

Ejemplo de Configuración de ASA Clientless Access con el Uso de Citrix Receiver en Dispositivos Móviles

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Dispositivos móviles compatibles](#)

[Demostración](#)

[Antecedentes](#)

[Limitaciones](#)

[Configurar](#)

[Comandos CLI](#)

[Ejemplo de configuración](#)

[Configuración de Adaptive Security Device Manager \(ASDM\)](#)

[Certificados de identidad ASA y autoridades certificadoras \(CA\)](#)

[Interfaz de usuario final/Experiencia de usuario](#)

[Agregar una nueva cuenta](#)

[Cierre de sesión de WebVPN](#)

[Verificación](#)

[Troubleshoot](#)

[Depuraciones](#)

[Preguntas frecuentes \(FAQ\)](#)

Introducción

Este documento describe cómo configurar Cisco Adaptive Security Appliance (ASA) como proxy para Citrix Receiver en dispositivos móviles. Esta función proporciona acceso remoto seguro para la aplicación Citrix Receiver que se ejecuta en dispositivos móviles a servidores de infraestructura de escritorio virtual (VDI) XenApp/XenDesktop a través de ASA, lo que elimina la necesidad de la puerta de enlace de acceso Citrix.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Citrix Reciever
- WebVPN sin cliente

Requisitos de la infraestructura:

- El ASA debe tener un certificado de identidad válido de confianza para los dispositivos móviles.
- La interfaz XML debe estar habilitada y configurada en el servidor Citrix XenApp/XenDesktop/Storefront.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Dispositivos móviles compatibles

Esta es una lista de los dispositivos móviles compatibles:

- iPad - Citrix Receiver versión 4.x o posterior
- iPhone/iTouch - Citrix Receiver versión 4.x o posterior
- Teléfono Android 2.x - Citrix Receiver Versión 2.x o posterior
- Tablet Android 3.x - Citrix Receiver versión 2.x o posterior
- Teléfono/Tablet Android 4.0/4.1 - Citrix Receiver Versión 2.x o posterior

Demostración

Para ver una demostración de este proceso, visite la siguiente página web:

[Demostración del proxy de Citrix Mobile Receiver de Cisco ASA 9.0](#)

Antecedentes

La puerta de enlace Citrix Access Gateway (CAG) era tradicionalmente la única forma de proporcionar acceso remoto seguro a los recursos virtualizados de Citrix (aplicaciones y escritorios). En una implementación típica, dicho dispositivo se ubicaría detrás del firewall en una zona desmilitarizada (DMZ). Esta función agrega funcionalidad ASA para soportar conexiones remotas seguras a recursos virtuales desde dispositivos móviles.

Las implementaciones tradicionales requieren la presencia de una CAG, que normalmente se encuentra detrás del firewall:



Con ASA, las conexiones a los recursos internos de Citrix son posibles sin la CAG:



Para que el ASA pueda realizar conexiones proxy desde un Citrix Receiver a un Citrix Server, el ASA se hace pasar por Citrix Access.

Gateway:

1. Al intentar conectarse a un recurso virtualizado de Citrix, no es necesario proporcionar la dirección o las credenciales del servidor Citrix; en su lugar, introduzca las credenciales y la dirección IP de VPN de Secure Sockets Layer (SSL) de ASA.
2. Se crea un nuevo controlador ASA para manejar las solicitudes, que incluye las solicitudes de autenticación de Citrix Receivers (solicitudes HTTPS con una cadena de agente que se identifica a sí misma como Citrix Receiver).
3. Después de que ASA haya verificado las credenciales, el cliente receptor comienza a recuperar las aplicaciones autorizadas a través del ASA. El ASA vuelve a escribir y envía los proxies a la interfaz de servicio XML de XenApp o XenDesktop Server (el servicio XML es un servicio que se ejecuta en un servidor Citrix que atiende las solicitudes relacionadas con los recursos de virtualización).

4. El ASA se conecta y autentica al servidor VDI con credenciales preconfiguradas (consulte la sección Configuración). Cuando envía las credenciales al servidor XenApp/XenDesktop de back-end, el ASA siempre confunde la contraseña de usuario con la codificación Citrix CTX1.

Esta es una lista de los métodos de autenticación ASA compatibles con Citrix Receiver:

- Local
- Dominio
- RSA SecurID con protocolo nativo SDI.
ASA también admite modos de desafío, que incluyen el siguiente token, el nuevo PIN y los modos PIN caducados.
- Autenticación de dos factores (RSA y protocolo ligero de acceso a directorios (LDAP))

Limitaciones

- Limitaciones de certificado:
La autenticación de certificado/tarjeta inteligente no se admite como método de inicio de sesión automático, ya que estos formularios de autenticación no permiten el ASA en el medio.

La firma Md5 en los certificados no funciona debido a un problema de seguridad y es un problema en las plataformas iOS. Se puede encontrar más información en el [Error del Receptor para iOS: Error de conexión. Citrix Receiver no pudo establecer la conexión con la conversación remota sobre el host.](#)

Si el nombre del asunto no coincide totalmente con el nombre de dominio completo (FQDN) de ASA, aunque el certificado de identidad de ASA contenga nombres alternativos de asunto (SAN), la sesión de la arquitectura informática independiente (ICA) no se iniciará (en función de la versión, se podría mostrar el error de certificado). Este problema ha sido corregido por el ID de bug de Cisco [CSCuj23632](#).

- El cliente Citrix Receiver sólo accede a un servidor XenApp/XenDesktop a la vez. Como resultado, los proxies de ASA también solicitan un XenApp/XenDesktop por sesión VPN. El ASA selecciona el primer XenApp/XenDesktop configurado cuando se conecta un cliente Citrix Receiver.
- No se admite la redirección HTTP, ya que la versión actual de la aplicación Citrix Receiver no funciona con redirecciones.
- Las verificaciones de certificados de cliente, la notificación de vencimiento de la contraseña, Cisco Secure Desktop (CSD) y todo lo que se incluye en CSD (no solo Secure Vault) no son compatibles cuando se utilizan clientes independientes/móviles, porque los clientes de infraestructura de virtualización independientes/móviles no entienden estos conceptos.

Configurar

Nota: Use la [Command Lookup Tool \(clientes registrados solamente\)](#) para obtener más información sobre los comandos usados en esta sección.

Comandos CLI

Cuando utiliza el cliente móvil Citrix Receiver para iniciar sesión en el ASA, el ASA debe conectarlo a un Citrix XenApp predefinido o a un servidor XenDesktop. Para ello, el administrador configura la dirección del servidor Citrix y las credenciales de inicio de sesión bajo la directiva de grupo o el nombre de usuario. En caso de que se configure el nombre de usuario y la CLI de política de grupo, la configuración del nombre de usuario tendrá prioridad sobre la política de grupo.

```
configure terminal
group-policy DfltGrpPolicy attributes
webvpn
[no] vdi { none | type <vdi_type>url domain username
password <password>}
```

```
configure terminal
username <username> attributes
webvpn
[no] vdi { none | type <vdi_type>url domain username
password <password>}
```

Nota:

tipo: tipo de VDI. Para Citrix Receiver, el tipo debe ser **citrix**.

url: URL completa del servidor XenApp o XenDesktop, que incluye HTTP o HTTPS, nombre de host, número de puerto, así como la ruta de acceso al servicio XML. El nombre de host y la ruta de acceso al servicio XML pueden contener una macro sin cliente. Si no se proporciona la ruta de acceso del servicio XML, se utiliza la ruta predeterminada de **/Citrix/pnagent/**.

username - nombre de usuario que se utiliza para iniciar sesión en el servidor de infraestructura de virtualización. Esta puede ser una macro sin cliente.

password: contraseña que se utiliza para iniciar sesión en el servidor de infraestructura de virtualización. Esta puede ser una macro sin cliente.

dominio: dominio que se utiliza para iniciar sesión en el servidor de infraestructura de virtualización. Esta puede ser una macro sin cliente.

Nota: Los servidores XenAPP generalmente se configuran para escuchar el puerto 80, por lo que la VDI se debe configurar con **HTTP** en lugar de **HTTPS**.

Los usuarios de Citrix Mobile Receiver pueden seleccionar el grupo de túnel mientras se autentican con el ASA. La selección del grupo de túnel permite el soporte de diferentes protocolos de autenticación y servidores XenApp/XenDesktop para el acceso VDI. Los administradores pueden configurar un grupo de túnel como el valor predeterminado para el acceso VDI. Este grupo de túnel configurado se utiliza cuando los usuarios no realizan una selección de grupo de túnel:

```
configure terminal
webvpn
```

[no] application-type default tunnel-group

- *application_name*: nombre de aplicación. La única aplicación actualmente soportada es **citrix-receive**.
- *tunnel-group-name*: nombre del grupo de túnel actual que se utilizará como valor predeterminado para el acceso VDI del tipo especificado.

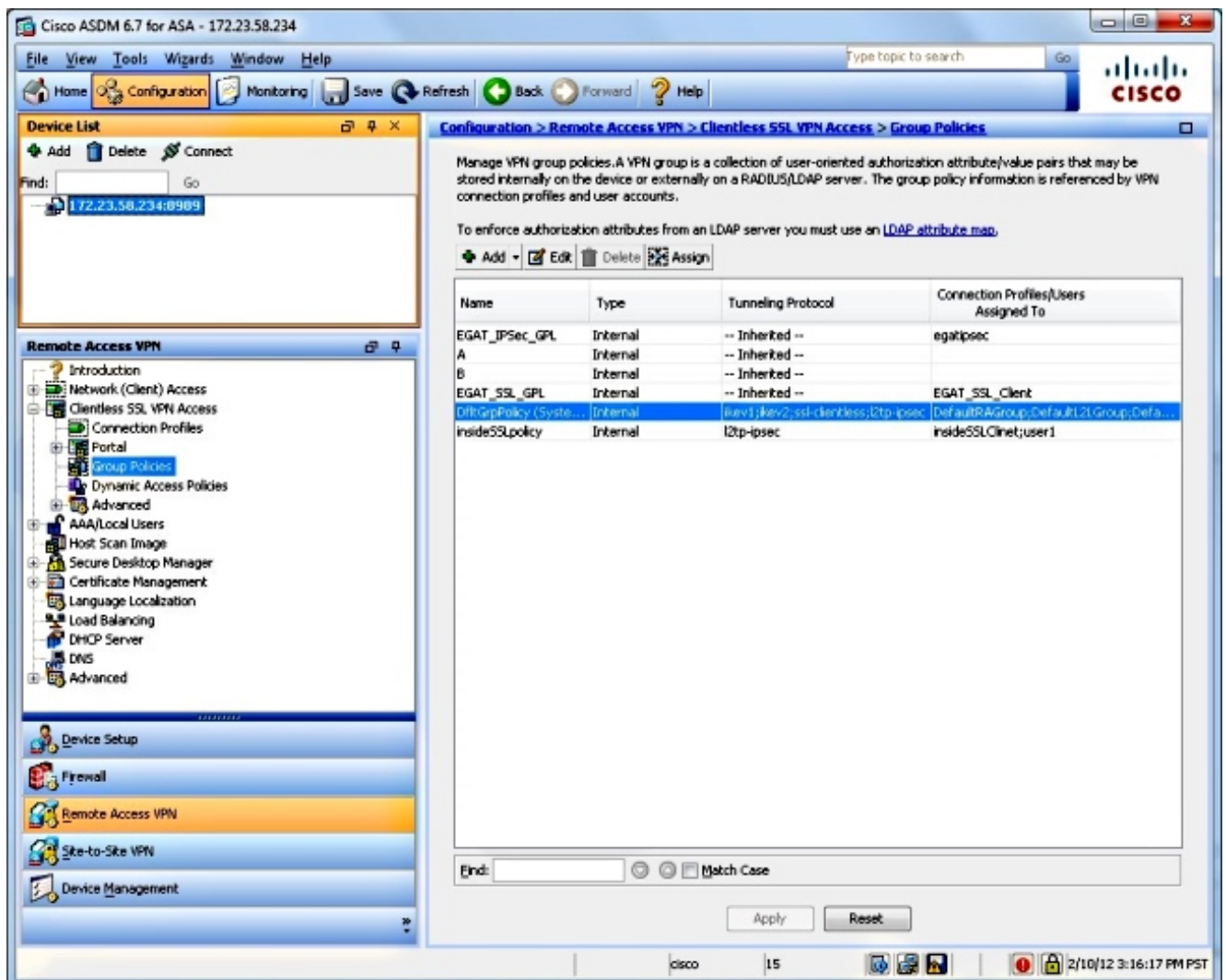
Ejemplo de configuración

Estos son ejemplos de configuración de VDI válidos:

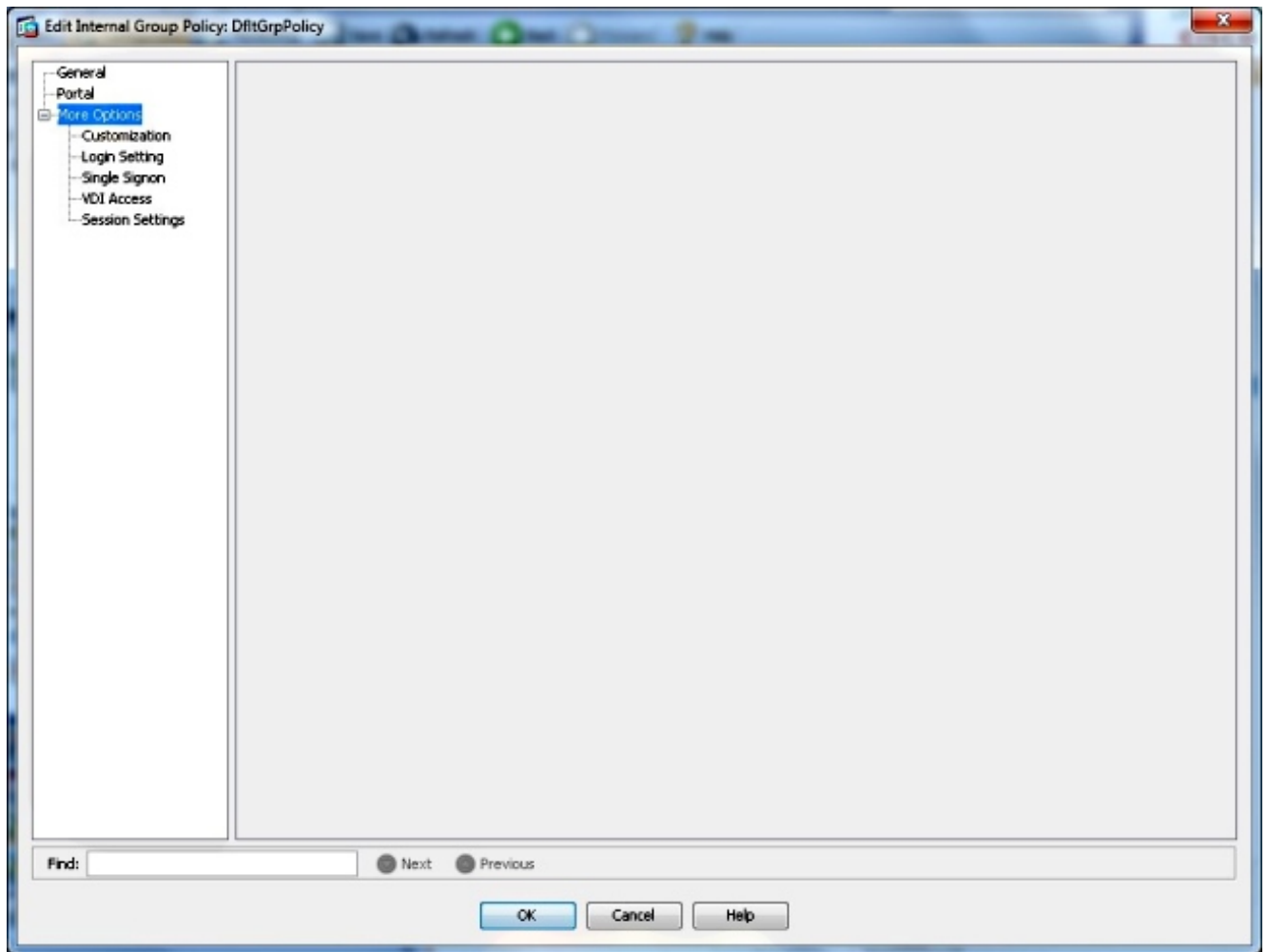
```
vdi type citrix url http://192.168.1.2 domain domain1 username user1 password pass1
vdi type citrix url https://192.168.1.2/Citrix/pnagent1/ domain domain2 username
username2 password password2
vdi type citrix url http://192.168.1.2:8080/Citrix/pnagent3 domain CSCO_WEBVPN_MACRO1
username CSCO_WEBVPN_USERNAME password CSCO_WEBVPN_PASSWORD
```

Configuración de Adaptive Security Device Manager (ASDM)

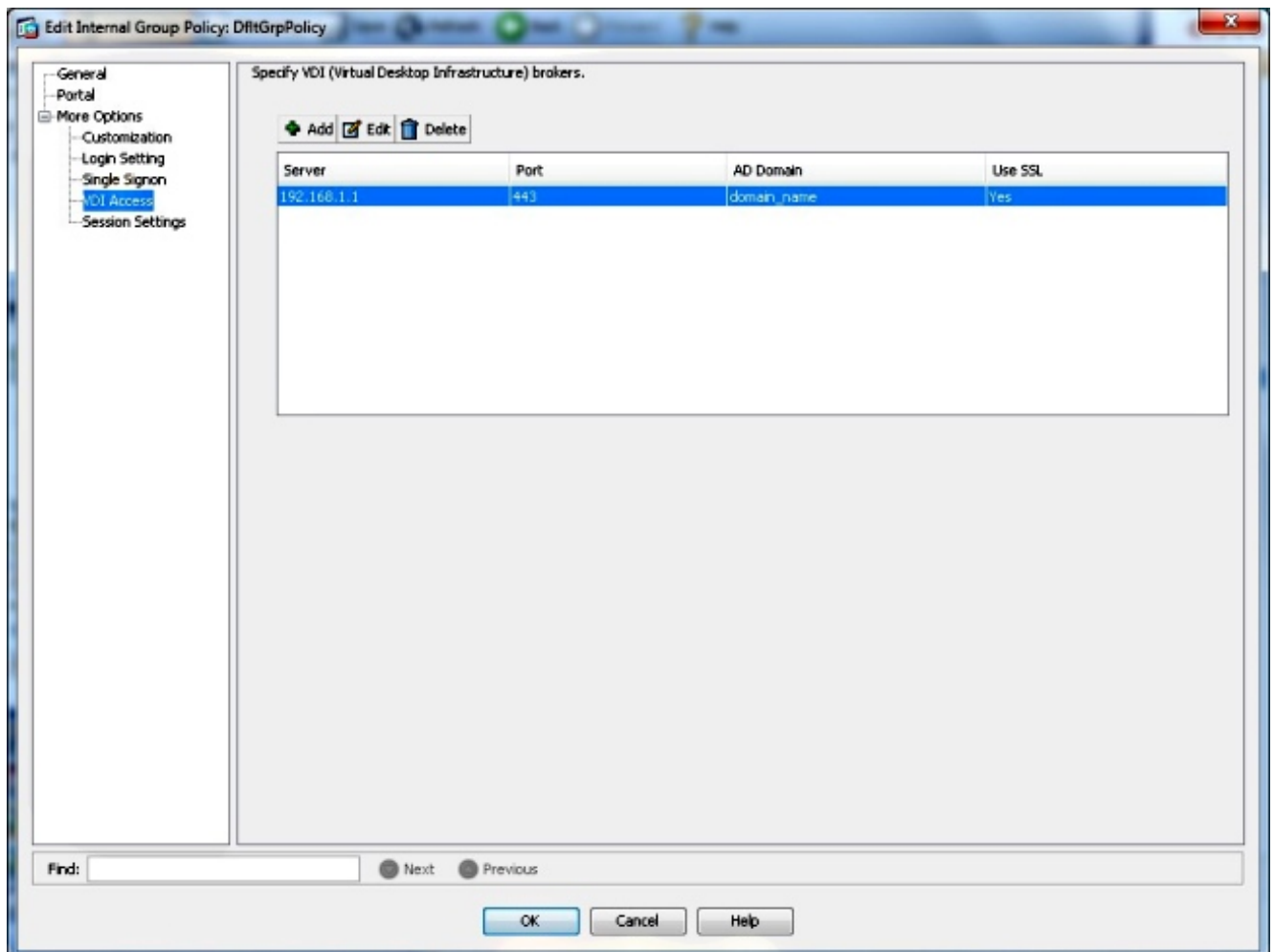
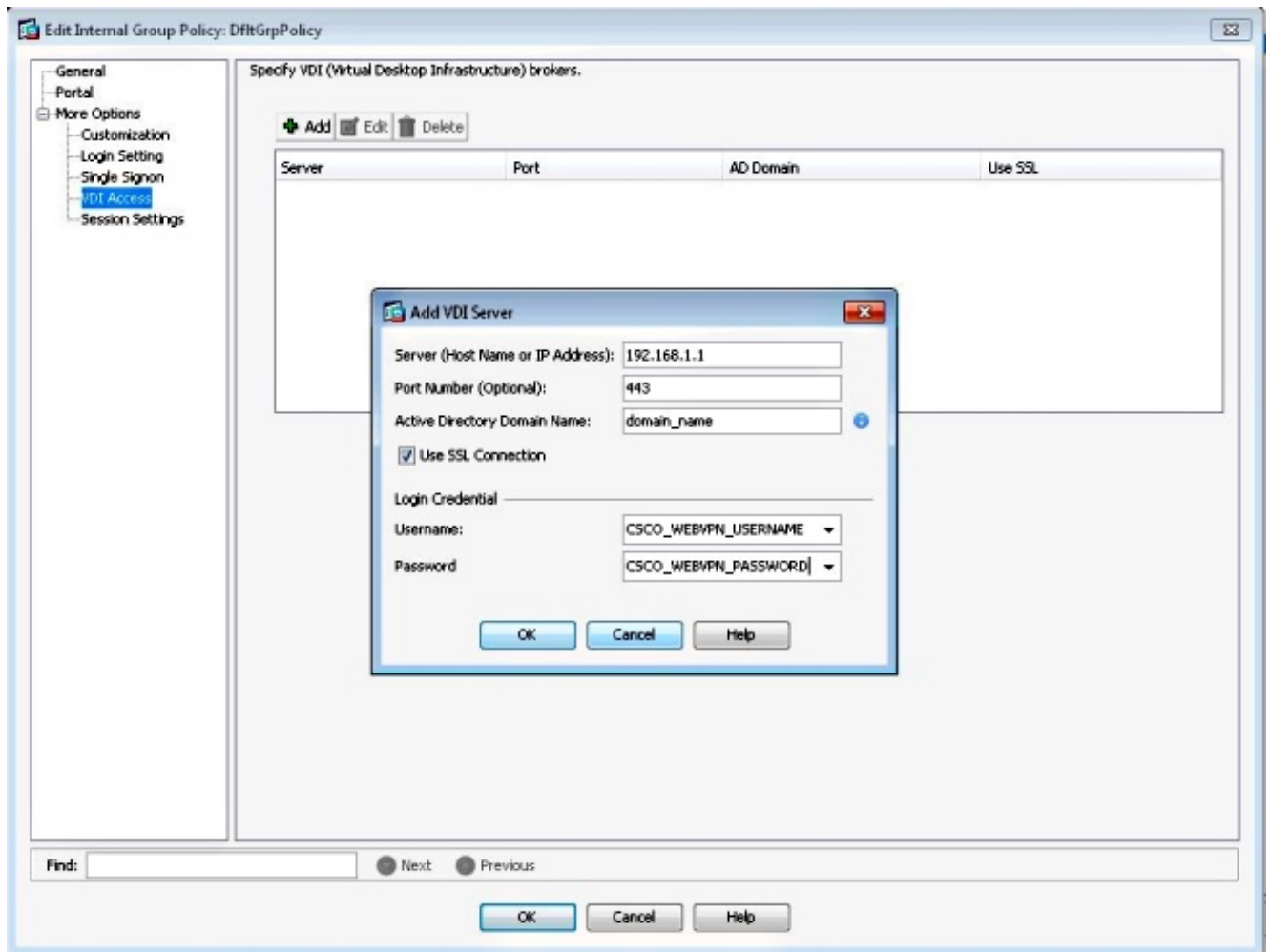
1. Vaya a **Asdm > Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policy**:



2. Vaya a **Edit > More Options > VDI Access**:



3. Agregue el **servidor VDI**:



Nota: El único modo admitido es el modo único.

Certificados de identidad ASA y autoridades certificadoras (CA)

- Para que Citrix Receiver funcione con el ASA, **los dispositivos móviles deben confiar en la CA que emitió el certificado de identidad del ASA. El certificado de ASA se debe emitir para un nombre de dominio completo** (por ejemplo, clientlessvdi.cisco.com) y NO para la dirección IP del ASA. Si el certificado de ASA ha sido emitido por una CA intermedia que no está presente en el almacén de claves del dispositivo móvil, la CA intermedia también debe ser de confianza.
- Cuando Citrix Receiver se conecta al ASA con un certificado no fiable, se le solicita al usuario advertencias emergentes sobre si debe continuar o no.
- Los dispositivos Apple que ejecutan iOS pueden admitir certificados ASA autofirmados, ya que admiten la importación directa de certificados y CA.
- En los dispositivos móviles Apple que ejecutan iOS, el receptor permite la conexión al ASA y la recuperación de la lista de aplicaciones, si se ignoran las advertencias del certificado. Sin embargo, es posible que el usuario no pueda iniciar ninguno de los recursos publicados hasta que se instale un certificado ASA válido.
- Algunos de los dispositivos móviles de sistemas operativos (SO) antiguos de Android no ofrecen ninguna forma legítima de importar certificados de terceros en el almacén de claves. Por lo tanto, para que un Receptor Citrix en dichos dispositivos Android funcione con el ASA/CAG, el ASA debe tener un certificado de identidad emitido por la CA que se ha incrustado en el almacén de claves, por ejemplo, Verisign o GoDaddy.
- En los dispositivos móviles Android, Citrix Receiver no permite conexiones al ASA si el certificado del ASA no está presente en el almacén de claves del dispositivo.
- Los dispositivos Android con OS versión 4.1 y posteriores admiten la importación de certificados y CA y deben funcionar como se describe anteriormente con iOS.

Interfaz de usuario final/Experiencia de usuario

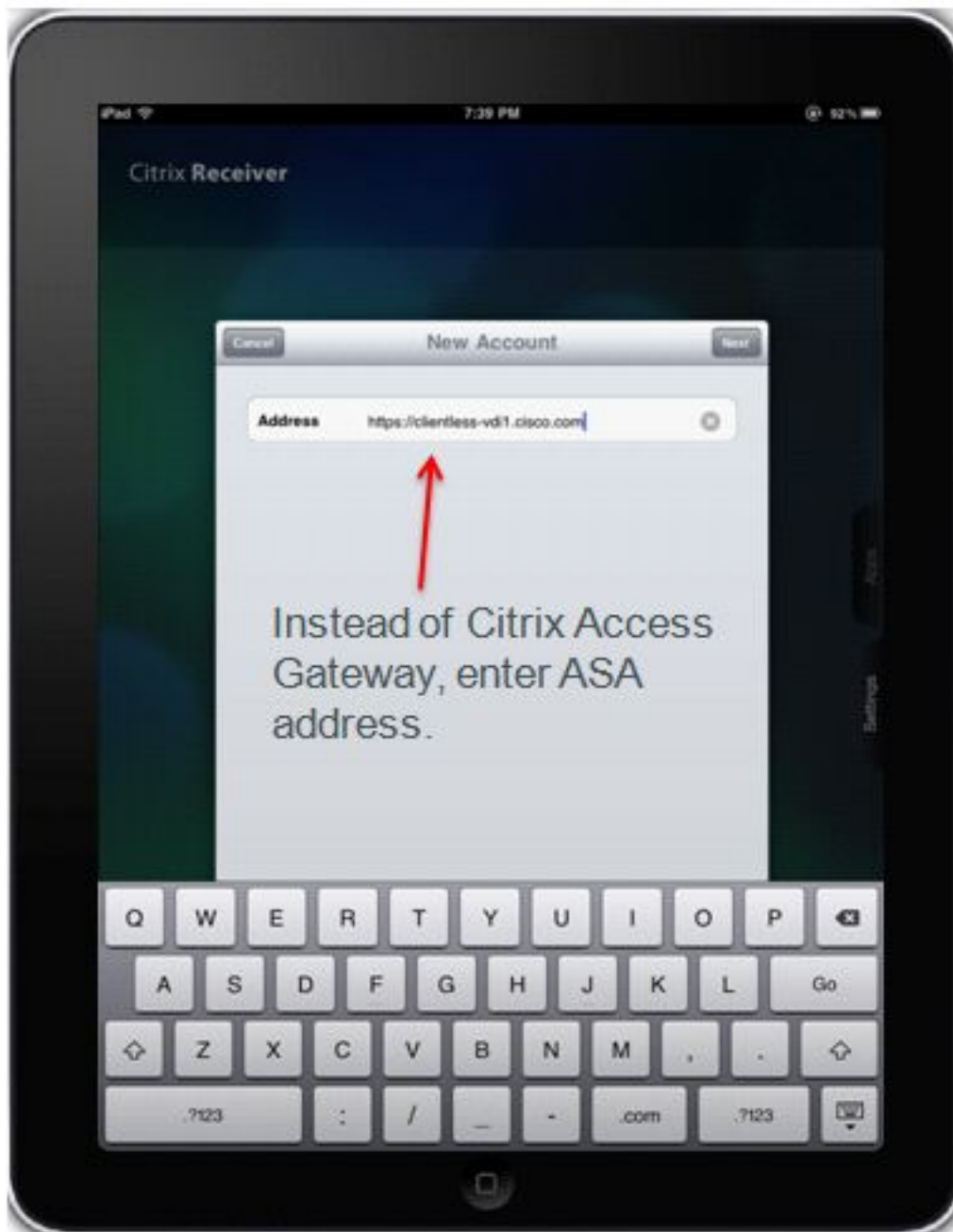
Agregar una nueva cuenta

El uso de Citrix Receiver para acceder a los recursos virtuales a través del ASA proporciona la misma experiencia de usuario que cuando se utiliza un gateway de acceso Citrix.

Si no hay servidores configurados, debe configurar un nuevo recurso virtual.



Proporcione el FQDN/dirección IP del ASA:



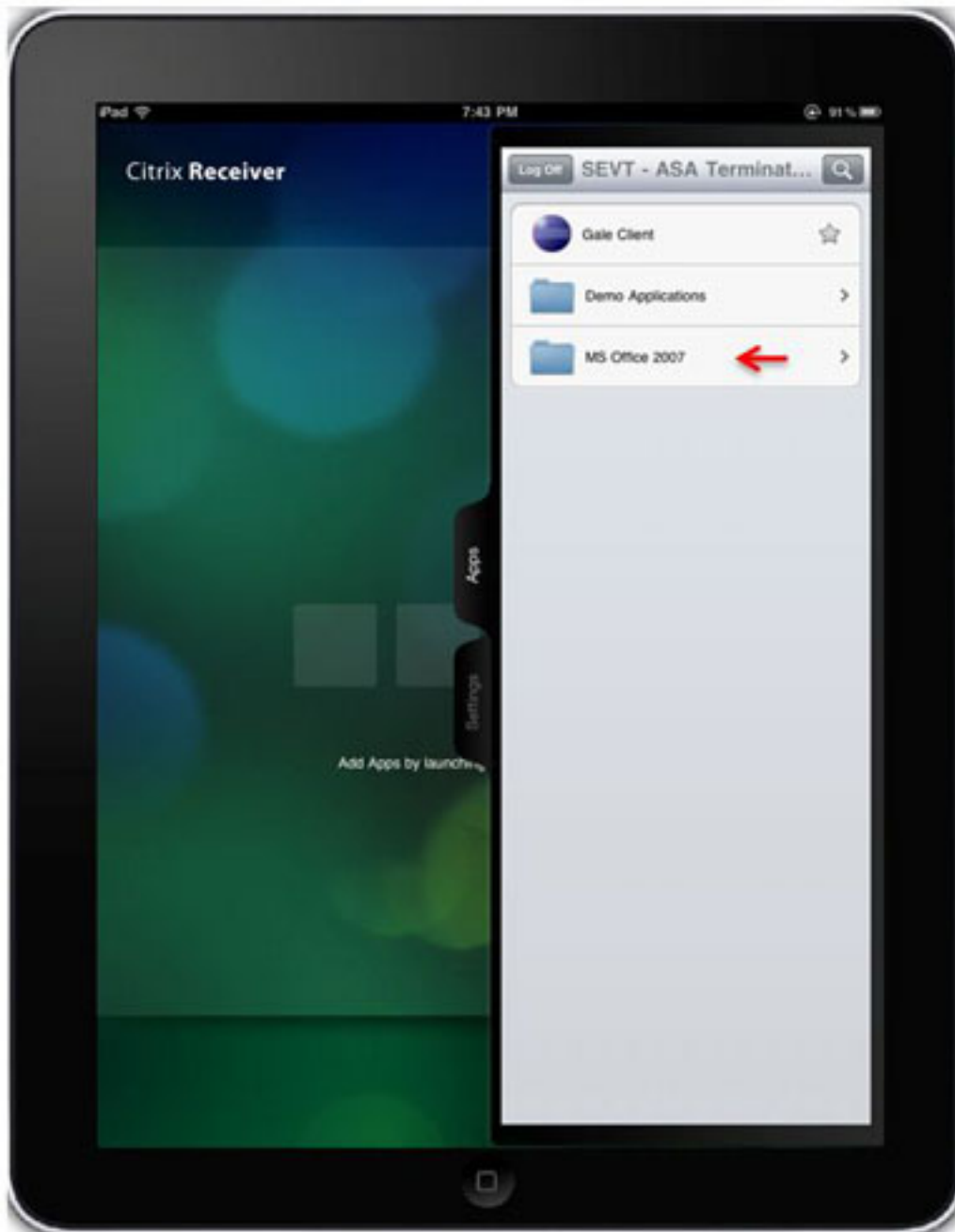
Verifique el **Access Gateway, Standard Edition**, e ingrese las credenciales para conectarse al ASA.



Cuando se guarda el perfil de usuario, la aplicación solicita automáticamente las credenciales (ASA) e intenta iniciar sesión.

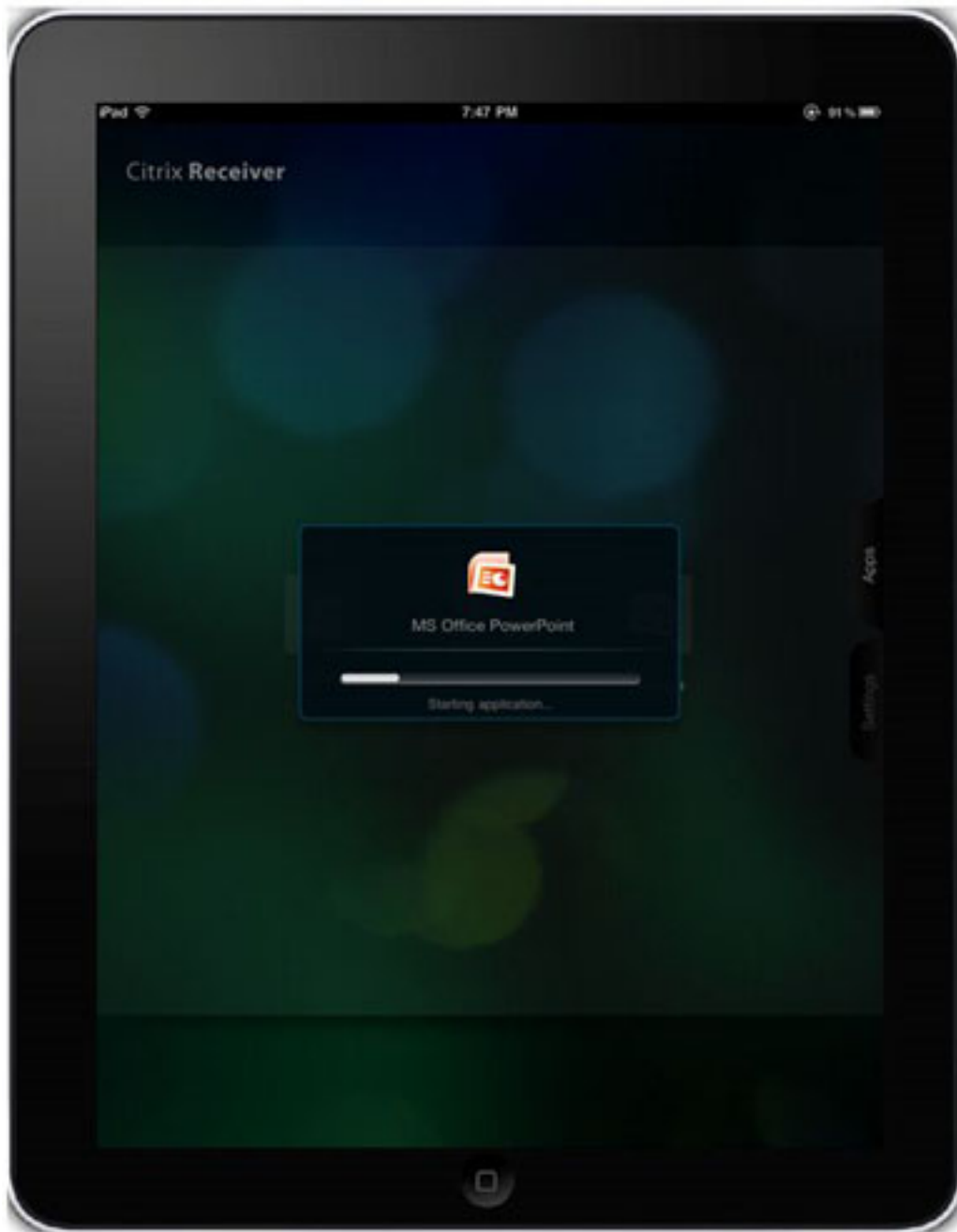


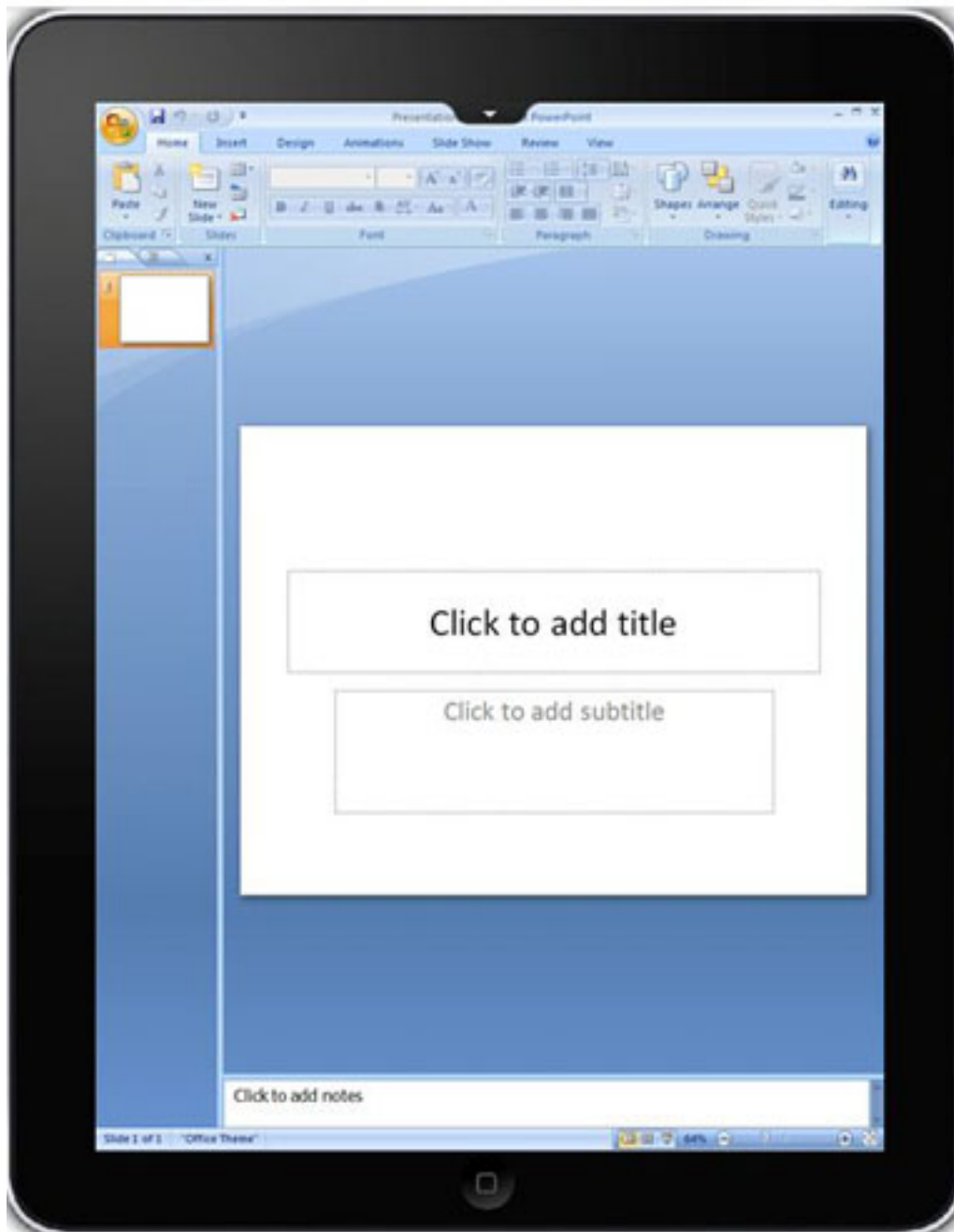
Cuando se inicia sesión, la aplicación muestra una lista de recursos publicados.



Puede navegar por las carpetas y hacer clic en un recurso para iniciarlo.







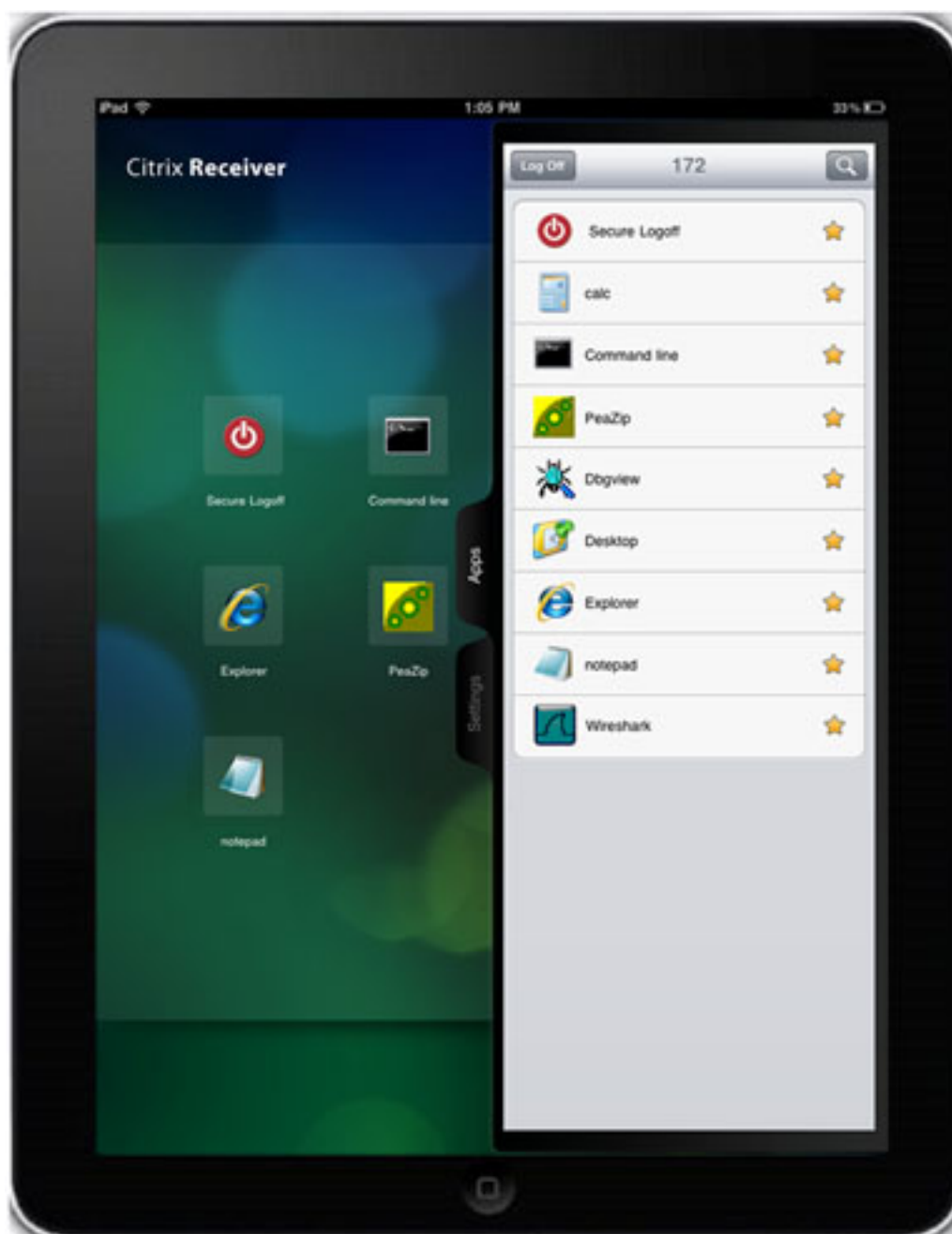
Cierre de sesión de WebVPN

La aplicación Citrix Receiver no proporciona la capacidad de finalizar una sesión WebVPN con un ASA o CAG conectado a voluntad. Normalmente, dicha sesión termina cuando alcanza el tiempo de espera configurado. Aunque la versión más reciente de Citrix Receiver tiene un nuevo botón **Log Off**, no finaliza la sesión actual con el ASA. En su lugar, cierra todas las aplicaciones abiertas y muestra la lista de servidores configurados. Por lo tanto, si ASA está configurado para utilizar solamente una licencia por usuario, los clientes que utilizan el botón **Cerrar sesión** no pueden volver a iniciar sesión hasta después de que la sesión se agote.

Para permitir que los usuarios finales terminen la sesión WebVPN a voluntad y, como resultado, liberen la licencia ASA, se ha agregado nueva funcionalidad para insertar el recurso **Secure Logoff**.



Esta inyección se produce cada vez que Citrix Receiver obtiene la lista de recursos publicados.

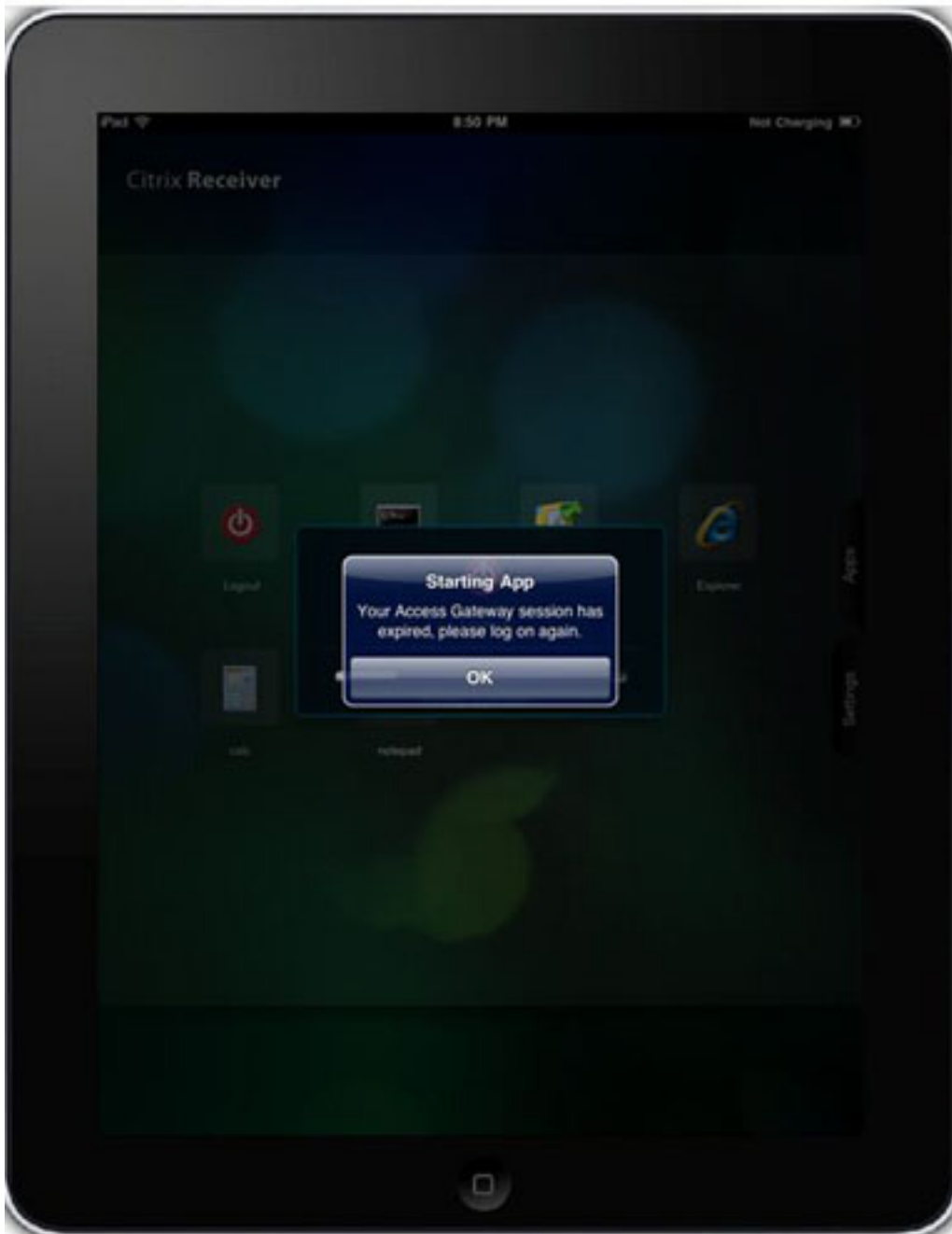


Cuando hace clic en la aplicación **Conexión segura**, finaliza la sesión entre el ASA y el receptor

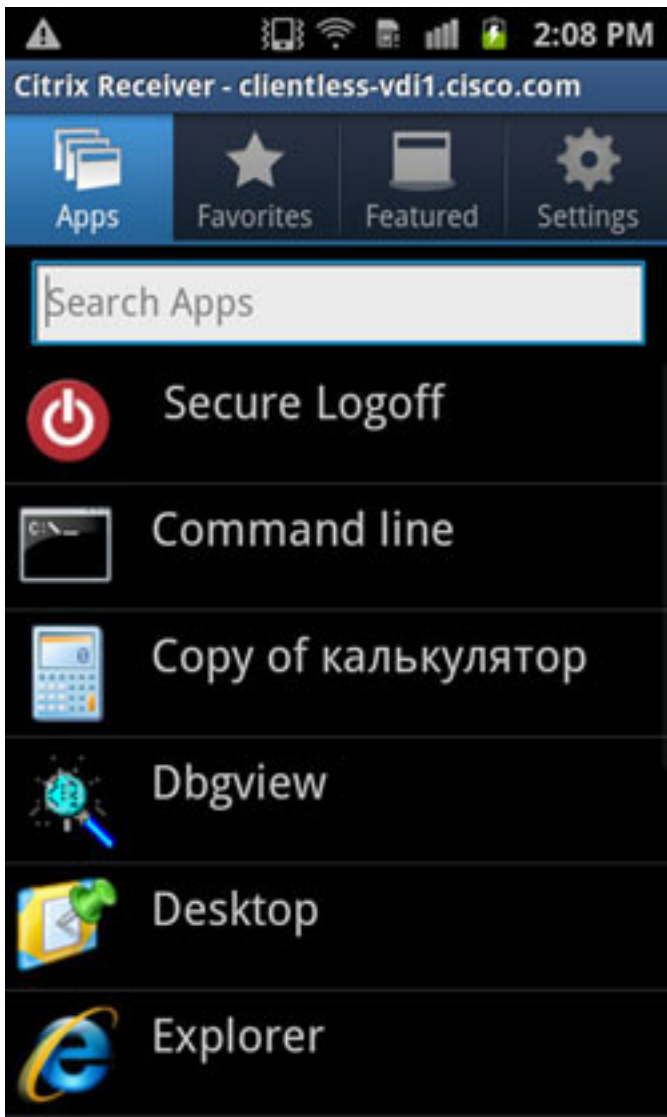
Citrix. Para liberar correctamente la licencia ASA, el recurso **de cierre de sesión seguro** debe utilizarse para terminar la sesión WebVPN en lugar del botón nativo de cierre de sesión de Citrix Receiver.

Se muestran diferentes mensajes como resultado de la finalización de la sesión en función de los dispositivos móviles y la versión de Citrix Receiver. Además, la diferencia en la forma en que se escribe Citrix Application para diferentes plataformas móviles ofrece una experiencia diferente cuando se desconecta de los dispositivos Android.

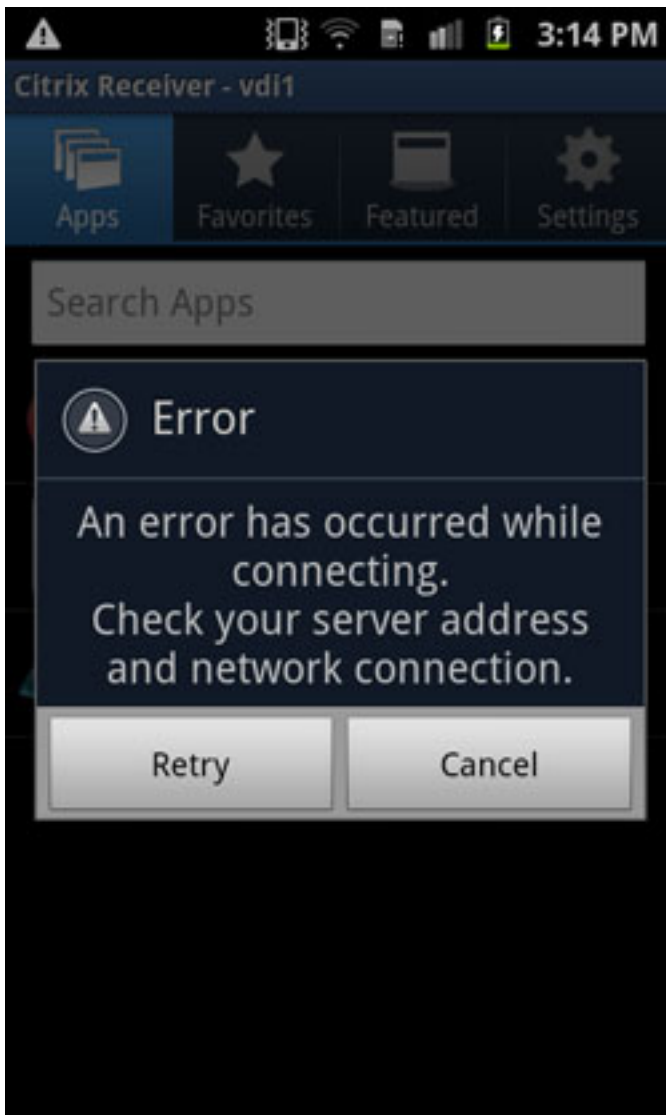
En el iPad y el iPhone, Citrix Receiver muestra el mensaje **Su acceso a la sesión de la puerta de enlace ha caducado. Vuelva a iniciar sesión.** Al hacer clic en **Aceptar**, Citrix Receiver muestra la pantalla con los servidores configurados.



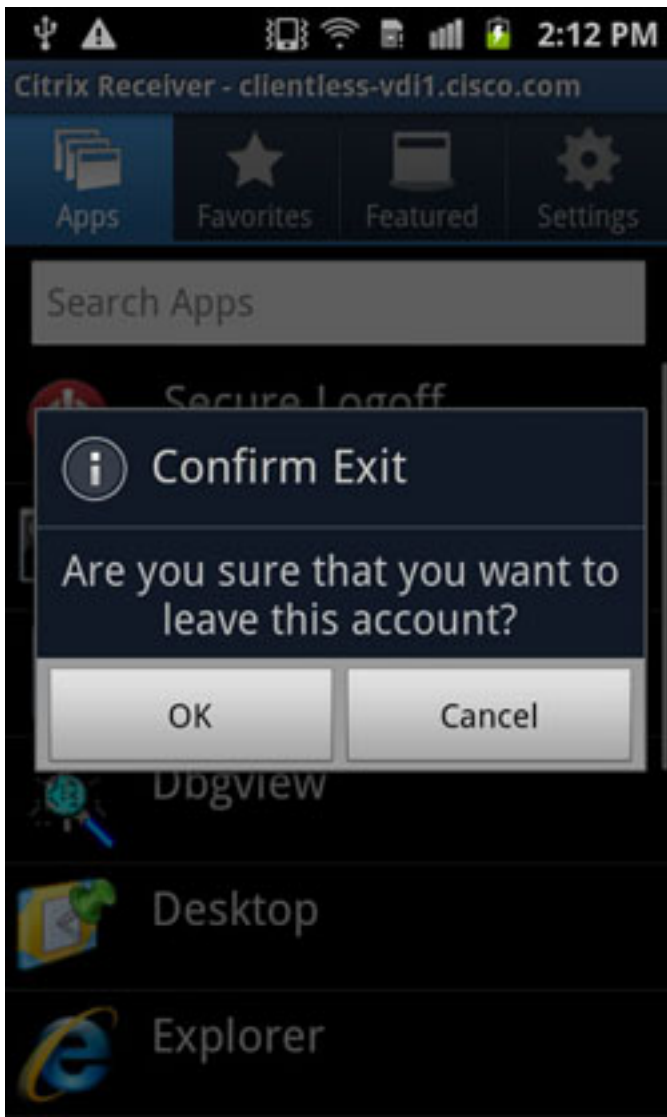
Los dispositivos Android también muestran el recurso **Secure Logoff** inyectado.



Sin embargo, al hacer clic en la aplicación **Cerrar sesión seguro**, se muestra un error de conexión de red.



Aunque para este momento la sesión WebVPN ha finalizado, la aplicación Citrix Receiver no tiene mensajes incrustados que le informen correctamente de otras acciones. Este es el comportamiento esperado. Cuando se muestra este mensaje de **error** como resultado de la sesión finalizada, espera que haga clic en el botón **Cancelar**, en el botón **Atrás** del dispositivo Android para salir de la cuenta actual, y luego en **Aceptar** cuando se le pregunte si desea salir de esta cuenta.



Después de salir de la cuenta actual, se le mostrará la lista de servidores preconfigurados.



Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshoot

En esta sección se brinda información que puede utilizar para resolver problemas en su configuración.

Depuraciones

Nota: Consulte [Información Importante sobre Comandos de Debug antes de usar un comando debug](#).

Puede mostrar la información de depuración para Citrix Receiver con este comando:

debug webvpn citrix <1-255>

Nota:

El nivel 1 muestra condiciones anormales, conexiones fallidas al servidor XenApp/XenDesktop y errores generales.

El nivel 50 muestra información sobre los datos que se están analizando o reescribiendo.

El nivel 255 muestra toda la información de depuración que se ha agregado para las conexiones de Citrix Receiver.

No se agregaron nuevos comandos para la autenticación de Citrix Receiver. Sin embargo, para ver las transacciones entre el cliente y el ASA, puede utilizar esta depuración:

debug webvpn transformation request

Para referencia. este resultado muestra estas dos depuraciones tomadas de una conexión que funciona:

```
=====  
Channel NP p=0x00000000 0/0 more bufferedchannel-np.c  
TEST-ASA#  
TEST-ASA# DBG:89:3178386013:7404365c:0000: netsal_accept returned 0x6d6ce7c0  
(unicorn-proxy.c:proxy_thread_asa:1250)  
DBG:90:3178386045:7404365c:0000: Creating fiber 0x74100d20 [unicorn-proxy],  
stack(16384) = 0x74136ed0..0x7413aecc (fc=3), sys 0x6d5abea8  
(FIBERS/fibers.c:fiber_create:519)  
DBG:91:3178386088:74100d20:0000: Jumpstarting unicorn-proxy 0x74100d20,  
sys 0x74043610 (FIBERS/fibers-jumpstart.c:_fiber_jumpstart:36)  
DBG:92:3178386111:74100d20:0000: New client http connection: start requests  
handling (CONN/aware.c:run_aware_fiber:1316)  
DBG:93:3178386125:74100d20:0000: new fiber for client_ch 0x6d6ce7c0  
(aware.c:run_aware_fiber:1318)  
DBG:94:3178386136:74100d20:0009: in process request  
(aware.c:aware_dispatch_request:301)  
DBG:95:3178386148:74100d20:0009: alloc aware ctx  
(aware_mem.c:mem_aware_ctx_alloc:56)  
DBG:96:3178433565:74100d20:0009: Hook: UrlSniff_cb  
(aware_webvpn_conf.re2c:UrlSniff_cb:927)  
DBG:97:3178433620:74100d20:0009: METHOD = 1, GET  
(aware_parse_headers.re2c:aware_parse_req_headers:619)  
DBG:98:3178433640:74100d20:0009: Hook: SharePoint_cb  
(aware_webvpn_conf.re2c:SharePoint_cb:1021)  
DBG:99:3178433652:74100d20:0009: Hook: SessionCheck_cb  
(aware_webvpn_conf.re2c:SessionCheck_cb:1897)  
DBG:00:3178433694:74100d20:0009: Hook: VCARedirect_cb  
(aware_webvpn_conf.re2c:VCARedirect_cb:1805)  
DBG:01:3178433713:74100d20:0009: Hook: NACRedirect_cb  
(aware_webvpn_conf.re2c:NACRedirect_cb:1866)  
DBG:02:3178433730:74100d20:0009: Hook: ClientServices_cb  
(aware_webvpn_conf.re2c:ClientServices_cb:2172)  
DBG:03:3178433742:74100d20:0009: Hook: SCEPProxy_cb  
(aware_webvpn_conf.re2c:SCEPProxy_cb:2154)  
DBG:04:3178433753:74100d20:0009: Hook: AdminURLCheck_cb  
(aware_webvpn_conf.re2c:AdminURLCheck_cb:345)  
DBG:05:3178433810:74100d20:0009: Hook: GroupURLCheck_cb  
(aware_webvpn_conf.re2c:GroupURLCheck_cb:1594)  
DBG:06:3178433883:74100d20:0009: Hook: PathCookie_cb  
(aware_webvpn_conf.re2c:PathCookie_cb:1088)  
DBG:07:3178433899:74100d20:0009: Hook: Webfolder_cb  
(aware_webvpn_conf.re2c:Webfolder_cb:1167)
```


DBG:08:3178433916:74100d20:0009: Hook: RootCheck_cb
(aware_webvpn_conf.re2c:RootCheck_cb:508)
DBG:09:3178433930:74100d20:0009: Load portal for the root request (null)
(aware_webvpn_conf.re2c:RootCheck_cb:578)
DBG:10:3178433942:74100d20:0009: => embedded
(aware.c:aware_dispatch_request:396)
DBG:11:3178433955:74100d20:0009: Serve embedded request [/
(aware.c:aware_serve_request:782)
DBG:12:3178433978:74100d20:0009: Open handler file [/+CSCOE+/portal.html]
(aware.c:aware_serve_request:822)
DBG:13:3178434028:74100d20:0009: No session redirect
(aware.c:aware_serve_request:888)
DBG:14:3178434104:74100d20:0009: STD HEADERS SENT
(aware.c:aware_send_resp_headers:151)
DBG:15:3178434149:74100d20:0009: HEADERS SENT
(aware.c:aware_send_resp_headers:162)
DBG:16:3178434188:74100d20:0009: + freeing ctx
(CONN/aware.c:aware_connection_clean_up:251)
DBG:17:3178434207:74100d20:0009: free aware ctx
(aware_mem.c:mem_aware_ctx_free:64)
DBG:18:3178434226:74100d20:0010: in process request
(aware.c:aware_dispatch_request:301)
DBG:19:3178434239:74100d20:0010: alloc aware ctx
(aware_mem.c:mem_aware_ctx_alloc:56)
DBG:20:3179015760:74100d20:0010: -- EOF in iobuf_channel input!!!
(iobuf_channel.c:ucte_input_buf_channel_input_fun:157)
DBG:21:3179015792:74100d20:0010: read_req_headers: first line: Unexpected
character 0x00 (aware_parse_headers.re2c:aware_parse_req_headers:241)
DBG:22:3179015809:74100d20:0010: + freeing ctx
(CONN/aware.c:aware_connection_clean_up:251)
DBG:23:3179015821:74100d20:0010: free aware ctx
(aware_mem.c:mem_aware_ctx_free:64)
DBG:24:3179015838:74100d20:0010: Fiber exit - client_ch 0x6d6ce7c0
(aware.c:run_aware_fiber:1339)
DBG:25:3179015852:74100d20:0010: Fiber 0x74100d20 finished leaving 4 more
(FIBERS/fibers-jumpstart.c:_fiber_jumpstart:64)
DBG:26:3179015865:74100d20:0010: Exiting fiber 0x74100d20
(FIBERS/fibers.c:fiber__kill:1257)
DBG:27:3179015934:74100d20:0010: SALNPCLOSENOTIFY: p=0x0 0/0 more buffered
(SAL/channel-np.c:_sal_np_ioctl:1269)
DBG:28:3179015965:74100d20:0010: Fiber 0x74100d20 terminated, 3 more
(FIBERS/fibers.c:fiber__kill:1330)
Channel NP p=0x00000000 0/0 more bufferedchannel-np.c
TEST-ASA#
TEST-ASA#
TEST-ASA#
TEST-ASA# DBG:29:3203022718:7404365c:0000: netsal_accept returned 0x6d6ce7c0
(unicorn-proxy.c:proxy_thread_asa:1250)
DBG:30:3203022750:7404365c:0000: Creating fiber 0x740ff6a0 [unicorn-proxy],
stack(16384) = 0x7413ef10..0x74142f0c (fc=3), sys 0x6d5abea8
(FIBERS/fibers.c:fiber_create:519)
DBG:31:3203022926:740ff6a0:0000: Jumpstarting unicorn-proxy 0x740ff6a0, sys
0x74043610 (FIBERS/fibers-jumpstart.c:_fiber_jumpstart:36)
DBG:32:3203022959:740ff6a0:0000: New client http connection: start requests
handling (CONN/aware.c:run_aware_fiber:1316)
DBG:33:3203022973:740ff6a0:0000: new fiber for client_ch 0x6d6ce7c0
(aware.c:run_aware_fiber:1318)
DBG:34:3203022986:740ff6a0:0011: in process request
(aware.c:aware_dispatch_request:301)
DBG:35:3203022996:740ff6a0:0011: alloc aware ctx
(aware_mem.c:mem_aware_ctx_alloc:56)
DBG:36:3203070771:740ff6a0:0011: Hook: UrlSniff_cb
(aware_webvpn_conf.re2c:UrlSniff_cb:927)
DBG:37:3203070845:740ff6a0:0011: METHOD = 1, GET

(aware_parse_headers.re2c:aware_parse_req_headers:619)
DBG:38:3203070870:740ff6a0:0011: Hook: SharePoint_cb
(aware_webvpn_conf.re2c:SharePoint_cb:1021)
DBG:39:3203070883:740ff6a0:0011: Hook: SessionCheck_cb
(aware_webvpn_conf.re2c:SessionCheck_cb:1897)
DBG:40:3203070894:740ff6a0:0011: Hook: VCARedirect_cb
(aware_webvpn_conf.re2c:VCARedirect_cb:1805)
DBG:41:3203070907:740ff6a0:0011: Hook: NACRedirect_cb
(aware_webvpn_conf.re2c:NACRedirect_cb:1866)
DBG:42:3203070919:740ff6a0:0011: Hook: ClientServices_cb
(aware_webvpn_conf.re2c:ClientServices_cb:2172)
DBG:43:3203070931:740ff6a0:0011: Hook: SCEPProxy_cb
(aware_webvpn_conf.re2c:SCEPProxy_cb:2154)
DBG:44:3203070940:740ff6a0:0011: Hook: AdminURLCheck_cb
(aware_webvpn_conf.re2c:AdminURLCheck_cb:345)
DBG:45:3203070996:740ff6a0:0011: Hook: GroupURLCheck_cb
(aware_webvpn_conf.re2c:GroupURLCheck_cb:1594)
DBG:46:3203071070:740ff6a0:0011: Hook: PathCookie_cb
(aware_webvpn_conf.re2c:PathCookie_cb:1088)
DBG:47:3203071090:740ff6a0:0011: Hook: Webfolder_cb
(aware_webvpn_conf.re2c:Webfolder_cb:1167)
DBG:48:3203071105:740ff6a0:0011: Hook: RootCheck_cb
(aware_webvpn_conf.re2c:RootCheck_cb:508)
DBG:49:3203071122:740ff6a0:0011: Load portal for the root request (null)
(aware_webvpn_conf.re2c:RootCheck_cb:578)
DBG:50:3203071135:740ff6a0:0011: => embedded request
(aware.c:aware_dispatch_request:396)
DBG:51:3203071147:740ff6a0:0011: Serve embedded request [/
(aware.c:aware_serve_request:782)
DBG:52:3203071169:740ff6a0:0011: Open handler file [/+CSCOE+/portal.html]
(aware.c:aware_serve_request:822)
DBG:53:3203071218:740ff6a0:0011: No session redirect
(aware.c:aware_serve_request:888)
DBG:54:3203071293:740ff6a0:0011: STD HEADERS SENT
(aware.c:aware_send_resp_headers:151)
DBG:55:3203071338:740ff6a0:0011: HEADERS SENT
(aware.c:aware_send_resp_headers:162)
DBG:56:3203071376:740ff6a0:0011: + freeing ctx
(CONN/aware.c:aware_connection_clean_up:251)
DBG:57:3203071396:740ff6a0:0011: free aware ctx
(aware_mem.c:mem_aware_ctx_free:64)
DBG:58:3203071414:740ff6a0:0012: in process request
(aware.c:aware_dispatch_request:301)
DBG:59:3203071427:740ff6a0:0012: alloc aware ctx
(aware_mem.c:mem_aware_ctx_alloc:56)
DBG:60:3204883539:740ff6a0:0012: -- EOF in iobuf_channel input!!!
(iobuf_channel.c:ucte_input_buf_channel_input_fun:157)
DBG:61:3204883574:740ff6a0:0012: read_req_headers: first line: Unexpected
character 0x00 (aware_parse_headers.re2c:aware_parse_req_headers:241)
DBG:62:3204883591:740ff6a0:0012: + freeing ctx
(CONN/aware.c:aware_connection_clean_up:251)
DBG:63:3204883603:740ff6a0:0012: free aware ctx
(aware_mem.c:mem_aware_ctx_free:64)
DBG:64:3204883619:740ff6a0:0012: Fiber exit - client_ch 0x6d6ce7c0
(aware.c:run_aware_fiber:1339)
DBG:65:3204883632:740ff6a0:0012: Fiber 0x740ff6a0 finished leaving 4 more
(FIBERS/fibers-jumpstart.c:_fiber_jumpstart:64)
DBG:66:3204883645:740ff6a0:0012: Exiting fiber 0x740ff6a0
(FIBERS/fibers.c:fiber__kill:1257)
DBG:67:3204883718:740ff6a0:0012: SALNPCLOSENOTIFY: p=0x0 0/0 more buffered
(SAL/channel-np.c:_sal_np_ioctl:1269)
DBG:68:3204883750:740ff6a0:0012: Fiber 0x740ff6a0 terminated, 3 more
(FIBERS/fibers.c:fiber__kill:1330)
Channel NP p=0x00000000 0/0 more bufferedchannel-np.cDBG:69:3212412660:7404365c:0000:

netsal_accept returned 0x6d6ce7c0 (unicorn-proxy.c:proxy_thread_asa:1250)
DBG:70:3212412691:7404365c:0000: Creating fiber 0x74100d20 [unicorn-proxy],
stack(16384) = 0x74136ed0..0x7413aecc (fc=3), sys 0x6d5abea8
(FIBERS/fibers.c:fiber_create:519)
DBG:71:3212413380:74100d20:0000: Jumpstarting unicorn-proxy 0x74100d20,
sys 0x74043610 (FIBERS/fibers-jumpstart.c:_fiber_jumpstart:36)
DBG:72:3212413415:74100d20:0000: New client http connection: start requests
handling (CONN/aware.c:run_aware_fiber:1316)
DBG:73:3212413429:74100d20:0000: new fiber for client_ch 0x6d6ce7c0
(aware.c:run_aware_fiber:1318)
DBG:74:3212413447:74100d20:0013: in process request
(aware.c:aware_dispatch_request:301)
DBG:75:3212413460:74100d20:0013: alloc aware ctx
(aware_mem.c:mem_aware_ctx_alloc:56)
DBG:76:3212462785:74100d20:0013: Hook: UrlSniff_cb
(aware_webvpn_conf.re2c:UrlSniff_cb:927)
DBG:77:3212462837:74100d20:0013: METHOD = 1, GET
(aware_parse_headers.re2c:aware_parse_req_headers:619)
DBG:78:3212462857:74100d20:0013: Hook: SharePoint_cb
(aware_webvpn_conf.re2c:SharePoint_cb:1021)
DBG:79:3212462873:74100d20:0013: Hook: SessionCheck_cb
(aware_webvpn_conf.re2c:SessionCheck_cb:1897)
DBG:80:3212462884:74100d20:0013: Hook: VCARedirect_cb
(aware_webvpn_conf.re2c:VCARedirect_cb:1805)
DBG:81:3212462895:74100d20:0013: Hook: NACRedirect_cb
(aware_webvpn_conf.re2c:NACRedirect_cb:1866)
DBG:82:3212462906:74100d20:0013: Hook: ClientServices_cb
(aware_webvpn_conf.re2c:ClientServices_cb:2172)
DBG:83:3212462918:74100d20:0013: Hook: SCEPPProxy_cb
(aware_webvpn_conf.re2c:SCEPPProxy_cb:2154)
DBG:84:3212462928:74100d20:0013: Hook: AdminURLCheck_cb
(aware_webvpn_conf.re2c:AdminURLCheck_cb:345)
DBG:85:3212462983:74100d20:0013: Hook: GroupURLCheck_cb
(aware_webvpn_conf.re2c:GroupURLCheck_cb:1594)
DBG:86:3212463058:74100d20:0013: Hook: PathCookie_cb
(aware_webvpn_conf.re2c:PathCookie_cb:1088)
DBG:87:3212463075:74100d20:0013: Hook: Webfolder_cb
(aware_webvpn_conf.re2c:Webfolder_cb:1167)
DBG:88:3212463091:74100d20:0013: Hook: RootCheck_cb
(aware_webvpn_conf.re2c:RootCheck_cb:508)
DBG:89:3212463104:74100d20:0013: Load portal for the root request (null)
(aware_webvpn_conf.re2c:RootCheck_cb:578)
DBG:90:3212463118:74100d20:0013: => embedded request
(aware.c:aware_dispatch_request:396)
DBG:91:3212463128:74100d20:0013: Serve embedded request [/
(aware.c:aware_serve_request:782)
DBG:92:3212463150:74100d20:0013: Open handler file [/+CSCOE+/portal.html]
(aware.c:aware_serve_request:822)
DBG:93:3212463202:74100d20:0013: No session redirect
(aware.c:aware_serve_request:888)
DBG:94:3212463305:74100d20:0013: STD HEADERS SENT
(aware.c:aware_send_resp_headers:151)
DBG:95:3212463351:74100d20:0013: HEADERS SENT
(aware.c:aware_send_resp_headers:162)
DBG:96:3212463388:74100d20:0013: + freeing ctx
(CONN/aware.c:aware_connection_clean_up:251)
DBG:97:3212463407:74100d20:0013: free aware ctx
(aware_mem.c:mem_aware_ctx_free:64)
DBG:98:3212463424:74100d20:0014: in process request
(aware.c:aware_dispatch_request:301)
DBG:99:3212463435:74100d20:0014: alloc aware ctx
(aware_mem.c:mem_aware_ctx_alloc:56)
DBG:00:3212610662:74100d20:0014: Hook: UrlSniff_cb
(aware_webvpn_conf.re2c:UrlSniff_cb:927)

DBG:01:3212610716:74100d20:0014: METHOD = 1, GET
(aware_parse_headers.re2c:aware_parse_req_headers:619)

DBG:02:3212610737:74100d20:0014: Hook: SharePoint_cb
(aware_webvpn_conf.re2c:SharePoint_cb:1021)

DBG:03:3212610750:74100d20:0014: Hook: SessionCheck_cb
(aware_webvpn_conf.re2c:SessionCheck_cb:1897)

DBG:04:3212610762:74100d20:0014: Hook: VCARedirect_cb
(aware_webvpn_conf.re2c:VCARedirect_cb:1805)

DBG:05:3212610774:74100d20:0014: Hook: NACRedirect_cb
(aware_webvpn_conf.re2c:NACRedirect_cb:1866)

DBG:06:3212610787:74100d20:0014: Hook: ClientServices_cb
(aware_webvpn_conf.re2c:ClientServices_cb:2172)

DBG:07:3212610799:74100d20:0014: Hook: SCEPProxy_cb
(aware_webvpn_conf.re2c:SCEPProxy_cb:2154)

DBG:08:3212610810:74100d20:0014: Hook: AdminURLCheck_cb
(aware_webvpn_conf.re2c:AdminURLCheck_cb:345)

DBG:09:3212610870:74100d20:0014: Hook: GroupURLCheck_cb
(aware_webvpn_conf.re2c:GroupURLCheck_cb:1594)

DBG:10:3212610945:74100d20:0014: Hook: PathCookie_cb
(aware_webvpn_conf.re2c:PathCookie_cb:1088)

DBG:11:3212610964:74100d20:0014: Hook: Webfolder_cb
(aware_webvpn_conf.re2c:Webfolder_cb:1167)

DBG:12:3212610980:74100d20:0014: Hook: RootCheck_cb
(aware_webvpn_conf.re2c:RootCheck_cb:508)

DBG:13:3212610997:74100d20:0014: Load portal for the root request (null)
(aware_webvpn_conf.re2c:RootCheck_cb:578)

DBG:14:3212611011:74100d20:0014: => embedded request
(aware.c:aware_dispatch_request:396)

DBG:15:3212611021:74100d20:0014: Serve embedded request [/
(aware.c:aware_serve_request:782)

DBG:16:3212611042:74100d20:0014: Open handler file [/+CSCOE+/portal.html]
(aware.c:aware_serve_request:822)

DBG:17:3212611090:74100d20:0014: No session redirect
(aware.c:aware_serve_request:888)

DBG:18:3212611162:74100d20:0014: STD HEADERS SENT
(aware.c:aware_send_resp_headers:151)

DBG:19:3212611231:74100d20:0014: HEADERS SENT
(aware.c:aware_send_resp_headers:162)

DBG:20:3212611270:74100d20:0014: + freeing ctx
(CONN/aware.c:aware_connection_clean_up:251)

DBG:21:3212611289:74100d20:0014: free aware ctx
(aware_mem.c:mem_aware_ctx_free:64)

DBG:22:3212611306:74100d20:0015: in process request
(aware.c:aware_dispatch_request:301)

DBG:23:3212611318:74100d20:0015: alloc aware ctx
(aware_mem.c:mem_aware_ctx_alloc:56)

DBG:24:3212711373:74100d20:0015: Hook: UrlSniff_cb
(aware_webvpn_conf.re2c:UrlSniff_cb:927)

DBG:25:3212711428:74100d20:0015: Cookie name:[webvpnlogin]: 11
(aware_parse_headers.re2c:aware_parse_cookie:754)

DBG:26:3212711458:74100d20:0015: METHOD = 2, POST
(aware_parse_headers.re2c:aware_parse_req_headers:619)

DBG:27:3212711479:74100d20:0015: => handoff (AWARE_HOOK_EXTERNAL_HANDOFF)
(aware.c:aware_dispatch_request:495)

DBG:28:3212711498:74100d20:0015: Channel NP p=0x6d6ce7c0 0/0 more buffered
(SAL/channel-np.c:_sal_np_close:908)

DBG:29:3212711568:74100d20:0015: Finish external handoff for client_ch
0x6d6ce7c0 (aware.c:aware_dispatch_request:497)

DBG:30:3212711589:74100d20:0015: + freeing ctx
(CONN/aware.c:aware_connection_clean_up:251)

DBG:31:3212711601:74100d20:0015: free aware ctx
(aware_mem.c:mem_aware_ctx_free:64)

DBG:32:3212711617:74100d20:0015: Fiber exit - client_ch 0x6d6ce7c0
(aware.c:run_aware_fiber:1339)

DBG:33:3212711630:74100d20:0015: Fiber 0x74100d20 finished leaving 4 more
(FIBERS/fibers-jumpstart.c:_fiber_jumpstart:64)

DBG:34:3212711644:74100d20:0015: Exiting fiber 0x74100d20
(FIBERS/fibers.c:fiber__kill:1257)

DBG:35:3212711658:74100d20:0015: Fiber 0x74100d20 terminated, 3 more
(FIBERS/fibers.c:fiber__kill:1330)

Creating fiber 0x73c63290 [fiber-ldap-class], stack(16384) =
0x73c9eae0..0x73ca2adc (fc=2), sys 0x6d5c1cacfibers.cDBG:36:3212712546:
73c63290:0000: Jumpstarting fiber-ldap-class 0x73c63290, sys 0x73c60ca0
(FIBERS/fibers-jumpstart.c:_fiber_jumpstart:36)

DBG:37:3212712646:73c63290:0000: Connecting to 00000000:1024239808
(SAL/netsal.c:netsal_connect:319)

DBG:38:3212712677:73c63290:0000: about to call netsal__safe_encapsulate for
(sal-np/tcp/CONNECT/3/192.168.12.61/389/M/VM) (SAL/netsal.c:netsal_connect:443)

DBG:39:3212712923:73c63290:0000: connection timeout set for 10 seconds
(SAL/netsal.c:netsal_connect:470)

DBG:40:3212723367:73c63290:0000: Exiting fiber 0x73c63290
(FIBERS/fibers.c:fiber__kill:1257)

DBG:41:3212723706:73c63290:0000: SALNPCLOSENOTIFY: p=0x0 0/0 more buffered
(SAL/channel-np.c:_sal_np_ioctl:1269)

DBG:42:3212723747:73c63290:0000: Fiber 0x73c63290 terminated, 2 more
(FIBERS/fibers.c:fiber__kill:1330)

DBG:36:3212726030:0:0000: Creating fiber 0x740ff6a0 [ak47_attach_class], stack
(256) = 0x741cb870..0x741cb96c (fc=3), sys 0x6d5ac2c0
(FIBERS/fibers.c:fiber_create:519)

DBG:37:3212726072:740ff6a0:0000: Remote storage is not configured
(pstorage.c:pStorage_restore:272)

Terminating fiber 0x740ff6a0fibers.cFiber 0x740ff6a0 terminated, 3 morefibers.
cDBG:38:3212726646:0:0000: Creating fiber 0x74100d20 [ak47_attach_class], stack
(256) = 0x741cb750..0x741cb84c (fc=3), sys 0x6d5ac2c0
(FIBERS/fibers.c:fiber_create:519)

DBG:39:3212726721:74100d20:0000: Creating fiber 0x740ff9a0 [unicorn-proxy], stack
(16384) = 0x74136ed0..0x7413aecc (fc=4), sys 0x6d5ac2c0
(FIBERS/fibers.c:fiber_create:519)

Terminating fiber 0x74100d20fibers.cFiber 0x74100d20 terminated, 4 morefibers.
cDBG:40:3212727006:740ff9a0:0000: Jumpstarting unicorn-proxy 0x740ff9a0, sys
0x74043610 (FIBERS/fibers-jumpstart.c:_fiber_jumpstart:36)

DBG:41:3212727039:740ff9a0:0000: New client http connection: start requests
handling (CONN/aware.c:run_aware_fiber:1316)

DBG:42:3212727052:740ff9a0:0000: new fiber for client_ch 0x6d6cf000
(aware.c:run_aware_fiber:1318)

DBG:43:3212727065:740ff9a0:0016: in process request
(aware.c:aware_dispatch_request:301)

DBG:44:3212727080:740ff9a0:0016: alloc aware ctx
(aware_mem.c:mem_aware_ctx_alloc:56)

Channel NP p=0x00000000 0/0 more bufferedchannel-np.cDBG:45:3212821243:740ff9a0:
0016: Hook: UrlSniff_cb (aware_webvpn_conf.re2c:UrlSniff_cb:927)

DBG:46:3212821289:740ff9a0:0016: Cookie name:[net6_cookie]: 11
(aware_parse_headers.re2c:aware_parse_cookie:754)

DBG:47:3212821312:740ff9a0:0016: Cookie name:[net6_user_session]: 17
(aware_parse_headers.re2c:aware_parse_cookie:754)

DBG:48:3212821327:740ff9a0:0016: Cookie name:[webvpn]: 6
(aware_parse_headers.re2c:aware_parse_cookie:754)

DBG:49:3212821341:740ff9a0:0016: Cookie name:[webvpnaac]: 9
(aware_parse_headers.re2c:aware_parse_cookie:754)

DBG:50:3212821354:740ff9a0:0016: Cookie name:[webvpnc]: 7
(aware_parse_headers.re2c:aware_parse_cookie:754)

DBG:51:3212821368:740ff9a0:0016: Cookie name:[webvpnx]: 7
(aware_parse_headers.re2c:aware_parse_cookie:754)

DBG:52:3212821389:740ff9a0:0016: METHOD = 1, GET
(aware_parse_headers.re2c:aware_parse_req_headers:619)

DBG:53:3212821407:740ff9a0:0016: => handoff (AWARE_HOOK_INTERNAL_HANDOFF)
(aware.c:aware_dispatch_request:508)

DBG:54:3212821420:740ff9a0:0016: in process request

```
(proxy.c:process_request:239)
DBG:55:3212821509:740ff9a0:0016: parse_req_headers(client_fd, p_req) ;
(proxy.c:process_request:275)
DBG:56:3212821531:740ff9a0:0016: Request: [GET /Citrix/pnagent/config.xml
HTTP/1.1]: 39 (parse_req_headers.re2c:parse_req_headers:1399)
DBG:57:3212821556:740ff9a0:0016: req headers array at 741f3480
(parse_req_headers.re2c:parse_req_headers:1500)
DBG:58:3212821577:740ff9a0:0016: in parse_cookie
(ucte_parse_cookie.re2c:parse_cookie:430)
DBG:59:3212821590:740ff9a0:0016: Process next cookie
(ucte_parse_cookie.re2c:parse_cookie:441)
DBG:60:3212821603:740ff9a0:0016: Process next cookie
(ucte_parse_cookie.re2c:parse_cookie:441)
DBG:61:3212821613:740ff9a0:0016: Process next cookie
(ucte_parse_cookie.re2c:parse_cookie:441)
DBG:62:3212821625:740ff9a0:0016: Cookie name: net6_user_session
(ucte_parse_cookie.re2c:parse_cookie:605)
DBG:63:3212821638:740ff9a0:0016: -->in ucte_process_req_cookie
(COOKIE/ucte_cookie.c:ucte_process_req_cookie:135)
DBG:64:3212821653:740ff9a0:0016: req cookie array at 741f3680
(COOKIE/ucte_cookie.c:ucte_process_req_cookie:144)
DBG:65:3212821665:740ff9a0:0016: Process next cookie
(ucte_parse_cookie.re2c:parse_cookie:441)
DBG:66:3212821675:740ff9a0:0016: Process next cookie
(ucte_parse_cookie.re2c:parse_cookie:441)
DBG:67:3212821685:740ff9a0:0016: Process next cookie
(ucte_parse_cookie.re2c:parse_cookie:441)
DBG:68:3212821695:740ff9a0:0016: Process next cookie
(ucte_parse_cookie.re2c:parse_cookie:441)
DBG:69:3212821705:740ff9a0:0016: Cookie name: webvpnaac
(ucte_parse_cookie.re2c:parse_cookie:605)
DBG:70:3212821718:740ff9a0:0016: -->in ucte_process_req_cookie
(COOKIE/ucte_cookie.c:ucte_process_req_cookie:135)
DBG:71:3212821730:740ff9a0:0016: Process next cookie
(ucte_parse_cookie.re2c:parse_cookie:441)
DBG:72:3212821740:740ff9a0:0016: Process next cookie
(ucte_parse_cookie.re2c:parse_cookie:441)
DBG:73:3212821750:740ff9a0:0016: Process next cookie
(ucte_parse_cookie.re2c:parse_cookie:441)
DBG:74:3212821759:740ff9a0:0016: Process next cookie
(ucte_parse_cookie.re2c:parse_cookie:441)
DBG:75:3212821768:740ff9a0:0016: Cookie name: webvpnx
(ucte_parse_cookie.re2c:parse_cookie:605)
DBG:76:3212821778:740ff9a0:0016: -->in ucte_process_req_cookie
(COOKIE/ucte_cookie.c:ucte_process_req_cookie:135)
DBG:77:3212821788:740ff9a0:0016: in parse Cookie -->
(ucte_parse_cookie.re2c:parse_cookie:777)
DBG:78:3212821844:740ff9a0:0016: User [test.user]
(proxy.c:process_request:418)
DBG:79:3212821870:740ff9a0:0016: Keepalive threshold forced to 4
(ucte_policy.c:ucte_get_ctx_session_settings:798)
DBG:80:3212821888:740ff9a0:0016: => reverse proxy request
(proxy.c:process_request:615)
ERR:81:3212821920:740ff9a0:0016: Failed expectation "this != NULL && this->start !=
NULL && cstr != NULL && value != NULL && this->signature == CLSTRING_SIGNATURE"
(clString.c:clString_replace_all_ncstring_:571)
ERR:82:3212821944:740ff9a0:0016: Failed expectation "this != NULL && this->start !=
NULL && cstr != NULL && value != NULL && this->signature == CLSTRING_SIGNATURE"
(clString.c:clString_replace_all_ncstring_:571)
ERR:83:3212821962:740ff9a0:0016: Failed expectation "this != NULL && this->start !=
NULL && cstr != NULL && value != NULL && this->signature == CLSTRING_SIGNATURE"
(clString.c:clString_replace_all_ncstring_:571)
ERR:84:3212821989:740ff9a0:0016: Failed expectation "this != NULL && this->start !=
NULL && cstr != NULL && value != NULL && this->signature == CLSTRING_SIGNATURE"
```

```
(clString.c:clString_replace_all_ncstring_:571)
ERR:85:3212822008:740ff9a0:0016: Failed expectation "this != NULL && this->start !=
NULL && cstr != NULL && value != NULL && this->signature == CLSTRING_SIGNATURE"
(clString.c:clString_replace_all_ncstring_:571)
ERR:86:3212822021:740ff9a0:0016: Failed expectation "this != NULL && this->start !=
NULL && cstr != NULL && value != NULL && this->signature == CLSTRING_SIGNATURE"
(clString.c:clString_replace_all_ncstring_:571)
ERR:87:3212822038:740ff9a0:0016: Failed expectation "this != NULL && this->start !=
NULL && cstr != NULL && value != NULL && this->signature == CLSTRING_SIGNATURE"
(clString.c:clString_replace_all_ncstring_:571)
ERR:88:3212822052:740ff9a0:0016: Failed expectation "this != NULL && this->start !=
NULL && cstr != NULL && value != NULL && this->signature == CLSTRING_SIGNATURE"
(clString.c:clString_replace_all_ncstring_:571)
ERR:89:3212822065:740ff9a0:0016: Failed expectation "this != NULL && this->start !=
NULL && cstr != NULL && value != NULL && this->signature == CLSTRING_SIGNATURE"
(clString.c:clString_replace_all_ncstring_:571)
ERR:90:3212822081:740ff9a0:0016: Failed expectation "this != NULL && this->start !=
NULL && cstr != NULL && value != NULL && this->signature == CLSTRING_SIGNATURE"
(clString.c:clString_replace_all_ncstring_:571)
ERR:91:3212822095:740ff9a0:0016: Failed expectation "this != NULL && this->start !=
NULL && cstr != NULL && value != NULL && this->signature == CLSTRING_SIGNATURE"
(clString.c:clString_replace_all_ncstring_:571)
ERR:92:3212822108:740ff9a0:0016: Failed expectation "this != NULL && this->start !=
NULL && cstr != NULL && value != NULL && this->signature == CLSTRING_SIGNATURE"
(clString.c:clString_replace_all_ncstring_:571)
ERR:93:3212822149:740ff9a0:0016: Failed expectation "this != NULL && this->start !=
NULL && cstr != NULL && value != NULL && this->signature == CLSTRING_SIGNATURE"
(clString.c:clString_replace_all_ncstring_:571)
ERR:94:3212822165:740ff9a0:0016: Failed expectation "this != NULL && this->start !=
NULL && cstr != NULL && value != NULL && this->signature == CLSTRING_SIGNATURE"
(clString.c:clString_replace_all_ncstring_:571)
DBG:95:3212822203:740ff9a0:0016: + About to dump request body to the file
(proxy.c:process_request:889)
DBG:96:3212822222:740ff9a0:0016: used_at_least_once [0], server_ch [0],
netsal_connection_is_closing [1] (proxy.c:process_request:1204)
DBG:97:3212822236:740ff9a0:0016: no old connection, create a new one
(proxy.c:process_request:1206)
DBG:98:3212822283:740ff9a0:0016: Decoded URL: /Citrix/pnagent/config.xml
(conn.c:establish_connection:626)
DBG:99:3212822326:740ff9a0:0016: Connecting to 00000000:84150794
(SAL/netsal.c:netsal_connect:319)
DBG:00:3212822355:740ff9a0:0016: otherPifNum 3, nexthop4 5080b0a
(SAL/netsal.c:netsal_connect:371)
DBG:01:3212822381:740ff9a0:0016: about to call netsal__safe_encapsulate for
(sal-np/tcp/CONNECT/3/10.10.4.5/80/T/PROXY/2/70.199.131.148/3007)
(SAL/netsal.c:netsal_connect:443)
DBG:02:3212822643:740ff9a0:0016: connection timeout set for 10 seconds
(SAL/netsal.c:netsal_connect:470)
DBG:03:3212824193:740ff9a0:0016: Back-end connection is READY [6d6ce680]
(proxy.c:process_request:1216)
DBG:04:3212824222:740ff9a0:0016: + sending headers to the server
(proxy.c:process_request:1240)
DBG:05:3212824242:740ff9a0:0016: CONNECT TO http://10.10.4.5/Citrix/pnagent/config.xml
(send_req_headers.c:ucte_send_request_headers:160)
DBG:06:3212824309:740ff9a0:0016: About to open cookie directory:
sessions/2375680/cookie (COOKIE/ucte_cookie.c:send_req_cookie_storage:670)
DBG:07:3212824328:740ff9a0:0016: Could not open cookie directory
(COOKIE/ucte_cookie.c:send_req_cookie_storage:674)
DBG:08:3212824507:740ff9a0:0016: Connection acquired; headers sent
(proxy.c:process_request:1335)
DBG:09:3212824536:740ff9a0:0016: + Request headers and data sent...
(proxy.c:process_request:1438)
DBG:10:3212824550:740ff9a0:0016: + getting headers from the back end server...
(proxy.c:process_request:1449)
```

DBG:11:3212828428:740ff9a0:0016: resp header array at 741f3500
(parse_resp_headers.re2c:parse_resp_headers:226)
DBG:12:3212828485:740ff9a0:0016: => Response headers received (proxy.c:
process_request:1522)
DBG:13:3212828509:740ff9a0:0016: => About to send response headers to
the client (proxy.c:process_request:1693)
DBG:14:3212828527:740ff9a0:0016: ucte_hint = 4, content_type = 4,
resp_code = 200, session_defined = 2 (CACHE/send_resp_headers.c:
ucte_send_response_headers:407)
DBG:15:3212828612:740ff9a0:0016: + Sending response body (6982 bytes) to the client
(proxy.c:process_request:1793)
DBG:16:3212828635:740ff9a0:0016: + sending response body
(proxy.c:process_request:1865)
DBG:17:3212828645:740ff9a0:0016: Response: content-type=4
(proxy.c:process_request:1867)
DBG:18:3212829517:740ff9a0:0016: Session update!!!!!!!
(ucte_ctx.c:ucte_session_update:645)
DBG:19:3212829566:740ff9a0:0016: + response body was sent
(proxy.c:process_request:1875)
DBG:20:3212829602:740ff9a0:0016: Backend connection reserved
(proxy.c:process_request:2145)
DBG:21:3212829618:740ff9a0:0016: free req_header, 74058210
(mem_man.c:mem_req_header_free:210)
DBG:22:3212829635:740ff9a0:0016: in req_header_light_destructor: free headers at
741f3480 (http_header.c:req_header_light_destructor:277)
DBG:23:3212829650:740ff9a0:0016: in req_header_light_destructor: free cookie at
741f3680 (http_header.c:req_header_light_destructor:282)
DBG:24:3212829664:740ff9a0:0016: free resp_header: 7406ab20
(mem_man.c:mem_resp_header_free:223)
DBG:25:3212829674:740ff9a0:0016: in resp_header_light_destructor: free headers at
741f3500 (http_header.c:resp_header_light_destructor:307)
DBG:26:3212829687:740ff9a0:0016: free ctx (mem_man.c:mem_ucte_ctx_free:197)
DBG:27:3212829708:740ff9a0:0016: Request finished gracefully
(proxy.c:process_request:2157)
DBG:28:3212829725:740ff9a0:0016: Finish internal handoff for client_ch 0x6d6cf000,
rc=1 (aware.c:aware_dispatch_request:510)
DBG:29:3212829738:740ff9a0:0016: + freeing ctx
(CONN/aware.c:aware_connection_clean_up:251)
DBG:30:3212829750:740ff9a0:0016: free aware ctx
(aware_mem.c:mem_aware_ctx_free:64)
DBG:31:3212829766:740ff9a0:0017: in process request
(aware.c:aware_dispatch_request:301)
DBG:32:3212829778:740ff9a0:0017: alloc aware ctx
(aware_mem.c:mem_aware_ctx_alloc:56)
DBG:33:3212941045:740ff9a0:0017: Hook: UrlSniff_cb
(aware_webvpn_conf.re2c:UrlSniff_cb:927)
DBG:34:3212941078:740ff9a0:0017: => handoff (AWARE_HOOK_INTERNAL_HANDOFF)
(aware.c:aware_dispatch_request:508)
DBG:35:3212941117:740ff9a0:0017: in process request (proxy.c:process_request:239)
DBG:36:3212941205:740ff9a0:0017: parse_req_headers(client_fd, p_req) ;
(proxy.c:process_request:275)
DBG:37:3212941240:740ff9a0:0017: Request: [POST /+CSCO+00756767633A2F2F313
02E31302E342E35++/Citrix/pnagent/launch.aspx HTTP/1.1]: 84
(parse_req_headers.re2c:parse_req_headers:1399)
DBG:38:3212941273:740ff9a0:0017: req headers array at 741f33c0
(parse_req_headers.re2c:parse_req_headers:1500)
DBG:39:3212941295:740ff9a0:0017: in parse_cookie
(ucte_parse_cookie.re2c:parse_cookie:430)
DBG:40:3212941308:740ff9a0:0017: Process next cookie
(ucte_parse_cookie.re2c:parse_cookie:441)
DBG:41:3212941332:740ff9a0:0017: Process next cookie
(ucte_parse_cookie.re2c:parse_cookie:441)
DBG:42:3212941342:740ff9a0:0017: Process next cookie
(ucte_parse_cookie.re2c:parse_cookie:441)

DBG:43:3212941353:740ff9a0:0017: Cookie name: net6_user_session
(ucte_parse_cookie.re2c:parse_cookie:605)

DBG:44:3212941366:740ff9a0:0017: -->in ucte_process_req_cookie
(COOKIE/ucte_cookie.c:ucte_process_req_cookie:135)

DBG:45:3212941383:740ff9a0:0017: req cookie array at 741f3400
(COOKIE/ucte_cookie.c:ucte_process_req_cookie:144)

DBG:46:3212941395:740ff9a0:0017: Process next cookie
(ucte_parse_cookie.re2c:parse_cookie:441)

DBG:47:3212941405:740ff9a0:0017: Process next cookie
(ucte_parse_cookie.re2c:parse_cookie:441)

DBG:48:3212941415:740ff9a0:0017: Process next cookie
(ucte_parse_cookie.re2c:parse_cookie:441)

DBG:49:3212941423:740ff9a0:0017: Process next cookie
(ucte_parse_cookie.re2c:parse_cookie:441)

DBG:50:3212941433:740ff9a0:0017: Process next cookie
(ucte_parse_cookie.re2c:parse_cookie:441)

DBG:51:3212941447:740ff9a0:0017: Process next cookie
(ucte_parse_cookie.re2c:parse_cookie:441)

DBG:52:3212941459:740ff9a0:0017: Cookie name: webvpnaac
(ucte_parse_cookie.re2c:parse_cookie:605)

DBG:53:3212941475:740ff9a0:0017: -->in ucte_process_req_cookie
(COOKIE/ucte_cookie.c:ucte_process_req_cookie:135)

DBG:54:3212941489:740ff9a0:0017: Process next cookie
(ucte_parse_cookie.re2c:parse_cookie:441)

DBG:55:3212941500:740ff9a0:0017: Process next cookie
(ucte_parse_cookie.re2c:parse_cookie:441)

DBG:56:3212941510:740ff9a0:0017: Process next cookie
(ucte_parse_cookie.re2c:parse_cookie:441)

DBG:57:3212941520:740ff9a0:0017: Process next cookie
(ucte_parse_cookie.re2c:parse_cookie:441)

DBG:58:3212941529:740ff9a0:0017: Cookie name: webvpnx
(ucte_parse_cookie.re2c:parse_cookie:605)

DBG:59:3212941540:740ff9a0:0017: -->in ucte_process_req_cookie
(COOKIE/ucte_cookie.c:ucte_process_req_cookie:135)

DBG:60:3212941551:740ff9a0:0017: in parse Cookie -->
(ucte_parse_cookie.re2c:parse_cookie:777)

DBG:61:3212941608:740ff9a0:0017: User [test.user]
(proxy.c:process_request:418)

DBG:62:3212941634:740ff9a0:0017: Keepalive threshold forced to 4
(ucte_policy.c:ucte_get_ctx_session_settings:798)

DBG:63:3212941651:740ff9a0:0017: => reverse proxy request
(proxy.c:process_request:615)

DBG:64:3212941677:740ff9a0:0017: + About to dump request body to the file
(proxy.c:process_request:889)

DBG:65:3212941792:740ff9a0:0017: potentially reusing existing backend channel,
old host=10.10.4.5, old port=80 (proxy.c:process_request:1098)

DBG:66:3212941814:740ff9a0:0017: new host=10.10.4.5, new port=80
(proxy.c:process_request:1101)

DBG:67:3212941826:740ff9a0:0017: match, reuse it (0x6d6ce680)
(proxy.c:process_request:1108)

DBG:68:3212941860:740ff9a0:0017: Decoded URL: /Citrix/pnagent/launch.aspx
(proxy.c:process_request:1145)

DBG:69:3212941900:740ff9a0:0017: Back-end connection is READY [6d6ce680]
(proxy.c:process_request:1216)

DBG:70:3212941916:740ff9a0:0017: + sending headers to the server
(proxy.c:process_request:1240)

DBG:71:3212941934:740ff9a0:0017: CONNECT TO
http://10.10.4.5/Citrix/pnagent/launch.aspx (send_req_headers.c:
ucte_send_request_headers:160)

DBG:72:3212941950:740ff9a0:0017: Session update!!!!!!!
(ucte_ctx.c:ucte_session_update:645)

DBG:73:3212942027:740ff9a0:0017: About to open cookie directory:
sessions/2375680/cookie (COOKIE/ucte_cookie.c:send_req_cookie_storage:670)

DBG:74:3212942047:740ff9a0:0017: Could not open cookie directory

(COOKIE/ucte_cookie.c:send_req_cookie_storage:674)
DBG:75:3212942220:740ff9a0:0017: Connection acquired; headers sent
(proxy.c:process_request:1335)
DBG:76:3212942307:740ff9a0:0017: + Request headers and data sent...
(proxy.c:process_request:1438)
DBG:77:3212942331:740ff9a0:0017: + getting headers from the back end server...
(proxy.c:process_request:1449)
DBG:78:3213277758:740ff9a0:0017: resp header array at 741f3500
(parse_resp_headers.re2c:parse_resp_headers:226)
DBG:79:3213277835:740ff9a0:0017: => Response headers received
(proxy.c:process_request:1522)
DBG:80:3213277857:740ff9a0:0017: => About to send response headers to the
client (proxy.c:process_request:1693)
DBG:81:3213277877:740ff9a0:0017: ucte_hint = 0, content_type = 12, resp_code = 200,
session_defined = 2 (CACHE/send_resp_headers.c:ucte_send_response_headers:407)
DBG:82:3213277968:740ff9a0:0017: + Sending response body (1162 bytes) to the client
(proxy.c:process_request:1793)
DBG:83:3213277991:740ff9a0:0017: + sending response body
(proxy.c:process_request:1865)
DBG:84:3213278030:740ff9a0:0017: Response: content-type=12
(proxy.c:process_request:1867)
DBG:85:3213278100:740ff9a0:0017: Generated SOCKS ticket: [V75E33CBB8657FB03V3233373
5363830V30V]: 36 (CISOCKS/../../unicorn/aware_apps/api/cisocks.c:
cisocks_ticket_create:446)
DBG:86:3213278499:740ff9a0:0017: + response body was sent
(proxy.c:process_request:1875)
DBG:87:3213278541:740ff9a0:0017: No front end keepalive
(proxy.c:process_request:2153)
DBG:88:3213278621:740ff9a0:0017: SALNPCLOSENOTIFY: p=0x0 0/0 more buffered
(SAL/channel-np.c:_sal_np_ioctl:1269)
DBG:89:3213278651:740ff9a0:0017: free req_header, 74058210
(mem_man.c:mem_req_header_free:210)
DBG:90:3213278669:740ff9a0:0017: in req_header_light_destructor: free headers at
741f33c0 (http_header.c:req_header_light_destructor:277)
DBG:91:3213278684:740ff9a0:0017: in req_header_light_destructor: free cookie at
741f3400 (http_header.c:req_header_light_destructor:282)
DBG:92:3213278697:740ff9a0:0017: free resp_header: 7406ab20
(mem_man.c:mem_resp_header_free:223)
DBG:93:3213278708:740ff9a0:0017: in resp_header_light_destructor: free headers at
741f3500 (http_header.c:resp_header_light_destructor:307)
DBG:94:3213278724:740ff9a0:0017: free ctx (mem_man.c:mem_ucte_ctx_free:197)
DBG:95:3213278756:740ff9a0:0017: Request finished gracefully
(proxy.c:process_request:2157)
DBG:96:3213278772:740ff9a0:0017: Finish internal handoff for client_ch 0x6d6cf000,
rc=-1 (aware.c:aware_dispatch_request:510)
DBG:97:3213278785:740ff9a0:0017: + freeing ctx
(CONN/aware.c:aware_connection_clean_up:251)
DBG:98:3213278796:740ff9a0:0017: free aware ctx
(aware_mem.c:mem_aware_ctx_free:64)
DBG:99:3213278809:740ff9a0:0017: Fiber exit - client_ch 0x6d6cf000
(aware.c:run_aware_fiber:1339)
DBG:00:3213278822:740ff9a0:0017: Fiber 0x740ff9a0 finished leaving 4 more
(FIBERS/fibers-jumpstart.c:_fiber_jumpstart:64)
DBG:01:3213278835:740ff9a0:0017: Exiting fiber 0x740ff9a0
(FIBERS/fibers.c:fiber__kill:1257)
DBG:02:3213278870:740ff9a0:0017: SALNPCLOSENOTIFY: p=0x0 0/0 more buffered
(SAL/channel-np.c:_sal_np_ioctl:1269)
DBG:03:3213278894:740ff9a0:0017: Fiber 0x740ff9a0 terminated, 3 more
(FIBERS/fibers.c:fiber__kill:1330)
Channel NP p=0x00000000 0/0 more bufferedchannel-np.cChannel NP p=0x00000000 0/0
more bufferedchannel-np.cDBG:04:3213773777:7404365c:0000: netsal_accept returned
0x6d6ce7c0 (unicorn-proxy.c:proxy_thread_asa:1250)
DBG:05:3213773808:7404365c:0000: Creating fiber 0x74100d20 [unicorn-proxy],
stack(16384) = 0x7413ef10..0x74142f0c (fc=3), sys 0x6d5abea8

```
(FIBERS/fibers.c:fiber_create:519)
DBG:06:3213773875:74100d20:0000: Jumpstarting unicorn-proxy 0x74100d20, sys
0x74043610 (FIBERS/fibers-jumpstart.c:_fiber_jumpstart:36)
DBG:07:3213773902:74100d20:0000: New client http connection: start requests
handling (CONN/aware.c:run_aware_fiber:1316)
DBG:08:3213773919:74100d20:0000: new fiber for client_ch 0x6d6ce7c0
(aware.c:run_aware_fiber:1318)
DBG:09:3213773932:74100d20:0018: in process request
(aware.c:aware_dispatch_request:301)
DBG:10:3213773943:74100d20:0018: alloc aware ctx
(aware_mem.c:mem_aware_ctx_alloc:56)
DBG:11:3213812394:74100d20:0018: => handoff (AWARE_HOOK_EXTERNAL_HANDOFF)
(aware.c:aware_dispatch_request:495)
DBG:12:3213812426:74100d20:0018: Connection accepted
(CISOCKS/../../unicorn/aware_apps/api/cisocks.c:cisocks_handle:143)
DBG:13:3213860698:74100d20:0018: Connecting to 00000000:-1257461568
(SAL/netsal.c:netsal_connect:319)
DBG:14:3213860731:74100d20:0018: otherPifNum 3, nexthop4 5080b0a
(SAL/netsal.c:netsal_connect:371)
DBG:15:3213860761:74100d20:0018: about to call netsal__safe_encapsulate
for (sal-np/tcp/CONNECT/3/192.168.12.181/1494/T)
(SAL/netsal.c:netsal_connect:443)
DBG:16:3213861036:74100d20:0018: connection timeout set for 10 seconds
(SAL/netsal.c:netsal_connect:470)
DBG:17:3213861857:74100d20:0018: RELAY notify(0x6d6ce7c0, 2, 0,
socket=0x6218aa8/0x6218aa8) (SAL/channel-np.c:sal_np_relay_cb:1574)
DBG:18:3213861893:74100d20:0018: sal_np_relay_notify: signaling condvar
(SAL/channel-np.c:sal_np_relay_cb:1604)
DBG:19:3213861908:74100d20:0018: Acquired relay_mutex on in 0x6d6e79e8
(SAL/channel-np.c:sal_np_midpath_relay:1775)
DBG:20:3213861920:74100d20:0018: Released relay_mutex on in 0x6d6e79e8
(SAL/channel-np.c:sal_np_midpath_relay:1791)
DBG:21:3213861935:74100d20:0018: RELAY notify(0x6d6ce840, 2, 0,
socket=0x621bb58/0x621bb58) (SAL/channel-np.c:sal_np_relay_cb:1574)
DBG:22:3213861949:74100d20:0018: sal_np_relay_notify: signaling condvar
(SAL/channel-np.c:sal_np_relay_cb:1604)
DBG:23:3213861961:74100d20:0018: Acquired relay_mutex on out 0x764a32f8
(SAL/channel-np.c:sal_np_midpath_relay:1822)
DBG:24:3213861973:74100d20:0018: Released relay_mutex on out 0x764a32f8
(SAL/channel-np.c:sal_np_midpath_relay:1838)
DBG:25:3213861991:74100d20:0018: Succeeded in detaching relay
(SAL/channel-np.c:sal_np_midpath_relay:1907)
DBG:26:3213862012:74100d20:0018: Finish external handoff for client_ch
0x6d6ce7c0 (aware.c:aware_dispatch_request:497)
DBG:27:3213862026:74100d20:0018: + freeing ctx
(CONN/aware.c:aware_connection_clean_up:251)
DBG:28:3213862042:74100d20:0018: free aware ctx
(aware_mem.c:mem_aware_ctx_free:64)
DBG:29:3213862058:74100d20:0018: Fiber exit - client_ch 0x6d6ce7c0
(aware.c:run_aware_fiber:1339)
DBG:30:3213862070:74100d20:0018: Fiber 0x74100d20 finished leaving 4 more
(FIBERS/fibers-jumpstart.c:_fiber_jumpstart:64)
DBG:31:3213862083:74100d20:0018: Exiting fiber 0x74100d20
(FIBERS/fibers.c:fiber__kill:1257)
DBG:32:3213862099:74100d20:0018: Fiber 0x74100d20 terminated, 3 more
(FIBERS/fibers.c:fiber__kill:1330)
```

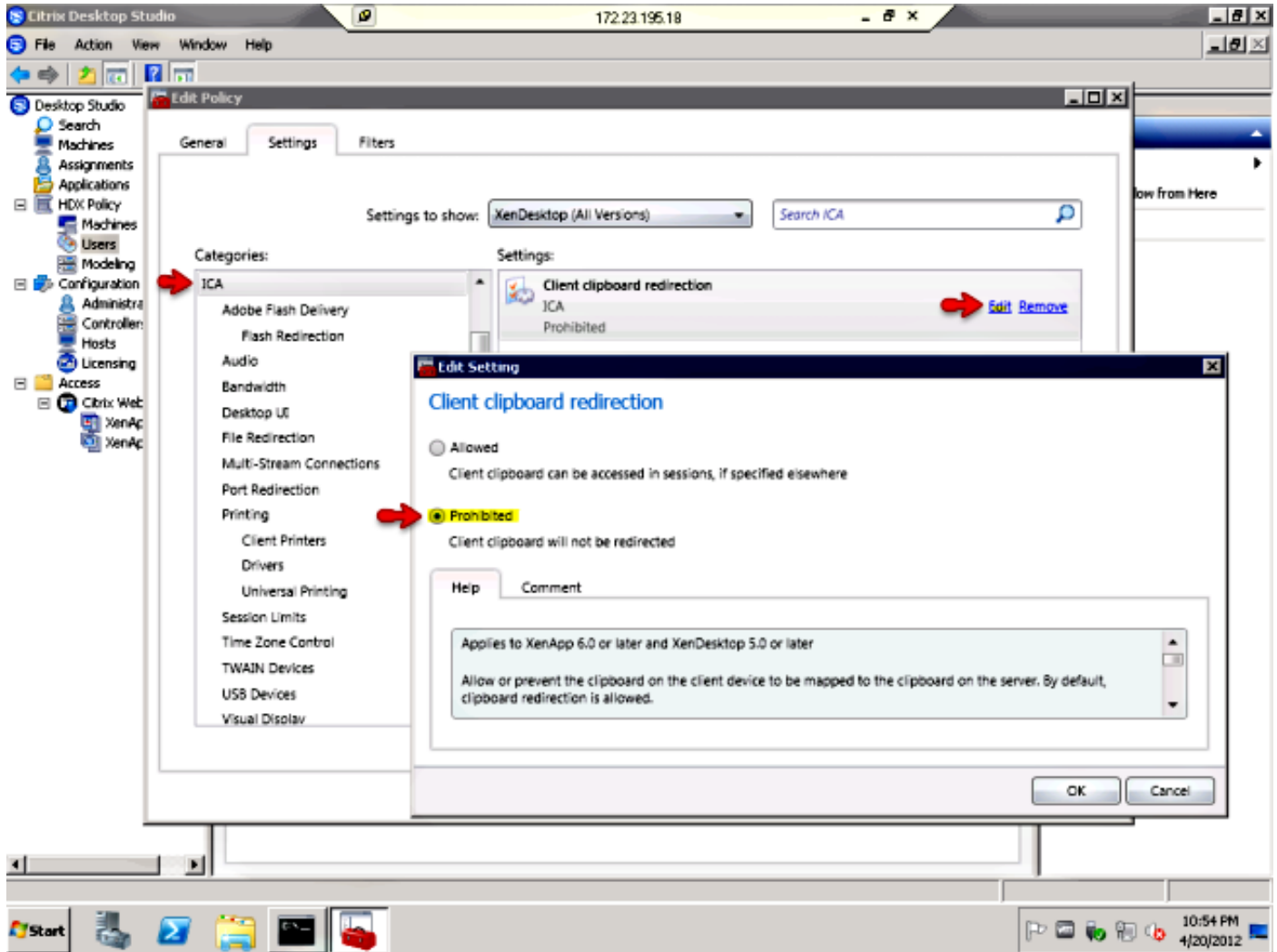
Utilice los comandos debug de autenticación genérica para depurar problemas de autenticación, tales como:

```
debug aaa commondebug ldapdebug radiusdebug sdi
```

Preguntas frecuentes (FAQ)

P. ¿Esta nueva función conserva los controles granulares configurados en XenServer (por ejemplo, controles como Client Drive Redirection, Client Printer Redirection, Client Clip Board Redirection y Client USB devices redirection)?

A. Estos parámetros se definen en XenServer y forman parte del archivo ICA. El ASA no modifica estos parámetros. Por lo tanto, la configuración que tiene en XenApp o XenDesktop se refleja en el cliente.



P. ¿El ASA tiene un control granular de la conexión ICA, como para evitar cortar y pegar, y controlar la redirección de la impresora, unidad, portapapeles o USB?

A. El ASA no modifica esas configuraciones. Por lo tanto, la configuración que tiene en XenApp o XenDesktop se refleja en el cliente Receptor. Cisco es consciente de la brecha existente entre las funciones, ya que su competencia (Juniper SA y Citrix CAG) puede evitar el corte y la pasta, independientemente de la configuración de XenApp.

P. ¿El servidor Citrix del escaparate funciona con ASA como proxy?

A. Sí, esta función no se admite. Se archivó la solicitud de mejora [CSCug18734](#) para agregar soporte para estos tipos de servidores. La compatibilidad con SSO de la versión 2.0 de Storefront se agrega como parte de la compatibilidad con XenDesktop. Todas las funciones antiguas de Citrix se admiten en la versión 2.0 de Storefront (XenApp y XenDesktop). Las funciones

relacionadas con el controlador de aplicaciones no se soportan a través del ASA.

Cuando configure el ASA para Citrix Receiver, asegúrese de especificar la ruta completa al servicio XML que se ejecuta en el escaparate, por ejemplo, <http://storefront.cisco.com/Citrix/storefrontweb/pnagent/>.

En las versiones que no tienen la corrección para [CSCug18734](#) y que tienen **debug webvpn citrix** habilitado, si intenta acceder a un servidor Storefront, verá esto en las depuraciones:

```
-----8<-----  
Received config.xml request  
+++ UNKNOWN EXCEPTION CAUGHT  
Terminating session for user [test]  
-----8<-----
```

P. Aunque el servidor Citrix ha habilitado y configurado el servicio XML, el error **+++ UNKNOWN EXCEPTION CAUGHT** sigue mostrándose. Esto solía funcionar. ¿Qué podría estar mal?

A. Esto puede ocurrir cuando AnyConnect Essentials está habilitado en ASA, como se muestra aquí:

```
webvpn  
  enable outside  
  anyconnect-essentials
```

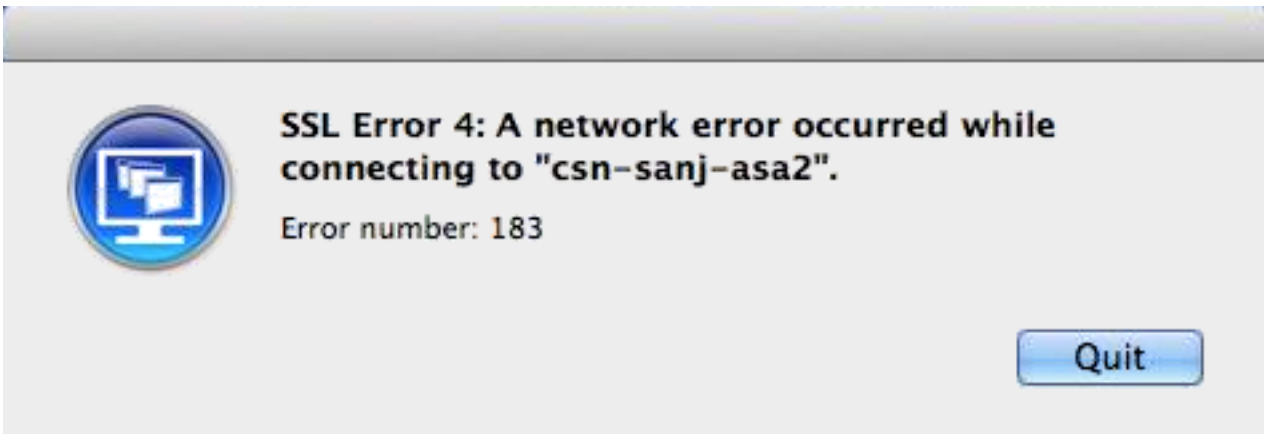
AnyConnect Essentials se utiliza para habilitar solo la compatibilidad completa con el cliente en el ASA, y esto inhabilita la capacidad del ASA para procesar los intentos de conexión sin cliente. Cuando esto sucede, si tiene **debug webvpn transform request** y **debug webvpn citrix** habilitados, entonces verá lo siguiente:

```
Received config.xml request  
DBG:29:4089679874:74100d20:9902: Finished with hooks  
(aware.c:aware_dispatch_request:389)  
DBG:30:4089679886:74100d20:9902: => handoff (AWARE_HOOK_INTERNAL_HANDOFF)  
(aware.c:aware_dispatch_request:508)  
DBG:31:4089679900:74100d20:9902: in process request  
(proxy.c:process_request:239)  
DBG:32:4089679950:74100d20:9902: Load proxy settings  
(ucte_policy.c:ucte_get_ctx_settings:690)  
DBG:33:4089679965:74100d20:9902: Load proxy settings  
(ucte_policy.c:ucte_get_ctx_settings:720)  
DBG:34:4089680019:74100d20:9902: parse_req_headers(client_fd, p_req) ;  
(proxy.c:process_request:275)  
DBG:35:4089680038:74100d20:9902: # req  
(parse_req_headers.re2c:parse_req_headers:1269)  
DBG:36:4089680049:74100d20:9902: # ver: cursor = 0x747e5a9e; lim = 0x747e5d0f  
(parse_req_headers.re2c:parse_req_headers:1383)  
DBG:37:4089680064:74100d20:9902: # ver: cursor = 0x747e5a9f; lim = 0x747e5d0f  
(parse_req_headers.re2c:parse_req_headers:1383)  
DBG:38:4089680077:74100d20:9902: Request: [GET /Citrix/pnagent/config.xml HTTP/1.1]:  
39 (parse_req_headers.re2c:parse_req_headers:1399)  
.  
.  
.  
DBG:96:4089680705:74100d20:9902: Clientless WebVPN is not enabled.  
(proxy.c:process_request:384)  
.  
.
```

```
DBG:31:4089681295:74100d20:9902: fwrite(0 ? ==> 90): [Connection:
close%0d%0aCache-Control: no-store%0d%0aContent-Type: text/html%0d%0aContent-Length:
0%0d%0a%0d%0a]: 90 (SAL/sal-stdio.c:sal_fwrite:92)
+++ UNKNOWN EXCEPTION CAUGHT
Terminating session for user [test.user]
```

P. Si recibe este mensaje de error **Error SSL 4: Número de error: 183**, ¿qué deberías hacer?

A. Este error aparece cuando se permite la conexión al agente XML (servidor XenDesktop), pero se bloquean los puertos 1494 y 2598 al conjunto real de XenDesktop. Puede depurar si habilita todos los puertos y luego reduce los puertos requeridos.



Para que XenDesktop funcione a través de la red sin cliente, si hay algún firewall intermedio entre el ASA (interno) y el servidor XenDesktop, asegúrese de que los puertos 443, 1494, 2598 y 80 estén abiertos en ese firewall. Además, asegúrese de que los puertos estén abiertos tanto para el servidor XenDesktop como para el grupo de escritorios XenDesktops.

P. ¿El ASA admite conexiones SSL que se originan en un cliente Citrix Receiver independiente desde una plataforma Microsoft Windows/Macintosh OSX, al igual que usted utiliza AnyConnect o Cisco VPN Client?

A. Actualmente, los receptores Citrix independientes de los escritorios se admiten únicamente a través de túnel inteligente (sin cliente).

[CSCum85649](#) ENH: Admita receptores Citrix independientes de escritorio a ASA

Se trata de un error de mejora para admitir una conexión Citrix Receiver independiente al ASA sin necesidad de iniciar sesión en el túnel inteligente o en el portal inicial, como ocurre con el Citrix Receiver móvil con ASA como gateway de acceso. Actualmente, ASA envía un reinicio después del intercambio de señales inicial a un receptor Citrix independiente (con el uso de la versión 4.1 más reciente para Windows y con el mismo comportamiento en otras plataformas también).