



# Good Device and Application Management

Last updated: April 7, 2016

Versions: GP 2.2.xx.yy, GC 2.2.xx.yy and GD SDK 2.1.xxxx



## Legal Notice

This document, as well as all accompanying documents for this product, is published by Good Technology Corporation ("Good"). Good may have patents or pending patent applications, trademarks, copyrights, and other intellectual property rights covering the subject matter in these documents. The furnishing of this, or any other document, does not in any way imply any license to these or other intellectual properties, except as expressly provided in written license agreements with Good. This document is for the use of licensed or authorized users only. No part of this document may be used, sold, reproduced, stored in a database or retrieval system or transmitted in any form or by any means, electronic or physical, for any purpose, other than the purchaser's authorized use without the express written permission of Good. Any unauthorized copying, distribution or disclosure of information is a violation of copyright laws.

While every effort has been made to ensure technical accuracy, information in this document is subject to change without notice and does not represent a commitment on the part of Good. The software described in this document is furnished under a license agreement or nondisclosure agreement. The software may be used or copied only in accordance with the terms of those written agreements.

The documentation provided is subject to change at Good's sole discretion without notice. It is your responsibility to utilize the most current documentation available. Good assumes no duty to update you, and therefore Good recommends that you check frequently for new versions. This documentation is provided "as is" and Good assumes no liability for the accuracy or completeness of the content. The content of this document may contain information regarding Good's future plans, including roadmaps and feature sets not yet available. It is stressed that this information is non-binding and Good creates no contractual obligation to deliver the features and functionality described herein, and expressly disclaims all theories of contract, detrimental reliance and/or promissory estoppel or similar theories.

## Legal Information

© Copyright 2016. All rights reserved. All use is subject to license terms posted at [www.good.com/legal](http://www.good.com/legal). GOOD, GOOD TECHNOLOGY, the GOOD logo, GOOD FOR ENTERPRISE, GOOD FOR GOVERNMENT, GOOD FOR YOU, GOOD APPCENTRAL, GOOD DYNAMICS, SECURED BY GOOD, GOOD MOBILE MANAGER, GOOD CONNECT, GOOD SHARE, GOOD TRUST, GOOD VAULT, and GOOD DYNAMICS APPKINETICS are trademarks of Good Technology Corporation and its related entities. All third-party technology products are protected by issued and pending U.S. and foreign patents.

## Table of Contents

<b>Revision History</b>	<b>10</b>
<b>What's New?</b>	<b>10</b>
Integrating BES12 and Good Dynamics	10
Device Management Setup for Split Billing on iOS Devices	11
Important Product Clarifications: Good Device Management, June 26, 2015	11
Apple Configurator Files Must Not Be Signed or Encrypted	11
Caution in Configuring iOS Device Access Controls	11
Turn Off iOS Inspection and Installation Controls in Pairs	12
Good Agent Possibly Misleading Message: "Device Encryption Required"	14
What's New from Previous Releases	14
Device Enrollment	14
Device Password Policy	14
Restrictions	14
<b>Conceptual Overview to Good Device and Application Management</b>	<b>15</b>
Structure of Doc and Task-Oriented Workflows	16
Good DM and AM Deployment Models	16
Good DM and AM Installation Procedure	16
Relationship to Cloud GC: Feature Supported	17
About Good Dynamics Software Version Numbers	17
<b>Device Management</b>	<b>18</b>
Requirements: Good Dynamics Software, Device OS, Certificates, and API Keys	18
Other Requirements	19
About Good for KNOX: No License Required	20
Device Management Lifecycle	20
Provisioning	21

Deployment, Enrollment, and Security .....	21
Operation .....	22
Post-Enrollment Monitoring and Compliance .....	22
Retirement .....	22
Example Business Scenarios .....	22
Scenario 1: Corporate-Owned Devices, but Not BYOD Devices, with WiFi .....	23
Scenario 2: BYOD Devices, but Not Corporate-Owned Devices, with VPN .....	24
<b>Planning Your DM Deployment: Devices, Policies, People .....</b>	<b>26</b>
How are your end-users organized in your enterprise? .....	26
What are your end-users' geographic locations? .....	26
Do your end-users use iOS devices, Android devices, Android with KNOX, Windows devices, or all? .....	26
Do you plan on relying on Apple DEP? .....	27
Which device features do you want to manage? .....	27
Will the administrator provision and enroll devices? .....	27
Corporate-Owned Enrollment vs End-User Self-Enrollment (or BYOD) .....	27
Apple DEP: Background and Planning .....	28
How Apple DEP with Good Control Works .....	28
Supervised and Userless Devices .....	28
Good Agent for iOS is Auto-Pushed to Devices .....	28
Planning Considerations .....	29
Important: Whitelist the DM Servers in Good Control proxy.urls After Upgrade .....	29
Migration to Good DM .....	29
IT Admin .....	29
End Users .....	30
<b>Device Management: Known Limitations .....</b>	<b>30</b>
Windows Tablet Device Management: Known Limitations .....	31
End-user Unenrollment Cannot be Detected .....	31
Scheduled Maintenance Works Only on Surface Pro Tablets .....	32
WNS Channel URI Errors Can Cause Unenrollment .....	32

About the Windows Update Field in Device Status in Good Control .....	32
Behavior of Password Restrictions on Windows Tablet .....	32
<b>Device Management Administrator's Workflow .....</b>	<b>35</b>
Non-Apple-DEP Devices .....	35
Apple DEP Devices .....	36
Blacklisting or Whitelisting Applications on Devices .....	37
Behavior .....	37
Steps for Blacklisting or Whitelisting .....	38
Steps for Removing Apps from Blacklist or Whitelist .....	39
Enabling Device Management in Good Control .....	39
Good Control Properties for Allowable-New-Device Platforms .....	40
Configuring Compliance Emails .....	40
<b>Certificates and API Keys .....</b>	<b>42</b>
Working with APNS Certificates .....	42
Generating a CSR .....	42
Uploading an APNS Certificate .....	43
Obtaining Google Cloud Messaging API Keys .....	43
Prerequisites .....	43
Steps .....	43
Installing Google Cloud Messaging API Keys .....	44
<b>Policies .....</b>	<b>45</b>
Example: Effects of Device Policies on End-User Devices .....	47
Different Policies by Type of Device Enrollment; Enrollment Key Expiration .....	47
Implementing Your Device Policies .....	47
<b>Apple DEP Profiles and Devices .....</b>	<b>47</b>
One-time Setup with Apple for DEP Profiles in Good Control .....	48
Careful: Effect of Changing the GC-Defined Apple MDM Server Token .....	48
Steps .....	48
Defining DEP Profiles in Good Control .....	49

Important GC Settings Affecting Apple DEP .....	51
Steps for Defining DEP Profiles in Good Control .....	51
About Errors from Apple .....	52
Effect of Removing MDM Profile, How to Prevent .....	52
Assigning DEP Profiles to Devices .....	52
Working with DEP-Enrolled Devices .....	53
Filtering and Searching .....	53
Filtering by CSV File from Apple .....	53
Synching with Apple .....	53
DEP Device Actions .....	54
Export to CSV .....	54
<b>Device Configurations .....</b>	<b>55</b>
About Active Directory and "Auto-fill Username" .....	55
iOS ActiveSync and Autofill Username .....	55
Android and Autofill Username .....	55
VPN Configuration .....	55
For iOS Only: Layer 2 Tunneling Protocol (L2TP) Fields .....	56
For iOS Only: Point to Point Tunneling Protocol (PPTP) Fields .....	56
For iOS Only: Cisco IPSec .....	57
Cisco AnyConnect .....	59
Wi-Fi Configuration .....	60
Email Configuration .....	62
Multiple Exchange Configurations on a Single Device .....	62
Creating an Exchange ActiveSync Configuration .....	63
GC Fields for Email Configuration for Android .....	63
GC Fields for Email Configuration for iOS .....	65
GC Fields for Email Device Configuration for Windows .....	66
Webclip .....	67
Webclip Fields for iOS .....	67

Custom iOS Profile .....	68
<b>DM Enrollment .....</b>	<b>69</b>
Enrolling Devices: Administrator's Tasks .....	69
Planning: Corporate-Owned Enrollment or End-User Self-Enrollment? .....	69
Admin Steps for Corporate-Owned Enrollment .....	70
Unenrolling a Device from MDM .....	72
Admin Setup for BYO DM Enrollment: Entitle End Users to Good Agent .....	73
BYO DM Enrollment on iOS .....	73
BYO DM Enrollment on Android .....	73
No BYO DM Enrollment on Windows Devices, Only Corporate Owned .....	73
End-user Device Unenrollment/Deactivation .....	73
iOS .....	74
Android without Samsung KNOX .....	74
Android with Samsung KNOX .....	74
<b>DM Operational Tasks: Device Status, Lock, Clear Password, Wipe, and Deactivate .....</b>	<b>75</b>
<b>Reports: Devices and App Inventory .....</b>	<b>75</b>
Device Management App Inventory Reports .....	76
Device Management Inventory Reports .....	76
<b>Application Management .....</b>	<b>78</b>
Supported and Unsupported Executable File Types for AM .....	78
How Application Management Works .....	79
Application Management Lifecycle .....	80
Key Concepts .....	80
Types of Applications .....	80
GD Entitlement ID and Version .....	81
Common Errors .....	85
Application Catalog .....	86
Form Factor or "Platform" .....	86
<b>Application Management Administrator's Workflow .....</b>	<b>87</b>

Good Control Administrators: Changes in Workflow .....	87
App Management-related Screens and Tabs in Good Control .....	87
Essential One-Time Setup Tasks .....	88
Whitelisting App Stores and Web Servers in Good Control .....	88
Entitling Users to the Application Catalog .....	89
Advice on Application Development .....	90
About Unique Native Identifiers for Enterprise Apps .....	90
APIs for Application Management .....	90
<b>Adding Applications .....</b>	<b>91</b>
Adding a Public Store Application .....	91
About Adding GFE .....	91
Adding Multiple Platforms for Public Store Apps .....	91
Adding a Custom Application .....	92
Adding a Web Application .....	92
Adding GD App ID and Version Only .....	93
Specifying App Servers .....	93
Adding New GD Entitlement Versions (GD App Versions) .....	94
Entitling End-users to Applications or Denying Them .....	95
Sequence of App Version Entitling and Denying: Entitle, Then Deny .....	95
Blocking Android or iOS GD Apps by Native Version .....	95
Wildcarding Native Versions .....	95
Steps .....	96
Managed Apps: Enabling App Auto-Push, Exempting Policy Sets .....	96
Behavior on iOS .....	97
Filtering the List of Applications, Viewing the Bar Chart .....	98
Details in List View .....	98
Filters .....	99
Display of Bundle ID Only: App Removed from GD NOC .....	100
Editing Application Details .....	100



General Steps .....	101
Updating Apps .....	101
Updating a Public Store App: Work in Public Store, Refresh in Good Control .....	102
Updating a Custom App: Upload New Binary .....	102
Updating a Web App: Add New Web App .....	102
Updating a GD-App-ID-Only App: Convert to Public Store or Custom App .....	102
Application or Container Policy Reference .....	104
Deleting a Managed Application .....	106
<b>Using the Launcher .....</b>	<b>106</b>
Viewing the Good Application Catalog in the Launcher .....	107
<b>Device Policy Reference .....</b>	<b>111</b>
Disabling US Government Notice and Consent Form .....	111
Device Policy Reference: General .....	111
Good For KNOX .....	111
Device Access Controls .....	112
Device Policy Reference: Passwords .....	112
Quality Simple .....	113
Quality Alphanumeric .....	113
Quality Complex .....	113
Password Restrictions on Windows Tablet .....	113
Device Policy Reference: Restrictions .....	114
iOS Restrictable Features .....	114
Android Restrictable Features .....	117
KNOX Standard (SAFE) Restrictable Features .....	117
Microsoft Windows Restrictable Features .....	119
<b>Good Dynamics Documentation .....</b>	<b>122</b>

## Revision History

### *Good Device and Application Management*

Date	Description
2016-04-07	Added <a href="#">Blocking Android or iOS GD Apps by Native Version</a> , which had been omitted in error.
2016-03-10	Truncated revision history to reduce bulk.
2016-02-17	Updated clickpaths/steps in <a href="#">Obtaining Google Cloud Messaging API Keys</a> because Google changed their site again.
2016-02-01	Included cross-reference to document describing <a href="#">Integrating BES12 and Good Dynamics</a> .
2016-01-15	Updated for latest release: some limitations now removed: <ul style="list-style-type: none"> <li>• Apple DEP Profiles can now be assigned to more than 100 devices at a time.</li> <li>• Auto-push of managed apps is no longer limited to the first version of an app.</li> </ul>
2015-12-23	Updated for latest release. See <a href="#">What's New?</a>
2015-09-24	Emphasized in <a href="#">Entitling End-users to Applications or Denying Them</a> that for publishing a new app version, be sure to first entitle the new version before you deny the old version.

## What's New?

### Integrating BES12 and Good Dynamics

Good Dynamics and BES12 can be integrated so you can take advantage of Good's mobile app containerization and BlackBerry's cross-platform MDM capabilities.

When you integrate BES12 and Good Dynamics, you get unparalleled features and flexibility. Documentation describing the steps to integrate, with integration paths both for current GD customers and for current BES 12 customers, is now available:

#### [Integrating BES12 and Good Dynamics](#)

- Apple Device Enrollment Program (DEP) Profiles and Devices
- Managed Apps: Enabling App Auto-Push, Exempting Policy Sets
- Entitling or Denying An Individual End-User
- Blocking Android or iOS GD Apps by Native Version
- Device Management Restrictions Regrouped, with Headings

- "GD App ID" Renamed to "GD Entitlement ID"
- GC Fields for Email Device Configuration for Windows

## Device Management Setup for Split Billing on iOS Devices

Good Technology's Split Billing solution keeps track of the roaming status on devices.

For iOS devices, to enable detection of roaming status, in Good Control you need to create at least one device policy and apply it to all iOS devices that will participate in Split Billing. The device policy does not need to have any restrictions; it can simply be an "empty" device policy. All that is needed is the device management profile on the iOS device itself. Follow the workflow in [Good Device and Application Management](#) to create this device policy in Good Control as you normally would and apply the policy to all affected iOS devices.

**Note:** This setup is not needed for Android devices, only for iOS devices to enable the querying of roaming status.

## Important Product Clarifications: Good Device Management, June 26, 2015

### Apple Configurator Files Must Not Be Signed or Encrypted

iOS devices can be configured via custom settings created with Apple's Configurator, as described in [Custom iOS Profile](#).

When you export the configuration from the Apple Configurator, you have the option to digitally sign (encrypt) the output file you want to load into the GC device configuration. *Do not sign or encrypt the output file.*

If the exported file is signed, the GC cannot read it.

### Caution in Configuring iOS Device Access Controls

Be sure to understand the impact of the settings you want in Good device management's device access control for iOS devices (Good Control menu path **Device Policies** > *edit a policy set* > **General** tab):

Device Access Controls

Cancel

Save

**NOTE: Changes to Device Access Controls will require re-enrollment of iOS devices assigned to this policy.**

ON	OFF	
<input checked="" type="radio"/>	<input type="radio"/>	MDM Enabled
<input checked="" type="radio"/>	<input type="radio"/>	Allow device erase
<input checked="" type="radio"/>	<input type="radio"/>	Allow inventory of personal apps
<input checked="" type="radio"/>	<input type="radio"/>	Check compliance against <a href="#">App Blacklist</a>
<input checked="" type="radio"/>	<input type="radio"/>	Allow query of Device Information (serial number, IMEI, etc) (iOS)
<input checked="" type="radio"/>	<input type="radio"/>	Allow query of Network information (carrier network, phone number, etc) (iOS)
<input checked="" type="radio"/>	<input type="radio"/>	Allow device lock and passcode removal (iOS)
<input checked="" type="radio"/>	<input type="radio"/>	Allow password-related queries
<input checked="" type="radio"/>	<input type="radio"/>	Allow restriction-related queries
<input checked="" type="radio"/>	<input type="radio"/>	Allow remote app installation/updates
<input type="radio"/>	<input checked="" type="radio"/>	Allow inspection of installed configuration profiles (iOS)
<input type="radio"/>	<input checked="" type="radio"/>	Allow installation and removal of configuration profiles (iOS)
<input type="radio"/>	<input checked="" type="radio"/>	Allow inspection of installed provisioning profiles (iOS)
<input type="radio"/>	<input checked="" type="radio"/>	Allow installation and removal of provisioning profiles (iOS)
<input checked="" type="radio"/>	<input type="radio"/>	Allow manipulation of settings (iOS)

**Important:** After a device access control policy has been applied on a device, *its strictness cannot be increased*; it can only be decreased.

The iOS operating system enforces the first policy settings and does not allow them to be changed after they are applied to a device. This means that if you want to increase the severity of the restrictions, you will have to unenroll and then re-enroll all affected devices.

## Turn Off iOS Inspection and Installation Controls in Pairs

There are two pairs of iOS device access controls in Good Control menu path **Device Policies > edit a policy set > General** tab that you must disable at the same time. You must not disable one in the pair and leave the other in the pair enabled.

The policies are the following. By default, the policies are set ON.

### Configuration Profile Pair

- OFF Allow inspection of installed configuration profiles (iOS)
- OFF Allow installation and removal of configuration profiles (iOS)

### Provisioning Profile Pair

- OFF Allow inspection of installed provisioning profiles (iOS)
- OFF Allow installation and removal of provisioning profiles (iOS)

#### Device Access Controls

**NOTE: Changes to Device Access Controls will require re-enrollment of iOS devices assigned to this policy.**

ON	OFF	
<input checked="" type="radio"/>	<input type="radio"/>	MDM Enabled
<input checked="" type="radio"/>	<input type="radio"/>	Allow device erase
<input checked="" type="radio"/>	<input type="radio"/>	Allow inventory of personal apps
<input checked="" type="radio"/>	<input type="radio"/>	Check compliance against <a href="#">App Blacklist</a>
<input checked="" type="radio"/>	<input type="radio"/>	Allow query of Device Information (serial number, IMEI, etc) (iOS)
<input checked="" type="radio"/>	<input type="radio"/>	Allow query of Network information (carrier network, phone number, etc) (iOS)
<input checked="" type="radio"/>	<input type="radio"/>	Allow device lock and passcode removal (iOS)
<input checked="" type="radio"/>	<input type="radio"/>	Allow password-related queries
<input checked="" type="radio"/>	<input type="radio"/>	Allow restriction-related queries
<input checked="" type="radio"/>	<input type="radio"/>	Allow remote app installation/updates
<input type="radio"/>	<input checked="" type="radio"/>	Allow inspection of installed configuration profiles (iOS)
<input type="radio"/>	<input checked="" type="radio"/>	Allow installation and removal of configuration profiles (iOS)
<input type="radio"/>	<input checked="" type="radio"/>	Allow inspection of installed provisioning profiles (iOS)
<input type="radio"/>	<input checked="" type="radio"/>	Allow installation and removal of provisioning profiles (iOS)
<input checked="" type="radio"/>	<input type="radio"/>	Allow manipulation of settings (iOS)

Cancel

Save

Pair 1

Pair 2

If you disable one policy in the pair but leave the other policy enabled, you will see an error message:

**Unable to update device policy on MDM server. Please try again.**

## Good Agent Possibly Misleading Message: "Device Encryption Required"

When an Android device (except for those with Samsung KNOX) has already been encrypted via device policy, Good Agent might display an erroneous message:

### **Device Encryption Required**

This message should be ignored.

The actual status of encryption is viewable on the device in **Settings > Security**.

## What's New from Previous Releases

Device management now includes Windows Phone 8.1 devices with the following features:

- Password
- Restrictions
- Device Details
- Device Actions
- Device Inventory Report

### Device Enrollment

Enrollment process to install device management profile on the device

### Device Password Policy

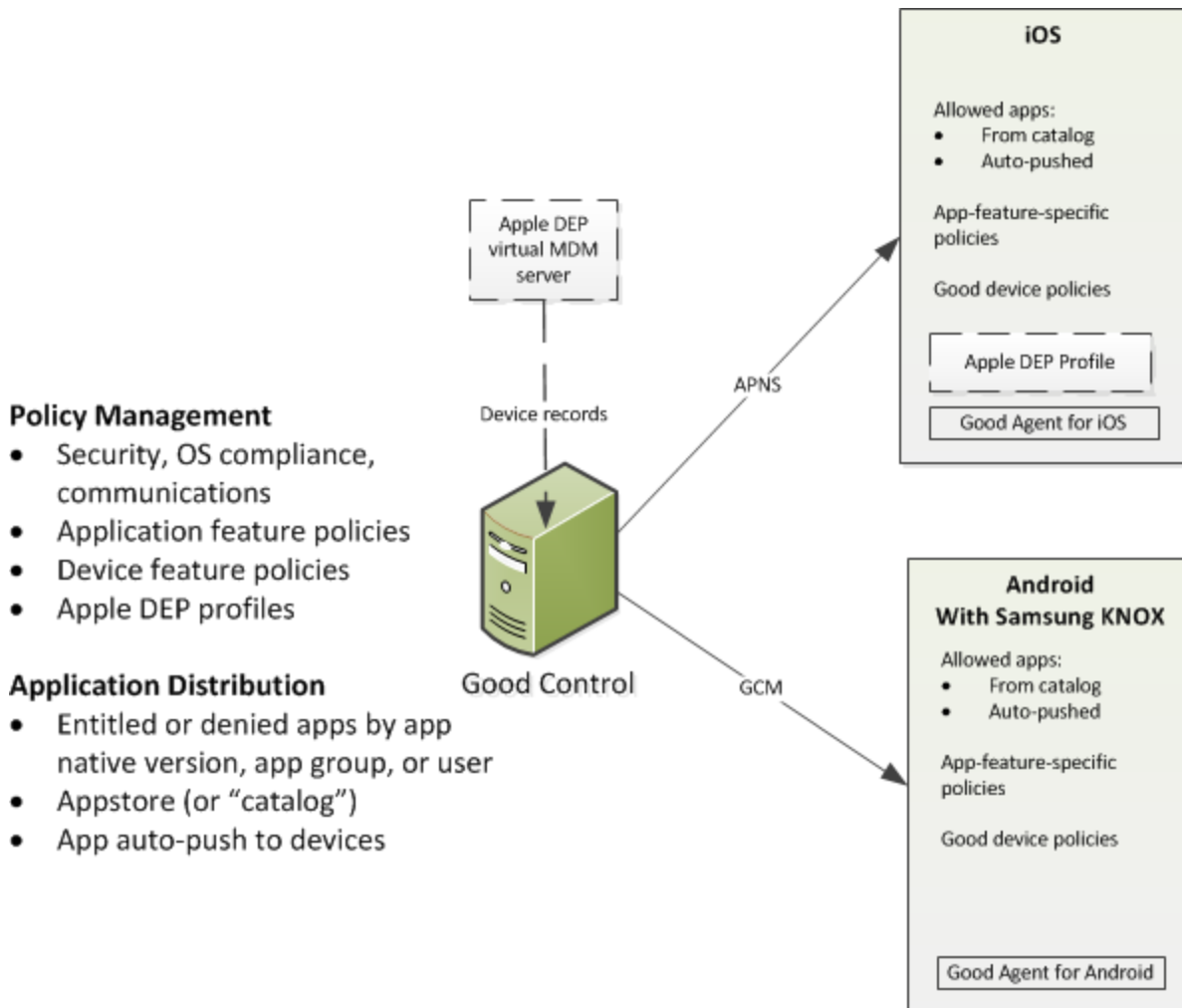
- Password quality
- Password length
- Password expiration duration
- Max # of failed password attempts
- Idle timeout after inactivity period
- Prevent last n passwords

### Restrictions

more details see [Windows Phone 8.1 Restrictable Features](#).

## Conceptual Overview to Good Device and Application Management

Good Technology's device management and application management are intrinsic parts of Good Control, which is the single console for managing policies for devices and for applications. The diagram below is a high-level, highly simplified, logical view of how the system works.



The GC administrator configures the system from start to finish. Device management and application management are intertwined to achieve distribution of approved applications, either auto-pushed to end-users' devices or selectable from a catalog defined by the administrator.

The administrator creates combinations of device and application policies into *policy sets*. The policy sets are then applied to app groups, which are administrator-defined collections of end-users who share common characteristics. The system then applies the defined policies to the devices and apps. Good Control policy is subdivided into modular parts:

- Basic security, such as authentication and OS compliance
- Application-specific features
- Device-specific features
- Apple DEP (Device Enrollment Program) profiles configure characteristics of iOS device activation and enrollment. Apple DEP, which is an optional feature of Good Control, is discussed in [Apple DEP: Background and Planning](#) and [Apple DEP Profiles and Devices](#).

An application on end users' Android and iOS devices, Good Agent enforces application and device policy on the device itself. For more information about Good Agent, see the documentation listed in [Good Dynamics Documentation](#).

Application distribution consists of:

- Entitling end users to applications on devices controls which apps are allowed by:
  - End-user-initiated selection and installation of applications via the administrator-defined catalog called the appstore.
  - Admin-initiated automatic push to devices of entitled applications.

**Note:** Automatic app push requires device management.

## Structure of Doc and Task-Oriented Workflows

Even though device and application management are integrated aspects of Good Control, this guide is divided somewhat arbitrarily into the following major parts. The guide is also task-oriented for the administrator. Detailed workflows for accomplishing all tasks are in the following sections:

- [Device Management](#) overview and [Device Management Administrator's Workflow](#)
- [Application Management](#) overview and [Application Management Administrator's Workflow](#)

## Good DM and AM Deployment Models

Good device management and application management are features of the Good Control server. As such, it is deployed in the same way as Good Control. There are two deployment models, in both of which the servers and other aspects of the management features are hosted by Good Technology:

- **Good Control Cloud.** In this model, an administrator can provision all major components of the solution in Good Technology's cloud, including a Good Control server.
- **On-premise.** In this model, the Good Control and Good Proxy servers are deployed on the customer's premises. Good Control and Good Proxy servers need connectivity to the Good NOC.

## Good DM and AM Installation Procedure

DM and AM are deployed along with Good Control itself. No additional installation or configuration is necessary.



## Relationship to Cloud GC: Feature Supported

The feature, service, server type, or software described here is fully supported on and compatible with Good Control Cloud.

## About Good Dynamics Software Version Numbers

The cover of this document shows the base or major version number of the product, but not the full, exact version number (which includes "point releases"), which can change over time while the major version number remains the same. The document, however, is always current with the latest release.

Product	Version
Good Control	2.2.511.26
Good Proxy	2.2.511.16
GD SDK for Android	2.1.1256
GD SDK for iOS	2.1.4439
GD SDK for Mac OS X	x.y.z
Good Launcher Library for Android	2.3.0.106
Good Launcher Library for iOS	2.3.0.161
GD SDK for Universal Windows Platform	
GD PhoneGap	2.1.78
Digital Authentication Framework (DAF) <ul style="list-style-type: none"><li>• Android</li><li>• iOS</li></ul>	<ul style="list-style-type: none"><li>• 2.1.207</li><li>• 2.1.171</li></ul>

If in doubt about the exact version number of a product, check the Good Developer Network for the latest release.

## Device Management

Good Technology's Device Management (DM ) allows you to securely connect and control iOS and Android devices, and Windows tablets and phones.

DM enables users to securely self-provision services and deploy internal apps while continuously enforcing security and protecting enterprise data on corporate- or employee-owned devices.

DM provides:

- Over-the-air (OTA) self-provisioning and connection configuration: The ability to set encryption, ActiveSync, VPN configuration and Wi-Fi settings with audit verification to streamline activations and eliminate the need for IT involvement.
- Security enforcement to continuously audit all connected devices and quarantine or revoke service for compromised devices. Security protection to maintain control of corporate information and selectively wipe only corporate data and apps, or all data, from managed devices with audit of successful completion.
- Simplifies and speeds app deployment with an enterprise-specific OTA catalog of mandatory, recommended and available apps.

Security Management allows faster and lower-cost adoption of productivity-enhancing devices; central control of corporate data (without impacting personal data); and enhanced security compliance across the enterprise.

DM enables IT to centrally manage and control all devices from a single unified console.

DM enables IT to fully manage the device life cycle from initial deployment to device retirement. Based on membership in Active Directory security groups, devices, supporting services and apps are provisioned and deployed over-the-air (OTA), leveraging user self-service to minimize operational overhead.

Security enforcement occurs on the device natively with customizing security settings per group-based policy and ensuring their persistence with continuous compliance enforcement. During the operation of the device, policy updates are made in near-real-time to combat emerging security threats and ensure that the device is operating at peak performance. Device retirement is done securely, OTA and automatically to complete the device life cycle.

## Requirements: Good Dynamics Software, Device OS, Certificates, and API Keys

The following are the minimum versions of Good Dynamics software for device management.

Product	Version
Good Control	2.2.511.26
Good Proxy	2.2.511.16
GD SDK for Android	

Product	Version
	2.1.1256
GD SDK for iOS	2.1.4439
GD SDK for Mac OS X	x.y.z
Good Launcher Library for Android	2.3.0.106
Good Launcher Library for iOS	2.3.0.161
GD SDK for Universal Windows Platform	
GD PhoneGap	2.1.78
Digital Authentication Framework (DAF) <ul style="list-style-type: none"> <li>Android</li> <li>iOS</li> </ul>	<ul style="list-style-type: none"> <li>2.1.207</li> <li>2.1.171</li> </ul>

## Other Requirements

- APNS: Apple Push Notification Service certificate from Apple, Inc., is used for data communications between Good DM and iOS devices.
- GCM: Google Cloud Messaging API keys from Google are needed for data communications between Good DM and Android devices.

Minimum Device OS and Capabilities	Needed by Administrator for Good Control		Software on End-User Device for DM Enrollment
	APNS Certificate	GCM API Keys	
iOS v6	Required		<ul style="list-style-type: none"> <li>• Corporate-owned enrollment: Safari</li> <li>• End-User Self-enrollment: <ul style="list-style-type: none"> <li>• Any application built with the minimum version of the GD SDK, such as Good Access</li> <li>• Safari</li> </ul> </li> </ul>
Android v4.0 with or		Required	For both kinds of enrollment: Good

Minimum Device OS and Capabilities	Needed by Administrator for Good Control		Software on End-User Device for DM Enrollment
	APNS Certificate	GCM API Keys	
without KNOX			Agent

## About Good for KNOX: No License Required

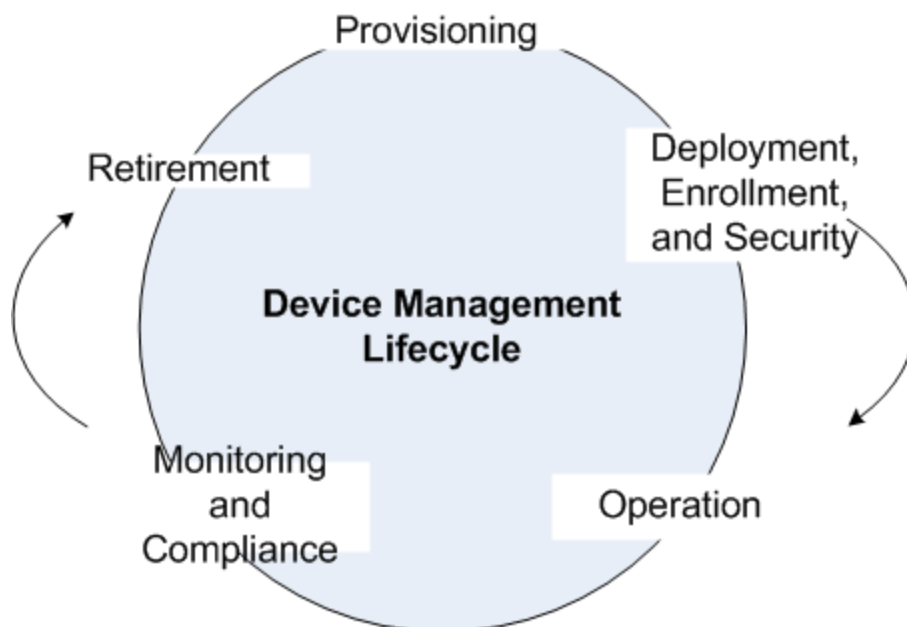
- The device you want to install Good Agent on must not be rooted.
- Good for KNOX is an underlying feature of Good Dynamics, which Good Agent relies on. To take advantage of Good for KNOX, your Samsung device must be running KNOX 2.1 or above.

**Note:** No license is required for Good for KNOX.

- Good for KNOX also requires your device to have the latest SE Android Policy (SPD) updates from Samsung. See the details in [Updating SE Android Policy on Samsung Devices](#).

## Device Management Lifecycle

The lifecycle of a managed device has the following distinct phases:



- Provisioning
- Deployment, Enrollment, and Security
- Operation

- Monitoring and Compliance
- Retirement

## Provisioning

Security policies and device configurations are provisioned from a simple to use web interface and applied according to groups defined within Active Directory. Policy settings reflect the native security enforcement provided by the managed device. For iOS and Android devices, security settings include:

- passcode requirements
- device restrictions
- mandatory support such as device encryption
- required and forbidden apps

The enterprise Information Technology (IT) department can auto-configure device features such as WiFi, VPN and e-mail. Non-Exchange mail server environments are also supported by Good (using ActiveSync), as are devices whose users are not issued e-mail addresses.

## Deployment, Enrollment, and Security

During the deployment phase, users can self-enroll a device (called BYOD, or "Bring Your Own Device", enrollment) or the administrator can enroll for the end-user (called "Corporate-owned" enrollment) to be managed and secured by Good Device Management according to the settings established in the provisioning phase.

During enrollment, DM applies the settings associated with certificate enrollment and device configuration to ensure only trusted users access enterprise services. It also ensures that devices are configured per established IT policies.

Typically, a user is directed by IT to an enrollment application or URL link to initiate activation of the device. The user is required to agree to terms of service prior to enrolling their device.

The user is authenticated, and the user's authorization to have a managed device is confirmed.

When enrollment is complete, required policies are pushed to the device.

DM ensures that incoming enrollment requests are only accepted if each user can be authenticated. The authentication check verifies the user's credentials, but also verifies that the user is a member of the default users group. Both have to be true before the user can proceed with enrollment.

Information about the device is collected before Certificate Enrollment begins. If the user passes the authentication step, a request is generated to the Certificate Authority (CA) embedded within the Good server via the Simple Certificate Enrollment Protocol (SCEP) protocol.

The certificate is installed on the device automatically, permitting the device to then receive trusted configuration profiles customized for only that unique device, sent by the Good server.

After the Good server verifies the device, it responds with a signed certificate. The device uses the new certificate to contact the Good server and pass a set of device attributes back to it. These attributes are used to ensure device meets IT specifications.

Once verified, the profile service transmits a configuration profile to the device containing policies and settings that are used to configure the device for use in the enterprise environment. The configuration profile contains the settings and restrictions needed within the enterprise environment, including corporate MS Exchange (or another ActiveSync enabled mail server), VPN, and Wi-Fi configurations.

## Operation

Once configured and activated, Good DM continually monitors the device reporting the results to the Service Desk:

- For iOS devices, the Good server connects with the Apple Push Notification Service (APNS) to enable policy updates and compliance checks.
- Good provides support for management of Android devices through integration with the Good Agent for Android application, which users must install and activate. Devices enrolled with Good Agent for Android can be monitored and supported via the GC console.

## Post-Enrollment Monitoring and Compliance

Policy updates are sent to the device transparently, enabling IT administrators to react to new security threats and changes to their environment.

The GC server performs regular compliance checks on devices, gathering and correlating information from several data sources to measure security compliance in near-real-time. For those devices deemed to be non-compliant, the Good server automatically takes action as dictated by IT policy, including alerts, notification, and wiping the device. Devices can be wiped completely, or users may wipe the device of corporate data only.

## Retirement

In the retirement phase, the user's device is securely decommissioned and removed from the enterprise environment. Retirement scenarios include:

- lost device
- device upgrade
- employee termination

## Example Business Scenarios

Here are some "real-world" business scenarios that illustrate many of the capabilities of Good device management.

Two different fictitious companies have different DM requirements:

- Scenario 1: DM for Corporate-Owned Device, but Not BYOD Devices, with WiFi
- Scenario 2: DM for BYOD Devices, but Not Corporate-Owned Devices, with VPN

Both companies plan on deploying both iOS and Android devices.

### Scenario 1: Corporate-Owned Devices, but Not BYOD Devices, with WiFi

A company wants to deploy both corporate-owned and BYOD devices:

- For corporate-owned devices, they want to use DM to enforce a passcode on the device and preconfigure the corporate WiFi.
- For BYOD devices, they do not want to enforce DM .

#### High-level Steps in Good Control

For the correlation between these tasks and the menus in Good Control, see the table in [Device Management Administrator's Workflow](#)

1. Setup your APNS certificate.
2. Setup your Google Cloud Messaging API keys.
3. Create a device configuration for WIFI management.
4. Create a device policy to enforce a passcode on the device.
5. Associate your device configuration for WIFI to your device Policy.
6. Create a policy set.
7. Associate your device policy to your policy set
  - Ensure that the device policy is only associated to **Corporate Owned / Enrolled by Admin** devices.
  - Ensure that NO Device Policy is associated to **BYOD / Enrolled by User** devices
8. Associate the policy set with the end-user.
9. For Android users, entitle the user to Good Agent.

#### On the End-User Devices: iOS

Enter user's email address and the GC-provided device enrollment key into Safari at the URL displayed by the GC.

#### On the End-User Devices: Android

1. Download the Good Agent application.
2. Start Good Agent.
3. Tap **Company Owned Setup**.
4. Enter the user's email address and the enrollment key from GC.
5. Step through the actual enrollment process.
6. After enrollment, you are prompted to activate Good Agent.
7. Generate an access key and enter it on the device.

On the End-User Devices: Windows Tablet

Follow the steps for corporate-owned enrollment in [Enrolling Devices: Administrator's Tasks](#).

## Scenario 2: BYOD Devices, but Not Corporate-Owned Devices, with VPN

A company wants to deploy both corporate-owned and BYOD devices:

- For corporate-owned devices, they do not want to enforce DM.
- For BYOD devices, DM will enforce a device passcode with VPN.

### High-level Steps in Good Control

For the correlation between these tasks and the menus in Good Control, see the table in [Device Management Administrator's Workflow](#)

1. Setup your APNS certificate.
2. Setup your Google Cloud Messaging API keys.
3. Create a device configuration for VPN management.
4. Create a device policy to enforce a passcode on the device.
5. Associate your device configuration for VPN to your device Policy.
6. Create a policy set.
7. Associate your device policy to your policy set
  - Ensure that the device policy is only associated to **BYOD / Enrolled by User** devices.
  - Ensure that NO Device Policy is associated to **Corporate Owned / Enrolled by Admin** devices.
8. Associate the policy set with the end-user.
9. For Android users, entitle the user to Good Agent.

#### On the End-User Devices: iOS

- Download and provision a Good Dynamics app that has been built with the required version of the GD SDK. Once provisioned, the application steps you through the device management enrollment process.

#### On the End-User Devices: Android

1. Download and install Good Agent. You have a choice:
  - a. Install Good Agent directly.
  - b. You can download any GD-based application and provision it. If device management enrollment is required, your application is blocked. You are prompted to enroll the device. Tap **Install Good Agent**, go to the Play Store, install Good Agent, and open it.
2. Tap **Next**.
3. If you have already previously activated other GD-based applications, you can choose to use Easy Activation



to activate Good Agent, or you can activate Good Agent with the GC-supplied activation key.

4. After activation, step through the actual device management enrollment process.

#### On the End-User Devices: Windows Tablet

Follow the steps for corporate-owned enrollment in [Enrolling Devices: Administrator's Tasks](#).

## Planning Your DM Deployment: Devices, Policies, People

Planning your deployment of device management is perhaps more time-consuming than the day-to-day operations. A generalized workflow for both administrators is in [Device Management Administrator's Workflow](#). The tasks described there can help you with your plans.

The precise preparations you need depend on many factors, some of which are raised as questions below.

### How are your end-users organized in your enterprise?

You might need special policies for one group but general policies for the others.

With an organization chart, start with the most general requirements that apply to the majority of organizational groups and refine the requirements for the special groups that need more strict controls.

### What are your end-users' geographic locations?

How do they access your network?

You can separate your device policies by geographic location or by the method of accessing your network: VPN, WiFi, email, and other kinds of device configurations.

### Do your end-users use iOS devices, Android devices, Android with KNOX, Windows devices, or all?

If the end-users' devices are homogeneous, you need policies only for that one type of device. Most likely, you need several sets of policies.

- To manage iOS devices, the system relies on the Apple Push Notification Service (APNS).

**Note:** You need to obtain an APNS certificate from Apple, Inc., to install in Good Control. For more information, see [Working with APNS Certificates](#).

- To manage Android devices, the system relies on the Google Cloud Messaging API.

**Note:** You need to obtain GCM API Keys to install in Good Control. For more information, see [Obtaining Google Cloud Messaging API Keys](#).

- Device management on Android is limited unless you rely on Samsung's KNOX. KNOX gives you the most features that can be managed. You do not need to do anything to take advantage of KNOX.
- Client applications on end-users' devices:
  - On iOS, your end-users must activate Good Agent for iOS. For details, see [DM Enrollment: Good Agent for iOS](#).
  - On Android devices, your end-users must activate Good Agent for Android. For details, see [DM Enrollment:](#)

*Good Agent for Android.*

- On Windows tablets, no client application is required for device management enrollment.

## Do you plan on relying on Apple DEP?

Apple Inc.'s Device Enrollment Program (DEP, described at <http://www.apple.com/business/dep/>) is for businesses to manage their devices via Apple's service. Good Control has an interface to Apple DEP so you can manage all your devices through the single Good Control console.

Some considerations in planning your Apple DEP deployment are detailed [Apple DEP: Background and Planning](#).

## Which device features do you want to manage?

The full set of device policies is comprehensive, large, and listed in [Device Policy Reference](#) to help you formulate which features on the device you want to manage.

In addition, log into the Good Control console to see how device policies are grouped. The names and descriptions of policies are clearly related to device-specific features.

## Will the administrator provision and enroll devices?

Or will the end-users voluntarily enroll their own devices? In either case, for the administrator, the preparations and the process are nearly identical.

If the administrator must retain control over the physical device itself to ensure that enrollment is accomplished, then the administrator must provision and enroll all devices before giving them to the end-users. Otherwise, the administrator does the same setup of device policies and configurations and sends the enrollment details via a system-generated email message to the end-user.

You can maintain two sets of device policies, one for end-user self-enrolled devices and one for administrator-enrolled devices. For more information, see [Different Policies by Type of Device Enrollment; Enrollment Key Expiration](#).

## Corporate-Owned Enrollment vs End-User Self-Enrollment (or BYOD)

There are two general kinds of enrollment in device management. They are initiated by the administrator of Good Control with two different buttons on the **Manage Users** screen.

- Corporate-owned: The administrator retains full control of the physical devices. The administrator prepares for the enrollment, provisions the device, and enrolls it himself, before giving the device to the end-user.

**Important:** In Good Control, corporate-owned device enrollment is initiated under **Manage Users** with the **New Device Enrollment Key** button.

- End-user self-enrollment (or "Bring Your Own Device", BYOD): The administrator only prepares the enrollment, but the end-user enrolls his own device himself.

**Important:** In Good Control, the administrator initiates end-user self-enrollment under **Manage Users** with the **New Access Key** button.

## Apple DEP: Background and Planning

Apple Inc.'s Device Enrollment Program (DEP, described at <http://www.apple.com/business/dep/>) is for businesses to manage their devices via Apple's service. Good Control has an interface to Apple DEP so you can manage all your devices through the single Good Control console.

### How Apple DEP with Good Control Works

With Apple DEP and Good Control, after one-time setup with Apple, you allow Good Control to access your virtual Apple DEP MDM server, which contains all the information about your devices (serial numbers and more). This information is synchronized between Apple and Good Control once every hour, although you can force the synchronization sooner, if you require.

You then use Good Control to define "DEP profiles", which are sets of device enrollment and activation characteristics you establish. In Good Control, you can operate Apple DEP in three primary modes:

- Auto-pilot mode: a profile you define is applied automatically to all new devices.
- Manual mode: You yourself apply a profile to specific devices.
- Combo mode: you define a DEP profile that are automatically applied and you also manually apply profiles or policies to specific devices.

After defining the DEP profile, you associate it with a GC policy set, which is then applied to specific groups of users.

Profiles are applied to the device only when the device is activated or after it is factory reset. Thus, one risk of "Manual" mode is that an end-user might receive a device and activate it before you have applied a DEP profile to it.

### Supervised and Userless Devices

In addition to managing devices that are in use by specific end-users (which is a loose definition of *supervised devices*), the GC can also manage so-called *userless devices*, which do not belong to any particular human being. Examples of userless devices are kiosk equipment, such as at conferences.

Technically, a supervised device is an Apple device that has been entered into Apple DEP or has been configured using the Apple Configurator. Apple provides an article to determine if a device is supervised or not. See <https://support.apple.com/en-us/HT202837>.

### Good Agent for iOS is Auto-Pushed to Devices

When you implement Apple DEP, when a profile is applied to a device the Good Agent for iOS application is auto-pushed to devices. The end user is prompted to install it.

## Planning Considerations

Here are some planning considerations for Apple DEP with Good Control:

1. Before you sign up for Apple DEP, consider creating a single, "global" Apple DEP account, rather than multiple accounts, one per sub-organization. The reason for this recommendation is that Good Control interfaces with only a single Apple DEP virtual MDM server.
2. If you purchase Apple devices through carriers or resellers, before you sign up for Apple DEP, verify with those carriers and resellers that they too support Apple DEP. If they do not support Apple DEP, setting up the DEP interfaces in Good Control will not be as advantageous as it could be otherwise.
3. Protect your Apple DEP public certificate, which you generate in Good Control. In addition to storing it in the GC, keep a backup along with your system backup, in case you ever need to re-insert that cert into the GC from backup.
4. You can create as many Apple DEP profiles as you need, but be advised that you cannot edit a profile (that is, change it) after it is created.
5. The device access settings of your DEP-related device policies must be set to full access. That is, every setting must be enabled.

## Important: Whitelist the DM Servers in Good Control proxy.urls After Upgrade

If you upgrade to this version of Good Control, In your Good Control setup, make sure that you whitelist the Good DM servers so that your GC can communicate with them.

**Note:** Add these names or IP addresses to the GC server property **proxy.urls** in **Servers > Server Properties** tab.

Hostname	IP Address	Port
bxenroll.good.com	206.124.122.130	443
bxcheckin.good.com	206.124.122.131	443

## Migration to Good DM

Here are the high-level steps for the general process for migrating from GFE or Boxtone device management to Good device management.

**Note:** Consider contacting Good Professional Services to assist in the migration.

## IT Admin

Some options you can consider to reduce cost:

- Custom scripts or professional services help to minimize manual effort.
  - You can turn on automated user/policy creation process between Good Mobile Control (GMC) and Good Control.
1. Set up DM certificates and keys. See [Certificates and API Keys](#).
  2. Add users to Good Control. See the Good Control online help topics relating to adding users.
  3. Add compliance and device policies. See [Implementing Your Device Policies](#).
  4. Add device configurations. See [Device Configurations](#).
  5. Assign policies to users. See the Good Control online help topics relating to **App Groups**.
  6. Turn off GFE MDM for users who must be migrated. See the GFE documentation for details.
  7. Optionally, remove the GFE application from Good Control.

## End Users

1. On MDM removal via GMC, install any GD app, such as Good Work or Good Access.
2. Complete DM enrollment
  - For iOS see the [Good Access Secure Browser Product Guide](#). The Good DM profile must be installed, replacing the GFE profile, which must be removed.
  - Android DM enrollment requires installing Good Agent. See [BYO DM Enrollment on Android](#).
3. Optionally, remove GFE app from the device.

## Device Management: Known Limitations

The following are known issues in Good device management on the indicated platforms.

Description of limitation		OS
1	DEP 'Android Migration' is truncated when 'Restore' screen is skipped. (Android Migration is only applicable with restore is allowed.)	iOS
2	Managed app status is reported incorrectly as "ManagedButUninstalled" during DEP device "userless" enrollment or when app installation failed on device.	iOS
3	If simple password policy is applied on the device, user is prompted "PIN required" during upgrade from Windows 8.1 to Windows 10 on Windows Phone.	Windows
4	If user initiates the remote device wipe, GC can not unenroll the device.	iOS
5	"Disable custom email accounts" restriction allows to add non-Microsoft email accounts and does not allow the removal on an existing existing account on the device. This is a limitation imposed	Windows

Description of limitation		OS
	by Windows itself.	
6	Win32 Network Adapter is not available for Windows 10 tablet (is always false for Windows 10 tablet).	Windows
7	<p>If something causes MDM to not receive a device unenroll event, GC not remove the device item from its display. Thus, if the user re-enrolls a device, the GC might display duplicate entries for the same device.</p> <p><b>Workaround:</b> After 10 days, MDM backend service will remove the orphaned device and send unenroll event to GC.</p>	Windows
8	Windows Tablet doesn't support Remote Lock. The Remote Lock is only supported in Windows 10 Mobile Insider Preview.	Windows
9	<p>Upgrade to this version of Good Control causes new policies to be pushed to any supervised devices that might already be enrolled before the upgrade. (Supervised devices are those that have a custom iOS configuration created with the Apple Configurator.)</p> <p>The Good device management service will reconcile policies to ensure that the most restrictive policies apply.</p>	iOS
10	Duplicate native identifiers can prevent the proper installation or upgrade of your own app.	iOS Android
11	Microsoft documentation states that a device password for a local account can be up to 16 characters long, but the documentation is incorrect. The maximum length of a local account device password is 14 characters.	Windows

## Windows Tablet Device Management: Known Limitations

For managing Windows tablets, Good device management services rely on Microsoft's Windows 8.1 operating system, the Windows Push Notification Service (WNS), and other Microsoft software discussed below.

Described here is some of the behavior of Good device management of Windows tablets because of this reliance on Microsoft.

### End-user Unenrollment Cannot be Detected

The Windows implementation of the Open Mobile Alliance (OMA) DM client does not send meaningful information to the Good device management service when an end-user unenrolls from Good device

management. In this case, Good device management services record that the end-user device is still enrolled, although it might not be.

## Scheduled Maintenance Works Only on Surface Pro Tablets

Windows' scheduled maintenance feature is supposed to automatically check with the Good device management service for any new policies or other configuration updates. However, with Windows 8.1 operating system, scheduled maintenance works correctly only on Surface Pro tablets, not other tablet models.

To work around this limitation to communicate with other tablet models, Good device management relies on Microsoft's Windows Push Notification Service (WNS).

## WNS Channel URI Errors Can Cause Unenrollment

Good device management depends on Microsoft's Windows Push Notification Service (WNS) to communicate with enrolled devices, for policy and other updates.

In the unlikely case that Microsoft's WNS servers return an error, Good device management cannot communicate with the devices. In this circumstance Good device management unenrolls the device, which is reported in Good Control.

## About the Windows Update Field in Device Status in Good Control

On end-users' Windows devices, the Windows operating system's update feature has four different settings:

1. Scheduled
2. Choose
3. Auto
4. Disabled

However, for device management status in Good Control, the Windows operating system does not return the "Scheduled" value to Good device management. Good device management treats the "Scheduled" and "Choose" values as equivalent. For "Scheduled", the **Windows Update** field in GC's device status shows **Choose**.

## Behavior of Password Restrictions on Windows Tablet

The behavior of password restrictions on Windows tablet devices varies from other platforms. A key distinction is whether the device is enrolled by a Microsoft account (one created on a Microsoft service) or an account that is local to the device (called a *local account*).

Device Setting in Good Control	Microsoft Account on Windows Tablet	Local Account on Windows Tablet
Require a password	A password is always required.	A password must have been set on the device prior to enrollment.  After a password has been set, it cannot be removed or changed.



Device Setting in Good Control	Microsoft Account on Windows Tablet	Local Account on Windows Tablet
Quality	Windows does not support the concept of password quality.	Windows does not support the concept of password quality.
<ul style="list-style-type: none"> <li>Minimum password contains...</li> <li>Minimum password length</li> </ul>	Allow from 4 to 16 characters	<ul style="list-style-type: none"> <li>Allow up to 14 characters</li> <li>Cannot be set less restrictive.</li> <li>After length has been set, it cannot be removed or changed on the device.</li> </ul>
Password expiration	Not applicable	<ul style="list-style-type: none"> <li>Allow from zero to 731 days.</li> <li>Cannot be set less restrictive.</li> <li>After expiration period is set it cannot be removed or changed on the device.</li> </ul>
Prevent reuse of last password (password history)	Not applicable	Allow from zero to 24 unique passwords Cannot be set less restrictive. Once enforced on the device, the setting cannot be removed or changed.
Device lockout (maximum number of allowed failed attempts)	Allow from four to 10 Once set, cannot be made less restrictive. If device does not have encryption enabled, user must restart device. If device has encryption enabled, locked-out user has two options: <ul style="list-style-type: none"> <li>Factory-reset the device</li> <li>Provide lockout code supplied by Microsoft</li> </ul>	Allow from four to 10 Once set, cannot be made less restrictive. Locked out device is restarted.
Screen locks after X minutes of inactivity (also called inactivity timeout)	One to 120 minutes Once set, cannot be made less restrictive.	One to 120 minutes Once set, cannot be made less restrictive.
Complex combinations of characters cannot be managed because they are not displayed in the GC console.		



Device Setting in Good Control	Microsoft Account on Windows Tablet	Local Account on Windows Tablet
Disallow convenience logon is set OFF and cannot be managed via the GC console.		

**Effect of "Reset Security Policies"**

The end-user can manually remove them with the “Reset Security Policies” option on the Windows tablet. If the end-user initiates “Reset Security Policies,” the password restrictions are not enforced on the Local Account and the password can be removed.

**After Unenrollment, Password Restrictions Still Enforced**

After device management deactivation (unenrollment) all password restrictions are still present and enforced on the device. They can be removed with the “Reset Security Policies” option on the device. See [Effect of "Reset Security Policies"](#) .

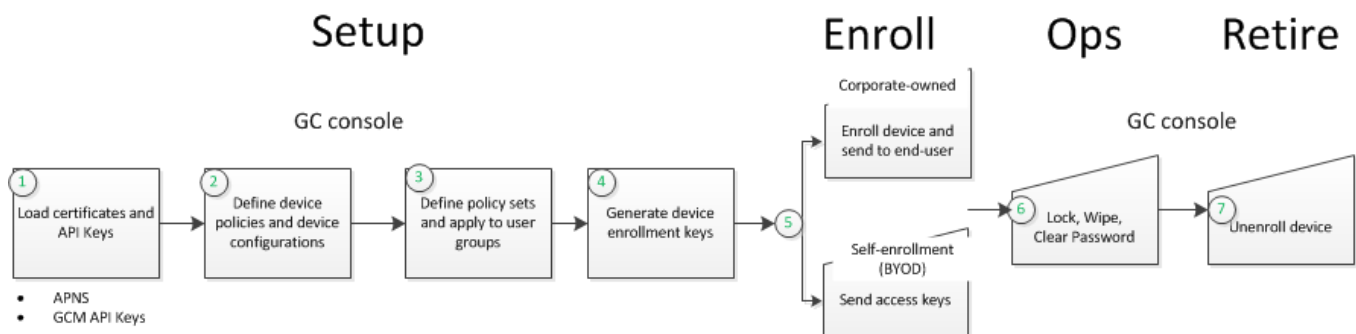
## Device Management Administrator's Workflow

Included here are the high-level workflows of device management for the administrator. These workflow corresponds to all phases of the [Device Management Lifecycle](#)

**Important:** You need to complete these administrator tasks in the order presented.

Detailed task steps for the administrator correspond to menu items and settings in Good Control. Below is the correlation between the administrator's workflow and the left-hand navigation menu selections in Good Control to accomplish them.

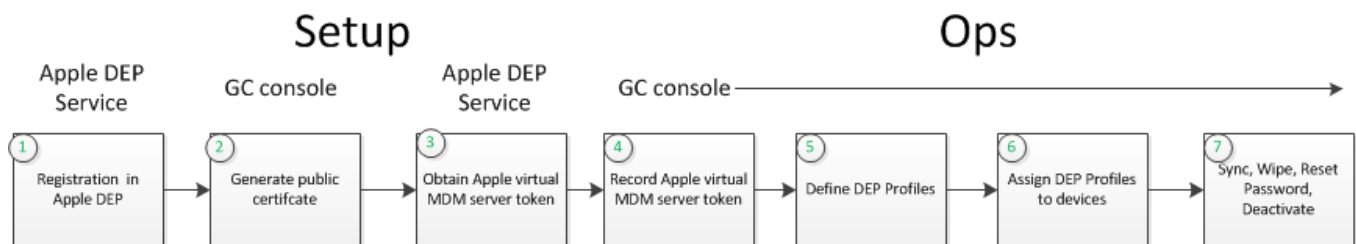
### Non-Apple-DEP Devices



Task Number	Task Description	Menu Selections in Good Control
1	Load certificates and API Keys	<ul style="list-style-type: none"> <li>• <b>Certificates &gt; APNS.</b> Device Management &gt; iOS. See <a href="#">Working with APNS Certificates</a> .</li> <li>• <b>Licenses &gt; API Keys.</b> Device Management &gt; Android tab. See <a href="#">Obtaining Google Cloud Messaging API Keys</a> .</li> </ul>
2	Define device policies and device configurations	<ul style="list-style-type: none"> <li>• <b>Device Policies.</b> See <a href="#">Policies</a> .</li> <li>• <b>Device Configurations.</b> See <a href="#">Device Configurations</a> .</li> </ul>
3	Define policy sets and apply to user groups/applications	<ul style="list-style-type: none"> <li>• <b>Policy Sets</b></li> </ul>
4	Generate device enrollment keys	<b>Manage Users &gt; Edit a selected user:</b> <ul style="list-style-type: none"> <li>• <b>New Device Enrollment Key:</b> Corporate-owned enrollment.</li> <li>• <b>New Access Key:</b> BYOD or end-user self-enrollment.</li> </ul>

Task Number	Task Description	Menu Selections in Good Control
		See <a href="#">DM Enrollment</a> .
5	Corporate-Owned device enrollment	Not done in GC; done on the device. Follow same workflow as end-user for iOS or Android.
6	Operational tasks	<ul style="list-style-type: none"> <li>• <b>Manage Users &gt; Edit a selected user &gt; Devices and Keys:</b> <ul style="list-style-type: none"> <li>• Lock Device</li> <li>• Clear Device Password: for iOS only.</li> <li>• Wipe Device</li> <li>• Deactivate Device</li> <li>• Installed Apps</li> </ul> </li> </ul> See <a href="#">DM Operational Tasks: Device Status, Lock, Clear Password, Wipe, and Deactivate</a> .
7	Unenroll device	<b>Manage Users &gt; Edit a selected user &gt; Devices and Keys &gt; Deactivate Device.</b> See <a href="#">Unenrolling a Device from MDM</a> .

## Apple DEP Devices



Task Number	Task Description	Menu Selections in Good Control or Elsewhere
1	Registration and participation in Apple DEP.	Apple Inc.'s Device Enrollment Program (DEP) is described at <a href="http://www.apple.com/business/dep/">http://www.apple.com/business/dep/</a> . You must first register with Apple.
2	Generate public key for use with DEP	<ul style="list-style-type: none"> <li>• <b>Device Management &gt; iOS tab &gt; DEP Account Edit &gt; Generate Public Key &gt; Download</b></li> <li>• Login to Apple's portal and upload your public key.</li> </ul>

Task Number	Task Description	Menu Selections in Good Control or Elsewhere
		See <a href="#">One-time Setup with Apple for DEP Profiles in Good Control</a> .
3	Obtain Apple virtual MDM server token	Apple Inc.'s Device Enrollment Program (DEP) is described at <a href="http://www.apple.com/business/dep/">http://www.apple.com/business/dep/</a> . Apple supplies you with a virtual MDM server token.
4	Record Apple virtual MDM server token	<ul style="list-style-type: none"> <li>• Device Management &gt; iOS tab &gt; DEP Account Edit &gt; Import MDM Server Token</li> <li>• Upload the token from step 4.</li> </ul> See <a href="#">One-time Setup with Apple for DEP Profiles in Good Control</a> .
5	Define DEP Profiles	Apple DEP Profiles See <a href="#">Defining DEP Profiles in Good Control</a> .
6	Assign DEP Profiles to Devices	Apple DEP Devices > select devices > Assign DEP Profile See <a href="#">Assigning DEP Profiles to Devices</a> .
7	Operational tasks	Apple DEP Devices > <i>select devices</i> > Action menu: <ul style="list-style-type: none"> <li>• Sync Now</li> <li>• Wipe</li> <li>• Reset Password</li> <li>• Deactivate Device</li> <li>• Export in CSV</li> </ul> See <a href="#">DEP Device Actions</a> .

## Blacklisting or Whitelisting Applications on Devices

In Good Control's **Manage Apps**, the **Blacklist** and **Whitelist** tabs give you large-grained control over the applications not allowed or allowed to run on end-user devices:

- Blacklist: Applications not allowed to run on the device
- Whitelist: The only applications allowed to run on the device

### Behavior

The precise effect on a device depends on the operating system and type of application.

If your device policy checks compliance against the blacklist, then applications on the blacklist cannot be run on the device, subject to the device's operating system constraints.

OS	How Enforced
<ul style="list-style-type: none"> <li>iOS</li> <li>Android</li> </ul>	<p>The iOS and Android (without Samsung KNOX) operating systems do not have any programmatic mechanism to enforce the restrictions.</p> <p>If email notification is configured, non-compliance is reported in email. For details about compliance emails, see <a href="#">Configuring Compliance Emails</a>.</p>
Android with Samsung KNOX	<p>Disallowed applications (either blacklisted or not whitelisted) are blocked or removed from the device.</p> <p>If email notification is configured, non-compliance is reported in email. For details about compliance emails, see <a href="#">Configuring Compliance Emails</a>.</p>

If your device policy checks compliance against the whitelist, then applications not on the whitelist cannot be run on the device, subject to the device's operating system constraints.

The behavior of blacklisting or whitelisting is different for Good-based applications (those that have a GD App ID) and non-Good-based applications:

- Apps added to the whitelist are displayed in the user-accessible application catalog and in case of Good-based apps are permitted to run.
- However, apps added to blacklist are *not* displayed in the user-accessible application catalog and in the case of Good-based apps are *not* permitted to run.

## Steps for Blacklisting or Whitelisting

The steps for blacklisting and whitelisting are nearly identical. You need to know the following:

- Android: The package name of the application
- iOS: The bundle ID of the application
- The device policy you want to use to apply the lists

The steps have the following general parts:

- Defining the blacklist or whitelist: **Manage Apps > Blacklist** tab or **Whitelist** tab
- Applying the list in a device policy: **Device Policies > edit a policy > General > Check compliance against App Blacklist or App Whitelist**

1. Navigate to **Manage Apps**.
2. Click either the **Blacklist** or the **Whitelist** tab.
3. Click **Add App**.

4. Click either **Android App** or **Apple iOS App**.
  - For Android applications, enter the package name.
  - For iOS applications, enter the bundle ID.
5. Click **Blacklist** or **Whitelist**, or click **Cancel** to discard your changes.
6. Navigate to **Device Policies > edit a policy > General**
7. Click **Edit**.
8. Find the setting: **Check compliance against**
9. Make sure the **ON** radio button is active.
10. From the pulldown select either **App Blacklist** or **App Whitelist**.
11. Click **Save** to save your changes or **Cancel** to discard them.

### Steps for Removing Apps from Blacklist or Whitelist

1. Navigate to **Manage Apps**.
2. Click either the **Blacklist** or the **Whitelist** tab.
3. On either the **Blacklist** or the **Whitelist** tab, to select all Android applications or all iOS applications, click the appropriate checkbox above the list, or scroll through the list to checkmark the desired applications.
4. Click **Remove App**.

## Enabling Device Management in Good Control

If DM has not been enabled in your Good Control server, you cannot see the user interface related to it.

### To enable DM in Good Control:

1. Navigate to **Servers > Server Properties** tab.
2. Scroll to find the property **gc.mdm.enabled**.
3. Check the property's checkbox.
4. In the upper left, click **Submit**.
5. Click **OK** to the acknowledgment that the properties have been updated.
6. Log out of Good Control.
7. Allow approximately 30 seconds to pass while the property change takes effect.

After you log back in, you will see additional DM-related entries in the navigation and elsewhere, as documented in these topics.

## Good Control Properties for Allowable-New-Device Platforms

The following server properties in Good Control enable or disable new devices of the indicated platform.

By default, new devices are allowed.

**To set properties in Good Control:**

1. Navigate to **Servers > Settings** tab.
2. Find the desired property.
3. Set the property.
4. Click **Save** to retain your changes or **Cancel** to discard them.

Property	Description
allow.new.android.device	Android
allow.new.iOS.device	iOS
allow.new.Windows.device	All Windows devices other than Windows Phone, such as Windows tablet
allow.new.WindowsPhone.device	Windows Phone

## Configuring Compliance Emails

When end-users' device become out compliance with the policies you set, the system can send email to the end-users to advise them of the non-compliant devices

**Important:** Sending compliance emails is not enabled by default. Adding a value for the property **mdm.compliance.email.admin** (the administrator's email address) enables compliance emails

Compliance emails are controlled by properties you set on Good Control's **Servers> Server Properties** tab. Except for **mdm.compliance.email.admin** all properties are templated and include variables that are populated when email is sent.

Property	Meaning
mdm.compliance.admin.email	Email address of the Good Control administrator in standard Internet email address format, like <b>someone@somewhere.com</b> .
mdm.compliance.email.body	Body of the email message. <div style="border: 1px solid gray; padding: 5px; margin-top: 5px;"><b>Note:</b> Do not change the variable names embedded in the template.</div>
mdm.compliance.email.sender	Display name of sender, like "Good Mobile Administrator".



Property	Meaning
mdm.compliance.email.subject	<div>Subject line of non-compliance email.</div> <div><b>Important:</b> Do not change the variable names embedded in the template.</div>

## Certificates and API Keys

You need SSL certificates and some third-party API keys for device management, as shown below.

- APNS: Apple Push Notification Service certificate from Apple, Inc., is used for data communications between Good DM and iOS devices.
- GCM: Google Cloud Messaging API keys from Google are needed for data communications between Good DM and Android devices.

Device OS and Capabilities	APNS Certificate	GCM API Keys
iOS v6	Required	
Android v4.1 with or without KNOX		Required

### Working with APNS Certificates

Apple Push Notification Service (APNS) certificates are needed to secure the communications between the system and end-users' iOS devices.

**Note:** Before you work with APNS certificates, you need to have an account on the Apple Push Certificates Portal at <https://identity.apple.com/pushcert/>.

In Good Control's **Device Management > iOS** tab, you store certificates needed for communication with end-users' iOS devices. The general process is as follows:

1. Generate a Certificate Signing Request (CSR) to load into to the Apple Push Certificates Portal to obtain your APNS certificates.
2. Upload APNS certificates after you receive them from Apple.

### Generating a CSR

The Certificate Signing Requests (CSRs) from GC are digitally signed by Good Technology Corporation.

**To download a CSR to supply to Apple, Inc.:**

1. Navigate to **Device Management > iOS** tab.
2. Click **Generate CSR**.
3. Note the location of and name of the CSR file on your local machine.
4. Log in to your account on Apple's APNS server.
5. Upload the CSR you generated from Good Control.
6. Download the returned certificate from Apple.

## Uploading an APNS Certificate

After you receive from Apple your certificate for use with APNS, upload it on the **Certificates > APNS** screen.

**To upload an APNS certificate:**

1. Navigate to **Device Management > iOS** tab.
2. On the far right, click **Upload**.
3. Click **Browse** to navigate to and open the desired certificate file that you received from Apple on your local computer.
4. Click **Upload**.

Results of the upload are displayed.

## Obtaining Google Cloud Messaging API Keys

These are the details for obtaining keys for the Google Cloud Messaging (GCM) API, which is used by Good DM for communication between the DM service and Android devices.

### Prerequisites

You must have a Google account. Avoid using your personal account.

### Steps

After getting the API key from Google, you will enter its name and the value of the key into Good Control.

1. In a browser, open <https://console.developers.google.com> and login with any account you want to use.
2. If this is the first time you have created a project, follow the leading prompts to create it.
3. Under the heading **Mobile APIs**, click **Google Cloud Messaging**.
4. Click **Enable API**.
5. In the left nav, click **Credentials**.
6. Click **Create Credentials**, and select **API Key**.
7. Click **Server key**.
8. Enter a mnemonic name for this key.
9. Make a note of this name, because you will enter it into Good Control.
10. Leave the field **Accept requests from these server IP addresses** empty.
11. Click **Create**.
12. Copy the displayed API key and save it in a file.
13. Click **OK**.

You now have a copy of the project name and the API key you need to add to Good Control.

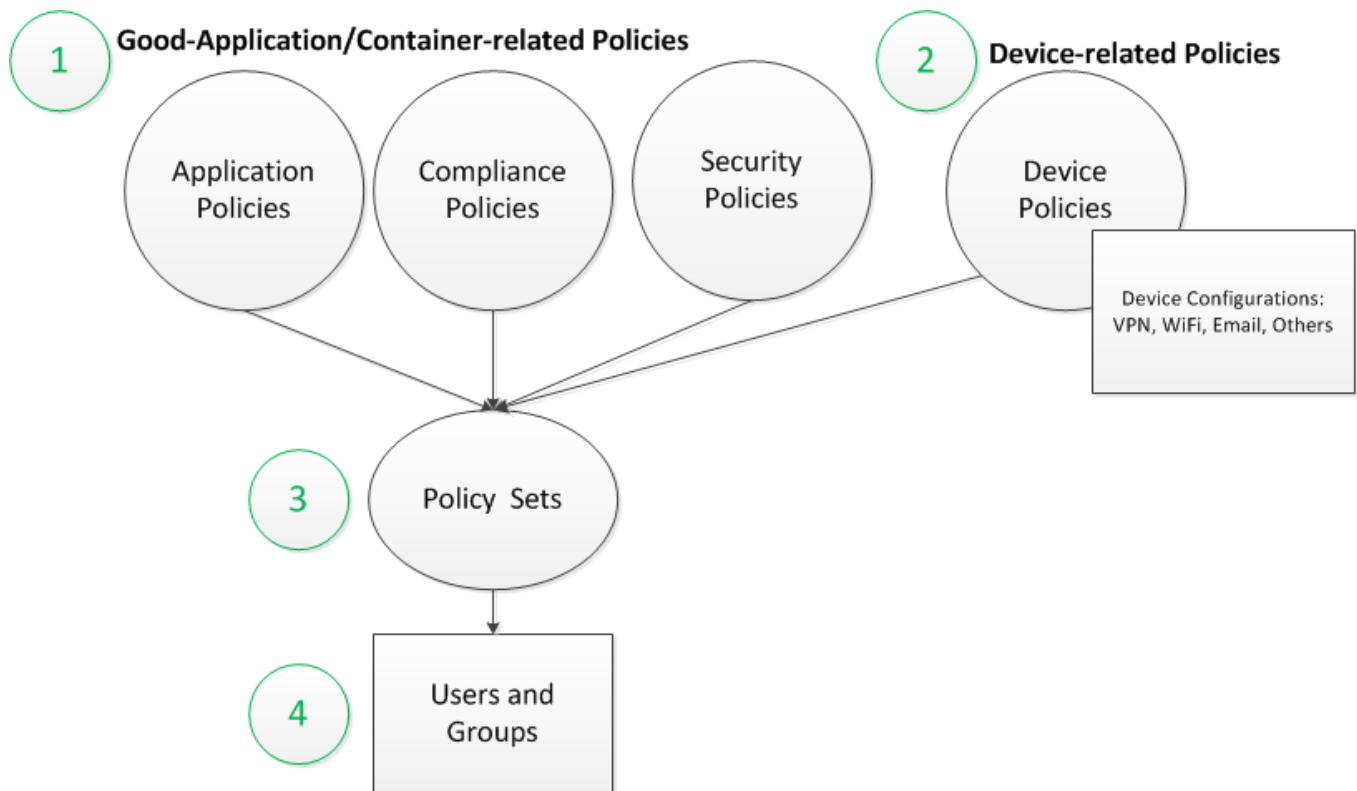
## Installing Google Cloud Messaging API Keys

To enter Google Cloud Messaging API Key details, in the GEMS Console:

1. In the console, **Good Mail Service Configuration > Android Push Notification**.
2. Under **Google Cloud Messaging**, click **Edit**.
3. For the **Sender ID** field, enter the value of name you specified for the name of the Server Key you created in Google, as detailed in [Obtaining Google Cloud Messaging API Keys](#) .
4. For the **Key** field enter the value of your API key from Google.
5. Click **Save** to store the values or **Cancel** to discard them.

## Policies

The diagram below shows the relationships of the various types of policies in Good Dynamics and the general sequence of working with them. At the highest level (the circled green numbers), there are *Good-application-related container policies, device policies, policy sets, users and application groups*.



The application/container policies control the behavior of the containers on the device, while device policies control the features of the device itself. Thus, you have layers of control. For instance, with the container security policies, you might require that an application password be six characters long, while with device policies, you might require that the device password be seven characters long.

Device configurations give you even finer-grained capabilities with device policies. For example, you might want one policy for users who access your systems with VPN and another for users who access your systems with WiFi.

### Security Policies

These policies govern the security of GD application passwords and access keys and define security related application behavior.

- With Password Policies, you control the required format of GD application passwords and how often users must change their passwords.

- You cannot deselect the **Require at least X characters** option or set a minimum length of zero characters, because passwords are required for GD applications.
- The setting **Do not allow more than one password change per day** affects the behavior of the GD SDK APIs by which users can be allowed to change application passwords. The specific APIs involved are `showPreferenceUI` on iOS and `openChangePasswordUI` on Android.
- With Lock Screen Policies, you control when the GD applications on users' devices ask for a password. You can also configure whether to lock or to wipe applications after a number of authentication failures.
- You can choose to prevent data from being copied from GD applications to other applications on the device.
- You can configure the GD application, if any, that serve as the authentication delegate on devices for all users assigned this policy set.
- With Provisioning Policies, you configure the text for provision emails. These emails contain the access keys your users use to activate GD applications on their devices. You can also configure how long the access keys are valid.

### Compliance Policies

Compliance policies include rules that are specific to mobile device platforms. You can set how often the compliance rules are enforced.

For each platform, you can set compliance rules for device connectivity, jailbroken/rooted devices, and allowed device OS versions, hardware models, and GD Library versions. If a user's device is out of compliance with one or more of the rules, the specified failure action is triggered for GD applications on the device. For example, if you have specified the Wipe Container failure action for devices that have not connected in the last 7 days, and a user's device is out of compliance with that rule, GC sends the command to the user's device to wipe data for any installed GD applications the next time it connects.

### Application Policies

You can configure policy rules specific to GD applications configured for each policy set. Applications that have configurable policies are each displayed in a collapsible section under this tab.

### Device Policies and Device Configurations

Device policies represent accessible settings on the managed device. These include but are not limited to device passcode requirements, device restrictions, and mandatory support, such as device encryption.

You can associate device policies with device configurations, which you can think of conceptually as representing groups of users who access your network in common ways.

### Policy Sets and Policy Reconciliation

A policy set defines a common set of rules that are applied to a collection of users. These policies affect every GD application installed by all of the users in the collection, across all of their devices that have been enrolled in mobile device management.

You can also assign a policy set to a GD application. If you do this, the application's policy rules override the rules in all users' policy sets only for the given application.

Periodically, the GC server retrieves policies from the NOC to ensure that the latest are being enforced. This is called *policy reconciliation*.

## Example: Effects of Device Policies on End-User Devices

The precise behavior of a device policy on an end-user's device depends on the type of device and the feature being managed.

In general on iOS, if a device policy disables a feature, that feature is entirely hidden on the device. For example, if a policy disallows use of the camera, the camera application is not visible to the end-user.

On Android, if a feature is disabled or disallowed, the associated application is still visible to the end-user but cannot be used.

## Different Policies by Type of Device Enrollment; Enrollment Key Expiration

You can segregate your policy sets by the type of enrollment in device management: Corporate-owned (enrollment by the administrator) or end-user self-enrollment (or "BYOD").

In the Good Control console, when you are adding a device policy to a policy set, there is a checkbox that allows you to make this distinction:

**Use different policies for employee-enrolled (BYOD) and administrator-enrolled (Corporate-owned) devices.**

**Note:** If you choose *not* to separate your policies by enrollment type, you can also specify different expiration times for the device enrollment keys associated with the device policy. Under each type of enrollment, set the following field:

**Device Enrollment Keys expire after:** from 1 hour to 90 days.

## Implementing Your Device Policies

For the steps to implement a device policy, with device configurations, see the Good Control online help or offline reference, [Good Control Cloud Administrator Help](#).

## Apple DEP Profiles and Devices

Apple Inc.'s Device Enrollment Program (DEP, described at <http://www.apple.com/business/dep/>) is for businesses to manage their devices via Apple's service. Good Control has an interface to Apple DEP so you can manage all your devices through the single Good Control console.

After prerequisite setup with Apple, the general process for working with DEP profiles and policies in Good Control is as follows:

1. You create as many DEP profiles (collections of DEP policies) as necessary for your organization.

**Note:** After you create a DEP profile in GC, it cannot be edited.

2. You apply the DEP profile to the desired devices.
3. You use Good Control to manage the device.

### Prerequisites

- You must be enrolled in Apple's DEP.
- You must have completed all of Apple's required setup, including your virtual MDM servers.
- You have recorded in Good Control your DEP-related keys and information you received from Apple.
- Your devices must be ready for deployment to your end users. In Apple terminology, your devices have been assigned to your virtual MDM server.

## One-time Setup with Apple for DEP Profiles in Good Control

You need to setup your configuration with Apple in Good Control, including your DEP public key and the MDM server token given to you by Apple, Inc.

### Careful: Effect of Changing the GC-Defined Apple MDM Server Token

Be advised that after you have set up your Apple MDM server token in Good Control, if you change the token in GC (to attempt to map a different MDM server), either in the same DEP account or from a different DEP account, the following occurs.

- Devices that are already enrolled in MDM:
  - Will continue to be managed and available in the device view.
  - Admin can take MDM actions – change device policy, password reset, lock & wipe.
  - Any change in DEP Profile will not be applied until the device is factory-reset.
  - Once unenrolled, the device will no longer be accessible.
- Devices that are not already enrolled in MDM:
  - All device serial numbers that were associated with the old MDM Server will be removed and no longer accessible in the device list view in Good Control.

### Steps

**To setup Apple DEP service in Good Control:**

1. Navigate to **Device Management**.
2. Click the **iOS** tab.
3. Under **DEP Account**, click **Edit**.
4. Enter a description of your DEP account.



5. Click **Generate DEP Public key**.
6. Click **Download Key** to save the generated key to your local computer.
7. Login to Apple's DEP Portal and upload this public key to create your virtual MDM server.

Apple's portal will give you an MDM server token to save to your local computer.

8. In Good Control, click **Import MDM Server Token**.
9. Navigate your computer to find the MDM server token you downloaded from Apple.
10. Click **Import** to finish or **Cancel** to stop.
11. Checkmark **Auto-assign to new DEP devices** if you want a certain DEP profile to be assigned automatically to all new devices.
12. From the **DEP Profile** pulldown menu, select the name of the DEP profile you want automatically assigned to new devices.
13. From the **Initial Device Policy** pulldown menu, select the name of the defined device policy you want to apply to all new devices.
14. Click **Save** to save your changes or **Cancel** to discard them.

## Defining DEP Profiles in Good Control

The following settings and device policies can be defined in an Apple DEP profile via Good Control.

With a profile, you define sets of characteristics of device management for Apple devices, essentially relieving the end user of any need to decide. You can indicate which parts of the device initialization can be skipped entirely. These settings are the **Skip Setup Screens** policies.

Group	Policy/Info	Default	Description
Optional Support Information	Department	None	The name of your department
	Support Phone Number	None	Phone number users can call for assistance.
	Support Email	None	Email address users can contact for assistance.
DEP Policies	Supervised Devices	Enabled	<p>A supervised device has been entered into Apple DEP or has been configured using the Apple Configurator.</p> <p><b>Note:</b> Either this setting or <b>MDM Profile Removable</b> (see below) must be enabled.</p>

Group	Policy/Info	Default	Description
	MDM Mandatory	Enabled	Enroll the device in device management.
	MDM Profile Removable	Not enabled	<p>If enabled, the user is allowed to delete the device management profile from the device. Also, see discussion in <a href="#">Effect of Removing MDM Profile, How to Prevent</a> .</p> <p><b>Note:</b> Either this setting or <b>Supervised Devices</b> (see above) must be enabled.</p>
	Allow Pairing	Not enabled	If enabled, the device can pair with the user's associated wearable devices.
Skip Setup Screens	Passcode	Not skipped	If skipped, the user does not need to set a passcode on the device.
	Location Services	Skipped	If not skipped, Location Services are enabled.
	Restoring from backup	Skipped	If not skipped, backup and restore from backup are allowed.
	Apple ID and iCloud	Not skipped	If skipped, user is not prompt for Apple ID for the Apple App Store and iCloud services.
	Terms of Use	Not skipped	If skipped, user is not prompted to accept Apple's Terms of Service.
	Touch ID	Not skipped	If skipped, user is not prompted to activate and train the fingerprint identification system.
	Apple Pay	Skipped	If not skipped, user is prompted to enroll in Apple's payment system.
	Zoom	Skipped	Accessibility option. Not skipping Zoom enables a magnifying glass and other features described for Zoom at <a href="http://www.apple.com/accessibility/ios/">http://www.apple.com/accessibility/ios/</a>
	Send diagnostic info to Apple	Skipped	If not skipped, diagnostic information is sent to Apple.
	Siri	Skipped	If not skipped, user is prompted to enable and train the voice recognition system.
	Android Migration iOS 9	Skipped	If not skipped, enable the moving of files from Android devices to iOS, as described at <a href="https://support.apple.com/en-us/HT201196">https://support.apple.com/en-us/HT201196</a> .

## Important GC Settings Affecting Apple DEP

Be aware that there are some key policy settings and standard device restrictions you can set in GC that affect how Apple DEP operates.

**Important:** Make sure you follow these recommendations for the policy sets and device policies you associate with Apple DEP profiles.

### Good Agent: Allow Self-Authentication in Auth Delegation, Auto-Push Delegates

Multi-authentication delegation is a standard Good Dynamics feature that allows the function of authenticating the user to be "shared" among a group of defined GD applications. For details and steps, see the good Control online help topic "Assigning Authentication Delegates".

**Note:** For the Good Agent application, make sure that you enable the setting **Allow self-authentication when no authentication delegate application is detected**.

Good Agent activation is required for Good MDM to determine a device's user. You should exercise care in setting user policy sets that have authentication delegation enabled. The 'Allow self-authentication when no authentication delegation application is detected' must be set to allow user to complete the activation of Good Agent without the need for additional apps on the DEP device

In addition, make sure that the required authentication delegate applications (defined by the administrator) are configured for auto-push (see [Managed Apps: Enabling App Auto-Push, Exempting Policy Sets](#)) so they are loaded on end-users' devices without the users' intervention and so you can manage the multi-auth delegation and other aspects of the proper versions of these delegate apps.

### Device Access Controls: Allow Inventory of Personal Apps

**Note:** In your device profiles associated with the policy sets that you associate with your Apple DEP profiles, be sure you set the **Allow Inventory of Personal Apps** in the Device Access Control section of [Device Policy Reference: General](#).

This setting is needed to support the following functions of Good Agent:

- To determine the exact user of a device
- To monitor the state of applications pushed to the device of the app pushes themselves

## Steps for Defining DEP Profiles in Good Control

To define Apple DEP profiles in Good Control:

1. Navigate to **Apple DEP Profiles**.
2. Click **New DEP Profile**.
3. If you have already created a profile you want to use as a basis for the new profile, from the **Copy from** pulldown menu, select the name of the base profile.

4. Enter a mnemonic name for this profile.

**Note:** The DEP profile name cannot exceed 100 characters.

5. Complete the settings using the information in the table above.
6. Click **Save** to save your changes or **Cancel** to discard them.

## About Errors from Apple

Good Control attempts to verify the settings you specify in a DEP profile for consistency before submitting them to Apple.

Unfortunately, Apple might reject a profile without giving the exact combination of settings that might have been invalid. Testing by Good Technology has shown that there is often no indication in errors returned from the DEP portal about the precise nature of an error.

## Effect of Removing MDM Profile, How to Prevent

If the DEP profile allows user to remove MDM profile and the user actually does remove it *before activating any application/container*, then subsequent app activation treats the device as a BYO ("Bring Your Own", that is, personal) device.

If such a situation is a security concern, Good Technology recommends the following:

- In the DEP profile, enable supervised mode, disallow MDM removal and disallow skipping MDM enrollment.
- Set the iOS device restriction to disallow managed app removal and disallow access to the Apple App Store. Disallowing the Apple App Store ensures that only MDM can install apps on the device. See [iOS Restrictable Features](#).

You can further ensure that end-user activates Good Agent (so GC can provide visibility about DEP device's actual user) by making Good Agent the first authentication delegate.

## Assigning DEP Profiles to Devices

Before assigning DEP profiles, you must have completed the details in [One-time Setup with Apple for DEP Profiles in Good Control](#) and [Defining DEP Profiles in Good Control](#).

**To assign Apple DEP profiles in Good Control:**

1. Navigate to **Apple DEP Devices**.
2. Select the devices you want to assign a DEP Profile.

You have several ways to select:

- From the **Filter** pulldown menu, select **No DEP Profile Assigned**.
- Manually checkmark individual serial numbers.

3. Click **Assign DEP Profile**.

4. From the **DEP Profile** pulldown menu, select the desired profile.
5. Click **Assign** to assign the selected profile, or **Cancel** to discard your changes.

## Working with DEP-Enrolled Devices

On Good Control's **Apple DEP Devices** page, you can work with your DEP-enrolled devices in several ways.

**Important:** In general, you should perform all actions with DEP-enrolled devices in Good Control itself, not in Apple's portal.

### Filtering and Searching

To filter and search Apple DEP devices, in Good Control:

1. Navigate to **Apple DEP Devices**.
2. Use the **Filter** pulldown menu to narrow the displayed devices:
  - All DEP Devices
  - DEP Profile Assigned
  - MDM Enrolled
  - No DEP Profile Assigned
  - Pending DEP Profile Change
  - Filter based on CSV file

### Filtering by CSV File from Apple

Good Control does not have knowledge of your order numbers from Apple, Inc. You can use "Filter by CSV" to get the device serial numbers by order number. Your CSV file to filter the display of DEP devices requires only a single column: the exact serial numbers you want to see. All other columns are ignored.

1. From Apple DEP's site, download a CSV file of the serial numbers for a given order.
2. Use this CSV to filter in Good Control.

There is no partial string matching. Your column 1 must include the full, exact serial numbers, as it does when you download from Apple.

### Syncing with Apple

Your inventory of devices on file with Apple is synchronized with Good Control once an hour.

To force the synchronization of the device records in Good Control with Apple's inventory of your devices, in Good Control:

1. Navigate to **Apple DEP Devices**.
2. Click **Sync Now**.

## DEP Device Actions

To perform various administrative action on Apple DEP devices, in Good Control:

1. Navigate to **Apple DEP Devices**.
2. Select the desired device records. See [Filtering and Searching](#) .
3. From the **Device Actions** pulldown menu, select the desired action:
  - Wipe
  - Reset Password
  - Deactivate Device
4. Follow the leading prompts to complete the action.

## Export to CSV

To export the selected Apple DEP device records in comma-separated value (CSV) format from Good Control:

1. Navigate to **Apple DEP Devices**.
2. Select the desired device records. See [Filtering and Searching](#) .
3. Click **Export**.
4. Follow the leading prompts to complete the action.

## Device Configurations

In order for device configurations to be sent to enrolled devices, the setting **MDM Enabled** must be ON (which is default). See [Device Policy Reference: General](#) for a list of general policies, including MDM Enabled.

### About Active Directory and "Auto-fill Username"

Good device management reads information from the Active Directory service that was associated with Good Control at installation.

Some of the device configurations have the option to "auto-fill username". The behavior of this field varies by platform.

#### iOS ActiveSync and Autofill Username

In the ActiveSync for iOS device configurations, the **Autofill Username** field is set by default and cannot be unchecked.

#### Android and Autofill Username

On Android, this field is not populated for non-Active Directory users.

This setting can sometimes result in improper user names on iOS devices that should be corrected by end-users so that data from Active Directory can be synchronized correctly.

#### %login%

The end-user should change this value to his own correct Active Directory username.

### VPN Configuration

This section contains settings which configure the Virtual Private Network (VPN), which protects the network connections between devices and their corporate servers.

1. Navigate to **Device Configurations > VPN** tab.
2. On the right, click **Add VPN Configuration** and select **Android** or **iOS**.
3. Complete the platform-specific fields described in the remaining sections, by **Connection Type**:

[For iOS Only: Layer 2 Tunneling Protocol \(L2TP\) Fields](#)

[For iOS Only: Point to Point Tunneling Protocol \(PPTP\) Fields](#)

[For iOS Only: Cisco IPsec](#)

Android is supported only for [Cisco AnyConnect](#) .

4. Click **Save** to keep your changes or **Cancel** to discard them.

The following sections describe the inputs required for each of the VPN connection types.

## For iOS Only: Layer 2 Tunneling Protocol (L2TP) Fields

The following table describes the fields for the VPN connection type L2TP.

Setting	Description
Connection Name	A descriptive name for the connection
Connection Type	Select <b>L2TPConfig</b> .
Server	Enter the fully qualified domain name of your VPN server (e.g. secure.mycompany.com).
Auto-fill Username	Check this field to have the user's name filled automatically from your Active Directory service
User Authentication	Select from: <ul style="list-style-type: none"> <li>• <b>Password</b></li> <li>• <b>RSAToken</b>: The RSA SecurID authentication mechanism assigns a “soft token” to a device which generates an authentication code at fixed intervals.</li> </ul>
Shared Secret	A pre-shared key for authentication that the VPN must receive before requesting username and password credentials. Must not exceed 100 characters in length
Send all traffic	Check this field if you want all network traffic to go over the VPN connection regardless of the user's network services (such as WiFi or other connections in addition to VPN).
Proxy Type	Select from: <ul style="list-style-type: none"> <li>• <b>None</b></li> <li>• <b>Automatic:</b> <ul style="list-style-type: none"> <li>• Protocol and fully qualified domain name of the proxy server</li> <li>• Allow direct connection, if PAC is unreachable</li> </ul> </li> <li>• <b>Manual</b> <ul style="list-style-type: none"> <li>• Proxy Server and Port in <i>servername:port</i> format</li> <li>• Auto-fill Username: Do not use this field reserved for future use.</li> </ul> </li> </ul>

## For iOS Only: Point to Point Tunneling Protocol (PPTP) Fields

The following table describes the fields for the VPN connection type PPTP.

Setting	Description
Connection Name	A descriptive name for the connection
Connection Type	Select <b>PPTPConfig</b> .



Setting	Description
Server	Enter the fully qualified domain name of your VPN server (e.g. secure.mycompany.com).
Auto-fill Username	Check this field to have the user's name filled automatically from your Active Directory service.
PPTP Authentication Type	Select from: <ul style="list-style-type: none"> <li>• <b>Password</b></li> <li>• <b>RSAToken</b>: The RSA SecurID authentication mechanism assigns a “soft token” to a device which generates an authentication code at fixed intervals.</li> </ul>
Encryption Level	Select from: <ul style="list-style-type: none"> <li>• <b>None</b>: Not recommended. Non-encrypted PPTP connections send the PPP frame in plain text and are not secure.</li> <li>• <b>Auto</b></li> <li>• <b>Maximum</b>: 128-bit encryption</li> </ul>
Send all traffic	Check this field if you want all network traffic to go over the VPN connection regardless of the user's network services (such as, WiFi or other connections in addition to VPN).
Proxy Type	Select from: <ul style="list-style-type: none"> <li>• <b>None</b></li> <li>• <b>Automatic</b> <ul style="list-style-type: none"> <li>• Protocol and fully qualified domain name of the proxy server</li> <li>• Allow direct connection, if PAC is unreachable</li> </ul> </li> <li>• <b>Manual</b> <ul style="list-style-type: none"> <li>• Proxy Server and Port in <i>servername:port</i> format</li> <li>• Auto-fill Username: Do not use this field reserved for future use.</li> </ul> </li> </ul>

### For iOS Only: Cisco IPSec

These are the fields for the VPN connection type IPSec (Cisco).

Setting	Description
Connection Name	A descriptive name for the connection
Connection Type	Select <b>IPSec (Cisco)</b> .
Server	Enter the fully qualified domain name of your VPN server (e.g. secure.mycompany.com).

Setting	Description
Auto-fill Username	Check this field to have the user's name filled automatically from your Active Directory service.
Machine Authentication	<p>Select from:</p> <ul style="list-style-type: none"> <li>• <b>Shared secret/Group name</b> <ul style="list-style-type: none"> <li>• <b>Group Name:</b> Enter the user group defined by the Good Administrator for the Device Users. The name must not exceed 64 alphanumeric characters. The following special characters are permitted: . _ ~ ! # \$ % ^ &amp; ( ) { } ' ?</li> <li>• <b>Shared Secret:</b> A pre-shared key for authentication that the VPN must receive before requesting username and password credentials. Must not exceed 100 characters in length</li> <li>• <b>Use Hybrid Authentication:</b> An extension of Internet Key Exchange (IKE) over IP Security (IPSec) tunneling protocol. A digital certificate is deployed on the VPN server at the central site, while remote users use SecurID to access the network. The client authenticates the server certificate, and the server authenticates the client's credentials.</li> <li>• <b>Prompt for Password:</b> The user is challenged for the password.</li> </ul> </li> <li>• <b>Certificate:</b> <ul style="list-style-type: none"> <li>• Click <b>Upload Certificate</b> and navigate your computer to select and upload the certificate.</li> <li>• <b>Password:</b> Enter the password for the certificate.</li> <li>• <b>Include User Pin:</b> [means what?]</li> </ul> </li> </ul>
Send all traffic	Check this field if you want all network traffic to go over the VPN connection regardless of the user's network services (such as WiFi or other connections in addition to VPN).
Proxy Type	<p>Select from:</p> <ul style="list-style-type: none"> <li>• <b>None</b></li> <li>• <b>Automatic:</b> <ul style="list-style-type: none"> <li>• Protocol and fully qualified domain name of the proxy server</li> <li>• Allow direct connection, if PAC is unreachable</li> </ul> </li> <li>• <b>Manual</b> <ul style="list-style-type: none"> <li>• Proxy Server and Port in <i>servername:port</i> format</li> <li>• Auto-fill Username: Do not use this field reserved for future use.</li> </ul> </li> </ul>

## Cisco AnyConnect

Your end-users' devices must have the Cisco AnyConnect application for the appropriate platform:

- Android: Cisco AnyConnect for ICS+ from the Google Play Store.
- iOS: Cisco AnyConnect from the Apple App Store.

### GC Fields for Cisco AnyConnect for Android

For Android, your end-user's devices must have the Cisco AnyConnect for ICS+ application from the Google Play Store..

**Note:** Certificate authentication is optional. Some notes:

- Using certificate authentication with Cisco AnyConnect for ICS+ only has relevance if authentication mode is manual.
- After a certificate is installed on the Android device, removing the VPN profile from the device does not remove the certificate, which must also be removed manually.

The following table describes the configuration settings for Cisco AnyConnect for Android.

Setting	Description
Server	Enter the fully qualified domain name of your VPN server (for example, secure.mycompany.com).
Certificate Authentication Mode	Select from: <ul style="list-style-type: none"><li>• Automatic</li><li>• Disabled</li><li>• Manual</li></ul>
Certificate	Click <b>Upload Certificate</b> , navigate your local computer, select the desired certificate file, and complete the upload. Certificate must be in PKCS12 format.
Certificate Password	Enter the password associated with the uploaded certificate file.

### GC Fields for Cisco AnyConnect for iOS

For iOS, your end-user's devices must have Cisco AnyConnect from the Apple App Store.

The following table describes the configuration settings for Cisco AnyConnect for iOS.

Setting	Description
Connection Name	Enter the defined name of the VPN connection.
Connection Type	Select <b>Cisco AnyConnect</b> .

Setting	Description
Server	Enter the fully qualified domain name of your VPN server (e.g. secure.mycompany.com).
Auto-fill Username	Do not use this field reserved for future use.
Group	Do not use this field reserved for future use.
User Authentication	Select from: <ul style="list-style-type: none"> <li>• <b>Password</b></li> <li>• <b>Certificate</b></li> </ul>
Certificate	Click <b>Upload Certificate</b> and follow leading prompts. <div> <b>Note:</b> If you do not upload a certificate, authentication mode is set to "Automatic".           </div>
Password	For certificate authentication, enter the password associated with the uploaded certificate.
Send all traffic	Check this field if you want all network traffic to go over the VPN connection regardless of the user's network services (such as WiFi or other connections in addition to VPN).
Proxy Type	Select from: <ul style="list-style-type: none"> <li>• <b>None</b></li> <li>• <b>Automatic:</b> <ul style="list-style-type: none"> <li>• Protocol and fully qualified domain name of the proxy server</li> <li>• Allow direct connection, if PAC is unreachable</li> </ul> </li> <li>• <b>Manual</b> <ul style="list-style-type: none"> <li>• Proxy Server and Port in <i>servername:port</i> format</li> <li>• Auto-fill Username: Do not use this field reserved for future use.</li> </ul> </li> </ul>

## Wi-Fi Configuration

This section contains settings which configure access of managed devices to the corporate Wi-Fi network connection.

**Important:** The Service Set Identifier (SSID) for a WiFi connection is a unique value by platform, with one configuration each for iOS or Android. Good device management does not create multiple WiFi configurations for the same SSID.

The SSID can be hidden by selecting or deselecting the **Hidden Network** checkbox. When hidden, the SSID (name) will not be echoed to the display of the managed device and will not be broadcast by the Wi-Fi network. Click the **Hidden Network** check box to prevent the SSID from being broadcast.

Once entered and saved, the SSID will appear inside the parentheses of the displayed name of the configuration set, but it will not appear on the device.

WPA/WPA2 provides stronger encryption than WEP but may not be supported by older routers. For more information, contact your network administrator.

**To create a Wi-Fi configuration that uses the identity certificate, in Good Control:**

1. Navigate to **Device Configurations > WiFi** tab.
2. On the right, from the pulldown menu, select **Android** or **iOS**.
3. Complete the platform-specific fields described below.
4. Click **Save** to keep your changes or **Cancel** to discard them.

The following table describes the configuration settings for WiFi for both Android and iOS.

Setting	Description
Service Set Identifier (SSID)	Enter the SSID for the WiFi network.
Hidden Network	Check this if you want to disable broadcast of this network's information.
Auto Join	Check this if devices are allowed to join the WiFi network automatically.
iOS only: Proxy Setup	<ul style="list-style-type: none"> <li>• <b>Automatic:</b> <ul style="list-style-type: none"> <li>• Protocol and fully qualified domain name of the proxy server</li> <li>• Allow direct connection, if PAC is unreachable</li> </ul> </li> <li>• <b>Manual</b> <ul style="list-style-type: none"> <li>• Proxy Server and Port in two separate fields</li> <li>• Auto-fill Username: Do not use this field reserved for future use.</li> </ul> </li> </ul>
Security Type	Select from: <ul style="list-style-type: none"> <li>• <b>None</b></li> <li>• <b>WEP</b></li> <li>• <b>WPA/WPA2</b></li> <li>• <b>ANY</b></li> <li>• <b>WPA/WPA2 Enterprise</b> <ul style="list-style-type: none"> <li>• <b>EAP</b>, or Extensible Authentication Protocol:               <ul style="list-style-type: none"> <li>• <b>TLS</b>: Transport Layer Security</li> <li>• <b>TTLS</b>: Tunneled Transport Layer Security</li> <li>• <b>PEAP</b>: Protected Extensible Authentication Protocol</li> </ul> </li> </ul> </li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>• <b>Inner Authentication:</b> <ul style="list-style-type: none"> <li>• <b>MSCHAPv2:</b> Microsoft's version 2 of Challenge-Handshake Authentication Protocol</li> <li>• <b>PAP:</b> Password Authentication Protocol</li> <li>• <b>MSCHAP:</b> Microsoft's version of Challenge-Handshake Authentication Protocol</li> <li>• <b>GTC:</b> Generic Token Card</li> </ul> </li> <li>• <b>Auto-fill Username:</b> Check this field to have the user's name filled automatically from your Active Directory service.</li> <li>• <b>Certificate:</b> <ul style="list-style-type: none"> <li>• Click <b>Upload Certificate</b> and navigate your computer to select and upload the certificate.</li> <li>• <b>Password:</b> Enter the password for the certificate.</li> </ul> </li> <li>• <b>Outer Identity:</b> This key is only relevant to TTLS, PEAP, and EAP-FAST. Allows the user to hide his or her identity. It can increase security because an attacker can't see the authenticating user's name in the clear. The user's actual name appears only inside the encrypted tunnel. For example, it could be set to "anonymous" or "anon", or "anon@mycompany.net".</li> </ul>

## Email Configuration

This section contains settings which configure the secure connection to the Exchange server or another non-Exchange server with ActiveSync capability. It permits the administrator to set the frequency of synchronization between devices and the mail server and the amount of historical e-mail data that will be kept in sync with the devices.

In non-Exchange environments, the administrator must ensure that users have Windows authentication credentials and that Active Directory is populated with the correct user e-mail addresses. Good will automatically use the e-mail addresses found in Active Directory to push ActiveSync profiles to the appropriate devices, allowing users to log into the non-Exchange corporate mail server.

### Multiple Exchange Configurations on a Single Device

It is possible for an end-user's device to receive more than one e-mail ActiveSync profile. Conditions are described below:

Description
When multiple e-mail configurations are defined in a single configuration set, members of assigned groups will receive multiple Exchange profiles.
When the Default configuration contains an Exchange configuration and a separate configuration also contains an Exchange configuration, members of groups associated with the second configuration set will receive two Exchange profiles (because every device receives a Default configuration).
When multiple Active Directory groups each have Exchange configurations, users who are members of multiple groups will receive multiple Exchange profiles pushed to their devices.

The following situations can result if a single device is pushed multiple Exchange configuration profiles:

- When two identical Exchange profiles are pushed to the device, the device will reject the second configuration, regardless of the profile name; the device rejects the second profile because it has the same CAS server configuration.
- If a second configuration refers to an alias for the CAS server, iOS does not recognize it as a duplicate, and will accept the second configuration. This will lead to two separate Exchange profiles existing simultaneously on the device, both communicating with the same ActiveSync mailbox configuration. This situation will negatively impact the ability to manage mail delivery.

## Creating an Exchange ActiveSync Configuration

To create an Exchange/ActiveSync configuration, in Good Control:

1. Navigate to **Device Configurations > Email** tab.
2. On the right, click **Add Email**, and select **Android**, **iOS**, or **Windows**.
3. Complete the platform-specific fields described below.
4. Click **Save** to keep your changes or **Cancel** to discard them.

## GC Fields for Email Configuration for Android

The following table describes the configuration settings for Email for Android.

Setting	Description
Account Name	The account name for the Exchange server.
Exchange Host	The fully qualified domain name of the Exchange server
Exchange Password	The password for logging in to the Exchange host
Use SSL	Check this box if you want to use SSL for data communications between your Exchange service and Good Dynamics servers.

Setting	Description
Use TLS	Check this box if you want to use TLS for data communications between your Exchange service and Good Dynamics servers.
Auto-fill Username	Check this field to have the user's name filled automatically from your Active Directory service.
Server Path Prefix	The IMAP path prefix. With the value <b>INBOX</b> in this field, all "peer folders" such as Sent, Drafts, Trash, and Junk are not visible to the end-user, leaving only the Inbox visible.
Always Vibrate for Email Notification	Check this box to make the user's device vibrate on receipt of new mail.
Vibrate for email notification when silent mode	Check this box to make the user's device vibrate on receipt of new mail even in silent mode.
Notification for new email	Allow on-screen notification of new mail
<ul style="list-style-type: none"> <li>• Sync Contacts</li> <li>• Sync Calendar</li> <li>• Sync Tasks</li> <li>• Sync Notes</li> </ul>	Check the appropriate box to synchronize the listed feature.
Peak Period Sync Schedule	Select from: <ul style="list-style-type: none"> <li>• Never</li> <li>• Automatic</li> <li>• 5, 10, 15 or 30 minutes</li> <li>• 1, 4, or 12 hours</li> </ul>
Off-peak Period Sync Schedule	Select from: <ul style="list-style-type: none"> <li>• Never</li> <li>• Automatic</li> <li>• 5, 10, 15 or 30 minutes</li> <li>• 1, 4, or 12 hours</li> </ul>
Retrieval Size	Select from: <ul style="list-style-type: none"> <li>• All</li> <li>• Headers only</li> </ul>



Setting	Description
Roaming Sync Schedule	Select from: <ul style="list-style-type: none"> <li>• <b>Manual</b></li> <li>• <b>Use Sync Setting</b></li> </ul>
Sync Interval	Select from: <ul style="list-style-type: none"> <li>• Never</li> <li>• Automatic</li> <li>• 5, 10, 15 or 30 minutes</li> <li>• 1, 4, or 12 hours</li> </ul>
Past Days of Email to Sync	Select from: <ul style="list-style-type: none"> <li>• 1 or 3 days</li> <li>• 1 or 3 weeks</li> <li>• 1 month</li> </ul>
Allow Incoming Attachment	Click this box if you want to allow attachments on incoming email

## GC Fields for Email Configuration for iOS

The following table describes the configuration settings for email configuration for iOS.

Setting	Description
Account Name	The account name for the Exchange server.
Exchange Host	The fully qualified domain name of the Exchange server
Use SSL	Check this box if you want to use SSL for data communicated between your Exchange service and Good Dynamics servers.
Past Days of Mail to Sync	Select from: <ul style="list-style-type: none"> <li>• <b>No Limit</b></li> <li>• <b>1 day</b></li> <li>• 3 days</li> <li>• 1 week</li> <li>• 2 weeks</li> <li>• 1 month</li> </ul>

Setting	Description
Allow messages to be moved	Allow messages to be moved from user account to user account
Allow Recent address to be synced	Synchronize the user's "Recent Addresses" list
Use only in Mail	Synchronize the mail only for the standard mail client, not third-party mail clients
Credentials Password	For certificate authentication, enter the password associated with the uploaded certificate.
Send all traffic	Check this field if you want all network traffic to go over the VPN connection regardless of the user's network services (such as WiFi or other connections in addition to VPN).
Proxy Type	Select from: <ul style="list-style-type: none"> <li>• <b>None</b></li> <li>• <b>Automatic:</b> <ul style="list-style-type: none"> <li>• Protocol and fully qualified domain name of the proxy server</li> <li>• Allow direct connection, if PAC is unreachable</li> </ul> </li> <li>• <b>Manual</b> <ul style="list-style-type: none"> <li>• Proxy Server and Port in <i>servername:port</i> format</li> <li>• Auto-fill Username: Do not use this field reserved for future use.</li> </ul> </li> </ul>

## GC Fields for Email Device Configuration for Windows

The following table describes the configuration settings for email device configuration for Windows.

Setting	Description
Account Name	The account name for the Exchange server.
Exchange Host	The fully qualified domain name of the Exchange server
Use SSL	Check this box if you want to use SSL for data communicated between your Exchange service and Good Dynamics servers.
Account Domain	The Active Directory domain of the account
<ul style="list-style-type: none"> <li>• Sync Email</li> <li>• Sync Contacts</li> <li>• Sync Calendar</li> <li>• Sync Tasks</li> </ul>	Click the radio buttons desired settings.

Setting	Description
Sync Interval	<p>From the pulldown menu, select one of the following:</p> <ul style="list-style-type: none"> <li>• Never</li> <li>• 15 minutes</li> <li>• 30 minutes</li> <li>• 1 hour</li> </ul>
Past Days of Mail to Sync	<p>Select from:</p> <ul style="list-style-type: none"> <li>• All Days</li> <li>• 3 days</li> <li>• 1 week</li> <li>• 2 weeks</li> <li>• 1 month</li> </ul>

### About Exchange Email Settings on Windows Phone

When Good device management sends the profile for Exchange email to the user's device, the user's email password is set to a generic account's password, not the user.

To correct this problem, on the device, the user must edit **Settings > Email Accounts** to set the correct password.

## Webclip

This section contains details on configuring custom webclips.

**To upload a custom profile for iOS devices:**

1. Navigate to **Device Configurations > Webclip**.
2. Click **Add WebClip**.
3. Complete the necessary fields, as described below.
4. Click **Save** to preserve your changes or **Cancel** to discard them.

### Webclip Fields for iOS

Field	Description
URL	The publicly accessible URL to retrieve the webclip
Label	The desired label to associate with the webclip.
Icon	Click <b>Upload</b> to upload a graphic to associate with this webclip.

Field	Description
ON/OFF	Click the desired radio button for: <ul style="list-style-type: none"><li>• Webclip can be removed</li><li>• Show as full screen</li><li>• Display without visual effect</li></ul>

## Custom iOS Profile

Here are details on uploading a custom device configuration that you have created with Apple Configurator or similar program. For information about how to export profiles from the Apple Configurator, consult the latest Apple documentation.

Some points:

- If there are multiple profiles, some of which are not managed by Good, only the profile directly associated with a given, specific device policy is applied.
- If there are device policies and a custom iOS profile, the device management service sends both to the device. Apple iOS reconciles them and applies the most restrictive settings.
- A new custom profile can be uploaded at any time, which will be applied to all devices that rely on the associated device configuration.

**Important:** Do not encrypt or sign the configuration profile.

Your configuration file name must end with the **.mobileconfig** file extension.

### To upload a custom profile for iOS devices:

1. Make sure you have exported your profile from Apple Configurator.
2. Navigate to **Device Configurations > Other** tab.
3. Click **Upload File**.
4. Navigate your computer to select the exported custom device configuration.
5. Follow the leading prompts to complete the task.



# DM Enrollment

Every device to be managed must be *enrolled* in the service. Enrollment is a series of steps that places the device under managed control.

## Enrolling Devices: Administrator's Tasks

The administrator's tasks for enrolling end-users in mobile device management are detailed here.

### Planning: Corporate-Owned Enrollment or End-User Self-Enrollment?

Decide whether you will enroll your end-users' devices ("Corporate-owned" enrollment) or end-users will self-enroll.

In the Good Control interface, these two types of enrollment are distinguished by two different buttons on the **Users and Groups** screen.

Type of Enrollment	Corporate-Owned	End-User Self-Enroll
Button Text	New Device Enrollment Key	New Access Key
Result	Displays enrollment URL and device enrollment key directly on the GC screen.	By default, sends application activation information in email to end-user. <div><b>Note:</b> Enrollment in device management occurs only if the related policy set contains at least one device policy; otherwise,</div>

Type of Enrollment	Corporate-Owned	End-User Self-Enroll
		only application activation occurs.

### Prerequisites

1. All end-users whose devices are to be enrolled have been added to Good Control.
2. Device and application policies have been defined in Good Control:
  - Be sure you have at least one device policy in your policy sets that matches the OSs or form factors (tablet, phone) of your end-users' devices; otherwise, enrollment in mobile device management does not occur.
  - In your application policies, you have granted users access to the necessary applications:
    - For enrollment on iOS, access to at least one GD-SDK-based application.
    - For device enrollment on Android, access to Good Agent.
    - For Windows devices, no application is needed.
3. Policy sets including device policies and application policies created in Good Control.
4. Policy sets applied to users or application groups in Good Control.
5. Necessary software installed on end-users' devices:
  - On iOS, Good Agent for iOS, which you have given the users access to.
  - On Android, Good Agent for Android, which you have given the users access to.
  - For Windows devices, no application is needed.

### Admin Steps for Corporate-Owned Enrollment

For each end-user device, follow these steps:

1. All prerequisites described above are ready.
2. In Good Control, go to **Users and Groups**.
3. Check the checkbox associated with the end-user whose devices you want to enroll in device management.
4. Click **Edit**.
5. Click the **Keys** tab.
6. Click **New Device Enrollment Key**.

#### iOS

1. With the end-user's device, open Safari.
2. Enter the URL displayed on the screen in Good Control.

3. In the displayed fields, enter the end-user's email address and device enrollment key.
4. Follow the leading prompts to install the profile presented to you and allow the enrollment to complete.

When the DM profile has been successfully installed, enrollment is complete.

### Android

1. With the end-user's Android device, open Good Agent.
2. Do *not* tap **Next**.
3. At the bottom of the displayed screen, tap the label **Corporate-Owned Signup**.
4. In the displayed fields, enter the end-user's email address and the device enrollment key.
5. Tap **Done**.
6. Follow the leading prompts and allow the enrollment to complete.

After enrollment, you are prompted to activate the Good Agent application.

1. In Good Control, click **New Access Key**.
2. In the prompts in Good Agent, enter the user's email address and access key.
3. Follow the leading prompts to complete the activation.

After activation is complete, DM enrollment is also complete.

### Windows Tablet and Windows Pro

**Important:** Before beginning, in the **Action Center** slide the user settings to lower than **Always Notify**. If **Always Notify** is in effect, many of the fields detailed below do not appear on the device.

1. With the end-user's device, Navigate to **Settings > Workplace Settings**.
2. In the **User ID** field, enter the email address of the end-user whose device you are enrolling.
3. Turn off **Automatically detect server address**.
4. In the **Server Address** field, enter the following case-sensitive URL: <https://bxenroll.good.com/>
5. Tap **Turn on**.
6. In the displayed field showing **Device Token**, enter the device enrollment key from Good Control.
7. Tap **Enroll**.
8. Tap **I agree**.
9. Tap **Turn on**.

When the **Turn on** control changes to **Turn off**, enrollment is complete.

## Windows Phone 8.1

1. With the end-user's device, Navigate to **Settings > Workplace**.
2. Tap **Add account**.
3. Enter the email address of the end-user whose device you are enrolling.
4. Tap **Sign in**.
5. Turn off **Automatically detect server address**.
6. In the **Server Address** field, enter the following case-sensitive string. Do *not* enter a leading https:// or a trailing :443: **bxenrol11.good.com**
7. Tap **Sign in**.
8. In the displayed field under the heading **Device Activation**, enter the device enrollment key from Good Control.

**Note:** Click to move through the fields of the key. (The cursor is not automatically advanced.)

9. Tap **Enroll**.

The enrollment process moves through a series of screens and then displays done.

10. Tap **done**.

When you see that the device is under control of GOODMDM, enrollment is complete.

### Viewing DM Details on Windows Phone 8.1

To see the status of device management on a Windows Phone 8.1 device:

1. Navigate to **Settings > Workplace**.
2. Tap **GOODMDM**.

The screen displays the name of the user, the DM server, and the time of the last policy push from Good DM.

The controls at the bottom:



- Tap the control on the left to force retrieval of policies from Good Control.
- The control on the right unenrolls the device from device management, but this ability is controlled by device policy itself, so the control might not be active.

## Unenrolling a Device from MDM

As administrator, you can unenroll previously enrolled end-users' devices from MDM.



1. In Good Control, navigate to **Users and Groups**.
2. Check the checkbox associated with the end-user whose devices you want to unenroll from device management.
3. Click **Edit**.
4. Click the **Devices and Apps** tab.
5. On the far right, click **Deactivate Device**.
6. Follow the leading prompts to complete the unenrollment.

## Admin Setup for BYO DM Enrollment: Entitle End Users to Good Agent

BYO enrollment is done by the end-users themselves using the Good Agent application. For end-users to enroll, in Good Control, you must entitle them to use the applications.

You must entitle them to Good Agent, which has a GD App ID of **com.good.gdmdmagent**, and is the same for both iOS and for Android versions of Good Agent.

The steps for entitling are detailed in [Entitling End-users to Applications or Denying Them](#)

### BYO DM Enrollment on iOS

The steps for end-users of iOS devices for BYO enrollment in device management are published as a separate document suitable for giving directly to end-users. See [DM : Enrollment on iOS with Good Agent](#).

### BYO DM Enrollment on Android

The steps for end-users of Android devices for BYO enrollment in device management are published as a separate document suitable for giving directly to end-users: [DM Enrollment: Good Agent for Android](#).

## No BYO DM Enrollment on Windows Devices, Only Corporate Owned

End-users of Windows tablets and Windows Phone do not directly enroll in device management. The administrator must enroll all devices via corporate-owned enrollment. See [Enrolling Devices: Administrator's Tasks](#).

## End-user Device Unenrollment/Deactivation

Except when Samsung KNOX is relied on, end-users can unenroll their devices from device management. The ability to unenroll/deactivate DM is built into the device operating systems and cannot be prevented.

Below are the general steps to unenroll on iOS and Android without KNOX. Your end-users might discover this ability on their own.

## iOS

1. Go to **Settings > General > Device Management / Profiles**.
2. Remove the device management profile.

## Android without Samsung KNOX

1. Go to **Settings > Security > Device Administrators**.
2. Uncheck the applications that enforce device management, such as Good Agent.

## Android with Samsung KNOX

End-users can follow the same steps as described above for Android without KNOX, but the changes have no effect. DM is still enforced.

To deactivate, the end-user must factory-reset the device.

## DM Operational Tasks: Device Status, Lock, Clear Password, Wipe, and Deactivate

You can manage end users' device from two general locations in Good Control:

- For devices that are not under control of Apple's DEP, go to the individual end user's information as detailed below.
- For devices under control of Apple's DEP, go to the Apple DEP Devices menu, as described in [Working with DEP-Enrolled Devices](#).

You can see the status of end-users' devices, and you can manage the end-user's device with the buttons described here.

### Actions on Non-Apple DEP Devices

The status details are updated from the Good device management service to Good Control every 60 minutes.

1. In Good Control, navigate to **Users and Groups**.
2. Check the checkbox associated with the end-user whose devices you want to manage.
3. Click **Edit**.
4. Click the **Devices and Apps** tab.
5. Scroll to find the desired end-user's device.
6. Choose the operation you want from the **Device Actions** pulldown:
  - Lock Device
  - Clear Device Password: for iOS only.
  - Wipe Device
  - Deactivate Device
  - Installed Apps

Auto-pushed apps that have been deleted from the GD NOC are not displayed here. See [Display of Bundle ID Only: App Removed from GD NOC](#).

7. Follow the leading prompts to complete the chosen task.

## Reports: Devices and App Inventory

See the following:

- [Device Management App Inventory Reports](#)
- [Device Management Inventory Reports](#)

## Device Management App Inventory Reports

**Note:** Your username in the GC must be a member of a role that has permission to view reports. For instance, the Help Desk Administrators predefined role does not have permission to view reports. Follow the steps in [Creating and Configuring a Custom Role](#) to create a role with the Reports and Troubleshooting permission that the Help Desk people need.

### To generate the App Inventory report:

1. Navigate to **App Inventory**.
2. From the pulldown menu, select the time to generate the report.
3. Click **Schedule**.

### To export the app inventory reports:

You can export the following kinds of data to comma-separated value (CSV) format:

- App inventory
- App summary

1. Navigate to **App Inventory**.
2. Click **Export App Inventory List**.
3. Click the report with the data you want.

## Device Management Inventory Reports

**Note:** Your username in the GC must be a member of a role that has permission to view reports. For instance, the Help Desk Administrators predefined role does not have permission to view reports. Follow the steps in [Creating and Configuring a Custom Role](#) to create a role with the Reports and Troubleshooting permission that the Help Desk people need.

### To generate the Device Inventory report:

1. Navigate to **Device Inventory**.
2. From the pulldown menu, select the time to generate the report.
3. Click **Schedule**.

### To export the device inventory reports:

You can export the following kinds of data to comma-separated value (CSV) format:

Export the following kinds of data to CSV file:

- Device inventory list
- Device inventory change audit

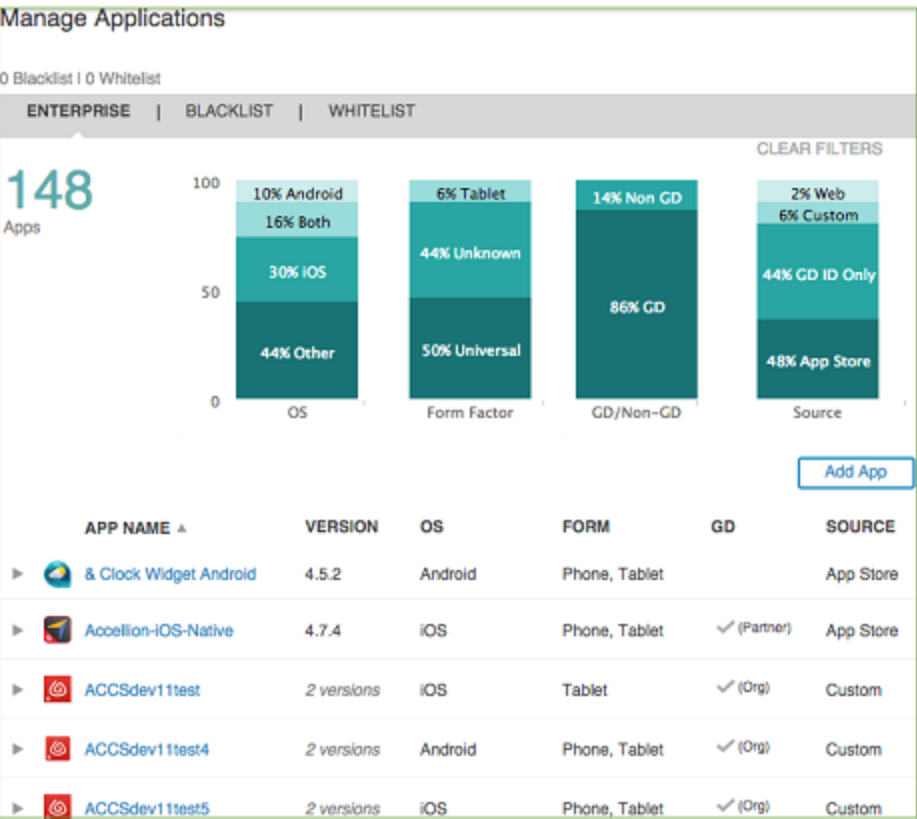
- Device policy and configuration audit
1. Navigate to **Device Inventory**.
  2. Click **Export Device Inventory List**.
  3. Click the report with the data you want.

# Application Management

Built on existing features already in Good Control, Good application administration organizes the distribution of approved applications to end-user devices. High-level benefits include:

- Distribute both Good Dynamics (GD) and non-GD applications via Good Control
- Centralization of management and distribution controls in a single console: Good Control

Most application management functions in Good Control are located in the **Manage Apps** screen's **Enterprise** tab. From this screen, the administrator manages the catalog of applications, classified into four types, discussed in [Types of Applications](#) . The screen below is described in [Filtering the List of Applications, Viewing the Bar Chart](#) .



With the Good Control user interface you can add applications for distribution, edit their metadata, such as name and description, change icons that represent the application, add release notes about your applications, include screenshots of the application, and more. These features are discussed in [Application Management Administrator's Workflow](#) and the remainder of this document.

## Supported and Unsupported Executable File Types for AM

Good application management supports applications of the following kinds:

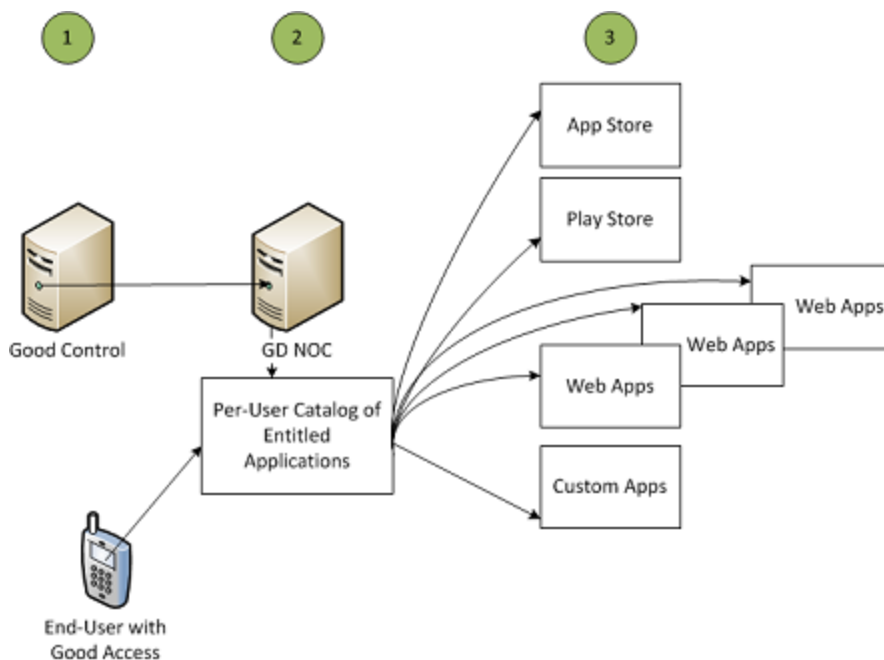
- iOS (.ipa file extension) and Apple iTunes Store
- Android (.apk file extension) and Google Play Store
- Web applications identified by URL

The following platforms are supported by Good Dynamics but not currently supported for distribution via application management:

- Microsoft Windows (.exe or other file extensions)

## How Application Management Works

Shown below is a simplified diagram of how Good application management works.



1. The Good Control administrator defines the applications to be distributed through Good Control. There are four types of applications:
  - Public applications available from application stores
  - Custom applications whose installable files are uploaded to Good Control
  - Web applications on web servers
  - GD-App-ID-only applications for development and test, when executable files are not yet available

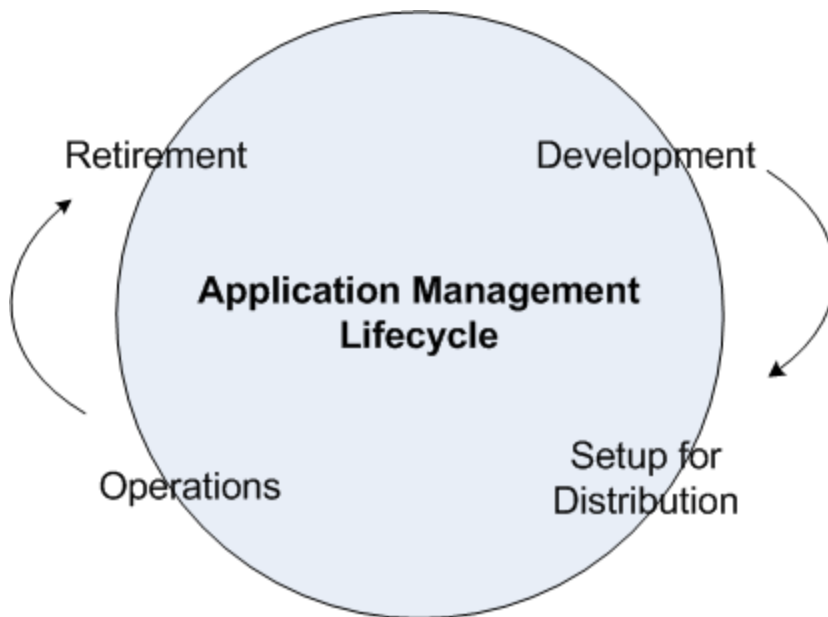
The administrator entitles users or user groups to the various applications.

2. The end-user with Good Access (or other GD-based application) taps an icon to see a catalog of applications to which the end-user is entitled. This catalog is served by the Good Dynamics Network Operations Center (NOC).

3. Depending on the type of application, the end-user is redirected to the appropriate location to install or use the application.
4. Instead of your end users having to download an app, you can define apps to be pushed automatically to devices.

## Application Management Lifecycle

The phases of the AM lifecycle correspond to tasks for the Good Control administrator described in [Application Management Administrator's Workflow](#).



## Key Concepts

Some of the more important concepts underlying application management are described here.

## Types of Applications

Good AM categorizes applications for management under several headings.

Type	Description
Public store application	Public store applications are those that are posted to either Apple App Store or Google Play Store.
Custom application	Application binaries not in the public stores can be uploaded to Good Control.
Web application	Applications that are accessed via a URL on either the public Internet or the private intranet
GD App ID and Version Only	For development and testing, when the actual executable application binaries are not yet available.



## GD Entitlement ID and Version

### About GD Entitlement ID and Version

In the Good Control console and the Good Developer Network, Good-based applications are identified by a *GD Entitlement ID* and *Entitlement Version*. Among other features, these identifiers are used in support of Inter Container Communication (ICC). A primary purpose of the GD Entitlement ID and Entitlement Versions is for you to manage end-user entitlement to your applications; in this context you might hear the GD Entitlement ID referred to as "entitlement ID"; for Good-based applications, the terms are equivalent.

A single GD Entitlement ID must be used to represent the same application across all platforms. Other restrictions also apply.

By default, access to applications varies by type of application:

- All versions of Partner/ISV applications are by default permitted to all to authorized users of any organization to which the application has been published.
- Each version of custom applications by default require the GD administrator's explicit granting of access on the GC console to run.

Good Technology recommends that you devise a naming scheme to meet your needs. Use these guidelines to help you formulate that naming scheme.

Many organization schemes are possible, but in one of the simpler schemes, Good Technology strongly recommends that you do not associate your GD Entitlement ID with a platform. A single GD Entitlement ID should be used for all versions of an application on all platforms. Furthermore, for simplicity's sake, the version number associated with GD Entitlement IDs should also be kept independent of your versioning scheme for your application on different platforms.

Other variations on naming schemes for GD Entitlement ID and Entitlement Versions are also possible, but keep these details in mind when you devise your own GD Entitlement ID naming scheme.

### GD Entitlement and Entitlement Version Both Required for All GD-based Apps

You need to define both the GD Entitlement ID and the Entitlement Version for all your GD-based applications, regardless of whether or not you use the GD Shared Services Framework. Many standard GD features, such as Easy Activation and multi-authentication delegation, rely on your app having both. Furthermore, developers and administrators should ensure that the value specified for the `GDApplicationVersion` key in an app's application configuration files is the same as the value the administrator specifies in Good Control.

The Entitlement Version is independent of any native version identifier; see more information in [Distinction from and Use with Native Language Identifiers](#).

### When to Change the GD Entitlement Version?

The GD Entitlement Version is distinct from any highly visible, published version number you might use for your application. For example, your GD Entitlement Version might be "1.0.0.0" while at the same time you publicly show a visible version number "2.1".

Because each new GD Entitlement Version of your GD-based application requires “publishing” it to your existing customers, it is recommended to change the GD Entitlement ID version number as infrequently as possible.

There are three primary reasons to change the GD Entitlement ID version number:

1. To provide early access or limited access to a new version for specific customers For Partners/ISVs, after the new version has been published to all customers, revert back to the original version number.
2. For Partners/ISVs, to monetize new functionality differently from your existing version.
3. To represent large level differences in functionality. For example, you might update a Service definition, that is, publish a service update that is not supported on an older Entitlement Version.

When a new version is to be made available per above (rarely), ensure that the version is published on the GDN by a partner or on the GC console for custom applications well before an application reporting that GD version is ever available in the App Store/Play or elsewhere. If the new version of the application is downloaded to a device before the version is published on GDN or in GC, the application is blocked. You should never unpublish a version unless it is to enforce payment, force end-of-life, or remove a version with a fatal security issue. If a GD Entitlement ID or Entitlement Version is ever unpublished or an end-user unentitled from an a previously entitled application, the container is wiped from end-user devices.

#### Format of GD Entitlement ID and Version Values

The general form of a GD Entitlement ID is:

***your\_company\_name.your\_application***

The value of your GD Entitlement IDs must follow these rules:

- Must be in reverse domain name form, like *com.yourcompany.something*.
- Must not begin with any of the following:
  - **com.good**
- No uppercase letters.
- In addition, the string must conform to the **<subdomain>** format defined in section 2.3.1 of [RFC 1035](#), as amended by Section 2.1 of [RFC 1123](#).

**Note:** In the GD SDK for Microsoft Windows 8.1, the value of GD Entitlement ID (Application ID) cannot be longer than 35 characters. This does not apply to the GD SDK for UWP.

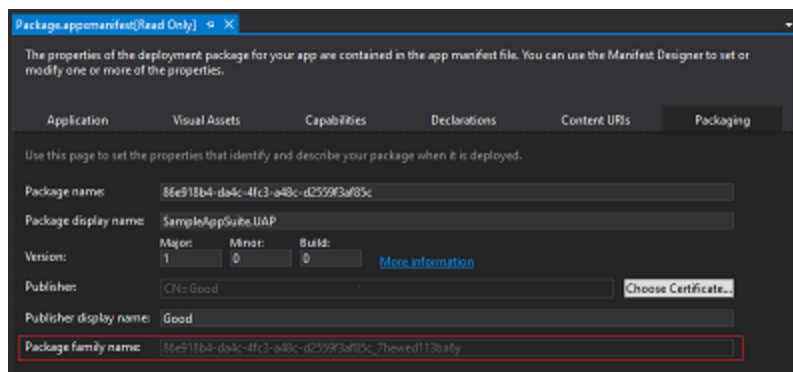
The value of your Entitlement Versions must follow these rules:

- From one to four segments of digits, separated by periods, like **100** or **1.2.3.4**.
- No leading zeroes in the numeric segments. For example, these are *not* allowed: **0100** or **01.02.03.04**.
- The length of the numeric segments can be from one to three characters. This is an allowable example: **100.200.300.400**.

## Distinction from and Use with Native Language Identifiers

The GD Entitlement ID and Entitlement Version are Good-specific metadata and are independent of the identifiers needed by the application platforms themselves. The key point is that the Good values and the native language identifiers' values *can* be the same but they do not necessarily *have* to be. Listed below by platform are the equivalent native identifiers, which are where the values of GD Entitlement ID and version are stored.

Platform	Location	Platform-specific Names
Android	<b>settings.json</b>	<ul style="list-style-type: none"> <li><b>packageName</b></li> <li><b>packageVersion</b></li> </ul>
iOS	<b>Info.plist</b>	<ul style="list-style-type: none"> <li><b>CFBundleIdentifier</b></li> <li><b>CFBundleVersion</b></li> </ul>
MacOS	<b>Info.plist</b>	<ul style="list-style-type: none"> <li><b>CFBundleIdentifier</b></li> <li><b>CFBundleVersion</b></li> </ul>
Universal Windows Platform (UWP)	<b>Package.appxmanifest</b>	For Windows 10/UWP, the GD SDK relies on Package Family Name, which is not explicitly set but is generated by Visual Studio and is displayed in the GUI editor of the package manifest, as shown below.



## Mapping GD Entitlement ID to Native Identifiers

To take advantage of many Good Dynamics features, such as Easy Activation, multi-authentication delegation, and the GD shared services framework, developers need to set up a map in Good Control between your defined GD Entitlement ID and the native identifiers on the platforms for which your application is distributed. The native platforms have no knowledge of the GD Entitlement ID; thus the mapping is needed for the operating systems to take over the actual function of the app.

**To map the GD Entitlement ID to native identifiers, in Good Control:**

1. Navigate to **Managed Apps > Enterprise** tab.
2. Find the affected GD-based application.
3. Click the name of the application to edit it.
4. Go to the **Good Dynamics** tab,
5. For the **GD Entitlement ID** heading, click **Edit**.
6. For all affected platforms, enter the associated native identifier.
7. Click **Save** to save your changes, or **Cancel** to discard them.

#### Native Version Identifiers: \* Wildcard Allowed for Blocking App

The GD SDK supports use of native version identifiers in keeping with the conventions described by the major vendors. These same conventions apply to the use of the \* wildcard in Good Control to deny apps by native version.

Platform	Definition	Reference
Android <b>packageVersion</b>	A string of the format <i>major.minor.point</i> with no explicit requirement to use integers, although this is implied and followed by convention.	<a href="https://developer.android.com/studio/publish/versioning">Link to android.com</a>
iOS <b>CFbundleVersion</b>	A series of integers separated by ".". No explicit limit on number of words.	<a href="https://developer.apple.com/documentation/general/about-property-lists">Link to apple.com</a>
Mac OS X <b>CFbundleVersion</b>	A series of integers separated by ".". No explicit limit on number of words.	<a href="https://developer.apple.com/documentation/general/about-property-lists">Link to apple.com</a>
UWP <b>/Package/Identity/@Version</b>	A string in quad notation, " <i>Major.Minor.Build.Revision</i> "	<a href="https://docs.microsoft.com/en-us/windows/uwp/package-versioning">Link to microsoft.com</a>

The \* character can be used in native version identifiers, but must always be preceded by a period (.) and must be the last character in the native version string. Examples:

- Allowed: 2.3.\*
- Not allowed: 2.\*.3
- 2.\* includes 2.\*.\*

#### About Unique Native Identifiers for Enterprise Apps

If you are developing a private app for use in your enterprise, make sure that the value you choose for the app's native identifiers (Bundle ID and others constructs used on other platforms) is unique, especially with respect to apps that are available through the public app stores.

Duplicate native identifiers can prevent the proper installation or upgrade of your own app.

For all your native identifiers, devise a naming scheme that you can be relatively certain is unique.

## Enforcement of GD Entitlement ID and Version in Good Control

The following are the basic rules that application developers must comply with. In this discussion, the terms "BundleIdentifier" and "BundleVersion" are used to cover all similar platform-specific identifiers, such as package name or Application ID.

1. Application name is unique within the organization.
2. Bundle Version, Bundle Identifier combination is unique for a platform.
3. Bundle Version, Bundle Identifier combination is unique for an operating system.
4. Change in GD Version enforces change in Bundle Version. The other way round is not true.
5. An application (family of binaries) is either GD (all binaries under it are GD) or non-GD (all binaries under it are non-GD). This rule derives from that entitlement ID is locked at the time of creation. The entitlement ID is the GD Entitlement ID if the application is a Good-enabled app.
6. GD Entitlement ID is unique throughout the system.
7. Bundle Identifier for a platform is unique for a GD Entitlement ID and vice versa. Therefore, a change in GD Entitlement ID requires a change in Bundle Identifier, and vice versa.
8. Non-GD and GD versions of same binary have different Bundle Identifiers.

### Common Errors

The following are errors in usage of the GD Entitlement ID and Entitlement Version that are checked by Good Control when GD-based applications are added.

Use Case	Explanation of Error
Administrator submits an app with an existing GD Entitlement ID for an app with some other org.	The GD Entitlement ID must be unique across organizations.
Administrator submits an app with an existing GD Entitlement ID, Bundle Identifier, Bundle Version but different GD Entitlement Version.	The Bundle Version must be changed when there is a change in GD version.
Administrator submits an app with an existing Bundle Identifier and Bundle Version but different GD Entitlement ID.	The Bundle Identifier should be different for different GD Entitlement ID.
Administrator submits an app with an existing GD Entitlement ID, but different Bundle Identifier for an existing platform.	The Bundle Identifier for the same platform should be unique within a GD App.
Administrator submits a GD-enabled app with same Bundle Identifier as an existing non-GD app	Upgrading a non-GD app to a GD app binary requires a change in Bundle Identifier.
Administrator submits a non-GD enabled app with same Bundle Identifier as an existing GD app	Downgrading a non-GD app to a GD app requires a change in Bundle Identifier

## Application Catalog

This document uses the term *application catalog* to refer to the display of per-user entitled applications from which end-users can access approved, managed applications via a Good-based application, such as Good Access. The applications displayed by the catalog are defined by the Good Control administrator, but the application catalog itself is served by the GD NOC:

- The application catalog always serves the latest version of an application to be uploaded or defined.
- The application catalog is sometimes referred to as the "app store", which is not to be confused with the public app stores from Apple or Google.
- End-users must be entitled to the application catalog; see [Essential One-Time Setup Tasks](#) .
- In Good Access, the application catalog is accessed via the **Applications** shopping bag icon, as described in [Viewing the Good Application Catalog in Good Access](#).

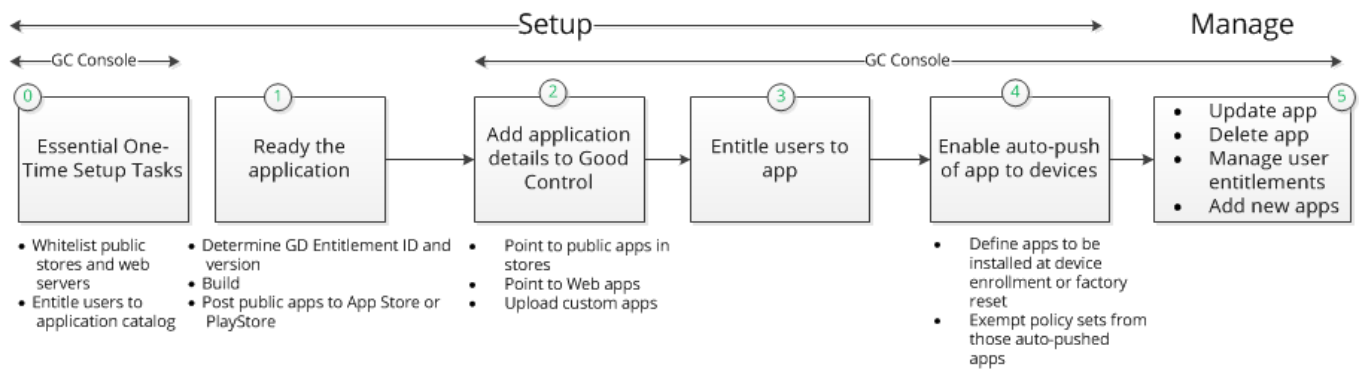
## Form Factor or "Platform"

What type of hardware does the application run on? This is called the *form factor* or "platform" of the application. AM distinguishes the following types:

- For iOS:
  - Phone
  - Tablet
- Android, for all types of devices

## Application Management Administrator's Workflow

Shown below is the high-level workflow for the administrator. This is the process for a new app and for an app update.



Considerations about updating an app are discussed in [Updating an Application](#).

## Good Control Administrators: Changes in Workflow

Entitling end-users to applications is a key function that conceptually remains as it has been in past releases of Good Control. However, administrators already familiar with Good Control need to know that the workflow and clickpaths have changed somewhat. For an overview, with mapping of administrative functions to the Good Control steps, see [Application Management Administrator's Workflow](#). In addition, you can now edit many details about your applications, which is described in .

## App Management-related Screens and Tabs in Good Control

Here is a correlation among the [Application Management Administrator's Workflow](#) and the screens and tabs in Good Control.

Task	Good Control Screen or Tab	See Also
0. <a href="#">Essential One-Time Setup Tasks</a>	<ul style="list-style-type: none"> <li>Whitelist public stores and web servers: <b>Servers &gt; Server Properties &gt; proxy.urls</b> property</li> <li>Entitle users to application catalog: <b>App Groups &gt; Everyone &gt; Entitled Apps &gt; Add More</b></li> </ul>	
1. Ready the application	Application development is not affected by application management, except for the enforcement of proper use of GD App ID and application version.	<a href="#">GD Entitlement ID and Version</a>
2. Add application details to Good Control	<ul style="list-style-type: none"> <li><b>Manage Apps &gt; Enterprise</b> tab</li> <li><b>Manage Apps &gt; Blacklist or Whitelist</b> tab</li> </ul>	<ul style="list-style-type: none"> <li><a href="#">Adding Applications</a></li> <li><a href="#">Blacklisting or</a></li> </ul>

Task	Good Control Screen or Tab	See Also
Large-grained Application Blacklist or Whitelist		<a href="#">Whitelisting Applications on Devices</a>
3. Entitle end-users to the app	This can be done in several places: <ul style="list-style-type: none"> <li>For individual users: <b>Manage Users</b> &gt; <i>edit a user</i> &gt; <b>Apps</b> tab &gt; <b>Entitled Enterprise Apps</b> or <b>Denied Enterprise Apps</b> or <b>Entitlement Groups</b></li> <li>For user groups: <b>App Groups</b> &gt; <i>edit a group</i> &gt; <b>Entitled Enterprise Apps</b> or <b>Denied Enterprise Apps</b></li> </ul>	Good Control online help
4. Enable auto-push of app to devices	<b>Manage Apps</b> > <b>Enterprise</b> tab > <i>edit an app</i> > <b>General</b> tab > <b>Auto-Push Settings</b> > <b>Auto-Push Enabled</b>	<a href="#">Managed Apps: Enabling App Auto-Push, Exempting Policy Sets</a>
5. Ongoing maintenance	<b>Manage Apps</b> > select app > <b>Edit</b> > edit details on desired tab	<ul style="list-style-type: none"> <li><a href="#">Filtering the List of Applications, Viewing the Bar Chart</a></li> <li><a href="#">Entitling End-users to Applications or Denying Them</a></li> <li><a href="#">Editing Application Details</a></li> <li><a href="#">Updating Apps</a></li> <li><a href="#">Admin Actions for Auto-Pushed Apps</a></li> </ul>

## Essential One-Time Setup Tasks

Here are administrator's tasks in preparation for implementing AM. In general, you need to do these tasks only once.

### Whitelisting App Stores and Web Servers in Good Control

To allow your end-users' device to access applications on the Google Play Store, Apple App Store, or web servers, you need to "whitelist" the hostnames and ports for these resources in Good Control.

To whitelist these stores, in Good Control, add the hostname and port values to the **proxy.urls** property in **Servers** > **Server Properties** tab. For more details, see the Good Control online help.



Required?	Resource	Hostname and Port	Notes
Required	Apple App Store	store.apple.com:80	For retrieving applications' associated images
Required	Google Play Store	play.google.com:443	For retrieving applications' associated images
Required if you are serving Web applications	Web Applications	Exact hostnames and ports depend on the web servers host your applications, either on the public Internet or on your private intranet	When you add new web applications, check that their details have been whitelisted.
Optional depending on networking configuration	Good's App Store	appstore.good.com:443 good.com:80	Needed if you have enabled the GD Route All feature, which directs all network traffic through the Good Proxy. For more info, see the Good Control help topic <a href="#">Routing All Traffic Through Good Proxy: "Route All"</a> .

## Entitling Users to the Application Catalog

For your end-users to see the AM application catalog, they need to be entitled to it. This entitlement is done via a "placeholder application" name in Good Control's application policies and application groups:

- Application Name: **Feature – AppStore**
- GD App ID: **com.good.feature.appstore**

**Note:** Unless you want to allow access to the AM catalog to only a subset of your end-users, Good Technology recommends that you entitle all end-users via **App Groups > Everyone**, to which all end-users are automatically added. Otherwise, entitle only the groups you want.

**To entitle end-users to the application management "virtual application" in Good Control:**

1. Navigate to **App Groups**.
2. Checkmark the group you want to entitle, such as **Everyone**.
3. Click the pencil icon on the far right of the group name to edit it.
4. Under **Allowed Applications**, click **Add More**.
5. From the displayed list of applications, find and select the "placeholder application" named:

**Feature – AppStore**

6. Click **OK** to save your changes or the large **X** in the upper right to discard them.

## Advice on Application Development

Application management does not change how Good-based or other applications are developed, except that Good-based applications must conform to the proper use of the GD App ID and application version discussed in [GD Entitlement ID and Version](#).

### About Unique Native Identifiers for Enterprise Apps

If you are developing a private app for use in your enterprise, make sure that the value you choose for the app's native identifiers (Bundle ID and others constructs used on other platforms) is unique, especially with respect to apps that are available through the public app stores.

Duplicate native identifiers can prevent the proper installation or upgrade of your own app.

For all your native identifiers, devise a naming scheme that you can be relatively certain is unique.

### APIs for Application Management

Except as noted below, the GD SDK includes one public API method and one supporting class to get the supported versions for a named entitlement ID (GD App ID). For details and examples, see the API reference.

#### GD SDK for iOS in GDiOS.h

- `-(void)getEntitlementVersionsFor:(NSString*)identifier`
- `callbackBlock:(void (^)(NSArray* entitlementVersions, NSError* error))block;`
- `GDVersion` class

#### GD SDK for Android in GDAndroid.java

- `public int getEntitlementVersions(String identifier, GDEntitlementVersionsRequestCallback callback)`
- `GDEntitlementVersionsRequestCallback` interface
- `GDVersion` class

#### GD SDK for Microsoft Windows

The GD SDK for Microsoft Windows does not have any APIs related to mobile application management.

## Adding Applications

These are the steps for adding an application to application management.

### Adding a Public Store Application

You need the following:

- For Good-Dynamics-based applications, the GD App ID and application version for the application must have been compiled into the application binary.
- The URL to the application's "landing page" or "preview page" in either Apple App Store or Google Play Store

**Important:** If the public app store is down or its interfaces are not available or not responsive, Good Control cannot retrieve details from it.

**In Good Control:**

1. Navigate to **Manage Apps**.
2. Click the **Enterprise** tab.
3. Click **Add App**.
4. From the dialog, click the radio button for **Public App Store**.
5. Click **Next**.
6. Enter the URL to the public app store for this public app.

**Important:** The URL for a public store app must be unique by platform. You cannot reuse the same URL.

7. Click **Cancel** to discard or **Next** to continue.

GC displays information about the application: its version, operating system, form factor, size, and (for Good-based applications) GD App ID and application version.

8. Click **Back** to select a different URL, **Add App** to finish, or **Cancel** to discard.

### About Adding GFE

Good for Everyone (GFE) is a popular Good application that was created before Good Dynamics. As such, GFE does not have a GD App ID or application version number, as do Good Dynamics applications.

Because of this, for distribution via Good Control, GFE must be added as a public store app.

### Adding Multiple Platforms for Public Store Apps

Imagine you have an application available for two or more different "platforms" (hardware types, or form factors), such as the same application for the iPhone and the iPad or the iPhone and Android devices. You want to give your users access to the applications of both platforms or form factors.

#### Prerequisites:

- Make sure you have added at least one of the platforms or form factors to Good application management.
- You need the URL to the public app store for each of the desired platform-specific versions of the application.

#### In Good Control:

1. Navigate to **Manage Apps**.
2. In the list, find the desired application you want to add form factors for and click its line in the list.
3. In the upper right, click **Add URL**.
4. In the displayed dialog box, enter the appropriate URL to the public app store.
5. For GD-based apps, choose either one of the already existing GD application versions or click the radio button for **New GD App Version** and enter the new version number.
6. Click **Next** to continue or **Cancel** to discard your changes.

## Adding a Custom Application

You need the following:

- The GD App ID and application version for the application, if it is Good-based
- The application's compiled binary file, either Android package (.apk) or Apple bundle (.ipa).

#### In Good Control:

1. Navigate to **Manage Apps**.
2. Click the **Enterprise** tab.
3. Click **Add App**.
4. From the dialog, click the radio button for **Custom**.
5. Click **Next**.
6. Click **Choose File**.
7. Navigate your computer to select the desired binary: Android package (.apk), Apple bundle (.ipa), or Microsoft Windows (.appxupload) file.
8. Click **Add App** to upload or **Cancel** to discard.

GC displays information about the uploaded binary: its version, operating system, form, size, GD App ID and application version.

9. Click **Back** to select a different file, **Cancel** to discard, or **Add App** to finish.

## Adding a Web Application

You need the following:

- The URL to the application's "landing page" or "preview page" on a web server

In Good Control:

1. Navigate to **Manage Apps**.
2. Click the **Enterprise** tab.
3. Click **Add App**.
4. From the dialog, click the radio button for **Web**.
5. Click **Next**.
6. Enter the URL to the application, with the protocol either **http://** or **https://** (default).
7. Click **Cancel** to discard or **Next** to continue.
8. Verify the displayed details:
  - Edit the displayed text, if desired.
  - To upload your own icon in place of the displayed one, under the icon click **UPLOAD** and follow the leading prompts.
9. Click **Back** to specify a different URL, **Cancel** to start over, or **Add App** to finish.

## Adding GD App ID and Version Only

You need the following:

- The GD App ID and application version for the application

In Good Control:

1. Navigate to **Manage Apps**.
2. Click the **Enterprise** tab.
3. Click **Add App**.
4. From the dialog, click the radio button for **GD Entitlement and Version Only**.
5. Click **Next**.
6. Enter the values for the following fields.
  - Display name
  - GD App ID. For details on acceptable values, see [Key Concepts](#) .
  - GD Entitlement Version. For details on acceptable values, see [Key Concepts](#) .
  - Custom Description displayed in the GC console.
7. Click **Add App** to finish or **Cancel** to discard.

## Specifying App Servers

If you have a GD-based application (one with a GD App ID and version) that is served from an application server or web server, you can specify the name of that application server and the priority of the Good Proxy clusters

used for communication with it.

**To specify an application server and its GP cluster priority for a GD-based application, in Good Control:**

1. Navigate to **Manage Apps** > *edit an application* > **Good Dynamics** tab.
2. For **Host Name**, specify the fully qualified domain name of the application server where this application is.
3. Specify any required port number.
4. For **Priority**, select one of **Primary**, **Secondary**, or **Tertiary**.
5. For **Primary GP Cluster**, from the pulldown menu, select the name of the desired cluster.
6. For **Secondary GP Cluster**, from the pulldown menu, select the name of the desired cluster.
7. To add another row, under **Action**, click the plus sign (+), and repeat the steps above as many times as needed.
8. For the Configuration field, see the discussion below.
9. Click **Save** to retain your changes or **Cancel** to discard them.

### Configuration Field

In the **Configuration** field you can add text in the format required by the application developer (typically JSON/XML). This configuration is sent to all the clients for any user; that is, it is a global setting.

The **Configuration** field is an older mechanism for passing initialization or other information that should be passed to the application when it starts. The preferred mechanism is application-specific policies, described in [Configuring Application Specific Policy Rules](#). Application-specific policies allows for configuration to be user-group-, the administrator does not have to worry about formatting in JSON/XML.

## Adding New GD Entitlement Versions (GD App Versions)

Imagine you have an update available for a GD-based application that has already been deployed, and you want to require an upgrade to this new version, because of new features and bug fixes.

You can accomplish this by adding a new GD entitlement version (formerly known as GD app version).

**Note:** Be sure you understand the effects of adding a new entitlement version. See the details and guidance in [GD Entitlement ID and Version](#), in particular the advice on when and when not to change the entitlement version.

### Prerequisites:

- Make sure you have added at least one version of the GD-based app to Good application management.

### In Good Control:

1. Navigate to **Manage Apps**.
2. In the list, find the desired application you want to update and click its line in the list.
3. **Good Dynamics** tab

4. For the **Version** heading, click **Edit**.
5. In the text box next to **Add Version**, enter the new entitlement version, making sure to follow the specified in [GD Entitlement ID and Version](#).
6. Click **Add Version**.
7. Following the remaining prompts.
8. Click **Update** to save your change or **Cancel** to discard them.

## Entitling End-users to Applications or Denying Them

Your end-users must be entitled to view or run the applications defined in the application catalog. You can also deny them the right to applications. You can entitle or deny end-users in several ways:

- With app groups
- Per individual end-user

### Sequence of App Version Entitling and Denying: Entitle, Then Deny

**Important:** If you are entitling a new app version and denying an older version, be sure to entitle the new version first before you deny access to the older version. If you deny the older versions first, the app will be wiped from the device.

## Blocking Android or iOS GD Apps by Native Version

In Good Control's **Manage Apps** screen, you can selectively block access to specific versions of your GD-based application on Android or iOS. The blocking of the app on the device is sent from Good Control in the form of a compliance policy. To uniquely identify an app, the GC admin denies via the app's GD Entitlement ID (also known as "GD App ID") and a native version identifier, which can include a wildcard. For definitions, see [Distinction from and Use with Native Language Identifiers](#).

**Note:** Only Android or iOS apps can be blocked by native version. Windows is not supported.

The blocking only affects the GD Runtime of the app on the device, blocking it so it cannot run. It does not prevent the end user from downloading and installing the latest binaries of the app that are allowed on the device. An end user who attempts to install a blocked version of an app sees the following message:

**The version of <appname> is blocked. An updated version is available.**

Unless you want to completely block access to the app regardless of its version, be sure your end users are entitled to a later version of the app *before* you deny access to an older version they might also have on their devices. If you deny the older first before entitling, the app is wiped from the device.

## Wildcarding Native Versions

You can use the \* wildcard character with the native version identifier to deny a certain range of versions. Follow the vendor recommendations in [Distinction from and Use with Native Language Identifiers](#).

The \* wildcard character:

- Must come last in the native version string. **Invalid usage:** 1.\*.8
- The closer the \* is to the left, the more versions it masks. **Example:** 2.\* denies 2.1, 2.2, and 2.3.

## Steps

### Prerequisites

- You need to know the exact GD Entitlement ID (GD App ID) of the Android or iOS app whose native version you want to block
- You need to know the native versions of the app you want to block.

To deny specific versions of an application, in Good Control:

1. Navigate to **Manage Apps > Enterprise tab > *edit the appropriate app* > platform-specific** tab.
2. For the heading **Blocked Versions**, click **Edit**.
3. Enter the native versions to deny, separated by commas, be sure that any \* wildcard you use comes last in the version identifier.
4. Click **Save** to retain your change or **Cancel** to discard them.

## Managed Apps: Enabling App Auto-Push, Exempting Policy Sets

With Good Control's auto-push feature, you can enforce changes to apps on your end-users' devices, such as automatically pushing the latest version of an app or removing disapproved versions of apps:

- The app auto-push feature is available for all app types except web apps. Note that for other types of apps, the auto-push option is displayed in Good Control only if the app has an associated binary executable file uploaded either to the GC (a custom app) or to one of the public app stores ( a public app store app).
- About auto-push of purchasable applications: GC does not prevent you from auto-pushing an app that must be purchased (from an app store or otherwise). The status in the GC of a purchasable app that has been pushed to a device is: **Payment Required**.
- GC permissions that include the auto-push feature: Applications, Shared Services, and Application Wrapping permissions.
- Except for specific policy sets that you exempt, the auto-push of an app is applied to all policy sets that include devices policies for the desired platform.
- Supported device operating systems:
  - With Good Agent for iOS: iOS 8.0 or later.
  - Android (minimum API Level 14) with Samsung KNOX(minimum KNOX 2.1)

### Prerequisites



For auto-push, the end-user must have been associated with a policy set in Good Control that includes at least one device policy for the desired platform, and the end-user's device must be enrolled in Good device management. If the device is not enrolled, apps cannot be pushed to it:

- To use app auto-push, Good device management must be in effect in Good Control. See [Device Management Administrator's Workflow](#).
- The policy sets that enforce the auto-push must have an associated device policy that includes the platforms to which you want to auto-push the app.
- You must have already done the basic set-up of a public store or custom app in Good Control, as shown in [Application Management Administrator's Workflow](#).
- To configure auto-push, a user of Good Control must have the **Applications, Shared Services, and Application Wrapping** permission.
- If you want to exempt certain policy sets from auto-pushing the app, determine the names of those policy sets.

To enable auto-push of an app to end-users' devices, in Good Control:

1. Navigate to **Manage Apps > Enterprise tab > *edit an app* > General tab > Auto-Push Settings**.
2. Click **Edit**.
3. Check the **Auto-Push Enabled** checkbox.
4. If you want to exempt policy sets from enforcing this auto-push, click **Add Policy Set**.
5. In the displayed list of policy sets, check those that you want to exempt from auto-pushing this app to devices.
6. Click **Add** to exempt these policy sets, or **Cancel** to discard your selection.
7. Click **Save** to retain your changes to this app, or **Cancel** to discard them.

## Behavior on iOS

Noted here are some behaviors of auto-pushed apps on iOS.

### Cannot Auto-Push on Top of Unmanaged App

If a version of an application that is not managed by the GC is already installed on a user's iOS device, an attempt to auto-push a later, managed version of the app will fail.

**Workaround:** Delete the previously installed, unmanaged version of the app from the device, and then auto-push the later, managed version.

### Duplicate Apple ID on Multiple Devices

If a user uses his Apple ID (the ID for logging into the Apple Store) on more than one device, one of which is enrolled in Good device management, and with sync enabled, managed apps that are auto-pushed to the enrolled device are also pushed to the other device.

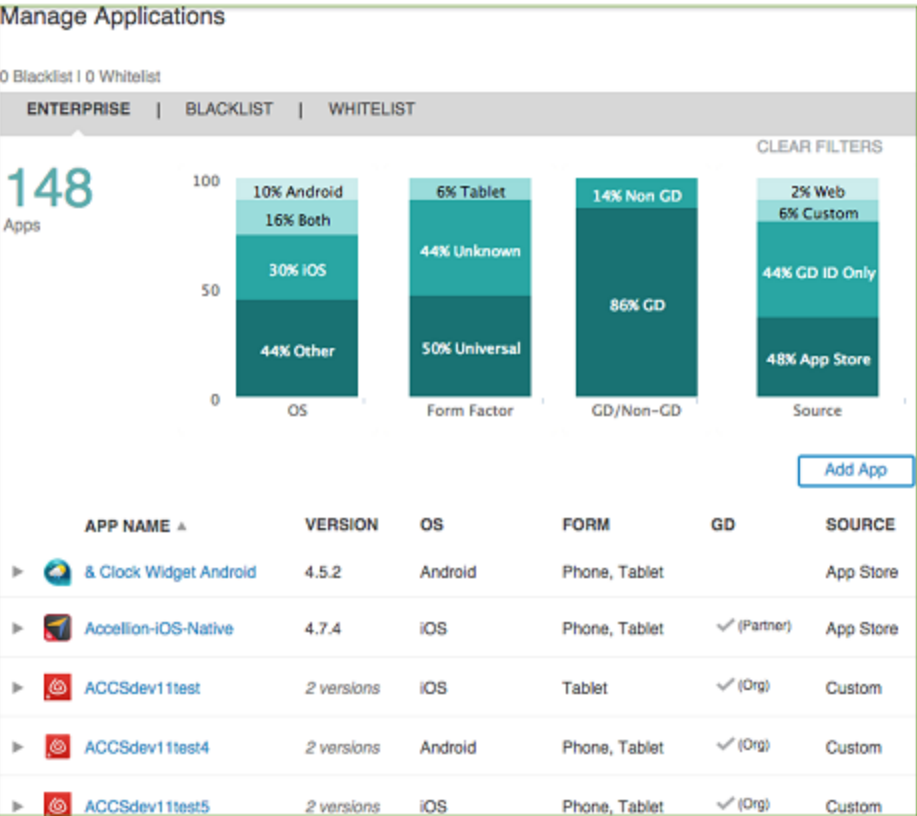
If the enrolled device is subsequently unenrolled, the auto-pushed apps are removed from formerly enrolled device but not removed from the other device.

Remove iOS MDM Profile: Auto-pushed Apps are Deleted

On iOS, the end-user always has the ability to remove any device management profile imposed the device. If the iOS end-user removes the installed profile, any apps that have been auto-pushed to the device are also removed.

Filtering the List of Applications, Viewing the Bar Chart

In Good Control's **Manage App** screen, some details about applications that have been put under management are listed and summarized in graphic form.



Details in List View

For each managed application, the following fields are shown in the list:

- **App Name:** field is sortable in ascending or descending order.
- **Version:** latest version to have been uploaded or put under management.
- **OS:** operating system, either **Android** or **iOS**.
- **Form:** the form factor (that is hardware types the app runs on), **Phone** or **Tablet**.

- **GD:** Whether the app is Good-based, with details as follows;
  - A blank means that the application is not Good-based.
  - A **checkmark (Org)** means that your own organization originated the Good-based app.
  - A **checkmark (Partner)** means that a Good partner company or Independent Software Vendor (ISV) originated the Good-based app.
- **Source:** Either **App Store**, **Custom**, **Web** or GD App ID only. In the case of the Apple App Store (not the Google Play Store), applications that are purchasable show the price, or if not purchasable, show **Free**.

## Filters

At the top of the **Manage Apps** page are several filters that you can use to restrict the data summarized in the bar chart and the list of applications beneath the graphic, from left to right.

Filter Name	Description
Filter: Name/GD App ID	Enter either the name of the application or its GD App ID
All OSs	Select from: <ul style="list-style-type: none"> <li>• All OSs</li> <li>• Android</li> <li>• iOS</li> </ul>
All Form Factors	Select from: <ul style="list-style-type: none"> <li>• All Form Factors</li> <li>• Phone</li> <li>• Tablet</li> </ul>
All Apps	Select from: <ul style="list-style-type: none"> <li>• All Apps</li> <li>• GD apps</li> <li>• Non-GD Apps</li> </ul>
All Sources	Select from: <ul style="list-style-type: none"> <li>• App Store</li> <li>• Custom</li> <li>• Web</li> <li>• GD App ID</li> </ul>

The result of your selection is:

- The bar chart is redrawn to show the percentages of data that match the selections you made.
- The list of applications beneath the bar chart is constrained to include only data that matches the selections you made.

To clear the selections after you have selected filters, in the upper right, click **Clear Filters**.

## Display of Bundle ID Only: App Removed from GD NOC

In the list of apps displayed by Managed Apps page, an app listed without a name and with only a Bundle ID has been removed from the Good Dynamics Network Operations Center (GD NOC) servers.

## Editing Application Details

There are several different tabs where you can edit details about the application. The displayed tabs depend on the type of application.

You can edit the details for all application types, including the GD App ID and application version.

The app stores are the source of details for public store apps; after updating details in the app store, in Good Control, you refresh the metadata for the affected app, as described in the steps below.

Good AM uses APIs from Apple to retrieve details about iOS applications in the App Store. However, because Google does not provide a callable API to retrieve details from the Google Play Store, Good AM attempts to collect these details by analysis of the Google Play Store pages themselves.

The complete set of tabs is as follows.

Tab Name	Editable Details
General	Application name, icon, and description. The fields vendor, source, and minimum OS are also displayed.
Android	Description, release notes, package name and versions, and screenshots
iOS	Description, release notes, package name and versions, and screenshots
Good Dynamics	<ul style="list-style-type: none"> <li>• GD App ID, and corresponding fields for iOS, Android, and Microsoft Windows.</li> </ul> <p>See also <a href="#">GD Entitlement ID and Version</a> .</p> <ul style="list-style-type: none"> <li>• Android Package ID</li> <li>• Apple iPad Bundle ID</li> <li>• Apple iPhone Bundle ID</li> <li>• Windows Phone Application ID</li> <li>• Windows Application ID</li> </ul>

Tab Name	Editable Details
	<ul style="list-style-type: none"> <li>• Policy Set Override</li> <li>• Server configuration for primary and secondary GP clusters</li> <li>• Versions, including: <ul style="list-style-type: none"> <li>• Release status: development or production</li> <li>• Alternate URL for Welcome email</li> <li>• Service names and bindings</li> </ul> </li> </ul>
Configuration	Upload application policy in XML format. For details, see the Good Control online help.

## General Steps

This guide does not detail the exact steps for updating all available fields, because their meanings are clear. The general process to edit details for an application in the application catalog:

1. For public store apps, be sure to update details about the app in the public store itself, where the details are stored.
2. In Good Control, navigate to **Manage Apps > Enterprise** tab.
3. Scroll to find the application you want, or use the GD App ID or name in the filter in the upper left, or sort the list of applications by descending or ascending application name.
4. Click the name of the application.
5. On the **General** tab:
  6. For public store applications, click **Refresh Metadata** to pull the latest details from the appropriate app store.
  7. On the **General** tab for all other application types, find the block that includes the details you want to change, and click **Edit**.
  8. Click **Cancel** to discard your changes or **Save** to save them.
  9. Repeat the previous two steps for the other tabs.

## Updating Apps

See the recommendations in [About Updating Applications](#).

Described here are the steps for updating applications that have been added to application management. "Updating applications" means changing the application itself, such as uploading new binary executables, as opposed to changing details about the application, which is described in [Editing Application Details](#).

**Note:** After updates are done in Good Control, it can take up to five minutes for the updates to appear in the end-user accessible application catalog.

## Updating a Public Store App: Work in Public Store, Refresh in Good Control

Because the binary executable files for public store applications are stored in the public stores themselves, your work related to updating public store apps has two general parts:

1. Upload new binary versions to the affected public app store and supply other details required by the store.
2. In Good Control, refresh the metadata for the affected application. See details in [Editing Application Details](#).

**Important:** If the public app store is down or its interfaces are not available or not responsive, Good Control cannot retrieve details from it.

## Updating a Custom App: Upload New Binary

Avoid uploading older application versions. The system allows you to upload older versions of an application (one whose GD application version is older than the application version already under managed control). Although this is possible, it is not best practice. You should use Good application management to distribute the latest version of an application, not old versions.

To update a custom application's binary executable file:

1. Make sure you have the new binary executable file you want to upload and that it has a different version number than the binaries already in the system.
2. In Good Control, navigate to **Manage Apps > Enterprise** tab.
3. Scroll to find the application you want, or use the GD App ID or application name in the filter in the upper left, or sort the list of applications by descending or ascending application name.
4. Click the name of the application.
5. In the upper right, click **Update App**.
6. In the displayed dialog, click **Choose**, and navigate your computer to find and select the desired binary executable file.
7. Click **Cancel** to discard the update, or **Update App** to continue.

## Updating a Web App: Add New Web App

A web application has no manageable binary executable associated with it.

If the URL for a previously added web application changes, define a new web application for it, as described in [Adding a Web Application](#). Each unique URL is considered a unique web application.

## Updating a GD-App-ID-Only App: Convert to Public Store or Custom App

By definition in [Types of Applications](#) a GD-App-ID-Only initially has no associated binary executable file. However, after the executable binary is ready, you can update the previously defined GD-App-ID-Only

application to be a public store or custom app.

**To convert a GD-App-ID-Only application to public store or custom app:**

1. Build the executable binary for the GD-App-ID-Only app, using the same GD App ID and application version values that you originally defined with the application was created in Good Control.
2. For public store applications, post your application to the appropriate store.
3. For custom application, have the executable binary ready to upload.
4. In Good Control, navigate to **Manage Apps**.
5. Find the previously defined GD-App-ID-Only application in the list.
6. Click the name of the application.
7. In the upper right click **Update App**.
8. Click the radio button for either Public Store App or Custom App.
9. Click **Next**.
10. For a public store app, specify the details required.
11. For a custom app, click Upload, browse your computer to find the executable binary, and upload it.

## Application or Container Policy Reference

Included here are the policies available to control applications or application containers. (Device policies are listed in [Device Policy Reference](#).) You can use these lists to help plan the device policies you need.

In Good Control, application/container policies are grouped under the following general headings:

- **Security Policies:** These policies relate to security aspects of the application, such as passwords, lock screen and inactivity timeout.
- **Compliance Policies:** These policies relate to controlling what hardware models and which versions of an operating system are allowed.
- **Application Policies:** These policies are Good-application-specific and relate to the features of an application itself.

### Security Policies

Security policies govern application password and other authentication, provisioning email template, and other features.

#### Password Policies

- Expire password after \_\_ days
- Require both letters and numbers
- Disallow \_\_ previously used passwords
- Require both upper and lower case
- Require at least 4 characters
- Require at least one special character
- Allow at most 3 occurrences of any given character
- Do not allow more than 2 numbers in sequence
- Do not allow more than one password change per day
- Do not allow personal information
- Allow Touch ID (iOS only)

#### Lock Screen Policies

- Always require password on application startup
- Require password when idle for more than 1 hour
- After 10 invalid password attempts *Lock Out User*

#### Wearable Policies

- Allow Wearables



## Authentication Delegation

*Add specific applications*

## Data Leakage Prevention

- Prevent copy from GD apps into non-GD apps (default = on)
- Prevent Android Screen Capture (default = on)
- Additionally, following new options have been added:
- Prevent copy from non-GD apps into GD apps (default = off)
- Prevent Android Dictation (default = on)
- Prevent iOS Dictation (default = on)

## Provisioning Policies

- Access Keys expire after 30 days
- Welcome Email Template

## Compliance Policies

Compliance policies relate to enforcement of allowed operating system versions and hardware models for

- iOS
- Android
- Microsoft Windows

Each platform has policies grouped as follows. The lowest level settings for hardware and OS versions are not shown here:

- OS Version Verification
  - With a checkbox to allow all OS versions or individual checkboxes to allow only specific versions
  - With a failure action for non-compliance: Application not allowed to run or wipe data
- Hardware Model Verification
  - With a checkbox to allow all models or individual checkboxes to allow only specific models
  - With a failure action for non-compliance: Application not allowed to run or wipe data
- Good Dynamics library version verification, with failure action
- Connectivity verification
- Antivirus Signature status

## About Windows OS Compliance Version "6.3"

The version number "6.3" shown in the GC console, which is actually the version of the underlying NT kernel, corresponds to Windows OS version 8.1.

## Application Policies

Application-specific policies for Good-based applications depend on the specific application and are not listed here.

Consult the Good Control console for the latest application-specific policies.

## Deleting a Managed Application

To remove the accessibility to an application, delete the application.

The exact effect of removing an application from managed apps depends on its type. If the application is Good-based, and thus has a defined GD Entitlement ID and version, the application is removed from the application catalog (appstore) and wiped from users' devices. Otherwise, the application is merely removed from the catalog but left intact on end-users' devices. Likewise, removing a web application from the catalog has no effect on the web application itself.

**Note:** If your GC is in development mode, you cannot delete a production app. This restriction is to prevent the inadvertent deletion of a production app by a development team.

Good Control operates in two modes: development and production. (By default, at installation, a GC runs in development mode. A production GC is one in which the administrator has set a production license.) Likewise, the status of an app is marked as production or development.

Non-GD apps (apps without a GD Entitlement ID) are always considered as production.

**To delete a managed app, in Good Control:**

1. Navigate to **Manage Apps > Enterprise** tab.
2. Scroll to find the application you want to remove from the catalog or sort the list of applications by descending or ascending application name.
3. Click the name of the application.
4. On the displayed **General** tab, in the upper right click **Remove App**. The **Remove App** button is displayed only if the conditions described in the note above are met.
5. Click **OK** to confirm the deletion or **Cancel** to keep it.

## Using the Launcher

Feature Support Matrix by Platform	
Applies to	Good Access for Android
	Good Access for iOS

	Good Access for MacOS
	Good Access for Windows

The Launcher allows you to quickly switch between the Good application currently open and any other Good Dynamics apps on your device, move between Mail, Calendar, Contacts, and Docs when Good Work is installed, as well as the Good AppStore, where available. The Launcher also gives you access to Quick Create tools for email, contacts, and calendar events, along with access to your configurable Good Work application settings.

**Using the Good Launcher is easy:**

- a. To open the Launcher, tap it.
- b. To move the Launcher, touch it, then slide it to place it anywhere on the screen.
- c. To open any of the apps listed, tap one.
- d. To open the Quick Create menu—Email, Event, Contact, or Note (when Notepad is available)—tap .
- e. To open your application **Settings**, tap .
- f. To close the Launcher, tap .

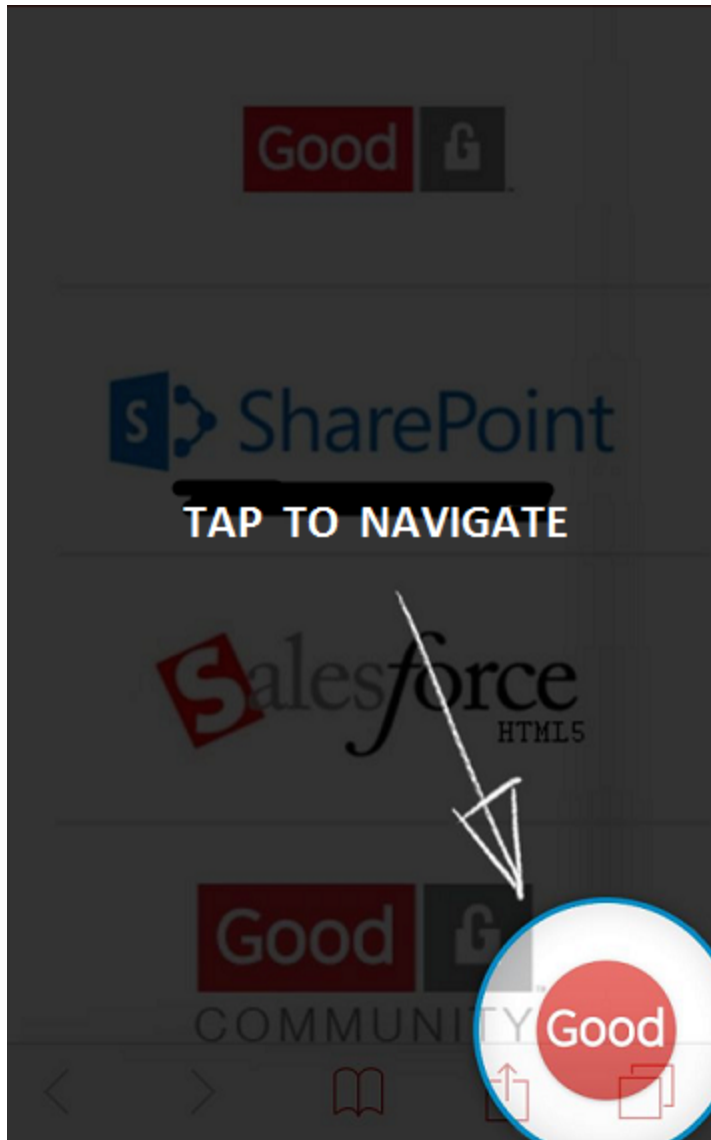
**Note:** The features you see in Quick Create are based on what software your company is entitled to and what software you have installed on your device. If you are using Good Access but do not have Good Work or other applications installed, you do not see the Quick Create menu.

## Viewing the Good Application Catalog in the Launcher

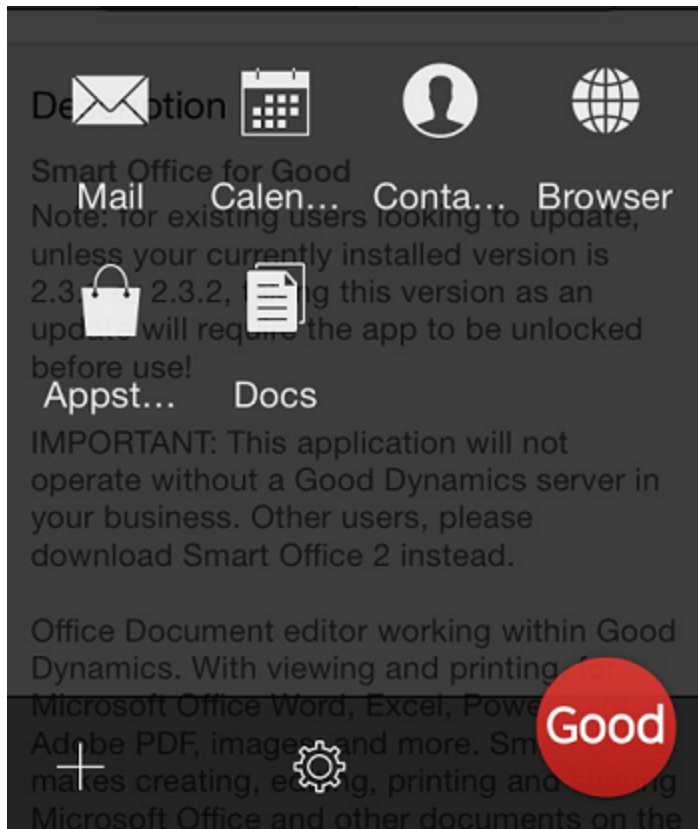
The application catalog, also sometimes known as the "app store" is configured by the administrator of Good Control. See full details in [Good Device and Application Management](#).

You can use Good Access to view the application catalog served by Good Dynamics and choose allowed applications you would like to install. Here are high-level steps.

1. Download, activate, start Good Access and authenticate yourself to it. The following page is displayed:





2. In the lower right is the circled red Good logo, which is sometimes called the *launcher*. Click the launcher.
3. To use the Good Access browser, click the **Browser** icon. Otherwise, to view the application catalog, click the **Appstore** shopping bag icon:





4. From the displayed application catalog, pick and choose the desired applications and follow the leading prompts to open or install them. You are directed to the appropriate source for the application.


Enterprise Appstore


 IBM Cognos Mobile for Good


 Qumu HD for Good


 Good Work


 Smart Office for Good

 EA Good Control

 Roambi Analytics for Good

 PhotoInk for Good

 Code Red RMS for Good

 Good for Salesforce1



To return to the Good Access browser or exit the application catalog, tap the launcher (the red-circled Good logo in the lower right).

## Device Policy Reference

Included here are the settings that can be configured for device policies. You can use these lists to help plan the device policies you need.

Device policies are organized into several sections:

- General
- Password: Strictness, format, length, and other characteristics of device passwords
- Restrictions: Specific device features that can be managed, grouped by operating system
- **Add Device Configurations:** To associate device policies with previously defined device configurations.

### Disabling US Government Notice and Consent Form

Samsung enforces the U.S. Federal Government's requirement to display a notice and consent form to end-users whenever U.S. government sites or data are accessed.

Samsung enables this notice by default, which might not be desirable outside the USA.

Good device management includes a device policy setting to disable it.

**To enable or disable the U.S. Government notice and consent device policy, in Good Control:**

1. Navigate to **Device Policies** > *edit a policy* > **Restrictions** tab.
2. Scroll to find **KNOX Standard (SAFE) Restrictions**.
3. Click **Edit**.
4. Scroll again to find **Disable Notice and Consent**.
5. Click the **OFF** radio button.
6. Click **Save** to save your change or **Cancel** to discard it.

### Device Policy Reference: General

These are the general settings that can be configured.

**Note:** Always consult the GC **Device Policies** > **General** tab for the latest list of restrictions.

#### Good For KNOX

**Note:** Good for KNOX settings are independent from the KNOX Safe restrictions listed in [Device Policy Reference: Restrictions](#).

- Good for KNOX Enabled
- Attestation trigger
  - Periodically every X hours

## Device Access Controls

You must set at least one of these access control policies.

**Note:** For your initial policy for use with Apple DEP device, be sure that you enable all these settings.

- **MDM Enabled:** In order for device configurations to be sent to devices, this setting must be ON.
  - Allow device erase
  - Allow inventory of personal apps
  - Check compliance against:
    - Black List / White List
  - Allow query of Device Information (serial number, IMEI, etc) (iOS)
  - Allow query of Network information (carrier network, phone number, etc) (iOS)
  - Allow device lock and passcode removal (iOS)
  - Allow password-related queries
  - Allow restriction-related queries
  - Allow remote app installation/updates
  - Allow inspection of installed configuration profiles (iOS)
  - Allow installation and removal of configuration profiles (iOS)
  - Allow inspection of installed provisioning profiles (iOS)
  - Allow installation and removal of provisioning profiles (iOS)
  - Allow manipulation of settings (iOS)

## Device Policy Reference: Passwords

These are settings for device passwords that can be configured in device policies.

**Note:** Always consult the GC **Device Policies > Passwords** tab for the latest list of restrictions.

### Require a password and Quality

If a password is required (default), the other settings appear.

The number of settable characteristics of passwords changes depending on your choice for password **Quality**:

- Simple
- Alphanumeric
- Complex

**Note:** On Windows tablet devices, password restrictions have significantly differing behavior. See [Password Restrictions on Windows Tablet](#) .



## Quality Simple

- Minimum password contains X characters
- Password expiration in X days
- Prevent users from reusing the last X unique passwords
- Device wipes out after X failed attempts
- Screen lock after X minutes of inactivity
- Maximum grace period of X minutes for screen lock (iOS)
- MaximumSequential Characters (Good for KNOX)
- MinimumChanged Characters (Good for KNOX)
- Simple password type (Android) Any | Numeric | Alphabetic

## Quality Alphanumeric

Same as Simple, without "Simple Password Type (Android)".

- Minimum password contains X characters.
- Password expiration in X days
- Prevent users from reusing the last X unique passwords
- Device wipes out after X failed attempts
- Screen lock after X minutes of inactivity
- Maximum grace period of X minutes for screen lock (iOS)
- Maximum X Sequential Characters (Good for KNOX)
- Minimum X Changed Characters (Good for KNOX)

## Quality Complex

- Minimum X Symbols Required
- Minimum X Digits Required (Android)
- Minimum X Lower Case Letters Required (Android)
- Minimum X Upper Case Letters Required (Android)
- Minimum X Letters Required (Android)
- Minimum X non-Letters Required (Android)

## Password Restrictions on Windows Tablet

See [Windows Tablet Device Management: Known Limitations](#) for details on the behavior of password policies and other limitations.

## Device Policy Reference: Restrictions

This is a list of the settable device restrictions for iOS, Android, Samsung KNOX Standard (SAFE), and Windows.

**Note:** Always consult the GC Device Policies > Restrictions tab for the latest list of restrictions.

In these lists:

- ✓ indicates that the restriction is enabled by default,
- — indicates that the restriction is disabled by default.

### iOS Restrictable Features

In these lists:

- ✓ indicates that the restriction is enabled by default,
- — indicates that the restriction is disabled by default.

#### Functionality

- ✓ Allow use of camera
- ✓ Allow Facetime
- ✓ Allow screenshots and screen recording (iOS9+)
- ✓ Allow Voice dialing
- ✓ Allow Siri (iOS 5+)
- ✓ Allow Siri while device is locked (iOS 5.1+)
- Enable Siri profanity filter
- ✓ Allow installing apps (including Apple Configurator and iTunes)
- ✓ Allow In-App Purchase
- Require iTunes Store password for all purchases
- ✓ Allow iCloud backup
- ✓ Allow iCloud documents & data
- ✓ Allow iCloud keychain (iOS 7+)
- ✓ Allow iCloud Photo Library (iOS 9+)
- ✓ Allow My Photo Stream
- ✓ Allow Shared Stream
- ✓ Allow managed apps to store data in iCloud (iOS 8+)
- ✓ Allow backup of enterprise books (iOS 8+)

- ✓ Allow notes and highlights sync for enterprise books (iOS 8+)
- ✓ Allow automatic sync while roaming
- Force encrypted backups
- Force limited ad tracking
- ✓ Allow Internet results in Spotlight (iOS 8+)
- ✓ Allow automatic updates to certificate trust settings (iOS 7+)
- ✓ Allow documents from unmanaged apps in managed apps (iOS 7+)
- ✓ Allow documents from managed apps in unmanaged apps (iOS 7+)
- ✓ Treat AirDrop as unmanaged destination (iOS 9+)
- ✓ Allow untrusted TLS prompt
- ✓ Allow sending diagnostic data to Apple (iOS 6+)
- ✓ Allow Touch ID to unlock device (iOS 7+)
- ✓ Allow HandOff (iOS 8+)
- Require pairing password on incoming AirPlay requests
- Require pairing password on outgoing AirPlay requests
- ✓ Allow Passbook notifications while locked (iOS 6+)
- ✓ Show Control Center in lock screen (iOS 7+)
- ✓ Show Notifications Center in lock screen (iOS 7+)
- ✓ Show Today View in lock screen (iOS 7+)

## Apps

- ✓ Allow use of YouTube (iOS 6 and below)
- ✓ Allow use of iTunes Store
- ✓ Allow adding Game Center friends
- ✓ Allow multiplayer gaming
- ✓ Allow Safari
- ✓ Enable autofill
- ✓ Enable JavaScript
- Block pop-ups
- Force fraud warning
- Accept Cookies: Always

- ✓ Trust new enterprise app authors (iOS 9+)

## Media Content

Allowed content ratings

Ratings Region: US

### Movies

Allow All Movies

### TV Shows

Allow All TV Shows

### Apps

Allow All Apps

- ✓ Allow playback of explicit music, podcasts & iTunes U media
- ✓ Allow explicit sexual content in iBooks Store (iOS 6+)

## Apple Watch

— Force Apple Watch wrist detection (iOS 8+)

## Supervised Mode

### General

- ✓ Allow AirDrop
- ✓ Allow iMessage
- ✓ Show user-generated content in Siri
- ✓ Allow iBooks store
- ✓ Allow erase all content and settings
- ✓ Allow modifying restrictions
- ✓ Allow installing configuration profiles
- ✓ Allow modifying account settings
- ✓ Allow modifying cellular data app settings
- ✓ Allow modifying Find My Friends settings
- ✓ Allow pairing with non-Configurator hosts
- ✓ Allow Define
- ✓ Allow modifying device passcode (iOS 9+)
- ✓ Allow modifying Touch ID fingerprints

✓ Allow modifying device name (iOS 9+)

✓ Allow modifying Wallpaper (iOS 9+)

### Keyboard

✓ Allow predictive keyboard

✓ Allow auto correction

✓ Allow spell check

✓ Allow keyboard shortcuts (iOS 9+)

### Apps

✓ Allow installing apps using App Store

✓ Allow Automatic App Downloads (iOS 9+)

✓ Allow removing apps

✓ Allow use of Podcasts

✓ Allow use of Game Center

✓ Allow use of Apple News (iOS 9+)

### Apple Watch

✓ Allow pairing with Apple Watch (iOS 9+)

## Android Restrictable Features

In these lists:

- ✓ indicates that the restriction is enabled by default,
- — indicates that the restriction is disabled by default.

— Disable camera

— Encrypt internal storage

## KNOX Standard (SAFE) Restrictable Features

The KNOX Standard (SAFE) restrictions here are independent from the settings for Good For KNOX listed in [Device Policy Reference: General](#) .

In these lists:

- ✓ indicates that the restriction is enabled by default,
- — indicates that the restriction is disabled by default.

## General Restrictions

— Encrypt SD Card

- Disable SMS
- Disable MMS
- Disable SD Card
- Disable NFC
- Disable Android Beam
- Disable Cellular data
- Disable Lock Screen Widgets
- Disable Factory Reset
- Disable Native Browser
- Disable lock screen shortcuts
- Notice and Consent Banner

### **Location & Roaming Restrictions**

- Disable Roaming Data
- Disable Roaming Sync
- Disable Roaming VoiceCalls

### **Capture Restrictions**

- Disable SVoice
- Disable Screen Capture

### **WiFi Restrictions**

- Disable WiFi
- Disable WiFi Auto Connect

### **Bluetooth Restrictions**

- Disable Bluetooth

### **Software & Update Restrictions**

- Disable Google Play Store
- Disable Non-Market apps
- Disable OTAOS Update

### **USB & Tethering Restrictions**

- ✓ Disable USB Debugging

- Disable USB Media Player (MTP — also controls USB MS and USB KIES)
- Disable USB Host Storage
- Disable Bluetooth Tethering
- Disable USB Tethering
- Disable WiFi Tethering

## KNOX Premium

- Enable Common Criteria Mode (Requires Good for KNOX)

## About Enabling Common Criteria Mode

This description is based on documentation from Samsung.

An administrator can enable Common Criteria configuration on a device. When enabled, the following are the effects:

- The bootloader blocks KIES download mode and enforces a check of integrity of the kernel and of the self-test crypto modules.
- The device will verify the additional signature on FOTA ("firmware over-the-air") update using a RSA-PSS signature
- The device will enforce the use of the FIPS 140-2 validated crypto module for EAP-TLS Wi-Fi connections. (For more information about WiFi device configuration in Good device management, see [Wi-Fi Configuration](#) .)

To fully enable Common Criteria-evaluated configuration, the following should also be enforced:

1. Enable Device Encryption
2. Enable SD Card Encryption
3. Set Attempts before Wipe.
4. Enable Certificate Revocation (since KNOX 2.2)
5. Disable Password History (since KNOX 2.2)

## Microsoft Windows Restrictable Features

Unless otherwise stated in the headings, policies apply to all platforms of Windows.

In these lists:

- ✓ indicates that the restriction is enabled by default,
- — indicates that the restriction is disabled by default.

## Windows Restrictions

- ✓ Disable Data While Roaming
- ✓ Disable Development Unlock

- Require Device Encryption
- Disable Removable Storage Card
- Disable MDM un-enrollment
- Disable Camera
- Disable Bluetooth
- Disable Wi-Fi
- Disable Location Services
- Disable Microsoft Account Connection
- Disable Custom Email Accounts
- Disable Cortana
- Disable Internet Sharing
- Disable VPN While Roaming
- Disable VPN Over Cellular

### Windows Desktop/Tablet Restrictions

- Allow Diagnostic Data Submission
  - ✓ Require SmartScreen in Internet Explorer
- User Account Control (Windows 8.1): Notify app changes
- Microsoft Account Optional to use Modern Applications

### Phone Restrictions

- Disable MDM software and hardware factory reset
- Disable NFC
- Disable Microsoft Store
- Disable Copy/Paste
- Disable Share Office File (Windows 8.1)
- Disable Save As Office File (Windows 8.1)
- Disable Screen Capture
- Disable MTP and IPoUSB
- Disable Manual Installation of Root and Intermediate CAP Certificates
- Disable Manual Wi-Fi Configuration
- Disable Wi-Fi Hotspot Reporting to Microsoft



- Disable Action Center Notifications Above Lock Screen
- Disable Voice Recording
- Disable Browser

## Good Dynamics Documentation

All documents are in PDF and available on the [Good Developer Network](#).

Category	Title	Description
Cross-platform	<ul style="list-style-type: none"> <li><a href="#">Getting Started Guide for Marketplace Partners</a></li> <li><a href="#">Good Dynamics Platform Overview for Administrators and Developers</a></li> <li><a href="#">Good Cloud Deployment</a></li> </ul>	Overviews of the Good Dynamics system
	<ul style="list-style-type: none"> <li><a href="#">Good Device and Application Management</a></li> <li><a href="#">DM Enrollment: Good Agent for iOS</a></li> <li><a href="#">DM Enrollment: Good Agent for Android</a></li> </ul>	Device and application management on Good Control, including app distribution, with client-side device enrollment details
Security	<a href="#">GD Security White Paper</a>	Description of the security aspects of Good Dynamics
	<a href="#">GD Security White Paper: Mobile Application Management</a>	Focus specifically on application management
	<a href="#">Good Dynamics with Apple Touch ID</a>	Discussion of the implementation of Good security with Apple's fingerprint recognition system
Servers	<a href="#">GD Sizing Guide</a>	Recommendations and details about capacity planning for your GD deployment
	<a href="#">GD Server Preinstallation Checklist</a>	Same checklist extracted from the installation guide below
	<a href="#">Good Dynamics Server Installation</a>	Details on installing Good Control, Good Proxy, and the GC database
	<a href="#">GD Server Clustering and Affinities</a>	Configuration details on increasing the capacity of your deployment
	<a href="#">Kerberos Constrained Delegation for Good Dynamics</a>	Configuration details for integrating the Kerberos authentication system with GD
	<a href="#">Direct Connect</a>	Configuring Good Dynamics servers to securely access internal resources from the external Internet
	<a href="#">Easy Activation Overview</a>	A look at the Easy Activation feature
	<a href="#">GD Server Backup and Restore</a>	Minimal steps for backing up and restoring the GD system
	<a href="#">Good Control Online Help</a>	Printable copy of the GC console online help
	<a href="#">Good Control Cloud Online Help</a>	Printable copy of the Cloud GC console online help
	<a href="#">Good Control Web Services</a> : Programmatic interfaces on Good Control	

Category	Title	Description
	<ul style="list-style-type: none"> <li>Basic control and application management: SOAP over HTTPS. Documentation is in the WSDL files included with GC.</li> <li>Device management: HTTP API (with JSON) for device management. <a href="#">Zipfile of API reference</a>.</li> </ul>	
	<a href="#">Good Wrapping Server Installation</a>	Details for installing Good Wrapping server
	<a href="#">GD Application Wrapping Guide</a>	Details about wrapping applications
Software Development	<a href="#">GD Shared Services Framework</a>	Description of the GD shared services framework for software developers
	<a href="#">GD Connecting to A Clustered Application Server</a>	Details necessary if you have clustered your application servers
Android	<ul style="list-style-type: none"> <li><a href="#">GD SDK for Android</a></li> <li><a href="#">API Reference for Android</a></li> </ul>	Working with the GD SDK for Android and the essential reference for developers
iOS	<ul style="list-style-type: none"> <li><a href="#">GD SDK for iOS</a></li> <li><a href="#">API Reference for iOS</a></li> </ul>	Working with the GD SDK for iOS and the essential reference for developers
Windows	<ul style="list-style-type: none"> <li><a href="#">GD SDK for Universal Windows Platform (UWP)</a></li> <li><a href="#">API Reference for GD SDK for UWP</a></li> </ul>	Working with the GD SDK for Universal Windows Platform (UWP) and the essential reference for developers
iOS, Android	<a href="#">Good Launcher Library</a>	Source code and header files for implementing the popular Good Launcher interface
Cross-platform	<a href="#">Getting Started Guide for PhoneGap Developers - iOS and Android</a>	Working with the GD SDK and the Cordova PhoneGap plugin
	<a href="#">GD Secure HTML5 Bundle Getting Started Guide for Developers</a>	Working with the GD SDK and the secure HTML5 bundle
	<a href="#">GD Bindings for Xamarin for Android and for iOS</a> and the <a href="#">API Reference for Xamarin.iOS</a>	<p>Working with the GD SDK and the Xamarin cross-platform integrated development environment</p> <p>For Xamarin.Android, no separate API reference is needed; see the standard GD SDK <a href="#">API Reference for Android</a></p>