

Good™ Mobile Messaging
Good™ Mobile Control
for Microsoft™ Exchange®

Wireless Enterprise Messaging and Data Access System

Quick Installation Guide

Good for Enterprise

Legal Notice

This document, as well as all accompanying documents for this product, is published by Visto Corporation dba Good Technology ("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.

Patents, Legal Information & Trademarks

©Copyright 2012. All rights reserved. Good Technology, Good, the Good logo, Good for Enterprise, Good For You, and Good Mobile Messaging, are either trademarks or registered trademarks of Good. All third-party trademarks, trade names, or service marks may be claimed as the property of their respective owners and are used only to refer to the goods or services identified by those third-party marks. Good's technology is protected by U.S. Patents 6,085,192; 5,968,131; 6,023,708; 5,961,590; 6,131,116; 6,151,606; 6,233,341; 6,131,096, 6,708,221 and 6,766,454 along with numerous other U.S. and foreign patents and applications pending.

Good Technology, Inc.
430 N. Mary Avenue, Suite 200
Sunnyvale, CA 94085

Be Good. Be Safe.
Please do not use while driving or engaged in any other activity that requires your full attention.

Contents

1	Quick Installation	1
	Prerequisites	1
	Pre-installation (Exchange 2003)	14
	Pre-Installation (Exchange 2007)	17
	Pre-Installation (Exchange 2010)	19
	Installing Good for Enterprise	27
	Setting Up the Handheld	28

1 Quick Installation

Welcome to Good for Enterprise, the behind-the-firewall, wireless corporate email and data system from Good Technology, Inc.

Good for Enterprise installation is simple and straightforward. An experienced Microsoft® Exchange® administrator should be able to complete the process in a few hours. No special wireless knowledge is required to perform the installation.

This chapter outlines the installation process. Chapter 2 provides an overview of the Good for Enterprise system. Chapters 3 through 6 provide detailed installation instructions, should you need them.

This *Quick Installation Guide* outlines the installation process. The *Good Mobile Messaging Administrator's Guide* provides an overview of the Good Messaging system and detailed installation instructions, should you need them.

Prerequisites

You will be creating a Good for Enterprise user account (named *GoodAdmin* in this guide) and a *GoodAdmin* Exchange mailbox. Then you will be installing:

Quick Installation

- A Good Mobile Control (GMC) Server, which provides facilities for managing Good for Enterprise users and their devices. You'll install this server first.

If you're upgrading, you can just use your current Good Mobile account.

- Good Mobile Messaging (GMM) Servers, which synchronize user devices with their Exchange accounts.

Ensure that the Good Mobile Messaging Server and Good Mobile Control Server host machines, and your Exchange server, conform to the following prerequisites. Good Mobile Messaging Server and Good Mobile Control Server can run on the same host machine, but cannot run on the same host machine as Microsoft Exchange Server®. For environments serving more than 1,000 devices, we recommend installing the Good Mobile Control Server on a separate host machine. The Good Mobile Messaging Server should be close to the Exchange Servers it communicates with (low latency, good bandwidth). The Good Mobile Control Server should be close to its SQL database.

Good Mobile Messaging Server minimum host system requirements:

- Hard drive space free for each Good Mobile Messaging Server:
 - 400MB system installation
 - 10GB logs
 - 40MB/device cache (leave room for growth)
- 32-bit: Dual-core Intel® Xeon® processor (2GHz or greater), 4GB RAM, Windows 2003.
- 64-bit: Intel Pentium IV quad-core processor (2GHz or greater), 8GB RAM, Windows 2008 R2 SP1.

For scalability information, refer to "Scalability" on page 7.

If a virtual machine session is used for Good Messaging, the free drive space and RAM requirements also apply.

- Good for Enterprise is an I/O intensive application; consider this fact when deciding which other applications are to run on the same host machine.

Good Mobile Messaging Server is supported as a Guest on VMware ESX 3.0.1, 3.5, 4.0, and 4.1 (using vSphere 4). Good Mobile Control is supported as a Guest on VMware ESX 3.5, 4.0, and 4.1. If Good Mobile Control is installed in the same Guest as another Good product, then VMware ESX 3.5, 4.0, or 4.1 is required. Good Mobile Messaging Server and Good Mobile Control are supported as Guests on a Windows 2008 64-bit Standard and Enterprise SP2 and R2 64 Bit Hyper-V Host.

- Required minimum LAN speed for the Good Mobile Messaging Servers: 100Mb/s. Note: When configuring Good Mobile Messaging Servers to connect with an Exchange server, the speed of the network connection must be a sustained minimum rate of at least 100Mb/s. Slower network connections between Exchange and Good Mobile Messaging Servers will cause increased message latency.
- Microsoft Outlook® must **not** be installed on the Good Mobile Messaging Server or Good Mobile Control Server host machines. Uninstall Outlook if it is present.
- Installing Good Mobile Messaging Server on a Microsoft Exchange server machine is not supported. Installing Good Mobile Messaging Server on a domain controller is not supported.

Good Mobile Control Server minimum host requirements:

- Hard drive space free for each Good Mobile Control Server:
 - 300MB system installation
 - 250MB logs
 - 38KB/device SQL server database

These space requirements do not include those for Good Mobile Messaging Server if it is on the same machine.

Quick Installation

- Dual-core Intel® Xeon® processor (2GHz or greater), 1.5GB RAM; for increased number of users: Intel Pentium IV dual processor (2GHz or greater), 2GB RAM
- A single Good Mobile Control Server can handle up to 10,000 users spread over multiple Good Mobile Messaging Servers.
- Microsoft Internet Explorer 7/8/9, Firefox 3.5/8/9/10, and Google Chrome 10/11 are supported.

Good Mobile Messaging Server and Good Mobile Control Server requirements:

- Note that during Server startup, significantly more processing occurs than during runtime. If the Messaging Server cache is located on VM disk or SAN rather than on a physical disk, the processing will be somewhat slower and will result in measurably more latency during startup.
- Good Mobile Control Server requires Windows 2003 with Service Pack 2, or Windows 64-bit 2008 Standard and Enterprise with Service Pack 2 or R2 SP1 64-bit. Windows 2000 is not supported.
- Good Mobile Messaging Servers must have access to the Microsoft Exchange Server that will manage user mailboxes (Microsoft 2003/2007/2010).
- Both the Good Mobile Messaging Server and Good Mobile Control Server host machines must have Internet access. They should be able to connect to http port 443 (secure https). To check this, use a browser on the host machine to connect to a secure remote location. If you'll be using a proxy server, you'll enter the necessary information for that server during the installation process (refer to the Administrator's Guide).

If you limit outbound HTTP and HTTPS on your firewall, you should open outbound ports 80 and 443 for IP ranges 216.136.156.64/27 and 198.76.161.0/24 for Good for Enterprise to work properly. (Version 5 required that you open outbound ports 80 and 443 for IP address 198.76.161.28 for Good for Enterprise to work properly. Version 6 requires, in addition, IP address

198.76.161.29 for use by Good Mobile Control.) Do not put the Good Mobile Messaging Server and Good Mobile Control Server in the DMZ zone or block any LAN ports. The Good Mobile Messaging Server and operating system calls have many port dependencies for interfacing with mail servers and AD, especially TCP 1433 (Database) and 1352 (NRPC).

Outbound network hostnames for Good Operations Center:

- www.good.com HTTPS 443 216.136.156.64/27
- upl01.good.com HTTPS 443 216.136.156.64/27
- xml28.good.com HTTPS 443 198.76.161.0/24
- xml29.good.com HTTPS 443 198.76.161.0/24
- xml30.good.com HTTPS 443 198.76.161.0/24
- gti01.good.com HTTPS 443 198.76.161.0/24

The Windows firewall is not supported for use with Good Mobile Control. Note that in Windows 2008, the Windows firewall is turned on by default. If currently on, turn off the firewall in Windows 2003 or 2008.

Good does not recommend a DMZ deployment nor is it supported, as a number of outbound ports need to be opened to connect to the Microsoft Exchange server

- Good Mobile Control Server requires port 19005 to be open for communication with Good Mobile Messaging Server and for web services. Good Mobile Messaging Server requires ports 10009 and 10010 to be open for communication with Good Mobile Control Server and other uses.
- In order to receive new message notifications while using the Good client for iOS devices on wifi networks, the following IP range and port need to be open:

TCP port 5223 incoming/outgoing

The firewall needs to accept traffic from 17.0.0.0/8 port 5223. This is the external IP range of the Apple Push Notification Service

Quick Installation

servers, which provide the message notifications for the Good email service on the iOS devices.

- The host machine should not have an MSDE or SQL Server installed on it, unless you choose to create a database on an existing Microsoft SQL 2005 or 2008 Server for use with Good for Enterprise.

To uninstall SQL Server if present, refer to Chapter 10 of the *Good Mobile Messaging Administrator's Guide*.

- Port 135 must be open for TCP connections from the Good Mobile Messaging Server to all Exchange Servers for enabled Good for Enterprise users. The Good Mobile Messaging Server will test connectivity to an Exchange Server by opening a TCP socket to port 135 before starting up users. If the Good Mobile Messaging Server fails to connect it will not allow users on that Exchange Server to start sending messages to their mobile device. This check is used as a health check in the event an Exchange Server is down and not able to handle requests.
- Before installing Good Mobile Messaging Servers and Good Mobile Control Servers, ensure that the host machines' time and date are set to your network's correct time and date. Otherwise, errors such as a Security Alert regarding a problem with the site's security certificate may occur.
- To activate the S/MIME secure-email feature in the Good Mobile Control Console, all installed Servers must be version 5.0 or higher.
- For native Microsoft Exchange 2003 and 2007 without the requisite hotfix, MAPI/CDO must be installed using Exchange System Manager. For pure Exchange 2003/2007 environments with the hotfix, the MAPI/CDO download from Microsoft can be used. For mixed Exchange 2003/2007/2010 environments or pure Exchange 2010 environments, the MAPI/CDO download from Microsoft must be used. **MAPI/CDO is required on all Good Mobile Messaging Server machines.** The Exchange MAPICDO version for this release must be 6.5.8211.0 or higher. All earlier versions should use 6.5.8190.0. **If you move the mailbox from an Exchange**

2007 server (or older) to an Exchange 2010 server (“Moving the GoodAdmin Mailbox” on page 304), you must reapply all necessary permissions and throttling policies as described below.

MAPI 6.5.8244.0 - <http://www.microsoft.com/download/en/details.aspx?id=1004>

- Good Mobile Messaging Server requires Microsoft .NET Framework 3.5 Service Pack 1.

Good Mobile Control SQL, .NET Framework, and Console requirements (links subject to change) (note these requirements if you plan to use an SQL server of your own; otherwise, Good Mobile Control will install SQL Express for you. SQL Express supports up to 4GB databases only.):

- Microsoft SQL Server 2005 Express Edition Service Pack 3:
<http://www.microsoft.com/downloads/details.aspx?familyid=3181842A-4090-4431-ACDD-9A1C832E65A6&displaylang=en>
<http://www.microsoft.com/sql/editions/express/sysreqs.msp>
- Microsoft SQL Server Management Studio Express Service Pack 2:
<http://www.microsoft.com/downloads/details.aspx?FamilyID=6053c6f8-82c8-479c-b25b-9aca13141c9e&DisplayLang=en#Requirements>
- Microsoft .NET Framework 2.0 Service Pack 1 (x86):
<http://www.microsoft.com/downloads/details.aspx?familyid=79BC3B77-E02C-4AD3-AACF-A7633F706BA5&displaylang=en#Requirements>

Scalability

Exchange Good Mobile Messaging Server has been certified to handle 1,050 users while accommodating HTML and GMA Secure Browser traffic. This performance was attained on the following server configurations:

Quick Installation

32-bit version

- Good Mobile Messaging Server build 6.3.1.20
- Windows 2003 SP2
- 4GB of RAM

64-bit version

- Good Mobile Messaging Server build 6.3.1.24
- Windows 2008 R2 SP1
- 8GB of RAM, quad-core processor

This assumes that 20% of users are currently actively using GMA Secure Browser and 100% are using the HTML email feature. This assumes a mix of 25% Windows Mobile/Android devices and 75% iOS devices.

Note that these are the minimum requirements to attain this performance. If you are running older configurations, do not scale to this number; remain at the users/server guideline that was communicated to you upon sale.

A single Good Mobile Control Server can handle up to 10,000 users spread over multiple Good Mobile Messaging Servers.

Preparing for SQL Server Use

Good Mobile Control requires access to a Microsoft SQL server. You can use an existing Enterprise or Standard Microsoft SQL Server 2005 SP3 and SP4, 2008 SP2 and R2, or 2008 ENT, or SQL server instance available within the organization. Good Mobile Control Server can connect to a remote SQL server/instance. If you don't have an SQL server that you want to use, a (non-remote) server will be installed along with the Good Mobile Control.

Note: SQL Server 2005 Cluster and SQL Server 2008 SP2 and R2 Cluster are supported.

SQL instance and database: An instance is an SQL installation, one per host. An instance can contain multiple databases.

Good for Enterprise requires ~38KB/device of SQL Server database space.

There is no transactional load. This is the size of the MDF file. The LDF file should be set to auto truncate at 10MB.

Multiple Good Mobile Control Servers can share an SQL instance but must use separate databases within that instance. If two Good Mobile Control servers attach to the same database, data loss may occur. An SQL instance is defined as a copy of SQL running on a computer.

Some knowledge of SQL installation, configuration, and maintenance will be useful if you plan to use an existing database.

You'll need the name of the service account you will use to run the Good Mobile Control service.

SQL Servers enforce their own authentication and authorization. If you encounter an SQL error during the installation process, you'll need to confirm that your SQL configuration information was entered correctly. If you will be using your own previously installed SQL Server instance, gather the following information in advance. You'll be required to provide it during Good Mobile Control Server installation.

- The fully qualified machine name of your SQL Server instance
- Method of connection to your existing SQL Server instance (static port, named instance (dynamic port), or connected to it as the default instance)
 - If static port, the port number
 - If named instance, the instance name

Quick Installation

- Authentication mode used to connect to your SQL Server instance (Windows authentication/SQL Server authentication)
 - If Windows authentication, the service account name entered above must already have a login to SQL Server, or, if not, add a login for the service account name to your SQL Server instance, granting it at least the Server-Level Role of “dbcreator.”
 - If SQL Server authentication, the SQL Server login name you use to connect to SQL Server with, and the password for this SQL Server login. You will be prompted for the login and password during the Good Mobile Control installation. The SQL Server login must be a member of the “dbcreator” security role. If not, add the login to the dbcreator security role so that the Good Mobile Control install can create its own database and table within the SQL Server instance.
- Whether your existing database is local or remote, ensure that TCP/IP is enabled for “Local and Remote connections” on your SQL Server instance.

Remote SQL

To use remote access, the IT administrator should configure the remote SQL server to accept the necessary connections from Good Mobile Control Server. This includes but is not limited to:

- Allowing connections via TCP/IP
- Allowing connections via a preconfigured port
- Opening any necessary port in any firewall between Good Mobile Control Server and the SQL server
- Creating or obtaining a valid SQL Server user name and password to connect to the remote SQL server during installation or the ability to log in as admin "sa."

We recommend testing remote database SQL server connectivity before beginning an installation.

Related articles from Microsoft:

- To Configure using TCP/IP - <http://support.microsoft.com/kb/914277>
- To configure using static Port - <http://support.microsoft.com/kb/823938>
- Installing SQL Server 2005 SP3 (complete process) - Installing SQL Server 2005 SP4 (complete process) - <http://www.microsoft.com/download/en/details.aspx?id=184>
- SQL Server Installation (SQL Server 2008 R2) - <http://msdn.microsoft.com/en-us/library/bb500469.aspx>

Microsoft Exchange configuration requirements

Microsoft Exchange configuration requirements:

- Exchange 2003 requires a host with a 32-bit OS; Exchange 2007 and 2010 require a host with a 64-bit OS. (Note that Good software can be installed on a Win2008 64-bit host regardless of which versions of Exchange are being used.)
- Every Good for Enterprise user account must be set up with an SMTP address (the standard Microsoft Exchange configuration).

The domain containing the Good for Enterprise account (*GoodAdmin*) must be trusted by the following domains: every domain containing one or more Exchange servers with mailboxes for Good for Enterprise device users; the domain containing the Exchange server where the GoodAdmin mailbox itself is located. Subject to this restriction, all Windows architectures are supported. To test, you can use the `manageprofile` command-line tool, installed with Good for Enterprise, on the Good Mobile Messaging Server host machines to open user mailboxes in each domain in question.

The tool is explained in Chapter 8 of the *Good Mobile Messaging Administrator's Guide*.

- MAPI Access is required for all Good for Enterprise users. Exchange 2003 SP2 introduced a way to turn MAPI Access off that

The following tables show the operating-system and Exchange software required on the Server and Console host machines.

Operating System

Good Mobile Messaging Server and Good Mobile Control Server

Windows 2008 Server[®] Standard and Enterprise SP2 and R2 SP1 64-bit (English (US)),* Windows 2003 Server[®] (English (US)) SP2, or Windows 2000 Server[®] (English (US)) with SP4 (Good Messaging Server only. Good Mobile Control Server not supported on Windows 2000).

Good Mobile Messaging Server is supported as a Guest on VMware ESX 3.0.1, 3.5, 4.0, and 4.1. Good Mobile Control is supported as a Guest on VMware ESX 3.5, 4.0, or 4.1. If Good Mobile Control is installed in the same Guest as another Good product, then VMware ESX 3.5, 4.0 or 4.1 is required. Good Mobile Messaging Server and Good Mobile Control are supported as Guests on a Windows 2008 64-bit Standard and Enterprise SP2 and R2 64 Bit Hyper-V Host.

*When deploying GMM using Windows 2008 64-bit hardware in a mixed Exchange 2003/Exchange 2007 environment, ensure that you install ExchangeMapiCDO on the GMM server and that all 2003 Exchange servers are upgraded to the latest service pack. If you are deploying GMM in an Exchange 2003-only environment, install MAPI/CDO.

Exchange Software

Good Mobile Messaging Server and Good Mobile Control Server

Quick Installation

Exchange Software

Exchange Server 2007/2010.® Exchange Server 2003 System Manager® with Service Pack 2 (recommended)(2003/2007 only)

Go to <http://customerportal.good.com/> or <http://www.good.com/support/compatibility-matrices> for any compatibility updates and for compatibility with older Good for Enterprise and GoodLink versions.

Good version 6, GMM, and GMC are tested with 32-bit OS for Windows 2003 and Exchange 2003 and with 64-bit OS for Windows 2008/ Windows 2008 R2 SP1 and Exchange 2007, and Windows 2008 R2 SP1 and Exchange 2010 SP1 and RU V2-5.

Pre-installation (Exchange 2003)

To get your users up and running, you'll need to perform the following tasks.

- First, check prerequisites; establish initial Good Mobile Messaging Server and Good Mobile Control Server host machine configuration (step 1 below)
- Second, set up the necessary user account and account permissions for Good Mobile Messaging Servers and Good Mobile Control Server (steps 2-11 below)
- Third, create a mailbox for the new *GoodAdmin* user account (step12 below)

For detailed instructions, refer to Chapter 3 of the *Good Mobile Messaging Administrator's Guide*.

1. First, confirm that the prerequisites for Good Mobile Messaging Servers and Good Mobile Control Server are in place.
2. Second (steps 2-11), create a new Windows 2000 (not supported for Good Mobile Control Server) or 2003 domain user account and give it the proper permissions. In this manual, the user is named *GoodAdmin*. This is the Good Mobile Messaging Servers user account. The name must not contain any special characters. Use

A-Z, a-z, 0-9, period (.), and dash (-). The Good Mobile Control Server can use this account but is not required to.

GoodAdmin should only be a member of Domain Users; it is added to this group by default. Do not add this user to any additional groups (Enterprise Admins or Domain Admins). By default, Exchange 2003 restricts the access of these groups to mailboxes, so administrators won't be able to read/write to a user's mailbox.

The Good Mobile Control account needs only local admin rights and should not have domain admin rights.

3. Follow the instructions below to display the Security tab in Exchange System Manager. (The Security tab must be available in Exchange System Manager for you to set Exchange permissions.) The instructions should be performed on a computer that has Exchange System Manager installed. This step only needs to be done once; skip it if you've already done it.

- a. (Recommended) Launch the self-extracting executable that was downloaded to extract the Good for Enterprise setup files. Double-click the file `ex_show_security_page.reg`. Go on to step 4.

- b. Otherwise, start Registry Editor (`Regedit32.exe`).

Warning: Do not use Regedit unless you are an experienced administrator and know exactly what you are doing.

Locate the following key in the registry:

`HKEY_CURRENT_USER\Software\Microsoft\Exchange\ExAdmin`

On the Edit menu, select New | DWORD Value and enter as its name `ShowSecurityPage`.

Double-click to assign it the value of 1.

Quit Registry Editor.

4. Launch Exchange System Manager
5. Right-click the Organization (Root) object and select Properties.
6. Choose the Security tab

Quick Installation

7. Click the Add button, and add the GoodAdmin domain account
8. Select the GoodAdmin domain account and grant the following permissions:
 - Read
 - Execute
 - Read permissions
 - List contents
 - Read properties
 - Read metabase properties
 - Administer information store
 - Create named properties in the information store
 - View information store status
 - Receive as
 - Send as
9. Verify that no security permissions for the GoodAdmin account are set to Deny.
10. Click Apply. Note: By default these permissions will be applied to all sub-containers. Do not change this setting.
11. You'll also need to assign an additional Send As permission to all domains and organizational units, as described in Chapter 3 of the *Good Mobile Messaging Administrator's Guide*.
12. On the Good for Enterprise host machines, add *GoodAdmin* to the local Administrators group with the following Advanced User Rights:
 - Back up files and directories
 - Allow log on locally
 - Profile system performance
 - Restore files and directories
13. Create an Exchange mailbox for the *GoodAdmin* account.
14. Create a Good Mobile Control account, or use *GoodAdmin*. The same account can be used for both Good Mobile Messaging and Good Mobile Control servers.

Create separate accounts if you want the Good Mobile Control account to have only the local admin rights listed in the previous step.

15. Log on using the new account to a machine that will host Good Mobile Control Server.

Now continue with “Pre-Installation (Exchange 2010)” on page 19.

Pre-Installation (Exchange 2007)

To get your users up and running, you’ll need to perform the following tasks, as described in the procedure below (Exchange 2007 SP1/SP2/SP3 supported).

- First, check prerequisites; establish initial Good Mobile Messaging Server and Good Mobile Control Server host machine configuration. (Step 1)
- Second, set up the necessary *GoodAdmin* user account with account permissions for the Good for Enterprise and Good Mobile Control Servers, and with a mailbox for the *GoodAdmin* account. (Steps 2-6)

For detailed instructions, refer to Chapter 3 of the *Good Mobile Messaging Administrator’s Guide*.

On a machine that has Exchange Management Shell installed, follow these instructions.

1. First, confirm that the prerequisites for Good Mobile Messaging Servers and Good Mobile Control Servers are in place.
2. Second (steps 2-7), create a new Windows 2000 (not supported for Good Mobile Control Server) or 2003 domain user account and mailbox for the Good Mobile Messaging Server and user account for the Good Mobile Control Server. Give these accounts the proper permissions. In this manual, the user is named

Quick Installation

GoodAdmin. The name must not contain any special characters. Use A-Z, a-z, 0-9, period (.), and dash (-).

GoodAdmin should only be a member of Domain Users; it is added to this group by default. Do not add this user to any additional groups (Enterprise Admins or Domain Admins). By default, Exchange 2007 restricts the access of these groups to mailboxes, so administrators won't be able to read/write to a user's mailbox.

3. The Good Mobile Control account can be *GoodAdmin* but needs only local admin rights and does not need domain admin rights.
4. Create the *GoodAdmin* account/mailbox from Exchange server 2007 using the Exchange Management Console or from a command shell prompt. Depending on your organization's configuration when a mailbox is created, the NT Domain login user account is also set for this *GoodAdmin* account. Once the mailbox is created, make sure that the Password Expired option is set to Never for this account.
5. Add the permissions for the *GoodAdmin* account necessary for the Good Mobile Messaging Server to work efficiently. To do this, on a machine that has Exchange Management Shell installed, do the following.

Note: By default these permissions will be applied to all sub-containers. Do not change this setting.

- a. Launch Exchange Management Shell. (Do not use Windows Powershell.)
- b. At the [MSH] prompt, enter:

```
[MSH] C:\Documents and Settings\username>
Get-OrganizationConfig | Add-AdPermission -user
GoodAdminName -AccessRights GenericRead
-ExtendedRights "Read metabase properties","Create
named properties in the information store","View
information store status","Administer information
store","Receive as","Send as"
```

6. Make sure that the *GoodAdmin* account is a member of Domain Users only.
7. To display the permissions you have set, you can enter the following command:

```
[MSH] C:\Documents and Settings\admin>Get-OrganizationConfig | Get-AdPermission -user GoodAdmin-Name | fl
```

8. For a shorter version of the output, substitute “-ft User, *rights*” for “-fl.”
9. Create a Good Mobile Control account if you will not be using *GoodAdmin* for the Good Mobile Control Server.
10. Set up Send As permissions as described in “Setting the ‘Send As’ Permission” in Chapter 3 of the *Good Mobile Messaging Administrator’s Guide*.
11. Set up Exchange Web Services Permissions as described in “Setting the Exchange Web Services Permissions in Chapter 3 of the *Good Mobile Messaging Administrator’s Guide*.”
12. Assign local permissions as described in “Assigning Good Messaging Server Host Local Permissions” as described in Chapter 3 of the *Good Mobile Messaging Administrator’s Guide*.

Pre-Installation (Exchange 2010)

To get your users up and running, you’ll need to perform the following tasks, as described in the procedure below (Exchange 2010 SP1 and RU V2-5 are supported).

- Check prerequisites; establish initial Good Mobile Messaging Server and Good Mobile Control Server host machine configuration. (Step 1)
- Set up the necessary *GoodAdmin* user account with account permissions for the Good for Enterprise and Good Mobile Control Servers, and with a mailbox for the *GoodAdmin* account. (Steps 2-6)

Quick Installation

- If you are using a load balancer in front of a CAS array, refer to “Hardware Load Balancers with Exchange 2010 CAS arrays” on page 21.

For detailed instructions, refer to Chapter 3.

On a machine that has Exchange Management Shell installed, follow these instructions.

1. First, confirm that the prerequisites for Good Mobile Messaging Servers and Good Mobile Control Servers are in place.
2. Second (steps 2-7), create a new Windows 2003 or 2008 domain user account and mailbox for the Good Mobile Messaging Server and user account for the Good Mobile Control Server. The same account can be used for both. Give this account the proper permissions. In this manual, the user is named *GoodAdmin*. The name must not contain any special characters. Use A-Z, a-z, 0-9, period (.), and dash (-).

GoodAdmin should only be a member of Domain Users; it is added to this group by default. Do not add this user to any additional groups (Enterprise Admins or Domain Admins). By default, Exchange 2010 restricts the access of these groups to mailboxes, so administrators won't be able to read/write to a user's mailbox.

3. The Good Mobile Control account, if different from *GoodAdmin*, needs only local admin rights and does not need domain admin rights.
4. Create the *GoodAdmin* account/mailbox from Exchange server 2010 using the Exchange Management Console or from a command shell prompt. Depending on your organization's configuration when a mailbox is created, the NT Domain login user account is also set for this *GoodAdmin* account. Once the mailbox is created, make sure that the Password Expired option is set to Never for this account.
5. Add the permissions for the *GoodAdmin* account necessary for the Good Mobile Messaging Server to work efficiently. To do this,

on a machine that has Exchange Management Shell installed, follow the instructions in the following section.

Hardware Load Balancers with Exchange 2010 CAS arrays

If you use third-party software that requires significantly longer-than-normal idle TCP/MAPI connections, which must be made to a load balancer in front of an Exchange 2010 CAS array, the factory default load-balancer TCP idle timeout settings for MAPI are not adequate.

In this configuration, Exchange 2010 CAS servers handle all MAPI connections from the Mobile Messaging Server. In Exchange 2007, the CAS simply re-directs the Mobile Messaging Server to the mailbox server and all MAPI calls are made to the mailbox server. Since the CAS in 2010 handles OWA, Outlook Anywhere, and internal client MAPI connections, hardware load balancers are the norm when multiple 2010 CAS servers are used to create a CAS array.

Errors that may occur on devices when using the default timeout settings on the load balancer include intermittent paused users with errors such as "Exchange not accessible," "Network error - 108 Host email system not functioning correctly." On the Mobile Control Console, you will see users paused due to errors such as "Exchange not accessible" and "MAPI failed provider." The Mobile Messaging Server may fail during install while creating a MAPI profile during installation.

For the Mobile Messaging Server to function as designed, Mobile Messaging MAPI connections to the CAS servers must be open for an extended period of time. Do the following to set this up:

1. Create a separate VIP on the load balancer.
2. Create a custom persistence and TCP Idle time out value for this virtual IP.
 - a. Persistence = Client IP Session(Source IP address)
 - b. TCP Idle timeout Value = 8 hours

Quick Installation

- c. Persistence timeout value can be default value.
3. Edit the hosts file on the Mobile Messaging server to point the network name of your F5(FQDN here) to the new VIP you have created.
4. Save this file.
5. On the Mobile Messaging machine, do `ipconfig /flushdns` from the command prompt.
6. Restart the GoodLink service or reboot the Mobile Messaging Server.

The CAS array also hosts the referral service and NSPI endpoint for exchange 2010. Therefore, the hosts file modification is mandatory.

Configuring Microsoft Exchange 2010 for GoodAdmin

(Differences for Exchange 2010 SP1 are noted.)

Ensure that the prerequisites for Exchange 2010 are met:

- Good Mobile Messaging Servers must have access to the Microsoft Exchange Server that will manage user mailboxes.
- For native Microsoft Exchange 2003 and 2007 without the requisite hotfix, MAPI/CDO must be installed using Exchange System Manager. For pure Exchange 2003/2007 environments with the hotfix, the MAPI/CDO download from Microsoft can be used. For mixed Exchange 2003/2007/2010 environments or pure Exchange 2010 environments, the MAPI/CDO download from Microsoft must be used. **MAPI/CDO is required on all Good Mobile Messaging Server machines.** The Exchange MAPICDO version for this release must be 6.5.8211.0 or higher. All earlier versions should use 6.5.8190.0. **If you move the mailbox from an Exchange 2007 server (or older) to an Exchange 2010 server (“Moving the GoodAdmin Mailbox” on page 304), you must reapply all necessary permissions and throttling policies as described below.**

MAPI 6.5.8244.0 - <http://www.microsoft.com/download/en/details.aspx?id=1004>

- Good version 6, Good Mobile Messaging, and Good Mobile Control Servers are tested with Exchange 2010 SP1 RU2-5.
- Good Mobile Messaging Server must be version 6.0.3.52 or higher.

Setting GoodAdmin permissions:

1. Start Exchange Management Shell on a machine where it is installed; do not use Windows Powershell. Go to "Start - > Programs - > Microsoft Exchange Server 2010 - > EMS."
2. At the [MSH] prompt, enter:

```
[MSH] C:\Documents and Settings\Administrator>
Get-OrganizationConfig | Add-AdPermission -user
GoodAdminName -AccessRights GenericRead
-ExtendedRights "Read metabase properties", "Create
named properties in the information store", "View
information store status", "Administer information
store", "Receive as", "Send as"
```

Note: By default these permissions will be applied to all subcontainers. Do not change this setting.

3. Make sure that the GoodAdmin account is a member of Domain Users only.

Set the "Send As" Permission

Set the "Send As" Permission in AD for the GoodAdmin user. Refer to Setting the Send As Permission in Chapter 3 of the *Good Messaging Administrator's Guide* for instructions.

Create and apply client throttling policy in Microsoft Exchange 2010

To create a custom throttling policy named GMMPolicy with required settings:

- Type cmdlet shown in red

Quick Installation

```
[PS] C:\Windows\system32> New-ThrottlingPolicy
GMMPolicy -RCAMaxConcurrency $NULL -RCAPercentTi-
meInCAS $NULL -RCAPercentTimeInMailboxRPC $NULL -
RCAPercentTimeInAD $NULL -EWSMaxConcurrency $NULL
-EWSPercentTimeInAD $NULL -EWSPercentTimeinCAS
$NULL -EWSPercentTimeInMailboxRPC $NULL -EWSMax-
Subscriptions $NULL -EWSFastSearchTimeoutInSeconds
$NULL -EWSFindCountLimit $NULL -CPAMaxConcurrency
$NULL -CPAPercentTimeInCAS $NULL -CPAPercentTi-
meInMailboxRPC $NULL
```

To add the *GoodAdmin* user to this newly created throttling policy

- Type cmdlet shown in red

```
[PS] C:\Windows\system32>Set-Mailbox "GoodAdmin"
-ThrottlingPolicy GMMPolicy
```

To verify the *GoodAdmin* user is added to throttling policy

- Type cmdlet shown in red

```
[PS] C:\Windows\system32>Get-ThrottlingPolicyAsso-
ciation GoodAdmin
```

To update the existing throttling policy for EWS:

- Type cmdlet shown in red

```
[PS] C:\Windows\system32>Set-ThrottlingPolicy
GMMPolicy -RCAMaxConcurrency $NULL -RCAPercentTi-
meInCAS $NULL -RCAPercentTimeInMailboxRPC $NULL -
RCAPercentTimeInAD $NULL -EWSMaxConcurrency $NULL
-EWSPercentTimeInAD $NULL -EWSPercentTimeinCAS
$NULL -EWSPercentTimeInMailboxRPC $NULL -EWSMax-
Subscriptions $NULL -EWSFastSearchTimeoutInSeconds
$NULL -EWSFindCountLimit $NULL -CPAMaxConcurrency
$NULL -CPAPercentTimeInCAS $NULL -CPAPercentTi-
meInMailboxRPC $NULL
```

Enable Exchange Impersonation Permissions

Option #1: To configure Exchange Impersonation for all users in an organization

1. Open the Exchange Management Shell.
2. Run the `New-ManagementRoleAssignment` cmdlet to add the permission to impersonate the specified user. The following example shows how to configure Exchange Impersonation to enable a service account to impersonate all other users in an organization.

```
New-ManagementRoleAssignment -Name:impersonation-
AssignmentName -Role:ApplicationImpersonation -
User:serviceAccount
```

Example:

```
New-ManagementRoleAssignment -Name:GMMEWSPermissions -Role:ApplicationImpersonation -User:"good-admin@sqadev.qagood.com"
```

Option #2: To configure Exchange Impersonation for specific users or groups of users.

1. Open the Exchange Management Shell.
2. Run the `New-ManagementScope` cmdlet to create a scope to which the impersonation role can be assigned. If an existing scope is available, you can skip this step. The following example shows how to create a management scope for a specific group.

```
New-ManagementScope -Name:scopeName -RecipientRestrictionFilter:recipientFilter
```

3. Run the `New-ManagementRoleAssignment` cmdlet to add the permission to impersonate the members of the specified scope. The following example shows how to configure Exchange Impersonation to enable a service account to impersonate all users in a scope.

Quick Installation

```
New-ManagementRoleAssignment -Name:impersonation-  
AssignmentName -Role:ApplicationImpersonation -  
User:serviceAccount -CustomRecipientWrite-  
Scope:scopeName
```

4. The RecipientRestrictionFilter parameter of the New-ManagementScope cmdlet defines the members of the scope. You can use properties of the Identity object to create the filter. The following example is a filter that restricts the result to a single user with the user name "john.

```
"Name -eq 'john'
```

Increase the maximum number of connections to the Address Book service in Microsoft Exchange 2010

This is not necessary for Exchange 2010 SP1.

1. On the computer that hosts the Microsoft Exchange CAS server, in <drive>:\Program Files\Microsoft\Exchange Server\V14\Bin, using a text editor, open the microsoft.exchange.addressbook.service.exe.config file.
2. Change the value of the MaxSessionsPerUser key to 100000.
3. Save and close the file.
4. Restart the Address Book service.

Increase the NSPI Connections on a Windows 2008-Based Domain Organization

This not necessary for pure Exchange 2010 environments, unless Exchange is installed on top of a Domain Controller/Active Directory.

If your organization uses Windows 2008 (or later) Domain Controller /Active Directory, modify the registry in domain controllers that hold the Global Catalog role, using the following procedure to add additional NSPI connections. This is recommended for more than 50 Exchange users. If more concurrent NSPI connections per user are legitimately required, you can change the default limit. To do this, follow these steps:

1. Click Start, click Run, type regedit, and then click OK.
2. Locate and then click the following registry key:
 HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NTDS
3. On the Edit menu, point to New, and then click Key.
4. Type Parameters, and then press ENTER.
5. Click the Parameters key.
6. On the Edit menu, point to New, and then click DWORD Value.
7. Type NSPI max sessions per user, and then press ENTER.
8. Double-click NSPI max sessions per user, type the maximum number of the NSPI connections that you want to have, and then click OK.
9. Restart the machine if your organization requires a reboot for the regkey to take effect. Problems such as paused users, MAPI logon failure, etc., should cease in less than 30 minutes.

Refer to <http://support.microsoft.com/kb/949469/en-us> for additional information.

Enable detailed calendar reminder notifications

To add subject/location information to iOS Calendar reminders, set the registry as follows and restart the GoodLink Server service:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\GoodLinkServer\parameters\PushManager]
"SendSubjectLocation"="1"
```

where

```
"sendsubjectlocation"="1"           ;Send the subject
and location
"sendsubjectlocation" = "0"         ; Send the default
generic Event Reminder message.
```

Quick Installation

Note: Only calendar items created after this change will contain detailed calendar reminders.

Installing Good for Enterprise

We recommend against running BlackBerry™ Enterprise Server on the same machine as a Good Mobile Messaging Server or Good Mobile Control Server, when both are present. (You can enable Good for Enterprise users who are also using BlackBerry.)

1. Download Good for Enterprise software and run setup.exe. You use this utility for the Good Mobile Control Server and Good Mobile Messaging Server software installations.
2. Install the Good Mobile Control server first and then install one or more Good Mobile Messaging Servers.

Note: During installation of the Good Mobile Messaging Server, a Choose Cache Directory screen is displayed.

Accept the default location for the Good Mobile Messaging Server cache or browse to select a different location. If the folder does not exist, the wizard will ask you if it should be created. For better performance, you can locate the directory on the fastest local disk. Specify a local disk, not a network share. For example, do not specify a location on M:, which is typically used by Exchange for an Exchange store. Do not locate the cache on a Network Attached Storage (NAS). This directory should be secure.

3. Run Good Mobile Control Console and create roles for use of the console on different machines. Roles for service administrator, administrator, and helpdesk are packaged with the console. Note: First Console access must be by the Superuser specified during Good Mobile Control Server installation. Launch the Console using `https://servername:8443` or `http://servername:8080`, where *servername* is the name of the machine on which Good Mobile Control Server is installed. You cannot access the console from a browser on the GMC machine. Use your Windows username and password to log in.

Note: The Good Mobile Control session in your browser will time out after one hour of no activity. The timeout is not configurable.

4. Set up user devices as described in the following section.
5. Create policies and assign them to devices as described in Chapter 6 of the *Good Mobile Messaging Administrator's Guide*.

Setting Up the Device

You set up devices wirelessly (Over The Air or "OTA" - distributed deployment model).

For details, refer to "Preparing New Devices" in Chapter 5 of the *Good Mobile Messaging Administrator's Guide*.

To set up the device:

1. Confirm with your service or sales representative that the device is a supported device type. It must have an active, supported network data service, as well as Good for Enterprise service. Some supported data services may not support roaming. In such cases, Good for Enterprise, like the device's browser, will not work outside service areas. Visit <http://www.good.com> for more information.
2. Devices should have the following available memory:
 - iOS - Application: 5MB. Runtime footprint: ~9MB (with occasional spikes to 14MB)
 - Android - Application: 16.6MB (may increase with future releases). Runtime footprint: up to 33MB, depending upon user mailbox data
 - Palm OS - 14.5MB
 - Pocket PC - 12MB (14MB for Treo 700WX)
 - Smartphone - 12MB

Quick Installation

Contact your authorized service representative for additional information on memory requirements.

Note that Palm is not supported by version 6.0 Client software, but earlier software versions do support Palm.

3. The device battery should be fully charged (an alert will be displayed if the battery is below 25%).
4. Use Good Mobile Control Console to set up and activate user devices wirelessly:
 - a. On the Console Home page, click the “Add devices” link.
 - b. Select the user who will be assigned the device. If the user already has one or more devices assigned to him/her, you’ll be prompted to add another. Click OK.
 - c. Specify a policy and group for the device.
 - d. When finished, an email is sent to the user's account. The email contains a PIN and URL. The device user connects to the URL and enters his/her email address and the PIN and from the site, Good downloads the OTA Setup application. OTA Setup is a wizard-like application that leads the user through a set of steps to authenticate the user, download and install Good for Enterprise Client software, and connect to Good Mobile Messaging Server to wirelessly synchronize the user's account. You can set policies for PIN expiration and reuse, as described in Chapter 5 of the *Good Mobile Messaging Administrator's Guide*. You can display the PIN and URL information at the Console by going to the OTA page for the device on the Handhelds tab.

You can quickly check the connection status between Good Mobile Messaging Servers and the Good Operations Center, and between the Servers and the devices they service, using the Good Monitoring Portal located at <http://www.good.com/gmp>. Like the Good Mobile Control Console, the Good Monitoring Portal provides information about users, their device types and service carriers, and much more.