ASA Clientless Access with the Use of Citrix Receiver on Mobile Devices Configuration Example

Document ID: 116742

Contributed by Sergei Miadzvezhanka, Atri Basu, and Lourdes Gino,
Cisco TAC Engineers.
Mar 26, 2014

Contents

Introduction

This document describes how to configure the Cisco Adaptive Security Appliance (ASA) as a proxy for the Citrix Reciever on mobile devices. This feature provides secure remote access for the Citrix Receiver application that runs on mobile devices to XenApp/XenDesktop Virtual Desktop Infrastructure (VDI) servers through ASA, which eliminates the need for the Citrix Access Gateway.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Citrix Reciever
- Clientless WebVPN

Infrastructure requirements:

- The ASA must have a valid identity certificate that is trusted by mobile devices.
- The XML interface must be enabled and configured on Citrix XenApp/XenDesktop/Storefront server.

Components Used

This document is not restricted to specific software and hardware versions.

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.

Supported Mobile Devices

This is a list of the supported mobile devices:

- iPad − Citrix Receiver Version 4.x or later
- iPhone/iTouch − Citrix Receiver Version 4.x or later
- Android 2.x Phone − Citrix Receiver Version 2.x or later
- Android 3.x Tablet − Citrix Receiver Version 2.x or later
- Android 4.0/4.1 Phone/Tablet − Citrix Receiver Version 2.x or later

Demo

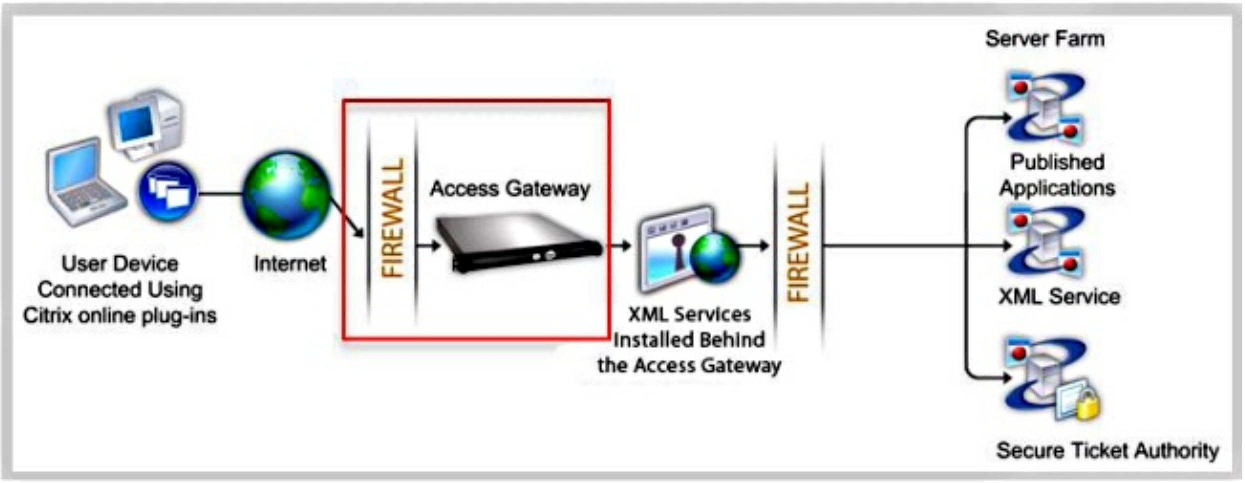
In order to see a demonstration of this process, visit the following web page:

Cisco ASA 9.0 Citrix Mobile Receiver Proxy Demo

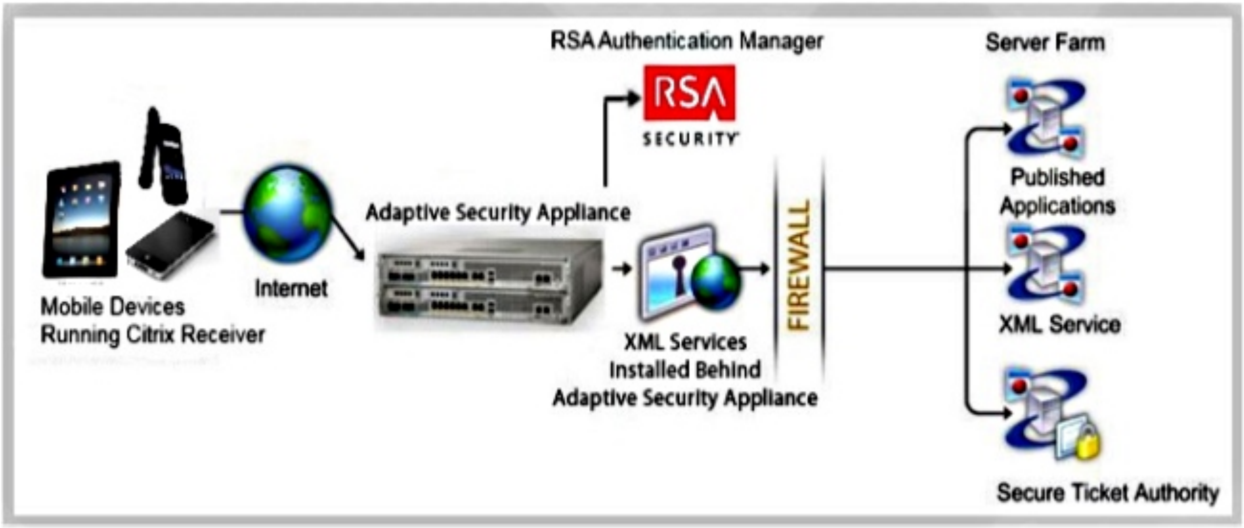
Background Information

The Citrix Access Gateway (CAG) was traditionally the only way to provide secure remote access to virtualized Citrix resources (desktops and applications). In a typical deployment, such a device would be located behind the firewall in a Demilitarized Zone (DMZ). This feature adds ASA functionality in order to support secure remote connections to virtual resources from mobile devices.

Traditional deployments require the presence of a CAG, which is typically located behind the firewall:



With ASA, connections to internal Citrix resources are possible without the CAG:


RSA Authentication Manager
RSA SECURITY
Server Farm
Published Applications
Adaptive Security Appliance
Mobile Devices Running Citrix Receiver
Internet
FIREWALL
XML Service
XML Services Installed Behind Adaptive Security Appliance
Secure Ticket Authority

In order for the ASA to be able to proxy connections from a Citrix Receiver to a Citrix Server, the ASA impersonates Citrix Access.

Gateway:

1. When you try to connect to a Citrix virtualized resource, you do not need to provide the Citrix Server?s address/credentials; instead you enter the ASA's Secure Sockets Layer (SSL) VPN IP address and credentials.
2. A new ASA handler is created in order to handle requests, which includes authentication requests from Citrix Receivers (HTTPS requests with an agent string that identifies itself as the Citrix Receiver).
3. After the ASA has verified the credentials, the Receiver client starts to retrieve entitled applications through the ASA. The ASA rewrites and proxies to the XenApp or XenDesktop Server?s XML service interface (XML service is a service that runs on a Citrix server that services virtualization resource related requests).
4. The ASA connects and authenticates to the VDI server with preconfigured credentials (see the Configure section). When you send credentials to the back−end XenApp/XenDesktop server, the ASA always obfuscates the user password with Citrix CTX1 encoding.

Here is a list of supported ASA authentication methods with the Citrix Receiver:

- Local
- Domain
- RSA SecurID using SDI native protocol.
    - ASA also supports challenge modes, which include next token, new PIN, and expired PIN modes.
- Two factor authentication (RSA and Lightweight Directory Access Protocol (LDAP))

Limitations

- Certificate Limitations:
    - Certificate/Smart Card authentication is not supported as a method of auto sign−on since these forms of authentication do not allow the ASA in the middle.

    - The Md5 signature in the certificates does not work due to a security issue and is a problem on the iOS platforms. More information can be found in the Receiver for iOS Error: Connection Error. Citrix Receiver could not establish connection with remote host discussion.
    - If the Subject name does not fully match the ASA Fully Qualified Domain Name (FQDN), even if the ASA identity certificate contains Subject Alternative Names (SANs), the Independent Computing Architecture (ICA) session will not start (based on the version, the Certificate error could be displayed). This issue has been fixed by Cisco bug ID CSCuj23632.

- The Citrix Receiver client accesses only one XenApp/XenDesktop Server at a time. As a result, the ASA proxies requests to one XenApp/XenDesktop per VPN session also. The ASA picks the first XenApp/XenDesktop configured when a Citrix Receiver client connects.
- The HTTP redirect is not supported since the current version of Citrix Receiver application does not work with redirects.
- Client certificate verifications, password expiration notification, Cisco Secure Desktop (CSD), and everything in CSD (not just Secure Vault) are not supported when standalone/mobile clients are used, because standalone/mobile virtualization infrastructure clients do not understand these concepts.

Configure

Note: Use the Command Lookup Tool (registered customers only) in order to obtain more information on the commands used in this section.

CLI Commands

When you use the Citrix Receiver mobile client in order to log on to the ASA, the ASA must connect it to a predefined Citrix XenApp or a XenDesktop server. In order to accomplish this, the administrator configures the Citrix server?s address and logon credentials under the Group Policy or username. In case both username and group−policy CLI are configured, username settings take precedence over group−policy.

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

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

Note:
type − type of VDI. For the Citrix Receiver, the type must be ***citrix***.
url − full URL of the XenApp or XenDesktop server, which includes HTTP or HTTPS, hostname, port number, as well as the path to the XML service. The hostname and XML service path can contain a clientless macro. If the XML service path is not provided, the default path of ***/Citrix/pnagent/*** is used.
username − username that is used in order to log into the virtualization infrastructure server. This can be a

clientless macro.
password − password that is used in order to log into the virtualization infrastructure server. This can be a clientless macro.
domain − domain that is used in order to log into the virtualization infrastructure server. This can be a clientless macro.

Note: XenAPP servers are usually configured in order to listen to Port 80, so the VDI should be configured with ***HTTP*** instead of ***HTTPS.***

Citrix Mobile Receiver users can select the tunnel group while they authenticate with the ASA. Tunnel group selection allows support of different authentication protocols and XenApp/XenDekstop servers for VDI access. Administrators are able to configure a tunnel group as the default for VDI access. This configured tunnel group is used when users do not make a tunnel group selection:

```
configure terminal
   webvpn
      [no] application−type <application_name> default tunnel−group <tunnel−group−name>
```

- *application_name* − application name. The only application currently supported is ***citrix−receiver***.
- *tunnel−group−name* − name of the current tunnel−group to be used as the default for VDI access of specified type.

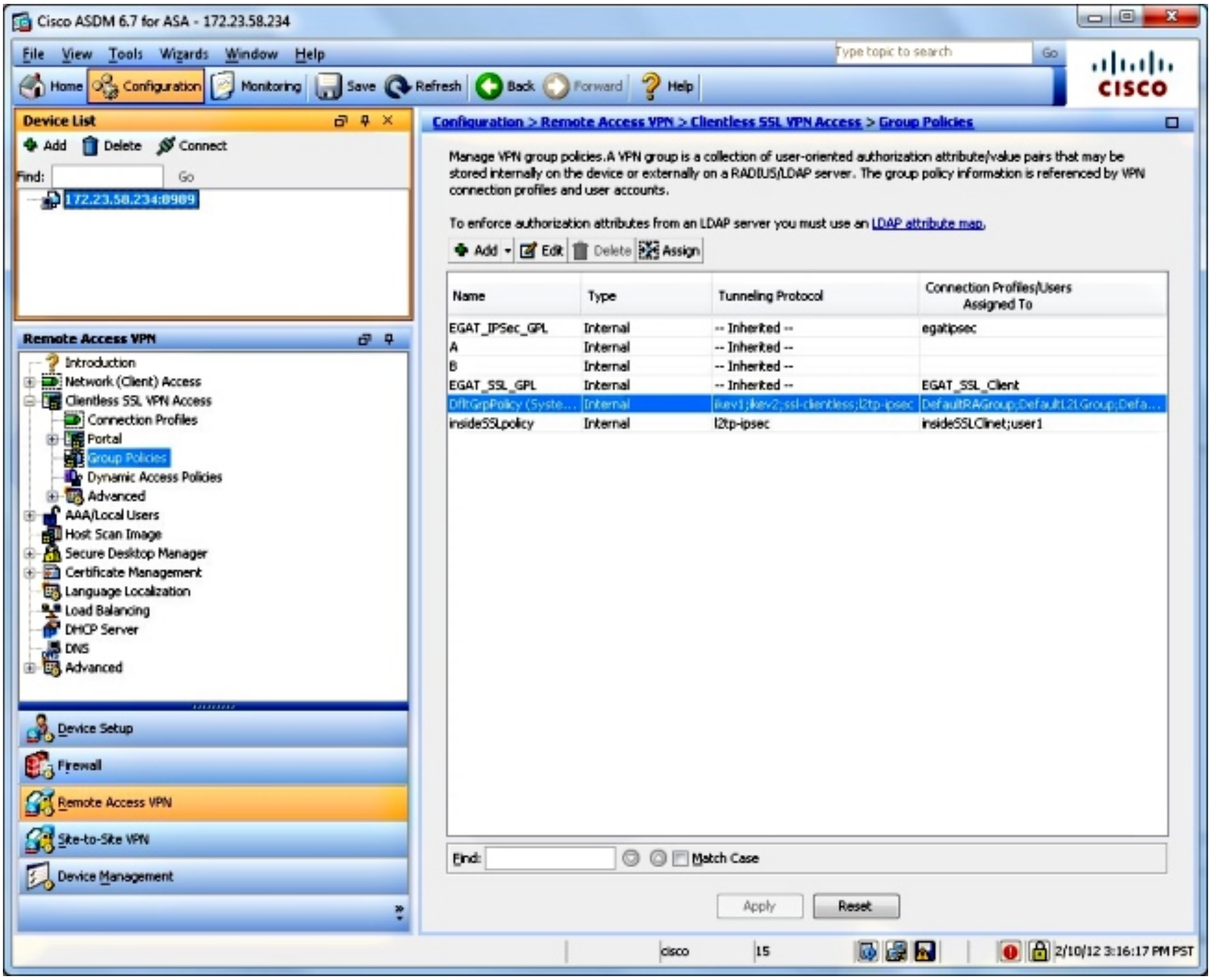
Example Configuration

These are valid VDI configuration examples:

```
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
```

Adaptive Security Device Manager (ASDM) Configuration

1. Navigate to ***Asdm > Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policy***:



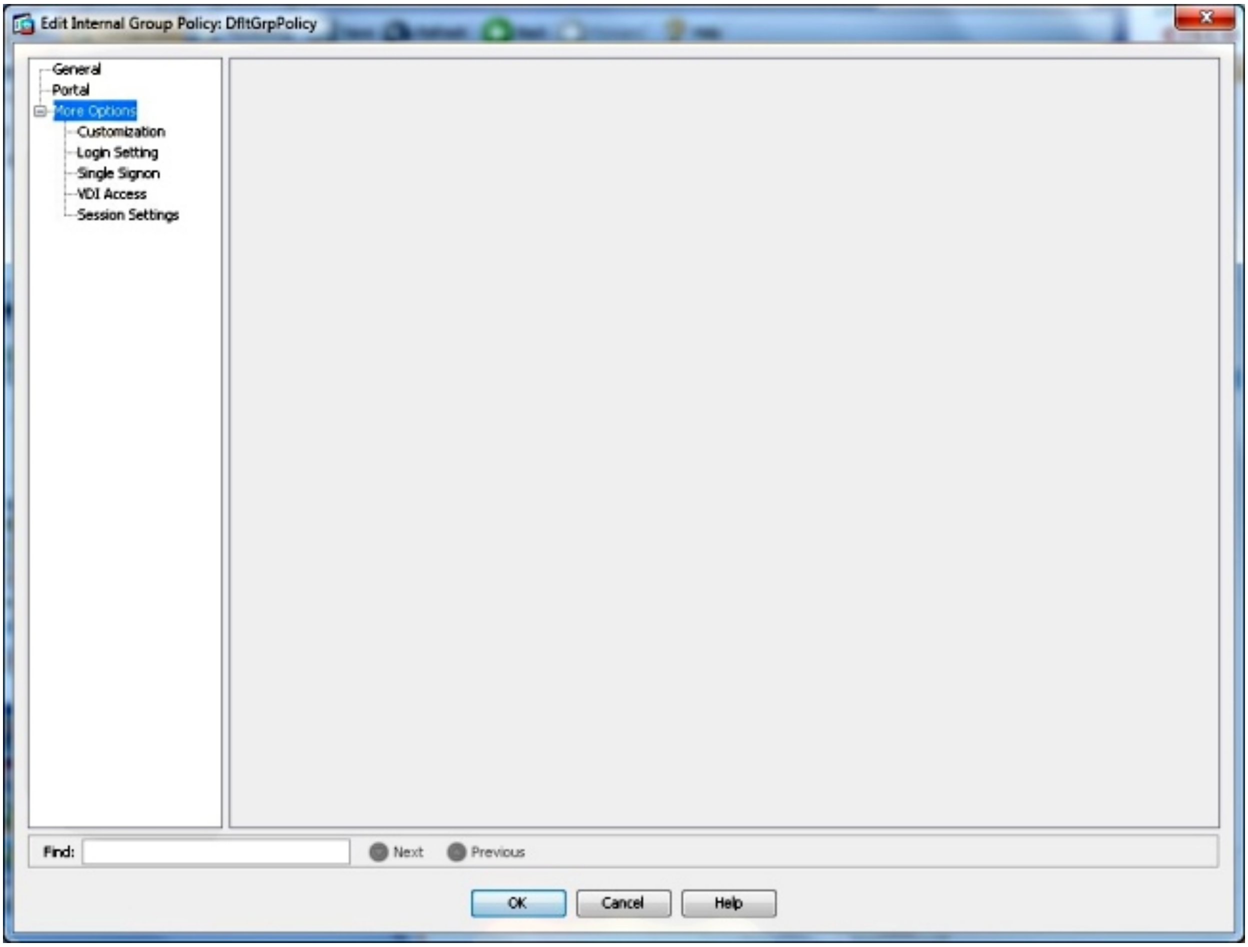
Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies

Manage VPN group policies.A VPN group is a collection of user-oriented authorization attribute/value pairs that may be stored internally on the device or externally on a RADIUS/LDAP server. The group policy information is referenced by VPN connection profiles and user accounts.

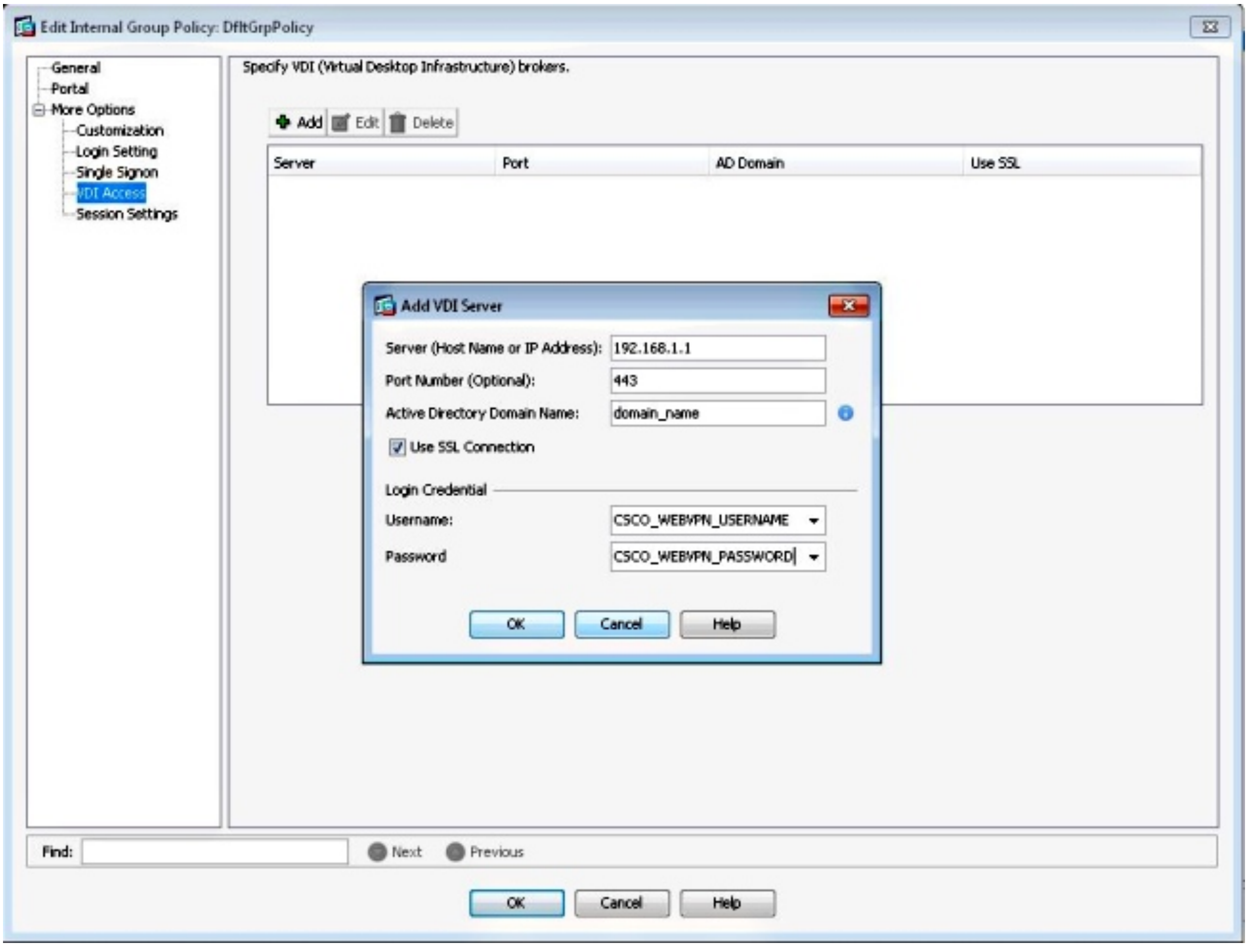
To enforce authorization attributes from an LDAP server you must use an LDAP attribute map.

Name	Type	Tunneling Protocol	Connection Profiles/Users Assigned To
EGAT_IPSec_GPL	Internal	-- Inherited --	egatipsec
A	Internal	-- Inherited --	
B	Internal	-- Inherited --	
EGAT_SSL_GPL	Internal	-- Inherited --	EGAT_SSL_Client
DfltGrpPolicy (Syste...	Internal	ikev1;ikev2;ssl-clientless;l2tp-ipsec	DefaultRAGroup;DefaultL2LGroup;Defa...
insideSSLpolicy	Internal	l2tp-ipsec	insideSSLClinet;user1

2. Navigate to ***Edit*** > ***More Options*** > ***VDI Access***:



3. Add the ***VDI Server***:



Edit Internal Group Policy: DfltGrpPolicy

Specify VDI (Virtual Desktop Infrastructure) brokers.

Server	Port	AD Domain	Use SSL

Add VDI Server

Server (Host Name or IP Address): 192.168.1.1

Port Number (Optional): 443

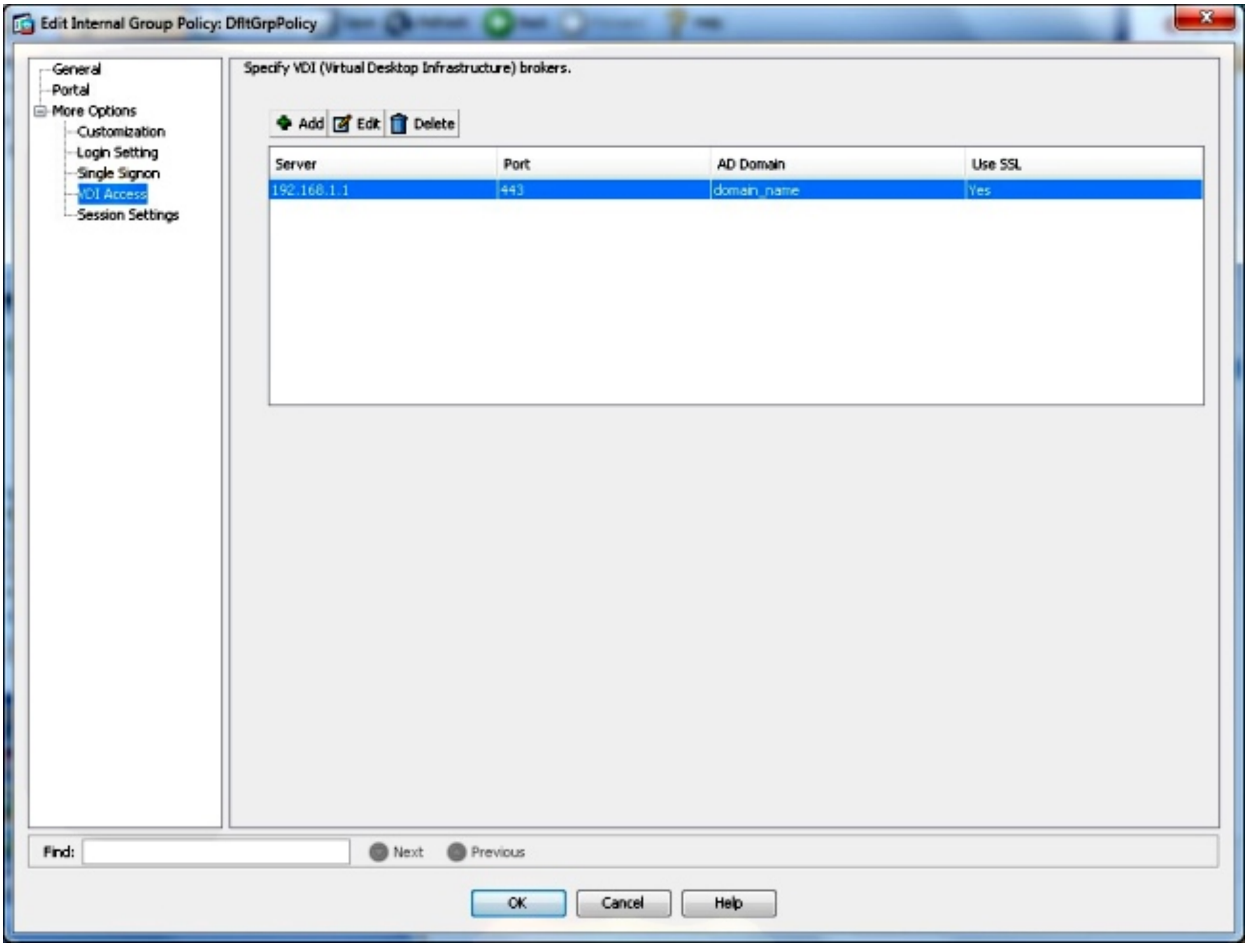
Active Directory Domain Name: domain_name

☑ Use SSL Connection

Login Credential

Username: CSCO_WEBVPN_USERNAME

Password CSCO_WEBVPN_PASSWORD



Specify VDI (Virtual Desktop Infrastructure) brokers.

Server	Port	AD Domain	Use SSL
192.168.1.1	443	domain_name	Yes

Note: The only supported mode is Single Mode.

ASA Identity Certificates and Certificate Authorities (CA)

- In order for Citrix Receiver to work with the ASA, ***mobile devices must trust the CA that issued the ASA's identity certificate***. ***The ASA's certificate must be issued for a fully qualified domain name*** (for example, clientlessvdi.cisco.com), and NOT the IP address of the ASA. If the ASA's certificate has been issued by an intermediate CA that is not present in the key−store of mobile device, the intermediate CA must also be trusted.

- When Citrix Receiver connects to the ASA with an untrusted certificate, the user is prompted with popup warnings whether to continue or not.

- Apple devices running iOS can support self−signed ASA certificates, since they support straightforward import of certificates and CAs.

- On Apple mobile devices that run iOS, the receiver allows connection to the ASA and retrieval of the list of applications, if the certificate warnings are ignored. However, the user might not be able to start any of the published resources until a valid ASA certificate is installed.

- Some of the older Android operating system (OS) mobile devices provide no legitimate way to import third−party certificates into the key store. Therefore, in order for a Citrix Receiver on such Android devices to work with the ASA/CAG, the ASA must have an identity certificate issued by the CA that has been embedded into the key store, for example,Verisign or Godaddy.

- On Android mobile devices, Citrix Receiver does not allow connections to the ASA if the ASA's certificate is not present in the key store of the device.

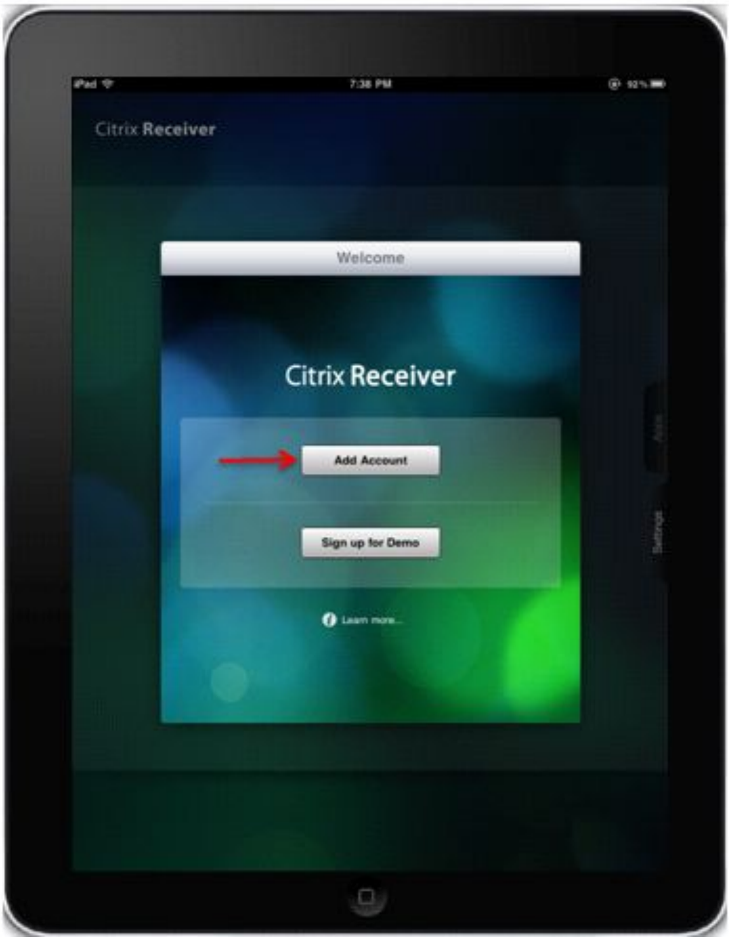
- Android devices with OS Version 4.1 and later support import of the certificates and CAs and should work as described above with iOS.

End User Interface/User Experience

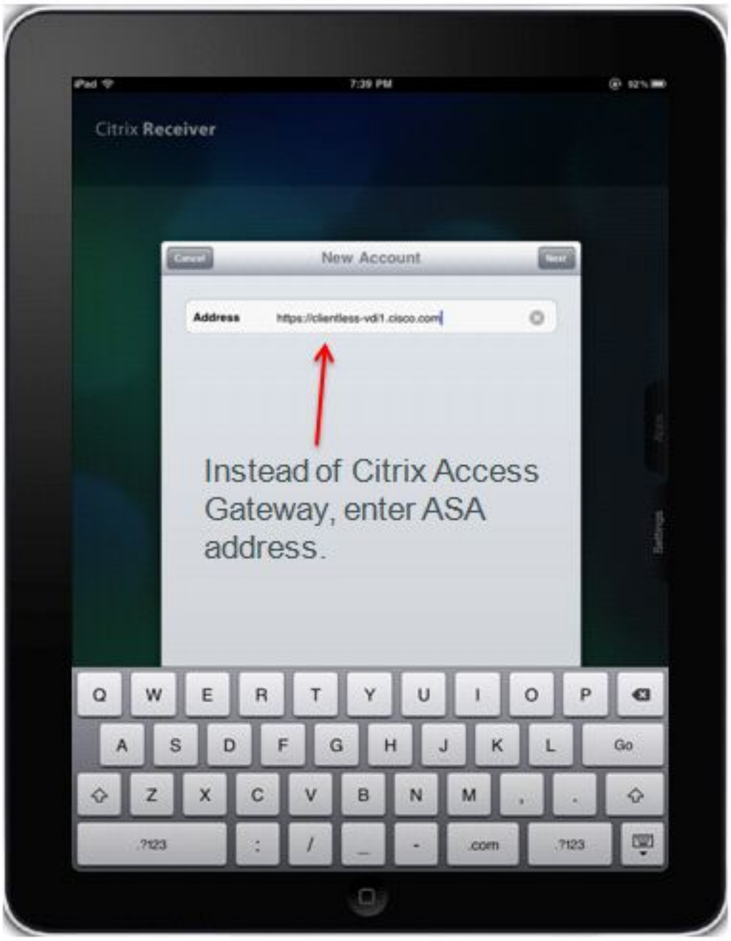
Add a New Account

Use of Citrix Receiver to access virtual resources via the ASA provides the same user experience as when a Citrix Access Gateway is used.

If no servers are configured, you must configure a new virtual resource.



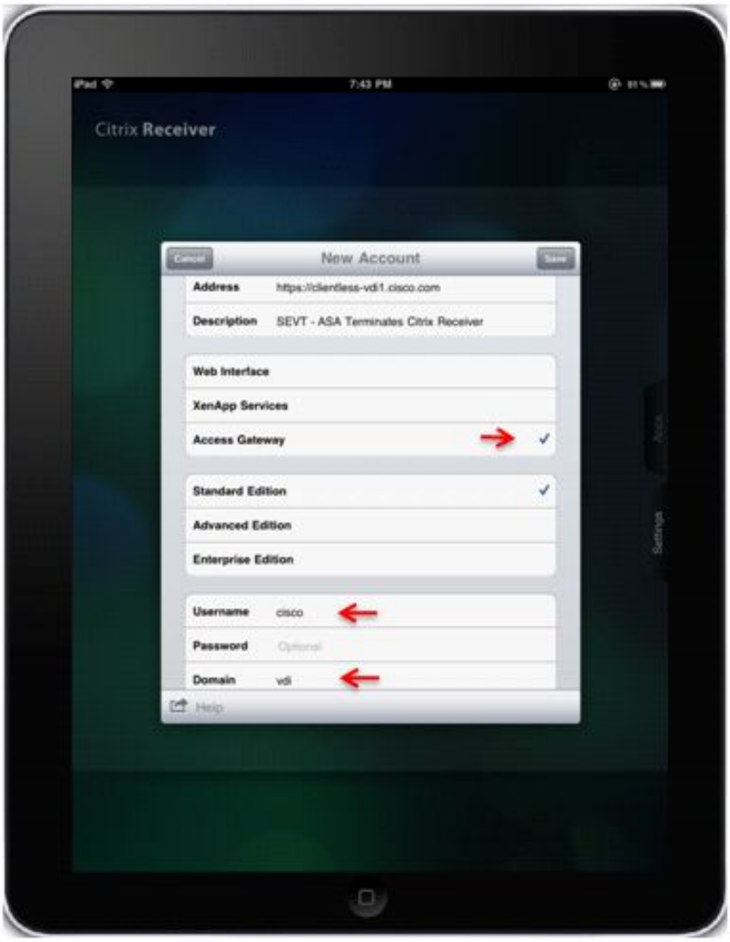
Provide the ASA's FQDN/IP address:



Address https://clientless-vdi1.cisco.com

Instead of Citrix Access Gateway, enter ASA address.

Check the ***Access Gateway***, ***Standard Edition***, and enter the credentials in order to connect to the ASA.



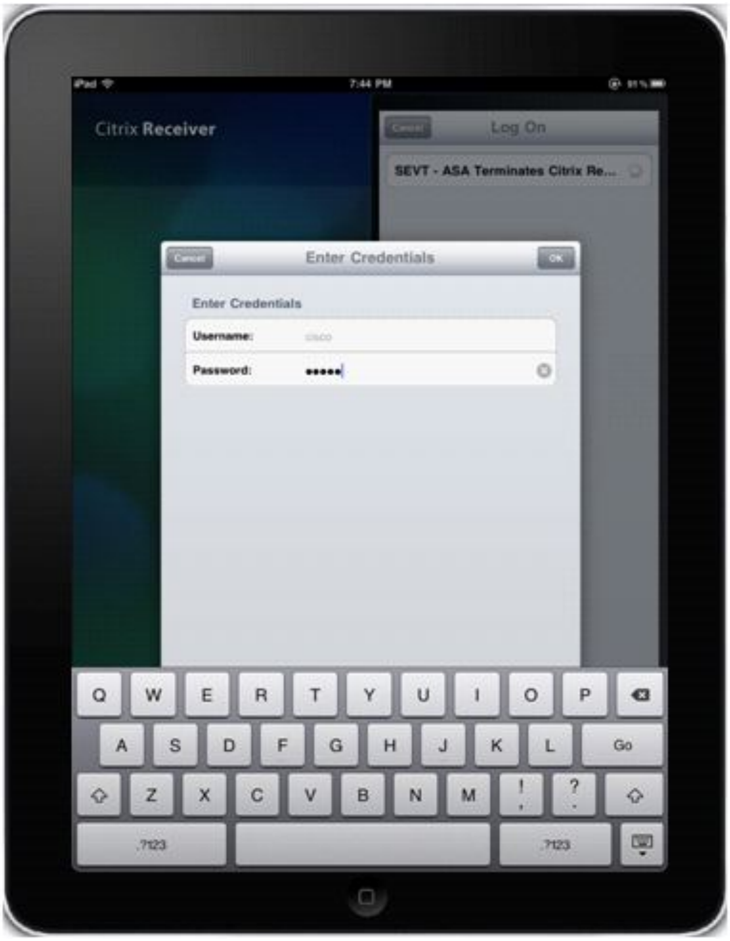
Address https://clientless-vdi1.cisco.com
Description SEVT - ASA Terminates Citrix Receiver

Web Interface
XenApp Services
Access Gateway ✓

Standard Edition ✓
Advanced Edition
Enterprise Edition

Username cisco
Password Optional
Domain vdi

When the user profile is saved, the application automatically asks for credentials (ASA) and tries to log in.

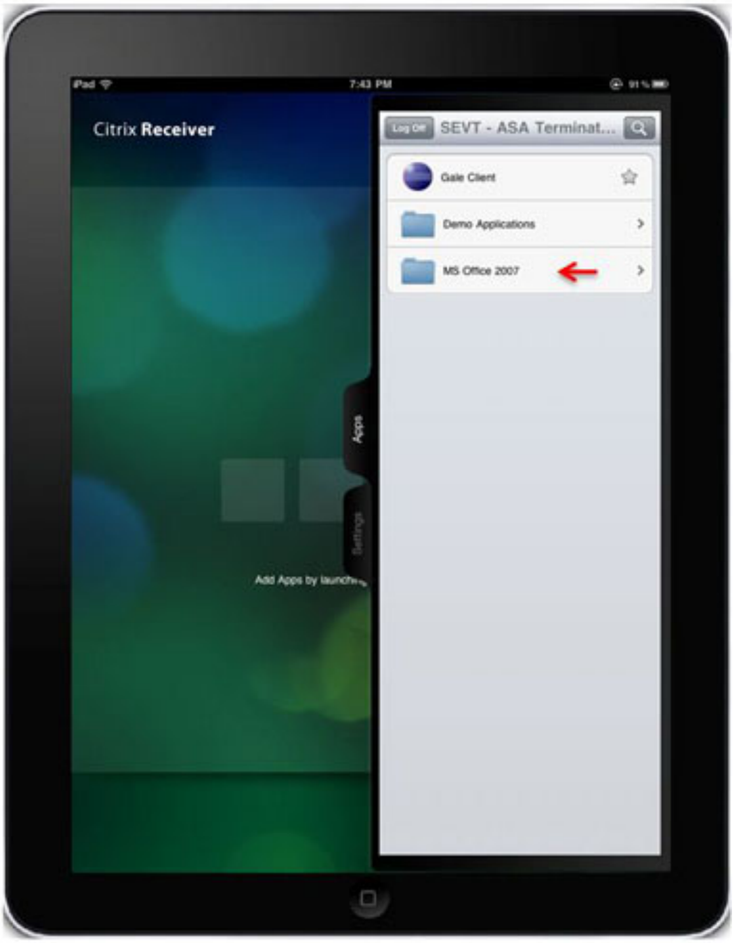


Enter Credentials

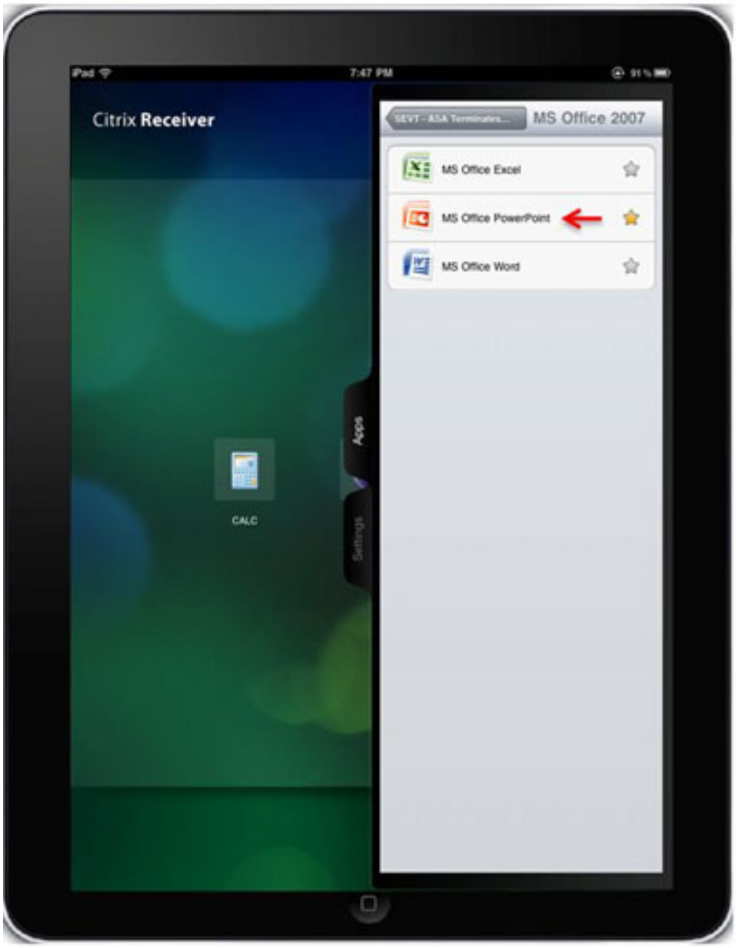
Username: cisco

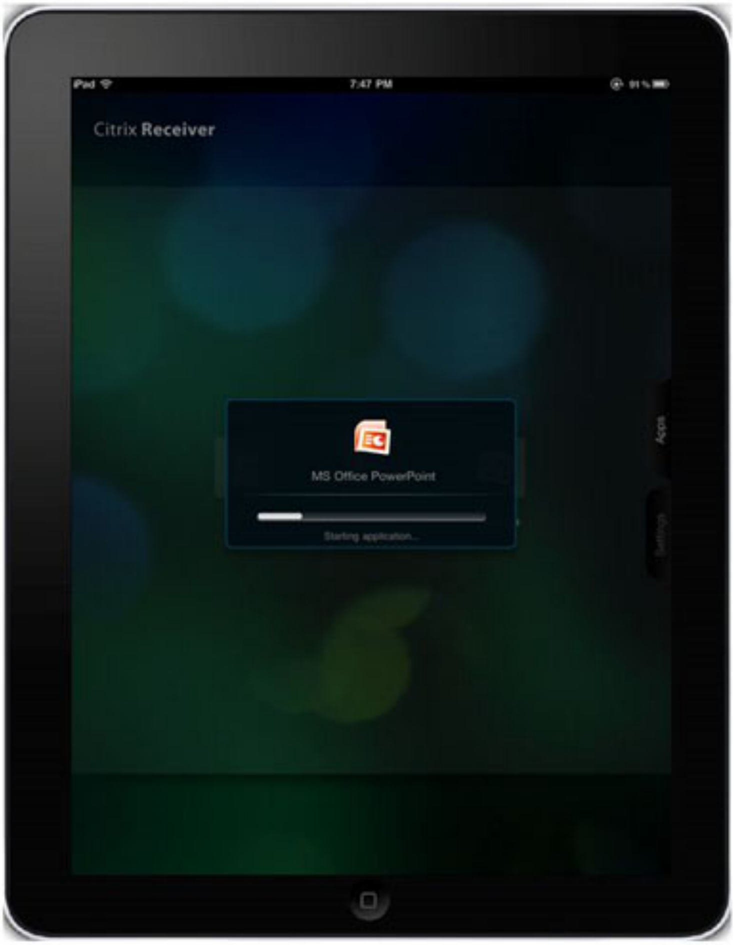
Password: ●●●●●

When logged in, the application displays a list of published resources.



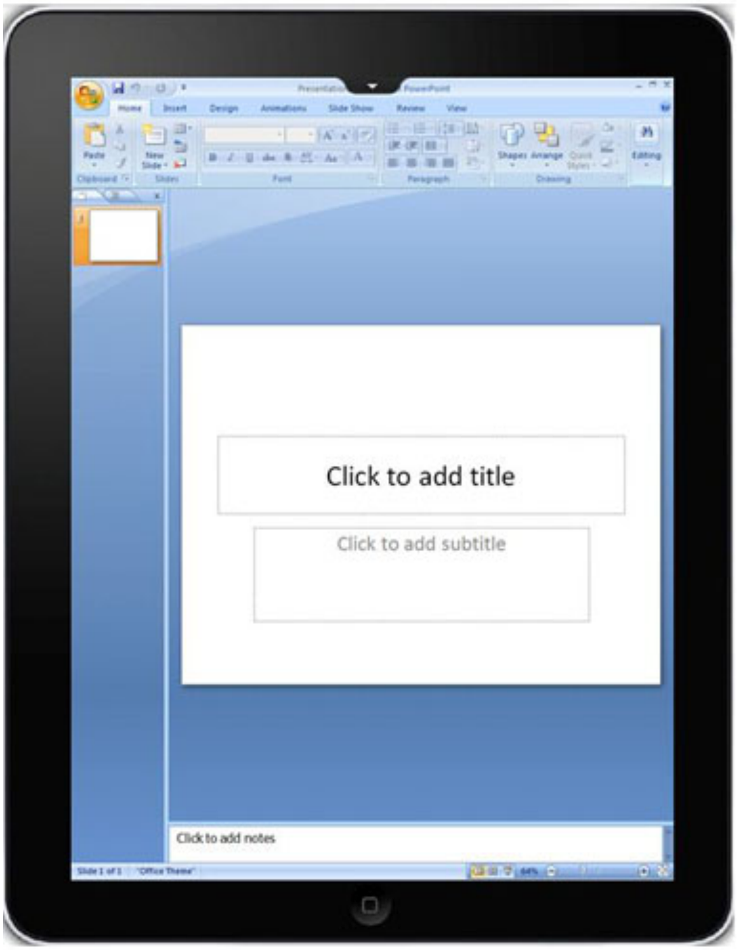
You can navigate the folders and click a resource in order to launch it.


iPad
7:47 PM
91 %
Citrix Receiver
SEVT - ASA Terminates...
MS Office 2007
MS Office Excel
MS Office PowerPoint
MS Office Word
Apps
Settings
CALC



MS Office PowerPoint

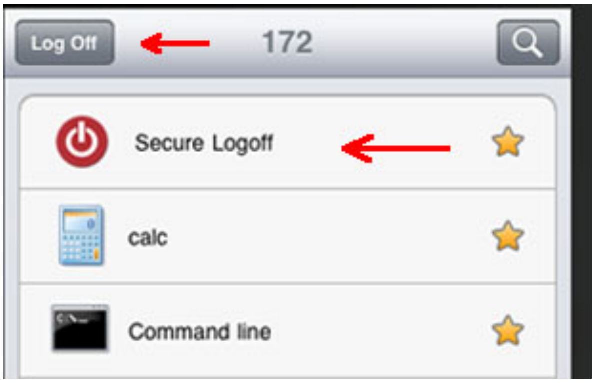
Starting application...



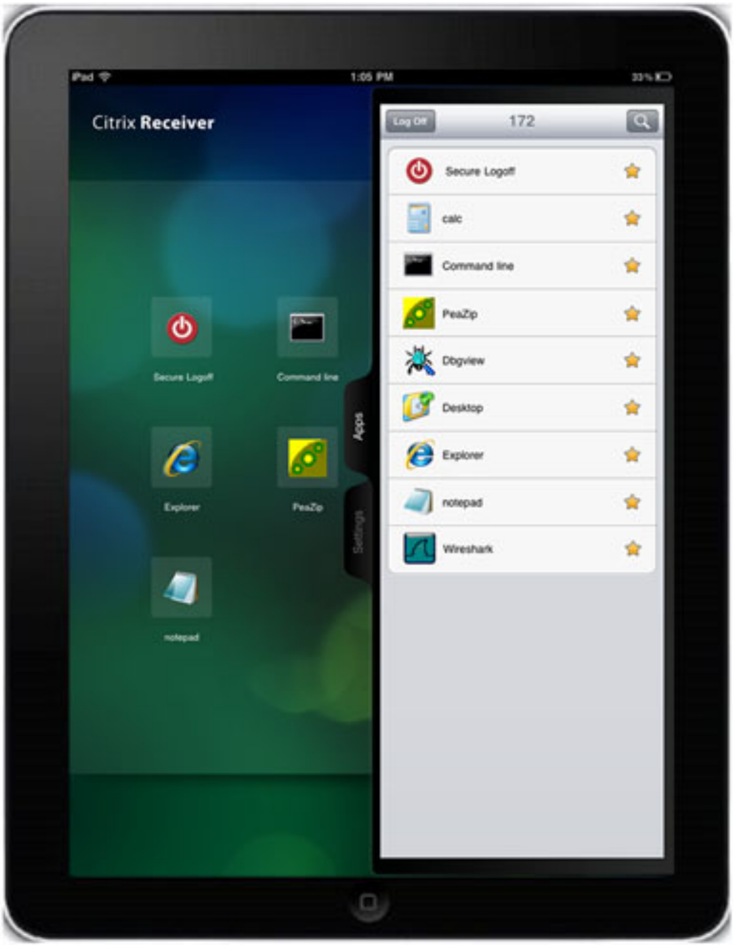
Log Out of the WebVPN Session

The Citrix Receiver application does not provide the ability to terminate a WebVPN session with a connected ASA or CAG at will. Typically such a session is terminated when you reach the configured timeout. Although the newest version of Citrix Receiver has a new ***Log Off*** button, it does not terminate the current session with the ASA. Instead it closes all open applications and displays the list of configured servers. Therefore, if the ASA is configured to use only one license per user, clients that use the ***Log Off*** button are not able to log in again until after the session times out.

In order to allow end−users to terminate the WebVPN session at will and, as a result, release the ASA license, new functionality has been added to injects ***Secure Logoff*** resource.



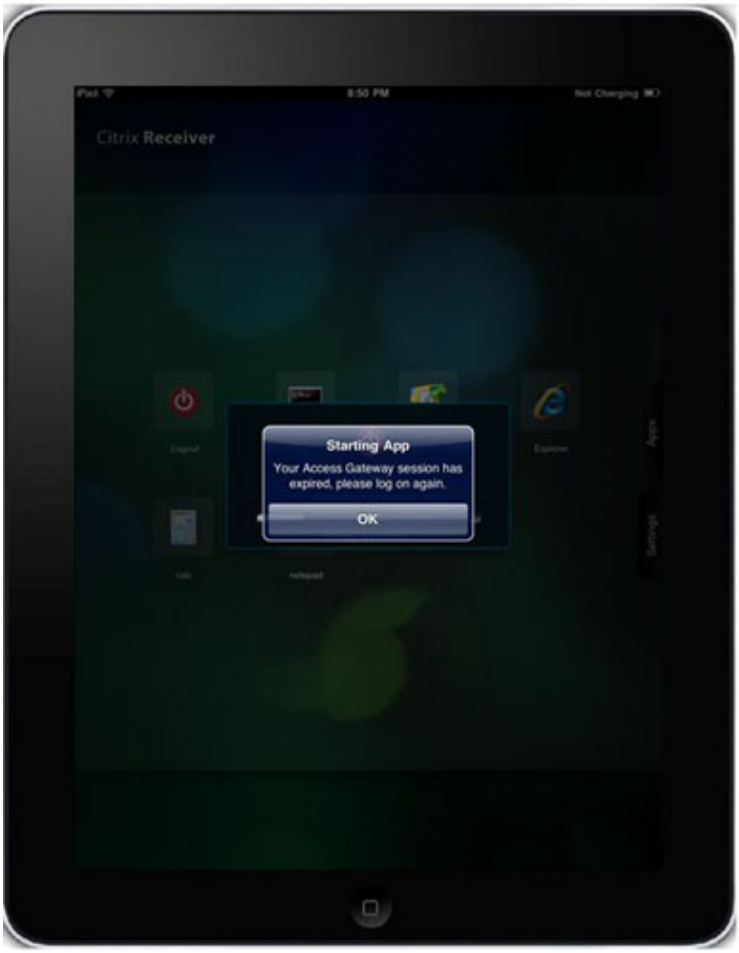
This injection occurs every time the Citrix Receiver fetches the list of published resources.



When you click the ***Secure Logoff*** application, the session between the ASA and the Citrix Receiver is terminated. In order to properly release the ASA license, the ***Secure logoff*** resource must be used in order to terminate the WebVPN session instead of the native Citrix Receiver Log Off button.

Different messages are displayed as a result of session termination based on the mobile devices and the version of Citrix Receiver. Also, the difference in the way the Citrix Application is written for different mobile platforms yields a different experience when you log off Android devices.

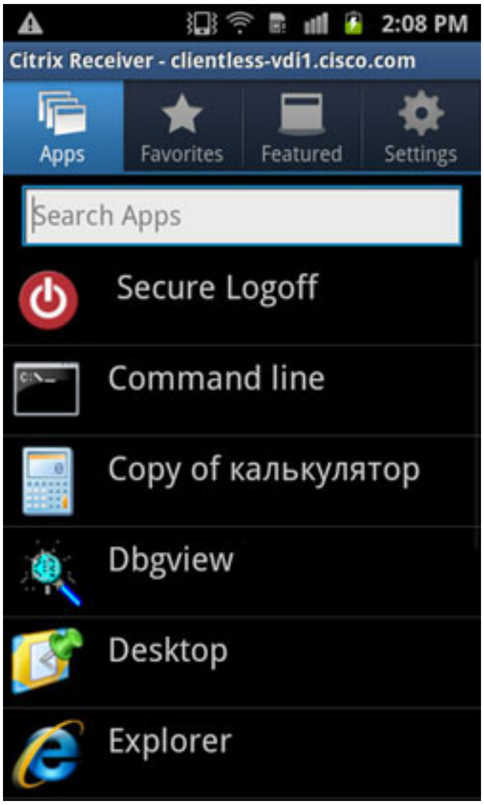
On the iPad and the iPhone, Citrix Receiver displays the message ***Your access to Gateway session has expired, please log on again.*** When you click ***OK***, Citrix Receiver displays the screen with the configured servers.



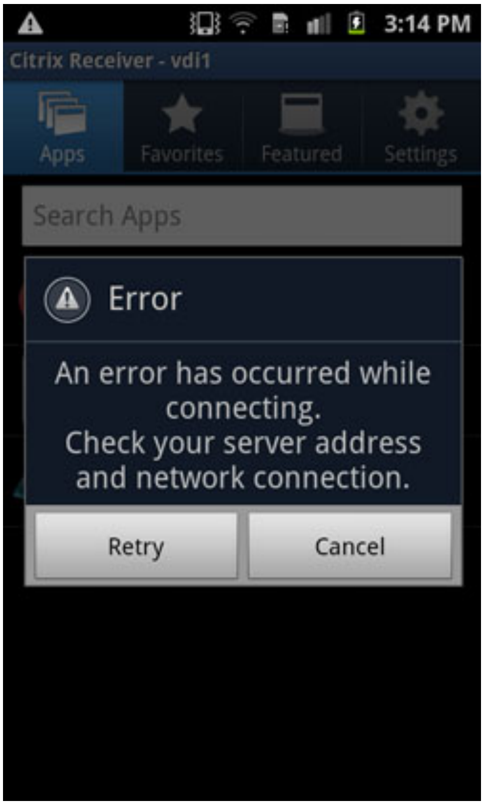
Starting App

Your Access Gateway session has expired, please log on again.

Android devices also display the injected ***Secure Logoff*** resource.



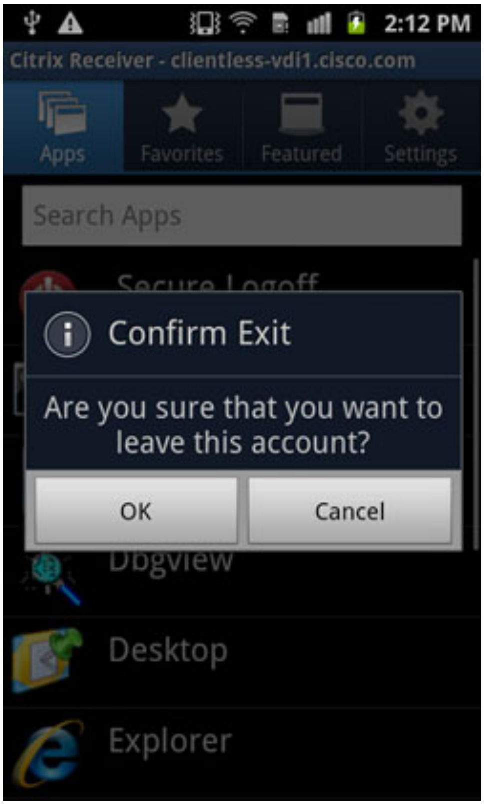
However, when you click the ***Secure logoff*** application, a network connection error displays.



Error

An error has occurred while connecting.
Check your server address and network connection.

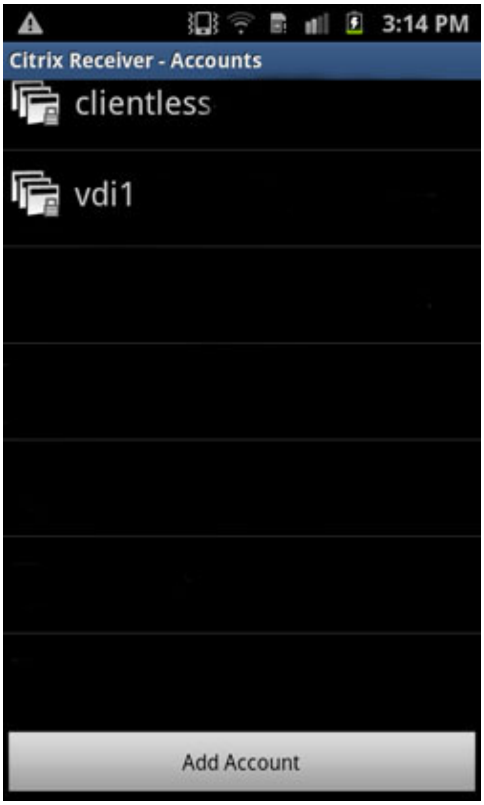
Although by this time the WebVPN session is terminated, the Citrix Receiver application does not have embedded messages to properly inform you of further actions.This is expected behavior. When this ***Error*** message displays as a result of terminated session, it expects you to click the ***Cancel*** button, the ***Back*** button on the Android device in order to exit the current account, and then ***OK*** when asked if you want to leave this account.



Confirm Exit

Are you sure that you want to leave this account?

After you exit the current account, you are presented with the list of preconfigured servers.



Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

This section provides information you can use in order to troubleshoot your configuration.

Debugs

Note: Refer to Important Information on Debug Commands before you use ***debug*** commands.

You can display debug information for Citrix Receiver with this command:

`debug webvpn citrix <1-255>`

Note:
Level 1 displays abnormal conditions, failed connections to the XenApp/XenDesktop server, and general errors.
Level 50 displays information on data being parsed/rewritten.
Level 255 displays all of the debugging information that as been added for the Citrix Receiver connections.

No new commands were added for the Citrix Receiver authentication. However, in order to view the transactions between the client and the ASA, you can use this debug:

`debug webvpn transformation request`

For reference. this output shows these two debugs taken from a connection that works:

```
=~=~=~=~=~=~=~=~=~=~=~= 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)
```

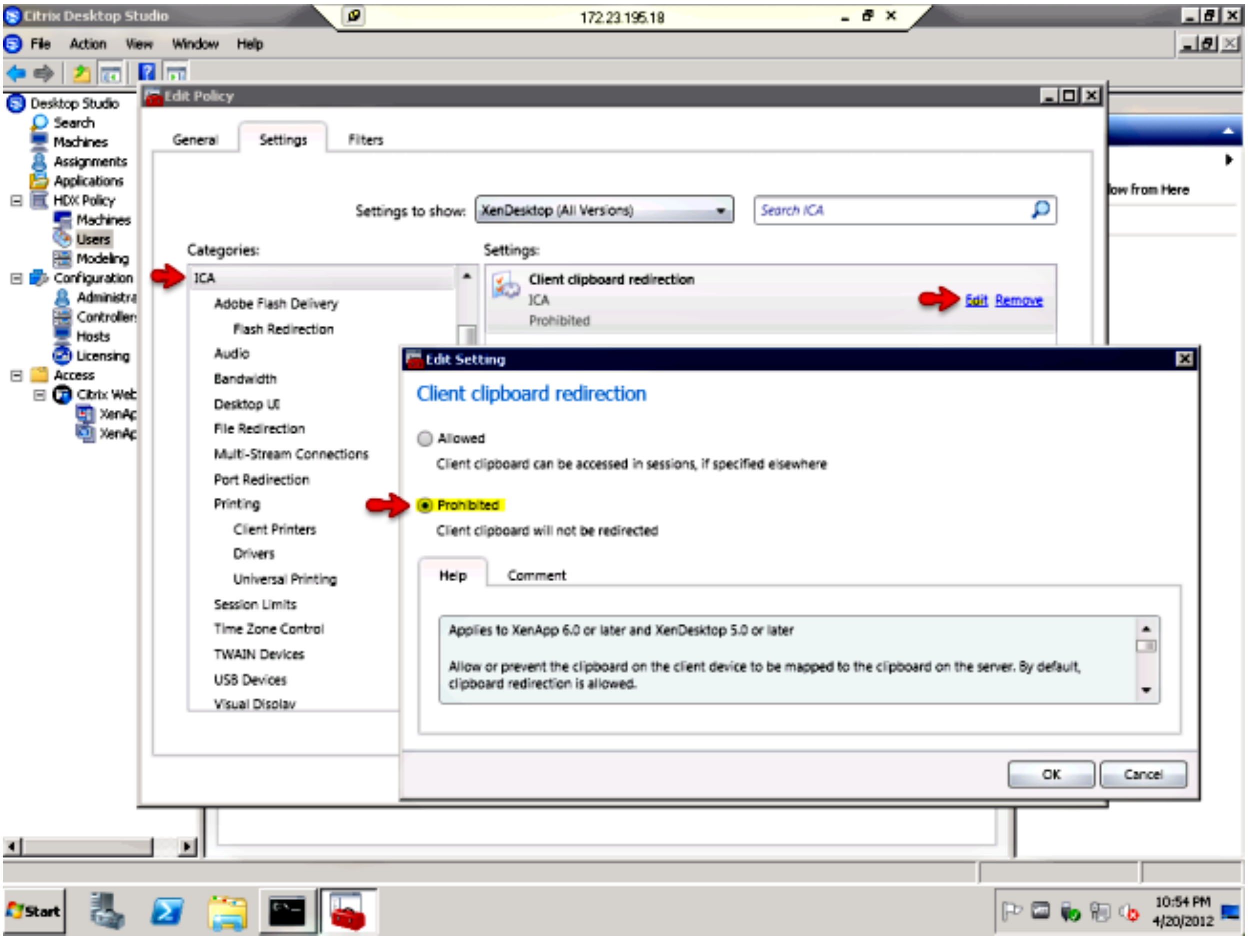
Use generic authentication debug commands in order to debug authentication issues, such as:

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

Frequently Asked Questions (FAQ)

Q. Does this new feature retain the granular controls configured on the XenServer (For example, controls such as Client Drive Redirection, Client Printer Redirection, Client Clip board Redirection, and Client USB devices redirection)?

A. These parameters are defined on the XenServer and are part of the ICA file. The ASA does not modify these parameters. Therefore, the setting you have on XenApp or XenDesktop is reflected on the client.



Settings to show: XenDesktop (All Versions)

Search ICA

Client clipboard redirection
ICA
Prohibited

Client clipboard redirection

○ Allowed
Client clipboard can be accessed in sessions, if specified elsewhere

● Prohibited
Client clipboard will not be redirected

Applies to XenApp 6.0 or later and XenDesktop 5.0 or later

Allow or prevent the clipboard on the client device to be mapped to the clipboard on the server. By default, clipboard redirection is allowed.

Q. Does the ASA have granular control of the ICA connection such as to prevent cut−and−paste, and to control the Printer, Drive, Clipboard, or USB redirection?

A. The ASA does not modify those settings. Therefore, the settings you have on the XenApp or XenDesktop are reflected on the Receiver client. Cisco is aware of the feature gap because its competition (Juniper SA and Citrix CAG) is able to prevent cut−and−paste regardless of the setting in the XenApp.

Q. Does the Storefront Citrix Server work with the ASA as a proxy?

A. Yes, this feature is not supported. Enhancement request CSCug18734 was filed in order to add support for these types of servers. Storefront Version 2.0 SSO support is added as part of XenDesktop support. All of the legacy Citrix features are supported in Storefront Version 2.0 (XenApp and XenDesktop). App−controller related functions are not supported via the ASA.

When you configure the ASA for Citrix Receiver, make sure to specify the full path to the XML−service running on the Storefront, for example, ***http://storefront.cisco.com/Citrix/storefrontweb/pnagent/***.

In versions that do not have the fix for CSCug18734 and that have the ***debug webvpn citrix*** enabled, if you try to access a Storefront server, then you see this in the debugs:

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

Q. Even though the Citrix server has enabled and configured XML−service, the error ***+++ UNKNOWN***

EXCEPTION CAUGHT continues to display. This used to work. What could be wrong?

A. This can happen when AnyConnect Essentials is enabled on the ASA as shown here:

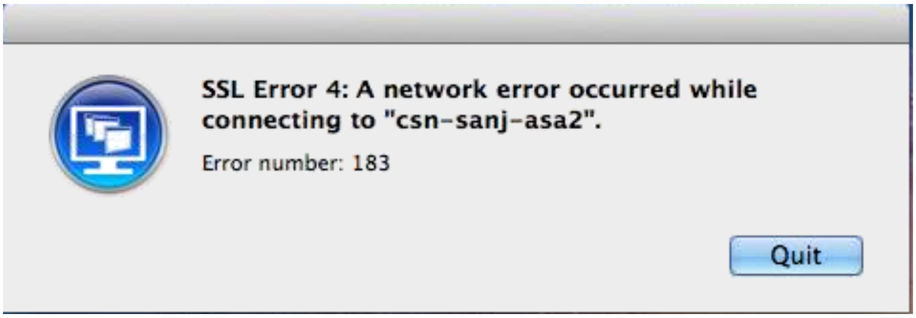
```
webvpn
 enable outside
 anyconnect-essentials
```

AnyConnect Essentials is used in order to enable only full client support on the ASA, and this disables the ability of the ASA to process clientless connection attempts. When this happens, if you have ***debug webvpn transform request*** and ***debug webvpn citrix*** enabled, then you see this:

```
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]
```

Q. If you receive this error message ***SSL Error 4: Error number: 183***, what should you do?

A. This error is seen when the connection to the XML broker (XenDesktop server) is allowed, but the Ports 1494 and 2598 to the actual XenDesktop pool are blocked. You can debug if you enable all of the ports and then narrow down the required ports.



SSL Error 4: A network error occurred while connecting to "csn-sanj-asa2".

Error number: 183

In order for the XenDesktop to work through the clientless, if there are any intermediate firewalls between the ASA (inside) and the XenDesktop server, make sure the Ports 443, 1494, 2598, and 80 are open on that firewall. Also, ensure that the ports are open for both the XenDesktop Server and the pool of XenDesktops.

Q. Does the ASA support SSL connections that originate from a standalone Citrix Receiver client from a Microsoft Windows/Macintosh OSX platform, just like you use AnyConnect or the Cisco VPN Client?
A. Currently, standalone Citrix Receivers from desktops are supported via smart tunnel only (w.r.t clientless).
CSCum85649 ENH: Support desktop standalone Citrix Recievers to ASA
This is an enhancement bug to support a standalone Citrix Receiver connection to the ASA without the need for the smart tunnel or initial portal login, like there is for the mobile Citrix Receiver with the ASA as the Access Gateway. Currently, the ASA sends a Reset after the initial handshake to a standalone Citrix Receiver (with the use of the latest 4.1 for Windows, and has the same behavior on other platforms as well).

Updated: Mar 26, 2014 Document ID: 116742