Secure Mobility: Collaborate from Anywhere, on Any Allowed Device

At-A-Glance

What Is the Value of Secure Mobility?

To be fully productive, government agency personnel need to collaborate and access agency services from anywhere, using any device their agency allows. Steven VanRoekel, U.S. chief information officer, has stated, "To fundamentally change the way we do things in government, we need to seize on this mobile opportunity both in how we serve the public and in how government employees work." The U.S. Army is also committed to enabling personnel to connect in any location, for humanitarian as well as military missions.

Secure mobility solutions support government missions by helping personnel work more efficiently and effectively. Examples include:

- **Bring Your Own Device (BYOD):** Civilian agency employees want to use personal devices for work, and satisfying this demand helps increase productivity and job satisfaction.
- **Secure remote collaboration:** Giving employees access to agency video and collaboration services from anywhere, including home or disaster scenes, supports continuity of operations (COOP).
- **Simplified access:** Productivity increases when federal workers can securely join the network from any agency office. Security requires authentication and policy control.
- **Field Productivity and Communications:** Front line resources need secure, resilient, real-time communications to share information and act decisively.

What Problems Does it Help Solve?

Confidently providing secure wireless access requires:

- Knowing who and what devices are connected to the network
- Enforcing access policy based on context: who is making the request, when, how, and on what device
- Automatically detecting and mitigating threats to security or wireless performance

Cisco is a leader in cybersecurity. Threats travel across the network, and most Cisco network devices have built-in security capabilities that agencies can enable as part of a comprehensive cybersecurity strategy.

- Connecting the wide variety of client devices used in government
- Providing a consistently good experience for voice and video over wireless
- Conserving bandwidth
- Simplifying the user experience to promote adoption
- Implementing the solution properly, quickly, and with the necessary management and security controls for the mission

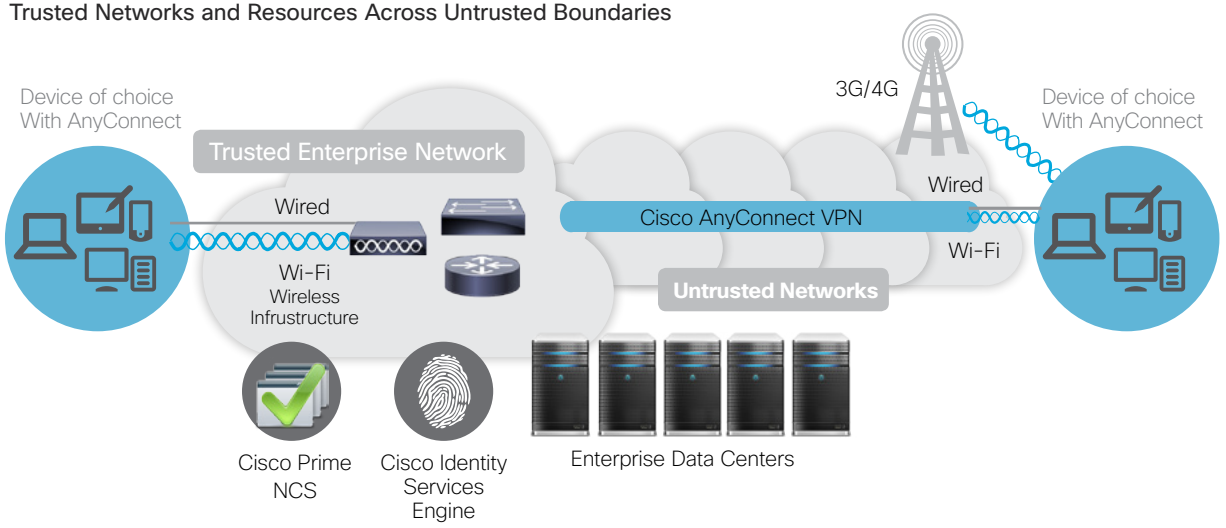
Cisco Secure Mobility Solution

The Cisco® Secure Mobility solution extends access to trusted networks and resources across untrusted boundaries, anywhere, anytime, and any device (Figure 1).

The solution includes multiple elements that work in concert to address the many aspects of secure mobility:

- **Cisco Core Routing and Switching:** Advanced security features are built into all Cisco switches and routers. For example, NetFlow Collection Engine monitors packet flow for auditing purposes. Cisco IOS® Embedded Event Manager provides real-time network event detection and onboard automation. Cisco Application Visibility and Control intelligently applies policy to network traffic based on mission and business priorities. Cisco TrustSec® provides policy-based access control, identity-aware networking, and data integrity and confidentiality services.
- **Cisco Secure Wireless Infrastructure:** Best-in-class security technology is integrated into the infrastructure. For instance, Cisco Mobility Services Engine provides real-time network visibility and asset management, including location tracking of wireless and wired assets. Cisco Adaptive Wireless Intrusion Prevention System (wIPS) detects wireless network anomalies, unauthorized access, and radio-frequency (RF) attacks. Scalable encryption is built directly into Cisco wireless hardware. Features that enhance the quality of the wireless experience include Cisco CleanAir®, ClientLink, BandSelect, and VideoStream technologies.

Figure 1 Cisco Secure Mobility Solution Extends Access to Trusted Networks and Resources Across Untrusted Boundaries



Secure Mobility: Collaborate from Anywhere, on Any Allowed Device

At-A-Glance

- **Cisco Identity Services Engine (ISE):** The main policy component for Cisco TrustSec, Cisco ISE combines policy definition, control, and reporting in one easy-to-manage appliance.
- **Cisco Prime Network Control System:** Cisco Prime combines with ISE to provide automated network management for wired and wireless access when viewed through the Prime Assurance Manager. It is also a critical component of Wireless IPS.
- **Cisco AnyConnect Secure Mobility Client:** The Cisco AnyConnect ™ client software, available for different devices and operating systems, enforces the agency's security policy for voice, video, data, and applications. Simple, always-on connectivity encourages adoption, and use of only one client minimizes support costs.
- **Cisco Services:** Cisco Services offers a Secure Mobility Network Strategy and Architecture workshop. Deliverables include a high-level architecture strategy, requirements document, and agency use cases.

What Are the Benefits?

- Mobile personnel can collaborate from anywhere, anytime, on any allowed device, with a predictable experience.
- Network managers easily set policy and manage the network to allow secure access to the appropriate resources.
- Agencies can more efficiently execute missions by empowering personnel to make more timely and informed decisions.

For More Information

To learn more about Cisco cybersecurity solutions for federal government, visit: www.cisco.com/go/uspscybersecurity

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

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**.