

Requisitos configuración de seguridad puestos cliente Rich Web

30 Octubre 2009



TABLE OF CONTENTS

TABLE OF CONTENTS.....	2
1 OBJETIVO	3
2 PERMISOS EN FORMATO CHECK-LIST	4
3 REQUISITOS CONFIGURACIÓN CLIENTE RICH WEB	5
3.1 CONFIGURACIÓN INTERNET EXPLORER	5
3.1.1 Descargar y ejecutar controles ActiveX firmados	5
3.1.2 Comprobación de firma digital	5
3.2 PERMISOS DE LECTURA, ESCRITURA Y EJECUCIÓN DE ARCHIVOS.....	6
3.3 PERMISOS EN EL REGISTRO DE WINDOWS	6
3.4 WINDOWS INSTALLER	6
3.5 WINDOWS VISTA Y ACTUALIZACIÓN DE CLIENTES RICH WEB DE VERSIONES ANTERIORES.....	6
3.6 TIPO DE USUARIO WINDOWS	6
3.7 ANTIVIRUS	7

1 OBJETIVO

Este documento describe los requisitos de configuración de seguridad de los puestos cliente Rich Web de PeopleNet para su correcta instalación, actualización y funcionamiento.

Para más detalle sobre la instalación de PeopleNet puede consultar la Guía de instalación de la tecnología base (Guia_instalacion.pdf) incluida en el CD de producto.

2 PERMISOS EN FORMATO CHECK-LIST

Internet Explorer: Descarga y ejecutar controles ActiveX firmados		
Seguridad Nivel Medio-Alto		<input type="checkbox"/>
Permisos para la descarga y ejecución de controles ActiveX		<input type="checkbox"/>
Internet Explorer: Revocación de certificados		
Si está Activado	Disponible lista de revocación (CRL)	<input type="checkbox"/>
	Certificado seguridad valido en conexión segura cliente-Servidor	<input type="checkbox"/>
Desactivado		
Internet Explorer: Política de validación del time stamp del certificado		
Si Política validación del timestamp activada	Permisos de acceso a Internet para validar con el proveedor el certificado	<input type="checkbox"/>
Política validación del timestamp desactivada		<input type="checkbox"/>
Disco duro usuario sistema		
Permisos de lectura, escritura y ejecución en %appdata%		<input type="checkbox"/>
Permisos de lectura, escritura y ejecución en %Temp%		<input type="checkbox"/>
Permisos de lectura, escritura y ejecución en Temporary Internet Files del Internet Explorer		<input type="checkbox"/>
Permisos de lectura para ubicación resto programas Windows		<input type="checkbox"/>
Registro		
Permisos de lectura en todo el registro		<input type="checkbox"/>
Permisos de escritura en la rama HKEY_CURRENT_USER		<input type="checkbox"/>
Windows Installer		
Servicio Windows Installer habilitado		<input type="checkbox"/>
Windows Vista con instalación anterior a 7.1SP3		
Internet Services Detection activado		<input type="checkbox"/>
Entorno servidor del RichWeb, basado en el IIS, con autenticación integrada con Windows		
Usuarios no locales		<input type="checkbox"/>
Antivirus		
Chequear que respeta todos los puntos anteriores		<input type="checkbox"/>

3 REQUISITOS CONFIGURACIÓN CLIENTE RICH WEB

3.1 CONFIGURACIÓN INTERNET EXPLORER

3.1.1 Descargar y ejecutar controles ActiveX firmados

La aplicación cliente funciona correctamente sobre un navegador con **nivel de permisos Medio-Alto**, tal como se define por defecto en Internet Explorer. Es necesario siempre poder **descargar y ejecutar controles ActiveX firmados**.

Con el citado nivel de seguridad se solicitará al usuario que confirme que confía en los componentes de Meta4 la primera vez que intente acceder a la aplicación.

3.1.2 Comprobación de firma digital

El proceso de instalación comprueba que los paquetes están firmados por Meta4. Se deben tener en cuenta una serie de aspectos:

Revocación de certificados: si esta política está activada se deben cumplir las siguientes condiciones:

- 1) El certificado de seguridad debe ser válido para las conexiones seguras entre cliente y el servidor.
- 2) Se dispone de la lista de revocación (CRL) en el servidor web.

Si no se cumplen esas condiciones, esta política se debe desactivar en el MS Internet Explorer.

Validación del time stamp: si esta política está activada, deberá tener acceso Internet a la información de time stamp de los proveedores de las firmas del certificado (sitio Verisign, por ejemplo). Si no se cumple esa condición debe desactivarse. Para ello puede utilizarse la utilidad setreg.exe (disponible en VSTDO 2008 o Win SDK) y poner la opción 9 a false.

Para asegurar que la comprobación de la firma digital de un componente de Meta4, por ejemplo el M4RichWebStart.exe, se valida correctamente pulse el botón derecho del ratón sobre el fichero en cuestión y en propiedades seleccione la pestaña "Firmas digitales". En esta pestaña no pueden existir errores de validación para que la aplicación funcione correctamente. Eso naturalmente se debe realizar en el contexto de seguridad del usuario final.

3.2 PERMISOS DE LECTURA, ESCRITURA Y EJECUCIÓN DE ARCHIVOS

Se necesitan permisos de lectura, escritura y ejecución en todos los directorios definidos a partir de lo especificados en las variables de usuario %appdata% y %temp% incluidos estos mismos.

También se debe tener en cuenta, que al tratarse de una aplicación que se descarga a través de MS Internet Explorer, cuando ésta es instalada por primera vez en un usuario/máquina deberá tener permisos de lectura, escritura y ejecución sobre los "Temporary Internet Files" del usuario. En este punto, existiría la alternativa de que el usuario descargara ese fichero a cualquier otra ruta donde tuviera permisos de ejecución. Con la asignación de permisos que mencionamos, la instalación sería directa sin necesidad de guardar previamente el fichero.

3.3 PERMISOS EN EL REGISTRO DE WINDOWS

Para la instalación de las componentes COM y de los distintos paquetes de instalación se requieren permisos de lectura y escritura en la rama del registro HKEY_CURRENT_USER.

Además, se requieren permisos de lectura en todo el registro de la máquina.

3.4 WINDOWS INSTALLER

El servicio de Windows Installer debe estar habilitado.

3.5 WINDOWS VISTA Y ACTUALIZACIÓN DE CLIENTES RICH WEB DE VERSIONES ANTERIORES

En los puestos cliente con Windows Vista y con versiones 7.1SP1 o 7.1SP2 de Rich Web, para llevar a cabo la actualización a 7.1SP3 será necesario tener iniciado el servicio de Windows "Interactive Services Detection". Para activar dicho servicio, vaya a Panel de control, Herramientas administrativas y, a continuación, seleccione Servicios. Para realizar esta acción es necesario disponer de una cuenta con privilegios de administrador. Una vez completado el paso anterior, el sistema operativo nos muestra un mensaje indicando que tenemos un mensaje en otra sesión y, tras aceptar el mensaje, accedemos a una serie de diálogos sobre un fondo que no es nuestro escritorio y a continuación le indicamos volver a nuestra sesión. Por último, volvemos a acceder a la URL de Rich Web para continuar con la instalación de la versión

3.6 TIPO DE USUARIO WINDOWS

Si el servidor web que contiene el Servicio de Actualización de Componentes se encuentra en plataforma Windows, debe revisar la configuración de IIS por si éste solicita Autenticación Integrada con Windows.

Si es así, se recomienda que no utilice usuarios locales de la máquina (ajenos al dominio, o no habilitados para que la autenticación integrada tenga lugar automáticamente) para su conexión al sitio Web que contiene los Servicios de Actualización, para evitar problemas con la autenticación de las descargas.

3.7 ANTIVIRUS

En general la instalación Rich Web es totalmente compatible con las opciones de seguridad habituales en los Antivirus más extendidos.

Es posible que tenga activadas en su antivirus políticas de seguridad que entren en conflicto con alguno de los aspectos de seguridad comentados en apartados anteriores.