Technology Brief

Securing Mobile Devices

HP Touchpoint Manager

The recent proliferation of mobile business devices means enhanced productivity for your employees. They can be productive in the office and work almost anywhere else—in an airport waiting for a connecting flight, at a dinner meeting with a client, while attending a conference, or from home. But with this increased flexibility comes increased vulnerability. Every employee with a mobile device—phone, tablet, or notebook—becomes a liability that could result in your organization's sensitive information being compromised, stolen, or destroyed.

In a few simple steps, HP Touchpoint Manager can provide protection and peace of mind for you and your employees.[1] It's a must-have solution for any company that supports a "bring your own device" (BYOD) program. Using HP Touchpoint Manager, an IT administrator can apply security settings quickly and consistently with configurable out-of-the-box security, Wi-Fi provisioning, and policy settings to groups of users or devices.

Security Profile settings include:

- Detect, monitor, and deploy antivirus software (Windows®)
  If virus protection software is not detected, then HP Touchpoint Manager will automatically deploy and/or activate Microsoft® Windows Defender (Windows 8.0 and above) or Microsoft® Security Essentials (Windows 7 systems).
- Detect, monitor, and manage Windows Firewall (Windows)
  If active firewall software is not detected, then the built-in Windows Firewall software will be enabled.
- Erase a device after a defined number of failed log-in attempts (Android™/iPhone® and iPad®)
- Trigger a device to auto-lock after a specified time of inactivity (Android/iPhone and iPad)
- Enforce device password/PIN length settings (Android/iPhone and iPad)
- Enable/disable the device camera (Android/iPhone and iPad)

HP Touchpoint Manager includes pre-defined security templates that incorporate security best practices appropriate for each customer's needs and also allows you to create your own security profiles.

Built-In HP Touchpoint Manager Security Profiles

Subscription level	Security settings	Built-In security profiles *Standard*	*Enhanced*	*Maximum*
Basic	Antivirus Monitoring	Off	On	On
Basic	Firewall Monitoring	Off	Off	On
Pro	Lock devices after X minutes inactivity	30	15	5
Pro	Passcodes must contain letters	Off	Off	On
Pro	Passcodes must contain numbers	Off	Off	On
Pro	Erase all data on devices after password is entered incorrectly X times	Off	Off	10
Pro	Passcode minimum length	0	4	8
Pro	Disable Camera	Off	Off	Off
Pro	Enable Device Encryption	Off	Off	Off
Pro	Password must contain special characters	Off	Off	On
Pro	Password expires after X days	Off	120	90
Pro	Password history enforcement. X unique passwords required	Off	3	5

Because different policies can be assigned to different groups of devices, it is simple to keep track of which settings are applied across the organization.

For example, devices from employees from a single department, such as finance or benefits, can be assigned a specific security policy, or the devices can be organized by type (e.g. all tablets). Once you create a Group, you'll be able to apply a Security Profile to the Group with a single click of the mouse. You can make changes just as quickly. If you identify risks, you can apply a more restrictive Security Profile as necessary.

Additional security benefits include the Find Device feature, which protects your organization against theft or loss by allowing you to locate the device on a map when it is connected to the internet.[2] This allows you to confirm that the device in question is located where it is supposed to be, and if you believe the device has been stolen or lost, you can take action to locate it or protect its data.

Lost Device Protection features include:

- **Sound Alarm:** triggers a loud sound, which can be useful if the device has been misplaced nearby [2]
- **Lock Device:** triggers a screen lock (Android/iPhone and iPad) or OS logout (Windows) [2]
- **Erase Device Data:** triggers a factory reset (Android/iPhone and iPad) or a secure erase of data files from the device (Windows) [2]

In the event that your organization or government's privacy policies require it, the Find Device feature can also be disabled.

As an IT administrator, HP Touchpoint Manager allows you to easily monitor the mobile devices you manage, view security settings and status, take action to change security policies, and take action on missing devices. Its security features enable your organization to retain the advantages of mobility, while ensuring your data is safe and accessible and your employees are productive.

[1] HP Touchpoint Manager supports Android™, iOS, and Windows operating systems and PCs, notebooks, tablets, and smartphones from various manufacturers. Not available in all countries see hp.com/touchpoint for availability information. Touchpoint Manager requires purchase of a subscription.

[2] Subject to various environmental features including that the lost product be powered on and have internet access. The service is not a guarantee.

Sign up for updates
hp.com/go/getupdated

Share with colleagues

Rate this document

4AA6-0367ENW, August 2015