Single Sign-on 5.0

Jul 19, 2016

Acerca de

Oct 12, 2015

Novedades

Single Sign-on 5.0 integra el Single Sign-on Plug-in en Citrix Receiver, simplifica la experiencia de uso del usuario, permite la distribución de Single Sign-on Plug-in mediante Merchandising Server e incluye el chino simplificado como idioma respaldado por Single Sign-on Plug-in.

- **Los usuarios acceden al Single Sign-on Plug-in a través del icono de Citrix Receiver.** En lugar de ver uno o varios iconos de Single Sign-on Plug-in en el área de notificación de Windows, los usuarios sólo ven el icono de Citrix Receiver. El icono de Citrix Receiver aparece solo una vez en el área de notificación independientemente de cuántas sesiones de Single Sign-on tenga activas el usuario. Los usuarios administran la información de inicios de sesión, pueden poner en pausa y reanudar Single Sign-on, determinar si Single Sign-on está en pausa y enviar contraseñas manualmente usando las opciones de menú en el icono de Citrix Receiver.
  Nota: Si hay instaladas versiones más antiguas del plug-in, pueden aparecer iconos adicionales en el área de notificación de Windows. Consulte Instalación del Single Sign-on Plug-in para obtener más información.
- **Para usar la funcionalidad completa, es necesario que el Single Sign-on Plug-in esté en los dispositivos de usuario.** A menos que el Single Sign-on Plug-in esté instalado en los dispositivos de los usuarios, éstos no pueden administrar la información de inicios de sesión, poner en pausa y reanudar Single Sign-on, determinar si Single Sign-on está en pausa y enviar contraseñas manualmente. Para obtener más información, consulte Casos de distribución del software de Single Sign-on Plug-in.
- **Los usuarios salen del Single Sign-on Plug-in cuando salen de Citrix Receiver**. Los usuarios salen de Single Sign-on seleccionando la opción Salir en el menú del icono de Citrix Receiver. Esto cierra la interfaz de usuario de Citrix Receiver y todos los plug-ins a los que se acceda con ella.
- **Los usuarios administran su información de inicio de sesión usando la ventana Administrar contraseñas.** El Administrador de inicios de sesión se llama ahora ventana Administrar contraseñas y se ha rediseñado para simplificar su utilización:
  - Los usuarios acceden a la ventana Administrar contraseñas mediante una opción del menú del icono de Citrix Receiver. Una vez abierta la ventana Administrar contraseñas, esta muestra la información de inicio de sesión para las aplicaciones de todas las sesiones del usuario.
  - La ventana Administrar contraseñas se puede configurar para mostrar varias columnas con los atributos de las credenciales almacenadas: nombre, descripción, grupo, fecha y hora del último uso y fecha y hora de la última modificación. Los usuarios pueden ordenar el listado según cada uno de estos atributos.
  - La ventana Administrar contraseñas no contiene menús desplegables. La funcionalidad a la que antes se accedía usando las opciones en dichos menús del Administrador de inicios de sesión ahora ya no existe o se accede a ella de otra forma:

Menú	Opción	¿Qué ocurre con esta funcionalidad en Single Sign-on 5.0?
Archivo	Nuevo inicio de sesión o Nuevo inicio de sesión > Agregar un	Los usuarios guardan las credenciales manualmente usando el botón Enviar disponible en el menú del icono de Citrix Receiver.

Menú	Opción	¿Qué ocurre con esta funcionalidad en Single Sign-on 5.0?
	inicio de sesión	
	Nuevo inicio de sesión > Agregar varios inicios de sesión	Los usuarios crean varios conjuntos de credenciales para una misma aplicación creando el primer conjunto de credenciales y luego copiándolo y modificando la copia.
	Copiar	Sustituido por el botón Copiar de la ventana Administrar contraseñas.
	Eliminar	Sustituido por el botón Quitar de la ventana Administrar contraseñas.
	Properties	Sustituido por el botón Modificar de la ventana Administrar contraseñas.
	Salir	Los usuarios salen de la ventana Administrar contraseñas usando el botón de cerrar de Windows.
View	Icono, Lista y Detalles	Esta funcionalidad se ha eliminado para simplificar la experiencia del usuario.
	Organizar iconos por	Esta funcionalidad no está disponible, pero los usuarios pueden ordenar las columnas en la ventana Administrar contraseñas haciendo clic en el encabezado de las mismas.
	Refresh	Sustituido por el enlace Actualizar de la ventana Administrar contraseñas.
	Revelar contraseñas	Los usuarios ven una contraseña cada vez usando el botón Mostrar contraseña de la ventana Administrar contraseña. No pueden revelar más de una contraseña simultáneamente.
Herramientas	Asociación de cuentas	Los usuarios no pueden habilitar la asociación de cuentas usando el Single Sign-on Plug-in Para dar a los usuarios la capacidad de habilitar la asociación de cuentas, hay que darles acceso a la herramienta AccAssoc.exe como aplicación publicada.
	Registrar las preguntas de seguridad	Los usuarios no pueden registrar respuestas para las preguntas de seguridad usando el Single Sign-on Plug-in, a menos que se les pida que vuelvan a registrarlas. Para dar a los usuarios la capacidad de volver a registrar sus respuestas a las preguntas de seguridad sin solicitud previa, hay que darles acceso a la herramienta QBAEnroll.exe como aplicación publicada.

Menú	Opción	¿Qué ocurre con esta funcionalidad en Single Sign-on 5.0?
	Opciones > Confirmar el cierre	La confirmación de cierre se controla mediante Citrix Receiver. El Single Sign-on Plug-in no pide confirmación de cierre.
Help	Ayuda del Administrador de inicios de sesión	Sustituido por el enlace Ayuda de la ventana Administrar contraseñas.
	Acerca de	Sustituido por el enlace Acerca de en la ventana Administrar contraseñas.

- La ventana Administrar contraseñas no contiene menú contextual. La funcionalidad a la que antes se accedía con este menú en el Administrador de inicios de sesión tiene otro modo de acceso:

Opción	¿Qué ocurre con esta funcionalidad en Single Sign-on 5.0?
Copiar	Sustituido por el botón Copiar de la ventana Administrar contraseñas.
Eliminar	Sustituido por el botón Quitar de la ventana Administrar contraseñas.
Properties	Sustituido por el botón Modificar de la ventana Administrar contraseñas.

- **No se puede solicitar a los usuarios que guarden sus credenciales la primera vez que usan Single Sign-on.** La opción inicial de configuración de credenciales se ha eliminado.
- **El Single Sign-on Plug-in puede distribuirse y administrarse usando Merchandising Server.** Si Citrix Receiver Updater está instalado en los dispositivos de usuario, se puede distribuir y administrar el Single-Sign-on Plug-in usando Merchandising Server.
- **El Single Sign-on Plug-in puede instalarse en chino simplificado.**

Problemas conocidos

Consulte [Problemas conocidos de XenApp 6.5 para Windows Server 2008 R2] para obtener información sobre los problemas registrados en Single Sign-on 5.0.

Introducción

Oct 12, 2015

Los componentes principales de Single Sign-on son:

- El almacén central
- El componente de Single Sign-on en Citrix AppCenter
- El Single Sign-on Plug-in
- El servicio Single Sign-on Service (opcional)

El almacén central

El almacén central es un punto centralizado que utiliza Single Sign-on para almacenar y administrar los datos de usuario y datos administrativos. Los datos de usuario incluyen credenciales, respuestas a preguntas de seguridad y otros datos de usuario. Los datos de administración incluyen directivas de contraseña, definiciones de aplicación, preguntas de seguridad y otros datos de mayor alcance. Cuando un usuario inicia la sesión, Single Sign-on compara las credenciales del usuario con las almacenadas en el almacén central. A medida que el usuario abre las aplicaciones o las páginas Web protegidas por contraseña, se obtienen las credenciales adecuadas del almacén central.

El componente de Single Sign-on en Citrix AppCenter

El componente de Single Sign-on en Citrix AppCenter es el centro de mando de Single Sign-on. Aquí se configura el modo en que funciona Single Sign-on, las funciones que se instalan, las medidas de seguridad que se utilizan y otros parámetros importantes relacionados con las contraseñas.

El componente dispone de cuatro elementos principales, o nodos, en el panel izquierdo. Al seleccionar un nodo, aparecen las tareas específicas a dicho nodo. Los nodos son los siguientes:

- Configuraciones de usuario: permite ajustar parámetros para los usuarios según su ubicación geográfica o la función que desempeñan dentro de la empresa.
- Definiciones de aplicación: proporcionan la información necesaria para que el Single Sign-on Plug-in suministre credenciales de usuario a las aplicaciones y detecte los errores que puedan producirse. Puede utilizar las plantillas de definición de aplicación suministradas con Single Sign-on para acelerar este proceso, o también puede crear definiciones personalizadas para las aplicaciones con las que no sea posible utilizar plantillas.
- Directivas de contraseña: controlan la longitud de las contraseñas y el tipo y variedad de los caracteres que pueden emplearse tanto en las contraseñas definidas por el usuario como en las generadas automáticamente. Las directivas de contraseña también permiten especificar caracteres cuyo uso se desea excluir de las contraseñas y permite decidir si se puede o no utilizar contraseñas anteriores. La creación de directivas de contraseña coherentes con las directivas de seguridad de la empresa garantiza que Single Sign-on administrará correctamente la seguridad de las contraseñas.
- Verificación de la identidad: permite crear preguntas de seguridad que proporcionan una capa de seguridad adicional para el Single Sign-on Plug-in. Las preguntas de seguridad protegen contra la suplantación de usuarios, los cambios de contraseña no autorizados y el desbloqueo de cuentas no autorizado. Los usuarios que se inscriben y contestan las preguntas de seguridad pueden verificar su identidad ingresando las respuestas correctas. Una vez verificados, los usuarios pueden llevar a cabo tareas de autoservicio en sus cuentas, tales como el restablecimiento de su contraseña primaria o el desbloqueo de su cuenta de usuario. Las preguntas de seguridad también se pueden usar para recuperar claves.

El Single Sign-on Plug-in

El Single Sign-on Plug-in envía las credenciales apropiadas a las aplicaciones que se ejecutan en el dispositivo cliente del

usuario, aplica las directivas de contraseña, proporciona las funciones de autoservicio y permite que los usuarios administren sus credenciales en la ventana Administrar contraseñas (antes conocida como Administrador de inicios de sesión). Además, el plug-in proporciona a los usuarios una serie de funciones que vienen determinadas por los parámetros administrativos que se hayan definido en las configuraciones de usuario.

El servicio Single Sign-on Service

El servicio Single Sign-on Service se ejecuta en un servidor Web que constituye la base de las funciones opcionales incluidas en esta versión. Es necesario instalar Single Sign-on Service si se piensa utilizar al menos uno de los siguientes módulos:

- Autoservicio de cuentas, que permite a los usuarios restablecer sus contraseñas de Windows y desbloquear sus cuentas de Windows
- Integridad de datos, que garantiza la seguridad de los datos en tránsito entre el almacén central y el Single Sign-on Plug-in
- Administración de claves, que le brinda a los usuarios la capacidad de recuperar sus credenciales secundarias cuando la contraseña primaria cambia usando la recuperación de claves automática o respondiendo a las preguntas de seguridad con la autenticación con preguntas
- Aprovisionamiento, que permite utilizar el componente de Single Sign-on en Citrix XenApp para agregar, eliminar o actualizar los datos de usuario y la información de credenciales de Single Sign-on
- Sincronización de credenciales, que sincroniza las credenciales de usuario entre varios dominios mediante un servicio Web

Si no va a utilizar ninguno de estos módulos, no instale el servicio Single Sign-on Service.

Evaluación

Oct 12, 2015

Si utiliza XenApp 6.5 para Windows Server 2008 R2 para publicar aplicaciones y desea utilizar Single Sign-on 5.0 para proporcionar seguridad de contraseñas y acceso mediante Single Sign-on a esas aplicaciones, este tema ayuda a implementar de forma rápida Single Sign-on. La implementación de Single Sign-on que se describe en este documento puede utilizarse para evaluar Single Sign-on o como una implementación piloto que se puede ampliar para incluir más usuarios y aplicaciones.

Nota: Para simplificar el proceso de implementación, los pasos descritos en este documento excluyen algunos componentes, funciones y opciones que se encuentran disponibles cuando se utiliza Single Sign-on 5.0 con XenApp 6.5.
La implementación que se describe en este documento incluye los siguientes componentes de Single Sign-on:

- **Almacén central.** El almacén central es un punto centralizado que utiliza Single Sign-on para almacenar y administrar los datos de usuario y datos administrativos. Los datos de usuario incluyen credenciales, respuestas a preguntas de seguridad y otros datos de usuario. Los datos de administración incluyen directivas de contraseña, definiciones de aplicación, preguntas de seguridad y otros datos de mayor alcance. Cuando un usuario inicia la sesión, Single Sign-on compara las credenciales del usuario con las almacenadas en el almacén central. A medida que el usuario abre las aplicaciones o las páginas Web protegidas por contraseña, se obtienen las credenciales adecuadas del almacén central.
- **Componente de Single Sign-on en Citrix AppCenter.** En esta implementación, es posible utilizar el componente de Single Sign-on en Citrix AppCenter para definir directivas de contraseña, configurar Single Sign-on de modo que reconozca aplicaciones y crear configuraciones de usuario.
- **Herramienta de definición de aplicaciones.** La herramienta de definición de aplicaciones ofrece las mismas funciones que la parte del componente de Single Sign-on en Citrix AppCenter que configura Single Sign-on para el reconocimiento de aplicaciones.
- **Single Sign-on Plug-in.** Single Sign-on Plug-in es el componente de Single Sign-on con el que interactúan los usuarios. Este plug-in envía las credenciales adecuadas a las aplicaciones que se ejecutan en el dispositivo cliente de cada usuario, aplica las directivas de contraseña y permite que los usuarios administren sus credenciales con la ventana Administrar contraseñas. En esta implementación, el plug-in se instala en cada dispositivo de usuario.

Esta implementación no incluye Single Sign-on Service ni las funciones opcionales que admite:

- Autoservicio, que permite que los usuarios restablezcan sus contraseñas de Windows y desbloqueen sus cuentas de Windows.
- Integridad de datos, que garantiza la seguridad de los datos en tránsito entre el almacén central y Single Sign-on Plug-in.
- La administración de claves, que le brinda a los usuarios la capacidad de recuperar sus credenciales secundarias cuando la contraseña primaria cambia usando la recuperación de claves automática o respondiendo a las preguntas de seguridad con la autenticación con preguntas.
- Aprovisionamiento, que permite utilizar el componente de Single Sign-on de Citrix AppCenter para agregar, eliminar o actualizar los datos de usuario y la información de credenciales de Single Sign-on.
- Sincronización de credenciales, que sincroniza las credenciales de usuario entre varios dominios mediante un servicio Web.

Realice las tareas de este tema en el orden en que aparecen las secciones aquí.

Planificación de la implementación

- Revise los requisitos del sistema para el almacén central, el componente de Single Sign-on en AppCenter, la herramienta de definición de aplicaciones y el plug-in: Requisitos del sistema.
- Revise los requisitos de licencias para Single Sign-on, instale y actualice las licencias si es necesario: Requisitos del sistema.

- Identifique las aplicaciones que desea incluir. En esta implementación, elija solamente aplicaciones Web y de Windows publicadas con XenApp.
  - En las aplicaciones de Windows, utilice aplicaciones de Windows de 32 bits (incluidas las aplicaciones Java) como Microsoft Outlook, Lotus Notes, SAP o cualquier aplicación de Windows habilitada para contraseña. Single Sign-on clasifica las aplicaciones iniciadas mediante un archivo con la extensión .exe como aplicaciones de Windows.
  - En las aplicaciones Web, utilice aplicaciones Web (incluidos los applets de Java y SAP) a las que se acceda mediante Microsoft Internet Explorer. Por lo general, Single Sign-on clasifica las aplicaciones que se ejecutan en un explorador como aplicaciones Web. Single Sign-on es compatible con aplicaciones Web que se ejecutan en las versiones 6.0, 7.0, 8.0 y 9.0 de Internet Explorer.
- Identifique los usuarios que desea incluir. Asegúrese de que los dispositivos de usuario admitan Single Sign-on Plug-in.
- Decida la ubicación en la que desea instalar el almacén central. El almacén central para esta implementación es un punto compartido de red NTFS.
- Decida la ubicación en la que desea instalar el componente de Single Sign-on de Citrix AppCenter. Puede utilizar una instancia de AppCenter que ya se encuentre instalada o instalar una instancia nueva de AppCenter.
- Decida si planea instalar la herramienta de definición de aplicaciones y la ubicación en la que desea instalarla. Si Citrix AppCenter no se encuentra instalado en el equipo que ejecuta la aplicación que desea incluir en la implementación, instale la herramienta de definición de aplicaciones en ese equipo. Cuando se configura Single Sign-on para que reconozca aplicaciones, se ejecutan las aplicaciones y se permite que los asistentes de la herramienta capturen información acerca de las aplicaciones.
- Planifique las directivas de contraseña. Las directivas de contraseña son reglas que controlan la forma en que se crean, envían y administran las contraseñas; es posible aplicar directivas de contraseña a todos los usuarios o a grupos específicos de aplicaciones. Single Sign-on incluye dos directivas de contraseña estándar llamadas Predeterminada y Dominio. Si los valores predeterminados de estas directivas estándar cumplen con los requisitos para esta implementación, puede utilizarlas sin modificación alguna. De lo contrario, puede crear nuevas directivas en función de esas directivas y modificar esos valores.
  - Para obtener una descripción general de las directivas de contraseña, consulte Directivas de contraseña.
  - Para obtener instrucciones sobre cómo lograr que las directivas de contraseña sean seguras y se puedan utilizar, consulte Directivas de contraseña.
  - Para comprender cómo aplica Single Sign-on las directivas de contraseña, consulte Cumplimiento de requisitos de contraseña.
  - Para determinar si los valores predeterminados de las reglas de las directivas de contraseña son adecuados para las aplicaciones y los usuarios, revise los valores predeterminados para cada parámetro en el tema de referencia Directivas de contraseña y todos sus subtemas. Las directivas de contraseña estándar (Predeterminada y Dominio) contienen estos valores predeterminados.
- Planifique las configuraciones de usuario. Las configuraciones de usuario son conjuntos únicos de parámetros, directivas de contraseña y aplicaciones que se aplican a los usuarios asociados a una jerarquía de Active Directory (unidad organizativa o usuario individual) o a un grupo de Active Directory. Las configuraciones de usuario permiten controlar el comportamiento y el aspecto del software del plug-in para usuarios.
  - Para obtener una visión general de las configuraciones de usuario y ver los parámetros de configuración de usuario utilizados en esta implementación con sus valores predeterminados, consulte Referencia de parámetros de configuración de Single Sign-on 5.0. Tenga en cuenta que algunas opciones y funciones analizadas en ese tema no se utilizan en esta implementación. Esta visión general incluye la siguiente información:
    - Interacción básica con el plug-in
    - Interfaz de usuario del plug-in
    - Sincronización

      Nota: No seleccione la opción Permitir acceso a credenciales de usuario a través del módulo de sincronización Esta

implementación de configuración de usuario no incluye el módulo de sincronización de credenciales.
    - Respaldo de aplicaciones
    - Licencias
- Para proteger las credenciales de los usuarios, consulte Métodos de protección de datos.
  Nota: Utilice los valores predeterminados para los parámetros de protección de datos secundaria. Otros valores requieren el módulo de administración de claves que no se incluye en esta implementación.
  En esta implementación, es posible utilizar los parámetros de configuración de usuario predeterminados (excepto los parámetros de licencias) de forma inicial en la mayoría de los entornos. Si los requisitos cambian cuando la implementación ya está en uso, es posible editar los valores de configuración de usuario.

  De forma predeterminada, los parámetros para las funciones que no se utilizan en esta implementación se encuentran inhabilitados.

Creación del almacén central

El almacén central de Single Sign-on puede ser de dos tipos: punto compartido de red NTFS o Active Directory. En esta implementación, se debe crear un punto compartido de red NTFS, ya que requiere menos permisos de creación que un almacén central de Active Directory. Para ver las ventajas y consideraciones de un almacén central de punto compartido de red NTFS, consulte Selección de un punto compartido NTFS.

Si es necesario, puede migrar los usuarios a un almacén central de Active Directory posteriormente.

Para crear un almacén central de punto compartido de red NTFS:

1. Cargue el medio de instalación de XenApp.
2. En el menú de Autorun, seleccione Instalar componentes manualmente > Componentes de servidor > Funciones adicionales > Single Sign-on.
3. Seleccione Almacén central.
4. Seleccione Punto compartido NTFS.

El almacén central se creará como %SystemDrive%\CITRIXSYNC$.

Instalación del componente de Single Sign-on de AppCenter

De forma predeterminada, AppCenter incluye el componente de Single Sign-on cuando se instala.

Para utilizar una instancia de AppCenter existente con Single Sign-on, configure y ejecute el descubrimiento después de crear el almacén central.

Para instalar una nueva instancia de AppCenter a fin de utilizarla con Single Sign-on, asegúrese de que los paquetes redistribuibles Microsoft Visual C++ Redistributable Package y los ensamblados de interoperabilidad primarios de Microsoft se encuentren instalados, como se describe en Requisitos del sistema.

Para instalar AppCenter:

1. Cargue el medio de instalación de XenApp en el equipo.
2. En el menú de Autorun, haga clic en Instalar componentes manualmente > Componentes comunes > Consolas de administración. Siga las instrucciones.
3. Seleccione Configurar y ejecutar descubrimiento y siga las instrucciones.

Una vez realizada la configuración, el componente de Single Sign-on en AppCenter se conecta con el almacén central y es posible utilizarlo para definir directivas de contraseña, configurar Single Sign-on de modo que reconozca aplicaciones y crear

configuraciones de usuario.

Instalación de la herramienta de definición de aplicaciones

Si Citrix AppCenter no se encuentra instalado en el equipo que ejecuta la aplicación que desea incluir en la implementación, instale la herramienta de definición de aplicaciones para crear definiciones de aplicación para la aplicación.

1. Cargue el medio de instalación de XenApp en el equipo.
2. Busque el archivo ASC_PasswordManager en la carpeta Administration y ejecútelo.
3. Seleccione Herramienta de definición de aplicaciones. Siga las instrucciones.

Definición de directivas de contraseña

Si ha determinado que los valores predeterminados para las directivas de contraseña estándar cumplen con las necesidades para esta implementación, no es necesario que defina ninguna directiva adicional. De lo contrario, cree nuevas directivas en función de las directivas estándar.

Para crear una nueva directiva de contraseña:

1. Haga clic en Inicio > Todos los programas > Citrix > Consolas de administración > Citrix AppCenter.
2. Expanda el nodo Single Sign-On y seleccione Directivas de contraseña.
3. En el menú Acción, haga clic en Crear nueva directiva de contraseña.
4. Siga las instrucciones del Asistente de directivas de contraseña.

Configuración de Single Sign-On para que reconozca aplicaciones

Single Sign-on reconoce y responde a aplicaciones basadas en los parámetros identificados en definiciones de aplicación. Las definiciones de aplicación proporcionan la información necesaria para que Single Sign-On Plug-in suministre credenciales de usuario a las aplicaciones y detecte posibles errores.

Las definiciones de aplicación están compuestas por definiciones de formulario. Las definiciones de formulario permiten que Single Sign-on Plug-in analice cada aplicación a medida que se inicia, reconozca determinadas características de identificación y determine si la aplicación iniciada requiere que el plug-in lleve a cabo alguna acción específica, como:

- Enviar credenciales de usuario en una petición de inicio de sesión
- Negociar una interfaz de cambio de credenciales
- Procesar una interfaz de confirmación de credenciales

Aunque la mayoría de las aplicaciones y sus correspondientes definiciones utilizan únicamente dos formularios para administrar las credenciales de usuario, es posible definir tantos formularios como necesite una aplicación.

Es posible crear estos tipos de formularios de administración de credenciales de usuario:

- Formulario de inicio de sesión
  Identifica la interfaz de inicio de sesión para una aplicación y administra las acciones necesarias para obtener acceso a la aplicación asociada.

- Formulario de cambio de contraseñas
  Identifica la interfaz de cambio de contraseña para una aplicación y administra las acciones necesarias para cambiar la contraseña de usuario de la aplicación asociada.

- Formulario de cambio de contraseñas satisfactorio
  Identifica la interfaz de cambio de contraseña para una aplicación y administra las acciones necesarias para reconocer el cambio de contraseña satisfactorio para la contraseña de usuario de la aplicación asociada.

- Formulario de cambio de contraseñas fallido
  Identifica la interfaz de cambio de contraseña incorrecto de una aplicación y define las acciones que se deben llevar a cabo cuando una operación de cambio de credenciales no se realiza correctamente.

Las definiciones de aplicación se crean mediante los asistentes disponibles en AppCenter o la herramienta de definición de aplicaciones. Cuando la aplicación que desee definir se encuentre en ejecución o disponible en una ventana del explorador, estos asistentes lo ayudarán a capturar la información que necesite para la definición de aplicación. Para crear una definición de aplicación, se debe poder acceder a ella desde el equipo donde se crea la definición de la aplicación.

Dado que las firmas de aplicación pueden variar según el sistema operativo subyacente, es necesario probar las definiciones de aplicación en todos los sistemas operativos en los que se ejecutarán.

Hay plantillas de aplicación disponibles para algunas aplicaciones. Estas plantillas simplifican el proceso de incorporación de definiciones de aplicación a la implementación de Single Sign-on, ya que suministran la mayor parte de la información necesaria para crear una definición de aplicación. Para obtener más información sobre plantillas de aplicaciones, consulte Plantillas de aplicaciones.

Para crear una definición de aplicación de Windows

Para crear definiciones de aplicación para una aplicación de Windows, ejecute la aplicación en un equipo en el cual inicie el Asistente de definición de aplicaciones desde la instancia de Citrix AppCenter de la herramienta de definición de aplicaciones. Se debe navegar hasta el formulario dentro de la aplicación que requiere un suceso de administración de credenciales de usuario (inicio de sesión de usuario, cambio de contraseñas, cambio de contraseñas satisfactorio o cambio de contraseñas fallido) mientras se ejecuta el asistente.

Para obtener una descripción general de las consideraciones para las definiciones de aplicación de Windows, consulte Definiciones de aplicación de tipo Windows.

1. Inicie la aplicación.
2. Prepárese para iniciar el Asistente de definición de aplicaciones.
   - En AppCenter: haga clic en Inicio > Todos los programas > Citrix > Consolas de administración > Citrix AppCenter. Expanda el nodo Single Sign-On y seleccione Definiciones de aplicación.
   - En la herramienta de definición de aplicaciones (desde AppCenter): haga clic en Inicio > Todos los programas > Citrix > Single Sign-On > Herramienta de definición de aplicaciones.
3. Seleccione Crear una definición de aplicación.
4. Asegúrese de que las opciones Windows y Crear nueva estén seleccionadas y haga clic en Iniciar el asistente
5. Especifique el nombre de la aplicación como desea que aparezca en el almacén central. De manera opcional, especifique una descripción. Haga clic en Siguiente.
6. Haga clic en Agregar formulario. Esto iniciará el Asistente de definición de formularios.
7. Si todavía no lo ha hecho, navegue hasta el formulario de inicio de sesión de usuario, cambio de contraseñas, cambio de contraseñas satisfactorio o cambio de contraseñas fallido de la aplicación.
8. En la página Identificar el formulario del Asistente definición de formularios, haga clic en Seleccionar.
9. En el selector de ventanas que aparece, seleccione la aplicación para la cual desea crear la definición. Aparecerá un borde parpadeante alrededor del símbolo de la aplicación.
10. En la página Nombrar formulario, especifique un nombre para el formulario y seleccione el tipo de formulario. Haga clic en Siguiente.
11. En el selector de ventanas, haga clic en Aceptar.
12. En la página Identificar el formulario, haga clic en Siguiente.

13. En la página Definir las acciones del formulario, configure los campos de credenciales y los botones que desea que aparezcan en el formulario:
    1. Haga clic en el hipervínculo Configurar/Cambiar asociado a una credencial de usuario específica. Esta acción abre el cuadro de diálogo Configurar el texto del control que se utiliza para identificar el control que recibirá la credencial seleccionada.
    2. Se debe seleccionar el candidato de tipo de control para recibir la credencial. A medida que se seleccionan los diferentes candidatos, el tipo de control asociado se resalta en la aplicación con un borde parpadeante.
    3. Esta acción se debe repetir para todas las credenciales que necesita el formulario y para el botón requerido para enviar el formulario.
       Algunos formularios requieren dominios u otras credenciales configurables por el usuario que se deben enviar correctamente para procesar el formulario. Para respaldar estos requisitos, hay dos campos personalizados disponibles. Asigne las credenciales de requisitos especiales a estos campos. Los nombres asociados a estos campos se definen en la página Dar nombres a los campos personalizados del Asistente de definición de aplicaciones.

       Nota: No es necesario configurar todas las credenciales identificadas en la parte superior de la página Definir las acciones del formulario.
14. Si la aplicación requiere formularios adicionales, utilice los asistentes para crearlos.

Para crear una definición de aplicación Web

Para crear definiciones de aplicación para una aplicación Web, ejecute la aplicación en un equipo en el cual inicie el Asistente de definición de aplicaciones desde la instancia de Citrix AppCenter de la herramienta de definición de aplicaciones. Se debe navegar hasta el formulario dentro de la aplicación que requiere un suceso de administración de credenciales de usuario (inicio de sesión de usuario, cambio de contraseñas, cambio de contraseñas satisfactorio o cambio de contraseñas fallido) mientras se ejecuta el asistente.

1. Inicie la aplicación.
2. Prepárese para iniciar el Asistente de definición de aplicaciones.
    - En AppCenter: haga clic en Inicio > Todos los programas > Citrix > Consolas de administración > Citrix AppCenter. Expanda el nodo Single Sign-On y seleccione Definiciones de aplicación.
    - En la herramienta de definición de aplicaciones (desde AppCenter): haga clic en Inicio > Todos los programas > Citrix > Single Sign-On > Herramienta de definición de aplicaciones.
3. Seleccione Crear una definición de aplicación.
4. Asegúrese de que las opciones Web y Crear nueva estén seleccionadas y haga clic en Iniciar el asistente.
5. En la página Identificar la aplicación, especifique el nombre de la aplicación como desea que aparezca en el almacén central. De manera opcional, especifique una descripción. Haga clic en Siguiente.
6. Haga clic en Agregar formulario. Esto iniciará el Asistente de definición de formularios.
7. En la página Nombrar formulario, haga clic en Siguiente.
    1. Introduzca un nombre para el formulario.
    2. Seleccione el tipo de formulario.
    3. Asegúrese de que la opción Sin acciones especiales esté seleccionada.
    4. Haga clic en Siguiente.
8. Si todavía no lo ha hecho, navegue hasta el formulario de inicio de sesión de usuario, cambio de contraseñas, cambio de contraseñas satisfactorio o cambio de contraseñas fallido de la aplicación.
9. En la página Identificar el formulario, haga clic en Seleccionar. Se iniciará el Asistente de formularios Web.
10. En el selector de página Web que aparece, seleccione la aplicación para la cual desea crear la definición. Haga clic en Aceptar. Aparecerá un borde parpadeante alrededor de la página Web donde se mostrará el formulario de credenciales

de la aplicación.

11. Especifique un nombre para el formulario y seleccione el tipo de formulario. Haga clic en Siguiente.
12. En la página Identificar el formulario, hay dos casillas disponibles para administrar el modo en que se interpretan las direcciones URL identificadas. Seleccione la casilla adecuada y haga clic en Siguiente.
    - Coincidencia estricta de URL
      Esta casilla de verificación se selecciona para reconocer únicamente los sucesos de administración de credenciales de usuario de las aplicaciones Web que se inician mediante las URL especificadas. Algunas URL pueden contener datos dinámicos como identificadores de administración de sesión, parámetros de aplicación u otros identificadores que pueden cambiar por cada instancia. En estas circunstancias, el uso de coincidencia estricta puede provocar que no se reconozca la URL.

    - Reconocer mayúsculas en URL
      Esta casilla de verificación se selecciona para utilizar URL con coincidencia exacta de mayúsculas y minúsculas.

13. En la página Definir las acciones del formulario, configure los campos de credenciales y los botones que desea que aparezcan en el formulario:
    1. Haga clic en el hipervínculo Configurar/Cambiar asociado a una credencial de usuario específica. Esta acción abre el cuadro de diálogo Configurar el texto del campo que se utiliza para identificar el campo que recibirá la credencial seleccionada. Si el formulario ya está abierto, este cuadro de diálogo muestra todos los candidatos posibles para el tipo de campo asociado a la credencial de usuario u opción de envío seleccionada.
    2. Si el formulario de credenciales de la aplicación no está abierto actualmente, inicie la aplicación y acceda al formulario de credenciales de usuario correcto. Después, seleccione Actualizar . Después de haber seleccionado el formulario de aplicación, a este cuadro de diálogo se incorporan los candidatos de tipo de control que son adecuados para la credencial de usuario seleccionada.
    3. Seleccione el candidato de tipo de campo para recibir la credencial. A medida que se seleccionan los distintos candidatos, el tipo de campo asociado aparece resaltado visiblemente en la aplicación para facilitar la identificación del tipo de campo que recibirá la credencial de usuario o botón de envío que se ha identificado.
    4. Esta acción se debe repetir para todas las credenciales que necesita el formulario y para el botón requerido para enviar el formulario.
       Algunos formularios requieren dominios u otras credenciales configurables por el usuario que se deben enviar correctamente para procesar el formulario. Para respaldar estos requisitos, hay dos campos personalizados disponibles. Asigne las credenciales de requisitos especiales a estos campos. Los nombres asociados a estos campos se definen en la página Dar nombres a los campos personalizados del Asistente de definición de aplicaciones.

       Nota: No es necesario configurar todas las credenciales identificadas en la parte superior de la página Definir las acciones del formulario.
14. Si la aplicación requiere formularios adicionales, utilice los asistentes para crearlos.

Para agregar una definición de aplicación para una aplicación con una plantilla disponible

El Asistente de definición de aplicaciones ayuda a ubicar las plantillas de aplicación y agregarlas a la implementación.

1. Prepárese para iniciar el Asistente de definición de aplicaciones.
   - En AppCenter: haga clic en Inicio > Todos los programas > Citrix > Consolas de administración > Citrix AppCenter. Expanda el nodo Single Sign-On y seleccione Definiciones de aplicación.
   - En la herramienta de definición de aplicaciones (desde AppCenter): haga clic en Inicio > Todos los programas > Citrix > Single Sign-On > Herramienta de definición de aplicaciones.

2. Seleccione Administrar plantillas.
3. Consulte la lista de plantillas para ver si la aplicación deseada aparece. También puede hacer clic en el enlace para descargar más aplicaciones de la Web e importarlas a la lista.
4. Seleccione la plantilla de aplicación que desee agregar y haga clic en Crear una definición de aplicación.
5. Utilice el asistente para editar los formularios para la aplicación o acepte los valores predeterminados.

Creación de configuraciones de usuario

1. Haga clic en Inicio > Todos los programas > Citrix > Consolas de administración > Citrix AppCenter.
2. Expanda el nodo Single Sign-On y seleccione Configuraciones de usuario.
3. Haga clic en Agregar configuración de usuario nueva.
4. Especifique el nombre de la aplicación como desea que aparezca en el almacén central. De manera opcional, especifique una descripción.
5. Especifique la forma en la que desea asociar esta configuración de usuario con los usuarios.
   Existen dos posibilidades: asociar usuarios según una jerarquía de Active Directory (unidad organizativa o usuario individual) o según un grupo de Active Directory. Si es necesario, se puede asociar la configuración de usuario a otra jerarquía o grupo posteriormente, haciendo clic en Mover configuración de usuario en el menú Acción.

   Importante: El modo en que se organice el entorno de Active Directory puede afectar al funcionamiento de las configuraciones de usuario. Si se utilizan ambos (jerarquía y grupo de Active Directory) y un usuario se encuentra en ambos contenedores, tiene prioridad la configuración de usuario asociada a la jerarquía y es la que se utiliza. Este esquema se considera un entorno mixto.
   Además, si un usuario pertenece a dos grupos de Active Directory y cada uno está asociado a una configuración de usuario, se antepone la que tenga mayor prioridad y es la que se utiliza.

   La asociación de configuraciones de usuario a grupos sólo se admite en dominios de Active Directory que utilizan la autenticación de Active Directory.

6. En la página Elegir aplicaciones, agregue las aplicaciones para la configuración de usuario. Al hacer clic en el botón Agregar, aparece un cuadro de diálogo y muestra las definiciones de aplicación que se han creado anteriormente.
7. Utilice la página Configurar la interacción con Single Sign-on Plug-in para determinar la experiencia de todos los usuarios de software del plug-in en el entorno.
8. Seleccione un servidor de licencias y un modelo de licencia en la página Configurar las licencias.
9. Utilice la página Seleccionar los métodos de protección de datos para seleccionar los métodos de protección de datos destinados a proteger las credenciales de usuario en función de los diversos métodos de autenticación que los usuarios están autorizados a utilizar.

Instalación de Single Sign-on Plug-in

El Single Sign-on Plug-in se ejecuta en el servidor XenApp y suministra credenciales y acceso a las aplicaciones publicadas. El plug-in también se ejecuta en cada dispositivo de usuario, envía las credenciales a las aplicaciones y permite que los usuarios administren sus credenciales.

Consideraciones acerca de la instalación:

- Después de instalar el plug-in en un sistema operativo compatible que esté usando el componente Microsoft Graphical Identification and Authentication (GINA) de Windows es necesario reiniciar el equipo. Esto incluye Windows XP, Microsoft Windows XP Embedded, Microsoft Windows Fundamentals for Legacy PCs, Microsoft Windows Server 2003 R2 y Microsoft Windows Server 2003 con Service Pack 2.
  WinLogon utiliza los controles GINA para el cuadro de diálogo que los usuarios ven cuando presionan la combinación de

teclas CTRL + ALT + SUPR. El cuadro de diálogo obtiene los datos necesarios para realizar la autenticación. XenApp, Single Sign-on Plug-in y el cliente de Novell NetWare interactúan con Microsoft GINA o requieren el reemplazo de su biblioteca DLL. Es posible que tenga que instalar o desinstalar software en un orden específico para conservar la cadena GINA correcta. Instalando el Single Sign-on Plug-in en último lugar, se garantiza que el proceso Winlogon invoque a la GINA de Single Sign-on en primer lugar.

- Una vez finalizada la instalación (y después de reiniciarse el dispositivo, si es necesario) el icono de Citrix Receiver aparecerá en la bandeja del sistema.
- Después de instalar el plug-in, si se configura o se cambia la información de licencias de Citrix hay que reiniciar el plug-in para aplicar esos cambios.

Para instalar Single Sign-on Plug-in en un dispositivo de usuario o en un servidor con XenApp instalado:

1. Cargue el medio de instalación de XenApp en el equipo o en el servidor.
2. En el menú de Autorun, seleccione Instalar componentes manualmente > Componentes de servidor > Funciones adicionales > Single Sign-on > Single Sign-on Plug-in.
3. Siga las instrucciones.

Introducción de los usuarios al uso de Single Sign-on

Antes de que los usuarios finales comiencen a usar Single Sign-on, revise la Ayuda para usuarios finales disponible mediante la interfaz de Single Sign-on. Informe a los usuarios sobre la forma en que funciona Single Sign-on y las funciones a las que pueden acceder en esta implementación.

Requisitos del sistema

Oct 12, 2015

Los equipos del entorno de Single Sign-on requieren el siguiente software de sistema:

Componente de software	Necesario para	Disponible en...
Microsoft Windows Installer 3.0 o posterior (se incluye automáticamente durante la instalación con Autorun)	Todas	• Carpeta Support que se encuentra en el medio de instalación de Single Sign-on • http://www.microsoft.com
Microsoft .NET Framework 3.5 Service Pack 1 (incluido automáticamente durante la instalación con Autorun)	• Servicio de inicio de sesión único • Componente de Single Sign-on en AppCenter • Herramienta de definición de aplicaciones	Carpeta Support que se encuentra en el medio de instalación de Single Sign-on
Microsoft Internet Explorer versión 6.0, 7.0, 8.0 ó 9.0 (modo no protegido)	Los usuarios que acceden a aplicaciones Web habilitadas para Single Sign-on	http://www.microsoft.com
ASP.NET	Servicio de inicio de sesión único	http://www.asp.net/

• Para equipos de 32 bits: Microsoft Visual C++ 2005 Redistributable Package (x86) Service Pack 1
  • vc80_vcredist_x86.exe
• Para equipos de 64 bits: Microsoft Visual C++ 2005 Redistributable Package (x64) Service Pack 1
  • vc80_vcredist_x86.exe
  • vc80_vcredist_x64.exe
	Componente de consola, servicio o plug-in de Single Sign-on: al instalar el componente de consola, el servicio o el plug-in desde una interfaz de comandos en un equipo con Windows Vista, Windows Server 2008 o Windows Server 2008 R2	Carpeta Support que se encuentra en el medio de instalación de Single Sign-on

• Para equipos de 32 bits: Microsoft Visual C++ 2008 Redistributable Package (x86) Service Pack 1
  • vc90_vcredist_x86.exe
• Para equipos de 64 bits: Microsoft Visual C++ 2008 Redistributable Package (x86) Service Pack 1
  • vc90_vcredist_x86.exe
  • vc90_vcredist_x64.exe
	Componente de consola, servicio o plug-in de Single Sign-on: al instalar el componente de consola, el servicio o el plug-in desde una interfaz de comandos en un equipo con Windows Vista, Windows Server 2008 o Windows Server 2008 R2	Carpeta Support que se encuentra en el medio de instalación de Single Sign-on

Componente de software	Necesario para	Disponible en...
Ensamblados de interoperabilidad primarios de Microsoft • vs90_piaredist.exe	Componente de consola de Single Sign-on: al instalar el componente de consola desde una interfaz de comandos en un equipo con Windows Vista, Windows Server 2008 o Windows Server 2008 R2	Carpeta Support que se encuentra en el medio de instalación de Single Sign-on
Configuración de seguridad mejorada de Internet Explorer	Single Sign-on Plug-in: desactive la Configuración de seguridad mejorada de Internet Explorer si instala el plug-in en un equipo con Windows Server 2003, Windows Server 2008 o Windows Server 2008 R2. Si se deja activada dicha configuración, el plug-in no responderá a las definiciones de aplicaciones Web.	

Requisitos de los componentes de Single Sign-on

Componente de Single Sign-on	Entorno respaldado o sistema operativo Microsoft Windows	Idioma compatible	Requisitos de hardware
Almacén central	• Active Directory • Punto compartido NTFS	• Inglés • Alemán • Francés • Español • Japonés	30 KB de espacio en el disco por usuario
Componente de Single Sign-on en AppCenter	• Microsoft Windows 7 Service Pack 1, 32 bits y 64 bits • Microsoft Windows 7, 32 bits y 64 bits • Microsoft Windows Vista Service Pack 2 (Business Edition, Ultimate Edition, Enterprise Edition), 32 bits y 64 bits • Microsoft Windows Vista (Business Edition, Ultimate Edition, Enterprise Edition), 32 y 64 bits • Windows XP Service Pack 3, 32 bits • Microsoft Windows XP Professional, Service Pack 2, 32 bits • Microsoft Windows XP Professional x64 Edition, 64 bits • Windows Server 2008 R2 Service Pack 1, 64 bits • Microsoft Windows Server 2008 R2, 64 bits	• Inglés • Alemán • Francés • Español • Japonés	• 64 MB de RAM • 60 MB de espacio en disco

Componente de Single Sign-on	Entorno respaldado o sistema operativo Microsoft Windows	Idioma compatible	Requisitos de hardware
	• Microsoft Windows Server 2008 (Standard Edition, Enterprise Edition, Datacenter Edition), 32 bits y 64 bits • Microsoft Windows Server 2003 R2 (Standard Edition, Enterprise Edition, Datacenter Edition), 32 bits y 64 bits • Microsoft Windows Server 2003 con Service Pack 2 (Standard Edition, Enterprise Edition, Datacenter Edition), 32 bits y 64 bits		
Plug-in	• Microsoft Windows 7 Service Pack 1, 32 bits y 64 bits • Microsoft Windows 7, 32 bits y 64 bits • Microsoft Windows Vista Service Pack 2 (Business Edition, Ultimate Edition, Enterprise Edition), 32 bits y 64 bits • Microsoft Windows Vista (Business Edition, Ultimate Edition, Enterprise Edition), 32 y 64 bits • Windows XP Service Pack 3, 32 bits • Microsoft Windows XP Professional, Service Pack 2, 32 bits • Microsoft Windows XP Professional x64 Edition, 64 bits • Microsoft Windows XP Embedded • Windows Server 2008 R2 Service Pack 1, 64 bits • Microsoft Windows Server 2008 R2, 64 bits • Microsoft Windows Server 2008 (Standard Edition, Enterprise Edition, Datacenter Edition), 32 bits y 64 bits • Microsoft Windows Server 2003 R2 (Standard Edition, Enterprise Edition, Datacenter Edition), 32 bits y 64 bits • Microsoft Windows Server 2003 con Service Pack 2 (Standard Edition, Enterprise Edition, Datacenter Edition), 32 bits y 64 bits	• Inglés • Alemán • Francés • Español • Japonés • Chino simplificado	• 10 MB de RAM • 25 MB de espacio en disco (si las funciones opcionales no se instalan) • 35 MB de espacio en disco (si las funciones opcionales se instalan)
Servicio	• Windows Server 2008 R2 Service Pack 1, 64 bits • Microsoft Windows Server 2008 R2, 64 bits • Microsoft Windows Server 2008 (Standard Edition, Enterprise Edition, Datacenter Edition), 32 bits • Microsoft Windows Server 2003 R2 (Standard Edition, Enterprise Edition, Datacenter Edition), 32 bits • Microsoft Windows Server 2003 con Service Pack 2 (Standard Edition, Enterprise Edition, Datacenter	• Inglés • Alemán • Francés • Español • Japonés	• 128 MB de RAM • 30 MB de espacio en disco

Componente de Single Sign-on	Entorno respaldado o sistema operativo Microsoft Windows	Idioma compatible	Requisitos de hardware
Herramienta de definición de aplicaciones	Igual que plug-in	• Inglés • Alemán • Francés • Español • Japonés	Igual que plug-in

Edition), 32 bits

Nota: Single Sign-on no está respaldado en Microsoft Windows XP Home Edition.
La función de Escritorio dinámico sólo se admite en:

- Microsoft Windows XP Professional, Service Pack 2, 32 bits
- Microsoft Windows XP Embedded

Escritorio dinámico no es compatible con sistemas operativos de servidor ni con sistemas operativos de 64 bits.

Requisitos del sistema de licencias

Instalar el servidor de licencias y agregar licencias antes de instalar Single Sign-on.

Para ejecutar esta versión, asegúrese de que tiene instalada la versión más reciente del servidor de licencias. Si está ejecutando una versión anterior del servidor de licencias, debe actualizarlo.
Importante: Las instancias de Single Sign-on Plug-in instaladas localmente no necesitan una licencia independiente para los usuarios que cuentan con acceso a las aplicaciones alojadas en entornos Citrix XenApp, Platinum Edition.

Modo desconectado

Si existen usuarios que trabajarán desconectados del servidor de licencias durante períodos prolongados (por ejemplo, usuarios que viajan y usan sus portátiles), debe especificar un período del modo desconectado para dichos usuarios. El período del modo desconectado se especifica como parte de los parámetros de licencias en la configuración de usuario. Dicho período especifica dos aspectos del comportamiento del sistema de licencias:

- El período en que el usuario puede estar desconectado del servidor de licencias sin entrar en el período de gracia de la licencia. Cuando caduca el período del modo desconectado, los usuarios emplean el lapso de configuración de usuario asociado en el período de gracia de la licencia, que es de 30 días.
- El período hasta que una licencia extraída que se está utilizando en modo desconectado se devuelve al grupo de licencias disponibles en el servidor de licencias independientemente de que el producto se vuelva a conectar a dicho servidor. Si se extrae una licencia y el modo desconectado asociado a dicha licencia caduca antes de que la licencia sea devuelta, el servidor de licencias recupera la licencia automáticamente, por lo que la licencia vuelve a estar disponible. Por ejemplo, si se pierde un equipo portátil con Single Sign-on y no se vuelve a conectar con la red de la organización, el servidor de licencias recupera automáticamente la licencia al final del período de modo desconectado.

Cuando se configura el modo desconectado, en realidad se especifica cuánto tiempo se esperará hasta que la licencia se devuelva al grupo de licencias disponibles.

Se recomienda configurar períodos de modo desconectado largos para los usuarios que no se conecten a la red de la organización de forma periódica, como, por ejemplo, el personal de ventas que trabaja de forma remota. No obstante, no hay que olvidar que no se puede recuperar ninguna de estas licencias extraídas, incluso de equipos perdidos o rotos, mientras dure este período.

Tipos de licencia mixta

Según el entorno de Single Sign-on y las necesidades de la empresa, es posible que se estén utilizando licencias independientes de Single-Sign-on previamente adquiridas. Por ejemplo, se pueden crear configuraciones de usuario basadas en el modelo de licencias de usuario definido para los usuarios móviles que utilizan Single Sign-on Plug-in mediante un equipo de escritorio y un equipo portátil. También se pueden crear configuraciones de usuario basadas en el modelo de licencias de usuario concurrente para los usuarios de Escritorio dinámico.

En algunos casos, es posible que todas las licencias de usuario definido estén en uso, por lo que Single Sign-on no estará disponible para algunos usuarios. En tal caso, se puede utilizar cualquier licencia de usuario concurrente disponible en la configuración de usuario para utilizarla sin conexión.

Planificación

Oct 12, 2015

Es necesario planificar el entorno antes de instalar Single Sign-on. Esto incluye decidir el tipo de almacén central que se desea utilizar, las aplicaciones que se habilitarán para el inicio de sesión único con Single Sign-on en la empresa, qué funciones de Single Sign-on se van a utilizar, y consolidar las directivas de contraseña.

Un entorno de Single Sign-on puede incluir los siguientes elementos:

- Carpetas de red compartidas o Active Directory que contenga el almacén central.
- Uno o más equipos que ejecuten Citrix AppCenter con el componente de Single Sign-on.
- Equipos de usuario que ejecuten Single Sign-on Plug-in.
- Un servidor dedicado que aloje el servicio Single Sign-on Service con uno o varios módulos de funciones instalados en él.
- Un entorno de Citrix XenApp que aloje Single Sign-on Plug-in.
- Dispositivos de autenticación, tales como tarjetas inteligentes.
- Funciones de Single Sign-on, como Escritorio dinámico y administración de claves.

Tipos de almacén central

Oct 12, 2015

Single Sign-on utiliza un punto denominado almacén central para almacenar y recuperar información sobre los usuarios y el entorno. Single Sign-on se basa en los datos del almacén central para llevar a cabo todas las funciones de Single Sign-on predeterminadas y configuradas. Se puede crear un almacén central automáticamente como parte del proceso de instalación de Single Sign-on, o se puede crear manualmente mediante las utilidades de configuración de almacén central.

El almacén central contiene datos de usuario y datos administrativos:

- Los datos de usuario en el almacén central incluyen las credenciales secundarias de usuario, preguntas y respuestas de seguridad, datos relacionados con los servicios (por ejemplo, datos de aprovisionamiento, datos de autenticación con preguntas, inscripción de recuperación de claves, etc.) y los datos del Registro de Windows relativos al usuario asociados a Single Sign-on.
- Los datos administrativos en el almacén central incluyen definiciones de aplicación, directivas de contraseña, preguntas de seguridad y otros parámetros establecidos mediante la consola para las funciones y componentes de Single Sign-on.

El almacén central básicamente permite que el software del plug-in se ejecute en un equipo de usuario o en un servidor Citrix XenApp para comunicarse con el almacén central y los servicios, con el fin de proporcionar credenciales de usuario a las aplicaciones a las que se le ha concedido acceso al usuario.

El software del plug-in mantiene un almacén central en el equipo del usuario. El almacén local sólo contiene las credenciales secundarias del usuario, la información de recuperación de claves y las preguntas y respuestas de seguridad (si corresponde). Se sincroniza con el almacén central para permitir a los usuarios que se desplacen por la empresa y siempre dispongan de acceso a las credenciales de usuario guardadas.

El almacén central puede ser uno de los siguientes tipos:

- Active Directory
  El almacén central utiliza el entorno y los objetos de Active Directory para almacenar y actualizar los datos de Single Sign-on.

- Punto compartido NTFS
  El almacén central utiliza un punto compartido de red de Windows para almacenar los datos de Single Sign-on.

Si es necesario, se pueden migrar los usuarios de un tipo de almacén central a otro.

Selección de un almacén central de Active Directory

Al seleccionar el uso de Active Directory como almacén central se puede aprovechar la comodidad de la administración de autenticación de usuario y objetos de Active Directory existentes. Por ejemplo, puede aplicarse una configuración de usuario específica a cualquier nivel de un dominio (al dominio en su totalidad, a una unidad organizativa, a un grupo o a usuarios concretos).

Se han agregado dos clases y dos atributos nuevos al esquema de Active Directory al crear un almacén central de Active Directory:

Class	Descripción
citrix-SSOConfig	Describe el objeto que contiene datos para la configuración del software del plug-in, el estado de sincronización, las definiciones de aplicación y el comportamiento de uso del

Class	Descripción
	software del plug-in por primera vez. Esta clase incluye los atributos siguientes: citrix-SSOConfigData: contiene los datos reales y citrix-SSOConfigType: especifica el tipo de datos
citrix-SSOSecret	Describe el objeto de datos secretos que se utiliza para autenticar a un usuario de Single Sign-on. Esta clase incluye el atributo siguiente: citrix-SSOSecretData: contiene datos de credenciales cifrados para una aplicación y datos de restablecimiento de contraseñas del Autoservicio de cuentas

Nota: Para obtener más información sobre estas clases y atributos, consulte el archivo CitrixMPMSchema.xml de la carpeta \Tools del disco de instalación.
En general, se debe elegir Active Directory como almacén central si:

- Se puede ampliar correctamente el esquema de Active Directory sin que se vea afectada la empresa.
- Ya se han implementado directrices recomendadas por Microsoft para copia de seguridad y restauración de Active Directory (aunque no es un requisito).
- Se prefiere que la alta disponibilidad que está incorporada en Active Directory se amplíe a los datos del almacén central.

Ventajas de un almacén central en Active Directory

A continuación se detallan las ventajas del uso de un almacén central de Active Directory:

- Active Directory incluye conmutación por error y redundancia incorporadas, por lo que no se precisan medidas adicionales para la recuperación de desastres.
- La duplicación de Active Directory ayuda a distribuir los datos administrativos y de usuario del almacén central por toda la empresa.
- No se necesita hardware adicional al utilizar un almacén central de Active Directory

Consideraciones del almacén central en Active Directory

Tenga en cuenta lo siguiente antes de utilizar un almacén central de Active Directory:

- Se debe ampliar el esquema cuando se utiliza un almacén central de Active Directory, lo que requiere una planificación e instalación cuidadosas. La ampliación del esquema afecta a todo el bosque.
- Se recomienda ampliar el esquema y crear el almacén central de Active Directory durante las horas de poco uso. El retardo de ciclo de duplicación de Active Directory afectará a la velocidad con que estos cambios se copien en todos los controladores de dominio del bosque.
- La duplicación entre sitios de los datos del almacén central en empresas grandes que utilicen WAN requiere la configuración correcta de la duplicación para reducir el retardo. No obstante, la duplicación dentro del sitio normalmente supone menos retardo.

Selección de un punto compartido NTFS

Al seleccionar el uso de un punto compartido NTFS como almacén central se puede aprovechar la comodidad de la autenticación de usuarios y la estructura de árbol de Active Directory existentes sin tener que ampliar el esquema de Active Directory. Por ejemplo, puede aplicarse una configuración de usuario específica a cualquier nivel de un dominio (al dominio en su totalidad, a una unidad organizativa, a un grupo o a usuarios concretos).

Importante: Use un recurso compartido oculto como almacén central en este caso.
Single Sign-on crea una carpeta compartida llamada CITRIXSYNC$ con dos subcarpetas denominadas People y

CentralStoreRoot.

La carpeta People contiene una subcarpeta para cada usuario e incluye las propiedades de permiso de lectura y escritura adecuadas para el usuario. La carpeta CentralStoreRoot contiene datos administrativos.

Ventajas de un punto compartido NTFS

A continuación se detallan las ventajas del uso de un punto compartido NTFS:

- Se puede emular el aspecto de un almacén central de Active Directory sin tener que ampliar el esquema de Active Directory. Se pueden aprovechar la jerarquía o los grupos de Active Directory existentes.
  Nota: La asociación de configuraciones de usuario a grupos sólo se admite en dominios de Active Directory que utilizan la autenticación de Active Directory.
- Los datos de usuario siempre están actualizados, ya que se almacenan en una ubicación central y se evita el retardo de duplicación asociado con Active Directory.
- Se puede equilibrar la carga de los puntos compartidos entre varios equipos que pueden alojar un punto compartido NTFS para una mayor disponibilidad.
- El punto compartido NTFS contribuye a reducir la carga de trabajo de las tareas de autenticación del entorno de Active Directory.
- Single Sign-on permite migrar el almacén central del punto compartido NTFS a un almacén central de Active Directory si posteriormente se decide implementar un almacén central de Active Directory.

Consideraciones del punto compartido NTFS

Tenga en cuenta la siguiente información antes de utilizar un punto compartido NTFS:

- Es posible que se necesite hardware adicional para alojar el almacén central.
- Es necesario realizar una copia de seguridad de los archivos y las carpetas (incluidos los permisos relacionados) del almacén central periódicamente. También se deben mantener e implementar planes de recuperación de desastres donde se dupliquen archivos y carpetas para la recuperación del sitio.
- Es posible que la topología de la red empresarial requiera que los usuarios (y el software Single Sign-on Plug-in) transfieran datos de usuario entre uno o varios vínculos WAN. En este caso, se recomienda implementar la tecnología DFS de sistema de archivos distribuidos (Distributed File System), incluida como parte de Microsoft Windows Server 2003 y 2008. En el sitio Web de Microsoft http://support.microsoft.com se describe con más detalle la tecnología DFS de sistema de archivos distribuidos.

Uso de asociación de cuenta con varios almacenes centrales y credenciales de cuenta de usuario en una empresa de varios dominios

Los administradores pueden crear varios almacenes centrales en las empresas que contengan varios dominios. De hecho, se pueden utilizar varios tipos de almacén central en estos entornos. Por ejemplo, es posible asociar configuraciones de usuarios a un almacén central de punto compartido NTFS en un dominio y a un almacén central de Active Directory en otro dominio.

Como las empresas pueden mantener varios dominios de Windows, los usuarios también pueden tener varias cuentas de Windows. Single Sign-on incluye una función denominada Asociación de cuentas que permite que el usuario inicie sesión en cualquier aplicación desde una o varias cuentas de Windows. Como Single Sign-on normalmente vincula las credenciales de usuario a una sola cuenta, la información de credenciales no se sincroniza automáticamente entre las distintas cuentas que posee un usuario.

No obstante, los administradores pueden configurar la asociación de cuentas para que sincronice las credenciales de usuario mediante el módulo de sincronización de credenciales. Los usuarios que tienen configurada la asociación de cuentas disponen de acceso a todas las aplicaciones desde cualquiera de sus cuentas en su entorno de Single Sign-on. Cuando las credenciales de usuario se cambian, agregan o eliminan de una cuenta, se sincronizarán automáticamente con cada una de las cuentas asociadas del usuario.

Sin la asociación de cuentas, un usuario con varias cuentas de Windows está obligado a cambiar manualmente su información de inicio de sesión independientemente en cada cuenta de Windows.

Para permitir que los usuarios sincronicen sus credenciales usando la asociación de cuentas, hay que darles acceso a AccAssoc.exe como aplicación publicada.

Ventajas de la asociación de cuenta

- La asociación de cuentas puede contribuir a aumentar la productividad y a reducir las llamadas al servicio técnico mediante la sincronización de las credenciales de usuario para disminuir el mantenimiento o los errores de inicio de sesión.
- Las cuentas se pueden sincronizar entre distintos tipos de almacén central. Es decir, una cuenta de usuario configurada para utilizar Active Directory como almacén central puede sincronizarse con una cuenta de usuario asociada que esté configurada para utilizar un punto compartido NTFS.
- Las cuentas también se pueden sincronizar entre distintas configuraciones de usuario. Por ejemplo, una configuración de usuario puede estar asociada a una jerarquía de almacén de datos (unidad organizativa o usuario) en un dominio y a un grupo de almacén de datos en otro dominio.
- Las cuentas también se pueden sincronizar entre distintas configuraciones de usuario en el mismo dominio y en el mismo almacén central.
- Para utilizar la asociación de cuentas no son necesarias las relaciones de confianza entre los controladores de dominio.

Deben tenerse en cuenta los siguientes puntos antes de configurar la asociación de cuentas:

- La asociación de cuentas no es compatible con las tarjetas inteligentes cuando éstas se utilizan como el mecanismo de autenticación principal para iniciar sesión en Windows.
  Nota: La configuración de usuario en cada dominio puede tener distintas directivas de contraseña que podrían bloquear el acceso a un recurso, pero la asociación de cuentas sólo sincroniza las credenciales de usuario, no las directivas de configuración de usuario. Se debe tener en cuenta el modo de establecer las directivas de contraseña en la empresa.
- Cada cuenta de dominio asociada debe utilizar Single Sign-on.
- Los nombres de definición de aplicación deben ser los mismos en cada configuración de usuario para que la función de asociación de cuentas pueda sincronizar las credenciales.
- Las credenciales de usuario se comparten únicamente para las aplicaciones especificadas en las definiciones de aplicación que ha creado el administrador de Single Sign-on.
- Como parte del servicio Single Sign-on Service, el módulo de sincronización de credenciales es un servicio Web que está disponible mediante una conexión HTTP segura, por lo que se debe poder acceder a este módulo desde todos los equipos de la empresa que utilicen la asociación de cuentas.

Directivas de contraseña

Oct 12, 2015

Las directivas de contraseña son reglas que controlan el modo en que se crean, envían y administran las contraseñas. En la instalación de Single Sign-on se incluyen dos directivas de contraseña denominadas Predeterminada y Dominio, que no se pueden eliminar. Estas directivas se pueden copiar y modificar según las directivas y normativas de la empresa.

Directiva de contraseña Predeterminada

Single Sign-on aplica la directiva Predeterminada a las aplicaciones habilitadas para contraseña que se utilizan en la empresa (excepto las que requieren credenciales de dominio de usuario). Esta directiva se aplica a cualquier aplicación que no haya definido un administrador (mediante la función de definición de aplicaciones de la consola) o a cualquier aplicación que no forme parte de un grupo de aplicaciones.

Cuando un usuario agrega sus credenciales a la ventana Administrar contraseñas (anteriormente conocida como Administrador de inicios de sesión) para una aplicación que no está definida por un administrador, Single Sign-on utiliza la directiva Predeterminada para administrar esa aplicación.

Directiva de contraseña Dominio

Normalmente, los administradores crean un grupo de aplicaciones y seleccionan la directiva Dominio para que se aplique a las aplicaciones de dicho grupo. A continuación, Single Sign-on aplica la directiva Dominio a las aplicaciones que requieren las credenciales de dominio del usuario para acceder. La directiva Dominio se puede modificar o copiar para reflejar las directivas de dominio de NT o de Active Directory de la empresa para las cuentas de usuario.

Para que un grupo de aplicaciones se considere un grupo de contraseñas de dominio, es necesario aplicar la directiva de dominio al grupo de aplicaciones. Un grupo de aplicaciones es un conjunto de aplicaciones definidas que están asociadas a una o varias configuraciones de usuario, incluida la directiva para administrar las aplicaciones.

Directivas de contraseña personalizadas

Puede crear directivas de contraseña según sea necesario: puede aplicar una directiva para el grupo que comparte dominio, crear directivas individuales que se aplicarán a grupos individuales de aplicaciones para protegerlas, etc.

Al crear una directiva de contraseña personalizada o modificar directivas existentes, es necesario asegurarse de que coinciden los requisitos de la empresa y los de la aplicación. Por ejemplo, si se crea una directiva que no corresponde al menos con los requisitos de una aplicación, los usuarios no podrán autenticarse en dicha aplicación.

En general, las directivas de contraseña pueden especificar restricciones como las siguientes:

- Un número de caracteres mínimo y máximo para las contraseñas
- El uso de caracteres alfabéticos y numéricos
- La cantidad de veces que se puede repetir un carácter
- La exclusión u obligación de los caracteres o caracteres especiales que pueden usarse
- Si los usuarios pueden ver las contraseñas guardadas
- El número de intentos permitidos cuando el usuario indica una contraseña errónea
- Los parámetros que regulan la caducidad de las contraseñas
- El historial y las excepciones de contraseñas

Consideraciones de las directivas de contraseña

Analice lo siguiente antes de establecer las directivas de contraseña:

- Se deben tener en cuenta los requisitos de seguridad en el contexto de la facilidad de uso para los usuarios. Los usuarios pueden tener dificultades para crear, implementar o recordar contraseñas si son excesivamente restrictivas.
- Dado que Single Sign-on está diseñado de manera segura, la directiva de contraseña Predeterminada define el nivel mínimo de seguridad de contraseña recomendado por Citrix para proteger la mayoría de las aplicaciones habilitadas para ser utilizadas con Single Sign-on. Estos parámetros se pueden modificar según las directivas y normativas de la empresa.
- Dado que Single Sign-on aplica la directiva de contraseñas Predeterminada a todas las aplicaciones agregadas por el usuario, la directiva Predeterminada debe configurarse lo más ampliamente posible de modo que acepte contraseñas para las aplicaciones para las que se permita almacenar contraseñas.
- Cuando los usuarios cambian una contraseña en una aplicación, Single Sign-on se puede configurar mediante un parámetro de configuración de usuario para que compare la contraseña anterior con la nueva y para que no se pueda utilizar la misma contraseña dos veces seguidas.
- Los usuarios pueden tener una sola contraseña que se utiliza para varias aplicaciones (una suite de productos, por ejemplo). Este esquema se denomina contraseñas compartidas, donde la misma autoridad de autenticación se utiliza para las aplicaciones.
  Aunque el resto de las credenciales de estas aplicaciones (como el nombre de usuario y los campos especiales) pueden ser diferentes, la contraseña es la misma. En este caso, se debe crear un grupo de aplicaciones que sea a su vez un grupo de contraseñas compartidas para garantizar que el software del plug-in administra la contraseña de todas las aplicaciones del grupo como si fueran una única aplicación. Cuando se modifica la contraseña de una aplicación, el software del plug-in hace que el cambio se refleje en las credenciales almacenadas para todas las aplicaciones del grupo.

- En los grupos de contraseñas compartidas de dominio, la contraseña compartida de dominio del usuario es válida para todo el grupo de aplicaciones. Cuando el usuario modifica la contraseña de dominio, el software del plug-in aplica el cambio a las credenciales del resto de las aplicaciones del grupo. Sólo puede modificarse la contraseña de dominio. Los usuarios no pueden cambiar las contraseñas de ninguna de las otras aplicaciones del grupo a menos que el administrador elimine la aplicación del grupo de contraseñas de dominio compartidas.

Definiciones de aplicación

Oct 12, 2015

Los administradores de Single Sign-on pueden crear una definición de aplicación o modificar una plantilla de definición de aplicación para cada aplicación que vaya a ser administrada con Single Sign-on. Se pueden crear definiciones de aplicación con la consola o con la Herramienta de definición de aplicaciones independiente, que se puede instalar en las estaciones de trabajo sin consola.

También se puede permitir a los usuarios que agreguen sus credenciales a Single Sign-on para cualquier aplicación de cliente que detecte, según los parámetros de las configuraciones de usuario. El software del plug-in puede detectar y responder a los cambios de inicio de sesión para la mayoría de las aplicaciones, incluidos los siguientes tipos de aplicaciones:

Tipos de aplicación	Descripción
Windows	Aplicaciones de Windows de 32 bits (incluidas las aplicaciones Java) como Microsoft Outlook, Lotus Notes, SAP o cualquier aplicación de Windows habilitada para contraseña
Web	Aplicaciones Web (incluidas los applets de Java y SAP) a las que se accede mediante Microsoft Internet Explorer
Emuladores de terminal	Aplicaciones a las que se accede mediante un emulador de terminal compatible con HLLAPI (Single Sign-on no es compatible con el software de emulación de terminal de 64 bits).

El software del plug-in responde a las definiciones de aplicación que se crean desde el principio o se copian de plantillas existentes. Las definiciones de aplicación:

- Permiten que el software del plug-in reconozca y responda a las aplicaciones y formularios que utilizan las aplicaciones para procesar las credenciales de usuario.
- Constan de un conjunto de identificadores que establecen parámetros para llevar a cabo este reconocimiento y respuesta.

En cada definición se crean los formularios de inicio de sesión y relacionados con contraseña necesarios para acceder a la aplicación. Los asistentes de definiciones de aplicación pueden ayudar a crear una definición si se abre la aplicación; los asistentes pueden detectar los formularios y campos de la mayoría de las aplicaciones mediante las funciones de coincidencia de ventana de Single Sign-on.

Sugerencia: Single Sign-on incluye plantillas de definición de aplicaciones predeterminadas para una serie de aplicaciones o funciones de aplicación de Citrix. Hay más plantillas disponibles en el sitio Web de asistencia técnica (Support) de Citrix.

Tarjetas inteligentes

Oct 12, 2015

Citrix ha probado las tarjetas inteligentes que cumplen el estándar 7816 de ISO para tarjetas con contactos eléctricos (tarjetas de contacto) que interactúan con sistemas informáticos mediante un dispositivo denominado lector de tarjetas inteligentes. El lector se puede conectar al equipo host con el puerto serie, USB o PC Card (PCMCIA).

Citrix respalda la utilización de tarjetas inteligentes de cifrado basadas en PC/SC. Estas tarjetas proporcionan la capacidad de realizar operaciones criptográficas como, por ejemplo, las firmas digitales y el cifrado. Las tarjetas de cifrado están diseñadas de forma que permiten el almacenamiento seguro de las claves privadas, como las utilizadas en los sistemas de seguridad PKI (infraestructura de clave pública).

Estas tarjetas llevan a cabo las funciones criptográficas en la propia tarjeta, lo que significa que las claves privadas nunca salen de ella. Por otra parte, las tarjetas inteligentes proporcionan autenticación de dos factores para mayor seguridad: la tarjeta y el número PIN del usuario. Cuando se combinan ambos elementos, el titular de la tarjeta puede demostrar que es el propietario de la tarjeta inteligente.

Requisitos del software de tarjetas inteligentes

Póngase en contacto con el proveedor o integrador de la tarjeta inteligente para determinar los requisitos de configuración pertinentes para la implantación de dicha tarjeta inteligente. Los siguientes componentes son necesarios en el servidor o el cliente:

- Software PC/SC
- Software CSP (proveedor de servicios de cifrado)
- Controladores del software del lector de tarjetas inteligentes

Es posible que los sistemas operativos de servidor y cliente Windows ya incluyan controladores PC/SC, CSP o de lector de tarjetas inteligentes. Póngase en contacto con el proveedor de tarjetas inteligentes para obtener información sobre la compatibilidad con estos componentes de software o si éstos han de reemplazarse por software específico del proveedor.

Para poder usar tarjetas inteligentes en entornos con Windows Server 2008 o Windows Vista, el almacén central debe crearse o actualizarse con una consola de Single Sign-on 4.5 (anteriormente Password Manager) o una consola posterior, y hay que seleccionar API de protección de datos de Microsoft (necesita perfiles móviles) en las configuraciones de usuario.

Requisitos para la verificación de identidad

Oct 12, 2015

Dependiendo de los parámetros de configuración, se puede exigir a los usuarios que verifiquen sus identidades cuando ocurran los siguientes sucesos:

- Los usuarios cambian sus tipos de autenticación; por ejemplo, un usuario puede cambiar de la autenticación por tarjeta inteligente a la de contraseña (se puede crear una configuración de usuario que requiera la verificación inicial sólo cuando se cambie de tipo de autenticación).
- Un administrador cambia la contraseña primaria de un usuario.
- Los usuarios restablecen su contraseña primaria con el autoservicio de contraseñas.
- Los usuarios desbloquean sus cuentas de dominio con el autoservicio de contraseñas.
- Los usuarios cambian su contraseña primaria en un dispositivo que no tiene instalado el software del plug-in y luego inician una sesión en uno donde sí está instalado.

Single Sign-on se puede configurar para verificar la identidad del usuario y asegurar que el usuario esté autorizado a usar Single Sign-on. Se pueden seleccionar dos métodos de verificación de identidad:

Método	Descripción
Contraseña anterior	En este caso, los usuarios verifican su identidad indicando sus contraseñas primarias anteriores.
Preguntas de seguridad (también se denomina autenticación con preguntas)	En este caso, se crea un cuestionario que contiene tantos grupos de pregunta y respuesta como se quiera. Se pueden utilizar las preguntas predeterminadas que proporciona Single Sign-on o crear preguntas propias.

Precaución: Si sólo se pone a disposición de los usuarios el método de verificación de identidad mediante contraseñas anteriores, los usuarios que no recuerden su contraseña primaria anterior estarán bloqueados. El administrador deberá utilizar la tarea Restablecer los datos de usuario en el componente Single Sign-on para hacer que los usuarios puedan volver a inscribirse. Es posible que el administrador también tenga que restablecer las contraseñas en las aplicaciones del usuario.

Verificación de la identidad del usuario mediante preguntas de seguridad (autenticación con preguntas)

Single Sign-on permite utilizar la autenticación con preguntas para verificar la identidad de los usuarios. Single Sign-on incluye cuatro preguntas (en inglés, francés, alemán, japonés, chino y español) que se pueden utilizar con esta finalidad.

La autenticación con preguntas se puede utilizar:

- Como parte del registro de preguntas de seguridad de un usuario durante la inscripción en el software del plug-in por primera vez
- Después de la inscripción, si se ha configurado el autoservicio de cuentas para permitir que los usuarios cambien sus credenciales primarias o desbloquear sus cuentas

Cuando los usuarios cambian sus contraseñas primarias, se puede confirmar su identidad pidiendo que respondan a unas preguntas de seguridad sacadas de un cuestionario. El cuestionario aparece la primera vez que los usuarios inician el software del plug-in. A continuación, se les pedirá que respondan varias preguntas de seguridad cuyo número habrá definido el administrador. En adelante, se puede utilizar el mismo procedimiento cuando se produzcan determinados sucesos relacionados con el cambio de contraseñas.

Para permitir que los usuarios vuelvan a registrar sus respuestas a las preguntas de seguridad sin que lo solicite el sistema, hay que darles acceso a QBAEnroll.exe como aplicación publicada.

Si no se configuran preguntas de seguridad, los usuarios deberán escribir su contraseña primaria anterior cuando inicien sesión por primera vez y cuando cambien su contraseña primaria actual. También se puede permitir que los usuarios elijan el método que prefieran utilizar al autenticarse (contraseñas anteriores o preguntas de seguridad).

Recuperación o desbloqueo automáticos de las credenciales de usuario

Importante: La administración de claves automática no es tan segura como los otros mecanismos de recuperación de claves, tales como las preguntas de seguridad o la contraseña anterior.
Puede configurar Single Sign-on para que omita la verificación de identidad y recupere automáticamente las credenciales de usuario (es decir, las claves de cifrado asociadas a los datos de usuario) si instala Single Sign-on Service y utiliza el módulo de administración de claves.

El flujo de trabajo básico para utilizar la administración automática de claves es el siguiente:

1. Instale Citrix Single Sign-on Service con el módulo de administración de claves.
2. Cree o modifique las configuraciones de usuarios y seleccione el método de recuperación de claves que permite administrar las claves automáticamente sin necesidad de verificar la identidad. Esta opción está disponible como parte de la propiedad Protección de datos secundaria de la configuración del usuario.

Planificación de Single Sign-On Plug-in en configuraciones de usuario

Oct 12, 2015

Una configuración de usuario es un conjunto único de parámetros, directivas de contraseña y aplicaciones que se aplica a usuarios asociados a una jerarquía de Active Directory (unidad organizativa o usuario individual) o a un grupo de Active Directory (excepto para grupos de distribución y grupos locales de dominio en modo mixto de Active Directory, que no se admiten). Las configuraciones de usuario permiten controlar el comportamiento y el aspecto del software del plug-in para usuarios.

Las configuraciones de usuario establecen la información de usuario, las definiciones de aplicación, las directivas de contraseña y los métodos de verificación de identidad. También se debe especificar la información de licencia (servidor de licencias y tipo de licencia) en cada configuración de usuario. Por lo tanto, los usuarios no pueden utilizar el software del plug-in hasta que se establezcan sus parámetros de configuración.

Antes de crear las configuraciones de usuario, es necesario asegurarse de que se han creado o definido los siguientes elementos:

- Almacén central
- Módulos de servicio opcionales
- Definiciones de aplicación
- Directivas de contraseña
- Preguntas de seguridad (opcional)

Las configuraciones de usuario constan de los siguientes elementos:

- Usuarios asociados a una jerarquía de dominio (unidad organizativa o usuario individual) de Active Directory.
- Métodos de protección de datos.
- Las definiciones de aplicación que se han creado, que se pueden combinar en un grupo de aplicaciones al crear una configuración de usuario.
- Directivas de contraseña asociadas a cualquier grupo de aplicaciones. (Al crear una configuración de usuario, se pueden crear uno o varios grupos de aplicaciones para asociarlos a una configuración de usuario; también se puede agregar un grupo de aplicaciones a una configuración de usuario después de haberla creado).
- Funciones de autoservicio (desbloqueo de cuenta y restablecimiento de contraseña) y opciones de administración de claves (uso de contraseñas anteriores, preguntas de seguridad que se crean para los usuarios y administración automática de claves).
- Parámetros de configuración de Escritorio dinámico, aprovisionamiento de credenciales y compatibilidad con aplicaciones.

La asociación de configuraciones de usuario a grupos sólo se admite en dominios de Active Directory que utilizan la autenticación de Active Directory.

Tenga en cuenta lo siguiente al planificar el entorno de usuario de Single Sign-on Plug-in:

- Si es necesario aplicar los mismos parámetros de configuración de usuario a un grupo distinto de usuarios, se debe duplicar la configuración de usuario en la consola y modificar los parámetros según sea necesario.
- El modo en que se organice el entorno de usuario de Single Sign-on puede afectar el funcionamiento de las configuraciones de usuario. Es decir, las configuraciones de usuario se asocian en el entorno de Single Sign-on a una jerarquía (unidad organizativa o usuarios) o a un grupo de Active Directory. Si se utilizan ambos (jerarquía y grupo) y un

usuario se encuentra en ambos contenedores, tiene prioridad la configuración de usuario asociada a la jerarquía y es la que se utiliza. Este esquema se considera un entorno mixto.

- La información de configuración de usuario que se mantiene en el almacén central tiene prioridad sobre la información guardada en el almacén local (es decir, los datos de usuario almacenados en el equipo). Los datos de usuario del almacén local se utilizan principalmente cuando el almacén central no está disponible o está desconectado.

Activación de distribución de los mismos recursos o estaciones de trabajo entre varios usuarios (Escritorio dinámico)

Oct 12, 2015

La función Escritorio dinámico permite a los usuarios compartir estaciones de trabajo de forma segura y eficaz. Con Escritorio dinámico, se agilizan los cambios de usuario además de contar con las ventajas que ofrece el inicio de sesión único a través de Single Sign-on.

Para instalar Escritorio dinámico, deben realizarse las siguientes tareas:

- Crear configuraciones de usuario relacionadas con Escritorio dinámico
- Configurar una cuenta compartida de Escritorio dinámico
- Modificar los scripts que definen las aplicaciones que se ejecutan en los dispositivos de Escritorio dinámico y sus comportamientos de inicio y cierre

La función Escritorio dinámico no se instala de forma predeterminada; se puede seleccionar durante el proceso inicial de instalación del software del plug-in. También pueden actualizarse las instalaciones existentes para incorporarla.

Si se instala Escritorio dinámico en un entorno donde los usuarios inician sesión con tarjetas inteligentes y el origen de clave de tarjeta inteligente seleccionado es DPAPI con perfil, no se debe seleccionar Pedirle al usuario que entre su contraseña anterior ya que es el único método de recuperación de claves para dichos usuarios. Los usuarios en un entorno de este tipo no pueden introducir la contraseña anterior correcta y, por lo tanto, están bloqueados de forma irrecuperable en el sistema. Para evitar este problema, se debe seleccionar la opción de administración automática de claves o poner a disposición de los usuarios la autenticación con preguntas.

Control de aplicaciones con Escritorio dinámico

Con Escritorio dinámico, los usuarios pueden autenticarse rápidamente mediante sus credenciales de cuenta de Windows o el autenticador seguro de tarjetas inteligentes. Los administradores pueden configurar Escritorio dinámico para iniciar aplicaciones en el entorno de Escritorio dinámico de modo que los usuarios no tengan que buscarlas ni esperar a que se inicien.

Asimismo, se puede configurar Escritorio dinámico para garantizar que todas las aplicaciones se cierren correctamente, dejando un entorno limpio para la siguiente sesión de usuario.

Interacción del usuario con Escritorio dinámico

Cuando la cuenta compartida inicia la sesión, el dispositivo pasa al modo de “cambio rápido de usuario” y aparece la solicitud de autenticación de Windows en la pantalla. La cuenta compartida permanece conectada independientemente de la actividad del usuario de Escritorio dinámico.

Cuando los usuarios se autentican, no inician la sesión en Escritorio dinámico como ocurre con otras aplicaciones, sino que Escritorio dinámico utiliza sus credenciales de Windows para iniciar una sesión de Escritorio dinámico. Debido a que los usuarios no están iniciando la sesión realmente sino simplemente autenticándose, se omiten todos los procesos que suelen asociarse al inicio de sesión (como la aplicación de la directiva de grupo o la inicialización de impresoras) y es posible pasar rápidamente de un usuario a otro. El usuario puede iniciar una sesión, realizar tareas relacionadas con su trabajo y finalizar la sesión para que el siguiente usuario pueda acceder al sistema y hacer lo mismo. El cambio de un usuario a otro se produce

de forma rápida y eficaz.

El software Single Sign-on Plug-in se inicia cuando comienza la sesión de Escritorio dinámico. Después de establecerse la sesión, Escritorio dinámico accede a las credenciales de cuenta de Windows del usuario para iniciar las aplicaciones mediante la interfaz de shell estándar. Normalmente, estas aplicaciones de cliente ligero solicitan a los usuarios sus credenciales, que pueden ser suministradas por el software del plug-in utilizando las configuraciones asociadas a sus cuentas de Windows.

Planificación de funciones opcionales de Single Sign-on Service

Oct 12, 2015

Single Sign-on Service es un servicio Web que utiliza el protocolo SSL (Secure Sockets Layer) para cifrar los datos que comparten el software de Single Sign-on Service, la consola y el plug-in. Utiliza un servidor Web dedicado para alojar las funciones opcionales incluidas en Single Sign-on.

Es necesario instalar el servicio Single Sign-on Service si se piensa utilizar uno o varios de los siguientes módulos:

- Administración de claves
- Integridad de datos
- Aprovisionamiento
- Autoservicio
- Sincronización de credenciales

Importante: El servidor donde se encuentra Single Sign-on Service contiene información confidencial relacionada con los usuarios, por lo que Citrix recomienda utilizar un servidor dedicado y colocarlo en un lugar seguro.

Administración de claves

La administración de claves permite a los usuarios iniciar sesión en la red y tener acceso inmediato a las aplicaciones que administra Single Sign-on sin tener que verificar sus identidades mediante autenticación con preguntas (conocido también como administración automática de claves). Para reducir las amenazas de seguridad, la administración automática de claves utiliza la división de claves (un proceso mediante el que se divide la clave privada en dos partes).

No obstante, la administración automática de claves no protege frente a los usuarios no autorizados o frente a los administradores que suplanten a usuarios, porque no hay ningún "secreto de usuario" para proteger la contraseña de red del usuario. Para evitar en lo posible este problema, se puede implementar la administración automática de claves combinada con el módulo de autoservicio de cuentas y la autenticación con preguntas.

Importante: El acceso de los administradores a las contraseñas de las aplicaciones administradas por Single Sign-on está regido por las directivas de seguridad de la empresa. Consulte los requisitos de seguridad de su empresa antes de permitir que Single Sign-on administre contraseñas que los usuarios quieran mantener totalmente en privado. Eliminando la selección de las funciones de administración automática de claves en el parámetro Métodos de protección de datos en la configuración del usuario también se contribuye a evitar este acceso no autorizado.

Integridad de datos

El módulo de integridad de datos contiene los archivos de claves públicas y privadas que se emplean para firmar los datos. Utiliza la criptografía de claves públicas RSA para garantizar que el software del plug-in sólo obtenga los datos de configuración que provienen de fuentes autorizadas. El módulo de integridad de datos nunca divulga su clave privada.

Después de que la consola firme los datos, ésta envía los datos y la firma al almacén central. El software del plug-in recibe los datos y la firma del almacén central durante la sincronización. A continuación, el software del plug-in se pone en contacto con el servicio Single Sign-on Service para obtener una copia de la clave pública que se necesita para verificar la firma que ha recibido del almacén central.

Instale el módulo de integridad de datos cuando desee garantizar que los datos transmitidos entre los componentes de Single Sign-on provienen de un origen autorizado y de confianza. Este módulo es opcional y está diseñado para los usuarios que tienen redes que no son de confianza.

Si el software del plug-in está configurado para utilizar el módulo de integridad de datos, no aceptará datos de configuración que no hayan superado la comprobación de integridad de datos. Si no se cumple este requisito, el software del plug-in registra el suceso y muestra un mensaje de error en el que se indica a los usuarios que se pongan en contacto directamente con el administrador. A continuación, el software del plug-in utiliza de forma predeterminada las configuraciones anteriores o vuelve a un estado sin conexión.

Si ya se dispone de una infraestructura de seguridad que protege los datos en tránsito, como la firma con IPsec (Internet Protocol Security) o SMB (Server Message Block), no es necesario instalar el módulo de integridad de datos.

Aprovisionamiento

El aprovisionamiento (también conocido como aprovisionamiento de credenciales) permite automatizar ciertos procesos de administración de credenciales. Puede:

- Agregar, modificar y eliminar credenciales en el almacén central
- Restablecer la información de credenciales de los usuarios
- Eliminar usuarios y las credenciales de sus aplicaciones en Single Sign-on

El aprovisionamiento de credenciales consiste en obtener información sobre el entorno y utilizarla para crear una plantilla con la que agregar, quitar o modificar la información sobre credenciales del almacén central.

Autoservicio

Las funciones de autoservicio de cuentas de Single Sign-on pueden configurarse para que los usuarios puedan restablecer sus contraseñas primarias y desbloquear sus cuentas de dominio de Windows por sí mismos, sin que tenga que intervenir un administrador o el servicio de asistencia técnica. Según cuáles sean sus necesidades, el autoservicio de restablecimiento de contraseñas y el autoservicio de desbloqueo de cuentas pueden implementarse separada o conjuntamente, de forma segura, en el entorno de Single Sign-on.
Nota: También es posible utilizar exclusivamente la función de autoservicio de cuentas en entornos de Active Directory para permitir que los usuarios restablezcan sus contraseñas primarias o desbloqueen sus cuentas de dominio de Windows.
Estas funciones de cuentas están protegidas por la autenticación con preguntas, que contribuye a garantizar que los usuarios autorizados son quienes restablecen sus contraseñas o desbloquean sus cuentas. Si el autoservicio de cuentas está habilitado, los usuarios deben registrarse, un proceso durante el cual deberán responder las preguntas de seguridad que el administrador ha creado y seleccionado anteriormente. Dichas preguntas de seguridad vuelven a formularse a los usuarios cuando éstos necesitan cambiar la contraseña o desbloquear su cuenta. Cuando las preguntas se responden correctamente, los usuarios pueden restablecer la contraseña o desbloquear su cuenta.

Sincronización de credenciales

Con la sincronización de credenciales (también llamada asociación de cuentas) los usuarios pueden iniciar sesión en cualquier aplicación desde una o varias cuentas de Windows. Como Single Sign-on normalmente vincula las credenciales de usuario a una sola cuenta, la información de credenciales no se sincroniza automáticamente entre las distintas cuentas que posee un usuario. No obstante, los administradores pueden configurar la asociación de cuentas para sincronizar las credenciales de usuario. Los usuarios que tienen configurada la asociación de cuentas disponen de acceso a todas las aplicaciones desde cualquiera de sus cuentas en su entorno de Single Sign-on. Cuando las credenciales de usuario se cambian, agregan o eliminan de una cuenta, se sincronizarán automáticamente con cada una de las cuentas asociadas del usuario.

Entornos de instalación del software Single Sign-On Plug-in

Oct 12, 2015

Single Sign-on puede usarse en entornos que incluyen aplicaciones alojadas en servidores XenApp, aplicaciones instaladas localmente, o ambos tipos.

En un entorno XenApp, el software de Single Sign-on Plug-in debe instalarse en cada uno de los servidores de la comunidad XenApp que aloje aplicaciones para las que se necesite autenticación con credenciales. Los usuarios acceden a estas aplicaciones a través de conexiones Citrix. El software del plug-in en el servidor determina el tipo de aplicación (Windows, Web o basada en emuladores de terminal) y obtiene las credenciales apropiadas en el almacén de credenciales local del perfil del usuario.

También se puede instalar Single Sign-on Plug-in en cada dispositivo cliente. Para entornos de XenApp, consulte las notas descritas más adelante. Si los usuarios ejecutan aplicaciones que están instaladas localmente en sus dispositivos, Single Sign-on plug-in debe estar instalado en los mismos para poder suministrar las credenciales de acceso a las aplicaciones locales.

Independientemente de si Single Sign-on Plug-in está instalado en el dispositivo del usuario, los usuarios pueden volver a registrar las respuestas a las preguntas de seguridad sin que lo pida el sistema, o sincronizar sus credenciales usando únicamente la función de Asociación de cuentas, usando aplicaciones publicadas a las que se les puede dar acceso después de instalar el plug-in en un servidor XenApp.

Single Sign-on se puede utilizar con:

- Access Gateway Advanced Edition (las aplicaciones están disponibles desde XenApp a través de un explorador Web)
- Componentes de Citrix XenApp:
  - Citrix Receiver para Windows
  - Citrix Offline Plug-in
  - Interfaz Web

Instalación del Single Sign-on Plug-in en dispositivos de usuario en entornos XenApp

En los entornos XenApp, la decisión de instalar o publicar Single Sign-on Plug-in en el dispositivo del usuario depende de qué tareas se quiera dejar realizar a los usuarios. Las credenciales se envían a las aplicaciones publicadas en todos los casos.

- Si no instala Single Sign-on Plug-in en los dispositivos de los usuarios, éstos pueden:
  - Registrar respuestas para las preguntas de seguridad cuando lo solicite el sistema
  - Almacenar credenciales automáticamente cuando lo solicite Single Sign-on
  - Cambiar la contraseña de un programa o sitio Web cuando lo solicite Single Sign-on
- Si publica la aplicación Administrar contraseñas (LogonManager.exe, instalada durante la instalación de Single Sign-on Plug-in), los usuarios pueden:
  - Registrar respuestas para las preguntas de seguridad cuando lo solicite el sistema
  - Almacenar credenciales automáticamente cuando lo solicite Single Sign-on
  - Cambiar la contraseña de un programa o sitio Web cuando lo solicite Single Sign-on
  - Modificar, eliminar o revelar las contraseñas almacenadas en Single Sign-on
- Si instala Single Sign-on Plug-in en los dispositivos de los usuarios, éstos pueden realizar todas las tareas disponibles de Single Sign-on:
  - Registrar respuestas para las preguntas de seguridad cuando lo solicite el sistema

- Almacenar credenciales automáticamente cuando lo solicite Single Sign-on
- Cambiar la contraseña de un programa o sitio Web cuando lo solicite Single Sign-on
- Modificar, eliminar o revelar las contraseñas almacenadas en Single Sign-on
- Almacenar credenciales automáticamente cuando lo solicite Single Sign-on
- Agregar contraseñas adicionales para programas y sitios Web que ya existen en Single Sign-on
- Poner Single Sign-on en pausa, reanudar Single Sign-on o averiguar si Single Sign-on está en pausa
- Cómo usar el autoservicio de cuentas

Planificación para autenticación principal múltiple y protección de credenciales de usuario

Oct 12, 2015

Al crear o modificar una configuración de usuario, pueden seleccionarse los métodos de protección de credenciales de usuario según los esquemas de autenticación que se utilizan en la empresa.

Las siguientes páginas de propiedades de configuración de usuario permiten ajustar el comportamiento del software de Single Sign-on Plug-in y el método de protección de datos de credenciales empleado cuando los usuarios aplican uno o varios métodos de autenticación principal.

Página Métodos de protección de datos

La página de propiedades Métodos de protección de datos de configuración de usuario permite seleccionar uno o varios métodos de protección de datos de autenticación principal. Asimismo, también se puede regular el acceso de los administradores a los datos de credenciales de los usuarios para evitar que los administradores suplanten a los usuarios y obtengan acceso no autorizado a la información de los mismos.

Página Protección de datos secundaria

Para mejorar la seguridad, cuando los usuarios cambien su autenticación principal (por ejemplo, se cambie una contraseña de dominio o se reemplace una tarjeta inteligente), la página de propiedades Protección de datos secundaria de configuración de usuario permite solicitar a los usuarios que se vuelvan a autenticar y verificar sus identidades antes de desbloquear sus credenciales de aplicación.

Seguridad y facilidad de uso

Las dos preguntas clave que hay que plantearse al decidir las opciones que se elegirán en estas dos páginas de propiedades de configuración de usuario son:

- ¿Qué tipos de autenticación se utilizan en el entorno para los usuarios que se van a administrar en esta configuración de usuario?
- ¿Cómo se pueden equilibrar los requisitos de seguridad para la empresa y la facilidad de uso para todos los usuarios?

También se debe tener en cuenta que las siguientes opciones no se excluyan entre sí y que se pueda emplear una combinación de ellas en la empresa (es decir, la autenticación principal múltiple). En última instancia, la decisión se basa en la necesidad de seguridad en vez de la facilidad de uso para los usuarios de la empresa.

Suplantación de usuarios

Si desea prohibir el acceso de administrador a las credenciales de usuario, seleccione Sí para la opción ¿Necesita regular el acceso del administrador de la cuenta a los datos del usuario?. como opción. Las credenciales se protegen de modo que los administradores no puedan suplantar a los usuarios y obtener acceso a la información del usuario.

El valor predeterminado para la página Métodos de protección de datos es Sí. Con esta configuración, el administrador de la cuenta, u otro administrador, no tiene acceso a las contraseñas o a los datos del usuario. Con este parámetro se evita que los administradores suplanten a los usuarios. El administrador no puede iniciar la sesión como el usuario con esta configuración predeterminada ni acceder a los datos que se encuentran en el almacén de credenciales local.

El parámetro Sí desactiva el uso de la opción API de protección de datos de Microsoft en esta página y la opción No

preguntarle a los usuarios; restaurar la protección de datos primaria automáticamente en la página Protección de datos secundaria siguiente. En este caso, no se permiten las tarjetas inteligentes ni los perfiles móviles y las credenciales no se restauran automáticamente después de un cambio de contraseña sin autenticación o verificación.

Para permitir el uso de todas las funciones de autenticación múltiple disponibles en esta página y en la página Protección de datos secundaria (incluida la capacidad para restaurar las credenciales automáticamente sin volver a realizar la autenticación o la verificación de identidad), se debe seleccionar No.

Nombre de usuario y contraseña

La implementación más simple es el valor predeterminado para la página Métodos de protección de datos: un entorno de sólo contraseña. El valor predeterminado permite a los usuarios utilizar su nombre de usuario y contraseña a la vez que se protegen sus credenciales frente al acceso no autorizado por parte de los administradores.

Importante: La seguridad de esta opción de configuración depende de la solidez relativa de la directiva de contraseña de dominio. Cuanto más sólido (o más complejo) sea el requisito de contraseña, más segura será esta opción.

Opción	Descripción
¿Necesita regular el acceso del administrador de la cuenta a los datos del usuario?	Consulte *— Suplantación de usuarios* .
Datos de autenticación de los usuarios	Seleccionado. Se utiliza un secreto de usuario para acceder y proteger los datos del usuario. En este caso, el secreto de usuario es una contraseña. La seguridad de la contraseña se puede derivar de la contraseña de dominio escrita del usuario o una contraseña de un solo uso de los dispositivos de token, de proximidad o biométricos.

Tarjetas inteligentes con certificados y datos de autenticación de usuario

Utilice Certificado de tarjetas inteligentes y Datos de autenticación de usuario si combina certificados incrustados o firmas digitales y datos de autenticación del usuario en su empresa. La combinación de tarjetas inteligentes con un nombre de usuario y una contraseña para la autenticación constituye la opción más segura para la protección de los datos de autenticación de usuario.

si se utilizan tarjetas inteligentes con Escritorio dinámico, se debe seleccionar la opción Certificados de tarjetas inteligentes.

Para poder usar tarjetas inteligentes en entornos con Windows Server 2008 o Windows Vista, el almacén central debe crearse o actualizarse con una consola de Single Sign-on 4.5 (anteriormente Password Manager) o una consola posterior, y hay que seleccionar API de protección de datos de Microsoft (necesita perfiles móviles) en las configuraciones de usuario.

Opción	Descripción
¿Necesita regular el acceso del administrador de la cuenta a los datos del usuario?	Consulte *— Suplantación de usuarios* .
Datos de autenticación de los usuarios	Seleccionado. Se utiliza un secreto de usuario para acceder y proteger los

Opción	Descripción
	datos del usuario. En este caso, el secreto de usuario es una contraseña. La seguridad de la contraseña se puede derivar de la contraseña de dominio escrita del usuario o una contraseña de un solo uso de los dispositivos de token, de proximidad o biométricos.
Certificados de tarjetas inteligentes	Seleccionado. En ese caso, el secreto de usuario se protege mediante cifrado y descifrado que proporciona el certificado de seguridad de la tarjeta.

Tarjetas inteligentes con PIN

Si se utilizan tarjetas inteligentes que no admiten certificados de seguridad como autenticador principal en un dominio de Windows o no se utilizan perfiles móviles, se debe usar la opción Permitir PIN de tarjetas inteligentes. Si se selecciona esta opción, las claves de cifrado utilizadas para proteger las credenciales secundarias se obtienen a partir del PIN de la tarjeta inteligente.

Se debe tener en cuenta la posibilidad de exigir el uso de un PIN difícil. En algunas empresas, los PIN de tarjetas inteligentes son números de cuatro dígitos que no proporcionan un nivel de protección tan sólido como el que ofrecen, por ejemplo, las contraseñas de ocho caracteres y pueden ser más vulnerables a los ataques. Sólo se utilice la opción PIN como contraseña si la directiva de seguridad de la empresa obliga a utilizar PIN que estén compuestos por un mínimo de ocho caracteres y en los que se mezclen letras y números.

Opción	Descripción
¿Necesita regular el acceso del administrador de la cuenta a los datos del usuario?	Consulte *— Suplantación de usuarios* .
Datos de autenticación de los usuarios	Seleccionado. Se utiliza un secreto de usuario para acceder y proteger los datos del usuario. En este caso, el secreto de usuario es un número de identificación personal (PIN).
Permitir PIN de tarjetas inteligentes	Seleccionado. Permitir que se utilice el PIN de tarjetas inteligentes como secreto de usuario para la protección. Esta opción sólo se debe utilizar si la empresa o el entorno dispone de una directiva de “PIN seguro”

Esta opción está respaldada por la versión 4.1 del plug-in de Single Sign-on (anteriormente Password Manager) si selecciona Usar la protección de datos como en Password Manager 4.1 y versiones anteriores y PIN como contraseña, en caso de que considere utilizar los plug-ins antiguos.

Perfiles móviles (DPAPI de Microsoft)

Seleccione No como respuesta a ¿Necesita regular el acceso del administrador de la cuenta a los datos del usuario? para

habilitar el uso de perfiles móviles y de la API de protección de datos de Microsoft en su entorno. Esta opción es la siguiente opción más segura después de las tarjetas inteligentes con certificados y los datos de autenticación de usuarios.

Esta opción se debe seleccionar si se utilizan perfiles móviles mediante un protocolo de autenticación de red Kerberos para los usuarios. La opción sólo funciona si hay perfiles móviles disponibles. Si se van a almacenar perfiles móviles en las estaciones de trabajo, se debe seleccionar esta opción.

Single Sign-on deriva las claves de cifrado que protegen las credenciales secundarias a partir de la contraseña principal del usuario. No obstante, si un usuario utiliza una tarjeta inteligente para la autenticación principal, no existe una contraseña principal y por tanto no se puede usar. En este caso, la mejor opción de plug-in es API de protección de datos de Microsoft. Esta opción utiliza DPAPI de Microsoft para derivar las claves de cifrado y proteger las credenciales secundarias. Este mecanismo de cifrado utiliza las credenciales de Windows o de dominio del usuario para derivar las claves de cifrado.

Si los usuarios emplean contraseña para acceder a sus equipos y un protocolo de autenticación de red Kerberos para acceder a servidores XenApp, se debe seleccionar:

- No como respuesta a ¿Necesita regular el acceso del administrador de la cuenta a los datos del usuario?
- Datos de autenticación de los usuarios
- API de protección de datos de Microsoft

Este método también permite el uso de credenciales de usuario y tarjetas inteligentes para iniciar la sesión.

Para poder usar tarjetas inteligentes en entornos con Windows Server 2008 o Windows Vista, el almacén central debe crearse o actualizarse con una consola de Single Sign-on 4.5 (anteriormente Password Manager) o una consola posterior, y hay que seleccionar API de protección de datos de Microsoft (necesita perfiles móviles) en las configuraciones de usuario.

Este método está respaldado por la versión 4.1 de Single Sign-on Plug-in y es compatible con las plataformas Windows XP y Windows 2003 Server. Si se van a utilizar plug-ins antiguos, se debe seleccionar las opciones Usar la protección de datos como en Single Sign-on 4.1 y versiones anteriores y DPAPI con perfil.

Contraseñas en blanco

Permitir el uso de contraseñas en blanco se debe considerar un caso especial y sólo se debe utilizar en entornos de baja seguridad que requieran una gran facilidad de uso. Una situación de este tipo se produce, por ejemplo, cuando hay que instalar una estación de trabajo común en la planta de una fábrica para que accedan numerosos usuarios. Se puede seguir utilizando Single Sign-on para controlar el acceso a las aplicaciones, pero las credenciales de usuario para acceder a dicha estación de trabajo pueden tener una contraseña en blanco.

Importante: Si no se selecciona esta opción y en el entorno se permiten las contraseñas en blanco, el plug-in no deriva un secreto de usuario ni realiza ninguna protección de datos con la contraseña en blanco.

Opción	**Descripción**
¿Necesita regular el acceso del administrador de la cuenta a los datos del usuario?	Consulte *— Suplantación de usuarios* .
Datos de autenticación de los usuarios	Seleccionado. Se utiliza un secreto de usuario para acceder y proteger los datos del usuario. En este caso, el secreto de usuario es una contraseña.

Opción	Descripción
Permitir la protección usando contraseñas en blanco	Seleccionado. Cuando se selecciona esta opción y el software del plug-in detecta que el usuario tiene una contraseña en blanco, se deriva un secreto de usuario para la protección de los datos a partir del ID de usuario.

Instalación y actualización

Oct 12, 2015

Se recomienda utilizar el siguiente orden de instalación de Single Sign-on:

1. Cree un almacén central.
2. Instale Citrix AppCenter, que incluye el componente de consola de Single Sign-on.
3. Instale el servicio Single Sign-on Service, si desea usar uno de los siguientes módulos:
   - Administración de claves
   - Autoservicio
   - Aprovisionamiento
   - Sincronización de credenciales
   - Integridad de datos
     Si decide instalar el módulo de integridad de datos más tarde o después de instalar Citrix AppCenter y Single Sign-on Plug-in, debe firmar digitalmente los datos del almacén central existente mediante la herramienta de firma de datos CtxSignData.exe. (Esta herramienta está disponible después de instalar el módulo de integridad de datos). Del mismo modo, si se desinstala el módulo de integridad de datos, es necesario eliminar la firma de los datos del almacén central.
4. Instale la Herramienta de definición de aplicaciones en uno o varios equipos del entorno cuando sólo sea necesario crear definiciones de aplicación. (Cuando se instala la función de servidor XenApp con sus componentes predeterminados, la Herramienta de definición de aplicaciones está incluida en la instalación).
5. Instale el Single Sign-on Plug-in en cada uno de los equipos de los usuarios y en el servidor XenApp.

Importante: Los servidores que alojan el servicio Single Sign-on Service y el almacén central de NTFS contienen información confidencial relacionada con los usuarios. Use un servidor dedicado y ubique dicho servidor en una ubicación segura físicamente.

Las siguientes combinaciones de instalación no se recomiendan ni se respaldan:

- El servicio y el plug-in no se deben instalar en el mismo equipo.
- El servicio y la función de servidor XenApp no se deben instalar en el mismo equipo.
- Single Sign-on no debe instalarse en un controlador de dominio. No está respaldada la instalación del plug-in, el servicio o la consola ni la creación de un almacén central de punto compartido NTFS en un controlador de dominio.

Actualización a Single Sign-on 5.0

Puede actualizar el entorno completo a Single Sign-on, versión 5.0, o bien planificar una actualización en etapas.

Para actualizar todo el entorno

1. A pesar de que no es necesario, Citrix recomienda actualizar a la versión más reciente de Licensing Server y agregar las licencias necesarias antes de actualizar a Single Sign-on.
2. Si va a usar uno de los modelos siguientes, actualice Single Sign-on Service. También puede instalar módulos adicionales en este momento.
   - Administración de claves
   - Autoservicio
   - Aprovisionamiento
   - Sincronización de credenciales
   - Integridad de datos

Nota: Si decide instalar el módulo de integridad de datos más tarde, o después de instalar el componente Single Sign-on de Citrix AppCenter y Single Sign-on Plug-in, debe firmar digitalmente los datos del almacén central existente mediante la herramienta de firma de datos CtxSignData.exe. (Esta herramienta está disponible después de instalar el módulo de integridad de datos). Del mismo modo, si se desinstala el módulo de integridad de datos, es necesario eliminar la firma de los datos del almacén central.

3. Actualice el componente de la consola de Single Sign-on de Citrix AppCenter (anteriormente Delivery Services Console) en uno o más de los equipos del entorno.
   Nota:
   - Citrix recomienda usar Single Sign-on Service y el componente de la consola con el mismo nivel de versión.
   - La actualización del componente de la consola, versión 5.0, también realiza una actualización en el almacén central de Single Sign-on. Después de actualizar una consola de Single Sign-on 4.8 a la versión 5.0, otras consolas de la versión 4.8 no podrán hacer cambios al almacén central.
4. Si necesita crear definiciones de aplicación solamente, actualice o instale la Herramienta de definición de aplicaciones en uno o más equipos de su entorno. (Cuando se instala la función de servidor XenApp con sus componentes predeterminados, la Herramienta de definición de aplicaciones está incluida en la instalación).
5. Actualice el almacén central de Single Sign-on.
   - Para los almacenes centrales NTFS compartidos de la red:
     - Realice una copia de seguridad de la carpeta compartida de red antes de actualizar el almacén central de Single Sign-on.
     - Seleccione el nodo Single Sign-on y ejecute el asistente de Configuración y ejecución del descubrimiento desde Citrix AppCenter para actualizar automáticamente el almacén central de Single Sign-on.
     - En el asistente, especifique la ruta UNC del punto compartido NTFS, normalmente \\nombre_servidor\CITRIXSYNC$, donde nombre_servidor es el nombre del servidor donde se ha creado el almacén central.
   - Para los almacenes centrales basados en Active Directory, seleccione el nodo Single Sign-on y ejecute el asistente de Configuración y ejecución del descubrimiento desde Citrix AppCenter para actualizar automáticamente el almacén central de Single Sign-on.
   - Si va a actualizar desde una versión de Citrix Password Manager compatible con la carpeta compartida de Novell (por ejemplo, versión 4.6), es posible que necesite realizar una copia de seguridad, y luego exportar e importar los datos administrativos para continuar usando los parámetros configurados en ese tipo de almacén de datos. Consulte la documentación de administración e instalación de Password Manager 4.6 para obtener información sobre el traslado de datos del almacén de datos. Existe documentación disponible en Citrix Knowledge Center.
6. Después de configurar las funciones de Single Sign-on en Citrix XenApp, actualice o instale el Single Sign-on Plug-in en cada dispositivo de usuario de su entorno.

Para realizar la actualización en etapas

1. Empiece agregando dispositivos de usuario con Single Sign-on 5.0 Plug-in a su entorno (Single Sign-on 4.8) existente.
2. Cuando esté listo, actualice Single Sign-on Service y la consola a la versión 5.0.
3. Distribuya Single Sign-on 5.0 Plug-in al resto de los dispositivos de usuario.

Configuración de seguridad y cuentas antes de instalar Single Sign-on

Oct 12, 2015

Antes de instalar el servicio Single Sign-on Service hay que asegurarse de que están disponibles las cuentas y componentes necesarios para respaldar el servicio. Además, debido a que el servicio utiliza HTTP seguro (HTTPS), requiere un certificado de autenticación de servidor para la comunicación mediante el protocolo SSL (Secure Sockets Layer) con la consola y el plug-in.

Obtención e instalación de un certificado de autenticación de servidor

Obtenga un certificado de autenticación del servidor para la comunicación SSL solicitándolo a una entidad de certificación (Certificate Authority o CA) o, si dispone de una infraestructura de claves públicas (PKI), descargue su propio certificado en el servidor que ejecuta el servicio.

Se necesita un certificado SSL para garantizar la comunicación segura desde el servicio hacia la consola y el plug-in, así como para garantizar que el plug-in y la consola se estén comunicando con el servidor de servicio correcto.

- Debido a que este certificado se utiliza para la comunicación SSL, el nombre común del mismo debe coincidir con el nombre completo de dominio (FQDN) del servidor que ejecuta el servicio. Se debe especificar un tamaño de clave mínimo de 1024.
- Instale el certificado en el almacén de certificados del equipo local y establezca las relaciones de confianza correspondientes para el plug-in y el componente de Single Sign-on de Citrix AppCenter.
- Instale este certificado en los equipos que ejecutan el componente de Single Sign-on de Citrix AppCenter, el servicio Single Sign-on Service y el plug-in.
- En un entorno con equilibrio de carga o clúster para el servicio, se puede utilizar un certificado para varios servidores de servicio si el nombre común del certificado SSL utiliza un carácter comodín (normalmente un asterisco) en él. Por ejemplo, se puede utilizar un certificado SSL con el nombre común servidor*.nombredemiempresa.com para un entorno con servidores denominados servidor1.nombredemiempresa.com, servidor2.nombredemiempresa.com y servidor3.nombredemiempresa.com. En este caso, también se puede utilizar un certificado SSL con el nombre común *.nombredemiempresa.com, donde el nombre común no coincide con el nombre completo de dominio (FQDN) del servidor.

Importante: Si obtiene el certificado de una entidad de certificación que no es de confianza de forma predeterminada (por ejemplo, una entidad de certificación instalada en su empresa), instale el certificado raíz de la entidad en el almacén de certificados raíz de confianza del equipo local para establecer la relación de confianza.
Si los usuarios ven errores de SSL, probablemente se deba a que el certificado del servidor no es de confianza. Consulte el sitio Web de Microsoft para obtener instrucciones sobre cómo extraer e instalar certificados raíz de entidades de certificación.

Los certificados de firma y validación creados durante la instalación de Single Sign-on no tienen ninguna relación con el certificado SSL.

Cuentas necesarias para los módulos del servicio

El servicio Single Sign-on Service puede necesitar hasta tres tipos de cuenta de sistema para leer y escribir datos mientras actúa en el entorno. La cantidad y el tipo de las cuentas necesarias dependen de los módulos de servicio que se utilicen. En esta tabla se muestran las cuentas que necesita cada módulo del servicio. En los casos donde los distintos módulos requieren el mismo tipo de cuenta, se puede utilizar la misma cuenta para varios módulos o se pueden especificar distintas

cuentas personalizadas para cada módulo.

Módulo	Cuentas necesarias		
	Servicio	Proxy de datos	Autoservicio
Integridad de datos	Sí	No	No
Administración de claves	Sí	Sí	No
Aprovisionamiento	Sí	Sí	No
Autoservicio	Sí	Sí	Sí
Sincronización de credenciales	Sí	No	No

Requisitos de la cuenta de servicio

En el servidor donde se ejecuta el servicio Single Sign-on Service, utilice las cuentas Servicio de red o Servicio local existentes.

No se puede especificar una cuenta de usuario local como la cuenta de servicio en esta versión de Single Sign-on. Se puede especificar la cuenta Servicio local incorporada.

Si se decide crear una cuenta de dominio como la cuenta de servicio, se debe registrar un nombre principal de servicio para esta cuenta dominio y el servidor de servicio en Active Directory mediante la utilidad setspn.exe. Si usa una cuenta de usuario de dominio, la cuenta debe tener asignados derechos para "iniciar sesión como servicio". El equipo que ejecuta el servicio debe ser de confianza para la delegación.

Visite el sitio Web de Microsoft para obtener más información sobre los nombres principales de servicio.

Requisitos de cuenta del proxy de datos

En el servidor donde se ejecuta el servicio Single Sign-on Service, cree una cuenta de administrador de dominio con los siguientes parámetros, que se utilizará para la comunicación del proxy de datos con el servicio.

La cuenta requiere permisos de lectura y escritura en el almacén central. Los requisitos de cuenta dependen del tipo de almacén central que se instale.

Tipo de almacén central	Descripción de la cuenta
Punto compartido NTFS	La cuenta: • Requiere permisos de lectura y escritura en el almacén central. • Es miembro del dominio. Después de crear el almacén central: • Conceda a la cuenta permisos de Control total para uso compartido en el recurso compartido CITRIXSYNC$.

Tipo de almacén central	Descripción de la cuenta
	• Conceda a la cuenta permisos de Control total en la carpeta CITRIXSYNC y sus subcarpetas: CentralStoreRoot y People. • Conceda a la cuenta permisos de Control total en todos los objetos de archivo dentro de la carpeta CITRIXSYNC y sus subcarpetas. • Asegúrese de que el grupo Usuarios autenticados tiene el derecho para crear carpetas dentro de la carpeta People.
Active Directory	La cuenta: • Requiere permisos de lectura y escritura en el almacén central. • Es miembro del grupo de administradores del dominio.

Requisitos de Self-Service

Si se utilizan las funciones de Autoservicio de restablecimiento de contraseñas o Autoservicio de desbloqueo de cuentas del módulo Autoservicio de cuentas, se debe utilizar una cuenta que sea miembro del grupo de administradores del dominio.

Cuentas necesarias para instalar y utilizar Single Sign-on

El usuario que instala el servicio Single Sign-on y ejecuta el asistente de configuración del servicio debe ser miembro del dominio (un usuario de dominio) y miembro del grupo Administradores local en el equipo que ejecuta el servicio (se agrega una cuenta de usuario de dominio al grupo Administradores local).

El usuario que instala el componente de consola de Single Sign-on, realiza una operación de descubrimiento y configuración y utiliza el componente de consola debe ser un administrador de dominio y un miembro del grupo Administradores local en el equipo donde se ejecuta la consola. Esta cuenta de usuario debe tener permisos de lectura y escritura en el almacén central. A una cuenta de usuario no administrador se le puede asignar el derecho de administrar el componente de consola y sus funciones relacionadas mediante la delegación de Active Directory o la delegación restringida.

El usuario que instala Single Sign-on Plug-in debe ser un miembro del dominio (un usuario de dominio) y un miembro del grupo Administradores local en el dispositivo del usuario. El usuario que instala el plug-in debe ser un miembro del dominio (un usuario de dominio) y un miembro del grupo Administradores local en el dispositivo del usuario. El usuario que ejecuta el plug-in debe ser un miembro del dominio (usuario de dominio).

Instalación de Java Runtime Environment (JRE)

Oct 12, 2015

Single Sign-On respalda Java Runtime Environment (JRE), versiones 1.4.x, 5 (1.5.x) y 6 (1.6.x). Descargue la versión con respaldo del sitio Web de Sun Microsystems (http://java.sun.com).

Si se instala o actualiza JRE después de instalar los componentes de Single Sign-On

Si instala o actualiza JRE después de instalar el componente de Single Sign-On de Delivery Services Console, Herramienta de definición de aplicaciones o plug-in, asocie el JRE actual al componente de Single Sign-On.

1. En Panel de control, vaya al área Programas y seleccione el componente de Single Sign-On.
2. Haga clic en Cambiar.
3. En el cuadro de diálogo de instalación, seleccione Reparar.

Solución de problemas del mensaje de error de Java al instalar o desinstalar el plug-in

Puede aparecer el siguiente mensaje de error cuando se intenta instalar o desinstalar el plug-in:

"Citrix Single Sign-On detectó que uno o más programas o archivos de software Java están en uso. Cierre todos los programas y detenga todos los servicios vinculados con Java antes de continuar". "

Normalmente, este error se produce si se instala el plug-in en un equipo que también ejecuta un servicio de servidor Web, como Apache Tomcat, servidor Apache HTTP. Además, este error puede aparecer si se instala el plug-in en un servidor XenApp con License Management Console instalada.

En este caso, realice los siguientes pasos:

1. Detenga el servicio.
2. Instale o desinstale el plug-in.
3. Reinicie el servicio.

Creación de un almacén central

Oct 12, 2015

1. Cargue el medio de instalación de XenApp.
2. En el menú de Autorun, seleccione Instalar componentes manualmente > Componentes de servidor > Funciones adicionales > Single Sign-on.
3. Seleccione Almacén central.
4. Seleccione un tipo de almacén central: punto compartido NTFS o Active Directory.
   - Si selecciona Punto compartido NTFS, el almacén central se crea como %SystemDrive%\CITRIXSYNC$.
   - Si selecciona Active Directory:
     1. Seleccione Paso 1: Extender Active Directory. Se extenderá el esquema de Active Directory.
     2. Seleccione Paso 2: Crear el almacén central.
     3. Una vez creado el almacén central, reinicie el servidor donde está instalada la consola de Single Sign-On. Es necesario hacer esto para poder detectar el almacén central.

     Importante: El servidor actual debe ser parte del dominio de Active Directory y el usuario actual debe ser miembro de los grupos Administradores del esquema y Administradores del dominio. Hay que asegurarse de que el maestro de esquema de Active Directory está configurado para permitir actualizaciones. Además, si el servidor en el que está extendiendo el esquema de Active Directory no es el controlador de dominio, asegúrese de que la utilidad de Microsoft Windows Ldifde.exe esté instalada en el mismo antes de llevar a cabo este paso. Encontrará la utilidad en el disco de instalación de Windows o en el sitio Web de Microsoft. Este proceso no podrá completarse si Ldifde.exe no está instalado.

Instalación del componente de la consola

Oct 12, 2015

El componente de consola de Single Sign-on está incluido al instalar Citrix AppCenter.

Importante: Es necesario crear el almacén central de Single Sign-on antes de completar el asistente Configurar y ejecutar descubrimiento y usar Single Sign-on.

Para instalar AppCenter (con el componente de consola de Single Sign-on) al instalar XenApp

1. Siga el procedimiento de instalación de las Funciones del servidor Citrix XenApp. De manera predeterminada, AppCenter viene incluido en la instalación.
2. Seleccione Configurar y ejecutar descubrimiento y siga las instrucciones.

Para instalar AppCenter (con el componente de consola de Single Sign-on) manualmente

Asegúrese de que los paquetes redistribuibles Microsoft Visual C++ Redistributable Package y los ensamblados de interoperabilidad primarios de Microsoft se encuentren instalados, como se describe en Requisitos del sistema.

1. Cargue el medio de instalación de XenApp en el equipo.
2. En el menú de Autorun, haga clic en Instalar componentes manualmente > Componentes comunes > Consolas de administración. Siga las instrucciones.
3. Seleccione Configurar y ejecutar descubrimiento y siga las instrucciones.

Instalación y configuración de módulos del servicio

Oct 12, 2015

El flujo de trabajo de la instalación y la configuración es el siguiente:

1. Adquirir e instalar un certificado SSL en los equipos que ejecutan el servicio, la consola y el plug-in de Single Sign-on
2. Crear el tipo de cuenta necesario para los módulos del servicio que se van a instalar
3. Instalar los módulos del servicio
4. Configurar los módulos del servicio

En los siguientes procedimientos se presupone que el disco de instalación está cargado en el equipo elegido para alojar los módulos del servicio Single Sign-on Service y que se está viendo la pantalla de Autorun de XenApp.

Para instalar los módulos del servicio

1. Cargue el medio de instalación de XenApp.
2. En el menú de Autorun, seleccione Instalar componentes manualmente > Componentes de servidor > Funciones adicionales > Single Sign-on > Single Sign-on Service.
3. Siga las instrucciones.

Para configurar los módulos del servicio

El Asistente de configuración del servicio se inicia cuando finaliza la instalación de los módulos de servicio. Si lo desea, puede abrir el asistente en otro momento seleccionando Inicio > Todos los programas > Citrix > Password Manager > Configuración del servicio.

Siga las instrucciones.

- En la página Configuración del servicio:

Parámetros de conexión	Especifique el número de puerto de la conexión del servicio; el predeterminado es 443. Se puede usar cualquier otro puerto disponible en el servidor que ejecuta el servicio. Si más adelante instala uno o varios módulos de servicio, use el mismo número de puerto especificado al instalar el servicio por primera vez. El servicio no se puede ejecutar en varios puertos a la vez. Si especifica un puerto erróneo, Single Sign-on puede mostrar mensajes de error del tipo “no es posible comunicarse o conectarse con Single Sign-on Service”. Especifique el número de puerto de servicio correcto cuando use la Herramienta de firma de integridad de datos.
Certificado SSL	Seleccione el certificado SSL instalado en el equipo del servicio que se utilizará para la comunicación con los dispositivos cliente. Seleccione la casilla de verificación Mostrar el nombre largo para mostrar la información de LDAP Parámetro de conexión que está incluida en el certificado.

Nombre de host virtual	De forma predeterminada, está seleccionado Usar el valor predeterminado si el nombre de certificado SSL y el nombre de host virtual coinciden. El nombre de host virtual debe coincidir con el nombre de certificado SSL. El host virtual es el nombre de equipo mostrado a los usuarios al crear el certificado y es posible que no sea el nombre real del equipo. Por ejemplo, el nombre de certificado puede incluir un nombre de dominio comodín (asterisco) o en mayúsculas o minúsculas que no coincida con las letras minúsculas y mayúsculas del nombre de dominio de certificado. Este parámetro resulta útil en un entorno de servicios con equilibrio de carga o en clúster.
Credenciales de la cuenta	Seleccione la cuenta de equipo local que se utilizará para el servicio. Normalmente, se puede seleccionar la cuenta Servicio de red.

- En la página Configurar dominios:
  1. Seleccione la casilla contigua a cada uno de los dominios en los que quiera habilitar el respaldo al servicio.
  2. Seleccione uno o más dominios y haga clic en Propiedades para abrir el cuadro de diálogo Modificar configuración.
  3. Si creó un almacén central en Active Directory, seleccione Controlador de dominio y seleccione el controlador de dominio correcto en la lista.
  4. Haga clic en Cuenta del proxy de datos y escriba el nombre de usuario, la contraseña y el dominio de la cuenta del proxy de datos para establecer comunicación con el almacén central.
  5. Si instaló el módulo de autoservicio, seleccione Cuenta de las funciones del autoservicio y escriba las credenciales de la función. Haga clic en Aceptar para cerrar el cuadro de diálogo Modificar configuración.
     Importante: Si el servicio se está ejecutando en un entorno Windows Server 2008 o Windows Server 2008 R2 con un almacén central de NTFS, deberá usar CtxFileSyncPrep.exe para agregar la cuenta de proxy de datos como administrador del almacén central. Escriba:
     CtxFileSyncPrep [/Admin:nombre de la cuenta]

     Si el servicio se está ejecutando en un entorno Windows Server 2008 o Windows Server 2008 R2 con un almacén central de Active Directory, también deberá agregar la cuenta de proxy de datos como administrador del almacén central. Encontrará sugerencias para hacerlo en el sitio Web de Citrix (http://support.citrix.com/article/ctx107690)

Configuración del servicio para su uso en varios dominios

El servicio Single Sign-on Service puede procesar solicitudes de servicio de usuarios de distintos dominios con relación de confianza. Un administrador puede instalar Citrix AppCenter con el componente de consola de Single Sign-on en equipos de distintos dominios y crear una o más configuraciones de usuario en cada dominio.

Por ejemplo, con el equipo de Single Sign-on Service ubicado en DominioA, los usuarios asociados con una configuración en ese dominio pueden usar la función de autoservicio de cuentas para desbloquear sus cuentas. Los usuarios asociados con una configuración de usuario en el DominioB también pueden usarla, provista por el equipo de DominioA. En este caso, existen varias configuraciones de usuario en varios dominios y todas ellas deben compartir el mismo servicio.

Requisitos de la función de dominios múltiples

Antes de implementar la función de dominios múltiples, asegúrese de que satisfagan los siguientes requisitos:

Componente	Requisito
Dominios	Cada dominio que comparta el servicio debe ser parte del mismo bosque. Los dominios del bosque deben tener una relación de confianza transitiva bidireccional.
Almacén central	Esta función está disponible para implementaciones que usan Active Directory o puntos compartidos NTFS para los almacenes centrales. Todos los usuarios que compartan el equipo del servicio deben implementarse usando el mismo tipo de almacén central: Active Directory o punto compartido NTFS. El uso de varios tipos de almacén central no está respaldado. No está respaldado en este caso el uso de un almacén central de punto compartido NTFS para cada dominio. Sin embargo, se puede usar un almacén central en un punto compartido NTFS por bosque.
Función de integridad de datos	La función de integridad de datos se debe configurar consistentemente en todos los dominios. Es decir, debe estar activada o desactivada en las configuraciones del servicio y Single Sign-on Plug-in para todos los dominios. Por ejemplo, no se puede activar esta función en la configuración del servicio y desactivarla al instalar el plug-in.
Componente de consola de Single Sign-on en Citrix AppCenter	Cada consola puede ver únicamente un almacén central, no varios. El administrador de Single Sign-on debe instalar una consola en cada dominio e instalarla usando una cuenta de usuario con privilegios de administrador en el dominio. De forma alternativa, el administrador puede instalar una consola con la capacidad de acceder a otros dominios y, según sea necesario, cambiar a uno de esos dominios iniciando una sesión con las credenciales específicas de dicho dominio.
Cuentas del proxy de datos y del autoservicio	Sólo se puede configurar una cuenta de proxy de datos y de autoservicio de cuentas que tenga acceso de lectura y escritura al almacén central y privilegios suficientes para restablecer las contraseñas de usuario y desbloquear las cuentas de usuario. Opcionalmente, estas cuentas se pueden especificar para cada dominio, en la herramienta de configuración del servicio.

Para configurar el servicio para su uso con varios dominios

1. Inicie una sesión como administrador en el equipo en el que está instalado el servicio.
2. Inicie la herramienta de Configuración del servicio, hacienco clic en Inicio > Todos los programas > Citrix > Password Manager > Configuración del servicio.
3. Cuando aparezca la Herramienta de configuración del servicio, haga clic en Configuraciones de dominios en el panel

izquierdo.

4. Elija la casilla de verificación junto a los dominios para habilitar el respaldo del servicio en cada dominio seleccionado.
5. Seleccione uno o más dominios y haga clic en Propiedades para abrir el cuadro de diálogo Modificar configuración.
6. En el cuadro de diálogo Modificar configuración:
    1. Si creó un almacén central de Active Directory, haga clic en Controladores de dominio y, en la lista, seleccione el controlador de dominio que desea vincular con Single Sign-on, o seleccione Cualquier controlador de dominio en que se pueda escribir.
    2. Haga clic en Cuenta del Proxy de datos y escriba el nombre de usuario, la contraseña y el dominio de la cuenta del Proxy de datos para establecer comunicación con el almacén central.
    3. Si instaló el módulo de autoservicio, haga clic en Cuenta de las funciones del autoservicio y escriba las credenciales de la función.

Instalación del Single Sign-on Plug-in

Oct 12, 2015

El Single Sign-on Plug-in se ejecuta en el servidor XenApp y suministra credenciales y acceso a las aplicaciones publicadas. El plug-in también se ejecuta en cada uno de los dispositivos de usuario, suministrando las credenciales, el acceso a aplicaciones ejecutadas localmente en el dispositivo y la capacidad de controlar el funcionamiento de Single Sign-on.

Nota: Cuando se usa esta versión del plug-in en XenApp para publicar aplicaciones habilitadas para Single Sign-on, los dispositivos de usuario también deben tener instalado el plug-in. Si el dispositivo de usuario no tiene instalado el plug-in, Single Sign-on enviará automáticamente las credenciales correspondientes a las aplicaciones publicadas con XenApp, pero el usuario no podrá modificar, eliminar ni revelar las contraseñas, ni poner en pausa o reanudar Single Sign-on, ni averiguar si Single Sign-on está en pausa ni enviar contraseñas manualmente.
Consideraciones acerca de la instalación:

- La instalación de esta versión de Single Sign-on Plug-in en un dispositivo de usuario actualiza la versión 4.8.
- Después de instalar el plug-in en un sistema operativo compatible que esté usando el componente Microsoft Graphical Identification and Authentication (GINA) de Windows es necesario reiniciar el equipo. Esto incluye Windows XP, Microsoft Windows XP Embedded, Microsoft Windows Fundamentals for Legacy PCs, Microsoft Windows Server 2003 R2 y Microsoft Windows Server 2003 con Service Pack 2.
  WinLogon utiliza los controles GINA para el cuadro de diálogo que los usuarios ven cuando presionan la combinación de teclas CTRL + ALT + SUPR. El cuadro de diálogo obtiene los datos necesarios para realizar la autenticación. XenApp, Single Sign-on Plug-in y el cliente de Novell NetWare interactúan con Microsoft GINA o requieren el reemplazo de su biblioteca DLL. Es posible que tenga que instalar o desinstalar software en un orden específico para conservar la cadena GINA correcta. Instalando el Single Sign-on Plug-in en último lugar, se garantiza que el proceso Winlogon invoque a la GINA de Single Sign-on en primer lugar.
- Una vez finalizada la instalación (y después de reiniciarse el dispositivo, si es necesario) el icono de Citrix Receiver aparecerá en la bandeja del sistema.
- Después de instalar el plug-in, si se configura o se cambia la información de licencias de Citrix hay que reiniciar el plug-in para aplicar esos cambios.

Para instalar el Single Sign-on Plug-in en un servidor al instalar XenApp (con el asistente)

1. Siga las instrucciones indicadas en
   — Instalación de XenApp mediante el Administrador de funciones del servidor basado en asistentes
   . En la lista de Componentes optativos, seleccione Single Sign-on Plug-in.
2. Cuando se configura XenApp usando la herramienta de configuración del servidor basada en asistentes, el sistema le pide que seleccione el tipo de almacén central: Microsoft Active Directory (predeterminado) o Punto compartido NTFS y su ruta.

Para instalar el Single Sign-on Plug-in en un servidor al instalar XenApp (con la interfaz de comandos)

1. Siga las instrucciones indicadas en
   — Instalación de XenApp desde la línea de comandos
   . Incluya la opción SSONAgentFeature (/install:XenApp,SSONAgentFeature).
2. Cuando se configura XenApp mediante la línea de comandos se puede incluir la opción /SSOPluginUncPath:ruta para especificar la ruta UNC del punto compartido NTFS donde está el almacén central. Si se omite esta opción, se presupone el uso de Active Directory.

Para instalar el Single Sign-on Plug-in en un dispositivo de usuario o en un servidor con XenApp instalado

1. Cargue el medio de instalación de XenApp en el equipo o en el servidor.
2. En el menú de Autorun, seleccione Instalar componentes manualmente > Componentes de servidor > Funciones adicionales > Single Sign-on > Single Sign-on Plug-in.
3. Siga las instrucciones. Tendrá que seleccionar el tipo de almacén central y los componentes a instalar (tales como paquetes de idioma, autoservicio e integridad de datos).

Para instalar Single Sign-on Plug-in en un dispositivo de usuario usando Merchandising Server

Siga las instrucciones para la descarga o distribución de plug-ins incluida en la documentación de Merchandising Server.

Consolidación de iconos en el área de notificación de Microsoft Windows

Cuando se usa esta versión de Single Sign-on Plug-in para todas las sesiones de XenApp y en cada uno de los dispositivos de usuario, el área de notificación de Microsoft Windows en cada dispositivo de usuario contiene un único icono de Receiver, que incluye un menú de Single Sign-on integrado que consolida todas las sesiones.

No obstante, si XenApp o el dispositivo de usuario utilizan una versión más antigua de plug-in, el área de notificación de Windows puede contener otros iconos correspondientes a Single Sign-on. Esta tabla muestra los posibles casos.

Dispositivo de usuario		**Servidor XenApp**		**Área de notificación de Windows**	**¿Menú de contraseñas disponible en el icono de Receiver?**
Citrix Receiver	**Single Sign-on Plug-in**	**Citrix Receiver**	**Single Sign-on Plug-in**		
Actual *	5.0	Actual	5.0	Un icono de Receiver	Sí
Actual	-	Actual	5.0	Un icono de Receiver	No
Actual	5.0	-	4.8	Un icono de Receiver y un icono de Single Sign-on para cada sesión de XenApp conectada. **	Sí
Actual	4.8	Actual	5.0	Un icono de Receiver y un icono de Single Sign-on	No
Actual	4.8	Actual	4.8	Un icono de Receiver y un icono de Single Sign-on, más un icono de Single Sign-on para cada sesión de XenApp conectada. **	No
Online plug-in anterior	4.8	Actual	5.0	Un icono de Single Sign-on y un icono de online plug-in	No

* Actual = Receiver para Windows, que contiene el Online Plug-in

** Si los servidores XenApp están ejecutando una versión más antigua de Single Sign-on Plug-in, y el Receiver actual está instalado en el dispositivo del usuario (independientemente de si hay algún Single Sign-on Plug-in instalado en el

Dispositivo de usuario		Servidor XenApp		Área de notificación de Windows	¿Menú de contraseñas disponible en el icono de Receiver?
Citrix Receiver	Single Sign-on Plug-in	Citrix Receiver	Single Sign-on Plug-in		
dispositivo del usuario), el área de notificación de Windows en el dispositivo del usuario contendrá un icono de Single Sign-on para cada uno de esos servidores XenApp (que ejecutan la versión antigua del plug-in) con los que esté conectado.					

Administración

Oct 12, 2015

Puede utilizar las directivas de contraseña para definir las reglas que controlan las características de las contraseñas guardadas de los usuarios. Las reglas constan de directivas de contraseña, que pueden aplicarse a todos los usuarios o a determinados grupos de aplicaciones, dependiendo de las necesidades de la empresa.

Nota: Citrix XenApp cuenta con diversas reglas de directivas que permiten configurar y controlar qué usuarios pueden acceder a Single Sign-on cuando se conectan a servidores y aplicaciones publicadas en la comunidad de servidores. A pesar de los nombres similares, estos dos tipos de directivas no están relacionados.
Single Sign-on incluye dos directivas de contraseña estándar llamadas Predeterminada y Dominio. Estas directivas se pueden utilizar tal como están, copiar o modificar según las directivas y normativas de la empresa. No es posible eliminar las directivas Predeterminada y Dominio.

Cuando un usuario agrega sus credenciales a la ventana Administrar contraseñas (anteriormente conocida como Administrador de inicios de sesión) para una aplicación que no está definida por un administrador, Single Sign-on utiliza la directiva Predeterminada para administrar esa aplicación. Para que un grupo de aplicaciones se considere un grupo de contraseñas compartidas de dominio, aplique la directiva Dominio al grupo de aplicaciones.

Dado que Single Sign-on aplica la directiva de contraseñas Predeterminada a todas las aplicaciones agregadas por el usuario, es necesario que la directiva Predeterminada se configure lo más ampliamente posible de modo que acepte contraseñas para las aplicaciones para las que se permita almacenar contraseñas.

Se pueden crear tantas directivas como se necesiten en la empresa. Por ejemplo, puede aplicar una directiva para el grupo que comparte dominio y crear directivas individuales que se aplicarán a grupos individuales de aplicaciones con el fin de establecer unos requisitos concretos. Con una directiva de contraseña, se puede:

- Automatizar los cambios de contraseña de las aplicaciones.
- Implementar planes de seguridad, incluido el uso de contraseñas complejas y contraseñas ocultas específicas de cada aplicación.
- Definir cuándo caducarán las contraseñas de las aplicaciones, aunque éstas no tengan funciones que permitan especificar la caducidad de las contraseñas.
- Evitar que los usuarios vuelvan a utilizar la misma contraseña para la misma aplicación dos veces seguidas.

Grupos de contraseñas compartidas

Los usuarios pueden tener una sola contraseña que se utiliza para varias aplicaciones (una suite de productos, por ejemplo). Esto se denomina contraseñas compartidas, donde la misma autoridad de autenticación se utiliza para las aplicaciones.

Aunque el resto de las credenciales de estas aplicaciones (como el nombre de usuario y los campos personalizados) pueden ser diferentes, la contraseña del usuario es la misma. En este caso, se debe crear un grupo de aplicaciones que sea a su vez un grupo de contraseñas compartidas para garantizar que Single Sign-on Plug-in administre la contraseña de todas las aplicaciones del grupo como si fueran una única aplicación. Cuando se modifica la contraseña de una aplicación, Single Sign-on Plug-in hace que el cambio se refleje en las credenciales almacenadas para todas las aplicaciones del grupo.

Grupos de contraseñas de dominio compartidas

Los grupos de contraseñas de dominio compartidas son distintos de otros grupos de contraseñas compartidas ya que la contraseña de dominio del usuario es válida para todo el grupo de aplicaciones. Cuando el usuario modifica la contraseña de dominio, Single Sign-on Plug-in refleja el cambio en las credenciales del resto de las aplicaciones del grupo. Sólo puede

modificarse la contraseña de dominio. Los usuarios no pueden cambiar las contraseñas de ninguna de las otras aplicaciones del grupo a menos que el administrador elimine la aplicación del grupo de contraseñas de dominio compartidas.

Aplicación de directivas de contraseña

Single Sign-on aplica las directivas de contraseña, independientemente de que la contraseña sea definida por el usuario o generada automáticamente por Single Sign-on.

Las directivas de contraseñas no se aplican cuando:

- Los usuarios se registran con Single Sign-on (durante el primer uso).
- Los usuarios editan una contraseña desde la ventana Administrar contraseñas (anteriormente conocida como Administrador de inicios de sesión).
- El administrador crea una definición de aplicación.

Single Sign-on no aplica directivas de contraseña a contraseñas existentes (aquellas creadas antes de la implementación de Single Sign-on en la empresa) dado que es probable que se les niegue el acceso a los usuarios a determinadas aplicaciones o recursos actualmente en uso.

Configuración de Single Sign-On para que reconozca aplicaciones

Oct 12, 2015

Single Sign-On reconoce y responde a aplicaciones basadas en los parámetros identificados en definiciones de aplicación.

Las definiciones de aplicación contienen formularios que permiten al Single Sign-on Plug-in analizar cada aplicación a medida que se inicia, reconocer determinadas características de identificación y determinar si la aplicación iniciada requiere que el plug-in lleve a cabo alguna acción específica, como:

- Enviar credenciales de usuario en un diálogo de inicio de sesión
- Negociar una interfaz de cambio de credenciales
- Procesar una interfaz de confirmación de credenciales

Las definiciones de aplicación constan de conjuntos de características de reconocimiento y acciones de formulario de credenciales de usuario, denominadas definiciones de formulario, y el conjunto de opciones de configuración que se aplican a todos los formularios de la configuración.

Los parámetros de definición de formularios establecen las acciones que realiza Single Sign-On cuando una aplicación solicita una acción de credenciales de usuario específica.

Una definición de aplicación se compone de todos los formularios de administración de credenciales de usuario asociados a una sola aplicación.

Aunque la mayoría de las aplicaciones y sus correspondientes definiciones utilizan únicamente dos formularios para administrar las credenciales de usuario, es posible definir tantos formularios como necesite una aplicación.

Single Sign-on proporciona compatibilidad con una variedad de aplicaciones, incluidas las de Windows, Web y basadas en emuladores de terminal. Funciona en aplicaciones Java, soluciones SAP y aplicaciones alojadas en un Mainframe, sistema AS/400 o servidor UNIX.

Para crear definiciones de aplicación destinadas a aplicaciones que no tienen plantillas de aplicación predefinidas, se deben utilizar los asistentes disponibles. El Asistente de definición de aplicaciones configura las características asociadas a todos los formularios incluidos en la definición. El Asistente de definición de formularios presenta un procedimiento paso a paso para definir el respaldo para aplicaciones de Windows, Web y basadas en emuladores de terminal.

Single Sign-on también ofrece la capacidad de llevar a cabo un descubrimiento de aplicaciones externas y el procesamiento de acciones. Esto permite a otros implementadores ampliar las tareas de detección de aplicaciones y envío de credenciales asociadas a un formulario al proporcionar acceso a procesos externos durante las fases de detección de aplicaciones y de procesamiento de envío de acciones en Single Sign-on Plug-in.

Estas funciones se combinan para proporcionar un entorno de desarrollo de definiciones de aplicación flexible y adaptable para respaldar a su comunidad de usuarios con un acceso de inicio de sesión único, seguro y flexible a las aplicaciones importantes.

Precaución: Single Sign-on depende del funcionamiento seguro de todos los equipos en los que haya componentes del producto. Si el equipo del usuario se infecta con un código destructivo, existe el riesgo de que dicho código afecte la seguridad que brinda Single Sign-on. Para evitar en lo posible dichos riesgos, siga las prácticas de seguridad estándar para mantener la infraestructura de su empresa segura.

Plantillas de aplicación

Las plantillas de aplicación son archivos XML que se utilizan para compartir definiciones de aplicaciones entre distintos entornos de Single Sign-on. Las plantillas de aplicación ahorran tiempo y esfuerzo porque pueden convertirse en definiciones de aplicación con una mínima intervención o configuración. Las plantillas requieren la introducción de información para completar la definición de aplicación, ya sea una URL o nombre de archivo ejecutable, caducidad de la contraseña y cualquier parámetro avanzado de detección.

Instale las plantillas de aplicación mediante el nodo Single Sign-on de Citrix AppCenter o la Herramienta de definición de aplicaciones. Ambas herramientas incluyen plantillas para las aplicaciones de Windows y Web más habituales.

Importante: Para escribir en un almacén central de Active Directory mientras está ejecutando Windows Server 2008, Windows Server 2008 R2, Windows Vista o Windows 7, otorgue a la Herramienta de definición de aplicaciones un nivel de integridad Alto. Inicie sesión en una cuenta que sea miembro del grupo de administradores locales para iniciar la herramienta en el equipo del sistema, y que sea miembro del grupo de administradores de dominio o que tenga privilegios de escritura para los objetos de Active Directory en el almacén central. Ingrese estas credenciales al ejecutar la herramienta, ya sea con el Control de cuentas de usuario o al iniciar la sesión en el sistema. Si lo hace, la herramienta tendrá un nivel de integridad alto y podrá escribir en Active Directory.
Cuando no se encuentra una plantilla para una aplicación, se puede crear una definición de aplicación mediante el nodo Single Sign-on de Citrix AppCenter o la Herramienta de definición de aplicaciones.

Identificación de aplicaciones y de sucesos de administración de credenciales de usuario por parte de Single Sign-On Plug-in

Oct 12, 2015

La interfaz de usuario de una aplicación incluye distintos formularios que se utilizan para administrar los sucesos de credenciales de usuario asociados a la aplicación.

Por ejemplo, un formulario ingresa las credenciales de inicio de sesión, otro formulario cambia la contraseña de la aplicación y un tercer formulario confirma un cambio correcto en las credenciales de usuario.

Según el tipo de aplicación que se defina (Windows, Web o emuladores de terminal), Single Sign-on utiliza distintos tipos de identificadores recopilados en definiciones de aplicación para responder a los formularios e identificarlos. Se incluyen, entre otros, el tipo de aplicación, el título de la ventana y el nombre del archivo ejecutable.

Cuando Single Sign-on Plug-in identifica la aplicación y el formulario, solicita al usuario que proporcione o almacene las credenciales, envía credenciales almacenadas, o pide a los usuarios que actualicen la información de las credenciales en función de los parámetros definidos.

Las definiciones de aplicación pueden crearse mediante AppCenter o con la Herramienta de definición de aplicaciones.

Una sola definición de aplicación respalda todos los sucesos de administración de credenciales de usuario asociados a una sola aplicación, incluidos los siguientes:

- Autenticación del usuario.
- Cambio de las credenciales del usuario.
- Confirmación de los cambios de credenciales.

Las definiciones de aplicación se clasifican en tres tipos principales que determinan la información recopilada:

- Aplicaciones de Windows (incluidas las aplicaciones Java y SAP Logon Pad)
- Aplicaciones Web (incluidos los applets Java)
- Aplicaciones de emulador de terminal compatible con HLLAPI

Una definición de aplicación consta de:

- Características de la aplicación que se aplican a todos los formularios incluidos en la definición. Se definen mediante el asistente de definición de aplicaciones.
- Datos específicos de formulario que se emplean para reconocer cada suceso de administración de credenciales distinto asociado a la aplicación. Definición de estos formularios y sucesos mediante el Asistente de definición de formularios. Este asistente se ejecuta durante la operación del Asistente de definición de aplicaciones.

Las características de la aplicación para todos los tipos de aplicaciones contienen información de configuración similar. No obstante, los datos específicos de formulario que se incluyen en la definición de la aplicación varían considerablemente según el tipo de aplicación que se esté definiendo.

Para crear una definición de aplicación, se debe poder acceder a ella desde el equipo donde se crea la definición de la aplicación. Dado que algunas firmas de aplicación pueden variar según el sistema operativo subyacente, es necesario probar las definiciones de aplicación en el software de todos los sistemas operativos de su organización.

Cualquier cambio o actualización en una aplicación después instalar una definición de aplicación se debe probar para garantizar que no existan cambios en las firmas de aplicación que requieran un cambio en la definición de aplicación.

Importante: Como medida de seguridad, en su estado predeterminado, Windows Server 2008, Windows Server 2008 R2, Windows Vista y Windows 7 se ejecutan con el aislamiento de privilegios de la interfaz de usuario (UIPI) habilitado. Este aislamiento impide que las aplicaciones envíen mensajes a otras aplicaciones con un nivel de integridad mayor. El resultado es que Single Sign-on Plug-in, que de forma predeterminada opera con el nivel de integridad medio, no detecta ni envía las credenciales a las aplicaciones que se ejecutan con un nivel de integridad mayor. Para mantener el nivel de seguridad esperado de estos sistemas operativos y de Single Sign-on, continúe usando los valores predeterminados.

Vista general del asistente de definición de aplicaciones y formularios

Oct 12, 2015

Todas las definiciones de aplicación se crean inicialmente mediante el Asistente de definición de aplicaciones y el Asistente de definición de formularios integrado.

El Asistente de definición de formularios define las características asociadas con todos los formularios de administración de credenciales de usuario que se incluyen en la definición de aplicación.

Introducción al Asistente de definición de aplicaciones

Para iniciar el Asistente de definición de aplicaciones, seleccione el nodo Definiciones de aplicación en AppCenter y, a continuación, en el menú Acción, seleccione Crear una definición de aplicación.

El asistente recopila información para cada tipo de aplicación (Windows, Web y basadas en emuladores de terminal).

Datos recopilados	Windows	Web	Emuladores de terminal
Identificar la aplicación	X	X	X
Administrar formularios	X	X	X
Dar nombres a los campos personalizados	X	X	X
Especificar el icono	X		
Configurar la detección avanzada	X	X	X
Configurar la caducidad de contraseñas	X	X	X
Confirmar los parámetros	X	X	X

Administración de formularios mediante el Asistente de definición de aplicaciones

La mayoría de las aplicaciones disponen de formularios independientes para el inicio de sesión y cambios de contraseña. Algunas aplicaciones también tienen formularios independientes que notifican a los usuarios cuando cambian su contraseña de forma satisfactoria.

Para agregar formularios a la definición de aplicación, utilice la página Administrar formularios. En esta página, también puede editar o eliminar formularios.

Si selecciona Agregar formulario, se inicia el Asistente de definición de formularios que se emplea para recopilar los datos para un solo formulario. Utilice el asistente para cada formulario de la definición de aplicación.

Asignación de nombre a los campos personalizados

Single Sign-on incluye los campos de nombre de usuario y contraseña al igual que cualquier formulario de inicio de sesión. Algunas aplicaciones precisan información adicional, como un nombre de base de datos, un nombre de dominio o un nombre de sistema, para autenticar al usuario.

Con el Asistente de definición de formularios, se pueden agregar dos campos personalizados como máximo. Si agrega campos, cuando regrese al asistente de definición de aplicaciones, utilice la página Dar nombres a los campos personalizados para asignar nombres a tales campos.

Para crear una tecla de acceso rápido para el nombre de campo personalizado, coloque el signo & en el nombre de campo inmediatamente delante de la letra que desee especificar como la tecla de acceso rápido. Si no se identifica ninguna tecla de este tipo, Single Sign-on Plug-in anexa automáticamente un valor numérico como la tecla de acceso rápido para el control. Aparecerá en el botón como (1) o (2), según el número de campos personalizados que se haya definido.

Especificación de un icono para aplicaciones de Windows

De forma predeterminada, Single Sign-on utiliza un icono diferente para representar las aplicaciones de Windows, Web y de emuladores de terminal en la ventana Administrar contraseñas (anteriormente conocida como Administrador de inicios de sesión). No obstante, mediante la página Especificar el icono, se puede definir un icono personalizado para las aplicaciones de Windows para que les resulte más sencillo a los usuarios identificar aplicaciones específicas. Si selecciona la opción de icono personalizado, guarde el archivo de icono en la misma ubicación que la aplicación.

Cómo impedir bucles de credenciales

Las opciones de la página Configurar la detección avanzada se usan para evitar en lo posible los bucles de envío y cambio de credenciales.

A veces, es posible que los usuarios se encuentren en un sitio Web con un bucle de envío de credenciales. En estos casos, los usuarios cierran la sesión de una aplicación y vuelven a la pantalla de inicio de sesión. Single Sign-on Plug-in detecta la pantalla de inicio de sesión y envía las credenciales de los usuarios para volver a iniciar la sesión automáticamente. Para evitar el envío automático de credenciales, se debe activar la opción Procesar sólo el primer inicio de sesión de esta aplicación.

Cuando se inicia una aplicación predefinida por primera vez y esta opción está seleccionada, Single Sign-on Plug-in envía las credenciales en la instancia inicial del formulario de inicio de sesión sin que sea necesaria la intervención del usuario. Cuando los usuarios cierran la sesión y se vuelve a presentar la pantalla de inicio de sesión, aparece una ventana y permanece visible durante 10 segundos aproximadamente. Los usuarios disponen de tres opciones:

- Cerrar la ventana: no se envía ninguna credencial
- Ignorar la ventana: no se envía ninguna credencial
- Hacer clic en el vínculo: se envían las credenciales

Si se cierra la ventana, la aplicación finaliza la sesión y Single Sign-on envía las credenciales la próxima vez que se abre la aplicación.

Para evitar un bucle de cambio de credenciales, active la opción Procesar sólo el primer cambio de contraseña de esta aplicación. De este modo, cuando los usuarios intenten cambiar su contraseña varias veces mientras acceden a una

determinada aplicación, se les solicitará que verifiquen los cambios de contraseña posteriores.

Configurar la caducidad de contraseñas

La página Configurar la caducidad de contraseñas incluye opciones para:

- Identificar un script que se ejecutará cuando caduque la contraseña
- Usar la advertencia de caducidad de Single Sign-on.

Tanto usted como otra persona de la empresa puede crear un script para indicarles a los usuarios que deben cambiar las contraseñas de determinadas aplicaciones (o de todas ellas) de manera periódica o de manera automática, o bien, una combinación de estos procedimientos para cumplir con las necesidades normativas y de seguridad de la empresa. Para ejecutar este tipo de script cuando caduca la contraseña asociada a esta definición de aplicación (según se define en la directiva de contraseñas), active la opción de ejecución de script e indique la ruta absoluta del script. La ruta del script debe estar a disposición de todos los usuarios. No utilice una ruta UNC (Convención de nomenclatura universal).

Normalmente, el script invoca una aplicación asociada mediante una interfaz de línea de comandos con un parámetro de cambio de contraseña.

También puede activar la opción Usar la advertencia de caducidad de Single Sign-on. Al activar esta opción, se mostrará una advertencia de caducidad de contraseña de Single Sign-on cuando la directiva de contraseña asociada a esta aplicación indique que la contraseña ha caducado. Esta acción muestra en un mensaje que aparece continuamente que el período de tiempo asociado ha caducado, pero no obliga a una acción de cambio de contraseña.

Introducción al asistente de definición de formularios

Utilice el Asistente de definición de formularios para:

- Definir un formulario mediante el Asistente de definición de aplicaciones.
- Editar un formulario existente.
- Agregar un formulario a una definición de aplicación existente.

Utilice el Asistente de definición de formularios para definir los formularios estándar de administración de credenciales para usuarios:

- Formulario de inicio de sesión
  Identifica la interfaz de inicio de sesión para una aplicación y administra las acciones necesarias para obtener acceso a la aplicación asociada.

- Formulario de cambio de contraseñas
  Identifica la interfaz de cambio de contraseña para una aplicación y administra las acciones necesarias para cambiar la contraseña de usuario de la aplicación asociada.

- Formulario de cambio de contraseñas satisfactorio
  Identifica la interfaz de cambio de contraseña para una aplicación y administra las acciones necesarias para reconocer el cambio de contraseña satisfactorio para la contraseña de usuario de la aplicación asociada.

- Formulario de cambio de contraseñas fallido
  Identifica la interfaz de cambio de contraseña incorrecto de una aplicación y define las acciones que se deben llevar a cabo cuando una operación de cambio de credenciales no se realiza correctamente.

El Agente de Password Manager de las versiones 4.0 y 4.1 no respalda los formularios de cambio de contraseña

satisfactorio o fallido y no responde a las definiciones de aplicación que contienen dichos formularios.

Los datos recopilados por cada formulario tienen dos funciones:

- Identifica de forma exclusiva cuándo se inicia un formulario específico de la aplicación.
- Lleva a cabo las acciones de procesamiento de credenciales de usuario que están asociadas al formulario.

El Asistente de definición de formularios se inicia desde la página Administrar formularios del Asistente de definición de aplicaciones seleccionando la opción Agregar formulario.

En la siguiente tabla se muestra la información de formulario que se recopila para cada tipo de aplicación (Windows, Web y emuladores de terminal) mediante el asistente de definición de formularios.

Datos recopilados	**Windows**	**Web**	**Emuladores de terminal**
Nombrar formulario	X	X	X
Identificar el formulario	X	X	X
Definir las acciones del formulario	X	X	
Configurar las reglas de detección de campos			X
Configurar otros parámetros	X	X	X
Confirmar los parámetros	X	X	X

Definiciones de aplicación de tipo Windows

Oct 12, 2015

Use las definiciones de aplicación de tipo Windows se utilizan para identificar las aplicaciones de Windows, las aplicaciones Java y las aplicaciones que se inician desde SAP Logon Pad.

Para crear una definición de aplicación, categorice cualquier aplicación iniciada por un archivo con extensión ejecutable (.exe) como una aplicación de Windows.

Para recopilar información necesaria para las definiciones de aplicación de Windows, inicie la aplicación y vaya al formulario que precisa un suceso de administración de credenciales de usuario (inicio de sesión, cambio de contraseña, cambio de contraseña satisfactorio o cambio de contraseña fallido), mientras el Asistente de definición de formularios se ejecuta desde la consola o desde la Herramienta de definición de aplicaciones. El asistente proporciona instrucciones para encontrar e identificar los componentes correspondientes de la aplicación.

Identificación de formularios

Al crear definiciones de aplicación para las aplicaciones de tipo Windows, utilice la página Identificar el formulario para brindar la información necesaria para que Single Sign-on Plug-in reconozca de forma exclusiva el formulario que se está definiendo.

La información de identificación incluye el título de la ventana y el nombre del archivo ejecutable. Cuando Single Sign-on Plug-in detecta el nombre del archivo ejecutable, supervisa la aplicación para encontrar los títulos de ventana definidos.

Cuando se detecta un título de ventana, Single Sign-on Plug-in realiza las acciones definidas para el formulario.

Para identificar un formulario

1. Si aún no lo ha hecho, inicie el programa de Windows y vaya al formulario de inicio de sesión, cambio de contraseña, cambio de contraseña satisfactorio o cambio de contraseña fallido.
2. En la página Identificar el formulario del Asistente definición de formularios, haga clic en Seleccionar.
3. Si el programa deseado no se muestra resaltado, utilice el Selector de ventanas para seleccionar otro de los programas disponibles.

Identificación de títulos de ventanas dinámicos

En la página Identificar el formulario, se pueden editar los títulos de Títulos de ventanas de este formulario para gestionar datos de títulos de ventana dinámicos, como una fecha o un identificador de sesión. Para ello, sustituya los siguientes caracteres comodín de los datos dinámicos que aparecen en el título de ventana:

Carácter comodín	**Descripción**
?	Representa un solo carácter variable o dinámico que aparece en un título de ventana.
*	Representa uno o varios caracteres que aparecen en datos de título dinámicos. No se recomienda utilizarlo para títulos de ventana vacíos. (en esos casos, debe utilizarse NULL).

Carácter comodín	Descripción
NULL	Representa títulos de Windows vacíos (la palabra “NULL” debe estar en mayúsculas).

Identificación de rutas seguras

El área Nombres de archivos ejecutables muestra el nombre del archivo ejecutable y la información de la ruta segura.

Las rutas seguras limitan el reconocimiento de la aplicación sólo a las instancias de programa iniciadas desde las rutas definidas aquí. Si se identifican una o varias rutas seguras, Single Sign-on Plug-in envía las credenciales únicamente cuando el programa identificado se ejecuta desde la ruta definida y todos los demás identificadores de formulario definidos están presentes.

Puede especificar una ruta segura haciendo clic en la opción Usar la ruta completa del ejecutable del Selector de ventanas.

Si no se define información de ruta, se muestra No se ingresó y Single Sign-On Plug-in proporciona información de credenciales a cualquier programa que coincida con los otros identificadores de formulario.

Separe varias rutas con puntos y comas. Para identificar la ruta, se pueden utilizar rutas absolutas o variables de entorno.

Nota: Las definiciones de aplicación que incluyen información de ruta segura pueden utilizarse para crear una plantilla de definición de aplicación; no obstante, la ruta segura no se incluye como parte de la plantilla.

Definición de acciones del formulario

La página Definir las acciones del formulario se utiliza para definir las acciones que debe realizar Single Sign-on Plug-in para enviar las credenciales para el formulario específico que se está definiendo.

La parte superior de la página muestra la selección de las credenciales de usuario asociadas al formulario específico:

	Formulario de inicio de sesión	Formulario de cambio de contraseñas	Formulario de cambio de contraseñas satisfactorio	Formulario de cambio de contraseñas fallido
Nombre de usuario/ID	X	X	X	X
Contraseña	X		X	X
Contraseña anterior		X		
Contraseña nueva		X		
Confirmar contraseña		X		
Campo personalizado 1	X		X	X
Campo personalizado	X		X	X

2 Aceptar	**Formulario de inicio de sesión** X	**Formulario de cambio de contraseñas** X	**Formulario de cambio de contraseñas satisfactorio** X	**Formulario de cambio de contraseñas fallido** X

La parte inferior de la página muestra la secuencia de acciones definida.

El objetivo de esta página es definir las acciones que realizará Single Sign-on Plug-in para enviar correctamente las credenciales de usuario necesarias al formulario identificado.

Para definir acciones del formulario

Para la mayoría de las aplicaciones de Windows, sólo basta con seguir el siguiente procedimiento:

1. Haga clic en el hipervínculo Configurar/Cambiar asociado a una credencial de usuario específica. Esta acción abre el cuadro de diálogo Configurar el texto del control que se utiliza para identificar el control que recibirá la credencial seleccionada.
2. Se debe seleccionar el candidato de tipo de control para recibir la credencial. A medida que se seleccionan los distintos candidatos, el tipo de control asociado aparece resaltado visiblemente en la aplicación para facilitar el tipo de control que recibirá la credencial de usuario o botón de envío que se ha identificado.
3. Esta acción se debe repetir para todas las credenciales que necesita el formulario y para el botón requerido para enviar el formulario.
   Algunos formularios requieren dominios u otras credenciales configurables por el usuario que se deben enviar correctamente para procesar el formulario. Para respaldar estos requisitos, hay disponibles dos campos personalizados. Asigne las credenciales de requisitos especiales a estos campos. Los nombres asociados a estos campos se definen en la página Dar nombres a los campos personalizados del Asistente de definición de aplicaciones.

   Nota: No es necesario configurar todas las credenciales identificadas en la parte superior de la página Definir las acciones del formulario.

Identificador de ventana

La página Identificador de ventana se utiliza para definir un ID de control de Windows que identifique un formulario de manera exclusiva cuando se puedan identificar varias ventanas únicamente mediante el título de Windows definido y el nombre del archivo ejecutable. Sólo resulta útil si el ID de control de Windows se puede usar para diferenciar entre los diferentes formularios que se pueden identificar.

Seleccione la casilla de verificación Habilitar la coincidencia con ID de control de ventana y proporcione el ID de control que diferencia de manera exclusiva la ventana del formulario que se está definiendo de todos los demás formularios posibles.

Extensiones de identificación

Las extensiones de identificación forman parte de las extensiones de definición de aplicación. Estas extensiones proporcionan compatibilidad para utilizar aplicaciones que son externas al software del plug-in para reconocer la aparición de un suceso de administración de credenciales de usuario y realizar el proceso de envío de credenciales.

Aunque los administradores de Single Sign-on generalmente pueden crear definiciones de aplicación mediante el componente de la consola de Single Sign-on y la Herramienta de definición de aplicaciones, algunas aplicaciones tienen consideraciones o requisitos especiales que requieren un medio alternativo para detectar la aplicación y enviar las credenciales de usuario o realizar otras acciones similares.

Para respaldar estas aplicaciones, los administradores de Single Sign-on pueden utilizar las extensiones de definición de aplicación con el fin de ofrecer una abstracción para los controles de aplicación y los mecanismos de entrada de datos asociados.

Las extensiones de identificación están desarrolladas por otros implementadores y la implementación es específica de la aplicación. Por lo tanto, los procedimientos necesarios para configurar su uso son específicos de la aplicación.

Por lo general, los administradores de Single Sign-on no participan en el desarrollo de estas extensiones. Las extensiones las crean otros implementadores. Como la configuración de estas extensiones es específica de cada extensión, es muy probable que las instrucciones para configurar la extensión estén incluidas con ella.

Definición de secuencias de acciones para formularios de Windows a través del Editor de acciones

La página Definir las acciones del formulario se utiliza para definir las acciones que debe realizar el software del plug-in para enviar las credenciales del formulario de administración de credenciales de un usuario específico que se está definiendo.

Para muchas aplicaciones de Windows, la información básica recopilada en el Asistente de definición de formularios es suficiente para definir el formulario. No obstante, algunos formularios requieren más información, pasos, teclas especiales u otras acciones para realizar correctamente una tarea de administración de credenciales de usuario. En el caso de estos formularios, en la página Definir las acciones del formulario, haga clic en Editor de acciones para abrir el cuadro de diálogo Editor de acciones.

El cuadro de diálogo Editor de acciones consta de:

- Seleccionar acciones
  Muestra todas las acciones posibles de secuencia de acciones.
- Configurar acciones
  Se utiliza para definir las opciones específicas de acción que se incluirán en la secuencia de acciones.
- Secuencia de acciones
  Muestra la secuencia de acciones definidas que se realizarán para procesar el formulario específico de administración de credenciales de usuario.

Al final del cuadro de diálogo Editor de acciones está el botón Configuración avanzada que se utiliza para acceder al cuadro de diálogo Configuración avanzada. El cuadro de diálogo Configuración avanzada tiene dos controles:

- Números de control ordinales
  Seleccione esta casilla de verificación para utilizar números de control ordinales (normalmente se denomina orden Z) en vez de números de ID de control. Los números de control ordinales se enumeran de forma independiente durante el proceso de definición (por el software del plug-in) con el fin de identificar los controles independientemente de los números de ID de control definidos por la aplicación.

  Es recomendable que se seleccione esta función al definir aplicaciones .NET que generan números de ID de control dinámicamente o aplicaciones con números de ID de control duplicados.
- Demora inicial
  Seleccione esta opción y defina el período de tiempo que el software del plug-in demora el procesamiento antes de comenzar la secuencia de acciones. También puede configurarse una demora iniciando la secuencia de acciones con una demora, usando la acción Insertar demora.

A diferencia del uso de la opción Insertar demora, a la cual se accede desde el área Seleccionar acciones del cuadro de diálogo Editor de acciones, que se define como una operación de envío de tecla, cualquier demora inicial definida aquí se puede utilizar para evitar la creación de una definición de aplicación que sólo se admita en las versiones 4.5, 4.6, 4.6 con Service Pack 1, 4.8 y 5.0 del Single Sign-on Plug-in.

Para definir una secuencia de acciones

1. Seleccione una acción de las distintas opciones que figuran en Seleccionar acciones.
2. Configure la acción mediante las opciones Configurar acciones. Cuando esté satisfecho con los parámetros de configuración, haga clic en Insertar. La acción configurada se muestra en Secuencia de acciones.
3. Repita los pasos 1 y 2 para todas las acciones que requiera el formulario de credenciales de usuario.
4. Seleccione las acciones en Secuencia de acciones y haga clic en Subir o Bajar para organizar las acciones en la secuencia de ejecución correcta que requiere el formulario de administración de credenciales de usuario que se está definiendo.
5. Cuando la secuencia de acciones sea correcta y esté completa, haga clic en Aceptar. Con esta acción se vuelve a la página Definir las acciones del formulario con la secuencia de acciones mostrada en el área Secuencia de acciones.
6. Haga clic en Siguiente para continuar con el proceso de definición de formularios en la página Configurar otros parámetros. Si alguna combinación de acciones de formulario limita la secuencia definida al plug-in/agente de Password Manager 4.5, Password Manager 4.6, Password Manager 4.6 con Service Pack 1, Single Sign-On 4.8 y Single Sign-on 5.0 solamente, aparecerá un mensaje para continuar o volver a cambiar la configuración.

Consideraciones para las definiciones de tipo Windows

Al crear definiciones de aplicación de tipo Windows, se debe tener en cuenta lo siguiente:

- Las plantillas de aplicación facilitan la creación de definiciones de aplicación.
- Las definiciones de aplicación se deben probar con el software del plug-in antes de ponerlas a disposición de los usuarios.
- La mayoría de las definiciones de aplicación funcionan utilizando sólo la información básica. Si una definición de aplicación no funciona del modo previsto en el entorno de prueba, puede deberse a la existencia de características exclusivas, como un título de ventana dinámico, ID de control dinámicos u otros identificadores o acciones especiales que se han programado en la aplicación.
- Para exportar definiciones de aplicación desde un entorno de prueba a uno de producción, se utiliza la tarea Exportar datos de administración del componente Single Sign-on de Citrix AppCenter.
- Los parámetros que se seleccionan en el nivel de definición de aplicación se aplican a todos los formularios en la definición de aplicación.
- Algunos parámetros que se seleccionan en el nivel de la definición de aplicación se pueden anular en el nivel del formulario. Por ejemplo, en una aplicación con tres formularios definidos, puede activarse la función de envío automático en el nivel de la aplicación. Cada vez que el software del plug-in se encuentre con uno de estos tres formularios para la aplicación, se proporcionarán y enviarán automáticamente las credenciales de usuario. No obstante, el envío automático se puede desactivar para uno de los formularios en el nivel del formulario y el software del plug-in no enviará automáticamente las credenciales para ese formulario en concreto; en este caso, el usuario tiene que hacer clic en Enviar o Aceptar del formulario seleccionado.
- Para crear una tecla de acceso rápido para el nombre de campo personalizado, coloque el signo & en el nombre de campo inmediatamente delante de la letra que desee especificar como la tecla de acceso rápido.
  Si no se identifica ninguna tecla de este tipo, el software del plug-in anexa automáticamente un valor numérico como la tecla de acceso rápido para el control. Aparecerá en el botón como (1) o (2), según el número de campos personalizados que se haya definido.

  Se debe probar el formulario resultante para garantizar que el nombre definido no supera la cantidad de espacio asignado al nombre de campo personalizado.

Configuración de Redirigir a la aplicación Windows

Cuando no se reconoce ningún formulario para la aplicación Web en el Asistente de formularios Web, la definición de formulario se debe redirigir para utilizar una definición de formulario creada para una aplicación de Windows.

Es posible que no se reconozcan los formularios cuando la aplicación Web utiliza controles ActiveX, controles basados en Flash, algunos tipos de controles Ajax u otros controles no basados en HTML que se utilizan para administrar los sucesos de administración de credenciales de usuario.

En estos casos, asegúrese de que la casilla de verificación Redirigir a la aplicación Windows se ha seleccionado en la página Nombrar formulario. Haga clic en Siguiente para avanzar por cada una de las páginas restantes del Asistente de definición de formularios y haga clic en Finalizar en la página Confirmar los parámetros.

Las características de reconocimiento de formulario y las acciones de credenciales ahora se deben definir mediante definiciones de tipo Windows y acciones de envío de tecla.

Uso de la coincidencia avanzada para identificar formularios de Windows

Oct 12, 2015

La página Identificar el formulario del Asistente de definición de formularios brinda las coincidencias de identificación de formularios suficientes para la mayoría de las aplicaciones de Windows. No obstante, algunos formularios de administración de credenciales de usuario requieren identificadores adicionales. Para estos formularios, Single Sign-on ofrece Coincidencia avanzada. Puede acceder a esta característica desde la página Identificar el formulario del Asistente de definición de formularios al hacer clic en Coincidencia avanzada.

La Coincidencia avanzada ofrece cinco identificadores avanzados para las aplicaciones de Windows:

- Información de la clase
- Coincidencia de controles
- Información de la sesión SAP
- Identificador de ventana
- Extensiones de identificación

Omisión de formularios mediante Información de la clase

Si utiliza la página Información de la clase, puede identificar los formularios que desea que Single Sign-on ignore. Si escribe una clase de ventana en el campo Ignorar esta clase de ventana, Single Sign-on Plug-in no reacciona cuando aparece un formulario con esa información de clase.

Este tipo de coincidencia no se debe utilizar para aplicaciones .NET o aplicaciones que utilizan la clase de ventana 32770 (la clase predeterminada).

Este parámetro resulta útil cuando la clase de ventana es dinámica. En este caso, se utilizan caracteres comodín para realizar una coincidencia con un identificador de clase de ventana dinámica.

Carácter comodín	**Descripción**
?	Representa un solo carácter variable o dinámico.
*	Use este valor para representar datos de identificador dinámicos para uno o varios caracteres. No se recomienda utilizarlo para identificadores de clase de ventana vacíos. (en esos casos, debe utilizarse NULL).
NULL	Use este valor para identificadores de clase de ventana vacíos (la palabra “NULL” debe estar en mayúsculas).

Utilice identificadores de clase de ventana al intentar identificar una clase de ventana entre muchos destinos de clase de ventana posibles. Se aplican las siguientes condiciones:

- El título de ventana asociado y el archivo ejecutable asociado dan lugar a varios candidatos de coincidencia. Esta condición se produce con más frecuencia cuando el título de la ventana contiene datos dinámicos y se especifican caracteres comodín.

- El formulario de destino debe estar asociado a un identificador de clase de ventana único y todos los demás candidatos deben utilizar diferentes identificadores de clase de ventana.

Para identificar la información de clase

Inicie este procedimiento en la página Identificar el formulario del Asistente de definición de formularios.

1. Haga clic en Coincidencia avanzada y, a continuación, seleccione la opción Información de la clase.
2. Haga clic en Seleccionar para elegir la aplicación de destino de entre las aplicaciones que están abiertas actualmente en el equipo.
   Nota: Para ampliar las opciones, seleccione las casillas de verificación Mostrar las ventanas de programa ocultas o Mostrar ventanas secundarias.

Definición de criterios de coincidencia con Coincidencia de controles cuando los identificadores asociados son idénticos

Algunas aplicaciones asignan información dinámica a las etiquetas de los controles. En estos casos, el título de la ventana, su aplicación ejecutable asociada y el ID de control (o los ID) pueden ser los mismos para diferentes formularios de administración de credenciales de usuario, mientras que las etiquetas de texto u otras propiedades del formulario cambian como respuesta a sucesos específicos de la aplicación.

Para estos tipos de formularios, se utilizan las opciones de configuración de coincidencia de controles para identificar un formulario para una acción de plug-in específica según los valores de clase, estilo o texto exclusivos asociados al ID de control (o varios ID de control si se precisan definiciones múltiples para identificar el formulario de manera exclusiva).

Para definir el criterio de coincidencia

Inicie este procedimiento en la página Identificar el formulario del Asistente de definición de formularios.

1. Haga clic en Coincidencia avanzada y, a continuación, seleccione la opción Coincidencia de controles.
2. Haga clic en Agregar coincidencia.
   Nota: Defina solo los criterios de coincidencia de controles que sean suficientes para identificar de manera exclusiva el formulario de administración de credenciales de usuario que se está definiendo.
3. En el cuadro de diálogo Definir el criterio de coincidencia, haga clic en Seleccionar.
4. Haga clic con el botón secundario en una entrada de ID de control.
5. Elija Clase, Estilo o Texto para elegir las características que se usarán para calificar el formulario del ID de control seleccionado.
6. Repita los pasos 4 y 5 para cada ID de control que se utilizará para identificar el formulario de manera exclusiva.

Identificación de coincidencias al utilizar varias sesiones SAP

Las versiones anteriores de SAP se administran mediante las definiciones de aplicación de Windows y Web. No obstante, el cuadro de diálogo Coincidencia avanzada ofrece compatibilidad para las aplicaciones SAP cuando varios sistemas SAP están definidos para utilizar una misma interfaz de inicio de sesión de interfaz gráfica de usuario de SAP (como SAP Logon Pad).

La compatibilidad de Información de la sesión SAP requiere que el administrador SAP habilite el uso de scripts de GUI en el servidor. De este modo se permite que la consola y Single Sign-on Plug-in consulten SAP Logon Pad para determinar el ID de sistema o el Nombre de servidor (o ambos) necesarios para identificar de manera exclusiva el formulario específico de administración de credenciales de usuario.

Al utilizar la opción Información de la sesión SAP, la información de sesión se puede extraer de una ventana de SAP para identificar de manera exclusiva y diferenciar una ventana de inicio de sesión SAP de otra.

Para definir manualmente la información de la sesión SAP

Los valores de los campos ID del sistema SAP y Nombre del servidor se pueden modificar manualmente. Ambos campos aceptan expresiones regulares para sus respectivos valores. Esto resulta útil para controlar la capacidad de coincidencia de varios servidores.

También puede introducir manualmente los valores para que coincidan los nombres DNS y NetBIOS de un servidor.

El siguiente formato de expresión regular se utiliza para respaldar ambos DNS y NetBIOS.

^nombreservidor(\.dominio\.com)?$

Para generar un mensaje de scripting de la GUI de SAP

Los mensajes de scripting de GUI de SAP se pueden generar siempre que un programa intenta establecer una conexión con SAP Logon Pad mediante la GUI de SAP. En este caso, se puede cambiar un parámetro del Registro para impedir el mensaje.

La clave es HKEY_CURRENT_USER\Software\SAP\SAPGUI Front\SAP Frontend Server\Security\WarnOnAttach. Se trata de un valor DWORD. Si este valor de clave se establece en 0, no se muestra ningún mensaje. El valor predeterminado es 1.

Definiciones de aplicación de tipo Web

Oct 12, 2015

Las definiciones de aplicación de tipo Web se utilizan para identificar las aplicaciones basadas en Web, incluidos los applets Java.

Normalmente, cualquier aplicación que se ejecuta en un explorador se clasifica como una aplicación Web en lo que respecta a la creación de una definición de aplicación. Single Sign-on es compatible con aplicaciones Web que se ejecutan en las versiones 6.0, 7.0, 8.0 y 9.0 de Internet Explorer.

Las definiciones de aplicación Web se crean, en parte, mediante la identificación de componentes de la aplicación Web a medida que ésta se ejecuta. Para recopilar información necesaria para las definiciones de aplicación Web, inicie la aplicación y vaya al formulario que precisa un suceso de administración de credenciales de usuario (inicio de sesión, cambio de contraseña, cambio de contraseña satisfactorio o cambio de contraseña fallido), mientras el Asistente de definición de formularios se ejecuta desde la consola o desde la Herramienta de definición de aplicaciones. El texto en pantalla del asistente proporciona instrucciones para encontrar e identificar los componentes correspondientes de la aplicación.

Nombrar formulario

Al crear definiciones para las aplicaciones de tipo Web, la página Nombrar formulario del Asistente de definición de formularios se utiliza para:

- Asignar un nombre definido por el usuario para el formulario que se está creando
- Identificar el tipo de formulario que se está creando
- Identificar cualquier acción especial

Hay que tener en cuenta que el nombre asignado al formulario se muestra en la página Administrar formularios del Asistente de definición de aplicaciones. Se debe asignar un nombre significativo para el tipo de formulario que se está creando.

Se pueden definir varios tipos de formularios de procesamiento de credenciales de usuario mediante el Asistente de definición de formularios:

- Formulario de inicio de sesión
  Se utiliza para identificar la interfaz de inicio de sesión de una aplicación y para administrar las acciones de credenciales de usuario necesarias para obtener acceso a la aplicación asociada.

- Formulario de cambio de contraseñas
  Se utiliza para identificar la interfaz de cambio de contraseña de una aplicación y para administrar las acciones de credenciales de usuario necesarias para cambiar la contraseña de usuario para la aplicación asociada.

- Formulario de cambio de contraseñas satisfactorio
  Se utiliza para identificar la interfaz de cambio de contraseña de una aplicación y para administrar las acciones de credenciales de usuario necesarias para reconocer el cambio de la contraseña para la aplicación asociada.

- Formulario de cambio de contraseñas fallido
  Se utiliza para identificar la interfaz de cambio de contraseña incorrecto de una aplicación y para definir las acciones que se deben llevar a cabo cuando una operación de cambio de credenciales no se realiza correctamente.

El Agente de Password Manager de las versiones 4.0 y 4.1 no respalda los formularios de cambio de contraseña satisfactorio o fallido y no responde a las definiciones de aplicación que contienen dichos formularios.

El área Acciones especiales se utiliza para identificar los tratamientos de formulario especiales para el formulario que está definiendo:

- Sin acciones especiales
  Esta opción se selecciona para el procesamiento normal de formularios Web.
- Redirigir a la aplicación Windows
  Esta opción se selecciona cuando no se reconoce ningún formulario para la aplicación Web del Asistente de formularios Web. Esto sucede cuando la aplicación Web utiliza controles ActiveX, controles basados en Flash, algunos tipos de controles Ajax u otros controles no basados en HTML que se utilizan para administrar los sucesos de administración de credenciales de usuario.
- Ignorar este formulario cuando sea detectado por Single Sign-on Plug-in
  Esta opción se selecciona para que el software del plug-in ignore el formulario.

Identificar el formulario

Al crear definiciones de aplicación para las aplicaciones de tipo Web, la página Identificar el formulario se utiliza para proporcionar la información necesaria para que el software de Single Sign-on Plug-in reconozca de forma exclusiva el formulario que se está definiendo.

Las aplicaciones Web se identifican mediante la dirección URL asociada al formulario de administración de credenciales de usuario que se está definiendo.

Haga clic en Seleccionar para abrir el selector de página Web. Utilice este selector para identificar la página Web que desea asociar con el formulario.

Después de completar el selector de página Web, se volverá a esta página. Hay disponibles dos casillas de verificación para administrar el modo en que se interpretan las URL identificadas:

- Coincidencia estricta de URL
  Esta casilla de verificación se selecciona para reconocer únicamente los sucesos de administración de credenciales de usuario de las aplicaciones Web que se inician mediante las URL especificadas. Algunas URL pueden contener datos dinámicos como identificadores de administración de sesión, parámetros de aplicación u otros identificadores que pueden cambiar por cada instancia. En estas circunstancias, el uso de coincidencia estricta puede provocar que no se reconozca la URL.
- Reconocer mayúsculas en URL
  Esta casilla de verificación se selecciona para utilizar URL con coincidencia exacta de mayúsculas y minúsculas.

Definir las acciones del formulario

La página Definir las acciones del formulario se utiliza para definir las acciones que debe realizar Single Sign-on Plug-in para enviar las credenciales para el formulario específico que se está definiendo.

La parte superior de la página muestra la selección de las credenciales de usuario asociadas al formulario específico:

	Formulario de inicio de sesión	**Formulario de cambio de contraseñas**	**Formulario de cambio de contraseñas satisfactorio**	**Formulario de cambio de contraseñas fallido**

	Formulario de inicio de sesión	Formulario de cambio de contraseñas	Formulario de cambio de contraseñas satisfactorio	Formulario de cambio de contraseñas fallido
Nombre de usuario/ID Contraseña	X X	X	X	X
Contraseña anterior		X		
Contraseña nueva		X		
Confirmar contraseña		X		
Campo personalizado 1	X		X	X
Campo personalizado 2	X		X	X
Aceptar	X	X	X	X

La parte inferior de la página muestra la secuencia de acciones definida.

El objetivo de esta página es definir las acciones que realizará el software del plug-in para enviar correctamente las credenciales de usuario necesarias al formulario identificado.

Para muchas aplicaciones Web, el proceso siguiente es todo lo que se precisa:

1. Haga clic en el hipervínculo Configurar/Cambiar asociado a una credencial de usuario específica. Esta acción abre el cuadro de diálogo Configurar el texto del campo que se utiliza para identificar el campo que recibirá la credencial seleccionada. Si el formulario ya está abierto, este cuadro de diálogo muestra todos los candidatos posibles para el tipo de campo asociado a la credencial de usuario u opción de envío seleccionada.
   Si el formulario de credenciales de la aplicación no está abierto actualmente, inicie la aplicación y acceda al formulario de credenciales de usuario correcto. Después, seleccione Actualizar . Después de haber seleccionado el formulario de aplicación, a este cuadro de diálogo se incorporan los candidatos de tipo de control que son adecuados para la credencial de usuario seleccionada.

2. Seleccione el candidato de tipo de campo para recibir la credencial. A medida que se seleccionan los distintos candidatos, el tipo de campo asociado aparece resaltado visiblemente en la aplicación para facilitar la identificación del tipo de campo que recibirá la credencial de usuario o botón de envío que se ha identificado.
3. Esta acción se debe repetir para todas las credenciales que necesita el formulario y para el botón requerido para enviar el formulario.
   Algunos formularios requieren dominios u otras credenciales configurables por el usuario que se deben enviar correctamente para procesar el formulario. Para respaldar estos requisitos, hay disponibles dos campos personalizados. Asigne las credenciales de requisitos especiales a estos campos. Los nombres asociados a estos campos se definen en la

página Dar nombres a los campos personalizados del Asistente de definición de aplicaciones.

Nota: No es necesario configurar todas las credenciales identificadas en la parte superior de la página Definir las acciones del formulario.

Para numerosas aplicaciones Web, después de haber definido los campos del formulario que recibirán la credencial de usuario identificada y el botón que se tiene que seleccionar para enviar el formulario, ya se habrá terminado el proceso de definición de acciones del formulario y se podrá avanzar a la siguiente página del asistente.

No obstante, algunos formularios requieren más información, pasos, teclas especiales u otras acciones para realizar correctamente una tarea de administración de credenciales. En el caso de estos formularios, haga clic en Editor de acciones para abrir el cuadro de diálogo Editor de acciones.

Definición de secuencias de acciones para formularios Web a través del Editor de acciones

La página Definir las acciones del formulario se utiliza para definir las acciones que debe realizar el software del plug-in para enviar las credenciales del formulario de administración de credenciales de un usuario específico que se está definiendo.

Para muchas aplicaciones Web la información básica recopilada en el Asistente de definición de formularios es suficiente para definir el formulario. No obstante, algunos formularios requieren más información, pasos, teclas especiales u otras acciones para realizar correctamente una tarea de administración de credenciales de usuario. En el caso de estos formularios, en la página Definir las acciones del formulario, haga clic en Editor de acciones para abrir el cuadro de diálogo Editor de acciones.

El cuadro de diálogo Editor de acciones para Web consta de:

- Seleccionar acciones
  Muestra todas las acciones posibles de secuencia de acciones.
- Configurar acciones
  Se utiliza para definir las opciones específicas de acción que se incluirán en la secuencia de acciones.
- Secuencia de acciones
  Muestra la secuencia de acciones definidas que se realizarán para procesar el formulario específico de administración de credenciales de usuario.

Configurar otros parámetros

En el caso de las definiciones Web, la página Configurar otros parámetros se utiliza para especificar si el software del plug-in pulsa automáticamente el botón de envío de la página Web o si el usuario debe pulsar manualmente el botón.

Para que el formulario se envíe sin intervención del usuario, se debe seleccionar la casilla de verificación Enviar automáticamente este formulario.

Cuadro de diálogo Configuración avanzada para aplicaciones Web

Oct 12, 2015

Algunas aplicaciones Web utilizan URL dinámicas. Si se produce esta situación, se deben utilizar criterios adicionales de definición de formularios (denominados entradas de coincidencia de detección) para identificar de manera exclusiva un formulario de administración de credenciales de usuario.

Estas entradas de coincidencia de detección se definen mediante el cuadro de diálogo Detalles de la coincidencia y se muestran en el cuadro de diálogo Configuración avanzada. Para acceder al cuadro de diálogo Detalles de la coincidencia, haga clic en Coincidencia avanzada en la página Identificar el formulario para acceder al cuadro de diálogo Configuración avanzada y, a continuación, haga clic en Agregar.

Utilice las opciones y los controles del cuadro de diálogo Detalles de la coincidencia para definir los criterios que se utilizarán para identificar de manera exclusiva un formulario específico de administración de credenciales de usuario. Su funcionamiento se basa en la búsqueda de valores específicos en el contenido con etiquetas del formulario HTML presentado para administrar una acción específica de administración de credenciales de usuario. Sólo es necesario definir las condiciones de coincidencia suficientes para identificar de manera exclusiva el formulario de administración de credenciales de usuario que se está definiendo.

Escriba el elemento Web que desea que coincida en el cuadro Buscar. Si no se encuentra el elemento, expanda la sección Parámetros adicionales para identificar el elemento manualmente.

La sección Parámetros adicionales se divide del siguiente modo:

- Etiqueta
  Este campo se usa para buscar la etiqueta HTML identificada. Si se conoce la instancia específica de la etiqueta, se debe seleccionar la casilla de verificación Hacer coincidir instancia e identificar la instancia que se utilizará en el documento. Si no se identifica ninguna instancia específica, se evaluarán todas las instancias del documento. Sólo es necesario especificar la etiqueta, no el delimitador (por ejemplo, p en vez de

). Como norma, se debe seleccionar la etiqueta más próxima al contenido que se desea hacer coincidir.

  Nota: Dado que la opción Hacer coincidir instancia puede variar según el explorador, esta función sólo se debe utilizar cuando sea necesario y la configuración se debe probar bien.
- Tipo de valor
  Esta sección se utiliza para definir los criterios para la coincidencia. Se puede seleccionar uno de los siguientes criterios:

Criterio	Descripción
Texto	Puede ser cualquier texto que se encuentre en el código HTML.
HTML	Cualquier código específico que se encuentre en la etiqueta especificada.
Atributo	Cualquier atributo del código HTML (como un atributo name de una etiqueta form).

- Valor de coincidencia
  Este campo se utiliza para ingresar el valor de la coincidencia. La casilla de verificación Hacer coincidir todo el valor se selecciona para obligar la coincidencia estricta del valor (cualquier texto no especificado aquí que se encuentre en el elemento de etiqueta provocará que falle la coincidencia). Se deben incluir todos los delimitadores y comillas que se puedan encontrar.

  Nota: La casilla de verificación Hacer coincidir todo el valor sólo se debe seleccionar cuando haya varias instancias de criterios de coincidencia similares.
- Operador
  Esta sección se utiliza para definir la relación de esta entrada de coincidencia con otras definidas para este formulario. Las opciones son:

Opciones	Descripción
AND	Seleccione esta opción cuando esta entrada de coincidencia es una de las varias coincidencias que deben ser satisfactorias para identificar el formulario. Seleccionando esta opción, el resultado de coincidencia actual se compara con el siguiente resultado de coincidencia. Si ambos son verdaderos, la coincidencia se realiza de forma satisfactoria.
o	Seleccione esta opción cuando esta coincidencia por sí sola puede identificar correctamente el formulario. Seleccionando esta opción el resultado de coincidencia actual se compara con el siguiente resultado de coincidencia. Si ambos son verdaderos, la coincidencia se realiza de forma satisfactoria. Esta opción se utiliza para definiciones de coincidencia única.
NOT	Esta operación se selecciona para aplicar lógica negativa al operador. Este operador se utiliza para definir criterios de coincidencia que no deben aparecer en la página para que se realice correctamente.

Definiciones de aplicación del tipo de emulador de terminal

Oct 12, 2015

Las definiciones de aplicación del tipo de emulador de termina se usan para identificar aplicaciones de emuladores de terminal incluyendo mainframe, AS/400, OS/390 ó UNIX. Single Sign-on proporciona funciones de inicio de sesión único a las aplicaciones de emuladores de terminal que utilizan la Interfaz de programación de aplicaciones de lenguaje de alto nivel (HLLAPI) o que disponen de un lenguaje de scripts incorporado capaz de mostrar cuadros de diálogo.

Recopilación de la información necesaria para las definiciones de aplicación de emulador de terminal

Normalmente, la mejor forma (y la más simple) de recopilar información necesaria para las definiciones de aplicación de emuladores de terminal (HLLAPI) es iniciarla.

Las definiciones de aplicación basadas en emuladores de terminal se crean utilizando el Asistente de definición de formularios. El asistente se utiliza para identificar una o varias cadenas de texto que deben estar presentes (o no) en las pantallas de la aplicación de emuladores de terminal para un determinado formulario de administración de credenciales de usuario (inicio de sesión de usuario, cambio de contraseña, cambio de contraseñas satisfactorio o cambio de contraseñas fallido).

A medida que se desplaza por el formulario de administración de credenciales de usuario que se está definiendo, registre todas las acciones de usuario necesarias para acceder al formulario. Estas acciones se deben proporcionar en la definición de formulario para cada formulario mientras se ejecuta el Asistente de definición de formularios desde la consola o la Herramienta de definición de aplicaciones.

Después de identificar el formulario de administración de credenciales de usuario, se definen las coordenadas de los campos de entrada de datos utilizadas para enviar la información de credenciales de usuario adecuada. Se definen mediante la especificación de la secuencia de acciones o pulsaciones de teclado necesarias para desplazarse por los campos o pantallas e introducir el texto.

Proceso de definición de formularios

Oct 12, 2015

El proceso de definición de formularios consta de la recopilación de la información de identificación específica de formulario y la información de acciones mediante las siguientes páginas del Asistente de definición de formularios para las aplicaciones Web:

- Nombrar formulario
- Identificar el formulario
- Configurar otros parámetros
- Confirmar los parámetros

Después de realizar las acciones necesarias para una página específica, haga clic en Siguiente para continuar por el asistente. Por lo general, el botón Atrás está disponible en cada página para volver a algunas opciones configuradas anteriormente. No obstante, el cambio de opciones configuradas anteriormente puede suponer la modificación de los parámetros posteriores.

Nombrar formulario

Al crear definiciones para las aplicaciones de tipo emuladores de terminal (HLLAPI), la página Nombrar formulario del asistente de definición de formularios se utiliza para:

- Asignar un nombre definido por el usuario para el formulario que se está creando
- Identificar el tipo de formulario que se está creando

Hay que tener en cuenta que el nombre asignado al formulario se muestra en la página Administrar formularios del Asistente de definición de aplicaciones. Se debe asignar un nombre significativo para el tipo de formulario que se está creando.

Se pueden definir varios tipos de formularios de procesamiento de credenciales de usuario mediante el Asistente de definición de formularios:

- Formulario de inicio de sesión
  Se utiliza para identificar la interfaz de inicio de sesión de una aplicación y para administrar las acciones de credenciales de usuario necesarias para obtener acceso a la aplicación asociada.

- Formulario de cambio de contraseñas
  Se utiliza para identificar la interfaz de cambio de contraseña de una aplicación y para administrar las acciones de credenciales de usuario necesarias para cambiar la contraseña de usuario para la aplicación asociada.

- Formulario de cambio de contraseñas satisfactorio
  Se utiliza para identificar la interfaz de cambio de contraseña de una aplicación y para administrar las acciones de credenciales de usuario necesarias para reconocer el cambio de la contraseña para la aplicación asociada.

- Formulario de cambio de contraseñas fallido
  Se utiliza para identificar la interfaz de cambio de contraseña incorrecto de una aplicación y para definir las acciones que se deben llevar a cabo cuando una operación de cambio de credenciales no se realiza correctamente.

El Agente de Password Manager de las versiones 4.0 y 4.1 no respalda los formularios de cambio de contraseña satisfactorio o fallido y no responde a las definiciones de aplicación que contienen dichos formularios.

Si el emulador utilizado muestra más de una página de inicio de sesión o cambio de contraseña, debe crearse un formulario para cada página.

Identificar el formulario

Al crear definiciones de aplicación para las aplicaciones de tipo emuladores de terminal (HLLAPI), la página Identificar el formulario se utiliza para proporcionar la información necesaria para que Single Sign-on Plug-in reconozca de forma exclusiva el formulario que se está definiendo.

Las aplicaciones de emuladores de terminal se identifican mediante la búsqueda de cadenas de texto que se muestran en ubicaciones de fila y columna específicos en la página de la aplicación de emuladores de terminal. Sólo es necesario definir las coincidencias de cadena de texto necesarias para identificar de forma exclusiva el host.

Para agregar una entrada de cualificación por coincidencia de texto

1. Asegúrese de que la aplicación de emuladores de terminal se ha iniciado y de haber determinado las cadenas de texto que se utilizarán para identificar de forma exclusiva la aplicación de destino.
2. En la página Identificar el formulario del Asistente definición de formularios, haga clic en Agregar para agregar una nueva entrada de coincidencia de texto a la lista de entradas de coincidencia de texto que se utiliza para calificar la aplicación. Con esta acción se abre el cuadro de diálogo Texto que coincidirá.
3. Rellene los campos siguientes del cuadro de diálogo Texto que coincidirá:
   - Cadena de texto
     Introduzca el texto exacto que se utilizará para identificar la aplicación.
   - Línea
     Introduzca el número de línea exacto de la cadena.
   - Columna
     Introduzca el número de columna exacto de la cadena.

   Nota: Cuando el software del plug-in analiza una aplicación de emuladores de terminal, examina la pantalla para comprobar si la cadena de texto exacta aparece en la ubicación de línea y columna definida. Si el texto en las coordenadas definidas no coincide con el texto especificado, la pantalla se ignora.
4. Haga clic en OK. La entrada Texto que coincidirá definida se muestra en la página Identificar el formulario.

Con frecuencia se deben definir varias cadenas de texto para identificar exactamente el inicio correcto de la aplicación de emuladores de terminal de destino. Si se necesitan más cadenas de Texto que coincidirá, repita los pasos 2 a 4 para cada cadena.

Configurar las reglas de detección de campos

La página Configurar las reglas de detección de campos se utiliza para identificar la ubicación y las acciones de las teclas necesarias para administrar el formulario de credenciales de usuario que se está definiendo.

El objetivo es crear entradas de campo que indiquen la credencial de usuario que se procesará, la ubicación en la pantalla donde se insertará la credencial de usuario (coordenadas de línea y columna) y las pulsaciones de teclado necesarias para avanzar el cursor a la siguiente credencial o acción de envío.

Para agregar una entrada de campo

1. Haga clic en Agregar para abrir el cuadro de diálogo Definir campo.
2. Complete los siguientes campos del cuadro de diálogo Definir campo:
   - Función del campo
     Seleccione la credencial de usuario que se enviará de las opciones que aparecen en el cuadro de lista.

- Línea
  Introduzca el número de línea exacto de la cadena.
- Columna
  Introduzca el número de columna exacto de la cadena.
- Teclas después
  Introduzca los códigos de tecla necesarios para avanzar al siguiente campo de credencial o para realizar la acción de envío.

  Nota: Seleccione el hipervínculo Códigos de teclas virtuales para acceder a la información sobre los códigos de tecla válidos.

3. Haga clic en Aceptar. La entrada definida aparece en la página Configurar las reglas de detección de campos.
4. Repita los pasos del 1 a 3 para cada credencial de usuario que necesite el formulario que se está definiendo.
5. Las entradas de campo que se muestran en la página Configurar las reglas de detección de campos se procesan de arriba a abajo, tal como aparecen en la página. Con las teclas de flecha Arriba y Abajo se pueden organizar las entradas en la secuencia que requiere el formulario de credenciales de usuario que se está procesando.

Configurar otros parámetros

La página Configurar otros parámetros se utiliza para acceder a opciones de configuración avanzada del formulario que se está definiendo. La configuración avanzada incluye:

- Definición de una demora inicial en el procesamiento del formulario
- Definición de las pulsaciones de teclado necesarias para acceder al formulario de administración de credenciales de usuario que se está definiendo
- Definición de los criterios de coincidencia de cadenas de texto que indican al software del plug-in que ignore el procesamiento

Si se necesita la configuración avanzada del formulario de administración de credenciales de usuarios que se quiere definir, haga clic en Avanzada para abrir el cuadro de diálogo Configuración avanzada.

Configuración avanzada de las aplicaciones de emulador de terminal

Oct 12, 2015

Algunas aplicaciones de emuladores de terminal requieren una configuración adicional para garantizar que se identifica el formulario correcto de administración de credenciales de usuario. Pueden ser:

- Esperar un tiempo definido para que la aplicación de emuladores de terminal se inicie antes de intentar identificar la aplicación
- Procesar una serie de pulsaciones de teclado para acceder a la página de inicio de sesión o página de cambio de contraseñas
- Ignorar el procesamiento de una página cuando aparezca un texto específico

Si se requiere una configuración avanzada del formulario de administración de credenciales de usuario que se está definiendo, haga clic en Avanzada en la página Configurar otros parámetros del Asistente de definición de formularios para abrir el cuadro de diálogo Configuración avanzada.

El cuadro de diálogo Configuración avanzada tiene dos páginas de configuración a las que se accede desde el panel izquierdo de la página:

- Resalte la opción Parámetros adicionales de formulario de host para acceder a las opciones de Parámetros adicionales:
  - Demorar entradas en los campos (ms). Introduzca la cantidad de milisegundos que demorará el procesamiento del formulario mientras se espera que la aplicación termine de cargarse.
  - Teclas antes. Indique los códigos de tecla virtual que se deben introducir para acceder al primer campo del formulario de administración de credenciales de usuario que se está procesando. Seleccione el hipervínculo Códigos de teclas virtuales para acceder a la ayuda de los códigos de tecla virtual válidos.
- Resalte la opción Ignorar coincidencia para acceder a la opción Coincidencia de texto para evitar el envío de credenciales. Esta opción se utiliza para especificar cadenas de texto que aparecen en la página de aplicación para los formularios que se ignorarán.

Consideraciones para las definiciones del tipo de emuladores de terminal

Oct 12, 2015

Al crear definiciones de aplicación del tipo emuladores de terminal (HLLAPI), se debe tener en cuenta lo siguiente:

- Se debe activar la compatibilidad de emulación de terminal para cada configuración de usuario que utilice aplicaciones de emuladores de terminal.
- Verificar que el programa de emulador de terminal sea compatible con HLLAPI.
- Verificar que el programa de emulador de terminal esté definido en el archivo mfrmlist.ini del software del plug-in.
- Se puede ahorrar tiempo mediante el uso de un emulador de terminal que muestre las coordenadas de fila y columna de la posición del cursor. De este modo resulta más fácil determinar la ubicación del texto y los campos que se utilizan para identificar la aplicación de host y sus formularios de inicio de sesión.
- Para la detección de HLLAPI, el emulador de terminal debe establecer un nombre corto para cada sesión. El software del plug-in no puede detectar aplicaciones basadas en emuladores de terminal sin el nombre corto de la sesión del emulador de terminal.
- Es posible que la documentación de la aplicación basada en emuladores de terminal incluya identificadores únicos, como números de pantalla, de las pantallas que se utilizan para enviar la información de inicio de sesión del usuario. En este caso, se debe utilizar el número de pantalla como el identificador único que garantiza que el software del plug-in identifica y envía credenciales al formulario correcto.

Compatibilidad de emulación de terminal

Oct 12, 2015

Los emuladores de terminal admitidos se encuentran en el archivo Mfrmlist.ini. Este archivo representa todos los emuladores de terminal que ha probado Citrix.

Se pueden agregar emuladores de terminal a esta lista. Sin embargo, estas definiciones deberían probarse y verificarse antes de introducirse en un entorno de producción. A continuación se incluye una sección de muestra de este archivo:

[Emulators] Ver=20021101 EMU1=Rumba6 EMU2=Attachmate myExtra! EMU3=Attachmate Extra! 6.3 EMU4=Attachmate Extra! 6.4 EMU5=Attachmate Extra! 6.5 EMU7=Attachmate Extra! 7.1 EMU8=R

Las entradas de emuladores de terminal en la sección [Emulators] del archivo Mfrmlist.ini deben estar en orden numérico ascendente, desde EMU1 hasta EMU99 inclusive. Cualquier interrupción de la secuencia provoca la finalización del proceso Ssomho.exe antes de que se lean todas las entradas.

La eliminación o el ocultamiento con marcas de comentario de los emuladores que no se utilizan pueden acelerar el proceso de inicio. De este modo, Ssomho.exe no desperdicia recursos o tiempo buscando la ubicación de archivos DLL de HLLAPI que no son necesarios.

Para ocultar una entrada, desplácela hacia el final de la lista, coloque un punto y coma antes de la entrada y vuelva a numerar el resto de entradas EMU de forma que no se omita ningún valor numérico.

Single Sign-on no puede actualizar globalmente este archivo mfrmlist.ini; debe sobrescribir el archivo manualmente tras instalar el plug-in. En entornos grandes, se recomienda utilizar lotes de archivos o scripts que se ejecuten a través de la instalación del software System Management Server (SMS), CA-Unicenter o Active Directory.

Definiciones de campo de Mfrmlist.ini

Oct 12, 2015

Los emuladores de terminales agregados al archivo Mfrmlist.ini sólo funcionarán si respetan el estándar HLLAPI. En la siguiente tabla se describen las definiciones de campo del archivo Mfrmlist.ini. Si es necesario agregar una definición de emulador de terminal, se recomienda consultar al fabricante para averiguar si el emulador de terminal es compatible con HLLAPI y para obtener las entradas de definición de campo correctas. Para averiguar si un emulador de terminal es compatible o no con Single Sign-on, pruébelo fuera del entorno de producción.

Campo	Definiciones
[EmulatorName]	El valor de EmulatorName debe coincidir con el valor utilizado para la línea EMUnn=EmulatorName en la sección [Emulators].
GroupName	Sólo para uso interno.
DisplayName	Nombre del emulador de terminal, que consta de uno de los dos parámetros que se utilizan cuando se crea un proceso nuevo para administrar la sesión y debe ser único para el archivo Mfrmlist.ini.
RegistryLoc	Clave de Registro en HKEY_LOCAL_MACHINE\SOFTWARE que hace referencia a la ruta en la que se encuentra la DLL HLLAPI. Si el programa no guarda esta información en HKEY_LOCAL_MACHINE\SOFTWARE, deberá utilizarse el parámetro ExplicitPath en lugar del parámetro RegistryLoc. Si se han definido los dos parámetros RegistryLoc y ExplicitPath, el parámetro ExplicitPath tiene prioridad.
ExplicitPath	Ruta explícita del archivo DLL HLLAPI utilizado por este emulador. Este parámetro se utiliza en lugar del parámetro RegistryLoc cuando el programa emulador no guarda la ubicación del archivo DLL HLLAPI en el Registro del sistema. Si se han definido los dos parámetros RegistryLoc y ExplicitPath, el parámetro ExplicitPath tiene prioridad.
ValueName	Nombre del valor en la clave RegistryLoc que contiene el valor de ruta real.
DLLFile	Nombre del archivo DLL de HLLAPI.
StripFileName	Indica que el valor de ValueName contiene una barra inclinada inversa que debe quitarse al ensamblar la ruta de la DLL de HLLAPI a partir de las entradas ValueName y DLLFile.
IntSize	Define el tamaño de enteros que respalda el emulador de terminal (16 bits o 32 bits).
WindowClass	Nombre de la clase de ventana para el emulador de terminal. Se obtiene usando consola de Single Sign-on o la Herramienta de definición de aplicaciones.

Campo	Definiciones
WindowTitle	Una parte del título de una ventana que Single Sign-on puede utilizar para garantizar que esta ventana esté asociada al emulador de terminal. Debe incluirse como mínimo una palabra que siempre aparezca en el título y no es necesario indicar el título completo.
UseSendKeys	Indica a Single Sign-on que utilice el método SendKeys para comunicarse con el emulador de terminal. La opción no es la misma que se utiliza para las aplicaciones de Windows.

Creación de configuraciones de usuario

Oct 12, 2015

Las configuraciones de usuario permiten controlar el comportamiento y el aspecto del software del plug-in para usuarios. La creación de una o varias configuraciones de usuario es el paso final que se realiza antes de distribuir el software de Single Sign-on Plug-in a los usuarios del entorno. Se pueden agregar o editar configuraciones de usuario existentes en cualquier momento.

Una configuración de usuario es un conjunto único de parámetros, directivas de contraseña y aplicaciones que se aplica a los usuarios asociados a una jerarquía de Active Directory (unidad organizativa [UO] o un usuario individual) o a un grupo de Active Directory.

Una configuración de usuario consta de los siguientes elementos:

- Usuarios asociados a una jerarquía de dominio (unidad organizativa o usuario individual) o grupo de Active Directory Importante: No se admiten los grupos de distribución y grupos de dominio local en modo mixto de Active Directory.
- Tipo de licencia y parámetros relacionados asociados a los usuarios (modelo de licencia de usuarios concurrentes o usuarios definidos)
- Métodos de protección de datos
- Las definiciones de aplicación que se han creado, que se pueden combinar en un grupo de aplicaciones al crear una configuración de usuario
- Directivas de contraseña asociadas a cualquier grupo de aplicaciones
- Funciones de autoservicio (desbloqueo de cuenta y restablecimiento de contraseña) y opciones de administración de claves (uso de contraseñas anteriores, preguntas de seguridad y administración automática de claves)
- Parámetros de configuración de aprovisionamiento de credenciales y compatibilidad con aplicaciones

Antes de crear las configuraciones de usuario, es necesario asegurarse de que se han creado o definido los siguientes elementos:

- Almacén central
- Definiciones de aplicación
- Directivas de contraseña
- Preguntas de seguridad

Las configuraciones de usuario deben crearse antes de instalar el software de Single Sign-on Plug-in en los equipos de los usuarios. Entre otros parámetros, una configuración de usuario contiene la información de servidor de licencias y de licencia que necesita el software del plug-in para funcionar.

Para obtener los detalles y los valores predeterminados de la configuración de usuario, consulte los temas de *— Referencia de configuración de Single Sign-on > Configuraciones de usuario*
.

Para especificar un controlador de dominio para una configuración de usuario existente

En los entornos donde se utiliza un almacén central basado en Active Directory y hay varios controladores de dominio, se puede seleccionar el controlador de domino al que se vincularán las configuraciones de usuario al escribir en el almacén central.

Este esquema de vinculación contribuye a reducir las demoras de sincronización provocadas por la duplicación de Active

Directory. Dichas demoras se pueden producir en entornos donde los usuarios acceden a Single Sign-on en varios sitios de Active Directory simultáneamente.

Durante el proceso de descubrimiento disponible a través de la consola, Single Sign-on puede descubrir todos los controladores de dominio en el dominio. A continuación se pueden vincular las configuraciones de usuario que se han creado a un controlador de dominio específico seleccionándolo al crear una configuración de usuario.

Por ejemplo, se puede exigir a los usuarios que estén vinculados a un controlador de dominio en su red local. Después de especificar un controlador de dominio, los usuarios quedan vinculados a ese controlador la próxima vez que inician sesión en Single Sign-on.

De forma predeterminada, los usuarios se vinculan a cualquier controlador de dominio en el que se pueda escribir hasta que se seleccione el controlador de dominio al que se deben vincular. Se puede cambiar el parámetro de controlador de dominio en cualquier momento actualizando la configuración de usuario según sea necesario sin perder la integridad de datos de usuario.

Nota: Al elegir un controlador de dominio para vinculación, debe verificarse que los recursos disponibles en el mismo puedan aceptar el tráfico de comunicaciones que generan los usuarios al conectarse a él durante las horas de máxima actividad. Si el controlador de dominio especificado no está disponible o está desconectado, el software del plug-in utiliza los datos de usuario del almacén local (es decir, los datos de usuario que se encuentran en el equipo del usuario). Si el controlador de dominio está desconectado durante un largo período (según se haya definido), se puede seleccionar la tarea Modificar configuración de usuario en la consola y elegir otro controlador de dominio o la opción Cualquier controlador de dominio en que se pueda escribir.

1. Haga clic en Inicio > Todos los programas > Citrix > Consolas de administración > Citrix AppCenter.
2. Expanda el nodo Single Sign-on y las Configuraciones de usuario.
3. Seleccione una configuración de usuario.
4. En el menú Acción, seleccione Modificar configuración de usuario.
5. Seleccione Controlador de dominio en las opciones de la parte izquierda de la página del asistente Modificar configuración de usuario.
6. Seleccione un controlador de dominio disponible o Cualquier controlador de dominio en que se pueda escribir.

Para crear una configuración de usuario

1. Haga clic en Inicio > Todos los programas > Citrix > Consolas de administración > Citrix Delivery Services Console.
2. Expanda el nodo Single Sign-On y seleccione Configuraciones de usuario.
3. En el menú Acción, haga clic en Agregar configuración de usuario nueva.

Designación de nombres de configuraciones de usuario

La página Nombre de la configuración de usuario del Asistente de configuración de usuarios permite dar nombres a las configuraciones y elegir como se asociarán las mismas a los usuarios.

- Name
  El nombre de la configuración de usuario se debe asignar según el modo en que se piense agrupar los usuarios y asociarlos a aplicaciones específicas. Por ejemplo, Usuarios Marketing, Usuarios Desarrollo de software, Usuarios América del Norte, etc.

- Asociación de la configuración de usuario
  Existen dos posibilidades: asociar usuarios según una jerarquía de Active Directory (unidad organizativa o usuario

individual) o según un grupo de Active Directory. Si es necesario, se puede asociar la configuración de usuario a otra jerarquía o grupo posteriormente, haciendo clic en Mover configuración de usuario en el menú Acción.

Importante: El modo en que se organice el entorno de Active Directory puede afectar al funcionamiento de las configuraciones de usuario. Si se utilizan ambos (jerarquía y grupo de Active Directory) y un usuario se encuentra en ambos contenedores, tiene prioridad la configuración de usuario asociada a la jerarquía y es la que se utiliza. Este esquema se considera un entorno mixto.
Además, si un usuario pertenece a dos grupos de Active Directory y cada uno está asociado a una configuración de usuario, se antepone la que tenga mayor prioridad y es la que se utiliza.

La asociación de configuraciones de usuario a grupos sólo se admite en dominios de Active Directory que utilizan la autenticación de Active Directory.

Especificación de un controlador de dominio

Si está usando un almacén central en Active Directory, la página Especificar el controlador de dominio del Asistente de configuración de usuarios le permite seleccionar un controlador de dominio disponible o elegir Cualquier controlador de dominio en que se pueda escribir.

Selección de aplicaciones y configuración de parámetros del usuario

Oct 12, 2015

En la página Elegir aplicaciones del Asistente de configuración de usuarios, agregue las aplicaciones de la configuración de usuario. Al hacer clic en el botón Agregar, aparece un cuadro de diálogo y muestra las definiciones de aplicación que se han creado anteriormente. Podrá combinar estas definiciones de aplicación en un grupo de aplicaciones. Un grupo de aplicaciones puede contener varias aplicaciones o solamente una aplicación.

También puede definir el grupo de aplicaciones como un grupo de contraseñas compartidas para automatizar y simplificar el proceso de cambio de contraseña. Si cambia la contraseña de una definición de aplicación que forma parte de un grupo de contraseñas compartidas, el software del plug-in hace que el cambio se refleje en las credenciales almacenadas de todas las aplicaciones del grupo.

Los grupos de contraseñas compartidas permiten que el software del plug-in administre varias credenciales para aplicaciones que utilizan la misma autoridad de autenticación. Por ejemplo, si hay dos aplicaciones que usan la misma base de datos de Oracle para la autenticación (como una aplicación de finanzas y otra de recursos humanos), pueden colocarse ambas aplicaciones en el mismo grupo de contraseñas. Cuando el usuario cambia la contraseña en una de las aplicaciones, las credenciales de la otra aplicación se actualizan automáticamente.

Importante: Para obtener mejores resultados, todas las contraseñas del grupo de contraseñas se deben administrar mediante una autoridad de autenticación común. Por ejemplo, se puede implementar un grupo de contraseñas compartidas si las aplicaciones del grupo comparten una autoridad de sistema de autenticación común, como una base de datos, donde el usuario envíe las mismas credenciales para cada aplicación con el fin de autenticarse con la base de datos. No se deben agrupar aplicaciones no relacionadas, como un programa de correo electrónico, una aplicación Web y un programa personalizado habilitado para Single Sign-on en la intranet donde un usuario podría enviar tres conjuntos distintos de credenciales, pero sólo por coincidencia utiliza las mismas credenciales para las tres aplicaciones. En este caso, si un usuario cambia las credenciales de una aplicación en este grupo de contraseñas compartidas, estas credenciales no serán válidas necesariamente para las otras dos aplicaciones.

Configuración de parámetros del usuario

Use las siguientes páginas para configurar los parámetros del usuario: Para obtener detalles de configuración, consulte los temas de

— Referencia de configuración de Single Sign-on > Configuraciones de usuario

.

- La página Configurar la interacción con Single Sign-on Plug-in del Asistente de configuración de usuarios le permite determinar la experiencia de los usuarios del software del plug-in en el entorno.
- Elija un servidor de licencias y un modelo de licencia en la página Configurar las licencias del Asistente de configuración de usuarios.
  Importante: Si se edita la configuración de usuario posteriormente y se cambian las ediciones de producto, cambiará el modelo de licencias. Por ejemplo, el cambio de la edición de producto de Single Sign-on Enterprise a Single Sign-on Advanced modificará el modelo de licencias de Usuario concurrente a Usuario definido.
- La página Seleccionar los métodos de protección de datos del Asistente de configuración de usuarios le permite seleccionar métodos de protección de datos para proteger las credenciales de los usuarios usando distintos métodos de autenticación. En algunos entornos, los usuarios pueden utilizar más de un método.
- Cuando los usuarios cambien su autenticación primaria (por ejemplo, se cambie una contraseña de dominio o se

reemplace una tarjeta inteligente), la página Seleccionar la protección de datos secundaria del Asistente de configuración de usuarios permite especificar opciones de protección de datos de credenciales secundarias que se utilizarán antes de desbloquear las credenciales de usuario. También permite exigir a los usuarios que verifiquen su identidad para mayor seguridad. Alternativamente, también permite especificar que las credenciales se restauren automáticamente mediante la implementación del Módulo de administración de claves.

- Las opciones disponibles en la página Habilitar las funciones de autoservicio del Asistente de configuración de usuarios requieren la instalación del Módulo de administración de claves. Esta función inserta el botón Autoservicio de cuentas en los cuadros de diálogo de Inicio de sesión de Windows y Desbloquear equipo y contribuye a reducir los gastos asociados con la intervención del administrador o del servicio de asistencia técnica de la empresa.
- Las páginas Módulo de administración de claves y Módulo de aprovisionamiento del Asistente de configuración de usuarios necesitan que se especifique la ruta URL y el puerto de los módulos de servicio instalados.

Sincronización de credenciales mediante la asociación de cuentas

Oct 12, 2015

En las empresas que mantienen varios dominios de Windows, los usuarios también pueden tener varias cuentas de Windows. Single Sign-on incluye un servicio denominado Sincronización de credenciales para activar la asociación de cuentas.

Con la asociación de cuentas los usuarios pueden iniciar sesión en cualquier aplicación desde una o varias cuentas de Windows. Como Single Sign-on normalmente vincula las credenciales de usuario a una sola cuenta, la información de credenciales no se sincroniza automáticamente entre las distintas cuentas que posee un usuario. No obstante, los administradores pueden configurar la asociación de cuentas para sincronizar las credenciales de usuario. Los usuarios que tienen configurada la asociación de cuentas disponen de acceso a todas las aplicaciones desde cualquiera de sus cuentas en su entorno de Single Sign-on. Cuando las credenciales de usuario se cambian, agregan o eliminan de una cuenta, se sincronizarán automáticamente con cada una de las cuentas asociadas del usuario.

Sin la asociación de cuentas, una persona con varias cuentas de Windows está obligada a cambiar manualmente su información de inicio de sesión independientemente en cada cuenta de Windows.

Para configurar la asociación de cuentas, los administradores de dominio de Windows de la empresa deben realizar las siguientes tareas en el orden indicado:

1. Elegir un dominio en el que se instalará y ejecutará el módulo de sincronización de credenciales, que forma parte del Servicio Single Sign-on.
2. Instalar el certificado raíz de confianza en todos los equipos de la empresa que utilizarán la asociación de cuentas.
3. Sincronizar manualmente las definiciones de aplicación entre los dominios.
4. Configurar los parámetros de usuario de la asociación de cuentas en otros dominios para conectarse con el módulo de sincronización de credenciales.
5. Poner la herramienta de asociación de cuentas a disposición de los usuarios como una aplicación publicada.

Cada usuario debe activar la asociación de cuentas en el Single Sign-on Plug-in.

Elección y configuración de un dominio para alojar el módulo de sincronización de credenciales

Elija el dominio que contiene las cuentas de todos los usuarios de la empresa que utilizarán la asociación de cuentas. El módulo de sincronización de credenciales actúa de concentrador de toda la información de credenciales de usuario en la empresa. Instale este módulo en el dominio del mismo modo que cualquier otro Servicio Single Sign-on.

Importante: Póngase en contacto con el administrador de red para determinar si es necesario realizar algunos cambios en el servidor de seguridad y si éstos son compatibles con las directivas de la compañía.
Después de haber instalado el módulo de sincronización de credenciales, se deben crear o editar las configuraciones de usuario desde Citrix AppCenter para autorizar a las cuentas de usuario individuales el uso del módulo de sincronización de credenciales.

Para configurar las funciones de sincronización de credenciales en el dominio host

Abra la consola desde el dominio que aloja el módulo de sincronización de credenciales. Algunos dominios pueden acceder a varios almacenes centrales. Asegúrese de que la consola que utiliza está configurada para conectarse al mismo almacén central que el servicio del módulo de sincronización de credenciales.

1. Haga clic en Inicio > Todos los programas > Citrix > Consolas de administración > Citrix AppCenter.
2. Expanda el nodo Single Sign-On y seleccione Configuraciones de usuario.
3. Seleccione una configuración de usuario existente o cree una nueva.
   - Si va a crear una nueva configuración de usuario, las siguientes opciones están disponibles en el botón Configuración avanzada de la página Configurar la interacción con el plug-in del Asistente de configuración de usuarios.
   - Si va a editar una configuración de usuario existente, las siguientes opciones están disponibles en la página de propiedades Modificar configuración de usuario.
4. Haga clic en Sincronización y seleccione Permitir acceso a credenciales de usuario a través del módulo de sincronización.
5. Haga clic en Aceptar y repita los pasos 3 y 4 para cada configuración de usuario existente y nueva.

Para sincronizar manualmente las definiciones de aplicación entre los dominios

Las cuentas también se pueden sincronizar entre distintas configuraciones de usuario. Por ejemplo, una configuración de usuario puede estar asociada a una jerarquía de Active Directory (unidad organizativa o usuario) en un dominio y a un grupo de Active Directory en otro dominio. Siempre que los nombres de definición de aplicación sean los mismos en cada configuración, la función de asociación de cuentas sincronizará las credenciales.

Las credenciales de usuario se comparten únicamente para las aplicaciones que ha definido el administrador de Single Sign-on. Los administradores deben asegurarse de que cada definición de aplicación en cada dominio tenga el mismo nombre en cada almacén central.

Por ejemplo, si la definición de aplicación para SAP se denomina SAP Logon en un dominio, SAP en otro y SAP Launch Pad en otro, las credenciales de usuario para estas aplicaciones no se sincronizarán entre las cuentas de estos dominios.

Una práctica recomendada al crear una nueva definición de aplicación entre dominios consiste en utilizar las tareas Exportar definiciones de aplicación e Importar datos de administración en la consola. Estas tareas se utilizan para exportar las definiciones de aplicación recién creadas que se importarán en cada almacén central. El nombre de las aplicaciones definidas anteriormente ya existentes se debe cambiar manualmente.

Para configurar los parámetros de usuario de la asociación de cuentas en otros dominios

instale y abra la consola desde una estación de trabajo en cada dominio que no aloje el módulo de sincronización de credenciales. Algunos dominios tienen varios almacenes centrales; por lo tanto, asegúrese de configurar cada almacén central.

Todos los administradores de dominio deben permitir que los usuarios de dominio asocien sus cuentas a su cuenta de dominio host. Edite la sección de asociación de cuentas de las configuraciones de usuario adecuadas en la consola.

1. Haga clic en Inicio > Todos los programas > Citrix > Consolas de administración > Citrix AppCenter.
2. Expanda el nodo Single Sign-On y seleccione Configuraciones de usuario.
3. Seleccione una configuración de usuario existente o cree una nueva.
   - Si va a crear una nueva configuración de usuario, las siguientes opciones están disponibles en el botón Configuración avanzada de la página Configurar la interacción con el plug-in del Asistente de configuración de usuarios.
   - Si va a editar una configuración de usuario existente, las siguientes opciones están disponibles en la página de propiedades Modificar configuración de usuario.
4. Haga clic en Asociación de cuentas.
5. Seleccione Permitir que los usuarios asocien cuentas.

Las siguientes opciones no son obligatorias pero contribuyen a proporcionar una interacción del usuario fluida.

6. Seleccione Suministrar la dirección del servicio predeterminado y escriba la dirección del Servicio Single Sign-on y el puerto del dominio que aloja el módulo de sincronización de credenciales.
7. Desactive Permitir que los usuarios modifiquen la dirección del servicio.
8. Seleccione Suministrar dominio predeterminado y el nombre del dominio que aloja el módulo de sincronización de credenciales. Si no se proporciona el dominio, es posible que los usuarios no sepan a qué cuenta de dominio deben proporcionar las credenciales de usuario.
9. Desactive Permitir que los usuarios modifiquen el dominio.
10. Según las directivas de seguridad de la compañía, seleccione Permitir al usuario recordar su contraseña.
11. Haga clic en Aceptar y repita esta operación para cada configuración de usuario.

Publicación de la herramienta de asociación de cuentas

Como esta versión de Single Sign-on Plug-in no ofrece una opción de menú que permita a los usuarios activar la asociación de cuentas, se proporciona a los usuarios una herramienta para activar la asociación de cuentas como una aplicación publicada:

1. Instale Single Sign-on Plug-in en un servidor XenApp.
2. Busque el archivo AccAssoc.exe en el servidor XenApp.
3. Publique el archivo AccAssoc.exe y póngalo a disposición de los usuarios.
4. Informe a los usuarios sobre cómo acceder a la herramienta de asociación de cuentas y cómo utilizarla.

Nota: Los usuarios que ejecutan la versión 4.8 y las versiones anteriores de Single Sign-on Plug-in pueden utilizar una opción de menú del plug-in para activar la asociación de cuentas. Estos usuarios no necesitan acceso a la herramienta de asociación de cuentas como una aplicación publicada.

Para activar la asociación de cuentas en Single Sign-on Plug-in

Oct 12, 2015

Al iniciar la sesión en el dominio que aloja el módulo de sincronización de credenciales, los usuarios no tienen que realizar ninguna acción para activar la asociación de cuentas. Estas cuentas actúan como un punto central para la información de credenciales de cada usuario.

Al iniciar la sesión en otros dominios, los usuarios pueden activar la asociación de cuentas de dos formas, según la versión de Single Sign-on Plug-in que utilicen:

- En esta versión de Single Sign-on Plug-in, los usuarios deben acceder a la herramienta de asociación de cuentas como una aplicación publicada. Es necesario publicar la herramienta de asociación de cuentas e informar a los usuarios sobre la forma de acceder a esa herramienta y utilizarla.
- En la versión 4.8 y las versiones anteriores de Single Sign-on Plug-in, los usuarios pueden ver una opción Asociación de cuentas en el menú Herramientas del Administrador de inicios de sesión del software del plug-in. Los usuarios deben seleccionar esta opción para activar la asociación de cuentas.

1. Según la versión del plug-in, los usuarios pueden acceder a la herramienta de asociación de cuentas como una aplicación publicada o seleccionar Herramientas > Asociación de cuentas en el Administrador de inicios de sesión. Se muestra el cuadro de diálogo Asociación de cuentas.
2. Los usuarios deben seleccionar Habilitar la asociación de cuentas.
   Nota: Si usted no proporcionó la dirección del servicio que aloja el módulo de sincronización de credenciales, los usuarios deben escribirla en el campo de texto. Si el campo no está disponible, significa que ya se ha indicado esta dirección de servicio y los usuarios no pueden escribir en este campo.
3. Los usuarios deben hacer clic en Aceptar. Se muestra el cuadro de diálogo Autenticarse para la asociación de cuentas.
4. Los usuarios deben escribir el nombre de usuario y la contraseña de la cuenta de Windows asociada del usuario. Si el dominio donde se instaló el módulo de sincronización de credenciales no se muestra, los usuarios deben escribirlo en el campo Dominio.
   Nota: Si usted ya indicó este nombre de dominio, los usuarios no pueden escribir en este campo.
5. Los usuarios deben hacer clic en Aceptar. La asociación de cuentas ya está activada. Las credenciales de usuario se sincronizarán cuando se produzca la sincronización del software del plug-in.

Administración de configuraciones de usuario

Oct 12, 2015

Single Sign-On permite administrar las configuraciones de usuario. Se puede:

- Restablecer los datos del usuario
- Eliminar los datos del usuario
- Pedir a los usuarios que vuelvan a registrarse
- Establecer la prioridad de una configuración de usuario
- Asignar la configuración de usuario a diferentes usuarios
- Actualizar la configuración de usuario de usuarios existentes

Para restablecer los datos del usuario

La tarea Restablecer los datos de usuario requiere la instalación y configuración del módulo de aprovisionamiento.

Restablecer los datos de usuario permite restablecer la información del usuario en el almacén central, con lo que el usuario seleccionado vuelve al estado inicial.

- En los almacenes centrales de Active Directory, los datos de usuario (credenciales, preguntas y respuestas de seguridad, etc.) se eliminan y se marca al usuario para indicar que se han restablecido sus datos.
- En los almacenes centrales de un punto compartido de red NTFS, las carpetas del usuario se conservan y todos sus datos se eliminan, y se marca al usuario para indicar que se han restablecido sus datos.

Se puede utilizar Restablecer los datos de usuario si los usuarios han olvidado las respuestas a sus preguntas de seguridad o para restablecer sus datos de credenciales si los datos de los usuarios se han dañado de alguna forma. Cuando el usuario posteriormente utiliza el software del plug-in para ponerse en contacto con el almacén central, se eliminan todos los datos del almacén de credenciales local del usuario y el usuario debe volver a inscribirse.

Esta tarea también resulta útil cuando un usuario no puede iniciar sesión en el software del plug-in.

Importante: Se conserva un historial de contraseñas para cada usuario. Si se restablecen los datos de un usuario, su historial de contraseñas se elimina y no se puede aplicar para las contraseñas eliminadas.

1. Haga clic en Inicio > Todos los programas > Citrix > Consolas de administración > Citrix AppCenter.
2. Expanda el nodo Single Sign-On y seleccione Configuraciones de usuario.
3. En el menú Acción, haga clic en Otras tareas > Restablecer los datos de usuario. Aparece el cuadro de diálogo Seleccionar usuario.
4. Escriba el nombre de usuario en el campo de texto y haga clic en Comprobar nombres.
5. Si se encuentra al usuario, haga clic en Aceptar.
6. Seleccione un usuario del almacén central y haga clic en Restablecer.
7. Haga clic en Aceptar. Aparece un mensaje de advertencia.
8. Compruebe que los usuarios que puedan estar ejecutando Single Sign-on como una aplicación alojada por Citrix XenApp hayan cerrado la sesión y haga clic en Continuar para marcar el restablecimiento de los datos del usuario.
   Nota: Si los usuarios no han cerrado la sesión, haga clic en Cancelar, restablezca su sesión ICA y vuelva a este procedimiento.
9. Haga clic en Aceptar en el cuadro de diálogo Restablecer los datos de usuario cuando se verifique y restablezca la información del usuario. Los datos del usuario se restablecen la próxima vez que éste inicia sesión en Single Sign-on mediante el software del plug-in.

Para eliminar los datos del usuario

La tarea Eliminar los datos de usuario del almacén central elimina todos los datos e información del usuario del almacén central. Se puede utilizar Eliminar los datos de usuario del almacén central cuando un usuario se marche de la empresa definitivamente.

El almacén de credenciales local del equipo del usuario permanece intacto hasta que lo elimina un administrador u operador de forma explícita.

Si el usuario eliminado ejecuta el software del plug-in, éste sincroniza su almacén de credenciales local con el almacén central a menos que un administrador u operador haya eliminado el almacén de credenciales local de forma explícita. Para evitar esta situación, se debe eliminar al usuario de la empresa (por ejemplo, desactivar o eliminar al usuario de Active Directory).

1. Haga clic en Inicio > Todos los programas > Citrix > Consolas de administración > Citrix AppCenter.
2. Expanda el nodo Single Sign-On y seleccione Configuraciones de usuario.
3. En el menú Acción, haga clic en Otras tareas > Eliminar los datos de usuario del almacén central. Aparece el cuadro de diálogo Seleccionar usuario.
4. Escriba el nombre de usuario en el campo de texto y haga clic en Comprobar nombres.
5. Si se encuentra al usuario, haga clic en Aceptar. Haga clic en Sí para confirmar. Aparece un mensaje de confirmación.
6. Haga clic en Aceptar. El usuario se elimina del almacén central.

Para pedir a los usuarios que vuelvan a registrarse

Se puede pedir a uno o a todos los usuarios que vuelvan a registrar respuestas a sus preguntas de seguridad. Estas funciones se utilizan por motivos de seguridad o cuando se dañan los datos de usuario:

- Revocar el registro de preguntas de seguridad del usuario
  Al seleccionar esta opción, se eliminan los datos de pregunta de seguridad de un usuario. La autenticación con preguntas no estará disponible hasta que el usuario se vuelva a registrar.

- Pedirle a todos los usuarios que vuelvan a registrar las preguntas de seguridad
  Al seleccionar esta opción, se les pide a los usuarios que vuelvan a registrar sus preguntas y respuestas de seguridad cuando inicien el software del plug-in. Los datos de pregunta de seguridad se mantienen y cualquier función que requiera la autenticación con preguntas sigue estando disponible con las respuestas actuales. A los usuarios se les hace la petición hasta que se vuelven a registrar.

Si los usuarios deciden no volver a registrar sus respuestas mediante la cancelación del cuadro de diálogo Registro con Citrix Single Sign-on cuando se les pide, no podrán utilizar las funciones que usan la autenticación con preguntas, como el autoservicio de cuentas, hasta que vuelvan a registrar las respuestas.

1. Haga clic en Inicio > Todos los programas > Citrix > Consolas de administración > Citrix AppCenter.
2. Expanda el nodo Single Sign-on y seleccione Configuraciones de usuario.
3. En el menú Acción, haga clic en Otras tareas y en alguna de las siguientes:
   - Revocar el registro de preguntas de seguridad del usuario
     Aparece el cuadro de diálogo Seleccionar usuario. Escriba un nombre o seleccione un usuario. Confirme que desea revocar el registro de preguntas de seguridad de dicho usuario.

   - Pedirle a todos los usuarios que vuelvan a registrar las preguntas de seguridad
     Haga clic en Sí para realizar la petición a todos los usuarios y, a continuación, haga clic en Aceptar.

Para establecer una prioridad de configuración de usuario

Al crear o editar una configuración de usuario, se pueden asociar usuarios de grupos de Active Directory a configuraciones de usuario. Es posible que un usuario de un grupo pueda estar asociado a una o varias configuraciones de usuario. En este caso, se puede establecer la prioridad de la configuración de usuario.

Importante: El modo en que se organice el entorno de usuario de Single Sign-on puede afectar el funcionamiento de las configuraciones de usuario. Es decir, las configuraciones de usuario se asocian en el entorno de Single Sign-on a una jerarquía (unidad organizativa o usuarios) o a un grupo de Active Directory. Si se utilizan ambos (jerarquía y grupo) y un usuario se encuentra en ambos contenedores, tiene prioridad la configuración de usuario asociada a la jerarquía y es la que se utiliza. Este esquema se considera un entorno mixto.

1. Haga clic en Inicio > Todos los programas > Citrix > Consolas de administración > Citrix AppCenter.
2. Expanda el nodo Single Sign-On y seleccione Configuraciones de usuario.
3. En el menú Acción, haga clic en Otras tareas > Configurar la prioridad de la configuración de usuario. Se muestra el cuadro de diálogo Configurar la prioridad de la configuración de usuario.
4. Seleccione una configuración de usuario y haga clic en Subir o en Bajar, según sus preferencias.

Asignación de una configuración de usuario a diferentes usuarios

Al editar una configuración de usuario existente, no se puede modificar la ubicación de la misma. Se puede realizar uno de los siguientes procedimientos:

- Duplicar una configuración de usuario para aplicarla a un conjunto de usuarios adicional.
- Mover una configuración de usuario para aplicarla a otro conjunto de usuarios.

Para duplicar una configuración de usuario

1. Haga clic en Inicio > Todos los programas > Citrix > Consolas de administración > Citrix AppCenter.
2. Expanda el nodo Single Sign-On y seleccione Configuraciones de usuario.
3. Seleccione la configuración de usuario.
4. En el menú Acción, haga clic en Duplicar configuración de usuario.
5. Escriba un nombre para la configuración duplicada.
6. Especifique la unidad organizativa, el usuario o el grupo que contiene a los usuarios a los que se aplicará la configuración de usuario.

Para mover una configuración de usuario a diferentes usuarios

No se puede mover una configuración de usuario que esté asociada a un grupo de Active Directory. Para asociar la configuración de usuario a una jerarquía de Active Directory (unidad organizativa o usuario), se debe duplicar y especificar la asociación que se desee.

1. Haga clic en Inicio > Todos los programas > Citrix > Consolas de administración > Citrix AppCenter.
2. Expanda el nodo Single Sign-On y seleccione Configuraciones de usuario.
3. Seleccione la configuración de usuario.
4. En el menú Acción, haga clic en Mover configuración de usuario.
5. Especifique la unidad organizativa, el usuario o el grupo que contiene a los usuarios a los que se aplicará la configuración de usuario.

Actualización de configuraciones de usuario existentes

En las versiones 4.0 y 4.1 de Password Manager, los usuarios se asocian a una configuración de usuario mediante una

jerarquía de Active Directory (unidad organizativa o usuario). En Password Manager 4.5 y 4.6 y Single Sign-on 4.8 y 5.0, puede elegir asociar los usuarios por un grupo de Active Directory.

- Si se utiliza una configuración de usuario existente organizada por jerarquía, se crean configuraciones de usuario organizadas por grupo y un usuario se encuentra en ambos contenedores, tiene prioridad la configuración de usuario asociada a la jerarquía y es la que se utiliza. Este esquema se considera un entorno mixto. En dicho caso, los usuarios pueden sufrir comportamientos inesperados en el software del plug-in. Es decir, tendrán acceso a recursos asociados con la configuración de usuario sobre la base de la jerarquía en lugar de los asociados con la configuración de usuario basada en el grupo.
- Si se desea mantener los parámetros de las configuraciones de usuario basadas en jerarquía y cambiar su asociación, mueva la configuración de usuario a un usuario diferente. Este procedimiento se aplica a las configuraciones de usuario basadas en jerarquía de las versiones 4.1, 4.5, 4.6, 4.8. y 5.0.

Se debe tener en cuenta lo siguiente si se desea actualizar las configuraciones de usuario existentes cuyos usuarios estén organizados por unidad organizativa o usuario:

Si se actualizan el servicio y la consola de Single Sign-on pero no se actualiza el software del plug-in, éste seguirá proporcionando funciones básicas a los usuarios cuyas configuraciones de usuario estén asociadas a jerarquías de Active Directory (unidades organizativas o usuarios). No obstante, los usuarios no tendrán acceso a las funciones de Single Sign-on más recientes. Actualice el software del plug-in siempre que sea posible para que coincida con las versiones de servicio y consola.

Autenticación de usuarios y verificación de la identidad

Oct 12, 2015

Single Sign-on ofrece dos tipos de autenticación:

- La autenticación primaria, que ocurre cuando los usuarios escriben sus nombres de usuario, contraseñas y, opcionalmente, nombre de dominio al iniciar la sesión en Microsoft Windows para acceder a la red de la empresa. El subsistema de seguridad de Windows existente es responsable de administrar la autenticación en la red.
- La autenticación secundaria, que ocurre cuando se configura Single Sign-on para que envíe las credenciales con las que los usuarios acceden a recursos protegidos y habilitados con inicio de sesión único (Single Sign-on). Entre dichos recursos se pueden contar aplicaciones empresariales, aplicaciones Web, campos protegidos de aplicaciones, direcciones IP, URL, etc.

Tras una autenticación de red satisfactoria, Single Sign-on obtiene la contraseña primaria del inicio de sesión de Windows y, junto con otras variables, usa esa información para crear la clave de cifrado que protege las credenciales. El software del plug-in utiliza esta clave para obtener y descifrar las credenciales cuando las solicitan las aplicaciones o los recursos.

Importante: Si la contraseña de un usuario ha visto comprometida su seguridad, restablézcala dos veces en lugar de una para que la contraseña que presenta riesgo de seguridad deje de figurar en la función de contraseña anterior. Los usuarios deben iniciar sesión con cada una de las contraseñas para que el software del plug-in capture los cambios.

Situaciones en las que los usuarios deben confirmar su identidad

Cada vez que un usuario inicie sesión en el entorno, deberá confirmar su identidad indicando su nombre de usuario y contraseña, o bien utilizando una tarjeta inteligente o cualquier otro dispositivo de identificación que permita verificar su identidad.

No obstante, cuando se producen ciertos sucesos, es necesario un segundo nivel de autenticación para comprobar que el usuario que solicita el cambio es el autorizado para hacerlo.

Event (Suceso)	Descripción
Un administrador cambia la contraseña primaria de un usuario	Cuando los administradores modifican las contraseñas primarias de los usuarios, éstos reciben un mensaje de aviso en el que se les pide que confirmen su identidad. De este modo, se garantiza que el usuario que ha iniciado sesión es el usuario autorizado.
Los usuarios restablecen su contraseña primaria con el autoservicio de contraseñas.	Cuando los usuarios restablecen su contraseña primaria mediante la opción Autoservicio de cuentas, se les pide que confirmen su identidad. No use la opción de autenticación Pedir al usuario que introduzca su contraseña anterior si habilitará las funciones de autoservicio.
Los usuarios desbloquean sus cuentas de dominio con el autoservicio de contraseñas.	Cuando los usuarios desbloquean sus cuentas mediante las funciones del autoservicio, se les pide que confirmen su identidad.
Los usuarios cambian sus tipos de autenticación.	Por ejemplo, cuando los usuarios cambian de método de autenticación (por ejemplo, si dejan de usar tarjetas inteligentes

Event (Suceso)	Descripción
	para usar la autenticación con contraseñas), se les pide que confirmen su identidad.
Se realiza un cambio de contraseña en un dispositivo cliente que no ejecuta Single Sign-on.	Los usuarios que modifiquen su contraseña primaria en un dispositivo cliente en el que no se ejecute el software del plug-in deberán confirmar su identidad cuando inicien sesión en otro dispositivo donde sí se ejecute.

Los usuarios pueden confirmar sus identidades usando una o varias de las opciones que pueden especificarse dependiendo de las necesidades de la empresa.

Métodos de verificación de identidad

Single Sign-on incluye dos métodos de verificación de identidad que permiten garantizar que el usuario esté autorizado a utilizar Single Sign-on:

- Contraseña anterior
- Preguntas de seguridad

También se puede elegir suplantar la verificación de la identidad usando la función de administración de claves.

Se puede permitir que los usuarios usen el método de verificación de identidad (contraseña anterior o preguntas de seguridad) que prefieran para autenticarse. Esta opción está disponible como parte de la propiedad Protección de datos secundaria de la configuración de usuario.

Contraseña anterior

Con este método, los usuarios verifican su identidad indicando sus contraseñas primarias anteriores.

Precaución: Si sólo se utiliza el método de contraseña anterior, los usuarios que no recuerden su contraseña principal anterior no podrán acceder al sistema, sus datos de usuario se borrarán en el almacén central y en todos los dispositivos cliente donde estén almacenados, y deberán volver a introducir sus credenciales para todas las aplicaciones.

Preguntas de seguridad

Cuando los usuarios cambian sus contraseñas primarias, se puede confirmar su identidad pidiendo que respondan a unas preguntas de seguridad sacadas de un cuestionario. El cuestionario aparece la primera vez que los usuarios inician el software del plug-in. A continuación, se les pedirá que respondan varias preguntas de seguridad cuyo número habrá definido el administrador. En adelante, se utilizará el mismo procedimiento cuando se produzcan determinados sucesos de cambio de contraseñas.

Las preguntas deben reunir las características de seguridad necesarias para garantizar la identidad del usuario. Se pueden utilizar las preguntas predeterminadas que proporciona Single Sign-on o crear preguntas propias.

Suplantación de la verificación de la identidad

Importante: La administración de claves automática no es tan segura como los otros mecanismos de recuperación de claves, tales como las preguntas de seguridad o la contraseña anterior.
Si desea que Single Sign-on suplante la verificación de identidad y obtenga las claves de cifrado de los usuarios automáticamente, puede especificar la opción Protección de datos secundaria No preguntar a los usuarios; restaurar la protección de datos primaria automáticamente.

Este método, conocido como administración automática de claves, está disponible cuando se instala el módulo de administración de claves y se crea una configuración de usuario con esta opción seleccionada.

Con este método, los usuarios inician sesión en la red y tienen acceso inmediato a las aplicaciones administradas con Single Sign-on. No tienen que responder ninguna pregunta. Cuando cambian su contraseña primaria, el software del plug-in detecta el cambio y recupera las claves de cifrado de los usuarios mediante el Servicio de Single Sign-on.

La recuperación automática de claves brinda acceso más rápido y sencillo a las aplicaciones. Sin embargo, no brinda protección frente a los usuarios no autorizados, pues no hay secretos de usuario que salvaguarden la contraseña de red del usuario. Para intentar evitar este problema, se puede implementar la administración automática de claves combinada con el módulo de autoservicio. Este módulo exige la autenticación con preguntas para que los usuarios confirmen su identidad cuando restablezcan sus contraseñas primarias o desbloqueen sus cuentas de dominio.

Si los usuarios cambian entre métodos de autenticación primaria

En Single Sign-on, los usuarios pueden alternar entre varios métodos de autenticación primaria. Single Sign-on protege las contraseñas del usuario con una copia exclusiva de la clave de seguridad como método de autenticación para desbloquear eficientemente los datos del usuario cada vez que este cambia de método de autenticación, sin necesidad de verificar la identidad.

La opción de seleccionar varios métodos de autenticación primaria está disponible como parte de la página Métodos de protección de datos de la configuración de usuario.

Considere la situación siguiente:

- El supervisor de un centro de comunicaciones inicia una sesión usando sus credenciales primarias (nombre de usuario y contraseña de Windows). El software de Single Sign-on Plug-in está instalado en el equipo y permite que el usuario use las aplicaciones con Single Sign-on (SSO) activado.
- El supervisor usa ocasionalmente una tarjeta inteligente con PIN para iniciar sesiones en un equipo compartido e iniciar otra aplicación publicada con XenApp. Este equipo usa la función de escritorio dinámico para permitir el cambio rápido de cuentas de usuario.

En Password Manager 4.0 y 4.1, este usuario debe verificar su identidad antes de usar las aplicaciones con inicio de sesión unificado cada vez que cambiara su método de autenticación primario. En este caso de uso, el supervisor utilizó dos métodos de autenticación primaria: primero un nombre de usuario y contraseña y, a continuación, una tarjeta inteligente con PIN. En Password Manager 4.0 y 4.1, el cambio del método de autenticación requiere la recuperación de la clave de seguridad y, posiblemente, requiere que el supervisor verifique la identidad.

Los usuarios deben registrar cada nuevo método de autenticación la primera vez que usan o que cambian el método. Sin embargo, los cambios posteriores no necesitan que los usuarios se vuelvan a registrar (es decir, no se requiere la recuperación de claves posteriormente).

Administración de la autenticación con preguntas

Oct 12, 2015

La autenticación con preguntas permite que se brinde autenticación segura a usuarios que cambian su contraseña primaria en circunstancias específicas, cambian su método de autenticación o bloquean sus cuentas.

El uso de preguntas de seguridad y de la autenticación con preguntas aumenta el grado de protección frente a usuarios no autorizados, ya que solicita información que sólo conocen los distintos usuarios. Las preguntas de seguridad que se creen deben solicitar información de carácter privado que sólo el usuario está en condiciones de proporcionar. Por consiguiente, las respuestas deben ser difíciles de adivinar y no ser palabras que puedan encontrarse en un diccionario, lo que las haría vulnerables a los ataques informáticos.

Importante: Si tiene pensado utilizar las funciones de autoservicio de restablecimiento de contraseñas o desbloqueo de cuentas de dominio del módulo de administración de claves de Single Sign-on, debe utilizar el método de autenticación con preguntas para que los usuarios confirmen su identidad cuando desbloqueen sus cuentas de dominio o restablezcan sus contraseñas primarias.

Confirmación de la identidad de los usuarios mediante la autenticación con preguntas

Si va a implementar las funciones de autoservicio de restablecimiento de contraseñas o desbloqueo de cuentas de dominio del módulo de administración de claves de Single Sign-on, use el método de autenticación con preguntas para la verificación de identidad. También puede usar la autenticación con preguntas como una forma de protección de datos secundaria si la autenticación primaria de un usuario cambia.

Dependiendo de los parámetros de configuración de usuario, se puede exigir a los usuarios que verifiquen sus identidades cuando ocurran los siguientes sucesos:

- Los usuarios cambian sus tipos de autenticación; por ejemplo, un usuario puede cambiar entre autenticación con tarjeta inteligente o contraseña.
- Un administrador cambia la contraseña primaria de un usuario.
- Los usuarios restablecen su contraseña primaria con el autoservicio de contraseñas.
- Los usuarios desbloquean sus cuentas de dominio con el autoservicio de contraseñas.
- Los usuarios cambian su contraseña primaria en un dispositivo que no tiene instalado el software del plug-in y luego inician una sesión en uno donde sí está instalado.

Nota: También puede crear una configuración de usuario que no requiera una verificación posterior al cambiar entre tipos de autenticación; consulte

— Si los usuarios cambian entre métodos de autenticación primaria

.

Si está configurado, el software de Single Sign-on Plug-in solicita a los usuarios que contesten las preguntas de seguridad durante el primer uso. Cuando ocurre un suceso que necesita que los usuarios verifiquen su identidad, el software del plug-in inicia el cuestionario. Un cuestionario es una lista preconfigurada de preguntas creadas por el administrador.

Cada pregunta del cuestionario aparece en una página separada. Por ejemplo, si hay cinco preguntas en el cuestionario, los usuarios verán cinco páginas diferentes, una para cada pregunta. Los usuarios deben contestar todas las preguntas correctamente. Según los parámetros que establezca el administrador, será necesaria la coincidencia exacta (incluida la relación de mayúsculas y minúsculas, así como la puntuación) con las respuestas ingresadas al utilizar Single Sign-on por primera vez.

Si las respuestas a las preguntas elegidas son correctas, se confirmará su identidad. Una vez confirmado el usuario, el

software del plug-in vuelve a cifrar las claves mediante la nueva contraseña principal y almacena las credenciales secundarias del usuario.

Consideraciones

- Si decide no configurar las respuestas a las preguntas de seguridad, los usuarios deberán ingresar sus contraseñas principales anteriores cuando cambien la contraseña e intenten iniciar sesiones con la nueva contraseña. Se puede permitir que los usuarios usen el método de verificación de identidad. Esta opción está disponible como parte de la propiedad Protección de datos secundaria de la configuración del usuario.
- Para evitar el bloqueo de usuarios, no combine el método de restablecimiento de contraseñas del autoservicio de cuentas con la opción Pedir al usuario que introduzca su contraseña anterior. Los usuarios que restablezcan su contraseña probablemente no recuerden su contraseña principal anterior y no podrán recuperar sus credenciales secundarias.
- Las preguntas que solicitan varios tipos de información son las más seguras.
- De forma predeterminada, la autenticación con preguntas se asocia a cuatro preguntas de seguridad. Aunque es posible utilizar las predeterminadas, es recomendable agregar nuevas preguntas y grupos de preguntas de seguridad.

Importante: Según los parámetros que establezca el administrador, el uso de mayúsculas y minúsculas, la puntuación y los espacios se tienen en cuenta en la respuesta del usuario y deben coincidir exactamente cuando el usuario responda la pregunta de seguridad seleccionada más adelante.

Flujo de trabajo de la autenticación con preguntas

No olvide crear las preguntas de seguridad y ponerlas a disposición de los usuarios antes de instalar el software del plug-in. Una vez que el usuario haya seleccionado una pregunta, ésta debe permanecer siempre disponible. Si se cambian o eliminan preguntas que están utilizando los usuarios, éstos no podrán utilizarlas para recuperar sus credenciales secundarias, hasta que y a menos que los fuerce a registrarse nuevamente.

1. Cree las preguntas de seguridad y defina la longitud mínima y si se distinguirá entre mayúsculas y minúsculas. Las preguntas pueden presentarse en cualquiera de los idiomas compatibles con Single Sign-on.
2. Si lo desea, puede agrupar las preguntas en grupos de preguntas de seguridad. Se recomienda crear varias preguntas para que los usuarios puedan elegir aquéllas cuyas respuestas les resulte más fácil recordar. De ese modo, podrá definir cuántas preguntas deberán responder los distintos grupos de usuarios.
3. Agregue las preguntas (o las preguntas y los grupos de preguntas) al cuestionario.
4. Elija la pregunta o preguntas (dos) que se usarán para la recuperación de claves. Las preguntas que elija se usarán para cifrar los datos para la recuperación de claves. Los usuarios deberán seguir respondiendo a las preguntas que seleccionaron al registrarse.
5. Si lo desea, puede habilitar el Ocultamiento de las respuestas. Esta función brinda la opción de ocultar las respuestas de los usuarios a las preguntas de autenticación. Si se habilita, las respuestas de los usuarios se protegen durante el registro y la verificación de identidad.
   El ocultamiento de las respuestas sólo está disponible en el software de la consola y del plug-in de Password Manager 4.6 y 4.6 con Service Pack 1 y Single Sign-on 4.8 y 5.0.

Diseño de las preguntas de seguridad: Seguridad y facilidad de uso

Single Sign-on incluye cuatro preguntas predeterminadas que pueden utilizarse para administrar el registro de usuarios. Estas preguntas están disponibles en todos los idiomas compatibles (inglés, francés, alemán, japonés, chino simplificado y español). Citrix recomienda que cada administrador cree sus propias preguntas de seguridad y que éstas se presenten a los usuarios en los idiomas de su sistema operativo.

Para que un usuario no autorizado pueda utilizar la contraseña de otro usuario, deberá responder correctamente todas las preguntas que el usuario autorizado seleccionó y respondió en primer lugar. No obstante, conviene tener en cuenta que si los usuarios tienen que responder demasiadas preguntas, puede resultarles difícil confirmar su identidad.

Las preguntas de seguridad deben solicitar información de carácter privado que sólo el usuario pueda proporcionar. Por consiguiente, las respuestas deben ser difíciles de adivinar y no ser palabras que puedan encontrarse en un diccionario, lo que las haría vulnerables a los ataques informáticos. El grado de seguridad de una pregunta viene dado por la dificultad para averiguar la respuesta que tendría otra persona que no sea el usuario al que va dirigida.

Las buenas preguntas son aquellas con una gran entropía, es decir, preguntas para las cuales:

- El número de respuestas posibles es muy elevado.
- La probabilidad de averiguar la respuesta correcta es muy baja.

Por cuestiones prácticas, es preferible formular preguntas cuya respuesta sea fácil de recordar pero difícil de adivinar. Por ejemplo:

- ¿Cómo se llamaba tu profesor favorito?
- ¿Qué país o ciudad elegirías para unas vacaciones? (ciudad, país)
- ¿Cuál es tu canción favorita y quién es el autor?
- ¿Cuál es tu libro favorito y quién es el autor?
- ¿Cuál es tu obra de arte favorita, quién es el autor y dónde la viste por primera vez?

Hay que tener en cuenta que, en los ejemplos anteriores, si los usuarios comparten un mismo contexto cultural, la probabilidad de adivinar la respuesta puede ser mayor aunque los usuarios no sean conscientes de ello, lo cual podría aumentar los riesgos de seguridad.

No cree preguntas con las siguientes características:

- Preguntas cuya respuesta sea simple y fácil de adivinar, como “¿Cuál es su color favorito?”.
- Preguntas cuya respuesta pueda variar a lo largo del tiempo, o que puedan conocer otras personas, como “¿Cuál es su dirección?”.

Cómo permitir que los usuarios cambien sus respuestas a las preguntas de seguridad

Single Sign-on permite que los usuarios vuelvan a registrar sus respuestas a las preguntas de seguridad en cualquier momento, sin necesidad de que intervenga un administrador.

Si el entorno incluye preguntas de seguridad o funciones de autoservicio de cuentas, los usuarios que registren sus preguntas y respuestas de seguridad podrán usar el software del plug-in para ingresar nuevas respuestas a las preguntas disponibles.

Cuando hayan recibido confirmación de que las respuestas se guardaron en el almacén central, las respuestas anteriores ya no serán válidas.

Los usuarios cambian sus respuestas a las preguntas de seguridad accediendo al Asistente de registro de preguntas de seguridad.

Proporcione a los usuarios acceso al Asistente de registro de preguntas de seguridad como una aplicación publicada:

1. Instale Single Sign-on Plug-in en un servidor XenApp.
2. Busque el archivo QBAEnroll.exe en el servidor XenApp.

3. Publique el archivo QBAEnroll.exe y póngalo a disposición de los usuarios.
4. Informe a los usuarios sobre la forma de acceder al Asistente de registro de preguntas de seguridad y utilizar este asistente.

Nota: Los usuarios que utilizan el Single Sign-on Plug-in versión 4.8 pueden acceder al Asistente de registro de preguntas de seguridad al seleccionar Herramientas > Registro de preguntas de seguridad en el Administrador de inicios de sesión. Estos usuarios no necesitan acceso al Asistente de registro de preguntas de seguridad como una aplicación publicada. Los usuarios que utilizan el Single Sign-on Plug-in de la versión 4.6 Service Pack 1 o versiones anteriores no pueden acceder al Asistente de registro de preguntas de seguridad como una aplicación publicada.

Administración de las preguntas

Oct 12, 2015

El nodo Autenticación con preguntas del componente Single Sign-on de Citrix AppCenter permite que se use una ubicación central para administrar todas las preguntas de seguridad asociadas con la verificación de identidad, el restablecimiento personal de contraseñas y el desbloqueo de cuentas. Puede agregar preguntas de seguridad propias a la lista y crear grupos de preguntas y dirigirlos a usuarios específicos.

- Si modifica las preguntas predeterminadas después de que los usuarios registraron sus respuestas, tenga en cuenta el significado de las preguntas modificadas. Si sólo se modifica una pregunta, no es necesario que los usuarios vuelvan a registrarse, pero si cambia el significado, es posible que los usuarios no la respondan correctamente.
- Si se agregan, eliminan o sustituyen preguntas de seguridad una vez que los usuarios se han registrado, los usuarios que utilicen un grupo de preguntas anterior no podrán autenticarse ni restablecer sus contraseñas hasta que vuelvan a registrarse. Al abrir de nuevo el software del plug-in, los usuarios deberán responder un nuevo conjunto de preguntas.
- Todas las preguntas de seguridad pueden pertenecer a varios grupos. Cuando se crean grupos de preguntas de seguridad, todas las preguntas creadas pueden usarse con a cualquier otro grupo.

Use estos pasos para acceder a la configuración mencionada en los siguientes procedimientos:

1. Haga clic en Inicio > Todos los programas > Citrix > Consolas de administración > Citrix AppCenter.
2. Expanda el nodo Single Sign-on y Verificación de la identidad y, a continuación, seleccione Autenticación con preguntas.
3. En el menú Acción, haga clic en Administrar preguntas.

Para crear nuevas preguntas de seguridad

Puede crear tantas preguntas como desee, establecer distintos idiomas para cada una e indicar varias traducciones para una pregunta en particular. El software del plug-in presenta al usuario un cuestionario en el idioma establecido en la configuración de idioma de su perfil de usuario. Si el idioma no está disponible, Single Sign-on mostrará las preguntas en el idioma predeterminado.

Nota: Cuando se especifica un idioma para una pregunta de seguridad, ésta se muestra a los usuarios cuyo sistema operativo está configurado en ese idioma. Si el idioma del sistema operativo no coincide con el de ninguna de las preguntas disponibles, éstas se mostrarán en el idioma predeterminado.

1. Seleccione Preguntas de seguridad.
2. Seleccione un idioma en la lista Idioma y haga clic en Agregar pregunta. Aparecerá el cuadro de diálogo Pregunta de seguridad.
3. Cree la nueva pregunta en el cuadro de diálogo Preguntas de seguridad.

Importante: El texto traducido de las preguntas sólo puede agregarse mediante el comando Modificar. Si selecciona Agregar pregunta, se creará una nueva pregunta que no estará asociada a la original.

Para configurar el idioma predeterminado

En la mayoría de los casos, los usuarios verán las preguntas en el idioma asociado a su perfil de usuario. Si el idioma no está disponible, Single Sign-on mostrará las preguntas en el idioma predeterminado que especifique.

1. Seleccione Autenticación con preguntas.
2. En la lista Idioma predeterminado, elija uno.

Nota: La opción Compatibilidad con versiones anteriores de este diálogo garantiza que el software del plug-in de Password Manager 4.0 y Password Manager 4.1 pueda continuar mostrando las preguntas de verificación de identidad.

Para agregar o modificar el texto de preguntas existentes

Si se agregan, eliminan o sustituyen preguntas de seguridad una vez que los usuarios se han registrado, los usuarios que utilicen un grupo de preguntas anterior no podrán autenticarse ni restablecer sus contraseñas hasta que vuelvan a registrarse. Al abrir de nuevo el software del plug-in, los usuarios deberán responder un nuevo conjunto de preguntas. Si sólo se modifica una pregunta, no es necesario que los usuarios vuelvan a registrarse, pero si cambia el significado de la pregunta, es posible que los usuarios no la puedan responder correctamente.
Importante: Si va a modificar una pregunta existente, tenga cuidado de no cambiar el significado de la pregunta. Esto podría provocar una discordancia con las respuestas del usuario durante la repetición de la autenticación. Es decir, un usuario podría contestar de forma que no coincida con la respuesta almacenada.

1. Seleccione Preguntas de seguridad.
2. Seleccione un idioma en la lista Idioma.
3. Elija la pregunta y haga clic en Modificar. Aparecerá el cuadro de diálogo Pregunta de seguridad.
4. Edite la pregunta en el cuadro de diálogo Preguntas de seguridad.

Para crear un grupo de preguntas de seguridad

Los administradores pueden crear varias preguntas de seguridad que deberán responder los usuarios para confirmar su identidad. Dichas preguntas se agregarán al cuestionario que responden los usuarios para autenticarse. No obstante, las preguntas también pueden estructurarse en grupos de preguntas de seguridad.

Por ejemplo, la organización de preguntas por grupos permite agregar un grupo de seis preguntas al cuestionario e indicar a los usuarios que deben responder tres de las seis. De este modo, los usuarios tienen más libertad a la hora de elegir las preguntas y respuestas que se utilizan para confirmar su identidad.

1. Seleccione Preguntas de seguridad.
2. Haga clic en Agregar grupo.
3. En el cuadro de diálogo Grupo de preguntas de seguridad, especifique un nombre para el grupo, seleccione las preguntas y luego configure la cantidad de preguntas a las que debe contestar el usuario.

Para modificar un grupo de preguntas de seguridad

1. Seleccione Preguntas de seguridad.
2. Seleccione el grupo de preguntas de seguridad que quiera modificar y haga clic en Modificar. Aparecerá el cuadro de diálogo Grupo de preguntas de seguridad, en el que se muestra una lista de preguntas de seguridad que pueden incluirse en el grupo. En las preguntas que ya forman parte del grupo, la casilla de verificación está seleccionada. Es posible modificar el nombre del grupo, agregar preguntas al mismo o seleccionar cuántas preguntas deberá responder el usuario.

Para seleccionar una o más preguntas para la recuperación de claves

El cifrado de datos para la recuperación de claves requiere que se seleccionen una o dos preguntas de seguridad. Los usuarios deberán responder todas las preguntas que eligieron al registrarse, pero las seleccionadas para el cifrado de datos se usarán para recopilar los datos necesarios para el cifrado y la recuperación de claves.

1. Elija Recuperación de claves.
2. Marque la casilla de verificación que aparece junto a la pregunta o preguntas que se usarán para la recuperación de claves durante la verificación de identidad.
3. Haga clic en Aceptar para guardar la pregunta y los parámetros asociados. Puede aparecer un mensaje preguntándole si desea que los usuarios tengan que volver a inscribir sus preguntas. Haga clic en Sí para confirmar.

Para habilitar el ocultamiento de respuestas

Ocultamiento de respuestas de seguridad está disponible solamente con Password Manager versiones 4.6 y 4.6 con Service Pack 1, y Single Sign-on 4.8 y 5.0.

El ocultamiento de respuestas brinda un nivel de seguridad mayor para los usuarios cuando registran sus repuestas o ingresan las respuestas durante la verificación de identidad. Cuando esta función está habilitada, se ocultan las respuestas de los usuarios que ejecutan Password Manager 4.6, Password Manager 4.6 con Service Pack 1, Single Sign-on 4.8 o Single Sign-on 5.0. Durante el proceso de registro de las respuestas, dichos usuarios deberán ingresar sus respuestas dos veces para evitar errores de tecleado y ortografía. Los usuarios deberán escribir sus respuestas sólo una vez durante la validación de la identidad porque se les pedirá que vuelvan a intentarlo si hay un error.

Nota: Las respuestas a las preguntas de seguridad registradas con el software del Agente de Password Manager 4.5 se pueden ocultar cuando el software se actualiza a Single Sign-on 5.0. Las preguntas de seguridad y las respuestas de los usuarios con el software del agente para Password Manager 4.5, 4.1 o 4.0 permanecerán visibles sin importar el parámetro de la consola.

1. Elija Ocultamiento de respuestas.
2. Elija Ocultar las respuestas a las preguntas de seguridad.

Para crear cuestionarios compatibles con versiones anteriores

El modo de compatibilidad con las versiones anteriores permite que el software del plug-in siga pidiéndole a los usuarios las preguntas de verificación de identidad utilizadas con las versiones 4.0 y 4.1 de Password Manager. El modo de compatibilidad con las versiones anteriores también le permite continuar usando la pregunta predeterminada: "¿Cuál es su frase de verificación de identidad?". Si actualiza desde le versión 4.1, las preguntas de verificación de identidad y las preguntas que utilizó para el autoservicio de restablecimiento de contraseña aparecen como un cuestionario en el cuadro de diálogo Administrar preguntas.

Importante: Cuando cree y edite configuraciones de usuario, no habilite la compatibilidad con versiones anteriores si se trata de una nueva instalación de Single Sign-on porque eso limita las funciones del software del plug-in a las de las versiones 4.0 y 4.1 del producto. Asimismo, no desactive el modo de compatibilidad con versiones anteriores si se está ejecutando el software del agente de las versiones 4.0 y 4.1, dado que eso impedirá que los usuarios lleven a cabo los registros para la recuperación de claves y el restablecimiento de contraseñas.
Si usa la administración automática de claves no habilite el modo de compatibilidad. La recuperación automática de claves no necesita que los usuarios contesten preguntas de verificación de identidad.

Para que los cuestionarios sean compatibles con las versiones 4.0 y 4.1 deben incluir al menos una pregunta de seguridad asociada a la función de restablecimiento de contraseñas del autoservicio de cuentas.

Cada pregunta de seguridad debe incluir uno de los siguientes parámetros:
- No reconocer mayúsculas de minúsculas
- Tamaño mínimo de la respuesta igual a 1
- Las preguntas no pueden habilitarse para la recuperación de claves

Para verificar la compatibilidad con versiones anteriores

Puede comprobar la compatibilidad con versiones anteriores si actualiza desde una versión anterior de Single Sign-on/Password Manager:
1. Seleccione Autenticación con preguntas.
2. Seleccione Verificar compatibilidad con versiones anteriores y haga clic en Aceptar.

Single Sign-on llevará a cabo la verificación de la compatibilidad con versiones anteriores y mostrará los errores en un cuadro

de diálogo.

Cómo permitir que los usuarios administren sus credenciales primarias con el autoservicio de cuentas

Oct 12, 2015

Las funciones de autoservicio de cuentas de Single Sign-on pueden configurarse para que los usuarios puedan restablecer sus contraseñas primarias y desbloquear sus cuentas de dominio de Windows por sí mismos, sin que tenga que intervenir un administrador o el servicio de asistencia técnica. Según las necesidades de la empresa, los servicios de restablecimiento personal de contraseñas y desbloqueo de cuentas pueden implementarse en el entorno de Single Sign-on de forma segura.
Nota: Para implementar el autoservicio de cuentas con la Interfaz Web de Citrix, consulte
— Interfaz Web
.

El módulo de autoservicio está protegido por la autenticación con preguntas, que garantiza que los usuarios autorizados son quienes restablecen sus contraseñas o desbloquean sus cuentas. Durante el primer uso del software de Single Sign-on Plug-in o la primera vez después de que se configura el autoservicio, los usuarios deben registrar sus respuestas a las preguntas de seguridad creadas y seleccionadas durante la configuración de Single Sign-on.

Dichas preguntas de seguridad vuelven a formularse a los usuarios cuando éstos necesitan cambiar la contraseña o desbloquear su cuenta. Si las preguntas se responden correctamente, los usuarios pueden restablecer la contraseña o desbloquear su cuenta sin tener que recurrir al servicio técnico o al administrador.

Importante: Las funciones de autoservicio para restablecimiento de contraseña y desbloqueo de cuentas necesitan que se implemente la autenticación con preguntas. Los usuarios deben registrar las respuestas a las preguntas de seguridad para poder usar estas funciones. Si decide no usar la autenticación con preguntas en el entorno de Single Sign-on, las funciones de autoservicio para restablecimiento de contraseña y desbloqueo de cuentas no estarán disponibles.
Factores a tener en cuenta:

- Las funciones del módulo de autoservicio sólo pueden utilizarse para que los usuarios restablezcan su contraseña primaria (cuenta de dominio) o desbloqueen sus cuentas de dominio de Windows en entornos Active Directory.
- Cuando un usuario cambia su contraseña de aplicación con el software de Single Sign-on Plug-in o su contraseña primaria mediante la combinación de las teclas Ctrl+Alt+Supr en un dispositivo en el que está instalado el software del plug-in, Single Sign-on detecta automáticamente el cambio.
- Para evitar el bloqueo de usuarios, no combine el método de autoservicio de restablecimiento de contraseñas con la opción Pedir al usuario que introduzca su contraseña anterior para confirmar las identidades de los usuarios de manera exclusiva. Si sólo se utiliza el método de contraseña anterior, los usuarios que no recuerden su contraseña principal anterior no podrán acceder al sistema, sus datos de usuario se restablecerán o borrarán en el almacén central y en todos los dispositivos de usuario donde estén almacenados, y deberán volver a introducir sus credenciales para todas las aplicaciones.

Resumen de las tareas de implementación del autoservicio

Para usar el la función de autoservicio de cuentas, haga lo siguiente:

1. Instale el Módulo de autoservicio y el Módulo de administración de claves.
2. Configuración de la autenticación con preguntas.
3. Creación de una configuración de usuario con una o más de las funciones de restablecimiento de contraseñas o desbloqueo de cuentas habilitadas.
4. Instalación y configuración del software del plug-in.

Use de la administración de claves automática con el autoservicio

La combinación de la administración de claves con el autoservicio brinda mayor facilidad de uso para los usuarios que necesitan acceder a aplicaciones protegidas con contraseñas administradas con el Single Sign-on Plug-in. Por ejemplo, si los usuarios restablecen sus contraseñas primarias, no necesitan contestar las preguntas de seguridad. Sin embargo, deben hacerlo durante el proceso de restablecimiento de contraseñas.

Con la administración de claves, los usuarios no necesitan verificar sus identidades después de desbloquear las cuentas o restablecer las contraseñas.

Para restablecer el registro de los usuarios en el autoservicio

Si los usuarios quedan bloqueados de sus cuentas de Windows y no pueden recordar las respuestas a sus preguntas de seguridad, deberá usar el componente Single Sign-on de Citrix AppCenter para restablecer el registro de autoservicio para los usuarios. Una vez realizada la operación, el asistente para el registro en el autoservicio aparecerá la próxima vez que el usuario abra el software del plug-in. Los usuarios deberán volver a registrar las respuestas a las preguntas de seguridad.

1. Haga clic en Inicio > Todos los programas > Citrix > Consolas de administración > Citrix AppCenter.
2. Expanda el nodo Single Sign-on, expanda el nodo Verificación de la identidad y seleccione Autenticación con preguntas.
3. En el menú Acción, haga clic en Otras tareas > Revocar el registro de preguntas de seguridad del usuario.
4. En el cuadro de diálogo Seleccionar usuario, escriba el nombre de usuario o el grupo de usuarios.

Experiencia de usuario

Después de instalar y configurar el software del servicio y del plug-in, el Módulo de autoservicio modifica el cuadro de diálogo de inicio de sesión de Windows del usuario y el cuadro Desbloquear equipo, o la ventana de bienvenida de Windows Vista. Usuarios de Windows 7, Windows Server 2008 y Windows Server 2008 R2, (disponible cuando los usuarios bloquean sus equipos con la combinación de teclas CTRL-ALT-SUPR) al incluir el botón Autoservicio de cuentas.

Antes de que los usuarios puedan acceder a las funciones del autoservicio, deben iniciar una sesión con su cuenta de dominio primaria y registrar las respuestas a las preguntas de seguridad. Una vez que se hayan inscripto podrán usar las funciones de autoservicio para restablecimiento de contraseña y desbloqueo de cuentas.

Con la administración de claves, los usuarios no necesitan verificar sus identidades después de desbloquear las cuentas o restablecer las contraseñas.

Autoservicio de cuentas

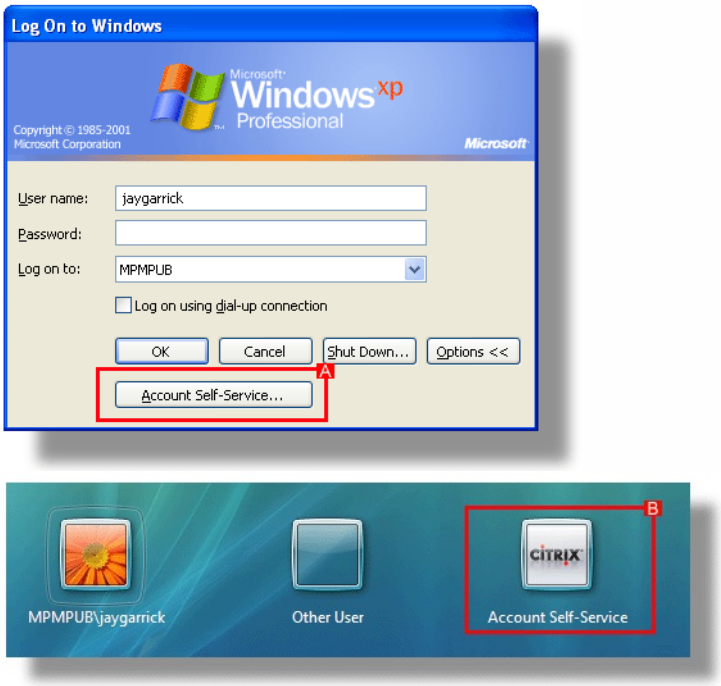
Oct 12, 2015

Los usuarios de Single Sign-on tienen la opción de instalar las funciones de autoservicio de cuentas (Restablecimiento de contraseñas y Desbloqueo de cuentas) sin ninguna otra función de Single Sign-on para los usuarios.

Las funciones del autoservicio de cuentas de Single Sign-on ayudan a reducir las llamadas al servicio de asistencia técnica de la empresa ya que permiten que los empleados lleven a cabo las siguientes tareas por sí mismos:

- Cambio de la contraseña de dominio de Microsoft Windows
- Desbloqueo de las cuentas de dominio de Windows

Las funciones de autoservicio de cuentas permiten configurar un grupo de preguntas de seguridad para verificar la identidad de los usuarios. Una vez que se habilita la autenticación con preguntas y las funciones de autoservicio de cuentas se ponen a disposición de los usuarios, estos pueden registrarse con el servicio contestando una serie de preguntas de seguridad. Una vez registrados, los usuarios pueden hacer clic en Autoservicio de cuentas (A), que se encuentra en el cuadro de diálogo Inicio de sesión de Windows o, en el caso de Microsoft Windows Vista, en la pantalla de Bienvenida (B).



Los administradores pueden hacer que los usuarios vuelvan a registrarse de las siguientes formas:

- Revocando los datos de preguntas de un usuario en particular
- Pidiendo a todos los usuarios que vuelvan a registrarse
- Cambiando el cuestionario existente

Los usuarios registrados también pueden iniciar el proceso para volver a registrarse, cuando quieran cambiar las respuestas a las preguntas de seguridad.

Este documento describe la forma de instalar y configurar Single Sign-on para otorgar a los usuarios solo las funciones de autoservicio de cuentas.

Nota: El autoservicio de cuentas no respalda los inicios de sesión con nombre de usuario principal (UPN), como nombreusuario@dominio.com.

Uso de licencias

Cuando los usuarios presentan nuevas respuestas para la autenticación con preguntas, se consume una licencia de Single Sign-on durante el proceso de reinscripción. El uso de licencias de usuario concurrente (o simultáneo) asegura la máxima disponibilidad de licencias dentro de la organización. Las licencias de usuario concurrente se devuelven a la agrupación de licencias después de que los usuarios completan el proceso de reinscripción. En esa misma situación, una licencia de usuario definido permanece con el usuario, aunque no esté siendo utilizada, por un mínimo de dos días.

Se usan unos índices para ofrecer un mayor número de licencias para Autoservicio de cuentas exclusivamente por cada licencia de Single Sign-on. Las licencias de usuario concurrente usan un índice de 10:1, donde 100 licencias de usuario concurrente se traducen en 1.000 licencias para Autoservicio de cuentas. Las licencias de usuario definido usan un índice de 5:1, es decir que 100 licencias de este tipo se traducen en 500 licencias para Autoservicio de cuentas.

Para permitir el uso sin conexión de licencias de usuarios concurrentes

1. Cree una configuración de usuario.
2. En la página Configurar las licencias del Asistente de configuración de usuarios, seleccione Licencias de usuarios concurrentes (sólo en Enterprise y Platinum Edition).
3. Seleccione Permitir consumo de licencia para uso desconectado y configure el período de tiempo que la licencia puede estar extraída del servidor de licencias.
4. Finalice el ajuste de la configuración de usuario.

Para los usuarios asociados a esta configuración de usuario, el modelo de licencia es el mismo que una licencia de usuario definido: la pueden utilizar los usuarios que trabajen ocasionalmente de forma remota y estén sin conexión durante largos períodos. Las licencias de usuarios concurrentes se consumen por usuario.

Importante: Las instancias de Single Sign-on Plug-in instaladas localmente no necesitan una licencia independiente para los usuarios que cuentan con acceso a las aplicaciones alojadas en entornos Citrix XenApp, Platinum Edition.

Creación de una configuración de usuario con Autoservicio de cuentas únicamente

Siga estos pasos para crear una configuración de usuario que proporcione la funcionalidad de Autoservicio de cuentas sin necesidad de habilitar el componente de inicio de sesión único (Single Sign-on).

Nota: Las definiciones de aplicación no se incluyen en esta configuración de usuario debido a que no incluyen el componente Single Sign-on. Si los usuarios requieren la funcionalidad completa del componente Single Sign-on, colóquelos en una configuración de usuario que no incluya las modificaciones Autoservicio de cuentas exclusivamente.

1. Haga clic en Inicio > Todos los programas > Citrix > Consolas de administración y seleccione Citrix AppCenter.
2. Para iniciar el asistente, expanda el nodo Single Sign-on y haga clic en Configuraciones de usuario. En el área Acciones, haga clic en Agregar configuración de usuario nueva para abrir el Asistente de configuración de usuarios.
3. En la página Nombre de la configuración de usuario:
    1. En el campo Nombre, escriba el nombre de la configuración de usuario.
    2. En el área Asociación de la configuración de usuario, elija cómo se asociará la configuración de usuario a los usuarios, mediante la identificación de la jerarquía de Active Directory (unidad organizativa o usuario) o el grupo Active Directory.
4. En la página Seleccionar la edición del producto, seleccione Single Sign-On Enterprise.
5. En la página Elegir aplicaciones, haga clic en Siguiente.
6. En la página Configurar la interacción con el plug-in, deje sin marcar las casillas siguientes:

- Detectar automáticamente las aplicaciones y pedirle al usuario que almacene las credenciales
- Procesar automáticamente formularios definidos detectados por Single Sign-on Plug-in

Haga clic en Configuración avanzada.

7. En Parámetros avanzados de Single Sign-on Plug-in:
   - Seleccione Respaldo de aplicaciones y quite la marca de la casilla Detectar definiciones de aplicación del cliente.

   Haga clic en Aceptar para cerrar Configuración avanzada y haga clic en Siguiente.
8. En la página Configurar las licencias, del área Dirección del servidor de licencias, introduzca el nombre del servidor de licencias y el número de puerto correspondiente.
   En el área Modelo de licencia seleccione Licencias de usuario definidos o Licencias de usuarios concurrentes.

   Nota: El uso de licencias de usuario concurrente (o simultáneo) asegura la máxima disponibilidad de licencias dentro de la organización. Las licencias de usuario concurrente se devuelven a la agrupación de licencias cuando los usuarios completan el proceso de reinscripción. En esa misma situación, una licencia de usuario definido permanece con el usuario, aunque no esté siendo utilizada, por un mínimo de dos días.
9. En la página Seleccionar los métodos de protección de datos, proporcione información según se requiera.
10. En la página Seleccione las opciones de protección de datos secundaria, seleccione Pedir al usuario que elija el método: Contraseña anterior o preguntas de seguridad.
11. En la página Habilitar las funciones de autoservicio, seleccione una de las opciones siguientes, o ambas:
    - Permitir que los usuarios restablezcan sus contraseñas primarias
    - Permitir que los usuarios desbloqueen sus cuentas
12. En la página Ubicar los módulos del servicio > Módulo de administración de claves, proporcione la dirección del servicio.
13. Complete el asistente sin cambios adicionales.

Preparación del equipo que ejecutará el software del plug-in

Nota: Considere la posibilidad de automatizar los procedimientos siguientes mediante el uso de scripts para aumentar la eficacia y mejorar la precisión.
Después de instalar el software de Single Sign-on Plug-in en los equipos de los usuarios, debe modificar el acceso directo a ssoShell.exe y el menú Inicio para proporcionar acceso de usuario a las funciones de Autoservicio de cuentas solamente.

Durante la instalación básica del software de Single Sign-on Plug-in, el acceso directo a ssoShell.exe contiene el siguiente conmutador de línea de comandos:

/background

Cambie el conmutador a:

/qbaenroll /noforceqbaenroll

Este cambio hace que el software de Single Sign-on Plug-in en el equipo del usuario se sincronice con el almacén central cuando el usuario inicia la sesión y determine el estado del registro de la autenticación del usuario con preguntas. Si el proceso de registro ha finalizado y está actualizado, no se solicitará al usuario que se registre. Se solicitará al usuario que se registre si se detecta una de las condiciones siguientes durante la sincronización:

- El usuario no completó el proceso de registro de la autenticación con preguntas.
- El administrador reinicializó la preguntas de la autenticación con preguntas del usuario.
- El administrador modificó las preguntas de la autenticación con preguntas del usuario.

Después de completar la sincronización y, si es necesario, de iniciar el proceso de registro, ssoShell se cierra

automáticamente.

Para actualizar el acceso directo de ssoShell.exe de Single Sign-on

Para una instalación de escritorio:

1. Equipos con Windows Vista: En el Explorador de Windows, vaya a %SystemDrive%\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup.
   Equipos sin Windows Vista: En el Explorador de Windows, vaya a %SystemDrive%\Documents and Settings\Todos los usuarios\Menú Inicio\Programas\Inicio.
2. En la carpeta Inicio, seleccione el proceso de segundo plano Single Sign-on y luego seleccione Archivo > Propiedades.
3. En el cuadro de diálogo de las Propiedades del proceso de segundo plano Single Sign-On, haga clic en el campo Destino, desplácese hasta el final del texto y elimine /background.
4. En el campo Destino, a continuación del texto, escriba /qbaenroll /noforceqbaenroll.

Para una instalación de servidor:
Precaución: Si edita el Registro de forma incorrecta podrían generarse problemas graves que pueden obligar a instalar nuevamente el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Asegúrese de hacer una copia de seguridad del registro antes de modificarlo.

1. Abra el Registro y vaya a HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\windows NT\CurrentVersion\Winlogon\AppSetup.
2. En la subclave, haga doble clic en la entrada predeterminada para abrir el cuadro de diálogo Editar cadena.
3. En el campo Datos de valor:
   cambie %SystemDrive%\Citrix\Metaframe Password Manager\WTS\SSOlauncher.exe /no ssoshutdown

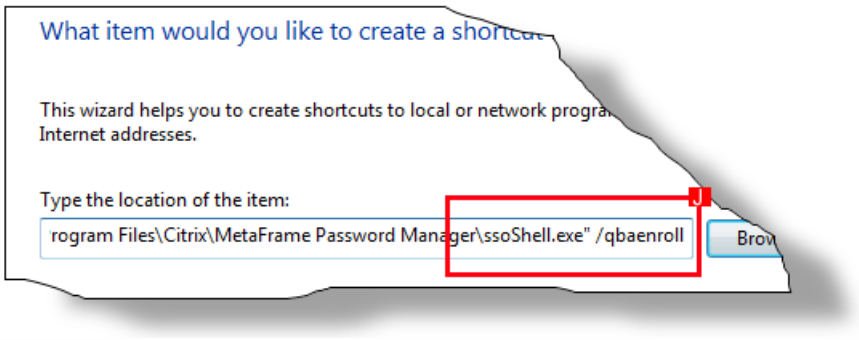
   por: %SystemDrive%\Citrix\Metaframe Password Manager\ssoshell.exe /qbaenroll /noforceqbaenroll.

El archivo ssoShell.exe se modifica para el elemento Autoservicio de cuentas solamente.

Para agregar un acceso directo de registro de autoservicio al menú Inicio

Agregue un acceso directo al menú Inicio para permitir que los usuarios inicien el proceso de inscripción personalmente. Esto ayuda a eliminar las llamadas al servicio técnico en caso de que los usuarios no proporcionen respuestas durante los inicios de sesión iniciales, o bien, deseen cambiar algunas de las respuestas suministradas.

1. Equipos con Windows Vista: En el Explorador de Windows, vaya a %SystemDrive%\ProgramData\Microsoft\Windows\Start Menu\Programs\Citrix\.
   Equipos sin Windows Vista: En el Explorador de Windows, vaya a %SystemDrive%\Documents and Settings\Todos los usuarios\Menú Inicio\Programas\Citrix\.
2. En el menú Archivo, seleccione Nuevo > Acceso directo. Se abre el asistente Crear acceso directo.
3. Haga clic en Examinar.
4. Vaya a %InstallationDirectory%\Archivos de programa\Citrix\Metaframe Password Manager\, seleccione ssoShell.exe y después haga clic en Aceptar. El cuadro de diálogo Buscar carpeta se cierra y se muestra la ruta a ssoShell.exe en el campo Escriba la ubicación del elemento.
5. En el campo Escriba la ubicación del elemento, coloque el punto de inserción después de ssoShell.exe y escriba un espacio seguido de /qbaenroll (J).



6. Haga clic en Siguiente.
7. Escriba Registro de autoservicio de cuentas de Citrix A continuación, haga clic en Frinalizar.

El acceso directo se muestra en Inicio > Todos los programas > Citrix.

Para eliminar el acceso directo de Single Sign-on

Durante la instalación del software de Single Sign-on Plug-in se coloca un acceso directo en el menú Inicio. Si un usuario que se ha configurado para usar solamente las funciones del Autoservicio de cuentas selecciona este comando, se ejecutará ssoShell.exe y, a menos que existan cambios en la autenticación con preguntas del usuario, se volverá a cerrar. Este comportamiento puede confundir a los usuarios y generar llamadas al servicio técnico. Para evitar este problema, quite el acceso directo del menú Inicio.

1. Equipos con Windows Vista: En el Explorador de Windows, vaya a %SystemDrive%\ProgramData\Microsoft\Windows\Start Menu\Programs\Citrix\.
   Equipos sin Windows Vista: En el Explorador de Windows, vaya a %SystemDrive%\Documents and Settings\Todos los usuarios\Menú Inicio\Programas\Citrix\.
2. Elimine el acceso directo de Single Sign-on.

El acceso directo de Single Sign-on se elimina del menú Inicio.

Para quitar el acceso directo de Single Sign-on Plug-in de la carpeta Inicio

Quite el acceso directo de Single Sign-on Plug-in del dispositivo de usuario para evitar que el software del plug-in se inicie cada vez que el usuario inicie sesión en el equipo. Esta tarea evita que el usuario consuma una licencia sin necesidad.

1. Mediante el Explorador de Windows, vaya a %SystemDrive%\Documents and Settings\Todos los usuarios\Menú Inicio\Programas\Inicio.
2. En la carpeta Inicio, elimine el Proceso en segundo plano de Single Sign-on Plug-in.
   Nota: Si el software del plug-in ya está instalado en Citrix Presentation Server o en un entorno de Servicios de Terminal Server, la subclave de Registro AppSetup, que se encuentra en HKLM\SOFTWARE\microsoft\Windows NT\CurrentVersion\Winlogon\AppSetup, se debe modificar para quitar la referencia a Password Manager o Single Sign-on.

El acceso directo al Single Sign-on Plug-in dejará de iniciarse automáticamente cuando el usuario inicia la sesión.

Uso del aprovisionamiento para automatizar el ingreso de credenciales

Oct 12, 2015

Use el Módulo de aprovisionamiento (también conocido como aprovisionamiento de credenciales) para manipular las credenciales de usuario asociadas con las aplicaciones definidas en una configuración de usuario. El aprovisionamiento permite que se automaticen estos procedimientos y se los aplique a varios usuarios. Si se va distribuir nuevo software a los usuarios, basta con crear una definición de aplicación para el mismo y utilizar el aprovisionamiento de credenciales para todos los usuarios que vayan a usar la aplicación.

Resumen de las tareas de aprovisionamiento

Para manipular la información de credenciales del almacén central para aplicaciones con inicio de sesión unificado habilitado contenidas en configuraciones de usuario, es necesario llevar a cabo las siguientes tareas:

1. Instalar el módulo de aprovisionamiento de Single Sign-On Service.
2. Crear una configuración de usuario que use el servicio de aprovisionamiento.
3. Generar una plantilla de aprovisionamiento.
4. Completar la plantilla con datos de credenciales de usuarios y seleccionar un comando a ejecutar.
5. Procesar los datos de aprovisionamiento.

Importante: El archivo XML de aprovisionamiento de credenciales contiene información confidencial sobre los usuarios. Tenga en cuenta eliminar el archivo o moverlo a una ubicación segura cuando haya finalizado con el aprovisionamiento de credenciales.
Una vez que se han agregado, eliminado o modificado las credenciales en el almacén central, estarán listas para usarse en el entorno. Cuando los usuarios inicien el software del plug-in, las credenciales actualizadas en el software del plug-in están a disposición de los usuarios.

Al agregar, quitar o modificar credenciales en el almacén central se puede consumir un número elevado de recursos del sistema. Cuando sea posible, lleve a cabo el aprovisionamiento durante las horas de menor uso.

SDK de aprovisionamiento de credenciales

Si necesita trabajar con las credenciales de muchos usuarios, considere la posibilidad de usar el kit de desarrollo de software (SDK) de aprovisionamiento de credenciales. El SDK brinda una descripción de las API disponibles al instalar el módulo de aprovisionamiento de Single Sign-On Service. Con este SDK y el código de muestra incluido pueden crearse clientes de aprovisionamiento personalizados para usar con Single Sign-on.

Generación de una plantilla de aprovisionamiento

Para el siguiente procedimiento se asume que se creó una configuración de usuario que consiste en al menos uno de los siguientes elementos: definición de aplicación, grupo de aplicaciones, directiva de contraseñas (que puede incluir un grupo de contraseñas compartidas) y que el aprovisionamiento está habilitado en la configuración de usuario.

Una plantilla de aprovisionamiento en un documento XML que contiene información sobre las aplicaciones que se incluyen en la configuración de usuario:

- Grupo de aplicaciones

- Nombre de definición de aplicación y número de identificación único (GUID)
- Información de usuario, como nombre de usuario y contraseña

También incluye comandos de adición, eliminación y modificación que pueden importarse cuando se importa la plantilla modificada desde la consola para ejecutar el aprovisionamiento.

La plantilla resultante incluye un ejemplo de información específica y de comandos sobre la configuración de usuario seleccionada.

Para generar una plantilla de aprovisionamiento

1. Haga clic en Inicio > Todos los programas > Citrix > Consolas de administración > Citrix AppCenter.
2. Expanda el nodo Single Sign-On y seleccione Configuraciones de usuario.
3. Seleccione una configuración de usuario.
4. En el menú Acción, haga clic en Generar plantilla de aprovisionamiento.
5. En el cuadro de diálogo Generar plantilla de aprovisionamiento, escriba un nombre para la plantilla.

Para procesar la plantilla de aprovisionamiento

Use el componente Single Sign-on de Citrix AppCenter para llevar a cabo las tareas de aprovisionamiento especificadas en el archivo XML. Single Sign-on valida la sintaxis de cada comando, ejecuta los comandos y agrega o modifica los datos del almacén central.

Precaución: No cierre la pantalla de aprovisionamiento hasta que el proceso finalice o se detenga. De lo contrario, no podrá procesarse la información ni detenerse el proceso. Si la pantalla está cerrada mientras se ejecuta el proceso de presentación, no hay modo de capturar la información o de detener el proceso antes de que se complete.

1. Haga clic en Inicio > Todos los programas > Citrix > Consolas de administración > Citrix AppCenter.
2. Expanda el nodo Single Sign-On y expanda Configuraciones de usuario.
3. Elija una configuración de usuario o un grupo de aplicaciones de una configuración de usuario.
4. En el menú Acción, haga clic en Ejecutar el aprovisionamiento. Aparece el Asistente de aprovisionamiento.
5. Haga clic en Siguiente.
6. Escriba el nombre del archivo de aprovisionamiento o haga clic en Examinar para ubicarlo y luego haga clic en Siguiente. Single Sign-on valida el archivo XML.
   - Si no se detectan errores de sintaxis, se mostrará un resumen de los cambios que pueden realizarse. Se puede guardar el resumen.
   - Si hay errores de sintaxis o de otro tipo, se mostrará un archivo de registro de errores. Guárdelo si lo desea y haga clic en Cancelar para cerrar el asistente.
7. Si no se encuentran errores, haga clic en Siguiente para ejecutar los comandos del archivo. En cuanto se modifica la información en el almacén central, se muestran los errores derivados del aprovisionamiento (si los hay). Para detener el proceso de aprovisionamiento, haga clic en Anular. El proceso se detendrá cuando Single Sign-on llegue al final de la sección de datos que está procesando (de forma predeterminada, los datos se procesan en grupos de 50 líneas de código).

Cuando haya finalizado el asistente, puede guardar los resultados de aprovisionamiento.

Ajuste del proceso de aprovisionamiento de credenciales

Precaución: Para realizar este procedimiento es necesario hacer modificaciones en el Registro del sistema. La utilización inadecuada del Editor del Registro puede causar problemas graves que obliguen a volver instalar el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del registro puedan resolverse. Si

utiliza el Editor del Registro, será bajo su propia responsabilidad. Siempre se debe realizar una copia de seguridad del Registro del sistema antes de continuar

De forma predeterminada, si se utiliza Single Sign-on para el aprovisionamiento de credenciales, la información se procesa en lotes de 50 comandos con un tiempo de espera de 100.000 milésimas de segundo. Para cambiar los valores predeterminados, pueden modificarse las siguientes claves de Registro:

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\MetaFrame Password Manager\Console\Provisioning\BatchSize

Tipo: DWORD

Valor predeterminado si se deja en blanco: 50

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\MetaFrame Password Manager\Console\Provisioning\ServiceTimeout

Tipo: DWORD

Valor predeterminado (en milésimas de segundo) si se deja en blanco: 100000

Modificación de la plantilla de aprovisionamiento

Jul 19, 2016

Use un editor de texto o un editor de archivos XML para modificar la plantilla. La plantilla de aprovisionamiento usa lenguaje SPML (Service Provisioning Markup Language), que es un estándar basado en XML para el intercambio de datos. Como en el caso de XML, asegúrese de que cada etiqueta o elemento SPML (por ejemplo, la etiqueta) tenga el formato correcto y cumpla con las reglas de sintaxis de XML. Por ejemplo, al eliminar caracteres de comentario como !-- y --, asegúrese de eliminar los caracteres < y > sobrantes, de otro modo se producirán errores durante el procesamiento de la plantilla de aprovisionamiento. Para obtener información detallada sobre XML, consulte el sitio Web de W3C en http://www.w3.org/. Asegúrese de eliminar los caracteres de comentario (!-- y --) cuando sea necesario.

Ejemplo de resultado

La plantilla generada incluye lo siguiente:

- contiene información sobre el usuario que generó la plantilla
- El comando para el nombre de aplicación en la configuración de usuario
- El comando con el nombre de definición de aplicación

Cerca del final del archivo XML se encuentra la información específica sobre la configuración de usuario seleccionada, que se puede copiar y usar en la plantilla. Por ejemplo:

Por ejemplo, se puede copiar la información de usuario entre las etiquetas y , quitar el comentario y modificarla para cada usuario cuyas credenciales se quieren agregar.

Nota: En el ejemplo anterior, es el dominio y el nombre de usuario del usuario que generó la plantilla. Esta información se puede ocultar con un comentario o eliminar si no se la quiere guardar en la plantilla.

La etiqueta

Tenga en cuenta que se deben incluir las etiquetas y comandos dentro de la etiqueta de aprovisionamiento (que se encuentra cerca de la línea 70 del archivo XML):

```
version="1.0" xmlns="http://citrix.com/Provision/Import">

inserte la etiqueta y los comandos aquí
```

La etiqueta

Use la etiqueta para agregar información de dominio y nombre de usuario para cada usuario cuyas credenciales de aplicación desea aprovisionar. Se debe ingresar una etiqueta para cada usuario que se desea aprovisionar. Cada etiqueta también contendrá los comandos para ejecutar en la cuenta de usuario.

La sintaxis del comando es la siguiente:

```
 suDominio\IdDeUsuario"> <comando>
```

donde:

suDominio	Indica el nombre de dominio del usuario que se agregará.
IdDeUsuario	Indica el nombre de usuario del usuario que se agregará.
comando	Indica uno o más comandos que se pueden ejecutar en el usuario: • • • • • •

El comando

El comando permite agregar el nombre de usuario y la contraseña necesarios para las aplicaciones que se incluyen en la configuración de usuario.

La sintaxis del comando es la siguiente:

```
 %APPNAME%">%APPGUID% longDescription%CREDENTIALNAME% longDescription %APPNAME% hidden description userid password %LABELTEXT%">custom-field1  %LABELTEXT%">custo
```

donde:

	Requerido. El elemento y sus atributos normalmente se generan automáticamente cuando se genera una plantilla. El atributo name= es optativo. • %APPNAME% es el nombre de la definición de aplicación en la configuración de usuario seleccionada. • %APPGUID% es la GUID de la aplicación y debe coincidir
	Requerido. El elemento y sus atributos generalmente se generan automáticamente. • %CREDENTIALNAME% es el nombre de la aplicación en la definición de aplicación.
	Opcional. Escriba el texto que describe la configuración de usuario.
	Opcional. Se puede escribir cualquier texto.

	Requerido. userid es el nombre de usuario que se agregará.
	Requerido. password es la contraseña del usuario que se agregará.
	Se requiere si es necesario otro campo para la autenticación (por ejemplo, para un campo donde el usuario debe ingresar el dominio). Se puede usar tantos campos personalizados como sea necesario.

El comando

El comando permite modificar el nombre de usuario y la contraseña necesarios para las aplicaciones que se incluyen en la configuración de usuario.

Importante: Este comando necesita las credenciales de usuario. Las credencial de usuario se pueden obtener usando el comando antes del comando .
Incluye sólo aquellos elementos que se quieren modificar:

- Para dejar un valor sin modificar, elimine la línea. Por ejemplo, elimine el elemento para dejar el nombre de aplicación sin modificar.
- Para cambiar el valor, especifique el valor en la plantilla. Por ejemplo, incluya el elemento para especificar un nuevo nombre de aplicación.
- Los valores se eliminan incluyendo el elemento sin un valor. Por ejemplo, use para eliminar la descripción actual.

La sintaxis del comando es la siguiente:

%CREDENTIAL-ID% %CREDENTIALNAME% longDescription %APPNAME% hidden description userid password %LABELTEXT%"> custom-field1 %LABELTEXT%">custom-field2
donde:

	Requerido. El valor de la GUID de la credencial %CREDENTIAL-ID% del usuario debe coincidir con el valor devuelto por el comando .
	Opcional. El elemento y sus atributos generalmente se generan automáticamente. • %CREDENTIALNAME% es el nombre de la aplicación en la definición de aplicación.
	Opcional. Escriba el texto que describe la configuración de usuario.
	Opcional. Se puede escribir cualquier texto.
	Requerido. userid es el nombre de usuario que se modifica.
	Requerido. password es la contraseña del usuario que se modifica.
	Se requiere si es necesario otro campo para la autenticación (por ejemplo, para un campo donde el usuario debe ingresar el dominio). Se puede usar tantos campos personalizados como sea necesario.

El comando

El comando permite eliminar las credenciales de un usuario para una aplicación específica basada en SSO.

Importante: Este comando necesita las credenciales de usuario. Las credencial de usuario se pueden obtener usando el comando antes del comando .
La sintaxis del comando es la siguiente:

suDominio\IdDeUsuario"> %CREDENTIAL-ID%
donde:

suDominio	Indica el nombre de dominio del usuario.
IdDeUsuario	Indica el nombre de usuario.
	Requerido. El valor de la GUID de la credencial %CREDENTIAL-ID% del usuario debe coincidir con el valor devuelto por el comando .

El comando

El comando permite eliminar los datos de usuario y la información del almacén central. Use este comando cuando un usuario deje la empresa permanentemente. El almacén de credenciales local del dispositivo del usuario permanece intacto hasta que lo elimina un administrador u operador de forma explícita.

La sintaxis del comando es la siguiente:

suDominio\IdDeUsuario">
donde:

suDominio	Indica el nombre de dominio del usuario.
IdDeUsuario	Indica el nombre de usuario.

Nota: Este comando es similar a la tarea Eliminar los datos de usuario del almacén central de Single Sign-on que se ejecuta en Citrix AppCenter.

El comando

El comando permite restablecer la información del usuario en el almacén central, lo que da como resultado que el usuario seleccionado vuelva al estado inicial. En el caso de los almacenes centrales

que no son Active Directory, se mantienen las carpetas del usuario, pero los datos del usuario (credenciales, preguntas y respuestas, etc.) se eliminan. En los almacenes centrales Active Directory, los datos de usuario se eliminan y el usuario se marca como que tiene los datos restablecidos.

La sintaxis del comando es la siguiente:

suDominio\IdDeUsuario">
donde:

suDominio	Indica el nombre de dominio del usuario.
IdDeUsuario	Indica el nombre de usuario.

Nota: Este comando es similar a la tarea Restablecer los datos del usuario de Single Sign-on que se ejecuta en Citrix AppCenter.

El comando

El comando permite que se obtengan las credenciales específicas de usuario para cada aplicación asociada con una configuración de usuario. Los comandos y necesitan que se use la GUID de credencial como valor para el parámetro %CREDENTIAL-ID%.

El número de identificador que obtiene este comando es la GUID de la credencial, por ejemplo, 634EE015-10C2-4ed2-80F5-75CCA9AA5C11.

La sintaxis del comando es la siguiente:

suDominio\IdDeUsuario">
donde:

suDominio	Indica el nombre de dominio del usuario.
IdDeUsuario	Indica el nombre de usuario.

Escritorio dinámico: entorno de escritorio compartido para los usuarios

Oct 12, 2015

Escritorio dinámico combina la rapidez de los cambios de usuario con la seguridad que ofrece Single Sign-on. La función Escritorio dinámico no se instala de forma predeterminada; se puede seleccionar durante el proceso inicial de instalación de Single Sign-on Plug-in. También pueden actualizarse las instalaciones existentes de Single Sign-on Plug-in para incorporarla. No obstante, para implementar Escritorio dinámico debe configurarlo según los requisitos del entorno y de la empresa.

La función de Escritorio dinámico sólo se admite en:

- Microsoft Windows XP Professional, Service Pack 2, 32 bits
- Microsoft Windows XP Embedded

Escritorio dinámico no es compatible con sistemas operativos de servidor ni con sistemas operativos de 64 bits.

Escritorio dinámico no está disponible cuando Single Sign-on se distribuye mediante Citrix Receiver Updater.

La función Escritorio dinámico de Single Sign-on permite a los usuarios compartir estaciones de trabajo de forma segura y eficaz. Escritorio dinámico amplía el entorno de Windows estándar al permitir al usuario:

- Autenticarse rápidamente en Windows mediante el cuadro de diálogo de inicio de sesión interactivo GINA estándar.
- Ejecutar aplicaciones activadas para Single Sign-on en el entorno de usuario interactivo mediante las credenciales de Single Sign-on del usuario.
- Cerrar la sesión de la estación de trabajo de Escritorio dinámico de modo que otros usuarios puedan ejecutar aplicaciones.

Resumen de las tareas de Escritorio dinámico

Antes de poder implementar Escritorio dinámico, debe realizar lo siguiente:

- Crear una cuenta compartida de Escritorio dinámico
- Crear configuraciones de usuario con parámetros específicos relacionados con Escritorio dinámico para controlar la interacción del usuario de Escritorio dinámico
- Definir el comportamiento de inicio y cierre de Escritorio dinámico:
  - Decidir las aplicaciones que se ejecutan al inicio y las aplicaciones que utilizan las credenciales y los permisos de usuario o de cuenta compartida de Escritorio dinámico.
  - Decidir las aplicaciones que son persistentes y se ejecutan aunque los usuarios cierren la sesión (para el cambio rápido de usuario) y las aplicaciones que terminan cuando los usuarios cierran la sesión, incluidos los scripts de limpieza opcionales o las aplicaciones que eliminan información de usuario de una sesión a otra.

Realice las siguientes tareas para configurar y activar Escritorio dinámico:

1. Crear una cuenta compartida de Escritorio dinámico que esté disponible para cada estación de trabajo o dispositivo cliente que ejecute Escritorio dinámico.
2. Decidir la aplicación habilitada para el inicio de sesión unificado que se debe ejecutar en el entorno de Escritorio dinámico.
3. Decidir el modo en que las aplicaciones se ejecutan en Escritorio dinámico y configuran el entorno de usuario de Escritorio dinámico.

4. Crear o modificar una configuración para seleccionar las opciones de Escritorio dinámico.
5. Instalar el software del plug-in con la función de Escritorio dinámico seleccionada.
6. Desinstale Escritorio dinámico si es necesario.

Procedimiento de inicio y cierre de Escritorio dinámico

A continuación se describen los sucesos relacionados con el inicio y el cierre de Escritorio dinámico. Cuando la estación de trabajo o el dispositivo se inicie, iniciará sesión automáticamente en la cuenta compartida, lo cual permite que el dispositivo se ejecute en modo de escritorio compartido.

Nota: La cuenta compartida de Escritorio dinámico permanece siempre activa, ya que los usuarios no tienen permisos para cerrarla.

1. Un usuario de Escritorio dinámico inicia sesión en la estación de trabajo e introduce un nombre de usuario y contraseña o utiliza un autenticador seguro, como una tarjeta inteligente.
2. Una vez que el usuario se ha autenticado, se inicia la sesión de Escritorio dinámico.
3. Se inicia Single Sign-on. El software del plug-in sincroniza sus datos con el almacén central. Con esto se garantiza que el usuario dispone de las definiciones de aplicación más recientes, las directivas de contraseña y otros parámetros relacionados con el software del plug-in.
4. Se lee el archivo session.xml y se inician las aplicaciones especificadas para ejecutarse en la cuenta compartida o en la cuenta de usuario de Escritorio dinámico. Éstas pueden ser aplicaciones locales o aplicaciones remotas publicadas con XenApp. El usuario accede a las aplicaciones para realizar las tareas relacionadas con su trabajo.
5. El usuario de Escritorio dinámico cierra la sesión.
   Nota: Cuando los usuarios dejan una estación de trabajo sin actividad, Escritorio dinámico inicia un período de tiempo de espera de la sesión. Mediante Access Management Console, puede especificarse el tiempo que puede permanecer inactiva una estación de trabajo. Cuando se excede ese intervalo, Escritorio dinámico bloquea la estación de trabajo. Si transcurre más tiempo y el usuario no vuelve, Escritorio dinámico cierra la sesión.
6. Escritorio dinámico deja las aplicaciones en ejecución o las finaliza según los parámetros de process.xml.
7. Se cierra Single Sign-on.
8. Se ejecutan los scripts de cierre especificados en session.xml.
9. Se cierra la sesión de Escritorio dinámico.

Solución de problemas de inicio de Escritorio dinámico

Cuando un usuario inicia sesión en un equipo con Single Sign-on configurado para Escritorio dinámico, es posible que los scripts de inicio especificados en el archivo session.xml se ejecuten antes de que el software de Single Sign-on Plug-in se haya iniciado por completo.

Durante su inicio, Escritorio dinámico espera 30 segundos para que se inicie el software del plug-in antes de comenzar la ejecución de los scripts de inicio. Al cabo de 30 segundos, se ejecutan estos scripts de inicio, aunque el software del plug-in no se haya iniciado por completo.

Esta situación se produce con mayor probabilidad durante el inicio de sesión inicial del usuario (también conocido como usuario de primera vez), cuando el administrador de Single Sign-on ha identificado una lista de aplicaciones que requieren registro de credenciales de inicio de sesión o respuestas necesarias para preguntas de seguridad. En este caso, la secuencia es:

1. El usuario inicia la sesión en el equipo o dispositivo cliente que ejecuta el plug-in y se muestra una petición para que el usuario registre las credenciales de inicio de sesión para las aplicaciones enumeradas o registre respuestas a preguntas de seguridad.

2. Mientras se llevan a cabo estas tareas, transcurren los 30 segundos y se ejecutan los scripts de inicio de Escritorio dinámico. Es posible que se abran y cierren varias ventanas, según las aplicaciones especificadas en los scripts de inicio de session.xml.
3. La frustración del usuario puede sobrevenir porque el equipo sigue moviendo el enfoque a las ventanas de los scripts de inicio.
4. Cuando los scripts de inicio finalizan, aparece un mensaje de error. El error es similar a “Se produjeron errores durante la operación. Consulte el registro de sucesos para más información”.

Aunque este comportamiento pueda provocar frustración en el usuario, no se dañan los datos del usuario, el entorno de trabajo ni Single Sign-on.

Aconseje a los usuarios no registrar sus credenciales de inicio de sesión y las respuestas a las preguntas de seguridad hasta que aparezca el mensaje de error. A continuación, pueden cerrar el mensaje de error y finalizar el proceso de inscripción y registro.

Tras el mensaje de error y el registro, si no se ha abierto alguna aplicación especificada en session.xml, se debe aconsejar al usuario que cierre la sesión y vuelva a iniciarla en la cuenta. De este modo se reinician los scripts de inicio de Escritorio dinámico, que se ejecutan ininterrumpidamente porque ha finalizado el registro y no demora el proceso.

Creación de una cuenta compartida de Escritorio dinámico

Debe crearse una cuenta compartida de Escritorio dinámico para los dispositivos cliente o estaciones de trabajo en los que vaya a ejecutarse Escritorio dinámico. Esta cuenta compartida puede ser una cuenta de dominio o local en el dispositivo. Cuando se instala Escritorio dinámico en el dispositivo cliente, se facilitan las credenciales para cada cuenta compartida. Cuando el dispositivo o la estación de trabajo se inicie, iniciará sesión automáticamente en la cuenta compartida, lo cual le permite ejecutarse en modo de estación de trabajo de Escritorio compartido.

Las sesiones de usuario se ejecutan “encima” de la sesión de Windows de la cuenta compartida (los usuarios no pueden realizar cambios en la cuenta compartida a no ser que se les autorice). Los usuarios inician la sesión de Escritorio dinámico escribiendo sus credenciales de dominio de Windows. En un entorno de Escritorio dinámico, la cuenta de Windows del usuario se conoce como usuario de Escritorio dinámico.

Organización de los usuarios de Escritorio dinámico

Antes de instalar Escritorio dinámico, es recomendable configurar el entorno de usuario. Por ejemplo, puede agruparse a los usuarios de Escritorio dinámico en una o más unidades organizativas o grupos de Active Directory. Además, pueden organizar los usuarios que son de Escritorio dinámico y también utilizar sus estaciones de trabajo en varios grupos y asignar prioridades a dichos grupos.

Esto permite aplicar parámetros de Herramienta de definición de aplicaciones, definiciones de aplicación, directivas de contraseña y otra información de configuración de usuario a varios usuarios de Escritorio dinámico en dichas unidades organizativas.

Restricción de los derechos de usuario

Debido a que todos los usuarios de Escritorio dinámico comparten el dispositivo de Escritorio dinámico, puede ser necesario restringir los permisos y establecerlos al mínimo necesario para utilizar sus aplicaciones asignadas. Por ejemplo, los usuarios de Escritorio dinámico no deben tener derechos para cerrar el dispositivo. Este derecho debe quedar restringido a los miembros del grupo Administradores.

Escritorio dinámico, tarjetas inteligentes y recuperación de claves

Nota: Si los usuarios utilizan tarjetas inteligentes en el entorno de Escritorio dinámico, se debe seleccionar la opción Certificado de tarjetas inteligentes de Protección de datos para la configuración de usuario.
Si se instala Escritorio dinámico en un entorno donde los usuarios inician sesión con tarjetas inteligentes, no se debe seleccionar Pedir al usuario que introduzca su contraseña anterior ya que es el único método de recuperación de claves y de protección de datos para dichos usuarios. Los usuarios en un entorno de este tipo no pueden introducir la contraseña anterior correcta y, por lo tanto, están bloqueados en el sistema. Para evitar este problema, se debe seleccionar la opción de recuperación de claves para la administración automática de claves o poner a disposición de los usuarios la autenticación con preguntas.

Instrucciones para la cuenta compartida de Escritorio dinámico

Siga estas instrucciones para crear una cuenta compartida:

- Asegúrese de que la cuenta no pertenece al grupo Administradores local o del dominio.
- La cuenta compartida puede ser una cuenta local o de dominio. Los privilegios disponibles para la cuenta compartida también lo estarán para el usuario de Escritorio dinámico sólo para las aplicaciones que se especifiquen. Es decir, se pueden especificar las aplicaciones que se ejecutan con las credenciales de cuenta compartida de Escritorio dinámico y las que se inician con las credenciales de dominio de Windows del usuario.
- El proceso de instalación de Escritorio dinámico comprueba el nombre de inicio de sesión y el dominio de la cuenta compartida. Al crear esta cuenta, es necesario seleccionar la opción La contraseña nunca caduca. No use credenciales caducadas.
- Asegúrese de que la cuenta tiene privilegios limitados. Los permisos deben limitarse únicamente al uso de Escritorio dinámico.
- Especifique el nombre de dominio al que pertenece la estación de trabajo mediante el nombre NetBIOS; no indique el nombre completo de dominio. Si utiliza una cuenta local, especifique el nombre de host del dispositivo.
- Como práctica recomendada, la cuenta compartida debe llamarse “Escritorio dinámico”. Esto garantiza que los usuarios vean el mensaje de cierre de sesión de Escritorio dinámico cuando cierren la sesión. Si la cuenta compartida tiene un nombre cifrado, los usuarios pueden confundirse al ver el nombre cuando cierren la sesión. Si tiene varios grupos de usuarios de Escritorio dinámico, puede denominar la cuenta compartida a partir de éstos; por ejemplo, “Escritorio dinámico Marketing”, “Escritorio dinámico Contabilidad” y así sucesivamente.

Requisitos para las aplicaciones utilizadas con Escritorio dinámico

Las aplicaciones que se utilicen en un entorno de Escritorio dinámico deben cumplir los siguientes requisitos:

- Las aplicaciones que requieran credenciales de usuario deben definirse de forma que puedan utilizarse con Single Sign-on en las definiciones de aplicación y las configuraciones de usuario.
- Las aplicaciones iniciadas por la cuenta compartida deben poder ejecutarse en el entorno interactivo de Windows. En este tipo de entorno, las aplicaciones (y los usuarios de Escritorio dinámico) deben tener acceso a los perfiles de usuario, a las redes compartidas y a otros recursos relacionados con la cuenta compartida.
- Las aplicaciones deben cerrarse sin errores cuando reciben la solicitud de cierre. Escritorio dinámico cierra las aplicaciones mediante un procedimiento similar al de los cierres de sesión de las sesiones interactivas de Windows. El cierre de aplicaciones es especialmente importante en entornos de Escritorio dinámico, ya que es posible que la aplicación se utilice muchas veces antes de que se apague el dispositivo o la estación de trabajo.
- Cualquier aplicación que guarde datos confidenciales en el perfil de usuario u obtenga sus parámetros de configuración del perfil de usuario debe ejecutarse como cuenta de usuario de Escritorio dinámico. Las aplicaciones que pueden compartir información de configuración de la “comunidad” pueden ejecutarse como cuentas compartidas. Los

administradores pueden usar el script de cierre de sesión especificado en el archivo session.xml para asegurarse de que los archivos específicos de usuario se suprimen al final de cada sesión.

Importante: Para que Single Sign-on envíe las credenciales en un entorno de Escritorio dinámico para emuladores de terminal que almacenen información en el subárbol del Registro HKEY_CURRENT_USER, es necesario ejecutar las aplicaciones como cuenta de usuario de Escritorio dinámico. Para ello, debe especificarse que los emuladores de terminal se ejecuten como la cuenta de usuario de Escritorio dinámico en la sección ShellExecute del archivo process.xml. Para que se ejecute un emulador de terminal al iniciar la sesión, especifíquelo en la sección del script de inicio del archivo session.xml. Los emuladores de terminal deben ejecutarse como cuenta de usuario de Escritorio dinámico en el script de inicio.

Control del comportamiento de las aplicaciones para los usuarios de Escritorio dinámico

Single Sign-on ofrece dos archivos para controlar el comportamiento de las aplicaciones en un entorno de Escritorio dinámico: session.xml y process.xml.

Importante: No se puede especificar que un proceso se ejecute como cuenta compartida de Escritorio dinámico en el archivo session.xml y a continuación especificarse que se ejecute como usuario de Escritorio dinámico en el archivo process.xml. Las entradas del archivo session.xml anulan las entradas realizadas en el elemento del archivo process.xml.
Antes de comenzar:

- Para iniciar sesión en la estación de trabajo o dispositivo de usuario con fines de administración (por ejemplo, para editar el archivo process.xml), mantenga pulsada la tecla Mayús durante el proceso de inicio de Windows. Para obtener más información sobre cómo omitir el proceso de inicio de sesión automático de Windows, visite el sitio Web de Microsoft.
- Al ejecutar el archivo session.xml de Escritorio dinámico, los scripts de caducidad de contraseñas o de otro tipo, archivos ejecutables o archivos por lotes desde una sesión de usuario de Escritorio dinámico, no se admiten las siguientes variables de entorno: APPDATA, HOMEDRIVE, HOMEPATH, HOMESHARE y LOGONSERVER Si se utiliza alguna de las variables incompatibles, es posible que no se ejecute el script, la aplicación o el archivo ejecutable. Para evitar este problema, las aplicaciones no deben acceder a variables de entorno incompatibles mientras se ejecutan en una sesión de usuario de Escritorio dinámico.
- Debe indicarse a los usuarios que cierren las aplicaciones que están definidas como procesos persistentes. Por ejemplo, si un usuario inicia un proceso persistente, crea un archivo y lo deja abierto cuando salga de la sesión de Escritorio dinámico, el siguiente usuario que inicie sesión podrá ver el contenido del archivo.
  Importante: Indique a los usuarios que cierren siempre las aplicaciones confidenciales que estén definidas como persistentes antes de cerrar sus sesiones de Escritorio dinámico.
  Si define una aplicación como persistente en process.xml y la especifica en el script de inicio en session.xml, el número de copias de la aplicación puede aumentar si los usuarios no cierran esas copias de la aplicación durante la sesión de Escritorio dinámico. Para evitar que esto ocurra, limite el número de copias creando un script o una aplicación contenedora que inicie la aplicación. También puede modificar la propia aplicación para garantizar que sólo se ejecutará una copia cada vez.

- Las aplicaciones que se inician desde el símbolo del sistema se ejecutan como cuenta compartida de Escritorio dinámico aunque estén definidas como cuenta de usuario de Escritorio dinámico. Para iniciar aplicaciones desde el símbolo del sistema como usuario de Escritorio dinámico, se debe especificar el símbolo del sistema en la sección de del archivo process.xml. Además, si el símbolo del sistema se está ejecutando como cuenta compartida, la asociación del tipo de archivo está definida en la sección del archivo process.xml (como *.txt) y el usuario ejecuta un archivo con la extensión .txt, la aplicación se inicia como usuario de Escritorio dinámico.
- Las aplicaciones persistentes que usen el formato de archivo 8.3, deben emplear dicho formato en la ruta del ejecutable al especificarlas en process.xml.
- Mientras que las etiquetas y los formatos XML del archivo process.xml distinguen entre mayúsculas y minúsculas, las rutas y los nombres de ejecutables no lo hacen.

- Si los usuarios ejecutan SAP Logon para Windows (saplogon.exe), se debe ejecutar como usuario de Escritorio dinámico. En el archivo process.xml, especifique saplogon.exe en la etiqueta .

Parámetros de configuración de usuario para Escritorio dinámico

Jul 19, 2016

Se puede controlar la interacción del usuario de Escritorio dinámico mediante los siguientes parámetros de configuración de usuario.

Precaución: Algunos procedimientos requieren la modificación del Registro del sistema. La utilización inadecuada del Editor del Registro puede causar problemas graves que obliguen a volver instalar el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Siempre se debe realizar una copia de seguridad del Registro del sistema antes de continuar.

Ruta del script de inicio de sesión

Localice la configuración de Escritorio dinámico en una configuración de usuario:

- Al crear una nueva configuración de usuario, dichos parámetros están disponibles en Configuración avanzada del cuadro de diálogo Configurar la interacción con el plug-in.
- Al modificar una configuración de usuario existente, los parámetros están disponibles en el panel Escritorio dinámico del cuadro de diálogo Modificar configuración de usuario.
  Para obtener detalles de configuración, consulte el tema de Escritorio dinámico en
  — Referencia de configuración de Single Sign-on > Configuraciones de usuario
  .

Para configurar la ruta del script de parámetros de sesión

1. En la página Escritorio dinámico del cuadro de diálogo Modificar configuración de usuario, en el campo Ruta del script de parámetros de sesión, escriba la ubicación del archivo session.xml. La ubicación puede ser una carpeta compartida de red. Por ejemplo, si coloca el archivo session.xml en un punto compartido de la red, como \\Citrix\MPM\Share\, escriba dicha ruta.
2. Después de guardar la configuración de usuario e instalar el archivo session.xml, reinicie la estación de trabajo de Escritorio dinámico.

Interacción con la recuperación automática de claves

Si el entorno de Single Sign-on combina la opción de recuperación automática de claves con Escritorio dinámico, los cambios de contraseña que realice el administrador no se comunicarán al software del plug-in de los usuarios que tengan sesiones de Escritorio dinámico activas. Si dichos usuarios ven bloqueadas sus sesiones e intentan desbloquearlas, es posible que se les pida que indiquen sus contraseñas anteriores. En ese caso, los usuarios deberán cerrar el cuadro de diálogo de las contraseñas anteriores y, a continuación, finalizar y reiniciar la sesión de Escritorio dinámico mediante el cierre de la sesión para seguir usando el plug-in

Protector de pantalla de Escritorio dinámico

Para que los usuarios puedan identificar más fácilmente las estaciones de trabajo que están ejecutando Escritorio dinámico, las instalaciones de Escritorio dinámico incluyen un protector de pantalla personalizado. El protector de pantalla no se ejecuta hasta que la estación de trabajo queda inactiva durante 10 minutos.

Nota: Las sesiones bloqueadas se consideran activas. El protector de pantalla se inicia transcurridos 10 minutos de tiempo de inactividad y una vez que todos los usuarios hayan cerrado su sesión en las estaciones de trabajo.

Para instalar Escritorio dinámico

Escritorio dinámico se puede instalar con una instalación existente o una instalación nueva de Single Sign-on Plug-in.

1. Inicie la sesión en el dispositivo del usuario como administrador local.
2. En el Panel de control, seleccione Agregar o quitar programas.
3. Seleccione Single Sign-on Plug-in y haga clic en Cambiar.
4. Seleccione Modificar y haga clic en Siguiente.
5. Seleccione Escritorio dinámico y haga clic en Siguiente.
6. Haga clic en Sí en el cuadro de diálogo de confirmación para inhabilitar Servicios de Terminal Server y Escritorio remoto.
7. Especifique la ubicación del almacén central y haga clic en Siguiente.
8. Especifique la dirección del servidor de servicios y haga clic en Siguiente.
9. Escriba las credenciales de usuario para la cuenta compartida de Escritorio dinámico y haga clic en Siguiente. Especifique el nombre de dominio al que pertenece la estación de trabajo mediante el nombre NetBIOS; no indique el nombre completo de dominio.
10. Haga clic en Instalar. Acceda al medio de instalación de manera que el proceso de instalación encuentre el archivo .msi para la instalación de Single Sign-on Plug-in.

Una vez terminada la instalación, reinicie el dispositivo de usuario.

Para desinstalar Escritorio dinámico

Si necesita quitar la característica Escritorio dinámico de la estación de trabajo, es posible que también deba ejecutar los procedimientos siguientes antes de desinstalar esta característica:

- Desinstalación de Servicios de Terminal Server después de desinstalar Escritorio dinámico
- Activación de varias sesiones después de desinstalar Escritorio dinámico

1. Para iniciar sesión en la estación de trabajo o dispositivo cliente compartidos para realizar tareas de administrador, mantenga pulsada la tecla Mayús durante el proceso de inicio de Windows.
   De este modo se impide que la cuenta compartida de Escritorio dinámico inicie la sesión y se inicie el entorno de Escritorio dinámico. Para obtener más información sobre cómo omitir el proceso de inicio de sesión automático de Windows, visite el sitio Web de Microsoft.

   Inicie la sesión como administrador.
2. Abra el Panel de control y seleccione Agregar o quitar programas.
3. Seleccione Single Sign-On Plug-in.
4. Haga clic en Cambiar para quitar la función de Escritorio dinámico únicamente.
5. En la página Mantenimiento de la aplicación, seleccione Modificar.
6. En la página Selección de funciones, elija Escritorio dinámico para que no esté disponible la función.
7. Siga las instrucciones para seleccionar el tipo de almacén central y confirmar los cambios del plug-in.
8. Reinicie la estación de trabajo.

Escritorio dinámico no se elimina por completo hasta que se reinicie la estación de trabajo.
Importante: Cuando se desinstala el software que puede haber roto la cadena GINA, es importante desinstalarlo en el orden inverso en el que se instaló en el dispositivo cliente. De lo contrario, el equipo no funcionará correctamente. No modifique el registro.

Para habilitar los servicios de Terminal Server tras la desinstalación de Escritorio dinámico

El proceso de instalación de Escritorio dinámico desactiva los servicios de Terminal Server. Realice el siguiente procedimiento para habilitar Servicios de Terminal Server.

1. Inicie la sesión en la estación de trabajo como administrador.
2. Haga clic en Inicio > Ejecutar y escriba regedit.
3. Cambie el valor de la clave de Registro a 1 como sigue: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server]TSEnabled=dword:00000001

Para habilitar varias sesiones

Durante la instalación de Escritorio dinámico, el instalador restaura el valor de la clave de Registro a 0. Realice el siguiente procedimiento para habilitar sesiones múltiples.

1. Inicie la sesión en la estación de trabajo como administrador.
2. Haga clic en Inicio > Ejecutar y escriba regedit.
3. Cambie el valor de la clave de Registro a 1 como sigue: [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current Version\Winlogon] AllowMultipleSessions =dword:00000001

Para ver perfiles de Escritorio dinámico

En un entorno de Escritorio dinámico, el shell (explorer.exe) se ejecuta como la cuenta compartida de Escritorio dinámico. Por lo tanto, el shell no tiene los derechos de acceso necesarios para la carpeta del perfil de usuario del Escritorio dinámico.

1. En el archivo process.xml, en la sección , incluya Internet Explorer (iexplore.exe) de forma que se ejecute como el usuario del Escritorio dinámico.
2. Inicie la sesión como usuario del Escritorio dinámico y ejecute Internet Explorer.
3. Para ver los perfiles, escriba en la barra de direcciones la ruta completa del directorio de perfiles de usuario del Escritorio dinámico. Por ejemplo: C:\Documents and Settings\All Users\Application Data\Citrix\MetaFrame Password Manager

Para inhabilitar el respaldo de AutoAdminLogon

Algunos autenticadores de otros fabricantes podrían no funcionar si la función AutoAdminLogon está activada. Algunas aplicaciones de otros fabricantes desactivan o eliminan el valor AutoAdminLogon durante la instalación. En tal caso, debe desactivar AutoAdminLogon de Escritorio dinámico.

1. Reinicie la estación de trabajo o dispositivo de usuario compartidos, mientras mantiene pulsada la tecla Mayús durante el proceso de inicio de Windows. De este modo se impide que la cuenta compartida de Escritorio dinámico inicie la sesión y se inicie el entorno de Escritorio dinámico. Para obtener más información sobre cómo omitir el proceso de inicio de sesión automático de Windows, visite el sitio Web de Microsoft.
2. Inicie la sesión como administrador.
3. Modifique el Registro y establezca los valores siguientes en HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\MetaFrame Password Manager\HotDesktop

Nombre del valor	Tipo	Valor
AutoAdminLogon	REG_SZ	0 para desactivar

4. Tras establecer el valor, reinicie la estación de trabajo e inicie manualmente la sesión utilizando la cuenta compartida. Aparece la página de inicio de sesión de Escritorio dinámico, que permite a los usuarios utilizar el autenticador de otro

fabricante.

Para cambiar la contraseña de la cuenta compartida de Escritorio dinámico

Es posible que se tenga que cambiar la contraseña de la cuenta compartida de Escritorio dinámico. Las credenciales de cuenta se especificaron por primera vez durante la instalación del plug-in. Para cambiar la contraseña, realice el siguiente procedimiento.

1. Inicie la sesión en una estación de trabajo donde esté instalado Escritorio dinámico.
   Importante: No utilice las credenciales de la cuenta de administrador o la cuenta compartida de Escritorio dinámico para el paso 1.
2. Presione la combinación Ctrl+Alt+Supr. Aparecerá el cuadro de diálogo Seguridad de Windows.
3. Haga clic en Cambiar contraseña.
4. Escriba o seleccione uno de los siguientes elementos:
   - Nombre de usuario de la cuenta compartida de Escritorio dinámico
   - Nombre de dominio o nombre de equipo local
   - Contraseña anterior
   - Contraseña nueva
5. Haga clic en Aceptar.
6. En el cuadro de diálogo Seguridad de Windows, haga clic en Apagar y luego en Reiniciar para reiniciar el equipo.

Para cerrar las estaciones de trabajo de Escritorio dinámico

Puesto que sólo los administradores pueden cerrar las estaciones de trabajo de Escritorio dinámico, la opción Cerrar no está disponible en el menú Inicio de una estación de trabajo de Escritorio dinámico.

Para cerrar una estación de trabajo de Escritorio dinámico para uso administrativo, pulse CTRL+ALT+SUPR. Cuando aparezca el cuadro de diálogo Seguridad de Windows, haga clic en Cerrar.

Interacción con otros productos de Citrix

Single Sign-on admite el uso de los plug-ins de Citrix con Escritorio dinámico. Deberán tenerse en cuenta las instrucciones siguientes si se desea usar Escritorio dinámico con estos plug-ins y la Interfaz Web:

- Edite el archivo process.xml para asegurarse de que Citrix Receiver y Citrix Offline Plug-in sean procesos transitorios (en caso de que el plug-in se haya definido para que lo inicie un programa de inicio de Windows y se ejecute después de iniciarse la primera sesión de Escritorio dinámico).
- Si se utiliza Security Service Provider Interface, debe ejecutarse el plug-in como usuario de Escritorio dinámico. También puede ejecutarse el plug-in como usuario de Escritorio dinámico por motivos de seguridad; los archivos ICA se almacenan en el perfil.
  - Modifique la sección del archivo process.xml para que Citrix Receiver y Citrix Offline Plug-in se ejecuten como usuarios de Escritorio dinámico cuando se inicien desde el shell de Windows.
  - Modifique el archivo session.xml para especificar un script de inicio o un ejecutable para ejecutar Citrix Receiver y Citrix Offline Plug-in cuando se inicie la primera sesión de Escritorio dinámico.

Citrix Receiver

Citrix Receiver puede configurarse para que utilice Security Service Provider Interface. Security Service Provider Interface permite que Receiver se autentique en el servidor XenApp con las credenciales de usuario de Escritorio dinámico. Debe asegurarse de que XenApp confíe en la entidad de seguridad de Windows utilizada para autenticar al usuario de Escritorio

dinámico. Para obtener más información sobre la configuración de Security Service Provider Interface para Receiver, consulte los temas sobre la
— Administración de XenApp
.

Interfaz Web

El plug-in de Escritorio dinámico puede enviar credenciales a través de la Interfaz Web a un servidor XenApp. Para más información, consulte los temas sobre configuración de la
— Interfaz Web
.

Archivo session.xml

Jul 19, 2016

El archivo session.xml se utiliza para indicar las aplicaciones que se ejecutan cuando se inicia una sesión de Escritorio dinámico (script de inicio) y elimina los archivos u otra información que hayan quedado de una sesión de usuario (script de cierre). Una vez modificado este archivo según sea preciso, debe colocarse en un punto compartido de la red u otra ubicación central para que las estaciones de trabajo de Escritorio dinámico puedan acceder a él. Esta ubicación del archivo session.xml se especifica en la configuración de usuario.

Las etiquetas se deben incluir entre las etiquetas y en el archivo.

Nota: En la carpeta \Support del CD de Password Manager se incluye un archivo session.xml de muestra.

Ejemplo: limpieza de una sesión con un script

Se utiliza un script de Visual Basic para limpiar todos los datos de usuario que puedan haber quedado tras el cierre de una sesión. El script session_cleanup.vbs se inicia como cuenta compartida (denominada HDSA) y está ubicado en C:\.

Ejemplo: Inicio de Internet Explorer

Se inicia Internet Explorer con la URL de la intranet mycompany.com. En este caso, Internet Explorer se ejecuta como un proceso asociado al usuario de Escritorio dinámico.

Las etiquetas se deben incluir entre las etiquetas y < /session_settings> en el archivo.

startup_scripts

Esta sección del archivo se utiliza para especificar las aplicaciones que se inician en la cuenta compartida de Escritorio dinámico y la cuenta de Windows asociada al usuario de Escritorio dinámico.

donde:

cuenta	Indica la cuenta en la que se ejecutará la aplicación. Las opciones son HDU o el nombre de usuario de la cuenta compartida de Escritorio dinámico.
directorio_de_trabajo	Indica el directorio de trabajo de la aplicación.
opciones_de_ruta	Indica la ruta de carpeta completa al archivo ejecutable o script de la aplicación en el equipo local y las opciones con que se ejecutará la aplicación. Por ejemplo: c:\archivos de programa\Internet Explorer\iexplore.exe http://www.yahoo.com

shutdown_scripts

Para eliminar todos los datos no utilizados procedentes de la sesión de usuario anterior es necesario modificar las aplicaciones de cierre de session.xml. Estas aplicaciones suelen eliminar los archivos de configuración que pueden impedir el trabajo del otro usuario que se conecte después del anterior, los archivos confidenciales (por ejemplo, registros) y los

documentos almacenados en el sistema. Estas aplicaciones deben garantizar que el entorno de Escritorio dinámico se vacíe para la siguiente sesión de usuario. Esta parte del archivo resulta muy útil para la seguridad de los datos.

Nota: Si fuera necesario, se pueden iniciar programas de administrador o scripts para limpiar el entorno de usuario cuando se cierre la sesión. Por ejemplo, puede escribirse un script de Visual Basic mediante una aplicación de otro proveedor para eliminar archivos .ini específicos de usuario.

donde:

cuenta	Indica la cuenta en la que se ejecutará la aplicación de cierre. Las opciones sonHDU y el nombre de usuario de la cuenta compartida de Escritorio dinámico.
directorio_de_trabajo	Indica el directorio de trabajo de la aplicación.
opciones_de_ruta	Indica la ruta de carpeta completa al archivo ejecutable o script de la aplicación en el equipo local y las opciones con que se ejecutará la aplicación. Por ejemplo: c:\cleanup.vbs

Inicio de aplicaciones mediante session.xml

Se deben tener en cuenta las siguientes cuestiones:

- Las aplicaciones que se definan en el archivo session.xml deben haberse instalado antes en la estación de trabajo.
- Dado que Escritorio dinámico forma parte del software de Single Sign-on Plug-in, el plug-in se inicia automáticamente y no necesita especificarse en este archivo.

Otras aplicaciones especificadas en session.xml pueden iniciarse en el shell de cuenta compartida de Escritorio dinámico que, a continuación, puede solicitar las credenciales a los usuarios. Después, el plug-in actúa según los parámetros de las configuraciones de usuario.

Importante: El archivo session.xml se debe guardar en formato UTF-8. La codificación ANSI es aceptable si todos los caracteres están en el intervalo de 0 a 127 (juego de caracteres estándar del inglés). Si el archivo session.xml contiene caracteres especiales, como los caracteres de idiomas asiáticos, es necesario guardarlo en formato UTF-8.

Archivo process.xml

Jul 19, 2016

Nota: El archivo process.xml se crea en la carpeta C:\Archivos de programa\Citrix\MetaFrame Password Manager\HotDesktop de cada estación de trabajo o dispositivo donde está instalado Escritorio dinámico. En la carpeta \Support del medio de instalación del producto también se incluye un archivo process.xml de muestra. Por lo tanto, cualquier cambio que se haga en este archivo debe llevarse a cabo en cada uno de los dispositivos. No obstante, consulte el artículo de Citrix Support http://support.citrix.com/article/CTX110394 para obtener información sobre cómo reemplazar cada archivo process.xml de usuario mediante una directiva de grupo de equipos en Active Directory.
El archivo process.xml se utiliza para especificar las aplicaciones que se siguen ejecutando después de que el usuario de Escritorio dinámico cierre la sesión. Estas aplicaciones se denominan aplicaciones persistentes o procesos persistentes.

El archivo process.xml también se puede utilizar para especificar las aplicaciones que finalizan después de que el usuario de Escritorio dinámico cierre la sesión. Estas aplicaciones se denominan aplicaciones efímeras o procesos efímeros.

Las etiquetas se deben incluir entre las etiquetas y en el archivo.

Importante: El archivo process.xml se debe guardar en formato UTF-8. La codificación ANSI es aceptable si todos los caracteres están en el intervalo de 0 a 127 (juego de caracteres estándar del inglés). Si el archivo process.xml contiene caracteres especiales, como los caracteres de idiomas asiáticos, es necesario guardarlo en formato UTF-8.

shellexecute_processes

Esta sección del archivo se utiliza para especificar las aplicaciones o tipos de archivo que se ejecutarán como el usuario de Escritorio dinámico. Este parámetro contribuye a garantizar la seguridad de las aplicaciones que se ejecutarán mediante las credenciales de los usuarios que han iniciado sesión.

Nota: Después de la instalación, el software del plug-in especifica automáticamente una aplicación de ejecución de shell denominada ssoshell.exe (el software de Single Sign-on Plug-in) en el archivo process.xml. De forma predeterminada, se especifica como proceso que se ejecutará como el usuario de Escritorio dinámico.
Mientras que el script de inicio del archivo session.xml especifica las aplicaciones que se ejecutarán cuando se inicie por primera vez una sesión de Escritorio dinámico, enumera las aplicaciones que los usuarios pueden iniciar en el contexto de su sesión de Escritorio dinámico.

nombre_de_aplicación
donde:

nombre_de_aplicación	Indica sólo el nombre de aplicación del proceso o la aplicación que se ejecutará. No es necesaria la ruta completa. Por ejemplo: pnagent.exe.

Nota: process.xml permite usar un comodín (*) además de nombres de archivo estáticos como Notepad.exe. Los comodines pueden usarse de forma independiente o bien con los nombres de archivo. Por ejemplo, *.txt, pnagent.exe y *.doc son nombres de aplicación válidos.

persistent_processes

Esta sección del archivo se utiliza para especificar las aplicaciones que se siguen ejecutando después de que el usuario de Escritorio dinámico cierre la sesión. Las aplicaciones especificadas no finalizarán al cerrar las sesiones de Escritorio dinámico, aunque se hayan iniciado durante una sesión. Se debe especificar la ruta completa del proceso persistente para garantizar

que sólo los procesos correctos siguen ejecutándose después de cada sesión.

opciones_de_ruta

donde:

opciones_de_ruta	Indica la ruta de carpeta completa al archivo ejecutable o script de la aplicación en el equipo local y las opciones con que se ejecutará la aplicación. Por ejemplo: c:\archivos de programa\Internet Explorer\iexplore.exe http://www.yahoo.com

Nota: Después de la instalación, el software del plug-in crea automáticamente una entrada para una aplicación persistente denominada activator.exe en el archivo process.xml. La aplicación activator.exe proporciona a los usuarios el indicador de sesión de Escritorio dinámico. El indicador de sesión es una ventana móvil transparente que ven los usuarios cuando están conectados, y que contiene información sobre los usuarios y sus sesiones definida por el administrador. De forma predeterminada, activator.exe se especifica como proceso persistente, de modo que no se reinicia cada vez que un usuario de Escritorio dinámico inicia o cierra una sesión.

transient_processes

Esta sección del archivo se utiliza para especificar las aplicaciones que se cerrarán después de que el usuario de Escritorio dinámico cierre la sesión.

Nota: Después de la instalación, el plug-in especifica automáticamente una aplicación efímera denominada shellexecute.exe en el archivo process.xml. De forma predeterminada, se especifica como proceso efímero, de modo que termina cada vez que un usuario de Escritorio dinámico cierra una sesión.

nombre_de_aplicación

donde:

nombre_de_aplicación	Indica sólo el nombre de aplicación del proceso o la aplicación que se cerrará. No es necesaria la ruta completa. Por ejemplo: pnagent.exe.

Referencia

Oct 12, 2015

En este capítulo se describen los parámetros de configuración, y sus valores predeterminados, disponibles en el nodo Single Sign-on de Citrix AppCenter, agrupados por la posición que ocupan en la consola.

Configuraciones de usuario

En esta sección se describen los parámetros y controles de configuración de usuario. Todas las sugerencias de exploración que se ofrecen en esta sección se efectúan en una configuración de usuario existente cuando se realiza una función de edición. Para acceder al cuadro de diálogo Modificar configuración de usuario, haga lo siguiente:

Inicio > Todos los programas > Citrix > Consolas de administración > Citrix AppCenter > Single Sign-on > Configuraciones de usuario > [configuración] > Modificar configuración de usuario

Interacción básica con el plug-in

Estos controles permiten personalizar la forma en que el Single Sign-on Plug-in funciona para esta configuración de usuario. Aquí se establecen las preferencias de interfaz de usuario.

Inicio > Todos los programas > Citrix > Consolas de administración > Citrix AppCenter > Single Sign-on > Configuraciones de usuario > [configuración] > Modificar configuración de usuario > Interacción básica con el plug-in

Permitir que los usuarios revelen las contraseñas

Este parámetro controla si los usuarios pueden revelar sus contraseñas en la ventana Administrar contraseñas. Cuando no se selecciona este parámetro, el botón Revelar contraseñas queda desactivado. Para restringir la capacidad de revelar contraseñas a ciertas aplicaciones, seleccione este parámetro y use el control correspondiente de la directiva de contraseñas para controlar si los usuarios pueden revelar las contraseñas de las aplicaciones administradas con dicha directiva.

Parámetro predeterminado: seleccionado

Forzar la autenticación antes de revelar las contraseñas del usuario

Este parámetro controla si los usuarios deben volver a autenticarse en Single Sign-on antes de poder revelar las contraseñas.

Parámetro predeterminado: seleccionado

Detectar automáticamente las aplicaciones y pedirle al usuario que almacene las credenciales

Este parámetro controla si el software del plug-in debe indicar al usuario que agregue credenciales para aplicaciones nuevas que detecta el software del plug-in.

Al anular la selección de esta opción, se desactiva la capacidad del software de Single Sign-on Plug-in de detectar las aplicaciones que no están asociadas a esta configuración de usuario. Si esta opción no está seleccionada, los usuarios pueden enviar manualmente las credenciales a estas aplicaciones. Con este parámetro se impide que los usuarios agreguen

aplicaciones que no forman parte de su configuración de usuario asignada a su conjunto de aplicaciones habilitadas para inicio de sesión unificado.

Si se desactiva, ésta anula la opción Permitir que los usuarios cancelen el almacenamiento de credenciales cuando se detecta una aplicación nueva disponible en la página Configuración avanzada > Interacción en el cliente. Además, si se prevé utilizar el aprovisionamiento, al desactivar esta opción se impide que a los usuarios se les pida que introduzcan sus credenciales.

Parámetro predeterminado: seleccionado

Procesar automáticamente formularios definidos detectados por Single Sign-on Plug-in

Al seleccionar esta opción, se permite que el software del plug-in envíe las credenciales almacenadas automáticamente sin intervención del usuario. Se incorporarán datos a los campos de credenciales de la aplicación si se ha seleccionado el parámetro correspondiente Enviar automáticamente este formulario en la definición de aplicación asociada a esta configuración de usuario.

Parámetro predeterminado: seleccionado

Tiempo de espera entre solicitudes de autenticación

Este parámetro especifica el tiempo de espera entre solicitudes de autenticación del plug-in. Cuando se agota el tiempo especificado, se bloquea el dispositivo del usuario y los usuarios deben volver a autenticarse introduciendo sus credenciales primarias. El valor mínimo permitido es 1 minuto.

Parámetro predeterminado: 8 horas

Interfaz de usuario del plug-in

Estos controles se utilizan para establecer la demora de envío de credenciales y las columnas en la ventana Administrar contraseñas.

Inicio > Todos los programas > Citrix >Consolas de administración > Citrix AppCenter > Single Sign-on > Configuraciones de usuario > [configuración] > Modificar configuración de usuario > Interfaz de usuario del plug-in

Especificar cuánto tiempo demora el plug-in en enviar las credenciales

Al seleccionar este parámetro se indica cuánto tiempo tarda el plug-in en enviar las credenciales tras detectar una aplicación permitida. Si se selecciona, se debe especificar cuánto tiempo se demora (en segundos) en enviar las credenciales. Los usuarios utilizan este parámetro para garantizar que la aplicación está preparada para recibir las credenciales. Durante este tiempo, el software del plug-in mostrará un indicador de progreso que indica que está en funcionamiento.

Parámetro predeterminado: no seleccionado (0 segundos)

Configurar las columnas predeterminadas y el orden de estas en el Administrador de inicios de sesión

Este parámetro controla las columnas que se deben mostrar en la vista detallada de la ventana Administrar contraseñas (anteriormente conocida como Administrador de inicios de sesión). También controla el orden en que se muestran las

columnas.

Los parámetros predeterminados son:

- Nombre de la aplicación
- Descripción
- Grupo
- Fecha último uso
- Modificado

Interacción en el cliente

Estos parámetros se utilizan para configurar el registro de sucesos del software del plug-in, la retención de claves del registro en el cierre y el almacenamiento de credenciales en las aplicaciones recién detectadas.

Inicio > Todos los programas > Citrix > Consolas de administración > Citrix AppCenter > Single Sign-on > Configuraciones de usuario > [configuración] > Modificar configuración de usuario > Interacción en el cliente

Registrar los sucesos de Single Sign-on Plug-in mediante el registro de sucesos de Windows

Este control se selecciona para mantener un registro de los sucesos de información del software del plug-in en el registro de sucesos de Windows. Los sucesos de errores y advertencias siempre se registran, independientemente de este parámetro.

Parámetro predeterminado: no seleccionado

Eliminar la carpeta de datos del usuario y las claves del Registro al cerrar el Single Sign-on Plug-in

Seleccione este control para eliminar la carpeta de datos del usuario (con las credenciales cifradas) y las claves del Registro cuando se cierre el software del plug-in.

Parámetro predeterminado: no seleccionado

Permitir que los usuarios cancelen el almacenamiento de credenciales cuando se detecta una aplicación nueva

Este parámetro controla si se les debe pedir a los usuarios que almacenen las credenciales cada vez que el software del plug-in reconozca una aplicación para la que no existen credenciales almacenadas. Si se selecciona, los usuarios pueden elegir almacenar sus credenciales en la ventana Administrar contraseñas (anteriormente conocida como Administrador de inicios de sesión) ahora, más tarde o nunca. Si no se selecciona el parámetro Detectar automáticamente las aplicaciones y pedirle al usuario que almacene las credenciales en la página Configurar la interacción con el plug-in, el software del plug-in no solicita a los usuarios que almacenen las credenciales.

Parámetro predeterminado: seleccionado

Limitar la cantidad de días que se mantendrá un registro de las credenciales eliminadas

Estos controles se utilizan para indicar durante cuánto tiempo el almacén central debe registrar las credenciales borradas de la ventana Administrar contraseñas (anteriormente conocida como Administrador de inicios de sesión). Si las credenciales del usuario están almacenadas en varios dispositivos de cliente, el plug-in borra las credenciales cuando efectúa una sincronización con el almacén central durante este período. Si las credenciales siguen almacenadas en el dispositivo cliente cuando se agota el tiempo, se restauran cuando el plug-in efectúa una sincronización con el almacén central.

Parámetro predeterminado: seleccionado / 180 días

Sincronización

Estos controles se usan para permitir que los usuarios actualicen los parámetros de Single Sign-on Plug-in, para sincronizar la información de configuración, para permitir que el plug-in continúe funcionando aunque no pueda conectarse al almacén central y para especificar intervalos de sincronización automática.

Inicio > Todos los programas > Citrix > Consolas de administración > Citrix AppCenter > Single Sign-on > Configuraciones de usuario > [configuración] > Modificar configuración de usuario > Sincronización

Permitir a los usuarios actualizar los parámetros de Single Sign-on Plug-in

Este parámetro se selecciona para permitir que los usuarios actualicen los parámetros del software del plug-in en la ventana Administrar contraseñas (anteriormente conocida como Administrador de inicios de sesión). Cuando no se selecciona este parámetro, el botón Actualizar de la ventana Administrar contraseñas queda desactivado.

Parámetro predeterminado: seleccionado

Sincronizar cuando los usuarios inicien aplicaciones reconocidas o el Administrador de inicios de sesión

Este parámetro se selecciona para que el software del plug-in sincronice la información de configuración del usuario cada vez que el usuario ejecute una aplicación reconocida o la ventana Administrar contraseñas (anteriormente conocida como Administrador de inicios de sesión). Una sincronización frecuente puede ir en detrimento del rendimiento del cliente y del servidor e incluso aumentar el tráfico de red.

Parámetro predeterminado: no seleccionado

Permitir que funcione Single Sign-on Plug-in cuando no se pueda reconectar con el almacén central

Este parámetro controla si Single Sign-on funcionará aún cuando no pueda conectarse al almacén central para sincronizarse. Cuando se selecciona, una instancia con licencia de Single Sign-on Plug-in continúa funcionando, incluso aunque falle la conexión. Si no se selecciona, el software del plug-in funciona sólo si está conectado al almacén central.

Parámetro predeterminado: seleccionado

Especificar el tiempo transcurrido entre solicitudes de sincronización automática

Este control se utiliza para indicar el intervalo en minutos que transcurre entre los intentos de sincronización automática. La sincronización automática es independiente de la actividad del usuario y se lleva a cabo además de otros sucesos que inician una sincronización.

Parámetro predeterminado: no seleccionado / 0 minutos

Permitir acceso a credenciales de usuario a través del módulo de sincronización

Este parámetro se selecciona para permitir que los clientes remotos puedan acceder a las credenciales por medio del servicio. Esta opción se utiliza con la función de asociación de cuentas que permite a un usuario del software del plug-in iniciar sesión en cualquier aplicación desde una o varias cuentas de Windows.

Parámetro predeterminado: no seleccionado

Asociación de cuentas

Así como las empresas pueden mantener varios dominios de Windows, los usuarios también pueden tener varias cuentas de Windows. Con la opción de asociación de cuentas los usuarios pueden iniciar sesión en cualquier aplicación desde una o varias cuentas de Windows. Estos controles permiten que los usuarios asocien su información de inicio de sesión entre distintas cuentas de Windows.

Inicio > Todos los programas > Consolas de administración > Citrix AppCenter > Single Sign-on > Configuraciones de usuario > [configuración] > Modificar configuración de usuario > Asociación de cuentas

Permitir que los usuarios asocien cuentas

Al seleccionar este parámetro se permite a los usuarios que asocien varias cuentas de Windows, proporcionen la URL y el puerto donde está instalado el módulo de sincronización de credenciales. Esta opción no se puede establecer al configurar inicialmente una configuración de usuario. Sólo puede definirse cuando se modifique una configuración existente.

Parámetro predeterminado: no seleccionado

Ingresar la dirección del servicio predeterminado

Este parámetro se selecciona para poder definir la dirección y el puerto de servicio predeterminados del módulo de sincronización de credenciales. Después de definir los parámetros se puede seleccionar la opción Validar para comprobar la dirección y puerto.

Parámetro predeterminado: /MPMService/

puerto del servicio: 443

Permitir que los usuarios modifiquen la dirección del servicio

Si se definió una dirección del servicio, este parámetro permite que el usuario modifique los parámetros en la interfaz del plug-in. Esta opción se debe seleccionar si la sincronización de credenciales se ejecuta en varios sitios y los usuarios deben poder cambiar.

Parámetro predeterminado: no seleccionado

Ingresar el dominio predeterminado

Elija este parámetro para especificar el dominio predeterminado utilizado para la autenticación cuando el software del plug-in se sincroniza con la cuenta de Windows asociada. Si está seleccionado, se debe introducir el nombre de dominio predeterminado en el espacio correspondiente. Si no se indica el dominio, es posible que los usuarios no sepan qué

credenciales de usuario deben proporcionar.

Parámetro predeterminado: no seleccionado

Permitir que los usuarios modifiquen el dominio

Elija este parámetro para permitir que los usuarios modifiquen el dominio predeterminado utilizado para la autenticación cuando el software del plug-in se sincroniza con la cuenta de Windows asociada.

Parámetro predeterminado: no seleccionado

Permitir al usuario recordar su contraseña

Al seleccionar este parámetro, el usuario puede guardar su contraseña de Windows asociada en el software del plug-in.

Parámetro predeterminado: no seleccionado

Respaldo de aplicaciones

Estos controles permiten que el plug-in detecte las definiciones de aplicación en el cliente, activan la compatibilidad con emuladores de terminal y especifican el número mínimo de niveles de nombre de dominio que deben coincidir para las aplicaciones Web.

Inicio > Todos los programas > Consolas de administración > Citrix AppCenter > Single Sign-on > Configuraciones de usuario > [configuración] > Modificar configuración de usuario > Respaldo de aplicaciones

Detectar definiciones de aplicación del cliente

Seleccione este parámetro para permitir que Single Sign-on detecte aplicaciones de una de las siguientes maneras.

- Todas las aplicaciones
  Detecta y responde a las aplicaciones definidas por un administrador o usuario (en la ventana Administrar contraseñas, anteriormente conocida como Administrador de inicios de sesión) y definidas en los parámetros predeterminados durante la instalación.
- Sólo aplicaciones definidas con el administrador de inicios de sesión
  Detecta y responde a las aplicaciones definidas por un administrador y usuario en la ventana Administrar contraseñas (anteriormente conocida como Administrador de inicios de sesión). El software del plug-in no reconocerá o responderá a las aplicaciones definidas en la configuración predeterminada en la instalación.
- Sólo aplicaciones que se incluyen con el Single Sign-on Plug-in
  Detecta y responde a las aplicaciones definidas por un administrador y definidas en los parámetros predeterminados durante la instalación. Los usuarios no podrán crear sus propias definiciones de aplicación en la ventana Administrar contraseñas (anteriormente conocida como Administrador de inicios de sesión).

Parámetro predeterminado: Todas las aplicaciones

Habilitar el respaldo para emuladores de terminales

Este parámetro controla la compatibilidad con programas de emulación de terminal. Si se activa este parámetro, el software del plug-in ejecuta un proceso que detecta los emuladores de terminal y las aplicaciones basadas en emuladores de terminal.

Parámetro predeterminado: no seleccionado

Intervalo de tiempo en el que el plug-in controla cambios en el emulador de terminales

Este parámetro se utiliza para indicar cuánto tiempo en milisegundos debe transcurrir para que el software del plug-in compruebe si hay cambios de pantalla en el emulador de terminal. Los valores más bajos pueden consumir más tiempo de CPU en el cliente y aumentar el tráfico de red.

Parámetro predeterminado: 3000 milisegundos

Cantidad de niveles de nombre de dominio que se harán coincidir

Este parámetro se utiliza para indicar la cantidad mínima de niveles de nombre de dominio que se harán coincidir para aplicaciones Web permitidas. Un valor de 2 o menos coincidiría con *.domain1.topleveldomain; un valor de 3 o menos coincidiría con *.domain2.domain1.topleveldomain. Los niveles de nombre de dominio superiores al número especificado se tratan como comodines. Para controlar estrictamente la coincidencia de URL para aplicaciones Web se debe configurar una coincidencia de URL estricta en las definiciones de aplicación.

Parámetro predeterminado: 99

Escritorio dinámico

Estos controles especifican cómo se manejan las sesiones de Escritorio dinámico.

Inicio > Todos los programas > Consolas de administración > Citrix AppCenter > Single Sign-on > Configuraciones de usuario > [configuración] > Modificar configuración de usuario > Escritorio dinámico

Ruta del script de inicio de sesión

Este control indica la ruta del archivo de parámetros de sesión que define los scripts que se ejecutarán al inicio y al final de la sesión de Escritorio dinámico. El script de inicio puede utilizarse para iniciar aplicaciones. El script de detención puede utilizarse para realizar tareas de limpieza, como borrar archivos. El archivo utilizado debe ser accesible para todos los usuarios.

Parámetro predeterminado: [en blanco]

Tiempo de bloqueo de la sesión

Este control se utiliza para indicar el tiempo en minutos que permanecerá activa una sesión de Escritorio dinámico cuando no se utiliza la estación de trabajo. Si se excede ese tiempo, la estación de trabajo se bloquea.

Parámetro predeterminado: 10 minutos

Tiempo de desconexión de la sesión

Este control se utiliza para indicar el tiempo en minutos durante el que se ejecutará una sesión de Escritorio dinámico mientras el escritorio está bloqueado. Si se supera este tiempo, se termina la sesión y se inicia una nueva sesión cuando se desbloquea el escritorio.

Parámetro predeterminado: 5 minutos

Habilitar el indicador de sesiones

Este parámetro controla si se activa una ventana que identifica la sesión de Escritorio dinámico. Cuando se selecciona este parámetro, se muestra una ventana transparente y móvil en el escritorio durante las sesiones de Escritorio dinámico. Esta ventana muestra el nombre del usuario y el tiempo transcurrido de la sesión activa.

Parámetro predeterminado: seleccionado

Habilitar el gráfico

Este control se utiliza para indicar la ruta del archivo gráfico que se muestra en el indicador de sesión de Escritorio dinámico. El archivo especificado debe estar en una ubicación accesible para todos los usuarios y en el formato de archivo de mapa de bits de Windows (.bmp).

Hay un mapa de bits predeterminado, denominado Citrix.bmp, en la carpeta %Archivos de programa%\Citrix\MetaFrame Password Manager\Hot Desktop de cada estación de trabajo de Escritorio dinámico.

Parámetro predeterminado: [ninguno]

Licencias

Estos controles se utilizan para identificar el servidor de licencias y el modelo de licencias.

Inicio > Todos los programas > Consolas de administración > Citrix AppCenter > Single Sign-on > Configuraciones de usuario > [configuración] > Modificar configuración de usuario > Licencias

Importante: Las instancias de Single Sign-on Plug-in instaladas localmente no necesitan una licencia independiente para los usuarios que cuentan con acceso a las aplicaciones alojadas en entornos Citrix XenApp, Platinum Edition.

Nombre del servidor de licencias

Se debe identificar el nombre de dominio calificado (nombrehost.dominio.tld) asociado al servidor de licencias.

Parámetro predeterminado: [en blanco]

Usar el valor predeterminado (para el número de puerto del servidor de licencias)

Este parámetro se selecciona para utilizar el puerto de acceso predeterminado en el servidor de licencias. Si el servidor de licencias está escuchando en otro puerto, desactive este parámetro e ingrese el puerto en el campo correspondiente.

Parámetro predeterminado: seleccionado

Puerto predeterminado: 27000

Licencias de usuarios definidos

Esta opción se selecciona si se elije Single Sign-on Advanced como edición del producto. También se puede elegir esta opción si se selecciona la edición de producto como Single Sign-on Enterprise. Con este tipo de licencia, solo los usuarios específicos e identificados pueden utilizar Single Sign-on. Si esta opción está seleccionada, se debe especificar el período (en días, horas y minutos) durante el que la licencia está asignada al usuario definido antes de que caduque la licencia y el software del agente se vuelva a conectar al servidor de licencias. El usuario mantiene el control de la licencia durante el

período especificado incluso si se cierra el equipo del usuario.

Parámetro predeterminado: seleccionado en Single Sign-on Advanced Edition; no disponible en XenApp Platinum Edition

Parámetro de desconexión predeterminado: 21 días

licencia de usuarios concurrentes (sólo en Enterprise Edition y Platinum Edition)

Esta opción se habilita si se elije Single Sign-on Enterprise o XenApp Platinum como edición del producto. No está disponible si se elige Advanced Edition como la edición de producto.
Nota: Este modelo de licencias se encuentra habilitado si se ha actualizado el producto desde la versión 4.1 de Password Manager. Citrix Systems considera esta versión anterior como equivalente a Single Sign-on 5.0 Enterprise Edition en lo que se refiere a licencias cuando se realiza la actualización.
Con este tipo de licencia, varios usuarios pueden compartir una sola licencia de Single Sign-on (aunque no simultáneamente; este tipo se suele denominar licencia flotante).

Parámetro predeterminado: seleccionado en Single Sign-on Enterprise o XenApp Platinum Edition; no disponible en Single Sign-on Advanced Edition

Parámetro de desconexión predeterminado: 1 hora, 30 minutos si Permitir consumo de licencia para uso desconectado no está seleccionado; 21 días si Permitir consumo de licencia para uso desconectado está seleccionado

permitir consumo de licencia para uso desconectado

Esta opción estará disponible sólo si se ha seleccionado Licencias de usuarios concurrentes. Al seleccionar este parámetro se puede especificar el período durante el cual el usuario puede estar desconectado antes de que la licencia caduque y vuelva al grupo de licencias disponibles. Si se especifica, el usuario mantiene el control de la licencia durante el período especificado incluso si se cierra el equipo del usuario. El período predeterminado es de 1 hora y 30 minutos; el valor recomendado está entre 2 y 365 días.

Parámetro predeterminado: no seleccionado

Continuar sin validar la información de licencia

Este parámetro permite que el proceso de modificación continúe sin exigir un nombre y puerto del servidor de licencias válido.

Parámetro predeterminado: no seleccionado

Métodos de protección de datos

Oct 12, 2015

Estos parámetros se utilizan para seleccionar los métodos de protección de datos principales que se usarán para proteger las credenciales de los usuarios. En algunos entornos, los usuarios pueden utilizar más de un método.

Inicio > Todos los programas > Consolas de administración > Citrix AppCenter > Single Sign-on > Configuraciones de usuario > [configuración] > Modificar configuración de usuario > Métodos de protección de datos

¿Necesita regular el acceso del administrador de la cuenta a los datos del usuario?

Para impedir al acceso de los administradores a las credenciales de usuario, se debe seleccionar Sí. Si se selecciona esta opción, se desactivan las opciones de la API de protección de datos de Microsoft (incluida la selección DPAPI con perfil en el menú Origen de la clave de la tarjeta inteligente) y la opción No preguntar a los usuarios; restaurar la protección de datos primaria automáticamente en los parámetros de Protección de datos secundaria. Con esta configuración, el administrador de la cuenta, u otro administrador, no tiene acceso a las contraseñas o a los datos del usuario. Con este parámetro se evita que los administradores suplanten a los usuarios. El administrador no puede iniciar la sesión como el usuario con la configuración predeterminada ni acceder a los datos que se encuentran en el almacén de credenciales local.

Para permitir el uso de todas las funciones de autenticación múltiple disponibles aquí y los métodos de protección de datos secundaria en los parámetros de configuración de Protección de datos secundaria, se debe seleccionar No.

Parámetro predeterminado: Sí

Para mejorar la experiencia del usuario frente a los sucesos de inicio de sesión, seleccione todos los métodos de protección de datos que correspondan

Elija esta selección para utilizar las funciones de autenticación primaria que están disponibles en los parámetros que se describen en la siguiente tabla.

Parámetro predeterminado: seleccionado

Usar la protección de datos como en Password Manager 4.1 y versiones anteriores

Control	Descripción
Datos de autenticación de los usuarios	Se utiliza un secreto de usuario para acceder y proteger los datos del usuario. El secreto de autenticación puede ser una contraseña de usuario o un dispositivo basado en PIN empleado en el entorno. Parámetro predeterminado: seleccionado Para aumentar la protección de los datos de usuario, también se puede seleccionar lo siguiente: Permitir PIN de tarjetas inteligentes Al seleccionar esta opción se permite que se utilice el PIN de tarjetas inteligentes como secreto de usuario para la protección. Esta opción sólo se debe utilizar si la empresa o el entorno dispone de una directiva de “PIN seguro”.

Control	Descripción
	Parámetro predeterminado: no seleccionado Permitir la protección usando contraseñas en blanco Esta opción sólo se debe seleccionar si el dominio tiene unos requisitos de seguridad bajos y permite a los usuarios que tengan contraseñas de dominio en blanco. Si se selecciona esta opción y el software del plug-in detecta que el usuario tiene una contraseña en blanco, se deriva un secreto de usuario a partir del ID de usuario. Si no se selecciona esta opción, el software del plug-in no deriva un secreto de usuario ni realiza ninguna protección de datos con la contraseña en blanco. Si se selecciona Datos de autenticación de los usuarios y no se selecciona Permitir PIN de tarjetas inteligentes ni Permitir la protección usando contraseñas en blanco, después de que el usuario inicia la sesión por primera vez para la inscripción original y el proceso de registro utilizando una contraseña en blanco, se muestra un mensaje de error y el software del plug-in se desactiva. Parámetro predeterminado: no seleccionado
API de protección de datos de Microsoft	Esta opción se debe seleccionar si se utilizan perfiles móviles mediante un protocolo de autenticación de red Kerberos para los usuarios. La opción sólo funciona si hay perfiles móviles disponibles. Por ejemplo, si los usuarios utilizan contraseñas para acceder a sus equipos y un protocolo de autenticación de red Kerberos para acceder a una comunidad de equipos que ejecutan Citrix XenApp, se debe seleccionar Datos de autenticación de los usuarios y esta opción. Este método también permite el uso de credenciales de usuario y tarjetas inteligentes para iniciar la sesión. Parámetro predeterminado: no seleccionado
Certificados de tarjetas inteligentes	Al seleccionar esta opción, se permite a los usuarios que utilicen tarjetas criptográficas que permitan el cifrado y descifrado de datos de autenticación. Citrix recomienda que, si es posible, se seleccione esta opción si se utiliza Escritorio dinámico en el entorno. Parámetro predeterminado: no seleccionado

Para permitir que los usuarios usen un único método de autenticación primaria y/o se utilizan las versiones 4.0 o 4.1 del software de Password Manager Plug-in, se debe seleccionar esta opción y elegir un método del menú Origen de la clave de la tarjeta inteligente. Si se actualizó el almacén central de la versión 4.1 a la versión 5.0, esta opción se selecciona automáticamente.

Esta opción está disponible sólo cuando se usa el método de cifrado Triple DES.

Las opciones de Origen de la clave de la tarjeta inteligente son:

- PIN como contraseña

- Protección de datos de tarjeta inteligente
- DPAPI con perfil (no disponible si se selecciona No en ¿Necesita regular el acceso del administrador de la cuenta a los datos del usuario?

Parámetro predeterminado: no seleccionado

Protección de datos secundaria

Estas opciones permiten especificar funciones de protección de datos de credenciales secundaria que se utilizarán antes de desbloquear las credenciales de usuario cuando los usuarios cambien su autenticación primaria (por ejemplo, cuando cambien una contraseña de dominio o reemplacen una tarjeta inteligente). Alternativamente, también permite especificar la opción de que las credenciales se restauren automáticamente mediante la implementación del módulo de administración de claves.

Inicio > Todos los programas > Consolas de administración > Citrix AppCenter > Single Sign-on > Configuraciones de usuario > [configuración] > Modificar configuración de usuario > Protección de datos secundaria

Pedir a los usuarios que verifiquen su identidad

Parámetro predeterminado: seleccionado

Use este botón para seleccionar uno de los siguientes métodos de reautenticación:

Control	Descripción
Pedir al usuario que introduzca su contraseña anterior	Si se selecciona esta opción, los usuarios que han olvidado su contraseña anterior quedarán bloqueados y deberán volver a inscribir sus credenciales secundarias. Si los usuarios emplean tarjetas inteligentes para la autenticación primaria, no se debe seleccionar esta opción. Parámetro predeterminado: seleccionado
Pedir al usuario que elija el método: contraseña anterior o preguntas de seguridad	Si se selecciona esta opción, a los usuarios se les piden las credenciales según la opción de método de verificación que hayan elegido. Esta opción incluye la subopción siguiente: Usar verificación de identidad como en versiones anteriores Password Manager Si se ha actualizado desde las versiones 4.0 ó 4.1 de Password Manager y se ha activado la autenticación con preguntas o las preguntas de verificación de identidad, se debe seleccionar esta opción. En este caso, las versiones 4.0 y 4.1 del software del plug-in no necesitan acceder al servicio. Parámetro predeterminado: no seleccionado

No preguntar a los usuarios; restaurar la protección de datos primaria automáticamente

Seleccione esta opción cuando implemente el módulo del servicio de administración de claves para omitir la verificación de identidad y desbloquear las credenciales de usuario automáticamente. Este método es menos seguro que los demás métodos de protección de datos, pero aumenta la facilidad de uso de los usuarios al recuperar las credenciales automáticamente.

Parámetro predeterminado: no seleccionado

Funciones de Self-Service

Las opciones disponibles en esta sección requieren la instalación del módulo de servicio de administración de claves. Este módulo inserta un botón en el cuadro de diálogo de inicio de sesión de Windows que se utiliza para que los usuarios restablezcan sus contraseñas.

Inicio > Todos los programas > Consolas de administración > Citrix AppCenter > Single Sign-on > Configuraciones de usuario > [configuración] > Modificar configuración de usuario > Funciones de autoservicio

Permitir que los usuarios restablezcan sus contraseñas primarias

Al seleccionar este parámetro se permite a los usuarios que cambien su contraseña de dominio primaria sin intervención administrativa.

Parámetro predeterminado: no seleccionado

Permitir que los usuarios desbloqueen sus cuentas

Al seleccionar esta opción se permite que los usuarios desbloqueen sus cuentas de dominio.

Parámetro predeterminado: no seleccionado

Módulo de administración de claves

Estos controles identifican la ubicación y el puerto del servicio para el módulo de administración de claves.

Inicio > Todos los programas > Consolas de administración > Citrix AppCenter > Single Sign-on > Configuraciones de usuario > [configuración] > Modificar configuración de usuario > Módulo de administración de claves

Ubicación del servicio (módulo de administración de claves)

Este parámetro se utiliza para identificar la ubicación y el puerto del servicio para el módulo de administración de claves. Use el botón Validar para asegurarse de que los parámetros son válidos.

Parámetro predeterminado: [en blanco]

puerto del servicio: 443

Módulo de aprovisionamiento

El módulo de aprovisionamiento permite importar, modificar y quitar las credenciales asociadas a los usuarios en esta configuración de usuario. En esta página es necesario especificar la ubicación y el puerto de servicio del módulo de aprovisionamiento.

Inicio > Todos los programas > Consolas de administración > Citrix AppCenter > Single Sign-on > Configuraciones de usuario > [configuración] > Modificar configuración de usuario > Módulo de aprovisionamiento

Usar el aprovisionamiento

Al seleccionar este parámetro se puede utilizar el aprovisionamiento.

Parámetro predeterminado: no seleccionado

Ubicación del servicio (módulo de aprovisionamiento)

Este parámetro se utiliza para identificar la ubicación y el puerto del servicio para el módulo de aprovisionamiento. Use el botón Validar para asegurarse de que los parámetros son válidos.

Parámetro predeterminado: [en blanco]

puerto del servicio: 443

Definiciones de aplicación

Oct 12, 2015

En esta sección se describen los parámetros y controles de una definición de aplicación. Todas las sugerencias de exploración ofrecidas en este tema se efectúan en una definición de aplicación cuando se realiza una función de edición.

Formularios de aplicación

Estos controles configuran las reglas que especifican el tamaño de la contraseña y la repetición de caracteres.

Inicio > Todos los programas > Citrix > Consolas de administración > Citrix AppCenter > Single Sign-on > Definiciones de aplicación > [definición] > Modificar la definición de aplicación > Formularios de aplicación > [formulario definido] > Modificar > Otros parámetros

Enviar automáticamente este formulario

Este parámetro se utiliza para especificar si el plug-in pulsa automáticamente el botón de envío o si el usuario debe pulsar manualmente el botón. Para que el formulario se envíe automáticamente sin intervención del usuario, se debe seleccionar la casilla de verificación Enviar automáticamente este formulario.

Parámetro predeterminado: seleccionado

Icono de la aplicación

Este control se utiliza para identificar el icono que se mostrará junto a la aplicación en la ventana Administrar contraseñas (anteriormente conocida como Administrador de inicios de sesión).

Inicio > Todos los programas > Citrix > Consolas de administración > Citrix AppCenter > Single Sign-on > Definiciones de aplicación > [definición] > Modificar la definición de aplicación > Icono de la aplicación

Icono de la aplicación

Este parámetro controla el icono de la aplicación que se mostrará junto al nombre de la aplicación en la ventana Administrar contraseñas (anteriormente conocida como Administrador de inicios de sesión). Hay dos opciones disponibles:

- Usar el icono predeterminado
- Usar un icono especial (ingrese la ruta del icono).

Si se va a utilizar un icono personalizado, se debe usar la función de búsqueda para identificar la ruta al archivo de icono. Se puede identificar cualquier archivo de icono de Windows estándar. Se admiten las variables de entorno de Microsoft Windows.

Parámetro predeterminado: usar el icono predeterminado

Detección avanzada

Estos controles se usan para forzar al plug-in a ignorar formularios posteriores de inicio de sesión o de cambio de contraseña durante la sesión de la aplicación cuando ya se procesaron los mismos.

Inicio > Todos los programas > Citrix > Consolas de administración > Citrix AppCenter > Single Sign-on > Definiciones de aplicación > [definición] > Modificar la definición de aplicación > Detección de la aplicación

Procesar solamente el primer inicio de sesión de esta aplicación

Al seleccionar este control sólo se procesa el primer inicio de sesión de esta aplicación y se ignoran las peticiones de inicio de sesión posteriores.

Parámetro predeterminado: No seleccionado

Procesar solamente el primer cambio de contraseña de esta aplicación

Al seleccionar este control sólo se procesa la primera petición de cambio de contraseña de esta aplicación y se ignoran las peticiones de cambio de contraseña posteriores.

Parámetro predeterminado: No seleccionado

Caducidad de contraseñas

Estos controles se usan para especificar los parámetros de esta aplicación cuando caduca la contraseña. La política de caducidad de Single Sign-on sólo se aplica si se selecciona en la directiva de contraseñas asociada a esta aplicación.

Inicio > Todos los programas > Citrix > Consolas de administración > Citrix AppCenter > Single Sign-on > Definiciones de aplicación > [definición] > Modificar la definición de aplicación > Caducidad de contraseñas

Ejecutar un script cuando caduque la contraseña

Para ejecutar un archivo de script específico cuando caduque la contraseña, se debe seleccionar este parámetro e identificar el script y su ruta absoluta. No utilice una ruta UNC (Convención de nomenclatura universal).

Parámetro predeterminado: No seleccionado

Usar la advertencia de caducidad de Citrix Single Sign-on

Para usar la advertencia de caducidad de Single Sign-on cuando caduque la contraseña, se debe seleccionar este parámetro.

Parámetro predeterminado: No seleccionado

Directivas de contraseña

Oct 12, 2015

En esta sección se describen los parámetros y controles de directiva de contraseña. Todas las sugerencias de exploración ofrecidas en esta sección se efectúan en una directiva de contraseña existente cuando se realiza una función de edición. Para acceder al cuadro de diálogo Modificar directiva de contraseñas, utilice la siguiente ruta:

Inicio > Todos los programas > Citrix > Consolas de administración > Citrix AppCenter > Single Sign-on > Directivas de contraseña > [directiva] > Modificar directiva de contraseñas

Reglas básicas de las contraseñas

Estos controles configuran las reglas que especifican el tamaño de la contraseña y la repetición de caracteres.

Inicio > Todos los programas > Citrix > Consolas de administración > Citrix AppCenter > Single Sign-on > Directivas de contraseña > [directiva] > Modificar la directiva de contraseñas > Reglas básicas de las contraseñas

Tamaño mínimo de la contraseña

Indica la cantidad mínima de caracteres necesarios para la contraseña. Valor mínimo permitido = 0. Valor máximo permitido = 128.

parámetro predeterminado: 8

Tamaño máximo de la contraseña

Indica el número máximo de caracteres permitidos para la contraseña. Valor mínimo permitido = 1. Valor máximo permitido = 128.

parámetro predeterminado: 20

Cantidad máxima de veces que se puede usar un carácter

Indica la cantidad máxima de veces que se puede repetir un carácter en una contraseña. Valor mínimo permitido = 1. Valor máximo permitido = 128.

parámetro predeterminado: 6

Cantidad máxima de veces que se puede usar el mismo carácter sucesivamente

Especifica la cantidad máxima de veces que se puede usar el mismo carácter secuencialmente. Valor mínimo permitido = 1. Valor máximo permitido = 128.

parámetro predeterminado: 4

Reglas de uso de caracteres alfabéticos

Estos controles configuran las reglas que especifican el uso de letras en las contraseñas.

Inicio > Todos los programas > Citrix > Consolas de administración > Citrix AppCenter > Single Sign-on > Directivas de contraseña > [directiva] > Modificar la directiva de contraseñas > Reglas de uso de caracteres alfabéticos

Permitir minúsculas

Controla si se usarán minúsculas en las contraseñas.

parámetro predeterminado: permitir minúsculas

La contraseña puede comenzar con una minúscula

Controla si las contraseñas pueden comenzar con una minúscula.

parámetro predeterminado: la contraseña puede comenzar con una minúscula

La contraseña puede terminar con una minúscula

Controla si las contraseñas pueden finalizar con una minúscula.

parámetro predeterminado: la contraseña puede finalizar con una minúscula

Cantidad mínima de minúsculas necesarias

Indica el número mínimo de letras minúsculas necesarias para una contraseña. Valor mínimo permitido = 0. Valor máximo permitido = 128.

parámetro predeterminado: 0

Permitir mayúsculas

Controla si se usarán mayúsculas en las contraseñas.

parámetro predeterminado: permitir mayúsculas

La contraseña puede comenzar con una mayúscula

Controla si las contraseñas pueden comenzar con una mayúscula.

parámetro predeterminado: la contraseña puede comenzar con una mayúscula

La contraseña puede terminar con una mayúscula

Controla si las contraseñas pueden finalizar con una mayúscula.

parámetro predeterminado: la contraseña puede finalizar con una mayúscula

Cantidad mínima de mayúsculas necesaria

Indica la cantidad mínima de letras mayúsculas necesarias para una contraseña. Valor mínimo permitido = 0. Valor máximo permitido = 128.

parámetro predeterminado: 0

Reglas de uso de números

Estos controles configuran las reglas que especifican el uso de números (0-9) en las contraseñas.

Inicio > Todos los programas > Citrix > Consolas de administración > Citrix AppCenter > Single Sign-on > Directivas de contraseña > [directiva] > Modificar la directiva de contraseñas > Reglas de uso de números

Permitir números

Controla si se usarán números en las contraseñas.

parámetro predeterminado: permitir números

La contraseña puede comenzar con un número

Controla si las contraseñas pueden comenzar con un número.

parámetro predeterminado: la contraseña puede comenzar con un número

La contraseña puede terminar con un número

Controla si las contraseñas pueden terminar con un número.

parámetro predeterminado: la contraseña puede terminar con un número

Cantidad mínima de números necesarios

Indica la cantidad mínima de caracteres numéricos necesarios en una contraseña. Valor mínimo permitido = 0. Valor máximo permitido = 128.

parámetro predeterminado: 0

Cantidad máxima de números permitida

Indica la cantidad máxima de caracteres numéricos permitidos en una contraseña. Valor mínimo permitido = 1. Valor máximo permitido = 128.

parámetro predeterminado: 20

Reglas de uso de caracteres especiales

Estos controles configuran las reglas que especifican el uso de caracteres especiales (ni alfabéticos ni numéricos) en las contraseñas.

Inicio > Todos los programas > Citrix > Consolas de administración > Citrix AppCenter > Single Sign-On > Directivas de contraseña > [directiva] > Modificar directiva de contraseñas > Reglas de uso de caracteres especiales

Permitir caracteres especiales

Controla si se pueden usar caracteres especiales (ni alfabéticos ni numéricos) en las contraseñas.

parámetro predeterminado: permitir números

La contraseña puede comenzar con un carácter especial

Controla si las contraseñas pueden comenzar con un carácter especial.

parámetro predeterminado: la contraseña puede comenzar con un carácter especial

La contraseña puede terminar con un carácter especial

Controla si las contraseñas pueden terminar con un carácter especial.

parámetro predeterminado: la contraseña puede finalizar con un carácter especial

Cantidad mínima de caracteres especiales necesaria

Indica la cantidad mínima de caracteres especiales necesarios en una contraseña. Valor mínimo permitido = 0, Valor máximo permitido = 128.

parámetro predeterminado: 0

Cantidad máxima de caracteres especiales permitida

Indica la cantidad máxima de caracteres especiales permitidos en una contraseña. Valor mínimo permitido = 0, Valor máximo permitido = 128.

parámetro predeterminado: 20

Lista de caracteres especiales permitidos

Indica los caracteres especiales permitidos en una contraseña.

Parámetro predeterminado: !@#$^&*()_-+=[]\|,?

Reglas de exclusión

Estos controles especifican los caracteres y cadenas de caracteres que no se permiten en las contraseñas.

Inicio > Todos los programas > Citrix > Consolas de administración > Citrix AppCenter > Single Sign-on > Directivas de contraseña > [directiva] > Modificar la directiva de contraseñas > Reglas de exclusión

Excluir la siguiente lista de caracteres o grupos de caracteres de las contraseñas

Seleccione la opción Editar lista para abrir el cuadro de diálogo Editar lista de exclusiones que se utiliza para especificar hasta 256 caracteres individuales o grupos de caracteres que no se permiten en las contraseñas. Introduzca un carácter o grupo de caracteres por línea. Cada grupo puede contener hasta 32 caracteres. Los caracteres individuales o grupos de caracteres no distinguen entre mayúsculas y minúsculas.

parámetro predeterminado: [en blanco]

No permitir el nombre de usuario de la aplicación en la contraseña

Controla si el nombre de usuario de la aplicación está prohibido en la contraseña. Al seleccionar esta casilla de verificación se permite el nombre de usuario de la aplicación en la contraseña.

parámetro predeterminado: no seleccionado

No permitir porciones del nombre de usuario de la aplicación en la contraseña

Controla si se permiten partes del nombre de usuario de la aplicación en la contraseña. Esto incluirá todos los grupos de caracteres posibles que puedan tomarse del nombre de usuario. Este parámetro está estrechamente ligado al parámetro Cantidad de caracteres en las porciones. Por ejemplo, cuando se selecciona este parámetro y Cantidad de caracteres en las porciones se configura en 4, no se permitirá una contraseña que incluya grupos de caracteres de “citr”, “itri” o “trix” para un usuario de Windows con el nombre “citrix”.

parámetro predeterminado: no seleccionado

No permitir el nombre de usuario de Windows en la contraseña

Controla si se prohíbe usar el nombre de usuario de Windows en la contraseña. Si no está seleccionado, se permite el nombre de usuario de Windows en la contraseña. Este parámetro está estrechamente ligado con el parámetro Cantidad de caracteres en las porciones. Por ejemplo, cuando se selecciona este parámetro y Cantidad de caracteres en las porciones se configura en 4, no se permitirá una contraseña que incluya grupos de caracteres de “citr”, “itri” o “trix” para un usuario con el nombre de usuario de Windows “citrix”.

parámetro predeterminado: no seleccionado

Historial y caducidad de contraseñas

Estos controles especifican si una contraseña nueva puede ser igual que otra anterior y el parámetro de caducidad de contraseña.

El historial de contraseñas se mantiene por usuario. Si se restablecen los datos de un usuario, el historial de contraseñas se elimina y no se puede aplicar para las contraseñas eliminadas.

La opción Caducidad de contraseñas sólo notifica a los usuarios que una contraseña está a punto de caducar o que ya ha caducado. Los usuarios pueden utilizar las credenciales caducadas, pero reciben avisos de cambio de contraseñas o solicitudes de cambio de contraseña hasta que se cambia la contraseña en la ventana Administrar contraseñas (anteriormente conocida como Administrador de inicios de sesión).

Inicio > Todos los programas > Citrix > Consolas de administración > Citrix AppCenter > Single Sign-on > Directivas de contraseña > [directiva] > Modificar directiva de contraseñas > Historia y caducidad de contraseñas

La nueva contraseña no puede ser igual a las anteriores

Controla si la contraseña nueva puede ser la misma que una anterior. Las contraseñas anteriores se guardan en un historial de contraseñas.

parámetro predeterminado: la nueva contraseña puede ser la misma que la anterior (no está seleccionada la casilla de verificación)

Cantidad de contraseñas anteriores recordadas

Especifica la cantidad de contraseñas anteriores que se guardarán en el historial de contraseñas. El valor mínimo permitido es 1. El valor máximo permitido es 24.

parámetro predeterminado: 1

Usar los parámetros de caducidad de contraseña asociados con las definiciones de aplicación

Cuando se selecciona esta opción, los parámetros (Cantidad de días hasta que caduque la contraseña y Cantidad de días antes de que caduque la contraseña que se advertirá al usuario) especificados aquí se aplican a las definiciones de aplicación asociados a esta directiva. La directiva de Single Sign-on funciona independientemente de cualquier directiva de caducidad de contraseñas incorporada en la aplicación.

parámetro predeterminado: no se especifica la caducidad de contraseñas (no está seleccionada la casilla de verificación)

Cantidad de días hasta que caduque la contraseña

Indica la cantidad máxima de días que la contraseña puede permanecer sin cambiar. El valor mínimo permitido es 1. El valor máximo permitido es 99999.

parámetro predeterminado: 42

Cantidad de días antes de que caduque la contraseña que se advertirá al usuario

Indica cuántos días antes de que caduque una contraseña el usuario empezará a recibir advertencias al respecto. El valor mínimo permitido es 0. El valor máximo permitido es 99998.

parámetro predeterminado: 14

Probar directiva de contraseñas

Estos controles se utilizan para probar una contraseña generada manualmente para verificar el cumplimiento de la directiva definida, generar automáticamente una contraseña compatible y verificar que las restricciones definidas no limitan la capacidad de generar suficientes contraseñas para la organización.

Inicio > Todos los programas > Citrix > Consolas de administración > Citrix AppCenter > Single Sign-on > Directivas de contraseña > [directiva] > Modificar directiva de contraseñas > Probar directiva de contraseñas

Comprobar si una contraseña manual cumple con la directiva

Este campo se utiliza para comprobar si una contraseña manual cumple con la directiva. Introduzca la contraseña creada manualmente y haga clic en Probar. La contraseña introducida se prueba con todos los criterios definidos.

parámetro predeterminado: ninguno

Generar una contraseña aleatoria

Este control se utiliza para generar una contraseña que cumpla con los criterios de contraseña definidos actualmente. Haga clic en Generar para generar una contraseña compatible que se pueda copiar del campo (Ctrl-C).

parámetro predeterminado: ninguno

Generar y probar varias contraseñas únicas que cumplan con las directivas

Se puede definir un conjunto de restricciones de contraseña que admita una cantidad limitada de posibilidades totales de

contraseña. Este control se usa para generar una cantidad definida por el usuario de contraseñas compatibles para determinar si la directiva definida es lo suficientemente flexible como para cumplir las necesidades de la organización. Haga clic en Generar varias contraseñas para abrir un cuadro de diálogo en el que generar una cantidad definida por el usuario de contraseñas.

parámetro predeterminado: ninguno

Preferencias de inicio de sesión

Estos controles se utilizan para definir si la opción Revelar está disponible para las definiciones de aplicación que utilizan esta directiva, obligar a que el usuario se vuelva a autenticar antes de enviar las credenciales de aplicación, configurar la cantidad de reintentos de inicio de sesión y establecer el tiempo que tiene el usuario para autenticarse correctamente después de que falle un intento de autenticación.

Inicio > Todos los programas > Citrix > Consolas de administración > Citrix AppCenter > Single Sign-on > Directivas de contraseña > [directiva] > Modificar la directiva de contraseñas > Preferencias de inicio de sesión

Permitir que los usuarios revelen las contraseñas de las aplicaciones

Este control se utiliza para determinar si el botón Revelar de la ventana Administrar contraseñas (anteriormente conocida como Administrador de inicios de sesión) estará disponible para las aplicaciones administradas con la directiva. Cuando los usuarios seleccionan el botón Revelar en la ventana Administrar contraseñas, pueden ver su contraseña en texto sin cifrar. Si no se selecciona este parámetro, los usuarios no podrán revelar sus contraseñas.

parámetro predeterminado: no se muestra el botón Revelar (no está marcada la casilla de verificación)

Hacer que el usuario tenga que volver a autenticarse antes de enviar las credenciales de la aplicación

Este control se utiliza para determinar si los usuarios deben introducir sus credenciales primarias de inicio de sesión antes de que el plug-in envíe las credenciales a la aplicación. Si este parámetro está seleccionado, Single Sign-on Plug-in bloquea inmediatamente la estación de trabajo cuando reconoce una aplicación para la que se ha seleccionado esta opción. Los usuarios deben introducir sus credenciales primarias para desbloquear la estación de trabajo. Si se desbloquea la estación de trabajo con las credenciales adecuadas, el plug-in envía las credenciales de usuario a la aplicación. Este parámetro es útil para aplicaciones desde las que se accede a información confidencial o de mucha importancia porque obliga a los usuarios a verificar su identidad antes de que el plug-in envíe las credenciales a la aplicación.

parámetro predeterminado: el usuario no se tiene que volver a autenticar (no está seleccionada la casilla de verificación)

Número de reintentos de inicio de sesión

Este control se utiliza para configurar la cantidad de veces adicionales que el software del plug-in puede enviar las credenciales de usuario a la misma aplicación dentro del límite de tiempo especificado. Si se establece en el valor mínimo de 0, los usuarios reciben un mensaje de error cuando intentan enviar credenciales a la aplicación por segunda vez.

parámetro predeterminado: 0

Límite de tiempo para la cantidad de reintentos

Este control se utiliza para indicar el tiempo (en segundos) durante el cual el usuario podrá enviar las credenciales de usuario

a la misma aplicación después de que falle el envío inicial de credenciales.

parámetro predeterminado: 30 segundos

Asistente para el cambio de contraseñas

Este control se utiliza para determinar cómo responde el asistente de cambio de contraseñas a los formularios de cambio de contraseña. Se debe configurar una de las cuatro opciones posibles:

- Permitir que los usuarios elijan una contraseña generada por el sistema o creen su propia contraseña
- Sólo creadas por el usuario
- Generadas automáticamente, informando al usuario
- Generar una contraseña y enviarla a la aplicación sin mostrar el Asistente para el cambio de contraseñas

Inicio > Todos los programas > Citrix > Consolas de administración > Citrix AppCenter > Single Sign-on > Directivas de contraseña > [directiva] > Modificar la directiva de contraseñas > Asistente para el cambio de contraseñas

Permitir que los usuarios elijan una contraseña generada por el sistema o creen su propia contraseña

Al seleccionar esta opción, el asistente para el cambio de contraseñas permite que los usuarios elijan una contraseña generada por el sistema o creen su propia contraseña.

parámetro predeterminado: seleccionado

Sólo creadas por el usuario

Al seleccionar esta opción, el asistente para el cambio de contraseñas no permite que los usuarios elijan una contraseña generada por el sistema y hace que introduzcan una propia.

parámetro predeterminado: no seleccionado

Generadas automáticamente, informando al usuario

Al seleccionar esta opción, el Asistente para el cambio de contraseñas usará automáticamente una contraseña generada por el sistema sin permitir que los usuarios creen su propia contraseña.

parámetro predeterminado: no seleccionado

Generar una contraseña y enviarla a la aplicación sin mostrar el asistente para el cambio de contraseñas

Al seleccionar esta opción, Single Sign-on Plug-in envía automáticamente una contraseña generada por el sistema sin mostrar el asistente para el cambio de contraseñas al usuario. El usuario puede ver los campos de la pantalla de cambio de contraseña rellenados y el resultado de la aplicación que indica si la contraseña se ha cambiado correctamente.

parámetro predeterminado: no seleccionado

Operaciones

Oct 12, 2015

Single Sign-on registra sucesos generados por el plug-in o por el usuario en el registro de sucesos de Windows del equipo host. Los sucesos se clasifican como información, advertencias o errores. Los sucesos de errores y advertencias siempre se registran. De forma predeterminada, el registro de sucesos de información se encuentra desactivado pero es posible activarlo en la consola después de crear la configuración de usuario.

Single Sign-on registra los sucesos de funciones como Escritorio dinámico, tarjetas inteligentes, licencias y Servicio Single Sign-on. El registro de sucesos detecta y verifica sucesos relacionados con la seguridad que pueden ser necesarios para garantizar la conformidad normativa; por ejemplo, con el estándar FIPS (Federal Information Processing Standard), o con el Decreto de 1996 de HIPAA (Health Insurance Portability and Accountability). Las funciones de registro de sucesos de Single Sign-on también contribuyen a mejorar la seguridad de los sistemas.

Si se está utilizando Single Sign-on en un entorno de XenApp, el registro de sucesos identifica la información de usuario y de sesión. Se registran todos los intentos sin éxito de inicio de sesión.

Para activar el registro de sucesos de información:
1. En la consola, busque la configuración de usuario y en el menú Acción, haga clic en Editar configuración de usuario.
2. En las propiedades de la configuración del usuario, seleccione Interacción en el cliente.
3. Haga clic en Registrar los sucesos de Single Sign-on Plug-in usando el registro de Windows.

La siguiente tabla contiene algunos sucesos estándar que registra Single Sign-on:

Tipo de sucesos estándar
Intentos fallidos de inicio de sesión (autenticación en el software del plug-in)
Se registra si falla la autenticación de usuario en Single Sign-on. No se puede abrir el almacén de credenciales.
Intentos satisfactorios de inicio de sesión (autenticación en el software del plug-in)
Se registra si no hay fallos de autenticación y el usuario accede sin problemas al almacén central.
Intento de inicio de sesión (envío de credenciales)
Se registra si se producen intentos de enviar credenciales a una aplicación externa.
Operaciones con credenciales
Se registra en caso de operaciones relacionadas con las contraseñas (como cambiar y divulgar contraseñas y verificar la identidad).
Errores de sincronización (comunicación)

Tipo de sucesos estándar
Se registra si se producen errores de sincronización con el almacén central debido a problemas de comunicación.
Errores de sincronización (permisos)
Se registra si se producen errores de sincronización con el almacén central debido a credenciales de usuario incorrectas.
Error de cifrado/descifrado de DataProtect en tarjeta inteligente
Se registra si se produce un error general asociado con el cifrado o descifrado de los datos de una tarjeta inteligente.
Error de cifrado/descifrado de DataProtect en tarjeta inteligente (falta tarjeta)
Se registra cuando la tarjeta inteligente no está disponible.
Inicio y cierre del software del plug-in
Se registra cuando la tarjeta inteligente no está disponible.
Archivos .dll inexistentes o dañados
Se registra cuando no se puede cargar un archivo .dll correctamente.

La tabla siguiente contiene algunos sucesos de Escritorio dinámico que registra Single Sign-on.

Tipo de sucesos de Escritorio dinámico
Error de inicio de sesión en Escritorio dinámico
Se registra sólo si se produce un error grave al iniciar la sesión.
Inicio de sesión satisfactorio en Escritorio dinámico
Se registra cuando el Escritorio dinámico inicia una sesión tras una autenticación de usuario satisfactoria.
Error de cierre de sesión de Escritorio dinámico
Se registra si se produce un error grave al cerrar la sesión.

Cierre de sesión satisfactorio en Escritorio dinámico
Tipo de sucesos de Escritorio dinámico
Se registra si la sesión se cierra satisfactoriamente a petición del usuario o al alcanzar el tiempo de desconexión de la sesión.

Archivo Mfrmlist.ini

Feb 06, 2011

El archivo Mfrmlist.ini contiene una lista de los emuladores de terminal y las ubicaciones de la dll de HLLAPI que supervisa el software de Single Sign-on Plug-in. El archivo se encuentra en:

%Archivos de programa%\Citrix\MetaFrame Password Manager\Helper\MFEmu

El software de Single Sign-On Plug-in no envía credenciales

Mar 24, 2011

En algunos casos, el Single Sign-on Plug-in no envía las credenciales de un usuario a una aplicación configurada. Este problema puede deberse a un número de razones, como por ejemplo:

- Cambios en la aplicación Web que generan una definición de aplicación desactualizada.
- La configuración involuntaria de un parámetro al crear una definición de aplicación.

Realice las siguientes actividades iniciales para determinar la causa del error de envío:

- Compruebe si existen conflictos en los parámetros.
- Verifique que el software del plug-in está configurado para detectar aplicaciones.
- Compare el plug-in y las definiciones de la consola Single Sign-on.
- Elimine los campos de envío y criterios de coincidencia uno por vez hasta que el plug-in inicie el envío de las credenciales.

Importante: Single Sign-on contiene muchos parámetros que ayudan a crear definiciones de aplicación, directivas de contraseñas, configuraciones de usuario y métodos de verificación de identificación. Se pueden crear parámetros contradictorios que podrían provocar, por ejemplo, que las credenciales no se envíen a una aplicación.
Si el Single Sign-on Plug-in sigue sin enviar las credenciales del usuario, pruebe las siguientes técnicas de resolución de problemas para las aplicaciones Web y basadas en emuladores de terminal.

Aplicaciones Web

- Comprobación de que StrictURL se utiliza correctamente
  1. En el componente Single Sign-on de AppCenter, seleccione la aplicación Web que desea visualizar.
  2. En el menú Acción, haga clic en Modificar definición de aplicación.
  3. Haga clic en Formularios de aplicación, elija un formulario de aplicación y, a continuación, en Editar.
  4. Haga clic en Identidad del formulario. Aquí puede activar la coincidencia de URL estricta así como la función de reconocer mayúsculas de minúsculas en las URL.
  5. Asegúrese de que las páginas utilizan tipos de campo compatibles con HTML. Las definiciones de aplicación Web requieren tipos de campo compatibles con HTML. No se detectan los tipos de campo no definidos ni los definidos por el usuario.

- Cuando utilice InPrivate Browsing en Internet Explorer 8, asegúrese de que Desactivar barras de herramientas y extensiones cuando se inicia InPrivate Browsing no esté seleccionado. Consulte el sitio Web de Microsoft para conocer los detalles de las funciones de privacidad de Internet Explorer.

Aplicaciones de emulador de terminal

Cree definiciones de aplicaciones de emulador de terminal utilizando el asistente de definición de aplicaciones y el asistente de definición de formularios. Al agregar la definición de aplicación a una configuración de usuario, asegúrese de activar la compatibilidad con los emuladores de terminal.

- Compruebe que el emulador de terminal está configurado en el archivo Mfrmlist.ini
  El proceso Ssomho.exe que controla la interacción de Single Sign-on con los emuladores de terminal reconoce sólo los emuladores definidos en el archivo Mfrmlist.ini. Si el emulador de terminal compatible no está definido en este archivo, el proceso Ssomho.exe no intenta comunicarse con el emulador.

- Compruebe que se ha especificado un nombre de sesión corto

El proceso Ssomho.exe utiliza el nombre de sesión corto para comunicarse con la dll de HLLAPI. Sin un nombre de sesión corto, Ssomho.exe se carga pero no puede controlar la actividad de la pantalla, por lo que es necesario configurar el nombre de sesión corto en el emulador del dispositivo cliente.

- Compruebe que el proceso Ssomho.exe está en ejecución
  Siga estas instrucciones para asegurarse de que Ssomho.exe está en ejecución:
  1. En el equipo con el software de Single Sign-on Plug-in, abra el Administrador de tareas y seleccione la ficha Procesos.
  2. Haga clic en el encabezado Nombre de imagen para ordenar los procesos por nombre de imagen.
  3. Compruebe que Ssomho.exe está en la lista.

  Si el proceso Ssomho.exe no aparece en la lista, podría no encontrarse ninguna dll de HLLAPI o podría finalizar antes de tiempo por problemas relacionados con emuladores de terminal de otros fabricantes.

  Nota: Aunque el proceso Ssomho.exe aparezca en la lista, podría no comunicarse correctamente con la dll de HLLAPI. Compruebe que el nombre corto de sesión es correcto antes de buscar otra solución al problema.
- Pruebe cada emulador por separado
  Si hay instalados varios emuladores compatibles en el mismo sistema, Ssomho.exe intentará comunicarse con todos ellos. En ocasiones, una de las implementaciones de dll de HLLAPI puede provocar la inestabilidad de Ssomho.exe. En ese caso, es necesario probar cada emulador de terminal por separado eliminando el resto de los emuladores de terminal o convirtiendo en comentarios las entradas y cambiando su secuencia en el archivo Mfrmlist.ini.

  Este paso es muy útil para verificar que el proceso ssomho no se está conectando a un emulador distinto al que presenta el problema.

Compatibilidad con emuladores de terminal

May 11, 2015

Para activar la compatibilidad HLLAPI para cualquier emulador de terminal en Single Sign-on, es necesario activar la compatibilidad con los emuladores de terminal en la consola.

Si se activa el soporte de emuladores de terminal, SSOShell inicia el proceso Ssomho.exe. En primer lugar, este proceso lee el archivo Mfrmlist.ini ubicado en %Archivos de programa%\Citrix\MetaFrame Password Manager\Helper\MFEmu y, a continuación, busca todos los emuladores configurados e intenta cargar el archivo .dll compatible con HLLAPI asignado en el archivo.

El archivo Mfrmlist.ini puede ampliarse para admitir otros emuladores compatibles con HLLAPI.

El proceso Ssomho.exe busca en el subárbol del Registro HKEY_LOCAL_MACHINE\SOFTWARE la ubicación del archivo .dll compatible con HLLAPI a menos que se especifique lo contrario en el archivo Mfrmlist.ini.

Algunos emuladores lo buscan en el subárbol HKEY_CURRENT_USER. Para estos emuladores, especifique manualmente la ubicación del archivo DLL utilizando el parámetro de ruta explícito en el archivo mfrmlist.ini.

Para configurar la compatibilidad con emuladores

Para que funcione con los programas de emulación de terminal puestos a prueba, la configuración de Single Sign-on implica varios pasos. Este proceso requiere que se instale el software del emulador, se cree una sesión de emulador para usar con Single Sign-on y se configure Single Sign-On con una definición de aplicación de emuladores de terminal que use coincidencias de texto para reconocer una sesión de emulador en particular.

1. Instale el emulador de terminal y reinicie el equipo.
2. Inicie el emulador de terminal y cree una sesión nueva definiendo la pantalla y la conexión.
3. Establezca el nombre corto de sesión.
4. Habilite la compatibilidad con la API HLLAPI.
   Nota: Se necesita una definición de aplicación de emuladores de terminal independiente para cada sesión única que vaya a utilizarse con Single Sign-on. El software del plug-in detecta las sesiones mediante la coincidencia del texto de la pantalla de la aplicación de emulador de terminal con el texto de una fila y columna específicas facilitado en la definición de la aplicación. Single Sign-on envía las credenciales según la información de fila y columna facilitada en la definición de la aplicación. Por lo tanto, cada sesión requiere su propia definición de aplicación host.
5. Guarde la sesión y ciérrela.
6. Cierre el emulador de terminal.
7. Cree una definición de aplicación para la aplicación host.
8. Abra la consola y compruebe que se ha activado el soporte de emuladores de terminal en las configuraciones de usuario apropiadas.
9. Ejecute el emulador y abra la sesión.
10. Inicie o actualice el software de Single Sign-on Plug-in.

El plug-in reconocerá la pantalla de conexión y mostrará un formulario en el que podrá introducir y guardar sus credenciales.

El software de Single Sign-On Plug-in no se inicia

Feb 07, 2011

El software de Single Sign-on Plug-in debe ser el último software de alteración de GINA instalado en los dispositivos de usuario que no incluyan Windows Server 2008, Windows Server 2008 R2, Windows Vista o Windows 7. Si el software de Single Sign-on Plug-in se instaló pero no se inicia como es de esperar, puede deberse a una cadena GINA rota. Esto ocurre cuando el software que se instala o se actualiza después del software deSingle Sign-on Plug-in modifica la cadena GINA de Windows. Los paquetes de software que permiten la autenticación con tarjetas inteligentes, Symantec y XenApp también alteran la cadena GINA de Windows.

Si ya se ha instalado Single Sign-on y se desea instalar o actualizar un software que altera la cadena GINA de Windows, se recomienda desinstalar el software de Single Sign-on Plug-in primero. Cuando desinstale el software de Single Sign-on Plug-in, instale (o actualice) el nuevo software y luego instale el software de Single Sign-on Plug-in. De esta forma se instalará el archivo .dll correcto y se registrará para poder utilizarlo con Single Sign-on.

Pasos recomendados para la reinstalación

1. Desinstale cualquier software de otro fabricante que altere la cadena GINA.
2. Desinstale el software del plug-in.
3. Instale el software de otro fabricante.
4. Instale el software del plug-in.

Si recientemente se ha actualizado o instalado software de otros fabricantes y se sospecha que puede haber alterado la cadena GINA de Windows, puede consultar la entrada del Registro de Windows y el dispositivo cliente para comprobar la presencia y la ubicación de los archivos .dll de la cadena GINA apropiados para la instalación. Si los archivos no se encuentran en el equipo, desinstale y vuelva a instalar el software de Single Sign-on Plug-in.

Importante: Cuando se desinstala el software que puede haber roto la cadena GINA, es importante desinstalarlo en el orden inverso en el que se instaló en el dispositivo del usuario. De lo contrario, el equipo no funcionará correctamente. No modifique el registro.

Creación de un certificado de firma

Feb 07, 2011

El Servicio Single Sign-on genera alertas del registro de sucesos inmediatamente antes y después de que caduque el certificado. Para detener las alertas del registro de sucesos, es necesario crear un certificado nuevo. con CtxCreateSigningCert.exe. Use la Herramienta de firma de datos, CtxSignData.exe, para firmar los datos (mediante las claves proporcionadas por el certificado nuevo) del almacén central.

No es necesario crear un certificado de firma nuevo después de configurar el Servicio Single Sign-on por primera vez, a menos que una de las siguientes afirmaciones sea cierta:

- El certificado de firma está a punto de caducar o ha caducado.
- El certificado de firma está en peligro.

Para crear un certificado nuevo, debe ejecutarse CtxCreateSigningCert.exe, disponible en la carpeta %Archivos de programa%\Citrix\MetaFrame Single Sign-on\Service. En el símbolo del sistema del equipo que ejecuta el Servicio Single Sign-on, escriba CtxCreateSigningCert.exe.

Introduzca el nombre del archivo de claves públicas y el período de validez del certificado, expresado en meses. Se creará el certificado nuevo.

CtxCreateSigningCert	
Uso:	CtxCreateSigningCert
Donde:	= nombre de archivo del certificado público = nombre de archivo del certificado privado = período de validez del certificado, expresado en meses
Ejemplo:	ctxcreatesigningcert “C:\PublicKeyCert.cert” “C:\PrivateKeyCert.cert” “12”

Firma, anulación de firma, nueva firma y verificación de datos

May 11, 2015

La herramienta de firma de datos, CtxSignData.exe, permite firmar los datos, anular la firma de los mismos, firmarlos de nuevo y verificar los datos del almacén central. Se trata de una herramienta que se controla desde la línea de comandos y está disponible en la carpeta \Service del medio de instalación del producto. CtxSignData.exe también está instalado en el servidor en el que se encuentra el servicio, en %ProgramFiles%\Citrix\MetaFrame Password Manager\Service\SigningTool\CtxSignData.exe.

Nota: La herramienta de firma de datos (Data Signing Tool) se instala con el módulo de integridad de datos del Servicio Single Sign-on. Este módulo se puede instalar posteriormente si no forma parte de la instalación inicial de Single Sign-on.
Para iniciar la herramienta de firma de datos, abra un símbolo del sistema en el equipo donde ejecute el servicio Single Sign-on y escriba CtxSignData.exe y use el parámetro de línea de comandos adecuado (-s, -r, -u, -v).

Firma de datos (-s)

Este parámetro de línea de comandos (sign) se utiliza para activar la integridad de datos en entornos con datos existentes sin firmar.

Nota: Si se tiene un entorno de Single Sign-on que se ejecuta sin tener instalada la integridad de datos y posteriormente se decide usar la integridad de datos, es necesario utilizar la herramienta de firma de datos (Data Signing Tool) para firmar los datos del almacén central existente.
Debe proporcionarse el nombre de archivo del certificado de firma, el Identificador de recursos uniformes (URI) del Servicio Single Sign-on, la ubicación del almacén central y el tipo de almacén central (punto compartido de red NTFS o Active Directory). Todos los datos se leen y se firman mediante el certificado de firma nuevo.

La sintaxis del comando CtxSignData con el parámetro -s:

```
CtxSignData [-s ruta_del_servicio archivo_del_certificado ubicación_del_almacén_central NTFS|AD|AD]
```

donde:

-s	Firma los archivos de datos del almacén central
ruta_del_servicio	Indica la ruta del Servicio Single Sign-on en formato URI
archivo_del_certificado	Nombre de archivo del certificado que se utiliza para firmar o firmar nuevamente los datos
ubicación_del_almacén_central	Ruta en formato UNC de la ubicación del punto compartido de archivos o DNS del controlador de dominio de Active Directory
NTFS|AD	NTFS|AD = Tipo de servicio de directorio de red del almacén central, donde: • NTFS = Punto compartido de archivos NTFS de Microsoft • AD = Microsoft Active Directory

Los siguientes son ejemplos del comando CtxSignData con el parámetro -s:

```
ctxsigndata -s “mpmserver.mycompany.com/MPMService” "C:\priv12mos.cert" “\\MPMCentralServer\citrixsync$” NTFS
ctxsigndata -s mpmserver.mycompany.com/MPMService “C:\priv12mos.cert" DC1.mycompany.com AD
```

Nueva firma de datos (-r)

Este parámetro de línea de comandos se utiliza para firmar de nuevo (re-sign) un certificado cuando está a punto de caducar, ha caducado o está en peligro. Debe proporcionarse el nuevo nombre de archivo del certificado de firma, el URI del Servicio Single Sign-on, la ubicación del almacén central y el tipo de almacén central (punto compartido de red NTFS o Active Directory). Todos los datos se leen, se verifican y se firman mediante el certificado nuevo. No es necesario cambiar la configuración en la consola ni en el software del plug-in porque ya tienen la integridad de datos activada.

Utilice los siguientes pasos para volver a firmar los datos dañados:

1. Abra el componente Single Sign-on de Citrix AppCenter y localice la configuración de usuario que esté afectada.
2. Abra la configuración de usuario para comprobar que pueden leerse los datos desde el almacén central.
3. Cierre la configuración de usuario para guardar los nuevos datos sin dañar en el almacén central.
4. Utilice la herramienta de firma (ctxsigndata) para volver a firmar los datos del almacén central.

Nota: Si los datos parecen haberse dañado como consecuencia de una infracción de seguridad, lleve a cabo este procedimiento para todas las configuraciones de usuario antes de volver a firmar los datos para evitar que se firmen datos no protegidos.
La sintaxis del comando CtxSignData con el parámetro -r es:

```
CtxSignData [-s ruta_del_servicio archivo_del_certificado ubicación_del_almacén_central NTFS|AD]
```

donde:

-r	Firma de nuevo los archivos de datos del almacén central (incluye -v)
ruta_del_servicio	Indica la ruta del Servicio Single Sign-on en formato URI
archivo_del_certificado	Indica el nombre de archivo del certificado que se usará para firmar o volver a firmar los datos
ubicación_del_almacén_central	Ruta en formato UNC de la ubicación del punto compartido de archivos o DNS del controlador de dominio de Active Directory
NTFS|AD	NTFS|AD = Tipo de servicio de directorio de red del almacén central, donde: • NTFS = Punto compartido de archivos NTFS de Microsoft • AD = Microsoft Active Directory

Los siguientes son ejemplos del comando CtxSignData con el parámetro -r:

```
ctxsigndata -r “mpmserver.mycompany.com/MPMService” "C:\priv12mos.cert" “\\MPMCentralServer\citrixsync$” NTFS
ctxsigndata -r mpmserver.mycompany.com/MPMService "C:\priv3mos.cert" DC1.mycompany.com AD
```

Anulación de la firma de datos (-u)

Este parámetro de línea de comandos se utiliza para anular la firma (unsign) cuando se desactiva la integridad de datos. Debe proporcionarse el nombre de archivo del certificado de firma, el URI del Servicio Single Sign-on, la ubicación del almacén central y el tipo de almacén central (punto compartido de red NTFS o Active Directory). Todos los datos se leen sin verificarse y las firmas se eliminan.

La sintaxis del comando CtxSignData con el parámetro -u es:

```
CtxSignData [-u ubicación_del_almacén central NTFS|AD]
```

donde:

-u	Anula la firma de todos los archivos de datos del almacén central

ubicación_del_almacén_central	Ruta en formato UNC de la ubicación del punto compartido de archivos o DNS del controlador de dominio de Active Directory
NTFS|AD	NTFS|AD = Tipo de servicio de directorio de red del almacén central, donde: • NTFS = Punto compartido de archivos NTFS de Microsoft • AD = Microsoft Active Directory

Los siguientes son ejemplos del comando CtxSignData con el parámetro -u:

```
ctxsigndata -u "\\MPMCentralServer\citrixsync$" NTFS
ctxsigndata -u DC1.mycompany.com AD
```

Verificación de datos (-v)

Este parámetro de línea de comandos se utiliza para verificar (verify) que todos los datos del almacén central estén firmados y verificados. Debe proporcionarse el nombre de archivo del certificado de firma, el URI del Servicio Single Sign-on, la ubicación del almacén central y el tipo de almacén central (punto compartido de red NTFS o Active Directory). Todos los datos se leen con verificación y se firman.

La sintaxis del comando CtxSignData con el parámetro -v es:

```
CtxSignData [-v ruta_del_servicio ubicación_del_almacén central NTFS|AD]
```

Donde:

-v	Verifica las firmas en los archivos de datos del almacén central
ruta_del_servicio	Indica la ruta del Servicio Single Sign-on en formato URI
ubicación_del_almacén_central	Ruta en formato UNC de la ubicación del punto compartido de archivos o DNS del controlador de dominio de Active Directory
NTFS|AD	NTFS|AD = Tipo de servicio de directorio de red del almacén central, donde: • NTFS = Punto compartido de archivos NTFS de Microsoft • AD = Microsoft Active Directory

Los siguientes son ejemplos del comando CtxSignData con el parámetro -v:

```
ctxsigndata -v "mpmserver.mycompany.com/MPMService" "\\MPMCentralServer\citrixsync$" NTFS
ctxsigndata -v mpmserver.mycompany.com/MPMService "https://mpmserver.mycompany.com/MPMService" DC1.mycompany.com AD
```

Presentación de ayuda (-h)

Use el parámetro de ayuda de la línea de comandos para mostrar la ayuda de CtxSignData.

La sintaxis del comando CtxSignData con el parámetro -h es:

```
CtxSignData [-h]
```

Donde:

-h	Muestra la ayuda

El siguiente es un ejemplo del comando CtxSignData con el parámetro -h:

```
ctxsigndata -h
```

Activación y desactivación del servicio de integridad de datos en el software de Single Sign-On Plug-in

Feb 06, 2011

La siguiente clave de Registro puede modificarse para activar o desactivar la integridad de datos para el software de Single Sign-on Plug-in.

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\MetaFrame Password Manager\Extensions\SyncManager\PerformIntegrityCheck

Tipo: DWORD

Valores:

0=Validación de integridad de datos desactivada

1=Validación de integridad de datos activada

Traslado de datos a otro almacén central

May 11, 2015

Existen varios motivos por los que puede ser necesario migrar directivas de contraseña, plantillas de aplicación, definiciones de aplicación, preguntas de seguridad y otros tipos de datos administrativos de Single Sign-on.

- El usuario se cambia a un nuevo dominio.
- Se ha agregado un nuevo servidor al entorno de Single Sign-on.
- Se ha agregado un nuevo dominio, de modo que los usuarios puedan utilizar la función de asociación de cuentas de Single Sign-on.
- Los usuarios empiezan a utilizar la asociación de cuentas entre dominios existentes.
- Single Sign-on se traslada de un entorno de prueba a un entorno de producción.

La migración involucra un proceso de dos pasos que se ejecuta mediante el componente Single Sign-on de Citrix AppCenter: Paso 1. Exportar los datos administrativos existentes; Paso 2. Importar los datos administrativos al nuevo entorno. En la mayoría de los casos, también es necesario redireccionar a los usuarios al nuevo almacén central.

La siguiente tabla muestra los datos que migran y los que no migran al utilizar el comando Exportar:

Migran	**No migran**
Directivas de contraseña (excepto las directivas Predeterminada y de Dominio)	Configuraciones de usuario
Plantillas de aplicación	Carpetas personales
Definiciones de aplicación	Grupos de aplicaciones
Preguntas de seguridad y grupos de preguntas de seguridad utilizados en la autenticación con preguntas	Credenciales de identificación del usuario
	Cuestionarios
	Datos del Servicio Single Sign-on

El Servicio Single Sign-on no se migra de un almacén central a otro. Para completar satisfactoriamente la migración si está utilizando un servicio, es necesario instalar el Servicio Single Sign-on en una nueva ubicación. Es necesario que el Servicio nuevo y el existente estén disponibles circunstancialmente después de la migración.

Precaución: Se requieren pasos adicionales para asegurar la migración satisfactoria si los módulos de servicio de Integridad de datos o Autoservicio están instalados o si Eliminar la carpeta de datos del usuario y las claves del Registro cuando se cierra Single Sign-on Plug-in está habilitado en una configuración de usuario.
Las configuraciones de usuario no migran de un almacén central a otro automáticamente. Es necesario volver a crearlas y redirigir a los usuarios al nuevo almacén central. Cuando Single Sign-on Plug-in sincroniza sus datos con los datos del almacén central original, reconoce que los valores han cambiado. A continuación, el plug-in copia las credenciales en el nuevo almacén central.

Migración de datos a un nuevo almacén central

El Asistente de exportación de datos de administración le permite exportar todas las definiciones de aplicación, plantillas de aplicación, directivas de contraseña y grupos y preguntas de seguridad en el almacén central. Puede elegir si desea exportar o descartar todos los tipos de datos, pero este asistente no le permite actuar en un subconjunto de datos: por ejemplo, debe exportar todas las directivas de contraseña o dejarlas en el almacén central antiguo.

A diferencia de otros tipos de datos administrativos, puede elegir qué definiciones de aplicación se van a exportar mediante el comando de definición de aplicación Exportar.

Precaución: Es necesario llevar a cabo ciertos pasos manualmente para asegurar la migración satisfactoria, si los módulos de servicio de Integridad de datos o Autoservicio están instalados, o si Eliminar la carpeta de datos del usuario y las claves del Registro cuando se cierra Single Sign-on Plug-in está habilitado en una configuración de usuario.

Para exportar datos de administración

1. En Citrix AppCenter, mientras está conectado al almacén central original, haga clic en el nodo Single Sign-on y, en el menú Acción, haga clic en Exportar datos de administración.
2. Siga las instrucciones en pantalla para el Asistente de exportación de datos de administración.

Para importar datos de administración

1. En la nueva máquina, instale e inicie el componente de la consola de Single Sign-on, completando el proceso Configurar y ejecutar descubrimiento.
   Nota: El proceso Configurar y ejecutar descubrimiento le permite identificar el almacén central con el que desea conectarse.

2. En Citrix AppCenter, mientras está conectado al almacén central nuevo, haga clic en el nodo Single Sign-on y, en el menú Acción, haga clic en Importar datos de administración.
3. Siga las instrucciones en pantalla para el Asistente de importación de datos de administración.
4. Cree nuevas configuraciones de usuario.
5. En Citrix AppCenter, mientras está conectado al almacén central original, seleccione una configuración de usuario migrada y, en el menú Acción, seleccione Redirigir usuarios e identifique la ubicación del nuevo almacén central. Repita según sea necesario.
6. Asegúrese de que los usuarios inicien sesión en Single Sign-on al menos una vez. Ahora es seguro cerrar el almacén central original y el servicio.

Para migrar a un almacén central nuevo si Eliminar la carpeta de datos del usuario y las claves del Registro cuando se cierra Single Sign-on Plug-in está habilitado

Si su empresa habilita la opción Eliminar la carpeta de datos del usuario y las claves del Registro cuando se cierra Single Sign-on Plug-in en las configuraciones de usuario, complete los siguientes pasos para migrar los datos administrativos del usuario a un nuevo almacén central. Si lo hace, obliga a los usuarios migrados a reinscribirse, ya sea a través de una autenticación basada en preguntas o mediante una recuperación de claves automática cada vez que inicien sesión en su equipo. Esto se debe a que los datos administrativos de los usuarios se borran cada vez que cierran sesión o cierran el Single Sign-on Plug-in.

1. Realice la migración de los datos administrativos a un nuevo almacén central.
2. En Citrix AppCenter, mientras está conectado al nuevo almacén central, cree las nuevas configuraciones de usuario. No habilite Eliminar la carpeta de datos del usuario y las claves del Registro cuando se cierra Single Sign-on Plug-in.
3. En Citrix AppCenter, mientras está conectado al almacén central original, seleccione una configuración de usuario migrada y, en el menú Acción, seleccione Redirigir usuarios e identifique la ubicación del nuevo almacén central. Repita según sea necesario.
4. Asegúrese de que los usuarios inicien sesión en Single Sign-on al menos una vez.
5. Escriba y ejecute un script para actualizar el tipo y la ubicación del almacén central en el registro de los equipos de los usuarios. La siguiente tabla suministra los parámetros del Registro en función del tipo de almacén central.

Tipos de almacén central	Parámetros anteriores	Parámetros nuevos
De NTFS a NTFS	HKEY_Local_Machine\SOFTWARE\Citrix\Metaframe Password Manager\Extensions\SyncManager\Syncs\DefaultSync\SSOSyncType = FileSyncPath HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\MetaFrame Password Manager\Extensions\SyncManager\Syncs\DefaultSync\Servers\Server1 =	HKEY_Local_Machine\SOFTWARE\Citrix\Metaframe Password Manager\Extensions\SyncManager\Syncs\DefaultSync\SSOSyncType = FileSyncPath HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\MetaFrame Password Manager\Extensions\SyncManager\Syncs\DefaultSync\Servers\Server1 =
De NTFS a Active Directory	HKEY_Local_Machine\SOFTWARE\Citrix\Metaframe Password Manager\Extensions\SyncManager\Syncs\DefaultSync\SSOSyncType = FileSyncPath HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\MetaFrame Password Manager\Extensions\SyncManager\Syncs\DefaultSync\Servers\Server1 =	HKEY_Local_Machine\SOFTWARE\Citrix\Metaframe Password Manager\Extensions\SyncManager\Syncs\DefaultSync\SSOSyncType = ADSyncPath
De Active Directory a NTFS	HKEY_Local_Machine\SOFTWARE\Citrix\Metaframe Password Manager\Extensions\SyncManager\Syncs\DefaultSync\SSOSyncType = ADSyncPath	HKEY_Local_Machine\SOFTWARE\Citrix\Metaframe Password Manager\Extensions\SyncManager\Syncs\DefaultSync\SSOSyncType = FileSyncPath HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\MetaFrame Password Manager\Extensions\SyncManager\Syncs\DefaultSync\Servers\Server1 =

Precaución: Si edita el Registro de forma incorrecta podrían generarse problemas graves que pueden obligar a instalar nuevamente el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Asegúrese de hacer una copia de seguridad del registro antes de modificarlo.

6. En Citrix AppCenter, mientras está conectado al nuevo almacén central, seleccione las nuevas configuraciones de usuario y habilite Eliminar la carpeta de datos del usuario y las claves del Registro cuando se cierra Single Sign-on Plug-in. Ahora es seguro cerrar el almacén central original y el servicio.

Exportación de las definiciones de aplicación

Puede exportar definiciones de aplicación individuales o cualquier número de ellas a un archivo .xml.

Para exportar una sola definición de aplicación

1. En Citrix AppCenter, mientras está conectado al almacén central original, expanda el nodo Single Sign-on y luego expanda Definiciones de aplicación.
2. Elija la definición de la aplicación a exportar y en el menú Acción haga clic en Exportar definición de aplicación.

3. En el cuadro de diálogo Exportar definición de aplicación, guarde la definición de aplicación en una ubicación a la que pueda acceder desde el equipo de la nueva consola.

Para exportar múltiples definiciones de aplicación

1. En Citrix AppCenter, mientras está conectado al almacén central original, expanda el nodo Single Sign-on y luego haga clic en Definiciones de aplicación.
2. En el menú Acción, haga clic en Exportar definición de aplicación.
3. Siga las instrucciones en pantalla para el Asistente de exportación de definiciones de aplicación.

Para hacer una copia de seguridad del servicio

Cuando realice una copia de seguridad de archivos importantes, asegúrese de incluir el almacén central y su contenido, certificados y claves personales y privadas en los procedimientos de copia de seguridad periódicas de la empresa.

Importante: Se deben modificar los permisos de estos archivos en Windows si el almacén central está en un punto compartido de red NTFS para que pueda acceder a ellos el programa de copia de seguridad.

1. Anote los parámetros que ha configurado al ejecutar la herramienta Configuración del servicio para configurar el servicio.
2. Exporte los datos de servicio a un punto compartido seguro o a un disco mediante CtxMoveServiceData.exe:
   1. En el símbolo del sistema, acceda a %ProgramFiles%\Citrix\Metaframe Password Manager\Service\Tools.
   2. EscribaCtxMoveServiceData.exe –export \\server\share\backupfile.
      Nota: No utilice variables de entorno en la ruta.
   3. Cuando se le pida, escriba la contraseña que desee. Anótela.
      Importante: Los datos de servicio que guarde en el archivo de copia de seguridad se cifrarán con esta contraseña. No la pierda.
   4. Cuando se le pida confirmar la contraseña, vuelva a escribirla.
   5. Verifique que el archivo de copia de seguridad se ha creado.

Para restaurar el servicio

1. Instale el servicio desde el medio de instalación.
2. Configure el servicio con los parámetros correctos, sirviéndose de las notas que ha tomado antes de la copia de seguridad.
   Nota: Si utiliza la integridad de datos, asegúrese de configurar la ubicación del servidor de integridad de datos correctamente, tanto si ha cambiado la ubicación de dicho servidor como si sigue siendo la misma.
3. Finalice la configuración para que el servicio se inicie. Tras el inicio del servicio, puede detenerlo si lo desea.
4. Importe los datos de servicio desde un punto compartido seguro o desde un disco mediante CtxMoveServiceData.exe:
   1. En el símbolo del sistema, vaya a %ProgramFiles%\Citrix\MetaFrame Password Manager\Service\Tools.
   2. EscribaCtxMoveServiceData.exe –import <\\server\share\backupfile>.
   3. Introduzca la contraseña correcta cuando se le pida.
   4. Para la pregunta de si desea sobrescribir AKR.DAT, seleccione Sí.
5. Reinicie el servicio. El servicio ya está listo para usarse.

Eliminación de objetos eliminados del almacén central

Use la herramienta CtxFileSyncClean para eliminar archivos de datos de configuración abandonados de los almacenes centrales de puntos compartidos NTFS. Estos archivos quedan abandonados cuando los objetos a los que señalaban se eliminaron. La herramienta CtxFileSyncClean no elimina archivos de datos de usuario, incluso si se eliminó el usuario. Ejecute CtxFileSyncClean.exe desde la carpeta \Tools del medio de instalación del producto.

Extensiones de definición de aplicación

Jul 19, 2016

Aunque los administradores de Single Sign-on pueden normalmente crear definiciones de aplicaciones mediante el componente Single Sign-on de Citrix AppCenter y la Herramienta de definición de aplicaciones, algunas aplicaciones tienen requisitos especiales que necesitan usar un proceso externo para determinar si se inició una aplicación o bien, para enviar credenciales de usuario con Single Sign-on Plug-in.

Para admitir este tipo de aplicaciones, los encargados de implementar sistemas que creen procesos para satisfacer estos requisitos de procesamiento externo pueden usar las Extensiones de definición de aplicaciones del componente Single Sign-on de Citrix AppCenter y la Herramienta de definición de aplicaciones para configurar el momento y la forma en que se iniciarán estos procesos.

Funcionamiento del software de Single Sign-on Plug-in

Hay dos tipos distintos de extensiones de definición de aplicación:

- Extensiones de identificación
  Usan procesos externos para determinar si la aplicación de destino es un formulario que necesita acciones de administración de credenciales de usuario. Estos procesos externos pueden usarse en lugar de, o junto con, otros algoritmos de detección de ventanas definidos en la definición del formulario.
- Extensiones de acciones
  Usan procesos externos para llevar a cabo las acciones de administración de credenciales necesarias. Estos procesos externos pueden usarse en lugar de, o junto con, otros algoritmos de acción en ventanas definidos en la definición del formulario.

Una misma definición de formulario puede configurarse para que use extensiones de definición de aplicación para llevar a cabo una o ambas operaciones.

Extensiones de identificación

Single Sign-on Plug-in usa conectores de escucha para detectar sucesos en el escritorio como instalaciones de aplicaciones, cargas de URL, notificaciones de carga de documentos HTML y otros sucesos similares.

A medida que ocurren, el plug-in determina si la aplicación de destino necesita acciones de administración de credenciales de usuario (como ignorar, iniciar sesión, cambiar contraseña, etc.). La determinación se basa en la comparación de las características expuestas por la aplicación y las que definen exclusivamente al formulario. Estas características incluyen el título de la ventana y el nombre de archivo ejecutable (como mínimo) y, si es necesario, otras características avanzadas como el uso de un proceso externo para identificar el formulario (extensión de identificación).

Si es necesario un proceso de identificación externo, el mismo se identifica en la definición del formulario. La definición del formulario incluye información sobre la extensión de identificación y sus parámetros asociados. Estos se asocian directamente con un parámetro del Registro del sistema.

Después de que el plug-in procesa los algoritmos de coincidencia mínimos y avanzados, se evalúan las extensiones de identificación que usan procesos externos.

Cuando hay varias extensiones de identificación definidas para evaluar un formulario, las extensiones se ejecutan en el orden en que aparecen en la página de extensiones de identificación.

Para cada extensión de identificación, Single Sign-On Plug-in espera un período de tiempo especificado (definido en el parámetro del Registro del sistema) para que se cierre el proceso externo antes de analizar el código de salida del proceso.

Si los procesos de coincidencia mínima, avanzada y externa se completan con un código de respuesta cero, la aplicación de destino es una aplicación coincidente. Si un proceso termina con otro valor, el proceso de evaluación se detiene y la aplicación no se considera coincidente.

Si se encuentra un valor negativo, se registra un error en el Visor de sucesos de Windows. Los valores positivos se registran en un archivo de registro, si dicha opción está activada.

La acción de administración de credenciales de usuario subsiguiente se puede llevar a cabo usando cualquier combinación de acciones de formulario estándar de Windows, secuencias de acciones o extensiones de acciones.

Para definir una extensión de identificación

Configure extensiones de identificación usando el Asistente de definición de formularios durante el proceso de desarrollo de definiciones de aplicación.

1. En AppCenter, expanda el nodo Single Sign-on, seleccione Definiciones de aplicación y, en el menú Acción, haga clic en Crear una definición de aplicación.
2. En el Asistente de definición de aplicaciones, continúe hasta la página Administrar formularios y luego, seleccione Agregar formulario para iniciar el Asistente de definición de formularios.
3. Avance en el proceso de definición hasta que aparezca la página Identificar el formulario.
4. En la página Identificar el formulario, haga clic en Coincidencia avanzada. .
5. En el cuadro de diálogo Coincidencia avanzada, haga clic en Extensiones de identificación.
6. En la página Extensiones de identificación, haga clic en Agregar para abrir el cuadro de diálogo Agregar extensión de identificación. El cuadro de diálogo Agregar extensión de identificación se usa para definir lo siguiente:

ID de extensión	El ID de extensión identifica el ExtensionName a buscar en los parámetros del Registro.
Descripción	Una descripción definida por el usuario para la extensión de identificación definida.
Parámetros	Cualquier par de nombre y valor de parámetros utilizado para transferir parámetros predefinidos al proceso externo iniciado por la extensión.

ExtensionName identifica el nombre de una clave del Registro del sistema. Este nombre de clave y sus valores asociados definen el ejecutable del proceso externo de identificación y sus características operacionales. El nombre de la clave del Registro y sus claves asociadas se encuentran en:

[HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\MetaFrame Password Manager\Extension\{ExtensionName}]

Donde ExtensionName se identifica usando el valor de ID de extensión del cuadro diálogo Agregar extensión de identificación.

En las plataformas de 64 bits, el nombre de la clave del Registro y sus claves asociadas se encuentran en:

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\MetaFrame Password Manager\Extension\{ExtensionName}]

La siguiente tabla define las características del valor de la clave.

Tecla	Tipo	Valor
Tipo	REG_SZ	Debe ser un ejecutable
Tiempo de espera	REG_DWORD	0 para esperar para siempre que la aplicación complete su acción. Cualquier otro valor en milisegundos para esperar.
TerminateProcess	BOOL implementado como REG_DWORD	(optativo) Cuando se alcanza el tiempo de espera, terminar el proceso. TRUE—(predeterminado) Terminar el proceso. FALSE—(0) No terminar el proceso.
Ejecutable	REG_EXPAND_SZ	El ejecutable del proceso y su ruta completa.
Arguments	REG_SZ	Parámetros del ejecutable.

El valor Executable es la ruta completa del archivo ejecutable. Están permitidas las variables de entorno. Si la extensión se implementa como script, el intérprete de script se debe usar para el Executable, y el nombre de script como parte de Arguments. Los procesos externos se pueden desarrollar con cualquier editor e idioma o IDE que se desee.

El valor Arguments respalda parámetros que el software del plug-in pueda reemplazar con parámetros de tiempo de ejecución o los pares de nombre/valor especificados en el cuadro de diálogo Agregar extensión de identificación. Cada parámetro que necesite sustitución debe tener un signo de dólar ($) delimitador como prefijo y sufijo. Por ejemplo, la siguiente línea de comandos Arguments:

```
/h $_HANDLE$ /s $SAPSERVER$ /t $SAPTYPE$
```

aparece para el ejecutable como:

```
/h 1275366 /s "México DF" /t 43
```

El control de Microsoft Windows asociado con la aplicación es un parámetro interno definido como $_HANDLE$.

Todos los parámetros internos usan $_ como prefacio para evitar conflictos de nombrado. Los parámetros del implementador no pueden usar guiones en los nombres de clave.

La precedencia de sustitución se define para preservar los valores de parámetros después de que se escriben. La precedencia se define como parámetros internos (como $_HANDLE$), seguidos de los parámetros del implementador, seguidos por las variables de entorno.

Todos los parámetros de implementador pueden usar minúsculas, mayúsculas y números en los nombres de clave. Los nombre de clave no distinguen entre mayúsculas y minúsculas.

Si el ejecutable de la extensión de identificación necesita que los parámetros se presenten en una secuencia específica, Argument debe respaldar la secuencia necesaria. No importa el orden en que se definan los pares de nombre y valor en Agregar extensión de identificación.

Extensiones de acción

Las extensiones de acción usan procesos externos para administrar las acciones de administración de credenciales. El proceso de definición de extensiones tiene la capacidad de pasar las credenciales de usuario a la aplicación externa.

Después de identificarse con éxito un formulario de administración de credenciales (consulte
— Extensiones de identificación
), la acción de administración de credenciales de usuario subsiguiente se puede llevar a cabo usando cualquier combinación de acciones de formulario estándar de Windows, secuencias de acciones o extensiones de acciones.

Single Sign-on Plug-in admite las mismas características descritas en
— Extensiones de identificación
.

El plug-in ejecuta el proceso externo y espera el tiempo especificado a que termine (si WaitForCompletion se configura como TRUE) y luego, analiza el código de salida del proceso. Si el proceso termina con un valor cero, la extensión se ejecutó satisfactoriamente. Cualquier valor que no sea cero significa que hubo un error.

Si se encuentra un valor negativo, se registra un error en el Visor de sucesos de Windows. Los valores positivos se escriben en un archivo de registro, si se lo habilita (consulte
— Habilitación de registros
para obtener más información).

Para definir una extensión de acción

A través del Asistente de definición de formularios configure las extensiones de acciones durante el proceso de desarrollo de definiciones de aplicación.

1. En Citrix AppCenter, expanda el nodo Single Sign-on, seleccione Definiciones de aplicación y, en el menú Acción, haga clic en Crear una definición de aplicación.
2. En el Asistente de definición de aplicaciones, continúe hasta la página Administrar formularios y luego, seleccione Agregar formulario para iniciar el Asistente de definición de formularios.
3. Avance en el proceso de definición hasta que aparezca la página Definir las acciones del formulario.
4. En la página Definir las acciones del formulario, haga clic en Editor de acciones.
5. En el cuadro de diálogo Editor de acciones, seleccione la opción Iniciar extensión de acción. Aparece el panel Configurar acciones. Este panel se usa para ver, modificar o agregar entradas de Iniciar extensión de acción a la secuencia de acciones.
6. Para agregar una extensión de acción a la secuencia, ingrese la siguiente información y haga clic en Insertar:

ID	El ID identifica el ExtensionName a buscar en los parámetros del Registro.
Descripción	Una descripción definida por el usuario para la extensión de acción definida.
Parámetros	Cualquier par de nombre y valor de parámetros utilizado para transferir parámetros predefinidos al proceso externo iniciado por la extensión.

Como en el caso de las extensiones de identificación, ExtensionName identifica el nombre de una clave del Registro. Este nombre de clave y sus valores asociados definen el ejecutable del proceso externo de acción y sus características operacionales. El nombre de la clave del Registro y sus claves asociadas se encuentran en:

[HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\MetaFrame Password Manager\Extension\{ExtensionName}]

Donde el valor ExtensionName se identifica usando el valor de ID del panel Configurar acciones.

En las plataformas de 64 bits, el nombre de la clave del Registro y sus claves asociadas se encuentran en:

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\MetaFrame Password Manager\Extension\{ExtensionName}]

La siguiente tabla define las características del valor de la clave.

Tecla	Tipo	Valor
Tipo	REG_SZ	Debe ser un ejecutable
Tiempo de espera	REG_DWORD	0 para esperar para siempre que la aplicación complete su acción. Cualquier otro valor en milisegundos para esperar.
TerminateProcess	BOOL implementado como REG_DWORD	(optativo) Cuando se alcanza el tiempo de espera, terminar el proceso. TRUE—(predeterminado) Terminar el proceso. FALSE—(0) No terminar el proceso.
WaitForCompletion	BOOL implementado como REG_DWORD	(optativo) El plug-in espera que el proceso se cierre. TRUE—(predeterminado) Esperar. FALSE—(0) No esperar.
Ejecutable	REG_EXPAND_SZ	El ejecutable del proceso y su ruta completa.
Arguments	REG_SZ	Parámetros del ejecutable.

El valor Executable sigue las mismas convenciones que en las extensiones de identificación.

El valor Arguments respalda parámetros que el plug-in pueda reemplazar con parámetros de tiempo de ejecución o los pares de nombre/valor especificados en el cuadro de diálogo Iniciar extensión de acción del Editor de acciones. Cada parámetro que necesite sustitución debe tener un signo de dólar ($) delimitador como prefijo y sufijo. Por ejemplo, la siguiente línea de comandos Arguments:

```
/h $_HANDLE$ /s $SAPSERVER$ /t $SAPTYPE$
```

aparece para el ejecutable como:

```
/h 1275366 /s "México DF" /t 43
```

El control de Microsoft Windows asociado con la aplicación es un parámetro interno definido como $_HANDLE$.

Todos los parámetros internos usan $_ como prefacio para evitar conflictos de nombrado. Los parámetros del implementador no pueden usar guiones en los nombres de clave.

Además del control de Windows, los siguientes parámetros están respaldados en la administración de credenciales de usuario:

- Nombre de usuario ($_USERNAME$)
- Contraseña ($_PASSWORD$)
- Personalizado1 ($_CUSTOM1$)
- Personalizado2 ($_CUSTOM2$)
- Contraseña anterior ($_OLDPASSWORD$)

La precedencia de sustitución se define para preservar los valores de parámetros después de que se escriben. La precedencia se define como parámetros internos, seguidos de los parámetros del implementador, seguidos por las variables de entorno.

Todos los parámetros de implementador pueden usar minúsculas, mayúsculas y números en los nombres de clave. Los nombre de clave no distinguen entre mayúsculas y minúsculas.

Si el ejecutable de la extensión de identificación necesita que los parámetros se presenten en una secuencia específica, Argument debe respaldar la secuencia necesaria. No importa el orden en que se definan los pares de nombre y valor en la página Configurar acciones.

Requisitos del implementador

El proceso externo que lleva a cabo las acciones de coincidencia avanzada o de administración de credenciales se define como cualquier proceso o aplicación que pueda iniciarse usando una interfaz de línea de comandos. Los argumentos necesarios u optativos para las extensiones de identificación o extensiones de acción también deben poder especificarse usando una interfaz de línea de comandos.

En el caso de las extensiones de acción, el implementador debe respaldar las funciones descritas para la detección de ventanas. Los valores de nombre de usuario, contraseña, personalizado1, personalizado2 y contraseña anterior pueden pasarse al ejecutable.

En el caso de las extensiones de identificación y las extensiones de acción, el implementador es responsable de:

- Distribuir todos los archivos y módulos ejecutables y de respaldo necesarios para dar respaldo a la extensión en el Single Sign-on Plug-in.
- Mantener todos los módulos distribuidos.
- Agregar en el plug-in todas las entradas de Registro especificadas.
- Mantener la exclusividad del nombre de extensión en los dominios.

El esquema de nombrado de extensiones recomendado es uno de nombrado de dominio inverso (por ejemplo: com.citrix.cpm.ext4).

Habilitación de registros (log)

Para activar el seguimiento de depuración de Single Sign-on Plug-in, se debe implementar un cambio en el Registro del sistema.

El nombre de la clave del Registro y sus claves asociadas se encuentran en:

[HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\MetaFrame Password Manager\Log]

La siguiente tabla define las características del valor de la clave.

Clave	Tipo	Valor
Habilitado	REG_DWORD	El valor predeterminado es 0. 0 significa inhabilitado. 1 significa habilitado.
Filtro	REG_DWORD	Máscara de bits que indica lo que se registra. 0x00000001: marca de aplicación de Windows usada para la identificación de errores de extensión. 0x00000004: llenado de contraseña de aplicación de Windows usada para la identificación de errores de extensión de acción.
MaxSizeInBytes	REG_DWORD	Tamaño del archivo en bytes. El tamaño máximo teórico puede ser 4 GB (2^32). Predeterminado: 819200

Los datos se registran en el archivo sso_.log en:

```
%LocalAppData%\Citrix\MetaFrame Password Manager
```

Teclas virtuales para aplicaciones de Windows, Web y basadas en emuladores de terminal.

Oct 12, 2015

Single Sign-on es compatible con las teclas virtuales para aplicaciones de Windows, Web y basadas en emuladores de terminal. Estos códigos se utilizan para enviar acciones del teclado específicas para los campos de inicio de sesión o de formulario de cambio de contraseñas.

Códigos de VTabKeyN (Windows y Web)

Utilice los siguientes identificadores para crear una secuencia de códigos de teclas para aplicaciones de Windows y basadas en la Web.

Código	Descripción
'DELAY=N'	N es el número de milésimas de segundo de retraso.
'VKEY=N'	N es la tecla virtual para el envío.

Por ejemplo, para enviar Tab, Fin, espacio, un retraso de 1,5 segundos, el nombre de usuario de inicio de sesión, espacio, el nombre de usuario/ID, Inicio, un retraso de 0,35 segundos, Tab y, por último, la contraseña use lo siguiente:

VTabKey1= 'VKEY=9''VKEY=35' 'DELAY=1500 'nombre de usuario de inicio de sesión'VKEY=32' VTabKey2='VKEY=36''DELAY=350''VKEY=9'

Códigos de VirtualKeyCode y VKEY (Windows y Web)

Tecla	Código	Tecla	Código	Tecla	Código	Tecla	Código
Pausa	3	5	53	V	86	F5	116
Backspace (retroceso)	8	6	54	W	87	F6	117
Fichas	9	7	55	X	88	F7	118
Borrar	12	8	56	S	89	F8	119
Intro	13	9	57	Z	90	F9	120
Mayús	16	A	65	Izquierda (ventana)	91	F10	121
Ctrl	17	B	66	Derecha (ventana)	92	F11	122
Alt	18	C	67	0 (teclado numérico)	96	F12	123
Bloq Mayús	20	D	68	1 (teclado numérico)	97	F13	124
Esc	27	E	69	2 (teclado numérico)	98	F14	125
Barra espaciadora	32	F	70	3 (teclado numérico)	99	F15	126
Re Pág	33	G	71	4 (teclado numérico)	100	F16	127

Tecla	Código	Tecla	Código	Tecla	Código	Tecla	Código
Avpag	34	H	72	5 (teclado numérico)	101	F17	128
Fin	35	I	73	6 (teclado numérico)	102	F18	129
Inicio	36	J	74	7 (teclado numérico)	103	F19	130
Izquierda	37	K	75	8 (teclado numérico)	104	F20	131
Subir	38	L	76	9 (teclado numérico)	105	F21	132
Right (Derecho)	39 lbs (17 Kg)	M	77	Asterisco(*)	106	F22	133
Bajar	40	N	78	Signo más (+)	107	F23	134
Impr Pant	44	O	79	Signo menos (-)	109	F24	135
Help	47	P	80	Punto (.)	110	Bloq num	144
0	48	Q	81	Barra diagonal (/)	111	Bloq Despl	145
1	49	R	82	F1	112	Mayús Izq	160
2	50	A	83	F2	113	Mayús Der	161
3	51	T	84	F3	114	Ctrl Izq	162
4	52	U	85	F4	115	Ctrl Der	163

Teclas virtuales para emuladores de terminal compatibles con HLLAPI

Carácter/Comando	Código	Carácter/Comando	Código	Carácter/Comando	Código
Alt Cursor	@$	Local Print (impresión local)	@P	PF12/F12	@c
Backspace (retroceso)	@<	Reset	@R	PF13/F13	@d
@	@@	Mayús	@S	PF14/F14	@e
Alt	@A	Dup (copiar)	@S@x	PF15/F15	@f
Field - (campo -)	@A@-	Field Mark (marca de campo)	@S@y	PF16/F16	@g
Field + (campo +)	@A@+	Tab (Right Tab) (tabulador a la derecha)	@T	PF17/F17	@h
Field Exit (salida de campo)	@A@E	Cursor Up (arriba)	@U	PF18/F18	@i

Carácter/Comando	Código	Carácter/Comando	Código	Carácter/Comando	Código
Erase Input (borrar entrada)	@A@F	Cursor Left (izquierda)	@L	PF20/F20	@k
Sys Request (solicitud del sistema)	@A@H	Cursor Right (derecha)	@Z	PF21/F21	@l
Insert Toggle (alternancia modo inserción)	@A@I	Re Pág	@u	PF22/F22	@m
Cursor Select (selección del cursor)	@A@J	Av Pág	@v	PF23/F23	@n
Atención	@A@Q	Fin	@q	PF24/F24	@o
Impr Pant	@A@T	Inicio	@0	PA1	@x
Hexadecimal	@A@X	PF1/F1	@1	PA2	@y
Cmd/Func Key (comando/tecla de función)	@A@Y	PF2/F2	@2	PA3	@z
Print (PC) (imprimir, PC)	@A@T	PF3/F3	@3	PA4	@+
Back/Left Tab (tabulador atrás/izqda.)	@B	PF4/F4	@4	PA5	@%
Borrar	@C	PF5/F5	@5	PA6	@&
Eliminar	@D	PF6/F6	@6	PA7	@’
Intro	@E	PF7/F7	@7	PA8	@(
Erase EOF (borrar final de línea)	@F	PF8/F8	@8	PA9	@)
Help	@H	PF9/F9	@9	PA10	@*
Insert (insertar)	@I	PF10/F10	@a		
New Line (nueva línea)	@N	PF11/F11	@b		

Single Sign-on Provisioning Software Development Kit. (SDK)

Oct 12, 2015

Single Sign-on Provisioning Software Development Kit (SDK) permite que los administradores gestionen completamente las credenciales secundarias de los usuarios. Las credenciales secundarias son credenciales específicas de aplicaciones que Single Sign-on envía en lugar del usuario después de llevarse a cabo la autenticación principal en el dominio.

El aprovisionamiento de credenciales permite que se automaticen muchas tareas asociadas con la administración de credenciales de usuario. Gracias al aprovisionamiento de credenciales, tareas como instalar Single Sign-on, agregar nuevos usuarios o aplicaciones, o eliminar información superflua son ahora mucho más rápidas y eficaces.

Esta ayuda en pantalla describe el diseño general de la función de aprovisionamiento de credenciales de Single Sign-on y brinda un resumen de las funciones de la API que pueden usarse para definir acciones en el archivo XML de aprovisionamiento.

El módulo de aprovisionamiento

El módulo de aprovisionamiento forma parte del Servicio Single Sign-on y es un servicio Web estándar que presenta una interfaz de protocolo simple de acceso a objetos y lenguaje de marcado de abastecimiento de servicios (SOAP/SPML) para recibir los comandos de aprovisionamiento. Todas las comunicaciones entre el cliente y el módulo de aprovisionamiento se producen a través de un canal con seguridad de la capa de transporte (TLS).

Al enviar comandos de aprovisionamiento a la cola, asegúrese de que los datos se almacenen de forma segura y no se transmitan a través de una conexión de red insegura.

El módulo de aprovisionamiento debe tener acceso de lectura y escritura al almacén central de Single Sign-on para poder poner en cola los comandos de aprovisionamiento entrantes hasta que el Single Sign-on Plug-in ejecute los comandos.

Los comandos enviados al módulo de aprovisionamiento no se pueden recuperar. Una vez enviados, los comandos permanecen en cola hasta que el Single Sign-on Plug-in los ejecuta. Si necesita quitar un comando de la cola, envíe el comando opuesto para cada objeto de credencial, usuario y aplicación que deba eliminar de la cola.

Nota: El módulo de aprovisionamiento utiliza una interfaz que cumple con SPML 2.0. Sólo se admiten las operaciones centrales que son necesarias para respetar el cumplimiento.

El modelo SPML 2.0

El archivo XML de aprovisionamiento y todos los componentes de terceros que emiten solicitudes de SPML se denominan autoridades solicitantes (RA).

El módulo de aprovisionamiento es un proveedor de servicio de aprovisionamiento (PSP). Este PSP admite un solo destino de servicio de aprovisionamiento (PST) que coloque en cola por usuario los comandos de aprovisionamiento de Single Sign-on.

Proporcionar credenciales secundarias a los usuarios es la acción que se lleva a cabo al ejecutar el aprovisionamiento. Esto significa que los usuarios finales y las credenciales secundarias son los objetos de servicio de aprovisionamiento (PSO) del destino de servicio de aprovisionamiento. El identificador único (PSO-ID) para cada usuario es un nombre de dominio completamente calificado (FQDN). El identificador único (PSO-ID) para cada credencial secundaria es el GUID asignado a la credencial cuando se crea. Como las credenciales secundarias están asociadas a un usuario determinado, el PSO del usuario

funciona como contenedor para los PSO de la credencial. Esto se ve representado por el elemento containerID en una solicitud de SPML.

En rigor, Single Sign-on no agrega, modifica ni elimina usuarios; sin embargo, Single Sign-on sí agrega, modifica y elimina datos asociados a un usuario.

Aprovisionamiento y Single Sign-on Plug-in

Como el Single Sign-on Plug-in es, en última instancia, el responsable de proteger las credenciales secundarias de un usuario con claves de cifrado específicas del usuario, la ejecución de las operaciones de aprovisionamiento constituye un proceso de dos pasos. Primero, es necesario otorgar el comando de aprovisionamiento a un módulo de aprovisionamiento. Luego, el Single Sign-on Plug-in aplica, en nombre del usuario actual, todos los comandos de aprovisionamiento en cola al almacén de credenciales secundarias del usuario.

El Single Sign-on Plug-in detecta la presencia de operaciones de aprovisionamiento en cola durante el proceso de sincronización regular que se produce en el inicio. El plug-in ejecuta los comandos de aprovisionamiento en cola antes de reanudar las actividades normales. Esto garantiza que, en una situación de primer uso, el plug-in ejecute las acciones de aprovisionamiento primero y así, minimice las acciones de configuración de primer uso del usuario final.

Todas las comunicaciones entre el Single Sign-on Plug-in y el módulo de aprovisionamiento se producen a través de una conexión con seguridad TLS.

La aplicación de aprovisionamiento del cliente debe definir la asignación de las aplicaciones disponibles para el aprovisionamiento y la representación de la aplicación del lado del cliente.

Aprovisionamiento de credenciales secundarias

Las credenciales secundarias se asocian a una definición de aplicación específica creada mediante el componente Single Sign-on de AppCenter; por lo tanto, la operación addRequest debe incluir datos que vinculen los detalles del usuario en la solicitud a una definición de aplicación específica. Esto significa que la autoridad solicitante debe determinar la lista de aplicaciones disponibles para el aprovisionamiento para cada usuario y debe proporcionar el ID de una definición de aplicación como parte de la operación addRequest. Esto implica una carga para la autoridad solicitante ya que debe determinar la asociación entre las definiciones de aplicación de Single Sign-on y la identificación externa (como el nombre de la aplicación) de las aplicaciones que se están aprovisionando.

Puesto que la persona que administra Single Sign-on y la persona que realiza tareas de aprovisionamiento pueden ser distintas personas, hay un riesgo de confusión. Por ejemplo, un administrador puede definir la aplicación "Microsoft Outlook", mientras que otro administrador de aprovisionamiento crea cuentas para "Microsoft Exchange". Single Sign-on permite crear varias credenciales secundarias para una definición de aplicación determinada. Por ejemplo, un usuario puede disponer de varias cuentas de MSN Hotmail para las cuales Single Sign-on posee credenciales almacenadas. Esta capacidad implica que un administrador puede emitir varios addRequests con parámetros idénticos. En este caso, se crean varias credenciales secundarias. Del mismo modo, es posible que el administrador desee aprovisionar varias credenciales diferentes para la misma aplicación; sin embargo, el Single Sign-on Plug-in cifra los secretos de la credencial (ID de usuario, contraseña y campos personalizados) y el módulo de aprovisionamiento no puede recuperarlos para ayudar a la autoridad solicitante a distinguir las credenciales en otro momento.

Para solucionar estos problemas existe un campo de datos privados opcional para la autoridad solicitante, provision-description, en las operaciones y addRequest y modifyRequest. Esto proporciona a la autoridad solicitante la capacidad de agregar un ID o datos descriptivos para ayudar a distinguir las credenciales. El Single Sign-on Plug-in y el módulo de aprovisionamiento no pueden modificar ni mostrar este campo. Cuando se solicita una lista de credenciales a través de

lookupRequest, este campo se retiene y se devuelve a la autoridad solicitante.

El Single Sign-on Plug-in tiene acceso completo para editar todas las credenciales secundarias. Esto incluye acciones como duplicar, eliminar y modificar las credenciales. Esto significa que los usuarios pueden modificar sus datos para que ya no coincidan con el estado creado a través de las operaciones de aprovisionamiento.

Además, los usuarios pueden definir aplicaciones según su voluntad, es decir, pueden agregar credenciales para las aplicaciones que no se encuentran definidas en la consola de Single Sign-on. Esta capacidad puede generar problemas de propiedad como, por ejemplo, si el administrador puede o no puede eliminar o modificar una credencial secundaria, o si estas credenciales deben enumerarse en lookupResponse. Esta versión de Single Sign-on no admite restricciones de propiedad; el administrador y el usuario final pueden modificar todas las credenciales.

Grupos de aplicaciones

Single Sign-on permite agrupar aplicaciones. Un atributo de este agrupamiento es usar o no usar la misma contraseña en todas las credenciales definidas para las aplicaciones del grupo. Cuando un usuario modifica una credencial asociada a un grupo, el cambio se aplica a todas las credenciales de todas las aplicaciones del grupo.

Este comportamiento persiste cuando los cambios se realizan a través de la API de aprovisionamiento. Más específicamente, cuando se agrega una credencial a un grupo de aplicaciones, la nueva contraseña suministrada como parámetro para el comando se convierte en la nueva contraseña para cada aplicación del grupo. Por lo tanto, el comando tiene el efecto neto de una adición y varios comandos . De forma similar, un comando modifica todas las aplicaciones de un grupo y, como consecuencia, tiene el efecto neto de varios comandos .

Códigos de error

Código	Descripción
101	Faltan uno o varios campos de credenciales requeridos en la solicitud de aprovisionamiento.
102	Nombre de usuario especificado no válido. Falta el nombre de usuario o el formato es incorrecto.
103	No se encontró el usuario especificado.
104	Definición de aplicación no válida. Falta la definición de aplicación o su estructura no es válida.
105	El formato del identificador de credenciales no es válido.
106	No se encontró la credencial especificada.
107	Token de seguridad para autorización no válido.
108	Token de acceso no autorizado. El token especificado no puede ejecutar la operación solicitada.
109	Otro proceso utiliza el acceso al mecanismo de almacenamiento. Vuelva a intentarlo en otro momento.

Código	Descripción
110	Ocurrió un error al consumir los comandos de aprovisionamiento.
111	El usuario no tiene autorización para acceder a la cola de comandos de aprovisionamiento.
112	Ocurrió un error al obtener la clave secreta de aprovisionamiento.
113	No se puede asignar memoria de cifrado.
114	No se puede asignar un búfer de datos de entropía.
115	Error en el cifrado.
116	No se puede asignar el búfer cipherText.
117	Error en el descifrado.
118	No se pudo dar el formato de mensaje de error al código de error de las ventanas.
119	Falta psoID o este elemento no posee el formato adecuado.
120	No se pudo encontrar la aplicación a la que se hace referencia.
121	No se pudo encontrar la configuración de usuario para el usuario solicitado.
122	Falta el atributo "join" para la credencial en el grupo de contraseñas compartidas.
123	Falta el atributo "use-new-password" para la credencial en el grupo de contraseñas compartidas.
124	Falta la contraseña para la credencial en el grupo de contraseñas compartidas.
125	Falta el nombre de la credencial o el nombre no es válido. Especifique un nombre de credencial válido.
126	El ID de aplicación especificado no es válido.
127	La credencial no puede volver a unirse al grupo de contraseñas compartidas.
128	El aprovisionamiento no se encuentra habilitado para la cuenta de usuario especificada.

Resumen de las funciones de la API (inglés únicamente)

Feb 07, 2011

Las funciones de la API proporcionan un método que se puede utilizar para definir acciones en el archivo XML de aprovisionamiento. Además del código de muestra de estos temas, existen más códigos de muestra disponibles en el medio de instalación del producto.

Todos los elementos y los atributos específicos de Single Sign-on introducidos llevan el prefijo indicador de espacio de nombres "ctxs". El icono XML en cada cuadro de texto indica una solicitud y una respuesta correspondiente.

Sólo se admite el modo de ejecución sincrónica. Todas las solicitudes de ejecución asíncrona generan errores unsupportedExecutionMode.

Para abreviar, se utilizan los siguientes marcadores de posición descriptivos en lugar de los valores de ejemplo:

Texto de marcador de posición	**Interpretación**
FQDN	El nombre de dominio completamente calificado del usuario.
GUID de aplicación	El GUID asignado a una definición de aplicación cuando se crea mediante el componente Single Sign-on de Citrix AppCenter.
GUID de credencial	El GUID asignado a la credencial secundaria aprovisionada mediante el servicio de aprovisionamiento al finalizar una operación addRequest.
ID generado por RA	Un ID único para una solicitud creada por la autoridad solicitante. Esto se utiliza en el atributo requestID opcional de los elementos de solicitud. Sólo es relevante si se agrega la compatibilidad con la ejecución asincrónica.
AuthToken	El elemento authentication-token es obligatorio pero no se utiliza en esta oportunidad.

Aprovisionamiento de una sola aplicación: addRequest

Feb 06, 2011

Use la operación addRequest para agregar credenciales a una aplicación para el usuario.

Una operación addRequest solicita que se agregue un nuevo objeto (la credencial) al objeto contenedor especificado (el almacén de datos del usuario). Se debe especificar un elemento containerID (nombre de dominio completamente calificado [FQDN] del usuario) y se devuelve el elemento psoID (GUID de la credencial) para el objeto recientemente creado. La información de la solicitud representa los datos específicos de la credencial que se va a crear.

Si la definición de aplicación asignada a la nueva credencial es un miembro del grupo de contraseñas compartidas, se actualizan todas las credenciales asociadas a los miembros de ese grupo para usar la nueva contraseña.

Sintaxis

AuthToken Credential name Admin Text Credential description appdefGuid Domain salima pass123 domain database

Parámetros

requestID (obligatorio)	Este es el ID generado por el cliente que asocia los valores de retorno con esta solicitud.
targetID (obligatorio)	Este es el ID del módulo de aprovisionamiento que se identifica mediante el targetID "CPM Provisioning 1.0.".
returnData (obligatorio)	data: detalles de una credencial secundaria. identifier: lista de credenciales para un usuario. name: no es compatible con Single Sign-on. everything: definiciones de aplicación disponibles para el usuario especificado.
executionMode (obligatorio)	Single Sign-on admite el modo de ejecución sincrónica.
authentication-token (obligatorio)	El elemento authentication-token es obligatorio pero no se utiliza en esta oportunidad. .
containerID (obligatorio)	El elemento containerID proporciona el nombre de dominio completo (FQDN) del usuario que posee la credencial.
data (obligatorio)	El elemento data es la descripción de los datos que se encuentran bajo modificación. Este es el elemento credential y puede incluir cualquier elemento secundario de la credencial o cualquier elemento de la aplicación.
ctxs:credential (obligatorio)	El elemento credential se utiliza para describir una sola credencial secundaria. El nombre y la descripción derivados del elemento credential son opcionales. Si no se proporcionan, el plug-in utiliza el nombre y la descripción de la definición de aplicación.

ctxs:application (obligatorio)	El elemento application se utiliza para describir una definición de aplicación y los detalles de una credencial. El elemento application debe coincidir con uno previamente obtenido de una operación lookupApplicationsRequest.

Sintaxis para los valores de retorno (addResponse)

Parámetros para los valores de retorno (addResponse)

status (obligatorio)	Valores posibles: Success, Failure, Pending
requestID (obligatorio)	Este es el ID generado por el cliente que asocia estos valores de retorno con la solicitud asociada.
pso (obligatorio)	Los datos de pso representan una credencial según se describe en ctxs:credential.
psoID (obligatorio)	El elemento psoID es un identificador único para cada usuario final; PSOID es el número de identificación único (GUID) de la credencial que devuelve lookupResponse.
containerID (obligatorio)	El elemento containerID proporciona el nombre de dominio completo (FQDN) del usuario que posee la credencial.
data (obligatorio)	El elemento data es la descripción de los datos que se encuentran bajo modificación. Este es el elemento credential y puede incluir cualquier elemento secundario de la credencial o cualquier elemento de la aplicación.

Atributos del elemento group

Los atributos join y use-new-password del elemento group controlan la forma en que la nueva credencial afecta a los miembros del grupo existente. Si el grupo de aplicaciones no se encuentra configurado para compartir contraseñas, el elemento group se omite.

Valor join	**Valor use-new-password**	**Efecto**
False	False	La nueva credencial se desvincula de las credenciales existentes en el grupo. No se produce ningún efecto sobre el grupo existente.
False	True	La nueva credencial se desvincula de las credenciales existentes en el grupo. No se produce ningún efecto sobre el grupo existente.
True	False	La nueva credencial se une al grupo existente. La contraseña de la nueva credencial es la contraseña que comparten los miembros del grupo existente. Si no hay miembros en el grupo existente, se utiliza el valor password.
True	True	La nueva credencial se une al grupo existente. La contraseña incluida en el comando se utiliza para la nueva credencial y se asigna a todos los miembros del grupo existente.

Valor join	Valor use-new-password	Efecto
		El GUID de la credencial que se devuelve como psoID en la respuesta es el mismo que se enumerará en la operación lookupResponse. También puede utilizarse para identificar esta credencial secundaria en una operación modifyRequest o deleteRequest.

batchRequest: Ejecución de un lote

Feb 07, 2011

La operación batchRequest funciona como un contenedor para una lista que enumera otras operaciones (requestnameRequest). Single Sign-on sólo admite el modo de procesamiento secuencial. Si batchRequest especifica un procesamiento paralelo, no se genera un error, pero el procesamiento se realiza de forma secuencial.

Sintaxis

```
AuthToken Credential name appdefGuid janed pwd123 AuthToken Credential name appdefGuid2 salima pass123
```

Parámetros

processing (obligatorio)	Este es el modo de procesamiento. Los valores válidos son "sequential" y "parallel"; no obstante, Single Sign-on sólo admite el modo secuencial. Cuando se especifica un modo de procesamiento paralelo, Single Sign-on procesa la solicitud de forma secuencial.
onError	Esta es la medida que el usuario desea que Single Sign-on tome cuando se produce un error durante el procesamiento. Los valores válidos son "resume" y "exit".
requestnameRequest (obligatorio, variable)	Indica cada solicitud que el usuario desea procesar en este lote mediante la sintaxis y los parámetros especificados para esa solicitud.

Sintaxis para los valores de retorno (batchResponse)

Parámetros para los valores de retorno (batchResponse)

requestnameResponse (variable)	Indica el nombre de cada solicitud que se especificó para procesar en esta solicitud de lote. Para ver la sintaxis de los valores de retorno relacionados con cada solicitud, consulte la documentación para esa solicitud.

Eliminación de una credencial: deleteRequest

Feb 07, 2011

Use la operación deleteRequest para eliminar una sola credencial. El GUID de la credencial especifica la credencial que se va a eliminar.

Sintaxis

AuthToken

Parámetros

requestID (obligatorio)	Este es el ID generado por el cliente que asocia los valores de retorno con esta solicitud.
executionMode (obligatorio)	Single Sign-on admite el modo de ejecución sincrónica.
authentication-token (obligatorio)	El elemento auth-token es obligatorio pero no se utiliza en esta oportunidad.
psoID (obligatorio)	El elemento psoID es un identificador único para cada usuario final; PSOID es el número de identificación único (GUID) de la credencial que devuelve lookupResponse.
containerID (obligatorio)	El elemento containerID proporciona el nombre de dominio completo (FQDN) del usuario que posee la credencial.

Sintaxis para los valores de retorno

Parámetros para los valores de retorno

status (obligatorio)	Valores posibles: Success, Failure, Pending
requestID	Este es el ID generado por el cliente que asocia estos valores de retorno con la solicitud asociada.

Eliminación de un usuario: deleteRequest

Feb 06, 2011

Use la operación deleteRequest para eliminar todos los datos asociados a un usuario desde el almacén central.

Sintaxis

AuthToken

Parámetros

requestID (obligatorio)	Este es el ID generado por el cliente que asocia los valores de retorno con esta solicitud.
executionMode	Single Sign-on admite el modo de ejecución sincrónica.
authentication-token	El elemento authentication-token es obligatorio pero no se utiliza en esta oportunidad.
psoID (obligatorio)	El elemento psoID es un identificador único para cada usuario final; PSOID es el número de identificación único (GUID) de la credencial que devuelve lookupResponse.

Sintaxis para los valores de retorno (deleteResponse)

Parámetros para los valores de retorno

status (obligatorio)	Valores posibles: Success, Failure, Pending
requestID (obligatorio)	Este es el ID generado por el cliente que asocia estos valores de retorno con la solicitud asociada.

Comentarios

Puede optar por eliminar completamente los datos asociados a usuarios específicos que abandonan la empresa. Además, si los usuarios olvidan información esencial y no pueden acceder a sus credenciales, puede optar por restablecer su estado de Single Sign-on para que puedan comenzar de cero (consulte resetRequest).

Es necesario diferenciar estas dos situaciones, la eliminación completa de los datos y el restablecimiento de los datos, ya que el Single Sign-on Plug-in se comporta de un modo diferente en cada caso. Según los parámetros que establezca el administrador, es posible que exista una copia local de los datos de Single Sign-on del usuario en el perfil del usuario. Si no existen datos para el usuario en el almacén central, el plug-in ejecuta un asistente de registro y copia los datos locales del usuario en el almacén central.

En la situación de restablecimiento del usuario, el software del plug-in descarta los datos locales y luego ejecuta el asistente de registro.

Consulta de destinos: listTargetsRequest

Feb 07, 2011

La operación listTargetsRequest realiza consultas sobre los destinos configurados en el sistema. El Servicio Single Sign-on admite un solo destino único (el módulo de aprovisionamiento) que se identifica mediante el targetID "CPM Provisioning 1.0.".

Sintaxis

```
AuthToken
```

Parámetros

requestID (obligatorio)	Este es el ID generado por el cliente que asocia los valores de retorno con esta solicitud.
executionMode (obligatorio)	Single Sign-on admite el modo de ejecución sincrónica.
authentication-token (obligatorio)	El elemento authentication-token es obligatorio pero no se utiliza en esta oportunidad.

Sintaxis para los valores de retorno

Parámetros para los valores de retorno

requestID (obligatorio)	Este es el ID generado por el cliente que asocia estos valores de retorno con la solicitud asociada.
status (obligatorio)	Valores posibles: Success, Failure, Pending
targetID (obligatorio)	Este es el ID del módulo de aprovisionamiento: targetID="CPM Provisioning 1.0".
schema (obligatorio)	La respuesta de esta operación contiene un ID único para el módulo y un esquema que describe los objetos que administra el módulo de aprovisionamiento, como los usuarios y sus credenciales secundarias.

Obtención de una lista de las aplicaciones disponibles para el usuario: lookupApplicationRequest

Feb 07, 2011

Use la operación lookupApplicationRequest para obtener una lista de las aplicaciones (incluidos los ID de aplicación) disponibles para un usuario específico. En Single Sign-on, la configuración de usuario asociada al usuario en la consola determina el conjunto de definiciones de aplicación disponibles para un usuario. Estas definiciones de aplicación no pertenecen a un usuario y no pueden modificarse fuera de la consola.

Sintaxis

```
AuthToken
```

Parámetros

requestID (obligatorio)	Este es el ID generado por el cliente que asocia los valores de retorno con esta solicitud.
authentication-token (obligatorio)	El elemento authentication-token es obligatorio pero no se utiliza en esta oportunidad.
psoID (obligatorio)	El elemento psoID es un identificador único para cada usuario final; PSOID es el nombre de dominio completamente calificado (FQDN) del usuario.

Sintaxis para los valores de retorno: lookupApplicationResponse

```
app-GUID1 Outlook Outlook 2003 Domain app-GUID2 Vantive Bug Database SAP
```

Parámetros para los valores de retorno

status (obligatorio)	Valores posibles: Success, Failure, Pending
requestID (obligatorio)	Este es el ID generado por el cliente que asocia estos valores de retorno con la solicitud asociada.
psoID (obligatorio)	El elemento psoID es un identificador único para cada usuario final; PSOID es el nombre de dominio completamente calificado (FQDN) del usuario.
data (obligatorio)	El elemento data es la descripción de los datos que se encuentran bajo modificación. Este es el elemento credential y puede incluir cualquier elemento secundario de la credencial o cualquier elemento de la aplicación.
ctxs:application (obligatorio)	El elemento application se utiliza para describir una definición de aplicación y los detalles de una credencial. El elemento application debe coincidir con uno previamente obtenido de una operación lookupApplicationRequest. Hay exactamente un elemento application para cada elemento application de cada definición de aplicación disponible en la configuración de usuario. Consulte ctxs:application para obtener información.

Comentarios

Una búsqueda de este tipo de datos constituye una anomalía que la semántica SPML estándar no abarca. Se utiliza una característica personalizada para obtener la lista de definiciones de aplicación disponibles para un usuario.

Obtención de una lista de aplicaciones para las cuales se almacenan credenciales: lookupRequest

Mar 24, 2011

Use la operación lookupRequest para obtener la lista de aplicaciones para las cuales el usuario ha almacenado credenciales. El valor del atributo returnData determina el nivel de detalles que se devuelve.

Sintaxis

```
AuthToken
```

Parámetros

requestID (obligatorio)	Este es el ID generado por el cliente que asocia los valores de retorno con esta solicitud.
returnData (obligatorio)	data: detalles de una credencial secundaria. identifier: lista de credenciales para un usuario. name: no es compatible con Single Sign-on. everything: definiciones de aplicación disponibles para el usuario especificado.
executionMode (obligatorio)	Single Sign-on admite el modo de ejecución sincrónica.
authentication-token (obligatorio)	El elemento authentication-token es obligatorio pero no se utiliza en esta oportunidad.
psoID (obligatorio)	El elemento psoID es un identificador único para cada usuario final; PSOID es el número de identificación único (GUID) de la credencial que devuelve lookupResponse.

Sintaxis para los valores de retorno: lookupResponse

```
credential-GUID1 Aviva Aviva 5250 Demo Aviva 5250  app-GUID1 Aviva 5250 Demo AppGroup  credential-GUID2 Dynamic App1
```

Parámetros para los valores de retorno

status (obligatorio)	Valores posibles: Success, Failure, Pending
requestID (obligatorio)	Este es el ID generado por el cliente que asocia estos valores de retorno con la solicitud asociada.
pso (obligatorio)	Los datos de pso representan una credencial según se describe en ctxs:credential.
psoID (obligatorio)	El elemento psoID es un identificador único para cada usuario final; PSOID es el nombre de dominio completamente calificado (FQDN) del usuario. Según el modelo SPML de Single Sign-on, los datos de pso representan una credencial como se describe en ctxs:credential. Estos se incluyen si el atributo returnData se configura en data o everything. Hay exactamente un elemento pso para cada credencial secundaria. El atributo ID del elemento psoID proporciona el GUID de la credencial.
data (obligatorio)	Data es la descripción de los datos que se buscaron. Este es el elemento credential y puede incluir cualquier elemento secundario de la credencial o cualquier elemento de la aplicación.

ctxs:credential (obligatorio)	El elemento credential se utiliza para describir una sola credencial secundaria. El nombre y la descripción derivados del elemento credential son opcionales. Si no se proporcionan, el plug-in utiliza el nombre y la descripción de la definición de aplicación. Consulte ctx:credential para obtener más información.
ctxs:application (obligatorio)	El elemento application se utiliza para describir una definición de aplicación y los detalles de una credencial. El elemento application debe coincidir con uno previamente obtenido de una operación lookupApplicationRequest. Hay exactamente un elemento application para cada definición de aplicación en la configuración de usuario del usuario. Consulte ctxs:application para obtener información.

Comentarios

Cuando una operación lookupRequest especifica una credencial, la respuesta contiene los detalles de la credencial. En general, el software del plug-in cifra los secretos de cada credencial y el módulo de aprovisionamiento no puede acceder a ellos. Eso significa que los datos con caracteres de los elementos de campo específicos quedan vacíos en las credenciales que ya se encuentran bajo la administración del software del plug-in.

El aprovisionamiento es un proceso de dos pasos. Primero, el módulo de aprovisionamiento pone en cola los comandos de aprovisionamiento. A continuación, el software del plug-in ejecuta los comandos en cola. Para poder verificar una acción recientemente ejecutada, la lista de credenciales devuelta debe dar cuenta de los comandos en cola. Como los comandos en cola se encuentran bajo la protección del módulo de aprovisionamiento y no del software del plug-in, el módulo de aprovisionamiento puede descifrar los parámetros de los comandos. Las credenciales que contienen comandos o en cola también incluyen en la operación lookupResponse los parámetros de los comandos a los que se puede acceder. Tenga en cuenta que los parámetros de los comandos pueden incluir los valores userID, password y custom-field.

Recuperación de credenciales secundarias: lookupRequest

Feb 06, 2011

Use esta operación para recuperar los detalles de una credencial secundaria.

Sintaxis

AuthToken

Parámetros

requestID (obligatorio)	Este es el ID generado por el cliente que asocia los valores de retorno con esta solicitud.
returnData (obligatorio)	data: detalles de una credencial secundaria. identifier: lista de credenciales para un usuario. name: no es compatible con Single Sign-on. everything: definiciones de aplicación disponibles para el usuario especificado.
executionMode (obligatorio)	Sólo se admite el modo de ejecución sincrónica. Todas las solicitudes de uso de la ejecución sincrónica generan errores unsupportedExecutionMode.
authentication-token (obligatorio)	El elemento authentication-token es obligatorio pero no se utiliza en esta oportunidad.
psoID (obligatorio)	El elemento psoID es un identificador único para cada usuario final; PSOID es el nombre de dominio completamente calificado (FQDN) del usuario.
containerID (obligatorio)	El elemento containerID proporciona el nombre de dominio completo (FQDN) del usuario que posee la credencial.

Sintaxis para los valores de retorno: lookupResponse

Credential-name Admin text Credential description app-GUID Outlook description from app-def Domain

Parámetros para los valores de retorno

status (obligatorio)	Valores posibles: Success, Failure, Pending
requestID (obligatorio)	Este es el ID generado por el cliente que asocia estos valores de retorno con la solicitud asociada.
psoID (obligatorio)	El elemento psoID es un identificador único para cada usuario final; PSOID es el nombre de dominio completamente calificado (FQDN) del usuario. Según el modelo SPML de Single Sign-on, los datos de pso representan una credencial como se describe en Elemento ctxs:credential. Estos se incluyen si el

	atributo returnData se configura en data o everything. Hay exactamente un elemento pso para cada credencial secundaria. El atributo ID del elemento psoID proporciona el GUID de la credencial.
containerID (obligatorio)	El elemento containerID proporciona el nombre de dominio completo (FQDN) del usuario que posee la credencial.
data (obligatorio)	Data es la descripción de los datos que se buscaron. Este es el elemento credential y puede incluir cualquier elemento secundario de la credencial o cualquier elemento de la aplicación.
ctxs:credential (obligatorio)	El elemento credential se utiliza para describir una sola credencial secundaria. El nombre y la descripción derivados del elemento credential son opcionales. Si no se proporcionan, Single Sign-on Plug-in utiliza el nombre y la descripción de la definición de aplicación. Consulte Elemento ctxs:credential para obtener más información.
ctxs:application (obligatorio)	El elemento application se utiliza para describir una definición de aplicación y los detalles de una credencial. El elemento application debe coincidir con uno previamente obtenido de una operación lookupApplicationRequest. Hay exactamente un elemento application para cada definición de aplicación en la configuración de usuario del usuario. Consulte Elemento ctxs:credential para obtener más información.

Modificación de una credencial: modifyRequest

Apr 22, 2011

Use la operación modifyRequest para modificar una credencial previamente aprovisionada. Si la definición de aplicación asociada a la credencial modificada es un miembro del grupo de contraseñas compartidas, se actualizan todas las credenciales asociadas a los miembros de ese grupo para usar la nueva contraseña.

Sintaxis

```
AuthToken   New Credential Name   username
```

Parámetros

requestID (obligatorio)	Este es el ID generado por el cliente que asocia los valores de retorno con esta solicitud.
ctxs:authentication-token	El elemento authentication-token es obligatorio pero no se utiliza en esta oportunidad.
psoID (obligatorio)	El ID de la credencial es un GUID (creado por el sistema Single Sign-on y almacenado en el almacén central). Debe coincidir con el valor que devuelve lookupRequest y se utiliza para localizar la credencial que se está modificando.
containerID (obligatorio)	El elemento containerID proporciona el nombre de dominio completo (FQDN) del usuario que posee la credencial.
modification (obligatorio)	modificationMode (opcional) add: para agregar credenciales. Esto produce el mismo resultado que addRequest. Si modificationMode se configura en add, las restricciones en los elementos psoID y data son las mismas que en addRequest. El elemento psoID sólo debe especificar un contenedor (como en deleteRequest) y el elemento data debe contener un elemento credential (como en addRequest). replace: para reemplazar un valor de campo, coloque el nuevo valor en la etiqueta. delete: para borrar un valor de campo. Se omite el contenido del elemento data.
data (obligatorio)	El elemento data es la descripción de los datos que se encuentran bajo modificación. Este es el elemento credential y puede incluir cualquier elemento secundario de la credencial o cualquier elemento de la aplicación.
credential (obligatorio)	El elemento credential se utiliza para describir una sola credencial secundaria. El nombre y la descripción derivados del elemento credential son opcionales. Si no se proporcionan, el plug-in utiliza el nombre y la descripción de la definición de aplicación. Consulte ctx:credential para obtener más información.
name	El elemento name es el nombre de la definición de aplicación tal como aparece en el componente Single Sign-on de AppCenter.
application	El elemento application se utiliza para describir una definición de aplicación y los detalles de una

(obligatorio)	credencial. El elemento application debe coincidir con uno previamente obtenido de una operación lookupApplicationsRequest. Consulte ctxs:application para obtener información. Si se proporciona un elemento secundario de ID, este elemento debe coincidir con el valor almacenado en la credencial.
group	Si el elemento group no forma parte de la solicitud de incorporación, se proporcionan valores predeterminados. Este elemento describe la relación entre la credencial nueva y las credenciales existentes asociadas al grupo. Consulte la información sobre los atributos del elemento group.
fields (obligatorio)	Cada elemento secundario del elemento fields enumerado en la operación lookupResponse debe incluirse en la operación addRequest; de lo contrario, se devuelve un error.
userID (obligatorio)	El elemento userID proporciona la cuenta del usuario para esta credencial.
password (obligatorio)	El elemento password proporciona la contraseña del usuario asociada a esta credencial.
custom-field	Los elementos custom-field proporcionan valores personalizados para esta credencial. Single Sign-on admite dos campos personalizados además de los campos de nombre de usuario y contraseña.
psoID (obligatorio)	El elemento psoID es un identificador único para cada usuario final; PSOID es el nombre de dominio completo (FQDN) del usuario y se utiliza para especificar el contenedor de la credencial que se está modificando.

Sintaxis para los valores de retorno: modifyResponse

Parámetros para los valores de retorno

status (obligatorio)	Valores posibles: Success, Failure, Pending
requestID (obligatorio)	Este es el ID generado por el cliente que asocia estos valores de retorno con la solicitud asociada.

Comentarios

El elemento modifyRequest puede utilizarse para solicitar que una credencial desvinculada se una al grupo mediante la configuración del atributo join en "true" (consulte addRequest). El elemento group está sujeto a las mismas limitaciones y genera el mismo efecto que se describe en addRequest.

Tenga en cuenta que cualquiera de los subelementos de ctxs:fields definidos para la aplicación pueden estar incluidos en modifyRequest. Los campos disponibles se enumeran en
— lookupResponse
.

Atributos del elemento group

Valor join	Valor use-new-password	Efecto
False	True	La nueva credencial se desvincula de las credenciales existentes en el grupo. No se produce ningún efecto sobre el grupo existente.
True	False	La nueva credencial se une al grupo existente. La contraseña de la nueva credencial es la contraseña que comparten los miembros del grupo existente. Si no hay miembros en el grupo existente, se utiliza el valor password.
True	True	La nueva credencial se une al grupo existente. La contraseña incluida en el comando se utiliza para la nueva credencial y se asigna a todos los miembros del grupo existente.

El GUID de la credencial que se devuelve como psoID en la respuesta es el mismo que se enumerará en la operación lookupResponse. También puede utilizarse para identificar esta credencial secundaria en una operación modifyRequest o deleteRequest.

Restablecimiento de un usuario: resetRequest

Feb 07, 2011

Use la operación resetRequest para restablecer el estado de Single Sign-on de los usuarios cuando no pueden acceder a sus credenciales.

Sintaxis

```
AuthToken
```

Parámetros

requestID (obligatorio)	Este es el ID generado por el cliente que asocia los valores de retorno con esta solicitud.
executionMode	Single Sign-on admite el modo de ejecución sincrónica.
authentication-token	El elemento authentication-token es obligatorio pero no se utiliza en esta oportunidad.
psoID (obligatorio)	El elemento psoID es un identificador único para cada usuario final; PSOID es el nombre de dominio completamente calificado (FQDN) del usuario.

Sintaxis para los valores de retorno: resetResponse

Parámetros para los valores de retorno

status (obligatorio)	Valores posibles: Success, Failure, Pending
requestID (obligatorio)	Este es el ID generado por el cliente que asocia estos valores de retorno con la solicitud asociada.

Elementos del espacio de nombres

May 11, 2015

Todos los elementos personalizados de Single Sign-on que se utilizan en los comandos SPML son miembros del espacio de nombres http://citrix.com/Provision. Este espacio de nombres también se conoce como prefijo ctxs. Existen tres elementos superiores en este espacio de nombres que se utilizan en los comandos SPML: authentication-token, application y credential.

Elemento authentication-token: ctxs:authentication-token

El elemento authentication-token se utiliza como contenedor para el token de autenticación (AuthToken). Este elemento es obligatorio pero no se utiliza. El elemento authentication-token no incluye elementos secundarios.

Sintaxis

```
AuthToken
```

Elemento application: ctxs:application

El elemento application puede presentarse como un elemento superior o como un elemento secundario del elemento credential.

El elemento application se utiliza para describir una definición de aplicación (consulte lookupApplicationRequest) y los detalles de una credencial (consulte addRequest).

Sintaxis

```
app-GUID Outlook description from app-def  Domain
```

Nota: Ninguno de los elementos secundarios del elemento "fields" contiene datos con caracteres en este ejemplo.

Parámetros

ctxsID (obligatorio)	Especifica el GUID asignado a la definición de aplicación cuando se crea en la consola.
name	Especifica el nombre definido por el administrador para la definición de aplicación.
description	Especifica la descripción definida por el administrador para la definición de aplicación.
group (obligatorio si se utilizan contraseñas compartidas)	Especifica el grupo de aplicaciones al que se asigna esta definición en la consola. El atributo de las contraseñas compartidas es un valor booleano que se utiliza para indicar si este grupo se ha configurado para compartir contraseñas. Para obtener más información, consulte addRequest.
fields (obligatorio)	Enumera los campos de datos que se van a configurar para las credenciales mediante esta definición de aplicación. Es posible definir cualquier subconjunto de los campos enumerados para cualquier definición de aplicación determinada. Elementos secundarios del elemento fields:

	• userID: corresponde al ID de usuario. • password: corresponde a la contraseña del usuario. • custom-field: corresponde a los campos personalizados que pueden incluirse en una definición; el atributo index indica el campo en particular ("1" o "2") y el atributo label contiene el texto opcional de la etiqueta.

Consulte ctxs:credential para obtener un ejemplo de un elemento application que funcione como elemento secundario de un elemento credential.

Elemento credential: ctxs:credential

El elemento credential se utiliza para describir una sola credencial secundaria. La mayoría de las credenciales se asocian a una definición de aplicación determinada; esto se expresa mediante un elemento application secundario. Las credenciales que los usuarios ingresan manualmente no contienen un elemento application.

Sintaxis

```
Credential Name user visible description  optional-RA provided-description   appdefGuid  johnd pass123 mydomain
```

Parámetros

status (obligatorio)	El atributo status del elemento credential indica el estado de esta credencial desde la perspectiva de Single Sign-on Plug-in. El estado puede ser activo o en cola. Un valor activo significa que la credencial se encuentra disponible para que el Single Sign-on Plug-in la utilice. Un valor en cola significa que un comando para agregar la credencial se encuentra en cola pero que Single Sign-on Plug-in todavía no ha procesado ese comando.
pendingAction	El atributo pendingAction del elemento credential indica si existen comandos en cola que afectan a esta credencial. Los valores de pendingAction son agregar, modificar y eliminar. Un valor delete indica que se ha colocado un comando en cola para esta credencial. Un valor modify indica que se ha colocado un comando en cola para esta credencial. Este atributo es opcional y se omite cuando no se colocan comandos en cola para la credencial.
name	El atributo name del elemento credential es el valor que el Single Sign-on Plug-in muestra en la ventana Administrar contraseñas (anteriormente conocida como Administrador de inicios de sesión). El usuario puede editar este valor mediante la página de propiedades de la credencial.
description	El valor description del elemento credential es el valor que el Single Sign-on Plug-in muestra en la ventana Administrar contraseñas (anteriormente conocida como Administrador de inicios de sesión). El usuario puede editar este valor mediante la página de propiedades de la credencial.
provision-description	El elemento provision-description contiene los datos del administrador que el Single Sign-on Plug-in no puede ver ni modificar. Este elemento se suministra únicamente para la comodidad del administrador de aprovisionamiento.
application	El elemento application indica el ID de la definición de aplicación, así como los datos con caracteres para los elementos userID, password y custom-field que proporcionan los detalles del usuario para esta credencial.