StoreFront 2311

Contents

Descripción general

February 26, 2024

StoreFront es un intuitivo almacén de aplicaciones de empresa que combina aplicaciones y escritorios de los sitios de Citrix Virtual Apps and Desktops y Citrix DaaS en un solo almacén.

En StoreFront, puede configurar uno o varios almacenes. Cada almacén tiene su propia configuración, que incluye:

- La lista de feeds de recursos que StoreFront consulta para enumerar las aplicaciones y escritorios disponibles para el usuario.
- La apariencia del sitio web utilizado para acceder al almacén.
- Qué métodos de autenticación utilizan los usuarios para iniciar sesión.
- Acceso externo a través de un dispositivo NetScaler Gateway.

Los usuarios pueden usar la aplicación Citrix Workspace instalada localmente o la aplicación Citrix Workspace para HTML5 en un explorador web para acceder a los almacenes de StoreFront. Para obtener más información, consulte Opciones de acceso de usuarios.

Para empezar, planifique la implementación de StoreFront, consulte los requisitos del sistema e instale StoreFront.

Novedades

Consulte Novedades.

Versiones anteriores

La documentación sobre otras versiones disponibles actualmente se encuentra aquí.

Para ver los pasos para actualizar desde una versión anterior, consulte Actualizar.

Respaldo al ciclo de vida útil

La estrategia de ciclos de vida del producto para las versiones Current Release (CR) y las versiones Long Term Service (LTSR) de StoreFront se describe en Hitos del ciclo de vida. En CTX200356 se ofrece información adicional sobre el ciclo de vida de StoreFront.

Novedades

April 17, 2024

2311

Citrix Secure Private Access en StoreFront

Ahora puede conectarse al servidor local de Citrix Secure Private Access mediante los nuevos comandos de PowerShell o los controles de interfaz de usuario de administración de StoreFront. Permite a los usuarios acceder de forma segura a aplicaciones web y SaaS a través de StoreFront.
Para obtener más información, consulte Administrar los recursos disponibles en los almacenes.

Inicio ininterrumpido de VDA en caso de que el servidor de FAS no esté disponible

Ahora puede configurar StoreFront para que el inicio de un VDA se realice correctamente aunque el servidor de FAS no esté disponible. En estos casos, los usuarios finales pueden iniciar sesión con su nombre de usuario y contraseña. Anteriormente, el inicio en un VDA fallaba si no se podía acceder a los servidores de FAS.
Esta función está inhabilitada de forma predeterminada y se puede habilitar mediante el siguiente comando de PowerShell.

`Set-STFStoreLaunchOptions` con parámetro `FederatedAuthenticationServiceFailover`

Puede usar el mismo comando para inhabilitar esta función, si fuera necesario.
Para obtener más información, consulte FAS.

Registros de las acciones de usuario mejorado

Anteriormente, de forma predeterminada solo se registraban los errores. El nivel de registro predeterminado ahora se ha cambiado para incluir advertencias e información de seguimiento. Además, se han mejorado los mensajes de registro. Esto garantiza que, de forma predeterminada, ahora se registren todos los eventos que forman parte de las acciones principales de los usuarios. El tamaño predeterminado del archivo de registro se aumentó a 1 GB (5*200 MB) para cada servicio. Por lo general, esto requerirá 1 GB (para el servicio de roaming) y 3 GB por almacén (ya que cada servicio de almacén suele tener un servicio de autenticación y un servicio Receiver para Web correspondientes). Asegúrese de que dispone de suficiente espacio en disco. Para obtener más información, consulte Registro de diagnósticos.

Extensiones web de Citrix Workspace: disponibilidad general

Las extensiones web de Citrix Workspace ya están disponibles de forma general para su uso con StoreFront. Estas extensiones web le ayudan a iniciar recursos en una aplicación Citrix Workspace instalada localmente sin tener que abrir Workspace Launcher o descargar un archivo `.ica`, lo que hace que su experiencia sea más segura y fiable. Para obtener más información, consulte Extensiones web de Citrix.

Con la versión 2312, el uso de las extensiones web de Citrix Workspace está habilitado de forma predeterminada para cada nueva instalación de StoreFront. No obstante, los usuarios finales todavía tienen que descargar las extensiones para usar esta función.

Los usuarios existentes pueden habilitar esta función mediante el siguiente comando:

```
Add-STFFeatureState -Name "Citrix.StoreFront.EnableBrowserExtension "
-IsEnabled $True
```

> **Nota:**
>
> La extensión web de Citrix Workspace no se habilita automáticamente durante la actualización de una versión de StoreFront. Si esta función estaba desactivada antes de la actualización, permanecerá en el mismo estado después de la actualización de la versión.

Nueva interfaz de usuario para almacenes locales (Technical Preview)

La nueva interfaz de usuario ya está disponible para los almacenes locales. Esta interfaz de usuario, que anteriormente solo estaba disponible para los almacenes en la nube, garantiza una apariencia uniforme para todos los almacenes locales y en la nube.

La nueva interfaz de usuario incluye las siguientes mejoras clave:

- **Interfaz de usuario fácil de usar**: reduce la complejidad visual y proporciona un fácil acceso a las funciones esenciales. Para obtener más información, consulte Mejoras visuales y de diseño del espacio de trabajo.
- **Administrador de actividades**: facilita las acciones rápidas en aplicaciones y escritorios virtuales activos para ahorrar recursos y optimizar el rendimiento. Para obtener más información, consulte Administrador de actividades.
- **Categorización mejorada de las aplicaciones**: estructura de carpetas de varios niveles que se adapta al tamaño de la pantalla del usuario final. Para obtener más información, consulte la ayuda sobre categorización de aplicaciones.
- **Capacidades de búsqueda mejoradas**: las nuevas capacidades de búsqueda proporcionan mejores resultados y con mayor rapidez. Para obtener más información, consulte Opciones de búsqueda.

Para obtener información detallada sobre esta Preview, consulte Nueva interfaz de usuario (Technical Preview).

> **Nota:**
>
> Puede enviar comentarios sobre esta función a través del formulario de Podio.

Aplicación Citrix Workspace para HTML5

Esta versión incluye la aplicación Citrix Workspace para HTML5 2310.

Problemas resueltos

- Es posible que la aplicación Citrix Workspace para Mac se bloquee tras despertarse del modo de suspensión al conectarse a un almacén de StoreFront. [CVADHELP-23217]
- Una condición de carrera puede provocar que Citrix Subscriptions Store Service se cierre inesperadamente en el servidor de StoreFront con mensajes de advertencia. [CVADHELP-23326]

Problemas conocidos

- Los nombres de usuario con caracteres especiales podrían mostrarse alterados en el menú desplegable **Parámetros**. [WSP-22210]
- El parámetro de PowerShell `-override` es necesario para realizar cualquier cambio en los parámetros de TraceLevel. [WSP-22214]

2308.1

Problemas resueltos

- Esta versión soluciona una vulnerabilidad de seguridad en un componente subyacente. Para obtener más información, consulte CTX583759. [CVADHELP-23724]

2308

App Protection para inicios híbridos

App Protection proporciona un nivel de seguridad adicional al bloquear los programas de registro de tecleo y las capturas de pantalla. Antes, esta funcionalidad solo estaba disponible al acceder a un almacén a través de las aplicaciones de Citrix Workspace para Windows, Mac y Linux. Al ver un almacén a través de un explorador web, no se mostraban las aplicaciones protegidas. Con esta versión, ahora

es posible configurar el sitio web de un almacén para que muestre las aplicaciones que requieren App Protection cuando se ven a través de un explorador, siempre que StoreFront haya detectado que el usuario tiene instalada una versión suficientemente reciente de la aplicación Citrix Workspace para Windows, Mac o Linux como para iniciar la aplicación.

Para obtener más información, consulte App Protection.

Habilitación de forma predeterminada de Comprobación de estado avanzada

A partir de esta versión, la función de comprobación de estado avanzada está habilitada de forma predeterminada para nuevos almacenes. Anteriormente, tenía que habilitarse manualmente.

Cuando se usa con Citrix DaaS, la comprobación de estado avanzada permite a StoreFront detectar los conectores presentes en las ubicaciones de recursos. En caso de interrupción, cuando un usuario inicia un recurso, StoreFront elige un conector adecuado para iniciar el recurso mediante la caché de host local.

Problemas resueltos

Esta versión incluye todas las correcciones de la 2203 CU3, además de las siguientes:

- [CVADHELP-22435] Un año después de detectar que el usuario tiene instalada la aplicación Citrix Workspace, las aplicaciones se inician en un explorador en lugar de en la aplicación Citrix Workspace.
- [CVADHELP-21886] Cuando se usa la API de StoreFront Store Service para iniciar una aplicación, omitiendo parámetros como la calidad de audio e inhabilitando impresoras, los parámetros pueden afectar a todas las solicitudes posteriores y no solo a la solicitud actual.

Retirada de XenApp Services

A partir de esta versión, se retirará la compatibilidad con las URL de XenApp Services (también conocido como PNAgent). Se eliminará en una versión futura. Use la aplicación Citrix Workspace para conectarse a almacenes mediante la URL de almacén.

Eliminación de la capacidad de agregar Delivery Controllers de XenApp 6.5

Ya no es posible agregar nuevos feeds de recursos de XenApp 6.5 mediante la consola de administración de StoreFront. Aún es posible agregarlos mediante PowerShell Add-STFStoreFarm especificando `XenApp` como FarmType. Por ejemplo:


```
$store = Get-STFStoreService
Add-STFStoreFarm -StoreService $store -FarmName "XenApp" -FarmType
    XenApp -Port 80 -TransportType HTTP -Servers Xen1
<!--NeedCopy-->
```

Los feeds de recursos de XenApp 6.5 existentes se pueden modificar mediante la consola de administración.

> **Nota:**
>
> Citrix no admite XenApp 6.5. En una versión futura, no se podrán usar Delivery Controllers de XenApp 6.5.

Eliminación de la capacidad de abrir recursos en Internet Explorer 11

Ya no se pueden abrir recursos en el explorador web Internet Explorer 11. Aún es posible acceder a almacenes desde Internet Explorer 11, pero debe instalar la aplicación Citrix Workspace para Windows para poder iniciar recursos.

Problemas conocidos

No hay ningún problema nuevo conocido en esta versión.

Nueva interfaz de usuario para almacenes locales (Technical Preview)

February 26, 2024

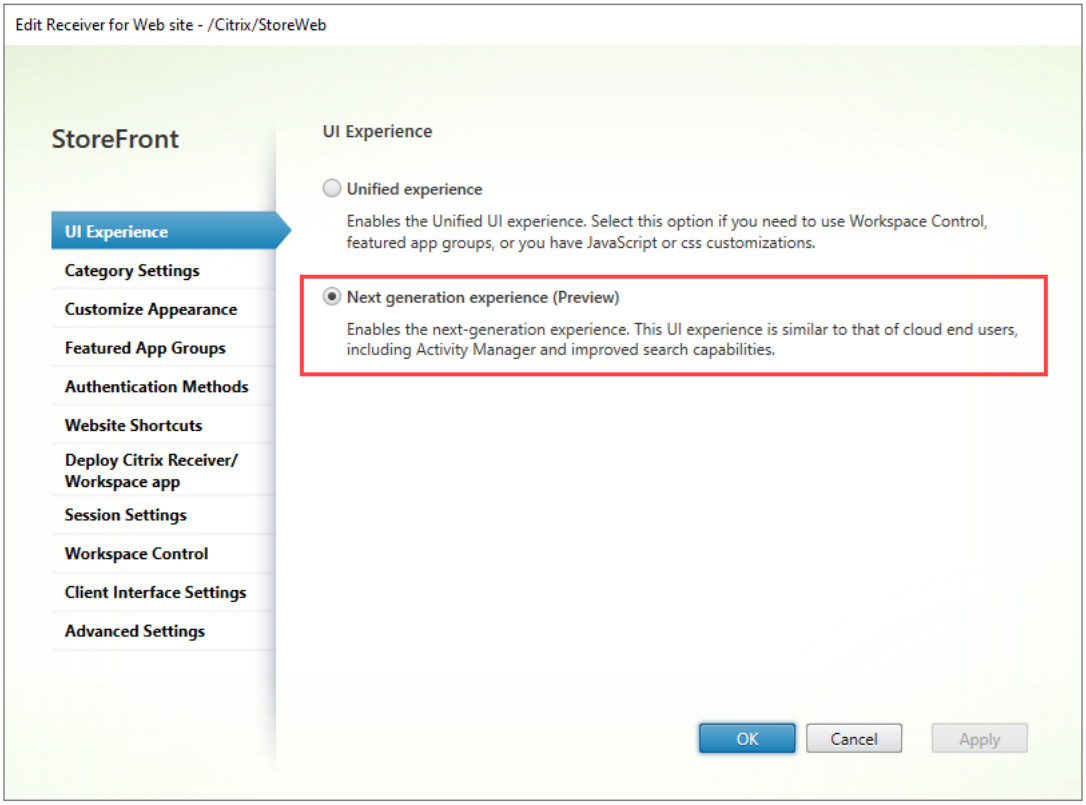
La nueva interfaz de usuario ya está disponible para los almacenes locales. Esta interfaz de usuario, que anteriormente solo estaba disponible para almacenes en la nube, garantiza una apariencia uniforme para todos los almacenes locales y en la nube.

La nueva interfaz de usuario está diseñada para mejorar y simplificar la experiencia del usuario final a la hora de acceder a aplicaciones y escritorios de Citrix. Reduce la complejidad visual, proporciona un acceso fácil a las funciones esenciales y optimiza el uso de la aplicación StoreFront. Es compatible con nuevas funciones, como Administrador de actividades, que facilita la administración eficaz de los recursos de aplicaciones y escritorios virtuales.

> **Nota:**
>
> En este artículo, la experiencia de la interfaz de usuario actual se denomina experiencia de interfaz de usuario unificada.

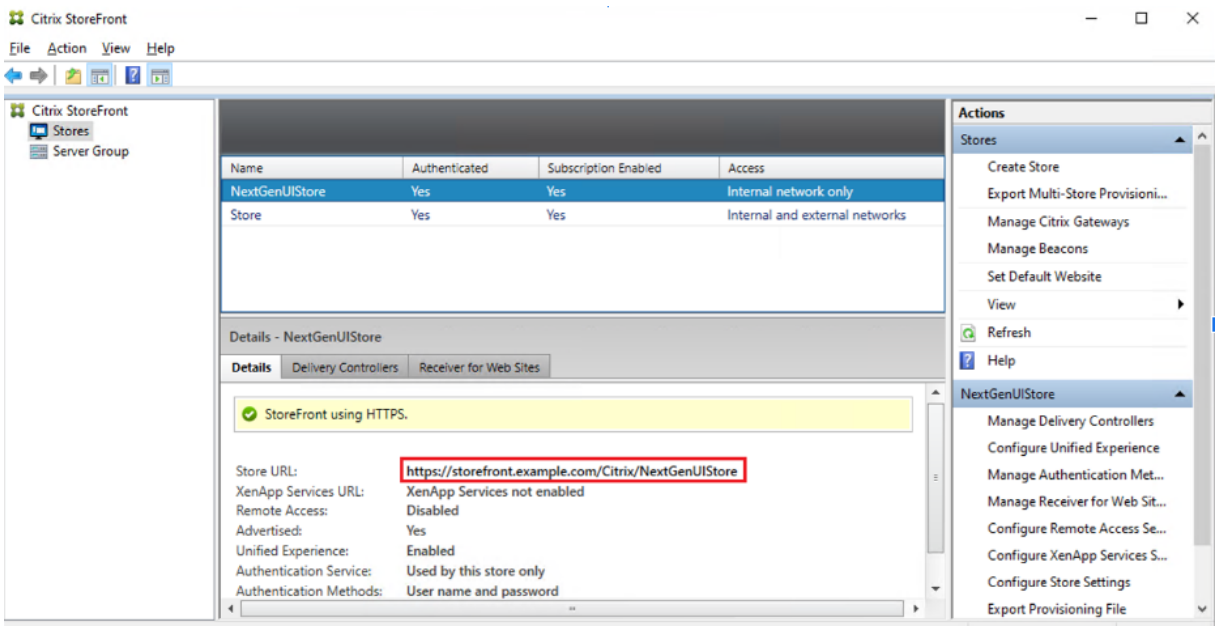
Habilite la nueva experiencia de interfaz de usuario para almacenes locales

Puesto que esta función es actualmente una versión preliminar, se recomienda crear un nuevo almacén y después habilitar la nueva experiencia de interfaz de usuario para ese almacén en particular. Una vez que haya creado el almacén, debe habilitar la nueva interfaz de usuario seleccionando **Next generation experience** en la página de configuración del sitio web. Habilitar la nueva interfaz de usuario para un nuevo almacén le ayuda a probar la interfaz de usuario con un número limitado de usuarios.

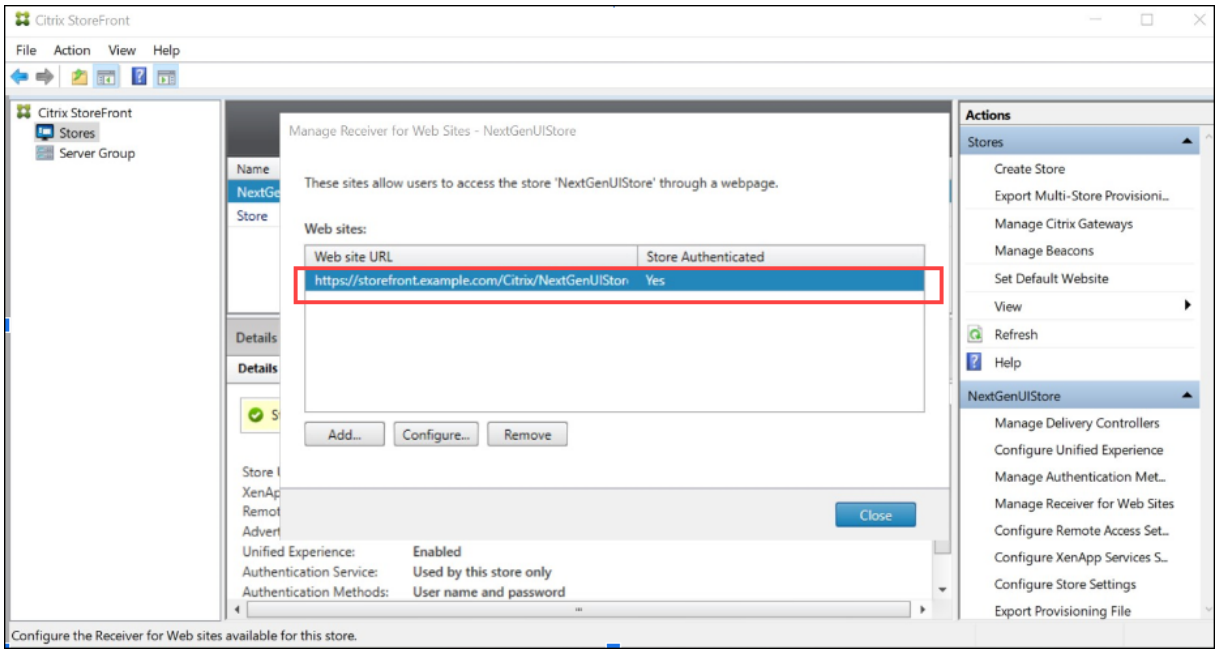


Una vez que haya creado un nuevo almacén con la nueva interfaz de usuario habilitada, tendrá que compartir el sitio web o el enlace del almacén con sus usuarios finales.

- Si sus usuarios finales usan la aplicación nativa, debe compartir con ellos el enlace del nuevo almacén.



- Si los usuarios finales inician sesión a través de un explorador web, es preciso compartir con ellos el enlace del nuevo sitio web.



Personalizar el tema y el logotipo

Puede personalizar el tema y el logotipo de su almacén habilitado para la nueva interfaz de usuario. Puede administrar estos parámetros desde la ficha **Personalizar apariencia** en **Administrar su sitio web**. Para obtener información detallada sobre la configuración de un tema y un logotipo, consulte Personalizar apariencia.

Ventajas clave

La nueva interfaz de usuario incluye las siguientes mejoras clave:

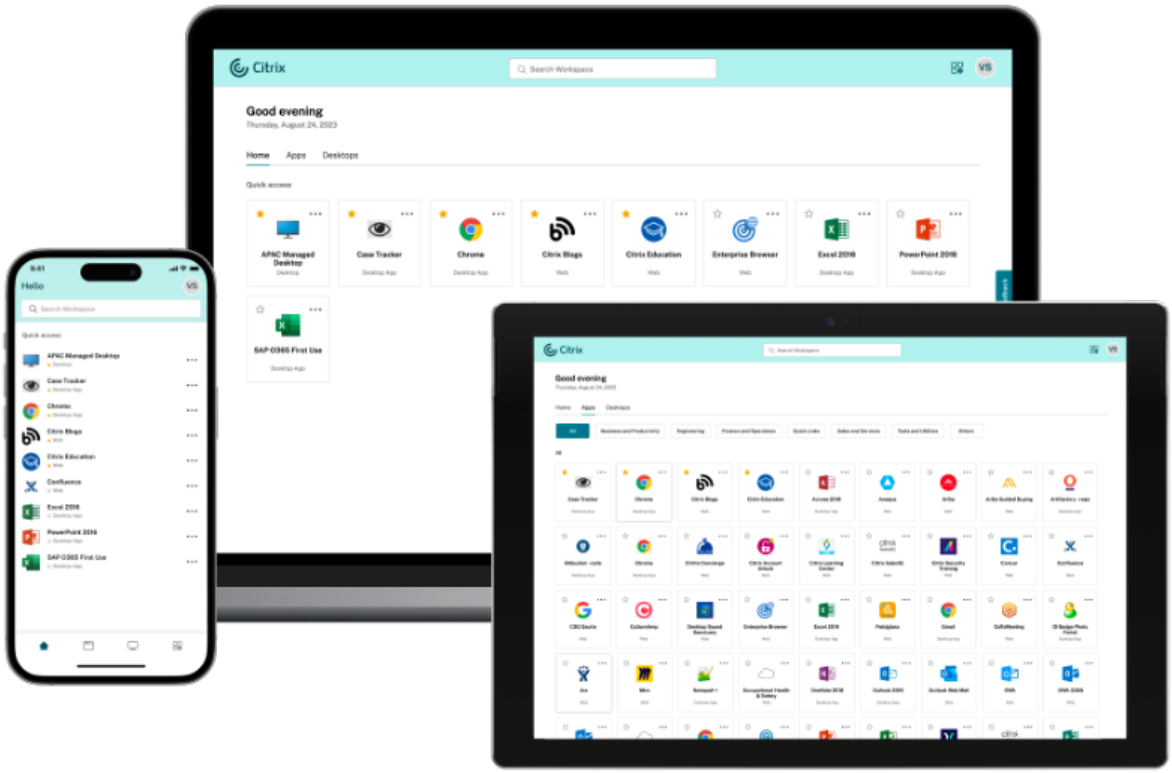
- **Interfaz de usuario fácil de usar**: reduce la complejidad visual y proporciona un fácil acceso a las funciones esenciales. Para obtener más información, consulte Mejoras visuales y de diseño del espacio de trabajo.
- **Administrador de actividades**: permite realizar acciones rápidas en aplicaciones y escritorios virtuales activos para ahorrar recursos y optimizar el rendimiento. Para obtener más información, consulte Administrador de actividades.
- **Categorización mejorada de las aplicaciones**: estructuras de carpetas de varios niveles que se adaptan al tamaño de la pantalla del usuario. Para obtener más información, consulte la ayuda sobre categorización de aplicaciones.
- **Capacidades de búsqueda mejoradas**: las nuevas capacidades de búsqueda proporcionan mejores resultados y con mayor rapidez. Para obtener más información, consulte Opciones de búsqueda.

Mejoras visuales y de diseño del espacio de trabajo

La nueva experiencia del usuario está diseñada para ofrecer un uso intuitivo y simplificado. Las aplicaciones y los escritorios se organizan en las páginas **Inicio**, **Aplicaciones** y **Escritorios** para facilitar la navegación. Las aplicaciones y los escritorios marcados como favoritos se colocan al principio de la lista para facilitar el acceso.

Si los usuarios tienen menos de 20 aplicaciones, se les presenta una vista sencilla sin fichas ni categorías. Todas las aplicaciones y escritorios aparecen en la misma página. Las aplicaciones marcadas como favoritas se colocan al principio de la lista, seguidas de las demás aplicaciones en orden alfabético.

Los usuarios finales pueden marcar cualquier aplicación o escritorio como favoritos haciendo clic en el icono de estrella correspondiente. Del mismo modo, pueden quitar una aplicación o un escritorio de la lista de favoritos haciendo clic en el icono de estrella correspondiente.



Si los usuarios tienen más de 20 aplicaciones, acceden a la página **Inicio** después de iniciar sesión. Desde la página **Inicio** se puede acceder a las aplicaciones y los escritorios favoritos y a las cinco aplicaciones y escritorios utilizados más recientemente. Las aplicaciones y los escritorios exigidos por los administradores se indican con un icono de estrella. Los usuarios finales no pueden quitar estas aplicaciones y escritorios de la lista de Favoritos.

Si el administrador aún no ha habilitado la página de inicio, los usuarios acceden a la página **Aplicaciones**. También en esta página, las aplicaciones favoritas aparecen primero, seguidas de todas las demás aplicaciones en orden alfabético. Si el administrador ha creado categorías de aplicaciones, los usuarios pueden hacer clic en las categorías para buscar sus aplicaciones.

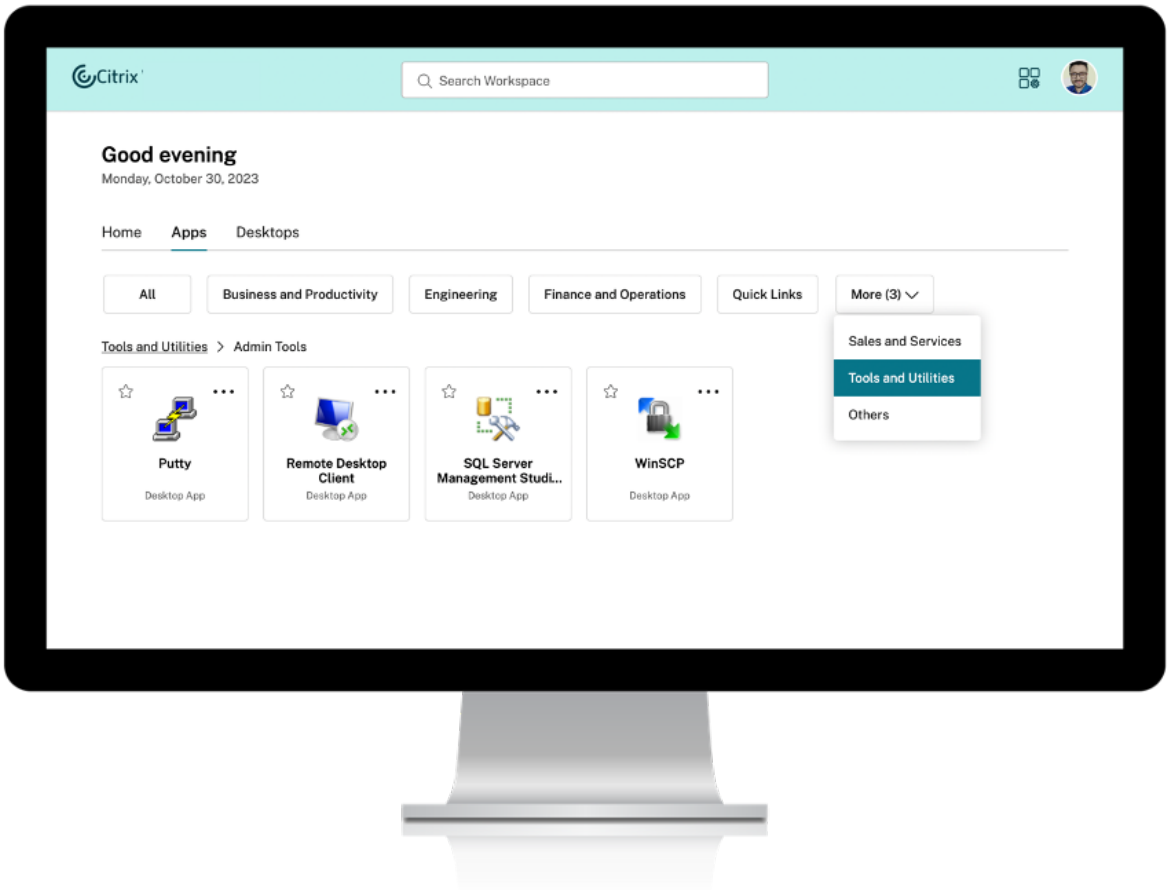
Categorización de aplicaciones en la nueva interfaz de usuario

En la nueva interfaz de usuario, los usuarios finales pueden ver sus aplicaciones organizadas en categorías y subcategorías. Las subcategorías se muestran en una estructura de carpetas. La estructura organizada en varios niveles ofrece una experiencia optimizada y ordenada que ayuda a aumentar la satisfacción general del usuario. Para obtener más información sobre la creación de carpetas y subcarpetas, consulte Parámetros de las categorías.

Cuando el número de categorías principales creadas por los administradores supera el espacio disponible en la pantalla del usuario, la interfaz de usuario se ajusta en función del tamaño de

la pantalla y desplaza las categorías de forma dinámica bajo el **menú desplegable *Más**. Los usuarios también pueden ver las rutas de navegación.

En plataformas móviles, vaya a la ficha **Aplicaciones** y haga clic en el menú desplegable **Categorías** para ver una lista de las categorías disponibles. Las subcategorías se muestran como carpetas. Las subcarpetas pueden contener otras subcarpetas o aplicaciones según configure el administrador.

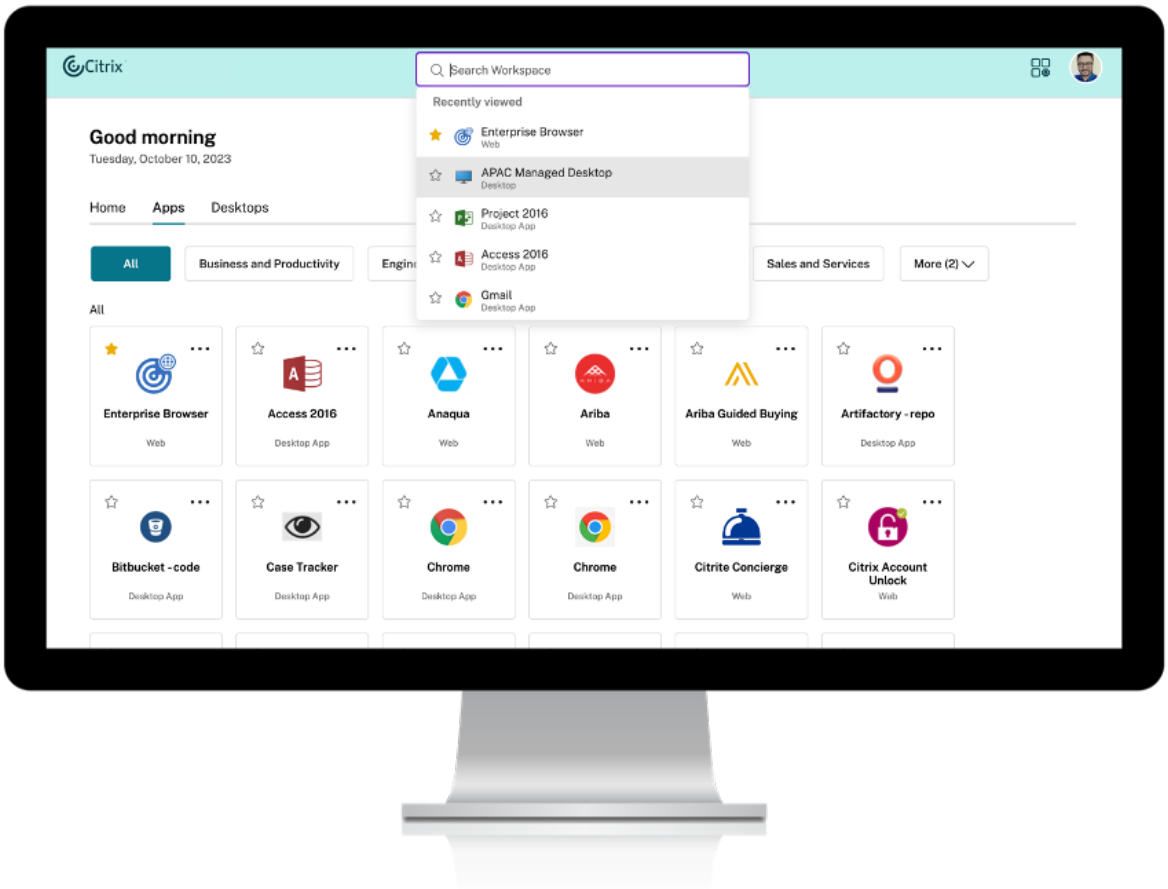


> **Nota:**
>
> En la experiencia de interfaz de usuario unificada, las aplicaciones se categorizan en carpetas. La jerarquía de carpetas se muestra en forma de rutas de navegación mientras se navega por las aplicaciones o los escritorios. Para obtener más información, consulte Parámetros de las categorías.

Opciones de búsqueda

La capacidad de búsqueda de la nueva interfaz de usuario es una mejora con respecto a la interfaz de usuario unificada. La función de búsqueda mejorada de la nueva interfaz de usuario ofrece mejores

resultados de los motores de búsqueda mediante mecanismos de búsqueda borrosa. La opción de búsqueda se muestra en la barra de herramientas para facilitar su uso y le permite hacer búsquedas rápidas e intuitivas.



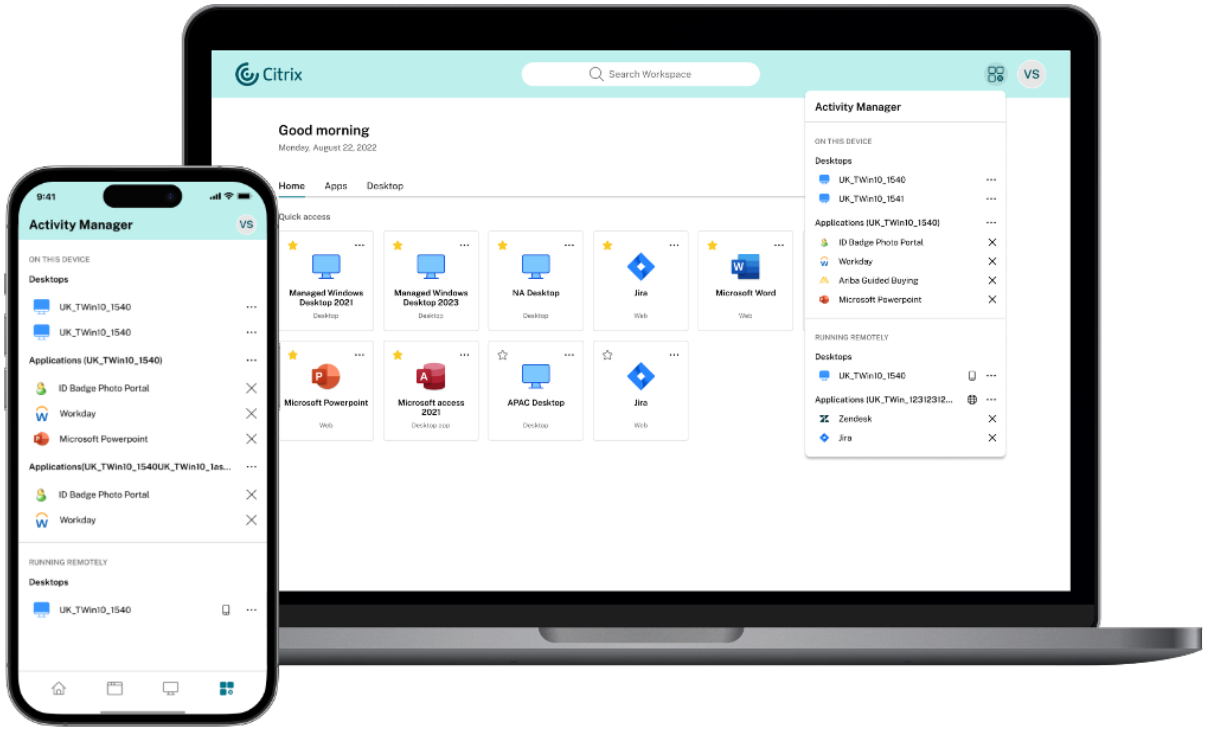
Incluye las siguientes mejoras:

- La búsqueda predeterminada muestra las cinco aplicaciones o escritorios utilizados más recientemente
- Las búsquedas se habilitan con corrector ortográfico y muestran resultados de autocompletar
- Realización de búsquedas por categorías creadas por el administrador
- Los resultados de la búsqueda muestran los favoritos en la parte superior
  La interfaz de usuario unificada implementa mecanismos de búsqueda básicos que podrían no ser tan eficaces como las capacidades de búsqueda de la nueva interfaz de usuario.

Administrador de actividades

El administrador de actividades es una función sencilla pero eficaz de Citrix Workspace que permite a los usuarios administrar sus recursos de manera eficaz. Mejora la productividad al facilitar acciones rápidas en aplicaciones y escritorios activos desde cualquier dispositivo. Los usuarios pueden interactuar de forma fluida con sus sesiones para finalizar o desconectar las sesiones que ya no sean necesarias, liberar recursos y optimizar el rendimiento.

El panel del administrador de actividades muestra una lista consolidada de las aplicaciones y escritorios que están activos no solo en el dispositivo actual, sino también en cualquier dispositivo remoto que tenga sesiones activas. Para ver esta lista, los usuarios pueden hacer clic en el icono del administrador de actividades situado junto al icono del perfil en el escritorio y en la parte inferior de la pantalla en dispositivos móviles.

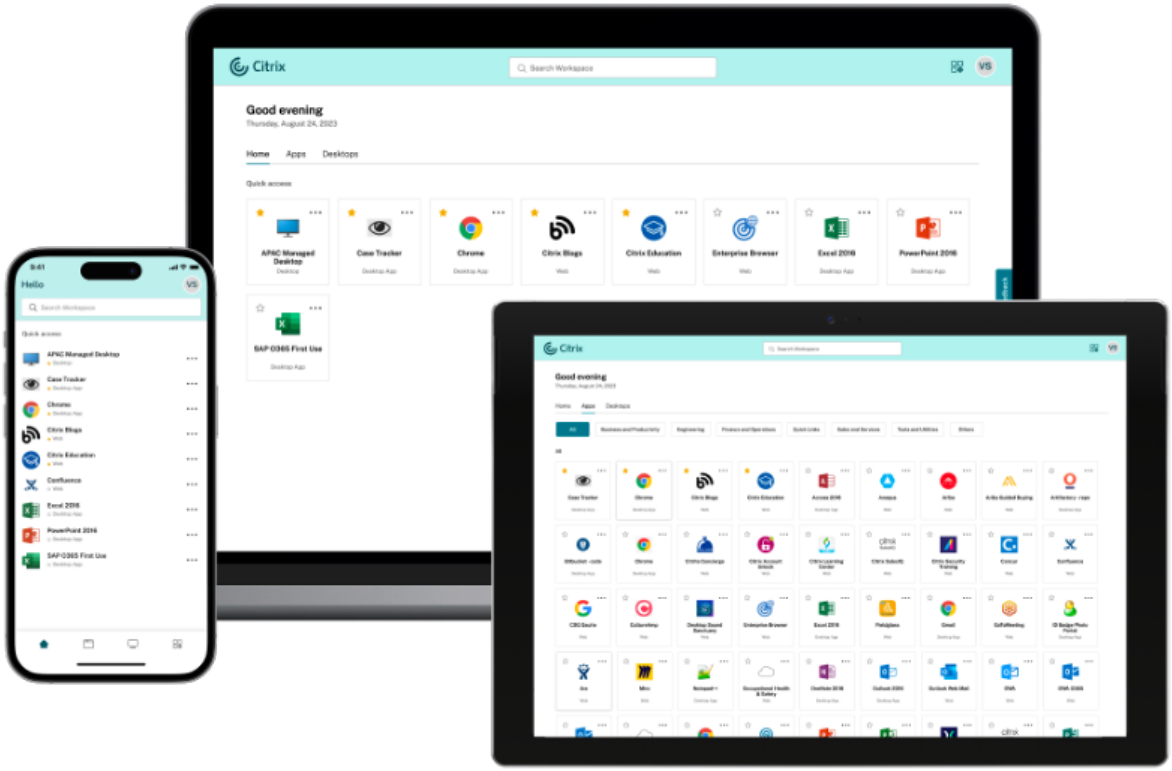


> **Importante:**
>
> La función Administrador de actividades solo está disponible para los almacenes que tienen habilitada la nueva interfaz de usuario. No está disponible en la experiencia de interfaz de usuario unificada.

Usar el administrador de actividades

Las aplicaciones y los escritorios activos se agrupan de la siguiente forma en el panel del administrador de actividades.

- Las aplicaciones y los escritorios que están activos en el dispositivo actual se encuentran agrupados en **En este dispositivo**.
- Las aplicaciones y los escritorios que están activos en otros dispositivos se encuentran agrupados en **Ejecución remota**.



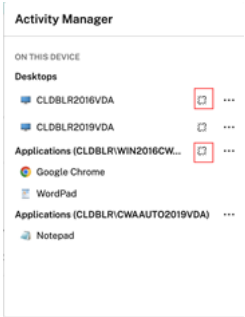
Los usuarios pueden realizar estas acciones en una aplicación o un escritorio al hacer clic en el botón de puntos suspensivos (…) correspondiente.

- **Desconectar**: La sesión remota se desconecta, pero las aplicaciones y los escritorios están activos en segundo plano.
- **Cerrar sesión**: Cierra la sesión en curso. Se cierran todas las aplicaciones de la sesión, y se pierden los archivos no guardados.
- **Apagar**: Cierra los escritorios desconectados.
- **Forzar cierre**: apaga el escritorio en caso de problemas técnicos.
- **Reiniciar**: Apaga el escritorio y lo inicia de nuevo.

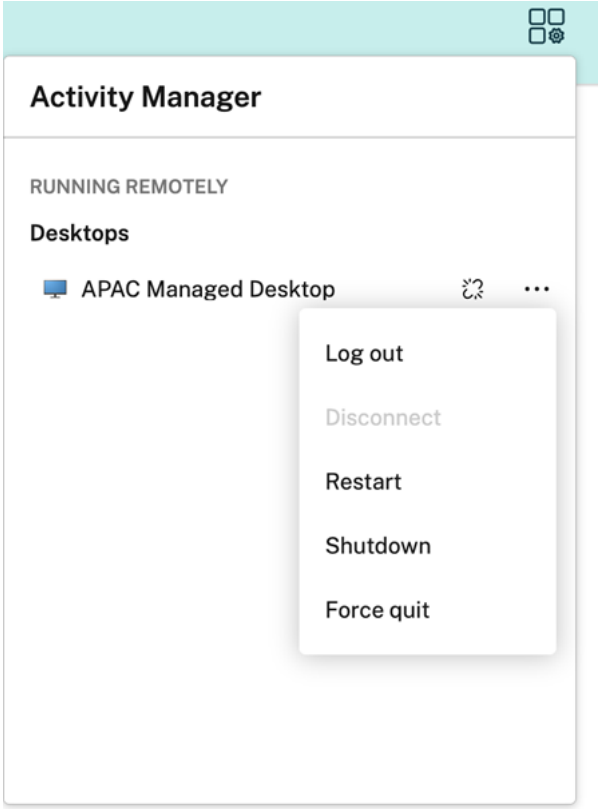
Aplicaciones y escritorios desconectados

Ahora, el administrador de actividades permite a los usuarios finales ver y realizar acciones en aplicaciones y escritorios que se ejecutan en modo desconectado, ya sea de forma local o remota. Las se-

siones se pueden administrar desde dispositivos móviles o de escritorio, lo que permite a los usuarios finales realizar acciones sobre la marcha. Realizar acciones en sesiones desconectadas, como cerrar la sesión o el apagado, promueve el uso optimizado de recursos y reduce el consumo de energía.



- Las aplicaciones y los escritorios desconectados se muestran en el panel del administrador de actividades y se indican mediante un icono de desconexión.
- Las aplicaciones desconectadas se agrupan en las sesiones respectivas y las sesiones se indican mediante un icono de desconexión.



Los usuarios finales pueden realizar estas acciones en sus escritorios desconectados al hacer clic en el botón de puntos suspensivos:

- **Cerrar sesión**: use esta opción para cerrar sesión en el escritorio desconectado. Se cierran

todas las aplicaciones de la sesión, y se pierden los archivos no guardados.
- **Apagar**: Use esta opción para cerrar los escritorios desconectados.
- **Forzar cierre**: use esta opción para forzar el cierre de los escritorios desconectados en caso de problemas técnicos.
- **Reiniciar**: use esta opción para apagar e iniciar de nuevo el escritorio desconectado.

El comportamiento de las sesiones desconectadas en el administrador de actividades difiere de esta manera.

- Si ha iniciado sesión a través de un explorador web y se desconecta de una sesión local, la sesión aparece primero en **En este dispositivo**. Sin embargo, cuando cierra y abre de nuevo el administrador de actividades, la sesión desconectada pasará a **Ejecución remota**.
- Si ha iniciado sesión en un dispositivo nativo y se desconecta de una sesión local, la sesión desconectada desaparece de la lista. Sin embargo, cuando cierra y abre de nuevo otra vez el administrador de actividades, la sesión desconectada pasará a **Ejecución remota**.

Limitaciones conocidas

- La nueva interfaz de usuario no admite una personalización profunda mediante la API de JavaScript y CSS. Actualmente, esta función está disponible en la experiencia de interfaz de usuario unificada.
- La nueva interfaz de usuario no admite accesos directos de direcciones URL incrustados que llevan directamente a aplicaciones o a escritorios. Esta funcionalidad está disponible en la experiencia de interfaz de usuario unificada.
- La función Workspace Control, que permite a los usuarios finales volver a conectarse a sus sesiones desde un dispositivo remoto, no es compatible actualmente con la nueva experiencia de interfaz de usuario. Esta función está disponible en la experiencia de interfaz de usuario unificada.
- La función de cambio de contraseña no está disponible en la nueva interfaz de usuario.

Problemas conocidos

- Cuando se cambia la experiencia de interfaz de usuario de un almacén existente, los usuarios que se conectan a través de una aplicación Citrix Workspace instalada localmente no se actualizan. Deben quitar el almacén y volver a agregarlo a su aplicación. [WSP-21493]
- Las extensiones de explorador web no son compatibles con la Technical Preview de la nueva interfaz de usuario. [WSUI-8503]
- Las operaciones del administrador de actividades, como cerrar sesión, desconectar, etc., no están disponibles para aplicaciones que tienen habilitadas directivas de App Protection. [WSP-21324]

- En la aplicación Citrix Workspace para iOS, las iniciales del usuario no se muestran en el avatar. [WSUI-8482]

Instalación, configuración, actualización de versiones y desinstalación

August 15, 2023

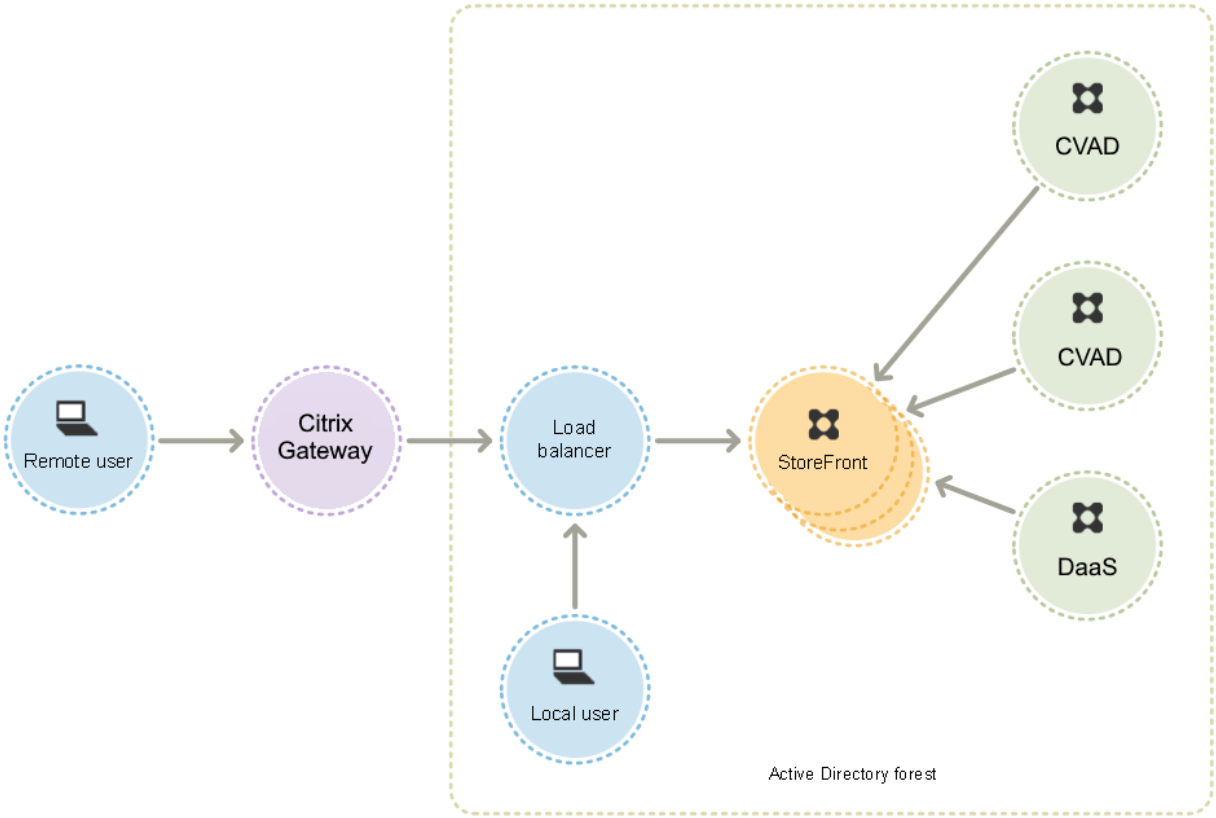
Tarea	Detalles
Planificar una implementación de StoreFront	Descripción general de los componentes que intervienen en una implementación de StoreFront
Opciones de acceso de los usuarios	Resumen sobre cómo los usuarios pueden acceder a sus almacenes
Requisitos del sistema	Asegurarse de cumplir los requisitos previos para instalar StoreFront
Instalar StoreFront	Instalar StoreFront en un servidor nuevo
Proteger StoreFront con HTTPS	Cifrar el acceso de los clientes a StoreFront mediante HTTPS
Proteger la implementación de StoreFront	Configurar StoreFront para una mayor seguridad
Crear una implementación	Configurar un nuevo servidor de StoreFront con un almacén nuevo
Unirse a un grupo de servidores existente	Configurar un nuevo servidor de StoreFront para que se una a un grupo de servidores existente
Actualizar la versión de StoreFront	Actualizar la versión de un servidor de StoreFront desde una versión anterior
CEIP	Participar o salir del programa Customer Experience Improvement Program de Citrix (CEIP)
Citrix Analytics Service	Configurar StoreFront para enviar datos a Citrix Analytics Service
Desinstale StoreFront	Quitar StoreFront de su servidor
Restablecer un servidor a los valores predeterminados de fábrica	Borrar todos los parámetros de StoreFront para poder configurarlo de nuevo

Planificar una implementación de StoreFront

February 26, 2024

StoreFront se integra con las implementaciones de Citrix Virtual Apps and Desktops para proporcionar a los usuarios un único punto de acceso de autoservicio a sus escritorios y aplicaciones.

La imagen muestra una implementación típica de StoreFront.



Active Directory

StoreFront usa Active Directory para autenticar a usuarios y buscar la pertenencia a grupos y otros detalles, así como para sincronizar los datos entre servidores de StoreFront.

En el caso de implementaciones de servidor único, StoreFront puede instalarse en un servidor que no esté unido a un dominio, aunque ciertas funciones no estarán disponibles. Los servidores de StoreFront deben residir ya sea en el dominio de Active Directory que contiene las cuentas de los usuarios, o en un dominio que tenga una relación de confianza con el dominio de las cuentas de usuario, a menos que se habilite la delegación de la autenticación en las comunidades o sitios de Citrix Virtual Apps and Desktops. Todos los servidores de StoreFront pertenecientes a un grupo deben residir en el mismo dominio.

Grupos de servidores de StoreFront

StoreFront se puede configurar en un único servidor o como una implementación de varios servidores denominada grupo de servidores de StoreFront. Los grupos de servidores no solo proporcionan capacidad adicional, sino también una mayor disponibilidad. StoreFront garantiza que la información acerca de la configuración y las suscripciones de los usuarios a las aplicaciones se almacena y se sincroniza entre todos los servidores de un grupo de servidores. Esto significa que, si algún servidor de StoreFront deja de estar disponible por alguna razón, los usuarios pueden usar los demás servidores para seguir accediendo a sus almacenes. Entretanto, los datos de configuración y suscripciones existentes en el servidor fallido se actualizan cuando dicho servidor se reconecta con su grupo de servidores. Los datos de suscripción se actualizan cuando se reanuda la conexión del servidor, pero debe propagar los cambios de la configuración si alguno se ha perdido mientras el servidor estaba sin conexión. En el caso de producirse un fallo de hardware que requiera la sustitución del servidor, puede instalar StoreFront en un nuevo servidor y agregarlo al grupo de servidores existente. El nuevo servidor se configurará y actualizará automáticamente con las suscripciones de los usuarios a las aplicaciones cuando se incorpore al grupo de servidores.

Citrix recomienda un máximo de cinco servidores en un grupo de servidores. En casos con más de cinco servidores, la sobrecarga de la sincronización de datos es mayor que las ventajas de los servidores adicionales, y el rendimiento baja.

Las implementaciones de grupos de servidores de StoreFront solo se admiten cuando los vínculos entre servidores de un grupo de servidores tienen una latencia inferior a 40 ms (con suscripciones inhabilitadas) o inferior a 3 ms (con suscripciones habilitadas). Lo ideal sería que todos los servidores de un grupo de servidores residan en la misma ubicación (centro de datos, zona de disponibilidad), pero los grupos de servidores pueden abarcar varias ubicaciones dentro de la misma región siempre que los vínculos entre los servidores del grupo cumplan estos criterios de latencia. Algunos ejemplos incluyen grupos de servidores que abarcan varias zonas de disponibilidad dentro de una región en la nube o entre centros de datos de áreas metropolitanas. Tenga en cuenta que la latencia entre zonas varía según el proveedor de la nube. Citrix no recomienda abarcar varias ubicaciones como configuración de recuperación ante desastres, pero puede ser una opción adecuada para la alta disponibilidad.

Equilibrio de carga

En el caso de varios servidores de un grupo de servidores de StoreFront, debe configurar el equilibrio de carga externo. Use un equilibrador de carga con monitores integrados y persistencia de sesiones, como NetScaler ADC. Para obtener más información acerca del equilibrio de carga con NetScaler ADC, consulte Equilibrio de carga.

Citrix Gateway para acceso remoto

Si piensa habilitar el acceso a StoreFront desde fuera de la red corporativa, se necesita un dispositivo Citrix Gateway para proteger las conexiones de los usuarios remotos. Implemente Citrix Gateway fuera de la red corporativa, con firewalls que separen Citrix Gateway de redes tanto públicas como internas. Asegúrese de que Citrix Gateway puede acceder al bosque de Active Directory que contiene los servidores de StoreFront.

Equilibrador de carga de servidores globales

En grandes implementaciones de Citrix, es posible que tenga implementaciones de StoreFront y NetScaler en varios centros de datos. Con un equilibrador de carga de servidores globales (GSLB), puede configurar una única URL global que GSLB redirija a la URL específica de una puerta de enlace en una de las regiones. Por lo general, GSLB elige la puerta de enlace más cercana en función de un algoritmo de equilibrio de carga, como el tiempo de ida y vuelta (RTT) o la proximidad estática.

Por ejemplo, puede tener 3 puertas de enlace regionales:

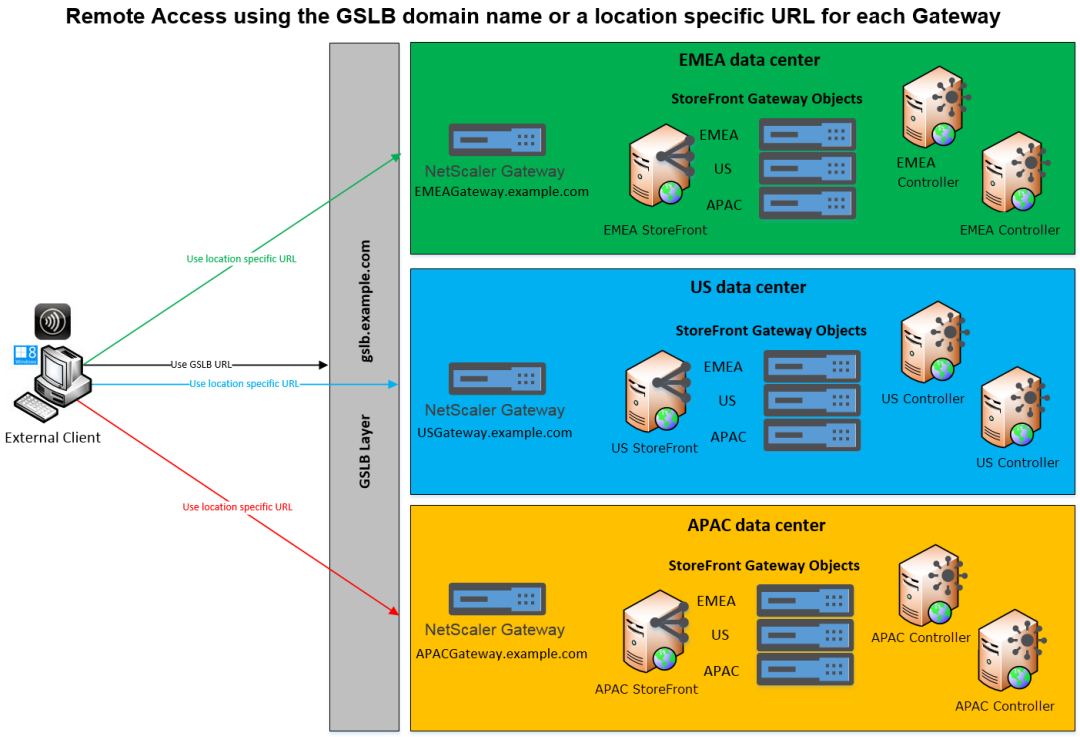
`emeagateway.example.com`: Puerta de enlace de Europa

`usgateway.example.com`: Puerta de enlace de EE. UU.

`apacgateway.example.com`: Puerta de enlace de Asia Pacífico

Junto con GSLB

`gslb.example.com`



Antes de configurar GSLB, revise los certificados de servidor que tiene y cómo su organización lleva a cabo la resolución de DNS. Las direcciones URL que se quieran usar en la implementación de Citrix Gateway y StoreFront deben estar presentes en los certificados del servidor.

StoreFront no tiene ningún mecanismo integrado para sincronizar la configuración entre grupos de servidores. En su lugar, es el administrador quien debe configurar cada grupo de servidores de StoreFront de la misma manera para que los usuarios disfruten de una experiencia uniforme independientemente del grupo de servidores al que se conecten.

StoreFront puede sincronizar periódicamente las suscripciones (favoritas) entre grupos de servidores. Consulte Sincronización de suscripciones.

Acceso de usuarios

Consulte Opciones de acceso de los usuarios.

Opciones de acceso de los usuarios

April 17, 2024

Los usuarios pueden acceder a los almacenes de StoreFront mediante tres métodos distintos.

- Aplicación Citrix Workspace instalada localmente: Los usuarios con versiones compatibles de la aplicación Citrix Workspace pueden acceder a almacenes de StoreFront desde la interfaz de usuario de la aplicación Citrix Workspace. Esto ofrece la mejor experiencia del usuario y la máxima funcionalidad posibles.
- Aplicación Citrix Workspace para HTML5: Los usuarios con exploradores web compatibles pueden acceder a almacenes de StoreFront a través del sitio web del almacén. De forma predeterminada, los usuarios también necesitan una versión compatible de la aplicación Citrix Workspace para acceder a sus escritorios y aplicaciones, lo que se conoce como inicio híbrido. Sin embargo, puede configurar su sitio web para que los usuarios puedan acceder a sus recursos a través del explorador web sin necesidad de instalar la aplicación Citrix Workspace.
- Direcciones URL de XenApp Service: Los usuarios con clientes Citrix antiguos cuya versión no se puede actualizar pueden acceder a almacenes mediante la URL de XenApp Services del almacén. Al crear un almacén, la URL de XenApp Services correspondiente se habilita de forma predeterminada.

Aplicación Citrix Workspace instalada localmente

Acceder a almacenes desde la aplicación Citrix Workspace instalada localmente ofrece la mejor experiencia de usuario. Para ver las versiones de la aplicación Citrix Workspace que pueden usarse para acceder a los almacenes de esta manera, consulte Requisitos del sistema.

La aplicación Citrix Workspace utiliza direcciones URL internas y externas como balizas. Al intentar ponerse en contacto con estas balizas, la aplicación Citrix Workspace puede determinar si los usuarios están conectados a redes locales o públicas. Cuando un usuario accede a un escritorio o a una aplicación, la información de ubicación se transfiere al servidor que proporciona el recurso para que se puedan devolver los correspondientes datos de conexión a la aplicación Citrix Workspace. Esto permite que la aplicación Citrix Workspace se asegure de no pedir a los usuarios que vuelvan a iniciar sesión al acceder a un escritorio o a una aplicación. Para obtener más información, consulte Configurar balizas.

Agregar un almacén a la aplicación Workspace

Después de la instalación, la aplicación Citrix Workspace debe configurarse con los datos de conexión de los almacenes que suministran aplicaciones y escritorios de usuario. Si quiere facilitar el proceso de configuración para los usuarios, proporcióneles la información necesaria de una de las siguientes formas.

> **Importante:**
>
> De forma predeterminada, la aplicación Citrix Workspace requiere conexiones HTTPS a los almacenes. Si StoreFront no está configurado para HTTPS, los usuarios deben llevar a cabo

> pasos de configuración adicionales para usar conexiones HTTP. Citrix recomienda encarecidamente no habilitar conexiones de usuario no seguras a StoreFront en un entorno de producción. Para obtener más información, consulte Parámetros de configuración de almacenes en la documentación de la aplicación Citrix Workspace para Windows.

Configuración manual Los usuarios pueden conectar la aplicación Citrix Workspace a su almacén al agregar direcciones URL de almacén en la aplicación Citrix Workspace. Para obtener más información, consulte la documentación de la aplicación Citrix Workspace.

Archivos de aprovisionamiento Es posible proporcionar a los usuarios archivos de aprovisionamiento que contengan los datos de conexión a sus almacenes. Después de instalar la aplicación Citrix Workspace, los usuarios pueden abrir el archivo CR para configurar automáticamente las cuentas para los almacenes. De forma predeterminada, el sitio web ofrece a los usuarios un archivo de aprovisionamiento para el único almacén para el que esté configurado el sitio en cuestión. Puede indicar a los usuarios que visiten los sitios web de los almacenes a los que deseen tener acceso y descarguen los archivos de aprovisionamiento desde esos sitios. También, para lograr un mayor control, puede usar la consola de administración de Citrix StoreFront para generar archivos de aprovisionamiento que contengan los datos de conexión para uno o más almacenes. A continuación, puede distribuir estos archivos a los usuarios adecuados. Para obtener más información, consulte Exportar archivos de aprovisionamiento del almacén para los usuarios.

Direcciones URL de configuración generadas automáticamente Para los usuarios con macOS, es posible utilizar Setup URL Generator de la aplicación Citrix Workspace para Mac con el fin de crear una URL que contenga los datos de conexión de un almacén. Después de instalar la aplicación Citrix Workspace, los usuarios pueden hacer clic en la URL para configurar automáticamente una cuenta para el almacén. Introduzca información de su implementación en la herramienta y genere una URL que se pueda distribuir automáticamente a los usuarios.

Detección de cuentas basada en direcciones de correo electrónico Con la detección de cuentas por correo electrónico, en lugar de tener que conocer los detalles de acceso a sus almacenes, los usuarios introducen sus direcciones de correo electrónico durante el proceso de configuración inicial de la aplicación Citrix Workspace. Para obtener detalles sobre cómo configurar esto, consulte Detección de cuentas por correo electrónico.

Global App Config Service

Use Global App Config Service con tal de configurar la aplicación Citrix Workspace para sus almacenes de StoreFront. Consulte Configurar los parámetros de los almacenes locales.

Aplicación Citrix Workspace para HTML5

Como alternativa a la aplicación Workspace instalada localmente, los usuarios pueden acceder a su almacén a través de un explorador web con la aplicación Workspace para HTML5. Cuando los usuarios vienen a iniciar sus recursos, hay dos posibilidades.

1. Los recursos se inician en la aplicación Citrix Workspace instalada localmente. Esto se conoce como inicio híbrido. Esto ofrece a los usuarios la mejor experiencia, ya que pueden aprovechar la integración total del sistema operativo. Para obtener más información detallada, consulte Inicio híbrido.
2. Los recursos se inician en el explorador web. Esto permite a los usuarios acceder a recursos sin necesidad de instalar software localmente.

La configuración predeterminada exige que la aplicación Citrix Workspace esté instalada localmente para inicios híbridos. Puede cambiar la configuración para iniciar siempre los recursos en el explorador web o de modo que el usuario pueda elegir. Consulte Implementar la aplicación Workspace.

Si el administrador seleccionó **Usar Receiver para HTML5 si el Receiver local no está disponible**, cuando el usuario abra por primera vez el sitio web del almacén en su explorador web, tendrá la opción de hacer clic en **Usar versión simplificada** para iniciar recursos en su explorador web.

Requisitos para abrir recursos en el explorador web

Para los usuarios de la red interna, el acceso a través de la aplicación Citrix Workspace para HTML5 para los recursos proporcionados por Citrix Virtual Apps and Desktops se encuentra inhabilitado de manera predeterminada. Para habilitar el acceso local a escritorios y aplicaciones mediante la aplicación Citrix Workspace para HTML5, habilite la directiva Conexiones de WebSockets en los servidores Citrix Virtual Apps and Desktops. Citrix Virtual Apps and Desktops utiliza el puerto 8008 en las conexiones de la aplicación Citrix Workspace para HTML5. Asegúrese de que los firewalls y otros dispositivos de red permitan el acceso a este puerto. Para obtener más información, consulte Configuraciones de directiva de WebSockets.

Para que los recursos de Citrix Virtual Apps and Desktops se inicien correctamente, configure las conexiones TLS a los VDA que alojan aplicaciones y escritorios. Las conexiones remotas a través de Citrix Gateway pueden iniciar recursos mediante la aplicación Citrix Workspace para HTML5 sin configurar conexiones TLS al VDA.

Inicio híbrido

Cuando los usuarios abren Citrix Workspace para HTML5 por primera vez a través de su explorador web, pero inician aplicaciones dentro de la aplicación Citrix Workspace instalada localmente, esto

se conoce como inicio híbrido. Hay varias formas en las que el sitio web puede comunicarse con la aplicación Workspace instalada localmente para iniciar recursos.

Citrix Workspace Launcher

Cuando el usuario visita por primera vez un sitio web de StoreFront con un sistema operativo y un explorador web compatibles, la aplicación Citrix Workspace para HTML5 intenta invocar Citrix Workspace Launcher. Si hay instalada una versión compatible de la aplicación Citrix Workspace, la aplicación lo notifica a StoreFront. La aplicación Citrix Workspace para HTML5 lo recuerda y, al iniciar una aplicación, usa Citrix Workspace Launcher.

El sitio web del almacén invoca Citrix Workspace Launcher en Windows, Mac y Linux cuando se utilizan los siguientes exploradores web:

- Firefox 52 o una versión posterior
- Chrome 42 o una versión posterior
- Safari 12 o una versión posterior
- Edge 25 o una versión posterior

Citrix Workspace Launcher requiere estas versiones mínimas de Citrix Receiver o de la aplicación Citrix Workspace.

- Receiver para Windows 4.3 o una versión posterior
- Receiver para Mac 12.0 o una versión posterior
- Aplicación Workspace para Linux 2003 o una versión posterior

Si el Launcher de la aplicación Workspace no está disponible o el usuario no permite que se abra, no podrá detectar la aplicación Citrix Workspace instalada localmente. El usuario tiene la opción de intentarlo de nuevo o hacer clic en **Ya instalado**, en cuyo caso recurrirá a iniciar aplicaciones con archivos ICA. El usuario puede intentarlo de nuevo más adelante. Para ello, vaya a la pantalla Parámetros y haga clic en **Cambiar la aplicación Citrix Workspace**.

Si usa varios grupos de servidores StoreFront activos detrás de Global Server Load Balancing, es posible que Citrix Workspace Launcher falle de forma intermitente. Para evitarlo, debe configurar Global Server Load Balancing para forzar que la sesión web del usuario sea persistente para un grupo de servidores de StoreFront durante todo el proceso de detección de clientes (consulte CTX460312). También puede implementar las extensiones web de Citrix Workspace.

Extensiones web de Citrix Workspace

Las extensiones web de Citrix Workspace son extensiones para los exploradores web de uso común que mejoran la experiencia del usuario para detectar la aplicación Citrix Workspace instalada local-

mente e iniciar aplicaciones y escritorios virtuales. En comparación con Citrix Workspace Launcher, proporciona una mejor experiencia de usuario y evita problemas con Global Server Load Balancing.

Para habilitar la detección de clientes basada en extensiones de explorador web:

- Habilite la funcionalidad en el servidor StoreFront.
- Implemente la extensión del explorador web en los dispositivos cliente.
- Implemente la aplicación Citrix Workspace para Windows 2303, Mac 2304 o Linux 2302 o superior.

La primera vez que un usuario visita el sitio web de un almacén en una plataforma compatible, se le pide que detecte la aplicación Workspace instalada localmente. Primero se intenta usar la extensión web y, si eso falla, prueba con Citrix Workspace Launcher. Los usuarios actuales que ya hayan completado la detección de la aplicación Workspace pueden ir a **Parámetros de cuenta** y hacer clic en **Cambiar la aplicación Citrix Workspace** para volver a detectar la aplicación Workspace.

Esta función está desactivada de forma predeterminada. Los administradores pueden habilitar esta función mediante este script de PowerShell en un servidor de StoreFront: `Add-STFFeatureState -Name "Citrix.StoreFront.EnableBrowserExtension"-IsEnabled $True`.

Internet Explorer

La primera vez que el usuario abre el sitio web del almacén en Internet Explorer, se le pide que instale la aplicación Citrix Workspace, que incluye el complemento de cliente ICA de Citrix para Internet Explorer. Una vez instalado el complemento, se usa para iniciar aplicaciones y escritorios a través de la aplicación Citrix Workspace instalada localmente.

Descargas de archivos ICA

Si la aplicación Citrix Workspace para HTML5 no puede detectar una aplicación Citrix Workspace instalada localmente por ningún otro medio, cuando un usuario inicie una aplicación o un escritorio, descarga un archivo ICA. El usuario puede abrir este archivo con la aplicación Citrix Workspace instalada localmente.

Accesos directos a los recursos

Puede generar direcciones URL que proporcionen acceso a escritorios y aplicaciones disponibles en su almacén. Inserte estos enlaces en los sitios web alojados en la red interna y los usuarios tendrán acceso inmediato a los recursos. Los usuarios hacen clic en un enlace y se les redirige al sitio web del almacén, donde deben iniciar sesión si todavía no lo han hecho. El sitio web del almacén inicia automáticamente el recurso. Para obtener más información acerca de la generación de accesos directos a recursos, consulte Accesos directos a sitios web.

Al crear el acceso directo a una aplicación, asegúrese de que no haya otras aplicaciones disponibles en el almacén que tengan el mismo nombre. Los accesos directos no pueden distinguir varias instancias de una aplicación con el mismo nombre. Del mismo modo, si pone varias instancias de un escritorio de un solo grupo de escritorios disponibles desde el almacén, no puede crear accesos directos independientes para cada instancia. Los accesos directos no pueden pasar parámetros de línea de comandos a las aplicaciones.

Para crear accesos directos de aplicaciones, se puede configurar StoreFront con las direcciones URL de los sitios web internos que alojarán los accesos directos. Cuando un usuario hace clic en el acceso directo de una aplicación en un sitio web, StoreFront coteja ese sitio web con la lista de direcciones URL que ha indicado para asegurarse de que la solicitud proviene de un sitio web de confianza. Sin embargo, los sitios web que alojan accesos directos no se validan cuando se trata de usuarios que se conectan a través de Citrix Gateway porque las direcciones URL no se transfieren a StoreFront. Para asegurarse de que los usuarios remotos puedan acceder a accesos directos de aplicaciones de sitios web internos y de confianza, configure Citrix Gateway para limitar el acceso de los usuarios a solamente esos sitios específicos.

Personalizar la interfaz de usuario

Citrix StoreFront proporciona un mecanismo para personalizar la interfaz de usuario. Se aplican tanto si se accede a un almacén a través de la aplicación Citrix Workspace como si se hace a través de un explorador web. Puede personalizar las cadenas de texto, la hoja de estilo en cascada y los archivos de JavaScript. También puede agregar pantallas personalizadas que se mostrarán antes y después del inicio de sesión, así como paquetes de idioma. Para obtener más información, consulte Personalizar apariencia.

Direcciones URL de XenApp Services

> **Nota:**
>
> XenApp Services (también conocido como PNAgent) queda retirado desde StoreFront 2308. Se recomienda utilizar la aplicación Citrix Workspace para conectarse a StoreFront mediante una URL de almacén.

Los usuarios con versiones anteriores de clientes Citrix que no se pueden actualizar pueden acceder a los almacenes mediante la configuración de sus clientes con la URL de XenApp Services para un almacén. También puede habilitar el acceso a los almacenes a través de las direcciones URL de XenApp Services desde dispositivos de escritorio unidos a un dominio y equipos reasignados que tengan Citrix Desktop Lock. En este contexto, la unión a un dominio se refiere a dispositivos que se han vinculado a un dominio del bosque de Active Directory que contiene los servidores de StoreFront.

StoreFront admite la autenticación PassThrough con tarjetas de proximidad a través de la aplicación Citrix Workspace para las direcciones URL de XenApp Services. En los productos asociados de Citrix Ready, se utiliza Citrix Fast Connect API para optimizar los inicios de sesión a través de Citrix Receiver para Windows o la aplicación Citrix Workspace para Windows y conectarse a los almacenes con la URL de XenApp Services. Los usuarios se autentican en estaciones de trabajo mediante tarjetas de proximidad y se conectan rápidamente a los escritorios y las aplicaciones que proporcionan Citrix Virtual Apps and Desktops. Para obtener más información, consulte la documentación más reciente de la aplicación Citrix Workspace para Windows.

Al crear un almacén, la URL de XenApp Services correspondiente se habilita de forma predeterminada. La URL de servicios XenApp para un almacén tiene el formato http[s]://dirección de servidor/Citrix/nombre de almacén/PNAgent/config.xml, donde dirección de servidor es el nombre de dominio completo (FQDN) del servidor o del entorno de equilibrio de carga de su implementación de StoreFront y nombre de almacén es el nombre especificado para el almacén cuando este se creó. Esto permite que las aplicaciones Citrix Workspace que solo pueden usar el protocolo PNAgent puedan conectarse a StoreFront. Para saber los clientes que pueden utilizarse para acceder a almacenes mediante las direcciones URL de servicios XenApp, consulte Requisitos del dispositivo del usuario.

Consideraciones importantes

Las direcciones URL de XenApp Services se han diseñado para los usuarios que no pueden actualizar su versión a la de la aplicación Citrix Workspace y para los casos en que no están disponibles otros métodos de acceso. A la hora de optar por utilizar las direcciones URL de XenApp Services para proporcionar a los usuarios acceso a los almacenes, tenga en cuenta las siguientes restricciones.

- No se puede modificar la URL de XenApp Services para un almacén.
- No se puede modificar la configuración de la URL de XenApp Services mediante la edición del archivo de configuración, config.xml.
- Las direcciones URL de XenApp Services admiten la autenticación explícita, la autenticación PassThrough de dominio, la autenticación con tarjeta inteligente y la autenticación PassThrough con tarjeta inteligente. La autenticación explícita está habilitada de forma predeterminada. Solo se puede configurar un método de autenticación para cada dirección URL de XenApp Services, y solo está disponible una dirección URL por almacén. Para habilitar varios métodos de autenticación, debe crear almacenes independientes, cada uno con una URL de XenApp Services, para cada método de autenticación. Los usuarios deben conectarse al almacén adecuado para su método de autenticación. Para obtener más información, consulte Autenticación basada en XML.
- El control del espacio de trabajo está habilitado de forma predeterminada para las direcciones URL de XenApp Services y no se puede configurar ni inhabilitar.
- Las solicitudes de los usuarios para cambiar sus contraseñas se dirigen al controlador de dominio directamente a través de servidores Citrix Virtual Apps and Desktops que proporcionan

escritorios y aplicaciones para el almacén. De esta forma, se omite el servicio de autenticación de StoreFront.

Requisitos del sistema

April 17, 2024

Antes de instalar StoreFront, consulte Planificar la implementación de StoreFront.

Requisitos del servidor de StoreFront

Después de las pruebas pertinentes, Citrix admite las instalaciones de StoreFront en las siguientes plataformas:

- Windows Server 2022 ediciones Datacenter y Standard
- Windows Server 2019 ediciones Datacenter y Standard
- Windows Server 2016 ediciones Datacenter y Standard

> **Nota:**
>
> StoreFront requiere la experiencia de escritorio de Windows, por lo que no se puede instalar en Windows Server Core.

Todos los servidores de StoreFront de un grupo de servidores deben usar la misma versión del sistema operativo, idioma y configuración regional.

No se admite la actualización de versiones de los sistemas operativos en un servidor con StoreFront. Citrix recomienda instalar StoreFront en una instalación limpia del sistema operativo.

Los servidores de Storefront deben cumplir estos requisitos mínimos, además de los requisitos del sistema operativo:

- Procesador: 2 CPU virtuales
- RAM: 4 GB, más 700 bytes por recurso disponible y por usuario.
- Almacenamiento:
  - 250 MB para StoreFront.
  - 30 MB para cada almacén, suponiendo un sitio web por almacén.
  - Por cada almacén que tenga los favoritos habilitados, 5 MB más 8 MB por cada 1000 favoritos.

  - Espacio suficiente para los archivos de registros de IIS según sus necesidades. Consulte la documentación de Microsoft sobre la administración del almacenamiento de archivos de registros de IIS.
  - Espacio suficiente para los registros de diagnóstico de StoreFront. De forma predeterminada, StoreFront 2311 y las versiones posteriores mantienen 1 GB de registros por servicio. Una implementación de StoreFront suele tener 1 servicio de roaming y 3 servicios por almacén (servicio de almacén, servicio de autenticación y servicio Receiver para Web). Consulte Solucionar problemas de StoreFront.

Antes de poder instalar StoreFront, las siguientes funciones de Windows deben estar habilitadas en el servidor web. Estos componentes están habilitados de forma predeterminada en una nueva instalación de Windows, por lo que no es necesario realizar ninguna acción a menos que se hayan desinstalado explícitamente.

- NET-Framework-45-Features
  - NET-Framework-45-Core
- PowerShellRoot
  - PowerShell

Si la versión de .NET Framework instalada es anterior a 4.7.2, el instalador instalará automáticamente .NET Framework 4.7.2. Tenga en cuenta que esto requiere que la funcionalidad NET-Framework-45-Core de Windows ya esté instalada.

Si el instalador de StoreFront detecta que falta alguna de las siguientes funciones de Windows, se instalará automáticamente:

- Web-Server
  - Web-WebServer
    - Web-Common-Http
      - Web-Default-Doc
      - Web-Http-Errors
      - Web-Static-Content
      - Web-Http-Redirect
    - Web-Health
      - Web-Http-Logging
    - Web-Security
      - Web-Filtering
      - Web-Basic-Auth
      - Web-Windows-Auth

    - Web-App-Dev
        - Web-Net-Ext45
        - Web-AppInit
        - Web-Asp-Net45
        - Web-ISAPI-Ext
        - Web-ISAPI-Filter
    - Web-Mgmt-Tools
        - Web-Mgmt-Console
    - Web-Scripting-Tools

- NET-Framework-45-Features
  - NET-Framework-45-ASPNET
  - NET-WCF-Services45
    - NET-WCF-TCP-PortSharing45

Es posible mover el sitio web de IIS a un directorio o unidad diferente antes de instalar StoreFront. La ruta relativa a StoreFront en IIS debe ser la misma para todos los servidores de un grupo de servidores.

StoreFront utiliza los siguientes puertos para comunicarse. Asegúrese de que los firewalls y otros dispositivos de red permitan el acceso a estos puertos.

- Los puertos TCP 80 o 443 se usan para comunicaciones HTTP y HTTPS respectivamente, y deben ser accesibles tanto desde dentro como desde fuera de la red corporativa.
- El puerto TCP 808 se usa para las comunicaciones entre los servidores StoreFront de un grupo de servidores.
- Para las comunicaciones entre los servidores de StoreFront en un grupo de servidores se usa un puerto TCP, seleccionado de forma aleatoria de entre todos los puertos no reservados. Al instalar StoreFront, se configura una regla del Firewall de Windows para habilitar el acceso al ejecutable de StoreFront. Sin embargo, puesto que el puerto se asigna de forma aleatoria, debe asegurarse de que los firewalls u otros dispositivos de la red interna no bloqueen el tráfico a ninguno de los puertos TCP que no estén asignados.
- La aplicación Citrix Workspace para HTML5 y otras versiones admitidas de la aplicación Citrix Workspace utilizan el puerto TCP 8008, cuando está habilitado, para la comunicación de los usuarios locales de la red interna con los servidores que suministran sus escritorios y aplicaciones.

StoreFront admite tanto entornos de solo IPv6 como entornos de doble pila de IPv4/IPv6.

Almacenar datos de suscripción mediante Microsoft SQL Server

Si quiere, puede almacenar datos de suscripción mediante microsoft SQL Server. StoreFront admite las mismas versiones de Microsoft SQL Server para esto que Citrix Virtual Apps and Desktops para bases de datos. En los requisitos del sistema de Citrix Virtual Apps and Desktops, consulte Bases de datos.

Requisitos de infraestructura

Después de las pruebas pertinentes, Citrix admite StoreFront cuando se usa con las siguientes versiones de productos Citrix.

Citrix Virtual Apps and Desktops

StoreFront admite las siguientes versiones de Citrix Virtual Apps and Desktops:

- Citrix Virtual Apps and Desktops 2311
- Citrix Virtual Apps and Desktops 2308
- Citrix Virtual Apps and Desktops 2305
- Citrix Virtual Apps and Desktops 2203 LTSR
- Citrix Virtual Apps and Desktops 1912 LTSR

Citrix Gateway

Se pueden usar estas versiones de Citrix Gateway para proporcionar acceso a StoreFront para los usuarios de redes públicas.

- Citrix Gateway 14.1
- Citrix Gateway 13.1
- Citrix Gateway 13.0

Es posible establecer conexiones a través de Citrix Gateway mediante el proxy ICA, el plug-in de Citrix Gateway o la red VPN sin cliente (cVPN).

Requisitos del dispositivo del usuario

StoreFront ofrece varias opciones para que los usuarios accedan a sus escritorios y aplicaciones. Los usuarios de Citrix pueden acceder a almacenes a través de la aplicación Citrix Workspace instalada localmente o utilizar la aplicación Citrix Workspace para HTML5 en su explorador web.

Aplicación Citrix Workspace instalada localmente

Puede usar todas las versiones admitidas actualmente de la aplicación Citrix Workspace para acceder a los almacenes de StoreFront desde conexiones de red internas o mediante Citrix Gateway. Para conocer las fechas de los ciclos de vida de la aplicación Citrix Workspace, consulte https://www.citrix.com/support/product-lifecycle/workspace-app.html.

Aplicación Citrix Workspace para HTML5 en un explorador web

Puede usar la aplicación Citrix Workspace para HTML5 para acceder a su almacén mediante un explorador web. Las aplicaciones y los escritorios se pueden iniciar mediante una aplicación Citrix Workspace instalada de forma nativa (lo que se conoce como inicio híbrido) o desde el explorador web. Según la configuración de su sitio web, los usuarios finales pueden elegir cualquiera de los dos métodos de inicio de recursos.

Use las versiones más recientes de los siguientes exploradores web.

En Windows:

- Microsoft Edge
- Google Chrome
- Mozilla Firefox
- Internet Explorer 11: Solo para navegar por el almacén, no para conectarse a recursos.

En Mac:

- Safari
- Google Chrome
- Mozilla Firefox

En Linux:

- Google Chrome
- Mozilla Firefox

Para obtener más información sobre los requisitos para usar la aplicación Citrix Workspace para HTML5 para conectarse a los recursos a través de un explorador web, consulte la documentación de la aplicación Citrix Workspace para HTML5.

Dispositivos antiguos

Los clientes de productos antiguos de Citrix pueden usar direcciones URL de XenApp Services para acceder a almacenes de StoreFront con una funcionalidad reducida. Las direcciones URL de XenApp

Services ofrecen retrocompatibilidad con versiones anteriores para las conexiones realizadas por Citrix Receiver 3.4 Enterprise y clientes más antiguos. Esta funcionalidad está obsoleta y se retirará en una versión futura.

Requisitos de tarjetas inteligentes

Uso de la aplicación Citrix Workspace con tarjetas inteligentes

Citrix hace pruebas de compatibilidad con tarjetas Common Access Card (CAC) del departamento de Defensa del Gobierno de los Estados Unidos, NIST PIV (Personal Identity Verification) del National Institute of Standards and Technology de Estados Unidos y con tokens de tarjeta inteligente USB. Puede usar los lectores de tarjeta con contacto que cumplen la especificación de los dispositivos de interfaz de tarjeta inteligente / de chip USB (CCID), que Zentraler Kreditausschuss (ZKA) clasifica como lectores de tarjetas inteligentes de Clase 1. Los lectores de tarjeta con contacto de Clase 1 de ZKA requieren que los usuarios inserten sus tarjetas inteligentes en el lector. No se admiten otros tipos de lectores de tarjetas inteligentes, incluidos los lectores de Clase 2 (que tienen teclados numéricos para escribir los PIN), los lectores de tarjetas sin contacto y las tarjetas inteligentes virtuales basadas en chips del Módulo de plataforma segura (TPM).

Para los dispositivos Windows, la compatibilidad con tarjetas inteligentes se basa en las especificaciones estándar PC/SC de Microsoft. Como requisito mínimo, las tarjetas inteligentes y los lectores de tarjetas deben ser admitidos por el sistema operativo y haber recibido la Certificación de hardware en Windows.

Para obtener más información acerca de tarjetas inteligentes y middleware compatibles con Citrix, consulte Tarjetas inteligentes en la documentación de Citrix Virtual Apps and Desktops, y http://www.citrix.com/ready.

Requisitos de Citrix Analytics Service

Puede configurar Citrix StoreFront para que la aplicación Citrix Workspace pueda enviar datos a Citrix Analytics Service. Los detalles de configuración se describen en Citrix Analytics Service. Esta funcionalidad se admite en los casos siguientes:

- Almacenes a los que se accede mediante exploradores web.
- Almacenes a los que se accede desde la versión 1903 de la aplicación Citrix Workspace para Windows o una versión posterior.
- Almacenes a los que se accede desde la versión 1901 de la aplicación Citrix Workspace para Linux o una versión posterior.

Instalar StoreFront

December 4, 2023

Antes de instalar y configurar

Para instalar y configurar StoreFront, siga estos pasos en el orden indicado.

1. Consulte los requisitos del sistema.
2. Si quiere utilizar StoreFront para entregar recursos de Citrix Virtual Apps and Desktops a los usuarios, compruebe que el servidor de StoreFront está unido al dominio de Microsoft Active Directory que contiene las cuentas de los usuarios o a un dominio que tiene una relación de confianza con el dominio de las cuentas de usuario.

   > **Importante:**
   >
   > - En implementaciones de servidor único, puede instalar StoreFront en un servidor que no esté unido a ningún dominio.
   > - StoreFront no se puede instalar en un controlador de dominio.

3. Si, además, piensa configurar una implementación de StoreFront con varios servidores, configure un entorno de equilibrio de carga para los servidores de StoreFront.

   Para utilizar NetScaler ADC para el equilibrio de carga, defina un servidor virtual como proxy de los servidores StoreFront. Para obtener más información sobre cómo configurar NetScaler ADC para el equilibrio de carga, consulte Equilibrar la carga con NetScaler ADC.

4. Asegúrese de que los firewalls y otros dispositivos de red permiten el acceso a los puertos TCP 80 o 443, según corresponda, desde dentro y fuera de la red corporativa. Además, asegúrese de que ni los firewalls ni otros dispositivos de la red interna bloqueen el tráfico a los puertos TCP no asignados.

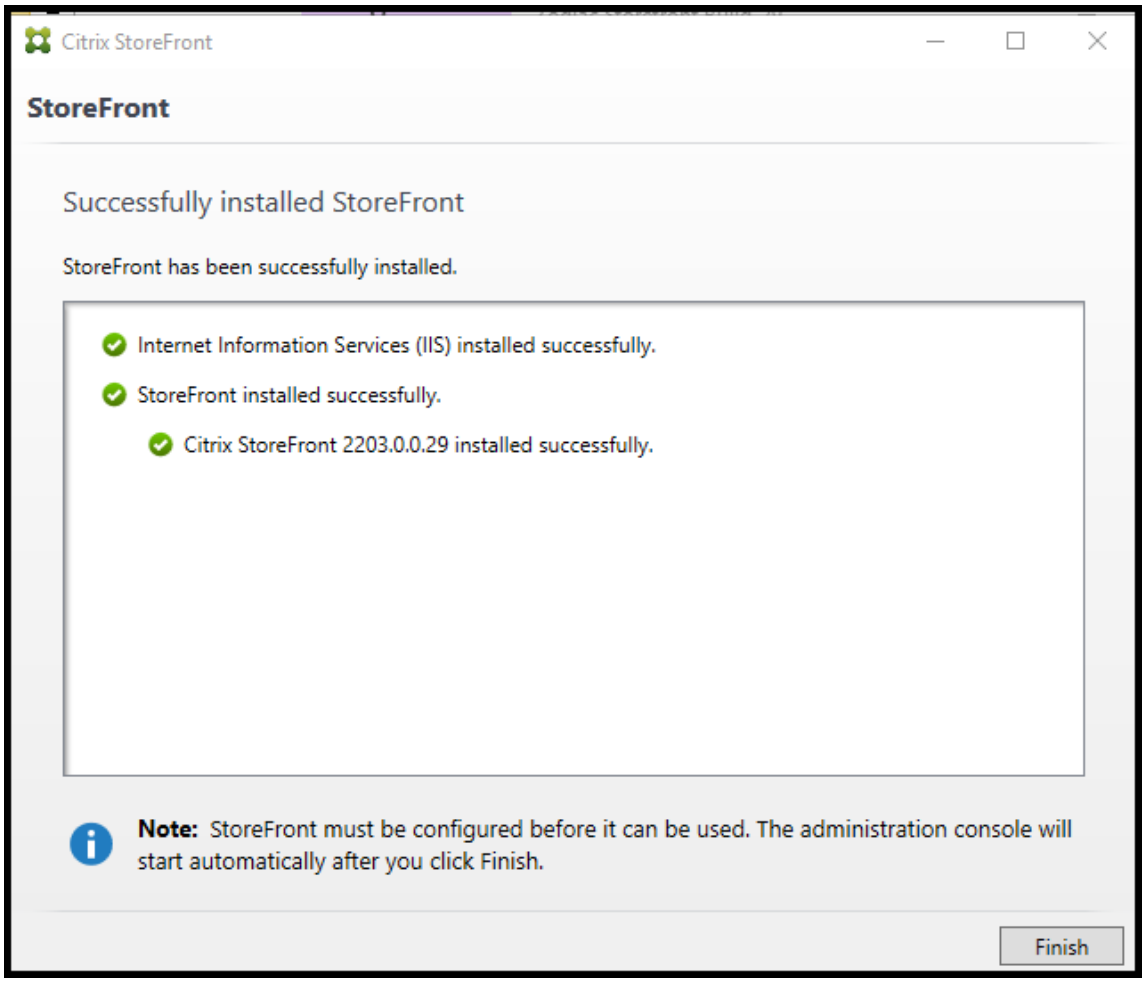
   Al instalar StoreFront, se configura una regla del Firewall de Windows. Esta regla habilita el acceso al archivo ejecutable de StoreFront a través de un puerto TCP aleatorio seleccionado de los puertos no reservados. Este puerto se utiliza para comunicaciones entre los servidores de StoreFront en un grupo de servidores.

Instalar StoreFront

> **Importante**
>
> Para evitar posibles errores y la pérdida de datos durante la instalación de StoreFront, asegúrese

> de que todas las aplicaciones están cerradas y de que no hay otras tareas u operaciones ejecutándose en el sistema de destino.

1. Descargue el programa de instalación desde la página de descarga.
2. Inicie sesión en el servidor de StoreFront con una cuenta con permisos de administrador local.
3. Busque CitrixStoreFront-x64.exe y ejecute el archivo como administrador.
4. Lea y acepte el contrato de licencia. A continuación, haga clic en **Siguiente**.
5. Si aparece la página Revisar requisitos previos, haga clic en **Siguiente**.
6. En la página Listo para instalar, consulte los requisitos previos y los componentes de StoreFront que se van a instalar y haga clic en **Instalar**.
7. Cuando termine la instalación, haga clic en **Finalizar**.



8. Es posible que StoreFront solicite el reinicio para completar la instalación. Haga clic en **Sí** para reiniciar en el momento.
9. Configure Microsoft Internet Information Services (IIS) para HTTPS. Para ver los pasos, consulte Proteger StoreFront con HTTPS.

Para instalar StoreFront desde un símbolo del sistema

1. Inicie sesión en el servidor de StoreFront con una cuenta con permisos de administrador local.
2. Asegúrese de que se cumplan los requisitos para la instalación de StoreFront antes de instalar StoreFront. Para obtener información más detallada, consulte Antes de instalar y configurar.
3. En los medios de instalación o el paquete de descarga, busque CitrixStoreFront-x64.exe y copie el archivo a una ubicación temporal en el servidor.
4. En un símbolo del sistema, vaya a la carpeta que contiene el archivo de instalación y escriba el siguiente comando.

```
CitrixStoreFront-x64.exe [-silent] [-INSTALLDIR
    installationlocation] [-WINDOWS_CLIENT filelocation\filename.
    exe] [-MAC_CLIENT filelocation\filename.dmg]
<!--NeedCopy-->
```

   Utilice el argumento **-silent** para realizar una instalación silenciosa de StoreFront y todos los requisitos previos. De forma predeterminada, StoreFront se instala en C:\Archivos de programa\Citrix\Receiver StoreFront. No obstante, puede especificar otra ubicación de instalación con el argumento **-INSTALLDIR**, donde *installationlocation* es el directorio en el que se instalará StoreFront. Si quiere que el servidor forme parte de un grupo de servidores, la ubicación de la instalación de StoreFront y los parámetros del sitio web de IIS, la ruta física y los ID del sitio deben ser idénticos en todos los servidores del grupo.

   Cuando un usuario abre un almacén en un explorador web en Windows o macOS, de forma predeterminada, si no puede detectar la aplicación Citrix Workspace, pide al usuario que descargue e instale la aplicación Citrix Workspace adecuada para su plataforma desde el sitio web de Citrix. Puede modificar este comportamiento para que los usuarios puedan descargarse los archivos de instalación de la aplicación Citrix Workspace desde el servidor de StoreFront. Para obtener más información, consulte Configurar cómo se muestran los recursos a los usuarios.

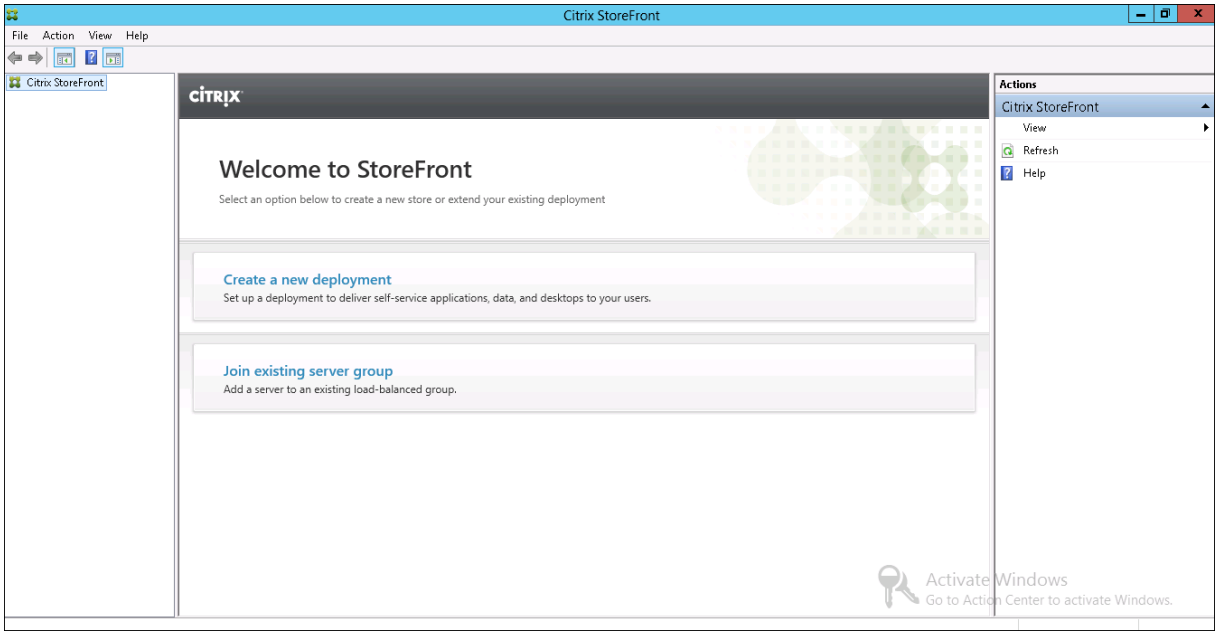
   Si va a cambiar esta configuración, especifique los argumentos **-WINDOWS_CLIENT** y **-MAC_CLIENT** para copiar los archivos de instalación de Citrix Receiver para Windows o la aplicación Citrix Workspace para Windows y Citrix Receiver para Mac o la aplicación Citrix Workspace para Mac, respectivamente, a la ubicación adecuada en la implementación de StoreFront. Reemplace *filelocation* por el directorio que contiene el archivo de instalación a copiar y *filename* por el nombre del archivo de instalación. Los archivos de la aplicación Citrix Workspace para Windows y Citrix Receiver para Mac o de la aplicación Citrix Workspace para Mac se incluyen en los medios de instalación de Citrix Virtual Apps and Desktops.

Registros de la instalación

Para obtener más información sobre los archivos de registro, consulte Registros de instalación.

Configurar StoreFront

Al finalizar la instalación, la consola de administración de Citrix StoreFront se inicia automáticamente. También puede abrir StoreFront desde el menú Inicio. Cuando la consola de administración de Citrix StoreFront se inicia por primera vez, existen dos opciones disponibles.



- Cree una implementación. Configure el primer servidor de una nueva implementación de StoreFront. Las implementaciones de un servidor único son idóneas para la evaluación de StoreFront o para implementaciones pequeñas de producción. Después de configurar el primer servidor de StoreFront, puede agregar más servidores al grupo en cualquier momento para aumentar la capacidad de la implementación.
- Incorporarse a un grupo existente de servidores. Agregue otro servidor a una implementación existente de StoreFront. Seleccione esta opción para aumentar rápidamente la capacidad de la implementación de StoreFront. Se necesita equilibrio de carga externo para las implementaciones con varios servidores. Para agregar un servidor, necesita acceso a un servidor existente de la implementación.

Ahora, los usuarios pueden acceder a su almacén a través de un explorador web o de la aplicación Citrix Workspace. Consulte la Guía para usuarios.

Customer Experience Improvement Program (CEIP) de Citrix

January 26, 2024

Si se participa en el programa CEIP de mejora de la experiencia del usuario (Customer Experience Improvement Program), se envían estadísticas e información de uso anónimos a Citrix para mejorar la calidad y el rendimiento de sus productos.

De forma predeterminada, se inscribe automáticamente en el programa CEIP cuando instala StoreFront. La primera carga de datos tiene lugar aproximadamente siete días después de instalar StoreFront. Puede cambiar esta opción predeterminada en el parámetro de Registro del sistema. Si cambia el parámetro de Registro del sistema antes de instalar StoreFront, se usará ese valor. Si cambia el parámetro de Registro del sistema antes de actualizar la versión de StoreFront, se usará ese valor.

> **Advertencia:**
>
> Si se modifica el Registro de forma incorrecta, pueden producirse problemas graves que obliguen a reinstalar el sistema operativo. Citrix no puede garantizar que los problemas derivados del uso inadecuado del Editor del Registro puedan resolverse. Si usa el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

El parámetro de Registro que controla la carga automática de los datos de análisis (predeterminado = 1):

```
Location: HKLM:\Software\Citrix\Telemetry\CEIP
Name: Enabled
Type: REG_DWORD
Value: 0 = disabled, 1 = enabled
<!--NeedCopy-->
```

De forma predeterminada, la propiedad **Enabled** está oculta en el registro. Si no se especifica, significa que la funcionalidad de carga automática está habilitada.

Con PowerShell, el cmdlet siguiente inhabilita la inscripción en el programa CEIP:

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\Telemetry\CEIP -Name
Enabled -PropertyType DWORD -Value 0
```

> **Nota:**
>
> El parámetro de Registro controla la carga automática de información anónima de uso y estadísticas para todos los componentes en el mismo servidor. Por ejemplo, si ha instalado StoreFront en el mismo servidor que el Delivery Controller y decide no participar en el programa CEIP mediante el parámetro de Registro, la ausencia de participación se aplicará a ambos componentes.

Datos de CEIP recopilados desde StoreFront

La siguiente tabla ofrece ejemplos del tipo de información anónima que se recopila. Los datos no contienen detalles que lo identifiquen a usted como cliente.

Datos	Descripción
Versión de StoreFront	Cadena que indica la versión instalada de StoreFront. Por ejemplo, “3.8.0.0”
Recuento de almacenes	Un contador de la cantidad de almacenes que hay en la implementación.
Recuento de servidores en el grupo de servidores	Un contador de la cantidad de servidores que hay en el grupo de servidores.
Recuento de Delivery Controllers por almacén	Lista de valores numéricos que indican la cantidad de Delivery Controllers disponibles para cada almacén que haya en la implementación.
HTTPS habilitado	Cadena que indica si HTTPS (“True”o “False”) está habilitado para la implementación.
Parámetro de HTML5 para Citrix Receiver para web	Lista de las cadenas de texto que indican el parámetro de HTML5 de cada Receiver para web.
Control del espacio de trabajo habilitado para la aplicación Citrix Workspace/Citrix Receiver	Lista de valores booleanos que indican si el “Control del espacio de trabajo”está habilitado (“True”o “False”) en cada sitio de Receiver para web.
Acceso remoto habilitado en el almacén	Lista de las cadenas de texto que indican si el “Acceso remoto”está habilitado (“HABILITADO”o “INHABILITADO”) para cada almacén que haya en la implementación.
Recuento de puertas de enlace	Un contador de la cantidad de puertas de enlace Citrix Gateway configuradas en la implementación.

Citrix Analytics Service

January 26, 2024

Si es cliente de Monitor y tiene una implementación local de StoreFront, puede configurar StoreFront para que los datos se envíen a Citrix Analytics Service en Monitor. Al configurarse, la aplicación Citrix Workspace y los exploradores web envían eventos de usuario a Citrix Analytics para su procesamiento. Citrix Analytics recoge y agrupa métricas de usuarios, aplicaciones, dispositivos de punto final, redes y datos para proporcionar información completa sobre el comportamiento de los usuarios. Para

obtener información sobre esta función en la documentación de Citrix Analytics, consulte Incorporar sitios de Virtual Apps and Desktops mediante StoreFront.

Para configurar este comportamiento:

- Descargue un archivo de configuración de Citrix Analytics.
- Importe datos de Citrix Analytics en la implementación local de StoreFront mediante PowerShell.

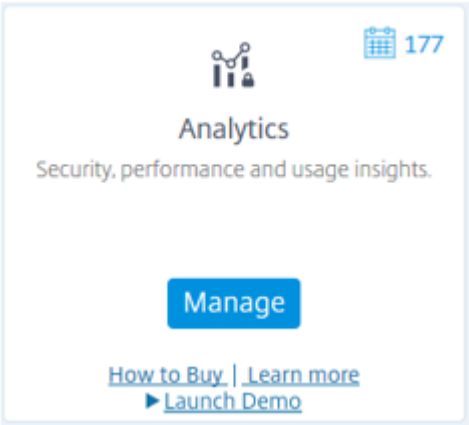
Una vez configurado StoreFront, la aplicación Citrix Workspace puede enviar datos desde almacenes StoreFront cuando Citrix Analytics Service lo solicite.

> **Importante:**
>
> La implementación de StoreFront debe poder contactar con las siguientes direcciones en el puerto 443 para que esta función funcione correctamente y consuma los servicios de Monitor:
>
> - `https://*.cloud.com`
> - `https://*.citrixdata.com`

Descargue el archivo de configuración de Citrix Analytics

> **Importante:**
>
> Se requiere un archivo de configuración que contiene información confidencial para la configuración inicial. Mantenga el archivo seguro después de la descarga. No comparta este archivo con nadie fuera de su organización. Después de la configuración, puede eliminar este archivo. Si necesita volver a aplicar la configuración en otro equipo, puede descargar el archivo de nuevo desde la consola de administración de Citrix Analytics Service.

1. Inicie sesión en Monitor (`https://citrix.cloud.com/`) con una cuenta de administrador.
2. Seleccione un cliente de Monitor.
3. Para abrir la consola de administración de servicios de Citrix Analytics, haga clic en **Administrar**.



4. En la consola de administración de servicios de Citrix Analytics, seleccione **Settings > Data Sources**.
5. En la tarjeta Virtual Apps and Desktops, seleccione el icono de menú (⊠) y, luego, **Connect StoreFront deployment**.
6. En la página Connect StoreFront Deployment, seleccione **Download File** para descargar el archivo *StoreFrontConfigurationFile.json*.

Archivo de configuración de ejemplo

```
{

  "customerId": "<yourcloudcustomer>",
  "enablementService": " https://api.analytics.cloud.com /casvc/<
     yourcloudcustomer>/ctxana/v1/cas/<yourcloudcustomer>/XenDesktop/<
     deviceid>/dsconfigdata",
  "cwsServiceKey": "PFJTPn…… .. T4=",
  "enablementServiceStatus": " https://api.analytics.cloud.com /casvc/<
     yourcloudcustomer>/ctxana/v1/cas/storefront/config",
  "instanceId": "d98f21d0-56e0-11e9-ba52-5136d90862fe",
  "name": "CASSingleTenant"
 }

<!--NeedCopy-->
```

donde

customerId es el identificador único del cliente actual de Monitor.

cwsServiceKey es una clave única que identifica la cuenta de cliente actual de Monitor.

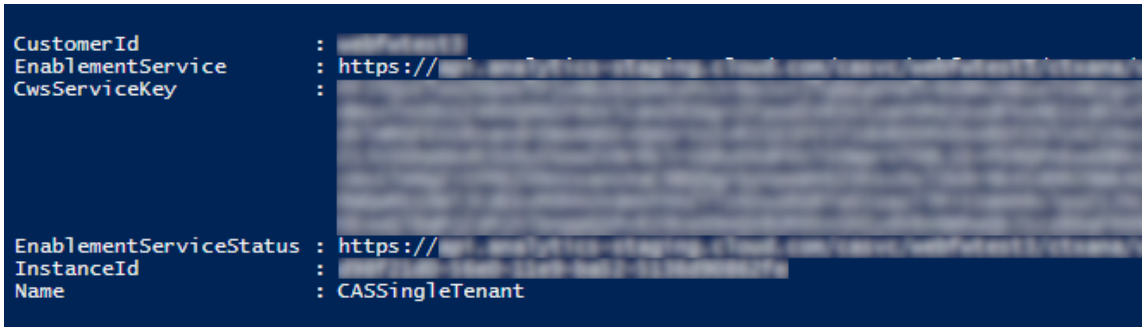
instanceID es un ID generado que se utiliza para firmar (proteger) las solicitudes realizadas desde la aplicación Citrix Workspace para Citrix Analytics. Si registra varios servidores o grupos de servidores de StoreFront con Monitor, cada uno tiene un instanceID único.

Importar datos de Citrix Analytics en su implementación de StoreFront

1. Copie el archivo *StoreFrontConfigurationFile.json* en una carpeta adecuada del servidor local de StoreFront (o en un servidor de un grupo de servidores de StoreFront). Los siguientes comandos dan por supuesto que el archivo se guarda en el escritorio.
2. Abra PowerShell ISE y seleccione **Ejecutar como administrador**.
3. Ejecute los comandos siguientes:

```
Import-STFCasConfiguration -Path "$Env:UserProfile\Desktop\
    StoreFrontConfigurationFile.json"
Get-STFCasConfiguration
<!--NeedCopy-->
```

4. Este comando devuelve una copia de los datos importados y los muestra en la consola de PowerShell.



> **Nota:**
>
> Los servidores locales de StoreFront, que están instalados en Windows Server 2012 R2, pueden requerir que los componentes de software del runtime de C++ se instalen manualmente para que puedan registrarse con el servicio CAS. Si StoreFront se instala durante la instalación de Citrix Virtual Apps and Desktops, este paso no es necesario porque el metainstalador de CVAD ya instala los componentes del runtime de C++. Si StoreFront se instala solamente con el metainstalador CitrixStoreFront-x64.exe y sin el runtime de C++, es posible que no se registre con Monitor después de importar el archivo de configuración del servicio CAS.

Propagar datos de Citrix Analytics en un grupo de servidores de StoreFront

Si realiza estas acciones en un grupo de servidores de StoreFront, debe propagar los datos importados de Citrix Analytics en todos los miembros del grupo de servidores. Este paso no es necesario en implementaciones con un solo servidor de StoreFront.

Para propagar los datos, utilice uno de los siguientes métodos:

- Utilice la consola de administración de StoreFront.

- Utilice el cmdlet de PowerShell **Publish-STFServerGroupConfiguration**.

Comprobar el ID del grupo de servidores de StoreFront

Para comprobar si la implementación se ha registrado correctamente en Citrix Analytics Service, puede usar PowerShell para detectar ServerGroupID en la implementación.

1. Inicie sesión en el servidor de StoreFront o en un servidor de StoreFront del grupo de servidores.
2. Abra PowerShell ISE y seleccione **Ejecutar como administrador**.
3. Ejecute los comandos siguientes:

```
$WebConfigPath = "C:\Program Files\Citrix\Receiver StoreFront\
    Framework\FrameworkData\Framework.xml"
$XMLObject = (Get-Content $WebConfigPath) -as [Xml]
$XMLObject.framework.properties.property
<!--NeedCopy-->
```

Por ejemplo, estos comandos generan resultados como los siguientes:

```
name value
---- -----
ClusterId 8b8ff5c8-44ba-46e4-87f0-2df8cff31432
HostBaseUrl https://storefront.example.com/
SelectedIISWebSiteId 1
AdminConsoleOperationMode Full
<!--NeedCopy-->
```

Dejar de enviar datos a Citrix Analytics desde StoreFront

1. Abra PowerShell ISE y seleccione **Ejecutar como administrador**.
2. Ejecute los comandos siguientes:

   `Remove-STFCasConfiguration`

   `Get-STFCasConfiguration`

   Get-STFCasConfiguration no devuelve nada si los datos importados anteriormente de Citrix Analytics se han eliminado correctamente.

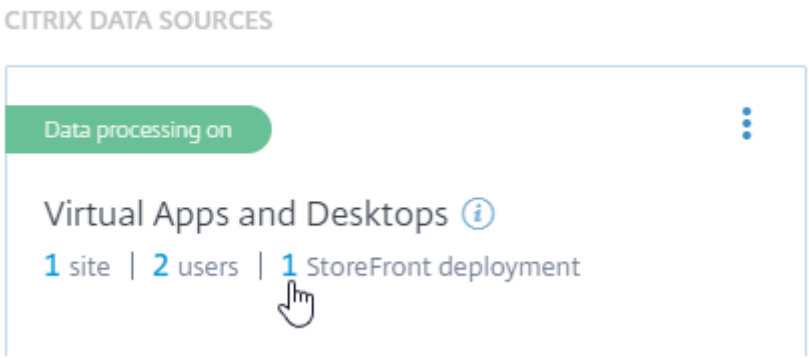
3. Si realiza estas acciones en un grupo de servidores de StoreFront, propague el cambio y elimine los datos importados de Citrix Analytics de todos los miembros del grupo de servidores. En un servidor del grupo de servidores, ejecute el siguiente comando:

   `Publish-STFServerGroupConfiguration`

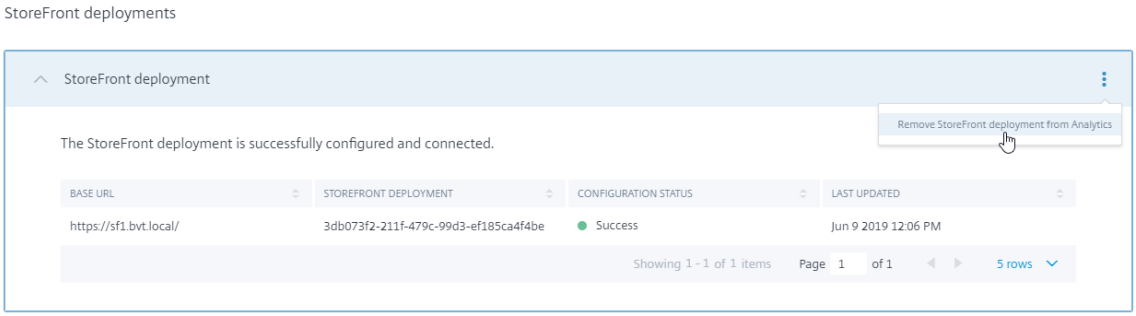
4. En cualquier otro miembro del grupo de servidores, ejecute el siguiente comando para confirmar que la configuración de Citrix Analytics se ha eliminado correctamente de todos los servidores del grupo:

   ```
   Get-STFCasConfiguration
   ```

5. Inicie sesión en Monitor (`https://citrix.cloud.com/`) con una cuenta de administrador.
6. Seleccione un cliente de Monitor.
7. Para abrir la consola de administración de servicios de Citrix Analytics, haga clic en **Administrar**.
8. En la consola de administración de servicios de Citrix Analytics, seleccione **Settings > Data Sources**.
9. En la tarjeta Virtual Apps and Desktops, seleccione el recuento de implementaciones de StoreFront.



10. Para identificar la implementación de StoreFront que quiere eliminar, haga referencia a la URL base de su host y a ServerGroupID.
11. En el menú (⋮), seleccione **Remove StoreFront deployment from Analytics**.



> **Nota:**
>
> Si quita la configuración del servidor, pero no de Citrix Analytics, la entrada de la implementación de StoreFront permanece en Citrix Analytics, pero no recibe datos de StoreFront.

> Si quita la configuración solamente de Citrix Analytics, la entrada de la implementación de StoreFront se vuelve a agregar en el siguiente reciclaje del grupo de aplicaciones (tiene lugar al restablecer IIS o automáticamente cada 24 horas).

Configurar StoreFront para que use un proxy web para contactar con Monitor y registrarse con Citrix Analytics

Si StoreFront se coloca en un servidor web host detrás de un proxy web, ocurrirá un error en el registro con Citrix Analytics. Si los administradores de StoreFront utilizan un proxy HTTP en su implementación de Citrix, el tráfico de StoreFront asociado a Internet debe pasar a través del proxy web antes de que llegue a Citrix Analytics en la nube. StoreFront no utiliza automáticamente la configuración de proxy del SO de alojamiento; se requiere una configuración adicional para indicar al almacén que envíe el tráfico saliente a través del proxy web. Puede establecer una configuración de proxy `<system.net>` agregando una nueva sección al archivo web.config del almacén. Haga esto para cada almacén del servidor de StoreFront que se utilice para enviar datos a Citrix Analytics.

Método 1: Establecer la configuración del proxy del almacén a través de PowerShell para uno o varios almacenes (recomendado)

La ejecución del script de PowerShell Config-StoreProxy.ps1 automatiza este proceso para uno o varios almacenes e inserta automáticamente XML válido para configurar `<system.net>`. El script también realiza una copia de seguridad del archivo web.config del almacén en el escritorio del usuario actual, para permitir restaurar el archivo web.config no modificado si es necesario.

> **Nota:**
>
> Ejecutar el script más de una vez puede dar lugar a que se agreguen varias copias del código XML de `<system.net`. Cada almacén solo debe tener una entrada para `<system.net>`. Agregar varias copias impide que la configuración del proxy de almacén funcione correctamente.

1. Abra PowerShell ISE y seleccione **Ejecutar como administrador**.
2. Configure `$Stores = @("Store","Store2")` para que incluya los almacenes que quiere configurar con un proxy web.
3. Especifique:
   - Una dirección IP
   - O un nombre de dominio completo (FQDN) para el proxy web
4. Ejecute el siguiente comando de PowerShell:

```
1 $Stores = @("Store","Store2")
2 $ProxyIP = "10.0.0.1"
```



```
3  $ProxyFQDN = "proxyserver.example.com"
4  $ProxyPort = 8888
5
6  # Set this for every Store using Stores array
7  function Set-StoreProxyServer() # Tested with both IP and FQDN
8  {
9
10     [CmdletBinding()]
11     param([Parameter(Mandatory=$true,ParameterSetName="ProxyIP")][
           Parameter(Mandatory=$true,ParameterSetName="ProxyFQDN")][
           array]$Stores,
12         [Parameter(Mandatory=$true,ParameterSetName="ProxyIP")][
               string]$ProxyIP,
13         [Parameter(Mandatory=$true,ParameterSetName="ProxyFQDN")][
               string]$ProxyFQDN,
14         [Parameter(Mandatory=$true,ParameterSetName="ProxyIP")][
               Parameter(Mandatory=$true,ParameterSetName="ProxyFQDN")
               ][int]$ProxyPort)
15
16     foreach($Store in $Stores)
17     {
18
19         Write-Host "Backing up the Store web.config file for store
                $Store before making changes..." -ForegroundColor "
               Yellow"
20         Write-Host "`n"
21
22         if(!(Test-Path "$env:UserProfile\desktop$Store"))
23         {
24
25             Write-Host "Creating $env:UserProfile\desktop$Store\
                   directory for backup..." -ForegroundColor "Yellow"
26             New-Item -Path "$env:UserProfile\desktop$Store" -
                   ItemType "Directory" | Out-Null
27             Write-Host "`n"
28          }
29
30
31         Write-Host "Copying c:\inetpub\wwwroot\Citrix$Store\web.
               config to $env:UserProfile\desktop$Store..." -
               ForegroundColor "Yellow"
32         Copy-Item -Path "c:\inetpub\wwwroot\Citrix$Store\web.
               config" -Destination "$env:UserProfile\desktop$Store" -
               Force | Out-Null
33
34         if(Test-Path "$env:UserProfile\desktop$Store\web.config")
35         {
36
37             Write-Host "$env:UserProfile\desktop$Store\web.config
                   file backed up" -ForegroundColor "Green"
38          }
39
40         else
```



```
41          {
42
43              Write-Host "$env:UserProfile\desktop$Store\web.config
                    file NOT found!" -ForegroundColor "Red"
44           }
45
46          Write-Host "`n"
47
48          Write-Host "Setting the proxy server to $ProxyAddress for
                Store $Store..." -ForegroundColor "Yellow"
49          Write-Host "`n"
50
51          $StoreConfigPath = "c:\inetpub\wwwroot\Citrix$Store\web.
                config"
52          $XMLObject = (Get-Content $StoreConfigPath) -as [Xml]
53
54          if([string]::IsNullOrEmpty($ProxyFQDN))
55          {
56
57              $ProxyServer = ("HTTP://$ProxyIP"+":"+$ProxyPort)
58           }
59
60          else
61          {
62
63              $ProxyServer = ("HTTP://$ProxyFQDN"+":"+$ProxyPort)
64           }
65
66
67          $XMLObject = (Get-Content $StoreConfigPath) -as [Xml]
68
69          # Create 3 elements
70          $SystemNet = $XMLObject.CreateNode("element","system.net",
                "")
71          $DefaultProxy = $XMLObject.CreateNode("element","
                defaultProxy","")
72          $Proxy = $XMLObject.CreateNode("element","proxy","")
73          $Proxy.SetAttribute("proxyaddress","$ProxyServer")
74          $Proxy.SetAttribute("bypassonlocal","true")
75
76          # Move back up the XML tree appending new child items in
                reverse order
77          $DefaultProxy.AppendChild($Proxy)
78          $SystemNet.AppendChild($DefaultProxy)
79          $XMLObject.configuration.AppendChild($SystemNet)
80
81          # Save the modified XML document to disk
82          $XMLObject.Save($StoreConfigPath)
83
84          Write-Host "Getting the proxy configuration for c:\inetpub
                \wwwroot\Citrix$Store..." -ForegroundColor "Yellow"
85          $XMLObject = (Get-Content $StoreConfigPath) -as [Xml]
86          $ConfiguredProxyServer = $XMLObject.configuration.'system.
```



```
                net'.defaultProxy.proxy.proxyaddress | Out-Null
            Write-Host ("Configured proxy server for Store $Store"+":
                "+ $ConfiguredProxyServer) -ForegroundColor "Green"
            Write-Host "`n"
        }

        Write-Host "Restarting IIS..." -ForegroundColor "Yellow"
        IISReset /RESTART
    }


Set-StoreProxyServer -Stores $Stores -ProxyFQDN $ProxyFQDN -
    ProxyPort $ProxyPort
# OR
Set-StoreProxyServer -Stores $Stores -ProxyIP $ProxyIP -ProxyPort
    $ProxyPort
<!--NeedCopy-->
```

5. Compruebe que C:\inetpub\wwwroot\Citrix\web.config contiene ahora una nueva sección “ al final del archivo web.config.

```
        </dependentAssembly>
    </assemblyBinding>
</runtime>
<system.net>
    <defaultProxy>
    <proxy proxyaddress="HTTP://proxyserver.example.com:8888"
        bypassonlocal="true" />
    </defaultProxy>
</system.net>
</configuration>
<!--NeedCopy-->
```

6. Importe los datos de Citrix Analytics como se describe en Importar datos de Citrix Analytics en su implementación de StoreFront.

Método 2: Agregar manualmente una sección `<system.net>` al archivo web.config del almacén

Esto se debe hacer para cada almacén del servidor de StoreFront que se utilice para enviar datos a Citrix Analytics.

1. Haga una copia de seguridad del archivo web.config del almacén y cópielo en otra ubicación, fuera de C:\inetpub\wwwroot\Citrix\web.config.
2. Modifique el siguiente XML con su configuración de proxy mediante una combinación de FQDN y puerto o mediante una combinación de IP y puerto.

   Por ejemplo, mediante una combinación de FQDN y puerto, utilice el siguiente elemento `<system.net>`:


```
<system.net>
    <defaultProxy>
    <proxy proxyaddress="HTTP://proxyserver.example.com:8888"
        bypassonlocal="true" />
    </defaultProxy>
</system.net>
<!--NeedCopy-->
```

Por ejemplo, mediante una combinación de IP y puerto, utilice el siguiente elemento `<system.net>`:

```
<system.net>
    <defaultProxy>
    <proxy proxyaddress="HTTP://10.0.0.1:8888" bypassonlocal="true
        " />
    </defaultProxy>
</system.net>
<!--NeedCopy-->
```

3. Al final del archivo web.config del almacén, inserte el elemento `<system.net>` apropiado donde se indica aquí:

```
<runtime>
<gcServer enabled="true" />
<assemblyBinding xmlns="urn:schemas-microsoft-com:asm.v1">
    <dependentAssembly>
    <assemblyIdentity name="System.Web.MVC" publicKeyToken="31
        BF3856AD364E35" culture="neutral" />
    <bindingRedirect oldVersion="0.0.0.0-5.0.0.0" newVersion="
        5.0.0.0" />
    </dependentAssembly>
    <dependentAssembly>
    <assemblyIdentity name="Newtonsoft.Json" publicKeyToken="30
        ad4fe6b2a6aeed" culture="neutral" />
    <bindingRedirect oldVersion="0.0.0.0-9.0.0.0" newVersion="
        9.0.0.0" />
    </dependentAssembly>
</assemblyBinding>
</runtime>

Insert the <system.net> element here

</configuration>
<!--NeedCopy-->
```

4. Importe los datos de Citrix Analytics como se describe en Importar datos de Citrix Analytics en su implementación de StoreFront.

Protección de StoreFront con HTTPS

April 17, 2024

Citrix recomienda encarecidamente proteger la comunicación entre los dispositivos de los usuarios y StoreFront mediante HTTPS. Esto garantiza el cifrado de contraseñas y otros datos que se envíen entre el cliente y StoreFront. Además, las conexiones HTTP simples pueden verse comprometidas por varios ataques, como los ataques del tipo "Man in the middle", especialmente cuando las conexiones se realizan desde ubicaciones no seguras, como puntos de acceso Wi-Fi públicos. Sin una configuración de IIS adecuada, StoreFront utiliza HTTP para las comunicaciones.

Según la configuración, los usuarios pueden acceder a StoreFront a través de una puerta de enlace o un equilibrador de carga. Puede cerrar la conexión HTTPS en la puerta de enlace o en el equilibrador de carga. Sin embargo, en este caso, Citrix sigue recomendando proteger las conexiones entre la puerta de enlace y StoreFront mediante HTTPS.

Si StoreFront no está configurado para HTTPS, aparecerá esta advertencia:

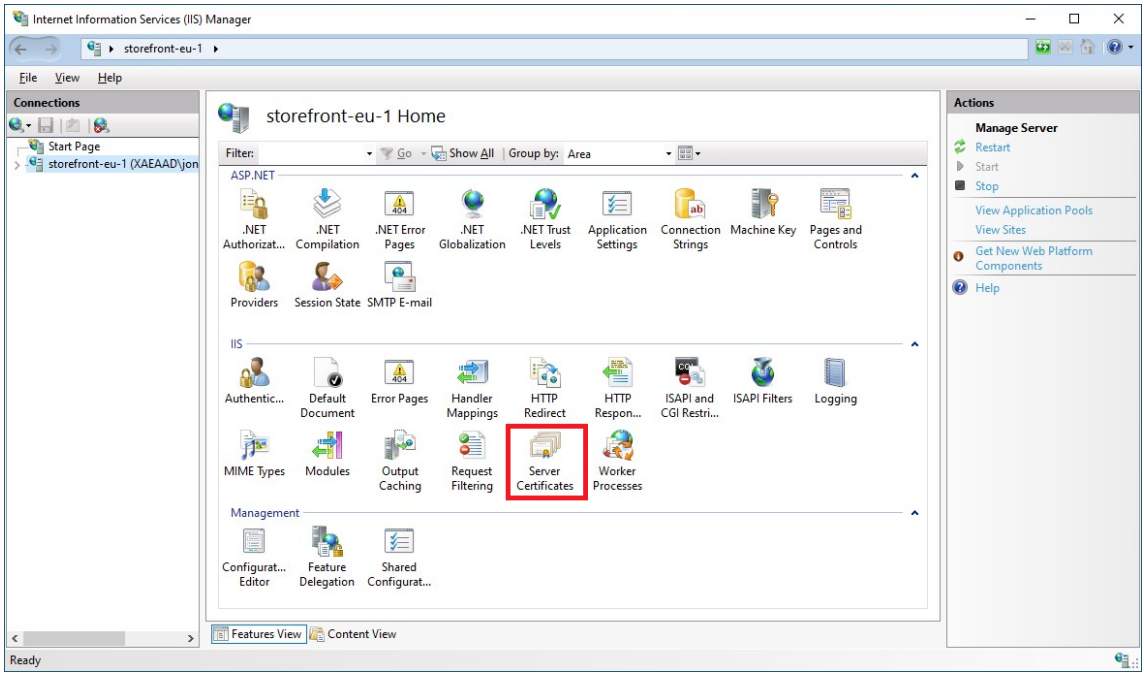
Creación de certificados

- Asegúrese de que los FQDN utilizados para acceder a StoreFront estén incluidos en el campo DNS como nombre alternativo del sujeto (SAN). Si usa un equilibrador de carga, incluya tanto el FQDN del servidor individual como el FQDN del equilibrador de carga.
- Firme el certificado con una entidad de certificación de terceros, como Verisign o una CA raíz de la empresa para su organización.
- Exporte el certificado en formato PFX e incluya la clave privada.

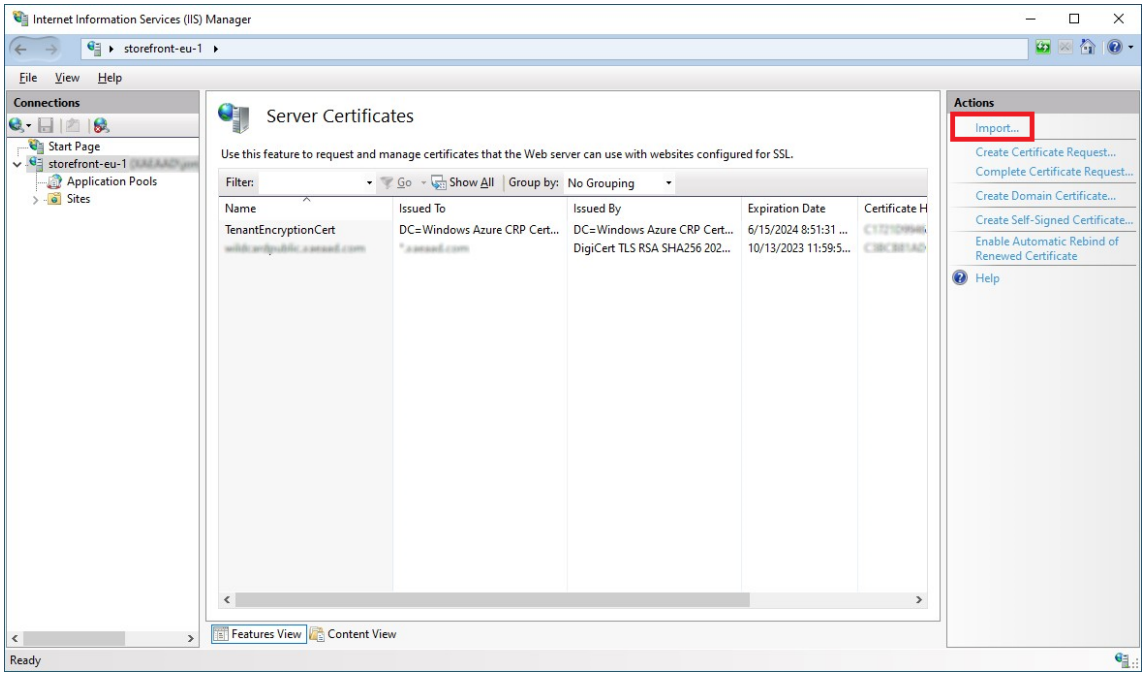
Configurar IIS para HTTPS

Para configurar Microsoft Internet Information Services (IIS) para HTTPS en el servidor de StoreFront:

1. Abra la consola del Administrador de Internet Information Services (IIS).
2. En la vista de árbol de la izquierda, seleccione el servidor.
3. En el panel derecho, haga doble clic en **Certificados de servidor**.

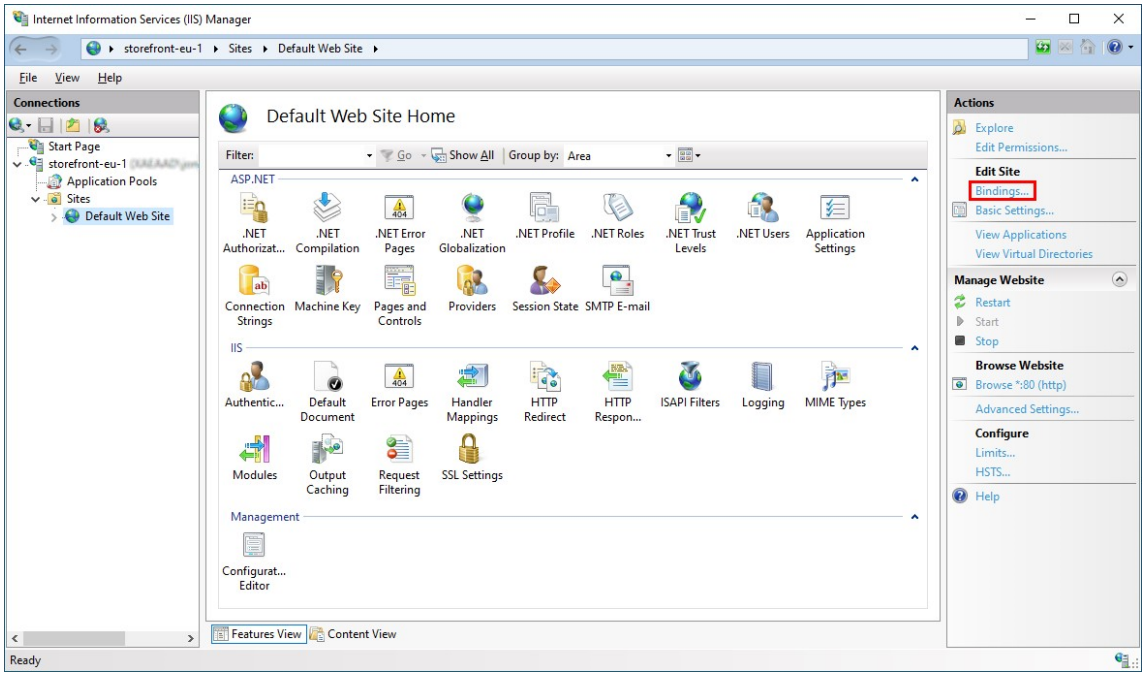


4. Desde la pantalla Certificados de servidor, puede importar un certificado existente o crear uno.



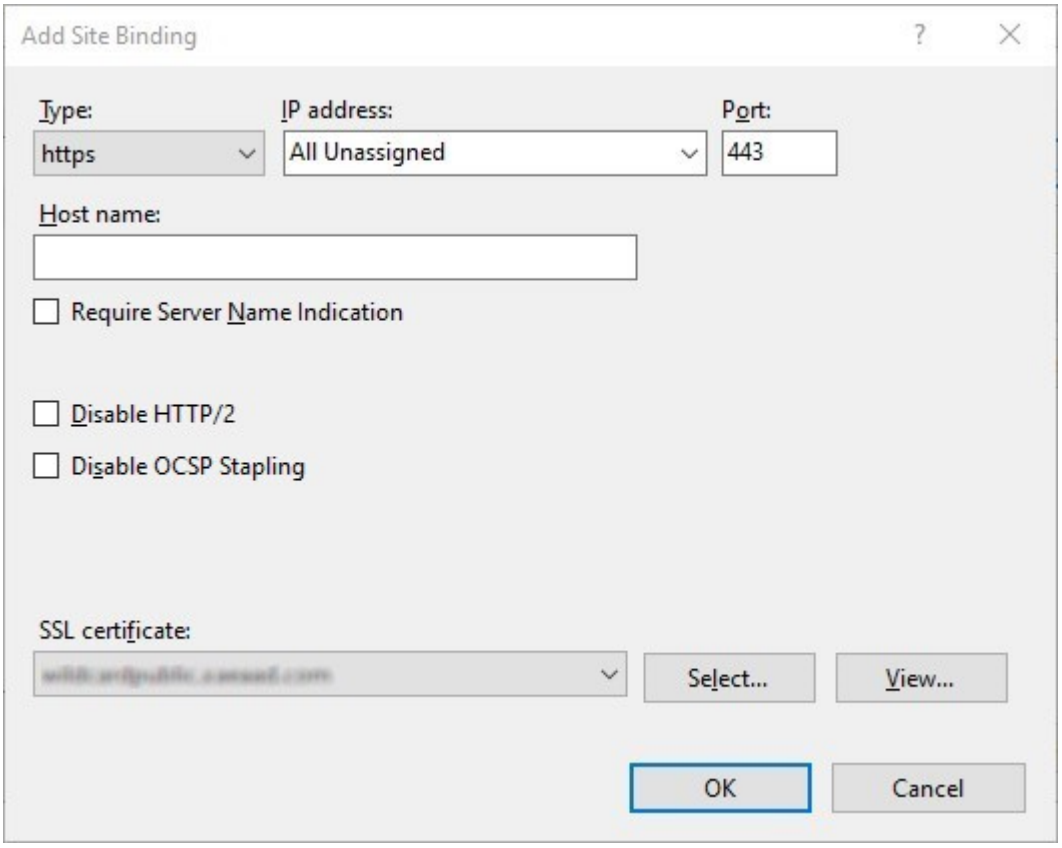
5. En la vista de árbol de la izquierda, seleccione **Sitio web predeterminado** (o el sitio web correspondiente)

6. En el panel Acciones, haga clic en **Enlaces…**

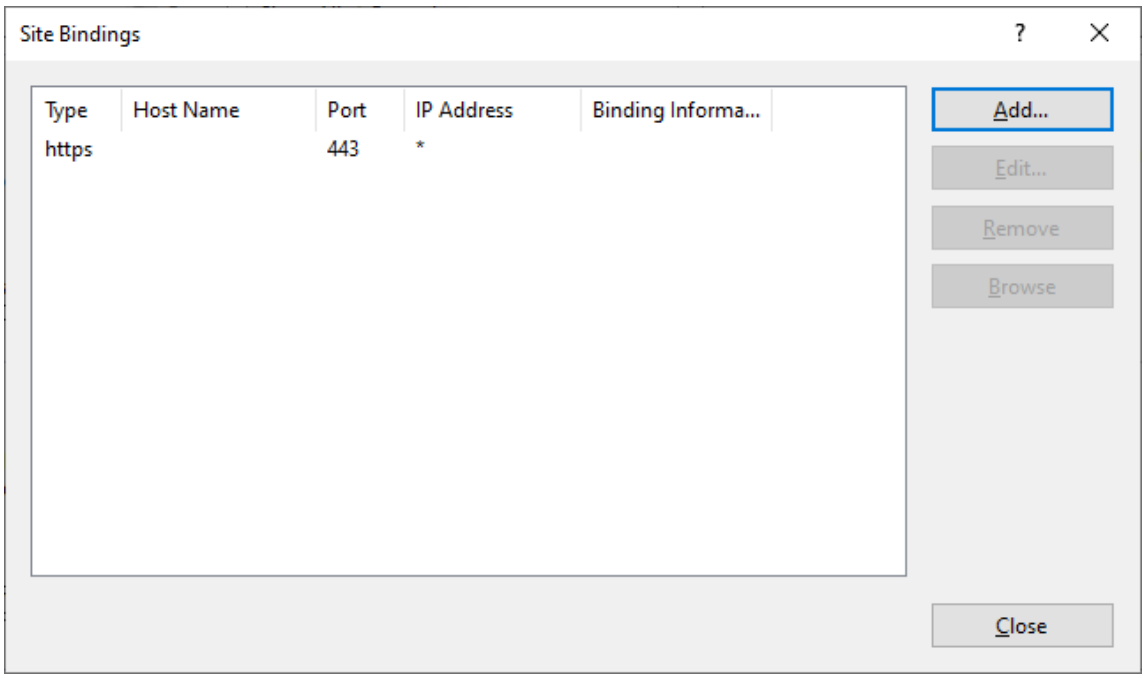


7. En la ventana de enlaces, haga clic en **Agregar…**
8. En el menú desplegable **Tipo**, seleccione **https**.
9. En Windows Server 2022 o una versión posterior, haga clic en **Deshabilitar TLS antiguo** para inhabilitar TLS anterior a 1.2.

   En versiones anteriores de Windows Server, puede inhabilitar versiones del TLS antiguo mediante los parámetros del Registro de Windows. Consulte la documentación de Windows Server.
10. Seleccione el certificado importado anteriormente. Presione Aceptar.



11. Para quitar el acceso HTTP, seleccione HTTP y haga clic en **Quitar**.

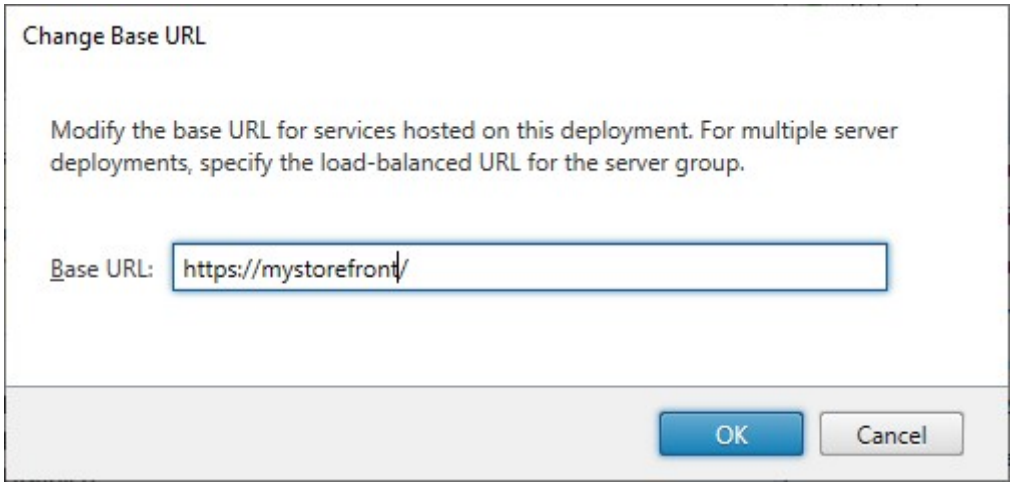


Cambiar la dirección URL base del servidor de StoreFront de HTTP a HTTPS

Si instala y configura Citrix StoreFront sin instalar y configurar primero un certificado SSL, StoreFront utiliza HTTP para las comunicaciones.

Si instala y configura un certificado SSL más adelante, utilice el siguiente procedimiento para asegurarse de que StoreFront y sus servicios utilizan conexiones HTTPS.

1. En la consola de administración de Citrix StoreFront, en el panel izquierdo seleccione **Grupo de servidores**.
2. En el panel Acciones, seleccione **Cambiar URL base**.
3. Actualice la URL base para que empiece por `https:` y haga clic en **Aceptar**.



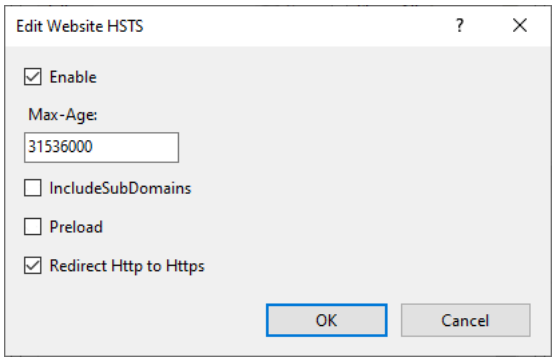
HSTS

El dispositivo cliente del usuario es vulnerable incluso después de habilitar HTTPS en el servidor. Por ejemplo, un atacante del tipo "Man in the middle"podría falsificar el servidor de StoreFront y engañar al usuario para que se conecte al servidor falsificado a través de HTTP simple. A continuación, podría acceder a información confidencial, como credenciales de usuario. La solución consiste en garantizar que el explorador web del usuario no intente acceder al servidor de RfWeb a través de HTTP. Puede lograrlo con el protocolo HTTP Strict Transport Security (HSTS).

Cuando HSTS está activado, el servidor indica a los exploradores web que las solicitudes al sitio web solo deben realizarse a través de HTTPS. Si un usuario intenta acceder a la URL mediante HTTP, el explorador cambiará automáticamente a HTTPS en su lugar. Esto garantiza la validación del lado del cliente de una conexión segura, así como la validación del lado del servidor en IIS. El explorador web mantiene esta validación durante un período configurado.

En Windows Server 2019 y versiones posteriores:

1. Abra **Administrador de Internet Information Services (IIS)**.
2. Seleccione **Sitio web predeterminado** (o el sitio web correspondiente).
3. En el panel Acciones de la derecha, haga clic en **HSTS...**
4. Marque **Habilitar**, introduzca una antigüedad máxima (p. ej. 31536000 para un año) y marque **Redirigir HTTP a HTTPS**.
5. Presione **Aceptar**.



> **Nota:**
>
> La activación de HSTS afecta a todos los sitios web del mismo dominio. Por ejemplo, si se puede acceder al sitio web en https://www.company.com/Citrix/StoreWeb, la directiva de HSTS se aplicará a todos los sitios web que figuran bajo https://www.company.com, lo que tal vez no resulte conveniente.

Proteger la implementación de StoreFront

April 17, 2024

En este artículo se muestran las áreas que pueden afectar la seguridad del sistema durante la implementación y la configuración de StoreFront.

Comunicación entre usuarios finales y StoreFront

Citrix recomienda proteger la comunicación entre los dispositivos de los usuarios y StoreFront mediante HTTPS. Esto garantiza el cifrado de contraseñas y otros datos que se envíen entre el cliente y StoreFront. Además, las conexiones HTTP simples pueden verse comprometidas por varios ataques, como los ataques del tipo "Man in the middle", especialmente cuando las conexiones se realizan desde ubicaciones no seguras, como puntos de acceso Wi-Fi públicos. Sin una configuración de IIS adecuada, StoreFront utiliza HTTP para las comunicaciones.

Según la configuración, los usuarios pueden acceder a StoreFront a través de una puerta de enlace o un equilibrador de carga. Puede cerrar la conexión HTTPS en la puerta de enlace o en el equilibrador de carga. Sin embargo, en este caso, Citrix sigue recomendando proteger las conexiones entre la puerta de enlace o el equilibrador de carga y StoreFront mediante HTTPS.

Para habilitar HTTPS, inhabilitar HTTP y habilitar HSTS, consulte Proteger StoreFront con HTTPS.

Comunicaciones de StoreFront con los servidores de Citrix Virtual Apps and Desktops

Citrix recomienda usar el protocolo HTTPS para proteger los datos que pasan entre StoreFront y los Delivery Controllers de Citrix Virtual Apps and Desktops. Consulte Instalar certificados de servidor TLS en los Controllers. StoreFront no admite los protocolos TLS 1.0 ni TLS 1.1 entre StoreFront y el Delivery Controller. Como alternativa, también puede configurar Windows para proteger la comunicación entre los servidores mediante IPSec.

Puede configurar el Delivery Controller y StoreFront para garantizar que solo los servidores de confianza de StoreFront puedan comunicarse con el Delivery Controller (consulte Administrar claves de seguridad).

Comunicaciones de StoreFront con Cloud Connectors

Citrix recomienda usar el protocolo HTTPS para proteger los datos que pasan entre StoreFront y los Cloud Connectors. Consulte How to Enable SSL on Cloud Connectors to Secure XML Traffic. StoreFront no admite los protocolos TLS 1.0 ni TLS 1.1 entre StoreFront y los Cloud Connectors. Como alternativa, también puede configurar Windows para proteger la comunicación entre los servidores mediante IPSec.

Acceso remoto

Citrix no recomienda exponer el servidor de StoreFront directamente a Internet. Citrix recomienda utilizar un dispositivo Citrix Gateway para proporcionar autenticación y acceso a usuarios remotos.

Refuerzo de Microsoft Internet Information Services (IIS)

StoreFront puede configurarse con una configuración restringida de IIS. Esta no es la configuración predeterminada de IIS.

Extensiones de nombre de archivo

Puede usar el filtrado de solicitudes para configurar una lista de extensiones de archivo permitidas y no permitir las extensiones de nombre de archivo que no figuren en la lista. Consulte la documentación de IIS.

StoreFront requiere estas extensiones de nombre de archivo:

- . (extensión en blanco)
- .appcache
- .aspx
- .cr
- .css
- .dtd
- .png
- .htm
- .html
- .ica
- .ico
- .jpg
- .js
- .png
- .svg
- .txt
- .xml

Si la descarga o la actualización de la versión de la aplicación Citrix Workspace está habilitada para el sitio web de un almacén, StoreFront también requiere estas extensiones de nombre de archivo:

- .dmg
- .exe

Si la aplicación Citrix Workspace para HTML5 está habilitada, StoreFront también requiere estas extensiones de nombre de archivo:

- .eot
- .ttf
- .woff
- .wasm

Verbos

Puedes usar el filtrado de solicitudes para configurar una lista de verbos permitidos y no permitir los verbos no listados. Consulte la documentación de IIS.

- GET
- POST
- HEAD

Caracteres que no son ASCII en las URL

Si se asegura de que el nombre del almacén y el nombre del sitio web solo usen caracteres ASCII, las URL de StoreFront no contienen caracteres ASCII. Puede usar el filtrado de solicitudes para no permitir caracteres que no sean ASCII. Consulte la documentación de IIS.

Tipos MIME

Puede quitar los tipos MIME del shell del sistema operativo correspondientes a estas extensiones de archivo:

- .exe
- .dll
- .com
- .bat
- .csh

Consulte la documentación de IIS.

Quitar el encabezado X-Powered-By

De forma predeterminada, IIS notifica que utiliza ASP .NET al agregar un encabezado `X-Powered-By` con valor `ASP.NET`. Puede configurar IIS para quitar este encabezado. Consulte la documentación de encabezados personalizados de IIS.

Quitar el encabezado de servidores con la versión de IIS

De forma predeterminada, IIS notifica la versión de IIS al agregar un encabezado `Server`. Puede configurar IIS para quitar este encabezado. Consulte la documentación de filtrado de solicitudes de IIS.

Mover el sitio web de StoreFront a una partición independiente

Puede alojar los sitios web de StoreFront en una partición independiente de los archivos del sistema. En IIS, debe mover el **sitio web predeterminado**o crear un sitio independiente en la partición adecuada antes de crear la implementación de StoreFront.

Funciones de IIS

Para ver la lista de las funciones de IIS instaladas y utilizadas por StoreFront, consulte Requisitos del sistema. Puede quitar otras funciones de IIS.

Aunque StoreFront no usa filtros ISAPI directamente, ASP .NET requiere esta función, por lo que no se puede desinstalar.

Asignaciones de controladores

StoreFront requiere estas asignaciones de controladores. Puede quitar otras asignaciones de controladores.

- ExtensionlessUrlHandler-Integrated-4.0
- PageHandlerFactory-Integrated-4.0
- StaticFile

Consulte la documentación de controladores de IIS.

Filtros ISAPI

StoreFront no requiere ningún filtro ISAPI. Puede quitar todos los filtros ISAPI. Consulte la documentación de los filtros ISAPI de IIS.

Reglas de autorización de .NET

De forma predeterminada, los servidores de IIS tienen la “regla de autorización de .NET”establecida en Permitir a todos los usuarios. De forma predeterminada, el sitio web que usa StoreFront hereda esta configuración.

Si quita o cambia la regla de autorización de .NET al nivel del servidor, debe supeditar las reglas del sitio web que usa StoreFront para agregar una regla de permiso para “Todos los usuarios”y quitar cualquier otra regla que haya.

Grupos de aplicaciones

StoreFront crea los siguientes grupos de aplicaciones:

- API de configuración de Citrix
- Autenticación de Citrix Delivery Services
- Recursos de Citrix Delivery Services
- y Citrix Receiver para Web

No cambie los grupos de aplicaciones que usa cada aplicación de IIS ni la identidad de cada grupo. Si usa varios sitios, no es posible configurar cada sitio para usar grupos de aplicaciones independientes.

En Parámetros de reciclaje, puede establecer el tiempo de espera por inactividad del grupo de aplicaciones y el límite de memoria virtual. Tenga en cuenta que, cuando el grupo de aplicaciones "Citrix Receiver para Web"se recicla, se cierra la sesión de los usuarios que hayan iniciado sesión a través de un explorador web, por lo que está configurado de forma predeterminada para reciclarse a las 2:00 todos los días para minimizar las interrupciones del servicio. Si cambia alguno de los parámetros de reciclaje, es posible que se cierre la sesión de los usuarios en otros momentos del día.

Parámetros requeridos

- No cambie los parámetros de autenticación de IIS. StoreFront administra la autenticación y configura los directorios apropiados del sitio de StoreFront con los parámetros de autenticación adecuados.
- Para el servidor de StoreFront, en **Parámetros de SSL**, no seleccione **Certificados de cliente: Requerir**. La instalación de StoreFront configura las páginas apropiadas del sitio de StoreFront con este parámetro.
- StoreFront requiere cookies para el estado de la sesión y otras funcionalidades. En ciertos directorios, en **Estado de la sesión**, **Parámetros de cookies**, el **Modo** debe estar configurado en **Usar cookies**.
- StoreFront requiere que **Nivel de confianza de .NET** esté establecido en **Confianza total**. No establezca el nivel de confianza de .NET en ningún otro valor.

Servicios

La instalación de StoreFront crea los siguientes servicios de Windows:

- Citrix Configuration Replication (NT SERVICE\CitrixConfigurationReplication)
- Citrix Cluster Join (NT SERVICE\CitrixClusterService)
- Citrix Peer Resolution (NT SERVICE\Citrix Peer Resolution Service)

- Citrix Credential Wallet (NT SERVICE\CitrixCredentialWallet)
- Citrix Subscriptions Store (NT SERVICE\CitrixSubscriptionsStore)
- Citrix Default Domain Services (NT SERVICE\CitrixDefaultDomainService)

Estas cuentas inician sesión como `Network Service`. No cambie esta configuración.

Si configura la delegación restringida de Kerberos en StoreFront para XenApp 6.5, también se crea el servicio Citrix StoreFront Protocol Transition (NT SERVICE\CitrixStoreFrontProtocolTransition). Este servicio se ejecuta como `NT AUTHORITY\SYSTEM`. No cambie esta configuración.

Asignación de derechos de usuario

La modificación de los valores predeterminados en la asignación de derechos de usuario puede provocar problemas con StoreFront. En particular:

- Microsoft IIS está habilitado como parte de la instalación de StoreFront. Microsoft IIS concede el derecho de inicio de sesión **Iniciar sesión como proceso por lotes** y el privilegio **Suplantar un cliente después de la autenticación** en el grupo integrado IIS_IUSRS. Este es el comportamiento normal de instalación de Microsoft IIS. No cambie estos derechos de usuario. Consulte la documentación de Microsoft para obtener información detallada.
- Al instalar StoreFront, crea grupos de aplicaciones a los que IIS concede derechos de usuario **Iniciar sesión como un servicio**, **Ajustar las cuotas de memoria para un proceso**, **Generar auditorías de seguridad** y **reemplazar un símbolo (token) de nivel de proceso**.
- Para que un servidor se una a un grupo de servidores, el grupo Administradores debe tener derechos para **Restaurar archivos y directorios**, **Acceder a este equipo desde la red** y **Administrar el registro de auditoría y seguridad**.
- Para que los usuarios inicien sesión mediante autenticación de nombre de usuario y contraseña (directamente o a través de una puerta de enlace), deben tener derechos para “Permitir el inicio de sesión local”, a menos que haya configurado StoreFront para validar las contraseñas mediante el Delivery Controller.

Esta no es una lista exhaustiva y es posible que se requieran otros derechos de acceso de usuario.

Configurar la pertenencia a grupos

Al configurar un grupo de servidores de StoreFront, se agregan los siguientes servicios al grupo de seguridad Administradores:

- Citrix Configuration Replication (NT SERVICE\CitrixConfigurationReplication)
- Citrix Cluster Join (NT SERVICE\CitrixClusterService). Este servicio solo es visible en servidores que forman parte de un grupo y solo se ejecuta mientras la unión está en curso.

La pertenencia de estos grupos es necesaria para que StoreFront funcione correctamente, para:

- Crear, exportar, importar y eliminar certificados y definir permisos de acceso en ellos
- Leer y escribir en el Registro de Windows
- Agregar y quitar ensamblados de Microsoft .NET Framework en la caché Global Assembly Cache (GAC)
- Acceder a la carpeta **Archivos de programa\Citrix**<*Ubicación de StoreFront*>
- Agregar, modificar y quitar identidades de grupos de aplicaciones de IIS y aplicaciones web de IIS
- Agregar, modificar y quitar grupos de seguridad local y reglas de firewall
- Agregar y quitar servicios de Windows y complementos de PowerShell
- Registrar puntos finales de Microsoft Windows Communication Framework (WCF)

En actualizaciones de StoreFront, esta lista de operaciones puede cambiarse sin previo aviso.

La instalación de StoreFront también crea los siguientes grupos de seguridad locales:

- CitrixClusterMembers
- CitrixCWServiceReadUsers
- CitrixCWServiceWriteUsers
- CitrixDelegatedAuthenticatorUsers
- CitrixDelegatedDirectoryClaimFactoryUsers
- CitrixPNRSReplicators
- CitrixPNRSUsers
- CitrixStoreFrontAdministrators
- CitrixSubscriptionServerUsers
- CitrixSubscriptionsStoreServiceUsers
- CitrixSubscriptionsSyncUsers

StoreFront mantiene la pertenencia de los miembros de estos grupos de seguridad. Se utilizan para el control de acceso dentro de StoreFront y no se aplican a recursos de Windows tales como archivos y carpetas. No modifique los miembros de estos grupos.

Certificados en StoreFront

Certificados de servidor

Los certificados de servidor se usan para identificar las máquinas y para aplicar seguridad TLS (Transport Layer Security) al transporte de datos en StoreFront. Si decide habilitar ICA File Signing, StoreFront también puede utilizar los certificados para firmar los archivos ICA de forma digital.

Para obtener más información, consulte Comunicación entre usuarios finales y StoreFront y ICA File Signing.

Certificados de administración de tokens

Tanto los servicios de autenticación como los almacenes requieren certificados para la administración de tokens. StoreFront genera un certificado autofirmado cuando se crean servicios de autenticación o almacenes. Los certificados autofirmados que genera StoreFront no deben utilizarse para otros fines.

Certificados de Citrix Delivery Services

StoreFront guarda una serie de certificados en un almacén de certificados de Windows personalizado (Citrix Delivery Services). Los siguientes servicios usan estos certificados: Citrix Configuration Replication Service, Citrix Credential Wallet Service, y Citrix Subscriptions Store Service. Cada servidor de StoreFront de un clúster tiene una copia de estos certificados. Estos servicios no dependen de TLS para las comunicaciones seguras y no se usan como certificados TLS. Estos certificados se crean cuando se crea un almacén de StoreFront o cuando se instala StoreFront. No modifique el contenido de este almacén de certificados de Windows.

Certificados de firma de código

StoreFront incluye una serie de scripts de PowerShell (.ps1) en la carpeta *<directorio de instalación>*\Scripts. La instalación predeterminada de StoreFront no hace uso de estos scripts. Con ellos se pueden simplificar los pasos de configuración para tareas específicas que se llevan a cabo con poca frecuencia. Estos scripts están firmados, lo que permite que StoreFront admita la directiva de ejecución de PowerShell. Recomendamos usar la directiva **AllSigned** (La directiva **Restringida** no se admite, ya que impide la ejecución de scripts de PowerShell.) StoreFront no altera la directiva de ejecución de PowerShell.

Aunque StoreFront no instala un certificado de firma de código en el almacén Editores de confianza, Windows puede agregar automáticamente el certificado de firma de código ahí. Esto ocurre cuando el script de PowerShell se ejecuta con la opción **Ejecutar siempre**. (Si selecciona la opción **No ejecutar nunca**, el certificado se agrega al almacén de Certificados en los que no se confía, y los scripts de PowerShell de StoreFront no se ejecutarán.) Una vez que el certificado de firma de código haya sido agregado al almacén Editores de confianza, Windows ya no comprueba su caducidad. Puede quitar este certificado del almacén Editores de confianza después de que las tareas de StoreFront se hayan completado.

Inhabilitar versiones antiguas de TLS

Citrix recomienda inhabilitar TLS 1.0 y 1.1 para la comunicación entre cliente y servidores en el servidor Windows. Puede hacerlo mediante una directiva de grupo o, también, mediante parámetros del

Registro de Windows. Consulte la documentación de Microsoft.

Separar la seguridad de StoreFront

Si implementa aplicaciones web en el mismo dominio Web (nombre de dominio y puerto) que StoreFront, cualquier posible problema de seguridad de esas aplicaciones web podrían afectar a su vez a la seguridad de la implementación de StoreFront. Cuando se necesita un mayor nivel de seguridad es necesario separarlos: Citrix recomienda implementar StoreFront en un dominio Web aparte.

ICA File Signing

StoreFront ofrece la opción de firmar de forma digital los archivos ICA mediante un certificado especificado en el servidor, para que las versiones de la aplicación Citrix Workspace que admiten esta función puedan verificar que el archivo proviene de una fuente de confianza. Los archivos ICA se pueden firmar con cualquier algoritmo hash que admita el sistema operativo que se ejecuta en el servidor de StoreFront, incluidos SHA-1 y SHA-256. Para obtener más información, consulte Habilitar ICA File Signing.

Cambio de contraseña por parte de los usuarios

Puede permitir que los usuarios que inicien sesión con credenciales de dominio de Active Directory desde un explorador web cambien sus contraseñas, ya sea en cualquier momento o solo cuando hayan caducado. No obstante, esto deja funciones de seguridad importantes al alcance de cualquier persona que pueda acceder a los almacenes que utilizan el servicio de autenticación. Si su organización cuenta con una directiva de seguridad que solo permite utilizar las funciones de cambio de contraseñas de los usuarios para uso interno, asegúrese de que no se pueda acceder a los almacenes desde fuera de la red corporativa. Al crear el servicio de autenticación, la configuración predeterminada impide que los usuarios cambien sus contraseñas, incluso aunque hayan caducado. Para obtener más información, consulte Permitir que los usuarios cambien sus contraseñas.

Personalizaciones

Para reforzar la seguridad, no escriba personalizaciones que carguen contenido o scripts desde servidores que no estén bajo su control. Copie el contenido o el script en la carpeta de personalización del sitio web que está personalizando. Si StoreFront está configurado para conexiones HTTPS, asegúrese de que todos los enlaces con el contenido o scripts personalizados usan también HTTPS.

Encabezados de seguridad

Al ver el sitio web de un almacén a través de un explorador web, StoreFront devuelve estos encabezados relacionados con la seguridad que imponen restricciones al explorador web.

Nombre del encabezado	Valor	Descripción
`content-security-policy`	`frame-ancestors 'none'`	De esta forma, se evita que otros sitios incrusten sitios web de StoreFront dentro de un marco y los ataques de secuestro de clics. StoreFront usa scripts y estilos integrados, por lo que no es posible usar una directiva de seguridad de contenido que los bloquee. Los sitios web de StoreFront solo muestran el contenido configurado por los administradores y no muestran ningún contenido introducido por el usuario, por lo que no es necesario bloquear los scripts en línea.
`X-Content-Type-Options`	`nosniff`	Esto evita la detección de tipos de MIME.
`X-Frame-Options`	`deny`	De esta forma, se evita que otros sitios incrusten sitios web de StoreFront dentro de un marco que impide ataques de secuestro de clics. Ya no se reconoce gracias a `content-security-policy` con `frame-ancestors 'none'`, pero algunos exploradores web antiguos sí que lo reconocen porque no admiten `content-security-policy`.

Nombre del encabezado	Valor	Descripción
`X-XSS-Protection`	`1; mode=block`	Utilizado por algunos exploradores web para mitigar ataques XSS (scripting entre sitios)

Cookies

StoreFront usa varias cookies. Algunas de las cookies utilizadas en el funcionamiento del sitio web son las siguientes:

Cookie	Descripción
`ASP.NET_SessionId`	Rastrea la sesión del usuario, incluido el estado de autenticación. Tiene `HttpOnly` establecido.
`CtxsAuthId`	Para evitar los ataques de fijación de sesiones, StoreFront también controla si el usuario está autenticado mediante esta cookie. Tiene `HttpOnly` establecido.
`CsrfToken`	Se usa para evitar la falsificación de solicitudes entre sitios mediante el patrón estándar de token de cookie a encabezado. El servidor establece un token en la cookie. El cliente lee el token de la cookie e incluye el token en la cadena de consulta o en un encabezado en las solicitudes posteriores. Esta cookie no debe tener `HttpOnly` establecido para que el JavaScript del cliente pueda leerla.
`CtxsDeviceId`	Identifica el dispositivo. Tiene `HttpOnly` establecido.

StoreFront establece otras cookies para rastrear el estado del usuario, algunas de las cuales deben leerse mediante JavaScript, por lo que no tienen `HttpOnly` establecido. Estas cookies no contienen ninguna información relacionada con la autenticación ni otros datos confidenciales.

Información adicional de seguridad

> **Nota:**
>
> Esta información puede cambiar en cualquier momento y sin previo aviso.

Es posible que su organización quiera realizar análisis de seguridad de StoreFront por motivos normativos. Las opciones de configuración anteriores pueden ayudar a eliminar algunos hallazgos en los informes de análisis de seguridad.

Si hay una puerta de enlace entre el analizador de seguridad y StoreFront, algunos hallazgos pueden estar relacionados con la puerta de enlace en lugar de con StoreFront. Los informes de análisis de seguridad generalmente no distinguen estos hallazgos (por ejemplo, la configuración de TLS). Debido a esto, las descripciones técnicas de los informes de análisis de seguridad pueden ser engañosas.

Detección de cuentas basada en direcciones de correo electrónico

August 15, 2023

Configure la detección de cuentas basada en direcciones de correo electrónico para que los usuarios que instalan la aplicación Citrix Workspace por primera vez en un dispositivo puedan configurar sus cuentas con sus direcciones de correo electrónico sin tener que saber la URL del almacén.

Durante el proceso de configuración inicial, la aplicación Citrix Workspace pide a los usuarios que introduzcan una dirección de correo electrónico o una URL de almacén. Si el usuario introduce una dirección de correo electrónico, la aplicación Citrix Workspace busca el dominio de correo electrónico en varias ubicaciones para determinar el servidor de StoreFront. A continuación, muestra todos los almacenes visibles para que el usuario pueda elegir.

Citrix recomienda usar Global App Config Service para configurar la detección por correo electrónico. Como alternativa, puede configurar la detección por correo electrónico mediante registros SVR de DNS o con alias de DNS.

Global App Config Service

Para configurar la detección por correo electrónico mediante Global App Config Service, consulte Configurar la detección por correo electrónico.

Registros SVR de DNS

Como alternativa a Global App Config Service, puede usar los registros SVR de DNS para configurar qué servidor de StoreFront debe usar la aplicación Citrix Workspace para un dominio de correo electrónico.

En el servidor DNS de du dominio de correo electrónico, agregue un registro **SRV** con estas propiedades:

Propiedad	Valor
Servicio	_citrixreceiver
Proto	TCP
Dispositivo de destino	El FQDN y el puerto para el dispositivo Citrix Gateway (para admitir a usuarios locales y remotos) o el servidor de StoreFront (para admitir solamente a los usuarios de la red local) con el formato *nombre de servidor.dominio:puerto*.

Si su entorno incluye servidores DNS internos y externos, puede agregar un registro SRV que especifique el FQDN del servidor de StoreFront en su servidor DNS interno y otro registro en su servidor externo que especifique el FQDN de Citrix Gateway. Con esta configuración, los usuarios de la red local reciben la información de StoreFront, mientras que los usuarios remotos reciben los datos de conexión de Citrix Gateway.

Registro DNS discoverReceiver

Como reserva de los otros métodos, puede crear un alias de DNS para el servidor de StoreFront `discoverReceiver` del dominio de correo electrónico. Por ejemplo, si su dominio de correo electrónico es `example.com`, cree un alias de DNS llamado `discoverReceiver.example.com`. Si no se encuentra ningún registro SRV en el dominio especificado, la aplicación Citrix Workspace busca una máquina denominada "discoverReceiver"para identificar un servidor de StoreFront.

Si usa este mecanismo, asegúrese de incluir `discoverReceiver` como nombre alternativo del sujeto en el certificado HTTPS de su servidor de StoreFront.

Crear una implementación

December 4, 2023

1. Si la consola de administración de Citrix StoreFront aún no está abierta después de la instalación de StoreFront, haga clic en la pantalla Inicio o Aplicaciones de Windows y haga clic en el icono Citrix StoreFront.

2. En el panel de resultados de la consola de administración de Citrix StoreFront, haga clic en **Crear implementación**.
3. Si hay varios sitios de IIS, elija en el menú desplegable **Sitio de IIS** el sitio que quiera usar.
4. Si usa un único servidor de StoreFront, introduzca la **URL base** de la URL del servidor. Si piensa configurar varios servidores de StoreFront tras un equilibrador de carga, introduzca la URL de equilibrio de carga como la **URL base**.

   Si aún no ha configurado el entorno de equilibrio de carga, especifique la URL del servidor. Puede modificar la URL base de la implementación en cualquier momento.
5. Haga clic en **Siguiente** y configure su primer almacén tal y como se describe en Crear almacén.
6. Una vez que haya completado todos los pasos de configuración, haga clic en **Crear** para crear la implementación y el almacén.
7. StoreFront muestra un resumen del almacén que creó. Haga clic en **Finalizar**.

Crear una implementación con el SDK de PowerShell

Para crear una implementación con el SDK de PowerShell, llame al cmdlet Add-STFDeployment.

Varios sitios web de Internet Information Services (IIS)

StoreFront le permite implementar distintos almacenes de aplicaciones en sitios web de IIS diferentes en cada servidor Windows, de forma que cada almacén tenga un nombre de host y un enlace de certificado diferentes.

Para crear varios sitios web, consulte la documentación de Microsoft IIS.

No es posible crear varias implementaciones de StoreFront mediante la consola de administración; debe usar el SDK de PowerShell. Por ejemplo, para crear dos implementaciones de sitios web de IIS, una para aplicaciones y otra para escritorios, use estos comandos:

```
Add-STFDeployment -SiteID 1 -HostBaseURL "https://apps.example.com"
Add-STFDeployment -SiteID 2 -HostBaseURL "https://desktops.example.com"
<!--NeedCopy-->
```

Una vez que haya habilitado varios sitios, StoreFront inhabilita la consola de administración, y no es posible devolver StoreFront al modo de sitio único. Debe configurar los sitios mediante el SDK de StoreFront e incluir el `SiteID` en cada comando.

Unirse a un grupo de servidores existente

December 4, 2023

Antes de instalar StoreFront en un servidor que está agregando al grupo, asegúrese de que:

- El servidor que está agregando utiliza la misma versión de sistema operativo con la misma configuración regional que el resto de los servidores del grupo. No se admiten los grupos de servidores de StoreFront que contengan combinaciones de versiones de sistema operativo y configuraciones regionales.
- La ruta relativa a StoreFront en IIS en el servidor que intenta agregar es el mismo que el resto de los servidores en el grupo.

> **Nota:**
>
> Para obtener recomendaciones sobre el tamaño de los grupos de servidores, consulte Grupos de servidores de StoreFront.

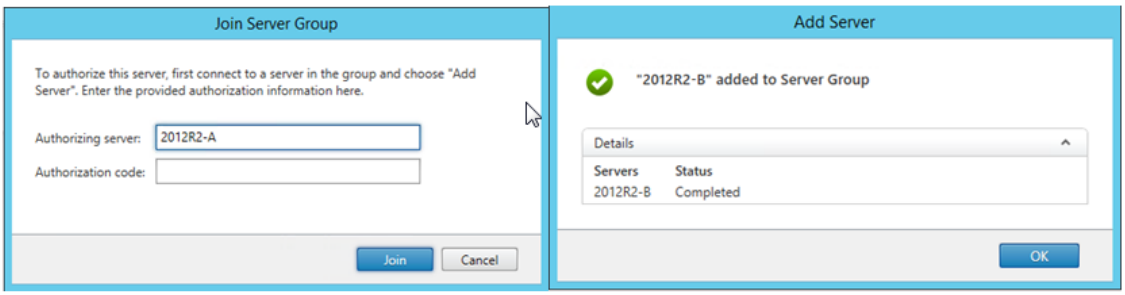
Si el servidor de StoreFront que está agregando pertenecía anteriormente a un grupo de servidores y se ha eliminado, antes de que pueda agregarse de nuevo, ya sea al mismo grupo de servidores o a otro, debe restablecer el servidor de StoreFront a un estado predeterminado de fábrica. Consulte Restablecer un servidor a los valores predeterminados de fábrica.

> **Importante:**
>
> Cuando agrega un nuevo servidor a un grupo de servidores, las cuentas de servicio de StoreFront se agregan como miembros del grupo de administradores locales en el nuevo servidor. Estos servicios requieren permisos de administrador local para unirse y sincronizarse con el grupo de servidores. Si usa Directivas de grupo para impedir la incorporación de nuevos miembros al grupo de administradores locales, o si tiene restringidos los permisos del grupo de administradores locales en los servidores, StoreFront no puede incorporarse al grupo de servidores.

1. Si la consola de administración de Citrix StoreFront aún no está abierta después de la instalación de StoreFront, haga clic en la pantalla Inicio o Aplicaciones de Windows y haga clic en el icono Citrix StoreFront.
2. En el panel de resultados de la consola de administración de Citrix StoreFront, haga clic en **Incorporarse a un grupo de servidores existente**.
3. Inicie sesión en un servidor de la implementación de StoreFront al que quiera unirse y abra la consola de administración de Citrix StoreFront. Seleccione el nodo Grupo de servidores en el panel izquierdo de la consola y, en el panel Acciones, haga clic en **Agregar servidor**. Anote el código de autorización que aparece.

4. Vuelva al nuevo servidor y, en el cuadro de diálogo Incorporarse a grupo de servidores, especifique el nombre del servidor existente en el cuadro Servidor de autorización. Introduzca el código de autorización obtenido a partir de ese servidor y haga clic en **Incorporarse**.

   Una vez incorporado al grupo, la configuración del nuevo servidor se actualiza para que coincida con la configuración del servidor existente. Todos los demás servidores del grupo se actualizan con la información del nuevo servidor.



Para administrar implementaciones con varios servidores, use solo un servidor a la vez para hacer cambios en la configuración del grupo de servidores. Compruebe que la consola de administración de Citrix StoreFront no se está ejecutando en ninguno de los demás servidores de la implementación. Cualquier cambio de configuración realizado debe propagarse a los demás servidores para garantizar una configuración coherente en toda la implementación.

Actualizar la versión de StoreFront

February 26, 2024

La actualización conserva la configuración de StoreFront y deja intactos los favoritos de los usuarios. Por el contrario, desinstalar StoreFront quita StoreFront y los servicios, sitios, favoritos (en servidores independientes) y la configuración asociados.

Rutas de actualización de la asistencia

Puede actualizar a StoreFront 2311 desde:

- StoreFront 2308
- StoreFront 2203 LTSR (cualquier CPU)
- StoreFront 1912 LTSR (cualquier actualización acumulativa)
- StoreFront 3.12 LTSR CU9

Para actualizar desde versiones anteriores a la 3.12 CU9, primero debe actualizar a StoreFront 3.12 CU9.

> **Advertencia:**
>
> Al actualizar una versión de StoreFront anterior a la versión 1912, todos los sitios de Desktop Appliance de la implementación se quitan automáticamente. Como alternativa, Citrix recomienda usar Desktop Lock de la aplicación Citrix Workspace para todos los casos de uso no asociados a un dominio.

Información útil

- No se admite la actualización a la versión más reciente de StoreFront desde una versión antigua que esté en el ciclo Fin de vida. Para obtener más información, consulte CTX200356.
- StoreFront no admite implementaciones de varios servidores que contengan versiones diferentes del producto, por lo que todos los servidores de un grupo de servidores deben actualizarse a la misma versión antes de conceder el acceso a la implementación.
- No se admite la actualización de versión simultánea para las implementaciones con varios servidores; los servidores deben actualizarse de forma secuencial.
- Antes de que se ejecute la actualización de la versión de StoreFront, se realizan algunas comprobaciones previas a la actualización. Si falla alguna comprobación previa a la actualización de versiones, la actualización no se inicia y se le notifica de los errores. Su instalación de StoreFront no cambia. Tras haber corregido la causa de los fallos, vuelva a ejecutar la actualización de versiones.
- Si se produce un error en la propia actualización de versiones de StoreFront, es posible que la instalación existente de StoreFront pierda su configuración inicial. Restaure la instalación de StoreFront a un estado funcional y vuelva a ejecutar la actualización de versiones. Para restaurar StoreFront a un estado funcional, tenga en cuenta los siguientes enfoques:
  - Restaurar la instantánea de VM que creó antes de la actualización de versiones
  - importar la configuración de StoreFront que exportó antes de la actualización (consulte Exportar e importar la configuración de StoreFront),
  - Seguir los consejos para solucionar problemas en Solucionar problemas de actualización de versiones de StoreFront.
- Cualquier error de actualización de versiones de StoreFront que se produzca desde el metainstalador de Citrix Virtual Apps and Desktops queda notificado en un cuadro de diálogo, con un enlace al registro de errores correspondiente.

Prepararse para la actualización de versiones

Antes de iniciar la actualización de la versión, se recomienda seguir estos pasos para evitar errores en la actualización:

- Planifique su estrategia de seguridad antes de actualizar la versión.
- Compruebe que no intenta actualizar StoreFront desde una versión de fin de vida. Para obtener más información, consulte CTX200356.
- Compruebe que va a actualizar StoreFront solamente desde una versión compatible a la versión actual.
- Descargue el instalador de StoreFront desde el sitio web de Citrix.

Actualizar la versión de un único servidor de StoreFront

1. Haga una copia de seguridad del servidor mediante la creación de una instantánea de VM.
2. Exporte la configuración existente de StoreFront. Si tiene varios servidores en un grupo de servidores, exporte únicamente la configuración del grupo de servidores de un servidor. Siempre que haya propagado todos los cambios entre ellos, todos los servidores de un grupo de servidores conservan copias idénticas de la configuración. Esta copia de reserva le permite crear fácilmente otro grupo de servidores para que pueda restaurar fácilmente la configuración en caso de problemas. Tenga en cuenta que solo podrá restaurar esta copia de reserva en un servidor que tenga la misma versión desde la que se exportó.
3. Si ha hecho modificaciones en los archivos de `C:\inetpub\wwwroot\Citrix\<StoreName>\App_Data`, como default.ica y usernamepassword.tfrm, realice una copia de seguridad de ellos para cada almacén. Después de la actualización de la versión, puede restaurarlos para restablecer las modificaciones.
4. Para impedir que los usuarios se conecten, quite el servidor de cualquier equilibrador de carga o, si no, bloquee las conexiones.
5. Reinicie el servidor.
6. Asegúrese de que no haya aplicaciones en ejecución, como la consola de administración de StoreFront, la línea de comandos o ventanas de PowerShell, ni ninguna otra aplicación que pueda estar bloqueando archivos de StoreFront. De esta manera, el instalador puede acceder a todos los archivos de StoreFront durante la actualización de versiones. Si el instalador no puede acceder a los archivos, estos no se reemplazan y la actualización de versiones no se produce, lo que provoca la eliminación de la configuración existente de StoreFront.
7. Asegúrese de no tener ningún Explorador de Windows ni ninguna línea de comandos abierta en los directorios que contienen archivos de StoreFront.
8. Inhabilite las aplicaciones antivirus.
9. Ejecute el archivo de instalación de la versión requerida de StoreFront.

Para actualizar la versión de un grupo de servidores de StoreFront

La actualización de versiones de grupos de servidores de StoreFront conlleva el uso de uno de los servidores para quitar los demás servidores del grupo. Los servidores eliminados conservan la con-

figuración relacionada con el grupo, lo que puede impedir que se unan a un nuevo grupo de servidores. Antes de que puedan volver a utilizarse para crear grupos de servidores o como servidores de StoreFront independientes, deben restablecerse a los valores predeterminados de fábrica o reinstalar StoreFront en ellos. No se admite la actualización simultánea de servidores de un grupo de servidores de StoreFront.

Ejemplo 1: Actualizar la versión de un grupo de servidores de StoreFront de tres nodos durante el tiempo de inactividad programado por mantenimiento

Esto describe la actualización de la versión de un grupo de servidores de StoreFront de tres servidores, A, B y C, durante el tiempo de inactividad programado.

1. Para inhabilitar el acceso de los usuarios al grupo de servidores, inhabilite la URL de equilibrio de carga. Esto impide que los usuarios se conecten a la implementación durante la actualización de versiones.
2. Utilice el servidor A para quitar los servidores B y C del grupo.

   Los servidores B y C se quedan "huérfanos"del grupo de servidores.
3. Actualice la versión del servidor A a partir de las instrucciones de Actualizar la versión de un único servidor de StoreFront.
4. Compruebe que la versión del servidor A se haya actualizado correctamente.
5. En los servidores B y C, desinstale la versión actualmente instalada de StoreFront y, luego, instale la nueva versión de StoreFront.
6. Una los servidores B y C al servidor actualizado A para crear un grupo de servidores actualizado. Este grupo de servidores consta de un servidor actualizado (A) y dos servidores recién instalados (B y C).

   El proceso Incorporarse a un grupo de servidores existente propaga automáticamente todos los datos de configuración y de suscripción a los nuevos servidores B y C.
7. Compruebe que todos los servidores funcionan correctamente.
8. Para habilitar el acceso de los usuarios al grupo de servidores actualizado, habilite la URL de equilibrio de carga.

Ejemplo 2: Actualizar la versión de un grupo de servidores de StoreFront de tres nodos sin tiempo de inactividad programado

Esto describe la actualización de la versión de un grupo de servidores de StoreFront de tres servidores, A, B y C, sin tiempo de inactividad programado.

Antes de actualizar la versión de un grupo de servidores:

1. Exporte la configuración de StoreFront mediante **Export-STFConfiguration**. Esta copia de reserva es necesaria porque los servidores se restablecen a sus valores de fábrica más adelante en el proceso, lo que elimina los datos de configuración.
2. Exporte los datos de suscripción del servidor A mediante **Export-STFStoreSubscriptions**. Esta copia de reserva es necesaria porque los servidores se restablecen a sus valores de fábrica más adelante en el proceso, lo que elimina los datos de suscripción. Consulte Administrar datos de suscripción a un almacén.
3. Inhabilite el acceso de los usuarios al servidor C eliminándolo del equilibrador de carga. Esto impide que los usuarios se conecten al servidor C durante el proceso de actualización. El equilibrador de carga sigue enviando solicitudes a los servidores A y B.
4. Utilice el servidor A para quitar el servidor C del grupo.
   Los servidores A y B siguen ofreciendo acceso a los recursos de sus usuarios. El servidor C se ha quedado huérfano del grupo de servidores, y se han restablecido sus valores de fábrica.
5. Restablezca el servidor huérfano C a sus valores predeterminados de fábrica mediante **Clear-STFDeployment**.
6. Importe la configuración de StoreFront que exportó antes al servidor C mediante **Import-STFConfiguration**. El servidor C ahora tiene una configuración idéntica a la del grupo de servidores anterior. *No* es necesario repetir este paso más adelante. Solamente un servidor necesita una copia de los datos de configuración para propagarlos a los demás servidores que se unan al grupo.
7. Actualice la versión del servidor C a partir de las instrucciones de Actualizar la versión de un único servidor de StoreFront. Ahora el servidor C tiene una configuración idéntica a la del grupo de servidores anterior y se actualiza a una nueva versión de StoreFront.
8. Importe los datos de suscripción que exportó antes al servidor C. *No* es necesario repetir este paso más adelante. Solamente un servidor necesita una copia de los datos de suscripción para propagarlos a los demás servidores que se unan al grupo.
9. Repita los pasos 3, 4, 5 y 7 con el servidor B (no repita el paso 6). Durante este tiempo, solo el servidor A proporciona a los usuarios acceso a los recursos. Por lo tanto, se recomienda seguir este paso durante períodos de poca actividad, donde se espere que la carga en el grupo de servidores de StoreFront sea mínima.
10. Incorpore el servidor B al servidor C mediante el proceso Incorporarse a un grupo de servidores existente. Esto proporciona una implementación de un solo servidor en la versión actual de StoreFront (servidor A) y un nuevo grupo de servidores de dos nodos en la nueva versión de StoreFront (servidores B y C).
11. Agregue los servidores B y C al servicio de equilibrio de carga de modo que puedan tomar el relevo del servidor A.
12. Quite el servidor A del equilibrador de carga para que los usuarios se dirijan a los servidores B y C recién actualizados.
13. Repita los pasos 3, 4, 5 y 7 con el servidor A (no repita el paso 6). El proceso de actualización

de versiones del grupo de servidores se ha completado. Los servidores A, B y C tienen datos de configuración y de suscripción idénticos al del grupo original.

> **Nota:**
>
> Durante el breve período en que el servidor A es el único servidor accesible, se pueden perder suscripciones (paso 9). Esto puede provocar que el nuevo grupo de servidores tenga una copia ligeramente obsoleta de la base de datos de suscripción después de la actualización de versiones y que se pierdan los nuevos registros de suscripción.
>
> Esto no tiene ningún impacto funcional porque los datos de suscripción no son esenciales para que los usuarios puedan iniciar sesión e iniciar recursos. Sin embargo, los usuarios tendrían que volver a suscribirse a un recurso después de que el servidor A se haya restablecido a sus valores de fábrica y se haya unido al grupo recién actualizado. Aunque es poco probable que se pierdan bastantes registros de suscripción, es una consecuencia posible de la actualización en vivo de la versión de un entorno de producción de StoreFront sin tiempo de inactividad.

Si falla la actualización

1. En *C:\Windows\Temp\StoreFront*, abra el archivo *CitrixMsi*.log* más reciente y busque los errores de excepción que pueda haber.

   Excepciones del tipo **Thumbs.db Access**: Provocadas por los archivos *thumbs.db* que hay en *C:\inetpup\wwwroot\citrix* o en alguno de sus subdirectorios. Elimine los archivos *thumbs.db* que encuentre.

   Excepciones del tipo **Cannot get exclusive file access \in use**: Restaure la instantánea o copia de seguridad si está disponible, o bien reinicie el servidor y detenga manualmente los servicios de StoreFront.

   Excepciones del tipo **Service cannot be started**: Restaure la instantánea o copia de seguridad si está disponible, o bien instale la versión completa de .NET Framework 4.5 (no el perfil de cliente).

2. Si no hay errores de excepción en *CitrixMsi*.log*, compruebe **Visor de eventos > Delivery Services** en el servidor para ver si hay errores que contengan mensajes de los errores de excepción anteriores. Siga el consejo correspondiente.

3. Si no hay errores de excepción en el Visor de eventos, compruebe los registros de administración en *C:\Archivos de programa\Citrix\Receiver StoreFront\Logs* para ver si hay errores que contengan mensajes de los errores de excepción anteriores. Siga el consejo correspondiente.

Para obtener más información sobre los archivos de registro, consulte Registros de instalación.

Restablecer un servidor a los valores predeterminados de fábrica

August 15, 2023

En algunas situaciones, es necesario restablecer una instalación de StoreFront a su estado de instalación inicial. Esto es necesario, por ejemplo, para poder volver a agregar un servidor de StoreFront a un grupo de servidores.

Se puede realizar una desinstalación manual y reinstalación, pero esto requiere más tiempo y puede causar otros problemas inesperados. En su lugar, puede ejecutar el cmdlet de PowerShell **Clear-STFDeployment** para restablecer un servidor de StoreFront a un estado predeterminado de fábrica.

1. Asegúrese de que la consola de administración de StoreFront esté cerrada.
2. Abra PowerShell ISE y seleccione **Ejecutar como administrador**.
3. Establezca la ruta de acceso de PowerShell:

```
$env:PSModulePath = [Environment]::GetEnvironmentVariable('
    PSModulePath','Machine')
<!--NeedCopy-->
```

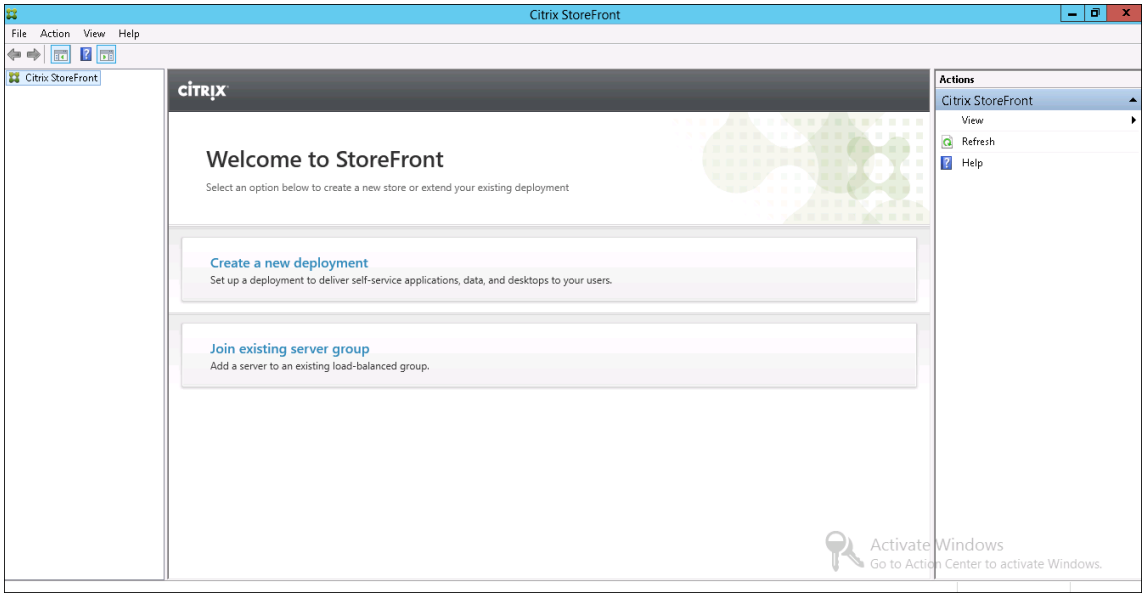
4. Importe el módulo Citrix StoreFront.

```
Import-Module citrix.storefront -verbose
<!--NeedCopy-->
```

5. Después de importar el módulo, ejecute el comando **Clear-STFDeployment** para restablecer el servidor de StoreFront a los parámetros predeterminados:

```
Clear-STFDeployment -Confirm $False
<!--NeedCopy-->
```

6. Cuando el comando se haya completado correctamente, abra la consola de administración de StoreFront y asegúrese que se restablezcan todas las configuraciones. Las opciones para **Crear una implementación** o **Incorporarse a un grupo de servidores existente** están disponibles.



Desinstale StoreFront

August 15, 2023

Además del producto en sí, la desinstalación de StoreFront conlleva la eliminación del servicio de autenticación, los almacenes, los sitios de Citrix Receiver para Web, las direcciones URL de XenApp Services y sus configuraciones asociadas. El servicio de suscripción de almacenes que contiene los datos de suscripción a aplicaciones de los usuarios también se elimina. En implementaciones de un solo servidor, la información sobre suscripciones a aplicaciones de los usuarios se pierde. No obstante, en implementaciones de varios servidores, estos datos se conservan en otros servidores del grupo. Los requisitos previos habilitados por el instalador de StoreFront, como las funciones de .NET Framework y los servicios de rol de Servidor web (IIS), no se eliminarán del servidor cuando se desinstala StoreFront.

1. Inicie sesión en el servidor de StoreFront con una cuenta con permisos de administrador local.
2. Cierre la consola de administración de StoreFront si está abierta.
3. Cierre las sesiones de PowerShell que se hayan utilizado para administrar StoreFront a través de su SDK de PowerShell.
4. Abra el menú **Inicio**, presione **Configuración** (icono de engranaje) y vaya a **Aplicaciones**.
5. En las ventanas de **Programas y características**, seleccione **Citrix StoreFront** y haga clic en **Desinstalar** para eliminar todos los componentes de StoreFront del servidor.
6. En el cuadro de diálogo **Desinstalar Citrix StoreFront**, haga clic en **Sí**. Cuando termine la desinstalación, haga clic en **Aceptar**.

Para quitar StoreFront manualmente

Después de desinstalar StoreFront, para asegurarse de que StoreFront se haya quitado por completo:

1. Quite el rol de servidor web.
2. Elimine la carpeta *C:\Archivos de programa\Citrix\Receiver StoreFront*.
3. Elimine cualquier subdirectorio de *C:\Archivos de programa\Citrix\StoreFront Install*.
4. Elimine la carpeta *C:\Inetpub*.

Ya puede reinstalar StoreFront.

Registros de la instalación

Para obtener más información sobre los archivos de registro, consulte Registros de instalación.

Configurar la autenticación y la delegación

December 4, 2023

Según sus requisitos, hay varios métodos de autenticación y delegación.

Método	Detalles
Configurar la autenticación	Configure los métodos que pueden emplear los usuarios para iniciar sesión en StoreFront a través de la aplicación Citrix Workspace.
Autenticación con tarjeta inteligente	Configure la autenticación con tarjeta inteligente.
Autenticación con nombre de usuario y contraseña	Permita que los usuarios se autentiquen con su nombre de usuario y su contraseña de Active Directory, y configure las opciones para cambiar las contraseñas y las notificaciones de caducidad de las contraseñas.
Autenticación PassThrough de dominio	Permita que los dispositivos Windows inicien sesión mediante Single Sign-On con sus credenciales de Windows.
Autenticación SAML	Delegue la autenticación a proveedores de identidades de terceros mediante SAML.

Método	Detalles
Configuración del Servicio de autenticación federada	Configurar StoreFront para integrarlo con el Servicio de autenticación federada para iniciar sesión con Single Sign-On en los VDA

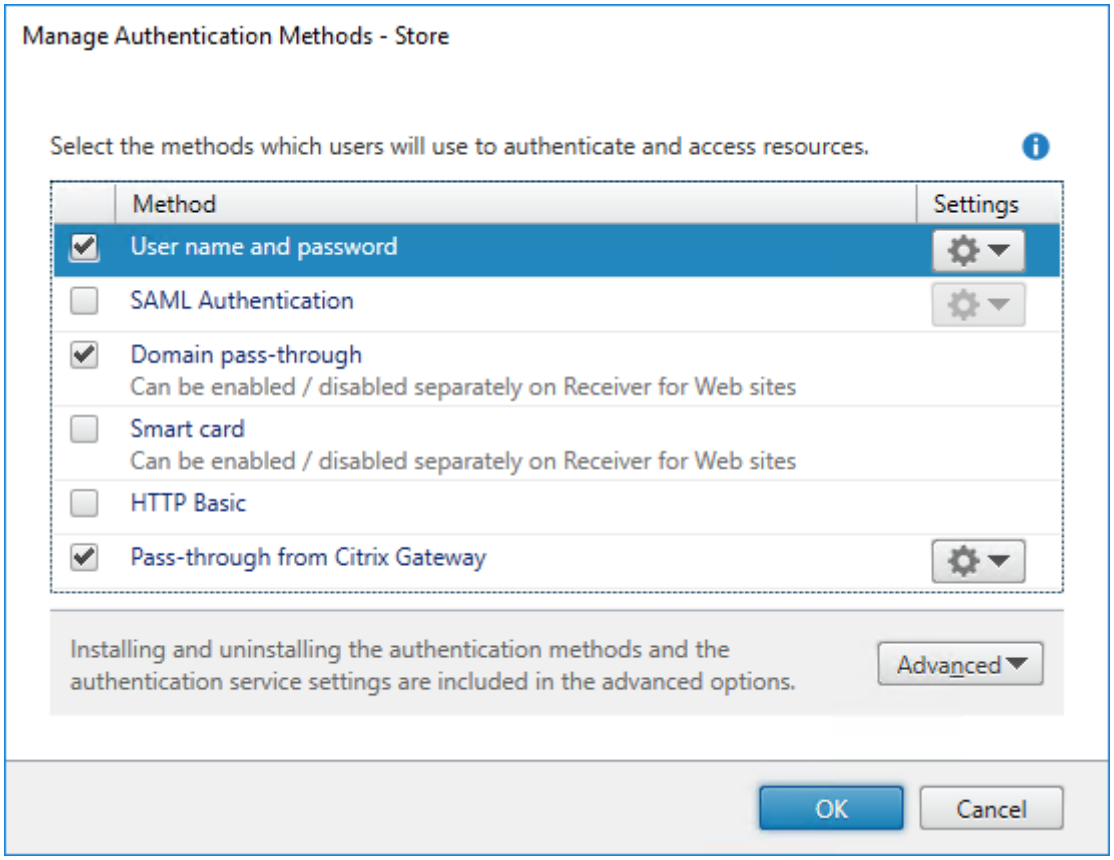
Configurar la autenticación

December 4, 2023

Administrar métodos de autenticación

Para cada almacén, puede elegir uno o más métodos de autenticación disponibles al iniciar sesión en el almacén a través de la aplicación Citrix Workspace.

1. Seleccione el nodo **Almacenes** en el panel izquierdo de la consola de administración de Citrix StoreFront y, en el panel **Acciones**, haga clic en **Administrar métodos de autenticación**.
2. Especifique los métodos de acceso que quiere habilitar para los usuarios.



- Seleccione la casilla **Nombre de usuario y contraseña** para habilitar la autenticación explícita de nombre de usuario y contraseña de Active Directory. Para obtener más información, consulte Autenticación con nombre de usuario y contraseña.
- Marque la casilla **Autenticación SAML** para permitir la integración en proveedores de identidades SAML. Para obtener más información, consulte Autenticación SAML.
- Marque la casilla **PassThrough de dominio** para habilitar la autenticación PassThrough de las credenciales de dominio de Active Directory desde los dispositivos de los usuarios. Para obtener más información, consulte Autenticación PassThrough de dominio.
- Marque **Tarjeta inteligente** para habilitar la autenticación con tarjeta inteligente. Para obtener más información, consulte Autenticación con tarjeta inteligente.
- Marque **Básica HTTP** para habilitar la autenticación básica HTTP. Los usuarios se autentican en el servidor web IIS del servidor de StoreFront.
- Marque **PassThrough desde Citrix Gateway** para habilitar la autenticación PassThrough desde Citrix Gateway. Habilite esta opción si los usuarios se conectan a StoreFront a través de un dispositivo Citrix Gateway con la autenticación habilitada. Para obtener más información, consulte PassThrough desde Citrix Gateway.

La modificación de los métodos de autenticación de un almacén también actualiza los métodos de autenticación que se utilizan al acceder al almacén a través de un explorador web. Para cambiar los métodos de autenticación al iniciar sesión a través de un explorador web, consulte Métodos de aut-

enticación.

Administrar los métodos de autenticación mediante el SDK de PowerShell

Para configurar la autenticación mediante el SDK de PowerShell:

1. Llame a Get-STFAuthenticationService para obtener el servicio de autenticación de un almacén o un directorio virtual y ver su configuración actual.
2. En el servicio de autenticación, habilite o inhabilite los protocolos de autenticación necesarios. Para obtener una lista de los protocolos disponibles, ejecute Get-STFAuthenticationServiceProtocol. Para habilitar los protocolos, ejecute Enable-STFAuthenticationServiceProtocol con una lista de protocolos que habilitar. Para inhabilitar los protocolos, ejecute Disable-STFAuthenticationServiceProtocol con la lista de protocolos que quiere inhabilitar.
3. Configure los protocolos de autenticación que habilitó. Para obtener información detallada, consulte la documentación de cada protocolo.

Parámetros del servicio de autenticación compartido

Utilice la tarea Shared Authentication Service Settings para especificar los almacenes que compartirán el servicio de autenticación al habilitar el inicio sesión Single Sign-On.

1. Seleccione el nodo **Almacenes** en el panel izquierdo de la consola de administración de Citrix StoreFront y, en el panel de resultados, seleccione un almacén. En el panel **Acciones**, haga clic en **Administrar métodos de autenticación**.
2. En el menú desplegable **Avanzado**, seleccione **Parámetros del servicio de autenticación compartido**.
3. Marque la casilla **Usar un servicio de autenticación compartido** y seleccione un almacén en el menú desplegable **Almacén**.

> **Nota:**
>
> No hay ninguna diferencia funcional entre un servicio de autenticación compartido y uno dedicado. Un servicio de autenticación compartido entre dos o más almacenes se trata como uno solo y los cambios que se hagan en su configuración afectarán a todos los almacenes que lo comparten.

Autenticación con tarjeta inteligente

April 17, 2024

Los usuarios realizan la autenticación con tarjetas inteligentes y PIN cuando acceden a los almacenes. Al instalar StoreFront, la autenticación con tarjeta inteligente se inhabilita de forma predeterminada. La autenticación con tarjeta inteligente puede habilitarse para los usuarios que se conectan a los almacenes a través de la aplicación Citrix Workspace, exploradores web y las direcciones URL de XenApp Services.

Use la autenticación con tarjeta inteligente para agilizar el proceso de inicio de sesión para sus usuarios y al mismo tiempo mejorar la seguridad del acceso de los usuarios a su infraestructura. El acceso a la red corporativa interna está protegido por la autenticación de dos factores basada en un certificado con infraestructura de clave pública. Las claves privadas están protegidas por controles de hardware y nunca salen de la tarjeta inteligente. Los usuarios obtienen la comodidad de acceder a sus escritorios y aplicaciones desde una serie de dispositivos de la empresa con sus tarjetas inteligentes y sus PIN.

Puede usar tarjetas inteligentes para la autenticación de usuarios a través de StoreFront en los escritorios y las aplicaciones que proporcionan Citrix Virtual Apps and Desktops. Los usuarios de tarjetas inteligentes que inician sesión en StoreFront también pueden acceder a las aplicaciones proporcionadas por Endpoint Management. No obstante, los usuarios deben volver a autenticarse para acceder a las aplicaciones web de Endpoint Management que usan la autenticación de certificados del cliente.

Para habilitar la autenticación con tarjeta inteligente, las cuentas de los usuarios deben configurarse ya sea en el dominio de Microsoft Active Directory que contiene los servidores de StoreFront, o bien, en un dominio que tenga una relación de confianza bidireccional directa con el dominio del servidor de StoreFront. Se admiten las implementaciones multibosque de confianza bidireccional.

La configuración de la autenticación con tarjeta inteligente para StoreFront depende de los dispositivos del usuario, de los clientes instalados y de si los dispositivos están unidos a un dominio o no. En este contexto, la unión a un dominio se refiere a dispositivos que se han vinculado a un dominio del bosque de Active Directory que contiene los servidores de StoreFront.

El documento Configuración de tarjetas inteligentes para entornos Citrix describe cómo configurar un entorno de Citrix para tarjetas inteligentes con un tipo de tarjeta inteligente específico. Para tarjetas inteligentes de otros proveedores hay que seguir un proceso similar.

Requisitos previos

- Asegúrese de que las cuentas de todos los usuarios estén configuradas ya sea en el dominio Microsoft Active Directory en el que planea implementar los servidores de StoreFront, o bien, dentro de un dominio que tenga una relación de confianza bidireccional directa con el dominio del servidor de StoreFront.
- Si tiene pensado habilitar la autenticación PassThrough con tarjeta inteligente, asegúrese de

que los tipos de lector de tarjeta inteligente, el tipo y la configuración de middleware y la directiva de almacenamiento en caché de PIN del middleware lo permiten.

- Instale el middleware de la tarjeta inteligente de su proveedor en las máquinas virtuales o físicas con el Virtual Delivery Agent que proporcionan los escritorios y las aplicaciones a los usuarios. Para obtener más información acerca del uso de tarjetas inteligentes con Citrix Virtual Desktops, consulte Tarjetas inteligentes.
- Asegúrese de que la infraestructura de clave pública está configurada correctamente. Compruebe que la asignación de certificados a cuentas está configurada correctamente para el entorno de Active Directory y de que la validación de certificados de usuario puede realizarse correctamente.

Configurar StoreFront

- Debe utilizar HTTPS para las comunicaciones entre los dispositivos de los usuarios y StoreFront para habilitar la autenticación con tarjeta inteligente. Consulte Proteger StoreFront con HTTPS.
- Para habilitar la autenticación con tarjeta inteligente al conectarse a un almacén mediante las aplicaciones de Citrix Workspace, en Métodos de autenticación marque o desmarque **Tarjeta inteligente**.
- Al habilitar la autenticación con tarjeta inteligente para un almacén de forma predeterminada, también se habilita para todos los sitios web de ese almacén. Puede habilitar o inhabilitar de forma independiente la autenticación con tarjeta inteligente para un sitio web específico en la ficha Métodos de autenticación de Administrar un sitio de Receiver para Web.
- Si se configura tanto la autenticación con nombre de usuario y contraseña como la autenticación con tarjeta inteligente, primero se solicita a los usuarios que inicien sesión con sus tarjetas inteligentes y sus PIN. En caso de problemas con las tarjetas inteligentes, también tendrán la opción de seleccionar la autenticación explícita.

Configurar Delivery Controller para que confíe en StoreFront

Cuando se utiliza la autenticación con tarjeta inteligente, StoreFront no tiene acceso a las credenciales del usuario, por lo que no puede autenticarse en Citrix Virtual Apps and Desktops. Por lo tanto, debe configurar Delivery Controller para que confíe en las solicitudes de StoreFront. Consulte Consideraciones y prácticas recomendadas de seguridad de Citrix Virtual Apps and Desktops.

Acceso remoto a través de Citrix Gateway

Para el acceso remoto, puede habilitar la tarjeta inteligente en el dispositivo Citrix Gateway y, a continuación, habilitar la autenticación PassThrough en StoreFront con autenticación delegada. Para

obtener más información, consulte PassThrough con Gateway.

Para garantizar que los usuarios no reciban una solicitud adicional de credenciales en el servidor virtual cuando se establezcan las conexiones a sus recursos, cree una segunda puerta de enlace e inhabilite la autenticación del cliente en los parámetros de la Capa de sockets seguros (SSL). Para obtener más información, consulte Configurar la autenticación con tarjeta inteligente. Al acceder a StoreFront a través de una puerta de enlace con autenticación con tarjeta inteligente. Configure la redirección óptima de Citrix Gateway a través de este servidor virtual para las conexiones a las implementaciones que proporcionan los escritorios y las aplicaciones del almacén. Para ver más información, consulte Configurar la redirección óptima de HDX Gateway para un almacén.

Single Sign-On en los VDA

Puede habilitar Single Sign-On en los VDA con PassThrough de credenciales con tarjeta inteligente de los usuarios. Se puede acceder al almacén mediante un explorador web o la aplicación Citrix Workspace para Windows, pero el recurso debe abrirse en la aplicación Citrix Workspace para Windows. En otros sistemas operativos o cuando se accede a los recursos mediante un explorador web, los usuarios deben volver a introducir sus credenciales al conectarse a un VDA.

1. Incluya el componente Single Sign-On al instalar Citrix Workspace para Windows y configúrelo para Single Sign-On. Consulte Configurar la autenticación PassThrough de dominio.
2. Use un editor de texto para abrir el archivo default.ica del almacén. Consulte Parámetros ICA predeterminados.
3. Para habilitar la autenticación PassThrough de credenciales con tarjeta inteligente para usuarios que acceden a almacenes sin Citrix Gateway, agregue el siguiente parámetro a la sección [Aplicaciones].

   ```
   DisableCtrlAltDel=Off
   ```

   Este parámetro se aplica a todos los usuarios del almacén. Si quiere habilitar tanto la autenticación PassThrough de dominio como la autenticación PassThrough con tarjeta inteligente para acceder a los escritorios y las aplicaciones, debe crear almacenes independientes para cada método de autenticación. A continuación, debe dirigir a los usuarios al almacén adecuado para su método de autenticación.
4. Para habilitar la autenticación PassThrough de credenciales con tarjeta inteligente para usuarios que acceden a almacenes a través de Citrix Gateway, agregue el siguiente parámetro a la sección [Aplicaciones].

   ```
   UseLocalUserAndPassword=On
   ```

   Este parámetro se aplica a todos los usuarios del almacén. Si quiere habilitar la autenticación PassThrough para algunos usuarios y requerir que otros inicien sesión para acceder a sus es-

critorios y aplicaciones, debe crear almacenes independientes para cada grupo de usuarios. A continuación, debe dirigir a los usuarios al almacén adecuado para su método de autenticación.

Single Sign-On en los VDA mediante FAS

Como alternativa, puede configurar el Servicio de autenticación federada para Single Sign-On en los VDA cuando use la aplicación Citrix Workspace instalada localmente, pero no la aplicación Citrix Workspace para HTML5.

Consideraciones importantes

El uso de tarjetas inteligentes para la autenticación de usuarios con StoreFront está sujeto a los siguientes requisitos y restricciones.

- Para utilizar túneles VPN con la autenticación mediante tarjeta inteligente, los usuarios deben instalar el plug-in de Citrix Gateway, iniciar sesión a través de una página web y utilizar las tarjetas inteligentes y los PIN en cada paso de la autenticación. La autenticación PassThrough en StoreFront con el plug-in de Citrix Gateway no está disponible para los usuarios de tarjetas inteligentes.
- Se pueden utilizar varias tarjetas inteligentes y varios lectores en el mismo dispositivo de usuario, pero si quiere habilitar la autenticación PassThrough con tarjeta inteligente, los usuarios deben asegurarse de que haya solamente una tarjeta inteligente insertada durante el acceso a un escritorio o aplicación.
- Cuando se utiliza una tarjeta inteligente dentro de una aplicación (por ejemplo, para las funciones de cifrado o firma digital), es posible que se muestren solicitudes adicionales para insertar una tarjeta inteligente o introducir un PIN. Esto puede suceder cuando se inserta más de una tarjeta inteligente al mismo tiempo. También puede deberse a parámetros de configuración, tales como parámetros de middleware como el caché de PIN, que se configuran generalmente con directivas de grupo. Cuando se solicite la inserción de una tarjeta inteligente y la tarjeta inteligente ya está insertada en el lector, los usuarios deben hacer clic en Cancelar. Si se solicita un PIN, los usuarios deben introducir de nuevo los PIN.
- Si habilita la autenticación PassThrough con tarjeta inteligente en Citrix Virtual Apps and Desktops para los usuarios de la aplicación Citrix Workspace para Windows con dispositivos unidos a un dominio que no acceden a los almacenes a través de Citrix Gateway, este parámetro se aplica a todos los usuarios del almacén. Si quiere habilitar tanto la autenticación PassThrough de dominio como la autenticación PassThrough con tarjeta inteligente para acceder a los escritorios y las aplicaciones, debe crear almacenes independientes para cada método de autenticación. Los usuarios deben conectarse al almacén adecuado para su método de autenticación.

- Si habilita la autenticación PassThrough con tarjeta inteligente en Citrix Virtual Apps and Desktops para los usuarios de la aplicación Citrix Workspace para Windows con dispositivos unidos a un dominio que acceden a los almacenes a través de Citrix Gateway, este parámetro se aplica a todos los usuarios del almacén. Si quiere habilitar la autenticación PassThrough para algunos usuarios y solicitar a otros usuarios que inicien sesión en los escritorios y aplicaciones, debe crear almacenes independientes para cada grupo de usuarios. A continuación, debe dirigir a los usuarios al almacén adecuado para su método de autenticación.
- Solo se puede configurar un método de autenticación para cada dirección URL de XenApp Services, y solo está disponible una dirección URL por almacén. Si quiere habilitar otros tipos de autenticación (además de la autenticación con tarjeta inteligente), debe crear almacenes independientes, cada uno de ellos con una URL de XenApp Services, para cada método de autenticación. A continuación, debe dirigir a los usuarios al almacén adecuado para su método de autenticación.
- Cuando se instala StoreFront, la configuración predeterminada de Microsoft Internet Information Services (IIS) solo requiere que se presenten certificados del cliente para conexiones HTTPS para la URL de autenticación de certificados del servicio de autenticación de StoreFront. IIS no solicita certificados del cliente para otras direcciones URL de StoreFront. Estas configuraciones le permiten ofrecer a los usuarios de tarjeta inteligente la opción de utilizar la autenticación explícita si tienen problemas con las tarjetas inteligentes. Según la configuración de las directivas de Windows, los usuarios también pueden quitar sus tarjetas inteligentes sin necesidad de volver a autenticarse.

  Si decide configurar IIS para solicitar certificados del cliente en caso de conexiones HTTPS a todas las direcciones URL de StoreFront, el servicio de autenticación y los almacenes deben colocarse en el mismo servidor. Debe usar un certificado del cliente válido para todos los almacenes. Con esta configuración de sitio de IIS, los usuarios de tarjetas inteligentes no pueden conectarse a través de Citrix Gateway y no pueden utilizar la autenticación explícita. Los usuarios deben iniciar sesión de nuevo si quitan las tarjetas inteligentes de los dispositivos.

Autenticación PassThrough de dominio

April 17, 2024

Los usuarios se autentican en sus equipos Windows unidos a un dominio, y sus credenciales se utilizan para iniciar sesión automáticamente en la aplicación Citrix Workspace. Esto se puede hacer a través de la aplicación Citrix Workspace para Windows y desde estos exploradores web en Windows:

- Internet Explorer
- Microsoft Edge

- Google Chrome
- Mozilla Firefox

Configuración de StoreFront

Para habilitar PassThrough de dominio para las aplicaciones Citrix Workspace para Windows, en los Métodos de autenticación, seleccione **PassThrough de dominio**.

Al habilitar la autenticación PassThrough de dominio para un almacén de forma predeterminada, también se habilita para la aplicación Citrix Workspace para HTML5 para todos los sitios web de ese almacén. Puede inhabilitar la autenticación PassThrough de dominio para un sitio web específico en la ficha Métodos de autenticación de Administrar un sitio de Receiver para Web.

Configurar Delivery Controller para que confíe en StoreFront

Cuando se utiliza la autenticación PassThrough de dominio, StoreFront no tiene acceso a las credenciales del usuario, por lo que no puede autenticarse en Citrix Virtual Apps and Desktops. Por lo tanto, debe configurar Delivery Controller para que confíe en las solicitudes de StoreFront. Consulte Consideraciones y prácticas recomendadas de seguridad de Citrix Virtual Apps and Desktops.

Single Sign-On en los VDA

Para el inicio de sesión único Single Sign-On en los VDA, debe usar la aplicación Citrix Workspace para Windows con el componente **Habilitar Single Sign-On**. Consulte Configurar la autenticación PassThrough de dominio. Si usa la aplicación Citrix Workspace para HTML5, debe configurarse para conectar con los recursos de la aplicación Citrix Workspace para Windows en lugar del explorador.

Configuración de la aplicación Citrix Workspace para Windows

Para habilitar PassThrough de dominio con Single Sign-on en el almacén y los VDA mediante la aplicación Citrix Workspace para Windows, consulte la documentación de la aplicación Citrix Workspace para Windows.

Configuración de la aplicación Citrix Workspace para HTML5

Es posible que tenga que actualizar la configuración del explorador web de los usuarios para permitir la autenticación PassThrough de dominio. Puede usar PassThrough de dominio para iniciar sesión en un almacén mediante un explorador web. Para iniciar sesión con Single Sign-On en los VDA, los usuarios deben abrir los recursos en la aplicación Citrix Workspace para Windows en lugar de hacerlo en el explorador web.

Internet Explorer, Edge y Chrome La mayoría de los exploradores web usan la configuración de zonas de Internet Explorer de Windows para decidir si habilitan Single Sign-On. De forma predeterminada, solo se habilita para los sitios de la zona de intranet local. Para agregar su sitio a la zona de intranet:

1. Abra Panel de control.
2. Abra Opciones de Internet.
3. Vaya a la ficha **Seguridad**.
4. Seleccione **Intranet local**.
5. Haga clic en **Sitios**.
6. Haga clic en **Avanzado**.
7. Agregue su sitio web de StoreFront.

Estos parámetros se pueden implementar mediante directivas de grupo.

FireFox Modifique los parámetros avanzados del explorador web para confiar en el URI del sitio web de StoreFront para Single Sign-On.

> **Advertencia:**
>
> Modificar incorrectamente la configuración avanzada puede causar problemas graves. Por tanto, las modificaciones serán bajo su propia responsabilidad.

1. Abra Firefox en el equipo que se va a autenticar mediante PassThrough de dominio.
2. En la barra de direcciones, escriba about:config.
3. Haga clic en la opción para aceptar el riesgo.
4. En la barra de búsqueda, escriba negotiate.
5. Haga doble clic en network.negotiate-auth.delegation-uris.
6. Introduzca el nombre de su dominio corporativo de Windows (por ejemplo, midominio.com).
7. Haga clic en Aceptar.
8. Haga doble clic en network.negotiate-auth.trusted-uris.
9. Introduzca el nombre de su dominio corporativo de Windows (por ejemplo, midominio.com).
10. Haga clic en Aceptar.
11. Cierre y reinicie Firefox.

Single Sign-On en los VDA mediante FAS

Como alternativa, puede configurar el Servicio de autenticación federada para Single Sign-On en los VDA cuando use la aplicación Citrix Workspace instalada localmente, pero no la aplicación Citrix Workspace para HTML5.

PassThrough desde Citrix Gateway

February 26, 2024

Los usuarios se autentican en Citrix Gateway y su sesión se inicia automáticamente cuando acceden a sus almacenes. La autenticación PassThrough desde Citrix Gateway está habilitada de forma predeterminada al configurar el acceso remoto a un almacén. Los usuarios pueden conectarse a través de Citrix Gateway a almacenes mediante la aplicación Citrix Workspace o un explorador web. Para obtener más información acerca de la configuración de StoreFront para Citrix Gateway, consulte Configurar Citrix Gateway.

StoreFront admite la autenticación PassThrough con los siguientes métodos de autenticación de Citrix Gateway.

- Los usuarios de **dominio** inician sesión con su nombre de usuario y su contraseña de Active Directory.
- Los usuarios de **RSA** inician sesión en Citrix Gateway mediante códigos de acceso derivados de tokencodes generados por tokens de seguridad combinados, en algunos casos, con códigos PIN. Si habilita la autenticación PassThrough con token de seguridad solamente, asegúrese de que los recursos disponibles no requieren formas de autenticación adicionales o alternativas, como credenciales de dominio de Microsoft Active Directory.
- Los usuarios con **tarjeta inteligente** inician sesión con tarjetas inteligentes
- Los usuarios de **RSA y dominio** que inician sesión en Citrix Gateway deben introducir sus credenciales de dominio y los códigos de acceso de tokens de seguridad.

Si en el dispositivo Citrix Gateway inhabilitó la autenticación o Single Sign-On, no se utiliza PassThrough, y debe configurar uno de los otros métodos de autenticación.

Si quiere configurar la autenticación de doble origen en Citrix Gateway para usuarios remotos que accedan a los almacenes desde la aplicación Citrix Workspace, debe crear dos directivas de autenticación en Citrix Gateway. Configure RADIUS (Servicio de autenticación remota telefónica de usuario) como el método principal de autenticación y LDAP (Protocolo ligero de acceso a directorios) como el método secundario. Modifique el índice de credenciales para usar el método secundario de autenticación en el perfil de sesión, de manera que las credenciales de LDAP se transfieran a StoreFront. Cuando agregue el dispositivo Citrix Gateway a su configuración de StoreFront, configure el tipo de inicio de sesión en Dominio y token de seguridad. Para obtener más información, consulte http://support.citrix.com/article/CTX125364

Para habilitar la autenticación multidominio a través de Citrix Gateway en StoreFront, configure el atributo de nombre del SSO en userPrincipalName en la directiva de autenticación LDAP de Citrix Gateway para cada dominio. Es posible que deba especificar un dominio a los usuarios en la página de inicio de sesión de Citrix Gateway para que se pueda determinar la directiva de LDAP correspon-

diente. Al configurar los perfiles de sesión de Citrix Gateway para las conexiones con StoreFront, no especifique un dominio Single Sign-On. Debe configurar las relaciones de confianza entre cada uno de los dominios. Asegúrese de permitir que los usuarios inicien sesión en StoreFront desde cualquier dominio al no restringir el acceso a solo aquellos dominios que sean explícitamente de confianza.

Cuando la implementación de Citrix Gateway lo admita, puede utilizar SmartAccess para controlar el acceso de los usuarios a los recursos de Citrix Virtual Apps and Desktops sobre la base de las directivas de sesión de Citrix Gateway.

Habilitar PassThrough con Gateway

Para habilitar o inhabilitar la autenticación de PassThrough con Gateway para un almacén cuando se conecta a través de aplicaciones Workspace, en la ventana Métodos de autenticación, marque o desmarque la opción **PassThrough desde Citrix Gateway**.

Al habilitar la autenticación PassThrough con Citrix Gateway para un almacén de forma predeterminada, también se habilita para todos los sitios web de ese almacén. Puede inhabilitar la autenticación con nombre de usuario y contraseña para un sitio web específico en la ficha Métodos de autenticación.

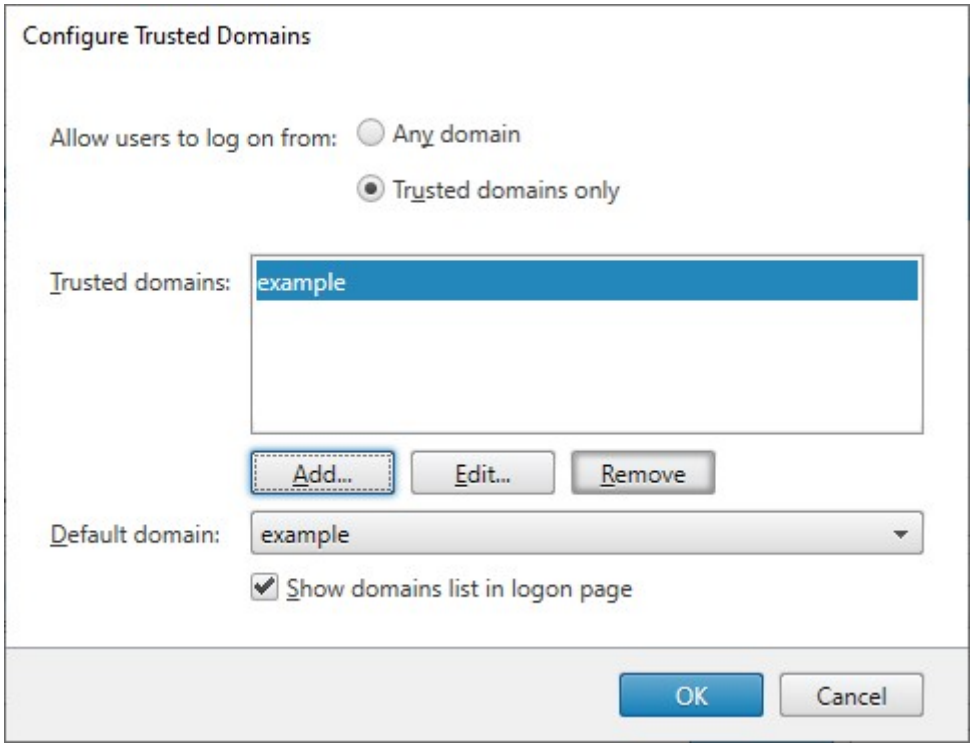
Configurar dominios de usuarios de confianza

Si su Citrix Gateway está configurado para usar autenticación LDAP, puede restringir el acceso a dominios específicos.

1. En la ventana "Administrar métodos de autenticación", en el menú desplegable **PassThrough desde Citrix Gateway** > **Parámetros**, seleccione **Configurar dominios de confianza**.
2. Seleccione **Solo dominios de confianza** y haga clic en **Agregar** para introducir el nombre de un dominio de confianza. Los usuarios con cuentas en ese dominio pueden iniciar sesiones en todos los almacenes que usen el servicio de autenticación. Para modificar un nombre de dominio, seleccione la entrada correspondiente en Dominios de confianza y haga clic en **Modificar**. Para interrumpir el acceso a los almacenes para las cuentas de usuario en ese dominio, seleccione un dominio de la lista y haga clic en **Quitar**.

   La manera en que se especifica el nombre del dominio determina el formato en el que los usuarios deben introducir sus credenciales. Si quiere que los usuarios introduzcan sus credenciales en un formato de nombre de usuario de dominio, agregue el nombre NetBIOS a la lista. Para exigir que los usuarios introduzcan sus credenciales en el formato de nombre principal de usuario, agregue el FQDN a la lista. Si quiere permitir que los usuarios introduzcan sus credenciales en el formato de nombre de usuario de dominio y en el formato de nombre principal de usuario, debe agregar el nombre NetBIOS y el FQDN a la lista.

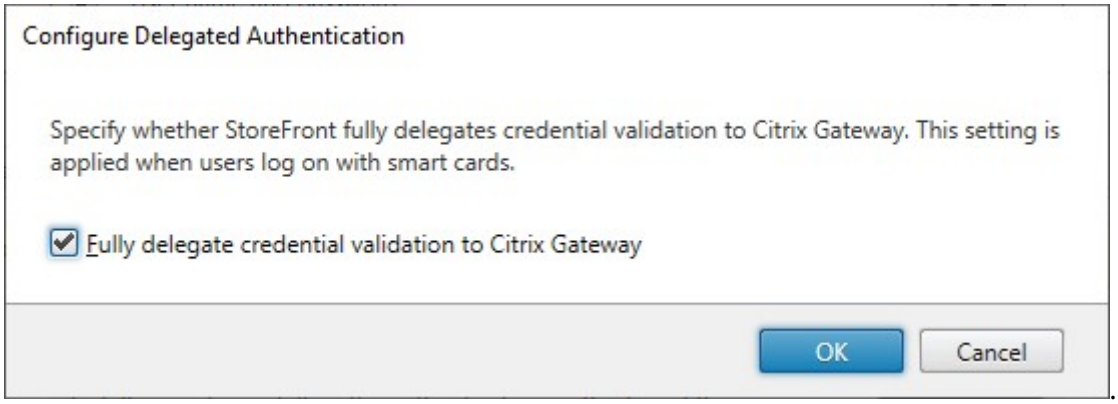
3. Si configura varios dominios de confianza, seleccione de la lista Dominio predeterminado el dominio que aparece seleccionado de forma predeterminada cuando los usuarios inician sesión en StoreFront.
4. Si quiere ver una lista de los dominios de confianza en la página de inicio de sesión, marque la casilla Mostrar lista de dominios en la página de inicio de sesión.



Delegar la validación de credenciales a Citrix Gateway

De forma predeterminada, StoreFront valida el nombre de usuario y la contraseña que recibe de Gateway. Si su Citrix Gateway está configurado para usar métodos de autenticación sin contraseña, como tarjetas inteligentes, debe configurar StoreFront para que no valide las credenciales y dependa de la autenticación de Gateway. En este caso, se recomienda introducir una URL de respuesta al configurar el dispositivo Gateway para que StoreFront pueda verificar que la solicitud proviene de dicho dispositivo. Consulte Administrar dispositivos Citrix Gateway.

1. En la ventana **Administrar métodos de autenticación**, en el menú desplegable **PassThrough desde Citrix Gateway** > **Parámetros**, seleccione **Configurar autenticación delegada**.
2. Seleccione **Delegar totalmente la validación de credenciales a Citrix Gateway**.



SDK de PowerShell

Para configurar el almacén para delegar la autenticación en la puerta de enlace mediante el SDK de PowerShell, use el cmdlet Set-STFCitrixAGBasicOptions para establecer `CredentialValidationMode` en `Auto`. Para configurar StoreFront para que valide las credenciales, establezca `CredentialValidationMod` en `Password`.

Permitir a los usuarios cambiar contraseñas caducadas al iniciar sesión

Si su dispositivo Citrix Gateway está configurado para usar la autenticación LDAP (nombre de usuario y contraseña), puede configurar NetScaler para que permita cambiar las contraseñas caducadas al iniciar sesión.

1. Iniciar sesión en el sitio web de administración de NetScaler
2. En el menú lateral, vaya a **Authentication** > **Dashboard**.
3. Haga clic en el servidor de autenticación.
4. En **Other Settings**, marque **Allow Password Change**.

Permitir a los usuarios cambiar las contraseñas después de iniciar sesión

Con **PassThrough desde Citrix Gateway**, el dispositivo Citrix Gateway es el que gestiona la autenticación. Puede configurar StoreFront para permitir a los usuarios cambiar sus contraseñas después de iniciar sesión. Esta funcionalidad solo está disponible cuando se accede a los almacenes de StoreFront a través de la aplicación Citrix Workspace para HTML5, no a través de las aplicaciones Citrix Workspace instaladas localmente.

La configuración predeterminada de StoreFront impide que los usuarios cambien sus contraseñas aunque estas hayan caducado. Si decide habilitar esta función, asegúrese de que las directivas para los dominios que contengan los servidores no impidan a los usuarios cambiar sus contraseñas.

Cuando se permite a los usuarios cambiar las contraseñas, algunas funciones importantes de seguridad se dejan a merced de cualquier persona que pueda acceder a los almacenes a través del servicio de autenticación. Si su organización cuenta con una directiva de seguridad que solo permite utilizar las funciones de cambio de contraseñas de los usuarios para uso interno, asegúrese de que no se pueda acceder a los almacenes desde fuera de la red corporativa.

1. En la ventana **Administrar métodos de autenticación**, en el menú desplegable **PassThrough desde Citrix Gateway** > **Parámetros**, seleccione **Administrar opciones de contraseña**.
2. Para permitir que los usuarios cambien las contraseñas, marque **Permitir a los usuarios cambiar sus contraseñas**.

> **Nota:**
>
> Si selecciona o desactiva **Permitir a los usuarios cambiar sus contraseñas**, eso también afectará a los parámetros de **Administrar opciones de contraseña** para la autenticación con Nombre de usuario y contraseña.

SDK de PowerShell

Para modificar las opciones de cambio de contraseña mediante el SDK de PowerShell, use el cmdlet Set-STFExplicitCommonOptions.

Configurar Delivery Controller para que confíe en StoreFront

Cuando Citrix Gateway está configurado con la autenticación LDAP, transfiere las credenciales a StoreFront. Para otros métodos de autenticación, StoreFront no tiene acceso a las credenciales, por lo que no puede autenticarse en Citrix Virtual Apps and Desktops. Por lo tanto, debe configurar Delivery Controller para que confíe en las solicitudes de StoreFront. Consulte Consideraciones y prácticas recomendadas de seguridad de Citrix Virtual Apps and Desktops.

Single Sign-On en los VDA mediante Servicio de autenticación federada

Cuando la puerta de enlace se configura con la autenticación LDAP, pasa las credenciales a StoreFront para que pueda iniciar sesión con Single Sign-On en los VDA. Para otros métodos de autenticación, StoreFront no tiene acceso a las credenciales, por lo que Single Sign-On no está disponible de forma predeterminada. Puede usar el Servicio de autenticación federada para proporcionar Single Sign-On.

Autenticación SAML

February 26, 2024

SAML (Security Assertion Markup Language) es un estándar abierto utilizado por los productos de identidad y autenticación. Con SAML, puede configurar StoreFront para redirigir a los usuarios a un proveedor de identidades externo para la autenticación.

> **Nota**
>
> Configure StoreFront con la autenticación SAML para el acceso interno. Para el acceso externo, configure Citrix Gateway con la autenticación SAML y, a continuación, configure StoreFront con la autenticación PassThrough de Gateway.

StoreFront requiere un proveedor de identidades (IdP) compatible con SAML 2.0, como:

- Microsoft AD Federation Services utilizan enlaces SAML (no enlaces de WS-Federation). Para obtener más información, consulte AD FS Deployment y AD FS Operations.
- Citrix Gateway (configurado como IDP).
- ID de Microsoft Entra. Para obtener más información, consulte CTX237490.

La aserción SAML debe contener un atributo `saml:Subject` que contenga el UPN del usuario.

Para habilitar o inhabilitar la autenticación SAML en un almacén al conectarse a través de aplicaciones de Workspace, en la ventana Métodos de autenticación, seleccione **Autenticación SAML**. Al habilitar la autenticación SAML de un almacén de forma predeterminada, también se habilita para todos los sitios web de ese almacén. Puede configurar SAML de forma independiente para un sitio web concreto en la ficha Métodos de autenticación.

Dispositivos finales SAML de StoreFront

Para configurar SAML, su proveedor de identidades puede necesitar estos dispositivos de punto final:

- La URL del ID de entidad. Esta es la ruta al servicio de autenticación del almacén, normalmente https://[host de StoreFront]/Citrix/[nombre de almacén]Auth
- La URL de Assertion Consumer Service, normalmente https://[host de StoreFront]/Citrix/[nombre de almacén]Auth/SamlForms/AssertionConsumerService
- El servicio de metadatos, normalmente https://[host de StoreFront]/Citrix/[nombre de almacén]Auth/SamlForms/ServiceProvider/Metadata

Además, hay un dispositivo de punto final de prueba, normalmente https://[host de StoreFront]/Citrix/[nombre de almacén]Auth/SamlTest

Puede usar este script de PowerShell para enumerar los dispositivos de punto final de un almacén específico.

```
# Change this value for your Store
$storeVirtualPath = "/Citrix/Store"

$auth = Get-STFAuthenticationService -Store (Get-STFStoreService -
    VirtualPath $storeVirtualPath)
$spId = $auth.AuthenticationSettings["samlForms"].SamlSettings.
    ServiceProvider.Uri.AbsoluteUri
$acs = New-Object System.Uri $auth.Routing.HostbaseUrl, ($auth.
    VirtualPath + "/SamlForms/AssertionConsumerService")
$md = New-Object System.Uri $auth.Routing.HostbaseUrl, ($auth.
    VirtualPath + "/SamlForms/ServiceProvider/Metadata")
$samlTest = New-Object System.Uri $auth.Routing.HostbaseUrl, ($auth.
    VirtualPath + "/SamlTest")
Write-Host "SAML Service Provider information:
Entity ID: $spId
Assertion Consumer Service: $acs
Metadata: $md
Test Page: $samlTest
<!--NeedCopy-->
```

Ejemplo de salida:

```
SAML Service Provider information:
Entity ID: https://storefront.example.com/Citrix/StoreAuth
Assertion Consumer Service: https://storefront.example.com/Citrix/
    StoreAuth/SamlForms/AssertionConsumerService
Metadata: https://storefront.example.com/Citrix/StoreAuth/SamlForms/
    ServiceProvider/Metadata
Test Page: https://storefront.example.com/Citrix/StoreAuth/SamlTest
<!--NeedCopy-->
```

Configuración mediante el intercambio de metadatos

Para simplificar la configuración, puede intercambiar metadatos (identificadores, certificados, dispositivos de punto final y otras configuraciones) entre el proveedor de identidades y el proveedor de servicios, que en este caso es StoreFront.

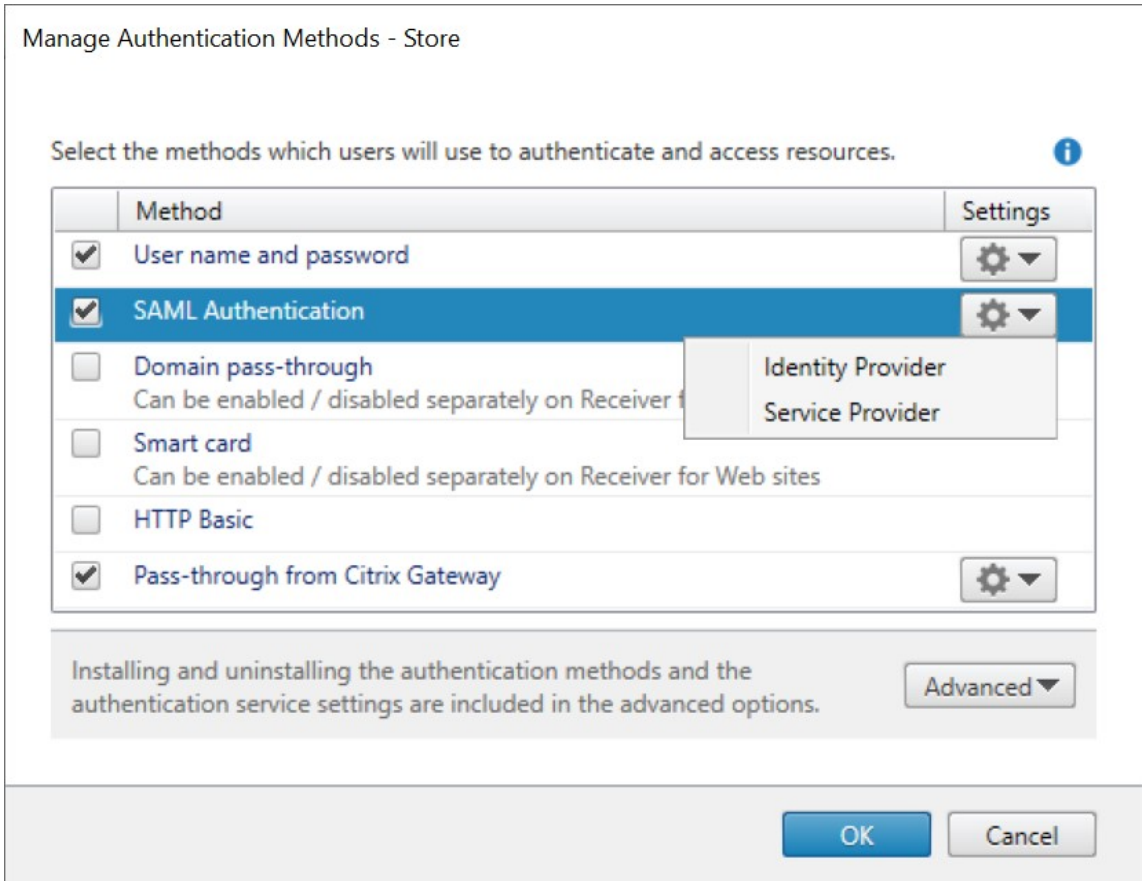
Si su proveedor de identidades admite la importación de metadatos, puede dirigirlo al dispositivo de punto final de metadatos de StoreFront. **Nota:** Esto debe llevarse a cabo a través de HTTPS.

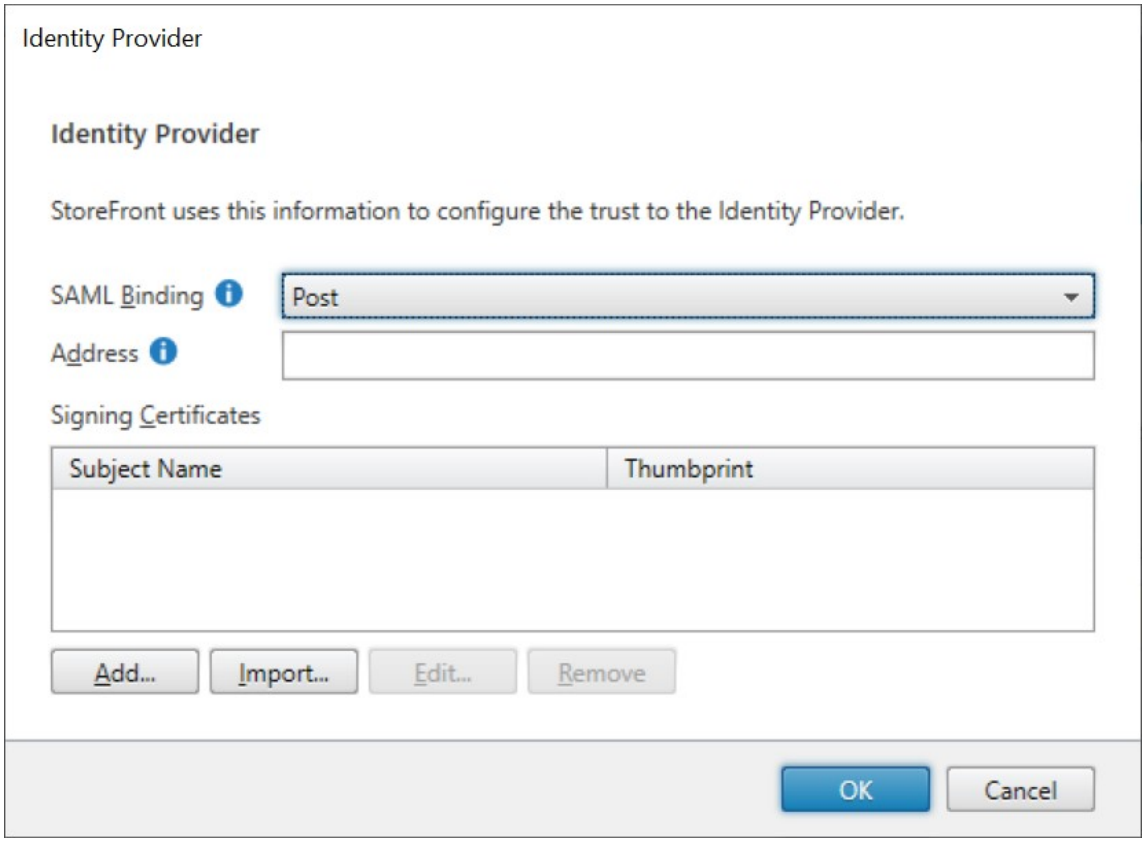
Para configurar StoreFront con los metadatos de un proveedor de identidades, utilice el cmdlet Update-STFSamlIdPFromMetadata. Por ejemplo:

```
Get-Module "Citrix.StoreFront*" -ListAvailable | Import-Module

# Remember to change this with the virtual path of your Store.
$StoreVirtualPath = "/Citrix/Store"

$store = Get-STFStoreService -VirtualPath $StoreVirtualPath
$auth = Get-STFAuthenticationService -StoreService $store

# To read the metadata directly from the Identity Provider, use the following:
# Note again this is only allowed for https endpoints
Update-STFSamlIdPFromMetadata -AuthenticationService $auth -Url https://example.com/FederationMetadata/2007-06/FederationMetadata.xml

# If the metadata has already been download, use the following:
# Note: Ensure that the file is encoded as UTF-8
Update-STFSamlIdPFromMetadata -AuthenticationService $auth -FilePath "C:\Users\exampleusername\Downloads\FederationMetadata.xml"
<!--NeedCopy-->
```

Configurar el proveedor de identidades

1. Haga clic en el menú desplegable de los parámetros de la fila **Autenticación SAML** y, a continuación, haga clic en **Proveedor de identidades**.

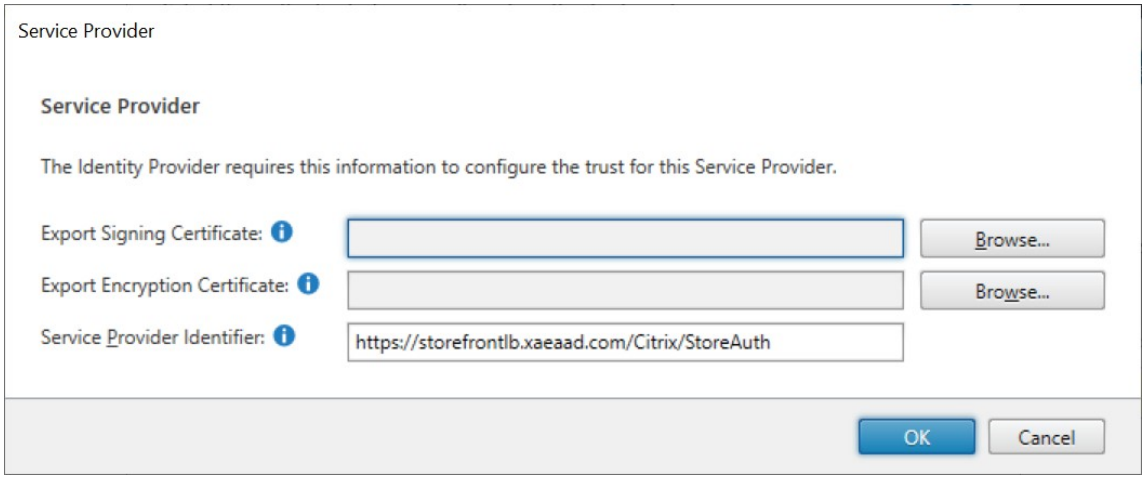




2. Elija **Enlace SAML** para **POST** o **Redirección**.
3. Introduzca la **dirección** del proveedor de identidades.
4. Importe el certificado utilizado para firmar los tokens SAML.
5. Presione **Aceptar** para guardar los cambios.

Configurar el proveedor de servicios

1. Haga clic en el menú desplegable de los parámetros de la fila **Autenticación SAML** y, a continuación, haga clic en **Proveedor de servicios**.



2. También puede elegir un **certificado de firma de exportación** que se utiliza para firmar mensajes en el proveedor de identidades.
3. También puede elegir un **certificado de cifrado de exportación** que se utiliza para descifrar mensajes recibidos del proveedor de identidades.
4. El **identificador del proveedor de servicios** viene prerrellenado con el servicio de autenticación del almacén.
5. Presione **Aceptar** para guardar los cambios.

SDK de PowerShell

Mediante el SDK de PowerShell:

- Para importar un certificado de firma, llame al cmdlet Import-STFSamlSigningCertificate.
- Para importar un certificado de cifrado, llame al cmdlet Import-STFSamlEncryptionCertificate.

Pruebas

Para probar la integración de SAML:

1. Vaya a la página de pruebas de SAML y consulte Dispositivos de punto final SAML de StoreFront.
2. Esto le redirigirá al proveedor de identidades. Introduzca sus credenciales.
3. Se le redirigirá de nuevo a la página de pruebas que muestra las aserciones y las reclamaciones de identidad.

Configurar Delivery Controller para que confíe en StoreFront

Al usar la autenticación SAML, StoreFront no tiene acceso a las credenciales del usuario, por lo que no puede autenticarse en Citrix Virtual Apps and Desktops. Por lo tanto, debe configurar Delivery

Controller para que confíe en las solicitudes de StoreFront. Consulte Consideraciones y prácticas recomendadas de seguridad de Citrix Virtual Apps and Desktops.

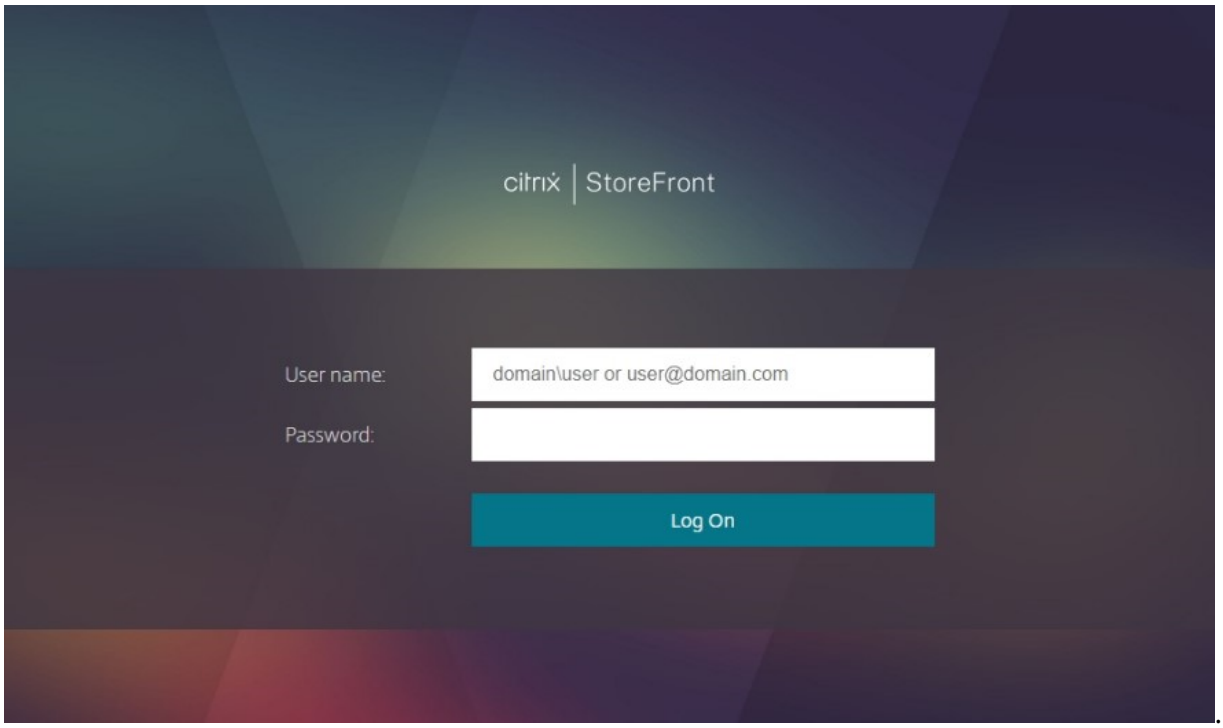
Single Sign-On en los VDA mediante Servicio de autenticación federada

Al usar la autenticación SAML, StoreFront no tiene acceso a las credenciales del usuario, por lo que Single Sign-On en los VDA no está disponible de forma predeterminada. Puede usar el Servicio de autenticación federada para proporcionar Single Sign-On.

Autenticación con nombre de usuario y contraseña

February 26, 2024

Con la autenticación con nombre de usuario y contraseña, los usuarios introducen sus credenciales de Active Directory.



Para habilitar o inhabilitar la autenticación con nombre de usuario y contraseña para un almacén al conectarse a través de aplicaciones Workspace, en la ventana Métodos de autenticación, marque o desmarque **Nombre de usuario y contraseña**.

Al habilitar la autenticación con nombre de usuario y contraseña para un almacén de forma predeterminada, también se habilita para todos los sitios web de ese almacén. Puede inhabilitar la aut-

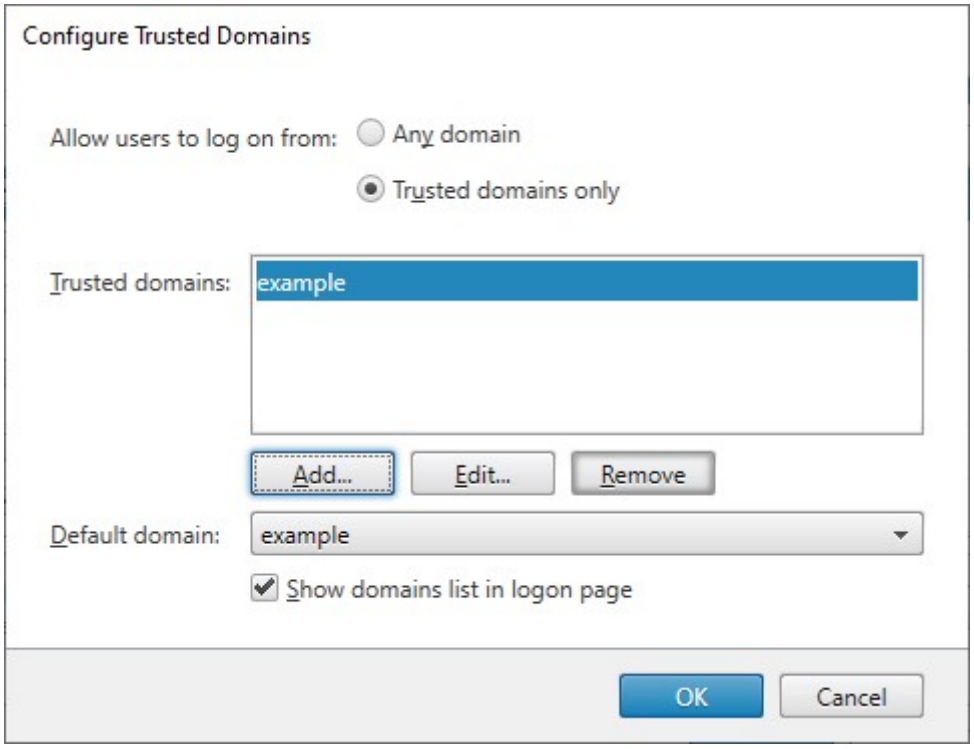
enticación con nombre de usuario y contraseña para un sitio web específico en la ficha Métodos de autenticación de Administrar un sitio de Receiver para Web.

Configurar dominios de usuarios de confianza

Puede restringir el acceso a los almacenes por parte de usuarios que inician sesión con credenciales de dominio explícitas, ya sea directamente o a través de la autenticación PassThrough desde Citrix Gateway.

1. Seleccione el nodo "Almacenes"en el panel izquierdo de la consola de administración de Citrix StoreFront y, en el panel de resultados, seleccione el método de autenticación apropiado. En el panel Acciones, haga clic en **Administrar métodos de autenticación**.
2. En la lista **Nombre de usuario y contraseña > Parámetros**, seleccione **Configurar dominios de confianza**.
3. Seleccione **Solo dominios de confianza** y haga clic en **Agregar** para introducir el nombre de un dominio de confianza. Los usuarios con cuentas en ese dominio pueden iniciar sesiones en todos los almacenes que usen el servicio de autenticación. Para modificar un nombre de dominio, seleccione la entrada correspondiente en Dominios de confianza y haga clic en **Modificar**. Para interrumpir el acceso a los almacenes para las cuentas de usuario en ese dominio, seleccione un dominio de la lista y haga clic en **Quitar**.

   La manera en que se especifica el nombre del dominio determina el formato en el que los usuarios deben introducir sus credenciales. Si quiere que los usuarios introduzcan sus credenciales en un formato de nombre de usuario de dominio, agregue el nombre NetBIOS a la lista. Para exigir que los usuarios introduzcan sus credenciales en el formato de nombre principal de usuario, agregue el FQDN a la lista. Si quiere permitir que los usuarios introduzcan sus credenciales en el formato de nombre de usuario de dominio y en el formato de nombre principal de usuario, debe agregar el nombre NetBIOS y el FQDN a la lista.
4. Si configura varios dominios de confianza, seleccione de la lista Dominio predeterminado el dominio que aparece seleccionado de forma predeterminada cuando los usuarios inician sesión en StoreFront.
5. Si quiere ver una lista de los dominios de confianza en la página de inicio de sesión, marque la casilla Mostrar lista de dominios en la página de inicio de sesión.



Permitir que los usuarios cambien sus contraseñas

Puede permitir que los usuarios cambien sus contraseñas cuando quieran. También puede restringir los cambios de contraseña a los usuarios cuyas contraseñas han caducado. De esta manera, los usuarios siempre podrán acceder a sus escritorios y aplicaciones, aunque su contraseña haya caducado.

La funcionalidad de cambio de contraseña está disponible en estos clientes:

Aplicaciones Citrix Workspace	El usuario puede cambiar una contraseña caducada si esta función está habilitada en StoreFront	Se notifica al usuario que la contraseña va a caducar	El usuario puede cambiar la contraseña antes de que caduque si esta función está habilitada en StoreFront
Windows	Sí		
Mac	Sí		
Android			
iOS			
Linux	Sí		
Web	Sí	Sí	Sí

Aplicaciones Citrix Workspace	El usuario puede cambiar una contraseña caducada si esta función está habilitada en StoreFront	Se notifica al usuario que la contraseña va a caducar	El usuario puede cambiar la contraseña antes de que caduque si esta función está habilitada en StoreFront

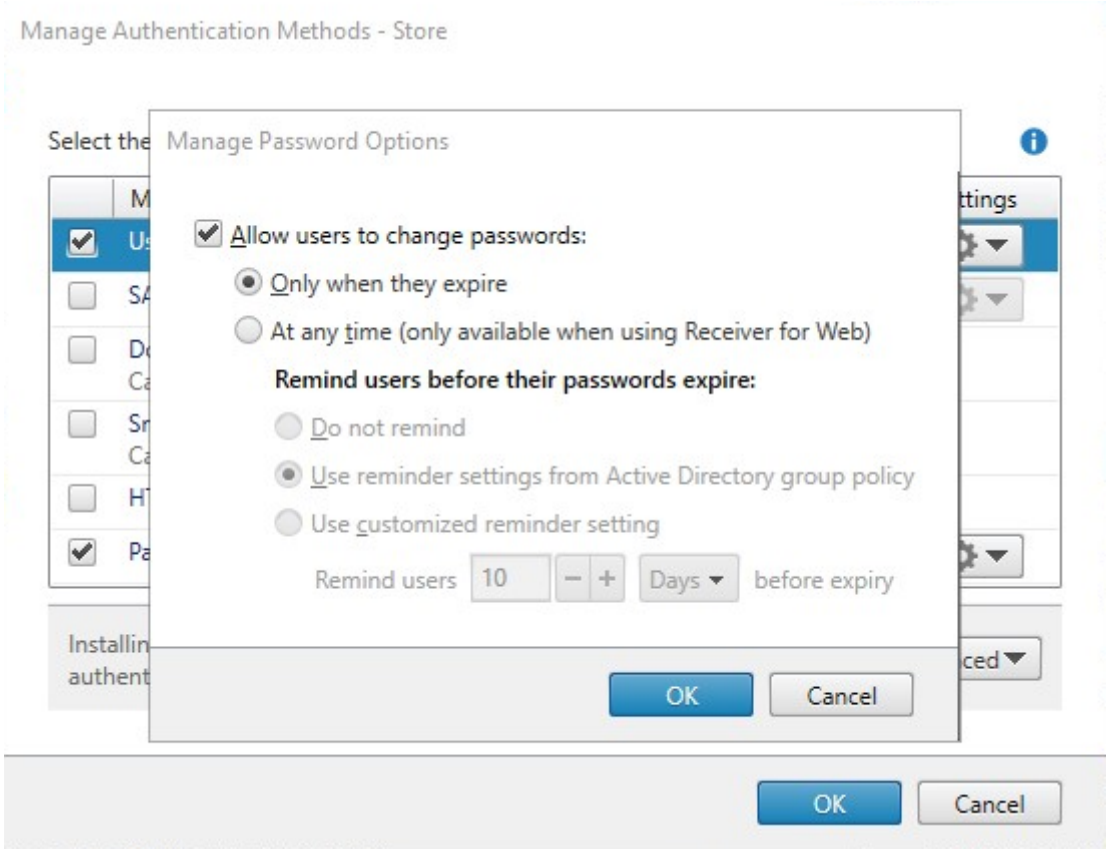
La configuración predeterminada impide que los usuarios de la aplicación Citrix Workspace y del explorador web cambien sus contraseñas aunque estas hayan caducado. Si decide habilitar esta función, asegúrese de que las directivas para los dominios que contengan los servidores no impidan a los usuarios cambiar sus contraseñas. Cuando se permite a los usuarios cambiar las contraseñas, algunas funciones importantes de seguridad se dejan a merced de cualquier persona que pueda acceder a los almacenes a través del servicio de autenticación. Si su organización cuenta con una directiva de seguridad que solo permite utilizar las funciones de cambio de contraseñas de los usuarios para uso interno, asegúrese de que no se pueda acceder a los almacenes desde fuera de la red corporativa.

Si permite que los usuarios cambien sus contraseñas en cualquier momento, los usuarios locales cuyas contraseñas están a punto de caducar reciben una advertencia cuando inician sesión. De forma predeterminada, el período de notificación para un usuario se determina mediante la configuración de directiva de Windows correspondiente. También puede configurar un período de notificación personalizado.

1. En la ventana **Administrar métodos de autenticación**, en el menú desplegable **Nombre de usuario y contraseña** > **Parámetros**, seleccione **Administrar opciones de contraseña**.
2. Para permitir que los usuarios cambien las contraseñas, marque **Allow users to change passwords**.

   > **Nota:**
   > Si no selecciona esta opción, deberá organizar cómo ofrecer asistencia a los usuarios que no puedan acceder a los escritorios y aplicaciones porque sus contraseñas hayan caducado.

3. Elija si permitir que los usuarios cambien las contraseñas **Solo cuando caduquen** o **En cualquier momento**.
4. Elija si enviar un recordatorio a los usuarios antes de que caduquen sus contraseñas.



Nota 1:

StoreFront no admite directivas específicas de contraseña (fine-grained) en Active Directory.

Nota 2:

Asegúrese de que haya suficiente espacio en disco en los servidores de StoreFront para almacenar los perfiles de todos los usuarios. Para comprobar si la contraseña de un usuario está a punto de caducar, StoreFront crea un perfil local para ese usuario en el servidor. StoreFront debe poder ponerse en contacto con el controlador de dominio para cambiar las contraseñas de los usuarios.

Nota 3:

Si habilita o inhabilita el cambio de contraseñas en cualquier momento, eso también afectará a los parámetros de **Administrar las opciones de contraseña** para la autenticación PassThrough desde Citrix Gateway.

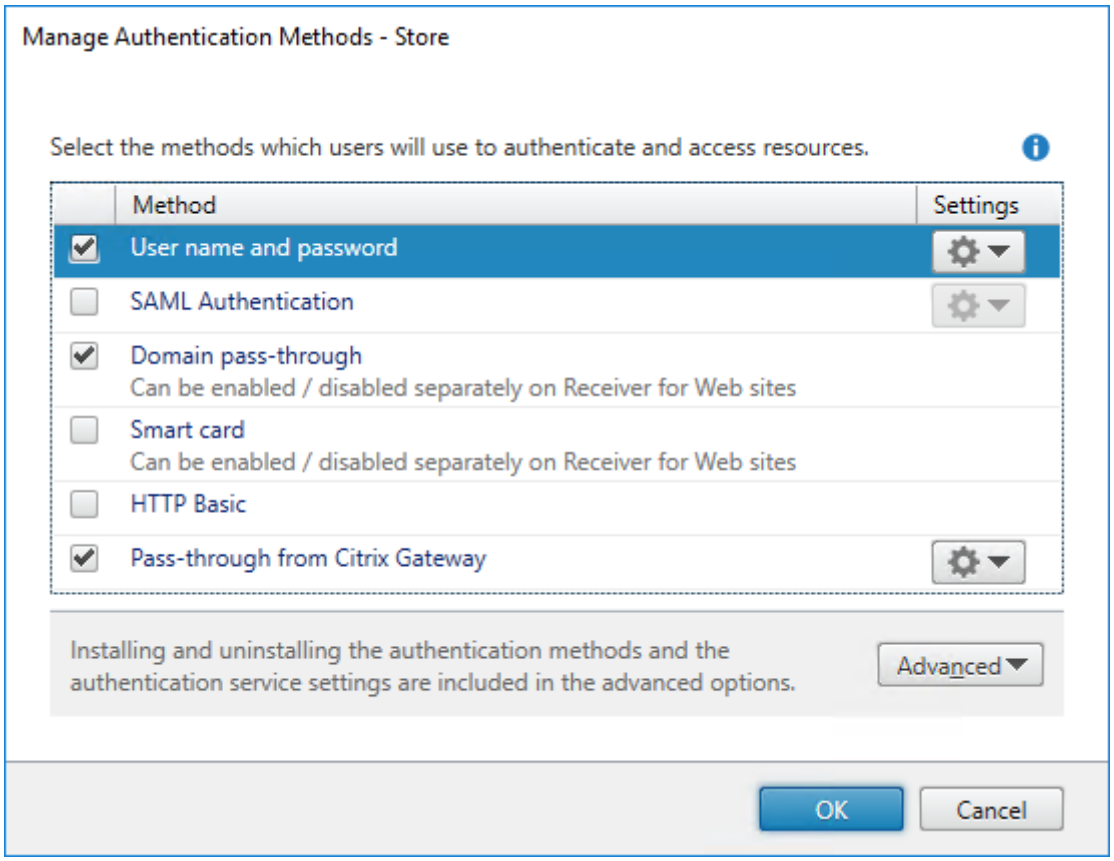
Validación de la contraseña en las credenciales

Normalmente, StoreFront se comunica directamente con Active Directory para validar las credenciales.

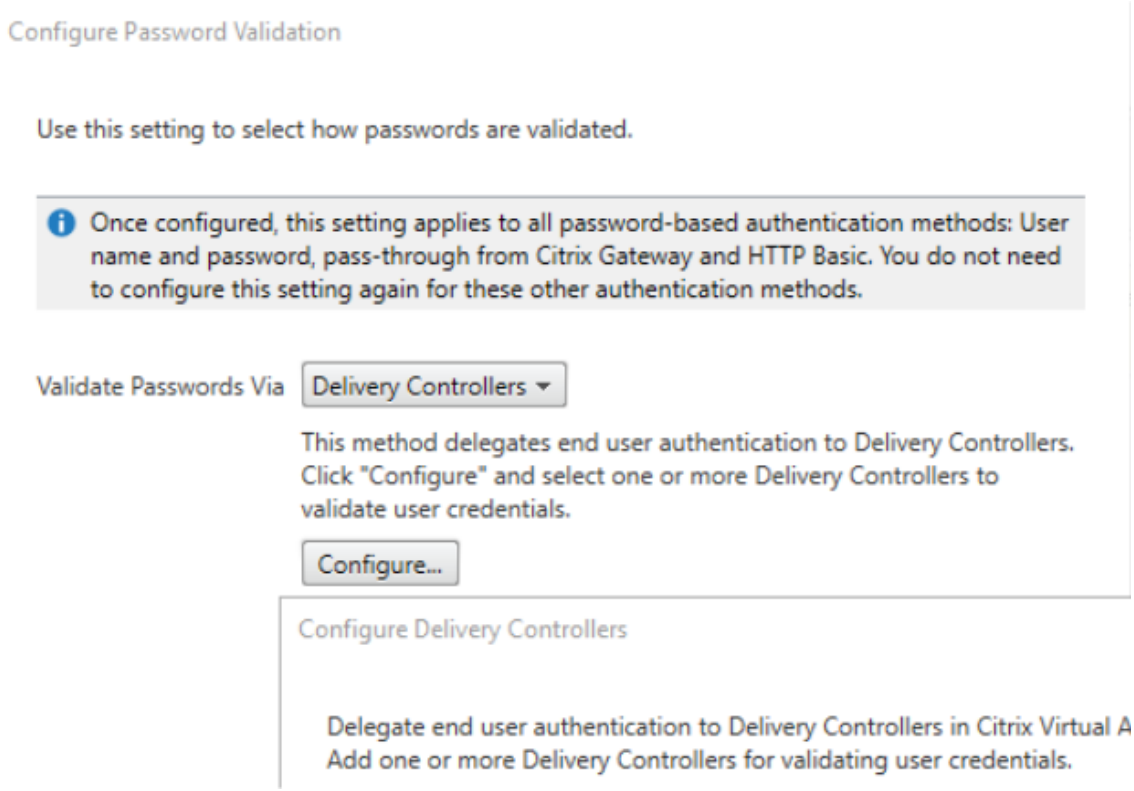
Si StoreFront no está en el mismo dominio que Citrix Virtual Apps and Desktops y no se pueden es-

tablecer relaciones de confianza de Active Directory, puede configurar StoreFront para que use Delivery Controllers de Citrix Virtual Apps and Desktops en la autenticación de las credenciales de nombre de usuario y contraseña de los usuarios:

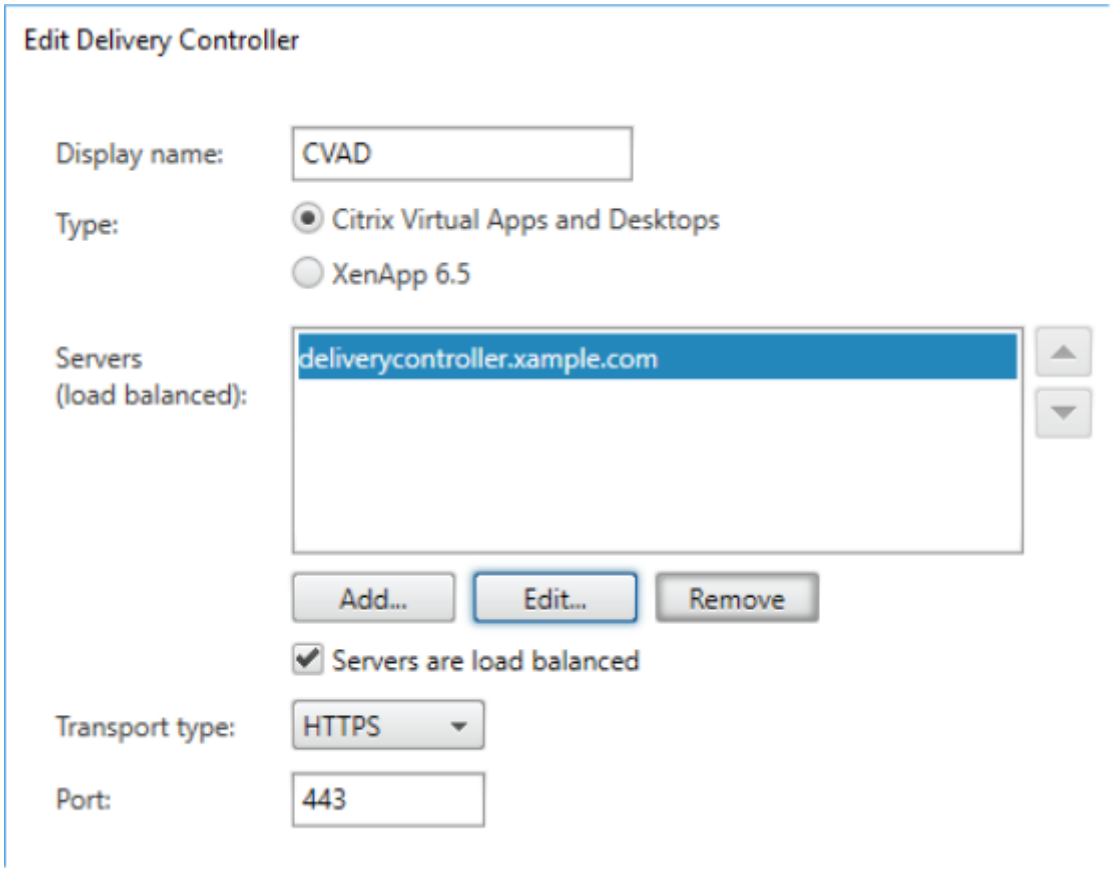
1. En la ventana **Administrar métodos de autenticación**, en el menú **Nombre de usuario y contraseña > Parámetros**, seleccione **Configurar validación de contraseñas**.



2. En la lista **Validar contraseñas mediante**, seleccione **Delivery Controllers** y haga clic en **Configurar**.



3. Siga las instrucciones de las pantallas **Configurar Delivery Controllers** para agregar uno o varios **Delivery Controllers** para validar las credenciales de usuario y haga clic en **Aceptar**.



Usar Active Directory

1. En la página **Administrar métodos de autenticación**, en el menú **Nombre de usuario y contraseña** > **Parámetros**, seleccione **Configurar validación de contraseñas**.
2. En el menú desplegable **Validar contraseñas mediante**, seleccione **Active Directory** y haga clic en **Aceptar**.

Single Sign-On en los VDA

Cuando los usuarios inician un recurso, StoreFront usa las credenciales que el usuario usó para iniciar sesión en el almacén para iniciar sesión con Single Sign-On en los VDA.

Personalizar la pantalla de inicio de sesión

La pantalla de inicio de sesión se genera a partir de una plantilla, que normalmente se encuentra en C:\inetpub\wwwroot\Citrix\[Nombre del almacén]Auth\App_Data\Templates\ UsernamePassword.tfrm. Puede personalizar la pantalla.

Texto de título

De forma predeterminada, cuando los usuarios inician sesión en un almacén, no se muestra ningún texto de título en el cuadro de diálogo de inicio de sesión. Es posible mostrar el texto "Please log on" o redactar un mensaje personalizado propio:

1. Use un editor de texto para abrir el archivo UsernamePassword.tfrm del servicio de autenticación.
2. Busque las siguientes líneas en el archivo.

```
@* @Heading("ExplicitAuth:AuthenticateHeadingText") *@
<!--NeedCopy-->
```

3. Quite la marca de comentario de la instrucción eliminando los elementos iniciales y finales **@*** y ***@**.

```
@Heading("ExplicitAuth:AuthenticateHeadingText")
<!--NeedCopy-->
```

   Los usuarios de la aplicación Citrix Workspace ven el texto de título predeterminado "Please log on"o la versión localizada de este texto cuando inician sesión en los almacenes donde se utiliza este servicio de autenticación.

4. Para modificar el texto de título, utilice un editor de texto para abrir el archivo *ExplicitFormsCommon.xx.resx* del servicio de autenticación, que suele estar en el directorio C:\inetpub\wwwroot\Citrix\[Nombre del almacén]Auth\App_Data\resources\.
5. Localice los siguientes elementos en el archivo. Modifique el texto escrito dentro del elemento <value> para modificar el texto del título que los usuarios ven en el cuadro de diálogo de inicio de sesión al acceder a almacenes en los que se utiliza este servicio de autenticación.

```
<data name="AuthenticateHeadingText" xml:space="preserve">
    <value>My Company Name</value>
</data>
<!--NeedCopy-->
```

   Para modificar el texto de título del cuadro de diálogo de inicio de sesión para los usuarios con otras configuraciones regionales, modifique los archivos *ExplicitAuth.languagecode.resx* traducidos, donde **languagecode** es el identificador de configuración regional.

Impedir que la aplicación Citrix Workspace para Windows almacene en caché contraseñas y nombres de usuario

De manera predeterminada, la aplicación Citrix Workspace para Windows almacena las contraseñas de los usuarios cuando inician sesión en los almacenes de StoreFront. Para evitar que la aplicación

Citrix Workspace para Windows almacene en caché las contraseñas de los usuarios, modifique los archivos del servicio de autenticación.

1. Use un editor de texto para abrir el archivo inetpub\wwwroot\Citrix\[Nombre del almacén]Auth\App_Data\Templates\UsernamePassword.tfrm.
2. Busque la siguiente línea en el archivo.

```
@SaveCredential(id: @GetTextValue("saveCredentialsId"), labelKey:
    "ExplicitFormsCommon:SaveCredentialsLabel", initiallyChecked:
    ControlValue("SaveCredentials"))
<!--NeedCopy-->
```

3. Comente la instrucción como se muestra a continuación.

```
<!-- @SaveCredential(id: @GetTextValue("saveCredentialsId"),
    labelKey: "ExplicitFormsCommon:SaveCredentialsLabel",
    initiallyChecked: ControlValue("SaveCredentials")) -->
<!--NeedCopy-->
```

   Los usuarios deben introducir sus contraseñas cada vez que inician sesión en almacenes que utilizan este servicio de autenticación.

   De manera predeterminada, la aplicación Citrix Workspace para Windows rellena el formulario automáticamente con el último nombre de usuario que se utilizó. Para evitar que se rellene el campo de nombre de usuario o para usar otro mecanismo para suprimir el almacenamiento en caché de contraseñas, consulte Impedir que la aplicación Citrix Workspace para Windows almacene en caché contraseñas y nombres de usuario.

Acceso remoto a través de Citrix Gateway

Puede configurar su Citrix Gateway para que los usuarios inicien sesión en la puerta de enlace con su nombre de usuario y contraseña de dominio. Estas credenciales se transfieren a StoreFront para iniciar sesión en el almacén. Para configurar Citrix Gateway para la autenticación de nombre de usuario y contraseña de LDAP, consulte en la documentación de NetScaler: Autenticación LDAP. Para configurar StoreFront, consulte PassThrough desde Citrix Gateway.

Configuración del Servicio de autenticación federada

April 17, 2024

Al usar métodos de autenticación como SAML, en los que el usuario no introduce sus credenciales directamente en la aplicación Citrix Workspace, de forma predeterminada no es posible usar Single

Sign-On en los VDA. En estos casos, puede usar el Servicio de autenticación federada (FAS) para proporcionar Single Sign-On a los VDA mediante la autenticación de certificados.

Para usar FAS con StoreFront, debe configurar StoreFront con el SDK de PowerShell. Use Set-STFClaimsFactoryNames para configurar la fábrica de reclamaciones en `FASClaimsFactory` y use Set-STFStoreLaunchOptions para configurar el proveedor de datos de inicio de sesión de los VDA en `FASLogonDataProvider`.

Por ejemplo, para habilitar FAS en un almacén:

```
$store = Get-STFStoreService -VirtualPath [VirtualPath]
$auth = Get-STFAuthenticationService -StoreService $store
Set-STFClaimsFactoryNames -AuthenticationService $auth -
    ClaimsFactoryName "FASClaimsFactory"
Set-STFStoreLaunchOptions -StoreService $store -VdaLogonDataProvider "
    FASLogonDataProvider"
<!--NeedCopy-->
```

Para inhabilitar FAS en un almacén:

```
$store = Get-STFStoreService -VirtualPath [VirtualPath]
$auth = Get-STFAuthenticationService -StoreService $store
Set-STFClaimsFactoryNames -AuthenticationService $auth -
    ClaimsFactoryName "standardClaimsFactory"
Set-STFStoreLaunchOptions -StoreService $store -VdaLogonDataProvider ""
<!--NeedCopy-->
```

Sustituya `[VirtualPath]` por la ruta virtual apropiada. Por ejemplo: `/Citrix/Store`.

Para configurar la lista de servidores de FAS y otros parámetros, debe usar la directiva de grupo. Para obtener más información detallada, consulte la documentación de FAS.

FAS no se usa cuando se autentica mediante PassThrough de dominio o tarjeta inteligente a través de un explorador.

Falta de disponibilidad del servidor de FAS

Si no está disponible el servidor de FAS, de forma predeterminada se produce un error al iniciar. Sin embargo, puede configurar StoreFront de forma que, si el servidor de FAS no está disponible, los usuarios puedan iniciar sesión en el VDA introduciendo sus credenciales. Para cambiar la configuración, use el cmdlet Set-STFStoreLaunchOptions de PowerShell con el parámetro `FederatedAuthenticationServiceFailover`. Por ejemplo, para habilitar la conmutación por error en un almacén:

```
$storeService = Get-STFStoreService -VirtualPath [VirtualPath]
Set-STFStoreLaunchOptions $storeService -
    FederatedAuthenticationServiceFailover $True
<!--NeedCopy-->
```


Configurar y administrar almacenes

September 27, 2023

En Citrix StoreFront, puede crear y administrar almacenes que combinan escritorios y aplicaciones desde Citrix Virtual Apps and Desktops, con lo que ofrecerá a los usuarios un acceso de autoservicio y a demanda a los recursos.

Tarea	Detalles
Crear un almacén	Configura tantos almacenes adicionales como se necesiten.
Configurar un almacén	Configurar los parámetros de almacén
Quitar un almacén	Quite los almacenes innecesarios.
Exportar archivos de aprovisionamiento de almacenes para los usuarios	Genera archivos que contengan datos de conexión a los almacenes, incluidas las implementaciones de Citrix Gateway y las balizas configuradas para los almacenes.
Anunciar y ocultar almacenes para los usuarios	Evita que se muestren los almacenes a los usuarios y, por tanto, que los puedan agregar a sus cuentas cuando configuren la aplicación Citrix Workspace mediante la detección de cuentas basada en direcciones de correo electrónico o FQDN.
Configurar la delegación Kerberos	Configure si StoreFront usa la delegación Kerberos para autenticarse en Delivery Controllers.
Administrar los recursos disponibles en los almacenes	Agrega y quita recursos de los almacenes.
Administrar el acceso remoto a los almacenes a través de Citrix Gateway	Configura el acceso a los almacenes a través de Citrix Gateway para los usuarios que se conectan desde redes públicas.
la comprobación de listas de revocación de certificados (CRL)	Configure StoreFront para que este compruebe el estado de los certificados TLS que utilizan los utilizados los controladores de entrega de CVAD mediante una lista de revocación de certificados (CRL) publicada.

Tarea	Detalles
Configurar dos almacenes de StoreFront para compartir un almacén de datos de suscripción común	Configure dos almacenes de StoreFront para compartir un almacén de datos de suscripción común.
Habilitar o inhabilitar favoritos	Habilita o inhabilita los favoritos del almacén.
Administrar datos de suscripción a un almacén	Vea, importe, exporte y borre los datos de suscripción (favoritos).
Configurar dos almacenes de StoreFront para compartir un almacén de datos de suscripción común	Configura dos almacenes para que compartan una base de datos de suscripción común.
Almacenar datos de favoritos con Microsoft SQL Server	Utilice una base de datos de SQL Server externa para almacenar datos de suscripción (favoritos).
Configuración de Citrix Virtual Apps and Desktops	Configurar los parámetros de Citrix Virtual Apps and Desktops que afectan a la forma en que se muestran los recursos en el sitio web del almacén
Parámetros avanzados de los almacenes	Configura los parámetros avanzados de los almacenes.
Redirección óptima de HDX	Configura qué puerta de enlace se usa para conectarse a los distintos recursos.
Parámetros ICA predeterminados	Configura los parámetros de HDX agregándolos a default.ica
ICA File Signing	Configura la firma de archivos ICA
Accesos directos de Windows	Configura la forma en que la aplicación Citrix Workspace para Windows crea los accesos directos a las aplicaciones favoritas y obligatorias en el menú Inicio y el escritorio.

Crear almacén

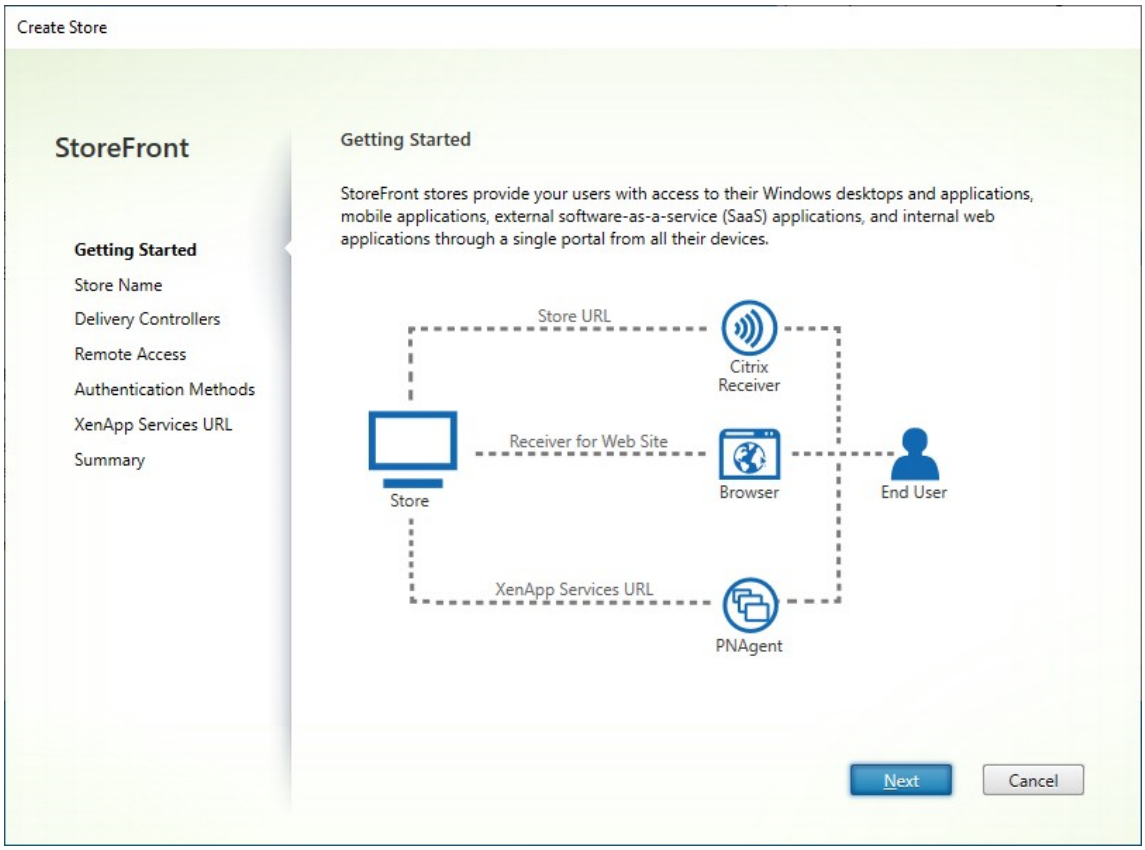
December 4, 2023

Puede crear tantos almacenes como necesite. Por ejemplo: puede crear un almacén para un determinado grupo de usuarios o para agrupar un conjunto específico de recursos.

> Importante:
>
> En implementaciones con varios servidores, use solo un servidor a la vez para hacer cambios en la configuración del grupo de servidores. Compruebe que la consola de administración de Citrix StoreFront no se está ejecutando en ninguno de los demás servidores de la implementación. Una vez completados,
> propague los cambios de configuración al grupo de servidores de modo que los demás servidores de la implementación se actualicen.

Para crear un almacén, identifique y configure las comunicaciones con los servidores que ofrecen los recursos que quiere entregar desde ese almacén. A continuación, opcionalmente, configure el acceso remoto al almacén a través de Citrix Gateway.

1. En el panel de acciones, haga clic en **Crear almacén**.

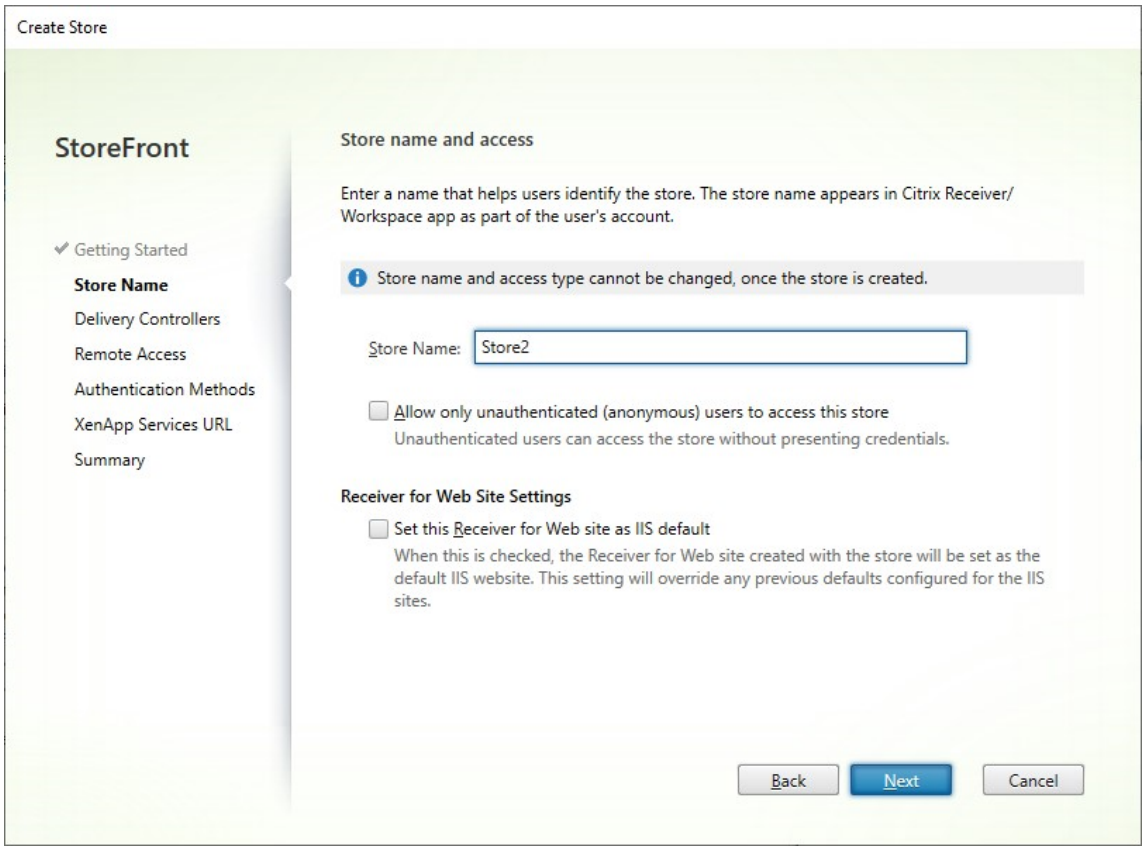


   Haga clic en **Siguiente**.

2. En la ficha **Nombre de almacén**, complete lo siguiente:

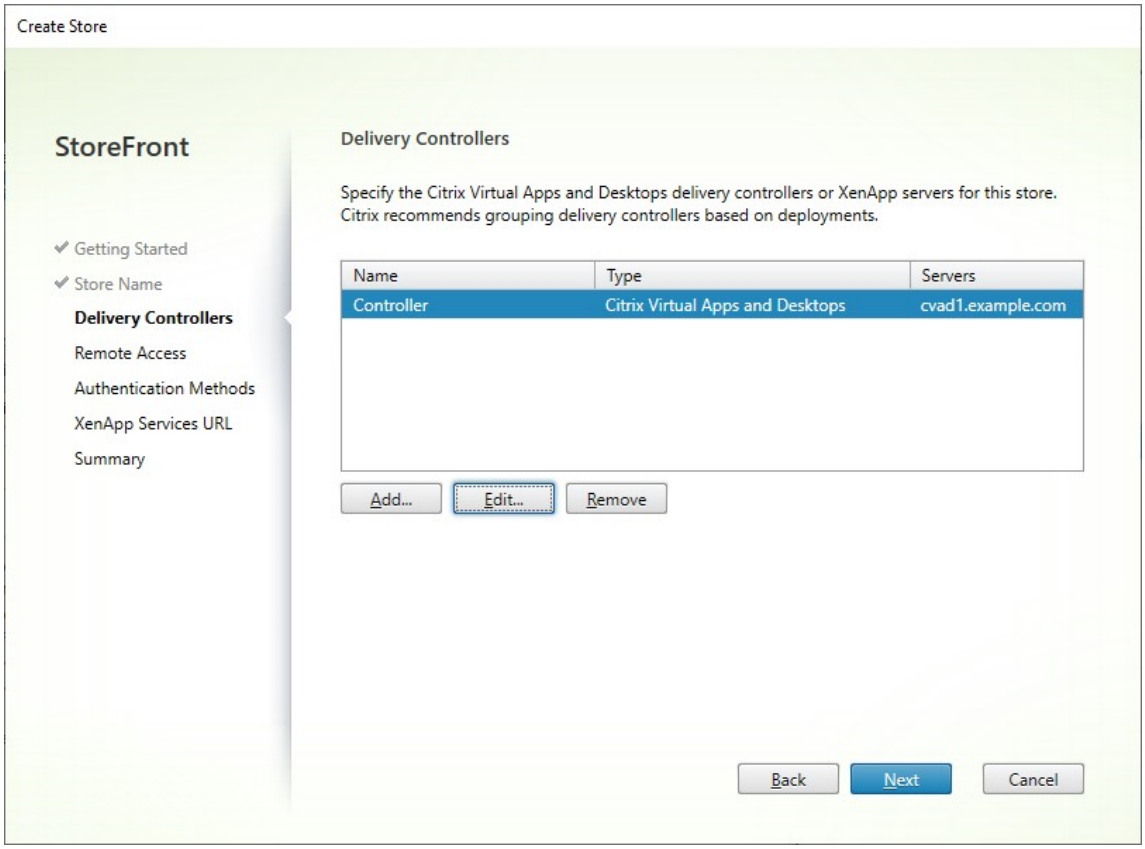
   - Introduce un nombre de almacén.
   - Si quiere permitir que los usuarios accedan al almacén de forma anónima o sin autenticarse, marque **Permitir al acceso a este almacén solo a usuarios no autenticados**.

Cuando se crea un almacén no autenticado, las páginas **Métodos de autenticación** y **Acceso remoto** no están disponibles, mientras que **Nodo de grupo de servidores** situado a la izquierda y el panel Acciones se reemplazan por **Cambiar URL base**. (Esta es la única opción disponible porque los grupos de servidores no están disponibles en servidores que no están unidos a un dominio).



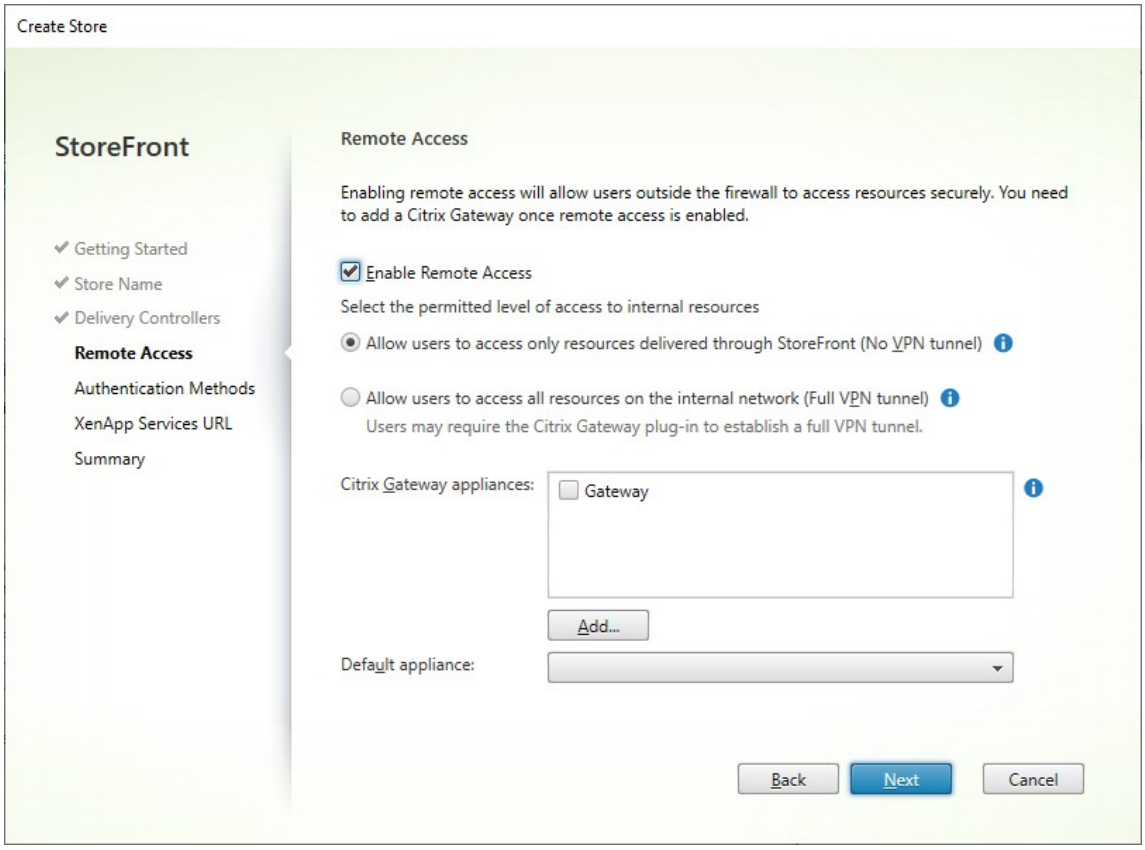
Haga clic en **Siguiente**.

3. En la ficha **Delivery Controllers**, agregue feeds de recursos para sus escritorios y aplicaciones virtuales. Para obtener más detalles, consulte Administrar los recursos disponibles en los almacenes.



Haga clic en **Siguiente**.

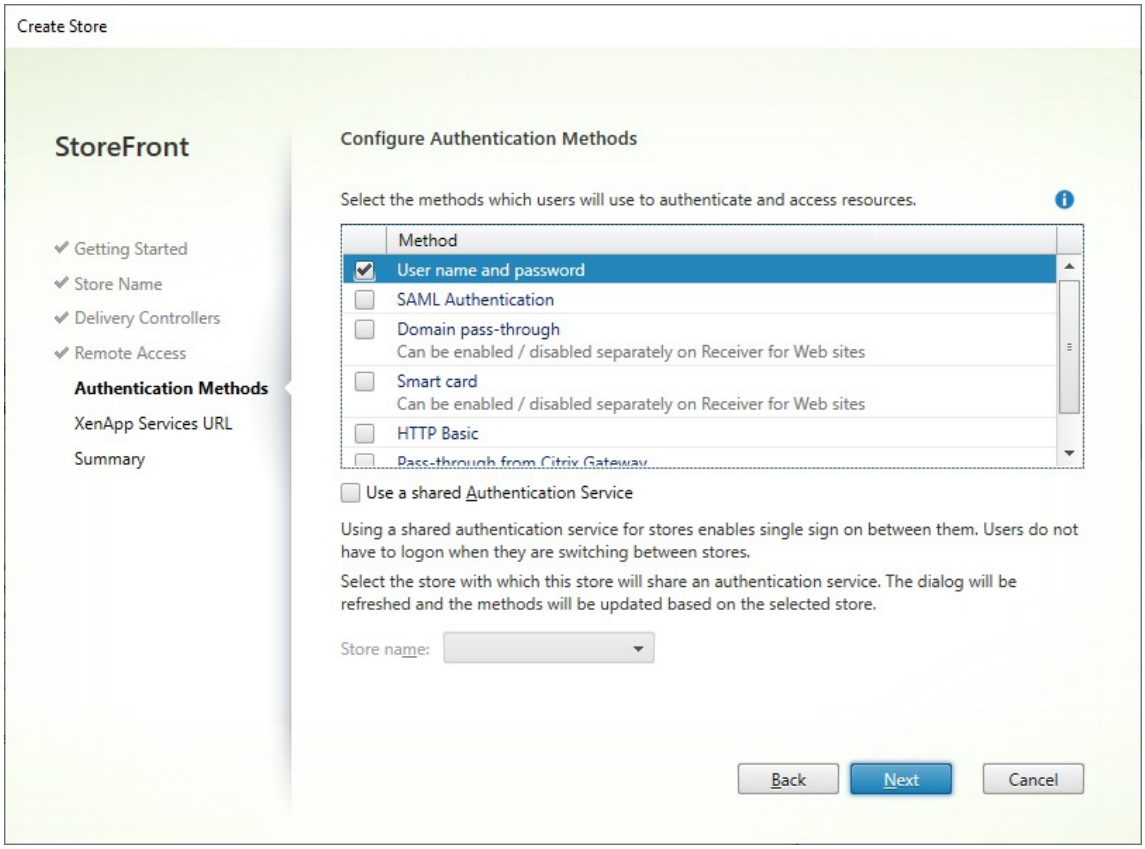
4. En la ficha **Acceso remoto**, elija si quiere que el almacén esté disponible a través de un dispositivo Citrix Gateway. Para obtener más detalles, consulte Administrar el acceso remoto a los almacenes a través de Citrix Gateway.



5. En la ficha **Métodos de autenticación**, seleccione los métodos que utilizarán los usuarios para autenticarse y acceder al almacén, y haga clic en **Siguiente**.

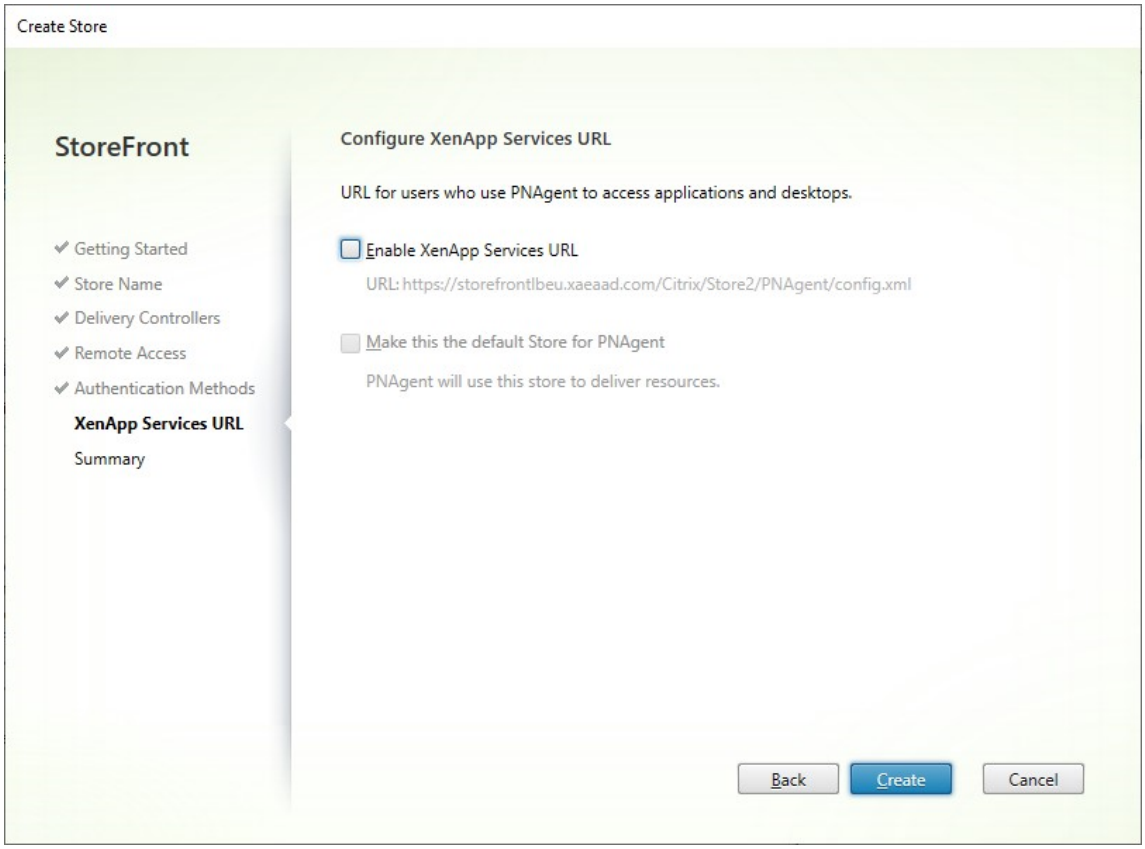
   Para obtener más detalles sobre los métodos de autenticación disponibles, consulte Configurar autenticación.

   En lugar de configurar métodos de autenticación por separado para este almacén, es posible compartir la configuración de autenticación con otro almacén. Para ello, marque **Usar un servicio de autenticación compartido** y, a continuación, seleccione un almacén existente.



Haga clic en **Siguiente**.

6. En la ficha **URL de XenApp Services**, si tiene dispositivos antiguos que requieren PNAgent, deje marcada la opción **Habilitar URL de XenApp Services**. De lo contrario, desmárquela.



Haga clic en **Crear**.

7. Después de haber creado el almacén, haga clic en **Finalizar**.

Al crear un almacén, también se crea un sitio web para permitir a los usuarios acceder al almacén. Puede configurar este sitio web o crear sitios web adicionales.

SDK de PowerShell

Para crear un almacén con el SDK de PowerShell:

1. Cree un servicio de autenticación mediante Add-STFAuthenticationService. Por convención, la ruta virtual suele ser `/Citrix/[StoreName]Auth`. Como alternativa, puede obtener un servicio de autenticación existente mediante Get-STFAuthenticationService. Este paso no es obligatorio para almacenes anónimos.
2. Configure el servicio de autenticación según sea necesario. Consulte Configurar la autenticación.
3. Llame a Add-STFStoreService.
   - Elija una ruta virtual para el almacén y establézcala como el parámetro `-VirtualPath`. Normalmente es /Citrix/[nombre de almacén].

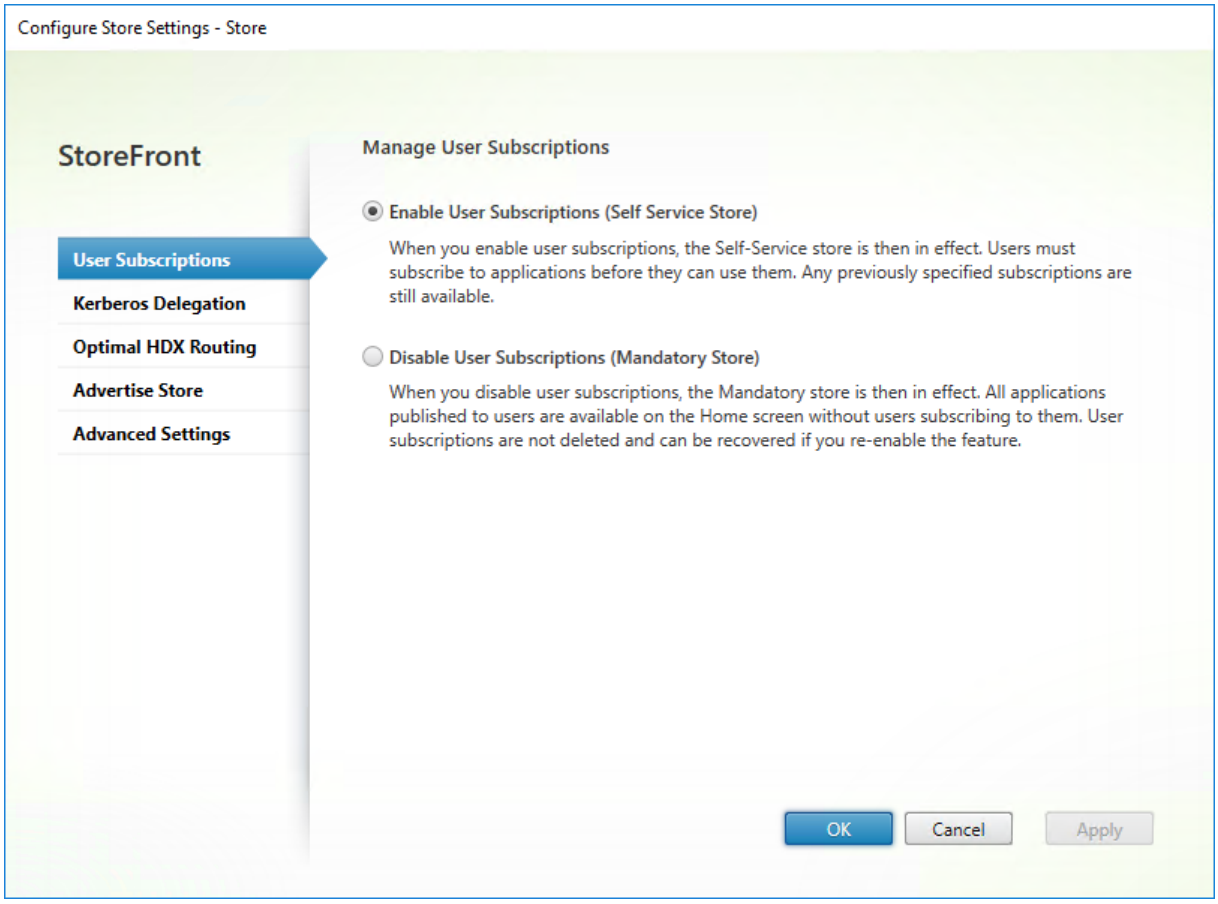
- Configure `-AuthenticationService` en el servicio de autenticación creado en el paso 1. Como alternativa, para un almacén anónimo, configure `-Anonymous $True`.
- Puede incluir los detalles de un feed de recursos. Cualquier feed de recursos adicional debe configurarse por separado.

Configurar un almacén

August 15, 2023

Para modificar un almacén:

1. Seleccione el nodo **Almacenes** en el panel izquierdo de la consola de administración de Citrix StoreFront y, en el panel **Acciones**, haga clic en **Configurar parámetros del almacén**.
2. Vaya a la ficha Suscripciones de usuarios para configurar si los favoritos están habilitados.
3. Vaya a la ficha Delegación Kerberos para configurar si el almacén usa la delegación Kerberos para autenticarse en el Delivery Controller.
4. Vaya a la ficha Redirección óptima de HDX para configurar qué puerta de enlace se utiliza para iniciar aplicaciones y escritorios según su ubicación.
5. Vaya a la ficha Anunciar almacén para configurar si la aplicación Workspace presenta el almacén a los usuarios cuando estos introducen el FQDN o la dirección de correo electrónico.

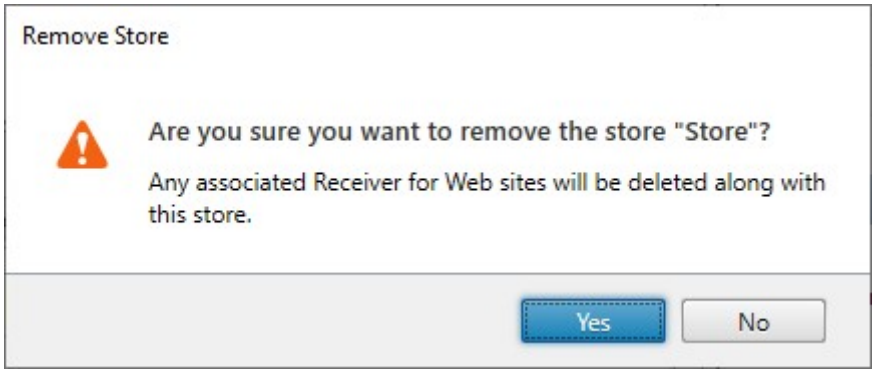


Quitar un almacén

August 15, 2023

Para quitar un almacén:

1. Seleccione el nodo **Almacenes** en el panel izquierdo de la consola de administración de Citrix StoreFront.
2. En el panel **Acciones**, haga clic en **Quitar almacén**.
3. En la ventana de confirmación, haga clic en **Sí**.



Al quitar un almacén, también se quitan todos los sitios web asociados.

Exportar archivos de aprovisionamiento de almacenes para los usuarios

January 26, 2024

Puede generar archivos que contengan datos de conexión a los almacenes, incluidas las implementaciones de Citrix Gateway y las balizas configuradas para los almacenes. Ponga estos archivos a disposición de los usuarios para permitirles que configuren la aplicación Citrix Workspace automáticamente con la información de los almacenes. Los usuarios también pueden descargar los archivos de aprovisionamiento de la aplicación Citrix Workspace al acceder a un almacén a través de un explorador web.

> Importante:
>
> En implementaciones con varios servidores, use solo un servidor a la vez para hacer cambios en la configuración del grupo de servidores. Compruebe que la consola de administración de Citrix StoreFront no se está ejecutando en ninguno de los demás servidores de la implementación. Una vez completados,
> propague los cambios de configuración al grupo de servidores de modo que los demás servidores de la implementación se actualicen.

1. Para generar un archivo de aprovisionamiento que contenga información de varios almacenes, en el panel Acciones haga clic en **Exportar archivo de aprovisionamiento multialmacén** y seleccione los almacenes que quiera incluir en el archivo.
2. Haga clic en **Exportar** y en **Guardar** para guardar el archivo de aprovisionamiento con la extensión CR en una ubicación adecuada de la red.

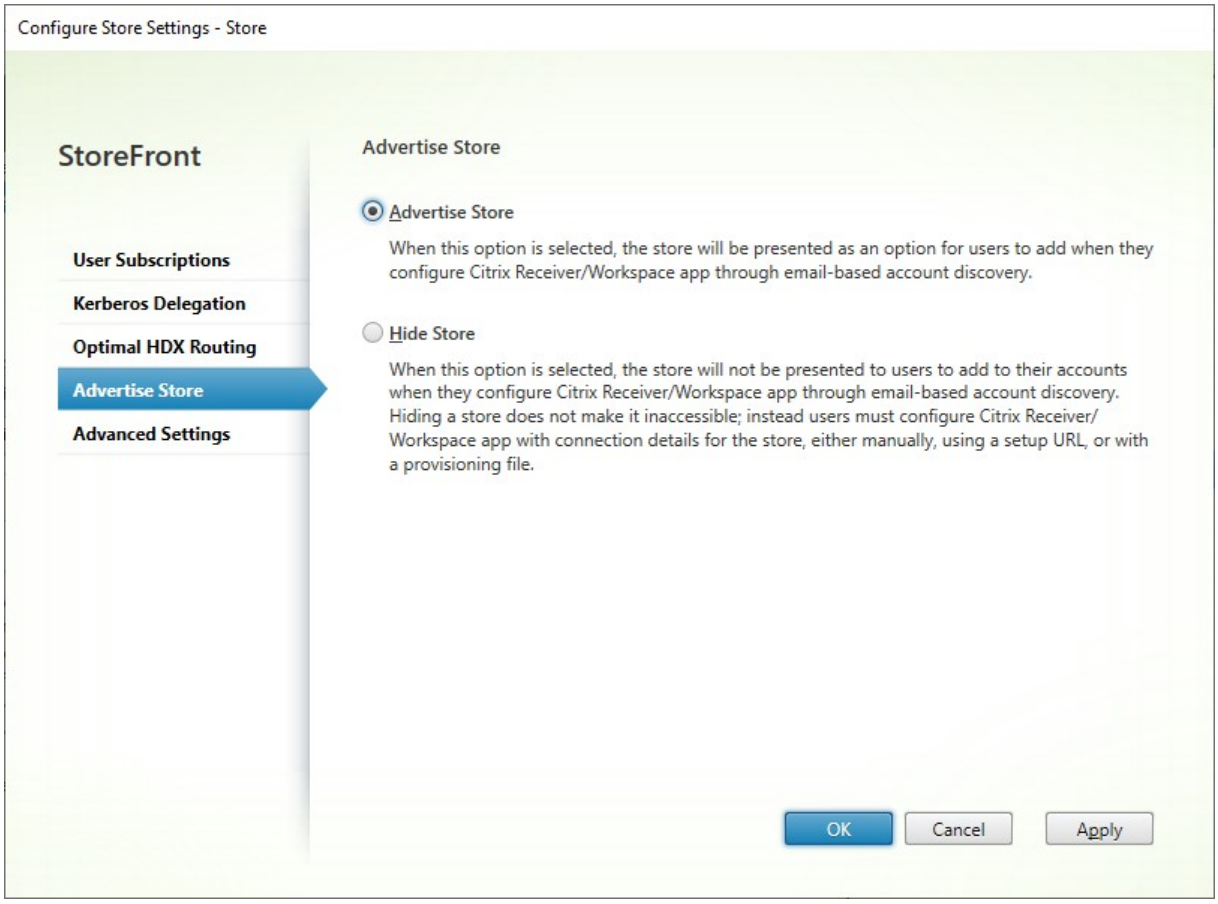
Anunciar y ocultar almacenes para los usuarios

August 15, 2023

Puede elegir si se muestran almacenes a los usuarios para que los agreguen a sus cuentas cuando configuren la aplicación Citrix Workspace mediante la detección de cuentas por correo electrónico o FQDN. Cuando crea un almacén, este se muestra de forma predeterminada como una opción para que los usuarios lo agreguen a Citrix Receiver al detectarse la implementación de StoreFront que aloja el almacén. Ocultar un almacén no lo hace inaccesible; los usuarios deben configurar la aplicación Citrix Workspace con los datos de conexión del almacén. Pueden hacerlo de forma manual, mediante una URL de configuración o con un archivo de aprovisionamiento.

> Importante:
>
> En implementaciones con varios servidores, use solo un servidor a la vez para hacer cambios en la configuración del grupo de servidores. Compruebe que la consola de administración de Citrix StoreFront no se está ejecutando en ninguno de los demás servidores de la implementación. Una vez completados,
> propague los cambios de configuración al grupo de servidores de modo que los demás servidores de la implementación se actualicen.

1. Seleccione el nodo **Almacenes** en el panel izquierdo de la consola de administración de Citrix StoreFront y, en el panel **Acciones**, haga clic en **Configurar parámetros del almacén** > **Anunciar almacén**.
2. En la página **Anunciar almacén**, seleccione **Anunciar almacén** u **Ocultar almacén**.



Delegación Kerberos

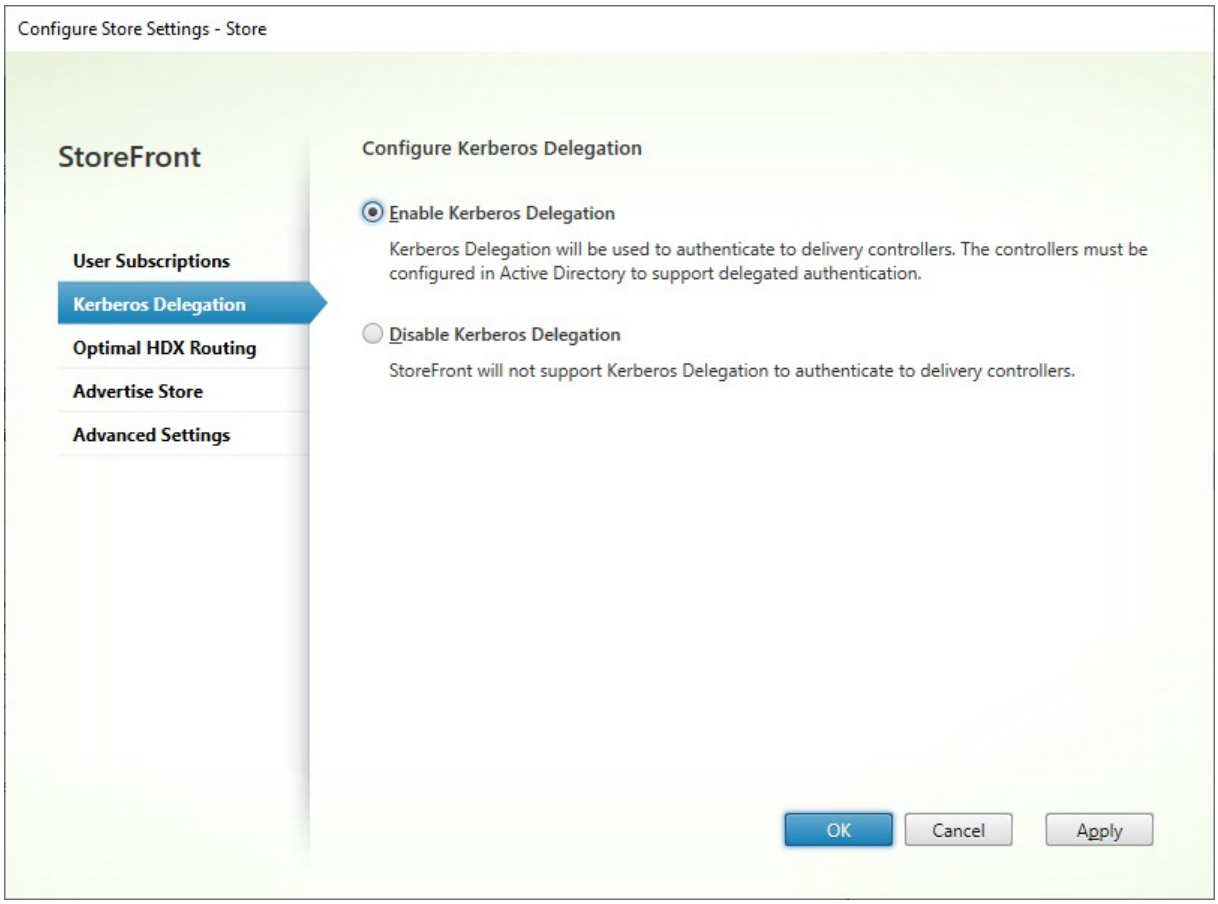
April 17, 2024

> **Nota:**
>
> La delegación Kerberos es obsoleta y solo se puede usar con XenApp 6.5 y versiones anteriores. No se puede usar con ninguna versión compatible de Citrix Virtual Apps and Desktops.

Cuando se usa la autenticación PassThrough de dominio o con tarjeta inteligente, ya sea directamente o mediante Citrix Gateway, StoreFront no tiene las credenciales del usuario, por lo que no puede autenticarse en el Delivery Controller con las credenciales del usuario. Al usar XenApp 6.5 y versiones anteriores, puede habilitar la delegación Kerberos para permitir que StoreFront se haga pasar por el usuario para autenticarse en el Delivery Controller. Esto requiere que la delegación esté configurada en Active Directory.

1. Seleccione un almacén y, en el panel Acciones, haga clic en **Configurar parámetros de almacén**.

2. Seleccione la ficha **Delegación Kerberos**.
3. Elija si quiere **habilitar la delegación Kerberos** o **inhabilitar la delegación Kerberos**.
4. Presione **Aplicar** o **Aceptar** para guardar los cambios.



SDK de PowerShell

Para configurar la delegación Kerberos, use el cmdlet Set-STFStoreService con el parámetro `-KerberosDelegation`

Administrar los recursos disponibles en los almacenes

April 17, 2024

Use la pantalla **Administrar Delivery Controllers** para agregar, modificar y eliminar feeds de recursos proporcionados por Citrix Virtual Apps and Desktops, Citrix Desktops as a Service y Citrix Secure Private Access.

Ver feeds de recursos

1. Desde la consola de administración de Citrix StoreFront, en el panel de la izquierda, seleccione el nodo **Almacenes**.
2. Seleccione un almacén en el panel de resultados.
3. En el panel **Acciones**, haga clic en **Administrar Delivery Controllers**.

Ver feeds de recursos mediante el SDK de PowerShell

Con el SDK de PowerShell, use el comando Get-STFStoreFarm para enumerar todos los feeds de recursos o un feed de recursos específico.

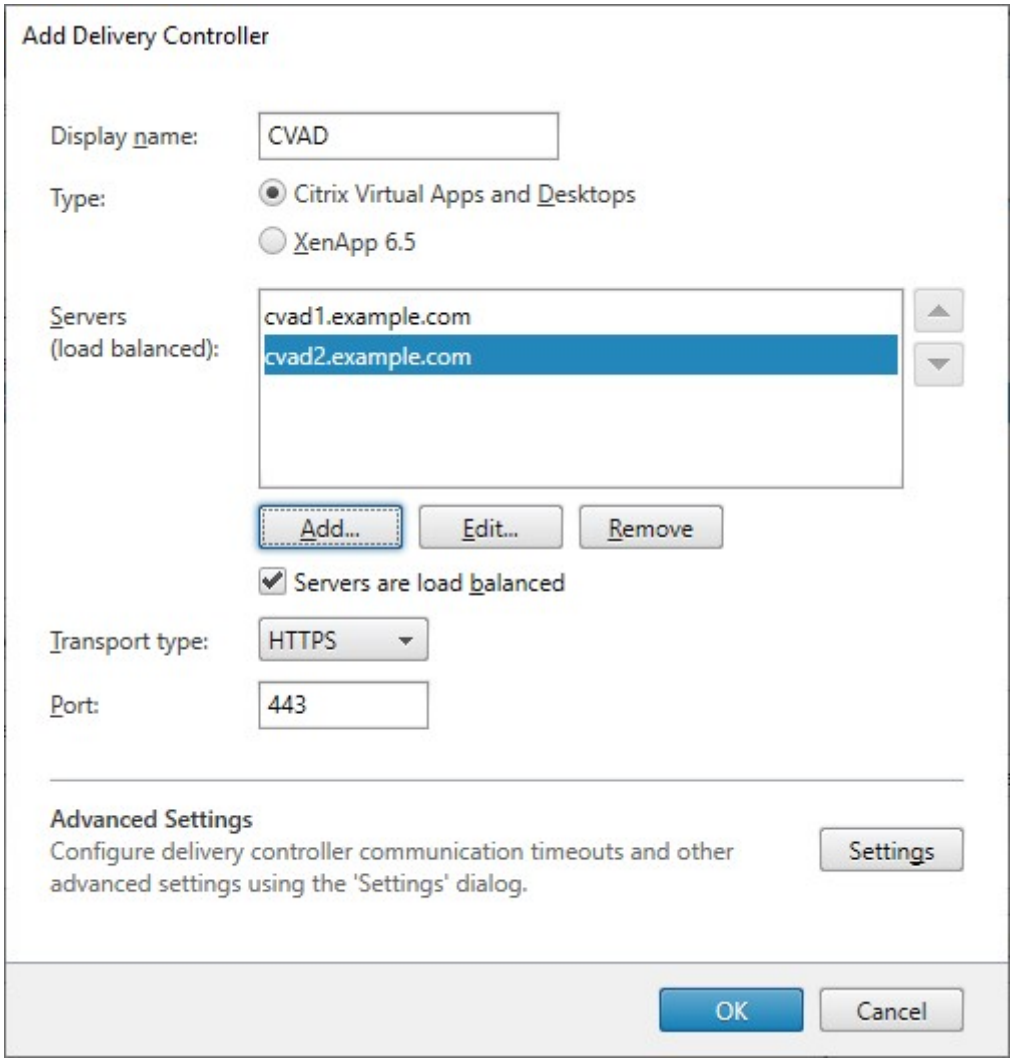
Agregar feeds de recursos

Agregar feeds de recursos para Citrix Virtual Apps and Desktops

1. En la pantalla **Administrar Delivery Controllers**, haga clic en **Agregar**.
2. Introduzca un **Nombre simplificado** que le ayude a identificar el feed.
3. Seleccione el **Tipo** como **Citrix Virtual Apps and Desktops**.
4. En **Servidores**, haga clic en **Agregar** e introduzca el nombre del Delivery Controller. Repita el procedimiento para cada Delivery Controller. Citrix recomienda tener al menos dos servidores para el equilibrio de carga o la conmutación por error.
5. Citrix recomienda seleccionar la opción **Servidores (con equilibrio de carga)**. Esto hace que StoreFront distribuya la carga entre todos los Delivery Controllers o conectores al seleccionar un servidor de la lista de forma aleatoria durante cada inicio. Si esta opción no está seleccionada, la lista de servidores se tratará como una lista de conmutación por error, por orden de prioridad. En este caso, el 100 % de los inicios ocurre en el primer Delivery Controller o conector activos de la lista. Si ese servidor se desconecta, el 100% de los inicios ocurre en el segundo de la lista, y así sucesivamente.
6. En la lista **Tipo de transporte**, seleccione el tipo de conexiones que debe utilizar StoreFront para las comunicaciones con los servidores.
   - Para enviar datos a través de conexiones sin cifrar, seleccione **HTTP**. Si selecciona esta opción, deberá definir su propia configuración para proteger las conexiones entre StoreFront y los servidores.
   - Para enviar datos a través de conexiones cifradas (recomendado), seleccione **HTTPS**. Si selecciona esta opción para servidores Citrix Virtual Apps and Desktops, debe comprobar que Citrix XML Service esté configurado para compartir su puerto con Microsoft Internet Information Services (IIS) y que IIS esté configurado para admitir HTTPS.

> **Nota:**
>
> Si utiliza HTTPS para proteger las conexiones entre StoreFront y los servidores, compruebe que los nombres especificados en la lista de servidores coincidan exactamente (incluidas mayúsculas y minúsculas) con los nombres que constan en los certificados para dichos servidores.

7. Especifique el puerto que StoreFront debe utilizar para las conexiones con los servidores. El puerto predeterminado para las conexiones HTTP es 80, y para las conexiones HTTPS es 443. El puerto especificado debe ser el puerto utilizado por Citrix XML Service.



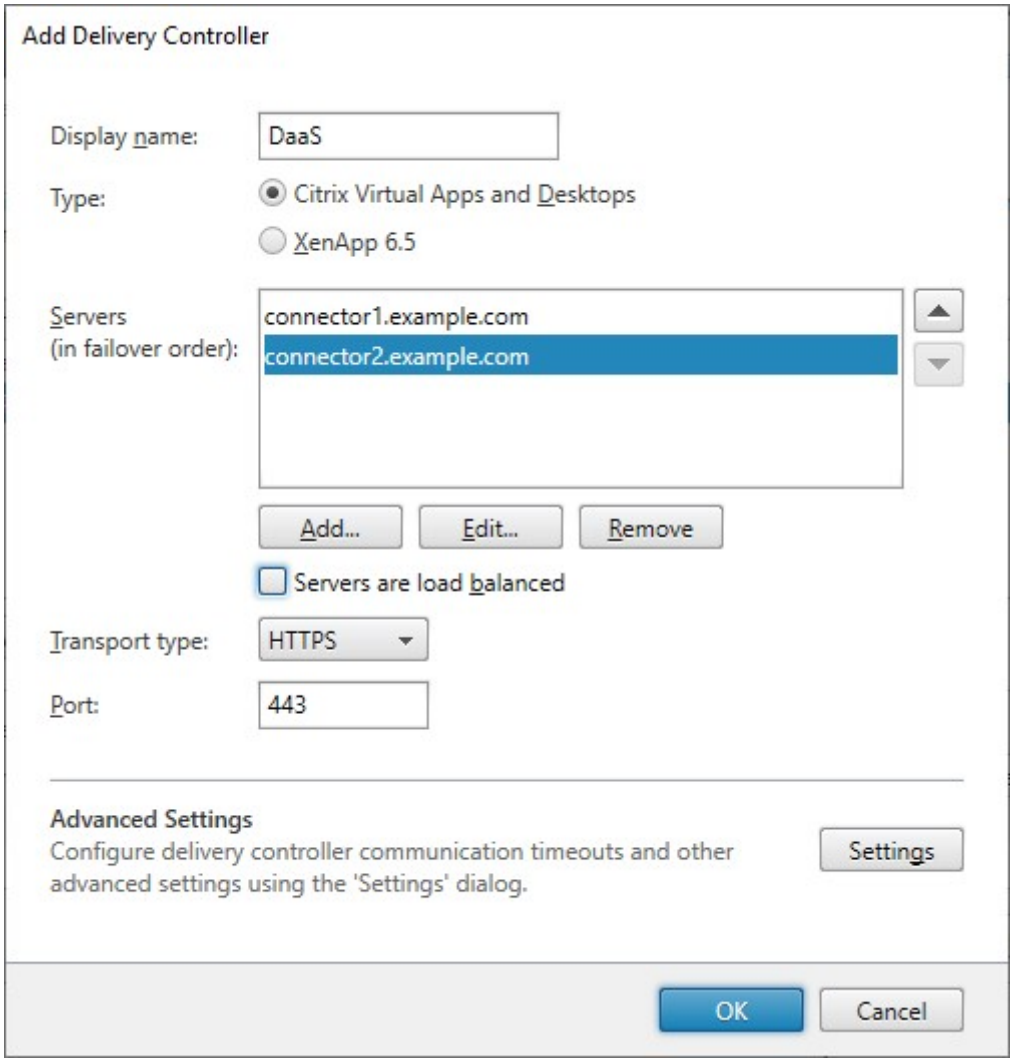
Agregar feeds de recursos para Citrix Desktops as a Service

1. En la pantalla **Administrar Delivery Controllers**, haga clic en **Agregar**.
2. Introduzca un **Nombre simplificado** que le ayude a identificar el feed.

3. Seleccione el **Tipo** como **Citrix Virtual Apps and Desktops**.
4. En **Servidores**, haga clic en **Agregar** e introduzca el nombre de un Cloud Connector. Repita el procedimiento para cada servidor o conector. Citrix recomienda tener al menos dos conectores por redundancia. Si tiene varias ubicaciones de recursos, Citrix recomienda agregar los Cloud Connectors de todas las ubicaciones de recursos para que, en caso de una interrupción del servicio, StoreFront pueda usar la memoria caché del host local para iniciar los VDA en la ubicación adecuada.
5. Si tiene conectores en varias ubicaciones, Citrix recomienda colocar los conectores con la latencia más baja con el servidor de StoreFront en la parte superior de la lista y desmarcar la opción **Servidores (con equilibrio de carga)**. Como los conectores solo envían información por proxy a los Delivery Controllers de DaaS, el uso del equilibrio de carga ofrece beneficios limitados.
6. En la lista **Tipo de transporte**, seleccione el tipo de conexiones que debe utilizar StoreFront para las comunicaciones con los servidores.
   - Para enviar datos a través de conexiones sin cifrar, seleccione **HTTP**. Si selecciona esta opción, deberá organizar cómo proteger las conexiones entre StoreFront y sus Cloud Connector.
   - Para enviar datos a través de conexiones cifradas (recomendado), seleccione **HTTPS**. Si selecciona esta opción, deberá asegurarse de que los Cloud Connector estén configurados para HTTPS.

   > **Nota:**
   >
   > Si utiliza HTTPS para proteger las conexiones entre StoreFront y los servidores, compruebe que los nombres especificados en la lista de servidores coincidan exactamente (incluidas mayúsculas y minúsculas) con los nombres que constan en los certificados para dichos servidores.

7. Especifique el puerto que StoreFront debe utilizar para las conexiones con los servidores. El puerto predeterminado para las conexiones HTTP es 80, y para las conexiones HTTPS es 443.



Agregar feeds de recursos para XenApp 6.5

Citrix no admite XenApp 6.5. A partir de la versión 2308 de StoreFront, ya no es posible agregar feeds de recursos de XenApp 6.5 mediante la consola de administración, pero puede seguir usando PowerShell.

Agregar fuentes de recursos para Citrix Secure Private Access

Si el servidor StoreFront está configurado para Citrix Secure Private Access, puede agregar fuentes de recursos de Citrix Secure Private Access.

1. Vaya a **Almacenes** > **Delivery Controllers** en StoreFront.
2. Haga clic en **Agregar**.

3. En la ventana **Agregar Delivery Controller**, introduzca un **Nombre simplificado** para identificar el feed.
4. Seleccione el **Tipo** como **Citrix Secure Private Access**.
5. Introduzca el nombre del servidor de Citrix Secure Private Access.
6. En el menú desplegable **Tipo de transporte**, seleccione el tipo de conexión que se puede usar para las comunicaciones con los servidores.
   - **HTTP:** envía datos a través de conexiones no cifradas

   > **Nota:**
   >
   > Si selecciona **HTTP**, deberá definir su propia configuración para proteger las conexiones entre StoreFront y los servidores.

   - **HTTPS:** envía datos a través de conexiones HTTP seguras mediante SSL (Secure Sockets Layer) o TLS (Transport Layer Security).
7. Especifique el puerto que se utilizará para las conexiones a los servidores. El puerto predeterminado para **HTTP** es 80 y para **HTTPS** es 443.
8. Haga clic en **Aceptar**.

Crear un feed de recursos con el SDK de PowerShell

Para agregar un feed de recursos, use el comando Add-STFStoreFarm.

- Para Citrix Virtual Apps and Desktops o Citrix Desktops as a Service, establezca `FarmType` en `XenDesktop`.
- Para XenApp 6.5, establezca `FarmType` en `XenApp`.
- Para Citrix Secure Private Access, establezca `FarmType` en `SPA`.

Modificar un feed de recursos

En la pantalla **Administrar Delivery Controllers**, seleccione un feed de recursos y haga clic en **Modificar**.

Modificar un feed de recursos mediante el SDK de PowerShell

Para modificar un feed de recursos mediante PowerShell, use el comando Set-STFStoreFarm.

Eliminar un feed de recursos

En la pantalla **Administrar Delivery Controllers**, seleccione un feed de recursos y haga clic en **Quitar**.

Eliminar un feed de recursos mediante el SDK de PowerShell

Para eliminar un feed de recursos mediante PowerShell, use el comando Remove-STFStoreFarm.

Configurar el comportamiento de omisión de servidores

Para mejorar el rendimiento cuando alguno de los servidores que proporcionan recursos deja de estar disponible, StoreFront omite temporalmente los servidores que no responden. Cuando un servidor se omite, StoreFront lo ignora y no lo utiliza para acceder a los recursos. Use estos parámetros para especificar la duración del comportamiento de omisión:

- **Duración de la omisión si no hay respuesta** especifica una duración reducida en minutos que StoreFront emplea en lugar de la duración indicada en **Duración de la omisión** si se omiten todos los servidores de un Delivery Controller en particular. El valor predeterminado es 0 minutos.
- **Duración de omisión** especifica el tiempo en minutos que StoreFront omite un servidor individual después de intentar ponerse en contacto sin éxito con dicho servidor. La duración de omisión predeterminada es 60 minutos.

Consideraciones al especificar el parámetro de Duración de la omisión si no hay respuesta

Al establecer un valor mayor en **Duración de la omisión si no hay respuesta**, se reduce el impacto causado por la falta de disponibilidad de un Delivery Controller concreto, pero se produce un efecto negativo: los recursos de dicho Delivery Controller no estarán disponibles para los usuarios durante el tiempo especificado después de que se interrumpa temporalmente la red o de que el servidor no esté disponible. Considere la opción de usar valores elevados para **Duración de la omisión si no hay respuesta** cuando se han configurado muchos Delivery Controllers para un almacén, especialmente Delivery Controllers que no son importantes y que no afectan al trabajo.

Al establecer un valor menor en **Duración de la omisión si no hay respuesta**, se aumenta la disponibilidad de los recursos ofrecidos por dicho Delivery Controller, pero también aumenta la posibilidad de generar esperas en el cliente si hay muchos Delivery Controllers configurados para un almacén y varios de ellos dejan de estar disponibles. Vale la pena mantener el valor predeterminado de 0 minutos cuando no se han configurado muchas comunidades y para Delivery Controllers importantes que afectan al trabajo.

Para cambiar los parámetros de omisión

1. Desde la consola de administración de Citrix StoreFront, en el panel de la izquierda, seleccione el nodo **Almacenes**.
2. Seleccione un almacén en el panel de resultados.
3. En el panel **Acciones**, haga clic en **Administrar Delivery Controllers**.
4. Seleccione un Controller, haga clic en **Modificar** y luego en **Parámetros** en la pantalla **Modificar Delivery Controller**.
5. En Parámetros avanzados, haga clic en **Parámetros**.
6. En el cuadro de diálogo Configurar parámetros avanzados:

   a) En la fila **Todas las fechas de omisión de omisión**, haga clic en la segunda columna e introduzca un tiempo, en minutos, tras el cual un Delivery Controller se considerará fuera de línea después de que todos sus servidores no respondan.
   b) En la fila **Duración de omisión**, haga clic en la segunda columna e introduzca un tiempo, en minutos, tras el cual un solo servidor se considerará fuera de línea después de que no responda.

Asignar usuarios a feeds de recursos

De forma predeterminada, los usuarios que acceden a un almacén ven una combinación de todos los recursos disponibles en todos los feeds configurados para ese almacén. Para proporcionar diferentes recursos a diferentes usuarios, puede configurar almacenes independientes o incluso separar las implementaciones de StoreFront. Como alternativa, puede proporcionar acceso a implementaciones específicas en función de la pertenencia de los usuarios a grupos de Microsoft Active Directory. Esto le permite definir experiencias diferentes para grupos de usuarios diferentes con un único almacén.

Por ejemplo: puede agrupar los recursos comunes para todos los usuarios en una implementación, y las aplicaciones de finanzas para el departamento de Cuentas en otra implementación. En esta configuración, un usuario que no es miembro del grupo de usuarios de Cuentas ve solamente los recursos comunes cuando accede al almacén. En cambio, un miembro del grupo de usuarios de Cuentas verá tanto los recursos comunes como las aplicaciones de finanzas.

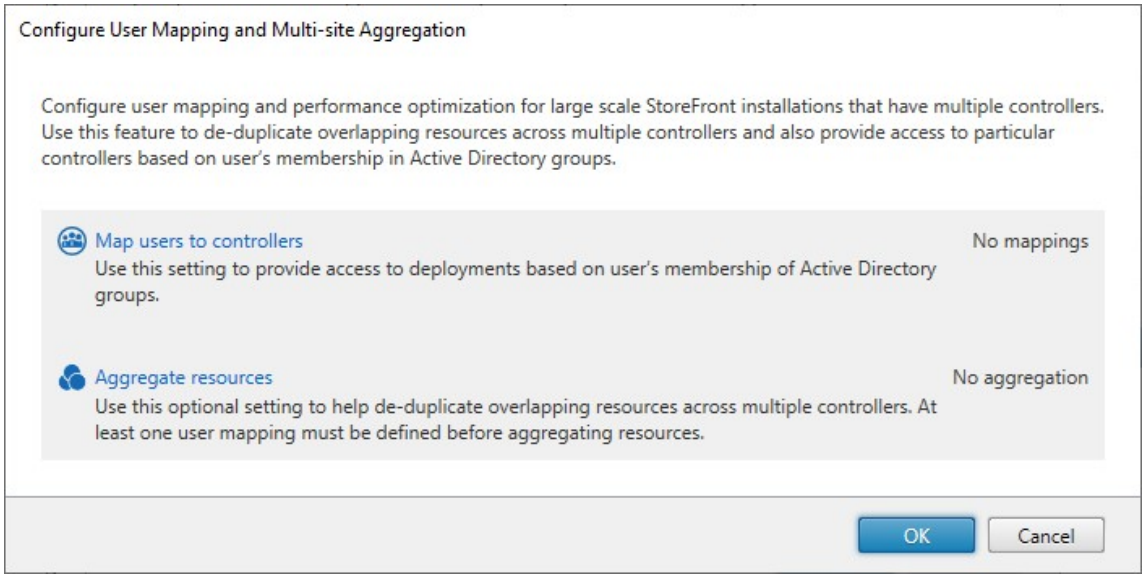
También puede crear una implementación para usuarios avanzados que proporcione los mismos recursos que las demás implementaciones, pero con hardware más rápido y eficaz. Esto le permite ofrecer una experiencia mejorada a usuarios fundamentales de la empresa, como el equipo ejecutivo. Todos los usuarios verán los mismos escritorios y las mismas aplicaciones cuando inicien sesión en el almacén, pero los miembros del grupo de usuarios Ejecutivos se conectarán de forma preferente a los recursos proporcionados por la implementación de usuario avanzado.

> Nota:
>
> Esto filtra feeds de recursos al completo. Además, dentro de un feed de recursos, se pueden filtrar aplicaciones por grupo de usuarios en la configuración de Studio de Citrix Virtual Apps and Desktops.

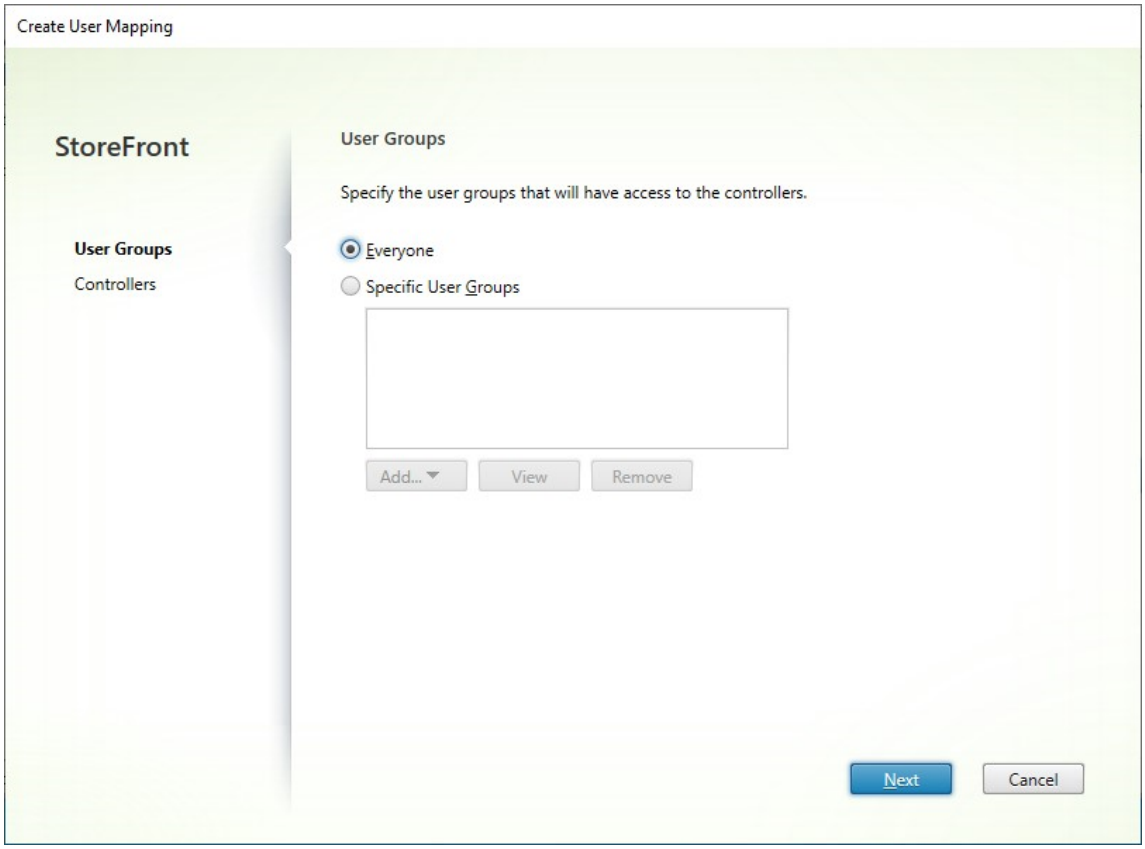
Para configurar feeds de recursos específicos para grupos de usuarios concretos:

1. En la pantalla **Administrar Delivery Controllers**, en **Configuración de la agrupación multisitio y la asignación de usuarios**, haga clic en **Configurar**. Esta opción solo está disponible si se configuran dos o más feeds de recursos.

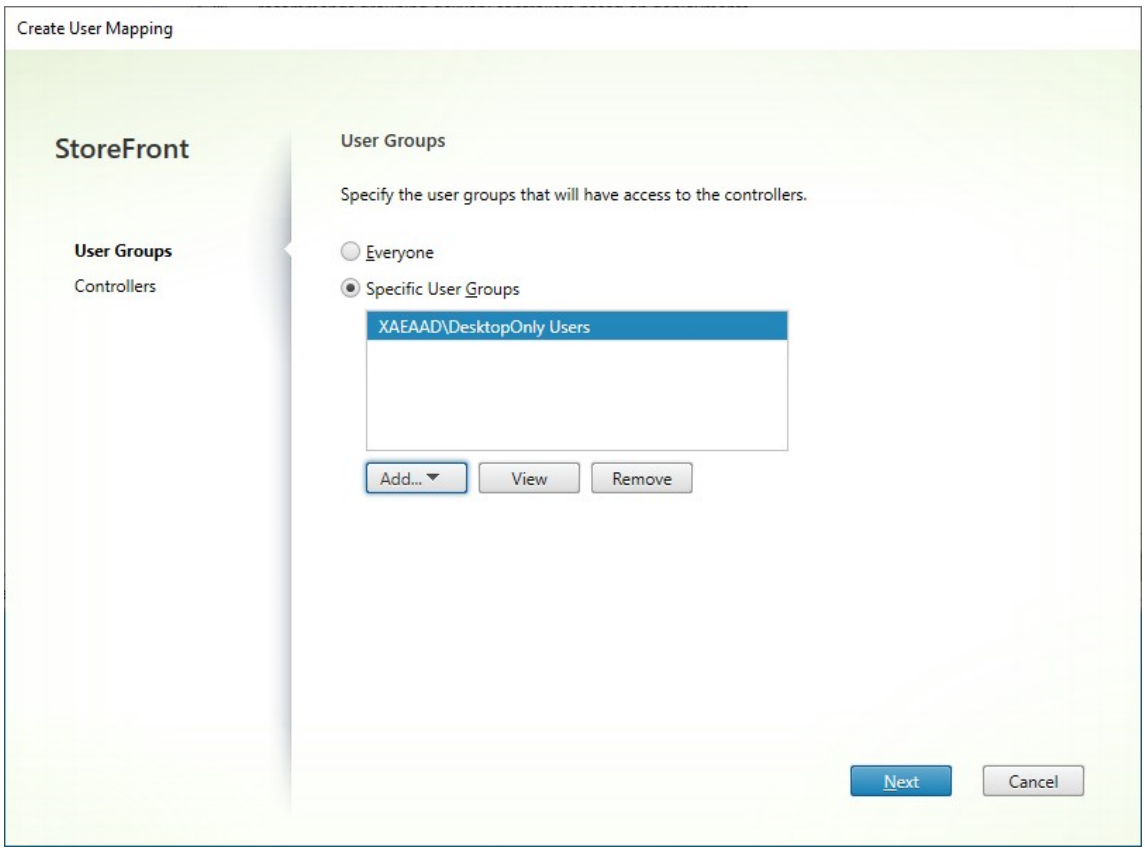
   Se abre la pantalla **Configurar asignación de usuarios y agrupación multisitio**.



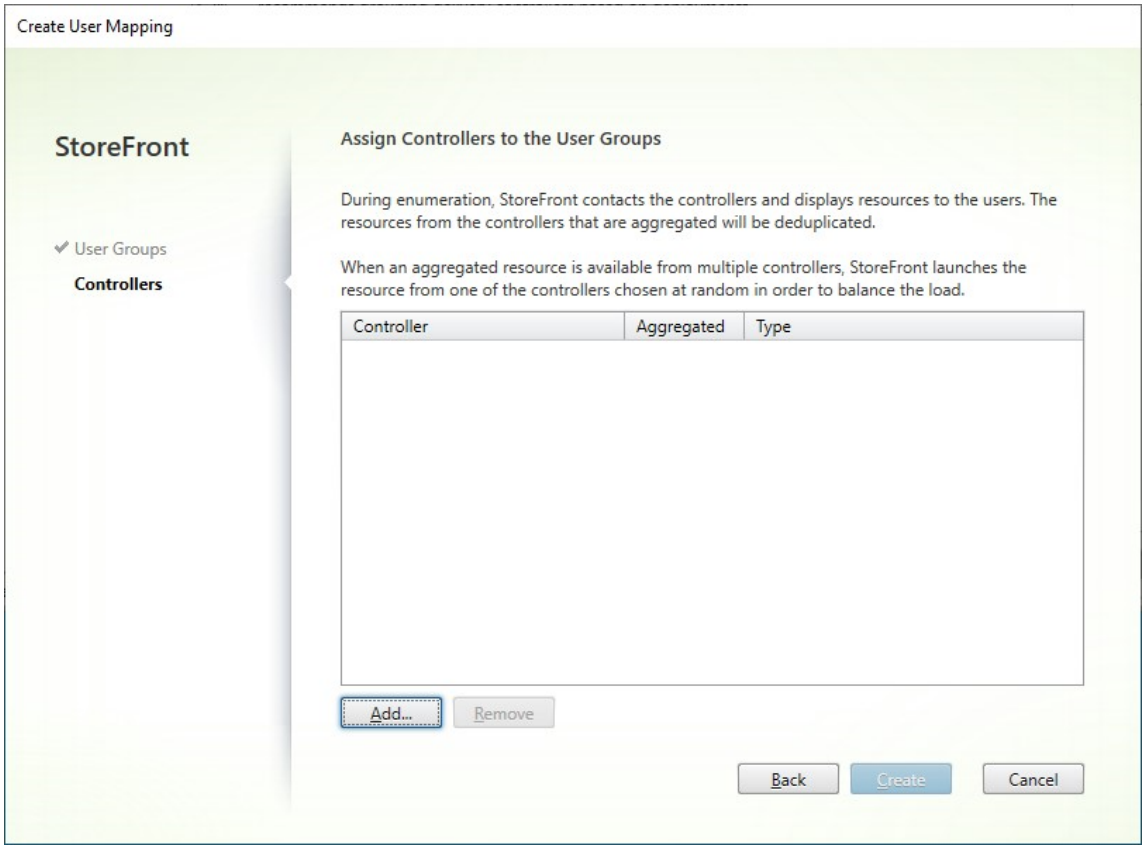
2. Haga clic en **Asignar usuarios a controladores**. Esto abre la pantalla **Crear asignación de usuarios** para crear su primera asignación. Podrá crear más asignaciones más adelante.



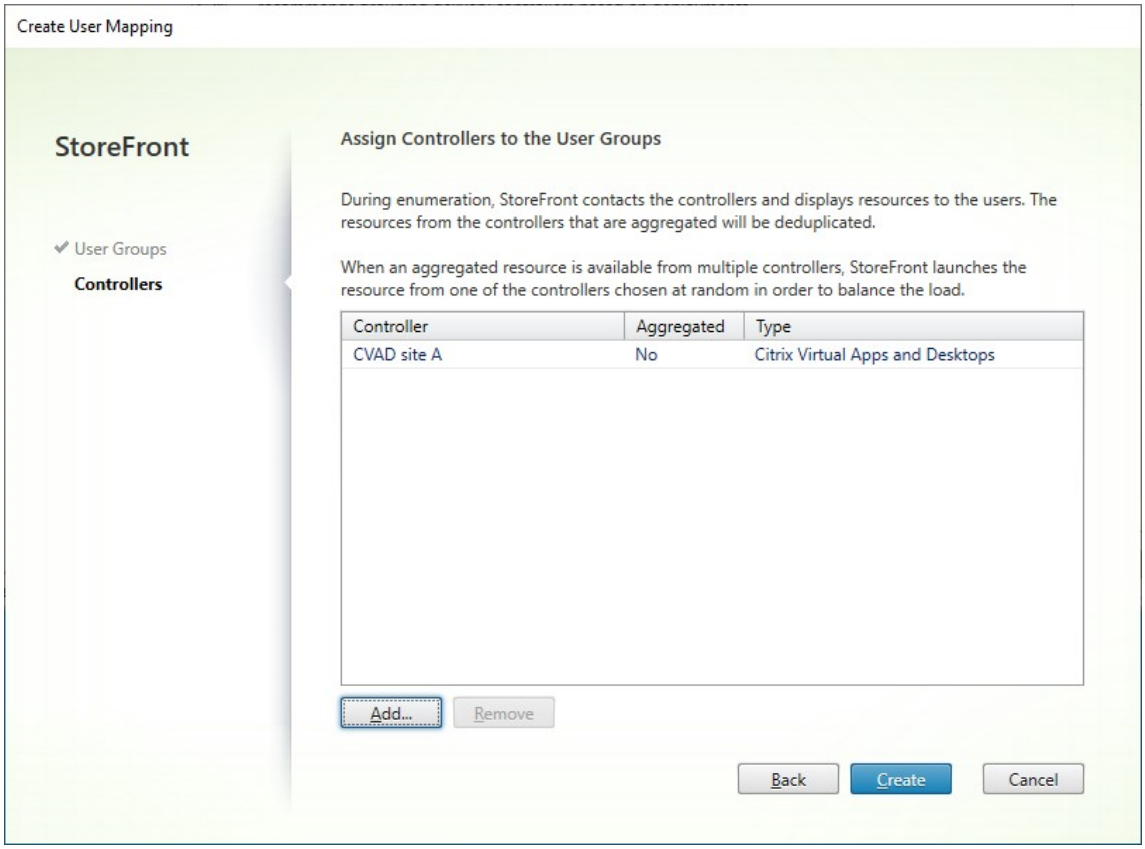
3. Elija **Todos** o **Grupos de usuarios específicos** y agregue al menos un grupo.



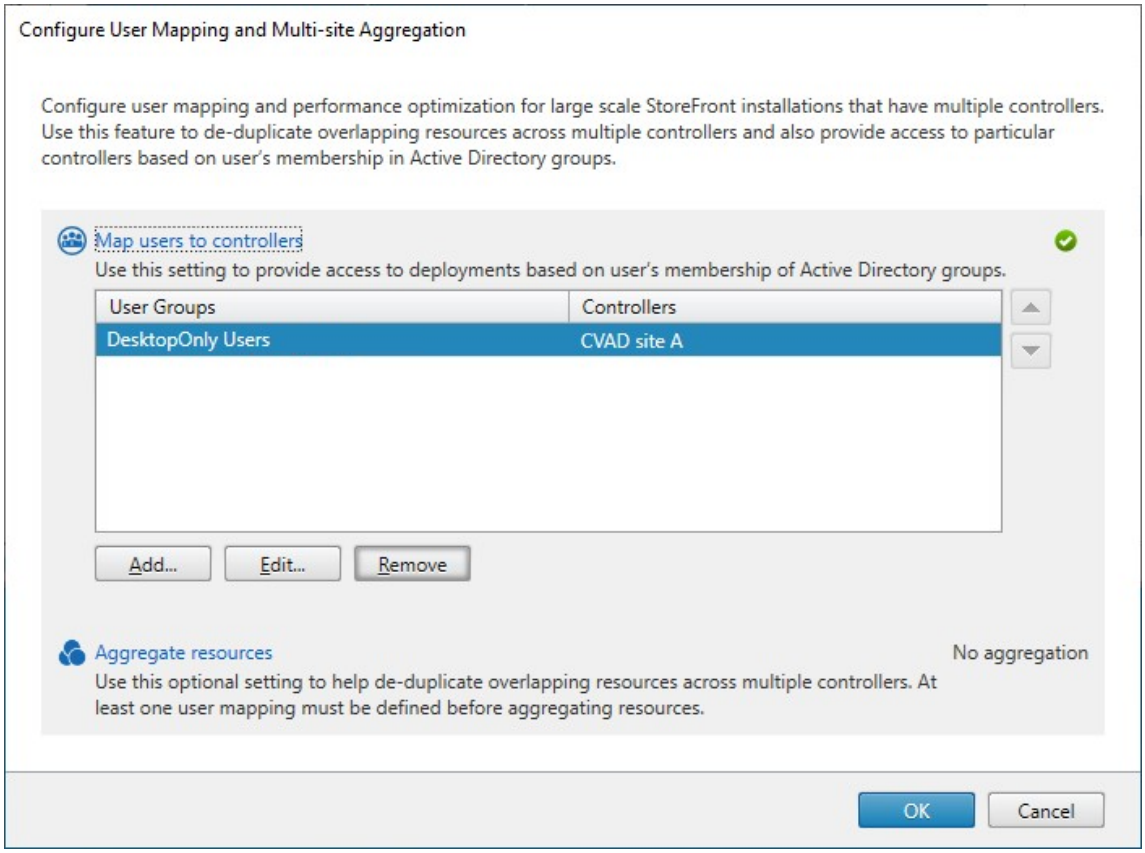
4. Haga clic en **Siguiente**. Esto le lleva a la ficha **Controladores**.



5. Haga clic en **Agregar** y agregue al menos un controlador.



6. Haga clic en **Crear**.



7. Haga clic en **Agregar…** para crear más asignaciones según sea necesario.

Asignar usuarios a recursos mediante el SDK de PowerShell

Puede asignar usuarios a recursos mediante el SDK de PowerShell.

1. Para cada feed de recursos, cree un conjunto EquivalentFarmset. Todos los feeds de recursos deben formar parte de un conjunto de comunidades; de lo contrario, no estarán disponibles para ningún usuario. Llame a New-STFEquivalentFarmset con estos parámetros:

   - `Name`: Un nombre único para el conjunto EquivalentFarmSet
   - `PrimaryFarms`: El nombre del feed de recursos no agregado (comunidad).

2. Para cada conjunto de usuarios que necesite acceso a un conjunto diferente de feeds de recursos, cree asignaciones entre esos usuarios y cada uno de los conjuntos EquivalentFarmSet. Para crear la asignación UserFarmMapping, llame a Add-STFUserFarmMapping con estos parámetros:

   - `StoreService`: El servicio del almacén al que agregar la asignación UserFarmMapping.
   - `Name`: Un nombre único para la asignación.

- `GroupMembers`: Una tabla hash que contiene los nombres y los SID de los grupos de usuarios que forman parte de la asignación. El nombre se usa solo para mostrarse; el SID define el grupo. Para agregar todos los usuarios, cree una sola entrada en la tabla hash con el nombre `Everyone` y el valor `Everyone`.
- `EquivalentFarmSet`: Un conjunto EquivalentFarmSet creado en el paso anterior.

Debe asegurarse de que cada feed de recursos (comunidad) esté incluida en al menos un UserFarmMapping; de lo contrario, ningún usuario podrá acceder a ese recurso.

Agrupación multisitio

De forma predeterminada, StoreFront enumera todas las implementaciones que proporcionan escritorios y aplicaciones a un almacén y trata todos esos recursos de manera diferenciada. Esto significa que, si el mismo recurso está disponible en más de una implementación, los usuarios verán un icono para cada recurso. Esto puede ser confuso si los recursos tienen el mismo nombre. Al definir una configuración multisitio de alta disponibilidad, puede agrupar las implementaciones de Citrix Virtual Apps and Desktops que entregan el mismo escritorio o aplicación. De esta manera, los recursos que son idénticos se pueden combinar de cara a los usuarios. Las implementaciones agrupadas no tienen por qué ser idénticas. Sin embargo, los recursos deben tener el mismo nombre y la misma ruta de acceso para cada servidor que se va a combinar.

Con la agrupación multisitio, cuando un escritorio o aplicación están disponibles desde varias implementaciones de Citrix Virtual Apps and Desktops configuradas para un almacén concreto, StoreFront combina todas las instancias de ese recurso y presenta a los usuarios un solo icono. Cuando un usuario inicia un recurso combinado, StoreFront determina la instancia más adecuada de ese recurso para el usuario. Esta determinación se realiza en función de la disponibilidad del servidor, de si el usuario ya tiene una sesión activa y del orden especificado en la configuración.

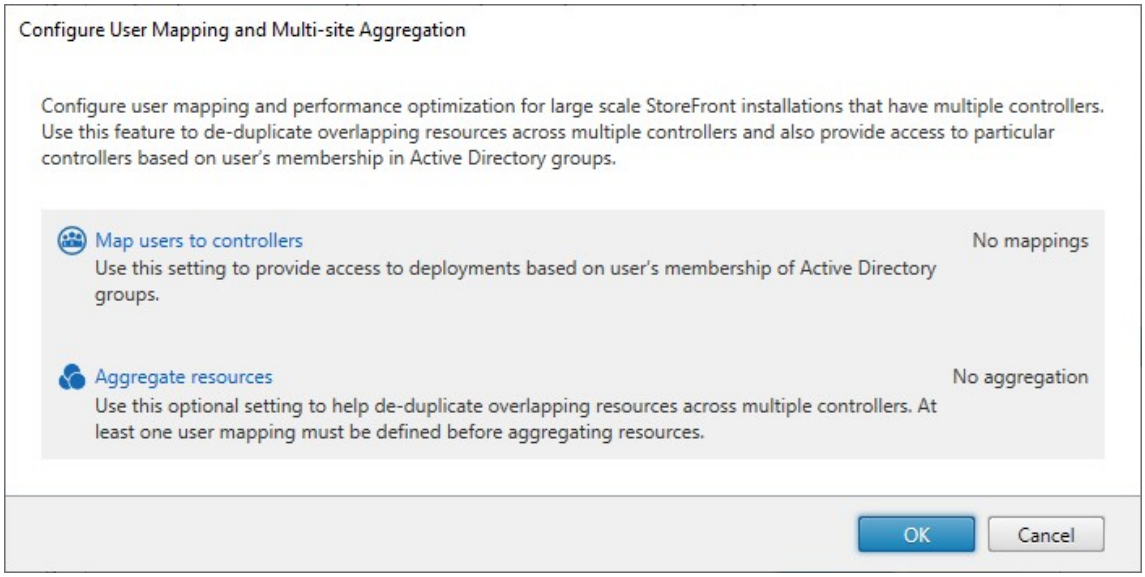
StoreFront supervisa de manera dinámica los servidores que no responden a las solicitudes porque están experimentando una sobrecarga o no están disponibles temporalmente. Los usuarios son dirigidos a instancias de recursos en otros servidores hasta que se restablezcan las comunicaciones. En los servidores que puedan proporcionar los recursos, StoreFront intenta volver a usar las sesiones existentes para entregar recursos adicionales. Si un usuario ya tiene una sesión activa en una implementación que también proporciona el recurso solicitado, StoreFront vuelve a utilizar la sesión si es compatible con ese recurso. Minimizar el número de sesiones de cada usuario reduce el tiempo necesario para iniciar aplicaciones o escritorios adicionales, y puede permitir un uso más eficaz de las licencias de productos.

Después de comprobar la disponibilidad y las sesiones de usuario existentes, StoreFront utiliza el orden especificado en la configuración para determinar la implementación a la que se conecta el usuario. Si hay más de una implementación equivalente disponible para el usuario, puede especificar que los usuarios se conecten o a la primera implementación disponible o, de forma aleatoria,

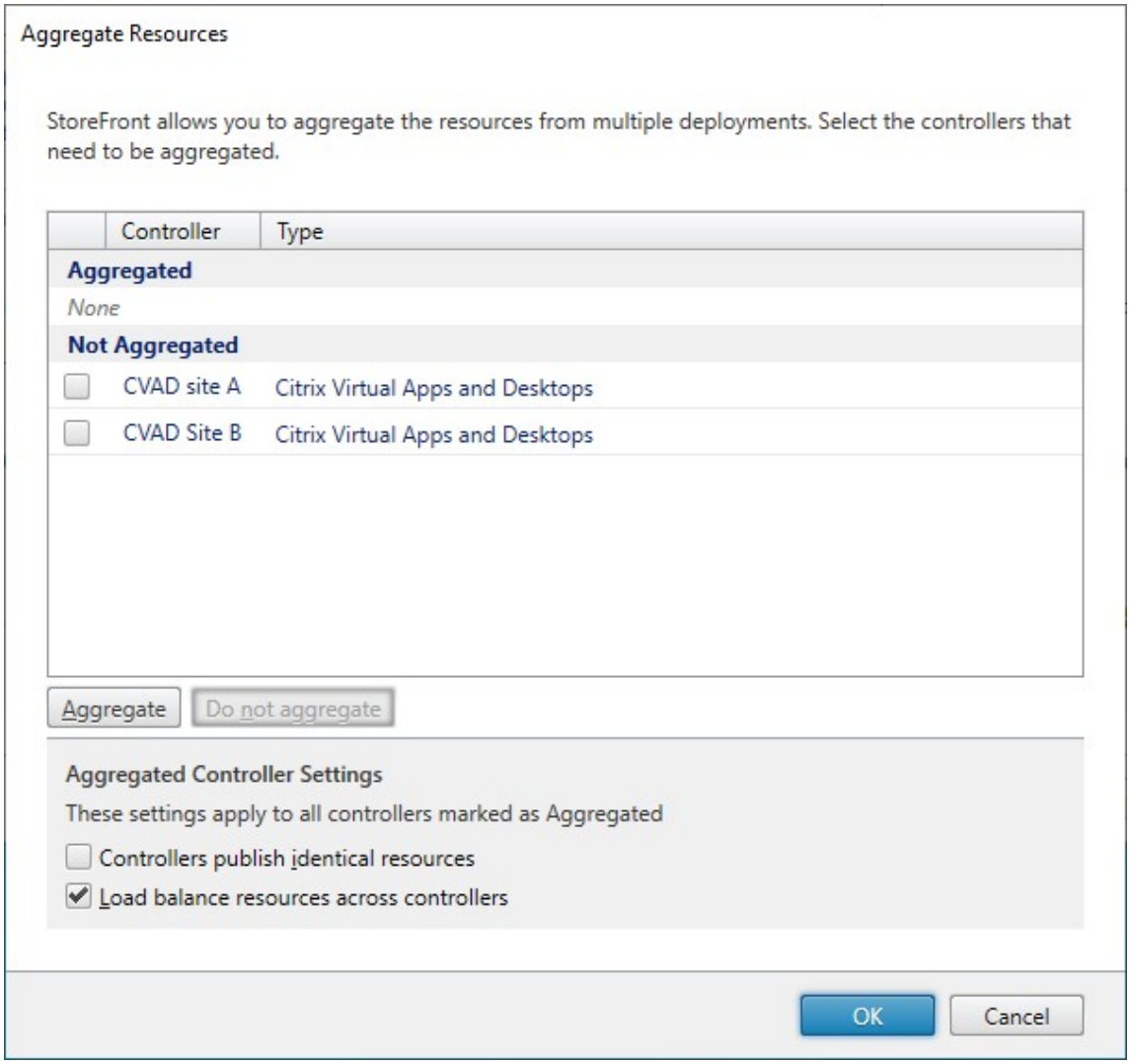
a cualquier implementación de la lista. Si los usuarios se conectan a la primera implementación disponible, se minimiza el número de implementaciones en uso para el número actual de usuarios. En cambio, la conexión aleatoria de usuarios proporciona una distribución más equitativa de los usuarios por todas las implementaciones disponibles.

Puede anular la ordenación de implementación especificada para recursos individuales de Citrix Virtual Apps and Desktops. De esta manera, podrá definir las implementaciones preferidas a las que se conectarán los usuarios cuando accedan a un escritorio o aplicación concretos. Esto le permite, por ejemplo, especificar que los usuarios se conecten preferiblemente a una implementación específicamente adaptada para entregar un escritorio o aplicación concretos, mientras que utiliza las implementaciones restantes para otros recursos. Para ello, agregue la cadena `KEYWORDS:Primary` a la descripción de la aplicación o escritorio de la implementación preferida y `KEYWORDS:Secondary` al recurso en otras implementaciones. Cuando sea posible, los usuarios se conectarán a la implementación que proporcione el recurso principal, independientemente del orden de implementación especificado en la configuración. Los usuarios se conectan con implementaciones que suministran recursos secundarios cuando la implementación preferida no está disponible.

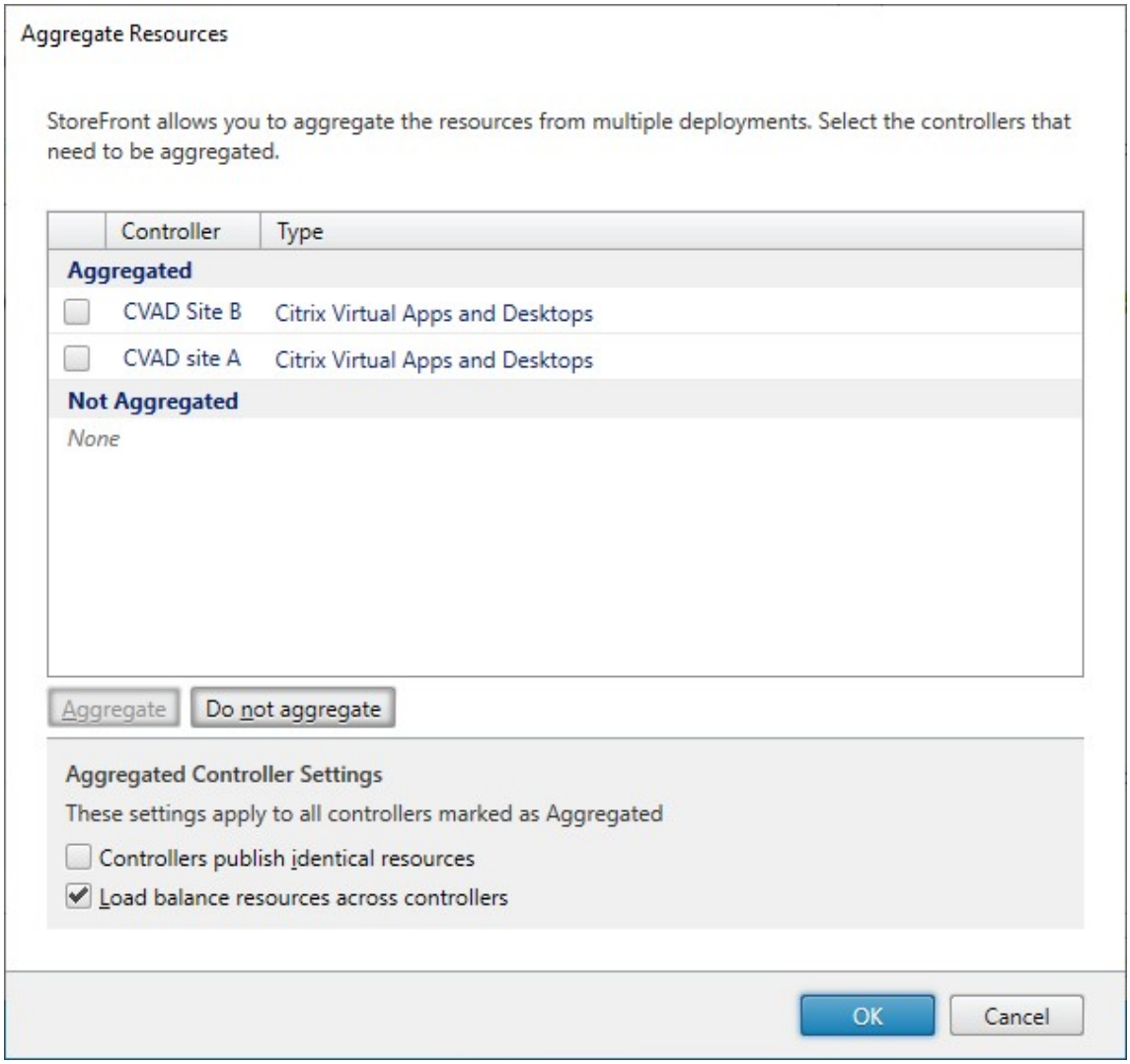
1. En la pantalla **Administrar Delivery Controllers**, en **Configuración de la agrupación multisitio y la asignación de usuarios**, haga clic en **Configurar**. Esta opción solo está disponible si se configuran dos o más feeds de recursos.



2. Haga clic en **Agregar recursos**. Esto muestra la pantalla **Agrupar recursos**.



3. Elija los feeds de recursos que tengan los mismos recursos y haga clic en **Agrupar**.



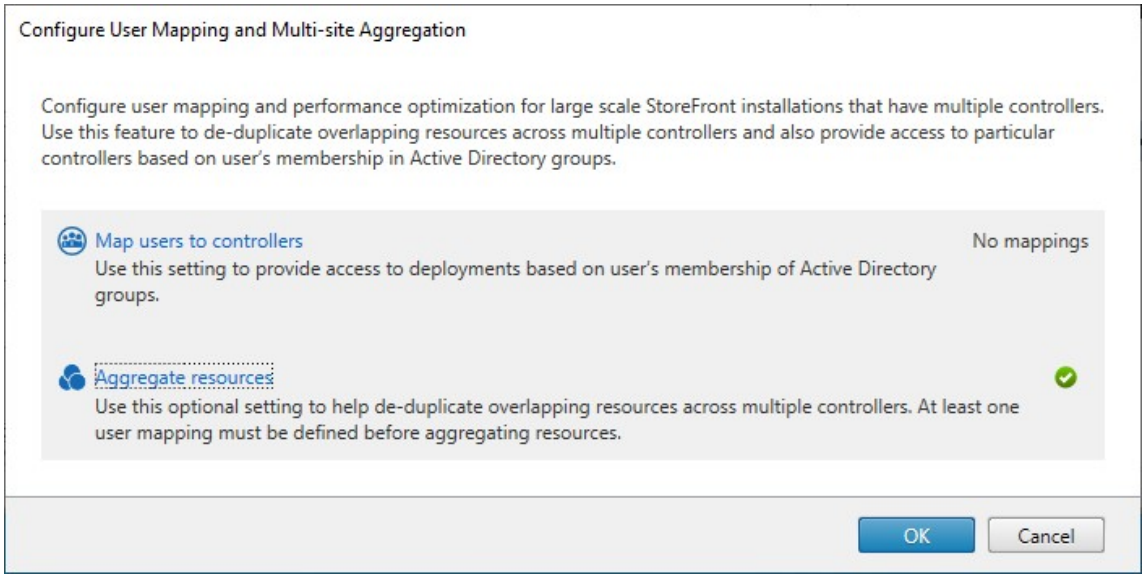
4. Seleccione las opciones de **Parámetros de Controllers agrupados** que necesite:

   - **Los Controllers publican recursos idénticos:** Al seleccionar esta opción, StoreFront enumera los recursos de solo uno de los Controllers agrupados. Si no se selecciona, StoreFront enumera los recursos de todos los Controllers agrupados (para acumular todo el conjunto de recursos disponibles del usuario). Seleccionar esta opción ofrece un mejor rendimiento para enumerar recursos, pero no se recomienda a menos que esté seguro de que la lista de recursos es idéntica en todos los feeds agrupados.

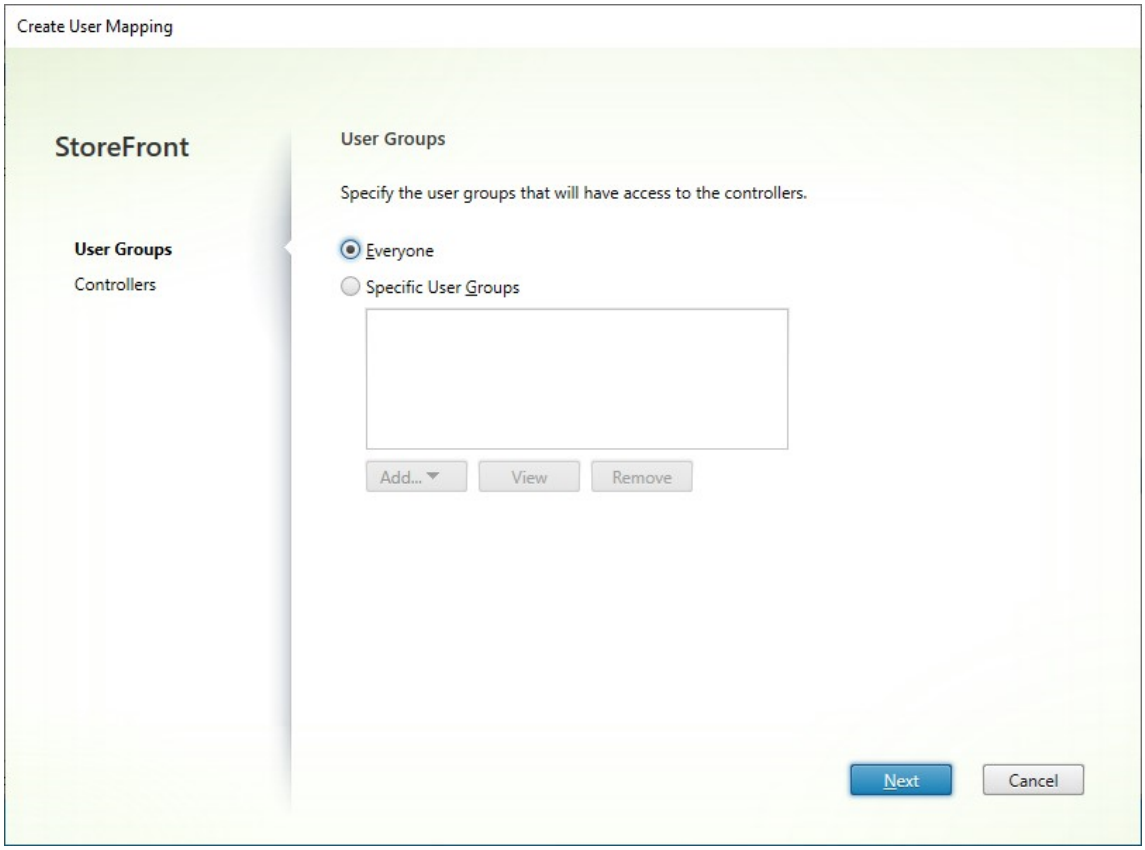
   - **Equilibrar la carga de los recursos entre los Controllers:** Al seleccionar esta opción, los inicios de recursos se distribuyen de forma uniforme entre los Controllers disponibles. Si no se selecciona, los inicios de recursos se dirigen al primer Controller especificado en el diálogo de asignación de usuarios, y en caso de error, se pasa al siguiente Controller sucesivamente.

5. Haga clic en **Aceptar** para volver a la pantalla **Configurar asignación de usuarios y agrupación**

multisitio. Ahora, **Agrupar recursos** está marcado.



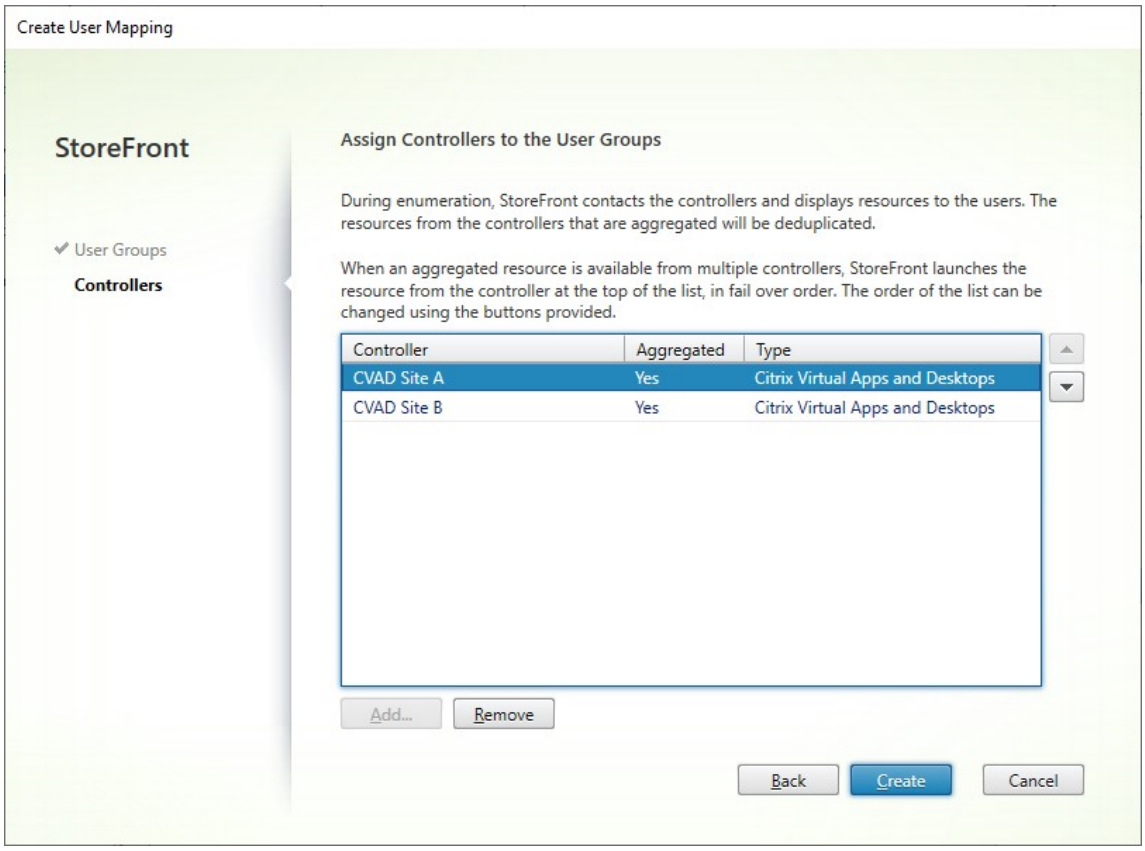
6. Al agrupar recursos, de forma predeterminada, ningún usuario tiene acceso a los recursos, por lo que debe agregar las asignaciones de usuarios. Haga clic en **Asignar usuarios a controladores**. Esto abre la pantalla **Crear asignación de usuarios**.



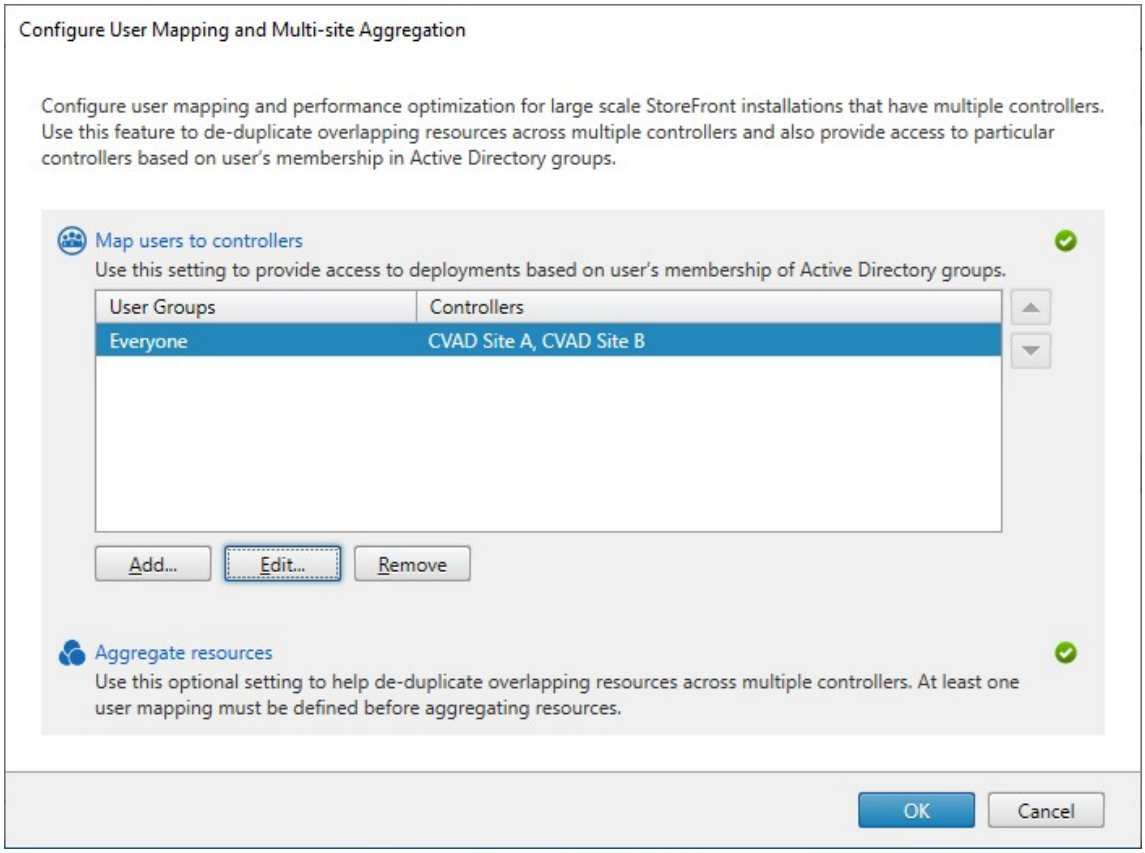
7. Elija **Todos** o **Grupos de usuarios específicos** y agregue al menos un grupo. Por ejemplo, es

posible que quiera elegir un grupo que represente a los usuarios en una ubicación determinada.

8. Agregue los feeds de recursos agrupados. Debe agregar todos los feeds de recursos agregados. Los que no estén incluidos pasarán al estado No agrupado. También puede incluir recursos no agrupados.
9. Si no marcó **Equilibrar la carga de los recursos entre los Controllers**, puede elegir el orden en el que StoreFront debería iniciar recursos.



10. Presione **Crear** para volver a **Configurar asignación de usuarios y agrupación multisitio**.



11. Agregue más asignaciones según sea necesario. Asegúrese de que cada feed de recursos esté asignado a un grupo de usuarios; de lo contrario, nadie podrá utilizar esos recursos.
12. Haga clic en **Aceptar**.

Configuraciones avanzadas con el SDK de PowerShell

Puede configurar muchas operaciones comunes multisitio y de alta disponibilidad con la consola de administración de StoreFront. También puede configurar StoreFront con el SDK de PowerShell, que proporciona estas funcionalidades adicionales:

- La capacidad para especificar varias agrupaciones de implementaciones para agruparlas.
  - La consola de administración solo permite una sola agrupación de implementaciones, que es suficiente para la mayoría de los casos.
  - Para almacenes con implementaciones que tengan conjuntos de recursos dispares, se pueden conseguir mejoras al aplicar agrupaciones múltiples.
- La capacidad para especificar un nivel de preferencia complejo para implementaciones agrupadas. La consola de administración permite equilibrar la carga de implementaciones agrupadas, o usarlos como una lista de servidores de conmutación por error. Con PowerShell, puede

tener varios grupos de feeds con carga equilibrada y conmutación por error entre diferentes grupos.

> **Advertencia:**
>
> Tras configurar las opciones avanzadas de multisitio mediante PowerShell, no es posible modificar las opciones mediante la consola de administración.

1. Debe decidir qué grupos de agregación quiere usar. Dentro de un grupo de agregación, las aplicaciones con el mismo nombre simplificado se agrupan en un solo icono. Cada grupo de agregación necesita un nombre. Con la consola de administración, solo puede crear un grupo de agregación. A través de PowerShell, puede definir varios grupos de agregación.

2. Para cada grupo de agregación, cree al menos un listado de conjuntos EquivalentFarmset con los feeds de recursos (conocidos en el SDK como comunidades) que quiera agregar. Si se van a asignar diferentes feeds de recursos dentro del grupo de agregación a diferentes usuarios, debe crear un conjunto EquivalentFarmSet independiente para cada conjunto de usuarios, pero que comparta el mismo nombre `AggregationGroupName`. Para crear el conjunto EquivalentFarmSet, llame a New-STFEquivalentFarmset con estos parámetros:

   - `Name`: Un nombre único para el conjunto EquivalentFarmset.
   - `AggregationGroupName`: El nombre del grupo de agregación del que forma parte el conjunto de comunidades.
   - `LoadBalanceMode`: `LoadBalanced` o `Failover`.
   - `PrimaryFarms`: Las comunidades que quiera agrupar. Si `LoadBalanceMode` es `Failover`, asegúrese de que las comunidades aparezcan en el orden requerido. Si hay varios conjuntos EquivalentFarmSet para un grupo de agregación, este orden se combina con el número IndexNumber definido en la asignación UserFarmMapping al evaluar qué feed de recursos se usa para iniciar un recurso.
   - `BackupFarms`: Una lista de comunidades que usar en caso de que ninguna de las comunidades principales esté disponible. Esta funcionalidad se ha retirado. En su lugar, agregue conjuntos EquivalentFarmSet adicionales con un número IndexNumber más alto.

3. Para cada feed de recursos que no forme parte de un grupo de agregación, cree un conjunto EquivalentFarmset sin especificar ningún nombre `AggregationGroupName`. Todos los feeds de recursos deben formar parte de un conjunto de comunidades. Llame a New-STFEquivalentFarmset con estos parámetros:

   - `Name`: Un nombre único para el conjunto EquivalentFarmSet
   - `PrimaryFarms`: El nombre de la comunidad no agrupada.

4. Para cada conjunto de usuarios que necesite acceso a un conjunto diferente de feeds de recursos, cree asignaciones entre esos usuarios y cada uno de los conjuntos EquivalentFarmSet. Para

crear la asignación UserFarmMapping, llame a Add-STFUserFarmMapping con estos parámetros:

- `StoreService`: El servicio del almacén al que agregar la asignación UserFarmMapping.
- `Name`: Un nombre único para la asignación.
- `GroupMembers`: Una tabla hash que contiene los nombres y los SID de los grupos de usuarios que forman parte de la asignación. El nombre se usa solo para mostrarse; el SID define el grupo. Para agregar todos los usuarios, cree una sola entrada en la tabla hash con el nombre `Everyone` y el valor `Everyone`.
- `EquivalentFarmSet`: Un conjunto EquivalentFarmSet creado en el paso anterior.
- `IndexNumber`: Establece el orden de los feeds de recursos que se evalúan. Esto establece el orden de preferencia de los feeds de recursos que se usarán para iniciar un recurso.

Debe asegurarse de que cada feed de recursos (comunidad) se incluya en al menos una asignación UserFarmMapping; de lo contrario, ningún usuario podrá acceder a ese recurso.

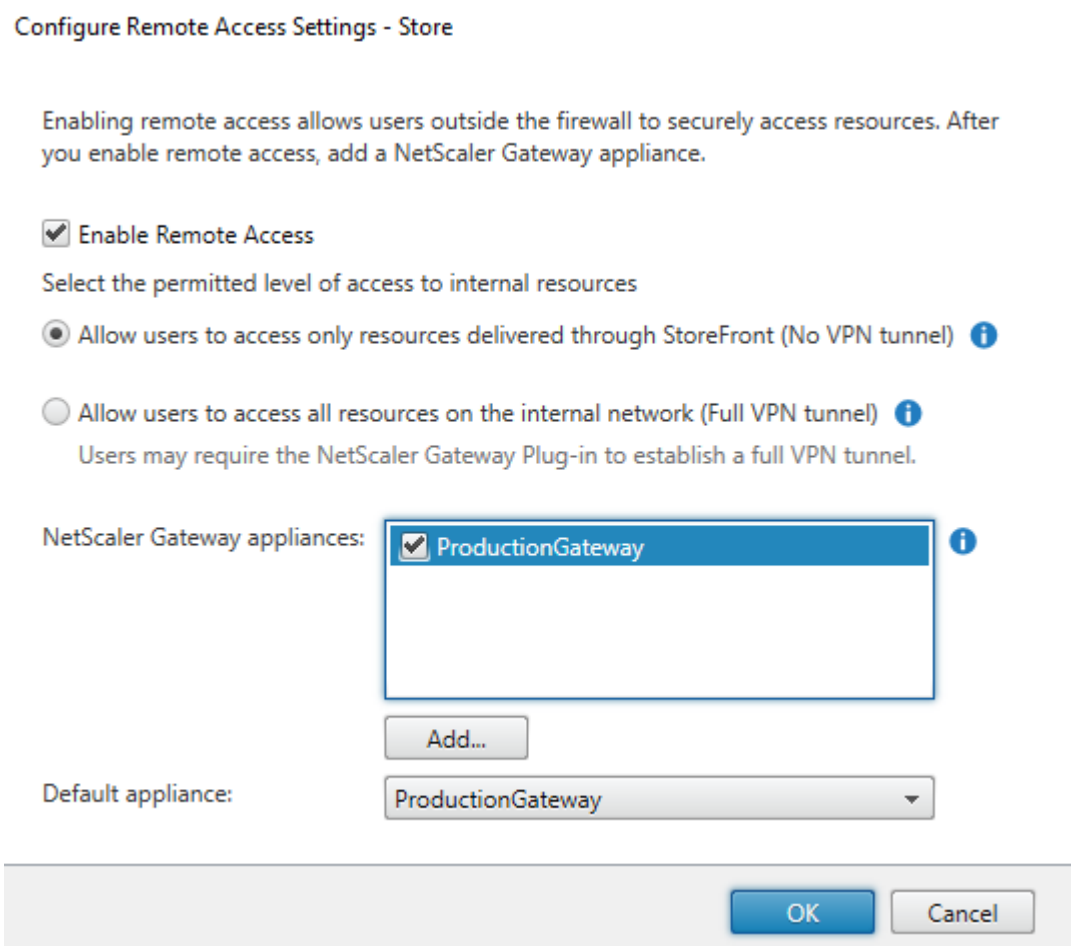
Administrar el acceso remoto a los almacenes a través de Citrix Gateway

February 26, 2024

Utilice la tarea Configurar parámetros de acceso remoto para definir el acceso a los almacenes a través de Citrix Gateway que se les otorga a los usuarios que se conectan desde redes públicas. El acceso remoto mediante Citrix Gateway no se puede aplicar a almacenes no autenticados.

> **Importante:**
>
> En implementaciones con varios servidores, use solo un servidor a la vez para hacer cambios en la configuración del grupo de servidores. Compruebe que la consola de administración de Citrix StoreFront no se está ejecutando en ninguno de los demás servidores de la implementación. Una vez completados,
> propague los cambios de configuración al grupo de servidores de modo que los demás servidores de la implementación se actualicen.

1. Seleccione el nodo Almacenes en el panel derecho de la consola de administración de Citrix StoreFront y, en el panel de resultados, seleccione un almacén. En el panel Acciones, haga clic en **Configurar parámetros de acceso remoto**.



2. En el cuadro de diálogo Configurar parámetros de acceso remoto, especifique si los usuarios que se conectan desde redes públicas pueden acceder al almacén a través de Citrix Gateway y la forma en que pueden hacerlo.

   - Para que el almacén no esté disponible para los usuarios de redes públicas, deje sin marcar la casilla **Habilitar acceso remoto**. Solo los usuarios locales de la red interna podrán acceder al almacén.
   - Para habilitar el acceso remoto, marque la casilla **Habilitar acceso remoto**.
     - Para que los recursos entregados mediante Citrix Gateway estén disponibles en el almacén, seleccione **Sin túnel VPN**. Los usuarios inician sesión en Citrix Gateway con ICAProxy o una VPN sin cliente (cVPN), y no necesitan usar el plug-in de Citrix Gateway para establecer una VPN completa.
     - Para determinar que el almacén y todos los demás recursos de la red interna estén disponibles a través de un túnel de red privada virtual (VPN) con Secure Sockets Layer (SSL), seleccione **Túnel VPN completo**. Los usuarios necesitan el plug-in de Citrix Gateway para establecer el túnel VPN.

   Al habilitar el acceso remoto al almacén, el método de autenticación **PassThrough desde**

Citrix Gateway se habilita automáticamente. Los usuarios se autentican en Citrix Gateway y su sesión se inicia automáticamente cuando acceden a sus almacenes.

3. Si ha habilitado el acceso remoto, en la lista **Dispositivos Citrix Gateway**, seleccione las implementaciones a través de las que los usuarios pueden acceder al almacén. Las implementaciones previamente configuradas para este y otros almacenes están disponibles y se pueden seleccionar de la lista. Si quiere agregar otra implementación a la lista, haga clic en **Agregar** y siga los pasos que se indican en Configurar Citrix Gateway.
4. Si habilita el acceso a través de varios dispositivos porque selecciona más de una entrada de la lista, especifique el **Dispositivo predeterminado** que se utilizará para acceder al almacén desde la aplicación Citrix Workspace.
5. Haga clic en **Aceptar** para guardar la configuración y cerrar el cuadro de diálogo Configurar acceso remoto.

La aplicación Citrix Workspace utiliza balizas para determinar si los usuarios están conectados a redes locales o públicas y, luego, selecciona el método de acceso adecuado. Para obtener más información sobre cómo cambiar balizas, consulte Configurar balizas.

De forma predeterminada, StoreFront usa el dispositivo Gateway a través del cual el usuario se conecta al almacén para iniciar los recursos. Para configurar StoreFront de modo que inicie recursos con o sin una puerta de enlace alternativa, consulte Redirección óptima de HDX.

la comprobación de listas de revocación de certificados (CRL)

April 17, 2024

Introducción

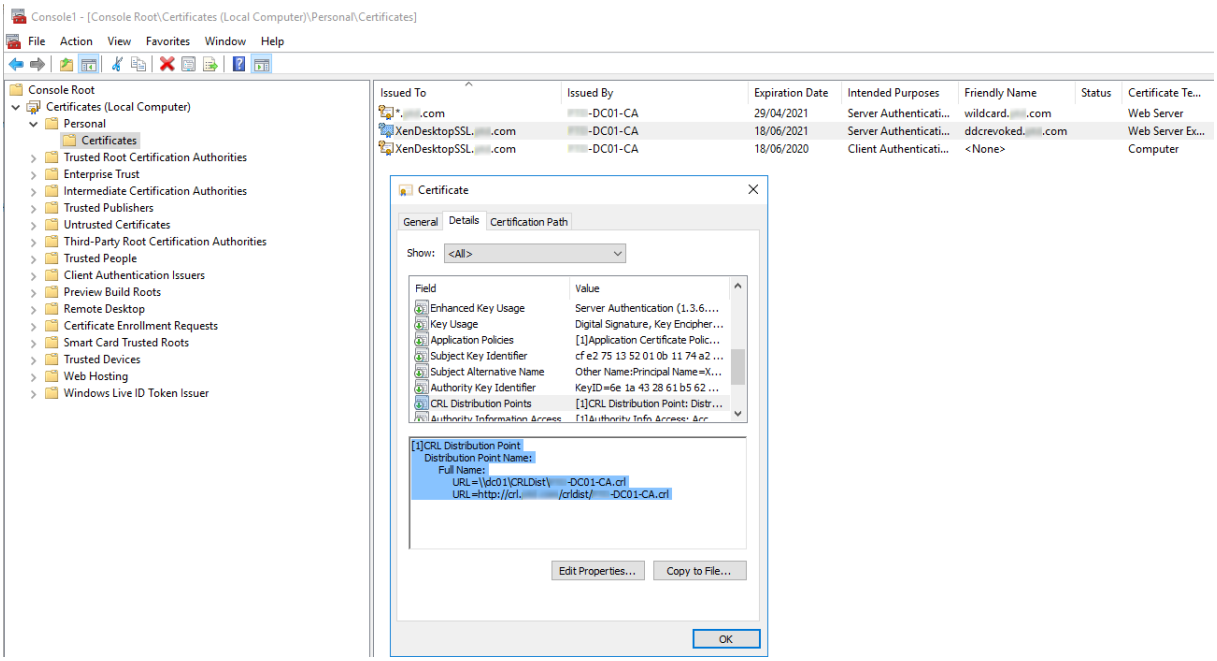
Puede configurar StoreFront para que este compruebe el estado de los certificados TLS que utilizan los utilizados los controladores de entrega de CVAD mediante una lista de revocación de certificados (CRL) publicada. Es posible que deba revocar el acceso a un certificado si:

- cree que la clave privada haya podido desvelarse
- la CA no es segura
- la afiliación ha cambiado
- el certificado se ha reemplazado

> **Nota:**
>
> Este tema solo es relevante cuando se utilizan conexiones HTTPS entre StoreFront y controladores de entrega de Citrix Virtual Apps and Desktops. Las conexiones HTTP a los controladores de entrega no requieren certificado, por lo que el parámetro -CertRevocationPolicy para el almacén, descrito aquí, no tiene ningún efecto.
>
> StoreFront admite la comprobación de revocación de certificados mediante extensiones de certificado de
> puntos de distribución de CRL (CDP) y
> listas de revocación de certificados (CRL) instaladas localmente. StoreFront solo admite listas CRL completas, por lo que no se admiten listas CRL delta.

Extensiones de puntos de distribución CRL (CDP)

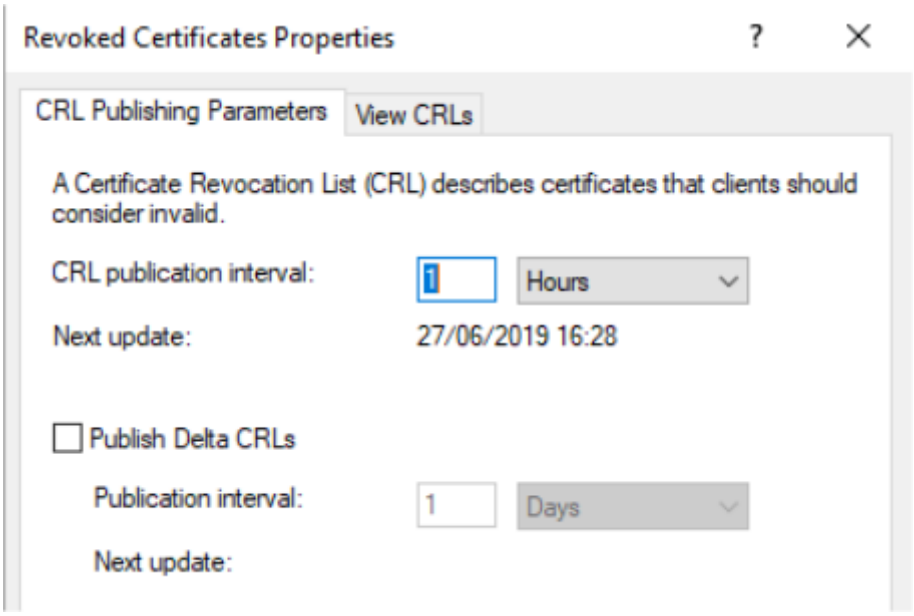
StoreFront no enumera los recursos de los controladores de entrega provenientes de Citrix Virtual Apps and Desktops que utilizan certificados revocados cuyos números de serie aparecen en la lista CRL publicada. Para detectar qué certificados se han revocado, StoreFront debe poder acceder a la CRL publicada mediante una de las URL definidas en las extensiones de certificado CDP.



Intervalo de publicación de CRL

Para que StoreFront detecte los certificados revocados en el Delivery Controller más rápidamente, reduzca el intervalo de publicación de CRL en la CA. Modifique las propiedades de la extensión de puntos

de distribución de CRL para establecer un valor de intervalo de publicación CRL inferior adecuado a su infraestructura de clave pública.



Almacenamiento en caché de listas CRL del cliente

El cliente de infraestructura de clave pública de Windows almacena en caché las CRL localmente. Una CRL más reciente no se descarga hasta que la CRL almacenada localmente haya caducado.

Acceso de StoreFront a listas de revocación de certificados (CRL)

La comprobación de revocación de certificados depende de la capacidad de StoreFront para acceder a las listas CRL. Tenga en cuenta cómo StoreFront se pone en contacto con el servidor web o la entidad de certificación (CA) que publica la CRL, y cómo StoreFront recibe las actualizaciones de CRL.

CA empresariales internas y certificados privados en los controladores de entrega Para utilizar entidades CA y certificados privados, StoreFront necesita una CA de empresa debidamente configurada y una CRL publicada a la que pueda acceder sin salir de la organización ni la red interna. Consulte la documentación de Microsoft para obtener información sobre cómo configurar la CA de empresaria para publicar extensiones CDP. Puede que sea necesario volver a emitir todos los certificados que hubiera en los controladores de entrega que existieran antes de que la CA se configurara para incluir extensiones CDP.

Los servidores de StoreFront y Citrix Virtual Apps and Desktops suelen estar en redes privadas aisladas sin acceso a Internet. En este caso, se deben utilizar CA privadas.

CA públicas externas y certificados públicos en controladores de entrega Los servidores de StoreFront y los controladores de entrega de Citrix Virtual Apps and Desktops pueden usar certificados emitidos por entidades de certificación públicas. StoreFront debe poder establecer contacto con el servidor web de la CA pública a través de Internet mediante la URL a la que se hace referencia en las extensiones CDP. Si StoreFront no puede descargar una copia de la CRL mediante una URL de CDP una vez que se haya revocado un certificado público, StoreFront no puede realizar la comprobación de CRL.

configuración de la directiva de revocación de certificados

Si quiere establecer la directiva de revocación de certificados para un almacén, utilice los cmdlets **Get-STFStoreFarmConfiguration**y **Set-STFStoreFarmConfiguration** de PowerShell para Citrix StoreFront. Tras ejecutar **Get-Help Set-STFStoreFarmConfiguration -detailed**, aparece la ayuda de PowerShell, con ejemplos de la opción -CertRevocationPolicy. Para obtener más información sobre estos cmdlets de PowerShell para StoreFront, consulte Citrix StoreFront SDK PowerShell Modules.

La opción **-CertRevocationPolicy** se puede establecer en los siguientes valores:

Parámetro	Descripción
NoCheck	StoreFront no comprueba el estado de revocación del certificado que haya presente en el controlador de entrega. StoreFront sigue enumerando los recursos provenientes de los controladores de entrega que utilizan certificados revocados. Esta es la opción predeterminada.
MustCheck	Esta es la opción más segura. StoreFront intenta obtener una CRL tras acceder a las URL a las que se hace referencia en las extensiones CDP del certificado en el Delivery Controller. StoreFront no enumera los recursos del Delivery Controller si la CRL no está disponible o si se ha revocado el certificado en uso en el Delivery Controller. La dirección URL puede apuntar a un servidor web interno si el certificado es privado o a un servidor web público de Internet si el certificado es emitido por una entidad de certificación pública.

Parámetro	Descripción
FullCheck	StoreFront intenta acceder a las URL publicadas en las extensiones CDP del certificado del controlador de entrega. Si StoreFront no consigue obtener una copia de la CRL a partir de las URL, sigue permitiendo la enumeración de recursos del Delivery Controller. Si StoreFront obtiene la CRL y se ha revocado el certificado del Delivery Controller, StoreFront no enumera los recursos. La dirección URL puede apuntar a un servidor web interno si el certificado es privado o a un servidor web público de Internet si el certificado es emitido por una entidad de certificación pública.
NoNetworkAccess	Solo se comprueban las CRL, que se han importado localmente en el almacén de certificados de Citrix Delivery Servers en el servidor de StoreFront. StoreFront no intenta ponerse en contacto con ninguna de las URL especificadas en las extensiones CDP. Si StoreFront no consigue obtener una copia local de la CRL, seguirá permitiendo la enumeración de recursos del Delivery Controller. Si StoreFront obtiene una copia local de la CRL proveniente del almacén de certificados de Citrix Delivery Servers y se ha revocado el certificado del Delivery Controller, StoreFront no enumera los recursos.

Configurar un almacén para la comprobación de la revocación de certificados

Para establecer la directiva de revocación de certificados para un almacén, abra PowerShell ISE con **Ejecutar como administrador** y, a continuación, ejecute los siguientes cmdlets de PowerShell. Si tiene varios almacenes, repita este procedimiento en todos ellos. -CertRevocationPolicy es una configuración al nivel del almacén que afecta a todos los Delivery Controllers configurados para el almacén especificado en $StoreVirtualPath.

```
1 $SiteID = 1
2 $StoreVirtualPath = "/Citrix/Store"
```



```
$StoreObject = Get-STFStoreService -SiteId $SiteID -VirtualPath
$StoreVirtualPath
Set-STFStoreFarmConfiguration -StoreService $StoreObject -
    CertRevocationPolicy "MustCheck"
<!--NeedCopy-->
```

Para comprobar que la configuración se ha aplicado correctamente o para ver la configuración actual de
-CertRevocationPolicy, ejecute lo siguiente:

```
(Get-STFStoreFarmConfiguration -StoreService $StoreObject).
    CertRevocationPolicy
<!--NeedCopy-->
```

Usar CRL importadas localmente en el servidor de StoreFront

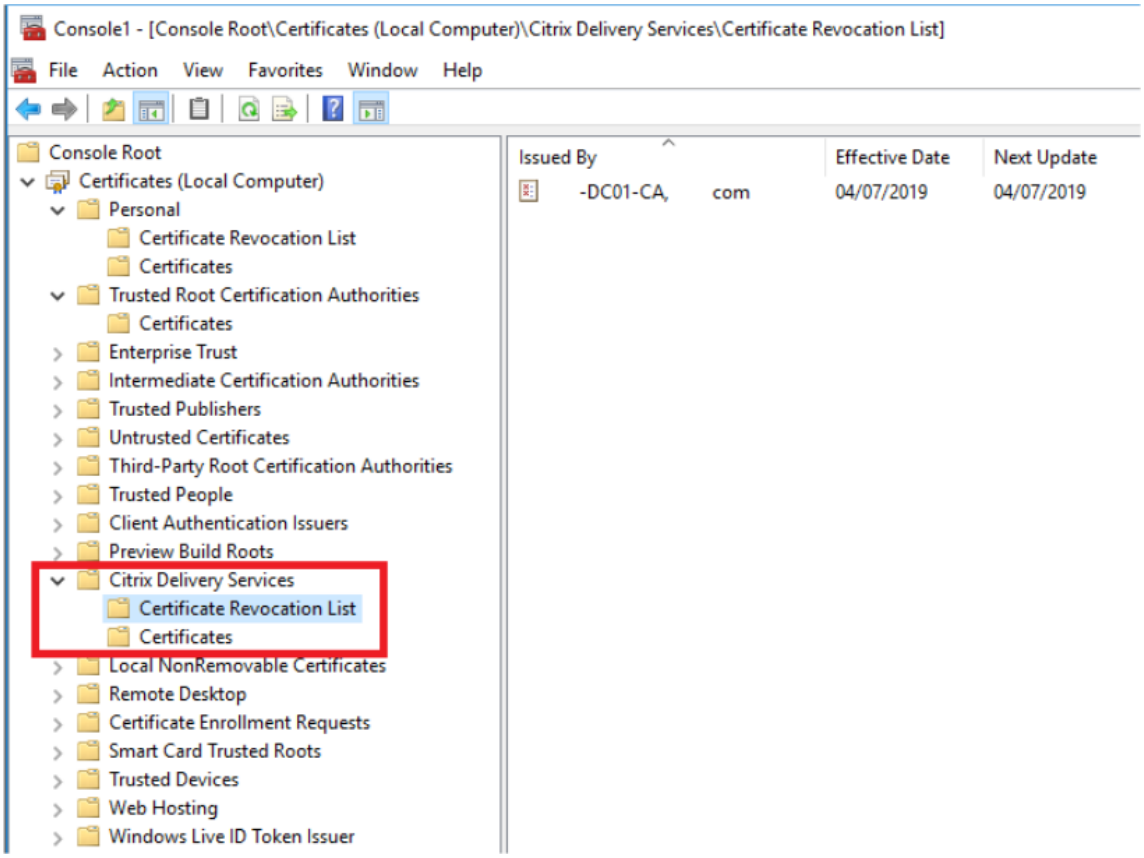
Se pueden usar CRL importadas localmente, aunque Citrix no lo recomienda porque:

- Son difíciles de administrar y actualizar en grandes implementaciones empresariales, donde puede tratarse de varios grupos de servidores de StoreFront.
- La actualización manual de las CRL en cada servidor de StoreFront, cada vez que se revoca un certificado, es mucho menos eficiente que usar extensiones CDP y CRL publicadas en todo el dominio de Active Directory.

El uso de CRL instaladas localmente o actualizadas se puede utilizar si -CertRevocationPolicy se establece en “NoNetworkAccess”y dispone de los medios para distribuir la CRL de manera eficiente a todos los servidores de StoreFront.

Para utilizar CRL importadas localmente

1. Copie la CRL en el escritorio del servidor de StoreFront. Si el servidor de StoreFront forma parte de un grupo de servidores, cópiela a todos los servidores de StoreFront del grupo.
2. Abra el complemento MMC y seleccione **Archivo > Agregar o quitar complementos > Certificados > Cuenta de equipo > Almacén de certificados de Citrix Delivery Services**.
3. Haga clic con el botón secundario y seleccione **Todas las tareas > Importar** y, a continuación, vaya al archivo CRL y elija **Seleccionar todos los archivos > Abrir > Colocar todos los certificados en el siguiente almacén > Citrix Delivery Services**.



Para agregar la CRL al almacén de certificados de Citrix Delivery Services mediante PowerShell o la línea de comandos

1. Inicie sesión en StoreFront y copie el archivo CRL al escritorio del usuario actual.
2. Abra PowerShell ISE y seleccione **Ejecutar como administrador**.
3. Ejecute lo siguiente:

```
1  certutil -addstore "Citrix Delivery Services" "$env:UserProfile\
      Desktop\Example-DC01-CA.crl"
```

Si la operación se lleva a cabo correctamente, el resultado es el siguiente:

```
1  Citrix Delivery Services
2  CRL "CN=Example-DC01-CA, DC=example, DC=com" added to store.
3  CertUtil: -addstore command completed successfully.
```

Puede utilizar este comando como ejemplo para distribuir automáticamente la CRL a todos los servidores de StoreFront de su implementación mediante scripts.

Autenticación XML mediante Delivery Controllers

Puede configurar StoreFront para delegar la autenticación de usuarios en los Delivery Controllers de Citrix Virtual Apps and Desktops. Los usuarios no pueden iniciar sesión en StoreFront si se ha revocado el certificado del Delivery Controller. Este comportamiento es preferible ya que los usuarios de Active Directory no deberían poder iniciar sesión en StoreFront si se ha revocado el certificado del Delivery Controller de Citrix Virtual Apps and Desktops, que es lo que los autentica.

Para delegar la autenticación de usuarios a los Delivery Controllers

1. Configure el almacén para la revocación de certificados tal y como se describe en la sección anterior, Configurar un almacén para la comprobación de la revocación de certificados.
2. Configure el Delivery Controller para que use HTTPS y siga el procedimiento descrito en Autenticación basada en el servicio XML.

Configurar un servicio de autenticación XML para la comprobación de la revocación de certificados

Estos pasos solo son necesarios si utiliza la autenticación XML en su implementación.

> **Nota:**
>
> StoreFront admite dos modelos para asignar almacenes a un servicio de autenticación. El método recomendado es una asignación individual entre almacén y servicio de autenticación. En este caso, debe seguir los pasos de esta sección en todos los almacenes y sus respectivos servicios de autenticación.
>
> Compruebe que el modo de revocación de certificados tiene el mismo valor tanto en el almacén como en el servicio de autenticación. Como alternativa, si la configuración de la autenticación es idéntica para todos los almacenes, se pueden configurar varios almacenes para que compartan un único servicio de autenticación.

Los cmdlets de PowerShell del servicio de autenticación no tienen el equivalente de**Set-STFStoreFarmConfiguration**, por lo que se necesita un estrategia ligeramente diferente con PowerShell. Utilice la misma configuración de directiva de revocación de certificados descrita en la sección anterior.

1. Abra PowerShell ISE y seleccione **Ejecutar como administrador**.

```
$SiteID = 1
$StoreVirtualPath = "/Citrix/Store"
$AuthVirtualPath = "/Citrix/StoreAuth"
<!--NeedCopy-->
```


2. Seleccione el servicio de almacén, el servicio de autenticación y el Delivery Controller para que se utilicen en la autenticación XML. Compruebe que el Delivery Controller ya está configurado para el almacén.

```
$StoreObject = Get-STFStoreService -SiteId $SiteID -VirtualPath
    $StoreVirtualPath
$FarmObject = Get-STFStoreFarm -StoreService $StoreObject -
    FarmName "CVAD"
$AuthObject = Get-STFAuthenticationService -SiteID $SiteID -
    VirtualPath $AuthVirtualPath
<!--NeedCopy-->
```

3. Modifique directamente la propiedad CertRevocationPolicy del servicio de autenticación.

```
$AuthObject.FarmsConfiguration.CertRevocationPolicy = "FullCheck"
$AuthObject.Save()
Enable-STFXmlServiceAuthentication -AuthenticationService
    $AuthObject -Farm $FarmObject
<!--NeedCopy-->
```

4. Confirme que ha establecido el modo de revocación de certificados correcto.

```
$AuthObject = Get-STFAuthenticationService -SiteID 1 -VirtualPath
    $AuthVirtualPath
$AuthObject.FarmsConfiguration.CertRevocationPolicy
<!--NeedCopy-->
```

Errores previsibles del Visor de eventos de Windows

Cuando la comprobación CRL está habilitada, se notifican errores en el Visor de eventos de Windows en el servidor de StoreFront.

Para abrir el Visor de eventos:

- En el servidor de StoreFront, escriba **Run**.
- Escriba **eventvwr** y luego presione Intro.
- En Aplicaciones y servicios, busque eventos de Citrix Delivery Services.

Ejemplo de error: El almacén no puede contactar con un Delivery Controller mediante un certificado revocado

```
An SSL connection could not be established: An error occurred during
    SSL crytography: Access is denied.

This message was reported from the Citrix XML Service at address https:
    //deliverycontrollerTLS.domain.com/scripts/wpnbr.dll.
```



```

The specified Citrix XML Service could not be contacted and has been
    temporarily removed from the list of active services.
<!--NeedCopy-->
```

Ejemplo de error: En Receiver para Web, si el usuario no puede iniciar sesión por un error en la autenticación XML

```
An unexpected response was received during the authentication process.

Citrix.DeliveryServicesClients.Authentication.Exceptions.
    ExplicitAuthenticationFailure,
Citrix.DeliveryServicesClients.Authentication, Version=3.20.0.0,
Culture=neutral, PublicKeyToken=null

General Authentication Failure

ExplicitResult.State: 5

AuthenticationControllerRequestUrl:
https://storefront.example.com/Citrix/StoreWeb/ExplicitAuth/
    LoginAttempt

ActionType: LoginAttempt

at
Citrix.Web.AuthControllers.Controllers.ExplicitAuthController.
    GetExplicitAuthResult(ActionType
type, Dictionary`2 postParams)
<!--NeedCopy-->
```

Configurar dos almacenes de StoreFront para compartir un almacén de datos de suscripción común

January 6, 2020

El proceso de instalación de StoreFront instala localmente un almacén de datos de Windows en cada servidor de StoreFront para mantener sus datos de suscripción. En los entornos de grupos de servidores de StoreFront, cada servidor también mantiene una copia de los datos de suscripción que emplea su almacén. Estos datos se propagan a otros servidores para el mantenimiento de las suscripciones de los usuarios en todo el grupo. De forma predeterminada, StoreFront crea un almacén de datos único para cada almacén. Cada almacén de datos de suscripción se actualiza de forma independiente con respecto a otros almacenes.

Es común que los administradores configuren StoreFront con dos almacenes diferentes allá donde se necesiten diferentes parámetros de configuración. Uno de los almacenes es para el acceso externo a recursos a través de Citrix Gateway y el otro es para el acceso interno a través de la red LAN de la organización. Puede configurar almacenes "externos"e "internos"para compartir un mismo almacén de datos de suscripción con solo realizar un pequeño cambio en el archivo web.config del almacén.

En la situación predeterminada con dos almacenes y sus correspondientes almacenes de datos de suscripción, el usuario debe suscribirse al mismo recurso dos veces. Si se configuran ambos almacenes para compartir una misma base de datos de suscripción, puede mejorar y simplificar la experiencia de los usuarios itinerantes cuando estos acceden al mismo recurso desde dentro o desde fuera de la red corporativa. Con un almacén de datos de suscripción compartido, no importa si usan el almacén "externo"o el "interno"cuando se suscriben por primera vez a un nuevo recurso.

- Cada almacén tiene un archivo web.config ubicado en C:\inetpub\wwwroot\citrix\<storename>.
- Cada archivo web.config contiene un punto final de cliente para el servicio de almacenes de suscripción.

```
<clientEndpoint uri="net.pipe://localhost/Citrix/Subscriptions/1
__Citrix_<StoreName>"authenticationMode="windows"transferMode="
Streamed">
```

Los datos de suscripción de cada almacén se encuentran en:

```
C:\Windows\ServiceProfiles\NetworkService\AppData\Roaming\Citrix\
SubscriptionsStore\1__Citrix_<StoreName>
```

Para que dos almacenes compartan un almacén de datos de suscripción, solo necesita apuntar un almacén al punto final del servicio de suscripción del otro almacén. Si se trata de la implementación de un grupo de servidores, todos los servidores tienen definidos pares idénticos de almacenes y copias idénticas del almacén de datos que comparten.

> Nota:
>
> Los Controllers de Citrix Virtual Apps and Desktops configurados en cada almacén deben coincidir exactamente; de lo contrario, puede haber incoherencias al comparar los conjuntos de suscripciones a recursos de los almacenes. El uso compartido de un almacén de datos solo se admite cuando los dos almacenes se encuentran en el mismo servidor de StoreFront o en la misma implementación de un grupo de servidores.

Puntos finales de los almacenes de datos de suscripción de StoreFront

1. En una implementación de StoreFront, abra el archivo web.config del almacén externo con el Bloc de notas y busque clientEndpoint. Por ejemplo:


```
<subscriptionsStoreClient enabled="true">
<clientEndpoint uri="net.pipe://localhost/Citrix/Subscriptions/1
    __Citrix_External" authenticationMode="windows" transferMode="
    Streamed">
<clientCertificate thumbprint="0" />
</clientEndpoint>
</subscriptionsStoreClient>
<!--NeedCopy-->
```

2. Cambie el punto final del almacén externo para que coincida con el punto final del almacén interno:

```
<subscriptionsStoreClient enabled="true">
<clientEndpoint uri="net.pipe://localhost/Citrix/Subscriptions/1
    __Citrix_Internal" authenticationMode="windows" transferMode="
    Streamed">
<clientCertificate thumbprint="0" />
</clientEndpoint>
</subscriptionsStoreClient>
<!--NeedCopy-->
```

3. Si está usando un grupo de servidores de StoreFront, propague a todos los nodos del grupo los cambios que haya realizado en el archivo web.config del nodo principal.

Ahora, ambos almacenes están configurados para compartir el almacén de datos de suscripción del almacén interno.

Administrar los favoritos de un almacén

February 26, 2024

Puede administrar los datos de suscripción (favoritos) de un almacén mediante cmdlets de PowerShell.

> **Nota:**
>
> Use la consola de administración de StoreFront o PowerShell para administrar StoreFront. No use ambos métodos al mismo tiempo. Cierre siempre la consola de administración de StoreFront antes de usar la consola de PowerShell para cambiar la configuración de StoreFront. Citrix también recomienda que se realice una copia de seguridad de los datos de suscripción existente antes de realizar cambios, de modo que se pueda revertir a un estado anterior.

Purgar datos de suscripción

Para cada almacén de la implementación, existe una carpeta y un almacén de datos de suscripción.

1. Detenga el servicio de suscripciones a almacenes de Citrix en el servidor de StoreFront. Mientras el servicio de suscripciones a almacenes de Citrix esté en ejecución, no se puede eliminar datos de suscripción de ningún almacén.
2. Busque la carpeta de suscripción al almacén, ubicada en el servidor de StoreFront: `C:\Windows\ServiceProfiles\NetworkService\AppData\Roaming\Citrix\SubscriptionsStore\1__Citrix_<StoreName>`
3. Elimine el contenido de la carpeta de suscripción al almacén, pero no elimine la carpeta en sí.
4. Vuelva a iniciar el servicio de suscripciones a almacenes de Citrix en el servidor de StoreFront.

En StoreFront 3.5 o versiones posteriores, puede utilizar el siguiente script de PowerShell para purgar los datos se suscripción a un almacén. Ejecute esta función PowerShell como un administrador con derechos para detener o iniciar servicios y eliminar archivos. Esta función PowerShell tiene el mismo resultado que los pasos manuales descritos anteriormente.

Para ejecutar los cmdlets de manera efectiva, el servicio Citrix Subscriptions Store debe estar ejecutándose en el servidor.

```
function Remove-SubscriptionData
{

    [CmdletBinding()]

    [Parameter(Mandatory=$False)][String]$Store = "Store"

    $SubsService = "Citrix Subscriptions Store"

    # Path to Subscription Data in StoreFront version 2.6 or later

    $SubsPath = "C:\Windows\ServiceProfiles\NetworkService\AppData\
        Roaming\Citrix\SubscriptionsStore\1__Citrix_$Store*"

    Stop-Service -displayname $SubsService

    Remove-Item $SubsPath -Force -Verbose

    Start-Service -displayname $SubsService

    Get-Service -displayname $SubsService
 }


Remove-SubscriptionData -Store "YourStore"
<!--NeedCopy-->
```

Exportar datos de suscripción

Puede obtener una copia de seguridad de los datos de suscripción a un almacén en el formato de archivo TXT con texto separado por tabulaciones. Para ello, ejecute el siguiente cmdlet de Power-

Shell.

```
$StoreObject = Get-STFStoreService -SiteID 1 -VirtualPath "/citrix/<yourstore>"

Export-STFStoreSubscriptions -StoreService $StoreObject -FilePath "$env:USERPROFILE\Desktop\Subscriptions.txt"
```

Si administra una implementación con varios servidores, puede ejecutar este cmdlet de PowerShell en cualquier servidor del grupo de servidores de StoreFront. Cada servidor del grupo de servidores mantiene una copia sincronizada idéntica de los datos de suscripción proveniente de sus homólogos. Si cree que hay problemas con la sincronización de suscripciones entre los servidores de StoreFront, exporte los datos de todos los servidores del grupo y compárelos para ver las diferencias.

Restaurar datos de suscripción

Use Restore-STFStoreSubscriptions para sobrescribir los datos existentes de suscripción. Puede restaurar los datos de suscripción a un almacén con la ayuda de la copia de seguridad del archivo TXT que contiene texto separado con tabulaciones que ha creado antes mediante Export-STFStoreSubscriptions.

```
$StoreObject = Get-STFStoreService -SiteID 1 -VirtualPath "/citrix/<yourstore>"
Restore-STFStoreSubscriptions -StoreService $StoreObject -FilePath "$env:USERPROFILE\Desktop\Subscriptions.txt"
<!--NeedCopy-->
```

Para obtener más información sobre Restore-STFStoreSubscriptions, consulte https://developer-docs.citrix.com/en-us/storefront-powershell-sdk/current-release/Restore-STFStoreSubscriptions/

Restaurar datos en un solo servidor de StoreFront

En una implementación de un solo servidor, no es necesario que finalice el servicio de suscripciones a almacenes. Tampoco es necesario eliminar los datos de suscripción existentes antes de restaurarlos.

Restaurar datos en un grupo de servidores de StoreFront

Para restaurar los datos de suscripción a un grupo de servidores, debe seguir estos pasos.

Ejemplo: implementación de un grupo de tres servidores de StoreFront.

- StoreFrontA
- StoreFrontB

- StoreFrontC

1. Haga una copia de los datos existentes de suscripción que contiene cualquiera de los tres servidores.
2. Detenga el servicio de suscripción a almacenes en los servidores de StoreFrontB y C. Esta acción impide que los servidores envíen o reciban datos de suscripción durante la actualización de StoreFrontA.
3. Purgue los datos de suscripción que contienen los servidores de StoreFrontB y C. Esto impide que haya diferencias entre los datos de suscripción restaurados.
4. Restaure los datos en StoreFrontA con el cmdlet **Restore-STFStoreSubscriptions**. No es necesario detener el servicio de suscripción a almacenes ni eliminar los datos de suscripción presentes en StoreFrontA (se sobrescriben durante la operación de restauración).
5. Vuelva a iniciar el servicio Subscriptions Store en los servidores de StoreFrontB y StoreFrontC. Los servidores ya pueden recibir una copia de los datos procedente de StoreFrontA.
6. Espere a que todos los servidores se sincronicen. El tiempo necesario depende de la cantidad de registros que existan en StoreFrontA. Si todos los servidores se encuentran en una red local, la sincronización suele producirse rápidamente. En cambio, la sincronización de suscripciones a través de una conexión WAN puede tardar más.
7. Exporte los datos de StoreFrontB y C para confirmar que se ha completado la sincronización o consulte los contadores de Store Subscription.

Importar datos de suscripción

Use **Import-STFStoreSubscriptions** cuando no hay datos de suscripción al almacén. Este cmdlet también permite que los datos de suscripción se transfieran de un almacén a otro, además de permitir que esos datos se importen a servidores de StoreFront recién aprovisionados.

```
1 $StoreObject = Get-STFStoreService -SiteID 1 -VirtualPath "/citrix/<
    yourstore>"
2 Import-STFStoreSubscriptions -StoreService $StoreObject -FilePath "$env
    :USERPROFILE\Desktop\Subscriptions.txt"
3 <!--NeedCopy-->
```

Para obtener más información sobre Import-STFStoreSubscriptions, consulte https://developer-docs.citrix.com/en-us/storefront-powershell-sdk/current-release/Import-STFStoreSubscriptions/

Detalles del archivo de datos de suscripción

El archivo de datos de suscripción es un archivo de texto que contiene una línea por suscripción de usuario. Cada línea es una secuencia de valores separada por tabulaciones:

`<user-identifier> <resource-id> <subscription-id> <subscription-status> <property-name> <property-value> <property-name> <property-value> ...`

Donde:

- `<user-identifier>`: Requerido. Una secuencia de caracteres que identifica al usuario. Es el identificador de seguridad de Windows perteneciente al usuario.
- `<resource-id>`: Requerido. Una secuencia de caracteres que identifica los recursos suscritos.
- `<subscription-id>`: Requerido. Una secuencia de caracteres que identifica de forma única la suscripción. Este valor no se utiliza (aunque debe haber un valor presente en el archivo de datos).
- `<subscription-status>`: Requerido. El estado de la suscripción: suscrito o no suscrito.
- `<property-name>` y `<property-value>`: Opcional. Una secuencia de cero o más pares de valores de nombre y valor. Estos representan propiedades asociadas a la suscripción por parte de un cliente StoreFront (suele ser una aplicación Citrix Workspace). Una propiedad del mismo nombre con varios valores, representada por varios pares de nombre y valor (por ejemplo, "…MyProp A MyProp B …"representa la propiedad MyProp con valores A, B).

Ejemplo

S-0-0-00-0000000000-0000000000-0000000000-0000 XenApp.Excel 21EC2020-3AEA-4069-A2DD-08002B30309D Subscribed dazzle:position 1

Tamaño de los datos de suscripción en el disco del servidor de StoreFront

Cantidad de registros	Tamaño en MB
0	6,02
1000	7,02
10 000	40,00
100 000	219,00
200 000	358,00
500 000	784,00
800 000	1213,02
1 000 000	1597,15

Cantidad de registros	Tamaño en MB
1 300 000	1919,15
1 500 000	2205,15
2 000 000	2915,15

Tamaño de archivos TXT importados y exportados

Cantidad de registros	Tamaño en MB
0	0,00
1000	0,13
10 000	1,30
100 000	12,80
200 000	25,60
500 000	64,10
800 000	102,00
1 000 000	1128,00
1 300 000	166,00
1 500 000	192,00
1 700 000	218,00
2 000 000	256,00

Contadores de Store Subscription

Puede usar los contadores de los monitores de rendimiento Windows de Microsoft (**Inicio > Ejecutar > perfmon**) para ver, por ejemplo, la cantidad total de registros de suscripción existente en el servidor o la cantidad de registros que se sincroniza entre grupos de servidores de StoreFront.

Ver contadores de suscripción mediante PowerShell

```
Get-Counter -Counter "\Citrix Subscription Store(1__citrix_store)\
    Subscription Entries Count (including unpurged deleted records)"

```



```
Get-Counter -Counter "\Citrix Subscription Store Synchronization\
    Subscriptions Store Synchronizing"

Get-Counter -Counter "\Citrix Subscription Store Synchronization\Number
     Subscriptions Synchronized"

Get-Counter -Counter "\Citrix Subscription Store Synchronization\Number
     Subscriptions Transferred"
<!--NeedCopy-->
```

Almacenar datos de suscripción mediante Microsoft SQL Server

April 17, 2024

> **Nota:**
>
> En este documento, se presupone que tiene conocimientos básicos de MS SQL Server y las consultas T-SQL. Los administradores deben estar familiarizados con la configuración, uso y administración de SQL Server antes de intentar seguir este documento.

Introducción

ESENT es un motor de base de datos transaccional incrustable que se puede usar con Windows. Todas las versiones de StoreFront son compatibles de forma predeterminada con el uso de una base de datos ESENT integrada. También pueden conectarse a una instancia de Microsoft SQL Server si el almacén está configurado para utilizar una cadena de conexión SQL.

La principal ventaja de cambiar StoreFront para uso de SQL, en lugar de ESENT, es que las instrucciones de actualización T-SQL le permiten administrar, modificar o eliminar registros de suscripción. Si utiliza SQL, no es necesario exportar, modificar ni volver a importar todos los datos de suscripción de ESENT cada vez que se hagan cambios menores en estos.

Para migrar los datos de suscripción de ESENT a Microsoft SQL Server, los datos planos de ESENT exportados desde StoreFront deben transformarse a un formato de fácil lectura para la importación en bloque en SQL. Para nuevas implementaciones sin nuevos datos de suscripción, este paso no es necesario. El paso de transformación de los datos solo es necesario completarlo una vez. En este artículo, se describe la configuración compatible que puede utilizarse en todas las versiones de StoreFront, a partir de la versión 3.5, en la que se introdujo el SDK de PowerShell -STF al que se hace referencia.

> **Nota:**
>
> Los fallos en la conexión a la instancia de SQL Server utilizada por StoreFront para almacenar los

> datos de suscripción debido a interrupciones en la red no hacen inutilizable la implementación de StoreFront. Las interrupciones solo afectan temporalmente a la experiencia de usuario: los usuarios no pueden agregar, quitar o ver sus recursos favoritos hasta que se restaura la conexión con el servidor SQL. Los recursos sí se pueden enumerar e iniciar durante la interrupción. El comportamiento previsto es el mismo que si el servicio Citrix Subscription Store se detuviera durante el uso de ESENT.
>
> **Consejo:**
>
> Los recursos configurados con las palabras clave Auto o Mandatory funcionan de la misma manera cuando se utilizan con ESENT o SQL. Los nuevos registros de suscripción de SQL se crean automáticamente cuando un usuario inicia sesión por primera vez si se incluye cualquiera de esas dos palabras clave en los recursos del usuario.

Ventajas de ESENT y SQL Server

ESENT	SQL
Predeterminado y no requiere configuración adicional para usar StoreFront “estándar”.	Mucho más manejable, y los datos de suscripción se pueden manipular o actualizar fácilmente mediante consultas T-SQL. Permite eliminar o actualizar registros por usuario. Permite hacer recuento de registros por aplicación, Delivery Controller o usuario. Ofrece un medio fácil para eliminar datos de usuario innecesarios cuando los usuarios dejan la empresa/organización. Ofrece una manera fácil de actualizar las referencias de los Delivery Controllers, por ejemplo, cuando el administrador cambia a uso de agregación o se aprovisionan nuevos Delivery Controllers.
Más fácil de configurar la replicación entre diferentes grupos de servidores mediante la sincronización de suscripciones y las programaciones de extracción. Consulte Configurar la sincronización de suscripciones.	Separado de StoreFront, por lo que no es necesario hacer copia de seguridad de los datos de suscripción antes de actualizar StoreFront, ya que los datos se conservan en un servidor SQL independiente. La copia de seguridad de las suscripciones es independiente de StoreFront y utiliza estrategias y mecanismos de copia de seguridad de SQL.

ESENT	SQL
SQL no es necesario cuando no se necesita administrar suscripciones. Si los datos de suscripción nunca necesitarán actualizarse, es probable que ESENT satisfaga las necesidades del cliente.	Una sola copia de los datos de suscripción que comparten todos los miembros del grupo de servidores, lo que reduce la probabilidad de que haya discrepancias en los datos de los distintos servidores o problemas de sincronización de datos.

Desventajas de ESENT y SQL Server

ESENT	SQL
No es fácil administrar los datos de suscripción de forma sencilla y granular. Requiere que la manipulación de las suscripciones se haga en archivos TXT exportados. Obliga a exportar y volver a importar toda la base de datos de suscripción. Posibilidad de tener que cambiar miles de registros mediante técnicas de búsqueda y reemplazo, que requieren mucho esfuerzo y son propensas a errores.	Requiere infraestructura y conocimientos básicos de SQL. Puede requerir la compra de una licencia SQL, lo que aumenta el coste total de propiedad de la implementación de StoreFront. Aun así, es posible compartir una instancia de base de datos de Citrix Virtual Apps and Desktops con StoreFront para reducir los costes.
Es necesario mantener una copia de la base de datos ESENT en cada servidor de StoreFront de un grupo de servidores. En raras ocasiones, esta base de datos puede desincronizarse dentro de un grupo de servidores o entre diferentes grupos de servidores.	Replicar datos de suscripción entre grupos de servidores no es una tarea de implementación trivial. Requiere múltiples instancias de SQL y replicación de transacciones entre cada una de ellas para cada centro de datos. Esto requiere unos conocimientos especializados de MS SQL. Requiere la migración de datos de ESENT y la transformación a un formato de fácil lectura para SQL. Este proceso solo se requiere una vez. Es posible que se necesiten licencias y servidores Windows adicionales. Pasos adicionales para implementar StoreFront.

Escenarios de implementación

> **Nota:**
>
> Cada almacén configurado en StoreFront requiere una base de datos ESENT o una base de datos de Microsoft SQL para compatibilidad con suscripciones de usuario. El método de almacenamiento de los datos de suscripción se establece en el nivel de almacén dentro de StoreFront.

Citrix recomienda que todas las bases de datos de almacenes residan en la misma instancia de Microsoft SQL Server para reducir la complejidad de la administración y la posibilidad de una configuración incorrecta.

Varios almacenes pueden compartir la misma base de datos, siempre que estén configurados para usar una cadena de conexión idéntica. No importa si utilizan Delivery Controllers diferentes. La desventaja de que varios almacenes compartan una misma base de datos es que no hay forma de saber a qué almacén corresponde cada registro de suscripción.

Una combinación de los dos métodos de almacenamiento de datos es técnicamente posible en una misma implementación de StoreFront con varios almacenes Es posible configurar un almacén para uso de ESENT y otro para uso de SQL. Esto no se recomienda debido a la mayor complejidad de la administración y a la posibilidad de una configuración incorrecta.

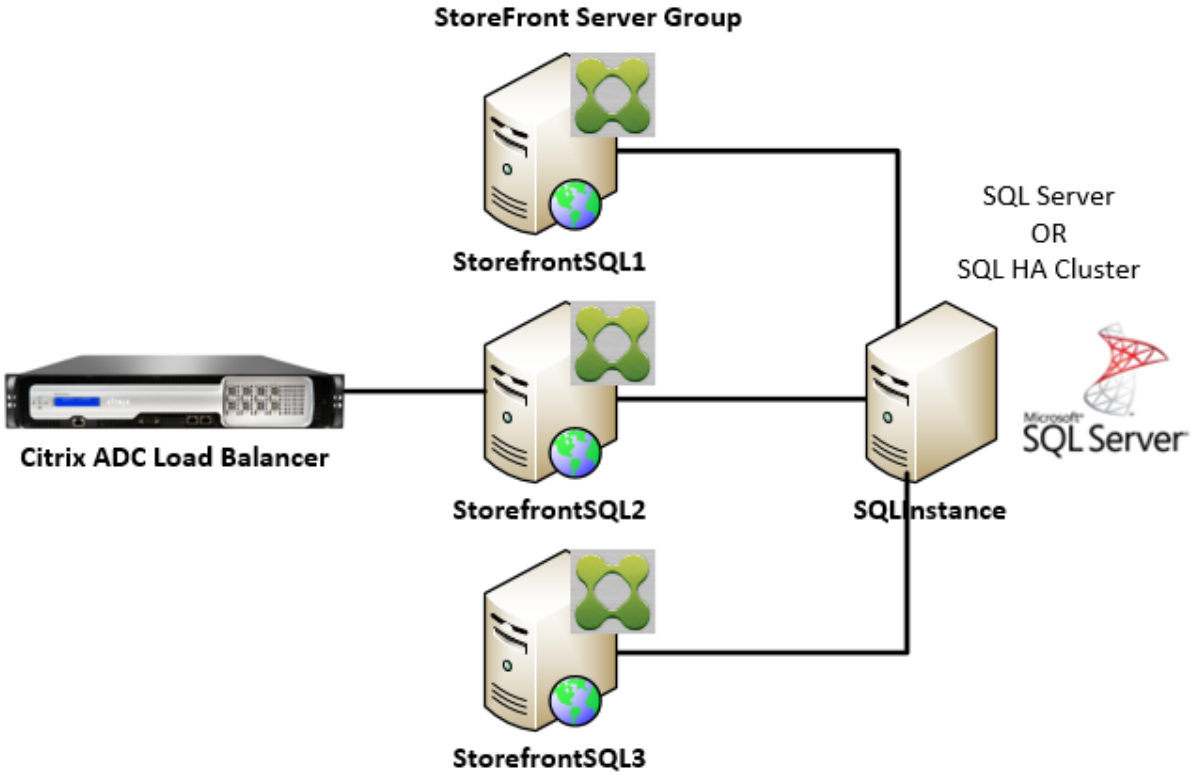
Hay cuatro escenarios que puede usar para almacenar datos de suscripción en SQL Server:

Escenario 1: Un único servidor o grupo de servidores de StoreFront con ESENT (predeterminado) De forma predeterminada, todas las versiones de StoreFront a partir de la versión 2.0 utilizan una base de datos ESENT plana para almacenar y replicar datos de suscripción entre miembros de un grupo de servidores. Cada miembro del grupo de servidores mantiene una copia idéntica de la base de datos de suscripción, que se sincroniza con todos los demás miembros del grupo. Este escenario no requiere pasos de configuración adicionales. Además, es adecuado para la mayoría de los clientes que no prevén cambios frecuentes en los nombres de los Delivery Controllers o que no necesitan realizar tareas de administración con frecuencia en los datos de suscripción, como eliminar o actualizar suscripciones de usuario antiguas.

Escenario 2: Un único servidor de StoreFront y una instancia local de Microsoft SQL Server StoreFront utiliza una instancia de SQL Server instalada localmente y ambos componentes residen en el mismo servidor. Este escenario es adecuado para una implementación simple de StoreFront en la que los clientes podrían necesitar hacer cambios frecuentes en los nombres de los Delivery Controllers o realizar tareas de administración con frecuencia en los datos de suscripción, como eliminar o actualizar suscripciones de usuario antiguas, pero no requieren una implementación de StoreFront de alta disponibilidad. Citrix no recomienda este escenario para grupos de servidores, ya

que da lugar a un punto único de error en el miembro del grupo de servidores que aloja la instancia de base de datos de Microsoft SQL. Este escenario no es adecuado para implementaciones en grandes empresas.

Escenario 3: Un grupo de servidores de StoreFront y una instancia dedicada de Microsoft SQL Server configurada para alta disponibilidad (recomendado) Todos los miembros del grupo de servidores de StoreFront se conectan a la misma instancia dedicada de Microsoft SQL Server o clúster de conmutación por error SQL. Este es el modelo más adecuado para implementaciones en grandes empresas, en las que los administradores de Citrix desean realizar cambios frecuentes en los nombres de los Delivery Controllers o realizar tareas de administración frecuentes en los datos de suscripción, como eliminar o actualizar suscripciones de usuario antiguas y requieren alta disponibilidad.

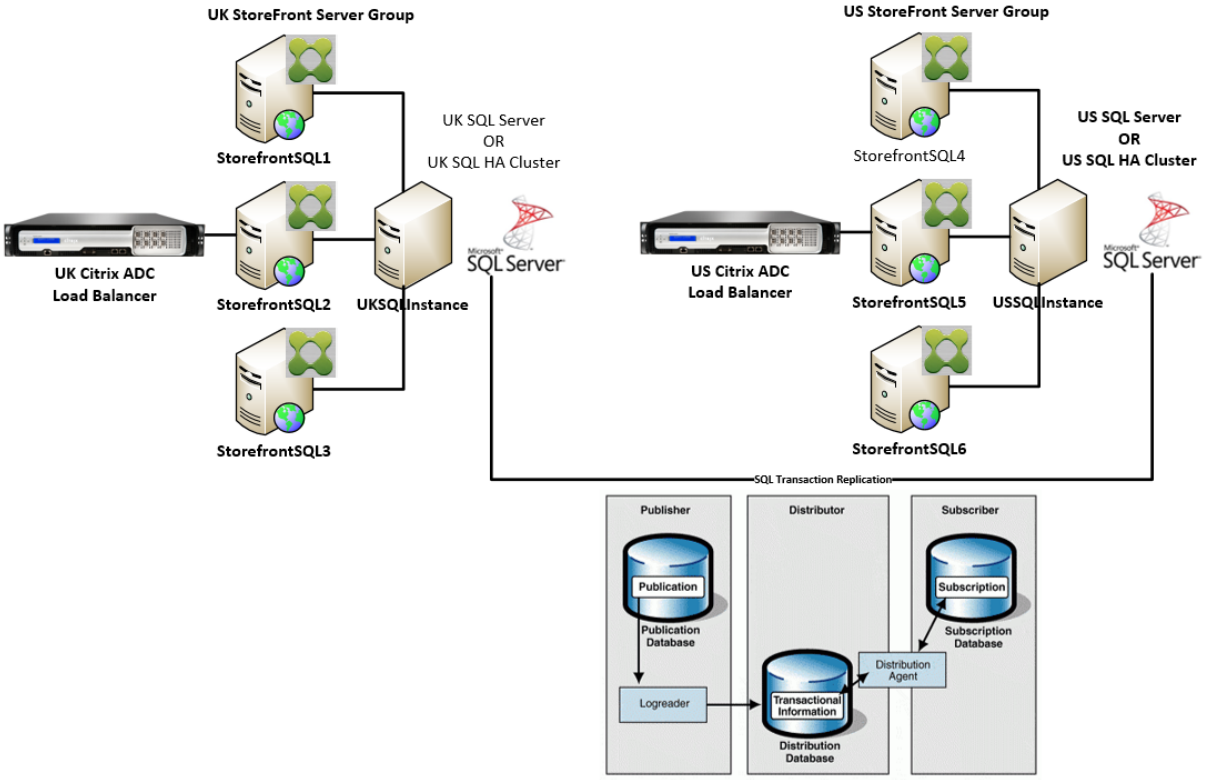


Escenario 4: Varios grupos de servidores de StoreFront y una instancia dedicada de Microsoft SQL Server en cada centro de datos para cada grupo de servidores

> **Nota:**
>
> Esta es una configuración avanzada. Inténtelo solo si es un administrador de SQL Server experimentado, está familiarizado con la replicación de transacciones y tiene las competencias necesarias para implementarlo correctamente.

Se trata de la misma situación que la 3, pero ampliada a situaciones en las que se requieren varios

grupos de servidores de StoreFront en diferentes centros de datos remotos. Los administradores de Citrix pueden elegir sincronizar los datos de suscripción entre diferentes grupos de servidores del mismo centro de datos o de diferentes centros de datos. Cada grupo de servidores del centro de datos se conecta a su propia instancia dedicada de Microsoft SQL Server para optimizar la redundancia, la conmutación por error y el rendimiento. Este escenario requiere una infraestructura y configuración de servidores Microsoft SQL extra considerables. Confía plenamente en la tecnología de Microsoft SQL para replicar los datos de suscripción y las transacciones SQL.



Recursos

Puede descargar los siguientes scripts de https://github.com/citrix/sample-scripts/tree/master/storefront como ayuda:

Scripts de configuración

- **Set-STFDatabase.ps1**: establece la cadena de conexión MS SQL para cada almacén. Se ejecuta en el servidor de StoreFront.
- **Add-LocalAppPoolAccounts.ps1**: concede a los grupos de aplicaciones locales del servidor de StoreFront acceso de lectura y escritura a la base de datos SQL. Se ejecuta para el escenario 2 en el servidor SQL.

- **Add-RemoteSFAccounts.ps1**: concede a todos los servidores de StoreFront de un grupo de servidores acceso de lectura y escritura a la base de datos SQL. Se ejecuta para el escenario 3 en el servidor SQL.
- **Create-StoreSubscriptionsDB-2016.sql**: crea el esquema y la base de datos SQL. Se ejecuta en el servidor SQL.

Scripts de transformación e importación de datos

- **Transform-SubscriptionDataForStore.ps1**: exporta y transforma los datos de suscripción existentes en ESENT a un formato de fácil lectura para importación en SQL.
- **Create-ImportSubscriptionDataSP.sql**: crea un procedimiento almacenado para importar los datos transformados con Transform-SubscriptionDataForStore.ps1. Ejecute este script una vez en el servidor SQL, después de haber creado el esquema de base de datos con Create-StoreSubscriptionsDB-2016.sql.

Configurar el grupo de seguridad local del servidor de StoreFront en SQL Server

Escenario 2: Un único servidor de StoreFront y una instancia local de Microsoft SQL Server

Cree un grupo de seguridad local llamado `<SQLServer>\StoreFrontServers` en el servidor Microsoft SQL y agregue las cuentas virtuales para `IIS APPPOOL\DefaultAppPool` y `IIS APPPOOL\Citrix Receiver for Web` para permitir que la instancia de StoreFront instalada localmente pueda leer y escribir en SQL. A este grupo de seguridad se hace referencia en el script .SQL que crea el esquema de base de datos de suscripciones del almacén, por lo que deberá asegurarse de que el nombre del grupo coincide.

Puede descargar el script Add-LocalAppPoolAccounts.ps1 para ayudarle.

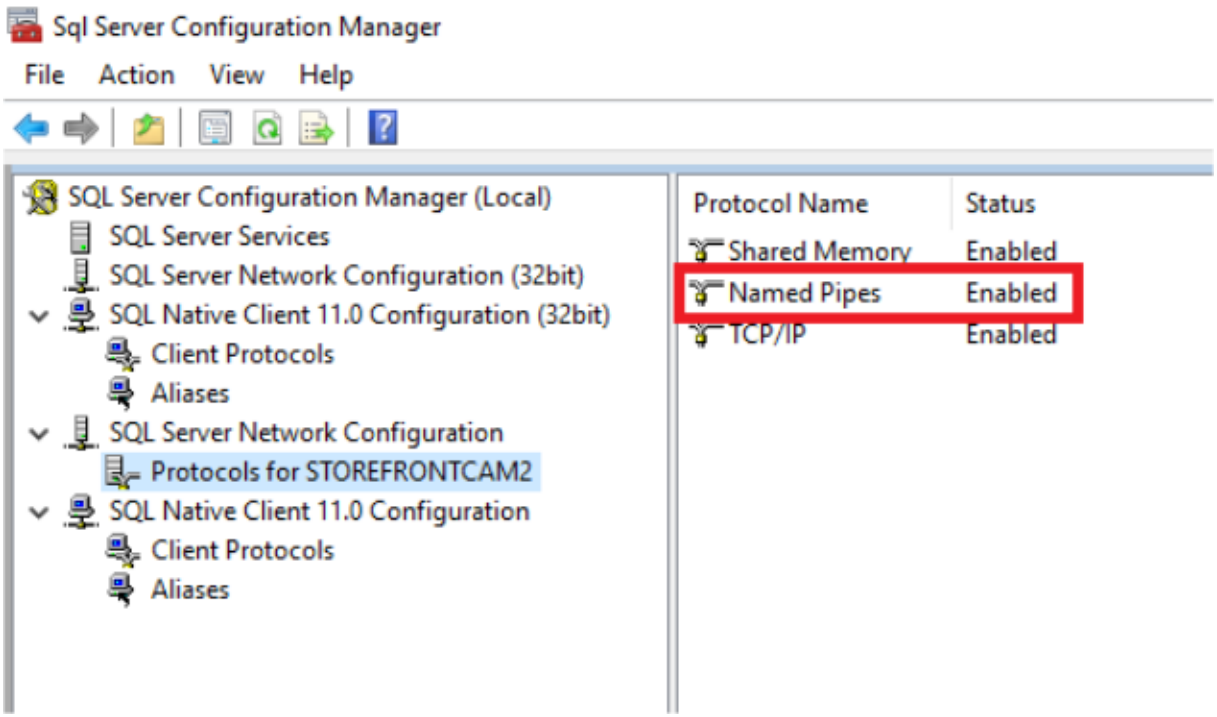
Instale StoreFront antes de ejecutar el script *Add-LocalAppPoolAccounts.ps1*. El script depende de la capacidad de localizar la cuenta virtual de IIS `IIS APPPOOL\Citrix Receiver for Web`, que no existe hasta que StoreFront se ha instalado y configurado. `IIS APPPOOL\DefaultAppPool` se crea automáticamente al instalar el rol de servidor web de IIS.

```
# Create Local Group for StoreFront servers on DB Server
$LocalGroupName = "StoreFrontServers"
$Description = "Contains StoreFront Server Machine Accounts or
    StoreFront AppPool Virtual Accounts"

# Check whether the Local Group Exists
if ([ADSI]::Exists("WinNT://$env:ComputerName/$LocalGroupName"))
{

    Write-Host "$LocalGroupName already exists!" -ForegroundColor "
        Yellow"
```



```
10  }
11
12 else
13 {
14
15 Write-Host "Creating $LocalGroupName local security group" -
      ForegroundColor "Yellow"
16
17 # Create Local User Group
18 $Computer = [ADSI]"WinNT://$env:ComputerName,Computer"
19 $LocalGroup = $Computer.Create("group",$LocalGroupName)
20 $LocalGroup.setinfo()
21 $LocalGroup.description = $Description
22 $Localgroup.SetInfo()
23 Write-Host "$LocalGroupName local security group created" -
      ForegroundColor "Green"
24  }
25
26 $Group = [ADSI]"WinNT://$env:ComputerName/$LocalGroupName,group"
27
28 # Add IIS APPPOOL\DefaultAppPool
29 $objAccount = New-Object System.Security.Principal.NTAccount("IIS
      APPPOOL\DefaultAppPool")
30 $StrSID = $objAccount.Translate([System.Security.Principal.
      SecurityIdentifier])
31 $DefaultSID = $StrSID.Value
32
33 $Account = [ADSI]"WinNT://$DefaultSID"
34 $Group.Add($Account.Path)
35
36 # Add IIS APPPOOL\Citrix Receiver for Web
37 $objAccount = New-Object System.Security.Principal.NTAccount("IIS
      APPPOOL\Citrix Receiver for Web")
38 $StrSID = $objAccount.Translate([System.Security.Principal.
      SecurityIdentifier])
39 $WebRSID = $StrSID.Value
40
41 $Account = [ADSI]"WinNT://$WebRSID"
42 $Group.Add($Account.Path)
43
44 Write-Host "AppPools added to $LocalGroupName local group" -
      ForegroundColor "Green"
45 <!--NeedCopy-->
```

Habilite las canalizaciones con nombre en su instancia SQL local con Administrador de configuración de SQL Server. Las canalizaciones con nombre son necesarias para la comunicación entre procesos entre StoreFront y SQL Server.

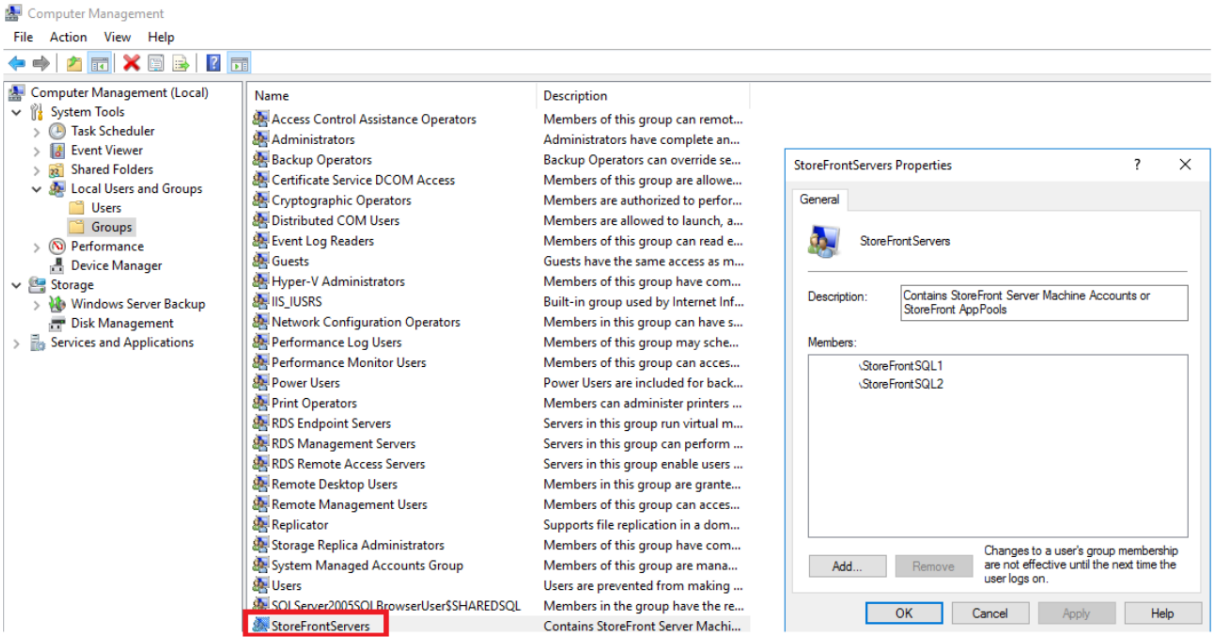


Asegúrese de que las reglas del firewall de Windows están configuradas correctamente para permitir conexiones de SQL Server a través de un puerto específico o de puertos dinámicos. Consulte la documentación de Microsoft para saber cómo hacerlo en su entorno.

> **Consejo:**
>
> Si se produce un error en la conexión a la instancia SQL local, compruebe que localhost o <`hostname`> utilizado en la cadena de conexión se resuelve en la dirección IPv4 correcta. Windows podría intentar usar IPv6 en lugar de IPv4, y la resolución DNS de localhost podría devolver ::1 en lugar de la dirección IPv4 correcta del servidor de StoreFront y SQL. Puede ser necesario inhabilitar completamente la pila de red IPv6 en el servidor host para resolver este problema.

Escenario 3: Un grupo de servidores de StoreFront y una instancia dedicada de Microsoft SQL Server

Cree un grupo de seguridad local llamado <`SQLServer`>\`StoreFrontServers` en el servidor Microsoft SQL y agregue todos los miembros del grupo de servidores de StoreFront. A este grupo de seguridad se hace referencia más adelante en el script **Create-StoreSubscriptionsDB-2016.sql** que crea el esquema de base de datos de suscripciones dentro de SQL.



Agregue todas las cuentas de equipo de dominio del grupo de servidores de StoreFront al grupo <SQLServer>\StoreFrontServers. Solo las cuentas de equipo de dominio de servidor de StoreFront enumeradas en el grupo podrán leer y escribir registros de suscripción en SQL si el servidor SQL utiliza la autenticación de Windows. Esta función de PowerShell, proporcionada en el script Add-RemoteSFAccounts.ps1, crea el grupo de seguridad local y le agrega dos servidores de StoreFront denominados StoreFrontSQL1 y StoreFrontSQL2.

```
function Add-RemoteSTFMachineAccounts
{

[CmdletBinding()]
param([Parameter(Mandatory=$True)][string]$Domain,
[Parameter(Mandatory=$True)][array]$StoreFrontServers)

# Create Local Group for StoreFront servers on DB Server
$LocalGroupName = "StoreFrontServers"
$Description = "Contains StoreFront Server Machine Accounts or
    StoreFront AppPool virtual accounts"

# Check whether the Local Security Group already exists
if ([ADSI]::Exists("WinNT://$env:ComputerName/$LocalGroupName"))
{

    Write-Host "$LocalGroupName already exists!" -ForegroundColor "
        Yellow"
 }

else
{

    Write-Host "Creating $LocalGroupName local group" -ForegroundColor
```

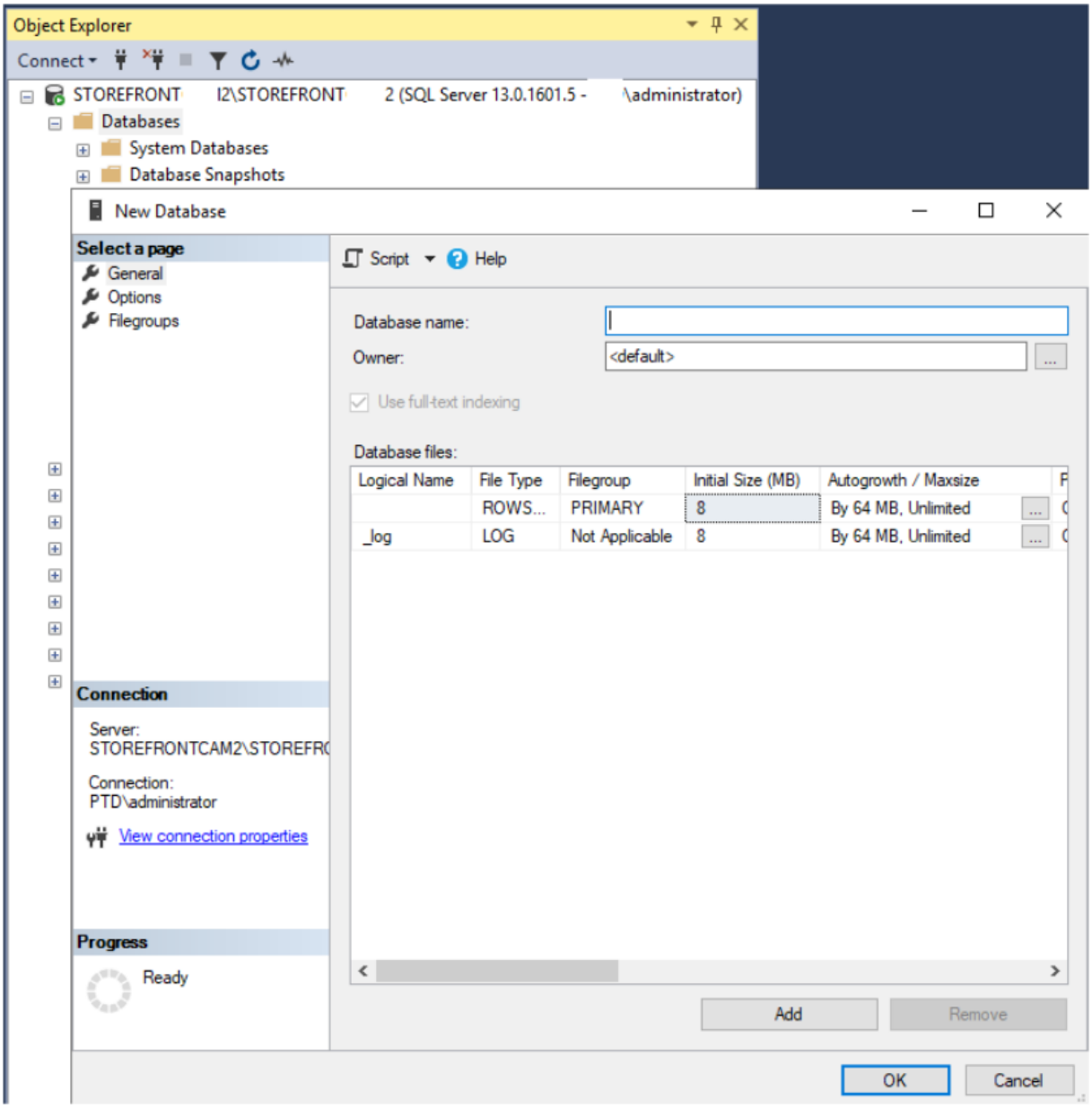


```
        "Yellow"

    # Create Local Security Group
    $Computer = [ADSI]"WinNT://$env:ComputerName,Computer"
    $LocalGroup = $Computer.Create("group",$LocalGroupName)
    $LocalGroup.setinfo()
    $LocalGroup.description = $Description
    $Localgroup.SetInfo()
Write-Host "$LocalGroupName local group created" -ForegroundColor "Green"
 }

Write-Host "Adding $StoreFrontServers to $LocalGroupName local group" -ForegroundColor "Yellow"

foreach ($StoreFrontServer in $StoreFrontServers)
{

    $Group = [ADSI]"WinNT://$env:ComputerName/$LocalGroupName,group"
    $Computer = [ADSI]"WinNT://$Domain/$StoreFrontServer$"
    $Group.Add($Computer.Path)
 }

Write-Host "$StoreFrontServers added to $LocalGroupName" -ForegroundColor "Green"
 }

Add-RemoteSTFMachineAccounts -Domain "example" -StoreFrontServers @("StoreFrontSQL1","StoreFrontSQL2")
<!--NeedCopy-->
```

Configurar el esquema de base de datos de suscripciones en Microsoft SQL Server para cada almacén

Cree una instancia con nombre en el servidor Microsoft SQL para uso en StoreFront. Establezca la ruta de acceso en el script .SQL para que se corresponda con el lugar donde está instalada la versión de SQL o donde se almacenan sus archivos de base de datos. El script de ejemplo Create-StoreSubscriptionsDB-2016.sql usa SQL Server 2016 Enterprise.

Haga clic con el botón derecho del mouse en **Bases de datos** y seleccione **Nueva base de datos** para crear una base de datos vacía con SQL Server Management Studio (SSMS).



Introduzca un **nombre de base de base de datos** que coincida con el de su almacén o elija otro nombre, como *STFSubscriptions*.

Antes de ejecutar el script, para cada almacén de la implementación de StoreFront, modifique las referencias del script de ejemplo para que coincidan con las implementaciones de StoreFront y SQL. Por ejemplo, modifique:

- Asigne un nombre a cada base de datos que cree, de manera que coincida con el nombre del almacén de StoreFront en `USE [STFSubscriptions]`.
- Establezca la ruta de acceso a los archivos .mdf y .ldf de la base de datos donde quiere almacenar esta.


```
C:\Program Files\Microsoft SQL Server\MSSQL13.SQL2016\MSSQL\DATA\
STFSubscriptions.mdf
```

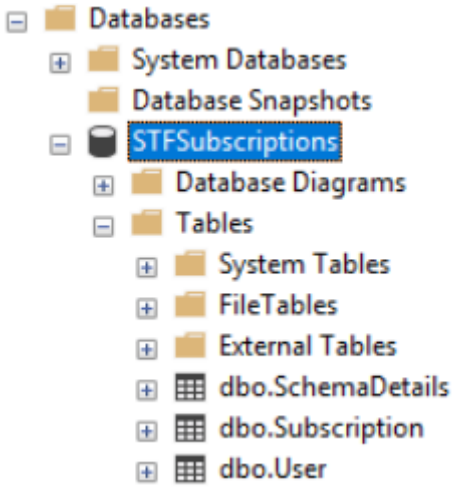
```
C:\Program Files\Microsoft SQL Server\MSSQL13.SQL2016\MSSQL\DATA\
STFSubscriptions.ldf
```

- Establezca la referencia al nombre de su servidor SQL dentro del script:

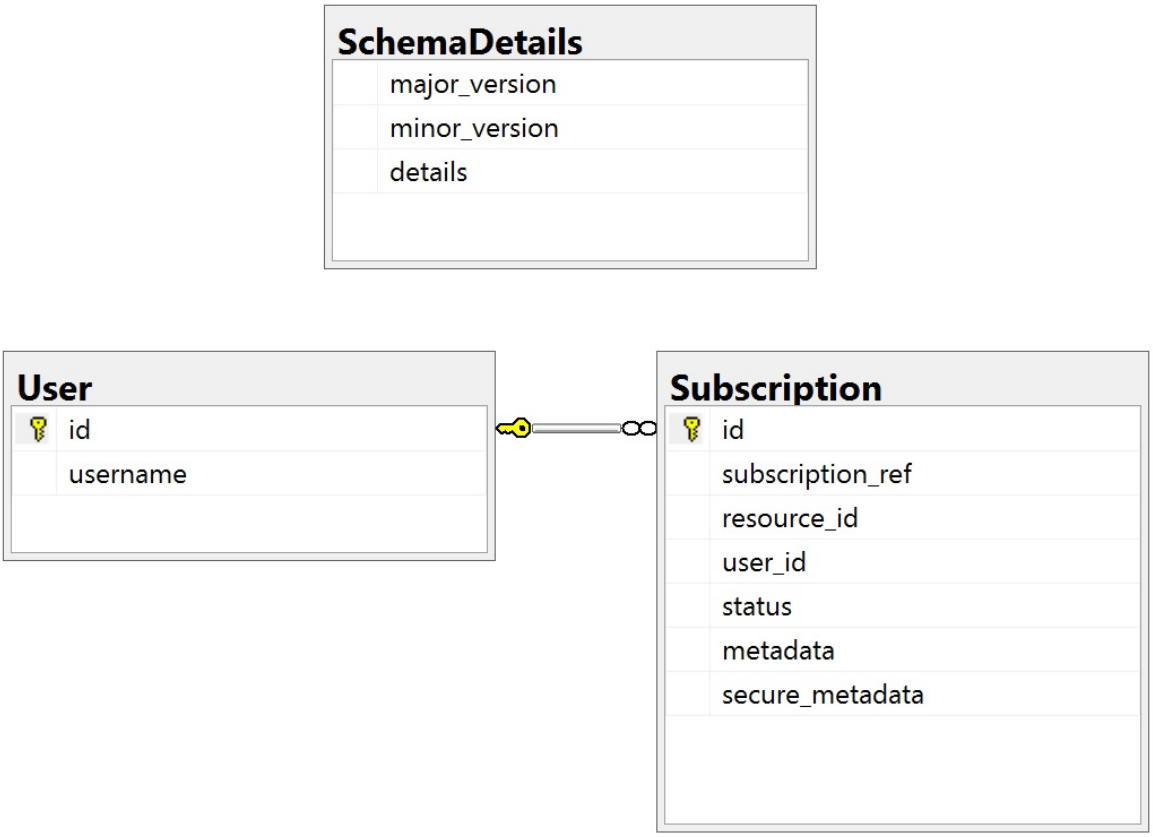
```
CREATE LOGIN [SQL2016\StoreFrontServers] FROM WINDOWS;
```

```
ALTER LOGIN [SQL2016\StoreFrontServers]
```

Ejecute el script. Después de configurar correctamente el esquema, se crean tres tablas de base de datos: *SchemaDetails*, *Subscription* y *User*.



El siguiente diagrama de base de datos muestra el esquema de base de datos de suscripciones que crea el script *Create-StoreSubscriptionsDB-2016.sql*:



Configurar la cadena de conexión de SQL Server para cada almacén de StoreFront

Caso 1

> **Consejo:**
>
> Los datos de suscripción originales almacenados en disco en la base de datos ESENT no se destruyen ni eliminan. Si decide revertir de Microsoft SQL Server a ESENT, es posible quitar la cadena de conexión del almacén y volver a utilizar los datos originales. Las suscripciones adicionales que se crearon mientras SQL estaba en uso para el almacén no existirán en ESENT, y los usuarios no podrán ver estos nuevos registros de suscripción. Todos los registros de suscripciones originales seguirán estando presentes.

Para volver a habilitar suscripciones ESENT en un almacén Abra PowerShell ISE y seleccione **Ejecutar como administrador**.

Utilice la opción **-UseLocalStorage** para especificar el almacén en el que quiere volver a habilitar las suscripciones ESENT:

```
$SiteID = 1
```



```
$StoreVirtualPath = "/Citrix/Store1"

# Sets SQL DB Connection String
$StoreObject = Get-STFStoreService -SiteID $SiteID -VirtualPath
    $StoreVirtualPath

# Removes the SQL DB Connection string and reverts back to using ESENT
Set-STFStoreSubscriptionsDatabase -StoreService $StoreObject -
    UseLocalStorage
Get-STFStoreSubscriptionsDatabase -StoreService $StoreObject
<!--NeedCopy-->
```

Escenarios 2, 3 y 4

Abra PowerShell ISE y seleccione **Ejecutar como administrador**.

Especifique el almacén para el que quiere establecer una cadena de conexión para usar **$StoreVirtualPath**

```
$SiteID = 1
$VirtualPath= "/Citrix/Store1"
$DBName = "Store1"
$DBServer = "SQL2016Ent"
$DBLocalServer = "localhost"
$SQLInstance = "StoreFrontInstance"

# For a remote database instance
$ConnectionString = "Server=$DBServer$SQLInstance;Database=$DBName;
    Trusted_Connection=True;"
<!--NeedCopy-->
```

O BIEN:

```
# For a locally installed database instance
$ConnectionString = "$DBLocalServer$SQLInstance;Database=$DBName;
    Trusted_Connection=True;"

# Sets SQL DB Connection String
$StoreObject = Get-STFStoreService -SiteID $SiteID -VirtualPath "/
    Citrix/Store"
Set-STFStoreSubscriptionsDatabase -StoreService $StoreObject -
    ConnectionString $ConnectionString
Get-STFStoreSubscriptionsDatabase -StoreService $StoreObject
<!--NeedCopy-->
```

Repita el proceso para cada almacén de la implementación si quiere configurarlos todos para que utilicen una cadena de conexión SQL.

Migrar datos existentes de ESENT a Microsoft SQL Server

Para migrar los datos existentes de ESENT a SQL se requiere un proceso de transformación de los datos en dos pasos. Se proporcionan dos scripts para ayudarle a realizar esta operación, que se ejecuta una sola vez. Si la cadena de conexión en StoreFront y la instancia SQL están correctamente configuradas, todas las nuevas suscripciones se crean automáticamente en SQL en el formato correcto. Después de la migración, los datos históricos de suscripción de ESENT se transforman a un formato SQL y los usuarios también pueden ver sus recursos de suscripción previos.

Ejemplo: cuatro suscripciones SQL para el mismo usuario de dominio

Results | Messages

	id	subscription_ref	resource_id	user_id	status	metadata	secure_metadata
1	1	D002E864B9A8997D5B5DCD90F92A7005	XenDesktopSSL.Notepad++ TLS	1	1	<SubscriptionProperties xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"><property key="dazzle:position"><value>1</value></property></SubscriptionProperties>	NULL
2	2	2A3C21FE0F14ECF4D9CFB83CC8118CE7	XenDesktopSSL.Windows Media Player TLS	1	1	<SubscriptionProperties xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"><property key="dazzle:position"><value>2</value></property></SubscriptionProperties>	NULL
3	3	425BE4AF0810286A0C600059EED9DEA23	XenDesktopSSL.Calculator TLS	1	1	<SubscriptionProperties xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"><property key="dazzle:position"><value>3</value></property><property key="position"><value>3</value></property></SubscriptionProperties>	NULL
4	4	9632ACE31700118E1EF79C5A269299CA	XenDesktopSSL.IE11 TLS	1	1	<SubscriptionProperties xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"><property key="dazzle:position"><value>4</value></property><property key="position"><value>4</value></property></SubscriptionProperties>	NULL

	id	username	
1	1	S-1-5-21-	6059

Paso 1. Utilice el script Transform-SubscriptionDataForStore.ps1 para convertir los datos de ESENT a un formato de fácil lectura en SQL para la importación en bloque Inicie sesión en el servidor de StoreFront para el que quiere transformar los datos de ESENT.

Cualquier miembro de un grupo de servidores es adecuado, siempre que todos contengan el mismo número de registros de suscripción.

Abra PowerShell ISE y seleccione **Ejecutar como administrador**.

Ejecute el script Transform-SubscriptionDataForStore.ps1, que exporta un archivo `<StoreName>.txt` de la base de datos ESENT al escritorio del usuario actual.

El script de PowerShell proporciona comentarios detallados sobre cada fila de suscripción que se procesa, a fin de ayudar a la depuración y evaluar el éxito de la operación. Esta operación puede tardar mucho tiempo en procesarse.

Los datos transformados se registran en `<StoreName>SQL.txt`, en el escritorio del usuario actual, una vez finalizado el script. El script resume el número de registros de usuario únicos y el número total de suscripciones procesadas.

Repita este proceso para cada almacén que quiera migrar a SQL Server.

Paso 2. Utilice un procedimiento almacenado T-SQL para importar en bloque, en SQL, los datos transformados Los datos de cada almacén deben importarse por separado.

Copie el archivo `<StoreName>SQL.txt` creado en el paso 1 desde el escritorio del servidor de StoreFront en `C:\`, en el servidor Microsoft SQL, y cambie el nombre a SubscriptionsSQL.txt.

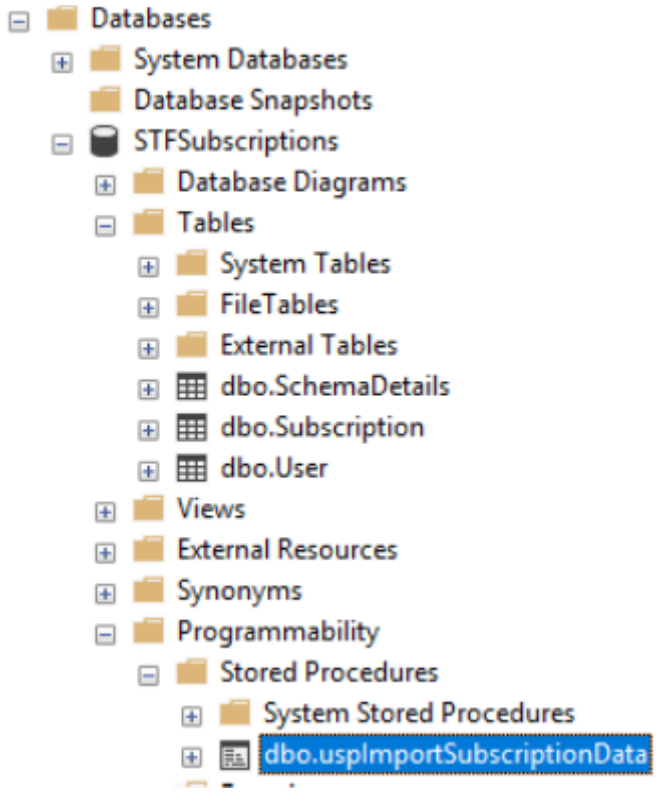
El script Create-ImportSubscriptionDataSP.sql crea un procedimiento almacenado T-SQL para importar los datos de suscripción en bloque. Además, elimina las entradas duplicadas para cada usuario único, de modo que los datos SQL resultantes se normalizan correctamente y se reparten en las tablas correctas.

Antes de ejecutar *Create-ImportSubscriptionDataSP.sql*, cambie `USE [STFSubscriptions]` para que coincida con la base de datos en la que quiere crear el procedimiento almacenado.

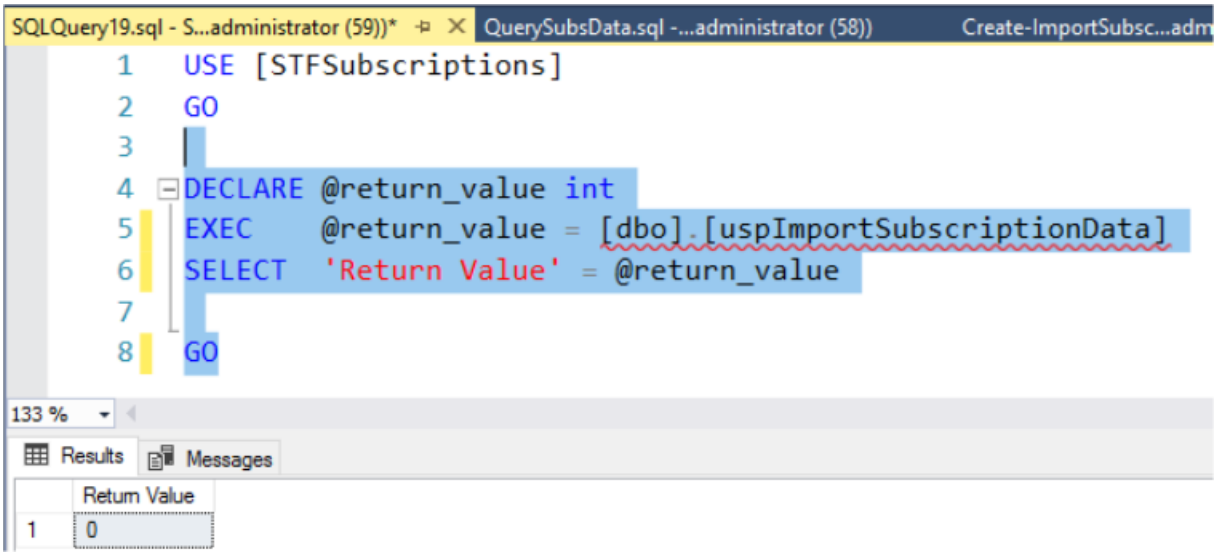
Abra el archivo *Create-ImportSubscriptionDataSP.sql* con SQL Server Management Studio y ejecute el código que contiene. Este script agrega el procedimiento almacenado *ImportSubscriptionDataSP* a la base de datos creada anteriormente.

Después de crearse el procedimiento almacenado, se muestra el siguiente mensaje en la consola de SQL y se agrega el procedimiento almacenado ImportSubscriptionDataSP a la base de datos:

```
Commands completed successfully.
```



Para ejecutar el procedimiento almacenado, haga clic con el botón derecho en él, seleccione **Ejecutar procedimiento almacenado** y haga clic en **Aceptar**.



El valor devuelto 0 indica que todos los datos se han importado correctamente. Cualquier problema al importar se registra en la consola de SQL. Una vez que el procedimiento almacenado se haya ejecutado correctamente, compare el número total de registros de suscripción y usuarios únicos que proporciona Transform-SubscriptionDataForStore.ps1 con el resultado de las dos consultas SQL siguientes. Los dos totales deben coincidir.

El número total de suscripciones del script de transformación debe coincidir con el número total notificado desde SQL por

```
SELECT COUNT(*) AS TotalSubscriptions
FROM [Subscription]
<!--NeedCopy-->
```

El número de usos únicos del script de transformación debe coincidir con el número de registros de la tabla de usuario notificados desde SQL por

```
SELECT COUNT(*) AS TotalUsers
FROM [User]
<!--NeedCopy-->
```

Si el script de transformación muestra 100 usuarios únicos y 1000 registros de suscripción totales, SQL debe mostrar los mismos dos números después de la migración.

Inicie sesión en StoreFront para comprobar si los usuarios existentes pueden ver sus datos de suscripción. Los registros de suscripción se actualizan en SQL cuando los usuarios suscriben o cancelan la suscripción de sus recursos. Los nuevos usuarios y los registros de suscripción también se crean en SQL.

Paso 3. Ejecute consultas T-SQL en los datos importados

> **Nota:**
>
> Todos los nombres de Delivery Controller distinguen entre mayúsculas y minúsculas, y deben coincidir exactamente con las mayúsculas y minúsculas utilizadas en StoreFront.

```
-- Get all SQL subscription records
Use [STFSubscriptions]
SELECT * FROM [Subscription]
SELECT * FROM [User]
<!--NeedCopy-->
```

```
-- Get all subscription records for a particular user SID
Use [STFSubscriptions]
SELECT * FROM [Subscription]
INNER JOIN [User]
ON [Subscription].[user_id] = [User].[id]
WHERE [User].[username] = 'S-1-5-21-xxxxxxxxxx-xxxxxxxxxx-xxxxxxxxxx-
    xxxx'

-- Get total number of Subscription records for a particular user SID
Use [STFSubscriptions]
SELECT COUNT(Subscription.id)
FROM [Subscription]
INNER JOIN [User]
ON [Subscription].[user_id] = [User].[id]
WHERE [User].[username] = 'S-1-5-21-xxxxxxxxxx-xxxxxxxxxx-xxxxxxxxxx-
    xxxx'
<!--NeedCopy-->
```

```
-- Get all subscription records for a particular delivery controller
Use [STFSubscriptions]
SELECT * FROM [Subscription]
WHERE [resource_id] LIKE 'DeliveryController.%'

-- OR for aggregated resources use the name of the aggregation group
Use [STFSubscriptions]
SELECT * FROM [Subscription]
WHERE [resource_id] LIKE 'DefaultAggregationGroup.%'

-- Get all subscription records for a particular application
Use [STFSubscriptions]
SELECT * FROM [Subscription]
WHERE [resource_id] = ' DeliveryController.Application'
<!--NeedCopy-->
```

Actualizar o eliminar registros de suscripción existentes mediante T-SQL

> **RENUNCIA DE RESPONSABILIDADES:**

> Todas las instrucciones SQL para actualización y eliminación de ejemplo las utiliza bajo su propio riesgo. Citrix no se hace responsable de ninguna pérdida o alteración accidental de sus datos de suscripción por el uso incorrecto de los ejemplos proporcionados. Las siguientes instrucciones T-SQL se proporcionan como guía para posibilitar una actualización sencilla. Haga una copia de seguridad de todos los datos de suscripción presentes en su base de datos SQL antes de intentar actualizar sus suscripciones o eliminar registros obsoletos. Si no se realizan las copias de seguridad necesarias, se pueden producir pérdidas o daños en los datos. Antes de ejecutar sus propias instrucciones UPDATE o DELETE de T-SQL en la base de datos de producción, pruebe con datos ficticios o con una copia redundante de los datos, fuera del entorno de la base de datos de producción real.
>
> **Nota:**
>
> Todos los nombres de Delivery Controller distinguen entre mayúsculas y minúsculas, y deben coincidir exactamente con las mayúsculas y minúsculas utilizadas en StoreFront.

```
-- Update the delivery controller used in all subscriptions.
Use [STFSubscriptions]
UPDATE [Subscription]
SET [resource_id] = REPLACE(resource_id,'OldDeliveryController.','
    NewDeliveryController.')
WHERE [resource_id] LIKE 'OldDeliveryController.%'
<!--NeedCopy-->
```

```
-- After enabling multi-site aggregation, update the resource_id
Use [STFSubscriptions]
UPDATE [Subscription]
SET [resource_id] = REPLACE(resource_id,'OldDeliveryController.','
    DefaultAggregationGroup.')
WHERE [resource_id] LIKE 'OldDeliveryController.%'
<!--NeedCopy-->
```

```
-- Delete all subscription records for a particular Delivery Controller
Use [STFSubscriptions]
DELETE FROM [Subscription]
WHERE [resource_id] LIKE 'DeliveryController.%'
<!--NeedCopy-->
```

```
-- OR for aggregated resources use the name of the aggregation group
Use [STFSubscriptions]
DELETE FROM [Subscription]
FROM [Subscription]
WHERE [resource_id] LIKE 'DefaultAggregationGroup.%'
<!--NeedCopy-->
```

```
-- Delete all subscription records for a particular application
Use [STFSubscriptions]
DELETE FROM [Subscription]
FROM [Subscription]
```



```
WHERE [resource_id] LIKE '%.Application'
<!--NeedCopy-->
```

```
-- Delete all subscription records for an application published via a specific delivery controller
Use [STFSubscriptions]
DELETE FROM [Subscription]
FROM [Subscription]
WHERE [resource_id] = 'DeliveryController.Application'
<!--NeedCopy-->
```

```
-- Delete all subscription records for a particular user SID
-- relies on cascade to delete records from [Subscription]
Use [STFSubscriptions]
DELETE FROM [User]
WHERE [User].[username] = 'S-1-5-21-xxxxxxxxxx-xxxxxxxxxx-xxxxxxxxxx-xxxx'
<!--NeedCopy-->
```

```
-- Delete ALL subscription data from a particular database and reset the primary key clustered index to start numbering from 0.
-- USE WITH EXTREME CARE AND NOT ON LIVE PRODUCTION DATABASES.
-- Can be useful whilst debugging data import issues to start with a clean database.

Use [STFSubscriptions]
DELETE FROM [Subscription]
DBCC CHECKIDENT ([Subscription], RESEED, 0)
DELETE FROM [User]
DBCC CHECKIDENT ([User], RESEED, 0)
<!--NeedCopy-->
```

Habilitar o inhabilitar favoritos

December 4, 2023

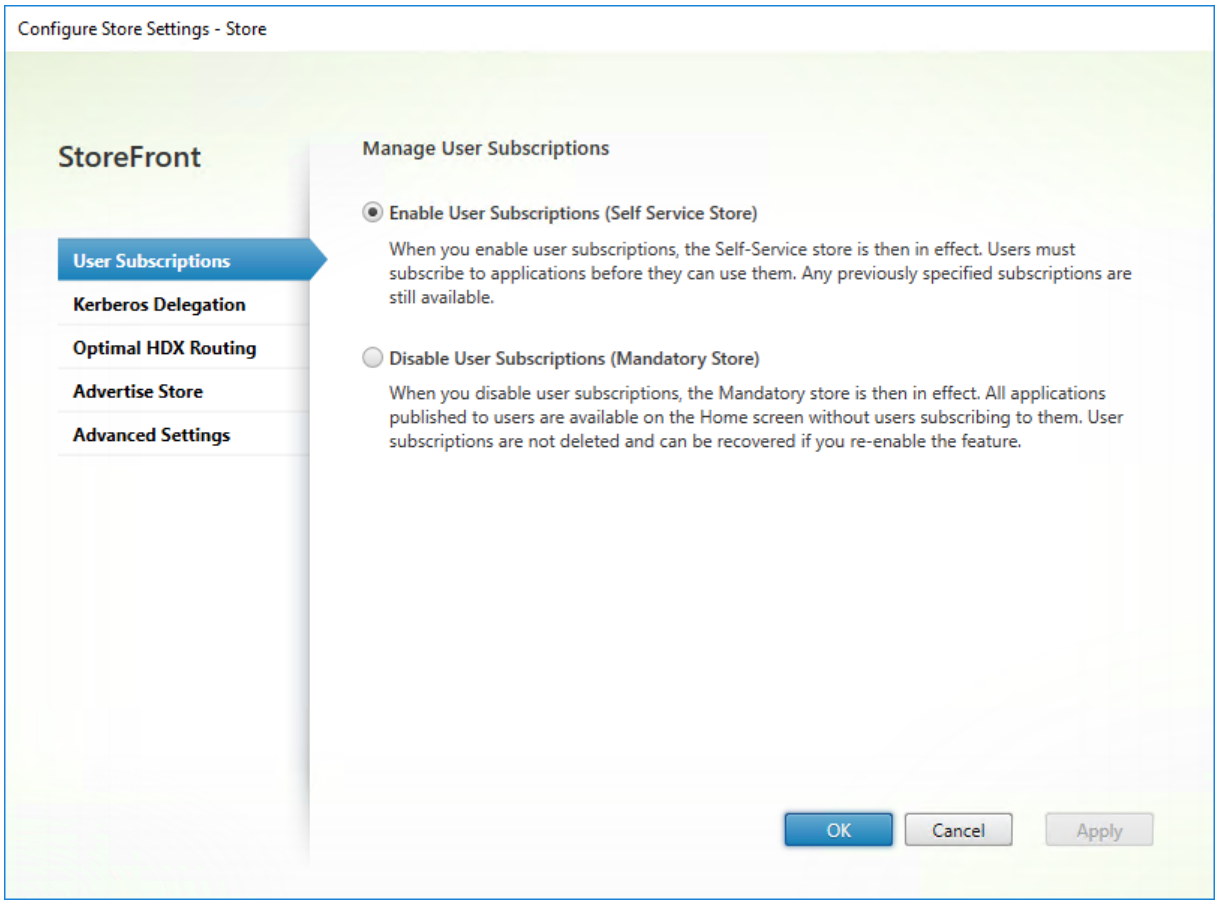
Utilice la pantalla “Suscripciones de usuarios”para seleccionar una de las siguientes opciones:

- Permitir a los usuarios crear y quitar favoritos (almacén de autoservicio). Los usuarios pueden marcar una aplicación como favorita al hacer clic en la estrella del icono de la aplicación. Los usuarios pueden hacer clic de nuevo en la estrella para quitar las aplicaciones de favoritos. Las aplicaciones favoritas se muestran en la ficha **Inicio**.
- Inhabilitar favoritos (almacén obligatorio). Los usuarios no pueden agregar ni quitar aplicaciones de los favoritos. No se muestra la ficha Inicio.

Inhabilitar las suscripciones no elimina los datos de suscripción a la tienda. Volver a habilitar las

suscripciones al almacén permitirá que un usuario vea sus elementos favoritos cada vez que inicie sesión.

1. Seleccione el nodo **Almacenes** en el panel izquierdo de la consola de administración de Citrix StoreFront y, en el panel de resultados, seleccione un almacén. En el panel **Acciones**, haga clic en **Configurar parámetros del almacén**.
2. Haga clic en la ficha **Suscripciones de usuarios** para activar o desactivar la función de favoritos de los usuarios.
3. Seleccione **Habilitar suscripciones de usuarios (almacén de autoservicio)** para habilitar los favoritos.
4. Seleccione **Inhabilitar suscripciones de usuarios (almacén obligatorio)** para inhabilitar los favoritos.



Como alternativa, puede usar el cmdlet Get-STFStoreService de PowerShell para configurar las suscripciones de los usuarios a un almacén. Por ejemplo:

```
$StoreObject = Get-STFStoreService -SiteID 1 -VirtualPath "/citrix/<yourstore>"
Set-STFStoreService -StoreService $StoreObject -LockedDown $True -Confirm:$False
<!--NeedCopy-->
```


Configuración de Citrix Virtual Apps and Desktops

April 17, 2024

Cuando entregue aplicaciones con Citrix Virtual Apps and Desktops o Citrix Desktops as a Service, tenga en cuenta las siguientes opciones para mejorar la experiencia de los usuarios que acceden a las aplicaciones a través de los almacenes: Para obtener más información acerca de la entrega de aplicaciones, consulte Aplicaciones.

- En el campo **Nombre de la aplicación (para el usuario)**, introduzca el nombre de la aplicación tal y como quiere que aparezca en el sitio web de su almacén.
- En el campo **Descripción y palabras clave**, introduzca la descripción que se muestra en el sitio web del almacén al ampliar los detalles de la aplicación, junto con las palabras clave.
- Elija el **icono de la aplicación** para ayudar a los usuarios a identificar visualmente una aplicación en el sitio web de StoreFront.
- En el campo **Categoría de la aplicación**, introduzca (optativamente) una categoría. Incluya \ en el nombre de la categoría para crear una jerarquía de carpetas. Podría, por ejemplo, agrupar aplicaciones según el tipo o, alternativamente, crear carpetas para diferentes roles de usuario en su organización. En la ficha **Aplicaciones** del sitio web del almacén, la vista **Categorías** muestra una lista de categorías y las aplicaciones incluidas en cada categoría.

Palabras clave

Para agregar palabras clave a una aplicación o a un escritorio, agregue la cadena `KEYWORDS:[keywordname]` a la descripción de la aplicación. Nota: Cuando se agregan varias palabras clave, hay que separarlas con espacios; por ejemplo, `KEYWORDS:Accounts Featured`. Las palabras clave se pueden utilizar de varias maneras:

- Filtrar aplicaciones: Consulte Parámetros avanzados de los almacenes).
- Crear grupos de aplicaciones destacadas.
- Algunas palabras clave tienen significados especiales.

Nombre de la palabra clave	Descripción
Obligatorio	Agrega una aplicación a la ficha Inicio. A diferencia de los favoritos, los usuarios no pueden quitar aplicaciones obligatorias de la ficha Inicio. No surte efecto si los favoritos están inhabilitados en el almacén.

Nombre de la palabra clave	Descripción
Auto (Automático)	Cuando los usuarios inician sesión en el almacén, la aplicación o el escritorio se marcan automáticamente como favoritos y se agregan a la ficha Inicio. Los usuarios pueden quitar estas aplicaciones de sus favoritos. No surte efecto si los favoritos están inhabilitados en el almacén.
TreatAsApp (Tratar como aplicación)	Aplíquelo a los escritorios para obligar a StoreFront a tratarlos como una aplicación. El escritorio se muestra en la ficha **Aplicaciones** en lugar de en la ficha **Escritorios**. Además, el escritorio no se iniciará automáticamente cuando el usuario inicie sesión en el sitio de web del almacén y no se accederá a él mediante Desktop Viewer, aunque el sitio se haya configurado para permitir esto con los demás escritorios.
prefer="*aplicación*"	Donde *aplicación* identifica una aplicación instalada localmente. Solo se aplica a la aplicación Citrix Workspace en Windows. Indica que debe utilizarse la versión instalada localmente de una aplicación, en vez de su instancia entregada equivalente, en caso de que ambas estén disponibles. Para obtener más información, consulte Configurar aplicaciones para el acceso a aplicaciones locales.
Principal y **Secundario**	Cuando se utiliza la Agrupación multisitio, siempre se preferirá el que tenga especificada la palabra clave **principal** sobre el que tenga la palabra clave **secundario**.

Parámetros avanzados de los almacenes

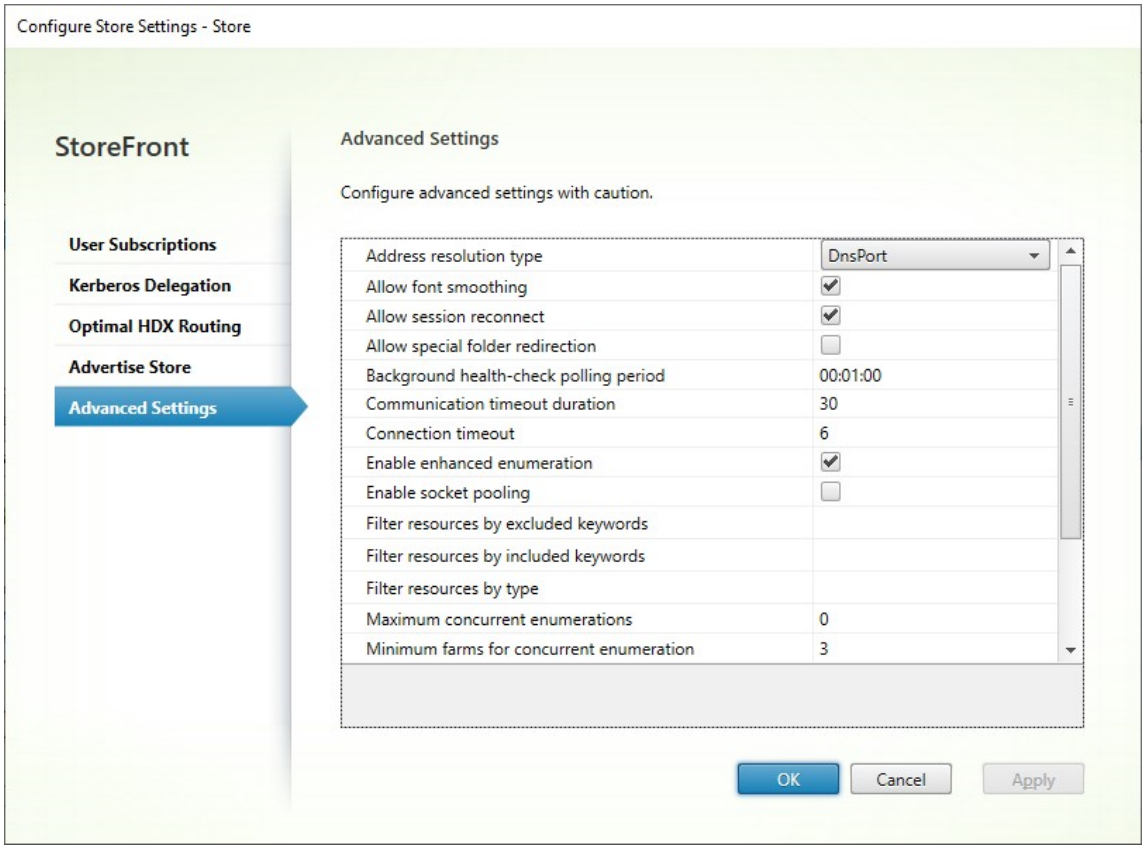
April 17, 2024

Puede configurar propiedades más avanzadas de los almacenes mediante la página Parámetros avan-

zados en Configurar parámetros del almacén. Algunos parámetros solo se pueden modificar con PowerShell.

> **Importante:**
>
> En implementaciones con varios servidores, use solo un servidor a la vez para hacer cambios en la configuración del grupo de servidores. Compruebe que la consola de administración de Citrix StoreFront no se está ejecutando en ninguno de los demás servidores de la implementación. Una vez completados, propague los cambios de configuración al grupo de servidores de modo que los demás servidores de la implementación se actualicen.

1. Seleccione el nodo Almacenes en el panel izquierdo de la consola de administración de Citrix StoreFront, seleccione un almacén en el panel central y, a continuación, seleccione **Configurar parámetros del almacén**.
2. En la página **Configurar parámetros de almacén**, seleccione **Parámetros avanzados** y haga los cambios necesarios.



3. Haga clic en **OK** para guardar los cambios.

Tipo de resolución de direcciones

Puede especificar el tipo de dirección que quiere solicitar del servidor. El valor predeterminado es DnsPort.

En la ventana **Parámetros avanzados**, elija un valor de la lista desplegable **Tipo de resolución de direcciones**.

- Dns
- DnsPort
- IPV4
- IPV4Port
- Dot
- DotPort
- Uri
- NoChange

Permitir suavizado de fuentes

Puede especificar si quiere usar suavizado de fuentes para las sesiones HDX. El valor predeterminado es Activado.

En la ventana **Parámetros avanzados**, seleccione la opción **Permitir suavizado de fuentes** y haga clic en **Aceptar**.

Permitir la reconexión de sesiones

Puede especificar si quiere que las sesiones HDX puedan reconectarse. El valor predeterminado es Activado.

En la ventana **Parámetros avanzados**, seleccione la opción **Permitir la reconexión de la sesión**.

Permitir la redirección de carpetas especiales

Si la redirección de carpetas especiales está configurada, los usuarios pueden asignar carpetas especiales de Windows del servidor a carpetas de sus equipos locales. El término "carpetas especiales" hace referencia a carpetas estándar de Windows, tales como las carpetas *\Documentos* y *\Escritorio*, que siempre se presentan del mismo modo, independientemente del sistema operativo.

En la ventana **Parámetros avanzados**, seleccione o desmarque la opción **Permitir la redirección de carpetas especiales**, según quiera habilitar o inhabilitar esta función, y haga clic en **Aceptar**.

Comprobación de estado avanzada

StoreFront realiza comprobaciones de estado periódicas en cada uno de los Delivery Controller de Citrix Virtual Apps and Desktops, en cada Cloud Connector y en cada servidor de Secure Private Access para reducir el impacto de disponibilidad intermitente de los servidores. Con la comprobación de estado avanzada, StoreFront realiza una comprobación más exhaustiva que tiene más probabilidades de detectar problemas.

Al conectarse a Citrix Desktops as a Service a través de un Cloud Connector, la comprobación de estado avanzada tiene la ventaja adicional de obtener información adicional sobre qué VDA están en la misma ubicación que el Cloud Connector. En caso de que los Cloud Connectors no puedan establecer contacto con Citrix Desktops as a Service, utilizan su memoria caché de host local para facilitar las conexiones a los VDA que están ubicados de forma conjunta. StoreFront usa la información adicional de los resultados de las comprobaciones de estado avanzadas para establecer contacto con el Connector en línea más adecuado para iniciar aplicaciones y escritorios.

Para garantizar la disponibilidad de recursos durante una interrupción del servicio sin tener que publicar recursos en cada zona (ubicación de recursos), asegúrese de configurar el feed de recursos en todos los servidores de StoreFront para incluir todos los Cloud Connectors en todas las ubicaciones de recursos y habilitar la función de comprobación de estado avanzada.

A partir de StoreFront 2308, la comprobación de estado avanzada está habilitada de forma predeterminada para nuevos almacenes. Citrix recomienda dejarlo habilitado para todas las implementaciones de StoreFront. Para habilitar o inhabilitar la comprobación de estado avanzada, use el cmdlet de PowerShell Set-STFStoreFarmConfiguration con el parámetro `AdvancedHealthCheck`.

Periodo de sondeo de comprobación de estado en segundo plano

StoreFront realiza comprobaciones de estado periódicas en cada uno de los Delivery Controller de Citrix Virtual Apps and Desktops, en cada Cloud Connector y en cada servidor de Secure Private Access para reducir el impacto de disponibilidad intermitente de los servidores. El valor predeterminado es realizar una comprobación cada minuto (00:01:00). En la ventana **Parámetros avanzados**, especifique el **Período de sondeo de comprobación de estado** en segundo plano y haga clic en **Aceptar** para controlar la frecuencia de las comprobaciones de estado. No se recomienda establecer el período de sondeo en un valor bajo cuando la comprobación de estado avanzada está habilitada, ya que eso puede afectar al rendimiento.

Duración del tiempo de espera de las comunicaciones

De forma predeterminada, las solicitudes de StoreFront para un servidor que proporciona los recursos para un almacén tienen un tiempo de espera máximo de 30 segundos. El servidor se considera no

disponible después de 1 intento de comunicación sin éxito. En la ventana **Parámetros avanzados**, haga los cambios que quiera en los valores de tiempo predeterminados y haga clic en **Aceptar** para cambiar estos parámetros.

Tiempo de espera de la conexión

Puede especificar cuántos segundos se debe esperar al establecer una conexión inicial con un Delivery Controller. El valor predeterminado es 6.

En la ventana **Parámetros avanzados** y especifique los segundos de espera que han de transcurrir al establecer la conexión inicial, y luego haga clic en **Aceptar**.

Habilitar enumeración mejorada

Esta opción controla si StoreFront consulta los Delivery Controllers de forma simultánea o secuencial al enumerar aplicaciones y escritorios en varios sitios de Citrix Virtual Apps and Desktops. La enumeración simultánea proporciona respuestas más rápidas a las consultas de los usuarios cuando se agregan recursos en varios sitios. Cuando se selecciona esta opción (predeterminada), StoreFront envía solicitudes de enumeración a todos los Delivery Controllers al mismo tiempo y agrupa las respuestas cuando todos han respondido. Puede utilizar las opciones **Máximo de enumeraciones simultáneas** y **Mínimo de comunidades para la enumeración simultánea** para ajustar el funcionamiento.

En la ventana **Parámetros avanzados**, seleccione (o desmarque) la opción **Habilitar enumeración mejorada** y haga clic en **Aceptar.**

Habilitar la agrupación de sockets

De forma predeterminada, la agrupación de sockets está inhabilitada en los almacenes. Cuando la agrupación de sockets está habilitada, StoreFront mantiene una agrupación de sockets en lugar de crear un socket cada vez que se necesita uno y devolverlo al sistema operativo cuando se cierra la conexión. La habilitación de la agrupación de sockets mejora el rendimiento, especialmente para conexiones SSL. Para habilitar la agrupación de sockets, modifique el archivo de configuración del almacén. En la ventana **Parámetros avanzados**, seleccione la opción **Habilitar la agrupación de sockets** y haga clic en **Aceptar**.

Asociación de tipos de archivos

De forma predeterminada, la asociación de tipos de archivo está habilitada en los almacenes para que el contenido se redirija directamente a las aplicaciones suscritas de los usuarios cuando estos abran

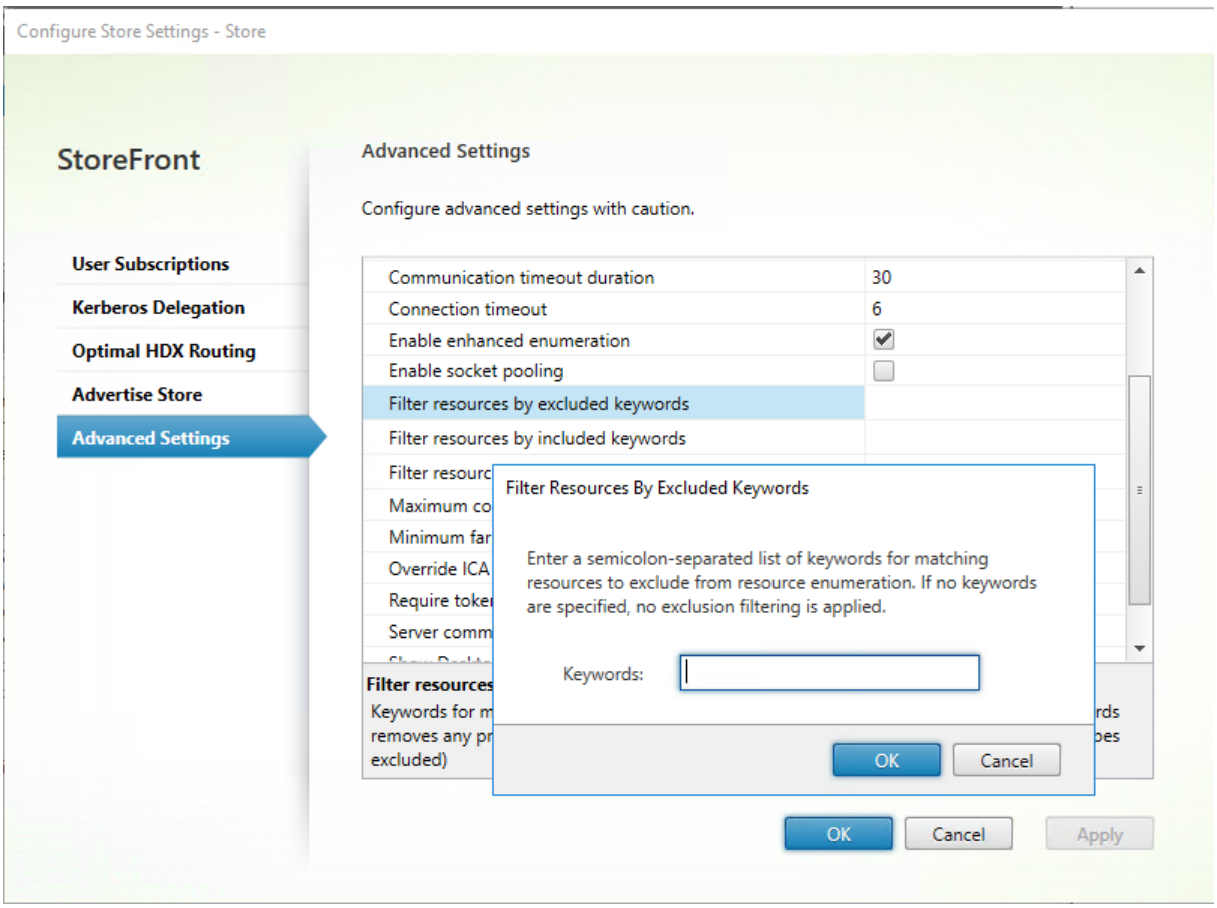
archivos locales de los correspondientes tipos. Para habilitar la inhabilitación de la asociación de tipos de archivos, utilice el comando Set-STFStoreFarmConfiguration de PowerShell. Por ejemplo:

```
$storeService = Get-STFStoreService – VirtualPath '/Citrix/Store'
Set-STFStoreFarmConfiguration $storeService -EnableFileTypeAssociation
    $false
<!--NeedCopy-->
```

Filtrar recursos por palabras clave excluidas

Puede filtrar los recursos utilizando palabras clave de exclusión. Cuando se especifican palabras clave de exclusión se quitan las palabras clave de inclusión previamente especificadas. El valor predeterminado es No filtrar (no se excluye ningún tipo de recurso).

1. En la ventana **Parámetros avanzados**, busque la fila **Filtrar recursos por palabras clave excluidas**.
2. Haga clic en la columna de la derecha para mostrar la ventana **Filtrar recursos por palabras clave excluidas**.
3. Introduzca una lista de palabras clave separadas por puntos y comas en el cuadro Introduzca palabras clave.
4. Haga clic en **Aceptar**.



Para cambiar el parámetro mediante PowerShell, utilice el cmdlet Set-STFStoreEnumerationOptions con el parámetro `-FilterByKeywordsExclude`.

Las siguientes palabras clave están reservadas y no se deben usar para el filtrado:

- Auto (Automático)
- Obligatorio

Filtrar recursos por palabras clave incluidas

Puede filtrar los recursos utilizando palabras clave incluidas. Cuando se especifican palabras clave de inclusión se quitan las palabras clave de exclusión previamente especificadas. El valor predeterminado es No filtrar (no se excluye ningún tipo de recurso).

1. En la ventana **Parámetros avanzados**, busque la fila **Filtrar recursos por palabras clave incluidas**.
2. Haga clic en la columna de la derecha para mostrar la ventana **Filtrar recursos por palabras clave incluidas**.
3. Introduzca una lista de palabras clave separadas por puntos y comas en el cuadro Introduzca palabras clave.

4. Haga clic en **Aceptar**.

Para cambiar el parámetro mediante PowerShell, utilice el cmdlet Set-STFStoreEnumerationOptions con el parámetro `-FilterByKeywordsInclude`.

Las siguientes palabras clave están reservadas y no se deben usar para el filtrado:

- Auto (Automático)
- Obligatorio

Filtrar recursos por tipo

Elija los tipos de recursos que se van a incluir en la enumeración de recursos. El valor predeterminado es No filtrar (se incluyen todos los tipos de recurso).

En la ventana **Parámetros avanzados**, seleccione **Filtrar recursos por tipo**, haga clic a su derecha, elija los tipos de recursos para incluir en la enumeración y haga clic en **Aceptar**.

Para cambiar el parámetro mediante PowerShell, utilice el cmdlet Set-STFStoreEnumerationOptions con el parámetro `-FilterByTypesInclude` y especifique una serie de tipos de recursos (aplicaciones, escritorios o documentos).

Máximo de enumeraciones simultáneas

Especifique la cantidad máxima de solicitudes simultáneas para enviar a todos los Delivery Controllers. Esta opción surte efecto cuando está habilitada la opción **Habilitar enumeración mejorada**. El valor predeterminado es 0 (no hay límite).

En la ventana **Parámetros avanzados**, seleccione **Máximo de enumeraciones simultáneas**, introduzca el número y haga clic en **Aceptar**.

Mínimo de comunidades para la enumeración simultánea

Especifique la cantidad mínima de Delivery Controllers necesarios para desencadenar la enumeración simultánea. Esta opción surte efecto cuando está habilitada la opción **Habilitar enumeración mejorada**. El valor predeterminado es 3.

En la ventana **Parámetros avanzados**, seleccione **Mínimo de comunidades para la enumeración simultánea**, introduzca el número y haga clic en **Aceptar**.

Sobrescribir nombre de cliente ICA

Supedita el parámetro del nombre de cliente en el archivo de inicio ICA con un ID único generado por el explorador web. Cuando está inhabilitado, la aplicación Citrix Workspace especifica el nombre del cliente. El valor predeterminado es Desactivado.

En la ventana **Parámetros avanzados**, seleccione la opción **Sobrescribir nombre de cliente ICA** y haga clic en **Aceptar**.

Requerir coherencia de token

Cuando está habilitado, StoreFront aplica uniformidad entre la puerta de enlace que se usa para autenticar y la puerta de enlace que se usa para acceder al almacén. Si los valores no son coherentes, los usuarios deben volver a autenticarse. Es necesario habilitar esta opción para aplicar SmartAccess. Debe inhabilitar esta opción si los usuarios acceden al almacén a través de un dispositivo Gateway con la autenticación inhabilitada. El valor predeterminado es Activado.

En la ventana **Parámetros avanzados**, seleccione la opción **Requerir coherencia de token** y haga clic en **Aceptar**.

Intentos de comunicación con los servidores

Especifique cuántos intentos fallidos de comunicación con un Delivery Controller pueden tener lugar antes de marcarlo como no disponible. El valor predeterminado es 1.

En la ventana **Parámetros avanzados**, seleccione **Intentos de comunicación con los servidores**, introduzca el número y haga clic en **Aceptar**.

Mostrar Desktop Viewer para clientes antiguos

Especifique si quiere mostrar la ventana y la barra de herramientas de Citrix Desktop Viewer cuando los usuarios acceden a sus escritorios desde clientes antiguos. El valor predeterminado es Desactivado.

En la ventana **Parámetros avanzados**, seleccione la opción **Mostrar Desktop Viewer para clientes antiguos** y haga clic en **Aceptar**.

Tratar los escritorios como si fueran aplicaciones

Especifique si, al acceder al almacén, los escritorios se muestran en la vista Aplicaciones en lugar de mostrarse en la vista Escritorios. El valor predeterminado es Desactivado.

En la ventana **Parámetros avanzados**, seleccione la opción **Tratar los escritorios como si fueran aplicaciones** y haga clic en **Aceptar**.

Configurar la redirección óptima de HDX Gateway para un almacén

January 26, 2024

Configure la redirección óptima de Citrix Gateway para mejorar el control de la redirección de la conexión ICA desde el motor HDX a aplicaciones publicadas de Citrix Virtual Apps and Desktops mediante StoreFront. Por regla general, la puerta de enlace óptima para un sitio se coloca en la misma ubicación geográfica.

Solo necesita definir los dispositivos Citrix Gateway óptimos para aquellas implementaciones donde el dispositivo a través del cual los usuarios acceden a StoreFront no es la mejor puerta de enlace. Si los inicios de recursos deben redirigirse a través de la puerta de enlace que los solicita, StoreFront hace esto automáticamente.

Puede asignar puertas de enlace a Delivery Controllers o a zonas específicos. Una zona es una agrupación de Delivery Controllers y, por lo general, representa un centro de datos en una ubicación geográfica. Las zonas se definen en Citrix Virtual Apps and Desktops y cualquier zona definida en StoreFront debe coincidir exactamente con los nombres de zona definidos en Citrix Virtual Apps and Desktops. Se puede asignar una puerta de enlace óptima a más de una zona, pero normalmente se usa una sola zona. Una zona representa normalmente un centro de datos en una ubicación geográfica. Es de esperar que cada zona tenga como mínimo un dispositivo Citrix Gateway óptimo que se utiliza para conexiones HDX con los recursos de esa zona.

Para obtener más información acerca de este tema, consulte Zonas.

Ejemplo de uso con comunidades de servidores

1 x Puerta de enlace en Reino Unido –> 1 x StoreFront en Reino Unido

- Aplicaciones y escritorios locales en Reino Unido
- Aplicaciones y escritorios en EE. UU., solo en caso de que fallen los del Reino Unido

1 x Puerta de enlace en EE. UU. –> 1 x StoreFront en EE. UU.

- Aplicaciones y escritorios locales en EE. UU.
- Aplicaciones y escritorios locales en Reino Unido, solo en caso de fallo de los de EE. UU.

Una puerta de enlace del Reino Unido proporciona acceso remoto a recursos alojados en el Reino Unido, como aplicaciones y escritorios que utilicen un StoreFront del Reino Unido.

El almacén de StoreFront del Reino Unido tiene definidas, en su lista de Delivery Controllers, puertas de enlace Citrix Gateway basadas tanto en Reino Unido como en Estados Unidos y Controllers también en ambos países. Los usuarios del Reino Unido acceden a los recursos remotos a través de la puerta de enlace, StoreFront y comunidades de servidores colocados en la misma ubicación. Si los recursos del Reino Unido dejan de estar disponibles, pueden conectarse a recursos de EE. UU. como solución temporal.

Sin una redirección de puerta de enlace óptima, todos los inicios ICA pasarían a través de la puerta de enlace del Reino Unido que realizó la solicitud de inicio, independientemente de la ubicación geográfica de los recursos. De manera predeterminada, las puertas de enlace utilizadas para realizar la solicitud de inicios de recursos son identificadas de manera dinámica por StoreFront cuando se hace una solicitud. La redirección óptima de puertas de enlace anula este comportamiento y obliga a hacer las conexiones de EE. UU. a través de la puerta de enlace más próxima a las comunidades de EE. UU. que ofrecen los escritorios y aplicaciones.

> **Nota:**
>
> Solo se puede asignar una puerta de enlace óptima por sitio, para cada almacén de StoreFront.

Ejemplo de uso con zonas

1 x ZonaCAM -> 2 x StoreFronts en Reino Unido

- Cambridge, Reino Unido: Aplicaciones y escritorios
- Fort Lauderdale, Costa Este de EE. UU.: Aplicaciones y escritorios
- Bangalore, India: Aplicaciones y escritorios

1 x ZonaFTL -> 2 x StoreFronts en EE. UU.

- Fort Lauderdale, Costa Este de EE. UU.: Aplicaciones y escritorios
- Cambridge, Reino Unido: Aplicaciones y escritorios
- Bangalore, India: Aplicaciones y escritorios

1 x ZonaBGL -> 2 x StoreFronts en India

- Bangalore, India: Aplicaciones y escritorios
- Cambridge, Reino Unido: Aplicaciones y escritorios
- Fort Lauderdale, Costa Este de EE. UU.: Aplicaciones y escritorios

Figura 1. Problemas de redirección de puertas de enlace

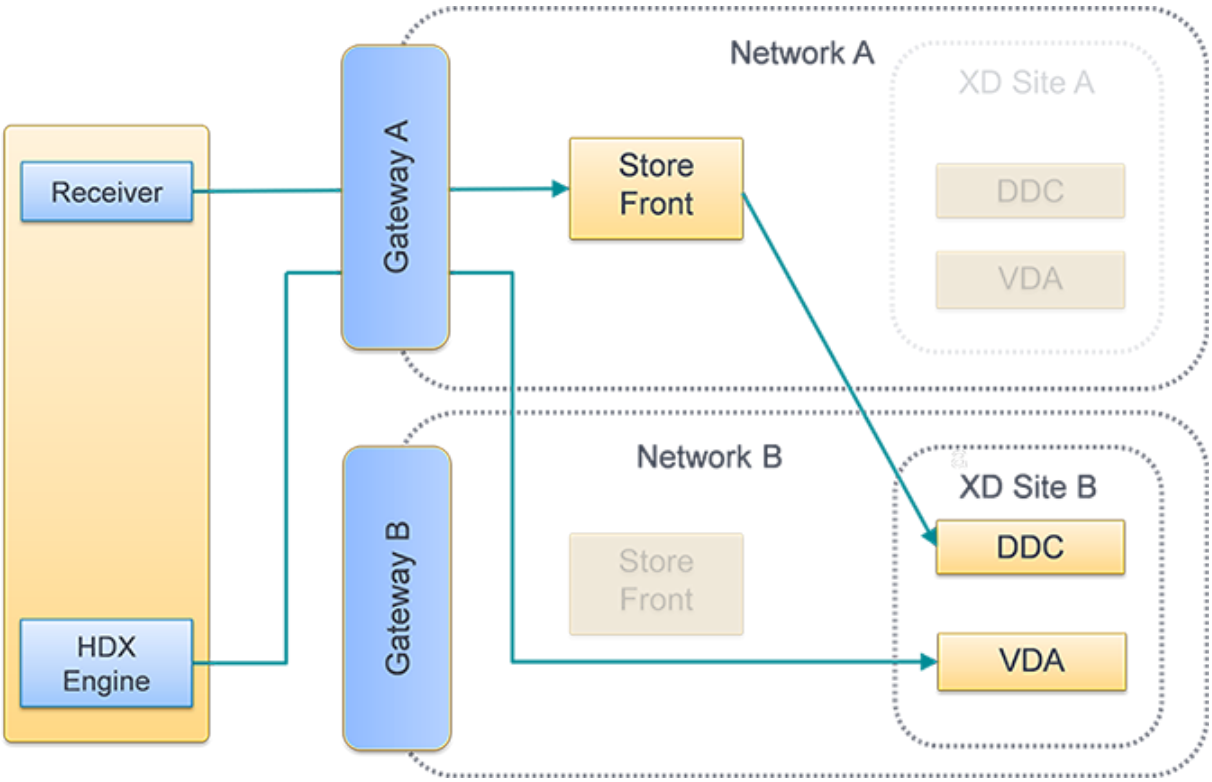
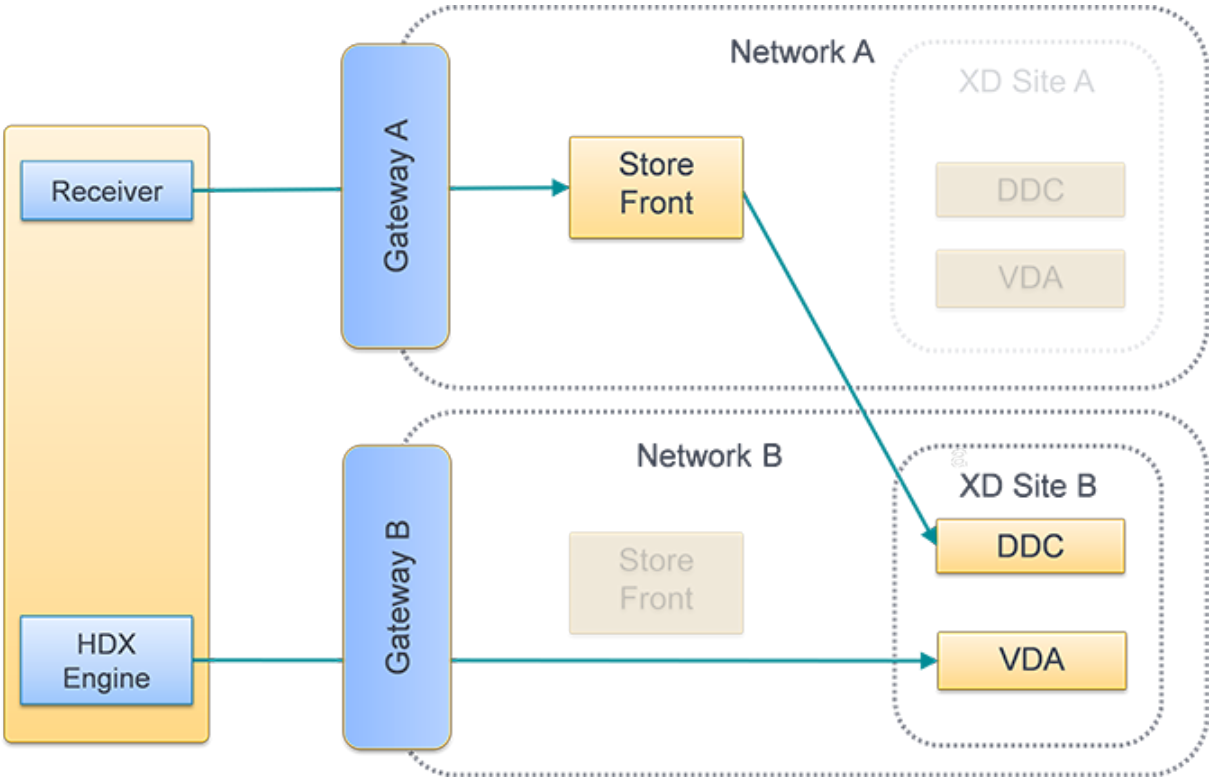


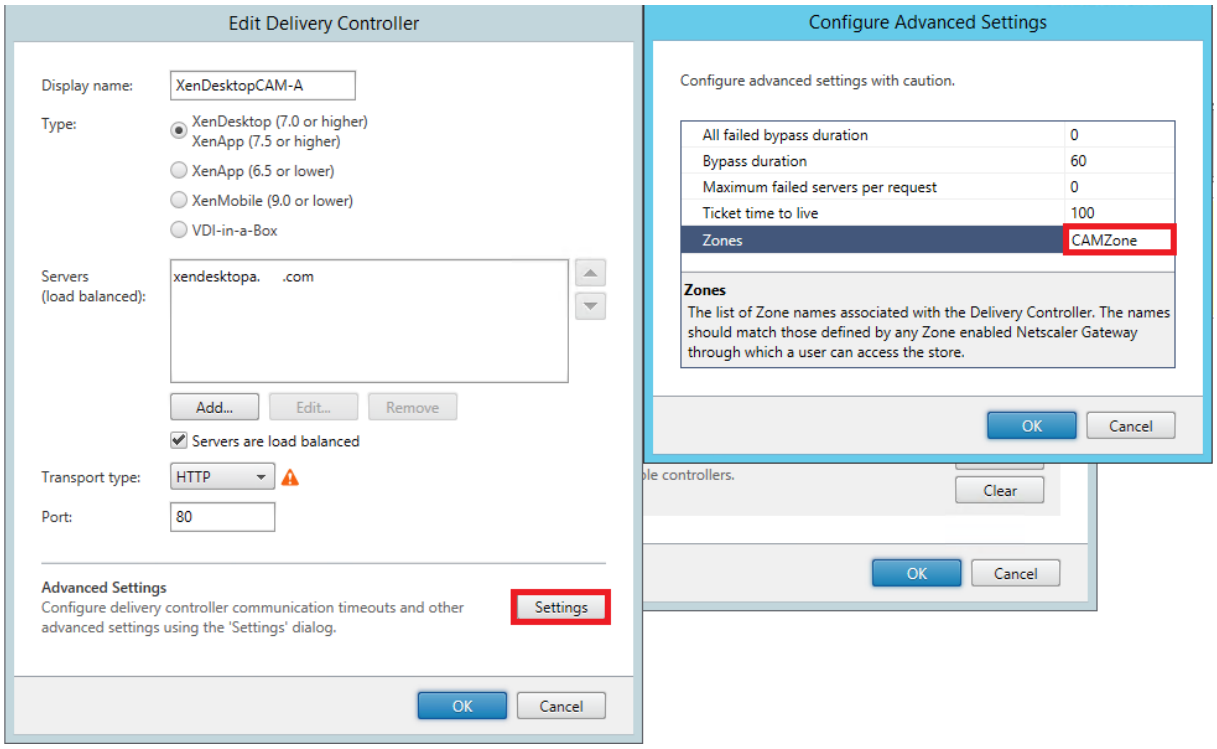
Figura 2. Redirección óptima de puertas de enlace



Colocar un Delivery Controller en una zona

Defina el atributo de zona en cada Delivery Controller que quiere colocar dentro de una zona.

1. Seleccione el nodo **Almacenes** en el panel izquierdo de la consola de administración de Citrix StoreFront y haga clic en **Administrar Delivery Controllers** en el panel **Acciones**.
2. Seleccione un Controller, haga clic en **Modificar** y luego en **Parámetros** en la pantalla **Modificar Delivery Controller**.
3. En la fila de **Zonas**, haga clic en la segunda columna.
4. Haga clic en **Agregar** en la pantalla **Nombres de zona de Delivery Controller** y agregue un nombre de zona.



Configuración de la redirección óptima de HDX

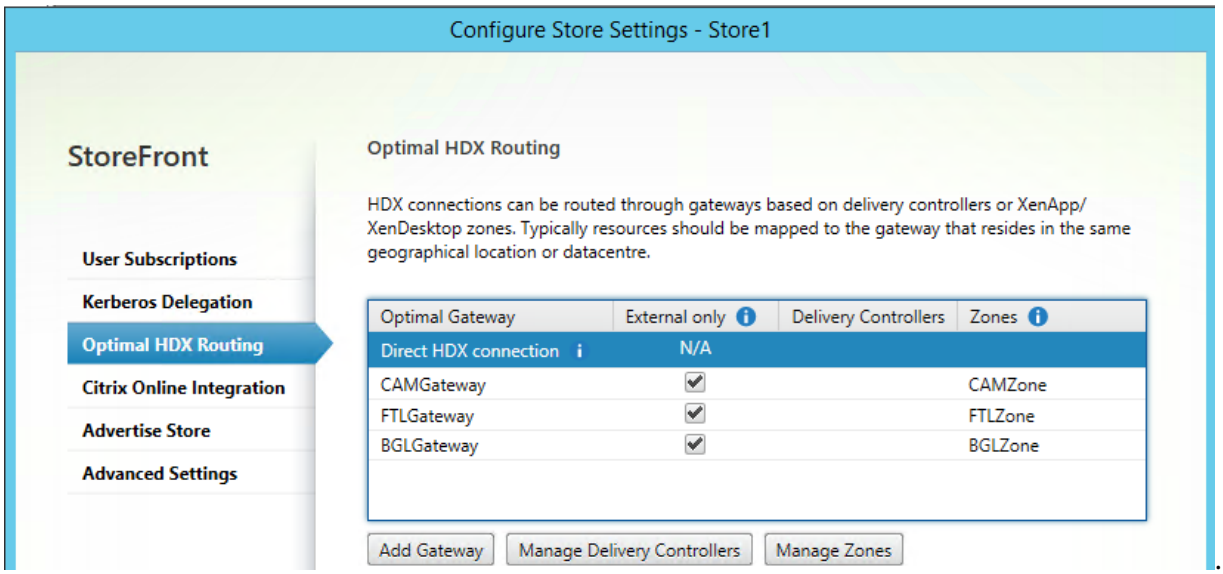
1. Seleccione el nodo **Almacenes** en el panel izquierdo de la consola de administración de Citrix StoreFront y, en el panel de resultados, seleccione un almacén. En el panel **Acciones**, haga clic en **Configurar parámetros del almacén**.
2. Seleccione la ficha **Redirección óptima de HDX**.
3. Seleccione un dispositivo Gateway.

   a) Para usar la puerta de enlace al acceder a recursos de Delivery Controllers específicos, haga clic en **Administrar Delivery Controllers** y marque uno o más Delivery Controllers.

b) Para usar la puerta de enlace al acceder a recursos de un grupo de Delivery Controllers de una zona, haga clic en **Administrar zonas** e introduzca una o más zonas.

c) De forma predeterminada, una vez que se haya agregado un Delivery Controller o una zona, la opción **Solo externo** se marca, lo que significa que StoreFront solo usa la puerta de enlace para iniciar StoreFront para los usuarios conectados a StoreFront a través de una puerta de enlace. Si también quiere usar la puerta de enlace para iniciar recursos para los usuarios que se han conectado directamente a StoreFront sin pasar por una puerta de enlace, desmarque **Solo externo**.

4. Si quiere conectarse siempre directamente a determinados recursos sin utilizar una puerta de enlace, incluso para usuarios que accedan a StoreFront de forma remota a través de una puerta de enlace, seleccione **Conexión HDX directa** y elija algunos Delivery Controllers o zonas.



Usar PowerShell para configurar la redirección óptima de Citrix Gateway para un almacén

- Para configurar la redirección óptima de la puerta de enlace de un almacén, use Register-STFStoreOptimalLaunchGateway.
- Para quitar la redirección óptima de la puerta de enlace de un almacén, use Unregister-STFStoreOptimalLaunchGateway.
- Para ver la redirección óptima de un almacén, utilice Get-STFStoreRegisteredOptimalLaunchGateway.

Sincronización de las suscripciones

November 10, 2023

StoreFront sincroniza automáticamente las suscripciones entre los servidores de un grupo de servidores de StoreFront. Si tiene varios grupos de servidores (normalmente, en ubicaciones geográficas diferentes), puede configurar la sincronización periódica de las suscripciones de los usuarios desde almacenes en diferentes implementaciones de StoreFront. Esto debe hacerse con PowerShell.

> **Nota:**
>
> Las consolas de StoreFront y PowerShell no pueden estar abiertas a la vez. Cierre siempre la consola de administración de StoreFront antes de usar la consola de PowerShell para administrar la configuración de StoreFront. Asimismo, cierre todas las instancias de PowerShell antes de abrir la consola de StoreFront.

Al establecer la sincronización de las suscripciones, tenga en cuenta que los Delivery Controllers configurados deben tener el mismo nombre en todos los almacenes sincronizados, incluidas las mayúsculas y las minúsculas. Si no duplica el nombre exacto de los Delivery Controllers se pueden crear suscripciones diferentes para los usuarios en los almacenes sincronizados. Si sincroniza suscripciones a partir de recursos agregados, el nombre de los grupos de agregación utilizados por ambos almacenes también debe coincidir. Los nombres de Delivery Controller y de grupos de agregación distinguen entre mayúsculas y minúsculas; por ejemplo, *CVAD_US* es distinto de *Cvad_Us*.

1. Utilice una cuenta con permisos de administrador local para iniciar Windows PowerShell ISE.
2. Para configurar la sincronización, utilice el comando Publish-STFServerGroupConfiguration. Puede especificar una hora de inicio y un intervalo recurrente o una lista de tiempos. Por ejemplo, empezar la sincronización a las 08:00 y luego cada 30 minutos:

   ```
   Add-STFSubscriptionSynchronizationSchedule -RecurringStartTime
       08:00:00 -RecurringInterval 30
   <!--NeedCopy-->
   ```

   Se recomienda escalonar las programaciones de extracción para evitar que dos grupos de servidores intenten extraer datos de suscripción entre sí al mismo tiempo. Por ejemplo, una programación para extraer datos de cada grupo de servidores cada 60 minutos se configuraría de la siguiente manera. El grupo de servidores 1 extrae datos del grupo de servidores 2 a las horas 01:00, 02:00, 03:00, etc. El grupo de servidores 2 extrae datos del grupo de servidores 1 a las horas 01:30, 02:30, 03:30, etc.
3. Para especificar la implementación remota de StoreFront que contiene el almacén que se sincronizará, escriba el siguiente comando Debe configurar esto para cada centro de datos en el

que reside un grupo de servidores de StoreFront, de manera que pueda extraer datos de suscripción de otros centros de datos remotos. Consulte los siguientes ejemplos de centros de datos de EE. UU. y Reino Unido:

- Proceso en servidores de StoreFront del centro de datos de Estados Unidos para extraer datos de los servidores del centro de datos del Reino Unido:

```
$StoreObject = Get-STFStoreService -SiteID 1 -VirtualPath "/
    Citrix/Store"
Add-STFSubscriptionSynchronizationSource -FriendlyName "
    SyncFromUKStore" -StoreService $StoreObject -
    RemoteStoreFrontAddress "UKloadbalancedStoreFront.example.
    com"
<!--NeedCopy-->
```

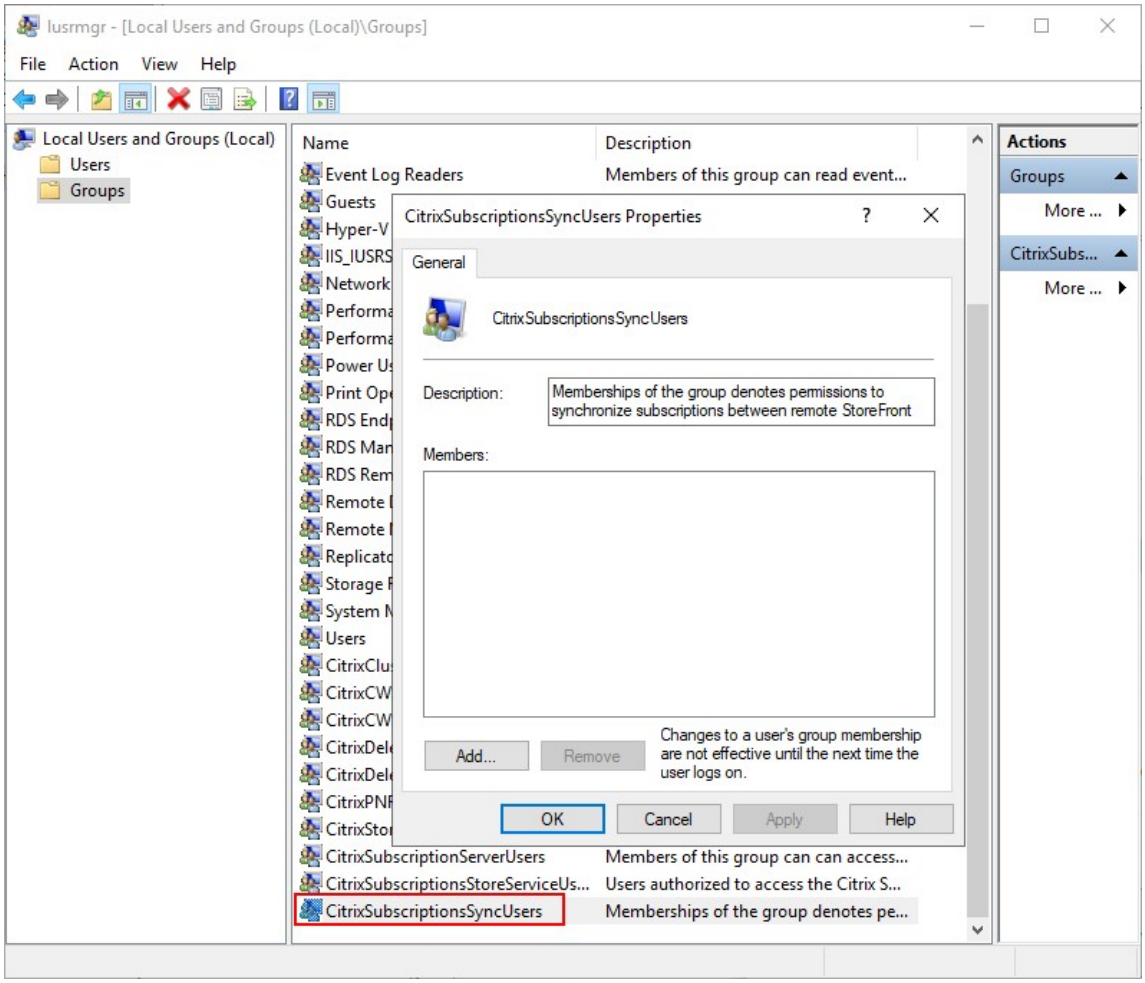
- Proceso en servidores de StoreFront del centro de datos del Reino Unido para extraer datos de los servidores del centro de datos de Estados Unidos:

```
$StoreObject = Get-STFStoreService -SiteID 1 -VirtualPath "/
    Citrix/Store"
Add-STFSubscriptionSynchronizationSource -FriendlyName "
    SyncFromUSStore" -StoreService $StoreObject -
    RemoteStoreFrontAddress "USloadbalancedStoreFront.example.
    com"
<!--NeedCopy-->
```

donde *FriendlyName* es un nombre que le ayuda a identificar la implementación remota y *RemoteStoreFrontAddress* es el nombre de dominio completo (FQDN) del servidor de StoreFront o grupo de servidores con equilibrio de carga para la implementación remota. Para sincronizar suscripciones a aplicaciones entre dos o más almacenes, todos los almacenes que se van a sincronizar deben tener el mismo nombre en sus respectivas implementaciones de StoreFront.

4. Agregue las cuentas de máquina del dominio de Microsoft Active Directory para cada servidor de StoreFront en la implementación remota al grupo de usuarios local de Windows CitrixSubscriptionSyncUsers en el servidor actual.

   Esto permite a los servidores actuales extraer datos de suscripción nuevos o actualizados de los servidores remotos enumerados en CitrixSubscriptionSyncUsers una vez que se haya configurado una programación de sincronización. Para obtener más información sobre la modificación de grupos de usuarios locales, consulte https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc772524(v=ws.11).



5. Cuando haya configurado la programación como quiera, utilice la consola de administración de Citrix StoreFront, o PowerShell más adelante, para propagar las programaciones y orígenes de sincronización de suscripciones a todos los demás servidores del grupo.

```
Publish-STFServerGroupConfiguration
<!--NeedCopy-->
```

Para obtener más información acerca de la propagación de cambios en una implementación con varios servidores StoreFront, consulte Configurar grupos de servidores.

6. Para quitar una programación de sincronización de suscripciones, ejecute el siguiente comando y, a continuación, propague el cambio de configuración por el resto de los servidores de StoreFront de la implementación.

```
Clear-STFSubscriptionSynchronizationSchedule
Publish-STFServerGroupConfiguration
<!--NeedCopy-->
```

7. Para quitar un origen de sincronización de suscripciones específico, ejecute el siguiente comando y, a continuación, propague el cambio de configuración a los demás servidores de Store-

Front de la implementación.

```
Remove-STFSubscriptionSynchronizationSource -FriendlyName "
    SyncFromUKStore"
Publish-STFServerGroupConfiguration
<!--NeedCopy-->
```

8. Para quitar todos los orígenes de sincronización de suscripciones existentes, ejecute el siguiente comando y, a continuación, propague el cambio de configuración a los demás servidores de StoreFront de la implementación.

```
Clear-STFSubscriptionSynchronizationSource
Publish-STFServerGroupConfiguration
<!--NeedCopy-->
```

9. Para enumerar las programaciones de sincronización de suscripciones configuradas actualmente para su implementación de StoreFront, ejecute el siguiente comando.

```
Get-STFSubscriptionSynchronizationSchedule
<!--NeedCopy-->
```

10. Para enumerar los orígenes de sincronización de suscripciones configuradas actualmente para su implementación de StoreFront, ejecute el siguiente comando.

```
Get-STFSubscriptionSynchronizationSource
<!--NeedCopy-->
```

Configurar los parámetros de sesión

February 26, 2024

Cuando un usuario inicia una aplicación, StoreFront genera un documento (conocido como archivo ICA) que contiene todos los parámetros que la aplicación Citrix Workspace necesita para iniciar y configurar esa sesión.

En la mayoría de los casos, se recomienda modificar los parámetros de las sesiones mediante las directivas de Citrix Virtual Apps and Desktops o las directivas de Citrix DaaS. Sin embargo, en algunos casos es útil anular estos parámetros para un almacén en particular. Esto puede resultar útil si un almacén agrega recursos de varios sitios y se quieren aplicar los mismos parámetros a todos los recursos de ese almacén.

Para definir los parámetros de sesión para un almacén, haga lo siguiente:

- Use el Global App Config Service. Es un servicio de Citrix Cloud. Para obtener más información, consulte Configurar la aplicación Citrix Workspace mediante Global App Configuration Service.

- En el servidor de StoreFront, agregue los parámetros al archivo default.ica del almacén.

Puede encontrar default.ica en el servidor de StoreFront, en el directorio `\inetpub\wwwroot\Citrix\[StoreName]\App_Data`.

Para obtener una lista de los parámetros disponibles, consulte Referencia para parámetros ICA. Algunos parámetros se aplican de forma global. Igualmente, para agregar secciones que se apliquen a aplicaciones específicas, puede agregar una sección cuyo nombre coincida exactamente con el nombre de la aplicación tal y como está configurado en Studio.

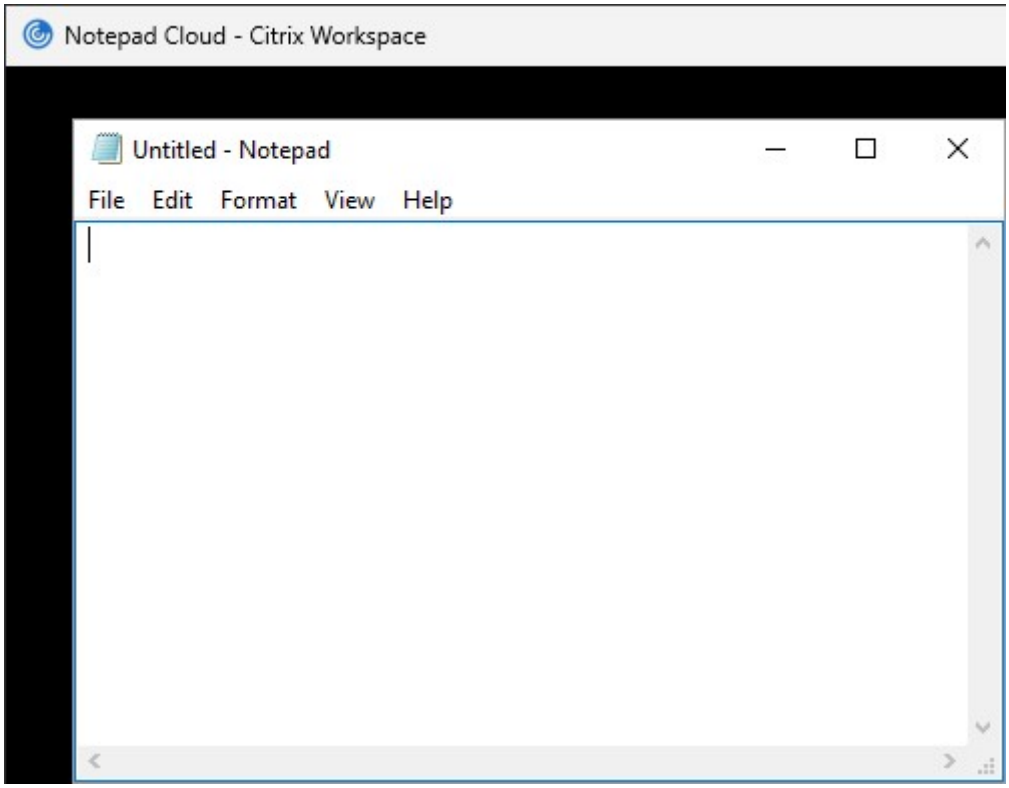
Ejemplo: iniciar el Bloc de notas en modo ventana

Para configurar una aplicación para que se inicie en modo de ventana, en default.ica, agregue una sección para la aplicación con estos parámetros:

- TWIMode: Desactívelo para habilitar el modo de ventana.
- DesiredHRES: Si quiere, establezca la cantidad horizontal de píxeles.
- DesiredVRES: Si quiere, establezca la cantidad vertical de píxeles.

Por ejemplo:

```
[Notepad]
TWIMode=Off
DesiredHRES=1024
DesiredVRES=768
<!--NeedCopy-->
```

ICA File Signing

April 17, 2024

StoreFront ofrece la opción de firmar digitalmente los archivos ICA para que las versiones de la aplicación Citrix Workspace que admiten esta función puedan verificar que el archivo proviene de una fuente de confianza. Cuando la firma de archivos está habilitada en StoreFront, el archivo ICA que se genera cuando un usuario inicia una aplicación se firma mediante un certificado procedente del almacén de certificados personales del servidor de StoreFront. Los archivos ICA pueden firmarse con cualquier algoritmo hash compatible con el sistema operativo que se ejecuta en el servidor de StoreFront. Los clientes que no admiten la función o que no están configurados para ICA File Signing ignoran la firma digital. Si el proceso de firma falla, el archivo ICA se genera sin firma digital y se envía a la aplicación Citrix Workspace, cuya configuración determina si se acepta el archivo sin firmar.

Los certificados deben incluir la clave privada y encontrarse en el período de validez para que puedan utilizarse con ICA File Signing en StoreFront. Si el certificado contiene una extensión de uso de clave, esto debe permitir que la clave se use para firmas digitales. Cuando se incluye una extensión de uso mejorado de clave, se debe configurar con firma de código o autenticación del servidor.

Para utilizar la función ICA File Signing, Citrix recomienda el uso de un certificado de firma de código o

firma SSL obtenido de una entidad de certificación pública o de la entidad de certificados privada de su organización. Si no puede obtener un certificado adecuado de una entidad de certificación, puede utilizar un certificado SSL existente, como un certificado de servidor, o crear un nuevo certificado de entidad de certificación raíz y distribuirlo a los dispositivos de los usuarios.

De forma predeterminada, la función ICA File Signing está inhabilitada en los almacenes. Para activar la función ICA File Signing, modifique el archivo de configuración del almacén y ejecute comandos de Windows PowerShell. Para obtener más información sobre cómo habilitar la firma de archivos ICA en la aplicación Citrix Workspace para Windows, consulte Firma de archivos ICA.

> Nota:
>
> Las consolas de StoreFront y PowerShell no pueden estar abiertas a la vez. Cierre siempre la consola de administración de StoreFront antes de usar la consola de PowerShell para administrar la configuración de StoreFront. Asimismo, cierre todas las instancias de PowerShell antes de abrir la consola de StoreFront.

1. Asegúrese de que el certificado que quiere usar para firmar los archivos ICA esté disponible en el almacén de certificados de Citrix Delivery Services en el servidor de StoreFront y no en el almacén de certificados del usuario actual.
2. Habilite la firma mediante el cmdlet `Set-STFStoreService` de PowerShell:

   ```
   $storeService = Get-STFStoreService
   Set-STFStoreService $storeService -IcaFileSigning $true -
       IcaFileSigningCertificateThumbprint [certificatethumbprint]
   <!--NeedCopy-->
   ```

   Donde **[certificatethumbprint]** es el resultado (o huella digital) de los datos del certificado generado por el algoritmo hash.

   Si quiere utilizar un algoritmo hash que no sea SHA-1, agregue el parámetro **-IcaFileSigningHashAlgorithm** establecido en sha256, sha384 o sha512, según sea necesario.

Configuración de la aplicación Citrix Workspace

February 26, 2024

Global App Config Service

Global App Config Service es un servicio en la nube para administrar la configuración de la aplicación Citrix Workspace. En su cuenta de Citrix Cloud, puede reclamar las URL de su almacén y definir la

configuración para cada una de sus almacenes. Para obtener más información, consulte Configurar los parámetros de los almacenes locales.

Parámetros de la cuenta del almacén

Como alternativa al Global App Config Service, puede configurar la aplicación Citrix Workspace mediante los parámetros de la cuenta del almacén. Cuando un usuario agrega un almacén a una aplicación Citrix Workspace instalada localmente, recupera los parámetros de la cuenta de almacén de StoreFront. Esto puede incluir propiedades de configuración, por ejemplo, para indicar a la aplicación Citrix Workspace para Windows si debe crear en el menú de inicio accesos directos para las aplicaciones. Consulte en la documentación de la aplicación Workspace más información sobre las propiedades, por ejemplo, Usar parámetros de cuenta de StoreFront para personalizar las ubicaciones de los accesos directos de aplicaciones.

Para modificar estos parámetros:

1. Abra el archivo web.config en `C:\inetpub\wwwroot\Citrix\Roaming`.
2. En la sección `<Accounts>`, busque el elemento `<account ... name="Store"... >` del almacén que quiere cambiar.
3. En la sección `Account`, busque la sección `<annotatedServices>/<annotatedServiceRecord>/<metadata>/<properties>`.
4. Después del elemento `<clear/>`, agregue las propiedades en el formulario `<property name="[name]"value="[value]"/>`. Por ejemplo:

```
<properties>
    <clear/>
    <property name="PutShortcutsOnDesktop" value="true"/>
    <property name="DesktopDir" value="Citrix Applications"/>
</properties>
<!--NeedCopy-->
```

> **Importante**
>
> En implementaciones con varios servidores, use solo un servidor a la vez para hacer cambios en la configuración del grupo de servidores. Compruebe que la consola de administración de Citrix StoreFront no se está ejecutando en ninguno de los demás servidores de la implementación. Una vez completados, propague los cambios de configuración al grupo de servidores de modo que los demás servidores de la implementación se actualicen.

Sitio web de la aplicación Workspace

Para configurar qué configuración de sitio web utiliza la aplicación Citrix Workspace instalada localmente, consulte Configurar el sitio web de la aplicación Workspace.

Administrar un sitio web

August 15, 2023

Para cada almacén, puede configurar uno o más sitios web a los que los usuarios puedan acceder mediante un explorador web o mediante la aplicación Citrix Workspace.

Use la consola de administración de StoreFront para realizar estas tareas:

Tarea	Detalles
Crear un sitio web	Cree sitios web que permitan a los usuarios acceder a almacenes a través de una página web o la aplicación Workspace.
Configurar un sitio web	Modifique los parámetros de su sitio web.
Quitar un sitio web	Quite un sitio de Citrix Receiver para Web.
Configurar el sitio web de la aplicación Workspace	Elija el sitio web que quiere utilizar desde la aplicación Citrix Workspace.

Crear un sitio web

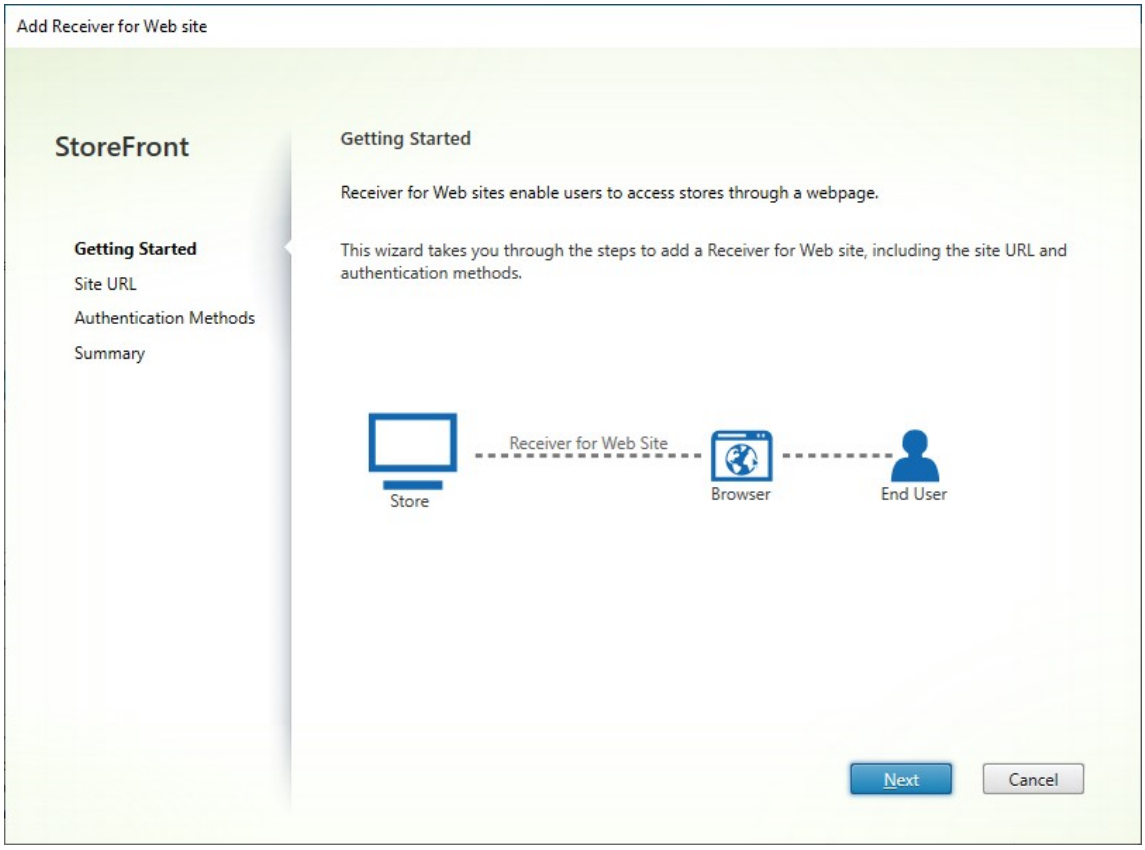
December 4, 2023

Al crear un almacén, se crea automáticamente un sitio web para él. Puede agregar sitios web adicionales a los almacenes existentes. Esto le permite proporcionar diferentes URL con diferentes configuraciones a sus usuarios. Sin embargo, solo se puede acceder a varios sitios web a través de un explorador web, ya que las aplicaciones Citrix Workspace están configuradas para usar un sitio web específico de un almacén. Consulte Configurar el sitio web de la aplicación Workspace.

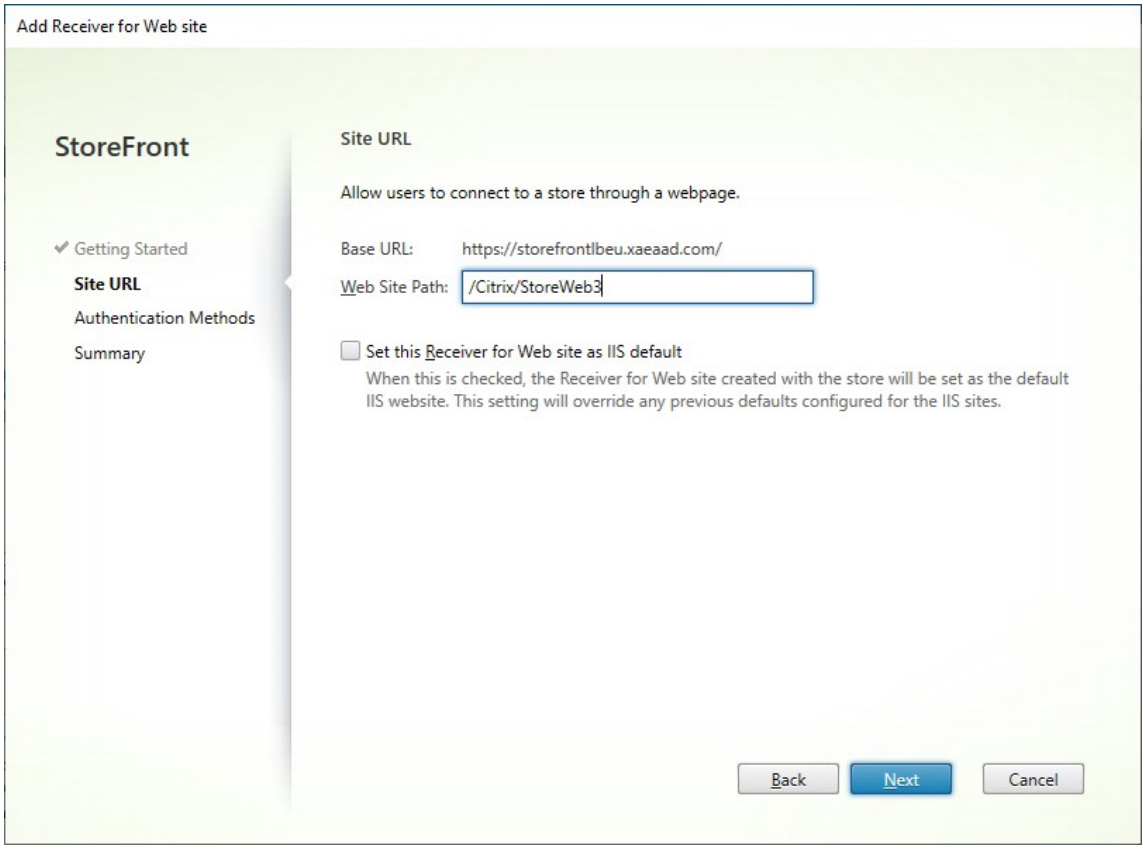
> Importante:
>
> En implementaciones con varios servidores, use solo un servidor a la vez para hacer cambios en

> la configuración del grupo de servidores. Compruebe que la consola de administración de Citrix StoreFront no se está ejecutando en ninguno de los demás servidores de la implementación. Una vez completados,
> propague los cambios de configuración al grupo de servidores de modo que los demás servidores de la implementación se actualicen.

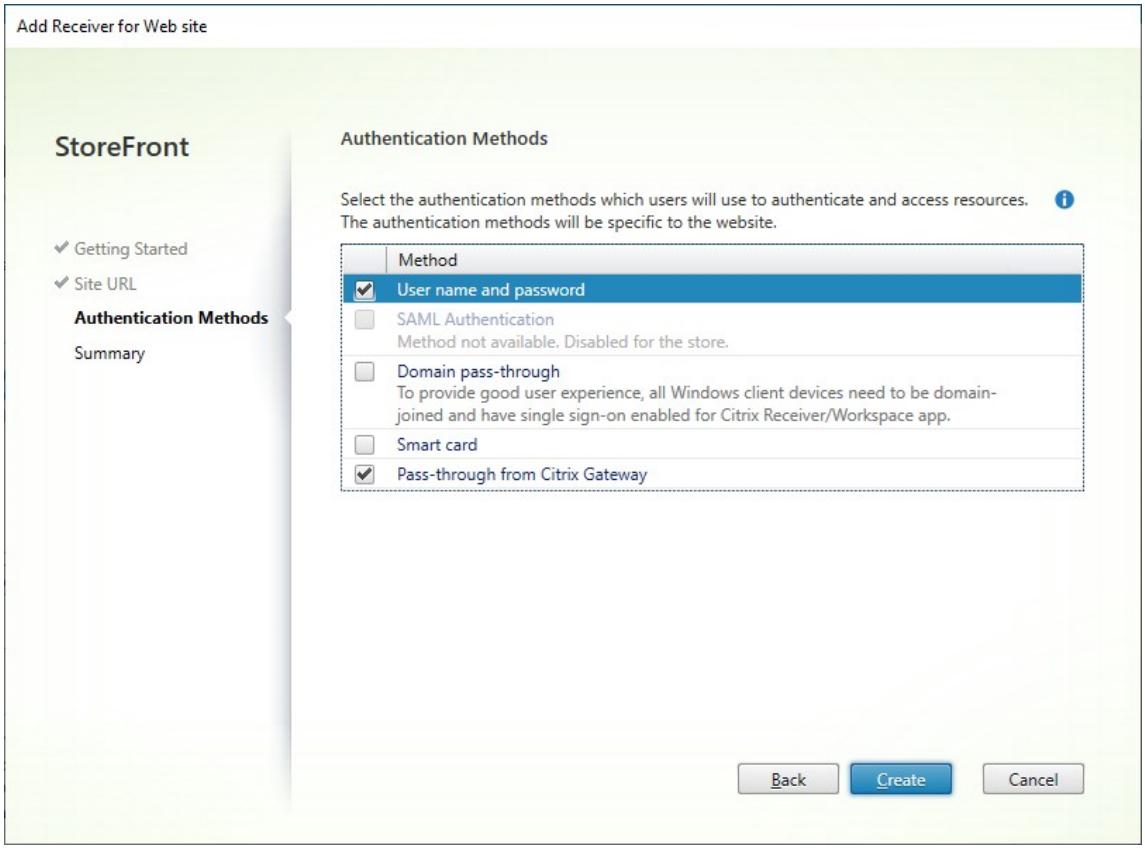
1. En la consola de administración, seleccione el almacén para el que quiere crear el sitio web y, en el panel Acciones, haga clic en **Administrar sitios de Receiver para Web**.
2. Haga clic en **Agregar** y, a continuación, en **Siguiente**.



3. Escriba la **Ruta del sitio web** que quiera, elija si quiere que este sea el sitio web predeterminado para la URL base y haga clic en **Siguiente**.



4. Marque o desmarque los métodos de autenticación que quiera. Algunos métodos solo están disponibles si se han configurado para el almacén. Presione **Siguiente**.



5. Después de haber creado el sitio, haga clic en **Finalizar**.
6. Seleccione el sitio recién creado y presione **Modificar** para configurar el sitio web según sea necesario. Consulte Configurar sitios web.

Crear un sitio web con el SDK de PowerShell

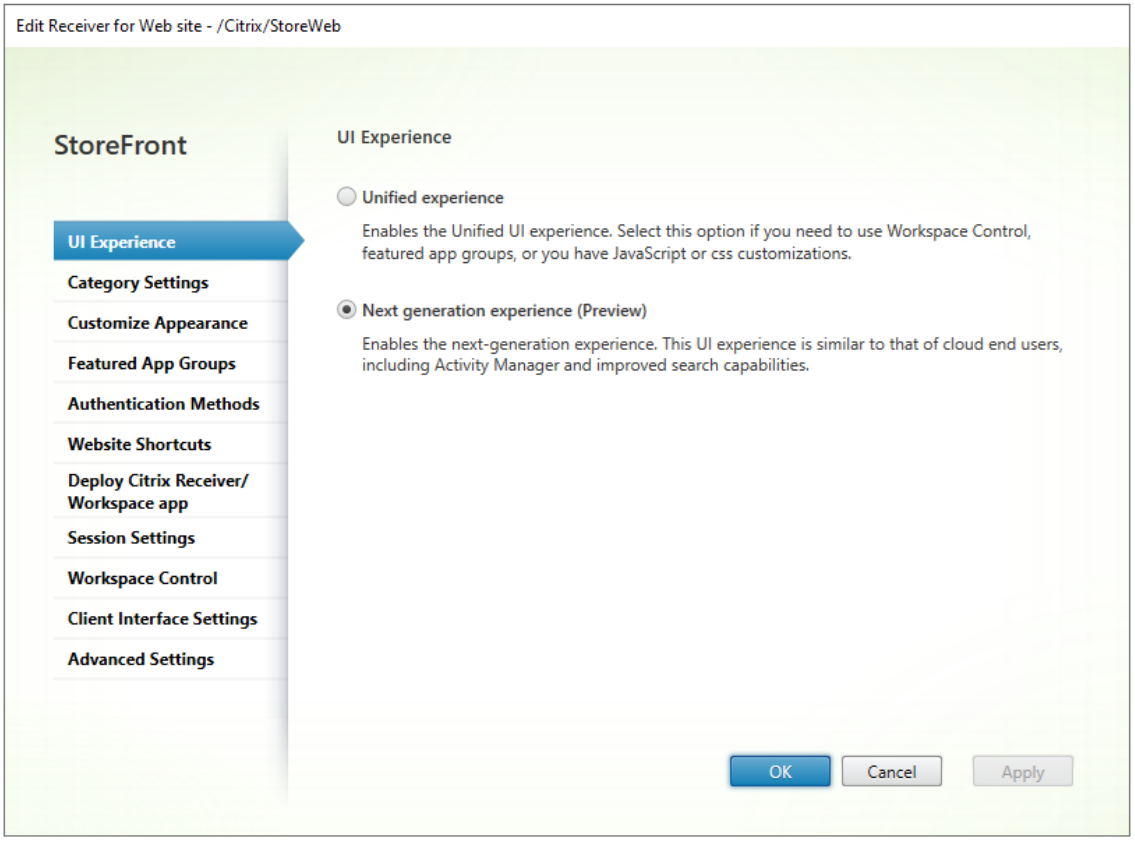
Para crear un sitio web con el SDK de PowerShell, llame al cmdlet Add-STFWebReceiverService.

Configurar un sitio web

January 26, 2024

Para configurar un sitio web:

1. Seleccione el nodo **Almacenes** en el panel izquierdo y, en el panel **Acciones**, haga clic en **Administrar sitios de Receiver para Web**.
2. Seleccione un sitio web y presione **Configurar…**



3. Modifique los parámetros en las fichas correspondientes.

   - Experiencia de interfaz de usuario
   - Parámetros de las categorías
   - Personalizar apariencia
   - Grupos de aplicaciones destacadas
   - Métodos de autenticación
   - Accesos directos a sitios web
   - Implementar la aplicación Workspace/Citrix Receiver
   - Parámetros de sesión
   - Control del espacio de trabajo
   - Parámetros de interfaz del cliente
   - Parámetros avanzados

4. Cuando haya terminado los cambios, haga clic en **Aceptar**.

5. Para configurar App Protection, debe usar PowerShell. Cierre la consola de administración de StoreFront antes de ejecutar comandos de PowerShell.

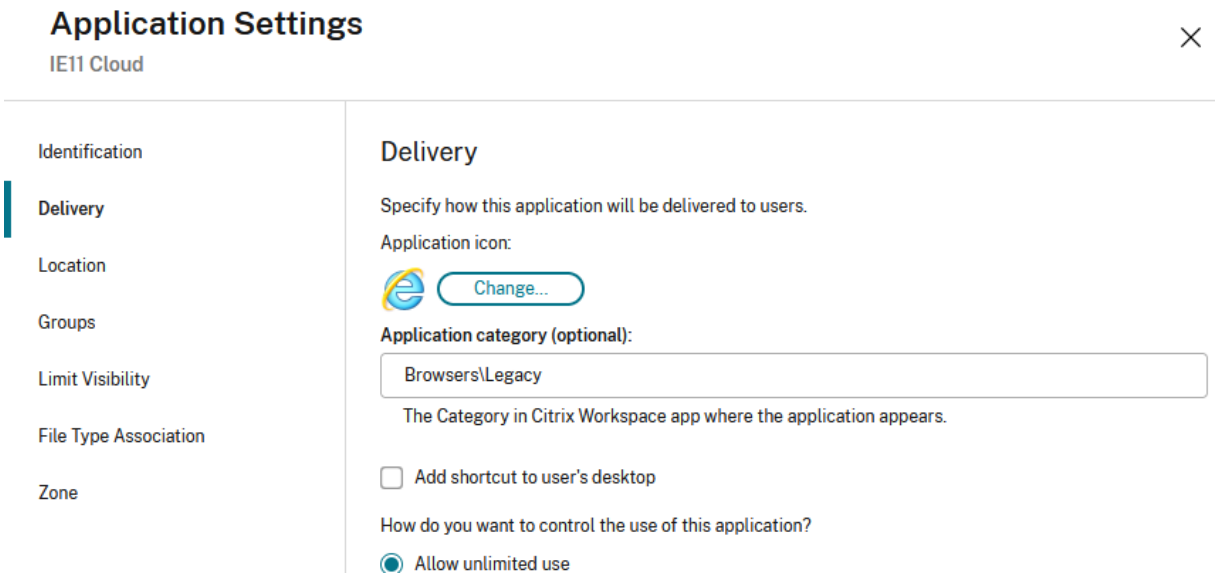
> **Importante:**
>
> En implementaciones con varios servidores, use solo un servidor a la vez para hacer cambios en

> la configuración del grupo de servidores. Compruebe que la consola de administración de Citrix StoreFront no se está ejecutando en ninguno de los demás servidores de la implementación. Una vez completados,
> propague los cambios de configuración al grupo de servidores de modo que los demás servidores de la implementación se actualicen.

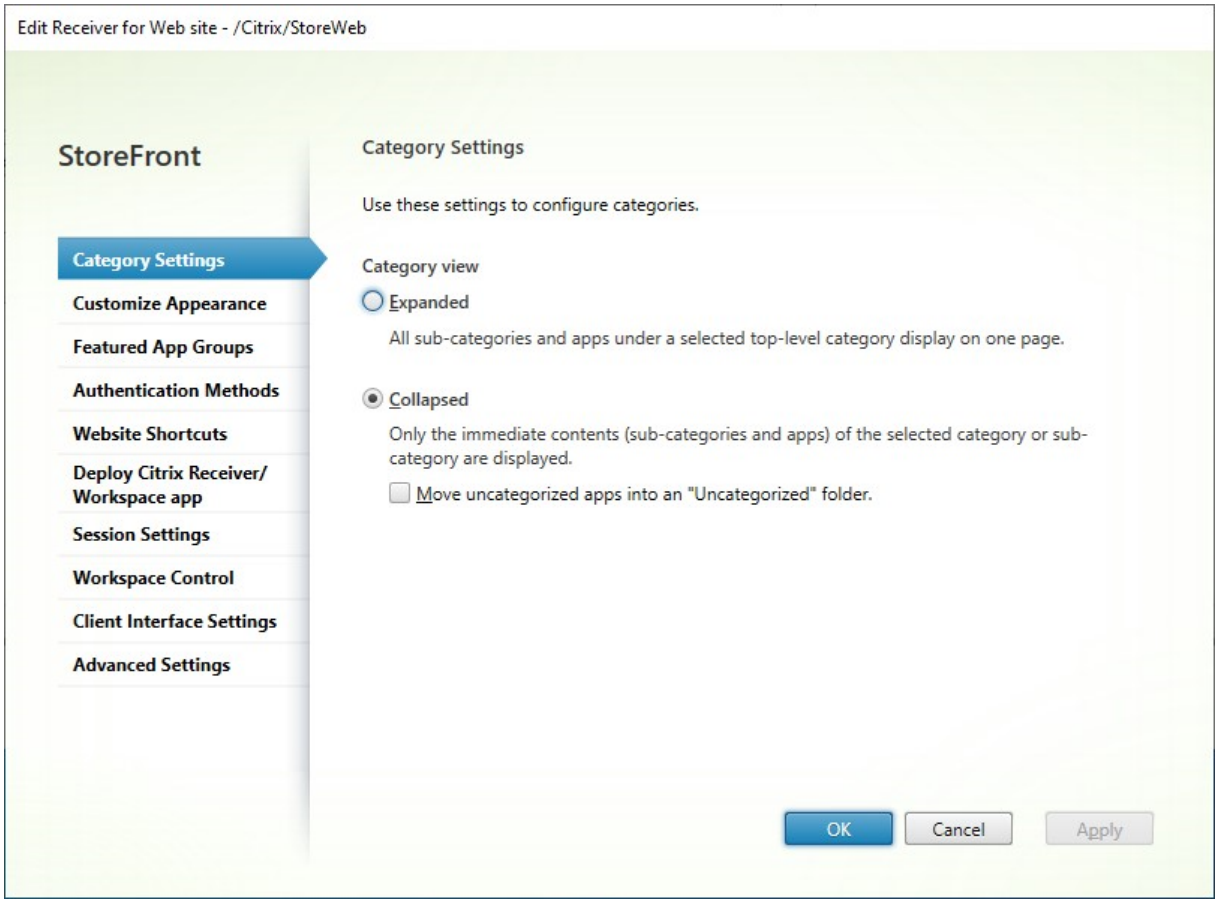
Parámetros de las categorías

December 4, 2023

En Citrix Virtual Apps and Desktops, puede asignar cada aplicación a una categoría, tal y como se describe en el artículo Aplicaciones. Utilice el símbolo \ para crear una jerarquía de categorías de carpetas. En StoreFront, puede configurar cómo se muestra esta jerarquía de carpetas.



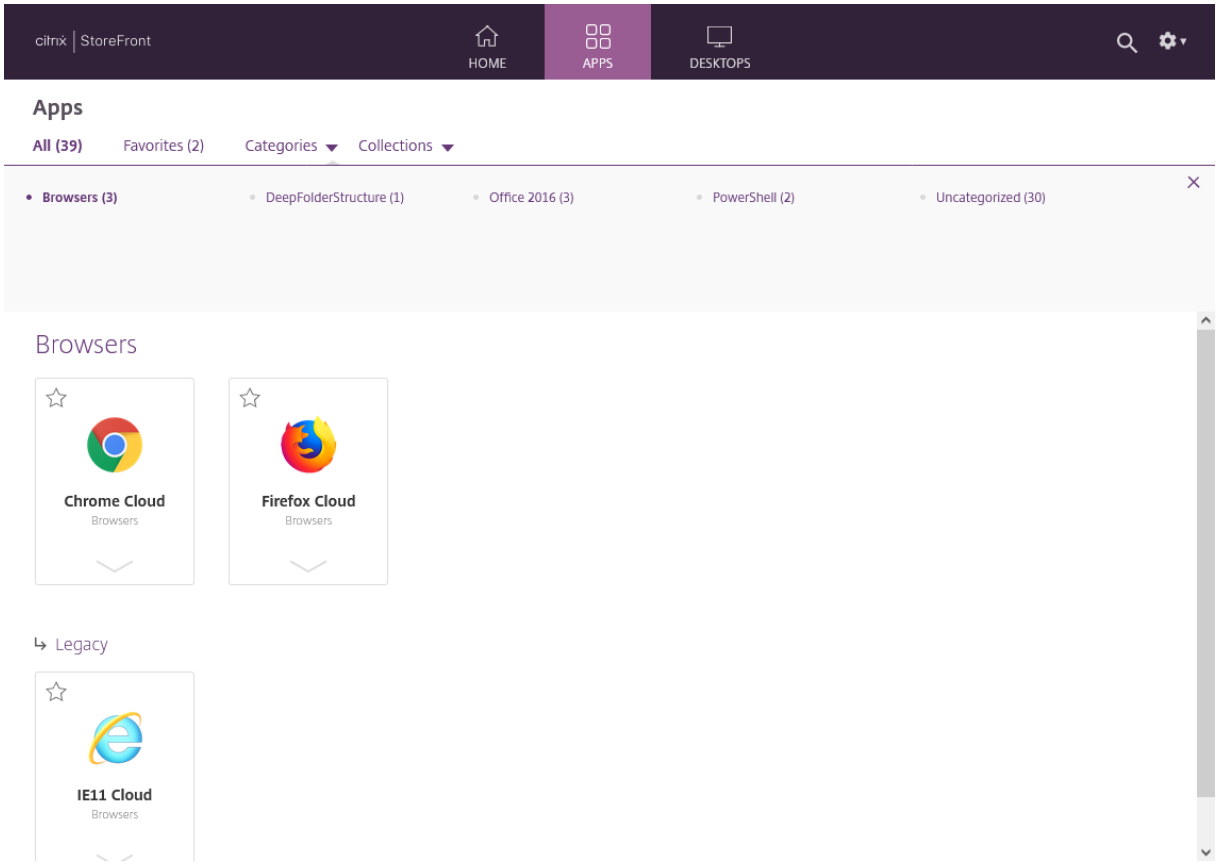
Para modificar los parámetros de categoría, vaya a Modificar sitio de Receiver para Web y seleccione la ficha **Parámetros de categoría**.



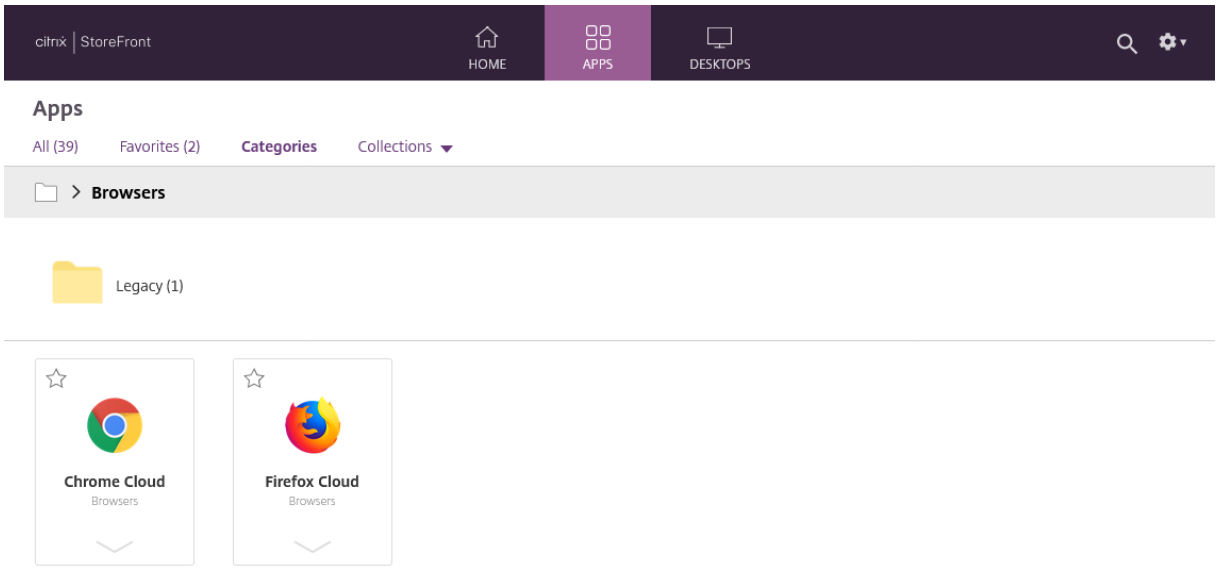
Vista de las categorías

En la vista ampliada, StoreFront muestra una lista de categorías de nivel superior. Cuando el usuario hace clic en una categoría de nivel superior, StoreFront muestra todas las aplicaciones de todas las subcategorías en una página.

Por ejemplo, si tiene una categoría Explorador web con la subcategoría Antiguo, mostrará todos los exploradores web, incluidos los de Antiguo, en una página:

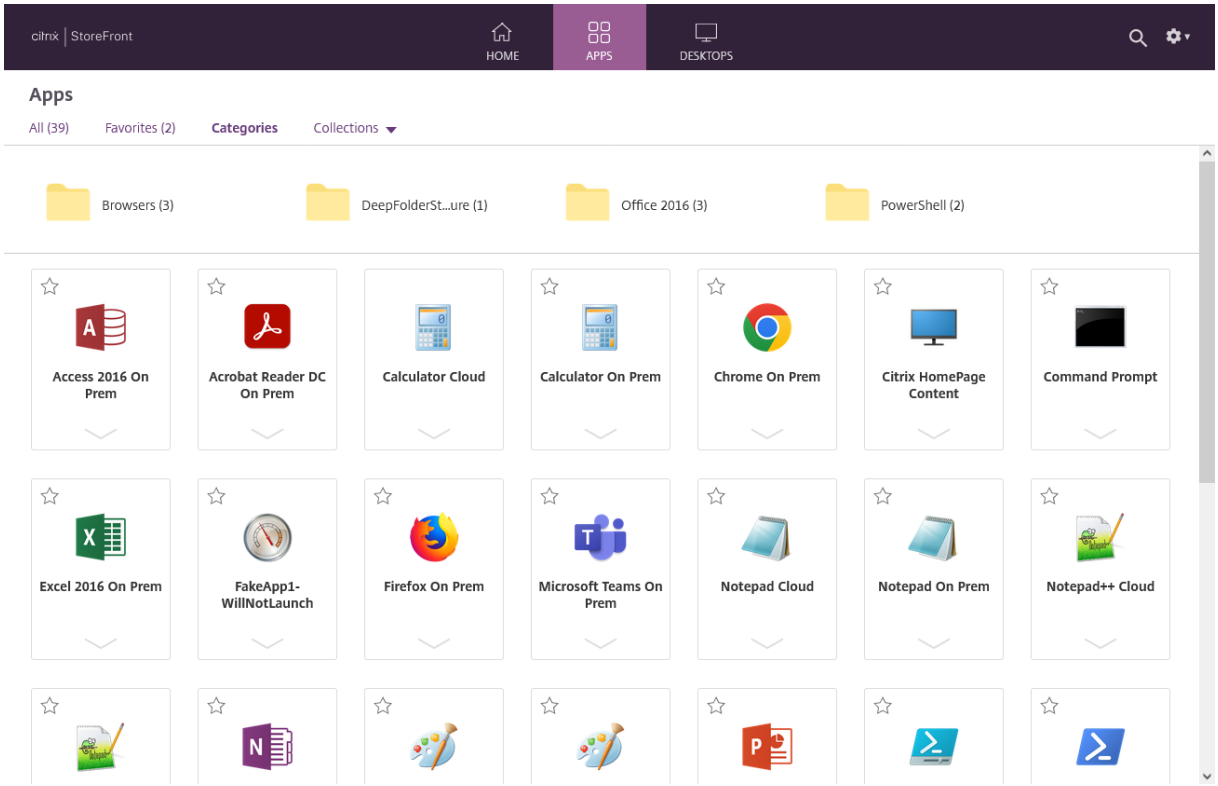


En la vista contraída, StoreFront muestra inicialmente una lista de categorías de nivel superior y, opcionalmente, todas las aplicaciones sin categoría. Cuando el usuario hace clic en una categoría, StoreFront muestra solo el contenido inmediato (subcategorías y aplicaciones) de la categoría seleccionada. El usuario puede hacer clic en cada subcategoría para ampliar el contenido.

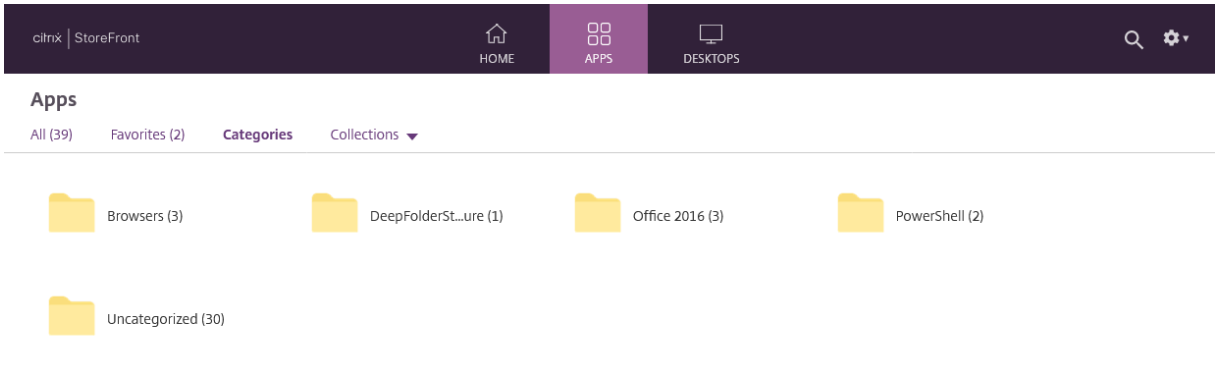


Aplicaciones sin categoría

En la vista contraída, desactive la opción **Mover aplicaciones sin categoría a una carpeta "Sin categoría"** para mostrar todas las aplicaciones y escritorios sin categorías en la vista inicial. Este comportamiento es similar al de las versiones anteriores de StoreFront.



En la vista colapsada, marque **Mover aplicaciones sin categoría a la carpeta "Sin categoría"** para mover todas las aplicaciones y escritorios sin categoría a una carpeta independiente **Sin categoría**.



Configurar parámetros de categoría con el SDK de PowerShell

Para usar el SDK de PowerShell para habilitar o inhabilitar la vista por categorías, llame al cmdlet Set-STFWebReceiverUserInterface con el parámetro `EnableAppsFolderView`.

Para usar el SDK de PowerShell para cambiar la vista por categorías, llame al cmdlet Set-STFWebReceiverUserInterface con el parámetro `CategoryViewCollapsed`.

Personalizar apariencia

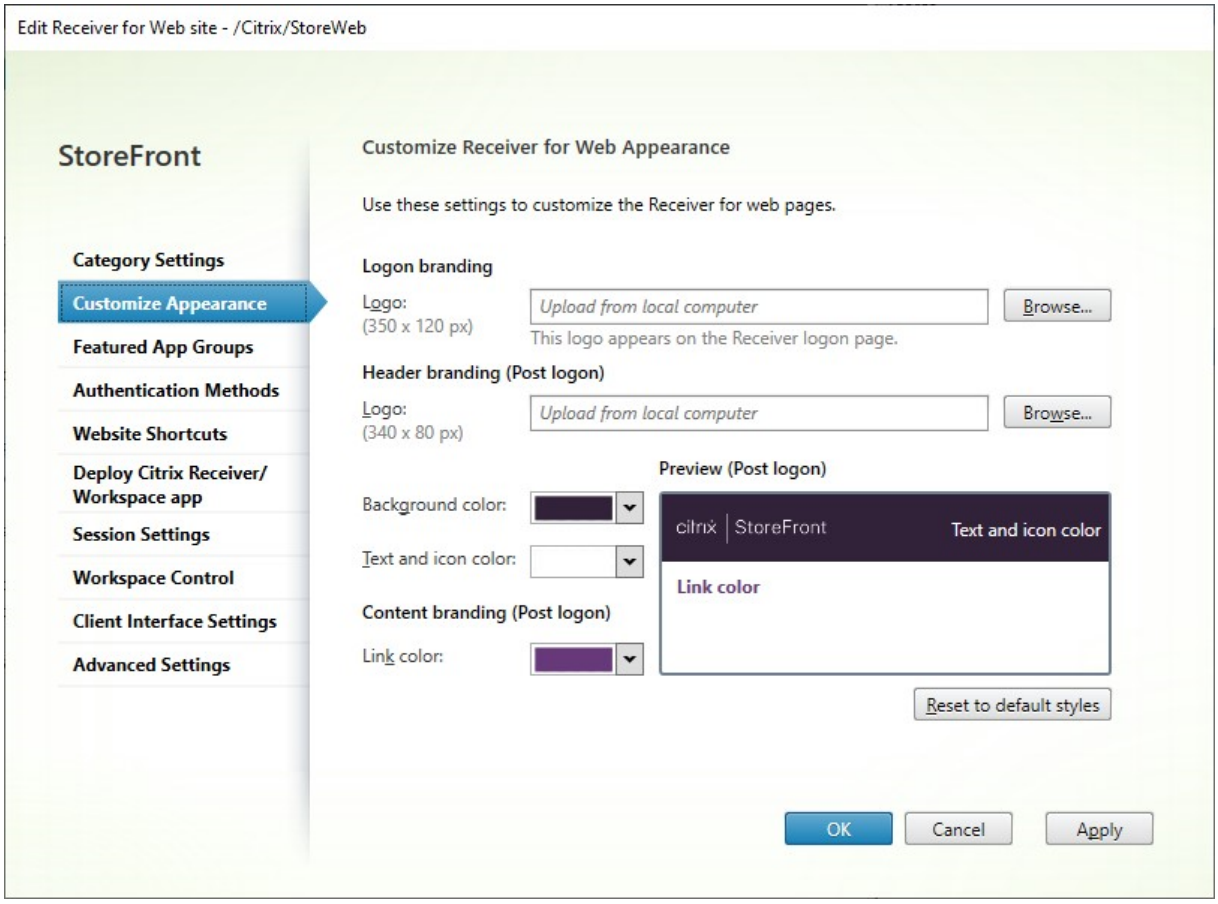
December 4, 2023

Puede modificar el logotipo y los colores que se usan en el sitio web de su almacén.

Modificar el logotipo y los colores

Para personalizar la apariencia, vaya a Modificar sitio de Receiver para Web y seleccione la ficha **Personalizar apariencia**. Puede modificar lo siguiente:

- **Logotipo de marca al iniciar sesión**: El logotipo que se muestra en la pantalla de inicio de sesión. No se muestra al iniciar sesión a través de Citrix Gateway. Presione **Examinar...** y seleccione un archivo de tipo .jpg, .jpeg, .png, .png o .bmp. Se recomienda utilizar una imagen de 350 x 120 píxeles.
- **Logotipo de marca del encabezado**. El logotipo se muestra en la esquina superior izquierda después de iniciar sesión. Presione **Examinar...** y seleccione un archivo de tipo .jpg, .jpeg, .png, .png o .bmp. Se recomienda utilizar una imagen de 340 x 80 píxeles.
- **Color de fondo**: El color de fondo de la sección de navegación en la parte superior de la página.
- **Color de iconos y texto**: El color de iconos y texto de la sección de navegación en la parte superior de la página.
- **Color de los enlaces**: El color que se utiliza para resaltar el elemento seleccionado actualmente.



Modificar el logotipo y los colores con el SDK de PowerShell

Con el SDK de PowerShell, llame al cmdlet Set-STFWebReceiverSiteStyle.

Restablecer la apariencia a su valor predeterminado

Presione **Restablecer estilos predeterminados** para devolver los logotipos y los colores a sus valores predeterminados.

Restablecer la apariencia a sus valores predeterminados con el SDK de PowerShell

Con el SDK de PowerShell, llame al cmdlet Clear-STFWebReceiverSiteStyle.

Personalización mediante JavaScript y CSS

Puede personalizar aún más el sitio web mediante la API de personalización de la IU del cliente de StoreFront.

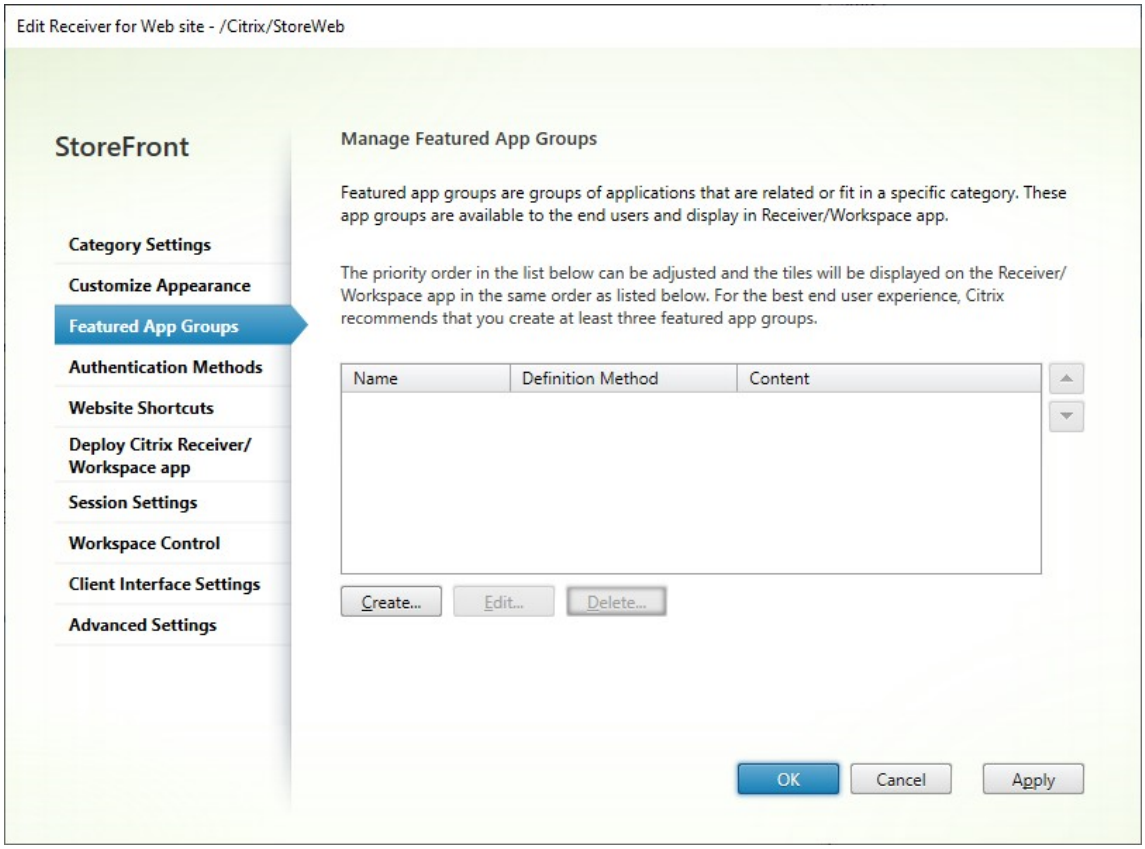
Grupos de aplicaciones destacadas

December 4, 2023

Se pueden crear grupos de aplicaciones destacadas de productos, relacionadas o pertenecientes a una categoría específica, para los usuarios finales. Por ejemplo, puede crear un grupo de las aplicaciones destacadas del departamento de ventas que contenga las aplicaciones que se usen en ese departamento. Para definir aplicaciones destacadas en la consola de administración de StoreFront, puede valerse de los nombres de las aplicaciones, las palabras clave o las categorías de aplicaciones que se han definido en la consola de Studio.

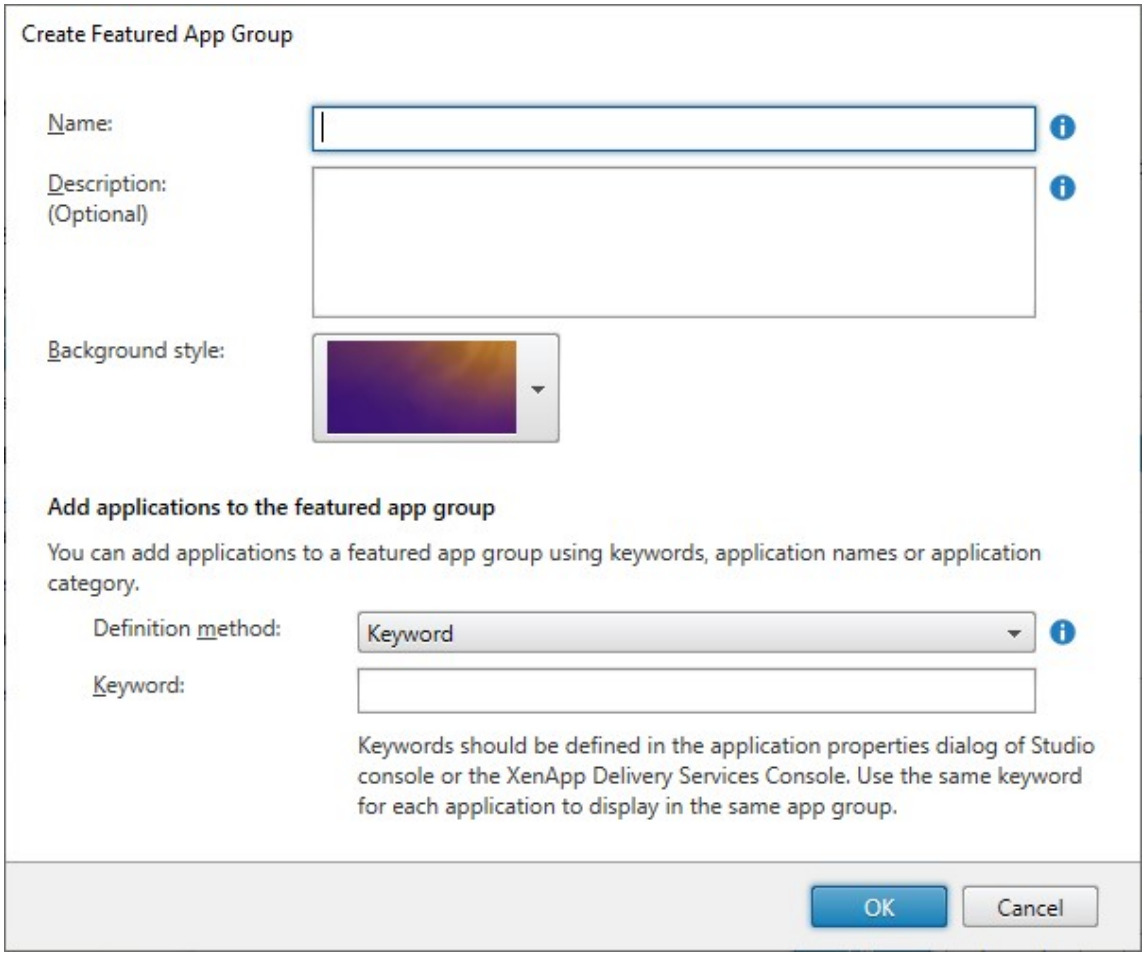
Crear grupo de aplicaciones destacadas

1. En la pantalla Modificar sitio de Receiver para Web, seleccione la ficha **Grupos de aplicaciones destacadas**.



2. Haga clic en **Crear** para definir un nuevo grupo de aplicaciones destacadas.
3. Especifique un nombre, una descripción (optativa) y un fondo para ellos, así como el método mediante el que se definen los grupos de aplicaciones destacadas. Puede elegir entre palabras clave, nombres de las aplicaciones o categoría de la aplicación.

Opción	Descripción
Palabras clave	Busca aplicaciones en función de la palabra clave, definida por Studio al incluir palabras clave en la descripción de la aplicación. Por ejemplo: “Se usa para enviar y recibir correos electrónicos KEYWORDS: colaboración”.
Categoría de aplicación	Busca aplicaciones de una categoría de aplicaciones específica introducida en Studio.
Nombres de las aplicaciones	Use el nombre de las aplicaciones para definir el grupo de aplicaciones destacadas. Los nombres de todas las aplicaciones que coincidan con el nombre que contenga el cuadro de diálogo “Crear un grupo de aplicaciones destacadas”se incluyen en el grupo de aplicaciones destacadas. StoreFront no admite comodines en los nombres de las aplicaciones. En las coincidencias no se distinguen mayúsculas de minúsculas, aunque sí se distinguen palabras completas. Por ejemplo, si escribe Excel, StoreFront establece la correspondencia con una aplicación publicada llamada Microsoft Excel 2013. Sin embargo, si escribe `Exc`, no hay coincidencias.

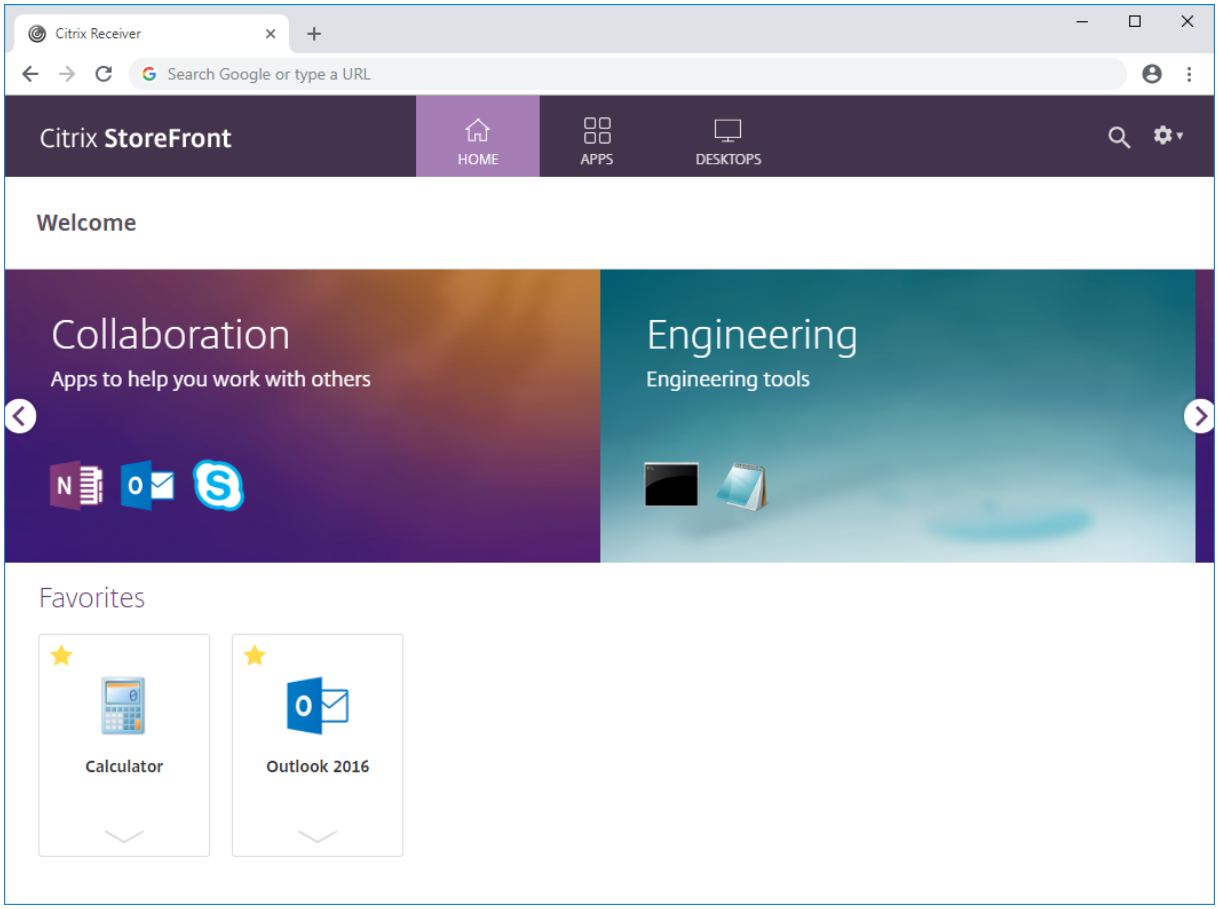


4. Haga clic en **OK**.

Ejemplo:

Hemos creado dos grupos de aplicaciones destacadas:

- Collaboration: Compuesto por aplicaciones de la categoría **Collaboration** de Studio.
- Engineering: Creado al nombrar el grupo de aplicaciones y especificar una colección de nombres de aplicaciones.



Crear un grupo de aplicaciones destacadas con el SDK de PowerShell

Para agregar un grupo de aplicaciones destacadas con el SDK de PowerShell, use el cmdlet New-STFWebReceiverFeaturedAppGroup.

Modificar grupo de aplicaciones destacadas

En la pantalla Modificar sitio de Receiver para Web, seleccione la ficha **Grupos de aplicaciones destacadas**. Seleccione el grupo que quiera modificar y haga clic en **Modificar...**

Modificar un grupo de aplicaciones destacadas con el SDK de PowerShell

Para modificar un grupo de aplicaciones destacadas con el SDK de PowerShell, use el cmdlet Set-STFWebReceiverFeaturedAppGroup.

Eliminar grupo de aplicaciones destacadas

En la pantalla Modificar sitio de Receiver para Web, seleccione la ficha **Grupos de aplicaciones destacadas**. Seleccione el grupo que quiera modificar y haga clic en **Eliminar…**

Eliminar un grupo de aplicaciones destacadas con el SDK de PowerShell

Con el SDK de PowerShell para eliminar un grupo de aplicaciones destacadas, use el cmdlet Remove-STFWebReceiverFeaturedAppGroup y, para eliminar todos los grupos de aplicaciones destacadas, use el cmdlet Clear-STFWebReceiverFeaturedAppGroup.

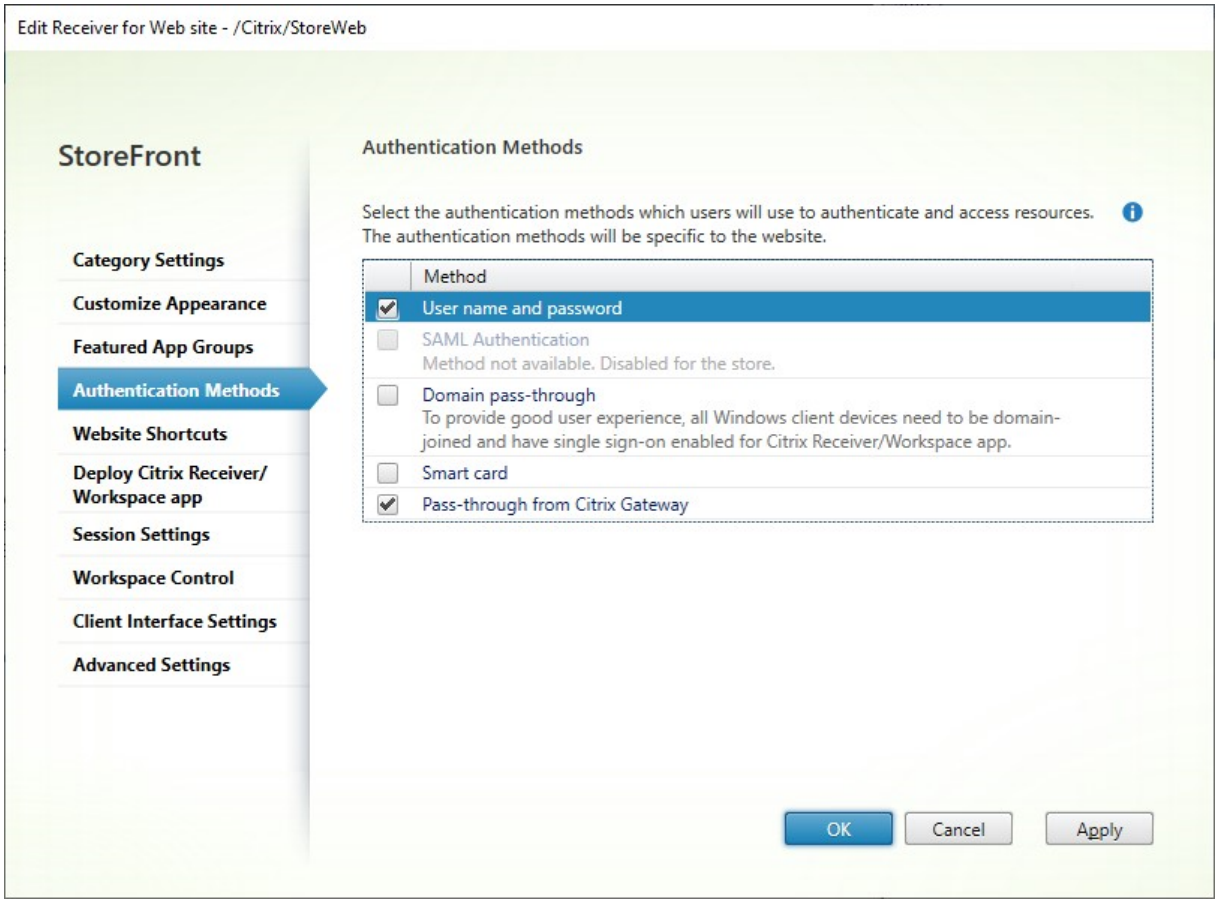
Métodos de autenticación

April 17, 2024

Para configurar los métodos de autenticación disponibles para un almacén, consulte Configurar la autenticación. Puede supeditar algunos de estos parámetros para un sitio web determinado. Estas supeditaciones solo se aplican mediante la aplicación Citrix Workspace para HTML5 a través de un explorador web. La aplicación Citrix Workspace instalada localmente usa los parámetros del almacén, no del sitio web.

> **Advertencia:**
> Cada vez que cambia los métodos de autenticación de un almacén, esto supedita los parámetros de todos los sitios web de ese almacén, por lo que los cambios deben aplicarse de nuevo.

Para modificar los métodos de autenticación, vaya a Modificar sitio de Receiver para Web y seleccione la ficha **Métodos de autenticación**.



- Marque la casilla **Nombre de usuario y contraseña** para habilitar la autenticación explícita. Consulte Autenticación con nombre de usuario y contraseña. Esta opción solo está disponible si está habilitada para el almacén.
- Marque la casilla **Autenticación SAML** para permitir la integración en proveedores de identidades SAML. Consulte Autenticación SAML. Esta opción solo está disponible si se habilitó para el almacén.
- Marque la casilla **PassThrough de dominio** para habilitar la autenticación PassThrough de las credenciales de dominio de Active Directory desde los dispositivos de los usuarios. Consulte Autenticación PassThrough de dominio. Esta opción solo está disponible si se habilitó para el almacén.
- Marque **Tarjeta inteligente** para habilitar la autenticación con tarjeta inteligente. Consulte Autenticación con tarjeta inteligente.
- Marque **PassThrough desde Citrix Gateway** para habilitar la autenticación PassThrough desde Citrix Gateway. Habilite esta opción si los usuarios se conectan a StoreFront a través de un dispositivo Citrix Gateway con la autenticación habilitada. Consulte PassThrough desde Citrix Gateway.

Configuración con el SDK de PowerShell

Para configurar los métodos de autenticación disponibles mediante el SDK de PowerShell, use el cmdlet Set-STFWebReceiverAuthenticationMethods.

Accesos directos a sitios web

December 4, 2023

Use accesos directos a sitios web para proporcionar a los usuarios acceso inmediato a escritorios y aplicaciones desde sitios web de confianza alojados en la red interna. Debe generar direcciones URL para los recursos disponibles a través del sitio de Citrix Receiver para Web e insertar estos vínculos en los sitios web. Los usuarios hacen clic en un enlace, y se les redirige al sitio de Receiver para Web, donde deben iniciar sesión si todavía no lo han hecho. El sitio de Receiver para Web inicia automáticamente el recurso. En el caso de las aplicaciones, los usuarios también se suscriben a ellas si no lo han hecho anteriormente.

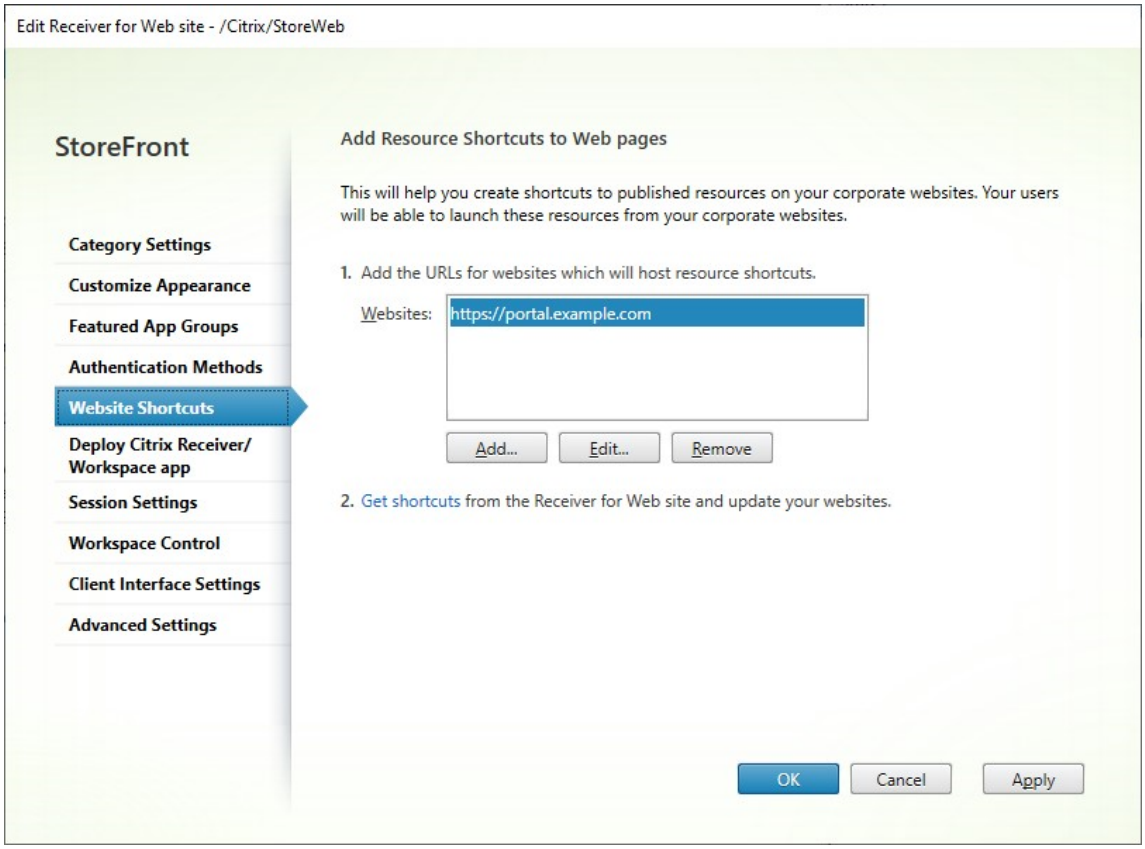
Para poder generar accesos directos a recursos, debe agregar las direcciones URL de sitios web host a la lista *URL de confianza* desde la consola de administración de Citrix StoreFront o mediante PowerShell.

De forma predeterminada, StoreFront avisa a los usuarios si intentan iniciar accesos directos a recursos desde sitios web que no son de confianza, pero los usuarios pueden optar por iniciar el recurso igualmente. Para que esos avisos dejen de aparecer, haga clic en **Administrar sitios de Receiver para Web**, en el panel Almacenes **>** haga clic en **Configurar >** elija **Parámetros avanzados >** desactive la opción **Preguntar si no se confía en los accesos directos**.

Por motivos de seguridad, es posible que los usuarios de Internet Explorer tengan que confirmar que desean iniciar los recursos a los que se accede a través de accesos directos. Indique a los usuarios que agreguen el FQDN del servidor de StoreFront a la zona de Intranet local o a Sitios de confianza en Internet Explorer para evitar este paso adicional.

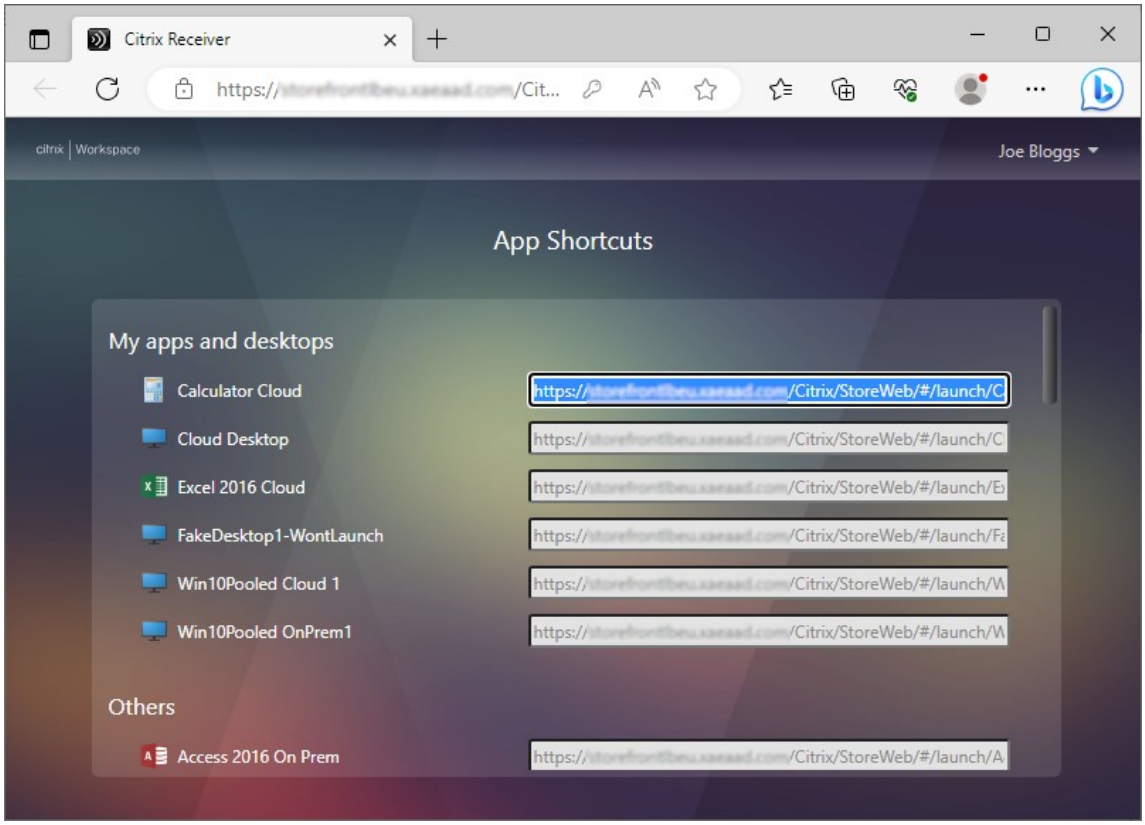
Agregar sitios web de confianza desde la consola de administración

1. En la pantalla Modificar sitio de Receiver para Web, seleccione la ficha **Accesos directos del sitio web**.



2. Haga clic en **Agregar** para introducir la dirección URL del sitio web donde va a colocar los accesos directos. Las direcciones URL deben especificarse siguiendo el formato *http[s]://hostname[:port]*, donde “hostname”es el nombre de dominio completo del host del sitio web y “port”es el puerto utilizado para la comunicación con el host, si el puerto predeterminado para el protocolo no está disponible. Las rutas a las páginas específicas del sitio web no son necesarias. Para modificar una URL, seleccione la entrada de la lista Sitios Web y haga clic en **Modificar**. Seleccione una entrada de la lista y haga clic en **Quitar** para eliminar la URL de un sitio web en el que ya no quiere alojar accesos directos a los recursos disponibles a través del sitio de Citrix Receiver para Web.

3. Haga clic en **Obtener accesos directos** y copie las URL que necesite para su sitio web.



Agregar sitios web de confianza con el SDK de PowerShell

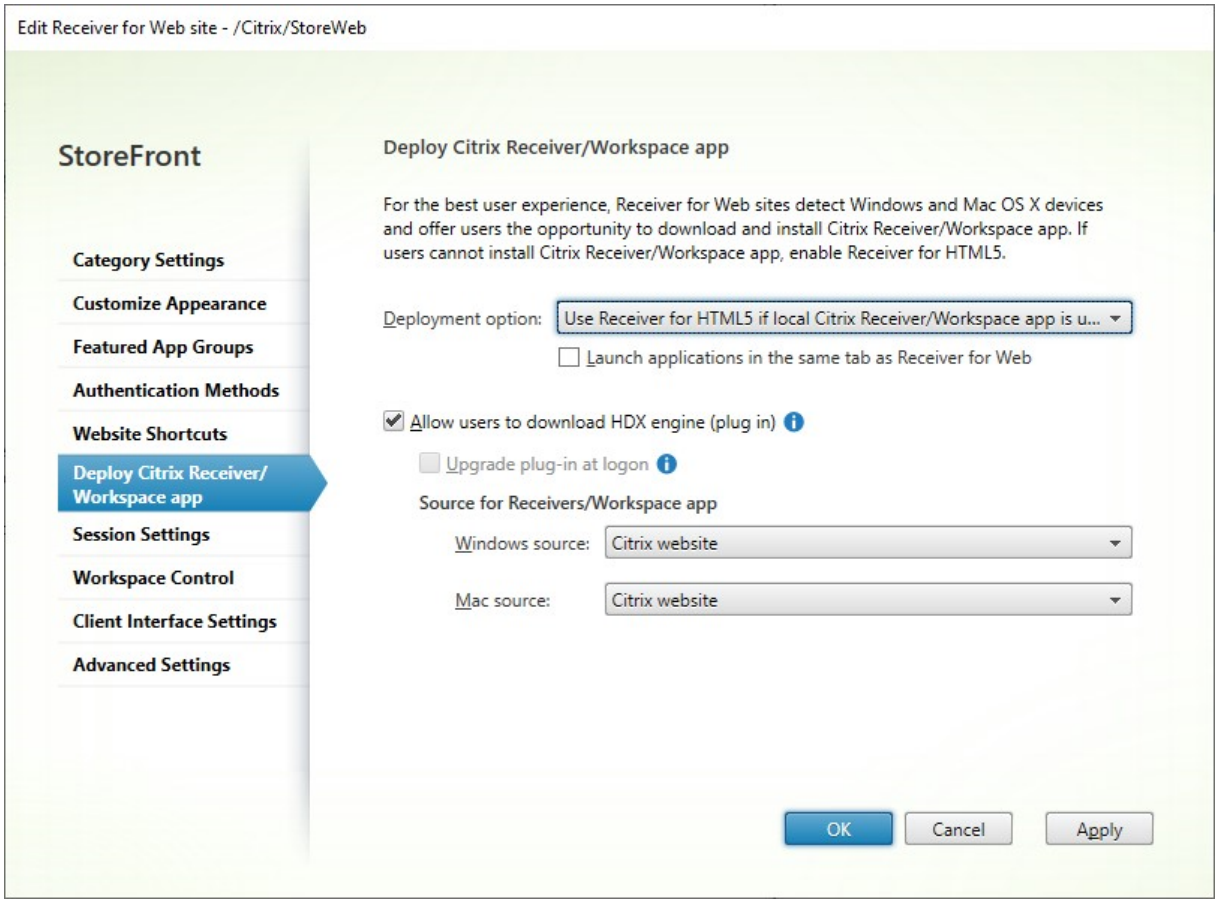
Puede agregar direcciones URL de confianza mediante el cmdlet de PowerShell Set-STFWebReceiverApplicationSh

Implementación de la aplicación Citrix Workspace

December 4, 2023

De forma predeterminada, cuando un usuario va por primera vez a un almacén desde un explorador web en Windows, macOS o Linux, StoreFront intenta determinar automáticamente si la aplicación Citrix Workspace está instalada.

Si no se detecta ninguna aplicación Citrix Workspace instalada localmente, se solicita al usuario que la descargue y la instale. La ubicación de descarga predeterminada es el sitio web de Citrix, pero también puede alojar los instaladores en el servidor de StoreFront o en otro lugar. Los usuarios que no puedan instalar la aplicación Citrix Workspace localmente pueden usar la aplicación Citrix Workspace para HTML5 a través de su explorador web.



Para modificar opciones de implementación, vaya a Modificar sitio de Receiver para Web y seleccione la ficha **Implementar la aplicación Citrix Receiver/Workspace**.

Opción de implementación

- Seleccione **Usar siempre Receiver para HTML5** si quiere que el usuario acceda siempre a los recursos a través de un explorador web sin pedirle que descargue ni instale la aplicación Citrix Workspace localmente. Con esta opción seleccionada, los usuarios de Workspace para HTML5 siempre acceden a recursos directamente a través de sus exploradores web.
- Seleccione **Usar Receiver para HTML5 si el Receiver local no está disponible** si quiere que el sitio web del almacén solicite al usuario que descargue e instale la aplicación Citrix Workspace localmente, pero que recurra al acceso a recursos a través de un explorador web si no se puede instalar la aplicación Citrix Workspace. A los usuarios sin la aplicación Citrix Workspace se les solicitará que la descarguen y la instalen cada vez que inicien sesión en el sitio.
- Seleccione **Instalar localmente** si quiere que el sitio siempre tenga acceso a los recursos a través de una aplicación Citrix Workspace instalada localmente. Se solicita a los usuarios que descarguen e instalen la aplicación Citrix Workspace adecuada para su plataforma. Los usuarios pueden seguir accediendo al almacén a través de un explorador web, pero, cuando inician

recursos, estos se abren en la aplicación Workspace instalada localmente.

Iniciar aplicaciones en la misma ficha

Si eligió **Usar siempre Receiver para HTML5** o **Usar Receiver para HTML5 si el Receiver local no está disponible**, de forma predeterminada, los recursos iniciados en el explorador web abren una nueva ficha del explorador web. Si quiere que los recursos se abran en la misma ficha y sustituyan a la aplicación Workspace para HTML5, seleccione **Iniciar aplicaciones en la misma ficha que Receiver para Web**.

Permitir a los usuarios descargar la aplicación Citrix Workspace para Windows o Mac

Si elige **Instalar localmente** o **Usar Receiver para HTML5 si el Receiver local no está disponible** y habilita **Permitir que los usuarios descarguen el plug-in de HDX Engine**, si la aplicación Workspace para HTML5 no detecta la aplicación Workspace instalada localmente, ofrece al usuario la opción de descargar la aplicación Citrix Workspace para Windows o Mac.

Actualizar la versión de la aplicación Workspace al iniciar sesión

Si selecciona **Actualizar el plug-in al iniciar sesión**, la aplicación Workspace para HTML5 ofrece a los usuarios la opción de actualizar la versión del cliente de la aplicación Citrix Workspace instalada localmente cuando inician sesión. Los usuarios pueden optar por omitir la actualización y no se les ofrecerá esta actualización a menos que se borren las cookies de su explorador web. Para habilitar esta función, asegúrese de que los archivos de la aplicación Citrix Workspace están disponibles en el servidor de StoreFront.

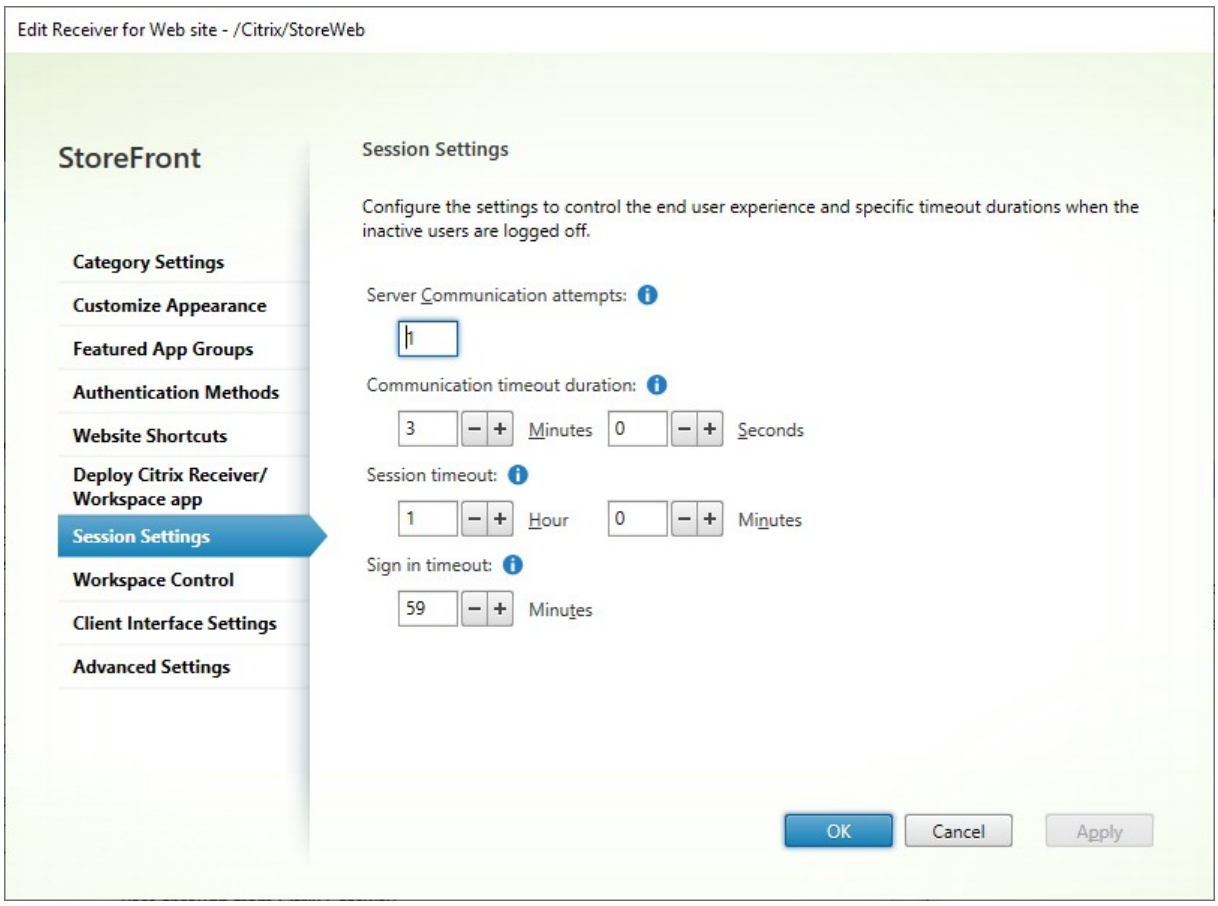
Descargar origen

Cuando los usuarios finales hacen clic en el botón de descarga, usted puede elegir si redirigirlos al sitio web de Citrix o si descargar los archivos directamente del servidor. Puede elegir **Sitio web de Citrix**, **Archivos locales en el servidor de StoreFront** o **Archivos en un servidor remoto (a través de una URL)**.

Configurar los parámetros de sesión

February 26, 2024

Para modificar la configuración de la sesión, vaya a la pantalla Modificar sitio de Receiver para Web y seleccione la ficha **Parámetros de sesión**.



Intentos de comunicación con los servidores

La cantidad de intentos de llamadas internas de StoreFront entre el proxy web y los servicios del almacén. Normalmente no es necesario modificar este parámetro.

Duración del tiempo de espera de las comunicaciones

La cantidad de tiempo permitido para las llamadas internas de StoreFront entre el proxy web y los servicios del almacén. Normalmente no es necesario modificar este parámetro.

Tiempo de espera por inactividad de la sesión

Al acceder a un almacén de StoreFront a través de un explorador web, después de un período de inactividad, el usuario ve el mensaje **La sesión agotó el tiempo de espera por inactividad.** Puede

cambiar el **Tiempo de espera de la sesión** para adaptarlo al patrón de uso de sus usuarios. Esto no afecta a las aplicaciones de Citrix Workspace.

Como alternativa, puede usar PowerShell. Por ejemplo, para establecer el tiempo de espera del sitio web "/Citrix/StoreWeb"en 30 minutos:

```
$rfw = Get-STFWebReceiverService '/Citrix/StoreWeb'
Set-STFWebReceiverService $rfw -SessionStateTimeout 30
<!--NeedCopy-->
```

Si modifica el tiempo de espera de la sesión para que sea superior a la Duración del token de autenticación o la Duración máxima del token, también se actualizan la duración del token de autenticación y la duración máxima del token para que coincidan.

Duración del token de autenticación

Cuando un usuario accede a un almacén de StoreFront a través de un explorador web, de forma predeterminada, se cierra la sesión del usuario después de ocho horas, independientemente de la actividad. Esto no afecta a las aplicaciones de Citrix Workspace. Para aumentar este tiempo de espera:

1. En StoreFront, vaya a **c:\inetpub\wwwroot\Citrix<StoreWeb>**.
2. Abra el`web.config` archivo.
3. Localice la entrada **`<authentication tokenLifeTime="08:00:00"method="Auto"/>`**
4. Cambie **`tokenLifeTime`** al valor pertinente. Para introducir un valor de 1 día o más, utilice el formato `d.h:m:s`.

Si aumenta el tiempo de espera de la sesión a más de 20 horas, también debe aumentar la Validez máxima del token del servicio de autenticación.

Validez máxima del token del servicio de autenticación

El servicio de autenticación emite tokens que se utilizan al conectarse a un almacén a través de un explorador web o de aplicaciones Citrix Workspace. Para las aplicaciones Citrix Workspace, este es el único tiempo de espera de inicio de sesión que debe actualizarse. Al acceder a StoreFront a través de un explorador web, este tiempo de espera se utiliza junto con los demás tiempos de espera. A diferencia de otros parámetros descritos en esta página, esto se aplica a todos los sitios web del almacén.

Al iniciar StoreFront con Citrix Gateway, Citrix Gateway tiene las credenciales de usuario y usa SSO en StoreFront. Si el token de StoreFront caduca, StoreFront emitirá un desafío de CitrixAG Basic, y Citrix Gateway proporcionará las credenciales para iniciar sesión en StoreFront. Por lo tanto, si también utiliza Citrix Gateway, también necesitará configurar su propio tiempo de espera de sesión.

1. Para la aplicación Citrix Workspace instalada en el servidor StoreFront, vaya a la ruta del servicio de autenticación de su almacén **`c:\inetpub\wwwroot\Citrix\<Store>Auth`** (que puede ser uno de los varios servicios de autenticación en función de la cantidad de almacenes que tenga).
2. En el archivo `web.config`, busque el servicio **Authentication Token Producer** y, dentro de él, busque el elemento `add` cuyo `id` coincida con el del **Authentication Token Producer**. En el siguiente ejemplo, necesitas el elemento `add` con `id="f7cac185-57c1-4629-a33c-88a89dd4295d"encipherId="2948f7ad-735e-4e03-8e01-8d4f5d3ca75b"`:

```
<service id="f7cac185-57c1-4629-a33c-88a89dd4295d" displayName="Authentication Token Producer">
    <relyingParties signingId="2948f7ad-735e-4e03-8e01-8d4f5d3ca75b" defaultLifetime="01:00:00" maxLifetime="01:00:00">
    <clear />
    <add id="f7cac185-57c1-4629-a33c-88a89dd4295d" encipherId="2948f7ad-735e-4e03-8e01-8d4f5d3ca75b" defaultLifetime="01:00:00" maxLifetime="20:00:00" />
<!--NeedCopy-->
```

3. Cambie **`maxLifetime`** al valor pertinente. El valor predeterminado es `20:00:00`. Para introducir un valor de 1 día o más, utilice el formato `dd.hh:mm:ss`.
4. Ejecute el comando **`iisreset`** para aplicar los cambios. La ejecución de este comando cierra la sesión de los usuarios de Citrix StoreFront Web, pero no afecta a su sesión ICA actual.

Control del espacio de trabajo

April 17, 2024

Cuando los usuarios se mueven entre los dispositivos, el control del espacio de trabajo garantiza que las aplicaciones que están usando sigan disponibles. Los usuarios pueden seguir trabajando con las mismas instancias de aplicaciones a través de varios dispositivos, en lugar de tener que reiniciar sus aplicaciones cada vez que inician sesión en un nuevo dispositivo. Esto permite, por ejemplo, que los médicos en los hospitales ahorren tiempo mientras se mueven de una estación de trabajo a otra para acceder a datos de los pacientes.

Cuando los usuarios inician sesión, vuelven a conectarse automáticamente a las aplicaciones que dejaron en ejecución. Por ejemplo, supongamos que un usuario inicia sesión en un almacén e inicia algunas aplicaciones. Si, a continuación, el usuario inicia sesión en el mismo almacén, con el mismo método de acceso, pero en otro dispositivo, las aplicaciones iniciadas se transfieren automáticamente al nuevo dispositivo. Todas las aplicaciones que el usuario inicia en un almacén específica se

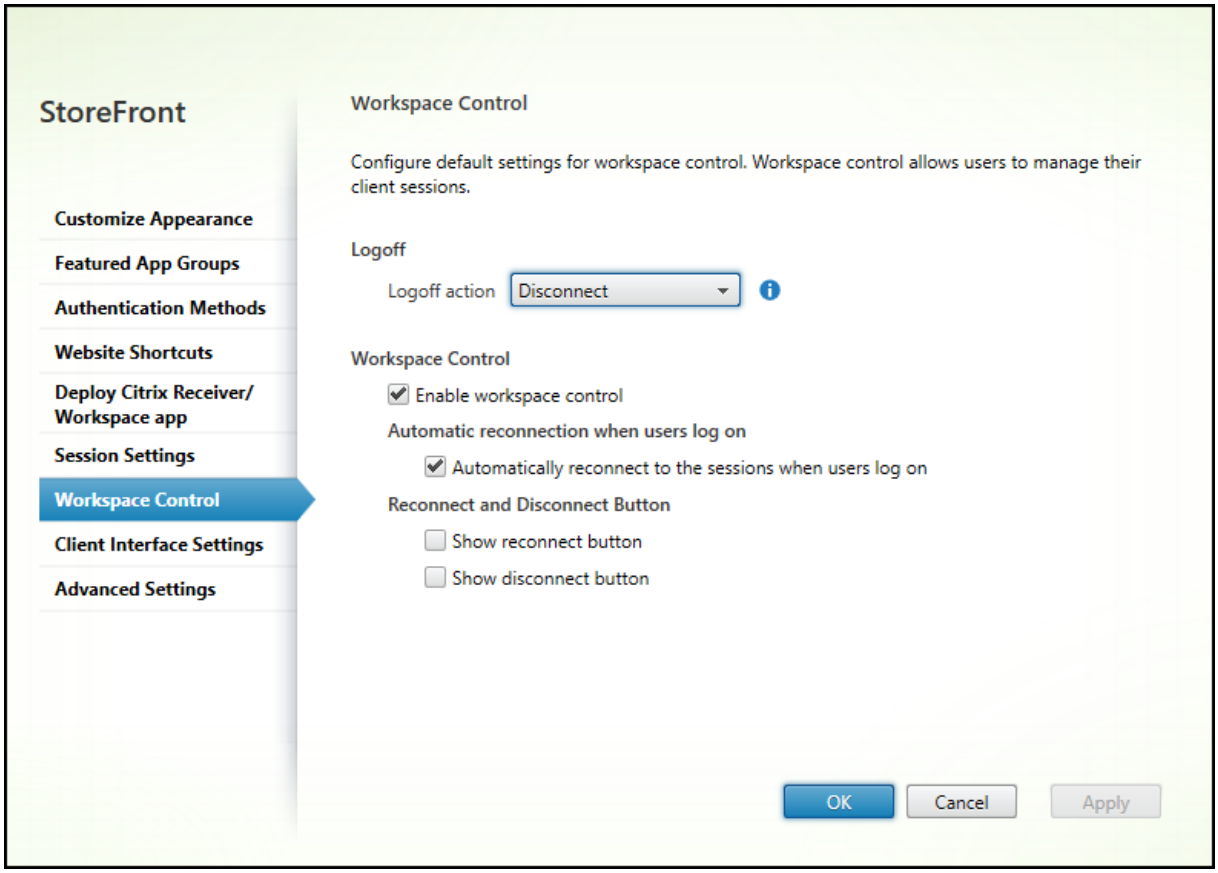
desconectan automáticamente (pero no se cierran) cuando el usuario cierra sesión en el almacén. En el caso de acceder a un almacén a través de un explorador web, se debe utilizar el mismo explorador web para iniciar sesión, iniciar las aplicaciones y cerrar sesión.

Configurar el control del espacio de trabajo en la aplicación Workspace para HTML5

Los parámetros de control del espacio de trabajo de la consola de administración de StoreFront solo se aplican al acceder al almacén a través de un explorador web. Esto está sujeto a los siguientes requisitos y restricciones:

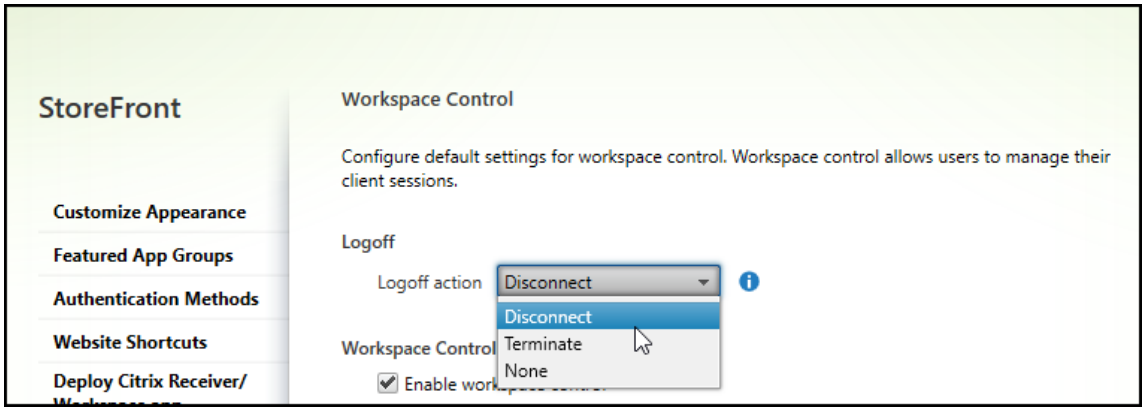
- El control del espacio de trabajo no está disponible cuando la aplicación Workspace para HTML5 se ejecuta en aplicaciones o escritorios alojados.
- Para los usuarios que acceden a sitios web desde dispositivos Windows, el control del espacio de trabajo solo se habilita si el sitio puede detectar que la aplicación Citrix Workspace para Windows se encuentra instalada en los dispositivos de los usuarios, o bien si se utiliza la aplicación Citrix Workspace para HTML5 para acceder a los recursos.
- Para poder reconectarse a aplicaciones desconectadas, los usuarios que acceden a sitios web a través de Internet Explorer deben agregar el sitio a las zonas de Intranet local o Sitios de confianza.
- Si solo hay un escritorio disponible para el usuario de un sitio web que está configurado con el objetivo de iniciar escritorios únicos automáticamente cuando el usuario inicia sesión, las aplicaciones de ese usuario no se vuelven a conectar, independientemente de la configuración del control del área de trabajo.
- Los usuarios deben desconectarse de las aplicaciones con el mismo explorador que utilizaron originalmente para iniciarlas. Los recursos que se iniciaron con otro explorador web o que se iniciaron de forma local desde el escritorio o desde el menú Inicio mediante la aplicación Citrix Workspace no pueden desconectarse ni cerrarse mediante Citrix Workspace app para HTML5.
- El control del espacio de trabajo no está disponible cuando los recursos se abren en la misma ficha del explorador. Para configurarlo, consulte Implementación de la aplicación Citrix Workspace.

Para modificar los parámetros de control del espacio de trabajo cuando se accede a un almacén a través de un explorador web, seleccione **Control del espacio de trabajo** en la pantalla Modificar sitio de Receiver para Web.



Configure los parámetros para el control del espacio de trabajo de la siguiente forma:

- Especifique la **acción Cerrar sesión**. Las acciones de cierre de sesión son las siguientes:
  - **Desconectar**: Cuando cierra sesión en el sitio, las sesiones de aplicaciones y escritorios se desconectan automáticamente del dispositivo cliente.
  - **Finalizar**: Cuando cierra sesión en el sitio, las sesiones de aplicaciones y escritorios finalizan automáticamente en el servidor.
  - **Ninguna**: Al cerrar sesión en el sitio, las sesiones de aplicaciones y escritorios siguen ejecutándose.



- Marque la casilla **Habilitar control del espacio de trabajo**.
- Seleccione la casilla **Reconectar automáticamente con las sesiones cuando los usuarios inician sesión** en **Reconexión automática cuando los usuarios inician una sesión**.

Configurar el control del espacio de trabajo con el SDK de PowerShell

Puede configurar el control del espacio de trabajo con el cmdlet de PowerShell Set-STFWebReceiverUserInterface.

Configurar el control del espacio de trabajo en la aplicación Workspace para Windows

Para configurar el control del espacio de trabajo en Workspace para Windows, consulte Administrar la reconexión del control del espacio de trabajo.

Configurar el control del espacio de trabajo en la aplicación Workspace para Mac

Para configurar el control del espacio de trabajo en la aplicación Workspace para Mac, consulte Configurar los parámetros del control del espacio de trabajo.

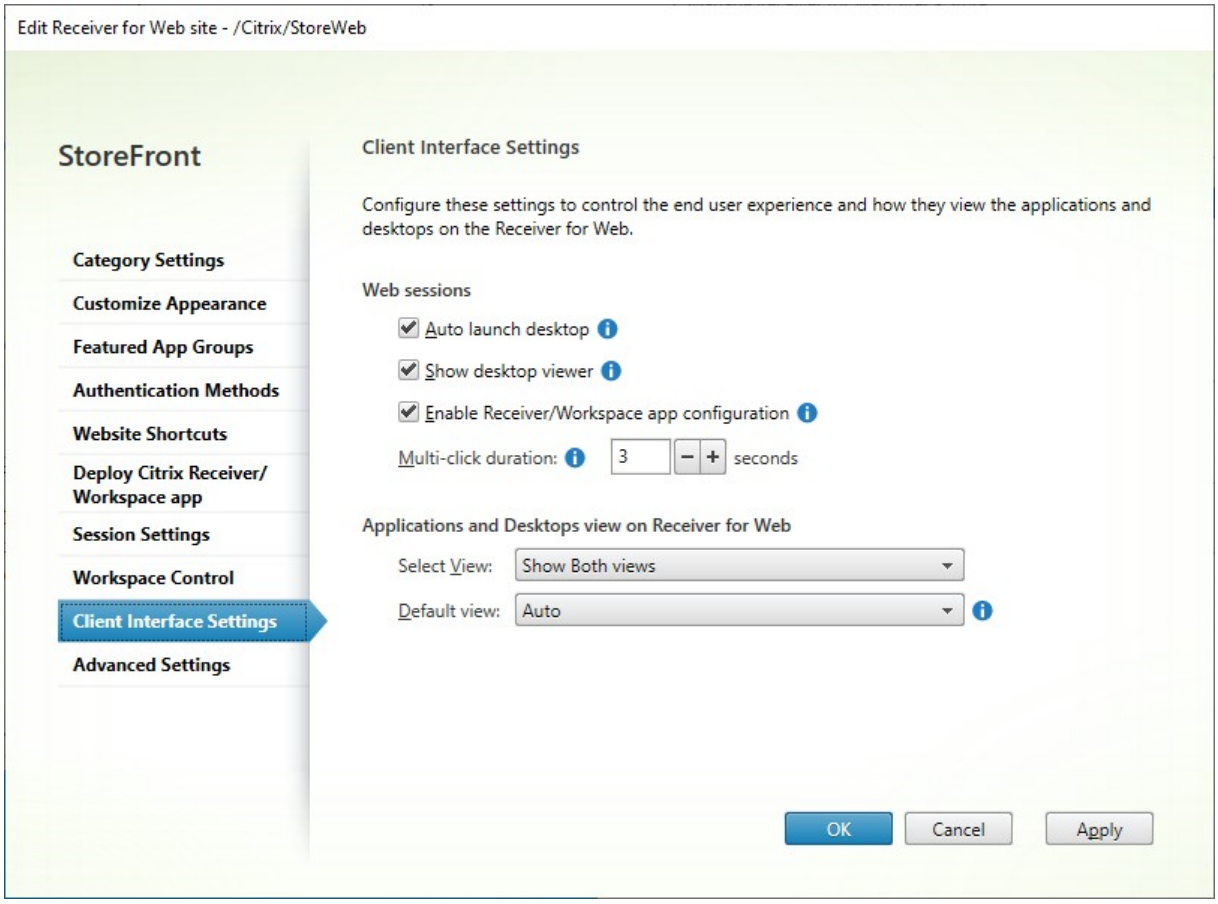
Inhabilitar el control del espacio de trabajo en todas las aplicaciones

Para inhabilitar la reconexión de sesiones en StoreFront en todas las aplicaciones Workspace independientemente de cómo estén configuradas, vaya a la ficha **Parámetros avanzados** y desmarque **Permitir la reconexión de sesiones**.

Parámetros de interfaz del cliente

February 26, 2024

Para modificar parámetros de la interfaz del cliente desde la pantalla Modificar sitio de Receiver para Web, seleccione la ficha **Parámetros de la interfaz del cliente**.



Inicio automático del escritorio

Si este parámetro está habilitada y el usuario solo tiene un escritorio, el escritorio se inicia cuando el usuario inicia sesión.

Para usar el SDK de PowerShell para cambiar el parámetro de inicio automático de escritorios, llame al cmdlet Set-STFWebReceiverUserInterface con el parámetro `AutoLaunchDesktop`.

Este parámetro solo se aplica a la aplicación Citrix Workspace para HTML5. No se aplica a las aplicaciones Citrix Workspace instaladas localmente.

Mostrar Desktop Viewer

Desktop Viewer es la barra de herramientas que proporciona un fácil acceso a las preferencias de HDX. Use este parámetro para elegir si se mostrará o no.

Este parámetro solo se aplica a la aplicación Citrix Workspace para HTML5. No se aplica a las aplicaciones Citrix Workspace instaladas localmente.

Duración de clics múltiples

Impide que los usuarios inicien la misma aplicación varias veces durante el tiempo configurado. Esto solo se aplica a la aplicación Citrix Workspace para HTML5 y no a la aplicación Citrix Workspace nativa.

Para usar el SDK de PowerShell con el fin de cambiar la duración de clics múltiples, llame al cmdlet Set-STFWebReceiverUserInterface con el parámetro `MultiClickTimeout`.

Este parámetro solo se aplica a la aplicación Citrix Workspace para HTML5. No se aplica a las aplicaciones Citrix Workspace instaladas localmente.

Habilitar configuración de la aplicación Workspace/Receiver

Si se marca, la aplicación Citrix Workspace para HTML5 ofrece archivos de aprovisionamiento que permiten a los usuarios configurar automáticamente la aplicación Citrix Workspace nativa para el almacén asociado. Los archivos de aprovisionamiento contienen los datos de conexión para el almacén que proporciona los recursos en el sitio, incluidos los detalles de las implementaciones de Citrix Gateway y las balizas configuradas para el almacén.

Para usar el SDK de PowerShell para cambiar esta opción, llame al cmdlet Set-STFWebReceiverUserInterface con el parámetro `ReceiverConfigurationEnabled`.

Vista de aplicaciones y escritorios

Cuando hay escritorios y aplicaciones disponibles, la aplicación Citrix Workspace muestra vistas separadas para los escritorios y las aplicaciones de forma predeterminada. Los favoritos se muestran en la vista de **Inicio**. Lo primero que ven los usuarios es la vista de **Inicio** al iniciar sesión en el sitio.

En la lista desplegable **Seleccionar vista**, seleccione si mostrar aplicaciones, escritorios o ambos.

En la lista desplegable **Vista predeterminada**, seleccione la vista que se mostrará cuando el usuario inicie sesión.

Opción	Descripción
Auto (Automático)	Mostrar la vista Inicio
Aplicaciones	Mostrar la vista Aplicaciones
Escritorios	Mostrar la vista Escritorios

Para usar el SDK de PowerShell con el fin de cambiar estas opciones, llame al cmdlet Set-STFWebReceiverUserInterface con los parámetros `ShowAppsView`, `ShowDesktopsView` y `DefaultView`.

App Protection

December 4, 2023

App Protection proporciona un nivel de seguridad adicional al bloquear el registro de tecleo y las capturas de pantalla. Para obtener más información, consulte la documentación de App Protection.

Aplicación Workspace

App Protection está disponible de forma predeterminada al acceder a un almacén a través de las aplicaciones de Citrix Workspace para Windows, Mac y Linux.

App Protection para el inicio híbrido

Al acceder a un almacén a través de un explorador web, las aplicaciones que requieren App Protection se ocultan de forma predeterminada. StoreFront se puede configurar para que muestre las aplicaciones protegidas cuando detecte las siguientes versiones mínimas de la aplicación Citrix Workspace:

Aplicación	Versión
Aplicación Citrix Workspace para Windows	1912
Aplicación Citrix Workspace para Mac	2001
Aplicación Citrix Workspace para Linux	2108

StoreFront no muestra aplicaciones protegidas cuando se usan versiones anteriores de la aplicación Workspace, o bien en iOS, Android o Chrome OS, ni cuando se inician aplicaciones en el explorador web mediante Citrix Workspace para HTML5.

Para permitir que StoreFront muestre aplicaciones protegidas en versiones compatibles de Workspace, use el cmdlet Set-STFWebReceiverAppProtection del SDK de PowerShell.

Si el usuario eligió iniciar aplicaciones de Workspace a través de un explorador web (ya sea mediante la configuración de administrador o porque el usuario eligió usar **Workspace lite**), App Protection no está disponible. Puede configurar el almacén para que se inicie siempre mediante la aplicación Workspace; consulte Implementación de la aplicación Citrix Workspace.

StoreFront determina la versión de la aplicación Citrix Workspace mediante la extensión web de Citrix Workspace si está disponible y configurada (consulte Detección de clientes basada en extensiones de explorador web). De lo contrario, StoreFront determina la versión de la aplicación Workspace como

parte de la detección de clientes la primera vez que el usuario visita el sitio web del almacén. Si el usuario omite la detección y selecciona **Ya instalado**, StoreFront no podrá determinar la versión de la aplicación y, por lo tanto, no mostrará las aplicaciones protegidas.

> **Advertencia**
>
> Si la extensión web de Citrix Workspace no está disponible, StoreFront determina la versión de la aplicación Citrix Workspace la primera vez que el usuario visita el sitio web. Si el usuario instala posteriormente una versión diferente de la aplicación Workspace, StoreFront no se dará cuenta del cambio y, por lo tanto, podría permitir o impedir el inicio de aplicaciones protegidas de forma incorrecta. Citrix recomienda configurar la verificación de la postura de App Protection, que bloquea el inicio de aplicaciones y escritorios virtuales desde versiones de la aplicación Citrix Workspace que no admiten App Protection.

Quitar un sitio web

August 15, 2023

1. Seleccione el nodo **Almacenes** en el panel izquierdo de la consola de administración de Citrix StoreFront, seleccione el almacén para la que quiere crear el sitio de Citrix Receiver para Web y haga clic en **Administrar sitios de Receiver para Web**, en el panel **Acciones**.
2. Seleccione un sitio y haga clic en **Quitar**. Al quitar un sitio, los usuarios ya no pueden usar esa página web para acceder al almacén.

Configurar el sitio web de la aplicación Workspace

August 15, 2023

Al crear un almacén mediante StoreFront, también se crea automáticamente un sitio web y se asocia a dicho almacén. Cuando un almacén tiene varios sitios web, seleccione qué sitio web se muestra cuando los usuarios acceden al almacén mediante la aplicación Citrix Workspace.

1. Seleccione el nodo **Almacenes** en el panel izquierdo de la consola de administración de Citrix StoreFront.
2. Seleccione un almacén en el panel central y haga clic en **Configurar la experiencia unificada** en el panel **Acciones**. Si no dispone de un sitio web creado de Citrix Receiver para Web, aparecerá un mensaje con un enlace al asistente para agregar un sitio de Receiver para Web.

3. Seleccione el sitio web que quiere que los clientes de la aplicación Citrix Workspace muestren cuando los usuarios accedan a este almacén.
4. Haga clic en **Aceptar**.

Configurar grupos de servidores

April 17, 2024

Las tareas siguientes permiten modificar los parámetros de las implementaciones de StoreFront con varios servidores. Para administrar implementaciones con varios servidores, use solo un servidor a la vez para realizar cambios en la configuración del grupo de servidores. Compruebe que la consola de administración de Citrix StoreFront no se está ejecutando en ninguno de los demás servidores de la implementación. Cualquier cambio de configuración realizado debe propagarse a los demás servidores para garantizar una configuración coherente en toda la implementación.

Los servidores incluidos en un grupo de servidores de StoreFront deben estar todos configurados idénticamente, en términos de ubicación de la instalación de StoreFront y parámetros del sitio web IIS, tales como la ruta física y el ID del sitio.

Agregar un servidor a un grupo de servidores

Utilice la tarea Agregar servidor para obtener un código de autorización que le permita unir un servidor de StoreFront recién instalado a la implementación existente. Para obtener más información acerca de la incorporación de nuevos servidores a las implementaciones ya existentes de StoreFront, consulte Unirse a un grupo de servidores existente. Consulte el apartado *Escalabilidad* incluido en Planificar una implementación de StoreFront para evaluar la cantidad necesaria de servidores en el grupo.

Eliminar servidores de un grupo de servidores

Utilice la tarea **Quitar servidor** para quitar servidores de una implementación de StoreFront con varios servidores. Puede quitar cualquier servidor del grupo, excepto el servidor en el que ejecuta la tarea. Antes de quitar un servidor de una implementación con varios servidores, primero quite el servidor del entorno de equilibrio de carga.

Para poder volver a agregar un servidor de StoreFront eliminado anteriormente, ya sea al mismo grupo de servidores o a otro, debe restablecerlo al estado predeterminado de fábrica. Consulte Restablecer un servidor a los valores predeterminados de fábrica.

Propagar cambios locales en un grupo de servidores

Utilice la tarea Propagar cambios para actualizar la configuración de todos los demás servidores de una implementación de StoreFront con varios servidores de modo que coincida con la configuración del servidor actual. La propagación de la información de configuración se inicia manualmente para que pueda mantener el control sobre si quiere y el momento en que quiere actualizar los servidores del grupo con los cambios de configuración. Mientras ejecuta esta tarea, no puede realizar cambios adicionales hasta que todos los servidores del grupo se hayan actualizado.

> **Importante:**
>
> Los cambios realizados en otros servidores del grupo se descartan durante la propagación. Si actualiza la configuración de un servidor, propague los cambios a los demás servidores del grupo para evitar que se pierdan si posteriormente propaga cambios desde otro servidor de la implementación.

La información propagada entre servidores del grupo incluye lo siguiente:

- Contenido de todos los archivos web.config, que contienen la configuración de StoreFront.
- Contenido de `C:\Program Files\Citrix\Receiver StoreFront\Receiver Clients`, como `C:\Program Files\Citrix\Receiver StoreFront\Receiver Clients\Windows\CitrixWorkspaceAppWeb.exe` y `C:\Program Files\Citrix\Receiver StoreFront\Receiver Clients\MAC\CitrixWorkspaceAppWeb.dmg`.
- Contenido de `C:\inetpub\wwwroot\Citrix\StoreWeb\Custom\contrib`.
- Contenido de `C:\inetpub\wwwroot\Citrix\StoreWeb\Custom\custom folder`, como imágenes copiadas y archivos .js de personalización.
- Contenido del almacén de certificados de Citrix Delivery Services, excepto las listas de revocación de certificados (CRL) importadas manualmente. (Para obtener información detallada sobre la distribución de listas de revocación de certificados locales, consulte Comprobación de listas de revocación de certificados (CRL).

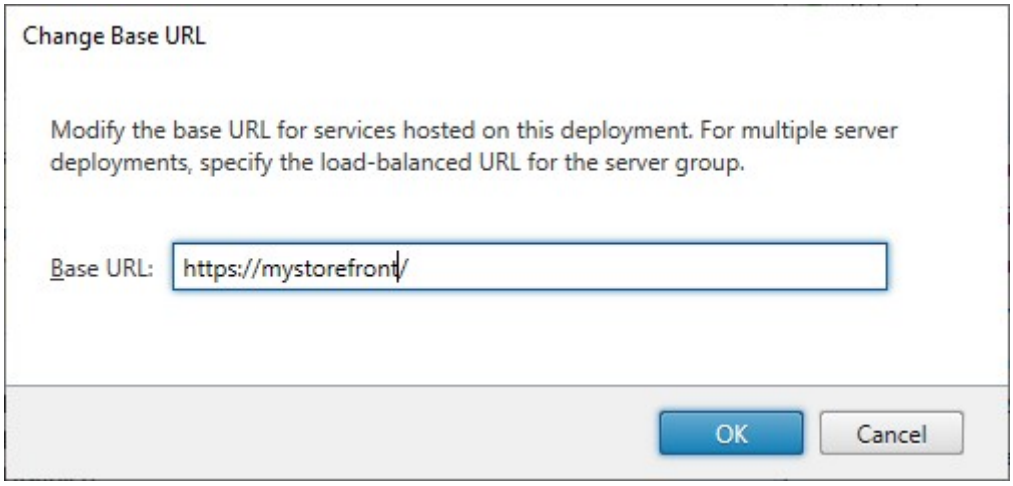
> **Nota:**
>
> Los datos de suscripción se sincronizan con los demás servidores, independientemente del mecanismo de propagación de cambios. Se produce automáticamente sin que se inicie la tarea Propagar cambios.

Cambiar la dirección URL base de una implementación

La URL base se usa como raíz de las URL de almacenes y otros servicios de StoreFront alojados en una implementación. Para las implementaciones con varios servidores, especifique la dirección URL con equilibrio de carga.

Para cambiar la URL base:

1. En el panel de la izquierda de la consola de administración de Citrix StoreFront, seleccione el nodo **Grupo de servidores**.
2. En el panel de acciones, haga clic en **Cambiar URL base…**
3. Introduzca la nueva URL.
4. Presione **OK**.



Integrar en Citrix Gateway y NetScaler ADC

April 17, 2024

Puede utilizar Citrix Gateway con StoreFront para ofrecer acceso remoto seguro a usuarios que se encuentren fuera de la red de la empresa. Asimismo, puede utilizar NetScaler ADC para equilibrar la carga.

Tarea	Detalles
Agregar una instancia de Citrix Gateway	Agregue una puerta de enlace a su dispositivo NetScaler y configúrela en StoreFront.
Importar un dispositivo Citrix Gateway	Exportar la configuración de su dispositivo Citrix Gateway e importarla en StoreFront
Administrar dispositivos Citrix Gateway	Agregar, quitar y modificar parámetros de conexión de Citrix Gateway
Equilibrar la carga con NetScaler ADC	Configurar NetScaler ADC como equilibrador de carga frente a un grupo de servidores de StoreFront

Tarea	Detalles
Configurar NetScaler ADC y StoreFront para la autenticación con formularios delegada (DFA)	
Autenticarse con dominios distintos	Configure StoreFront y Citrix Gateway para que los usuarios se autentiquen primero con la puerta de enlace en un dominio y, a continuación, en StoreFront en otro dominio.
Configurar balizas	Configure las URL de baliza que la aplicación Citrix Workspace pueda usar para determinar si está dentro o fuera de su red corporativa.
Crear un único nombre de dominio completo (FQDN) para acceder a un almacén de forma interna y externa	Cree un nombre de dominio completo (FQDN) único que pueda acceder a un almacén directamente desde su red corporativa y de forma remota a través del dispositivo Citrix Gateway.

Configurar Citrix Gateway

February 26, 2024

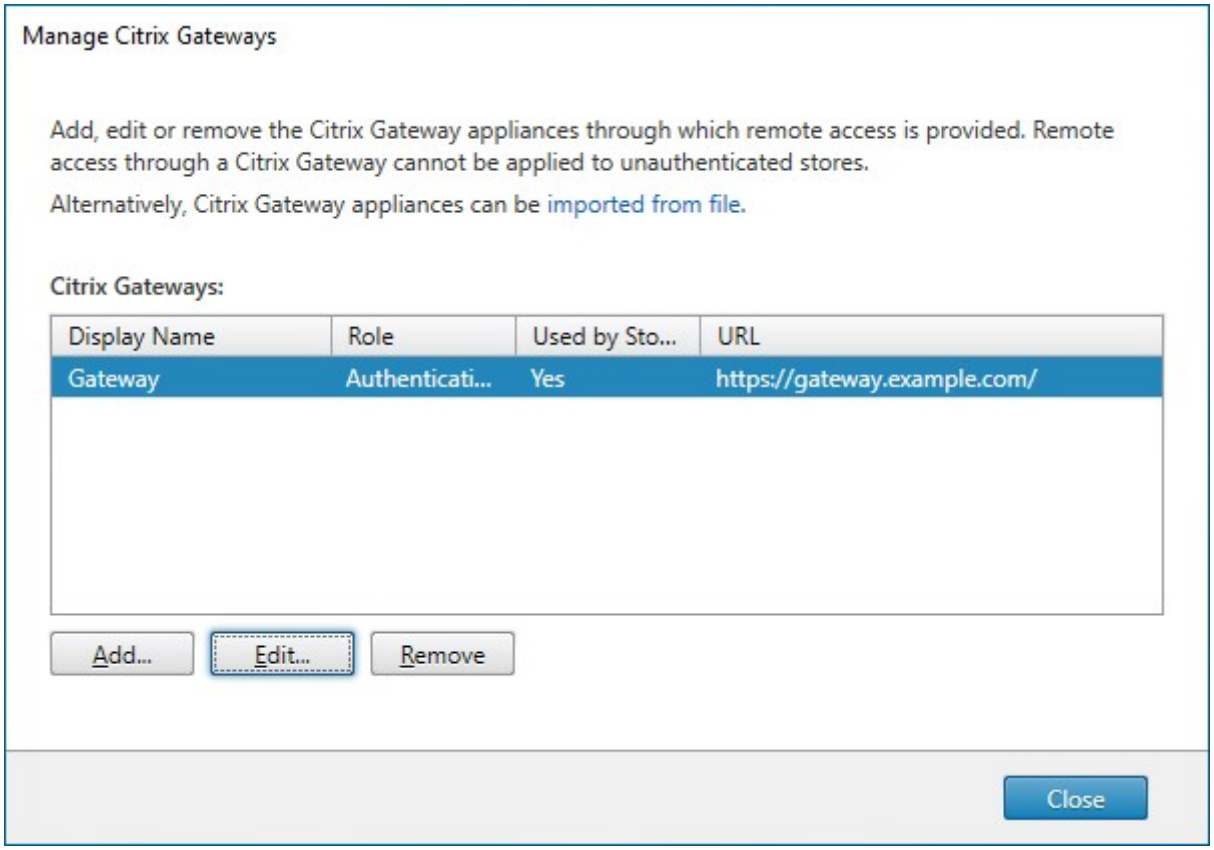
Use dispositivos Citrix Gateway para proporcionar acceso remoto a StoreFront. Los Citrix Gateway se ejecutan en un dispositivo NetScaler ADC o NetScaler Gateway de hardware o software.

Para obtener más información sobre la configuración del Gateway, consulte Integrar NetScaler Gateway con StoreFront.

Debe configurar la puerta de enlace en StoreFront para que StoreFront permita el acceso a través de esa puerta de enlace.

Ver dispositivos Gateway

Para ver las puertas de enlace configuradas en StoreFront, seleccione el nodo Almacenes en el panel izquierdo de la consola y el panel de administración de Citrix StoreFront y haga clic en **Administrar dispositivos Citrix Gateway**. Se muestra la ventana **Administrar dispositivos Citrix Gateway**.



PowerShell

Para obtener una lista de dispositivos Gateway y su configuración, llame a Get-STFRoamingGateway.

Agregar Citrix Gateway

> **Importante:**
>
> En implementaciones con varios servidores, use solo un servidor a la vez para hacer cambios en la configuración del grupo de servidores. Compruebe que la consola de administración de Citrix StoreFront no se está ejecutando en ninguno de los demás servidores de la implementación. Una vez completados, propague los cambios de configuración al grupo de servidores de modo que los demás servidores de la implementación se actualicen.

1. En la ventana **Administrar dispositivos Citrix Gateway**, haga clic en **Agregar**.
2. En la ficha Parámetros generales, introduzca los parámetros y, a continuación, presione **Siguiente**.
   - Especifique un **nombre simplificado** para la implementación de Citrix Gateway que ayude a los usuarios a identificarla.

Los usuarios verán el nombre simplificado que especifique en la aplicación Citrix Workspace, de modo que debe incluir la información relevante en el nombre para ayudarlos a decidir si utilizar esa implementación o no. Por ejemplo: puede incluir la ubicación geográfica en los nombres simplificados para las implementaciones de Citrix Gateway, de modo que los usuarios puedan identificar fácilmente la implementación más conveniente en función de su ubicación.

- Introduzca la URL de la puerta de enlace.

  El nombre de dominio completo (FQDN) de la implementación de StoreFront debe ser único y diferente del FQDN del servidor virtual de Citrix Gateway. No se admite el uso de un mismo FQDN para StoreFront y para el servidor virtual de Citrix Gateway. La puerta de enlace agrega la URL al encabezado HTTP `X-Citrix-Via`. StoreFront usa este encabezado para determinar qué puerta de enlace se está usando.

  Con la GUI solo es posible agregar una única URL de puerta de enlace. Si se puede acceder a una puerta de enlace mediante varias URL, debe agregar la misma puerta de enlace dos veces con la misma configuración, aparte de la URL. Para simplificar la configuración, puede configurar una URL secundaria que se utilice para acceder a la puerta de enlace. Esta opción no está disponible mediante la GUI, por lo que debe configurarla con PowerShell. Debe cerrar la consola de administración antes de ejecutar comandos de PowerShell. Por ejemplo, si tiene varias puertas de enlace detrás de un equilibrador de carga de servidor global, normalmente es útil agregar tanto la URL del GSLB como una URL que se pueda usar para acceder a cada puerta de enlace regional específica, como, por ejemplo, con fines de prueba o para solucionar problemas. Una vez que haya creado la puerta de enlace `Set-STFRoamingGateway`, puede agregar una URL adicional con el parámetro `-GSLBurl` de la URL secundaria. Aunque se llama al parámetro `GSLBurl`, puede usarse para cualquier situación en la que quiera agregar una segunda URL. Por ejemplo:

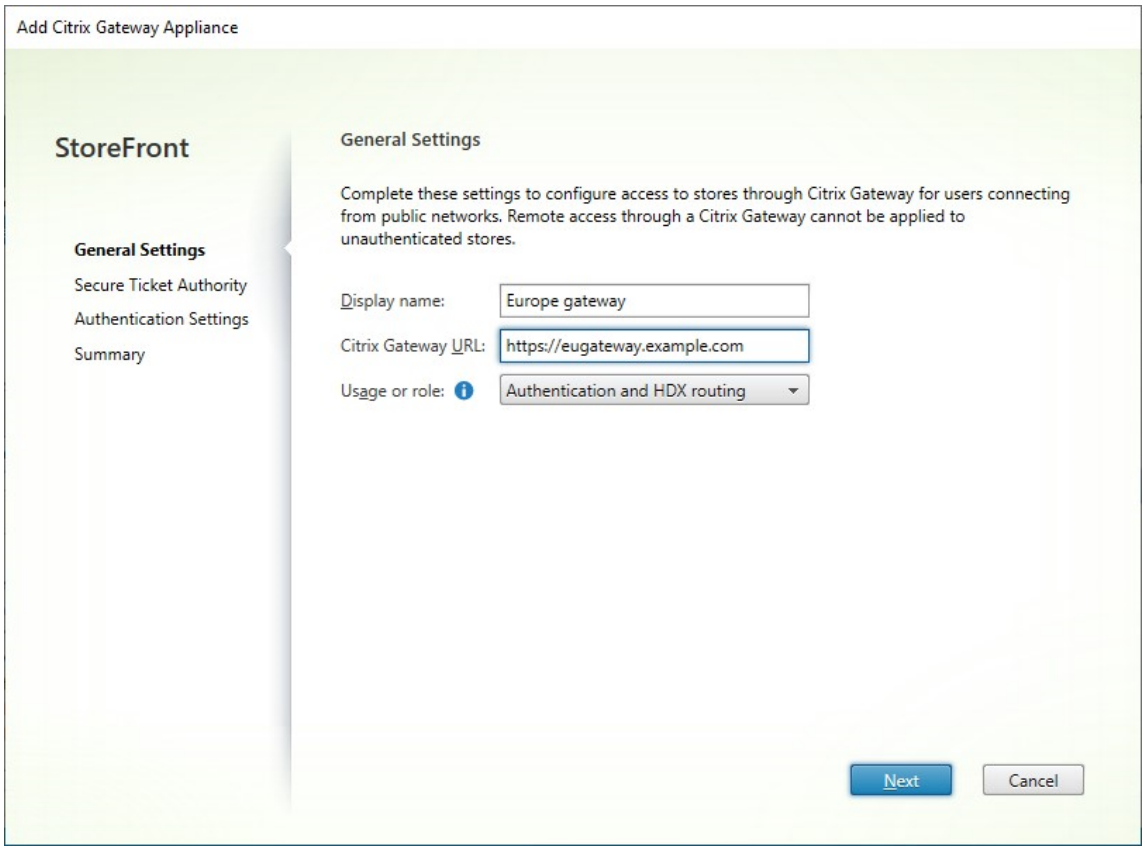
```
1  Set-STFRoamingGateway -Name "Europe Gateway" -GSLBurl "
       eugateway.example.com" -GatewayUrl "gslb.example.com"
2 <!--NeedCopy-->
```

> Nota:
>
> Aunque no sea intuitivo, en este ejemplo, el parámetro `GSLBurl` contiene la URL regional, mientras que el parámetro `GatewayUrl` contiene la URL del GSLB. Para la mayoría de los casos, las URL se tratan de manera idéntica y, si solo se accede al almacén a través de un explorador web, se pueden configurar de cualquiera de las dos maneras. Sin embargo, al acceder a StoreFront a través de la aplicación Citrix Workspace, este lee las `GatewayUrl` de StoreFront y, posteriormente, las usa para el acceso remoto, por lo que es preferible configurarlo para que siempre se conecte a la URL del GSLB.

Si necesita más de dos URL, tendrá que configurarlo como una puerta de enlace independiente.

- Seleccione el uso o el rol:

Uso o rol	Descripción
Autenticación y redirección de HDX	Use el dispositivo Gateway tanto para proporcionar acceso remoto a StoreFront como para acceder a los VDA.
Solo autenticación	Seleccione esta opción si la puerta de enlace se usa solo para el acceso remoto a StoreFront.
Solo redirección de HDX	Seleccione esta opción si la puerta de enlace se usa solo para proporcionar acceso HDX a los VDA, como, por ejemplo, en un sitio que no tiene ninguna instancia de StoreFront.



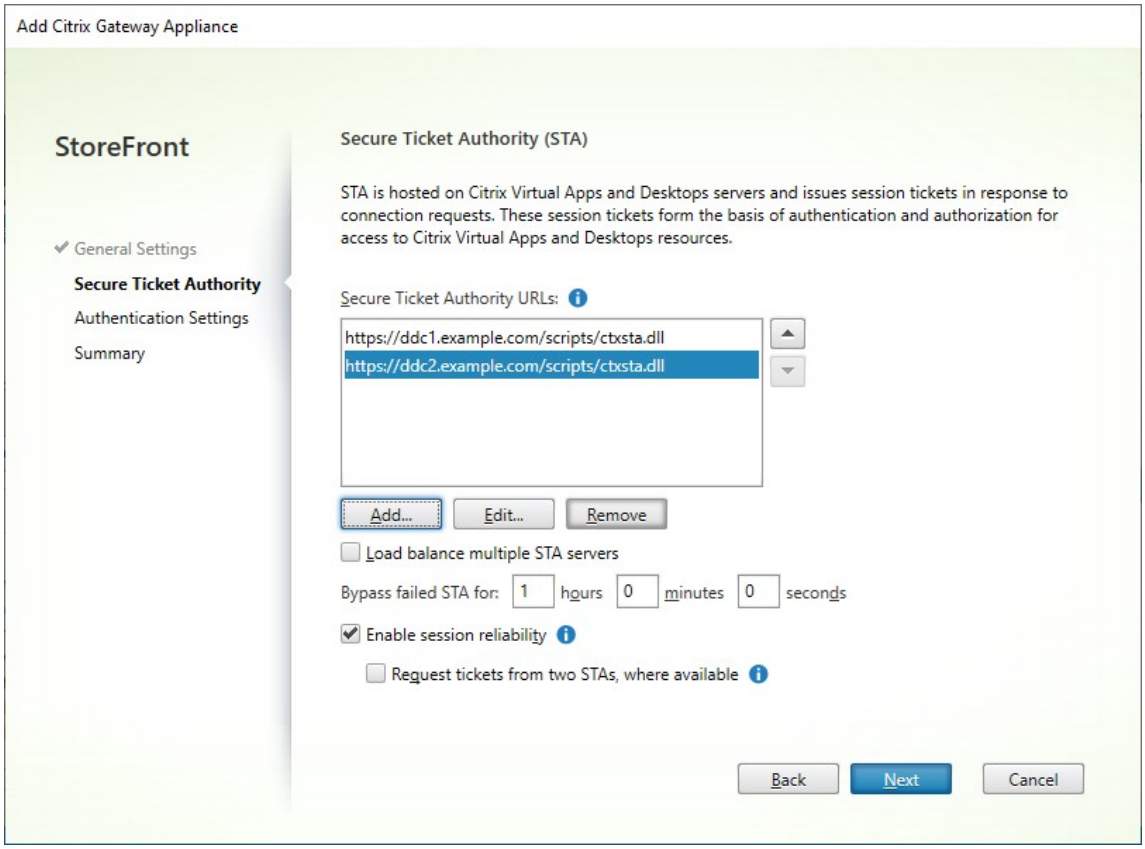
3. Rellene los parámetros en la ficha **Secure Ticketing Authority**.

   Secure Ticketing Authority emite tíquets de sesión en respuesta a solicitudes de conexión. Esos tíquets de sesión forman la base de la autenticación y la autorización para acceder a los recursos

de Citrix Virtual Apps and Desktops.

- Introduzca al menos una URL de servidor de Secure Ticket Authority. Si usa Citrix Virtual Apps and Desktops, puede usar el Delivery Controller como STA. Si utiliza Citrix Desktop as a Service, puede introducir los Cloud Connectors, que envían por proxy las solicitudes a la autoridad de emisión de tíquets de Citrix Cloud. Las entradas de esta lista deben coincidir exactamente con las de la lista configurada en Citrix Gateway.
- Marque **Equilibrar la carga de varios servidores STA** para distribuir las solicitudes entre los servidores STA. Si la opción está desmarcada, StoreFront probará los servidores en el orden en que aparecen en la lista.
- Si StoreFront no puede acceder a un servidor STA, evita usar ese servidor durante un período de tiempo. De forma predeterminada, lo evita durante 1 hora, pero se puede personalizar este valor.
- Si quiere que Citrix Virtual Apps and Desktops mantenga abiertas las sesiones desconectadas mientras la aplicación Citrix Workspace intenta volver a conectarse automáticamente, marque la casilla Habilitar fiabilidad de la sesión. Si configuró varios STA y quiere asegurarse de que la fiabilidad de la sesión esté siempre disponible, seleccione la casilla **Solicitar tíquets de dos STA, si están disponibles**.

  Cuando la casilla Solicitar tíquets de dos STA, si están disponibles está seleccionada, StoreFront obtiene tíquets de sesión de dos STA diferentes con el fin de que las sesiones de usuario no se interrumpan si un STA no está disponible durante el curso de la sesión. Si, por algún motivo, StoreFront no puede establecer contacto con dos STA, vuelve a utilizar un solo STA.



Una vez que haya rellenado los parámetros, presione **Siguiente**.

4. Rellene los parámetros en la ficha **Parámetros de autenticación**.

   - Elija la versión de NetScaler.
   - Si hay varias puertas de enlace con la misma URL (normalmente, cuando se utiliza un equilibrador de carga de servidor global) y ha introducido una URL de respuesta, debe introducir la VIP de la puerta de enlace. Esto permite a StoreFront determinar de qué puerta de enlace proviene la solicitud y, por lo tanto, con qué servidor contactar mediante la URL de respuesta. De lo contrario, puede dejar este parámetro vacío.
   - En la lista **Tipo de inicio de sesión**, seleccione el método de autenticación configurado en el dispositivo para los usuarios de la aplicación Citrix Workspace.

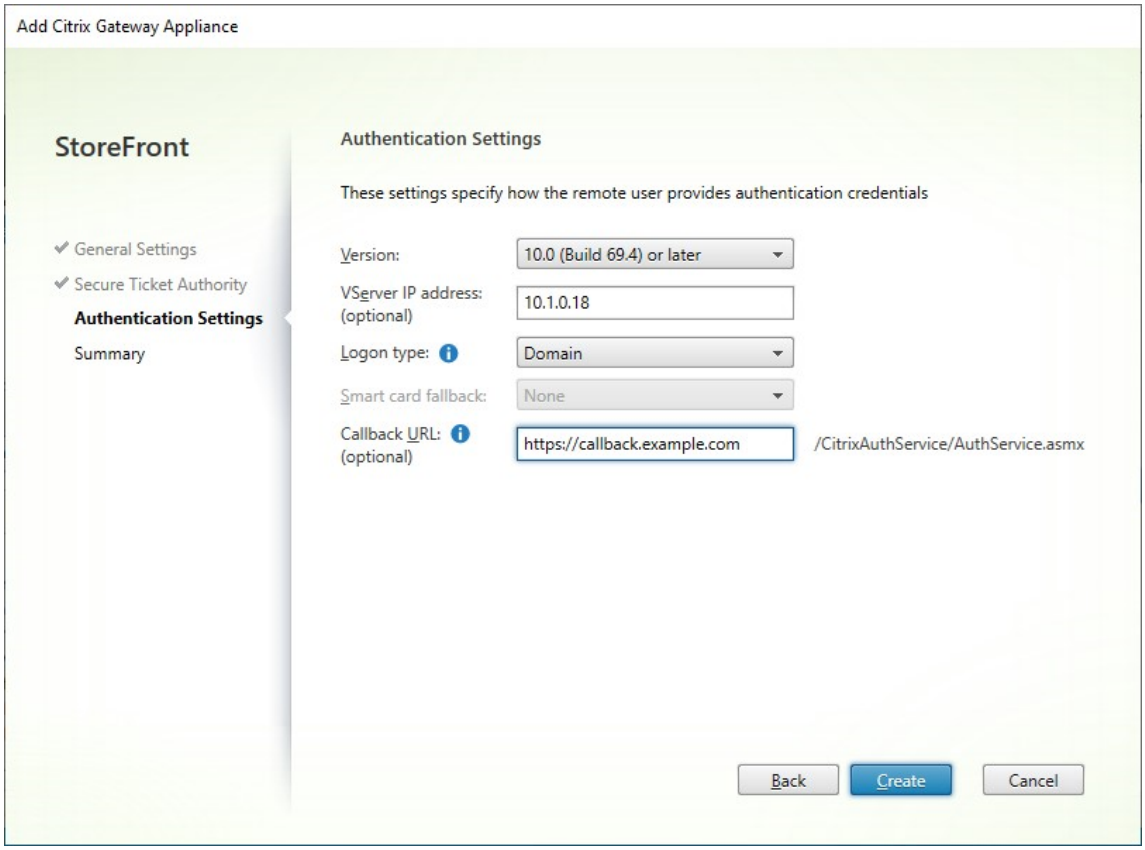
   La información que proporcione sobre la configuración de su dispositivo Citrix Gateway se agrega al archivo de aprovisionamiento para el almacén. Eso permite que la aplicación Citrix Workspace envíe la solicitud de conexión pertinente al comunicarse con el dispositivo por primera vez.

   - Si es necesario que los usuarios introduzcan sus credenciales de dominio de Microsoft Active Directory, seleccione Dominio.

- Si es necesario que los usuarios introduzcan un código de token obtenido de un token de seguridad, seleccione Token de seguridad.
- Si es necesario que los usuarios introduzcan sus credenciales de dominio y un código de token obtenido de un token de seguridad, seleccione Dominio y token de seguridad.
- Si es necesario que los usuarios introduzcan una contraseña de un solo uso enviada por mensaje de texto, seleccione Autenticación por SMS.
- Si es necesario que los usuarios presenten una tarjeta inteligente e introduzcan un PIN, seleccione Tarjeta inteligente.

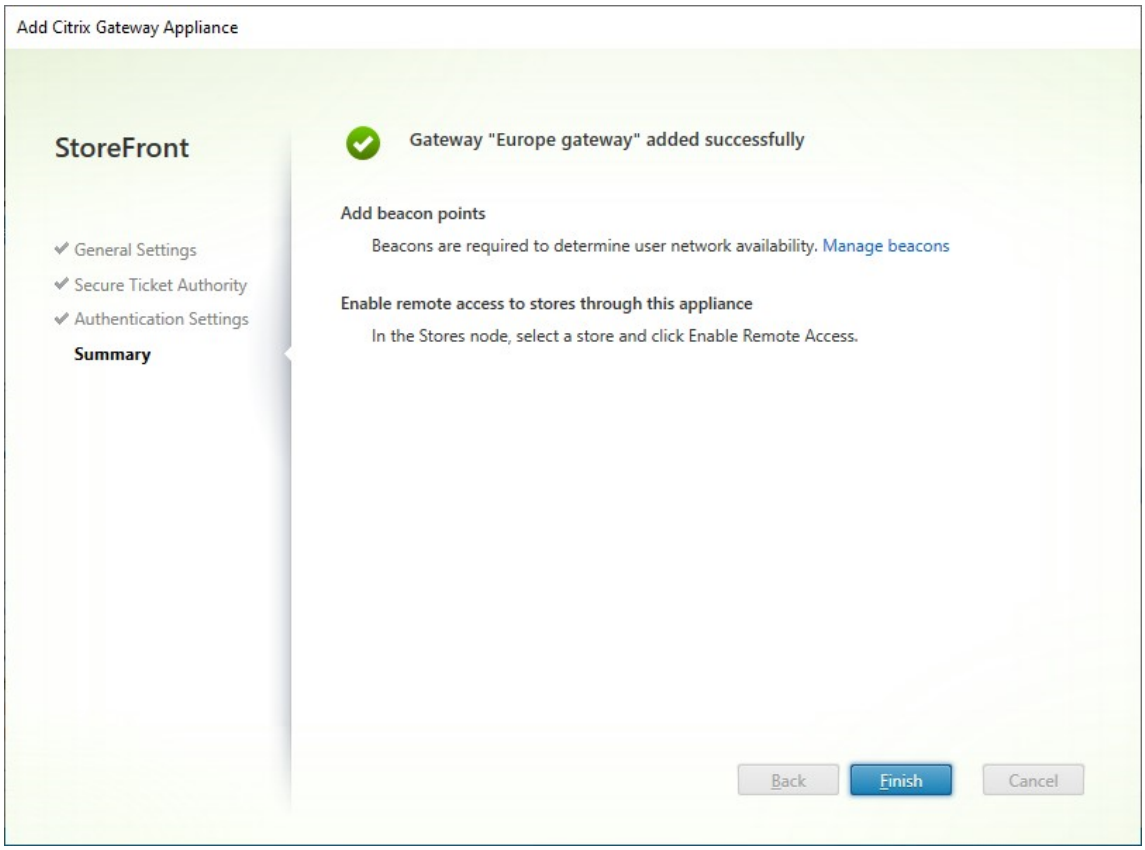
Si configura la autenticación con tarjeta inteligente con un método secundario de autenticación (al que los usuarios puedan recurrir en caso de tener problemas con su tarjeta inteligente), seleccione el método secundario de autenticación en la lista Alternativa a tarjeta inteligente.

- Si quiere, introduzca la URL de acceso interno de la puerta de enlace en el cuadro URL de respuesta. Esto permite que StoreFront contacte con el servicio de autenticación de Citrix Gateway para verificar que las solicitudes recibidas desde Citrix Gateway provienen de ese dispositivo. Es necesario para el acceso inteligente y para los casos de autenticación sin contraseña, como una tarjeta inteligente o SAML; de lo contrario, puede dejarlo vacío. Si tiene varios dispositivos Citrix Gateway con la misma URL, esta URL debe ser para el servidor de Gateway específico.



Una vez que haya rellenado los parámetros, presione **Siguiente**.

5. Haga clic en **Crear** para aplicar la configuración.



6. Una vez que la implementación se haya aplicado, haga clic en **Finalizar**.
7. Para permitir que los usuarios accedan a sus almacenes a través de Citrix Gateway, configure el acceso de usuarios remotos.

SDK de PowerShell

Para agregar un dispositivo Gateway mediante el SDK de PowerShell, llame al cmdlet New-STFRoamingGateway.

Modificar Citrix Gateway

1. En la ventana **Administrar dispositivos Citrix Gateway**, haga clic en la puerta de enlace que quiera cambiar y presione **Modificar**.

   Para obtener una descripción de los parámetros, consulte Agregar Citrix Gateway.

2. Presione **Guardar** para guardar los cambios.

SDK de PowerShell

Para modificar la configuración del dispositivo Gateway mediante el SDK de PowerShell, llame al cmdlet Set-STFRoamingGateway.

Quitar Citrix Gateway

1. En la ventana **Administrar dispositivos Citrix Gateway**, haga clic en la puerta de enlace que quiera cambiar y presione **Quitar**.
2. En la ventana de confirmación, presione **Sí**.

SDK de PowerShell

Para quitar la puerta de enlace mediante el SDK de PowerShell, llame a Remove-STFRoamingGateway.

Importar un dispositivo Citrix Gateway

February 26, 2024

Los parámetros de acceso remoto configurados en la consola de administración de Citrix Gateway deben ser idénticos a aquellos configurados en StoreFront. Este artículo muestra cómo importar los detalles de un servidor virtual de Citrix Gateway para que Citrix Gateway y StoreFront estén configurados correctamente para funcionar juntos.

Requisitos

- Se necesita NetScaler 11.1.51.21, o una versión posterior para exportar varios servidores virtuales de puerta de enlace a un archivo ZIP.

  > **Nota:**
  >
  > Los dispositivos Citrix Gateway solo pueden exportar servidores virtuales de puerta de enlace creados mediante el asistente de Citrix Virtual Apps and Desktops.

- DNS debe ser capaz de resolver todas las URL de los servidores STA (Secure Ticket Authority), y StoreFront debe ser capaz de contactar con ellas. Estas direcciones figuran en el archivo GatewayConfig.json en el archivo ZIP generado por Citrix Gateway.

- El archivo GatewayConfig.json dentro del archivo ZIP generado por Citrix Gateway debe contener la dirección URL de un sitio de Citrix Receiver para Web existente en el servidor de StoreFront. Para ocuparse de esto, Citrix Gateway 11.1 (y versiones posteriores) se pone en contacto con el servidor de StoreFront y enumera todos los almacenes y sitios de Citrix Receiver para Web existentes antes de generar el archivo ZIP para exportarlo.
- StoreFront debe ser capaz de resolver la URL de respuesta en DNS y recurrir a la dirección IP del servidor virtual VPN de la puerta de enlace para la autenticación mediante la puerta de enlace importada.

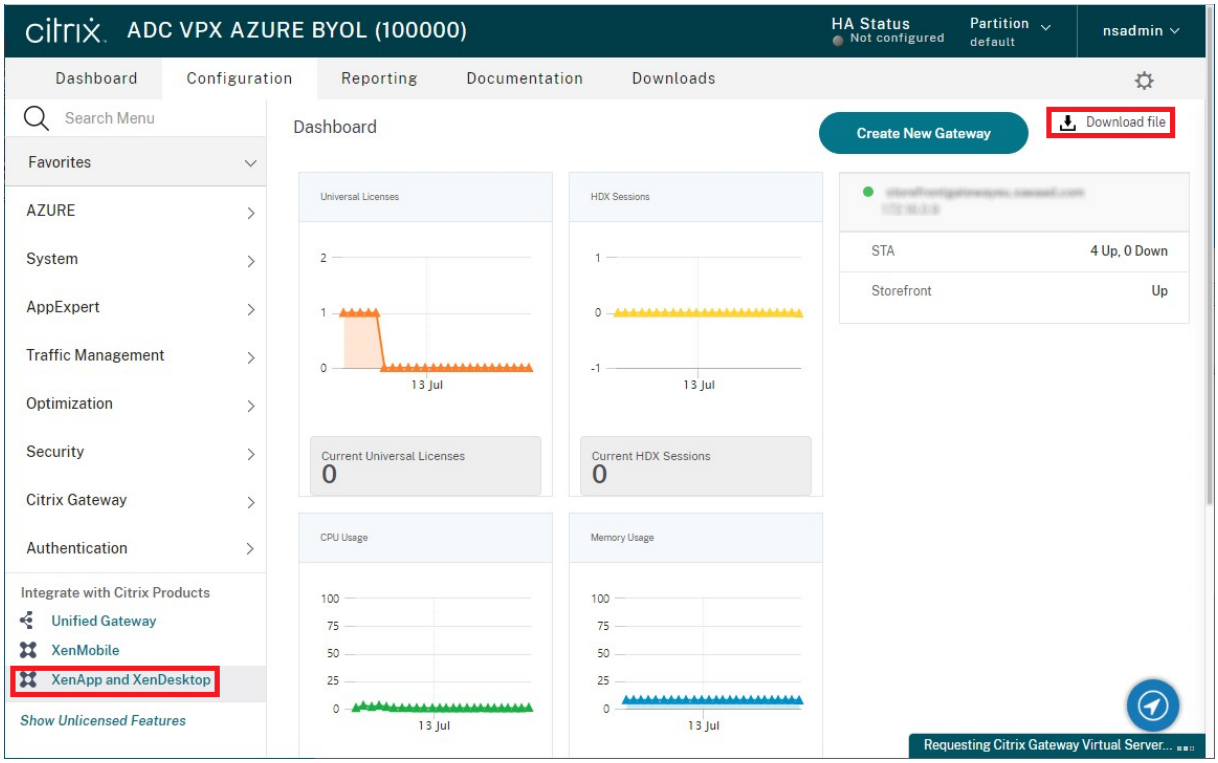
  La combinación de URL de respuesta y puerto que use es normalmente la misma que la combinación de URL y puerto de la puerta de enlace, siempre que StoreFront pueda resolver esta URL.

  o bien

  La combinación de URL de respuesta y puerto puede ser diferente de la URL y puerto de la puerta de enlace, si usa nombres de espacios DNS distintos para uso externo e interno en su entorno. Si su puerta de enlace se encuentra en una zona desmilitarizada (DMZ) y usa una URL <`example.com`>, y StoreFront se encuentra en la red privada de la empresa y usa una URL <`example.local`> puede utilizar una URL de respuesta <`example.local`> para apuntarla de vuelta al servidor virtual de la puerta de enlace en la DMZ.

Exportar la configuración desde Citrix Gateway

1. Inicie sesión en Citrix Gateway.
2. Vaya a la ficha Configuration.
3. En “Integrate with Citrix Products”, haga clic en XenApp y XenDesktop.
4. En la parte superior derecha, haga clic en “Download file”.



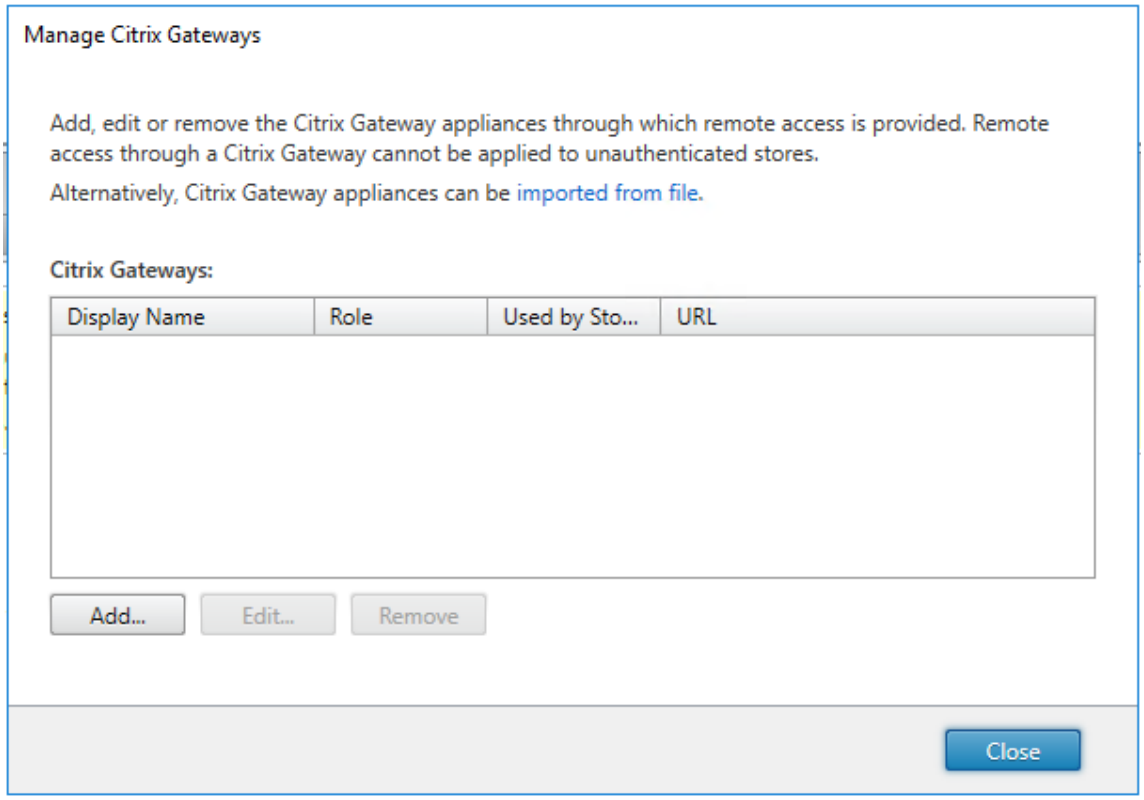
1. Elija si quiere descargar la configuración de todas las puertas de enlace o de una puerta de enlace específica.

Importar un dispositivo Citrix Gateway mediante la consola

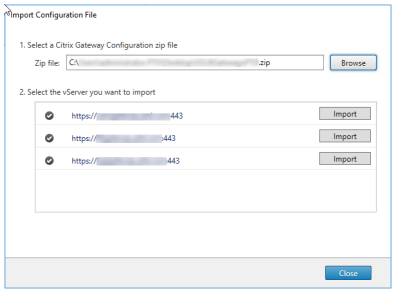
Puede importar una o varias configuraciones de servidor virtual de Citrix Gateway mediante el mismo archivo de importación. Si tiene varios servidores virtuales de puerta de enlace de diferentes dispositivos Citrix Gateway, debe utilizar varios archivos de importación.

> Importante:
>
> Citrix no admite la modificación manual del archivo de configuración exportado desde Citrix Gateway.

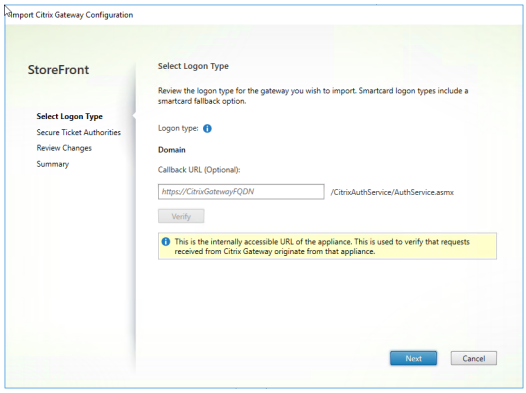
1. Seleccione el nodo **Almacenes** en el panel izquierdo de la consola de administración de Citrix StoreFront y, en el panel **Acciones**, haga clic en **Administrar Citrix Gateway**.
2. En la pantalla Administrar Citrix Gateway, haga clic en el enlace **Importar desde un archivo**.



3. Busque el archivo de configuración del servidor virtual de Citrix Gateway.
4. Se muestra una lista de servidores virtuales de puerta de enlace del archivo ZIP seleccionado. Seleccione el servidor virtual de puerta de enlace que quiere importar y haga clic en **Importar**. Si se repite la importación de un servidor virtual, el botón Importar aparece como botón Actualizar. Si elige **Actualizar**, tiene la opción más adelante de sobrescribir o crear otra puerta de enlace.



5. Revise el **tipo de inicio de sesión** para la puerta de enlace seleccionada y especifique una **URL de respuesta** si es necesario. El tipo de inicio de sesión es el método de autenticación configurado en Citrix Gateway para los usuarios de la aplicación Citrix Workspace. Algunos tipos de inicio de sesión necesitan direcciones URL de respuesta (consulte la tabla).
   - Haga clic en **Verificar** para comprobar si la URL de respuesta es válida y accesible desde el servidor de StoreFront.



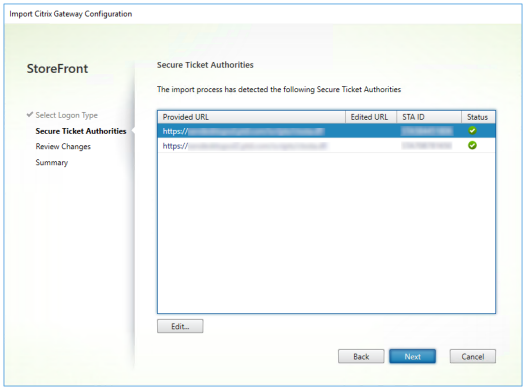
Tipo de inicio de sesión en consola	LogonType en el archivo JSON	URL de respuesta (requerida)
Dominio	Dominio	No
Dominio y token de seguridad	DomainAndRSA	No
Token de seguridad	RSA	Sí
Tarjeta inteligente: Sin alternativa	SmartCard	Sí
Tarjeta inteligente: Dominio	SmartCardDomain	Sí
Tarjeta inteligente: Dominio y token de seguridad	SmartCardDomainAndRSA	Sí
Tarjeta inteligente: Token de seguridad	SmartCardRSA	Sí
Tarjeta inteligente: Autenticación por SMS	SmartCardSMS	Sí
Autenticación por SMS	SMS	Sí

Si se requiere una URL de respuesta, StoreFront rellenará la URL de respuesta en función de la URL de la puerta de enlace encontrada en el archivo ZIP. Se puede cambiar a cualquier dirección URL válida que apunte a la dirección IP virtual de Citrix Gateway. Para las puertas de enlace GSLB, se requieren direcciones URL de respuesta únicas para cada puerta de enlace que importe.

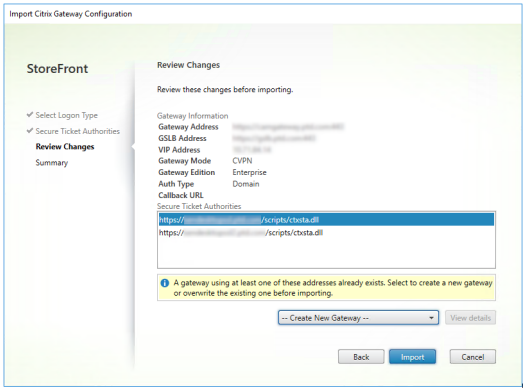
Para usar el acceso inteligente o la autenticación sin contraseña, se requiere una URL de respuesta.

6. Haga clic en **Siguiente**.
7. StoreFront contacta con todas las direcciones URL de servidor STA (Secure Ticket Authority) que figuran en el archivo ZIP que utilizan DNS y valida que sean servidores de generación de tíquets

STA operativos. La importación no continuará si alguna o varias de las direcciones URL de STA no son válidas.



8. Haga clic en **Siguiente**.
9. Revise los detalles de la importación. Si ya existe una puerta de enlace con la misma combinación de dirección URL y puerto (URL_PuertaDeEnlace:puerto), use la lista desplegable para seleccionar una puerta de enlace para sobrescribirla, o cree una nueva.



StoreFront utiliza la combinación de URL_PuertaDeEnlace:puerto para determinar si una puerta de enlace que se quiere importar coincide con otra ya existente que quiera actualizar. Si una puerta de enlace tiene una combinación URL_PuertaDeEnlace:puerto diferente, StoreFront la trata como si fuera una puerta de enlace nueva. Esta tabla de parámetros de puerta de enlace muestra los parámetros que se puede actualizar.

Parámetro de la puerta de enlace	Puede actualizarse
Combinación de URL de puerta de enlace URL:puerto	No
URL de GSLB	Sí
Huella digital y certificado de confianza de NetScaler	Sí
URL de respuesta	Sí

Parámetro de la puerta de enlace	Puede actualizarse
URL del sitio de Citrix Receiver para Web	Sí
VIP/dirección de la puerta de enlace	Sí
ID de STA y URL de STA	Sí
Todos los tipos de inicio de sesión	Sí

10. Haga clic en **Importar**. Si el servidor de StoreFront forma parte de un grupo de servidores, se muestra un mensaje donde se recuerda al usuario que tiene que propagar los parámetros de la puerta de enlace importada a los demás servidores del grupo.
11. Haga clic en **Finalizar**.

Para importar otra configuración de servidor virtual, repita los pasos anteriores.

> **Nota:**
>
> La puerta de enlace predeterminada de un almacén es la puerta de enlace a través de la que las aplicaciones Citrix Workspace intentan conectarse a menos que estén configurados para usar una puerta de enlace diferente. Si no hay ninguna puerta de enlace configurada para el almacén, la primera puerta de enlace que se importe desde el archivo ZIP se convertirá en la puerta de enlace predeterminada utilizada por las aplicaciones Citrix Workspace. La importación de puertas de enlace subsiguientes no cambia la puerta de enlace predeterminada que se haya configurado ya para el almacén.

Importar varios dispositivos Citrix Gateway mediante PowerShell

Read-STFNetScalerConfiguration

- Copie el archivo ZIP al escritorio del administrador de StoreFront conectado en ese momento.
- Lea el contenido del ZIP del archivo de configuración de servidor virtual de Citrix Gateway en memoria y consulte las tres puertas de enlace que contiene mediante sus valores de índice.

```
$ImportedGateways = Read-STFNetScalerConfiguration -path "$env:
    USERPROFILE\desktop\GatewayConfig.zip"
<!--NeedCopy-->
```

Consulte los tres objetos de puerta de enlace en memoria que se leyeron desde el paquete de importación ZIP de NetScaler con el cmdlet **Read-STFNetScalerConfiguration**.

```
$ImportedGateways.Document.Gateways[0]
$ImportedGateways.Document.Gateways[1]
```



```
$ImportedGateways.Document.Gateways[2]

GatewayMode            : CVPN
CallbackUrl            :
GslbAddressUri         : https://gslb.example.com/
AddressUri             : https://emeagateway.example.com/
Address                : https://emeagateway.example.com:443
GslbAddress            : https://gslb.example.com:443
VipAddress             : 10.0.0.1
Stas                   : {
 STA298854503, STA909374257 }

StaLoadBalance         : True
CertificateThumbprints : {
 F549AFAA29EBF61E8709F2316B3981AD503AF387 }

GatewayAuthType        : Domain
GatewayEdition         : Enterprise
ReceiverForWebSites    : {
 Citrix.StoreFront.Model.Roaming.NetScalerConfiguration.
    ReceiverForWebSite }


GatewayMode            : CVPN
CallbackUrl            :
GslbAddressUri         : https://gslb.example.com/
AddressUri             : https://emeagateway.example.com/
Address                : https://emeagateway.example.com:444
GslbAddress            : https://gslb.example.com:443
VipAddress             : 10.0.0.2
Stas                   : {
 STA298854503, STA909374257 }

StaLoadBalance         : True
CertificateThumbprints : {
 F549AFAA29EBF61E8709F2316B3981AD503AF387 }

GatewayAuthType        : DomainAndRSA
GatewayEdition         : Enterprise
ReceiverForWebSites    : {
 Citrix.StoreFront.Model.Roaming.NetScalerConfiguration.
    ReceiverForWebSite }


GatewayMode            : CVPN
CallbackUrl            : https://emeagateway.example.com:445
GslbAddressUri         : https://gslb.example.com/
AddressUri             : https://emeagateway.example.com/
Address                : https://emeagateway.example.com:445
GslbAddress            : https://gslb.example.com:443
VipAddress             : 10.0.0.2
Stas                   : {
 STA298854503, STA909374257 }
```



```
54
55 StaLoadBalance          : True
56 CertificateThumbprints : {
57  F549AFAA29EBF61E8709F2316B3981AD503AF387 }
58
59 GatewayAuthType         :SmartCard
60 GatewayEdition          : Enterprise
61 ReceiverForWebSites     : {
62  Citrix.StoreFront.Model.Roaming.NetScalerConfiguration.
       ReceiverForWebSite }
63
64 <!--NeedCopy-->
```

Cmdlet Import-STFNetScalerConfiguration sin especificar una dirección URL de respuesta

Copie el archivo ZIP al escritorio del administrador de StoreFront conectado en ese momento. Lea el paquete ZIP importado de configuración de Citrix Gateway en memoria y consulte las tres puertas de enlace que contiene mediante sus valores de índice.

```
1 $ImportedGateways = Read-STFNetScalerConfiguration -path "$env:
     USERPROFILE\desktop\GatewayConfig.zip"
2 <!--NeedCopy-->
```

Importe tres puertas de enlace nuevas en StoreFront mediante el cmdlet **Import-STFNetScalerConfiguration** y especifique los índices de puerta de enlace que necesite. El parámetro **-Confirm:$False** evita que la interfaz de usuario de PowerShell le pregunte si quiere permitir importar cada una de las puertas de enlace. Quite este parámetro si quiere importar una por una las puertas de enlace.

```
1 Import-STFNetScalerConfiguration -Configuration $ImportedGateways -
     GatewayIndex 0 -Confirm:$False
2 Import-STFNetScalerConfiguration -Configuration $ImportedGateways -
     GatewayIndex 1 -Confirm:$False
3 Import-STFNetScalerConfiguration -Configuration $ImportedGateways -
     GatewayIndex 2 -Confirm:$False
4 <!--NeedCopy-->
```

Cmdlet Import-STFNetScalerConfiguration especificando su propia dirección URL de respuesta

Importe tres nuevas puertas de enlace en StoreFront con el cmdlet **Import-STFNetScalerConfiguration** y especifique la URL de respuesta que quiera con el parámetro -callbackURL.

```
1 $ImportedGateways = Read-STFNetScalerConfiguration -path "$env:
     USERPROFILE\desktop\GatewayConfig.zip"
2
3 Import-STFNetScalerConfiguration -Configuration $ImportedGateways -
     GatewayIndex 0 -CallbackUrl "https://emeagatewaycb.example.com:443 -
     Confirm:$False
```



```
4
5 Import-STFNetScalerConfiguration -Configuration $ImportedGateways -
    GatewayIndex 1 -CallbackUrl "https://emeagatewaycb.example.com:444 -
    Confirm:$False
6
7 Import-STFNetScalerConfiguration -Configuration $ImportedGateways -
    GatewayIndex 2 -CallbackUrl "https://emeagatewaycb.example.com:445 -
    Confirm:$False
8 <!--NeedCopy-->
```

Cmdlet Import-STFNetScalerConfiguration para anular el método de autenticación almacenado en el archivo de importación y especificar su propia dirección URL de respuesta

Importe tres nuevas puertas de enlace en StoreFront con el cmdlet **Import-STFNetScalerConfiguration** y especifique la URL de respuesta que quiera con el parámetro -callbackURL.

```
1 $ImportedGateways = Read-STFNetScalerConfiguration -path "$env:
    USERPROFILE\desktop\GatewayConfig.zip"
2
3 Import-STFNetScalerConfiguration -Configuration $ImportedGateways -
    GatewayIndex 0 -LogonType "SmartCard" -CallbackUrl "https://
    emeagatewaycb.example.com:443" -Confirm:$False
4
5 Import-STFNetScalerConfiguration -Configuration $ImportedGateways -
    GatewayIndex 1 -LogonType "SmartCard" -CallbackUrl "https://
    emeagatewaycb.example.com:444" -Confirm:$False
6
7 Import-STFNetScalerConfiguration -Configuration $ImportedGateways -
    GatewayIndex 2 -LogonType "SmartCard" -CallbackUrl "https://
    emeagatewaycb.example.com:445" -Confirm:$False
8 <!--NeedCopy-->
```

Equilibrar la carga con NetScaler ADC

April 17, 2024

En este artículo se ofrecen instrucciones acerca de cómo implementar un grupo de servidores de StoreFront que contengan como mínimo dos servidores de StoreFront en toda la configuración activa de equilibrio de carga. En el artículo se ofrece información detallada acerca de cómo configurar un dispositivo NetScaler ADC para equilibrar la carga de solicitudes entrantes de la aplicación Citrix Workspace y exploradores web entre servidores de StoreFront del grupo de servidores.

Requisitos de certificados de servidor para la implementación con equilibrio de carga

Tenga en cuenta las siguientes opciones antes de: adquirir un certificado de una entidad de certificación comercial o emitir uno de la entidad de certificación (CA) de la empresa.

- **Opción 1:** Usar un certificado comodín **.ejemplo.com* en el servidor virtual de equilibrio de carga del dispositivo NetScaler ADC y en los nodos del grupo de servidores de StoreFront. Esto simplifica la configuración y permite agregar más servidores de StoreFront en el futuro, sin la necesidad de reemplazar el certificado.
- **Opción 2:** Usar un certificado que incluya nombres alternativos de sujeto (SAN) en el servidor virtual de equilibrio de carga del dispositivo NetScaler ADC y en los nodos del grupo de servidores de StoreFront. Los nombres SAN adicionales que contenga el certificado que coincidan con todos los nombres de dominio completos (FQDN) de servidor de StoreFront son opcionales aunque se recomiendan, ya que permiten una mayor flexibilidad en la implementación de StoreFront.

Crear registros DNS para el equilibrador de carga del grupo de servidores de StoreFront

Cree un registro DNS A y un registro PTR para el nombre de dominio completo compartido seleccionado. Los clientes de la red usarán este nombre de dominio completo para acceder al grupo de servidores StoreFront mediante el equilibrador de carga del dispositivo NetScaler ADC.

Ejemplo: `storefront.example.com` recurre a la dirección IP virtual (VIP) del servidor virtual del equilibrio de carga.

Configurar servidores de StoreFront

Todos los servidores de StoreFront cuya carga quiera equilibrar deben configurarse como parte de un grupo de servidores de StoreFront que sincronice la configuración entre servidores para garantizar que estén configurados de forma idéntica. Para obtener más detalles sobre cómo agregar servidores a un grupo de servidores, consulte Unirse a un grupo de servidores existente.

Cada servidor debe estar configurado para HTTPS de modo que la comunicación entre el equilibrador de carga y los servidores de StoreFront esté cifrada. Consulte Proteger StoreFront con HTTPS. El certificado debe contener el FQDN de equilibrio de carga como un nombre común (CN) o como un nombre alternativo de sujeto (SAN).

Configure la URL base del grupo de servidores para que sea la URL del equilibrador de carga. Para modificar la URL base, en la consola de administración de Citrix StoreFront, en el panel de la izquierda, haga clic con el botón secundario en **Grupo de servidores** y haga clic en **Cambiar URL base**. Introduzca la URL del servidor virtual del equilibrador de carga.

Configurar de forma opcional Citrix Service Monitor para HTTPS

Una instalación de StoreFront incluye el servicio de Windows **Citrix Service Monitor**. Este servicio no tiene otras dependencias de servicio y supervisa el estado de servicios importantes de StoreFront. Esto permite que NetScaler ADC y otras aplicaciones de terceros supervisen el estado relativo de la implementación de un servidor de StoreFront.

De forma predeterminada, el supervisor usa HTTP en el puerto 8000. Si quiere, puede cambiarlo para usar HTTPS en el puerto 443.

1. Abra el entorno Integrated Scripting Environment (ISE) de PowerShell en el servidor de StoreFront principal y ejecute los comandos siguientes para cambiar el supervisor predeterminado a HTTPS 443:

```
$ServiceUrl = "https://localhost:443/StorefrontMonitor"
Set-STFServiceMonitor -ServiceUrl $ServiceUrl
Get-STFServiceMonitor
<!--NeedCopy-->
```

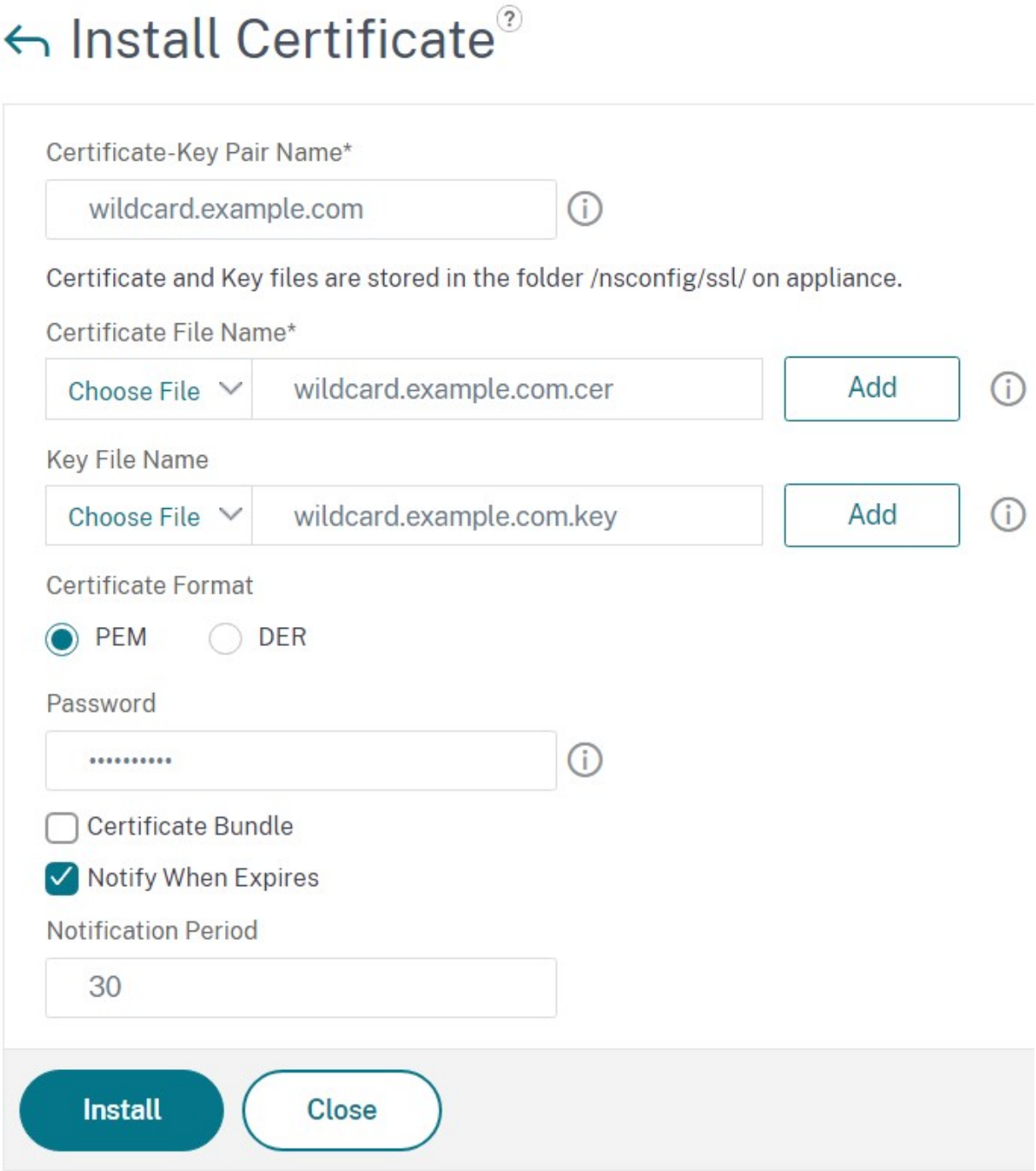
2. Una vez completada la operación, propague los cambios a los demás servidores del grupo de servidores de StoreFront.
3. Para realizar una prueba rápida en el supervisor, introduzca la URL siguiente en el explorador web presente en el servidor de StoreFront o en cualquier otra máquina con acceso de red al servidor de StoreFront. El explorador devuelve un resumen XML del estado de cada servicio de StoreFront.

   ```
   https://<loadbalancingFQDN>/StoreFrontMonitor/GetSFServicesStatus
   ```

Configurar el equilibrador de carga de NetScaler

Configurar el certificado de servidor en el dispositivo NetScaler ADC

1. Inicie sesión en la GUI de administración de dispositivos NetScaler ADC.
2. Seleccione **Traffic Management > SSL > Certificates > Server Certificates**.
3. Haga clic en **Instalar**.
4. En la página **Install Server Certificate**, introduzca el nombre de un par de clave y certificado, haga clic en **Choose File** y busque el archivo del certificado. Si el archivo de certificado no incluye la clave privada, también debe seleccionar un **archivo de clave**.

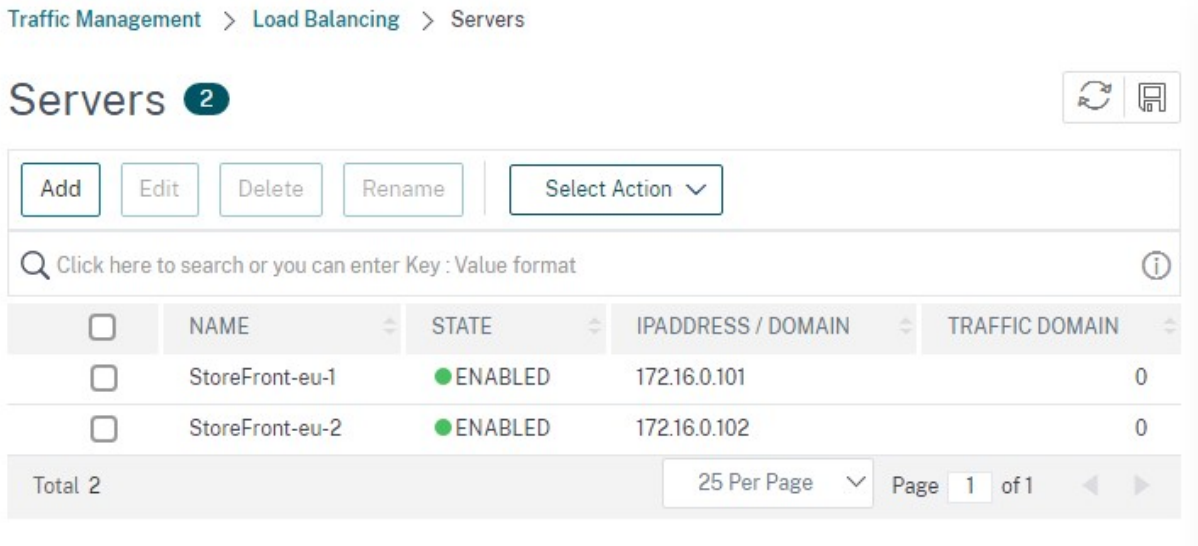


Agregar nodos de servidor StoreFront individuales al equilibrador de carga del dispositivo NetScaler ADC

1. Vaya a **Traffic Management -> Load Balancing -> Virtual Servers**. Haga clic en **Add** y agregue cada uno de los servidores de StoreFront cuya carga debe equilibrarse.

   Ejemplo = 2 servidores de StoreFront denominados StoreFront-eu-1 y StoreFront-eu-2

2. Use una configuración de servidor basada en IP y especifique la dirección IP del servidor de cada nodo de StoreFront.

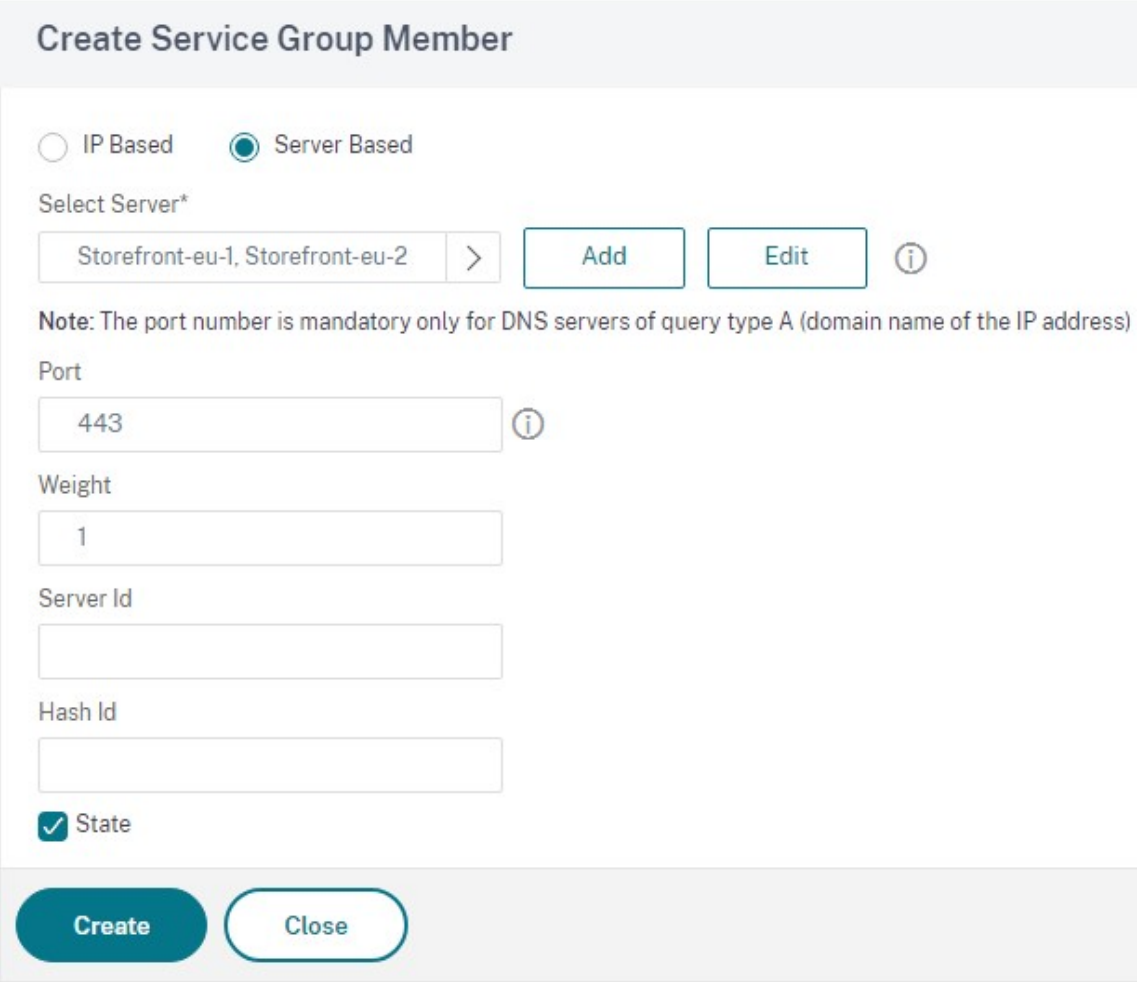


Definir un supervisor de StoreFront para comprobar el estado de todos los nodos de StoreFront en el grupo de servidores

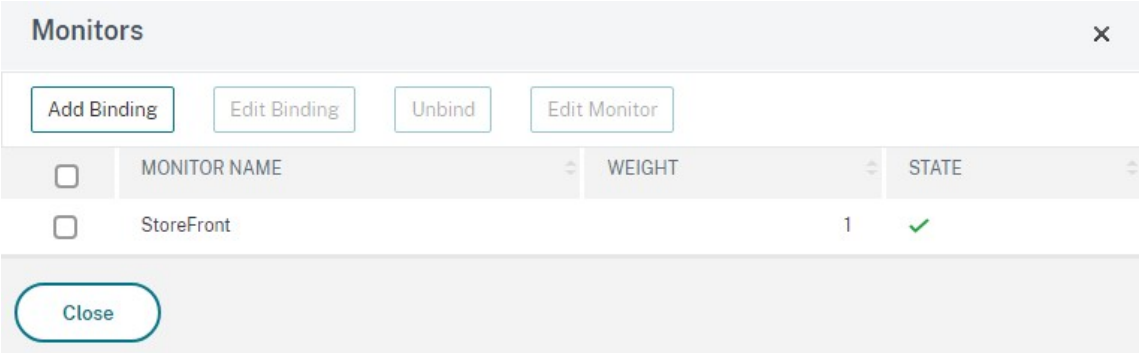
1. Inicie sesión en la interfaz gráfica de usuario de administración de NetScaler ADC.
2. Seleccione **Traffic Management > Load Balancing > Monitors > Add**, agregue un nuevo supervisor llamado *StoreFront* y acepte todos los parámetros predeterminados.
3. En el menú desplegable **Type**, seleccione **StoreFront**.
4. Si configuró su supervisor de StoreFront para HTTPS, asegúrese de que esté seleccionada la opción **Secure**. De lo contrario, deje esta opción sin seleccionar e introduzca un puerto de 8000.
5. Seleccione la opción **Check Backend Services**. Esta opción permite supervisar los servicios que se ejecuten en el servidor de StoreFront. Los servicios de StoreFront se supervisan por sondeo de un servicio Windows que se ejecuta en el servidor de StoreFront, el cual devuelve el estado de los siguientes servicios:
   - W3SVC (IIS)
   - Servicio WAS (Windows Process Activation Service)
   - CitrixCredentialWallet
   - CitrixDefaultDomainService

Crear un grupo de servicios que contenga todos los servidores de StoreFront

1. Vaya a **Traffic Management > Load Balancing > Service Groups**. Presione **Add**. Para conectarse a los servidores de StoreFront a través de HTTPS, seleccione un protocolo de SSL. Deje los demás parámetros como predeterminados. Presione **OK**.
2. Dentro de su grupo de servicios, en **Service Group Members**, haga clic en **No Service Group Member**.
   a) Haga clic en **Service Based**.
   b) Seleccione todos los servidores que definió anteriormente.
   c) Para usar SSL entre el equilibrador de carga y el servidor de StoreFront, introduzca el puerto 443. De lo contrario, introduzca el puerto 80.

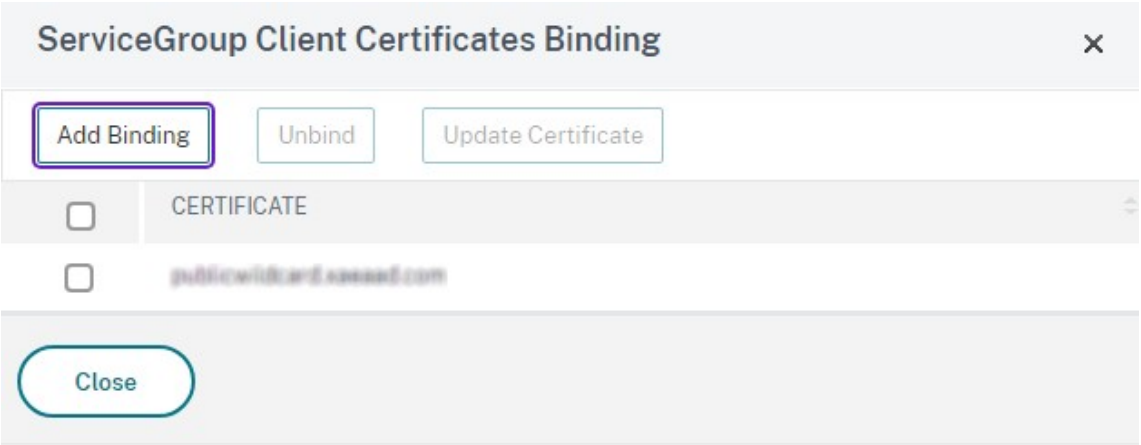


3. Agregue la sección **Monitors** y seleccione el supervisor de StoreFront que creó anteriormente.



4. Agregue la sección **Certificates**.

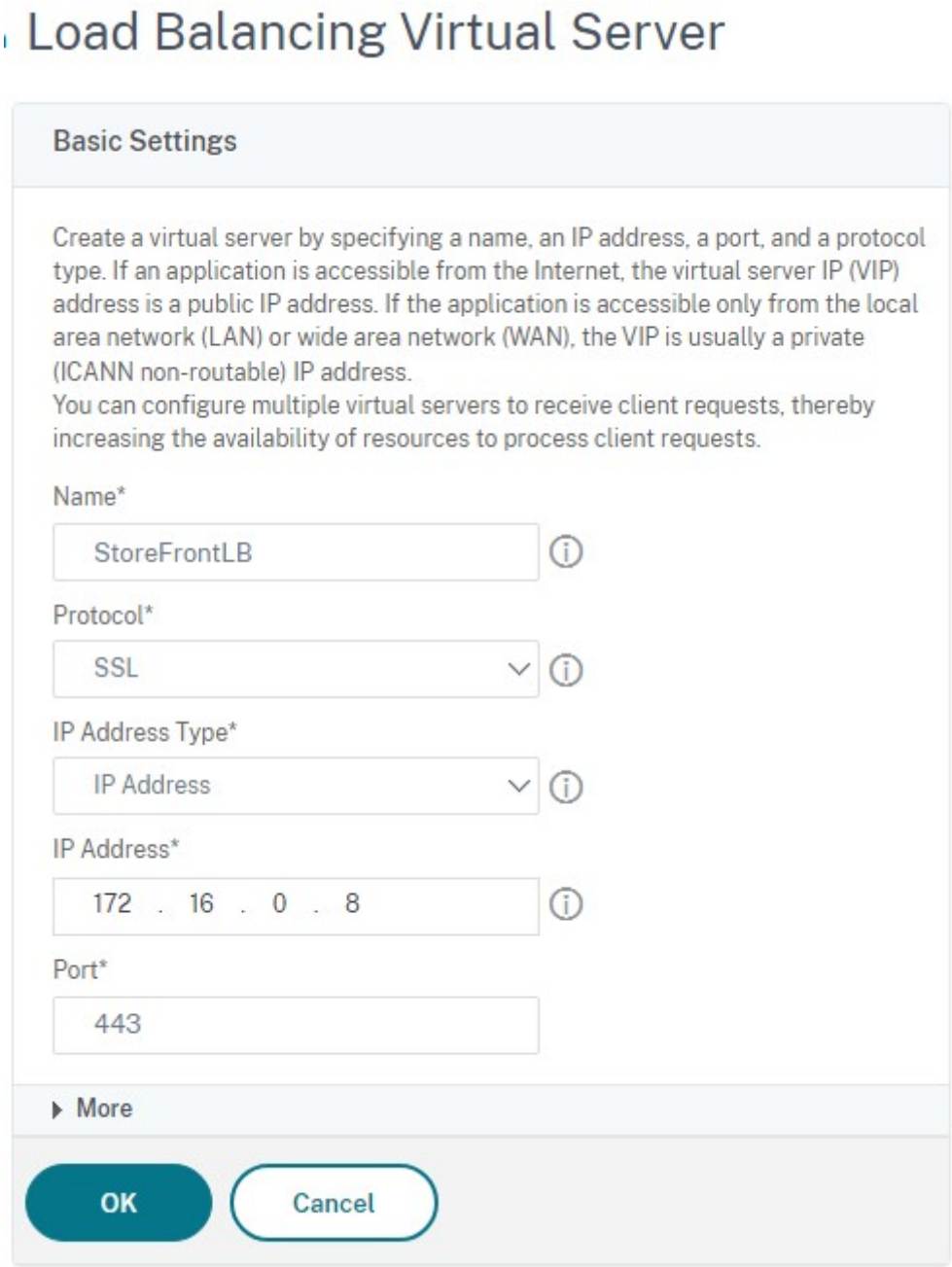
   a) Enlace el certificado de cliente.
   b) Enlace el certificado de CA usado para firmar el certificado de servidor que importó antes, así como cualquier otra entidad de certificación (CA) que pueda formar parte de la cadena de confianza de la infraestructura de clave pública (PKI).



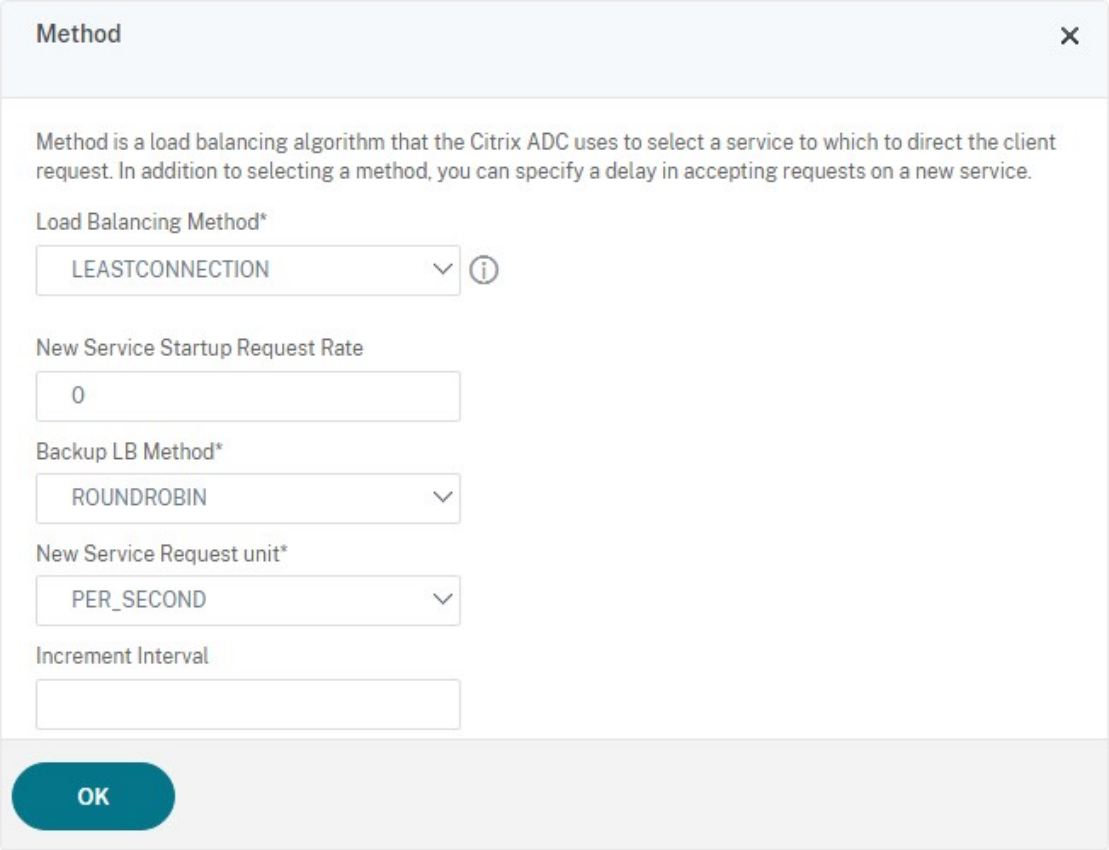
5. Agregue la sección **Settings**. Seleccione **Insert Client IP Header** e introduzca el nombre de encabezado de **X-Forwarded-For**. Esto permite utilizar la dirección IP del cliente en Directivas de Citrix Virtual Apps and Desktops.

Crear un servidor virtual de equilibrio de carga para el tráfico del usuario

1. Inicie sesión en la GUI de administración de dispositivos NetScaler ADC.
2. Seleccione **Traffic Management > Load Balancing > Virtual Servers > Add** para crear un servidor virtual.
3. Introduzca un nombre, elija un protocolo de SSL e introduzca el **Puerto**. Haga clic en Aceptar para crear el servidor virtual.



4. Vincule el **grupo de servicios** que ha creado anteriormente al servidor virtual de equilibrio de carga.
5. Enlace el mismo certificado de servidor y de CA (que ya enlazó al grupo de servicio) al grupo de servidores.
6. Agregue la sección **Method** y seleccione el método de equilibrio de carga. Las opciones más comunes para el equilibrio de carga de StoreFront son **round robin** o **least connection**.



7. Agregue la sección **Persistencia**.

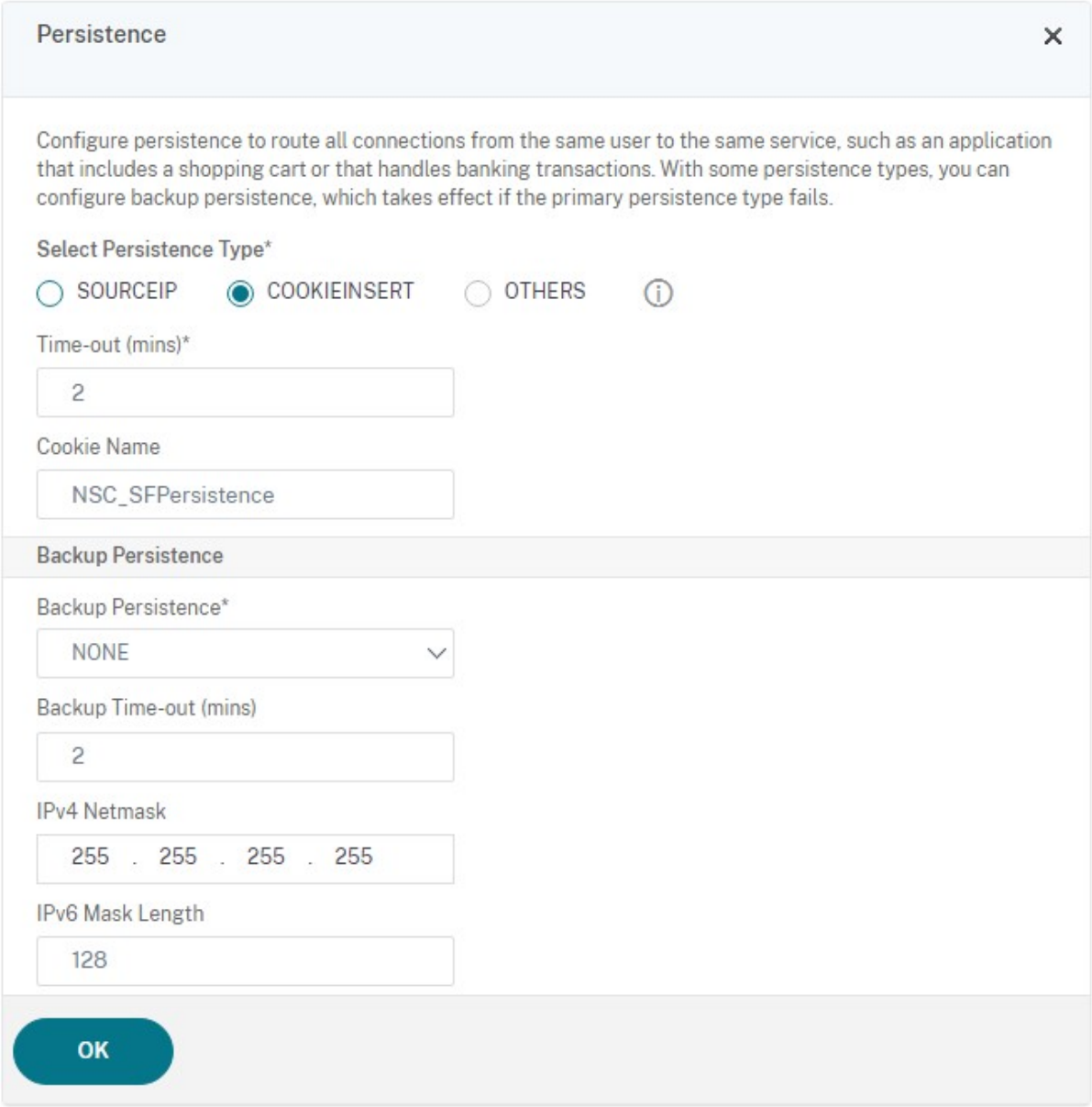
   a) Configure el método de persistencia como **COOKIEINSERT**.

   b) Configure el tiempo de espera para que sea el mismo que el tiempo de espera de sesión en StoreFront, que de forma predeterminada es de 20 minutos.

   c) Dé un nombre a la cookie. Por ejemplo, **NSC_SFPersistence**, ya que esto hace que sea fácil de identificar durante la depuración de errores.

   d) Establezca la persistencia de reserva en **NONE**.

> **Nota:**
>
> Si no se permite que el cliente almacene la cookie HTTP, las solicitudes subsiguientes no contienen la cookie HTTP y no se usará la persistencia.

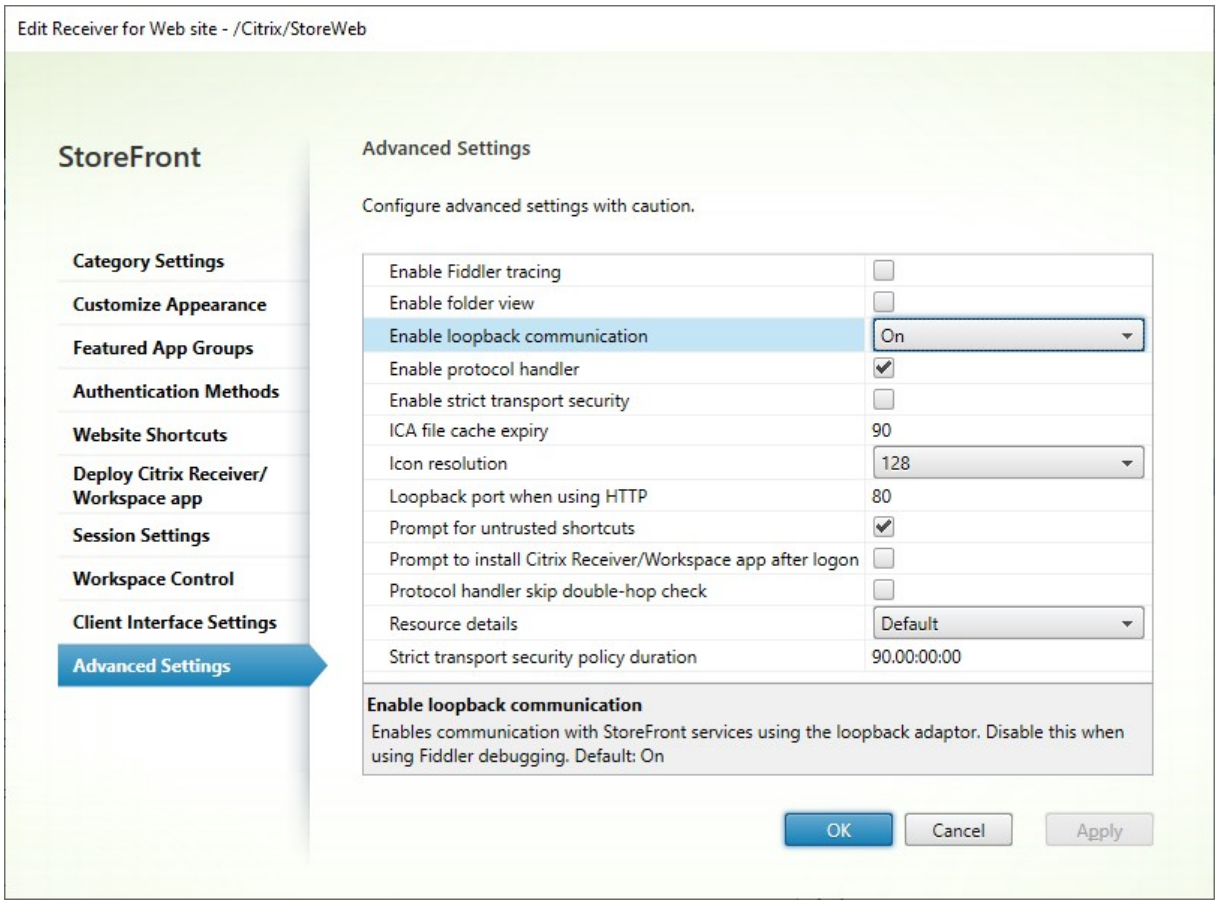


Configurar el bucle invertido de StoreFront

Cuando la dirección base es un equilibrador de carga, para la comunicación interna entre los servicios de StoreFront, podría provocar que el tráfico se dirija al equilibrador de carga y, potencialmente, a otro servidor. Esto se traduce en un rendimiento deficiente y un comportamiento inesperado. Utilice el parámetro **Habilitar comunicación de bucle invertido** de StoreFront para evitarlo. De forma predeterminada, está **activado**, lo que significa que reemplaza la parte del host de la dirección del servicio por la dirección IP de bucle invertido 127.0.0.1, mientras que mantiene el esquema (HTTP o HTTPS) tal y como está. Esto funciona para implementaciones de servidor único e implementaciones que tienen un equilibrador de carga sin terminación SSL.

Cuando el equilibrador de carga termine en SSL y se comunique con StoreFront a través de HTTP (no se recomienda), es necesario configurar la comunicación de bucle invertido de StoreFront con **OnUsingHttp**, lo que significa que StoreFront también cambiará el esquema de HTTPS a HTTP.

1. Abra Citrix StoreFront.
2. Para cada almacén, vaya a **Administrar sitios de Receiver para Web**. Para cada sitio web, vaya a **Configurar**.
3. Vaya a **Parámetros avanzados**.
4. Cambie el parámetro **Habilitar comunicación de bucle invertido** a **OnUsingHttp**.



Cuando el equilibrador de carga termine en SSL y se comunique con StoreFront a través de HTTP (no se recomienda), es necesario configurar la comunicación de bucle invertido de StoreFront con **OnUsingHttp**, lo que significa que StoreFront también cambiará el esquema de HTTPS a HTTP.

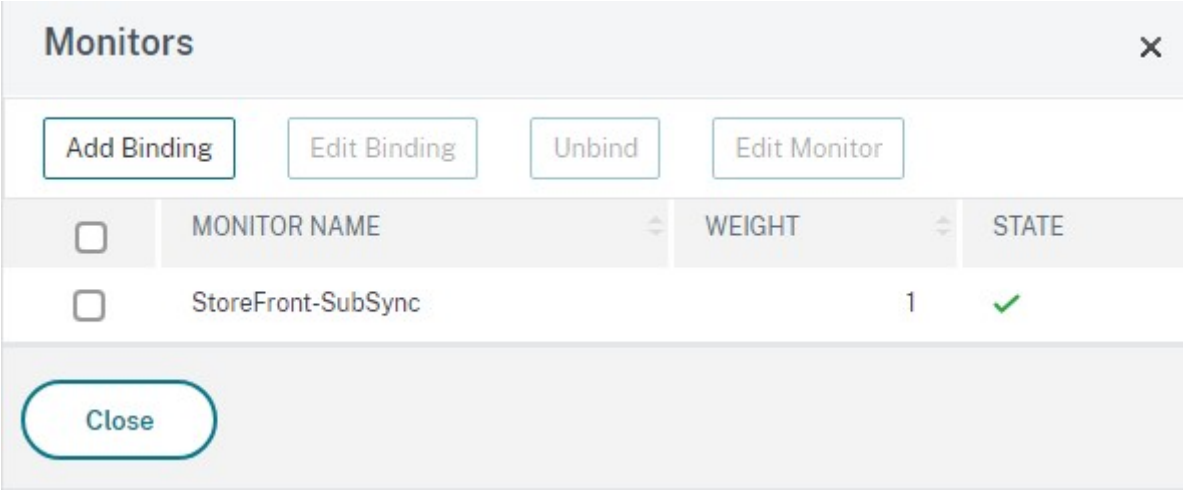
Configurar el equilibrador de carga de NetScaler ADC para la sincronización de suscripciones entre grupos de servidores

Si tiene una implementación en varios sitios que consta de dos o más grupos de servidores de StoreFront, puede replicar los datos de suscripción entre ellos mediante una estrategia de extracción

que siga una programación periódica. La replicación de datos de suscripción de StoreFront utiliza el puerto TCP 808, por lo que utilizar un servidor virtual existente de equilibrio de carga en el puerto HTTP 80 o HTTPS 443 da error. Para ofrecer una alta disponibilidad en este servicio, cree un segundo servidor virtual en cada dispositivo NetScaler ADC de la implementación. De esta manera, equilibrará la carga en el puerto TCP 808 proveniente de cada grupo de servidores de StoreFront.

Configurar un grupo de servicios para la sincronización de suscripciones

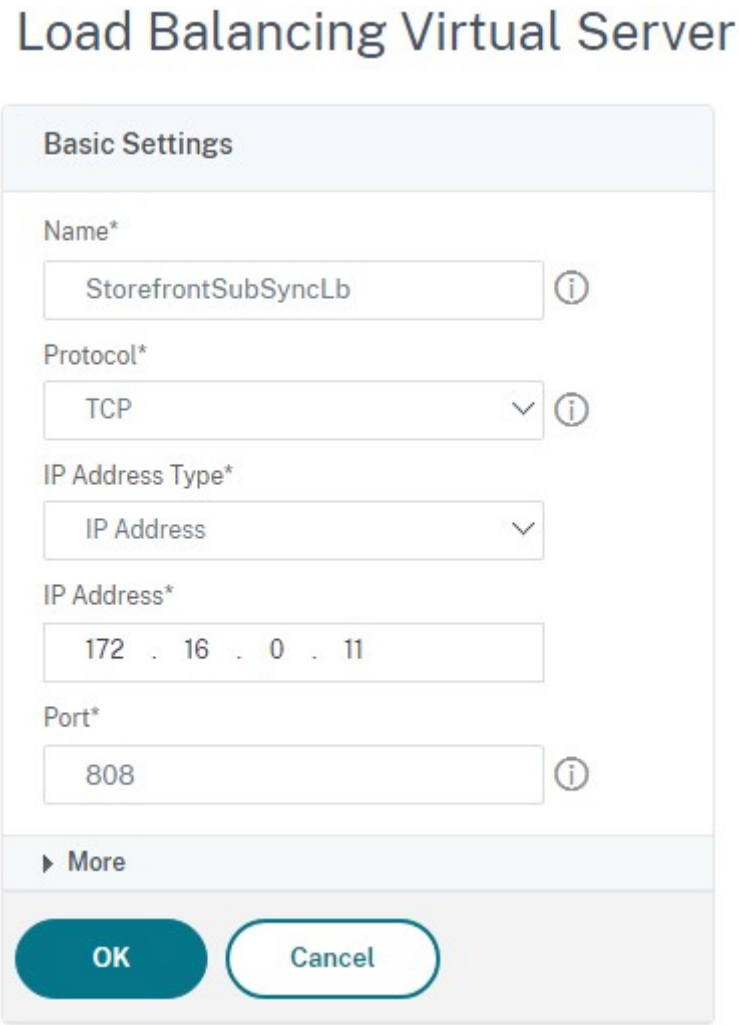
1. Inicie sesión en la GUI de administración de dispositivos NetScaler ADC.
2. Seleccione **Traffic Management > Load Balancing > Service Groups > Add**.
3. Introduzca un nombre de grupo de servicios, cambie el protocolo a **TCP** y haga clic en **OK** para guardar.
4. En la sección **Service Group Members**, agregue todos los nodos de servidores de StoreFront que definió anteriormente en la sección Servers y especifique el puerto **808** en **Port**.
5. Agregue la sección **Monitors**.
   a) Haga clic donde dice **No Service Group to Monitor Binding**.
   b) Haga clic en Agregar. Introduzca el nombre de monitor en **Name** y establezca su **Type** como **TCP**. Haga clic en **Crear**.
   c) Haga clic en **Bind**.



Crear un servidor virtual de equilibrio de carga para la sincronización de suscripciones

1. Inicie sesión en la GUI de administración de dispositivos NetScaler ADC.
2. Seleccione **Traffic Management> Load Balancing > Virtual Servers > Add** y agregue un nuevo grupo de servicios.
3. Escriba un nombre en **Name**.

4. Cambie el protocolo a **TCP**.
5. Introduzca una dirección IP.
6. Introduzca el puerto **808** en **Port**.



7. Haga clic en **Aceptar**.
8. Haga clic en **No Load Balancing Virtual Server ServiceGroup Binding**, seleccione el grupo de servicios que creó anteriormente y haga clic en **Bind**.
9. Agregue la sección **Method** y establezca **Load Balancing Method** en **ROUNDROBIN**.
10. Haga clic en **Done** para completar los cambios.

Configurar StoreFront para extraer datos de suscripción mediante un equilibrador de carga

Consulte Configurar la sincronización de suscripciones.

Cuando configure la programación de la replicación, especifique la dirección de un grupo de servidores que coincida con la dirección IP del equilibrador de carga del servidor virtual de sincronización de suscripciones.

Configurar Citrix Gateway y StoreFront para la autenticación con formularios delegada (DFA)

November 10, 2023

La autenticación extensible proporciona un único punto de personalización para la extensión de la autenticación con formularios de Citrix Gateway y StoreFront. Para lograr una solución de autenticación mediante el SDK de autenticación extensible, debe configurar la autenticación con formularios delegada (DFA) entre Citrix Gateway y StoreFront. El protocolo de autenticación con formularios delegada permite la generación y el procesamiento de formularios de autenticación, incluida la validación de credenciales, para que se deleguen a otro componente. Por ejemplo, Citrix Gateway delega su autenticación a StoreFront, el cual interactúa con un servidor o servicio externo de autenticación.

La configuración de la autenticación con formularios delegada en Citrix Gateway se describe en CTX200383.

Recomendaciones para la instalación

- Para garantizar que la comunicación entre Citrix Gateway y StoreFront está protegida, utilice el protocolo HTTPS en lugar del protocolo HTTP.
- Para la implementación de clústeres, compruebe que todos los nodos tengan el mismo certificado de servidor instalado y configurado en el enlace HTTPS de IIS antes de proceder a la configuración.
- Compruebe que Citrix Gateway tiene el emisor del certificado de servidor de StoreFront configurado como una entidad de certificación de confianza cuando HTTPS esté configurado en StoreFront.

Consideraciones acerca de la instalación de clústeres de StoreFront

- Instale un plug-in externo de autenticación en todos los nodos antes de unirlos.
- Configure todos los parámetros relacionados con la autenticación con formularios delegada en un nodo y propague los cambios a los demás. Consulte “Habilitación de la autenticación con formularios delegada”.

Habilitación de la autenticación con formularios delegada

Como no hay ninguna interfaz gráfica de usuario para la configuración del parámetro de claves pre-compartidas de Citrix en StoreFront, utilice la consola de PowerShell para instalar la autenticación con formularios delegada.

1. Instale la autenticación con formularios delegada. No se instala de forma predeterminada, por lo que deberá instalarla mediante la consola de PowerShell.

```
PS C:\Users\administrator.PTD.000> cd 'C:\Program Files\Citrix\Receiver StoreFront\Scripts'
PS C:\Program Files\Citrix\Receiver StoreFront\Scripts> & .\ImportModules.ps1
Adding snapins
Importing modules
Loading 'C:\Program Files\Citrix\Receiver StoreFront\Admin\Citrix.DeliveryServices.ConfigurationProvider.dll'
Loading 'C:\Program Files\Citrix\Receiver StoreFront\Admin\Citrix.DeliveryServices.ConfigurationProvider.dll'

PS C:\Program Files\Citrix\Receiver StoreFront\Scripts> Install-DSDFAServer
Id                              : bf694fbc-ae0a-4d56-8749-c945559e897a
ClassType                       : e1eb3668-9c1c-4ad8-bbae-c08b2682c1bc
FrameworkController             : Citrix.DeliveryServices.Framework.FileBased.FrameworkController
ParentInstance                  : 8dd182c7-f970-466c-ad4c-27a5980f716c
RootInstance                    : 5d0cdc75-1dee-4df7-8069-7375d79634b3
TenantId                        : 860e9401-39c8-4f2c-928d-34251102b840
Data                            : {
  }

ReadOnlyData                    : {
 [Name, DelegatedFormsServer], [Cmdlet, Add-DSWebFeature], [Snapin, Citrix.DeliverySer
                                  vices.Web.Commands], [Tenant, 860e9401-39c8-4f2c-928d-34251102b840] }

ParameterData                   : {
 [FeatureClassId, e1eb3668-9c1c-4ad8-bbae-c08b2682c1bc], [ParentInstanceId, 8dd182c7-f
                                  970-466c-ad4c-27a5980f716c], [TenantId, 860e9401-39c8-4f2c-928d-34251102b840] }

AdditionalInstanceDependencies : {
```



```
 b1e48ef0-b9e5-4697-af9b-0910062aa2a3 }

IsDeployed                      : True
FeatureClass                    : Citrix.DeliveryServices.Framework
    .Feature.FeatureClass
<!--NeedCopy-->
```

2. Agregue el Citrix Trusted Client. Configure la clave secreta compartida (frase secreta) entre StoreFront y Citrix Gateway. La frase secreta y el ID del cliente deben ser idénticos a los que configuró en Citrix Gateway.

```
PS C:\Program Files\Citrix\Receiver StoreFront\Scripts> Add-
    DSCitrixPSKTrustedClient -clientId netscaler.fqdn.com -
    passphrase secret
<!--NeedCopy-->
```

3. Establezca la Conversation Factory de la autenticación con formularios delegada para dirigir todo el tráfico al formulario personalizado. Para encontrar la Conversation Factory, busque ConversationFactory en C:\inetpub\wwwroot\Citrix\Authentication\web.config. Esto es un ejemplo de lo que puede ver.

```
<example connectorURL="http://Example.connector.url:8080/adapters-
    sf-aaconnector-webapp">
      <routeTable order="1000">
        <routes>
          <route name="StartExampleAuthentication" url="Example-
              Bridge-Forms/Start">
            <defaults>
              <add param="controller" value="
                  ExplicitFormsAuthentication" />
              <add param="action" value="AuthenticateStart" />
              <add param="postbackAction" value="Authenticate" />
              <add param="cancelAction" value="CancelAuthenticate"
                  />
              <add param="conversationFactory" value="
                  ExampleBridgeAuthentication" />
              <add param="changePasswordAction" value="
                  StartChangePassword" />
              <add param="changePasswordController" value="
                  ChangePassword" />
              <add param="protocol" value="CustomForms" />
            </defaults>
          </route>
<!--NeedCopy-->
```

4. En PowerShell, establezca la Conversation Factory de la autenticación con formularios delegada. En este ejemplo, se establece como ExampleBridgeAuthentication.

```
PS C:\Program Files\Citrix\Receiver StoreFront\Scripts> Set-
    DSDFAProperty -ConversationFactory ExampleBridgeAuthentication
<!--NeedCopy-->
```


Los argumentos de PowerShell no distinguen entre mayúsculas y minúsculas. Por ejemplo, **-ConversationFactory** es idéntico a **-conversationfactory**.

Desinstale StoreFront

Antes de desinstalar StoreFront, desinstale todos los plug-ins externos de autenticación, ya que afectará a la funcionalidad de StoreFront.

Autenticarse con dominios distintos

February 26, 2024

Algunas organizaciones han establecido directivas que no les permiten conceder a desarrolladores o contratistas externos el acceso a los recursos publicados en un entorno de producción. En este artículo se muestra cómo conceder acceso a los recursos publicados en un entorno de prueba. Para ello, los usuarios deberán autenticarse con un dominio a través de Citrix Gateway. Luego, puede usar otro dominio para autenticarse en StoreFront y el sitio de Receiver para Web. La autenticación a través de Citrix Gateway que se describe en este artículo se admite en caso de usuarios que inician sesión a través del sitio de Receiver para Web. Este método de autenticación no se admite en caso de usuarios nativos móviles o de escritorio procedentes de Citrix Receiver o de aplicaciones Citrix Workspace.

Configurar un entorno de prueba

En este ejemplo se usa un dominio de producción llamado “production.com”y un dominio de prueba llamado “development.com”.

Dominio `production.com`

Configuración del dominio `production.com` utilizado en este ejemplo:

- Citrix Gateway con la directiva de autenticación LDAP configurada para `production.com`.
- La autenticación a través de esa puerta de enlace se realiza con la cuenta y la contraseña production\testuser1.

Dominio `development.com`

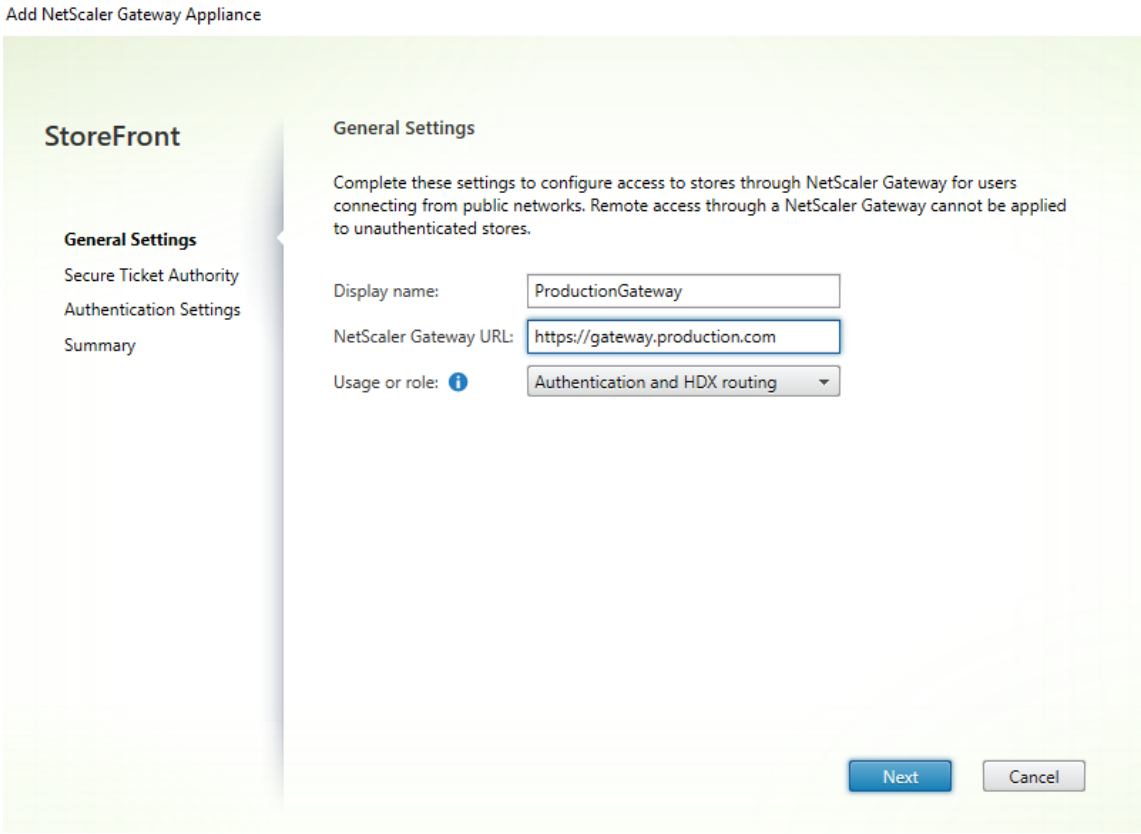
Configuración del dominio `development.com` utilizado en este ejemplo:

- StoreFront, Citrix Virtual Apps and Desktops y VDA se encuentran en el dominio `development.com`.
- La autenticación en el sitio web de Citrix Receiver se produce con la cuenta y la contraseña development\testuser1.
- No hay ninguna relación de confianza entre los dos dominios.

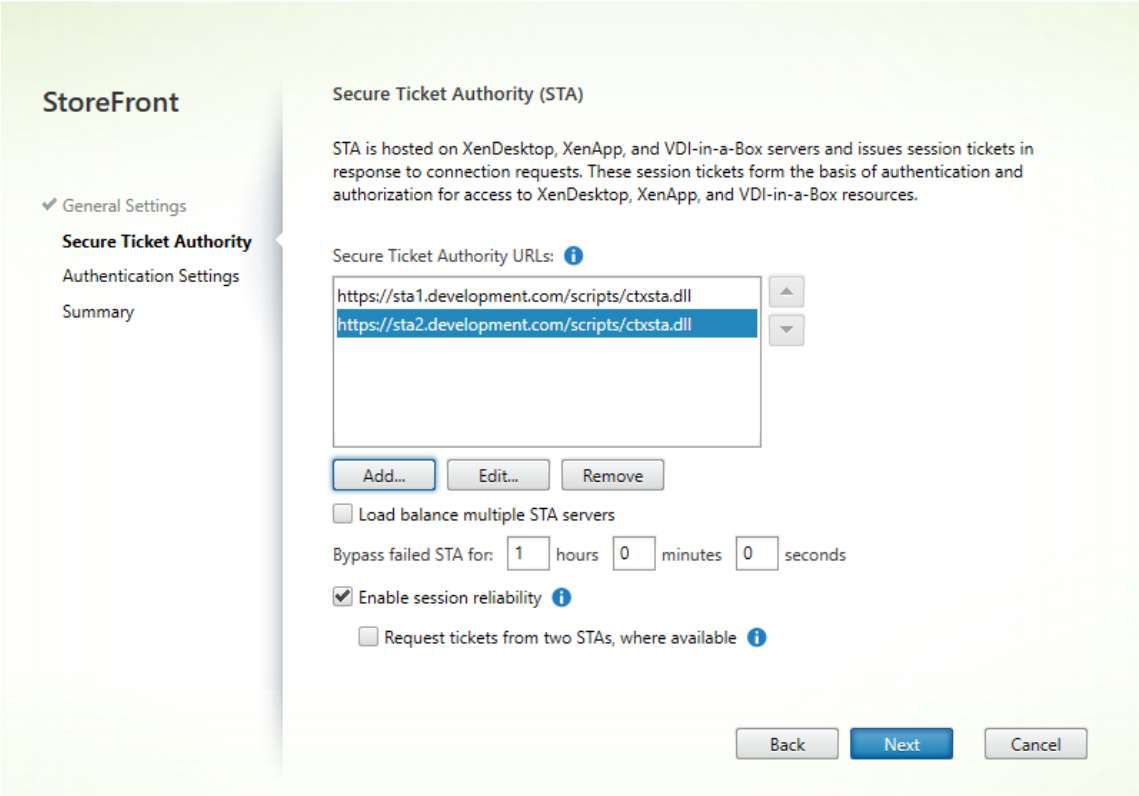
Configurar Citrix Gateway para el almacén

Para configurar Citrix Gateway para el almacén:

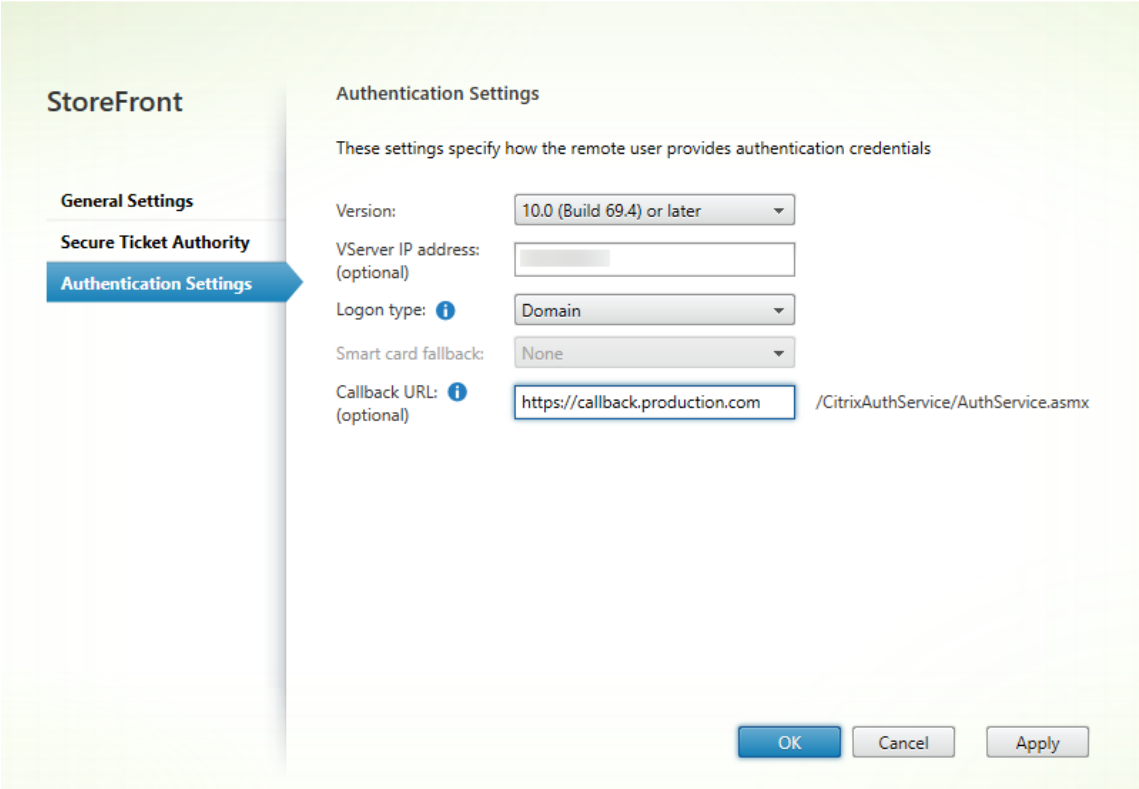
1. Seleccione el nodo **Almacenes** en el panel izquierdo de la consola de administración de Citrix StoreFront y, en el panel **Acciones**, haga clic en **Administrar Citrix Gateway**.
2. En la pantalla "Administrar Citrix Gateway", haga clic en **Agregar**.
3. Complete los pasos de Parámetros generales, de Secure Ticket Authority y de Autenticación.



Add NetScaler Gateway Appliance



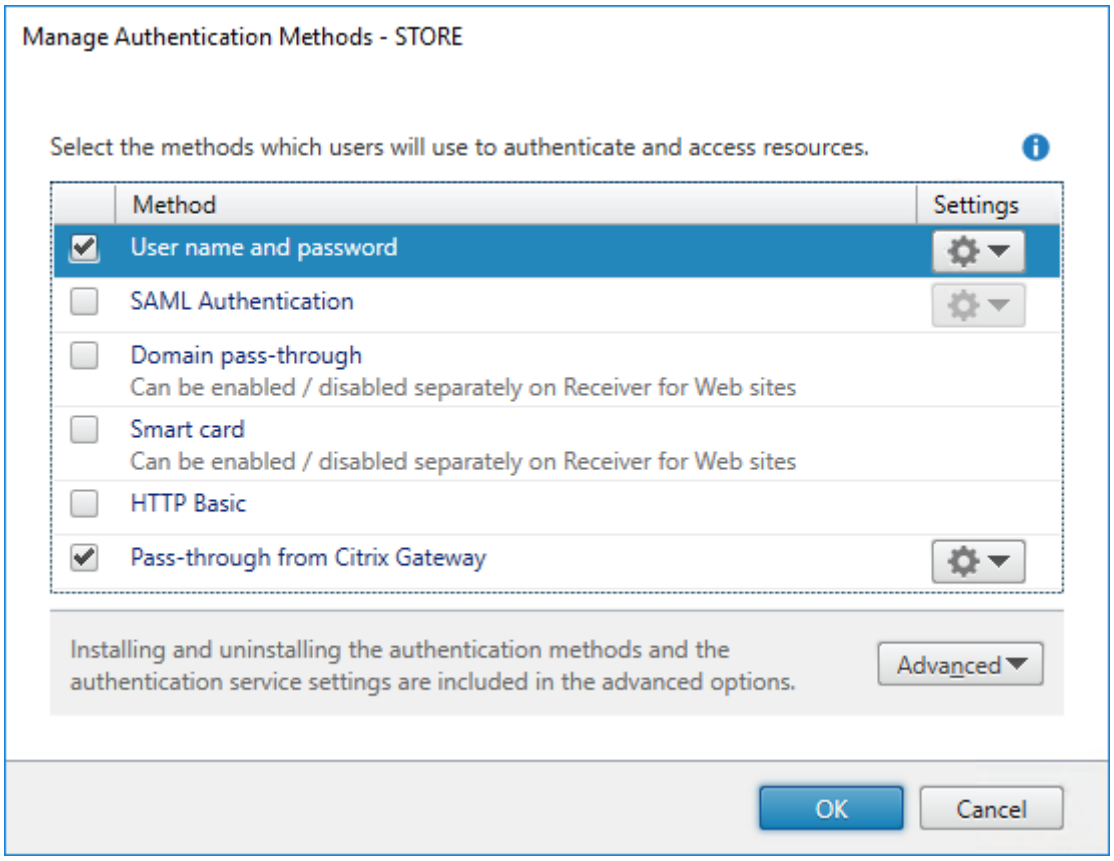
Edit NetScaler Gateway appliance - ProductionGateway



> **Nota:**
>
> Puede que deba agregar reenviadores DNS condicionales para que los servidores DNS en ejecución en ambos dominios puedan resolver los FQDN en el otro dominio. El dispositivo Citrix Gateway debe poder resolver los nombres FQDN del servidor STA en el dominio `development.com` con su servidor DNS de `production.com`. StoreFront también debe poder resolver la URL de respuesta en el dominio `production.com` con su servidor DNS de `development.com`. Si no, también se puede utilizar un nombre FQDN de `development.com` que recurra a la IP virtual (VIP) del servidor virtual de Citrix Gateway.

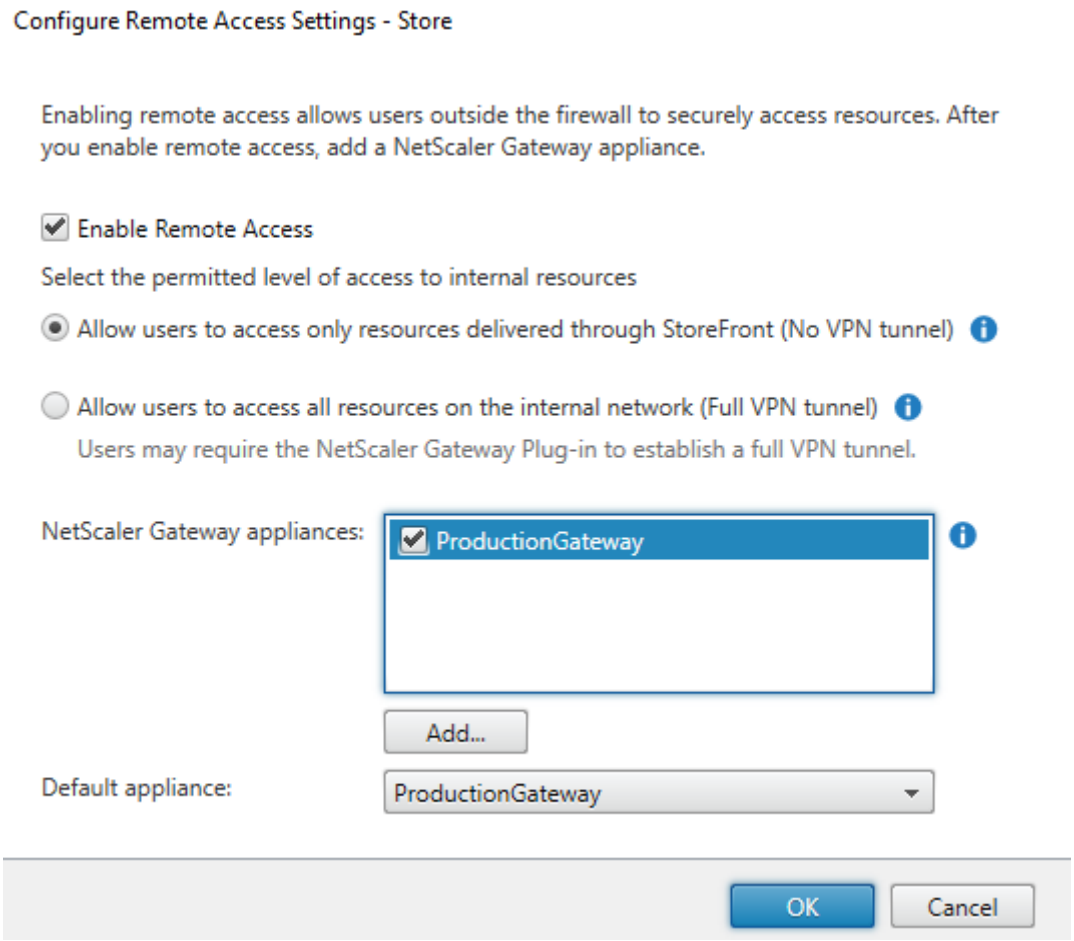
Habilitar PassThrough desde Citrix Gateway

1. Seleccione **Almacenes** en el panel izquierdo de la consola de administración de Citrix StoreFront y, en el panel **Acciones**, haga clic en **Administrar métodos de autenticación**.
2. En la pantalla Administrar métodos de autenticación, seleccione **PassThrough desde Citrix Gateway**.
3. Haga clic en **Aceptar**.



Configurar el almacén para el acceso remoto a través de Gateway

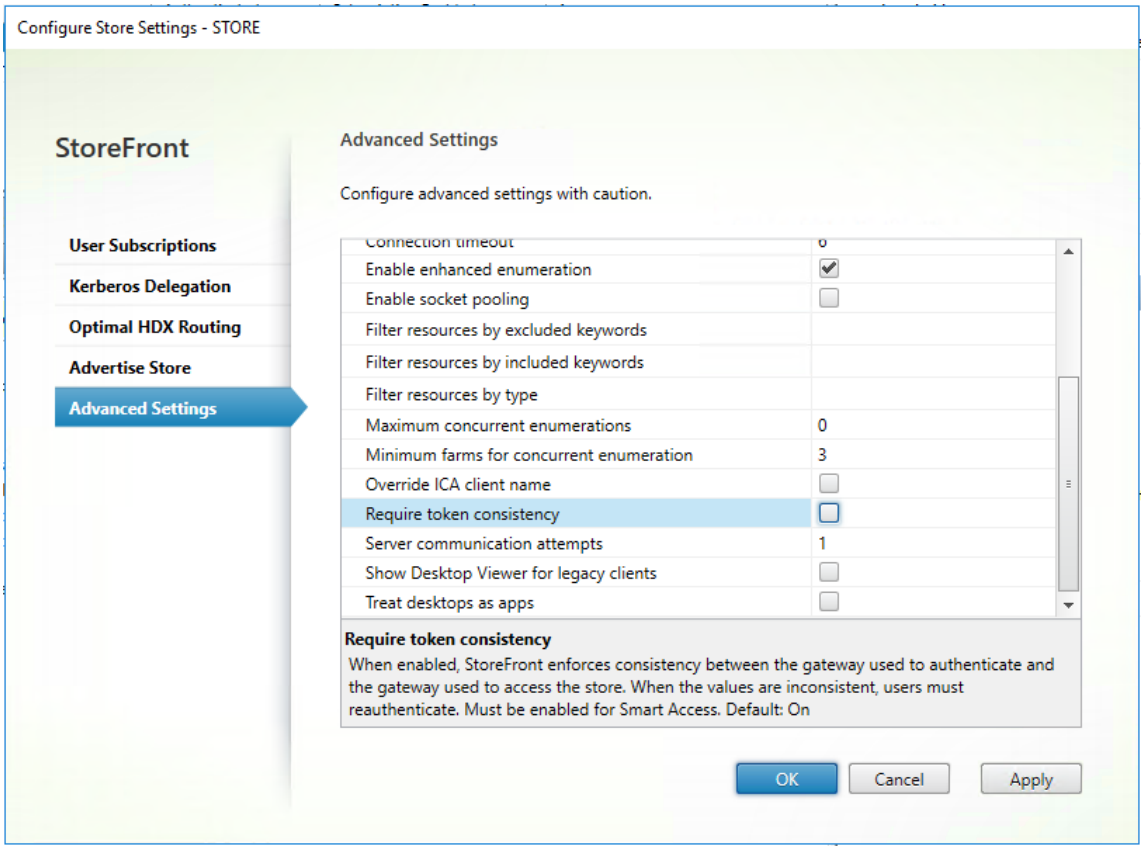
1. Seleccione el nodo **Almacenes** en el panel izquierdo de la consola de administración de Citrix StoreFront y, en el panel de resultados, seleccione un almacén. En el panel **Acciones**, haga clic en **Configurar parámetros de acceso remoto**.
2. Seleccione **Habilitar acceso remoto**.
3. Compruebe que ha registrado el dispositivo Citrix Gateway en el almacén. Si no lo registra, la generación de tíquets STA no funcionará.



Inhabilitar la coherencia de tokens

1. Seleccione el nodo **Almacenes** en el panel izquierdo de la consola de administración de Citrix StoreFront y, en el panel de resultados, seleccione un almacén. En el panel **Acciones**, haga clic en **Configurar parámetros del almacén**.
2. En la página Configurar parámetros del almacén, seleccione **Parámetros avanzados**.
3. Desmarque la casilla **Requerir coherencia de token**. Para obtener más información, consulte

Parámetros avanzados de almacenes.



4. Haga clic en **Aceptar**.

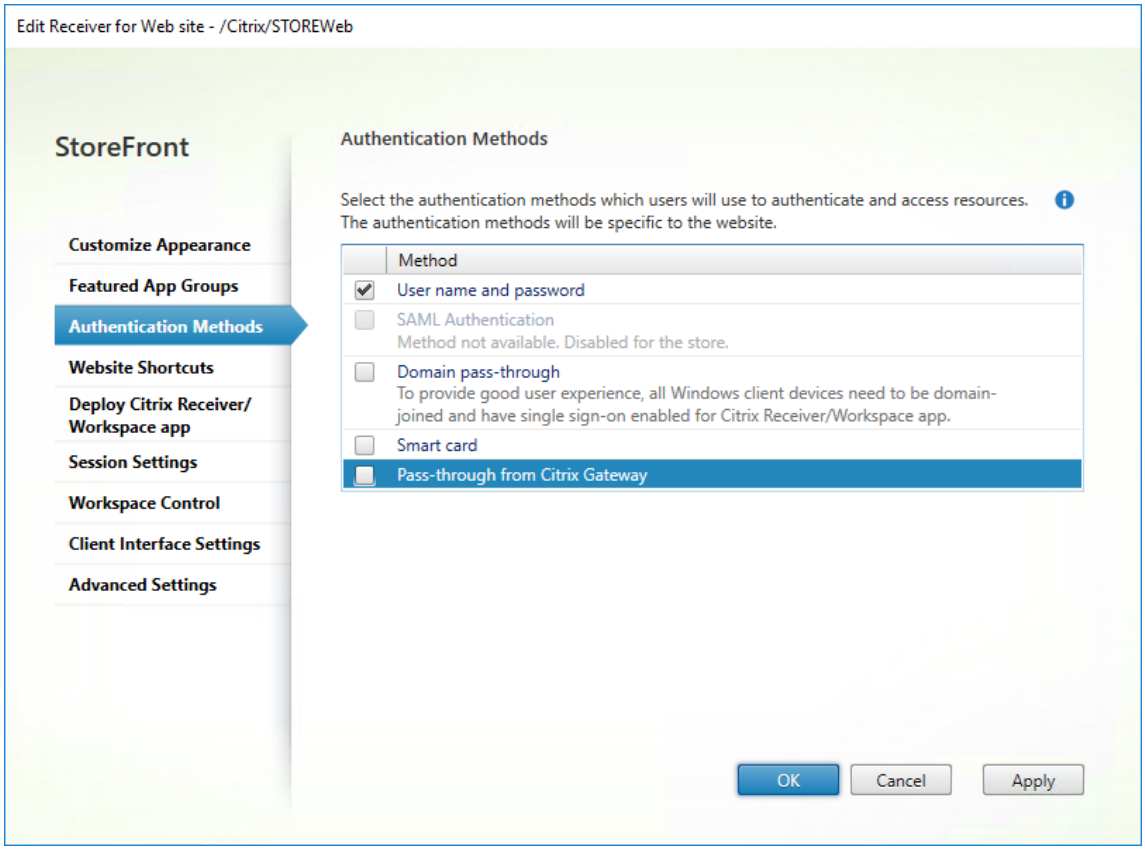
> Nota:
>
> El parámetro "Requerir coherencia de token"está marcado (activado) de forma predeterminada. Si lo inhabilita, las funciones de SmartAccess utilizadas para Citrix Gateway End Point Analysis (EPA) dejan de funcionar. Para obtener más información sobre SmartAccess, consulte CTX138110.

Inhabilitar la autenticación PassThrough desde Citrix Gateway para el sitio web

> **Importante:**
>
> Inhabilitar la autenticación PassThrough desde Citrix Gateway impide que el sitio web use las credenciales incorrectas del dominio `production.com` transferido desde el dispositivo Citrix Gateway. Inhabilitar la autenticación PassThrough desde Citrix Gateway hace que el sitio web solicite al usuario que introduzca las credenciales. Estas no son las credenciales que se utilizan para iniciar sesión a través de Citrix Gateway.

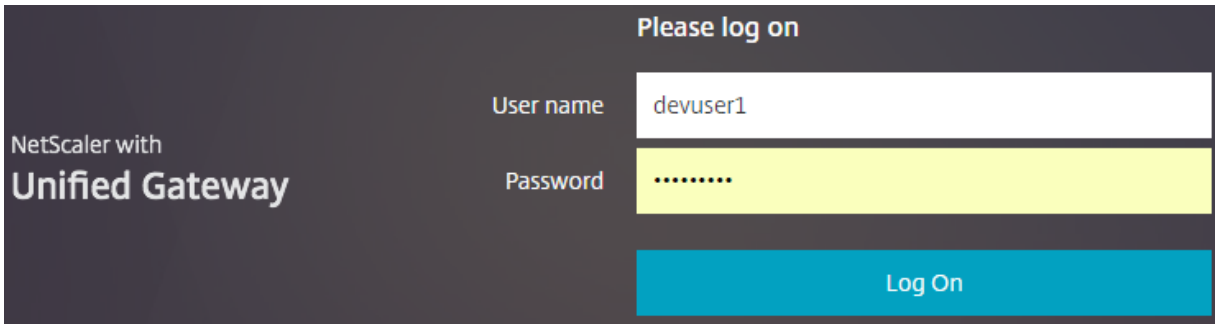
1. Seleccione el nodo **Almacenes** en el panel izquierdo de la consola de administración de Citrix StoreFront.

2. Seleccione el **almacén** que quiere modificar.
3. En el panel **Acciones**, haga clic en **Administrar sitios de Receiver para Web**.
4. En Métodos de autenticación, desmarque **PassThrough desde Citrix Gateway**.
5. Haga clic en **Aceptar**.

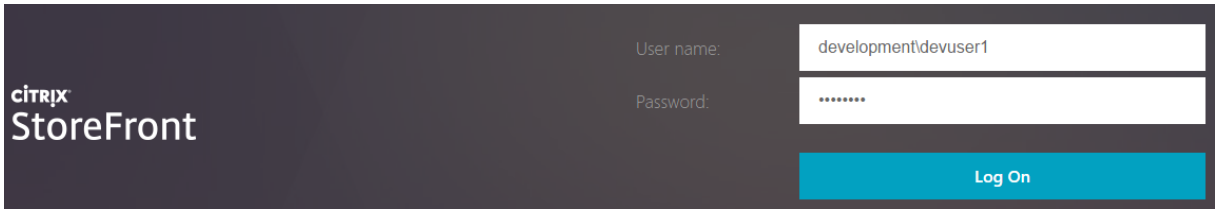


Iniciar sesión en Gateway con el usuario y las credenciales de `production.com`

Para realizar pruebas, inicie sesión en Gateway con un usuario y unas credenciales de `production.com`.



Después de iniciar sesión, se le solicita que introduzca las credenciales de `development.com`.

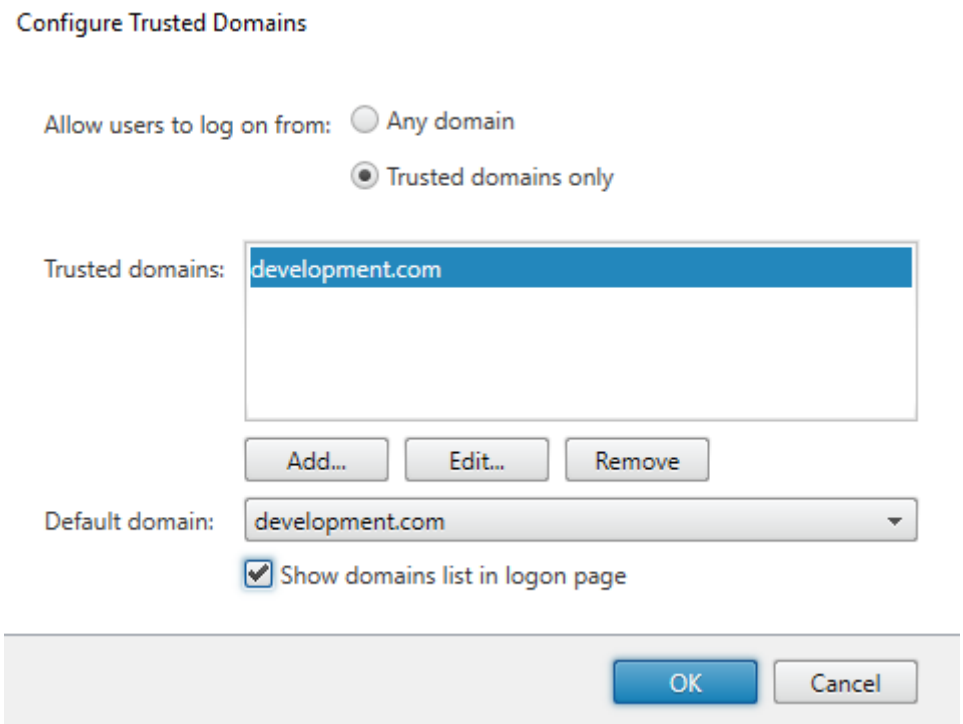


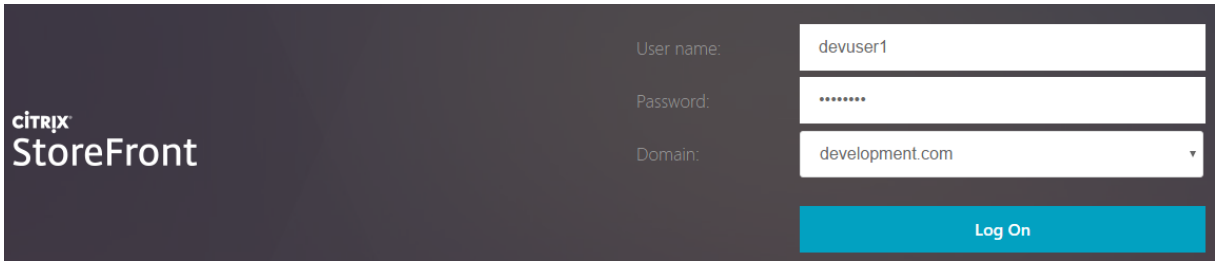
Agregar una lista desplegable de dominios de confianza en StoreFront (opcional)

Este parámetro es optativo, pero puede contribuir a evitar que el usuario introduzca accidentalmente el dominio incorrecto para autenticarse a través de Citrix Gateway.

Si el nombre de usuario es el mismo para ambos dominios, introducir el dominio incorrecto es más probable. También es posible que los usuarios nuevos tiendan a dejarse el dominio cuando inicien sesión a través de Citrix Gateway. Entonces, podrían olvidarse de introducir el dominio y el nombre de usuario para el segundo dominio cuando se les pida iniciar sesión en el sitio de Receiver para Web.

1. Seleccione **Almacenes** en el panel izquierdo de la consola de administración de Citrix StoreFront y, en el panel **Acciones**, haga clic en **Administrar métodos de autenticación**.
2. Seleccione la flecha desplegable ubicada junto a **Nombre de usuario y contraseña**.
3. Haga clic en **Agregar** para agregar `development.com` como dominio de confianza y marque la casilla **Mostrar lista de dominios en la página** de inicio de sesión.
4. Haga clic en **Aceptar**.

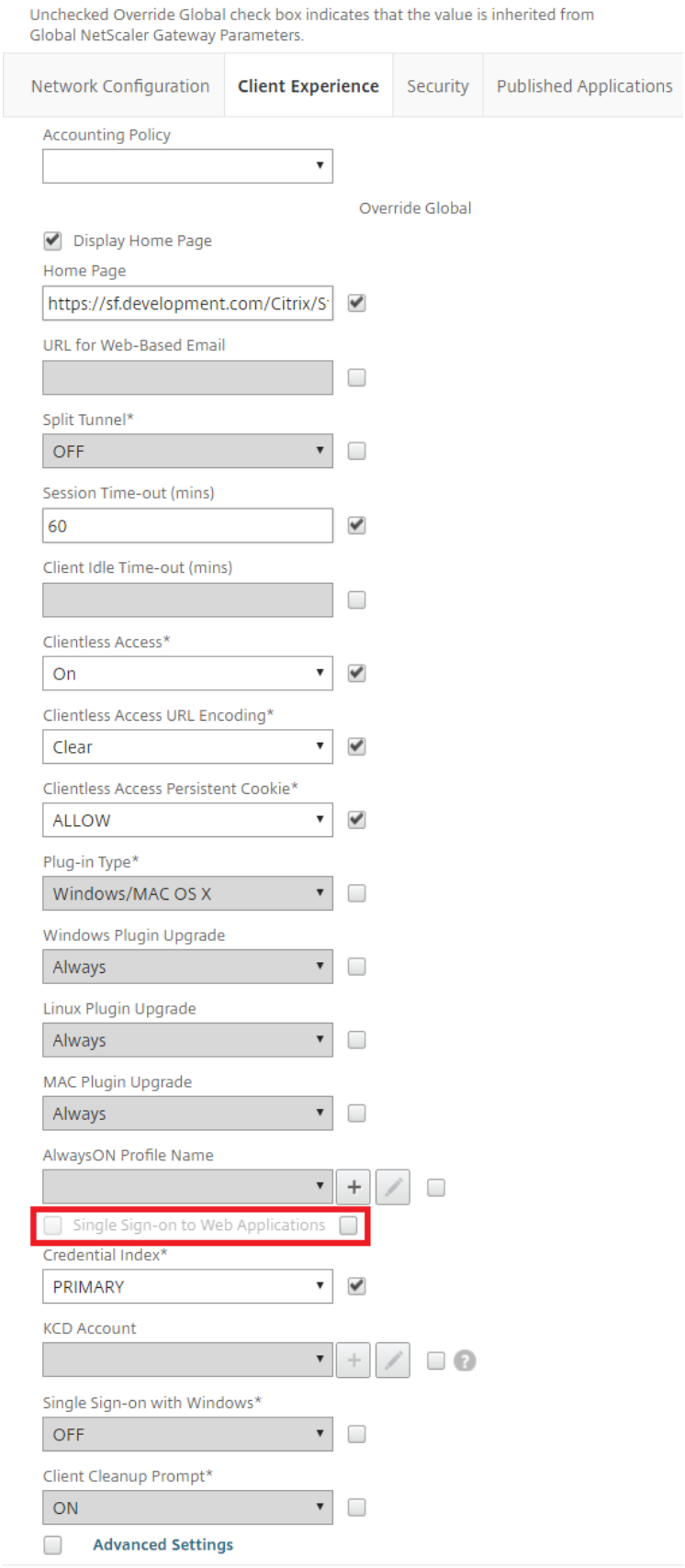


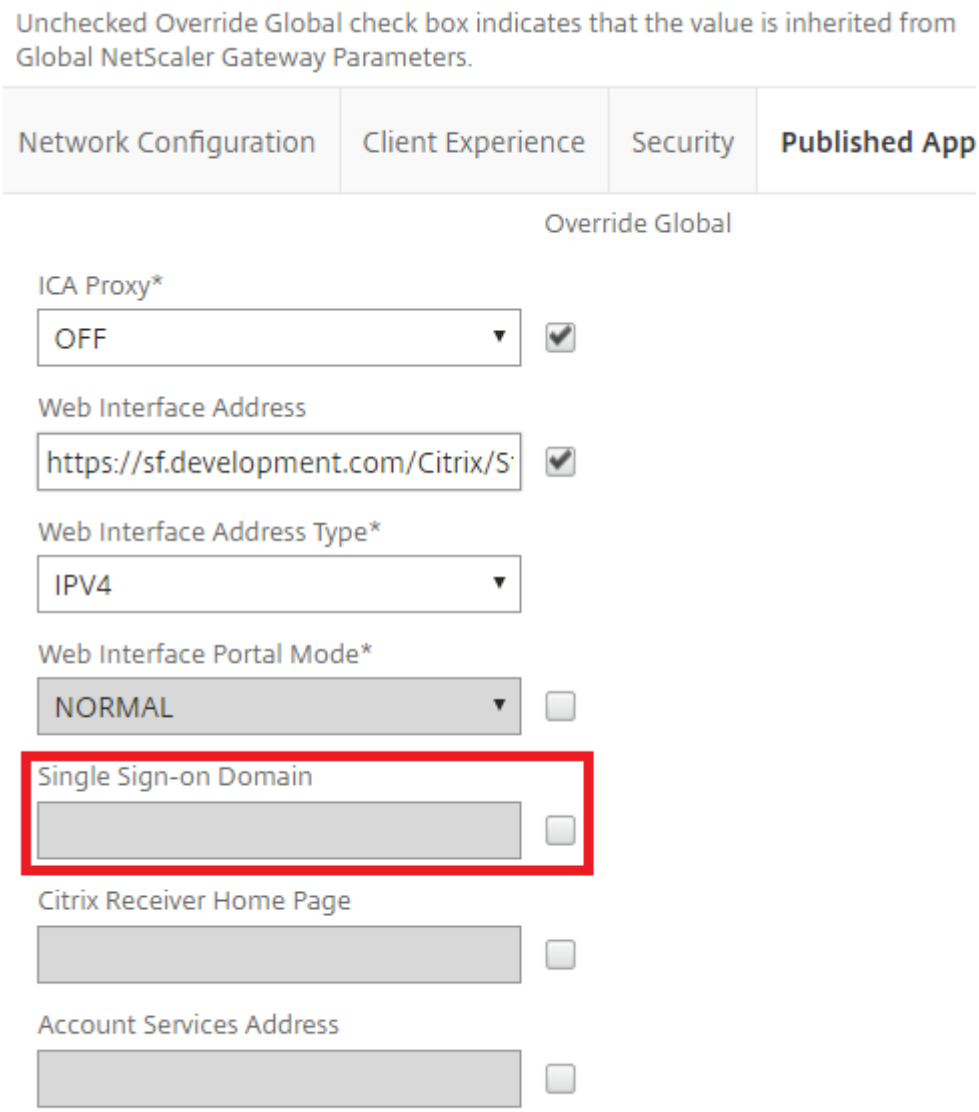


> **Nota:**
>
> En este caso de autenticación, no se recomienda que el explorador web tenga habilitado el almacenamiento en caché de las contraseñas. Si los usuarios tienen contraseñas diferentes para las dos cuentas de dominios distintos, el almacenamiento en caché de las contraseñas puede dar lugar a una mala experiencia del usuario.

Directiva de acción en la sesión de NetScaler

- Si se habilita el inicio Single Sign-On a aplicaciones web en la directiva de sesiones de Citrix Gateway, las credenciales incorrectas que envíe Citrix Gateway al sitio web se ignoran porque se inhabilitó el método de autenticación **PassThrough desde Citrix Gateway** en el sitio web. El sitio web solicita credenciales, independientemente de esta opción.
- Completar los datos de las entradas Single Sign-On en las fichas de experiencia de cliente y de aplicación publicada en Citrix Gateway no modifica el comportamiento que se describe en este artículo.





Configurar balizas

April 17, 2024

Utilice la tarea “Administrar balizas”para especificar las direcciones URL para utilizarlas como balizas. Estas URL pueden pertenecer tanto a la red interna como a la externa. La aplicación Citrix Workspace intenta comunicarse con las balizas y usa las respuestas para determinar si los usuarios están conectados a redes locales o públicas. Cuando un usuario accede a un escritorio o a una aplicación, la información de ubicación se transfiere al servidor que proporciona el recurso para que se puedan de-

volver los correspondientes datos de conexión a la aplicación Citrix Workspace. Esto garantiza que no se pida a los usuarios que vuelvan a iniciar sesión al acceder a un escritorio o a una aplicación.

Por ejemplo: si la baliza interna es accesible, esto indica que el usuario está conectado a la red local. Sin embargo, si la aplicación Citrix Workspace no puede ponerse en contacto con la baliza interna y recibe respuestas de las dos balizas externas, esto significa que el usuario tiene una conexión a Internet, pero está fuera de la red corporativa. Por lo tanto, el usuario tendrá que conectarse a escritorios y aplicaciones a través de Citrix Gateway. Cuando un usuario accede a un escritorio o aplicación, se notifica al servidor que proporciona el recurso para que proporcione la información del dispositivo Citrix Gateway a través del que debe redirigirse la conexión. Esto significa que el usuario no necesita iniciar sesión en el dispositivo para acceder al escritorio o a la aplicación.

De forma predeterminada, StoreFront establece:

- La baliza interna a la URL base de su implementación.
- Balizas externas a `http://ping.citrix.com` y la URL de la primera implementación de Citrix Gateway que agregue.

Si cambia una baliza, asegúrese de que los usuarios actualicen la aplicación Citrix Workspace con la información actualizada. Los usuarios pueden obtener un archivo de aprovisionamiento de la aplicación Citrix Workspace actualizado desde la aplicación Citrix Workspace para HTML5. De lo contrario, puede exportar un archivo de aprovisionamiento para el almacén y poner este archivo a disposición de los usuarios.

> Importante:
>
> En implementaciones con varios servidores, use solo un servidor a la vez para hacer cambios en la configuración del grupo de servidores. Compruebe que la consola de administración de Citrix StoreFront no se está ejecutando en ninguno de los demás servidores de la implementación. Una vez completados,
> propague los cambios de configuración al grupo de servidores de modo que los demás servidores de la implementación se actualicen.

1. Seleccione el nodo **Almacenes** en el panel izquierdo de la consola de administración de Citrix StoreFront y, en el panel Acciones, haga clic en **Administrar balizas**.
2. Especifique la URL que se utilizará como baliza interna.
   - Para usar la URL del servidor o la URL de equilibrio de carga de la implementación de StoreFront, seleccione **Usar URL de servicio**.
   - Para usar una URL alternativa, seleccione **Especificar dirección de baliza** y escriba una URL de alta disponibilidad que forme parte de la red interna.
3. Haga clic en **Agregar** para especificar la URL de una baliza externa. Para modificar una baliza, seleccione la URL de la lista Balizas externas y haga clic en **Modificar**. Seleccione una URL de la lista y haga clic en **Quitar** para dejar de utilizar esa dirección como baliza.

Debe especificar al menos dos balizas externas de alta disponibilidad que se pueden resolver desde redes públicas. Las direcciones URL de balizas deben ser nombres de dominio completos (`http://example.com`), no el nombre abreviado NetBIOS (`http://example`). Esto permite que la aplicación Citrix Workspace determine si los usuarios se encuentran en redes de Internet de pago, como las de un hotel o una cafetería con servicio de Internet. En tales casos, todas las balizas externas se conectan al mismo proxy.

> **Nota:**
>
> No use como baliza externa sitios web de terceros que no sean de su propiedad. En su lugar, use `http://ping.citrix.com` o sitios web controlados por su organización.

Crear un único nombre de dominio completo (FQDN) para acceder a un almacén de forma interna y externa

February 26, 2024

Puede crear un único nombre de dominio completo (FQDN) que pueda acceder a un almacén directamente desde su red corporativa y de forma remota a través de un dispositivo Citrix Gateway.

En este documento, utiliza como ejemplos:

- `https://storefront.example.com` como la URL única que utilizan los usuarios para acceder a StoreFront. Cuando está dentro de la red, se resuelve en el servidor de StoreFront o en el equilibrador de carga. Cuando está fuera de la red, se resuelve en la puerta de enlace.
- `https://storefrontcb.example.com` como la URL de respuesta. Esto se resuelve internamente en la puerta de enlace. Esto solo es necesario para el acceso inteligente o la autenticación sin contraseña. Debe asegurarse de que el certificado del dispositivo Gateway incluya esta dirección como SAN. Use un certificado comodín.

URL base del grupo de servidores

Cambie la URL base para que sea la URL única. Consulte Cambiar la dirección URL base de una implementación.

Balizas de StoreFront para la aplicación Citrix Workspace instalada localmente

La aplicación Citrix Workspace instalada localmente intenta comunicarse con las balizas y usa las respuestas para determinar si los usuarios están conectados a redes locales o públicas.

De forma predeterminada, StoreFront usa la URL base del grupo de servidores como URL de baliza interna. En esta configuración, la misma URL es válida tanto interna como externamente, por lo que no se puede usar como baliza. Por lo tanto, debe establecer la baliza interna en una URL que sepa que solo es accesible internamente.

Consulte Configurar baliza.

DNS externo

- storefront.example.com se resuelve en la IP externa del servidor virtual de Citrix Gateway.

DNS interno

- storefront.example.com recurre al equilibrador de carga de StoreFront o a la dirección IP única del servidor de StoreFront.
- storefrontcb.example.com se resuelve en la VIP de vServer de la puerta de enlace. Si existe un firewall entre la DMZ y la red local de la empresa, permítalo.

Exportar e importar la configuración de StoreFront

August 15, 2023

> Nota:
>
> Solo puede importar configuraciones de StoreFront que sean de la misma versión de StoreFront que la instalación de StoreFront de destino.

Puede exportar la configuración completa de una implementación de StoreFront. Esto incluye tanto implementaciones de un único servidor como implementaciones con un grupo de servidores. Si una implementación existente ya está presente en el servidor que realiza la importación, la configuración actual se borra y se sustituye por la configuración contenida en el archivo de copia de seguridad. Si el servidor de destino es una instalación limpia con los valores predeterminados de fábrica, se crea una implementación con la configuración importada almacenada en la copia de seguridad. La copia de seguridad de la configuración exportada es un archivo .zip único si no está cifrada, o un archivo .ctxzip si se eligió cifrar el archivo de copia de seguridad al crearlo.

Casos en los que se puede utilizar la exportación e importación de configuraciones

- Solo implementaciones de copia de seguridad de StoreFront en un estado de confianza y funcionamiento correcto. Cualquier cambio en la configuración requiere que se realice una nueva

copia de seguridad para reemplazar la anterior. No puede modificar las copias de seguridad existentes, ya que un hash del archivo backup.zip impide la modificación.
- Copia de seguridad ANTES de actualizar la versión de StoreFront a efectos de recuperación ante desastres.
- Clonación de implementaciones de prueba existentes de StoreFront para ponerlas en producción
- Creación de entornos de aceptación de usuarios mediante la clonación de implementaciones de producción en un entorno de prueba.
- Transferencia de StoreFront durante migraciones del sistema operativo, como la actualización del sistema operativo del host de Windows Server 2019 a Windows 2022. No se admiten las actualizaciones de versión locales del sistema operativo.
- Creación de grupos de servidores adicionales en implementaciones para múltiples regiones, como en grandes empresas con varios centros de datos.

Aspectos a tener en cuenta al importar y exportar una configuración de StoreFront

- ¿Está usando actualmente algún ejemplo de SDK de autenticación publicado de Citrix, por ejemplo, personalizaciones para autenticación con palabra mágica o para autenticación con productos de terceros? En ese caso, debe instalar esos paquetes en TODOS los servidores donde se importa la configuración ANTES de importar la configuración que contenga métodos de autenticación adicionales. La importación de la configuración falla si los paquetes del SDK de autenticación no están instalados en los servidores donde se importa la misma. Si importa una configuración en un grupo de servidores, instale los paquetes de autenticación en todos los miembros del grupo.
- Puede cifrar y descifrar los archivos de copia de seguridad. Los cmdlets PowerShell de importación y exportación admiten ambos casos de uso.
- Puede descifrar copias de seguridad cifradas (.ctxzip) más adelante, pero StoreFront no puede volver a cifrar archivos de copia de seguridad no cifrados (.zip). Si se requiere una copia de seguridad cifrada, realice la exportación de nuevo mediante un objeto de credenciales de PowerShell que contenga la contraseña que usted quiera.
- El ID de sitio del sitio web de IIS donde StoreFront está instalado actualmente (servidor de exportación) debe coincidir con el ID de sitio del sitio web de IIS de destino (servidor de importación) donde se quiere restaurar la copia de seguridad de la configuración de StoreFront.

Cmdlets de PowerShell

Export-STFConfiguration

Parámetro	Descripción
-TargetFolder (cadena)	La ruta de exportación al archivo de copia de seguridad. Ejemplo: "$env:userprofile\desktop\"
-Credential (PSCredential Object)	Especifica un objeto de credenciales para crear un archivo de copia de seguridad .ctxzip durante la exportación. El objeto de credenciales de PowerShell debe contener la contraseña que se usará para el cifrado y el descifrado. No use **-Credential** al mismo tiempo que el parámetro **-NoEncryption**. Ejemplo: $CredObject
-NoEncryption (conmutador)	Especifica que el archivo de copia de seguridad debe ser un archivo .zip no cifrado. No use **-NoEncryption** al mismo tiempo que el parámetro **-Credential**.
-ZipFileName (cadena)	El nombre del archivo de copia de seguridad de la configuración de StoreFront. No agregue ninguna extensión de archivo como .zip o .ctxzip. La extensión del archivo se agrega automáticamente dependiendo de si se especificó el parámetro **-Credential** o el parámetro **-NoEncryption** durante la exportación. Por ejemplo: "copiaSeguridad"
-Force (booleano)	Este parámetro sobrescribe automáticamente los archivos de copia de seguridad con el mismo nombre de archivo que los ya existentes en la ubicación de exportación especificada.

> **Importante:**
>
> El parámetro **-SiteID** de StoreFront 3.5 se retiró en la versión 3.6. Ya no es necesario especificar el ID de sitio **SiteID** cuando se realiza una importación, porque siempre se usará el parámetro SiteID contenido en el archivo de copia de seguridad. Asegúrese de que el ID de sitio coincide con el sitio web de StoreFront existente ya configurado dentro de IIS en el servidor de importación.NO se admite la importación de configuraciones de **SiteID 1** a **SiteID 2**.

Import-STFConfiguration

Parámetro	Descripción
-ConfigurationZip (cadena)	La ruta completa del archivo de copia de seguridad que quiere importar. Esto debe incluir la extensión del archivo. Use .zip para copias de seguridad no cifradas y .ctxzip para las cifradas. Ejemplo:`$env:userprofile\desktop\backup.ctxzip`
-Credential (PSCredential Object)	Especifique un objeto de credenciales para descifrar una copia de seguridad cifrada durante la importación. Ejemplo:`$CredObject`
-HostBaseURL (cadena)	Si se incluye este parámetro, se usará la URL base de host que usted especifique en lugar de usarse la URL base de host del servidor desde donde se realiza la exportación. Ejemplo:`https://<importingserver>.example.com`

Unprotect-STFConfigurationBackup

Parámetro	Descripción
-TargetFolder (cadena)	La ruta de exportación al archivo de copia de seguridad. Ejemplo:$env:userprofile\desktop
-Credential (PSCredential Object)	Use este parámetro para crear una copia no cifrada del archivo de copia de seguridad cifrado. Especifique el objeto de credenciales de PowerShell que contiene la contraseña que debe usarse para el descifrado. Ejemplo:`$CredObject`
-EncryptedConfigurationZip (cadena)	La ruta completa del archivo de copia de seguridad cifrado que quiere descifrar. Debe especificar la extensión de archivo .ctxzip. Ejemplo:`$env:userprofile\\desktop\\backup.ctxzip`

Parámetro	Descripción
-OutputFolder (cadena) -Force (booleano)	La ruta para crear una copia no cifrada (.zip) del archivo de copia de seguridad cifrado (.ctxzip). El archivo cifrado de copia de seguridad original se conserva para poder volver a utilizarlo. No especifique ningún nombre de archivo ni una extensión de archivo para la copia no cifrada. Ejemplo:$env:userprofile\desktop Este parámetro sobrescribe automáticamente los archivos de copia de seguridad con el mismo nombre de archivo que los ya existentes en la ubicación de exportación especificada.

Ejemplos de exportación e importación de configuraciones

Importar los cmdlets de StoreFront en la sesión actual de PowerShell

Abra el entorno ISE (Integrated Scripting Environment) de PowerShell en el servidor de StoreFront y ejecute:

```
1 $env:PSModulePath = [Environment]::GetEnvironmentVariable('PSModulePath
    ','Machine')
2 $SDKModules = 'C:\Program Files\Citrix\Receiver StoreFront\
    PowerShellSDK\Modules\Citrix.StoreFront'
3 Import-Module "$SDKModules\Citrix.StoreFront.psd1" -verbose
4 Import-Module "$SDKModules.Authentication\Citrix.StoreFront.
    Authentication.psd1" -verbose
5 Import-Module "$SDKModules.Roaming\Citrix.StoreFront.Roaming.psd1" -
    verbose
6 Import-Module "$SDKModules.Stores\Citrix.StoreFront.Stores.psd1" -
    verbose
7 Import-Module "$SDKModules.WebReceiver\Citrix.StoreFront.WebReceiver.
    psd1" -verbose
8 <!--NeedCopy-->
```

Casos de un solo servidor

Crear una copia de seguridad no cifrada de una configuración existente en el Servidor A y restaurarla sobre la misma implementación Exporte la configuración del servidor del que quiere realizar una copia de seguridad.


```
Export-STFConfiguration -targetFolder "$env:userprofile\desktop" -
    zipFileName "backup" -NoEncryption
<!--NeedCopy-->
```

Copie el archivo backup.zip en una ubicación segura. Puede utilizar esta copia de seguridad para recuperación ante desastres a fin de restaurar el servidor a su estado anterior.

```
Import-STFConfiguration -configurationZip "$env:userprofile\desktop\
    backup.zip" -HostBaseURL "https://storefront.example.com"
<!--NeedCopy-->
```

Realizar una copia de seguridad de una configuración existente en el servidor A y restaurarla en el servidor B para crear un clon de un servidor existente Exporte la configuración del servidor del que quiere realizar una copia de seguridad.

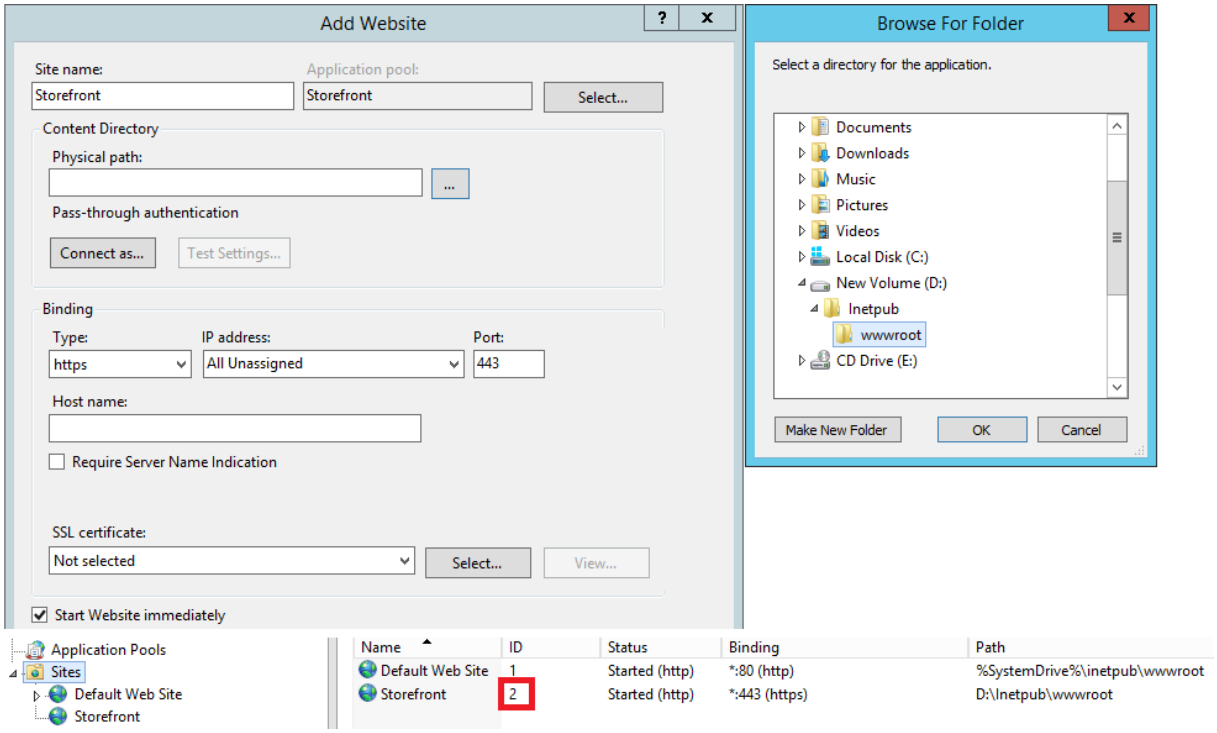
```
Export-STFConfiguration -targetFolder "$env:userprofile\desktop" -
    zipFileName "backup" -NoEncryption
<!--NeedCopy-->
```

Copie el archivo backup.zip en el escritorio del servidor B.

```
Import-STFConfiguration -configurationZip "$env:userprofile\desktop\
    backup.zip" -HostBaseURL "https://serverB.example.com"
<!--NeedCopy-->
```

StoreFront ya está implementado en un sitio web IIS personalizado. Restaurar la configuración en otra implementación de sitio web personalizado El servidor A tiene StoreFront implementado en una ubicación de sitio web personalizada, en lugar de ubicarse en el sitio web predeterminado de IIS. El ID de sitio de IIS para el segundo sitio web creado en IIS es 2. La ruta física del sitio web de StoreFront puede estar en otra unidad no perteneciente al sistema, como D:\, o en la unidad predeterminada del sistema C:\, pero debe usar un ID de sitio de IIS mayor que 1.

Se ha configurado un nuevo sitio web llamado StoreFront dentro de IIS, que usa **SiteID = 2**. StoreFront ya está implementado en el sitio web personalizado y su ruta física se encuentra en la unidad `d:\inetpub\wwwrooot`.



1. Exportar una copia de la configuración del servidor A.
2. En el Servidor B, configure IIS con un nuevo sitio web llamado **StoreFront**, que también usa **SiteID 2**.
3. Importar la configuración del Servidor A en el Servidor B. El ID de sitio que contiene la copia de seguridad es el ID que se utiliza y debe coincidir con el sitio web de destino donde se quiere importar la configuración de StoreFront.

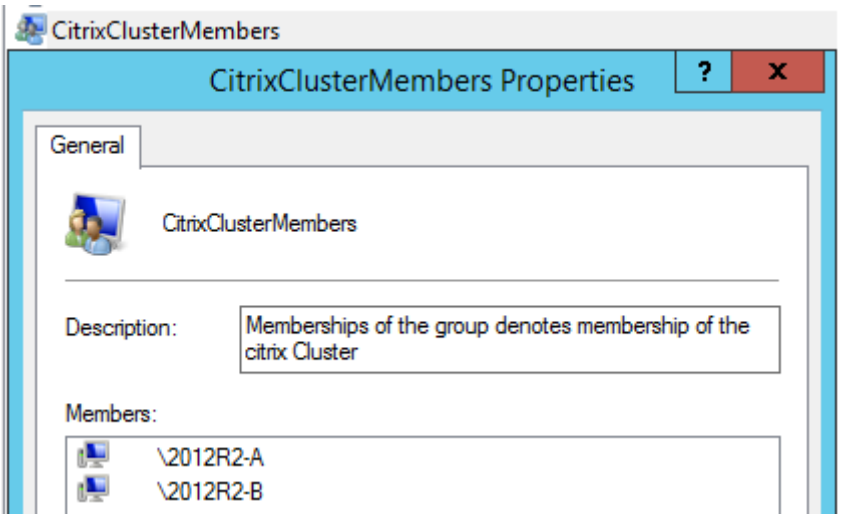
```
Import-STFConfiguration -configurationZip "$env:userprofile\
    desktop\backup.ctxzip" -HostBaseURL "https://serverB.example.
    com"
<!--NeedCopy-->
```

Casos de grupos de servidores

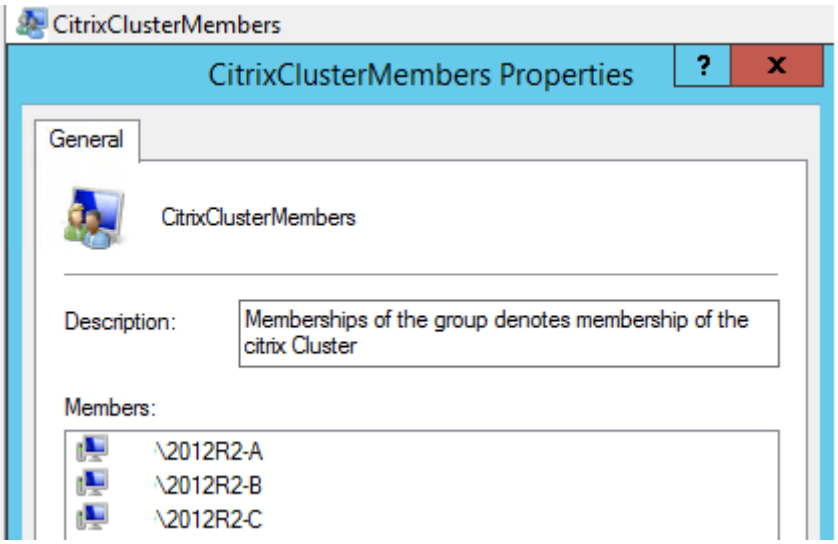
Caso 1: Hacer una copia de seguridad de la configuración de un grupo de servidores y restaurarla más tarde en la implementación del mismo grupo de servidores Anteriormente se hizo una copia de seguridad de la configuración, cuando el grupo de servidores solo tenía dos servidores de StoreFront, 2012R2-A y 2012R2-B. En el archivo de la copia de seguridad, dispone de un registro de **CitrixClusterMembership**. Este registro contiene el momento en el que se realizó la copia de seguridad con los dos servidores originales 2012R2-A y 2012R2-B. Posteriormente a la creación de esa copia de seguridad original, la implementación del grupo de servidores de StoreFront ha aumentado de tamaño y se ha agregado un nodo 2012R2-C al grupo de servidores. La configuración de StoreFront

subyacente del grupo de entrega que está guardada en la copia de seguridad no ha cambiado. La entrada de miembros del grupo CitrixClusterMembership de tres servidores debe conservarse, aunque se importe la antigua copia de seguridad que contiene solo los dos nodos originales del grupo de servidores. Durante la importación, se conserva la información de miembros del clúster CitrixClusterMembership y luego se vuelve a copiar, una vez que la configuración se haya importado correctamente en el servidor principal. La importación también conserva la información de miembros del clúster CitrixClusterMembership aunque se hayan quitado nodos del grupo de servidores posteriormente a la creación de la copia de seguridad original.

1. Exporte la configuración del grupo de servidores 1 desde 2012R2-A, que es el servidor principal utilizado para administrar todo el grupo de servidores.



2. Más tarde, se agrega un servidor adicional, 2012R2-C al grupo de servidores existente.



3. La configuración del grupo de servidores debe restaurarse a un estado de funcionamiento correcto previo conocido. StoreFront hace una copia de seguridad del clúster actual CitrixCluster-

Membership de tres servidores durante el proceso de importación, y luego la restaura, una vez completada correctamente la importación.

4. Importe la configuración del grupo de servidores 1 de vuelta en el nodo 2012R2-A.

```
Import-STFConfiguration -configurationZip "$env:userprofile\
    desktop\backup.ctxzip" -HostBaseURL "https://servergroup1.
    example.com"
<!--NeedCopy-->
```

5. Propague la configuración recién importada en todo el grupo de servidores, de modo que los servidores tengan una configuración uniforme después de la importación.

Caso 2: Hacer una copia de seguridad de una configuración existente desde el grupo de servidores 1 y usarla para crear un nuevo grupo de servidores en una instalación diferente predeterminada de fábrica. A continuación, se pueden agregar nuevos servidores miembros de grupo al nuevo servidor principal Se crea el grupo de servidores 2, que contiene dos servidores nuevos: 2012R2-C y 2012R2-D. La configuración del grupo de servidores 2 se basará en la configuración de una implementación existente, la del grupo de servidores 1, que también contiene dos servidores: 2012R2-A y 2012R2-B. El clúster CitrixClusterMembership contenido en el archivo de copia de seguridad no se usa al crear un nuevo grupo de servidores. Siempre se hace una copia de seguridad del clúster CitrixClusterMembership actual y luego se restaura después de una importación correcta. Al crear una implementación con una configuración importada, el grupo de seguridad de CitrixClusterMembership solo contiene el servidor que recibe la importación hasta que se agregan servidores adicionales al grupo. El grupo de servidores 2 es una nueva implementación que va a coexistir con el grupo de servidores 1. Especifique el parámetro -HostBaseURL. El grupo de servidores 2 se creará con una instalación de StoreFront limpia que tiene los valores predeterminados de fábrica.

1. Exporte la configuración del grupo de servidores 1 desde 2012R2-A, que es el servidor principal utilizado para administrar todo el grupo de servidores.

2. Importe la configuración del grupo de servidores 1 en el nodo 2012R2-C, que será el servidor principal utilizado para administrar todo el grupo de servidores 2 recién creado.

```
Import-STFConfiguration -configurationZip "$env:userprofile\
    desktop\backup.ctxzip" -HostBaseURL "https://servergroup2.
    example.com"
<!--NeedCopy-->
```

3. Incorpore servidores adicionales que formarán parte de la nueva implementación del grupo de servidores 2. La propagación de la configuración recién importada desde el grupo de servidores 1 a todos los nuevos miembros del grupo de servidores 2 es automática, ya que esto forma parte del proceso normal de incorporación de nuevos servidores a un grupo.

Caso 3: Hacer una copia de seguridad de una configuración existente desde el grupo de servidores 1 y usarla para sobrescribir la configuración existente del grupo de servidores 2 El grupo de servidores 1 y el grupo de servidores 2 ya existen, y están en dos centros de datos distintos. Se han hecho muchos cambios en la configuración de StoreFront del grupo de servidores 1 y deben aplicarse al grupo de servidores 2 situado en el otro centro de datos. Estos cambios pueden transferirse del grupo de servidores 1 al grupo de servidores 2. No use la información de **CitrixClusterMembership** contenida en el archivo de copia de seguridad en el grupo de servidores 2. Especifique el parámetro **-HostBaseURL** durante la importación, ya que la URL base de host del grupo de servidores 2 no debe cambiarse por el mismo FQDN que usa el grupo de servidores 1. El grupo de servidores 2 es una implementación existente.

1. Exporte la configuración del grupo de servidores 1 desde 2012R2-A, que es el servidor principal utilizado para administrar todo el grupo de servidores.
2. Importe la configuración del grupo de servidores 1 en el nodo 2012R2-C que tiene la instalación predeterminada de fábrica, y será el servidor principal utilizado para el grupo de servidores 2.

```
Import-STFConfiguration -configurationZip "$env:userprofile\
    desktop\backup.zip" -NoEncryption -HostBaseURL "https://
    servergroup2.example.com"
<!--NeedCopy-->
```

Crear una copia de seguridad cifrada de la configuración del servidor

Un objeto de credenciales de PowerShell se compone de un nombre de usuario y una contraseña de una cuenta de Windows. Los objetos de credenciales de PowerShell garantizan que su contraseña queda protegida en memoria.

> **Nota:**
>
> Para cifrar un archivo de copia de seguridad de configuración, necesita solo la contraseña para realizar el cifrado y el descifrado. El nombre de usuario guardado con el objeto de credenciales no se usa. Debe crear un objeto de credenciales que contenga la misma contraseña dentro de la sesión de PowerShell que se utiliza en los servidores de exportación y de importación. Dentro del objeto de credenciales puede especificar cualquier usuario.

PowerShell requiere la especificación de un usuario al crear un nuevo objeto de credenciales. Este ejemplo de código obtiene el usuario de Windows de la sesión actual.

Cree un objeto de credenciales de PowerShell dentro de su sesión de PowerShell en el servidor de exportación.

```
$User = [System.Security.Principal.WindowsIdentity]::GetCurrent().Name
$Password = "Pa55w0rd"
$Password = $Password | ConvertTo-SecureString -asPlainText -Force
```



```
$CredObject = New-Object System.Management.Automation.PSCredential(
    $User,$Password)
<!--NeedCopy-->
```

Exporte la configuración al archivo backup.ctxzip, que es un archivo zip cifrado.

```
Export-STFConfiguration -targetFolder "$env:userprofile\desktop" -
    zipFileName "backup" -Credential $CredObject
<!--NeedCopy-->
```

Cree un objeto de credenciales de PowerShell idéntico dentro de su sesión de PowerShell en el servidor de importación.

```
Import-STFConfiguration -configurationZip "$env:userprofile\desktop\
    backup.ctxzip" -Credential $CredObject -HostBaseURL "https://
    storefront.example.com"
<!--NeedCopy-->
```

Desproteger un archivo cifrado de copia de seguridad existente

```
$User = [System.Security.Principal.WindowsIdentity]::GetCurrent().Name
$Password = "Pa55w0rd"
$Password = $Password | ConvertTo-SecureString -asPlainText -Force
$CredObject = New-Object System.Management.Automation.PSCredential(
    $User,$Password)

Unprotect-STFConfigurationExport -encryptedConfigurationZip "$env:
    userprofile\desktop\backup.ctxzip" -credential $CredObject -
    outputFolder "c:\StoreFrontBackups" -Force
<!--NeedCopy-->
```

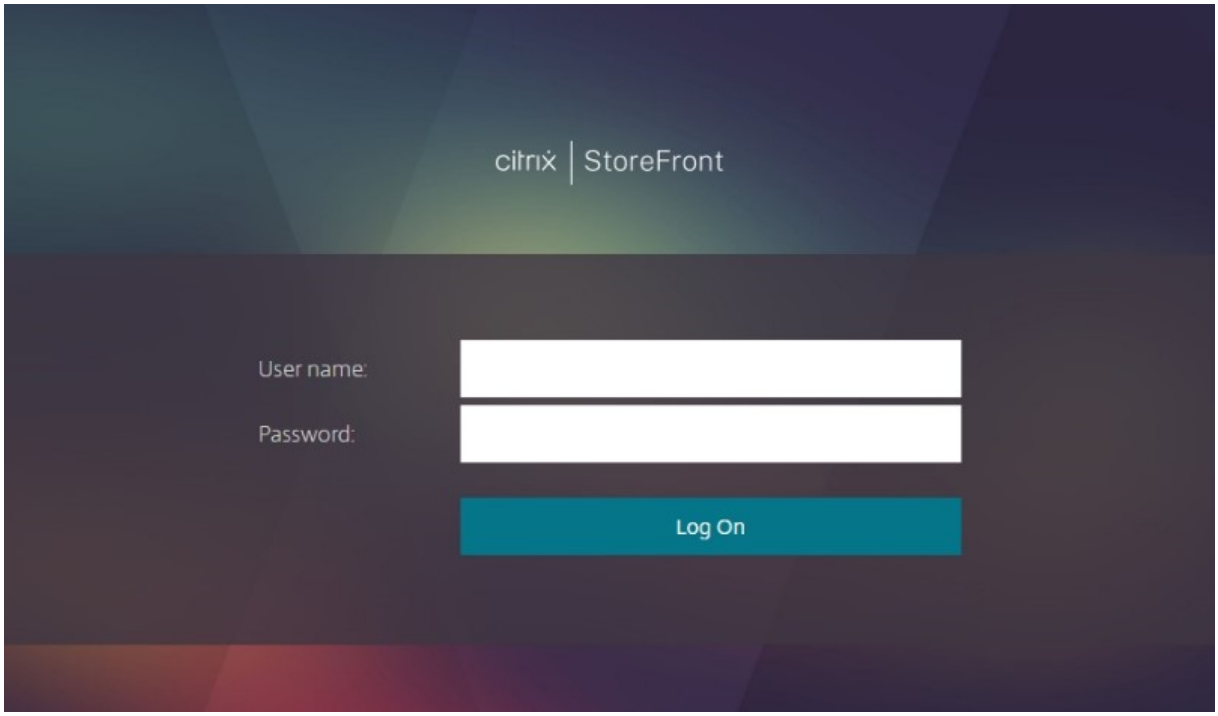
Guía para usuarios finales

December 4, 2023

En esta sección se describen las funciones y el aspecto de un almacén cuando se ve a través de un explorador web o a través de la aplicación Citrix Workspace.

Iniciar sesión

Según el método de autenticación y si Single Sign-On está habilitado, es posible que deba iniciar sesión.

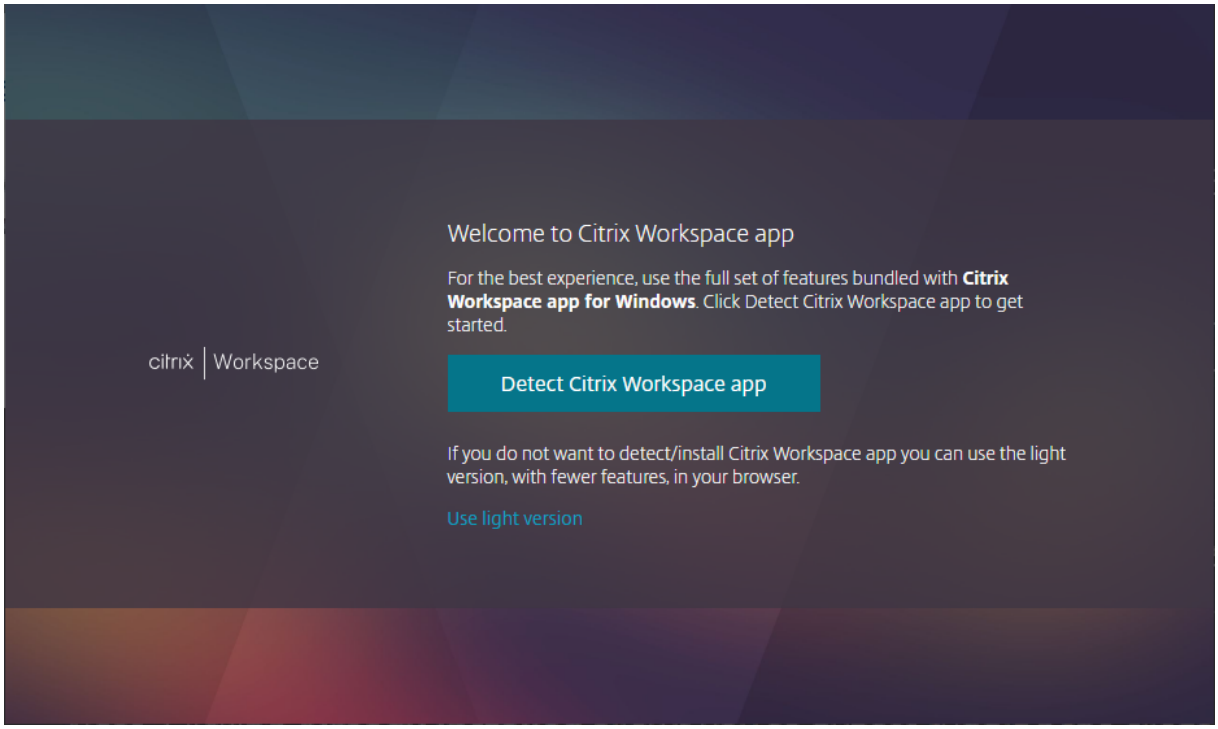


Detección de la aplicación Citrix Workspace

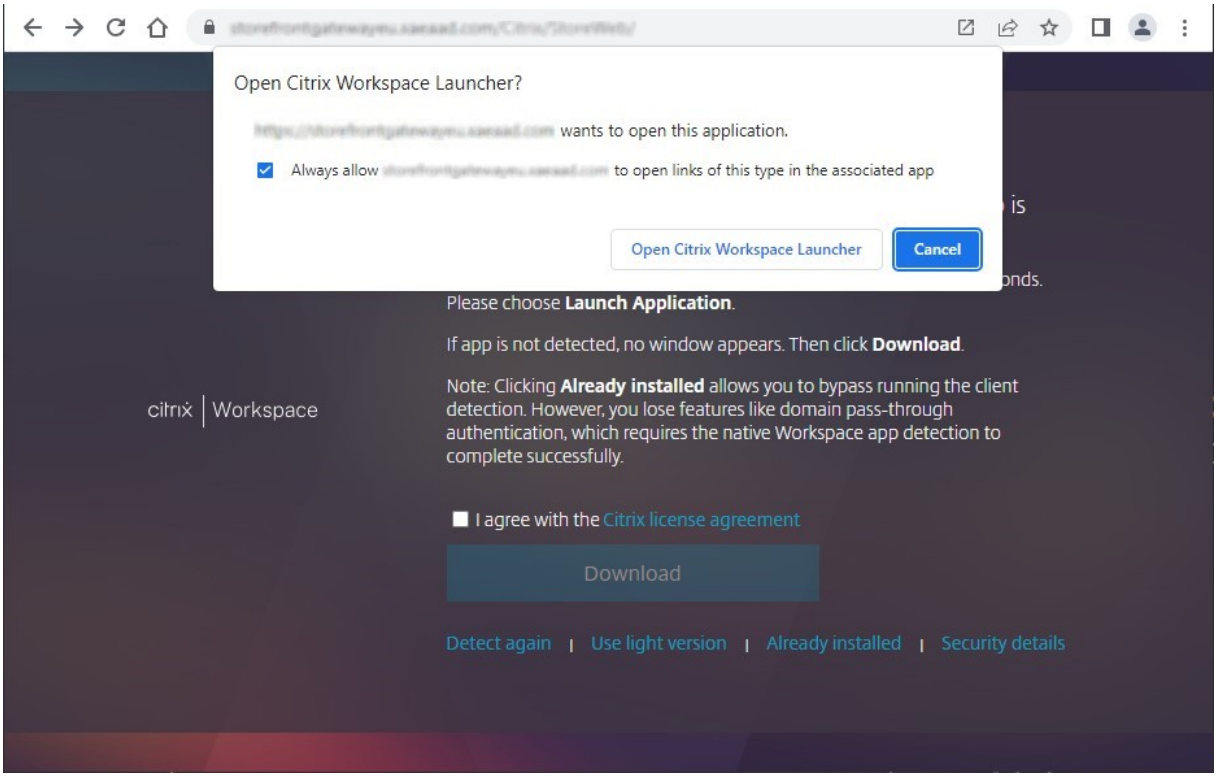
> **Nota:**
>
> Este paso solo se aplica al acceder al almacén a través de un explorador web, no a través de la aplicación Citrix Workspace instalada localmente. Este paso puede realizarse antes o después del inicio de sesión, según la configuración.

Según la configuración, al acceder al almacén a través de un explorador web por primera vez o después de borrar las cookies, es posible que aparezca la pantalla **Le damos la bienvenida a la aplicación Citrix Workspace**. Puede elegir entre:

- Haga clic en **Detectar la aplicación Citrix Workspace** si quiere iniciar recursos en la aplicación Citrix Workspace instalada localmente. Esto se recomienda para disfrutar de una experiencia óptima.
- Haga clic en **Usar versión simplificada** (si está disponible) para iniciar recursos siempre en el explorador web.



Al hacer clic en **Detectar la aplicación Citrix Workspace**, intenta detectar una aplicación Citrix Workspace instalada localmente. En primer lugar, intenta utilizar las extensiones web de Citrix Workspace. Si no está instalada o no detecta la aplicación Citrix Workspace instalada localmente, intenta abrir **Citrix Workspace Launcher**, que es un componente de la aplicación Citrix Workspace. Si la aplicación Citrix Workspace está instalada, su explorador web abrirá una ventana, en la que se le solicitará que ejecute **Citrix Workspace Launcher**. Haga clic en **Abrir Citrix Workspace Launcher** o en **Abrir enlace** (según el explorador). Se recomienda marcar también la casilla para **permitir siempre que el *dominio* abra enlaces de este tipo en la aplicación asociada** para evitar que esta ventana aparezca cada vez que inicie un recurso.



Si se detecta una aplicación Citrix Workspace instalada localmente, pasa a la siguiente pantalla unos segundos después. Al iniciar un recurso posteriormente, utilizará las extensiones web de Citrix Workspace o Citrix Workspace Launcher, según lo que se haya detectado, para abrir recursos en la aplicación Citrix Workspace instalada localmente.

Si la aplicación Citrix Workspace no está instalada o cancela el Launcher, según la configuración, tendrá estas opciones:

- **Descargar**: Descarga la aplicación Citrix Workspace del sitio web de Citrix o del servidor de StoreFront. Tras instalar la aplicación Citrix Workspace, haga clic en **Detectar de nuevo**.
- **Detectar de nuevo**: Intenta detectar de nuevo la aplicación Citrix Workspace instalada localmente.
- **Usa versión simplificada**: Omite la detección de la aplicación Workspace y siempre abre recursos en su explorador web.
- **Ya instalado**: Use esta opción si tiene instalada una versión antigua de Citrix Receiver que no es compatible con Citrix Workspace Launcher ni con extensiones web de Citrix Workspace. Si selecciona esta opción, al iniciar una aplicación o un escritorio virtual, el explorador descarga un archivo **launch.ica** que puede abrir con Citrix Receiver. Esta opción reduce la funcionalidad, por lo que no se recomienda.

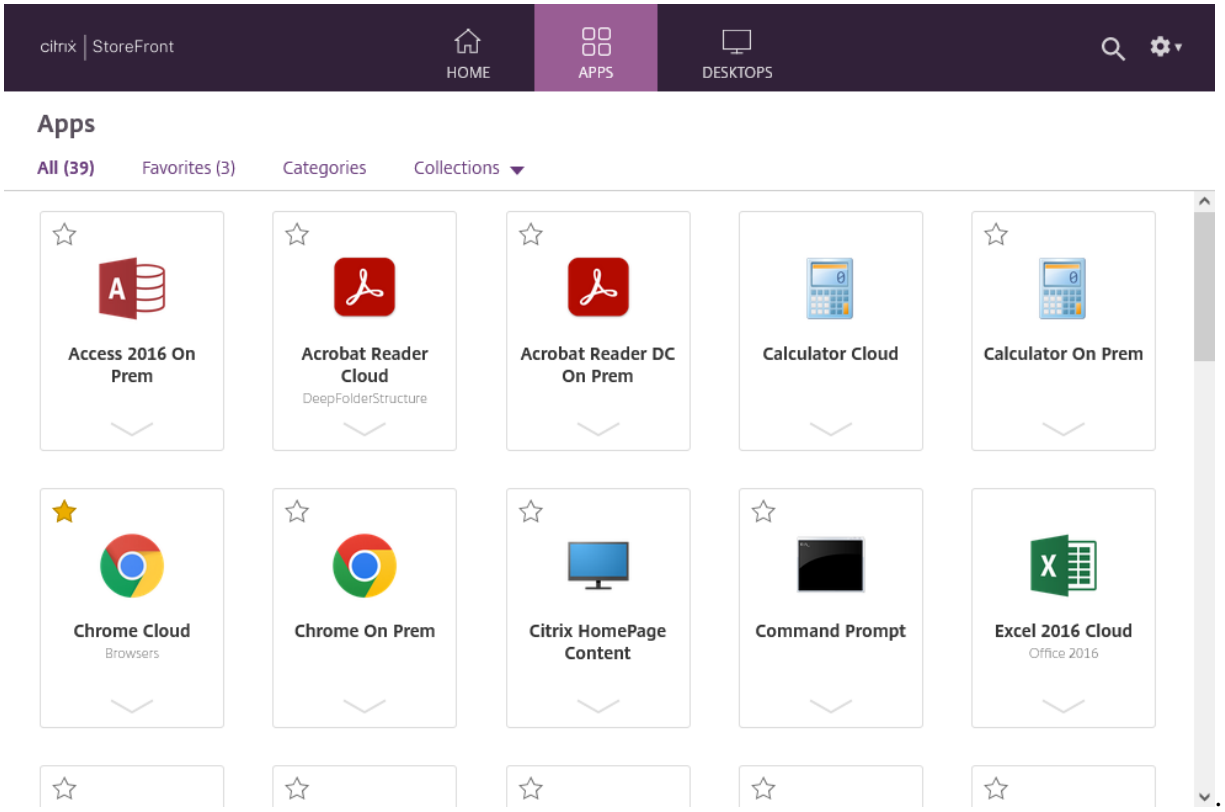
Ficha Inicio

La ficha **Inicio** muestra todos los grupos de aplicaciones destacadas junto con aplicaciones y escritorios favoritos u obligatorios. La ficha **Inicio** solo se muestra si los favoritos están habilitados para el almacén.

Ficha Aplicaciones

La ficha **Aplicaciones** tiene varias vistas secundarias:

- **Todas**: Muestra todas las aplicaciones.
- **Favoritos**: Muestra todas las aplicaciones favoritas.
- **Categorías**: Muestra las categorías y las aplicaciones dentro de esas categorías. La forma en que se muestran las categorías depende de los Parámetros de categoría.
- **Colecciones**: Muestra los grupos de aplicaciones destacadas.



Ficha Escritorios

La ficha **Escritorios** tiene dos vistas secundarias:

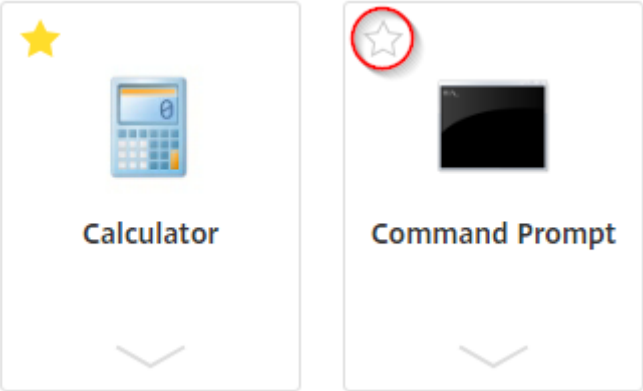
- **Todos**: Muestra todos los escritorios.
- **Favoritos**: Muestra sus escritorios favoritos.

Mosaicos de aplicaciones y escritorios

Haga clic en un icono para iniciar la aplicación o el escritorio.

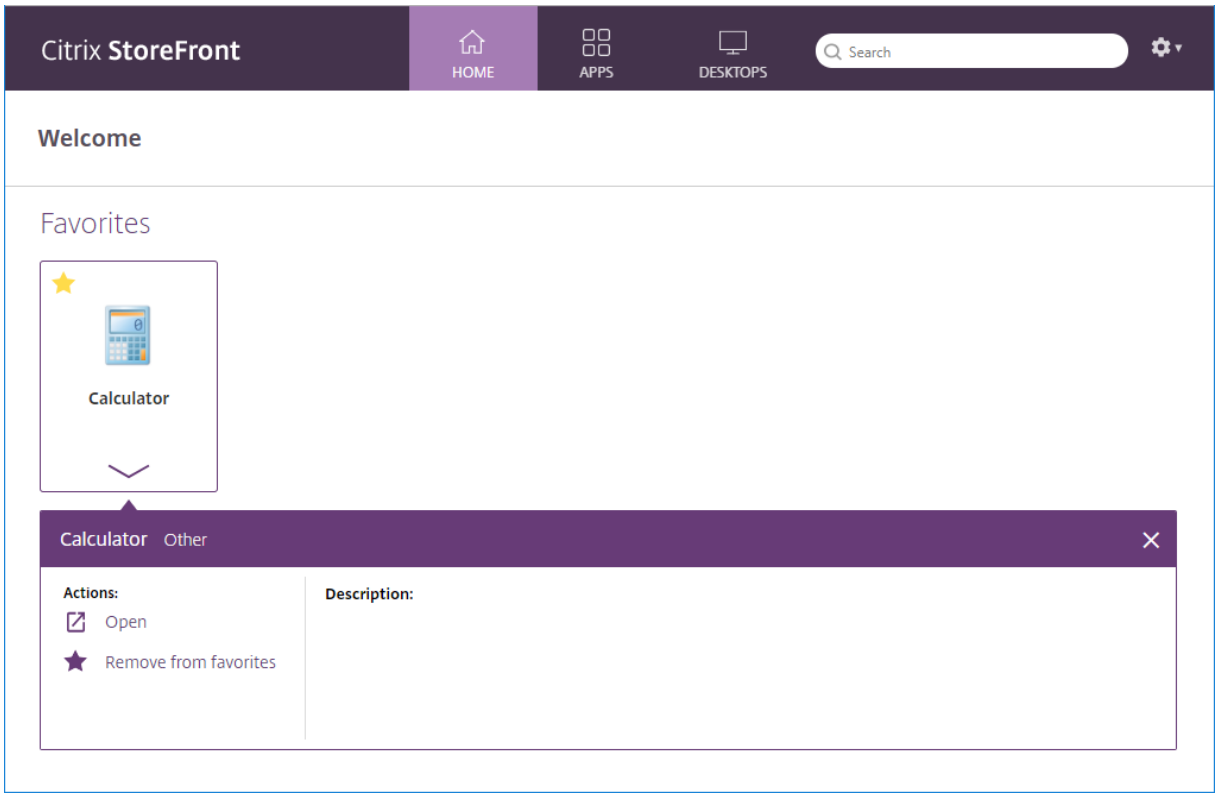
Favoritos

Haga clic o toque en la estrella para convertir un elemento en favorito:



Ver detalles y acciones

Puede expandir un panel debajo de cada icono para mostrar la descripción y las acciones de la aplicación.



Es posible que estén disponibles estas acciones:

- **Abrir**: Inicia la aplicación o el escritorio o se conecta de nuevo a ellos.
- **Agregar a favoritos**: Si el elemento no es uno de sus favoritos, no es obligatorio y los favoritos están habilitados en el almacén, se agrega la aplicación o el escritorio a sus favoritos.

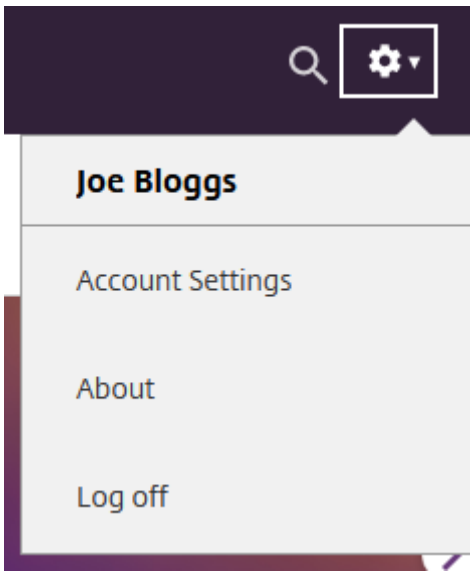
- **Quitar de favoritos**: Si el elemento es un favorito, no es obligatorio y los favoritos están habilitados en el almacén, quita la aplicación o el escritorio de sus favoritos.
- **Reiniciar**: Para los escritorios asignados en los que el reinicio esté disponible, esta opción reinicia el escritorio.

Buscar

Haga clic en el icono de la lupa para abrir el cuadro de búsqueda. Busque en todas las aplicaciones, escritorios y categorías:

Parámetros

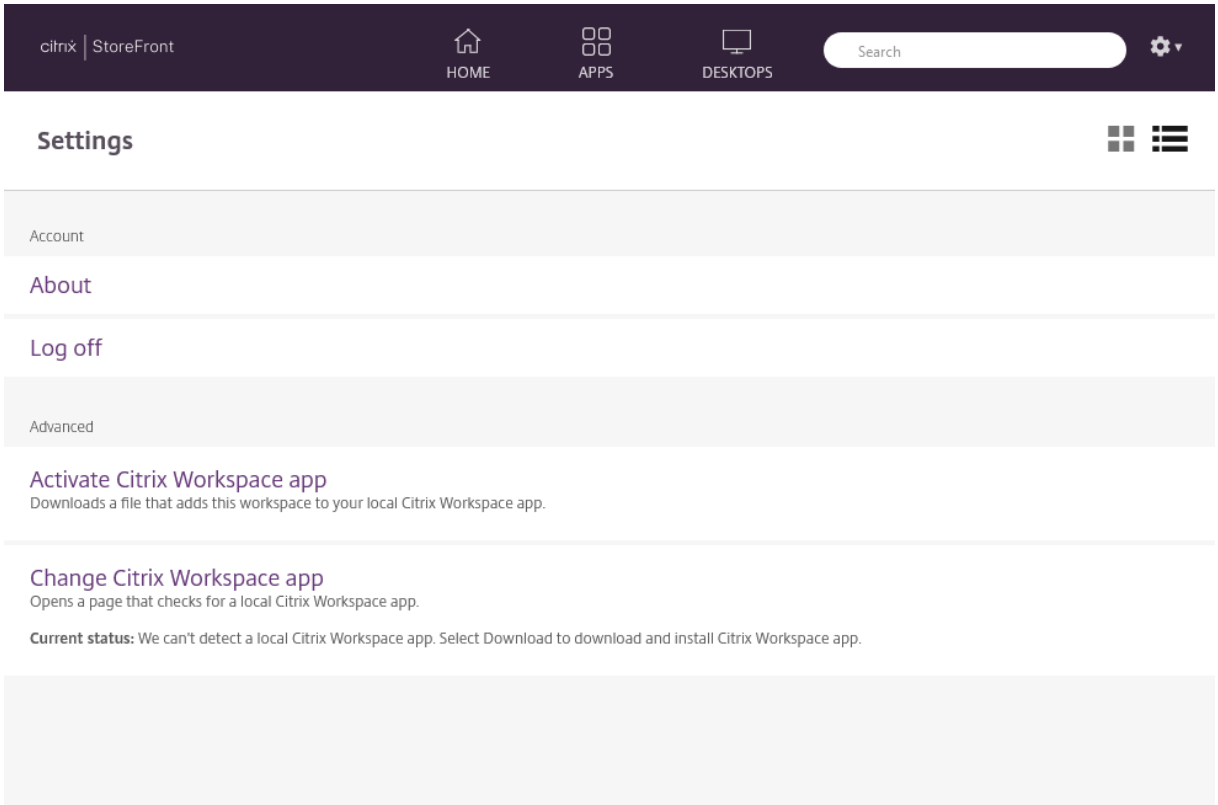
El menú de parámetros solo está disponible cuando se accede al almacén a través de un explorador web.



El menú de parámetros tiene estas opciones:

- **Parámetros de cuenta**: Abre la página de parámetros.
- **Acerca de**: Muestra información sobre la aplicación.
- **Cerrar sesión**: Cierra sesión en el sitio web.

Parámetros de cuenta



Es posible que estén disponibles estas opciones:

Conectar. Reanuda las sesiones desconectadas.

Desconectar. Desconecta todas las sesiones actuales y cierra la sesión.

Activar la aplicación Citrix Workspace. Descarga un archivo que agrega este almacén a la aplicación Citrix Workspace local.

Cambiar la aplicación Citrix Workspace. Abre una página que busca una aplicación Citrix Workspace instalada localmente. También permite a los usuarios cambiar entre iniciar recursos mediante la aplicación Citrix Workspace instalada localmente o iniciarlos en un explorador web.

Cerrar sesión

Para cerrar sesión, abra el menú de parámetros y haga clic en **Cerrar sesión**. Esto le desconecta del almacén. Si se ha conectado a algún recurso, según la configuración, podrá:

- Cerrar los recursos.
- Desconectarse de los recursos.
- Dejar los recursos conectados.

SDK de StoreFront

April 17, 2024

Citrix StoreFront proporciona un SDK basado en una serie de módulos de Microsoft Windows PowerShell 2.0. Con el SDK, se pueden realizar las mismas tareas que se llevan a cabo con la consola MMC de StoreFront, junto con otras tareas que no se pueden realizar con la consola.

> **Nota:**
>
> El SDK de PowerShell no es compatible con PowerShell 6 o superior.

Para la referencia del SDK, consulte SDK de StoreFront.

Uso de SDK

El SDK se compone de una serie de complementos de PowerShell que el asistente de instalación instala automáticamente cuando se instalan y se configuran varios componentes de StoreFront.

Para acceder a los cmdlets y ejecutarlos:

1. Inicie una línea de comandos de PowerShell o **ISE de Windows PowerShell** como administrador.

   Debe ejecutar el shell o el script con una cuenta miembro del grupo de administradores locales en el servidor de StoreFront.

2. Para utilizar los cmdlets del SDK en scripts, configure la directiva de ejecución en PowerShell.

   Para obtener más información acerca de la directiva de ejecución de PowerShell, consulte la documentación de Microsoft.

3. Agregue los módulos que necesite al entorno de PowerShell con el comando **Add -Module** en la consola de Windows PowerShell. Por ejemplo, escriba:

   ```
   Import-Module Citrix.StoreFront
   ```

   Para importar todos los cmdlets, escriba:

   ```
   Get-Module -ListAvailable | Where-Object { $_.Name.StartsWith("
   Citrix.StoreFront")} | Import-Module
   ```

Después de realizar la importación, tendrá acceso a los cmdlets y a la ayuda asociada.

Introducción al SDK

Para crear un script, siga los siguientes pasos:

1. Tome uno de los ejemplos del SDK instalado por StoreFront en la carpeta **%ProgramFiles%\Citrix\Receiver StoreFront\PowerShellSDK\Examples**.
2. Para ayudarle a personalizar su propio script, consulte el script de ejemplo para comprender lo que hace cada parte. Para obtener más información, consulte el caso de uso de ejemplo que describe con más detalle las acciones del script.
3. Adapte los scripts de ejemplo para convertirlos en scripts más útiles para su consumo. Para hacerlo:
    - Use PowerShell ISE o una herramienta similar para modificar el script.
    - Utilice variables para asignarles valores que se van a volver a utilizar o modificar.
    - Elimine los comandos que no sean necesarios.
    - Observe que los cmdlets de StoreFront se pueden identificar por el prefijo STF.
    - Use el cmdlet **Get-Help** con el nombre de un cmdlet y el parámetro **-Full** para obtener más información acerca de un comando en concreto.

Ejemplos

> **Nota:**
>
> Al crear un script, para asegurarse de obtener siempre las mejoras y revisiones más recientes, Citrix recomienda seguir el procedimiento descrito en este tema en lugar de copiar y pegar el script de ejemplo.

Ejemplos	Descripción
Crear una implementación simple	Script: crea una implementación simple de StoreFront con un controlador configurado con un único servidor XenDesktop.
Crear una implementación para acceso remoto	Script: Se basa en el script anterior y agrega acceso remoto a la implementación.
Crear una implementación para acceso remoto con una puerta de enlace óptima	Script: Se basa en el script anterior y agrega puertas de enlace preferidas óptimas para mejorar la experiencia del usuario.

Ejemplo: Crear una implementación simple

El siguiente ejemplo muestra cómo crear una implementación simple configurada con un Controller de XenDesktop.

Antes de comenzar, asegúrese de seguir los pasos detallados en Introducción a SDK. Este ejemplo se puede personalizar con los métodos descritos para generar un script que automatice la implementación de StoreFront.

> **Nota:**
>
> Para asegurarse de que siempre obtiene las últimas mejoras y revisiones, Citrix recomienda seguir el procedimiento descrito en este documento en lugar de copiar y pegar el script de ejemplo.

Entender el script Esta sección explica qué hace cada parte del script generado por StoreFront. Esto le ayudará con la personalización de su propio script.

- Establece los requisitos para la gestión de errores e importa los módulos de StoreFront necesarios. La importación no es necesaria en versiones más nuevas de PowerShell.

```
1  Param(
2      [Parameter(Mandatory=$true)]
3      [Uri]$HostbaseUrl,
4      [long]$SiteId = 1,
5      [ValidateSet("XenDesktop","XenApp","AppController","VDIinaBox
          ")]
6      [string]$Farmtype = "XenDesktop",
7      [Parameter(Mandatory=$true)]
8      [string[]]$FarmServers,
9      [string]$StoreVirtualPath = "/Citrix/Store",
10     [bool]$LoadbalanceServers = $false,
11     [int]$Port = 80,
12     [int]$SSLRelayPort = 443,
13     [ValidateSet("HTTP","HTTPS","SSL")]
14     [string]$TransportType = "HTTP"
15     )
16     # Import StoreFront modules. Required for versions of
          PowerShell earlier than 3.0 that do not support
          autoloading
17     Import-Module Citrix.StoreFront
18     Import-Module Citrix.StoreFront.Stores
19     Import-Module Citrix.StoreFront.Authentication
20     Import-Module Citrix.StoreFront.WebReceiver
21 <!--NeedCopy-->
```

- Automatiza la ruta virtual de los servicios de autenticación y Citrix Receiver para Web basándose en la ruta **$StoreVirtualPath** proporcionada. **$StoreVirtualPath** equivale a **$StoreIISpath** porque las rutas virtuales siempre son la ruta de IIS. Por lo tanto, en PowerShell tienen un

valor como “/Citrix/Store”, “/Citrix/StoreWeb”o “/Citrix/StoreAuth”.

```
# Determine the Authentication and Receiver virtual path to use based of the Store
$authenticationVirtualPath = "$($StoreIISPath.TrimEnd('/'))Auth"
$receiverVirtualPath = "$($StoreVirtualPath.TrimEnd('/'))Web"
<!--NeedCopy-->
```

- Crea una nueva implementación si todavía no hay ninguna, como preparación para agregar los servicios de StoreFront. **-Confirm:$false** suprime el requisito de confirmar que la implementación puede continuar.

```
# Determine if the deployment already exists
$existingDeployment = Get-STFDeployment
if(-not $existingDeployment)
{

    # Install the required StoreFront components
    Add-STFDeployment -HostBaseUrl $HostbaseUrl -SiteId $SiteId -Confirm:$false
 }

elseif($existingDeployment.HostbaseUrl -eq $HostbaseUrl)
{

    # The deployment exists but it is configured to the desired hostbase url
    Write-Output "A deployment has already been created with the specified hostbase url on this server and will be used."
 }

else
{

    Write-Error "A deployment has already been created on this server with a different host base url."
 }

<!--NeedCopy-->
```

- Crea un nuevo servicio de autenticación si todavía no hay ninguno en la ruta virtual especificada El método de autenticación predeterminado de nombre de usuario y contraseña está habilitado.

```
# Determine if the authentication service at the specified virtual path exists
$authentication = Get-STFAuthenticationService -VirtualPath $authenticationVirtualPath
if(-not $authentication)
{

    # Add an Authentication service using the IIS path of the
```



```
            Store appended with Auth
        $authentication = Add-STFAuthenticationService
            $authenticationVirtualPath
    }

    else
    {

        Write-Output "An Authentication service already exists at the
             specified virtual path and will be used."
    }

    <!--NeedCopy-->
```

- Crea un nuevo servicio de almacén configurado con un Controller de XenDesktop con los servidores en la matriz **$XenDesktopServers** en la ruta virtual especificada, si todavía no existe ninguna.

```
    # Determine if the store service at the specified virtual path
        exists
    $store = Get-STFStoreService -VirtualPath $StoreVirtualPath
    if(-not $store)
    {

    # Add a Store that uses the new Authentication service configured
         to publish resources from the supplied servers
    $store = Add-STFStoreService -VirtualPath $StoreVirtualPath -
        AuthenticationService $authentication -FarmName $Farmtype -
        FarmType $Farmtype -Servers $FarmServers -LoadBalance
        $LoadbalanceServers `
            -Port $Port -SSLRelayPort $SSLRelayPort -TransportType
                $TransportType
    }

    else
    {

        Write-Output "A Store service already exists at the specified
             virtual path and will be used. Farm and servers will be
            appended to this store."
        # Get the number of farms configured in the store
        $farmCount = (Get-STFStoreFarmConfiguration $store).Farms.
            Count
        # Append the farm to the store with a unique name
        Add-STFStoreFarm -StoreService $store -FarmName "Controller$(
            $farmCount + 1)" -FarmType $Farmtype -Servers $FarmServers
             -LoadBalance $LoadbalanceServers -Port $Port `
            -SSLRelayPort $SSLRelayPort -TransportType $TransportType
    }

    <!--NeedCopy-->
```

- Agrega un servicio de Citrix Receiver para Web en la ruta virtual de IIS especificada para obtener

acceso a las aplicaciones publicadas en el almacén creado anteriormente.

```
# Determine if the receiver service at the specified virtual path exists
$receiver = Get-STFWebReceiverService -VirtualPath $receiverVirtualPath
if(-not $receiver)
{

    # Add a Receiver for Web site so users can access the applications and desktops in the published in the Store
    $receiver = Add-STFWebReceiverService -VirtualPath $receiverVirtualPath -StoreService $store
 }

else
{

    Write-Output "A Web Receiver service already exists at the specified virtual path and will be used."
 }

<!--NeedCopy-->
```

- Habilita XenApp Services para el almacén de modo que las versiones anteriores de clientes de Citrix Receiver o de la aplicación Citrix Workspace puedan conectarse a las aplicaciones publicadas.

```
# Determine if PNA is configured for the Store service
$storePnaSettings = Get-STFStorePna -StoreService $store
if(-not $storePnaSettings.PnaEnabled)
{

# Enable XenApp services on the store and make it the default for this server
Enable-STFStorePna -StoreService $store -AllowUserPasswordChange -DefaultPnaService
 }

<!--NeedCopy-->
```

Ejemplo: Crear una implementación para acceso remoto

El siguiente ejemplo se basa en el script anterior y agrega una implementación de acceso remoto.

Antes de comenzar, asegúrese de seguir los pasos detallados en Introducción a SDK. Este ejemplo se puede personalizar con los métodos descritos para generar un script que automatice la implementación de StoreFront.

> **Nota:**
>
> Para asegurarse de que siempre obtiene las últimas mejoras y revisiones, Citrix recomienda seguir el procedimiento descrito en este documento en lugar de copiar y pegar el script de ejemplo.

Entender el script Esta sección explica qué hace cada parte del script generado por StoreFront. Esto le ayudará con la personalización de su propio script.

- Establece los requisitos para la gestión de errores e importa los módulos de StoreFront necesarios. La importación no es necesaria en versiones más nuevas de PowerShell.

```
Param(
    [Parameter(Mandatory=$true)]
    [Uri]$HostbaseUrl,
    [Parameter(Mandatory=$true)]
    [long]$SiteId = 1,
    [string]$Farmtype = "XenDesktop",
    [Parameter(Mandatory=$true)]
    [string[]]$FarmServers,
    [string]$StoreVirtualPath = "/Citrix/Store",
    [bool]$LoadbalanceServers = $false,
    [int]$Port = 80,
    [int]$SSLRelayPort = 443,
    [ValidateSet("HTTP","HTTPS","SSL")]
    [string]$TransportType = "HTTP",
    [Parameter(Mandatory=$true)]
    [Uri]$GatewayUrl,
    [Parameter(Mandatory=$true)]
    [Uri]$GatewayCallbackUrl,
    [Parameter(Mandatory=$true)]
    [string[]]$GatewaySTAUrls,
    [string]$GatewaySubnetIP,
    [Parameter(Mandatory=$true)]
    [string]$GatewayName
)
Set-StrictMode -Version 2.0

# Any failure is a terminating failure.
$ErrorActionPreference = 'Stop'
$ReportErrorShowStackTrace = $true
$ReportErrorShowInnerException = $true
# Import StoreFront modules. Required for versions of PowerShell
    earlier than 3.0 that do not support autoloading
Import-Module Citrix.StoreFront
Import-Module Citrix.StoreFront.Stores
Import-Module Citrix.StoreFront.Roaming
<!--NeedCopy-->
```

- Cree una implementación de StoreFront de acceso interno ejecutando los scripts de los ejemp-

los anteriores. La implementación básica se ampliará para ofrecer el acceso remoto.

```
# Create a simple deployment by invoking the SimpleDeployment example
$scriptDirectory = Split-Path -Path $MyInvocation.MyCommand.Definition -Parent
$scriptPath = Join-Path $scriptDirectory "SimpleDeployment.ps1"
& $scriptPath -HostbaseUrl $HostbaseUrl -SiteId $SiteId -FarmServers $FarmServers -StoreVirtualPath $StoreVirtualPath -Farmtype $Farmtype `
 -LoadbalanceServers $LoadbalanceServers -Port $Port  -SSLRelayPort $SSLRelayPort -TransportType $TransportType
<!--NeedCopy-->
```

- Obtiene los servicios creados en la implementación sencilla porque tienen que actualizarse para admitir el caso de acceso remoto.

```
# Determine the Authentication and Receiver sites based on the Store
$store = Get-STFStoreService -VirtualPath $StoreVirtualPath
$authentication = Get-STFAuthenticationService -StoreService $store
$receiverForWeb = Get-STFWebReceiverService -StoreService $store
<!--NeedCopy-->
```

- Habilita CitrixAGBasic en el servicio de Citrix Receiver para Web, requerido para el acceso remoto a través de Citrix Gateway. Obtiene el método de autenticación ExplicitForms y CitrixAGBasic de Citrix Receiver para Web de los protocolos admitidos.

```
# Get the Citrix Receiver for Web CitrixAGBasic and ExplicitForms authentication method from the supported protocols
# Included for demonstration purposes as the protocol name can be used directly if known
$receiverMethods = Get-STFWebReceiverAuthenticationMethodsAvailable | Where-Object {
 $_ -match "Explicit" -or $_ -match "CitrixAG"  }

# Enable CitrixAGBasic in Receiver for Web (required for remote access)
Set-STFWebReceiverService $receiverForWeb -AuthenticationMethods $receiverMethods
<!--NeedCopy-->
```

- Habilita CitrixAGBasic en el servicio de autenticación. Esto es necesario para el acceso remoto.

```
# Get the CitrixAGBasic authentication method from the protocols installed.
# Included for demonstration purposes as the protocol name can be used directly if known
$citrixAGBasic = Get-STFAuthenticationProtocolsAvailable | Where-Object {
 $_ -match "CitrixAGBasic"  }
```



```
5
6   # Enable CitrixAGBasic in the Authentication service (required
       for remote access)
7   Enable-STFAuthenticationServiceProtocol -AuthenticationService
       $authentication -Name $citrixAGBasic
8   <!--NeedCopy-->
```

- Agrega una nueva puerta de enlace de acceso remoto, lo que agrega la dirección IP de subred optativa y la registra con el almacén al que se va a acceder de forma remota.

```
1   # Add a new Gateway used to access the new store remotely
2   Add-STFRoamingGateway -Name "NetScaler10x" -LogonType Domain -
       Version Version10_0_69_4 -GatewayUrl $GatewayUrl '
3   -CallbackUrl $GatewayCallbackUrl -SecureTicketAuthorityUrls
       $GatewaySTAUrls
4   # Get the new Gateway from the configuration (Add-
       STFRoamingGateway will return the new Gateway if -PassThru is
       supplied as a parameter)
5   $gateway = Get-STFRoamingGateway -Name $GatewayName
6   # If the gateway subnet was provided then set it on the gateway
       object
7   if($GatewaySubnetIP)
8   {
9
10      Set-STFRoamingGateway -Gateway $gateway -SubnetIPAddress
           $GatewaySubnetIP
11   }
12
13  # Register the Gateway with the new Store
14  Register-STFStoreGateway -Gateway $gateway -StoreService $store -
       DefaultGateway
15  <!--NeedCopy-->
```

Ejemplo: Crear una implementación para acceso remoto con una puerta de enlace óptima

El siguiente ejemplo se basa en el script anterior y agrega una implementación de acceso remoto con puerta de enlace de inicio óptima.

Antes de comenzar, asegúrese de seguir los pasos detallados en Introducción a SDK. Este ejemplo se puede personalizar con los métodos descritos para generar un script que automatice la implementación de StoreFront.

> **Nota:**
>
> Para asegurarse de que siempre obtiene las últimas mejoras y revisiones, Citrix recomienda seguir el procedimiento descrito en este documento en lugar de copiar y pegar el script de ejemplo.

Entender el script Esta sección explica qué hace cada parte del script generado por StoreFront. Esto le ayudará con la personalización de su propio script.

- Establece los requisitos para la gestión de errores e importa los módulos de StoreFront necesarios. La importación no es necesaria en versiones más nuevas de PowerShell.

```
Param(
    [Parameter(Mandatory=$true)]
    [Uri]$HostbaseUrl,
    [long]$SiteId = 1,
    [string]$Farmtype = "XenDesktop",
    [Parameter(Mandatory=$true)]
    [string[]]$FarmServers,
    [string]$StoreVirtualPath = "/Citrix/Store",
    [bool]$LoadbalanceServers = $false,
    [int]$Port = 80,
    [int]$SSLRelayPort = 443,
    [ValidateSet("HTTP","HTTPS","SSL")]
    [string]$TransportType = "HTTP",
    [Parameter(Mandatory=$true)]
    [Uri]$GatewayUrl,
    [Parameter(Mandatory=$true)]
    [Uri]$GatewayCallbackUrl,
    [Parameter(Mandatory=$true)]
    [string[]]$GatewaySTAUrls,
    [string]$GatewaySubnetIP,
    [Parameter(Mandatory=$true)]
    [string]$GatewayName,
    [Parameter(Mandatory=$true)]
    [Uri]$OptimalGatewayUrl,
    [Parameter(Mandatory=$true)]
    [string[]]$OptimalGatewaySTAUrls,
    [Parameter(Mandatory=$true)]
    [string]$OptimalGatewayName
)
Set-StrictMode -Version 2.0
# Any failure is a terminating failure.
$ErrorActionPreference = 'Stop'
$ReportErrorShowStackTrace = $true
$ReportErrorShowInnerException = $true
# Import StoreFront modules. Required for versions of PowerShell
    earlier than 3.0 that do not support autoloading
Import-Module Citrix.StoreFront
Import-Module Citrix.StoreFront.Stores
Import-Module Citrix.StoreFront.Roaming
<!--NeedCopy-->
```

- Llama al script de implementación de acceso remoto para configurar la implementación básica y agregarle el acceso remoto.

```
# Create a remote access deployment
$scriptDirectory = Split-Path -Path $MyInvocation.MyCommand.
```



```
    Definition -Parent
$scriptPath = Join-Path $scriptDirectory "RemoteAccessDeployment.
    ps1"
& $scriptPath -HostbaseUrl $HostbaseUrl -SiteId $SiteId -
    FarmServers $FarmServers -StoreVirtualPath $StoreVirtualPath -
    Farmtype $Farmtype `
     -LoadbalanceServers $LoadbalanceServers -Port $Port  -
        SSLRelayPort $SSLRelayPort -TransportType $TransportType `
     -GatewayUrl $GatewayUrl -GatewayCallbackUrl
        $GatewayCallbackUrl -GatewaySTAUrls $GatewaySTAUrls -
        GatewayName $GatewayName
<!--NeedCopy-->
```

- Agrega la preferencia de puerta de enlace de inicio óptima y la obtiene de las puertas de enlace configuradas.

```
# Add a new Gateway used for remote HDX access to desktops and
    apps
$gateway = Add-STFRoamingGateway -Name $OptimalGatewayName -
    LogonType UsedForHDXOnly -GatewayUrl $OptimalGatewayUrl -
    SecureTicketAuthorityUrls $OptimalGatewaySTAUrls -PassThru
<!--NeedCopy-->
```

- Obtiene el servicio del almacén para usar la puerta de enlace óptima, registrarla y asignarla a inicios desde una comunidad especificada.

```
# Get the Store configured by SimpleDeployment.ps1
$store = Get-STFStoreService -VirtualPath $StoreVirtualPath
# Register the Gateway with the new Store for launch against all
    of the farms (currently just one)
$farmNames = @($store.FarmsConfiguration.Farms | foreach {
 $_.FarmName  }
)
Register-STFStoreOptimalLaunchGateway -Gateway $gateway -
    StoreService $store -FarmName $farmNames
<!--NeedCopy-->
```

Solucionar problemas de StoreFront

February 26, 2024

Registros de la instalación

Cuando StoreFront se instala o desinstala, el instalador de StoreFront crea los siguientes archivos de registros en el directorio *C:\Windows\Temp\StoreFront*. Los nombres de archivo reflejan los componentes que los han creado e incluyen marcas de tiempo.

- Citrix-DeliveryServicesRoleManager-*.log: creado cuando StoreFront se instala de forma interactiva.
- Citrix-DeliveryServicesSetupConsole-*.log: creado cuando StoreFront se instala de forma silenciosa, y cuando se desinstala, ya sea de forma interactiva o silenciosa.
- CitrixMsi-CitrixStoreFront-x64-*.log: creado cuando StoreFront se instala o desinstala, ya sea de forma interactiva o silenciosa.

Registros de eventos

StoreFront admite el registro de sucesos de Windows para el servicio de autenticación, los almacenes y los sitios de Receiver para Web. Todos los eventos que se generan se escriben en el registro de aplicaciones de StoreFront, que se puede ver a través de Visor de eventos ya sea en **Registros de aplicaciones y servicios > Citrix Delivery Services** o mediante **Registros de Windows > Aplicación**. Para controlar la cantidad de entradas de registro duplicadas de un solo suceso, modifique los archivos de configuración del servicio de autenticación, de los almacenes y de los sitios de Receiver para Web.

Limitación de registros

1. Utilice un editor de texto para abrir el archivo *web.config* del servicio de autenticación, el almacén o el sitio de Receiver para Web, que normalmente se encuentran en los directorios C:\inetpub\wwwroot\Citrix\Authentication, C:\inetpub\wwwroot\Citrix\storename, and C:\inetpub\wwwroot\Citrix\storenameWeb\ respectivamente, donde storename es el nombre que se especificó para el almacén cuando se creó.
2. Busque este elemento en el archivo.

   ```
   <logger duplicateInterval="00:01:00"duplicateLimit="10">
   ```

   De forma predeterminada, StoreFront se configura para limitar la cantidad de entradas de registro duplicadas a 10 por minuto.
3. Cambie el valor del atributo duplicateInterval para definir el período en el formato de horas, minutos y segundos durante el que se controlarán las entradas de registros duplicadas. Utilice el atributo duplicateLimit para definir la cantidad de entradas duplicadas que se deben registrar en el intervalo especificado para iniciar la limitación de registros.

Cuando se inicie la limitación de registros, se registrará un mensaje de advertencia para indicar que se omitirán las entradas de registro posteriores que sean idénticas. Después de este límite de tiempo, se reanuda el registro normal y se registra un mensaje informativo que indica que las entradas de registro duplicadas ya no se omitirán.

Registros de PowerShell y de la consola de administración

Los cambios de configuración realizados a través de PowerShell o la consola de administración se registran en `C:\Program Files\Citrix\Receiver StoreFront\Admin\logs`. Los nombres de los archivos de registro contienen acciones y sujetos de comandos, además de marcas de tiempo que se pueden usar para distinguir las secuencias de comandos.

Registro de diagnósticos

StoreFront escribe los registros de diagnóstico en `c:\Program Files\Citrix\Receiver StoreFront\admin\trace`

Para StoreFront versión 2311 y versiones superiores, de forma predeterminada, se registran los mensajes de nivel **Error**, **Advertencia** e **Información**. En la mayoría de los casos, esto incluye información suficiente para diagnosticar todos los problemas.

> **Nota:**
>
> En las versiones 2308 y anteriores de StoreFront, de forma predeterminada solo se registran los mensajes de nivel **Error**.

Para solucionar problemas, puede habilitar el registro detallado adicional. Esto solo es necesario si lo solicita el servicio de asistencia técnica de Citrix. Esto podría afectar al rendimiento, por lo que debe revertir `TraceLevel` a `Info` una vez que se complete la solución de problemas.

Para habilitar el registro detallado:

1. Con una cuenta con permisos de administrador local, inicie Windows PowerShell
2. Introduzca el comando:

   ```
   Set-STFDiagnostics -All -TraceLevel "Verbose" -Override -confirm:
      $False
   <!--NeedCopy-->
   ```

   > **Nota:**
   >
   > El parámetro `-Override` solo es necesario para la versión 2311 de StoreFront. Este parámetro se quitará en las versiones futuras de StoreFront.

   Esto permite el registro “detallado”de todos los servicios, sin solicitar confirmación. Cuando se introduce este comando, se reinician los servicios de Storefront. Espere a que vuelva a aparecer el mensaje de PowerShell para verificar que los servicios han terminado de reiniciarse. Mientras se reinician estos servicios, los usuarios no podrán acceder al servidor StoreFront.

3. Reproduzca el problema para crear los registros.

4. Vuelva a establecer el registro en el nivel predeterminado para todos los servicios

```
1  Set-STFDiagnostics -All -TraceLevel "Info" -Override -confirm:
      $False
2 <!--NeedCopy-->
```

> **Nota:**
>
> El parámetro `-Override` solo es necesario para la versión 2311 de StoreFront.

Puede personalizar aún más el registro de diagnósticos:

- StoreFront escribe un archivo de registros independiente para cada servicio. De forma predeterminada, cada archivo de registros tiene un tamaño máximo de 200 Mb y StoreFront escribe hasta 5 archivos de registros por servicio antes de purgar los archivos de registros antiguos. Si necesita personalizar el tamaño o la cantidad de registros escritos, puede hacerlo con los parámetros `-FileSizeKb` y `-FileCount`.
- Cambie el nivel de detalle registrado mediante `-TraceLevel`. Los valores permitidos son `Off`, `Error`, `Warning`, `Info` o `Verbose`.
- Al usar el parámetro `-All`, se establecen los parámetros de registro de todos los servicios. Puede personalizar el registro de un servicio individual mediante `-Service [Service name]`

Para obtener más información sobre el cmdlet `Set-STFDiagnostics`, consulte el apartado StoreFront PowerShell SDK de la documentación.

Registros del archivo Launch.ica

Cuando un usuario inicia una aplicación o un escritorio, StoreFront genera un archivo llamado launch.ica que la aplicación Workspace lee para determinar cómo conectarse a la aplicación o al escritorio. Según la configuración, este archivo puede estar almacenado en la memoria, por lo que no se puede acceder directamente a él. Para diagnosticar errores de inicio, puede ser útil ver el contenido de launch.ica.

Para habilitar la captura de registros del archivo launch.ica en el equipo cliente, siga estos pasos:

1. Vaya a la siguiente clave de Registro mediante el Editor del Registro:

   En sistemas de 32 bits: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\Logging`

   En sistemas de 64 bits: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\Logging`

2. Establezca estos dos valores de clave de cadena:

- LogFile=”ruta al archivo de registro”
- LogICAFile=true

Por ejemplo:

```
LogFile=C:\ica\ica.log
LogICAFile=true
<!--NeedCopy-->
```

> Nota:
>
> El uso de un archivo ICA en el entorno para un fin que no sea la solución de problemas se describe más detalladamente en CTX200126.

Avisos de obsolescencia

February 26, 2024

Los siguientes anuncios tienen por objeto avisarle por adelantado acerca de las plataformas, los productos y las funciones de Citrix que se están retirando progresivamente, de modo que pueda tomar a tiempo las decisiones empresariales pertinentes. Citrix examina el uso que hacen los clientes de una función que está por retirar y los comentarios que tengan sobre la eliminación de la función para determinar cuándo retirarla. Estos anuncios están sujetos a cambios en las versiones posteriores y es posible que no contengan todas las funciones o funciones retiradas. Para obtener información detallada sobre el ciclo de vida útil de los productos, consulte el artículo Product Lifecycle Support Policy. Para obtener información sobre la opción de servicio Long Term Service Release (LTSR), consulte https://support.citrix.com/article/CTX205549.

Elementos retirados

Los elementos retirados no se quitan inmediatamente. Citrix sigue admitiéndolos, pero se quitarán de la siguiente versión.

Elemento	Retirada anunciada en la versión	Alternativa
Servicios XenApp (también conocidos como PNAgent)	2308	En la aplicación Workspace, conéctese a los almacenes con la URL de almacén en lugar de la URL de los servicios XenApp

Elementos eliminados

Los elementos eliminados se quitan o ya no se ofrecen o admiten.

Elemento	Retirada anunciada en la versión	Eliminado en la versión	Alternativa
Internet Explorer 11 para conectarse a recursos mediante la aplicación Workspace para HTML5	2308	2308	Use un explorador web compatible o instale la aplicación Citrix Workspace para Windows. Aún es posible utilizar Internet Explorer 11 para acceder al almacén, pero, para iniciar recursos, debe estar instalada la aplicación Citrix Workspace para Windows.
Feeds de recursos de XenApp 6.5.	2308	2308	Actualice a la versión más reciente de Citrix Virtual Apps and Desktops. También es posible agregar feeds de recursos de XenApp 6.5 mediante PowerShell, pero tenga en cuenta que XenApp 6.5 ya no es compatible.
Compatibilidad con autoservicio de restablecimiento de contraseñas (SSPR)	2203	2203	-

Elemento	Retirada anunciada en la versión	Eliminado en la versión	Alternativa
Compatibilidad con los protocolos TLS 1.0 y TLS 1.1 entre Citrix Virtual Apps and Desktops y la aplicación Citrix Workspace.	3.14	2203	Actualice la versión de los Citrix Receiver a una aplicación Citrix Workspace que admita TLS 1.2.
Instalación de StoreFront en Windows Server 2012 R2	2203	2203	Instale StoreFront en un sistema operativo compatible.
Compatibilidad con las versiones de Microsoft .NET Framework anteriores a 4.7.2.	2203	2203	Actualice a .NET Framework 4.7.2 o una posterior. (El instalador instala automáticamente .NET Framework 4.7.2 si aún no está instalado.)
Eliminación de las opciones de Delivery Controller para los siguientes productos que han alcanzado el final de su ciclo de vida: VDI-in-a-Box y XenMobile (9.0 y versiones anteriores).	1903	1903	—
Internet Explorer 9 y 10.	1903	1903	—
Acceso para usuarios a escritorios en sitios de Desktop Appliance	1811	1912	Use Desktop Lock para casos de uso que no pertenezcan a ningún dominio.

Elemento	Retirada anunciada en la versión	Eliminado en la versión	Alternativa
Experiencia clásica en Citrix (interfaz de usuario “burbujas verdes”).	3.12	1903	Usar la interfaz de usuario unificada
Instalación de StoreFront en Windows Server 2012 y Windows Server 2008 R2 (incluidos los Service Packs).	3.12 LTSR	3.15	Instale los componentes en un sistema operativo compatible.
Integración de Citrix Online Integration (producto GoTo)	3.11	3.12	—
Actualizaciones locales desde StoreFront 2.0, 2.1, 2.5 y 2.5.2.	3.9	1818	Actualice una de estas versiones a la 3.12 y, a continuación, a una versión más reciente.
Instalar StoreFront en máquinas de 32 bits (x86).	3.8	3.13	Realice la instalación en un sistema operativo x64 compatible.

Para obtener información sobre los elementos retirados en la aplicación Citrix Workspace para HTML5, consulte la página Elementos retirados.

Avisos legales de terceros

September 27, 2023

StoreFront puede incluir componentes de software de terceros con estas condiciones de licencia. Esta lista se generó con el software de terceros en la fecha indicada. Esta lista puede cambiar con versiones específicas del producto y es posible que no esté completa, por lo que se proporciona “tal cual”. EN LA MEDIDA EN QUE LO PERMITA LA LEY APLICABLE, CITRIX Y SUS PROVEEDORES NO OFRECEN NINGUNA DECLARACIÓN NI GARANTÍA, EXPRESA O IMPLÍCITA, LEGAL O DE OTRO TIPO, CON RESPECTO A LA LISTA O SU PRECISIÓN O INTEGRIDAD, NI CON RESPECTO A LOS RESULTADOS QUE SE

OBTENGAN DEL USO O LA DISTRIBUCIÓN DE LA LISTA. SI UTILIZA O DISTRIBUYE ESTA LISTA, ACEPTA QUE DE NINGUNA MANERA PODRÁ SER CITRIX RESPONSABLE DE NINGÚN DAÑO, YA SEA ESPECIAL, DIRECTO, INDIRECTO, DERIVADO U ORIGINADO EN CONSECUENCIA DEL USO O DISTRIBUCIÓN DE DICHA LISTA.

Castle Windsor 3.3.0

Copyright 2004-2013 Castle Project - http://www.castleproject.org/

Con licencia Apache, versión 2.0

Microsoft Unity Application Block (Unity) 2.1

Copyright © 2011 Microsoft Corporation.

Con la Licencia pública de Microsoft (MS-PL) https://msdn.microsoft.com/en-us/library/hh237493.aspx

Patrones y prácticas de Microsoft: Prism 2.2

Copyright © 2010 Microsoft Corporation.

Con la Licencia pública de Microsoft (MS-PL) http://compositewpf.codeplex.com/releases/view/46046

Patrones y prácticas de Microsoft: Common Service Locator 1.0

Copyright © Microsoft Corporation.

Con la Licencia pública de Microsoft (MS-PL)

Origen de referencia de Microsoft .NET

Copyright © Microsoft Corporation. Con la licencia del MIT.

ManagedEsent, versión 1.9.4

Copyright © Microsoft Corporation.

Con la Licencia pública de Microsoft (MS-PL) http://managedesent.codeplex.com/license

jQuery UI - v1.10.4 - 2014-03-12

http://jqueryui.com/

Copyright 2014 jQuery Foundation y otros colaboradores; con licencia del MIT

Biblioteca de JavaScript jQuery v1.12.4

http://jquery.com/

Incluye Sizzle.js

http://sizzlejs.com/

Copyright jQuery Foundation y otros colaboradores

Con la licencia del MIT

http://jquery.org/license

Fecha: 2016-05-20T17:17Z

jQuery jScrollPane v2.0.0beta11

jScrollPane - v2.0.0beta11 - 2011-07-04 http://jscrollpane.kelvinluck.com/

Copyright (c) 2010 Kelvin Luck

Con doble licencia del MIT y de GPL.

jquery.contextmenu.js

Plug-in de jQuery para menús contextuales

http://www.JavascriptToolbox.com/lib/contextmenu

Copyright (c) 2008 Matt Kruse (javascripttoolbox.com)

Con doble licencia del MIT y de GPL.

Plug-in de jQuery para Hammer.JS - v1.0.0 - 2014-01-02

http://eightmedia.github.com/hammer.js

Copyright (c) 2014 Jorik Tangelder j.tangelder@gmail.com;

Con la licencia del MIT

jQuery MouseWheel

Copyright (c) 2011 Brandon Aaron (http://brandonaaron.net)

Con la licencia del MIT (LICENSE.txt).

WPF Toolkit 3.5

WPF Toolkit (http://wpf.codeplex.com/) Copyright (c) 2006-2014 Microsoft

Licencia de MS-PL http://wpf.codeplex.com/license

WPF Toolkit 3.0 ampliado

Copyright (C) 2007-2013 Xceed Software Inc.

Este programa se le proporciona bajo las condiciones de la Licencia pública de Microsoft (MS-PL) publicadas en http://wpftoolkit.codeplex.com/license.

Para obtener más funciones, controles y una asistencia rápida y profesional, elija la Edición Plus en http://xceed.com/wpf_toolkit.

Siga a @datagrid en Twitter o en Facebook para estar al día de novedades: http://facebook.com/datagrids

Conjunto de herramientas WiX

Copyright (c) Outercurve Foundation. Licencia pública común, versión 1.0.

Seguridad CLR

Copyright (c) Microsoft Corporation. Licencia permisiva limitada de Microsoft (MS-LPL)

Stack Exchange Redis 1.1

StackExchange.Redis.StrongName 1.1 https://stackexchange.github.io/StackExchange.Redis Copyright (c) 2014 Stack Exchange

Con la licencia del MIT

Newtonsoft JSON 9.0

Copyright (c) 2007 James Newton-King

Con la licencia del MIT.

Biblioteca de JavaScript jQuery v3.5.1

https://jquery.com/

Incluye Sizzle.js

https://sizzlejs.com/

Copyright JS Foundation y otros colaboradores

Con la licencia del MIT

https://jquery.org/license

Fecha: 2020-05-04T22:49Z

jQuery UI - v1.13.2 - 2022-07-14

http://jqueryui.com

Copyright jQuery Foundation y otros colaboradores; con licencia del MIT

Hammer.JS - v2.0.4 - 2014-09-28

Hammer.JS - v2.0.8 - 2016-04-23

http://hammerjs.github.io/

Copyright (c) 2016 Jorik Tangelder;

Con la licencia del MIT

VelocityJS.org (1.5.0)

velocity-animate (C) 2014-2017 Julian Shapiro.

Con la licencia del MIT. Consulte el archivo LICENSE en la raíz del proyecto para obtener detalles.

slick.js - 1.8.0

La licencia del MIT (MIT)

Copyright (c) 2013-2016

jQuery UI Touch Punch 0.2.3

Copyright 2011–2014, Dave Furfero

Con doble licencia del MIT o de GPL, versión 2.

APÉNDICE: Licencias referenciadas

Licencia del MIT

```
Permission is hereby granted, free of charge, to any person obtaining a copy
of this software and associated documentation files (the "Software"), to deal
in the Software without restriction, including without limitation the rights
to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
copies of the Software, and to permit persons to whom the Software is
furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in
all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE
AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER
LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,
OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN
THE SOFTWARE.
<!--NeedCopy-->
```

Licencia Apache, versión 2.0


```
                                Apache License
                           Version 2.0, January 2004
                        http://www.apache.org/licenses/


TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

   "License" shall mean the terms and conditions for use, reproduction,
   and distribution as defined by Sections 1 through 9 of this document
       .

   "Licensor" shall mean the copyright owner or entity authorized by
   the copyright owner that is granting the License.

   "Legal Entity" shall mean the union of the acting entity and all
   other entities that control, are controlled by, or are under common
   control with that entity. For the purposes of this definition,
   "control" means (i) the power, direct or indirect, to cause the
   direction or management of such entity, whether by contract or
   otherwise, or (ii) ownership of fifty percent (50%) or more of the
   outstanding shares, or (iii) beneficial ownership of such entity.

   "You" (or "Your") shall mean an individual or Legal Entity
   exercising permissions granted by this License.

   "Source" form shall mean the preferred form for making modifications
       ,
   including but not limited to software source code, documentation
   source, and configuration files.

   "Object" form shall mean any form resulting from mechanical
   transformation or translation of a Source form, including but
   not limited to compiled object code, generated documentation,
   and conversions to other media types.

   "Work" shall mean the work of authorship, whether in Source or
   Object form, made available under the License, as indicated by a
   copyright notice that is included in or attached to the work
   (an example is provided in the Appendix below).

   "Derivative Works" shall mean any work, whether in Source or Object
   form, that is based on (or derived from) the Work and for which the
   editorial revisions, annotations, elaborations, or other
       modifications
   represent, as a whole, an original work of authorship. For the
       purposes
   of this License, Derivative Works shall not include works that
       remain
   separable from, or merely link (or bind by name) to the interfaces
       of,
   the Work and Derivative Works thereof.
```



```
48
49      "Contribution" shall mean any work of authorship, including
50      the original version of the Work and any modifications or additions
51      to that Work or Derivative Works thereof, that is intentionally
52      submitted to Licensor for inclusion in the Work by the copyright
            owner
53      or by an individual or Legal Entity authorized to submit on behalf
            of
54      the copyright owner. For the purposes of this definition, "submitted
            "
55      means any form of electronic, verbal, or written communication sent
56      to the Licensor or its representatives, including but not limited to
57      communication on electronic mailing lists, source code control
            systems,
58      and issue tracking systems that are managed by, or on behalf of, the
59      Licensor for the purpose of discussing and improving the Work, but
60      excluding communication that is conspicuously marked or otherwise
61      designated in writing by the copyright owner as "Not a Contribution.
            "
62
63      "Contributor" shall mean Licensor and any individual or Legal Entity
64      on behalf of whom a Contribution has been received by Licensor and
65      subsequently incorporated within the Work.
66
67   2. Grant of Copyright License. Subject to the terms and conditions of
68      this License, each Contributor hereby grants to You a perpetual,
69      worldwide, non-exclusive, no-charge, royalty-free, irrevocable
70      copyright license to reproduce, prepare Derivative Works of,
71      publicly display, publicly perform, sublicense, and distribute the
72      Work and such Derivative Works in Source or Object form.
73
74   3. Grant of Patent License. Subject to the terms and conditions of
75      this License, each Contributor hereby grants to You a perpetual,
76      worldwide, non-exclusive, no-charge, royalty-free, irrevocable
77      (except as stated in this section) patent license to make, have made
            ,
78      use, offer to sell, sell, import, and otherwise transfer the Work,
79      where such license applies only to those patent claims licensable
80      by such Contributor that are necessarily infringed by their
81      Contribution(s) alone or by combination of their Contribution(s)
82      with the Work to which such Contribution(s) was submitted. If You
83      institute patent litigation against any entity (including a
84      cross-claim or counterclaim in a lawsuit) alleging that the Work
85      or a Contribution incorporated within the Work constitutes direct
86      or contributory patent infringement, then any patent licenses
87      granted to You under this License for that Work shall terminate
88      as of the date such litigation is filed.
89
90   4. Redistribution. You may reproduce and distribute copies of the
91      Work or Derivative Works thereof in any medium, with or without
92      modifications, and in Source or Object form, provided that You
93      meet the following conditions:
94
```



```
    (a) You must give any other recipients of the Work or
        Derivative Works a copy of this License; and

    (b) You must cause any modified files to carry prominent notices
        stating that You changed the files; and

    (c) You must retain, in the Source form of any Derivative Works
        that You distribute, all copyright, patent, trademark, and
        attribution notices from the Source form of the Work,
        excluding those notices that do not pertain to any part of
        the Derivative Works; and

    (d) If the Work includes a "NOTICE" text file as part of its
        distribution, then any Derivative Works that You distribute must
        include a readable copy of the attribution notices contained
        within such NOTICE file, excluding those notices that do not
        pertain to any part of the Derivative Works, in at least one
        of the following places: within a NOTICE text file distributed
        as part of the Derivative Works; within the Source form or
        documentation, if provided along with the Derivative Works; or,
        within a display generated by the Derivative Works, if and
        wherever such third-party notices normally appear. The contents
        of the NOTICE file are for informational purposes only and
        do not modify the License. You may add Your own attribution
        notices within Derivative Works that You distribute, alongside
        or as an addendum to the NOTICE text from the Work, provided
        that such additional attribution notices cannot be construed
        as modifying the License.

    You may add Your own copyright statement to Your modifications and
    may provide additional or different license terms and conditions
    for use, reproduction, or distribution of Your modifications, or
    for any such Derivative Works as a whole, provided Your use,
    reproduction, and distribution of the Work otherwise complies with
    the conditions stated in this License.

  5. Submission of Contributions. Unless You explicitly state otherwise,
    any Contribution intentionally submitted for inclusion in the Work
    by You to the Licensor shall be under the terms and conditions of
    this License, without any additional terms or conditions.
    Notwithstanding the above, nothing herein shall supersede or modify
    the terms of any separate license agreement you may have executed
    with Licensor regarding such Contributions.

  6. Trademarks. This License does not grant permission to use the trade
    names, trademarks, service marks, or product names of the Licensor,
    except as required for reasonable and customary use in describing
        the
    origin of the Work and reproducing the content of the NOTICE file.

  7. Disclaimer of Warranty. Unless required by applicable law or
    agreed to in writing, Licensor provides the Work (and each
    Contributor provides its Contributions) on an "AS IS" BASIS,
```



```
   WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or
   implied, including, without limitation, any warranties or conditions
   of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A
   PARTICULAR PURPOSE. You are solely responsible for determining the
   appropriateness of using or redistributing the Work and assume any
   risks associated with Your exercise of permissions under this
      License.

8. Limitation of Liability. In no event and under no legal theory,
   whether in tort (including negligence), contract, or otherwise,
   unless required by applicable law (such as deliberate and grossly
   negligent acts) or agreed to in writing, shall any Contributor be
   liable to You for damages, including any direct, indirect, special,
   incidental, or consequential damages of any character arising as a
   result of this License or out of the use or inability to use the
   Work (including but not limited to damages for loss of goodwill,
   work stoppage, computer failure or malfunction, or any and all
   other commercial damages or losses), even if such Contributor
   has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing
   the Work or Derivative Works thereof, You may choose to offer,
   and charge a fee for, acceptance of support, warranty, indemnity,
   or other liability obligations and/or rights consistent with this
   License. However, in accepting such obligations, You may act only
   on Your own behalf and on Your sole responsibility, not on behalf
   of any other Contributor, and only if You agree to indemnify,
   defend, and hold each Contributor harmless for any liability
   incurred by, or claims asserted against, such Contributor by reason
   of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS
<!--NeedCopy-->
```

Licencia pública de Microsoft (MS-PL)

```
This license governs use of the accompanying software. If you use the
    software, you accept this license. If you do not accept the license,
     do not use the software.

1. Definitions
The terms “reproduce,” “reproduction,” “derivative works,” and “
    distribution” have the
same meaning here as under U.S. copyright law.

A “contribution” is the original software, or any additions or
    changes to the software.

A “contributor” is any person that distributes its contribution under
     this license.

```


“Licensed patents” are a contributor’s patent claims that read directly on its contribution.

2. Grant of Rights

(A) Copyright Grant- Subject to the terms of **this** license, including the license conditions and limitations in section 3, each contributor grants you a non-exclusive, worldwide, royalty-free copyright license to reproduce its contribution, prepare derivative works of its contribution, and distribute its contribution or any derivative works that you create.

(B) Patent Grant- Subject to the terms of **this** license, including the license conditions and limitations in section 3, each contributor grants you a non-exclusive, worldwide, royalty-free license under its licensed patents to make, have made, use, sell, offer **for** sale, **import**, and/or otherwise dispose of its contribution in the software or derivative works of the contribution in the software.

3. Conditions and Limitations

(A) No Trademark License- This license does not grant you rights to use any contributors’ name, logo, or trademarks.

(B) If you bring a patent claim against any contributor over patents that you claim are infringed by the software, your patent license from such contributor to the software ends automatically.

(C) If you distribute any portion of the software, you must retain all copyright, patent, trademark, and attribution notices that are present in the software.

(D) If you distribute any portion of the software in source code form, you may **do** so only under **this** license by including a complete copy of **this** license with your distribution. If you distribute any portion of the software in compiled or object code form, you may only **do** so under a license that complies with **this** license.

(E) The software is licensed “as-is.” You bear the risk of using it. The contributors give no express warranties, guarantees or conditions. You may have additional consumer rights under your local laws which **this** license cannot change. To the extent permitted under your local laws, the contributors exclude the implied warranties of merchantability, fitness **for** a particular purpose and non-infringement.