How Cisco is Providing Corporate Network Access for Employee Mobile Devices

Cisco corporate policies and Cisco IT services help employees make cost-effective use of mobile smartphones and digital tablets for business communications

Cisco IT Case Study/Mobility/Mobility Services: This case study describes how Cisco IT provides network services for employees who want to use mobile devices for business calls and intranet access. Previously, smartphones were a productivity tool, paid for by Cisco for specific employees. But this model has been challenged by new devices, new capabilities, and a need to cut costs while enabling any Cisco employee to connect securely to the corporate network from his or her mobile device. Cisco IT now provides a wide range of mobility services to reflect these changes. Cisco customers can draw on Cisco IT's real-world experience in this area to help support similar enterprise needs.

BACKGROUND

Since 2007, Cisco has changed how it approves, pays for, and supports mobile phones and their associated service plans when used by employees for business purposes.

> "The demand among employees for connecting their mobile devices to our network is getting bigger and becoming more complicated. Our model for delivering mobility services is allowing us to easily handle this kind of growth."
>
> **– Brett Belding, Manager, Cisco IT Mobility Services**

In the early 2000s,the arrival of smartphones that could handle voice and data created the need for Cisco IT to offer mobility services. The goal was to deliver increased productivity to sales, customer support, and executive-level employees by giving them access to their business email, calendars, and contacts, as well as access to internal web content and applications from mobile devices.

In the initial mobility services offering, Cisco IT paid for, owned, provisioned, and supported a limited number of specific types of mobile devices and service plans used by eligible employees. In many ways, once an employee established his or her eligibility for a company-paid mobile device, Cisco IT's services for mobility mirrored its laptop computer policies. Employees could select from a very small number of approved devices, which would be paid for and supported by Cisco IT.

No network access was available for an employee's personally owned phone, because this access was perceived as both unnecessary and a potential network security risk. Many employees carried two phones, one for work and one for their personal use. Over time, more employees boughtsmartphones for personal use as well.

The early Cisco IT mobility services were offered on an externally developed secure messaging platform that supported a limited number of phone types. This platform allowed Cisco IT to accommodate the different device and service choices that were available from different carriers around the world, although the RIM BlackBerry was the mobile device preferred by Cisco IT.

EXECUTIVE SUMMARY

BACKGROUND

- Since 2007, Cisco has changed how it approves, pays for, and supports mobile phones and their associated service plans when used by employees for business purposes.

CHALLENGE

- Emergence of popular smartphones and digital tablets
- Cutting costs in a recession
- Finding a new delivery platform for mobility services

SOLUTION

- Approving mobile devices based on secure operating systems
- Establishing new requirements for mobile device security
- Reducing corporate-paid accounts while allowing access from employees' personal devices
- Creating online wiki for user self-support

RESULTS

- Reduced costs by 30 percent while serving 42,000 mobile devices
- Established a service delivery model that easily scales to meet growth in users and devices

LESSONS LEARNED

- Block network access by non-approved devices
- Educate users about SIM cards
- Control costs with regular eligibility reviews
- Encourage use of corporate network services
- Reduce potential exposure of confidential information
- Provide resources for user self-support

NEXT STEPS

- Support more user services and devices
- Improve VPN access
- Migrate user support wiki to Cisco IWE

CHALLENGE

Starting in 2007, three high-level challenges prompted Cisco IT to review and change key aspects of its mobility services strategy.

First, the Apple iPhone became popular among Cisco employees, and other mobile devices manufacturers started to sell their own smartphones. The emergence of tablet devices, such as the Apple IPad and the Cisco Cius™ business tablet, also increased employee interest in mobility services.

Second, the global economic downturn forced Cisco to cut expenses and to reviewthe ongoing costs of Cisco-paid mobile phone services, as well as the time and effort required to test individual mobile device models. Cisco evaluated factors such as which employees were entitled to company-paid mobile phones and service plans, the number and type of mobile devices that Cisco IT would support, and an internal budget charge for employee use of the Cisco IT mobility services.

Finally, a significant change occurred, which involved moving from the single mobile messaging software platform previously used by Cisco IT for all devices to using the native messaging platforms in newer smartphones. "We wanted to change our messaging platformin order to certify mobile devices more quickly and reduce the costs associated with our certification process," says Jason Freeth, Cisco IT architect for mobility solutions.

SOLUTION

Cisco IT found the solution to these challenges by refining policies and strategies in four major areas:

- Device approval and security
- Services offered to users and the service-delivery platform
- Cost reimbursement for employees and for Cisco IT
- Resources for user support

Approved Mobile Devices

During the early years of offering mobility services, Cisco IT performed extensive testing on individual mobile devices before adding them to the approved list. That support model proved impossible with the large and increasing number of mobile devices available over time.

Today, Cisco IT primarily approves new mobile devices based on the operating system, for example, Apple iOS, Android, and BlackBerry. "It's the operating system that provides most of the device security and other capabilities that we're concerned about," says Paul Clements, Cisco IT technical lead for mobile solutions. "If it's not a BlackBerry device, we also consider whether the device supports the security policies we require such as using Microsoft ActiveSync technology, which we now use forsynchronizing a user's email, calendar, and contact list between a mobile device and our Microsoft Exchange environment."

As of mid-2011, more than 50 different mobile devices, including smartphones and tablets, were on the Cisco IT

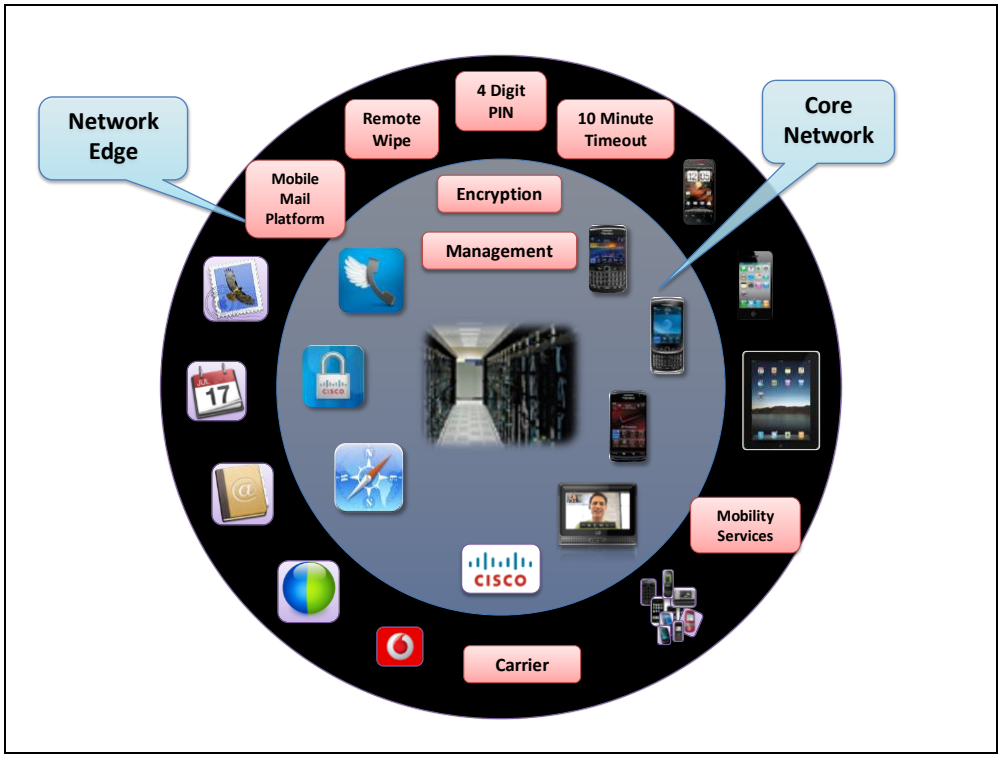
validated list, based on their wide availability and compliance with Cisco IT security requirements.

"Currently, the RIM BlackBerry, Apple devices running the latest Apple iOS version, and the Cisco Cius tablet provide the device security necessary for access to the broadest array of Cisco IT mobility services, including data and applications on the corporate intranet," says Brett Belding, manager of Cisco IT mobility services."Devices based on other operating systems can access a smaller subset of user features, or we restrictthem to accessing only the user's corporate email, calendar, and contacts."Even for access to these basic services, Cisco IT requires that the device meet certain security requirements.

Mobile Device Security

The type and strength of security measures in a mobile device present two critical concerns for any IT department that offers mobility services. First, the mobile device stores proprietary information such as contacts and emails. If the device is lost or stolen that information should not be accessible to others. Second, email and web applicationscontain confidential information, so users and their mobile devices must be authenticated before they can accessinternal resources. These concerns can be addressed by two types of security: securing the device's content and securing the device's access to the corporate network. (Figure 1)

Figure 1. Cisco IT Security Design for Mobility Services



"As a principle for mobile device security, the more the device can access, the more security we require," says Freeth.In order to access mobile services in the network edge (shown in the outer ring on this diagram), the mobile device must meet the security requirements listed below before it is considered to be a trusted device by Cisco IT.A device that does not comply with thesebasic requirements cannot connect to the Cisco network.

- Built-in content encryption to prevent display of sensitive information such as contacts and email if the device is lost or stolen

- Minimum four-digit password for accessing the phone's content and applications
- Password re-entry required after 10 minutes of inactivity
- Phone automatically wipes its content after 10 invalid password-entry attempts

Accessing the mobile services within Cisco core network (shown in the inner ring on the diagram) requires an additional security measure: use of the Cisco AnyConnect VPN client.

Additionally, the user must register with Cisco IT the phone number and/orunique device identifier (UDID) for the mobile device, and only that device can access internal services. Device registration also allows Cisco IT to apply encryption to content (data at rest) in the device and perform device management tasks such as checking the inventory of software versions and device status.

"These security requirements protect the device itself, but they can also help prevent a third party from getting unauthorized access to Cisco applications and confidential information," says Clements. "In addition, we have defined which services are available to users based on their device, which means they can't access anything their smartphone or tablet can't protect."

During the user-driven setup process, security practices are presented in a Rules of Use document, which users must view and acknowledge in order to receive approval for mobility services. This document covers security issues such as not "jailbreaking" the mobile device (that is, obtaining root level or command line access), protecting confidential data, and regularly updating the device's operating system software.

Mobility Services for Users

The growing popularity of smartphones and tablets prompted Cisco IT to transform itsmobility strategy from supporting only a small number of devices and a limited list of services to a strategy that supports many different devices and multiple user services.

PRODUCT LIST

Mobility
- Cisco Mobile solutions
- Cisco Cius
- Cisco AnyConnect VPN client
- Cisco Virtual Office

Unified Communications
- Cisco Unity®

Video and Collaboration
- Cisco WebEx®

In the earlier strategy, an employee would request a specific mobile device. Cisco IT would provision specific services to that device, delivering a predefined user experience.

In the new strategy, an employee requests access to a type of mobility service, which is approved and paid for by the employee’s department. Cisco IT provisions that service and allows the employee to connect to it natively from multiple devices, such as a smartphone and a tablet. The employee simply configures additional devices with the same set of access credentials. Activating multiple devices does not result in additional internal service charges to the employee's department, and approval from the employee’s manager is not required.

Today, most Cisco employees are choosing smartphones as their primary mobile device, and many are using tablets as a secondary mobile device. As of mid-2011, 15 percent of Cisco employees with mobile services carry a laptop, a smartphone, and a tablet, a trend that is increasing. Based on the device’s security level and capabilities, Cisco IT provides the mobility services listed in Table 1.

Table 1. Cisco IT Mobility Services Set

Mobile Mail Essentials: Access to corporate email, calendar, and contact lists Cisco® WebEx conference participation from a mobile phone Enterprise instant messaging (IM) Access to the Cisco intranet for business data and applications Dual-mode voice support (using a wireless LAN to make calls instead of mobile plan minutes). Dual-mode voice is delivered with device-specific Cisco Mobile solutions.	Single Number Reach (SNR) features for call forwarding from an employee's business phone number Visual Voicemail, which provides a visual display and tools for handling messages in a Cisco Unity voice mailbox Mobile access to the Integrated Workforce Experience (IWE) Powered by Cisco Quad™, Cisco employees' internal collaboration portal, using the Quad mobile client

The Mobile Mail Essentials service offers direct, secure access to Cisco email servers over a mobile carrier or wireless LAN connection and, in most cases, uses the device's native functionality for email, calendar, and contacts. To deliver the Mobile Mail Essentials services, Cisco IT uses the Microsoft ActiveSync platform, which is supported by many mobile device operating systems. BlackBerry users are supported by the BlackBerry Enterprise Server (BES) infrastructure, which isspecific to that operating system.

Not all devices can support all service features. For example, only some devices provide access to 802.11 wireless LAN connections; this access is required to make calls over a wireless LAN.Other devices cannot support a VPN client. To help guide user purchases, Cisco IT provides employees with a menu of popular mobile devices that shows which devices can support which features. Still, Cisco IT has a goal of increasing the services offered to each approved device, in part by leveraging the Cisco AnyConnect VPN client and third-party solutions for managing mobile devices.

Employee Eligibility and Who Pays for What

To control costs, Cisco has established corporate wide policies that define an employee's eligibility for company-paid mobile devices and associated service plans. In most cases, the employee pays for the mobile device and its associated service plan. However, this corporate policy can be modified by each Cisco department or regional/country organization as needed to match local business or legalrequirements.

For a small number of eligible employees, Cisco covers the cost of monthly mobile service plans as defined by company policy. (In most cases, the employee must purchase the mobile device.) Requests for a company-paid mobile account must be approved by a company vice president to control the costs of mobile communications. "At an average cost of US $120 per month per line, mobile service charges can quickly become a very large annual expense," says Belding. "With this policy, only employees whose job roles really justify a company-paid mobile account are likely to request approval at the VP level, which reduces the number of accounts that exist primarily for employee convenience."

Employees who are eligible for Cisco-paid smartphone service are added to the Cisco corporate plan(where applicable), and Cisco is billed directly for the employee's monthly mobile service charges. Cisco has negotiated contracts with mobile carriers worldwide to reduce costs.

Employees who are not eligible for Cisco-paid mobile service can request approval from their manager for accessingthe Cisco network with their personal smartphone and personal-paid service plan. In this case, the employee pays for any apps, family plan, termination fees, overage charges for call minutes or data usage, and additional mobile services. These options are not allowed on a Cisco corporate-paid mobile account.

Cisco IT also charges the employee's department for use of the mobility services. These monthly, per-user charges offset the costs incurred by Cisco IT for developing, maintaining, and delivering the mobility services. The charges are adjusted annually, based on Cisco IT's actual costs for the current infrastructure and to allow for ongoing growth

in the number of users.

User Support

Substantial variations exist in the availability of mobile devices, services, and service plans among different countries and different carriers. These variations are confusing for users and are the largest source of mobility-services support requests for Cisco IT.

Cisco IT provides most user support through an internal mobility services wiki. Employees can use the wiki for common tasks such as:

- Learning about mobility services availability, approved devices, and employee eligibility
- Requesting approval for a company-paid account or service access from a personal-paid account
- Obtaining online support for configuring specific device types through FAQ documents and user discussion forums
- Reporting a lost or stolen device
- Learning about device setup and finding support processes and tips

Because this is an open wiki, employees can update and improve these topic areas for everyone else."By encouraging user participation, we are building a user community where they can share ideas and recommendations and help us to quickly identify needed new services," says Belding.

RESULTS

"When the recession hit, we performed a complete audit of our mobile service expenses to identify where we could cut costs," says Belding. "We were able to reduce our expenses by 30 percent simply by identifying lines that were no longer used and employees who didn't really need company-paid mobile devices given their job role."

As ofmid-2011, Cisco IT provides mobility services to 42,000 mobile devices, an increase of more than 40 percent in one year. Nearly 7,000 of these devices are voice-only phones and pagers that are typically passed within a team of on-call employees. The number of voice-only devices is declining as they are replaced by smartphones when service contracts are renewed.

"The demand among employees for connecting their mobile devices to our network is getting bigger and becoming more complicated," says Belding. "Our model for delivering mobility services is allowing us tohandle this kind of growth."

“We were able to reduce our expenses by 30 percent simply by identifying lines that were no longer used and employees who didn't really need company-paid mobile devices given their job role.”

– Brett Belding, Manager, Cisco IT Mobility Services

Mobility services are used by Cisco employees in more than 70 countries, with the largest number of users in the United States and working in sales, customer support, and company operations roles. Approximately 15 percent of the mobile devices connecting to the Cisco network are secondary devices for the employee. The most popular device combinations are an iPhone or BlackBerry smartphone with a tablet. Some employees also connect using their company-paid BlackBerry phone and their own personal-paid smartphone.

The availability of online help resources for mobility services means the number of related support cases received by the Cisco helpdesk has declinedsteadily, with just three cases per 100 users per month as of early 2011.

LESSONS LEARNED

With more than a decade of experience in delivering mobility services to employees, Cisco IT has gained several valuable lessons.

Require secure VPN access. To protect the Cisco corporate network and the confidentiality of user sessions, employees must use the Cisco AnyConnect VPN client to establish a secure connection when outside of a Cisco

environment. However, employees can use their mobile devices to openly connect on the secure wireless LANs inCisco offices or on a Cisco Virtual Office wireless router at home.

Educate users about Subscriber Identity Module (SIM) cards. When employees buy a new phone, it is often possible to insert the SIM card from the old phone to maintain mobile service information. However, employees may not be aware of the differences in service plans and data usage that may not be compatible with the old SIM card, especially if it is designed for use with a different carrier or device. These differences can affect the employee's mobile service charges and create unexpectedly high bills. To help prevent this issue, Cisco IT advises users not to swap SIM cards among phones.

Control costs with regular eligibility reviews. The required approval from an employee's manager or VP provides an initial way for Cisco to control its costs for mobile services. Two additional procedures help with cost control: reviewing an employee's continued eligibility when a corporate-paid account reaches its service renewal date and requiring employees who change jobs to reapply for mobile services approval from their new manager.

Encourage use of corporate network services. Cisco IT gives employees tips for reducing use of mobile phoneminutes and the potential for overage charges. For example, Cisco IT recommends using the Cisco WebEx dial-back feature when participating in voice conferences from mobile phones. Using a local Wi-Fi service for data access can reduce roaming charges. However, employees may not realize that using a smartphone as a portable Wi-Fi hotspot can mean costly extra charges.

Reduce potential exposure of confidential information. Cisco corporate policies on information security prohibit employees from forwarding or synchronizing their business emails with an external service (for example, Apple MobileMe) that allows viewing messages on a webpage. As these types of services become popular for personal use, employees may need to receive specific communications about the security risks.

Provide resources for user self-support. It can be difficult for users to understand where to obtain support for network access and phone setup issues: should they call the Cisco help desk, the mobile carrier, or a phone retailer? To encourage users to find support information themselves, Cisco IT continues to add content to the internal support wiki, service activation emails, and other communications. However, some users prefer to call a helpdesk, especially when setting up the phone, and may never use self-support resources.

Develop policies and procedures for deleting device content. What happens to the sensitive information stored on a mobile device when an employee leaves the company is an important issue. As part of the Rules of Use, Cisco requires employees to agree that their mobile device content will be wiped completely when their employment ends. Depending on the circumstances, Cisco IT may perform this wipe remotely or provide instructions for the employee to perform this task.

NEXT STEPS

Cisco IT will continue to focus its mobility services efforts on supporting more user services and more devices as well as providing improved VPN access with the Cisco AnyConnect client.

To provide more online self-support resources for users, Cisco IT willmigrate the mobility services wiki to the internal Cisco IWE collaboration community, which is powered by the Cisco Quad platform (Figure 2). IWE will allow users to share information such as news and device reviews, access aportal for ordering Cisco IT mobility services, and receive support from other users around the globe.

Figure 2. Cisco IT Mobility Services Community Offers Employees Online Self-Support

FOR MORE INFORMATION

For information on Cisco solutions for mobility services, visit:www.cisco.com/go/mobility.

The Cisco on Cisco blog contains posts on mobile communications topics:http://blogs.cisco.com/category/ciscoit/.

For additional Cisco IT case studies on a variety of business solutions, visit Cisco on Cisco: Inside Cisco IT:www.cisco.com/go/ciscoit.

NOTE

This publication describes how Cisco has benefited from the deployment of its own products. Many factors may have contributed to the results and benefits described; Cisco does not guarantee comparable results elsewhere.

CISCO PROVIDES THIS PUBLICATION AS IS WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.Some jurisdictions do not allow disclaimer of express or implied warranties, therefore this disclaimer may not apply to

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.**

you.