White Paper

# Enterprise Mobility: Securing a Productive and Competitive Future

## What You Will Learn

As more organizations adopt new business models related to mobility, the cloud, the Internet of Things (IoT), and the Internet of Everything (IoE), the enterprise is becoming an amorphous environment. Smartphones, tablets, other endpoint devices, and web applications are irreversibly changing the way people work and play online. Cisco has embraced an “Any Device” vision. In this vision, enterprises:

- Give employees greater choice in the devices they use
- Maintain a common, predictable user experience
- Enhance their productivity, security, and global competitiveness

Enterprises and other large organizations must decide whether to allow certain users, devices, and locations access to company networks, data, and services and to what extent access should be tiered according to business and user needs. Based on real Cisco experiences, this white paper discusses the steps and business decisions that information and security officers, enterprise IT, and information security architects should consider as they begin the journey to Any Device.

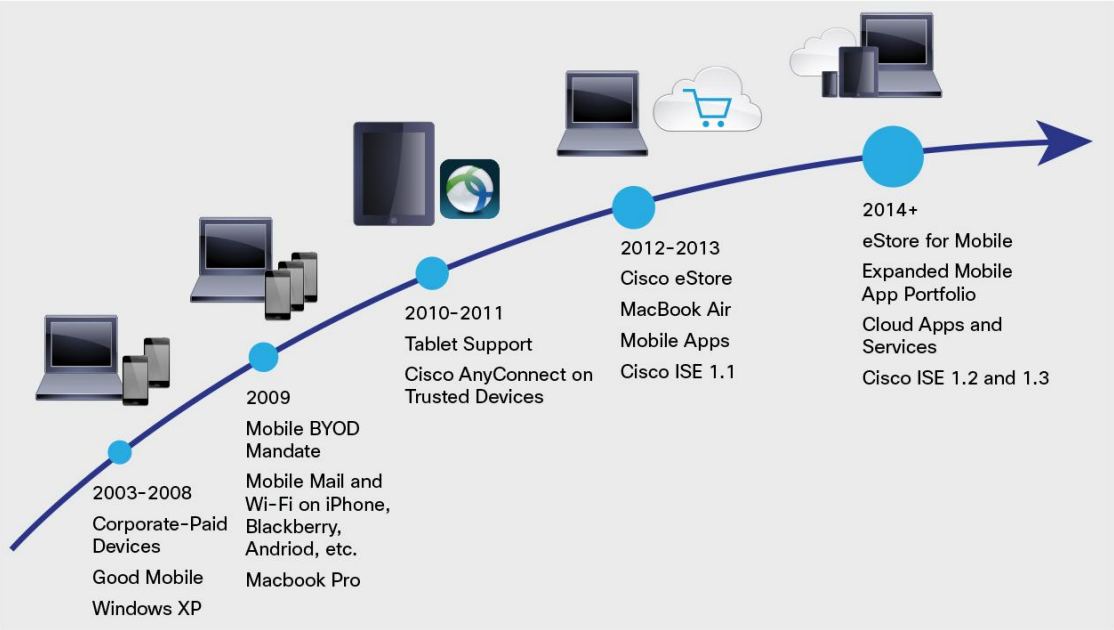
## Introduction

Every day, Cisco’s workforce uses more than 82,000 Windows laptops, 32,000 Macintosh computers, 10,000 Linux machines, and 72,000 iPhones, iPads, and Windows and Android devices. Our more than 70,000 employees and 30,000 global contractors, consultants, and business partners decidedly want more choice in the devices they use for work. And they want freedom in where they use those devices to access corporate networks, systems, applications, data, and online services. While all laptops are provided by Cisco, the vast majority of smartphones and tablets are personally owned. Most Cisco workers use both a computer and a smartphone to access company IT services, and more than 20 percent use more than two devices. The diversity of those devices is growing exponentially.

More than a decade ago, Cisco embarked on a long-term vision called Any Device (depicted in Figure 1). The goal is to allow greater choice in devices while maintaining a common, predictable user experience that enhances global organizational competitiveness and security in an increasingly mobile workspace.

© 2015 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

**Figure 1.** The Cisco Any Device Roadmap




The primary business reasons behind the Any Device vision include:

- **Productivity:** Tech-savvy Cisco employees can use their smartphones, tablets, or laptops of choice to do company work when and where they want, improving job satisfaction and productivity.
- **An evolving workforce:** Members of today's technology-savvy generation who are entering the workforce are used to having control of their work tools and environment, and they want to choose how they can be most productive.
- **Innovation:** Allowing workers to use next-generation devices as soon as they are released may result in further productivity gains. Early adopters often signal larger marketplace shifts, which can positively influence Cisco IT adoption and Cisco product strategy.
- **Acquisition integration:** Cisco's many corporate acquisitions join the fold with their own pools of nonstandard devices. Any Device helps to integrate new divisions quickly and reduce associated security risks.
- **Capital costs:** Cisco employs tens of thousands of contractors and consultants in locations around the world. Cisco must optimize and reduce costs associated with this workforce. By migrating contractors and consultants to the Any Device program, Cisco realizes a significant annual savings per user.

To support this business direction, Cisco's IT strategy includes the following considerations:

- A scaled architecture to support any trusted device through industry-standard platforms, transparent connectivity, integrated security, and ease of management
- Flexible liability from splitting voice and data costs from the hardware based on well-defined policy and usage rules across personal smartphones and tablets, corporate-owned laptops, and optional corporate mobile services
- Expense management to proactively optimize cost strategies with strong service provider relationships and innovative pricing models

© 2015 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

- Robust application lifecycles based on evolving user needs and enterprise and line of business requirements, with applications easily accessible through the Cisco eStore, a single mobile app store with more than 60 apps and growing
- Social support with self-service content, proactive communications, and one-to-many interactive support as well as traditional one-to-one support as needed

Other organizations have their own distinct reasons to adopt an Any Device strategy. They may need to strengthen their data security, increase their mobility, or create collaborative work environments to share access to real-time data. Any Device programs also vary depending on industry and regulatory requirements. As the choice and number of endpoint devices increase, and as new business models redefine connectivity in ways that are just emerging, enterprises must consider who and what they will allow to access their applications and data, both within their network and outside it. Then, they need to determine how to plan, track, account for, and enforce those policies.

This paper discusses the following aspects of the Any Device vision:

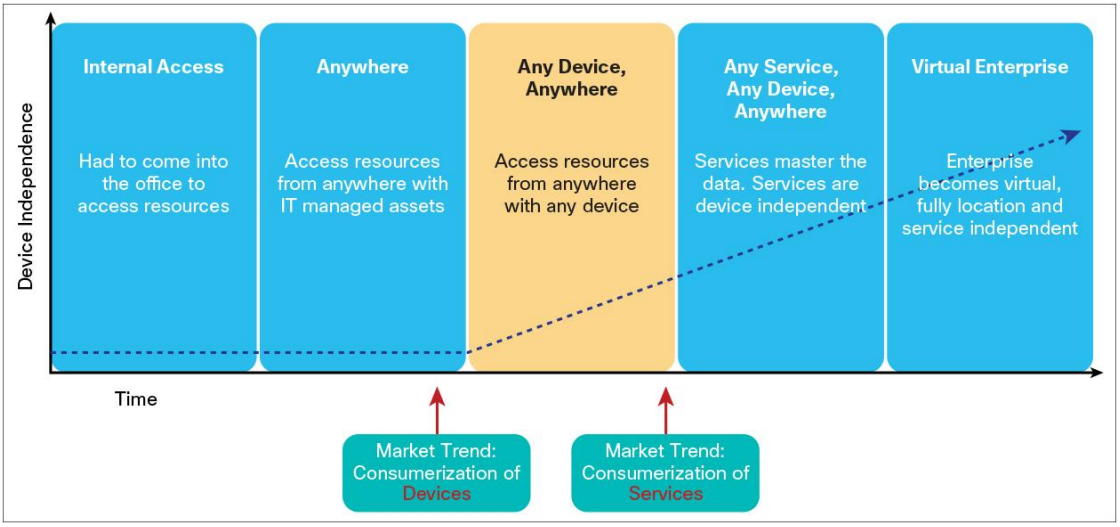
- Risks, rewards, and changes to business, IT, and security policies
- Solutions that Cisco is currently implementing
- Other considerations that Cisco has encountered along its Any Device journey

With a flexible, proactive approach, organizations can craft a model that best meets their needs and evolves with an ever-expanding, connected environment.

## Stages of the Cisco Any Device Journey

The past 15 years have brought a significant change in the way users access the Cisco network (see Figure 2).

**Figure 2.** The Stages of Workforce Access along the Any Device Journey




© 2015 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

### Stage 1: Internal Access

As the last millennium came to a close, all IT devices resided within corporate locations, and employees had to be physically in an office for **internal access** to IT resources, as shown in Stage 1 of Figure 2.

#### Cisco Trusted-Device Policy

Architectural principles should be translated into technical specifications to guide organizations toward implementable solutions. Trusted devices should comply with the following policy enforcement and asset-management requirements.

**Policy Enforcement**

Devices that access corporate services should validate the implementation of the following security controls before they are connected. Unauthorized removal of these controls should disable access to enterprise resources:

- Local access controls that enforce strong passwords (complexity)
- 10-minute inactivity timeouts, and a lockout after 10 unsuccessful login attempts
- Encryption that includes the encryption of any device or data that is sensitive to Cisco
- Remote wipe and lock capabilities when an employee is terminated or a device is lost or stolen
- Inventory tracking capabilities to check the presence of specific security software, patch updates, and corporate applications and versions

**Asset Management**

Devices that access corporate services should adhere to a number of controls. The devices should be:

- Uniquely identifiable where identification is not trivially spoofed
- Explicitly and individually authorized for corporate access, and registered and traceable to a specific user
- Capable of blocking corporate access
- Capable of producing forensic log data (for example, security software logs, user authentication and authorization, and configuration changes) if required for investigation

### Stage 2: Anywhere

Over time, laptops and VPNs gave workers mobility, and an increasingly globalized workforce made more flexible work patterns necessary. Stage 2 depicts how work environments and regular office hours no longer restricted productivity, as a more mobile workforce accessed corporate IT resources from such locations as customer sites, homes, cafés, or hotels. With this dissolution of geographic borders, users can access resources from anywhere with IT-managed assets.

### Stage 3: Any Device, Anywhere

In recent years the commoditization of smartphones, tablets, and laptops has brought about outstanding new features, upgrades to functions, more efficient form factors, and shortened device lifecycles. As a result, employees want to use their own devices to do everything from accessing the company email and intranet to using corporate business applications. These factors came into play in a relatively short timeframe that challenged corporate IT support and security teams. Furthermore, employees who joined Cisco through an acquisition wanted to continue to use their preferred devices for work even when those device profiles didn't align with Cisco corporate standards.

The rapid adoption of new client technologies has led to the implementation of approaches, tools, and technologies from other enterprises. It has created communities of users and allowed a transformational change in how the Cisco IT staff provides support and how end users are able to use the knowledge of their peers to solve common problems. Cisco IT's role within these communities is not to own a process but to contribute as a peer.

For example, the introduction of Apple products within Cisco was initially led by users who brought these devices into the environment as their preferred tools and platforms on which to conduct business. An estimated 3,000 Mac users were within Cisco before the IT team officially made these tools available to the greater population. Independent of IT, Mac users initiated an effort to provide setup, use, and maintenance assistance through email aliases, wikis, the intranet, and video content. When Cisco IT began offering the Mac as an option as part of its PC Refresh procedure, IT adopted the self-support model without disrupting or changing the Mac community. IT has embraced this model and used it to develop more self-supporting services.

© 2015 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Together, these developments signaled the need for a new corporate device strategy that answered a fundamental yet imperative question: As we see new business models related to mobility, cloud, the IoT, and IoE continue to expand, how can we provide people with safe access to corporate resources from any device, and from anywhere?

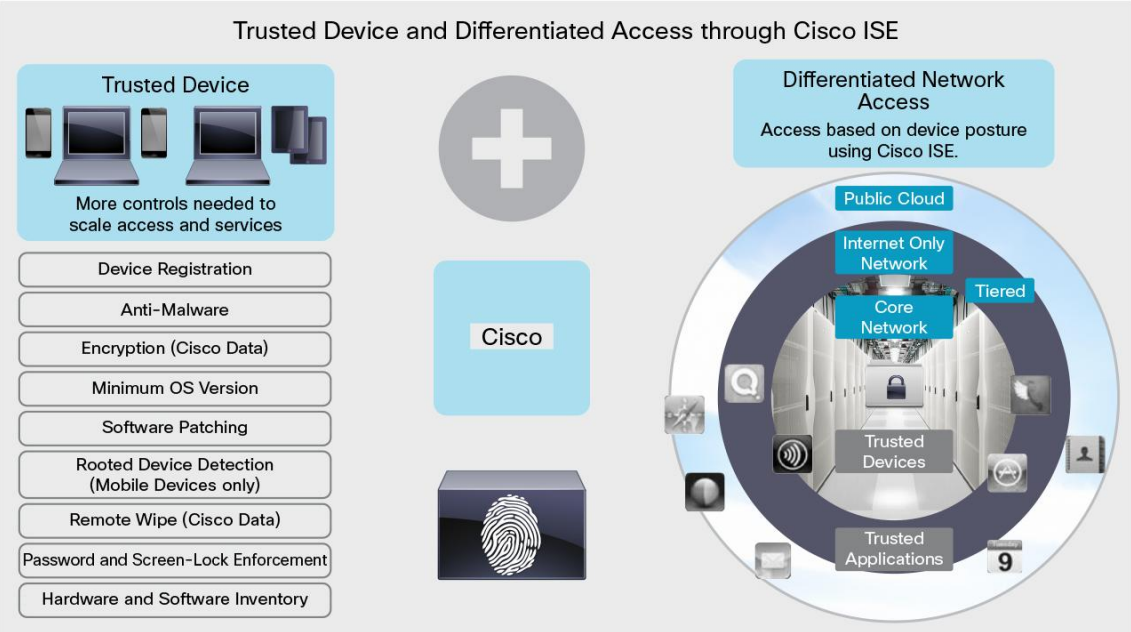
**Potential Any Device Risks**

Organizations should plan to address the following Any Device risks:

- Loss of control over corporate data stored on the device, including regulatory or customer data
- Loss of control over the device posture:
  - Less control of overall device security may increase the risk of exploitation and create an attack vector to infrastructure and services
  - Devices may not conform to policy and operational models, potentially damaging business relationships, affecting legal or regulatory requirements, and driving up support costs
- Less visibility into the devices connected to the network (where they are and who owns and operates them) leads to challenges for security, licensing, regulatory and legal assurance, and audits

Not every worker requires the same level or type of access to the corporate infrastructure. Some need only email and calendaring services on their smartphones, whereas others may require greater levels of access. For example, Cisco sales professionals can access ordering tools from their smartphones, increasing their ability to close a sale. This situation created tiers of network access depending on the sensitivity and location of the data being accessed, as shown in Figure 3. As a baseline, workers need to use "trusted applications" for business activities. As workers require deeper access to the core network, they must use "trusted devices." Protection measures on the device must increase from simple device registration, password and screen-lock enforcement, and remote content wiping to compliance with security policies enforced by the Cisco® Identity Services Engine (ISE).

**Figure 3.** Differentiated Network Access




## Stage 4: Any Service, Any Device, Anywhere

Cisco currently allows users to access corporate resources housed on premises and in the cloud. Transparent connectivity, trusted-device standards, a single mobile app store, a threat-centric security model, and a dynamic self-support model are foundational elements that continue to support the business in its Any Device journey. Business productivity, one of the primary reasons behind the Any Device vision, is increasing significantly along with employee satisfaction.

© 2015 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

### Stage 5: Virtual Enterprise

The Virtual Enterprise, a logical evolution from Stage 4, becomes increasingly location and service independent. In this stage, the enterprise has a mature identity model that allows for precise access control and external collaboration. The full extent of security controls and capabilities is applied to enterprise data. The Virtual Enterprise will be addressed as we progress further toward it.

## Making Any Device a Reality: A Closer Look at Cisco's Approach

At one time, Cisco employees were finding their own ways to access email and work files from their smartphones and tablets. Recognizing the need for more than a simple bring-your-own-device (BYOD) policy, Cisco developed a comprehensive Any Device strategy. The strategy took into consideration mobile devices issued by Cisco and purchased by the employee. It also addressed access to applications, security requirements, and the user experience.

**Cisco SalesMobile App Business Value**

In the first month that the SalesMobile app was introduced, results included:

- $561,671,325 in revenue transacted
- 40 percent acceleration of deal approval
- Viral adoption through Cisco eStore

"I have to say, I love this app. Approving a deal on the road lets sales flow!" - Cisco regional sales manager

"This app is super cool and super easy to use. Liberation!" - Cisco country manager

With a focus on business-to-employee (B2E) mobility, Cisco infrastructure and technologies are combined with strong partner solutions in a strategy that can evolve as the business and users require. Cisco's program lowered costs, improved user productivity and satisfaction, and reduced security risks. This section explores Cisco's journey to come to a more mature Any Device architecture, including how Any Device has challenged traditional security norms, and which solutions Cisco has deployed.

### Architecture Overview

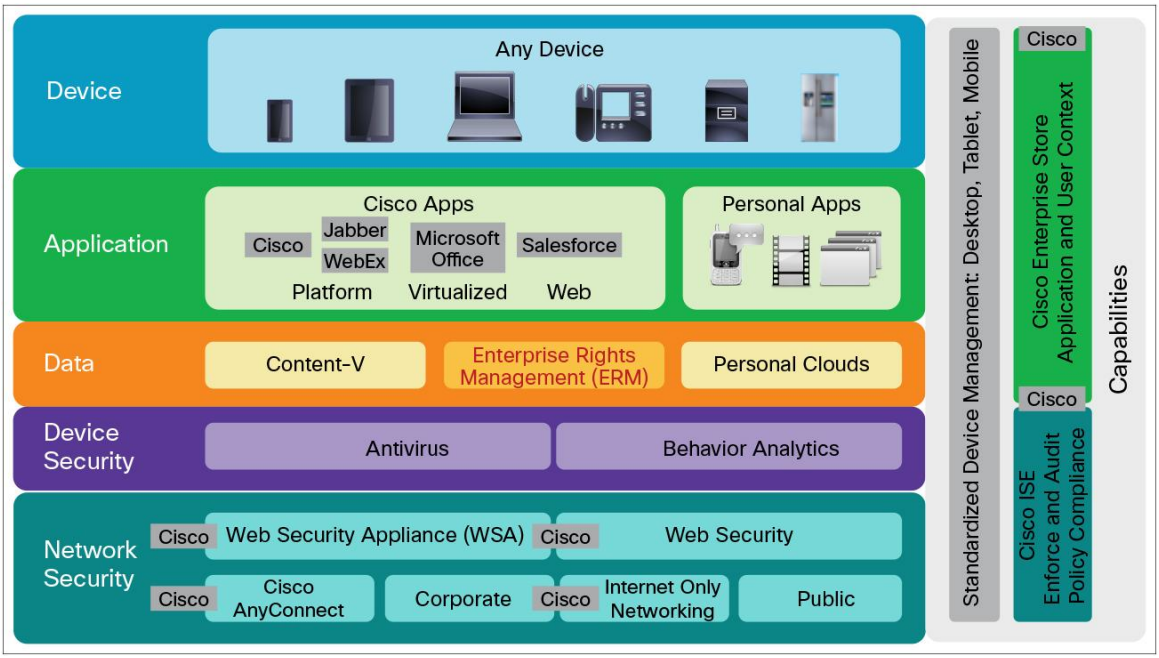
Today, all Cisco employees can connect to the network using any device that meets Cisco security standards. These devices can be issued by Cisco, in the case of laptops, or purchased by the employee. They include iPhones, iPads, Android devices, and Windows devices. Most employees choose and pay for their own smartphone or tablet. Either the employee or Cisco pays for the service plan, depending on the employee's role. Employees use these devices throughout the workday. They can receive calls to their office number on their device. They can synchronize their device's native calendar, email, and contacts with the corporate Microsoft Exchange environment. They can use collaboration applications such as Cisco WebEx® Meetings and Cisco Jabber®. They can also establish a highly secure VPN connection to the intranet to view internal webpages, approve sales, submit expense reports, find the nearest available meeting room, and more.

The Any Device solution takes advantage of Cisco technologies already deployed:

- Wired, wireless, and VPN access networks
- Cisco ISE, which enforces security policies based on who is asking and when, how, and from what device.
- Unified communications and collaboration applications. These include Cisco Unified Communications Manager, Cisco WebEx, and Cisco Jabber. The applications are hosted on Cisco Unified Computing System™ (Cisco UCS®) platforms.

© 2015 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

**Figure 4.** High-Level Architecture




## Design

Cisco designed the solution to provide highly secure access to collaboration tools and the intranet with as little IT development and testing as possible in order to save internal IT resources and expedite delivery. By using the native encryption, email, calendaring, and contacts capabilities in each device's operating system, Cisco eliminated the need for internal development and constant regression testing of third-party solutions as device vendors updated their operating systems.

Microsoft ActiveSync syncs the devices' native email, calendar, and contacts with Microsoft Exchange. ActiveSync also provides basic security functions, such as enforcing the use of a PIN to unlock the device and enabling remote content wiping.

### Application Design

The project lifecycle comprised planning, deployment, implementation, and operations. Throughout the lifecycle, the Cisco IT Mobility team worked with Cisco IT applications teams for Windows Messaging, Windows Exchange, Cisco WebEx, Cisco Jabber, and the Cisco AnyConnect® Secure Mobility Client.

The guiding principle for application design was to make the user experience at least as easy with a smartphone or tablet as it was with a laptop. To accomplish this, the team uses the native capabilities of the device's operating system (email, calendaring, encryption, and so on) whenever possible. When another step is necessary, such as establishing a VPN connection, Cisco tries to reduce the number of actions employees need to take. For example, Cisco AnyConnect automatically sets up a highly secure VPN connection whenever an employee opens any other application, such as a web browser, custom app, or Cisco Jabber. AnyConnect launches in just one to two seconds and stays connected until the smartphone or tablet is turned off.

© 2015 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

The team uses APIs to automate management tasks such as making sure that new users are in the right Active Directory group. APIs also integrate the internally developed Enterprise Management (EMAN) platform with Active Directory, the third-party mobile device management (MDM) solution, and the Cisco AnyConnect Secure Mobility Client.

The team also uses APIs in the Cisco eStore to automate service provisioning. The eStore is based on the Cisco Prime™ Service Catalog and Cisco Process Orchestrator, and it integrates with the MDM, Active Directory, and Cisco ISE. This integration enables Cisco to automate processes such as screening employees for eligibility, sending an email notification about the service to the employee's manager, provisioning the service, and managing the service lifecycle.

**Disaster Recovery**

Cisco uses the same disaster recovery architecture for email and VPN access that it uses for all other employee services. The email servers and Cisco AnyConnect VPN headends are deployed in its metro virtual data center (MVDC) in an active-active, load-balanced configuration. If one site goes down, the server in the other site takes over its workload. Any changes to the solution architecture are made in all data centers at the same time and tested thoroughly.

## Deployment

Cisco implemented the Any Device program in the following phases:

1. Automated the provisioning of email and cellular services (2008)
2. Deployed Microsoft ActiveSync so that employees could sync contacts and email with iPhones and Android devices (2009).
3. Began using the Cisco AnyConnect Secure Mobility Client to connect to the VPN from selected personal devices (2011)
4. Built eStore, a one-stop shop for provisioning BYOD services (2012)
5. Moved eStore into full production (2013)

Cisco conducted the pilot in one building in San Jose. The team used the building's existing wireless infrastructure, a pair of existing public key infrastructure (PKI) servers in a Cisco data center, and an existing Cisco ISE cluster in another Cisco data center.

After the pilot, Cisco rolled out the program one country at a time. In each country, Cisco added new business functions one by one. Managers were asked to inform their employees about the program.

## Security

As more - and more varied - devices connect, maintaining a strong security posture becomes increasingly challenging. Attackers will take advantage of any weak link in the environment to accomplish their mission. To combat their efforts, Cisco adopted a threat-centric approach to security with solutions that work together to address an array of attack vectors and provide protection anytime and anywhere a threat exists.

Cisco uses the native encryption capabilities in each device's operating system to protect data, such as contacts and email, at rest.

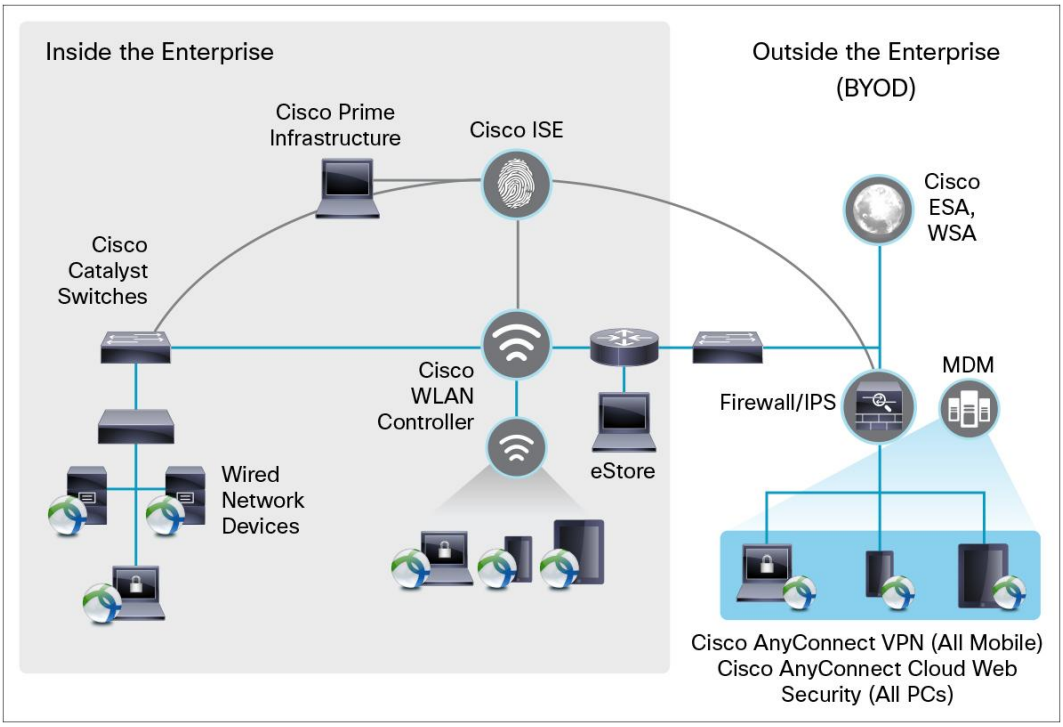
© 2015 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

The architecture for user access includes the following elements, shown in Figure 5:

- Cisco ASA Firewall: Cisco protects its data centers with the Cisco ASA Next-Generation Firewall. It has enterprise-class stateful inspection, application visibility and control, and remote access VPN and advanced clustering for highly secure, high-performance access and high availability.
- Cisco IPS: Cisco uses Cisco IPS to identify, classify, and stop malicious traffic from multiple threat vectors, including network, server, and desktop endpoints. The Cisco ASA Firewall and Cisco IPS are being replaced by Cisco ASA with FirePOWER™ Services. This solution combines the Cisco ASA 5500 Series firewall (with application visibility and control) with the industry-leading Sourcefire® Next-Generation Intrusion Prevention System (NGIPS) and Advanced Malware Protection (AMP) for an integrated threat defense.
- MDM solution: Cisco uses a third-party MDM application to check device posture and deliver applications: The MDM tool makes sure the device is registered and complies with the security posture. Requirements include an approved OS version, a PIN of minimum length, a 10-minute timeout, a remote-wipe capability, content encryption, anti-malware, and the capability to perform a device inventory.
- Cisco ISE: After the MDM solution checks whether a mobile device complies with security policy, Cisco ISE is used to enforce the policy by denying access to devices that are out of compliance. If an employee attempts to access internal resources from a personal device, Cisco ISE controls that access.
- Cisco AnyConnect Secure Mobile Client: Workers who want to access the intranet from mobile devices need to download the Cisco AnyConnect Secure Mobility Client. AnyConnect® supports a highly secure connection to the intranet using the IPsec Internet Key Exchange (IKEv2) and Secure Sockets Layer (SSL) protocols. Clients connect through the Cisco ASA Adaptive Security Appliance, which authenticates the user and encrypts the mobile data stream so that it cannot be read if intercepted.
- Cisco Web Security Appliance (WSA): The WSA screens all requests to access external websites from a device that has the Cisco AnyConnect Secure Mobility Client. WSA evaluates websites based on reputation as well as content. Based on Cisco's internal security policy, it can block or monitor access to entire websites or to specific features such as chat, messaging, video, and audio. Cisco IT blocks only about 2 percent of website requests, but this amounts to approximately 6 to 7 million requests daily. Most sites are blocked because of web reputation information, while 2 percent (500,000 daily) are blocked because of malware like Trojans or Trojan downloaders. For comprehensive malware defense, Cisco Advanced Malware Protection (AMP) is now part of WSA and will be added to the Cisco architecture. Cisco AMP delivers malware detection and blocking, continuous analysis, and retrospective alerting. Cisco plans to use Cisco Cloud Web Security for off-premises users.
- Cisco Email Security Appliance (ESA): The ESA screens all mail that originates outside Cisco, regardless of the device used to access the email. It blocks email from known spam providers and also looks for suspicious content or other email irregularities. Of the 5.6 million emails Cisco receives daily, almost two-thirds are blocked. About 15 percent of email with some marketing content is allowed through, but the ESA server marks it "Marketing" or "Possible Spam." To defeat advanced malware, Cisco AMP is now included in ESA as well and will be added to the Cisco architecture.

© 2015 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

**Figure 5.** Security Architecture for BYOD, Wired Access, and Wireless Access




## Management

Cisco IT delivers all Any Device services following the IT-as-a-service (ITaaS) model, delivering IT services based on how users are using the infrastructure or applications as opposed to an ad hoc approach based on a specific need or user request. Cisco has created a dashboard of service metrics that are reviewed monthly. These metrics include adoption rates, total cost of ownership (TCO), the number of support cases, user satisfaction, and security compliance. If any metric is below the program goals, Cisco investigates to find out why and then takes corrective action.

- Cisco Prime Infrastructure: Cisco IT uses this application for end-to-end network visibility. Visibility extends from the devices (including personal devices) to the data center across wired and wireless networks. End-to-end visibility helps Cisco IT teams to understand, troubleshoot, and fix issues related to applications and services.
- Cisco Prime Service Catalog and Cisco Process Orchestrator: Cisco employees can download mobile applications such as Cisco Jabber and Cisco WebEx through the Cisco eStore, Cisco's internal deployment of the Cisco Prime Service Catalog and Cisco Process Orchestrator. The eStore automates the provisioning process. It screens for eligibility, generates an approval request, provisions the service, and manages the service lifecycle.

### Service Request Management

Initially, Cisco set up an intranet site where employees could add personal devices to the network. Now employees request mobility services through the Mobility community in WebEx Social, which has an intuitive interface. IT's internal EMAN system performs the actual provisioning, but employees don't interact with the software. (Cisco plans to phase out EMAN).

© 2015 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

If an employee requests that Cisco pay for cellular service, the request is routed to the employee's vice president for approval. If the employee pays for the service plan, the eStore sends an email to the employee's manager stating that the service has been provisioned.

**Configuration Management**

Configuration management applies to devices as well as applications.

Whenever device vendors update their hardware or software, Cisco IT tests the upgrade in the Cisco environment. The goal is to make sure that the changes don't affect security and that the device is still compatible with WebEx, Jabber, and other mobile applications.

Cisco also periodically updates WebEx Social, EMAN, the MDM tool, and eStore to take advantage of new devices, operating systems, and applications. For example, when Apple introduced iOS 7 in September 2013, Cisco had to update the Cisco AnyConnect VPN headend and client software. Cisco adds new applications to the eStore monthly, making sure that the applications are highly secure and that they provide a good user experience.

**Capacity Management**

Cisco has been collecting metrics on the program since 2009. Cisco ASA reports the number of AnyConnect users. Cisco ISE reports device usage, such as who connects and with what type of device. This information helps accurately predict demand so that Cisco can scale the infrastructure and decide which devices to support. For example, the metrics showed early on that Symbian devices were losing popularity, so Cisco IT didn't spend time creating Symbian versions of mobile clients.

**Vendor Management**

Cisco IT and Cisco Global Procurement negotiate monthly plan fees from service providers. The team monitors prices to make sure that discounted voice and data plans continue to decrease at the same rate as consumer mobile services plans. Cisco also regularly renegotiates contracts with the vendors to provide discounts on employee-purchased devices.

**IT Infrastructure Considerations**

The Any Device program relieved Cisco IT from having to manage mobile devices, but the team still manages the following:

- Company-paid cellular service plans: Working with Cisco Global Procurement, Cisco IT manages about 35,000 accounts from more than 100 global carriers. Bandwidth for mobile video: Bandwidth inside Cisco TV studios, where employees tend to connect with multiple devices, has already been increased. Cisco expects video bandwidth to become in even greater demand when mobile video applications are added to the eStore so that employees can attend companywide meetings with an in-person experience.
- Wireless coverage: The networking team tracks the number of wireless devices each employee uses. This helps Cisco IT scale the network to provide a great user experience.
- IP address spaces.

**Software License Management**

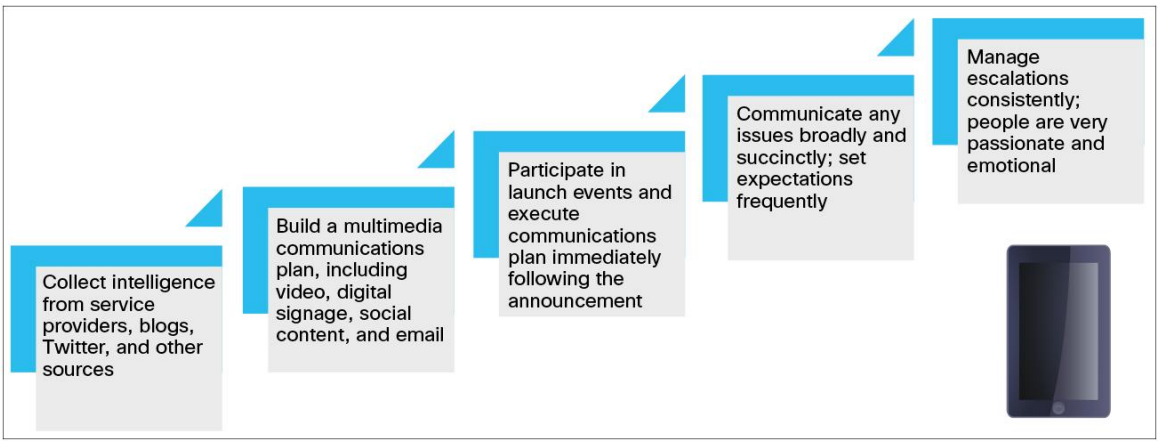
Most of the mobile applications in the eStore are free, so Cisco IT doesn't have to manage software licenses. However, Cisco IT does manage cloud accounts for each employee. When new employees join Cisco, all their cloud services are automatically set up. These include email, VPN access, WebEx, Jabber, and others. When employees leave Cisco, the accounts are automatically terminated.

© 2015 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

### Lifecycle Management

Following social media and other news sources helps Cisco find out about upgrades to device hardware and software as soon as possible (Figure 6). For example, Cisco knew about iOS 8 several months before the actual launch and was able to begin using the beta software the first day it was available. Cisco IT started testing it with Cisco mobile applications and started a WebEx Social discussion about which features did and did not work. On the day of the official launch, Cisco set up a live blog for interactive, real-time sharing of Cisco updates and user feedback.

**Figure 6.** Lifecycle Management




### Service Management

Each month Cisco produces a metrics package that includes adoption rates of new devices and software, help desk cases, user satisfaction scores, cost per user, service provider spending, and the number of fully secured devices. This information helps Cisco decide when to scale the network and which new applications to offer in the eStore. The information is posted to an internally viewable WebEx Social community because other Cisco teams find it valuable. For example, engineers refer to the adoption curves as they decide product strategy.

Cisco constantly monitors the Mobility community on WebEx Social for issues and suggestions. By collaborating closely with the WebEx application team, Cisco IT can make the user experience at least as easy with a smartphone or tablet as it is with a laptop.

## Service and Support

### Incident Support

Despite an 82 percent increase in users from 2011 to 2013, support cases dropped by 33 percent during that same period. The reason is that employees can obtain support through the Mobility community in WebEx Social, including self-help in:

- Choosing the right device and the right service plan
- Getting management authorization
- Signing up for and installing new services
- Supporting services on multiple devices
- Troubleshooting failures and common problems
- Dealing with unexpected costs (especially while traveling)

© 2015 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

- Dealing with the loss or theft of a phone
- Upgrading to a new phone

Employees who don't find answers to their questions in the WebEx Social community can post a question or send an email through one of the lively mailer lists. Approximately six Cisco IT staff members manage and moderate responses and post new content in all of these channels. Cisco encourages user participation in the community.

Employees can also call the Cisco Global Technical Response Center (the internal help desk) for issues that are time-sensitive or require a high level of device expertise. However, Cisco encourages self-support, and most employees prefer it because of the speed of response. The proof is that employee satisfaction rates have increased 28 percent since Cisco created the WebEx Social community.

#### Support Team

A small team makes sure that devices can connect to the network, are highly secure, and have access to critical services. In addition, at least two people support every mobile application in the eStore. The service manager works closely with the Global Technical Response Center, Cisco Employee Connection, Global Business Services, and Global Information Services.

### Funding

Cisco set up the Any Device program to operate as a self-funding business, paid for through a combination of corporate funding and cross-charges to the business units.

#### Initial Funding

With the exception of the bandwidth mentioned earlier, the program does not require the purchase of new infrastructure because it takes advantage of existing network, data center, collaboration, and security architectures. Cisco did add approximately 10 percent more wireless access points. The only application added was third-party MDM software.

Carrier fees represent 90 percent of the program cost. Infrastructure and management costs for Secure Mobility services account for the remaining 10 percent. IT workload decreased despite the addition of tens of thousands of new devices to the network. In 2013, Cisco managed the production service with approximately 33 percent fewer staff than in 2009.

#### Ongoing Funding

The employee's department is charged a small monthly service fee to offset costs for developing, maintaining, and delivering Any Device services. The charge to business units enabled Cisco to scale the infrastructure as the number of devices increased from 20,000 to 66,000 in four years. Charges are adjusted annually to reflect actual infrastructure costs and projected costs to support more users.

Cisco has negotiated contracts with more than 100 mobile carriers worldwide. Employees who are eligible for smartphone service paid by Cisco are added to the corporate plan if one is available. The service provider bills Cisco directly. Managers receive reports showing exceptionally large service bills for individual employees. Because their departments pay a portion of the bill, managers are motivated to meet with the employee to suggest changes to behavior or the calling plan.

Most employees pay for their own service plan, family plan, termination fee, 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 informs employees about the calling plans available for people who expect to be entirely in one country, or to be roaming for lesser or greater amounts of time.

© 2015 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

## Cisco Lessons Learned

Devising and implementing an Any Device strategy is a significant change for any organization. Such a transformation will be accepted more smoothly and more successfully with a consistent governance structure. Along this enterprisewide Any Device journey, Cisco business leaders and IT and security professionals have learned many lessons. Among them are the following.

Business lessons:

- The Any Device journey requires a cross-domain effort from desktop, security, network infrastructure, and communications departments.
- Organizations should recruit a single executive sponsor who assumes responsibility for organizing the cross- functional team, educating executives, and reporting on results and metrics.
- The Any Device journey has a ripple effect across the organization. All stakeholders must understand the extensive policy development work required and the implications of this strategy.

**Metrics At-a-Glance, 2011-2013**

Cost savings:

- Eliminated $500,000 per year in device spending by mandating BYOD smartphones and tablets
- Reduced gross annual service provider spending by 30 percent by revalidating company-paid services
- Lowered per-user support caseload 40 percent over two years due to rolling out social support and the WebEx Social community

Service metrics:

- Supported 82 percent more devices and 203 percent more data usage
- Supported 28 percent more users at 25 percent lower per-user cost
- Achieved a 28 percent higher user-satisfaction rating

- Do not underestimate the amount of effort required to segment your user population and conduct user analysis. This analysis should determine which users are entitled to what services, and it should be the first action when starting your Any Device journey.
- Control costs through regular eligibility review for employer-paid service plans as well as ongoing feedback and employee education on tips to reduce roaming and data usage charges as well as mobile phone minutes.
- Provide ongoing user education to help keep devices secure with discussion forums, user guides, best practices, videos, and training.
- Develop policies and procedures for deleting sensitive information when employees leave the company and require that employees agree to those procedures.
- To encourage user self-support, provide continuously updated content that is easy to find and understand.

Technical lessons:

- Educate users about subscriber identity module (SIM) cards and the unexpected charges that can occur when swapping SIM cards between different manufacturers' phones, and put systems in place to prevent that practice.
- Make sure the wireless address space across offices is large enough to accommodate the increasingly mobile workforce; add wireless IP address resource space at popular locations.
- Test new mobile applications and self-service portals with employees from multiple business functions; include employees who are not in IT as well as those from different countries.
- For guest wireless, make sure to set up multichannel communication processes for end users and the support team.

© 2015 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

- Stage limited deployments to test compatibility and provide hands-on training to smooth the ramp-up to global usage and support.
- When possible, use global engineering and support resources to optimize costs and service levels.
- Stay on top of industry, technology, and standards trends to help ensure ongoing compatibility, support, and expansion.

## First Steps along Your Own Any Device Journey

As Cisco ventured out on its Any Device journey, we identified 13 critical business areas that are affected by this new paradigm. Table 1 spotlights these focus areas and provides a list of questions that have helped Cisco - and can help you as you begin your own journey - to recognize and veer around potential problems and determine how best to approach these issues as you go. Consider these questions and be meticulously honest in your responses as you move forward.

**Table 1.** Questions to Ask for the Any Device Journey

| Business Area | Business Questions to Answer |
|---|---|
| **Business continuity planning and disaster recovery** | • Should noncorporate devices be granted access or restricted from business continuity planning?<br>• Should there be an ability to remotely wipe any end device accessing the network if it is lost or stolen? |
| **Host management (patching)** | • Will noncorporate devices be permitted to join existing corporate host-management streams? |
| **Client configuration management and device security validation** | • How will device compliance to security protocols be validated and kept up-to-date? |
| **Remote-access strategies** | • Who should be entitled to what services and platforms on which devices?<br>• Should a contingent worker be given the same entitlement to end devices, applications, and data? |
| **Software licensing** | • Should policy change to permit installation of corporate-licensed software on noncorporate devices?<br>• Do existing software agreements account for users accessing the same software application through multiple devices? |
| **Encryption requirements** | • Should noncorporate devices comply with existing disk-encryption requirements? |
| **Authentication and authorization** | • Will noncorporate devices be expected or permitted to join existing Microsoft Active Directory models? |
| **Regulatory compliance management** | • What will organizational policy be on the use of noncorporate devices in high-compliance or high-risk scenarios? |
| **Incident management and investigations** | • How will corporate IT security and privacy manage incidents and investigations with non- corporate-owned devices?<br>• How will the incident management team get the appropriate data to conduct investigations? |
| **Application interoperability** | • How will the organization handle application interoperability testing with noncorporate devices? |
| **Asset management** | • Does the organization need to change how it identifies the devices it owns to also identify what it does not own? |
| **Support** | • What will the organization's policies be for providing support to non–corporate-owned devices? |
| **Legal** | • Are there local laws that mandate certain changes and policies?<br>• Are internal end-user license agreements (EULAs) updated accordingly? |

© 2015 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

## For More Information

Cisco is well down the path in implementing an Any Service, Any Device, Anywhere environment based on employee choice, and we will continue to share experiences to help information and security officers, enterprise IT, and information security architects circumvent problems that may arise. The knowledge and methodology Cisco has used to transform its business and IT environments toward Any Device and beyond can be applied to other organizations large and small.

Speak with your Cisco representative to learn how to position your business, IT, and security infrastructure strategically to prepare for a move to an Any Device architecture.

For information about Cisco security solutions that enable Any Device, refer to: http://www.cisco.com/go/security.

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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Printed in USA C11-681837-01 01/15

© 2015 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.