Autoservicio de restablecimiento de contraseñas 1.0

Nov 02, 2016

Acerca del Autoservicio de restablecimiento de contraseñas

Sep 19, 2016

El Autoservicio de restablecimiento de contraseñas o SSPR (Self-service Password Reset) permite que los usuarios finales tengan un mayor control sobre sus cuentas. Cuando el Autoservicio de restablecimiento de contraseñas está configurado, si los usuarios finales tienen problemas para iniciar sesión en sus sistemas, pueden desbloquear sus cuentas o restablecer sus contraseñas respondiendo correctamente a varias preguntas de seguridad.

El restablecimiento de contraseñas de usuario es un proceso que afecta directamente a la seguridad. Le recomendamos que consulte el artículo Configuración segura para asegurarse de configurar correctamente su entorno.

El Autoservicio de restablecimiento de contraseñas consta de tres componentes:

- Consola de configuración del Autoservicio de restablecimiento de contraseñas
- Servicio de Autoservicio de restablecimiento de contraseñas
- Inscripción de preguntas de seguridad en StoreFront

Consola de configuración del Autoservicio de restablecimiento de contraseñas

- **Configuración del servicio.** Configura el servicio del Autoservicio de restablecimiento de contraseñas, incluida la dirección del almacén central, la cuenta del proxy de datos y la cuenta del Autoservicio de restablecimiento de contraseñas.
  - Dirección de almacén central: Ubicación del recurso compartido de red donde se guardan los datos del Autoservicio de restablecimiento de contraseñas.
  - Cuenta del proxy de datos: Cuenta que se comunica con el almacén central. La cuenta requiere permisos de lectura y escritura en el almacén central.
  - Cuenta del Autoservicio de restablecimiento de contraseñas: Cuenta que se utiliza para desbloquear la cuenta y restablecer la contraseña.
- **Configuración de usuario.** Configura el usuario, grupo o unidad organizativa que puede usar la función de Autoservicio de restablecimiento de contraseñas y especifica la dirección del servidor de licencias y la dirección del servicio predeterminada.
  - Nombre de la configuración de usuario: Define los grupos de usuarios de destino del servicio de Autoservicio de restablecimiento de contraseñas, que pueden incluir, grupos y unidades organizativas de Active Directory.
  - Dirección del servidor de licencias: Solo se puede usar el Autoservicio de restablecimiento de contraseñas con la edición Platinum de XenApp o XenDesktop. La versión del servidor de licencias debe ser 11.13.1 o una versión posterior.
  - Seleccione o deje sin seleccionar las funciones **Desbloquear** y **Restablecer**.
  - Dirección de servicio predeterminada: Especifique la dirección URL del servicio del Autoservicio de restablecimiento de contraseñas.
- **Verificación de la identidad.** Configura el cuestionario que se usa para la inscripción y para desbloquear o restablecer la contraseña.
  - Agregue una pregunta o un grupo de preguntas al almacén de preguntas desde el cual se generan los cuestionarios.
  - Seleccione una lista de preguntas desde el almacén de preguntas que se usará para la inscripción.
  - Exportar o importar las preguntas y grupos de preguntas de seguridad.

Servicio de Autoservicio de restablecimiento de contraseñas

El servicio de Autoservicio de restablecimiento de contraseñas (Self-Service Password Reset Service) se ejecuta en un servidor Web y permite a los usuarios restablecer sus contraseñas de Windows y desbloquear sus cuentas de Windows. Las solicitudes de los usuarios finales se envían a este servicio a través de StoreFront.

Inscripción de preguntas de seguridad en StoreFront

Utilice StoreFront para permitir que los usuarios inscriban sus respuestas a las preguntas de seguridad. Cuando se hayan inscrito, los usuarios podrán restablecer contraseñas de dominio y desbloquear cuentas de dominio. Para más información, consulte Autoservicio de restablecimiento de contraseñas en la documentación de StoreFront.

Problemas conocidos

Sep 19, 2016

- Después de abrir la consola del Autoservicio de restablecimiento de contraseñas, es posible que no pueda anclarla en la barra de tareas [#646300]

  Solución temporal: Ancle la consola a la barra de tareas desde el acceso directo en el menú **Inicio**.

- Debido a un problema conocido en Windows 2016, no se puede buscar la consola del Autoservicio de restablecimiento de contraseñas en Windows 2016. [#648939]

  Solución temporal: Use el menú **Inicio** para encontrar el Autoservicio de restablecimiento de contraseñas.

- Si la duración mínima de la contraseña en la directiva de contraseñas de la directiva de dominio predeterminada tiene el valor predeterminado (un día), y los usuarios intentan restablecer sus contraseñas pero el restablecimiento falla (por ejemplo, porque no cumplen los requisitos de complejidad exigidos), y cierran el asistente de restablecimiento de contraseñas, no podrán restablecerla de nuevo hasta pasadas 24 horas. [#653221]

- Cuando se usa Citrix Receiver para Mac, el botón de tarea para la inscripción aparece la primera vez que el usuario inicia sesión en StoreFront. Después de cerrar la sesión de StoreFront y, a continuación, iniciar otra sesión, el botón de tarea ya no aparece. [#657263]

  Solución:
  1. Haga clic en Nombre de usuario en la esquina superior derecha del almacén de StoreFront.
  2. Haga clic en el botón **Actualizar aplicaciones** en el menú desplegable.
  3. Cierre Citrix Receiver para Mac, vuelva a abrirlo y el botón de tarea aparecerá.

- Al migrar las preguntas de seguridad desde la Verificación de identidad de Single Sign-on al Autoservicio de restablecimiento de contraseñas, es posible que las preguntas no se muestren en la consola del Autoservicio de restablecimiento de contraseñas, incluso aunque se haga clic en **Actualizar**. [#657277]

  Solución temporal: Cierre la consola y, a continuación, vuelva a abrirla.

- Las preguntas de seguridad del cuestionario que contienen el carácter especial **&** no se muestran durante la inscripción en StoreFront. [#654913]

  Solución temporal: No incluya el carácter **&** en las preguntas de seguridad.

Requisitos del sistema

Nov 02, 2016

> **Important**
>
> Citrix no admite la instalación de los componentes del Autoservicio de restablecimiento de contraseñas en un controlador de dominio. Implemente los componentes del Autoservicio de restablecimiento de contraseñas en servidores dedicados.

En este artículo, se describen los requisitos de hardware y software para el Autoservicio de restablecimiento de contraseñas. En esta sección se presupone que todos los equipos cumplen los requisitos de hardware mínimos para el sistema operativo instalado.

Software

Los equipos del entorno del Autoservicio de restablecimiento de contraseñas pueden requerir el siguiente software de sistema:

- **Windows 2016, Windows 2012 R2, Windows 2008 R2** (Se recomienda usar Windows Server 2008 R2 solo con un recurso compartido de archivos local y aplicar una configuración de restricción de acceso adecuada. Para obtener más información, consulte Creación de un almacén central). **Nota**: Necesario para el servidor de Autoservicio de restablecimiento de contraseñas.
- **Microsoft Windows Installer 2.0 o posterior**: Necesario para todos los sistemas.
- **Microsoft .NET Framework**: Necesario para el servidor del Autoservicio de restablecimiento de contraseñas.
  - 4.6.x (Windows 2016)
  - 4.5.2 (Windows 2012 R2)
  - 3.5.1 (Windows 2008 R2)
- **Internet Information Services (IIS)**: Necesario para el servidor del Autoservicio de restablecimiento de contraseñas.
  - IIS 10.0 (Windows 2016)
  - IIS 8.5 (Windows 2012 R2)
  - IIS 7.5 (Windows 2008 R2)

Servidor de Autoservicio de restablecimiento de contraseñas

- Componente del Autoservicio de restablecimiento de contraseñas: Almacén central
- Entorno respaldado: Recurso compartido SMB
- Requisitos de hardware: 30 KB de espacio en disco por cada usuario

Requisitos de ASP.NET 3.5/4.X

El componente de ASP.NET para la versión de .NET Framework en su equipo Windows Server.

Requisitos de seguridad y de cuentas

Antes de instalar el servicio de Autoservicio de restablecimiento de contraseñas hay que asegurarse de que las cuentas y los componentes necesarios para respaldar el servicio están disponibles. Además, debido a que el servicio utiliza HTTP seguro (HTTPS), requiere un certificado de autenticación de servidor para la comunicación TLS (Transport Layer Security) con StoreFront.

Requisito de autenticación de servidor:

Antes de instalar el servicio, obtenga un certificado de autenticación del servidor para la comunicación TLS desde una entidad de certificación (CA) o desde su propia infraestructura de claves públicas (PKI), si dispone de una.

Cuentas necesarias para los módulos del servicio:

Nota: Asegúrese de que estas cuentas no caduquen.

El servicio del Autoservicio de restablecimiento de contraseñas necesita estos tipos de cuenta para leer y escribir datos mientras actúa en el entorno:

- Cuenta de proxy de datos
- Cuenta del autoservicio

Cuando distintos módulos requieran el mismo tipo de cuenta, puede usar la misma cuenta para varios módulos, o puede especificar cuentas personalizadas distintas para cada uno.

- **Cuenta de proxy de datos**

  Requiere permisos de lectura y escritura en el almacén central. Para obtener más información, consulte Creación de un almacén central.

- **Cuenta del autoservicio**

  Requiere privilegios suficientes para desbloquear y restablecer la contraseña de los usuarios especificados en la Configuración de usuario. Para obtener más información consulte Configuración segura.

StoreFront

StoreFront 3.7

Citrix Receivers

Respaldados:

- Citrix Receiver para Web
- Citrix Receiver para Windows
- Citrix Receiver para Linux

No respaldados:

- Citrix Receiver para Mac
- Citrix Receiver para Chrome
- Dispositivos móviles (aunque incluyan Receiver para Web)

Uso externo con NetScaler Gateway

No respaldado

Instalación y configuración

Sep 19, 2016

Este artículo consta de las siguientes secciones:

Lista de verificación de la Instalación y la configuración

Antes de iniciar la instalación, complete esta lista:

✓	Paso
	Elija los equipos de su entorno donde instalará el software y prepárelos para la instalación. Consulte Requisitos del sistema.
	Instale el certificado TLS y las cuentas necesarias para el servicio. Consulte *Requisitos de seguridad y de cuentas* en Requisitos del sistema.
	Instale el servidor de licencias. Consulte la documentación del servidor de licencias.
	Crear un almacén central. Consulte Creación de un almacén central.
	Instale el Autoservicio de restablecimiento de contraseñas. Consulte Instalación y configuración del Autoservicio de restablecimiento de contraseñas.
	Configure el Autoservicio de restablecimiento de contraseñas usando la consola. Consulte Instalación y configuración del Autoservicio de restablecimiento de contraseñas.
	Configure el Autoservicio de restablecimiento de contraseñas en StoreFront. Consulte Configuración de StoreFront.
	Asegúrese de que el Autoservicio de restablecimiento de contraseñas está configurado de forma segura. Consulte el artículo Configuración segura.

Instale el certificado SSL y las cuentas necesarias para el servicio. Consulte Requisitos de seguridad y de cuentas.

Instale el certificado SSL y las cuentas necesarias para el servicio. Consulte Requisitos de seguridad y de cuentas.

Configure el Autoservicio de restablecimiento de contraseñas en StoreFront. Consulte Configuración de StoreFront.

Orden de la instalación y la configuración

Para instalar el servicio y ejecutar el Asistente de configuración del servicio, debe iniciar una sesión con una cuenta de usuario de dominio que pertenezca al grupo Administradores locales del servidor.

Se recomienda instalar el Autoservicio de restablecimiento de contraseñas en este orden:

1. Instale o actualice el servidor de licencias a la versión 11.13.1.2 como mínimo. Descargue el servidor de licencias desde https://www.citrix.com/downloads/licensing.html.
2. Cree el almacén central.
3. Instale el Autoservicio de restablecimiento de contraseñas.
4. Configure el Autoservicio de restablecimiento de contraseñas en la consola.
5. Configure StoreFront con la dirección del servidor de Autoservicio de restablecimiento de contraseñas.

Creación de un almacén central

Por motivos de seguridad, se recomienda crear el almacén central directamente en la máquina donde se ejecuta el servicio de Autoservicio de restablecimiento de contraseñas. Para las implementaciones donde son necesarios varios servidores de Autoservicio de restablecimiento de contraseñas, se puede alojar el almacén central en un recurso compartido de red remoto, si el servidor de Autoservicio de restablecimiento de contraseñas y el servidor que aloja el recurso compartido dan respaldo al cifrado de SMB.

Esta función solo está disponible en Windows Server 2012 R2 o Windows Server 2016; por lo tanto, no se da respaldo a Windows Server 2008 R2 cuando se utiliza un recurso compartido de archivos remoto para el almacén central.

Creación de la cuenta del proxy de datos

Cree un usuario de dominio normal para usarlo como cuenta de proxy de datos. No configure un usuario del grupo de Administradores de dominio ni del grupo Administradores locales como cuenta del proxy de datos.

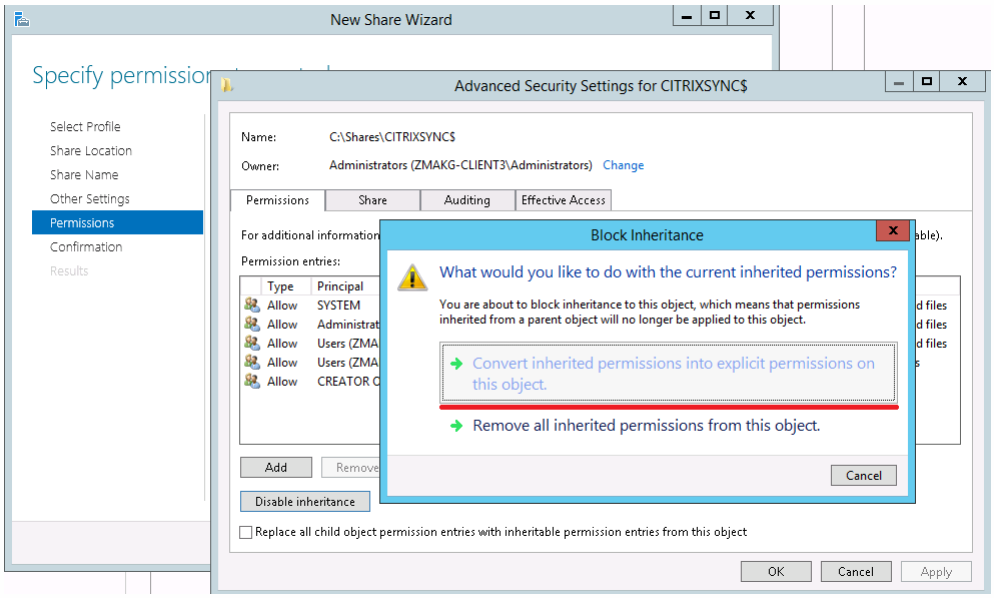
Creación de un almacén central para Windows Server 2012 R2 o Windows Server 2016

Cuando se utiliza Windows Server 2012 R2 o Windows Server 2016 para actuar como servidores de Autoservicio de restablecimiento de contraseñas y como almacén central, se puede usar un recurso compartido de red remoto si se configura como se describe en esta sección. Asegúrese de que la casilla **Cifrar acceso a datos** está seleccionada y aplique las instrucciones proporcionadas en Configuración segura.

1. Para iniciar el asistente **Nuevo recurso compartido**, abra el Administrador del servidor. En la página de detalles de **Servicios de archivos y almacenamiento**, seleccione **Recursos compartidos** en

el panel izquierdo y haga clic en **Tareas > Nuevo recurso compartido**.

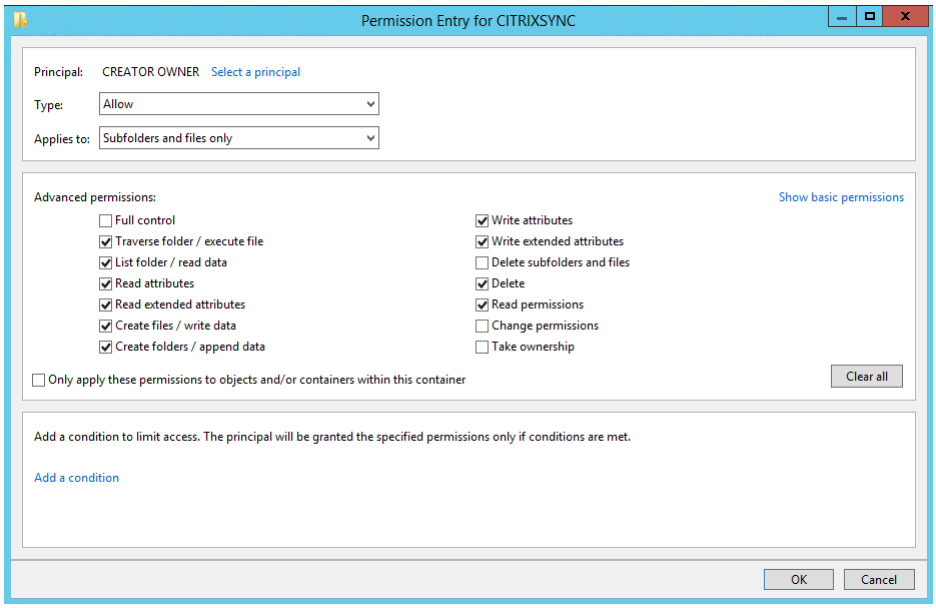
2. Elija **Seleccionar perfil** en el panel izquierdo, seleccione **Recurso compartido SMB - Rápido**, y haga clic en **Siguiente**.
3. Seleccione **Compartir Ubicación** en el panel izquierdo. En la lista, seleccione el servidor donde quiere crear el nuevo recurso compartido y el volumen donde crear la nueva carpeta compartida, y haga clic en **Siguiente**.
4. Seleccione **Nombre del recurso compartido** en el panel de la izquierda, escriba el nombre de su nuevo recurso compartido, por ejemplo **CITRIXSYNC$** y haga clic en **Siguiente**.
5. Seleccione **Otra configuración**, en el panel izquierdo, seleccione **Cifrar acceso a datos**, deje sin seleccionar **Permitir almacenamiento en caché del recurso compartido** y haga clic en **Siguiente**.
6. Para modificar los permisos del **Recurso compartido**, elija **Permisos** en el panel izquierdo y, a continuación, seleccione **Personalizar permisos > Recurso compartido**
   o Quite **Todos**
   o Agregue **Cuenta de proxy de datos** con control total
   o Agregue **Administradores locales** con control total
   o Agregue **Administradores de dominio** con control total
   o Agregue **Servicio de red** con permiso de lectura para el recurso compartido de archivos local
7. Para personalizar los permisos NTFS, elija **Permisos** en el panel izquierdo, seleccione **Personalizar permisos**, haga clic en **Deshabilitar herencia**, y seleccione **Convertir los permisos heredados en permisos explícitos en este objeto**.



8. Para quitar todos los usuarios excepto **CREATOR OWNER/Local Administrators/SYSTEM**, en **Personalizar permisos** > **Permisos**, haga clic en **Quitar.**

9. Para modificar **CREATOR OWNER** > **Permisos avanzados**, haga clic en **Modificar** y deje sin marcar estas opciones:

o Control total
o Eliminar subcarpetas y archivos
o Cambiar permisos
o Tomar posesión



10. Agregue una **Cuenta de proxy de datos** con control total.

11. Agregue **Servicio de red** con permisos de lectura para el recurso compartido de archivos local.

12. Elija **Confirmación** en el panel izquierdo del asistente Nuevo recurso compartido, revise los parámetros seleccionados para el uso compartido y haga clic en **Crear** para comenzar el proceso de creación de la nueva carpeta y, a continuación, haga clic en **Cerrar**.

13. Cree dos subcarpetas en la carpeta del recurso compartido **CITRIXSYNC$**: **CentralStoreRoot** y **People**.

Importante: Asegúrese de que la cuenta del proxy de datos tiene **Control total** para estos dos subcarpetas.

Creación de un almacén central para Windows Server 2008 R2

Asegúrese de crear el almacén central en el mismo servidor donde está el servicio del Autoservicio de restablecimiento de contraseñas y configure el Firewall de Windows para impedir el acceso remoto.

1. Cree una carpeta local (**CITRIXSYNC1**) como la raíz del recurso compartido de archivos, y, a continuación, cree dos subcarpetas: **CentralStoreRoot** y **People**.

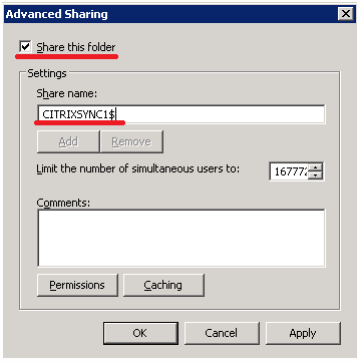
2. Configure un recurso compartido y conceda permisos de uso compartido:

    a. Haga clic con el botón secundario en la carpeta **CITRIXSYNC1**, seleccione **Propiedades > Compartir > Uso compartido avanzado.**

    b. Marque la casilla **Compartir esta carpeta** y establezca el **Nombre de recurso compartido** como **CITRIXSYNC1$**.

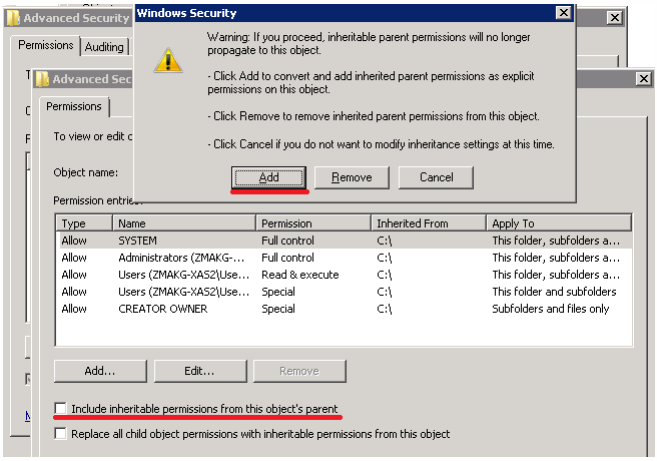
    c. Para conceder permisos de uso compartido, haga clic en **Permisos**, quite todos los usuarios predeterminados, y agregue la **Cuenta del proxy de datos** con permiso de **Control total**, el **Grupo de administradores locales** con permiso de **Control total**, el **Grupo de administradores de dominio** con permiso de **Control total** y **Servicio de red** con permiso de **Lectura**.

    d. Haga clic en **Caché** y marque la casilla **Ningún archivo o programa de la carpeta compartida estará disponible sin conexión**.



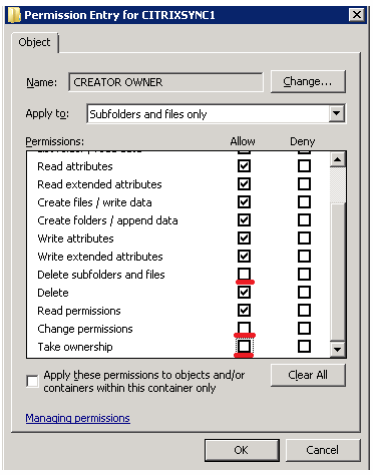
3. Para conceder permisos de seguridad, haga clic con el botón secundario en la carpeta **CITRIXSYNC1** y seleccione **Propiedades** > **Seguridad**.

4. Para inhabilitar los permisos heredables, haga clic en **Opciones avanzadas** > **Cambiar permisos**, deje sin marcar la opción **Incluir todos los permisos heredables del objeto primario de este objeto** y luego haga clic en **Agregar** en la ventana de advertencia.

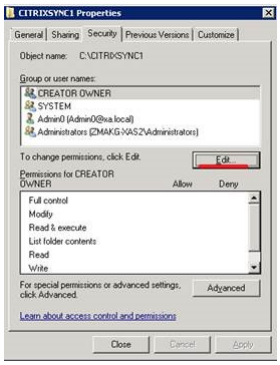


5. Haga clic en **Editar** para modificar los permisos de **CREATOR OWNER** y deje sin marcar lo siguiente:

- Control total
- Eliminar subcarpetas y archivos
- Cambiar permisos
- Tomar posesión



6. Para quitar el grupo de usuarios que no sea necesario y agregar la **Cuenta del proxy de datos**, haga clic en **Editar** en la pantalla de **Propiedades** y elimine todos los usuarios excepto **CREATOR OWNER/SYSTEM/Local Administrators**, y agregue **Cuenta del proxy de datos** con permiso de **Control total**.



7. Agregue **Servicio de red** con permisos de **Lectura**.

8. Para habilitar la función de firma de SMB, haga clic en **Inicio > Herramientas administrativas > Directiva de seguridad local**. En el panel izquierdo, elija **Configuración de seguridad > Directivas locales > Opciones de seguridad**.

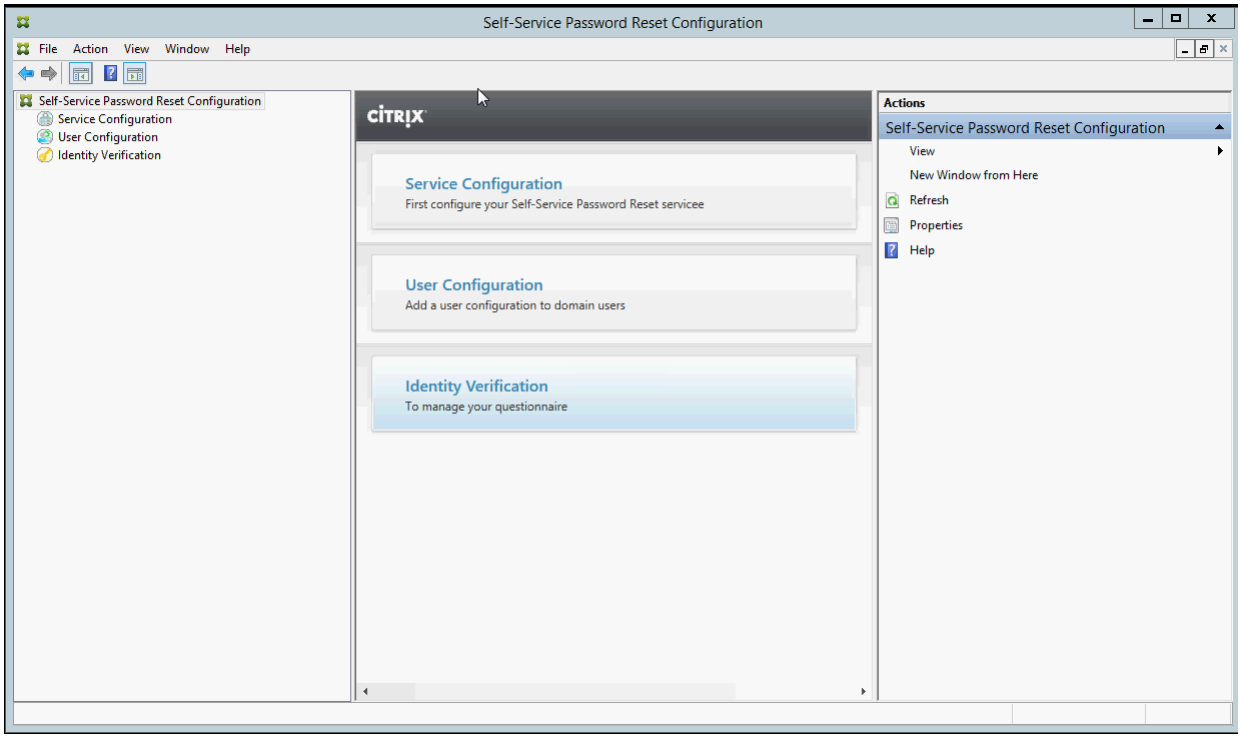
9. Habilite **Cliente de redes de Microsoft: firmar digitalmente las comunicaciones (si el servidor lo permite)** y **Servidor de red Microsoft: firmar digitalmente las comunicaciones (si el cliente lo permite)**.

10. Para impedir el acceso remoto al almacén central local, complete la configuración del Firewall de Windows. Para obtener más información, consulte Configuración de los parámetros del firewall.

Instalación y configuración del Autoservicio de restablecimiento de contraseñas

El paquete de instalación se encuentra en los medios de instalación de XenApp y XenDesktop.

1. Inicie el asistente de instalación del Autoservicio de restablecimiento de contraseñas y siga las instrucciones.
2. Haga clic en **Inicio > Programas > Citrix > Configuración del autoservicio de contraseñas de Citrix** para configurar el servicio de Autoservicio de restablecimiento de contraseñas de Citrix.
3. Cuando la consola se abra, siga estos tres sencillos procedimientos para configurar el servicio.



Configuración del servicio

Antes de configurar el servicio, asegúrese de haber creado el almacén central, la cuenta del proxy de datos y la cuenta del Autoservicio.

1. Seleccione **Configuración del servicio** en el panel central y, a continuación, haga clic en **Nueva configuración del servicio** en el panel de la derecha.
2. En la pantalla **Ubicación del almacén central**, especifique la ubicación del almacén central y haga clic en **Siguiente**.
3. En la pantalla **Configuraciones de dominios**, seleccione un dominio y haga clic en **Propiedades**.
4. Especifique el nombre de usuario de la **Cuenta del proxy de datos** y la contraseña y el nombre de usuario de la **Cuenta del autoservicio** y haga clic en **Aceptar**, **Siguiente** y **Finalizar**.

Configuración de usuario

1. En el panel izquierdo, seleccione **Configuración de usuario** y, a continuación, haga clic en **Nueva configuración de usuario** en el panel derecho.
2. En el cuadro **Nombrar la configuración de usuario**, defina los grupos de usuarios de destino del servicio de Autoservicio de restablecimiento de contraseñas, agregue usuarios, grupos y unidades organizativas desde Active Directory, y haga clic en **Siguiente**.
3. En la pantalla **Configurar las licencias**, especifique el servidor de licencias y haga clic en **Siguiente**.
4. En la pantalla **Configuración de restablecimiento de contraseñas**, utilice las casillas de verificación para especificar si los usuarios pueden restablecer sus contraseñas de Windows y desbloquear sus cuentas de dominio sin necesidad de intervención administrativa, especifique la dirección y el puerto del servicio y, a continuación, haga clic en **Crear**.

Para obtener más información sobre la administración de configuraciones de usuario, consulte Administración de configuraciones de usuario.

Verificación de la identidad

1. En el panel izquierdo, seleccione el nodo **Verificación de la identidad** y, a continuación, haga clic en **Administrar preguntas** en el panel derecho.
2. En la pantalla **Autenticación con preguntas**, seleccione el idioma predeterminado, utilice la casilla de verificación para habilitar o inhabilitar el ocultamiento de las respuestas a las preguntas de seguridad, y haga clic en **Siguiente**.
3. En la pantalla **Preguntas de seguridad**, haga clic en **Agregar pregunta**, escriba una pregunta en el cuadro de texto, haga clic en **Aceptar** y, a continuación, haga clic en **Siguiente**.
4. En la pantalla **Cuestionario**, haga clic en **Agregar** y seleccione una pregunta. Puede reorganizar sus preguntas y grupos con los botones **Subir** y **Bajar**. Cuando haya terminado en esta página, haga clic en **Crear** y, a continuación, en **Aceptar**.

Para obtener más información sobre la administración de las preguntas de verificación de identidad, consulte Administración de las preguntas de verificación de identidad.

Administración de configuraciones de usuario

Las configuraciones de usuario permiten controlar el comportamiento y el aspecto de la interfaz, cuando los usuarios inician sesión en StoreFront. La creación de una o varias configuraciones es el paso final que se realiza antes de distribuir el software del Autoservicio de restablecimiento de contraseñas a los usuarios del entorno. Las configuraciones de usuario existentes pueden editarse en cualquier momento.

Una configuración de usuario es un conjunto único de parámetros que se aplica a los usuarios asociados a una jerarquía de Active Directory (una unidad organizativa [OU] 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 da respaldo a grupos de distribución y grupos de dominio local en modo mixto de Active Directory.

- Servidor de licencias
- Funciones de autoservicio (desbloqueo de cuenta y restablecimiento de contraseña)

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

- Almacén central
- Configuración del servicio

Para crear una configuración de usuario

1. Haga clic en**Inicio** > **Todos los programas** > **Citrix** > **Configuración del autoservicio de restablecimiento de contraseñas de Citrix**.
2. En el panel izquierdo, seleccione el nodo **Configuraciones de usuario**.
3. En el menú **Acciones**, haga clic en **Agregar configuración de usuario nueva**.

Para agregar usuarios, unidad organizativa (OU) o grupo

La página **Nombrar la configuración de usuario** del asistente de **Configuración de usuario** permite asociar la configuración de usuario a los usuarios.

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 **Modificar configuración de usuario** en el menú **Acciones**.

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

Seleccione la unidad organizativa, los usuarios o el grupo en la página **Nombrar la configuración de usuario** (desde el asistente para Agregar nueva configuración de usuario o Modificar configuración de usuario).

Nota: Se recomienda no incluir cuentas con privilegios (por ejemplo, Administradores locales o Administradores de dominio) en el grupo de usuarios para los que la cuenta de Autoservicio de restablecimiento de contraseñas puede restablecer contraseñas. Use un nuevo grupo, dedicado.

Para configurar el sistema de licencias

La página **Configurar las licencias** del asistente **Configuración de usuario** le permite configurar el servidor de licencias utilizado por el servicio de Autoservicio de restablecimiento de contraseñas.

Nota: Puede usar las funciones de Desbloquear y Restablecer solo si tiene XenApp o XenDesktop Platinum Edition.

Introduzca el nombre del servidor de licencias y el número de puerto en la página **Configurar las licencias** (desde el asistente para Agregar nueva configuración de usuario o Modificar configuración de usuario).

Para habilitar las funciones Desbloquear y Restablecer

El Autoservicio de restablecimiento de contraseñas permite a los usuarios restablecer sus contraseñas de Windows y desbloquear sus cuentas de dominio sin la intervención de ningún administrador. En la página **Habilitar el autoservicio de restablecimiento de contraseñas**, puede seleccionar la función que quiera habilitar.

Seleccione qué función quiere que usen los usuarios: **Desbloquear** o **Restablecer**, en la página **Habilitar el autoservicio de restablecimiento de contraseñas** (desde el asistente para Agregar nueva configuración de usuario o Modificar configuración de usuario).

Administración de las preguntas de verificación de identidad

La verificación de identidad de la consola de Configuración del Autoservicio de restablecimiento de contraseñas de Citrix le ofrece una ubicación central desde donde administrar todas las preguntas de seguridad asociadas con la verificación de identidad, el autoservicio de restablecimiento de contraseñas y el desbloqueo de cuentas. Puede añadir sus propias preguntas de seguridad a la lista de preguntas predeterminadas y crear grupos de preguntas.

- 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. Los usuarios deben responder a las nuevas preguntas de seguridad cuando abran las Tareas en Receiver.
- 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** > **Configuración del autoservicio de restablecimiento de contraseñas de Citrix**.
2. En el panel izquierdo, seleccione el nodo **Verificación de la identidad**.
3. En el menú **Acciones**, haga clic en **Administrar preguntas**.

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 ese idioma no está disponible, el Autoservicio de restablecimiento de contraseñas muestra las preguntas en el idioma predeterminado que se haya definido.

1. Haga clic en**Inicio** > **Todos los programas** > **Citrix** > **Configuración del Autoservicio de restablecimiento de contraseñas de Citrix**.
2. En el panel izquierdo, seleccione el nodo **Verificación de la identidad**.
3. En el menú **Acciones**, haga clic en **Administrar preguntas**.
4. En la lista desplegable **Idioma predeterminado** en la página **Autenticación con preguntas**, seleccione el idioma predeterminado.

Para habilitar el ocultamiento de respuestas

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. Durante el proceso de registro de las respuestas, dichos usuarios deberán introducir sus respuestas dos veces para evitar errores de tecleado y ortografía. Los usuarios deberán escribir sus respuestas solo una vez durante la validación de la identidad porque se les pedirá que vuelvan a intentarlo si hay un error.

Seleccione **Ocultar las respuestas a las preguntas de seguridad** en la página **Autenticación con 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. La inscripción en Receiver presenta al usuario el cuestionario en el idioma correspondiente a la configuración de idioma de su perfil de usuario. Si el idioma no está disponible, al Autoservicio de restablecimiento de contraseñas 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 para 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. En la lista desplegable **Idioma** de la página **Preguntas de seguridad**, seleccione un idioma y haga clic en **Agregar pregunta**. Aparecerá el cuadro de diálogo Pregunta de seguridad.
2. Cree la nueva pregunta en el cuadro de diálogo **Pregunta de seguridad**.

Importante: El texto traducido de las preguntas ya existentes debe agregarse mediante el botón **Modificar**. Si selecciona **Agregar pregunta**, se creará una nueva pregunta que no estará asociada a la original.

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. Los usuarios deben responder a las nuevas preguntas de seguridad cuando abran las Tareas en Receiver. La modificación de una pregunta no obliga al usuario a reinscribirse.

Importante: Si va a modificar una pregunta existente, tenga cuidado de no cambiar el significado de la pregunta original. 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 un idioma en la lista desplegable **Idioma** en la página **Preguntas de seguridad**.
2. Seleccione la pregunta y haga clic en **Modificar**.
3. Edite la pregunta en el cuadro de diálogo **Pregunta 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. Haga clic en **Agregar grupo** en la página **Preguntas de seguridad**.
2. 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

Seleccione el grupo de preguntas de seguridad que quiera modificar y haga clic en **Modificar** en la página **Preguntas de seguridad**. 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 a cuántas preguntas de este grupo debe responder el usuario.

Para agregar o quitar el cuestionario existente

Agregue o quite preguntas de seguridad y grupos de preguntas del cuestionario. Mueva las preguntas arriba y abajo en el orden en que se presentan ante el usuario. Si el cuestionario ha cambiado, debe notificarse al usuario para que realice una reinscripción después de iniciar la sesión en StoreFront.

1. Haga clic en **Agregar** en la página **Cuestionario** para agregar preguntas o grupos al cuestionario.
2. Haga clic en **Quitar** para quitar una pregunta del cuestionario.
3. Haga clic en **Subir** o **Bajar** para organizar cómo se presentan las preguntas al usuario.

Administración de la verificación de identidad

Con el Autoservicio de restablecimiento de contraseñas se puede:

- Importar o exportar las preguntas de seguridad.
- Revocar el registro de preguntas de seguridad para un usuario.

Para importar o exportar las preguntas de seguridad

Puede importar o exportar los datos de preguntas de seguridad y grupos.

1. Haga clic en**Inicio** > **Todos los programas** > **Citrix** > **Configuración del autoservicio de restablecimiento de contraseñas de Citrix**.
2. En el panel izquierdo, seleccione el nodo **Verificación de la identidad**.
3. En el menú **Acciones**, seleccione una de las siguientes:

Importar preguntas de seguridad
Especifique la ubicación del archivo desde donde quiere importar los datos de preguntas de seguridad y grupos.

Exportar preguntas de seguridad
Especifique la ubicación del archivo adonde quiere exportar los datos de preguntas de seguridad y grupos.

Seguridad

Sep 19, 2016

Este artículo describe los procedimientos necesarios para asegurarse de que los componentes del Autoservicio de restablecimiento de contraseñas se implementan y se configuran de forma segura.

- Configurar los parámetros de Internet Information Services (IIS)
- Crear una cuenta de usuario de dominio con permiso para el restablecimiento de contraseñas y desbloqueo de cuentas de usuario
- Configurar los parámetros de firewall

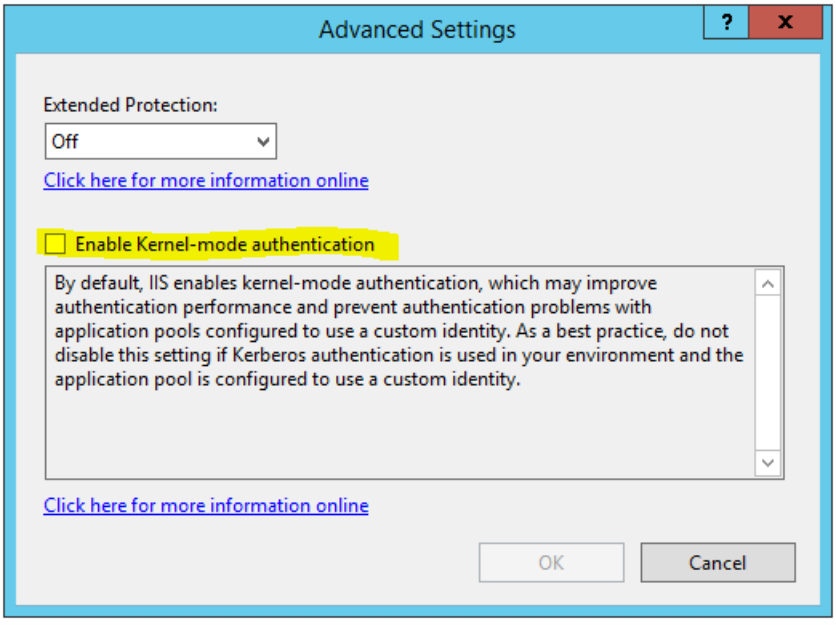
Configurar los parámetros de Internet Information Services (IIS)

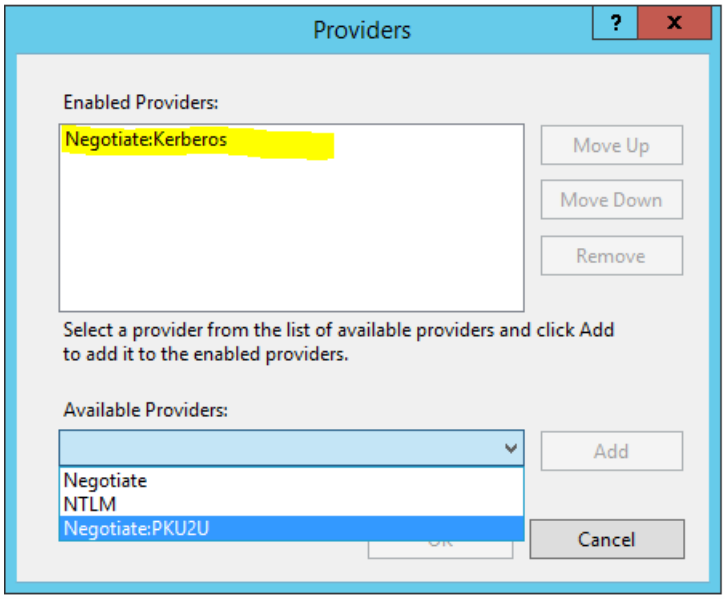
Utilice el siguiente procedimiento para asegurarse de que el sitio IIS MPMService está configurado de forma segura.

1. Después de instalar el servicio de Autoservicio de restablecimiento de contraseñas, haga clic en el sitio Web **MPMService** en el Administrador de IIS. En **Autenticación**, seleccione **Autenticación de Windows** y, a continuación, **Configuración avanzada** y **Proveedores**.

    a. El descifrado del tiquet de servicio de Kerberos falla si está habilitada la autenticación en modo kernel. Para configurar Kerberos para el sitio, deje sin marcar la casilla Habilitar la autenticación de modo kernel en la pantalla Configuración avanzada, para dar respaldo a Kerberos.

    b. En la pantalla Proveedores, agregue la opción Negociar: Kerberos en la sección Proveedores disponibles. Quite los demás proveedores de la lista Proveedores habilitados.





2. En el panel de la izquierda del Administrador de IIS, haga clic en el sitio Web **MPMService**. En **Configuración de SSL**, habilite **Requerir SSL**.

Crear una cuenta de autoservicio

Si utiliza las funciones de Restablecimiento de contraseñas o Desbloqueo de cuentas del Autoservicio de restablecimiento de contraseñas, especifique una cuenta de autoservicio durante la configuración del servicio que el módulo utilizará para ejecutar dichas funciones. Asegúrese de que la cuenta tiene privilegios suficientes para estas tareas, pero le recomendamos que no use una cuenta del grupo de Administradores de dominio en implementaciones de producción. Los privilegios de cuenta recomendados son:

- Miembro del dominio
- Permiso de restablecimiento de contraseñas y desbloqueo de cuentas para los usuarios del dominio en cuestión

En **Usuarios y equipos de Active Directory**, cree el grupo o la cuenta de usuario que tenga los permisos para restablecer contraseñas de usuario y desbloquear cuentas de usuario.

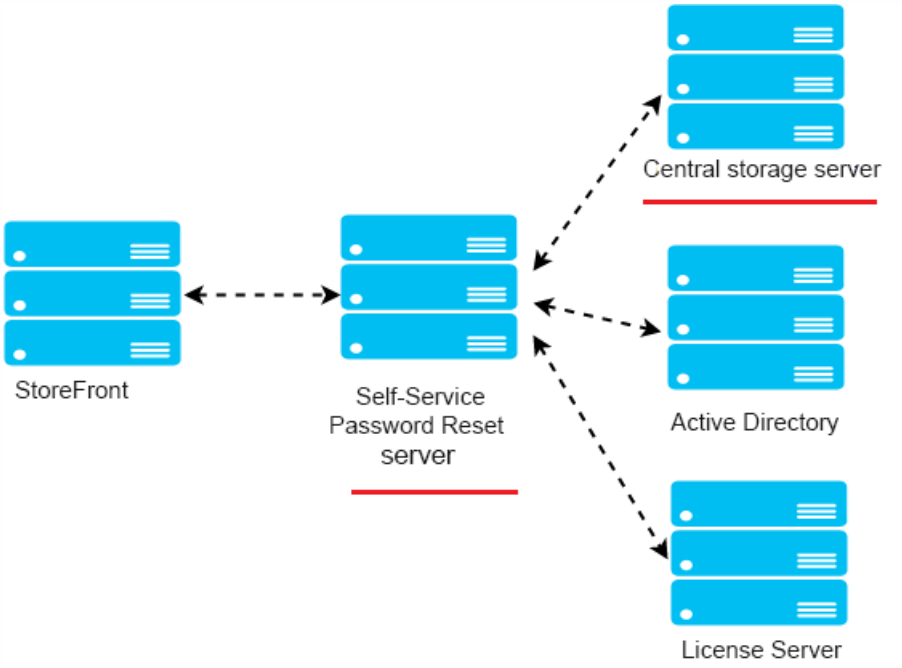
1. En **Usuarios y equipos de Active Directory**, haga clic con el botón secundario en el dominio y, a continuación, haga clic en **Delegar control** en el menú contextual.
2. Aparecerá el **Asistente para delegación de control**. En el cuadro de diálogo de **Bienvenida**, haga clic en **Siguiente**.
3. En el cuadro de diálogo **Usuarios y grupos**, haga clic en **Agregar**. En la lista, seleccione el grupo al que quiere dar permisos para desbloquear cuentas y luego haga clic en **Aceptar**. En el cuadro de diálogo **Usuarios y grupos**, haga clic en **Siguiente**.
4. En el cuadro de diálogo **Tareas que se delegarán**, haga clic en **Crear una tarea personalizada para delegar** y, a continuación, haga clic en **Siguiente**.
5. En el cuadro de diálogo **Tipo de objeto de Active Directory** , haga clic en Sólo los siguientes objetos en la carpeta > Objetos de usuario y, a continuación, haga clic en **Siguiente**.
6. En el cuadro de diálogo **Permisos**, marque las casillas **General** y **Específico de la propiedad**. En la lista **Permisos**, marque las casillas **Read lockoutTime** , **Write lockoutTime**, **Reset Password,Change Password, Read userAccountControl, Write userAccountControl, Read pwdLastSet, and Write pwdLastSet** y después, haga clic en **Siguiente**.
7. En el cuadro de diálogo **Finalización del Asistente para delegación de control**, haga clic en **Finalizar**.

Configurar los parámetros de firewall

El servidor de Autoservicio de restablecimiento de contraseñas y el servidor de almacén central son componentes que gestionan contraseñas de usuario, por lo que le recomendamos que implemente estos componentes dentro de una red de confianza y que solo sean accesibles para componentes muy concretos y también de confianza. Esta sección describe los pasos necesarios para asegurarse de que el Firewall de Windows esté configurado correctamente para estos servidores. También le recomendamos que configure la infraestructura de red existente de forma que estos servidores estén aislados del tráfico de red que no sea de confianza.

Después de completar estas configuraciones en la implementación, solo se puede acceder a los servidores de almacén central de Autoservicio de restablecimiento de contraseñas desde servidores de Autoservicio de restablecimiento de contraseñas que usen SMB (Server Message Block) y solo se puede acceder a los servidores de Autoservicio de restablecimiento de contraseñas desde servidores StoreFront con conexiones HTTPS.

Implementación de un recurso compartido de archivos remoto para Windows 2012 R2



Entorno

- Implemente los componentes del Autoservicio de restablecimiento de contraseñas en servidores dedicados. No los implemente en el mismo servidor donde ya existan componentes de StoreFront o de Delivery Controller; de hacerlo, la configuración del firewall que se describe abajo podría bloquear el tráfico de StoreFront o del Controller.
- No hay ningún proxy HTTP/HTTPS no transparente entre StoreFront y el servidor de Autoservicio de restablecimiento de contraseñas.

  Si existe algún servidor proxy no transparente entre StoreFront y el servidor de Autoservicio de restablecimiento de contraseñas, configure el servidor de Autoservicio de restablecimiento de contraseñas para que solo se pueda acceder a él desde el servidor proxy en las reglas del firewall.

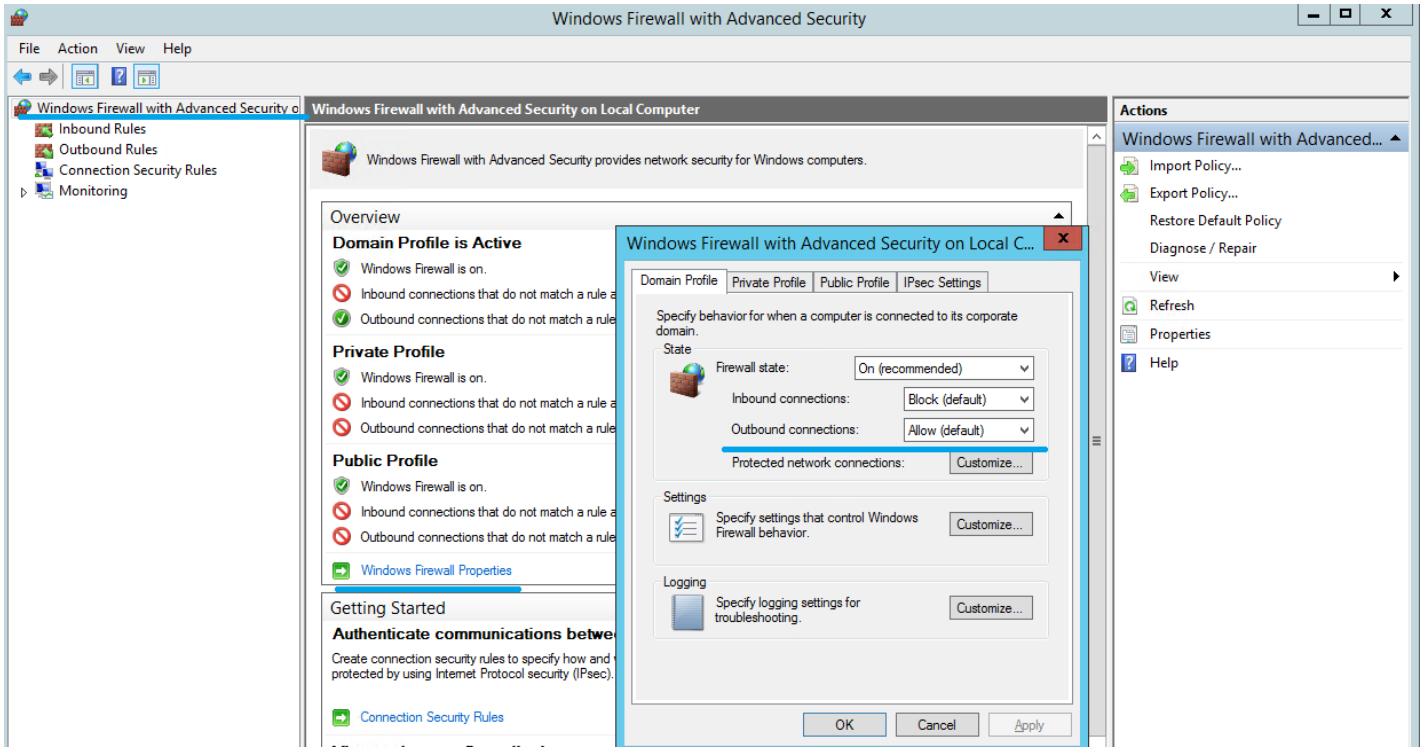
- Las configuraciones de estos procedimientos se basan en las reglas predeterminadas de firewall de Windows.

Configurar el firewall para el almacén central del Autoservicio de restablecimiento de contraseñas

Después de completar esta configuración, solo se puede acceder al servicio SMB suministrado por el almacén central de Autoservicio de restablecimiento de contraseñas desde los servidores de Autoservicio de restablecimiento de contraseñas en tráfico de entrada, y el servidor del almacén central de Autoservicio de restablecimiento de contraseñas solo puede acceder al servicio ubicado en la red corporativa en tráfico de salida.

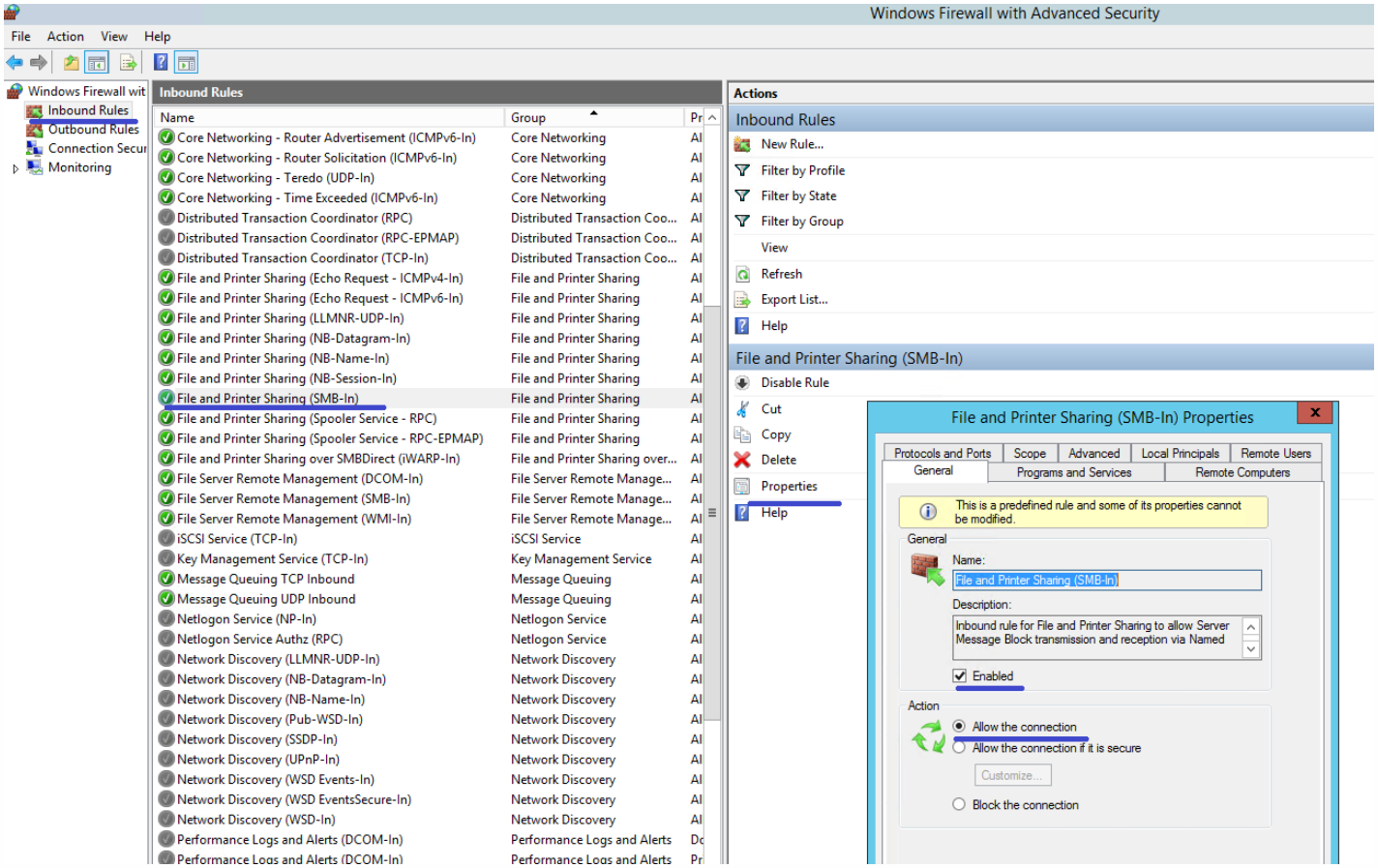
1. Abra el Administrador del servidor, y en el menú **Herramientas** en la barra de navegación superior, seleccione **Firewall de Windows con seguridad avanzada**.

2. En **Firewall de Windows con seguridad avanzada**, seleccione **Propiedades de Firewall de Windows** en el panel central. Existen tres perfiles de firewall: Dominio, Privado y Público. Seleccione la ficha **Perfil de dominio**. Asegúrese de que el **Estado del firewall** sea **Activo**, que el valor del parámetro **Conexiones entrantes** sea **Bloquear** y que el valor del parámetro **Conexiones salientes** sea **Permitir**.



3. Seleccione las fichas **Perfil privado** y **Perfil público** y asegúrese de que el **Estado del firewall** sea **Activo** y que tanto las **Conexiones entrantes** como las **Conexiones salientes** estén configuradas con la opción **Bloquear**. Aplique y guarde los cambios.

4. En la lista **Reglas de entrada**, seleccione **Compartir archivos e impresoras (SMB de entrada)** y asegúrese de que esta regla está **Habilitada** y que la **Acción** configurada es **Permitir la conexión**.



5. En las **Propiedades de Compartir archivos e impresoras (SMB de entrada)**, abra la ficha **Ámbito**, elija **Estas direcciones IP** y agregue a la lista todas las direcciones IP de servidores de Autoservicio de restablecimiento de contraseñas. Por ejemplo, el servidor A de Autoservicio de restablecimiento de contraseñas (192.168.1.10) y el servidor B de Autoservicio de restablecimiento de contraseñas (192.168.1.11).

6. En **Propiedades de Compartir archivos e impresoras (SMB de entrada)**, vaya a la ficha **Opciones avanzadas**, seleccione los perfiles **Dominio**, **Privado** y **Público**, y guarde los cambios de esta regla.

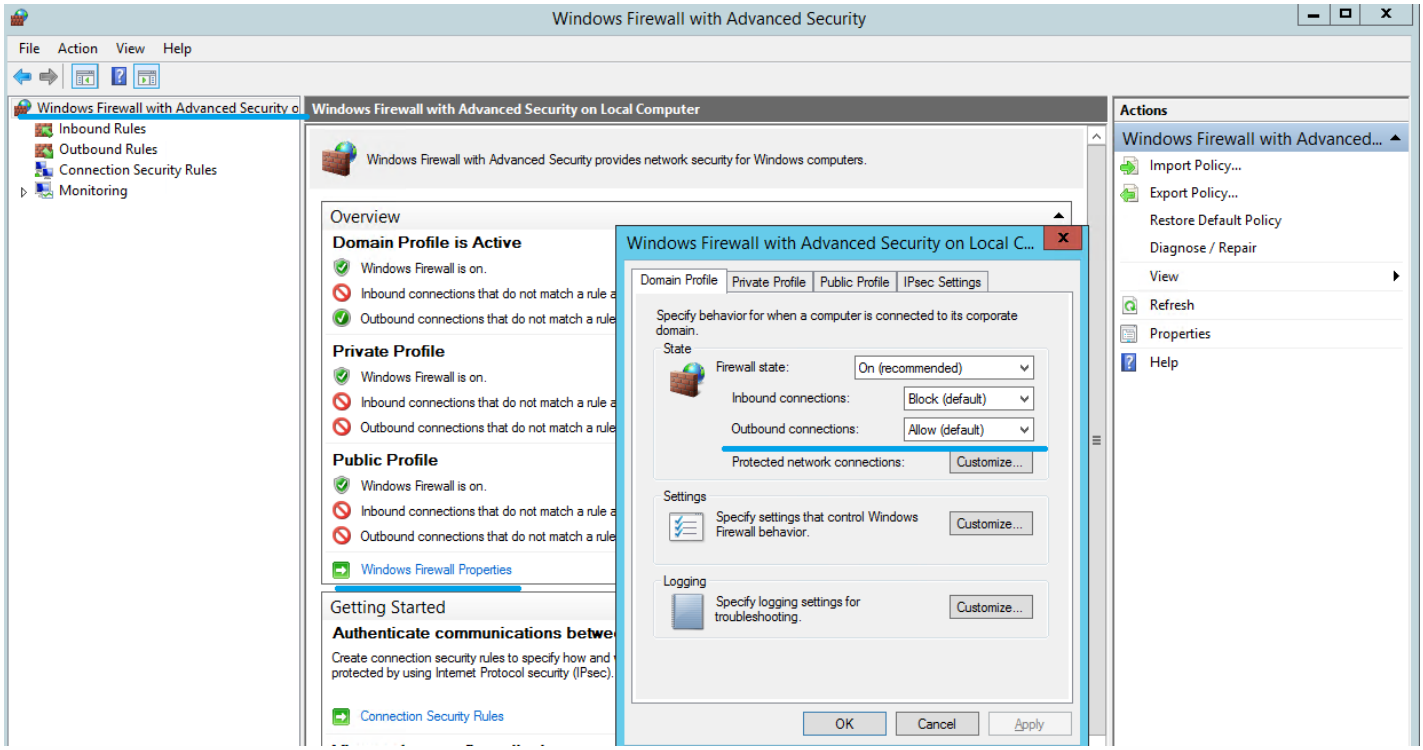
7. Repita este procedimiento en las **Reglas de entrada** de **Administración remota de servidores de archivos (SMB de entrada)** y de **Compartir archivos e impresoras (sesión NB de entrada)**.

Configurar el firewall para el servidor del Autoservicio de restablecimiento de contraseñas

Después de completar esta configuración, solo se puede acceder al servicio Web suministrado por los servidores de Autoservicio de restablecimiento de contraseñas desde los servidores StoreFront que usen HTTPS, y los servidores de Autoservicio de restablecimiento de contraseñas solo pueden acceder al servicio ubicado en la red corporativa.

1. Abra el Administrador del servidor, y en el menú **Herramientas** en la barra de navegación superior, seleccione **Firewall de Windows con seguridad avanzada**.

2. En **Firewall de Windows con seguridad avanzada**, seleccione **Propiedades de Firewall de Windows** en el panel central. Existen tres perfiles de firewall: Dominio, Privado y Público. Seleccione la ficha **Perfil de dominio**. Asegúrese de que el **Estado del firewall** sea **Activo**, que el valor del parámetro **Conexiones entrantes** sea **Bloquear** y que el valor del parámetro **Conexiones salientes** sea **Permitir**.

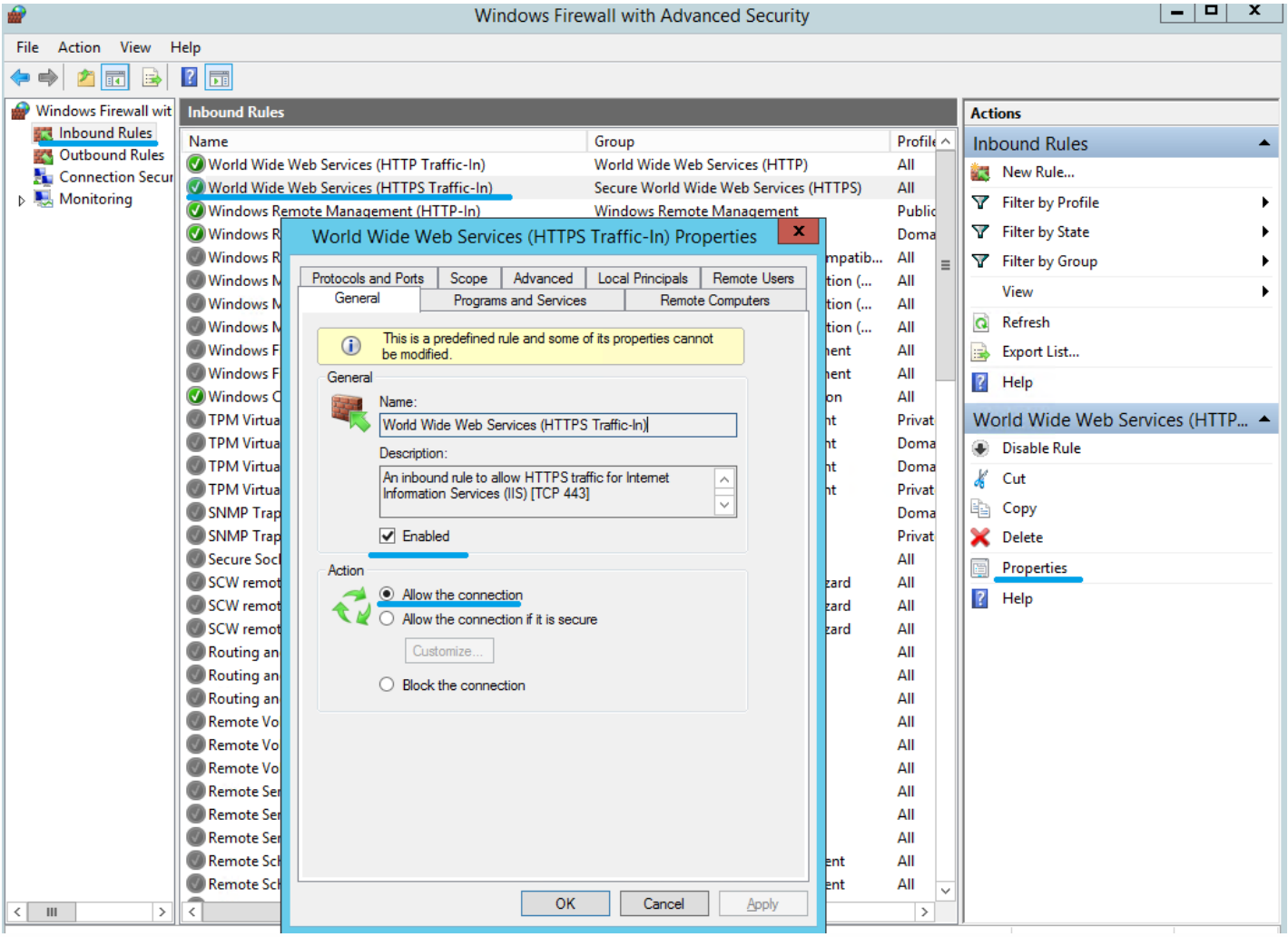


3. Seleccione las fichas **Perfil privado** y **Perfil público** y asegúrese de que el **Estado del firewall** sea **Activo** y que tanto las **Conexiones entrantes** como las **Conexiones salientes** estén configuradas con la opción **Bloquear**. Aplique y guarde los cambios.

4. En la lista **Reglas de entrada**, seleccione **Servicios de World Wide Web (Entrada de tráfico HTTP)** y asegúrese de que esta regla está **Habilitada** y que la **Acción** configurada es **Bloquear la conexión**.

5. En **Propiedades de Servicios de World Wide Web (Entrada de tráfico HTTP)**, vaya a la ficha **Opciones avanzadas**, seleccione los perfiles **Dominio**, **Privado** y **Público**, y guarde los cambios de esta regla.

6. En la lista **Reglas de entrada**, seleccione **Servicios de World Wide Web (Entrada de tráfico HTTPS)** y asegúrese de que esta regla está **Habilitada** y que la **Acción** configurada es **Permitir la conexión**.



7. En las **Propiedades de Servicios de World Wide Web (Entrada de tráfico HTTPS)**, abra la ficha **Ámbito**, elija **Estas direcciones IP** y agregue a la lista todas las direcciones IP de servidores StoreFront. Por ejemplo, StoreFront A (192.168.1.50) y StoreFront B (192.158.1.51).

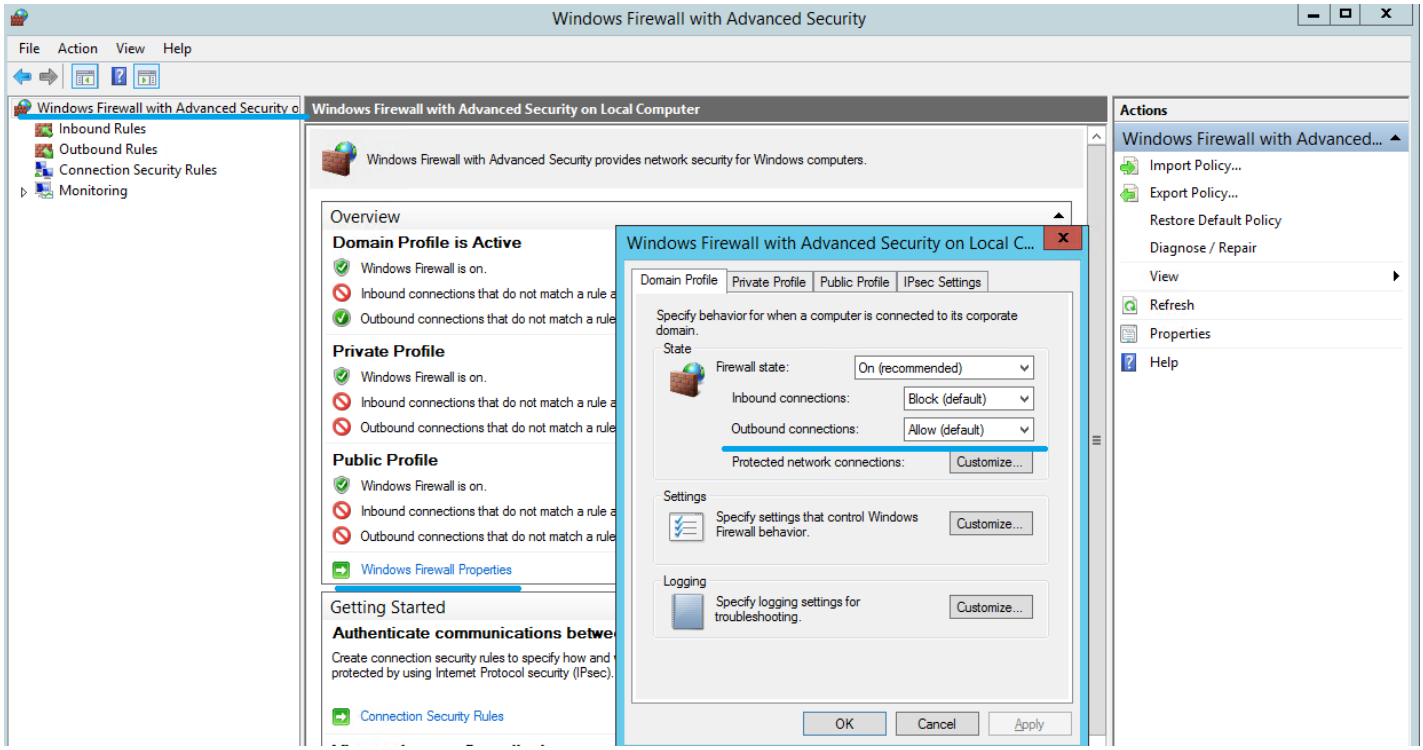
8. En **Propiedades de Servicios de World Wide Web (Entrada de tráfico HTTPS)**, vaya a la ficha **Opciones avanzadas**, seleccione los perfiles **Dominio**, Privado y **Público**, y guarde los cambios de esta regla.

Implementación de un recurso compartido de archivos local para Windows 2008 R2

Después de completar la configuración, cualquier acceso SMB desde un cliente remoto será bloqueado. Solo se podrá acceder al recurso compartido de archivos SMB desde el servicio local y solo se podrá acceder al servicio del Autoservicio de restablecimiento de contraseñas desde los servidores StoreFront que usen una conexión HTTPS.

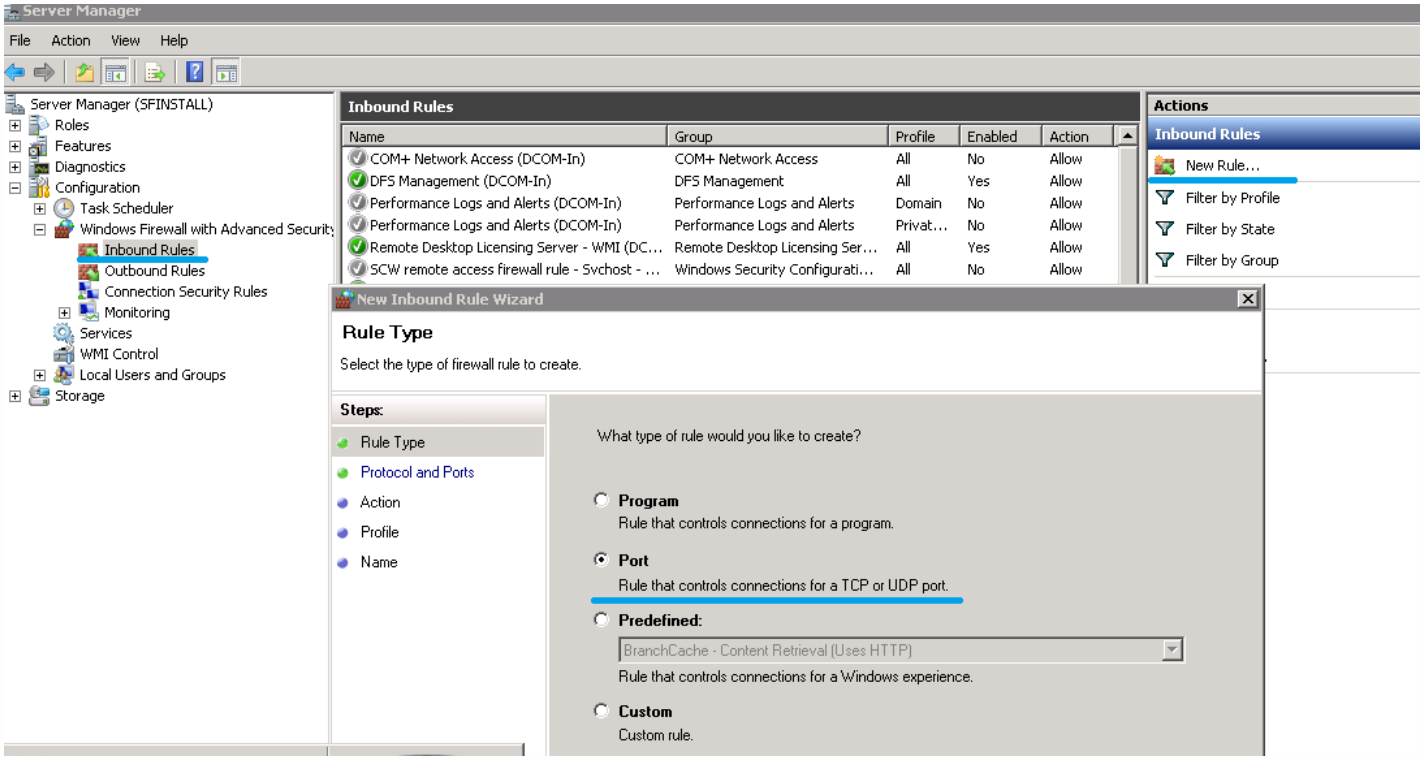
1. Abra el Administrador del servidor, y en el menú **Herramientas** en la barra de navegación superior, seleccione **Firewall de Windows con seguridad avanzada**.

2. En **Firewall de Windows con seguridad avanzada**, seleccione **Propiedades de Firewall de Windows** en el panel central. Existen tres perfiles de firewall: Dominio, Privado y Público. Seleccione la ficha **Perfil de dominio**. Asegúrese de que el **Estado del firewall** sea **Activo**, que el valor del parámetro **Conexiones entrantes** sea **Bloquear** y que el valor del parámetro **Conexiones salientes** sea **Permitir**.



3. Seleccione las fichas **Perfil privado** y **Perfil público** y asegúrese de que el **Estado del firewall** sea **Activo** y que tanto las **Conexiones entrantes** como las **Conexiones salientes** estén configuradas con la opción **Bloquear**. Aplique y guarde los cambios.

4. En la lista **Reglas de entrada**, seleccione **Nuevas reglas** para crear una nueva regla de entrada. En el **Asistente para nueva regla de entrada**, seleccione **Tipo de regla**, elija **Puerto** como el tipo de la nueva regla y, a continuación, haga clic en **Siguiente**.



5. En el **Asistente para nueva regla de entrada**, seleccione **Protocolo y puertos**, elija **TCP**, elija **Puertos locales**

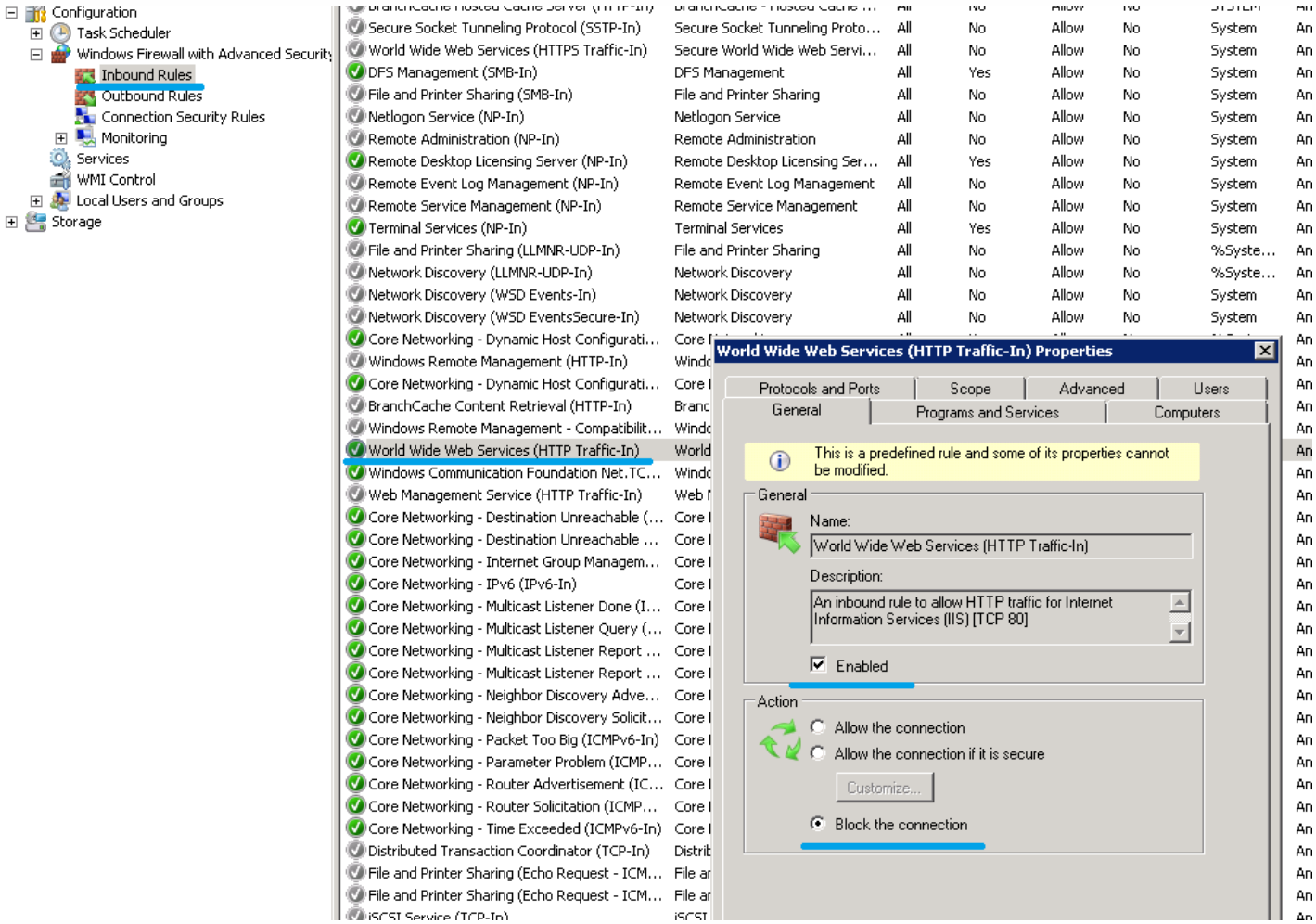
específicos, introduzca **445** en el cuadro de texto, y haga clic en **Siguiente**.

6. En el **Asistente para nueva regla de entrada**, seleccione **Acción**, elija **Bloquear la conexión** y haga clic en **Siguiente**.

7. En el **Asistente para nueva regla de entrada**, seleccione **Perfil**, elija **Dominio**, **Privado** y **Público** y haga clic en **Siguiente**.

8. En el **Asistente para nueva regla de entrada**, seleccione **Nombre**, introduzca un nombre y una descripción y haga clic en **Siguiente**.

9. En la lista **Reglas de entrada**, seleccione **Servicios de World Wide Web (Entrada de tráfico HTTP)** y asegúrese de que esta regla está **Habilitada** y que la **Acción** configurada es **Bloquear la conexión**.



10. En **Propiedades de Servicios de World Wide Web (Entrada de tráfico HTTP)**, vaya a la ficha **Opciones avanzadas**, seleccione los perfiles **Dominio**, **Privado** y **Público**, y guarde los cambios de esta regla.

11. En la lista **Reglas de entrada**, seleccione **Servicios de World Wide Web (Entrada de tráfico HTTPS)** y asegúrese de que esta regla está **Habilitada** y que la **Acción** configurada es **Permitir la conexión**.

12. En **Propiedades de Servicios de World Wide Web (Entrada de tráfico HTTPS)**, vaya a la ficha **Ámbito**. En la sección **Direcciones IP remotas**, elija **Estas direcciones IP** y agregue a la lista todas las direcciones IP de servidores StoreFront. Por ejemplo, StoreFront A (192.168.1.13) y StoreFront B (192.158.1.14).

13. En **Propiedades de Servicios de World Wide Web (Entrada de tráfico HTTP)**, vaya a la ficha **Opciones avanzadas**, seleccione los perfiles **Dominio**, **Privado** y **Público**, y guarde los cambios de esta regla.

Migración de datos desde el almacén central de Single Sign-on

Sep 19, 2016

El almacén central es un repositorio 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 administrativos incluyen directivas de contraseña, definiciones de aplicación, preguntas de seguridad y otros datos de mayor alcance.

No se puede migrar todos los datos desde el almacén central de Single Sign-on al almacén central del Autoservicio de restablecimiento de contraseñas. Esta tabla muestra los datos que se puede y no se puede migrar.

No se puede migrar	Se puede migrar
Directivas de contraseña: No respaldado	Carpetas de personas (People) que contienen datos de inscripción
Plantillas de aplicación: No respaldado	Cuestionarios utilizados por los clientes
Definiciones de aplicación: No respaldado	
Configuraciones de usuario: Creadas en la consola del Autoservicio de restablecimiento de contraseñas	
Grupos de aplicaciones: No respaldado	
Datos del servicio Single Sign-on: Creados en la consola del Autoservicio de restablecimiento de contraseñas	

Important

- El Autoservicio de restablecimiento de contraseñas no admite el uso de Active Directory como almacén central, solo admite recursos compartidos de red.
- El Autoservicio de restablecimiento de contraseñas solo respalda los datos de Single Sign-on 4.8 y 5.0.

Para migrar datos desde el almacén central de Single Sign-on

Antes de migrar los datos, familiarícese con la instalación y configuración del Autoservicio de restablecimiento de contraseñas. Para obtener más información, consulte Instalación y configuración.

1. Cree un nuevo almacén central.
2. Instale el servicio y la consola del Autoservicio de restablecimiento de contraseñas.
3. En la consola, especifique la ubicación del nuevo almacén central.
4. Cree una nueva configuración de usuario e incluya a los usuarios que tienen Autoservicio de restablecimiento de

contraseñas en Single Sign-on.

5. Copie los datos de inscripción y las preguntas de seguridad de Single Sign-on en el nuevo almacén central.

   Nota: Asegúrese de que la cuenta de proxy de datos tiene permiso de control total para todos los archivos copiados.

   Solo necesita dos carpetas/archivos.

   Ejemplos

   Copiar todos los datos de inscripción de los usuarios:

   \\SSO-SERVER\citrixsync$\People

   a

   \\SSPR-SVC\citrixsync$\People

   Use este comando:
   Robocopy \\SSO-SERVER\citrixsync$\People\ \\SSPR-SVC\citrixsync$\People /e /xd QBA /Log+:copylog.txt /tee

   Copiar las preguntas de seguridad utilizadas por los clientes:

   \\SSOSERVERcitrixsync$\CentralStoreRoot\AdminConsole\QuestionBasedAuthentication2\ QuestionBasedAuthentication2

   a

   \\SSPRSVCcitrixsync$\CentralStoreRoot\AdminConsole\QuestionBasedAuthentication2\

   Use este comando:
   Robocopy \\SSO-SERVER\citrixsync$\CentralStoreRoot\AdminConsole\QuestionBasedAuthentication2\ \\SSPR-SVC\citrixsync$\CentralStoreRoot\AdminConsole\QuestionBasedAuthentication2 /e /Log+:copylog.txt /tee

Ahora, todos los usuarios pueden desbloquear y restablecer contraseñas usando sus preguntas y respuestas de inscripción de Single Sign-on.

Configuración de StoreFront para permitir que los usuarios registren sus respuestas a las preguntas de seguridad

Nov 02, 2016

Configure StoreFront para permitir que los usuarios inscriban sus respuestas a las preguntas de seguridad. Cuando se hayan inscrito, los usuarios podrán restablecer contraseñas de dominio y desbloquear cuentas de dominio. Para obtener más información, consulte la documentación de StoreFront.

1. Configure los servicios Internet Information Services (IIS) de StoreFront con HTTPS.
2. Cree una nueva implementación de StoreFront.
3. En el panel de la derecha de la consola de administración de StoreFront, seleccione **Administrar métodos de autenticación > Nombre de usuario y contraseña**. Elija la opción **Administrar opciones de contraseña** en el menú desplegable.
4. Elija cuándo quiere dejar que los usuarios cambien las contraseñas y haga clic en **Aceptar**.
5. En el menú desplegable **Nombre de usuario y contraseña**, elija **Configurar autoservicio de cuentas**, seleccione **Citrix SSPR**, y haga clic en **Configurar**.
6. Especifique si se permite a los usuarios restablecer sus contraseñas y desbloquear sus cuentas con el Autoservicio de restablecimiento de contraseñas, agregue la dirección URL del servicio y haga clic en **Aceptar**.

Nota: Debe configurar el sitio para usar la experiencia unificada.

La próxima vez que el usuario inicie sesión en Citrix Receiver o Citrix Receiver para Web, la inscripción de seguridad estará disponible. Después de hacer clic en **Iniciar**, el usuario verá preguntas a las que tiene que responder.