Google Chrome OS User Guide for Cisco AnyConnect Secure Mobility Client, Release 4.0.x

Revised: December 17, 2020

AnyConnect User Guide

AnyConnect Overview

The Cisco AnyConnect Secure Mobility Client for provides seamless and secure remote access to enterprise networks. AnyConnect allows installed applications to communicate as though connected directly to the enterprise network. AnyConnect is a sophisticated networking application that also allows you to set preferences, control the operation of AnyConnect, and use diagnostic tools and facilities on your device as recommended by your administrator.

AnyConnect may be used in your enterprise in conjunction with Mobile Device Management software. If so, work with your administrator to abide by device management rules. Your organization may provide additional documentation on using AnyConnect for .

Your app store provides the application for initial installation and all upgrades. The Cisco Adaptive Security Appliance (ASA) is the secure gateway that admits access to the VPN, but it does not support updates of AnyConnect for mobile devices.

Open Software License Notices

- 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).

Google Chrome OS Supported Devices

Cisco AnyConnect on Google Chromebook requires Chrome OS 43 or later. Stability and feature enhancements are available in Chrome OS 45.

AnyConnect on Google Chromebook cannot be used from a standalone Chrome browser on another platform.

For all current Chromebooks, AnyConnect for Android is officially supported and strongly recommended for the optimal AnyConnect experience on ChromeOS. The native ChromeOS client is intended only for legacy Chromebooks incapable of running Android applications.

Install or Upgrade AnyConnect on Google Chrome OS

Before you begin

Verify you are using a device supported by AnyConnect, see Google Chrome OS Supported Devices, on page 2 for details.

Procedure

Step 1 On your Chrome device, go to the Chrome Web Store Cisco AnyConnect page.

Step 2 Select **Add to Chrome** or **Update**.

Launch App will be shown if you already have the latest version of Cisco AnyConnect on your device.

What to do next

After installing or updating it may take a few minutes before you are able to configure AnyConnect. "Initializing please wait" will be shown in the AnyConnect App during this time.

Configure AnyConnect Through Google Chrome's Management Services

On managed Chrome devices, administrators can push down a root certificate and an AnyConnect profile using Google's EMM service. The policy, specified in JSON, has the following structure:

```
{
  "Profile":{
    "Value":"Base64 Encoding AC Profile. Set to empty string to clear the profile."
  },
  "RootCertificates":{
    "Value":[
      "Base64 Encoding of Certificate1. Pass an empty list to clear any imported server certificates.",
      "Base64 Encoding of Certificate2.",
   ]
  }
 }
```

Import Client Certificate

You must import a certificate into Chrome Certificate Manager.

Note If you have logged in as a managed account user, you may only access certificates from the managed certificate store. These correspond to certificates that have been imported programmatically via the **chrome.enterprise.platformKeys** API. Certificates that are generated or imported by other means, such as manually, are not available to the API in the case of a managed account.

For more information, see https://support.google.com/chrome/a/answer/6080885?hl=en.

Procedure

Step 1 Navigate to **chrome://certificate-manager** or through **Chrome Settings** > **Show Advanced Settings** > **Manage Certificates**.

Step 2 Associate a client certificate to your VPN configuration.

Configure and Connect AnyConnect on Google Chrome OS

Managing your private network connection is shared between the AnyConnect app and native Chrome utilities:

- You must configure connection entries in the AnyConnect app.
- You must establish a Private network connection from the Chrome Status Area or Chrome Settings.
- You may Disconnect the VPN from the AnyConnect app, the Chrome Status Area, or the Chrome Settings.

Procedure

Step 1 Open the AnyConnect app to configure an AnyConnect VPN connection entry:

Note The VPN must be disconnected to create a new connection entry.

- Open the AnyConnect app from the launcher.
- Click in the Chrome Status Area, then in the Private Network area labeled VPN, and choose **Cisco AnyConnect**.
- Click in the Chrome Status Area, then choose **Settings**, then from the Internet Connection settings choose **Add Connection** > **Add Cisco AnyConnect**.

Step 2 Choose the **Connections** tab in the AnyConnect app.

You will see connection entries listed if they were previously configured.

Step 3 Add a new connection entry:

a) Click **Add New Connection**.

b) Enter a descriptive name for this connection entry In the **Name** field.

c) Enter the VPN server address in the the **Server Address** field.

d) Choose **Connect with IPsec** if desired. If not chosen, AnyConnect will use SSL (TLS/DTLS).

Note AnyConnect supports only EAP authentication for IPsec. Because of this limitation, AnyConnect cannot use IPsec to connect to a Cisco IOS headend.

e) Choose **Select Certificate** to configure certificate authentication.

f) Click **Save Changes**.

Step 4 Establish a VPN connection:

- Click in the Chrome Status Area, then in the Private Network area labeled VPN, and choose the desired connection entry.
- Click in the Chrome Status Area, then choose **Settings**. From the Internet Connection settings choose **Private network** and then the desired connection entry.

Monitor and Troubleshoot AnyConnect on Google Chrome OS

Use the AnyConnect app to view VPN connection statistics and logs, and to send diagnostic information to your administrator or Cisco when experiencing difficulties.

Procedure

Step 1 Choose **Statistics** to view statistics for the current connection.

A VPN Connection must be active to view VPN statistics.

Step 2 Choose **Diagnostics** to view or email AnyConnect logs.

Step 3 Click on a log file to view it directly or **Download** and view a log file.

Step 4 Choose **Email Logs** to gather and send diagnostic information.

a. When prompted save the zipped up log files to a local directory.

b. Attach the zip file to the created email.

c. Provide a description of the problem you are experiencing in the message body.

d. By default the email will be sent to Cisco, add your administrator or support contact as desired.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
CiscoSystems(USA)Pte.Ltd.
Singapore

Europe Headquarters
CiscoSystemsInternationalBV
Amsterdam,TheNetherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.