BlackBerry User Guide for Cisco AnyConnect Secure Mobility Client, Release 4.0.x

AnyConnect User Guide

AnyConnect Overview

The Cisco AnyConnect Secure Mobility Client for BlackBerry 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 BlackBerry.

Your BlackBerry 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).

BlackBerry Supported Devices

Full support for Cisco AnyConnect is provided on devices running BlackBerry OS 10.3.2 and later. For the best AnyConnect experience, Cisco strongly recommends you upgrade your device to 10.3.2.

Install or Upgrade AnyConnect on BlackBerry Devices

Before You Begin

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

Procedure

AnyConnect is available in the BlackBerry World store at http://appworld.blackberry.com/webstore/content/59952066.

Configure AnyConnect VPN Profiles on BlackBerry Devices

Before You Begin

Configure your Cisco AnyConnect VPN Profile as directed by your administrator. Contact your administrator if you do not have clear instructions.

Your administrator may also provide you with directions to configure a digital certificate for authorizing you VPN connection. Digital certificates are found under **System Settings** > **Security and Privacy** > **Certificates**.

Procedure

Step 1   Go to **System Settings** > **Networks and Connections** > **VPN**.
The **VPN Settings** screen displays VPN profiles configured on your device manually, downloaded by device management, or downloaded from the secure gateway an AnyConnect VPN has previously connected to.

Step 2   Add, edit or view a VPN profile by doing one of the following:

- To add a new VPN profile, choose + **Add** from the menu options.

- To edit or view a VPN profile, long-press the desired one and choose **Edit Profile** from the menu.

  From here you can also cancel this activity or delete the VPN profile at any time.

Step 3   For a new VPN Profile, set the following fields (required fields are marked with "*"):

- **Profile Name**—a descriptive name for this profile.

- **Server Address**—the FQDN or IP Address of your secure gateway. This should be provided by your administrator.

- **Gateway Type**—choose **Cisco AnyConnect**.

Step 4   Set additional connectivity options in the **Advanced** section. Tap to open this section if necessary.

- **Automatically Select Client Certficate**

    - On (default)—To complete a connection to the server, AnyConnect will select a client certificate from the BlackBerry certificate store without user intervention.

    - Off—To complete a connection to the server, the user will select a certificate from a list of available certificates in the BlackBerry store.

- **Allow Untrusted Certificates**

    ◦ On (default)—An untrusted certificate received from the secure gateway will not prevent AnyConnect from establishing a connection.

    ◦ Off—If an untrusted certificate is received from the secure gateway, the user will have to manually accept the certificate before AnyConnect establishes the connection.

- **Automatically Configured Proxy**

- **Connect using IPsec**

    ◦ Off (default)—an SSL VPN connection is established.

◦ On—an IPsec VPN connection is established.

What to Do Next

Choose **Connect** to save this VPN profile and Establish an AnyConnect VPN Connection on BlackBerry Devices, on page 4.

You can also **Save** this VPN profile and repeat this procedure to configure additional ones if your environment requires it.

Establish an AnyConnect VPN Connection on BlackBerry Devices

Before You Begin

You must have a VPN Profile configured on your device to establish a VPN connection.

Procedure

Step 1	Go to **System Settings** > **Networks and Connections** > **VPN**. The **VPN Settings** screen displays VPN profiles configured on your device manually, downloaded by device management, or downloaded from the secure gateway an AnyConnect VPN has previously connected to.
Step 2	Tap a VPN Profile to initiate a VPN connection. If a connection was previously established, manually or automatically, it will be disconnected before this connection initiates.
Step 3	(Optional) If the digital certificate from the server, the secure gateway, is unable to be automatically accepted by AnyConnect, you will be prompted to accept the certificate and complete the connection, or reject the certificate and terminate the connection.
Step 4	(Optional) Read and acknowledge the informational banner if one is displayed.
Step 5	(Optional) Depending on your secure gateway configuration you may need to choose a tunnel group. This information should be provided by your administrator.
Step 6	(Optional) If prompted, do one of the following to authenticate your connection: • Enter your username and password credentials. You may be prompted for secondary credentials as well. • Tap Get Certificate and enter the certificate enrollment credentials supplied by your administrator. AnyConnect saves the certificate and reconnects to the VPN secure gateway to use the certificate for authentication.

Once the connection has been established, the associated VPN Profile will be displayed in green.

Depending on the VPN secure gateway configuration, AnyConnect may add VPN Profiles to the VPN Settings.

Note   Tapping another VPN profile disconnects the current VPN connection and connects to the VPN secure gateway associated with the one that you tapped.

Monitor and Troubleshoot AnyConnect on BlackBerry Devices

View AnyConnect Status and Statistics

Before You Begin

A VPN connection must be active for status and statistics to be shown.

Procedure

Step 1	Go to **System Settings** > **Networks and Connections** > **VPN**. The **VPN Settings** screen displays VPN profiles configured on your device manually, downloaded by device management, or downloaded from the secure gateway an AnyConnect VPN has previously connected to.
Step 2	Choose **View Status Details** from the menu.

View AnyConnect Logging

Procedure

Step 1	Go to **System Settings** > **Networks and Connections** > **VPN**. The **VPN Settings** screen displays VPN profiles configured on your device manually, downloaded by device management, or downloaded from the secure gateway an AnyConnect VPN has previously connected to.
Step 2	Choose **View VPN Logs** from the menu or after long pressing the connected VPN Profile.
Step 3	Tap the **Messages** or **Debug** tab to view logs. Messages pertain to AnyConnect activity, Debug is used by your administrator and Cisco TAC to analyze AnyConnect issues.
Step 4	(Optional) Select **Send Logs** to send this information to your administrator or Cisco TAC for troubleshooting purposes. Enter steps to reproduce the problem in the email body. A configured email client on the device can be also be used to forward logs.
Step 5	(Optional) Select **Clear Logs** to remove the entire log history and restart logging.