Endpoint Manager for Mobile Devices User's Guide

Contents

IBM Endpoint Manager for Mobile Devices User's Guide

The IBM Endpoint Manager for Mobile Devices application manages corporate and employee-owned smartphones and media tablets that access enterprise resources. The application can be used to manage security controls, software and hardware inventory, and application management.

This *User's Guide* provides instruction to IT managers and system administrators on how to manage the apps, inventory, and security policies for the devices in your deployment. Specifically, it includes management instructions for Android, iOS, Lotus Traveler, and Microsoft Exchange.

For information on how to install and configure Mobile Devices, see the *Mobile Devices Setup Guide*.

Components

The following is a list of the primary components of the MDM application and a brief description of their respective functions:

Server The Tivoli Endpoint Manager server is a database that communicates with the Tivoli Endpoint Manager relays and the Tivoli Endpoint Manager console to manage the devices in your deployment.

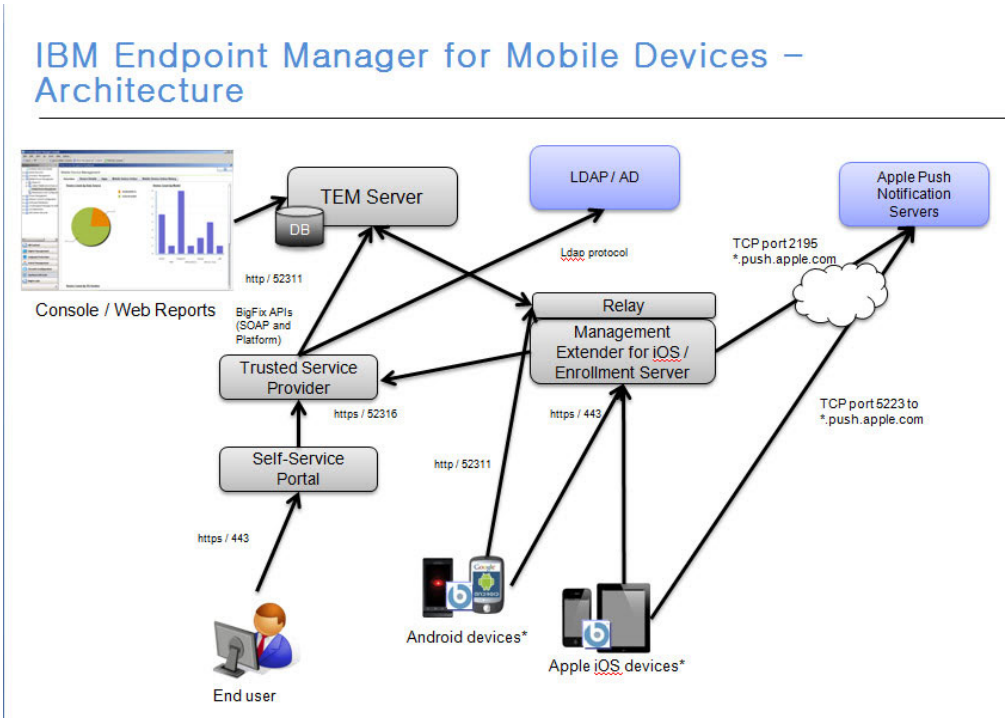
Relay Relays are network components designed to distribute the download burden from the Tivoli Endpoint Manager server and compile and compress data received from clients. In MDM, the relays process information from your mobile devices and transmit that information to the Tivoli Endpoint Manager server.

Management Extenders
Management Extenders allow devices to be managed without an agent on the device.

Email Servers
Includes Lotus Traveler and Microsoft Exchange servers.

Architecture

The diagram below depicts a visual representation of how MDM is designed to work in your environment.



Key Features

The following is a list of the most important features of Endpoint Manager for Mobile Devices:

- Integration with Tivoli Endpoint Manager platform
- Ability to import apps from Worklight server
- Support for basic management of devices using email-based management
- Support for advanced management of devices using agent-based management
- Device inventory
- Security and password policy management
- Management commands such as wipe, lock, clear-password, deny email access, push, and data roaming
- App Management
- Authenticated Enrollment for restrictive user access
- Self Service Portal for managing devices without the need for TEM or Web Reports
- Android WiFi
- Enterprise access configuration including email, WiFi, VPN

Note: Support for these features varies by device, OS, and management method.

System Requirements

General

See the following general requirements for using the Endpoint Manager for Mobile Devices application:

- Tivoli Endpoint Manager version 8.2 or higher must be used
- All management extenders must be installed on a system running Windows
- A Tivoli Endpoint Manager relay must already be installed on the system

Note: Before using this application, select an available port for the iOS Management Extender. The default is 443. If you want to use a different port, specify that port in the Configure Management Extender dashboard.

For Lotus Traveler

See the following requirements for Lotus Traveler:

On Traveler Server:

- Domino server must run the Traveler, DIIOP and HTTP tasks.
- HTTP must be listening on ports 80, 443 or both. The URL http(s)://<server>/diiop_ior.txt must be publicly accessible.
- DIIOP must be listening on ports 63148, 63149 or both. For configurations using port 63149, the SSL certificate must be valid and current, and a *TrustedCerts.class* file must have been generated in the Domino data folder.
- Create an administrative user. The administrative user must have both *read* and *edit* permissions in the ACL for LotusTraveler.nsf, and must be able to run restricted and unrestricted Domino commands.

On Management Extender for Lotus Traveler Server:

- The plugin must be able to contact the server in one HTTP and one DIIOP port. If DIIOP listens exclusively on port 63149, the plugin requires the server-specific TrustedCerts.class in its classpath. To do this, include the TrustedCerts.class in a TrustedCerts.jar file and deploy it in the plugin lib/ folder.
- The administrative user must have a username and password. Anonymous connections are not supported.

For Microsoft Exchange

See the following requirements for Microsoft Exchange:

On Exchange Server:

- Win 2008 Server
- WS-Management protocol
- WinRM
- Exchange Server 2007, 2010, 2013, or Office 365

On Management Extender for Exchange Server:

- WS-Management protocol and WinRM, or
- Exchange Management Tools (Exchange 2007 and 2010 only)

Note: If you intend to use this Management Extender to connect to a remote 2007 or 2010 Exchange server, first install Exchange Management Tools on the Management Extender so it connects properly to the remote server.

For Android

See the following requirements for Android:

- Android 2.2+ (Froyo) running on ARM processors
- Ability to connect to a Tivoli Endpoint Manager server or relay

Overview Dashboard

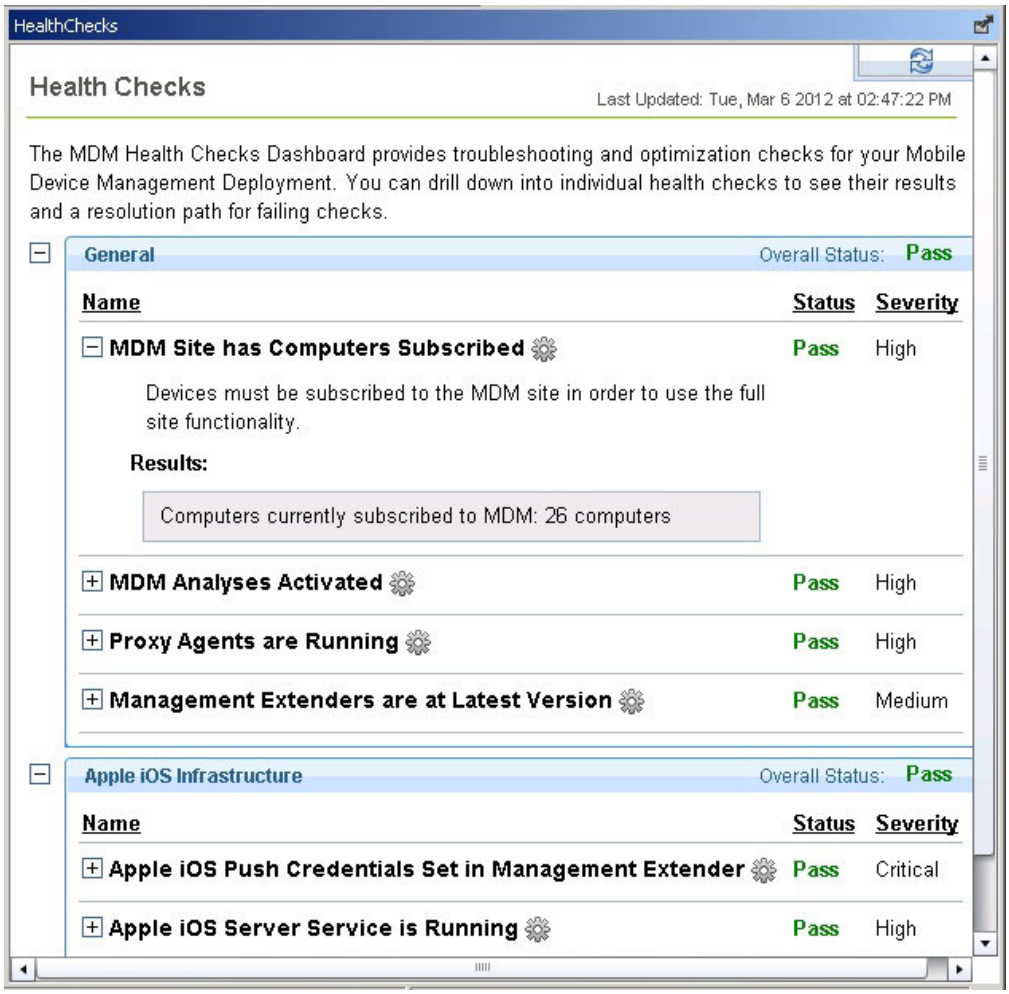
The MDM overview dashboard, accessible from the navigation tree, displays graphs that highlight the status of your MDM deployment. Graphs include:

- Device Count by OS
- Device Count by Data Source
- Device Count by Last Server Communication Time
- MDM Setup

You can change the way your data displays in the overview from the legend in the upper right corners of each graph. Content can display in a column chart, pie chart, or data table.

Health Checks Dashboard

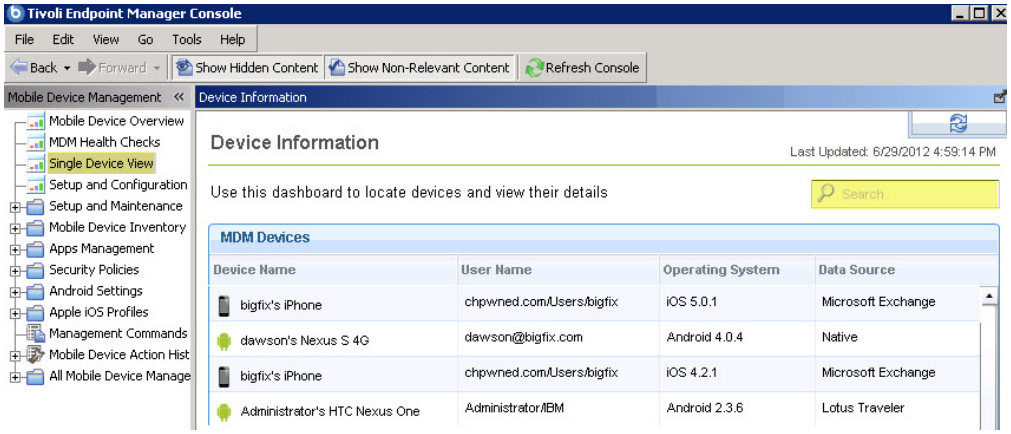
The Health Checks dashboard, located at the top of the navigation tree, provides troubleshooting checks for the devices in your deployment.



Use this dashboard to see the current health status of deployed extenders. If the deployment was set up properly, all the results should display as *Pass*. If the result of any check is *Fail,* expand the node and take the recommended action.

Single Device View Dashboard

The Single Device View Dashboard can be found at the top of the MDM navigation tree.

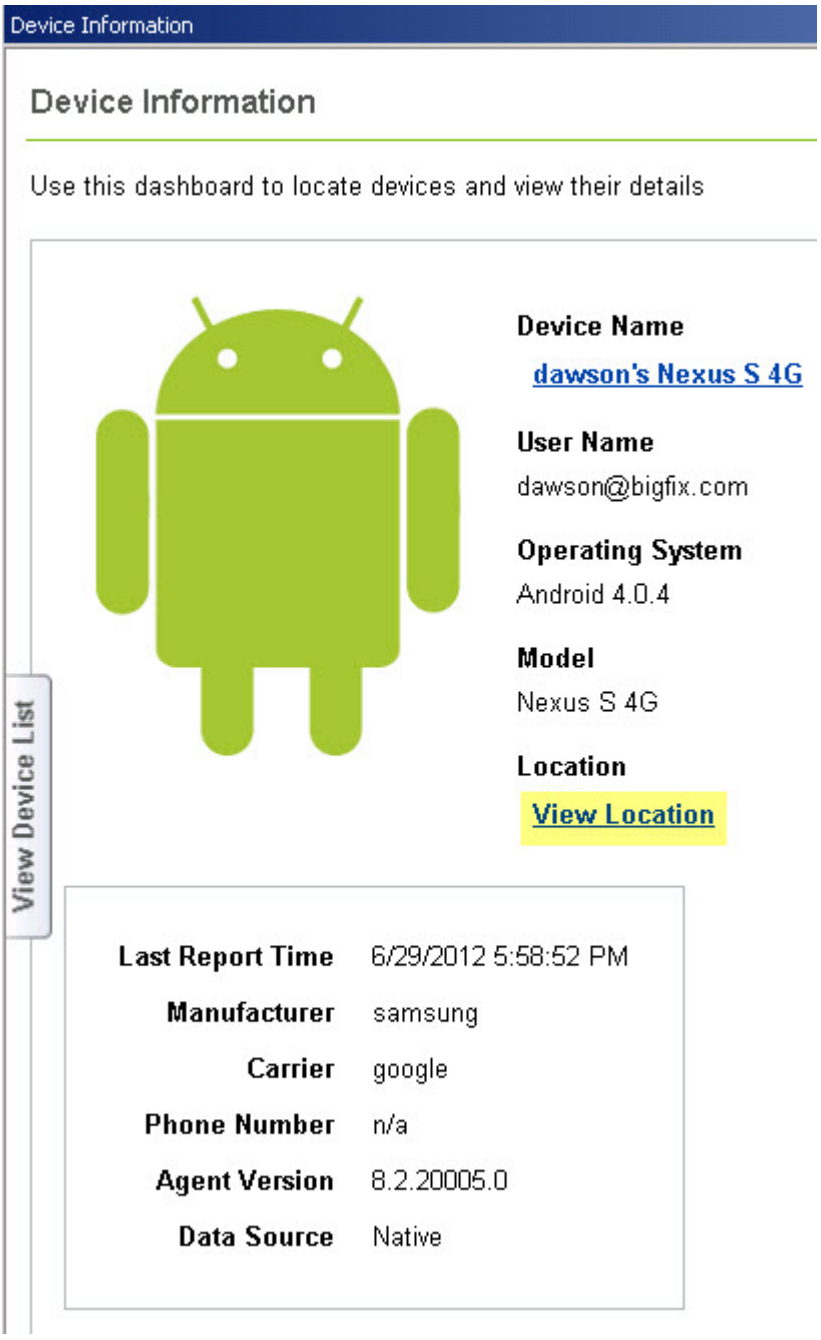


The dashboard has two ways of viewing device information – by device *list* and device *detail*.

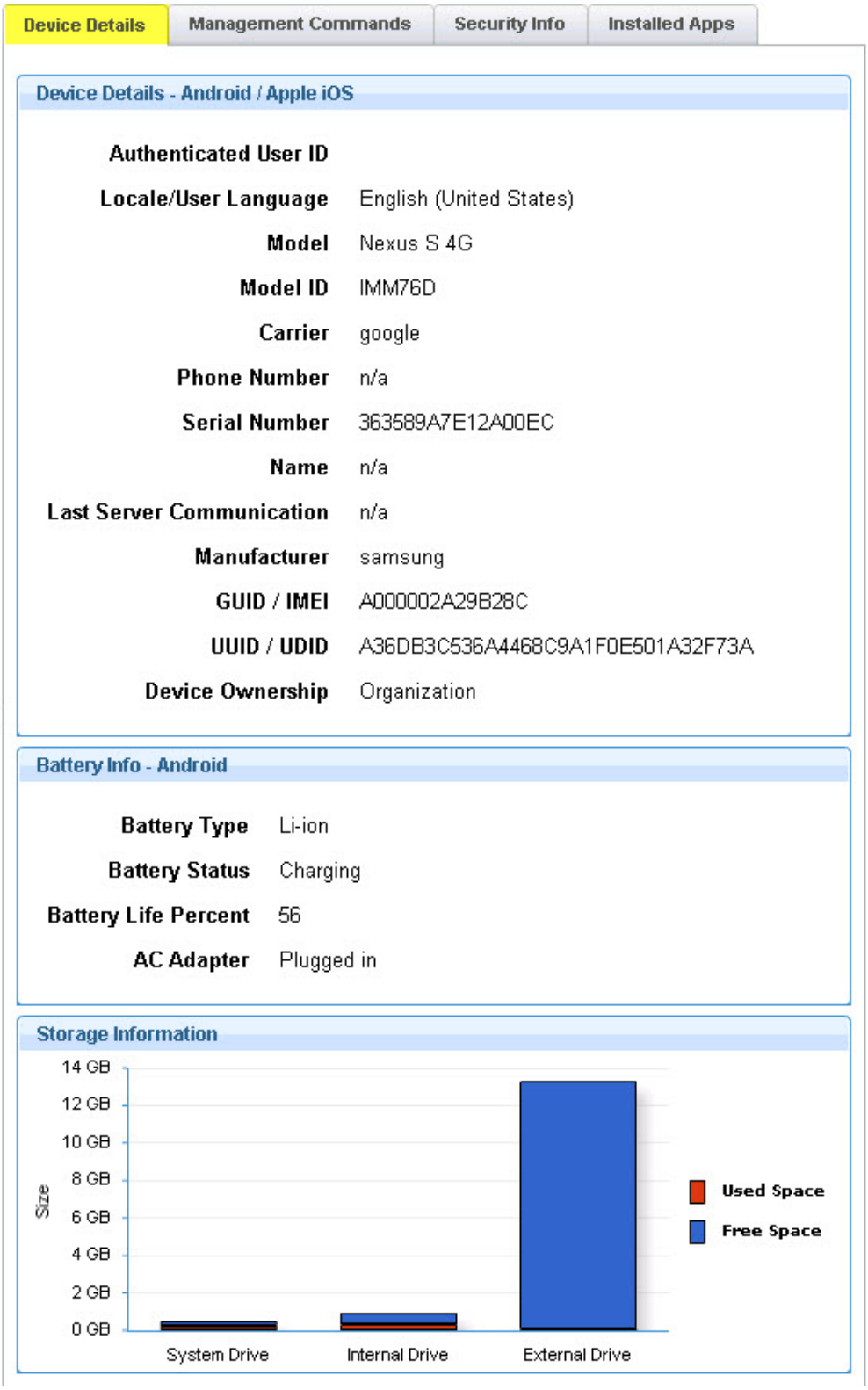
The device list view displays device information by device name, user name, operating system, and data source. Click any heading in the list view to sort columns and change the organization of the list. If you maintain many devices in your deployment, use the search box to quickly locate a device in the list.

To access the Device Detail view, click on any line in the device list view to display the accompanying detail view for that particular device.

The device detail view displays summary information about a device on the left side of the window. Click the *View Location* link to see the device location on Google Maps.



Content on the right side of this windows is organized by tabs: Device Details, Management Commands, Security Info, and Installed Apps. The datasource to which a device is connected determines the type of content that appears in the tabbed section of the detail view.



Click through each tab to view different types of information about each device.

How to Wipe a Device

From the Single Device View dashboard, you can wipe the internal storage data or specific application data on a device in your deployment.

To access the wipe feature, open the Single Device View dashboard and select a device from the Device List. Click the Management Commands tab. *Device Wipe* will remove internal storage data. Select Device Wipe and click Apply. In the Take Action dialog, select the device and click *OK* to deploy the action.

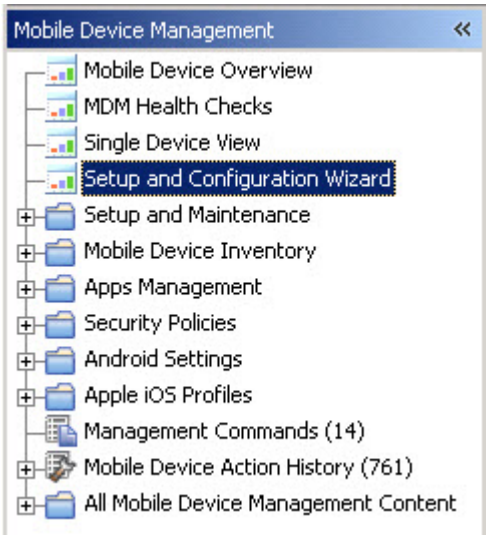
For devices managed under the iOS Management Extender, you can also "deprovision" a device, which means that the device is no longer managed by the extender.

For devices managed by the Lotus Traveler Management Extender, you can also selectively wipe data. Click *Apply* next to *Selectively Wipe Lotus Traveler Data*.

To access other management commands, see the *Management Commands* section in this document.

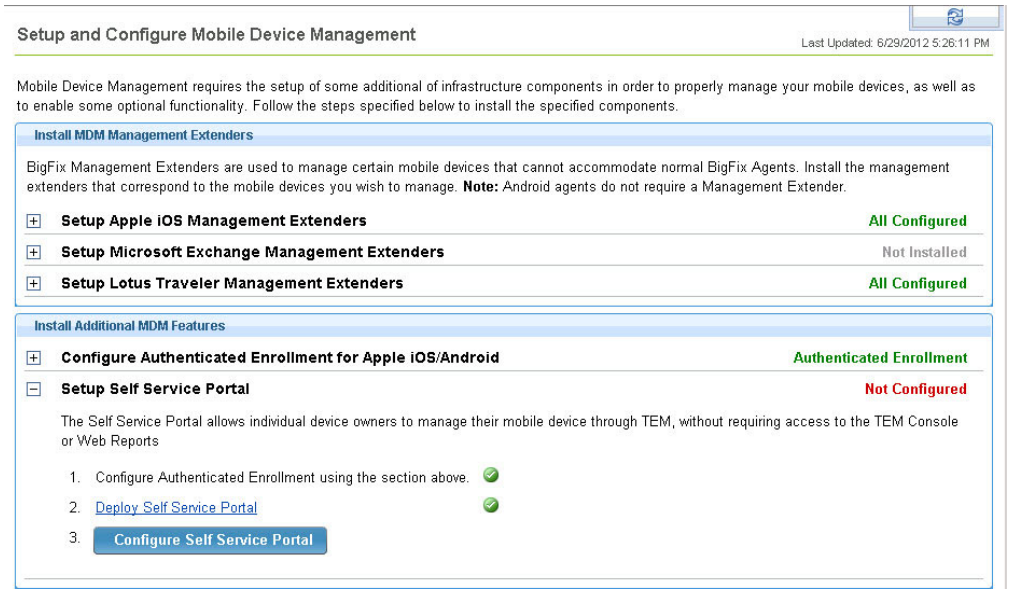
Setup and Configuration Wizard

The Setup and Configuration Wizard, located in at the top of the MDM navigation tree, configures your management extenders to enable them to connect to servers.



Click the plus sign beside each extender to open the menu of configuration options.

Click *Configure*. This will open the Configure Extender window for Apple iOS, Lotus Traveler, or Microsoft Exchange. In the Configure Extender window, you can set configuration parameters for each extender.



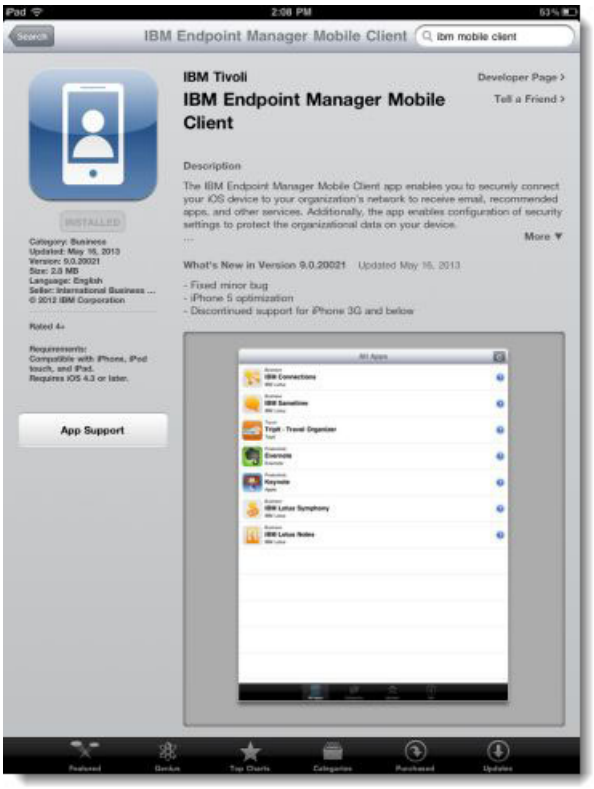
You can also install additional MDM features, such as Authenticated Enrolllment and Self Service Portal. For more detailed information, see the MDM Setup Guide.

IBM Mobile Client for Apple iOS

The IBM Mobile Client for Apple iOS is an app available from the Apple App Store that communicates with IBM Endpoint Manager.

Install the IBM Mobile Client for Apple iOS on an iOS device by opening the App Store app and searching for “IBM Mobile Client”.

Note: The IBM Mobile Client for Apple iOS can be referred to as the "mobile client”.



Enrolling a Device

The first step in managing a mobile device is to enroll the device to your IBM Endpoint Manager deployment.

After you install and open the mobile client on an iOS device, you are prompted for a server URL. This URL is generated during the configuration of an Enrollment and Apple iOS Management Extender. Request the URL from your IBM Endpoint Manager administrator.

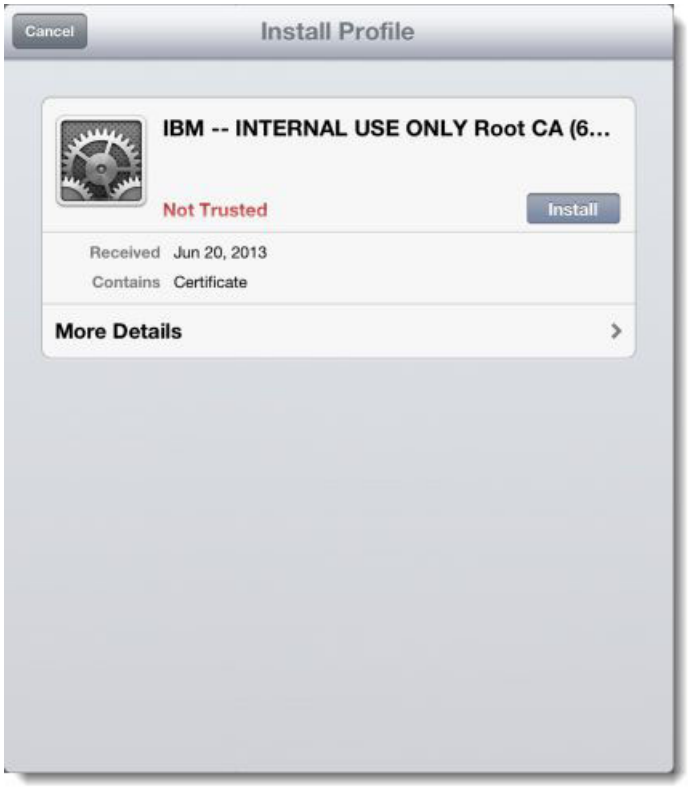
After you enter the URL, click **Start** to begin enrolling the device.

Installing a Certificate

If the device has not previously communicated with your IBM Endpoint Manager deployment, you are prompted to install a certificate.

If the following menu is not displayed, continue to “Installing a Profile” on page 14.

Click **Go**. The device browser opens momentarily and is quickly replaced by a prompt to install a profile. Click **Install** to proceed and follow the prompts to install the profile. After you install the profile, the device returns to the browser. Click **continue enrollment** to return to the IBM Mobile Client.



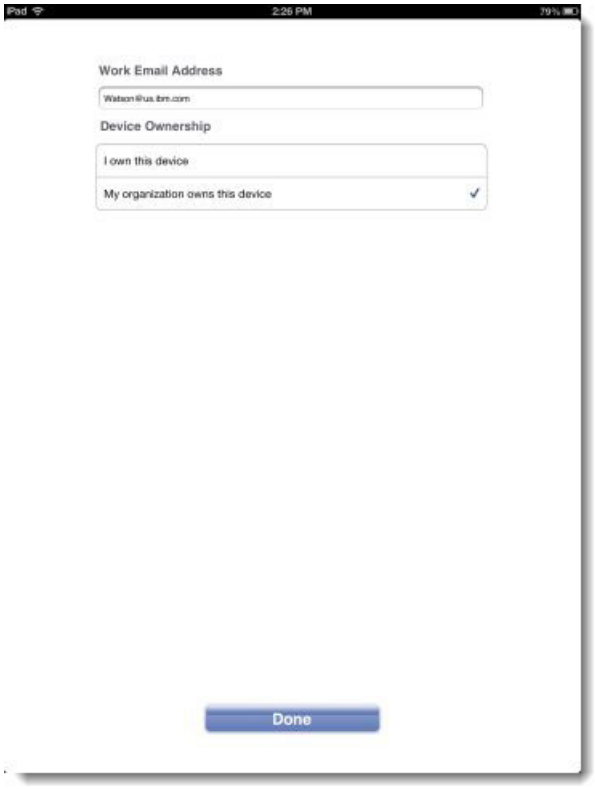
With the appropriate certificate installed on the device, the device can communicate with your deployment. Click **Start** to begin the enrollment process.

Installing a Profile

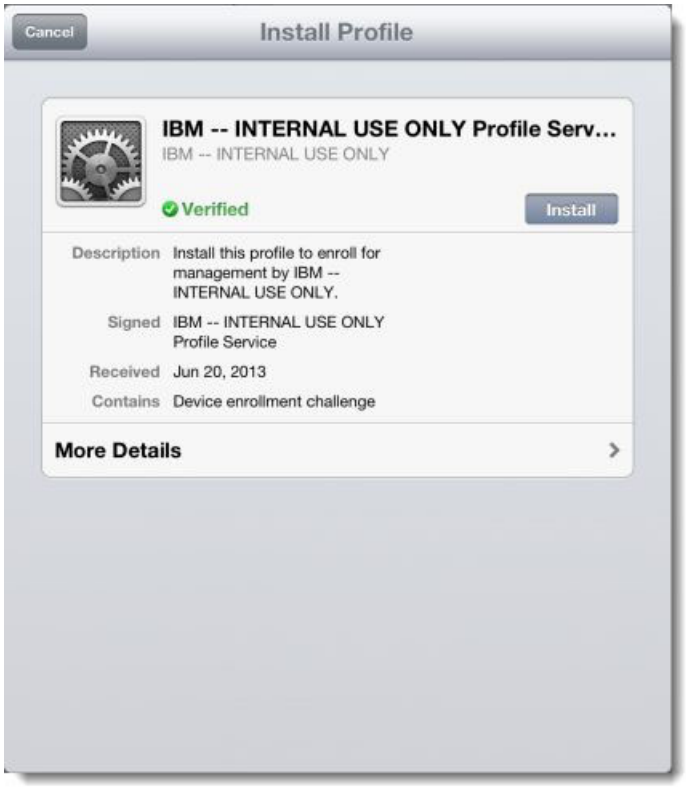
After you enter the server URL and communication with your deployment has been established, the next step in enrollment is the installation of an IBM Endpoint Manager profile.

To finish enrolling your device, perform the following steps:

1. Enter your email address and indicated whether you or your company owns the device.



2. Click **Done**. The device browser opens temporarily and is quickly replaced by a prompt to install a profile on the device.



3. Follow the displayed directions to install the profile. When this process is completed, the device browser displays an enrollment webpage.

4. Click **Return to the app** to return to the IBM Mobile Client.

After successfully enrolling the device, the mobile client is available for use.

Mobile Client Layout

The IBM Mobile Client for Apple iOS consists of several panels of information.

The mobile client contains three tabs that are located at the bottom of the panel:

- **Apps**
- **Messages**
- **Info**

A refresh button is available in the upper-right corner of the app. Click **Refresh** to have the device communicate with your IBM Endpoint Manager deployment.

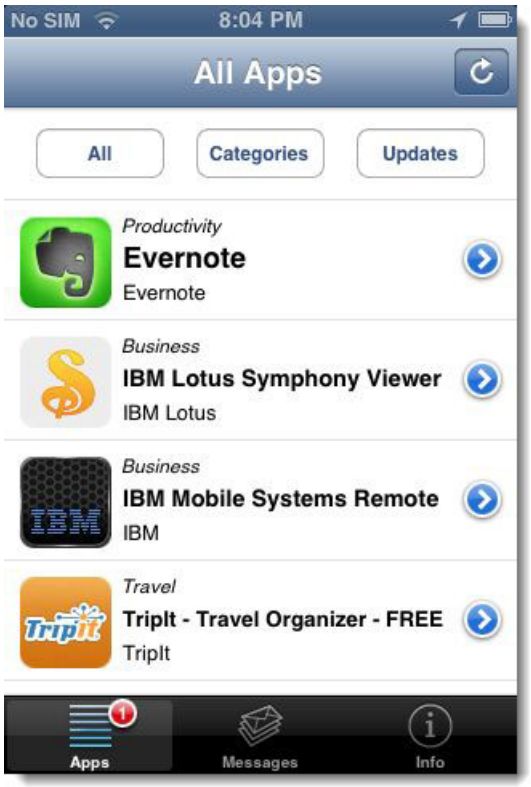
Apps Tab

The Apps tab displays any apps that are recommended by your administrator. Sort the apps by using the buttons at the top of the mobile client.

All Display all recommended apps.

Categories
Sort the recommended apps by their categories as defined by the app developer.

Updates
Display only recommended apps that must be updated to a newer version.

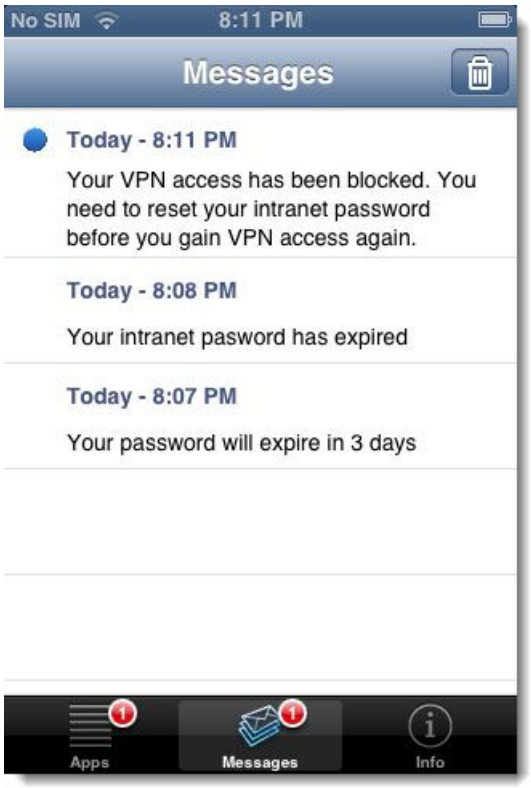


Click an app to display more information and allow the app to be installed or updated. A red badge displays how many recommended apps can be updated.

Messages Tab

The Messages tab displays all messages that are sent by your administrator.

A red badge on the Messages tab displays the number of unread messages. This badge is the same badge that is displayed on the app's icon on the iOS dashboard.



Info Tab

The Info tab lists important information that is related to the device.

Server The enrollment server URL for the device.

Work Email
Lists and enables editing of the email address that is associated with the device.

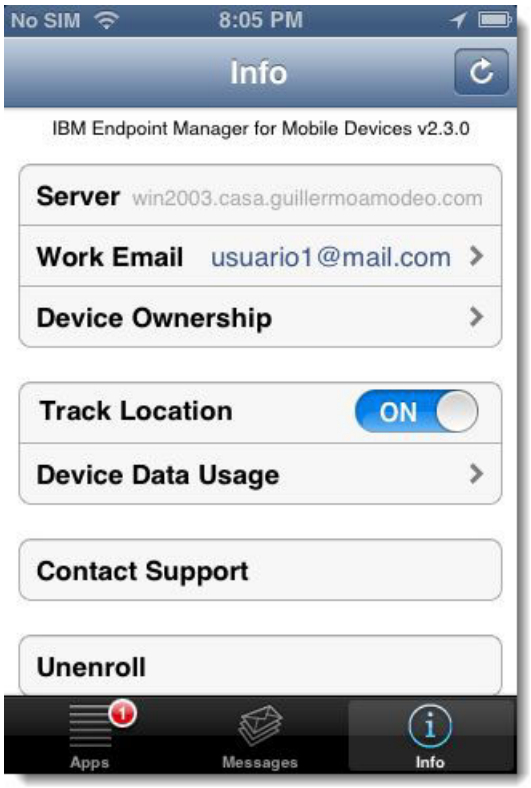
Device Ownership
Allows the designated ownership of the device to be changed.

Track Location
Toggles location tracking on or off. For more information about **Track Location**, see INSERT LINK.

Device Data Usage
This entry is visibly only if **Track Location** is turned on. The reporting of this data to the mobile client is tied to the reporting of location data. This data is the same data that is collected by iOS as reported in the iOS settings.

Contact Support
Sends an email to your IBM Endpoint Manager administrator. If the administrator did not set up this feature, this button is not displayed.

Unenroll
Unenrolls this device from the IBM Endpoint Manager for Mobile Devices deployment.



Track Location

The **Track Location** toggle in the IBM Mobile Client for Apple iOS allows device users to enable or disable the ability of administrators to track the location of a device.

The following conditions must be met for a device's location to be tracked:

- The IBM Endpoint Manager administrator must enable location tracking.
- The device user must enable Location Services in the iOS settings.
- The device user must turn on the **Track Location** switch within the IBM Mobile Client.

Because of the way iOS handles location services, the location data that is sent from iOS devices is limited. Location data is collected by the IBM Mobile Client only under the following circumstances:

- The IBM Mobile Client is open and is the currently displayed app.
- Another app that collects location data is open, such as a mapping app. Location data is passed to the IBM Mobile Client.
- The device operating system determines that a significant change in location occurs. This behavior is defined by Apple and is not fully understood. Changing to a new WiFi network might instigate this location update, for example.

When one of the preceding events occurs, location information is passed to the IBM Mobile Client. That information can then be communicated to the IBM Endpoint Manager for Mobile Devices deployment. This communication occurs only if the administrator set up location tracking, and it occurs at an interval that is defined by the administrator. In addition, this information is communicated only if the device has moved at least 100 meters.

Note: iOS displays a small arrow in the upper-right corner of the display when location services are being used. When the **Track Location** switch is turned off in the IBM Mobile Client, it might take several seconds for this arrow to disappear.

Android Agent Setup

To set up your Android agent, use the following steps. You will need an internet-facing relay for this process.

1. Launch the Android market app on your device and search for *IBM Endpoint Manager for Mobile Devices.* Select the app and click *download.* Click *Accept and Download.*
2. After the application is installed, select *Open.*
3. *Click Activate.*
4. Enter the TEM Server address (or internet-facing relay) that you obtained from your administrator and enter your work email address. Select one of the two available options to indicate if the device is personal or enterprise. Click *Enroll.*
5. If the connection is successful, the message *Successful set up of the Mobile Client* will display briefly, and service status will indicate that the service is running.

Note: To uninstall the TEM Android agent, unselect the Device Administrator option under Settings/Location and Security on the device.

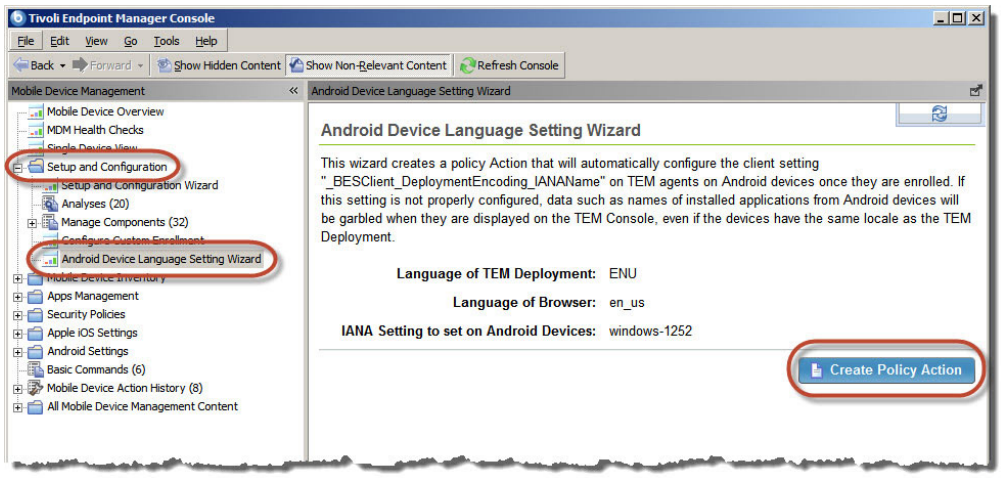
Note: To control your device location privacy, deploy the *Disable GPS Location Properties* Fixlet under Mobile Device Inventory/Data Configuration.

Android Device Language Settings (IANA)

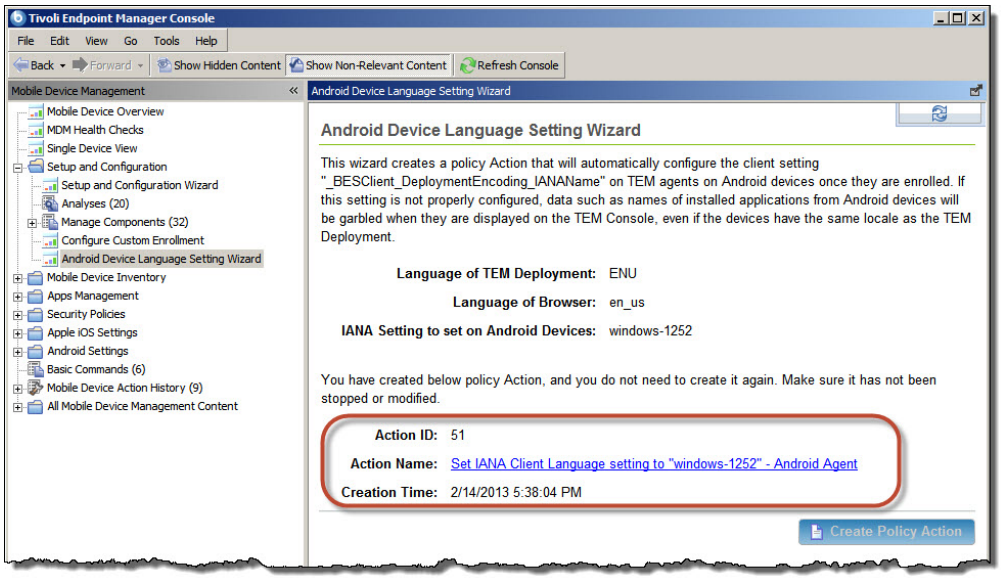
The IBM Mobile Client App has its own language settings, which must be in sync with the language used for IBM Endpoint Manager. For example, if IBM Endpoint Manager is installed in the English language, the IBM Mobile Client must also be set to the English language. If not, the language characters that are sent by the Endpoint Manager might not display correctly on the Android device. The enrollment process does not set the IANA language of the IBM Mobile Client App to match IBM Endpoint Manager automatically.

Synchronize the IANA language setting for the IBM Mobile Client App to the console by creating a policy action:

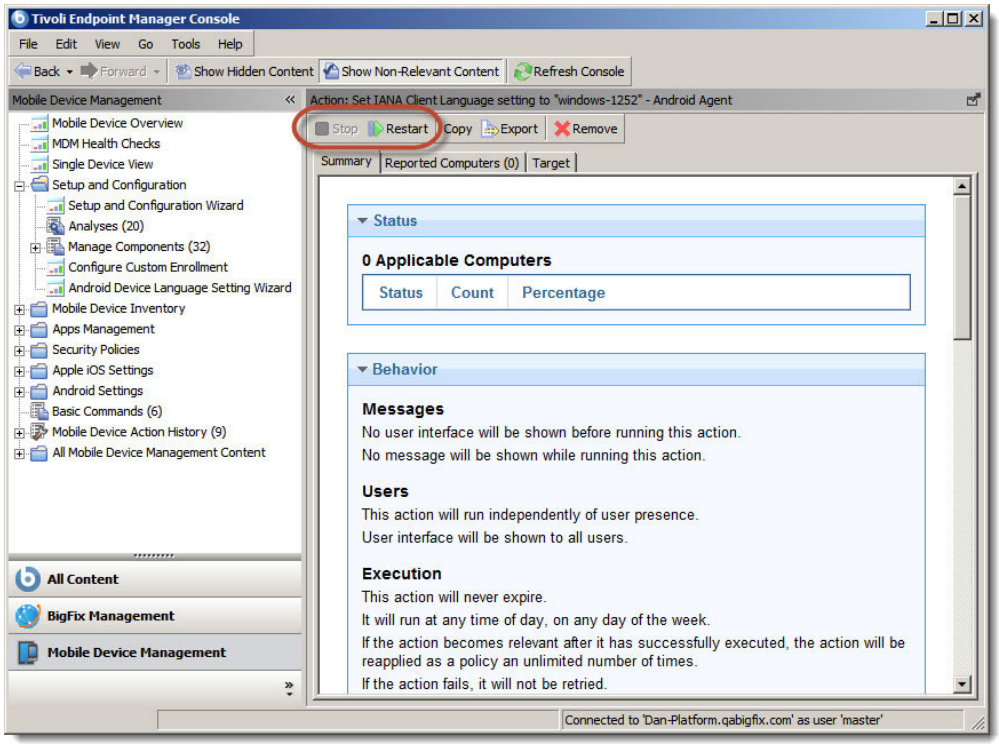
1. From the Mobile Device Management site on the left of the console, select **Setup and Configuration > Android Device Language Setting Wizard**. On the displayed page, you can see the three character language code that the Endpoint Manager is set to. The matching IANA language setting is also displayed.
2. Click **Create Policy Action**



After the policy action is created, the associated Action ID is listed. After the policy runs, the appropriate IANA setting is sent to all managed Android devices.



If the IBM Mobile Client App running on an Android device continues to display unrecognizable characters, you must wait for the polling interval. It is also possible that the policy action is stopped. Check whether the policy action is running, by clicking the **Action Name** link. In the displayed window, click **Restart** if it is available. If the button cannot be clicked, the policy action is already running.

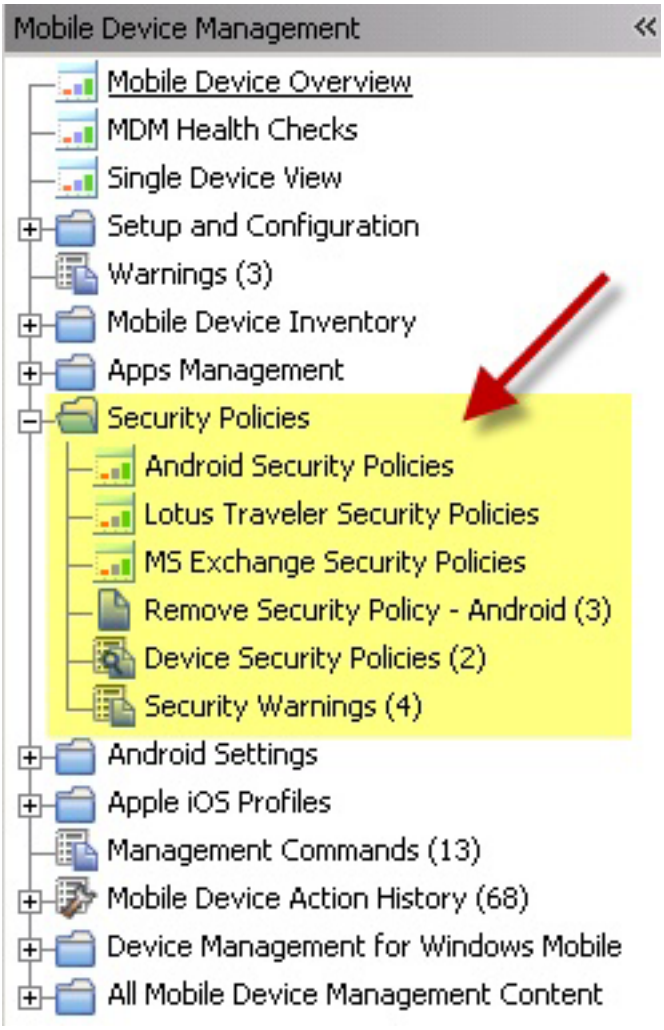


Managing Mobile Devices

With the MDM application, you can manage devices, manage apps on devices and in your deployment, set security policies, and set profile configurations. The following sections describe each feature.

Security Policies

The Security Policies node in the navigation tree includes dashboards for Android, Lotus Traveler, and MS Exchange security policies, as well as tasks for removing Android security policies, device security policies, and security warnings. Use Security Policies to set up password authentication credentials for each device and device type in your deployment.



Android Security Policies

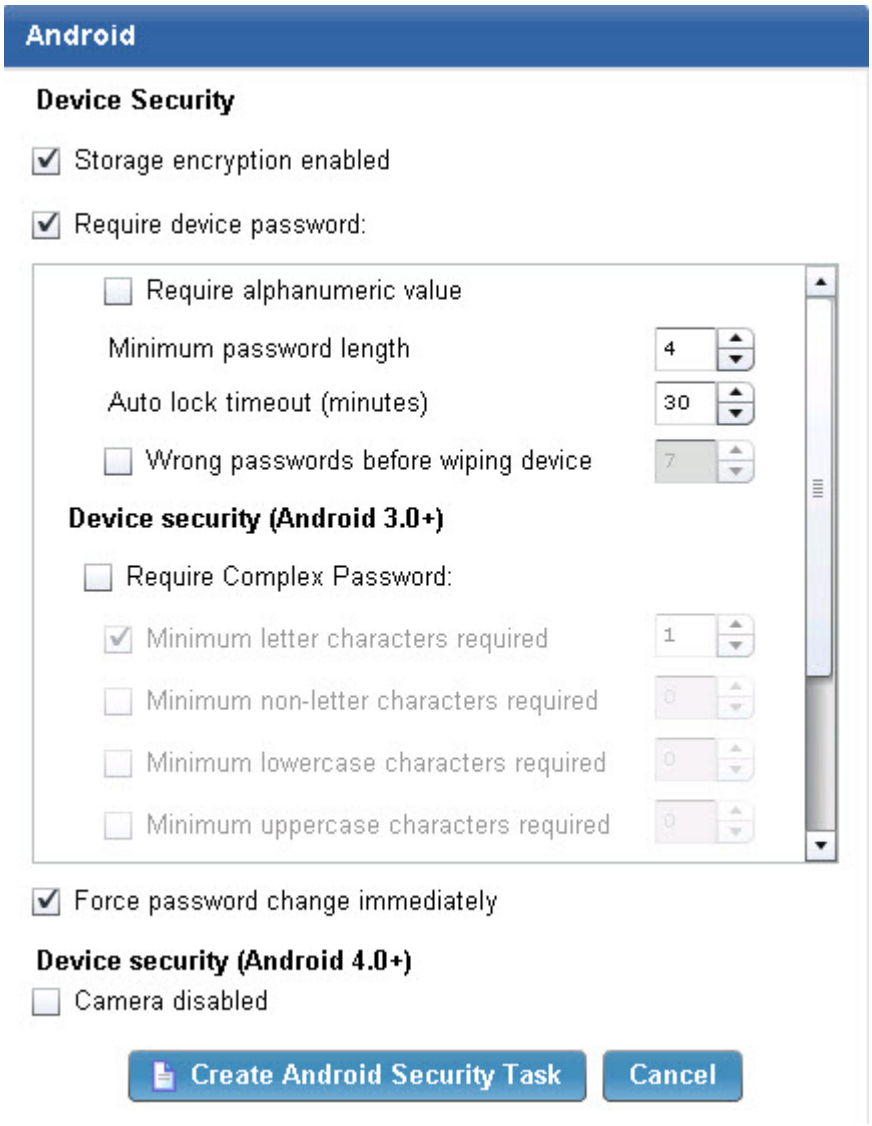
To manage the security settings on an Android device, click the Android Security Policies dashboard. Click *Create New Policy*.

In the Android Device Security window, you can set parameters for your device password, enable storage encryption, auto lock period, and the number of allowable wrong passwords before wiping the device. You can also set security

settings for Android 3.0 or 4.0 and disable the camera function. Click the *Force Password Change Immediately* check box to prompt the user for an immediate password change.

Note: This password prompt can be disruptive for the user on the mobile device.

After setting parameters, click *Create Android Security Task*.

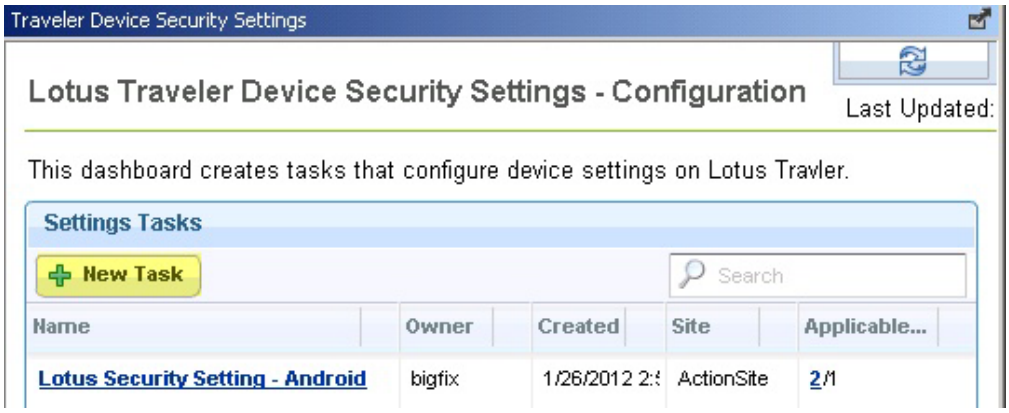


Deploy the created tasks to devices to configure their settings.

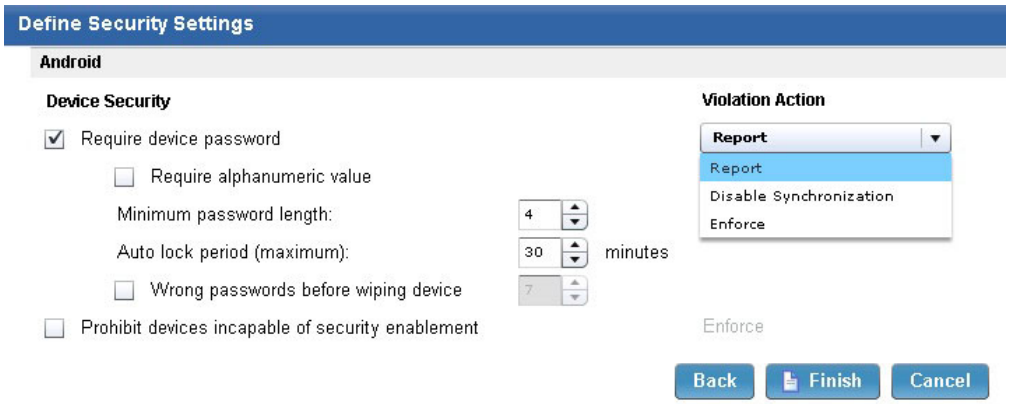
Note: To encrypt your Android device, click the Storage encryption enabled box in the Android Device Security Settings dashboard.

Lotus Traveler Security Policies

The Lotus Traveler Security Settings dashboard enables you to manage passwords, storage card encryption, prohibit camera, and prohibit devices incapable of security enablement. Click *New Task*.



Select a device type, and click *Next*. Select device security settings and click *Finish* to create a Lotus Traveler Security settings task.



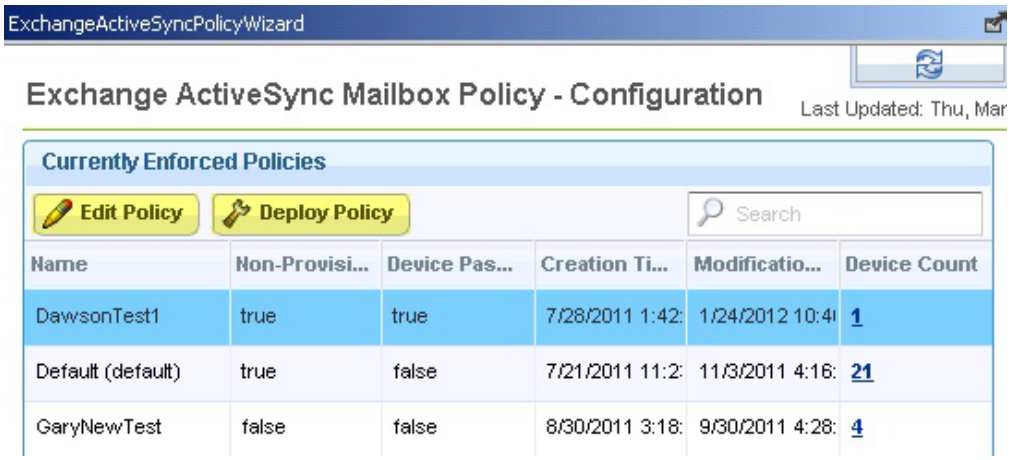
Deploy this task to a Traveler server to enforce a security policy for devices.

Note: This dashboard sets the Lotus Traveler policies on the Lotus server, rather than on the device itself. It will set the policy across all devices connected to this server.

Microsoft Exchange Security Policies

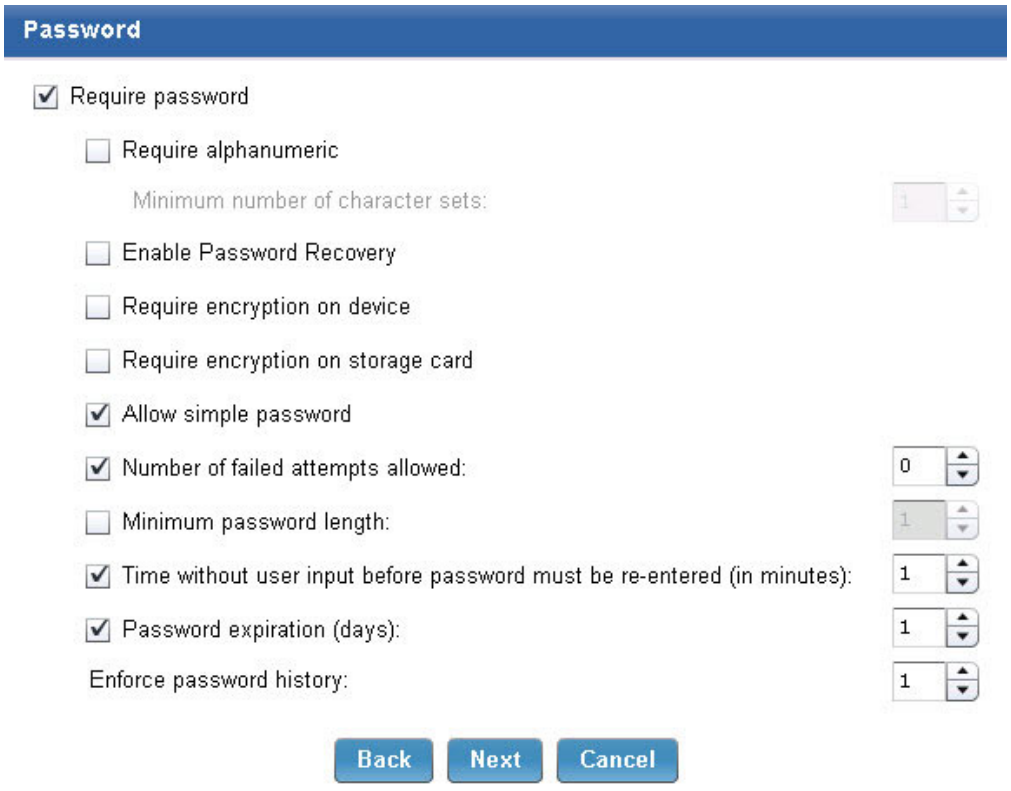
Use the *Exchange ActiveSync Mailbox Policy - Configuration* dashboard to select, display, and set parameters for how your device will handle email. The dashboard pulls existing ActiveSync policies from your exchange server.

You can edit an existing policy by selecting a policy in the Currently Enforced Policies list and clicking *Edit Policy*.



Use the dialogs to configure passwords, sync settings, device parameters, device applications, and other settings for your policy. When you have set parameters, click *Create Policy* to send an action to update the Exchange server.

After you have configured policies, you can deploy them to devices. Click *Deploy Policy* to access the Take Action Dialog. The policy will be applied to the targeted devices after the action completes.

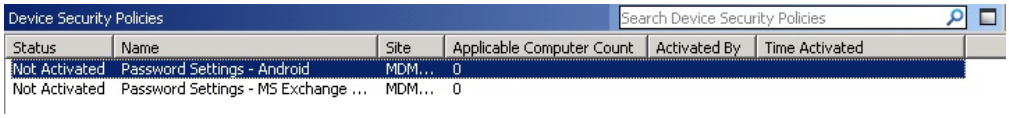


Note: This wizard will only assign or modify Exchange ActiveSync mailbox policies. You cannot create a new mailbox policy using this Wizard.

Note: When you assign a policy to a device, it will change the policy for all devices owned by that Exchange mailbox user. For example, if a user has an iPad and an iPhone, changing the iPhone policy will also change the iPad policy.

Device Security Policies

Click *Device Security Policies* under Security Policies in the navigation tree to activate analyses for managing password properties on your mobile devices.



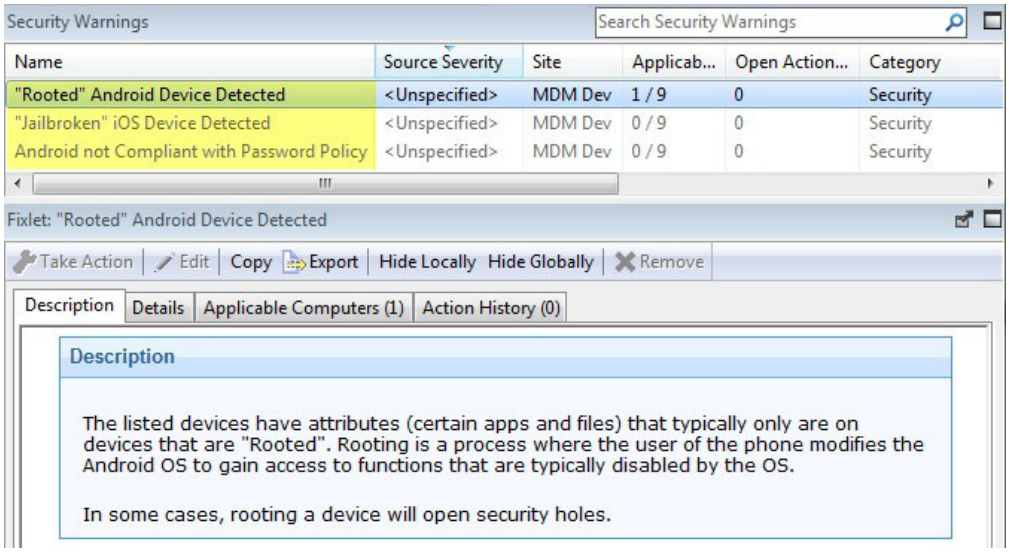
These properties include:

- Password Enabled
- Password Length
- Require Alphanumeric Password
- Inactivity Timeout
- Wrong Attempts Before Wipe
-
-

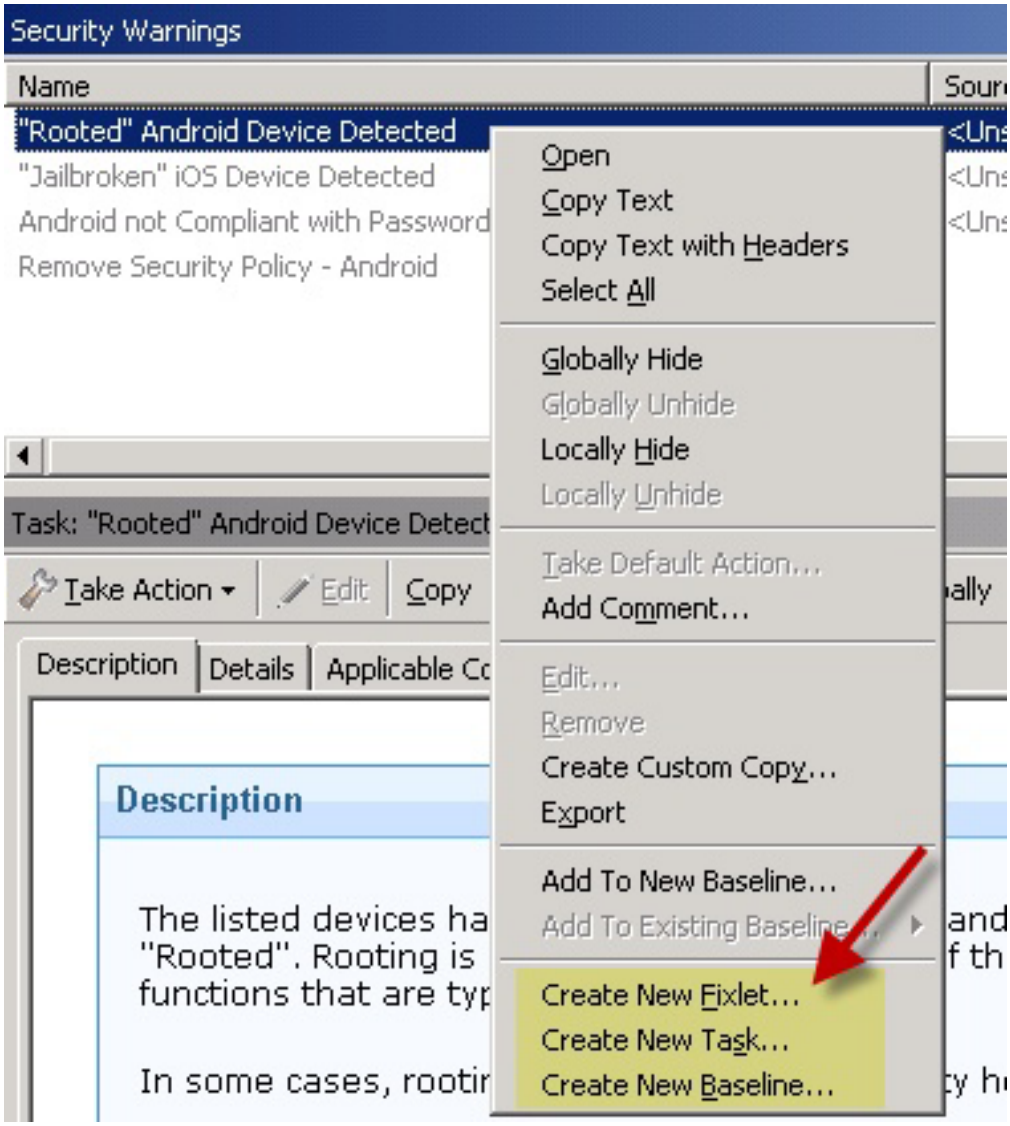
Click the link in the *Actions* box to activate or deactivate analyses.

Security Warnings

The MDM application displays security warnings in the navigation tree about the devices in your deployment. These include rooted devices, devices that have been jailbroken, or devices that are not compliant with your established password policies.

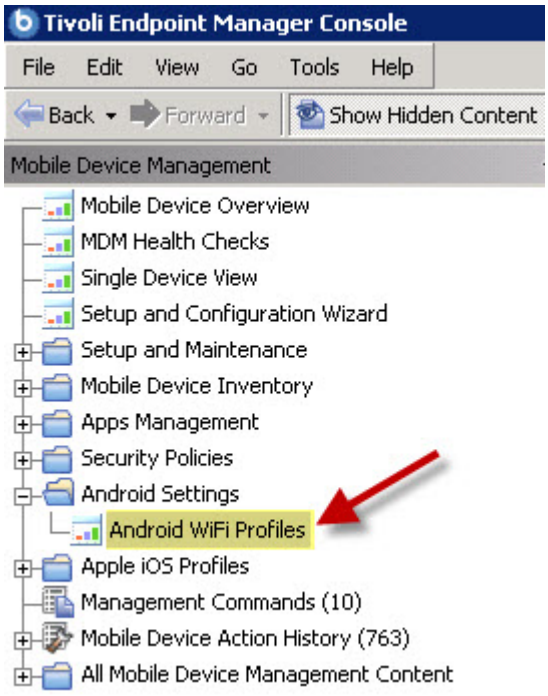


After you select the warning in the list panel, you can create a custom Fixlet, task or baseline for this warning through the right-click menu.



Android Settings

The *Android Settings* node in the navigation tree contains an Android WiFi Profiles dashboard that allows you to define WiFi access profiles for your devices.



The Android WiFi Profiles dashboard enables you to create WiFi profile actions for how your devices connect with wireless access points. Click *Create New Policy,* enter a mandatory SSID, and then click *Create Android WiFi Task.* The new profile is created on the targeted device.

Apple iOS Profiles

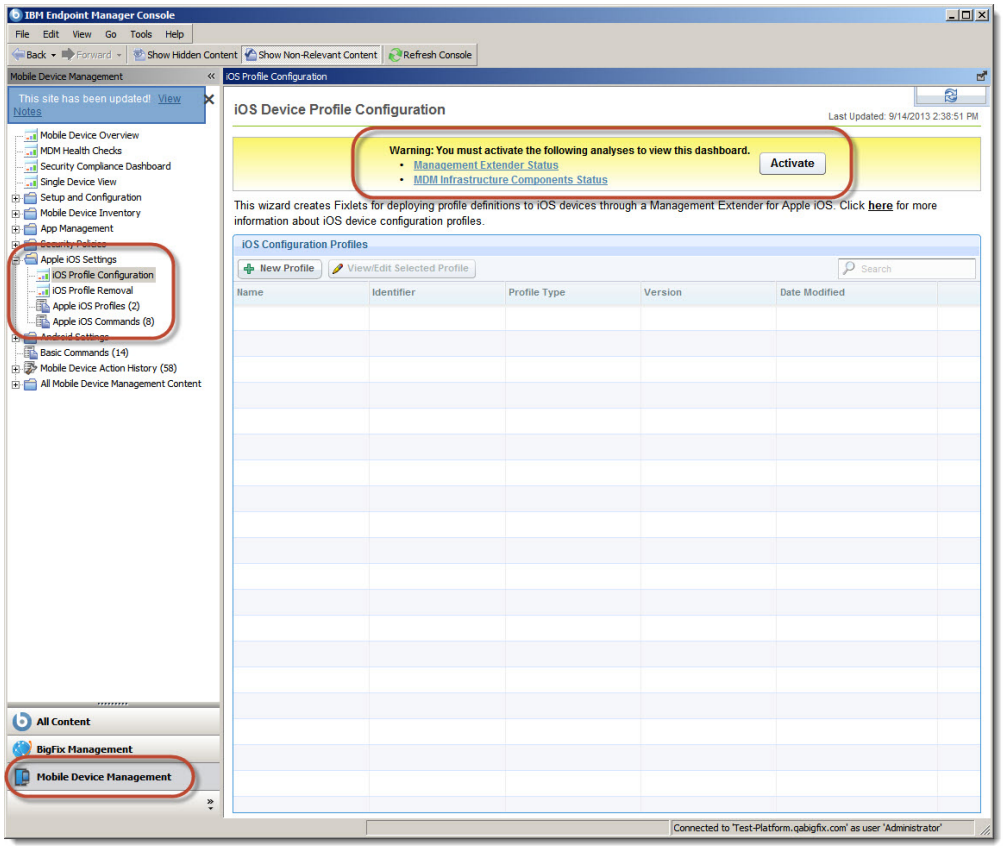
Apple iOS devices can be assigned profiles that manage a wide range of enterprise features.

Apple Inc. supports the creation and application of iOS profiles though its Apple Configurator tool. The ability to create, deploy, and remove profiles to and from iOS devices that are managed by IBM Endpoint Manager is implemented in the **iOS Profile Configuration** dashboard.

More information about Apple Configurator and iOS profiles can be found at http://www.apple.com/support/iphone/enterprise/.

The **iOS Profile Configurator** dashboard can be found by navigating to **Mobile Device Management > Apple iOS Settings > iOS Profile Configuration**.

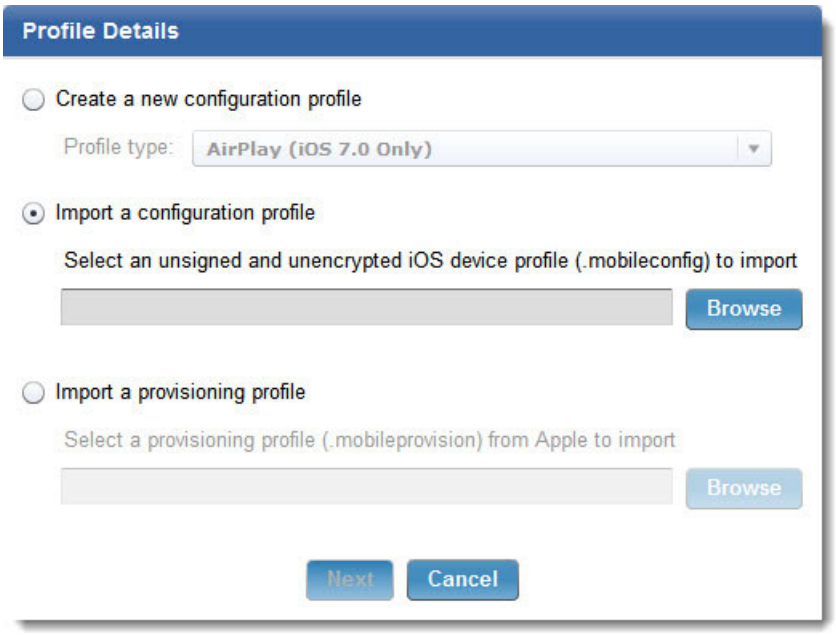
Note: You might be required to activate analyses for the dashboard to function. If so, a yellow warning banner is displayed at the top of the dashboard. Click **Activate** to turn on the listed analyses.



Import an iOS Profile

An existing configuration profile or provisioning profile can be imported. After it is imported, the profile can be edited and assigned to devices.

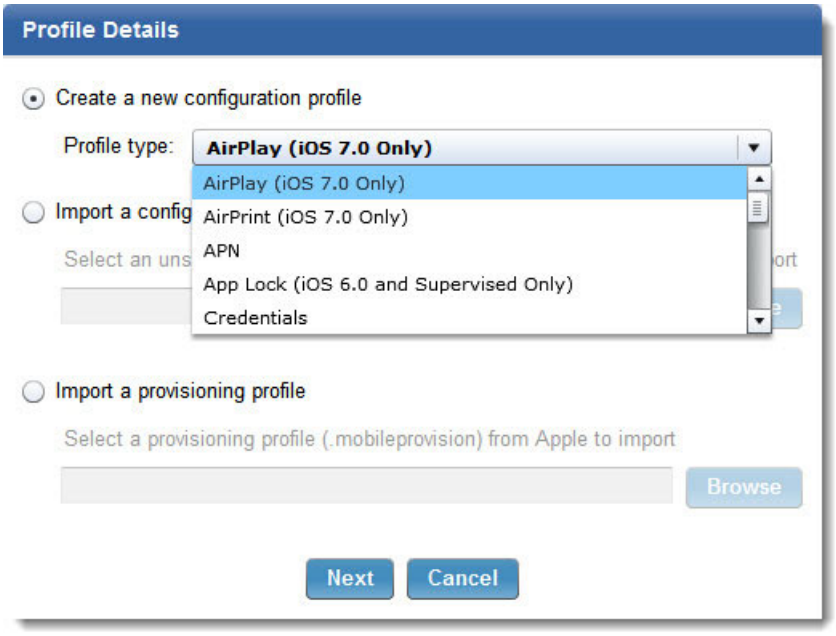
Click **New Profile**. The **Profile Details** window is displayed. Select the appropriate radio button and navigate to the existing profile. Configuration profiles must have a `.mobileconfig` extension and they must be both unsigned and unencrypted. Provisioning profiles must have a `.mobileprovision` extension and must be unencrypted.



Create or Edit an iOS Configuration Profile

Configuration profiles can be created within the iOS Profile Configuration dashboard. Existing configuration profiles can be edited.

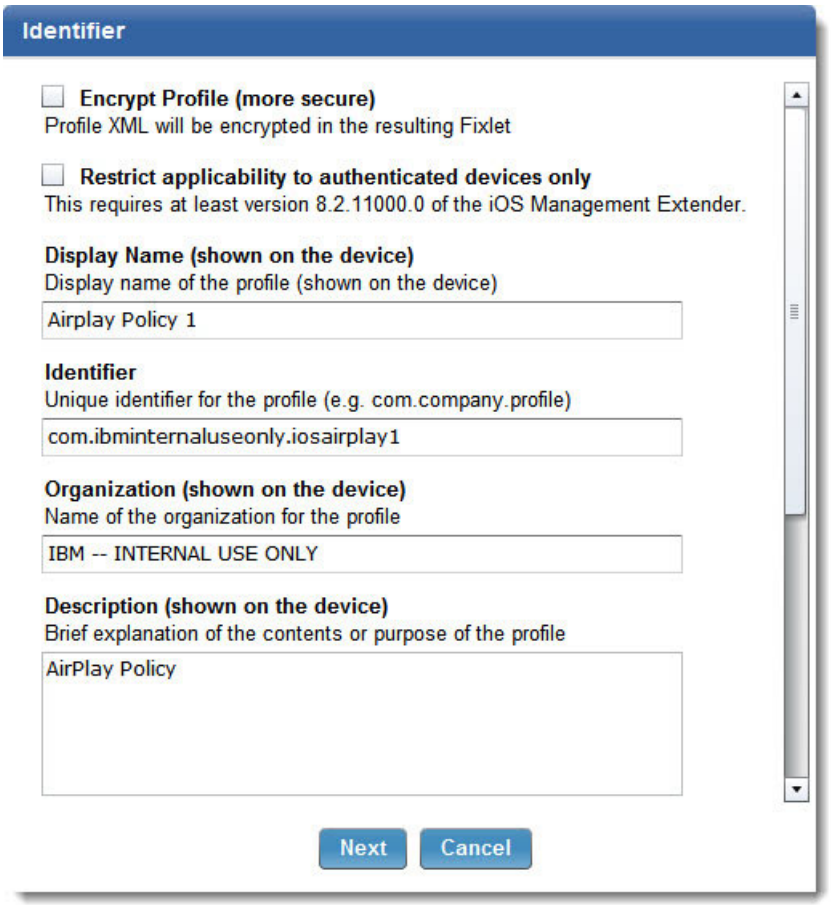
To create a new iOS Profile, click **New Profile** and select the profile type from the menu. Alternatively, you can edit an existing profile by selecting it from the list and clicking **View/Edit Selected Profile**. For information on the various profile types, see "iOS Profile Types" on page 31.



Regardless of the profile type that is selected, the **Identifier** window is displayed. The following options must be configured before you click **Next** to choose the profile specific settings for each profile:

- The profile can be encrypted for increased security.

- The profile can be restricted to apply to authenticated devices only.
- A name for the profile is defined. This name is displayed on the device when the profile is active on a device.
- A unique identifier must be assigned to the profile. A recommended identifier is entered by default.
- Organization information can be defined. This information is displayed on the device when the profile is active on a device.
- A description can be defined to help document the profile.
- A message can be defined that displays on iOS 6.0+ devices when the profile is installed.
- Control of the profile can be given to the device user always, or by a password that is defined here. Alternatively, control can be denied.
- The profile can be set to be removed automatically on the date that is specified, or after a number of days that are defined here.



Note: Some profile types require target devices to have iOS 6.0+ or iOS 7.0+. In addition, some profiles require supervision mode to be on. These restrictions are delineated in the profiles name.

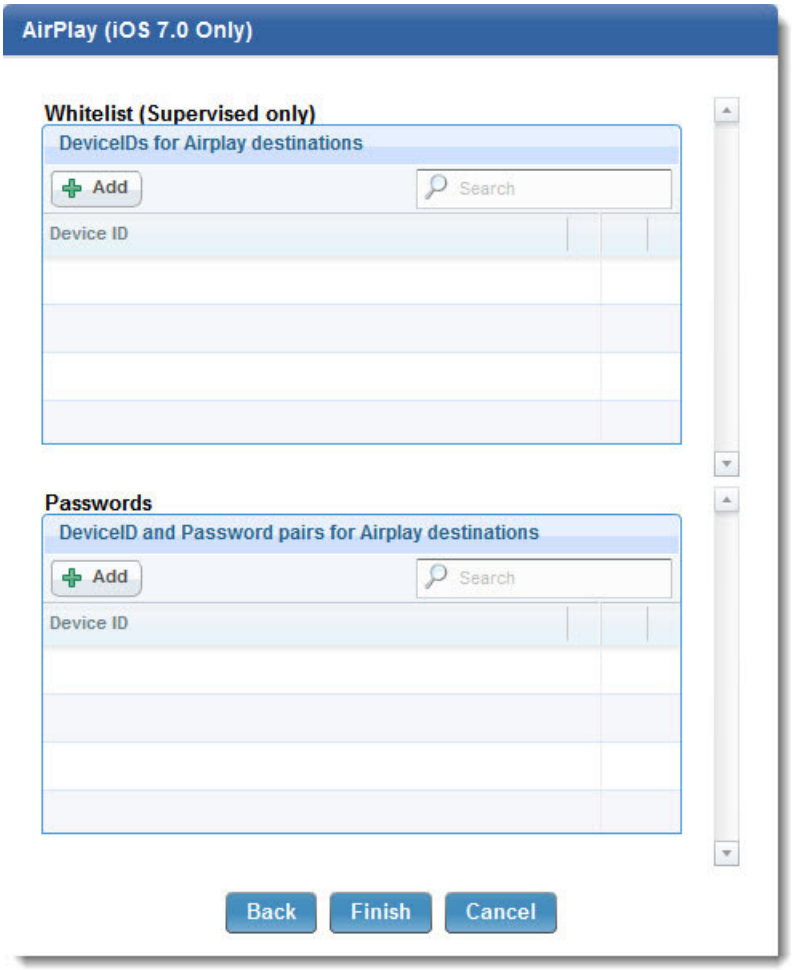
iOS Profile Types:

The following profiles can be created or edited.

The iOS profiles that are created in IBM Endpoint Manager for Mobile Device Management are implementations of profiles that are created and maintained by Apple Inc. For detailed information on profile settings, see http://www.apple.com/support/iphone/enterprise/

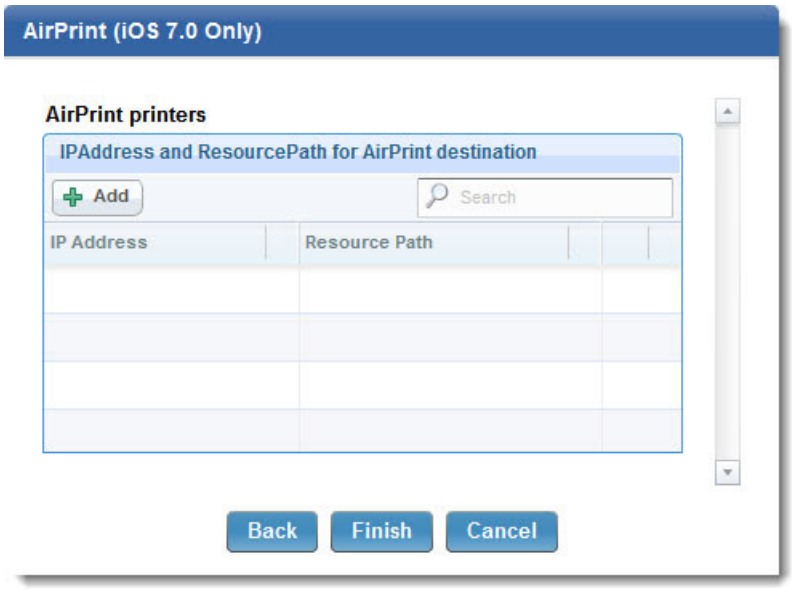
AirPlay (iOS 7.0+)

This profile allows the definition of paired AirPlay devices and associated passwords. In addition, a device whitelist can be created.

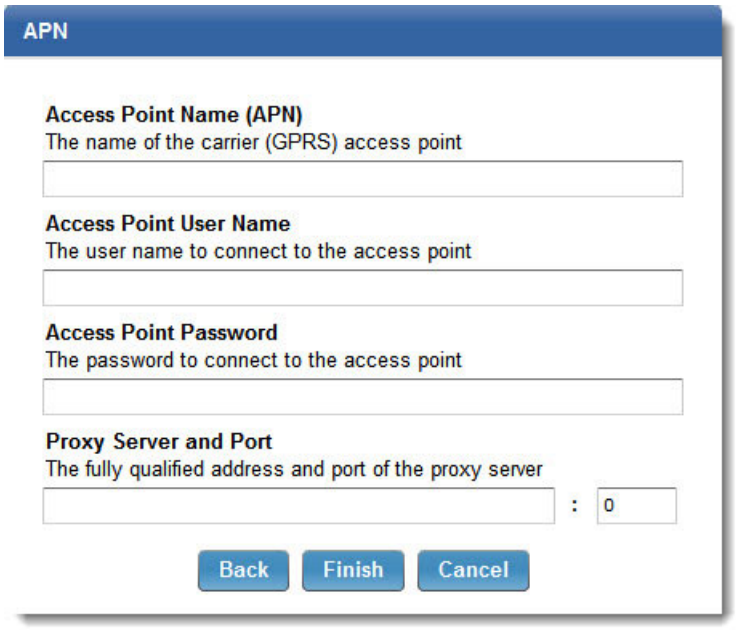


AirPrint (iOS 7.0+)

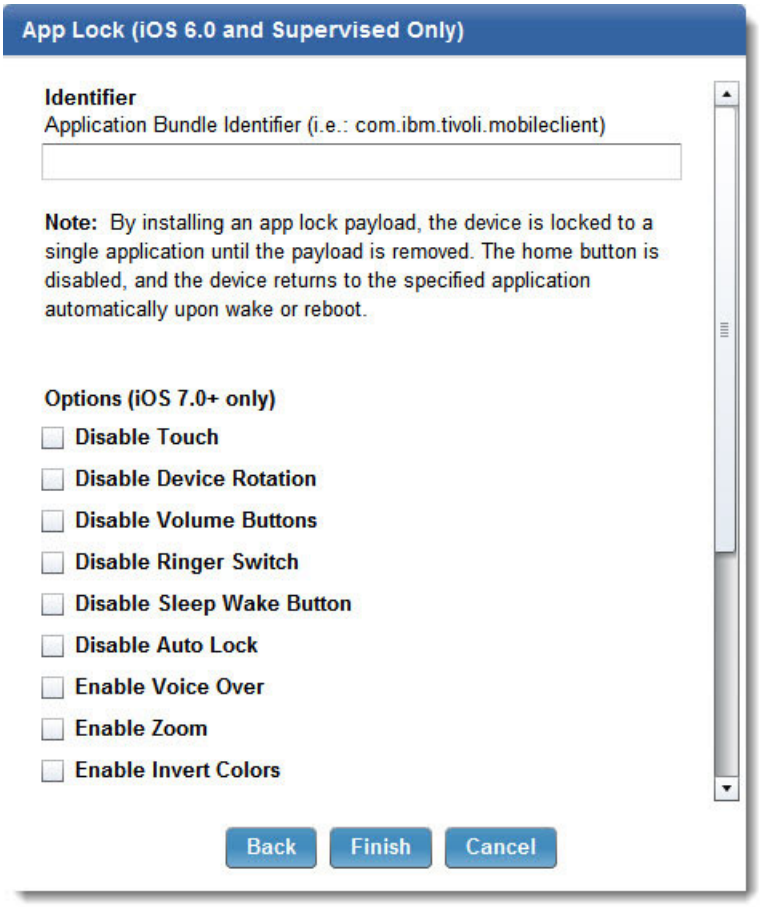
This profile allows the definition of IP addresses and associated resource paths for AirPrint printers.



APN APN settings can be used to change the proxy settings on your network and the Access Point Name (APN) on your devices. These settings define how a device connects to a network. In iOS 7 and later, the APN payload is deprecated in favor of the Cellular payload.

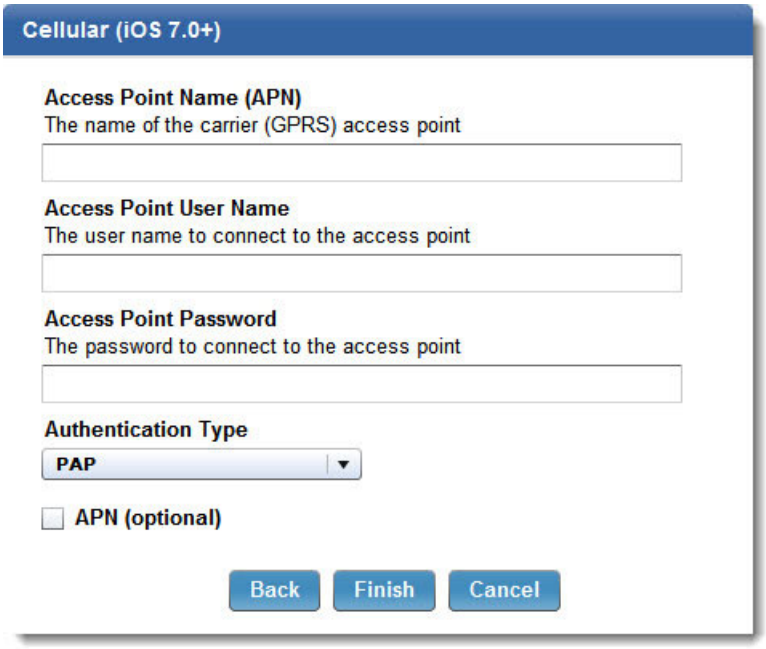


App Lock (iOS 6.0+, Supervised)
An App Lock locks a device to a single app. Enter the application bundle identifier and on devices with iOS 7.0+, define which functions are enabled or disabled during the App Lock.



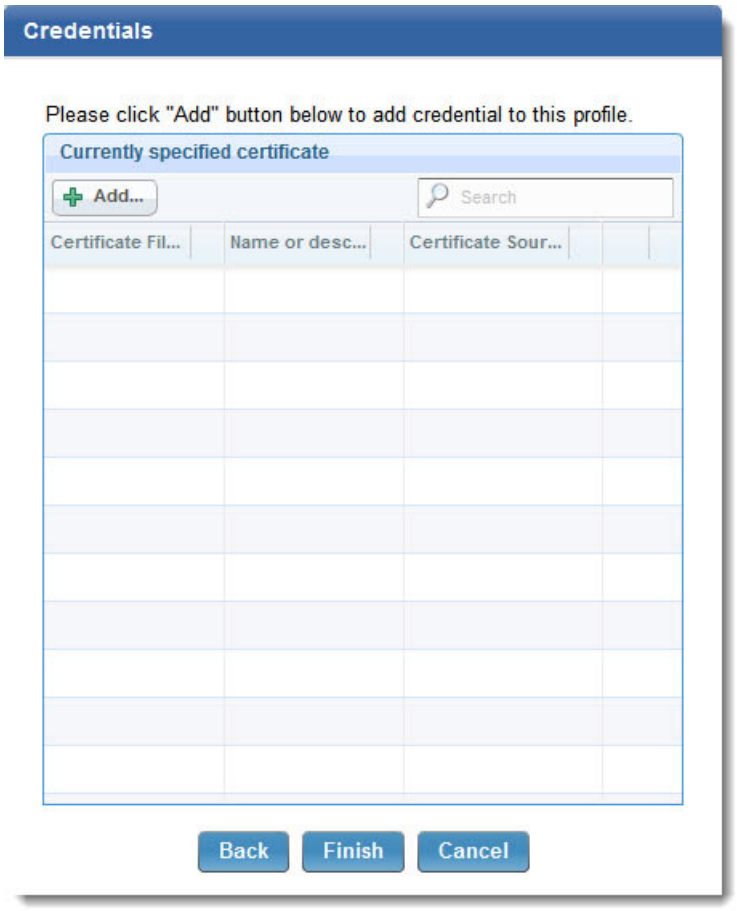
Cellular (iOS 7.0+)

A Cellular profile configures cellular network settings on devices. In iOS 7 and later, the APN profile is deprecated in favor of the Cellular profile.

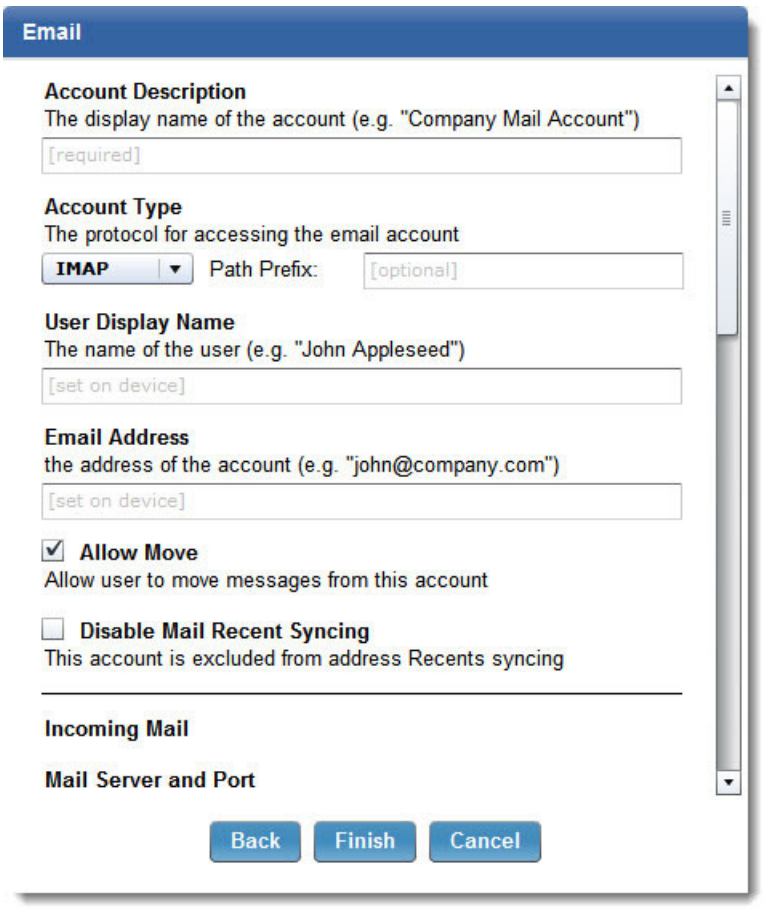


Credentials

This profile allows certificates to be installed on a device. Define the certificate type and designate the import parameters or select a specific certificate file.

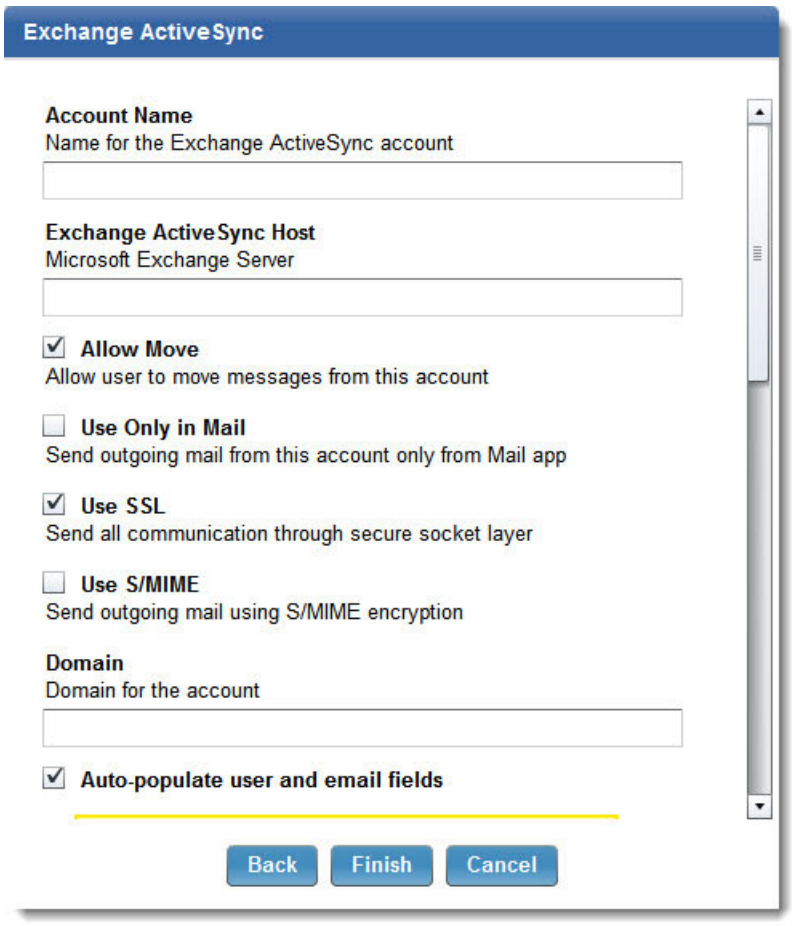


Email Use the email profile to configure POP or IMAP mail accounts. Users can modify some of the mail settings you provide in a profile, such as the account name, password, and alternative SMTP servers. If you omit any of this information from the profile, users are asked to enter it when they access the account.

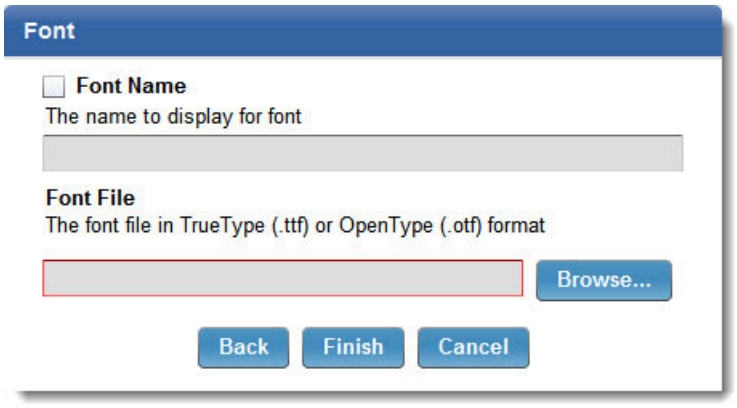


Exchange ActiveSync

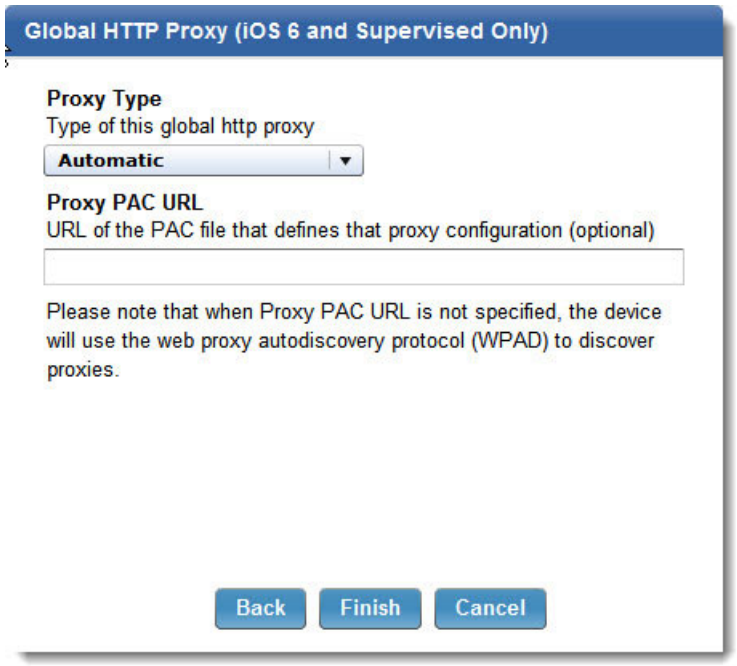
Use this profile to enter user settings for a Microsoft Exchange server. You can create a profile for a particular user by specifying the user name, host name, and email address, or you can provide just the host name. Users are prompted to complete the other values when they install the profile.



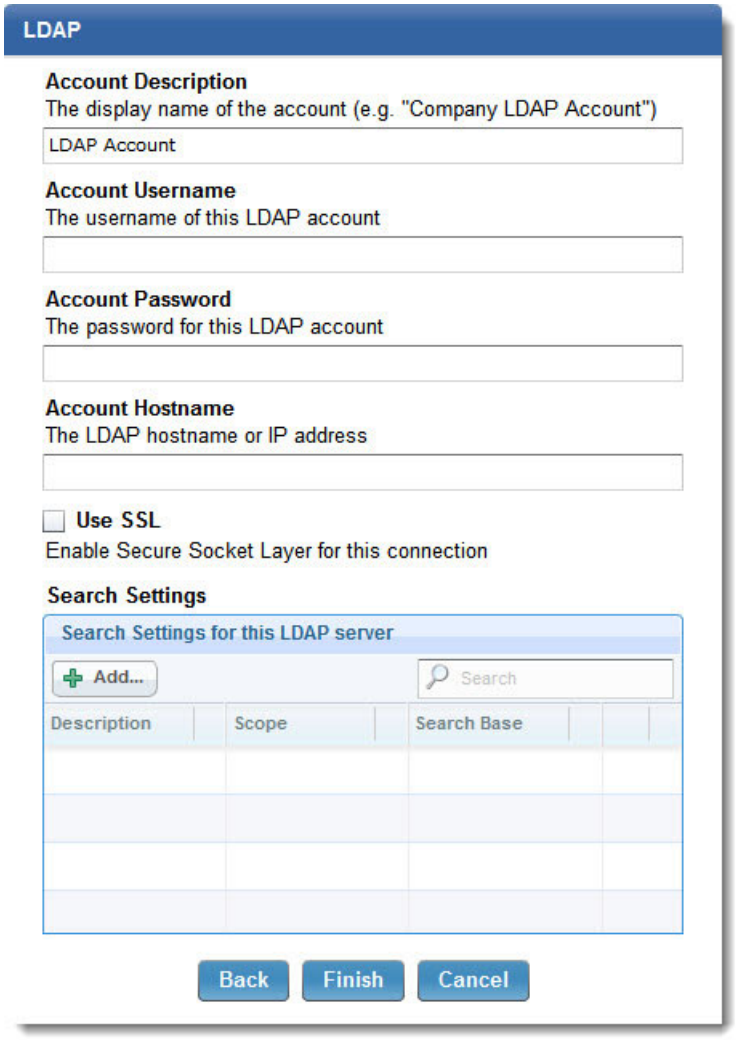
Font This profile allows a custom font to be defined. Select a custom font name, if wanted, and navigate to a TrueType or OpenType font file.



Global HTTP Proxy (iOS 6.0+, Supervised)
This profile is used to specify a proxy for all HTTP traffic to and from the target device. If you choose manual proxy type, you need the proxy server address and its port, and optionally a user name and password for logging in to the proxy server. If you choose auto proxy type, you can enter a proxy auto-configuration (PAC) URL.

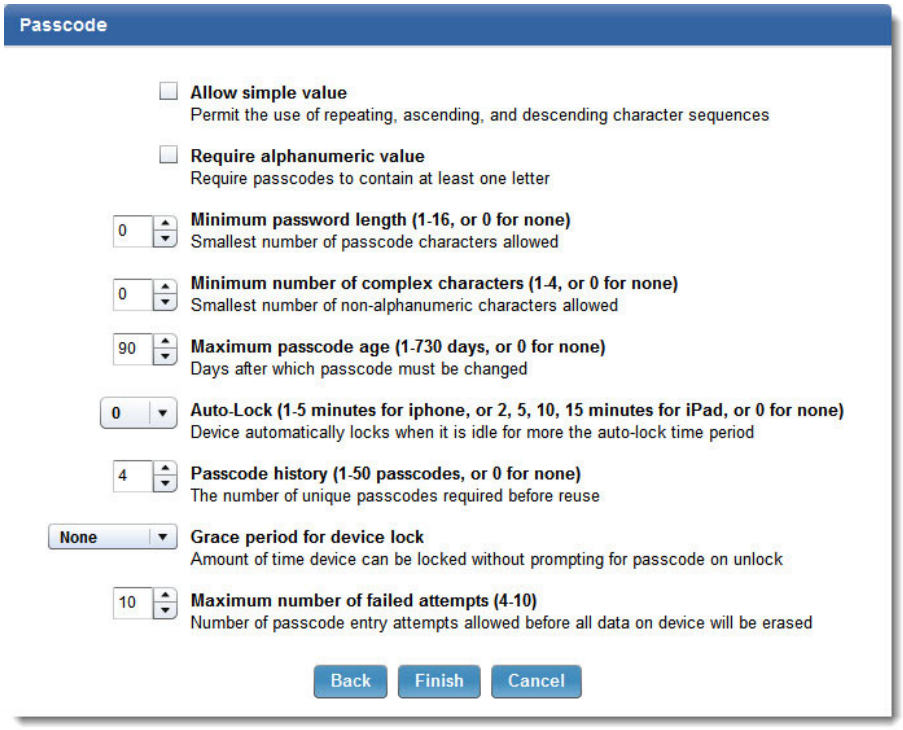


LDAP Use LDAP profiles to configure target devices to connect an LDAPv3 directory. Choose a display name and define the user name, password, and location of the LDAP server. Custom search settings can be defined by standard LDAP attribute aliases.



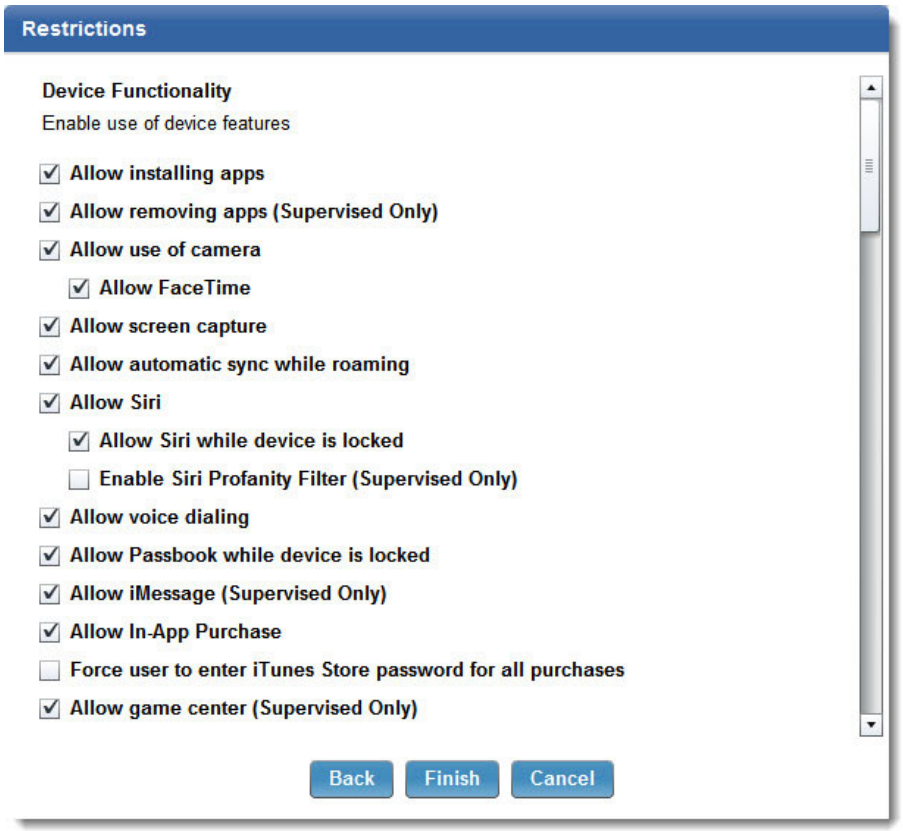
Passcode

This profile sets device password policies if you are not using ActiveSync policies. You can specify whether a passcode is required to use the device, and specify characteristics of the passcode and how often it must be changed. When the configuration profile is assigned to a device, the user is asked to enter a passcode that meets the policies you specify. Otherwise, the profile is not installed.

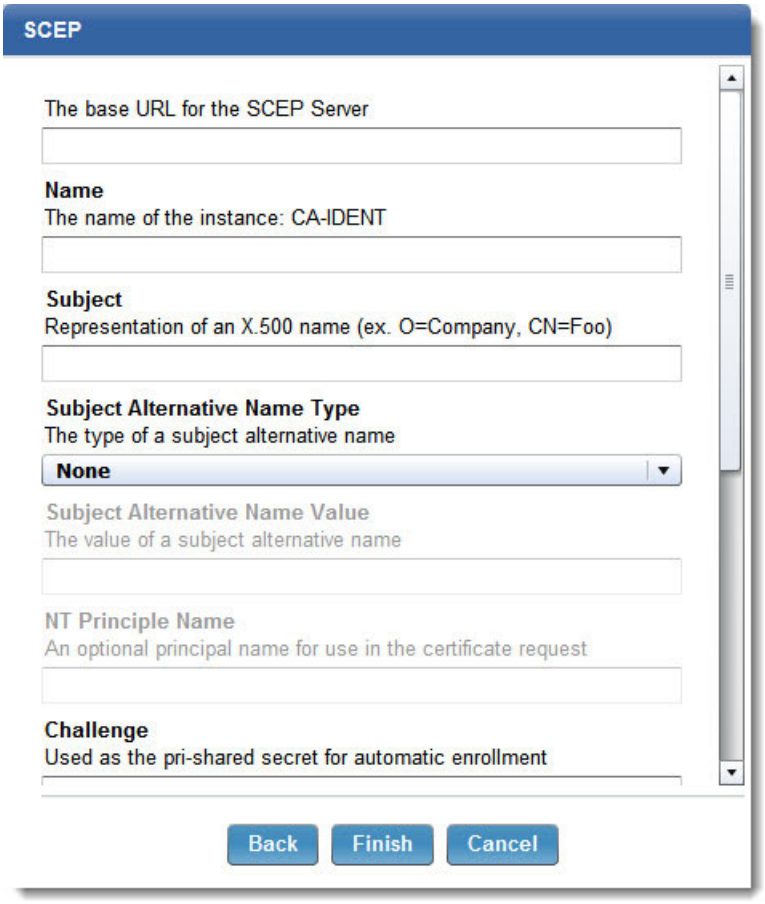


Restrictions

The Restrictions setting can be used to specify which device features are permitted on devices in your deployment. Some settings require supervision mode to be enabled, or require iOS 7.0+.



SCEP The Simple Certificate Enrollment Protocol (SCEP) feature can be used to specify settings that allow a device to obtain certificates from a certificate authority.

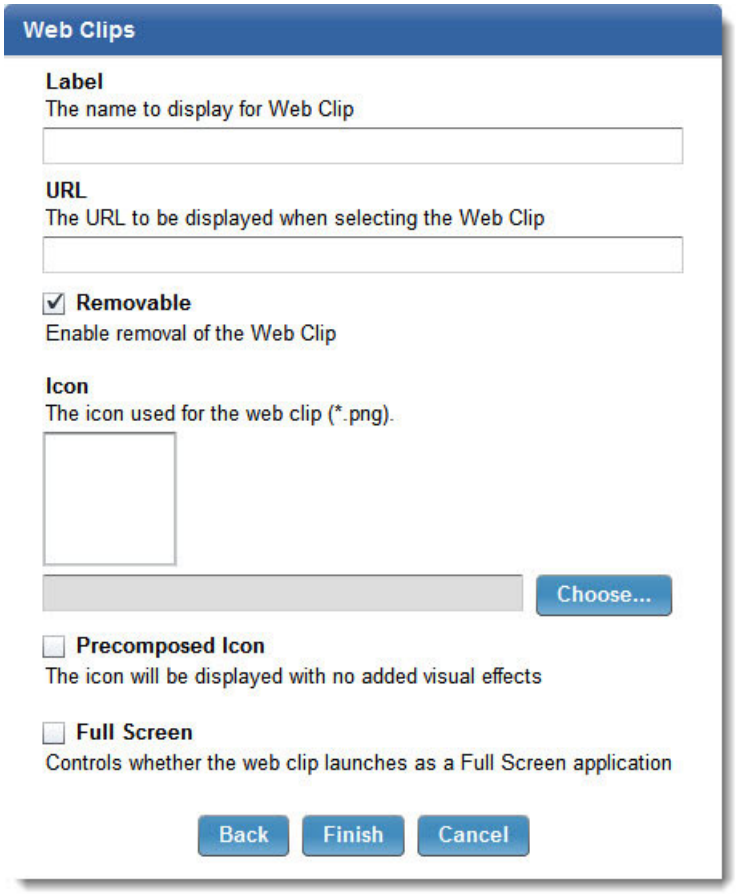


Single Sign-On Account (iOS 7.0+)
This profile configures a device to use a Kerberos based Single Sign-On (SSO) account for authentication.

VPN This profile configures a device to use a Virtual Private Network (VPN) for secured communication. For detailed information on this profile, see "VPN Profile and App Association" on page 45.

Web Clips

This profile allows the creation of a Web Clip to be displayed on target device's home screen. Web Clips are shortcuts that allow quick access to webpages or other various links.

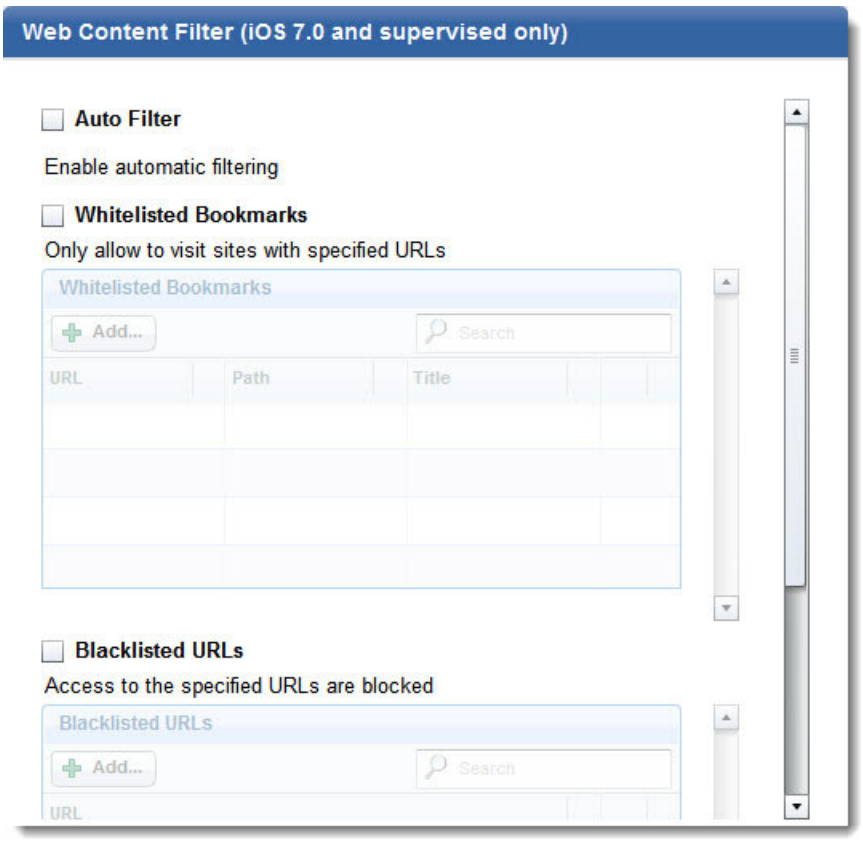


Web Content Filter (iOS 7.0+, Supervised)

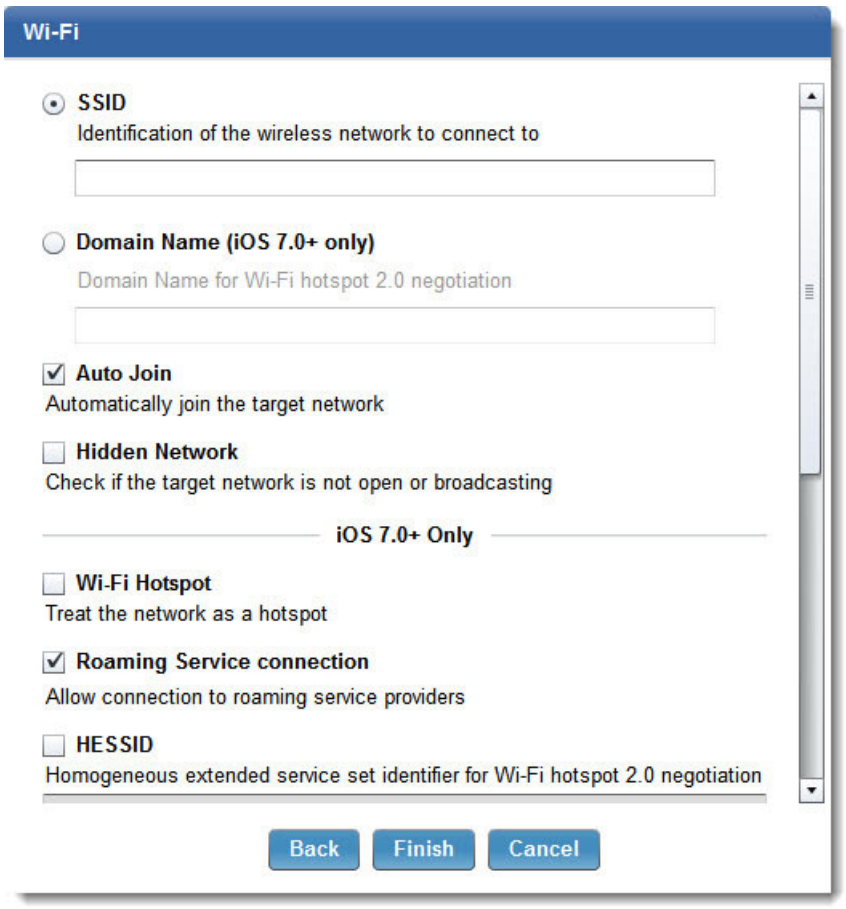
This profile allows control over the web content targeted devices can access. A whitelist or blacklist of URLs can be created. Automatic filtering can be enabled, and safe URLs can be permitted even if automatic filtering would otherwise block them.

Note: When multiple web content filters are assigned to a device:

- The blacklist is the union of all blacklists. Any URL that is present in any blacklist is inaccessible.
- The permitted list is the intersection of all permitted lists. Only URLs that are present in every permitted list are accessible when they would otherwise be blocked by the automatic filter.
- The whitelist is the intersection of all whitelists. Only URLs that are present in every whitelist are accessible.



Wi-Fi This profile configures target devices to use a specified Wi-Fi connection. Enter the connection's SSID and the appropriate settings such as the security type. Several features require iOS 7.0+.



VPN Profile and App Association:

The VPN profile configures a device or iOS app to use a Virtual Private Network for secure communication.

After you enter relevant information in the **Identifier** window, as is done with all profiles, continue to the **VPN** window to configure the available parameters. The type of VPN determines the settings that are required to configure the connection. The following settings are universal to all VPN types:

Connection Name
Choose a connection name that is displayed on target devices.

Connection Type
Select the type of connection. The following connection types are available:

- L2TP
- PPTP
- IPSec (Cisco)
- Cisco (AnyConnect)
- Juniper SSL
- F5 SSL
- SonicWall Mobile Connect
- Aruba VIA
- Custom SSL

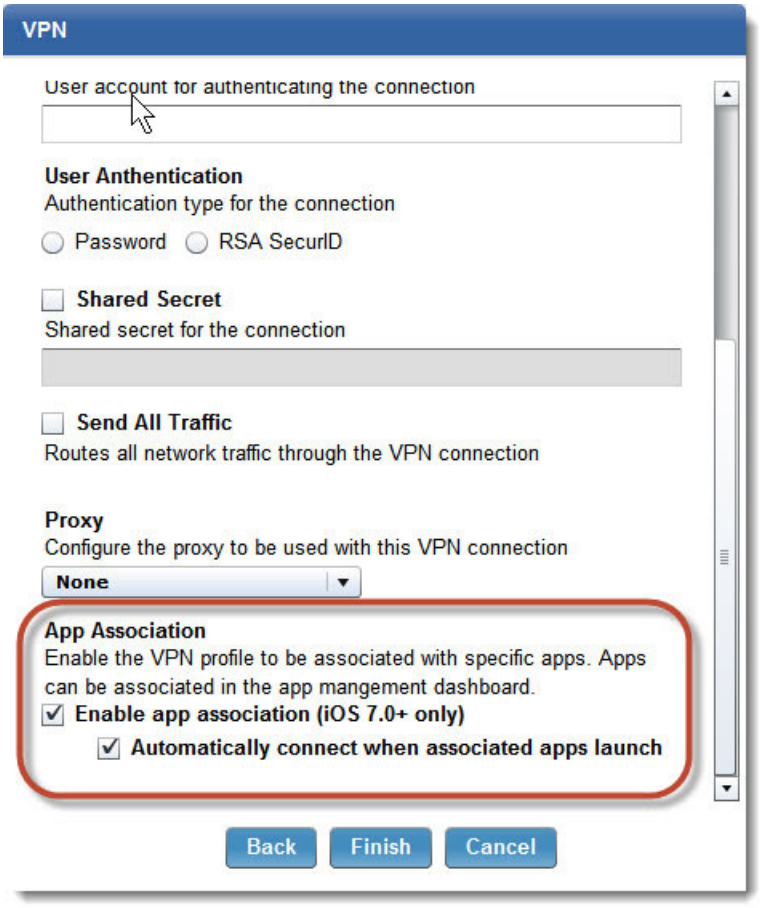
Server Enter the host name or IP address of the server.

Account
Enter the user account that is used to authenticate the connection.

Proxy Select the type of proxy that is used for the VPN. The options are None, Manual, or Automatic. For a manual proxy, enter the server address and port. For an automatic proxy, enter the server from where the proxy settings are obtained.

App Association
In iOS 7.0+, VPN profiles can be associated with specific iOS apps. App association enables secure communication on a per app basis. This process starts with the creation of a VPN profile. This profile is then assigned to iOS apps using the Enterprise App Management dashboard. For more information, see "App Management Tasks" on page 92.

Select the check box to enable app association with this VPN profile. To force apps to automatically connect to the VPN when they are started, select the associated check box.

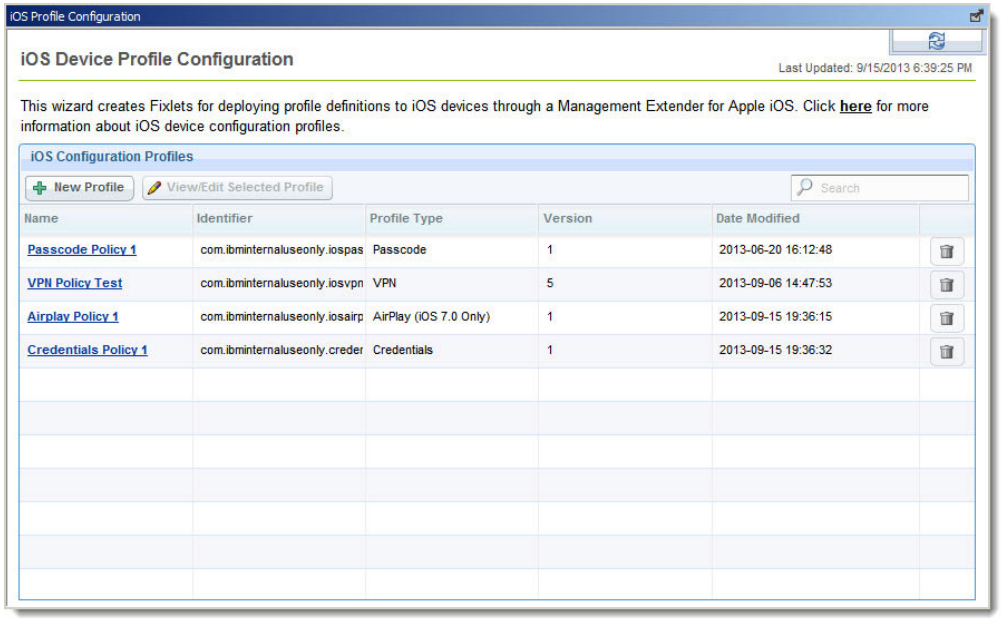


Manage and Assign iOS Configuration Profiles

iOS Profiles that are created are listed in the iOS Profile Configuration dashboard.

The profile's **Name** and **Identifier** are listed as designated during profile creation. The profile type and last date the profile was modified are listed. The **Version** number that is listed for each profile designates how many times the profile was

edited.



To delete an iOS Profile, click the trash icon to the right of a profile. An iOS profile cannot be deleted if it is assigned to any iOS devices. For more information about removing an iOS Profile, see “Remove an iOS Configuration Profile.”

After an iOS Profile is created as a Fixlet, it can be run like any other action. Do so by clicking the name of the iOS Profile to open the action window where relevant devices can be selected after you click **Take Action**.

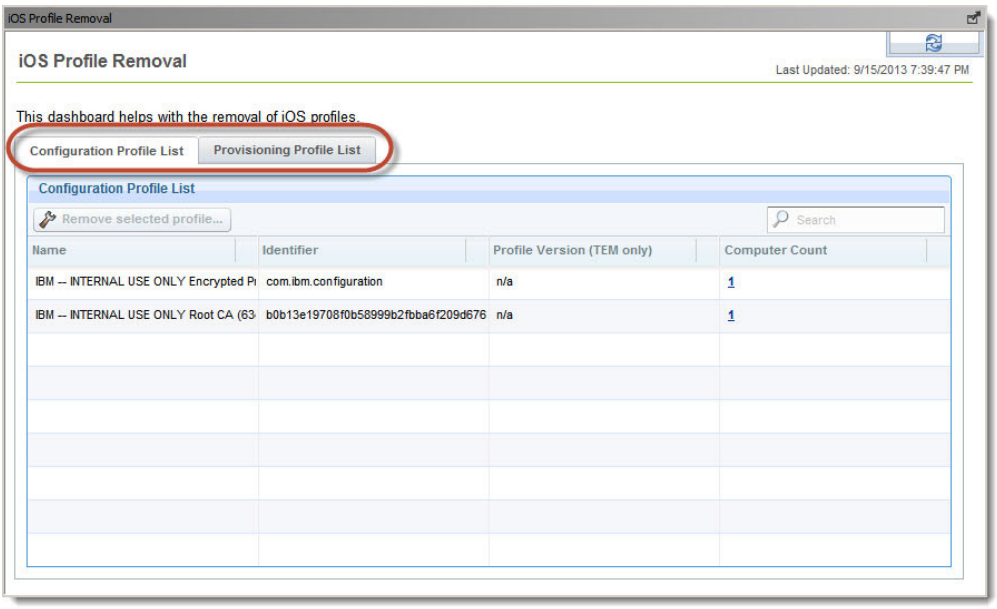
Note: iOS Configuration Profiles can also be found listed as Fixlets by navigating to **Mobile Device Management > Apple iOS Settings > Apple iOS Profiles**. Running them from this location is the same as clicking the profile name from the **iOS Profile Configuration** dashboard.

Remove an iOS Configuration Profile

iOS Configuration Profiles that are assigned to iOS device are listed in the **iOS Profile Removal** dashboard. This dashboard is used to remove profiles from assigned devices.

The iOS Profile Removal dashboard can be found by navigating to **Mobile Device Management > Apple iOS Settings > iOS Profile Removal**.

Note: You might be required to activate analyses for the dashboard to function. If so, a yellow warning banner is displayed at the top of the dashboard. Click **Activate** to turn on the listed analyses.



Two tabs at the top of the dashboard are used to display configuration or provisioning profiles. Any iOS Profiles currently assigned to an iOS device is listed in the dashboard, and the number of devices assigned to the profile is shown in the **Computer Count** column.

To remove a profile from currently provisioned devices, select the profile's row and click **Remove Selected Profile**. The standard action window is displayed where you can select relevant devices. The iOS Profile is removed from the selected devices.

NitroDesk TouchDown

NitroDesk TouchDown is a container application for Android devices available from the Google Play marketplace. TouchDown provides a secure container for corporate data, including email. IBM Endpoint Manager fully supports TouchDown: policy tasks can be created to provision, configure, or wipe the TouchDown application on Android devices.

Before proceeding, device users must have TouchDown installed on relevant Android devices. TouchDown can be downloaded from the Google Play Store, see https://play.google.com. In addition, it is necessary to understand your TouchDown deployment. Settings from your system administrator might be required.

IBM Endpoint Manager can be used to interact with the TouchDown application in several ways:

- Creation of policy tasks to provision and simultaneously configure multiple Android devices.
- Creation of policy tasks to configure multiple Android devices that are already provisioned.
- Provisioning of an individual Android device.
- Wiping data within the TouchDown container on an Android device.

For most deployments, administrators must set up a policy task to provision and simultaneously configure multiple devices. Provisioning TouchDown is the initial setup of the application, where it is given the primary information that it requires to function and communicate with its server. After this initial setup is complete, TouchDown can be configured further.

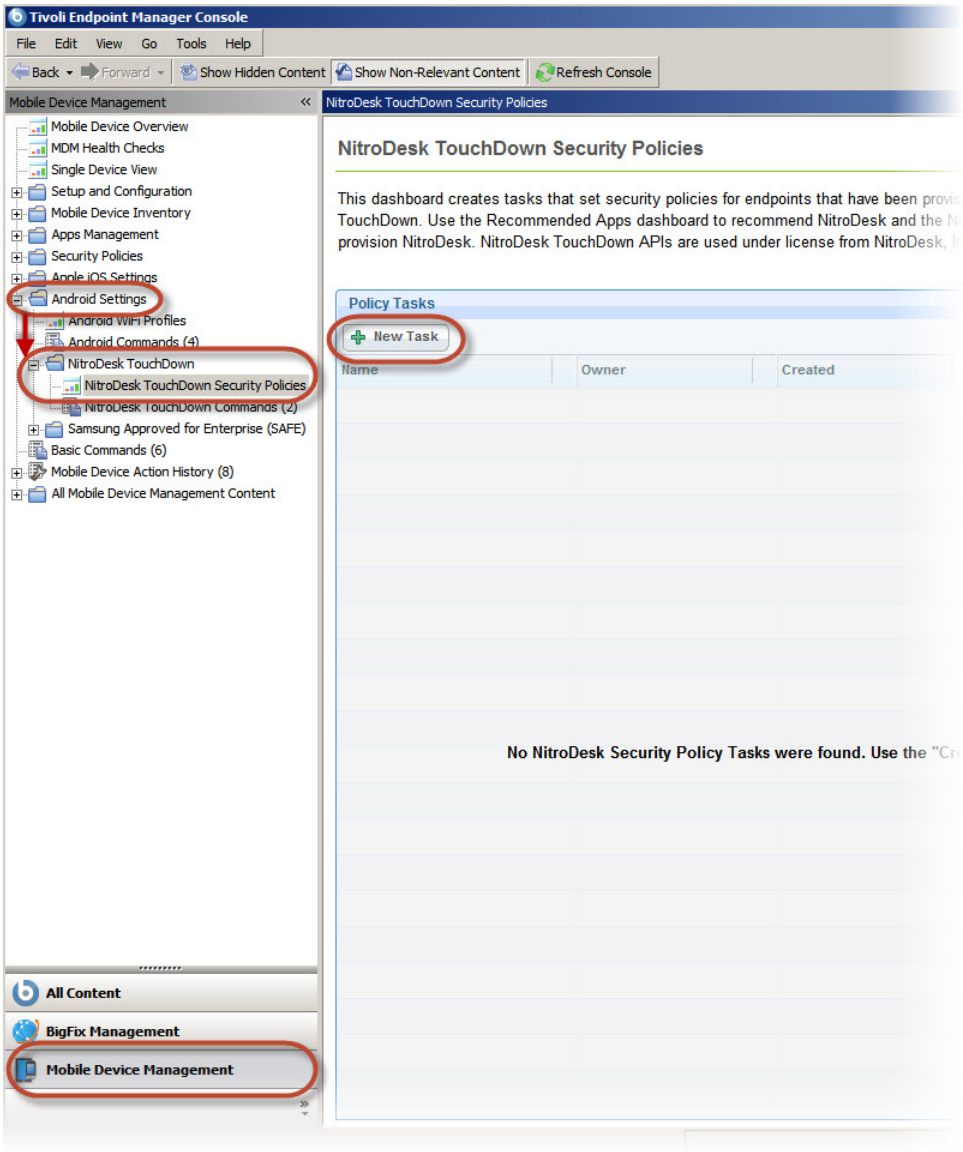
Note: TouchDown must be provisioned before it can be configured, or it must be provisioned at the same time that it is configured. Attempting to run a policy task to configure a TouchDown installation that is not provisioned will fail.

NitroDesk Provisioning Policy Tasks

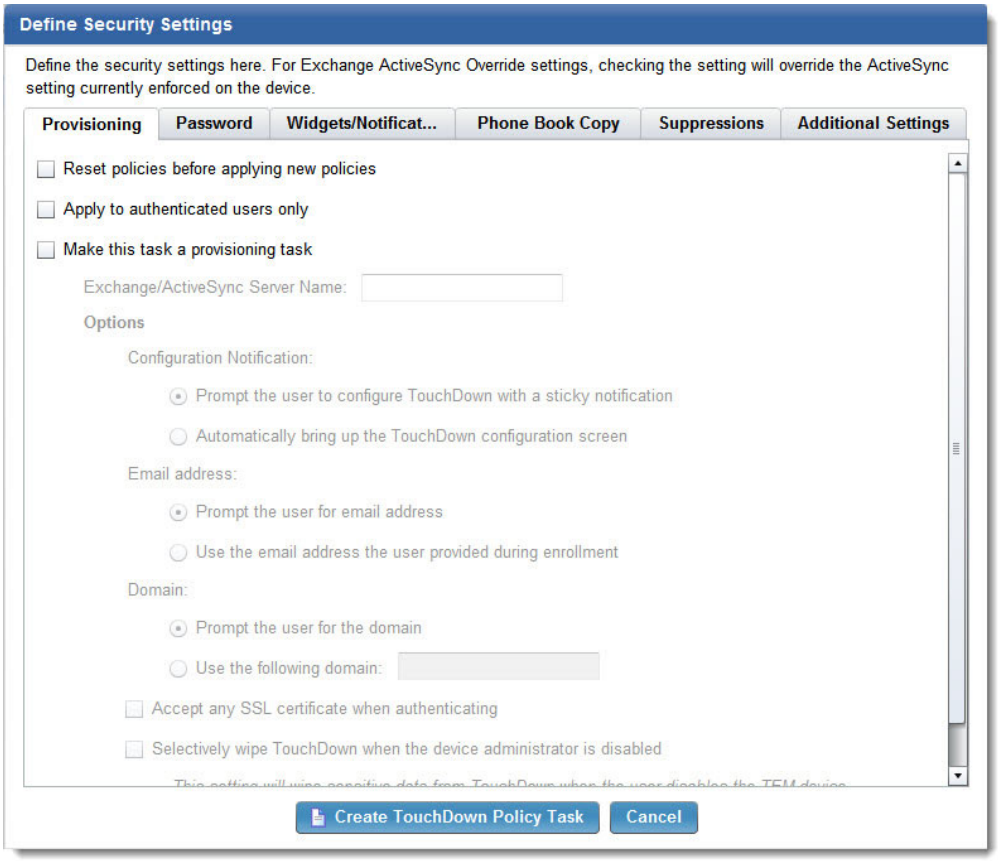
IBM Endpoint Manager allows the creation of policy tasks to provision multiple users with NitroDesk Touchdown. While devices are being provisioned, they can also be configured according to the deployment's needs.

To create a Policy Task to provision and configure TouchDown on multiple devices, perform the following steps:

1. From within the Endpoint Manager Console, select the **Mobile Device Management** site.
2. From the tree on the left of the console, expand the **Android Settings** node.
3. Expand the **NitroDesk TouchDown** node.
4. Select **NitroDesk TouchDown Security Policies**. You can see a list of policy tasks, if any exist.



5. Click **New Task**. The **Define Security Settings** window opens.

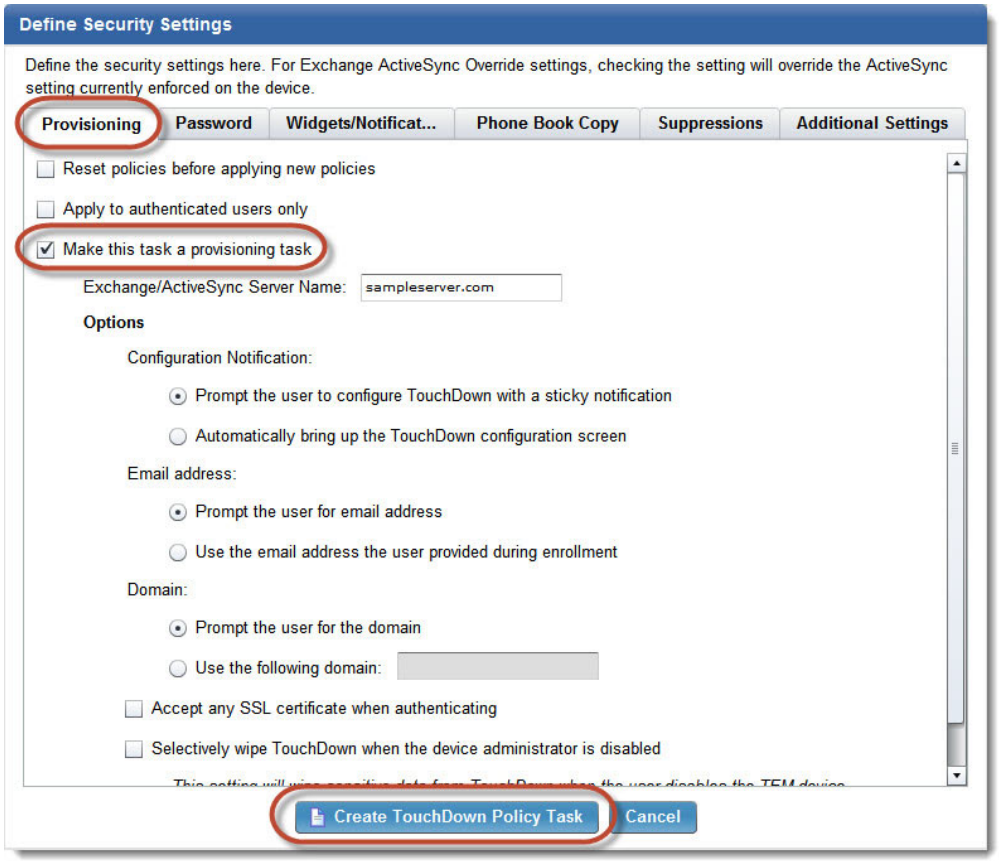


Note: Any settings that are configured in a policy task are set on the device and cannot be changed by the device user. Depending on your deployment, you might want to leave some settings that are not configured, or prompt the user for the relevant information.

Provisioning:

When you create a TouchDown policy, it can be configured to be a provisioning policy in addition to performing regular configuration. Provisioning is the initial setup of the application, where it is given the primary information that it needs to run and communicate with its server. A provisioning task can also configure TouchDown at the same time.

Within the **Define Security Settings** window, the **Provisioning** tab is where you define whether this policy is a provisioning policy or not. TouchDown must be provisioned before it can be configured, however a provisioning policy can configure TouchDown during the provisioning process. The other tabs allow various configuration options to meet the needs of your deployment.



To set the policy task to provision devices, perform the following steps on the **Provisioning** tab:

1. Select the wanted options by choosing the appropriate check boxes:

   Reset policies before applying new policies
   Wipe any policies before the policies you are configuring now are set. Not checking this option augments existing policies with the settings defined during the creation of this policy.

   Apply to authenticated users only
   Apply this policy only to devices that are enrolled through authenticated enrollment.

2. Select **Make this task a provisioning task**.
3. Enter your server name in the **Exchange/ActiveSync Server Name** field.
4. The following three settings are required. These settings can be set during provisioning or the device user can be prompted to enter the relevant information:

   Configuration Notification
   Select whether the TouchDown configuration screen is displayed when the policy takes effect, or if the device user is prompted to go to the configuration screen manually.

   Email Address
   Select whether the device user is prompted to enter an email address, or if the email address defined during device enrollment is automatically entered.

Domain

Select whether to prompt the device user for the domain, or enter it here to be automatically defined.

Note: Settings that are configured during provisioning are both defined and simultaneously blocked from being edited by the device user.

5. Check the box to allow all SSL certificates if wanted.
6. Check the box to delete all TouchDown data if a user removes Administrator rights for the IBM Mobile Client within their Android device settings.

Note: If a user disables administrator rights for the IBM Mobile Client, the ability to manage their device is reduced; this situation might pose a security risk. If this box is selected, the user is warned that TouchDown data will be erased before they can complete the removal of administrator rights on their device.

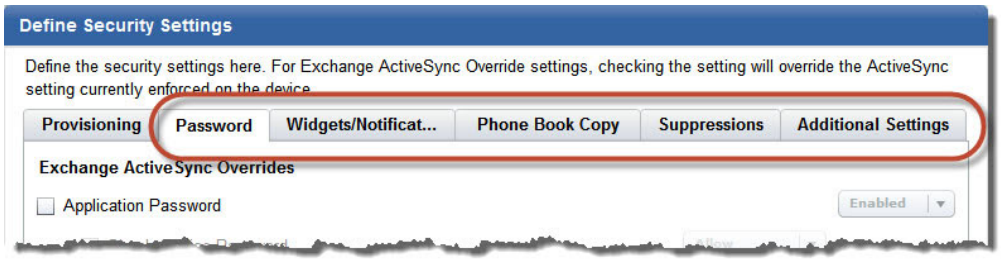
Create TouchDown Policy Task can now be selected to create the provisioning policy. You might decide to continue to the other available tabs before you create the policy task. This allows you to set up the policy to configure TouchDown at the same time it is provisioned.

NitroDesk Configuration Policy Tasks

Policy tasks can be created to configure NitroDesk TouchDown. Devices must be provisioned either before they are configured or as part of the configuration policy.

To set up a configuration policy task, use the following tabs in the **Define Security Settings** window:

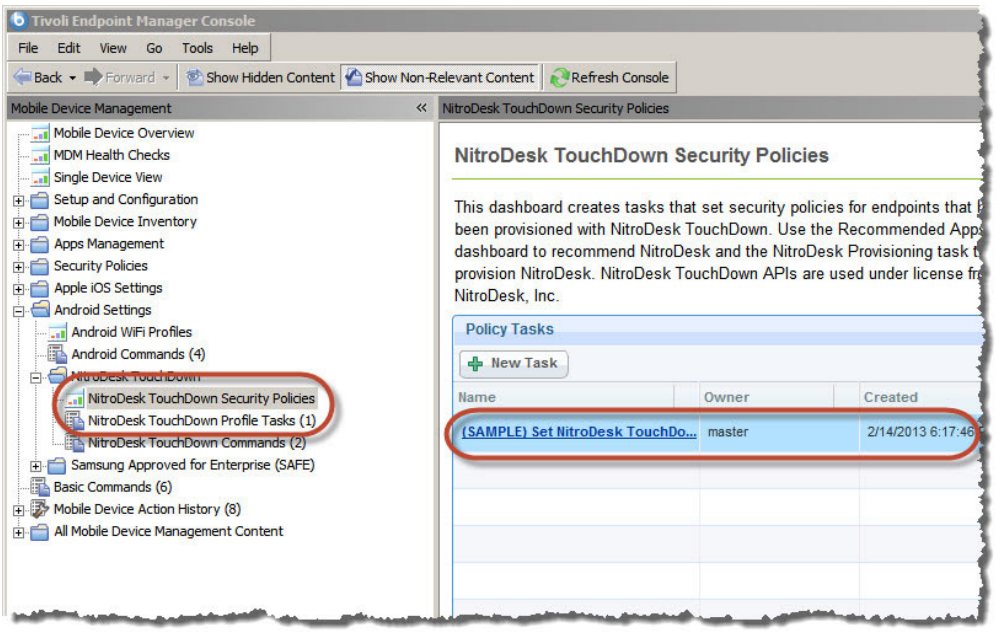
- **Password**
- **Widgets/Notifications**
- **Phone Book Copy**
- **Suppressions**
- **Additional Settings**



You can set a configuration policy task to provision devices, by following the instructions in the previous section. Remember, TouchDown must be provisioned before it can be configured. Whether a policy task is set to provision TouchDown, it is configured in the same manner.

Note: For detailed information about policy configuration settings, see the NitroDesk documentation at http://nitrodesk.com/.

When the settings in each of the tabs are configured according to your deployments needs, click **Create TouchDown Policy Task**. You can choose to customize the name of the policy task that you created. Click **OK** to finish the policy task, which can now be run. The new policy task is available from the NitroDesk TouchDown Security Policies node in the left tree of the console.



Note: Configure settings in a TouchDown policy task to have particular settings that are enabled, disabled, pre-populated, or user-configurable. Users cannot change settings that are controlled by the policy. Instead, if the policy does not address a particular setting, a user might be able to change that setting on their device.

Password

The settings in this tab allow the ability to enable or disable a password that is required to access the TouchDown application. If enabled, you can change the parameters of the password.

Widgets/Notifications

This tab allows the policy to dictate what types of TouchDown widgets and notifications are available and how they are displayed on the Android device. Any settings that are not enabled can be customized by the device user.

Phone Book Copy

The default behavior of TouchDown is to allow the TouchDown phone book to be copied into the Android device's internal phone book. Select the check box on this tab to remove the permission for the TouchDown phone book to be copied. You can specify which fields cannot be copied, or you can specify that all fields must be blocked.

Suppressions

This tab allows the policy to dictate what user interface elements are visible in the TouchDown application. Check a box to remove selected elements from the user interface.

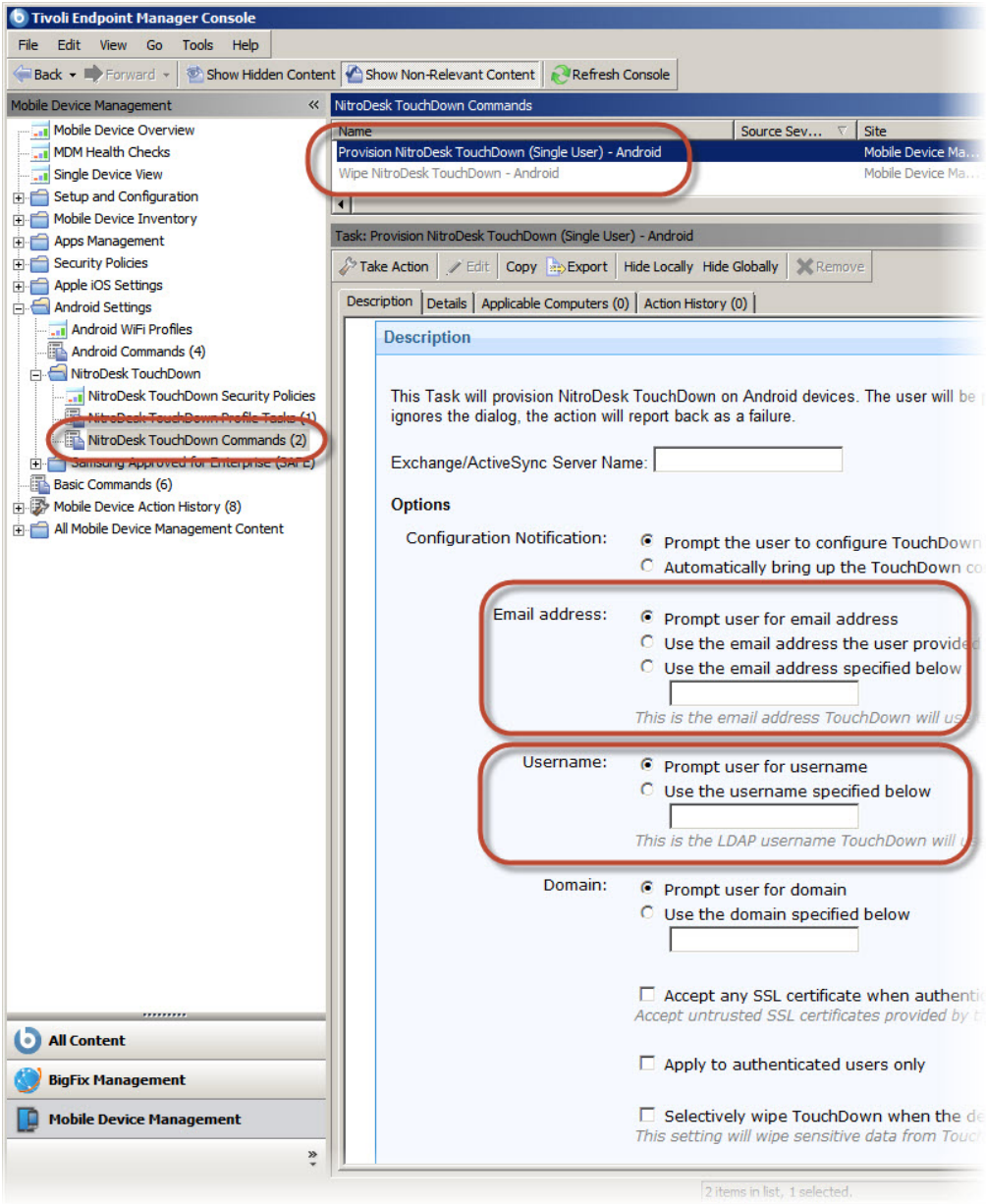
Additional Settings

This tab covers settings that allow control over Exchange ActiveSync, in addition to other security settings.

Provision a Single Device

It is possible to quickly provision TouchDown on a single device.

The task is found by selecting **Android Settings > NitroDesk Touchdown > NitroDesk TouchDown Commands** from the **Mobile Device Management** site tree on the left of the console. Select the **Provision NitroDesk TouchDown (Single User) – Android** task at the top of the window.



The use of this task is similar to the creation of a provisioning policy task. Additional capabilities include the following:

- The ability to specify the email address that is used to connect to the server.
- The option to prompt or specify the user name that is used to connect to the server.

Wipe NitroDesk TouchDown

It is possible to wipe all data from NitroDesk TouchDown. Running this task deletes information from TouchDown and does not affect any other data stores.

The task that allows the deletion of all data in the TouchDown container can be found by selecting **Android Settings > NitroDesk Touchdown > NitroDesk**

TouchDown Commands from the **Mobile Device Management** site on the left of the console. Select the **Wipe NitroDesk TouchDown – Android** task at the top of the window.

Select the link at the bottom of the window, or click **Take Action**to run the task. Choose the Android device or devices whose TouchDown containers are to be wiped.

Note: When you create a provisioning task, it is possible to set the application to wipe all information if a device user disables administration rights for the IBM Mobile Client application. If a user attempts to do so, they are warned before any information is erased. For more information, see "Provisioning" on page 51.

Samsung SAFE

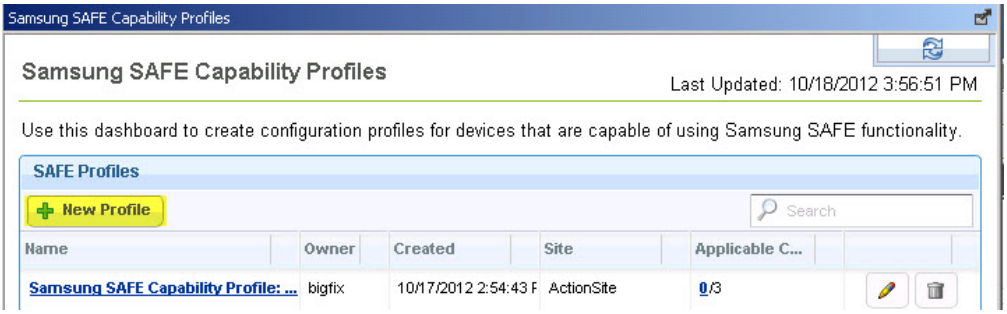
Samsung Approved for Enterprise (SAFE) is a set of management features that are available to be used on Samsung devices. IBM Endpoint Manager for Mobile Devices supports SAFE up to and including V3.0 (Build Code 5). Later versions are not supported.

Management features include:

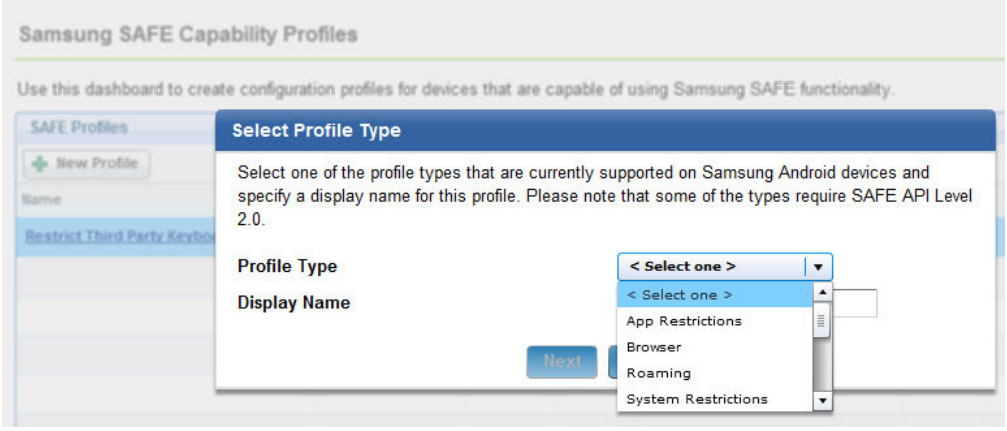
- SAFE Capability Profiles dashboard
- SAFE Fixlets, including Exchange Profile, Restart,and Shut Down
- Additional functionality in the Android Recommended Apps dashboard

SAFE Capability Profiles Dashboard - Similar to Nitrodesk Touchdown, you can create SAFE profiles that enforce various security settings and restrictions on your Samsung devices. This dashboard creates profiles that set numerous management features on your Samsung devices.

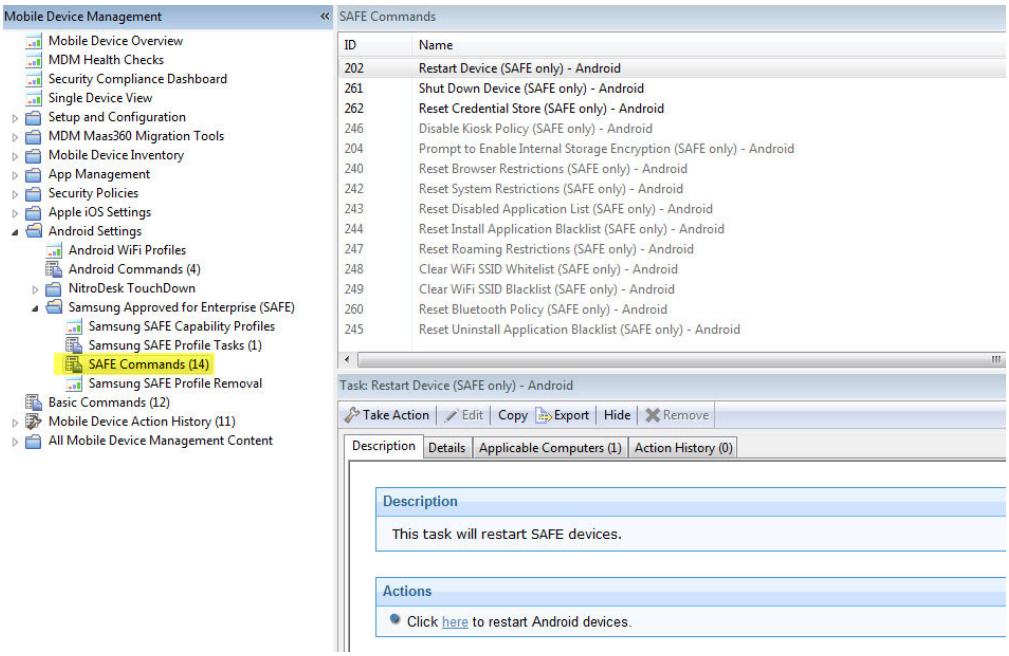
Expand the Samsung SAFE node in the Mobile Device Management navigation tree and click the Samsung SAFE Capability Profiles dashboard. Open the dashboard and click *New Profile*.



Select a profile type, enter a display name, and follow the prompts to create the new profile.



The SAFE commands are stored in the Safe Commands folder.



For more information about managing apps on SAFE-enabled devices, see App Management Android Tasks.

Bulk Certificate Import

Use Bulk Certificates to import a specific certificate into an iOS profile to deploy onto a large number of iOS devices at the same time. Certificates can be computer-specific or user-specific.

Use the following steps to set up your bulk certificate import:

1. Write a certificate script that corresponds to your certificate infrastructure. For a sample script, click here: https://www.ibm.com/developerworks/mydeveloperworks/wikis/home?lang=en#/wiki/Tivoli%20Endpoint%20Manager/page/Bulk%20Certificate%20Import%20setup%20for%20iOS%20Configuration%20Profile.
2. Configure a setting on the iOS MDM server. This must be done manually in the config.yaml file of the iOS Management Extender.

3. Restart the iOS MDM service on the Management Extender computer.

When you create a configuration profile for one of the following types (Email, Exchange, WiFi, Credentials), you can use the UI to import a certificate automatically, or to specify a certificate for an individual user. Certificates for individual users are not scalable.

If you use the import certificate feature, you specify parameters that are passed by MDM to the certificate import script prior to the profile installation for each device.

Note: Each user must write their own version of this script. You can easily integrate this customized script into your own certificate service or infrastructure. You can also create a folder to contain all certificates.

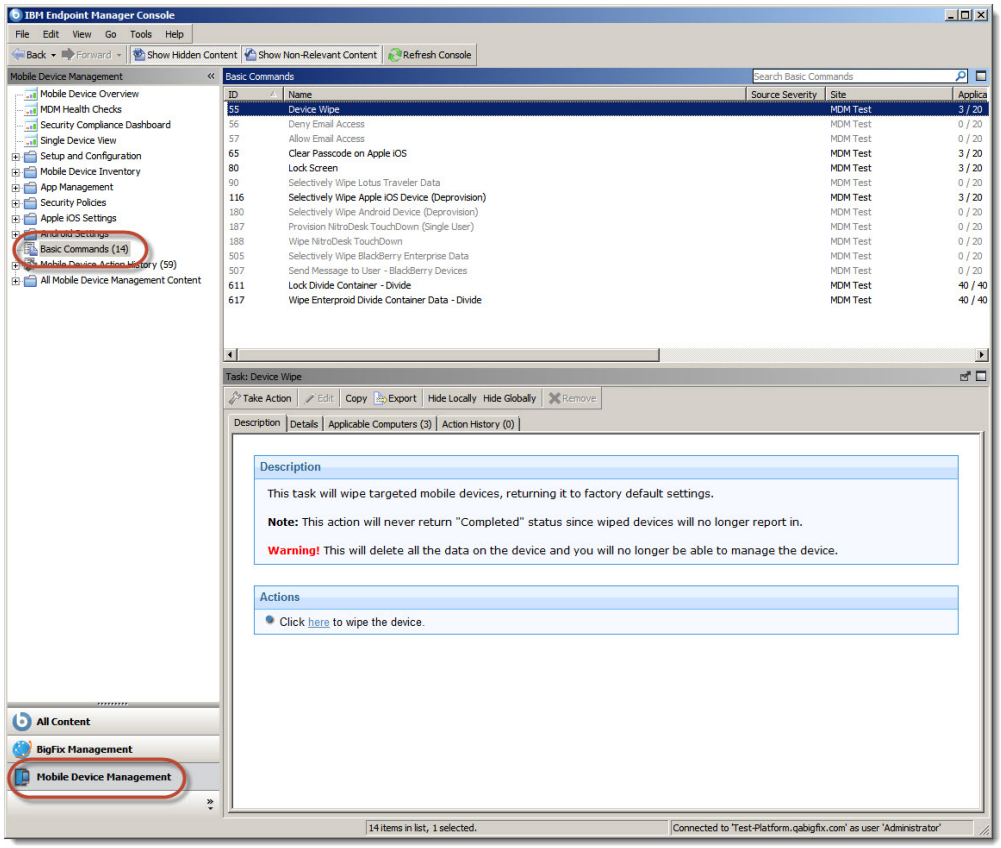
Management Commands

Management commands allow specific actions to be performed on the devices in your deployment. These include wiping the device, allowing or denying email access, clearing passcodes, and locking the screen. Actions and Tasks can be found in several places within the console.

Basic Commands

Several basic commands are grouped for easy access.

A selection of basic commands can be found by navigating to **Mobile Device Management > Basic Commands**. These tasks represent some simple management commands such as device wipe, and lock screen.



Some tasks are described in detail:

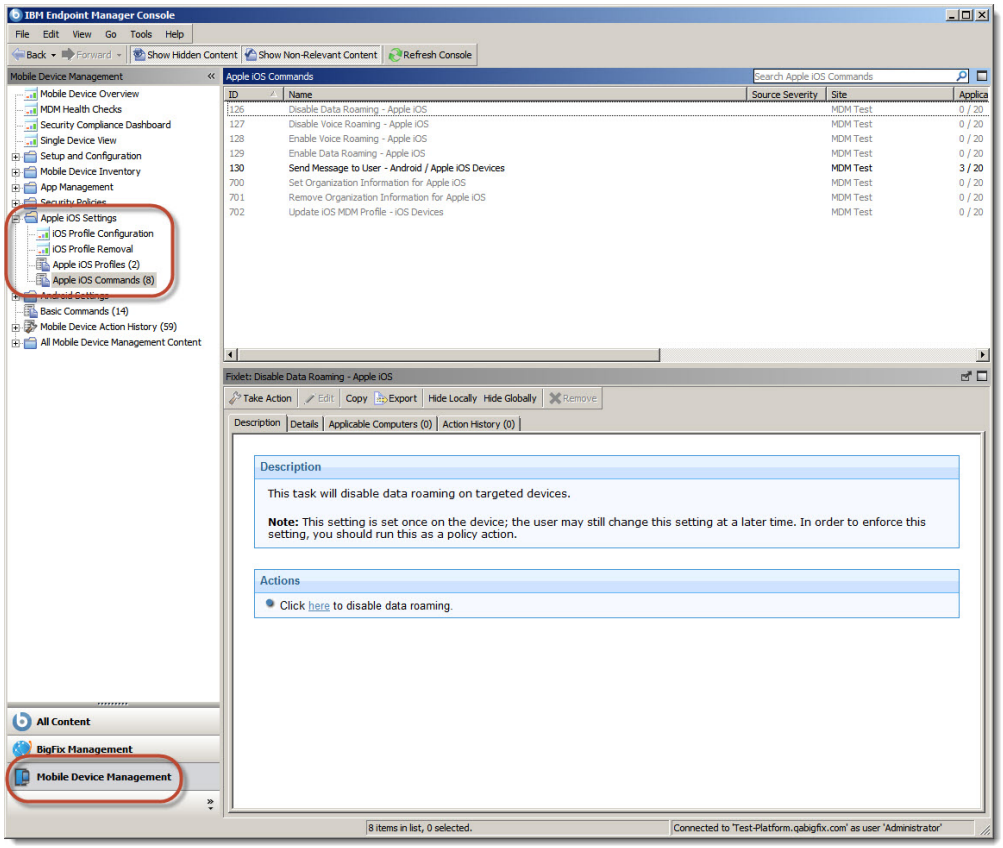
Lock Screen

Task ID 80 - Lock Screen causes the device screen to lock. Device users are required to enter the device password to regain access to the device. In iOS 7+ devices, a custom message can be displayed on the lock screen along with a phone number. Clicking the phone number on the lock screen allows a call to be made to that number only.

Apple iOS Commands

Several basic commands for Apple iOS devices are grouped for easy access.

A selection of basic commands for Apple iOS devices can be found by navigating to **Mobile Device Management > Apple iOS Settings > Apple iOS Commands**. These tasks represent some simple management commands such as enabling or disabling data or voice roaming.



Some tasks are described in detail:

Set Organization Information for Apple iOS

Task ID 700 - Set Organization Information for Apple iOS allows organizational information to be set on devices running iOS 7+. It is unknown how this information is used by the device and requires further documentation by Apple Inc. **Task 701 - Remove Organization Information for Apple iOS** removes the organization information from the selected device.

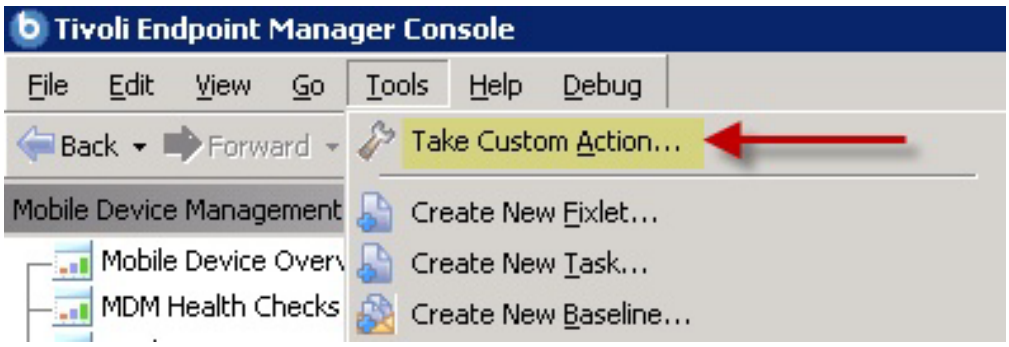
This task can be found by navigating to **Apple iOS Settings > Apple iOS Commands**.

Sending Notifications to Devices

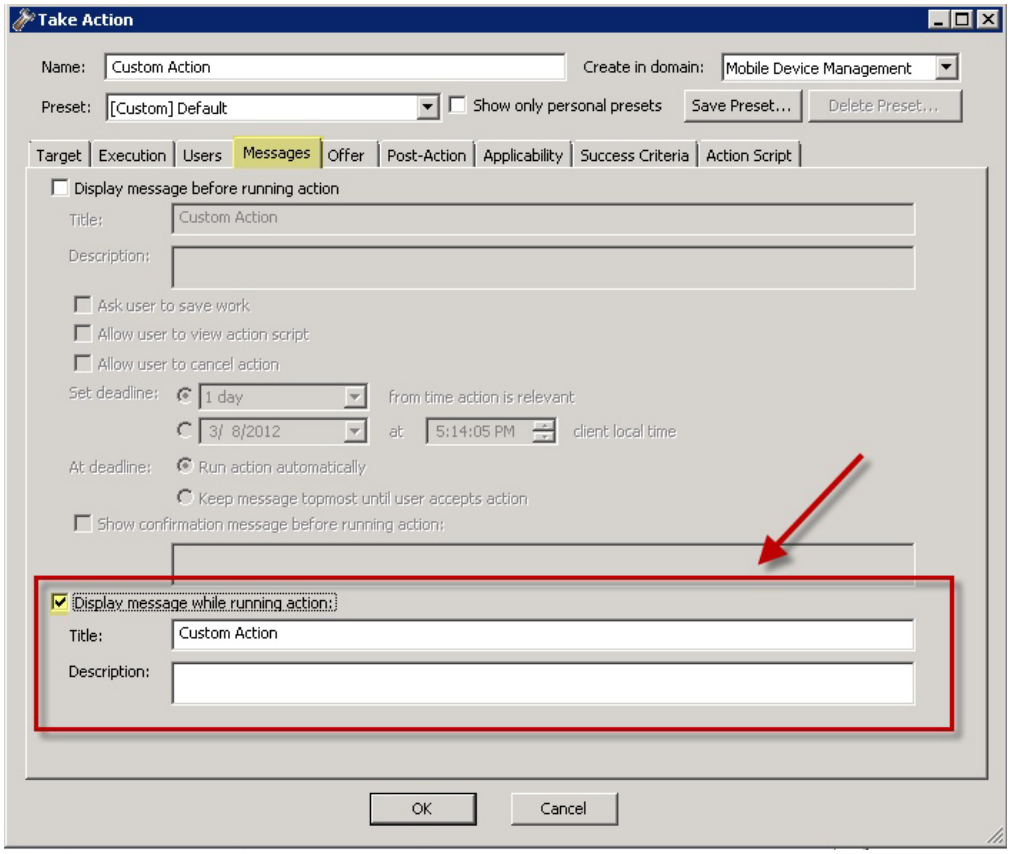
You can send messages to Android or Apple iOS mobile devices that have the IBM Mobile Client app installed.

Android Messages

Android devices use *sticky notifications* for messaging users. This means that the notification will remain in the Android status bar until the user opens and removes it. To send a message to Android devices, click the Tools menu in the TEM Console and select *Take Custom Action.*



Custom messages can be attached to any action (or sent with a "blank action" to show only the message). Click the *Messages* tab, and manually enter the message in the *Display message while running action* field. Then click *OK.*



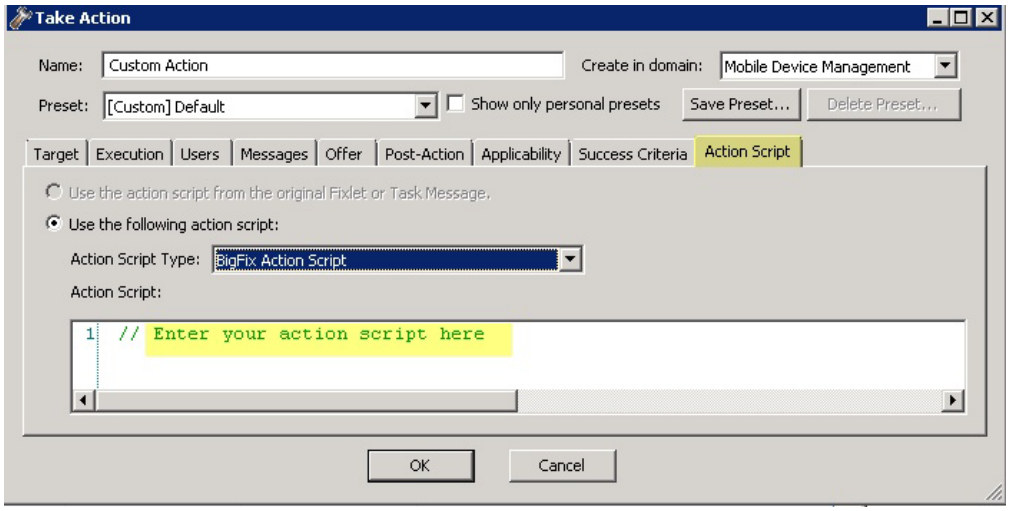
Currently, the Android Mobile Client does not support the *Display message before running action* pre-action messages, and only supports the *Display messages while running action* messages.

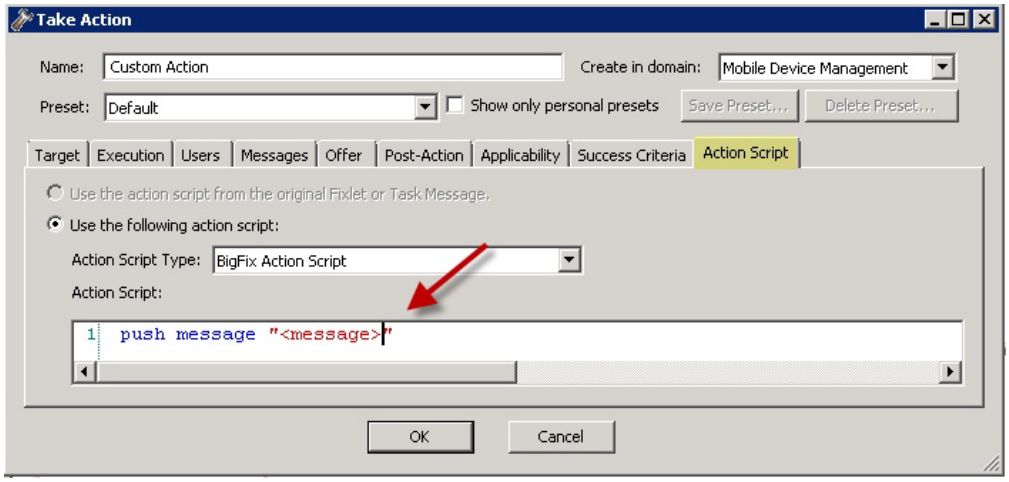
You can also send a notification through a default Fixlet message. Some Fixlets have actions that send messages to the Mobile Client by default. You can use the default messages or you can modify them using the Message tab in the Take Action Dialog.

Apple iOS Messages

Apple iOS uses *push notifications* to display message notifications to users. This notification will display as a message on the device and in the Apple Notification Center on devices using Apple iOS5 and above. Similar to Android devices, Apple iOS messages can be sent by custom actions and through a default Fixlet message.

To send a message to an Apple iOS device, click *Take Custom Action* from the TEM Console and select the *Action Script* tab. Custom messages for Apple iOS devices use an actionscript command **push message "<message>"**. The "Send Message to User - Apple iOS" task allows you to easily send a message. This Fixlet will only become relevant on devices that have the IBM Mobile Client app installed.



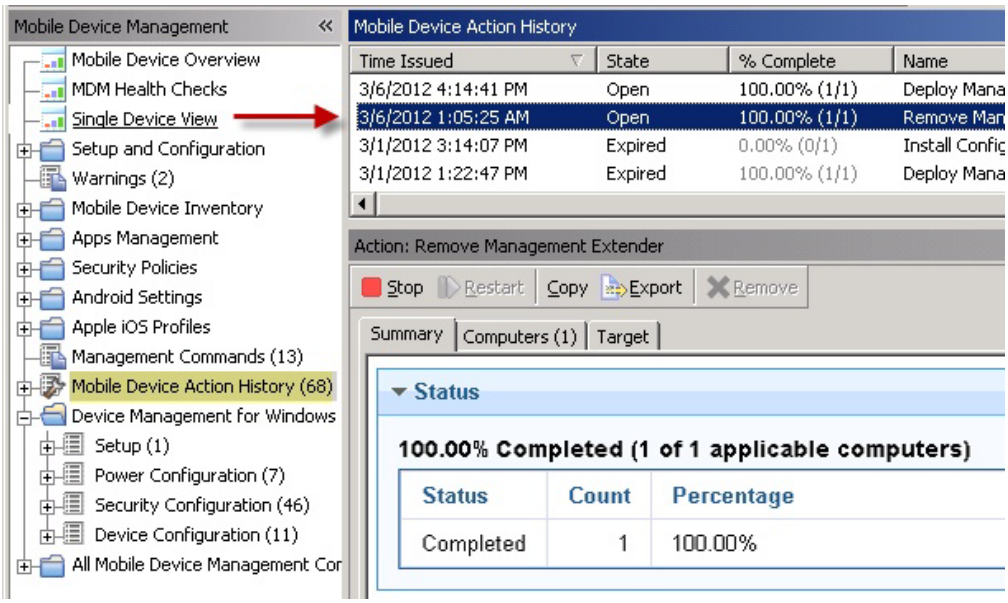


Manually enter your message in the Action Script field and click *OK*.

Mobile Device Action History

Click Mobile Device Action History from the navigation tree to see a summary list of the actions you have taken to manage the mobile devices in your deployment.

When you click any action in the list, specific details of that action display in the Action window below.



From the summary tab in the Action window, you can see information on status, downloads, source, behavior, details, and comments about each action you have taken on your mobile devices.

Apple iOS Profiles

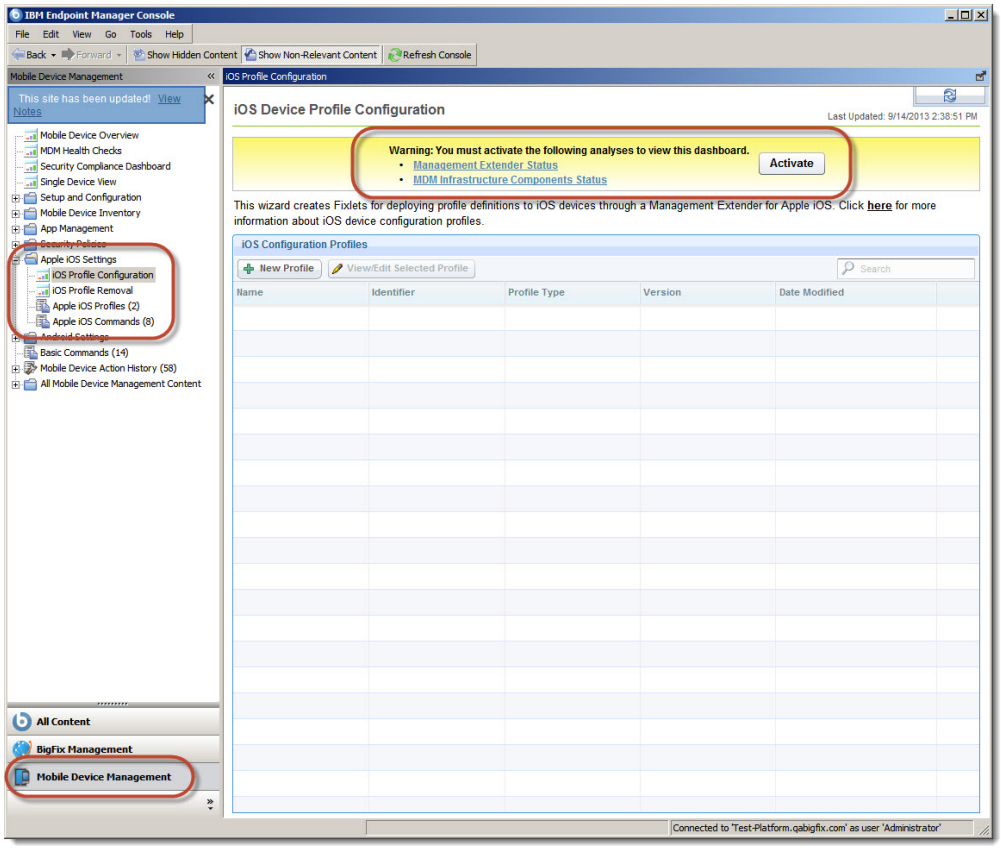
Apple iOS devices can be assigned profiles that manage a wide range of enterprise features.

Apple Inc. supports the creation and application of iOS profiles though its Apple Configurator tool. The ability to create, deploy, and remove profiles to and from iOS devices that are managed by IBM Endpoint Manager is implemented in the **iOS Profile Configuration** dashboard.

More information about Apple Configurator and iOS profiles can be found at http://www.apple.com/support/iphone/enterprise/.

The **iOS Profile Configurator** dashboard can be found by navigating to **Mobile Device Management > Apple iOS Settings > iOS Profile Configuration**.

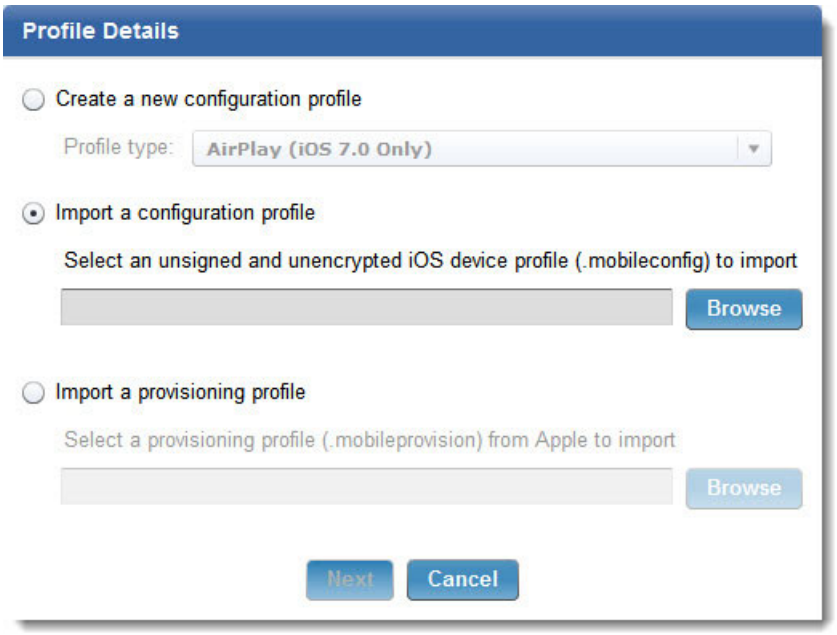
Note: You might be required to activate analyses for the dashboard to function. If so, a yellow warning banner is displayed at the top of the dashboard. Click **Activate** to turn on the listed analyses.



Import an iOS Profile

An existing configuration profile or provisioning profile can be imported. After it is imported, the profile can be edited and assigned to devices.

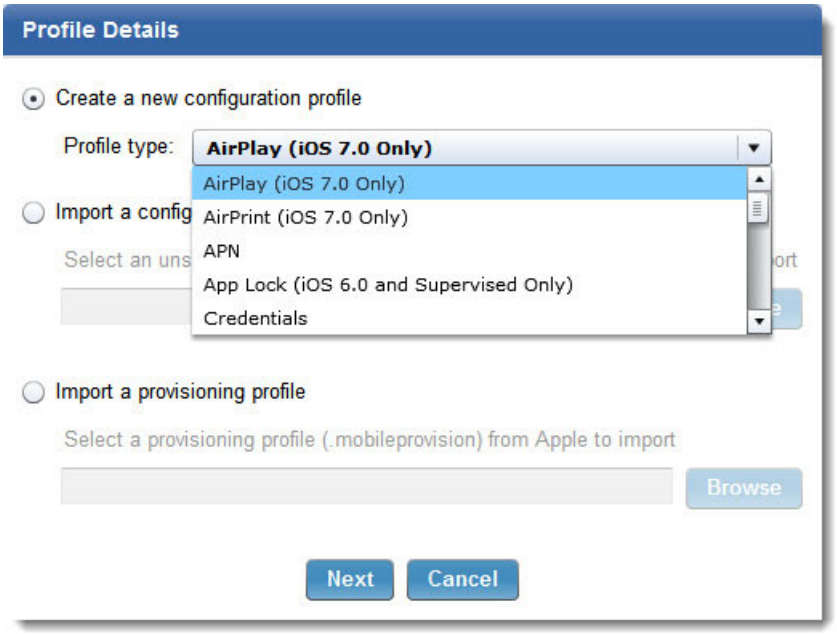
Click **New Profile**. The **Profile Details** window is displayed. Select the appropriate radio button and navigate to the existing profile. Configuration profiles must have a `.mobileconfig` extension and they must be both unsigned and unencrypted. Provisioning profiles must have a `.mobileprovision` extension and must be unencrypted.



Create or Edit an iOS Configuration Profile

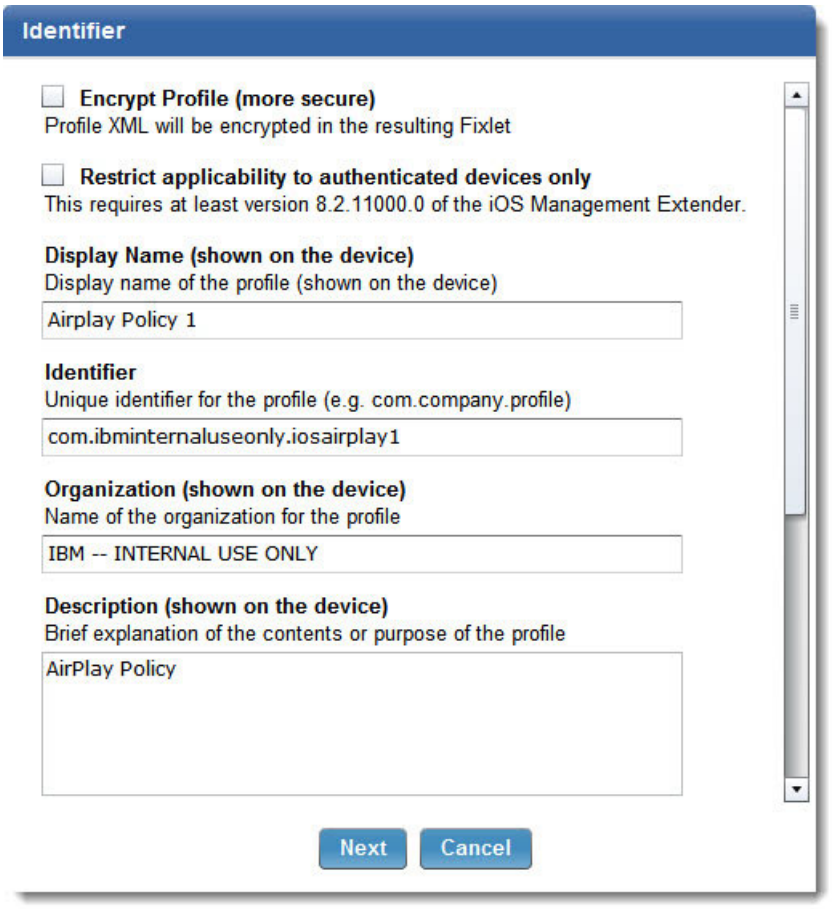
Configuration profiles can be created within the iOS Profile Configuration dashboard. Existing configuration profiles can be edited.

To create a new iOS Profile, click **New Profile** and select the profile type from the menu. Alternatively, you can edit an existing profile by selecting it from the list and clicking **View/Edit Selected Profile**. For information on the various profile types, see "iOS Profile Types" on page 31.



Regardless of the profile type that is selected, the **Identifier** window is displayed. The following options must be configured before you click **Next** to choose the profile specific settings for each profile:

- The profile can be encrypted for increased security.
- The profile can be restricted to apply to authenticated devices only.
- A name for the profile is defined. This name is displayed on the device when the profile is active on a device.
- A unique identifier must be assigned to the profile. A recommended identifier is entered by default.
- Organization information can be defined. This information is displayed on the device when the profile is active on a device.
- A description can be defined to help document the profile.
- A message can be defined that displays on iOS 6.0+ devices when the profile is installed.
- Control of the profile can be given to the device user always, or by a password that is defined here. Alternatively, control can be denied.
- The profile can be set to be removed automatically on the date that is specified, or after a number of days that are defined here.



Note: Some profile types require target devices to have iOS 6.0+ or iOS 7.0+. In addition, some profiles require supervision mode to be on. These restrictions are delineated in the profiles name.

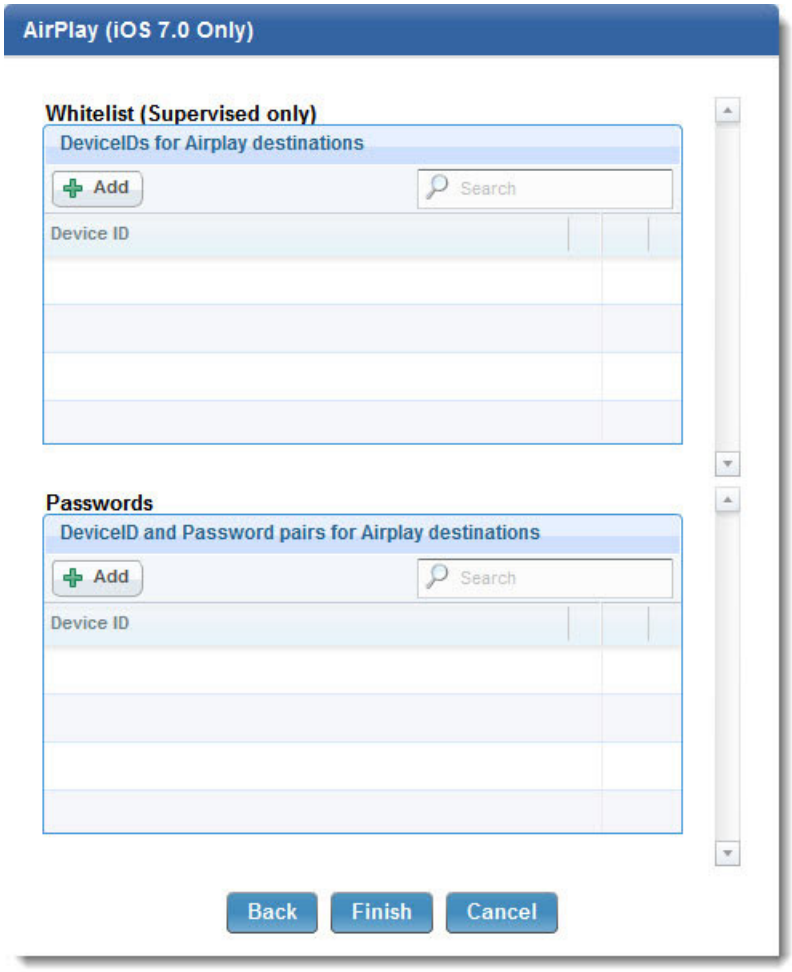
iOS Profile Types

The following profiles can be created or edited.

The iOS profiles that are created in IBM Endpoint Manager for Mobile Device Management are implementations of profiles that are created and maintained by Apple Inc. For detailed information on profile settings, see http://www.apple.com/support/iphone/enterprise/

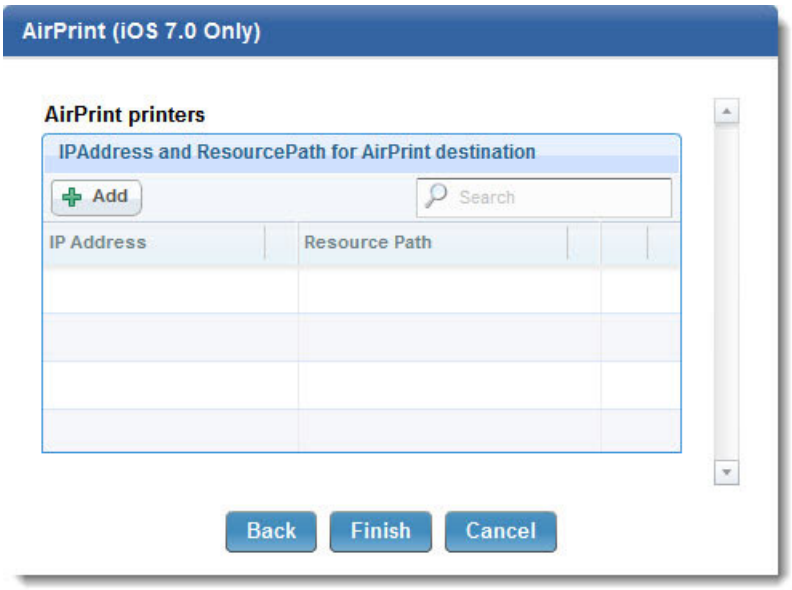
AirPlay (iOS 7.0+)

This profile allows the definition of paired AirPlay devices and associated passwords. In addition, a device whitelist can be created.

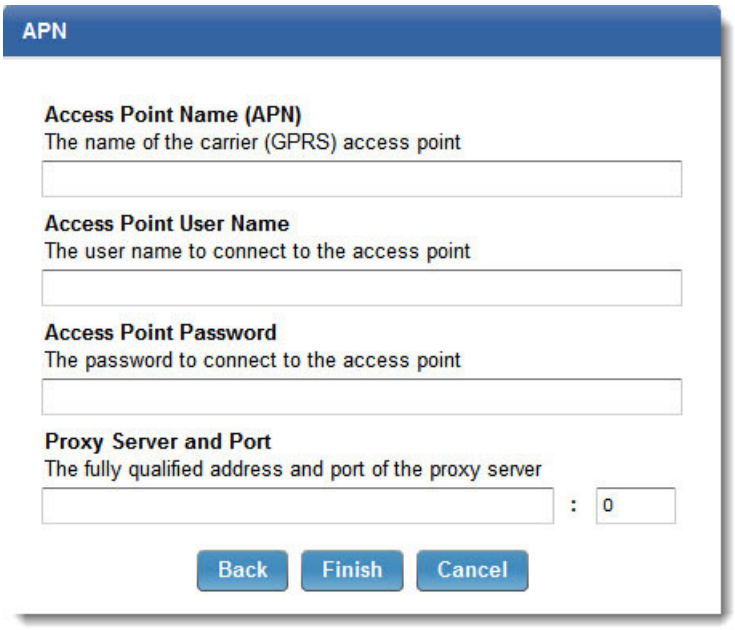


AirPrint (iOS 7.0+)

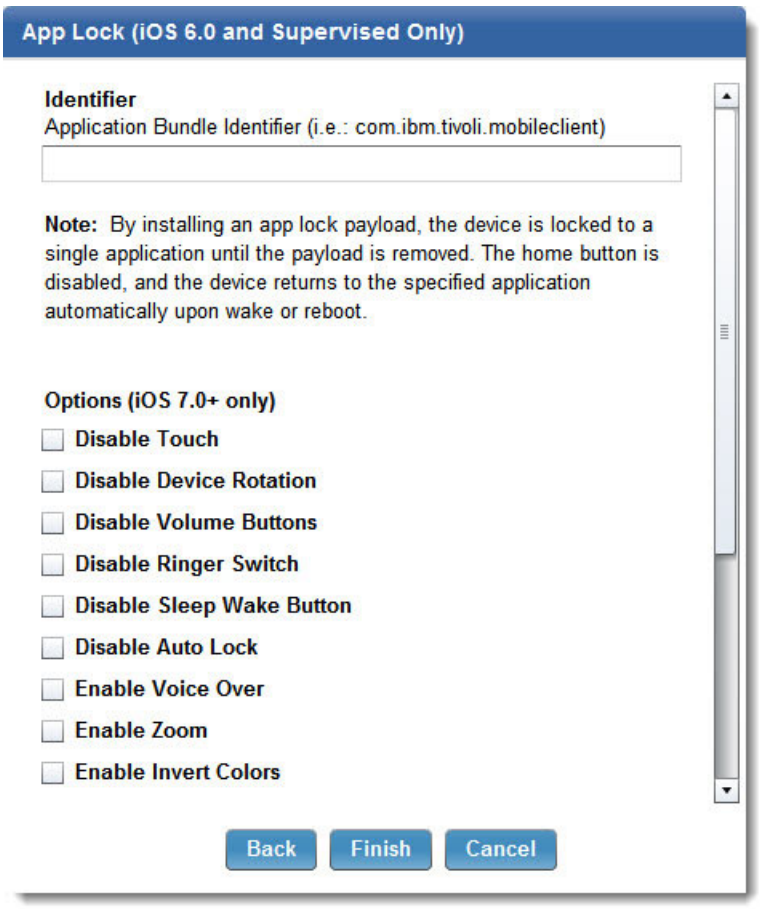
This profile allows the definition of IP addresses and associated resource paths for AirPrint printers.



APN APN settings can be used to change the proxy settings on your network and the Access Point Name (APN) on your devices. These settings define how a device connects to a network. In iOS 7 and later, the APN payload is deprecated in favor of the Cellular payload.

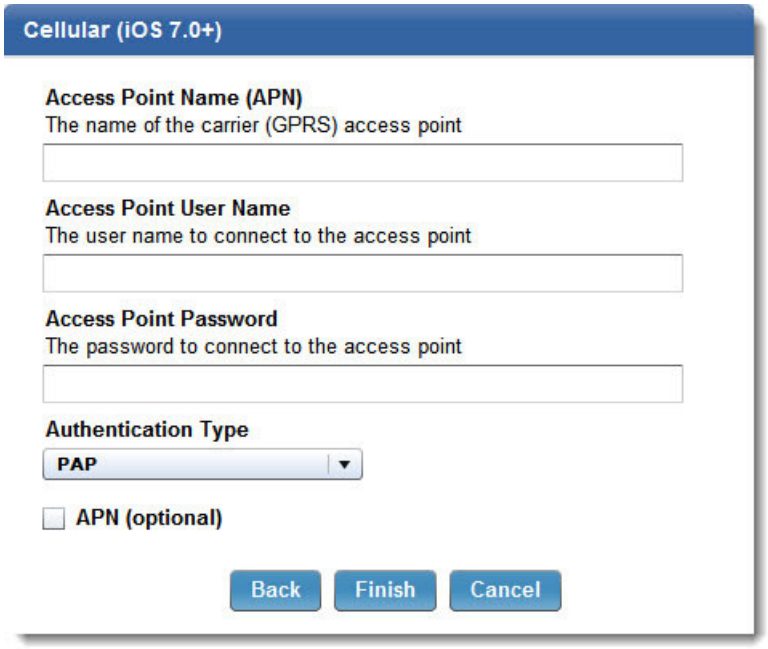


App Lock (iOS 6.0+, Supervised)
An App Lock locks a device to a single app. Enter the application bundle identifier and on devices with iOS 7.0+, define which functions are enabled or disabled during the App Lock.



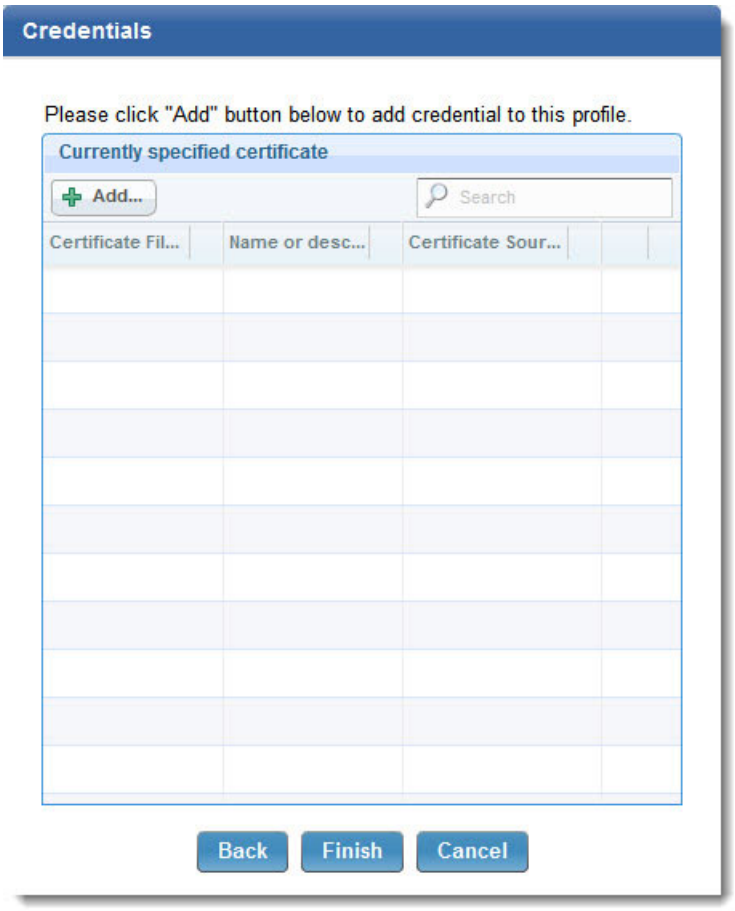
Cellular (iOS 7.0+)

A Cellular profile configures cellular network settings on devices. In iOS 7 and later, the APN profile is deprecated in favor of the Cellular profile.

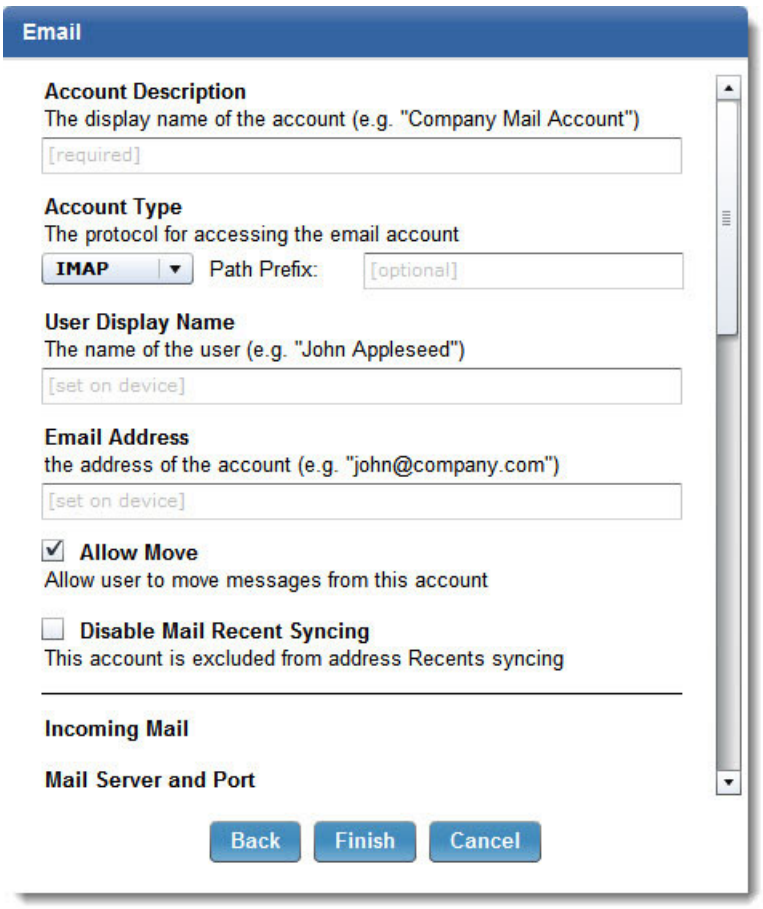


Credentials

This profile allows certificates to be installed on a device. Define the certificate type and designate the import parameters or select a specific certificate file.

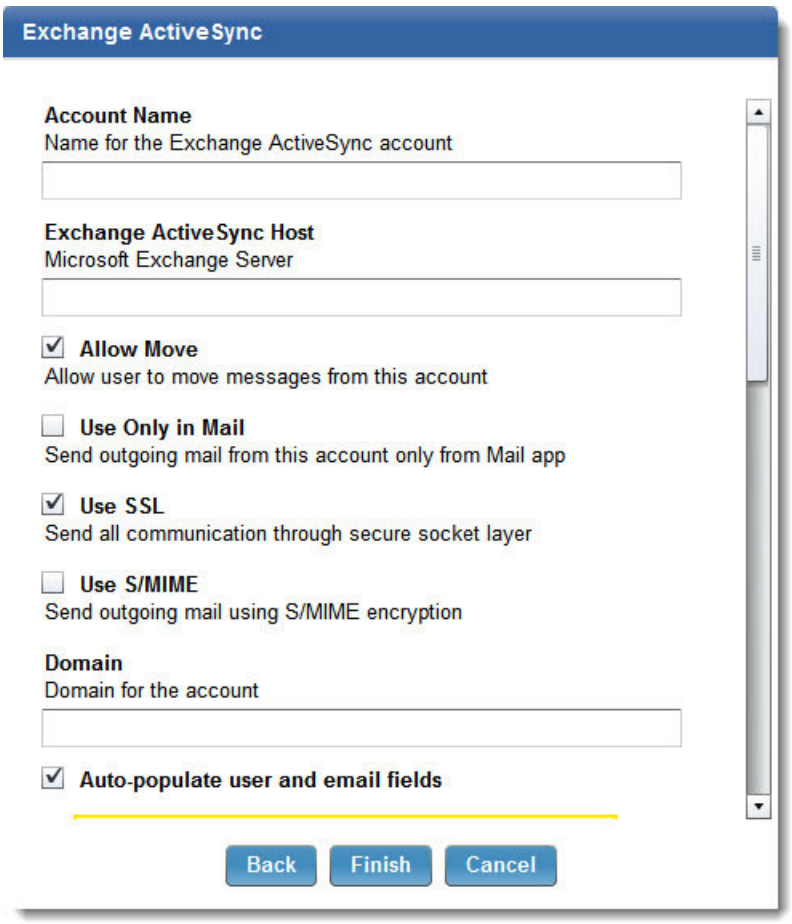


Email Use the email profile to configure POP or IMAP mail accounts. Users can modify some of the mail settings you provide in a profile, such as the account name, password, and alternative SMTP servers. If you omit any of this information from the profile, users are asked to enter it when they access the account.

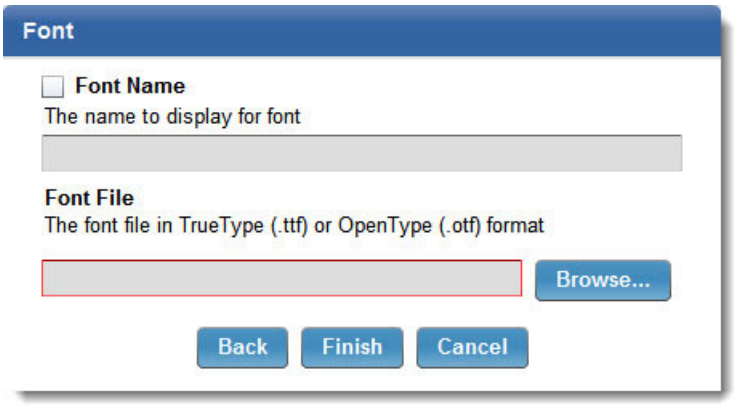


Exchange ActiveSync

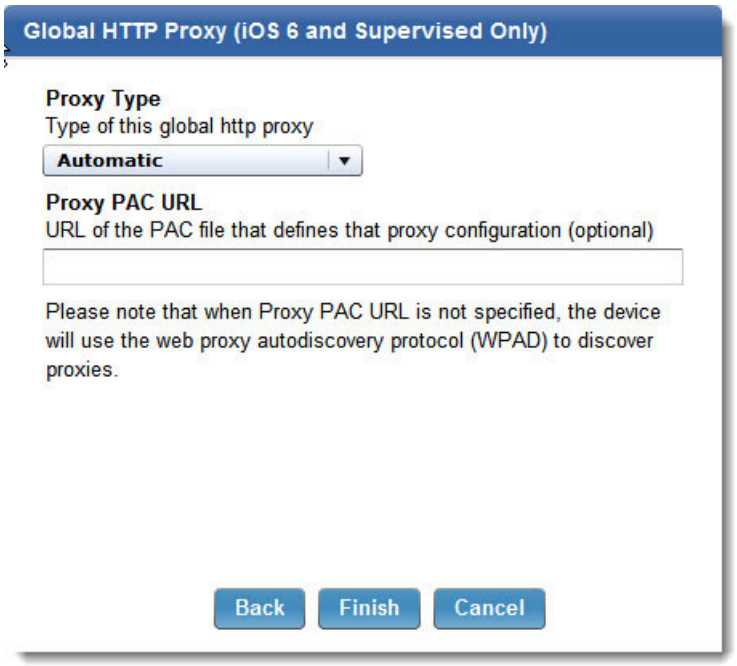
Use this profile to enter user settings for a Microsoft Exchange server. You can create a profile for a particular user by specifying the user name, host name, and email address, or you can provide just the host name. Users are prompted to complete the other values when they install the profile.



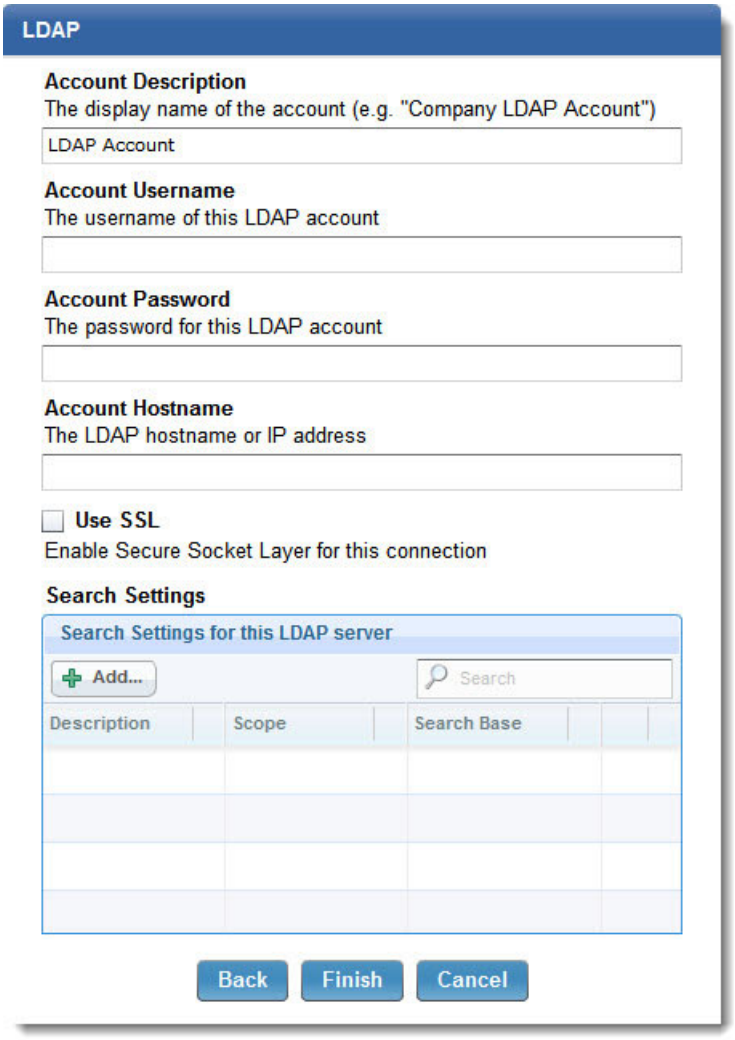
Font This profile allows a custom font to be defined. Select a custom font name, if wanted, and navigate to a TrueType or OpenType font file.



Global HTTP Proxy (iOS 6.0+, Supervised)
This profile is used to specify a proxy for all HTTP traffic to and from the target device. If you choose manual proxy type, you need the proxy server address and its port, and optionally a user name and password for logging in to the proxy server. If you choose auto proxy type, you can enter a proxy auto-configuration (PAC) URL.

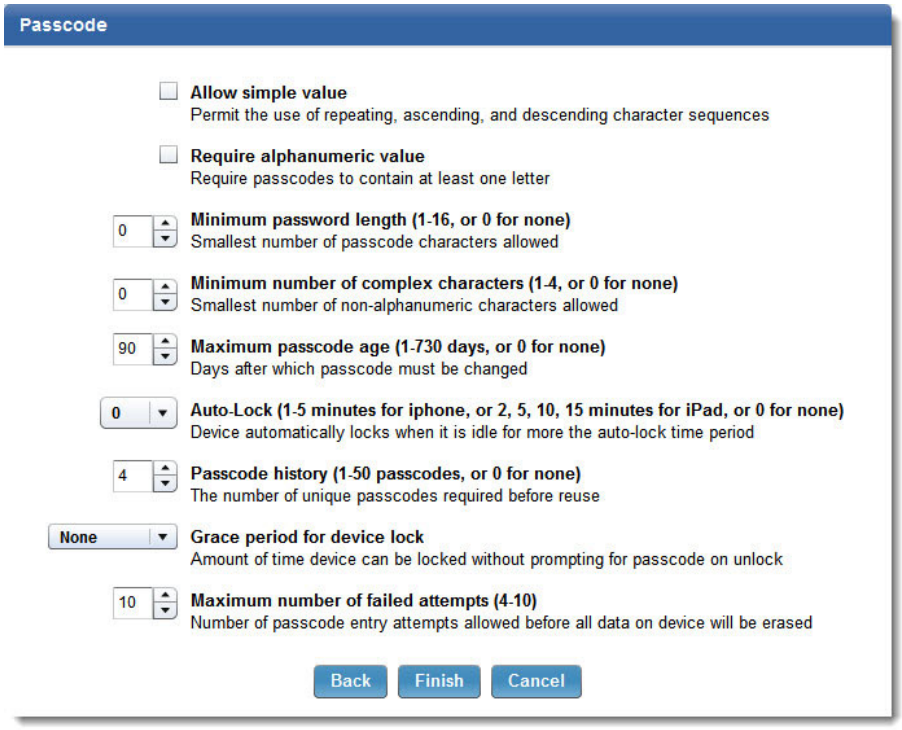


LDAP Use LDAP profiles to configure target devices to connect an LDAPv3 directory. Choose a display name and define the user name, password, and location of the LDAP server. Custom search settings can be defined by standard LDAP attribute aliases.



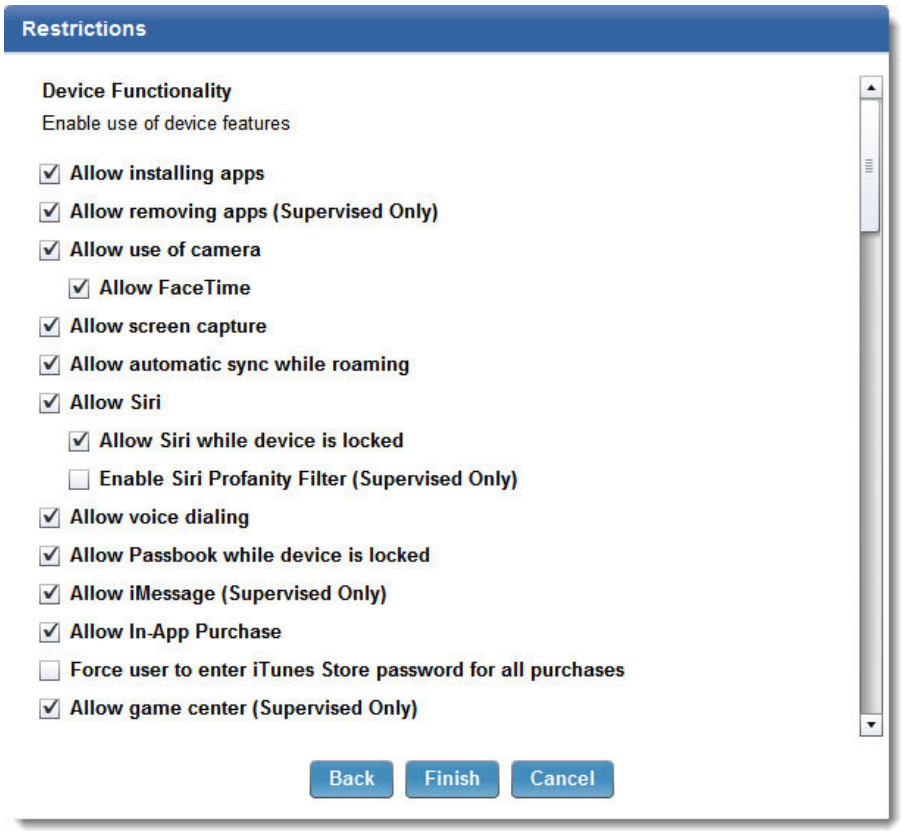
Passcode

This profile sets device password policies if you are not using ActiveSync policies. You can specify whether a passcode is required to use the device, and specify characteristics of the passcode and how often it must be changed. When the configuration profile is assigned to a device, the user is asked to enter a passcode that meets the policies you specify. Otherwise, the profile is not installed.

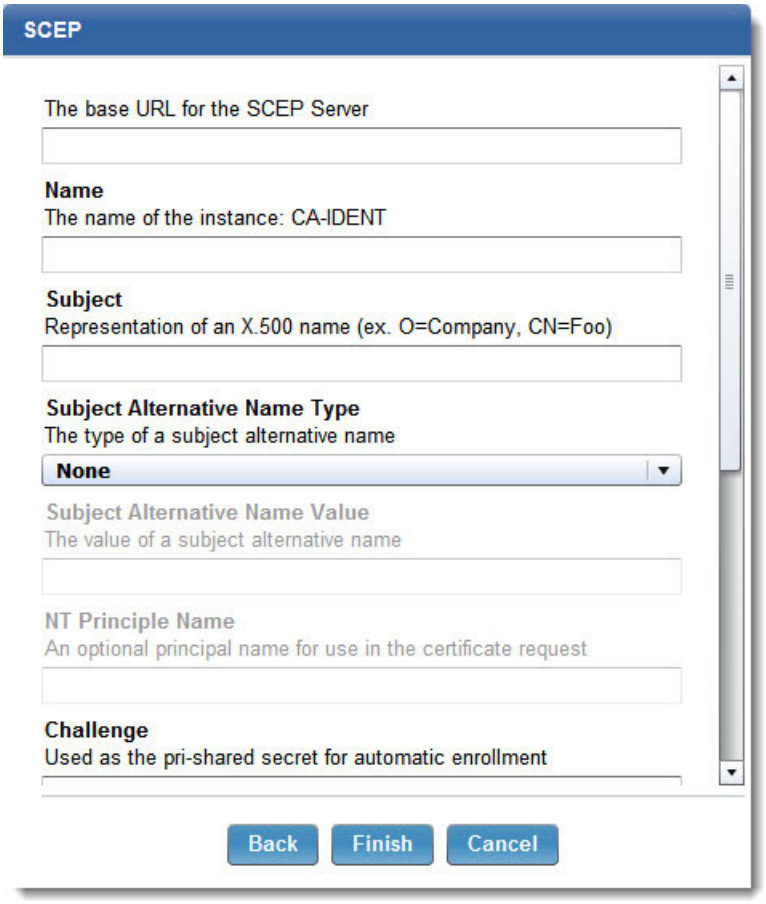


Restrictions

The Restrictions setting can be used to specify which device features are permitted on devices in your deployment. Some settings require supervision mode to be enabled, or require iOS 7.0+.



SCEP The Simple Certificate Enrollment Protocol (SCEP) feature can be used to specify settings that allow a device to obtain certificates from a certificate authority.

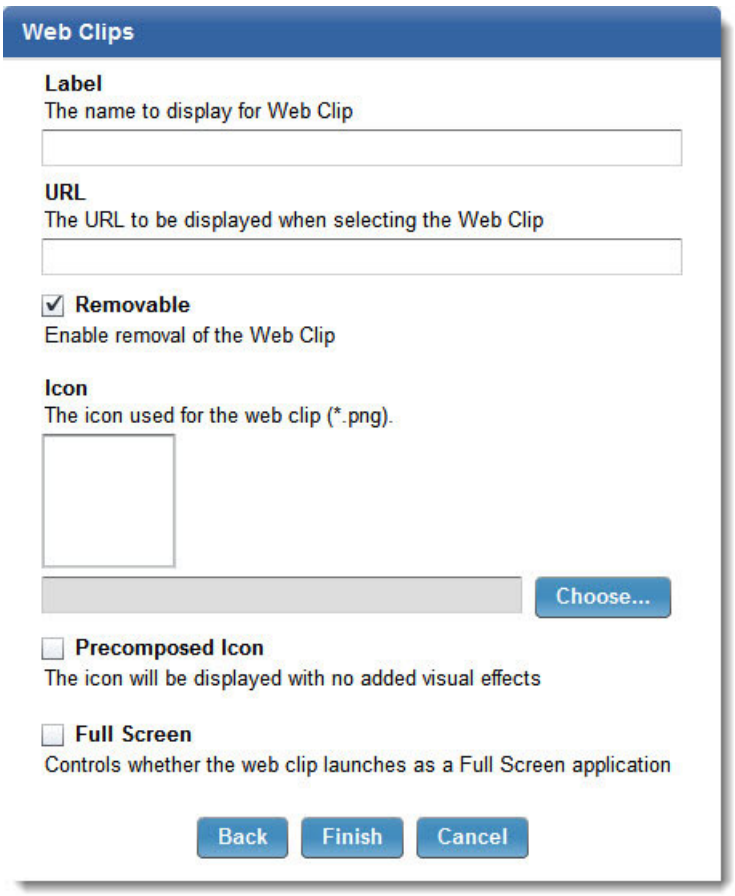


Single Sign-On Account (iOS 7.0+)
This profile configures a device to use a Kerberos based Single Sign-On (SSO) account for authentication.

VPN This profile configures a device to use a Virtual Private Network (VPN) for secured communication. For detailed information on this profile, see "VPN Profile and App Association" on page 45.

Web Clips

This profile allows the creation of a Web Clip to be displayed on target device's home screen. Web Clips are shortcuts that allow quick access to webpages or other various links.

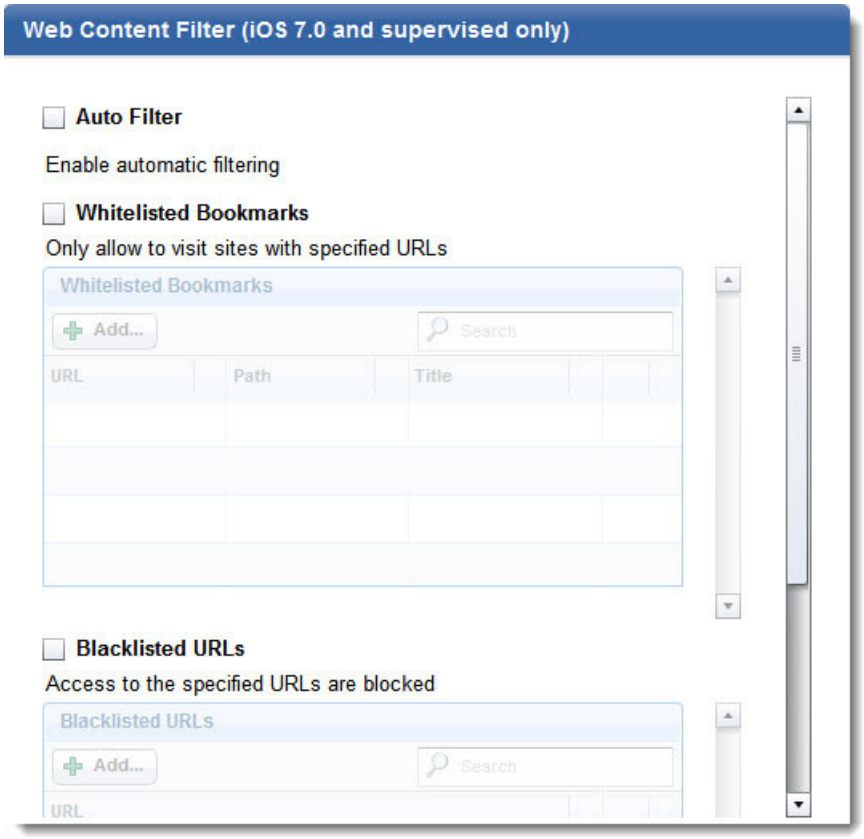


Web Content Filter (iOS 7.0+, Supervised)

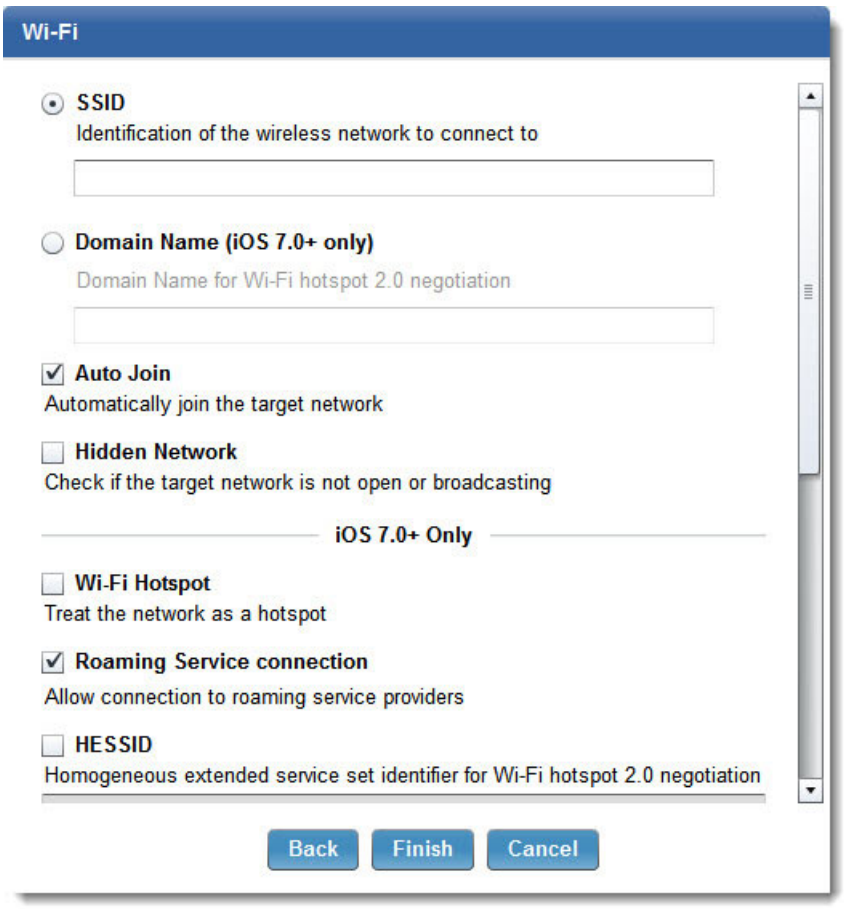
This profile allows control over the web content targeted devices can access. A whitelist or blacklist of URLs can be created. Automatic filtering can be enabled, and safe URLs can be permitted even if automatic filtering would otherwise block them.

Note: When multiple web content filters are assigned to a device:

- The blacklist is the union of all blacklists. Any URL that is present in any blacklist is inaccessible.
- The permitted list is the intersection of all permitted lists. Only URLs that are present in every permitted list are accessible when they would otherwise be blocked by the automatic filter.
- The whitelist is the intersection of all whitelists. Only URLs that are present in every whitelist are accessible.



Wi-Fi This profile configures target devices to use a specified Wi-Fi connection. Enter the connection's SSID and the appropriate settings such as the security type. Several features require iOS 7.0+.



VPN Profile and App Association

The VPN profile configures a device or iOS app to use a Virtual Private Network for secure communication.

After you enter relevant information in the **Identifier** window, as is done with all profiles, continue to the **VPN** window to configure the available parameters. The type of VPN determines the settings that are required to configure the connection. The following settings are universal to all VPN types:

Connection Name
Choose a connection name that is displayed on target devices.

Connection Type
Select the type of connection. The following connection types are available:

- L2TP
- PPTP
- IPSec (Cisco)
- Cisco (AnyConnect)
- Juniper SSL
- F5 SSL
- SonicWall Mobile Connect
- Aruba VIA
- Custom SSL

Server Enter the host name or IP address of the server.

Account

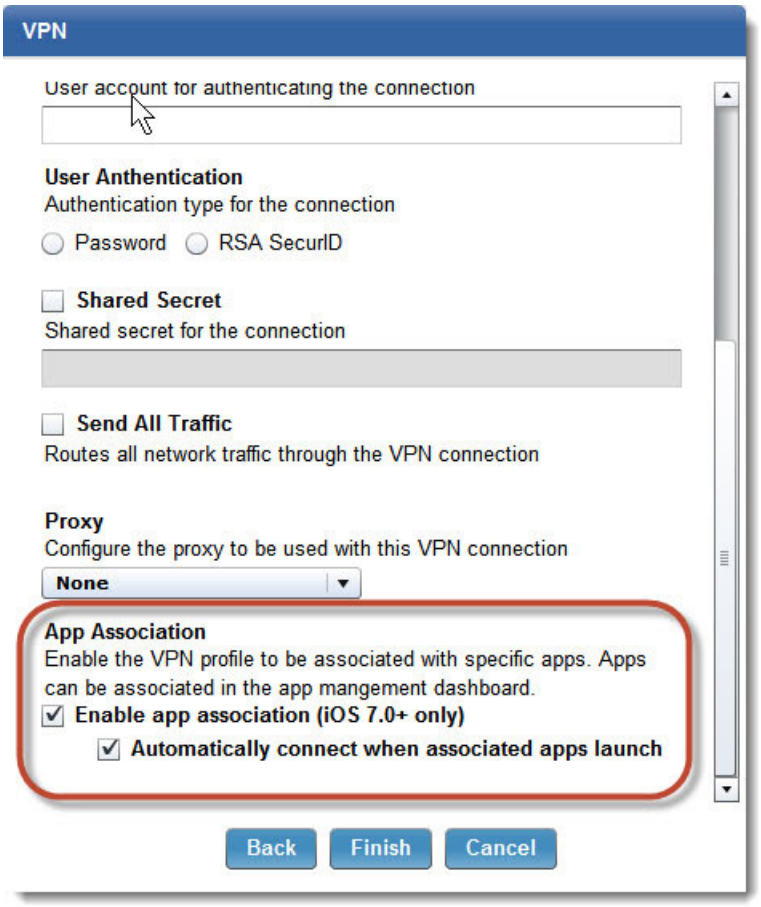
Enter the user account that is used to authenticate the connection.

Proxy Select the type of proxy that is used for the VPN. The options are None, Manual, or Automatic. For a manual proxy, enter the server address and port. For an automatic proxy, enter the server from where the proxy settings are obtained.

App Association

In iOS 7.0+, VPN profiles can be associated with specific iOS apps. App association enables secure communication on a per app basis. This process starts with the creation of a VPN profile. This profile is then assigned to iOS apps using the Enterprise App Management dashboard. For more information, see "App Management Tasks" on page 92.

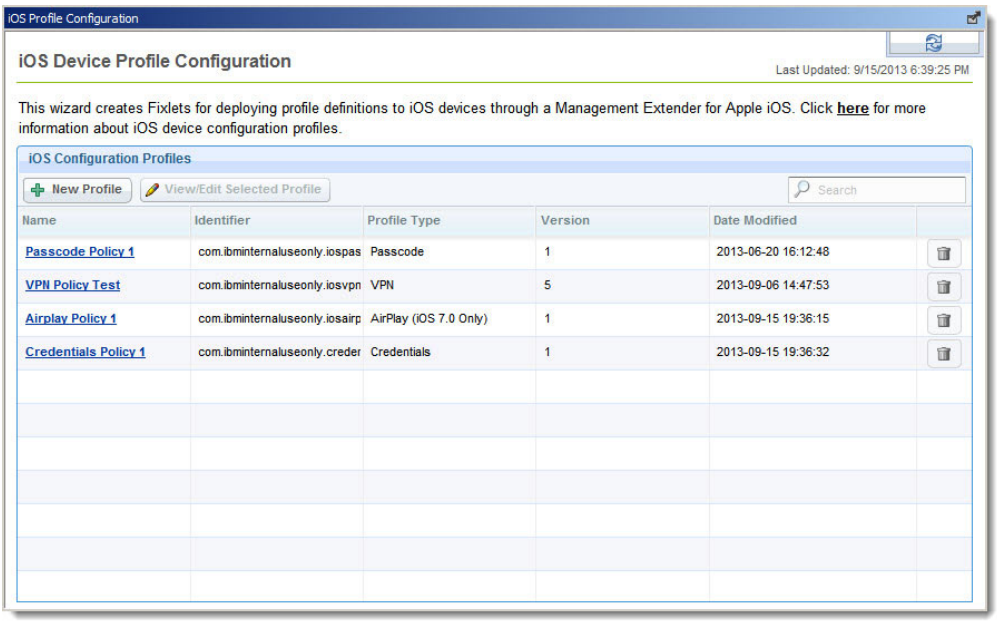
Select the check box to enable app association with this VPN profile. To force apps to automatically connect to the VPN when they are started, select the associated check box.



Manage and Assign iOS Configuration Profiles

iOS Profiles that are created are listed in the iOS Profile Configuration dashboard.

The profile's **Name** and **Identifier** are listed as designated during profile creation. The profile type and last date the profile was modified are listed. The **Version** number that is listed for each profile designates how many times the profile was edited.



To delete an iOS Profile, click the trash icon to the right of a profile. An iOS profile cannot be deleted if it is assigned to any iOS devices. For more information about removing an iOS Profile, see "Remove an iOS Configuration Profile" on page 47.

After an iOS Profile is created as a Fixlet, it can be run like any other action. Do so by clicking the name of the iOS Profile to open the action window where relevant devices can be selected after you click **Take Action**.

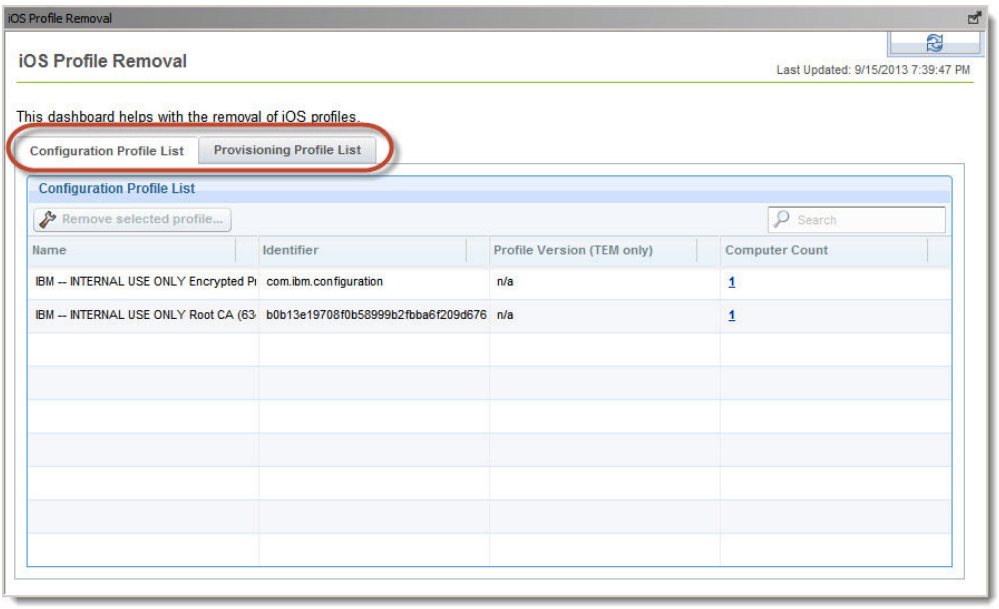
Note: iOS Configuration Profiles can also be found listed as Fixlets by navigating to **Mobile Device Management > Apple iOS Settings > Apple iOS Profiles**. Running them from this location is the same as clicking the profile name from the **iOS Profile Configuration** dashboard.

Remove an iOS Configuration Profile

iOS Configuration Profiles that are assigned to iOS device are listed in the **iOS Profile Removal** dashboard. This dashboard is used to remove profiles from assigned devices.

The iOS Profile Removal dashboard can be found by navigating to **Mobile Device Management > Apple iOS Settings > iOS Profile Removal**.

Note: You might be required to activate analyses for the dashboard to function. If so, a yellow warning banner is displayed at the top of the dashboard. Click **Activate** to turn on the listed analyses.



Two tabs at the top of the dashboard are used to display configuration or provisioning profiles. Any iOS Profiles currently assigned to an iOS device is listed in the dashboard, and the number of devices assigned to the profile is shown in the **Computer Count** column.

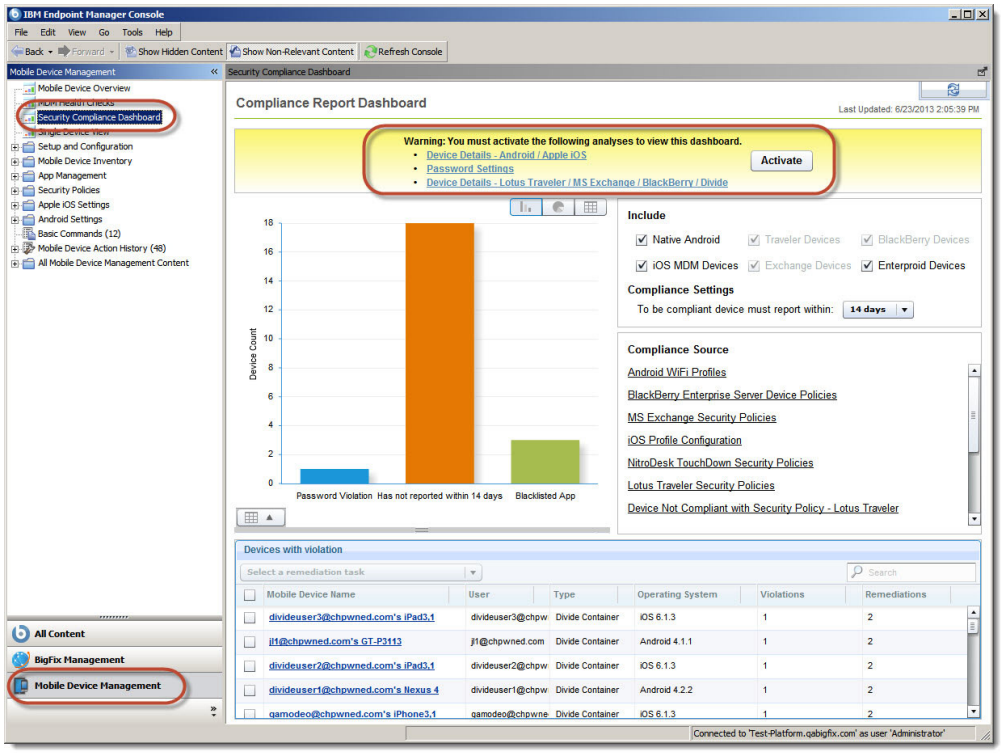
To remove a profile from currently provisioned devices, select the profile's row and click **Remove Selected Profile**. The standard action window is displayed where you can select relevant devices. The iOS Profile is removed from the selected devices.

Security Compliance Dashboard

IBM Endpoint Manager for Mobile Devices allows administrators to set up various security policies. The Security Compliance Dashboard provides a unified interface to view security violations as a whole or by individual device.

To access the Security Compliance Dashboard, select the **Mobile Device Management** site and click **Security Compliance Dashboard** from the tree on the left. The Security Compliance Dashboard is displayed on the right.

Note: You might be required to activate analyses for the dashboard to function. If so, a yellow warning banner is displayed at the top of the dashboard. Click **Activate** to turn the listed analyses on.



Security Compliance Dashboard layout

The Security Compliance Dashboard contains several discrete areas that perform various functions.

The Security Compliance Dashboard is composed of the following areas:

- Summary graphic
- Compliance filters
- Compliance source
- Devices with violations

Summary graphic

The summary graphic area of the Security Compliance Dashboard displays a graphical representation of the devices that are in violation of policies that are defined in your deployment. A graph displays information about each type of violation in addition to the number of devices that are in violation.

The graph summarizes four types of violations:

- Password Violations
- Jailbroken Status
- Device Reporting Delays
- Blacklisted Apps

Use the three buttons in the upper-right corner to display a bar graph, pie chart, or table view.

When you view a bar graph or pie chart, a button in the lower left provides a small table similar to the table view.

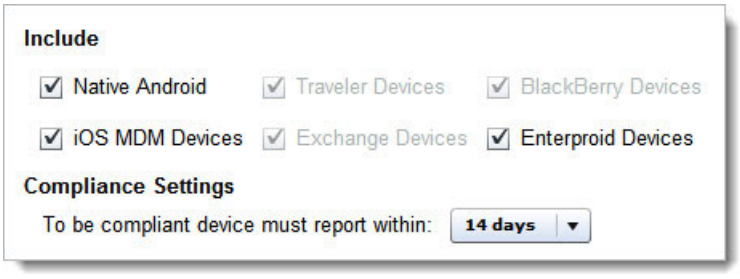
Compliance filters

The upper-left area of the dashboard determines the types of devices that are included in the analysis. You can also edit the threshold for inclusion of devices that have not reported recently.

You can filter the following device types according to the extenders that manage them.

- Native Android devices
- Lotus Traveler devices
- BlackBerry devices (BlackBerry OS 7.0 and earlier)
- iOS devices
- Exchange devices
- Enterproid Divide devices

The drop-down menu changes the threshold for devices that have not reported recently. Any device that has failed to report within the timeframe indicated here is listed as a violation.



Compliance Source

The Compliance Source area of the Security Compliance Dashboard lists the data sources for the information that is represented in the dashboard. Each item links to the associated dashboard, task, or analysis. This list provides a starting point for determining why devices are in violation.

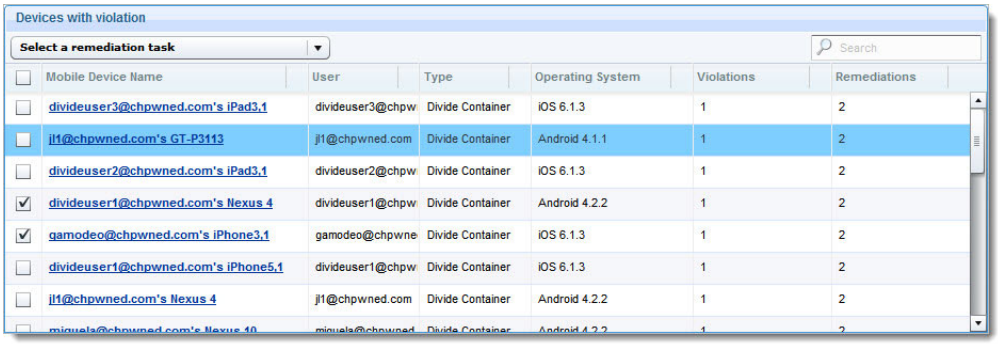
Devices with violations

The lower area of the Security Compliance Dashboard displays a table that lists the details of any devices that are reporting one or more violations.

The devices that are listed here can be filtered, see "Compliance filters" on page 85.

Click the device name to open the device's computer entry in the console. Click **Back** to return to the Security Compliance Dashboard.

Point to the **Violations** column for any device to display the exact violations that are reported. Similarly, the **Remediation** column lists the actions that can solve the reported violations.



You can select one or more devices by their associated check box. After you select devices, the **Select a Remediation Task** menu becomes accessible. This menu lists any tasks that apply to the selected devices. Selected tasks apply only to devices and violations that meet the requirements. If any selected devices must be excluded from the selected action, a window is displayed detailing which devices are excluded.

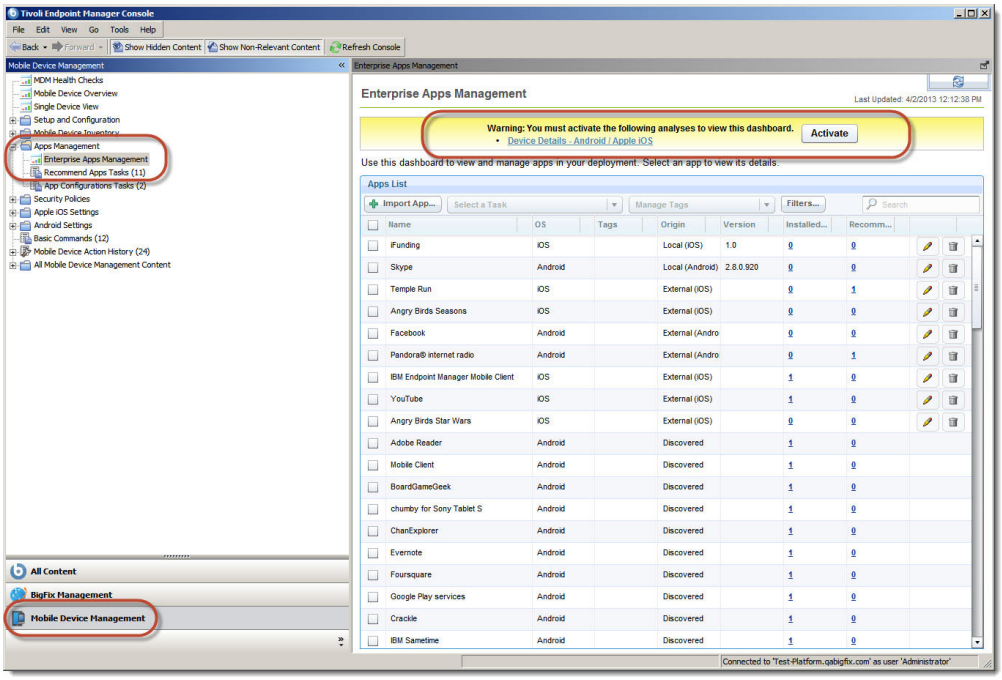
App Management

The Enterprise Apps Management dashboard presents a unified inventory of Apple iOS and Android mobile apps. Apps can be imported into this dashboard from multiple sources. After you import apps, they can be managed throughout your MDM deployment by using filters, tags, redemption codes, and other features.

The Enterprise Apps Management dashboard is found within the **Mobile Device Management** site at the following location in the navigation tree on the left of the console:

Apps Management > Enterprise Apps Management

Before you work with the dashboard, check whether there are any yellow notifications at the top of the dashboard that require your attention. Follow the directions that are provided to enable dashboard functions if necessary.



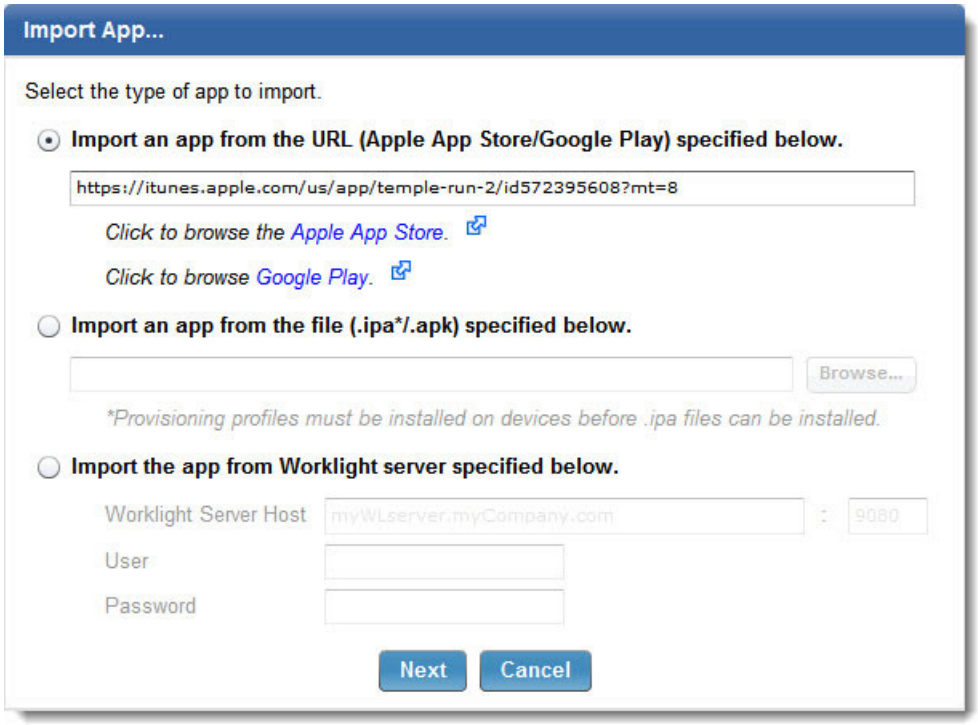
Import Apps

The first step in managing iOS and Android apps in your deployment is to populate the Enterprise App Management dashboard with apps from various sources.

To begin importing apps, click **Import App**. From the **Import App** window you can define three sources of apps:

- Apps can be imported by their Apple App Store or Google Play URL by extracting the metadata for the specified app to fill the Enterprise App Management dashboard. Apps that are imported in this way are called **external apps**.
- If you have access to IPA or APK files, you can import these files directly by copying them to your IBM Endpoint Manager Server and importing their metadata into the Enterprise App Management dashboard. Apps imported in this way are called **local apps**.

- A Worklight Server can be specified as a source of apps. This option requires the hostname of the Worklight Server in your network and a user name and password to access it. Apps imported in this way are also called **local apps**.



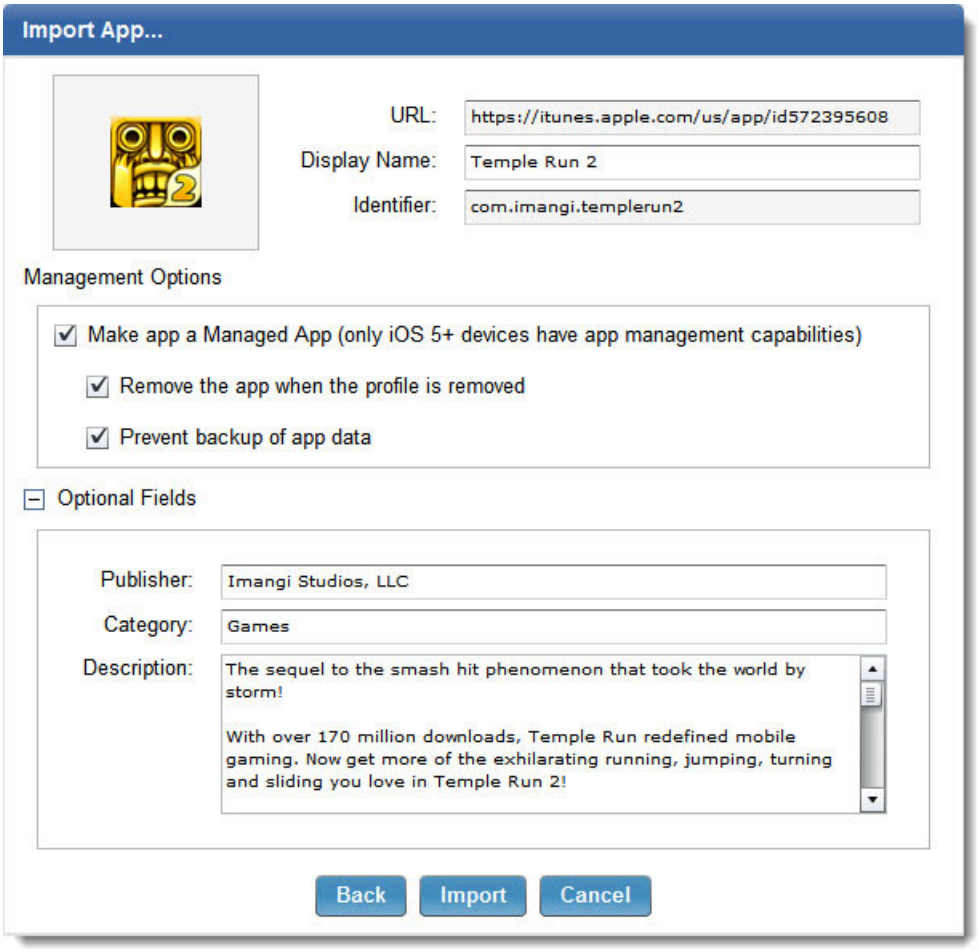
After selecting the source of the app, click **Next**. The following window displays the app metadata and several options:

URL The URL where the app is located. If the app was imported from an external URL, that URL is displayed here. If imported from an IPA or APK, the URL points to the copy of the app now located on the IBM Endpoint Manager Server.

Display Name
The name displayed in the Enterprise Apps Management dashboard. You can edit this field.

Identifier
The unique identifier obtained from the app metadata.

Version
The version and release of the app.



Apple iOS Managed Apps

The **Management Options** section of the **Import App** window specifies whether the imported iOS app is designated as an iOS Managed App. This option is present only when you import Apple iOS apps.

Check the associated box to enable extended features in device that run iOS 5.0 or later. If this feature is not checked, the management features of this app are severely limited. For example, iOS Managed Apps can be uninstalled and Redemption Codes can be managed through IBM Endpoint Manager. All iOS apps should be imported as Managed Apps.

You can also configure two other options to control iOS Managed Apps:

Remove the app when the profile is removed
: Uninstall this app from a device if that device is unenrolled from your Mobile Device Management deployment.

Prevent backup of app data
: Prevent this app from backing up its data during device synchronization.

Optional Fields

Using the **Optional Fields** section of the **Import App** window you can specify several fields that are associated with the app. This data is only visible to device users when they are presented with recommended apps. These fields might be prepopulated depending on the source of the imported app.

You can specify the following fields:

- **Publisher**
- **Category**
- **Description**
- **Minimum OS Version**: Sets a threshold for recommended apps. Recommended apps are only recommended to devices that run this OS version or later.

App Origin

Depending on how an app is imported into Enterprise App Management, it is assigned a different origin value. An app's origin dictates the types of management features that can be performed on the app. It is important to understand the concept of app origin and how this value is assigned.

Discovered
Discovered apps are apps that are found installed on managed devices. These apps were not imported into Enterprise Apps Management. Few management options are available for Discovered apps. If an app listed as discovered is later imported using the **Import App...** button, the app will be categorized as either internal or external depending on the import method.

External
External apps are apps that are imported using a URL from the Apple App Store or Google Play. These apps are not stored locally on the IBM Endpoint Manager Server.

Local Local apps are imported into Enterprise Apps Management directly by their IPA or APK file. Apps that are imported from a Worklight Server are also treated as local apps. When an app is imported, a copy of its IPA or APK is made on the IBM Endpoint Manager Server. Apps that are imported from a Worklight server are denoted as **Local (Worklight)**.

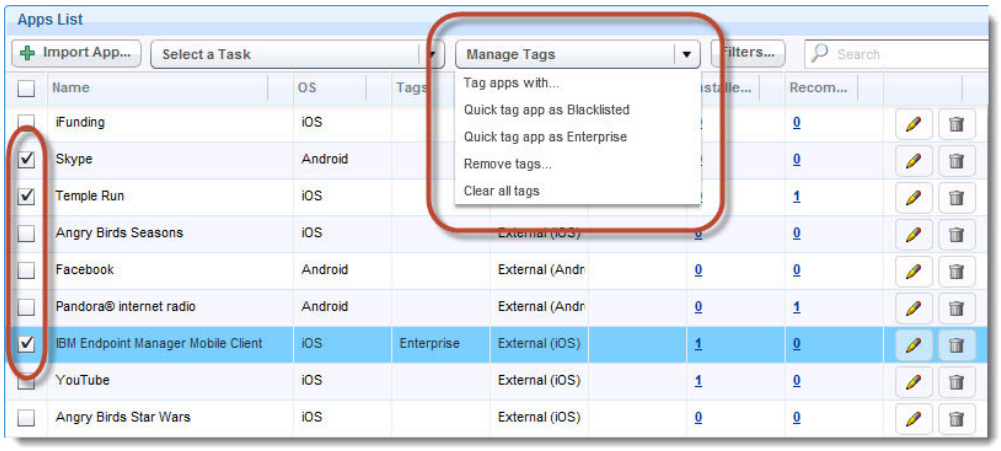
App Management Tags

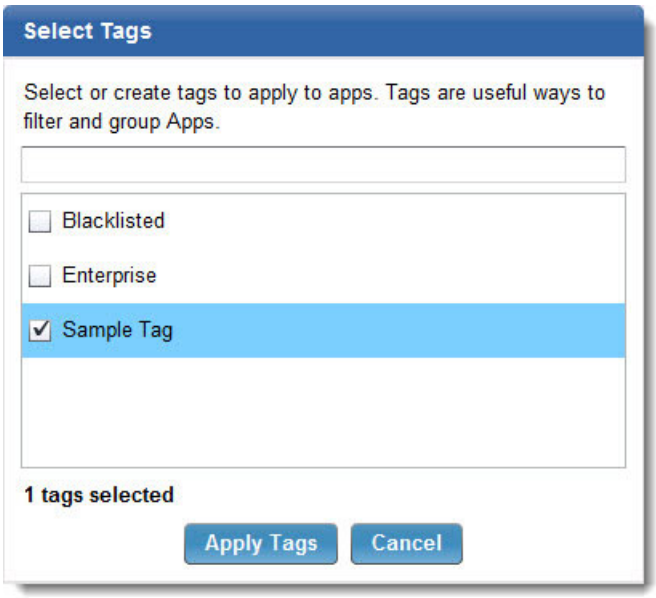
Apps that are imported into the Enterprise Apps Management dashboard can be assigned user-defined tags to help in their organization. Apps can be filtered by their tags.

To tag a selection of apps, or to define a new tag, perform the following steps:

1. Check the box next to any apps that you want to tag.
2. Select the **Manage Tabs** menu:
   a. To tag the checked apps with a single tag that is already defined, select that tag from the list. For example, **Quick tag app as Enterprise**.
   b. Select Tag apps with... from the menu to apply a single existing tag, multiple existing tags, or to define a new tag.
3. In the **Select Tags** window, select any tags that you want to apply to the chosen apps, or type a new tag description and click **Create New**.
4. With one or more selected tags, click **Apply Tags**.

Apps can have multiple tags that are applied to them. By checking an app with one or more tags and selecting the **Manage tags** menu, you can remove individual tags or clear all tags that are applied to the checked apps.





App Management Filters

You can control the apps that are displayed in the Enterprise Apps Management dashboard by applying filters. Click **Filters...** to display the **Additional Filtering Options** window.

You can filter apps by several criteria:

Platform

Choose to filter apps by their operating system, either iOS or Android.

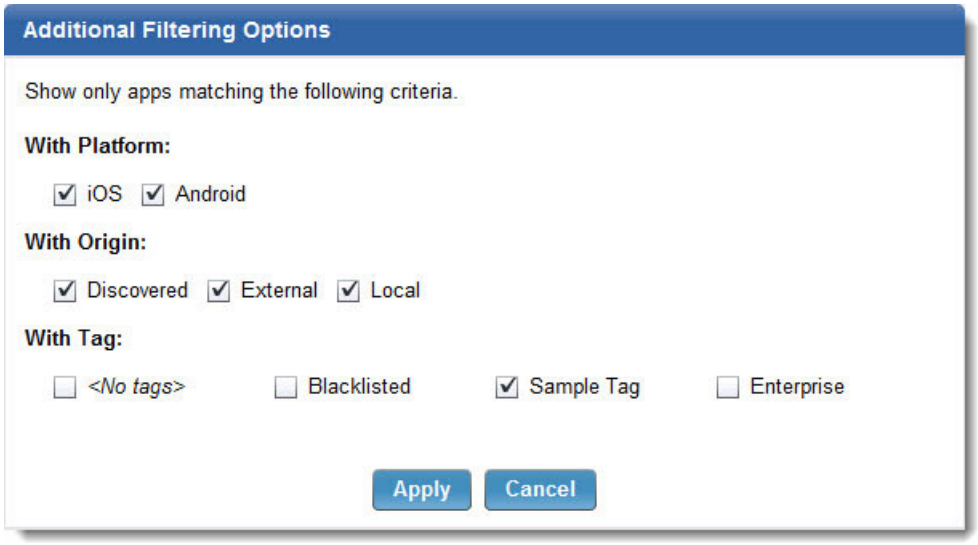
Origin

The original source of an imported app determines its origin. The origin of an app dictates the app management functions available when you manage the app.

- **Discovered**: Discovered apps are installed on user devices. Generally you cannot manage these apps, unless they are on Samsung SAFE enabled devices.
- **External**: External apps were imported by their store URL
- **Local**: Local apps are locally hosted and were imported directly from their IPA or APK file. After you import the app, a copy of the IPA or APK file is available on the IBM Endpoint Manager Server.

Note: More detailed information about the different types of app origin can be found here: "App Origin" on page 90

Tag Tags can be defined to help organize apps; they serve no purpose other than to help categorize apps.

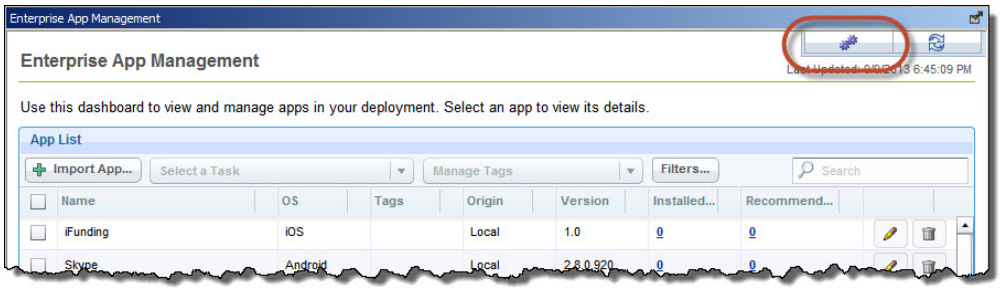


App Management Tasks

You can work with apps listed in the Enterprise Apps Management dashboard by using various tasks.

Check the box of one or more apps and select the **Select a Task** menu to see a list of tasks that relate to the checked apps. Not all tasks can be performed on all apps.

When a task is selected, the standard **Take Action** window is displayed by default. Select the devices that you want to perform the selected task on. Alternatively, instead of performing immediate actions, Fixlet tasks can be created allowing the task to be run later. This change in the default behavior is set by clicking the settings icon in the upper right corner of the dashboard.



Check the option to create tasks instead of performing immediate actions. After you select a task the standard **Create Task** window is displayed.

Note: Tasks that are displayed in the **Select a Task** menu correspond to any of the selected apps, even if they do not apply to all selected apps. For example, if an iOS

app and Android app are checked, both the **Recommend Android apps** and **Recommend iOS apps** tasks are displayed even though these tasks relate only to a subset of the checked apps.

iOS Tasks

You can apply the following tasks only to Apple iOS apps. Most of these tasks require that the app is an iOS Managed App, which you can configure when you import the app into Enterprise App Management.

Note: Apps that were not installed through IBM Endpoint Manager are not iOS Managed Apps. For example, if a device user installs an app from the Apple App Store directly, this app is not an iOS Managed App and cannot be targeted by tasks such as **Uninstall Apps** and **Prompt Install Apps**.

Associate with VPN Profile
This task is used to associate the checked app with a previously created VPN profile. The VPN profile must be configured with App Association. For more information, see "Apple iOS Profiles" on page 28. A window is displayed where a qualifying VPN profile is selected to be associated with the checked app. This task can be performed on iOS Managed Apps only.

Disassociate with VPN Profile
This task removes a VPN profile from the checked app if a VPN profile was previously associated with it.

Prompt Install iOS Apps (iOS 5.0+)
This task sends a notification to the target device to install the checked app and also recommends the app. Device owners can cancel this procedure, but the app is still listed as a recommended app. You can perform this task on both local and external iOS apps, but only if the target devices are running iOS version 5 or later. This task applies only to free apps or paid apps that have redemption codes available. This task can be performed only on iOS Managed Apps.

If the app is already installed on the target device, this task updates the app to the local version the task is being performed on. If an External app, the latest version on the Apple App Store is installed.

Note: When you prompt an app to install on supervised devices with iOS 7+, the app is installed in the background without user notification. The app is not listed as a Recommended App.

Recommend iOS Apps
Checked apps are recommended to the selected iOS devices. These apps display in the IBM Endpoint Manager Mobile Client as Recommended Apps. This task is applicable only to local and external iOS apps. This task applies only to free apps or paid apps that have redemption codes available. Apps are recommended only to devices that run the minimum OS version that is set in the **Optional Fields** metadata.

Uninstall iOS Apps
This task uninstalls the checked iOS app from selected devices without notification to the device user. This task is available only to local or external apps that are set as Apple iOS Managed Apps. The target devices must be running iOS version 5 or later.

Unrecommend iOS Apps
This task removes the checked iOS apps from the recommended apps

section of a device's IBM Endpoint Manager Mobile Client if the app was already recommended. This task is available only to local and external iOS apps.

Android Tasks

The following tasks apply only to Android apps. Several of the following tasks can be performed only on SAFE enabled devices.

Prompt Install Android Apps
This task sends a notification to the target device to install the checked app and also recommends the app. Device owners can cancel this procedure, but the app is still listed as a recommended app. You can perform this task on both local and external Android apps.

Recommend Android Apps
Checked apps are recommended to the selected Android devices. These apps display in the Recommended Apps section of the IBM Endpoint Manager Mobile Client. This task is applicable only to local and external Android apps. Apps are recommended only to devices that run the minimum OS version that is set in the **Optional Fields** metadata.

Silently Install Apps (Using SAFE)
This task installs the checked app without notification to the device user. This task is available only to local Android apps and it can be performed on SAFE enabled devices only.

Silently Uninstall Apps (Using SAFE)
This task uninstalls the checked app without notification to the device user. This task is available to local, external, and discovered Android apps and it can be performed on SAFE enabled devices only.

Silently Upgrade Apps (Using SAFE)
This task upgrades the checked app to the local version without notification to the device user. This task is available only to local Android apps and can be performed on SAFE enabled devices only.

Prompt Uninstall Android Apps
This task sends a notification to the target device to uninstall the checked app. Users can cancel this request.

Unrecommend Android Apps
This task removes the checked Android apps from a device's Recommended App section of the IBM Endpoint Manager Mobile Client. This task is available only to local and external Android apps.

Wipe User App Data (Using SAFE)
This task deletes the data that is associated with the checked app, but leaves the app otherwise intact. This task can be performed on local, external, and discovered Android apps, but only on devices that are SAFE enabled.

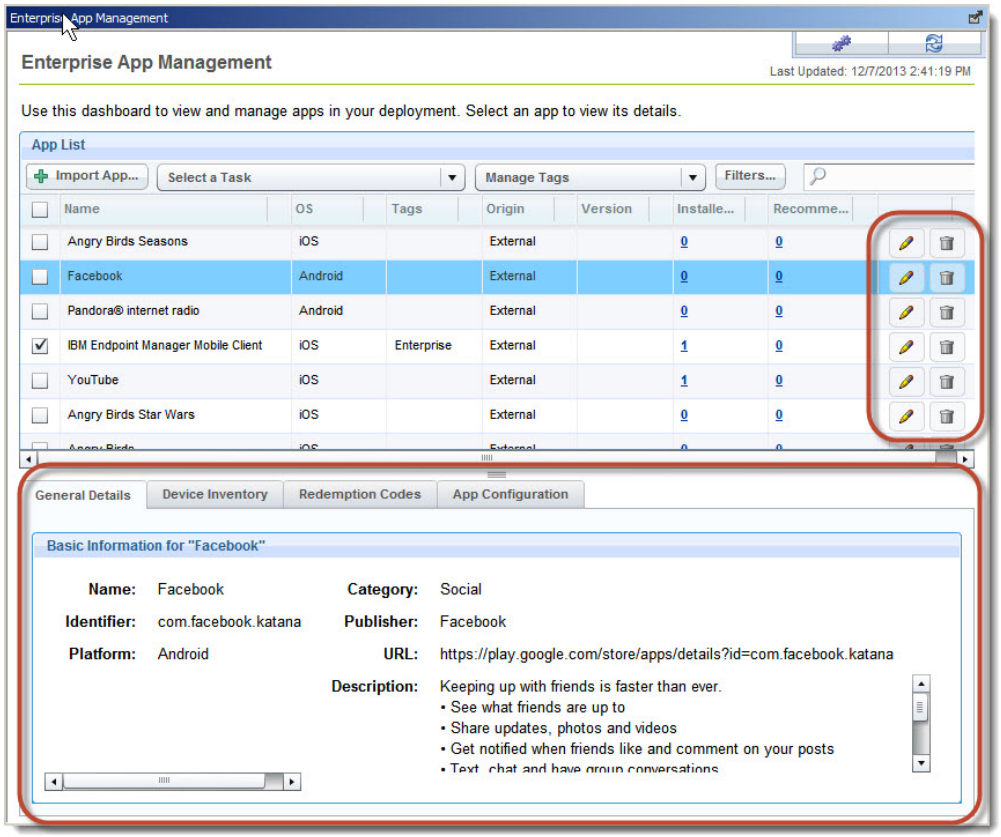
Manage Individual Apps

You can work with apps displayed in the Enterprise App Management dashboard on an individual basis.

You manage an app by selecting its row in the dashboard; selecting a row is different from checking an app's associated check box. When an app is selected, several tabs are shown at the bottom of the dashboard. For more information about these tabs, see the following sections.

Each imported app has an edit and trash button at the right end of its row. The edit button displays the **Import App...** window, which is used to alter the apps management options and optional fields. The fields that can be edited are the same fields that were available during the app import process.

Use the trash button to delete the app from the Enterprise App Management dashboard. This action does not delete the app from any devices, but just removes the app as an imported app. After an app is deleted, it can be imported again later.



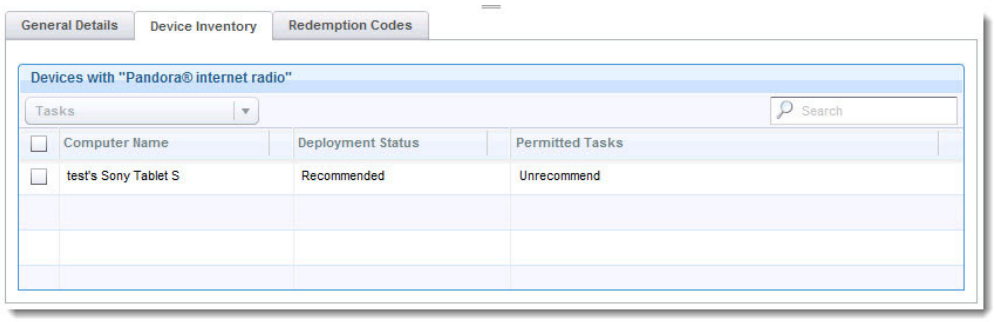
The following tabs can be used to interact with a selected app in various ways:

General Details

The General Details tab displays basic app information that is taken from the app's metadata. This data can also be edited when the app is imported, or by selecting the edit button at the far right of the app row in the dashboard.

Device Inventory

The Device Inventory tab lists the devices that are relevant to the selected app. The **Deployment Status** might include information such as the installed version of the app, or whether the app is recommended to the device. The **Permitted Tasks** column lists all tasks that can be performed on this app on the listed device. Tasks that are listed here can be selected and run from the **Tasks** menu in this tab.



Redemption Codes

The Redemption Codes tab manages redemption codes that are obtained through volume license app purchases with Apple. These codes can be assigned to Redemption Pools, which make them available to Management Extenders and the devices that they manage. For detailed information about managing redemption codes and Redemption Code Pools, see "Redemption Codes."

App Configuration

The App Configuration tab applies only to iOS Apps. In addition, this feature is only compatible with Apple iOS Managed Apps on iOS 7+ devices. Finally, the iOS app must be designed to take advantage of this feature. If the app developer included APIs that allow configuration of the app, the App Configuration tab is where these configurations can be defined and applied. For detailed information about creating and managing App Configurations, see "App Configuration" on page 99.

Redemption Codes

You can purchase iOS apps by volume license. Individual app licenses are represented by 12-character redemption codes. Redemption codes can be made available to all of your managed iOS devices, or to a subset of them. Redemption codes apply only to iOS apps that are non-free and that were imported as external, Apple iOS Managed Apps.

Redemption Codes are assigned to user-configured containers called Redemption Pools. When created, a Redemption Pool is assigned to a Management Extender. After a pool is created, redemption codes are entered into the pool. iOS devices, which are managed by the Management Extender that the pool is assigned to, can be provisioned to use the codes in the pool.

To be able to perform the tasks **Prompt Install Apps** and **Recommend iOS Apps** on non-free iOS apps, the app must have available redemption codes that are assigned to it.

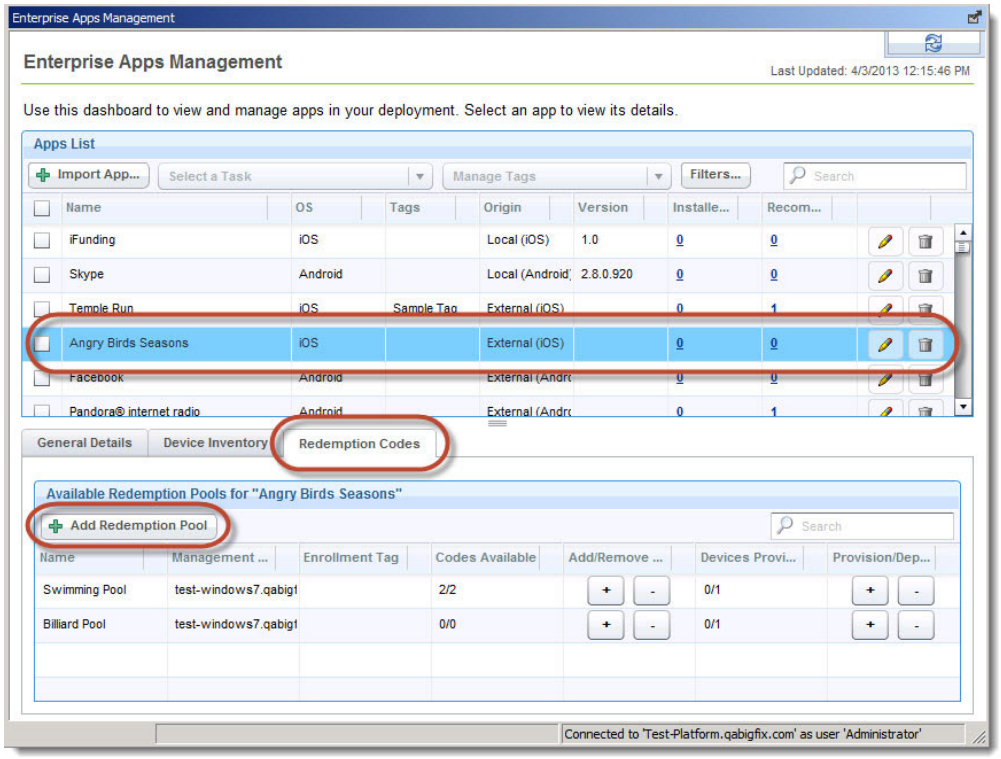
Create a Redemption Pool

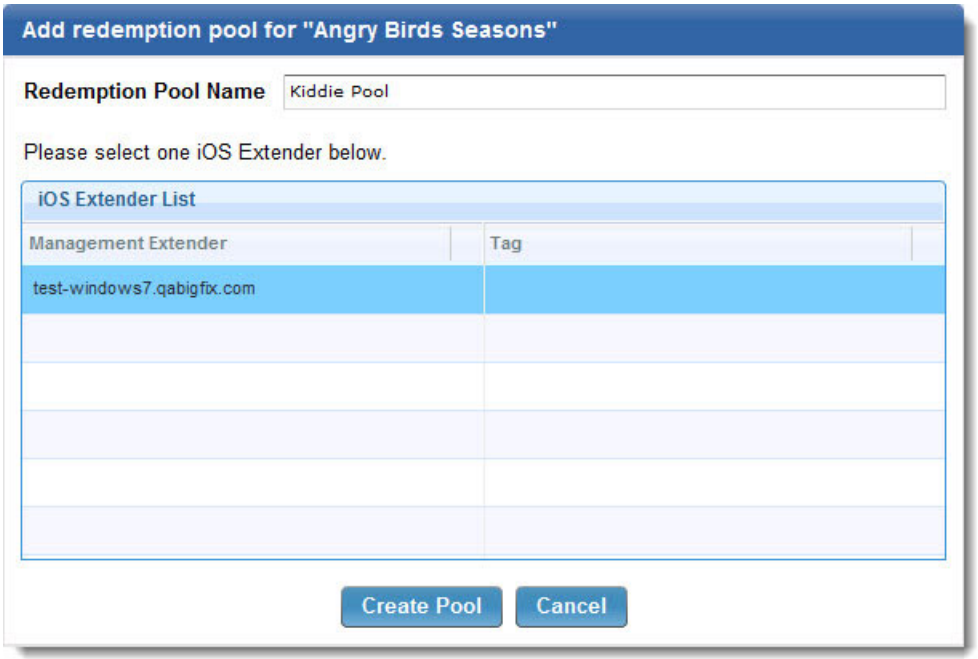
Pools are created for individual iOS apps and are assigned to a particular Management Extender.

To create a pool, perform the following steps:

1. Select an app from the Enterprise App Management dashboard by selecting the app's row. The app must be an iOS app that is non-free, is external, and was imported as an Apple iOS Managed App.
2. Select the **Redemption Codes** tab at the bottom of the dashboard.
3. Click **Add Redemption Pool** to display a new window.

4. Enter a name for the Redemption Pool, select the Management Extender that you want associated with the pool, and click **Create Pool**. A Fixlet is created. Click **OK**.
5. The Redemption Pool is listed in the **Redemption Codes** tab. The associated Management Extender is listed. In addition, the Enrollment Tag associated with that Management Extender is displayed, if in a multitenant environment.





Add Redemption Codes to a Redemption Pool

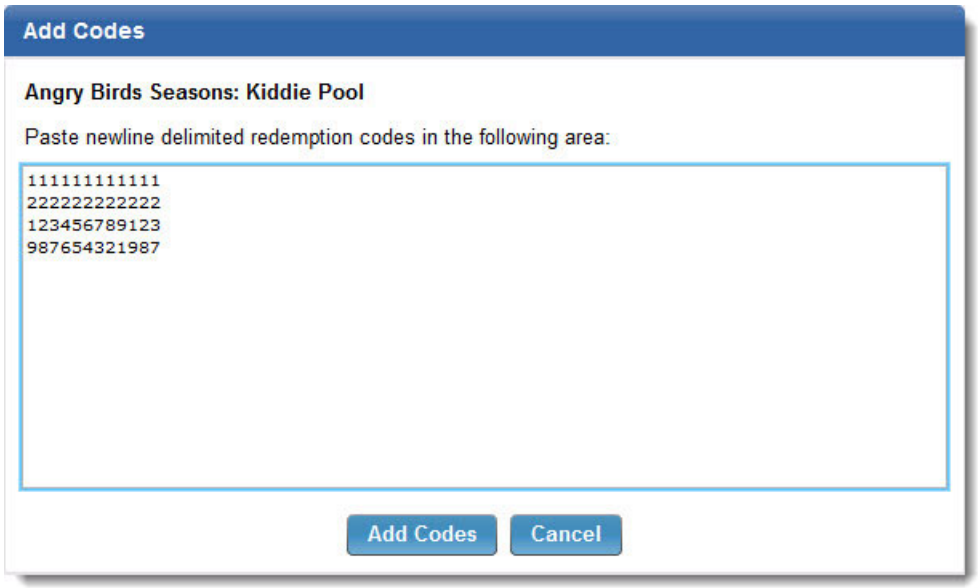
After a Redemption Pool is created for an iOS App and pool is assigned to a Management Extender, the next step is to populate the pool with redemption codes supplied by Apple Inc. through a volume license purchase.

To add Redemption Codes to a Redemption Pool, perform the following steps:

1. Click the **+** button in the **Add/Remove Codes** column of the Redemption Pool that you want to edit. The **Add Codes** window opens.
2. Type or paste one or more Redemption Codes into the field provided. Each Redemption Code must be on its own line (newline delimited).
3. Click **Add Codes** to run a task. Click the green**Back** button in the console to return to Enterprise App Management.

You can remove Redemption Codes from a pool by using the **–** button. Enter the codes that you want to remove from the pool.

Note: Adding codes to a Redemption Pool requires communication with the Management Extender that the pool is assigned to. This action might take a few moments to complete.



Assign Devices to a Redemption Pool

Individual Redemption Pools are assigned to a Management Extender. The devices that are managed by the Management Extender must be individually provisioned before they can take advantage of the redemption codes in the pool. This configuration allows a large degree of control over the management of your redemption codes.

To provision devices for a Redemption Pool, perform the following steps:

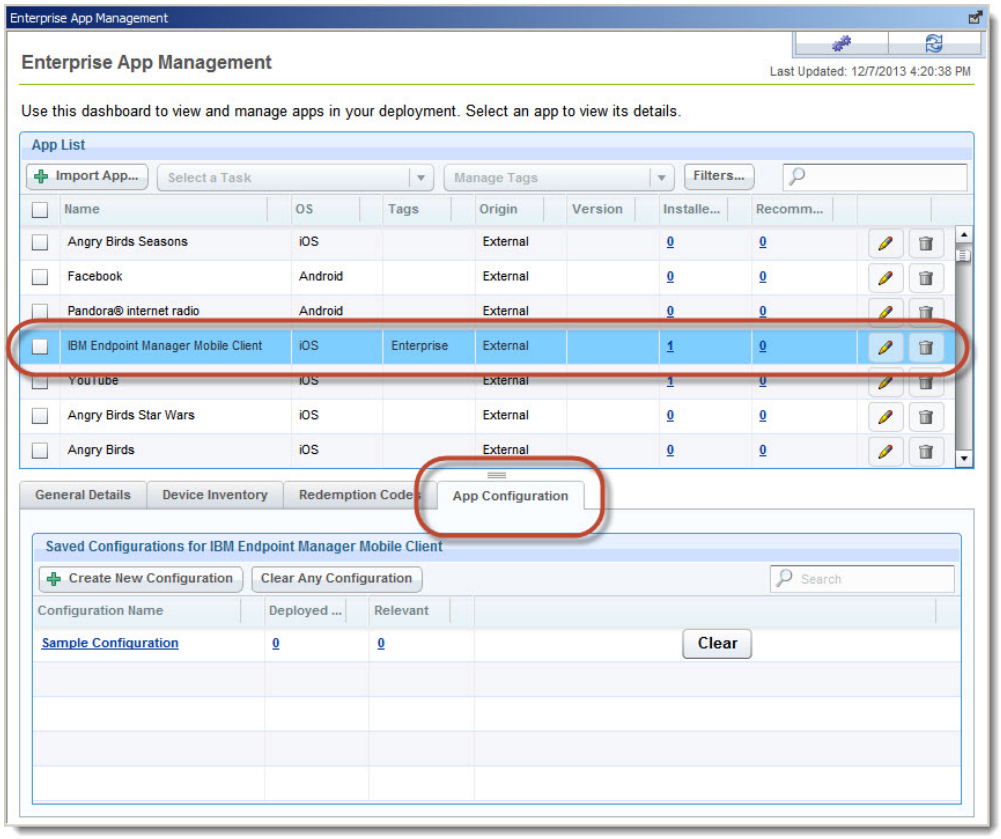
1. Select a Redemption Pool from the ones available in the **Redemption Codes** tab of an imported app in the Enterprise App Management dashboard, by selecting its row.
2. Click the **+** button in the **Provision/Deprovision Devices** column. A **Take Action** window opens.
3. Select the iOS devices that you want to provision and click **OK**. An action is created.

Note: Provisioning devices with a Redemption Pool requires communication with the Management Extender the pool is assigned to. This action might take a few moments to complete.

App Configuration

iOS 7 allows app developers to define APIs associated with their app. These APIs allow IBM Endpoint Manager for Mobile Devices to configure these apps.

To access the App Configuration tab, highlight any iOS app from App Management Dashboard that was imported as an Apple iOS Managed App. You can create app configurations for any managed app, however these configurations will only function on apps that have been developed to allow this interaction. In addition, app configurations will only function on iOS devices that are running Apple iOS 7.0+.



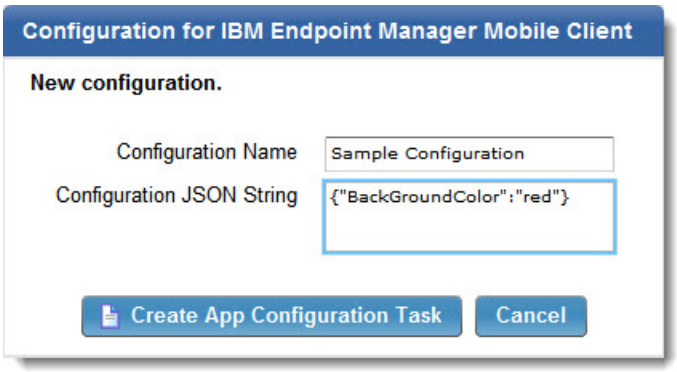
The developers for an app must create valid APIs to interact with the app. IBM Endpoint Manager for Mobile Devices cannot query apps for the existence of these APIs. Documentation for an app is required to understand what APIs are available and how they should be formatted. IBM Endpoint Manager for Mobile Devices uses JSON strings to interact with app APIs.

Create and Apply App Configurations

App configurations are created on a per app basis. They can then be applied to devices where the app is installed.

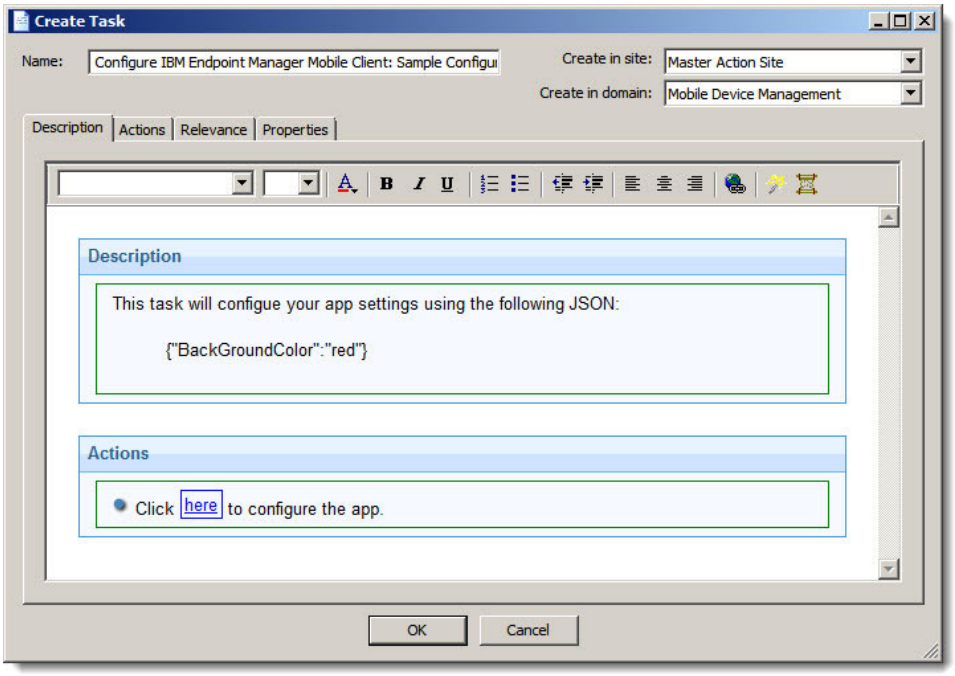
To create an iOS app configuration from the App Management Dashboard, perform the following steps:

1. Highlight an iOS app. The app must be an Apple iOS Managed App and it must be one that supports app configuration APIs that are documented.
2. Click the **App Configuration** tab at the bottom of the App Management Dashboard.
3. Click **Create New Configuration**. A small configuration window appears.



4. Enter a **Configuration Name** to identify the new configuration.
5. Enter a JSON string in the **Configuration JSON String** field. Valid strings are dependent on the API provided by the app developer. The following example string might be used to change the background color of an app to red if the app API allows it: `{"BackGroundColor":"red"}`

   Note: Check the app developer's documentation to determine what parameters can be configured on an iOS app.
6. Click **Create App Configuration Task**. The **Create Task** window is displayed. Click **OK**.



To apply an app configuration to an iOS 7+ device that has the relevant app installed, perform the following steps:

1. Click an app configuration name. A task window is displayed.

2. Click **Take Action** to display the **Take Action** window.
3. Select the device or devices to apply the app configuration, and click **OK**.

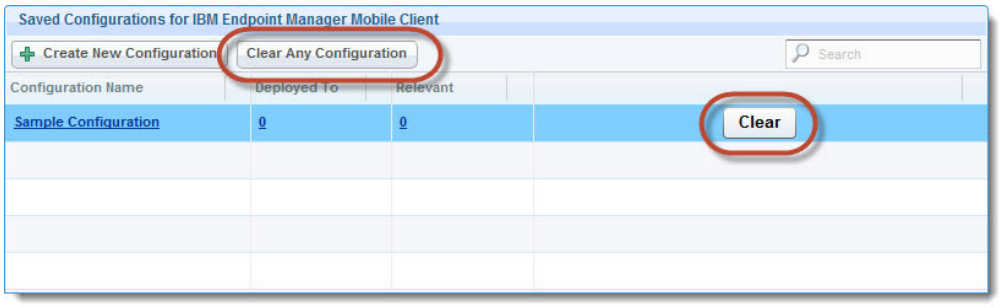
App configurations can be easily deleted like any other task:

1. Click the app configuration name.
2. In the task window, click **Remove** and confirm the deletion of the task by clicking **OK**.

Clear and Delete App Configurations

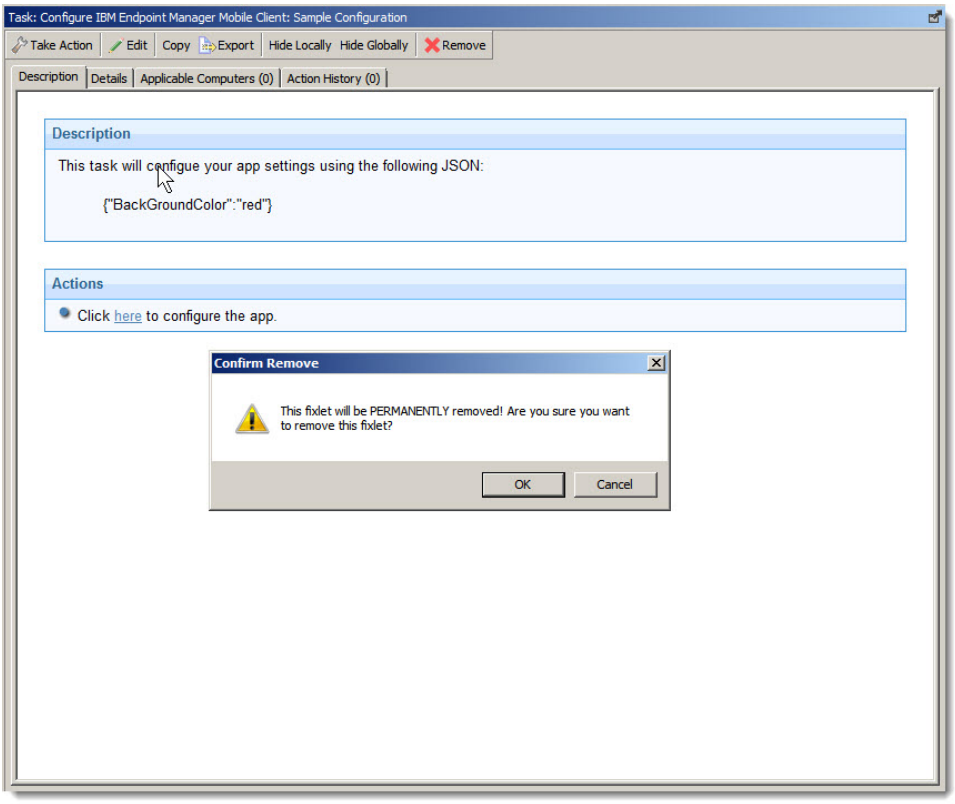
App configurations can be cleared individually or as a group. App configurations are deleted like any other task or fixlet.

App configurations can be individually removed from the related app on a device or all devices on a management extender by clicking the **Clear** button. You can also remove all of the app configurations that are associated with an app by clicking **Clear Any Configuration**. All configurations from the current app from the devices you specify are removed.



App configurations can be easily deleted like any other task:

1. Click the app configuration name.
2. In the task window, click **Remove** and confirm the deletion of the task by clicking **OK**.



Renew APNS Certificates

Managing iOS devices requires the use of the Apple Push Notification Service (APNS).

An APNS certificate is required to authorize communication between the Enrollment and Apple iOS Management Extender and Apple Inc. Apple sets APNS credentials to expire one year from their date of issue, so APNS certificates must be renewed annually to continue managing iOS devices. APNS certificate expiration cannot be extended by users or Mobile Device Management providers. APNS certificates are associated with Enrollment and Apple iOS Management Extenders. If you have multiple Enrollment and Apple iOS Management Extenders, use a single APNS certificate when you configure them. The following procedure works effectively whether you have previously used a single or multiple APNS certificates in your deployment.

Back Up the Private Folder

Renewing the APNS certificate requires modifying several certificate files. Create a backup of the folder that contains the Management Extender certificates to avoid problems in case an error is made.

1. Back up the following folder to a secure location on each relay that contains an Enrollment and iOS Management Extender:

   ```
   C:\Program Files (x86)>\BigFix Enterprise\Management Extender\MDM Provider\private
   ```

Restore the Push Key

When you originally configured an Enrollment and iOS Management Extender you were instructed to save a backup copy of your Apple Push Notification Private Key to a secure location.

1. Locate your backup copy of push_key.pem.
2. Restore the backup copy by placing it on the relay that contains your management extender in the following location:

   ```
   C:\Program Files (x86)>\BigFix Enterprise\Management Extender\MDM Provider\private
   ```

If you have multiple management extenders on different relays, make sure that:

- You keep each push_key.pem file separate.
- Each push_key.pem file gets replaced.

Important: Push_key.pem is the same file you used when you generated the original APNS certificate for your management extender. If this file has changed, a newly generated APNS certificate will not be valid for your current deployment and currently enrolled devices will be unable to communicate with the management extender. This situation occurs only if you did not back up your push_key.pem or if you did not match a given push_key.pem file with its appropriate management extender.

Generate New Certificate Signing Request

With the correct push key in the correct folder, the next step is to generate a Certificate Signing Request (CSR).

1. From the IBM Endpoint Manager console, navigate to **Mobile Device Management > All Mobile Device Management Content > Fixlets and Tasks.**
2. Search for the string "APNS" to locate Fixlet 250: Regenerate APNS Certificates for Apple iOS.
3. Run Fixlet 250 and select the computer relay that contains your Enrollment and Apple iOS Management Extender.
4. Download the new CSR by navigating to https://<relay_hostname>/csr.

If you have management extenders on multiple relays, repeat steps 3 and 4 for each relay.

Send CSR for Signature

IBM must sign the newly generated CSR.

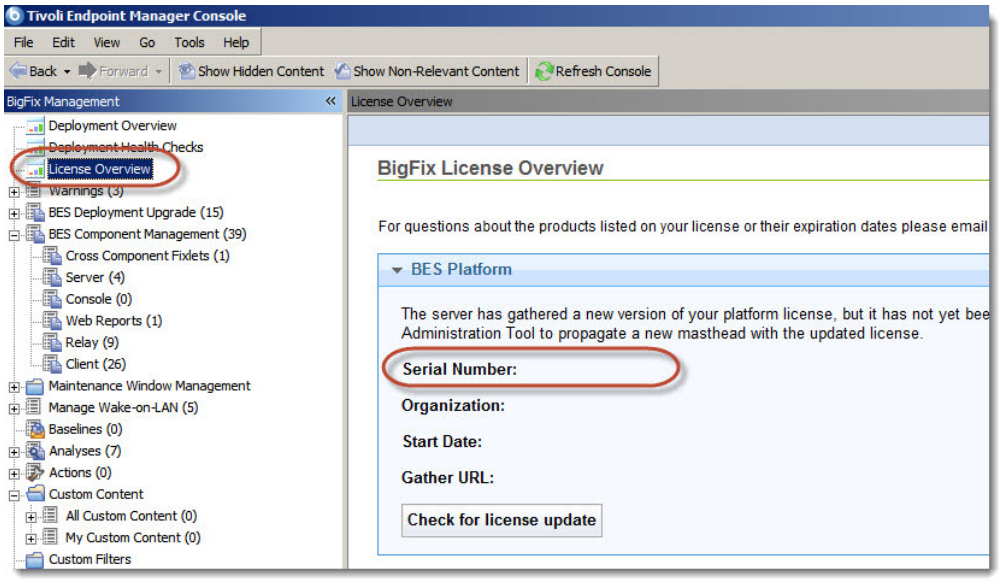
To request a signature:

1. Create an email to send to: `iem-mdm-signup@wwpdl.vnet.ibm.com.`
2. In the Subject line type: `MDM APNS CSR <Your Organization>.`
3. In the message body type: `Platform Serial Number: <Your Platform serial number>`.
4. Attach the CSR to the email and send.

The signed CSR will be emailed back to you as an attachment.

To find your platform serial number:

- Open the Endpoint Manager Console and select **Licence Overview**.



If you have multiple management extenders associated with multiple APNS certificates, send an individual email for each CSR.

Important: Exercise caution to ensure that the management extender requests and files are matched correctly, to avoid unnecessary problems later on.

Generate an APNS Certificate

When you have obtained a signed CSR from IBM, the next step is to generate a new APNS certificate. To obtain an APNS certificate from Apple Inc.:

1. Navigate to `https://identity.apple.com/pushcert/`.
2. Log in using an Apple ID.

   Note: A shared Apple ID associated with your organization, one can be used by other members of your organization in the future, is suggested.
3. Select the option to renew a certificate, and upload the signed CSR provided by IBM.
4. Download the newly created push certificate. This file has the extension `.pem`.
5. Rename the downloaded Apple file to: `<hostname>.cer`, using the host name of the relay that this certificate is matched to.

If there are multiple certificates associated with this Apple ID and you are unable to determine which one was newly created using the expiration date, you will need to manually verify the certificate. For more information, see “Match APNS Certificates to Correct Management Extender.”

Match APNS Certificates to Correct Management Extender

If you are unsure which certificate matches a specific management extender, use the method below to ensure compatibility. If you have tracked your certificates carefully this step is unnecessary.

To match a new APNS certificate from Apple Inc. to its correct management extender:

1. Install OpenSSL on the relay that contains your management extender. Information about OpenSSL and Windows binary files can be found at www.openssl.org.
2. Ensure that your OpenSSL binary is in your Windows path.
3. Move the newly generated APNS certificate from Apple Inc. that you want to verify to the directory: `C:\BigFix Enterprise\Management Extender\MDM Provider\private`.

   Note: You should have renamed the newly generated certificate after you downloaded it from Apple Inc. Do not replace any files.
4. Open a command line on your relay.
5. From within the command line navigate to the directory: `C:\BigFix Enterprise\Management Extender\MDM Provider\private.`
6. Obtain the user ID of the recently restored push key by running the command: `openssl x509 –noout –modulus –in push.cer |openssl md5.`
7. Compare the two values.
   a. If the values match, the new APNS certificate is the correct certificate for the management extender that you have checked.
   b. If the values do not match, repeat this process with your new APNS certificates until you locate the one that matches the management extender you are working with.

If you have multiple management extenders, it might be necessary to verify the correct APNS certificate for each one. Repeat this entire process on each relay that contains a management extender until you have identified all matching APNS certificates.

Apply a New APNS Certificate

After a new APNS certificate has been downloaded from Apple Inc., it must be copied to its matching management extender.

Rename the new APNS certificate to `push.cer` and copy it to the following location on the relay that contains your management extender: `C:\BigFix Enterprise\Management Extender\MDM Provider\private.`

You must replace the existing file. If you have multiple management extenders, replace the old certificate with the new one that was generated for the matching management extender.

Important: Do not replace the existing file unless you are sure that the new APNS certificate matches the management extender. If you are unsure, match the APNS Certificates as described in “Match APNS Certificates to Correct Management Extender” on page 104. Copying an incorrect APNS certificate will prevent currently enrolled devices from communicating with their management extender.

Enterproid Divide

Enterproid Divide is a container solution for Apple iOS and Android devices. Divide is an app that acts as a workspace, or container, that mimics device capabilities while isolated from the rest of the device. This container solution allows information within Divide to be secured and managed separately from the rest of the device.

IBM Endpoint Manager integrates with Divide and allows Mobile Device Management features for devices that are enrolled in a Divide deployment. To take advantage of these features, you must have an account with Enterproid. In addition, you must install the Divide app on relevant devices, and the devices must be enrolled in your deployment.

For more information about Enterproid Divide, app installation, and enrollment, see http://www.divide.com. You can download the Divide app from the Apple App Store and Google Play.

The first step in managing devices with Divide is to install and configure one or more Enterproid Divide Management Extenders. For detailed instructions, see the *Endpoint Manager for Mobile Devices Setup Guide*.

Divide Policy Dashboard

Enterproid Divide uses security policies that are defined and are then applied to devices. Policies define communication settings, password requirements, security settings, email settings, app management, and other parameters.

The implementation of Divide management in the IBM Endpoint Manager for Mobile Devices differs from Enterproid's implementation. Enterproid defines users as the most basic element of management. Users are assigned to a group and groups are assigned policies. In IBM Endpoint Manager, policies and groups are defined together so that when a policy is created within IBM Endpoint Manager, a corresponding group is created within your Divide deployment.

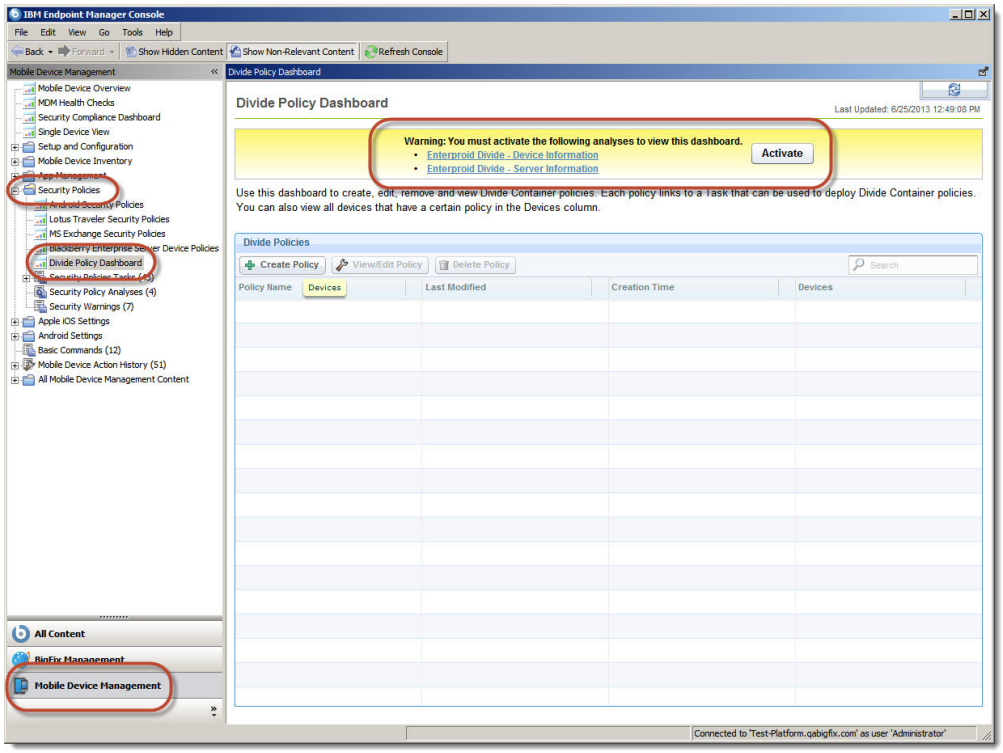
In IBM Endpoint Manager, policies are assigned to devices and the concept of a group is hidden, although they exist within your Divide deployment. In IBM Endpoint Manager for Mobile Devices, each device user is listed as a separate computer in the console.

Accessing the Divide Policy Dashboard

Divide policies are created and managed through the Divide Policy Dashboard.

The dashboard can be accessed by opening the **Mobile Device Management** site and navigating to **Security Policies > Divide Policy Dashboard**.

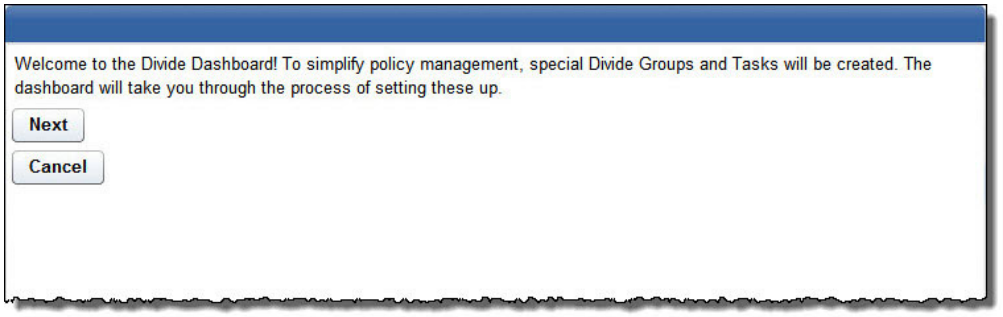
Note: You might be required to activate analyses for the dashboard to function. If so, a yellow warning banner is displayed at the top of the dashboard. Click **Activate** to turn the listed analyses on.



Creating Divide groups and tasks:

After you activate relevant analyses, if required, a wizard is displayed. This wizard synchronizes your Divide deployment with IBM Endpoint Manager. This process searches your Enterproid Divide deployment for existing policies (including the mandatory default policy) and creates an IBM Endpoint Manager version of that group. The wizard also creates associated tasks within IBM Endpoint Manager to manage these groups.

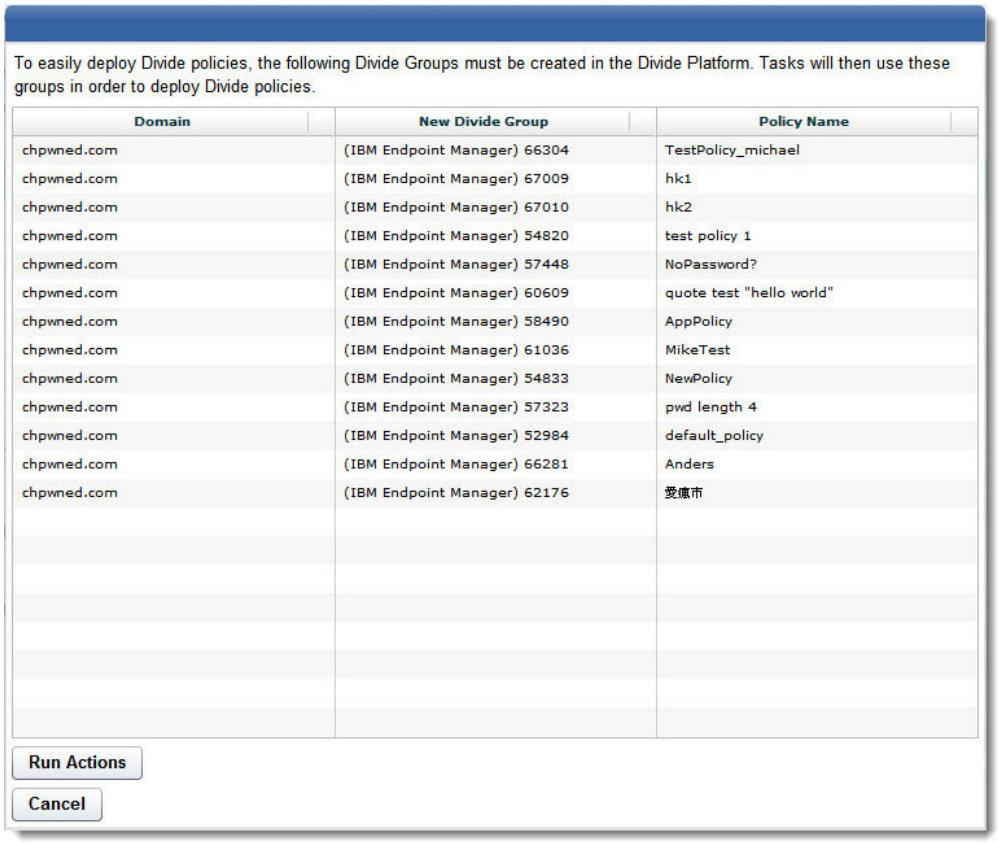
Click **Next** to proceed.



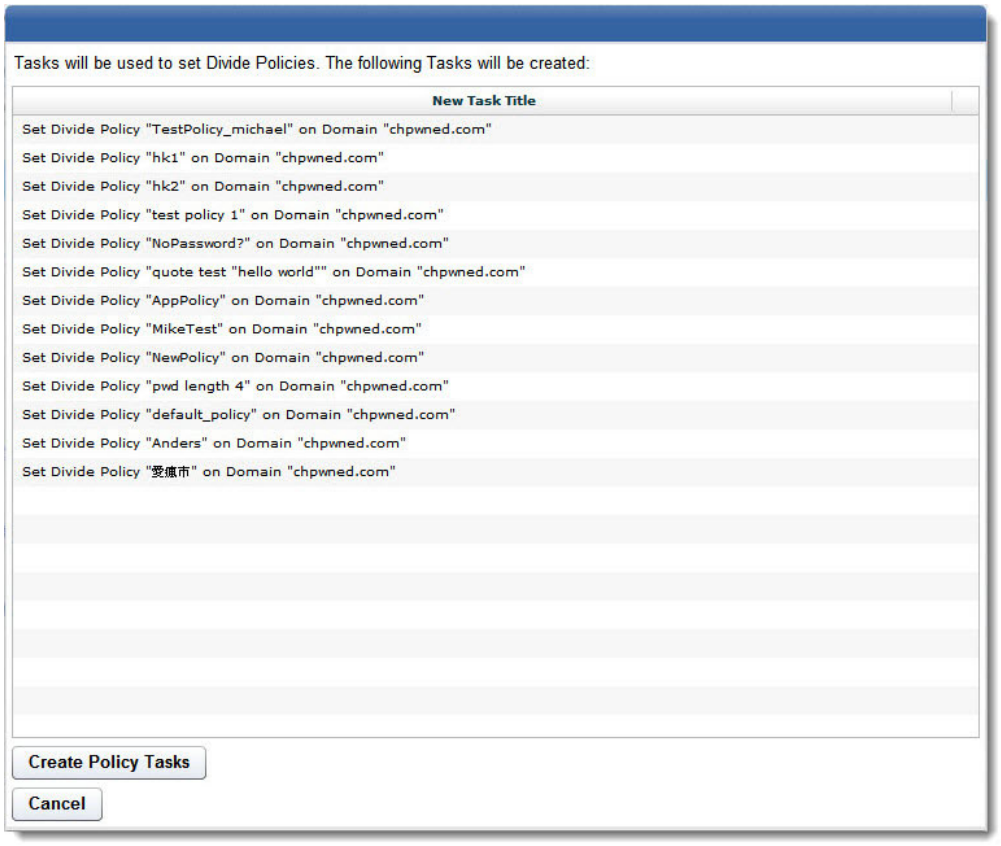
Note: The wizard runs the first time the Divide Policy Dashboard is opened. It also runs if new policies are created with the Divide Manager tool within your Divide deployment.

The wizard displays a list of policies that are in your Divide deployment. If there are no existing Divide policies, the default policy is displayed because it is always present. Click **Run Actions** to create IBM Endpoint Manager-defined groups.

Note: This process can take several minutes. Do not cancel the operation until it completes. Do not navigate away from this wizard until it completes.



After an IBM Endpoint Manager version of each group that previously existed in your Divide deployment is created, tasks must be created for each policy and paired group, within the IBM Endpoint Manager console. These tasks act as the interface between IBM Endpoint Manager and Enterproid. Click **Create Policy Tasks** to proceed.

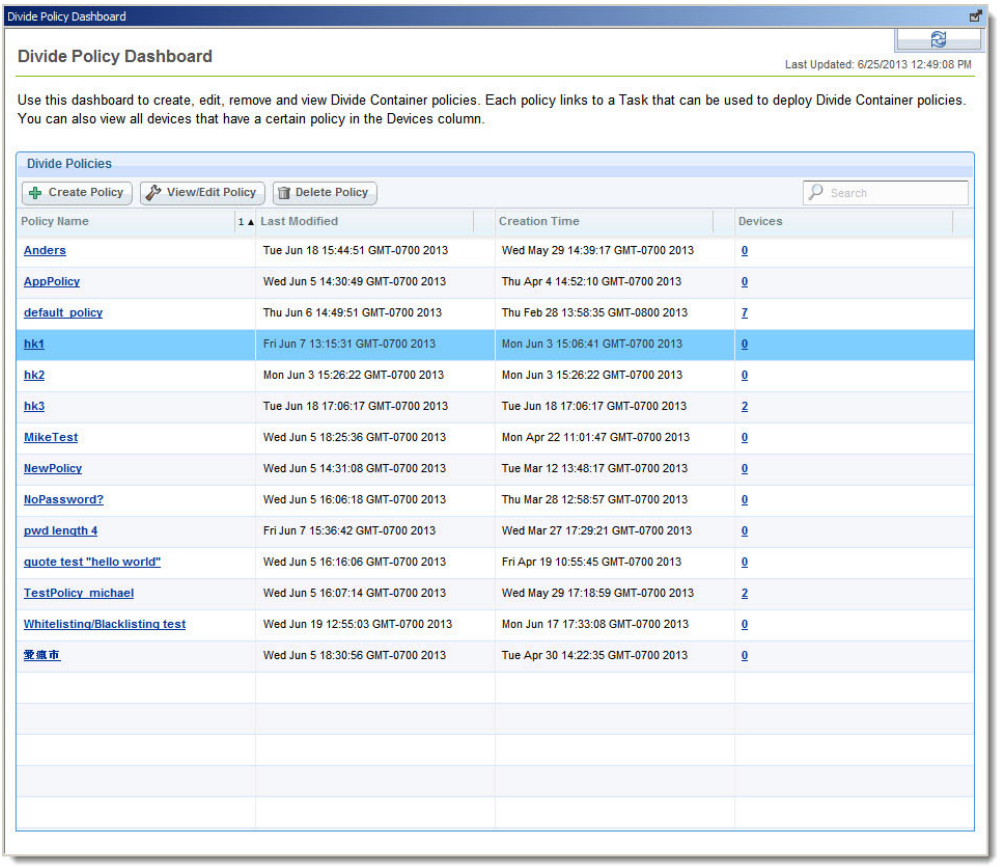


After the action completes, click **Close** to close the wizard and view the Divide Policy Dashboard.

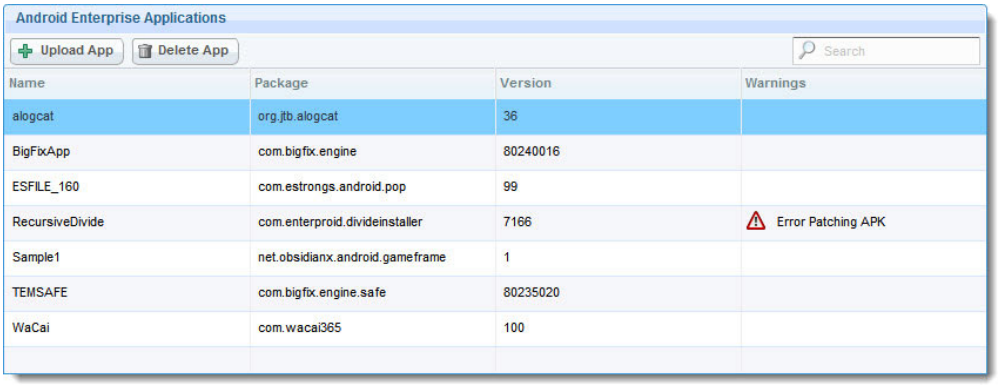
Divide Policy Dashboard layout

The Divide Policy Dashboard lists any existing policies, and the dashboard contains buttons to create, edit, and delete policies. Each policy is listed by its name, the last date it was modified, the time it was created, and how many devices are subscribed to each policy.

- Click a policy name to display the task that is associated with the policy. Click **Back** to return to the dashboard.
- Click a policy row, without clicking the policy name, to highlight the policy.
- Click the number in the **Devices** column to display the devices that the policy is assigned to. Click **Back** to return to the dashboard.



In addition to displaying policies, the lower portion of the Divide Policy Dashboard is dedicated to Android Enterprise Applications. Here, you can upload an Android application package file, or APK. APK's can be uploaded to Enterproid where they are modified or "wrapped", allowing the app to be installed within a Divide container. Apps that were uploaded for wrapping are displayed here, including apps that failed the wrapping process. Modified apps can also be deleted.

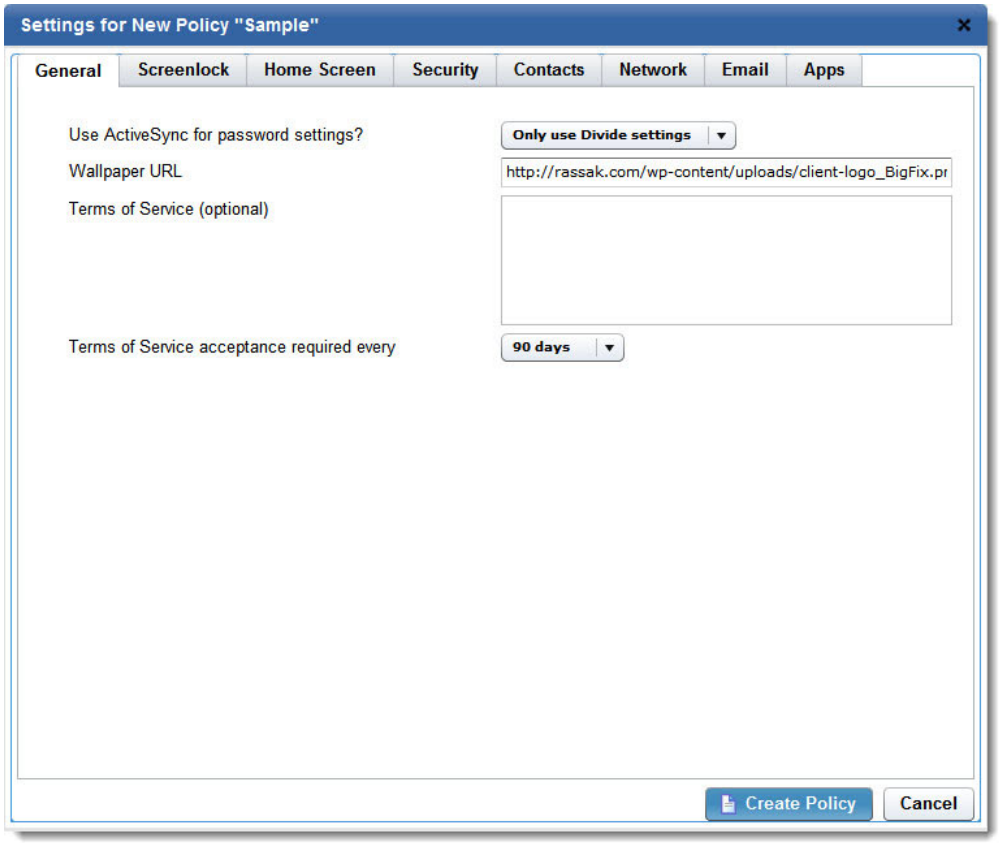


Create a Divide Policy

Divide Policies in IBM Endpoint Manager are assigned to devices and define many parameters of the Divide container on that device.

To create a new policy, click **Create Policy**. Enter a name in the **New Policy Name** text box. An existing policy can be used as a template by selecting it from the

menu. Click **Next** to proceed.



You define policies by defining settings available in several tabs. Information is provided for some policy settings in the following list, which is organized by tab name. For details about individual policy settings, see http://support.divide.com.

Note: The green Android robot logo next to an option indicates that it applies to Android devices only. Options that are not labeled with this logo apply to Android and iOS devices.

General

If you select **Use ActiveSync Policy** from the menu, policy password options are disabled. All settings in the **Screenlock** tab are disabled because these parameters are now defined by your ActiveSync settings.

Screenlock

Define a password policy for the Divide container. Trivial passwords are passwords that contain multiple repeated characters. The policy settings in this tab are disabled if ActiveSync policy settings are selected in the **General** tab.

Home Screen

The term “home screen” refers to the Divide app’s home screen, not the primary Android home screen.

Security

Whitelisted apps are apps that must be installed and present within the Divide container. Blacklisted apps are apps that are not permitted on the device outside of the container.

Contacts

Defines settings that are related to email and phone contacts. Phone numbers can be blocked for incoming or outgoing calls. Divide manages enterprise contacts through ActiveSync, however the Divide container has access to contacts from the standard Android contact list in a similar manner to all Android apps. For more information, see http://support.divide.com.

Network

You can define a whitelist of safe URLs or a blacklist of banned URLs. You cannot create both because they are mutually exclusive.

Email You can define an email signature in addition to settings related to email attachments and how they are handled within the Divide container.

Apps The nature of the Divide container implicitly dictates which apps are installed within the container. Usually, apps are created for the Divide container. Apps can be patched by Enterproid, which allows them to be installed in the Divide container. For more information, see "Android Enterprise Applications" on page 113.

The blacklist that is defined here denotes apps that cannot be installed on the device outside the container.

Note: Blacklisted apps can be defined within the App Management feature of IBM Endpoint Manager for Mobile Devices. For more information, see "App Management" on page 87. Do not define blacklisted apps in multiple ways.

Assign a Divide Policy

After a Divide policy is created, it can be assigned to devices. All devices must be assigned a policy. If no other policy exists, the default policy is applied.

To assign a policy to a device, perform the following steps:

1. Click the name of the policy. Clicking the policy name is not the same as clicking the policy row.
2. In the task that is now displayed, click **Take Action**.
3. Select the device that you want to assign the policy to, and click **OK**.

To change the policy on a device, apply the wanted policy to the device. The new policy is applied to the device, removing the previous policy. Divide policies cannot be "deleted" from a device, they can only be reassigned. Devices must always have a policy.

Editing and deleting Divide Policies

Editing Divide Policies is similar to creating new policies. Divide Policies can be deleted only if they are not assigned to any devices.

You can edit Divide Policies by highlighting the policy row. Highlighting a policy row is different from clicking the policy name. After you select a policy row, click **View/Edit Policy**. Policies are edited in the same manner that policies are created, see "Create a Divide Policy" on page 110.

You can delete Divide Policies by selecting the policy row and clicking **Delete Policy**. Policies that are assigned to devices cannot be deleted. To delete a policy, you must first apply a different policy to any devices that are currently assigned to the policy that you want to delete.

When you click **Delete Policy**, a warning is displayed. Click **OK** to proceed. An action is created that deletes the task that is associated with the policy. In addition, the policy is deleted from your Divide deployment. It can take several minutes for this process to fully complete even though it appears to finish from within the IBM Endpoint Manager console.

Note: If the delete policy action is interrupted, or if the Enterproid Divide Management Extender does not refresh before you view the Divide Policy Dashboard, the Divide Policy Dashboard prompts the creation of a replacement task. The preceding situation occurs because IBM Endpoint Manager is unaware of the current state of the Divide deployment until the Enterproid Divide Management Extender communicates with your Divide deployment. Avoid this situation by waiting a few minutes before you view the Divide Policy Dashboard after you delete a policy, or by canceling the prompt to create a task.

Android Enterprise Applications

Enterproid Divide provides a secure container that is separate from the normal Android environment. Normally, apps must be designed to run within the Divide container. However, it is possible to patch existing apps, allowing them to be installed and accessed through the Divide container. This process is referred to as “app wrapping”.

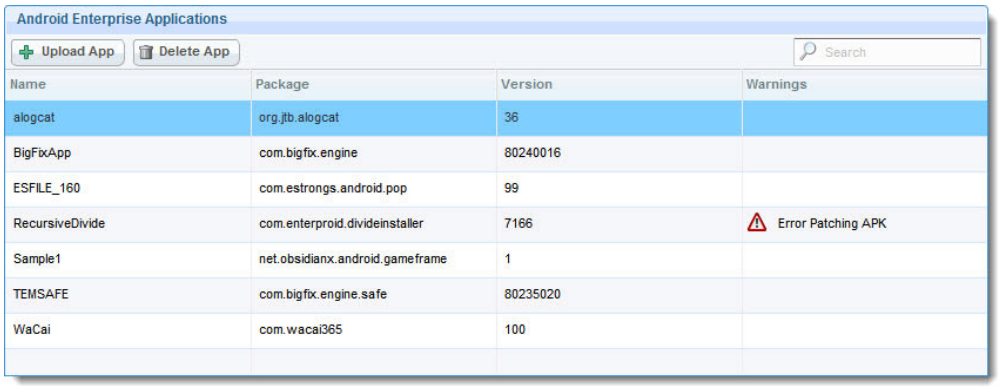
Apps patched in this manner are known as Android Enterprise Applications. Android Enterprise Applications allow apps that are normally restricted to the less secure standard Android environment to retain the security benefits of the Divide container.

The process that culminates in an Android app that is installed within a device's Divide container involves several steps:

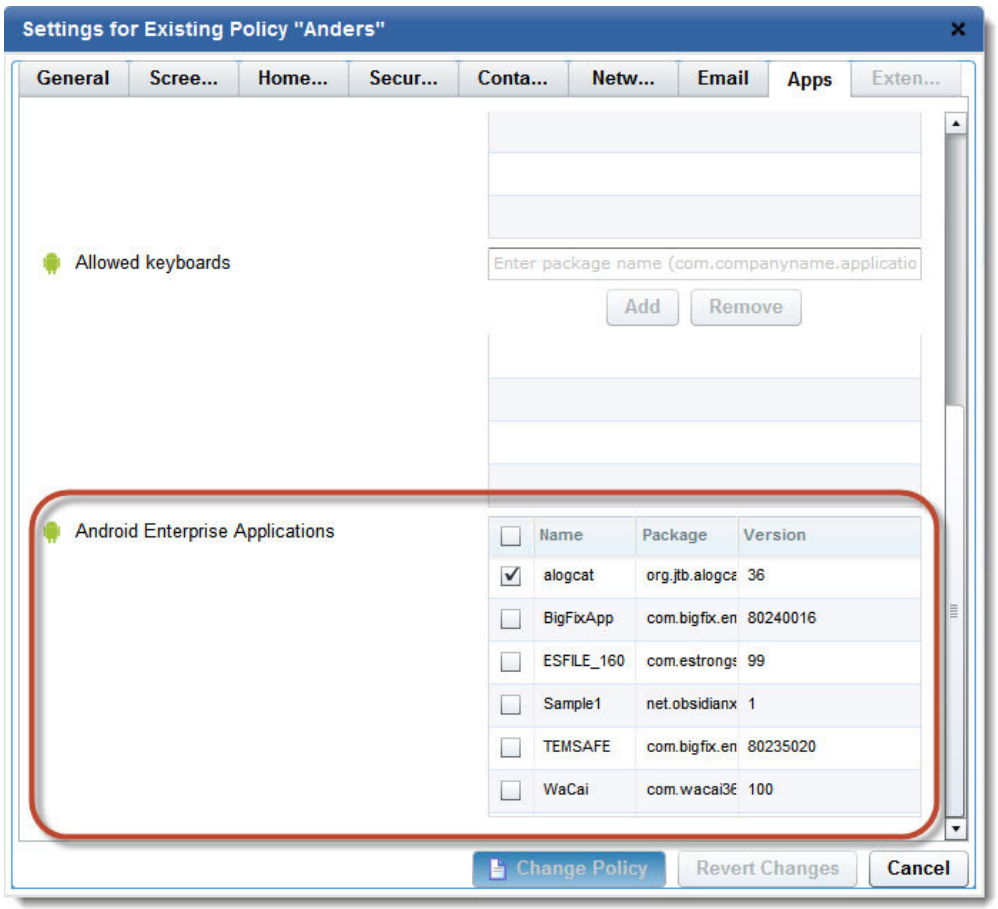
1. The Android application package file, or APK, must be uploaded to Enterproid to be patched.
2. An existing Divide Policy must be edited, and patched apps must be assigned to the policy.
3. The policy must be assigned to devices, or if any devices are already assigned to the policy, they are prompted to install assigned apps within the Divide container.

To upload an app, click **Upload App**. Specify the **Domain** registered with your Enterproid account, give the app a name, and browse to the location of the wanted APK file. Clicking **Upload** creates an action that sends the APK to Enterproid for patching. After the action completes, APKs that were sent to Enterproid are listed. If an APK fails to patch successfully, an error is displayed in the **Warnings** column.

Note: All APK files are not guaranteed to be successfully patched. This process is dependent on the APK and is not controlled by IBM.



After an app is patched, it can be assigned to an existing Divide Policy. For more information about editing Divide Policies, see "Editing and deleting Divide Policies" on page 112. Navigate to the **Apps** tab. At the bottom of the tab, you see the **Android Enterprise Applications** section. Here, you can check any apps that were successfully patched by Enterproid. Click **Change Policy** to continue.



Note: You can add Android Enterprise Applications only to previously existing Divide Policies. When you create a new Divide Policy, the **Android Enterprise Applications** section of the **Apps** tab is not present.

If the newly modified Divide Policy is assigned to devices, those devices receive a notification within their Divide container that prompt the user to install the app.

Device users must have Arbitrary APK Installation enabled on their Divide container. For more information, see http://support.divide.com.

There are several facts to be aware of regarding Android Enterprise Applications:

- Not all APKs can be successfully patched. This process is controlled by Enterproid and cannot be influenced.
- We recommend that you test patched apps before you deploy them widely. The app patching process might appear to succeed, but problems might manifest later.
- If an app is installed on the Android device outside of the Divide container, it cannot be installed within the container.
- Patched apps that are installed within the container cannot be configured like a normal Android app by a device user. This restriction is a part of the app's increased security.
- Wiping or uninstalling the Divide container removes any apps that are installed within the container.
- Device users can choose not to install a patched app, or can uninstall an app that was previously installed. Doing so contradicts the Divide Policy that is assigned to the device. Responses to these kinds of actions by a device user can be configured within the Divide Policy. For more information, see “Create a Divide Policy” on page 110.

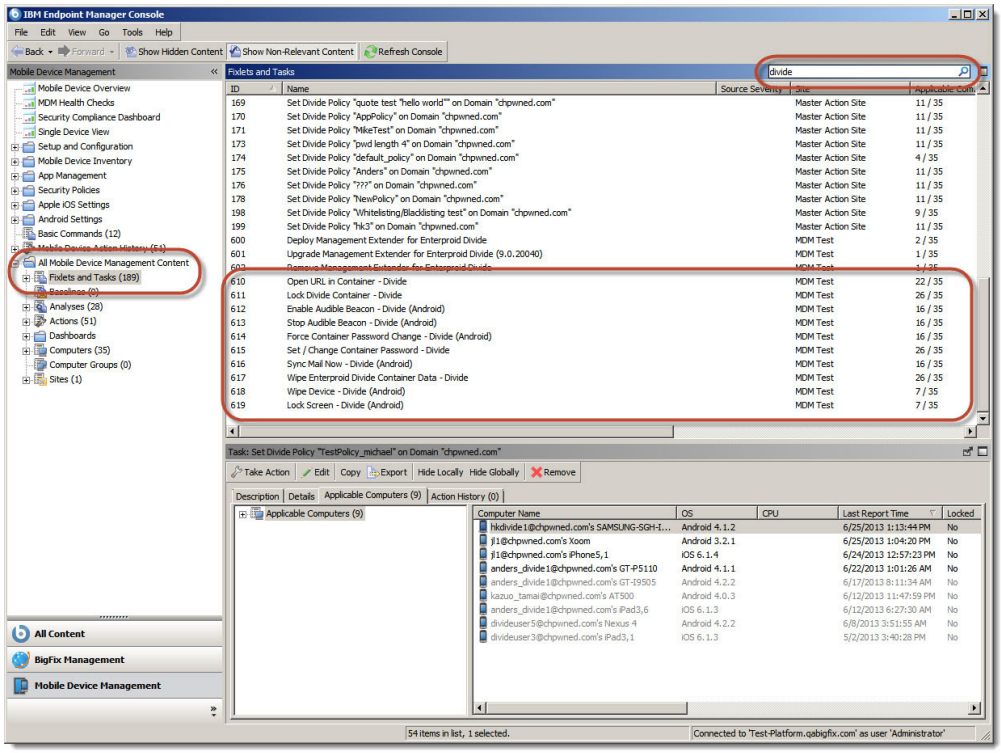
Enterproid Divide tasks

Divide policies define security and other features of devices that are enrolled in your Divide deployment. In addition to policies, a set of tasks in IBM Endpoint Manager for Mobile Devices allow specific actions to be taken on enrolled devices. Available tasks are dependent on the device operating system.

To see a full list of available tasks, perform the following steps:

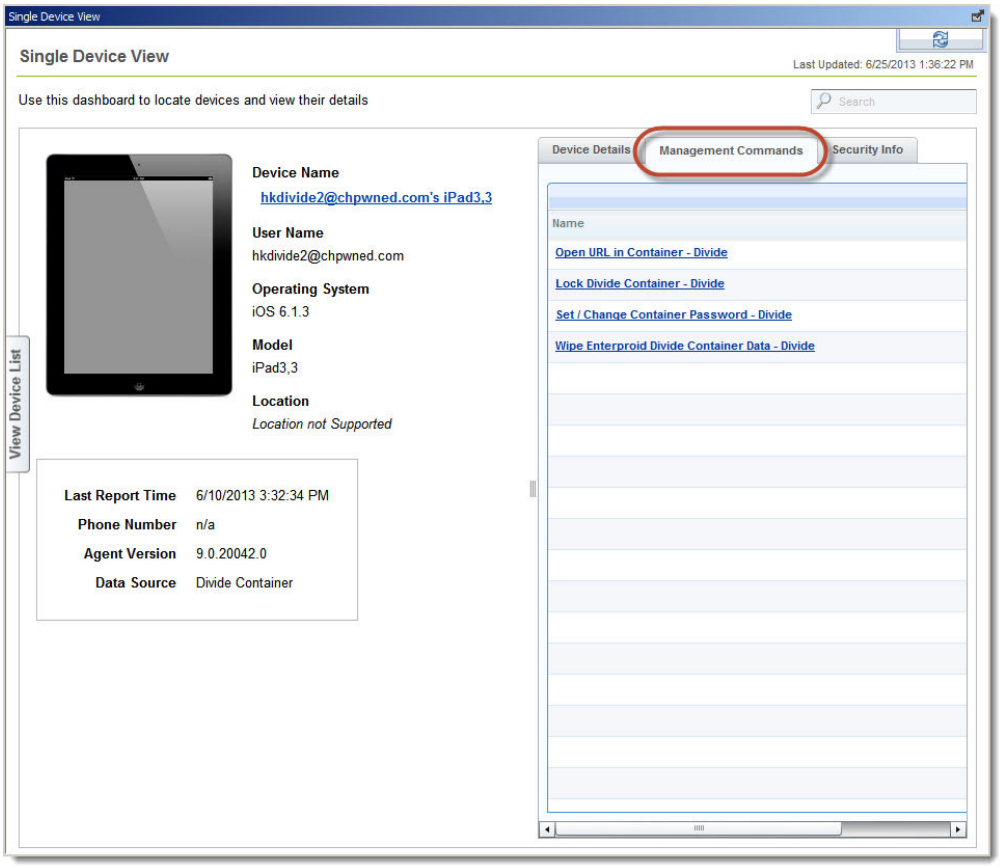
1. Select the Mobile Device Management Site and navigate to **All Mobile Device Management Content > Fixlets and Tasks**.
2. In the **Search Fixlets and Tasks** field, enter `divide`. A list of applicable tasks is displayed.

Note: Divide policy tasks and tasks that are related to the deployment of Divide Management Extenders are also displayed in the search results.



To perform tasks on a specific device, the Single Device View provides a more streamlined interface and lists only tasks relevant to the chosen device:

1. Select the Mobile Device Management Site and navigate to **Single Device View**.
2. From the list of managed devices, select a device whose **Data Source** is **Divide Container**.
3. Select the **Management Commands** tab. A list of tasks applicable to the chosen device is listed.



Android Divide tasks

The following tasks can be performed only on Android devices that are enrolled through an Enterproid Divide Management Extender.

Open URL in Container – Divide (Android)
Send a URL to the target device. The URL is opened in the Divide browser.

Enable Audible Beacon – Divide (Android)
Turn on an alert tone that sounds until it is stopped by another task.

Stop Audible Beacon – Divide (Android)
Turn off the alert tone.

Force Container Password Change – Divide (Android)
Prompt the device user to enter a new password for the Divide container. The new password must comply with the existing password policy.

Sync Mail Now – Divide (Android)
Start a synchronization between the Divide container and the email server.

Lock Screen – Divide (Android)
Lock the screen of the target device. The user must enter their device password to access the device.

Wipe Device – Divide (Android)
Delete all data on the target device. Data within the Divide container and all data outside the Divide container is deleted.

Note: Use caution when you start this task. This task completely deletes all information on the target device. The device will no longer be enrolled

in any deployments including your Divide deployment and IBM Endpoint Manager for Mobile Devices. You can Selectively wipe Divide data with **Fixlet 617: Wipe Enterproid Divide Container Data – Divide**.

Android and Apple iOS Divide tasks

The following tasks can be performed on both Apple iOS and Android devices.

Lock Divide Container – Divide
Lock the Divide container. Users must reenter the current password to regain access to Divide.

Set / Change Container Password – Divide
Create or change the password for the Divide container. You are prompted in the IBM Endpoint Manager Console to enter the password. The device user must be notified of the password change.

Note: The password that you create with this task is not secure and is visible in the console's action history. In addition, Android device users are not automatically notified that the password is changed.

Wipe Enterproid Divide Container Data – Divide
Delete all data in the Divide container. A consequence of this task is that the device is no longer enrolled in your Divide deployment. Device information outside of the Divide container remains safe.

Note: This task deletes the enrollment credentials of the Divide container, disconnecting it from its Enterproid Divide Management Extender. The device cannot be managed through IBM Endpoint Manager unless the device is enrolled again. This task will never report as complete because the target device is unable to communicate to IBM Endpoint Manager to report its complete status.

Managing App Licenses on iOS Devices (Apple VPP)

Use Mobile Device Management to manage distribution of mobile applications (apps) and content purchased through Apple's Volume Purchase Program (VPP) on Apple devices running iOS 7 or higher. Use the VPP App Assignment dashboard to:

- Invite device holders to enroll in the VPP program and track responses.
- Assign, revoke, and reassign licenses for apps and content.
- Display a list of licenses available for distribution.
- Search for specific devices.

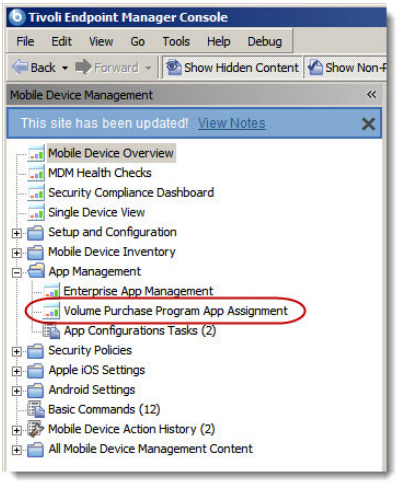
System Requirements

To use the VPP App Assignment dashboard:

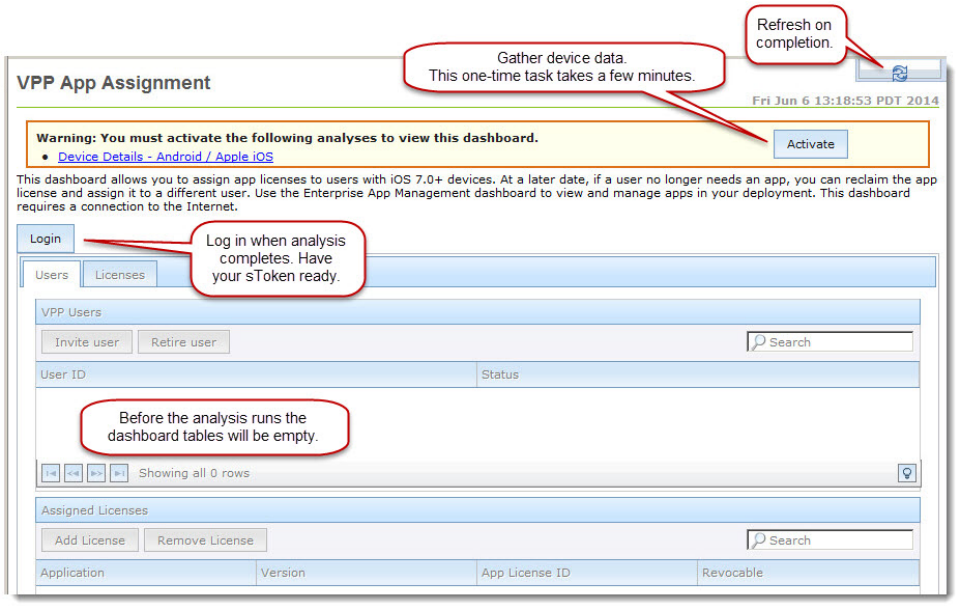
- Your company must be enrolled in Apple's Volume Purchase Program. You will need the sToken issued at VPP registration to log in.
- Devices must be enrolled in IEM Mobile Device Management, and run iOS 7 or later.
- Device holders must have an iTunes account.
- You must have an active Internet connection.

Dashboard Setup and Overview

Click the Volume Purchase Program App Assignment dashboard on the IBM Endpoint Manager console.



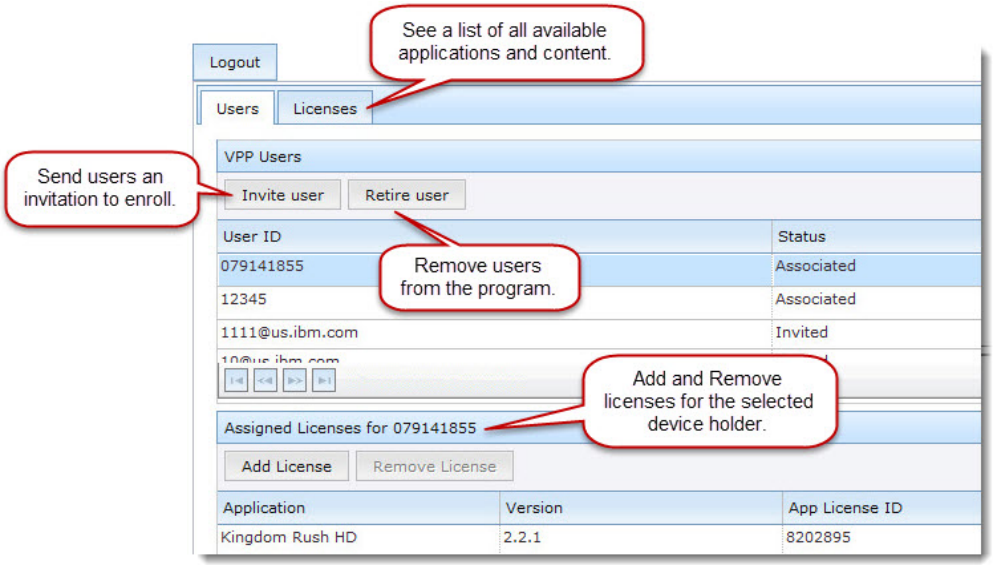
1. The first time that you open the dashboard its tables will be empty. Click **Activate** to start gathering iOS device data. Read about the analysis at the Device Details – Android / Apple iOS link; use the Console's Analysis node to monitor the data gathering process.
2. When the analysis completes click the dashboard's **Refresh** button.



3. Click the **Login** button. Enter your Apple sToken at the prompt. Pressing **Submit** at login stores the sToken in the dashboard; logging out removes it. Stay logged in to allow one or more administrators to use the dashboard without re-entering the sToken. Log out between sessions to require administrators to authenticate before they use the dashboard.

Note: Apple's sToken expires after one year, or after a password reset. If your sToken has expired go to Apple's VPP website to renew it.

While IBM Endpoint Manager associates licenses with devices, Apple associates licenses with users. In the dashboard, a device holder's email address functions as their VPP User ID. The dashboard tables are populated as device holders are invited to join the program.



Enrollment Status values:

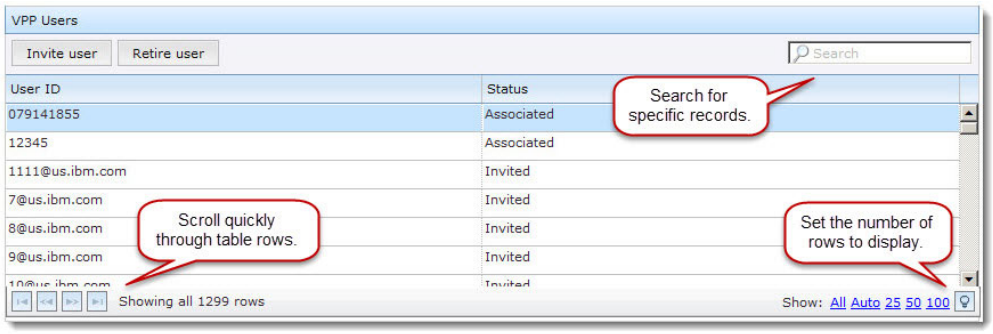
- Invited – An invitation to join the program was sent.
- Associated – The device holder has enrolled, and their company email address is associated with their iTunes account.

Click the Licenses tab to see a list of all available app and content licenses.

Click a User ID in the VPP Users table to display the licenses that are assigned to it in the License table. Use the **Add License** and **Remove License** buttons to add or revoke licenses from the selected device holder. App assignments are revocable but book assignments are not.

- Revocable = Yes: license can be removed or assigned to other users.
- Revocable = No: License is for use on one device only.

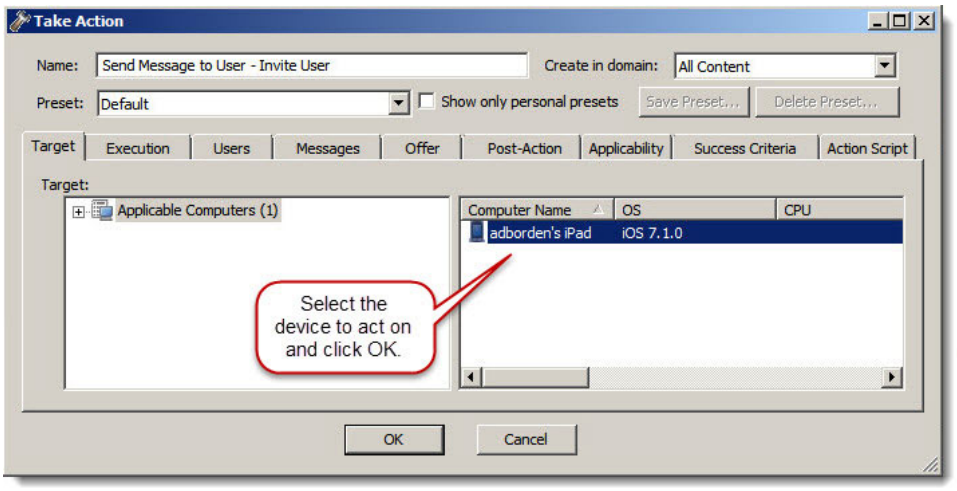
Use the Search box to find a specific User ID. Use the table controls to scroll through the data screen by screen and to set the number of rows displayed.



VPP App Management Procedures

Enroll a User in the VPP Program

1. Click the **Invite User** button. Select a device holder and click **Confirm**.
2. In the Take Action window select the name of the device to enroll, and click **OK**. If a device holder has two iOS devices and uses a VPP-issued app on both, a license is required for each device.



The device holder's User ID displays in the VPP Users table. Their Enrollment Status is "Invited," and the following notification is sent:

> "Dear iOS device holder, This is an invitation to join the company Volume Purchase Program (VPP), which allows your network administrator to deliver licenses for work-related applications to your device at no cost to you. Volume purchasing significantly lowers licensing costs company-wide. Employees eligible to receive work-related apps and books, such as yourself, are required to participate. Use the secure and your iTunes credentials to enroll. Once enrolled, you'll be able to download eligible apps at no cost. To learn more about the VPP program, see 'http://vpp.itunes.apple.com.' Thank you for your participation and support."

Once enrolled the user's Enrollment Status becomes "Associated."

Assign an App License to a Device

1. Select a device holder in the VPP User table to display their license information in the Assigned Licenses table.
2. Click the **Add License** button.
3. Select the wanted license from the list and click **Confirm** to display the Take Action window.
4. Select the device to assign the license to and click OK. To see or change the notification text, click the **Action Script** tab.
   - Mobile Device Management sends this message to the device: "Your administrator has assigned <App Name> to you."

Remove an App License from a Device

1. Select a device holder in the VPP User table to view their license information in the Assigned Licenses table.

2. Select the license that you wish to remove.
3. Click the **Remove License** button. Click Confirm at the prompt to display the Take Action window.
4. Select the device to remove the license from and click **OK**.
   - Mobile Device Management sends this message to the device: "Your administrator has removed the license for the app <Name> from your account. The app will not launch after a 30-day grace period."
   - Apple sends the message, "The app <Name> is no longer assigned to you."

Remove a User from Your Company's Apple VPP Program

1. Select a device holder in the VPP User table and click the **Retire User** button.
2. Click **Confirm** at the prompt.

   When you remove a user, you release and revoke any company-assigned app licenses from the device holder's iTunes account. Book assignments are not revocable. A user who was previously retired from the VPP program can be reinstated.
   - No notification is sent to the device when a user is removed from the program.

Support

For more information about this product, see the following resources:

- http://pic.dhe.ibm.com/infocenter/tivihelp/v26r1/topic/com.ibm.tem.doc_9.1/welcome/welcome.html
- IBM Endpoint Manager Support site
- IBM Endpoint Manager wiki
- Knowledge Base
- Forums and Communities

Notices

This information was developed for products and services that are offered in the USA.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
United States of America

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:
INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on

generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

Portions of this code are derived from IBM Corp. Sample Programs.

Programming interface information

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at www.ibm.com/legal/copytrade.shtml.

Adobe, Acrobat, PostScript and all Adobe-based trademarks are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, other countries, or both.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

ITIL is a registered trademark, and a registered community trademark of The Minister for the Cabinet Office, and is registered in the U.S. Patent and Trademark Office.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java™ and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Linear Tape-Open, LTO, the LTO Logo, Ultrium, and the Ultrium logo are trademarks of HP, IBM® Corp. and Quantum in the U.S. and other countries.

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the IBM website.

Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make

derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

NitroDesk Touchdown Legal Notices

If a customer chooses to use IBM Endpoint Manager for Mobile Devices to configure and manage NitroDesk TouchDown software, IBM Endpoint Manager for Mobile Devices will use the NitroDesk TouchDown APIs to communicate with the NitroDesk TouchDown product. Customers are responsible for independently purchasing NitroDesk TouchDown software by working directly with NitroDesk, Inc.

The NitroDesk TouchDown APIs are used under license from NitroDesk, Inc. IBM may update the NitroDesk Touchdown APIs from time to time at its sole discretion. NitroDesk may change the NitroDesk Touchdown software or APIs in such a way that the changes cause management of NitroDesk TouchDown via IBM Endpoint Manager for Mobile Devices to cease working. IBM shall have no obligation to support NitroDesk TouchDown software or APIs even if the capability ceases to function.

The NitroDesk Touchdown APIs and use of the APIs are provided AS-IS. SUBJECT TO ANY STATUTORY WARRANTIES THAT CANNOT BE EXCLUDED, IBM MAKES NO WARRANTIES OR CONDITIONS, EXPRESS OR IMPLIED, REGARDING THE NITRODESK APIS OR SUPPORT, IF ANY, INCLUDING, BUT NOT LIMITED TO, ANY IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, AND TITLE, AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT.

SOME STATES OR JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF EXPRESS OR IMPLIED WARRANTIES, SO THE ABOVE EXCLUSION MAY NOT APPLY TO LICENSEE. IN THAT EVENT, SUCH WARRANTIES ARE LIMITED IN DURATION TO THE MINIMUM PERIOD REQUIRED BY LAW. NO WARRANTIES APPLY AFTER THAT PERIOD. SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATIONS ON HOW LONG AN IMPLIED

WARRANTY LASTS, SO THE ABOVE LIMITATION MAY NOT APPLY TO LICENSEE. LICENSEE MAY HAVE OTHER RIGHTS THAT VARY FROM STATE TO STATE OR JURISDICTION TO JURISDICTION.