Citrix SSO

Machine translated content

Disclaimer

La versión oficial de este contenido está en inglés. Para mayor comodidad, parte del contenido de la documentación de Citrix solo tiene traducción automática. Citrix no puede controlar el contenido con traducción automática, que puede contener errores, imprecisiones o un lenguaje inadecuado. No se ofrece ninguna garantía, ni implícita ni explícita, en cuanto a la exactitud, la fiabilidad, la idoneidad o la precisión de las traducciones realizadas del original en inglés a cualquier otro idioma, o que su producto o servicio de Citrix se ajusten a cualquier contenido con traducción automática, y cualquier garantía provista bajo el contrato de licencia del usuario final o las condiciones de servicio, o cualquier otro contrato con Citrix, de que el producto o el servicio se ajusten a la documentación no se aplicará en cuanto dicha documentación se ha traducido automáticamente. Citrix no se hace responsable de los daños o los problemas que puedan surgir del uso del contenido traducido automáticamente.

Contents

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Citrix SSO para dispositivos iOS/macOS

April 3, 2020

El cliente VPN de Citrix heredado se creó mediante las API VPN privadas de Apple que ahora están obsoletas. La compatibilidad con VPN en Citrix SSO se vuelve a escribir desde cero mediante el marco de extensión de red pública de Apple.

Las siguientes son algunas de las principales funciones introducidas con la aplicación Citrix SSO:

- **Tokens de contraseña:** Un token de contraseña es un código de 6 dígitos que es una alternativa a los Servicios de contraseña secundaria como VIP, OKTA, etc. Este código utiliza el protocolo Time-based One Time Password (T-OTP) para generar el código OTP similar a servicios como Google Authenticator, Microsoft Authenticator, etc. Se solicita a los usuarios dos contraseñas durante la autenticación en Citrix Gateway para un usuario determinado de Active Directory. El segundo factor es un código cambiante de seis dígitos que los usuarios copian desde un servicio de terceros registrado como Google o Microsoft Authenticator en el explorador de escritorio. Los usuarios deben registrarse primero para T-OTP en el dispositivo Citrix ADC. Para obtener información sobre los pasos de registro, consulte https://support.citrix.com/article/CTX228454. En la aplicación, los usuarios pueden agregar la función OTP escaneando el código QR generado en Citrix ADC o introduciendo manualmente el secreto TOTP. Los tokens OTP una vez agregados aparecen en el segmento de tokens de contraseña en la interfaz de usuario.

Para mejorar la experiencia, al agregar un OTP se solicita al usuario que cree un perfil VPN automáticamente. Los usuarios pueden aprovechar este perfil VPN para conectarse a VPN directamente desde sus dispositivos iOS.

La aplicación Citrix SSO se puede utilizar para escanear el código QR mientras se registra para obtener compatibilidad con OTP nativo.La funcionalidad de notificación Push de
Citrix Gateway solo está disponible para los usuarios de la aplicación Citrix SSO.

- **Notificación push:** Citrix Gateway envía notificaciones push en su dispositivo móvil registrado para obtener una experiencia de autenticación simplificada de dos factores. En lugar de abrir la aplicación Citrix SSO para escribir el segundo factor OTP en la página de inicio de sesión de Citrix ADC, puede validar su identidad proporcionando el PIN de dispositivo/Touch ID/ID facial para el dispositivo registrado.

Una vez que registre el dispositivo para la notificación Push, también puede utilizar el dispositivo para la compatibilidad con OTP nativo mediante la aplicación Citrix SSO. El registro para notificaciones push es transparente para el usuario. Cuando los usuarios registran TOTP, el dispositivo también se registra para Notificaciones Push si Citrix ADC lo admite.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Notas de la versión

April 3, 2020

Las notas de versión de Citrix SSO describen las nuevas funciones, las mejoras a las funciones existentes, los problemas corregidos y los problemas conocidos disponibles en una versión de servicio. Las notas de la versión incluyen una o varias de las siguientes secciones:

Novedades: Las nuevas funciones y mejoras disponibles en la versión actual.

Problemas corregidos: Los problemas corregidos en la versión actual.

Problemas conocidos: Los problemas que existen en la versión actual y sus soluciones alternativas, siempre que corresponda.

V1.2.6

Problemas conocidos

- VPN a veces se bloquea después de que macOS se reactiva del modo de suspensión.

  [NSHELP-20656: macOS]

V1.2.5

Problemas conocidos

- VPN a veces se bloquea después de que macOS se reactiva del modo de suspensión.

  [NSHELP-20656: macOS]

V1.2.4

Problemas conocidos

- A veces, la sesión VPN no responde después de que el Mac se activa desde el modo de suspensión.

  [NSHELP-20656: macOS]

V1.2.3

Novedades

- Esquema de URL de Citrix SSO: Citrix SSO ahora registra un esquema de URL para que otras aplicaciones puedan determinar si Citrix SSO está instalado en un dispositivo iOS. El esquema

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

de URL es “citrixsso.”

[CGOP-11979: IOS]

Problemas resueltos

- La aplicación Citrix SSO se bloquea al enviar tráfico UDP intenso.

  [CGOP-11603: macOS]

- Citrix SSO para iPad se bloquea cuando la aplicación se inicia desde una notificación en iOS 13.

  [NSHELP-21087: IOS]

V1.2.2

Problemas resueltos

- En algunas implementaciones de GSLB, Citrix SSO resuelve el nombre de la Gateway varias veces, lo que provoca errores de conexión.

  [CGOP-12013]

- Citrix SSO para iOS no puede analizar OTPSecret con más de 16 bytes.

  [CGOP-11978: IOS]

- Se pide a los usuarios con perfiles configurados para la autenticación de solo certificado y una comprobación de NAC que introduzcan las credenciales de inicio de sesión y no pueden crear las conexiones VPN.

  [CGOP-11925: IOS]

- Aunque el indicador de túnel dividido por aplicación solo se comprueba para el tráfico TCP, el tráfico ICMP se tuneliza incluso en los casos en que el tráfico ICMP debe enviarse directamente.

  [CGOP-11614: IOS]

Problemas conocidos

- El complemento Citrix Gateway para macOS no admite la función que abre la página de inicio en la aplicación Citrix Workspace.

  [NSHELP-7047]

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

V1.2.0

Novedades

- **Compatibilidad con la autenticación nFactor.** La autenticación nFactor ahora se admite tanto en iOS como en macOS.

  [CGOP-11251]

- **Compatibilidad con la aplicación Citrix SSO.** La aplicación Citrix SSO ahora es compatible con iOS 13 y macOS Catalina.

  [CGOP-11714]

Problemas resueltos

- La dirección IP del cliente se muestra hacia atrás en la página Conexiones de la aplicación SSO.

  [CGOP-11596]

- Citrix SSO no respeta el bit truncado DNS en el indicador DNS de Citrix ADC versión 13.0.

  [CGOP-11777]

- El túnel dividido por aplicación no es compatible con Citrix ADC versión 13.0.

  [CGOP-11464]

- Citrix SSO ignora algunos de los mensajes de tiempo de espera de Citrix Gateway.

  [CGOP-11310]

- Cuando los usuarios inician sesión en la aplicación por primera vez, la última línea de la descripción de la aplicación no aparece en la pantalla del usuario.

  [CGOP-11595: macOS]

- El tamaño de la ventana de inicio de sesión de la aplicación Citrix SSO sigue aumentando al hacer clic repetidamente en el botón Inicio de sesión.

  [CGOP-11594: macOS]

- Cuando se supera el límite máximo de usuarios con licencia, se muestra un mensaje de error en el nivel del sistema y no en la ventana de la aplicación.

  [CGOP-11600: macOS]

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

V1.1.12

Novedades

- **Recopilación de datos de telemetría para macOS.** Citrix SSO recopila eventos de análisis personalizados relacionados con el uso de VPN en la aplicación.

  [CGOP-9789: macOS]

- **Soporte de túnel dividido por aplicación.** Los administradores pueden configurar el túnel dividido por aplicación. El tráfico por aplicación que coincide con las rutas de intranet de Citrix Gateway se canaliza al dispositivo Citrix Gateway.

  [CGOP-657]

- **FQDN Túnel Split Túnel tráfico basado en el FQDN del sistema.** FQDN Túnel Split Túnel tráfico basado en el FQDN del sistema en lugar de la IP resuelta por los servidores DNS.

  [CGOP-316]

Problemas resueltos

- Los elementos de la interfaz de usuario, como botones, campos de texto, etiquetas, etc., están desalineados en las pantallas del iPad.

  [CGOP-10141: IOS]

- Los usuarios no reciben notificación de un inicio de sesión remoto si no tienen un perfil VPN agregado.

  [CGOP-9731: IOS]

V1.1.10

Problemas resueltos

- La aplicación Citrix SSO no muestra el mensaje de error adecuado al alcanzar el número máximo de usuarios cuando.

  [CGOP-231]

- La casilla de verificación EULA no está desactivada de forma predeterminada.

  [CGOP-245]

- No se admite la funcionalidad de adición para el análisis “habilitado” de antiphishing en Endpoint Analysis.

  [CGOP-249]

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- La selección automática del certificado cliente/dispositivo para la autenticación no ocurre incluso si solo hay un cliente/dispositivo presente en el llavero.

  [CGOP-251]

- No se puede agregar un 'registro de conexión' después de modificar uno en la aplicación Citrix SSO.

  [CGOP-7256]

Configurar Citrix SSO para usuarios de iOS

April 3, 2020

> **IMPORTANTE:** Citrix VPN no se puede utilizar en iOS 12 y versiones posteriores. Para continuar con VPN, use la aplicación Citrix SSO.

En la siguiente tabla, se compara la disponibilidad de diversas funciones entre Citrix VPN y Citrix SSO.

Función	Citrix VPN	Citrix SSO
VPN a nivel de dispositivo	Se admite	Se admite
VPN por aplicación (solo MDM)	Se admite	Se admite
Túnel dividido por aplicación	No se admite	Se admite
Perfiles VPN configurados por MDM	Se admite	Se admite
VPN a demanda	Se admite	Se admite
Tokens de contraseña (basados en T-OTP)	No se admite	Se admite
Inicio de sesión basado en notificaciones push (segundo factor desde el teléfono registrado)	No se admite	Se admite
Autenticación basada en certificados	Se admite	Se admite
Autenticación de nombre de usuario/contraseña	Se admite	Se admite

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Función	Citrix VPN	Citrix SSO
Comprobación del control de acceso a redes con Citrix Endpoint Management (anteriormente XenMobile)	No se admite	Se admite
Comprobación del control de acceso a la red con Microsoft Intune	Se admite	Se admite
Compatibilidad con DTLS	No se admite	Se admite
Bloquear perfiles VPN creados por el usuario	Se admite	Se admite
Inicio de sesión único (SSO) para aplicaciones nativas administradas por Citrix Cloud	No se admite	Se admite
Versión de SO compatible	iOS 9, 10, 11 (no funciona a partir de iOS 12+)	iOS 9+

Compatibilidad con productos MDM

Citrix SSO es compatible con la mayoría de los proveedores de MDM, como Citrix Endpoint Management (anteriormente XenMobile), Microsoft Intune, etc.

Citrix SSO también admite una función denominada Control de acceso a redes (NAC). Para obtener más información sobre NAC, haga clic en aquí. Con NAC, los administradores de MDM pueden exigir el cumplimiento de los dispositivos del usuario final antes de conectarse a Citrix ADC. NAC en Citrix SSO requiere un servidor MDM como Citrix Endpoint Management o Intune y Citrix ADC.

Configurar un perfil de VPN administrado por MDM para el Citrix SSO

En la siguiente sección se recogen instrucciones paso a paso para configurar perfiles VPN de todo el dispositivo y por aplicación para Citrix SSO mediante Citrix Endpoint Management (anteriormente XenMobile) como ejemplo. Otras soluciones MDM pueden utilizar este documento como referencia cuando se trabaja con Citrix SSO.

> **Nota:** En esta sección se explican los pasos de configuración para un perfil VPN básico para todo el dispositivo y por aplicación. También puede configurar Proxies bajo demanda, Always-On,

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

> siguiendo la documentación de Citrix Endpoint Management (anteriormente XenMobile) o la configuración de carga útil de MDM VPN de Apple.

Perfiles VPN a nivel de dispositivo

Los perfiles VPN de nivel de dispositivo se utilizan para configurar una VPN en todo el sistema. El tráfico de todas las aplicaciones y servicios se canaliza a Citrix Gateway en función de las directivas VPN (como túnel completo, túnel dividido, túnel inverso) definidas en Citrix ADC.

Para configurar una VPN a nivel de dispositivo en Citrix Endpoint Management

Realice los siguientes pasos para configurar una VPN a nivel de dispositivo en Citrix Endpoint Management.

1. En la consola de Citrix Endpoint Management MDM, vaya a **Configurar** > **Directivas de dispositivo** > **Agregar nueva directiva**.

2. Seleccione **iOS** en el panel de la izquierda Plataforma de directivas. Seleccione **VPN** en el panel derecho.

3. En la página **Información de directiva**, introduzca un nombre y una descripción de directiva válidos y haga clic en **Siguiente**.

4. En la página **Directiva de VPN** para iOS, escriba un nombre de conexión válido y elija **SSL personalizado** en **Tipo de conexión**.

Nota: En la carga útil MDM VPN, el nombre de la conexión corresponde a la clave **UserDefinedName** y la **clave de tipo VPN**debe establecerse en **VPN**.

5. En **Identificador SSL personalizado (formato DNS inverso)**, escriba **com.citrix.NetScalerGateway.ios.app**. Este es el identificador de paquete para la aplicación Citrix SSO en iOS.

Nota: En la carga útil de MDM VPN, el identificador SSL personalizado corresponde a la clave **VPN-Subtype**.

6. En el **identificador del paquete del proveedor**, escriba **com.citrix.NetScalerGateway.ios.app.vpnPlugin**. Este es el identificador de paquete de la extensión de red contenida en el binario de la aplicación Citrix SSO iOS.

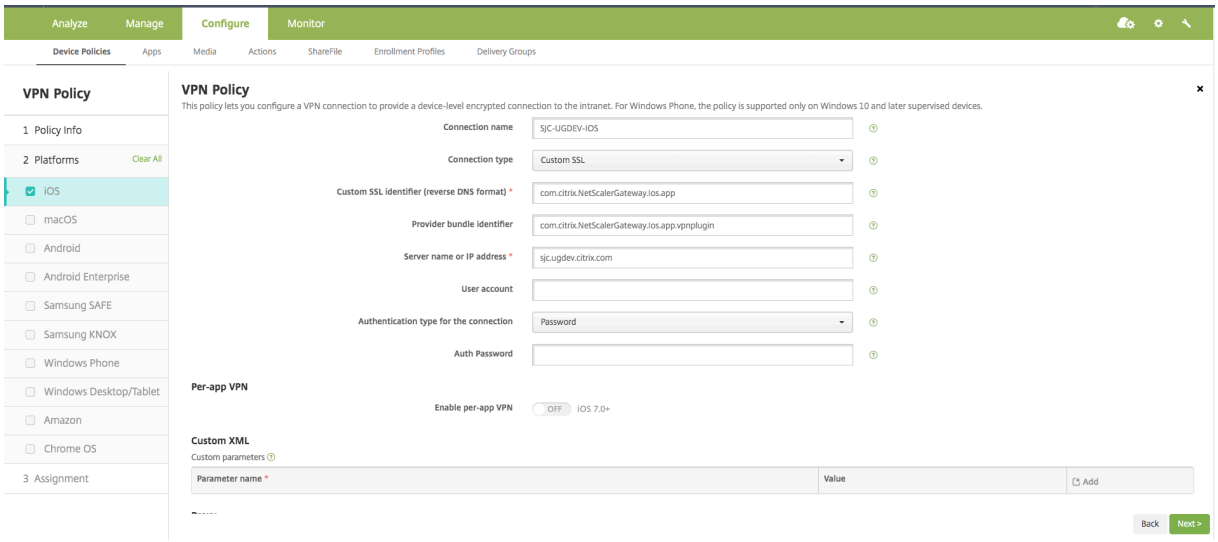
Nota: En MDM VPN payload, el identificador del paquete del proveedor corresponde a la clave **ProviderBundleIdentifier**.

7. En **Nombre del servidor o dirección IP**, introduzca la dirección IP o FQDN (nombre de dominio completo) de Citrix ADC asociado a esta instancia de Citrix Endpoint Management.

Los campos restantes de la página de configuración son opcionales. Las configuraciones para estos campos se pueden encontrar en la documentación de Citrix Endpoint Management (anteriormente XenMobile).

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

8. Haga clic en **Siguiente**.



9. Haga clic en **Save**.

Perfiles VPN por aplicación

Los perfiles VPN por aplicación se utilizan para configurar VPN para una aplicación específica. El tráfico de la aplicación específica se canaliza a Citrix Gateway. La carga útil de VPN por aplicación admite todas las claves para VPN en todo el dispositivo, además de algunas claves adicionales.

Para configurar una VPN a nivel de aplicación en Citrix Endpoint Management

Realice los siguientes pasos para configurar una VPN por aplicación:

1. Complete la configuración de VPN a nivel de dispositivo en Citrix Endpoint Management.

2. Activa el conmutador **Habilitar VPN por aplicación** en la sección VPN por aplicación.

3. Active el **interruptor On-Demand Match App Enabled** si Citrix SSO debe iniciarse automáticamente cuando se inicie la aplicación Match. Esto se recomienda para la mayoría de los casos por aplicación.

Nota: En la carga útil de MDM VPN, este campo corresponde a la clave **OnDemandMatchOpenabled**.

4. En **Tipo de proveedor**, seleccione **Túnel de paquetes**.

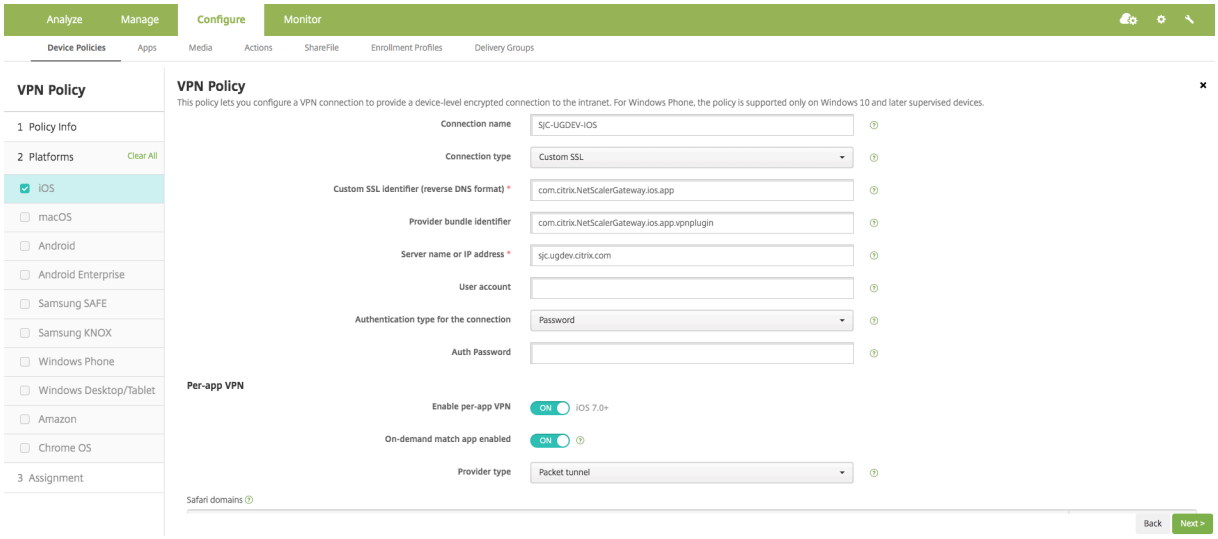
Nota: En la carga útil MDM VPN, este campo corresponde al **tipo de proveedor**clave.

5. La configuración de Safari Domain es opcional. Cuando se configura el dominio Safari, Citrix SSO se inicia automáticamente cuando los usuarios inician Safari y se desplazan a una URL que coincida con la del campo **Dominio**. Esto no se recomienda si quiere restringir VPN para una aplicación específica.

Nota: En la carga útil MDM VPN, este campo corresponde a la clave **SafariDomains**.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Los campos restantes de la página de configuración son opcionales. Las configuraciones para estos campos se pueden encontrar en la documentación de Citrix Endpoint Management (anteriormente XenMobile).



14. Haga clic en **Siguiente.**

15. Haga clic en **Save**.

Para asociar este perfil VPN a una aplicación específica en el dispositivo, debe crear una directiva de inventario de
aplicaciones y una directiva de proveedor de credenciales siguiendo esta guía: https://www.citrix.com/blogs/2016/04/19/per-app-vpn-with-xenmobile-and-citrix-vpn/.

Configuración del túnel dividido en VPN por aplicación

Los clientes de MDM pueden configurar el túnel dividido en VPN por aplicación para Citrix SSO. Para ello, se debe agregar el siguiente par clave/valor a la sección de configuración del proveedor del perfil VPN creado en el servidor MDM.

```
1 -  Key = "PerAppSplitTunnel"
2 -  Value = "true or 1 or yes"
3 <!--NeedCopy-->
```

La clave distingue entre mayúsculas y minúsculas y debe ser una coincidencia exacta mientras que el valor no distingue entre mayúsculas y minúsculas.

Nota: La interfaz de usuario para configurar la configuración del proveedor no es estándar entre los proveedores de MDM. Debe ponerse en contacto con el proveedor de MDM para encontrar la sección de configuración del proveedor en la consola de usuario de MDM.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

A continuación se muestra una captura de pantalla de ejemplo de la configuración (configuración específica del proveedor) en Citrix Endpoint Management.

A continuación se muestra una captura de pantalla de ejemplo de la configuración (configuración específica del proveedor) en Microsoft Intune.

Inhabilitar los perfiles VPN creados por el usuario

Los clientes de MDM pueden impedir que los usuarios creen manualmente perfiles VPN desde la aplicación Citrix SSO. Para ello, se debe agregar el siguiente par clave/valor a la sección de configuración del proveedor del perfil VPN creado en el servidor MDM.

```
1 -  Key = "disableUserProfiles"
2 -  Value = "true or 1 or yes"
3 <!--NeedCopy-->
```

La clave distingue entre mayúsculas y minúsculas y debe ser una coincidencia exacta mientras que el valor no distingue entre mayúsculas y minúsculas.

Nota: La interfaz de usuario para configurar la configuración del proveedor no es estándar entre los proveedores de MDM. Debe ponerse en contacto con el proveedor de MDM para encontrar la sección de configuración del proveedor en la consola de usuario de MDM.

A continuación se muestra una captura de pantalla de ejemplo de la configuración (configuración específica del proveedor) en Citrix Endpoint Management.

A continuación se muestra una captura de pantalla de ejemplo de la configuración (configuración específica del proveedor) en Microsoft Intune.

Problemas conocidos

Descripción del problema: Tunelización para direcciones FQDN que contienen un dominio ".local" en configuraciones VPN por aplicación o VPN bajo demanda. Hay un error en el marco de extensión de red de Apple que impide que las direcciones FQDN que contienen .local en la parte del dominio (por ejemplo, http://wwww.abc.local) pasen a ser de túnel a través de la interfaz TUN del sistema. El tráfico de esta dirección se envía a través de la interfaz física del dispositivo en su lugar. El problema se observa solo con las configuraciones VPN por aplicación o VPN bajo demanda y no se ve con las configuraciones VPN de todo el sistema. Citrix ha presentado un informe de error de radar a Apple, y Apple había señalado que, de acuerdo con RFC-6762:https://tools.ietf.org/html/rfc6762,.local es una consulta DNS de multidifusión (MDN) y, por lo tanto, no es un error. Sin embargo, Apple aún no ha cerrado el error y no está claro si el problema se resolverá en futuras versiones de iOS.

Solución alternativa: Asigne un nombre de dominio.local para direcciones como la solución alternativa.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Limitaciones

- La tunelización dividida basada en FQDN aún no es totalmente compatible.
- El análisis de punto final (EPA) no es compatible con iOS.
- No se admite el túnel dividido basado en puertos/protocolos.

Enviar identidad de certificado de usuario como datos adjuntos de correo electrónico a usuarios de iOS

April 3, 2020

Citrix SSO en iOS admite la autenticación de certificados de cliente con Citrix Gateway. En iOS, los certificados se pueden entregar a la aplicación Citrix SSO de una de las siguientes maneras:

- Servidor MDM: Este es el enfoque preferido para los clientes de MDM. Los certificados se configuran directamente en el perfil VPN administrado MDM. Los perfiles VPN y los certificados se envían a continuación a los dispositivos inscritos cuando el dispositivo se inscribe en el servidor MDM. Siga los documentos específicos del proveedor de MDM para este enfoque.
- Correo electrónico: único enfoque para clientes que no sean MDM. En este enfoque, los administradores envían un correo electrónico con la identidad del certificado de usuario (certificado y clave privada) adjunta como un archivo PCKS #12 a los usuarios. Los usuarios deben tener sus cuentas de correo electrónico configuradas en su dispositivo iOS para recibir el correo electrónico con datos adjuntos. El archivo se puede importar a la aplicación Citrix SSO en iOS. En la siguiente sección se explican los pasos de configuración para este enfoque.

Requisitos previos

- Certificado de usuario: Archivo de identidad PKCS #12 con una extensión.pfx o.p12 para un usuario determinado. Este archivo contiene tanto el certificado como la clave privada.
- Cuenta de correo electrónico configurada en el dispositivo iOS.
- Aplicación Citrix SSO instalada en el dispositivo iOS.

Pasos de configuración

1. Cambie el nombre del tipo de extensión o MIME del certificado de usuario.

Las extensiones de archivo más utilizadas para el certificado de usuario son ".pfx", ".p12", etc. Estas extensiones de archivo no son estándar para la plataforma iOS a diferencia de formatos como.pdf,.doc.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Tanto ".pfx" como ".p12" son reclamados por el sistema iOS y no pueden ser reclamados por aplicaciones de terceros como Citrix SSO. Por lo tanto, Citrix SSO ha definido un nuevo tipo de extensión o MIME llamado ".citrixsso-pfx" y ".citrixsso-p12". Los administradores deben cambiar el tipo de extensión o MIME del certificado de usuario, de ".pfx" estándar o ".p12" a ".citrixsso-pfx" o ".citrixsso-p12" respectivamente. Para cambiar el nombre de la extensión, los administradores pueden ejecutar el siguiente comando en el símbolo del sistema o terminal.

Windows 10

```
cd <DIRECTORY_PATH_TO_CERTIFICATE_FILE>
rename <CERTIFICATE_FILE_NAME>.pfx <CERTIFICATE_FILE_NAME>.citrixsso-
   pfx
<!--NeedCopy-->
```

macOS

```
cd <DIRECTORY_PATH_TO_CERTIFICATE_FILE>
mv <CERTIFICATE_FILE_NAME>.pfx <CERTIFICATE_FILE_NAME>.citrixsso-pfx
<!--NeedCopy-->
```

2. Enviar el archivo como un archivo adjunto de correo electrónico.
El archivo de certificado de usuario con la nueva extensión se puede enviar como un archivo adjunto de correo electrónico al usuario.

Al recibir el correo electrónico, los usuarios deben instalar el certificado en la aplicación Citrix SSO.

Configurar Citrix SSO para usuarios de macOS

January 4, 2022

La aplicación Citrix SSO para macOS proporciona la mejor solución de protección de datos y acceso a aplicaciones que ofrece Citrix Gateway. Ahora puede acceder de forma segura a las aplicaciones críticas para el negocio, los escritorios virtuales y los datos corporativos en cualquier momento y desde cualquier lugar.
Citrix SSO es el cliente VPN de próxima generación para Citrix Gateway para crear y administrar conexiones VPN desde dispositivos macOS. Citrix SSO se crea mediante el marco de extensión de red (NE) de Apple. NE framework de Apple es una biblioteca moderna que contiene API que se pueden utilizar para personalizar y ampliar las funciones principales de red de macOS. La extensión de red con soporte para SSL VPN está disponible en dispositivos que ejecutan macOS 10.11+.

La aplicación Citrix SSO reemplaza el complemento heredado de Citrix Gateway basado en Extensiones de núcleo (KE) que Apple va a dejar de utilizar pronto. Citrix SSO App admite funciones avanzadas como Conexiones iniciadas por el servidor y DTLS.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

La aplicación Citrix SSO proporciona compatibilidad completa con la administración de dispositivos móviles (MDM) en macOS. Con un servidor MDM, un administrador ahora puede configurar y administrar de forma remota perfiles VPN a nivel de dispositivo y por aplicación.
La aplicación Citrix SSO para macOS se puede instalar desde una almacén de aplicaciones Mac.

Comparación de funciones entre Citrix VPN y Citrix SSO

En la siguiente tabla, se compara la disponibilidad de diversas funciones entre Citrix VPN y Citrix SSO.

Función	Citrix VPN	Citrix SSO
Método de distribución de aplicaciones	página Descargas de Citrix	App Store
Número de conexiones en túnel	128	128
Acceso desde explorador	Se admite	No se admite
Acceso desde aplicación nativa	Se admite	Se admite
Túnel dividido (DESACTIVADO/ACTIVADO/INVERSO)	Se admite	Se admite
DNS dividido (LOCAL/REMOTO/AMBOS)	REMOTO	REMOTO
Acceso a LAN local	Habilitar o inhabilitar	Siempre habilitado
Compatibilidad con conexiones iniciadas por el servidor (SIC)	No se admite	Se admite
Transferir el inicio de sesión	Se admite	Se admite
Proxy del lado del cliente	Se admite	No se admite
Compatibilidad con EPA cásico/Opswat	Se admite	Se admite
Compatibilidad con certificados de dispositivo	Se admite	Se admite
Compatibilidad con tiempo de espera de sesión	Se admite	Se admite
Compatibilidad con tiempo de espera forzado	Se admite	Se admite

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Función	Citrix VPN	Citrix SSO
Compatibilidad con tiempo de espera inactivo	Se admite	No se admite
IPV6	No se admite	Se admite
Itinerancia de red (conmutación entre Wi-Fi, Ethernet, etc.)	Se admite	Se admite
Compatibilidad con aplicaciones de intranet	Se admite	Se admite
Compatibilidad con DTLS para UDP	No se admite	Se admite
Compatibilidad con contrato de licencia de usuario final	Se admite	Se admite
Integración de aplicaciones + Receiver	Se admite	No se admite
Autenticación: Local, LDAP, RADIUS	Se admite	Se admite
Autenticación de certificados de cliente	Se admite	Se admite
Compatibilidad con TLS (TLS1, TLS1.1 y TLS1.2)	Se admite	Se admite
Autenticación de dos factores	Se admite	Se admite

Compatibilidad con productos MDM

Citrix SSO para macOS es compatible con la mayoría de los proveedores de MDM, como Citrix XenMobile, Microsoft Intune, etc. Es compatible con una función denominada Control de acceso a redes (NAC) mediante la cual, los administradores de MDM pueden imponer el cumplimiento de los dispositivos del usuario final antes de conectarse a Citrix Gateway. NAC en Citrix SSO requiere un servidor MDM como XenMobile o Intune y Citrix Gateway. Para obtener más información sobre NAC, haga clic en aquí.

Configurar un perfil de VPN administrado por MDM para el Citrix SSO

En la siguiente sección se recogen instrucciones paso a paso para configurar perfiles VPN de todo el dispositivo y por aplicación para Citrix SSO mediante Citrix Endpoint Management (anteriormente

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

XenMobile) como ejemplo. Otras soluciones MDM pueden utilizar este documento como referencia cuando se trabaja con Citrix SSO.

> **Nota:** En esta sección se explican los pasos de configuración para un perfil VPN básico para todo el dispositivo y por aplicación. También puede configurar Proxies bajo demanda, Always-On, siguiendo la documentación de Citrix Endpoint Management (anteriormente XenMobile) o la de Configuración de carga útil VPN MDM de Apple.

Perfiles VPN a nivel de dispositivo

Los perfiles VPN de nivel de dispositivo se utilizan para configurar una VPN en todo el sistema. El tráfico de todas las aplicaciones y servicios se canaliza a Citrix Gateway en función de las directivas VPN (como túnel completo, túnel dividido, túnel inverso) definidas en Citrix ADC.

Para configurar una VPN a nivel de dispositivo en Citrix Endpoint Management

Realice los siguientes pasos para configurar una VPN a nivel de dispositivo.

1. En la consola de Citrix Endpoint Management MDM, vaya a **Configurar** > **Directivas de dispositivo** > **Agregar nueva directiva**.

2. Seleccione **macOS** en el panel de la izquierda Plataforma de directivas. Seleccione **Directiva VPN** en el panel derecho.

3. En la página **Información de directiva**, introduzca un nombre y una descripción de directiva válidos y haga clic en **Siguiente**.

4. En la página de **detalles de directiva** para macOS, escriba un nombre de conexión válido y elija **SSL personalizado** en **Tipo de conexión**.

Nota: En la carga útil MDM VPN, el nombre de la conexión corresponde a la clave **UserDefinedName** y la **clave de tipo VPN**debe establecerse en **VPN**.

5. En **Identificador SSL personalizado (formato DNS inverso)**, escriba **com.citrix.NetScalerGateway.macos.ap**
Este es el identificador de paquete para la aplicación Citrix SSO en macOS.

Nota: En la carga útil de MDM VPN, el identificador SSL personalizado corresponde a la clave **VPN-Subtype**.

6. En el **identificador del paquete del proveedor**, escriba **com.citrix.NetScalerGateway.macos.app.vpnPlugin**
Este es el identificador de paquete de la extensión de red contenida en el binario de la aplicación Citrix SSO macOS.

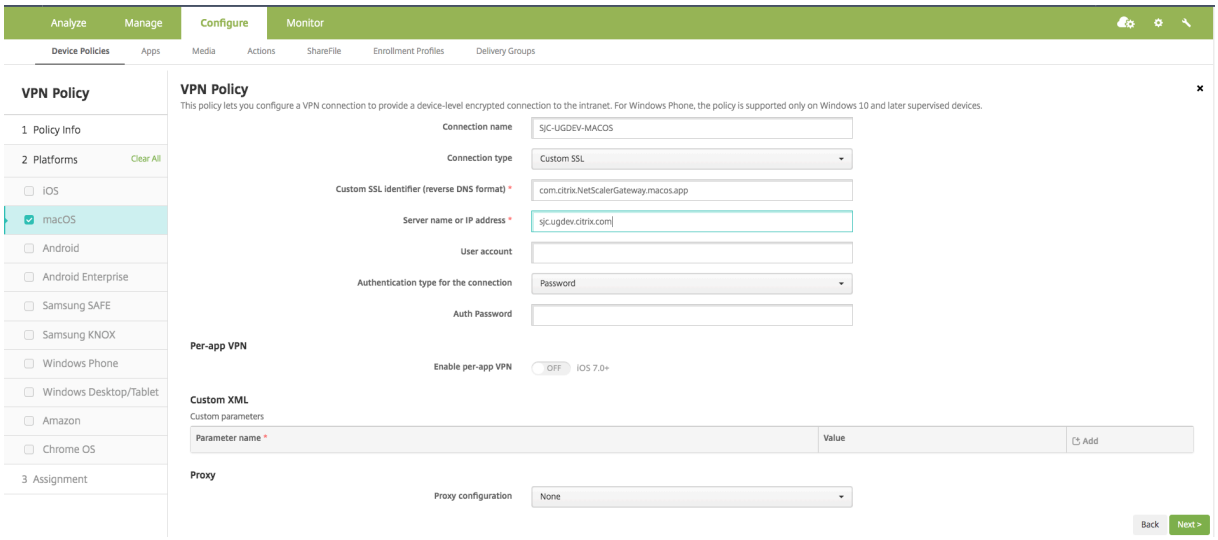
Nota: En MDM VPN payload, el identificador del paquete del proveedor corresponde a la clave **ProviderBundleIdentifier**.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

7. En **Nombre del servidor o dirección IP**, introduzca la dirección IP o FQDN de Citrix ADC asociado a esta instancia de Citrix Endpoint Management.

Los campos restantes de la página de configuración son opcionales. Las configuraciones para estos campos se encuentran en la documentación de Citrix Endpoint Management.

8. Haga clic en **Siguiente**.



9. Haga clic en **Save**.

Perfiles VPN por aplicación

Los perfiles VPN por aplicación se utilizan para configurar VPN para una aplicación específica. El tráfico de la aplicación específica se canaliza a Citrix Gateway. La carga útil de VPN por aplicación admite todas las claves para VPN en todo el dispositivo, además de algunas claves adicionales.

Para configurar una VPN a nivel de aplicación en Citrix Endpoint Management

Realice los siguientes pasos para configurar una VPN por aplicación en Citrix Endpoint Management:

1. Complete la configuración de VPN a nivel de dispositivo en Citrix Endpoint Management.

2. Activa el conmutador **Habilitar VPN por aplicación** en la sección VPN por aplicación.

3. Active el **interruptor On-Demand Match App Enabled** si Citrix SSO debe iniciarse automáticamente cuando se inicie la aplicación Match. Esto se recomienda para la mayoría de los casos por aplicación.

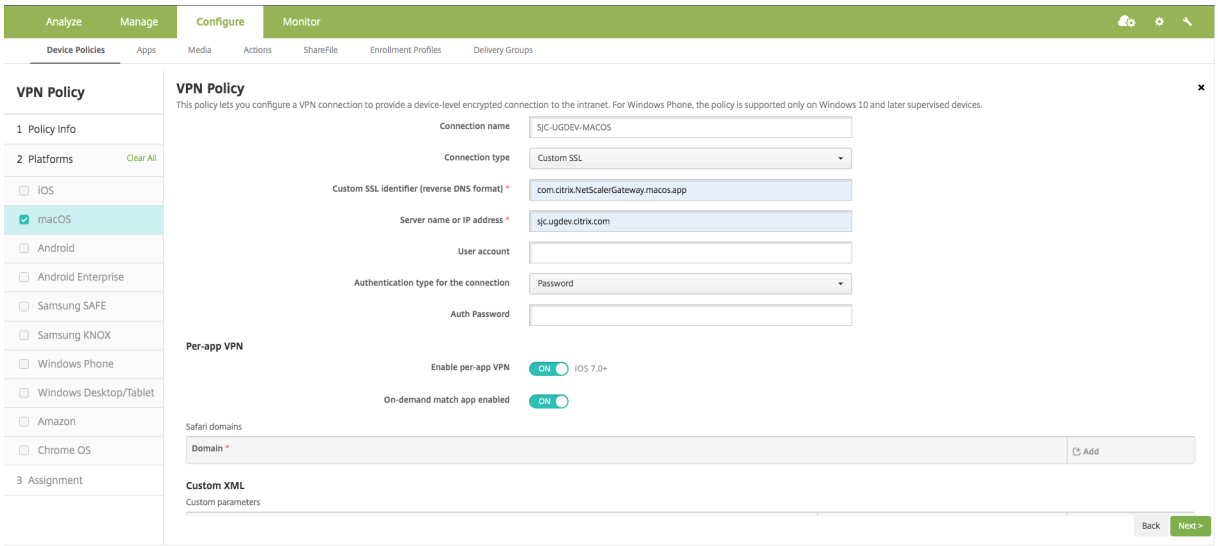
Nota: En la carga útil de MDM VPN, este campo corresponde a la clave **OnDemandMatchOpenabled**.

5. La configuración de Safari Domain es opcional. Cuando se configura el dominio Safari, Citrix SSO se inicia automáticamente cuando los usuarios inician Safari y se desplazan a una URL que coincida con la del campo **Dominio**. Esto no se recomienda si quiere restringir VPN para una aplicación específica.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Nota: En la carga útil MDM VPN, este campo corresponde a la clave **SafariDomains**.

Los campos restantes de la página de configuración son opcionales. Las configuraciones para estos campos se pueden encontrar en la documentación de Citrix Endpoint Management (anteriormente XenMobile).



13. Haga clic en **Siguiente**.

14. Haga clic en **Save**.

Para asociar este perfil VPN a una aplicación específica en el dispositivo, debe crear una directiva de inventario de
aplicaciones y una directiva de proveedor de credenciales siguiendo esta guía: https://www.citrix.com/blogs/2016/04/19/per-app-vpn-with-xenmobile-and-citrix-vpn/

Configuración del túnel dividido en VPN por aplicación

Los clientes de MDM pueden configurar el túnel dividido en VPN por aplicación para Citrix SSO. Para ello, se debe agregar el siguiente par clave/valor a la sección de configuración del proveedor del perfil VPN creado en el servidor MDM.

```
1 - Clave = "PerAppsPlitTunnel"
2 - Valor = "verdadero o 1 o sí"
```

La clave distingue entre mayúsculas y minúsculas y debe ser una coincidencia exacta mientras que el valor no distingue entre mayúsculas y minúsculas.

Nota: La interfaz de usuario para configurar la configuración del proveedor no es estándar entre los proveedores de MDM. Debe ponerse en contacto con el proveedor de MDM para encontrar la sección de configuración del proveedor en la consola de usuario de MDM.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

A continuación se muestra una captura de pantalla de ejemplo de la configuración (configuración específica del proveedor) en Citrix Endpoint Management.

A continuación se muestra una captura de pantalla de ejemplo de la configuración (configuración específica del proveedor) en Microsoft Intune.

Inhabilitar los perfiles VPN creados por el usuario

Los clientes de MDM pueden impedir que los usuarios creen manualmente perfiles VPN desde la aplicación Citrix SSO. Para ello, se debe agregar el siguiente par clave/valor a la sección de configuración del proveedor del perfil VPN creado en el servidor MDM.

```
- Clave = "DisableUserProfiles"
- Valor = "verdadero o 1 o sí"
```

La clave distingue entre mayúsculas y minúsculas y debe ser una coincidencia exacta mientras que el valor no distingue entre mayúsculas y minúsculas.

Nota: La interfaz de usuario para configurar la configuración del proveedor no es estándar entre los proveedores de MDM. Debe ponerse en contacto con el proveedor de MDM para encontrar la sección de configuración del proveedor en la consola de usuario de MDM.

A continuación se muestra una captura de pantalla de ejemplo de la configuración (configuración específica del proveedor) en Citrix Endpoint Management.

A continuación se muestra una captura de pantalla de ejemplo de la configuración (configuración específica del proveedor) en Microsoft Intune.

Problemas conocidos

Los siguientes son los problemas conocidos actualmente.

- El inicio de sesión de EPA falla si el usuario se coloca en el grupo de cuarentena.
- No se muestra el mensaje de advertencia de tiempo de espera forzado.
- La aplicación SSO permite iniciar sesión si el túnel dividido está activado y no hay aplicaciones de intranet configuradas.

Limitaciones

Las siguientes son las limitaciones actuales.

- Algunos de los análisis EPA (por ejemplo, análisis de administración de parches, exploración del explorador web, proceso de eliminación) podrían fallar debido al acceso restringido a la aplicación SSO debido al espacio limitado.
- No se admite el túnel dividido basado en puertos/protocolos.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Preguntas frecuentes

En esta sección se recogen las preguntas frecuentes de la aplicación Citrix SSO.

¿En qué se diferencia la aplicación Citrix SSO de la aplicación VPN?
Citrix SSO es el cliente SSL VPN de última generación para Citrix ADC. La aplicación utiliza el marco de extensión de red de Apple para crear y administrar conexiones VPN en dispositivos iOS y macOS. Citrix
VPN es el cliente VPN heredado que utilizó las API VPN privadas de Apple, que ahora están obsoletas. La compatibilidad con Citrix VPN se eliminará de la App Store en los próximos meses.

¿Qué es NE?
El marco de extensión de red (NE) de Apple es una biblioteca moderna que contiene API que se pueden utilizar para personalizar y ampliar las funciones principales de red de iOS y macOS. La extensión de red con soporte para SSL VPN está disponible en dispositivos con iOS 9+ y macOS 10.11+.

¿Para qué versiones de Citrix ADC es compatible con Citrix SSO?
Las funciones VPN de Citrix SSO son compatibles con las versiones 10.5 y superiores de Citrix ADC. El TOTP está disponible en Citrix ADC versión 12.0 y superior. Aún no se ha anunciado públicamente la notificación Push en Citrix ADC. La aplicación requiere iOS 9+ y macOS 10.11+ versiones.

¿Cómo funciona la autenticación basada en certificados para clientes que no son MDM?
Los clientes que previamente distribuyeron certificados por correo electrónico o explorador para realizar la autenticación de certificados de cliente en Citrix VPN deben tener en cuenta este cambio al usar Citrix SSO. Esto se aplica principalmente a los clientes que no son MDM que no utilizan un servidor MDM para distribuir certificados de usuario. Consulte “Importación de certificados en Citrix SSO a través de correo electrónico” para poder distribuir certificados.

¿Qué es el Control de acceso a la red (NAC)? ¿Cómo configuro NAC con Citrix SSO y Citrix Gateway?
Los clientes de MDM de Microsoft Intune y Citrix Endpoint Management (anteriormente XenMobile) pueden aprovechar la función de Control de acceso a redes (NAC) en Citrix SSO. Con NAC, los administradores pueden proteger su red interna empresarial agregando una capa adicional de autenticación para dispositivos móviles administrados por un servidor MDM. Los administradores pueden aplicar una comprobación de conformidad de dispositivos en el momento de la autenticación en Citrix SSO.

Para usar NAC con Citrix SSO, debe habilitarlo tanto en Citrix Gateway como en el servidor MDM.

- Para habilitar NAC en Citrix ADC, consulte este enlace.
- Si el proveedor MDM es Intune, consulte este enlace.
- Si el proveedor de MDM es Citrix Endpoint Management (anteriormente XenMobile), consulte este enlace.

Nota: La versión mínima de Citrix SSO admitida es 1.1.6 y superior.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Compatibilidad con nFactor para Citrix SSO en iOS y macOS

March 22, 2022

La autenticación multifactor (nFactor) mejora la seguridad de una aplicación al exigir a los usuarios que proporcionen varias pruebas de identificación para obtener acceso. Los administradores pueden configurar diferentes factores de autenticación que incluyen certificado de cliente, LDAP, RADIUS, OAuth, SAML, etc. Estos factores de autenticación se pueden configurar en cualquier orden según las necesidades de la organización.

Citrix SSO admite los siguientes protocolos de autenticación:

- **nFactor**: El protocolo nFactor se utiliza cuando un servidor virtual de autenticación está enlazado al servidor virtual VPN en la Gateway. Dado que el orden de los factores de autenticación es dinámico, el cliente utiliza una instancia de explorador que se representa en el contexto de la aplicación para presentar la interfaz gráfica de usuario de autenticación.
- **Clásico**: El protocolo clásico es el protocolo de reserva predeterminado que se utiliza si las directivas de autenticación clásicas están configuradas en el servidor virtual VPN de la Gateway. El protocolo clásico es el protocolo de reserva si NFactor falla para métodos de autenticación específicos como NAC.
- **Plataforma de identidad Citrix**: El protocolo de plataforma de identidad Citrix se utiliza cuando se autentica en CloudGateway o servicio de Gateway y requiere la inscripción de MDM en Citrix Cloud.

En la siguiente tabla se resumen los diversos métodos de autenticación admitidos por cada protocolo.

Método de autenticación	Factor nFactor	Clásico	IdP de Citrix
Certificado de cliente	Se admite	Se admite	No se admite
LDAP	Se admite	Se admite	No se admite
Locales	Se admite	Se admite	No se admite
RADIUS	Se admite	No se admite	No se admite
SAML	Se admite	No se admite	No se admite
OAuth	Se admite	No se admite	No se admite
TACOS	Se admite	No se admite	No se admite
WebAuth	Se admite	No se admite	No se admite
Negociar	Se admite	No se admite	No se admite
EPA	Se admite	Se admite	No se admite

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Método de autenticación	Factor nFactor	Clásico	IdP de Citrix
NAC	No se admite	Se admite	No se admite
StoreFront	No se admite	No se admite	No se admite
ADAL	No se admite	No se admite	No se admite
DS-AUTH	No se admite	No se admite	Se admite

Configuración de nFactor

Para obtener más información sobre la configuración de nFactor, consulte Configuración de la autenticación nFactor.

Importante: Para utilizar el protocolo nFactor con Citrix SSO, la versión recomendada de Citrix Gateway en locales es 12.1.50.xx y posterior.

Limitaciones

- El protocolo nFactor está inhabilitado, de forma predeterminada. Los clientes que deseen utilizar nFactor deben solicitar explícitamente soporte técnico de Citrix y proporcionar el FQDN de su servidor virtual VPN.
- Las directivas de autenticación específicas para dispositivos móviles, como NAC (control de acceso a red), requieren que el cliente envíe un identificador de dispositivo firmado como parte de la autenticación con Citrix Gateway. El identificador de dispositivo firmado es una clave secreta giratoria que identifica de forma única un dispositivo móvil que está inscrito en un entorno MDM. Esta clave está incrustada en un perfil VPN administrado por un servidor MDM. Es posible que no sea posible inyectar esta clave en el contexto WebView. Si NAC está habilitado en un perfil MDM VPN, Citrix SSO vuelve automáticamente al protocolo de autenticación clásico.

Preguntas frecuentes

January 4, 2022

En esta sección se recogen las preguntas más frecuentes en la aplicación Citrix SSO.

¿En qué se diferencia la aplicación Citrix SSO de la aplicación VPN?
Citrix SSO es el cliente SSL VPN de última generación para Citrix ADC. La aplicación utiliza el marco de extensión de red de Apple para crear y administrar conexiones VPN en dispositivos iOS y macOS.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Citrix
VPN es el cliente VPN heredado que utilizó las API VPN privadas de Apple, que ahora están obsoletas. La compatibilidad con Citrix VPN se eliminará de la App Store en los próximos meses.

¿Qué es NE?
El marco de extensión de red (NE) de Apple es una biblioteca moderna que contiene API que se pueden utilizar para personalizar y ampliar las funciones principales de red de iOS y macOS. La
extensión de red con soporte para SSL VPN está disponible en dispositivos con iOS 9+ y macOS 10.11+.

¿Para qué versiones de Citrix ADC es compatible con Citrix SSO?
Las funciones VPN de Citrix SSO son compatibles con las versiones 10.5 y superiores de Citrix ADC. El TOTP está disponible en Citrix ADC versión 12.0 y superior. Aún no se ha anunciado públicamente la notificación Push en Citrix ADC. La aplicación requiere iOS 9+ y macOS 10.11+ versiones.

¿Cómo funciona la autenticación basada en certificados para clientes que no son MDM?
Los clientes que previamente distribuyeron certificados por correo electrónico o explorador para realizar la autenticación de certificados de cliente en Citrix VPN deben tener en cuenta este cambio al usar Citrix SSO. Esto se aplica
principalmente a los clientes que no son MDM que no utilizan un servidor MDM para distribuir certificados de usuario. Consulte “Importación de certificados en Citrix SSO a través de correo electrónico” para poder
distribuir certificados.

¿Qué es el Control de acceso a la red (NAC)? ¿Cómo configuro NAC con Citrix SSO y Citrix Gateway?
Los clientes de MDM de Microsoft Intune y Citrix Endpoint Management (anteriormente XenMobile) pueden aprovechar la función de Control de acceso a redes (NAC) en Citrix SSO. Con NAC, los administradores pueden proteger su red interna empresarial agregando una capa adicional de autenticación para dispositivos móviles administrados por un servidor MDM. Los administradores pueden aplicar una comprobación de conformidad de dispositivos en el momento de la autenticación en Citrix SSO.

Para usar NAC con Citrix SSO, debe habilitarlo tanto en Citrix Gateway como en el servidor MDM.

- Para habilitar NAC en Citrix ADC, consulte este enlace.
- Si el proveedor MDM es Intune, consulte este enlace.
- Si el proveedor de MDM es Citrix Endpoint Management (anteriormente XenMobile), consulte este enlace.

Nota: La versión mínima de Citrix SSO admitida es 1.1.6 y superior.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Citrix SSO para dispositivos Android

April 3, 2020

Citrix SSO ofrece la mejor solución de protección de datos y acceso a las aplicaciones con Citrix Gateway. Ahora puede acceder de forma segura a las aplicaciones críticas para el negocio, los escritorios virtuales y los datos corporativos en cualquier momento y desde cualquier lugar.

Notas de la versión

October 18, 2021

Las notas de versión de Citrix SSO describen las nuevas funciones, las mejoras a las funciones existentes, los problemas corregidos y los problemas conocidos disponibles en una versión de servicio. Las notas de la versión incluyen una o varias de las siguientes secciones:

Novedades: Las nuevas funciones y mejoras disponibles en la versión actual.

Problemas corregidos: Los problemas corregidos en la versión actual.

Problemas conocidos: Los problemas que existen en la versión actual y sus soluciones alternativas, siempre que corresponda.

V2.3.14

Problemas resueltos

- Citrix SSO ahora maneja correctamente el mensaje final de establecimiento de sesión VPN.

  [CGOP-12488]

Problemas conocidos

- El estado de VPN Always-On no siempre se actualiza correctamente en la interfaz de usuario de la aplicación.

  [NSHELP-21709]

V2.3.13

Problemas resueltos

- La dirección IP de Citrix Gateway se resuelve solo una vez.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Anteriormente, la dirección IP de Citrix Gateway se resolvió varias veces, lo que ocasionaba errores de conexión a veces.

[CGOP-12101]

Problemas conocidos

- El estado de VPN Always-On no siempre se actualiza correctamente en la interfaz de usuario de la aplicación.

  [NSHELP-21709]

V2.3.12

Problemas resueltos

- Citrix SSO puede bloquearse al guardar un perfil VPN.

  [CGOP-12137]

V2.3.11

Problemas resueltos

- Citrix SSO puede bloquearse al guardar un perfil VPN.

  [CGOP-12137]

- La configuración DisableUserProfile no se refleja correctamente en la interfaz de usuario cuando un nuevo perfil VPN o una actualización a un perfil existente da como resultado el cambio del valor DisableUserProfile.

  [CGOP-11899]

- Citrix SSO para Android no procesa perfiles VPN en modo Propietario de dispositivo (DO).

  [CGOP-11981]

- La conexión VPN no se establece cuando hay IPv6 solo servidores DNS locales.

  [CGOP-12053]

V2.3.10

Problemas resueltos

- Conexión VPN perdida después de un tiempo de inactividad en el dispositivo.

  [CGOP-11381]

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

V2.3.8

Novedades

- **Configurar la aplicación Citrix SSO en un entorno de Intune Android Enterprise**

  Ahora puede configurar la aplicación Citrix SSO en un entorno de Intune Android Enterprise. Para obtener información detallada, consulte Configurar la aplicación Citrix SSO en un entorno de Intune Android Enterprise.

  [CGOP-635]

- **Compatibilidad con el Provisioning de perfiles VPN a través de Android Enterprise**

  Ahora se admite el Provisioning de perfiles VPN a través de Android Enterprise.

  [CGOP-631]

Problemas resueltos

- Si guarda un token que ya está guardado y, a continuación, intenta abrirlo, aparecerán caracteres confusos en el nombre del token.

  [CGOP-11696]

- La aplicación Citrix SSO no puede establecer una sesión VPN si no hay dominios de búsqueda DNS configurados en Citrix Gateway.

  [CGOP-11259]

V2.3.6

Novedades

- **Compatibilidad con AlwaysOn para Citrix SSO**

  La función AlwaysOn de Citrix SSO garantiza que los usuarios estén siempre conectados a la red empresarial. Esta conectividad VPN persistente se logra mediante el establecimiento automático de un túnel VPN.

  [CGOP-10015]

- **La notificación para volver a iniciar sesión se muestra si la expiración del token de Athena causa un cierre de sesión**

  Si se cumplen las condiciones siguientes, se muestra una notificación en la que se solicita a los usuarios que vuelvan a iniciar sesión en Citrix Workspace.

  - La función AlwaysOn está habilitada en el perfil VPN aprovisionado de Citrix Workspace
  - La autenticación de Athena se utiliza para el inicio de sesión único

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

- El usuario ha cerrado sesión de la aplicación Citrix Workspace debido a la expiración del token de Athena

[CGOP-10016]

- **El registro para el servicio de notificación Push se realiza mediante Citrix Gateway**

  Ahora puede registrarse para el servicio de notificación push mediante el dispositivo Citrix Gateway. Anteriormente, el registro se realizó en el dispositivo cliente.

  [CGOP-10542]

Problemas resueltos

A veces, Citrix SSO se bloquea cuando se analiza un nuevo token. Por ejemplo, Citrix SSO se bloquea cuando se elimina un token existente y se analiza otro con el mismo nombre de token.

[CGOP-10818]

V2.3.1

Novedades

- **Las configuraciones administradas se actualizan para incluir más configuraciones de usuario**

  Las configuraciones administradas se actualizan para incluir “BlockUntrustedServers”, “DefaultProfileName” y “DisableUserProfiles” para entornos Android Enterprise.

  [CGOP-10033]

- **Compatibilidad mejorada con notificaciones Push**

  Al configurar Citrix Gateway for Push Notification con el tipo “OTP”, no se solicita el PIN o la huella digital después de que el usuario seleccione “Permitir” en respuesta a la notificación Push solicitando el consentimiento del usuario para permitir que la autenticación continúe.

  [CGOP-9843]

- **Compatibilidad con Firebase Analytics**

  Se agrega compatibilidad con Firebase Analytics básica para proporcionar información sobre el uso de la aplicación Citrix SSO. La mejora es aplicable a geolocalizaciones gruesas, uso de pantalla, diferentes versiones de Android en uso, etc.

  [CGOP-7523]

- **Compatibilidad con configuración de perfil VPN basada en configuraciones administradas de Android**

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

La aplicación Citrix SSO se puede configurar en un entorno Android Enterprise mediante un proveedor de EMM/UEM como Citrix Endpoint Management. El Asistente para configuraciones administradas de Android Enterprise en CEM se puede utilizar para implementar configuraciones de VPN administradas en la aplicación Citrix SSO. Para obtener información sobre cómo configurar la aplicación Citrix SSO mediante Configuraciones administradas, consulte https://info.citrite.net/x/8TIFTw

V2.2.9

Novedades

- **Compatibilidad con notificaciones push**

  Citrix Gateway envía notificaciones Push en su dispositivo móvil registrado para obtener una experiencia de autenticación simplificada de dos factores.

  [CGOP-9592]

Problemas resueltos

- Se permiten caracteres que no sean URL en el campo del servidor en la pantalla Agregar conexión.

  [CGOP-588]

Configurar la aplicación Citrix SSO en un entorno MDM

April 3, 2020

Para configurar la aplicación Citrix SSO en un entorno MDM, consulte Configurar el protocolo Citrix SSO para Android.

Nota:

- En un evnirnoment que no sea MDM, los usuarios crean perfiles VPN manualmente.
- También puede crear una configuración administrada de Android Enterprise para Citrix SSO. Para obtener información detallada, consulte Configurar perfiles VPN para Android Enterprise.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Configurar la aplicación Citrix SSO en un entorno de Intune Android Enterprise

October 18, 2021

El tema captura detalles sobre la implementación y configuración de la aplicación Citrix SSO a través de Microsoft Intune. En este documento se supone que Intune ya está configurado para el soporte de Android Enterprise y que la inscripción de dispositivos ya está terminada.

Requisitos previos

- Intune está configurado para Android Enterprise Support
- Se ha completado la inscripción del dispositivo

Para configurar la aplicación Citrix SSO en un entorno de Intune Android Enterprise

- Agregar la aplicación Citrix SSO como aplicación administrada
- Configurar la directiva de aplicaciones administradas para la aplicación Citrix SSO

Agregar la aplicación Citrix SSO como aplicación administrada

1. Inicie sesión en su portal de Azure.

2. Haga clic en **Intune** en la hoja de navegación izquierda.

3. Haga clic en **Aplicaciones cliente** en el blade Microsoft Intune y, a continuación, haga clic en Aplicaciones en el blade Aplicaciones cliente.

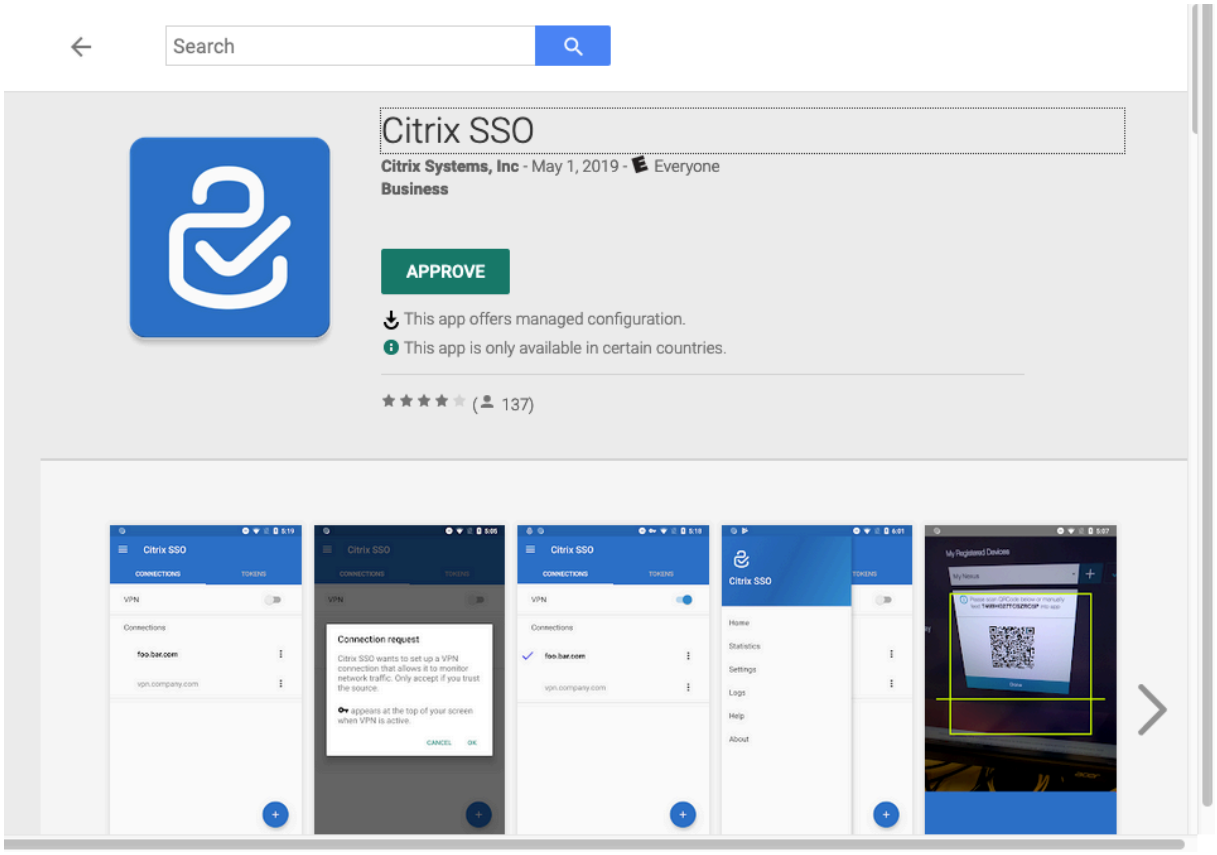
4. Haga clic en **+Agregar** enlace en las opciones del menú superior derecho. Aparecerá la hoja de configuración de Agregar aplicación.

5. Selecciona **Google Play administrado** para el tipo de aplicación.

Esto agrega Administrar la búsqueda de Google Play y la hoja de aprobación si ha configurado Android Enterprise.

6. Busque la aplicación Citrix SSO y selecciónela de la lista de aplicaciones.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



Nota: Si Citrix SSO no aparece en la lista, significa que la aplicación no está disponible en su país.

7. Haga clic en **APROBAR** para aprobar el inicio de Citrix SSO su implementación a través de la almacén Google Play administrada.

Se enumeran los permisos requeridos por la aplicación Citrix SSO.

8. Haga clic en **APROBAR** para aprobar la aplicación para su implementación.

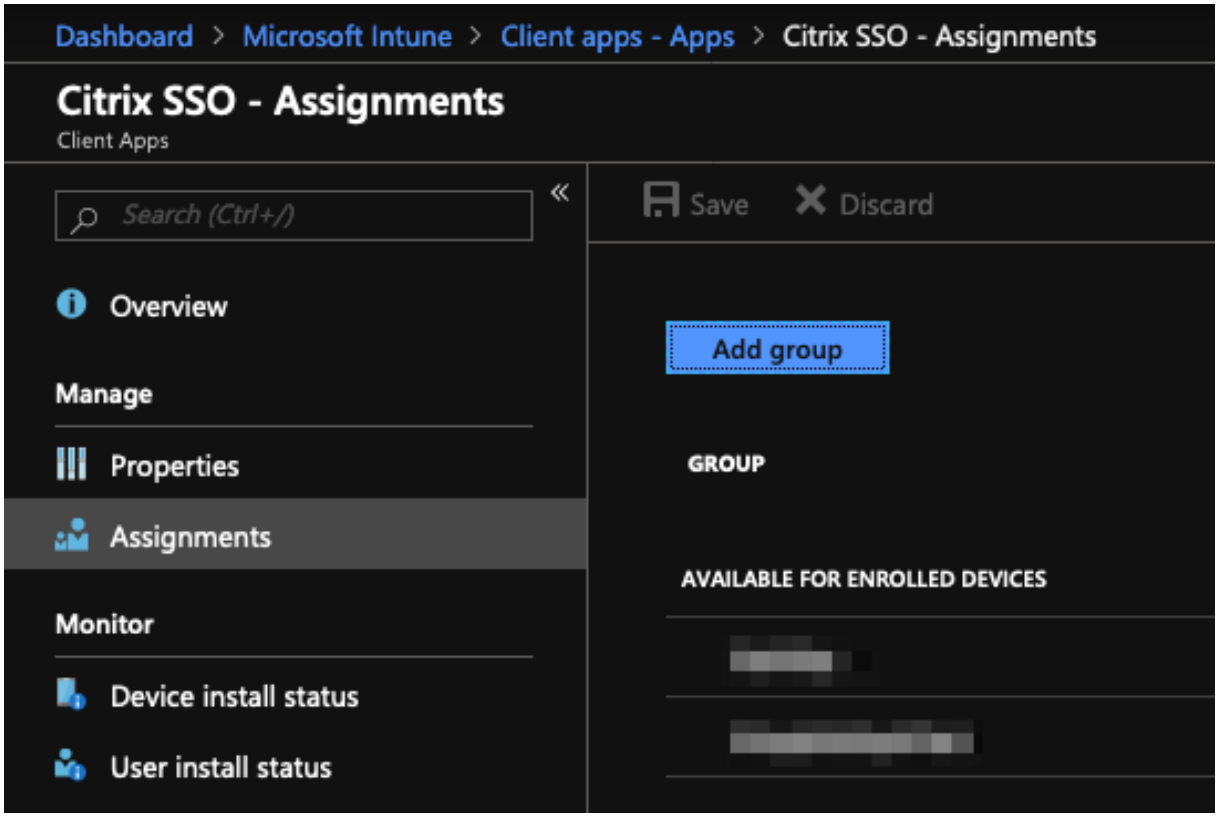
9. Haga clic en **Sincronizar** para sincronizar esta selección con Intune.

La aplicación Citrix SSO se agrega a la lista de aplicaciones cliente. Es posible que tenga que buscar la aplicación Citrix SSO si hay muchas aplicaciones agregadas.

10. Haga clic en la aplicación **Citrix SSO** para abrir la hoja de detalles de la aplicación.

11. Haga clic en **Asignaciones** en la hoja de detalles. Aparece la hoja de**asignación de Citrix SSO**.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



12. Haga clic en **Agregar grupo** para asignar los grupos de usuarios a los que quiere conceder permisos para instalar la aplicación Citrix SSO y haga clic en **Guardar**.

13. Cierre la hoja de detalles de la aplicación Citrix SSO.

La aplicación Citrix SSO se agrega y habilita para su implementación en los usuarios.

Configurar la directiva de aplicaciones administradas para la aplicación Citrix SSO

Después de agregar la aplicación Citrix SSO, debe crear una directiva de configuración administrada para la aplicación Citrix SSO para que el perfil VPN se pueda implementar en la aplicación Citrix SSO en el dispositivo.

1. Abra el blade **Intune** en el portal de Azure.

2. Abra **el blade de aplicaciones cliente** desde el blade Intune.

3. Seleccione el elemento **Directivas de configuración** de aplicaciones en el blade Aplicaciones cliente y haga clic en **Agregar** para abrir el blade **Agregar directiva de configuración**.

4. Escriba un nombre para la directiva y agregue una descripción para ella.

5. En **Tipo de inscripción de dispositivos**, seleccione **Dispositivos administrados**.

6. En **Plataforma**, selecciona **Android**.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Esto agrega otra opción de configuración para la aplicación asociada.

7. Haga clic en **Aplicación asociada** y seleccione la aplicación **Citrix SSO**.

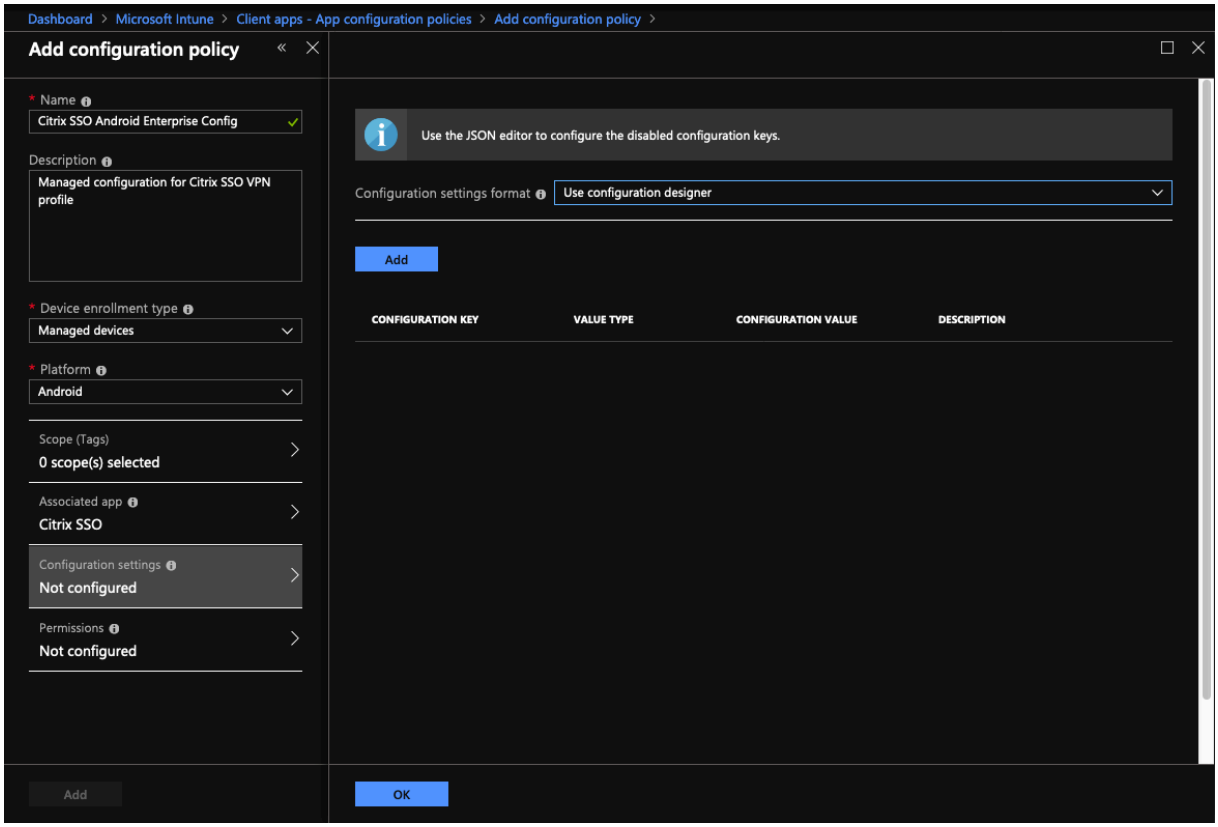
Es posible que tengas que buscarlo si tienes muchas aplicaciones.

8. Haga clic en **Aceptar**. Se agrega una opción de configuración en el blade Agregar directiva de configuración.

9. Haga clic en **Configuración**.

Aparecerá un blade para configurar la aplicación Citrix SSO.

10. En **Configuración de configuración**, seleccione **Usar diseñador de configuración**o **Introducir datos JSON**para configurar la aplicación Citrix SSO.



Nota: Para configuraciones VPN simples, se recomienda usar el diseñador de configuración.

Configuración de VPN mediante el diseñador de configuración de usuario

1. En **Configuración de configuración**, seleccione **Usar diseñador de configuración** y haga clic en **Agregar**.

Se le presenta una pantalla de entrada de valor clave para configurar varias propiedades compatibles con la aplicación Citrix SSO. Como mínimo, debe configurar las propiedades **Dirección del servidor**

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

y **Nombre del perfil de VPN**. Puede pasar el cursor sobre la sección **DESCRIPCIÓN** para obtener más información sobre cada propiedad.

2. Por ejemplo, seleccione las propiedades **Nombre del perfil VPN** y **Dirección del servidor (*)** y haga clic en **Aceptar**.

Esto agrega las propiedades al diseñador de configuración. Puede configurar las siguientes propiedades.

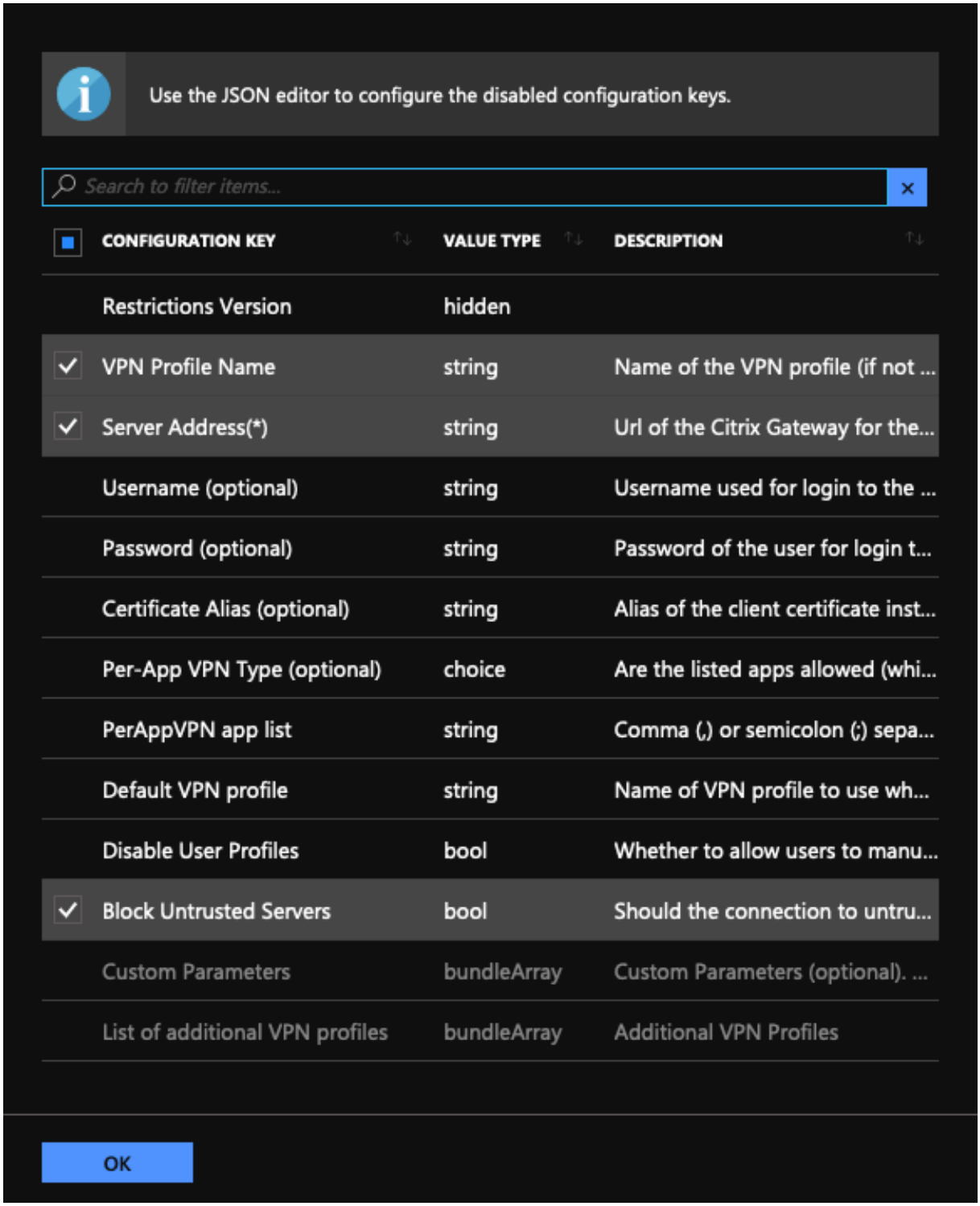
- **Nombre del perfil de VPN**. Escriba un nombre para el perfil VPN. Si va a crear más de un perfil VPN, utilice un nombre único para cada perfil. Si no proporciona un nombre, la dirección que introduzca en el campo Dirección del servidor se utilizará como nombre del perfil VPN.
- **Dirección del servidor (*)**. Escriba el FQDN base de Citrix Gateway. Si el puerto de Citrix Gateway no es 443, escriba también el puerto. Utilice un formato de URL. Por ejemplo, `https://vpn.mycompany.com:8443`.
- **Nombre de usuario (opcional)**. Introduzca el nombre de usuario que los usuarios finales utilizan para autenticarse en Citrix Gateway. Puede usar el token de valor de configuración de Intune para este campo si la Gateway está configurada para usarlo (consulte tokens de valor de configuración). Si no proporciona un nombre de usuario, se pedirá a los usuarios que proporcionen un nombre de usuario cuando se conecten a Citrix Gateway.
- **Contraseña (opcional)**. Introduzca la contraseña que los usuarios finales utilizan para autenticarse en Citrix Gateway. Si no proporciona una contraseña, se pedirá a los usuarios que proporcionen una contraseña cuando se conecten a Citrix Gateway.
- **Alias de certificado (opcional)**. Proporcione un alias de certificado en Android KeyStore que se utilizará para la autenticación de certificados del cliente. Este certificado está preseleccionado para los usuarios si utiliza autenticación basada en certificados.
- **Tipo de VPN por aplicación (opcional)**. Si utiliza VPN por aplicación para restringir las aplicaciones que usan esta VPN, puede configurar este parámetro.
  - Si selecciona **Permitir**, el tráfico de red para los nombres de paquetes de aplicaciones enumerados en la lista de aplicaciones PerAppVPN se enruta a través de la VPN. El tráfico de red de todas las demás aplicaciones se redirige fuera de la VPN.
  - Si selecciona No **permitir**, el tráfico de red para los nombres de paquetes de aplicaciones enumerados en la lista de aplicaciones PerAppVPN se enruta fuera de la VPN. El tráfico de red de todas las demás aplicaciones se redirige a través de la VPN. El valor predeterminado es Permitir.
- **Lista de aplicaciones PerAppVPN**. Una lista de aplicaciones cuyo tráfico está permitido o no permitido en la VPN, en función del valor de Tipo de VPN por aplicación. Indique los nombres de los paquetes de aplicaciones separados por comas o puntos y comas. Los nombres de los paquetes de aplicaciones distinguen entre mayúsculas y minúsculas y deben estar escritos en

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

esta lista tal y como lo están en la almacén de Google Play. Esta lista es opcional. Mantenga esta lista vacía para aprovisionar la VPN en todo el dispositivo.

- **Perfil VPN predeterminado**. Nombre del perfil VPN utilizado cuando Always-On VPN está configurado para la aplicación Citrix SSO. Si este campo está vacío, el perfil principal se utiliza para la conexión. Si solo se configura un perfil, se marca como perfil VPN predeterminado.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



Nota:

- Para convertir la aplicación Citrix SSO como aplicación VPN Always-On en Intune, utilice el proveedor VPN como personalizado y com.citrix.citrixVPN como nombre del paquete de la

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

> aplicación.
>
> - Solo la autenticación de cliente basada en certificados es compatible con la aplicación Citrix SSO Always-On VPN.
> - Los administradores deben seleccionar **Autenticación** de **cliente y establecer Certificado** de cliente como **Obligatorio** en el **Perfil SSLo Propiedades SSL** en Citrix Gateway para que la aplicación SSO funcione según lo previsto.

- **Inhabilitar perfiles de usuario**
  - Si establece este valor en true, los usuarios no pueden agregar nuevos perfiles VPN en sus dispositivos.
  - Si establece este valor en false, los usuarios pueden agregar sus propias VPN en sus dispositivos.

  El valor predeterminado es false.
- **Bloquear servidores que no son de confianza**
  - Establezca este valor en false cuando utilice un certificado autofirmado para Citrix Gateway o cuando el certificado raíz de la CA que emite el certificado de Citrix Gateway no esté en la lista de CA del sistema.
  - Establezca este valor en true para habilitar el sistema operativo Android para validar el certificado de Citrix Gateway. Si se produce un error en la validación, no se permite la conexión.

  El valor predeterminado es true.

3. Para la propiedad **Dirección del servidor(*)**, introduzca la dirección URL base de la VPN de Gateway (por ejemplo, `https://vpn.mycompany.com`).

4. En **Nombre de perfil de VPN**, escriba un nombre visible para el usuario final en la pantalla principal de la aplicación Citrix SSO (por ejemplo, Mi VPN corporativa).

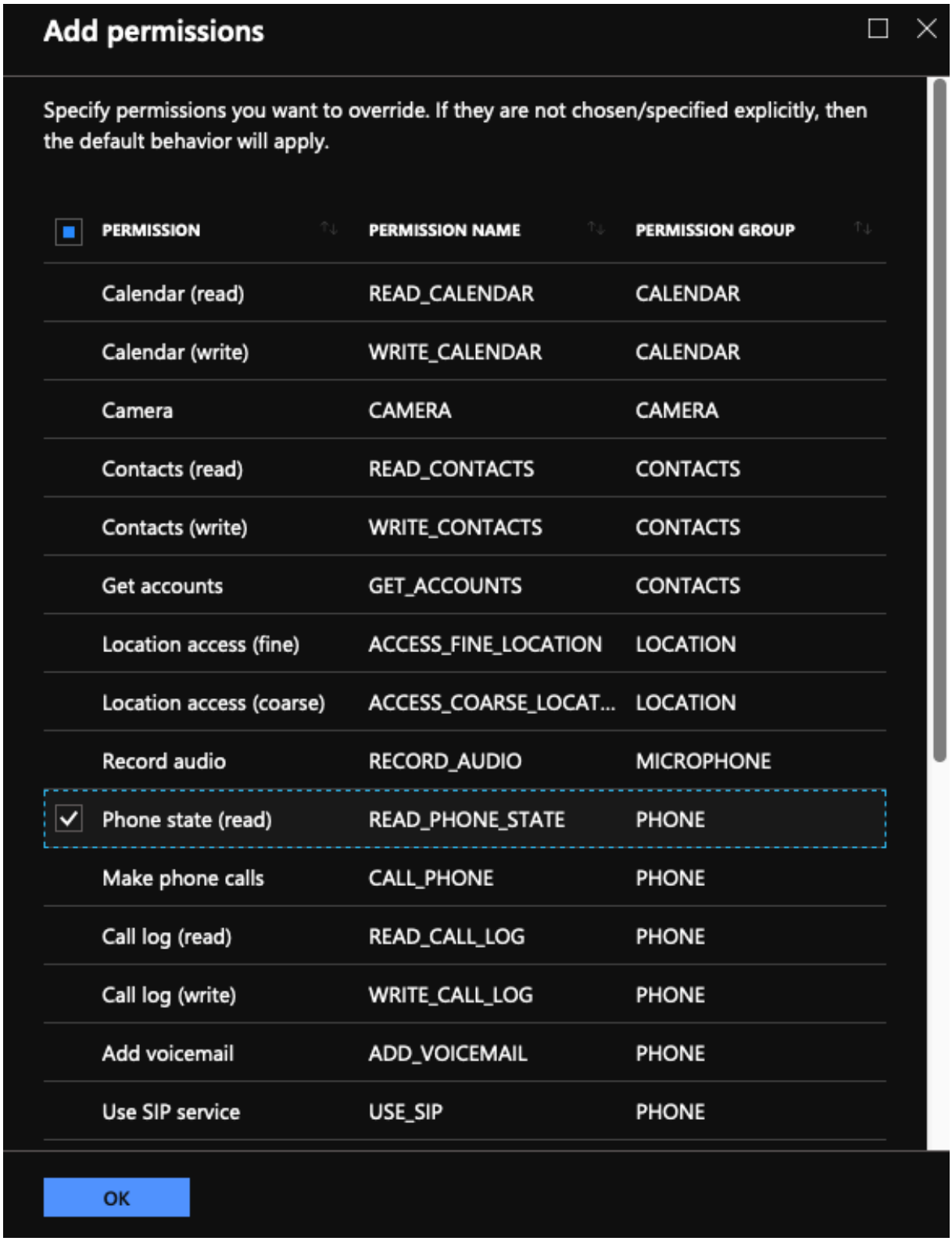
5. Puede agregar y configurar otras propiedades según corresponda a su implementación de Citrix Gateway. Haga clic en **Aceptar** cuando haya terminado con la configuración.

6. Haga clic en la sección **Permisos**. En esta sección, puede conceder los permisos requeridos por la aplicación Citrix SSO.

- Si está utilizando la comprobación de Intune NAC, la aplicación Citrix SSO requiere que conceda permiso **(lectura) del estado del teléfono**. Haga clic en el botón **Agregar** para abrir la hoja de permisos. Actualmente, Intune muestra una lista significativa de permisos disponibles para todas las aplicaciones.
- Si está utilizando la comprobación de Intune NAC, seleccione el permiso **Estado del teléfono (lectura)** y haga clic en **Aceptar**. Esto lo agrega a la lista de permisos para la aplicación. Selec-

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

cione **Solicitar** o **Conceder automáticamente** para que la comprobación de Intune NAC pueda funcionar y haga clic en **Aceptar**.



© 1999–2023 Cloud Software Group, Inc. All rights reserved.

7. Haga clic en **Agregar** en la parte inferior de la hoja de directivas de configuración de aplicaciones para guardar la configuración administrada para la aplicación Citrix SSO.

8. Haga clic en **Asignaciones** en el blade de directiva de configuración de aplicaciones para abrir el blade **Asignaciones**.

9. Seleccione los grupos de usuarios para los que quiere que se entregue y aplique esta configuración de Citrix SSO.

Configuración de VPN mediante la introducción de datos JSON

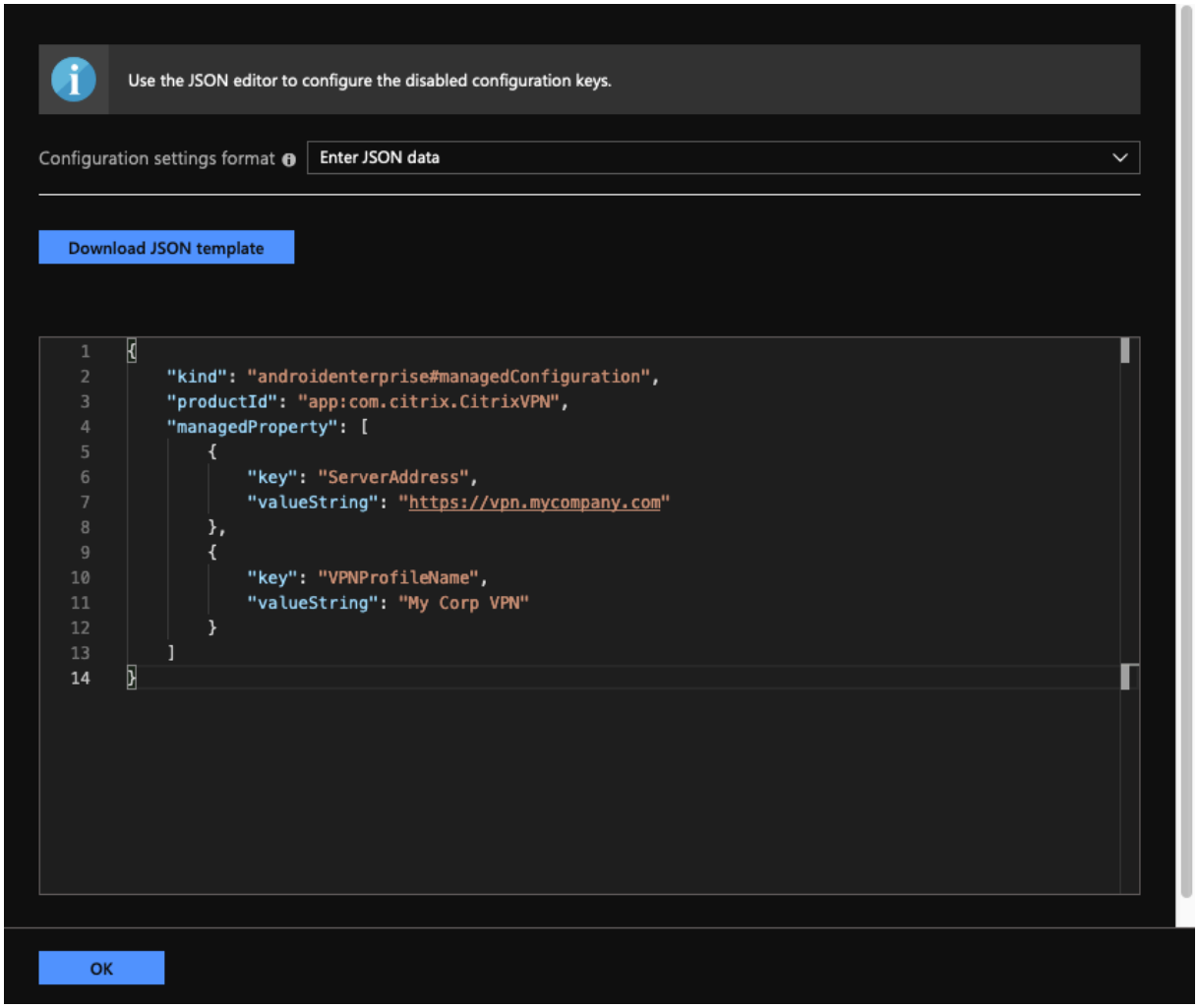
1. En **Configuración**, seleccione **Introducir datos JSON**para configurar la aplicación Citrix SSO.

2. Utilice el botón Descargar plantilla JSON para descargar una plantilla que permita proporcionar una configuración más detallada/compleja para la aplicación Citrix SSO. Esta plantilla es un conjunto de pares clave-valor JSON para configurar todas las posibles propiedades que la aplicación Citrix SSO entiende.

Para obtener una lista de todas las propiedades disponibles que se pueden configurar, consulte Propiedades disponibles para configurar el perfil VPN en la aplicación Citrix SSO.

3. Una vez creado un archivo de configuración JSON, copie y pegue su contenido en el área de edición. Por ejemplo, a continuación se muestra la plantilla JSON para la configuración básica creada anteriormente mediante la opción de diseñador de configuración.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.



Esto completa el procedimiento para configurar e implementar perfiles VPN para la aplicación Citrix SSO en el entorno Microsoft Intune Android Enterprise.

Importante: El certificado utilizado para la autenticación basada en certificados de cliente generalmente se implementa mediante el perfil SCEP de Intune. El alias de este certificado debe configurarse en la propiedad **Alias de certificado** de la configuración administrada para la aplicación Citrix SSO.

Propiedades disponibles para configurar el perfil VPN en la aplicación Citrix SSO

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Clave de configuración	Nombre de campo JSON	Tipo de valor	Descripción
Nombre del perfil VPN	VPNProfileName	Texto	Nombre del perfil VPN (si no se establece la dirección predeterminada del servidor).
Dirección del servidor(*)	ServerAddress	dirección URL	URL base de Citrix Gateway para la conexión (https://host%5B:port%5D). Este campo es obligatorio.
Nombre de usuario (opcional)	Nombre de usuario	Texto	Nombre de usuario utilizado para autenticar con Citrix Gateway (opcional).
Contraseña (opcional)	Contraseña	Texto	Contraseña del usuario para autenticarse con Citrix Gateway (opcional).
Alias de certificado (opcional)	Alias de certificado de cliente	Texto	Alias del certificado de cliente instalado en el almacén de credenciales de Android para su uso en la autenticación de cliente basada en certificados (opcional).

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Clave de configuración	Nombre de campo JSON	Tipo de valor	Descripción
Tipo de VPN por aplicación (opcional)	PerAppVPN_Allow_Disallow_Setting	Enum (Permitir, No permitir)	¿Se permiten las aplicaciones enumeradas (lista blanca) o no (lista negra) para usar el túnel VPN? Si se establece en **Permitir**, solo las aplicaciones enumeradas (en la propiedad de lista de aplicaciones PerAppVPN) pueden túnel a través de la VPN. Si se establece en **No permitir**, todas las aplicaciones excepto las enumeradas pueden túnel a través de la VPN. Si no aparece ninguna aplicación, todas las aplicaciones pueden túnel a través de la VPN.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Clave de configuración	Nombre de campo JSON	Tipo de valor	Descripción
Lista de aplicaciones de Per App VPN	Nombre_APP_APPNam	Texto	Lista separada por comas (,) o punto y coma (;) de nombres de paquetes de aplicaciones para VPN por aplicación. Los nombres de los paquetes deben ser exactamente los mismos que aparecen en la URL de la página de lista de aplicaciones de Google Play Store. Los nombres de los paquetes distinguen entre mayúsculas y minúsculas.
Perfil VPN predeterminado	DefaultProfileName	Texto	Nombre del perfil VPN que se va a utilizar cuando el sistema inicia el servicio VPN. Esta configuración se utiliza para identificar el perfil VPN que se va a utilizar cuando la VPN Always-On está configurada en el dispositivo.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Clave de configuración	Nombre de campo JSON	Tipo de valor	Descripción
Inhabilitar perfiles de usuario	Inhabilitar Perfiles de usuario	Booleano	Propiedad para permitir o no permitir que los usuarios finales creen manualmente perfiles VPN. Establezca este valor en **true** para inhabilitar a los usuarios de la creación de perfiles VPN. El valor predeterminado es **false.**
Bloquear servidores que no son de confianza	BlockUntrustedServers	Booleano	Propiedad para determinar si la conexión a puertas de enlace que no son de confianza (por ejemplo, el uso de certificados autofirmados o al emitir CA no es de confianza para el sistema operativo Android) se bloquea? El valor predeterminado es true (bloquear conexiones a puertas de enlace que no sean de confianza).

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Clave de configuración	Nombre de campo JSON	Tipo de valor	Descripción
Parámetros personalizados (opcional)	Parámetros personalizados	Lista	Lista de parámetros personalizados (opcional) compatibles con la aplicación Citrix SSO. Para obtener más información, consulte Parámetros personalizados. Consulte la documentación de Citrix Gateway para ver las opciones disponibles.
Lista de perfiles VPN adicionales	bundle_profiles	Lista	Lista de perfiles VPN adicionales. La mayoría de los valores mencionados anteriormente para cada perfil son compatibles. Para obtener información detallada, consulte Lista de propiedades admitidas.

Parámetros personalizados

Cada parámetro personalizado debe definirse mediante los siguientes nombres clave-valor.

Clave	Tipo de valor	Valor
ParameterName	Texto	Nombre del parámetro personalizado.
Valor del parámetro	Texto	Valor del parámetro personalizado.

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

Propiedades admitidas para cada VPN en la lista de perfiles VPN

Las siguientes propiedades se admiten para cada uno de los perfiles VPN cuando se configuran varios perfiles VPN mediante la plantilla JSON.

Clave de configuración	Nombre de campo JSON	Tipo de valor
Nombre del perfil VPN	nombre_VPNProfileBundle_	Texto
Dirección del servidor(*)	Bundle_ServerAddress	dirección URL
Nombre de usuario	nombre_de_usuario	Texto
Contraseña	Contraseña de paquete	Texto
Alias de certificado de cliente	Clientes_Bundle_Clientes_Lias	Texto
Tipo de VPN por aplicación	bundle_perappvpn_allow_disallow_setting	Enumeración (Permitir, No permitir)
Lista de aplicaciones de Per App VPN	bundle_perappvpn_appNames	Texto
Parámetros personalizados	Bundle_CustomParameters	Lista

© 1999–2023 Cloud Software Group, Inc. All rights reserved.

citrix

Locations
Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States

© 2023 Cloud Software Group, Inc. All rights reserved. Cloud Software Group, the Cloud Software Group logo, and other marks appearing herein are property of Cloud Software Group, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).