Interfaz Web 5.4

2015-05-07 20:30:12 UTC

Contenido

Interfaz Web 5.4 8

Léame de la Interfaz Web 5.4 10

Administración de la Interfaz Web 14

Funciones de la Interfaz Web 15

Funciones de administración 16

Características del acceso a los recursos 17

Características de seguridad 18

Características de la distribución de clientes 20

Novedades de esta versión 21

Componentes de la Interfaz Web 22

Funcionamiento de la Interfaz Web 24

Requisitos del sistema para la Interfaz Web 26

Requisitos mínimos de software 28

Requisitos generales de configuración 31

Requisitos del servidor Web 32

Requisitos del usuario 34

Requisitos para el acceso a aplicaciones sin conexión 37

Requisitos para otros dispositivos de usuarios 39

Requisitos de dispositivos de usuario 40

Instalación de la Interfaz Web 41

Consideraciones sobre seguridad 42

Para instalar la Interfaz Web en Microsoft Internet Information Services 43

Compatibilidad con otros componentes en Windows Server 2003 x64 Editions 45

Instalación de la Interfaz Web en servidores de aplicaciones de Java 46

Uso de los paquetes de idiomas 48

Eliminación de paquetes de idiomas 49

Actualización de una instalación existente 50

Qué hacer después de la instalación 51

Solución de problemas de instalación de la Interfaz Web 52
Desinstalación de la Interfaz Web 53
Introducción a la Interfaz Web 54
Configuración de sitios mediante la consola de administración de la Interfaz Web de Citrix 56
Configuración de sitios mediante archivos de configuración 57
Configuración compartida 58
Para crear un sitio en Microsoft Internet Information Services 59
Creación de sitios en servidores de aplicaciones de Java 60
Especificación del punto de autenticación 61
Distribución de Access Gateway con la Interfaz Web 63
Integración de un sitio Web XenApp con Access Gateway 65
Para habilitar a usuarios de tarjeta inteligente para que puedan acceder a los recursos, a través de Access Gateway, sin proporcionar un PIN 69
Para habilitar a usuarios de tarjeta inteligente para que puedan acceder a sus recursos a través de Access Gateway proporcionando un PIN 73
Coordinación de parámetros entre la Interfaz Web y Access Gateway 75
Especificación de los parámetros de configuración inicial para un sitio 76
Actualización de sitios existentes 78
Uso de las tareas de sitio 79
Reparación y desinstalación de sitios 80
Cómo poner la Interfaz Web a disposición de los usuarios 81
Administración de servidores y comunidades 83
Consideraciones sobre el cambio de contraseñas 84
Para agregar una comunidad de servidores 85
Para configurar la tolerancia de fallos 86
Para habilitar el equilibrio de carga entre los servidores 87
Configuración de parámetros para todos los servidores de la comunidad 88
Especificación de parámetros avanzados del servidor 90
Administración de la configuración de servidores 92
Configuración de la autenticación para la Interfaz Web 95
Configuración de la autenticación 97
Para usar autenticación basada en dominios 99
Para usar autenticación de Novell Directory Services 101
Habilitación de la autenticación explícita 102
Para configurar los parámetros de contraseñas para la autenticación explícita 103
Para habilitar la autenticación de dos factores 105

Configuración del autoservicio de cuentas 106
Habilitación de la autenticación por petición de credenciales 108
Para configurar los parámetros de contraseñas para la autenticación por petición de credenciales 109
Habilitación de la autenticación mediante paso de credenciales (PassThrough) 110
Paso 1: Instalación del plug-in para la autenticación mediante paso de credenciales 112
Paso 2: Habilitación del paso de credenciales (PassThrough) en los plugins 113
Paso 3: Habilitación del paso de credenciales (PassThrough) usando la consola 115
Habilitación de la autenticación con tarjeta inteligente 116
Paso 1: Instalar el plugin para la autenticación con tarjeta inteligente 117
Paso 2: Habilitación del Asignador de servicios de directorios de Windows 119
Paso 3: Habilitación de la autenticación con tarjeta inteligente en la Interfaz Web 120
Ejemplo: Habilitación de la autenticación con tarjeta inteligente para los usuarios 122
Configuración de la autenticación de dos factores 123
Habilitación de la autenticación con SafeWord en Microsoft Internet Information Services 124
Habilitación de la autenticación con RSA SecurID en Microsoft Internet Information Services 125
Para restablecer la clave de registro del secreto de nodo en el servidor Web 127
Habilitación de la autenticación RADIUS 128
Habilitación de RADIUS con SafeWord 130
Habilitación de RADIUS con RSA SecurID 131
Administración de clientes 133
Clientes para recursos en línea 134
Configuración de Citrix Online Plug-in 135
Copia de los archivos de instalación de clientes en la Interfaz Web 136
Para copiar los archivos de clientes en la Interfaz Web en Microsoft Internet Information Services 137
Para copiar los archivos de clientes en la Interfaz Web en servidores de aplicaciones de Java 139
Configuración de los mensajes de instalación y distribución de clientes 141
Para configurar los mensajes de instalación y distribución de clientes 142
Configuración de la firma de archivos ICA 143
Configuración de la supervisión de la sesión de streaming 145
Distribución del software de Conexión a escritorio remoto 146

Distribución del Cliente para Java 147
Para configurar el uso automático del Cliente para Java 148
Personalización de la distribución del Cliente para Java 149
Administración del acceso seguro 151
Para configurar rutas directas de acceso 152
Para configurar parámetros de dirección alternativa 153
Para configurar la traducción de direcciones en los servidores de seguridad internos 154
Para configurar los parámetros de puerta de enlace 155
Para configurar los parámetros de acceso predeterminados 157
Modificación de los parámetros del servidor proxy del lado del cliente 159
Para configurar los parámetros predeterminados del proxy 160
Personalización de la apariencia para los usuarios 161
Administración de accesos directos a los recursos 163
Uso de las opciones de actualización de recursos 164
Administración de las preferencias de sesión 165
Control de ancho de banda 167
Suavizado de fuentes de ClearType 168
Redirección de carpetas especiales 169
Habilitación de la redirección de carpetas especiales 170
Configuración del control del área de trabajo 171
Uso del control del área de trabajo con métodos de autenticación integrados para los sitios Web de XenApp 173
Para habilitar la reconexión automática al iniciar sesión 175
Para habilitar el botón Reconectar 176
Para configurar el cierre de sesiones 177
Configuración de la seguridad en la Interfaz Web 178
Secure Sockets Layer 180
Transport Layer Security 181
Traspaso SSL 182
Cifrado ICA 183
Access Gateway 184
Secure Gateway 185
Protección de las comunicaciones de la Interfaz Web 186
Protección de Citrix Online Plug-in con SSL 187
Comunicación entre el dispositivo del usuario y la Interfaz Web 188
Problemas de seguridad en la comunicación entre el dispositivo del usuario y la Interfaz Web 189

Recomendaciones para garantizar la comunicación entre el dispositivo de usuario y la Interfaz Web 190
Comunicación entre la Interfaz Web y el servidor Citrix..... 192
Uso del Traspaso SSL 193
Habilitar la Interfaz Web en el servidor que ejecuta XenApp o XenDesktop 195
Uso del protocolo HTTPS 196
Comunicación entre la sesión de usuario y el servidor 197
Recomendaciones para proteger la comunicación entre la sesión de usuario y el servidor 198
Control del registro de diagnóstico..... 199
Configuración de sitios mediante el archivo de configuración 200
Parámetros de WebInterface.conf..... 201
Contenido del archivo config.xml 228
Para configurar la Interfaz Web cuando se usa Citrix Online Plug-in 230
Parámetros del archivo bootstrap.conf 231
Para configurar la comunicación con el servidor 232
Para configurar la comunicación con el Traspaso SSL 233
Para configurar el respaldo para Secure Gateway 234
Para configurar la compatibilidad con XenApp 4.0, con Feature Pack 1, para UNIX..... 235
Para configurar comunidades de recuperación ante desastres 236
Para configurar el perfil móvil de usuarios..... 237
ID de suceso y mensajes registrados 238
Desactivación de mensajes de error 269
Configuración del soporte de AD FS para la Interfaz Web..... 270
Funcionamiento de los sitios integrados con los servicios de federación de Active Directory 271
Antes de crear sitios de servicios de federación de Active Directory..... 273
Configuración de las relaciones entre dominios 275
Cómo configurar la delegación para los servidores del entorno 278
Para asegurar que el dominio al que pertenece el asociado de recurso está en el nivel funcional correcto 279
Para establecer una relación de confianza con el servidor de la Interfaz Web para la delegación 280
Para establecer una relación de confianza con el servidor que ejecuta el servicio XML de Citrix para la delegación 281
Para determinar qué recursos son accesibles desde el servidor XenApp 282
Configuración de servidores para delegación limitada 283
Configuración de un límite de tiempo para el acceso a los recursos 284
Configuración de cuentas sombra 285

Creación de sitios integrados con servicios de federación de Active Directory 287
Configuración del sitio como aplicación de los servicios de federación de Active Directory 288
Cómo poner a prueba su entorno 289
Cierre de sesión en sitios integrados con servicios de federación de Active Directory 290

Interfaz Web 5.4

La Interfaz Web da acceso a los usuarios a las aplicaciones y el contenido de XenApp y a los escritorios virtuales de XenDesktop. Los usuarios acceden a sus recursos por medio de un explorador Web estándar o mediante Citrix Online Plug-in.

En esta sección

Esta sección de la biblioteca brinda información actualizada sobre la instalación, configuración y administración de la Interfaz Web, que incluye los siguientes temas:

Léame de la Interfaz Web 5.4	Información sobre las últimas actualizaciones y problemas conocidos.
Problemas solucionados en la Interfaz Web 5.4	Detalles sobre los problemas que se han solucionado de la versión anterior de la Interfaz Web.
Funciones de la Interfaz Web	Introducción a la Interfaz Web.
Novedades de esta versión	Descripción general de las nuevas funciones.
Componentes de la Interfaz Web	Descripción de un entorno de la Interfaz Web.
Requisitos del sistema para la Interfaz Web	Requisitos de software, configuración, servidores Web, usuarios y dispositivos.
Instalación de la Interfaz Web	Instalación de la Interfaz Web y configuración del servidor Web.
Introducción a la Interfaz Web	Creación y configuración de sitios de la Interfaz Web.
Administración de servidores y comunidades	Configuración y administración de los parámetros del servidor y la comunicación con las comunidades de servidores.
Configuración de la autenticación para la Interfaz Web	Configuración de la autenticación entre la Interfaz Web, las comunidades de servidores y los plugins de Citrix.
Administración de clientes	Instalación y uso de los plugins de Citrix en la Interfaz Web.
Administración del acceso seguro	Configuración y administración del acceso a los sitios.
Modificación de los parámetros del servidor proxy del lado del cliente	Configuración de los clientes de Citrix y los servidores que ejecutan XenApp o XenDesktop a través de servidores proxy.
Personalización de la apariencia para los usuarios	Personalización de la manera en que la Interfaz Web es presentada a los usuarios.
Administración de las preferencias de sesión	Especificación de los parámetros que los usuarios pueden ajustar.

Configuración del control del área de trabajo	Posibilidad para los usuarios de desconectar, volver a conectar y cerrar sesión en los recursos rápidamente.
Configuración de la seguridad en la Interfaz Web	Protección de sus datos en un entorno de Interfaz Web.
Configuración de sitios mediante el archivo de configuración	Administración de sitios de Interfaz Web mediante archivos de configuración.
Configuración del soporte de AD FS para la Interfaz Web	Creación y configuración de sitios de Interfaz Web integrados con servicios de federación de Active Directory (AD FS) de Microsoft.

Léame de la Interfaz Web 5.4

Versión del documento: 1.0

Contenido

- Documentación relacionada
- Asistencia técnica
- Problemas conocidos en esta versión

Documentación relacionada

Para los problemas relacionados con clientes, que puedan afectar a los usuarios de la Interfaz Web, consulte los archivos Léame para clientes Citrix actualmente distribuidos a sus usuarios.

Para obtener una lista de los problemas resueltos en esta versión, consulte el artículo http://support.citrix.com/article/CTX124164 en el sitio de Knowledge Center.

Para acceder a la documentación sobre el sistema de licencias, vaya a Licencias de productos.

Asistencia técnica

Citrix proporciona servicio técnico principalmente a través de Citrix Solution Advisor. Póngase en contacto con su proveedor si desea asistencia de primera línea o utilice la asistencia técnica en línea de Citrix para buscar el asociado de Citrix Solutions Advisor más cercano.

Citrix le ofrece servicios de asistencia técnica en línea en el sitio Web de asistencia técnica de Citrix. La página de asistencia técnica (Support) incluye enlaces con descargas, Citrix Knowledge Center, Citrix Consulting Services y otras páginas de utilidad.

Problemas conocidos en esta versión

A continuación, se presenta una lista de problemas conocidos en esta versión. **Léala con atención antes de instalar el producto**.

- Los iconos no se muestran correctamente en los dispositivos que ejecutan Internet Explorer 6 y WinCE 6.0 WFR3
- Se pueden producir errores de usuarios al agregar escritorios publicados a Favoritos en Internet Explorer

- Mensaje de error al intentar conectarse mediante clientes desaprobados
- No se puede actualizar Citrix online plug-in en dispositivos que ejecutan sistemas operativos Windows Embedded
- Falla el uso de Kerberos al configurar la delegación en servidores XenApp que ejecutan Windows Server 2008
- No se puede iniciar el escritorio virtual cuando se accede a la Interfaz Web desde algunos dispositivos que ejecutan Windows Embedded CE 6.0
- No está disponible la actualización de cliente y el control del área de trabajo para usuarios de Firefox 3.6
- No está disponible el control del área de trabajo en algunos dispositivos que ejecutan Windows Mobile 6.1
- No está disponible, de manera intermitente, el control del área de trabajo en algunos dispositivos que ejecutan Windows Embedded CE 6.0 R2
- No es posible utilizar el paso de credenciales (pass-through) con tarjeta inteligente desde Access Gateway con XenApp 6.0.

Los iconos no se muestran correctamente en los dispositivos que ejecutan Internet Explorer 6 y WinCE 6.0 WFR3

Los iconos en formato .png no se muestran correctamente al visualizarlos en dispositivos que ejecutan Internet Explorer 6 con WinCE 6.0 WFR3 (Hot Fix 3 compilación 664). Para resolver este problema, utilice Internet Explorer 5 o una versión anterior. De forma alternativa, para mostrar archivos .png en Internet Explorer 6, consulte la solución que se describe en el artículo http://support.microsoft.com/kb/294714 de Microsoft.

[#41839]

Es posible que los usuarios no puedan agregar aplicaciones y escritorios publicados a la lista Favoritos de Internet Explorer

Los usuarios pueden experimentar problemas al agregar aplicaciones y escritorios publicados a Favoritos en Internet Explorer. En algunas situaciones, el enlace de Favoritos resultante tendrá un título incorrecto y no funcionará correctamente cuando se seleccione. Para agregar aplicaciones a Favoritos, haga clic con el botón secundario en el icono de la aplicación. Para agregar escritorios, haga clic con el botón secundario en el texto del título del escritorio.

[#244446]

Mensaje de error al intentar conectarse mediante clientes desaprobados

Esta versión de la Interfaz Web no respalda el uso de clientes anteriores a la Versión 7.0. Al intentar conectarse a una aplicación remota con un cliente anterior, los usuarios pueden encontrarse con el error “50: no se puede conectar con el servidor”. Los usuarios pueden evitar este problema actualizando a las versiones más recientes de los clientes. Si esto no es posible, el error puede evitarse mediante la modificación de los archivos .ica de la plantilla, del siguiente modo:

1. Utilice un editor de texto, como el Bloc de notas, para abrir los siguientes archivos: default.ica, bandwidth_high.ica, bandwidth_low.ica, bandwidth_medium.ica y bandwidth_medium_high.ica. Estos archivos se encuentran normalmente en el directorio C:\inetpub\wwwroot\Citrix*SiteName*\conf en IIS y en el directorio /WEB-INF del sitio de la Interfaz Web en los servidores de aplicaciones de Java.

2. Busque y elimine las siguientes líneas en cada archivo:

   DoNotUseDefaultCSL=On
   BrowserProtocol=HTTPonTCP
   LocHttpBrowserAddress=!

[#163695]

No se puede actualizar Citrix online plug-in en dispositivos que ejecutan sistemas operativos Windows Embedded

La Interfaz Web puede ofrecerle instalar o actualizar Citrix online plug-in en dispositivos que ejecutan sistemas operativos Windows Embedded; sin embargo, la instalación fallará. Puede evitar este problema mediante la instalación manual de la versión más reciente de Citrix online plug-in en el dispositivo incrustado. Si esto no es posible, puede modificar los parámetros del sitio para impedir que aparezcan estos mensajes de instalación:

1. En el menú Inicio de Windows, haga clic en Todos los programas > Citrix > Management Consoles > Citrix Web Interface Management.

2. En el panel izquierdo de la consola Administración de la Interfaz Web de Citrix, haga clic en Sitios Web XenApp y seleccione el sitio en el panel de resultados.

3. En el panel Acción, haga clic en Distribución de clientes. Para los sitios que solo ofrecen aplicaciones en línea, seleccione la casilla de verificación Cliente nativo y haga clic en Propiedades.

4. Haga clic en Detección de clientes.

5. Quite la marca de la casilla de verificación Ofrecer actualizaciones para clientes y seleccione Sólo si no se puede acceder a los recursos o Nunca.

[#164709]

Falla el uso de Kerberos al configurar la delegación en servidores XenApp que ejecutan Windows Server 2008

Debido a un problema con Windows Server 2008, si se configura Active Directory para que use Kerberos solo para la autenticación cuando se establece una relación de confianza con los servidores XenApp para la delegación, esto provoca la falla de la autenticación. Este problema ocurre en los servidores XenApp que ejecutan Windows Server 2008 con Service Pack 2, Windows Server 2008 x64 Editions con Service Pack 2 y Windows Server 2008 R2. Para habilitar la integración con AD FS y la autenticación, mediante paso de credenciales (pass-through) con tarjeta inteligente desde Access Gateway con servidores XenApp que ejecutan Windows Server 2008, seleccione el parámetro Usar cualquier protocolo de autenticación en lugar del parámetro Solo usar Kerberos que se indica en la documentación. [#169269]

No se puede iniciar el escritorio virtual cuando se accede a la Interfaz Web desde algunos dispositivos que ejecutan Windows Embedded CE 6.0

En algunos casos, los usuarios de los clientes ligeros de WYSE V30LE que ejecutan Windows Embedded CE 6.0 e Internet Explorer 6.*x* pueden observar que al conectarse a sitios Web de XenApp y seleccionar un enlace de texto para iniciar un escritorio virtual, el escritorio no se inicia. Para evitar este problema, los usuarios deben iniciar el escritorio haciendo clic en el icono que se muestra junto al enlace. [#218317]

No está disponible la actualización de cliente y el control del área de trabajo para usuarios de Firefox 3.6

Debido a un cambio en Mozilla Firefox 3.6, el control del área de trabajo está automáticamente deshabilitado para los usuarios que acceden a la Interfaz Web con este explorador. Además, el proceso de detección e instalación de clientes no puede detectar los números de versión de clientes Citrix instalados por usuarios de Firefox 3.6 y, por lo tanto, no puede ofrecer a estos usuarios la oportunidad de actualizar sus clientes. [#230068]

No está disponible el control del área de trabajo en algunos dispositivos que ejecutan Windows Mobile 6.1

En algunos casos, los usuarios de dispositivos de mano HP iPAQ 910c, que ejecutan Windows Mobile 6.1 Professional e Internet Explorer Mobile, pueden observar que cuando inician sesión en sitios Web XenApp el control del área de trabajo no funciona correctamente. [#230580]

No está disponible, de manera intermitente, el control del área de trabajo en algunos dispositivos que ejecutan Windows Embedded CE 6.0 R2

En algunos casos, los usuarios de los clientes ligeros de HP t5540 que ejecutan Windows Embedded CE 6.0 R2 e Internet Explorer 6.*x* pueden observar que cuando inician sesión en sitios Web XenApp, en ocasiones el control del área de trabajo no funciona al hacer clic en el botón Reconectar. [#230654]

No es posible utilizar el paso de credenciales (pass-through) con tarjeta inteligente desde Access Gateway con XenApp 6.0.

Debido a un problema con XenApp 6.0, cuando está habilitado el paso de credenciales (pass-through) con tarjeta inteligente en Access Gateway, los usuarios de tarjeta inteligente que acceden a los sitios de Access Gateway integrados no pueden tener acceso a los recursos. Los usuarios que hacen clic en un vínculo para acceder a un recurso distribuido por XenApp 6.0 reciben el mensaje de error: "Ocurrió un error al establecer la conexión solicitada". Para evitar este problema, configure el sitio de manera que se solicite el PIN a los usuarios de tarjeta inteligente cada vez que acceden a un recurso. [#230942]

http://www.citrix.com/

Administración de la Interfaz Web

La Interfaz Web da acceso a los usuarios a las aplicaciones y el contenido de XenApp y a los escritorios virtuales de XenDesktop. Los usuarios acceden a sus recursos por medio de un explorador Web estándar o mediante Citrix Online Plug-in.

La Interfaz Web emplea tecnología Java y .NET que se ejecuta en un servidor Web para crear dinámicamente una representación HTML de las comunidades de servidores para sitios Web de XenApp. Los usuarios ven en su pantalla todos los recursos (aplicaciones, contenido y escritorios) publicados para ellos por los administradores en las comunidades de servidores. Es posible crear sitios Web independientes para el acceso a recursos o a sitios Web que pueden integrarse en el portal de la empresa. Además, la Interfaz Web permite configurar parámetros para los usuarios que accedan a los recursos mediante Citrix Online Plug-in.

Se pueden crear y configurar sitios de la Interfaz Web en Microsoft Internet Information Services (ISS) mediante la consola Administración de la Interfaz Web de Citrix. La consola solo se instala con la Interfaz Web para Microsoft Internet Information Services. Para obtener más información sobre el uso de esta herramienta, consulte Configuración de sitios mediante la consola de administración de la Interfaz Web de Citrix.

También es posible modificar el archivo de configuración de sitios (WebInterface.conf) para administrar los sitios de la Interfaz Web. Para obtener más información, consulte Configuración de sitios mediante archivos de configuración.

Los sitios Web XenApp también pueden personalizarse y ampliarse. La documentación del kit de desarrollo (SDK) de la Interfaz Web explica cómo configurar sitios usando estos métodos.

Funciones de la Interfaz Web

Los dos tipos de sitios de la Interfaz Web le permiten proporcionar a los usuarios diferentes métodos de acceso a sus recursos, según sus necesidades.

Sitios Web XenApp: Puede proporcionar a los usuarios un sitio Web al que pueden acceder mediante un explorador Web. Una vez que se autenticaron, los usuarios pueden acceder a los recursos en línea y a las aplicaciones sin conexión mediante un cliente Citrix.

Sitios de XenApp Services: Puede usar Citrix Online Plug-in junto con la Interfaz Web para integrar los recursos a los escritorios de los usuarios. Para acceder a aplicaciones, escritorios virtuales y contenido en línea, los usuarios pueden hacer clic en iconos de su escritorio o en el menú Inicio, o pueden hacer clic en el área de notificación del escritorio del equipo. Puede permitir que los usuarios accedan a y modifiquen ciertas opciones de configuración, como parámetros de sonido, presentación e inicio de sesión.

Funciones de administración

Funcionamiento con varias comunidades de servidores. Puede configurar varias comunidades de servidores y presentar a los usuarios los recursos que están a su disposición en todas las comunidades. Puede configurar cada comunidad de servidores por separado mediante la tarea Comunidades de servidores de la consola Administración de la Interfaz Web de Citrix. Para obtener más información, consulte Para configurar la comunicación con el servidor.

Recuperación ante desastres. Puede especificar comunidades de servidores XenApp y XenDesktop para usar en caso de emergencia cuando los usuarios no puedan tener acceso a ninguna de las comunidades de producción, quizá debido a un corte de suministro eléctrico o a un problema con la red. Esto permite establecer normas para afrontar la pérdida de acceso a todos los servidores de producción a fin de que los escritorios o las aplicaciones de líneas de negocios no dejen de estar disponibles de manera repentina.

Configuración de sitios compartidos. La Interfaz Web para Microsoft Internet Information Services permite especificar un sitio "maestro" que puede compartir su archivo de configuración en la red. Otros sitios pueden configurarse para usar la configuración del sitio maestro en lugar de usar un archivo local.

Integración con tecnologías Web conocidas. Puede acceder a la interfaz de programación de aplicaciones (API) de la Interfaz Web mediante ASP.NET de Microsoft y JavaServer Pages de Sun Microsystems. La Interfaz Web para servidores de aplicaciones de Java es independiente de la plataforma en que se utilice, por lo tanto, puede instalarse en sistemas operativos Windows donde no se use Microsoft Internet Information Services (IIS) como servidor Web.

Características del acceso a los recursos

XenApp VM Hosted Apps XenApp tiene la capacidad de distribuir aplicaciones en línea desde equipos virtuales. Esto permite publicar aplicaciones que no sean compatibles con Remote Desktop Services o que aún no estén validadas para dichos servicios, o aplicaciones cuya instalación no se admite en sistemas operativos Windows Server.

Perfil móvil de usuarios. Puede asociar grupos de usuarios con comunidades específicas de servidores a fin de proporcionar una experiencia uniforme a los usuarios, independientemente de su ubicación actual o del servidor en el que inician sesión. De esta manera, los usuarios que viajan al exterior por negocios, por ejemplo, pueden iniciar sesión en un servidor local de la Interfaz Web y recibir automáticamente recursos en su idioma nativo desde una comunidad ubicada en su país de origen.

Respaldo para comunidades UNIX. El respaldo para las comunidades de servidores XenApp para UNIX permite que la Interfaz Web muestre y distribuya aplicaciones que se ejecutan en plataformas UNIX en los dispositivos de los usuarios.

Respaldo para Active Directory y nombre principal de usuario. Todos los componentes de la Interfaz Web son compatibles con Active Directory de Microsoft. Los usuarios que visitan sitios Web XenApp pueden iniciar sesión en comunidades de servidores que forman parte de una instalación de Active Directory y acceder sin problemas a las aplicaciones y el contenido. Las pantallas de inicio de sesión son compatibles con los nombres principales de usuario (UPN) que usa Active Directory.

Usuarios anónimos. La Interfaz Web permite a los usuarios acceder a las aplicaciones de XenApp mediante el inicio de sesión en sitios Web XenApp con una cuenta anónima.

Características de seguridad

Respaldo para Secure Sockets Layer y Transport Layer Security. La Interfaz Web es compatible con el protocolo SSL (Secure Sockets Layer), que protege la comunicación entre el servidor de la Interfaz Web y las comunidades de servidores. La implementación de SSL en el servidor Web junto con el uso de exploradores Web compatibles con SSL aseguran la protección de los datos a medida que pasan por la red. La Interfaz Web usa Microsoft .NET Framework para implementar SSL y criptografía.

Respaldo para Access Gateway. Citrix Access Gateway es un dispositivo informático de red privada virtual (VPN) con SSL universal que, junto con la Interfaz Web, proporciona un punto de acceso único y seguro a cualquier recurso de información, tanto de datos como de voz. Access Gateway combina las mejores características del protocolo IPSec (Internet Protocol Security) y VPN con SSL sin los costosos y dificultosos procesos de implementación y administración, funciona por medio de cualquier servidor de seguridad y respalda todos los recursos y protocolos.

Respaldo para Secure Gateway. Secure Gateway, junto con la Interfaz Web, proporcionan un punto de acceso a Internet único, seguro y cifrado para los servidores situados en las redes internas de la organización. Secure Gateway simplifica la administración de certificados, dado que el certificado del servidor sólo es necesario en el servidor Secure Gateway, en lugar de tener que instalar uno por cada servidor de la comunidad.

Respaldo para tarjetas inteligentes. La Interfaz Web respalda el uso de tarjetas inteligentes para la autenticación de usuarios a fin de proporcionar acceso seguro a las aplicaciones, el contenido y los escritorios. El uso de tarjetas inteligentes simplifica el proceso de autenticación para los usuarios a la vez que mejora la seguridad de inicio de sesión.

Generación de tiquets. Esta característica mejora el nivel de seguridad de la autenticación. La Interfaz Web obtiene tiques para la autenticación de los usuarios ante los recursos. Los tiquets tienen un periodo de validez configurable y son válidos durante un solo inicio de sesión. Después de su utilización, o después de haber caducado, el tique deja de ser válido y ya no se puede usar para acceder a los recursos. El uso de tiques elimina la necesidad de incluir las credenciales de forma explícita en los archivos .ica que usa la Interfaz Web para conectarse con los recursos.

Redundancia de Secure Ticket Authority. Puede configurar varias Secure Ticket Authorities (STA) redundantes para los usuarios que acceden a los recursos por medio de Access Gateway. Esto permite disminuir la posibilidad de que STA se vuelva no disponible en medio de una sesión de usuario, lo que impide la reconexión con la sesión. Cuando se habilita la redundancia, la Interfaz Web intenta obtener y otorgar a la puerta de enlace dos tiques de dos STA diferentes. Si no se puede establecer contacto con una de las STA durante una sesión de usuario, la sesión continúa de manera ininterrumpida mediante el uso de la segunda STA.

Cambio de contraseñas. Los usuarios que inician sesiones en la Interfaz Web o en Citrix Online Plug-in mediante credenciales de dominio proporcionadas de manera explícita tienen la opción de cambiar su contraseña de Windows si ésta caduca. Los usuarios pueden cambiar sus contraseñas independientemente de si su equipo se encuentra en el dominio en el que intentan autenticarse.

Autoservicio de cuentas. La integración con el autoservicio de cuentas de Citrix Password Manager permite a los usuarios restablecer su contraseña de red y desbloquear su cuenta respondiendo a una serie de preguntas de seguridad.

Características de la distribución de clientes

Instalación de clientes basada en la Web. Cuando un usuario visita un sitio Web XenApp, la Interfaz Web detecta el tipo de dispositivo y de explorador Web, y solicita al usuario que instale el cliente Citrix adecuado, si hay alguno disponible. Debido a las mayores restricciones de seguridad en los modernos sistemas operativos y exploradores Web, los usuarios pueden tener problemas a la hora de descargar e instalar clientes Citrix. Para facilitar esta tarea, la Interfaz Web ofrece un proceso de detección e instalación de clientes que guía a los usuarios a través de la instalación de clientes, incluida, cuando corresponde, la reconfiguración del explorador Web. Esto facilita el trabajo de los usuarios cuando deben acceder a sus recursos, incluso desde los entornos más restringidos.

Respaldo para Citrix Online Plug-in. Citrix Online Plug-in permite a los usuarios acceder a los recursos directamente desde su escritorio, sin necesidad de usar un explorador Web. La interfaz de usuario de Citrix Online Plug-in también se puede “bloquear” para evitar que el usuario realice una configuración errónea.

Respaldo para Citrix Offline Plug-in. Citrix Offline Plug-In permite a los usuarios transmitir por secuencias aplicaciones XenApp a sus escritorios y abrirlas localmente. Puede instalar el plug-in con Citrix Online Plug-In para proporcionar el conjunto completo de funciones de virtualización de aplicaciones del cliente Citrix o bien, puede instalar solo el plug-in en los escritorios de los usuarios para que estos puedan acceder a las aplicaciones por medio de un explorador Web mediante un sitio Web XenApp.

Novedades de esta versión

La Interfaz Web ofrece las siguientes mejoras y funciones nuevas en esta versión:

Interfaz del usuario final actualizada. Se ha actualizado el diseño y el esquema de colores para los usuarios finales con el fin de mejorar la navegación y la legibilidad.

Sesiones compartidas para las aplicaciones alojadas en equipos virtuales. Ahora la Interfaz Web admite las sesiones compartidas para las aplicaciones alojadas en equipos virtuales (VM). Esta función solamente se encuentra disponible para aplicaciones integradas y usuarios no anónimos.

Acceso a varios escritorios para los usuarios. En las versiones anteriores de la Interfaz Web, los usuarios solamente podían obtener acceso a una sola sesión de un escritorio por grupo de escritorios. Ahora los usuarios pueden obtener acceso a varias sesiones de los escritorios en los grupos de escritorios. Para obtener más información sobre la asignación de escritorios a los usuarios, consulte la documentación de la versión 5 de XenDesktop.

Mayor compatibilidad de tarjeta inteligente para Access Gateway. Ahora la autenticación con tarjeta inteligente para la Interfaz Web es compatible con más entornos. Ahora la Interfaz Web puede aceptar nombres principales de usuario (UPN) de Access Gateway así como nombres de usuarios y dominios. Además, se ha actualizado la Interfaz Web para cumplir con los requisitos de FIPS. Esta nueva función solamente se puede utilizar con la opción de autenticación mediante paso de credenciales con tarjeta inteligente. Además, es necesario iniciar sesión como administrador de dominio. Para obtener más información sobre la configuración de la compatibilidad con la tarjeta inteligente en Access Gateway, consulte la documentación de Access Gateway.

Capacidad de establecer valores predeterminados adicionales. Los administradores pueden configurar valores predeterminados para todos los parámetros relacionados con el ancho de banda como la calidad del audio, la profundidad del color, el perfil del ancho de banda, las asignaciones de las impresoras y el tamaño de las ventanas.

Firma de archivos ICA. La Interfaz Web firma digitalmente los archivos ICA generados para que los clientes ICA compatibles puedan validar el hecho de que los archivos provienen de un origen de confianza.

Componentes de la Interfaz Web

Un sistema de Interfaz Web comprende la interacción de tres componentes de red:

- Una o varias comunidades de servidores
- Un servidor Web
- Un dispositivo de usuario con un explorador Web y un cliente Citrix

Comunidades de servidores

Un grupo de servidores administrados como una entidad única que funcionan conjuntamente para ofrecer recursos a los usuarios se denomina colectivamente *comunidad de servidores*. Una comunidad de servidores se compone de varios servidores que ejecutan XenApp o XenDesktop, pero no una mezcla de ambos.

Una de las funciones fundamentales de una comunidad de servidores es la publicación de recursos. Se trata de un proceso mediante el cual los administradores ponen a disposición de los usuarios una serie de recursos (aplicaciones, contenido y escritorios) distribuidos desde la comunidad de servidores. Cuando un administrador publica un recurso para un grupo de usuarios, dicho recurso se presenta como un objeto con el que los clientes Citrix pueden conectarse e iniciar sesiones.

Con la Interfaz Web, los usuarios pueden iniciar una sesión en la comunidad de servidores y recibir una lista personalizada de los recursos publicados para su nombre de usuario. La lista de recursos se denomina conjunto de recursos. El servidor de la Interfaz Web funciona como un punto de acceso para la conexión con una o varias comunidades de servidores. El servidor de la Interfaz Web busca la información sobre conjuntos de recursos disponibles en las comunidades de servidores y presenta el resultado en páginas HTML que el usuario puede ver en un explorador Web.

Para obtener información de las comunidades de servidores, el servidor Interfaz Web se comunica con el servicio XML de Citrix que se ejecuta en uno o más servidores de la comunidad. Citrix XML Service es un componente de XenApp y XenDesktop que proporciona información sobre recursos a los clientes Citrix y los servidores de la Interfaz Web mediante TCP/IP y HTTP. Este servicio sirve de punto de contacto entre la comunidad de servidores y el servidor de la Interfaz Web. Citrix XML Service se instala con XenApp y XenDesktop.

Servidor Web

El servidor Web aloja a la Interfaz Web. La Interfaz Web proporciona los siguientes servicios:

- Autentica a los usuarios ante las comunidades de servidores
- Obtiene información sobre los recursos disponibles, incluida una lista de los recursos a los que puede acceder cada usuario

Dispositivo del usuario

Un *dispositivo de usuario* es cualquier dispositivo informático capaz de ejecutar un cliente Citrix y un explorador Web. Los dispositivos de usuarios pueden ser equipos de escritorio, equipos portátiles, equipos de red, terminales y equipos de mano, entre otros.

En un dispositivo de usuario, el explorador y el cliente Citrix funcionan en conjunto como visor y motor. El explorador permite que los usuarios vean los conjuntos de recursos (creados por los scripts del servidor alojados en el servidor de la Interfaz Web), mientras el cliente actúa como el motor que permite que los usuarios accedan a los recursos.

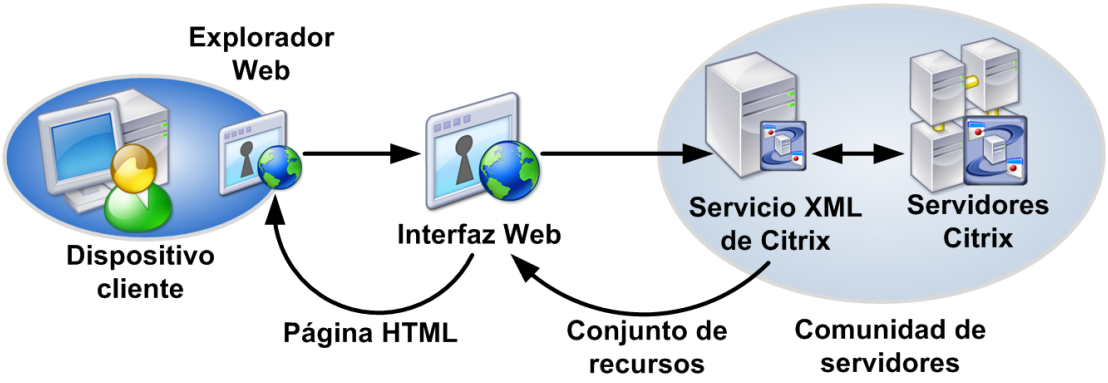
La Interfaz Web permite la *distribución de clientes basada en la Web*, que es un método de instalación de clientes Citrix desde un sitio Web. Cuando un usuario visita un sitio creado con la Interfaz Web, el proceso de detección e instalación de clientes basado en la Web detecta el dispositivo, y se le solicita al usuario la instalación de un cliente Citrix apropiado. En algunos entornos, el proceso de detección e instalación de clientes también puede detectar la presencia o la ausencia de un cliente instalado, y solicitar una instalación al usuario solo cuando sea necesario. Para obtener más información, consulte Configuración de los mensajes de instalación y distribución de clientes.

La Interfaz Web respalda numerosas combinaciones de exploradores y clientes Citrix. Para obtener una lista completa de las combinaciones de exploradores y clientes respaldadas, consulte Requisitos de dispositivos de usuario.

Funcionamiento de la Interfaz Web

A continuación se describen las interacciones típicas entre una comunidad de servidores, un servidor que ejecuta la Interfaz Web y un dispositivo del usuario.

Este gráfico muestra un ejemplo de una interacción típica de la Interfaz Web. El explorador Web del dispositivo del usuario envía información al servidor Web, el cual se comunica con la comunidad de servidores para permitir al usuario acceder a los recursos.



- Los usuarios se autentican en la Interfaz Web mediante un explorador Web.
- El servidor Web lee las credenciales del usuario y reenvía esta información al servicio XML de Citrix ubicado en los servidores de las comunidades de servidores. El servidor designado actúa como un intermediario entre el servidor Web y los demás servidores de la comunidad.
- El servicio XML de Citrix en el servidor designado obtiene de los servidores la lista de recursos a los que puede acceder el usuario. Estos recursos constituyen el conjunto de recursos del usuario. El servicio XML de Citrix obtiene el conjunto de recursos desde el sistema Independent Management Architecture (IMA).
- En una comunidad de servidores XenApp para UNIX, el servicio XML de Citrix en el servidor designado usa la información obtenida a partir del examinador ICA para determinar a qué aplicaciones puede acceder el usuario.
- Posteriormente, pasa la información sobre el conjunto de recursos del usuario a la Interfaz Web que se ejecuta en el servidor.
- El usuario hace clic en el icono que representa un recurso en la página HTML.
- A continuación, se contacta con el servicio XML de Citrix para buscar el servidor menos ocupado de la comunidad. El servicio XML de Citrix identifica el servidor menos ocupado y devuelve la dirección de este servidor a la Interfaz Web.
- La Interfaz Web se comunica con el cliente Citrix (en algunos casos, usa el explorador Web como intermediario).
- El cliente Citrix inicia una sesión en el servidor de la comunidad, según la información de conexión suministrada por la Interfaz Web.

Requisitos del sistema para la Interfaz Web

Para iniciar la interfaz Web, los servidores deben ejecutar un producto de Citrix respaldado.

La Interfaz Web respalda las siguientes versiones del producto:

- Citrix XenDesktop 5.6 Service Pack 1
- Citrix XenDesktop 5.6
- Citrix XenDesktop 5.5
- Citrix XenDesktop 5.0 Service Pack 1
- Citrix XenDesktop 5.0
- Citrix XenDesktop 4.0
- Citrix XenDesktop 3.0
- Citrix XenDesktop 2.1
- Citrix XenDesktop 2.0
- Citrix XenApp 6.5 para Microsoft Windows Server 2008 R2
- Citrix XenApp 6.0 para Microsoft Windows Server 2008 R2
- Citrix XenApp 5.0, con Feature Pack 2, para Microsoft Windows Server 2003 x64 Edition
- Citrix XenApp 5.0, con Feature Pack 2, para Microsoft Windows Server 2003
- Citrix XenApp 5.0, con Feature Pack 1, para Microsoft Windows Server 2008 x64 Edition
- Citrix XenApp 5.0, con Feature Pack 1, para Microsoft Windows Server 2008
- Citrix XenApp 5.0, con Feature Pack 1, para Microsoft Windows Server 2003 x64 Edition
- Citrix XenApp 5.0, con Feature Pack 1, para Microsoft Windows Server 2003
- Citrix XenApp 5.0 para Microsoft Windows Server 2008 x64 Edition
- Citrix XenApp 5.0 para Microsoft Windows Server 2008
- Citrix XenApp 5.0 para Microsoft Windows Server 2003 x64 Edition
- Citrix XenApp 5.0 para Microsoft Windows Server 2003

- Citrix XenApp 4.0 con Feature Pack 1 para sistemas operativos UNIX
- Citrix Presentation Server 4.5 con Feature Pack 1 para Windows Server 2003 x64 Edition
- Citrix Presentation Server 4.5 con Feature Pack 1 para Windows Server 2003
- Citrix Presentation Server 4.5 para Windows Server 2003 x64 Edition
- Citrix Presentation Server 4.5 para Windows Server 2003

Importante: Para la compatibilidad con XenApp 4.0 con Feature Pack 1 para UNIX es necesario realizar una configuración manual adicional en los sitios. Para obtener más información, consulte Para configurar la compatibilidad con XenApp 4.0, con Feature Pack 1, para UNIX.

La Interfaz Web funciona con estos productos en todas sus plataformas compatibles. Para obtener una lista de las plataformas respaldadas, consulte la documentación de su servidor Citrix. Citrix recomienda instalar el Service Pack más reciente para los sistemas operativos de los servidores.

Requisitos mínimos de software

Si no se tiene instalada la versión más reciente, algunas funciones nuevas no estarán disponibles. Por ejemplo, la migración de comunidades integrada solo está disponible cuando se realiza la actualización a XenApp 6.0.

La siguiente tabla resume los requisitos mínimos de software para las funciones fundamentales de la Interfaz Web.

Nota: Para confirmar el respaldo para la Interfaz Web 5.4 en versiones específicas de productos Citrix, consulte los Requisitos del sistema para el producto en cuestión.

Función de la Interfaz Web	Requisitos de software
migración de comunidades XenApp	Citrix XenApp 6.0
Perfil móvil de usuarios	Citrix XenDesktop 4.0 Citrix XenApp 6.0
Aplicaciones de servidor de equipos virtuales (VM) en XenApp	Citrix XenApp 5.0 con Feature Pack 2
Recuperación ante desastres	Citrix XenDesktop 4.0 Citrix XenApp 5.0 con Feature Pack 2
Redundancia de Secure Ticket Authority	Citrix XenDesktop 4.0 Citrix XenApp 5.0 con Feature Pack 2 Citrix Access Gateway 4.6, Standard Edition
Respaldo para Windows 7 e Internet Explorer 8.0	Citrix XenDesktop 4.0 Citrix XenApp 5.0 con Feature Pack 2 Citrix Online Plug-in 11.2 Citrix Offline Plug-in 5.2
Reinicio de escritorios virtuales	Citrix XenDesktop 3.0 Citrix Desktop Receiver 11.1
Redirección de carpetas especiales	Citrix XenApp 5.0 Citrix XenApp Plugin para aplicaciones alojadas en servidor 11.0 para Windows
Suavizado de fuentes	Citrix XenApp 5.0 Citrix XenApp Plugin para aplicaciones alojadas en servidor 11.0 para Windows

Respaldo para XenDesktop	Citrix XenDesktop 2.0 Citrix Desktop Receiver Embedded Edition 10.250
Compatibilidad con Windows Vista e Internet Explorer 7.0	Citrix XenDesktop 2.0 Citrix Presentation Server 4.5 Clientes de Citrix Presentation Server 10.1 para Windows
Respaldo para aplicaciones sin conexión	Citrix Presentation Server 4.5 Citrix Streaming Client 1.0 Agente de Citrix Program Neighborhood 10.0
Soporte para AD FS	Citrix Presentation Server 4.5
Respaldo para directivas de control de acceso	Citrix XenDesktop 2.0 Citrix Presentation Server 4.5 Citrix Access Gateway 4.2 con Advanced Access Control Clientes de Citrix MetaFrame Presentation Server para Windows de 32 bits, versión 9.0
Autoservicio de cuentas	Citrix Password Manager 4.0
Cambio de contraseña del usuario	Citrix XenDesktop 2.0 Citrix Presentation Server 4.5 Agente de Citrix Program Neighborhood 10.1
Fiabilidad de la sesión	Citrix XenDesktop 2.0 Citrix Presentation Server 4.5 Clientes de Citrix MetaFrame Presentation Server para Windows de 32 bits, versión 9.0
Control del área de trabajo	Citrix XenDesktop 2.0 Citrix Presentation Server 4.5 Cliente de Citrix MetaFrame Presentation Server para Windows de 32 bits, versión 8.0
Respaldo para tarjeta inteligente	Citrix XenDesktop 3.0 Citrix Presentation Server 4.5 Citrix Desktop Receiver 11.1 Cliente ICA Citrix para Windows de 32 bits 7.0

Respaldo para Secure Gateway	Citrix XenDesktop 2.0 Citrix Presentation Server 4.5 Citrix XenApp 4.0 con Feature Pack 1 para sistemas operativos UNIX Cliente ICA Citrix para Windows de 32 bits 7.0
Autenticación NDS	Citrix Presentation Server 4.5 Cliente ICA Citrix para Windows de 32 bits 7.0
Direcciones DNS	Citrix XenDesktop 2.0 Citrix Presentation Server 4.5 Citrix XenApp 4.0 con Feature Pack 1 para sistemas operativos UNIX Cliente ICA Citrix para Windows de 32 bits 7.0
Publicación mejorada de contenido	Citrix Presentation Server 4.5 Cliente ICA Citrix para Windows de 32 bits 7.0
Equilibrio de carga	Citrix XenDesktop 2.0 Citrix Presentation Server 4.5 Citrix XenApp 4.0 con Feature Pack 1 para sistemas operativos UNIX
Respaldo para servidor de seguridad (firewall) en el lado del servidor	Citrix XenDesktop 2.0 Citrix Presentation Server 4.5 Citrix XenApp 4.0 con Feature Pack 1 para sistemas operativos UNIX
Respaldo para servidor de seguridad (firewall) en el lado del cliente	Cliente ICA Citrix para Windows de 32 bits 7.0
Autenticación mediante paso de credenciales (PassThrough)	Citrix Presentation Server 4.5 Cliente Program Neighborhood completo para Windows de 32 bits Agente de Citrix Program Neighborhood 7.0
Conexión a escritorio remoto (RDP)	Citrix XenDesktop 4.0 Citrix Presentation Server 4.5

Requisitos generales de configuración

Los servidores deben ser miembros de una comunidad de servidores. Los servidores de la comunidad deben tener recursos publicados (aplicaciones, contenido o escritorios). Para obtener más información sobre la pertenencia a una comunidad de servidores y la publicación de recursos en una comunidad de servidores, consulte la documentación de su servidor Citrix.

Los servidores XenApp para UNIX también deben tener aplicaciones publicadas. Además, estas aplicaciones deben estar configuradas para ser utilizadas con la Interfaz Web. Para obtener más información sobre la instalación de Citrix XML Service para UNIX y la configuración de aplicaciones para utilizarlas con la Interfaz Web, consulte la documentación de XenApp para UNIX.

Requisitos del servidor Web

Actualizado: 2014-09-24

Los clientes Citrix deben estar en el servidor para poder llevar a cabo la instalación basada en la Web de ellos. Para obtener más información sobre las versiones de clientes respaldadas, consulte Requisitos de dispositivos de usuario. Para obtener más información sobre cómo copiar los clientes en el servidor de la Interfaz Web, consulte Copia de los archivos de instalación de clientes en la Interfaz Web.

En plataformas Windows

Puede instalar la Interfaz Web en las siguientes plataformas Windows:

Sistema operativo	Servidor Web	Runtime/JDK	Motor de servlet

Windows Server 2008 R2 x64 Windows Server 2008 R2 con Service Pack 1	Internet Information Services 7.5	.NET Framework 3.5 con Service Pack 1 Visual J#.NET 2.0 Second Edition ASP.NET 2.0	N/D
Windows Server 2008 x64 Editions con Service Pack 2 Windows Server 2008 x86 con Service Pack 2	Internet Information Services 7.0		
Windows Server 2003 R2 x86 con Service Pack 2 Windows Server 2003 Standard Edition x86 con Service Pack 2 Windows Server 2003 Enterprise Edition x86 con Service Pack 2 Windows Server 2003 R2 Standard Edition x86 con Service Pack 2 Windows Server 2003 R2 Standard Edition x64 con Service Pack 2	Internet Information Services 6.0		
Windows Server 2003 Standard Edition x86 con Service Pack 2	Apache 2.2.*x*	Java 1.6.*x*	Apache Tomcat 6.0.*x*

Si desea utilizar Microsoft Internet Information Services (IIS), debe configurar el servidor para agregarle la función de servidor apropiada e instalar IIS y ASP.NET (que es un subcomponente de IIS). Si IIS no está instalado cuando usted instala .NET Framework, debe instalar IIS y volver a instalar el Framework, o bien instalar IIS y ejecutar el comando aspnet_regiis.exe -i en el directorio C:\Windows\Microsoft.NET\Framework*Version*. Los archivos redistribuibles de .NET Framework y J# se encuentran en la carpeta \Support del soporte de instalación de XenApp y XenDesktop.

Requisitos del usuario

Actualizado: 2014-05-23

Las siguientes combinaciones de explorador Web y sistema operativo son compatibles para los usuarios que quieren acceder a sitios de la Interfaz Web:

Explorador Web	Sistema operativo
Internet Explorer 11	Windows 8.1 de 32 bits Windows 8.1 de 64 bits Windows 8 de 32 bits Windows 8 de 64 bits Windows 2012 de 64 bits Windows 2012 R2 de 64 bits Windows 7 de 32 bits con Service Pack 1 (SP1) Windows 7 de 64 bits con Service Pack 1 (SP1) Windows Server 2008 R2 con Service Pack 1 (SP1) de 64 bits
Internet Explorer 10	Windows 7 de 32 bits con Service Pack 1 (SP1) Windows 7 de 64 bits con Service Pack 1 (SP1) Windows Server 2008 R2 con Service Pack 1 (SP1) de 64 bits
Internet Explorer 9.*x* (modo de 32 bits)	Windows Vista de 32 bits con Service Pack 2 o superior Windows Vista de 64 bits con Service Pack 2 o superior Windows 7 de 32 bits RTM o superior Windows 7 de 64 bits RTM o superior Windows Server 2008 de 32 bits con Service Pack 2 o superior Windows Server 2008 de 64 bits con Service Pack 2 o superior Windows Server 2008 R2 de 64 bits

Internet Explorer 8.*x* (modo de 32 bits)	Windows 7 de 64 bits Windows 7 de 32 bits Windows XP Professional con Service Pack 3 Windows XP Professional x64 Edition con Service Pack 2 Windows Vista de 32 bits con Service Pack 2 Windows Vista de 64 bits con Service Pack 2 Windows Server 2008 R2 Windows Server 2008 con Service Pack 2 Windows Server 2003 con Service Pack 2
Internet Explorer 7.*x* (modo de 32 bits)	Windows Vista de 64 bits con Service Pack 2 Windows Vista de 32 bits con Service Pack 2 Windows Server 2008 con Service Pack 2 Windows Server 2003 con Service Pack 2
Safari 5.*x*	Mac OS X Snow Leopard 10.6
Safari 4.*x*	Mac OS X Leopard 10.5
Mozilla Firefox 4.*x* (modo de 32 bits)	Windows 7 de 64 bits Windows 7 de 32 bits Windows XP Professional con Service Pack 3 Windows XP Professional x64 Edition con Service Pack 2 Windows Vista de 32 bits con Service Pack 2 Windows Vista de 64 bits con Service Pack 2 Windows Server 2003 con Service Pack 2
Mozilla Firefox 3.*x*	Mac OS X Snow Leopard 10.6 Mac OS X Leopard 10.5 Windows XP Professional x32 Edition con Service Pack 3 Windows Vista de 32 bits con Service Pack 2 Windows 7 de 32 bits Red Hat Enterprise Linux 5.4 Desktop Windows Server 2003 con Service Pack 2

Mozilla 1.7	Solaris 10

Nota: La Interfaz Web 5.4 solo recibe respaldo para las versiones de software indicadas en esta página. Aunque es posible que las versiones más recientes del software también funcionen, su operación no ha sido sometida a pruebas y por lo tanto no reciben respaldo.

Requisitos para el acceso a aplicaciones sin conexión

Las siguientes combinaciones de exploradores Web y sistemas operativos ofrecen respaldo para los usuarios que desean acceder a las aplicaciones sin conexión:

Explorador Web	Sistema operativo
Internet Explorer 8.*x* (modo de 32 bits)	Windows 7 64-bit Editions Windows 7 32-bit Editions Windows Vista de 64 bits Editions con Service Pack 2 Windows Vista de 32 bits Editions con Service Pack 2 Windows XP Professional x64 Edition con Service Pack 2 Windows XP Professional con Service Pack 3 Windows Server 2008 R2 Windows Server 2008 x64 Editions con Service Pack 2 Windows Server 2008 con Service Pack 2 Windows Server 2003 x64 Editions con Service Pack 2 Windows Server 2003 con Service Pack 2
Internet Explorer 7.*x* (modo de 32 bits)	Windows Vista de 64 bits Editions con Service Pack 2 Windows Vista de 32 bits Editions con Service Pack 2 Windows XP Professional x64 Edition con Service Pack 2 Windows XP Professional con Service Pack 3 Windows Server 2008 x64 Editions con Service Pack 2 Windows Server 2008 con Service Pack 2 Windows Server 2003 x64 Editions con Service Pack 2 Windows Server 2003 con Service Pack 2

Mozilla Firefox 3.*x*	Windows 7 64-bit Editions Windows 7 32-bit Editions Windows Vista de 64 bits Editions con Service Pack 2 Windows Vista de 32 bits Editions con Service Pack 2 Windows XP Professional x64 Edition con Service Pack 2 Windows XP Professional con Service Pack 3 Windows Server 2003 con Service Pack 2

Requisitos para otros dispositivos de usuarios

Los usuarios pueden acceder a la Interfaz Web desde clientes ligeros, PDA y otros dispositivos de mano con las siguientes configuraciones:

Dispositivo	Sistema operativo	Explorador Web
iPhone	N/D	Safari 5.*x*
iPad	N/D	Safari 5.*x*
HTC Touch2	Windows Mobile 6.5 Professional	Pocket/WinCE Internet Explorer Opera Mobile 10
HP GY227 WYSE V90	Windows XP Embedded con Service Pack 2	Internet Explorer 6.*x*
HP T5730	Windows Embedded Standard 2009	Internet Explorer 7.*x*
HP T5540	Windows Embedded CE 6.0 R2	Internet Explorer 6.*x*
HP RK270 WYSE V30	Windows Embedded CE 6.0	Internet Explorer 6.*x*
HP GY231	Debian Linux 4.0	Debian Iceweasel 2.0
Symbian E61/E70	Symbian	Explorador Symbian

Requisitos de dispositivos de usuario

Para que los dispositivos de los usuarios funcionen con la Interfaz Web, deben tener, como mínimo, un cliente Citrix respaldado o un explorador Web compatible con Java Runtime Environment. Todos los clientes incluidos en el soporte de instalación de XenApp y XenDesktop son compatibles con la Interfaz Web. Los clientes también pueden descargarse de manera gratuita desde el sitio Web de Citrix.

Citrix recomienda distribuir las versiones más recientes de los clientes entre los usuarios para aprovechar las funciones más avanzadas. Las funciones y capacidades de cada cliente difieren entre sí. Para obtener más información sobre las funciones respaldadas de los clientes, consulte la documentación de cada cliente en particular.

Instalación de la Interfaz Web

La Interfaz Web se instala usando el soporte de instalación de XenApp o XenDesktop.

Puede instalar la Interfaz Web en las siguientes plataformas:

- Un sistema operativo Windows compatible que esté ejecutando:
  - Microsoft Internet Information Services (IIS)
  - Apache Tomcat
- Un sistema operativo UNIX compatible que esté ejecutando:
  - Apache Tomcat
  - IBM WebSphere
  - Sun GlassFish Enterprise Server

Es posible realizar instalaciones y administrar sitios sin supervisión mediante scripts de línea de comandos. Para obtener más información sobre el uso de la línea de comandos con la Interfaz Web, visite Knowledge Center.

Para obtener más información sobre cómo instalar la Interfaz Web, consulte Para instalar la Interfaz Web en Microsoft Internet Information Services e Instalación de la Interfaz Web en servidores de aplicaciones de Java.

Consideraciones sobre seguridad

Si va a instalar la Interfaz Web en un servidor basado en Windows, Citrix recomienda seguir las instrucciones estándar de Microsoft para configurarlo. Para implementaciones en UNIX, siga las recomendaciones del fabricante para su sistema operativo específico.

Cómo ver la asignación de puerto del servicio XML de Citrix

Durante la creación de sitios de la Interfaz Web (IIS) o la generación de archivos .war (Java), el sistema pide el puerto usado por el servicio XML de Citrix. El servicio XML de Citrix es el enlace de comunicación entre la comunidad de servidores y el servidor de la Interfaz Web.

En plataformas Windows se puede configurar Citrix XML Service para compartir el puerto TCP/IP de Internet Information Services. Si este es el caso, debe encontrar el puerto usado por el servicio WWW de Internet Information Services para determinar el puerto de Citrix XML Service. De forma predeterminada, el servicio WWW utiliza el puerto 80. Si se requiere un puerto dedicado para Citrix XML Service, Citrix recomienda utilizar el puerto 8080.

Para obtener una lista de los puertos que están siendo utilizados en plataformas Windows, escriba netstat -a en una línea de comandos. En servidores XenApp para UNIX, escriba ctxnfusesrv -l cuando se le pida introducir un comando para ver la información sobre puertos.

Nota: Si es necesario, puede cambiar el puerto usado por el servicio XML de Citrix en el servidor. Para obtener más información, consulte la documentación del servidor Citrix.

Para instalar la Interfaz Web en Microsoft Internet Information Services

Antes de instalar la Interfaz Web, debe configurar el servidor para agregarle la función de servidor Web e instalar IIS y ASP.NET.

Para usar IIS 7.*x* en Windows Server 2008, instale la función Servidor Web (IIS) y luego habilite los siguientes servicios de función:

- Servidor Web > Desarrollo de aplicaciones > ASP.NET
- Herramientas de administración > Compatibilidad con la administración de IIS 6 > Compatibilidad con la metabase de IIS 6

Si tiene previsto habilitar la autenticación por paso de credenciales (pass-through), por tarjeta inteligente y/o por paso de credenciales con tarjeta inteligente, también necesita instalar los siguientes servicios de función:

- Para la autenticación mediante paso de credenciales y paso de credenciales con tarjeta inteligente, habilite Servidor Web > Seguridad > Autenticación de Windows
- Para usar la autenticación con tarjeta inteligente, habilite Servidor Web > Seguridad > Autenticación de asignaciones de certificado de cliente

Para usar IIS 6.0 en Windows Server 2003, agregue la función Servidor de aplicaciones (IIS, ASP.NET) y habilite ASP.NET.

En IIS cada sitio se asigna a un grupo de aplicaciones. La configuración del grupo de aplicaciones contiene un parámetro que determina el número máximo de procesos de trabajo. Si cambia el valor predeterminado (1), es posible que no pueda ejecutar la Interfaz Web.

Una vez configurada la función del servidor, asegúrese de haber instalado .NET Framework 3.5 con Service Pack 1 y Visual J#.NET 2.0 Second Edition.

Si realiza una actualización desde una versión anterior de la Interfaz Web (hasta la versión 4.5), el programa de instalación le pedirá que cree una copia de seguridad de los sitios existentes antes de actualizarlos.

Importante: Los sitios de configuración centralizada y los sitios de participante invitado de Conferencing Manager ya no reciben respaldo. Si actualiza desde una versión anterior de la Interfaz Web, el programa de instalación eliminará los sitios de participante invitado de Conferencing Manager que existan en el servidor Web. Si hay sitios de configuración centralizada, éstos serán actualizados y convertidos para utilizar la configuración local.

1. Inicie la sesión como administrador.

   Si desea instalar la Interfaz Web desde el soporte de instalación de XenApp o XenDesktop, introduzca el disco en la unidad óptica del servidor Web.

Si descargó la Interfaz Web desde el sitio Web de Citrix, copie el archivo WebInterface.exe en el servidor Web.

2. Desplácese hasta el archivo WebInterface.exe y haga doble clic en él.

3. Seleccione el idioma deseado en la lista. Se detecta el idioma de su sistema operativo y éste aparece como selección predeterminada. Haga clic en OK.

4. En la página de Bienvenida, haga clic en Siguiente.

5. En la página Contrato de licencia, seleccione Acepto el contrato de licencia y haga clic en Siguiente.

6. En la página Ubicación de la instalación, busque la ubicación de la instalación de la Interfaz Web (de forma predeterminada, C:\Archivos de programa (x86)\Citrix\Web Interface\). Haga clic en Next.

7. En la página Ubicación de los clientes, seleccione Copiar los clientes en este equipo. Haga clic en Examinar para buscar los archivos de instalación de los clientes Citrix en el soporte de instalación o en la red.

   El programa de instalación copia el contenido de la carpeta \Citrix Receiver and Plug-ins del soporte de instalación o del punto compartido en la carpeta \Clients de la Interfaz Web, por lo general, C:\Archivos de programa (x86)\Citrix\Web Interface*Versión*\Clients. Todos los sitios Web creados por el proceso de instalación suponen que el servidor Web contiene los archivos cliente en esta estructura de directorios.

   Si no desea copiar los clientes en el servidor Web durante la instalación de la Interfaz Web, seleccione Omitir este paso. Puede copiar los clientes en el servidor en otro momento.

8. Haga clic en Siguiente para continuar, y haga clic de nuevo en Siguiente para confirmar que está preparado para comenzar la instalación.

9. Cuando termine la instalación, haga clic en Finish.

10. En el menú Inicio de Windows, haga clic en Todos los programas > Citrix > Consolas de administración > Citrix Web Interface Management para obtener acceso a la consola Administración de la Interfaz Web de Citrix y comenzar a crear y configurar sus sitios.

Compatibilidad con otros componentes en Windows Server 2003 x64 Editions

En las versiones de 64 bits de Windows Server 2003, la instalación de la Interfaz Web para Microsoft Internet Information Services habilita el respaldo de extensión Web de 32 bits en IIS 6.0 y esto inhabilita el respaldo de extensión de 64 bits. Si desea instalar la Interfaz Web para Microsoft Internet Information Services en una versión de 64 bits de Windows Server 2003, asegúrese de instalar la Interfaz Web antes de instalar cualquier otro software de Citrix, incluidos XenApp, XenDesktop y License Management Console. Este orden de instalación permite que los productos se adapten al respaldo de 32 bits en IIS 6.0. Si instala estos productos en un orden distinto, el servidor Web puede presentar mensajes de error de "servicio no disponible" cuando se intenta acceder a él.

Cuando la Interfaz Web para Microsoft Internet Information Services se instala en Windows Server 2003 x64 Editions, puede no ser compatible con otros productos que requieran filtros ISAPI de 64 bits, como el componente de Windows RPC sobre proxy HTTP. Antes de instalar la Interfaz Web, debe desinstalar RPC sobre proxy HTTP.

Para desinstalar RPC sobre proxy HTTP

1. En el menú Inicio de Windows, haga clic en Panel de control > Agregar o quitar programas.
2. Seleccione Agregar o quitar componentes de Windows.
3. Seleccione Servicios de red y haga clic en Detalles.
4. Seleccione la casilla RPC sobre el proxy HTTP y haga clic en Aceptar.
5. Haga clic en Siguiente para desinstalar el componente RPC sobre proxy HTTP y reinicie el servidor.

Instalación de la Interfaz Web en servidores de aplicaciones de Java

Nota: Si instala la Interfaz Web en IBM WebSphere, aparecerá un mensaje de advertencia de seguridad de aplicaciones indicando que hay un problema con el contenido del archivo was.policy. WebSphere crea este archivo de directivas al seleccionar la opción Enforce Java 2 Security en Security > Global Security. Asegúrese de modificar el archivo was.policy respetando las directivas de Java 2 Security de WebSphere. De lo contrario, la Interfaz Web podría no funcionar correctamente. Este archivo de directivas está ubicado en WEBSPHERE_HOME/AppServer/installedApps/*NodeName*/*WARFileName*.ear/META-INF.

La Interfaz Web para servidores de aplicaciones de Java necesita un motor de servlet para funcionar. Para funcionar con la Interfaz Web, el servidor Web Apache requiere un motor de servlet adicional, como Tomcat (tenge en cuenta que Tomcat se puede usar como un servidor Web autónomo o como un motor de servlet).

Para instalar la Interfaz Web en Tomcat

1. Copie el archivo WebInterface.jar desde el directorio Web Interface del soporte de instalación en un directorio temporal.

2. En una petición de comandos, sitúese en el directorio donde descargó el archivo de instalación y ejecute el programa de instalación escribiendo el comando java -jar WebInterface.jar.

3. Presione INTRO para leer el contrato de licencia.

4. Escriba S para aceptar el contrato de licencia.

5. Seleccione un tipo de sitio en la lista suministrada.

6. Especifique la configuración inicial del sitio respondiendo a las preguntas que verá en pantalla.

7. Luego verá un resumen de las opciones seleccionadas. Si los detalles del sitio son correctos, escriba S para crear el archivo .war. Se crea el archivo .war y se copian los clientes Citrix desde el soporte de instalación, en caso de ser necesario.

8. Siga las instrucciones que aparecen en pantalla para finalizar la instalación del archivo .war.

Para configurar la directiva de seguridad en Sun GlassFish Enterprise Server

Antes de crear sitios Web XenApp configurados para permitir el autoservicio de cuentas en Sun GlassFish Enterprise Server, debe configurar manualmente la directiva de seguridad del servidor.

1. Distribuya el archivo .war del sitio en el servidor.

2. Detenga el servidor Web.

3. Modifique el archivo server.policy en el directorio de configuración del dominio donde está instalado. Por ejemplo, si Sun GlassFish Enterprise Server está instalado en *SunGlassFishEnterpriseServerRoot*/AppServer y el sitio se distribuye en “domain1”, el archivo reside en *SunGlassFishEnterpriseServerRoot*/AppServer/domains/domain1/config.

4. Agregue la configuración siguiente antes de cualquier bloque de concesión de permisos genéricos:

   grant codeBase "file:${com.sun.aas.instanceRoot}/applications/ j2ee-modules/*WARFileName*/-"{ permis

   donde *WARFileName* es la primera parte del nombre de archivo del archivo .war del sitio; por ejemplo, “XenApp.”

5. Modifique el archivo launcher.xml ubicado en *SunGlassFishEnterpriseServerRoot*/ApplicationServer/lib para agregar javax.wsdl a la lista de valores del elemento sysproperty key="com.sun.enterprise.overrideablejavaxpackages".

6. Inicie el servidor Web.

Uso de los paquetes de idiomas

Los paquetes de idiomas contienen todo lo necesario para presentar los sitios en un idioma específico (chino [tradicional y simplificado], inglés, francés, alemán, japonés, coreano, ruso y español), incluidos los siguientes elementos:

- Archivos de recursos para sitios
- Ayuda del usuario
- Iconos e imágenes traducidos

En ISS, se pueden agregar paquetes de idioma a la instalación de la Interfaz Web copiando el árbol o extrayendo los archivos en la carpeta \languages, que normalmente se encuentra en: C:\Archivos de programa (x86)\Citrix\Web Interface*Versión*\languages. Para personalizar un idioma para un sitio específico, puede copiar el paquete de idioma en la ubicación del sitio y modificarlo. El sitio utilizará entonces el paquete de idioma modificado, mientras que los otros sitios continuarán utilizando el predeterminado.

Nota: Para que los mensajes de error de Windows aparezcan en el idioma correcto en IIS, es necesario instalar el paquete de idioma correspondiente de Microsoft .NET Framework.

En los servidores de aplicaciones de Java, se pueden instalar paquetes de idioma adicionales moviéndolos al directorio adecuado dentro del sitio en cuestión y extrayendo los archivos.

El paquete inglés se usa como idioma automático predeterminado y siempre debe estar presente en el servidor. Los paquetes de idioma son específicos para la versión de la Interfaz Web con la que se suministran y no pueden usarse con versiones anteriores o posteriores de la misma. Para obtener más información sobre cómo usar los paquetes de idioma, consulte el kit de desarrollo (SDK) de la Interfaz Web.

Eliminación de paquetes de idiomas

Algunos dispositivos, como aquellos que ejecutan Windows CE, no tienen la capacidad de mostrar determinados idiomas (por ejemplo, japonés). En este caso, la lista para la selección del idioma en la interfaz del usuario muestra caracteres de bloque para los idiomas no disponibles. Para evitar esto, puede eliminar un idioma de todos los sitios o sólo de sitios específicos.

En sitios de IIS, elimine el archivo *LanguageCode*.lang (por ejemplo, ja.lang) de la carpeta \languages, que normalmente es: C:\Archivos de programa (x86)\Citrix\Web Interface*Version*\languages. Esta acción elimina el idioma de todos los sitios en el servidor. Si desea activar este idioma para un sitio concreto, coloque el archivo .lang en la carpeta \languages de ese sitio.

En los sitios de servidores de aplicaciones de Java, tras crear un archivo .war, abra éste con una herramienta adecuada, elimine el archivo .lang y vuelva a empaquetarlo. Esta acción elimina el idioma de los sitios distribuidos desde ese archivo .war.

Actualización de una instalación existente

Si desea actualizar la Interfaz Web desde la versión 4.5 o versiones posteriores a la versión más reciente, puede hacerlo instalando la Interfaz Web, desde el soporte de instalación de XenApp o XenDesktop, o usando los archivos descargados del sitio Web.

No es posible volver a una versión anterior de la Interfaz Web.

Importante: Los sitios de configuración centralizada y los sitios de participante invitado de Conferencing Manager ya no reciben respaldo. Si actualiza desde una versión anterior de la Interfaz Web, el programa de instalación eliminará los sitios de participante invitado de Conferencing Manager que existan en el servidor Web. Si hay sitios de configuración centralizada, éstos serán actualizados y convertidos para utilizar la configuración local.

La estructura del directorio de la carpeta \Clients, que se utiliza para la distribución de clientes a usuarios basada en la Web, es diferente en la versión 5.1 y versiones anteriores de la Interfaz Web. Si actualiza la instalación de la Interfaz Web a través del soporte de instalación de XenApp o XenDesktop, copie la estructura del directorio del soporte de instalación cuando actualice la instalación. Si realiza la actualización a través de una descarga Web, debe recrear en forma manual la estructura del directorio requerida para la instalación de la Interfaz Web. Luego, puede descargar los clientes que necesita del sitio Web de Citrix. Para obtener más información sobre la estructura del directorio \Clients, consulte Copia de los archivos de instalación de clientes en la Interfaz Web.

De forma predeterminada, la Interfaz Web asume que los nombres de archivo de los archivos de instalación de clientes son los mismos que los archivos suministrados en el soporte de instalación de XenApp o XenDesktop. Si descarga clientes del sitio Web de Citrix o si planea distribuir clientes anteriores, verifique que los nombres de los archivos de instalación de clientes estén especificados para los parámetros ClientIcaLinuxX86, ClientIcaMac, ClientIcaSolarisSparc, ClientIcaSolarisX86, ClientIcaWin32 y ClientStreamingWin32 en los archivos de configuración de los sitios Web XenApp. Para obtener más información sobre los parámetros del archivo de configuración de la Interfaz Web, consulte Parámetros de WebInterface.conf.

Qué hacer después de la instalación

Después de instalar la Interfaz Web, debe ponerla a disposición de los usuarios. Para ello, cree y configure sitios mediante la consola Administración de la Interfaz Web de Citrix o modifique directamente el archivo de configuración WebInterface.conf.

Además, es posible que necesite configurar la Interfaz Web para interactuar correctamente con los demás componentes de la instalación; o puede que desee personalizar o ampliar las capacidades de la Interfaz Web.

- Para obtener información sobre cómo configurar la Interfaz Web usando la consola o el archivo WebInterface.conf, consulte Configuración de sitios mediante la consola de administración de la Interfaz Web de Citrix o Configuración de sitios mediante archivos de configuración, respectivamente.
- Para obtener información sobre cómo configurar la Interfaz Web para Access Gateway o Secure Gateway mediante la consola Administración de la Interfaz Web de Citrix, consulte Para configurar los parámetros de puerta de enlace
- Para obtener información sobre cómo configurar la Interfaz Web para utilizar AD FS, consulte Configuración del soporte de AD FS para la Interfaz Web
- Para obtener información sobre consideraciones de seguridad, consulte Configuración de la seguridad en la Interfaz Web
- Para obtener información sobre cómo extender y personalizar la funcionalidad de la Interfaz Web, consulte el kit de desarrollo (SDK) de la Interfaz Web

Solución de problemas de instalación de la Interfaz Web

En las plataformas Windows con IIS, puede usar la opción Reparar para solucionar problemas de instalación de la Interfaz Web. Si la opción Reparar no soluciona el problema, o si esta opción no está disponible (por ejemplo, en instalaciones de servidor de aplicaciones de Java), intente desinstalando y volviendo a instalar la Interfaz Web. Para obtener más información, consulte Desinstalación de la Interfaz Web. Si reinstala la Interfaz Web tendrá que volver a crear todos los sitios.

Para usar la opción Reparar

Si tiene problemas con la instalación de la Interfaz Web, intente usar la opción Reparar para solucionar el problema. La opción Reparar vuelve a instalar los archivos comunes; no repara ni sustituye los sitios existentes.

Importante: Si la instalación de su Interfaz Web incluye un código personalizado y selecciona la opción Reparar, se elimina ese código personalizado. Citrix recomienda realizar copias de seguridad de los archivos personalizados antes de usar esa opción.

1. Haga doble clic en el archivo WebInterface.exe.
2. Seleccione Reparar y haga clic en Siguiente.
3. Siga las instrucciones que aparecen en pantalla.

Desinstalación de la Interfaz Web

Al desinstalar la Interfaz Web, se eliminan todos los archivos de la misma, incluida la carpeta \Clients. Por consiguiente, si desea conservar algún archivo de la Interfaz Web, haga una copia de esos archivos en otra ubicación antes de desinstalar la Interfaz Web.

Puede ocurrir que el programa de desinstalación de la Interfaz Web falle. Las razones posibles son:

- El programa de desinstalación no tiene acceso total al Registro del sistema
- IIS fue eliminado del sistema después de instalar la Interfaz Web

Para desinstalar la Interfaz Web en Microsoft Internet Information Services

1. En el menú Inicio de Windows, haga clic en Panel de control > Programas y funciones.
2. Seleccione Interfaz Web de Citrix y haga clic en Desinstalar.
3. Siga las instrucciones que aparecen en pantalla.

Para desinstalar la Interfaz Web en servidores de aplicaciones de Java

Si el servidor Web tiene una herramienta para ayudarlo a desinstalar aplicaciones Web, siga el procedimiento recomendado por el fabricante para desinstalar la Interfaz Web. También puede desinstalarla manualmente, si lo prefiere.

1. Desde una línea de comandos, busque el directorio donde copió originalmente el archivo .war.
2. Detenga el servidor Web y elimine el archivo .war.

   También es posible que necesite eliminar el directorio donde se descomprimió el archivo .war. Normalmente dicho directorio suele estar en el mismo directorio que el archivo .war y tiene el mismo nombre. Por ejemplo, el contenido de “mysite.war” se descomprime en un directorio llamado /mysite.

   Nota: Al desinstalar la Interfaz Web, algunos archivos pueden quedar en el servidor. Para obtener más información sobre los archivos que permanecen en el sistema tras la desinstalación, consulte el archivo Léame de Citrix XenApp.

Introducción a la Interfaz Web

Cómo elegir el mejor método de configuración

Para configurar y personalizar la Interfaz Web, se puede utilizar la consola Administración de la Interfaz Web de Citrix o los archivos de configuración.

Uso de la consola Administración de la Interfaz Web de Citrix

La consola Administración de la Interfaz Web de Citrix es un complemento de Microsoft Management Console (MMC) 3.0 que permite crear y configurar sitios Web XenApp y sitios de servicios XenApp alojados en Microsoft Internet Information Services (IIS). En el panel izquierdo aparecen los tipos de sitio de la Interfaz Web. El panel central de resultados muestra los sitios disponibles dentro del contenedor de tipos de sitio seleccionado en el panel izquierdo.

La consola Administración de la Interfaz Web de Citrix permite llevar a cabo las tareas diarias de administración de una forma sencilla y rápida. El panel Acción enumera las tareas disponibles en ese momento. Las tareas relacionadas con los elementos seleccionados en el panel izquierdo se muestran en la parte superior y las acciones disponibles para dichos elementos se muestran más abajo.

Cuando se utiliza la consola, la configuración creada se aplica al confirmar los cambios mediante la consola. Como resultado, es posible que se deshabiliten algunos parámetros de la interfaz Web si sus valores no son relevantes para la configuración actual y los parámetros correspondientes se restablecen a los valores predeterminados del archivo WebInterface.conf. Citrix recomienda crear regularmente copias de respaldo de los archivos WebInterface.conf y config.xml para los sitios.

La consola Administración de la Interfaz Web de Citrix se instala en forma automática al instalar la Interfaz Web para Microsoft Internet Information Services. Para ejecutar la consola, haga clic en Inicio > Todos los programas > Citrix > Management Consoles > Citrix Web Interface Management.

Nota: debe asegurarse de que MMC 3.0 esté presente en el servidor en el que se instala la Interfaz Web, dado que es un requisito previo para la instalación de la consola Administración de la Interfaz Web de Citrix. MMC 3.0 está disponible de forma predeterminada en todas las plataformas Windows que respaldan el alojamiento de la Interfaz Web.

Uso de los archivos de configuración

Para configurar los sitios de la Interfaz Web se puede modificar los siguientes archivos de configuración:

- **Archivo de configuración de la Interfaz Web:** El archivo de configuración de la Interfaz Web, WebInterface.conf, permite cambiar muchas propiedades de la Interfaz Web; está disponible tanto en Microsoft Internet Information Services (IIS) como en servidores de aplicaciones de Java. Puede usar este archivo para realizar tareas diarias de administración y también para personalizar muchos otros parámetros de configuración. Sólo tiene que modificar los valores en WebInterface.conf y guardar el archivo actualizado para aplicar los cambios. Para obtener información sobre cómo configurar la Interfaz Web mediante WebInterface.conf, consulte Configuración de sitios mediante el archivo de configuración.

- **Archivo de configuración de Citrix Online Plug-in.** Se puede configurar Citrix Online Plug-in mediante el archivo config.xml situado en el servidor de la Interfaz Web.

Configuración de sitios mediante la consola de administración de la Interfaz Web de Citrix

La consola Administración de la Interfaz Web de Citrix es un complemento de Microsoft Management Console (MMC) 3.0 que permite crear y configurar sitios Web XenApp y sitios de servicios XenApp alojados en Microsoft Internet Information Services (IIS). En el panel izquierdo aparecen los tipos de sitio de la Interfaz Web. El panel central de resultados muestra los sitios disponibles dentro del contenedor de tipos de sitio seleccionado en el panel izquierdo.

La consola Administración de la Interfaz Web de Citrix permite llevar a cabo las tareas diarias de administración de una forma sencilla y rápida. El panel Acción enumera las tareas disponibles en ese momento. Las tareas relacionadas con los elementos seleccionados en el panel izquierdo se muestran en la parte superior y las acciones disponibles para dichos elementos se muestran más abajo.

Cuando se utiliza la consola, la configuración creada se aplica al confirmar los cambios mediante la consola. Como resultado, es posible que se deshabiliten algunos parámetros de la interfaz Web si sus valores no son relevantes para la configuración actual y los parámetros correspondientes se restablecen a los valores predeterminados del archivo WebInterface.conf. Citrix recomienda crear regularmente copias de respaldo de los archivos WebInterface.conf y config.xml para los sitios.

La consola Administración de la Interfaz Web de Citrix se instala en forma automática al instalar la Interfaz Web para Microsoft Internet Information Services. Para ejecutar la consola, haga clic en Inicio > Todos los programas > Citrix > Management Consoles > Citrix Web Interface Management.

Nota: debe asegurarse de que MMC 3.0 esté presente en el servidor en el que se instala la Interfaz Web, dado que es un requisito previo para la instalación de la consola Administración de la Interfaz Web de Citrix. MMC 3.0 está disponible de forma predeterminada en todas las plataformas Windows que respaldan el alojamiento de la Interfaz Web.

Configuración de sitios mediante archivos de configuración

Para configurar los sitios de la Interfaz Web se puede modificar los siguientes archivos de configuración:

- **Archivo de configuración de la Interfaz Web:** El archivo de configuración de la Interfaz Web, WebInterface.conf, permite cambiar muchas propiedades de la Interfaz Web; está disponible tanto en Microsoft Internet Information Services (IIS) como en servidores de aplicaciones de Java. Puede usar este archivo para realizar tareas diarias de administración y también para personalizar muchos otros parámetros de configuración. Sólo tiene que modificar los valores en WebInterface.conf y guardar el archivo actualizado para aplicar los cambios. Para obtener información sobre cómo configurar la Interfaz Web mediante WebInterface.conf, consulte Configuración de sitios mediante el archivo de configuración.

- **Archivo de configuración de Citrix Online Plug-in.** Se puede configurar Citrix Online Plug-in mediante el archivo config.xml situado en el servidor de la Interfaz Web.

Configuración compartida

Para los sitios alojados en IIS, se puede especificar que un sitio de la Interfaz Web obtenga su configuración a partir de un sitio "maestro" que se haya configurado para compartir sus archivos de configuración por medio de la red. Una vez configurados los permisos de archivo apropiados, puede hacer que otros sitios compartan la configuración del sitio maestro especificando la ruta absoluta a su archivo de configuración (WebInterface.conf) en el archivo bootstrap.conf del sitio local. En el caso de los sitios de XenApp Services que usan configuración compartida, la Interfaz Web también intenta leer el archivo de configuración de Citrix Online Plug-in (config.xml) desde el mismo directorio que el especificado para WebInterface.conf.

Una vez que el sitio ha sido modificado para obtener su configuración desde un archivo compartido ya no es posible administrar su configuración directamente. En su lugar, es necesario cambiar la configuración del sitio maestro usando la consola, o modificar directamente los archivos de configuración en el servidor Web que aloja el sitio maestro. Los cambios que se hagan en la configuración del sitio maestro afectarán a todos los demás sitios que compartan su archivo de configuración. La configuración compartida no está disponible para sitios alojados en servidores de aplicaciones de Java.

Para compartir configuraciones de sitios

1. Configure adecuadamente los permisos para compartir archivos de forma que se pueda acceder a través de la red a la carpeta \conf (normalmente, en C:\inetpub\wwwroot\Citrix*SiteName*\conf) del sitio maestro y al archivo de configuración del sitio (WebInterface.conf), que normalmente se encuentra en la carpeta \conf. Para los sitios maestros de XenApp Services, se deben configurar los mismos permisos para el archivo de configuración de Citrix Online Plug-in (config.xml), que también se encuentra normalmente en la carpeta \conf del sitio.

2. Use un editor de texto para abrir el archivo bootstrap.conf (normalmente está dentro de la carpeta \conf) del sitio que obtendrá su configuración del archivo de configuración compartido.

3. Cambie el valor del parámetro ConfigurationLocation para especificar la ruta de red absoluta del archivo de configuración del sitio maestro. Por ejemplo:

   ConfigurationLocation=*Servidor**PuntoCompartido*\WebInterface.conf

Para crear un sitio en Microsoft Internet Information Services

Utilice la tarea Crear sitio de la consola Administración de la Interfaz Web de Citrix para crear uno de los siguientes sitios:

- **Sitios Web XenApp.** Para los usuarios que acceden a los recursos mediante un explorador Web.
- **Sitios de XenApp Services.** Para los usuarios que acceden a los recursos mediante Citrix Online Plug-in.

Esta tarea se utiliza para especificar la ubicación del sitio en IIS, la dirección URL para aplicar cambios y los parámetros de autenticación del sitio. Puede actualizar estos parámetros más adelante mediante las tareas Mantenimiento de sitios. Para crear sitios, se debe ser administrador local del servidor en que se ejecuta la Interfaz Web.

1. En el menú Inicio de Windows, haga clic en Todos los programas > Citrix > Management Consoles > Citrix Web Interface Management.
2. En el panel izquierdo de la consola Administración de la Interfaz Web de Citrix, haga clic en el contenedor Interfaz Web de Citrix.
3. En el panel Acción, haga clic en Crear sitio.
4. Seleccione el tipo de sitio que desea crear.
5. Especifique la dirección URL y el nombre del sitio.
6. Siga las instrucciones en pantalla para crear el sitio.

Alojamiento de Microsoft Internet Information Services

Utilice la tarea Administrar el alojamiento IIS en Mantenimiento de sitios de la consola Administración de la Interfaz Web de Citrix para cambiar la ubicación de su sitio de Interfaz Web en IIS.

Creación de sitios en servidores de aplicaciones de Java

En los servidores de aplicaciones de Java, ejecute el programa de instalación de la Interfaz Web para crear nuevos sitios. El programa de instalación crea un archivo .war personalizado para el sitio, que luego puede instalar (típicamente colocando el archivo .war en la ubicación correspondiente para el motor de su servlet). Puede modificar los sitios editando el contenido del archivo .war desempaquetado y eliminar sitios borrando el archivo .war.

Especificación del punto de autenticación

Cuando se crea un sitio Web XenApp con la consola Administración de la Interfaz Web de Citrix, se debe especificar el *punto de autenticación*, que es el punto de su entorno donde se lleva a cabo la autenticación de los usuarios.

Autenticación en la Interfaz Web

La autenticación de usuarios mediante la Interfaz Web puede habilitarse usando diversos métodos de autenticación: explícita, mediante paso de credenciales (PassThrough) y mediante el uso de tarjeta inteligente. Para obtener más información sobre los métodos de autenticación de la Interfaz Web, consulte Configuración de la autenticación para la Interfaz Web.

Autenticación en un asociado de cuenta de los servicios de federación de Active Directory

Es posible habilitar el asociado de cuenta de una distribución de servicios de federación de Active Directory (AD FS) para que tenga acceso a las aplicaciones de XenApp. Esto permite el acceso de los usuarios del asociado de cuenta a las aplicaciones.

Si piensa crear sitios integrados con AD FS, tenga en cuenta lo siguiente:

- XenDesktop no respalda la autenticación mediante AD FS.
- El uso de AD FS no está disponible con la Interfaz Web para servidores de aplicaciones de Java.
- El Cliente para Java y el software incrustado de Conexión a escritorio remoto (RDP) no están respaldados para acceder a sitios integrados con AD FS.
- Los sitios integrados con AD FS sólo permiten la autenticación con AD FS. No se respalda ningún otro método de autenticación.
- Tras crear un sitio integrado con AD FS, no puede configurarlo para usar un método integrado de autenticación o la autenticación mediante Access Gateway en lugar de AD FS.

Para obtener más información, consulte Configuración del soporte de AD FS para la Interfaz Web.

Autenticación en Access Gateway

Es posible habilitar la autenticación y el paso de credenciales de usuarios, a través de Access Gateway, para la autenticación explícita y con tarjeta inteligente. El acceso de los usuarios a los recursos se controla mediante el uso de directivas.

Si los usuarios inician sesión en Access Gateway utilizando credenciales explícitas, se habilita la autenticación mediante el paso de credenciales (pass-through) de forma predeterminada. Los usuarios inician sesión en Access Gateway y no tienen que volver a autenticarse en la Interfaz Web para acceder a sus recursos. Para aumentar la seguridad, es posible deshabilitar la autenticación mediante paso de credenciales para que se les pida a los usuarios una contraseña antes de mostrar el conjunto de recursos.

Si los usuarios inician sesión en Access Gateway con una tarjeta inteligente, no tienen que volver a autenticarse en la Interfaz Web. Sin embargo, de forma predeterminada, a los usuarios se les solicita un PIN cuando intentan acceder a un recurso. Es posible configurar el sitio para que los usuarios tengan acceso a los recursos de XenApp, sin tener que proporcionar un PIN. XenDesktop no admite esta función.

Puede actualizar estos parámetros en cualquier momento con la tarea Método de autenticación de la consola Administración de la Interfaz Web de Citrix.

Autenticación en otro producto mediante Kerberos

Puede autenticar a los usuarios mediante otros productos de terceros para federación o inicio de sesión único y asignar las identidades de los usuarios a cuentas de usuario de Active Directory. Después puede usar Kerberos para el inicio de sesión único en la Interfaz Web. Para obtener más información sobre Kerberos, consulte Administración de XenApp.

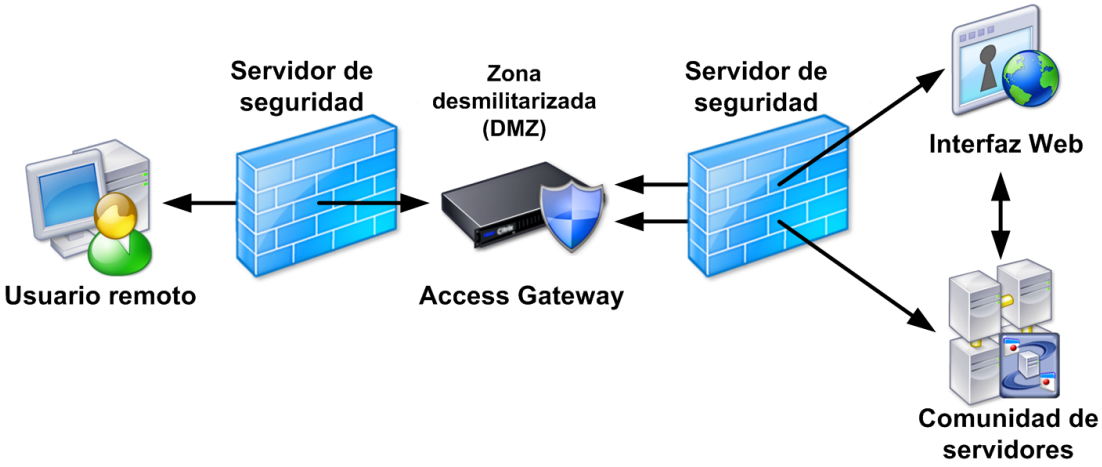
Autenticación en el servidor Web

Puede habilitar la autenticación de usuarios en el servidor Web mediante Kerberos. Para obtener más información sobre Kerberos, consulte Administración de XenApp.

Distribución de Access Gateway con la Interfaz Web

Cuando se instala Access Gateway, junto con la Interfaz Web, Citrix recomienda que XenApp/XenDesktop y la Interfaz Web se instalen en servidores de la red interna y que el dispositivo Access Gateway se instale en la zona desmilitarizada (DMZ).

Este gráfico muestra la configuración recomendada para la distribución de Access Gateway con la Interfaz Web.



Una DMZ es una subred ubicada entre la red interna segura e Internet (o cualquier red externa). Cuando Access Gateway se distribuye en la DMZ, los usuarios acceden a ella mediante Citrix Secure Access Plug-in o un cliente Citrix. Los usuarios inician sesión, Access Gateway los autentica y los dirige a los recursos en función de las directivas de acceso que se hayan configurado.

Recursos a disposición de los usuarios

Con Access Gateway, los usuarios inician sesión en un dominio (para Access Gateway Standard Edition), un punto de entrada (para Access Gateway Advanced Edition y Acess Gateway 5.0) o un servidor virtual (para Access Gateway Enterprise Edition) para tener acceso a sus recursos. Para poner los recursos publicados a disposición de los usuarios, se debe configurar un dominio, un punto de entrada o un servidor virtual de manera que proporcione acceso a un sitio Web XenApp.

Access Gateway ofrece varios métodos para integrar sitios Web XenApp creados con la Interfaz Web, entre los que se incluyen:

- Un sitio Web XenApp configurado como página de inicio predeterminada de un dominio, un punto de entrada o un servidor virtual. Una vez iniciada la sesión, los usuarios ven el sitio Web XenApp.

- Un sitio Web XenApp incrustado dentro de la Interfaz de acceso. Cuando se selecciona la Interfaz de acceso como página de inicio predeterminada, el sitio Web XenApp aparece junto a archivos compartidos, centros de acceso y aplicaciones Web. Access Interface solo está disponible con Access Gateway Advanced Edition y Enterprise Edition.

Integración de un sitio Web XenApp con Access Gateway

Para integrar un sitio con Access Gateway, se debe crear un sitio Web XenApp y configurar un recurso Web para el sitio en Access Gateway.

Para crear un sitio integrado con Access Gateway

1. En el menú Inicio de Windows, haga clic en Todos los programas > Citrix > Management Consoles > Citrix Web Interface Management.

2. En el panel izquierdo de la consola Administración de la Interfaz Web de Citrix, haga clic en el contenedor Interfaz Web de Citrix.

3. En el panel Acción, haga clic en Crear sitio.

4. Seleccione Web XenApp y, a continuación, haga clic en Siguiente.

5. En la página Especificar ubicación IIS, especifique la ubicación IIS, la ruta y un nombre para el sitio. Haga clic en Next.

6. En la página Especificar punto de autenticación, seleccione En Access Gateway y haga clic en Siguiente.

7. En la página Especificar parámetros de Access Gateway, escriba la dirección URL del servicio de autenticación de Access Gateway en la casilla URL del servicio de autenticación .

8. Especifique de qué manera sus usuarios inician sesión en Access Gateway y haga clic en Siguiente:

   - Si los usuarios inician sesión en Access Gateway con un nombre de usuario y una contraseña, seleccione Explícita. Para aumentar la seguridad mediante la deshabilitación del paso de las credenciales de los usuarios de Access Gateway a la Interfaz Web, marque la casilla de verificación Pedir contraseñas a los usuarios antes de mostrar aplicaciones y escritorios.

   - Si los usuarios inician sesión en Access Gateway con una tarjeta inteligente, seleccione Tarjeta inteligente. Antes de activar la opción de autenticación mediante paso de credenciales con tarjeta inteligente, asegúrese de iniciar sesión como administrador de dominio.

   Importante: los sitios Web XenApp integrados en Access Gateway pueden admitir la autenticación explícita o la autenticación con tarjeta inteligente, pero no ambas. Si algunos usuarios inician sesión en Access Gateway con autenticación explícita y otros lo hacen con tarjeta inteligente, debe crear y configurar sitios separados para cada método de autenticación. Luego, configure Access Gateway para que dirija a los usuarios al sitio correspondiente según el método de autenticación.

9. Si configura el sitio para la autenticación explícita, continúe con el paso 10. Si configura la autenticación con tarjeta inteligente, en la página Especificar parámetros de tarjeta inteligente, especifique si los usuarios deben proporcionar su PIN antes de acceder a un recurso.

   - Si desea que los usuarios introduzcan un PIN cada vez que acceden a un recurso, seleccione Pedir PIN a los usuarios. Para habilitar esta función se necesitan pasos adicionales en la configuración. Para obtener más información, consulte Para habilitar a usuarios de tarjeta inteligente para que puedan acceder a sus recursos a través de Access Gateway proporcionando un PIN.

Nota: Es posible habilitar a los usuarios de Windows XP, que inician sesión en sus escritorios con la misma tarjeta inteligente que utilizan para iniciar sesión en Access Gateway, para que puedan acceder a los recursos sin tener que proporcionar un PIN. Para obtener más información, consulte Para habilitar a usuarios de tarjeta inteligente para que puedan acceder a sus recursos a través de Access Gateway proporcionando un PIN.

- Si desea habilitar a todos los usuarios para que accedan a los recursos de XenApp sin tener que proporcionar un PIN, seleccione Habilitar autenticación mediante paso de credenciales (pass-through) con tarjeta inteligente. XenDesktop no admite esta función y solo se puede utilizar cuando el servidor Web está en el mismo dominio de los usuarios. Es posible que deba reiniciarse el servidor Web para habilitar la autenticación mediante paso de credenciales (pass-through) con tarjeta inteligente desde el servicio de Access Gateway. Para habilitar esta función se necesitan pasos adicionales en la configuración. Para obtener más información, consulte Para habilitar a usuarios de tarjeta inteligente para que puedan acceder a los recursos, a través de Access Gateway, sin proporcionar un PIN.

  Nota: De forma predeterminada, la autenticación mediante paso de credenciales (pass-through) con tarjeta inteligente desde Access Gateway está habilitada para todos los usuarios del dominio. Para restringir la lista de usuarios permitidos, edite los permisos de usuario para el archivo PTSAccess.txt, que normalmente se encuentra en el directorio C:\Archivos de programa (x86)\Citrix\DeliveryServices\ProtocolTransitionService\.

10. Confirme los parámetros del nuevo sitio y, a continuación, haga clic en Siguiente para crear el sitio.

Para proporcionar acceso al sitio a través de Access Gateway

1. Configure XenApp o XenDesktop para comunicarse con Access Gateway. Para obtener más información, consulte el tema correspondiente a la edición de Access Gateway:
   - Para Access Gateway Standard Edition, consulte Integración de Access Gateway Standard Edition con Citrix XenApp y Citrix XenDesktop
   - Para Access Gateway Advanced Edition, consulte Integración con Citrix XenApp
   - Para Access Gateway Enterprise Edition, consulte Integración de Access Gateway Enterprise Edition con Citrix XenApp y Citrix XenDesktop
2. Configure Access Gateway para proporcionar acceso al sitio Web XenApp. Para obtener más información, consulte el tema correspondiente a la edición de Access Gateway:
   - Para Access Gateway Standard Edition, consulte Configuración de Access Gateway Standard Edition para establecer comunicación con la Interfaz Web
   - Para Access Gateway Advanced Edition, consulte Integración con la Interfaz Web
   - Para Access Gateway Standard Edition, consulte Configuración de Access Gateway Enterprise Edition para establecer comunicación con la Interfaz Web

   Importante: Especifique el dominio con el formato *dominio* en lugar de *dominio.com*. La autenticación mediante paso de credenciales (pass-through) con tarjeta inteligente de la Interfaz Web desde el servicio de Access Gateway, no reconoce dominios con el formato *dominio.com*; por esta razón, los usuarios no pueden iniciar sesión, si el dominio se especifica de esta manera.
3. Asegúrese de que los parámetros de control del área de trabajo (únicamente para Access Gateway Advanced Edition) y de tiempo de espera de sesión estén configurados correctamente tanto en Access Gateway como en la Interfaz Web. Para obtener más información, consulte el tema correspondiente a la edición de Access Gateway:
   - Para Access Gateway Standard Edition, consulte Brindar acceso a las aplicaciones publicadas
   - Para Access Gateway Advanced Edition, consulte Coordinación de parámetros entre Advanced Access Control y la Interfaz Web
   - Para Access Gateway Enterprise Edition, consulte Configuración de directivas para aplicaciones publicadas y escritorios

Para habilitar a usuarios de tarjeta inteligente para que puedan acceder a los recursos, a través de Access Gateway, sin proporcionar un PIN

Si desea habilitar a todos los usuarios para que puedan acceder a los recursos de XenApp, sin tener que proporcionar un PIN, debe habilitar Secure Sockets Layer (SSL) para el sitio IIS que aloja el sitio Web XenApp. Para obtener más información, consulte la documentación de Microsoft para IIS 7.*x* e IIS 6.0.

Una vez habilitado SSL, asegúrese de que el servidor Web esté en el mismo dominio de los usuarios y configure Active Directory para permitir la delegación limitada.

Para asegurar que el dominio esté en el nivel funcional correcto

Importante: Para elevar el nivel de dominio, todos los controladores de dominio deben ejecutar Windows Server 2008 o Windows Server 2003. No eleve el nivel funcional de dominio a Windows Server 2008 si posee o tiene intenciones de agregar controladores de dominio que ejecutan Windows Server 2003. Una vez que se eleva el nivel funcional de dominio no es posible retroceder a un nivel inferior.

1. Inicie sesión en el controlador de dominio como administrador de dominio y abra el complemento Dominios y confianza de Active Directory en la consola MMC.
2. En el panel izquierdo, seleccione el nombre de dominio y haga clic en Propiedades en el panel Acción.
3. Si el dominio no se encuentra en el nivel funcional máximo, seleccione el nombre del dominio y, en el panel Acción, haga clic en Elevar el nivel funcional del dominio.
4. Para elevar el nivel funcional del dominio, haga clic en el nivel adecuado y luego en Elevar.

Para establecer una relación de confianza con los servidores que ejecutan la Interfaz Web y Citrix XML Service para la delegación

1. Inicie sesión en el controlador de dominio como administrador de dominio y abra el complemento Usuarios y equipos de Active Directory en la consola MMC.
2. En el menú Ver, haga clic en Funciones avanzadas.
3. En el panel izquierdo, haga clic en el nodo Equipos y seleccione el servidor Web.
4. En el panel Acción, haga clic en Propiedades.
5. En la ficha Delegación, haga clic en Confiar en este equipo para la delegación sólo a los servicios especificados y Usar cualquier protocolo de autenticación y, a continuación, haga clic en Agregar.
6. En el cuadro de diálogo Agregar servicios, haga clic en Usuarios o equipos.
7. En el cuadro de diálogo Seleccionar usuarios o equipos, escriba el nombre del servidor que ejecuta el servicio XML de Citrix en el cuadro Escriba los nombres de objeto que desea seleccionar y, a continuación, haga clic en Aceptar.
8. Seleccione el tipo de servicio http en la lista y, a continuación, haga clic en Aceptar.
9. En la ficha Delegación, verifique que el tipo de servicio http del servidor que ejecuta Citrix XML Service aparezca en la lista Servicios a los que esta cuenta puede presentar credenciales delegadas y, a continuación, haga clic en Aceptar.
10. Repita los pasos 3 a 9 para cada uno de los servidores de la comunidad que ejecutan Citrix XML Service y con los que la Interfaz Web está configurada para conectarse.
11. En el panel izquierdo, haga clic en el nodo Equipos y seleccione el servidor que ejecuta Citrix XML Service con el que la Interfaz Web está configurada para conectarse.
12. En el panel Acción, haga clic en Propiedades.
13. En la ficha Delegación, haga clic en Confiar en este equipo para la delegación sólo a los servicios especificados y Usar solamente Kerberos y, a continuación, haga clic en Agregar.
14. En el cuadro de diálogo Agregar servicios, haga clic en Usuarios o equipos.
15. En el cuadro de diálogo Seleccionar usuarios o equipos, escriba el nombre del servidor que ejecuta el servicio XML de Citrix en el cuadro Escriba los nombres de objeto que desea seleccionar y, a continuación, haga clic en Aceptar.
16. Seleccione el tipo de servicio HOST en la lista y, a continuación, haga clic en Aceptar.
17. En la ficha Delegación, verifique que el tipo de servicio HOST del servidor que ejecuta el servicio XML de Citrix aparezca en la lista Servicios a los que esta cuenta puede presentar credenciales delegadas y, a continuación, haga clic en Aceptar.

18. Repita los pasos 11 a 17 para cada uno de los servidores de la comunidad que ejecutan Citrix XML Service y con los que la Interfaz Web está configurada para conectarse.

19. Por razones de seguridad, debe configurar todos los servidores de la comunidad para la delegación limitada. Para dar acceso a los usuarios a los recursos en esos servidores, debe agregar los servicios pertinentes, como el servicio http para un servidor Web, a la Lista de servicios a los que esta cuenta puede presentar credenciales delegadas.

    Para obtener información más detallada, consulte el documento técnico *Service Principal Names and Delegation in Presentation Server* (CTX110784) en la base de conocimientos en línea Citrix Knowledge Center.

Para determinar los recursos a los que se puede acceder desde la comunidad de servidores

1. Inicie sesión en el controlador de dominio como administrador de dominio y abra el complemento Usuarios y equipos de Active Directory en la consola MMC.

2. En el panel izquierdo, haga clic en el nodo Equipos y seleccione un servidor de la comunidad.

3. En el panel Acción, haga clic en Propiedades.

4. En la ficha Delegación, haga clic en Confiar en este equipo para la delegación sólo a los servicios especificados y Usar solamente Kerberos y, a continuación, haga clic en Agregar.

5. En el cuadro de diálogo Agregar servicios, haga clic en Usuarios o equipos.

6. En el cuadro de diálogo Seleccionar usuarios o equipos, escriba el nombre del servidor en el cuadro Escriba los nombres de objeto que desea seleccionar y, a continuación, haga clic en Aceptar.

7. Seleccione los tipos de servicio cifs e ldap de la lista y, a continuación, haga clic en Aceptar.

    Nota: Si aparecen dos opciones para el servicio ldap, seleccione la que coincida con el nombre de dominio completo (FQDN) del controlador de dominio.

8. En la ficha Delegación, verifique que los tipos de servicio cifs e ldap del controlador de dominio aparezcan en la lista Servicios a los que esta cuenta puede presentar credenciales delegadas y, a continuación, haga clic en Aceptar.

9. Repita el procedimiento para cada servidor de la comunidad.

Para configurar el límite de tiempo para el acceso a los recursos en el nivel de dominio

Precaución: Si se usa el editor del Registro de forma incorrecta, pueden producirse problemas graves que derivarán en la necesidad de instalar nuevamente el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad.

De forma predeterminada, los usuarios tienen acceso a los recursos de una red durante 15 minutos. Es posible aumentar este límite modificando la siguiente entrada en el Registro del sistema del servidor que ejecuta el servicio XML de Citrix:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\
Kerberos\Parameters\S4UTicketLifetime

Este valor especifica el tiempo, en minutos, durante el cual los usuarios pueden acceder a los recursos una vez iniciada la sesión.

La directiva de seguridad del dominio controla el valor máximo que puede definirse en el parámetro S4ULifetime. Si especifica un valor para el parámetro S4UTicketLifetime mayor que el valor especificado en el nivel de dominio, el parámetro del nivel de dominio tiene preferencia.

1. Inicie sesión en el controlador de dominio como administrador de dominio y abra el complemento Directiva de seguridad de dominio en la consola MMC.
2. En el panel izquierdo, seleccione Directivas de cuenta > Directiva Kerberos.
3. En el panel de resultados, seleccione Vigencia máxima del tique de servicio.
4. En el panel Acción, haga clic en Propiedades.
5. Introduzca el límite necesario (en minutos) en el cuadro El tique caduca en.

Si no desea configurar un límite de tiempo para acceder a los recursos, marque la casilla Usar cualquier protocolo de autenticación cuando determine los recursos a los que se puede acceder desde la comunidad de servidores. Si selecciona esta opción, no se tendrá en cuenta ningún valor especificado para S4UTicketLifetime. Para obtener más información, visite el sitio Web de Microsoft en http://support.microsoft.com/.

Para habilitar a usuarios de tarjeta inteligente para que puedan acceder a sus recursos a través de Access Gateway proporcionando un PIN

Actualizado: 2014-07-04

Si desea que los usuarios de tarjeta inteligente ingresen un PIN cada vez que acceden a un recurso a través de Access Gateway, debe habilitar la enumeración de los identificadores de seguridad (SID) de usuarios en Citrix XML Service.

Precaución: Si se usa el editor del Registro de forma incorrecta, pueden producirse problemas graves que derivarán en la necesidad de instalar nuevamente el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad.

1. Si existen cuentas de usuario en otro dominio distinto al que contiene la comunidad de servidores, asegúrese de que los dominios compartan una relación de confianza bidireccional.

2. Verifique que Citrix XML Service pueda resolver la dirección IP y comuníquese con el controlador de dominio del dominio de cuenta de usuario. Si no se logra la comunicación con los controladores de dominio, es posible que se agote el tiempo para las solicitudes al Citrix XML Service.

3. Conceda acceso de lectura al atributo TGGAU en Active Directory para cada dominio a la cuenta de Windows en la cual se ejecuta Citrix XML Service. Para obtener más información sobre el atributo TGGAU, consulte el artículo 331951 de Microsoft Knowledge Base. De forma predeterminada, Citrix XML Service está configurado para ejecutarse como la cuenta Servicio de red. Para conceder los permisos requeridos, agregue esta cuenta a los siguientes grupos incorporados de Active Directory:

   - Acceso de compatibilidad anterior a Windows 2000

   - Acceso de autorización de Windows

4. En el servidor que ejecuta Citrix XML Service, vaya a HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\XMLService\ en el registro del sistema.

5. En el nodo Servicio XML, agregue un valor DWORD denominado EnableSIDEnumeration y establezca el valor en 1.

   Nota: Para XenDesktop 5 y versiones posteriores, la clave de Registro es: [HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\DesktopServer] "EnableXmlServiceSidEnumeration"=REG_DWORD:1

6. Reinicie IIS en el servidor Web. Si desea que los nuevos permisos se apliquen de inmediato en lugar de esperar que caduque el período de caché del tiquet de Kerberos, reinicie el servidor que ejecuta Citrix XML Service.

7. Si lo desea, puede permitir que los usuarios de Windows XP que inician sesión en sus escritorios con la misma tarjeta inteligente que utilizan para iniciar sesión en Access Gateway accedan a recursos sin tener que proporcionar un PIN. Para ello, configure la autenticación mediante paso de credenciales (pass-through) con tarjeta inteligente:

   a. Instale Citrix online plug-in o Citrix Desktop Viewer en los dispositivos de los usuarios mediante una cuenta de administrador.

   b. Agregue la plantilla de cliente al Editor de objetos de directiva de grupo. Para obtener más información, consulte Paso 1: Instalar el plugin para la autenticación con tarjeta inteligente.

   c. Habilite la autenticación mediante paso de credenciales (PassThrough) para todos los clientes Citrix por medio de la directiva de grupo. Para obtener más información, consulte Paso 1: Instalar el plugin para la autenticación con tarjeta inteligente.

Coordinación de parámetros entre la Interfaz Web y Access Gateway

Algunos parámetros de XenApp y XenDesktop se pueden configurar dentro de la Interfaz Web y Access Gateway. Sin embargo, dado que es posible hacer referencia a un sitio Web XenApp integrado con Access Gateway desde más de un dominio (para Access Gateway Standard Edition), punto de entrada (para Access Gateway Advanced Edition) o servidor virtual (para Access Gateway Enterprise Edition), puede ocurrir que un dominio, punto de entrada o servidor virtual incruste un sitio Web XenApp en su interfaz de acceso, mientras que otro dominio, punto de entrada o servidor virtual muestre el sitio como la página de inicio predeterminada. Esto puede ocasionar conflictos con determinados parámetros de recursos.

Para garantizar que la configuración funciona correctamente, siga estas instrucciones:

- **Tiempo de espera de sesión.** Asegúrese de que todos los dominios, puntos de entrada o servidores virtuales utilicen los mismos parámetros del sitio Web XenApp.

- **Control del área de trabajo:** Para Access Gateway Advanced Edition, desactive todos los parámetros de control del área de trabajo para los puntos de entrada que tengan un sitio Web XenApp como página de inicio. Esto garantiza que se utilizarán los parámetros configurados en la Interfaz Web. El control del área de trabajo puede configurarse como se desee en todos los demás puntos de entrada.

Especificación de los parámetros de configuración inicial para un sitio

Después de crear un sitio usando la consola, puede especificar sus parámetros de configuración inicial marcando la casilla Configurar este sitio ahora en la página final del asistente Crear sitio. Utilice el asistente Especificar configuración inicial para configurar la comunicación con una o varias comunidades de servidores y especificar los tipos de recursos disponibles para los usuarios.

Especificación de comunidades de servidores

Al configurar un sitio nuevo, debe introducir detalles de las comunidades de servidores que proporcionarán los recursos para los usuarios del sitio.

Puede actualizar estos parámetros en cualquier momento con la tarea Comunidades de servidores de la consola Administración de la Interfaz Web de Citrix. Para obtener más información sobre la configuración de la comunicación con comunidades de servidores, consulte Administración de servidores y comunidades.

Importante: Para la compatibilidad con XenApp 4.0 con Feature Pack 1 para UNIX es necesario realizar una configuración manual adicional en los sitios. Para obtener más información, consulte Para configurar la compatibilidad con XenApp 4.0, con Feature Pack 1, para UNIX.

Especificación de los métodos de autenticación

Cuando se configura un nuevo sitio Web XenApp creado con el punto de autenticación En la Interfaz Web, se puede especificar cómo se autenticarán los usuarios cuando inicien sesión en la Interfaz Web.

Puede actualizar estos parámetros en cualquier momento con la tarea Métodos de autenticación de la consola Administración de la Interfaz Web de Citrix. Para obtener más información sobre cómo configurar la autenticación, consulte Configuración de la autenticación para la Interfaz Web.

Especificación de restricciones de dominio

Cuando se configura un nuevo sitio Web XenApp creado con el punto de autenticación En la Interfaz Web, se puede restringir el acceso a los usuarios de determinados dominios.

Puede actualizar estos parámetros en cualquier momento con la tarea Métodos de autenticación de la consola Administración de la Interfaz Web de Citrix. Para obtener más información sobre cómo configurar las restricciones de dominio, consulte Para configurar los parámetros de restricción de dominios.

Especificación de la apariencia de la pantalla de inicio de sesión

Cuando se configura un nuevo sitio Web XenApp, se puede especificar un estilo para las pantallas de Inicio de sesión de los usuarios. Puede elegir entre un diseño minimalista, donde sólo aparecen los campos de inicio de sesión necesarios, y un diseño más complejo que incluye la barra de navegación.

Puede actualizar este parámetro en cualquier momento con la tarea Apariencia del sitio Web de la consola Administración de la Interfaz Web de Citrix. Para obtener más información sobre cómo personalizar la apariencia de la interfaz de usuario, consulte Personalización de la apariencia para los usuarios.

Especificación de los tipos de recursos disponibles para los usuarios

Cuando se configura un sitio nuevo, se deben especificar los tipos de recursos que se desean poner a disposición de los usuarios. La Interfaz Web proporciona a los usuarios acceso a los recursos (aplicaciones, contenido y escritorios) mediante un explorador Web o por medio de Citrix Online Plug-in. La integración con la función de aplicaciones sin conexión permite a los usuarios transmitir por secuencias aplicaciones a sus escritorios y abrirlas localmente.

Puede permitir que los usuarios accedan a los recursos del siguiente modo:

- **En línea.** Los usuarios acceden a aplicaciones, contenido y escritorios alojados en servidores remotos. Los usuarios necesitan una conexión de red para poder trabajar con los recursos.
- **Sin conexión.** Los usuarios descargan aplicaciones en sus escritorios y las abren localmente. Para los sitios de XenApp Services, una vez distribuidas las aplicaciones, los usuarios pueden ejecutarlas en cualquier momento sin necesidad de conectarse a la red. Con los sitios Web XenApp, los usuarios necesitan conexiones de red para iniciar sesión en el sitio e iniciar las aplicaciones. Cuando las aplicaciones están en ejecución, no es necesario mantener la conexión.
- **Modo dual:** Los usuarios acceden a las aplicaciones sin conexión y a las aplicaciones, el contenido y los escritorios en línea en el mismo sitio. Si las aplicaciones sin conexión no están disponibles, se ofrecen las versiones en línea, si es posible.

Puede actualizar este parámetro en cualquier momento con la tarea Tipos de recursos de la consola Administración de la Interfaz Web de Citrix. Para obtener más información sobre los tipos de clientes Citrix, consulte Administración de clientes.

Actualización de sitios existentes

Si actualiza la instalación desde una versión anterior de la Interfaz Web (hasta la versión 4.5 incluida), podrá actualizar los sitios existentes (excepto los sitios de participante invitado de Conferencing Manager).

Importante: Los sitios de participante invitado de Conferencing Manager ya no reciben respaldo. Si actualiza desde una versión anterior de la Interfaz Web, el programa de instalación eliminará los sitios de participante invitado de Conferencing Manager que existan en el servidor Web.

Los sitios existentes de Access Platform/Web XenApp y de servicios de Agente de Program Neighborhood/servicios XenApp se tratan de la siguiente forma:

- **Sitios de configuración local:** Durante la instalación, el programa de instalación de la Interfaz Web actualiza automáticamente a la última versión todos los sitios de configuración local.

- **Sitios agrupados y de configuración centralizada:** Durante la instalación de la Interfaz Web, el programa convierte automáticamente todos los sitios de configuración centralizada o sitios agrupados para utilizar la configuración local. Una vez convertidos, los sitios se actualizan a la versión más reciente.

De forma predeterminada, la Interfaz Web asume que los nombres de archivo de los archivos de instalación de clientes son los mismos que los archivos suministrados en el soporte de instalación de XenApp o XenDesktop. Si descarga clientes del sitio Web de Citrix o si planea distribuir clientes anteriores, verifique que los nombres de los archivos de instalación de clientes estén especificados para los parámetros ClientIcaLinuxX86, ClientIcaMac, ClientIcaSolarisSparc, ClientIcaSolarisX86, ClientIcaWin32 y ClientStreamingWin32 en los archivos de configuración de los sitios Web XenApp. Para obtener más información sobre los parámetros del archivo de configuración de la Interfaz Web, consulte Parámetros de WebInterface.conf.

Uso de las tareas de sitio

Para configurar un sitio, seleccione el tipo de sitio en el panel izquierdo de la consola Administracián de la Interfaz Web de Citrix, haga clic en el sitio en el panel de resultados y seleccione una de las tareas disponibles en el panel Acción o el menú Acción. También puede hacer clic con el botón secundario en el nombre de un sitio en el panel de resultados y seleccionar tareas en el menú contextual.

Algunas tareas sólo están disponibles en ciertos tipos y configuraciones de sitio. La tabla siguiente muestra detalles de las tareas disponibles para cada tipo de sitio.

Tarea	Sitios Web XenApp		Sitios de XenApp Services		Sitios integrados con AD FS
	En línea/modo dual	Sin conexión solamente	En línea/modo dual	Sin conexión solamente	
Método de autenticación	*	*			
Métodos de autenticación	*	*	*	*	*
Servidor proxy del cliente	*		*		*
Distribución de clientes	*	*			*
Actualización de recursos			*	*	
Tipos de recursos	*	*	*	*	*
Acceso seguro	*		*		*
Comunidades de servidores	*	*	*	*	*
Configuración del servidor			*	*	
Opciones de la sesión			*		
Preferencias de sesión	*	*			*
Accesos directos			*	*	
Mantenimiento de sitios	*	*	*	*	*
Apariencia del sitio Web	*	*			*
Control del área de trabajo	*				*

Reparación y desinstalación de sitios

Para reparar y desinstalar sitios, utilice las tareas Reparar sitio y Desinstalar sitio, respectivamente, en Mantenimiento de sitios de la consola Administración de la Interfaz Web de Citrix. Al desinstalar un sitio, éste se elimina totalmente del sistema y será imposible realizar tareas en él.

Importante: Si se crearon scripts o imágenes personalizados para el sitio y se ejecuta la tarea Reparar sitio, estos archivos personalizados se eliminarán. También se eliminan archivos personalizados al usar la tarea Administrar el alojamiento IIS. Citrix recomienda realizar copias de seguridad de los archivos creados antes de usar alguna de estas tareas.

Cómo poner la Interfaz Web a disposición de los usuarios

Cuando la Interfaz Web esté instalada y configurada, proporcione a los usuarios la dirección URL de la página de Inicio de sesión. Si los usuarios desean agregar esta página a los favoritos/marcadores de su explorador Web, Citrix recomienda que la agreguen como http://*NombreServidor*/*RutaSitio* sin especificar ninguna página en particular (por ejemplo, login.aspx).

En los servidores de aplicaciones de Java, la ruta del sitio (es decir, la parte de la dirección URL que aparece detrás del nombre de host y el puerto) es determinada por el motor del servlet. Esta ruta se puede modificar al instalar el archivo .war dentro del motor del servlet. La ruta predeterminada suele ser */WARFileName*, donde *WARFileName* es la primera parte del nombre del archivo .war del sitio.

Acceso directo a los sitios

Si los usuarios acceden a sitios Web XenApp directamente o por medio de Access Gateway Enterprise Edition con un plug-in de acceso seguro Citrix, se puede habilitar la compatibilidad con direcciones URL de recursos. Esto permite a los usuarios crear enlaces persistentes a los recursos a los que se accede mediante la Interfaz Web.

Nota: no se respaldan direcciones URL de recursos para los usuarios que acceden a sitios por medio de Access Gateway Standard Edition o Advanced Edition, ni tampoco aquellos que usan acceso sin cliente por medio de Access Gateway Enterprise Edition.

Los usuarios pueden agregar enlaces persistentes al escritorio o a la lista de accesos directos. Para habilitar el respaldo para direcciones URL de recursos mediante la consola Administración de la Interfaz Web de Citrix, haga clic en Sitios Web XenApp en el panel izquierdo, seleccione el sitio en el panel de resultados, haga clic en Preferencias de sesión en el panel Acción, haga clic en URL persistentes y seleccione la casilla de verificación Permitir acceso a recursos mediante los favoritos del explorador Web.

Importante: Si habilita esta función se inhabilitará la protección contra falsificación de solicitudes entre sitios, o CSRF (Cross-Site Request Forgery).

Cómo hacer que la pantalla de inicio de sesión sea la predeterminada en Microsoft Internet Information Services

Puede hacer que la pantalla de Inicio de sesión de la Interfaz Web sea la página predeterminada de los usuarios del servidor Web, de manera que la dirección URL sea http://*ServerName*/. Para ello, seleccione la casilla de verificación Definir como página predeterminada para el sitio IIS al momento de crear el sitio o posteriormente en la tarea Administrar el alojamiento IIS en Mantenimiento de sitios de la consola Administración de la Interfaz Web de Citrix.

Administración de servidores y comunidades

Esta sección describe cómo configurar la Interfaz Web para comunicarse con las comunidades de servidores. También describe cómo configurar y administrar los parámetros de los servidores y activar el equilibrio de carga entre los servidores que ejecutan el servicio XML de Citrix.

Consideraciones sobre el cambio de contraseñas

Si hay diferencias entre las comunidades de servidores, existen problemas adicionales que pueden impedir que los usuarios puedan cambiar sus contraseñas. Por ejemplo:

- Las directivas de dominio pueden impedir que los usuarios cambien sus contraseñas
- Cuando se combinan comunidades de XenApp para UNIX y comunidades de XenApp para Windows y/o XenDesktop en un mismo sitio, solo es posible cambiar la contraseña de Windows

Citrix recomienda inhabilitar el cambio de contraseñas de usuario en estas situaciones.

Cuando combine recursos de varias comunidades de servidores, asegúrese de que la primera comunidad enumerada en el archivo de configuración del sitio sea una comunidad que esté ejecutando Presentation Server 4.5 o una versión posterior, o XenDesktop.

Si es necesario, se puede habilitar el cambio de contraseña en una distribución mixta de comunidades de servidores. La Interfaz Web se comunica con las comunidades de servidores en el orden en el que se han definido hasta que una comunidad confirma que el cambio de contraseña se ha realizado satisfactoriamente, después de lo cual se detiene el proceso. Esto permite especificar la comunidad de servidores a la que se dirigirá la solicitud de cambio de contraseña. Si la solicitud de cambio de contraseña falla, la siguiente comunidad de servidores en la lista recibirá la solicitud de cambio de contraseña. Conviene utilizar mecanismos adecuados de duplicación de contraseñas entre las distintas comunidades de servidores para asegurar que las contraseñas de usuario permanezcan coherentes.

Para agregar una comunidad de servidores

1. En el menú Inicio de Windows, haga clic en Todos los programas > Citrix > Management Consoles > Citrix Web Interface Management.
2. En el panel izquierdo de la consola Administración de la Interfaz Web de Citrix, haga clic en Sitios Web XenApp o Sitios de servicios XenApp, según corresponda, y seleccione el sitio en el panel de resultados.
3. En el panel Acción, haga clic en Comunidades de servidores.
4. Haga clic en Agregar.
5. Introduzca un nombre para la comunidad de servidores en la casilla Nombre de la comunidad.
6. En el área Configuración del servidor, haga clic en Agregar para especificar un nombre de servidor. Para cambiar un nombre de servidor, seleccione el nombre en la lista y haga clic en Editar. Para eliminar un nombre de servidor, seleccione el nombre y haga clic en Eliminar.
7. Si especifica varios nombres de servidor, seleccione un nombres de la lista y utilice los botones Subir o Bajar para colocarlo en el orden apropiado para la conmutación por error.

Importante: Para la compatibilidad con XenApp 4.0 con Feature Pack 1 para UNIX es necesario realizar una configuración manual adicional en los sitios. Para obtener más información, consulte Para configurar la compatibilidad con XenApp 4.0, con Feature Pack 1, para UNIX.

Para configurar la tolerancia de fallos

La Interfaz Web proporciona tolerancia de fallos entre los servidores que ejecutan el servicio XML de Citrix. Utilice la tarea Comunidades de servidores de la consola Administración de la Interfaz Web de Citrix para configurar la tolerancia de fallos. Si ocurre algún error durante la comunicación con un servidor, la Interfaz Web no intentará comunicarse de nuevo con dicho servidor hasta que haya transcurrido el tiempo especificado en el cuadro Descartar servidores si no responden durante, pero la comunicación continúa con los demás servidores que figuran en la lista Servidores.

De forma predeterminada, un servidor que da error se descarta durante una hora. Si ninguno de los servidores de la lista responde, la Interfaz Web repetirá el intento de comunicación con los servidores cada 10 segundos.

1. En el menú Inicio de Windows, haga clic en Todos los programas > Citrix > Management Consoles > Citrix Web Interface Management.

2. En el panel izquierdo de la consola Administración de la Interfaz Web de Citrix, haga clic en Sitios Web XenApp o Sitios de servicios XenApp, según corresponda, y seleccione el sitio en el panel de resultados.

3. En el panel Acción, haga clic en Comunidades de servidores.

4. Haga clic en Agregar si va a añadir una comunidad, o seleccione un nombre de la lista y haga clic en Modificar para configurar una comunidad existente.

5. En la lista Servidores, coloque los servidores según el orden de prioridad. Seleccione un nombre de servidor en la lista y haga clic en Subir o Bajar para colocar los servidores en el orden apropiado.

6. Cambie el periodo de tiempo durante el cual se descartarán los servidores que den error, introduciendo el número de minutos en la casilla Descartar servidores si no responden durante.

Para habilitar el equilibrio de carga entre los servidores

Puede activar el equilibrio de carga entre los servidores que ejecutan el servicio XML de Citrix. La implementación del equilibrio de carga permite distribuir las conexiones de forma uniforme entre estos servidores, para que ningún servidor se sobrecargue. De forma predeterminada, el equilibrio de carga está desactivado.

Si ocurre un error durante la comunicación con un servidor, se realiza un equilibrio de carga del resto de las comunicaciones entre los distintos servidores de la lista. El servidor que presentó la falla se omite durante un periodo específico (de forma predeterminada es una hora), pero se puede modificar este valor mediante la tarea Comunidades de servidores de la consola Administración de la Interfaz Web de Citrix.

1. En el menú Inicio de Windows, haga clic en Todos los programas > Citrix > Management Consoles > Citrix Web Interface Management.

2. En el panel izquierdo de la consola Administración de la Interfaz Web de Citrix, haga clic en Sitios Web XenApp o Sitios de servicios XenApp, según corresponda, y seleccione el sitio en el panel de resultados.

3. En el panel Acción, haga clic en Comunidades de servidores.

4. Haga clic en Agregar si va a añadir una comunidad, o seleccione un nombre de la lista y haga clic en Modificar para configurar una comunidad existente.

5. En la lista Servidores, agregue los servidores que desea usar para el equilibrio de carga.

6. Marque la casilla Usar la lista de servidores para el equilibrio de carga.

7. Cambie el periodo de tiempo durante el cual se descartarán los servidores que den error, introduciendo el número de minutos en la casilla Descartar servidores si no responden durante.

Configuración de parámetros para todos los servidores de la comunidad

Puede utilizar la tarea Comunidades de servidores de la consola Administración de la Interfaz Web de Citrix para especificar el modo en que Citrix XML Service transporta los datos entre la Interfaz Web y el servidor que ejecuta XenApp o XenDesktop. Citrix XML Service es un componente de XenApp y XenDesktop que actúa como punto de contacto entre la comunidad de servidores y el servidor de la Interfaz Web. De forma predeterminada, el número de puerto es el valor introducido durante la creación del sitio. Este número de puerto debe coincidir con el puerto utilizado por el servicio XML de Citrix.

También se puede especificar un periodo de validez para los tiquets generados por el servidor. La generación de tiques mejora la seguridad de la autenticación para los inicios de sesión explícitos, ya que elimina las credenciales del usuario de los archivos .ica enviados desde el servidor Web a los dispositivos de los usuarios.

Cada tiquet de la Interfaz Web tiene, de forma predeterminada, un periodo de validez de 200 segundos. Este valor puede ajustarse, por ejemplo, para que se adapte a la rapidez de la red, ya que un tiquet caducado no puede autenticar a un usuario satisfactoriamente en la comunidad de servidores. Si cambia la dirección o direcciones IP de un servidor que ejecuta el servicio XML de Citrix, la generación de tiquets no funcionará hasta que reinicie el servidor. Después de cambiar la dirección o direcciones IP de un servidor, asegúrese de reiniciar el servidor.

Para especificar parámetros para todos los servidores

1. En el menú Inicio de Windows, haga clic en Todos los programas > Citrix > Management Consoles > Citrix Web Interface Management.

2. En el panel izquierdo de la consola Administración de la Interfaz Web de Citrix, haga clic en Sitios Web XenApp o Sitios de servicios XenApp, según corresponda, y seleccione el sitio en el panel de resultados.

3. En el panel Acción, haga clic en Comunidades de servidores.

4. Haga clic en Agregar si va a añadir una comunidad, o seleccione un nombre de la lista y haga clic en Modificar para configurar una comunidad existente.

5. En el área Configuración de comunicaciones, introduzca el número de puerto en el cuadro Puerto de servicio XML. Este número de puerto debe coincidir con el puerto utilizado por el servicio XML de Citrix.

6. En la lista Tipo de transporte, seleccione una de las opciones siguientes:

   - HTTP: Permite enviar datos a través de una conexión HTTP estándar. Use esta opción si ha tomado otras medidas para garantizar la seguridad de este enlace.

   - HTTPS: Permite enviar datos a través de una conexión HTTP segura usando SSL (Secure Sockets Layer) o TLS (Transport Layer Security). Asegúrese de que el servicio XML de Citrix esté compartiendo el puerto con IIS (Internet Information Services) y de que IIS esté configurado para funcionar con HTTPS.

   - Traspaso SSL: Envía datos a través de una conexión segura que usa el Traspaso SSL ejecutado en un servidor donde se ejecuta XenApp o XenDesktop, para realizar la autenticación del host y el cifrado de datos.

7. Si va a usar el Traspaso SSL, especifique el puerto TCP del Traspaso SSL en el cuadro Puerto del Traspaso SSL (el puerto predeterminado es 443). La Interfaz Web utiliza los certificados raíz cuando realiza la autenticación de un servidor que ejecuta el Traspaso SSL. Asegúrese de que todos los servidores que ejecutan el Traspaso SSL estén configurados para escuchar en el mismo puerto.

   Nota: si está utilizando el Traspaso SSL o HTTPS, asegúrese de que los nombres de los servidores que especifique coincidan exactamente (incluyendo mayúsculas y minúsculas) con los nombres que figuran en los certificados del servidor que ejecuta XenApp o XenDesktop.

8. Para configurar la generación de tiquets, haga clic en Configuración de tiquets.

9. Introduzca la duración de los tiques de los clientes Citrix para los recursos en línea en los cuadros Duración de tiques ICA.

10. Introduzca la duración de los tiques de Citrix Offline Plug-in en los cuadros Duración de tiques de streaming.

Especificación de parámetros avanzados del servidor

En el cuadro de diálogo Parámetros avanzados de la comunidad se puede habilitar la agrupación de sockets y la redirección de contenido, especificar el tiempo de espera del servicio XML de Citrix y el número de intentos para comunicarse con dicho servicio antes de darlo por fallido.

Para habilitar la agrupación de sockets

Cuando está habilitada la agrupación de sockets, la Interfaz Web 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.

La agrupación de sockets solo está disponible para sitios creados con puntos de autenticación En la Interfaz Web o En Access Gateway y se encuentra activada de forma predeterminada. La agrupación de sockets no debe utilizarse si la Interfaz Web está configurada para usar uno o varios servidores que ejecuten XenApp para UNIX.

1. En el menú Inicio de Windows, haga clic en Todos los programas > Citrix > Management Consoles > Citrix Web Interface Management.
2. En el panel izquierdo de la consola Administración de la Interfaz Web de Citrix, haga clic en Sitios Web XenApp o Sitios de servicios XenApp, según corresponda, y seleccione el sitio en el panel de resultados.
3. En el panel Acción, haga clic en Comunidades de servidores.
4. Haga clic en Avanzado.
5. En el área Agrupación de sockets, marque la casilla Habilitar agrupación de sockets.

Para habilitar la redirección de contenido

Puede utilizar la tarea Comunidades de servidores de la consola Administración de la Interfaz Web de Citrix para habilitar o deshabilitar la redirección de contenido del plug-in al servidor para sitios de servicios XenApp individuales. Este parámetro sobrescribe cualquier otro parámetro de redirección de contenido configurado para XenApp.

Al habilitar la redirección de contenido del plug-in al servidor, los usuarios que ejecuten Citrix Online Plug-In abren el contenido en línea y los archivos locales con aplicaciones distribuidas desde los servidores. Por ejemplo, un usuario de Citrix Online Plug-In que recibe un archivo adjunto de correo electrónico en un programa de correo ejecutado localmente abrirá el archivo adjunto con una aplicación en línea. Si se deshabilita la redirección de contenido, los usuarios abren el contenido en línea y los archivos locales con

aplicaciones instaladas localmente.

De forma predeterminada, la redirección de contenido del plug-in al servidor está habilitada para los sitios de XenApp Services.

Puede configurar la redirección de contenido del plug-in al servidor mediante la asociación de aplicaciones con tipos de archivo. Para obtener más información sobre la asociación de tipos de archivos, consulte Administración de XenApp.

1. En el menú Inicio de Windows, haga clic en Todos los programas > Citrix > Management Consoles > Citrix Web Interface Management.
2. En el panel izquierdo de la consola Administración de la Interfaz Web de Citrix, haga clic en Sitios de servicios XenApp y seleccione el sitio en el panel de resultados.
3. En el panel Acción, haga clic en Comunidades de servidores.
4. Haga clic en Avanzado.
5. En el área Redirección de contenido, marque la casilla Habilitar la redirección de contenido.

Para configurar la comunicación con el servicio XML de Citrix

De forma predeterminada, el tiempo de espera del servicio XML de Citrix se agota transcurrido un minuto y el servicio se considera fallido después de haber realizado dos intentos de comunicación sin éxito. Es posible modificar estos parámetros predeterminados con la tarea Comunidades de servidores de la consola Administración de la Interfaz Web de Citrix.

1. En el menú Inicio de Windows, haga clic en Todos los programas > Citrix > Management Consoles > Citrix Web Interface Management.
2. En el panel izquierdo de la consola Administración de la Interfaz Web de Citrix, haga clic en Sitios Web XenApp o Sitios de servicios XenApp, según corresponda, y seleccione el sitio en el panel de resultados.
3. En el panel Acción, haga clic en Comunidades de servidores.
4. Haga clic en Avanzado.
5. Para configurar la duración del tiempo de espera del servicio XML de Citrix, introduzca los valores adecuados en los cuadros Tiempo de espera del socket.
6. Para especificar cuántas veces se intentará comunicarse con el servicio XML de Citrix antes de considerarlo fallido y descartarlo, introduzca un valor en el cuadro Intentos de contacto con el servicio XML.

Administración de la configuración de servidores

Utilice la tarea Configuración del servidor de la consola Administración de la Interfaz Web de Citrix para configurar la forma en que Citrix online plug-in se comunica con un sitio y si los usuarios son redirigidos o no a sitios alternativos en caso de falla.

Para configurar los parámetros de comunicaciones del servidor

Utilice los parámetros de comunicaciones del servidor para:

- **Activar SSL/TLS para la comunicación:** De forma predeterminada, el inicio de sesión con tarjeta inteligente y las comunicaciones seguras mediante SSL/TLS entre el plug-in y el servidor de la Interfaz Web no están habilitados. Desde este cuadro de diálogo puede activar la comunicación SSL/TLS, y obligar así a las URL a aplicar el protocolo HTTPS automáticamente. Además, debe activar SSL en el servidor que ejecuta XenApp o XenDesktop.

- **Permitir al usuario personalizar la URL del servidor:** La dirección URL del servidor dirige a Citrix Online Plug-in al archivo de configuración correcto. La ruta predeterminada se basa en la dirección de servidor que se haya introducido durante la instalación. Se puede permitir que los usuarios cambien la dirección URL, lo que habilita la casilla Dirección URL del servidor en la página Opciones del servidor del cuadro de diálogo Opciones de Citrix Online Plug-in.

- **Configurar la actualización automática:** Se puede especificar la frecuencia con la que el plug-in debe actualizar sus parámetros de configuración.

1. En el menú Inicio de Windows, haga clic en Todos los programas > Citrix > Management Consoles > Citrix Web Interface Management.

2. En el panel izquierdo de la consola Administración de la Interfaz Web de Citrix, haga clic en Sitios de servicios XenApp y seleccione el sitio en el panel de resultados.

3. En el panel Acción, haga clic en Configuración del servidor.

4. Si desea utilizar la comunicación segura entre Citrix Online Plug-in y un sitio, seleccione Usar SSL/TLS para la comunicación entre los plug-ins y el sitio.

5. Si desea permitir que los usuarios cambien la dirección URL que dirige a Citrix Online Plug-in al archivo de configuración, seleccione Permitir al usuario personalizar la URL del servidor.

6. Si desea configurar la frecuencia con la que Citrix Online Plug-in actualizará sus parámetros de configuración, seleccione Actualización automática cada e introduzca un intervalo de horas, días, semanas o años.

Especificación de las URL de respaldo de Citrix Online Plug-in

Puede especificar servidores de respaldo con los que se pondrá en contacto Citrix Online Plug-in si el servidor principal de la Interfaz Web no está disponible. Utilice la tarea Configuración del servidor de la consola Administración de la Interfaz Web de Citrix para especificar las URL de los servidores de respaldo. En caso de producirse un fallo en el servidor, los usuarios se conectarán automáticamente al servidor de respaldo especificado en primer lugar en la lista Rutas de sitios de respaldo. Si este servidor falla, Citrix Online Plug-in intentará ponerse en contacto con el siguiente servidor de la lista.

Importante: Todas las direcciones URL de respaldo deben apuntar a sitios que estén alojados en el mismo tipo de servidor Web que el sitio principal. Por ejemplo, si el sitio principal es un sitio de Interfaz Web para Microsoft Internet Information Services, los sitios de respaldo especificados también deben ser sitios de Interfaz Web para Microsoft Internet Information Services.

1. En el menú Inicio de Windows, haga clic en Todos los programas > Citrix > Management Consoles > Citrix Web Interface Management.
2. En el panel izquierdo de la consola Administración de la Interfaz Web de Citrix, haga clic en Sitios de servicios XenApp y seleccione el sitio en el panel de resultados.
3. En el panel Acción, haga clic en Configuración del servidor.
4. Haga clic en Respaldo.
5. Haga clic en Agregar.
6. En el cuadro URL de respaldo, introduzca la dirección URL del sitio al que se conectará a los usuarios. Puede definir un máximo de cinco direcciones URL de respaldo por cada sitio.
7. Haga clic en OK.
8. Si especifica varias direcciones URL de servidores de respaldo, colóquelas en el orden apropiado de conmutación por error seleccionándolas en la lista y usando los botones Subir o Bajar.

Para configurar la redirección de sitios

Utilice los parámetros de redirección para definir cuándo se redirigirá a los usuarios a un sitio diferente. Por ejemplo, puede crear un nuevo sitio para el departamento de RRHH y redirigir a todos los usuarios del sitio antiguo al sitio nuevo sin que tengan que introducir la dirección URL manualmente. Puede especificar detalles del sitio nuevo con la tarea Configuración del servidor de la consola Administración de la Interfaz Web de Citrix. Los usuarios se redirigen al sitio nuevo inmediatamente o la próxima vez que inician Citrix Online Plug-in.

1. En el menú Inicio de Windows, haga clic en Todos los programas > Citrix > Management Consoles > Citrix Web Interface Management.

2. En el panel izquierdo de la consola Administración de la Interfaz Web de Citrix, haga clic en Sitios de servicios XenApp y seleccione el sitio en el panel de resultados.

3. En el panel Acción, haga clic en Configuración del servidor.

4. Haga clic en Redirección.

5. Seleccione una de estas opciones:

   - Si no desea configurar la redirección de sitios, seleccione No redirigir

   - Si desea redirigir a los usuarios a un sitio alternativo inmediatamente, seleccione la opción Redirigir al actualizar la configuración de Citrix Online Plug-in.

   - Si desea redirigir a los usuarios a un sitio alternativo la próxima vez que se inicie el plug-in, seleccione Redirigir al iniciar de nuevo Citrix Online Plug-in.
6. Introduzca la dirección URL del sitio alternativo en el campo URL de redirección.

Configuración de la autenticación para la Interfaz Web

Métodos de autenticación

La autenticación se lleva a cabo cuando un usuario accede a los recursos (aplicaciones, contenido y escritorios). Si la autenticación es satisfactoria, se muestra el conjunto de recursos del usuario.

Puede configurar los siguientes métodos de autenticación para la Interfaz Web:

- **Explícita (sitios Web XenApp) o petición de credenciales (sitios de XenApp Services):** Los usuarios deben iniciar sesión introduciendo un nombre de usuario y una contraseña. Se pueden usar nombres principales de usuario (UPN), autenticación basada en dominios de Microsoft, y Novell Directory Services (NDS). Para sitios Web XenApp, también puede utilizarse la autenticación RSA SecurID y SafeWord.

  Nota: la autenticación Novell no está disponible con la Interfaz Web para servidores de aplicaciones de Java y no es compatible con XenApp 6.0, XenApp 5.0 para Windows Server 2008, o XenDesktop. Sin embargo, XenApp 6.0 es compatible con Novell Domain Services para Windows.

- **Paso de credenciales (PassThrough):** Los usuarios se pueden autenticar usando las credenciales que introdujeron al iniciar una sesión en sus escritorios físicos de Windows. No necesitan volver a introducir sus credenciales y su correspondiente conjunto de recursos aparece automáticamente. También se puede usar la autenticación de Windows integrada con Kerberos para la conexión con comunidades de servidores. Si elige la autenticación Kerberos y ésta falla, la autenticación mediante paso de credenciales fallará también y los usuarios no podrán iniciar sesión. Para obtener más información sobre Kerberos, consulte Administración de XenApp.

- **Paso de credenciales (PassThrough) con tarjeta inteligente:** Los usuarios se pueden autenticar mediante la inserción de una tarjeta inteligente en un lector de tarjetas inteligente conectado al dispositivo del usuario. Si los usuarios instalaron Citrix Online Plug-in, se les solicitará el PIN de su tarjeta inteligente cuando inicien sesión en el dispositivo del usuario. Después de iniciar sesión, los usuarios pueden acceder a sus recursos sin que vuelvan a aparecer más solicitudes de inicio de sesión. A los usuarios que se conectan con sitios Web XenApp no se les solicita un PIN. Si está configurando un sitio de XenApp Services, puede usar la autenticación de Windows integrada con Kerberos para realizar una conexión con la Interfaz Web y utilizar las tarjetas inteligentes para la autenticación en la comunidad de servidores. Si elige la autenticación Kerberos y ésta falla, la autenticación mediante paso de credenciales fallará también y los usuarios no podrán iniciar sesión. Para obtener más información sobre Kerberos, consulte Administración de XenApp.

  Nota: las mejoras de seguridad introducidas en Windows Vista requieren que los usuarios de tarjetas inteligentes, que utilicen Windows Vista o Windows 7, introduzcan su PIN al acceder a una aplicación, incluso si se ha habilitado la autenticación mediante paso de credenciales (pass-through) con tarjeta inteligente.

- **Tarjeta inteligente:** Los usuarios se pueden autenticar con una tarjeta inteligente. Este método requiere que el usuario introduzca un número de identificación personal (PIN) para la tarjeta inteligente.

  Nota: Los métodos de autenticación por paso de credenciales, por paso de credenciales con tarjeta inteligente y por tarjeta inteligente no están disponibles con la Interfaz Web para servidores de aplicaciones de Java.

- **Anónimo:** Los usuarios anónimos pueden iniciar sesión sin necesidad de suministrar un nombre de usuario y contraseña, y pueden acceder a recursos que hayan sido publicados para usuarios anónimos.

  Importante: Los usuarios anónimos pueden obtener tiquets de Secure Gateway, a pesar de no estar autenticados por la Interfaz Web. Debido a que Secure Gateway se basa en la emisión de tiques por parte de la Interfaz Web únicamente a usuarios autenticados, esto compromete una de las ventajas de seguridad que da el uso de Secure Gateway.

  Nota: XenDesktop no permite usuarios anónimos.

Recomendaciones para la autenticación

Si va a habilitar la autenticación mediante paso de credenciales (PassThrough), la autenticación mediante paso de credenciales con tarjeta inteligente o la autenticación por tarjeta inteligente, tenga en cuenta lo siguiente:

- Si los usuarios inician sesión en sus equipos usando tarjetas inteligentes y desea habilitar la autenticación mediante paso de credenciales, seleccione la opción para usar autenticación Kerberos.

- Si los usuarios inician sesión en sus equipos usando credenciales explícitas, no habilite la autenticación con tarjeta inteligente o la autenticación mediante paso de credenciales con tarjeta inteligente para el acceso a la Interfaz Web de dichos usuarios.

  Nota: los usuarios que inician sesión en Windows con credenciales explícitas y posteriormente acceden a un sitio configurado para la autenticación mediante paso de credenciales (pass-through) con tarjeta inteligente se encuentran con el cuadro de diálogo Bienvenido a Windows cuando acceden a los recursos. Para cancelar este cuadro de diálogo, los usuarios deben presionar ALT GR + SUPR. Citrix recomienda crear sitios separados para usuarios que inician sesión con tarjetas inteligentes y usuarios que inician sesión con credenciales explícitas.

Si cambia los métodos de autenticación en la Interfaz Web, puede que los usuarios que tengan sesiones iniciadas vean mensajes de error. Si alguno de estos usuarios está usando el explorador Web para acceder a la Interfaz Web, deberá cerrar su explorador Web y volver a abrirlo antes de intentar iniciar nuevamente la sesión.

Configuración de la autenticación

Utilice la tarea Métodos de autenticación de la consola Administración de la Interfaz Web de Citrix para configurar las formas en que los usuarios pueden autenticarse en XenApp, XenDesktop y Citrix online plug-in.

Para configurar los parámetros de restricción de dominios

1. En el menú Inicio de Windows, haga clic en Todos los programas > Citrix > Management Consoles > Citrix Web Interface Management.
2. En el panel izquierdo de la consola Administración de la Interfaz Web de Citrix, haga clic en Sitios Web XenApp o Sitios de servicios XenApp, según corresponda, y seleccione el sitio en el panel de resultados.
3. En el panel Acción, haga clic en Métodos de autenticación y asegúrese de que la autenticación anónima no sea el único método de autenticación habilitado para los usuarios.
4. Haga clic en Propiedades y seleccione Restricción de dominios.
5. Especifique si se va a restringir o no el acceso a los usuarios de dominios seleccionados. Elija una de las siguientes opciones:
   - Si no desea restringir el acceso basado en dominios, seleccione Permitir cualquier dominio
   - Si desea restringir el acceso a usuarios de dominios seleccionados, elija Restringir a los siguientes dominios
6. Haga clic en Agregar.
7. Introduzca el nombre de los dominios que desea agregar a la lista de restricción de dominios en el cuadro Dominio de inicio de sesión.

   Nota: Para restringir el acceso a usuarios de dominios específicos, se deben introducir los mismos nombres de dominio en las listas de Dominio y Restricción de UPN. Para obtener más información, consulte Para usar autenticación basada en dominios.

Para configurar parámetros de inicio de sesión automático

Utilice la tarea Métodos de autenticación de la consola Administración de la Interfaz Web de Citrix para configurar los parámetros de inicio de sesión automático para los usuarios que acceden a sus recursos por medio de la autenticación mediante paso de credenciales (pass-through), la autenticación mediante paso de credenciales con tarjeta inteligente o la autenticación con tarjeta inteligente.

Si el único método de autenticación habilitado para los usuarios es la autenticación anónima, los usuarios iniciarán la sesión en forma automática independientemente de los parámetros configurados por el administrador o por el usuario.

1. En el menú Inicio de Windows, haga clic en Todos los programas > Citrix > Management Consoles > Citrix Web Interface Management.

2. En el panel izquierdo de la consola Administración de la Interfaz Web de Citrix, haga clic en Sitios Web XenApp y seleccione el sitio en el panel de resultados.

3. En el panel Acción, haga clic en Métodos de autenticación y seleccione una o más de las casillas de verificación Paso de credenciales (PassThrough), Paso de credenciales con tarjeta inteligente y Tarjeta inteligente.

4. Haga clic en Propiedades y seleccione Inicio de sesión automático.

5. Especifique si desea permitir que los usuarios inicien la sesión automáticamente y si tendrán la opción de habilitar o inhabilitar el inicio de sesión automático en su pantalla Configuración de la cuenta.

Para usar autenticación basada en dominios

Si utiliza la autenticación explícita o por petición de credenciales, utilice la tarea Métodos de autenticación de la consola Administración de la Interfaz Web de Citrix para configurar si los usuarios se deben autenticar con Windows o Novell Directory Services (NDS).

1. En el menú Inicio de Windows, haga clic en Todos los programas > Citrix > Management Consoles > Citrix Web Interface Management.

2. En el panel izquierdo de la consola Administración de la Interfaz Web de Citrix, haga clic en Sitios Web XenApp o Sitios de servicios XenApp, según corresponda, y seleccione el sitio en el panel de resultados.

3. En el panel Acción, haga clic en Métodos de autenticación y seleccione las casillas de verificación Explícita, Petición de credenciales o Paso de credenciales (PassThrough), según sea necesario.

4. Haga clic en Propiedades y seleccione Tipo de autenticación.

5. Seleccione Windows o NIS (UNIX).

6. Especifique el formato de credenciales para los inicios de sesión de los usuarios. Seleccione una de estas opciones:

   - Para permitir que los usuarios introduzcan su información de inicio de sesión con formato de nombre de usuario principal (UPN) o nombre de usuario de dominio, seleccione Nombre de usuario de dominio y UPN

   - Para especificar que los usuarios deben introducir su información de inicio de sesión sólo con formato de nombre de usuario de dominio, seleccione Sólo nombre de usuario de dominio

   - Para especificar que los usuarios deben introducir su información de inicio de sesión sólo con formato UPN, seleccione Sólo UPN
7. Haga clic en Configuración.

8. En el área Presentación de dominios, configure los siguientes parámetros:

   - Especifique si se va a mostrar o no el cuadro Dominio en la pantalla de Inicio de sesión

   - Especifique si el cuadro Dominio aparece ya rellenado con una lista de dominios que pueden seleccionar los usuarios, o si los usuarios deben introducir un valor en el cuadro Dominio manualmente

     Nota: Si durante el inicio de sesión los usuarios reciben un mensaje de error indicando que "Es necesario especificar un dominio", esto puede deberse a que el campo Dominio está vacío. Para resolver este problema, seleccione Ocultar el campo de dominio. Si la comunidad incluye sólo servidores XenApp para UNIX, en

el cuadro Lista de dominios, seleccione Pre-rellenado y agregue UNIX como nombre de dominio.

- Especifique los dominios que desea que aparezcan en el cuadro Dominio de la pantalla Inicio de sesión

9. En el área Restricción de UPN, configure los siguientes parámetros:

   - Especifique si se aceptarán o no todos los sufijos UPN. De manera predeterminada se permiten todos los sufijos UPN.

   - Especifique los sufijos UPN que desea aceptar.

     Nota: Para restringir el acceso a usuarios de dominios específicos, se deben introducir los mismos nombres de dominio en las listas de Dominio y Restricción de UPN. Para obtener más información, consulte Configuración de la autenticación.

Para usar autenticación de Novell Directory Services

Si utiliza la autenticación explícita o por petición de credenciales, utilice la tarea Métodos de autenticación de la consola Administración de la Interfaz Web de Citrix para configurar si los usuarios se deben autenticar con Windows o Novell Directory Services (NDS).

1. En el menú Inicio de Windows, haga clic en Todos los programas > Citrix > Management Consoles > Citrix Web Interface Management.

2. En el panel izquierdo de la consola Administración de la Interfaz Web de Citrix, haga clic en Sitios Web XenApp o Sitios de servicios XenApp, según corresponda, y seleccione el sitio en el panel de resultados.

3. En el panel Acción, haga clic en Métodos de autenticación y seleccione las casillas de verificación Explícita, Petición de credenciales o Paso de credenciales (PassThrough), según sea necesario.

4. Haga clic en Propiedades y seleccione Tipo de autenticación.

5. Seleccione NDS.

6. Introduzca un nombre en el cuadro Árbol predeterminado.

7. Haga clic en Configuración y configure la restricción de contextos o autenticación sin contexto, según corresponda.

   Nota: De forma predeterminada, eDirectory no permite el acceso con conexión anónima al atributo cn, que es necesario para el inicio de sesión sin contexto. Para obtener información sobre cómo volver a configurar eDirectory, visite http://developer.novell.com/wiki/index.php/Developer_Home.

8. Para sitios XenApp Services, seleccione la opción Usar credenciales de Windows si desea que los usuarios de Citrix Online Plug-in que tengan instalado el cliente Novell usen las credenciales de Windows para la autenticación mediante paso de credenciales.

Habilitación de la autenticación explícita

Si se habilita la autenticación explícita, los usuarios deben tener una cuenta de usuario y suministrar las credenciales apropiadas para iniciar la sesión.

La consola permite cambiar los parámetros para la autenticación explícita. Por ejemplo, puede configurar si los usuarios están autorizados o no para cambiar sus contraseñas dentro de una sesión.

La autenticación explícita sólo está disponible para sitios Web XenApp.

Para habilitar la autenticación explícita

1. En el menú Inicio de Windows, haga clic en Todos los programas > Citrix > Management Consoles > Citrix Web Interface Management.

2. En el panel izquierdo de la consola Administración de la Interfaz Web de Citrix, haga clic en Sitios Web XenApp y seleccione el sitio en el panel de resultados.

3. En el panel Acción, haga clic en Métodos de autenticación y seleccione la casilla de verificación Explícita.

4. Haga clic en Propiedades para configurar más parámetros para la autenticación explícita.

Para configurar los parámetros de contraseñas para la autenticación explícita

Utilice la tarea Métodos de autenticación de la consola Administración de la Interfaz Web de Citrix para configurar las opciones de cambio de contraseña y aviso de caducidad de contraseña para los usuarios. Algunos parámetros de contraseñas se ven afectados por otros parámetros de autenticación configurados para el sitio:

- La opción En todo momento no está disponible si se seleccionan las opciones RSA SecurID y Usar integración de contraseñas de Windows en la página Autenticación de dos factores.

- Si se elige la opción Usar parámetros de aviso de la directiva de grupos de Active Directory es posible que los parámetros de aviso se configuren de acuerdo con su directiva actual de Windows. Si la directiva actual de Windows no tiene ningún periodo de aviso configurado, los usuarios no recibirán ningún aviso para que cambien su contraseña antes de que esta caduque.

1. En el menú Inicio de Windows, haga clic en Todos los programas > Citrix > Management Consoles > Citrix Web Interface Management.

2. En el panel izquierdo de la consola Administración de la Interfaz Web de Citrix, haga clic en Sitios Web XenApp y seleccione el sitio en el panel de resultados.

3. En el panel Acción, haga clic en Métodos de autenticación y seleccione la casilla de verificación Explícita.

4. Haga clic en Propiedades y seleccione Parámetros de contraseñas.

5. Si desea permitir que los usuarios cambien sus contraseñas dentro de una sesión de la Interfaz Web, seleccione la casilla de verificación Permitir al usuario cambiar su contraseña.

6. Para especificar cuándo los usuarios pueden cambiar su contraseña, seleccione una de las siguientes opciones:

    - Para permitir que los usuarios cambien su contraseña cuando ésta caduque, seleccione Solo cuando caduque. Con esta opción, si un usuario no logra iniciar una sesión en la Interfaz Web debido a una contraseña caducada, se le redirigirá al cuadro de diálogo Cambiar contraseña. Después de cambiar la contraseña, se inicia la sesión del usuario automáticamente usando la contraseña nueva.

    - Para permitir que los usuarios cambien sus contraseñas en la Interfaz Web siempre que lo deseen, seleccione En todo momento. Cuando se activa esta opción, aparece el botón Cambiar contraseña en las pantallas de Aplicaciones y Configuración de la cuenta de los usuarios. Cuando el usuario hace clic en este botón, aparece un cuadro de diálogo en el que puede introducir una contraseña nueva.

7. Para configurar un mensaje de aviso para los usuarios cuando su contraseña esté a punto de caducar, seleccione una de las siguientes opciones:

   - Si no desea enviar notificaciones a los usuarios antes de que caduquen sus contraseñas, seleccione No avisar.

   - Para utilizar los parámetros actuales de recordatorio de la directiva de Windows, seleccione Usar parámetros de aviso de la directiva de grupos de Active Directory.

   - Para avisar a los usuarios que su contraseña va a caducar dentro de un número determinado de días, seleccione Usar un parámetro de aviso personalizado. Especifique el número de días, semanas o años en los cuadros de la sección Avisar a los usuarios antes de que caduque su contraseña.

Para habilitar la autenticación de dos factores

Utilice la tarea Métodos de autenticación de la consola Administración de la Interfaz Web de Citrix para habilitar la autenticación de dos factores para los usuarios, si es necesario.

1. En el menú Inicio de Windows, haga clic en Todos los programas > Citrix > Management Consoles > Citrix Web Interface Management.
2. En el panel izquierdo de la consola Administración de la Interfaz Web de Citrix, haga clic en Sitios Web XenApp y seleccione el sitio en el panel de resultados.
3. En el panel Acción, haga clic en Métodos de autenticación y seleccione la casilla de verificación Explícita.
4. Haga clic en Propiedades y seleccione Autenticación de dos factores.
5. Seleccione el tipo de autenticación de dos factores que desea utilizar de la lista Configuración de dos factores y configure los parámetros adicionales según corresponda.

Para obtener más información sobre cómo configurar la autenticación con Aladdin SafeWord, RSA SecurID y RADIUS, consulte Configuración de la autenticación de dos factores.

Configuración del autoservicio de cuentas

La integración con el autoservicio de cuentas de Password Manager permite a los usuarios restablecer su contraseña de red y desbloquear su cuenta con solo responder una serie de preguntas de seguridad.

Cuando se habilita el autoservicio de cuentas en un sitio, se dejan al descubierto funciones de seguridad importantes para cualquiera que acceda a dicho sitio. Si el sitio es accesible desde Internet no existe ningún tipo de restricción sobre quién puede acceder a dichas funciones. Si su organización o empresa tiene una directiva de seguridad que restringe las funciones de administración de cuentas de usuario al uso exclusivamente interno, asegúrese de que el sitio no sea accesible desde fuera de la red interna.

Importante: Al configurar Password Manager, se especifican los usuarios que podrán restablecer contraseñas y desbloquear sus cuentas. Si habilita esta funcionalidad para la Interfaz Web, es posible que a los usuarios se les siga denegando el permiso para realizar estas tareas según los parámetros que configure para Password Manager.

El autoservicio de cuentas sólo está disponible para los usuarios que acceden a la Interfaz Web mediante conexiones HTTPS. Si los usuarios acceden a la Interfaz Web usando una conexión HTTP, el autoservicio de cuentas no estará disponible. El autoservicio de cuentas no está disponible para sitios integrados de Access Gateway.

El autoservicio de cuentas no admite el uso de credenciales UPN para el inicio de sesión, tales como *NombreDeUsuario*@*dominio.com*.

Antes de configurar el autoservicio de cuentas de un sitio, debe asegurarse de lo siguiente:

- Que el sitio esté configurado para utilizar la autenticación explícita basada en Windows.
- Que el sitio esté configurado para utilizar solamente un servicio Password Manager. Si la Interfaz Web está configurada para utilizar varias comunidades en el mismo dominio o en dominios de confianza, Password Manager debe estar configurado para aceptar credenciales de todos esos dominios.
- Que el sitio esté configurado para permitir que los usuarios cambien sus contraseñas en cualquier momento si se desea permitir la funcionalidad de restablecimiento de contraseñas.

Para configurar el autoservicio de cuentas

1. En el menú Inicio de Windows, haga clic en Todos los programas > Citrix > Management Consoles > Citrix Web Interface Management.

2. En el panel izquierdo de la consola Administración de la Interfaz Web de Citrix, haga clic en Sitios Web XenApp y seleccione el sitio en el panel de resultados.

3. En el panel Acción, haga clic en Métodos de autenticación y seleccione la casilla de verificación Explícita.

4. Haga clic en Propiedades y seleccione Autoservicio de cuentas.

5. Especifique si desea o no que los usuarios puedan restablecer sus contraseñas o desbloquear sus cuentas.

6. Introduzca la dirección URL de Password Manager en el cuadro URL del servicio Password Manager.

Habilitación de la autenticación por petición de credenciales

Si se habilita la autenticación por petición de credenciales, los usuarios deben tener una cuenta de usuario y suministrar las credenciales apropiadas cuando deseen iniciar sesión.

La autenticación por petición de credenciales sólo está disponible para sitios de XenApp Services.

Para habilitar la autenticación por petición de credenciales

1. En el menú Inicio de Windows, haga clic en Todos los programas > Citrix > Management Consoles > Citrix Web Interface Management.
2. En el panel izquierdo de la consola Administración de la Interfaz Web de Citrix, haga clic en Sitios de servicios XenApp y seleccione el sitio en el panel de resultados.
3. En el panel Acción, haga clic en Métodos de autenticación y seleccione la casilla de verificación Petición de credenciales.
4. Haga clic en Propiedades para configurar más parámetros para la autenticación por petición de credenciales.

Para configurar los parámetros de contraseñas para la autenticación por petición de credenciales

Utilice la tarea Métodos de autenticación de la consola Administración de la Interfaz Web de Citrix para especificar si los usuarios pueden guardar sus contraseñas y para configurar otras opciones de cambio de contraseña.

1. En el menú Inicio de Windows, haga clic en Todos los programas > Citrix > Management Consoles > Citrix Web Interface Management.

2. En el panel izquierdo de la consola Administración de la Interfaz Web de Citrix, haga clic en Sitios de servicios XenApp y seleccione el sitio en el panel de resultados.

3. En el panel Acción, haga clic en Métodos de autenticación y seleccione la casilla de verificación Petición de credenciales.

4. Haga clic en Propiedades y seleccione Parámetros de contraseñas.

5. Para permitir a los usuarios guardar sus contraseñas, seleccione la opción Permitir al usuario guardar su contraseña.

6. Si desea permitir que los usuarios cambien sus contraseñas cuando estas caduquen, marque la casilla Permitir a los usuarios cambiar contraseñas caducadas comunicándose con.

7. Especifique la ruta para la solicitud del cambio de contraseña, eligiendo una de estas opciones:

   - Si desea que los usuarios de Citrix Online Plug-in cambien sus contraseñas comunicándose directamente con el controlador de dominio, seleccione Controlador de dominio directamente. Esta es la opción más segura porque la solicitud de cambio de contraseña se dirige directamente de Citrix online plug-in al controlador de dominio, sin pasar por la Interfaz Web ni por XenApp/XenDesktop.

   - Si prefiere que los usuarios de Citrix online plug-in cambien sus contraseñas conectándose directamente con el controlador de dominio, pero desea permitir conexiones por medio de la Interfaz Web y XenApp/XenDesktop si falla el método de conexión preferido, seleccione Controlador de dominio directamente, con servicio de soporte para comunidad de servidores.

   - Si desea que los usuarios de Citrix online plug-in puedan cambiar sus contraseñas comunicándose con el controlador de dominio por medio de la Interfaz Web y XenApp/XenDesktop, seleccione Comunidad de servidores. Con esta opción, tan pronto como los usuarios cambien sus contraseñas, la Interfaz Web y XenApp y/o XenDesktop se actualizarán con la nueva contraseña. No obstante, esta opción es menos segura porque la nueva contraseña se encamina a través de un mayor número de conexiones de red.

Habilitación de la autenticación mediante paso de credenciales (PassThrough)

Actualizado: 2013-02-21

Desde la consola puede habilitar la autenticación mediante paso de credenciales (PassThrough) para usuarios que inicien sesión en sus escritorios físicos con credenciales de dominio, contraseña y nombre de usuario. Esta función permite que los usuarios se autentiquen usando las credenciales que introdujeron al iniciar sesión en sus escritorios físicos de Windows. Los usuarios no necesitan volver a introducir sus credenciales. Su correspondiente conjunto de recursos aparece automáticamente.

Requisitos del paso de credenciales (PassThrough)

Para usar la función de autenticación mediante el paso de credenciales (PassThrough), la Interfaz Web debe ejecutarse en IIS y los usuarios deben ejecutar versiones respaldadas de Internet Explorer. Para sitios Web XenApp, los usuarios deben agregar el sitio a los sitios de confianza de Windows o las zonas de intranet local utilizando Internet Explorer.

Si está usando Internet Explorer versión 7 o posterior:

1. Agregue el sitio a los sitios de confianza de Windows, haga clic en Opciones de Internet y vaya a la ficha Seguridad.

2. Seleccione la zona de Sitios de confianza y haga clic en Nivel personalizado.

3. Vaya a Autenticación del usuario en la ventana de Configuración de seguridad, haga clic en Inicio de sesión y seleccione Inicio de sesión automático con el nombre de usuario y contraseña actuales.

Para IIS 7.*x* que se ejecuta en Windows Server 2008, asegúrese de que esté activado el servicio de función Servidor Web > Seguridad > Autenticación de Windows para la función Servidor Web (IIS).

Importante: Si los servidores ejecutan una versión anterior a Citrix MetaFrame XP Feature Release 2, es posible que los usuarios puedan ver la totalidad de las aplicaciones y el contenido al usar la autenticación mediante el paso de credenciales.

Si los usuarios usan Clientes para Windows de versiones anteriores a la 6.30 y el cifrado ICA (SecureICA) está activado, no se puede usar la autenticación por paso de credenciales. Para usar el paso de credenciales con el cifrado ICA, los usuarios deben tener instalados los clientes Citrix más recientes. La autenticación por paso de credenciales no está disponible con la Interfaz Web para servidores de aplicaciones de Java.

Importante: Cuando un usuario accede a un recurso, se envía un archivo al cliente Citrix (en algunos casos, mediante el explorador Web como intermediario). El archivo puede contener un parámetro que solicite al cliente enviar al servidor las credenciales de la estación de trabajo del usuario. De forma predeterminada, el cliente no cumple con este

parámetro; no obstante, existe el riesgo de que, si se habilita la función de paso de credenciales en Citrix Online Plug-In, una persona no autorizada pueda enviar al usuario un archivo que ocasione el desvío de las credenciales del usuario a un servidor falso o no autorizado. Por lo tanto, use la autenticación por paso de credenciales sólo en entornos seguros y de confianza.

Paso 1: Instalación del plug-in para la autenticación mediante paso de credenciales

Debe instalar Citrix online plug-in o Citrix Desktop Viewer en los dispositivos de los usuarios mediante una cuenta de administrador. La autenticación mediante paso de credenciales (pass-through) solo está disponible con estos plug-ins, que se incluyen en el soporte de instalación de XenApp y XenDesktop. Por razones de seguridad, Citrix Online Plug-in – web no incluye esta función. Esto significa que no se puede usar la instalación de clientes basada en la Web para distribuir los plug-ins de Citrix que disponen de esta función entre los clientes.

Después de la instalación, se debe habilitar la autenticación mediante paso de credenciales (PassThrough) para todos los clientes Citrix que usan directivas de grupo. Para obtener más información, consulte http://support.citrix.com/article/CTX122676 y la documentación de *Receiver y Plug-ins* > y *Online Plug-in para Windows* en Citrix eDocs.

Paso 2: Habilitación del paso de credenciales (PassThrough) en los plugins

La habilitación de la autenticación mediante paso de credenciales en los clientes es un proceso que consta de dos pasos. En primer lugar, agregue la plantilla del cliente en el Editor de objetos de directiva de grupo. Una vez agregada esta plantilla, utilícela para habilitar la autenticación mediante paso de credenciales para todos los clientes.

Para agregar la plantilla cliente al Editor de objetos de directiva de grupo para la autenticación mediante paso de credenciales (PassThrough)

1. Abra el complemento Editor de objetos de directiva de grupo en la consola MMC.
2. Seleccione el objeto de directiva de grupo que desea modificar.
3. Seleccione el nodo Plantillas administrativas y en el menú Acción haga clic en Agregar/Quitar plantillas.
4. Haga clic en Agregar y busque el archivo de plantilla cliente, icaclient.adm. Este archivo se instala en la carpeta \Configuration de los clientes, que generalmente se encuentra en C:\Archivos de programa(x86)\Citrix*ClientName*\Configuration.
5. Haga clic en Abrir para agregar la plantilla; después, haga clic en Cerrar.

Para habilitar la autenticación mediante paso de credenciales (PassThrough) para todos los clientes

1. Abra el complemento Editor de objetos de directiva de grupo en la consola MMC.
2. Seleccione el objeto de directiva de grupo que desea modificar.
3. En el panel izquierdo, expanda el nodo Plantillas administrativas.
4. Seleccione Plantillas administrativas clásicas (ADM) > Componentes Citrix. Expanda el nodo del cliente que ha instalado y seleccione Autenticación de usuario.
5. En el panel de resultados, seleccione Nombre de usuario local y contraseña.
6. En el menú Acción, haga clic en Editar.
7. Haga clic en Habilitada y compruebe que la casilla de verificación Habilitar autenticación mediante paso de credenciales (pass-through) esté seleccionada.
8. Asegúrese de completar los pasos anteriores tanto para el usuario como para el equipo en el Editor de objetos de directiva de grupo.
9. Cierre la sesión y vuelva a iniciarla para que se apliquen los cambios en las directivas.

Paso 3: Habilitación del paso de credenciales (PassThrough) usando la consola

Utilice la consola Administración de la Interfaz Web de Citrix para habilitar la autenticación mediante paso de credenciales (pass-through). Cuando se habilita esta función, los usuarios no necesitan volver a introducir sus credenciales y ven su correspondiente conjunto de recursos automáticamente.

También puede habilitar Kerberos con autenticación mediante paso de credenciales para sitios Web XenApp y sitios de servicios XenApp. Para los sitios de servicios XenApp también puede especificarse Kerberos para autenticación mediante paso de credenciales con tarjeta inteligente.

Para habilitar la autenticación mediante paso de credenciales (PassThrough)

1. En el menú Inicio de Windows, haga clic en Todos los programas > Citrix > Management Consoles > Citrix Web Interface Management.

2. En el panel izquierdo de la consola Administración de la Interfaz Web de Citrix, haga clic en Sitios Web XenApp o Sitios de servicios XenApp, según corresponda, y seleccione el sitio en el panel de resultados.

3. En el panel Acción, haga clic en Métodos de autenticación y seleccione la casilla de verificación Paso de credenciales (PassThrough).

4. Haga clic en Propiedades y seleccione Autenticación Kerberos.

5. Si quiere habilitar la autenticación Kerberos, marque la casilla Usar autenticación Kerberos para conectar con servidores (para sitios Web XenApp) o la casilla Usar sólo Kerberos (para sitios de servicios XenApp).

Habilitación de la autenticación con tarjeta inteligente

Para usar la autenticación con tarjeta inteligente, la Interfaz Web debe ejecutarse en IIS y los usuarios deben ejecutar versiones respaldadas de Internet Explorer o Firefox. Para la autenticación mediante paso de credenciales (pass-through) con tarjeta inteligente, los usuarios deben ejecutar versiones compatibles de Internet Explorer. Firefox no es compatible con este tipo de autenticación.

Si desea habilitar la autenticación mediante paso de credenciales (pass-through) con tarjeta inteligente para un sitio Web XenApp, los usuarios deben agregar el sitio a los sitios de confianza de Windows o las zonas de intranet local utilizando Internet Explorer.

Si tiene IIS 7.*x* ejecutándose en Windows Server 2008, asegúrese de que esté activado el servicio de función Servidor Web > Seguridad > Autenticación de asignaciones de certificado de cliente para la función Servidor Web (IIS). Si desea habilitar la autenticación mediante paso de credenciales (pass-through) con tarjeta inteligente, asegúrese de que también esté activado el servicio de función Servidor Web > Seguridad > Autenticación de Windows.

La autenticación con tarjeta inteligente no se encuentra respaldada por la Interfaz Web para servidores de aplicaciones de Java.

El servidor Web debe tener habilitado Secure Sockets Layer (SSL) porque es necesario usar SSL para proteger la comunicación entre el explorador Web y el servidor. Para obtener más información, consulte la documentación del servidor Web.

Para habilitar la autenticación con tarjeta inteligente (con o sin otros métodos de autenticación), debe configurar la pantalla de Inicio de sesión para que sea accesible solo mediante conexiones HTTPS. Si se utiliza HTTP o si la conexión HTTPS no está correctamente configurada, los usuarios recibirán un mensaje de error y no podrán iniciar sesión. Para evitar este problema, proporcione la dirección URL HTTPS completa a todos los usuarios; por ejemplo: https://www.*MyCompany.com*:443/Citrix/XenApp.

Para obtener más información sobre los requisitos del dispositivo de usuario y del servidor para la autenticación con tarjeta inteligente, consulte Online Plug-in para Windows y Administración de XenApp.

Paso 1: Instalar el plugin para la autenticación con tarjeta inteligente

Para usar la autenticación con tarjeta inteligente, los usuarios deben instalar Citrix online plug-in o Citrix Desktop Viewer. De manera alternativa, pueden utilizar la instalación de clientes basada en la Web para descargar e instalar Citrix online plug-in para Web, desde un sitio Web XenApp correctamente configurado. No obstante, para utilizar la autenticación mediante paso de credenciales (pass-through) con tarjeta inteligente, se debe instalar Citrix online plug-in o Citrix Desktop Viewer en los dispositivos de los usuarios mediante una cuenta de administrador. La autenticación mediante paso de credenciales (pass-through) solo está disponible con estos plug-ins, que se incluyen en el soporte de instalación de XenApp y XenDesktop. Por razones de seguridad, Citrix Online Plug-in – web no incluye esta función.

Si desea habilitar la autenticación mediante paso de credenciales (pass-through) con tarjeta inteligente, primero debe habilitar la autenticación mediante paso de credenciales para todos los clientes Citrix por medio de la directiva de grupo después de instalar el plug-in. La habilitación de la autenticación mediante paso de credenciales en los clientes es un proceso que consta de dos pasos. En primer lugar, agregue la plantilla del cliente en el Editor de objetos de directiva de grupo. Una vez agregada esta plantilla, utilícela para habilitar la autenticación mediante paso de credenciales para todos los clientes.

Para agregar la plantilla cliente al Editor de objetos de directiva de grupo para la autenticación mediante paso de credenciales (PassThrough)

1. Abra el complemento Editor de objetos de directiva de grupo en la consola MMC.
2. Seleccione el objeto de directiva de grupo que desea modificar.
3. Seleccione el nodo Plantillas administrativas y en el menú Acción haga clic en Agregar/Quitar plantillas.
4. Haga clic en Agregar y busque el archivo de plantilla cliente, icaclient.adm. Este archivo se instala en la carpeta \Configuration de los clientes, que generalmente se encuentra en C:\Archivos de programa(x86)\Citrix*ClientName*\Configuration.
5. Haga clic en Abrir para agregar la plantilla; después, haga clic en Cerrar.

Para habilitar la autenticación mediante paso de credenciales con tarjeta inteligente para todos los clientes

1. Abra el complemento Editor de objetos de directiva de grupo en la consola MMC.
2. Seleccione el objeto de directiva de grupo que desea modificar.
3. En el panel izquierdo, expanda el nodo Plantillas administrativas.
4. Seleccione Plantillas administrativas clásicas (ADM) > Componentes Citrix. Expanda el nodo del cliente que ha instalado y seleccione Autenticación de usuario.
5. En el panel de resultados, seleccione Autenticación con tarjeta inteligente.
6. En el menú Acción, haga clic en Editar.
7. Haga clic en Habilitada y seleccione las casillas de verificación Permitir autenticación con tarjeta inteligente y Usar autenticación mediante paso de credenciales (pass-through) para PIN.

Paso 2: Habilitación del Asignador de servicios de directorios de Windows

Para habilitar la autenticación con tarjeta inteligente, debe asegurarse de que el Asignador de servicios de directorios de Windows esté habilitado en el servidor de la Interfaz Web.

La autenticación de la Interfaz Web usa cuentas de dominio de Windows; es decir, credenciales de nombre de usuario y contraseña. Las tarjetas inteligentes contienen certificados. El asignador de servicios de directorios asigna un certificado a una cuenta de dominio de Windows usando Active Directory de Windows.

Para habilitar el asignador de servicios de directorios de Windows en Microsoft Internet Information Services 7.x

1. En el servidor de la Interfaz Web, asegúrese de que el servicio de función Servidor Web > Seguridad > Autenticación de asignaciones de certificado de cliente de IIS *no* esté instalado para la función Servidor Web (IIS).

2. Abra el complemento Administrador de Internet Information Services (IIS) en la consola MMC.

3. Seleccione el servidor Web en el panel de la izquierda y, en la Vista funciones, haga doble clic en Autenticación.

4. En la página Autenticación, habilite el método Autenticación de certificados de cliente de Active Directory.

Para habilitar el asignador de servicios de directorios de Windows en Microsoft Internet Information Services 6.0

1. Abra el complemento Administrador de Internet Information Services (IIS) en la consola MMC en el servidor de la Interfaz Web.

2. Seleccione el nodo Sitios Web en el servidor de la Interfaz Web y, en el panel Acción, haga clic en Propiedades.

3. En la ficha Seguridad de directorios, seleccione Habilitar el asignador de servicios de directorio de Windows en la sección Comunicaciones seguras.

Paso 3: Habilitación de la autenticación con tarjeta inteligente en la Interfaz Web

Es necesario configurar la Interfaz Web para habilitar la autenticación con tarjeta inteligente (para que los usuarios puedan acceder a la Interfaz Web y obtener su conjunto de recursos) y la autenticación en el servidor (para que los usuarios puedan acceder a los recursos en una sesión usando la Interfaz Web).

Para habilitar la autenticación con tarjeta inteligente en sitios Web XenApp

1. En el menú Inicio de Windows, haga clic en Todos los programas > Citrix > Management Consoles > Citrix Web Interface Management.

2. En el panel izquierdo de la consola Administración de la Interfaz Web de Citrix, haga clic en Sitios Web XenApp y seleccione el sitio en el panel de resultados.

3. En el panel Acción, haga clic en Métodos de autenticación y seleccione la casilla de verificación Tarjeta inteligente o Paso de credenciales (pass-through) con tarjeta inteligente, según corresponda.

4. Haga clic en Propiedades para configurar más parámetros para la autenticación con tarjeta inteligente.

Para habilitar la autenticación con tarjeta inteligente en sitios de XenApp Services

1. En el menú Inicio de Windows, haga clic en Todos los programas > Citrix > Management Consoles > Citrix Web Interface Management.

2. En el panel izquierdo de la consola Administración de la Interfaz Web de Citrix, haga clic en Sitios de servicios XenApp y seleccione el sitio en el panel de resultados.

3. En el panel Acción, haga clic en Métodos de autenticación y seleccione la casilla de verificación Tarjeta inteligente o Paso de credenciales (pass-through) con tarjeta inteligente, según corresponda.

4. Haga clic en Propiedades y seleccione Perfil móvil.

5. Para configurar el comportamiento de la Interfaz Web cuando se quita una tarjeta inteligente, seleccione Habilitar movilidad y elija una de estas opciones:

   - Para desconectar la sesión de un usuario cuando quite su tarjeta inteligente, seleccione Desconectar las sesiones al quitar la tarjeta inteligente.

   - Para cerrar la sesión de un usuario cuando quite su tarjeta inteligente, seleccione Cerrar las sesiones al quitar la tarjeta inteligente.

6. Si habilita la autenticación mediante paso de credenciales (pass-through) con tarjeta inteligente y desea utilizar la autenticación Kerberos entre el plug-in y el sitio de servicios XenApp, haga clic en Autenticación Kerberos y marque la casilla de verificación Usar Kerberos para autenticar al sitio de servicios XenApp.

Ejemplo: Habilitación de la autenticación con tarjeta inteligente para los usuarios

Suponga que desea habilitar la autenticación mediante paso de credenciales (pass-through) con tarjeta inteligente para un usuario. El equipo del usuario está ejecutando Windows XP. El equipo tiene conectado un lector de tarjetas inteligentes y el uso de éstas ya se ha habilitado en la comunidad de servidores. Actualmente, la Interfaz Web está configurada para permitir solo la autenticación explícita/petición (mediante un nombre de usuario y una contraseña).

Para habilitar la autenticación mediante paso de credenciales (pass-through) con tarjeta inteligente

1. Utilice el soporte de instalación apropiado para instalar Citrix online plug-in o Citrix Desktop Viewer en el equipo del usuario. La instalación del plug-in se lleva a cabo mediante una cuenta de administrador. Para sitios Web XenApp, agregue el sitio a los sitios de confianza de Windows o las zonas de intranet local utilizando Internet Explorer en el equipo del usuario.

2. Habilite la autenticación mediante paso de credenciales (PassThrough) para todos los clientes Citrix por medio de la directiva de grupo. Para obtener más información, consulte Paso 1: Instalar el plugin para la autenticación con tarjeta inteligente. También debe asegurarse de que la autenticación por paso de credenciales esté habilitada en la comunidad de servidores. Para obtener más información, consulte la documentación del servidor Citrix.

3. Asegúrese de que el asignador de servicios de directorios de Windows esté activado. Para obtener más información, consulte Paso 2: Habilitación del Asignador de servicios de directorios de Windows.

4. Utilice la tarea Métodos de autenticación de la consola Administración de la Interfaz Web de Citrix para habilitar la autenticación mediante paso de credenciales (pass-through) con tarjeta inteligente. Para obtener más información, consultePaso 3: Habilitación de la autenticación con tarjeta inteligente en la Interfaz Web Los usuarios inician sesión en sus escritorios físicos de Windows con sus tarjetas inteligentes. Cuando los usuarios acceden a los recursos, la sesión se inicia en forma automática. Cuando está habilitada la autenticación con tarjeta inteligente sin paso de credenciales, los usuarios tienen que volver a ingresar sus PIN cuando acceden a los recursos.

Configuración de la autenticación de dos factores

Puede configurar los siguientes métodos de autenticación de dos factores para sitios Web XenApp:

- **Aladdin SafeWord para Citrix.** Es un método de autenticación que utiliza códigos alfanuméricos generados por tokens de SafeWord y, de manera opcional, números PIN para crear un código de acceso. Los usuarios deben introducir sus credenciales de dominio y los códigos de acceso de SafeWord en la pantalla de Inicio de sesión para poder acceder a las aplicaciones en el servidor.

- **RSA SecurID.** Es un método de autenticación que utiliza números generados por tokens de RSA SecurID (*códigos token*) y números PIN para crear un *CÓDIGO DE ACCESO*. Los usuarios deben introducir sus nombres de usuario, dominios, contraseñas y códigos de acceso de RSA SecurID en la pantalla de Inicio de sesión para poder acceder a los recursos en el servidor. Al crear usuarios en el servidor RSA ACE/Server, los nombres de inicio de sesión de los usuarios deben ser los mismos que sus correspondientes nombres de usuario de dominio.

  Nota: Cuando se utiliza la autenticación RSA SecurID, el sistema puede generar un nuevo número PIN para el usuario. El PIN aparece en pantalla durante 10 segundos o hasta que el usuario hace clic en Aceptar o Cancelar para evitar que otras personas puedan verlo. Esta función no está disponible para dispositivos PDA.

- **Servidor RADIUS.** Es un método de autenticación que utiliza el protocolo de autenticación RADIUS (Remote Authentication Dial-in User Service) en lugar del software de propiedad exclusiva de agente. Tanto SafeWord como SecurID pueden instalarse y configurarse para presentarse como servidor RADIUS. En el caso de la Interfaz Web para servidores de aplicaciones de Java, la autenticación RADIUS es la única opción disponible para la autenticación de dos factores.

Habilitación de la autenticación con SafeWord en Microsoft Internet Information Services

Esta sección describe cómo habilitar el respaldo de RSA SecurID 6.0.

Requisitos de SafeWord

Para usar la autenticación SafeWord con la Interfaz Web para Microsoft Internet Information Services:

- Obtenga la última versión del SafeWord Agent de Aladdin Knowledge Systems. Si necesita respaldo para la autenticación con UPN, asegúrese de aplicar las actualizaciones más recientes del SafeWord Agent para la Interfaz Web y para el servidor SafeWord.
- Asegúrese de que la Interfaz Web esté instalada antes de instalar SafeWord Agent para la Interfaz Web.
- Asegúrese de que SafeWord Agent para la Interfaz Web esté instalado en el servidor de la Interfaz Web.

Para obtener más información sobre la configuración de su producto SafeWord, visite http://www.aladdin.com/safeword/default.aspx.

Habilitación de la autenticación RSA SecurID en la consola

Debe configurar la Interfaz Web para permitir que los usuarios usen la autenticación con RSA SecurID y puedan acceder a su conjunto de recursos y visualizarlos. Para ello, debe utilizar la tarea Métodos de autenticación de la consola Administración de la Interfaz Web de Citrix.

Habilitación de la autenticación con RSA SecurID en Microsoft Internet Information Services

Esta sección describe cómo habilitar el respaldo de RSA SecurID 7.0.

Requisitos de SecurID

Para usar la autenticación SecurID con la Interfaz Web para Microsoft Internet Information Services:

- RSA ACE/Agent para Windows 7.0 o una versión posterior debe estar instalado en el servidor Web.
- La Interfaz Web debe instalarse después de instalar RSA ACE/Agent.
- La Interfaz Web debe estar alojada en Microsoft Internet Information Services 6.0.

Cómo agregar el servidor de la Interfaz Web como Agent Host

Se debe crear un Agent Host para el servidor Web en la base de datos del servidor RSA ACE/Server para que el servidor RSA ACE/Server reconozca y acepte las solicitudes de autenticación provenientes del servidor Web. Cuando se crea Agent Host, se debe configurar la Interfaz Web como un Agente NetOS. El servidor RSA ACE/Server utiliza este parámetro para determinar el modo en que se produce la comunicación con la Interfaz Web.

Copia del archivo sdconf.rec

Localice el archivo sdconf.rec (o créelo, si es necesario) en el servidor RSA ACE/Server y cópielo en la carpeta \System32 del servidor de la Interfaz Web, que normalmente se encuentra en C:\Windows\System32. Este archivo proporciona a la Interfaz Web toda la información necesaria para establecer una conexión con el servidor RSA ACE/Server.

Habilitación de la autenticación RSA SecurID en la consola

Debe configurar la Interfaz Web para permitir que los usuarios usen la autenticación con RSA SecurID y puedan acceder a su conjunto de recursos y visualizarlos. Para ello, debe utilizar la tarea Métodos de autenticación de la consola Administración de la Interfaz Web de Citrix.

Uso de varios dominios con RSA SecurID

Si varias cuentas de usuario tienen el mismo nombre de usuario pero se ubican en distintos dominios de Windows, debe identificarlas en la base de datos del servidor RSA ACE/Server con un inicio de sesión predeterminado con la forma *DOMINIO\nombredeusuario* (a diferencia del nombre de usuario solamente) y utilizar la tarea Métodos de autenticación de la consola Administración de la Interfaz Web de Citrix para configurar la Interfaz Web de modo que envíe el dominio y el nombre de usuario al servidor RSA ACE/Server.

Habilitación de la integración de contraseñas de Windows en RSA SecurID

La Interfaz Web es compatible con la función de integración de contraseñas de Windows de RSA SecurID. Cuando esta función está habilitada, los usuarios de la Interfaz Web pueden iniciar sesión y acceder a los recursos con su código de acceso de SecurID. Los usuarios sólo necesitan indicar la contraseña de Windows la primera vez que se conectan a la Interfaz Web, o bien cuando tienen que cambiarla.

Para utilizar la función de integración de contraseñas de Windows de SecurID con la Interfaz Web para Microsoft Internet Information Services:

- El cliente de autenticación local RSA ACE/Agent para Windows debe estar instalado en el servidor Web (los administradores deben iniciar sesión en la Interfaz Web utilizando las credenciales de administrador local del servidor)
- La Interfaz Web debe instalarse después de instalar RSA ACE/Agent
- El servicio local sin conexión de RSA Authentication Agent debe estar ejecutándose en el servidor Web
- El Agent Host del servidor Web en la base de datos de RSA ACE/Server debe estar configurado para permitir la integración de contraseñas de Windows
- Los parámetros del sistema de la base de datos deben estar configurados de manera que la función de integración de contraseñas de Windows esté habilitada en el nivel del sistema

Para restablecer la clave de registro del secreto de nodo en el servidor Web

El secreto de nodo se utiliza para garantizar comunicaciones seguras entre la Interfaz Web y el servidor RSA ACE/Server.

Es posible que el secreto de nodo se desincronice entre los dos servidores en las situaciones siguientes:

- Cuando se vuelve a instalar la Interfaz Web
- Cuando se vuelve a instalar el servidor RSA ACE/Server
- Cuando se elimina y se vuelve a agregar el registro de Agent Host del servidor Web
- Cuando la clave de registro del secreto de nodo se elimina en el servidor Web
- Cuando la casilla de verificación Secreto de nodo creado no está marcada en el cuadro de diálogo Editar Agent Host en el servidor RSA ACE/Server

Si el secreto de nodo en el servidor de la Interfaz Web y el servidor RSA ACE/Server no coinciden, SecurID falla. Deberá reiniciarse el secreto de nodo en el servidor de la Interfaz Web y el servidor RSA ACE/Server.

Precaución: Si se usa el editor del Registro de forma incorrecta, pueden producirse problemas graves que derivarán en la necesidad de instalar nuevamente el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad.

1. Busque la siguiente clave en el Registro del sistema:
    - HKEY_LOCAL_MACHINE\SOFTWARE\SDTI\ACECLIENT en servidores de 32 bits
    - HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SDTI\ACECLIENT en servidores de 64 bits
2. Elimine la clave del secreto de nodo (NodeSecret).

Nota: La reinstalación de la Interfaz Web no elimina la clave NodeSecret. Si la entrada de Agent Host no se cambia en el servidor RSA ACE/Server, se puede volver a usar el secreto de nodo.

Habilitación de la autenticación RADIUS

Esta sección describe cómo instalar y configurar Aladdin SafeWord y RSA SecurID para presentarlos como servidores RADIUS. La autenticación RADIUS es la única opción de autenticación de dos factores disponible en la Interfaz Web para servidores de aplicaciones de Java.

Habilitación de RADIUS con SafeWord

Cuando instala el software de servidor SafeWord, instale también el agente IAS RADIUS.

Siga las instrucciones en pantalla para la instalación de los clientes RADIUS con el complemento de Servicio de autenticación de Internet (IAS) de Windows en la consola Microsoft Management Console. Es necesario configurar un nuevo cliente RADIUS para cada servidor de Interfaz Web que autentique usuarios con el servidor SafeWord.

Cada nuevo cliente RADIUS deberá contener la siguiente información:

- El nombre completo de dominio o la dirección IP del servidor de la Interfaz Web al que está asociado el cliente RADIUS.
- Un secreto conocido por el servidor de la Interfaz Web asociado.
- El tipo de cliente debe ser RADIUS standard.
- Para más seguridad, debe seleccionar la opción Request must contain the Message Authenticator attribute.

Creación de un secreto compartido para RADIUS

El protocolo RADIUS requiere el uso de un secreto compartido: información que sólo conoce el cliente RADIUS (es decir, la Interfaz Web) y el servidor RADIUS donde se realiza la autenticación. La Interfaz Web guarda este secreto compartido en un archivo de texto del sistema de archivos local. La ubicación de este archivo está determinada por el valor de configuración RADIUS_SECRET_PATH en el archivo web.config (para los sitios alojados en IIS) o el archivo web.xml (para los sitios alojados en servidores de aplicaciones de Java). La ubicación dada es relativa a la carpeta \conf para los sitios alojados en IIS, y relativa al directorio /WEB_INF para los sitios alojados en aplicaciones de Java.

Para crear el secreto compartido, cree un archivo de texto (con el nombre radius_secret.txt) que contenga una cadena. Mueva el archivo a la ubicación especificada en el archivo de configuración que corresponda y asegúrese de que el archivo tenga permisos bloqueados y sólo los usuarios o procesos autorizados tengan acceso a él.

Especificación de un identificador del servidor de acceso a red para RADIUS

El protocolo RADIUS requiere que las solicitudes de acceso a servidores RADIUS incluyan la dirección IP u otro identificador del cliente RADIUS (es decir, la Interfaz Web). Para activar la autenticación de RADIUS, debe proporcionar la dirección IP del servidor Web o especificar un valor para el atributo del identificador del servidor de acceso a red (NAS) RADIUS. El valor del atributo del identificador de NAS puede ser cualquier cadena que contenga tres caracteres o más. A pesar de que no es necesario que este atributo sea único para cada cliente RADIUS, establecer un identificador único para cada cliente puede ayudar a diagnosticar problemas de comunicación con RADIUS.

Para proporcionar una dirección IP del cliente RADIUS, ingrese la dirección IP del servidor Web como el valor del parámetro de configuración DIRECCIÓN_IP_RADIUS en el archivo web.config (para los sitios alojados en IIS) o en el archivo web.xml (para los sitios alojados en servidores de aplicaciones de Java). Para establecer el identificador de NAS para RADIUS, especifique un valor para IDENTIFICADOR_NAS_RADIUS en el archivo web.config o web.xml.

Habilitación de la autenticación RADIUS de dos factores mediante la consola

Debe habilitar la autenticación de dos factores en la Interfaz Web para que los usuarios puedan acceder a su conjunto de recursos. Para ello, debe utilizar la tarea Métodos de autenticación de la consola Administración de la Interfaz Web de Citrix. Además de habilitar la autenticación de dos factores, puede especificar una o varias direcciones (y, si lo desea, puertos) de servidores RADIUS, el equilibrio de carga o la conmutación por error de los servidores, y el tiempo de espera de respuesta.

Importante: al activar la autenticación RADIUS se debe también proporcionar la dirección IP del cliente RADIUS, o bien especificar un valor para el atributo de identificador de servidor de acceso RADIUS en el archivo web.config (IIS) o web.xml (servidores de aplicaciones de Java) del sitio.

Habilitación de RADIUS con SafeWord

Cuando instala el software de servidor SafeWord, instale también el agente IAS RADIUS.

Siga las instrucciones en pantalla para la instalación de los clientes RADIUS con el complemento de Servicio de autenticación de Internet (IAS) de Windows en la consola Microsoft Management Console. Es necesario configurar un nuevo cliente RADIUS para cada servidor de Interfaz Web que autentique usuarios con el servidor SafeWord.

Cada nuevo cliente RADIUS deberá contener la siguiente información:

- El nombre completo de dominio o la dirección IP del servidor de la Interfaz Web al que está asociado el cliente RADIUS.
- Un secreto conocido por el servidor de la Interfaz Web asociado. Para obtener más información, consulte Habilitación de la autenticación RADIUS.
- El tipo de cliente debe ser RADIUS standard.
- Para más seguridad, debe seleccionar la opción Request must contain the Message Authenticator attribute.

Habilitación de RADIUS con RSA SecurID

RADIUS se activa en RSA Authentication Manager mediante la herramienta de configuración de SecurID. Para obtener más información sobre esta herramienta, consulte la documentación de RSA Authentication Manager.

Cómo agregar la Interfaz Web y los servidores RADIUS como agentes de autenticación

Si el RSA Authentication Manager en el que se autentican los usuarios también actúa como servidor RADIUS, se debe crear un registro de Authentication Agent para el servidor RADIUS local en la base de datos de RSA Authentication Manager. Al crear este registro se debe indicar el nombre y la dirección IP del servidor local y configurar este servidor como NetOS Authentication Agent. El servidor local debe estar asignado como servidor activo.

Asimismo, se debe crear un registro de Authentication Agent para cada servidor de la Interfaz Web en la base de datos de RSA Authentication Manager para que RSA Authentication Manager reconozca y acepte las solicitudes de autenticación de la Interfaz Web a través del servidor RADIUS. Al crear un registro de Authentication Agent, se debe configurar la Interfaz Web como servidor de comunicación y establecer la clave de cifrado en el valor del secreto compartido con la Interfaz Web.

Uso de RADIUS Challenge Mode

De forma predeterminada, el servidor RADIUS de SecurID está en *RADIUS Challenge Mode* (modo de desafío). En este modo:

- La Interfaz Web muestra una pantalla de mensaje de desafío genérica, un cuadro HTML de contraseña y los botones Aceptar y Cancelar.
- Los mensajes de desafío no están traducidos en la Interfaz Web. Aparecen en el idioma de los mensajes de desafío definidos en el servidor RADIUS de SecurID.

Si los usuarios no envían una respuesta (por ejemplo, si hacen clic en Cancelar), regresarán a la pantalla de Inicio de sesión.

Citrix recomienda utilizar este modo únicamente si hay otros componentes o productos del software, además de la Interfaz Web, que utilizan el servidor RADIUS para la autenticación.

Uso de mensajes de desafío personalizados

Puede configurar mensajes de desafío personalizados para el servidor RADIUS de SecurID. Cuando se usan mensajes personalizados reconocidos por la Interfaz Web, el servidor RADIUS puede presentar páginas de interfaz de usuario idénticas a las mostradas por la Interfaz Web para Microsoft Internet Information Services, y estas páginas están traducidas en varios idiomas.

Esta función requiere cambios en la configuración del servidor RADIUS y sólo debe implementarse si este servidor se usa para autenticar únicamente usuarios de la Interfaz Web.

Puede modificar los mensajes de desafío ejecutando la utilidad de configuración de RSA RADIUS. Para obtener más información sobre el uso de esta herramienta, consulte la documentación del software SecurID. Para mostrar los mismos mensajes a usuarios que acceden a sitios en IIS y en servidores de aplicaciones de Java, deben actualizarse los siguientes desafíos:

Contenido de mensaje	Paquete	Valor actualizado
¿El usuario desea un PIN del sistema?	Desafío	CHANGE_PIN_EITHER
¿El usuario está listo para obtener PIN del sistema?	Desafío	SYSTEM_PIN_READY
¿El usuario está satisfecho con el PIN del sistema?	Desafío	CHANGE_PIN_SYSTEM_[%s]
Nuevo PIN numérico de extensión fija	Desafío	CHANGE_PIN_USER
Nuevo PIN alfanumérico de extensión fija	Desafío	CHANGE_PIN_USER
Nuevo PIN numérico de extensión variable	Desafío	CHANGE_PIN_USER
Nuevo PIN alfanumérico de extensión variable	Desafío	CHANGE_PIN_USER
Nuevo PIN aceptado	Desafío	SUCCESS
Ingrese Sí o No	Desafío	FAILURE
Se requiere siguiente código de token	Desafío	NEXT_TOKENCODE

Administración de clientes

Esta sección ofrece información sobre cómo instalar y usar los clientes Citrix con la Interfaz Web. También se explica cómo configurar el acceso seguro.

Clientes para recursos en línea

Para acceder a los recursos en línea se pueden usar los siguientes clientes Citrix:

- **Cliente nativo.** Los administradores instalan el cliente nativo apropiado en los dispositivos de los usuarios. Por otro lado, los usuarios que no tienen un cliente nativo pueden descargar e instalar web Citrix Online Plug-In mediante el proceso de detección e instalación de clientes. Se respalda el uso de ventanas integradas; los recursos se abren en ventanas del escritorio cuyo tamaño puede modificarse. Si los usuarios accederán a los recursos desde dispositivos PDA, se debe habilitar el cliente nativo.

- **Cliente para Java:** Los usuarios ejecutan el Cliente para Java cuando se accede al recurso. Por lo general, este cliente se utiliza en los casos en que los usuarios no tienen instalado un cliente nativo y no pueden descargar e instalar Citrix Online Plug-In – Web o la configuración de los dispositivos o el sitio Web XenApp no se los permite. El Cliente para Java respalda el uso de ventanas integradas; los recursos se abren en ventanas del escritorio cuyo tamaño puede modificarse.

- **Software incrustado de Conexión a escritorio remoto (RDP):** Si ha habilitado esta opción, los usuarios pueden usar el software de Conexión a escritorio remoto (RDP) que ya está instalado como parte del sistema operativo Windows. El proceso de detección e instalación de clientes no pone el software de Conexión a escritorio remoto (RDP) a disposición de los usuarios que no lo tienen instalado. No se respalda el uso de ventanas integradas; los recursos se abren incrustados en ventanas del explorador.

  Nota: El Cliente para Java y el software incrustado de Conexión a escritorio remoto (RDP) no son compatibles con dispositivos que ejecutan Windows CE o Windows Mobile. El Cliente para Java y el software incrustado de Conexión a escritorio remoto (RDP) no están respaldados para ser utilizados con sitios integrados con AD FS.

Configuración de Citrix Online Plug-in

Con Citrix Online Plug-in, los usuarios pueden acceder a aplicaciones, contenido y escritorios virtuales directamente desde el escritorio físico de Windows, sin necesidad de usar un explorador Web. Es posible la configuración remota de la ubicación de enlaces a recursos en el menú Inicio, en el escritorio de Windows o en el área de notificación de Windows. La interfaz de usuario de Citrix Online Plug-in también se puede "bloquear" para evitar que el usuario realice una configuración errónea. Puede utilizar la consola Administración de la Interfaz Web de Citrix o el archivo config.xml para configurar Citrix online plug-in.

Uso de la consola Administración de la Interfaz Web de Citrix para la configuración

Citrix Online Plug-in está configurado con opciones de presentación, métodos de autenticación y opciones de conexión a servidor predeterminadas. La consola Administración de la Interfaz Web de Citrix permite modificar los parámetros predeterminados para impedir que los usuarios cambien opciones específicas.

Uso de los archivos de configuración

También puede configurar Citrix Online Plug-in mediante los archivos config.xml y WebInterface.conf. Estos archivos se encuentran normalmente en el directorio C:\inetpub\wwwroot\Citrix\PNAgent\conf en el servidor de la Interfaz Web.

Administración de archivos de configuración de plug-ins

Las opciones de Citrix Online Plug-in configuradas en la consola se guardan en un archivo de configuración en el servidor de la Interfaz Web. El archivo de configuración controla los parámetros que aparecen como opciones en el cuadro de diálogo Opciones de Citrix Online Plug-In del usuario. Los usuarios pueden elegir entre las opciones disponibles para establecer las preferencias aplicables a las sesiones ICA, entre ellas, el modo de inicio de sesión, el tamaño de pantalla, la calidad de sonido y las ubicaciones de los enlaces a los recursos.

Para los sitios nuevos se instala un archivo de configuración estándar, config.xml, con parámetros predeterminados, listo para usar sin necesidad de modificación en la mayoría de los entornos de red. El archivo config.xml se almacena en la carpeta \conf del sitio.

Copia de los archivos de instalación de clientes en la Interfaz Web

Para usar la instalación de clientes basada en la Web, los archivos de instalación de los clientes deben estar disponibles en el servidor de la Interfaz Web.

Durante la instalación de la Interfaz Web, el programa de instalación pide acceso al soporte de instalación de XenApp o XenDesktop. En IIS, el programa de instalación copia el contenido de la carpeta \Citrix Receiver and Plug-ins del disco de instalación en una carpeta denominada \Clients en el directorio raíz (por ejemplo, C:\Archivos de programa (x86)\Citrix\Web Interface*Version*\Clients). En los servidores de aplicaciones de Java, el programa de instalación copia los clientes Citrix del soporte de instalación y los empaqueta en un archivo .war.

Si no copió los archivos de instalación de los clientes en el servidor Web durante la instalación de la Interfaz Web, asegúrese de copiarlos en el servidor Web antes de utilizar la instalación de clientes basada en la Web; por ejemplo, puede copiar los archivos desde la carpeta Citrix Receiver and Plug-ins/Windows. Si no está disponible el soporte de instalación de XenApp o XenDesktop, se debe recrear en forma manual la estructura de directorio requerida y luego descargar los clientes necesarios del sitio Web de Citrix.

De forma predeterminada, la Interfaz Web asume que los nombres de archivo de los archivos de instalación de clientes son los mismos que los archivos suministrados en el soporte de instalación de XenApp o XenDesktop. Si descarga clientes del sitio Web de Citrix o si planea distribuir clientes anteriores, verifique que los nombres de los archivos de instalación de clientes estén especificados en los archivos de configuración de sus sitios Web XenApp.

Para copiar los archivos de clientes en la Interfaz Web en Microsoft Internet Information Services

1. Busque la carpeta \Clients en la instalación de la Interfaz Web; por ejemplo: C:\Archivos de programa (x86)\Citrix\Web Interface*Version*\Clients.

2. Introduzca el soporte de instalación en la unidad óptica del servidor Web o busque en la red una imagen de uso compartido del soporte de instalación.

3. Busque la carpeta \Citrix Receiver and Plug-ins en el disco de instalación. Copie el contenido de la carpeta del disco de instalación en la carpeta \Clients del servidor de la Interfaz Web. Asegúrese de copiar solamente el *contenido* de la carpeta y no la carpeta \Citrix Receiver and Plug-ins propiamente dicha.

   Si no está disponible el soporte de instalación de XenApp o XenDesktop, se debe volver a crear manualmente la estructura de directorio siguiente y luego descargar los clientes necesarios del sitio Web de Citrix.

   C:\Archivos de programa (x86)\Citrix\Web Interface*Versión*\Clients

   - \de
     - \Unix

       Coloque en esta carpeta los archivos de instalación de Clientes para UNIX (solaris.tar.Z, sol86.tar.Z) con respaldo para alemán.
   - \en
     - \Unix

       Coloque en esta carpeta los archivos de instalación de Clientes para UNIX (solaris.tar.Z, sol86.tar.Z) con respaldo para inglés.
   - \es
     - \Unix

       Coloque en esta carpeta los archivos de instalación de Clientes para UNIX (solaris.tar.Z, sol86.tar.Z) con respaldo para español.
   - \fr
     - \Unix

       Coloque en esta carpeta los archivos de instalación de Clientes para UNIX (solaris.tar.Z, sol86.tar.Z) con respaldo para francés.
   - \ja
     - \Unix

Coloque en esta carpeta los archivos de instalación de Clientes para UNIX (solaris.tar.Z, sol86.tar.Z) con respaldo para japonés.

- \Java

  Coloque en esta carpeta los archivos de Cliente para Java.

- \Linux

  Coloque en esta carpeta el archivo de instalación de Citrix Receiver para Linux (linuxx86-*Versión*.tar.gz).

- \Mac

  - \Web Online Plug-in

    Coloque en esta carpeta el archivo de instalación de Citrix online plug-in para Web para Macintosh {Citrix online plug-in (web).dmg}.

- \Windows

  - \Offline Plug-in

    Coloque en esta carpeta el archivo de instalación de Citrix offline plug-in (CitrixOfflinePlugin.exe).

  - \Online Plug-in

    Coloque en esta carpeta el archivo de instalación de Citrix online plug-in para Web (CitrixOnlinePluginWeb.exe).

De forma predeterminada, la Interfaz Web asume que los nombres de archivo de los archivos de instalación de clientes son los mismos que los archivos suministrados en el soporte de instalación de XenApp o XenDesktop. Si descarga clientes del sitio Web de Citrix o si planea distribuir clientes anteriores, verifique que los nombres de los archivos de instalación de clientes estén especificados para los parámetros ClientIcaLinuxX86, ClientIcaMac, ClientIcaSolarisSparc, ClientIcaSolarisX86, ClientIcaWin32 y ClientStreamingWin32 en los archivos de configuración de los sitios Web XenApp.

Después de copiar los archivos de instalación en la estructura de directorio anterior, cualquier sitio Web XenApp que se configure para la instalación de clientes basada en la Web ofrecerá automáticamente los clientes a los usuarios que requieran uno.

Para copiar los archivos de clientes en la Interfaz Web en servidores de aplicaciones de Java

1. En el archivo .war descomprimido del sitio, busque el directorio /Clients.

2. Introduzca el soporte de instalación en la unidad óptica del servidor Web o busque en la red una imagen de uso compartido del soporte de instalación.

3. Cambie los directorios al directorio /Citrix Receiver and Plug-ins en el disco de instalación. Copie el contenido del directorio del disco de instalación en el directorio /Clients del servidor de la Interfaz Web. Asegúrese de copiar solamente el *contenido* del directorio y no el directorio /Citrix Receiver and Plug-ins propiamente dicho.

   Si no está disponible el soporte de instalación de XenApp o XenDesktop, se debe volver a crear manualmente la estructura de directorio siguiente y luego descargar los clientes necesarios del sitio Web de Citrix.

   RaízSitioWebXenApp/Clients

   - /de
     - /Unix

       Coloque en este directorio los archivos de instalación de Clientes para UNIX (solaris.tar.Z, sol86.tar.Z) con respaldo para alemán.
   - /en
     - /Unix

       Coloque en este directorio los archivos de instalación de Clientes para UNIX (solaris.tar.Z, sol86.tar.Z) con respaldo para inglés.
   - /es
     - /Unix

       Coloque en este directorio los archivos de instalación de Clientes para UNIX (solaris.tar.Z, sol86.tar.Z) con respaldo para español.
   - /fr
     - /Unix

       Coloque en este directorio los archivos de instalación de Clientes para UNIX (solaris.tar.Z, sol86.tar.Z) con respaldo para francés.
   - /ja
     - /Unix

Coloque en este directorio los archivos de instalación de Clientes para UNIX (solaris.tar.Z, sol86.tar.Z) con respaldo para japonés.

- /Java

  Coloque en este directorio los archivos de Cliente para Java.

- /Linux

  Coloque en este directorio el archivo de instalación de Citrix Receiver para Linux (linuxx86-*Versión*.tar.gz).

- /Mac

  - /Web Online Plug-in

    Coloque en este directorio el archivo de instalación de Citrix online plug-in para Web para Macintosh {Citrix online plug-in (web).dmg}.

- /Windows

  - /Offline Plug-in

    Coloque en este directorio el archivo de instalación de Citrix offline plug-in (CitrixOfflinePlugin.exe).

  - /Online Plug-in

    Coloque en este directorio el archivo de instalación de Citrix online plug-in para Web (CitrixOnlinePluginWeb.exe).

De forma predeterminada, la Interfaz Web asume que los nombres de archivo de los archivos de instalación de clientes son los mismos que los archivos suministrados en el soporte de instalación de XenApp o XenDesktop. Si descarga clientes del sitio Web de Citrix o si planea distribuir clientes anteriores, verifique que los nombres de los archivos de instalación de clientes estén especificados para los parámetros ClientIcaLinuxX86, ClientIcaMac, ClientIcaSolarisSparc, ClientIcaSolarisX86, ClientIcaWin32 y ClientStreamingWin32 en los archivos de configuración de los sitios Web XenApp.

4. Después de copiar los archivos de instalación en la estructura de directorio anterior, reinicie el servidor Web. Si ha configurado el sitio Web XenApp para la instalación de clientes basada en la Web, se ofrecerán los clientes a los usuarios que requieran uno.

Configuración de los mensajes de instalación y distribución de clientes

La Interfaz Web ofrece un proceso de detección e instalación de clientes que detecta los clientes Citrix que pueden instalarse en el entorno del usuario y luego, guía a los usuarios a lo largo del proceso de instalación, incluida la reconfiguración del explorador Web, si es necesario.

Puede permitir a los usuarios el acceso al proceso de detección e instalación de clientes de tres formas:

- Puede configurar el proceso de detección e instalación de clientes para que se ejecute automáticamente cuando los usuarios accedan a un sitio Web XenApp. El proceso de instalación y detección de clientes se inicia automáticamente. Esto permite que los usuarios identifiquen e instalen el cliente Citrix adecuado para obtener acceso a sus recursos. En algunos entornos, el proceso de detección e instalación de clientes también puede detectar la presencia o la ausencia de un cliente instalado, y solicitarle al usuario una instalación solo cuando sea necesario.

- Puede permitir que los usuarios especifiquen su cliente preferido para acceder a los recursos en línea. En este caso, se agrega el botón Ejecutar detección de clientes a la pantalla Configuración para que los usuarios puedan iniciar el proceso de instalación y detección de clientes de forma manual.

- Puede presentar mensajes de instalación a los usuarios; estos son enlaces que los usuarios ven en su pantalla Mensajes. Los usuarios hacen clic en el enlace para iniciar el proceso de detección e instalación de clientes.

Cuando un usuario accede a un sitio Web XenApp, el proceso de detección e instalación de clientes basado en la Web intenta determinar si el cliente Citrix de preferencias está instalado en el equipo del usuario. Antes de que el usuario inicie sesión en un sitio Web de XenApp configurado para la instalación y la detección automática de clientes, el proceso se inicia automáticamente y guía al usuario a través de los pasos para identificar e instalar un cliente Citrix adecuado que le permita obtener acceso a sus recursos, lo que incluye en determinados casos, la modificación de la configuración de su explorador Web.

Los usuarios también pueden acceder al proceso de detección e instalación de clientes mediante los enlaces que aparecen en la pantalla Mensajes. Los usuarios hacen clic en el enlace para iniciar el proceso de detección e instalación de clientes. Estos enlaces se denominan *mensajes de instalación*.

Se pueden proporcionar mensajes de instalación para los usuarios que no tengan un cliente adecuado; también se pueden utilizar para permitir a los usuarios acceder al proceso de detección e instalación de clientes para actualizar los clientes Citrix a una versión más reciente o a un tipo alternativo de clientes que ofrezca mayor funcionalidad.

Utilice la tarea Distribución de clientes de la consola Administración de la Interfaz Web de Citrix para especificar en qué circunstancias los usuarios pueden acceder al proceso de detección e instalación de clientes.

Para configurar los mensajes de instalación y distribución de clientes

1. En el menú Inicio de Windows, haga clic en Todos los programas > Citrix > Management Consoles > Citrix Web Interface Management.

2. En el panel izquierdo de la consola Administración de la Interfaz Web de Citrix, haga clic en Sitios Web XenApp y seleccione el sitio en el panel de resultados.

3. En el panel Acción, haga clic en Distribución de clientes. Para los sitios que solo ofrecen aplicaciones en línea, seleccione la casilla de verificación Cliente nativo y haga clic en Propiedades.

4. Haga clic en Detección de clientes.

5. Si desea que el proceso de instalación y detección de clientes se inicie automáticamente cuando los usuarios que no posean un cliente Citrix adecuado obtengan acceso al sitio Web de XenApp, seleccione la casilla de verificación Detectar clientes al iniciar la sesión.

6. Para solicitar a los usuarios que actualicen los clientes cuando el proceso de detección e instalación de clientes detecte la existencia de nuevas versiones disponibles para descargar desde el sitio Web de XenApp, seleccione la casilla de verificación Ofrecer actualizaciones para clientes.

7. Especifique cuándo se mostrarán mensajes de instalación a los usuarios, seleccionando una de las opciones siguientes:

   - Para notificar al usuario si no se puede detectar ningún cliente adecuado, o si hay disponible un cliente más apropiado, seleccione Siempre que se necesite un cliente. Esta es la opción predeterminada.

   - Para notificar al usuario sólo si no se detecta ningún cliente adecuado, seleccione Sólo si no se puede acceder a los recursos.

   - Si no desea mostrar mensajes de instalación en ningún caso, seleccione Nunca.

Configuración de la firma de archivos ICA

La Interfaz Web permite firmar digitalmente los archivos ICA generados mediante un certificado seleccionado, para que los clientes ICA compatibles puedan corroborar que los archivos provienen de su organización.

Para utilizar la función Firma de archivos ICA, se requieren los siguientes componentes:

- Interfaz Web 5.4 o una versión posterior
- Merchandising Server 1.2 o una versión posterior (para un entorno no administrado de directivas de seguridad de clientes)
- Objetos de directivas de grupos para un entorno administrado de directivas de seguridad de clientes
- Formato de archivo de plantilla administrativa para Windows Server 2003 o una versión posterior

Citrix recomienda que (en orden de prioridad):

- Adquiera un certificado de firma de código o un certificado de firma SSL emitido por una autoridad de certificación pública (como Verisign).
- Si la empresa ya dispone de una autoridad de certificación privada, cree un certificado de firma de código o un certificado de firma SSL mediante la autoridad de certificación privada.
- Utilice un certificado SSL existente, como el certificado de servidor de Dazzle o de la Interfaz Web.
- Cree una nueva autoridad de certificación raíz y distribúyala entre los clientes mediante los objetos de directivas de grupos.

El certificado debe cumplir con los siguientes requisitos:

- El certificado debe incluir una clave privada.
- El certificado no debe tener fecha de caducidad.
- Se debe cumplir una de las siguientes condiciones:
    - El certificado no incluye un campo de uso de la clave o de uso de la clave mejorado.
    - El campo de uso de la clave permite utilizar la clave para las firmas digitales.
    - El campo de uso de la clave mejorado se establece en Firma de código o Autenticación de servidor.

La Interfaz Web firma los archivos ICA mediante el algoritmo hash SHA-1 o SHA-256. El algoritmo hash SHA-256 es más nuevo y más seguro pero solo es compatible con los

servidores que ejecuten Windows 2008 o una versión posterior y clientes que ejecuten Windows Vista o una versión posterior. El algoritmo hash SHA-1 se puede utilizar en todos los servidores y los sistemas operativos compatibles del cliente.

La firma de archivos ICA no se puede utilizar en el cliente para Java, el cliente RDP, el cliente Citrix Streaming ni en los documentos publicados que se descarguen de redes compartidas.

Para activar la función de firma de archivos ICA, el sitio debe configurarse de manera que se utilice el cliente nativo (para mostrar las aplicaciones en línea) y EnableLegacyIcaClientSupport debe establecerse en Off en el archivo Webinterface.conf.

Para obtener más información sobre cómo activar la firma de archivos ICA para Citrix Online Plug-in, consulte la documentación de Citrix Merchandising Server.

Para activar la firma de archivos ICA en Web Interface Management Console

1. En el menú Inicio de Windows, haga clic en Todos los programas > Citrix > Management Consoles > Citrix Web Interface Management.
2. En el panel izquierdo de la consola Administración de la Interfaz Web de Citrix, haga clic en Sitios Web XenApp y seleccione el sitio en el panel de resultados.
3. En el panel Acción, haga clic en Distribución de clientes.
4. Haga clic en Firma de archivos ICA.
5. Seleccione Activar firma de archivos ICA y seleccione un certificado del menú desplegable. Si el certificado requerido no figura en la lista, haga clic en Importar para importar un certificado al almacén de certificados personal.
6. Si ejecuta Windows 2008 o una versión posterior, puede seleccionar el tipo de algoritmo hash que desea utilizar. De lo contrario, se utilizará SHA-1. Después de configurar la firma de archivos ICA en Windows 2003, deberá reiniciar el equipo.

Configuración de la supervisión de la sesión de streaming

Puede utilizar la tarea Distribución de clientes de la consola Administración de la Interfaz Web de Citrix para configurar la Interfaz Web para que proporcione información sobre las sesiones de usuario al administrador Citrix. La Interfaz Web suministra esta información por medio de la URL de sesión, que habilita la comunicación con Citrix Offline Plug-in. En la mayoría de los casos, esta URL se detecta automáticamente. No obstante, puede ser necesario configurarla manualmente; por ejemplo, si se utiliza un proxy en el lado del cliente.

Puede usar Delivery Services Console para ver la información de sesión. Puede acceder a la información de todas las sesiones de usuarios en varias comunidades, aplicaciones específicas, sesiones que se conectan a un servidor determinado, o sesiones y aplicaciones de un usuario específico.

Para configurar la supervisión de la sesión de Streaming

1. En el menú Inicio de Windows, haga clic en Todos los programas > Citrix > Management Consoles > Citrix Web Interface Management.

2. En el panel izquierdo de la consola Administración de la Interfaz Web de Citrix, haga clic en Sitios Web XenApp y seleccione el sitio en el panel de resultados.

3. En el panel Acción, haga clic en Distribución de clientes.

4. Haga clic en Citrix Offline Plug-in.

5. Seleccione la forma en que la Interfaz Web se debe comunicar con Citrix Offline Plug-in. Elija una de las siguientes opciones:

   - Para detectar automáticamente la dirección URL de sesión utilizada para comunicarse con el plug-in, seleccione Detectar automáticamente la URL de la sesión.

   - Para establecer la dirección URL de sesión manualmente, seleccione Especificar la URL de sesión e introduzca los detalles de la URL

Distribución del software de Conexión a escritorio remoto

La funcionalidad de Conexión a escritorio remoto (RDP) está disponible en los sistemas Windows de 32 bits que ejecutan Internet Explorer. Los usuarios que tengan instalada la versión 6.0 (incluida en Windows XP con Service Pack 3) o una versión posterior del software de Conexión a escritorio remoto (RDP) de Microsoft pueden usarla para acceder a los recursos. Si los usuarios no pueden usar ningún otro cliente, el proceso de detección e implementación de clientes comprueba si el software de Conexión a escritorio remoto (RDP) está disponible y ayuda a los usuarios a habilitar el control ActiveX de Terminal Services, si es necesario. La opción de utilizar el software de Conexión a escritorio remoto (RDP) solo está disponible para los sitios que ofrecen únicamente aplicaciones en línea.

Nota: Si Internet Explorer no coloca el sitio Web XenApp en la zona de Intranet local o de Sitios de confianza, aparecerá un mensaje de error. El proceso de detección e implementación de clientes de la Interfaz Web proporciona instrucciones a los usuarios sobre cómo incorporar el sitio a la zona de seguridad de Windows pertinente.

Distribución del Cliente para Java

Si va a distribuir clientes Citrix por medio de una red con poco ancho de banda, o no está seguro de las plataformas que utilizan los usuarios, considere utilizar el Cliente para Java. El Cliente para Java es un applet que funciona en diversas plataformas, y el servidor de la Interfaz Web puede distribuirlo a cualquier explorador Web compatible con Java.

Dado que el Cliente para Java ofrece el mayor respaldo en términos de entornos de usuario, dispositivos, sistemas operativos y exploradores Web, se puede utilizar como sistema de soporte para los casos en que no se puede utilizar un cliente nativo. El proceso de detección e instalación de clientes puede configurarse para ofrecer el Cliente para Java a los usuarios que no tengan instalado un cliente nativo o que no puedan descargar e instalar un cliente desde el sitio Web XenApp.

Debe asegurarse de que el Cliente para Java esté disponible en el directorio \Clients del sitio Web XenApp para que pueda ser distribuido a los usuarios que lo necesiten.

Para configurar el uso automático del Cliente para Java

1. En el menú Inicio de Windows, haga clic en Todos los programas > Citrix > Management Consoles > Citrix Web Interface Management.

2. En el panel izquierdo de la consola Administración de la Interfaz Web de Citrix, haga clic en Sitios Web XenApp y seleccione el sitio en el panel de resultados.

3. En el panel Acción, haga clic en Distribución de clientes. Para los sitios que solo ofrecen aplicaciones en línea, seleccione la casilla de verificación Cliente nativo y haga clic en Propiedades.

   Nota: Para ofrecer el uso automático del Cliente para Java, no es necesario poner éste a disposición de los usuarios.

4. Haga clic en Comportamiento en caso de fallo.

5. Especifique las circunstancias en las cuales se ofrecerá el Cliente para Java a los usuarios que no cuenten con un cliente nativo. Para ello, seleccione una de las siguientes opciones:

   - Si desea que los usuarios que no tienen un cliente nativo descarguen e instalen un cliente Citrix adecuado, seleccione Instalar cliente nativo. Esta es la opción predeterminada.

   - Si desea ofrecer el Cliente para Java a los usuarios que no cuenten con un cliente nativo y que solo se les solicite descargar e instalar un cliente nativo si no pueden usar el Cliente para Java, seleccione Instalar un cliente nativo y permitir al usuario elegir entre éste y el Cliente para Java.

   - Si desea solicitarles a los usuarios que no cuenten con un cliente nativo que descarguen e instalen un cliente adecuado, además de ofrecerles el Cliente para Java, seleccione En caso de fallo, recurrir al Cliente para Java automáticamente.

Personalización de la distribución del Cliente para Java

Puede configurar los componentes incluidos en la distribución del Cliente para Java.

El tamaño del Cliente para Java está determinado por los paquetes que usted incluya. Cuantos menos paquetes se seleccionen, menor será el tamaño (el mínimo es 540 KB). Si desea limitar el tamaño del Cliente para Java para aquellos usuarios que disponen de conexiones con poco ancho de banda, distribuya sólo un conjunto mínimo de componentes. También puede dejar que sean los usuarios quienes seleccionen qué componentes necesitan. Para obtener más información sobre el Cliente para Java y sus componentes, consulte la documentación del Cliente para Java.

Nota: Algunos componentes disponibles en el Cliente para Java pueden requerir una configuración adicional en los dispositivos de los usuarios o en el servidor.

Esta tabla explica las opciones disponibles:

Paquete	Description
Sonido	Permite que los recursos que se ejecutan en el servidor reproduzcan sonidos por medio de los dispositivos de audio instalados en los equipos de los usuarios. Es posible controlar la cantidad de ancho de banda utilizada por la asignación de sonido del cliente en el servidor. Para obtener más información, consulte Administración de XenApp.
Portapapeles	Permite a los usuarios copiar texto y gráficos entre las aplicaciones y los recursos en línea que se ejecutan localmente en los dispositivos.
Repetición local del texto	Acelera la presentación del texto introducido en los dispositivos de los usuarios.
SSL/TLS	Protege las comunicaciones usando Secure Sockets Layer (SSL) y Transport Layer Security (TLS). SSL/TLS proporciona autenticación de servidores, cifrado del flujo de datos y comprobación de la integridad de los mensajes.
Cifrado	Proporciona cifrado de alta seguridad para aumentar la privacidad de las conexiones de los clientes Citrix.

Asignación de unidades del cliente	Permite a los usuarios acceder a sus unidades locales desde la sesión. Cuando los usuarios se conectan con el servidor, sus unidades cliente (disquetes, unidades de red y unidades ópticas) se montan automáticamente. Los usuarios pueden acceder a los archivos almacenados localmente, trabajar con ellos durante sus sesiones y guardarlos nuevamente en una unidad local o en una unidad del servidor. Para activar este parámetro, los usuarios también deben configurar la asignación de unidades del cliente en el cuadro de diálogo Configuración del Cliente para Java. Para obtener más información, consulte la documentación del Cliente para Java.
Asignación de impresoras	Permite a los usuarios imprimir en sus impresoras locales o de red desde la sesión.
Interfaz de configuración	Activa el cuadro de diálogo Configuración del Cliente para Java. Los usuarios utilizan este cuadro de diálogo para configurar el Cliente para Java.

Uso de certificados raíz privados con el Cliente para Java versión 9.x

Si ha configurado Secure Gateway o el Traspaso SSL con un certificado de servidor obtenido de una entidad emisora de certificados privados (por ejemplo, si emite sus propios certificados con Servicios de certificados de Microsoft), debe importar el certificado raíz al almacén de claves de Java en cada dispositivo de usuario. Para obtener más información, consulte la documentación del Cliente para Java.

Administración del acceso seguro

Todos los sitios nuevos de la Interfaz Web están configurados de manera predeterminada para acceso directo, lo que implica que la dirección real del servidor Citrix es la dirección que se entrega a todos los clientes Citrix. No obstante, si utiliza Access Gateway, Secure Gateway o un servidor de seguridad en su entorno, puede usar la tarea Acceso seguro de la consola Administración de la Interfaz Web de Citrix para configurar la Interfaz Web para incluir los parámetros adecuados. También puede configurar diferentes métodos de acceso para diferentes grupos de usuarios. Por ejemplo, los usuarios internos que inician sesiones en la red LAN de la organización pueden configurarse con un tipo de acceso directo, mientras que los usuarios externos que inician sesiones a través de Internet pueden acceder a la Interfaz Web mediante Access Gateway.

En esta sección, se explica cómo usar la tarea Acceso seguro para especificar parámetros de acceso, modificar traducciones de direcciones y configurar parámetros de puerta de enlace.

Para configurar rutas directas de acceso

Si desea proporcionar la dirección real del servidor Citrix a un determinado conjunto de clientes Citrix, puede especificar las máscaras de red y direcciones de dispositivos de usuarios mediante la tarea Acceso seguro de la consola Administración de la Interfaz Web de Citrix.

1. En el menú Inicio de Windows, haga clic en Todos los programas > Citrix > Management Consoles > Citrix Web Interface Management.

2. En el panel izquierdo de la consola Administración de la Interfaz Web de Citrix, haga clic en Sitios Web XenApp o Sitios de servicios XenApp, según corresponda, y seleccione el sitio en el panel de resultados.

3. En el panel Acción, haga clic en Acceso seguro.

4. En la página Especificar métodos de acceso, haga clic en Agregar para agregar una nueva ruta de acceso o seleccione una entrada en la lista y haga clic en Modificar para cambiar una ruta existente.

5. En la lista Método de acceso, seleccione Directa.

6. Introduzca la dirección de red y la máscara de subred que identifican a la red de cliente.

7. Use los botones Subir y Bajar para colocar las rutas de acceso según el orden de prioridad en la tabla Direcciones de dispositivos de usuarios.

Para configurar parámetros de dirección alternativa

Si desea proporcionar la dirección alternativa del servidor Citrix a un determinado conjunto de clientes Citrix, puede especificar las máscaras de red y direcciones de dispositivos de usuarios mediante la tarea Acceso seguro de la consola Administración de la Interfaz Web de Citrix. El servidor debe configurarse con una dirección alternativa y el servidor de seguridad debe configurarse para la traducción de direcciones de red.

Nota: No se puede acceder a los escritorios virtuales de XenDesktop si se utilizan direcciones alternativas.

1. En el menú Inicio de Windows, haga clic en Todos los programas > Citrix > Management Consoles > Citrix Web Interface Management.
2. En el panel izquierdo de la consola Administración de la Interfaz Web de Citrix, haga clic en Sitios Web XenApp o Sitios de servicios XenApp, según corresponda, y seleccione el sitio en el panel de resultados.
3. En el panel Acción, haga clic en Acceso seguro.
4. En la página Especificar métodos de acceso, haga clic en Agregar para agregar una nueva ruta de acceso o seleccione una entrada en la lista y haga clic en Modificar para cambiar una ruta existente.
5. En la lista Método de acceso, seleccione Alternativa.
6. Introduzca la dirección de red y la máscara de subred que identifican a la red de cliente.
7. Use los botones Subir y Bajar para colocar las rutas de acceso según el orden de prioridad en la tabla Direcciones de dispositivos de usuarios.

Para configurar la traducción de direcciones en los servidores de seguridad internos

Si usa un servidor de seguridad o firewall en su entorno, puede usar la Interfaz Web para definir asignaciones desde direcciones internas a direcciones y puertos externos. Por ejemplo, si el servidor Citrix no se ha configurado con una dirección alternativa, puede configurar la Interfaz Web para proporcionarle una dirección alternativa al cliente Citrix. Para ello, debe utilizar la tarea Acceso seguro de la consola Administración de la Interfaz Web de Citrix.

1. En el menú Inicio de Windows, haga clic en Todos los programas > Citrix > Management Consoles > Citrix Web Interface Management.

2. En el panel izquierdo de la consola Administración de la Interfaz Web de Citrix, haga clic en Sitios Web XenApp o Sitios de servicios XenApp, según corresponda, y seleccione el sitio en el panel de resultados.

3. En el panel Acción, haga clic en Acceso seguro.

4. En la página Especificar métodos de acceso, haga clic en Agregar para agregar una nueva ruta de acceso o seleccione una entrada en la lista y haga clic en Modificar para cambiar una ruta existente.

5. En la lista Método de acceso, seleccione Traducida.

6. Introduzca la dirección de red y la máscara de subred que identifican a la red de cliente. Use los botones Subir y Bajar para colocar las rutas de acceso según el orden de prioridad en la tabla Direcciones de dispositivos de usuarios y haga clic en Siguiente.

7. En la página Especificar traducción de direcciones, haga clic en Agregar para agregar una nueva traducción de direcciones o seleccione una entrada en la lista y haga clic en Modificar para cambiar una traducción de direcciones existente.

8. En la sección Tipo de acceso, seleccione una de las opciones siguientes:

   - Si desea que el cliente Citrix use la dirección traducida para conectarse con el servidor Citrix, seleccione Traducción de rutas de dispositivos de usuarios.

   - Si ya ha configurado la ruta traducida de la puerta de enlace en la tabla Direcciones de dispositivos de usuarios y desea que tanto el cliente como el servidor de puerta de enlace utilicen la dirección traducida para conectarse con el servidor Citrix, seleccione Traducción de rutas de dispositivos de usuarios y puertas de enlace.

9. Introduzca las direcciones y los puertos internos y externos (traducidos) para el servidor Citrix. Los clientes que se conecten con el servidor usan la dirección y el número de puerto externos. Asegúrese de que las asignaciones creadas coincidan con el tipo de dirección usado por el servidor Citrix.

Para configurar los parámetros de puerta de enlace

Si utiliza Access Gateway o Secure Gateway en su entorno, debe configurar la Interfaz Web para funcionar con estas puertas de enlace. Para ello, debe utilizar la tarea Acceso seguro de la consola Administración de la Interfaz Web de Citrix.

1. En el menú Inicio de Windows, haga clic en Todos los programas > Citrix > Management Consoles > Citrix Web Interface Management.

2. En el panel izquierdo de la consola Administración de la Interfaz Web de Citrix, haga clic en Sitios Web XenApp o Sitios de servicios XenApp, según corresponda, y seleccione el sitio en el panel de resultados.

3. En el panel Acción, haga clic en Acceso seguro.

4. En la página Especificar métodos de acceso, haga clic en Agregar para agregar una nueva ruta de acceso o seleccione una entrada en la lista y haga clic en Modificar para cambiar una ruta existente.

5. En la lista Método de acceso, seleccione una de las opciones siguientes:

   - Seleccione Directa con gateway, si desea que la puerta de enlace (gateway) reciba la dirección real del servidor Citrix.

   - Seleccione Alternativa con gateway, si desea que la puerta de enlace (gateway) reciba la dirección alternativa del servidor XenApp. El servidor XenApp debe configurarse con una dirección alternativa y el servidor de seguridad debe configurarse para la traducción de direcciones de red.

     Nota: No se puede acceder a los escritorios virtuales de XenDesktop si se utilizan direcciones alternativas.

   - Seleccione Traducida con Gateway, si desea que la puerta de enlace (gateway) reciba la dirección asignada por la traducción de direcciones definida en la Interfaz Web.

6. Introduzca la dirección de red y la máscara de subred que identifican a la red de cliente. Use los botones Subir y Bajar para colocar las rutas de acceso según el orden de prioridad en la tabla Direcciones de dispositivos de usuarios y haga clic en Siguiente.

7. Si no utiliza traducción de direcciones con puerta de enlace, continúe en el paso 10. Si usa la traducción de direcciones con puerta de enlace, haga clic en Agregar en la página Especificar traducción de direcciones para agregar una nueva traducción de direcciones, o seleccione una entrada en la lista y haga clic en Modificar para cambiar una traducción de direcciones existente.

8. En la sección Tipo de acceso, seleccione una de las opciones siguientes:

   - Si quiere que la puerta de enlace use la dirección traducida para conectarse con el servidor Citrix, seleccione Traducción de ruta de puerta de enlace.

- Si ya ha configurado la ruta traducida de un cliente en la tabla Direcciones de dispositivos de usuarios y desea que tanto el cliente Citrix como la puerta de enlace utilicen la dirección traducida para conectarse con el servidor Citrix, seleccione Traducción de rutas de dispositivos de usuarios y puertas de enlace.

9. Introduzca las direcciones y puertos internos y externos (traducidos) para el servidor Citrix y haga clic en Aceptar. Cuando la puerta de enlace se conecte con el servidor Citrix, usará la dirección y el número de puerto externos. Asegúrese de que las asignaciones creadas coinciden con el tipo de dirección usado por la comunidad de servidores. Haga clic en Next.

10. En la página Especificar parámetros de puerta de enlace, especifique el nombre completo de dominio (FQDN) y el número de puerto de la puerta de enlace que deben usar los clientes. El nombre completo de dominio debe coincidir con el nombre que figura en el certificado instalado en la puerta de enlace.

11. Si desea que el servidor Citrix mantenga abiertas las sesiones desconectadas mientras el cliente intenta reconectarse automáticamente, seleccione la casilla de verificación Habilitar la fiabilidad de sesiones.

12. Si habilitó la fiabilidad de sesiones y desea usar tiques simultáneos de dos Secure Ticket Authorities (STA), seleccione la casilla de verificación Solicitar tiques de dos STA, en caso de que estén disponibles. Cuando esta opción está habilitada, la Interfaz Web obtiene tiques de dos STA distintas por lo que no se interrumpen las sesiones de usuarios si una STA deja de estar disponible durante el transcurso de la sesión. Si, por algún motivo, la Interfaz Web no puede establecer comunicación con las dos STA, vuelve a utilizar una sola STA. Haga clic en Next.

    Nota: debe implementar Access Gateway para poder utilizar esta función. Actualmente, Secure Gateway no admite varias STA redundantes.

13. En la página Especificar parámetros de Secure Ticket Authority haga clic en Agregar para especificar la dirección URL de una STA que pueda usar la Interfaz Web, o seleccione una entrada de la lista y haga clic en Modificar para modificar los detalles existentes de la STA. Las STA se incluyen con Citrix XML Service; por ejemplo, en http[s]://*NombreDeServidor.Dominio.com*/scripts/ctxsta.dll. Puede especificar más de un STA para tolerancia de fallos; sin embargo, Citrix recomienda que no use un balanceador de carga externo con este fin. Use los botones Subir y Bajar para colocar los STA por orden de prioridad.

14. Elija si desea habilitar el equilibrio de carga entre los STA marcando la opción Usar para el equilibrio de carga. La implementación del equilibrio de carga permite distribuir las conexiones de forma uniforme entre los distintos servidores, para que ningún servidor se sobrecargue.

15. Especifique durante cuánto tiempo se ignorará a los STA que no respondan, en las casillas del campo Descartar servidores si no responden durante. La Interfaz Web permite la tolerancia de fallos entre los servidores incluidos en la lista URL de Secure Ticket Authority, de modo que si hay algún problema de comunicación, el servidor que falla se ignora durante el tiempo especificado.

Para configurar los parámetros de acceso predeterminados

El orden en que aparecen las entradas en la tabla Direcciones de dispositivos de usuarios es el mismo orden en el que se aplican las reglas. Si la dirección de un dispositivo de usuario no tiene una regla de acceso definida explícitamente, se aplica la regla predeterminada. Cuando se crea un sitio, la ruta predeterminada se configura automáticamente para el acceso directo. Puede especificar un método de acceso predeterminado adecuado para su entorno mediante la tarea Acceso seguro de la consola Administración de la Interfaz Web de Citrix.

1. En el menú Inicio de Windows, haga clic en Todos los programas > Citrix > Management Consoles > Citrix Web Interface Management.

2. En el panel izquierdo de la consola Administración de la Interfaz Web de Citrix, haga clic en Sitios Web XenApp o Sitios de servicios XenApp, según corresponda, y seleccione el sitio en el panel de resultados.

3. En el panel Acción, haga clic en Acceso seguro.

4. En la página Especificar métodos de acceso, seleccione la entrada de la lista con el nombre Predeterminado y haga clic en Modificar.

5. En la lista Método de acceso, seleccione una de las opciones siguientes:

   - Seleccione Directa si desea que el cliente Citrix reciba la dirección real del servidor Citrix.

   - Seleccione Alternativa si desea que el cliente reciba la dirección alternativa del servidor XenApp. El servidor XenApp debe configurarse con una dirección alternativa y el servidor de seguridad debe configurarse para la traducción de direcciones de red.

     Nota: No se puede acceder a los escritorios virtuales de XenDesktop si se utilizan direcciones alternativas.

   - Seleccione Traducida si desea que la dirección proporcionada al cliente esté determinada por la traducción de direcciones definida en la Interfaz Web.

   - Seleccione Directa con gateway, si desea que la puerta de enlace (gateway) reciba la dirección real del servidor Citrix.

   - Seleccione Alternativa con gateway, si desea que la puerta de enlace (gateway) reciba la dirección alternativa del servidor XenApp. El servidor XenApp debe configurarse con una dirección alternativa y el servidor de seguridad debe configurarse para la traducción de direcciones de red.

     Nota: No se puede acceder a los escritorios virtuales de XenDesktop si se utilizan direcciones alternativas.

- Seleccione Traducida con Gateway, si desea que la puerta de enlace (gateway) reciba la dirección asignada por la traducción de direcciones definida en la Interfaz Web.

6. Introduzca la dirección de red y la máscara de subred que identifican a la red de cliente. Use los botones Subir y Bajar para colocar las rutas de acceso según el orden de prioridad en la tabla Direcciones de dispositivos de usuarios.

7. Si está usando una traducción de direcciones o una puerta de enlace en su entorno, haga clic en Siguiente y especifique los parámetros adicionales necesarios para la configuración predeterminada. Para obtener más información, consulte Para configurar la traducción de direcciones en los servidores de seguridad internos y Para configurar los parámetros de puerta de enlace.

Modificación de los parámetros del servidor proxy del lado del cliente

Si utiliza un servidor proxy en el lado del cliente de la instalación de la Interfaz Web, puede configurar si los clientes Citrix se deben comunicar con el servidor que ejecuta XenApp o XenDesktop por medio del servidor proxy. Para ello, debe utilizar la tarea Proxy del cliente de la consola Administración de la Interfaz Web de Citrix.

Un servidor proxy ubicado en el lado del cliente de una instalación de la Interfaz Web proporciona varias ventajas de seguridad, que incluyen:

- Ocultar información de manera que los nombres de sistema dentro del ámbito del servidor de seguridad o firewall no se difundan fuera del mismo a través de DNS (sistema de nombres de dominio).
- Canalizar las diferentes conexiones TCP a través de una conexión.

Mediante la consola Administración de la Interfaz Web de Citrix se pueden configurar las reglas predeterminadas del servidor proxy para los clientes Citrix. No obstante, también se pueden configurar las excepciones de este comportamiento para dispositivos de usuarios específicos. Para configurar excepciones, debe asociar la dirección IP externa del servidor proxy con la configuración proxy de la Interfaz Web.

Asimismo, se puede determinar que el cliente controle el comportamiento del servidor proxy. Por ejemplo, para usar la función de Proxy seguro en XenApp y XenDesktop, configure la Interfaz Web para usar los parámetros del proxy especificados en el cliente y configure el cliente para utilizar Proxy seguro. Para obtener más información sobre el uso de clientes Citrix para controlar el comportamiento del proxy, consulte la documentación del cliente en cuestión.

Para configurar los parámetros predeterminados del proxy

1. En el menú Inicio de Windows, haga clic en Todos los programas > Citrix > Management Consoles > Citrix Web Interface Management.

2. En el panel izquierdo de la consola Administración de la Interfaz Web de Citrix, haga clic en Sitios Web XenApp o Sitios de servicios XenApp, según corresponda, y seleccione el sitio en el panel de resultados.

3. En el panel Acción, haga clic en Proxy del cliente.

4. Haga clic en Agregar para crear una nueva asignación, o seleccione una entrada en la lista y haga clic en Editar para cambiar una asignación existente.

5. Introduzca la dirección externa del proxy y la máscara de subred del dispositivo del usuario en las casillas Dirección IP y Máscara de subred, respectivamente.

6. En la lista Proxy, seleccione una de las opciones siguientes:

   - Si desea que el cliente Citrix detecte automáticamente el proxy Web en función de la configuración del explorador del usuario, seleccione Parámetro del explorador del usuario.

   - Si desea que el cliente detecte automáticamente el proxy Web mediante el protocolo de detección automática del proxy Web (WPAD), seleccione Detección automática del proxy Web.

   - Si desea usar los parámetros configurados por el usuario para el cliente, seleccione Definido por el cliente.

   - Si desea usar un servidor proxy SOCKS, seleccione SOCKS. Si selecciona esta opción, debe ingresar la dirección y el número de puerto del servidor proxy. La dirección del proxy puede ser una dirección IP o un nombre DNS.

   - Si desea usar un servidor proxy seguro, seleccione Seguro (HTTPS). Si selecciona esta opción, debe ingresar la dirección y el número de puerto del servidor proxy. La dirección del proxy puede ser una dirección IP o un nombre DNS.

   - Si no desea usar ningún proxy, seleccione Ninguno.
7. Si introdujo varias asignaciones, use los botones Subir y Bajar para colocarlas por orden de prioridad en la tabla.

Personalización de la apariencia para los usuarios

Es posible personalizar la apariencia de la interfaz de usuario si, por ejemplo, desea que el sitio tenga un estilo determinado propio de la organización.

Utilice la tarea Apariencia del sitio Web de la consola Administración de la Interfaz Web de Citrix para personalizar lo siguiente:

- **Diseño:** Especifique los controles que estarán disponibles para los usuarios y defina cómo se presenta el sitio Web. Puede:
    - Seleccionar un diseño de pantalla automático, con gráficos o sin gráficos para el sitio Web XenApp. La interfaz de usuario sin gráficos es una versión compacta diseñada para los usuarios que acceden a sus recursos mediante dispositivos de factor de forma pequeño o por medio de conexiones de red lentas. Con la opción Automático el sistema elige el diseño de sitio más adecuado para cada usuario según el tamaño de la pantalla de su equipo.
    - Configurar las funciones y los controles disponibles en la pantalla Aplicaciones de los usuarios, incluidos los controles de búsqueda y sugerencias; y especificar si los usuarios tienen permiso para personalizar sus propias pantallas.
    - Definir los estilos de vista predeterminados para los conjuntos de recursos de los usuarios en los diseños de pantalla con gráficos y sin ellos. También se puede especificar qué estilos de vista están disponibles para que los elija el usuario.
    - Especificar la manera en que deben agruparse los recursos en las pantallas de Aplicaciones de los usuarios. Pueden configurarse fichas separadas para aplicaciones, contenido y escritorios, o bien, se pueden agrupar todos los recursos en una única ficha.
- **Apariencia.** Cambie la apariencia de la interfaz de usuario y agregue un toque personalizado mediante imágenes y colores diferentes en todo el sitio. Puede:
    - Especificar el estilo de las pantallas de Inicio de sesión de los usuarios. Elegir entre un diseño minimalista que sólo muestra los campos de inicio de sesión necesarios y un diseño más complejo que incluye la barra de navegación desde la que los usuarios pueden acceder a las pantallas de Mensajes y Preferencias de pre-inicio de sesión.
    - Usar imágenes de marca personalizadas para el sitio en los diseños con y sin gráficos y agregar hipervínculos en las imágenes. También puede cambiar la imagen de fondo en el encabezado del sitio o usar un color específico.
- **Contenido:** Puede definir texto personalizado para pantallas y mensajes y especificar versiones de este texto en distintos idiomas según el idioma que usen los usuarios para acceder al sitio. Puede especificar títulos de páginas y mensajes para las pantallas Inicio de sesión y Aplicaciones de los usuarios, y un texto de pie de página común que aparecerá en todas las pantallas. Además, se puede configurar un aviso de renuncia de responsabilidades antes del inicio de sesión, que los usuarios deben aceptar antes de iniciar sesión.

Administración de accesos directos a los recursos

Puede utilizar la tarea Accesos directos de la consola Administración de la Interfaz Web de Citrix para especificar la forma en que Citrix online plug-In muestra los accesos directos a los recursos.

Puede crear los siguientes tipos de accesos directos:

- **Menú Inicio:** Puede usar los parámetros definidos en la tarea Accesos directos, los parámetros definidos en el momento de publicar los recursos en XenApp y XenDesktop, o ambos parámetros. También puede definir si los accesos directos deben aparecer en el menú Inicio y cómo; y permitir que los usuarios configuren este parámetro. Además puede crear accesos directos en el menú Todos los programas, crear un submenú adicional, y/o permitir que los usuarios especifiquen un nombre de submenú.

- **Escritorio:** Puede usar los parámetros definidos en la tarea Accesos directos, los parámetros definidos en el momento de publicar los recursos en XenApp y XenDesktop, o ambos parámetros. También puede definir si los accesos directos deben aparecer en el escritorio y cómo; y permitir que los usuarios configuren este parámetro. Además, puede utilizar un nombre de carpeta personalizado o permitir a los usuarios seleccionar un nombre.

- **Área de notificación:** Puede mostrar los recursos en el área de notificación o permitir a los usuarios especificar la forma en que deben mostrarse los recursos.

Por medio de la tarea Accesos directos también se pueden eliminar accesos directos. Puede especificar el momento en que se deben eliminar los accesos directos (cuando se cierra Citrix Online Plug-In o cuando los usuarios cierran la sesión de XenApp) y, para los usuarios que ejecutan Windows CE o Linux, si se deben eliminar los accesos directos creados por el usuario además de los accesos directos de Citrix Online Plug-In. Si elige eliminar ambos accesos directos, los creados por Citrix Online Plug-In y los creados por el usuario, también puede limitar la profundidad de carpetas para la búsqueda y así mejorar el rendimiento.

Uso de las opciones de actualización de recursos

Utilice la tarea Actualización de recursos de la consola Administración de la Interfaz Web de Citrix para especificar cuándo se deben actualizar las listas de recursos de los usuarios y si éstos pueden personalizar estos parámetros. Se puede permitir que la actualización tenga lugar al iniciarse Citrix Online Plug-in o al acceder a los recursos, y puede especificarse la frecuencia con que se debe actualizar la lista.

Administración de las preferencias de sesión

Use la tarea Configuración de la sesión de Citrix Web Interface Management Console para especificar los parámetros que los usuarios pueden ajustar. También puede usar esta tarea para especificar el período después del cual se cerrará la sesión de la Interfaz Web de los usuarios inactivos, y si la Interfaz Web debe sobrescribir el nombre del dispositivo de usuario en el caso de los clientes para recursos en línea.

Para los sitios Web XenApp se pueden configurar los siguientes parámetros de sesión de usuario:

- **Personalizaciones del usuario:** Active o desactive el modo kiosco y especifique si debe mostrarse el botón Configuración en las pantallas de Aplicaciones de los usuarios.
- **Sesiones Web:** Especifique el tiempo que una sesión de usuario puede estar inactiva antes de cerrarse.
- **URL persistentes.** Especifique si los usuarios pueden usar los favoritos del explorador para acceder al sitio.
- **Rendimiento de la conexión:** Especifique los parámetros de configuración predeterminados o permita que los usuarios personalicen los parámetros de control del ancho de banda, profundidad del color, calidad del audio y asignación de las impresoras.
- **Presentación:** Especifique si los usuarios pueden controlar los tamaños de las ventanas en las sesiones en línea y permitir que la Interfaz Web use el suavizado de fuentes de ClearType, siempre que los parámetros correspondientes hayan sido configurados para los sistemas operativos Windows de los usuarios, el software cliente Citrix de los usuarios y la comunidad de servidores.
- **Recursos locales:** Configure los parámetros para la combinación de teclas de Windows, la sincronización de PDA y la redirección de carpetas especiales.
- **Nombres de dispositivos de usuarios.** Especifique si la Interfaz Web debe sobrescribir los nombres de los dispositivos de los usuarios en el caso de recursos en línea.

  Importante: debe habilitar el parámetro Sobrescribir los nombres de dispositivos de usuarios si desea utilizar el control del área de trabajo con las versiones 8.*x* y 9.*x* de los Clientes para Windows.

En los sitios de servicios XenApp que proporcionan recursos en línea, puede usar la tarea Opciones de sesión de la consola Administración de la Interfaz Web de Citrix para configurar los siguientes parámetros para las sesiones de usuarios:

- **Presentación:** Seleccione los tamaños de ventana disponibles para sesiones ICA y defina tamaños personalizados en pixeles o en porcentaje de pantalla. Además, puede

permitir que la Interfaz Web use el suavizado de fuentes de ClearType, siempre que los parámetros correspondientes estén configurados para los sistemas operativos Windows de los usuarios, Citrix Online Plug-in y la comunidad de servidores.

- **Color y sonido:** Los usuarios pueden elegir las opciones que se habilitan en esta sección.

- **Recursos locales:** Habilite los destinos de las combinaciones de teclas de Windows que los usuarios pueden seleccionar. Las combinaciones de teclas de Windows no afectan a las conexiones integradas. Se pueden activar los siguientes destinos:

  - **Escritorio local:** Las combinaciones de teclas sólo se aplican al escritorio físico local; no tienen efecto en las sesiones ICA.

  - **Escritorio remoto:** Las combinaciones de teclas sólo se aplican al escritorio virtual en la sesión ICA.

  - **Sólo escritorios en modo pantalla completa:** Las combinaciones de teclas se aplican al escritorio virtual en la sesión ICA sólo cuando está en modo de pantalla completa.

  Habilite la Redirección de carpetas especiales, de modo que cuando los usuarios abran, cierren o guarden archivos en las carpetas \Documentos o \Escritorio desde los recursos en línea, sus acciones sean redirigidas a las carpetas de los equipos locales. Para obtener más información, consulte Redirección de carpetas especiales.

- **Control del área de trabajo.** Configure la reconexión y el cierre de sesión. Para obtener más información, consulte Configuración del control del área de trabajo.

Control de ancho de banda

El control de ancho de banda permite a los usuarios seleccionar parámetros de sesión según el ancho de banda de su conexión. Estas opciones aparecen en la pantalla Configuración, antes o después de iniciar sesión. La función de control de ancho de banda permite ajustar la profundidad del color, la calidad del sonido y la asignación de impresoras. Además, es posible utilizar Web Interface Management Console para especificar parámetros predeterminados o personalizados para los usuarios. Utilice la tarea Administrar configuración de la sesión para personalizar la configuración de ancho de banda con las opciones Rendimiento de la conexión. Seleccione Personalizar de la lista desplegable Velocidad de conexión para activar las opciones Calidad de color, Sonido y Activar asignación de impresoras.

Si se utiliza el Cliente para Java, el control de ancho de banda determina si están disponibles los paquetes de asignación de impresoras y sonido. Si se utiliza el software de Conexión a escritorio remoto (RDP), la calidad del sonido sólo puede activarse o desactivarse, sin posibilidad de ajustar más la calidad de sonido. Para conexiones WAN inalámbricas se recomiendan los parámetros para un ancho de banda bajo.

Nota: Si se utiliza el software de Conexión a escritorio remoto (RDP) junto con el control de ancho de banda, la Interfaz Web especifica los parámetros apropiados para el ancho de banda seleccionado. Pero el comportamiento real depende de la versión del software de Conexión a escritorio remoto (RDP) que se esté utilizando, los servidores Terminal Server y la configuración del servidor.

De forma predeterminada, los usuarios pueden ajustar el tamaño de la ventana de las sesiones.

Si no permite que los usuarios ajusten un parámetro determinado, éste no aparecerá en la interfaz de usuario y se utilizarán los parámetros que se hayan especificado en el servidor para el recurso en cuestión.

Suavizado de fuentes de ClearType

ClearType es una tecnología de suavizado de subpixel desarrollada por Microsoft que mejora la presentación del texto en pantallas LCD, reduciendo irregularidades y suavizando los bordes del texto. El suavizado de fuentes de ClearType es una función incluida en Windows XP. El suavizado de fuentes está habilitado de manera predeterminada en Windows 7 y Windows Vista, pero no en Windows XP.

La Interfaz Web y Citrix Online Plug-in respaldan el suavizado de fuentes de ClearType durante las sesiones ICA. Cuando un usuario que ejecuta Windows XP o una versión posterior se conecta al servidor, el plug-in detecta automáticamente los parámetros de suavizado de fuentes del equipo del usuario y los envía al servidor. Este parámetro se usa durante la sesión.

El suavizado de fuentes debe estar habilitado en los sistemas operativos de los usuarios, en Citrix Online Plug-in, en el sitio de la Interfaz Web y en la comunidad de servidores. Utilice la tarea Configuración de la sesión de Citrix Web Interface Management Console para habilitar el suavizado de fuentes para los sitios Web de XenApp y la tarea Opciones de sesión para los sitios de servicios XenApp.

El suavizado de fuentes se aplica únicamente a los recursos en línea. Esta función no está disponible para aplicaciones sin conexión.

Redirección de carpetas especiales

La función de Redirección de carpetas especiales permite a los usuarios asignar las carpetas especiales de Windows del servidor al equipo local para facilitar su utilización con los recursos en línea. 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.

Nota: Antes de Windows Vista, las carpetas especiales llevaban el pronombre "Mi/Mis"; por ejemplo, la carpeta "Documentos" era "Mis documentos" en Windows XP.

Cuando los usuarios abren, cierran o guardan archivos en una sesión sin tener habilitada la función de Redirección de carpetas especiales, los iconos de Documentos y Escritorio que aparecen en los cuadros de diálogo de navegación dentro de los recursos en línea de los usuarios representan las carpetas \Documentos y \Escritorio en el servidor. La redirección de carpetas especiales redirige las acciones del usuario (por ejemplo, al abrir o guardar un archivo), de manera que cuando los usuarios abren o guardan archivos en las carpetas \Documentos y \Escritorio, dichas carpetas son las de sus equipos locales y no las del servidor. Actualmente la redirección de carpetas especiales sólo está disponible para las carpetas \Documentos y \Escritorio.

La Redirección de carpetas especiales se aplica a los recursos en línea únicamente. Esta función no está disponible para aplicaciones sin conexión.

Habilitación de la redirección de carpetas especiales

La redirección de carpetas especiales se encuentra desactivada de forma predeterminada tanto en los sitios Web XenApp como en los sitios de servicios XenApp. Si se activa la redirección de carpetas especiales para un sitio, debe asegurarse de que ninguna de las reglas de directiva existentes en su comunidad de servidores prohíba a los usuarios el acceso o el almacenamiento en sus unidades locales.

Utilice la tarea Configuración de la sesión de Citrix Web Interface Management Console para activar la redirección de carpetas especiales para los sitios Web de XenApp y la tarea Opciones de sesión para los sitios de servicios XenApp. También puede permitir que los usuarios activen esta función, si lo desean, en la pantalla Configuración.

Cuando se habilita la redirección de carpetas especiales, los usuarios siempre deben conceder a los recursos acceso completo de lectura y escritura a carpetas y archivos locales. Para ello, se debe seleccionar Acceso completo en el cuadro de diálogo Seguridad de archivos de clientes de la Central de conexiones de Citrix. Los usuarios deben cerrar las sesiones que estén activas antes de iniciar una nueva sesión en otro dispositivo. Citrix recomienda no habilitar la redirección de carpetas especiales para los usuarios que se conecten simultáneamente a la misma sesión desde varios dispositivos.

Configuración del control del área de trabajo

Utilice el control del área de trabajo para permitir que los usuarios se desconecten rápidamente de todos los recursos (aplicaciones, contenido y escritorios), vuelvan a conectarse con recursos desconectados y cierren sesión en todos los recursos. Esto permite a los usuarios moverse entre dispositivos y obtener acceso a todos sus recursos (desconectados únicamente, o desconectados y activos) al iniciar sesión o manejarse manualmente en el momento en que lo deseen. Por ejemplo, los médicos de hospitales pueden tener la necesidad de moverse entre estaciones de trabajo y acceder al mismo conjunto de recursos cada vez que inician sesión.

Requisitos del control del área de trabajo

A continuación se describen los requisitos y recomendaciones para usar la función del control del área de trabajo:

- Para utilizar el control del área de trabajo con las versiones 8.*x* y 9.*x* de los Clientes para Windows, debe habilitar el parámetro Sobrescribir los nombres de dispositivos de usuarios en la tarea Preferencias de sesión de la consola Administración de la Interfaz Web de Citrix.

- Si la Interfaz Web detecta un acceso desde una sesión de Citrix, la función del control del área de trabajo se desactiva.

- En función de los parámetros de seguridad, Internet Explorer puede bloquear la descarga de archivos que no haya sido directamente iniciada por el usuario; por lo tanto, se pueden bloquear los intentos de reconexión con los recursos mediante un cliente nativo. En situaciones en que no sea posible volver a realizar una conexión, aparecerá un mensaje de advertencia para el usuario y se le dará la opción de cambiar los parámetros de seguridad de Internet Explorer.

- Cada sesión Web se cierra automáticamente después de un periodo de inactividad (normalmente 20 minutos). Cuando se agota el tiempo de espera de la sesión HTTP, aparece la pantalla de cierre de sesión. No obstante, los recursos que se iniciaron o reconectaron durante dicha sesión no se desconectan. Los usuarios deben desconectar, cerrar sesión o volver a iniciar sesión en la Interfaz Web manualmente y utilizar los botones Cerrar sesión o Desconectar.

- Los recursos publicados para uso anónimo se cierran cuando los usuarios anónimos y autenticados se desconectan de ellos, siempre que el servicio XML de Citrix esté configurado para confiar en las credenciales de la Interfaz Web. Por lo tanto, los usuarios no pueden volver a conectarse con recursos para uso anónimo una vez que se desconectan.

- Para utilizar la autenticación mediante paso de credenciales (PassThrough), tarjeta inteligente, o paso de credenciales con tarjeta inteligente, es necesario configurar una relación de confianza entre el servidor de la Interfaz Web y el servicio XML de Citrix.

Para obtener más información, consulte Uso del control del área de trabajo con métodos de autenticación integrados para los sitios Web de XenApp.

- Si el paso de credenciales no está habilitado para los sitios Web XenApp, el sistema pedirá el PIN a los usuarios de tarjeta inteligente cada vez que vuelvan a conectarse a una sesión de Citrix. Esto no supone ningún problema para la autenticación mediante paso de credenciales o mediante paso de credenciales con tarjetas inteligentes en los sitios de XenApp Services, porque el paso de credenciales está habilitado con estas opciones.

Limitaciones del control del área de trabajo

Si piensa habilitar el control del área de trabajo, tenga en cuenta lo siguiente:

- El control del área de trabajo no está disponible para sitios configurados para distribuir aplicaciones sin conexión. Si configura un sitio para la distribución en modo dual, el control del área de trabajo sólo se aplica a los recursos en línea.

- No puede utilizar el control del área de trabajo con el Cliente para Windows de 32 bits de una versión anterior a la Versión 8, ni tampoco con el software de Conexión a escritorio remoto (RDP). Además, esta función solo funciona con servidores que ejecutan Presentation Server 4.5 o posterior.

- El control del área de trabajo sólo permite la reconexión con escritorios virtuales de XenDesktop que estén desconectados. Los usuarios no pueden volver a conectarse con escritorios virtuales en estado suspendido.

Uso del control del área de trabajo con métodos de autenticación integrados para los sitios Web de XenApp

La siguiente sección se aplica solamente a los sitios Web de XenApp. Si los usuarios inician sus sesiones mediante paso de credenciales (PassThrough), tarjeta inteligente o paso de credenciales con tarjeta inteligente, es necesario configurar una relación de confianza entre el servidor de la Interfaz Web y cualquier otro servidor que ejecute el servicio XML de Citrix con el que se comunica la Interfaz Web. Citrix XML Service transfiere la información sobre recursos entre la Interfaz Web y los servidores que ejecutan XenApp y XenDesktop. Sin esta relación de confianza, los botones Desconectar, Reconectar y Cerrar sesión no funcionarán para los usuarios que inicien sesión mediante autenticación con tarjeta inteligente o mediante paso de credenciales.

No es necesario configurar una relación de confianza si los usuarios son autenticados por la comunidad de servidores; es decir, si no inician sesión con los métodos de autenticación con tarjeta inteligente o paso de credenciales.

Para configurar la relación de confianza

Si configura un servidor para que confíe en las solicitudes enviadas al servicio XML de Citrix, tenga en cuenta lo siguiente:

- Cuando configura la relación de confianza, depende del servidor de la Interfaz Web para la autenticación del usuario. Para evitar riesgos de seguridad, use IPSec, servidores de seguridad o firewalls, o cualquier tecnología que asegure que sólo los servicios de confianza pueden comunicarse con el servicio XML de Citrix. Si configura una relación de confianza sin utilizar IPSec, servidores de seguridad, o ninguna otra tecnología de seguridad, cualquier dispositivo de la red puede desconectar o terminar sesiones. No se necesita una relación de confianza si los sitios están configurados para usar únicamente autenticación explícita.

- Habilite la relación de confianza sólo en servidores conectados directamente a la Interfaz Web. Estos servidores se muestran en la tarea Comunidades de servidores de la consola Administración de la Interfaz Web de Citrix.

- Configure la tecnología que utiliza para garantizar la seguridad de su entorno y limitar el acceso al servicio XML de Citrix sólo al servidor de la Interfaz Web. Por ejemplo, si el servicio XML de Citrix comparte un puerto con Microsoft Internet Information Services (IIS), puede usar las capacidades de restricción de direcciones IP de IIS para restringir el acceso al servicio XML de Citrix.

1. Inicie sesión en un servidor de la comunidad y haga clic en Inicio > Todos los programas > Citrix > Consolas de administración > Citrix Delivery Services Console.

2. En el panel izquierdo de la consola, vaya a Recursos de Citrix > XenApp, expanda el nodo de su comunidad y, a continuación, haga clic en Directivas.

3. En el panel de detalles de la consola, seleccione la ficha Equipo y haga clic en Nueva.

4. Escriba un nombre y, de manera opcional, una descripción de la nueva directiva y, a continuación, haga clic en Siguiente.

5. En la lista Categorías haga clic en Servicio XML, y en Parámetros seleccione Confiar en las solicitudes XML y, a continuación, haga clic en Agregar.

6. Seleccione Habilitado y haga clic en Aceptar. Haga clic en Next.

7. Si fuera necesario, aplique filtros a su directiva para determinar las circunstancias en las que se aplicará, y luego haga clic en Siguiente.

8. Compruebe que la casilla Habilitar esta directiva esté marcada y haga clic en Guardar.

Para habilitar la reconexión automática al iniciar sesión

1. En el menú Inicio de Windows, haga clic en Todos los programas > Citrix > Management Consoles > Citrix Web Interface Management.

2. En el panel izquierdo de la consola Administración de la Interfaz Web de Citrix, haga clic en Sitios Web XenApp o Sitios de servicios XenApp, según corresponda, y seleccione el sitio en el panel de resultados.

3. En el panel Acción, seleccione la tarea adecuada para el tipo de sitio:

   - Para sitios Web XenApp, haga clic en Control del área de trabajo

   - Para sitios de XenApp Services, haga clic en Opciones de sesión y seleccione Control del área de trabajo
4. Marque la opción Reconectar automáticamente al iniciar sesión.

5. Seleccione una de estas opciones:

   - Para reconectar automáticamente con sesiones activas y sesiones desconectadas, seleccione Reconectar todas las sesiones

   - Para reconectar automáticamente sólo con sesiones desconectadas, seleccione Reconectar sólo sesiones desconectadas
6. Marque la casilla Permitir personalizar al usuario si desea permitir que los usuarios configuren este parámetro. Los usuarios pueden cambiar este parámetro en la pantalla Configuración de los sitios Web de XenApp o en el cuadro de diálogo Opciones de Citrix Online Plug-In.

Para habilitar el botón Reconectar

1. En el menú Inicio de Windows, haga clic en Todos los programas > Citrix > Management Consoles > Citrix Web Interface Management.

2. En el panel izquierdo de la consola Administración de la Interfaz Web de Citrix, haga clic en Sitios Web XenApp o Sitios de servicios XenApp, según corresponda, y seleccione el sitio en el panel de resultados.

3. En el panel Acción, seleccione la tarea adecuada para el tipo de sitio:

   - Para sitios Web XenApp, haga clic en Control del área de trabajo

   - Para sitios de XenApp Services, haga clic en Opciones de sesión y seleccione Control del área de trabajo
4. Marque la opción Habilitar el botón Reconectar.

5. Seleccione una de estas opciones:

   - Para configurar el botón Reconectar para reconectar a los usuarios con sesiones activas y sesiones desconectadas, seleccione Reconectar todas las sesiones

   - Para configurar el botón Reconectar para reconectar a los usuarios sólo con sesiones desconectadas, seleccione Reconectar sólo sesiones desconectadas
6. Marque la casilla Permitir personalizar al usuario si desea permitir que los usuarios configuren este parámetro. Los usuarios pueden cambiar este parámetro en la pantalla Settings de los sitios Web de XenApp o en el cuadro de diálogo Opciones de Citrix Online Plug-In para los sitios de servicios XenApp.

Para configurar el cierre de sesiones

1. En el menú Inicio de Windows, haga clic en Todos los programas > Citrix > Management Consoles > Citrix Web Interface Management.

2. En el panel izquierdo de la consola Administración de la Interfaz Web de Citrix, haga clic en Sitios Web XenApp y seleccione el sitio en el panel de resultados.

3. En el panel Acción, haga clic en Control del área de trabajo.

4. Seleccione la casilla de verificación Cerrar sesiones activas al cerrar la sesión en el sitio si desea que cuando un usuario cierre sesión, se cierre la sesión de la Interfaz Web y de todas las sesiones activas. Si no selecciona esta opción, las sesiones de los usuarios permanecen activas después de cerrarse.

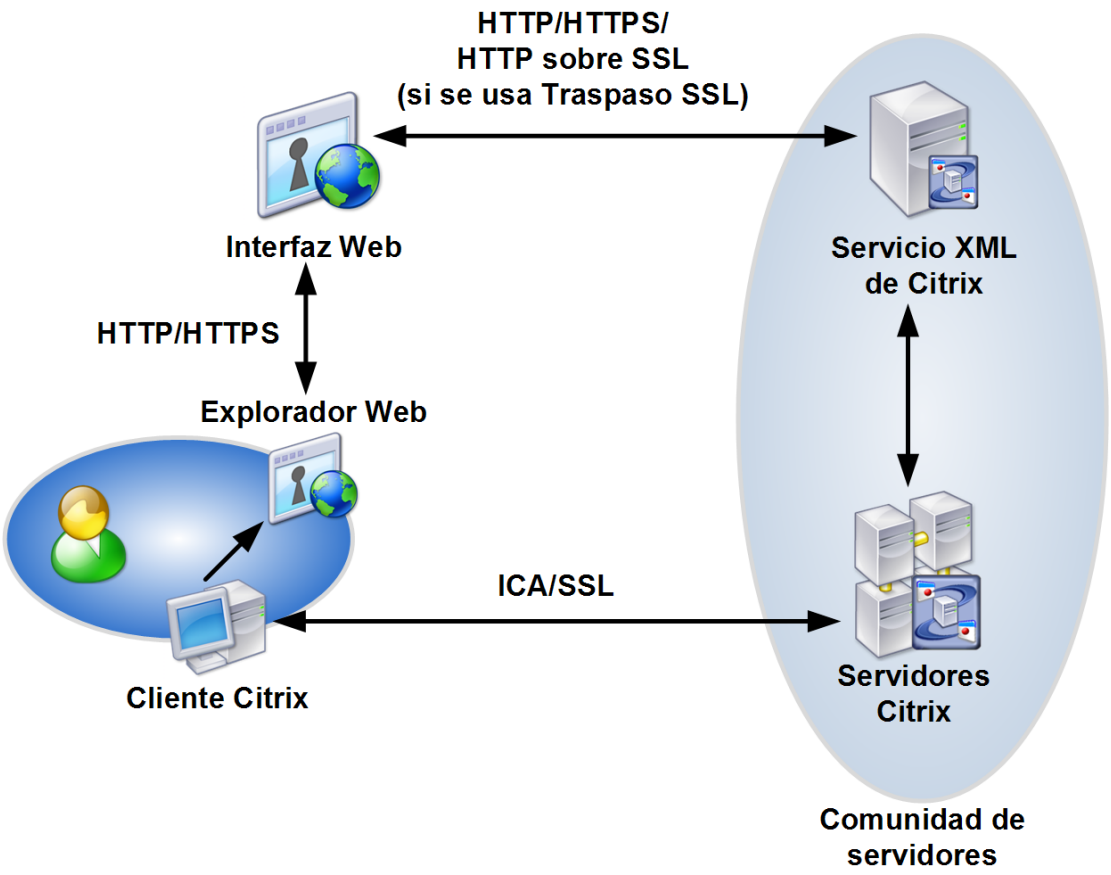
5. Seleccione la casilla de verificación Permitir personalizar al usuario si desea permitir que los usuarios configuren este parámetro en la pantalla Configuración del sitio.

Configuración de la seguridad en la Interfaz Web

Un plan integral de seguridad debe incluir la protección de los datos en todas las etapas del proceso de distribución de recursos. En esta sección se describen problemas y recomendaciones relacionados con la seguridad de la Interfaz Web para cada uno de los siguientes enlaces de comunicación:

- **Comunicación entre el dispositivo del usuario y la Interfaz Web.** Explica los problemas asociados con el paso de datos de la Interfaz Web entre los exploradores Web y los servidores, y sugiere estrategias para la protección de los datos en tránsito y los datos escritos en los dispositivos de los usuarios.
- **Comunicación entre la Interfaz Web y el servidor Citrix:** Describe cómo proteger la información de autenticación y de recursos que se transmite entre el servidor de la Interfaz Web y la comunidad de servidores.
- **Comunicación entre la sesión de usuario y el servidor.** Explica los problemas relacionados con el paso de información de sesión entre los servidores y los clientes Citrix. Describe las implementaciones de la Interfaz Web y las funciones de seguridad de XenApp/XenDesktop que protegen dicha información.

Este gráfico muestra cómo interactúan los dispositivos de los usuarios con el servidor que ejecuta XenApp o XenDesktop y el servidor de la Interfaz Web.



Consideraciones generales sobre seguridad

Citrix recomienda que, al igual que con cualquier servidor Windows, siga las recomendaciones estándar de Microsoft para configurar su servidor.

Asegúrese de que todos los componentes estén actualizados y de haber instalado las revisiones de software más recientes. Para obtener más información y consultar las recomendaciones sobre descargas más recientes, visite el sitio Web de Microsoft en http://support.microsoft.com/.

Secure Sockets Layer

El protocolo Secure Sockets Layer (SSL) permite proteger las comunicaciones de datos a través de redes. SSL proporciona la autenticación de servidores, el cifrado del flujo de datos y la comprobación de la integridad de los mensajes.

SSL usa criptografía para codificar mensajes, autenticar la identidad de los mismos y asegurar la integridad del contenido. Esto evita riesgos de intrusiones, encaminamientos incorrectos y manipulación de datos. SSL utiliza certificados de clave pública emitidos por entidades emisoras de certificados (Certificate Authority) para asegurar la prueba de identidad. Para obtener más información sobre SSL, criptografía y certificados, consulte Administración de XenApp, Secure Gateway y Administración del Traspaso SSL para UNIX.

Transport Layer Security

Transport Layer Security (TLS) es la versión estándar más reciente del protocolo SSL. El ente Internet Engineering Taskforce (IETF) le cambió el nombre a TLS cuando asumieron la responsabilidad de desarrollar SSL como un estándar abierto. Al igual que SSL, el protocolo TLS permite la autenticación de servidores, el cifrado del flujo de datos y la comprobación de la integridad de los mensajes.

El respaldo para TLS Versión 1.0 se incluye en todas las versiones respaldadas de XenApp para Windows y XenDesktop. Al existir sólo pequeñas diferencias técnicas entre la versión 3.0 de SSL y la versión 1.0 de TLS, los certificados de servidor que se usan para SSL en la instalación también funcionan con TLS.

Algunas organizaciones, entre las que se encuentran organizaciones del gobierno de los EE. UU., requieren el uso de TLS para las comunicaciones de datos seguras. Estas organizaciones pueden exigir también el uso de cifrado validado, como FIPS 140 (Federal Information Processing Standard). FIPS es un estándar de cifrado.

Nota: El tamaño máximo de clave de certificado de SSL/TLS admitido por la Interfaz Web para servidores de aplicaciones de Java es 2048 bits.

Traspaso SSL

El Traspaso SSL es un componente que usa SSL para proteger las comunicaciones entre los servidores de la Interfaz Web y las comunidades de servidores. El Traspaso SSL proporciona autenticación de servidores, cifrado de datos y comprobación de integridad de mensajes para una conexión TCP/IP. El Traspaso SSL es suministrado por el servicio XTE de Citrix.

El Traspaso SSL funciona como un intermediario en las comunicaciones entre el servidor de la Interfaz Web y el servicio XML de Citrix. Cuando se usa el Traspaso SSL, el servidor Web primero verifica la identidad del Traspaso SSL comparando el certificado del servidor de traspaso con una lista de entidades emisoras de certificados de confianza.

Después de esta autenticación, el servidor Web y el Traspaso SSL negocian un método de cifrado para la sesión. A continuación, el servidor Web envía todas las solicitudes de información en modo cifrado al Traspaso SSL. El Traspaso SSL descifra las solicitudes y las envía al servicio XML de Citrix. Cuando devuelve la información al servidor Web, el servicio XML de Citrix envía toda la información a través del servidor que ejecuta el Traspaso SSL, el cual cifra los datos y luego los reenvía al servidor Web para descifrarlos. La comprobación de la integridad de los mensajes verifica que las comunicaciones no fueron intervenidas o manipuladas. Para obtener más información sobre el Traspaso SSL, consulte Administración de XenApp o Administración del Traspaso SSL para UNIX.

Cifrado ICA

El cifrado ICA permite cifrar la información que se envía entre un servidor y un cliente Citrix. Esto hace más difícil la interpretación de la transmisión cifrada para usuarios no autorizados.

En consecuencia, el cifrado ICA proporciona confidencialidad, lo que ayuda a proteger el sistema contra intrusos. No obstante, hay otros riesgos de seguridad y el uso de cifrado es sólo una parte de la política integral de seguridad. A diferencia de SSL/TLS, el cifrado ICA no proporciona autenticación del servidor. En consecuencia, en teoría, la información podría ser interceptada cuando atraviesa la red y ser derivada a un servidor falso. Asimismo, el cifrado ICA no proporciona comprobación de integridad.

El cifrado ICA no está disponible para servidores XenApp para UNIX.

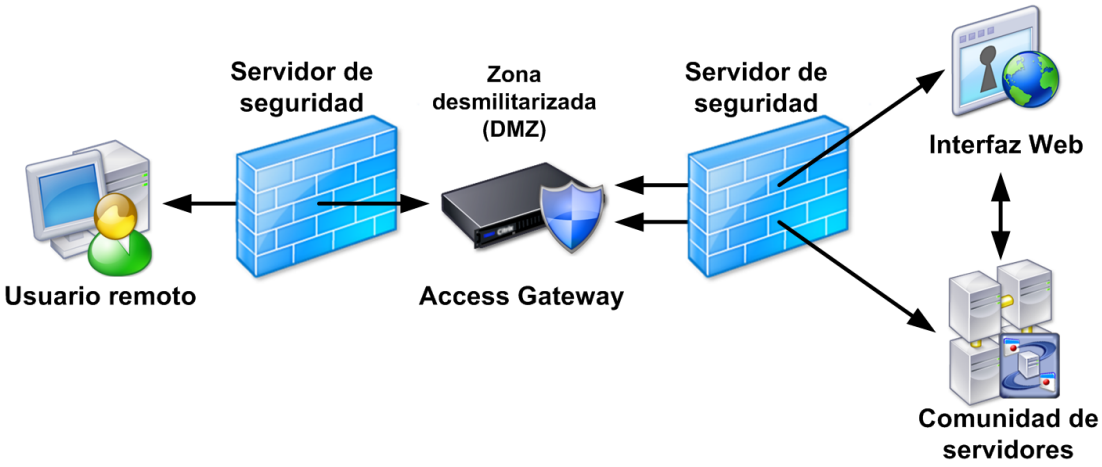
Access Gateway

Se puede utilizar Access Gateway con la Interfaz Web y Secure Ticket Authority (STA) para proporcionar autenticación, autorización y redirección a recursos (aplicaciones, contenido y escritorios) distribuidos desde un servidor que ejecuta XenApp o XenDesktop.

Access Gateway es un dispositivo universal de red privada virtual (VPN) con Secure Socket Layer (SSL) que proporciona un punto de acceso único y seguro a cualquier recurso de información, tanto de voz como de datos. Access Gateway cifra y admite todos los recursos y protocolos.

Access Gateway proporciona acceso seguro e integral a aplicaciones, contenido, escritorios y recursos de red autorizados a los usuarios remotos, lo que les permite trabajar con archivos en unidades de red, correo electrónico, sitios de intranet y recursos del mismo modo en que lo hacen dentro del servidor de seguridad de la organización.

Esta figura muestra cómo Access Gateway protege la comunicación entre los clientes Citrix y los servidores que tienen habilitados los protocolos SSL/TLS.



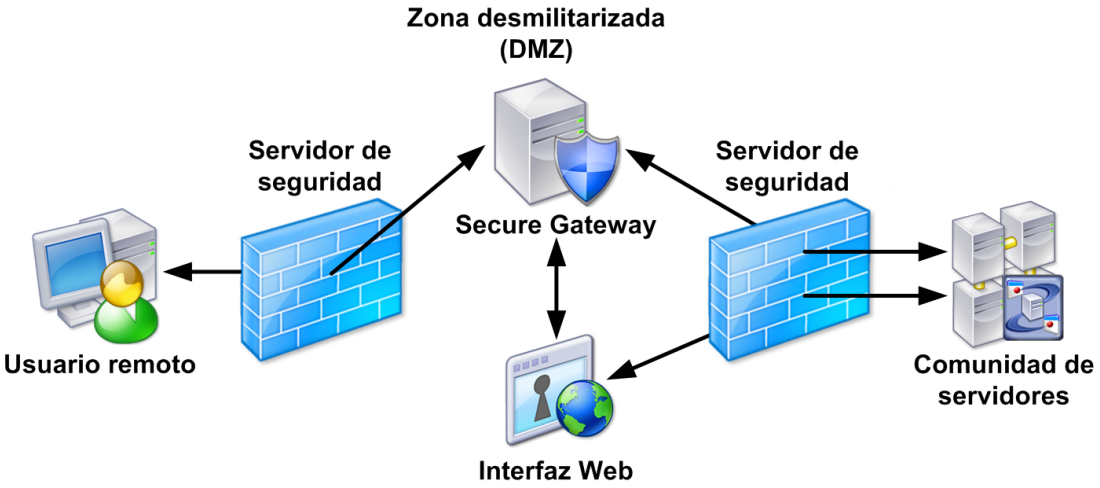
Para obtener más información sobre Access Gateway, consulte la documentación de Access Gateway. Para obtener más información sobre cómo configurar la Interfaz Web para su funcionamiento con Access Gateway mediante la consola Administración de la Interfaz Web de Citrix, consulte Para configurar los parámetros de puerta de enlace.

Secure Gateway

Puede utilizar Secure Gateway junto con la Interfaz Web para proporcionar un punto de acceso único, seguro y cifrado a Internet para los servidores situados en las redes internas de la organización.

Secure Gateway actúa como una puerta de enlace segura de Internet entre los servidores y los clientes Citrix que tienen habilitado SSL/TLS, mediante el cifrado del tráfico ICA. La porción del tráfico de Internet entre los dispositivos de los usuarios y el servidor Secure Gateway se cifra mediante SSL/TLS. Esto significa que los usuarios pueden acceder a la información de forma remota sin comprometer la seguridad. Secure Gateway también simplifica la administración de los certificados, ya que sólo se requiere un certificado en el servidor Secure Gateway en lugar de necesitar uno en cada servidor de la comunidad.

Esta figura muestra cómo Secure Gateway protege la comunicación entre los servidores y los clientes Citrix que tienen habilitado los protocolos SSL/TLS.



Para obtener más información sobre Secure Gateway, consulte Secure Gateway. Para obtener más información sobre cómo configurar la Interfaz Web para su funcionamiento con Secure Gateway mediante la consola Administración de la Interfaz Web de Citrix, consulte Para configurar los parámetros de puerta de enlace.

Protección de las comunicaciones de la Interfaz Web

Cuando utiliza la Interfaz Web, puede implementar las siguientes medidas de seguridad para las comunicaciones entre el cliente y el servidor:

- Indique a los usuarios que se conecten a las páginas de la Interfaz Web usando HTTPS (HTTP seguro sobre SSL/TLS). El servidor Web debe tener un certificado SSL instalado para establecer una conexión HTTP segura.
- Configure la Interfaz Web para usar el Traspaso SSL para el cifrado entre el servidor de la Interfaz Web y los servidores que ejecutan XenApp y XenDesktop. También puede usar HTTPS para proteger la conexión si IIS está instalado en el servidor que ejecuta XenApp o XenDesktop.

Protección de Citrix Online Plug-in con SSL

Para usar SSL para proteger las comunicaciones entre Citrix online plug-in y el servidor de la Interfaz Web mediante la consola Administración de la Interfaz Web de Citrix, haga clic en Sitios de servicios XenApp en el panel izquierdo, seleccione el sitio en el panel de resultados, haga clic en Configuración del servidor en el panel Acción y seleccione la casilla de verificación Usar SSL/TLS para la comunicación entre los plug-ins y el sitio.

Asegúrese de que la casilla Habilitar los protocolos SSL y TLS esté marcada en la página Opciones del Cliente del cuadro de diálogo Propiedades de la aplicación en Delivery Services Console.

Comunicación entre el dispositivo del usuario y la Interfaz Web

La comunicación entre los clientes Citrix y el servidor de la Interfaz Web consiste en la transferencia de diversos tipos de datos. Cuando los usuarios se identifican, buscan recursos y finalmente seleccionan un recurso al que desean acceder, el explorador Web y el servidor Web transfieren las credenciales de usuario, los conjuntos de recursos y los archivos de inicialización de sesión. Específicamente, este tráfico de red incluye:

- **Información de formulario HTML:** Los sitios de la Interfaz Web usan un formulario HTML estándar para transmitir las credenciales del usuario desde el explorador Web al servidor Web durante el inicio de sesión. El formulario de la Interfaz Web pasa los nombres de usuario y las credenciales como texto sin formato.

- **Páginas HTML y cookies de sesión:** Después que el usuario escribe sus credenciales en la pantalla de Inicio de sesión, estas credenciales se almacenan en el servidor Web y se protegen mediante un cookie de sesión. Las páginas HTML que se envían desde el servidor Web al explorador Web contienen conjuntos de recursos. Estas páginas enumeran los recursos disponibles para el usuario.

- **Archivos ICA:** Cuando el usuario selecciona un recurso, el servidor Web envía un archivo .ica para ese recurso al cliente Citrix (en algunos casos, mediante el explorador Web como intermediario). El archivo .ica contiene un tiquet que se puede usar para iniciar sesión en el servidor. Los archivos ICA no incluyen un tiquet para autenticación mediante paso de credenciales (PassThrough) o autenticación con tarjeta inteligente.

  En algunos casos, cuando se ejecuta un cliente, el archivo .ica se guarda como archivo de texto sin formato en el disco duro del usuario. Sin embargo, esto no impide que el cliente se ejecute de manera correcta.

  La función Firma de archivos ICA permite a los usuarios verificar que están iniciando aplicaciones o escritorios de un servidor Web de confianza. Para obtener más información, consulte Configuración de la firma de archivos ICA

Problemas de seguridad en la comunicación entre el dispositivo del usuario y la Interfaz Web

Un intruso puede manipular los datos de la Interfaz Web cuando atraviesan la red entre el servidor Web y el explorador, y cuando se escriben en el dispositivo del usuario:

- Un intruso puede interceptar los datos de inicio de sesión, el cookie de sesión y las páginas HTML en tránsito entre el servidor Web y el explorador Web.
- Aunque la cookie de sesión que usa la Interfaz Web es temporal y desaparece cuando el usuario cierra el explorador Web, un intruso con acceso al explorador Web del usuario puede obtener la cookie y, posiblemente, utilizar la información de las credenciales.
- Aunque el archivo .ica no contiene ninguna credencial de usuario, contiene un tiquet de un solo uso que caduca al cabo de 200 segundos de manera predeterminada. Un intruso podría usar el archivo .ica interceptado para conectarse al servidor antes que el usuario autorizado pueda usar el tiquet y realizar la conexión.
- Si los usuarios de Internet Explorer que acceden al servidor Web mediante una conexión HTTPS seleccionan la opción para evitar que las páginas cifradas se guarden en caché, el archivo .ica se guarda como un archivo de texto sin formato en la carpeta de archivos temporales de Internet de Windows. Un intruso que tuviera acceso al caché de Internet Explorer de un usuario podría recuperar el archivo .ica y obtener así información sobre la red.
- Si está habilitada la autenticación mediante paso de credenciales (PassThrough) en el cliente Citrix, un intruso puede enviar al usuario un archivo .ica para hacer que las credenciales del usuario se desvíen a un servidor falso o no autorizado. Esto ocurre cuando el cliente captura las credenciales de los usuarios cuando inician sesión en sus dispositivos y las reenvía a cualquier servidor si el archivo .ica posee la configuración adecuada.

Recomendaciones para garantizar la comunicación entre el dispositivo de usuario y la Interfaz Web

Las siguientes recomendaciones combinan prácticas de seguridad estándar del sector y prácticas de seguridad proporcionadas por Citrix para proteger los datos que se envían entre los dispositivos de los usuarios y el servidor Web, y los datos que se escriben en los dispositivos de los usuarios.

Implementación de servidores Web y exploradores Web compatibles con SSL/TLS

La protección del componente de la comunicación entre el servidor Web y el explorador Web en las comunicaciones de la Interfaz Web comienza con la implementación de servidores Web y exploradores Web seguros. Muchos servidores Web seguros utilizan la tecnología SSL/TLS para proteger el tráfico de la Web.

En una transacción típica entre un servidor Web y un explorador Web, el explorador primero comprueba la identidad del servidor verificando el certificado del servidor en una lista de entidades emisoras de certificados de confianza. Después de la verificación, el explorador cifra las solicitudes de páginas del usuario y descifra los documentos devueltos por el servidor Web. En cada extremo de la transacción, la comprobación de integridad de los mensajes con TLS o SSL aseguran que no se han manipulado los datos en tránsito.

En un entorno de la Interfaz Web, el cifrado y la autenticación SSL/TLS crean una conexión segura a través de la cual el usuario puede pasar las credenciales introducidas en la página de Inicio de sesión. Los datos que se envían desde el servidor Web, incluidos los archivos .ica, las credenciales, los cookies de sesión y las páginas HTML con los conjuntos de recursos, están igualmente protegidos.

Para implementar la tecnología SSL/TLS en la red, debe contar con un servidor Web compatible con SSL/TLS y exploradores Web compatibles con SSL/TLS. El uso de estos productos es transparente para la Interfaz Web. no es necesario configurar los servidores Web ni exploradores Web para poder utilizarlos con la Interfaz Web. Para obtener más información sobre la configuración del servidor Web para su compatibilidad con SSL/TLS, consulte la documentación del servidor Web.

Importante: Muchos servidores Web compatibles con SSL/TLS usan el puerto TCP/IP 443 para las comunicaciones HTTP. De forma predeterminada, el Traspaso SSL usa también este puerto. Si el servidor Web también es el servidor que ejecuta el Traspaso SSL, asegúrese de configurar el servidor Web o el Traspaso SSL para que usen puertos diferentes.

Desactivación de la autenticación mediante paso de credenciales (PassThrough)

Para evitar que las credenciales de usuario se encaminen incorrectamente a un servidor falso o no autorizado, no habilite la autenticación mediante paso de credenciales (PassThrough) en una instalación segura. Use esta función sólo en entornos pequeños y de confianza.

Comunicación entre la Interfaz Web y el servidor Citrix

La comunicación entre la Interfaz Web y el servidor que ejecuta XenApp o XenDesktop implica el paso de información sobre credenciales de usuario y conjuntos de recursos entre la Interfaz Web y Citrix XML Service en la comunidad de servidores.

En una sesión típica, la Interfaz Web pasa las credenciales al servicio XML de Citrix para autenticar al usuario y el servicio XML de Citrix devuelve la información del conjunto de recursos disponibles. El servidor y la comunidad usan una conexión TCP/IP y el protocolo XML de Citrix para pasar la información.

Problemas de seguridad en la comunicación entre la Interfaz Web y el servidor Citrix

El protocolo XML de la Interfaz Web usa texto sin formato para intercambiar todos los datos, con excepción de las contraseñas, para cuya transmisión se usan técnicas de ofuscación. La comunicación es vulnerable a los siguientes ataques:

- Un intruso puede interceptar el tráfico XML y robar la información del conjunto de recursos y los tiquets. Un intruso con capacidad para descifrar la ofuscación también puede obtener las credenciales de usuario.
- Un intruso puede emular al servidor e interceptar las solicitudes de autenticación.

Recomendaciones para proteger la comunicación entre la Interfaz Web y el servidor Citrix

Citrix recomienda implementar alguna de las siguientes medidas de seguridad para proteger el tráfico XML transferido entre el servidor de la Interfaz Web y la comunidad de servidores:

- Use el Traspaso SSL como intermediario de seguridad entre el servidor de la Interfaz Web y la comunidad de servidores. El Traspaso SSL realiza la autenticación del host y el cifrado de datos.
- En entornos que no admiten el uso del Traspaso SSL, instale la Interfaz Web en el mismo servidor que ejecuta XenApp o XenDesktop.
- Use el protocolo HTTPS para enviar la información de la Interfaz Web mediante una conexión HTTP segura usando SSL si IIS está instalado en el servidor que ejecuta XenApp o XenDesktop.

Uso del Traspaso SSL

Actualizado: 2014-09-15

El Traspaso SSL es un componente predeterminado de XenApp y XenDesktop.

En el lado del servidor, es necesario instalar un certificado de servidor en el servidor que ejecuta el Traspaso SSL y verificar la configuración del mismo. Para obtener más información sobre la instalación de un certificado de servidor y la configuración del Traspaso SSL en los servidores, consulte Administración de XenApp. También puede consultar la ayuda de la aplicación en la herramienta de configuración del Traspaso SSL. Para los servidores XenApp para UNIX, consulte Administración del Traspaso SSL para UNIX.

Cuando configure el Traspaso SSL, asegúrese de que el servidor que ejecuta el Traspaso SSL permite el tráfico SSL a los servidores que usa como contactos del servicio XML de Citrix. De forma predeterminada, el Traspaso SSL reenvía el tráfico sólo al servidor en el que se encuentra instalado. Sin embargo, puede configurar el Traspaso SSL para reenviar el tráfico a otros servidores. Si el Traspaso SSL se encuentra en un equipo diferente del equipo al que desea enviar los datos de la Interfaz Web, asegúrese de que la lista de servidores del Traspaso SSL contenga el servidor al que quiere reenviar los datos de la Interfaz Web.

Para configurar la Interfaz Web para usar el Traspaso SSL, puede utilizar la consola Administración de la Interfaz Web de Citrix o el archivo WebInterface.conf. Para obtener más información acerca del uso de la consola para configurar la Interfaz Web de modo que utilice el Traspaso SSL, consulte Configuración de parámetros para todos los servidores de la comunidad.

Para configurar la Interfaz Web para usar el Traspaso SSL usando el archivo WebInterface.conf

1. Utilice un editor de texto y abra el archivo WebInterface.conf.
2. Cambie el valor de SSLRelayPort en el parámetro **Farm<*n*>** por el número de puerto del Traspaso SSL del servidor.
3. Cambie el valor de Transport en el parámetro **Farm<*n*>** por SSL.

Para agregar un certificado raíz nuevo en el servidor de la Interfaz Web

Si quiere permitir el uso de una determinada entidad emisora de certificados, debe agregar el certificado raíz de la entidad correspondiente en el servidor de la Interfaz Web.

Copie el certificado raíz en el servidor Web.

- En IIS, el certificado se copia usando el complemento de administración de certificados en Microsoft Management Console (MMC).

- En los servidores de aplicaciones de Java, use la herramienta de línea de comandos keytool para copiar el certificado en el directorio de almacén de claves apropiado según la plataforma utilizada. El certificado debe agregarse al almacén de claves asociado con la máquina virtual Java que sirve a las páginas Web. El almacén de claves se encuentra normalmente en una de estas ubicaciones:

  - {javax.net.ssl.trustStore}

  - {java.home}/lib/security/jssecacerts

  - {java.home}/lib/security/cacerts

Para obtener más información sobre certificados, consulte Administración de XenApp. Para los servidores XenApp para UNIX, consulte SSL Relay for UNIX Administration.

Habilitar la Interfaz Web en el servidor que ejecuta XenApp o XenDesktop

Para los entornos que no son compatibles con el Traspaso SSL, puede eliminar la posibilidad de un ataque de red ejecutando un servidor Web en el mismo servidor que suministra los datos de la Interfaz Web. El alojamiento de los sitios de la Interfaz Web en dicho servidor Web encamina todas las solicitudes de la Interfaz Web al servicio XML de Citrix del host local; de esta manera, se elimina la transmisión de los datos de la Interfaz Web a través de la red. No obstante, se deben comparar las ventajas de eliminar la transmisión por la red con el riesgo de manipulación del servidor Web.

Como primera medida, puede colocar el servidor Web y el servidor que ejecuta XenApp o XenDesktop detrás de un servidor de seguridad o firewall para que la comunicación entre ambos no esté expuesta a las condiciones abiertas de Internet. En este caso, es necesario que los dispositivos de los usuarios puedan comunicarse por medio del servidor de seguridad tanto con el servidor Web como con el servidor que ejecuta XenApp o XenDesktop. El servidor de seguridad debe permitir el tráfico HTTP para la comunicación entre el dispositivo del usuario y el servidor Web (normalmente mediante un puerto HTTP 80 estándar o 443 si se usa un servidor Web seguro). Para las comunicaciones entre el cliente y el servidor, el servidor de seguridad debe permitir el tráfico ICA entrante en los puertos 1494 y 2598. Para obtener más información sobre cómo usar ICA con servidores de seguridad o firewalls de red, consulte la documentación de su servidor Web. Para obtener más información sobre el uso de la Interfaz Web con la traducción de direcciones de red, consulte el kit de desarrollo (SDK) de la Interfaz Web.

Nota: En los sistemas que ejecutan XenApp, el programa de instalación permite obligar al servicio XML de Citrix a que comparta el puerto TCP/IP de Internet Information Services, en lugar de usar un puerto dedicado. Con XenDesktop, el programa de instalación habilita automáticamente el uso compartido de puertos. Cuando se habilita el uso compartido del puerto, el servicio XML de Citrix y el servidor Web usan el mismo puerto de forma predeterminada.

Uso del protocolo HTTPS

Puede usar el protocolo HTTPS para proteger el paso de los datos de la Interfaz Web entre el servidor Web y el servidor que ejecuta XenApp o XenDesktop. HTTPS usa SSL/TLS para proporcionar un potente cifrado de datos.

El servidor Web realiza una conexión HTTPS al IIS del servidor donde se ejecuta XenApp o XenDesktop. Esto requiere compartir el puerto IIS en el servidor que ejecuta XenApp o XenDesktop y que el IIS de dicho servidor tenga activado SSL. El nombre del servidor que usted especifica (usando la consola o mediante el parámetro **Farm<*n*>** del archivo WebInterface.conf) debe ser un nombre DNS completo que coincida con el nombre del certificado SSL del servidor IIS.

El servicio XML de Citrix se encuentra en https://*ServerName*/scripts/wpnbr.dll. Para obtener más información sobre cómo configurar la Interfaz Web para utilizar el protocolo HTTPS mediante la consola Administración de la Interfaz Web de Citrix, consulte Administración del acceso seguro.

Para configurar la Interfaz Web para el uso de HTTPS mediante el archivo WebInterface.conf

1. Utilice un editor de texto y abra el archivo WebInterface.conf.
2. Cambie el valor de Transport en el parámetro **Farm<*n*>** por HTTPS.

Comunicación entre la sesión de usuario y el servidor

La comunicación de la Interfaz Web entre los servidores y los dispositivos de los usuarios consiste en la transferencia de diversos tipos de datos de sesión, incluidas las solicitudes de inicialización y la información de la sesión.

- **Solicitudes de inicialización:** El primer paso para establecer una sesión, llamado *inicialización*, requiere que el cliente Citrix solicite una sesión y produzca una lista de parámetros de configuración de la sesión. Estos parámetros controlan diferentes aspectos de la sesión como, por ejemplo, el usuario que la inicia, el tamaño de la ventana y el programa que se ejecutará en ella.

- **Información de la sesión:** Después de la inicialización de la sesión, la información se transfiere entre el cliente Citrix y el servidor por medio de una serie de canales virtuales; por ejemplo, la entrada del mouse (del cliente al servidor) y las actualizaciones gráficas (del servidor al cliente).

Problemas de seguridad en la comunicación entre la sesión de usuario y el servidor

Para poder capturar e interpretar las comunicaciones de red entre el cliente y el servidor, un intruso debe ser capaz de descifrar el protocolo binario del cliente. Un intruso con conocimiento del protocolo binario del cliente puede:

- Interceptar la información de solicitud de inicialización enviada desde el cliente Citrix, incluidas las credenciales del usuario.

- Interceptar la información de la sesión, incluido el texto y los clics del puntero introducidos por el usuario y las actualizaciones de pantalla que se envían desde el servidor.

Recomendaciones para proteger la comunicación entre la sesión de usuario y el servidor

Citrix recomienda proteger la información que se envía entre los servidores y los dispositivos de los usuarios mediante el cifrado del tráfico o la implementación de Access Gateway.

Uso de SSL/TLS o de cifrado ICA

Citrix recomienda implementar el cifrado SSL/TLS o ICA para proteger el tráfico entre los servidores y los clientes Citrix. Ambos métodos respaldan el cifrado de 128 bits del flujo de datos entre el cliente y el servidor, pero SSL/TLS permite además la verificación de la identidad del servidor.

El respaldo para SSL se incluye en todas las versiones respaldadas de XenApp y XenDesktop. El respaldo para SSL/TLS y cifrado ICA se incluye en todas las versiones respaldadas de XenApp para Windows y XenDesktop. Para ver una lista de los clientes Citrix que soportan cada uno de estos métodos, consulte la documentación de los clientes o el sitio de descargas de Citrix. Para obtener más información sobre el cifrado ICA, consulte Administración de XenApp.

Uso de Access Gateway

Puede usar Access Gateway para proteger el tráfico entre los servidores y los clientes Citrix en Internet. Access Gateway es un dispositivo de red privada virtual (VPN) con SSL universal que ofrece un punto de acceso único y seguro a todos los recursos. Para obtener más información sobre Access Gateway, consulte la documentación de Access Gateway. Para obtener más información sobre cómo configurar la Interfaz Web para su funcionamiento con Access Gateway mediante la consola Administración de la Interfaz Web de Citrix, consulte Para configurar los parámetros de puerta de enlace.

Control del registro de diagnóstico

Utilice la tarea Registro de diagnóstico en Mantenimiento de sitios de la consola Administración de la Interfaz Web de Citrix para aumentar la seguridad del sistema para el registro de errores. Puede evitar que se repitan registros duplicados de sucesos y configurar el número exacto de duplicados de sucesos que deben registrarse y con qué frecuencia.

Mediante esta tarea también es posible especificar la URL requerida para la redirección de errores. Si especifica una URL de respuesta de error personalizada, debe gestionar todas las ID de error con esa URL y suministrar mensajes de error a los usuarios. Además, esta URL de respuesta de error sustituirá a la pantalla de cierre de sesión del usuario, incluso cuando los usuarios cierren la sesión sin que se produzcan errores.

Configuración de sitios mediante el archivo de configuración

Archivos de configuración de sitios

Los sitios de la Interfaz Web incluyen un archivo denominado WebInterface.conf, que contiene la información de configuración del sitio. Puede usar este archivo para realizar tareas diarias de administración y personalizar los parámetros de un sitio. Por ejemplo, puede especificar los parámetros que los usuarios pueden cambiar y puede configurar la autenticación en la Interfaz Web.

Si introduce un valor no válido para un parámetro cuando modifica un archivo de configuración y después usa la consola Administración de la Interfaz Web de Citrix, la consola reemplazará el valor no válido por el valor predeterminado cuando se guarde el archivo.

Si se ejecuta la consola Administración de la Interfaz Web de Citrix mientras se modifica manualmente el archivo de configuración, los cambios posteriores realizados mediante la consola sobrescribirán todas las modificaciones efectuadas en el archivo de configuración. Citrix recomienda cerrar la consola Administración de la Interfaz Web de Citrix antes de modificar los archivos de configuración de los sitios. Si esto no es posible, actualice la consola para aplicar las modificaciones realizadas manualmente en el archivo de configuración antes de efectuar otros cambios mediante la consola.

El archivo WebInterface.conf está disponible en el directorio de configuración de sitios:

- En Microsoft Internet Information Services (IIS), se encuentra normalmente en el directorio C:\inetpub\wwwroot\Citrix*SiteName*\conf
- En los servidores de aplicaciones de Java, como Apache Tomcat, la ubicación puede ser ./usr/local/tomcat/webapps/Citrix/XenApp/WEB-INF

Es posible sobrescribir algunos valores de configuración en WebInterface.conf para algunas páginas en los scripts del servidor Web. Para obtener más información sobre los scripts o archivos de comandos del servidor Web, consulte el kit de desarrollo (SDK) de la Interfaz Web.

Nota: en los servidores de aplicaciones de Java, es posible que tenga que detener y reiniciar el servidor Web para que se apliquen los cambios hechos en WebInterface.conf. Asegúrese de guardar los cambios respetando el formato de codificación UTF-8.

Parámetros de WebInterface.conf

Actualizado: 2014-06-03

La siguiente tabla muestra los parámetros que puede contener el archivo WebInterface.conf (por orden alfabético). Los valores predeterminados aparecen en **negrita**. Si alguno de los parámetros en WebInterface.conf no se especifica, se utilizará su valor predeterminado.

AccountSelfServiceUrl

- Descripción: Especifica la dirección URL del servicio Password Manager.
- Valor: Una URL válida con HTTPS
- Tipo de sitio: Web XenApp

Autenticaciónexplícitaadicional

- Descripción: Especifica la autenticación explícita de dos factores que debe realizarse además de SAM, ADS o NDS.
- Valor: None | SecurID | SafeWord | RADIUS
- Tipo de sitio: Web XenApp

Tipo de resoluciónde dirección

- Descripción: Especifica el tipo de dirección que se va a utilizar en el archivo .ica de inicio.
- Valor: dns-port | dns | ipv4-port | ipv4
- Tipo de sitio: Web XenApp y Servicios XenApp

AGAuthenticationMethod

- Descripción: Especifica los métodos de autenticación permitidos para los sitios integrados de Access Gateway. Este parámetro se debe establecer en Explicit si los usuarios inician sesión en Access Gateway con un nombre de usuario y una contraseña. Si los usuarios inician sesión con una tarjeta inteligente en Access Gateway y este parámetro se establece en SmartCard, los usuarios deberán introducir un PIN todas las veces que accedan a un recurso. La opción SmartCardKerberos permite que los usuarios inicien sesión en Access Gateway con una tarjeta inteligente para acceder a sus recursos sin proporcionar un PIN.
- Valor: Explicit | SmartCard | SmartCard Kerberos
- Tipo de sitio: Web XenApp

AGEPromptPassword

- Descripción: Especifica si se pide o no a los usuarios que vuelvan a introducir sus contraseñas al iniciar la sesión desde la página de inicio de sesión de Access Gateway.
- Valor: Off | On
- Tipo de sitio: Web XenApp

AGEWebServiceURL

- Descripción: Especifica la dirección URL del servicio de autenticación de Access Gateway.
- Valor: Una URL válida
- Tipo de sitio: Web XenApp

AllowBandwidthSelection

- Descripción: Especifica si se permite a los usuarios indicar la velocidad de su conexión de red de forma que puedan optimizarse los parámetros ICA.
- Valor: Off | On
- Tipo de sitio: Web XenApp

AllowCustomizeAudio

- Descripción: Especifica si los usuarios pueden o no ajustar la calidad de sonido de sus sesiones ICA.
- Valor: Off | On
- Tipo de sitio: Web XenApp

AllowCustomizeAutoLogin

- Descripción: Especifica si se permite a los usuarios activar y desactivar el inicio de sesión automático.
- Valor: On | Off
- Tipo de sitio: Web XenApp

AllowCustomizeClientPrinterMapping

- Descripción: Especifica si se permite a los usuarios activar y desactivar la asignación de impresoras de cliente.
- Valor: Off | On
- Tipo de sitio: Web XenApp

AllowCustomizeJavaClientPackages

- Descripción: Especifica si se permite a los usuarios elegir los paquetes del Cliente para Java que quieran usar.

- Valor: Off | On
- Tipo de sitio: Web XenApp

AllowCustomizeLayout

- Descripción: Especifica si se permite a los usuarios elegir si usar una interfaz de usuario con gráficos o sin gráficos.
- Valor: Off | On
- Tipo de sitio: Web XenApp

AllowCustomizeLogoff

- Descripción: Especifica si se permite a los usuarios sobrescribir el comportamiento de control de área de trabajo cuando cierran sesión en el servidor.
- Valor: On | Off
- Tipo de sitio: Web XenApp

AllowCustomizePersistFolderLocation

- Descripción: Especifica si se permite a los usuarios activar y desactivar la opción de volver a la última carpeta visitada en la pantalla Aplicaciones la próxima vez que inicien sesión.
- Valor: Off | On
- Tipo de sitio: Web XenApp

AllowCustomizeReconnectAtLogin

- Descripción: Especifica si se permite a los usuarios sobrescribir el comportamiento de control del área de trabajo al iniciar sesión.
- Valor: On | Off
- Tipo de sitio: Web XenApp

AllowCustomizeReconnectButton

- Descripción: Especifica si se permite a los usuarios sobrescribir el comportamiento de control del área de trabajo al hacer clic en el botón Reconectar.
- Valor: On | Off
- Tipo de sitio: Web XenApp

AllowCustomizeSettings

- Descripción: Especifica si se permite a los usuarios personalizar sus sesiones en la Interfaz Web. Cuando el parámetro está en Off, el botón Preferencias no aparece en las pantallas de Inicio de sesión y Aplicaciones de los usuarios.

- Valor: On | Off
- Tipo de sitio: Web XenApp

AllowCustomizeShowHints

- Descripción: Especifica si se permite a los usuarios mostrar y ocultar sugerencias en la pantalla Aplicaciones.
- Valor: On | Off
- Tipo de sitio: Web XenApp

AllowCustomizeShowSearch

- Descripción: Especifica si se permite a los usuarios habilitar e inhabilitar la opción de búsqueda en la pantalla Aplicaciones.
- Valor: Off | On
- Tipo de sitio: Web XenApp

AllowCustomizeSpecialFolderRedirection

- Descripción: Especifica si se permite a los usuarios habilitar y deshabilitar la función de redirección de carpetas especiales.
- Valor: Off | On
- Tipo de sitio: Web XenApp

AllowCustomizeTransparentKeyPassthrough

- Descripción: Especifica si se permite a los usuarios seleccionar el comportamiento del paso de combinaciones de teclas.
- Valor: Off | On
- Tipo de sitio: Web XenApp

AllowCustomizeVirtualCOMPortEmulation

- Descripción: Especifica si se permite a los usuarios habilitar e inhabilitar la sincronización de PDA.
- Valor: Off | On
- Tipo de sitio: Web XenApp

AllowCustomizeWinColor

- Descripción: Especifica si se permite a los usuarios cambiar la profundidad de color de las sesiones ICA.
- Valor: Off | On

- Tipo de sitio: Web XenApp

AllowCustomizeWinSize

- Descripción: Especifica si se permite a los usuarios cambiar el tamaño de ventana de las sesiones ICA.
- Valor: On | Off
- Tipo de sitio: Web XenApp

AllowDisplayInFrames

- Descripción: Especifica si se pueden mostrar los sitios Web XenApp dentro de los cuadros incrustados en páginas Web de terceros.
- Valor: On | Off
- Tipo de sitio: Web XenApp

AllowFontSmoothing

- Descripción: Especifica si se permite el suavizado de fuentes en las sesiones ICA.
- Valor: On | Off
- Tipo de sitio: Web XenApp y Servicios XenApp

AllowUserAccountUnlock

- Descripción: Especifica si se permite a los usuarios desbloquear sus cuentas utilizando el autoservicio de cuentas.
- Valor: Off | On
- Tipo de sitio: Web XenApp

AllowUserPasswordChange

- Descripción: Especifica bajo qué condiciones los usuarios pueden cambiar sus contraseñas.
- Valor: Never | Expired-Only | Always (sólo sitios Web XenApp)
- Tipo de sitio: Web XenApp y Servicios XenApp

AllowUserPasswordReset

- Descripción: Especifica si se permite a los usuarios restablecer sus contraseñas utilizando el autoservicio de cuentas.
- Valor: Off | On
- Tipo de sitio: Web XenApp

AlternateAddress

- Descripción: Especifica si es preciso devolver la dirección del servidor alternativo en el archivo .ica.
- Valor: Off | Mapped | On
- Tipo de sitio: Web XenApp y Servicios XenApp

ApplicanceEmbeddedSmartCardSSO

- Descripción: Especifica si la autenticación con tarjeta inteligente debe utilizar el control ActiveX incrustado para el inicio de sesión único.
- Valor: Off | On
- Tipo de sitio: Desktop Appliance Connector

ApplianceEmbeddedSmartCardSSOPinTimeout

- Descripción: La cantidad de segundos que la pantalla de entrada de PIN para la autenticación con tarjeta inteligente incrustada espera antes de regresar a la pantalla de inicio de sesión cuando se encuentra inactiva.
- Valor: 20
- Tipo de sitio: Desktop Appliance Connector

ApplianceMultiDesktop

- Descripción: Especifica si la lista de escritorios se debe mostrar en caso de que los usuarios tengan varios escritorios asignados a ellos.
- Valor: Off | On
- Tipo de sitio: Desktop Appliance Connector

ApplicationAccessMethods

- Descripción: Especifica si los usuarios pueden acceder a las aplicaciones mediante un cliente para recursos en línea, Citrix offline plug-in, o ambos.
- Valor: Remote, Streaming
- Tipo de sitio: Web XenApp y Servicios XenApp

AppSysMessage _<*código de idioma*>

- Descripción: Especifica el texto traducido que aparecerá en la parte inferior del área principal de contenido de la pantalla de aplicaciones. *LanguageCode* puede ser en, de, es, fr, ja, o cualquier otro identificador de idioma compatible.
- Valor: None. Texto sin formato más cualquier número de etiquetas e hipervínculos HTML de línea nueva
- Tipo de sitio: Web XenApp

AppTab<*n*>

- Descripción: Especifica las fichas que se mostrarán en la pantalla de aplicaciones. Se pueden usar varias instancias para definir varias fichas. O bien, se puede definir una ficha única que contenga todos los recursos disponibles para el usuario usando el valor AllResources.
- Valor: Applications | Desktops | Content | AllResources
- Tipo de sitio: Web XenApp

AppWelcome Message _<*código de idioma*>

- Descripción: Especifica el texto traducido que aparecerá en la parte superior del área principal de contenido de la pantalla de aplicaciones. *LanguageCode* puede ser en, de, es, fr, ja, o cualquier otro identificador de idioma compatible.
- Valor: None. Texto sin formato más cualquier número de etiquetas e hipervínculos HTML de línea nueva
- Tipo de sitio: Web XenApp

AuthenticationPoint

- Descripción: Especifica dónde tiene lugar la autenticación del usuario.
- Valor: WebInterface | ADFS | AccessGateway | 3rdParty | WebServer
- Tipo de sitio: Web XenApp

AutoLaunchDesktop

- Descripción: Especifica si se debe activar el acceso automático a los escritorios. Cuando este parámetro se establece en On, la Interfaz Web inicia automáticamente el escritorio del usuario si este es el único recurso disponible en todas las comunidades.
- Valor: Off | On
- Tipo de sitio: Web XenApp

AutoLoginDefault

- Descripción: Especifica si se habilitan los inicios de sesión automáticos de manera predeterminada para los usuarios que acceden a sus recursos mediante la autenticación por paso de credenciales (PassThrough), por paso de credenciales con tarjeta inteligente o solo con tarjeta inteligente.
- Valor: On | Off
- Tipo de sitio: Web XenApp

BrandingColor

- Descripción: Especifica el color para las zonas de encabezado y pie de página.
- Valor: Color (nombre o número hexadecimal)
- Tipo de sitio: Web XenApp

BrandingImage

- Descripción: Especifica la dirección URL de la imagen que se desea mostrar en las zonas de encabezado y pie de página.
- Valor: Una URL válida
- Tipo de sitio: Web XenApp

BypassFailedRadiusServerDuration

- Descripción: Especifica el periodo de tiempo que debe transcurrir antes de intentar volver a utilizar un servidor RADIUS que no responde.
- Valor: Tiempo en minutos (60)
- Tipo de sitio: Web XenApp

BypassFailedSTADuration

- Descripción: Especifica el período de tiempo que debe transcurrir antes de intentar reutilizar un servidor en el que se produjo un fallo y que ejecuta Secure Ticket Authority para un dispositivo de puerta de enlace.
- Valor: Tiempo en minutos (60)
- Tipo de sitio: Web XenApp

ClientAddressMap

- Descripción: Especifica pares de dirección de cliente y tipo de dirección para la configuración del firewall (servidor de seguridad) del servidor. El primer campo de la entrada es una dirección y máscara de subred; el segundo campo puede tomar los valores siguientes: Normal, Alternate, Translated, SG, SGAlternate y SGTranslated. El uso de un asterisco (*) en lugar de una dirección de cliente o subred indica el valor predeterminado para todos los clientes Citrix que no se hayan especificado.
- Valor: <*Dirección de subred*>/ <*Máscara de subred*> |*, Normal | Alternate | Translated | SG | SGTranslated | SGAlternate, …
- Tipo de sitio: Web XenApp

ClientDefaultURL

- Descripción: Especifica la dirección URL a la que el proceso de detección e instalación de clientes redirige a los usuarios cuando el cliente adecuado no está disponible para la descarga.
- Valor: http://www. citrix.com/ download. Dirección URL válida.
- Tipo de sitio: Web XenApp

ClientIcaLinuxX86

ClientIcaMac

ClientIcaSolarisSparc

ClientIcaSolarisX86

ClientIcaWin32

ClientStreamingWin32

- Descripción: Configura el proceso de detección e instalación de clientes para la plataforma especificada. Si no se ha configurado el parámetro adecuado, los usuarios son redirigidos a la página Web especificada en el parámetro ClientDefaultURL. De manera predeterminada, estos parámetros se configuran para los clientes nativos suministrados en el soporte de instalación de XenApp 6.0.

  Los dos primeros campos especifican la ubicación y el nombre de archivo del programa de instalación del cliente. Si no se encuentra el archivo, los usuarios son redirigidos a la página Web especificada en el parámetro ClientDefaultURL.

  El campo Mui indica si el cliente especificado en los campos Directory y Filename puede usarse en varios idiomas. Si el valor está establecido en No, el proceso de detección e instalación de clientes busca el archivo especificado en la carpeta <*LanguageCode*>\<*FolderName*>.

  El campo Version presenta el número de versión, separado por comas, del cliente especificado en los campos Directory y Filename. Si no se especifica ningún número de versión, el proceso de detección e instalación de clientes intenta determinar la versión a partir del archivo especificado.

  El campo ShowEULA indica si los usuarios tienen que aceptar el Contrato de licencia de Citrix para poder instalar el cliente especificado.

  El campo ClassID especifica el ID de clase de los clientes para Windows y es un parámetro obligatorio para dichos clientes.

  El campo Url especifica la página Web a la que se redirige a los usuarios cuando hacen clic en el botón Descargar y no se ha especificado ningún archivo de cliente en los campos Directory y Filename. Este parámetro sólo debe usarse cuando no haya ningún archivo de cliente disponible.

  El campo Description especifica el mensaje personalizado que se muestra sobre el botón Descargar. El texto no está traducido a ningún idioma.

- Valor: Directory: <*nombre de carpeta*>, Filename: <*nombre de archivo*>, [Mui:Yes | No,] [Version: <*número de versión*>,] [ShowEULA: Yes | No,] [ClassID: <*Valor*>,] [Url: <*URL válida*>,] [Description: <*descripción*>]

- Tipo de sitio: Web XenApp

ClientProxy

- Descripción: Especifica direcciones de subred y máscaras de red de cliente y los parámetros de proxy asociados para el firewall (servidor de seguridad) del cliente. La dirección de cliente del archivo ICA devuelto está determinada por estos parámetros. Cada entrada consta de tres campos. El primero es una máscara y dirección de subred. El uso de un asterisco (*) indica el valor predeterminado para los clientes Citrix que no se hayan especificado. El segundo campo es uno de los seis tipos de proxy. El valor del

tercer campo (dirección del proxy) en cada grupo de tres se ignora, a menos que el segundo campo (tipo de proxy) sea explícito (SOCKS o Secure), aunque debe estar presente siempre. El valor predeterminado para este campo es el signo menos (-).

- Valor: <*Dirección de subred*>/ <*Máscara de subred*> |*, Auto | WpadAuto | Client | None | SOCKS | Secure, - | <*Dirección del proxy*> | <*Dirección del proxy*>: <*Puerto del proxy*>, …
- Tipo de sitio: Web XenApp y Servicios XenApp

CompactHeaderImage

- Descripción: Especifica la dirección URL de la imagen del encabezado para la versión sin gráficos de la interfaz de usuario.
- Valor: Una URL válida
- Tipo de sitio: Web XenApp

CompactViewStyles

- Descripción: Especifica los estilos de vista disponibles para el usuario en la pantalla de aplicaciones en la interfaz de usuario sin gráficos.
- Valor: Icons, List
- Tipo de sitio: Web XenApp

CredentialFormat

- Descripción: Especifica los formatos de credenciales aceptados para inicios de sesión Windows y NIS explícitos.
- Valor: All | UPN | DomainUsername
- Tipo de sitio: Web XenApp y Servicios XenApp

CSG_EnableSessionReliability

- Descripción: Especifica si se debe utilizar la fiabilidad de la sesión con Access Gateway o Secure Gateway.
- Valor: On | Off
- Tipo de sitio: Web XenApp y Servicios XenApp

CSG_Server

- Descripción: Especifica la dirección del dispositivo Access Gateway o del servidor Secure Gateway.
- Valor: None. Dirección del servidor como nombre completo de dominio (FQDN)
- Tipo de sitio: Web XenApp y Servicios XenApp

CSG_ServerPort

- Descripción: Especifica el puerto del dispositivo Access Gateway o del servidor Secure Gateway.
- Valor: None. Puerto servidor
- Tipo de sitio: Web XenApp y Servicios XenApp

CSG_STA_URL<*n*>

- Descripción: Especifica la dirección URL del servidor que ejecuta Secure Ticket Authority para un dispositivo de puerta de enlace.
- Valor: None. Dirección URL de un Secure Ticket Authority (STA)
- Tipo de sitio: Web XenApp y Servicios XenApp

CSG_UseTwoTickets

- Descripción: Especifica si la Interfaz Web debe solicitar tiquets de dos Secure Ticket Authorities distintas cuando se acceda a un recurso mediante Access Gateway.
- Valor: Off | On
- Tipo de sitio: Web XenApp y Servicios XenApp

DefaultAudioQuality

- Descripción: Especifica la calidad del sonido predeterminada que se utilizará con las conexiones ICA.
- Valor: NoPreference | High | Medium | Low | Off
- Tipo de sitio: Web XenApp

DefaultBandwidthProfile

- Descripción: Especifica el perfil del ancho de banda predeterminado (es decir, el conjunto de parámetros relacionados con el ancho de banda, como la calidad del sonido y la profundidad del color) que se utilizará con las conexiones ICA.
- Valor: Custom | High | Medium High | Medium | low
- Tipo de sitio: Web XenApp

DefaultColorDepth

- Descripción: Especifica la profundidad del color predeterminada que se utilizará con las conexiones ICA.
- Valor: NoPreference | TrueColor | HighNoPreferenceColor
- Tipo de sitio: Web XenApp

DefaultCompactViewStyle

- Descripción: Especifica el estilo de vista predeterminado para la pantalla de aplicaciones en la interfaz de usuario sin gráficos.
- Valor: List | Icons
- Tipo de sitio: Web XenApp

DefaultCustomTextLocale

- Descripción: Especifica el código del idioma predeterminado para el texto personalizado. Es necesario especificar el mismo código de idioma en todos los parámetros de texto personalizados (*_<*LanguageCode*>) que estén definidos.
- Valor: None. en | de | es | fr | ja | cualquier otro identificador de idioma compatible
- Tipo de sitio: Web XenApp

DefaultPrinterMapping

- Descripción: Especifica si se debe activar la asignación de impresoras de forma predeterminada para las conexiones ICA.
- Valor: On | Off
- Tipo de sitio: Web XenApp

DefaultViewStyle

- Descripción: Especifica el estilo de vista predeterminado para la pantalla de aplicaciones en la interfaz de usuario con gráficos.
- Valor: Icons | Details | Groups | List | Tree
- Tipo de sitio: Web XenApp

DefaultWindowSize

- Descripción: Especifica el modo de la ventana predeterminado que se utilizará para las sesiones ICA. Se puede especificar como un porcentaje del área de la pantalla total mediante el formato X% o con dimensiones personalizadas de tamaño fijas mediante el formato XxY
- Valor: FullScreen | Seamless | X% | XxY
- Tipo de sitio: Web XenApp

DisplayBrandingImage

- Descripción: Especifica si se mostrará una imagen de marca para las zonas de encabezado y pie de página.
- Valor: On | Off
- Tipo de sitio: Web XenApp

DomainSelection

- Descripción: Especifica los nombres de dominio mostrados en la pantalla de Inicio de sesión para la autenticación explícita.
- Valor: Lista de nombres de dominio NetBIOS
- Tipo de sitio: Web XenApp y Servicios XenApp

DuplicateLogInterval

- Descripción: Especifica el periodo de tiempo durante el que se controlan las entradas de registro DuplicateLogLimit.
- Valor: Tiempo en segundos (60)
- Tipo de sitio: Web XenApp y Servicios XenApp

DuplicateLogLimit

- Descripción: Especifica el número de entradas de registro duplicadas permitidas durante el periodo de tiempo especificado en DuplicateLogInterval.
- Valor: Número entero mayor que 0 (10)
- Tipo de sitio: Web XenApp y Servicios XenApp

EnableFileTypeAssociation

- Descripción: Especifica si la asociación de tipos de archivos está habilitada o inhabilitada para un sitio. Si el parámetro está en Off, la redirección de contenido no está disponible para el sitio.
- Valor: On | Off
- Tipo de sitio: Web XenApp y Servicios XenApp

EnableKerberosToMPS

- Descripción: Especifica si la autenticación Kerberos está habilitada o no.
- Valor: Off | On
- Tipo de sitio: Web XenApp y Servicios XenApp

EnableLegacyICAClientSupport

- Descripción: Especifica si se respaldan clientes Citrix anteriores que no pueden leer archivos .ica codificados con UTF-8. Si el parámetro está en Off, el servidor produce archivos .ica codificados con UTF-8.
- Valor: Off | On
- Tipo de sitio: Web XenApp y Servicios XenApp

EnableLogoffApplications

- Descripción: Especifica si la función de control del área de trabajo cierra la sesión en los recursos activos cuando los usuarios cierran sesión en el servidor.
- Valor: On | Off
- Tipo de sitio: Web XenApp

EnablePassthroughURLs

- Descripción: Especifica si los usuarios pueden crear enlaces persistentes a los recursos a los que acceden mediante la Interfaz Web.
- Valor: Off | On
- Tipo de sitio: Web XenApp

EnableRadiusServerLoadBalancing

- Descripción: Especifica si se debe equilibrar la carga de las sesiones entre los servidores RADIUS configurados. El respaldo entre servidores sigue existiendo independientemente de cómo se defina este parámetro.
- Valor: Off | On
- Tipo de sitio: Web XenApp

EnableSTALoadBalancing

- Descripción: Especifica si se debe equilibrar la carga de las solicitudes entre los servidores Secure Ticket Authority configurados para un dispositivo de puerta de enlace.
- Valor: Off | On
- Tipo de sitio: Web XenApp y Servicios XenApp

EnableVirtualCOMPortEmulation

- Descripción: Especifica si debe o no activarse la sincronización de PDA mediante conexiones USB con cable.
- Valor: Off | On
- Tipo de sitio: Web XenApp

EnableWizardAutoMode

- Descripción: Especifica si el proceso de detección e instalación de clientes se ejecuta en modo automático.
- Valor: On | Off
- Tipo de sitio: Web XenApp

EnableWorkspaceControl

- Descripción: Especifica si la funcionalidad de control del área de trabajo está disponible para los usuarios.
- Valor: On | Off
- Tipo de sitio: Web XenApp

ErrorCallbackURL

- Descripción: Especifica una dirección URL para redirección de la Interfaz Web al producirse un error. La página Web a la que hace referencia la URL debe aceptar y procesar cuatro parámetros de cadena de consulta:

  CTX_MessageType

  CTX_MessageKey

  CTX_MessageArgs

  CTX_LogEventID

- Valor: Una URL válida
- Tipo de sitio: Web XenApp

Farm<*n*>

- Descripción: Especifica toda la información para una comunidad. Puede configurarse un máximo de 512 comunidades.
- Valor: Dirección de Citrix XML Service [,Dirección de Citrix XML Service,] [,Name:<*nombre*>] [,XMLPort: <*puerto*>] [,Transport: <HTTP | HTTPS | SSL>] [,SSLRelayPort: <*Puerto*>] [,Bypass Duration: <*Minutos* (60)>] [,LoadBalance: <off | on>] [,TicketTime ToLive: <*Segundos* (200)>] [,RADETicket TimeToLive: <*Segundos* (200)>]
- Tipo de sitio: Web XenApp y Servicios XenApp

Farm<*n*>Groups

- Descripción: Especifica los grupos de Active Directory que pueden enumerar los recursos de las comunidades de servidores. Si se incluye un valor para este parámetro, se activa la función de perfil móvil del usuario. Se puede especificar un máximo de 512 grupos de usuarios para cada comunidad definida con el parámetro Farm<*n*>.
- Valor: None. *Domain*\ *UserGroup*[,...]
- Tipo de sitio: Web XenApp, Servicios XenApp y XenDesktop

FooterText _<*Language Code*>

- Descripción: Especifica el texto traducido que aparecerá en la zona de pie de página de todas las páginas. *LanguageCode* puede ser en, de, es, fr, ja, o cualquier otro identificador de idioma compatible.
- Valor: None. Texto sin formato más cualquier número de etiquetas e hipervínculos HTML de línea nueva

- Tipo de sitio: Web XenApp

HeaderFontColor

- Descripción: Especifica el color de la fuente para el área del encabezado.
- Valor: Color (nombre o número hexadecimal)
- Tipo de sitio: Web XenApp

HeadingHomePage

- Descripción: Especifica la dirección URL de la imagen para el encabezado de la página principal.
- Valor: Una URL válida
- Tipo de sitio: Web XenApp

HeadingImage

- Descripción: Especifica la dirección URL de la imagen para el encabezado de la Interfaz Web.
- Valor: Una URL válida
- Tipo de sitio: Web XenApp

HideDomainField

- Descripción: Especifica si el campo Dominio aparecerá en la página de Inicio de sesión.
- Valor: Off | On
- Tipo de sitio: Web XenApp

IcaFileSigningCertificateThumbprint

- Descripción: Los sellos de los certificados que se utilizarán para la firma de archivos ICA.
- Valor: None. Los sellos pueden contener espacios
- Tipo de sitio: Web XenApp y Desktop Appliance Connector

IcaFileSigningEnabled

- Descripción: Activa o desactiva la función de firma de archivos ICA.
- Valor: Off | On
- Tipo de sitio: Web XenApp y Desktop Appliance Connector

IcaFileSigningHashAlgorithm

- Descripción: El algoritmo hash que se utilizará en la firma de archivos ICA.

- Valor: SHA1 | SHA256
- Tipo de sitio: Web XenApp y Desktop Appliance Connector

IgnoreClientProvidedClientAddress

- Descripción: Especifica si debe omitirse la dirección suministrada por el cliente Citrix.
- Valor: Off | On
- Tipo de sitio: Web XenApp y Servicios XenApp

InternalServerAddressMap

- Descripción: Especifica pares de direcciones normales/traducidas. La dirección normal identifica al servidor con el que se comunica la puerta de enlace, y se devuelve la dirección traducida al cliente Citrix.
- Valor: DirecciónNormal = DirecciónTraducida, …
- Tipo de sitio: Web XenApp y Servicios XenApp

JavaClientPackages

- Descripción: Especifica el conjunto predeterminado de paquetes del Cliente para Java que se ponen a disposición de los usuarios.
- Valor: ClipBoard, ConfigUI, PrinterMapping, SecureICA, SSL, Audio, ClientDriveMapping, ZeroLatency
- Tipo de sitio: Web XenApp

JavaFallbackMode

- Descripción: Especifica si se recurrirá al Cliente para Java cuando los usuarios no tengan instalado un cliente nativo. Este parámetro sólo se aplica cuando el valor Ica-Local está incluido en el parámetro LaunchClients. Con el valor Manual se permite a los usuarios elegir si quieren intentar usar el Cliente para Java.
- Valor: None | Manual | Auto
- Tipo de sitio: Web XenApp

KioskMode

- Descripción: Especifica si los parámetros del usuario deben guardarse permanentemente o si, por el contrario, deben aplicarse sólo mientras dure la sesión. Cuando está activado este modo, los parámetros del usuario sólo se conservan mientras dura la sesión.
- Valor: Off | On
- Tipo de sitio: Web XenApp

LaunchClients

- Descripción: Especifica los clientes Citrix que pueden seleccionar los usuarios. Este parámetro se ignora en los sitios de modo dual, para los que el valor es siempre Ica-Local. La omisión del valor Ica-Java no impide que se ofrezca a los usuarios el Cliente para Java. Para ello también habría que definir el parámetro JavaFallbackMode con el valor None.

- Valor: Ica-Local, Ica-Java, Rdp-Embedded

- Tipo de sitio: Web XenApp

LoginDomains

- Descripción: Especifica los nombres de dominio utilizados para restringir el acceso.

- Valor: Lista de nombres de dominio NetBIOS

- Tipo de sitio: Web XenApp y Servicios XenApp

LoginSys Message _<*código de idioma*>

- Descripción: Especifica el texto traducido que aparecerá en la parte inferior del área principal de contenido de la pantalla de Inicio de sesión. *LanguageCode* puede ser en, de, es, fr, ja, o cualquier otro identificador de idioma compatible.

- Valor: None. Texto sin formato más cualquier número de etiquetas e hipervínculos HTML de línea nueva

- Tipo de sitio: Web XenApp

LoginTitle _<*Language Code*>

- Descripción: Especifica el texto traducido que aparecerá sobre el mensaje de bienvenida en la pantalla de Inicio de sesión. *LanguageCode* puede ser en, de, es, fr, ja, o cualquier otro identificador de idioma compatible.

- Valor: None. Texto sin formato más cualquier número de etiquetas e hipervínculos HTML de línea nueva

- Tipo de sitio: Web XenApp

LoginType

- Descripción: Especifica el tipo de pantalla de Inicio de sesión que se muestra a los usuarios. La pantalla de Inicio de sesión puede estar basada en sistema de dominios o en NDS.

- Valor: Default | NDS

- Tipo de sitio: Web XenApp y Servicios XenApp

LogoffFederationService

- Descripción: Especifica si se cierra la sesión de los usuarios sólo de los sitios Web XenApp, o si se cierra globalmente la sesión de los servicios de federación cuando se hace clic en el botón Cerrar sesión en un sitio integrado con AD FS.

- Valor: On | Off
- Tipo de sitio: Web XenApp

MultiFarmAuthenticationMode

- Descripción: Este modo tiene tres opciones para especificar el método de autenticación permitido. La opción “All” es la predeterminada; con ella, todas las comunidades se autentican para enumerar cualquier aplicación. La opción “Any” permite la enumeración de aplicaciones desde cualquier comunidad para el usuario autenticado; no obstante, si el usuario introduce sus credenciales incorrectamente, éstas se presentan en todas las comunidades para la autenticación, aunque ésta falle en alguna de las comunidades. Esto puede hacer que la cuenta se bloquee. La opción “Primary” permite al usuario autenticarse en la comunidad principal (la primera de la lista configurada en la Interfaz Web); si no es posible, se pasa al modo “Any”. Con esta opción se intenta evitar que las cuentas se bloqueen.
- Valor: All | Any | Primary
- Tipo de sitio: Web XenApp

MultiLaunchTimeout

- Descripción: Especifica el tiempo durante el cual los iconos de los recursos permanecen inactivos después del clic inicial que los usuarios realizan al iniciar el recurso.
- Valor: Tiempo en segundos (2)
- Tipo de sitio: Web XenApp

NDSContextLookupLoadbalancing

- Descripción: Especifica si se debe equilibrar la carga de las solicitudes NDS entre los servidores LDAP configurados. El respaldo entre servidores sigue existiendo independientemente de cómo se defina este parámetro.
- Valor: Off | On
- Tipo de sitio: Web XenApp

NDSContextLookupServers

- Descripción: Especifica los servidores LDAP que se deben utilizar. Si no se especifica el puerto, se deduce del protocolo: Si el parámetro está definido en ldap, se usa el puerto LDAP predeterminado (389); si el parámetro es ldaps, se usa el puerto LDAP sobre SSL predeterminado (636). Puede configurarse un máximo de 512 servidores LDAP.

  Si este parámetro no existe o no se ha definido, se inhabilitan los inicios de sesión sin contexto.
- Valor: None. ldap://[:] | ldaps://[:],
- Tipo de sitio: Web XenApp

NDSTreeName

- Descripción: Especifica el árbol NDS que debe usarse con la autenticación NDS.
- Valor: None. Nombre de árbol NDS
- Tipo de sitio: Web XenApp y Servicios XenApp

OverlayAutologonCredsWithTicket

- Descripción: Especifica si hay que duplicar un tiquet de inicio de sesión en una entrada de tiquet de inicio de sesión o ubicarlo sólo en una entrada de tiquet de archivo de inicio .ica independiente. Cuando se habilita la superposición de credenciales, se duplican los tiquets de inicio de sesión.
- Valor: On | Off
- Tipo de sitio: Web XenApp

OverrideIcaClientname

- Descripción: Especifica si se debe transferir o no una ID generada por la Interfaz Web en la entrada del nombre del cliente de un archivo .ica de inicio.
- Valor: Off | On
- Tipo de sitio: Web XenApp

PasswordExpiryWarningPeriod

- Descripción: Especifica cuántos días antes de que caduque una contraseña se pedirá al usuario que la cambie.
- Valor: Número entero entre 0 y 999 (14)
- Tipo de sitio: Web XenApp

PersistFolderLocation

- Descripción: Especifica si los usuarios vuelven a la última carpeta visitada en la pantalla de aplicaciones cuando inician de nuevo sesión.
- Valor: Off | On
- Tipo de sitio: Web XenApp

PNAChangePasswordMethod

- Descripción: Especifica el comportamiento de Citrix online plug-in ante las solicitudes de cambio de contraseña de los usuarios. Si este parámetro se define como Direct-Only, el plug-in cambia la contraseña comunicándose directamente con el controlador de dominio. Direct-With-Fallback indica que el plug-in primero intenta establecer comunicación con el controlador de dominio, pero utiliza el sitio de servicios XenApp si dicha comunicación falla. La opción Proxy indica que el plug-in cambia contraseñas poniéndose en contacto con el sitio de servicios XenApp.
- Valor: Direct-Only | Direct-With- Fallback | Proxy

- Tipo de sitio: Servicios XenApp

PooledSockets

- Descripción: Especifica si se usa o no una agrupación de sockets.
- Valor: On | Off
- Tipo de sitio: Web XenApp y Servicios XenApp

PreLoginMessageButton _<*código de idioma*>

- Descripción: Especifica un nombre traducido para el botón de confirmación de mensajes de pre-inicio de sesión. *LanguageCode* puede ser en, de, es, fr, ja, o cualquier otro identificador de idioma compatible.
- Valor: None. Texto sin formato más cualquier número de etiquetas e hipervínculos HTML de línea nueva
- Tipo de sitio: Web XenApp

PreLoginMessageText _<*código de idioma*>

- Descripción: Especifica el texto traducido para que aparezca en la página de mensajes de pre-inicio de sesión. *LanguageCode* puede ser en, de, es, fr, ja, o cualquier otro identificador de idioma compatible.
- Valor: None. Texto sin formato más cualquier número de etiquetas e hipervínculos HTML de línea nueva
- Tipo de sitio: Web XenApp

PreLoginMessageTitle _<*código de idioma*>

- Descripción: Especifica un título traducido para la página de mensajes de pre-inicio de sesión. *LanguageCode* puede ser en, de, es, fr, ja, o cualquier otro identificador de idioma compatible.
- Valor: None. Texto sin formato más cualquier número de etiquetas e hipervínculos HTML de línea nueva
- Tipo de sitio: Web XenApp

RADERequestValidation

- Descripción: Especifica si se debe realizar la validación del texto en las solicitudes nuevas provenientes de Citrix Offline Plug-in.
- Valor:
- Tipo de sitio: Web XenApp y Servicios XenApp

RADESessionURL

- Descripción: Especifica la dirección URL de la página de la sesión RADE. Si este parámetro se define en auto, la dirección URL se genera automáticamente.

- Valor: Auto. Dirección URL válida
- Tipo de sitio: Web XenApp y Servicios XenApp

RadiusRequestTimeout

- Descripción: Especifica el valor de tiempo de espera para una respuesta procedente del servidor RADIUS de la sesión.
- Valor: Tiempo en segundos (30)
- Tipo de sitio: Web XenApp

RadiusServers

- Descripción: Especifica los servidores RADIUS que se usarán, y si es necesario, los puertos donde escuchan. Es posible especificar servidores usando nombres o direcciones IP; el servidor y el puerto de cada elemento se separan mediante dos puntos (:). Si no se especifica ningún puerto, se usa el puerto RADIUS predeterminado (1812). Puede configurarse un máximo de 512 servidores.
- Valor: *Servidor* [:*Puerto*] [,…]
- Tipo de sitio: Web XenApp

ReconnectAtLogin

- Descripción: Especifica si el control del área de trabajo debe volver a conectarse con los recursos cuando los usuarios inician sesión y, de ser así, especifica si lo hará con todos los recursos o sólo con los desconectados.
- Valor: Disconnected AndActive | Disconnected | None
- Tipo de sitio: Web XenApp

ReconnectButton

- Descripción: Especifica si el control del área de trabajo debe volver a conectarse con las aplicaciones cuando los usuarios hacen clic en el botón Reconectar y, de ser así, especifica si lo hará con todos los recursos o sólo con los desconectados.
- Valor: Disconnected AndActive | Disconnected | None
- Tipo de sitio: Web XenApp

RecoveryFarm<*n*>

- Descripción: Especifica toda la información para una comunidad de recuperación ante desastres. Puede configurarse un máximo de 512 comunidades.
- Valor: Dirección de Citrix XML Service [,Dirección de Citrix XML Service,] [,Name:<*nombre*>] [,XMLPort: <*puerto*>] [,Transport: <HTTP | HTTPS | SSL>] [,SSLRelayPort: <*Puerto*>] [,Bypass Duration: <*Minutos* (60)>] [,LoadBalance: <off | on>] [,TicketTime ToLive: <*Segundos* (200)>] [,RADETicket TimeToLive: <*Segundos* (200)>]
- Tipo de sitio: Web XenApp, Servicios XenApp y XenDesktop

RequestedHighColorIcons

- Descripción: Especifica si se solicitan iconos de 32 bits en color de alta densidad al servicio XML de Citrix y, en este caso, enumera los tamaños de icono en pixeles. Si este parámetro no se define en None, sólo se solicitan los iconos estándar 32 x 32 de 4 bits. El parámetro predeterminado varía según el tipo de sitio y su configuración.
- Valor: 16, 32, 48 | None

  Para los sitios de servicios XenApp, el valor predeterminado es solicitar todos los iconos. Para los sitios Web XenApp sólo se solicitan tamaños de 16 x 16 y 32 x 32 de manera predeterminada.
- Tipo de sitio: Web XenApp y Servicios XenApp

RequestICAClientSecureChannel

- Descripción: Especifica la configuración de TLS.
- Valor: Detect-Any Ciphers, TLS- GovCiphers, SSL-AnyCiphers
- Tipo de sitio: Web XenApp y Servicios XenApp

RequireLaunchReference

- Descripción: Especifica si se obliga el uso de referencias de inicio. Se requieren referencias de inicio para la autenticación PassThrough en las aplicaciones de VM Hosted Apps de XenApp. Si se requiere la compatibilidad con XenApp 4.0 Feature Pack 1 parar UNIX, entonces este parámetro se debe establecer en Off.
- Valor: On | Off
- Tipo de sitio: Web XenApp y Servicios XenApp

RestrictDomains

- Descripción: Especifica si se utiliza el parámetro LoginDomains para restringir el acceso de los usuarios.
- Valor: Off | On
- Tipo de sitio: Web XenApp y Servicios XenApp

SearchContextList

- Descripción: Especifica nombres de contexto para usarlos con la autenticación NDS.
- Valor: None. Lista de nombres de contexto separados por comas
- Tipo de sitio: Web XenApp y Servicios XenApp

ServerAddressMap

- Descripción: Especifica parejas de dirección normal y dirección traducida para la configuración del servidor de seguridad o firewall del lado del servidor. La dirección normal identifica la dirección del servidor, y se devuelve la dirección traducida al

cliente Citrix.

- Valor: DirecciónNormal, DirecciónTraducida, …
- Tipo de sitio: Web XenApp y Servicios XenApp

ServerCommunicationAttempts

- Descripción: Especifica el número de veces que se intentará enviar una solicitud al servicio XML de Citrix antes de considerar que hubo un error en el servicio.
- Valor: Número entero mayor que 0 (2)
- Tipo de sitio: Web XenApp y Servicios XenApp

ShowClientInstallCaption

- Descripción: Especifica cómo y cuándo aparecen los mensajes de instalación. Si este parámetro se establece en Auto, los mensajes de instalación se muestran cuando los usuarios no tienen ningún cliente Citrix instalado o cuando existe un cliente más adecuado. Si el valor del parámetro se establece en Quiet, los mensajes de instalación se muestran sólo si los usuarios no tienen ningún cliente. El comportamiento de la pantalla de Inicio de sesión es un poco diferente, ya que los mensajes solo aparecen para los clientes de recursos en línea y solo si no se detecta ningún cliente. Por lo tanto, no hay ninguna diferencia entre los parámetros Auto y Quiet en la pantalla de Inicio de sesión.
- Valor: Auto | Quiet | Off
- Tipo de sitio: Web XenApp

ShowDesktopViewer

- Descripción: Especifica si la barra de herramientas y la ventana de Citrix Desktop Viewer se habilitan de forma predeterminada cuando los usuarios acceden a sus escritorios.
- Valor: Off | On
- Tipo de sitio: Web XenApp y Servicios XenApp

ShowHints

- Descripción: Especifica si se muestran sugerencias en la pantalla de aplicaciones.
- Valor: On | Off
- Tipo de sitio: Web XenApp

ShowPasswordExpiryWarning

- Descripción: Especifica las condiciones en las que se presenta una advertencia de caducidad de contraseña a un usuario.
- Valor: Never | Windows Policy | Custom

- Tipo de sitio: Web XenApp

ShowRefresh

- Descripción: Especifica si el botón Actualizar está disponible para los usuarios en la pantalla de aplicaciones.
- Valor: Off | On
- Tipo de sitio: Web XenApp

ShowSearch

- Descripción: Especifica si está disponible el control de búsqueda para los usuarios en la pantalla de aplicaciones.
- Valor: On | Off
- Tipo de sitio: Web XenApp

SpecialFolderRedirection

- Descripción: Especifica si se habilita o no la redirección de carpetas especiales. Si el valor del parámetro es On, los recursos utilizan las carpetas \Documentos y \Escritorio de los equipos locales de los usuarios. Si el valor del parámetro es Off, las carpetas \Documentos y \Escritorio disponibles en las aplicaciones serán las carpetas del servidor.
- Valor: Off | On
- Tipo de sitio: Web XenApp y Servicios XenApp

SuppressDuplicateResources

- Descripción: Especifica si se debe ocultar la existencia de recursos con nombres idénticos y ubicaciones de carpetas publicadas en diferentes comunidades a los usuarios.
- Valor: Off | On
- Tipo de sitio: Web XenApp y Servicios XenApp

Tiempo de espera

- Descripción: Especifica el valor del tiempo de espera que se usará al comunicarse con el servicio XML de Citrix.
- Valor: Tiempo en segundos (60)
- Tipo de sitio: Web XenApp y Servicios XenApp

TransparentKeyPassthrough

- Descripción: Especifica el modo de paso de combinaciones de teclas de Windows.
- Valor: FullScreen Only | Local | Remote

- Tipo de sitio: Web XenApp y Servicios XenApp

TwoFactorPasswordIntegration

- Descripción: Especifica si se habilita la integración de contraseñas con RSA SecurID 6.0.
- Valor: Off | On
- Tipo de sitio: Web XenApp

TwoFactorUseFullyQualifiedUserNames

- Descripción: Especifica si se transfieren los nombres de usuario completos al servidor de autenticación durante la autenticación de dos factores.
- Valor: Off | On
- Tipo de sitio: Web XenApp

UpgradeClientsAtLogin

- Descripción: Especifica si el proceso de detección e instalación de clientes se ejecuta automáticamente cuando los usuarios inician sesión si hay una versión más reciente del cliente nativo adecuado o de Citrix offline plug-in. Este parámetro sólo se aplica cuando el parámetro de EnableWizardAutoMode está en On.
- Valor: Off | On
- Tipo de sitio: Web XenApp

UPNSuffixes

- Descripción: Especifica los sufijos permitidos para la autenticación explícita con UPN.
- Valor: Lista de sufijos UPN
- Tipo de sitio: Web XenApp y Servicios XenApp

UserInterfaceBranding

- Descripción: Especifica si el sitio está enfocado a usuarios de aplicaciones o de escritorios. Si el parámetro está en Desktops, se cambia la funcionalidad del sitio para mejorar la experiencia de uso de XenDesktop. Citrix recomienda usar este parámetro en entornos que incluyan XenDesktop.
- Valor: Applications | Desktops
- Tipo de sitio: Web XenApp

UserInterfaceLayout

- Descripción: Especifica si debe usarse la interfaz de usuario compacta.
- Valor: Auto | Normal | Compact
- Tipo de sitio: Web XenApp

UserInterfaceMode

- Descripción: Especifica la apariencia de la pantalla de Inicio de sesión. Si el parámetro se establece en Simple, sólo se mostrarán los campos de inicio de sesión para el método de autenticación seleccionado. Si se establece en Advanced, se mostrará la barra de navegación que da acceso a las pantallas de mensajes y preferencias de pre-inicio de sesión.
- Valor: Simple | Advanced
- Tipo de sitio: Web XenApp

ViewStyles

- Descripción: Especifica los estilos de vista disponibles para los usuarios en la pantalla de aplicaciones en la interfaz de usuario con gráficos.
- Valor: Details | Groups | Icons | List | Tree
- Tipo de sitio: Web XenApp

WebSessionTimeout

- Descripción: Especifica el valor de tiempo de espera para sesiones de explorador Web inactivas.
- Valor: Tiempo en minutos (20)
- Tipo de sitio: Web XenApp

Welcome Message _<*código de idioma*>

- Descripción: Especifica el mensaje de bienvenida traducido que aparecerá en la zona de presentación de la pantalla de Inicio de sesión. *LanguageCode* puede ser en, de, es, fr, ja, o cualquier otro identificador de idioma compatible.
- Valor: None. Texto sin formato más cualquier número de etiquetas e hipervínculos HTML de línea nueva
- Tipo de sitio: Web XenApp

WIAuthenticationMethods

- Descripción: Especifica los métodos de autenticación permitidos para los sitios no integrados con Access Gateway. Se trata de una lista separada por comas y es posible que contenga cualquiera de los valores especificados en cualquier orden.
- Valor: Cualquier combinación de: Explicit, Anonymous, Certificate SingleSignOn, Certificate, SingleSignOn
- Tipo de sitio: Web XenApp, Servicios XenApp y Desktop Appliance Connector

Contenido del archivo config.xml

El archivo config.xml contiene una serie de parámetros divididos en distintas categorías. Puede editar parámetros en las siguientes categorías:

- FolderDisplay. Especifica el lugar donde se mostrarán los iconos para los recursos: en el menú Inicio, en el escritorio físico de Windows o en el área de notificación. Existe un parámetro adicional para especificar una carpeta en particular en el menú Inicio. Estos parámetros corresponden a los controles de la página Presentación de la aplicación, en el cuadro de diálogo Opciones de Citrix Online Plug-in.

- DesktopIntegration. Especifica si se agregarán o no accesos directos al menú Inicio, al escritorio o al área de notificación.

- ConfigurationFile. Especifica una dirección URL diferente del archivo config.xml para su uso futuro por parte del plug-in. Esto facilita el traslado de usuarios a un servidor de Interfaz Web diferente.

- Request. Especifica la ubicación desde la cual el plug-in debe solicitar datos de recursos y la frecuencia con que se actualizará la información.

- Failover. Especifica una lista de direcciones URL de servidores de respaldo con las cuales comunicarse si el servidor principal no está disponible.

- Inicio de sesión. Especifica el método de inicio de sesión que se debe utilizar.

- ChangePassword. Especifica las circunstancias en las que los usuarios de Citrix Online Plug-in pueden cambiar sus contraseñas y la ruta mediante la cual se dirige la solicitud.

- UserInterface. Especifica si se ocultan o se muestran a los usuarios ciertos grupos de opciones como parte de la interfaz de usuario de Citrix Online Plug-in.

- ReconnectOptions. Especifica si la funcionalidad de control del área de trabajo está disponible o no para los usuarios.

- FileCleanup. Especifica si se eliminan los accesos directos cuando los usuarios cierran la sesión de Citrix Online Plug-in.

- ICA_Options. Define las opciones de presentación y de sonido para las conexiones de los plug-ins. Estos parámetros corresponden a las opciones de la página Opciones de sesión en el cuadro de diálogo Opciones de Citrix Online Plug-in.

- AppAccess. Especifica los tipos de recursos disponibles para los usuarios.

Para obtener más información sobre el uso del archivo config.xml, consulte Online Plug-in para Windows.

Consideraciones sobre Citrix Online Plug-in

Algunos parámetros de WebInterface.conf afectan la validación de las solicitudes de Citrix Online Plug-in. Citrix recomienda que los parámetros de WebInterface.conf sean coherentes con los del archivo config.xml para Citrix Online Plug-in.

Parámetros del archivo WebInterface.conf

La siguiente tabla contiene los parámetros del archivo WebInterface.conf que deben ser coherentes con los del archivo config.xml. También explica los parámetros que afectan a Citrix Online Plug-in y su configuración recomendada.

Parámetro	Configuración recomendada
LoginType	Si es NDS, la autenticación Novell también debe estar habilitada en config.xml.
NDSTreeName	DefaultTree en la sección Logon de config.xml debe tener el mismo valor.
PNAChangePasswordMethod	El método en la sección ChangePassword de config.xml debe tener el mismo valor.
WIAuthenticationMethods	Use el mismo método de autenticación configurado en el archivo WebInterface.conf. Si el método es distinto en config.xml, la autenticación fallará.

Para configurar la Interfaz Web cuando se usa Citrix Online Plug-in

1. Utilice un editor de texto y abra el archivo WebInterface.conf.
2. Busque los parámetros siguientes:
   - LoginType
   - NDSTreeName
   - PNAChangePasswordMethod
   - WIAuthenticationMethods
3. Modifique la configuración de estos parámetros como se describe en Contenido del archivo config.xml.
4. Reinicie el servidor de la Interfaz Web para aplicar los cambios.

Para obtener más información sobre los parámetros del archivo WebInterface.conf, consulte Parámetros de WebInterface.conf.

Parámetros del archivo bootstrap.conf

La siguiente tabla muestra los parámetros del archivo bootstrap.conf.

Parámetro	Description	Valores	Tipos de sitio
ConfigurationLocation	Especifica el archivo desde donde obtiene su configuración el sitio de la Interfaz Web. Puede ser un archivo local o, para sitios alojados en IIS, puede ser un archivo remoto compartido en la red.	Ruta absoluta a WebInterface.conf	Web XenApp XenApp Services
DefaultLocale	Especifica el idioma predeterminado que se usará si un explorador Web solicita un idioma no respaldado.	en | de | es | fr | ja | cualquier otro identificador de idioma compatible	Web XenApp XenApp Services
SiteName	Especifica el nombre del sitio que aparece en la consola Administración de la Interfaz Web de Citrix. El parámetro predeterminado usa la dirección URL del sitio.	Cadena válida	Web XenApp XenApp Services

Para configurar la comunicación con el servidor

En este ejemplo, se desea especificar el nombre de un servidor adicional que ejecuta el servicio XML de Citrix. El servicio XML de Citrix es el vínculo de comunicación entre la comunidad de servidores y el servidor de la Interfaz Web.

La comunicación está establecida con un servidor llamado “rock”, pero usted desea agregar un servidor llamado “roll” en caso de que el servidor rock falle. Para hacerlo:

1. Utilice un editor de texto para abrir el archivo WebInterface.conf y busque esta línea:

   Farm1=rock,Name:Farm1,XMLPort:80,Transport:HTTP, SSLRelayPort:443,…

2. Modifique esta línea para incluir el servidor adicional, como se muestra a continuación:

   Farm1=rock,roll,Name:Farm1,XMLPort:80,Transport:HTTP, SSLRelayPort:443,…

Para configurar la comunicación con el Traspaso SSL

En este ejemplo se desea proteger la comunicación entre el servidor Web y el servidor que ejecuta XenApp o XenDesktop a través de Secure Sockets Layer (SSL). El Traspaso SSL está instalado en el servidor que ejecuta XenApp o XenDesktop, cuyo nombre de dominio completo es “blues.mycompany.com”. El Traspaso SSL escucha las conexiones en el puerto TCP 443.

Actualmente, la comunicación se realiza con un servidor llamado "rhythm", pero se desea sustituir rhythm por el servidor blues.mycompany.com. Para hacerlo:

1. Utilice un editor de texto para abrir el archivo WebInterface.conf y busque esta línea:

   Farm1=rhythm,Name:Farm1,XMLPort:80,Transport:HTTP, SSLRelayPort:443

2. Cambie el transporte a SSL de la siguiente forma:

   Farm1=blues.mycompany.com,Name:Farm1,XMLPort:80, Transport:SSL,SSLRelayPort:443

   Nota: El nombre de servidor especificado debe coincidir con el nombre que figura en el certificado del servidor.

Para configurar el respaldo para Secure Gateway

En este ejemplo, se especifica un servidor Secure Gateway denominado “csg1.mycompany.com” en el que los clientes Citrix usan el puerto 443, con las siguientes dos direcciones de Secure Ticket Authority:

- http://country.mycompany.com/scripts/ctxsta.dll
- http://western.mycompany.com/scripts/ctxsta.dll

Incluya estas líneas en el archivo WebInterface.conf:

AlternateAddress=Mapped

CSG_STA_URL1=http://country.mycompany.com/scripts/ctxsta.dll

CSG_STA_URL2=http://western.mycompany.com/scripts/ctxsta.dll

CSG_Server=csg1.mycompany.com

CSG_ServerPort=443

ClientAddressMap=*,SG

La última línea habilita Secure Gateway para todos los usuarios.

Para configurar la compatibilidad con XenApp 4.0, con Feature Pack 1, para UNIX

En este ejemplo se quiere configurar un sitio para que sea compatible con XenApp 4.0, con Feature Pack 1, para UNIX. Inicialmente, los nuevos sitios de Interfaz Web no son compatibles con este producto; es necesario realizar una configuración manual adicional.

1. Utilice un editor de texto para abrir el archivo WebInterface.conf y ubique las siguientes líneas:

   OverrideIcaClientname=Off

   RequireLaunchReference=On

2. Modifique los parámetros como se muestra abajo:

   OverrideIcaClientname=On

   RequireLaunchReference=Off

   Nota: Al poner el parámetro RequireLaunchReference en Off se inhabilita la autenticación PassThrough o paso de credenciales para XenApp VM Hosted Apps. Los usuarios de este sitio necesitarán introducir sus credenciales cada vez que quieran acceder a una aplicación de VM Hosted Apps.

Para configurar comunidades de recuperación ante desastres

En este ejemplo, se han reservado dos comunidades de servidores que se utilizarán únicamente cuando surja un problema que impida a los usuarios el acceso a las comunidades de producción, como un corte en el suministro eléctrico o un problema con la red.

Los nombres de los servidores que ejecutan el servicio XML de Citrix en las comunidades son “jazz” y “fusion”. Desea designar estas comunidades para la recuperación ante desastres. Para hacerlo:

1. Utilice un editor de texto para abrir el archivo WebInterface.conf y agregue las siguientes líneas:

   RecoveryFarm1=jazz,Name:RecoveryFarm1,XMLPort:80,Transport:HTTP,SSLRelayPort:443,BypassDuratio

   configuración de los valores para este parámetro según el entorno.

   Tenga en cuenta que la segunda comunidad se utiliza sólo si no se puede acceder a la primera comunidad de recuperación ante desastes. Los recursos no se agregan en ambas comunidades de recuperación ante desastres dado que se destinan a las comunidades de producción. En cambio, la Interfaz Web intenta establecer contacto con cada comunidad de recuperación ante desastres en orden y enumera los recursos de la primera comunidad con la que se establece comunicación.

Para configurar el perfil móvil de usuarios

En este ejemplo, se desea asociar grupos de usuarios en la oficina de los EE. UU. de la empresa con comunidades de servidores específicas, a fin de que cuando visiten la oficina de Japón, puedan iniciar sesión en un servidor de la Interfaz Web local y recibir automáticamente recursos en inglés desde una comunidad en los EE. UU.

Una comunidad existente con el servicio XML de Citrix que se ejecuta en el servidor “waltz” ya está definida como Farm1 en el archivo de configuración y está disponible para todos los usuarios que inicien sesión en el servidor de la Interfaz Web de los EE. UU. Los grupos de usuarios “SalesMgrs” y “SalesTeam” se ubican en el dominio “ussales.mycompany.com” y el grupo de usuarios “Accounts” se ubica en el dominio “finance.mycompany.com”. Se desea asociar a los usuarios de estos grupos con las comunidades donde los nombres de los servidores que ejecutan Citrix XML Service son “foxtrot” y “tango”. Para hacerlo:

1. Utilice un editor de texto para abrir el archivo WebInterface.conf en el servidor de la Interfaz Web de los EE. UU y busque esta línea:

   Farm1=waltz,Name:Farm1,XMLPort:80,Transport:HTTP,SSLRelayPort:443,BypassDuration:60,LoadBalance

   Importante: cuando se activa el perfil móvil del usuario, la primera comunidad definida en el archivo de configuración debe estar ejecutando XenApp 6.0 o una versión posterior, o bien XenDesktop 4.0 o una versión posterior. Si la primera comunidad de la lista está ejecutando una versión anterior, no se mostrarán recursos para los usuarios.

2. Agregue las líneas siguientes para definir las comunidades nuevas:

   Farm2=foxtrot,Name:Farm2,XMLPort:80,Transport:HTTP,SSLRelayPort:443,BypassDuration:60,LoadBalan

3. Agregue las líneas siguientes para asignar los grupos de usuarios a las comunidades nuevas:

   Farm2Groups=ussales.mycompany.com\SalesMgrs,ussales.mycompany.com\SalesTeam,finance.mycompar

   Al agregar el parámetro **Farm<*n*>Groups** para una comunidad que se define mediante **Farm<*n*>**, se activa la función de perfil móvil de usuarios. Esto significa que los grupos de usuarios deben asignarse a todas las comunidades, no solo a aquellas que utilizarán los usuarios con perfil móvil.
4. Asegúrese de que los usuarios puedan seguir teniendo acceso a la comunidad existente. Para ello, agregue la línea siguiente:

   Farm1Groups=mycompany.com\DomainUsers

   Para permitir que los usuarios con perfil móvil tengan acceso a sus recursos cuando se encuentren en Japón, se deben replicar estos parámetros en el archivo de configuración del servidor de la Interfaz Web de Japón.
5. Utilice un editor de texto para abrir el archivo WebInterface.conf en el servidor de la Interfaz Web de Japón e introduzca las líneas especificadas en los pasos 2 y 3. Asegúrese también de asignar los grupos de usuarios a las comunidades japonesas existentes para que los usuarios locales puedan seguir accediendo a ellas.

ID de suceso y mensajes registrados

La Interfaz Web registra los ID de suceso de todos los tipos de sitios y las plataformas. En los sistemas operativos Windows, los ID de suceso se pueden visualizar mediante el Visor de sucesos y se pueden utilizar con Citrix EdgeSight o las herramientas de supervisión o creación de informes de terceros. En los servidores de aplicaciones Java, el ID de suceso forma parte de un mensaje de registro escrito en el archivo de registro del servidor Web.

En la siguiente tabla se muestran los ID de suceso de la Interfaz Web y los mensajes de registros asociados. Se incluyen descripciones breves de los problemas y las sugerencias para solucionarlos.

ID de suceso	Mensaje	Gravedad	Descripción
10001	Se produjo un error de análisis de la configuración: <*descripción del error* >	Error	Existe un problema en el archivo de configuración del sitio. Compruebe si existen errores en WebInterface.conf.
10002	Se produjo un error al cargar la configuración.	Error	No se puede encontrar el archivo de configuración del sitio o no se puede obtener acceso a este archivo. Compruebe que no se haya eliminado WebInterface.conf y que se hayan configurado los permisos adecuados de manera que se permita la lectura de este archivo.
10003	No se pudo recuperar la configuración de Citrix Online Plug-in.	Error	No se puede encontrar el archivo de configuración de Online Plug-in o no se puede obtener acceso a este archivo. Compruebe que no se haya eliminado config.xml y que se hayan configurado los permisos adecuados de manera que se permita la lectura de este archivo.
10004	Los datos de configuración se volvieron a cargar correctamente.	Información	Se han validado y aceptado los cambios recientes en el archivo de configuración del sitio (WebInterface.conf) o en el archivo de configuración de Online Plug-in (config.xml).
10005	Las siguientes claves se encuentran duplicadas en el archivo de configuración: <*nombre de la clave*>	Advertencia	Existe un parámetro duplicado en el archivo de configuración del sitio. Corrija el error en WebInterface.conf.

10006	Punto de autenticación desconocido: <*punto de autenticación*>.	Error	El valor especificado en el parámetro AuthenticationPoint del archivo de configuración del sitio es incorrecto. Corrija el error en WebInterface.conf.
10007	No se pueden utilizar inicios de sesión anónimos cuando el perfil móvil del usuario se encuentra activado.	Error	XenDesktop no permite usuarios anónimos. Para utilizar la función de perfil móvil del usuario con XenDesktop, desactive la opción de la autenticación anónima.
10008	La configuración no es válida: la autenticación NDS no es compatible con esta versión de la Interfaz Web.	Error	Vuelva a configurar el método de autenticación para el sitio y seleccione un nombre principal del usuario (UPN) o la autenticación basada en dominios de Microsoft.
10009	La configuración no es válida: La autenticación con tarjetas inteligentes o mediante el paso de credenciales (PassThrough) no es compatible con esta versión de la Interfaz Web.	Error	Este error se muestra cuando se utiliza la versión UNIX/JSP de la Interfaz Web y se utilizan los puntos de autenticación de la Interfaz Web con autenticación mediante paso de credenciales (PassThrough), tarjetas inteligentes o paso de credenciales con tarjetas inteligentes, o los puntos de autenticación de Access Gateway con autenticación mediante tarjetas inteligentes o mediante paso de credenciales con tarjetas inteligentes.
10010	Existe un problema en la configuración de la autenticación de dos factores.	Error	Compruebe que la autenticación del servidor RADIUS, Aladdin SafeWord para Citrix o RSA SecurID se haya configurado correctamente.
10011	Actualmente no existen métodos de autenticación disponibles.	Error	Compruebe que el sitio se haya configurado correctamente y que se hayan especificado uno o varios métodos de autenticación válidos.

10101	El servicio de transición de protocolos no se ha configurado correctamente. Asegúrese de que se haya definido tokenManager en web.config y que se hayan definido uno o varios servicios de tokens.	Error	Compruebe que el archivo web.config del sitio Web de XenApp especifique uno o varios emisores de tokens con referencias de certificaciones asociadas que se puedan utilizar para proteger la relación de confianza en el paso de credenciales con tarjeta inteligente del servicio de Access Gateway.
10201	La configuración no es válida: la firma de los archivos ICA no es compatible con esta versión de la Interfaz Web.	Error	Debe ejecutar la Interfaz Web 5.4 o una versión posterior para utilizar la función de firma de archivos ICA.
10202	La firma de archivos ICA no se puede utilizar cuando la opción de respaldo para clientes antiguos se encuentra activada.	Error	Para activar la función de firma de archivos ICA, el sitio debe configurarse de manera que se utilice el cliente nativo y EnableLegacyIcaClientSupport debe establecerse en Off en el archivo Webinterface.conf.
10203	La firma de archivos ICA no se puede utilizar con aplicaciones sin conexión.	Error	Compruebe que el sitio se haya configurado de manera que se muestren las aplicaciones de modo dual o con conexión.
10204	Para poder utilizar la firma de archivos ICA, debe permitir que los usuarios elijan el cliente nativo.	Información	Para activar la firma de archivos ICA, el sitio debe configurarse de manera que se utilice el cliente nativo.
10205	Se produjo un error al intentar firmar un archivo ICA: <*mensaje de error*>	Error	Consulte la información del mensaje de error para obtener más detalles en relación con las medidas que posiblemente deba tomar.
10206	Se produjo un error al intentar firmar un archivo ICA: <>. Reinicie el servidor Web para asegurarse de que el servicio de firma de archivos ICA se encuentre activado.	Error	Reinicie el servidor Web y utilice la consola de administración de la Interfaz Web para asegurarse de que la firma de archivos ICA se encuentre activada.
11001	La URL de redirección transferida al proceso de descarga y detección de clientes no es válida.	Error	La URL de redirección especifica la página Web a la que se redirigen los usuarios cuando finalizan el proceso de instalación y detección de clientes. Este error indica que la URL de redirección se ha modificado en el código para el sitio.

11002	El proceso de instalación y detección de clientes no pudo instalar ninguno de los clientes activados. Compruebe que el explorador, el sistema operativo y el método de acceso del cliente sean compatibles con los clientes activados y que esos clientes se encuentren disponibles en la carpeta \Clients del sitio Web de XenApp.	Error	El usuario no pudo obtener un cliente del sitio. Compruebe que haya un cliente adecuado para el dispositivo, el sistema operativo, el explorador y el método de acceso del usuario disponible en el servidor Web y activado en el sitio.
11003	El proceso de instalación y detección de clientes no es compatible con el sistema operativo del equipo del usuario.	Error	El usuario no pudo obtener un cliente del sitio porque el proceso de instalación y detección de clientes no pudo identificar el sistema operativo del equipo del usuario.
11004	No se puede procesar la solicitud del explorador que se ejecuta en el dispositivo del usuario <*dirección IP*> porque no se puede encontrar el encabezado HTTP Usuario-Agente que proporciona la información de la plataforma.	Error	El usuario no pudo obtener acceso al sitio porque la solicitud que envió el explorador no incluía un encabezado HTTP Usuario-Agente que identifique la plataforma y el explorador del usuario. Compruebe el entorno de la red para asegurarse de que los encabezados Usuario-Agente no se estén eliminando de las solicitudes de los usuarios.
12001	La Interfaz Web ha omitido <*un número de*> intentos de registro de mensajes con este ID de registro único. El índice de creación de informes ha disminuido.La Interfaz Web comenzará a registrar estos mensajes nuevamente.	Información	Utilice la tarea Registro de diagnóstico en Mantenimiento de sitios de la consola de administración de la Interfaz Web de Citrix para evitar que los sucesos duplicados se registren repetidamente y configurar la cantidad de sucesos duplicados que se deben registrar y la frecuencia con que se debe realizar esto.
12002	Los posteriores intentos de registro de mensajes con este ID de registro único se omitirán hasta que el índice de creación de informes disminuya.	Información	Utilice la tarea Registro de diagnóstico en Mantenimiento de sitios de la consola de administración de la Interfaz Web de Citrix para evitar que los sucesos duplicados se registren repetidamente y configurar la cantidad de sucesos duplicados que se deben registrar y la frecuencia con que se debe realizar esto.

12003	El archivo de ID de suceso no se pudo cargar. Compruebe que la ruta al archivo de ID de suceso en <*nombre del archivo*> sea correcta.	Advertencia	No se puede encontrar el archivo de ID de suceso o no se puede obtener acceso a este archivo. Compruebe que la ruta proporcionada en web.config (para los sitios alojados en IIS) o web.xml (para los sitios alojados en servidores de aplicaciones Java) sea correcta. Además, compruebe que no se haya eliminado WebInterfaceEventIds.txt y que se hayan configurado los permisos adecuados de manera que se permita la lectura de este archivo.
12004	La clave del mensaje <*nombre de la clave*> no corresponde a un ID de suceso válido. Compruebe que el archivo de ID de suceso incluya una entrada válida para <*nombre de la clave*>. El ID de suceso debe ser un número entero entre 1 y 65 535.	Advertencia	No se puede encontrar el ID de suceso especificado en el archivo de ID de suceso. Compruebe que no se haya eliminado este ID de suceso de WebInterfaceEventIds.txt.
13001	No se pudo establecer una conexión SSL con el servicio Web en <*dirección del servidor*>:<*puerto*>. El mensaje emitido desde la plataforma subyacente fue <*descripción del error*>.	Error	Se produjo un error SSL.Se proporcionan detalles específicos al final del mensaje de error. Compruebe que la Interfaz Web se haya configurado correctamente para integrarse con Access Gateway o Password Manager a través de SSL.
13002	No se pudieron recuperar los identificadores de seguridad de al menos un grupo. Compruebe si se puede obtener acceso a Citrix XML Service, si este servicio admite el perfil móvil del usuario y si los grupos del archivo de configuración son correctos.	Error	Existe un problema en uno o varios grupos de usuarios configurados para la función de perfil móvil del usuario. Compruebe que todos los servidores de la comunidad ejecuten una versión de XenApp o XenDesktop que sea compatible con la función de perfil móvil del usuario. Además, compruebe que los nombres de los grupos especificados sean válidos y que sea posible establecer una comunicación con los servidores Citrix.

14001	Se produjo un problema con RSA SecurID ACE/Agent. Compruebe que ACE/Agent se haya instalado correctamente y que se haya agregado la ruta del archivo aceclnt.dll a la variable del entorno PATH.	Error	Para utilizar la autenticación SecurID con la Interfaz Web para Microsoft Internet Information Services, la Interfaz Web debe instalarse después de instalar el agente de autenticación RSA de la Web para Internet Information Services.
14002	Se produjo un problema con RSA SecurID ACE/Agent. Compruebe que se haya instalado la versión de ACE/Agent correcta.	Error	Compruebe que se haya instalado una versión compatible del agente de autenticación RSA de la Web para Internet Information Services en el servidor Web.
14003	Se produjo un problema con SafeWord Agent de Aladdin. Compruebe que el agente se haya instalado correctamente.	Error	Asegúrese de que SafeWord Agent para la Interfaz Web esté instalado en el servidor de la Interfaz Web. La Interfaz Web debe instalarse antes de instalar SafeWord Agent.
14004	No se puede actualizar la contraseña que RSA SecurID ACE/Agent ha almacenado en la memoria caché. Compruebe que las versiones de RSA SecurID ACE/Agent y ACE/Server sean compatibles y que tanto ACE/Agent como ACE/Server se hayan configurado de manera que se utilice la integración de contraseñas de Windows.	Error	Compruebe que las versiones del agente de autenticación RSA y del administrador de autenticación RSA de la Web para Internet Information Services sean compatibles. Además, compruebe que los parámetros del sistema de la base de datos del administrador de autenticación RSA se hayan configurado de manera que la integración de contraseñas de Windows quede activada en el nivel del sistema.
14005	No se puede obtener la contraseña que RSA SecurID ACE/Agent ha almacenado en la memoria caché. Compruebe que las versiones de RSA SecurID ACE/Agent y ACE/Server sean compatibles y que tanto ACE/Agent como ACE/Server se hayan configurado de manera que se utilice la integración de contraseñas de Windows.	Error	Compruebe que las versiones del agente de autenticación RSA y del administrador de autenticación RSA de la Web para Internet Information Services sean compatibles. Además, compruebe que los parámetros del sistema de la base de datos del administrador de autenticación RSA se hayan configurado de manera que la integración de contraseñas de Windows quede activada en el nivel del sistema.

14006	Se produjo un problema en el autenticador de SafeWord al autenticar el usuario.	Error	Existe un problema en el servidor de SafeWord. Para obtener más información, consulte los archivos de registros en el servidor de SafeWord.
14007	Se produjo un problema con RSA SecurID ACE/Agent. Compruebe que el grupo de aplicaciones de la Interfaz Web se encuentre configurado para aplicaciones de 32 ó 64 bits según corresponda para la versión de ACE/Agent instalada.	Error	Compruebe los requisitos de la aplicación para la versión de ACE/Agent que esté ejecutando.
15001	Se produjo un problema al leer la versión del cliente en <*ruta del archivo*>. No se les solicitará a los usuarios que ejecuten actualizaciones a versiones más recientes de este cliente.	Error	Compruebe que se hayan configurado los permisos adecuados de manera que se permita la lectura del archivo del programa de instalación del cliente especificado.
15002	Se produjo un problema al leer el archivo del paquete de idiomas <*nombre del archivo*>. Compruebe que se pueda obtener acceso al archivo y que se utilice el formato correcto.	Error	Compruebe que no se haya eliminado el archivo especificado y que se hayan configurado los permisos adecuados de modo que se permita la lectura de este archivo.
15003	No se pudo obtener acceso al directorio <*nombre del directorio*>. Los clientes de este directorio no se pueden poner a disposición de los usuarios. Asegúrese de que la cuenta Servicio de la red incluya los permisos adecuados para obtener acceso al directorio y luego reinicie el servidor Web.	Error	Compruebe que no se haya eliminado el directorio especificado y que se hayan configurado los permisos adecuados de modo que se permita el acceso a este directorio.
15004	Se produjo un problema al leer el archivo del paquete de idiomas <*nombre del archivo*>. No se puede utilizar el paquete de idiomas porque falta la declaración de la versión en el archivo.	Error	Falta el número de la versión en el archivo del paquete de idiomas. Corrija el error en el archivo especificado.

15005	Se produjo un problema al leer el archivo del paquete de idiomas <*nombre del archivo*>. La versión del paquete de idiomas es <*número de la versión*> y no es compatible con la versión actual de la Interfaz Web.	Error	La versión de la Interfaz Web y la versión del archivo del paquete de idiomas no coinciden. Los paquetes de idiomas son específicos para la versión de la Interfaz Web con la que se suministran y no pueden utilizarse con versiones anteriores o posteriores. Actualice o revierta el archivo especificado, según corresponda.
15006	No se pudo encontrar un paquete de idiomas para la configuración regional predeterminada <*configuración regional de instalación*>. Se encontró el paquete de idiomas <*nombre del archivo*> que se utilizará como valor predeterminado.	Advertencia	Cuando la Interfaz Web no puede encontrar un paquete de idiomas para la configuración regional que se seleccionó durante la instalación, la Interfaz Web recurre al primer paquete de idiomas compatible disponible.
16001	No se puede leer el archivo del secreto de RADIUS <*ruta del archivo*>.	Error	No se puede encontrar el archivo del secreto de RADIUS o no se puede obtener acceso a este archivo. Compruebe que la ruta proporcionada en web.config (para los sitios alojados en IIS) o web.xml (para los sitios alojados en servidores de aplicaciones Java) sea correcta. Además, compruebe que no se haya eliminado el archivo del secreto de RADIUS y que se hayan configurado los permisos adecuados de manera que se permita la lectura de este archivo.
16002	El archivo del secreto de RADIUS <*ruta del archivo*> se encuentra vacío.	Error	El protocolo RADIUS requiere el uso de un secreto compartido: información que sólo conoce el cliente RADIUS (la Interfaz Web) y el servidor RADIUS donde se realiza la autenticación. El archivo del secreto de RADIUS puede contener cualquier tipo de cadena, pero no puede estar vacío.

16003	Se produjo un problema en el autenticador de RADIUS al autenticar el usuario.	Error	Existe un problema en el servidor de RADIUS. Para obtener más información, consulte los archivos de registros en el servidor de RADIUS.
16004	Los valores RADIUS_NAS_IDENTIFIER y/o RADIUS_IP_ADDRESS deben formar parte del archivo de configuración Web del sitio. El valor RADIUS_NAS_IDENTIFIER debe contener 3 caracteres como mínimo. El valor RADIUS_IP_ADDRESS debe ser una dirección IP válida.	Error	El protocolo RADIUS requiere que las solicitudes de acceso a servidores RADIUS incluyan la dirección IP u otro identificador del cliente RADIUS (la Interfaz Web). Compruebe que web.config (para los sitios alojados en IIS) o web.xml (para los sitios alojados en servidores de aplicaciones Java) contenga un identificador RADIUS NAS o una dirección IP válida.
17001	Error en la búsqueda por contexto en el servidor <*dirección del servidor*>:<*excepción*>. Este servidor se ha eliminado temporalmente de la lista de servidores activos.	Error	Existe un problema en el servidor de NDS especificado. Este servidor se ignorará hasta que se resuelva el problema. Para obtener más información, consulte los archivos de registros en el servidor de NDS.
17002	La búsqueda por contexto no se puede realizar porque todos los servidores de NDS presentaron errores. Intente iniciar sesión con un nombre de usuario completo; es decir, *.nombrede usuario.miempresa.com*.	Error	No se pudo establecer contacto con ninguno de los servidores de NDS. Intente introducir las credenciales en el formato *.nombredeusuario.miempresa.com*. Para obtener más información, consulte los archivos de registros en los servidores de NDS.
18001	Se produjo un error en la comunicación al intentar ponerse en contacto con el servicio de autenticación de Advanced Access Control a través de <*URL*>. Compruebe que el servicio de autenticación se encuentre en ejecución. El mensaje emitido desde la plataforma subyacente fue <*descripción del error*>.	Error	Existe un problema al ponerse en contacto con el servicio de autenticación de Access Gateway.Se proporcionan detalles específicos al final del mensaje de error. Para obtener más información, consulte los archivos de registros del dispositivo de Access Gateway.

18002	Se produjo un error en la comunicación al intentar cerrar sesión mediante el servicio de autenticación de Access Gateway a través de <*URL*>. Compruebe que el servicio de autenticación se encuentre en ejecución. El mensaje emitido desde la plataforma subyacente fue <*descripción del error*>.	Error	Existe un problema al ponerse en contacto con el servicio de autenticación de Access Gateway.Se proporcionan detalles específicos al final del mensaje de error. Para obtener más información, consulte los archivos de registros del dispositivo de Access Gateway.
18003	El servicio de autenticación de Access Gateway no pudo autenticar el usuario. El mensaje emitido desde el servicio fue <*descripción del error*> [código de estado: <*número de código*>].	Error	Existe un problema en el servicio de autenticación de Access Gateway.Se proporcionan detalles específicos al final del mensaje de error. Para obtener más información, consulte los archivos de registros del dispositivo de Access Gateway.
18004	El servicio de autenticación de Access Gateway no pudo cerrar la sesión. El mensaje emitido desde el servicio fue <*descripción del error*> [código de estado: <*número de código*>].	Error	Existe un problema en el servicio de autenticación de Access Gateway.Se proporcionan detalles específicos al final del mensaje de error. Para obtener más información, consulte los archivos de registros del dispositivo de Access Gateway.
18005	La dirección URL del servicio de autenticación de Access Gateway en la configuración del sitio no es válida: <*URL*>.	Error	La dirección URL especificada para el parámetro AGEWebServiceURL en el archivo de configuración del sitio no es válida. Corrija el error en WebInterface.conf.
18006	El usuario <*nombre del usuario*> no pudo iniciar sesión en el sitio: <*nombre del sitio*>. Reinicie el servidor Web para asegurarse de que el paso de credenciales con tarjeta inteligente del servicio de Access Gateway se encuentre activado.	Error	El usuario de la tarjeta inteligente no pudo iniciar sesión en el sitio integrado de Access Gateway. Reinicie el servidor Web para asegurarse de que el paso de credenciales con tarjeta inteligente del servicio de Access Gateway se encuentre en ejecución.
18007	Esta versión de Access Gateway no admite solicitudes de cambio de contraseña de la Interfaz Web. Para dejar que los usuarios cambien sus contraseñas, es necesario actualizar Access Gateway con una versión que admita esta funcionalidad.	Error	Este error se muestra si la función de cambio de contraseñas está habilitada en el sitio pero no se está usando una versión de Access Gateway compatible con dicha función. Inhabilite el cambio de contraseñas o actualice Access Gateway con una versión que admita dicha funcionalidad.

19001	Se produjo un error al desconectar los recursos de un usuario. El control del área de trabajo no se encuentra activado, el usuario es anónimo o se produjo un error al recuperar el nombre del cliente o las credenciales del usuario.	Error	Existe un problema en el control del área de trabajo. Compruebe que el control del área de trabajo esté activado para el sitio y que el usuario haya iniciado sesión con un método de autenticación distinto a la autenticación anónima.
19002	Se produjo un error al volver a conectar los recursos de un usuario. El control del área de trabajo no se encuentra activado, el usuario es anónimo o se produjo un error al recuperar el nombre del cliente o las credenciales del usuario.	Error	Existe un problema en el control del área de trabajo. Compruebe que el control del área de trabajo esté activado para el sitio y que el usuario haya iniciado sesión con un método de autenticación distinto a la autenticación anónima.
20001	Se produjo un error de comunicación al intentar establecer contacto con Password Manager Service a través de <*URL*>. Compruebe que el servicio se encuentre en ejecución. El mensaje emitido desde la plataforma subyacente fue <*descripción del error*>.	Error	Existe un problema al establecer contacto con Password Manager Service.Se proporcionan detalles específicos al final del mensaje de error. Para obtener más información, consulte los archivos de registros en el servidor de Password Manager.
20002	La dirección URL de Password Manager Service en la configuración del sitio no es válida: <*URL*>.	Error	La dirección URL especificada para el parámetro AccountSelfServiceUrl en el archivo de configuración del sitio no es válida. Corrija el error en WebInterface.conf.
21001	Se produjo un error crítico en el servidor.	Error	Se produjo una excepción Java en uno de los scripts que se ejecuta en la página Web. Intente volver a cargar la página. De forma alternativa, utilice la tarea Reparar sitio en Mantenimiento de sitios de la consola de administración de la Interfaz Web de Citrix para reinstalar los scripts del sitio.
21002	Error crítico en el servidor: <*descripción del error de .NET*>.	Error	Se produjo una excepción .NET en uno de los scripts que se ejecuta en la página Web. Intente volver a cargar la página. De forma alternativa, utilice la tarea Reparar sitio en Mantenimiento de sitios de la consola de administración de la Interfaz Web de Citrix para reinstalar los scripts del sitio.

21003	Debido a un error, no se pudo crear el monitor de archivos en la ruta <*directorio de configuración del sitio*>.	Error	Compruebe que la ruta a la carpeta de configuración del sitio sea la correcta y que se hayan configurado los permisos adecuados de manera que se permita la lectura de este directorio. De forma alternativa, intente reiniciar IIS para actualizar el sitio con los cambios de configuración más recientes.
21004	Un usuario no puede obtener acceso al sitio porque el nombre de dominio completo del servido Web contiene guiones (_). Cambie el nombre del servidor Web y/o del dominio para eliminar los guiones. Si esto no es posible, configure una dirección alternativa para el servidor Web que no contenga guiones o indique a los usuarios que deben obtener acceso al sitio mediante la dirección IP del servidor Web.	Error	No se puede obtener acceso a los sitios que contengan en su nombre caracteres no reconocidos, como los guiones. Compruebe que el nombre del servidor Web no contenga guiones y utilice la consola de administración de la Interfaz Web si necesita cambiar el nombre del servidor.
21005	El control ActiveX de Citrix Online Plug-in con el ID de clase <*número de ID*> no se pudo iniciar. Compruebe que se haya especificado el ID de clase correcto en el archivo de configuración del sitio.	Error	Compruebe que el ID de clase de ActiveX coincida con el número de ID en el archivo Webinterface.conf.
21006	El control ActiveX de Citrix Online Plug-in con el ID de clase <*número de ID*> no se pudo iniciar. Compruebe que se haya especificado el ID de clase correcto en el archivo de configuración del sitio.	Error	Compruebe que el ID de clase de ActiveX coincida con el número de ID en el archivo Webinterface.conf.
22001	No se pudo localizar el cliente para los archivos Java en el servidor. Compruebe que estos archivos se encuentren disponibles en la carpeta \Clients del sitio Web de XenApp.	Error	No se puede encontrar el cliente para los paquetes Java o no se puede obtener acceso a este cliente. Compruebe que no se hayan eliminado los archivos y que se hayan configurado los permisos adecuados de manera que se permita la lectura de estos archivos.

23001	Se produjo un error de ICA al intentar obtener acceso al escritorio del usuario <*nombre del usuario*>.	Error	Citrix Online Plug-in no pudo obtener acceso al escritorio del usuario. Compruebe que el escritorio se encuentre en ejecución y disponible.
23002	Internet Explorer no pudo otorgar acceso al escritorio del usuario <*nombre del usuario*>. Compruebe que Citrix Desktop Appliance Lock se encuentre instalado en el dispositivo del usuario y que Desktop Appliance Connector se haya agregado a una zona de seguridad de Windows adecuada en Internet Explorer.	Error	El usuario del dispositivo de escritorio no pudo obtener acceso a un escritorio en el modo solo de pantalla completa. Compruebe que Citrix Online Plug-in se haya instalado y configurado correctamente en el dispositivo del usuario.
23003	Se ha otorgado acceso al usuario <*nombre del usuario*> a <*número*> escritorios. Los usuarios que obtengan acceso a un escritorio en el modo solo de pantalla completa a través de Desktop Appliance Connector deben poder tener acceso únicamente a un solo escritorio.	Advertencia	Se ha puesto más de un escritorio a disposición del usuario del dispositivo de escritorio. El usuario puede obtener acceso a un escritorio. Sin embargo, como no existe una forma de seleccionar el escritorio requerido, es posible que el usuario no se conecte al mismo escritorio la próxima vez que inicie sesión. Configure Desktop Appliance Connector de manera que el usuario solamente pueda obtener acceso a un solo escritorio.
23004	El método de autenticación especificado no es válido. Debe especificar "Explícita" o "Certificada", pero no ambas opciones.	Error	Se especificaron los valores Explicit y Certificate para el parámetro WIAuthenticationMethods en el archivo de configuración del sitio. No se puede activar la autenticación explícita y con tarjeta inteligente en el mismo Desktop Appliance Connector. Corrija el error en WebInterface.conf.
23005	La configuración de autenticación SSO de la tarjeta inteligente incrustada no es válida. El método de autenticación debe incluir el valor "Certificate".	Error	Se debe especificar el valor Certificate para el parámetro WIAuthenticationMethods en el archivo de configuración del sitio para Desktop Appliance Connector. Corrija el error en WebInterface.conf.

23006	Los métodos de autenticación especificados no son válidos. No se admite la combinación de métodos de autenticación.	Error	Los métodos de autenticación especificados para Desktop Appliance Connector en el parámetro WIAuthenticationMethods del archivo de configuración del sitio no se pueden utilizar de forma conjunta. Corrija el error en WebInterface.conf.
24001	Un usuario sin autenticación ha intentado iniciar sesión. Verifique que se hayan creado cuentas sombra para todos los usuarios del sistema. Si el problema continúa, intente reparar el sitio mediante la consola de administración de la Interfaz Web.	Error	Existe un problema en el sitio integrado de AD FS. El usuario no pudo ser autenticado. Compruebe que se haya creado una cuenta sombra para el usuario en el dominio del asociado de recurso. De forma alternativa, utilice la tarea Reparar sitio en Mantenimiento de sitios de la consola de administración de la Interfaz Web de Citrix para reinstalar el sitio.
24002	Un usuario sin autenticación ha intentado iniciar sesión. Si el problema continúa, intente reparar el sitio mediante la consola de administración de la Interfaz Web.	Error	Existe un problema en el sitio Web de XenApp o el sitio de servicios XenApp. El usuario no pudo ser autenticado. Compruebe que se haya creado una cuenta de usuario para el usuario en el dominio. De forma alternativa, utilice la tarea Reparar sitio en Mantenimiento de sitios de la consola de administración de la Interfaz Web de Citrix para reinstalar el sitio.
30001	Se produjo un error al intentar leer la información de los servidores Citrix: <*nombre de la comunidad*>. Este mensaje se emitió desde XML Service en la dirección <*ruta del archivo*>. *descripción del error*>	Error	Existe un problema en Citrix XML Service.Se proporcionan detalles específicos al final del mensaje de error. Para obtener más información, consulte los archivos de registros en el servidor Citrix.
30002	Se produjo un error al intentar escribir información en los servidores Citrix: <*nombre de la comunidad*>. Este mensaje se emitió desde XML Service en la dirección <*ruta del archivo*>. *descripción del error*>	Error	Existe un problema en Citrix XML Service.Se proporcionan detalles específicos al final del mensaje de error. Para obtener más información, consulte los archivos de registros en el servidor Citrix.

30003	Se produjo un error al intentar establecer la conexión con el servidor <*dirección del servidor*> en el puerto <*puerto*>. Verifique que Citrix XML Service se encuentre en ejecución y utilice el puerto correcto. Si XML Service se ha configurado para compartir puertos con Microsoft Internet Information Services (IIS), verifique que IIS se encuentre en ejecución. Este mensaje se emitió desde XML Service en la dirección <*ruta del archivo*>. *descripción del error*>	Error	Existe un problema en Citrix XML Service.Se proporcionan detalles específicos al final del mensaje de error. Compruebe si XML Service se haya configurado para compartir puertos TCP/IP con IIS y, de ser así, compruebe que IIS se encuentre en ejecución. Para obtener más información, consulte los archivos de registros en el servidor Citrix.
30004	No se puede resolver el nombre del servidor <*dirección del servidor*>. *descripción del error*>	Error	Existe un problema en Citrix XML Service.Se proporcionan detalles específicos al final del mensaje de error. Para obtener más información, consulte los archivos de registros en el servidor Citrix.
30005	La sintaxis HTTP que envían los servidores Citrix es incorrecta. Verifique si la versión de la Interfaz Web vigente es compatible con los servidores que se utilizan. Este mensaje se emitió desde XML Service en la dirección <*ruta del archivo*>. *descripción del error*>	Error	Existe un problema en Citrix XML Service.Se proporcionan detalles específicos al final del mensaje de error. Compruebe que la comunidad de servidores ejecute XenDesktop o Presentation Server 4.5 (o una versión posterior). Citrix recomienda ejecutar el mismo producto y la misma versión en todos los servidores de una comunidad. Para obtener más información, consulte los archivos de registros en el servidor Citrix.
30006	La respuesta que envían los servidores Citrix es incorrecta o inesperada. Verifique si la versión de la Interfaz Web vigente es compatible con los servidores que se utilizan. Este mensaje se emitió desde XML Service en la dirección <*ruta del archivo*>. *descripción del error*>	Error	Existe un problema en Citrix XML Service.Se proporcionan detalles específicos al final del mensaje de error. Compruebe que la comunidad de servidores ejecute XenDesktop o Presentation Server 4.5 (o una versión posterior). Citrix recomienda ejecutar el mismo producto y la misma versión en todos los servidores de una comunidad. Para obtener más información, consulte los archivos de registros en el servidor Citrix.

30008	Los servidores Citrix desactivaron la conexión inesperadamente. Este mensaje se emitió desde XML Service en la dirección <*ruta del archivo*>. *descripción del error*>	Error	Existe un problema en Citrix XML Service.Se proporcionan detalles específicos al final del mensaje de error. Para obtener más información, consulte los archivos de registros en el servidor Citrix.
30009	Los servidores Citrix enviaron encabezados HTTP en los que indican que se produjo un error: <*detalles*>. Este mensaje se emitió desde XML Service en la dirección <*ruta del archivo*>. *descripción del error*>	Error	Existe un problema en Citrix XML Service.Se proporcionan detalles específicos al final del mensaje de error. Para obtener más información, consulte los archivos de registros en el servidor Citrix.
30010	Los servidores Citrix no pueden procesar la solicitud en este momento. Este mensaje se emitió desde XML Service en la dirección <*ruta del archivo*>. *descripción del error*>	Error	Existe un problema en Citrix XML Service.Se proporcionan detalles específicos al final del mensaje de error. Para obtener más información, consulte los archivos de registros en el servidor Citrix.
30011	Se produjo un error en los servidores Citrix al intentar completar la solicitud: <*detalles*>. Este mensaje se emitió desde XML Service en la dirección <*ruta del archivo*>. *descripción del error*>	Error	Existe un problema en Citrix XML Service.Se proporcionan detalles específicos al final del mensaje de error. Para obtener más información, consulte los archivos de registros en el servidor Citrix.
30012	Los servidores Citrix detectaron un error de discordancia de versiones. Este mensaje se emitió desde XML Service en la dirección <*ruta del archivo*>. *descripción del error*>	Error	Existe un problema en Citrix XML Service.Se proporcionan detalles específicos al final del mensaje de error. Para obtener más información, consulte los archivos de registros en el servidor Citrix.
30013	Los servidores Citrix recibieron una solicitud incorrecta. Este mensaje se emitió desde XML Service en la dirección <*ruta del archivo*>. *descripción del error*>	Error	Existe un problema en Citrix XML Service.Se proporcionan detalles específicos al final del mensaje de error. Para obtener más información, consulte los archivos de registros en el servidor Citrix.
30014	Se produjo un error en los servidores Citrix durante el análisis de la solicitud. Este mensaje se emitió desde XML Service en la dirección <*ruta del archivo*>. *descripción del error*>	Error	Existe un problema en Citrix XML Service.Se proporcionan detalles específicos al final del mensaje de error. Para obtener más información, consulte los archivos de registros en el servidor Citrix.

30015	Citrix XML Service en la dirección <*ruta del archivo*> no puede procesar las solicitudes.	Error	Existe un problema en Citrix XML Service.Se proporcionan detalles específicos al final del mensaje de error. Para obtener más información, consulte los archivos de registros en el servidor Citrix.
30016	No se pudo encontrar el objeto de Citrix XML Service: <*detalles*>. Este mensaje se emitió desde XML Service en la dirección <*ruta del archivo*>. *descripción del error*>	Error	Existe un problema en Citrix XML Service.Se proporcionan detalles específicos al final del mensaje de error. Para obtener más información, consulte los archivos de registros en el servidor Citrix.
30017	No se admite el método de Citrix XML Service: <*detalles*>. Este mensaje se emitió desde XML Service en la dirección <*ruta del archivo*>. *descripción del error*>	Error	Existe un problema en Citrix XML Service.Se proporcionan detalles específicos al final del mensaje de error. Para obtener más información, consulte los archivos de registros en el servidor Citrix.
30018	La respuesta de Citrix XML Service no es aceptable: <*detalles*>. Este mensaje se emitió desde XML Service en la dirección <*ruta del archivo*>. *descripción del error*>	Error	Existe un problema en Citrix XML Service.Se proporcionan detalles específicos al final del mensaje de error. Para obtener más información, consulte los archivos de registros en el servidor Citrix.
30019	La solicitud de Citrix XML Service presenta requisitos de extensión: <*detalles*>. Este mensaje se emitió desde XML Service en la dirección <*ruta del archivo*>. *descripción del error*>	Error	Existe un problema en Citrix XML Service.Se proporcionan detalles específicos al final del mensaje de error. Para obtener más información, consulte los archivos de registros en el servidor Citrix.
30020	La solicitud de Citrix XML Service es demasiado corta: <*detalles*>. Este mensaje se emitió desde XML Service en la dirección <*ruta del archivo*>. *descripción del error*>	Error	Existe un problema en Citrix XML Service.Se proporcionan detalles específicos al final del mensaje de error. Para obtener más información, consulte los archivos de registros en el servidor Citrix.
30021	La solicitud de Citrix XML Service supera el tamaño máximo: <*detalles*>. Este mensaje se emitió desde XML Service en la dirección <*ruta del archivo*>. *descripción del error*>	Error	Existe un problema en Citrix XML Service.Se proporcionan detalles específicos al final del mensaje de error. Para obtener más información, consulte los archivos de registros en el servidor Citrix.

30022	Es posible que Citrix XML Service o los servidores Citrix no estén disponibles o se encuentren sobrecargados temporalmente: <*detalles*>. Este mensaje se emitió desde XML Service en la dirección <*ruta del archivo*>. *descripción del error*>	Error	Existe un problema en Citrix XML Service.Se proporcionan detalles específicos al final del mensaje de error. Para obtener más información, consulte los archivos de registros en el servidor Citrix.
30023	No se pudo procesar el documento XML que enviaron los servidores Citrix. Este mensaje se emitió desde XML Service en la dirección <*ruta del archivo*>. *descripción del error*>	Error	Existe un problema en Citrix XML Service.Se proporcionan detalles específicos al final del mensaje de error. Para obtener más información, consulte los archivos de registros en el servidor Citrix.
30024	No se pudo procesar el documento XML que enviaron los servidores Citrix porque contiene un archivo XML no válido. Este mensaje se emitió desde XML Service en la dirección <*ruta del archivo*>. *descripción del error*>	Error	Existe un problema en Citrix XML Service.Se proporcionan detalles específicos al final del mensaje de error. Para obtener más información, consulte los archivos de registros en el servidor Citrix.
30025	Se produjo un error al intentar leer la información de los servidores Citrix: <*nombre de la comunidad*>. Este error se puede generar al intentar comunicarse con una herramienta alternativa al Traspaso SSL. Este mensaje se emitió desde XML Service en la dirección <*ruta del archivo*>. *descripción del error*>	Error	Existe un problema en Citrix XML Service.Se proporcionan detalles específicos al final del mensaje de error. Para utilizar el cifrado SSL/TLS en conexiones a la comunidad de servidores, es necesario utilizar el Traspaso SSL para configurar el respaldo de cada servidor. Para obtener más información, consulte los archivos de registros en el servidor Citrix.

30026	Se produjo un error al intentar establecer una conexión con el Traspaso SSL: <*dirección del servidor*>:<*puerto*>. Compruebe que exista un Traspaso SSL en ejecución y que funcione en un puerto válido. El nombre que figura en el certificado del servidor en el que el Traspaso SSL se ha configurado para contactar debe coincidir de forma exacta con el nombre del servidor con el cual se intentó establecer la conexión. Este mensaje se emitió desde Citrix XML Service en la dirección <*ruta del archivo*>. *descripción del error*>	Error	Existe un problema en Citrix XML Service.Se proporcionan detalles específicos al final del mensaje de error. Compruebe que el Traspaso SSL se encuentre en ejecución y funcione en el puerto adecuado (generalmente el puerto 443) y que el certificado del servidor del Traspaso SSL contenga el nombre completo del servidor (con el uso de mayúsculas y minúsculas correcto) con el que se intentó establecer la conexión. Para obtener más información, consulte los archivos de registros en el servidor Citrix.
30027	Es posible que la generación de tiquets no sea compatible con uno o varios servidores Citrix. Para utilizar esta función, debe actualizar los servidores que ejecutan XML Service, sino debe desactivar la generación de tiquets. Este mensaje se emitió desde XML Service en la dirección <*ruta del archivo*>. *descripción del error*>	Error	Existe un problema en Citrix XML Service.Se proporcionan detalles específicos al final del mensaje de error. Compruebe que todos los servidores de la comunidad ejecuten XenDesktop o MetaFrame XP 1.0 (o una versión posterior). Citrix recomienda ejecutar el mismo producto y la misma versión en todos los servidores de una comunidad. Para obtener más información, consulte los archivos de registros en el servidor Citrix.
30028	No se puede resolver el nombre del Traspaso SSL <*dirección del servidor*>. *descripción del error*>	Error	Existe un problema en Citrix XML Service.Se proporcionan detalles específicos al final del mensaje de error. Para obtener más información, consulte los archivos de registros en el servidor Citrix.
30029	No se pudo establecer una conexión SSL: <*descripción del error SSL*>. Este mensaje se emitió desde Citrix XML Service en la dirección <*ruta del archivo*>. *descripción del error*>	Error	Existe un problema en Citrix XML Service.Se proporcionan detalles específicos al final del mensaje de error. Para obtener más información, consulte los archivos de registros en el servidor Citrix.

30030	No se pudo establecer una conexión con Traspaso SSL: <*descripción del error SSL*>. Este mensaje se emitió desde Citrix XML Service en la dirección <*ruta del archivo*>. *descripción del error*>	Error	Existe un problema en Citrix XML Service.Se proporcionan detalles específicos al final del mensaje de error. Para obtener más información, consulte los archivos de registros en el servidor Citrix.
30031	Citrix XML Service en la dirección <*ruta del archivo*> no admite la característica <*nombre de la función*>.	Error	Compruebe que todos los servidores de la comunidad ejecuten una versión de XenApp o XenDesktop que sea compatible con la función especificada. Para obtener más información, consulte Requisitos mínimos de software.
30101	El intento de cambio de contraseña se dañó.	Error	Por razones de seguridad, el usuario no pudo cambiar la contraseña de Windows. Para obtener más información, consulte los archivos de registros de los servidores Citrix y/o del controlador de dominios.
30102	Los servidores Citrix notificaron un error no especificado desde XML Service en la dirección <*ruta del archivo*>.	Error	Existe un problema en Citrix XML Service.Se proporcionan detalles específicos al final del mensaje de error. Para obtener más información, consulte los archivos de registros en el servidor Citrix.
30103	Los servidores Citrix notificaron que no se pudo encontrar la dirección alternativa. Este mensaje se emitió desde XML Service en la dirección <*ruta del archivo*>. *descripción del error*>	Error	Existe un problema en Citrix XML Service.Se proporcionan detalles específicos al final del mensaje de error. Para obtener más información, consulte los archivos de registros en el servidor Citrix.
30104	Se produjo un error al establecer la conexión con el servidor Citrix para obtener acceso al recurso. Compruebe que el servidor se encuentre en ejecución y que la red esté en funcionamiento. Este error se emitió para un servicio XML Service en la dirección <*ruta del archivo*>. *descripción del error*>	Error	Existe un problema en Citrix XML Service.Se proporcionan detalles específicos al final del mensaje de error. Compruebe que no existan problemas en la comunidad de servidores y la red. Para obtener más información, consulte los archivos de registros en el servidor Citrix.

30105	Los servidores Citrix no confían en el servidor. Este mensaje se emitió desde XML Service en la dirección <*ruta del archivo*>. *descripción del error*>	Error	Compruebe que exista una relación de confianza entre el servidor de la Interfaz Web y Citrix XML Service. Para obtener más información, consulte Uso del control del área de trabajo con métodos de autenticación integrados para los sitios Web de XenApp.
30106	Los servidores Citrix no cuentan con las licencias para admitir la operación solicitada. Este mensaje se emitió desde XML Service en la dirección <*ruta del archivo*>. *descripción del error*>	Error	Existe un problema en Citrix XML Service.Se proporcionan detalles específicos al final del mensaje de error. Compruebe que el servidor de licencias de Citrix se encuentre en ejecución y disponible. Citrix recomienda actualizar el servidor de licencias a la versión más reciente para garantizar la compatibilidad con los últimos productos. Para obtener más información, consulte los archivos de registros del servidor Citrix y/o del servidor de licencias.
30107	Los servidores Citrix notificaron que se encuentran demasiado ocupados como para otorgar acceso al recurso seleccionado. Este mensaje se emitió desde XML Service en la dirección <*ruta del archivo*>. *descripción del error*>	Error	Existe un problema en Citrix XML Service.Se proporcionan detalles específicos al final del mensaje de error. Compruebe que la comunidad de servidores no se encuentre sobrecargada. Para obtener más información, consulte los archivos de registros en el servidor Citrix.
30108	La función de generación de tiquets se encuentra desactivada en el servidor Citrix. Este mensaje se emitió desde XML Service en la dirección <*ruta del archivo*>. *descripción del error*>	Error	Existe un problema en Citrix XML Service.Se proporcionan detalles específicos al final del mensaje de error. Compruebe que todos los servidores de la comunidad utilicen el mismo puerto para comunicarse con XML Service. Para obtener más información, consulte los archivos de registros en el servidor Citrix.
30109	Citrix XML Service en la dirección <*ruta del archivo*> notificó un error de registro. *descripción del error*>	Error	Existe un problema en Citrix XML Service.Se proporcionan detalles específicos al final del mensaje de error. Para obtener más información, consulte los archivos de registros en el servidor Citrix.

30110	Un error del tipo <*tipo de error*> con un ID de error <*ID de error*> se emitió desde Citrix XML Service en la dirección <*ruta del archivo*>. Según el servidor que ejecute XML Service, es posible que exista más información disponible en el registro de sucesos del servidor. *descripción del error*>	Error	Existe un problema en Citrix XML Service.Se proporcionan detalles específicos al final del mensaje de error. Para obtener más información, consulte los archivos de registros en el servidor Citrix.
30111	Los servidores Citrix no son compatibles con el tipo de dirección especificada. Este mensaje se emitió desde XML Service en la dirección <*ruta del archivo*>. *descripción del error*>	Error	Existe un problema en Citrix XML Service.Se proporcionan detalles específicos al final del mensaje de error. Para obtener más información, consulte los archivos de registros en el servidor Citrix.
30112	No se pudo encontrar ningún recurso disponible para el usuario <*nombre del usuario*> al obtener acceso al grupo de escritorios <*nombre del grupo*>. Este mensaje se emitió desde Citrix XML Service en la dirección <*ruta del archivo*>. *descripción del error*>	Error	Existe un problema en Citrix XML Service.Se proporcionan detalles específicos al final del mensaje de error. Compruebe que el usuario se haya asignado al grupo de escritorios especificado y que existan escritorios sin utilizar disponibles en el grupo. Para obtener más información, consulte los archivos de registros en el servidor Citrix.
30113	Se rechazó una solicitud del servidor Citrix para preparar una conexión durante el procesamiento de la inicialización del grupo de escritorios <*nombre del grupo*> para el usuario <*nombre del usuario*>. Este mensaje se emitió desde XML Service en la dirección <*ruta del archivo*>. *descripción del error*>	Error	Existe un problema en Citrix XML Service. Se proporcionan detalles específicos al final del mensaje de error. Para obtener más información, consulte los archivos de registros en el servidor Citrix.

30114	Se les denegó el acceso a los servidores Citrix para recuperar los identificadores de seguridad del usuario. Conceda permisos de lectura a XML Service para el atributo Token-Groups-Global-And-Universal en Active Directory, o bien, desactive la enumeración de identificadores de seguridad en XML Service. Este mensaje se emitió desde XML Service en la dirección <*ruta del archivo*>. *descripción del error*>	Error	Existe un problema en Citrix XML Service. Se proporcionan detalles específicos al final del mensaje de error. Si XML Service se ha configurado para enumerar los identificadores de seguridad de los usuarios, compruebe que se hayan otorgado los permisos adecuados en Active Directory. Para obtener más información, consulte CTX117489 y los archivos de registros en el servidor Citrix.
30115	Los servidores Citrix no pudieron recuperar los identificadores de seguridad del usuario. Este mensaje se emitió desde XML Service en la dirección <*ruta del archivo*>. *descripción del error*>	Error	Existe un problema en Citrix XML Service. Se proporcionan detalles específicos al final del mensaje de error. Para obtener más información, consulte CTX117489 y los archivos de registros en el servidor Citrix.
30116	No se pudo establecer la conexión con un escritorio en el modo de mantenimiento para el usuario <*nombre del usuario*> al inicializar el grupo de escritorios <*nombre del grupo*>. Este mensaje se emitió desde Citrix XML Service en la dirección <*ruta del archivo*>. *descripción del error*>	Error	Existe un problema en Citrix XML Service. Se proporcionan detalles específicos al final del mensaje de error. Compruebe que el escritorio del usuario no se encuentre en el modo de mantenimiento. Para obtener más información, consulte los archivos de registros en el servidor Citrix.
30117	Los servidores Citrix no admiten la operación de reinicio del escritorio. Este mensaje se emitió desde XML Service en la dirección <*ruta del archivo*>. *descripción del error*>	Error	Existe un problema en Citrix XML Service. Se proporcionan detalles específicos al final del mensaje de error. Compruebe que la comunidad de servidores ejecute XenDesktop 3.0 o una versión posterior. Citrix recomienda ejecutar el mismo producto y la misma versión en todos los servidores de una comunidad. Para obtener más información, consulte los archivos de registros en el servidor Citrix.

30118	Los servidores Citrix excedieron el tiempo de espera para que un equipo del grupo de escritorios <*nombre del grupo*> se apague para el usuario <*nombre del usuario*>. Este mensaje se emitió desde XML Service en la dirección <*ruta del archivo*>. *descripción del error*>	Error	Existe un problema en Citrix XML Service. Se proporcionan detalles específicos al final del mensaje de error. Para obtener más información, consulte los archivos de registros en el servidor Citrix.
30119	No se puede apagar un equipo en el modo de mantenimiento en el grupo de escritorios <*nombre del grupo*> para el usuario <*nombre del usuario*>. Este mensaje se emitió desde Citrix XML Service en la dirección <*ruta del archivo*>. *descripción del error*>	Error	Existe un problema en Citrix XML Service. Se proporcionan detalles específicos al final del mensaje de error. Compruebe que el escritorio del usuario no se encuentre en el modo de mantenimiento. Para obtener más información, consulte los archivos de registros en el servidor Citrix.
30120	No se puede encontrar el usuario <*nombre de usuario*>. Este mensaje se emitió desde Citrix XML Service en la dirección <*ruta del archivo*>. *descripción del error*>	Error	Existe un problema en Citrix XML Service. Se proporcionan detalles específicos al final del mensaje de error. Para obtener más información, consulte los archivos de registros en el servidor Citrix.
30201	La dirección de Secure Ticket Authority no es válida: <*URL*>. *descripción del error*>	Error	La dirección URL especificada para el parámetro **CSG_STA_ URL<*n*>** en el archivo de configuración del sitio no es válida. Corrija el error en WebInterface.conf.
30202	El servidor Secure Ticket Authority en <*URL*> no admite solicitudes de la versión 4. Todas las comunicaciones de Secure Ticket Authority recurrirán a la versión 1. Las nuevas conexiones a través de Secure Gateway no utilizarán la fiabilidad de la sesión.	Error	La versión de Secure Gateway en uso no admite la función de redundancia de Secure Ticket Authority. Como resultado, esta función se ha desactivado.
30203	El servidor Secure Ticket Authority en <*URL*> devolvió un tiquet con un tipo o autoridad inesperados - <*tipo de error*>, <*ID de error*>, <*descripción del error SSL*>, <*detalles*>. *descripción del error*>	Error	Existe un problema en Secure Ticket Authority.Se proporcionan detalles específicos al final del mensaje de error. Para obtener más información, consulte los archivos de registros en el servidor Citrix.

30204	No se pudo establecer contacto con la Secure Ticket Authority especificada y esta autoridad se ha eliminado temporalmente de la lista de servicios activos.	Error	Existe un problema en Secure Ticket Authority. Este servicio se ignorará hasta que se resuelva el problema. Para obtener más información, consulte los archivos de registros en el servidor Citrix.
30205	Ninguno de los servidores Secure Ticket Authority pudo responder a esta transacción XML.	Error	No se pudo establecer contacto con ninguna de las Secure Ticket Authorities. Intente reiniciar el servidor Web. Para obtener más información, consulte los archivos de registros en los servidores Citrix.
30301	La respuesta HTTP indica que la conexión subyacente se desactivó.	Error	Compruebe que la comunidad de servidores ejecute XenDesktop o Presentation Server 4.5 (o una versión posterior). Citrix recomienda ejecutar el mismo producto y la misma versión en todos los servidores de una comunidad.
30401	La capa de transacción destruyó un socket por la fuerza.	Error	Compruebe si existen aplicaciones dañadas en el almacén de datos de la comunidad. Para obtener más información, consulte CTX114769.
31001	No se pudo establecer contacto con el servicio Citrix XML Service especificado y se ha eliminado temporalmente de la lista de servicios activos.	Error	Existe un problema con Citrix XML Service. Este servidor se ignorará hasta que se resuelva el problema. Para obtener más información, consulte los archivos de registros en el servidor Citrix.
31002	No se pudo ejecutar esta transacción de XML Service pero este servicio permanece en la lista de servicios activos.	Error	Si bien se puede obtener acceso a Citrix XML Service, la solicitud o la instrucción no se pudo completar. Para obtener más información, consulte los archivos de registros en el servidor Citrix.
31003	Ninguno de los servicios Citrix XML Service configurados para la comunidad <*nombre de la comunidad*> pudo responder a esta transacción de XML Service.	Error	No se pudo establecer contacto con ninguno de los hosts de Citrix XML Service para la comunidad especificada. Intente reiniciar el servidor Web. Para obtener más información, consulte los archivos de registros en los servidores Citrix.

31004	No se pudo convertir el error de protocolo XML <*ID de error*> a un error de estado de acceso.	Error	Compruebe que el usuario posea derechos de inicio de sesión de Active Directory para los servidores Citrix.
31005	Se ignoraron <*número*> de <*número*> de recursos por no ser válidos.	Error	Citrix XML Service no pudo enumerar todos los recursos disponibles. Para obtener más información, consulte los archivos de registros en el servidor Citrix.
31006	Se rechazó el inicio de sesión del usuario <*nombre de usuario*> porque el usuario no contaba con ninguna licencia.	Error	El usuario no pudo iniciar sesión porque no había licencias de Citrix ni licencias de acceso de clientes a Servicios de Escritorio remoto de Microsoft disponibles. Compruebe que el servidor de licencias de Citrix se encuentre en ejecución y disponible. Citrix recomienda actualizar el servidor de licencias a la versión más reciente para garantizar la compatibilidad con los últimos productos. Para obtener más información, consulte los archivos de registros de los servidores Citrix y/o del servidor de licencias.
31007	Los servidores Citrix no cuentan con la licencia necesaria para admitir el control del área de trabajo. Este mensaje se emitió desde XML Service en la dirección <*ruta del archivo*>.	Error	Compruebe que las licencias de Citrix habiliten una edición del producto que incluya la función de control del área de trabajo. Además, compruebe que el servidor de licencias de Citrix se encuentre en ejecución y disponible. Citrix recomienda actualizar el servidor de licencias a la versión más reciente para garantizar la compatibilidad con los últimos productos. Para obtener más información, consulte los archivos de registros del servidor Citrix y/o del servidor de licencias.

31008	Los servidores Citrix no cuentan con la licencia necesaria para iniciar el recurso <*nombre del recurso*>. Este mensaje se emitió desde XML Service en la dirección <*ruta del archivo*>.	Error	Compruebe que las licencias de Citrix habiliten una edición del producto que incluya este tipo de recurso. Además, compruebe que el servidor de licencias de Citrix se encuentre en ejecución y disponible. Citrix recomienda actualizar el servidor de licencias a la versión más reciente para garantizar la compatibilidad con los últimos productos. Para obtener más información, consulte los archivos de registros del servidor Citrix y/o del servidor de licencias.
31009	No se pueden obtener los datos de la cuenta para las cuentas siguientes: <*lista de nombres de cuentas*> Compruebe si el nombre está escrito correctamente. Este mensaje se emitió desde Citrix XML Service en la dirección <*ruta del archivo*>.	Error	Citrix XML Service no puede obtener acceso a las cuentas especificadas. Compruebe que las cuentas no se hayan eliminado y que se hayan configurado los permisos adecuados para que XML Service pueda leerlas. Además, compruebe que los nombres de las cuentas se hayan introducido correctamente. Para obtener más información, consulte los archivos de registros en el servidor Citrix.
31101	El usuario <*nombre del usuario*> dispone de una sesión del servidor, <*ID de sesión*>, pero no cuenta con acceso a <*nombre del recurso*>, el recurso que originó la sesión. Como resultado, el usuario no puede obtener acceso a esa sesión.	Error	Los permisos de acceso del usuario se modificaron mientras la sesión del usuario se encontraba activa. Restablezca la sesión. Tenga en cuenta que esta acción generará una pérdida de datos para el usuario. Para obtener más información, consulte los archivos de registros en el servidor Citrix.
31201	La comunidad <*nombre de la comunidad*> se ha configurado para utilizar la generación de tiquets, pero no ha recibido ninguna etiqueta de tiquet. Compruebe si la comunidad admite la generación de tiquets.	Error	Compruebe que todos los servidores de la comunidad especificada ejecuten XenDesktop o MetaFrame XP 1.0 (o una versión posterior). Citrix recomienda ejecutar el mismo producto y la misma versión en todos los servidores de una comunidad. Para obtener más información, consulte los archivos de registros en los servidores Citrix.

31202	Un usuario intentó iniciar el recurso <*nombre del recurso*>, que se encuentra inhabilitado.	Error	Compruebe que el recurso especificado esté activado en el servidor en el que se encuentre alojado.
31203	La comunidad <*nombre de la comunidad*> se ha configurado para utilizar referencias de inicio, pero no ha recibido ninguna referencia de inicio desde Citrix XML Service. Compruebe si la comunidad admite referencias de inicio o desactive las solicitudes de referencias de inicio.	Error	Para utilizar referencias de inicio, todos los servidores de la comunidad especificada deben ejecutar XenDesktop o Presentation Server 4.5 (o una versión posterior). Citrix recomienda ejecutar el mismo producto y la misma versión en todos los servidores de una comunidad. Si la comunidad ejecuta XenApp 4.0 con Feature Pack 1, para UNIX o Presentation Server 4.0 y sus versiones anteriores, asegúrese de que el parámetro RequireLaunchReference esté configurado en Off y que OverrideIcaClientname esté configurado en On en el archivo de configuración del sitio Web de XenApp, WebInterface.conf.
31301	La configuración de la comunidad <*nombre de la comunidad*> no es válida.	Error	Existe un problema en la comunidad de servidores especificada. Para obtener más información, consulte los archivos de registros en los servidores Citrix.
32001	La configuración no incluye detalles sobre ninguno de los servidores Citrix.	Error	No se han especificado comunidades para el parámetro **Farm<*n*>** en el archivo de configuración del sitio de servicios XenApp. Corrija el error en WebInterface.conf.
32002	No se puede analizar la configuración de la cadena de proveedores.	Error	Existe un problema en el sitio de servicios XenApp. Compruebe si existen errores en los archivos de configuración del sitio.
32003	<*Causa del error*> Ocurrió el siguiente error de sistema: <*descripción del error*>	Error	Existe un problema en el sitio de servicios XenApp.Se proporcionan detalles específicos al final del mensaje de error. Compruebe si existen errores en los archivos de configuración del sitio.

33001	Citrix Streaming Service: No se pudo establecer contacto con el servicio Citrix XML Service especificado y se ha eliminado temporalmente de la lista de servicios activos.	Error	Citrix Offline Plug-in detectó un problema en Citrix XML Service. Este servicio se ignorará hasta que se resuelva el problema. Para obtener más información, consulte los archivos de registros en el servidor Citrix.
33002	Citrix Streaming Service: No se pudo ejecutar esta transacción de Citrix XML Service pero dicho servicio permanece en la lista de servicios activos.	Error	Si bien Citrix XML Service puede obtener acceso a Citrix Offline Plug-in, la solicitud o la instrucción no se pudo completar. Para obtener más información, consulte los archivos de registros en el servidor Citrix.
33003	Citrix Streaming Service: Ninguno de los servicios Citrix XML Service configurados para la comunidad <*nombre de la comunidad*> pudo responder a esta transacción de XML Service.	Error	Citrix Offline Plug-in no pudo establecer contacto con ninguno de los hosts de Citrix XML Service para la comunidad especificada. Intente reiniciar el servidor Web. Para obtener más información, consulte los archivos de registros en los servidores Citrix.
33004	Citrix Streaming Service: La configuración de la comunidad <*nombre de la comunidad*> no es válida.	Error	Citrix Offline Plug-in detectó un problema con la comunidad de servidores especificada. Para obtener más información, consulte los archivos de registros en los servidores Citrix.
33005	Citrix Streaming Service: La configuración no incluye detalles sobre ninguno de los servidores Citrix.	Error	No se han especificado comunidades para el parámetro **Farm<*n*>** en el archivo de configuración del sitio. Corrija el error en WebInterface.conf.
33006	No se pudo cargar el archivo de configuración RadeValidationRules.conf. Compruebe que el archivo se encuentre disponible en la carpeta de configuración del sitio.	Error	No se puede encontrar el archivo RadeValidationRules.conf o no se puede obtener acceso a este archivo. Compruebe que no se haya eliminado el archivo y que se hayan configurado los permisos adecuados de modo que se permita la lectura de este archivo.

33007	No se puede utilizar el archivo de configuración RadeValidationRules.conf porque contiene reglas no válidas. Compruebe que todas las reglas utilicen una sintaxis de expresiones regulares válida.	Error	Existe un problema en el archivo de configuración RadeValidationRules.conf. Todas las reglas de este archivo deben determinarse mediante una sintaxis de expresiones regulares. Busque errores en el archivo. De forma alternativa, utilice la tarea Reparar sitio en Mantenimiento de sitios de la consola de administración de la Interfaz Web de Citrix para reinstalar el sitio. Se descartarán todos los cambios que haya implementado en el archivo.
34001	La configuración no incluye detalles sobre ninguno de los servidores Citrix.	Error	No se han especificado comunidades para el parámetro **Farm<*n*>** en el archivo de configuración del sitio Web de XenApp o Desktop Appliance Connector. Corrija el error en WebInterface.conf.
34002	No se puede analizar la configuración de la cadena de proveedores.	Error	Existe un problema en el sitio Web de Desktop Appliance Connector o XenApp. Compruebe si existen errores en WebInterface.conf.
34003	<*Causa del error*> Ocurrió el siguiente error de sistema: <*descripción del error*>	Error	Existe un problema en el sitio de servicios XenApp.Se proporcionan detalles específicos al final del mensaje de error. Compruebe si existen errores en WebInterface.conf.
40001	Se produjo un error al enumerar los recursos de un usuario. Se recibió un mensaje XML no reconocido de un dispositivo del usuario.	Error	Citrix Online Plug-in detectó un problema al conectarse con los servidores Citrix. Compruebe que Citrix Online Plug-in se haya configurado correctamente en el dispositivo del usuario.
40002	Se produjo un error al enumerar los recursos de un usuario. Se recibió un mensaje XML no reconocido de un dispositivo del usuario.	Error	Citrix Online Plug-in detectó un problema al conectarse con los servidores Citrix. Compruebe que Citrix Online Plug-in se haya configurado correctamente en el dispositivo del usuario.

40003	Se produjo un error al volver a conectar los recursos de un usuario. Se recibió un mensaje XML no reconocido de un dispositivo del usuario.	Error	Citrix Online Plug-in detectó un problema al volver a conectarse con los servidores Citrix. Compruebe que Citrix Online Plug-in se haya configurado correctamente en el dispositivo del usuario.
40004	La *dirección IP*> *solicitó una configuración de Citrix Online Plug-in* en <nombre del archivo>, que no existe.	Error	Compruebe que en el dispositivo del usuario se haya introducido correctamente la dirección URL del archivo de configuración en el cuadro de diálogo Opciones para Citrix Online Plug-in.
40005	Se produjo un error al iniciar un recurso del usuario: <*descripción del error*>	Error	Citrix Online Plug-in detectó un problema.Se proporcionan detalles específicos al final del mensaje de error. Para obtener más información, consulte los archivos de registros en los servidores Citrix.
40006	Se produjo un error al ejecutar una operación de control de escritorios. Se recibió un mensaje XML no reconocido de un dispositivo del usuario.	Error	Citrix Online Plug-in detectó un problema al reiniciar el escritorio del usuario. Compruebe que Citrix Online Plug-in se haya configurado correctamente en el dispositivo del usuario.

Desactivación de mensajes de error

En IIS se pueden desactivar los mensajes de error suministrados con la Interfaz Web y mostrar en su lugar el error subyacente. Para ello, modifique el archivo web.config ubicado en el directorio raíz del sitio. Cambie la línea:

<customErrors mode="On" defaultRedirect="~/html/serverError.html">

por:

<customErrors mode="Off" defaultRedirect="~/html/serverError.html">

También se pueden mostrar mensajes de error personalizados. Para ello, cambie la línea por:

<customErrors mode="On" defaultRedirect="~/html/*CustomErrorPage*">

donde *CustomErrorPage* es el nombre de archivo de la página de errores personalizados.

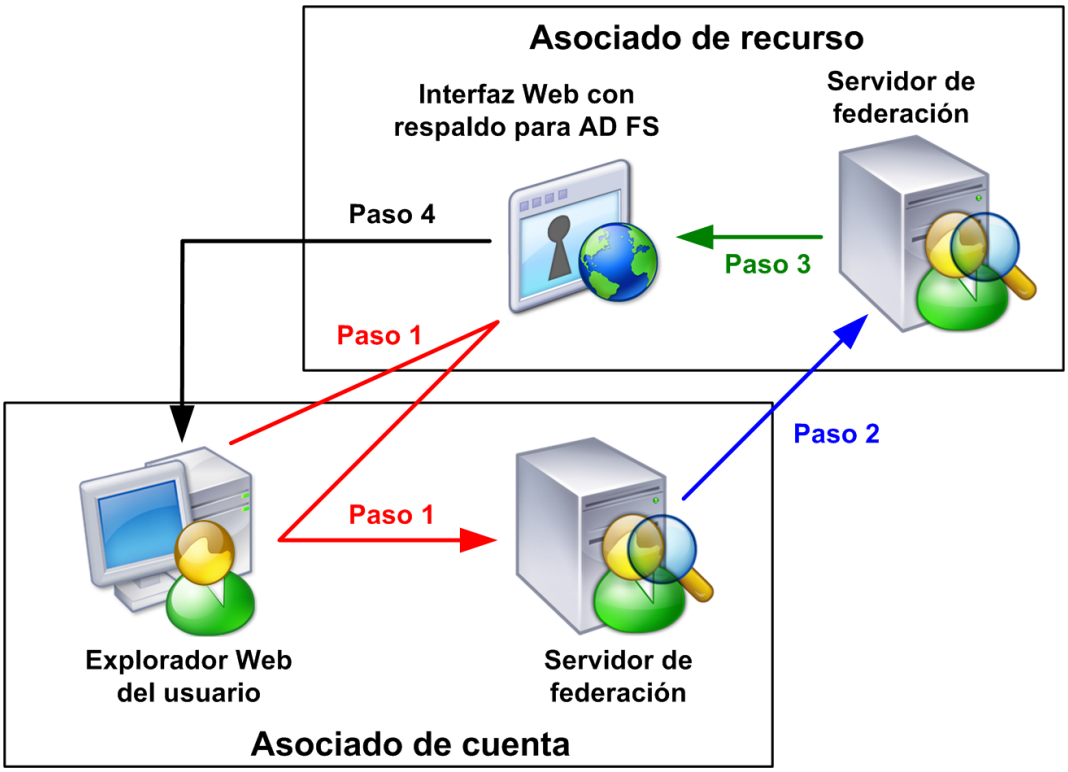
Configuración del soporte de AD FS para la Interfaz Web

El respaldo para los servicios de federación de Microsoft Active Directory para la Interfaz Web permite al asociado de recurso de un entorno AD FS utilizar XenApp. Los administradores pueden crear sitios AD FS para proporcionar a los usuarios el acceso a aplicaciones y contenido en el asociado de recurso.

Importante: AD FS necesita comunicaciones seguras entre el explorador Web, el servidor Web y los servidores de federación. Los usuarios de la Interfaz Web deben utilizar HTTPS/SSL para acceder al sitio.

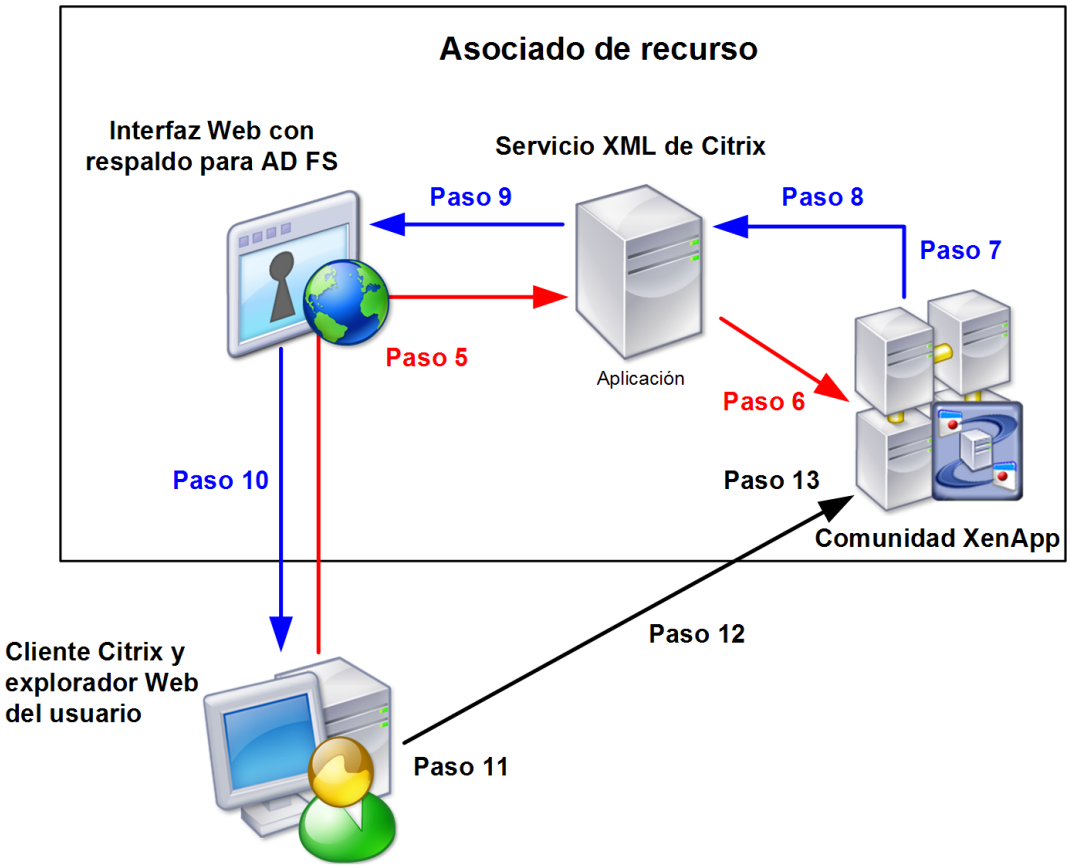
Funcionamiento de los sitios integrados con los servicios de federación de Active Directory

Los siguientes pasos se producen cuando un usuario en un asociado de cuenta accede a una aplicación en un asociado de recurso:

- **Paso 1:** Un usuario que abre la página de inicio de la Interfaz Web en el asociado de recurso es redirigido a la página de autenticación del asociado de cuenta.
- **Paso 2:** El asociado de cuenta autentica al usuario y envía un token de seguridad al asociado de recurso.
- **Paso 3:** El servicio AD FS del asociado de recurso valida el token de seguridad, lo transforma en una identidad de Windows (que representa una cuenta sombra) y redirige al usuario a la pantalla de Inicio de sesión de la Interfaz Web.
- 

  Paso 4: La Interfaz Web muestra el conjunto de aplicaciones del usuario. Esta figura muestra los pasos que tienen lugar cuando los usuarios del dominio del asociado de cuenta inician sesiones para acceder a sus conjuntos de aplicaciones.
- **Paso 5:** El usuario tiene acceso a una aplicación haciendo clic en un hipervínculo de la página. La Interfaz Web se comunica con Citrix XML Service para solicitar el acceso.

- **Paso 6:** El servicio XML de Citrix genera datos SSPI y los envía a un servidor XenApp.
- **Paso 7:** El servidor utiliza esos datos SSPI para autenticar al usuario y guarda un token de inicio de sesión para autenticaciones posteriores.
- **Paso 8:** El servidor genera un tiquet de apertura para representar de forma exclusiva al token de inicio de sesión almacenado y devuelve ese tiquet al servicio XML de Citrix.
- **Paso 9:** El servicio XML de Citrix devuelve el tiquet de apertura a la Interfaz Web.
- **Paso 10:** La Interfaz Web crea un archivo .ica que contiene el tiquet de apertura y lo envía al explorador Web del usuario.
- **Paso 11:** El dispositivo del usuario abre el archivo .ica e intenta una conexión ICA con el servidor.
- **Paso 12:** El cliente Citrix envía el tique de inicio al servidor XenApp.
-



Paso 13: El servidor recibe el tiquet de apertura, lo compara con el token de inicio de sesión generado previamente y utiliza este token para conectar al usuario a una sesión ICA en el servidor. La sesión ICA se ejecuta con la identidad de la cuenta sombra.Esta figura muestra los pasos que se llevan a cabo cuando los usuarios del dominio del asociado de cuenta tienen acceso a las aplicaciones.

De acuerdo con los parámetros que estén configurados para un sitio, cuando los usuarios cierran sesión se cierra la sesión de la Interfaz Web o de la Interfaz Web y de AD FS. Si los usuarios cierran sesión en la Interfaz Web y en AD FS, cierran sesión en todas las aplicaciones de AD FS.

Antes de crear sitios de servicios de federación de Active Directory

Antes de crear un sitio AD FS, debe realizar los siguientes pasos. Si no sigue estos pasos, puede que le sea imposible crear un sitio.

- Sincronice los relojes de los servidores de federación del asociado de cuenta y del asociado de recurso con una diferencia máxima de cinco minutos entre sí. De lo contrario, los tokens de seguridad generados por el asociado de cuenta podrían ser rechazados por el asociado de recurso, ya que parecerá que han caducado. Para evitar este problema, ambas organizaciones deben sincronizar sus servidores con el mismo servidor horario de Internet. Para obtener más información, consulte Configuración de las relaciones entre dominios.

- Asegúrese de que el servidor Web y el servidor de federación del asociado de recurso puedan acceder a las listas de revocación de certificados (CRL) de la entidad emisora de certificados. AD FS puede fallar si los servidores no pueden verificar que un certificado no fue revocado. Para obtener más información, consulte Configuración de las relaciones entre dominios.

- Asegúrese de que se confía en todos los servidores de la distribución para delegación. Para obtener más información, consulte Cómo configurar la delegación para los servidores del entorno.

- Configure cuentas sombra en el dominio del asociado de recurso para cada usuario externo que se pueda autenticar en la Interfaz Web mediante AD FS. Para obtener más información, consulte Configuración de cuentas sombra.

- Instale XenApp asegurándose de que el servicio XML de Citrix esté configurado para compartir el puerto con IIS y que IIS esté configurado para aceptar HTTPS.

- Configure una relación de confianza entre el servidor de la Interfaz Web y cualquier otro servidor de la comunidad que ejecute el servicio XML de Citrix con el que se comunica la Interfaz Web. Para obtener más información, consulte Uso del control del área de trabajo con métodos de autenticación integrados para los sitios Web de XenApp.

Importante: En esta sección no se explica cómo instalar AD FS. Antes de intentar crear un sitio AD FS, debe disponer de una instalación AD FS que funcione, con usuarios de cuentas externos que puedan acceder a aplicaciones integradas con AD FS en un asociado de recurso.

Requisitos de software para los servicios de federación de Active Directory

El siguiente software debe estar instalado y configurado en su entorno:

- Windows Server 2008 o Windows Server 2003 R2 para los servidores de federación y los servidores Web. En el caso del servidor Web, sólo se admiten versiones de Windows Server 2008 y Windows Server 2003 R2 de 32 bits.

- Servicios de federación de Active Directory (AD FS) en los asociados de recurso y de cuenta. Deben estar instalados ambos agentes Web de AD FS: el agente Web de aplicaciones para notificaciones y el agente Web basado en token.

Configuración de las relaciones entre dominios

El entorno descrito aquí consta de dos dominios (en sus propios bosques), uno para el asociado de cuenta y otro para el asociado de recurso. Tenga en cuenta que los componentes requeridos no tienen que estar necesariamente en equipos distintos.

Para configurar las relaciones entre dominios

1. Asegúrese de que dispone de los siguientes componentes: El asociado de cuenta necesita:

   - Controlador de dominio
   - Servidor de federación
   - Dispositivos de usuarios

   El asociado de recurso necesita:

   - Controlador de dominio
   - Servidor de federación
   - servidor Web
   - Uno o más servidores para la comunidad XenApp

   Los servidores de federación deben estar en equipos que ejecuten Windows Server 2008 o Windows 2003 R2 y tener instalada la función de servidor Servicios de federación de Active Directory.

   El servidor Web debe encontrarse en un equipo que ejecute una versión de Windows Server 2008 o Windows Server 2003 R2 de 32 bis. Se deben instalar los servicios de función Agente para notificaciones y Agente basado en tokens de Windows además de *todos* los servicios de la función de servidor Servidor Web (IIS).

2. Obtenga certificados de servidor distintos para el servidor Web y para ambos servidores de federación.

   - Los certificados debe estar firmados por una organización con autoridad y de confianza, denominada entidad emisora de certificados (Certificate Authority, CA).
   - El certificado del servidor identifica a un equipo concreto, por lo que es necesario conocer el nombre completo de dominio (FQDN) de cada servidor; por ejemplo, “xenappserver1.mydomain.com”.
   - Instale el certificado del servidor Web en Microsoft Internet Information Services (IIS) para permitir que el sitio Web predeterminado de IIS acepte tráfico SSL.
   - Instale los certificados del servidor de federación con el complemento Certificados en la consola Microsoft Management Console (MMC). Para obtener más información, consulte la *Guía paso a paso de Microsoft Management Console* en http://technet.microsoft.com/.

3. Para asegurarse de que el servidor de federación del asociado de recurso confía en el servidor de federación del asociado de cuenta, instale el certificado de federación del asociado de cuenta en el almacén Entidades de certificación raíz de confianza del servidor de federación del asociado de recurso.

4. Para asegurarse de que el servidor Web confía en el servidor de federación del asociado de recurso, instale el certificado de federación del asociado de recurso en el almacén Entidades de certificación raíz de confianza del servidor Web.

Importante: Es necesario que tanto el servidor Web como el servidor de federación de recurso tengan acceso a las listas de revocación de certificados (CRL) de la entidad emisora de certificados. El servidor de federación de recursos debe tener acceso a la entidad emisora de certificados del asociado de cuenta y el servidor Web debe tener acceso a la entidad emisora de certificados del asociado de recurso. AD FS puede fallar si los servidores no pueden verificar que un certificado no fue revocado.

5. En el servidor de federación del asociado de recurso, abra el complemento Servicios de federación de Active Directory en la consola MMC.

6. En el panel de la izquierda, seleccione Servicio de federación > Directiva de confianza > Organizaciones asociadas > Asociados de cuenta y, a continuación, elija el nombre del asociado de cuenta.

7. En el panel Acción, haga clic en Propiedades.

8. En la ficha Cuentas de recursos, seleccione Existen cuentas de recursos para todos los usuarios y haga clic en Aceptar.

9. Con el mismo servidor horario de Internet, sincronice los relojes del servidor de federación del asociado de cuenta y del asociado de recurso, con una diferencia máxima de cinco minutos entre sí. De lo contrario, los tokens de seguridad generados por el asociado de cuenta podrían ser rechazados por el asociado de recurso, ya que parecerá que han caducado. Los asociados de recurso y de cuenta pueden estar en distintas zonas horarias, pero deben estar correctamente sincronizados. Por ejemplo, suponga que el asociado de cuenta está situado en Nueva York y está configurado como 16.00 horas (hora estándar del este, EST). El asociado de recurso ubicado en California tiene que configurarse entre las 12:55 y las 13:05 horas (hora estándar del Pacífico, PST). (Hay una diferencia de tres horas entre las zonas horarias EST y PST.)

10. En el servidor Web, abra el complemento Administrador de Internet Information Services (IIS) en la consola MMC.

11. Seleccione el servidor Web en el panel de la izquierda y, en la vista Características, haga doble clic en URL del servicio de federación.

12. En la página URL del servicio de federación introduzca la dirección URL del servidor de federación del asociado de recurso y haga clic en Aplicar en el panel Acción.

Cómo configurar la delegación para los servidores del entorno

Debe asegurarse de que se confíe en todos los servidores del entorno para la delegación. Para ello, realice las tareas siguientes dentro de una sesión abierta como administrador de dominio en el controlador de dominio correspondiente al asociado de recurso. En esta sección se incluyen los procedimientos para cada una de las tareas.

- Asegúrese de que el dominio al que pertenece el asociado de recurso esté en el nivel funcional correcto
- Establezca una relación de confianza con el servidor de la Interfaz Web para la delegación
- Establezca una relación de confianza con el servidor que ejecuta el servicio XML de Citrix para la delegación
- Determine los recursos a los que se puede acceder desde el servidor XenApp

Para asegurar que el dominio al que pertenece el asociado de recurso está en el nivel funcional correcto

Importante: Para elevar el nivel de dominio, todos los controladores de dominio deben ejecutar Windows Server 2008 o Windows Server 2003. No eleve el nivel funcional de dominio a Windows Server 2008 si posee o tiene intenciones de agregar controladores de dominio que ejecutan Windows Server 2003. Una vez que se eleva el nivel funcional de dominio no es posible retroceder a un nivel inferior.

1. En el controlador de dominio del asociado de recurso, abra el complemento Dominios y confianza de Active Directory en la consola MMC.

2. En el panel izquierdo, seleccione el nombre de dominio del asociado de recurso y haga clic en Propiedades en el panel Acción.

3. Si el dominio no se encuentra en el nivel funcional máximo, seleccione el nombre del dominio y, en el panel Acción, haga clic en Elevar el nivel funcional del dominio.

4. Para elevar el nivel funcional del dominio, haga clic en el nivel adecuado y luego en Elevar.

Para establecer una relación de confianza con el servidor de la Interfaz Web para la delegación

1. En el controlador de dominio del asociado de recurso, abra el complemento Usuarios y equipos de Active Directory en la consola MMC.
2. En el menú Ver, haga clic en Funciones avanzadas.
3. En el panel izquierdo, haga clic en el nodo Equipos debajo del nombre de dominio del asociado de recurso y seleccione el servidor de la Interfaz Web.
4. En el panel Acción, haga clic en Propiedades.
5. En la ficha Delegación, haga clic en Confiar en este equipo para la delegación sólo a los servicios especificados y Usar cualquier protocolo de autenticación y, a continuación, haga clic en Agregar.
6. En el cuadro de diálogo Agregar servicios, haga clic en Usuarios o equipos.
7. En el cuadro de diálogo Seleccionar usuarios o equipos, escriba el nombre del servidor que ejecuta el servicio XML de Citrix en el cuadro Escriba los nombres de objeto que desea seleccionar y, a continuación, haga clic en Aceptar.
8. Seleccione el tipo de servicio http en la lista y, a continuación, haga clic en Aceptar.
9. En la ficha Delegación, verifique que el tipo de servicio http del servidor XenApp aparezca en la lista Servicios a los que esta cuenta puede presentar credenciales delegadas y, a continuación, haga clic en Aceptar.
10. Repita el proceso para cada uno de los servidores de la comunidad que ejecuten el servicio XML de Citrix y con los que la Interfaz Web esté configurada para conectarse.

Para establecer una relación de confianza con el servidor que ejecuta el servicio XML de Citrix para la delegación

1. En el controlador de dominio del asociado de recurso, abra el complemento Usuarios y equipos de Active Directory en la consola MMC.
2. En el panel izquierdo, haga clic en el nodo Equipos debajo del nombre de dominio del asociado de recurso y seleccione el servidor que ejecuta el servicio XML de Citrix con el que la Interfaz Web está configurada para conectarse.
3. En el panel Acción, haga clic en Propiedades.
4. En la ficha Delegación, haga clic en Confiar en este equipo para la delegación sólo a los servicios especificados y Usar solamente Kerberos y, a continuación, haga clic en Agregar.
5. En el cuadro de diálogo Agregar servicios, haga clic en Usuarios o equipos.
6. En el cuadro de diálogo Seleccionar usuarios o equipos, escriba el nombre del servidor que ejecuta el servicio XML de Citrix en el cuadro Escriba los nombres de objeto que desea seleccionar y, a continuación, haga clic en Aceptar.
7. Seleccione el tipo de servicio HOST en la lista y, a continuación, haga clic en Aceptar.
8. En la ficha Delegación, verifique que el tipo de servicio HOST del servidor que ejecuta el servicio XML de Citrix aparezca en la lista Servicios a los que esta cuenta puede presentar credenciales delegadas y, a continuación, haga clic en Aceptar.
9. Repita el proceso para cada uno de los servidores de la comunidad que ejecuten el servicio XML de Citrix y con los que la Interfaz Web esté configurada para conectarse.

Para determinar qué recursos son accesibles desde el servidor XenApp

1. En el controlador de dominio del asociado de recurso, abra el complemento Usuarios y equipos de Active Directory en la consola MMC.
2. En el panel izquierdo, haga clic en el nodo Equipos bajo el nombre de dominio del asociado de recurso y seleccione el servidor XenApp.
3. En el panel Acción, haga clic en Propiedades.
4. En la ficha Delegación, haga clic en Confiar en este equipo para la delegación sólo a los servicios especificados y Usar solamente Kerberos y, a continuación, haga clic en Agregar.
5. En el cuadro de diálogo Agregar servicios, haga clic en Usuarios o equipos.
6. En el cuadro de diálogo Seleccionar usuarios o equipos, escriba el nombre de los controladores de dominio del asociado de recurso en el cuadro Escriba los nombres de objeto que desea seleccionar y, a continuación, haga clic en Aceptar.
7. Seleccione los tipos de servicio cifs e ldap de la lista y, a continuación, haga clic en Aceptar.

   Nota: Si aparecen dos opciones para el servicio ldap, seleccione la que coincida con el nombre de dominio completo (FQDN) del controlador de dominio.
8. En la ficha Delegación, verifique que los tipos de servicio cifs e ldap del controlador de dominio del asociado de recurso aparezcan en la lista Servicios a los que esta cuenta puede presentar credenciales delegadas y, a continuación, haga clic en Aceptar.
9. Repita el proceso para cada servidor XenApp de la comunidad.

Configuración de servidores para delegación limitada

Por razones de seguridad, debe configurar todos los servidores que ejecuten XenApp para la delegación limitada. Para dar acceso a los usuarios a los recursos en esos servidores, debe agregar los servicios pertinentes a la Lista de servicios a los que esta cuenta puede presentar credenciales delegadas utilizando el complemento Usuarios y equipos de Active Directory en la consola MMC. Por ejemplo, para permitir que los usuarios se autentiquen en un servidor Web en el host “peter”, agregue el servicio http para el servidor peter; para permitir que los usuarios se autentiquen en un servidor SQL, en el host “lois” agregue el servicio MSSQLSvc para el servidor lois.

Para obtener información más detallada, consulte el documento técnico *Service Principal Names and Delegation in Presentation Server* (CTX110784) en la base de conocimientos en línea Citrix Knowledge Center.

Configuración de un límite de tiempo para el acceso a los recursos

Precaución: Si se usa el editor del Registro de forma incorrecta, pueden producirse problemas graves que derivarán en la necesidad de instalar nuevamente el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad.

De manera predeterminada, los usuarios de AD FS tienen acceso a los recursos de una red durante 15 minutos. Es posible aumentar este límite modificando la siguiente entrada en el Registro del sistema del servidor que ejecuta el servicio XML de Citrix:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\
Kerberos\Parameters\S4UTicketLifetime

Este valor especifica el tiempo, en minutos, durante el cual los usuarios pueden acceder a los recursos una vez iniciada la sesión.

La directiva de seguridad del dominio controla el valor máximo que puede definirse en el parámetro S4ULifetime. Si especifica un valor para el parámetro S4UTicketLifetime mayor que el valor especificado en el nivel de dominio, el parámetro del nivel de dominio tiene preferencia.

Para configurar el límite de tiempo para el acceso a los recursos en el nivel de dominio

1. En el controlador de dominio del asociado de recurso, abra el complemento Directiva de seguridad de dominio en la consola MMC.
2. En el panel izquierdo, seleccione Directivas de cuenta > Directiva Kerberos.
3. En el panel de resultados, seleccione Vigencia máxima del tique de servicio.
4. En el panel Acción, haga clic en Propiedades.
5. Introduzca el límite necesario (en minutos) en el cuadro El tique caduca en.

Si no desea configurar ningún límite para el tiempo durante el cual se puede acceder a los recursos, marque la casilla Usar cualquier protocolo de autenticación cuando determine qué recursos están accesibles desde el servidor XenApp. Si selecciona esta opción, no se tendrá en cuenta ningún valor especificado para S4UTicketLifetime. Para obtener más información, visite el sitio Web de Microsoft en http://support.microsoft.com/.

Configuración de cuentas sombra

Para proporcionar el acceso a las aplicaciones, XenApp necesita cuentas reales de Windows. Por lo tanto, debe crear manualmente una cuenta sombra en el dominio del asociado de recurso para cada usuario externo que se autentique en la Interfaz Web mediante AD FS.

Si tiene una gran cantidad de usuarios en el dominio del asociado de cuenta que vayan a acceder a las aplicaciones y el contenido dentro del dominio del asociado de recurso, puede utilizar un producto de creación de cuentas de otro fabricante para permitir la creación rápida de cuentas sombra de usuarios en Active Directory.

Para crear cuentas sombra, realice las tareas siguientes dentro de una sesión abierta como administrador de dominio en el controlador de dominio correspondiente al asociado de recurso.

Para agregar sufijos de nombre principal de usuario

1. En el controlador de dominio del asociado de recurso, abra el complemento Dominios y confianza de Active Directory en la consola MMC.
2. En el panel izquierdo, seleccione Dominios y confianza de Active Directory.
3. En el panel Acción, haga clic en Propiedades.
4. Agregue un sufijo UPN por cada asociado de cuenta externo. Por ejemplo, si el dominio de Active Directory del asociado de cuenta es “adomain.com”, agregue adomain.com como sufijo UPN.

Para definir el usuario de la cuenta sombra

1. En el controlador de dominio del asociado de recurso, abra el complemento Usuarios y equipos de Active Directory en la consola MMC.
2. En el panel izquierdo, seleccione el nombre de dominio del asociado de recurso.
3. En el panel Acción, haga clic en Nuevo > Usuario.
4. Escriba el nombre, las iniciales y el apellido del usuario en los cuadros correspondientes.
5. En el cuadro Nombre de inicio de sesión del usuario, escriba el nombre de cuenta. Asegúrese de que este nombre coincida con el nombre de la cuenta existente en el controlador de dominio del asociado de cuenta.
6. Seleccione el sufijo UPN externo en la lista y, a continuación, haga clic en Siguiente.
7. En los cuadros Contraseña y Confirmar contraseña, escriba una contraseña que cumpla con los requisitos definidos en su directiva de contraseñas. Dicha contraseña no se utiliza nunca porque el usuario se autentica a través de AD FS.
8. Desactive la casilla El usuario debe cambiar la contraseña en el siguiente inicio de sesión.
9. Marque las casillas El usuario no puede cambiar la contraseña y La contraseña nunca caduca.
10. Haga clic en Siguiente y, a continuación, en Finalizar.

Creación de sitios integrados con servicios de federación de Active Directory

Ejecute la tarea Crear sitio desde la consola Administración de la Interfaz Web de Citrix y configure el sitio de la Interfaz Web para que utilice AD FS para la autenticación.

Nota: Los entornos AD FS no respaldan la distribución de escritorios virtuales de XenDesktop. Asimismo, el Cliente para Java y el software incrustado de Conexión a escritorio remoto (RDP) no reciben soporte para acceder a sitios integrados con AD FS.

Para crear un sitio integrado con servicios de federación de Active Directory

1. En el menú Inicio de Windows, haga clic en Todos los programas > Citrix > Management Consoles > Citrix Web Interface Management.
2. En el panel izquierdo de la consola Administración de la Interfaz Web de Citrix, haga clic en el contenedor Interfaz Web de Citrix.
3. En el panel Acción, haga clic en Crear sitio.
4. Seleccione Web XenApp y, a continuación, haga clic en Siguiente.
5. En la página Especificar ubicación IIS, especifique la ubicación IIS, la ruta y un nombre para el sitio. Haga clic en Next.
6. En la página Especificar punto de autenticación, seleccione En el asociado de cuenta de Microsoft AD FS. Introduzca la dirección URL de respuesta de la Interfaz Web y haga clic en Siguiente.
7. Confirme los parámetros del nuevo sitio y, a continuación, haga clic en Siguiente para crear el sitio.

Configuración del sitio como aplicación de los servicios de federación de Active Directory

Después de crear el sitio, debe configurarlo como aplicación AD FS para que el servidor de federación lo reconozca.

Para configurar el sitio como aplicación de los servicios de federación de Active Directory

1. En el servidor de federación del asociado de recurso, abra el complemento Servicios de federación de Active Directory en la consola MMC.
2. En el panel de la izquierda, seleccione Servicio de federación > Directiva de confianza > Mi organización > Aplicaciones.
3. En el panel Acción, haga clic en Nuevo > Aplicación.
4. Haga clic en Siguiente, seleccione Aplicación para notificaciones y vuelva a hacer clic en Siguiente.
5. Escriba un nombre para el sitio en el cuadro Nombre para mostrar de la aplicación.
6. En el cuadro Dirección URL de la aplicación introduzca la URL del sitio de Interfaz Web *exactamente* igual que apareció en el cuadro URL de respuesta de la Interfaz Web al crear el sitio y, a continuación, haga clic en Siguiente.

   Nota: Asegúrese de utilizar HTTPS y el nombre completo de dominio (FQDN) del servidor Web.
7. Marque la casilla Nombre principal del usuario (UPN) y haga clic en Siguiente.
8. Compruebe que la casilla Habilitar esta aplicación esté marcada y haga clic en Aceptar.
9. Haga clic en Finalizar para agregar el sitio como aplicación AD FS.

Cómo poner a prueba su entorno

Después de configurar el sitio como aplicación AD FS, pruebe su entorno para asegurarse de que todo funciona correctamente entre el asociado de cuenta y el asociado de recurso.

Para poner a prueba el entorno de la Interfaz Web con servicios de federación de Active Directory

1. Inicie sesión en un dispositivo de usuario en el dominio del asociado de cuenta.
2. Abra el explorador Web y escriba la dirección URL con el nombre completo de dominio (FQDN) del sitio de la Interfaz Web integrado con AD FS previamente creado.

   Aparecerá el conjunto de aplicaciones.

   Nota: Si no ha configurado AD FS para la autenticación integrada, es posible que se le pida que introduzca las credenciales o que introduzca una tarjeta inteligente.
3. Si no ha instalado Citrix XenApp Online Plug-in, instálelo ahora. Para obtener más información, consulte Online Plug-in para Windows.
4. Haga clic en una aplicación para acceder a la misma.

Cierre de sesión en sitios integrados con servicios de federación de Active Directory

Utilice la tarea Métodos de autenticación de la consola Administración de la Interfaz Web de Citrix para especificar si los usuarios que hagan clic en los botones Cerrar sesión o Desconectar en el sitio Web cerrarán la sesión de:

- La Interfaz Web solamente
- Tanto la Interfaz Web como el servicio de federación AD FS

Si especifica que los usuarios cierren solamente la sesión de la Interfaz Web, serán redirigidos a la pantalla de cierre de sesión de la Interfaz Web. Si especifica que los usuarios cierren la sesión de la Interfaz Web y del servicio de federación AD FS, serán redirigidos a la página de cierre de sesión del servicio de federación y se cerrarán sus sesiones en todas las aplicaciones de AD FS.

Nota: Los usuarios que se autentican mediante AD FS no pueden desbloquear sus sesiones de XenApp porque no conocen sus contraseñas. Para desbloquear sesiones, los usuarios deben cerrar sesión en la Interfaz Web, volver a iniciar sesión mediante autenticación AD FS y, a continuación, reiniciar sus aplicaciones. Al hacer esto, la sesión anterior se desbloquea y se cierra la ventana nueva.

Para especificar desde qué servicios cierran sesión los usuarios

1. En el menú Inicio de Windows, haga clic en Todos los programas > Citrix > Management Consoles > Citrix Web Interface Management.
2. En el panel izquierdo de la consola Administración de la Interfaz Web de Citrix, haga clic en Sitios Web XenApp y en el panel de resultados, seleccione su sitio integrado de AD FS.
3. En el panel Acción, haga clic en Métodos de autenticación.
4. Para especificar que los usuarios cierren sesión desde la Interfaz Web y el servicio de federación AD FS, marque la casilla Cierre de sesión global. Para especificar que los usuarios cierren solamente la sesión desde la Interfaz Web, deje sin marcar la casilla Cierre de sesión global.