

Pre-Evaluating Small Devices for Use in the Enterprise

Intel IT's pre-evaluation process enables us to support the growing demand for use of small devices in our environment, while preserving the necessary security and manageability required for our enterprise.

Executive Overview

As part of Intel IT's overall program to support IT consumerization and the expansion of our compute continuum, we developed an evaluation process for certifying small devices for use in the enterprise. This small-device certification process starts with a pre-evaluation of operating systems (OSs) and devices to determine whether to proceed with the full evaluation process.

We use the pre-evaluation screening to focus on the top three to five handheld OSs, including those for smart phones and tablets. Within this scope, we further evaluate the most popular hardware models running on popular OSs.

The cornerstone of our screening process is the criteria we use, which were compiled by consulting with stakeholders across Intel. We grouped the criteria into five key categories of features and services that make small devices good candidates for support in the enterprise: security, manageability, productivity, performance, and ease-of-use. We score each OS version or new device against the criteria to determine the devices we want to further investigate.

This initial screening process enables us to do the following:

- Keep up with the increasing demand from Intel employees who want to use their personal handheld devices to access corporate data and applications
- Allocate IT resources more efficiently by eliminating inappropriate devices from the full evaluation process
- Focus on only the viable candidates, which allows us to finish an evaluation in as little as two weeks after a new device is available for purchase

With this process, employees can anticipate which personal devices they can and cannot use at Intel, and IT can support the growing demand for use of these devices in our environment, while preserving the necessary security and manageability our enterprise requires.

David Byrne

Handheld Technology Specialist, Intel IT

Rob Evered

Information Security Specialist, Intel IT

Contents

Executive Overview..... 1

Background..... 2

Solution..... 3

 Intel IT Criteria for
 Evaluating Small Devices..... 3

 Evaluation and Scoring..... 6

Conclusion..... 6

For More Information..... 6

Acronyms..... 7

BACKGROUND

The number and variety of connected devices in the marketplace is increasing every year, and these devices shape employees’ expectations about work and collaboration. Intel IT has embraced IT consumerization, recognizing that allowing employees to use their personal devices to access corporate data enhances employee satisfaction and productivity and improves enterprise security by eliminating use of unsecured, unmanaged devices. Addressing this trend and providing a seamless, consistent experience across devices so that employees can access information anywhere, at any time is a vision Intel calls the “compute continuum.”

In early 2010, Intel IT implemented a personal device program that allows employees to use their own smart phones and tablets to access corporate data. By aligning with our information security policy, Intel IT enables the use of a wide range of devices while protecting Intel’s data and intellectual property. Since 2010, we’ve been actively integrating corporate and personal small

devices into our environment, with nearly 29,000 smart phones and tablets enabled to date, about 58 percent of them employee-owned (see Figure 1).

Intel’s original program supported corporate-supplied small devices, including three mobile OSs using 70 service providers worldwide. As we considered including employee-owned small devices in the enterprise, we had to address the significant potential for overwhelming the IT Service Desk with requests for device support. For example, since 2010 employees have asked IT to support over 450 different types of devices on seven or eight of the most popular mobile operating systems (OSs). On average, each OS has three versions in use at any given time.

When a new device is released in the marketplace, employees naturally want to buy it and expect Intel IT to support it. However, given the high number of models and OSs, we do not have the resources to perform the full evaluation process, which would amount to as many as 500 certifications per year using our traditional method. Clearly, we needed a faster, more efficient way to evaluate devices to address employee’s requests while preserving necessary security and manageability for our enterprise.

IT@INTEL

The IT@Intel program connects IT professionals around the world with their peers inside our organization – sharing lessons learned, methods and strategies. Our goal is simple: Share Intel IT best practices that create business value and make IT a competitive advantage. Visit us today at www.intel.com/IT or contact your local Intel representative if you’d like to learn more.

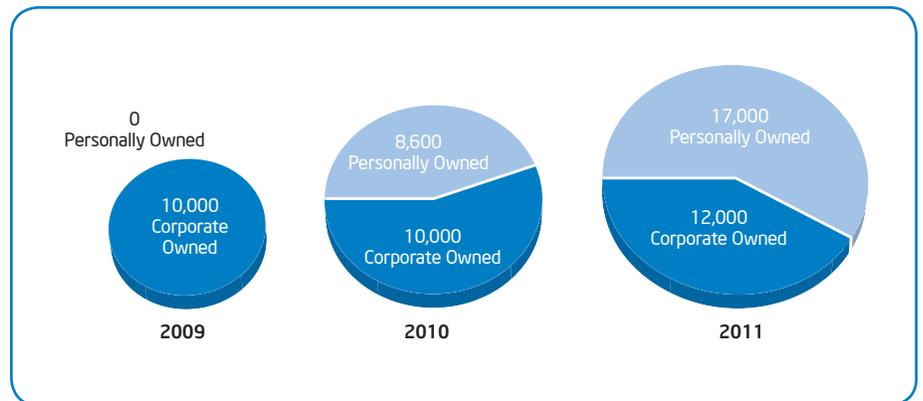


Figure 1. Use of handheld devices at Intel has grown, with 58 percent of devices personally owned in 2011, through the implementation of Intel IT’s personal device program.

SOLUTION

To support the growing demand for use of small devices in our environment, our solution is a pre-evaluation screening focused on the top three to five OS types based on market trends and business needs. Within this scope, we further evaluate only the most popular hardware models, focusing on how they will interact in our enterprise. This helps us keep the number of hardware versions we evaluate to a manageable level.

When a new device or OS version becomes available, we perform a pre-evaluation screening to review all technical, stakeholder, and business criteria to decide if performing the full certification process is warranted. We score the device according to entry-level enterprise considerations that we've developed and compare these scores to those of other devices available in the market. (We evaluate reference devices from original equipment manufacturers (OEMs) because service provider versions may deviate from the original OEM device.)

Our pre-evaluation process, shown in Figure 2, is based on detailed criteria and uses the manufacturer's published specifications and

market expectations of launch features. Intel IT ranks certain criteria higher than others and adds weighting to reflect the priorities and minimum requirements within each category or among individual features to help make the combination of criteria fit our needs.

If the device passes the pre-evaluation screening, we will then perform the full evaluation process on it. Once we decide whether or not to support the new device or OS version, we write a position statement, which is available to employees through our Web portal. Our goal is to publish a position statement within two weeks of when a new device is available for purchase.

Intel IT Criteria for Evaluating Small Devices

The effectiveness of the pre-evaluation screening depends on the criteria we use. Criteria are based on features and services that make a small device a good candidate for acceptance in the enterprise. These criteria were developed with stakeholder input, ensuring that devices selected for support meet employee needs throughout the company. Intel IT grouped the criteria into five key categories: security, manageability, productivity, performance, and ease-of-use.

Some criteria may be weighted such that if a minimum requirement is not met, the OS or device may be ruled out from further investigation. The five categories of criteria are detailed in the following sections:

SECURITY CRITERIA

The security criteria were defined by the IT Security team to ensure that information is secure in transit and in use, and that the device is reasonably protected from malware and aligned with our existing and new handheld policies. The security criteria along with the manageability criteria are especially important in the consideration of the device's acceptability in Intel's environment. This category encompasses features such as a power-on password, content encryption, and protection of information on the device.

Power-on password

A password is requested when the unit is powered on and before accessing data-based services. This feature helps prevent unauthorized access without making access difficult or impacting the device's user experience, such as enabling caller ID or global positioning system (GPS) navigation when locked.

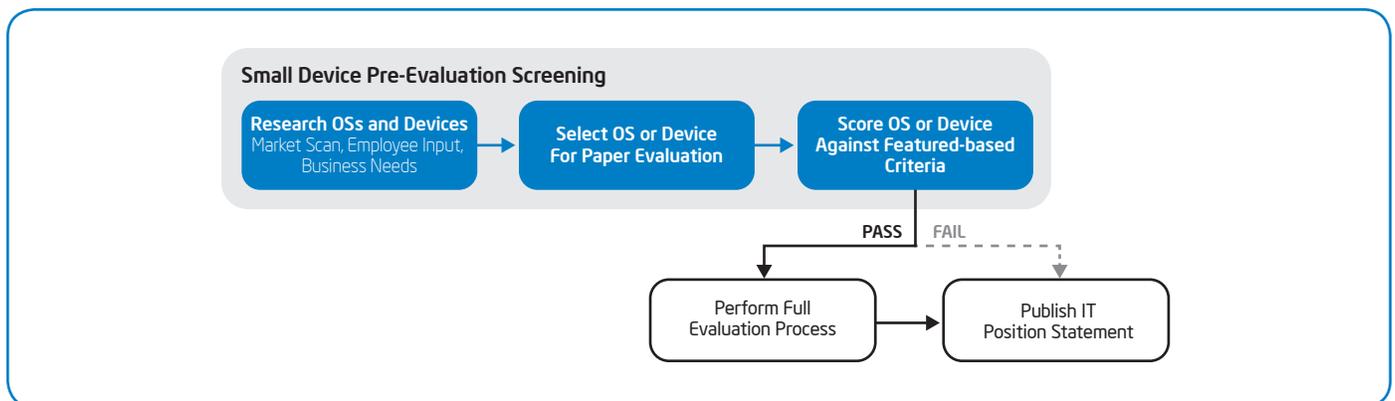


Figure 2. As part of Intel IT's small device certification process, the pre-evaluation screening helps us decide if performing the full certification process is warranted. Our goal is to publish position statements within two weeks of a new device being available for purchase.

Content encryption

The device must have the ability to encrypt information that the user or the enterprise wants to protect. The encryption state is easily understood and complies with an industry standard. The encryption state can be reported through standard Mobile Device Management (MDM) application programming interface (API) to a central mobile device management system.

Content separation

The user knows whether data is personal or corporate and can make decisions and store and protect accordingly. This feature applies to applications such as contacts, calendars, notes, and personal information.

VPN to enterprise

The device can securely access the Intel virtual private network (VPN) infrastructure either natively or with software applications to connect the user to the enterprise.

Credential store

The device stores certificates securely using industry standards and prevents the removal of credentials through any mechanism. The stronger this protection is, the more the enterprise can trust this device.

Device intrusion protection

Small device OSs typically implement a “deny by default” approach and have additional control features that make client-based anti-malware and anti-virus controls less effective. We consider the device level controls and how well the device can leverage infrastructure-based malware protections. The greater the level of device and infrastructure controls in place, the higher we score this criterion.

MANAGEABILITY CRITERIA

The manageability criteria evaluate the ability for the device to be managed both for the enterprise and consumer. Included in this category are features such as monitoring the health and status of the device, enterprise management, proactive monitoring support, and ability to get up and running quickly after device failure or when moving to a new device. Manageability criteria, coupled with the security criteria, are critical when considering whether IT will support the device and are weighted accordingly.

Enterprise management

The device supports enterprise device management solutions and the standard MDM features available in each OS.

Discovery

The device properties can be identified at the provisioning stage and, based on that device’s information, different levels of services are automatically provided.

Over-the-air (OTA) provisioning

The device can be provisioned and applications can be installed or activated OTA.

Configuration enforcement

The device has the ability to identify the preferred enterprise configuration profile centrally, to determine how this configuration is implemented at the OS level, and to implement the deployment. Configuration enforcement on devices connecting to IT services helps protect enterprise and personal information and meet market best practices. A balanced approach to the configuration profile is maintained by giving equal weighting to employee and enterprise needs.

Software delivery

New applications, updates, and line-of-business applications can be delivered and made available for download to employees. Applications developed in-house can be offered without the need to post to external application stores, speeding up delivery times and adoption.

Proactive monitoring support

The device supports health and status reporting and allows IT to provide auto-configuration options and profiles, which eliminate manual input errors for configuring services and reduce service desk calls. Information can also be used to measure configuration health. The more information the device reports, the more accurately the profiles can be made to improve services such as battery performance.

Backup and restore

The device configuration can be identified, and the data or configuration can be backed up for restoration in case of loss or when transferring to a new device either by the employee or through enterprise OTA configuration automation.

PRODUCTIVITY CRITERIA

Productivity criteria cover those features that affect the user’s ability to complete tasks efficiently, such as easily accessing corporate and personal information and the ability to access information when needed without searching for a data connection. Productivity criteria include features such as support for offline consumption and how productive a user can be during small amounts of time or longer interaction sessions.

Intelligent updates

Corporate and personal data are presented to the user in easily digestible formats. When a new OS update is available, the owner is advised, and the update can be easily completed.

Blended social interface

Consolidated interfaces are available for accessing multiple accounts or multiple social networking services. Features include a universal inbox, social interaction views, and the capability to manage those services. A balanced interface would be one that blends clear source information and allows granular control of responses through the user interface (UI).

Broadcast updates

Business and personal information can be broadcasted to the device (for example, using Really Simple Syndication (RSS) and streamed application feeds such as weather and stock information). Notification of pending or available information is visible and context aware so it doesn't intrude on a usage situation.

Tools and applications

The application ecosystem for this device's OS is mature, providing business and personal productivity gains.

Time use

Through effective use of small slices of time (5 to 15 seconds) tasks can be completed quickly with this device. For example, a user should be able to access and view information, and make personal and business decisions without having to access a laptop or desktop system.

Offline consumption

The device can access data and services that allow for review even when offline. This feature is especially important when evaluating larger screen devices with broader consumption and information views.

PERFORMANCE CRITERIA

The performance criteria describe the features that contribute to the speed and overall functionality of the device, such as battery life, processor speed, and screen size. These criteria directly affect the overall productivity users can achieve with their devices.

Battery life

The battery enables a minimum of one full day of active use before requiring charging, with the preferred battery life being two or more full days. The best in class provides greater than two days, and here is where we often see trade-offs between screen size, battery capacity, and usage.

Responsiveness

The device powers on immediately or is always on and has little or no lag between uses. While some lag may be unavoidable, a well-designed OS or interface will have features like pre-fetching information and activity indicators that hide performance limitations to minimize user frustration.

Application multitasking

Users can move between tasks with ease and without loss of data, application state, or progress.

Camera and HD video

Those devices with cameras provide sufficient image quality for their purpose and provide a simple interface to access content sharing, storage, user preferences, and privacy controls.

Screen sizes

The ranges of screen sizes available are appropriate for the device and are sufficient to provide a good user experience without significantly impacting battery life.

Radio frequencies

The device is capable of operating on multiple frequencies or bands, such as four-band Global System for Management communications (GSM), Wi-Fi*, WiMAX*, 2G/3G/4G, GPS, and Intel® Wireless Display (WiDi).

Storage capacity and RAM

The device has sufficient on-device storage and RAM, based on comparisons of the market at the time and current trends.

EASE-OF-USE CRITERIA

We consulted with typical users to determine what features are most important to them. Ease-of-use criteria are often subjective and describe the overall usability of the device. These criteria include features such as how intuitive the UI is, and how easily the user can switch between tasks.

Intuitive user interface

The device's UI should be intuitive and easy to use. If a user needs to read a manual in order to be productive, the device receives a lower score.

Easy updates

Updates to the OS, firmware, and applications are easy to receive and are non-destructive.

Fluidity of use

The device must allow users to easily switch between tasks, move data between applications, interact with social sites, and navigate the device's capabilities without adding complexity.

Input options

The device supports multiple input options, such as a touch-screen combined with an optional wirelessly-connected keyboard. This criteria looks at the optional accessories available for the device, with greater variety receiving a higher score.

Table 1. Example Scoring for a Mobile OS against the Security Criteria

Security Criteria 0-2 (higher is better)	Mobile OS
Power on password	2
Content encryption	2
Content separation	1
VPN to enterprise	1
Certificate store	2
Device intrusion protection	1
Average	1.5

Table 2. Example Evaluation Results and Cumulative Summary for a Mobile OS

Initial Evaluation 0-2 (higher is better)	Mobile OS
Security	1.5
Manageability	1.8
Productivity	1.8
Performance	2.0
Ease of Use	1.8
Summary	1.8

Evaluation and Scoring

The scoring process involves assigning a score of 0, 1, or 2 to each of the criteria as follows:

- 0 - The feature is not present or the requirements are otherwise not met. Scoring a zero on a critical feature or service may exclude a device from further consideration.
- 1 - The feature or service is present and meets minimum standards.
- 2 - The feature or service is not only present, but it meets or exceeds best-in-class standards.

The scoring process provides an objective evaluation and a comparison of strengths between the categories of criteria.

Table 1 shows how a mobile OS scored on the security criteria. Every feature was present, and for 50 percent of the criteria, the feature met or exceeded best-in-class standards. After scoring the criteria, an average score is calculated to arrive at an overall score for the security category.

Table 2 shows a summary matrix of all the average scores for the categories. The OS has a good security evaluation and even better results in the other categories. With a summary score of 1.8, this near-enterprise-class OS warrants further evaluation.

CONCLUSION

Having a formal and rapid process in place for evaluating mobile OS updates and new handheld devices helps Intel IT keep up with employee demand, even as the number of OS updates and connected devices continues to grow.

Our pre-evaluation screening—based on criteria carefully defined and vetted by stakeholders—helps us to keep up with the sheer number of new small devices reaching the market every quarter and to respond to requests from users fast and efficiently.

Our goal is to finish the full small device certification process and communicate the results to employees within two weeks of the device being available, when possible. Our process enables employees to achieve the productivity benefits of knowing which devices have been qualified as they become available. Intel benefits from increased employee productivity and improved enterprise security by eliminating use of unsecured, unmanaged devices.

FOR MORE INFORMATION

- “Personal Handheld Devices in the Enterprise”
- “Maintaining Information Security While Allowing Personal Hand-Held Devices in the Enterprise”
- “Cloud Computing: How Client Devices Affect the User Experience”
- “Enabling Device-Independent Mobility with Dynamic Virtual Clients”

For more information on Intel IT best practices, visit www.intel.com/it.

ACRONYMS

GPS	global positioning system
MDM	mobile device management
OEM	original equipment manufacturer
OS	operating system
OTA	over the air
UI	user interface
VPN	virtual private network

This paper is for informational purposes only. THIS DOCUMENT IS PROVIDED "AS IS" WITH NO WARRANTIES WHATSOEVER, INCLUDING ANY WARRANTY OF MERCHANTABILITY, NONINFRINGEMENT, FITNESS FOR ANY PARTICULAR PURPOSE, OR ANY WARRANTY OTHERWISE ARISING OUT OF ANY PROPOSAL, SPECIFICATION OR SAMPLE. Intel disclaims all liability, including liability for infringement of any patent, copyright, or other intellectual property rights, relating to use of information in this specification. No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted herein.

Intel and the Intel logo are trademarks of Intel Corporation in the U.S. and other countries. * Other names and brands may be claimed as the property of others.

Copyright © 2012 Intel Corporation. All rights reserved. Printed in USA

 Please Recycle

0212/JGLU/KC/PDF

326406 -001US

