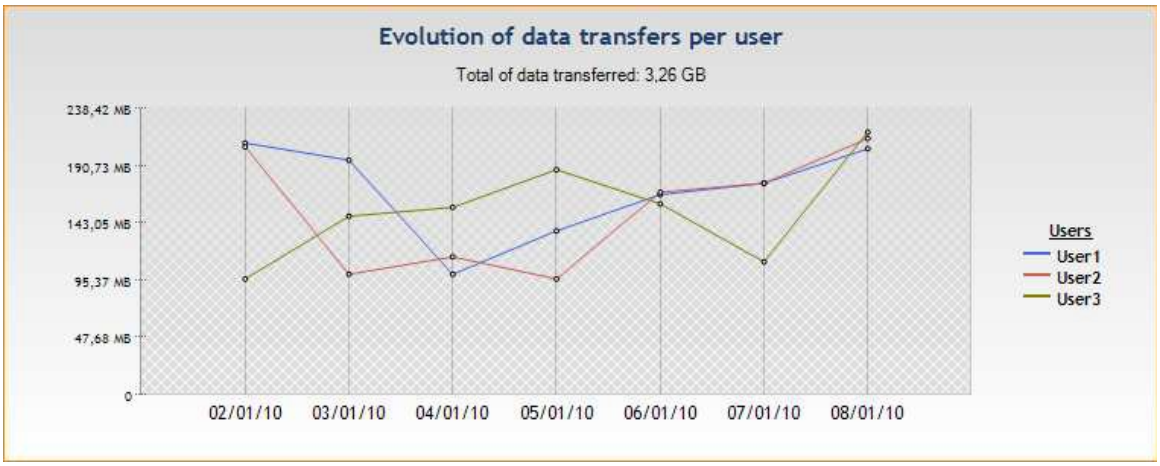
- Evolución del número de archivos bloqueados por host:



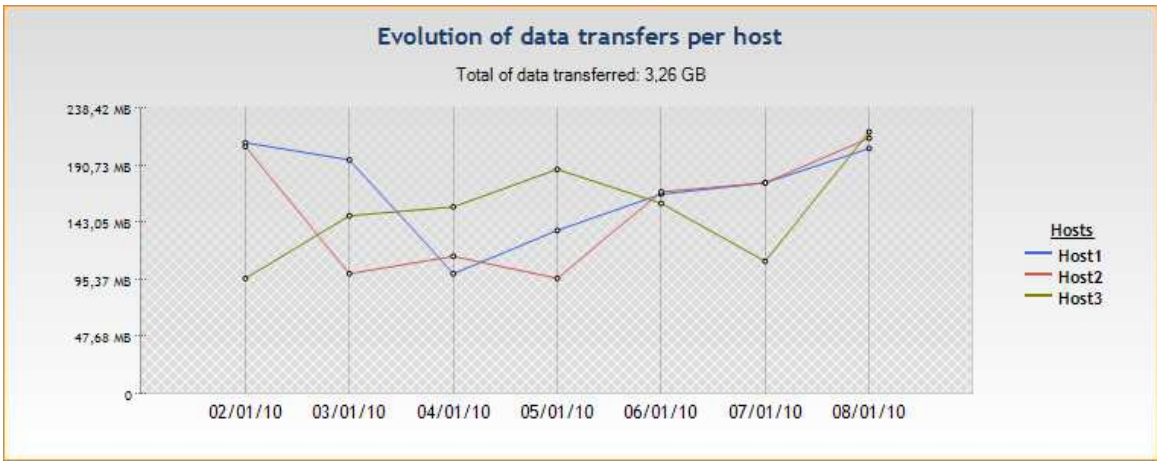
- Evolución de transferencia de datos por dispositivos:



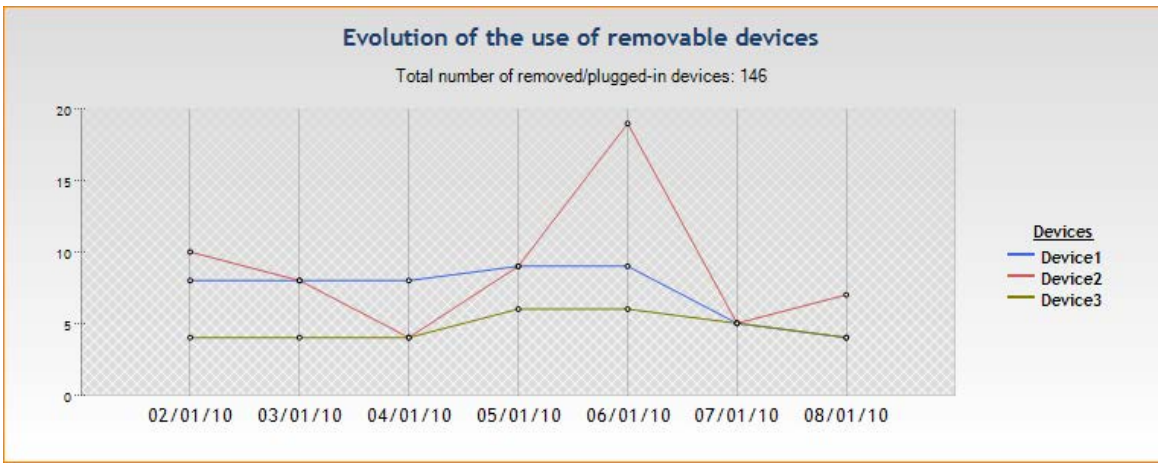
- Evolución de transferencia de datos por usuario



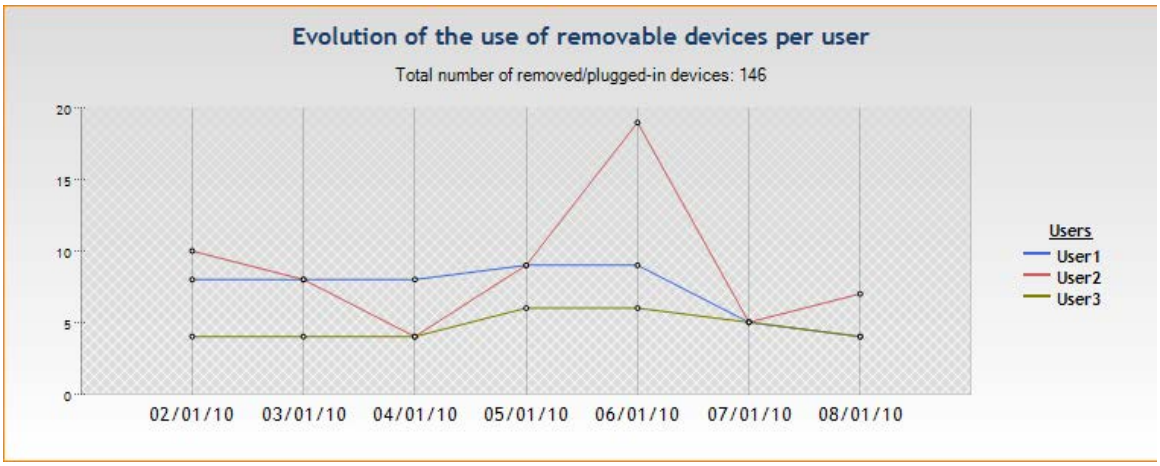
- Evolución de transferencia de datos por host



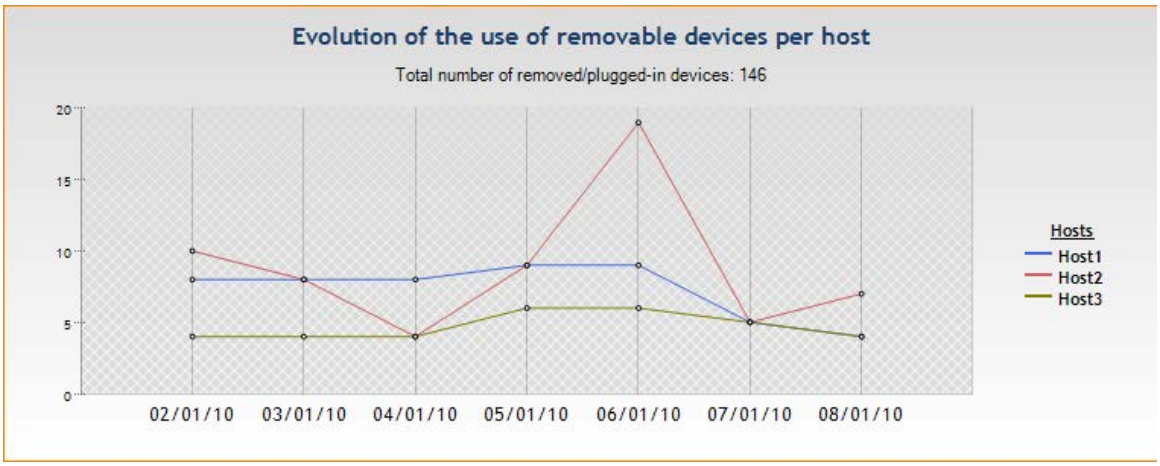
- Evolución de dispositivos extraíbles:



- Evolución del uso de dispositivos extraíbles por usuario:



- Evolución del uso de dispositivos extraíbles por host:



Integridad de las estaciones de trabajo

Los reportes de integridad de las estaciones de trabajo ofrecen la siguiente información en formato Excel:

- Violaciones de políticas por usuario y agente:
  Esto muestra el número de violaciones de cada tipo por cada usuario y por cada agente.

- Archivos bloqueados:
  Esto muestra el nombre de los archivos, el agente y la fecha de acceso.

- Accesos por dispositivos:
  Esto muestra los archivos copiados a una memoria USB para cada usuario y cada agente.

Capítulo 15 - ACTIVIDAD DE MONITOREO

ACERCA DE ESTE CAPÍTULO

Este capítulo describe las herramientas usadas para controlar, monitorear y grabar la actividad en las estaciones de trabajo. Se explicara como acceder a esta información.

Se incluye lo siguiente:

- Generalidades.
- Monitoreando el agente:
  - Interfaz grafica:
    - Opciones visuales.
    - Detalles.
    - Filtros.
- Presencia/Ausencia del agente en la estación de trabajo.
- Monitoreando el log:
  - Generalidades.
  - Interfaz grafica global:
    - área de “Logs”.
    - área de “Información”.
    - área de “Filtros”.
- Administrador de log:
  - Generalidades.
  - Interfaz gráfica:
    - Tipo de logs
    - Opciones visuales.
    - Mensajes.
- Exportando logs a sistemas externos (SMTP o Syslog):
  - Generalidades.
  - Exportando logs a través de SMTP.
  - Exportando logs a través de Syslog.
- Visor de eventos:
  - Generalidades.
  - interfaz grafica:
    - Menú.
    - Columnas.
    - Expandir/Colapsar.

- Detalles.

GENERALIDADES

Aranda 360 es usado para controlar, monitorear y registrar actividad en las estaciones de trabajo a través de las siguientes configuraciones ubicadas en el panel de administración:

- Monitoreando Agente.
- Monitoreando Log.
- Administrador de Log.
- Visor de eventos.

Si está utilizando Aranda 360 por primera vez, es poco probable que algún evento capturado por los agentes Aranda 360 haya sido registrado en la base de datos del reporte.

En este caso, las funciones previstas en este capítulo, por supuesto, estarán disponibles, pero sin ningún dato.

AGENTE DE MONITOREO

Interfaz Gráfica

Opciones

El monitoreo del agente mostrará en el menú las siguientes opciones:

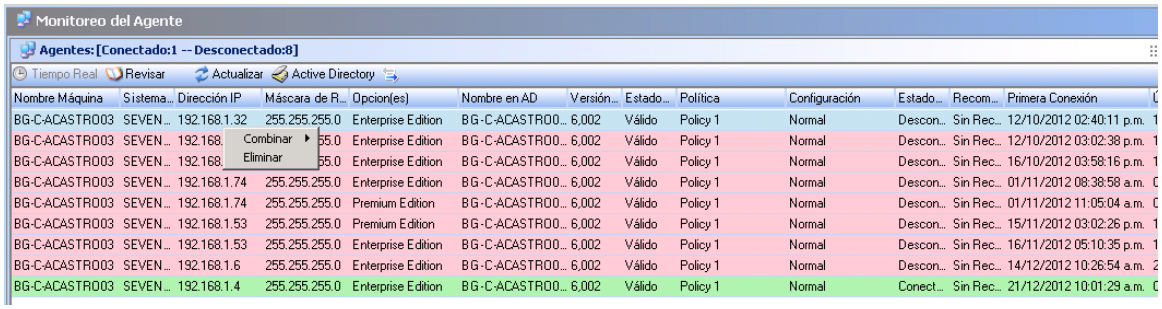
- Real-Time:
  Mostrará información de monitoreo que está siendo actualizada continuamente
  Por defecto, la información de monitoreo es actualizada automáticamente de acuerdo al tiempo de actualización en segundos para monitoreo de agente establecida en la configuración de consola.

- Revisión:
  Muestra información de monitoreo sin actualización automática. Haga clic en Actualizar si desea actualizar la información.

- Actualización:
  Fuerza la actualización de la información de monitoreo (mostrada en modo tiempo-real o en revisión).

- Directorio activo:
  Usado para determinar que maquinas no tienen el software Aranda 360 instalado.

- o o :
  Usado para mostrar información básica o detallada de los agentes. El número de columnas depende de su selección.



Detalles

En el área de monitoreo del agente, cada línea mostrara la siguiente información del agente seleccionado:

- Nombre del host.
- Sistema operativo.
- Dirección Ip.
- Mascara de red:
  Mascara de sub-red.
- Opciones:
  Paquetes y opciones Aranda 360 (Si existen).
- Nombre AD:
  Nombre complete en el dominio del directorio activo.
- Versión de agente:
  Numero de versión del agente de Aranda 360.
- Config. Estado:
  El estado de la configuración puede ser valido o invalido:
  - Válido indica que la configuración es válida hasta cierta fecha.
  - Invalido indica que el administrador ha enviado una nueva configuración pero que esta última aún no ha sido recibida por el agente.
- Política:
  Nombre de la política aplicada.
- Configuración:
  Nombre de la configuración aplicada.
- Estado de agente:
  - Conectado.
  - Desconectado.
  - Alerta.
  - En espera.
  - Desconocido.

- Recomendaciones:
  Estado de variables (usado en los scripts de acciones y pruebas) que pueden ser usados por clientes TNC (Trusted Network Connect) como clientes Odyssey Access Clients sobre redes Juniper (R).

  Las opciones disponibles son:
  - Permitido.
  - Aislado.
  - Sin acceso.
  - Sin recomendación.

  No recomendación esta activado por defecto y trabaja solamente en el modo servidor juniper.

  Podría perderse un driver (Heimdall, Loki, Thor), el valor aplicado por defecto será No hay recomendaciones. No será posible modificar este valor hasta el siguiente reinicio del agente. Además, los drivers tendrán que ser instalados correctamente.

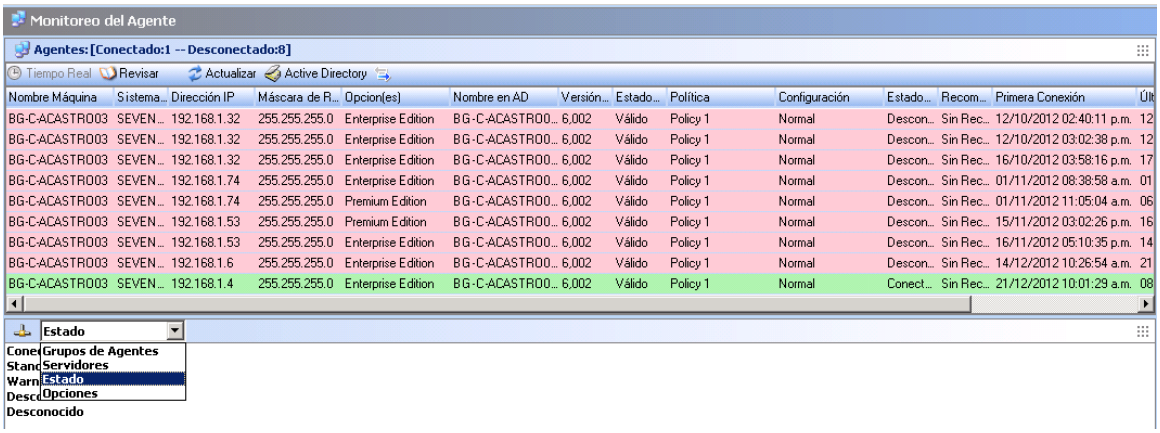
- Primera conexión:
  La primera vez que el agente y el servidor se comuniquen entre sí.

- última conexión:
  La última vez que el agente y el servidor se comunicaron entre sí.

- Config. Actualizada:
  La fecha y la hora en que la configuración actual se recibió y se aplicó.

Filtros

El administrador puede filtrar logs mediante los siguientes elementos:

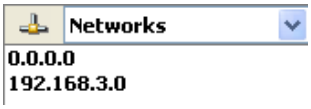


- Estado:
  - Agentes conectados.
  - Agentes en modo de espera.
  - Agentes en modo de alerta.
  - Agentes desconectados.
  - Agentes con estado desconocido.
- Redes
- Servidores.
- Opciones:
  - Professional Edition.
  - Secure Edition.

Cuando el administrador selecciona un filtro en el menú desplegable, se muestra una lista.

Ejemplo:

Si selecciona Redes, usted puede elegir una dirección de red específica. El log sólo mostrará la información de la red seleccionada.



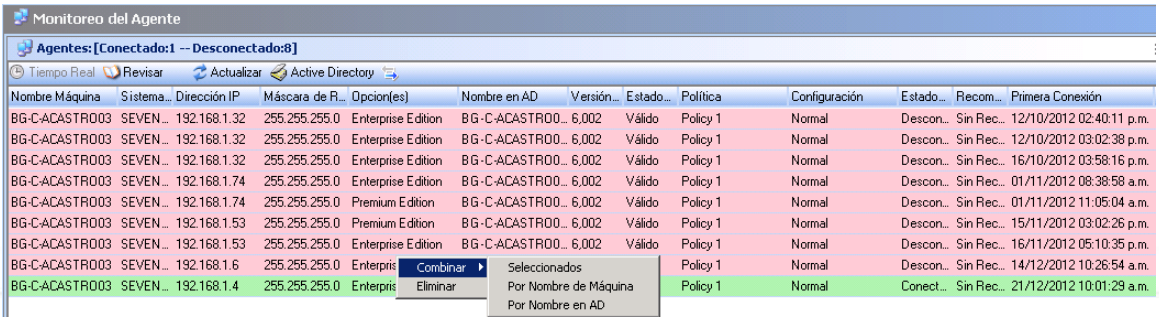
Menú (Clic derecho)

Unir

El administrador puede combinar los identificadores de máquina para mostrar sólo una entrada relativa para la vigilancia de un agente. Esto está diseñado para actualizar el número de licencias utilizadas de una manera eficazmente.

Para ello, el administrador debe hacer clic derecho en la lista de agentes para visualizar las siguientes opciones:

- Seleccionar:
  Las entradas seleccionadas por el administrador se fusionarán. El administrador debe seleccionar por lo menos dos entradas para habilitar esta opción.
- Por nombre de host:
  Todas las entradas en la misma máquina se fusionarán. La fusión por nombre de host se aplica a toda la lista de agentes.
- Por nombre AD:
  Todas las entradas que tengan el mismo nombre de AD (Directorio activo) se fusionarán.



Eliminar

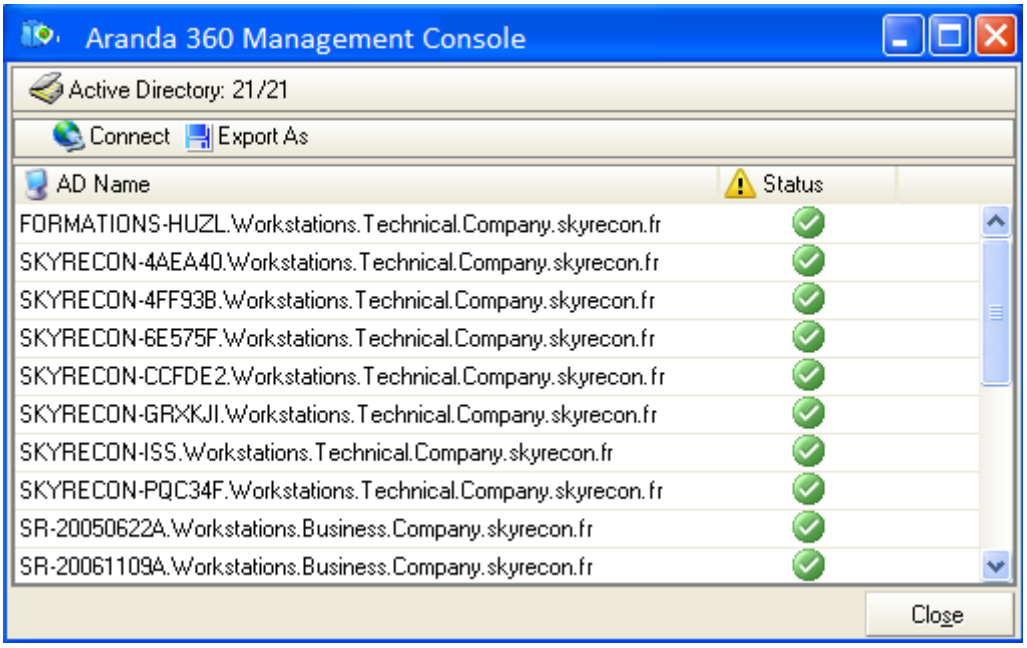
El administrador puede borrar el historial de estado de un agente. Si el agente ya no está presente en una estación de trabajo, su licencia quedará disponible para otra estación de trabajo.

Los avisos enviados por el agente se conservan.

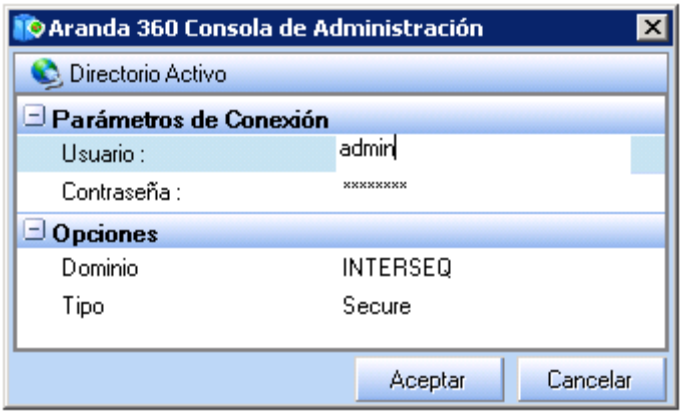
Presencia/ausencia del agente en la estación de trabajo

Para comprobar la presencia o ausencia del agente en las estaciones de trabajo, siga los siguientes pasos:

1. En la ventana Monitoreo de Agente, haga clic en Directorio Activo. La lista del directorio activo se mostrara.



2. Haga Clic en Conectar.
3. Ingrese la siguiente información:
   - Usuario de sesión.
   - Contraseña.
   - Dominio.
   - Tipo (de conexión).



4. Haga clic en OK.
   Aparecerá una lista de máquinas mostrando el estado respectivo de cada una:
   - Si el agente ha sido instalado, un icono de marcado se mostrará.

- Si el agente no ha sido instalado, un icono de cruz se mostrará.

5. Se puede utilizar Exportar como para guardar la información en un archivo con cualquiera de los siguientes formatos:
   - TXT (tabs usados como separadores).
   - CSV (comas usadas como separadores).
   - XML.

MONITOREO DEL LOG

Generalidades

En el monitoreo del log se registran actividades sospechosas que tienen lugar en las estaciones de trabajo y la reacción correspondiente del agente de Aranda 360.

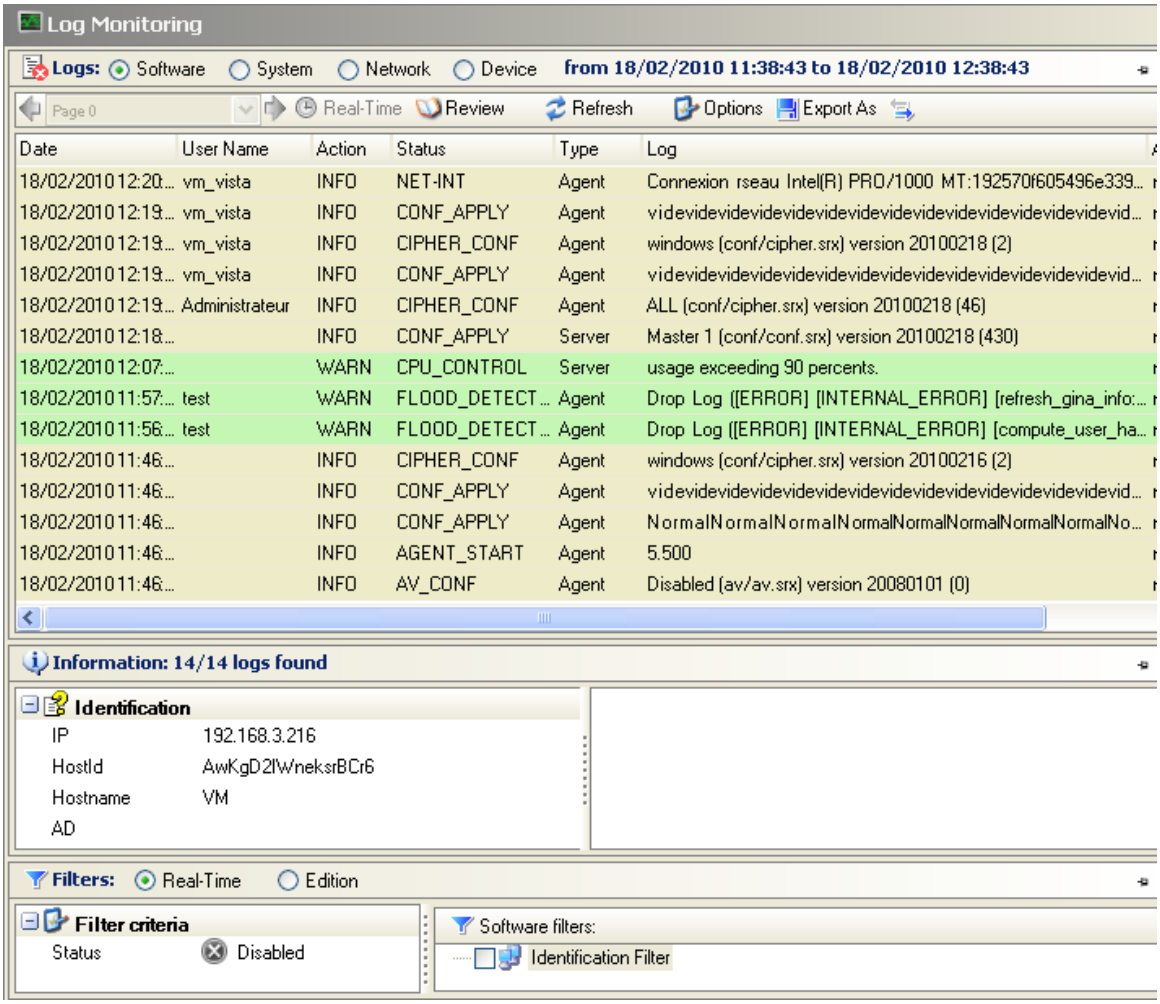
Estos datos se consolidan en una base de datos donde se puede consultar a través de la consola de administración de Aranda.

Los logs de Aranda 360 contienen un registro de todos los eventos desencadenados asociados a:

- Software.
- Sistema.
- Red.
- Dispositivo.

Las actividades que pueden desencadenar un evento se define en las políticas de seguridad.

Interfaz gráfica global



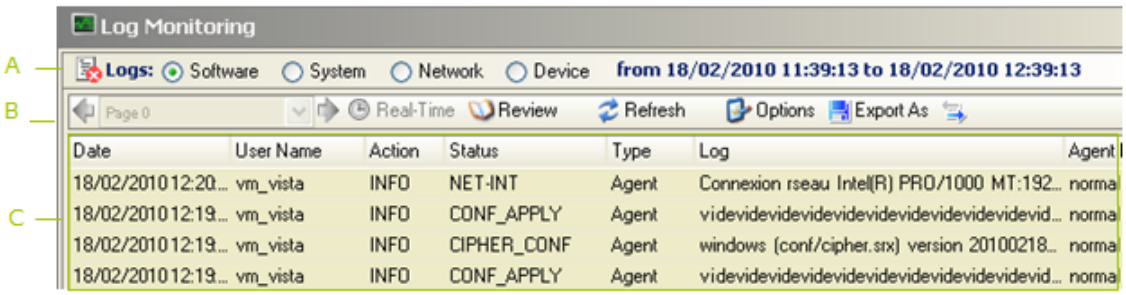
La interfaz gráfica de monitoreo de log incluye tres áreas:

- Logs.
- Información.
- Filtros.

Área "Logs"

El área de logs se divide en tres sub-áreas:

- Tipo de Log (A).
- Opciones visuales (B).
- Detalles (C).



Log de sub-área

El log de sub-área incluye los siguientes elementos:

- Software.
- Sistema.
- Red.
- Dispositivo

Logs del software

Propósito

Un log de software registra el comportamiento del agente cuando:

- El agente aplica una configuración o política.
- El agente descarga un certificado o una actualización.
- Hay una sobrecarga de la CPU de un servidor.
- El número de agentes excede el permitido por licencia.
- Etc.

> Los logs son mostrados en la consola de administración de Aranda con los filtros aplicados. De cualquier modo, cuando usted exporta un log a un archivo o a un correo electrónico, la entrada del log es incluida (sin ningún filtro aplicado).

Columnas del log del Software

En modo expandido (clic en), las columnas del log del "Software" son las siguientes:

- Fecha.
- Nombre de usuario:
  Identificador del usuario.

- Acción:
  Acción registrada.
  Las acciones posibles son [BLK] para bloqueo [INFO] para la auditoría y [WARN] para el modo de advertencia.

- Estado:
  Estado de acciones.
  Por ejemplo: [ACTION-FALLIDA].

- TIPO:
  Los Posibles tipos son [AGENTE] y [SERVIDOR].

- Mod. Nombre:
  Nombre del modulo.

- Log:
  Mensaje de información.

- Modo agente:
  Los posibles modos de agente por defecto son NORMAL y ADVERTENCIA.

En modo colapsado (clic en), las columnas del log del "Software" son las siguientes:

- Fecha.
- Nombre de usuario.
- Acción.
- Estado.
- Tipo.
- Log.
- Modo Agente.

Logs del sistema

Propósito

El log del "Sistema" contiene información de la protección del sistema.

Columnas del log del Sistema

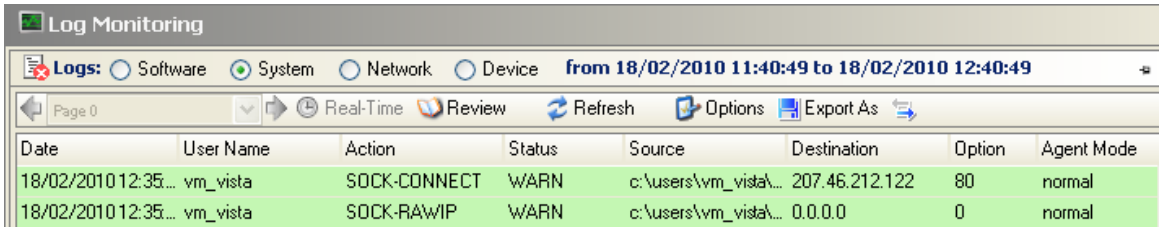
En modo Expandido, las columnas del log del "Sistema" son las siguientes:

- Fecha.
- Nombre del usuario:
  Identificador de usuario.
- Acción:
  Acción registrada.
- Estado:
  Estado de la acción.
- Fuente:
  Nombre del programa fuente.
- Destino:
  Nombre del programa o archivo Destino.
- Opción.
- RID:
  Regla de único identificador.
- Modo del agente:
  Los posibles modos de agente por defecto son NORMAL y ADVERTENCIA.

En Modo colapsado, las columnas del log del "Sistema" son las siguientes:

- Fecha.
- Nombre de usuario.
- Acción.
- Estado.
- Fuente.
- Destino.
- Opción.

- Modo de agente.



Logs de red

Propósito

Logs de "Red" contienen información de:

- Firewall de red (Categoría).
- Detección de intrusión al Sistema (Configuraciones generales > Control de actividad de red).

Columnas del log de red

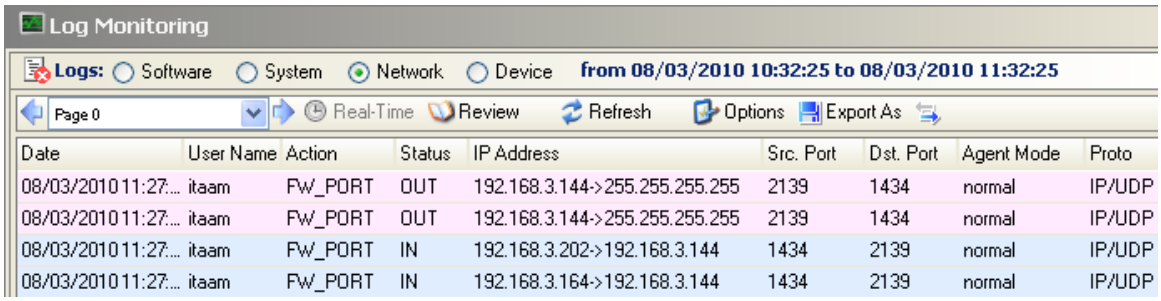
En modo expandido, las columnas del log de red son las siguientes:

- Fecha.
- Nombre de usuario:
  Identificador de usuario.
- Acción:
  Acción registrada.
- Estado:
  Estado de la acción.
- Metadata:
  Información del evento registrado.
  Ejemplo: En caso de desbordamiento, el campo indica cuantas veces ocurrió el evento. De lo contrario, mostrará la dirección MAC.
- Dirección IP:
  SSID (WiFi), fragmento de IP o dirección IP.
- Src. Port: Puerto origen.
- Dst. Port:
  Puerto destino.
- Proto1:
  Protocolo sobre Ethernet.
- Proto2:
  Protocolo IP.
- RID:
  Regla de único Identificador.
- Modo agente:
  Los Posibles modos de agente por defecto son NORMAL y ALERTA.

En modo Colapsado, las columnas del log son:

- Fecha.
- Nombre de usuario.
- Acción.
- Estado.
- Dirección IP.
- Src Port.
- Dst Port.
- Modo de agente.
- Proto:
  [Protocolo sobre Ethernet]: [protocolo IP].

Variables del log de red



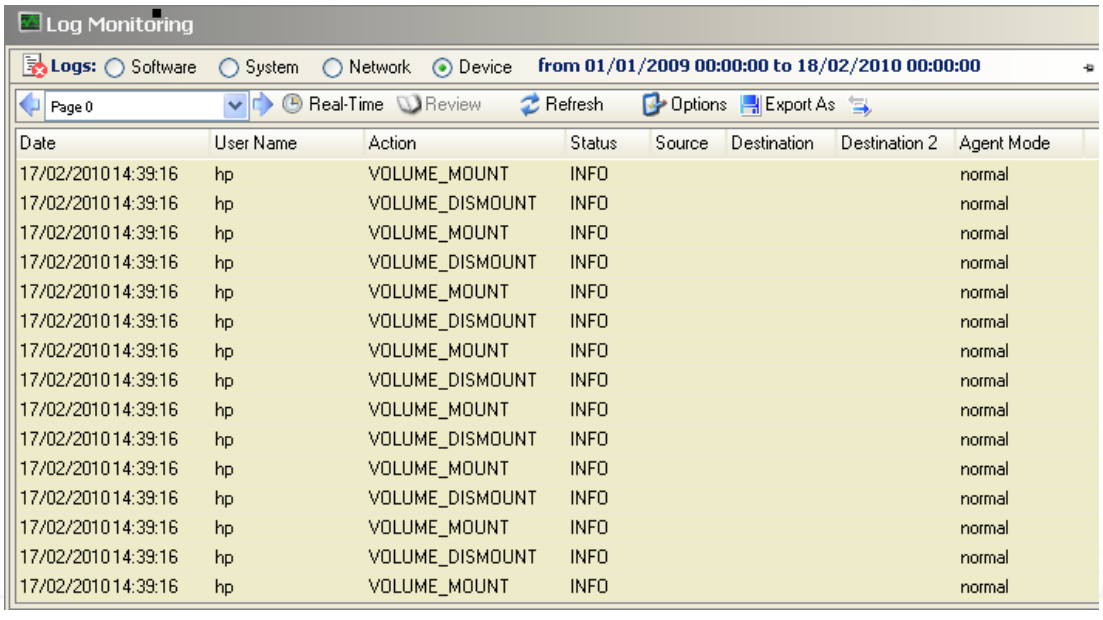
Date	User Name	Action	Status	IP Address	Src. Port	Dst. Port	Agent Mode	Proto
08/03/2010 11:27:...	itaam	FW_PORT	OUT	192.168.3.144->255.255.255.255	2139	1434	normal	IP/UDP
08/03/2010 11:27:...	itaam	FW_PORT	OUT	192.168.3.144->255.255.255.255	2139	1434	normal	IP/UDP
08/03/2010 11:27:...	itaam	FW_PORT	IN	192.168.3.202->192.168.3.144	1434	2139	normal	IP/UDP
08/03/2010 11:27:...	itaam	FW_PORT	IN	192.168.3.164->192.168.3.144	1434	2139	normal	IP/UDP

Log de dispositivos

Propósito

Log de "Dispositivo" contiene información:

- Dispositivos extraíbles (Categoría).
- Control de dispositivos (configuraciones generales).
- Autenticación y cifrado de wifi (configuraciones generales).



Date	User Name	Action	Status	Source	Destination	Destination 2	Agent Mode
17/02/2010 14:39:16	hp	VOLUME_MOUNT	INFO				normal
17/02/2010 14:39:16	hp	VOLUME_DISMOUNT	INFO				normal
17/02/2010 14:39:16	hp	VOLUME_MOUNT	INFO				normal
17/02/2010 14:39:16	hp	VOLUME_DISMOUNT	INFO				normal
17/02/2010 14:39:16	hp	VOLUME_MOUNT	INFO				normal
17/02/2010 14:39:16	hp	VOLUME_DISMOUNT	INFO				normal
17/02/2010 14:39:16	hp	VOLUME_MOUNT	INFO				normal
17/02/2010 14:39:16	hp	VOLUME_DISMOUNT	INFO				normal
17/02/2010 14:39:16	hp	VOLUME_MOUNT	INFO				normal
17/02/2010 14:39:16	hp	VOLUME_DISMOUNT	INFO				normal
17/02/2010 14:39:16	hp	VOLUME_MOUNT	INFO				normal
17/02/2010 14:39:16	hp	VOLUME_DISMOUNT	INFO				normal
17/02/2010 14:39:16	hp	VOLUME_MOUNT	INFO				normal
17/02/2010 14:39:16	hp	VOLUME_DISMOUNT	INFO				normal
17/02/2010 14:39:16	hp	VOLUME_MOUNT	INFO				normal
17/02/2010 14:39:16	hp	VOLUME_DISMOUNT	INFO				normal
17/02/2010 14:39:16	hp	VOLUME_MOUNT	INFO				normal

Columnas del log de dispositivos

En modo expandido, el log de "Dispositivos" tiene las siguientes columnas:

- Fecha.
- Nombre de usuario:
  Identificador de usuario.
- Acción:
  Acción registrada.
- Estado:
  Estado de una acción.
  Los posibles estados para una acción son [BLK] para bloqueos, [INFO] para auditoria y [WARN] para el modo de alerta.
- Fuente:
  Nombre de la tarjeta de red (WiFi) o proceso (dispositivo extraíble de almacenamiento masivo).
- Destino:
  Nombre del archivo, ruta o dirección MAC (WiFi bloqueada).
- Destino2:
  Nombre del archivo después de renombrado (dispositivo extraíble de almacenamiento masivo) o SSID (WiFi).
- Tamaño:
  Tamaño del Dispositivo.
- Tipo:
  Tipo de dispositivo.
  Los posibles tipos son [FIREWIRE], [NETWORK], [PCMCIA], [USB], [NONE].
- Clase:
  Identificador de la clase de dispositivo.
  Las posibles clases son [BLUETOOTH], [CDROM], [DISK], [IRDA], [MODEM], [PARALLEL], [PCMCIA], [SERIAL],[WIFI].
- RID:
  Regla de identificador único.

- Modo agente:
  Posible modo agente por defecto son NORMAL y ALERTA.

En modo colapsado, las columnas del log de "Dispositivo" son:

- Fecha.
- Nombre de usuario.
- Acción.
- Estado.
- Fuente.
- Destino.
- Destino2.
- Modo agente.

Opciones de sub-área

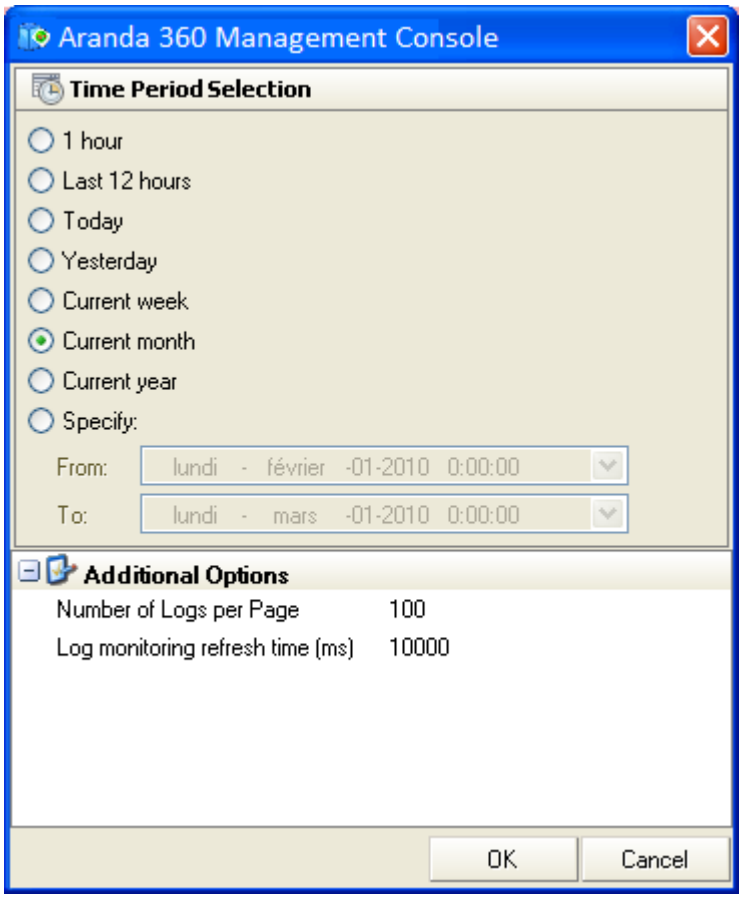
Las opciones visuales de la sub-área son:

- Tiempo-real:
  Muestra continua información del monitoreo la cual es actualizada constantemente.
  Por defecto, la información es actualizada cada 30 segundos.

- Revisión:
  Muestra las alertas reportadas a través de un periodo de tiempo definido por el administrador.

- Actualizar:
  Fuerza una actualización de la información de monitoreo.

- Opciones



Selección del periodo de tiempo:

Especifica el periodo de tiempo que será usado para mostrar información en modo de revisión.

- Opciones adicionales:
  Especifica el número de logs que serán mostrados por página y el tiempo de actualización de los datos.

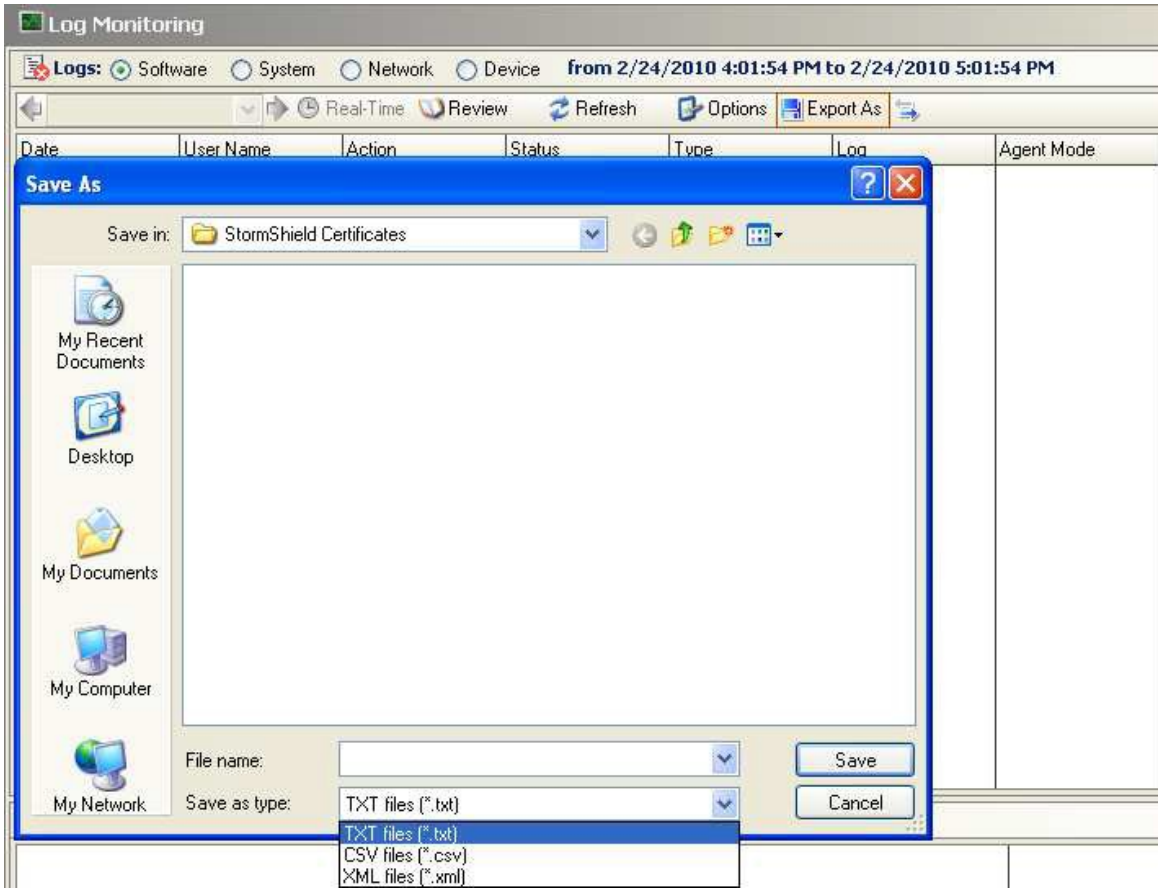
- Exportar como:
  Guarda la información del log a un archivo.
  La característica permite al administrador exportar un log visible (i.e. que es normalmente mostrado en la consola de administración de Aranda).
  Los siguientes formatos son los soportados por esta característica:

  - TXT (Separado por tabs).
  - CSV (separados por comas).
  - XML.

La información incluida en el archivo exportado es la del log seleccionado (el log mostrado) y la información de identificación.

Para exportar un log a un archivo, los pasos son:

1. Seleccione el log que usted quiere exportar.
2. Haga clic en Exportar como.
3. Desde la lista desplegable, seleccione el formato de archivo que quiere usar (Ejemplo: TXT).
4. Establezca la ruta e ingrese el nombre del archivo.
5. Haga clic en guardar.



Detalles de sub-área

La información dada en los Detalles de sub-área (columnas) depende del tipo de log seleccionado. Esta sub-área mostrará sistemáticamente las Acciones y los estados en columnas.

Haciendo Clic en el icono mostrara menos información. Con el icono mostrará más información.

Los Detalles de sub-área pueden ser configurados para un análisis posterior.

Área "información"

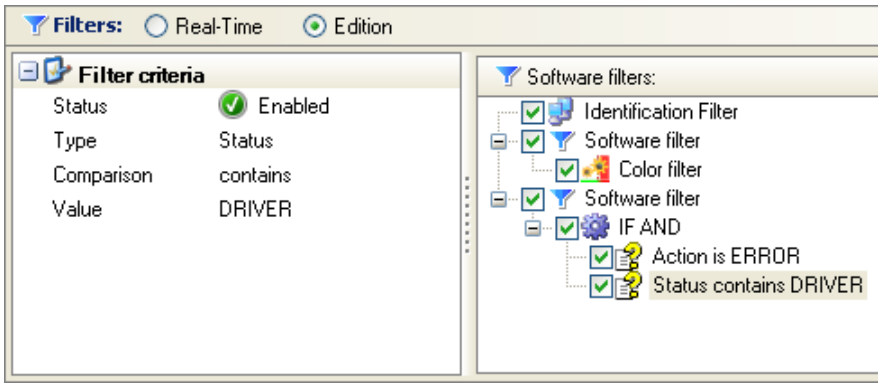
El área "Información" contiene información relevante a la maquina donde se generó el log:

- Su dirección IP.
- Su Id de host (identificador único creado por Aranda 360 para cada agente).
- Su nombre.
- Su nombre en el directorio activo.

Área "Filtros"

El área filtros contiene los criterios para los filtros que seleccionaran la información que se va a mostrar.

Ejemplo:
Usted puede filtrar en el log de "Software" las acciones de ERROR que contengan en estado DRIVER.



Existen dos opciones:

- Tiempo-real.
  Se aplica este filtro al log para mostrar información inmediatamente después de enviar la petición.

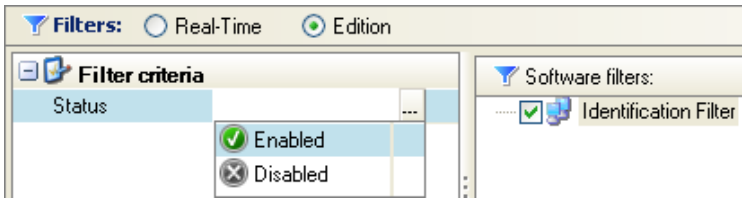
- Edición.
  El filtro es aplicado para mostrar el log después de que el administrador haga clic en actualizar.

  - Cuando se crean o modifican filtros, usted puede mover los ítems simplemente arrastrando y soltando.

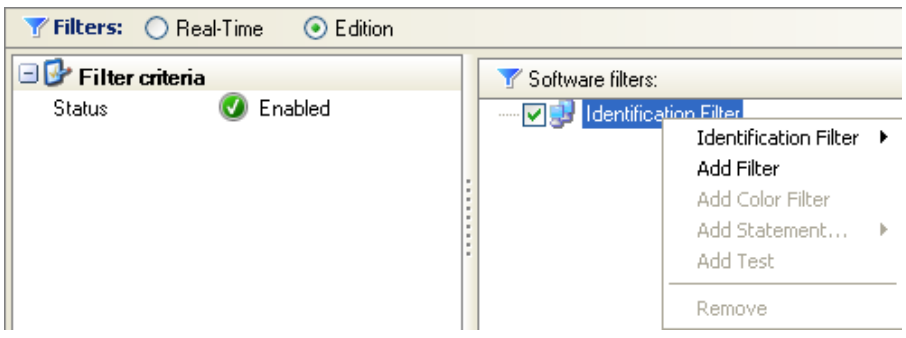
Adicionando un filtro

Para adicionar un filtro usted debe:

1. Hacer clic-derecho en la segunda columna para activar el filtro, justo en frente de estado en Criterios de filtro.

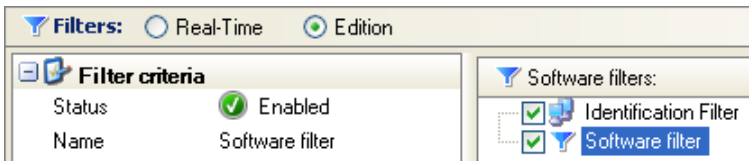


2. Hacer clic-derecho en Filtro identificación el cual es mostrado por defecto en la ventana de filtros (a la derecha).
   El siguiente menú desplegable se mostrará.



3. Haga clic en Adicionar Filtro.
   El Nuevo filtro aparecerá en la estructura de árbol.

Un filtro para "Software" es mostrado en este ejemplo porque usted se encontraba en la sección de logs de software.

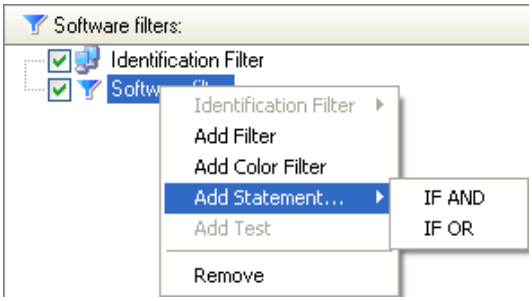


4. Defina las configuraciones para el filtro que acaba de adicionar (ejemplo: Adicione el color).
5. También puede adicionar otro filtro para "Software".

Adicionando una declaración

Para agregar una declaración a un filtro, usted debe:

1. Hacer clic-derecho en el filtro.
   Se mostrará el siguiente menú desplegable:



2. Haga clic en adicionar declaración.
3. Seleccione la declaración.

Adicionando una prueba

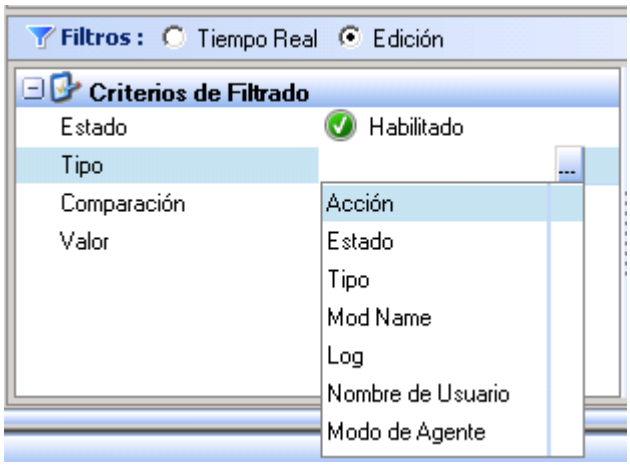
Para agregar una prueba a una declaración, usted debe:

1. Hacer clic-derecho en la declaración.
2. Seleccionar adicionar prueba.
3. Definir las configuraciones de la prueba.

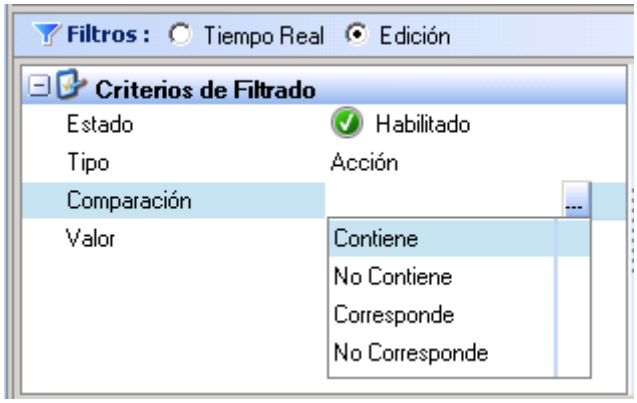
Usted puede configurar una prueba usando los siguientes campos:

- Estado:
  Activa o desactiva la prueba (Activar/Desactivar).

- Tipo:
  Define que elementos serán probados.



- Comparación:
  Define los valores de comparación usados en la prueba.



El uso de los valores de comparación "contienen" (o no contienen) están basados en el motor de búsqueda SQL y en su sintaxis. Esta sintaxis implica:

- _: representa cualquier carácter.
- %: representa cualquier carácter repetido 0 o n veces.

La consola encapsula la cadena de búsqueda dentro del carácter "%" cuando el usuario no introduce meta caracteres SQL (ejemplo: Archivo => %archivo%).

Si el usuario agrega un "_" o "%" en la cadena de búsqueda, la consola no encapsulará esta cadena. La búsqueda se realizará exactamente sobre lo que el usuario ha especificado (ejemplo: archivo_ => archivo_, la consola no cambia en nada la cadena de búsqueda).

- Para buscar un meta carácter y que se puedan entender literalmente, el usuario debe colocarlos entre corchetes (ejemplo: File [_]% para Búsquedas donde la cadena comienza con file_.

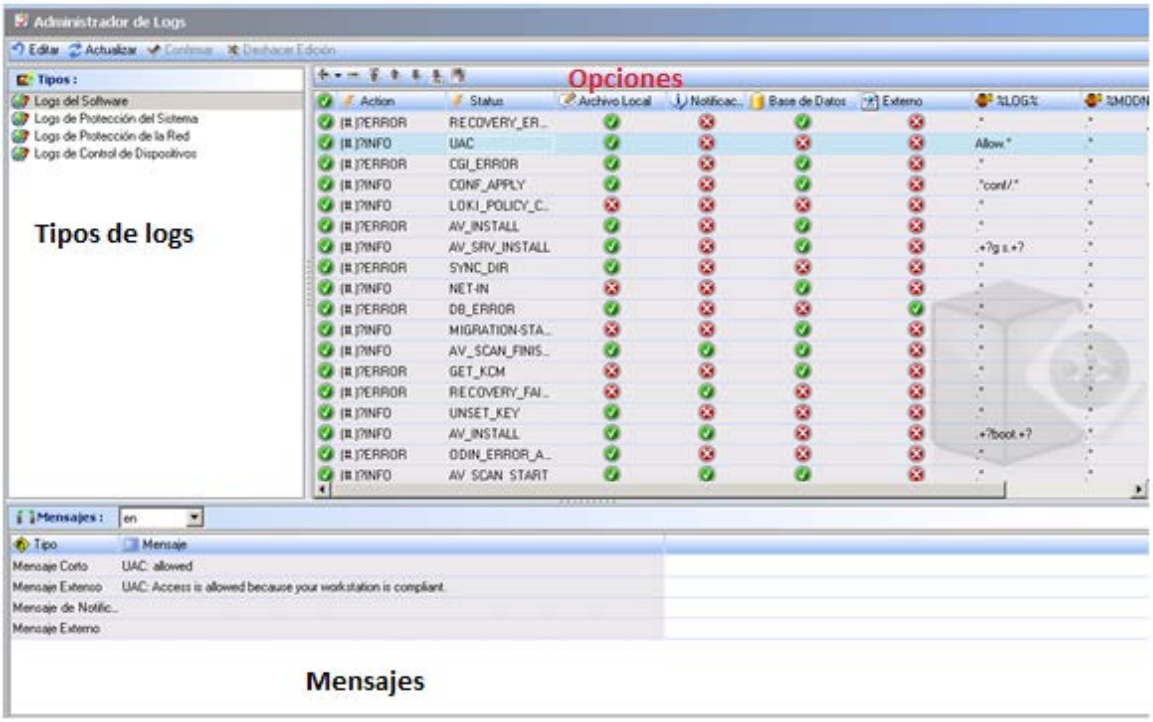
o Valor:
Para ser introducido por el administrador.

ADMINISTRADOR DE LOG

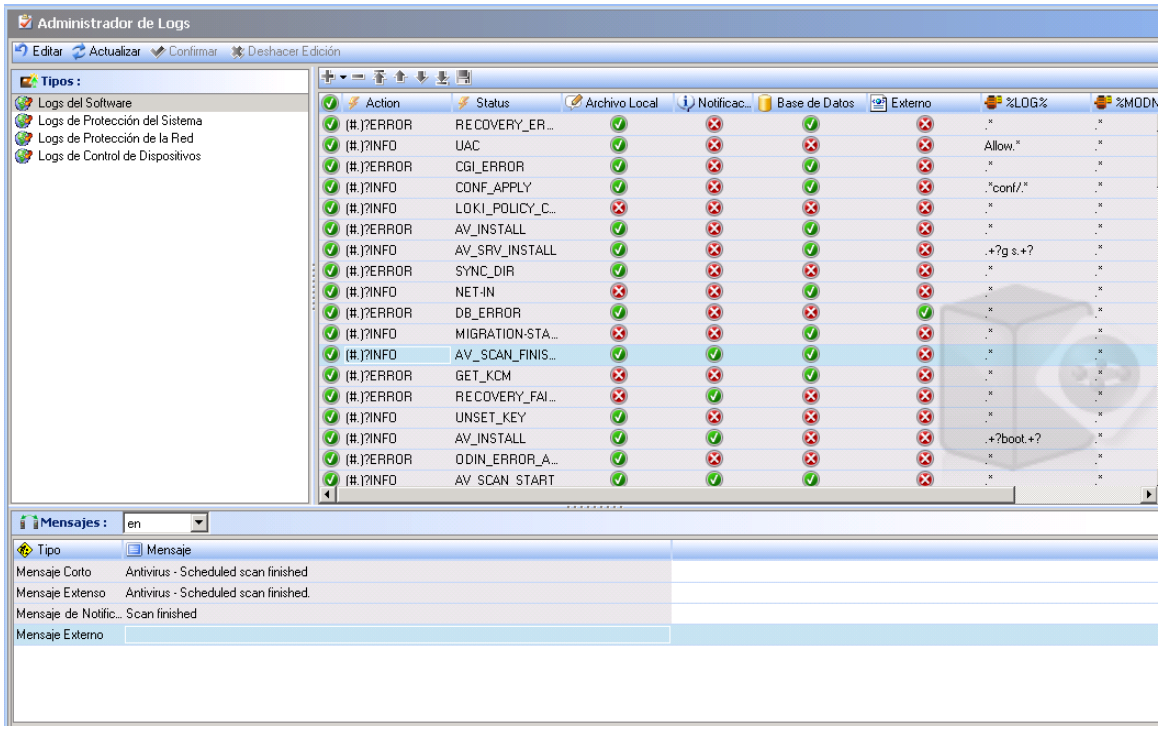
Generalidades

El administrador de Log se utiliza para personalizar los registros en el Log de los agentes de Aranda 360. Está diseñado para reportar los siguientes eventos:

- Logs de Software.
- Logs de Sistema
- Logs de red.
- Logs de dispositivo.



Los eventos se utilizan para generar informes que son provocados por ciertas acciones y estados. Las acciones y estados que activan un registro se definen en las políticas de seguridad.



Ejemplo 1:

La acción INFORMACION con el estado:

- EJECUCION_AGENTE:
  Creación de informes basado en la versión del agente

- VERSION_SERVIDOR:
  Creación de reportes basados en la versión y nombre del servidor

- APLICACION_CONFIGURACION:
  Creación de reportes basado en la política o configuración del nombre

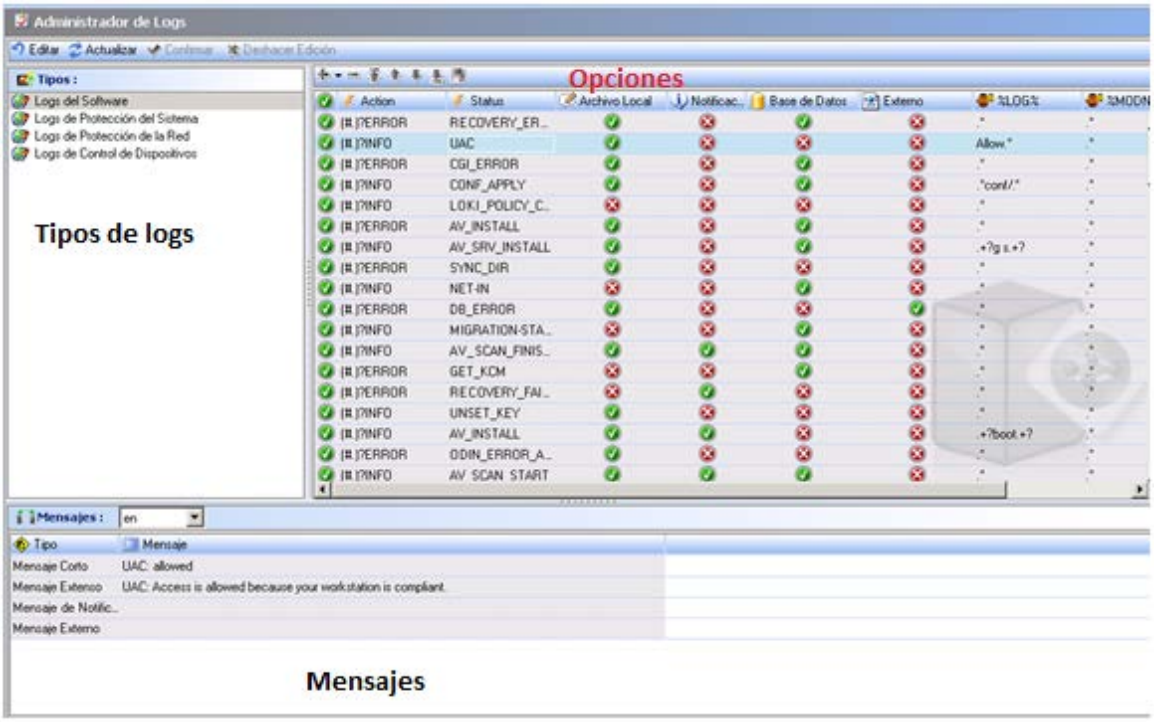
Ejemplo 2:

La acción WARN con el estado DETECCION_FLUJO es usado para crear reportes de flujo. (Repetir mensajes de Log hasta saturación)

- Si el administrador filtra cualquiera de estas acciones en el Administrador de Log, los informes basados en cualquiera de los siguientes no se podrán mostrar:
  - Versión
  - Política del nombre.
  - Configuración del nombre.
  - Servidor de flujo.

- Después de actualizar Aranda 360, los nuevos filtros de log no están habilitados de forma predeterminada.
  Para habilitar los filtros nuevos, el administrador debe seguir los siguientes pasos:
  - Ir a Administrador de Log
  - Activar manualmente los filtros nuevos (que son de color gris).
  - Sincronizar con el servidor.

Interfaz gráfica



La interfaz gráfica incluye tres sub-áreas:

- Tipos de registro.
- Opciones de visualización.
- Mensajes.

Tipo de logs

Los tipos de Logs que se pueden gestionar desde el Administrador de Logs son los siguientes:

- Software.
- Sistema.
- Red.
- Dispositivo.

Opciones

Simplemente haga clic en la columna correspondiente para parametrizar la visualización de cada Logs. Si se habilita un parámetro, la columna contendrá el icono.

Si desactiva un parámetro, la columna contendrá el icono.

Todos los Logs contienen la acción y las columnas de estado.

Según la configuración, los Logs pueden ser consultados y almacenados en las siguientes ubicaciones:

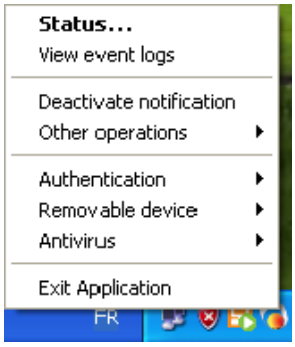
- Interfaz de usuario.
- Emergente.
- Base de datos.
- Aplicación externa.

> Usted puede agregar o eliminar Logs procedentes de un agente de Aranda 360 en el Administrador de Logs en la consola del administrador de Aranda

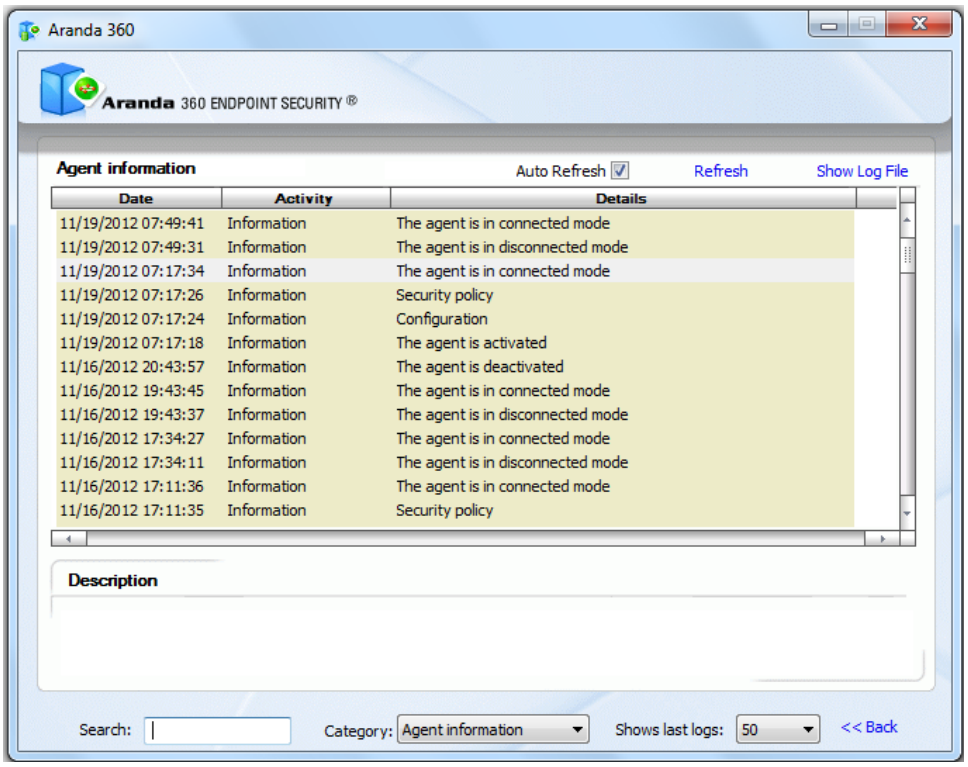
Interfaz de usuario

Este es el sistema de archivos de Logs de los agentes de Aranda 360. Para visualizar este archivo en el equipo del agente, siga los siguientes pasos:

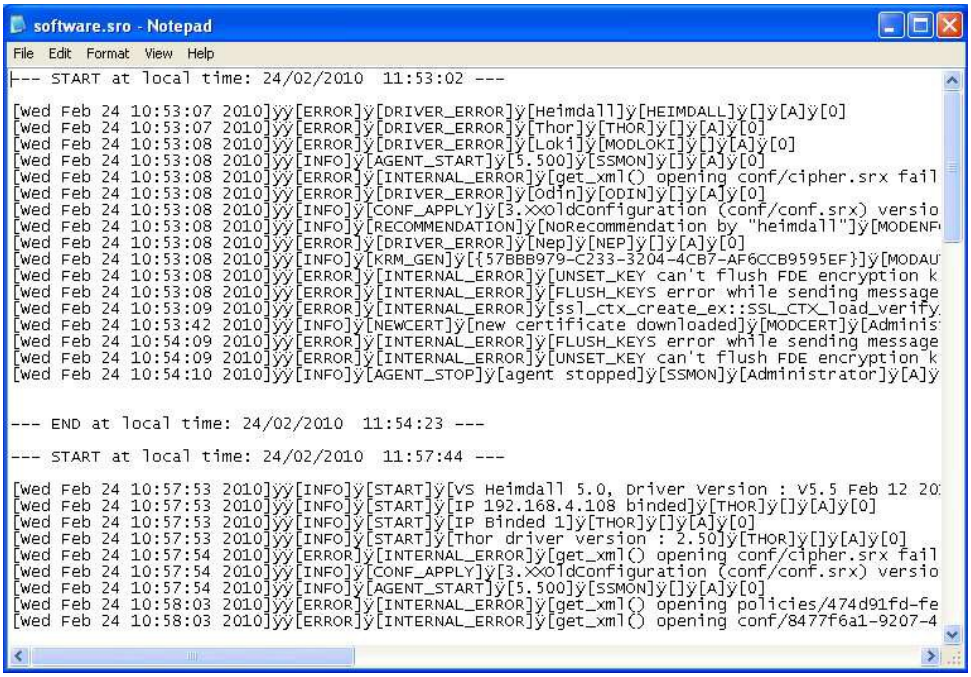
1. Haga clic en “ver eventos de Logs”



2. Haga clic en “mostrar archivo de Logs”



La siguiente pantalla es visualizada



Ventana emergente

El Log se mostrará en la ventana de notificación del agente de Aranda 360.

Base de datos

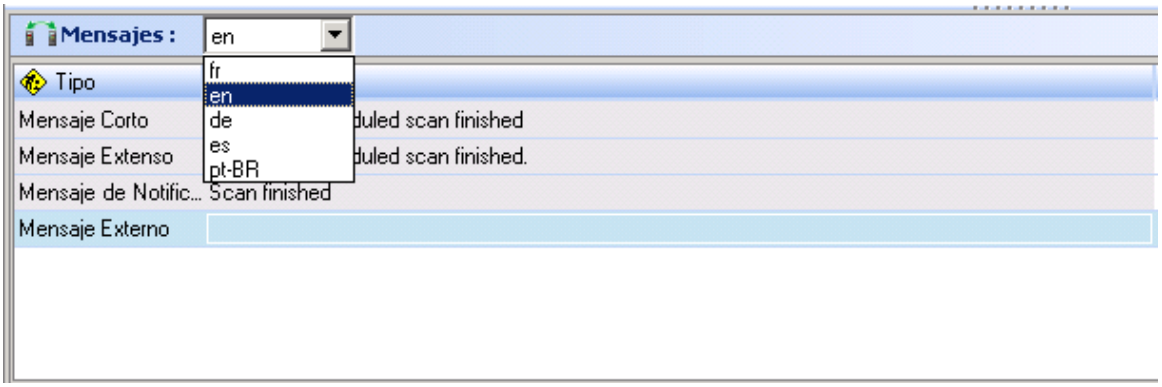
El Log se guardara en la base de datos de Log

Aplicación externa

El Log se envía a un sistema externo (syslog o SMTP)

Mensajes
Lenguaje

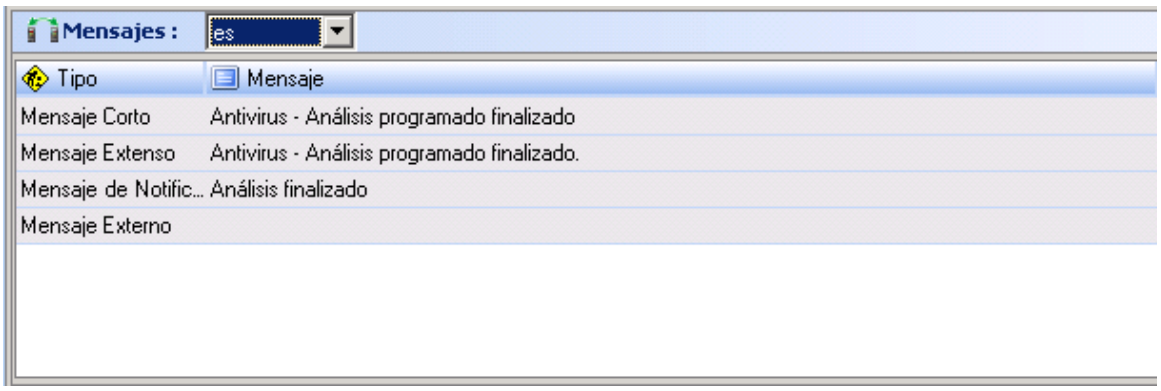
En la ventana de mensajes usted puede elegir el idioma que se utiliza para mostrar los mensajes. El idioma por defecto es el inglés.



Tipo de mensajes

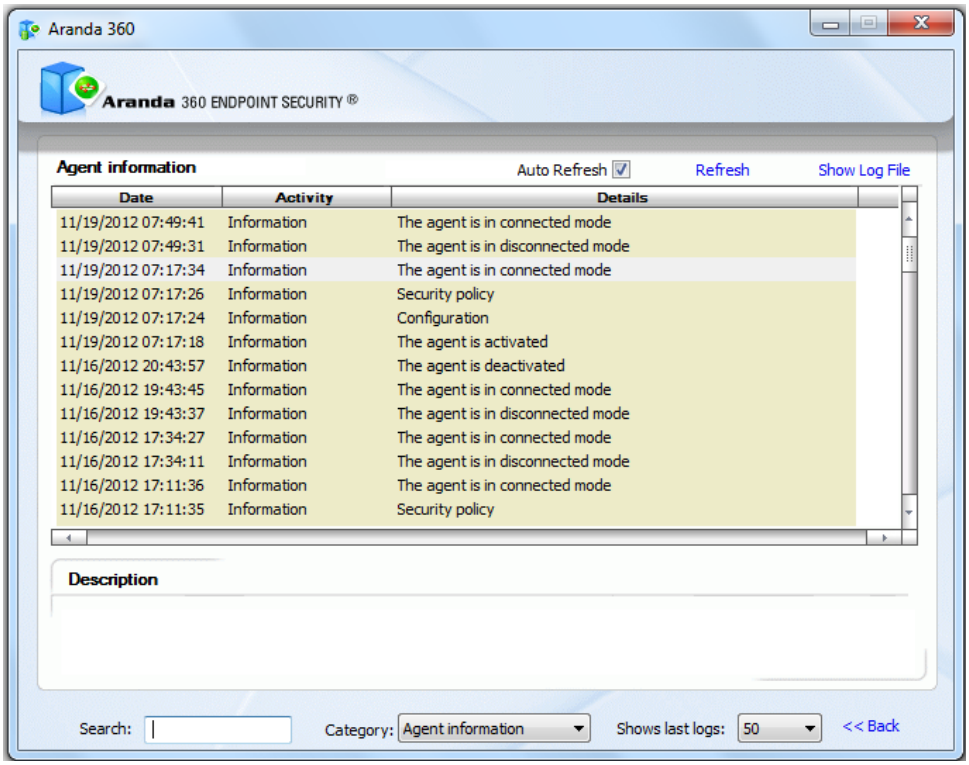
La ventana de mensajes incluye cuatro tipos de mensajes:

- Mensaje Corto.
- Mensaje largo.
- Notificación de mensajes.
- Mensajes externos.



1. Mensaje corto
   Este es el mensaje que aparece en la columna “Detalles” después de seleccionar Ver los eventos de Logs del agente de Aranda 360.

2. Mensaje largo
   Este es el mensaje que aparece en la columna “Descripción” después de seleccionar Ver los eventos de Logs del agente de Aranda 360.



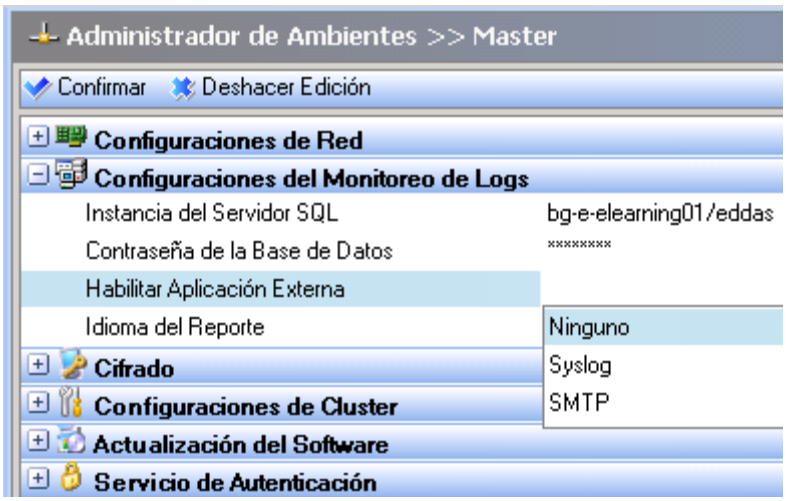
3. Notificación de mensaje
   Este es el mensaje que aparece en la notificación emergente del agente de Aranda 360.
4. Mensaje externo
   Este es el mensaje que será enviado a un sistema externo (syslog o SMTP).

EXPORTANDO LOGS A UN SISTEMA EXTERNO (SMTP O SYSLOG)

Generalidades

El administrador puede utilizar Syslog o SMTP (correo electrónico) para enviar los registros a un servidor externo. Se debe configurar la transferencia del log.

La Exportación de Log está configurada en el Administrador de ambientes> [Servidor Maestro] > Configuración del Monitoreo del Log

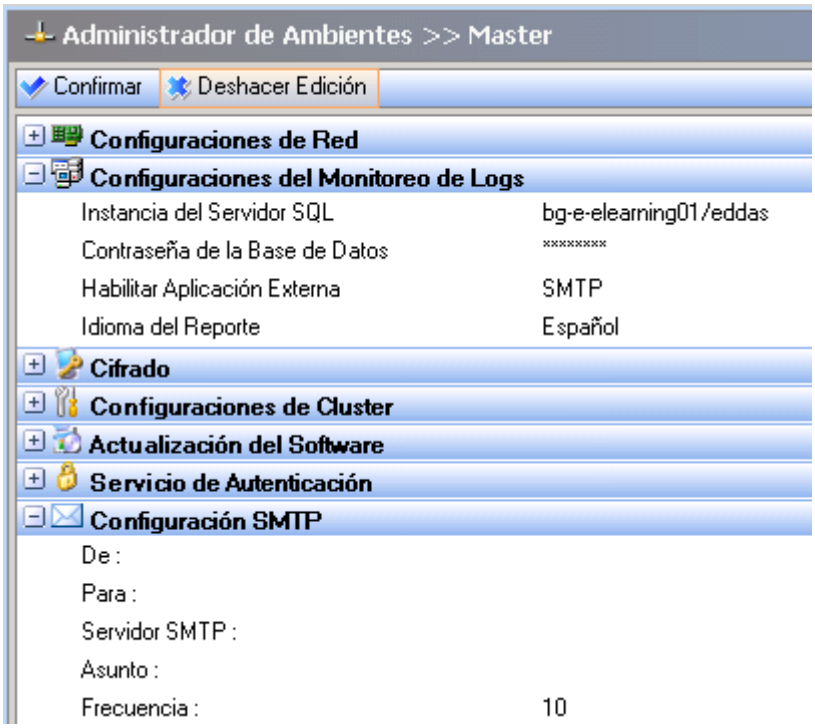


- Usted puede activar bien sea Sylog o SMTP para enviar Logs, pero no ambos. Dependiendo de su selección, la configuración correspondiente se mostrará en el Administrador de ambientes (panel de configuración de Syslog o de SMTP)

EXPORTANDO LOGS VÍA SMTP

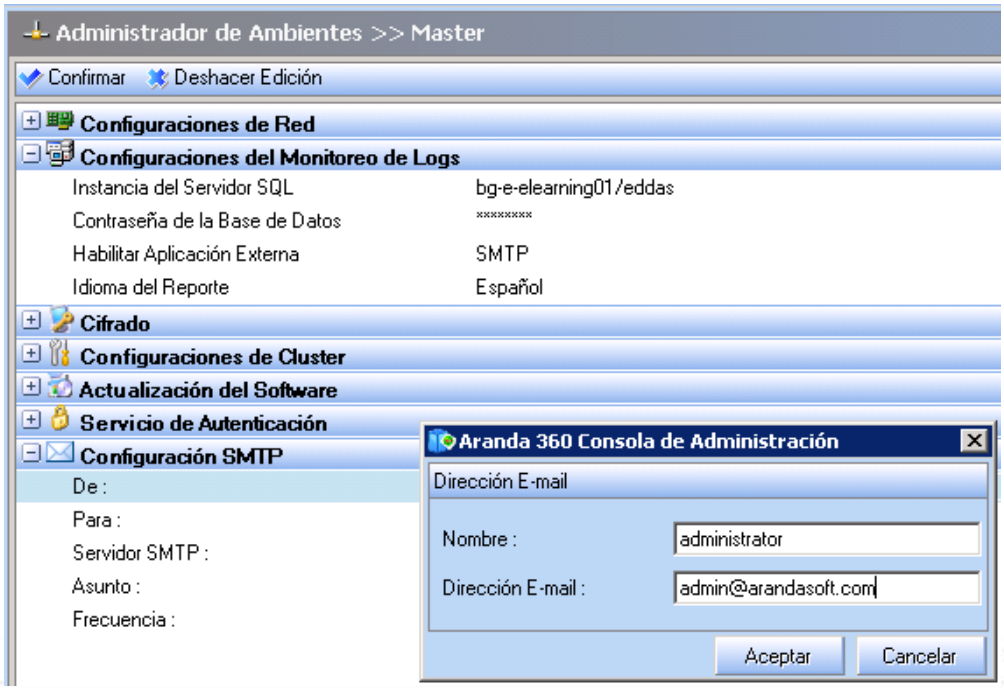
Para exportar Logs a través de SMTP, siga estos pasos:

1. Seleccione SMTP en la opción aplicación externa usada para generar reportes. La ventana de configuración de SMTP se aparecerá:

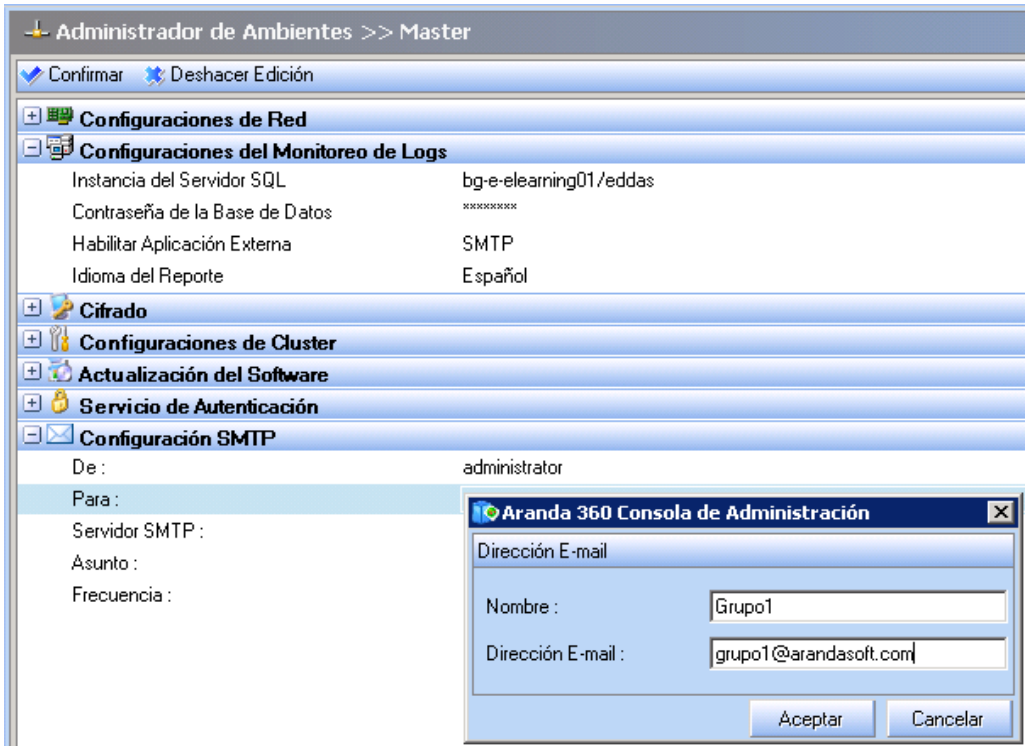


2. Definir la configuración de redirección SMTP en el panel de configuración de SMTP:

o Haga clic en “de”, como remitente del correo
Introduzca el nombre y la dirección del correo electrónico.

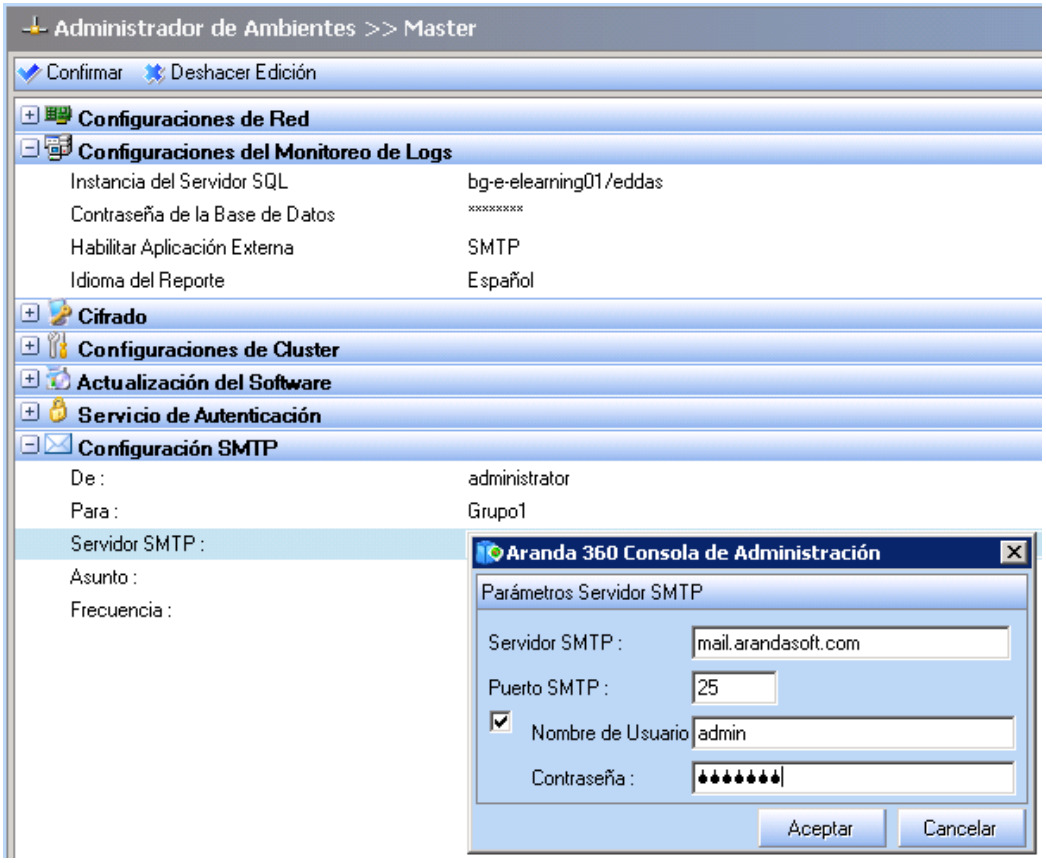


- Haga clic en “para”, como destinatario del correo
  Introduzca el nombre y la dirección del correo electrónico.

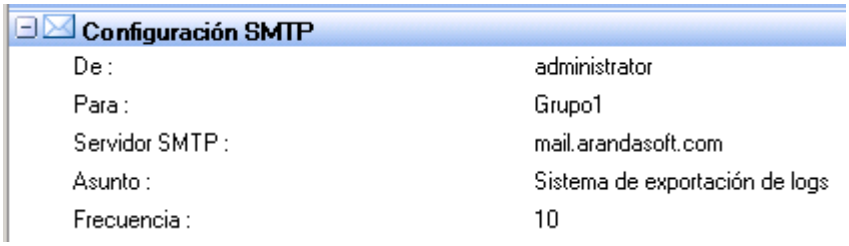


- Haga clic en “servidor SMTP”
  Introduzca el servidor SMTP y el puerto

Si desea utilizar un nombre de usuario y una contraseña, active la casilla de inicio e introduzca la información adecuada.



- Introduzca el número de Logs que se enviará por mensaje.



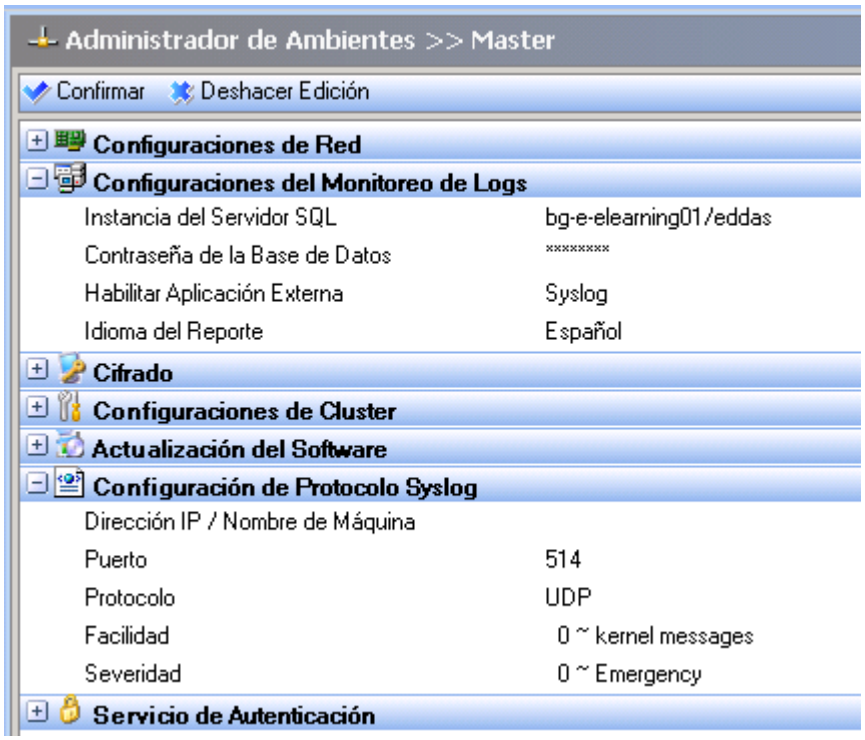
3. Verifique sus modificaciones.

- Utilice esta característica solo para enviar pocos logs y que sean específicos

EXPORTANDO LOGS VÍA SYSLOG

Para exportar Logs a través de Syslog, siga estos pasos:

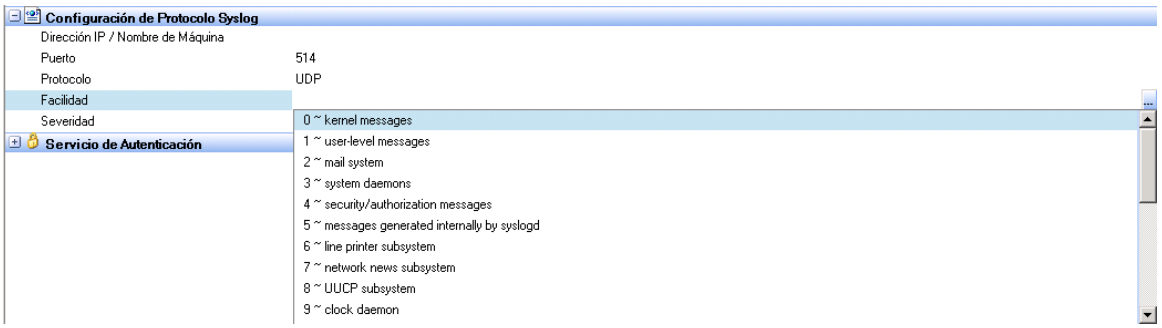
1. Seleccione Syslog en la opción aplicación externa usada para generar reportes. La ventana de configuración de Syslog aparecerá:



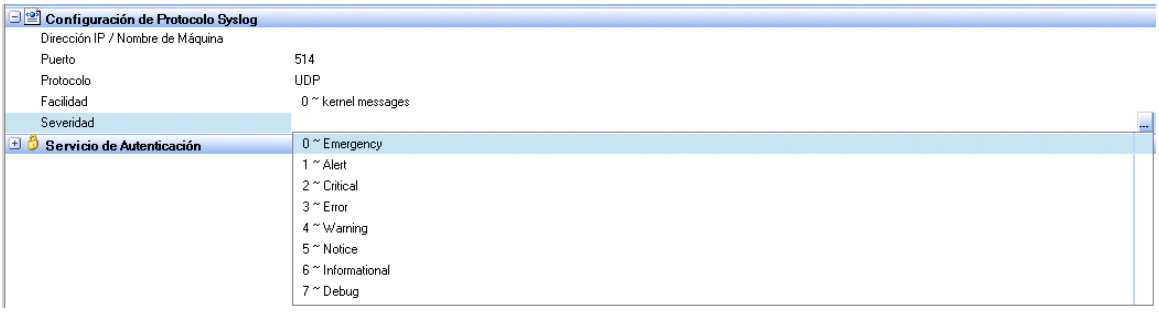
2. Definir la configuración de redirección del registro del sistema en el panel de configuración de syslog:

   - En el campo Dirección / Nombre del host, escriba la dirección IP del servidor Syslog.
   - En el campo de Puerto, cambie el número de puerto (si es necesario).
   - En el campo de Protocolo, introduzca el protocolo requerido (TCP o UDP).

- Seleccione el nivel de complejidad del mensaje



- Seleccione el nivel de severidad



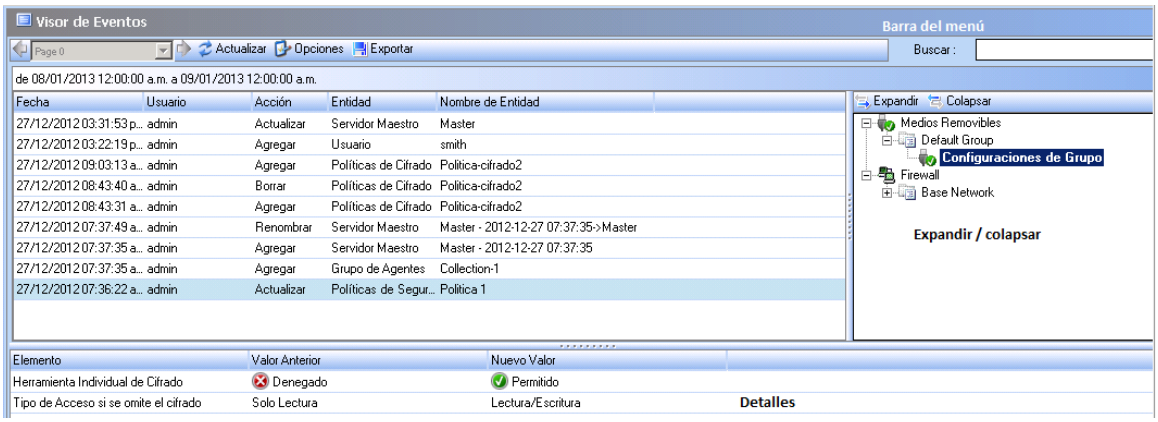
3. Verificar sus modificaciones

- Utilice esta característica para enviar algunos Logs específicos

VISOR DE EVENTOS

Generalidades

Todas las acciones realizadas en la consola de administración de Aranda por un administrador pueden ser registradas en logs disponibles desde el visor de eventos.



Las acciones del administrador que se registran en el visor de eventos son las siguientes:

- Directivas:
  - Adicionar
  - Eliminar
  - Renombrar
  - Modificar

- Grupos de agentes:
  - Adicionar
  - Eliminar
  - Renombrar
  - Modificar

- Configuraciones:
  - Adicionar
  - Eliminar
  - Renombrar
  - Modificar

- Scripts (Acción, prueba, procesos por lotes, etc.):
  - Adicionar
  - Eliminar
  - Renombrar
  - Modificar
- Adicionar un ambiente
- Enviar una política o configuración al servidor

- Crear un inicio de sesión para el administrador
- Cambiar la contraseña del administrador
- Etc.

INTERFAZ GRÁFICA

La interfaz grafica incluye cuatro aéreas:

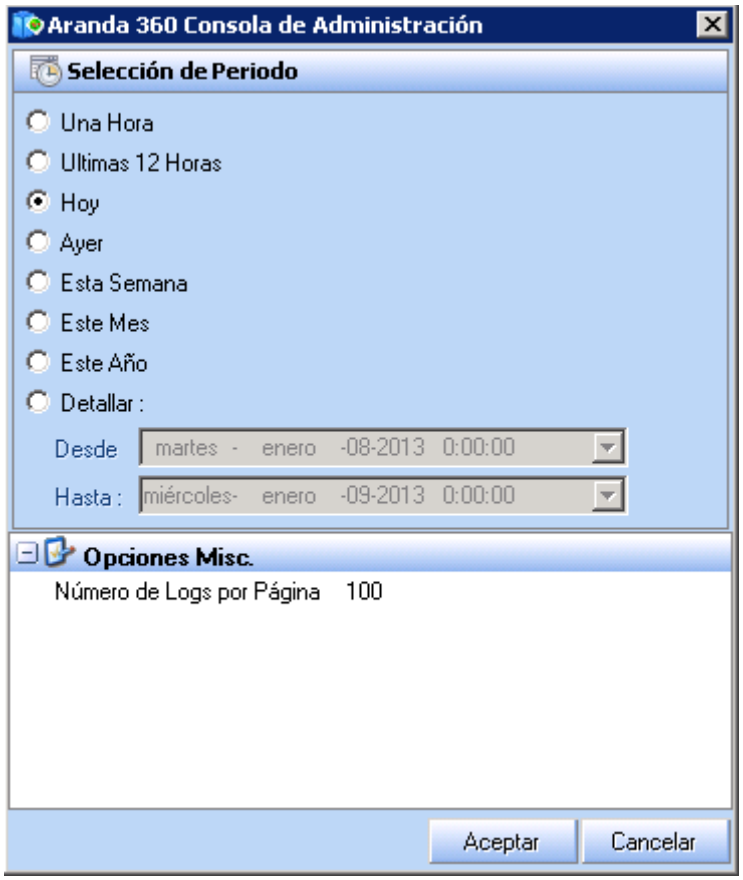
- El menú.
- Las columnas.
- El panel de Expandir / Contraer
- El panel de detalles

Menú

El menú incluye los siguientes comandos:

- Actualizar:
  Actualiza la visualización de las acciones del administrador, que se registran en el registro de Visor.

- Opciones:
  Define las opciones de visualización.



- Selección de Periodo de tiempo:
  Especifica el período de tiempo que se utiliza para mostrar los datos en el modo Revisión.

- Opciones adicionales:
  Especifica el número de registros que se mostrarán por página.

- Exportación:
  Se utiliza para guardar la información en un archivo en formato XML.

- Buscar:
  Para listas largas, puede utilizar el campo de búsqueda para localizar rápidamente el evento.

Columnas

La información contenida en la columna "Visor de sucesos" muestra la siguiente información:

- Fecha:
  Fecha y tiempo de las acciones del administrador

- Nombre del usuario:
  Nombre del administrador

- Acción:
  Tipo de acción del administrador que se registra en el Visor de sucesos. Aquí están algunos ejemplos de las acciones del administrador:

  - Sincronizar
  - Actualizar
  - Adicionar
  - Etc.

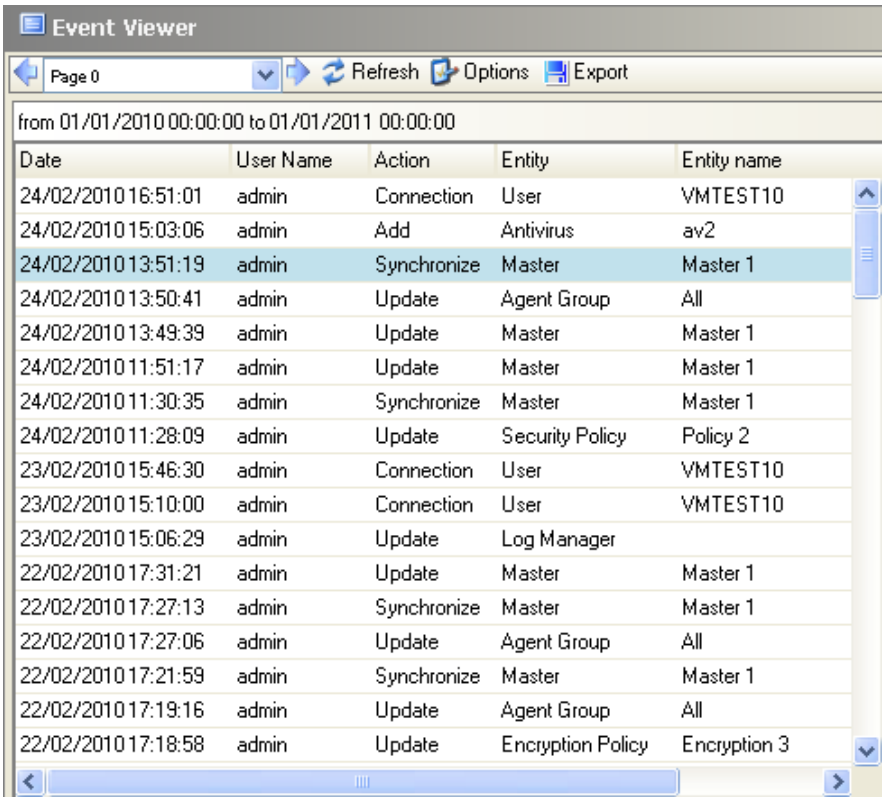
- Entidad:
  Elemento asociado con las acciones de reporte del administrador. Aquí están algunos ejemplos de entidades:

  - Políticas de seguridad
  - Políticas de cifrado
  - Antivirus.
  - Configuración
  - Script.
  - Grupo de agentes.
  - Servidor principal.

- Etc.

- Nombre de la entidad:
  Esta columna contiene información sobre los reportes de acciones del administrador.
  Ejemplo:
  08/01/201011:31:37||admin||Sincronización||Servidor principal||Principal 1

La columna especifica el nombre del servidor principal [Principal 1].



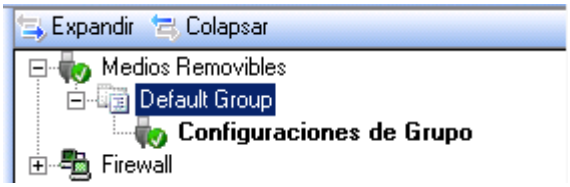
Date	User Name	Action	Entity	Entity name
24/02/2010 16:51:01	admin	Connection	User	VMTEST10
24/02/2010 15:03:06	admin	Add	Antivirus	av2
24/02/2010 13:51:19	admin	Synchronize	Master	Master 1
24/02/2010 13:50:41	admin	Update	Agent Group	All
24/02/2010 13:49:39	admin	Update	Master	Master 1
24/02/2010 11:51:17	admin	Update	Master	Master 1
24/02/2010 11:30:35	admin	Synchronize	Master	Master 1
24/02/2010 11:28:09	admin	Update	Security Policy	Policy 2
23/02/2010 15:46:30	admin	Connection	User	VMTEST10
23/02/2010 15:10:00	admin	Connection	User	VMTEST10
23/02/2010 15:06:29	admin	Update	Log Manager	
22/02/2010 17:31:21	admin	Update	Master	Master 1
22/02/2010 17:27:13	admin	Synchronize	Master	Master 1
22/02/2010 17:27:06	admin	Update	Agent Group	All
22/02/2010 17:21:59	admin	Synchronize	Master	Master 1
22/02/2010 17:19:16	admin	Update	Agent Group	All
22/02/2010 17:18:58	admin	Update	Encryption Policy	Encryption 3

Expandir/Contraer

La columna especifica el nombre del servidor principal [Principal 1].

El panel de Expandir / Contraer muestran una estructura de árbol actualizada con las acciones del administrador

Para mostrar un mayor nivel de detalles de la consola, haga clic en el nivel apropiado en el panel de Expandir / Contraer, por ejemplo: Parámetros de grupo



Clic para expandir la estructura de árbol

Clic para colapsar la estructura de árbol.

Detalles

Después de hacer clic en el nivel adecuado en el panel Expandir / Contraer, el panel de detalles mostrará información adicional (valor anterior y nuevo valor) en la acción del administrador actualizada

Ejemplo:

Aquí está el panel de detalles después de hacer clic en el grupo de parámetros en el panel de Expandir / Contraer.

Element	Old Value	New Value
Stand-alone decryption tool (SURT)		

Capítulo16 -LOGS Y ALERTAS

ACERCA DE ESTE CAPÍTULO

Este capítulo describe los Logs y sus interfaces gráficas. Este incluye lo siguiente:

- Generalidades
- Información en los Logs del agente
  - Logs de Software
  - Logs del sistema
  - Logs de la red
  - Logs de dispositivo
- Logs del servidor certificados.

GENERALIDADES

Los datos del log son recolectados por el agente de Aranda 360 en la estación de trabajo del cliente y almacenados localmente.

El camino seguido por la información utilizada para generar informes se describe a continuación:

1. Los Logs son enviado por los agentes al servidor de Aranda 360
2. El servidor envía sus logs a la base de datos SQL Aranda 360 .
3. Los Logs se muestran en la consola del administrador de Aranda

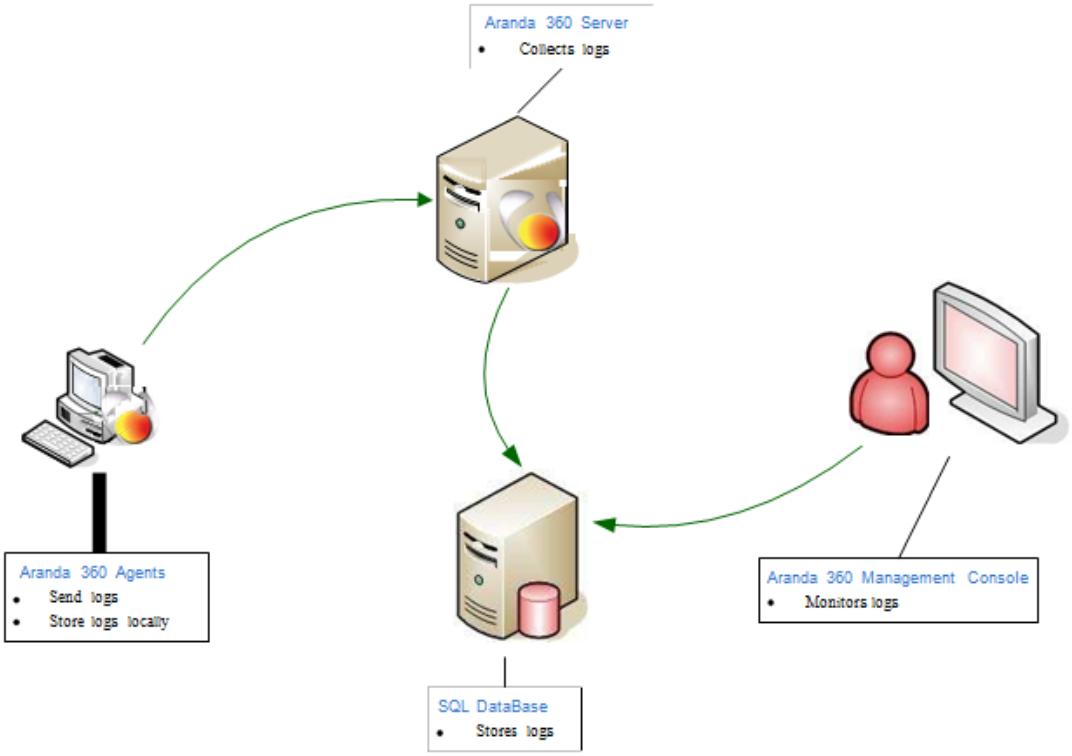


Fig. 17.1: Ruta del log de Aranda 360

LOGS DEL AGENTE

Logs de software

Localización

La información sobre la actividad del agente y el estado se almacena en un archivo de registro cuya ruta es:

[Archivos de programa]\Aranda\Aranda 360Agente\log\software.sro

Variables

Cada variable del log del software puede asumir los siguientes valores:

VARIABLE	DESCRIPCION
TIMESTAMP	Formato de fecha: Tue Apr 20 11:22:15 2010
ACCION	ERROR INFO WARN
ESTADO	
TIPO	AGENTE SERVIDOR
NOMBRE MOD	Nombre del modulo
LOG	Mensaje de información
ID USUARIO	Identificación del usuario

Tabla 17.1: Variables del log del software

Correspondencia entre variables y consola

Cada variable de registro se muestra en la consola de la siguiente manera:

VARIABLE	CONSOLA DE VISUALIZACIÓN
TIMESTAMP	Fecha
ACCION	Acción
ESTADO	Estado
TIPO	Tipo
NOMBRE MOD	Nombre Modo
LOG	Log

Tabla 17.2: Relación entre variables del log de software y la consola

Detalles

Cada variable de Log está asociada con una palabra clave cuyo significado se da en la tabla siguiente:

VARIABLE	PALABRA CLAVE	DESCRIPCION
TIMESTAMP	20/01/2010 11:16:30	Formato de fecha
ACTION	ERROR	Bloqueo
	INFO	Auditoria
	WARN	Modo de advertencia
STATUS	ACTION-FAILED	Una acción en el proceso por lotes que se encuentra en curso ha devuelto un error
	ACTION-MISSING	Motor de procesos por lotes no interpreta la acción
	AGENT-IN	Agente conectado
	AGENT-OUT	Agente discontinuado
	AGENT-START	Agente iniciado
	AGENT-STOP	Agente detenido
	AV_CORRUPTED	Instalación del antivirus corrupta El agente ha instalado el antivirus, pero falta una clave de registro que demuestra que el antivirus ha sido instalado
	AV_SCAN_FINISHED	Fin del escaneo del antivirus
	AV_SCAN_INTERRUPTED	Escaneo de antivirus interrumpido

Tabla 17.3: Detalles de las Variables del log del software (hoja 1 de 7)

VARIABLE	PALABRA CLAVE	DESCRIPCION
	AV_SCAN_START	Escaneo de antivirus iniciado
	BAN-HOST	Un HOST es prohibido en el servidor de Aranda 360 porque el certificado es utilizado por otras máquinas conectadas
	BATCH-LOG	Mensaje
	CGI-DENIED	El servidor de certificados deniega la solicitud del agente a descargar la solicitud de descarga
	CGI-ERROR	Error al descargar el certificado
	CGI-INVALID	Error al descargar el certificado
	CGI-SLEEP	El servidor de certificados está en modo inactivo y no se puede descargar certificados
	CHALLENGE_INVALID_VALUE	Una Acción o duración invalida
	CHALLENGE-FAILED	El servidor Aranda 360 falla al enviar una señal a un agente conectado porque la señal clave del agente es obsoleta
	CHECK-FAILED	Una prueba en el proceso por lotes es retornada como FALSA
	CHECK-MISSING	El motor de procesos por lotes no interpreta la prueba
	CIPHER_CONF	La Política de cifrado ha sido leída
	CIPHER_NEED_RECOVERY	El cifrado de archivos se ha desactivado. La recuperación manual es necesaria
	COM-ERROR	Un error de comunicación interna
	COM-EXT	Un elemento externo ha generado un mensaje en el log de Aranda 360.
	CONF_APPLY	aplicación de la configuración o política de seguridad en el agente
	CPU_CONTROL	Se ha producido una sobrecarga del CUP en el servidor
	CUSTOMACTION_1	El proceso por lotes 1 ha sido ejecutado
	CUSTOMACTION_2	El proceso por lotes 2 ha sido ejecutado
	CUSTOMACTION_3	El proceso por lotes 3 ha sido ejecutado
	CUSTOMACTION_4	El proceso por lotes 4 ha sido ejecutado
	CUSTOMACTION_5	El proceso por lotes 5 ha sido ejecutado
	CUSTOMACTION_ALLOWDRIVER	La acción instalación de controladores ha sido ejecutada
	CUSTOMACTION_AVDAMIN	La acción control de antivirus ha sido ejecutada
	CUSTOMACTION_NEPGUESTACCOUNT	La acción crear cuenta de invitados ha sido ejecutada
	CUSTOMACTION_STANDBY	La acción desactivar protección ha sido ejecutada

Tabla 17.3: Detalles de las Variables del log del software (hoja 2 de 7)

VARIABLE	PALABRA CLAVE	DESCRIPCION
	CUSTOMACTION_STOP	Solicitud desactivar protección/ detención complete ejecutada
	CUSTOMACTION_UNINSTALL	Solicitud desinstalar agente en % segundos ejecutada
	DB_ERROR	Error interno de comunicación con la base de datos
	DRIVER_ERROR	Agente no conectado con el controlador
	FILE_NOT_FOUND	Archivo no puede ser encontrado
	FLOOD_DETECTED	Repetición de registros en el Log y finalmente borrado
	GET_KCM	Intento de recuperar claves de recuperación negadas por el servidor
	GET_PATCH	La ruta de descarga falla porque el espacio del disco disponible es insuficiente
	HOTSPOT_START	Periodo temporal de acceso a la web Duración del acceso mostrado en segundos
	HOTSPOT_STOP	Fin del periodo de acceso a la web temporal
	INCORRECT_DATA	La configuración mínima del archivo presente en Apache es incorrecta
	INTERNAL_ERROR	Error interno (mensaje)
	INVALID_BATCH_PARAM	La prueba o acción en el proceso por lote incluye un número incorrecto de parámetros en su entrada
	KRM_GEN	El agente ha generado un único identificador
	KU_GEN	Las claves de cifrado han sido asignado al usuario que las ha descargado
	LICENCE	Se generan los Logs si el número de agentes conectados a los servidores supera el umbral de licencia.
	LOKI_POLICY_CHANGE	El estado de protección del núcleo ha cambiado
	LOKI_SET_CHALLENGE	Error cuando se ajusta el número de reinicios para la instalación del controlador
	MIGRATION_END	Fin de la migración de los archivos claves para la base de datos.
	MIGRATION_ERROR	Falla la migración de los archivos claves para la base de datos
	MIGRATION_START	A partir de la migración de archivos clave para la base de datos

Tabla 17.3: Detalles de las Variables del log del software (hoja 3 de 7)

VARIABLE	PALABRA CLAVE	DESCRIPCION
	NEP_GUEST_ACCOUNT	• Adicionar/eliminar una cuenta de invitado • Falla al crear/eliminar una cuenta de invitados
	NEP_INSTALL_BUSY	Falla el cambio de contraseña porque la configuración está siendo aplicada
	NEP_INSTALL_COM_FAILURE	Hay un error de comunicación cuando se aplica una configuración
	NEP_INSTALL_CONF_CANCELED	La aplicación de una configuración de cifrado ha sido cancelada
	NEP_INSTALL_DISK_FAILURE	Un error relacionado con el disco producido cuando se aplica la configuración
	NEP_INSTALL_INVALID_CONF	Hay una falla cuando se aplica la configuración. La configuración es invalida
	NEP_INSTALL_INVALID_DISK	Hay una falla cuando se aplica la configuración. El disco es invalido
	NEP_INSTALL_INVALID_SYSTEM	Hay una falla cuando se aplica la configuración. El sistema operativo es invalido
	NEP_INSTALL_REBOOT	Reinicie el equipo para completar la aplicación de política de cifrado de disco completo
	NEP_INSTALL_REGISTRY_FAILURE	Un error de registro basado ocurre cuando se aplica la configuración
	NEP_INSTALL_SHM_FAILURE	Un error de memoria compartida se produce cuando se aplica la configuración
	NEP_INSTALL_SIMU_FAILURE	Una simulación de error previene que la configuración comience ser aplicada
	NEP_INSTALL_SUCCESS	La aplicación exitosa de la configuración de cifrado de disco completo
	NEP_INSTALL_SYNC_FAILURE	Un error ocurre cuando se da la sincronización/desincronización del disco
	NEP_INSTALL_SYSTEM_FAILURE	Un error de sistema evita que la configuración se aplique
	NEP_INSTALL_UNKNOWN	Un error de sistema evita que la configuración se aplique
	NET-INT	La interface de red ha sido inicializada
	NEWCERT	Un nuevo certificado ha sido descargado
	NO_CONF	No hay configuración
	OBTAIN_FILE	El archivo no se puede conseguir porque el espacio disponible en el disco es insuficiente

Tabla 17.3: Detalles de las Variables del log del software (hoja 4 de 7)

VARIABLE	PALABRA CLAVE	DESCRIPCION
	ODIN_ERROR_ACCES	El agente falla en el acceso al archivo para cifrar/descifrar
	OPTIM	• Los filtros de las reglas de red ocultan un rango inferior de reglas(las reglas ocultas remueven la velocidad de procesamiento) • Un filtro para una regla es idéntico a uno existente (al adicionar estas operaciones ese impacta la velocidad de procesamiento)
	PIPE_CALL_FROM_NAME	Error ocurrido al llamar una función
	POLICY_CHANGE	Una nueva política ha sido recibida. Reiniciar para aplicar la política
	PWD_CHG_NOT_APPLY	Hay una falla al cambiar la contraseña asignada para un usuario especifico
	RECOMMENDATION	Cada vez que cambia el estado de UAC (NAP o Juniper)
	RECOVER_PATH	Recuperación de una maquina o de un directorio usando el archivo de clave incluido en un repositorio de llaves Param1: [Directorio]/Param2: [Archivo]
	RECOVERY_COMPLETE	Recuperación exitosa
	RECOVERY_ERROR	Error interno durante la recuperación
	RECOVERY_FAILURE	Error de recuperación
	SEND_FAILED	• La transferencia de datos a un servidor fallo • La solicitud de envió de un agente fallo
	SERVER_VERSION	Muestra el número de versión del servidor
	SET_KEY	Muestra si la sincronización se ha realizado correctamente o no y el tiempo necesario para su realización
	SIG_ERROR	El archivo de recursos de perfiles no es accesible
	SSMON_SESSION_HANDLER	Error en el manejo de eventos de sesión
	SSMON_STORECAMODE_FAILURE	Error al guardar la información
	SSMON_STORECAMODE_INVALID	Dato invalido
	START	La conexión de este modulo con el controlador fue exitosa
	STOP	Este modulo fue detenido satisfactoriamente
	STOPAGENTDENIED	La acción “detener agente” fallo
	STOPAGENTEXE	El agente fue detenido por stopagent.exe

Tabla 17.3: Detalles de las Variables del log del software (hoja 5 de 7)

VARIABLE	PALABRA CLAVE	DESCRIPCION
	SYNC_DIR	Se produjo un error al sincronizar / de sincronizar un directorio
	UAC	Cambio de estado UAC (NAP/Juniper)
	UNSET_KEY	Las llaves han sido reiniciadas
	UPDATING	Una nueva ruta ha sido descargada sobre el agente
	USER_REVOKED	Autenticación de un usuario revocado
	WTS_SYNC	Error al crear el enlace para SID
TYPE	AGENT	Agente
	SERVER	Servidor
MODNAME	ALL	
	HEIMDALL	
	HEIMDALL/THOR	
	MODACTION	
	MODAUTH	
	MODAV	
	MODCERT	
	MODCOM	
	MODDB	
	MODENFORCEMENT	
	MODFLOOD	
	MODGETCONF	
	MODKEYGEN	
	MODLDAP	
	MODMULTI	
	MODNEP	
	MODRECOVERY	
	MODROOTCERT	
	MODTOKENROOT	
	MODUPDATE	
	ODIN	

Tabla 17.3: Detalles de las Variables del log del software (hoja 6 de 7)

VARIABLE	PALABRA CLAVE	DESCRIPCION
	SSMON	
	THOR	

Tabla 17.3: Detalles de las Variables del log del software (Hoja 7 de 7)

Logs del sistema

Localización

La información sobre la actividad del sistema y el estado se almacena en un archivo de registro cuya ruta es:

[Archivos de programa]\Aranda\Aranda 360Agente\log\heimdall.sro

Variables

Cada variable de registro del sistema puede asumir los siguientes valores:

VARIABLE	DESCRIPCION
TIMESTAMP	Formato de fecha: Tue Apr 20 11:22:15 2010
ACCION	Ver la tabla "DETALLES DE LAS VARIABLES DEL LOG DEL SISTEMA"

Tabla 17.4: Variables del log del sistema (hoja 1 de 3

VARIABLE	DESCRIPCION
ESTADO	[BLK] [BLKCREATE] [BLKEXECUTE] [EXT-BLK] [HEAP-BLK] [LIBC-BLK] [PROFIL-BLK] [RDONLY] [STACK-BLK] [WARN] Antivirus : [ABORTED] [BLOCKED] [CLEANED] [ERASED] [FILE_UNKNOWN] [IGNORED] [MOVED] [MOVED_QUARENTINE] [MSG_ATT_DELETED] [MSG_ATT_MOVED_QUARANTINE] [MSG_ERASED] [MSG_BLOCKED] [MSG_IGNORED] [MSG_MOVED] [MSG_MOVED_CUARENTINE] [MSG_MARKED] [MSG_MARKED_MOVED] [OVERWRITTEN] [RENAMED] [WEB_FILE_MOVED_QUARANTINE] [WEB_FILE_BLOCKED] [WEB_IGNORED] Para ver más información ver la tabla "DETALLES DE LAS VARIABLES DEL LOG DEL SISTEMA"
SOURCE	Fuente nombre del programa
DEST	Destino del programa/ nombre del archivo
OPCION	Opciones

Tabla 17.4: Variables del log del sistema (hoja 2 de 3)

VARIABLE	DESCRIPCION
USERID	ID del usuario
RID	Regla de un único ID

Tabla 17.4: Variables del log del sistema (hoja 3 de 3)

Correspondencia entre variables y consola

Cada variable de registro se muestra en la consola de la siguiente manera:

VARIABLE	CONSOLA DE VISUALIZACION
TIMESTAMP	Fecha
ACTION	Acción
STATUS	Estado
SOURCE	Fuente
DEST	Destino
OPTION	Opción
RID	RID

Tabla 17.5: Relación entre variables del log del sistema y la consola

Detalles

Cada variable de registro está asociada con una palabra clave cuyo significado se da en la siguiente tabla:

VARIABLE	PALABRA CLAVE	DESCRIPCION
TIMESTAMP	Tue Apr 20 11:22:15 2010	Formato de fecha
ACTION	ACCESS-REG	Acceso al registro
	ATTACH-PROCESS	Intente asociar un proceso
	AV	Información sobre virus
	BAD-KEY	La clave de descifrado utilizada para abrir el archivo no es válida

Tabla 17.6: Detalles de las variables del log del sistema (hoja 1 de 3)

VARIABLE	PALABRA CLAVE	DESCRIPCION
	BLOCKED-DRIVER	La descarga de controladores ha sido bloqueada Posibles valores de protección del núcleo en la opciones de la columna inferior del monitoreo DEL LOG> sistema: 1: El controlador está oculto 2: El controlador está conectado 3: El nombre del controlador a cambiado 4: El archivo de controlador no existe en el disco 5: El controlador es enganchado
	CHECKSUM	El Hash de la aplicación ha sido modificado
	COPY-PASTE	Un proceso que no está autorizado para COPIAR/PEGAR ha sido bloqueado
	CREATE	Abrir el archivo en modo crear
	DELETE	Intento de eliminar un archivo
	HOOK	Intento de realizar un enlace global
	HOOKED-DRIVER	Controlador conectado por otro controlador Para más detalles sobre los valores de protección del núcleo, consulte CONTROLADOR BLOQUEADO
	KEYLOG	Intento de registro de clave
	LOAD-DRIVER	Notificación de que un nuevo controlador se ha cargado Para más detalles sobre los valores de protección del núcleo, consulte CONTROLADOR BLOQUEADO
	LOAD-OBJECT	Carga de una DLL o uso de una memoria compartida
	LOCK-KEY	El acceso a los archivos cifrados con el proceso de lote se rechaza
	OPEN-PROCESS	Intento de abrir un proceso
	OPEN	Archivo de apertura
	OVERFLOW	Desbordamiento de memoria
	PROCESS-INFORMATION	Intentar acceder a la lista de procesos activos
	REBOOT	Intentar reiniciar el sistema
	RENAME	Intentar cambiar el nombre de un archivo
	SOCK-ACCEPT	Aceptación (socket en el servidor)
	SOCK-BIND	Enlazar (socket en el servidor)
	SOCK-CONNECT	Conexión (socket en el cliente)
	SOCK-ICMP	Creación de un socket ICMP

Tabla 17.6: Detalles de las variables del log del sistema (hoja 2 de 3)

VARIABLE	PALABRA CLAVE	DESCRIPCION
	SOCK-LISTEN	Escuchar (socket en el servidor)
	SOCK-RAWIP	Creación de un archivo raw o socket de UDP
	SU	Tratar de elevar los privilegios de procesos
	SUSPECT-DRIVER	Operación sospechosa realizada por el controlador Para más detalles sobre los valores de protección del núcleo, consulte CONTROLADOR BLOQUEADO
	TERMINATE-PROCESS	El proceso se ha terminado (principalmente debido a sobrecarga del CPU)
	WRITE	Intento de escribir un archivo
STATUS	BLK	Bloqueado
	BLKCREATE	Bloqueado durante la creación
	BLKEXECUTE	Bloqueado durante la ejecución
	DYN-BLK	Bloqueado por una regla dinámica
	EXT-BLK	Bloqueado por una regla de extensión
	HEAP-BLK	Bloqueado debido al desbordamiento de pila
	LEVEL-BLK	Alerta y bloqueo por el nivel
	LIBC-BLK	Bloqueado por “ret-into-libc”
	PROFIL-BLK	Bloqueado por una desviación del perfil estándar
	RDONLY	Aplica acceso de sólo lectura
	STACK-BLK	Bloqueado por desbordamiento de pila
	WARN	Advertencia sin bloqueo
SOURCE		Nombre del proceso que desencadenó el evento
DEST		Ruta de ubicación del objeto
OPTION		• Socket (por defecto es valor es 0) • Identificador de referencia si el tipo de acción es HOOK o KEYLOG
RID		Regla de un único ID Observación: Puede hacer doble clic en la entrada del registro de RID para ir directamente a la regla.

Tabla 17.6: Detalles de las variables del log del sistema (hoja 3 de 3)

Logs de red

Localización

La información sobre la actividad de red se almacena en un archivo de registro cuya ruta es:

[Archivos de programa]\Aranda\Aranda 360Agente\log\thor.sro

Variables

Cada variable de Log puede asumir los siguientes valores:

VARIABLE	DESCRIPCION
TIMESTAMP	Formato de fecha Tue Apr 20 11:22:15 2010
ACTION	Para más información, ver tabla. “Detalles de las variables del Log de dispositivos”
STATUS	[INFO] [IN] [OUT] [CONNECTION_CLOSED] [IP_BLOCKED] [SCAN_IN] [SCAN_OUT] Para más información, ver tabla. “Detalles de las variables del Log de dispositivos”.
METADATA	Para más información, ver tabla. “Detalles de las variables del Log de dispositivos”
IP	• SSID (WiFi) • fragmento de IP • dirección de IP
PORTSRC	• Puerto de origen (TCP, UDP) • Canal (WiFi) • Tipo (ICMP)
PORTDST	Puerto de destino (TCP/UDP) Código (ICMP)
PROTO1	Protocolo para la Ethernet
PROTO2	Protocolo de IP

Tabla 17.7: Variables del log de red (hoja 1 de 2)

VARIABLE	DESCRIPCION
USERID	ID de usuario
RID	Regla para un único ID

Tabla 17.7: Variables del log de red (hoja 2 de 2)

Correspondencia entre variables y consola

Cada variable de registro se muestra en la consola de la siguiente manera:

VARIABLE	CONSOLA DE VISUALIZACION
TIMESTAMP	Fecha
ACTION	Acción
STATUS	Estado
TYPE	Tipo
MODNAME	Nombre Modulo
LOG	Log

Tabla 17.8: Relación entre variables del log de red y la consola

Detalles

Cada variable de Log está asociada con una palabra clave cuyo significado se da en la siguiente tabla:

VARIABLE	PALABRA CLAVE	DESCRIPCION
TIMESTAMP	Tue Apr 20 11 :22 :15 2010	Fecha
ACTION	ARP_ATTACKING 0x21	Intento de robo de identidad detectado en una Dirección IP en la red. Paquete de comandos.
	ARP_BLOCK 0x1	ARP con estado de error (respuesta sin solicitud) o desbordamiento de ARP_POISON
	ARP_DELETE 0x5	La entrada asociada con la dirección IP ha sido eliminada del cache Windows ARP. Paquete bloqueado después de enviar una solicitud gratuita (IDS establecida en Alto o Crítico).

Tabla 17.9: Detalles de las variables del log de red (hoja 1 de 3)

VARIABLE	PALABRA CLAVE	DESCRIPCION
	ARP_POISON 0x45	Intento de envenenamiento del ARP cache detectado Paquete bloqueado Entrada asociada con dirección IP sospechosa ha sido eliminada del Cache de Windows ARP
	ARP_POISON 0x49	Intento de envenenamiento del ARP cache detectado Caché ARP de Windows se ha actualizado desde la entrada anterior.
	ARP_SPOOF 0x112	Intento de robo de identidad detectado en la dirección IP Paquete bloqueado Protección de red (IDS establecida como crítica).
	ARP_SPOOF 0x12	Intento de robo de identidad detectado en la dirección IP Paquete bloqueado
	FLOOD	Registro de entrada repetida
	FW_ICMP	Una regla aplicada a un mensaje ICMP (METADATA, PROTO1, IP, PROTO2, PORTSRC y PORTDST) son variables llenadas
	FW_IP	Una regla aplicada a la dirección IP (METADATA, PROTO1, IP y PROTO2) son variables llenadas
	FW_MAC	Una regla aplicada a la dirección MAC (solo METADATA Y PROTO1) son variables llenadas. La dirección MAC (Dirección hardware de la tarjeta de red) indicada en la columna sigue siendo la misma que la dirección de la máquina a distancia desde su dirección local
	FW_PORT	Una regla aplicada al filtrado de puertos METADATA, PROTO1, IP, PROTO2, PORTSRC y PORTDST variables son llenadas
	PORTSCAN	Escaneo de puertos detectados
	STATEFUL_STATUS	La variable PROTO1 indica el código de estado de estado del paquete previamente bloqueado
STATUS	CONNECTION_CLOSED	Una o varias conexiones han sido cerradas debido a que son demasiado lentas
	IN	Filtrando el trafico que entra
	IP_BLOCKED	Dirección IP sospechosa causando bloqueo de desbordamientos
	OUT	Filtrando el trafico que sale

Tabla 17.9: Detalles de las variables del log de red (hoja 2 de 3)

VARIABLE	PALABRA CLAVE	DESCRIPCION
	SCAN_IN	Escaneo de puertos entrantes detectados
	SCAN_OUT	Escaneo de puertos salientes detectado
IP	IP	Dirección IP
METADATA		• En el caso de un desbordamiento, indica el número de ocurrencias del evento. • De lo contrario, indica las direcciones MAC.
PORTDST		numero de puerto de Destino
PORTSRC		Fuente del número de puerto
PROTO1: PROTO2		• Los protocolos están siendo filtrados
RID		Regla para un único ID

Tabla 17.9: Detalles de las variables del log de red (hoja 3 de 3)

Logs de dispositivos

Los Logs de dispositivo contienen información sobre los dispositivos extraíbles y la actividad WiFi

Localización

Información sobre el dispositivo extraíble y actividad WiFi se almacena en un archivo de registro, cuya ruta es:

[Archivos de programa]\Aranda\Aranda 360\Agente\device.sro

Variables

Cada variable del Log del dispositivo pueden asumir los siguientes valores:

VARIABLE	DESCRIPCION
TIMESTAMP	Formato de fecha Tue Apr 20 11:22:15 2010
ACTION	Ver "Detalles de las variables del Log de dispositivos"
STATUS	Posibles estados son: [BLK] [INFO] [WARN]
SOURCE	Nombre de tarjeta de red (WiFi) Nombre del proceso (dispositivo de almacenamiento masivo)
DEST1	Nombre del archivo (dispositivo de almacenamiento masivo) Dirección MAC (WiFi)
DEST2	Nombre del archivo después de renombrarlo (dispositivo de almacenamiento masivo) SSID (WiFi)
SIZE	Dispositivo de tamaño
TYPE	Posibles dispositivos de tamaño son: [FIREWIRE] [NETWORK] [PCMCIA] [USB]

Tabla 17.10: Variables del log de dispositivos (hoja 1 de 2)

VARIABLE	DESCRIPCION
CLASSID	Las posibles clases son: [BLUETOOTH] [CDROM] [DISK] [IRDA] [MODEM] [PARALLEL] [PCMCIA] [SERIAL] [USB_ACTIVE_SYNC] [USB_APPLICATION_SPECIFIC] [USB_AUDIO] [USB_CDCDATA] [USB_COMMUNICATION] [USB_CONTENT_SECURITY] [USB_DIAGNOSTIC] [USB_HID] [USB_HUB] [USB_IMAGING] [USB_MISCELLANEOUS] [USB_PALM_SYNC] [USB_PHYSICAL] [USB_PRINTER] [USB_SMARTCARD] [USB_STORAGE] [USB_VENDOR_SPECIFIC] [USB_VIDEO] [USB_WIRELESS_CONTROLLER] [WIFI]
VENDORID	ID del vendedor
PRODUCTID	ID del producto
SERIALID	ID del serial
VENDORNAME	Nombre del vendedor
PRODUCTNAME	Nombre del producto
USERID	ID del usuario
ENROLLMENTSTATE	Inscripción de estado
OWNERNAME	Propietario del dispositivo registrado
RID	Regla para un único ID

Tabla 17.10: Variables del log de dispositivos (hoja 2 de 2)

Correspondencia entre variables y consola

Cada variable de logs se muestra en la consola de la siguiente manera:

VARIABLE	CONSOLA DE VISUALIZACION
TIMESTAMP	Fecha
ACTION	Acción
STATUS	Estado
SOURCE	Fuente
DEST1	Destino
DEST2	Destino 2
SIZE	Tamaño
TYPE	Tipo
CLASSID	Clase
USERNAME	Nombre del usuario que usa la máquina cuando se produjo el bloqueo
RID	Regla para un único ID

Tabla 17.11: Relación entre variables del log de dispositivos y la consola

Detalles

Variables del log de dispositivos

Cada variable de log está asociada con una palabra clave cuyo significado se encuentra en la siguiente Tabla:

VARIABLE	PALABRA CLAVE	DESCRIPCION
TIMESTAMP		Formato de fecha: Tue Apr 20 11:22:15 2010
ACTION	AP_ACL	Regla de filtrado ACL para el punto de acceso (Estado: WARN)
	AP_ADHOC	Punto de acceso en modo adhoc (Estado: WARN)
	AP_INSECURE	Punto de acceso sin garantía (Estado: WARN)
	AP_WIFI	Punto de acceso WiFi activado / desactivado (Estado: WARN)
	BAD_UNPLUG	USB incorrectamente eliminada
	BLUETOOTH	Dispositivo Bluetooth bloqueado
	CD	Proceso de lectura de CD bloqueado

Tabla 17.12: Detalles de las variables del log de dispositivos (hoja 1 de 4)

VARIABLE	PALABRA CLAVE	DESCRIPCION
	CDWRITER	Proceso de grabación del CD bloqueado
	DEVICE_UNPLUG	Conexión de dispositivos externos
	DEVICE_PLUG	Conexión de dispositivos internos
	FILE_CREATE	Archivos creados (Estado: INFO)
	FILE_DELETE	Archivo borrado en el dispositivo extraíble (Estado: INFO).
	FILE_OPEN	Archivo abierto en el dispositivo extraíble (Estado: BLK o WARN)
	FILE_OVERWRITE	Archivo sobrescrito en el dispositivo extraíble (Estado: INFO)
	FILE_READ	Lectura de datos en el dispositivo extraíble (Estado: INFO)
	FILE_RENAME	Archivo renombrado en el dispositivo extraíble (Estado: BLK o WARN)
	FILE_WOPEN	Archivo abierto para sobrescribir la operación en el dispositivo extraíble (Estado: BLK o WARN)
	FILE_WRITE	Datos escritos en un archivo en el dispositivo extraíble (Estado: INFO)
	IRDA	Dispositivo mediante el puerto de infrarrojos bloqueado
	MODEM	Modem bloqueado
	PARALLEL	Dispositivo conectado al puerto paralelo bloqueado
	PCMCIA	Dispositivo PCMCIA bloqueado
	SERIAL	Dispositivo conectado al puerto serial bloqueado
	USB_CLASSID	Clase ID del dispositivo extraíble (en el campo de estado)
	VOLUME_DISMOUNT	Dispositivo extraíble desconectado (Estado: INFO)
	VOLUME_MOUNT	Dispositivo extraíble conectado (Estado: INFO)
	VOLUME_DENIED	El acceso al dispositivo está prohibido. Generado si una regla especifica un filtro en la inscripción del estado (Estado : INFO)
	VOLUME_READONLY	El acceso al dispositivo es de sólo lectura. Generado si una regla especifica un filtro en la inscripción del estado (Estado : INFO)
	VOLUME_READWRITE	El acceso al dispositivo es autorizado. Generado si una regla especifica un filtro en la inscripción del estado (Estado: INFO)
STATUS	BLK	Bloqueado
	INFO	Auditado

Tabla 17.12: Detalles de las variables del log de dispositivos (hoja 2 de 4)

VARIABLE	PALABRA CLAVE	DESCRIPCION
	WARN	Modo de alerta
SOURCE		Nombre de la tarjeta de red (WiFi) Nombre del proceso (dispositivo de almacenamiento masivo extraíble)
DEST1		Nombre del archivo
DEST2		Nombre de archivo después de renombrarlo (dispositivo extraíble de almacenamiento masivo) SSID (WiFi)
SIZE		Tamaño del dispositivo o modificación
TYPE	FIREWIRE NETWORK PCMCIA USB	Ver "Tipo de variable".
ClassID	BLUETOOTH CDROM DISK IRDA MODEM PARALLEL PCMCIA SERIAL USB_ACTIVE_SYNC USB_APPLICATION_SPECIFIC USB_AUDIO USB_CDCDATA USB_COMMUNICATION USB_CONTENT_SECURITY USB_DIAGNOSTIC USB_HID USB_HUB USB_IMAGING USB_MISCELLANEOUS USB_PALM_SYNC USB_PHYSICAL USB_PRINTER USB_SMARTCARD USB_STORAGE USB_VENDOR_SPECIFIC USB_VIDEO USB_WIRELESS_CONTROLLER WIFI	Ver "Variables de clase ID".

Tabla 17.12: Detalles de las variables del log de dispositivos (hoja 3 de 4)

VARIABLE	PALABRA CLAVE	DESCRIPCION
ENROLLMENT STATE	UNENROLLED UNENROLLED_CORRUPT_ENROLL UNENROLLED_CORRUPT_FOO TPRINT ENROLLED ENROLLED_CONTENTCHANGED ENROLLED_NOTRUST TRUSTED	Remitirse a “variables de estado de Inscripción”.
OWNERNAME		

Tabla 17.12: Detalles de las variables del log de dispositivos (hoja 4 de 4)

WiFi variables

Cada variable WiFi puede asumir los siguientes valores:

VARIABLE	PALABRA CLAVE	DESCRIPCION
ACTION	AP_ACL	Punto de acceso con regla de filtrado ACL
	AP_ADHOC	Punto de acceso con modo adhoc
	AP_INSECURE	Punto de acceso sin garantía
	AP_WIFI	Punto de acceso WiFi activado / desactivado
STATUS	WARN	Modo de alerta
SOURCE		Nombre de la interfaz de red
DEST1		Punto de acceso a la dirección MAC
DEST2		Punto de acceso SSID
SIZE		Canal
TYPE		Red
CLASSID		WiFi
USERID		Mensaje de información
ID		ID del usuario

Tabla 17.13: Variables Wi-Fi

Tipo de variables

Cada tipo de variable puede tomar los siguientes valores:

VARIABLE	PROPOSITO
FIREWIRE	Acceso Firewire controlado y auditado
NETWORK	Control de acceso WiFi
PCMCIA	Acceso PCMCIA controlado y auditado
USB	Acceso USB controlado y auditado

Tabla 17.14: Tipo de variables

Variables Clase ID

Cada variable Clase ID puede asumir los siguientes valores:

VARIABLE	DESCRIPCION	PROPOSITO
CDROM	CD-ROM, DVD-ROM, lector Blu-Ray	Control de acceso, protección escrita
DISK	dispositivo extraíble de almacenamiento masivo	Control de acceso, Auditado
FLOPPY	Disquete	Heimdall
NETWORK	Red WiFi	Control de acceso
U3	memorias USB U3	Control de acceso
USB_AUDIO	Tarjeta de audio USB	Control de acceso
USB_HID	Dispositivo USB HID (teclado, ratón, Tableta gráfica, etc.)	Control de acceso
USB_IMAGING	Dispositivos de imágenes USB (webcam, escáner, etc.)	Control de acceso
USB_ACTIVE_SYNC	Dispositivo de almacenamiento masivo extraíble USB	Control de clase ID
USB_APPLICATION_SPECIFIC	Dispositivo clase USB_APPLICATION_SPECIFIC	Control de clase ID
USB_CDCDATA	Dispositivo clase USB_CDCDATA	Control de clase ID
USB_COMMUNICATION	Dispositivo clase USB_COMMUNICATION	Control de clase ID
USB_CONTENT_SECURITY	Dispositivo clase USB_CONTENT_SECURITY	Control de clase ID
USB_DIAGNOSTIC	Dispositivo clase USB_DIAGNOSTIC	Control de clase ID
USB_HUB	Dispositivo clase USB_HUB	Control de clase ID
USB_MISCELLANEOUS	Dispositivo clase USB_MISCELLANEOUS	Control de clase ID

Tabla 17.15: Variables de clase ID (hoja 1 de 2)

VARIABLE	DESCRIPCION	PROPOSITO
USB_PALM_SYNC	Dispositivo clase USB_PALM_SYNC	Control de clase ID
USB_PHYSICAL	Dispositivo clase USB_PHYSICAL	Control de clase ID
USB_PRINTER	impresora USB	Control de acceso
USB_SMARTCARD	Lector de tarjetas inteligentes USB	Control de clase ID
USB_STORAGE	Dispositivo de almacenamiento masivo extraíble USB	Control de clase ID
USB_VENDOR_SPECIFIC	Dispositivo clase USB_VENDOR_SPECIFIC	Control de clase ID
USB_VIDEO	Dispositivo clase USB_VIDEO	Control de clase ID
USB_WIRELESS_CONTROLLER	Dispositivo clase USB_WIRELESS_CONTROLLER	Control de clase ID
WIFI	Interfaz de red Wireless	WIFI (modap)

Tabla 17.15: Variables de clase ID (hoja 2 de 2)

Variables de estado de registro

Cada variable de estado de registro puede asumir los siguientes valores:

VARIABLE	DESCRIPCION	ACCION
UNENROLLED	El dispositivo no está inscrito	
UNENROLLED_CORRUPT_ENROLL	El archivo de estado de registro está dañado	Se considera que el dispositivo no está inscrito
UNENROLLED_CORRUPT_FOOTP RINT	El archivo huella está dañado	Se considera que el dispositivo no está inscrito
ENROLLED	El dispositivo está inscrito	
ENROLLED_CONTENTCHANGED	El dispositivo está inscrito pero su contenido ha cambiado fuera del perímetro	Se considera que el dispositivo no está inscrito
ENROLLED_NOTRUST	El dispositivo está registrado pero su estado de confianza no se podrá restaurar	Se considera que el dispositivo no está inscrito
TRUSTED	El dispositivo es de confianza	Estado de confianza es mantenido mientras el dispositivo realiza operaciones.

Tabla 17.16: variables de estado de registro

Tipo de alertas

Las alertas emitidas para los dispositivos extraíbles por el administrador de Logs son las siguientes:

- Mensajes cortos:
  Este es el mensaje que se puede leer en la lista de Logs en el equipo del agente al hacer clic en el icono del monitor Aranda 360 .
  Proceso bloqueado:%SOURCE%

- Mensajes largos:
  Este es el mensaje detallado que se podrá leer cuando seleccione el Log en el monitor de Aranda 360 en el agente del computador
  El acceso al dispositivo [DEVICE NAME] realizado por %SOURCE% ha sido bloqueado %BR%Por favor contacte al administrador para más información

- Mensaje de notificación:
  Este es el mensaje que se podrá leer en la ventana emergente del agente (si el campo este vacío, la ventana emergente no aparecerá).
  El acceso al dispositivo [DEVICE NAME] no está permitido en esta estación de trabajo.

- Mensaje externo:
  Este es el mensaje que se puede leer en el sistema de registro externo
  (Ejemplo: Syslog).
  El acceso al dispositivo [DEVICE NAME] realizado por %SOURCE% ha sido bloqueado

  Variables entre % se sustituyen por el nombre del recurso cuando se muestra en el agente.

LOGS DE CERTIFICADO DEL SERVIDOR

Información emitida por el certificado del servidor es almacenada en el archivo Log cuya ruta es la siguiente:

[Archivo de programa]\Aranda\Servidor Aranda 360\Apache\logs\cgi.log

Las entradas del Log caen dentro de las siguientes 3 categorías:

- Info
  - Info: RECUPERACION del certificado creado [IP]:
    Un certificado de recuperación ha sido solicitado por el host IP
  - Info: permiso denegado [ERRCODE] [IP]:
    La solicitud de certificado de descarga desde el host IP ha sido rechazada.
  - ERRCODE = e:
    Error interno.
  - ERRCODE = s:
    Fecha y hora actual no están comprendidas dentro del período de descarga del certificado
  - ERRCODE = d:
    El agente de origen no es válido (el agente ha sido descargado de otro servidor principal).
  - Info: Crear certificado [IP]:
    Un certificado se ha generado para la IP del Host
- Alerta
  - Alerta: Borrando el anterior cgi.lock:
    La eliminación del bloqueo de archivos ha sido obligada. Esto ocurre cuando el servidor no se cierra normalmente
- Error
  - Error: CGI está bloqueado. Salir de proceso:
    CGI no ha podido acceder al archivo de bloqueo durante 5 minutos. Se cancela la solicitud de certificado
  - Error: Archivo de configuración invalida. Error: No se pudo recuperar la dirección IP
    No es válido el archivo de configuración. El servidor fallo al recuperar la dirección IP del cliente Host

- Error: recuperación incorrecta de nombre de usuario/contraseña:
  El nombre de usuario y la contraseña establecidos en el formulario de solicitud de certificado de recuperación no son válidos.

- Error: falla al crear certificado de recuperación [IP]:
  Se produce un error interno mientras se utiliza el formulario de requisitos para el certificado de recuperación

- Error: No se han podido recuperar parámetros de petición [IP]:
  El servidor fallo al recuperar parámetros de la petición.

- Error: Creación de certificado fallida [IP]:
  Un error interno ocurrió