

Manual de pGina



<http://pgina.xpasystems.com>

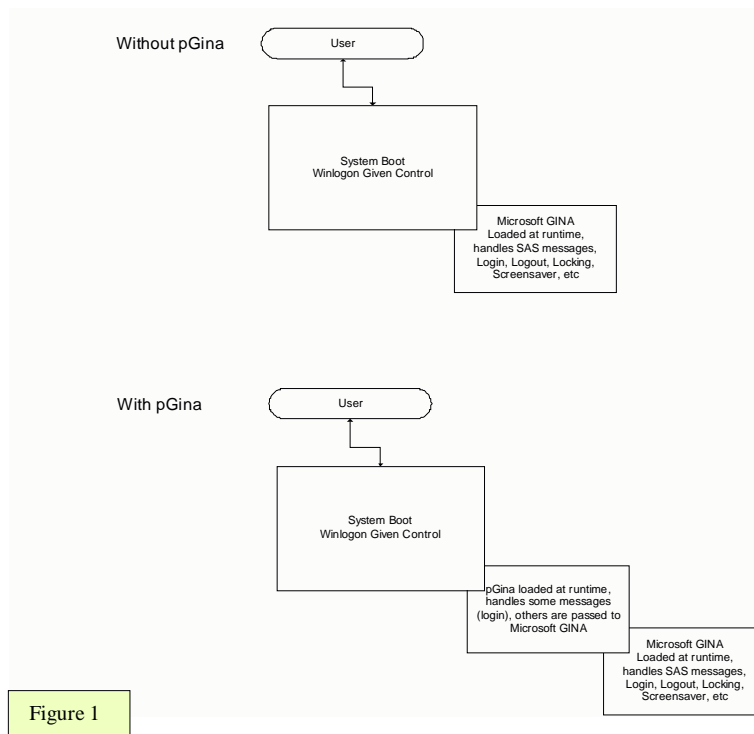


<http://www.xpasystems.com>

Introducción

pGina es, en resumen, un remplazo para la autenticación de dominio en un ambiente Windows. pGina, a través del uso de la tecnología de plugin, permite a un administrador escoger de entre un cierto número de fuentes y métodos de autenticación. Si una administradora deseara implementar un método de autenticación personalizado o extender uno existente, podría crear su propio plugin a partir del código del ejemplo fácilmente accesible y de la API para plugins de pGina.

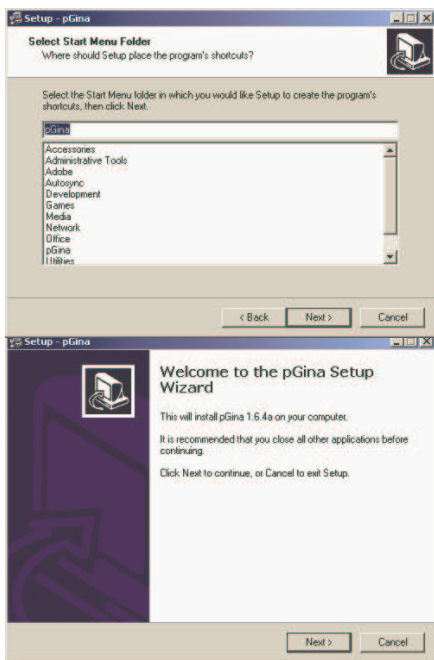
pGina funciona insertándose en el sistema operativo Windows como un módulo de autenticación e identificación gráfico (GINA por sus siglas en inglés), por eso el nombre. Sin pGina instalado, cuando un sistema Windows inicia, un proceso llamado Winlogon carga un GINA de Microsoft que es responsable del manejo de eventos del sistema como CTRL+ALT+SUPR, activación del protector de pantalla, intentos de acceso, etc. Cuando pGina está instalado, éste se inserta entre el proceso Winlogon y el GINA de Microsoft y maneja aquellos eventos relacionados con su propia operación (acceso, bloqueo, etc.) y pasa todo lo demás transparentemente al módulo de Microsoft.



Cuando Winlogon carga pGina, pGina a su vez carga un plugin elegido por el administrador. Cuando un usuario intenta entrar, pGina usará el plugin seleccionado para determinar si debería ser autenticado o no. Si el plugin permitiera al usuario proceder, pGina creará una cuenta para él en la máquina local, lo agregará a los grupos según esté especificado en el plugin, mapeará las unidades tanto globales como específicas para el usuario, y muchas otras cosas dependiendo de la configuración y la personalización.

Para comprender exactamente cómo pGina puede ayudar a alguien examinemos la situación de un administrador genérico llamado Joe. Joe es responsable de un conjunto de máquinas Windows 2000, así como de un amplio conjunto de máquinas Linux. Actualmente Joe se ve forzado a mantener nombres de usuario y contraseñas duplicados tanto en su servidor Windows como en su servidor UNIX. Adicionalmente, el servidor UNIX es también el servidor central de archivos, de manera que todo lo que el servidor Windows está haciendo realmente es autenticación de usuarios. Actualmente sus clientes Linux se autentican usando el protocolo LDAP. Joe puede usar pGina para autenticar a todos sus usuarios de windows desde el mismo servidor UNIX simplemente instalando pGina, y entonces instalando el plugin de LDAP. Ahora Joe sólo tiene que administrar un nombre de usuario y una contraseña, sin necesidad ya su servidor Windows. Esto libera una gran porción de su tiempo para otras tareas, y reduce la carga extra del costo del servidor Windows y de las licencias para los clientes que se apliquen.

Instalación

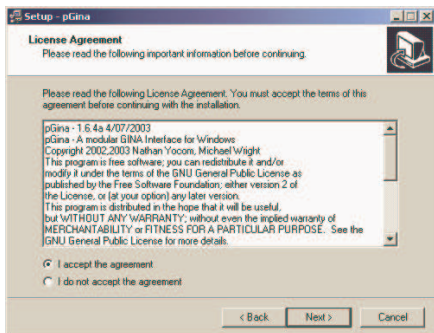


La instalación de pGina no tiene complicaciones y sigue muchas de las mismas convenciones que usan otros programas de Windows. **Nota: Si pGina falla, o se vuelve inusable de algún modo, impedirá todo acceso al sistema. Por esta razón es importante saber como arrancar en Modo a Prueba de Fallos, tener un disquete de rescate, o estar familiarizado con la edición remota del registro.**

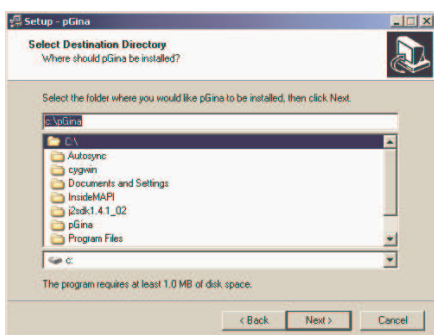
Primero lo primero: necesitará bajar el instalador más reciente del sitio web <http://pgina.xpasystems.com>. Después de bajarlo, asegúrese de estar acreditado como administrador local (o tiene privilegios de administrador local), que su máquina NO sea parte de un dominio (a menos que esté usando un plugin que haga interacción con el dominio) y ejecute el instalador. Confirme que desea instalar pGina y debe observar una pantalla similar a la Figura 2.

Aquí puede seleccionar la carpeta en la cual quiere instalar pGina. Se recomienda usar la opción por defecto (y se asumirá así en el resto del manual).

Después de seleccionar la ubicación deseada, presione el botón Siguiente para continuar a la Figura 3.

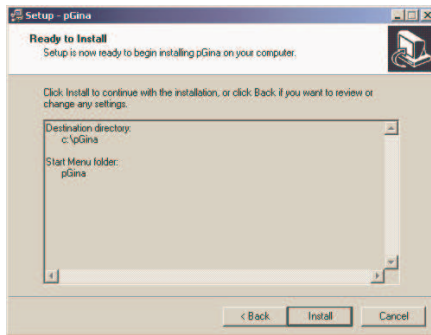


Este diálogo muestra una copia de la Licencia Pública GNU (GPL). Asegúrese de que la comprende y acepta y seleccione la opción “Acepto los términos”, entonces presione “Siguiente” para continuar a la figura 4.



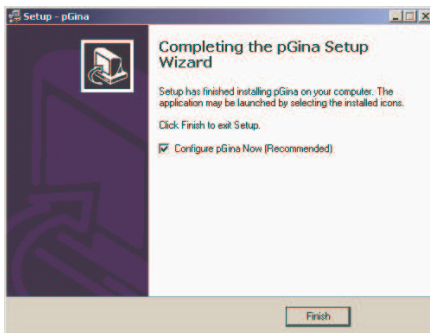
Ahora será presentado con la opción de dónde instalar pGina y los archivos necesarios. Puede seleccionar una ruta o carpeta diferente y presionar “Siguiente” para continuar a la Figura 5.

Puede elegir dónde en el menú de inicio de los usuarios actuales se creará el menú pGina. Después de elegir, seleccione “Siguiente” para continuar a la figura 6.



Esta pantalla le permite confirmar sus elecciones previas. Use el botón Atrás para regresar y cambiar algo. Después de seleccionar “Instalar”, todos los archivos necesarios serán desempaquetados e instalados en su sistema en la ubicación elegida.

Como regla la instalación por defecto trabajará sin configuración en la mayoría de los sistemas, sin embargo, no se recomienda que se salte la configuración antes de reiniciar. La Figura 7 muestra el diálogo final en el proceso de instalación.



Para saltarse la configuración, quite la marca en “Configurar pGina ahora” y seleccione “Terminar”. De otra manera seleccione “Terminar” para salir del instalador y ejecutar la utilidad de configuración.

Configurando pGina

Para configurar pGina, asegúrese de estar acreditado como administrador local o de que tiene privilegios administrativos completos, entonces ejecute el programa Configurar pGina yendo a Inicio -> Programas -> pGina -> Configurar pGina. Después de una breve pantalla de presentación, se mostrará un diálogo de configuración. A través de este diálogo puede cambiar la configuración y las opciones para pGina y su funcionamiento. Examinemos las opciones individuales y sus efectos sobre pGina.

CONFIGURACIÓN GENERAL

Las opciones más comúnmente usadas se encuentran en la tableta General. Esto incluye qué plugin usará pGina para la autenticación, las unidades que deben ser mapeadas para cada usuario, así como membresías grupales para todos los usuarios.

Opciones de plugin.

Para elegir o cambiar un plugin active el botón Explorar y localice el plugin de su elección. En la caja de “Información sobre el plugin elegido” se mostrará información sobre el plugin que elija. Si un plugin permite configuración adicional, el botón Configurar mostrará el diálogo.

Otras opciones.

También en la tableta General se encuentra la opción Mapeo de unidades. Si se configura, todas las unidades indicadas se mapearán para todos los usuarios que se autentifiquen exitosamente. Las unidades se especifican como UNIDAD:RUTA-UNC, por ejemplo, para el mapeo de la unidad J a \\juan\perez\tareas se hace como J:\\juan\perez\tareas. Se pueden especificar múltiples unidades separando las entradas con coma.

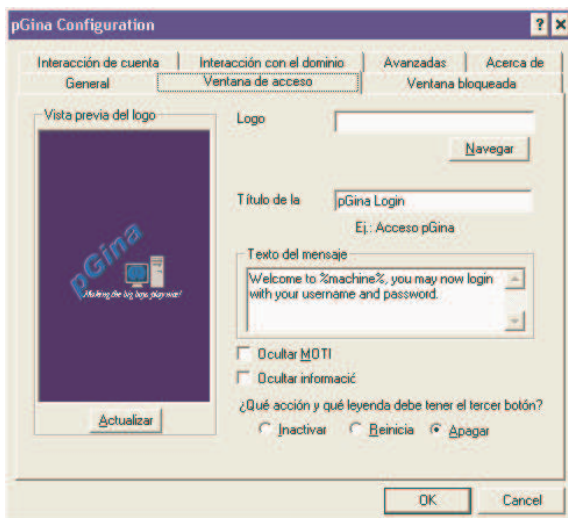
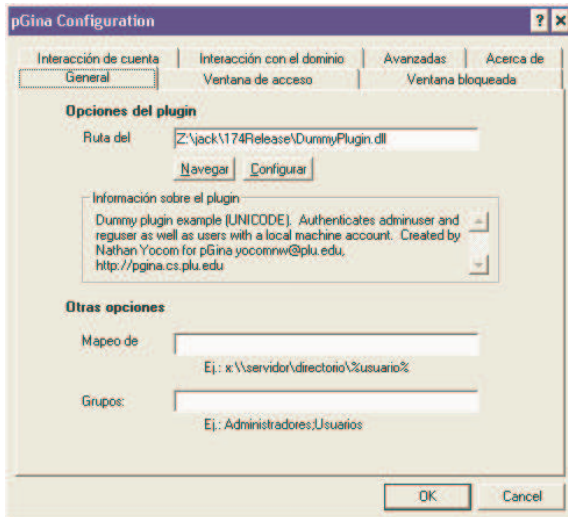
Adicionalmente, puede especificar un conjunto de grupos a los que todos los usuarios deben pertenecer. Esta lista toma la forma GRUPO1;GRUPO2. Por ejemplo, si todos los usuarios deben estar en los grupos Usuarios y Expertos, se debe escribir: “Usuarios;Expertos” sin las comas.

CONFIGURACIÓN DE LA VENTANA DE ENTRADA

Presionando en la tableta Ventana de acceso puede tener acceso a todas las opciones que afectan la apariencia y el comportamiento de la ventana de acceso.

Puede usar el botón explorar para buscar una imagen mapa de bits para usar como logo en la ventana de acceso. Una vez seleccionada, si es válida, la imagen se mostrará en la ventana de vista previa a la izquierda (si no, puede presionar el botón Actualizar para renovar la vista). Este espacio muestra el logo exactamente como aparecerá en la Ventana de acceso. Como referencia, el logo que viene incluido con pGina mide 100 pixels de ancho, 146 de alto y tiene una resolución de 300 x 300 a 24 bpp. Sólo son validas imágenes de mapa de bits.

La opción Título de la ventana le permite introducir un título particular para la ventana de acceso.



El texto del Mensaje del día se muestra arriba de las cajas de usuario y contraseña cuando se muestra la ventana de acceso. Por conveniencia, el texto %machine% es remplazado en tiempo de ejecución por el nombre de la máquina local (no el sufijo dns). Si elige ocultar el mensaje del día, no podrá editar el texto de arriba (y de todos modos no se mostrará).

La información del plugin como la que se muestra en la tableta General se muestra abajo de los campos usuario y contraseña. Si prefiere que tal información no se muestre, simplemente active la caja Ocultar información del plugin.

El tercer botón disponible en la ventana de acceso en la ejecución es configurable. Este botón puede desactivarse, reiniciar o apagar la máquina.

CONFIGURACIÓN DEL BLOQUEO DE VENTANA

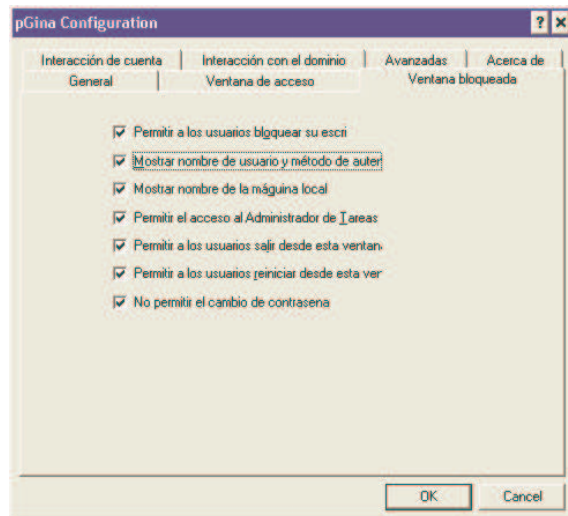
La ventana mostrada cuando un usuario autenticado intenta bloquear la máquina presionando CTRL+ALT+SUPR también es configurable.

Si **no** se activa, la opción “Permitir a los usuarios bloquear su escritorio” desactiva el botón Bloquear.

Si se activa, la segunda opción hace que se muestren el nombre de usuario y el método de autenticación (plugin, dominio, local).

La tercera opción permite que se muestre el nombre de la máquina local.

Si **no** se activa, la cuarta opción desactiva el botón Administrador de Tareas (aunque no impide atajos como CTRL+MAYUS+ESC).



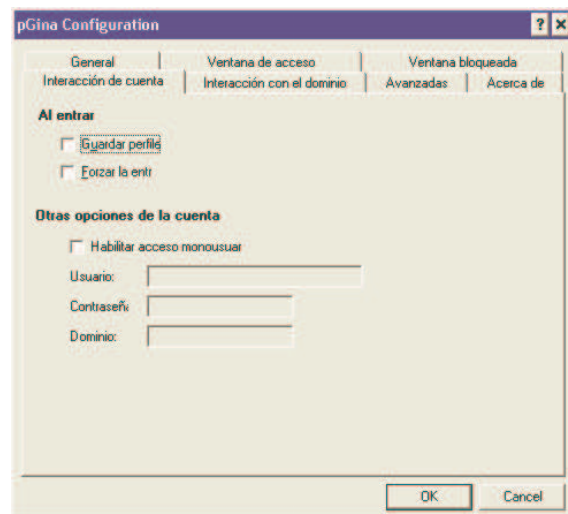
Las últimas dos opciones afectan la habilidad de los usuarios para reiniciar y terminar su sesión.

INTERACCIÓN DE CUENTA

Bajo circunstancias normales, pGina maneja los accesos creando cuentas locales que correspondan a los autenticados por el plugin. Esto resulta en la creación de un perfil en disco (de acuerdo a la política de la máquina y la configuración del perfil general). Es posible modificar este comportamiento usando la tableta Interacción de cuenta.

Cuando la opción Guardar perfiles está activada, la cuenta y el perfil en disco **no** son removidos al salir. Esto significa que los cambios al perfil son mantenidos entre accesos. Cuando **no** se activa, los perfiles y las cuentas locales son eliminados completamente de la máquina, resultando en un perfil nuevo (basado en el perfil por defecto, que es configurable en Windows) en cada acceso.

Siempre que Guardar perfiles esté activado, es posible que la contraseña de un usuario cambie, y esto resulte en un usuario que es autenticado por el plugin, pero que es inconsistente con la cuenta local. Cuando se activa la opción Forzar la entrada, se elimina este problema forzando la contraseña local a coincidir con aquella autenticada por el plugin en el acceso.

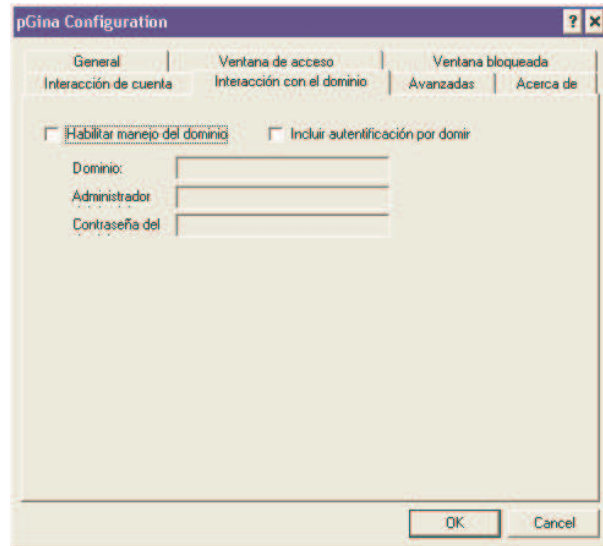


También está disponible la opción de acceso monousuario. Cuando se usa, el nombre de usuario y la contraseña dados (y el dominio si se introduce, o la máquina local de otra manera) son usados para acceder a la máquina, en lugar del nombre de usuario y la contraseña autenticados por el plugin. Esto permite basar el acceso a una sola cuenta basado en la habilidad para autenticar otra, por ejemplo autenticar con plugin y entonces acceder con una sola cuenta (sin necesidad de comprometer la contraseña de esa cuenta). Cuando se usa esta opción, las opciones Guardar perfiles y Forzar la entrada no tienen efecto.

INTERACCIÓN DE DOMINIO

pGina también tiene algunas opciones para interactuar de modos avanzados con una infraestructura de dominio existente. Aún cuando esta no fue la intención original de pGina, se ha vuelto una herramienta muy útil y necesaria en algunos casos. Cuando se activa la opción “Incluir autenticación por dominio”, el dominio introducido también se incluirá en la cadena de autenticación. Cuando este es el caso, pGina intentará primero autenticar con el plugin elegido, entonces con el dominio elegido, y al final con la máquina local.

Cuando la opción Habilitar manejo del dominio está activada pGina redireccionará su manejo de cuenta (ver la sección Interacción de cuenta) hacia el dominio introducido. Esto significa que las cuentas se crearán, eliminarán y serán manejadas tal y como pGina lo haría localmente. Desde la 1.7.4 esto requiere ya sea un servidor NT4 o un servidor Active Directory ejecutándose en modo mixto (se planea soporte AD puro para versiones futuras). Se requieren un nombre de usuario y una contraseña en el dominio, de manera que pGina pueda efectuar los cambios necesarios.



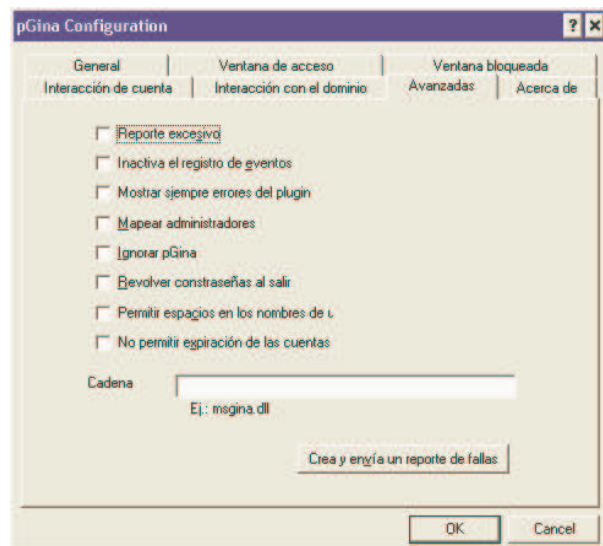
OPCIONES AVANZADAS

La última tableta de configuración disponible es la *tableta Avanzadas*.

La opción Reporte excesivo, cuando está activada, enciende el reporte para búsqueda de fallos que es enviado al registro de eventos y puede ser observado con la herramienta de administración de Windows Visor de eventos.

Si se activa la opción Desactivar todo reporte de eventos, se elimina todo la salida normal, así como la de búsqueda de errores. Esto evita el registro de cosas como eventos auditados.

La opción Mostrar siempre errores del plugin hace que se muestre un mensaje con cualquier error que el plugin haya encontrado *aun si la autenticación es exitosa con una cuenta local o de dominio. Si no se activa la opción, sólo se muestra un error si la autenticación falla completamente.*



Por defecto, pGina solamente aplica la configuración de mapeo de unidades a usuarios que son autenticados por el plugin elegido. Cuando se activa, la opción Mapear administradores hace el mapeo también se aplique a las cuentas de administradores locales.

Cuando se activa la opción Ignorar pGina, pGina se oculta y pasa todo el control al Gina normal de Microsoft, resultando en un comportamiento estándar de Gina de Windows.

A veces, el manejo deseado de perfiles es guardarlos con la opción Guardar perfiles de la sección interacción de cuenta. Sin embargo, el perfil que permanece en disco lo hace junto con la contraseña usada. Si la conexión de red es perdida, o el plugin falla la autenticación y el nombre de usuario local y la contraseña son usadas, entonces se permitirá el acceso. La opción Revolver contraseñas al salir permite la retención de las cuentas locales sin la inherente conservación del acceso local reiniciando la contraseña de la cuenta local a un valor aleatorio. Es **muy** importante que esta opción **sólo** se active cuando también se usa la opción Forzar contraseña. Si no se hace así, esto resultará en la incapacidad para acceder a las cuentas locales.

Algunos protocolos, tales como LDAP automáticamente ignoran los espacios al principio, cuando la opción “Permitir espacios en los nombres de usuario” **no** está activada, pGina no intentará la autenticación para nombres de usuario que sean introducidos con espacios.

Otras referencias

Artículo del soporte de Microsoft sobre creación de un perfil de usuario por defecto (“Setting up a custom default user profile”):

<http://support.microsoft.com/?kbid=305709>

Otra documentación de pGina

<http://pgina.xpasystems.com>

Foros de discusión en línea

<http://forums.xpasystems.com/>

Consultoría profesional, implementación y soporte

<http://www.xpasystems.com>

Listas de correo:

General: <http://lists.sourceforge.net/mailman/listinfo/pgina-general>

Actualizaciones: <http://lists.sourceforge.net/mailman/listinfo/pgina-updates>

Desarrolladores: <http://lists.sourceforge.net/mailman/listinfo/pgina-devel>

Otra documentación GINA

http://msdn.microsoft.com/library/en-us/security/security/winlogon_and_gina_start_page.asp