Esempio di configurazione dell'accesso senza client ASA con Citrix Receiver su dispositivi mobili

Sommario

Introduzione

In questo documento viene descritto come configurare Cisco Adaptive Security Appliance (ASA) come proxy per Citrix Receiver sui dispositivi mobili. Questa funzionalità fornisce accesso remoto sicuro per l'applicazione Citrix Receiver in esecuzione sui dispositivi mobili ai server XenApp/XenDesktop Virtual Desktop Infrastructure (VDI) tramite ASA, eliminando la necessità di Citrix Access Gateway.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Ricevitore Citrix
- WebVPN senza client

Requisiti dell'infrastruttura:

- L'appliance ASA deve avere un certificato di identità valido considerato attendibile dai dispositivi mobili.
- L'interfaccia XML deve essere abilitata e configurata sul server Citrix XenApp/XenDesktop/Storefront.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Dispositivi mobili supportati

Questo è un elenco dei dispositivi mobili supportati:

- iPad - Citrix Receiver versione 4.x o successiva
- iPhone/iTouch - Citrix Receiver versione 4.x o successiva
- Telefono Android 2.x - Citrix Receiver versione 2.x o successiva
- Tablet Android 3.x - Citrix Receiver versione 2.x o successiva
- Android 4.0/4.1 Phone/Tablet - Citrix Receiver versione 2.x o successiva

Demo

Per una dimostrazione di questo processo, visitare la seguente pagina Web:

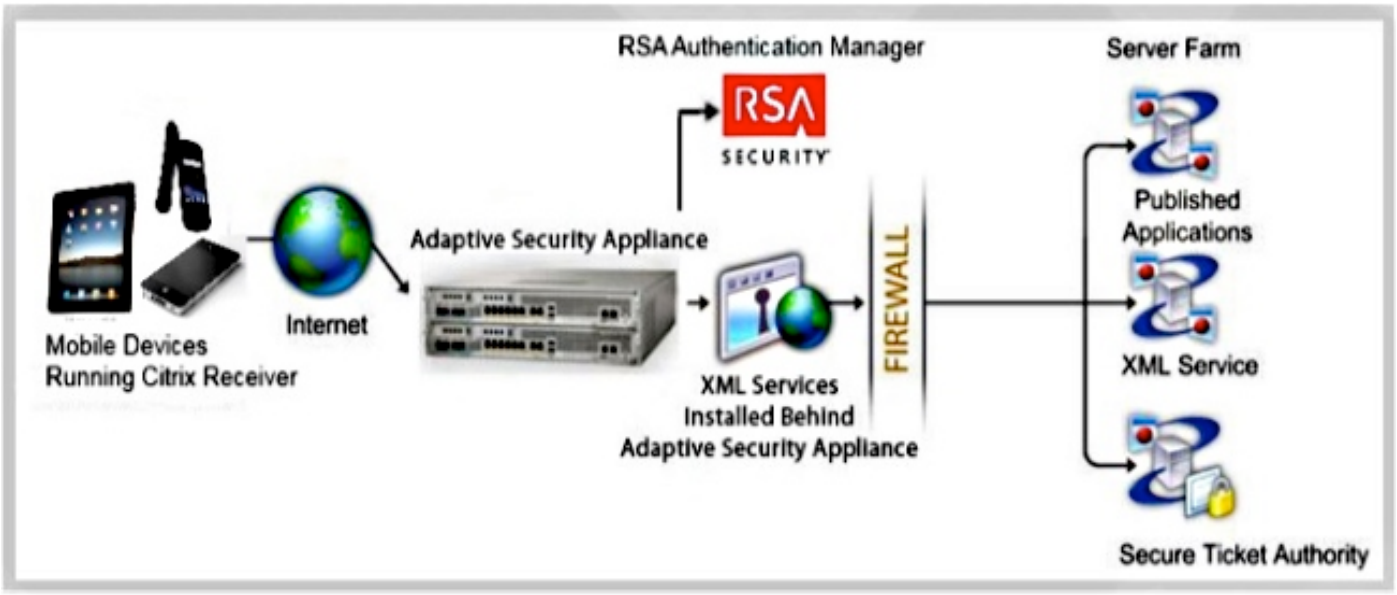
Cisco ASA 9.0 Citrix Mobile Receiver Demo proxy

Premesse

Il gateway di accesso Citrix (CAG) era tradizionalmente l'unico modo per fornire un accesso remoto sicuro alle risorse Citrix virtualizzate (desktop e applicazioni). In un'implementazione tipica, un dispositivo di questo tipo si troverebbe dietro il firewall in una zona demilitarizzata (DMZ). Questa funzionalità aggiunge la funzionalità ASA per supportare connessioni remote sicure alle risorse virtuali dai dispositivi mobili.

Le implementazioni tradizionali richiedono la presenza di un CAG, che in genere si trova dietro il firewall:

Con l'appliance ASA, le connessioni alle risorse Citrix interne sono possibili senza CAG:



Affinché l'appliance ASA possa fungere da proxy per le connessioni da un ricevitore Citrix a un server Citrix, l'appliance ASA rappresenta Citrix Access.

Gateway:

1. Quando si tenta di connettersi a una risorsa virtualizzata Citrix, non è necessario fornire l'indirizzo/le credenziali di Citrix Server; immettere l'indirizzo IP e le credenziali della VPN SSL (Secure Sockets Layer) dell'ASA.

2. Per gestire le richieste, viene creato un nuovo gestore ASA che include le richieste di autenticazione dei ricevitori Citrix (richieste HTTPS con una stringa agente che si identifica come ricevitore Citrix).

3. Dopo aver verificato le credenziali, il client ricevitore inizia a recuperare le applicazioni autorizzate tramite l'ASA. L'ASA riscrive e invia proxy all'interfaccia di servizio XML del server XenApp o XenDesktop (il servizio XML è un servizio eseguito su un server Citrix che gestisce le richieste relative alle risorse di virtualizzazione).

4. L'appliance ASA si connette e si autentica al server VDI con credenziali preconfigurate (vedere la sezione Configurazione). Quando si inviano le credenziali al server back-end XenApp/XenDesktop, l'ASA nasconde sempre la password dell'utente con la codifica Citrix CTX1.

Di seguito è riportato un elenco dei metodi di autenticazione ASA supportati con Citrix Receiver:

- Locale
- Dominio
- RSA SecurID utilizzando il protocollo nativo SDI.
  ASA supporta anche le modalità di richiesta, che includono token successivo, nuovo PIN e PIN scaduto.
- Autenticazione a due fattori (RSA e Lightweight Directory Access Protocol (LDAP))

Limitazioni

- Limitazioni certificato:
  L'autenticazione certificato/smart card non è supportata come metodo di accesso automatico perché queste forme di autenticazione non consentono l'appliance ASA centrale.

  La firma Md5 nei certificati non funziona a causa di un problema di protezione ed è un problema nelle piattaforme iOS. Per ulteriori informazioni, vedere l'errore Receiver for iOS: Errore di connessione. Citrix Receiver non è riuscito a stabilire la connessione con la discussione host remoto.

  Se il nome del soggetto non corrisponde esattamente al nome di dominio completo (FQDN) dell'ASA, anche se il certificato di identità ASA contiene nomi alternativi del soggetto (SAN), la sessione ICA (Independent Computing Architecture) non viene avviata (in base alla versione, è possibile che venga visualizzato l'errore del certificato). Il problema è stato risolto con l'ID bug Cisco CSCuj23632.

- Il client Citrix Receiver accede a un solo server XenApp/XenDesktop alla volta. Di conseguenza, i proxy ASA inviano le richieste anche a uno XenApp/XenDesktop per sessione VPN. L'ASA sceglie il primo XenApp/XenDesktop configurato quando si connette un client Citrix Receiver.

- Il reindirizzamento HTTP non è supportato perché la versione corrente dell'applicazione Citrix Receiver non funziona con i reindirizzamenti.

- Le verifiche dei certificati client, le notifiche di scadenza delle password, Cisco Secure Desktop (CSD) e tutti gli elementi in CSD (non solo Secure Vault) non sono supportati quando si utilizzano client standalone/mobili, in quanto i client dell'infrastruttura di virtualizzazione standalone/mobile non comprendono questi concetti.

Configurazione

Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento

di ricerca dei comandi (solo utenti registrati).

Comandi CLI

Quando si usa il client mobile Citrix Receiver per accedere all'appliance ASA, l'appliance ASA deve connetterla a un server Citrix XenApp o XenDesktop predefinito. A tale scopo, l'amministratore configura l'indirizzo del server Citrix e le credenziali di accesso in Criteri di gruppo o nome utente. Se sono configurati sia la CLI di nome utente che quella di Criteri di gruppo, le impostazioni del nome utente hanno la precedenza su Criteri di gruppo.

```
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:
type - tipo di VDI. Per il ricevitore Citrix, il tipo deve essere **citrix**.
url - URL completo del server XenApp o XenDesktop, che include HTTP o HTTPS, nome host, numero di porta e il percorso del servizio XML. Il nome host e il percorso del servizio XML possono contenere una macro senza client. Se il percorso del servizio XML non viene specificato, viene utilizzato il percorso predefinito **/Citrix/pnagent/**.
username - nome utente utilizzato per accedere al server dell'infrastruttura di virtualizzazione. Può trattarsi di una macro senza client.
password - password utilizzata per accedere al server dell'infrastruttura di virtualizzazione. Può trattarsi di una macro senza client.
dominio: dominio utilizzato per accedere al server dell'infrastruttura di virtualizzazione. Può trattarsi di una macro senza client.

Nota: I server XenAPP sono in genere configurati per l'ascolto della porta 80, quindi VDI deve essere configurato con **HTTP** anziché con **HTTPS.**

Gli utenti di Citrix Mobile Receiver possono selezionare il gruppo di tunnel durante l'autenticazione con l'ASA. La selezione dei gruppi di tunnel consente il supporto di diversi protocolli di autenticazione e server XenApp/XenDesktop per l'accesso VDI. Gli amministratori possono configurare un gruppo di tunnel come predefinito per l'accesso VDI. Questo gruppo di tunnel configurato viene utilizzato quando gli utenti non selezionano un gruppo di tunnel:

```
configure terminal
   webvpn
      [no] application-type  default tunnel-group
```

- *nome_applicazione* - nome applicazione. L'unica applicazione attualmente supportata è **citrix-receiver**.

- *tunnel-group-name*: nome del gruppo di tunnel corrente da utilizzare come predefinito per l'accesso VDI del tipo specificato.

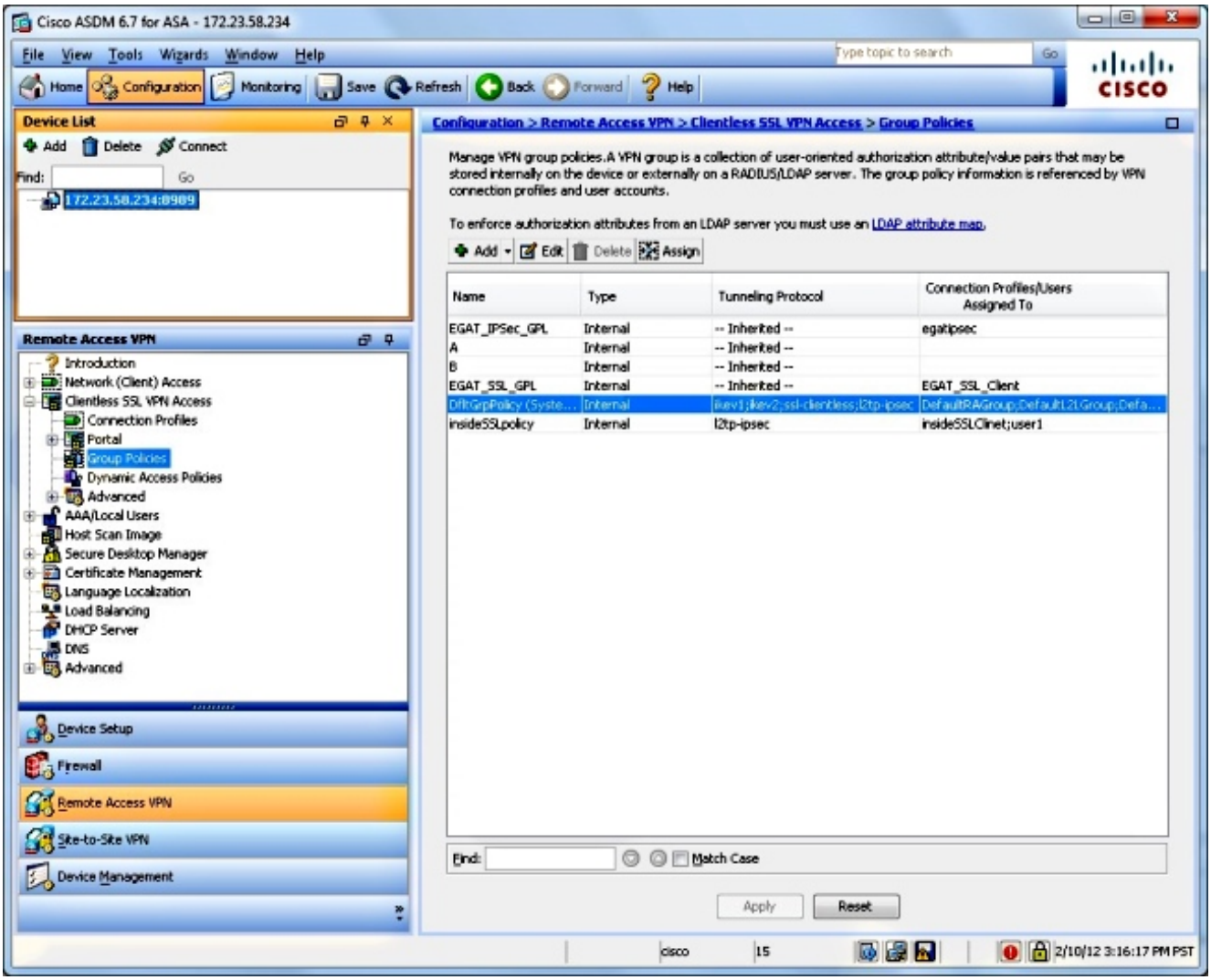
Esempio di configurazione

Di seguito sono riportati alcuni esempi di configurazione VDI validi:

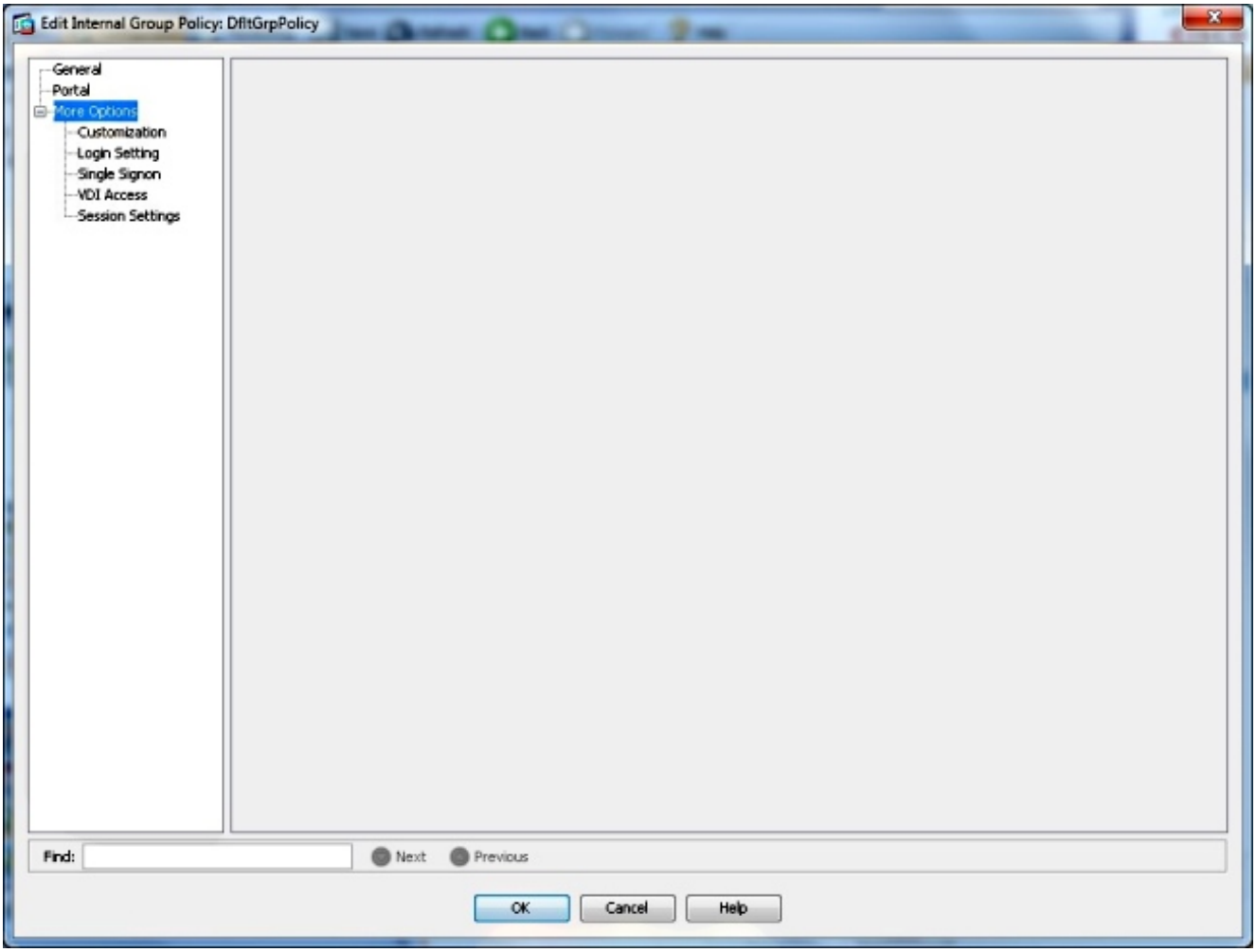
```
vdi type citrix url http://192.168.1.2 domain domain1 username user1 password pass1
vdi type citrix url https://192.168.1.2/Citrix/pnagent1/ domain domain2 username
username2 password password2
vdi type citrix url http://192.168.1.2:8080/Citrix/pnagent3 domain CSCO_WEBVPN_MACRO1
username CSCO_WEBVPN_USERNAME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

Configurazione di Adaptive Security Device Manager (ASDM)

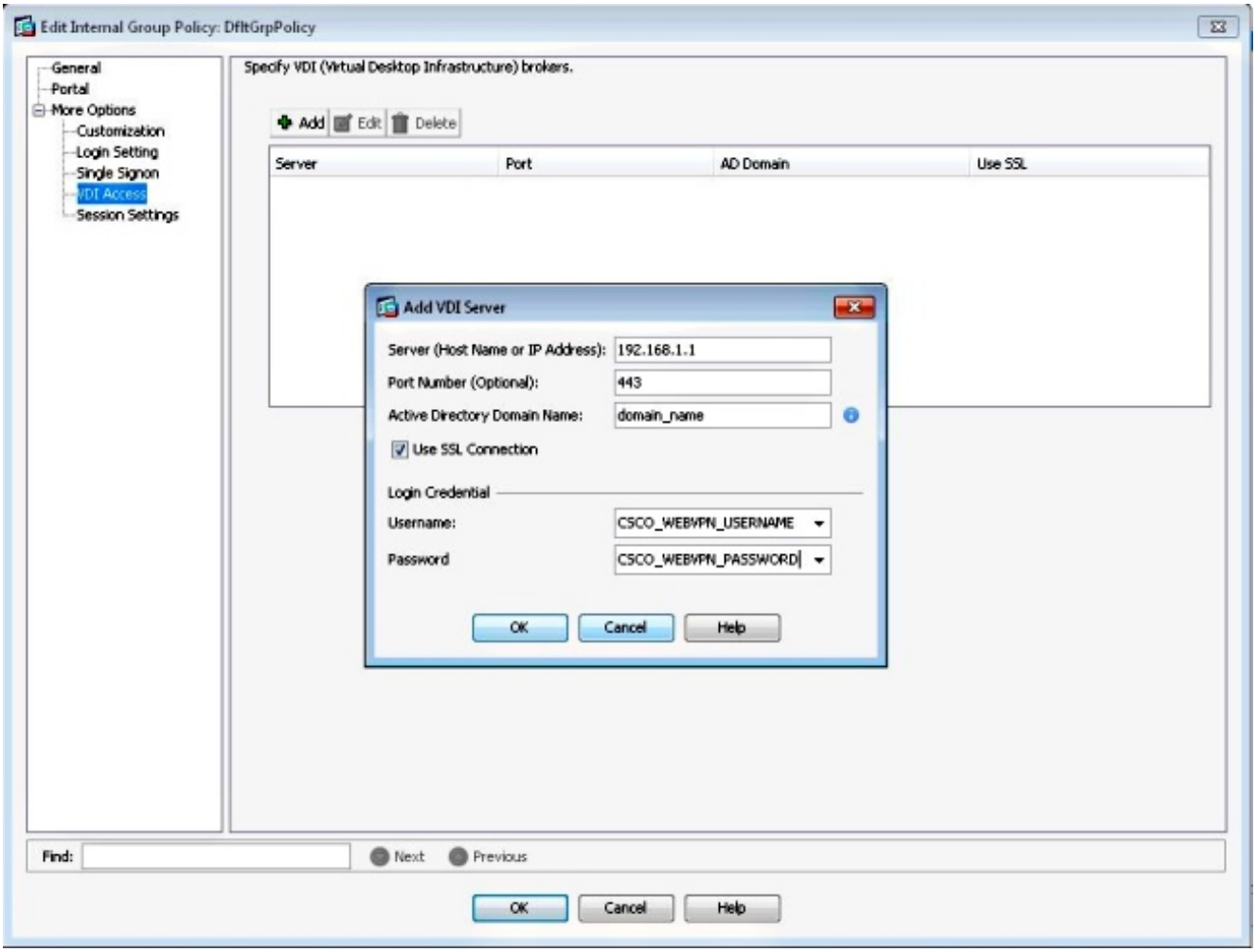
1. Selezionare **Asdm > Configurazione > VPN ad accesso remoto > Accesso VPN SSL senza client > Criteri di gruppo**:

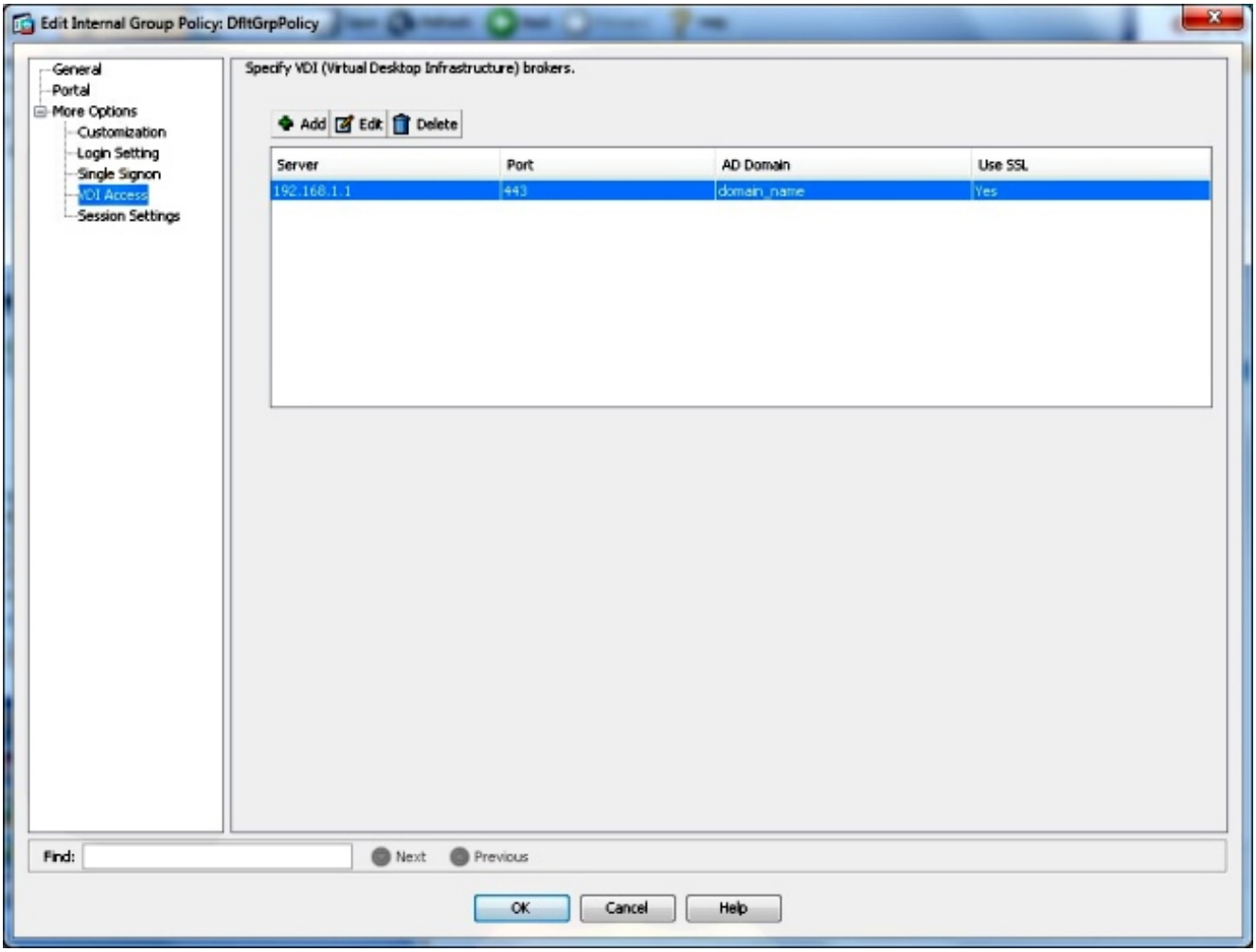


2. Selezionare **Modifica > Altre opzioni > Accesso VDI**:



3. Aggiungere il **server VDI**:


Edit Internal Group Policy: DfltGrpPolicy
General
Portal
More Options
Customization
Login Setting
Single Signon
VDI Access
Session Settings
Specify VDI (Virtual Desktop Infrastructure) brokers.
Add
Edit
Delete
Server
Port
AD Domain
Use SSL
Add VDI Server
Server (Host Name or IP Address):
192.168.1.1
Port Number (Optional):
443
Active Directory Domain Name:
domain_name
Use SSL Connection
Login Credential
Username:
CSCO_WEBVPN_USERNAME
Password
CSCO_WEBVPN_PASSWORD
OK
Cancel
Help
Find:
Next
Previous
OK
Cancel
Help


Edit Internal Group Policy: DfltGrpPolicy
General
Portal
More Options
Customization
Login Setting
Single Signon
VDI Access
Session Settings
Specify VDI (Virtual Desktop Infrastructure) brokers.
Add
Edit
Delete
Server
Port
AD Domain
Use SSL
192.168.1.1
443
domain_name
Yes
Find:
Next
Previous
OK
Cancel
Help

Nota: L'unica modalità supportata è la modalità singola.

Certificati di identità ASA e Autorità di certificazione (CA)

- Affinché Citrix Receiver funzioni con l'ASA, i **dispositivi mobili devono considerare attendibile la CA che ha emesso il certificato di identità dell'ASA**. **Il certificato dell'ASA deve essere emesso per un nome di dominio completo** (ad esempio, clientlessvdi.cisco.com) e NON per l'indirizzo IP dell'ASA. Se il certificato dell'ASA è stato rilasciato da una CA intermedia non presente nell'archivio chiavi del dispositivo mobile, anche la CA intermedia deve essere considerata attendibile.

- Quando Citrix Receiver si connette all'appliance ASA con un certificato non attendibile, viene visualizzato un messaggio di avviso popup che indica se continuare o meno.

- I dispositivi Apple con iOS possono supportare certificati ASA autofirmati, in quanto supportano l'importazione diretta di certificati e CA.

- Sui dispositivi mobili Apple che eseguono iOS, il ricevitore consente la connessione all'ASA e il recupero dell'elenco di applicazioni, se gli avvisi del certificato vengono ignorati. Tuttavia, l'utente potrebbe non essere in grado di avviare le risorse pubblicate finché non viene installato un certificato ASA valido.

- Alcuni dei dispositivi mobili del sistema operativo Android (OS) meno recenti non consentono di importare certificati di terze parti nell'archivio chiavi. Pertanto, affinché un ricevitore Citrix su tali dispositivi Android funzioni con ASA/CAG, l'ASA deve avere un certificato di identità rilasciato dalla CA e incorporato nell'archivio chiavi, ad esempio Verisign o Godaddy.

- Sui dispositivi mobili Android, Citrix Receiver non consente le connessioni all'ASA se il certificato dell'ASA non è presente nell'archivio chiavi del dispositivo.

- I dispositivi Android con OS versione 4.1 e successive supportano l'importazione di certificati e CA e dovrebbero funzionare come descritto in precedenza con iOS.

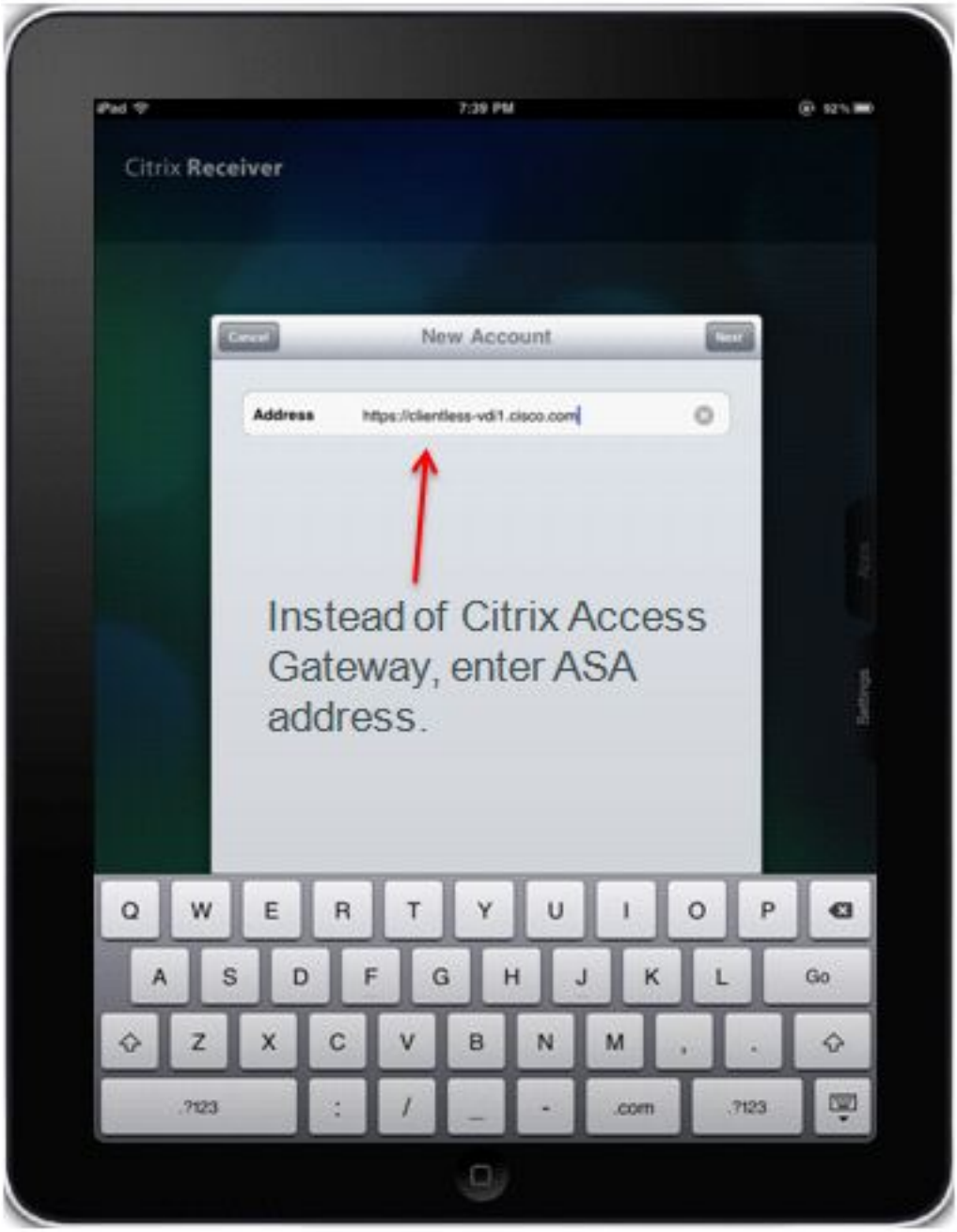
Interfaccia utente finale/Esperienza utente

Aggiungi nuovo account

L'uso di Citrix Receiver per accedere alle risorse virtuali tramite l'ASA offre la stessa esperienza utente di quando si utilizza Citrix Access Gateway.

Se non è configurato alcun server, è necessario configurare una nuova risorsa virtuale.

Specificare l'indirizzo FQDN/IP dell'ASA:



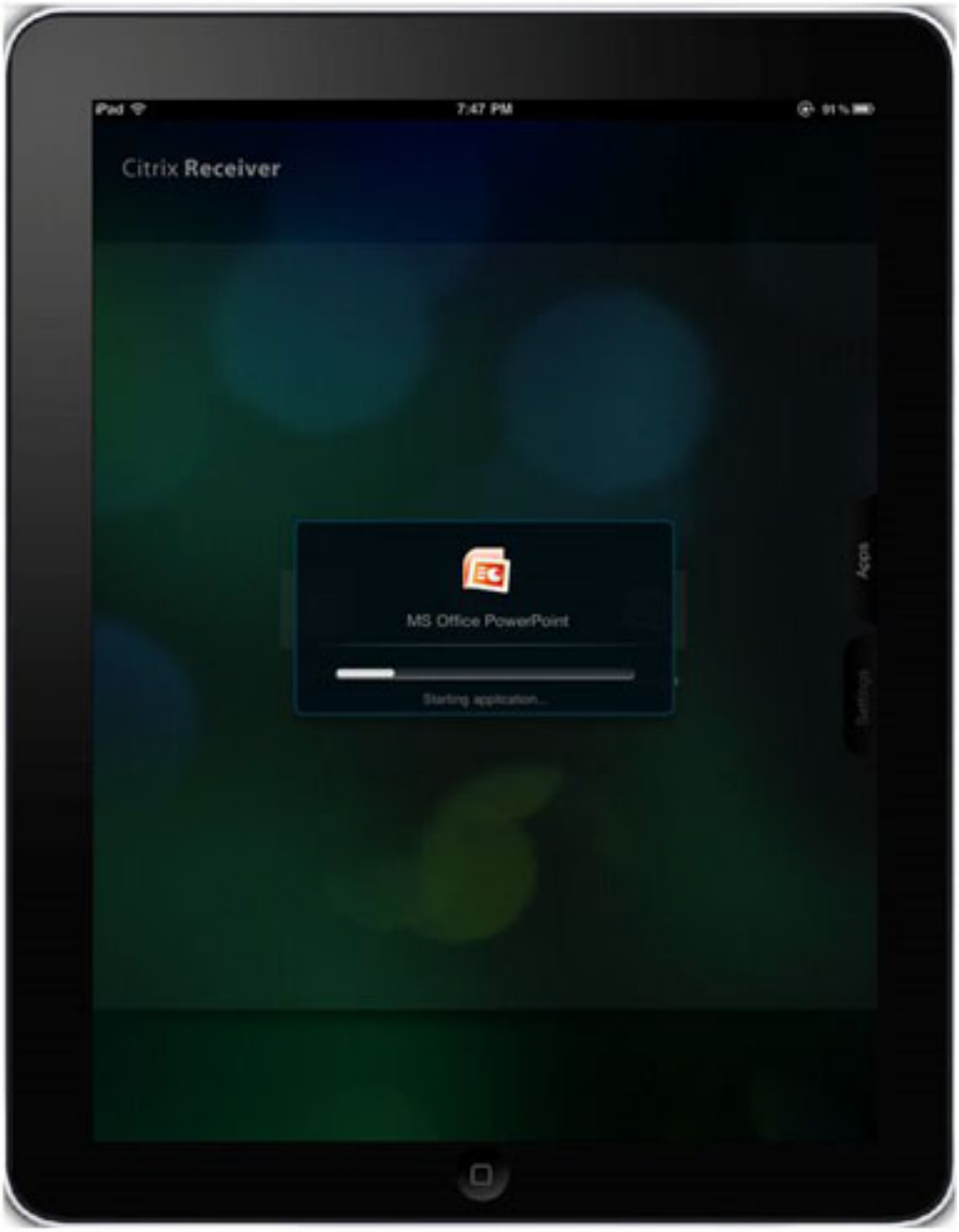
Controllare **Access Gateway**, **Standard Edition** e immettere le credenziali per connettersi all'appliance ASA.

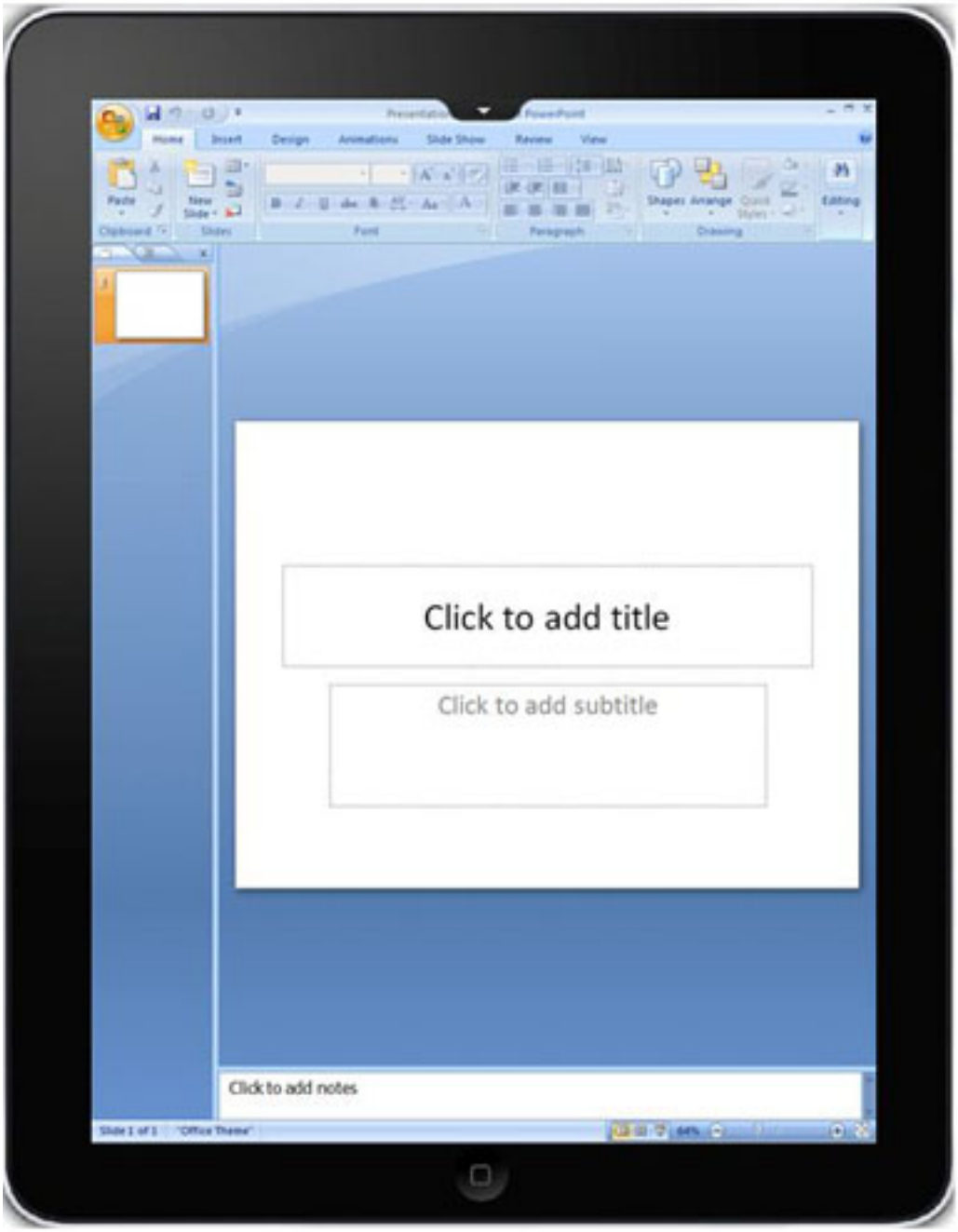
Quando il profilo utente viene salvato, l'applicazione richiede automaticamente le credenziali (ASA) e tenta di eseguire l'accesso.

Quando si esegue l'accesso, viene visualizzato un elenco delle risorse pubblicate.

Èpossibile spostarsi nelle cartelle e fare clic su una risorsa per avviarla.


iPad
7:47 PM
91 %
Citrix Receiver
MS Office 2007
MS Office Excel
MS Office PowerPoint
MS Office Word
Apps
Settings
CALC


iPad
7:47 PM
91 %
Citrix Receiver
MS Office PowerPoint
Starting application...
Apps
Settings



Esci dalla sessione WebVPN

L'applicazione Citrix Receiver non consente di terminare una sessione WebVPN con un'ASA o un CAG connesso. In genere, una sessione di questo tipo viene terminata quando si raggiunge il timeout configurato. Anche se la versione più recente di Citrix Receiver ha un nuovo pulsante di **disconnessione**, non termina la sessione corrente con l'ASA. Chiude invece tutte le applicazioni aperte e visualizza l'elenco dei server configurati. Pertanto, se l'ASA è configurata in modo da usare solo una licenza per utente, i client che usano il pulsante **Disconnetti** non possono accedere di nuovo fino al timeout della sessione.

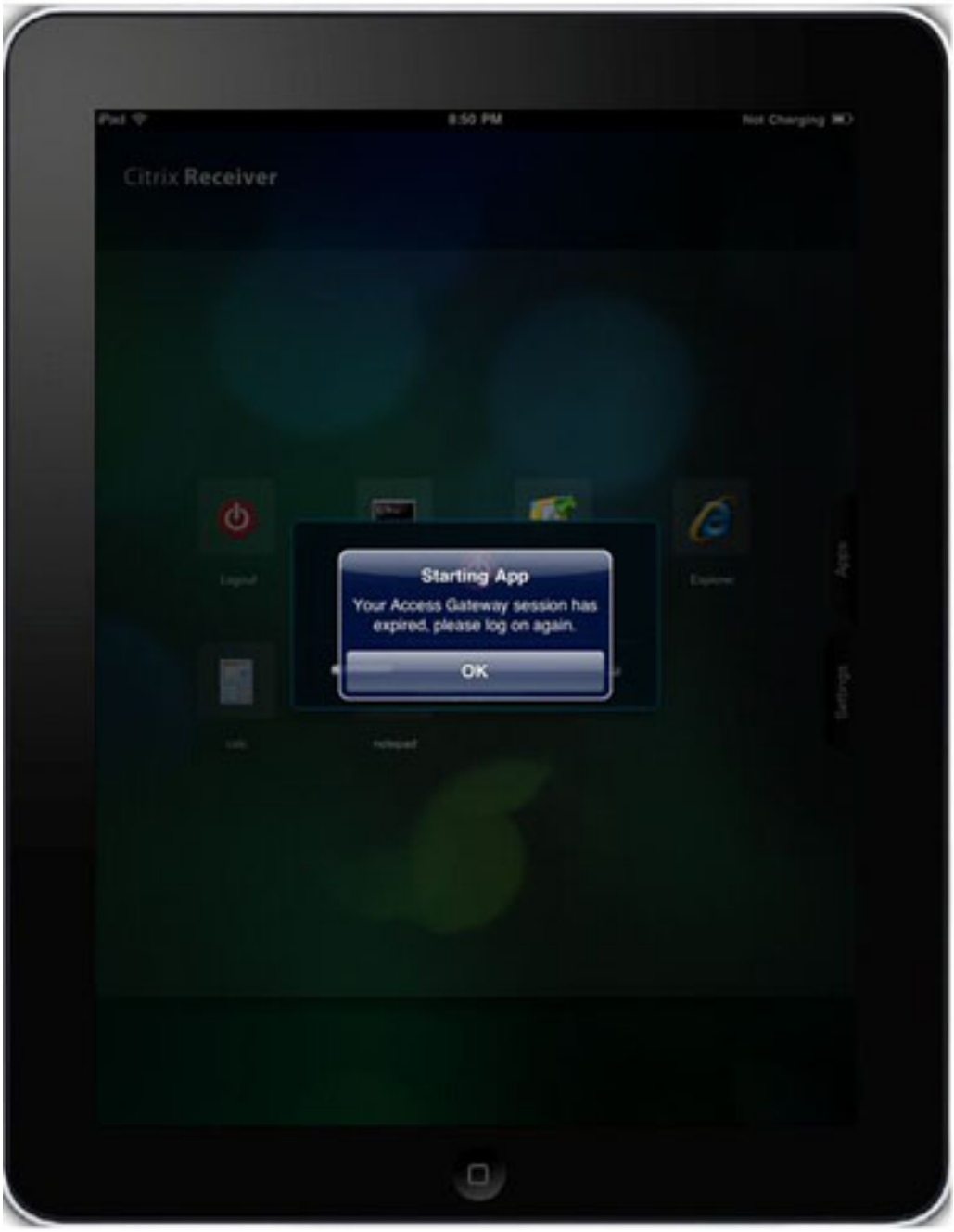
Per consentire agli utenti finali di terminare la sessione WebVPN a loro discrezione e, di conseguenza, rilasciare la licenza ASA, è stata aggiunta una nuova funzionalità alla risorsa **Secure Logoff**.

Questo inserimento viene eseguito ogni volta che Citrix Receiver recupera l'elenco delle risorse pubblicate.

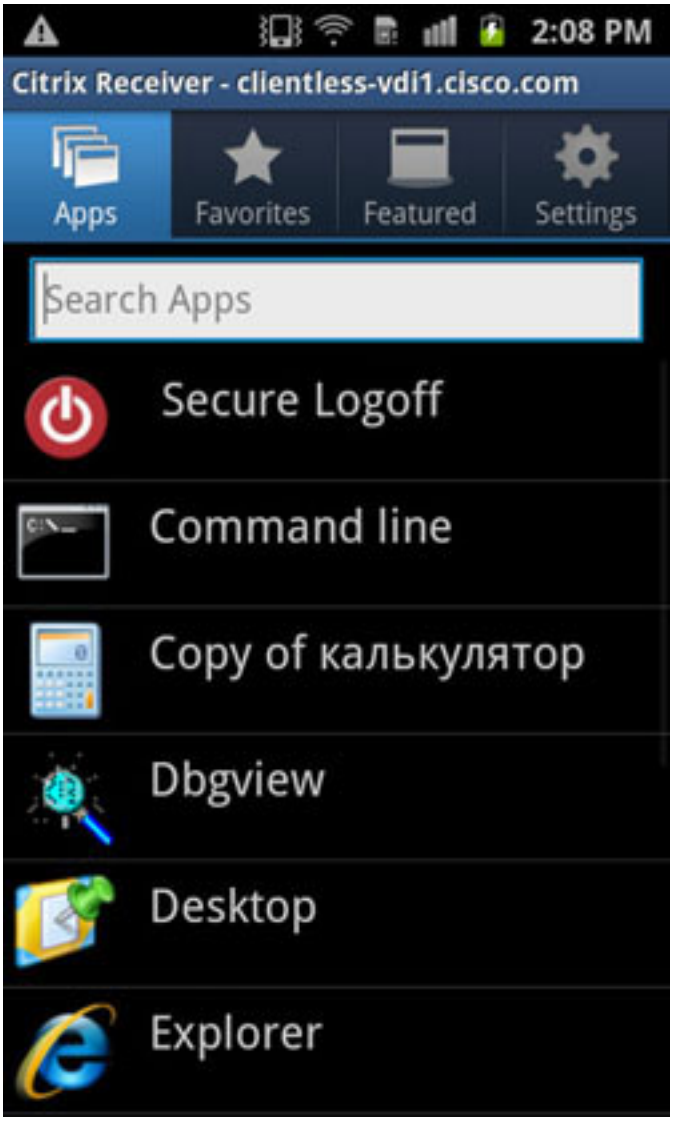
Quando si fa clic sull'applicazione **Secure Logoff**, la sessione tra l'ASA e il ricevitore Citrix viene terminata. Per rilasciare correttamente la licenza ASA, è necessario usare la risorsa **Secure logoff** per terminare la sessione WebVPN, anziché il pulsante di disconnessione Citrix Receiver nativo.

In seguito alla terminazione della sessione vengono visualizzati messaggi diversi a seconda dei dispositivi mobili e della versione di Citrix Receiver. Inoltre, la differenza nel modo in cui l'applicazione Citrix è scritta per diverse piattaforme mobili produce un'esperienza diversa quando si disconnettono i dispositivi Android.

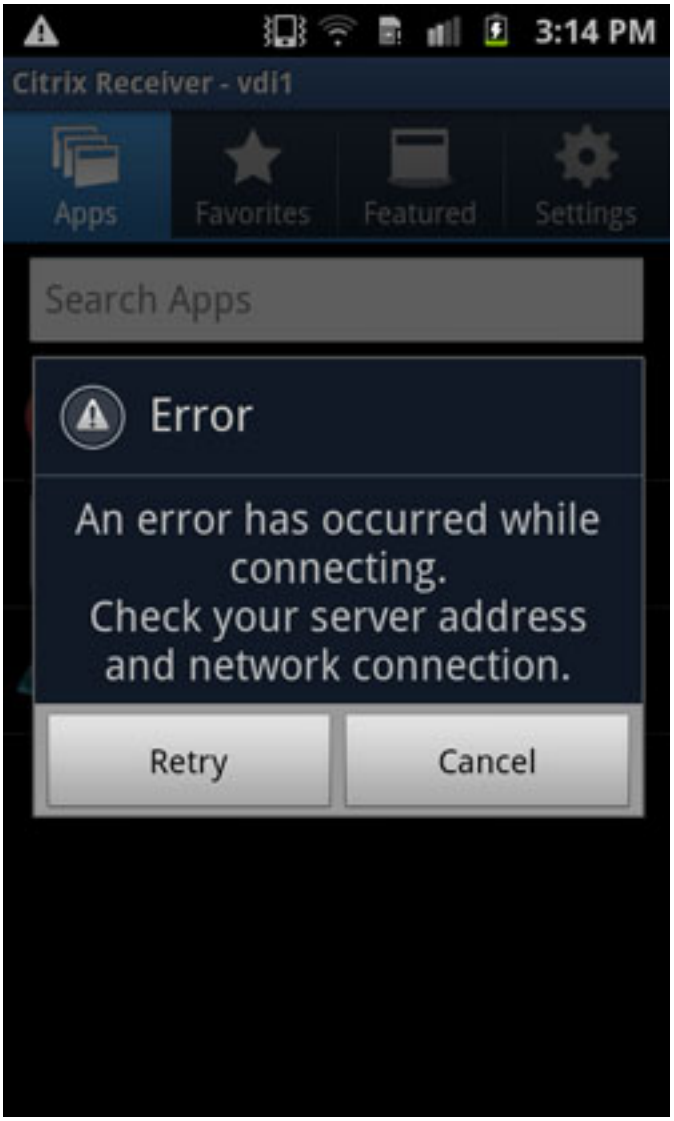
Sull'iPad e sull'iPhone, Citrix Receiver visualizza il messaggio **Il tuo accesso alla sessione del gateway è scaduto. Effettuare nuovamente l'accesso.** Quando si fa clic su **OK**, Citrix Receiver visualizza la schermata con i server configurati.



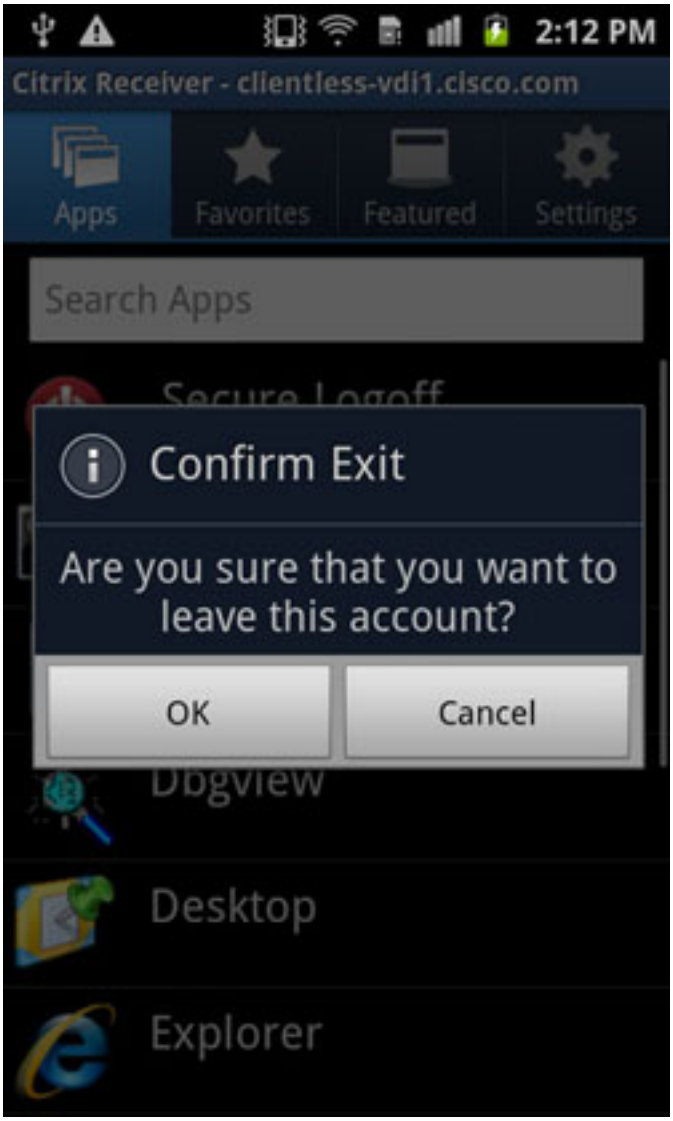
I dispositivi Android visualizzano anche la risorsa **Secure Logoff** inserita.



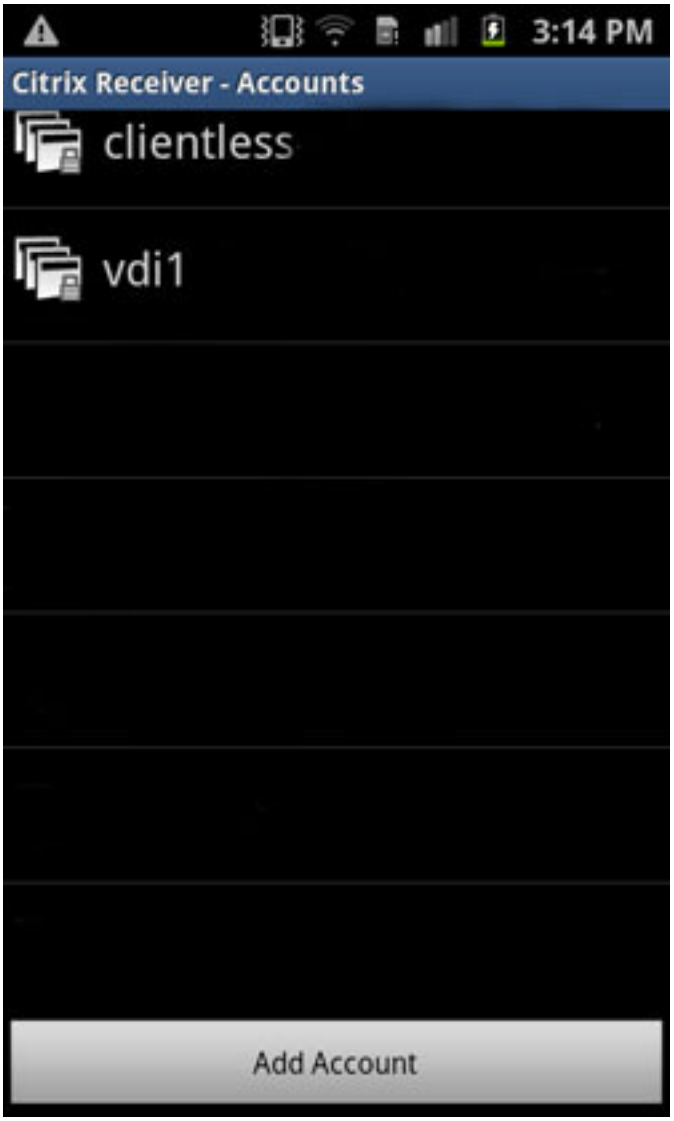
Tuttavia, quando si fa clic sull'applicazione di **disconnessione sicura**, viene visualizzato un errore di connessione di rete.



Anche se a questo punto la sessione WebVPN viene terminata, l'applicazione Citrix Receiver non dispone di messaggi incorporati per informare correttamente l'utente di ulteriori azioni. Questo è il comportamento previsto. Quando questo messaggio di **errore** viene visualizzato come risultato della sessione terminata, si aspetta che tu faccia clic sul pulsante **Annulla**, il pulsante **Indietro** sul dispositivo Android per uscire dall'account corrente, e quindi **OK** quando richiesto se si desidera lasciare questo account.



Dopo aver chiuso l'account corrente, viene visualizzato l'elenco dei server preconfigurati.



Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Debug

> **Nota:** consultare le informazioni importanti sui comandi di debug prima di usare i comandi di debug.

Per visualizzare le informazioni di debug per Citrix Receiver, usare questo comando:

debug webvpn citrix <1-255>

> **Nota:**
> Il livello 1 visualizza condizioni anomale, connessioni non riuscite al server XenApp/XenDesktop ed errori generali.
> Il livello 50 visualizza informazioni sui dati analizzati/riscritti.
> Il livello 255 visualizza tutte le informazioni di debug aggiunte per le connessioni Citrix Receiver.

Non sono stati aggiunti nuovi comandi per l'autenticazione Citrix Receiver. Tuttavia, per visualizzare le transazioni tra il client e l'ASA, è possibile usare questo comando di debug:

debug webvpn transformation request

Per riferimento. questo output mostra i due debug tratti da una connessione funzionante:

```
=~=~=~=~=~=~=~=~=~=~=~=~= PuTTY log 2013.07.24 14:42:38 =~=~=~=~=~=~=~=~=~=~=~=~=
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: Unrexpected
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: Unrexpected
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: SCEPProxy_cb
(aware_webvpn_conf.re2c:SCEPProxy_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)
```

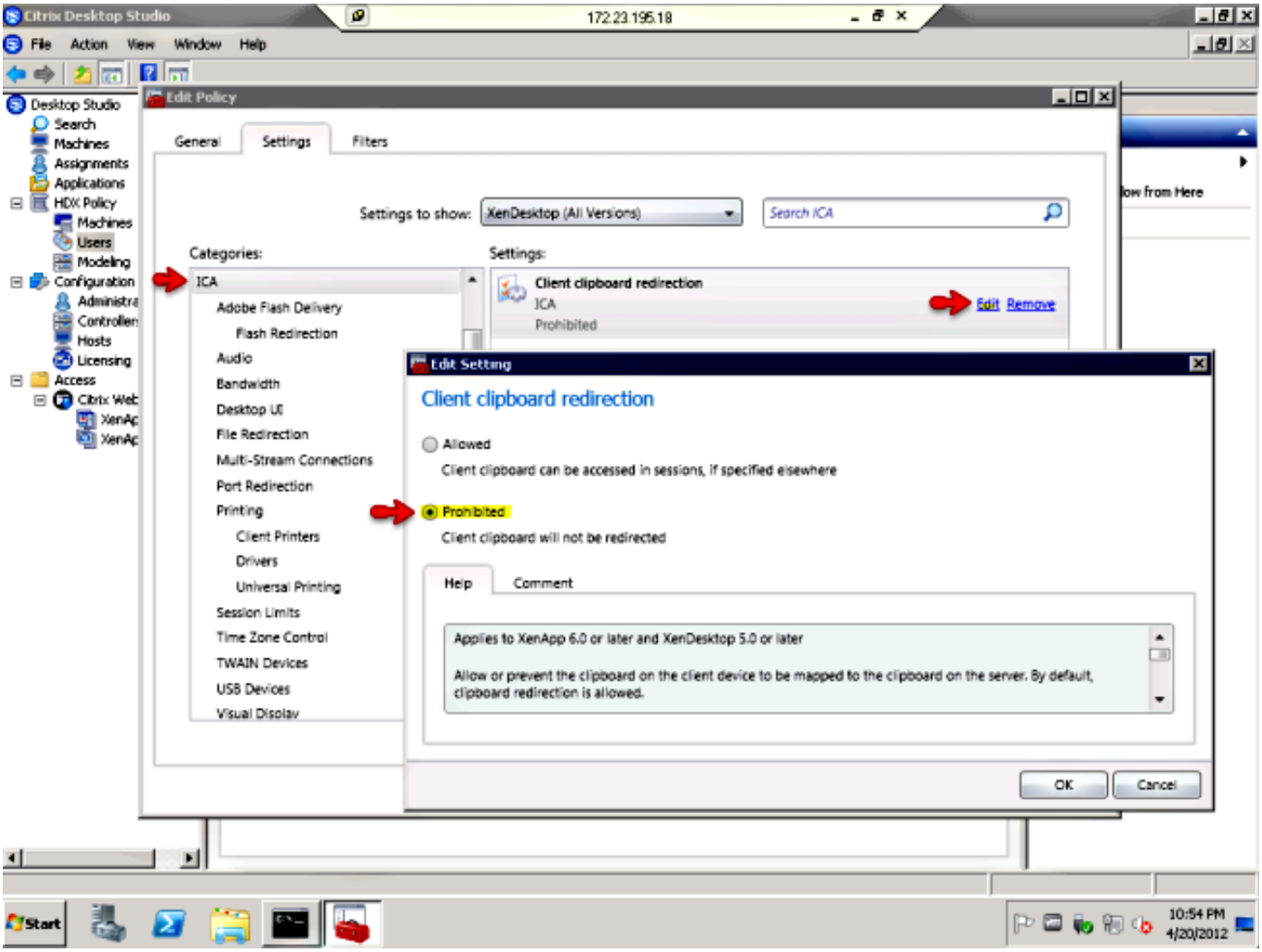
Utilizzare i comandi di debug dell'autenticazione generica per eseguire il debug dei problemi di autenticazione, ad esempio:

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

Domande frequenti (FAQ)

D. Questa nuova funzionalità mantiene i controlli granulari configurati su XenServer (ad esempio, controlli quali il reindirizzamento dell'unità client, il reindirizzamento della stampante client, il reindirizzamento della scheda Clip client e il reindirizzamento dei dispositivi USB client)?

R. Questi parametri sono definiti su XenServer e fanno parte del file ICA. L'appliance ASA non modifica questi parametri. Pertanto, l'impostazione di XenApp o XenDesktop viene riflessa sul client.



D. L'appliance ASA ha un controllo granulare della connessione ICA, ad esempio per impedire operazioni di taglia e incolla e per controllare il reindirizzamento della stampante, dell'unità, degli Appunti o di USB?

R. L'appliance ASA non modifica queste impostazioni. Pertanto, le impostazioni presenti su XenApp o XenDesktop si riflettono sul client di ricezione. Cisco è consapevole del divario di funzionalità perché la concorrenza (Juniper SA e Citrix CAG) è in grado di prevenire le operazioni di taglia e incolla indipendentemente dall'impostazione di XenApp.

D. Il server Storefront Citrix funziona con l'appliance ASA come proxy?

R. Sì, questa funzione non è supportata. La richiesta di miglioramento CSCug18734 è stata archiviata per aggiungere il supporto per questi tipi di server. Il supporto SSO di Storefront versione 2.0 è stato aggiunto come parte del supporto XenDesktop. Tutte le funzionalità Citrix legacy sono supportate in Storefront versione 2.0 (XenApp e XenDesktop). Le funzioni relative al controller dell'applicazione non sono supportate tramite l'ASA.

Quando si configura l'ASA per Citrix Receiver, accertarsi di specificare il percorso completo del servizio XML in esecuzione su Storefront, ad esempio **http://storefront.cisco.com/Citrix/storefrontweb/pnagent/**.

Nelle versioni in cui non è disponibile la correzione per CSCug18734 e in cui è abilitato il comando **debug webvpn citrix**, se si cerca di accedere a un server Storefront, nei debug viene visualizzato quanto segue:

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

D. Anche se il server Citrix ha abilitato e configurato il servizio XML, l'errore **+++ UNKNOWN EXCEPTION CAUGHT** continua a essere visualizzato. Questa funzionava. Cosa potrebbe essere sbagliato?

R. Ciò può verificarsi quando AnyConnect Essentials è abilitato sull'appliance ASA, come mostrato di seguito:

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

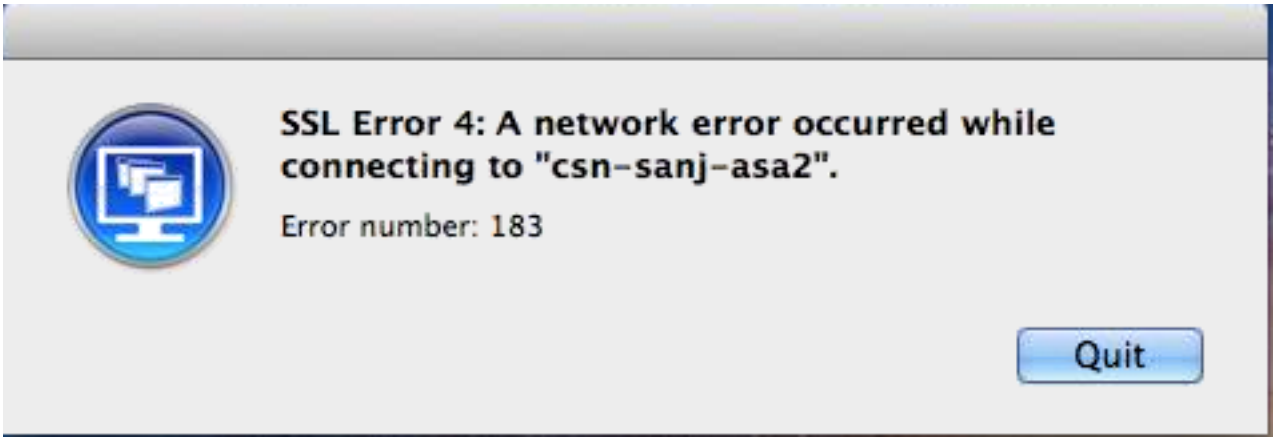
AnyConnect Essentials viene usato per abilitare solo il supporto client completo sull'appliance ASA e questo disabilita la capacità dell'appliance di elaborare tentativi di connessione senza client. In questo caso, se sono state abilitate le **richieste di trasformazione webvpn di debug** e **webvpn citrix di debug**, viene visualizzato quanto segue:

```
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]
```

D. Se viene visualizzato questo messaggio di errore **Errore SSL 4: Numero errore: 183**, cosa devi fare?

R. Questo errore viene visualizzato quando la connessione al broker XML (server XenDesktop) è consentita, ma le porte 1494 e 2598 al pool XenDesktop effettivo sono bloccate. Per eseguire il debug, abilitare tutte le porte e quindi restringere le porte richieste.



Affinché XenDesktop possa funzionare senza client, se esistono firewall intermedi tra l'ASA (interna) e il server XenDesktop, verificare che le porte 443, 1494, 2598 e 80 siano aperte su tale firewall. Verificare inoltre che le porte siano aperte sia per il server XenDesktop che per il pool di desktop Xen.

D. L'appliance ASA supporta connessioni SSL che hanno origine da un client Citrix Receiver standalone da una piattaforma OSX Microsoft Windows/Macintosh, proprio come si usa AnyConnect o il client VPN Cisco?
R. Attualmente, i ricevitori Citrix standalone dai desktop sono supportati solo tramite smart tunnel (senza client).
CSCum85649 ITA: Supporto di Citrix Receiver standalone da desktop ad ASA
Si tratta di un bug relativo a una versione migliorata che supporta una connessione standalone di Citrix Receiver all'appliance ASA senza la necessità di un tunnel intelligente o di un accesso iniziale al portale, come avviene per il Citrix Receiver mobile con l'ASA come gateway di accesso. Al momento, l'ASA invia un messaggio di ripristino dopo l'handshake iniziale a un Citrix Receiver standalone (con l'uso della versione 4.1 più recente per Windows, e ha lo stesso comportamento anche su altre piattaforme).