Integrating Good for Enterprise with Cisco Identity Services Engine

Revised: October 11, 2013

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Integrating Good for Enterprise with Cisco Identity Services Engine

Integrating Good for Enterprise with Cisco Identity Services Engine

This document supplements the Cisco Bring Your Own Device (BYOD) CVD (http://www.cisco.com/en/US/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/BYOD_Design_Guide.html) and provides mobile device management (MDM) partner-specific information as needed to integrate with Cisco ISE. In an effort to maintain readability, some of the information presented in the CVD is repeated here. However this document is not intended to provide standalone BYOD guidance. Furthermore, only a subset of the Good for Enterprise MDM functionality is discussed. Features not required to extend ISE's capabilities may be mentioned, but not in the detail required for a comprehensive understanding. The reader should be familiar with the The reader should be familiar with the Good for Enterprise Administrator's Guide before integrating Good for Enterprise with Cisco ISE.

This document is targeted at existing Good for Enterprise customers. Information necessary to select an MDM partner is not offered in this document. The features discussed are considered to be core functionality present in all MDM software and are required to be compatible with the ISE API.

Overview

Good for Enterprise is a leading provider of MDM software used to establish and enforce device policy on hand-held endpoints. This could include corporate- or employee-owned phones and tablets. Apple and Android devices are the primary focus, but Good for Enterprise also supports Windows Phone software versions 7.5 and 8, Palm, and Nokia devices. Only Apple iOS and Android devices are discussed in this document. Good Technology maintains an up-to-date database of supported devices on their monitoring portal.

Mobile Device management is a relatively new phenomenon and is in a constant state of expansion. Features can be thought of in several categories:

- Device Restrictions—There are two common types of restrictions. Either some feature of the device is disabled, such as the camera or there are additional requirements for basic usage, such as a PIN lock or storage encryption. When a restriction is in place, the user is not offered the choice of non-compliance. Restrictions are used to reduce security risks to the enterprise.
- Device Compliance—This may also be referred to as posture enforcement. The MDM will check the attributes of the device against a list of acceptable operational conditions. Compliance checks can be enforced based on their severity. For example, an email could be sent to the user when they have

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

exceeded 80% of their data plan or Good for Enterprise can automatically issue a corporate wipe if the device has been compromised. A compliance check is different from a restriction because the user can take the device out of compliance. Compliance can be used to increase security or reduce operational costs.

- Notifications—Administrators can send a message to a large population of devices. This could be a push message to the device notification page. For example, "The fire drill is complete, you may return to the building" could be sent to all devices on a particular campus. Notifications are used to increase productivity.
- Content Distribution—Bookmarks, documents, and other content can be pushed to devices in the background without user intervention or made available on demand. This data is then stored in a corporate container. Content distribution is used to increase productivity.
- Application Distribution—The MDM can offer a company catalog of available software or install required software. The software can come from public repositories or can be corporate-developed applications. Application distribution has both security and productivity gains. Security is enhanced because any software distributed by the MDM, including local storage associated to the software, is removed as part of a corporate wipe. This is not true if the user installs the same software from Apple's App Store or Google Play.

The Good for Enterprise system includes four major components:

- The Good Mobile Control (GMC) Server and Console—Provides facilities for managing MDM users and their devices.
- The Good Mobile Messaging Server (GMM)—Synchronize user devices with their Exchange accounts.
- The Good Monitoring Portal—Good Technology cloud-based server used to monitor and manage user handhelds.
- The Good for Enterprise Client—GFE Client—Device installed software supporting the handheld device itself.

Beyond these, there are additional components for enterprise integration, email, secure web, and data loss prevention. The majority of the base functionality is available through the MDM API built into the mobile device operating system. Good for Enterprise requires the client software to detect some conditions such as jailbroken[1] or rooted devices. Because ISE tests for these conditions, the Good for Enterprise server is configured to treat the client software as a required application and will install the software during the on-boarding process before full network access is granted.

On-Site Deployment Model

The GMC and GMM server components are installed and maintained at the customer premise behind the company's firewall. To gain full MDM functionality, the customer is required to integrate the on-premise server components into either a Microsoft Exchange or Lotus Domino environment. Starting with version 8, Good for Enterprise is compatible with Microsoft's Office-365 Cloud-Based Exchange offering, however the GMC and GMM servers will still be installed on the customer's local network. This document assumes a Microsoft Active Directory and Microsoft Exchange deployment. See the Good for Enterprise documentation for details on other configurations.

[1] Apple prefers the term Compromised OS when referring to devices where the user has gained elevated privileges to the operating system.

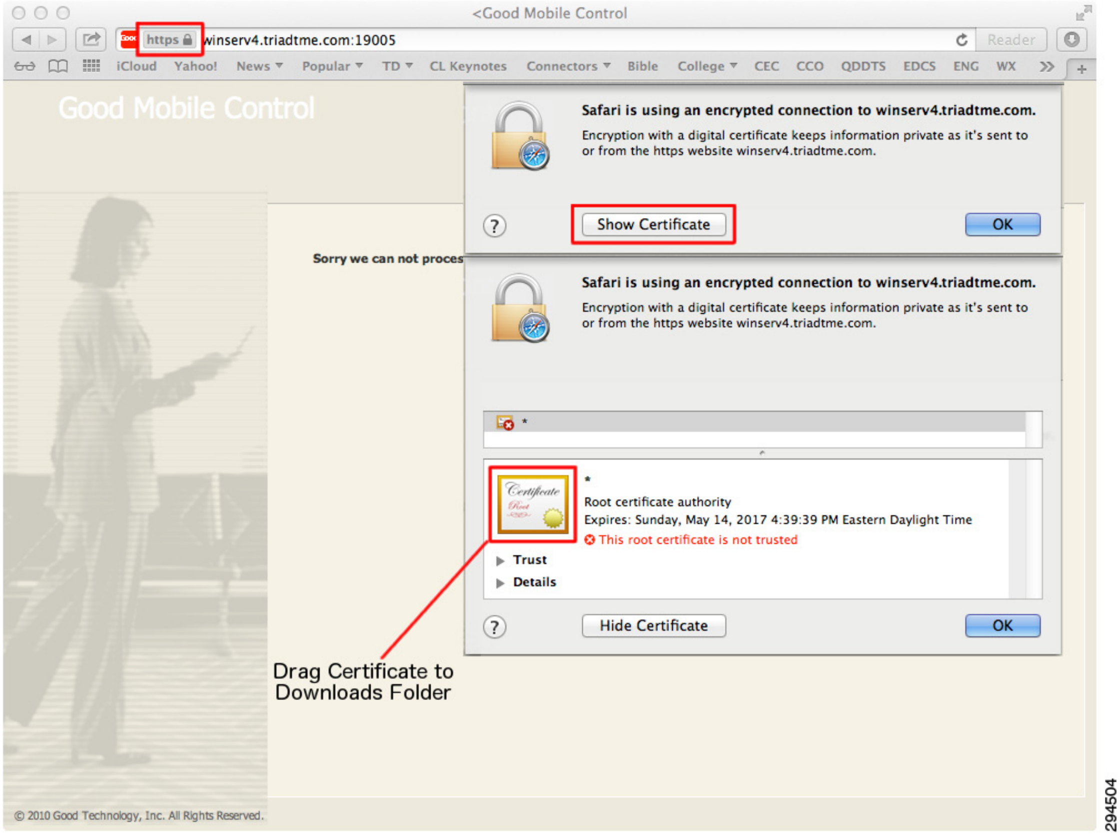
Getting Good for Enterprise Ready for ISE

The first requirement is to establish basic connectivity between the Cisco ISE server and the Good for Enterprise MDM. Both the Good Mobile Control and Good Mobile Messenger Servers must have Internet access. They should be able to connect to the public Internet using both http on port 80 and secure http on port 443. Both the Cisco ISE server and the Good for Enterprise server(s) should be located in the data center. Good does not recommend nor support a DMZ deployment for their MDM server components as a number of outbound ports must be opened to connect to the Microsoft Exchange server. Other specific corporate firewall ports must be opened to allow the Good Portal to send message notifications as well as push notifications for Apple and Android endpoints. A list of required ports is included later in this document, however the Good for Enterprise Administration Guide is the authoritative source.

Importing API Portal Certificate to ISE

The Good for Enterprise MDM server incorporates an HTTPS portal to support the various users of the system. ISE must establish trust with this website. Since ISE does not maintain a list of trusted root CAs, a system administrator must manually establish the trust relationship between ISE and the Good MDM. The simplest approach is to export the MDM site certificate and then import the certificate into the local cert store in ISE. Most browsers allow this. This process using the Safari browser is shown in Figure 1.

Figure 1 Exporting the MDM Site Certificate with Safari



Safari is using an encrypted connection to winserv4.triadtme.com.

Encryption with a digital certificate keeps information private as it's sent to or from the https website winserv4.triadtme.com.

Safari is using an encrypted connection to winserv4.triadtme.com.

Encryption with a digital certificate keeps information private as it's sent to or from the https website winserv4.triadtme.com.

*

Root certificate authority

Expires: Sunday, May 14, 2017 4:39:39 PM Eastern Daylight Time

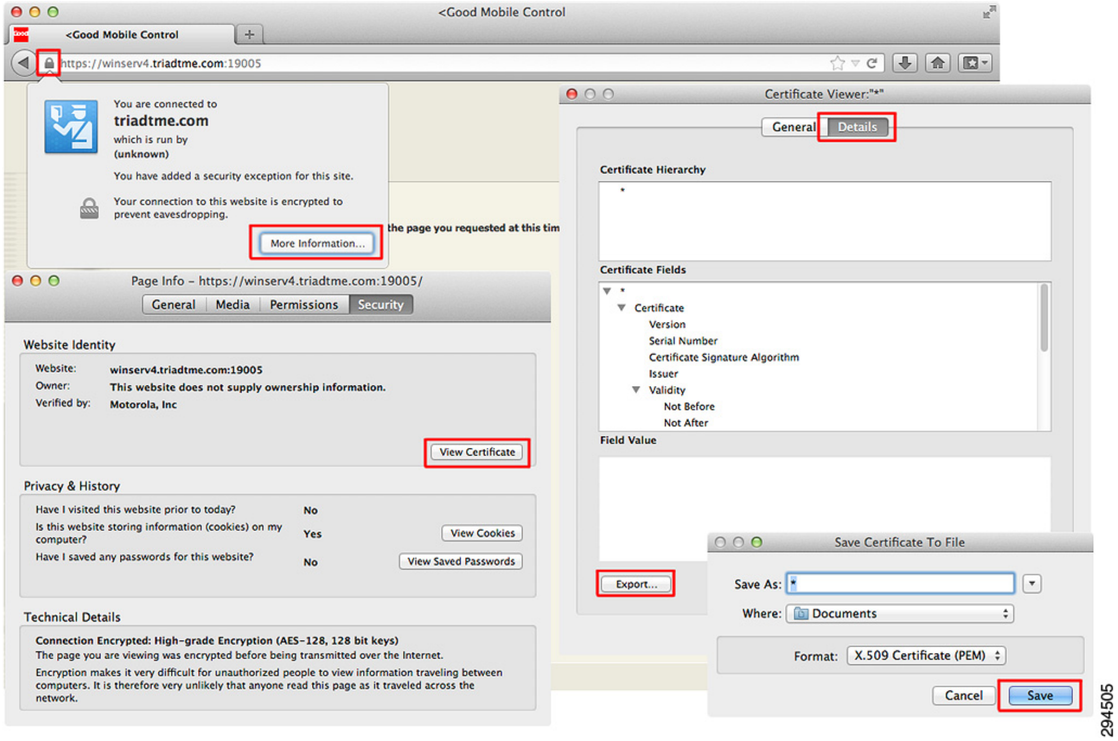
This root certificate is not trusted

Drag Certificate to Downloads Folder

Note Good for Enterprise utilizes a wildcard certificate that is valid for the server, however you must be sure to export the server's digital certificate from the correct secure http session. Be sure to browse to port 19005 to export the correct certificate. Your browser will say "Sorry we cannot process the page your requested at this time, please try again later". Ignore this message and export the certificate as shown in Figure 1.

Exporting a certificate from Firefox is shown in Figure 2.

Figure 2 Exporting the MDM Site Certificate with Firefox



https://winserv4.triadtme.com:19005

You are connected to
triadtme.com
which is run by
(unknown)

You have added a security exception for this site.

Your connection to this website is encrypted to prevent eavesdropping.

the page you requested at this tim

Website Identity

Website: winserv4.triadtme.com:19005
Owner: This website does not supply ownership information.
Verified by: Motorola, Inc

Privacy & History

Have I visited this website prior to today?	No
Is this website storing information (cookies) on my computer?	Yes
Have I saved any passwords for this website?	No

Technical Details

Connection Encrypted: High-grade Encryption (AES-128, 128 bit keys)
The page you are viewing was encrypted before being transmitted over the Internet.

Encryption makes it very difficult for unauthorized people to view information traveling between computers. It is therefore very unlikely that anyone read this page as it traveled across the network.

Certificate Hierarchy

*

Certificate Fields

```
▼ *
  ▼ Certificate
      Version
      Serial Number
      Certificate Signature Algorithm
      Issuer
    ▼ Validity
        Not Before
        Not After
```

Field Value

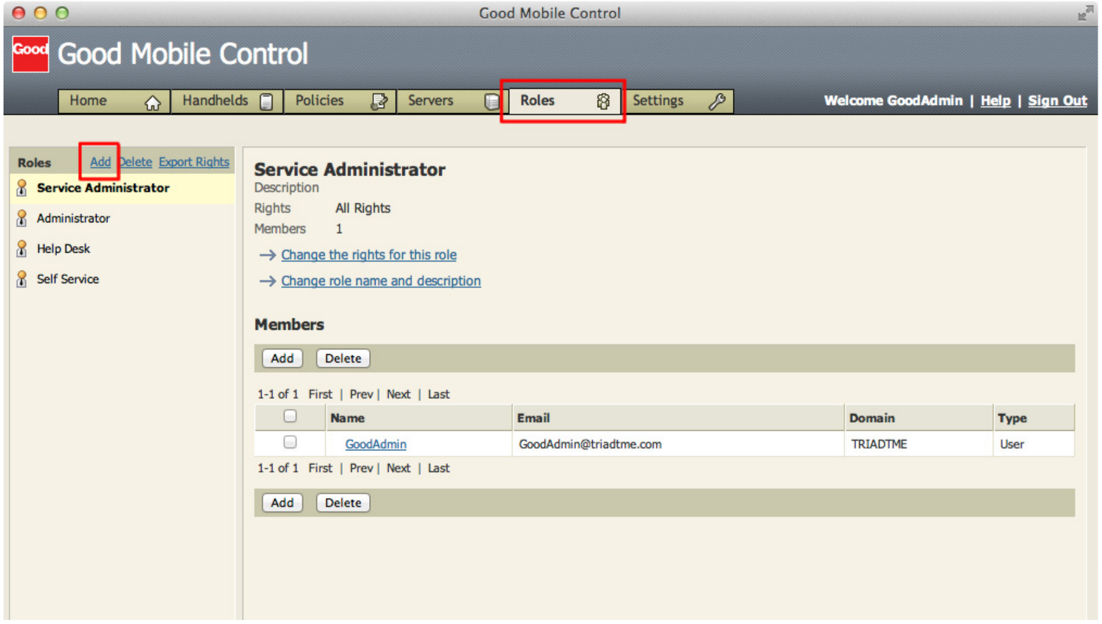
Save As: *
Where: Documents
Format: X.509 Certificate (PEM)

Granting ISE Access to the Good for Enterprise API

Good for Enterprise uses organization "roles" to logically partition access to the GMC control panel and the functions therein. Each role allows its members access to various controls while isolating the group from other administrative accounts. The highest-level role is known as "Service Administrator" and by default contains the user created during the original software installation (normally defined as GoodAdmin). Ideally a separate role and username would be configured for accessing the Good for Enterprise API. Figure 3 through Figure 7 show how to establish the needed access.

Note Organization roles and their implications for multi-domain ISE environments are out of scope for this document. Additional details concerning roles are available in the Good for Enterprise documentation.

Figure 3 Create API Administrator Role



Service Administrator

Description

Rights All Rights

Members 1

→ Change the rights for this role

→ Change role name and description

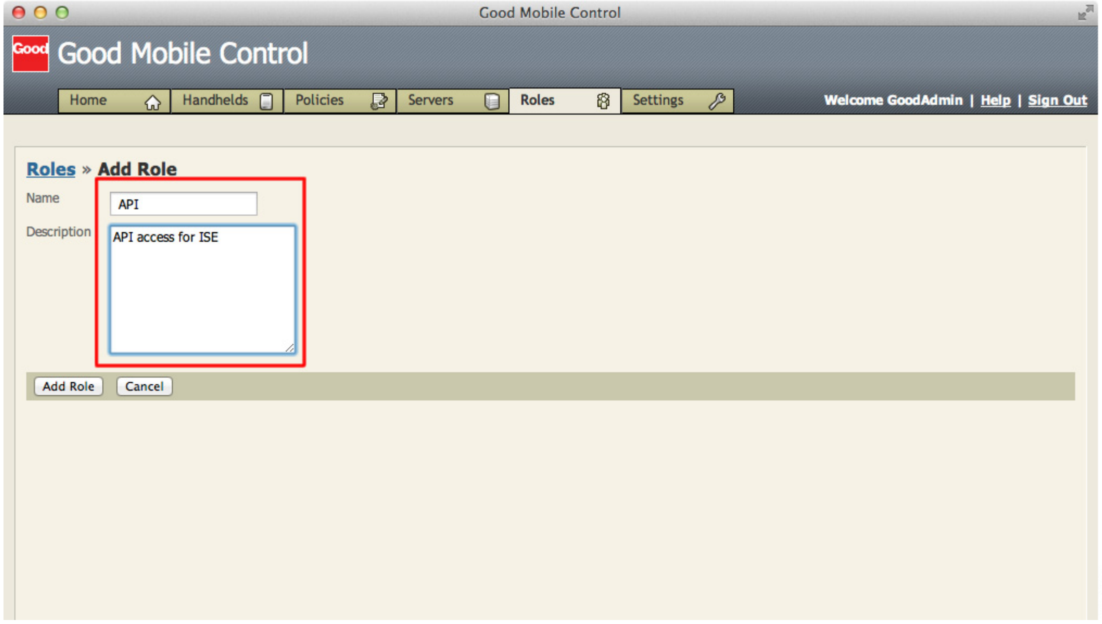
Members

1-1 of 1 First | Prev | Next | Last

□	Name	Email	Domain	Type
□	GoodAdmin	GoodAdmin@triadtme.com	TRIADTME	User

1-1 of 1 First | Prev | Next | Last

Figure 4 API Administrator Role Details



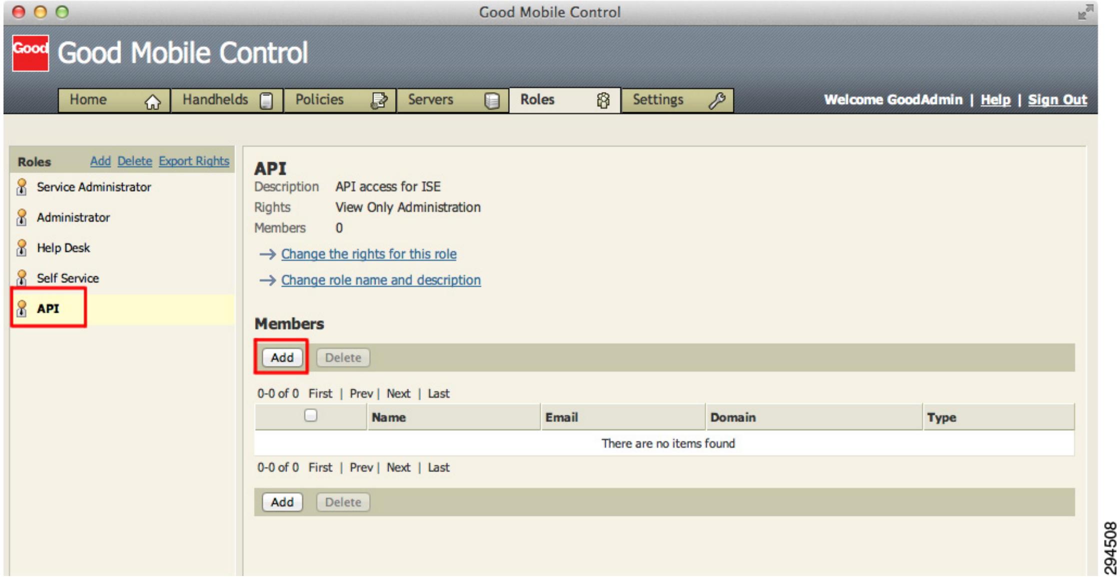
Roles » Add Role

Name: API

Description: API access for ISE

Note Once the new role is created, add a user account to grant API access to the Cisco ISE. The API member account must be created in the company's Active Directory and therefore is maintained through familiar channels. Figure 5 and Figure 6 show this process.

Figure 5 ***Add Active Directory Member to API Access Role***



API

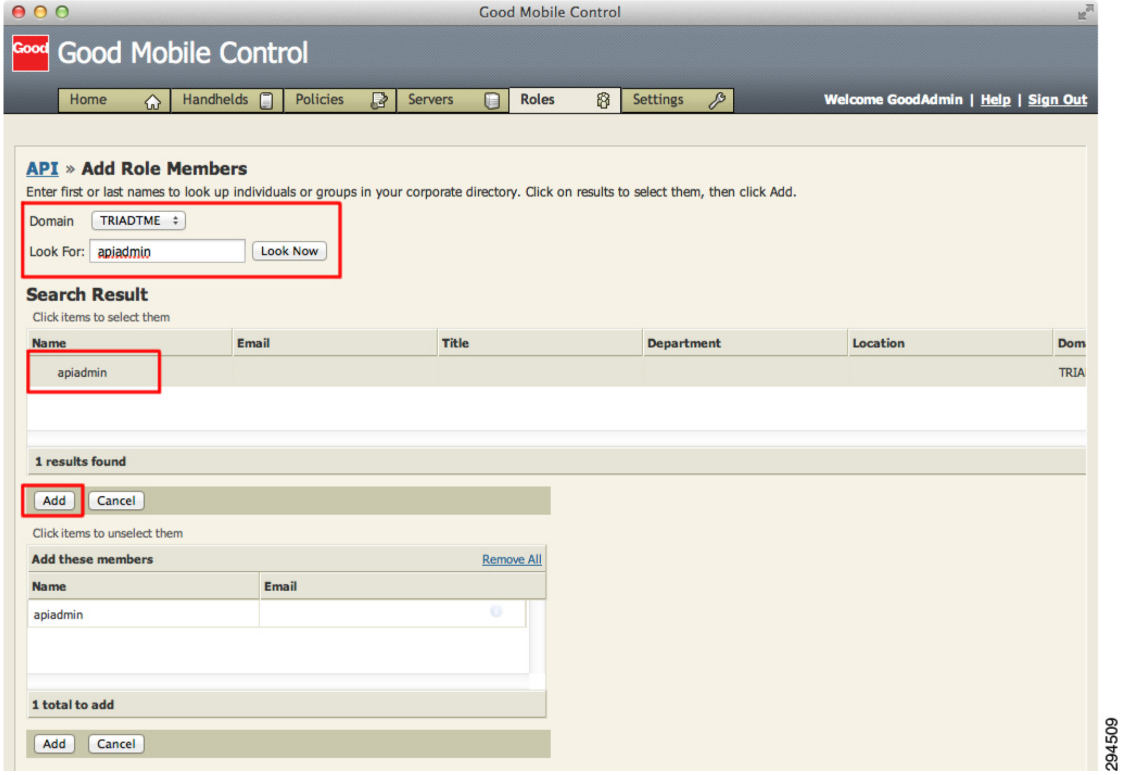
Description API access for ISE

Rights View Only Administration

Members 0

□	Name	Email	Domain	Type
		There are no items found		

Figure 6 ***Search Active Directory to Add the Proper ISE Account***



Enter first or last names to look up individuals or groups in your corporate directory. Click on results to select them, then click Add.

Domain TRIADTME

Look For: apiadmin

Name	Email	Title	Department	Location	Dom
apiadmin					TRIA

1 results found

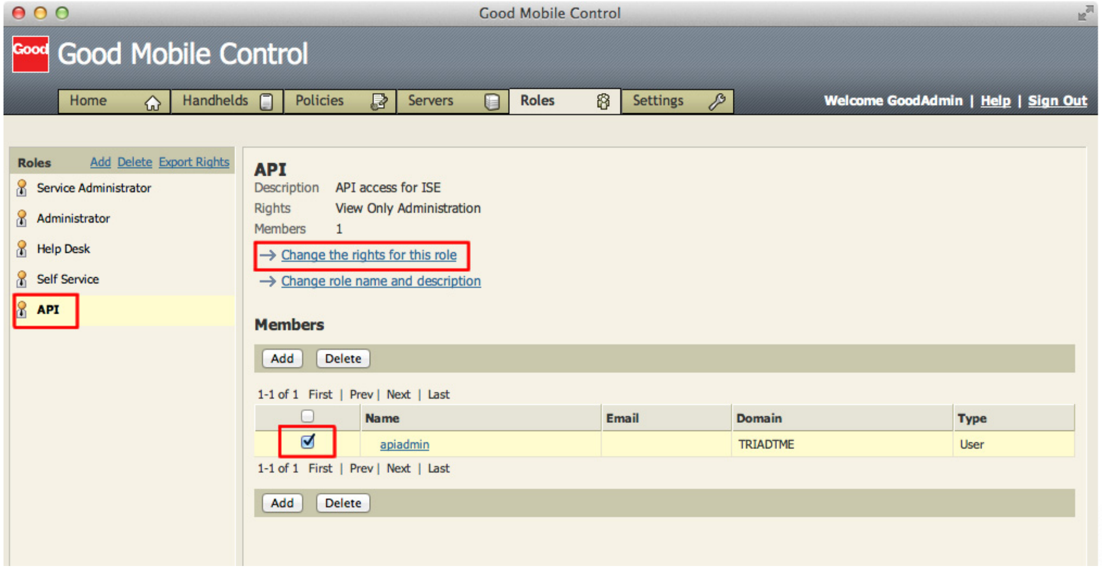
Add these members

Name	Email
apiadmin	

1 total to add

Each Role can be assigned rights entitling that group of users to specific system controls. Good for Enterprise provides default roles for the most common types of administrators and users. The majority of administrator roles have access to the MDM API by default, however it is a good idea to limit API access to specific accounts for added security. In Figure 7 and Figure 8, specific rights can be assigned per role. All users assigned to a specific role will have the same system rights based on role membership. Users can be members of multiple roles if needed.

Figure 7 Assign Specific Rights to API Role



Good Mobile Control

Good Mobile Control

Home | Handhelds | Policies | Servers | Roles | Settings

Welcome GoodAdmin | Help | Sign Out

Roles Add Delete Export Rights

- Service Administrator
- Administrator
- Help Desk
- Self Service
- API

API

Description API access for ISE

Rights View Only Administration

Members 1

→ Change the rights for this role

→ Change role name and description

Members

Add Delete

1-1 of 1 First | Prev | Next | Last

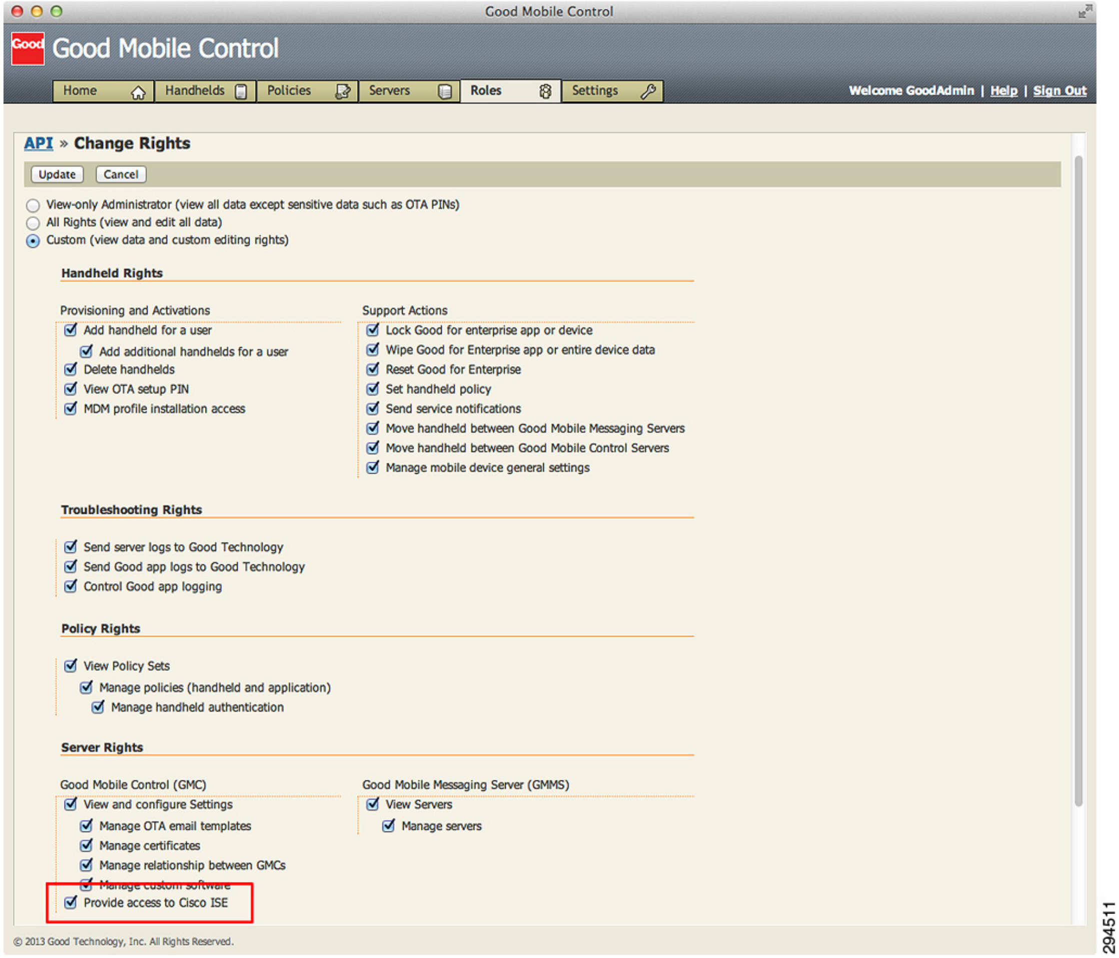
□	Name	Email	Domain	Type
☑	apiadmin		TRIADTME	User

1-1 of 1 First | Prev | Next | Last

Add Delete

294510

Figure 8 Assign API Access Rights to ISE Member Account



API » Change Rights

Update Cancel

○ View-only Administrator (view all data except sensitive data such as OTA PINs)
○ All Rights (view and edit all data)
● Custom (view data and custom editing rights)

Handheld Rights

Provisioning and Activations
- ☑ Add handheld for a user
  - ☑ Add additional handhelds for a user
- ☑ Delete handhelds
- ☑ View OTA setup PIN
- ☑ MDM profile installation access

Support Actions
- ☑ Lock Good for enterprise app or device
- ☑ Wipe Good for Enterprise app or entire device data
- ☑ Reset Good for Enterprise
- ☑ Set handheld policy
- ☑ Send service notifications
- ☑ Move handheld between Good Mobile Messaging Servers
- ☑ Move handheld between Good Mobile Control Servers
- ☑ Manage mobile device general settings

Troubleshooting Rights

- ☑ Send server logs to Good Technology
- ☑ Send Good app logs to Good Technology
- ☑ Control Good app logging

Policy Rights

- ☑ View Policy Sets
  - ☑ Manage policies (handheld and application)
    - ☑ Manage handheld authentication

Server Rights

Good Mobile Control (GMC)
- ☑ View and configure Settings
  - ☑ Manage OTA email templates
  - ☑ Manage certificates
  - ☑ Manage relationship between GMCs
  - ☑ Manage custom software
- ☑ Provide access to Cisco ISE

Good Mobile Messaging Server (GMMS)
- ☑ View Servers
  - ☑ Manage servers

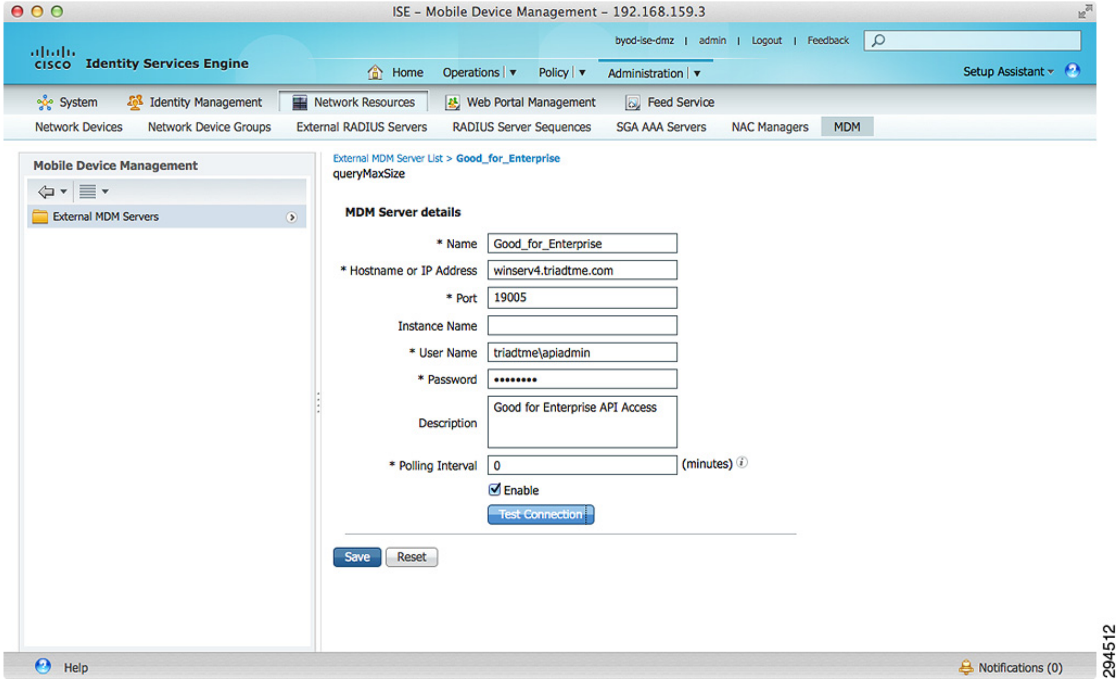
© 2013 Good Technology, Inc. All Rights Reserved.

Adding MDM Server to ISE

Once the Good for Enterprise server account has been defined with the proper access rights, ISE can be configured to use this account to query the MDM. ISE will contact the MDM to gather posture information about handlhelds or to issue device commands, such as corporate wipe or lock. The session is initiated from ISE towards the MDM server.

Figure 9 shows the server name and port number for the Good for Enterprise server to be the same as specified earlier to export the certificate. Inserting the Domain along with the User Name is critical to give ISE access to the Good for Enterprise APIs. The Instance Name field is used in multi-tenant deployments more commonly found when subscribing to a cloud service. The field is left blank for this deployment. The port should be configured for https port 19005.

Figure 9 *Configure the MDM API on ISE*



External MDM Server List > **Good_for_Enterprise**

queryMaxSize

MDM Server details

* Name: Good_for_Enterprise
* Hostname or IP Address: winserv4.triadtme.com
* Port: 19005
Instance Name:
* User Name: triadtme\apiadmin
* Password: ••••••••
Description: Good for Enterprise API Access
* Polling Interval: 0 (minutes)
☑ Enable

The polling interval specifies how often ISE will query the MDM for changes to device posture. Polling can be disabled by setting the value to 0 minutes. Polling can be used to periodically check the MDM compliance posture of an end station. If the device is found to be out of MDM compliance and the device is associated to the network, then ISE will issue a Change of Authorization (CoA), forcing the device to re-authenticate. Likely the device will need to remediate with the MDM, although this will depend on how the ISE policy is configured. Note that MDM compliance requirements are configured on the MDM and are independent of the policy configured on ISE. It is possible, although not practical, to set the polling interval even if the ISE policy does not consider the MDM_Compliant dictionary attribute.

The advantage of polling is that if a user takes the device out of MDM compliance, they will be forced to reauthorize that device. The shorter the window, the quicker ISE will discover the condition. There are some considerations to be aware of before setting this value. The MDM compliance posture could include a wide range of conditions not specific to network access. For example, the device administrator may want to know when an employee on a corporate device has exceeded 80% of the data plan to avoid any over usage charges. In this case, blocking network access based solely on this attribute would aggravate the MDM compliance condition and run counter the device administrator's intentions. In addition, the CoA will interrupt the user Wi-Fi session, possibly terminating real-time applications such as VoIP calls.

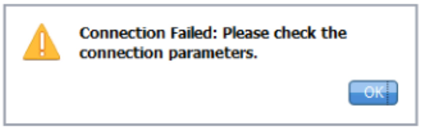
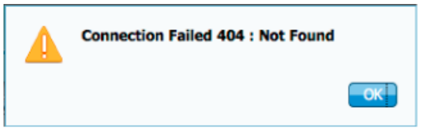
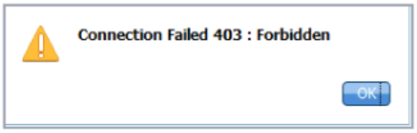
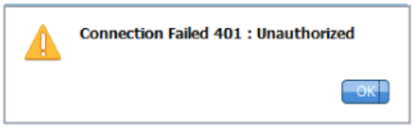
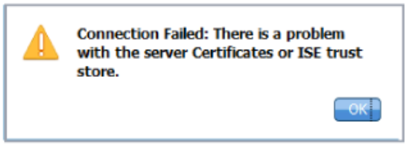
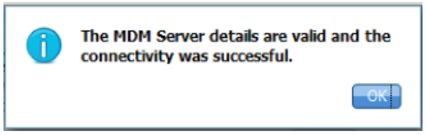
The polling interval is a global setting and cannot be set for specific users or asset classes. The recommendation is to leave the polling interval at 0 until a full understanding of the MDM's configuration is complete. If the polling interval is set, then it should match the device check-in period defined on the MDM. For example, if the MDM is configured such that devices will report their status every four hours, then ISE should be set to the same value and not less than half this value. Oversampling the device posture will create unnecessary loads on the MDM server and reduced battery life on the mobile devices. There are other considerations with respect to scan intervals. Changing MDM timers should be done only after consulting with Good for Enterprise's best practices.

The **Test Connection** button will attempt to log in to the API and is required prior to saving the settings with the MDM set to Enable. If the test does not complete successfully, the settings can still be saved, but the Enable box will be deselected and the MDM will not be active.

Verifying Connectivity to MDM

Some problems found while testing the connection to the MDM server. Table 1 shows some common messages generated when testing the connection between ISE and Goof for Enterprise. The last message shown below confirms a successful connection.

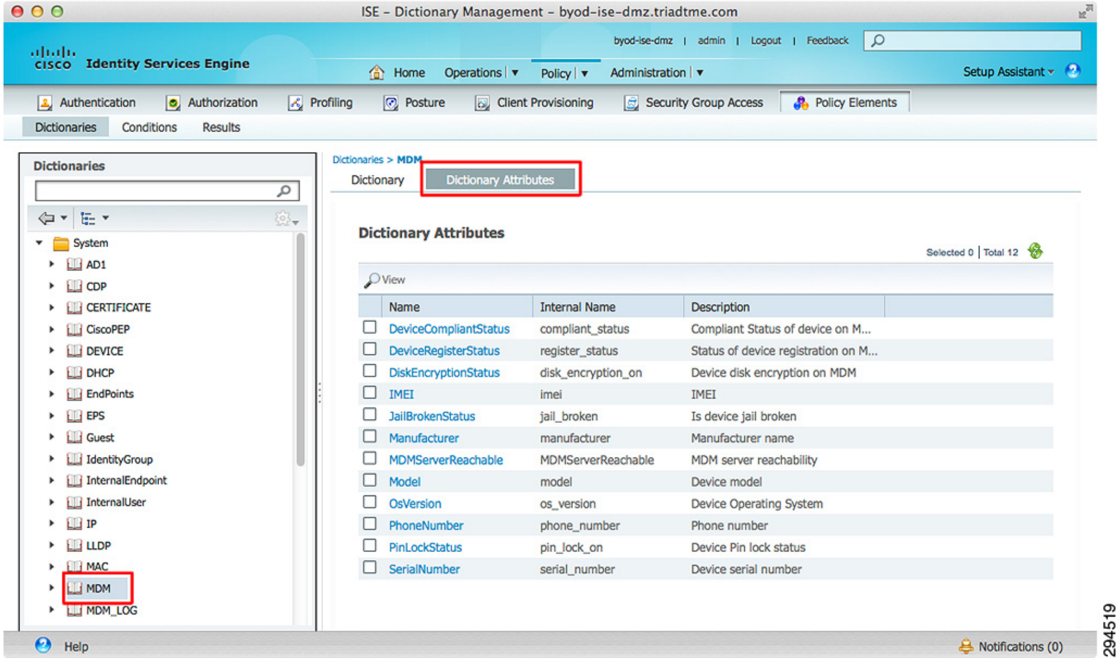
Table 1 Connection Messages

Message	Explanation
 Connection Failed: Please check the connection parameters.	A routing or firewall problem exists between the ISE located in the data center and the MDM located in either the DMZ or Cloud. The firewall's configuration should be checked to confirm HTTPS is allowed in this direction.
 Connection Failed 404 : Not Found	The most likely cause of an HTML 404 error code is that an instance was configured when it was not required or that the wrong instance has been configured.
 Connection Failed 403 : Forbidden	The user account setup on the Good for Enterprise server does not have the proper roles associated to it. Validate that the account being used by ISE is assigned the REST API MDM roles as shown above.
 Connection Failed 401 : Unauthorized	The user name or password is not correct for the account being used by ISE. Another less likely scenario is that the URL entered is a valid MDM site, but not the same site used to configure the MDM account above. Either of these could result in the Good for Enterprise server returning an HTML code 401 to ISE.
 Connection Failed: There is a problem with the server Certificates or ISE trust store.	ISE does not trust the certificate presented by the Good for Enterprise website. This indicates the certificate was not imported to the ISE certificate store as described above or the certificate has expired since it was imported.
 The MDM Server details are valid and the connectivity was successful.	The connection has successfully been tested. The administrator should also verify the MDM dictionary has been populated with attributes.

Reviewing MDM Dictionaries

When the Good for Enterprise MDM becomes active, ISE will retrieve a list of the supported dictionary attributes from the MDM. The dictionary attributes are shown in Figure 10.

Figure 10 Dictionary Attributes


ISE – Dictionary Management – byod-ise-dmz.triadtme.com
cisco Identity Services Engine
byod-ise-dmz | admin | Logout | Feedback
Home Operations ▾ Policy ▾ Administration ▾
Setup Assistant ▾
Authentication Authorization Profiling Posture Client Provisioning Security Group Access Policy Elements
Dictionaries Conditions Results
Dictionaries
System
AD1
CDP
CERTIFICATE
CiscoPEP
DEVICE
DHCP
EndPoints
EPS
Guest
IdentityGroup
InternalEndpoint
InternalUser
IP
LLDP
MAC
MDM
MDM_LOG
Dictionaries > MDM
Dictionary
Dictionary Attributes
Selected 0 | Total 12
View
Help
Notifications (0)
294519

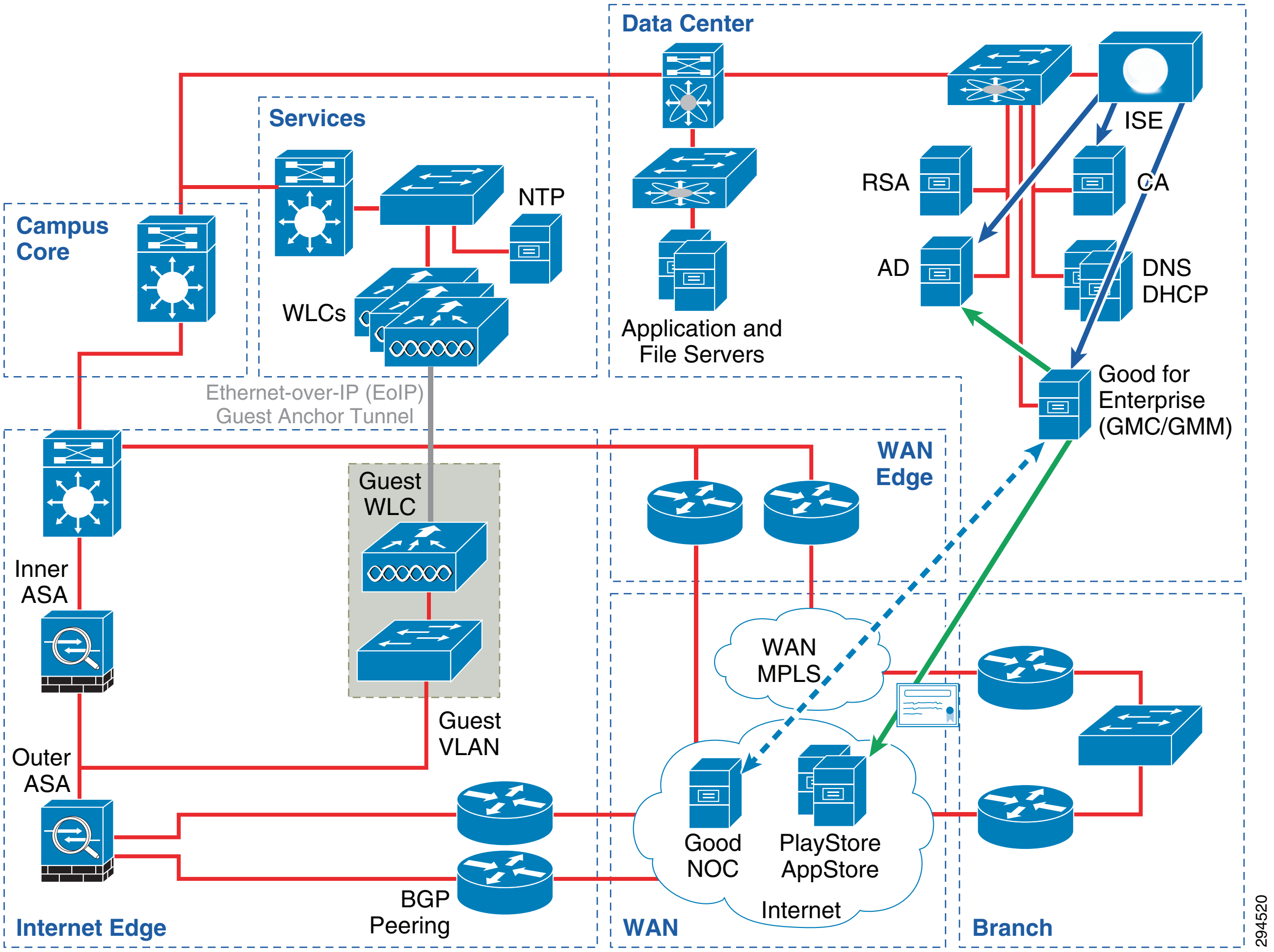
Dictionary Attributes

Name	Internal Name	Description
□ DeviceCompliantStatus	compliant_status	Compliant Status of device on M...
□ DeviceRegisterStatus	register_status	Status of device registration on M...
□ DiskEncryptionStatus	disk_encryption_on	Device disk encryption on MDM
□ IMEI	imei	IMEI
□ JailBrokenStatus	jail_broken	Is device jail broken
□ Manufacturer	manufacturer	Manufacturer name
□ MDMServerReachable	MDMServerReachable	MDM server reachability
□ Model	model	Device model
□ OsVersion	os_version	Device Operating System
□ PhoneNumber	phone_number	Phone number
□ PinLockStatus	pin_lock_on	Device Pin lock status
□ SerialNumber	serial_number	Device serial number

Enterprise Integration

Both ISE and the MDM must be integrated into a common Active Directory environment for account control, however Good for Enterprise does not participate in the Active Directory group structure with Cisco ISE. This means the Active Directory profiles created for ISE do not apply directly to the MDM configuration. Separate (but similar) policies should be created on the MDM. If a user is a member of the FULL_ACCESS Active Directory group, that membership and policy should be paralleled on the Good Mobile Control Server so the user account is treated consistently by both servers. For example, if the MDM installs an application on a device, then ISE should allow the application on the network for members of the users' AD group.

Figure 11 Typical Good for Enterprise On-Premise Deployment Model



Socket Requirements

The Good for Enterprise installation is fully documented by Good Technology in the Administrator's Guide located on the Good Technology Portal. Use the login/password credentials supplied with your Good Technology license purchase to access the information. Since Good for Enterprise is an on-premise deployment, the GMC and GMM server(s) are located in the customer's data center along with Cisco ISE. Good Technology does not recommend a DMZ deployment nor is it supported, as a number of outbound ports need to be opened to connect to your company's Microsoft Exchange server(s). The server will still need to reach the Apple Push Notification Service (APNS) and Google Cloud Messaging services over the public Internet as detailed in the Good for Enterprise Administrator's Guide.

There are also several flows that must be allowed between the various system components. Table 2 summarizes the required sessions (see the Good for Enterprise Administrator's Guide for more details).

Table 2 Common Socket Requirements

Source	Destination	TCP Port	Purpose	Comment
Good Mobile Messaging Server	Microsoft Exchange Server(s)	1433 (Database) 1352 (NRPC)	Good for Enterprise Messaging	
Good Mobile Control Server	Good Mobile Messaging Server	10009, 10010	GMC to GMM Communications	N/A if the GMC and GMM are installed on the same server
Administrator's Web Browser	Good Mobile Control Server (GMC)	8443	Good for Enterprise Administration	
Mobile Android Device	Google Cloud Messaging	5228, 5229, 5230 (outbound)	Google Cloud Messaging	
Mobile iOS Device	APNS	5223 (inbound + outbound)	Apple Push Notification	IP Range 17.0.0.0/8
Good Mobile Control and Good Mobile Messaging Servers	Good Portal (Good Technology Cloud)	80, 443	Server Monitoring via Good Technology Portal	IP Ranges 216.136.156.64/27 and 198.76.161.0/24
Good Mobile Control and Good Mobile Messaging Servers	Good Portal (Good Technology Cloud)	UDP 12000, TCP 15000	Used to pass outbound initiated traffic to Good once the Good client is installed on the handheld.	
Cisco ISE	Good Mobile Control Server	19005	MDM API Access	
Good Mobile Control Server	Good Mobile Messaging Server	19005	Web Services	
Good Mobile Messaging Server	Good Mobile Control Server	19009, 19010	Server Communications	

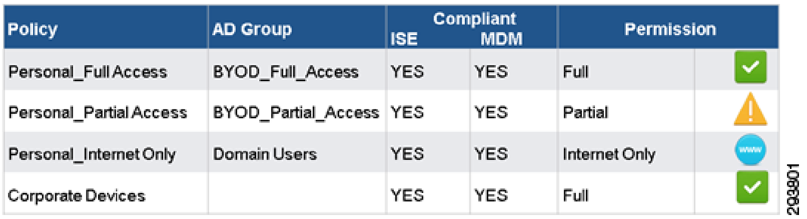
Active Directory/LDAP Integration

Integrating ISE and the MDM to a common directory is required for the overall system operation. One benefit is the ability to set a requirement that a user periodically change their directory password. If the MDM were using a local directory, it would be difficult to keep the accounts in synchronization. With a centralized user database structure, password management can be simplified.

Three possible AD groups are presented in the CVD to illustrate their usage—Domain Users, BYOD_Partial_Access, and BYOD_ Full_Access. ISE establishes the device's network access based on the associated user's membership.

Figure 12 shows the use cases presented in the CVD.

Figure 12 *CVD Use Policies*



Policy	AD Group	Compliant		Permission	
		ISE	MDM		
Personal_Full Access	BYOD_Full_Access	YES	YES	Full	✓
Personal_Partial Access	BYOD_Partial_Access	YES	YES	Partial	⚠
Personal_Internet Only	Domain Users	YES	YES	Internet Only	www
Corporate Devices		YES	YES	Full	✓

These groups should be paralleled as MDM Policies on the Good for Enterprise server such that members are joined to policies that complement their level of network access. Table 3 shows example policies that can be established and enforced based on the CVD use cases.

Table 3 *AD Groups and MDM Policies Based on CVD Cases*

Ownership	User Group	Corresponding MDM Policy	Restrictions
Employee-Owned Device	Domain Users	Domain Users	Internet Only, personal devices are not required to on-board with the MDM.
	BYOD_Partial_Access	BYOD_Partial_Access	Fairly restrictive policy that isolates corporate data into containers. Restrictions prevent users from disabling the policy.
	BYOD_Full_Access	BYOD_Full_Access	Trusted users are offered a slightly less restrictive policy. Corporate data is still isolated in containers.
Corporate-Owned Device	All Users classes	All Users classes	Very restrictive device policy disabling non-essential business functions such as the game center.

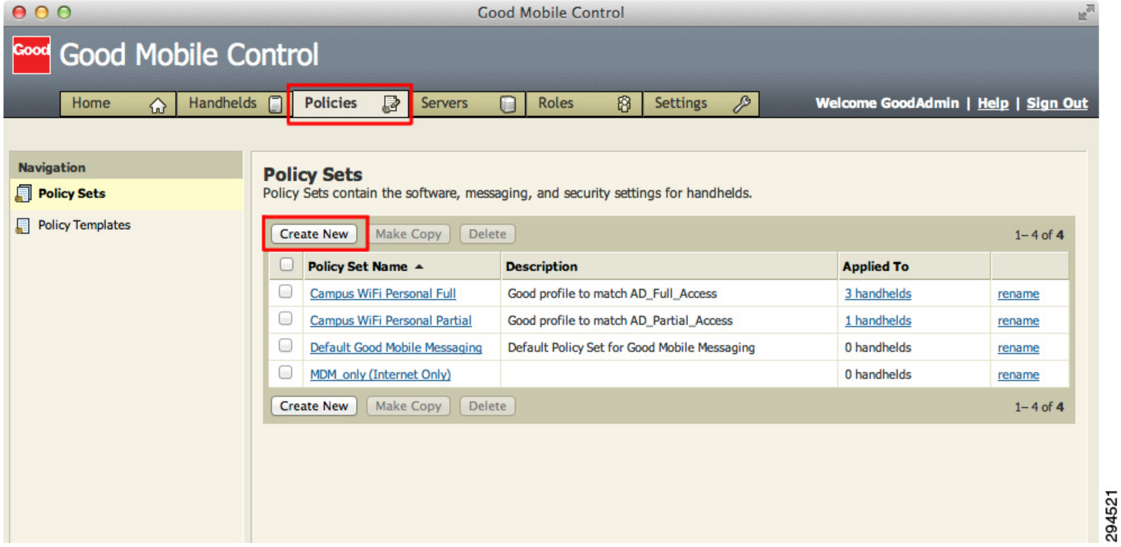
Domain Users is the default AD group. By definition, every user defined in the directory is a domain user. While it is possible to create a parallel group on the MDM, it is not needed for the default case. The CVD treats non-domain members as temporary guests. These guests are unlikely to need MDM management and likely represent a very small set of users (such as distinguished guests) that are handled as an exception. Consult the Good for Enterprise Administrator's Guide for details on setting up an MDM-Only device.

MDM policies and ISE AuthZ rules are fundamentally different with respect to AD Groups. ISE policy may include the AD group match as a condition for establishing a specific and single policy. Every device will be provisioned with basic security restrictions. ISE will check the device to ensure these restrictions are met before granting network access. These restrictions establish ISE compliance and are defined here as required PIN lock, encrypted storage, and non-jail broken or rooted devices.

MDM Policies

Access to the network through the Good for Enterprise MDM is controlled through specific policies linked to each user and device. By default, all handhelds are given a default policy defined by the system. System administrators can create policies tailored for each type of access and device ownership. Templates can also be created for major policy categories that system administrators encounter every day. Figure 13 and Figure 14 show how the GFE system administrator can create policies and customize permissions for each user group.

Figure 13 Create Custom MDM Policies for Each User Group



Policy Sets

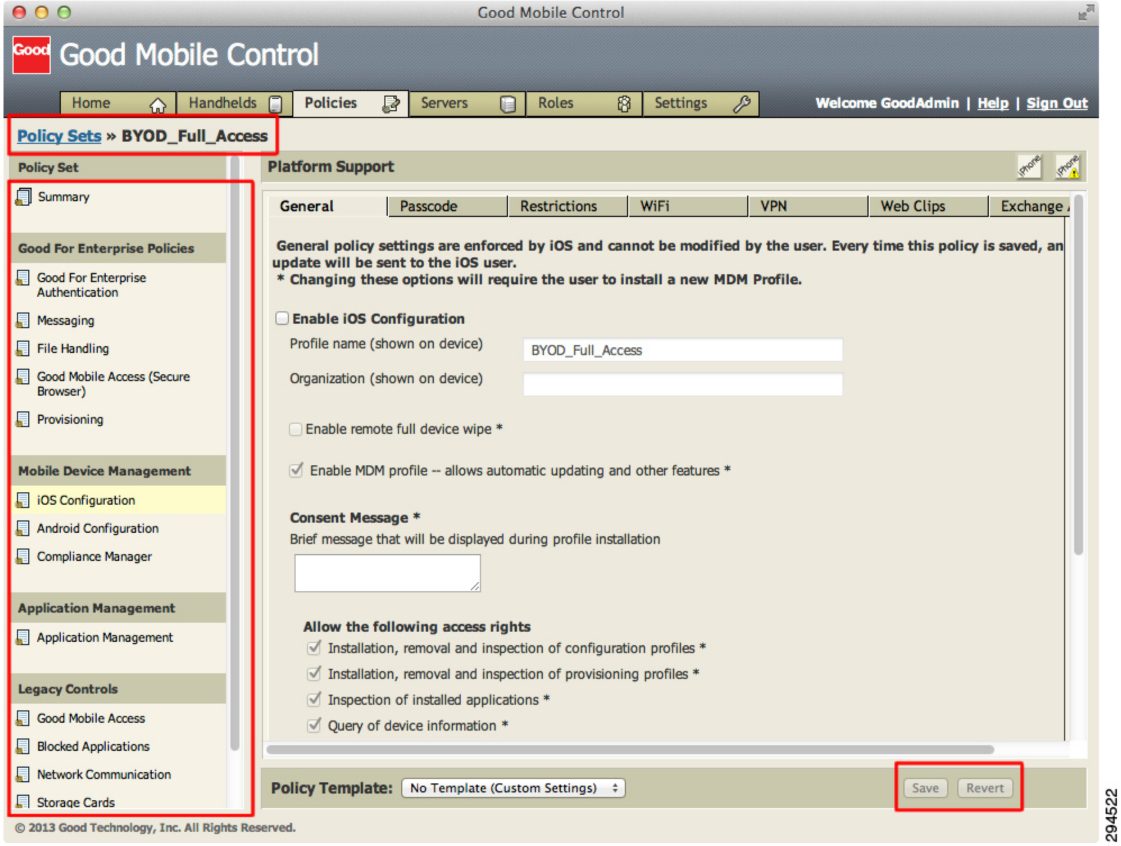
Policy Sets contain the software, messaging, and security settings for handhelds.

Create New | Make Copy | Delete — 1– 4 of 4

□	Policy Set Name ▲	Description	Applied To	
□	Campus WiFi Personal Full	Good profile to match AD_Full_Access	3 handhelds	rename
□	Campus WiFi Personal Partial	Good profile to match AD_Partial_Access	1 handhelds	rename
□	Default Good Mobile Messaging	Default Policy Set for Good Mobile Messaging	0 handhelds	rename
□	MDM_only (Internet Only)		0 handhelds	rename

Create New | Make Copy | Delete — 1– 4 of 4

Figure 14 Customize MDM Policy Features


Good Mobile Control

Home | Handhelds | Policies | Servers | Roles | Settings

Welcome GoodAdmin | Help | Sign Out

Policy Sets » BYOD_Full_Access

Policy Set
- Summary

Good For Enterprise Policies
- Good For Enterprise Authentication
- Messaging
- File Handling
- Good Mobile Access (Secure Browser)
- Provisioning

Mobile Device Management
- iOS Configuration
- Android Configuration
- Compliance Manager

Application Management
- Application Management

Legacy Controls
- Good Mobile Access
- Blocked Applications
- Network Communication
- Storage Cards

Platform Support

General | Passcode | Restrictions | WiFi | VPN | Web Clips | Exchange

General policy settings are enforced by iOS and cannot be modified by the user. Every time this policy is saved, an update will be sent to the iOS user.
* Changing these options will require the user to install a new MDM Profile.

☐ Enable iOS Configuration

Profile name (shown on device): BYOD_Full_Access

Organization (shown on device):

☐ Enable remote full device wipe *

☑ Enable MDM profile -- allows automatic updating and other features *

Consent Message *
Brief message that will be displayed during profile installation

Allow the following access rights
- ☑ Installation, removal and inspection of configuration profiles *
- ☑ Installation, removal and inspection of provisioning profiles *
- ☑ Inspection of installed applications *
- ☑ Query of device information *

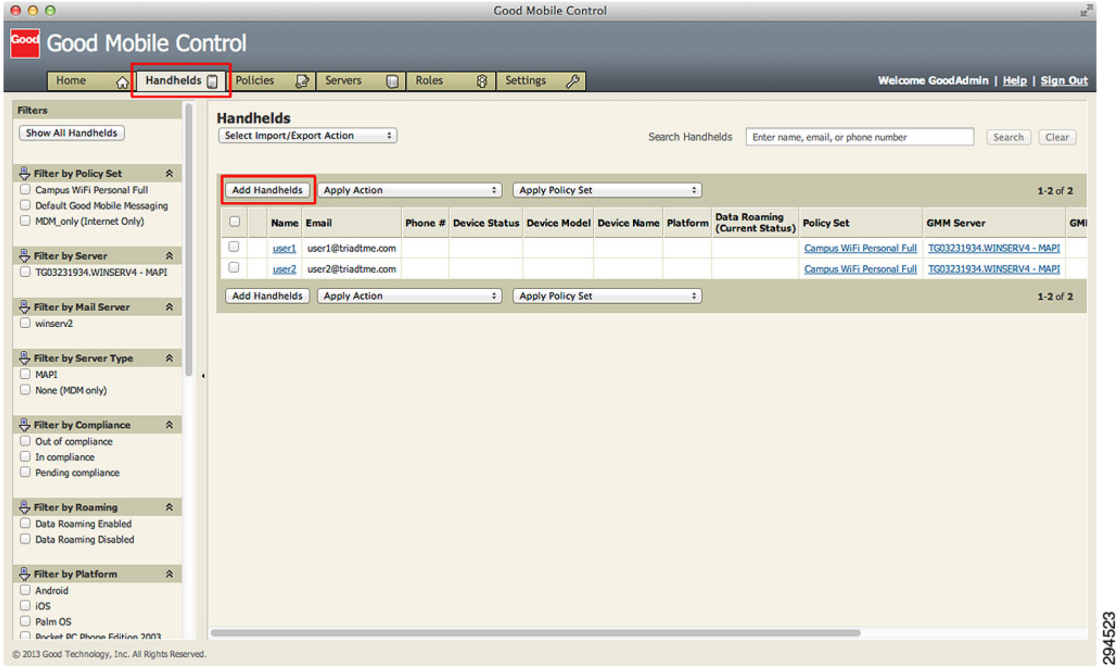
Policy Template: No Template (Custom Settings)

Save | Revert

© 2013 Good Technology, Inc. All Rights Reserved.

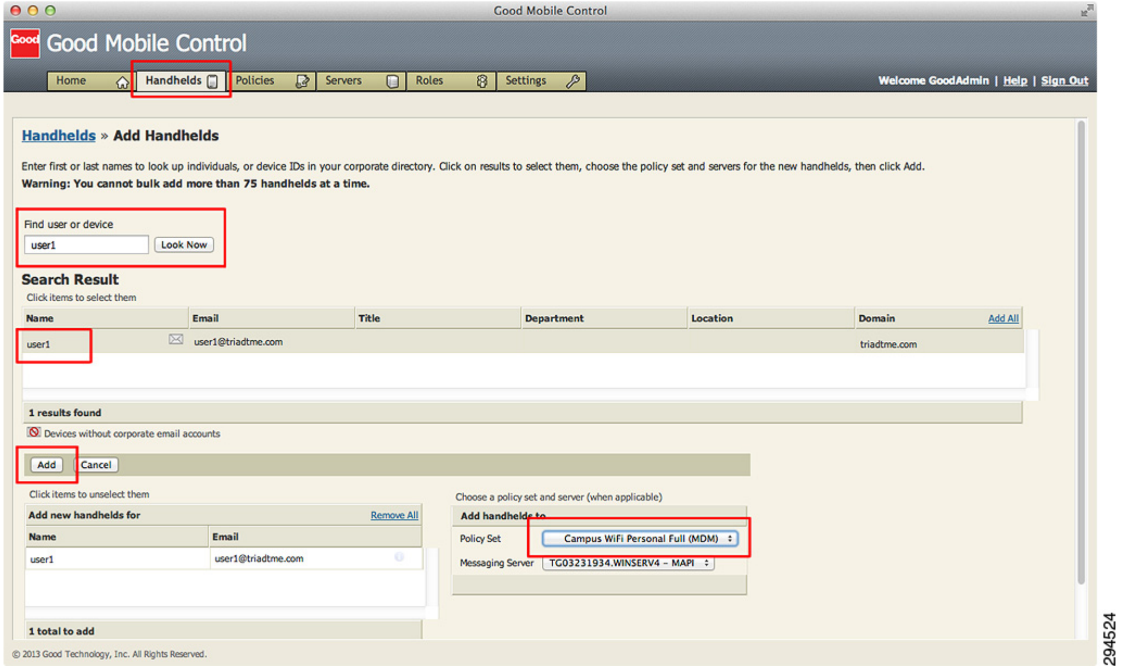
Once the proper and corresponding MDM policies are created, the system administrator can use the GMC to add handhelds in preparation for on-boarding. A separate instance must be added for each handheld. Figure 15 and Figure 16 show how to add handhelds one at a time. Good for Enterprise does allow devices to be bulk-imported into the system using a .CSV file and required parameters. More details can be found in the Good for Enterprise Administration Guide.

Figure 15 Adding Handhelds and Binding them to MDM Policies



□	Name	Email	Phone #	Device Status	Device Model	Device Name	Platform	Data Roaming (Current Status)	Policy Set	GMM Server	GMI
□	user1	user1@triadtme.com							Campus WiFi Personal Full	TG03231934.WINSERV4 - MAPI	
□	user2	user2@triadtme.com							Campus WiFi Personal Full	TG03231934.WINSERV4 - MAPI	

Figure 16 Adding Handhelds (Details)



Handhelds » Add Handhelds

Enter first or last names to look up individuals, or device IDs in your corporate directory. Click on results to select them, choose the policy set and servers for the new handhelds, then click Add.
Warning: You cannot bulk add more than 75 handhelds at a time.

Find user or device: user1

Search Result

Click items to select them

Name	Email	Title	Department	Location	Domain
user1	user1@triadtme.com				triadtme.com

1 results found

Devices without corporate email accounts

Click items to unselect them

Add new handhelds for

Name	Email
user1	user1@triadtme.com

1 total to add

Choose a policy set and server (when applicable)

Add handhelds to

Policy Set: Campus WiFi Personal Full (MDM)

Messaging Server: TG03231934.WINSERV4 – MAPI

When a handheld is added to the Good Mobile Control console, the device is joined to a specific user's account (maintained in the corporate AD server) and assigned a unique Over The Air (OTA) pin. This information, in the form of a Welcome Letter, is forwarded to the user's Exchange email account and is used during the on-boarding process. Once the device is on-boarded, the device is granted access based on the policy the MDM administrator has set. A user may have multiple devices, but each will have a unique OTA pin identifying it with the MDM. Devices may have differing access privileges depending on the MDM policy assigned to each.

It is important to note the difference between the on-boarding processes for ISE and the Good for Enterprise MDM. The CVD recommends using ISE authentication profiles to check for proper AD group membership during the on-boarding process. However since the MDM does not check AD membership, users must be careful to on-board the proper device with the proper pin and corresponding MDM policy. For instance, if a user wanted to on-board two new handheld devices (one for corporate access and one for personal), ISE would assign the device's network access based on an automated process. Since each device would use the same Exchange email account but would have a separate OTA pin, it is critical to use the proper credentials for the proper device so corporate versus personal integrity can be maintained.

Configuring the organization group with a default ownership allows employees the ability to on-board both corporate and personal devices. This minimizes the involvement of IT and associated support costs, yet still provides a MDM policy that distinguishes between ownership and users. IT will still need to populate the ISE whitelist with corporate MAC addresses.

Device Profiles

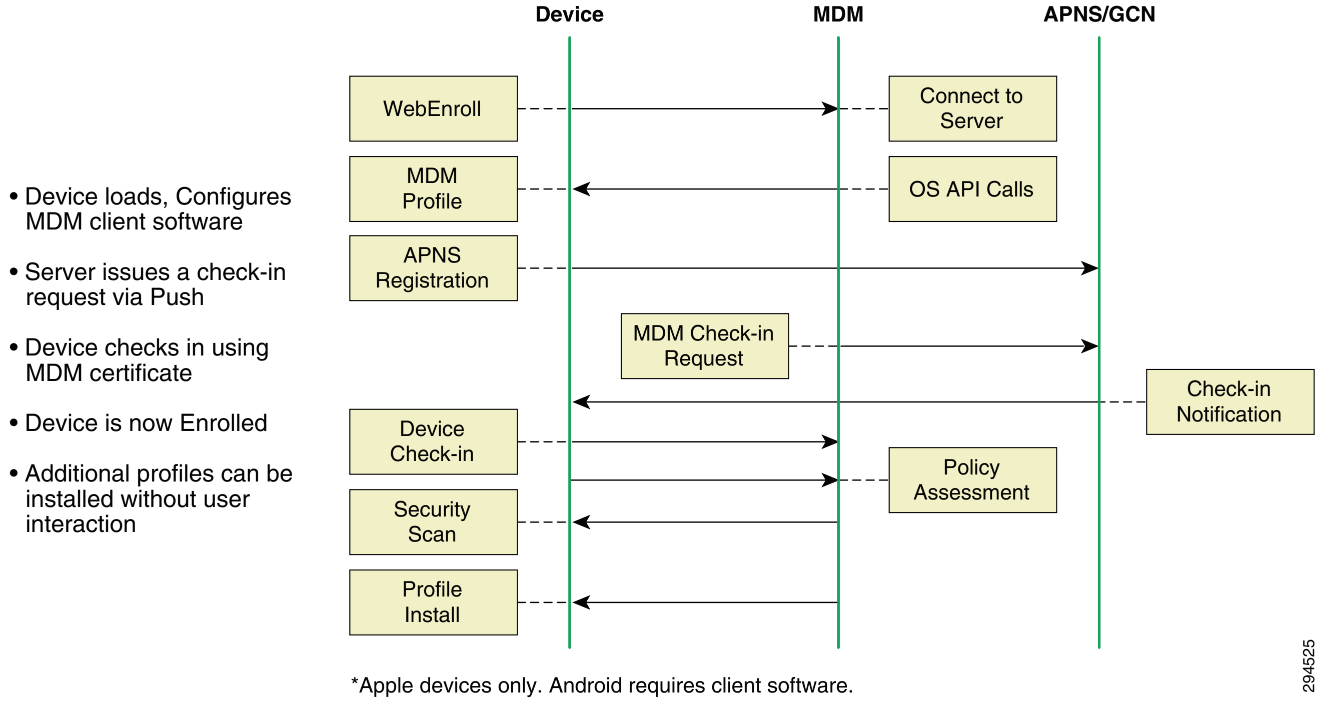
Apple and Android differ in how device management is implemented. Apple defines profiles that are an important concept of mobile device management. They are a foundational component of Apple's mobile device management protocol that is implemented by the operating system. This concept can be extended to application profiles, but as discussed here, they are found under the settings of the device. Each profile can contain one or more payloads. A payload has all the attributes needed to provision some aspect of built-in system functions, such as PIN lock. One special payload is the MDM payload that defines the MDM server as the device administrator. There can only be one MDM payload installed on any device. In iOS 5 and earlier, the profile containing the MDM payload cannot be locked and the user is free to delete it at any time. When this occurs, all other profiles installed by the MDM are also removed, essentially resulting in a corporate wipe. The MDM may lock any profile that it installed to prevent the user from removing them individually. The MDM is allowed to inspect other profiles such as the WiFi profile installed by ISE, but is not allowed to remove any profile that it did not install, including the WiFi as detailed in the BYOD CVD. Because multiple profiles can be installed on a device and profiles have payloads, it is possible to have a payload collision. Devices with multiple security payloads will install all the payloads by aggregating the most secure settings from each. In most other cases the first payload is installed and subsequent payloads are ignored or multiple payloads are accepted. For example, the device can have multiple VPNs provisioned, but only one can be named XYZ.

Note Starting in iOS6, Apple does allow the MDM payload to be locked if the user has not set a PIN lock.

Android devices generally implement device management functions through a specific set of APIs, most of which are manufacture or model specific. For example, Samsung uses their SAFE API, while HTC uses its One APIs.

Users that belong to Campus_WiFi_Personal_Full will see four profiles installed on their devices, two profiles installed by ISE and two from the MDM. The MDM server will install the MDM payload during the on-boarding process. After that profile has been installed, the device will be issued a check-in request via APNS or Google Cloud Messaging. When the device responds to the push notice, it will connect to the MDM where any additional profiles are installed. In our case, this includes at least the base restriction profile. Figure 17 shows the steps required of a device to enroll (on-board) with the MDM.

Figure 17 Enrollment Network Flows


Device
MDM
APNS/GCN
WebEnroll
Connect to Server
MDM Profile
OS API Calls
APNS Registration
MDM Check-in Request
Check-in Notification
Device Check-in
Policy Assessment
Security Scan
Profile Install
• Device loads, Configures MDM client software
• Server issues a check-in request via Push
• Device checks in using MDM certificate
• Device is now Enrolled
• Additional profiles can be installed without user interaction
*Apple devices only. Android requires client software.
294525

Mobile Client App

With Apple devices, some MDM functionality is implemented directly through the operating system and does not require a mobile device client application. However, advanced features do require a client running on the endpoint. In particular, jailbreak and rooted detection requires the MDM client. Because ISE depends on these features for policy enforcement, corporate devices and personal devices with partial or full access should include a profile that specifies the Good for Enterprise client as a mandatory application. Good for Enterprise client software is required to provide location information and to use push based notifications.

With Android devices, the client application is required to enroll with the server. Users are re-directed to Google Play during the enrollment process so that the GFE client application can be installed. With Apple devices, the client application can be installed by the user directly and used to on-board the device. Or the mobile client can be pushed to the device as a mandatory application during on-boarding.

In addition to providing specific device information, the client application offers the end users some useful information concerning the status of their devices. Users can determine if the device is successfully communicating with the server and whether the device is compliant. The mobile client also has activity logs that the user can view.

Device Ownership

One of the key components of BYOD is the mix of personal and corporate owned devices on the same network, and the ability to establish policy based on this attribute. This allows corporate devices to be distinguished from all other devices in the system and to be treated independently. For example, it is often recommend that support staff should not be allowed to issue a Full-Wipe or to track the location of personal devices. However corporate devices may get full wipes as a matter of normal operation and may be used to track the location of the holder as a normal part of the job. Having the ability to handle the information gathered from personal and corporate devices differently is important.

In this first release of the MDM dictionary, there is not a tight integration between assets classes defined on ISE and those defined on the MDM. The API does not support such a device attribute. Complicating matters somewhat is the key index used to identify a device: ISE uses the device's MAC address, which is unique across the network, whereas Good for Enterprise uses the device's UDID, which is globally unique. With GFE iOS Client v2.2, the UDID is no longer prompted for. Instead, Good Technology generates the random number as the method for uniquely identifying the device. This number starts with a "k".

ISE determines corporate devices through an identity group referred to as the Whitelist, which contains the MAC addresses of corporate assets. Discovering the MAC address of Android and Apple devices is typically a manual process. Apple lists the MAC on the Settings > General > About page.

User Experience

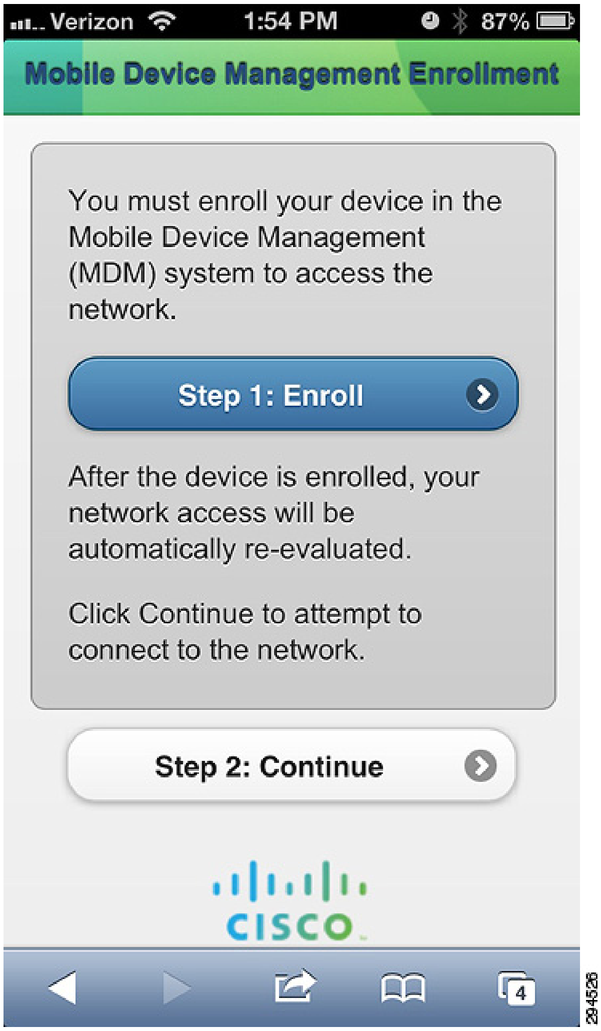
The fact that a handheld device is under management is for the most part seamless to the user. If a user is running the mobile client application as recommended for ISE compliance checks, then the user will have some additional information about their device that will be useful for troubleshooting. The initial user experience revolves around self-enrollment also known as on-boarding.

The user-completed device on-boarding workflow is set by the ISE policy. As presented in the CVD, the user will on-board with ISE before completing the process with the MDM. When a user first joins the BYOD_Employee SSID, ISE will check the device's MDM registration status through the MDM API. If the device is not registered, then a captive ACL is activated in the wireless LAN controller. This ACL will allow Internet access, but will capture any attempts to access corporate resources. A full explanation is provided in the CVD.

The device requires Internet access to complete the MDM on-boarding process including downloading the client application from either the Google Play Store or Apple's App Store. When the device is captured the user will be presented with a screen that includes two buttons as shown in Figure 18. The first button will redirect the client to the MDM registration page. The second button issues a CoA to force a re-evaluation of the AuthZ policy after MDM enrollment completes. The "Continue" button should be clicked after the GFE client is completely installed.

The following list show the steps to completing the on-boarding process with the Good for Enterprise MDM. Detailed descriptions are provided in the Good for Enterprise Administrator's Guide.

Figure 18 MDM Enrollment



Mobile Device Management Enrollment

You must enroll your device in the Mobile Device Management (MDM) system to access the network.

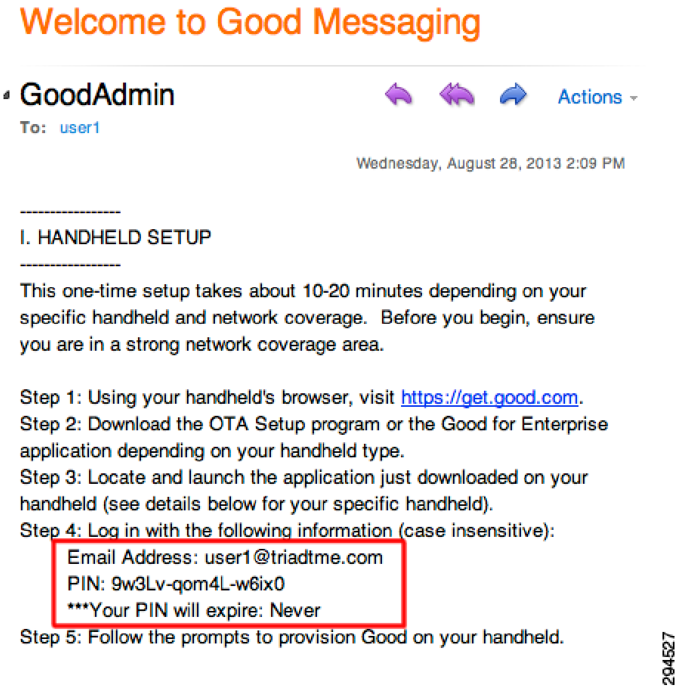
After the device is enrolled, your network access will be automatically re-evaluated.

Click Continue to attempt to connect to the network.

- The MDM system admin adds the user’s name to a Good Mobile Control policy granting the device network access and permissions. The policy should correspond to a similar access level that ISE will grant.
- The GMC sends an email message to the user containing the username (email address) and an Over The Air (OTA) Pin to allow the handheld to be on-boarded. The message can be edited, customized or suppressed by the system administrator.
- The user launches a web session to any URL inside the corporate firewall to trigger the GFE Client install. Because of the above-mentioned ACL, the browser is redirected to the ISE guest portal. When the user taps the “Enroll” button, they are redirected to either the Apple Apps Store or the Google Play Store where the Good for Enterprise App is offered.
- The user will see the app to be downloaded and will see a button marked “Free”. The “Free” button transforms into an Install button when tapped. The user taps the Install button and the GFE Client is downloaded and installed.
- Once the client is installed, the user taps the Open button to begin the on-boarding process.
- The user enters his or her device password when prompted and taps OK. A “loading” icon appears on the Home screen.

- With loading complete, the user can tap the new Good icon, then tap Start, and then accept the license information.
- When the user lands on the Good for Enterprise registration page, they will be asked for their registered email address and their device OTA pin, supplied in the Welcome Letter described above. An excerpt is shown in Figure 19. These credentials are bound to the user and their assigned policy. If the PIN has expired, the user must contact their administrator.

Figure 19 Excerpt from Good Messaging Welcome Email



Welcome to Good Messaging

GoodAdmin

To: user1

Wednesday, August 28, 2013 2:09 PM

I. HANDHELD SETUP

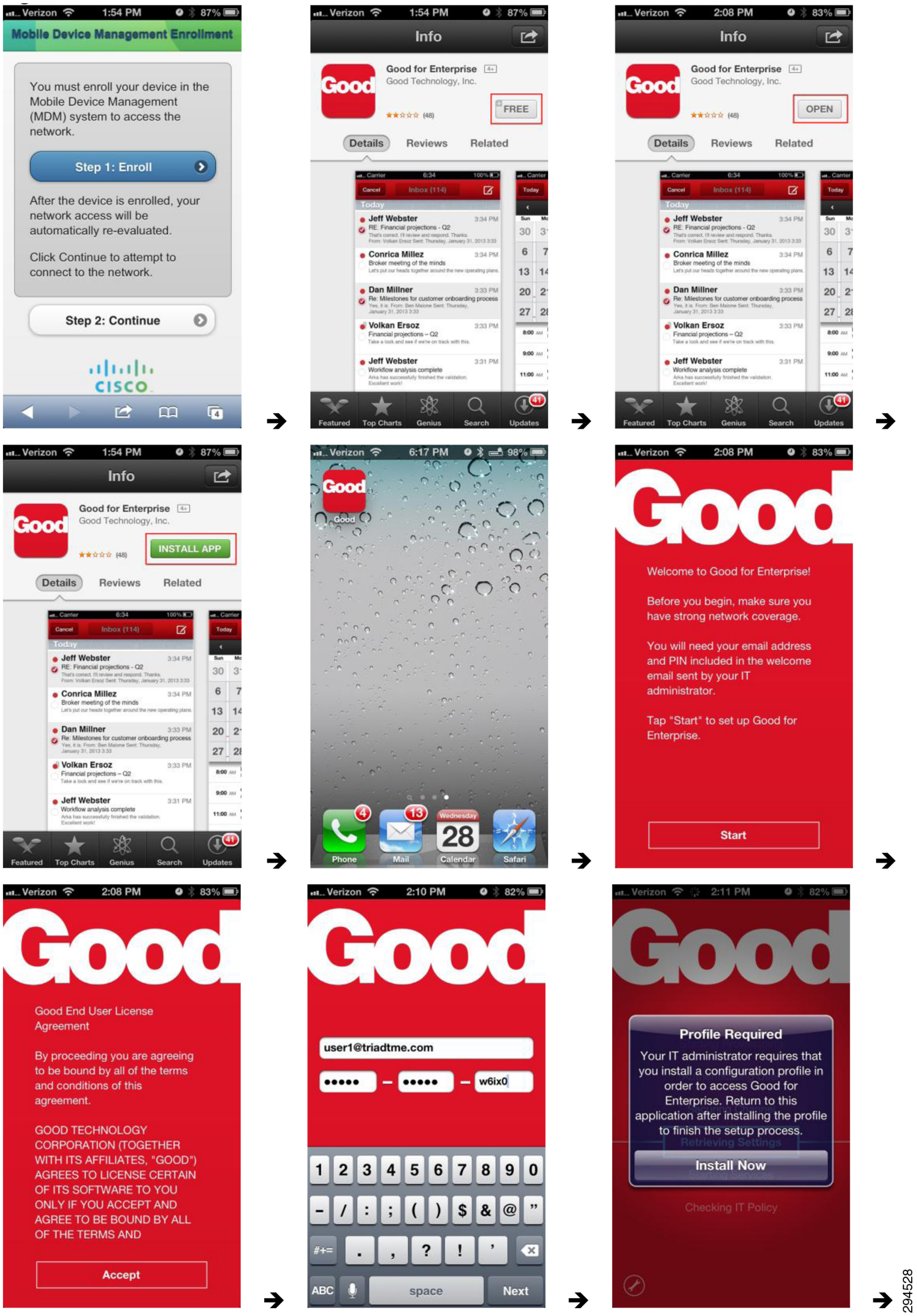
This one-time setup takes about 10-20 minutes depending on your specific handheld and network coverage. Before you begin, ensure you are in a strong network coverage area.

Step 1: Using your handheld's browser, visit https://get.good.com.
Step 2: Download the OTA Setup program or the Good for Enterprise application depending on your handheld type.
Step 3: Locate and launch the application just downloaded on your handheld (see details below for your specific handheld).
Step 4: Log in with the following information (case insensitive):
Email Address: user1@triadtme.com
PIN: 9w3Lv-qom4L-w6ix0
***Your PIN will expire: Never
Step 5: Follow the prompts to provision Good on your handheld.

- If you have set a policy requiring a password to access Good for Enterprise, the user will be prompted to enter and confirm a password. A message will display any restrictions that you have set on the password (minimum length, special characters, etc.).
- The user will be prompted to choose whether to delete the device's existing onboard native contacts, replacing them with the user's Outlook contacts, or whether to add the Outlook contacts to the existing contacts on the device. Whichever the user chooses, once setup is complete, changes to the Outlook and device contacts will be synchronized.
- Good for Enterprise now automatically synchronizes the device with information in the Exchange account. When synchronization is complete, the "Welcome to Good for Enterprise" message that was received will appear in the device email Inbox.

Based on the earlier discussion, corporate and personal devices should on-board with different policies. If the user successfully authenticates, a profile including the MDM payload and associated certificate is installed on the device and the user is notified that the on-boarding process is complete. The user is then returned to the redirect, where the "Continue" button is used to re-evaluate the devices MDM enrollment status that should now be set to "enrolled". Figure 20 and Figure 21 show the MDM enrollment process on an Apple iOS device.

Figure 20 MDM Enrollment on iOS



Mobile Device Management Enrollment

You must enroll your device in the Mobile Device Management (MDM) system to access the network.

Step 1: Enroll

After the device is enrolled, your network access will be automatically re-evaluated.

Click Continue to attempt to connect to the network.

Step 2: Continue

Welcome to Good for Enterprise!

Before you begin, make sure you have strong network coverage.

You will need your email address and PIN included in the welcome email sent by your IT administrator.

Tap "Start" to set up Good for Enterprise.

Start

Good End User License Agreement

By proceeding you are agreeing to be bound by all of the terms and conditions of this agreement.

GOOD TECHNOLOGY CORPORATION (TOGETHER WITH ITS AFFILIATES, "GOOD") AGREES TO LICENSE CERTAIN OF ITS SOFTWARE TO YOU ONLY IF YOU ACCEPT AND AGREE TO BE BOUND BY ALL OF THE TERMS AND

Accept

user1@triadtme.com

••••• – ••••• – w6ix0

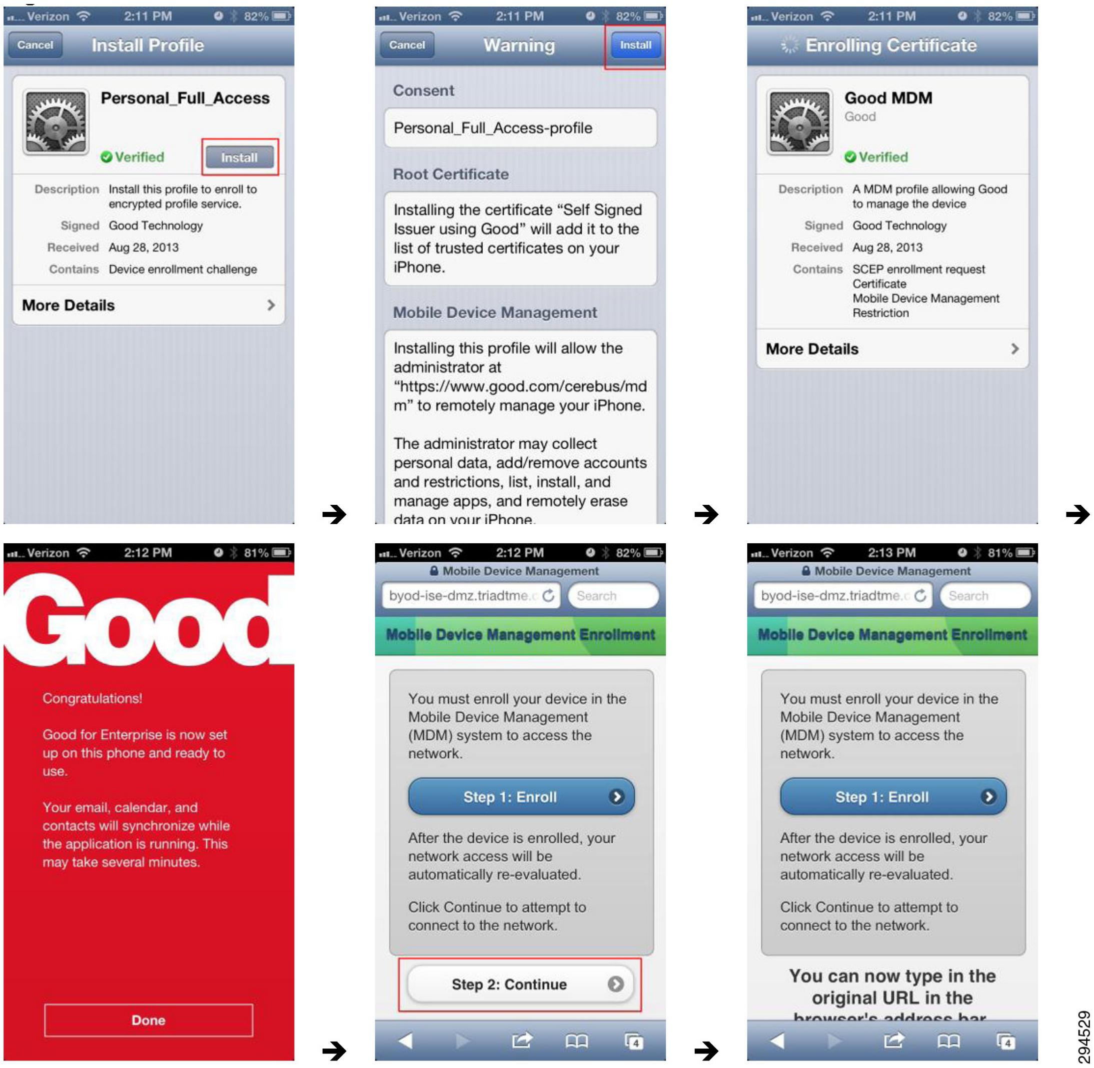
Profile Required

Your IT administrator requires that you install a configuration profile in order to access Good for Enterprise. Return to this application after installing the profile to finish the setup process.

Install Now

Checking IT Policy

Figure 21 MDM Enrollment Continued



Install Profile

Cancel

Personal_Full_Access

Verified

Install

Description: Install this profile to enroll to encrypted profile service.

Signed: Good Technology

Received: Aug 28, 2013

Contains: Device enrollment challenge

More Details

Warning

Cancel

Install

Consent

Personal_Full_Access-profile

Root Certificate

Installing the certificate "Self Signed Issuer using Good" will add it to the list of trusted certificates on your iPhone.

Mobile Device Management

Installing this profile will allow the administrator at "https://www.good.com/cerebus/mdm" to remotely manage your iPhone.

The administrator may collect personal data, add/remove accounts and restrictions, list, install, and manage apps, and remotely erase data on your iPhone.

Enrolling Certificate

Good MDM

Good

Verified

Description: A MDM profile allowing Good to manage the device

Signed: Good Technology

Received: Aug 28, 2013

Contains: SCEP enrollment request
Certificate
Mobile Device Management
Restriction

More Details

Good

Congratulations!

Good for Enterprise is now set up on this phone and ready to use.

Your email, calendar, and contacts will synchronize while the application is running. This may take several minutes.

Done

Mobile Device Management

byod-ise-dmz.triadtme.c

Mobile Device Management Enrollment

You must enroll your device in the Mobile Device Management (MDM) system to access the network.

Step 1: Enroll

After the device is enrolled, your network access will be automatically re-evaluated.

Click Continue to attempt to connect to the network.

Step 2: Continue

Mobile Device Management

byod-ise-dmz.triadtme.c

Mobile Device Management Enrollment

You must enroll your device in the Mobile Device Management (MDM) system to access the network.

Step 1: Enroll

After the device is enrolled, your network access will be automatically re-evaluated.

Click Continue to attempt to connect to the network.

You can now type in the original URL in the browser's address bar

Pass Code Complexity

The user may be required to configure a device lock (PIN lock) on their device during the on-boarding process if the device is not already configured with one. This requirement is configurable under each administrator-configured GMC policy. Once established, if you tighten passcode requirements, the user is prompted to define a new password and is given an hour to do so. The MDM administrator can chose the minimum password length and complexity for each GMC policy. The natural tendency is to require very strong passwords, however there may be unintended consequences. The PIN lock will need to be entered any time the employee wants to use their phone. While texting and driving is illegal in many locations, the PIN lock is also required to make phone calls. If the user is required to navigate through several keyboards to enter the PIN lock, the administrator may be creating an environment of risk taking. There may be legal implications outside the scope of this document that should be considered. The more likely scenario is that the user will opt-out of the BYOD network for their personal devices. Devices not managed could have no PIN lock at all and yet still contain corporate data that the employee improperly put on the device. A practical approach is to require a simple 4- digit PIN on personal mobile phones.

Corporate tablets can still be profiled with complex passcodes including special characters. This provides a balanced approach and will not discourage participation. Four-digit PINs or the last four digits of a SSN are used fairly often to provide some level of security.

Application Stores

The Good for Enterprise MDM can install public applications from either the App Store or the Play store or private applications that are uploaded to the GMC application store. Public applications can be part of a Volume Purchasing Program (VPP) where the enterprise can purchase licenses in bulk.

Corporate Data

Good for Enterprise and ISE can work closely together to create a fairly comprehensive approach to managing corporate data. This is generally known as data loss prevention (DLP). Data comes in two forms, data at-rest and data in-flight. Data at-rest is stored directly the mobile device and data in-flight is the movement of data.

Data at-Rest

Android and Apple handle stored data differently. Android has an open file structure that allows content to be shared between applications. Security is provided through file permissions. This creates a tight and integrated environment. Many Android devices also support external and removable storage in the form of SD Cards. Apple iOS creates a storage environment for each application. When an application is deleted, the partition holding that application's data is also removed. Because corporate data received via the GFE Client is housed in Good Technology's secure content container, all corporate data at-rest is considered secure.

Data in-Flight

Sharing data between applications is fairly common. Built-in system applications like Contacts can share their information. With Apple devices, the data is passed through the owning application. Apple iOS now provides privacy settings to control access to system data stores. The common thread with both Android and Apple is tight application integration. This functionality presents challenges when trying to contain data. Good for Enterprise Secure File Handling can help prevent data sharing.

Moving corporate data to and from the device is also a concern. The most common form is email attachments. Good for Enterprise email passes to and from the GFE client via an encrypted path between the handheld, the Good Technology Network Operations Center, and the corporate Exchange server thus protecting corporate email traffic.

Cloud storage services such as Dropbox and Skydrive are also a concern. ISE can deploy per-user ACLs through the Wireless LAN Controller to enforce an access policy at the network level for both corporate and personal devices. The system administrator can also use the GMC server to create a policy that blocks select applications.

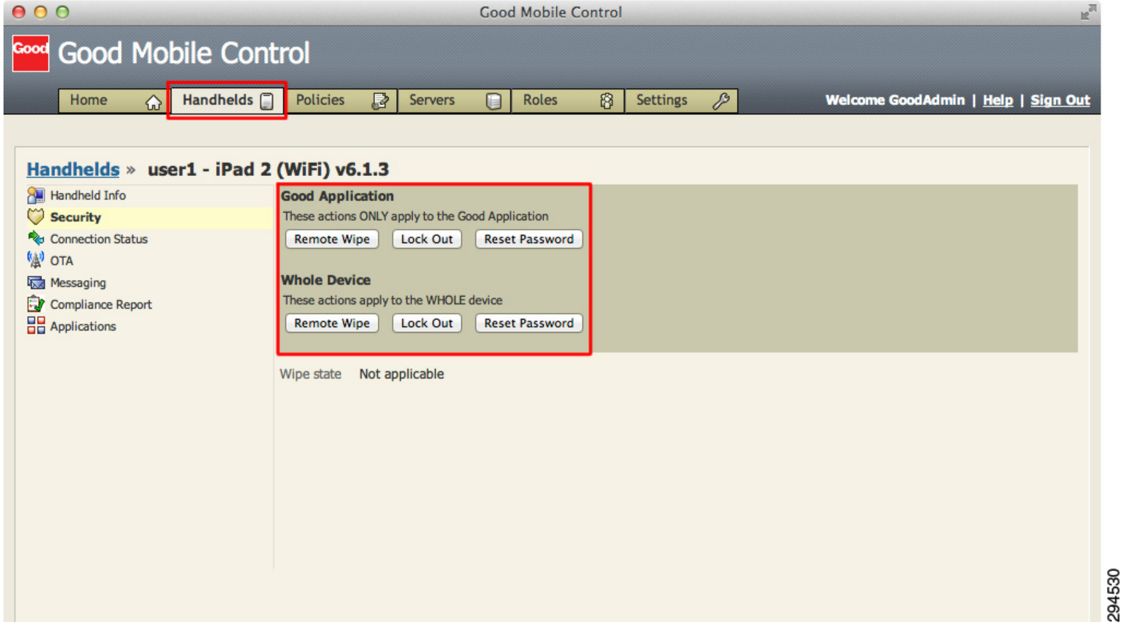
One final component of data security is the web browser. Good for Enterprise offers the option of using a secure web browser known as Good Mobile Access (GMA) to provide a browser on supported devices for use with your corporate Intranet. The browser is integrated to the Good Mobile Messaging Client on the device and provides seamless access to Intranet sites without need for an additional VPN. The secure browser uses Console policies to determine whether a web page should be loaded on the user's device or redirected to the native browser. The secure-browser policy lists all the Intranet domains, sub-domains, and embedded Internet domains that the administrator wants to make available on the mobile device.

Corporate Wipe

Both ISE and Good for Enterprise can remove corporate data from personal devices. Good for Enterprise calls this a device wipe, while ISE refers to it as a Corporate Wipe. Other common terms used are selective wipe or partial wipe. When ISE issues this command, it is forwarded to Good for Enterprise via an API call. The MDM can then remove corporate applications using privileges granted to the MDM Profile. When these complete, the MDM profile is removed, which will remove all the associated sub-profiles.

Good for Enterprise allows both a Good Application Wipe and a Whole Device wipe. Figure 22 shows the options for each handheld. With a Good Application Wipe, other device applications are left behind, however all MDM profiles and the GFE client are removed. Profiles not installed by the MDM are not deleted. This includes two profiles that were installed by ISE, one containing the CA certificate and the other containing the WiFi profile and user certificate. When an application is deleted, the associated data is also removed. If a built-in application was disabled by the MDM, it should be restored.

Figure 22 Good for Enterprise Good Application and Whole Device Wipe



Good Application

These actions ONLY apply to the Good Application

Whole Device

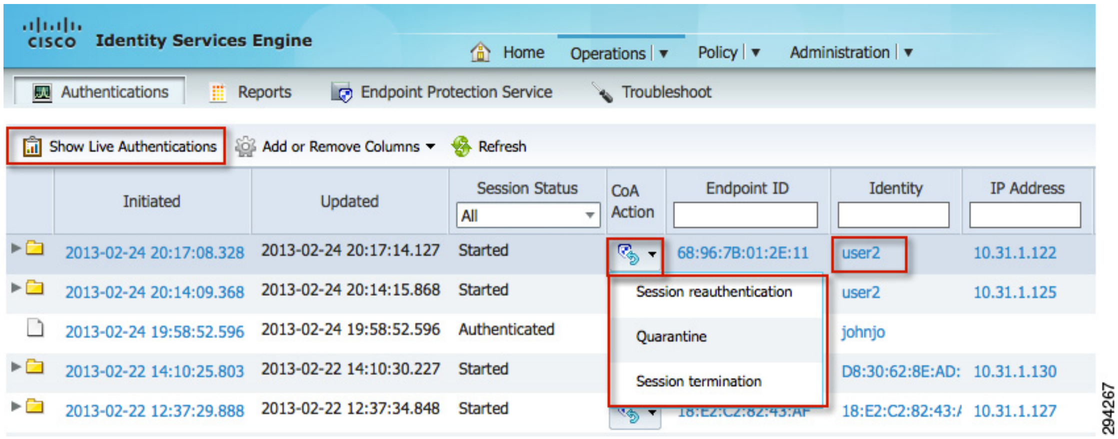
These actions apply to the WHOLE device

Wipe state Not applicable

The mobile client application can be removed. However there may be cases where the administrator would like to leave the Good for Enterprise client application on the device to allow an authenticated user to re-enroll the device. Corporate wipes by themselves do not blacklist the device from either the MDM or ISE. An ISE administrator, the MDM administrator, or the user from either the ISE My Devices Portal or the GMC control panel may issue a selective wipe. If a selective wipe is being issued as a result of an employee’s termination, then additional steps must be undertaken such as blacklisting the device with ISE and removing the user AD group memberships. This will prevent the user from re-enrolling the device. Optionally, the user certificate can be revoked on the CA server.

The final action is to force the user to re-authorize against ISE by disassociating them from the network. ISE release 1.2 now supports this directly from the Operations page, as shown in Figure 23. The device may immediately try to re-associate, but will match the blacklist, thereby denying the device network access. The user will not be able to self-enroll this particular device until IT has removed the MAC address from the blacklist.

Figure 23 Forced CoA from ISE



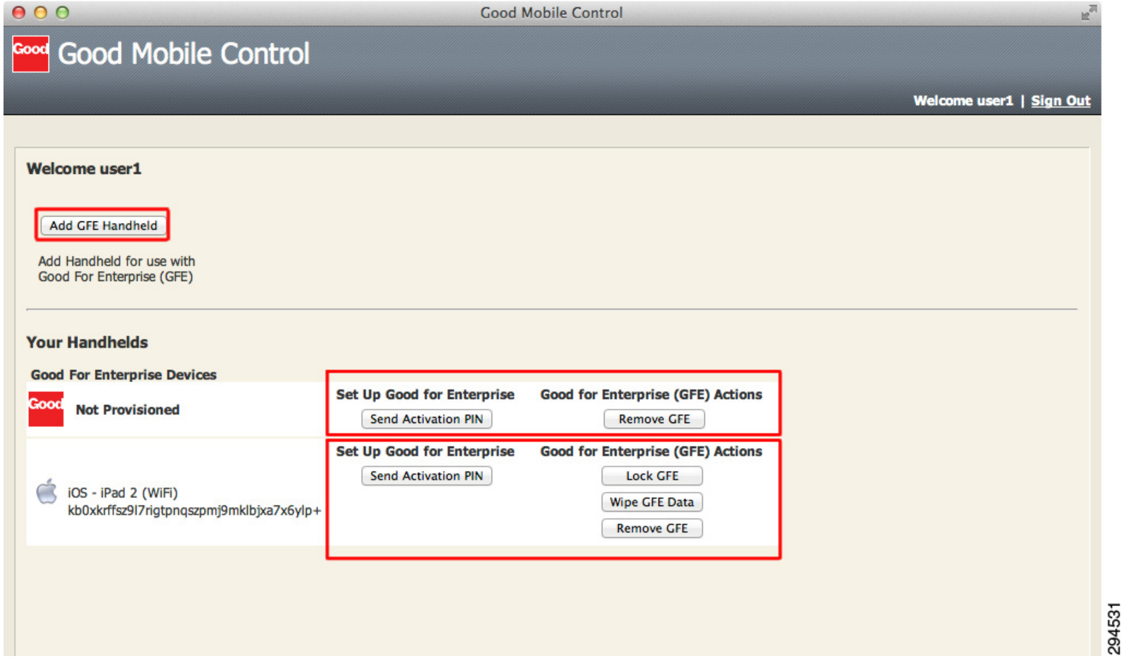
	Initiated	Updated	Session Status All	CoA Action	Endpoint ID	Identity	IP Address
	2013-02-24 20:17:08.328	2013-02-24 20:17:14.127	Started		68:96:7B:01:2E:11	user2	10.31.1.122
	2013-02-24 20:14:09.368	2013-02-24 20:14:15.868	Started			user2	10.31.1.125
	2013-02-24 19:58:52.596	2013-02-24 19:58:52.596	Authenticated			johnjo	
	2013-02-22 14:10:25.803	2013-02-22 14:10:30.227	Started			D8:30:62:8E:AD:	10.31.1.130
	2013-02-22 12:37:29.888	2013-02-22 12:37:34.848	Started		18:E2:C2:82:43:AF	18:E2:C2:82:43:/	10.31.1.127

Control Panel Access

Good for Enterprise allows a user to access the GFE Control Panel to manage their devices. User roles are defined to provide various level of functionality such as Send Activation Pin, Lock GFE, Wipe GFE Data or Remove the GFE Client completely. The user should browse to the GCM Console at https://<Good_for_Enterprise_Environment>:8443 and use the username and password supplied by the system administrator. It is important to note the user must explicitly specify a secure connection using port number 8443.

The system administrator must explicitly grant access to each user before they can access the console. A sample page with the default Self Service Policy enabled is shown in Figure 24. The Administrator guide has additional information on how to configure roles and allow user access.

Figure 24 Good for Enterprise Control Panel for Users



Welcome user1

Add Handheld for use with Good For Enterprise (GFE)

Your Handhelds

Good For Enterprise Devices

Not Provisioned

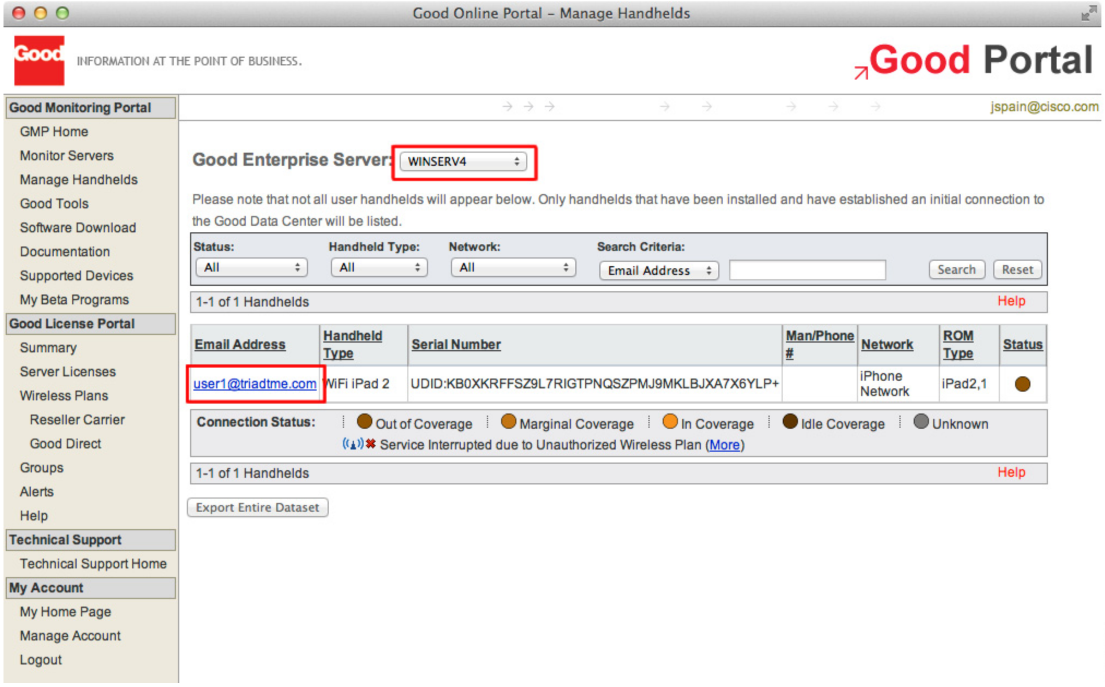
iOS - iPad 2 (WiFi)
kb0xkrffsz9l7rigtpnqszpmj9mklbjxa7x6ylp+

ISE also provides a My Devices Portal as detailed in the CVD. Currently the two sites are distinct and not cross- linked. Some of the functionality does overlap, such as the MDM actions, but users will likely want to Web Clip (bookmark) both locations.

Using the Good Monitoring Portal Dashboard

A system administrator can quickly list and check the connection status of user handhelds by logging in to the Good Monitoring Portal at: http://www.good.com/gmp. When you log in, the Good Monitoring Portal (GMP) home page is displayed showing the number of users/handhelds currently added to the server. To display a list of the users, together with information about their handhelds, click on the value displayed in the Users column. Figure 25 shows the details.

Figure 25 Good Monitoring Portal—Monitor Handhelds View



Good Online Portal – Manage Handhelds

Good Monitoring Portal
- GMP Home
- Monitor Servers
- Manage Handhelds
- Good Tools
- Software Download
- Documentation
- Supported Devices
- My Beta Programs

Good License Portal
- Summary
- Server Licenses
- Wireless Plans
  - Reseller Carrier
  - Good Direct
- Groups
- Alerts
- Help

Technical Support
- Technical Support Home

My Account
- My Home Page
- Manage Account
- Logout

Good Enterprise Server: WINSERV4

Please note that not all user handhelds will appear below. Only handhelds that have been installed and have established an initial connection to the Good Data Center will be listed.

Status: All Handheld Type: All Network: All Search Criteria: Email Address Search Reset

1-1 of 1 Handhelds Help

Email Address	Handheld Type	Serial Number	Man/Phone #	Network	ROM Type	Status
user1@triadtme.com	WiFi iPad 2	UDID:KB0XKRFFSZ9L7RIGTPNQSZPMJ9MKLBJXA7X6YLP+		iPhone Network	iPad2,1	●

Connection Status: ● Out of Coverage ● Marginal Coverage ● In Coverage ● Idle Coverage ● Unknown
✖ Service Interrupted due to Unauthorized Wireless Plan (More)

1-1 of 1 Handhelds Help

Export Entire Dataset

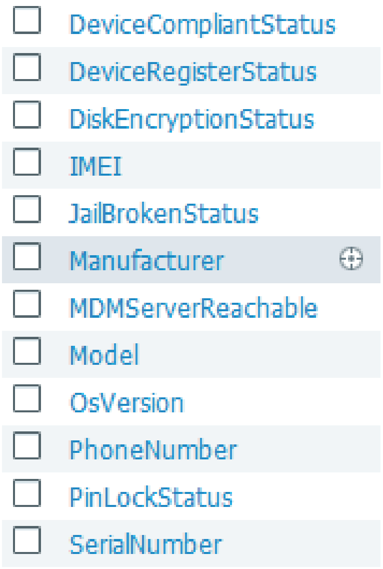
Verifying Device Compliance

ISE Compliance versus MDM Compliance

There are two compliance checks required of the device. The first is defined by policy configured on ISE. This is specific to network access control (NAC); the other is defined on the MDM and specific to mobile device policy (MDP). The use of an MDM to determine NAC is a fairly new concept, first supported in ISE 1.2. Mobile device compliance policy is an essential component of MDM and has context outside of network access. This is similar to NAC compliance prior to the integration of the MDM. Integrating the components together does not negate the need for two distinct compliance policies with meaning only within their respective context. The network administrator has to be careful not to confuse ISE compliance with MDM compliance with respect to NAC.

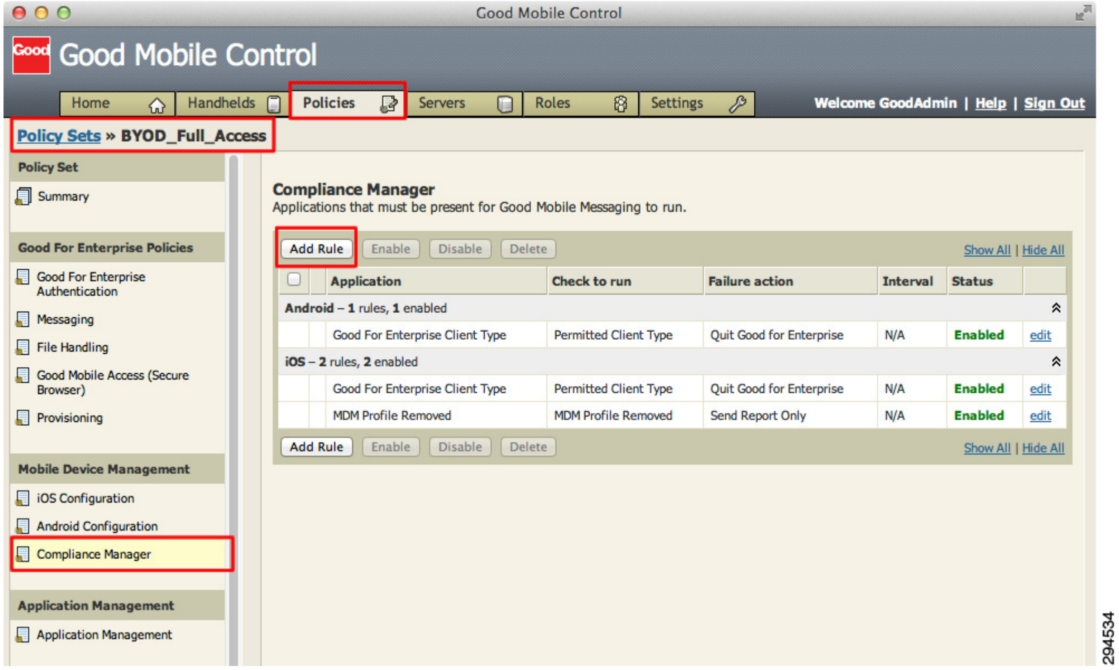
The attributes shown in Table 4 should help clarify the difference between compliance policies.

Table 4 *Compliance Attributes*

ISE Compliance Attributes	Good for Enterprise Compliance Attributes
 □ DeviceCompliantStatus □ DeviceRegisterStatus □ DiskEncryptionStatus □ IMEI □ JailBrokenStatus □ Manufacturer □ MDMServerReachable □ Model □ OsVersion □ PhoneNumber □ PinLockStatus □ SerialNumber	• Application Exceptions • Client Version Verification • Connectivity Verification • Hardware Model Verification • Jailbreak/Rooted Detection • MDM Profile Removed • OS Version Verification • Permitted Client Type

Good for Enterprise supports the built-in compliance attributes specified above as well as custom rules. Figure 26 details how to show existing rules and create new ones. Click Add Rule to add a new rule and then select Failure Action to choose the result of rule failure. The Good for Enterprise Administration Guide has complete details.

Figure 26 GMC Compliance Manager



Compliance Manager

Applications that must be present for Good Mobile Messaging to run.

☐	Application	Check to run	Failure action	Interval	Status	
Android – **1** rules, **1** enabled						
	Good For Enterprise Client Type	Permitted Client Type	Quit Good for Enterprise	N/A	**Enabled**	edit
iOS – **2** rules, **2** enabled						
	Good For Enterprise Client Type	Permitted Client Type	Quit Good for Enterprise	N/A	**Enabled**	edit
	MDM Profile Removed	MDM Profile Removed	Send Report Only	N/A	**Enabled**	edit

Device Compliance/Restrictions

Restrictions and compliance are distinct but related concepts. A user is not offered the option of not adhering to a restriction. If a PIN lock is required, the device will be locked until the user selects a PIN that meets the established complexity. If the camera has been disabled, the icon is removed and the user has no way to launch the camera application. Restrictions are policy elements that are enforced without exception. Compliance is when a device is operating outside of the established policy. Non-restrictive items that could cause compliance events are things such as the minimum OS version. The key point is that it is not possible to be non-compliant with a restriction. The exception is restrictions that include a grace period.

Device Scanning Intervals

The MDM client application can periodically scan the device. There are several different scans that run on different intervals. They also available as device queries and are:

- Device Information—General information about the device includes serial numbers, UDID, phone number, operating system, model, battery status, etc.
- Security—Includes encryption status, device compromised, data roaming, SIM card status, and the number of profiles installed but not active.
- Profiles—The installed profiles on the device, including those not installed by SAP Afaria.
- Apps—A complete inventory of all the applications installed on the device.
- Certificates—A list of the installed certificates on the device.

Scan information is available in device details screen. When a device periodically checks in with the MDM server, it will notify the server of the current scan results.

PINLockStatus

The PINLockStatus is available to the API and can be used by ISE to set a minimum requirement for network access. This is explained in the CVD. Typically PIN lock is set as a restriction. But there are some cases where the MDM can set compliance check against a restriction specific to PIN lock. It is possible to set a PIN lock with a grace period. During this time, the MDM can poll the device for the PIN lock status. When set, the triggered action could be the installation of additional profiles. By doing this, the device could be on-boarded with the MDM, but not granted full access until the user sets the password or the grace period expires.

There are some caveats to be aware of with respect to ISE creating a PIN lock requirement for network access. When users are issued instructions explaining the on-boarding process, they should be asked to set a PIN lock on their device prior to starting the on-boarding process rather than waiting for the forced PIN lock mid-way through the procedure. If the user does not follow this, they will possibly end up in a quarantine state. There are two issues at play:

- First, the MDM server does not get a triggered update when a user creates a PIN lock. Because it is set as a restriction, the user is required to enter one, but it will be some time before the server will becomes aware of the PIN lock.
- Second, the MDM on-boards by installing the MDM profile and certificate first. This secures the communications between the server and device. After this profile is installed on the device, the server will send a check-in request to the device.

Because the MDM payload is required to respond to check-in messages, this confirms the device is fully under management. On the initial check-in, the device is loaded with the remaining profiles, including the one containing the PIN lock restriction. Before this completes, the user may have clicked the continue button on the MDM redirect page, resulting in a CoA. This will re-authorize the device before the user has been prompted to enter a PIN lock and the user will end up being quarantined.

Jailbroken or Rooted devices

These are devices where the user has gained direct access to the operating system, bypassing the control imposed on the device by the service provider. Devices in this state are generally considered compromised and there has been some recent legislative action to prohibit users defeating locks imposed on the device by the providers. The BYOD CVD offers a policy that does not allow jailbroken or rooted devices on the network. This is based on the MDM API. The MDM server will require a mobile client app installed on the device to determine the root status of the device. There are a few limitations to consider. Usually the process of rooting a device requires the user to reinstall the operating system. There is a good chance the user will uninstall the Good for Enterprise mobile client at the same time. Without the software, the server cannot with certainty say the device is rooted, only that it has been compromised and is no longer under management. If the user also removes the MDM profile, then all profiles are also removed with it, effectively resulting in a selective wipe. As a reminder, the MDM profile may not be locked. At this point, the user may attempt to on-board the device in a rooted or jailbroken state. The server will not be able to assess this condition until the mobile client is reinstalled on the device and has had a chance to complete at least one device scan. There is a time delay between when a device is first compromised and when the MDM server will be first aware of a problem. There is no requirement in the MDM protocol that a device should contact the MDM when the MDM payload is removed. The server is left to poll for the condition periodically. This delay can carry forth into ISE policy because ISE can only respond to the attributes as they are returned by the MDM.

RegisterStatus

When a device is being on-boarded, ISE will check the RegisterStatus attribute of the device via an API call to the MDM. If the device is not registered, the user is redirected to the Good for Enterprise enrollment page. Obtaining a status of registered with the MDM means that the device is known to the MDM and that an MDM payload and the associated certificate is on the device, and that the device has responded to at least one check-in request issued through APNS or GCM. A register status does not guarantee that all the profiles have been pushed to the device. Instead it indicates that the profile containing the MDM payload has been installed and that the device has responded to the initial check-in request. It is possible for profiles to be withheld until a posture assessment has been completed and reported back to the server. This could result in a registered device that is not equipped with the full set of intended restrictions.

Managing Lost/Stolen Devices

Corporate and personal devices require specific responses when reported lost or stolen. Personal devices reported as stolen should undergo an enterprise wipe to remove all corporate data. The device can be restored if later found by the user. The admin may also choose to blacklist the device on the network depending on the situation, forcing the user to call support to regain access.

Corporate devices have some more flexibility with respect to providing location information. If this information is available, then the administrator may have some options. They could choose to:

- Reassign the device to a secured location group. This group effectively removes all corporate applications and data, provisions lock-down profiles—effectively rendering the device useless—and leaves the device under management, such that forensic data is available in the event the enterprise would pursue legal options.
- Blacklist the device in ISE to prevent corporate access. Also issue an Enterprise Wipe command to the device to remove all corporate data. This also removes the MDM profile. The device will become unmanaged, lifting all operational restrictions on the device including the ability to locate the device.
- Blacklist the device in ISE to prevent corporate access. Also issue a Full Wipe to the device to remove all information and return it to the factory default configuration. The carrier will need to be involved to prevent the now factory fresh device from having a resale value.

The exact response an enterprise would take in the event of a stolen device should not be public knowledge, especially when a full wipe is issued since the response could be an incentive to some criminals.

Application Distribution

Applications can be marked as required or optional. Required applications are usually automatically pushed to the device. Applications can be from the public application store or developed in-house. Apple and Google both offer a volume purchasing program if paid applications are distributed. In house, iOS applications can be customized with application profiles. Application management will be explored in future releases of this document. Readers are encouraged to view the Good for Enterprise Administrator’s Guide for additional information.

Cisco Applications (Jabber, etc.)

Cisco offers a wide range of mobile business applications for both increased productive and security. Table 5 shows some popular applications.

Table 5 Popular Cisco Mobile Applications

	AnyConnect—AnyConnect is a security application for improved VPN access, including on-demand domain-based split tunneling.
	WebEx—WebEx is a productive application to allow mobile users to connect to online meetings. The application allows content sharing, video sharing, and VoIP or cellular audio.
	Jabber—Jabber is a productivity application that integrates IP telephony, chat, and video conferencing using Cisco Call managers.

Conclusion

The integration of the network policy enforced by Cisco ISE and device policy offered by the Good for Enterprise MDM offers a new paradigm for BYOD deployments where security and productivity are not competing objectives.

Disclaimer

The Good for Enterprise configurations shown in this document should not be considered validated design guidance with respect to how the Good for Enterprise MDM should be configured and deployed. They are provided as a working example that details how the case studies explored in the CVD can be carried forward to the MDM in an effort to provide a fully integrated and complementary policy across both platforms. This in turn will result in a comprehensive solution where the network and mobile devices are in pursuit of a common business objective. Good for Enterprise is the only source for recommendations and best practices as it applies to their products and offerings.