HP Touchpoint Manager

Third Edition: January 2016

First Edition: October 2015

Document Part Number: 845310-003

Table of contents

1 HP Touchpoint Manager Overview

HP Touchpoint Manager is a powerful cloud-based solution that helps organizations short on IT resources easily manage data, devices, and users. With HP Touchpoint Manager, your IT staff can troubleshoot issues quickly in real-time and apply point-and-click security policies across different devices, brands, and operating systems. From a single, simple-to-understand dashboard with real-time insights and alerts, your IT staff can track computer and mobile device health quickly and easily and get a head start on troubleshooting.

HP Touchpoint Manager offers Basic subscription and Pro subscription (with premium capabilities) plans to address the needs of different organizations.

HP Touchpoint Manager offers a wide range of features and functions, including the following:

- Platform-agnostic solution to support various device types, manufacturer brands (HP and non-HP brands), and operating systems
- Security policy enforcement against virus and malware threats for Windows devices
- Centralized management of devices, including computers, tablets, and mobile devices across multiple operating systems (Windows®, Android™, and iOS)
- Proactive monitoring of hardware health, such as hard drive and battery health
- Proactive warranty tracking for HP devices with Windows and Android operating systems
- Location assistance for lost devices
- Data security by locking or erasing data of lost devices
- Application management and deployment

HP Touchpoint Manager architecture

HP Touchpoint Manager consists of three components:

- **HP Touchpoint Manager Web Portal**—The HP Touchpoint web portal, http://www.hptouchpointmanager.com, allows you to manage HP Touchpoint Manager settings and download the HP Touchpoint Manager Client software.
- **HP Touchpoint Manager Client**—The HP Touchpoint Manager Client software automatically installs all of the necessary components and settings that HP Touchpoint Manager uses to manage the device.
- **HP Touchpoint Manager Cloud Service**—The Internet-based server infrastructure interacts with enrolled devices that have HP Touchpoint Manager Client installed. The HP Touchpoint Manager Cloud Service uses the Internet to send tasks to and receive status updates from HP Touchpoint Manager Clients. If a managed device is offline at the time a command is sent, the HP Touchpoint Manager Cloud Service places the pending tasks into a queue to be sent to the client when it reconnects to the Internet.

HP Touchpoint Manager features

	Basic	Pro	Computers (Windows)	Tablets (Windows, Android, and iOS)	Smartphone (Android and iOS)
Application Deployment (see Application Deployment (Windows))		✓	✓	✓ (Windows only)	
Always on Remote Management (see Always On Remote Management (HP devices only))	✓	✓	✓	✓ (Windows only)	
Azure Active Directory (see Importing users from Azure Active Directory (Azure AD))	✓	✓	✓	✓	
Battery Health & Hardware Health (see Hardware Health (Windows devices only))	✓	✓	✓	✓	
Device Erase (see Erasing data from a device (Windows, Android, and iOS))	✓	✓	✓	✓	✓
Find Device (see Find Device (Windows, Android, and iOS))	✓	✓	✓	✓	✓
Firewall Policy (see Firewall (Windows devices only))	✓	✓	✓	✓ (Windows only)	
Help & Support (see Help & Support)	✓	✓	✓	✓	✓
Local Password Reset (see Resetting my HP Touchpoint Manager password)		✓	✓		
Lock (see Locking a device)	✓	✓	✓	✓	✓
Mobile Application Deployment (see Mobile Application Deployment (Windows, Android, and iOS))		✓		✓	✓
Mobile Device Security Policy (see Mobile Device Security (Android and iOS)).	✓	✓		✓	✓
Proactive Alerts (see Alerts)	✓	✓	✓	✓	✓
Software Inventory (see Viewing device details)	✓	✓	✓	✓ Windows and Android only	
Sound Alarm (see Sounding the alarm on a device)	✓	✓	✓	✓ (Windows and Android only)	✓ (Android only)
User and Device Inventory (see Viewing device details)	✓	✓	✓	✓	✓

	Basic	Pro	Computers (Windows)	Tablets (Windows, Android, and iOS)	Smartphone (Android and iOS)
Virus Protection Policy (see Virus Protection (Windows only))	✓	✓	✓	✓ (Windows only)	
Wi-Fi Provisioning (see Wi-Fi Provisioning (Android and iOS only))		✓			✓

HP Touchpoint Manager is a cloud-based solution. Your subscription includes new feature additions and regular service updates. For the latest feature lists, visit http://hp.com/go/touchpoint.

HP Touchpoint Manager roles

Portal Access/Role	Basic	Pro	Description
IT administrator	✓	✓	An IT administrator can perform all tasks in HP Touchpoint Manager, including upgrading/downgrading the service, adding or deleting user accounts, or changing the primary billing contact.
Managed user	✓	✓	Managed users can view and perform certain tasks on their own devices. Examples include the following: ● Viewing hardware health information. ● Performing Find, Lock and Sound Alarm tasks. Users cannot view or manage other users’ devices.
Primary Billing Contact	✓	✓	Each HP Touchpoint Manager customer account has a primary billing contact. This role is held by one of the IT administrator user accounts and can be reassigned to another IT administrator. An IT administrator account with this designation cannot be deleted unless the primary billing account is reassigned. The default assignee is the creator of the HP Touchpoint Manager customer account.

NOTE: For details, see IT administrator and managed user roles.

2 Getting started

Downloading and installing HP Touchpoint Manager

To get started with HP Touchpoint Manager:

1. Go to http://www.hptouchpointmanager.com.
2. Select one of the following:
   - **Start Free Trial**—Enter the required information, select the check box to acknowledge the terms and conditions, and then select **Start Free Trial Now**.
   - **Learn More**—View more information about HP Touchpoint Manager.

   NOTE: To sign out from HP Touchpoint Manager, select 👤 at the top right of the HP Touchpoint Manager dashboard.
3. Download and install HP Touchpoint Manager on the device selected to be the centralized management dashboard. To install and enroll managed devices, see Installing and enrolling HP Touchpoint Manager on managed devices.

   IMPORTANT: Invite additional users within your organization to use HP Touchpoint Manager, so that you can view and manage their devices.

   You can access HP Touchpoint Manager by logging in to http://www.hptouchpointmanager.com from any supported web browser.

Installing and enrolling HP Touchpoint Manager on managed devices

A small client application must be installed on all devices that you want to manage with HP Touchpoint Manager. You can install the HP Touchpoint Manager Client application on devices with Windows, Android, or iOS operating systems.

Windows managed devices

Installing HP Touchpoint Manager on Windows managed devices

Follow these instructions to download and install the HP Touchpoint Manager Client.

1. From the HP Touchpoint Manager dashboard, under **Quick Links**, select **Enroll my Device**.
2. To install the software, when prompted, select **Run**.

   The client installer window is displayed.
3. In the HP Touchpoint Manager Setup window, select **Next**.
4. In the License Agreement window, read the terms of the License Agreement, and then select the **I accept the Terms and Conditions of the End User License Agreement** check box.

5. Select **Install**.

   The HP Touchpoint Manager Client installs.

6. When the installation is complete, select **Close**.

7. Select the type of credentials to use for enrollment:

   - The email address and password used to sign in to HP Touchpoint Manager
   - A PIN code provided by the IT administrator
   - Azure Active Directory credentials

8. Sign in with your credentials, and then select **Enroll**.

9. To have HP Touchpoint Manager manage your device, select **Agree**.

Enrolling Windows managed devices

If the HP Touchpoint Manager Client is installed, but the computer is not enrolled, follow these steps:

1. Select the HP Touchpoint Manager icon in the lower-right corner of the taskbar.

2. Select the type of credentials to use for enrollment:

   - The email address and password used to sign in to HP Touchpoint Manager
   - A PIN code provided by the IT administrator
   - Azure Active Directory credentials

3. Sign in with your credentials, and then select **Enroll**.

To display HP Touchpoint Manager device status, select the HP Touchpoint Manager icon in the lower-right corner of the taskbar, and then select **Status**.

Configuring proxy server settings for the HP Touchpoint Manager client

If a proxy server is specified in Internet Explorer, the HP Touchpoint Manager client automatically attempts to use the specified proxy server. If the HP Touchpoint Manager client cannot connect to the proxy, then it will attempt to auto-detect the proxy or to connect without a proxy.

HP Touchpoint Manager does not support authenticated proxies.

Android managed devices

Installing HP Touchpoint Manager on Android managed devices

Downloading and installing the HP Touchpoint Manager Android Client

1. Go to the Google Play™ store.

2. Download the HP Touchpoint Manager app, and then install it on your device.

Enrolling Android managed devices

To enroll an Android mobile device:

NOTE: You must have an active HP Touchpoint Manager account before you can enroll a device.

1. Launch the HP Touchpoint Manager application.

2. If this is your personal device, select **Personal**, or if it is a company-owned device, select **Company**.

3. Select the type of credentials to use for enrollment:
   - The email address and password used to sign in to HP Touchpoint Manager
   - A PIN code provided by the IT administrator
   - Azure Active Directory credentials
4. Sign in with your credentials, and then select **Enroll**.
5. The HP Touchpoint Manager Client application starts and displays the End User License Agreement (EULA). Read the License Agreement, and then tap **Accept** to continue.
6. During the enrollment process, you are prompted to **Activate Device Administrator** privileges. Accepting this prompt allows the HP Touchpoint Manager Client application to manage your device.

   If you do not accept these additional permissions, HP Touchpoint Manager cannot manage your device, and the enrollment process is canceled.

iOS managed devices

Installing HP Touchpoint Manager on iOS managed devices

Obtaining an Apple Push Notification (APN) Certificate

Apple requires your company to obtain an Apple Push Notification (APN) certificate to manage iOS devices with HP Touchpoint Manager. When an IT administrator first creates an account, HP Touchpoint Manager generates the following alert: "Your company needs to set up an Apple Push Notification (APN) certificate before iOS devices can be managed. Click here to set up your company's certificate."

NOTE: You must obtain the APN before installing the HP Touchpoint Manager Client.

To obtain the certificate and set up your device, follow these steps:

Step 1—Initiate a certificate signing request:

1. Select the link within the alert.
2. To initiate the request, select **Request CSR**. When a new tab opens, follow the on-screen instructions to download the file.
3. Download the CSR file, and then return to the HP Touchpoint Manager tab.

Step 2—Set up your Apple Push Notification settings:

1. Select **Apple Push Notification Portal**.

   NOTE: You must use a browser other than Internet Explorer (such as Google Chrome™ or Firefox) for this step.
2. Sign in with your Apple ID and password.

   NOTE: You can use any Apple ID. However, creating an Apple ID for your company is recommended.
3. Follow the on-screen instructions to create the Apple Push Notification (APN) certificate.
4. Download your certificate.

Step 3—Upload the APN certificate:

1. Select **Browse**.
2. Select the APN certificate previously downloaded.

Step 4—Finish:

1. Select **Finish**.
2. The HP Touchpoint Manager screen displays the following message: “Success! You are now ready to manage iOS devices”.

Downloading and installing the HP Touchpoint Manager Apple iOS Client

1. Go to the iTunes App Store.

   – or –

   Open a browser on your Apple iOS device.
2. On the HP Touchpoint Manager dashboard, tap **Enroll my Device**.

   HP Touchpoint Manager directs you to the application in the iTunes App Store.

NOTE: Any prior management software must be removed from an iOS device before the HP Touchpoint Manager Client installation is complete. This is due to an iOS limitation, which allows only one mobile device management vendor to manage a device at a time.

Enrolling iOS managed devices

1. Launch the HP Touchpoint Manager application.
2. The HP Touchpoint Manager Client application starts and displays the End User License Agreement (EULA). Read through the License Agreement, and then tap **Accept** to continue.
3. Select the type of credentials to use for enrollment:
   - The email address and password used to sign in to HP Touchpoint Manager
   - A PIN code provided by the IT administrator
   - Azure Active Directory credentials
4. Sign in with your credentials, and then select **Enroll**.
5. The HP Touchpoint Manager Client informs you that location services must be enabled in order to find a lost or stolen device. You are then prompted to enable location services.
6. When you are asked to install a profile on your device to allow the device to be managed by HP Touchpoint Manager, accept the profile installation.

   Your device is now being managed by HP Touchpoint Manager and your IT administrator.

Rapid provisioning (Windows, Android, and iOS)

PIN-based device enrollment for Windows, Android, and iOS devices makes it easier to deploy HP Touchpoint Manager to your users without requiring an email address for each user.

Enrolling multiple users and devices

Once you have an IT administrator account login for HP Touchpoint Manager, complete these steps to add multiple users and devices that you can manage.

1. Sign in to your account at http://www.hptouchpointmanager.com.
2. Add multiple users by importing a list of users and their associated PINs. For more information, see Importing a list of users.

3. Obtain an Apple Push Notification (APN) certificate (iOS devices only).

4. Require each managed user to download and install HP Touchpoint Manager on the iOS or Android device.

5. Require each managed user to enroll the iOS or Android device to your HP Touchpoint Manager account.

Downloading a user’s PIN

An IT administrator can download a user’s PIN (see Downloading a user’s PIN).

1. On the HP Touchpoint Manager dashboard, select **Users**.

2. Select the check box to the left of each user whose PIN is to be downloaded, and then select **Download PINs**.

3. When the confirmation dialog is displayed, select **Download**.

4. Use the downloaded PIN to enroll the user’s Android or iOS device.

3 Dashboard

The HP Touchpoint Manager dashboard provides IT administrators a high-level view of the users and recent activity for the company. The IT administrator can take action from the Quick Links section of the dashboard or go to the Users, Devices, or Services pages to administer users, devices, and set policies.

Element	Description
HP Touchpoint Manager menu bar	Access the following HP Touchpoint Manager features ● **Home**—Returns to the Dashboard. ● Alerts ● Groups ● Users ● Devices ● Services
?	Help & Support—Access more information about HP Touchpoint Manager.
⚙	Settings—Manage account information.
👤	Signing out—Sign out of the HP Touchpoint Manager application.
Edit user profile	Editing a user profile: ● **Change picture** ● **Name** ● **Address** ● **Change Password** ● **Communication Preferences** ● **My Devices**
My account summary	View a summary of the **Services**, **Users**, and **Devices** for the company account.
Quick Links	Quick Links—Quickly access common tasks within HP Touchpoint Manager.
Alerts	Alerts—Access notifications of events that may require IT administrator attention.
My Devices	Devices—Users can view information on their enrolled devices.
Devices	Devices—An IT administrator can view information on all enrolled devices for the company.

Quick Links

To quickly access common tasks within HP Touchpoint Manager:

1. Select one of the following Quick Links:
   - **Add User** (see Adding users)
   - **Enroll My Device** (see Downloading and installing HP Touchpoint Manager)
   - **Lock a Device** (see Locking a device)
   - **Erase a Device's Data** (see Erasing data from a device (Windows, Android, and iOS)
   - **Locate a Device** (see Find Device (Windows, Android, and iOS))
   - **Sound a Device's Alarm** (see Sounding the alarm on a device)
   - **Add Subscription Key** (see Adding subscription keys)
   - **Remote Control** (Pro only) (see Remote Control)
2. In the search box, enter a device, user name, or email address, select **Search**, and then follow the on-screen instructions.

4 How to perform common tasks

HP Touchpoint Manager provides a simple cloud-based management dashboard. An IT administrator can view and manage users and devices (see Users and Devices). For more information about tasks that can be performed by IT administrators and managed users, see IT administrator and managed user roles.

NOTE: Some features require a Pro subscription (see Choosing a subscription).

To perform a task quickly, select one of the **Quick Links** on the dashboard (see Quick Links).

Alerts

Alerts are generated to notify an IT administrator about device activity that needs attention. Alerts display the device status, the device name, and the device owner.

You can view alerts when issues occur that may require further action. Alerts can be triggered by a number of conditions, including the following:

- Hardware Health (Windows devices only)
- Firewall (Windows devices only)
- Virus Protection (Windows only)

1. To view alerts, on the HP Touchpoint Manager dashboard, select **Alerts**.

   All alerts are displayed on the **Alerts** page.

2. To hide alerts, select the **X** to the right of the alert.

   NOTE: Alerts are not deleted.

3. To view the alert logs, select **Logs** in the upper-right corner of the **Alerts** page.

Groups

An IT administrator can apply settings to all devices and/or users in a group. You can view group details, and groups can be edited, cloned, or deleted. Default groups include the following:

- **Default-Devices**—Includes all enrolled devices.
- **Default-Users**—Includes all enrolled users.

An IT administrator can also create additional groups of devices or users, depending on the subscription level:

Subscription level	Feature				
	Application Deployment	Security	Find Device	Remote Control	Wi-Fi Provisioning
Basic subscription	✓	✓	✓		
Pro subscription	✓	✓	✓	✓	✓

Creating a new group

1. On the HP Touchpoint Manager dashboard, select **Groups**, select **Create New**, and then select **User Group** or **Device Group**.
2. Under **Description**, enter a name and description for the group, and then select **Next**.
3. Under **Settings**, select a service, select the settings that you want, and then select **Next**.
4. Under **Devices** or **Users**, select **Add** beside each device or user to be included in the group, and then select **Finish**.

Editing a group

1. On the HP Touchpoint Manager dashboard, select **Groups**, and then select a group.
2. From the group drop-down menu, select **Edit**.
3. When the group opens, make the necessary edits, and then select **Finish**.

Cloning a group

An IT administrator can clone a group to make an exact copy of the existing group without the members.

1. On the HP Touchpoint Manager dashboard, select **Groups**, and then select a group.
2. From the group drop-down menu, select **Clone**.
3. When the group opens, make the necessary edits to the cloned group, and then select **Next**.
4. Search and make new selections for the group, and then select **Finish**.

Deleting a group

1. On the HP Touchpoint Manager dashboard, select **Groups**, and then select a group.
2. From the group drop-down menu, select **Delete**.
3. Select **OK** to confirm the deletion.

NOTE: Users in the deleted group are not deleted from HP Touchpoint Manager. Members of the deleted group are moved to the Default Devices or the Default Users group. Default groups cannot be deleted.

Viewing group details

1. On the HP Touchpoint Manager dashboard, select **Groups**.
2. Select a group from the list that is displayed.

   The following information is displayed about the selected group:

   - **Settings**—Displays the group name, type of service (Device or User), and the Settings applied to the group (such as App Catalog (Pro), or Security).
   - **Users**—Displays group members and their roles.
   - **Devices**—Displays the device name, the name of the device owner, and the device operating system.
3. Select **Done**.

Users

To view a list of current users, on the HP Touchpoint Manager dashboard, select **Users**.

There are two types of users:

- **IT administrators**—Can add users, delete users, and edit user profiles. There is no limit to the number of users who can be managed with an HP Touchpoint Manager account.
- **Managed users**—Can view their own enrolled devices, edit their own user profiles, and reset their own passwords.

Adding users

An IT administrator can add a single user to HP Touchpoint Manager.

NOTE: To add multiple users, see Importing a list of users, Importing users from Azure Active Directory (Azure AD), or Rapid provisioning (Windows, Android, and iOS).

1. On the HP Touchpoint Manager dashboard, under **Quick Links**, select **Add Users**.

   – or –

   Select **Users**, and then select **Add Users**.

2. Enter the user's name, email address, and then select their default grouping.

   These are not required fields. If no information is provided, then a generic user is created (for example, User1).

3. To add a single additional user, select **Add another user**.

   To import a list of users, select **Import List** (see Importing a list of users) or **Import from Azure AD** (see Importing users from Azure Active Directory (Azure AD)).

4. Select one of the following payment methods:

   - To use previously purchased subscription keys, select **Submit**.
   - To add a previously purchased subscription key, select **Click here to enter a subscription key** (see Adding subscription keys).
   - To be billed with the credit card that is on file for the HP Touchpoint Manager account, select **Checkout**.

   A confirmation screen is displayed that shows the number of users successfully added. The IT administrator can either send email invitations to users with email addresses on file who need an HP Touchpoint Manager account or download a .CSV file with a list of PIN codes that can be used by a user to automatically activate the account and enroll a device.

Adding multiple users

An IT administrator can import a list of multiple users or import users from Azure AD.

Importing a list of users

An IT administrator can import multiple users at one time by using a text editing program to create a user list.

NOTE: You must add subscription keys to the account before you add new users (see Adding subscription keys).

1. Open a text editing program, such as Notepad.
2. Format each line item as follows: <User Name>, <User Email>, <User Group>, <Device Group>.

   NOTE: To import a user, either the <User Name> or the <User Email> must be provided in each entry.

3. For each user, start a new line, and then repeat step 2.
4. When you are finished adding users, save the file as **users.csv**.

To import a user list:

1. On the HP Touchpoint Manager dashboard, under **Quick Links**, select **Add Users**.

   – or –

   Select **Users**, and then select **Add Users**.

2. Select **Import List**.
3. Select the .csv file that you created, and then follow the on-screen instructions.
4. To view a list of the imported users, select **Pending Users**.
5. Select the user accounts to be fully activated. You can also modify the user account grouping.
6. To be billed with the credit card that is on file for the HP Touchpoint Manager account, verify the entries for accuracy, and then select **Submit** to add the users.

   – or –

   To use previously purchased subscription keys, select **Click here to enter a subscription key** (see Adding subscription keys), and then select **Submit** to add the users.

   A confirmation screen is displayed showing the number of users successfully added.

7. The IT administrator can send email invitations to users with email addresses on file who need an HP Touchpoint Manager account, or download a .CSV file with a list of PIN codes that can be used by a user to automatically activate the account and enroll the device.

Importing users from Azure Active Directory (Azure AD)

An IT administrator can import multiple users from Azure AD to allow users to sign in to HP Touchpoint Manager using their Azure AD credentials.

NOTE: You must add subscription keys to the account before you add new users (see Adding subscription keys).

NOTE: When performing a user import, the email address of the HP Touchpoint Manager IT administrator must be the same as that of the Azure AD administrator. For example, if the Touchpoint IT administrator's email address is **mailto:first.last@mycompany.com**, then the Azure AD account used for the import must be **mailto:first.last@mycompany.com**.

NOTE: Microsoft Live account credentials (such as **mailto:first.last@mycompany.com**) are different from Azure AD credentials, so they cannot be used to import users from Azure Active Directory. Only valid Azure AD user credentials can be used to perform this task.

1. On the HP Touchpoint Manager dashboard, under **Quick Links**, select **Add Users**.

   – or –

   Select **Users**, and then select **Add Users**.

2. Select **Import from Azure AD**.

3. Enter your Azure login credentials, select **Grant Access**, and then follow the on-screen instructions.

4. To view a list of the imported users, select **Pending Users**.

   HP Touchpoint Manager detects instances where an HP Touchpoint Manager user email address matches an Azure AD email address and merges the matching email addresses.

5. Select the user accounts to be fully activated. You can also modify the user account grouping.

6. To be billed with the credit card that is on file for the HP Touchpoint Manager account, verify the entries for accuracy, and then select **Submit** to add the users.

   – or –

   To use previously purchased subscription keys, select **Click here to enter a subscription key** (see Adding subscription keys), and then select **Submit** to add the users.

   A confirmation screen is displayed showing the number of users successfully added.

7. The IT administrator can send email invitations to users with email addresses on file who need an HP Touchpoint Manager account, or download a .CSV file with a list of PIN codes that can be used by a user to automatically activate the account and enroll the device.

Activating a new user account

1. Open the HP Touchpoint Manager account confirmation email message you received when your user account was created.

2. In the confirmation email, select **Activate my account**.

3. On the HP Touchpoint Manager home screen, follow the on-screen instructions.

   The HP Touchpoint Manager dashboard is displayed.

4. To complete signup and enrollment, install the client software.

Deleting users

An IT administrator can delete users from HP Touchpoint Manager.

1. On the HP Touchpoint Manager dashboard, select **Users**.

2. Select the check box to the left of each name to be removed, and then select **Remove users**.

3. When the confirmation dialog is displayed, select **Remove**.

Downloading a user’s PIN

An IT administrator can download a user’s PIN (see Rapid provisioning (Windows, Android, and iOS)). A PIN can be used to enroll devices for users who will not log on to http://www.hptouchpointmanager.com, or who do not have email addresses. For user accounts created in this way, the IT administrator distributes a unique enrollment code to each user. The PIN code can be used one time to enroll a single device.

1. On the HP Touchpoint Manager dashboard, select **Users**.

2. Select the check box to the left of each user whose PIN is to be downloaded, and then select **Download PINs**.

3. When the confirmation dialog is displayed, select **Download**.

Editing a user profile

An IT administrator can edit a user's profile, view a user's enrolled devices, or delete a user from HP Touchpoint Manager.

Users can edit their own profiles and change their own passwords.

1. On the HP Touchpoint Manager dashboard, select **Users**.
2. Select the name of the user whose information is to be edited.

   A detail page is displayed with photo, status, role, and devices for the selected user.
3. To edit the user’s information:
   - **Contact Info**—Select **Edit**, enter the new information, and then select **Save**.
   - **Change Password**—Select **Edit**, enter the old password, enter the new password, enter the new password to confirm, and then select **Save**.

     NOTE: An IT administrator cannot change a managed user’s password. Managed users can change their own passwords.
   - **Communication Preferences**—Select **Edit**, select or clear check boxes to set email and notification preferences, and then select **Save**.

Resetting my HP Touchpoint Manager password

1. On the HP Touchpoint Manager dashboard, select **Edit User Profile**.
2. Under **Change password**, select **Edit**.
3. Enter the old password, enter the new password, and then confirm the new password.
4. Select **Save**.

Verifying users

An IT administrator can verify information for enrolled users.

1. On the HP Touchpoint Manager dashboard, select **Users**.
2. Enter a managed user's email address in the search box, and then select **Search**.
3. Select the email address.

   Company name, user name, and device information are displayed.

Devices

HP Touchpoint Manager secures and tracks all computer assets, and provides device support for enrolled users. The device type, device name, user name, device owner, and last update are displayed.

- **IT administrators**
  - Can view a list of currently enrolled devices by selecting **Devices** on the HP Touchpoint Manager dashboard.
  - Can change ownership for a selected device by selecting **Company Device** or **Personal Device**.

NOTE: Some policies are not enforced for personal devices:

- **Erase Device**—Disabled
- **Find Device**—Disabled for IT administrators
- **Security Setting – Disable Camera**—Not enforced
- **Security Setting – Erase device after x password attempts**—Not enforced

  ◦ Can remove a selected device by selecting **Remove Device** (see Removing a device).

- **Users**—Can view their own enrolled devices by selecting **Devices** on the HP Touchpoint Manager dashboard.

Viewing device details

To view device details:

1. On the HP Touchpoint Manager dashboard, select **Devices**.
2. Select a device from the list that is displayed.

   The following information is displayed about the selected device:

   - **Summary**—Displays device type and inventory number, owner, last date updated, and group
   - **Overview**—Displays HP Touchpoint Manager version, device type, operating system, manufacturer, model number, BitLocker status, and device owner
   - **Health**—Displays alerts, hard disk health, battery health, antivirus status, and firewall status
   - **Hardware**—Displays hardware details, including hard drive status, battery status, date of last hard drive/battery check, model number, serial number, processor type, memory, and graphics card
   - **Software**—Displays installed software, version number, and installation date (Android and iOS only)
   - **Services**—Displays services enabled for the device
   - **Warranty**—Displays the manufacturer, warranty type (HP devices only), warranty start and end dates (HP devices with Windows or Android operating systems only), warranty description (HP devices only) and service details
3. Under **I Want To...**, you can select one of the following actions for the displayed device:

   - **Sound Alarm**—See Sounding the alarm on a device.
   - **Lock This Device**—See Locking a device.
   - **Erase This Device**—See Erasing data from a device (Windows, Android, and iOS).
   - **Activate Remote Control**—See Remote Control.
   - **Locate This Device**—See Find Device (Windows, Android, and iOS).
   - **View Alerts**—See Alerts.
   - **Remove Device**—See Removing a device.

Removing a device

An IT administrator can remove devices from HP Touchpoint Manager.

1. On the HP Touchpoint Manager dashboard, select **Devices**.
2. Select the check box to the left of the device(s) to be removed.
3. Select **Remove Selected Devices**.
4. When the confirmation banner appears, select **Remove**.

– or –

▲ On the **Device Details** page, select **Remove This Device** (see Viewing device details).

Find Device (Windows, Android, and iOS)

An IT administrator can find managed devices on a map. Users can find their own devices, but they cannot view other users' devices.

NOTE: This policy is not enforced for personal devices.

To find a device, on the HP Touchpoint Manager dashboard:

▲ Under **Quick Links**, select **Locate a Device**.

– or –

From the **Devices** list page, select a device, navigate to the device's **Device Detail** page, and then select **I want to locate this device**.

The device's last detected location is displayed on a map.

IT administrators can also view a list of other managed devices.

Find Device includes the following features:

Sound an alarm (Windows and Android only)—To help find a nearby lost device, the HP Touchpoint Manager service can sound a loud alarm on a device. The sound plays for 30 seconds by default unless stopped. HP Touchpoint Manager automatically enables sound and sets the speaker volume at maximum before the sound is played.

Lock device—For Android devices, the device screen is locked with a secret PIN code (visible on the **Device Details** page), and it cannot be used until the PIN code is entered. The user is then prompted to enter a new PIN for the device. For iOS devices, the device is locked with the passcode currently stored on the device.

NOTE: If a lost device is recovered, the IT administrator can provide the PIN to unlock the device.

Erase device data—This feature causes a device factory reset, which erases all on-device data, but does not erase data on any externally-attached media that may be connected to the device.

Find device on map— The device's last detected location is displayed on a map. You can also select the following actions:

- **Sound Alarm**—See Sounding the alarm on a device.
- **Lock**—See Locking a device.
- **Erase Device Data**—See Erasing data from a device (Windows, Android, and iOS).

Enabling Find Device

An IT administrator can enable the Find Device feature:

1. On the HP Touchpoint Manager dashboard, select **Services**, and then under **Find Device**, select **Configure**.
2. Select the **Activate Find Device** check box.

Disabling Find Device

An IT administrator can disable the Find Device feature:

1. On the HP Touchpoint Manager dashboard, under **Services**, select **Find Device**.
2. Clear the **Activate Find Device** check box.

Erasing data from a device (Windows, Android, and iOS)

For Android and iOS devices, this feature causes a device factory reset. For Windows devices, the feature erases all on-device data, but does not erase data on any externally-attached media that may be connected to the device.

Only an IT administrator can remotely erase data from an enrolled device.

This feature logs off the device and attempts to erase all data from the device.

⚠ **CAUTION:** This feature cannot be canceled once it is started. The operation takes a significant amount of time to complete.

NOTE: If a Windows device was locked, but is found later after data is erased, the IT administrator can provide the PIN to unlock the device.

NOTE: This policy is not enforced for personal devices.

1. On the HP Touchpoint Manager dashboard, under **Quick Links**, select **Erase data on a device**.

   - or –

   On the HP Touchpoint Manager dashboard, select **Devices**.
2. Select the device to be erased.
3. Select **Erase Device Data**.
4. Enter your IT administrator password, and then select **Erase**.

Erase device operation sequence (Windows)

An IT administrator can use the device erase feature when a lost device, which contains sensitive user data that you do not want others to access, cannot be retrieved.

The Windows device erase process erases user data and overwrites all data files on the computer’s fixed hard drives to render them unrecoverable by traditional utilities used to erase data.

When the data erase process completes, HP Touchpoint Manager then overwrites all unallocated file space on the fixed drive to ensure more comprehensive coverage. HP Touchpoint Manager does not delete the Windows operating system or program files. Because the full erase process can run for hours, the process focuses first on data files, and second on free drive space that may contain fragments of data from previously erased files. If the task has not completed, it resumes after a device restart.

⚠ **CAUTION:** After a device erase has been performed, the operating system or installed applications are not guaranteed to continue functioning on the device. If the lost device is ultimately retrieved, reinstalling the operating system and applications is recommended before continuing to use the device.

Erase device operation sequence (Android)

The Android device erase process conducts a factory reset. This process renders all data and applications on the lost device inaccessible.

Erase device operation sequence (iOS)

The iOS device erase process conducts a factory reset. This process renders all data and applications on the lost device inaccessible.

Locking a device

An IT administrator can lock a device remotely.

- **Android devices**—The device screen is locked with a secret PIN code (visible on the **Device Details** page), and it cannot be used until the PIN code is entered. Then the user is prompted to enter a new PIN for the device.
- **iOS devices**—The device is locked with the passcode currently stored on the device.
- **Windows devices**—The user’s session is logged off.

NOTE: If a lost device is recovered, the IT administrator can provide the PIN to unlock the device.

1. On the HP Touchpoint Manager dashboard, under **Quick Links**, select **Lock a Device**.

   - or –

   On the HP Touchpoint Manager dashboard, select **Devices**.
2. Select the device to be locked.
3. To lock the device, select **Lock**.

Sounding the alarm on a device

To help find a nearby lost device, the HP Touchpoint Manager service can sound a loud alarm on a device. The sound plays for 30 seconds by default unless stopped. HP Touchpoint Manager automatically enables sound and sets the speaker volume at maximum before the sound is played.

An IT administrator can remotely sound an alarm on an enrolled device.

1. On the HP Touchpoint Manager dashboard, under **Quick Links**, select **Sound alarm on a device**.

   - or –

   On the HP Touchpoint Manager dashboard, select **Devices**.
2. Select a device, and then select **Sound Alarm**.

   HP Touchpoint Manager turns on a loud sound on the device.

Alerts for Find/Erase/Lock/Alarm

NOTE: When the factory reset erase operation is complete, an alert is not generated because the device loses the ability to communicate with the HP Touchpoint Manager software.

Persistent Anti-Theft (select HP Android Slate tablets only)

Select HP Android Slate tablets include persistent anti-theft technology that allows HP Touchpoint Manager to alert an IT administrator that the device might be stolen.

If a supported device is reset to its factory state while the device is enrolled with an HP Touchpoint Manager account, then an IT administrator is alerted that the device may have been stolen.

The IT administrator can then use the Find device feature to find, lock, sound an alarm, or erase data from the device (see Find Device (Windows, Android, and iOS)). If the device is recovered, then the device owner can launch HP Touchpoint Manager and sign in with user-name and password to authenticate the device and release it from anti-theft mode.

Services

HP Touchpoint Manager monitors services 24 hours per day, 7 days per week.

1. The following services are displayed on the HP Touchpoint Manager dashboard:
   - Security
   - Find Device (Windows, Android, and iOS)
   - Wi-Fi Provisioning (Android and iOS only)
   - Password Recovery
   - Application Deployment
   - Remote Control
   - Software Inventory (Windows and Android)
   - Software Updates (Windows only)
2. To view and purchased services, select ⚙, and then select **Services**.
3. To view enrolled users for each purchased service, select **Go to the service**.

Always On Remote Management (HP devices only)

With Always On Remote Management, HP Touchpoint Manager can communicate with select HP devices while the device is in a low power mode, such as Sleep (S3), Hibernation (S4), or Soft Off (S5). This feature is enabled on select HP devices and is automatically activated when the HP Touchpoint Manager software is installed on an enrolled device.

The following BIOS-level features are available when the IT administrator accesses the device through the HP Touchpoint Manager server using Always On Remote Management:

- **Remote Lock**—Securely locks a lost or stolen device remotely. This lock requires a PIN number to unlock the computer.

  NOTE: The IT administrator can view the unlock PIN number on the Device Details page. The PIN must be entered locally to unlock the device.

- **Remote Erase**—Securely erases a device that has been lost, stolen, or reassigned. The device also performs a Remote Lock when the Remote Erase command is received. Once a Remote Erase begins, the device must complete the erase function before an unlock PIN can be entered.

- **Unlock**—The IT administrator can view the unlock PIN number on the Device Details page. The PIN must be entered locally to unlock the device.
- **Always On Remote Management Boot Error Reporting**—If the device cannot boot, an error is reported to the server if communication cannot be established. The server sends an alert to the IT administrator with a brief description of the error.

NOTE: The feature is not available in all countries (see http://www.hp.com/go/touchpoint for availability). Out-of-band HP only Erase, Lock, Unlock, and reporting of BIOS boot error codes are available on select HP EliteBooks and require an Internet connection, Intel vPro™ technology, and function in S3 (Sleep), S4 (Hibernate), and S5 (Soft Off) power states. Self-encrypting drives with hardware based encryption enabled do not support the Always On Remote Management Erase feature. During an erase process, SATA drives (standard hard drives) are wiped.

Select HP EliteBook and HP ZBook devices currently support Always on Remote Management. In addition, the device must include the following features:

- Windows 7 Service Pack 1 (SP1) or higher operating system
- Intel vPRO technology
- Only SATA (standard hard drives)

  NOTE: Hardware encrypted Self Encrypting Drives (SEDs) are not erased remotely.
- The Always On Remote Management feature must be enabled in the device BIOS.
- HP Touchpoint Manager client software must be installed, and the device must be enrolled with either a Basic or Pro subscription plan. Functionality varies with each subscription plan.

Viewing the Always On Remote Management state for a Device

To determine whether the Always On Remote Management feature is activated or supported on your device, view Device Details for the device. The state is displayed under the Always On Remote Management label (see Viewing device details). Possible states include:

- **Active**—Always On Remote Management is activated and ready for use.
- **Activated**—Always On Remote Management is being activated.
- **Disabled**—Always On Remote Management has been disabled in the BIOS and should be re-enabled.
- **Not Supported**—Always On Remote Management is not supported on the specified device.

Activating Always on Remote Management

To activate Always On Remote Management:

1. When the device restarts, press f10 to access F10 BIOS Setup.
2. Select **Advanced**, and then select **HP Touchpoint Manager Options**.
3. Select the **Allow Activation** check box.

   NOTE: HP recommends setting a BIOS administrator password to prevent unauthorized de-provisioning. Failure to implement a password allows anyone in physical possession of the device to inactivate or disable the Always On Remote Management feature, including removal of the lock and erase features.

Disabling or preventing activation of Always on Remote Management

To disable or prevent activation of Always On Remote Management:

1. When the device restarts, press f10 to access F10 BIOS Setup.
2. Select **Advanced**, and then select **HP Touchpoint Manager Options**.
3. Clear the **Allow Activation** check box.

   Removing the check mark after a device has been enrolled and provisioned causes the device to be de-provisioned and prevents HP Touchpoint Manager from re-provisioning the device. The device can be re-provisioned if **Allow Activation** is checked, and the settings are saved.

NOTE: HP recommends setting a BIOS administrator password to prevent unauthorized de-provisioning. Failure to implement a password allows anyone in physical possession of the device to inactivate or disable the Always On Remote Management feature, including removal of the lock and erase features.

Erasing data remotely with Always On Remote Management

For Always On Remote Management enabled devices, the BIOS securely erases all user, operating system, and program file data on all internal drives. After the BIOS completes the erasure, the BIOS requires a PIN before allowing the computer to install an operating system.

NOTE:

- Devices that support the Always On Remote Management feature can be in a low-power state such as Sleep (S3), Hibernation (S4), or Soft Off (S5), but the device must have an available Internet connection in order to receive the erase command.
- Devices that do not support the Always On Remote Management feature must be powered on and have Internet connectivity.

Application Deployment

An IT administrator can manage deployment of applications to Windows devices or to mobile devices:

- Application Deployment (Windows)
- Mobile Application Deployment (Windows, Android, and iOS)

Application Deployment (Windows)

An IT administrator can manage deployment of non-app store Windows applications (such as .MSI or setup.exe). When an app has been uploaded to the company's HP Touchpoint Manager store, it can be included in an App Catalog in the same way that free iOS and Android apps are deployed (see Mobile Application Deployment (Windows, Android, and iOS)

NOTE: Each company is limited to 20 GB of application uploads.

1. On the HP Touchpoint Manager dashboard, select **Services**, and then under **Application Deployment**, select **Custom Apps**.
2. To add an application, select **Add Applications**, enter information about the application, and then select **Upload**.

   The following table describes the available settings.

Setting	Description
Windows Application	
Name	Enter the name of the application.
Publisher	Enter the publisher of the application (optional).
Operating System	Select the operating systems on which the application should be installed. The application is installed only on target devices running this operating system.
File Type	● **Windows 64-bit**—Select this option if the application can be installed only on 64-bit versions of Windows. ● **Windows 32-bit**—Select this option if the application can be installed only on 32-bit versions of Windows.
Select Installer Startup File	● **.exe** or **.msi**—Select the type of Installer file to upload.
Installation Options	
Silent Install	Enter the command line option for silent install. If the installer requires user interaction, the install may fail.
Suppress Reboot	Enter the command line option to suppress reboots. If the installer requests a reboot, applications installed subsequently within an App Catalog may fail.
Other Custom Options	Enter additional command line options (optional).
Detection Rules	
File Exists	Enter the path to a file that will exist on the target device after the application is installed. ● **Program Files (x86)** or **Program Files**—Both folders are searched on 64-bit operating systems. ● **%System Drive%**—Represents the drive on which the Operating System is installed, typically Drive C.
Registry Key Exists	Enter the path to a registry key that will exist on the target device after the application is installed. The registry key must be under HKEY_LOCAL_MACHINE\SOFTWARE\. Both 32-bit and 64-bit versions of the registry path are searched.
Return Codes	
Success	HP Touchpoint Manager uses this return code to determine whether the application was installed successfully. Edit the Success return code only if your application returns a different code for successful installations.
Success with Restart	HP Touchpoint Manager uses this return code to determine whether the application was installed successfully. Edit the Success return code only if your application returns a different code for successful installations requiring a restart.

A list is displayed of all applications that are ready to be deployed and the free space remaining from the 20 GB allocation.

NOTE: Windows Installer files, which require user interaction during setup, cannot be installed by HP Touchpoint Manager. Be sure to test the application deployment before distributing the application to users.

3. To change information originally provided for the application, select **Edit**.

4. To remove the application from the store, select the application, and then select **Delete**.

   NOTE: Deleting an application from the store provides more storage space for application uploads, but it does not remove the application from devices to which it has been deployed.

5. Select **Add Applications**.

Mobile Application Deployment (Windows, Android, and iOS)

An IT administrator can create a new App Catalog for enrolled mobile devices:

NOTE: HP Touchpoint Manager allows free apps to be distributed via the Application Deployment feature.

1. On the HP Touchpoint Manager dashboard, select **Services**, and then under **Application Deployment**, select **Configure**.

2. Under **App Catalogs**, select **Create New**.

3. Enter the description details for the App Catalog, and then select **Next**.

4. Search and select the applications to add to the App Catalog, and then select **Next**.

5. Search and select the groups to receive the App Catalog, and then select **Finish**.

   - The new App Catalog is displayed on the Application Deployment home page.
   - All apps within the catalog are pushed to all devices in the selected groups enrolled under the company account, and each device receives a notification for the new apps that can be installed.

     After receiving the notification, users must install the applications on their devices.

   NOTE:

   - Search results are based on the browser language preference setting. To search for an application available only in a specific language, the browser language preference must be set to that language.
   - On Windows and Android devices, HP Touchpoint Manager checks periodically to determine if an application was uninstalled and notifies users to reinstall the application.

Edit an App Catalog

1. On the HP Touchpoint Manager dashboard, select **Services**, and then under **Mobile Application Deployment**, select **Configure**.

2. From the Productivity drop-down menu, select **Edit**.

3. When the App Catalog opens, make the necessary edits, and then select **Finish**.

Clone an App Catalog

An IT administrator can clone an App Catalog to make an exact copy of an existing App Catalog.

1. On the HP Touchpoint Manager dashboard, select **Services**, and then under **Mobile Application Deployment**, select **Configure**.

2. From the Productivity drop-down menu, select **Clone**.

3. When the App Catalog opens, make the necessary edits to the cloned App Catalog, and then select **Next**.
4. Search and select new applications for your App Catalog, and then select **Finish**.

Delete an App Catalog

1. On the HP Touchpoint Manager dashboard, select **Services**, and then under **Mobile Application Deployment**, select **Configure**.
2. From the Productivity drop-down menu, select **Delete**.
3. Select **OK** to confirm the deletion.

View App Catalog details

1. On the HP Touchpoint Manager dashboard, select **Services**, and then select **Application Deployment**.
2. From the Productivity drop-down menu, select **Details**.

Password Recovery

The HP Password Recovery (HPPR) feature allows Windows users to reset forgotten passwords on any enrolled Windows devices managed by HP Touchpoint Manager.

Activating HP Password Recovery

The HP Password Recovery (HPPR) feature can be distributed automatically to any enrolled devices associated with accounts where users have upgraded to Pro.

By default, the feature is not automatically distributed to enrolled devices, so users must enable this feature by following these steps:

1. On the HP Touchpoint Manager dashboard, select **Services**, and then under **Password Recovery**, select **Configure**.
2. Select the **Activate Password Recovery** check box, and then select **Save**.

   The setting takes effect immediately, and all Windows devices enrolled to the HP Touchpoint Manager account will receive the HP Password Recovery feature.

   NOTE: Clearing this check box does not uninstall this feature from devices that have Password Recovery.

NOTE: If a managed user has multiple Windows devices, then each computer has a separate question/answer pair for password reset.

Configuring HP Password Recovery

After the HP Password Recovery Provider is installed, users complete three security credential questions. The answers to these questions authenticate users who have forgotten their Windows passwords.

After the security questions are created, **HP Password Recovery** is displayed below the password entry text box on the Windows Login screen.

Resetting the Windows Password

To reset the Windows password on a computer:

1. Select **HP Password Recovery**, and then enter answers to three previously chosen questions.
2. After the correct answers have been provided, you can reset the forgotten Windows Password.

NOTE: If the Windows account is a domain account, the device must be connected to the domain to reset the Windows password.

NOTE: For domain accounts, if the Windows password was reset on another device, the security questions previously chosen will no longer take effect. The user must follow the instructions below and reset the HP Password Recovery security questions to get HP Password Recovery back to a working state.

Resetting the HP Password Recovery security questions

To change the security questions previously chosen:

1. Select **HP Password Recovery**, select **Reset HP Password Recovery**, and then enter the password for the Windows account.
2. After the correct Windows password is entered, you can choose a new set of security questions for the Windows account.

Disabling deployment of HP Password Recovery

To disable deployment of the HP Password Recovery feature to newly enrolled devices, follow these steps:

1. On the HP Touchpoint Manager dashboard, select **Services**, and then select **Password Recovery**.
2. Clear the **Deploy HP Password Recovery to Windows devices** check box, and then select **Save**.

   The setting take effect immediately, and any new devices enrolled to the HP Touchpoint Manager account will no longer receive the HP Password Recovery feature.

NOTE: Removing this setting does not remove HP Password Recovery from devices that already have this feature installed.

Remote Control

The Remote Control service, available with Pro subscriptions, allows an IT administrator to take control of enrolled Windows devices through the browser from virtually anywhere. An IT administrator can control managed Windows devices remotely through any device with an HTML-5 browser.

Starting a Remote Control session

IT administrators can establish a Remote Control connection with an enrolled device in one of the following ways:

1. On the HP Touchpoint Manager dashboard, under **Quick Links**, select **Remote Control**.
2. In the search box, enter a device, user name, or email address, select **Search**, and then follow the on-screen instructions.

– or –

1. On the HP Touchpoint Manager dashboard, select **Devices**.
2. Select the device that you want to control remotely.
3. Under **I Want To ...**, select **Activate Remote Control**.

   An IT administrator can manage all aspects of the remotely controlled desktop from the Remote Control Viewer.

Configuring Remote Control preferences

An IT administrator can configure preferences for Remote Control sessions.

1. On the HP Touchpoint Manager dashboard, select **Services**, select **Remote Control**, and then select **Configure**.

2. Select one or more of the following options:

   ### Session settings

   - **Lock out keyboard and mouse**—Select the check box to disable the remote device's keyboard and mouse. Only the remote control viewer's keyboard and mouse will operate during the remote control session.

     NOTE: Special key combinations in Windows such as ctrl+alt+del or Windows key +L" are not locked out.

   - **Suppress wallpaper**—Select the check box to substitute a solid color for the device wallpaper. Select this option to enhance speed during a remote control session.

   - **Image quality**—From the drop-down menu, select **High**, **Medium**, or **Low** image quality to enhance speed during a remote control session.

     NOTE: Colors in the remote control window may vary from the remote desktop.

   ### Advanced session settings

   - **Keyboard language**—Select the desired language for the keyboard.

   - **Minutes for inactivity timeout**—Enter the number of minutes for the remote control session to remain active after no mouse or keyboard activity is detected.

3. Select **Save**.

4. To display a confirmation prompt for every remote control session, select the **Prompt me at every remote session for settings confirmation** check box.

5. Select **Start Remote Session**.

Using the Remote Control Session Viewer

When the remote control session starts, the Remote Control Session Viewer is displayed. A toolbar displays the following controls on the left side of the screen:

- **Keyboard**—Displays the on-screen keyboard. You can use the keyboard to press keys that your browser can't normally pass to the remote computer. The ctrl, alt, and shift (up arrow) keys stay pressed until you click the key again.

- **Remote Execute**—Allows you to find and launch an executable on the remote device.

- **Screenshot**—Allows you to capture a screenshot and save the image.

- **Upload**—Allows you to remotely transfer files from your computer to the remote device.

- **Download**—Allows you to remotely transfer files to your computer from the remote device.

- **Monitors**— If the remote computer has multiple monitors, allows you to select a monitor. The monitor thumbnail images show what was on each monitor when the session started.

- **Zoom**—Allows you to scale the remote session to fit in your browser's window. If the window size is too small, the scaled session text and other session elements may be hard to see. When zoomed in, scroll bars appear that you can use to see session parts that don't fit in the window.
- **Chat**—Allows you to chat remotely with the user at the remote device.
- **Reboot**—Allows you to reboot a device remotely.

  NOTE: Restarting the device effectively ends the Remote Control session. Advise the user to remain available after the restart to approve another Remote Control session. An IT administrator usually activates another Remote Control session to ensure that the fixes implemented took effect and solved the user's problem.
- **Settings**—Displays the Settings dialog.

Using Remote Control from a mobile device

Remote control of a Windows computer can be performed with any device using an HTML-5 browser.

NOTE: Because mobile devices usually have slower processors than desktop devices, remote control sessions may have a slightly slower frame rate than an equivalent desktop remote control session.

Controlling another computer remotely from a mobile device with an older browser and then allowing the mobile device to sleep while the session is active may cause the browser on the mobile device to freeze. To release the HTML remote control page, try typing a new URL for the browser to navigate to.

Ending a Remote Control session

You can end a remote control session in one of the following ways:

- Right-click the **Your screen is visible to ...** tag on the screen, and then select **End session**.
- Use the **End Viewing Session** hot key defined in the settings for the Remote Control Session Viewer.
- On the Remote Control Session Viewer, select **End Session**.

Security

HP Touchpoint Manager can enforce security policies on devices. A Security Profile is a set of rules regarding the security features of a device.

To view existing Security Profiles:

▲ On the HP Touchpoint Manager dashboard, select **Services**, and then under **Security**, select **Status**.

The following Security Profile policy templates are available:

- **Standard**—Requires a 4-digit passcode, and the device is locked after 30 minutes of inactivity.
- **Enhanced**—Requires an 8-digit passcode. The device is locked after 15 minutes of inactivity, and then data is erased from the device after 15 failed unlock attempts.
- **Maximum**—Requires an 8-digit passcode that requires letters and numbers. The device is locked after 5 minutes of inactivity. Data is erased from the device after the password has been entered incorrectly 10 times in a row.
- **User Managed**—Allows the IT administrator to create a custom policy for the company. The following settings can be customized:

Setting	Description
Lock device after a period of inactivity	Default: 5 minutes
Password	Minimum length (4)
Password	Requires letters (Enable / **Disable**)
Password	Requires numbers (**Enable** / Disable)
Password	Requires special characters (Enable / **Disable**)
Password	Expires after [X] days (Enable / **Disable**)
Password history enforcement	[X] unique passwords required (Enable / Disable)
Device erase after [X] failed login attempts	(Enable & # value/ **Disable**) **NOTE:** This policy is not enforced for personal devices.
Camera	(**Enable** / Disable) **NOTE:** This policy is not enforced for personal devices.

Security Profiles can also be created for mobile devices (see Mobile Device Security (Android and iOS)).

Create a Security Profile

An IT administrator can create a Security Profile:

1. On the HP Touchpoint Manager dashboard, select **Services**, and then, under **Security**, select **Configure**.
2. Select the Security Profile to be edited, or select **Details** from the drop-down menu.
3. On the Security Profile page, select **Edit**.
4. To modify the devices for the Security Profile, select **Edit** on the device window.

   When the wizard opens, follow the same instructions to edit the Security Profile as you did when you created the Security Profile (see Create a Security Profile).

Edit a Security Profile

An IT administrator can edit a Security Profile:

1. On the HP Touchpoint Manager dashboard, select **Services**, and then, under **Security**, select **Configure**.
2. Select the Security Profile to be edited, or select **Details** from the drop-down menu.
3. On the Security Profile page, select **Edit**.
4. To modify the devices for the Security Profile, select **Edit** on the device window.

   When the wizard opens, follow the same instructions to edit the Security Profile as you did when you created the Security Profile (see Create a Security Profile).

Clone a Security Profile

An IT administrator can clone a Security Profile to make an exact copy of an existing Security Profile.

1. On the HP Touchpoint Manager dashboard, select **Services**, and then, under **Security**, select **Configure**.
2. Select the Security Profile to be cloned, or select **Details** from the drop-down menu.

3. On the Security Profile page, select **Clone**.

4. To clone the Security Profile, select **Clone** on the device window.

   When the wizard opens, follow the same instructions to clone the Security Profile as you did when you created the Security Profile (see Create a Security Profile).

Delete a Security Profile

1. On the HP Touchpoint Manager dashboard, select **Services**, and then, under **Security**, select **Configure**.

2. Select the Security Profile to be deleted, or select **Details** from the drop-down menu.

3. On the Security Profile page, select **Delete**.

4. Select **OK** to confirm the deletion.

Viewing Security Profile details

1. On the HP Touchpoint Manager dashboard, select **Services**, and then, under **Security**, select **Configure**.

2. Select **Details** from the drop-down menu.

Mobile Device Security (Android and iOS)

In addition to notebooks, desktops, and tablets, HP Touchpoint Manager can manage mobile devices with Android or iOS operating systems. To install and use the features of HP Touchpoint Manager from a mobile device, users must install the client and enroll the device using either their user name and password or a PIN code supplied by the IT administrator. Once the device is enrolled, a user can use all the features offered by HP Touchpoint Manager.

HP Touchpoint Manager can enforce security policies on mobile devices. For more information, see Security.

1. On the HP Touchpoint Manager dashboard, select **Services**, and then select **Security**.

2. Under **Security**, select **Status**, and then select **Mobile Security**.

   A list of all Android and iOS mobile devices enrolled in HP Touchpoint Manager is displayed.

Virus Protection (Windows only)

Antivirus software helps to prevent devices from computer viruses or malicious software (malware).

HP Touchpoint Manager detects whether anti-virus software is enabled and alerts when it cannot be enabled.

- If anti-virus software is installed, HP Touchpoint Manager displays the product name and whether it is enabled or disabled on the Virus Protection page.

- If no active anti-virus software product is detected, HP Touchpoint Manager automatically enables Windows Defender on devices with Windows 8.0 or higher operating systems, or downloads and/or enables Microsoft Security Essentials on devices with Windows 7.

- If a third-party (non-Microsoft) anti-virus software is installed but disabled, HP Touchpoint Manager cannot enable the third-party anti-virus product and does not attempt to enable Windows Defender or Microsoft Security Essentials on the device.

HP Touchpoint Manager continues to monitor the device and to ensure that Windows Defender or Microsoft Security Essentials remains enabled (if no other anti-virus software is installed). HP Touchpoint Manager also alerts the user if either Microsoft anti-virus product cannot be enabled.

An IT administrator can view or change the virus protection monitoring policy for devices.

- **Display the virus monitoring policy for devices**—On the HP Touchpoint Manager dashboard, select **Services**. Under **Security**, select **Status**, and then select **Virus Protection**.
- **Search for a device**—Enter the device name in the search box, and then select **Search**.

Firewall (Windows devices only)

Firewall protection activates the Windows Firewall service on the managed Windows computer. A firewall is software or hardware that helps to prevent unauthorized access to a device or network.

HP Touchpoint Manager detects whether firewall software is enabled and alerts when it cannot be enabled. If anti-virus software is installed, HP Touchpoint Manager displays the product name and whether it is enabled or disabled on the Firewall page.

- **Display the firewall monitoring policy for devices**—On the HP Touchpoint Manager dashboard, select **Services**. Under **Security**, select **Status**, and then select **Firewall**.
- **Search for a device**—Enter the device name in the search box, and then select **Search**.

Software Inventory (Windows and Android)

You can view information about applications installed on an enrolled device.

1. Select **Devices**, and then select the specific device from the list.
2. On the **Device Details** page, select **Software**, and then select **Inventory**.

   The list of installed applications is displayed:

   - **Company-owned devices**—The complete list of installed applications is displayed.
   - **Personal devices**—Installed applications are not displayed.

NOTE: The software inventory is automatically updated when applications are installed or removed.

Software Updates (Windows only)

IT administrators can manage deployment of software patches (Microsoft Windows and third-party software updates (Pro Only)) in the following ways:

- **Patch Deployment**—Installs specified patches on the targeted device. If a patch does not complete installation because a connection times out, then the installation resumes when the device is reconnected. The IT administrator is notified whether or not a patch is successfully installed.
- **Patch Filtering**—Allows the IT administrator to filter patches based on severity, user group, device group, device type, or define a custom search. Filtered results can be exported to a .CSV file for later analysis.
- **Patch Scan**—Scans the managed device ecosystem to identify devices that do not have the latest updates installed.
- **Deployment Timing**—Allows the IT administrator to start Patch Management manually or set up a schedule in advance for deployment.
- **View patches at the device-specific level**—Allows the IT administrator to view all patches installed on a specific device in the **Device Details** view.

1. Select **Services**, and then select **Software Updates**.
2. On the **Patch Management** page, select **Status** or **Manage**.

Status tab

On the **Status** tab, the IT administrator can perform the following tasks:

- View the status of all managed patches to determine which installed successfully, which failed to install, and which are pending.
- Filter patches by standard or customer-defined criteria.
- Start patch installation manually.
- Export the filtered results to a .CSV file for later analysis.

Manage tab

The **Manage** tab allows the IT Administrator to create or edit software patch management profiles.

Each software patch management profile has a unique name and description that is defined by the IT Administrator. The IT Administrator can also specify the following options:

- The types of patches to be installed:
  - Install important updates automatically
  - Install important and recommended updates automatically
  - Install all patches automatically
  - Do not install patches
- Day(s) and time(s) that the patch scan and installation will occur
- Group(s) to which the profile is applicable

Wi-Fi Provisioning (Android and iOS only)

An IT administrator can deploy and manage wireless connections for enrolled mobile devices.

NOTE: The device must be connected to the Internet in order to manage wireless connections.

▲ On the HP Touchpoint Manager dashboard, select **Services**, and then, under **Wi-Fi Provisioning**, select **Configure**.

Create a wireless connection

1. On the HP Touchpoint Manager dashboard, select **Services**, and then under **Wi-Fi Provisioning**, select **Configure**.
2. Under **Wi-Fi Provisioning**, select **Create New**.
3. Enter the description details for Wi-Fi Provisioning, and then select **Next**.
4. Enter the requested information (Network Name/SSID, Security Type, Security Key, etc.), and then select **Next**.
5. Select the devices to which Wi-Fi Provisioning applies, and then select **Finish**.

   The new wireless connection is displayed on the Wi-Fi Provisioning home page.

Edit a wireless connection

1. Select **Services**, and then select **Wi-Fi Provisioning**.
2. From the **Productivity** drop-down menu of Wi-Fi Provisioning to be edited, select **Edit**.
3. When Wi-Fi Provisioning opens, make the necessary edits, and then select **Finish**.

Clone a wireless connection

An IT administrator can clone a wireless connection to make an exact copy of an existing wireless connection.

1. On the HP Touchpoint Manager dashboard, select **Services**, and then select **Wi-Fi Provisioning**.
2. From the **Productivity** drop-down menu of the wireless connection to be edited, select **Clone**.
3. When Wi-Fi Provisioning opens, make the necessary edits to the cloned Wi-Fi Provisioning settings, and then select **Finish**.

Deleting a wireless connection

1. On the HP Touchpoint Manager dashboard, select **Services**, and then select **Wi-Fi Provisioning**.
2. From the **Productivity** drop-down menu of the wireless connection to be removed, select **Delete**.
3. Select **OK** to confirm the deletion.

Viewing Wi-Fi Provisioning details

1. On the HP Touchpoint Manager dashboard, select **Services**, and then select **Wi-Fi Provisioning**.
2. From the **Productivity** drop-down menu of the wireless connection to be viewed, select **Details**.

Settings

An IT administrator can view or change account information or manage subscriptions by selecting ⚙ in the upper-right corner of the HP Touchpoint Manager dashboard.

▲ On the HP Touchpoint Manager dashboard, select ⚙, and then select **Company**, **Subscriptions**, or **Certificates**.

Company

To view or change user information, select ⚙, select **Company**, and then select one of the following options:

- **Company Name and Address**—Select **Edit**, enter the new information, and then select **Save**.
- **Primary Contact**—Select the down arrow beside **Change Primary Contact**, select the desired name, and then select **Save**. Only an IT administrator can be selected as a primary contact.

Subscriptions

You can use a credit card or previously purchased subscription keys to add users.

1. On the HP Touchpoint Manager dashboard, select ⚙, and then select **Subscriptions**.
2. To add a new card, under **Billed Monthly**, select **Update Payment Methods**, and then follow the on-screen instructions
3. To view unpaid, pending, and enrolled orders, select **Purchase History**.
4. To cancel your HP Touchpoint Manager subscription, under **Cancel my HP Touchpoint Manager subscription**, select **Cancel Subscription**, and then select **Proceed** to confirm.

NOTE: If you cancel your HP Touchpoint Manager account, all of your users, devices, and services are deleted.

Credit cards

You can change the method of payment for an order that has already been placed, update your credit card information, or add a new credit card.

1. On the HP Touchpoint Manager dashboard, select ⚙, and then select **Company**.

   The Payment Methods screen is displayed.
2. To update your payment information, select **Update card**.
3. To add a new card, select **Add a new card**, and then enter the new information.
4. To change the payment method for an order that has already been placed, select **Click here**, and then follow the on-screen instructions.

Subscription Keys

To view or add subscription key information, under **Quick Links**, select **Add Subscription Key**.

– or –

Select ⚙, and then select **Subscriptions**.

For more information, see Adding subscription keys.

Adding subscription keys

You can purchase subscription keys for HP Touchpoint Manager Services for 1 or more users for a period of 1, 2, or 3 years from a partner or reseller.

When your purchase is complete, you will receive an email containing the subscription key number(s) and any additional instructions.

To add one pre-purchased subscription key:

1. On the HP Touchpoint Manager dashboard, under **Quick Links**, select **Add Subscription Key**.

   – or –

   Select ⚙, and then select **Subscriptions**.
2. Under **Subscription Keys**, select **Add Key**, type or paste a pre-purchased key, and then select **Add**.

NOTE: When you enter the subscription key, be sure that it matches the key in the email that you received. It may take up to 24 hours to activate your subscription key.

NOTE: Activate your subscription key as soon as possible. If you don't activate your key immediately, it is activated automatically 90 days after purchase, which could reduce the length of your subscription.

Adding multiple subscription keys

An IT administrator can import multiple subscription keys at one time by using a text editing program to create a user list:

1. Open a text editing program, such as Notepad.
2. List each subscription key on a separate line.
3. When you are finished adding subscription keys, save the file as **keys.csv**.

To add multiple pre-purchased subscription keys:

1. On the HP Touchpoint Manager dashboard, under **Quick Links**, select **Add Subscription Key**.

   – or –

   Select ⚙, and then select **Subscriptions**.

2. Select **Add Multiple Subscription Keys**, select **Browse**, select a .csv file containing a list of pre-purchased keys, and then select **Import**.

When the keys have been added, a list of subscriptions is displayed with the following information:

- Current status
- Start date
- Expiration date
- Term
- Number of subscriptions

Choosing a subscription

An IT administrator can select a Basic or Pro subscription and then select a payment option. Payment options include a pre-purchased subscription key, and/or a credit card. Each user needs a subscription key in order to upgrade. For more information, see Subscriptions.

NOTE: If you are purchasing a prepaid subscription, you must add subscription keys to the account before you add new users (see Adding subscription keys).

1. On the HP Touchpoint Manager dashboard, select **Buy Pro Now**.
2. Under **1. Choose Subscription**, select **Get Basic** or **Get Pro**.
3. Under **2. Payment Method**:
   - To use previously purchased subscription keys:
     a. Under **Subscription Key**, select **Enter Key**, type or paste a subscription key, and then select **Add** (Adding subscription keys).

        The subscription key is displayed.

     b. To complete the order, select **Submit**.
   - To pay for a monthly subscription with a credit card:

a. Under **Credit Card**, select **Enter Credit Card** (Credit cards).

b. Under **Complete Order**, select **Continue to Checkout**.

You are redirected to the ecommerce website (see Credit cards).

NOTE: To access help during the billing and purchase process, select **Avangate Billing Support**. You must provide the number Avangate provided during the purchase process.

NOTE: After the subscription upgrade, you may need to log out from HP Touchpoint Manager and then log on again to view the updated subscription options.

NOTE: A customer's users must have the same subscription level, either Basic or Pro.

Downgrading from Pro

1. On the HP Touchpoint Manager dashboard, select ⚙, and then select **Subscriptions**.
2. Under **Pro Subscription**, select **Manage**.
3. Select **Get Basic**.

Certificates

An IT administrator can manage Apple Push Notification (APN) Certificates from the Settings page.

▲ On the HP Touchpoint Manager dashboard, select ⚙, and then select **Certificates**.

Available certificates are displayed.

Reactivating a suspended account

An account can be suspended because the subscription has expired or because of a lack of payment.

NOTE: The same level subscription key is required to reactivate a suspended account. For example: A Basic subscription requires a basic key, and a Pro subscription requires a Pro key. At this time, a Basic key cannot reactivate a Pro subscription, and a Pro key cannot reactivate a Basic subscription.

Subscription costs continue to accrue during the time an account is suspended.

When an account is suspended, follow these instructions to resolve the issue:

1. On the **Account Suspended** screen under **How to Solve**, select one of the following:
   - **Enter Key**—See Adding subscription keys.
   - **Enter Credit Card**—See Credit cards.
   - **User Management**—See Users.
2. Follow the on-screen instructions.

Hardware Health (Windows devices only)

You can view a list of devices with owner name and device status. Hard drive and battery status are monitored for both HP and non-HP devices.

▲ On the HP Touchpoint Manager dashboard, select ⚙, and then select **Services**.

- **View details about a problem with a device**—Select **Click for information**.

Hardware Health monitors the device and displays one of the following: **Healthy** or **Problem detected-Click for information**.

- **Search for a device**—Enter the device name in the search box, and then select **Search**.

Signing out

▲ On the HP Touchpoint Manager dashboard, select 👤, and then select **Sign out**.

Help & Support

On the HP Touchpoint Manager dashboard, select ❔, and then, under **Help & Support**, select one of the available options.

5 Appendix

IT administrator and managed user roles

The user role determines the tasks and operations that persons can perform in HP Touchpoint Manager. The following table lists the roles and their respective permissions.

Accessing HP Touchpoint Manager

Permission	IT administrator	Managed user
Accept Invitation/Confirm Account	✓	✓
Access Alerts page	✓	
Access Device Details page (other users' devices)	✓	
Access Device Details page (user's own devices)	✓	✓
Access Devices page	✓	
Access Services page	✓	
Create account	✓	
Manage Service settings	✓	
Reset my lost HP Touchpoint Manager password	✓	✓
View Dashboard	✓	✓

Using HP Touchpoint Manager Services

HP Touchpoint Manager Services	IT administrator	Managed user
Find/Lock/Alarm (user's own devices)	✓	✓
Find/Lock/Alarm (other users' devices)	✓	
Erase data (user's own devices)	✓	✓
Erase data (other users' devices)	✓	
View change service settings and policy	✓	
Enroll my device	✓	✓
View Device Details page (user's own devices)	✓	✓
View Device Details page (other users' devices)	✓	
Reset forgotten Windows password (user's own devices)	✓	✓
Set question and answer details for forgotten Windows password reset (user's own devices)	✓	✓

IT Administration of HP Touchpoint Manager

Task	IT administrator	Managed user
Manage User/Device policy settings	✓	
View/Manage Company and Billing settings	✓	
Add/Update/Delete users	✓	
Enroll/Unenroll device (user’s own devices)	✓	✓
Delete Device (other users' devices)	✓	

Manage Accounts and Billing

Task	IT administrator	Managed user
Upgrade to Pro	✓	
Downgrade from Pro to Basic	✓	
Cancel HP Touchpoint Manager subscription	✓	

Uninstalling HP Touchpoint Manager

Android devices

To remove the HP Touchpoint Manager app from an Android device:

Step 1—Disable HP Touchpoint Manager.

1. Tap **Settings**, and then tap **Security**.
2. Tap **Device administrators**, and then clear the HP Touchpoint Manager check box.

Step 2—Uninstall HP Touchpoint Manager from the device.

1. Tap **All apps**.
2. Tap and hold the HP Touchpoint Manager app, and then drag the icon over **Uninstall** at the top of the screen.
3. If prompted, tap **Uninstall** to confirm.

NOTE: The app can only be removed from the device. Uninstallation via the Google Play store is not supported.

iOS devices

To remove the HP Touchpoint Manager app from an iOS device:

1. Tap and hold the **HP Touchpoint Manager** icon until it starts to move, and then tap the **X** in the corner of the icon.
2. Remove HP Touchpoint Manager Device Management Profile from your device.
3. Launch the **Settings** app, and then tap **General**.

4. For iOS 7, tap **Profiles**.

   – or –

   For iOS 8 or higher, tap **Device Management**.

5. Tap the **HP Touchpoint Manager Device Management** profile.

6. To complete the process, tap **Remove Management**.

Index