Blue Cedar Connect

Blue Cedar Connect, an in-app VPN that is optimized for mobile environments, enables IT to ensure secure access to remote corporate data from mobile apps even when the mobile device does not have mobile device management (MDM) control.

VPN for Mobile Has Unique Requirements

Transient connections, rather than long-lived VPN connections, are essential to handle the power conservation and bandwidth optimization needs unique to mobile and edge environments. Discrete in-app VPN connections instead of a shared device-level VPN connection are convenient for IT and users, and work well in a Bring Your Own Device (BYOD) context. Different apps can connect via different VPN configurations and servers, depending on the security level designated. Traffic from different apps is kept separate and apps can't exchange data. In-app VPNs ensure that users do not need to remember to turn the device-level VPN on and off, and the use of personal apps is not impacted.

Add In-App VPNs Without Writing Code

The Blue Cedar Platform can integrate the Blue Cedar Connect in-app into ISV and custom mobile apps without requiring code to be written. The Blue Cedar Platform automatically configures Blue Cedar Connect to create transient app-level secure microtunnels to backend services or applications through a IKEv2 standards compliant VPN gateway.

Features

- Works with IKEv2 standards compliant VPN gateways
- Supported for mobile apps built for iOS v13 and higher, and Android v5 and higher
- Enables the following controls
  - Security Controls: Connection Method, VPN Server, Offline Use
  - Access Controls: Authentication Groups, Managed Device Check
- Can be integrated into apps created using any development framework, including Xcode, Android Studio, Xamarin, Cordova, Adobe PhoneGap, HTML5, and React Native

Enable Granular Policy Controls

The following policy controls are enabled in apps into which Blue Cedar Connect has been integrated.

Security Controls	
Policy Name	**Description**
Connection Method	Control whether the app connects to its backend service or application through a direct connection, specified proxy server(s), or a proxy auto-config (PAC) file.
VPN Server	Specify the VPN gateway to which the app can connect.
Offline Use	Allows the app to be used locally even when it is unable to connect to a VPN gateway.

Access Controls	
Policy Name	**Description**
Authentication Groups	Configure security features and access levels for different groups of users, such as executives, employees, and contractors.
Managed Device Check	Require that a device be managed by the organization's mobile device management (MDM) or enterprise mobility management (EMM) solution in order for the app to make a remote connection.