



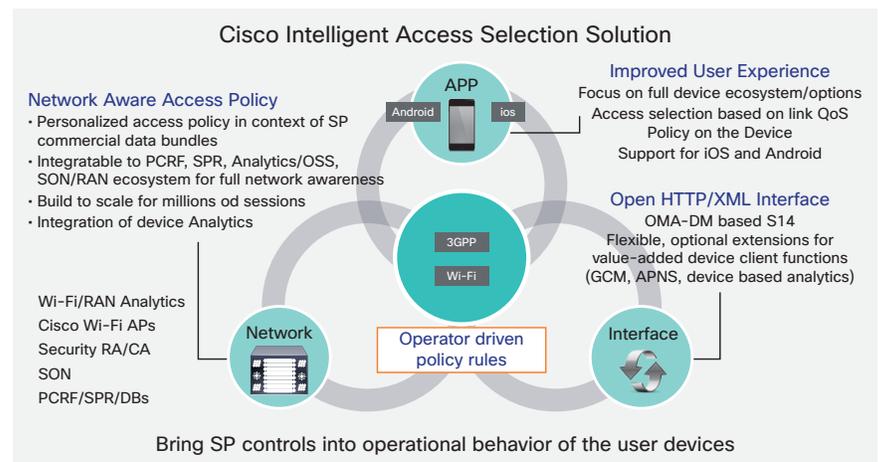
Cisco Access Policy Server

Carrier Wi-Fi is a great way to effectively handle data growth and to offload subscriber traffic. But you want your subscribers to have a seamless, highly secure experience discovering, selecting, and authenticating onto a Wi-Fi network. You want to help them avoid issues such as poor connection and network “ping-pong” that often occur in mixed-carrier Wi-Fi and macro-cellular environments. Their quality of experience should not suffer as they move between networks. So you don’t want to leave network connectivity to device-only based logic, which is typical today.

A better choice is the Cisco® Access Policy Server. Cisco’s Access Policy Server solution is a Cisco policy module focused specifically on device to network related policy controls, enabling network-driven access selection in the immediate timeframe, and other related device to network related policy functions in the future. With this solution, your subscribers can enjoy personalized, network-aware access selection based on dynamic, responsive policies running in the SP network. Cisco’s Access Policy Server is responsive to network congestion and busy hours, to traffic trends (daily, weekly, and per geolocation), to carrier cellular site and access point expansion changes, and to subscriber’s data plan network status, all of which can be coordinated to determine optimal connectivity for each subscriber device.

Benefits

- Delivers best-connected user experience consistently
- Provides seamless connectivity experience for network subscribers
- Proactively promotes cellular offload to select Wi-Fi
- Pushes network-based policies to the handset
- Provides an open interface strategy for broad device and OS integration



The Power of Network-Aware Access Selection Policies

The Cisco Access Policy Server provides fundamental intersystem mobility policies (ISMP) along with access network discovery management objects (ANDI MOs) to enhance your subscribers' quality of experience. The policies include access selection policies based on time and location (cell site or geo-fence) and push/pull updates.

The Cisco Access Policy Server also supports personalized policy (push) Google Cloud Messaging (GCM), Apple Push Notification Service (APNS), based on user profile state and profile changes, including user groups.

Specific features include:

- Subscriber Management: Refine policies by adding personalization based on user or user group profiles, preferences, and state changes
- Link Quality of Service (QoS): Assess Wi-Fi link quality before attaching or as a condition of remaining connected
- Wi-Fi Power Geo-fence: Provide network-driven, on/off control of a device's Wi-Fi radio power
- Smart Security: Deliver policy-driven support for managed (trusted) and unmanaged (untrusted) Wi-Fi attachments

Next Steps

For more information about the Cisco Access Policy Server, contact your local account representative.

For more information about Cisco Policy Suite, go to: <http://www.cisco.com/go/mobilepolicy>