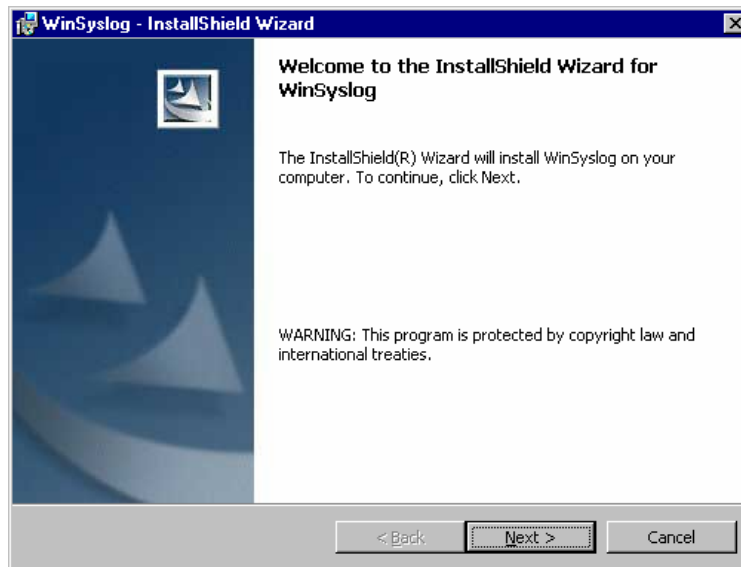


Guía rápida para instalar Winsyslog v5.2

Por: Sergio Untiveros
<http://www.aprendaredes.com>
Setiembre, 2004

Paso1. Instalación

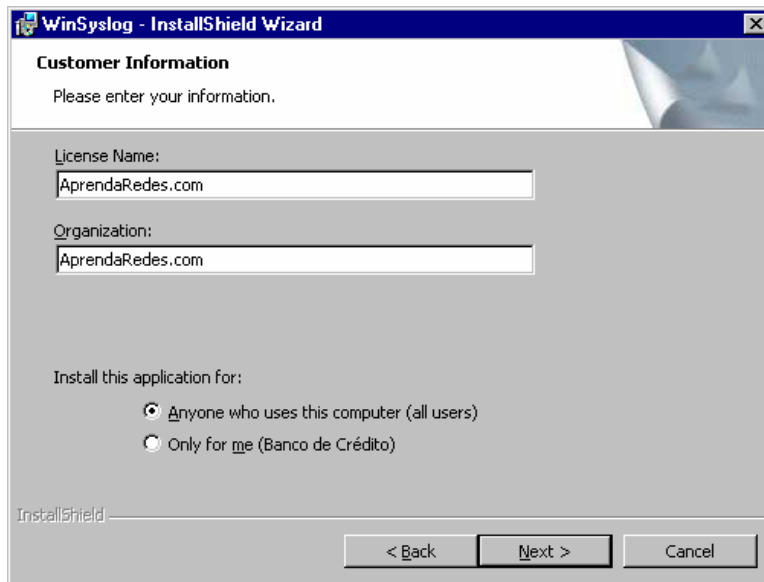
- Después de haber bajado el archivo **wnsyslog.exe** , hacer clic para iniciar la instalación.
- Saldrá la siguiente ventana.



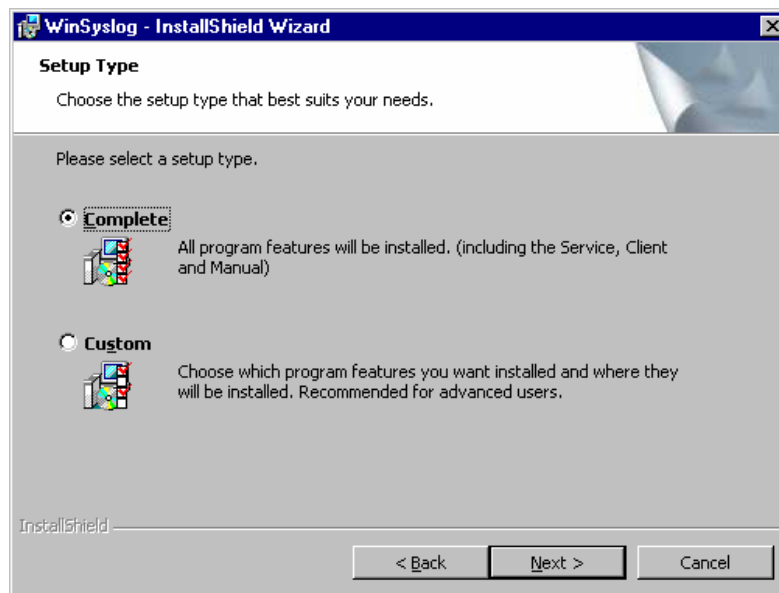
- Hacer clic en **Next>**, saldrá la siguiente ventana:



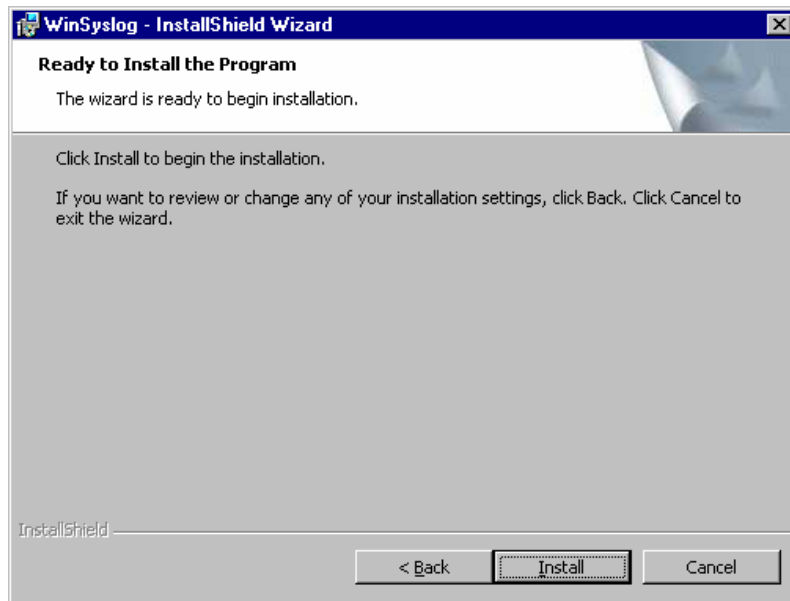
- Seleccionar **"I accept the terms in the license agreement"** y hacer clic en **Next>**



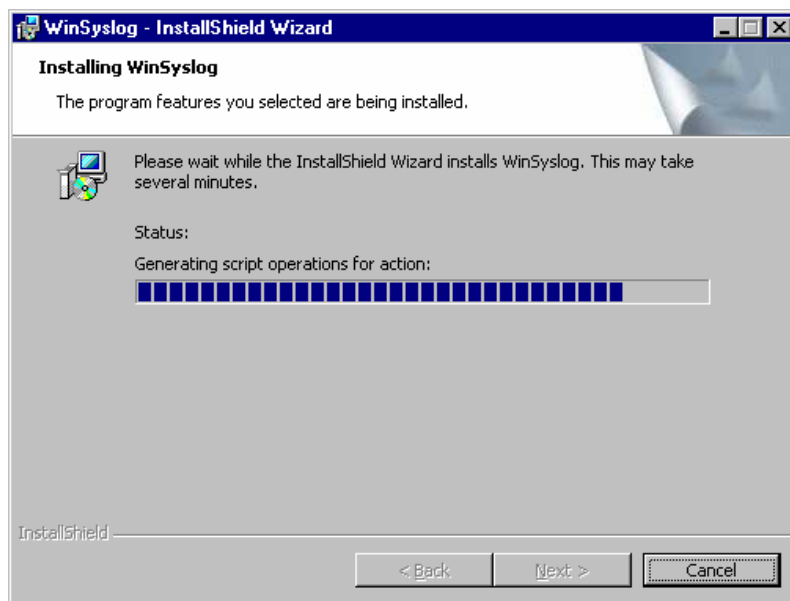
- Escribe el Nombre de la Licencia. Para probar este software durante 1 mes, puedes poner cualquier nombre. Al final del mes el software se desactivará. Si quieres seguir utilizando solo tendrás que comprar la licencia en <http://www.aprendaredes.com/winsyslog/index.htm>
- Escribe el nombre de la organización tal como se muestra. Presiona **Next>**



- Elige **Complete** y presiona **Next>**



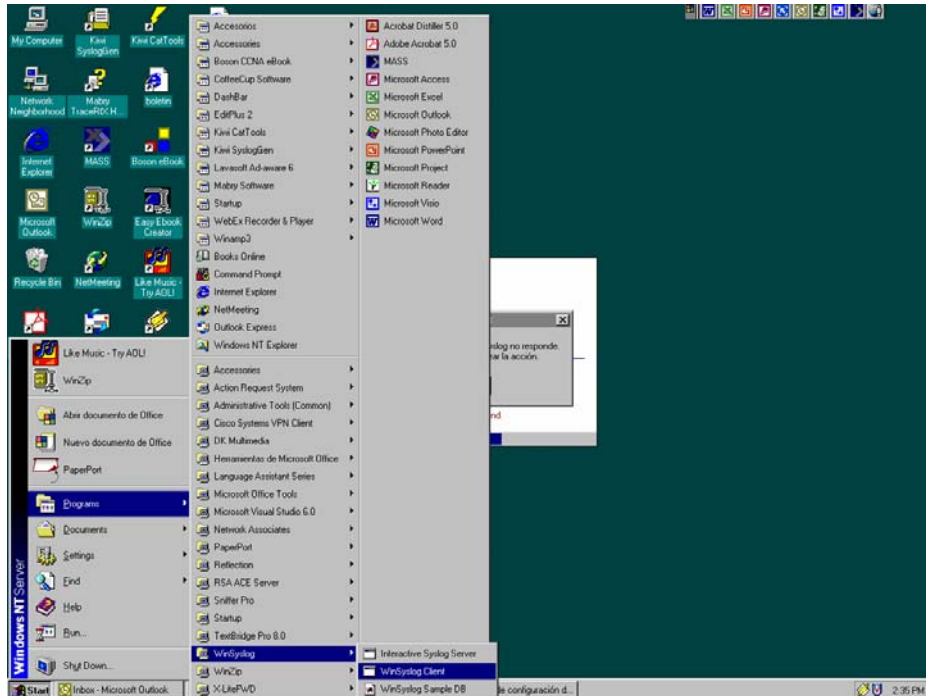
- Presiona en el botón **Install**, y arrancará la instalación.



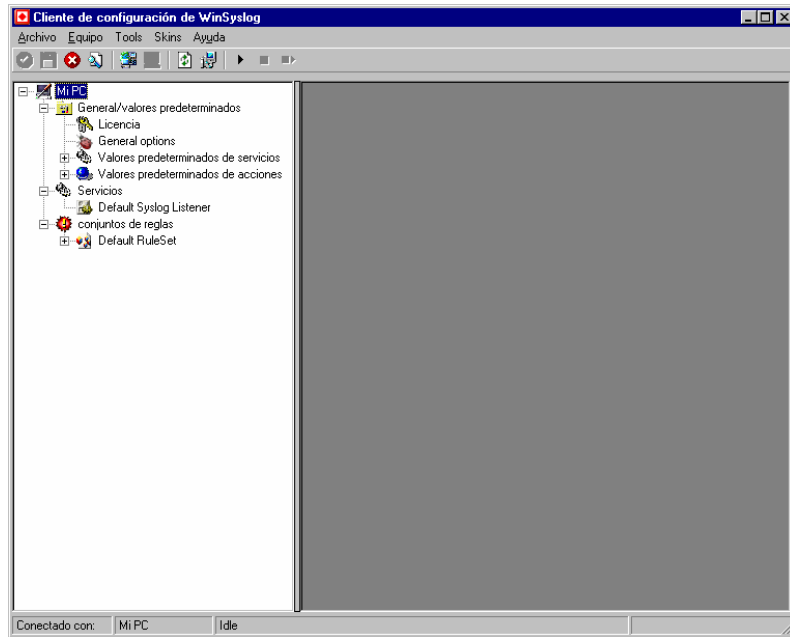
- Siga con el procedimiento de instalación hasta finalizar.

Paso 2. Configuración Winsyslog

- Para arrancar el Winsyslog ir a Start o Inicio y ubicar la carpeta Winsyslog. Dentro de esa carpeta hay 2 ejecutables: **Interactive Syslog Server** y **WinSyslog Client**. Hacer clic en **WinSyslog Client**.



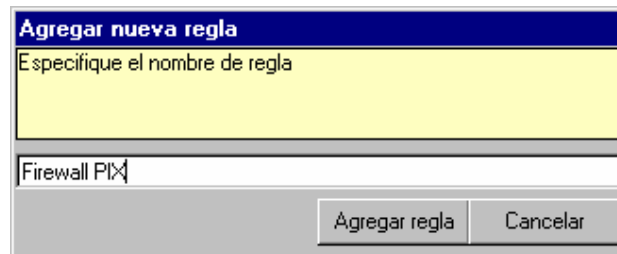
- Aparecerá la siguiente ventana. La primera vez te sale una ventana donde te pregunta el idioma que quieres utilizar.



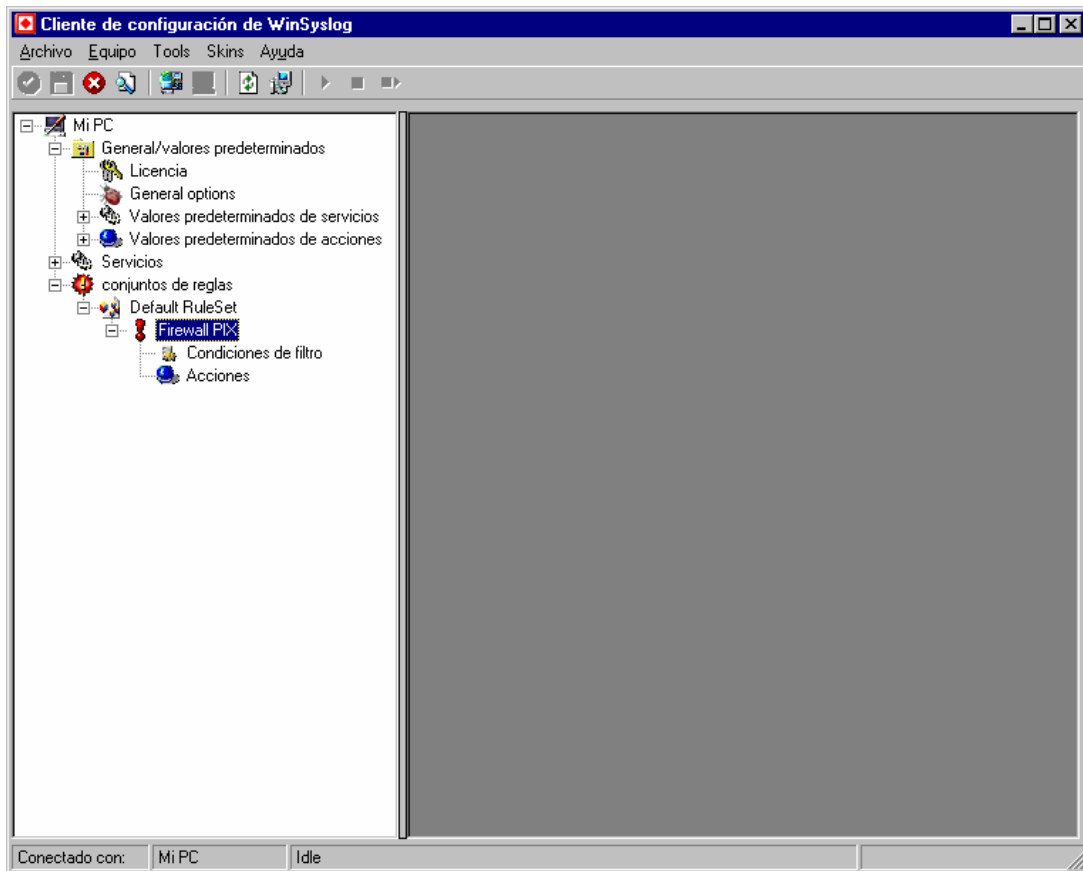
- Hacer click en Default Rule Set
- Aparecerá una regla con el siguiente nombre: **ForwardSyslog**
- Ubicar el puntero del mouse sobre **ForwardSyslog** presionar el botón derecho del mouse y aparecerá una pequeña ventanita con la opción **Eliminar Regla**. Prosigua con la ejecución de esta opción.
- Observará que la regla ha desaparecido.

Configuración de una Regla ~ Para grabar mensajes syslog en archivo .txt

- Para ello ubique el mouse sobre la opción **Default RuleSet**
- Presionar el botón derecho y elija la opción **Añadir Reglas** ó **Add Rules**
- Aparecerá la siguiente ventana



- Ponga el nombre de la regla
- Presione el botón Agregar regla
- Aparecerá la siguiente pantalla.



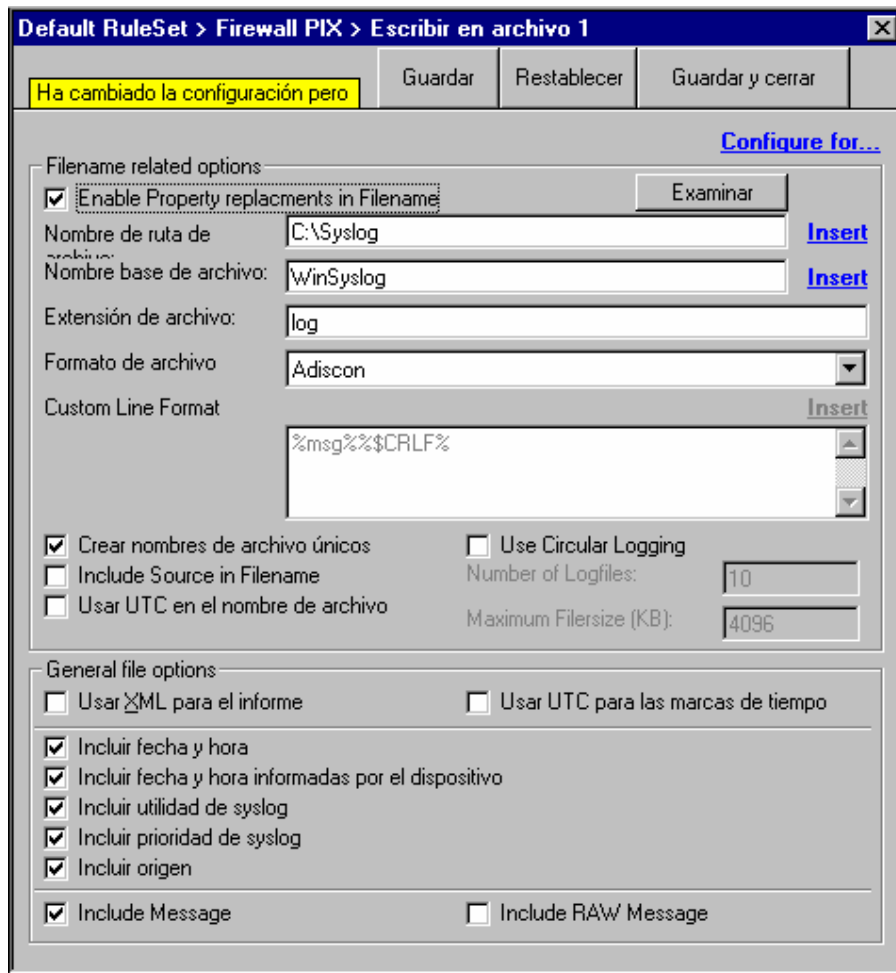
- Observa que la regla Firewall PIX tiene dentro 2 opciones:
 - Condiciones de Filtro
 - Acciones
- Haga clic en el botón derecho del mouse y elija la opción **Agregar Acción** (Add Action) y dentro elija **Grabar en Archivo (Write to File)**. Saldrá la siguiente ventana.



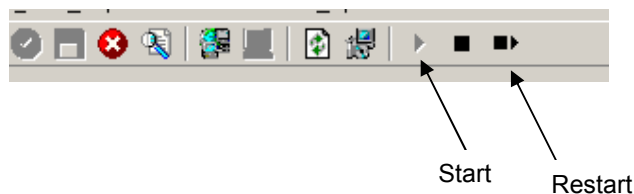
- Presiones siguiente y aparecerá la siguiente pantalla:



- Luego presione **Finalizar** y aparecerá la siguiente ventana, donde se tiene que configurar lo siguiente:



- En esta ventana se tienen que realizar 2 configuraciones. Habilitar el Check Box “**Enable Property replacement in Filename**” y el directorio donde se van a grabar los archivos diarios con los mensajes syslog, en esta guía C:\Syslog.
- Nota: Cada día se graban los archivos de mensajes syslog con nombre diferente
- Después de configurar presionar el botón “**Guardar y cerrar**”
- Verificar que el servidor esté corriendo. Fíjate en la barra de herramientas o en el menú file si el símbolo **Start** está desactivado, solo debe estar activo **Stop** y **Restart**, eso significa que el Syslog está corriendo. Después de configurar una Regla debes hacer clic en **Restart**.



Paso 3. Configuración Syslog en el PIX

```
!  
PIX Version 6.3(1)  
!  
logging on  
logging timestamp  
logging buffered debugging  
logging trap critical  
logging host inside IP_Servidor_Syslog  
!  
!
```

Este parámetro se puede cambiar del 0~7, en el nivel 7 recibes todos los mensajes del PIX

Nota: Esta guía no está orientada a como configurar el PIX Firewall

• Opcional. Configuración Syslog en un Router Cisco

```
!  
!  
!  
version 12.1  
service timestamps debug datetime localtime  
service timestamps log datetime localtime  
!  
logging buffered 30000 debugging  
!  
logging trap debugging  
logging source-interface Interface_Del_Router  
logging IP_Servidor_Syslog  
!  
!
```

Paso 4. Verificación

- Para verificar que el Winsyslog está trabajando, revisar en el directorio C:\Syslog (para este ejemplo). Dentro de este directorio se grabarán archivos de mensajes por cada día.

Paso 5. Soporte Técnico

En caso de tener problemas o alguna pregunta puedes hacerlo a la siguiente dirección:

Soporte@aprendaredes.com

Si deseas más información puedes ingresar a nuestra web:
<http://www.aprendaredes.com>

Inscríbete en forma gratuita a nuestro Boletín Electrónico
"Todo Sobre Redes" el cual es publicado cada 15 días
Para suscribirte puedes hacerlo en la web o enviando un
correo electrónico a:
<mailto:suscribir-boletin@aprendaredes.com>