Release Notes for Cisco AnyConnect VPN Client, Release 2.0, for HP webOS

Updated: November 2010

Contents

This document includes the following sections:

Overview

This document is intended as a supplement to the *Cisco AnyConnect 2.4 Administrator Guide* and includes only HP webOS specific information. For additional information refer to the following topics in the 2.4 Administrator Guide:

- Chapter 8: Managing, Monitoring, and Troubleshooting AnyConnect Sessions
  - Disconnecting All VPN Sessions

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

  - Disconnecting Individual VPN Sessions
  - Viewing Detailed Statistical Information
  - Resolving VPN Connection Issues
- Additional tools and information on deploying webOS devices in an enterprise environment are available from Palm at http://www.palm.com/intl/support/index.html.

Introduction

The Cisco AnyConnect Secure Mobility Client provides remote users with secure VPN connections to the Cisco ASA 5500 Series using the Secure Socket Layer (SSL) protocol and the Datagram TLS (DTLS) protocol.

The Cisco AnyConnect Secure Mobility Client for HP webOS provides seamless and secure remote access to enterprise networks. The client provides a full tunneling experience that allows any installed application to communicate as though connected directly to the enterprise network. It runs on HP webOS version 2.0 or later and supports connections over an IPv4 network tunnel. AnyConnect is integrated as part of HP webOS VPN. Updates to AnyConnect functionality will be provided by HP when available.

Devices Supported by Cisco AnyConnect 2.4 for HP webOS

The Cisco AnyConnect Secure Mobility Client requires HP webOS 2.0 or later and runs on all compatible devices.

Security Appliances and Software Supported

The Cisco AnyConnect Secure Mobility Client supports all Cisco Adaptive Security Appliance models. It does not support PIX devices. See the Adaptive Security Appliance VPN Compatibility Reference: http://www.cisco.com/en/US/docs/security/asa/compatibility/asa-vpn-compatibility.html for a complete list of compatibility requirements.

Table 1 shows the minimum Cisco ASA 5500 software images that support AnyConnect.

Table 1 Software Images that Support AnyConnect, Release 2.4

Image Type	Version
ASA Boot image	8.0(3).1 or later
Adaptive Security Device Manager (ASDM)	6.1(3).1 or later

Note **The Cisco IOS VPN head-ends are not currently supported.**

Supported Features

The following AnyConnect features are supported:

- Tunnel Protocols

  - Cisco TLS/DTLS Tunneling Protocol (CSTP/CDTP)
- SSL Cipher Suites
  - AES256-SHA
  - AES128-SHA
  - DES-CBC3
  - RC4-SHA
  - RC4-MD5
  - DES-CBC-SHA
- DTLS Cipher Suites
  - AES256-SHA
  - AES128-SHA
  - DES-CBC3
  - DES-CBC-SHA
- Authentication
  - Manual certification import
  - Username/password
  - Tokens/challenge
  - Double authentication
  - Group selection
- Client Certificate Authentication
- Routing Policy
  - Tunnel All
  - Split Include
- Simultaneous full-tunnel and clientless connections
- Rekey
- Network Roaming
- TLS Compression
- IPv4 external tunnel
- IPv4 over IPv4
- Post-Login Banner
- Dead Peer Detection
- Tunnel Keep-Alive
- VPN load balancing
- Default Domain
- Cluster Support
- DNS Server Configuration
- Network Change Monitoring
- Statistics

- Graphical User Interface
- Pre-login Banner

Limitations of the AnyConnect Secure Mobility Client for HP webOS

The initial release of Cisco AnyConnect Secure Mobility Client for HP webOS supports only the features that are strictly related to remote access.

Tunnel Keep-Alive is supported, but this may reduce the battery life of the device if the update interval is set to the minimum value.

Because webOS 2.0 does not support AnyConnect client profiles, you must configure the ASA for use with webOS (see the "Configuring the ASA for Use with webOS" section on page 6.)

When you connect to tunnel groups configured for CSD, a "Posture Assessment Failed" message is displayed. You should use group URLs that bypass CSD. The workaround for this is only for webOS 2.0 on launch.

Note AnyConnect 2.4 for HP webOS does not support features introduced in later versions of AnyConnect.

Client Installation

The Palm comes equipped with a pre-installed client. For client support and updates, refer to this site http://www.palm.com/intl/support/index.html.

Configuration and Deployment Overview

Very few steps are required to set up the Cisco AnyConnect Secure Mobility Client. The client needs only:

- a description; used to uniquely identify one VPN connection from another
- the server address; the fully qualified domain name or IP address of the destination including any URL path if a specific group is configured.

Connection Persistence

AnyConnect for HP webOS supports a full suite of authentication capabilities similar to the AnyConnect for Windows, Mac OS X, and Linux.

To achieve the most transparent end user experience, you should use certificate-only authentication.

Network Roaming

The Network Roaming, or reconnect, feature enables AnyConnect to re-establish VPN connectivity when switching between networks, for example EDGE/1xRTT, 3G/EVDO, and Wi-Fi. This provides the user with seamless mobility and a secure connection that persists across networks.

Note In certain situations when Network Roaming is enabled, the client may keep the tunnel open when it is not required. This can lead to data that should not be sent through the tunnel being passed through your organization. If you have any policies that restrict VPN traffic, these could prevent the device from accessing non-corporate Internet resources.

The ASA administrator has full control over the tunneling policy. You can require that all network traffic to the corporate network uses the VPN connection, or you can enable a split tunneling policy that will tunnel only certain networks. For further details refer to your ASA Administrator Guide.

Recommended Configurations

For the best user experience, Cisco recommends that system administrators run the latest maintenance release of ASA. Specific caveats have been fixed in the ASA that affect mobile clients (such as CSCti08822—ASA sends TCP keepalive packets for CSTP tunnel and CSCtj46900—Last CSD data element is not being loaded into DAP).

Also, Cisco recommends using multiple tunnel-groups for mobile devices, depending on the authentication configuration. You will have to decide how best to balance user experience with security.

For AAA-based authentication tunnel-groups for mobile devices, the tunnel-group should have a very long idle-timeout (such as 24 hours). This enables the client to remain in Reconnecting state without requiring the user to re-authenticate. You should consider setting a shorter idle timeout for certificate-only based authentication compared to AAA-based authentication.

HP webOS Specific Considerations

The following considerations should be taken into account when deploying the Cisco AnyConnect Security Mobility Client 2.4 to HP webOS devices.

- HP webOS does not support discerning between trusted and untrusted networks.
- To conserve battery life, you should switch off keep-alive in user profiles. It is switched off by default. In the tunnel-group's group policy, you should also switch off svc keepalive.

Note Due to the constraints of webOS, push email notifications will not work via VPN. However, you can use AnyConnect in parallel with externally accessible ActiveSync connections which can be excluded from the tunneling policy.

Known Issues

The following items are known issues with the AnyConnect client and are scheduled to be fixed in the first maintenance release of HP webOS 2.0.

- When establishing an SSL VPN tunnel, the AnyConnect client may report the headend as untrusted. If the user accepts the certificate, the thumbprint of the certificate is retained so that users are not prompted again, unless they switch headends or reboot the device.
- If you choose Certificate + AAA with pre-filled usernames, the username is hidden instead of pre-filled.

- When you connect to tunnel groups configured for CSD, a “Posture Assessment Failed” message is displayed. You should use group URLs that bypass CSD.

Configuring the ASA for Use with webOS

WebOS 2.0 does not support AnyConnect client profiles. Perform the following to configure support for webOS 2.0 VPN connections.

Step 1 Add a group policy that specifies no client profile.

For example, on ASDM 6.3, choose **Configuration > Network (Client) Access > Group Policies > Add > Advanced > SSL VPN Client** and do not specify any profiles. Uncheck **Inherit** next to Client Profiles to download if the policy is not the default group policy.

Step 2 Add a connection profile and assign the group policy to it.

Step 3 Assign a group URL to the connection profile. You can do so on the Advanced > SSL VPN panel (such as http://webos.example.com).

Step 4 Use the CLI to enter the **without-CSD** command for the connection profile (also called tunnel group in the CLI). This step is necessary only if CSD is enabled on the ASA. For example, enter the following commands for a tunnel group you named webOS:

```
asa1(config)#tunnel-group webOS webvpn-attributes
asa1(config-tunnel-webvpn)# without-csd
```

CSCtj36459 is preventing ASA support for webOS connections if CSD is enabled; therefore, you must disable CSD on the tunnel group. This caveat is scheduled to be fixed in the first maintenance release of webOS 2.0.

Step 5 Connect to the group URL.

Troubleshooting

Initially you should enable logging and follow the troubleshooting steps in the webOS 2.0 help documentation. If you are unable to resolve the issue by following those steps, try the following:

- Check to see if the same problem occurs with the desktop client.
- Ensure that the AnyConnect Mobile license is installed on the ASAs. See Notices and Licensing on page 7 for more information.
- If you see an authentication screen when you are expecting to use certificate-only authentication, configure the connection to use a Group URL and ensure that secondary authentication is not configured for the tunnel group. For further details refer to your ASA Administrator Guide.

Support Policy

If you are experiencing issues with the AnyConnect client, including configuration, setup, and operation of AnyConnect on HP products, contact HP support at 1-877-426-3777 or visit their support website at http://www.palm.com/intl/support/index.html.

If you are experiencing issues with configuring Cisco head-end equipment, including configuration, setup, and operation of that equipment, contact Cisco support at 1-800-553-2447 or visit our support website at http://tools.cisco.com/ServiceRequestTool/create.

Note You must have a support contract with the appropriate party to obtain support from that party.

Notices and Licensing

See the following sections for Cisco AnyConnect Secure Mobility Client license information.

The following options support full AnyConnect client functionality while specifying the number of SSL VPN sessions supported:

- Cisco AnyConnect Essentials license
- Cisco AnyConnect Premium Clientless SSL VPN Edition license

These licenses are mutually exclusive per device (that is, per security appliance), but you can configure a mixed network. A nominally priced AnyConnect Mobile license is also required.

License Options

For brief descriptions and example product numbers (SKUs) of the AnyConnect user license options, see Cisco Secure Remote Access: VPN Licensing Overview.

For the latest detailed information about the AnyConnect user license options, see Managing Feature Licenses in the *Cisco ASA 5500 Series Configuration Guide using the CLI, 8.3*.

End-User License Agreement

For the end-user license agreement, go to:
http://www.cisco.com/univercd/cc/td/doc/es_inpck/eu1jen__.pdf

OpenSSL Project

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

For Open Source License information for this product, please see the following link:
http://www.cisco.com/en/US/docs/security/asa/asa83/license/opensrce.html#wp50053.

Related Documentation

For more information, refer to the following documentation:

- *Release Notes for Cisco AnyConnect VPN Client Release 2.4:*

  http://www.cisco.com/en/US/docs/security/vpn_client/anyconnect/anyconnect24/release/notes/anyconnect24rn.html
- The webOS 2.0 online help
- *Navigating the Cisco ASA 5500 Series Documentation*:

  http://www.cisco.com/en/US/docs/security/asa/roadmap/asaroadmap.html
- *Cisco AnyConnect VPN Client, Release 2.4, Administrator Guide*

  http://www.cisco.com/en/US/docs/security/vpn_client/anyconnect/anyconnect24/administration/guide/anyconnectadmin24.html

Additional information on using VPN connections with webOS devices is available from Palm at http://www.palm.com/intl/support/index.html.
