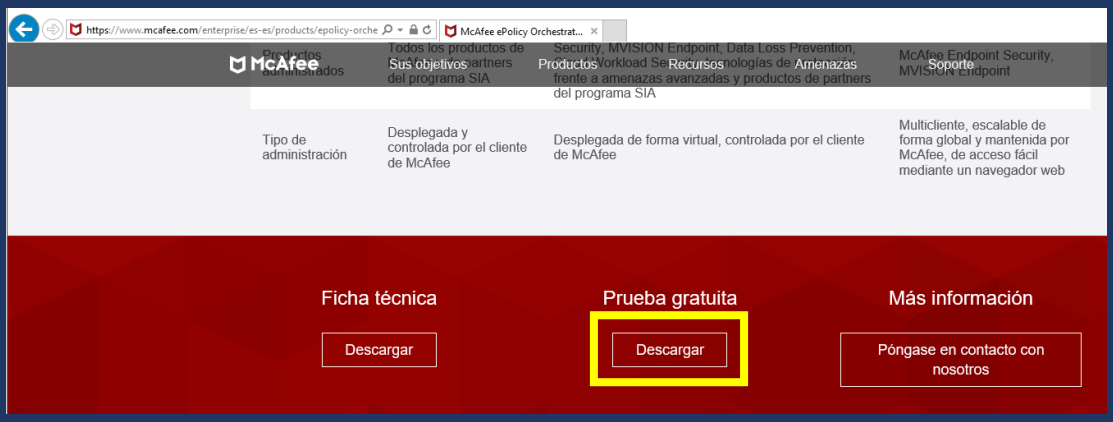
Presentación

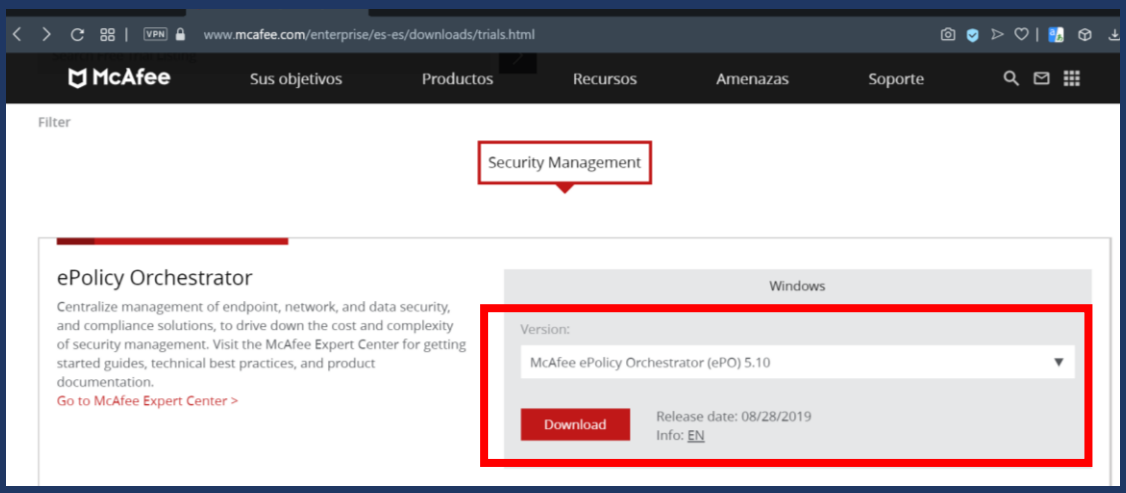
- **Nombre del estudiante:** Jamiel Santana.
- **Matricula:** 2019-8095
- Nombre del profesor: Geancarlos Sosa
- **Mat:** Seguridad de SO.
- **Tema:** Windows Server Update Service (WSUS).
- **Centro Educativo:** Instituto tecnológico de las Américas.

- **Instalar McAfee ePolicy Orchestrator en Windows Server 2016:**
  - Para iniciar con el proceso de descarga, ingresaremos a la página oficial **https://www.mcafee.com/enterprise/es-es/home.html nos iremos a la sección de productos.**

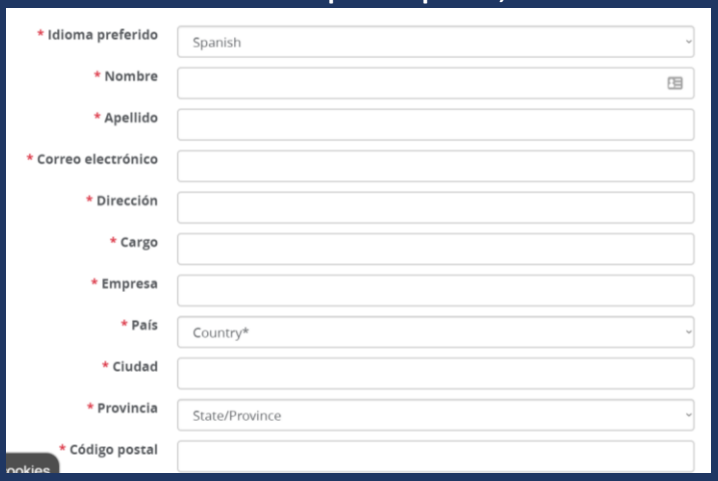
  - **Dentro de la sección, buscaremos el producto llamado ePolicy Orchestrator, daremos click sobre ella, buscaremos las opciones de más abajo donde nos aparece un botón para poder descargar un prueba gratuita del producto.**



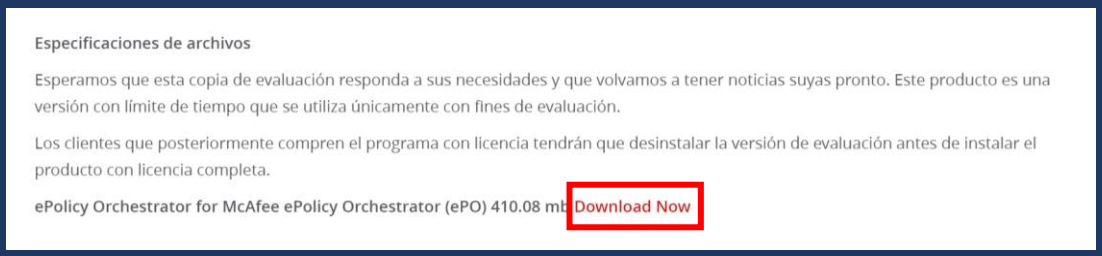
  - **Dado click en dicho botón, nos aparecerá para escoger la versión disponible del producto, junto con su botón de descarga.**



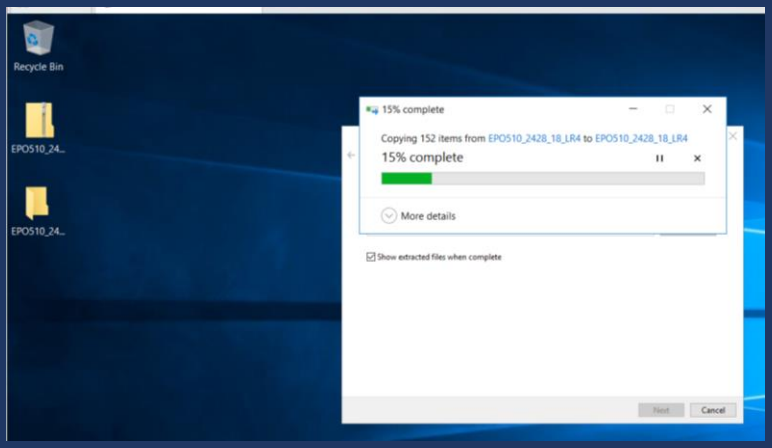
- **Llenaremos el formulario que nos ponen, con la información que nos piden.**



- **Llenado y enviado el formulario ya nos aparecerá ora sección con el link de descarga del software.**

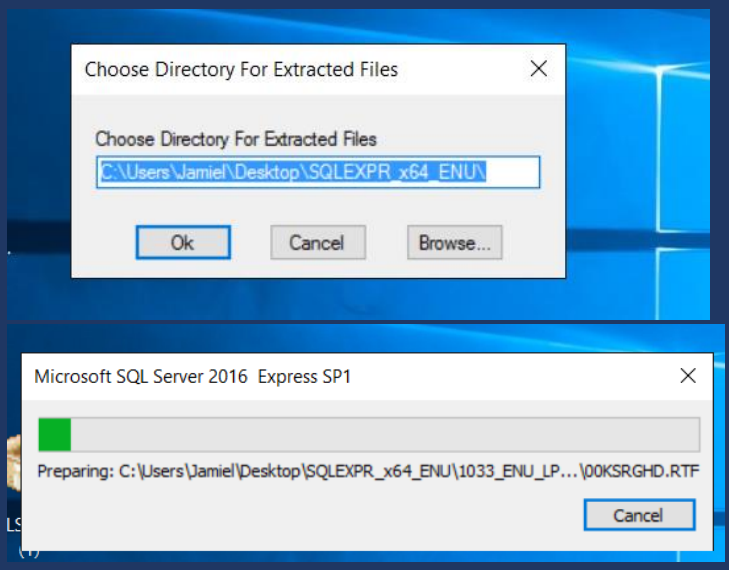


- Ya descargado el archivo comenzamos con el proceso de descompresión

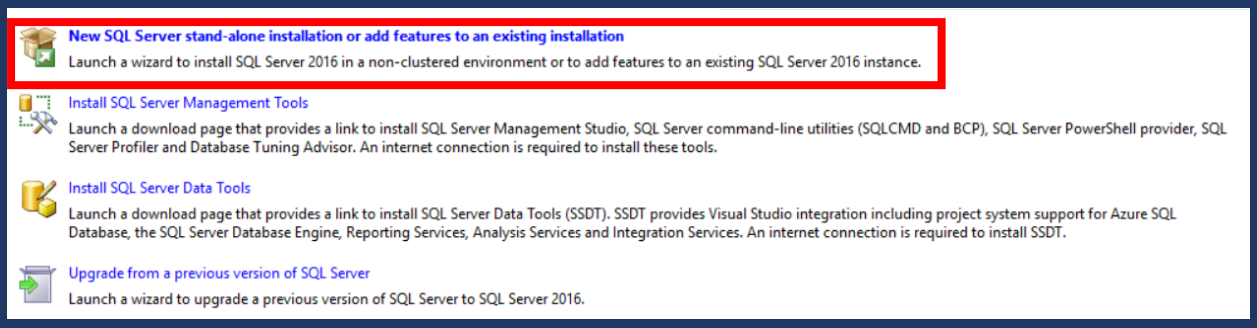


- Ahora procederemos con el proceso de instalación de la base de datos para mcafee, en este caso SQL SERVER EXPRESS 2016 **LINK DE DESCARGA (https://download.microsoft.com/download/9/0/7/907AD35F-9F9C-43A5-9789-52470555DB90/ENU/SQLEXPR_x64_ENU.exe)**
- Una vez descargado procederemos a instalar el sql 2016 click derecho en el archivo y ejecutar como administrador.

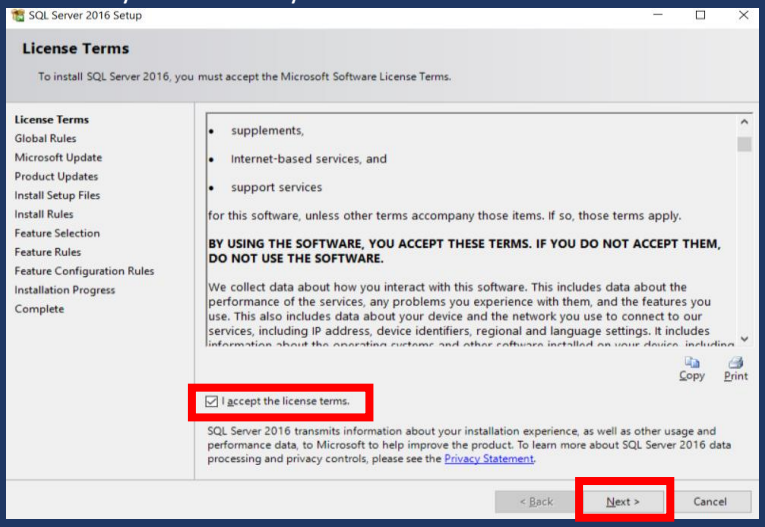
- Vamos a elegir el directorio donde se guardarán o mejor dicho se van a extraer los archivos.



- Extraído todos los archivos nos aparecerá una ventana con las opciones sobre la instalación que queramos elegir, para nuestro caso elegimos la primera opción donde le indicamos que es una nueva base de datos standard.



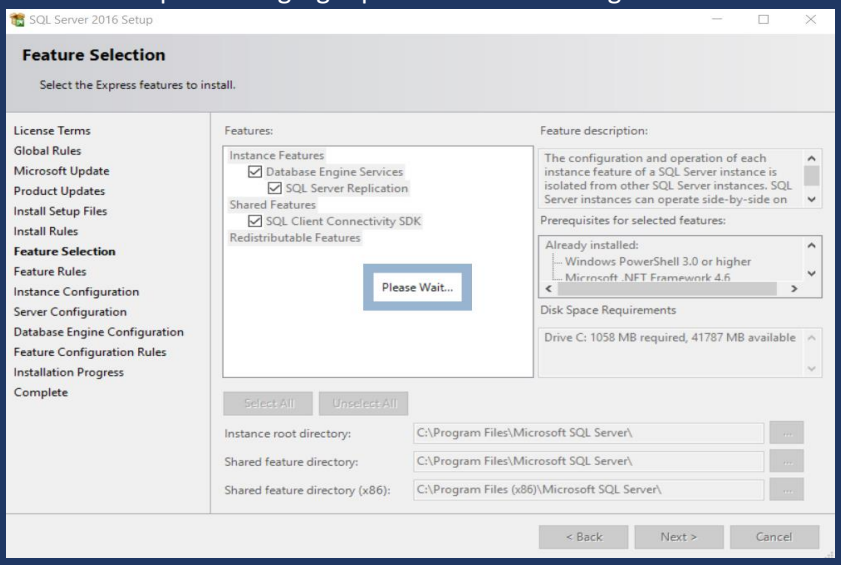
- Se nos abrirá el wizard para completar el proceso de la actualización, aceptamos los términos y condiciones y damos click en next.



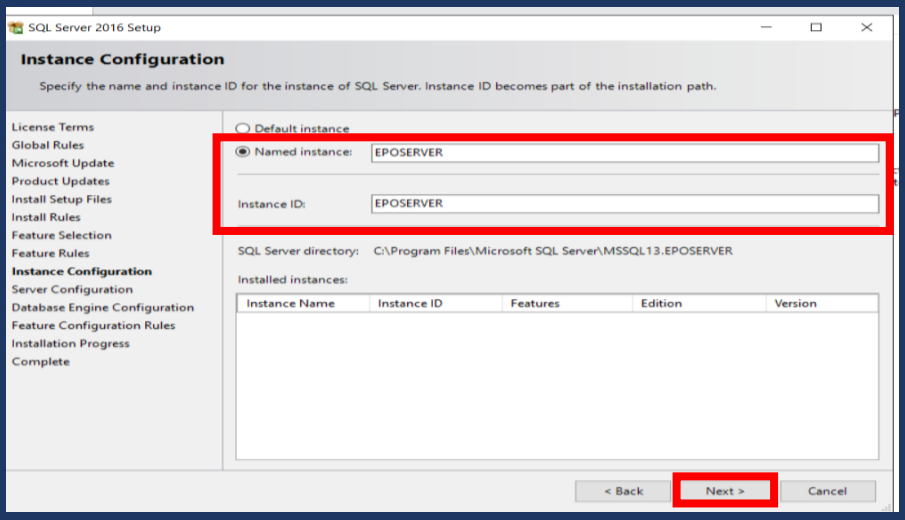
-

- Las recomendaciones de macafee para el correcto funcionamiento es deshabilitar cualquier firewall que tengamos activo e instalar dicho software a parte del controlador de dominio.

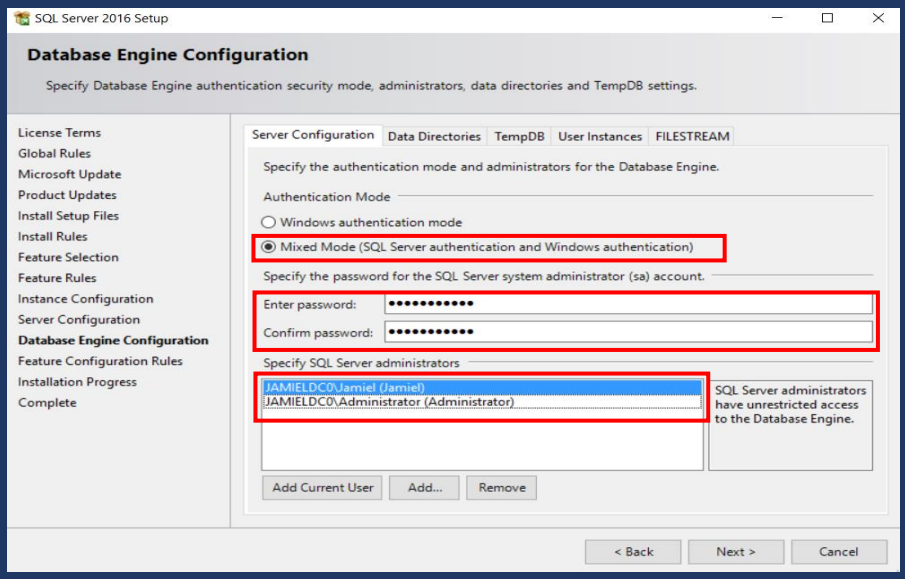
- En el siguiente paso nos muestra donde se instalará la base de datos por default, y las features que se le agregar por default a la configuración.



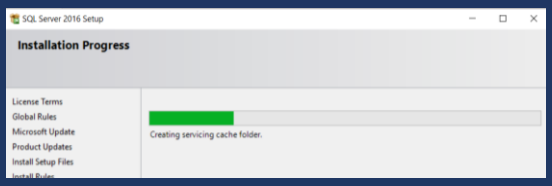
- Finalizado el paso anterior finalizamos con la configuración del name instance o el nombre que tomara nuestra base de datos, como estamos trabajando con epolicy, le pondremos como nombre **EPOSERVER. Hacemos click en next.**



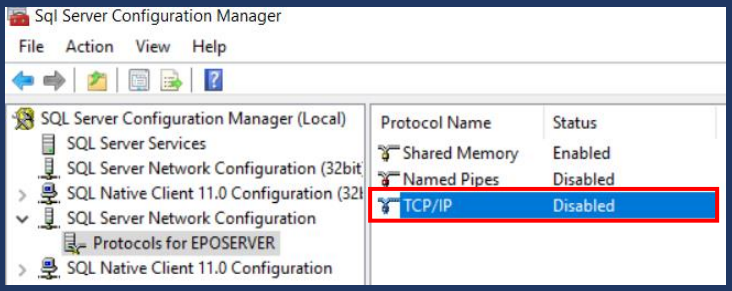
- En la opción de **authentication mode** seleccionaremos la segunda, para poder asignarle una clave a la cuenta de administrador de la base de datos.



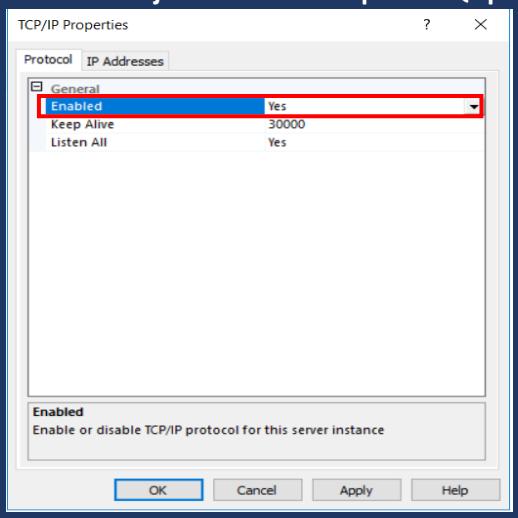
- **Esperamos que se complete la instalación.**



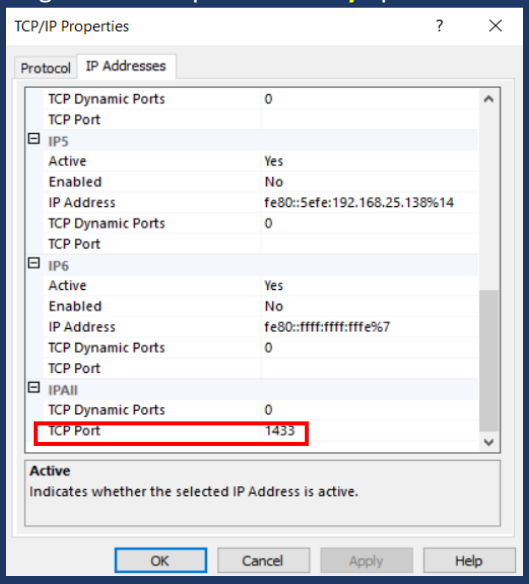
- Realizada la instalación nos dirigimos al **sql server configuration manager** donde nos dirigimos a la sección de **sql server network configuration > protocols (NOMBRE DE INSTANCE)** ya en esta sección nos dirigimos al apartado de **TCP/IP.**



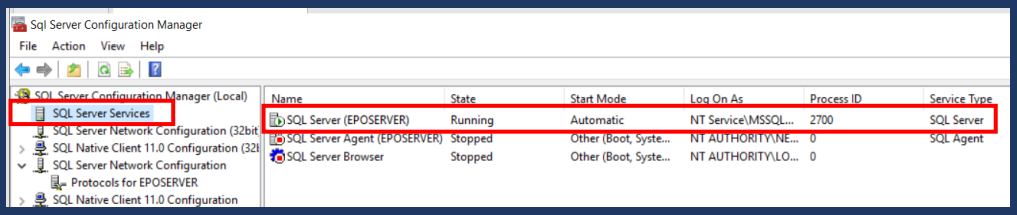
- **Donde el objetivo es activar que el SQL pueda correr por dicho protocolo.**

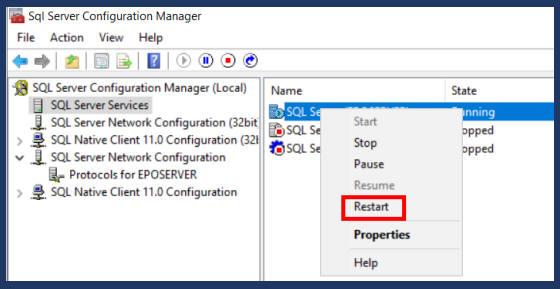


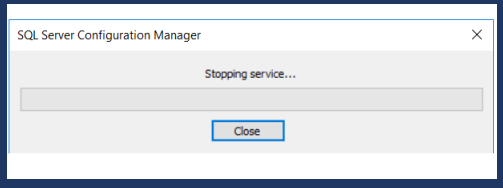
- Realizado esto nos dirigimos a la pestaña **ip addresses,** donde nos dirigiremos a la parte más baja de las opciones y buscaremos la llamada **TCP PORT** donde le asignaremos el puerto **1433 y** aplicamos los cambios.



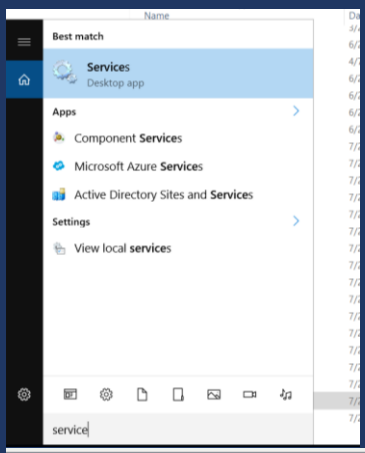
- **En este paso vamos a reiniciar nuestro sql server, para eso en nuestro mismo server manager nos dirigimos a sql server services > sql server (NOMBRE DE INSTANCE), le damos click derecho y reiniciar**

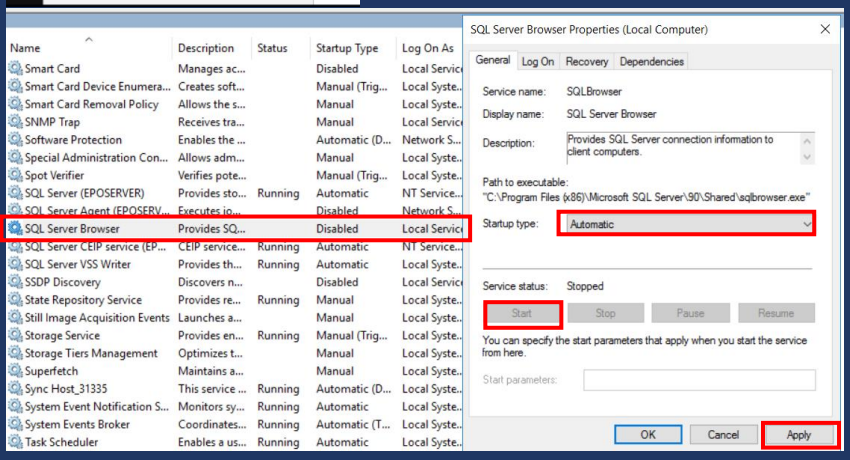




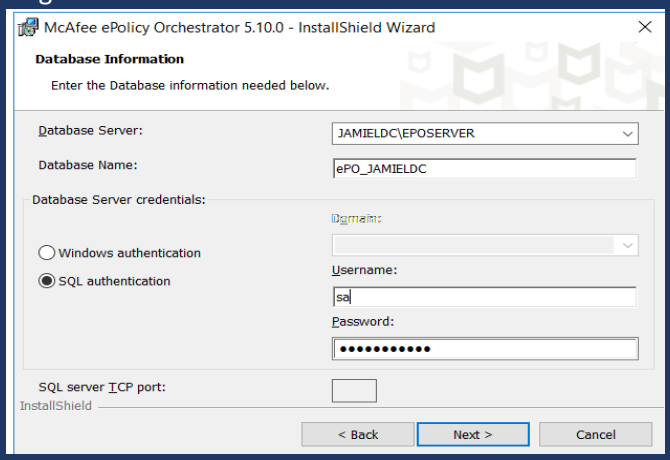


- Terminada la configuración de sql, ahora activaremos el servicio **sql browser**, esto lo haremos dirigiéndonos al programa services, donde buscaremos el servicio **sql browser**, y le asignaremos su **startup type** en a**utomatic.**

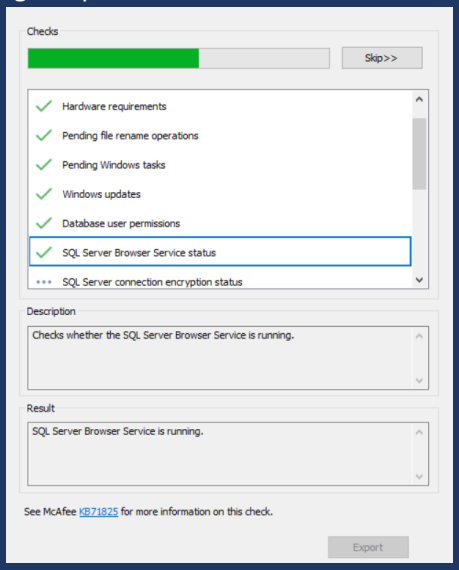




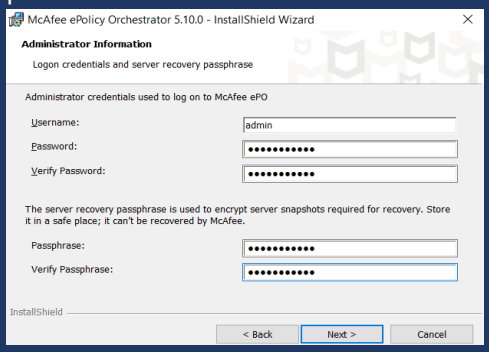
- Hecho esto comenzaremos con la instalación de nuestro MaCafee EPO, nos dirigimos a nuestra carpeta donde tenemos todos los recursos de la descarga de Macafee, y en la parte baja encontraremos un archivo que lleva por nombre setup.
- Dejaremos todo por default hasta llegar al paso de configuración y autentificación en la base de datos, donde en el data base server le pondremos el que hemos creado EPOSERVER, pasaremos la configuración a SQL AUTHENTICATION, donde pondremos el username como el predeterminado sa y en password pondremos la que hemos asignado al crear la base de datos



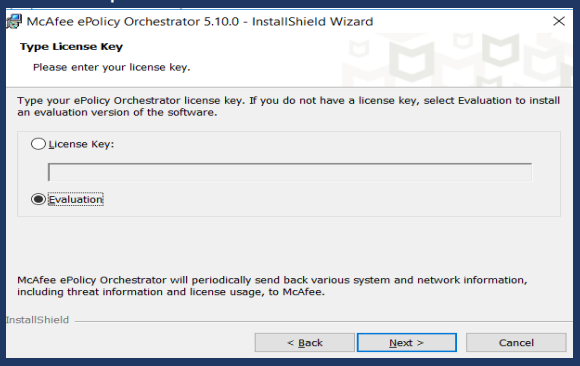
- Haciendo click en next, esperamos a que confirme y configure todo lo necesario en caso de haber algún tipo de error nos lo va a notificar.



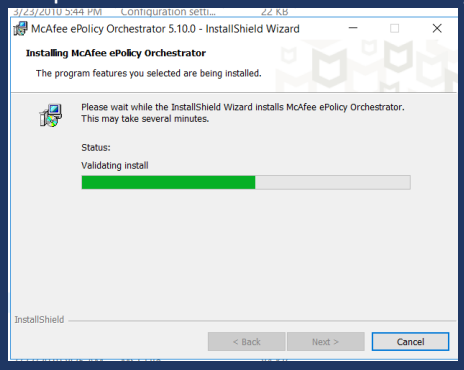
- Al finalizar el proceso vemos como todo se ha realizado y verificado correctamente sin ningún tipo de error.
- El siguiente paso seria configurar los puertos por donde va a trabajar Macafee en mi caso por motivos prácticos lo dejaremos por default en dado caso que cambiemos algo de dicha configuración tendremos que aplicarlo en el firewall para que pueda funcionar.
- Pasado este paso ahora vamos a configurar la cuenta administrador de la interfaz de Macafee, donde dejaremos el user por defecto admin, al cual le asignaremos una password.



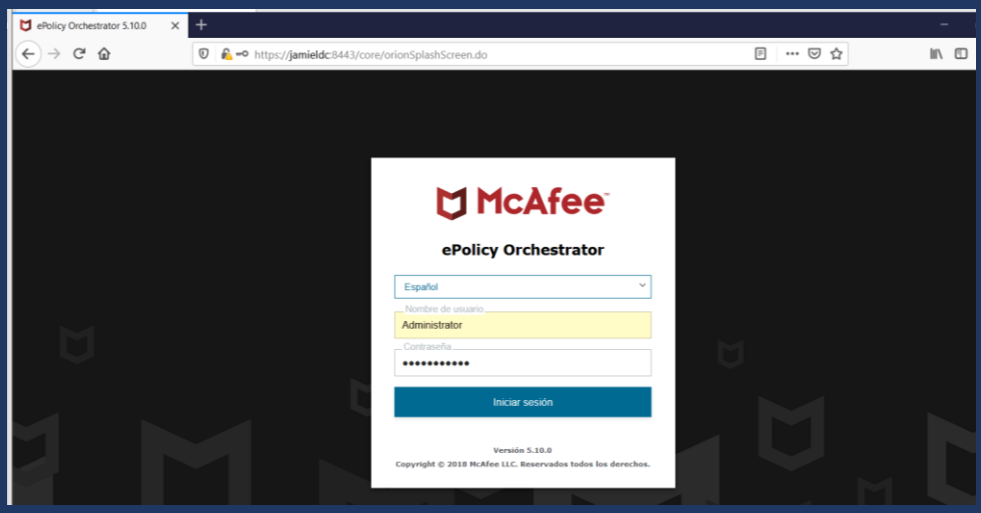
- En cuanto a los fines de licencia le ponemos que solo es evaluación ya que es con motivos prácticos.



- Aceptamos nuevamente los términos y condiciones y ejecutamos la instalación.

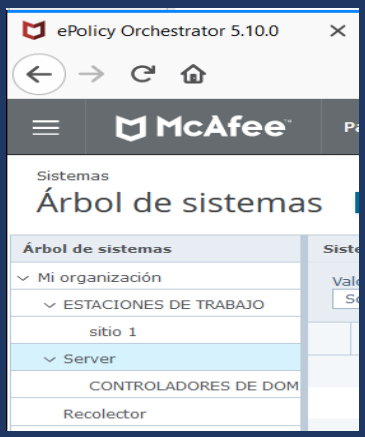


- Realizada la instalación se nos creará un acceso directo para poder acceder a la interfaz web, donde ingresaremos con el user y la pass que hemos creado anteriormente.



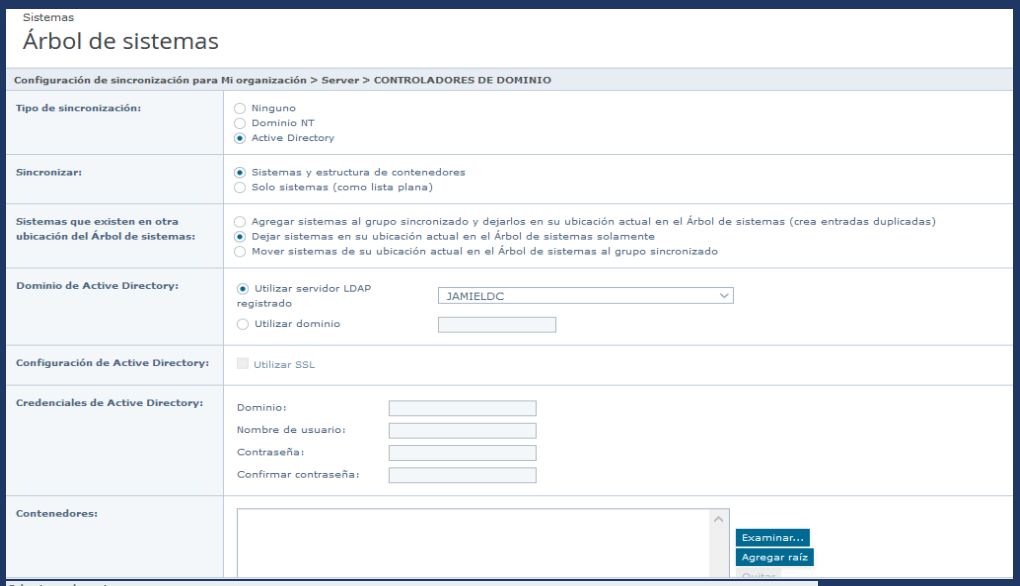
b. Integrar McAfee epo con Active Directory

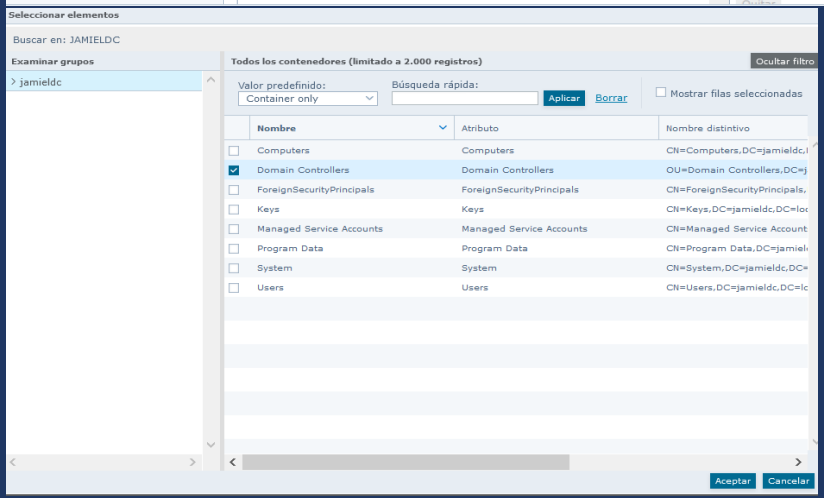
- Ya adentro de la interfaz web comenzaremos con la sincronización de Macafee con Active directory.
- Primero crearemos algunos subgrupos en el árbol de sistemas de la siguiente manera.



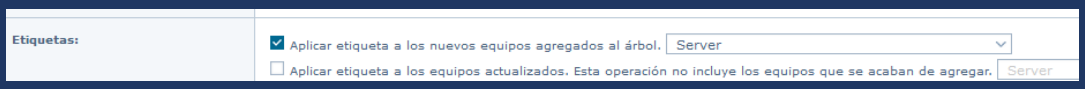
- Ahora en el grupo creado Controladores de dominio vamos a sincronizar nuestro dominio esto se hace dirigiéndonos al grupo y buscamos la opción tipo de sincronización y le daremos en editar.

- Ya cuando estemos en la sección eligiremos que es un dominio de AD, las siguientes dos opciones la dejamos por default y nos pasamos a la llamada Dominio de AD, donde escogeremos la opción de utilizar un servidor LDAP registrado, en caso de no tener se pueden crear uno en macafee o escoger la segunda opción, ya en el sexto apartado vamos a elegir el contenedor que en este caso seria controlador de dominio.

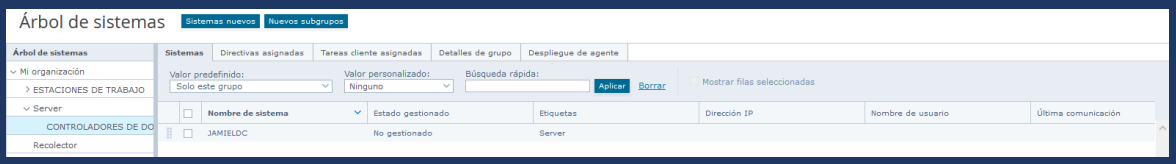




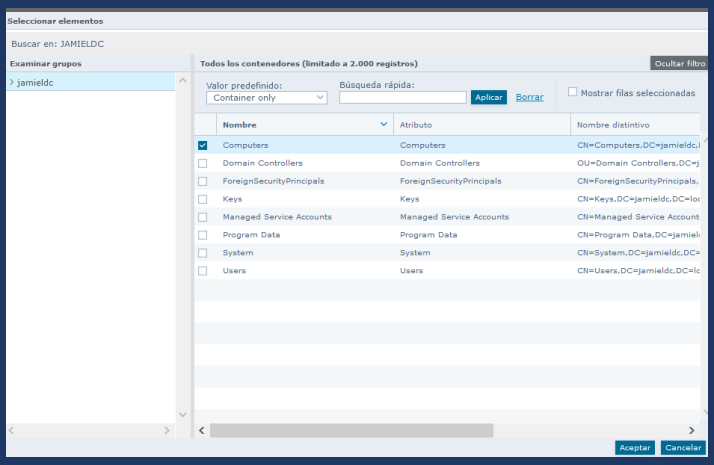
- En la sección de etiquetas como estaremos trabajando con los servidores marcaremos la casilla de aplicar etiquetas a los nuevos equipos agregados al árbol y le pondremos que server.



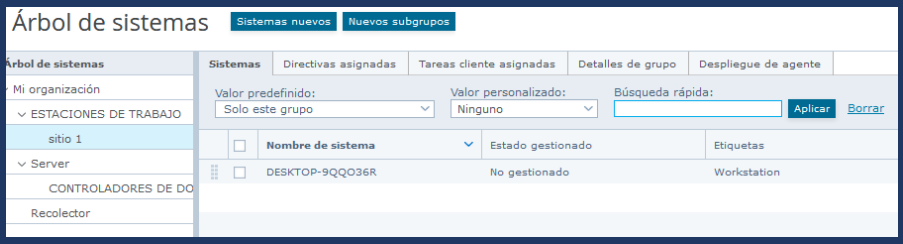
- Después de este paso ya podemos guardar la configuración.
- Vemos como despues de un tiempo de sincronización ya nos aparece nuestro controlador en la sección de sistemas en el subgrupo de controladores de dominio.



- Ahora vamos al mismo sitio de configuración, pero en el subgrupo de estaciones de trabajo.
- Lo único que cambiaremos es que, en la sección de contenedores, marcaremos la casilla de computers.

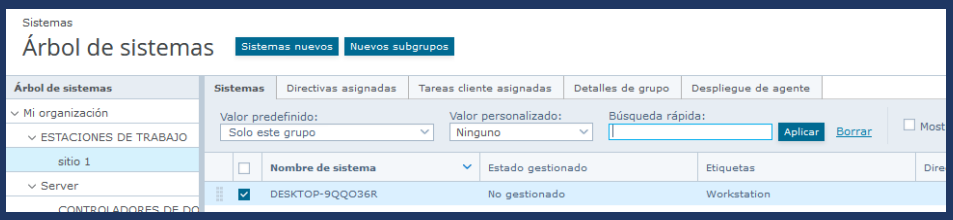


- Hecho esto si sincronizamos y guardamos la configuración vemos como ya nos aparecen todos los computadores que se encuentran en el dominio de AD, en mi caso solo una.

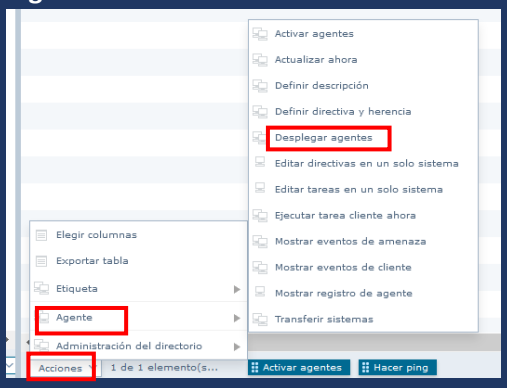


c. Desplegar el cliente de McAfee Agent a los computadores miembros del dominio

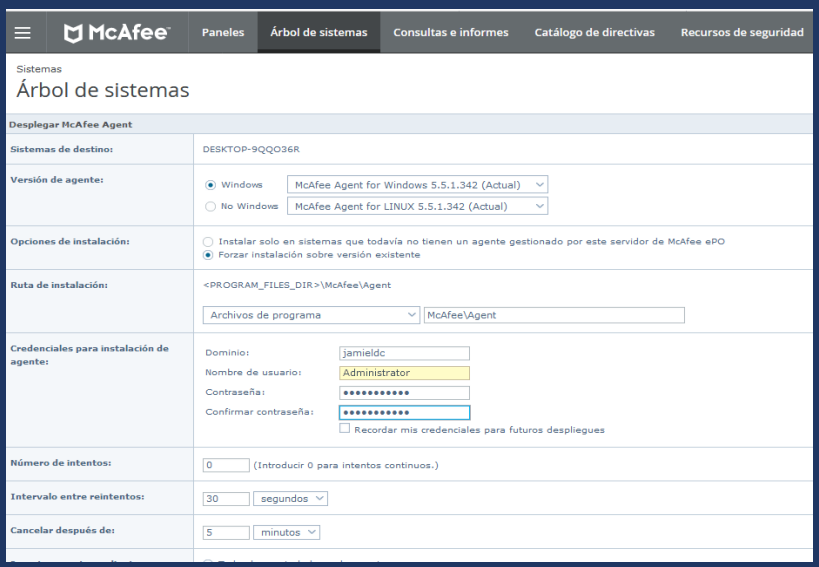
- **Para desplegar los agentes para saber información sobre los equipos de la red y monitorearlos, solo tendremos que marcar los dispositivos a los cuales queremos enviar los agentes.**



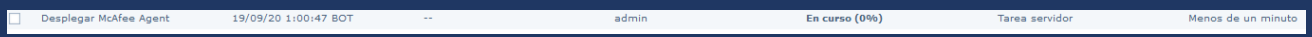
- **En la parte baja tal y como muestra la imagen damos click en acciones > agente > desplegar agentes.**



- Inmediatamente se nos abre una venta para la configuración del agente, su ruta de instalación, si esta va a ser forzada o no…, en nuestro caso forzaremos la instalación.



- Realizada la configuración y posteriormente guardada podemos ver el transcurso del despliegue del agente.



- Una vez terminada la instalación se nos notificará de la siguiente manera.

- Si nos vamos a nuestro system tree y nos fijamos en el equipo que hemos desplegado el agente, vemos como ya nos aparece la ip del dispositivo y el user con el que se ha logueado

- Si nos fijamos en la información de la ventana security status, el despliegue y el funcionamiento esta habilitado, y en la ventana de about vemos la versión que se esta ejecutando junto con otras informaciones adicionales.