

Vocera Smartphone Configuration Guide

Version 4.4.4

v o c e r a





Copyright © 2002-2015 Vocera Communications, Inc. All rights reserved.
Protected by US Patent Numbers D486,806; D486,807; 6,892,083; 6,901,255;
7,190,802; 7,206,594; 7,248,881; 7,257,415; 7,310,541; 7,457,751; AU
Patent Number AU 2002332828 B2; CA Patent Number 2,459,955; EEC Patent
Number ED 7513; and Japan Patent Number JP 4,372,547.

Vocera® is a registered trademark of Vocera Communications, Inc.

This software is licensed, not sold, by Vocera Communications, Inc. ("Vocera").
The reference text of the license governing this software can be found at
www.vocera.com/legal. The version legally binding on you (which includes
limitations of warranty, limitations of remedy and liability, and other provisions)
is as agreed between Vocera and the reseller from whom your system was
acquired and is available from that reseller.

Certain portions of Vocera's product are derived from software licensed by the
third parties as described at

Java® is a registered trademark of Oracle Corporation and/or its affiliates.

Microsoft®, Windows®, Windows Server®, Internet Explorer®, Excel®, and
Active Directory® are registered trademarks of Microsoft Corporation in the
United States and other countries.

All other trademarks, service marks, registered trademarks, or registered service
marks are the property of their respective owner/s. All other brands and/or
product names are the trademarks (or registered trademarks) and property of
their respective owner/s.

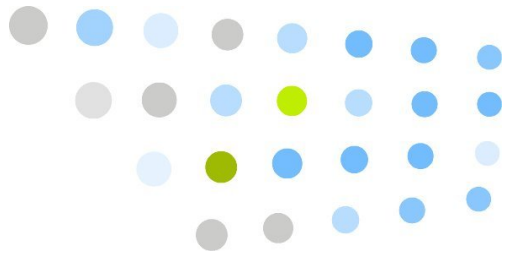
Vocera Communications, Inc.

www.vocera.com

tel :: +1 408 882 5100

fax :: +1 408 882 5101

2015-04-18 11:50:28



Contents

1. Introduction.....	11
Smartphone Configuration Overview.....	11
Staging and Provisioning using MSP.....	11
Typical MSP Setup.....	12
Tethered Configuration.....	13
MSP Server Requirements.....	14
MSP Requirements on the Vocera Client Gateway Computer.....	14
MSP Requirements on the Configuration Computer.....	14
Browser Requirements.....	15
MSP Requirements on VMware.....	15
Prerequisite Software.....	16
MSP Documentation.....	16
2. Installation.....	17
Installing Microsoft IIS.....	17
Configuring the FTP Server.....	19
Creating an MSP FTP Folder.....	19
Configuring Windows IIS FTP Service as a Relay Server.....	19
Installing .NET Framework.....	21
Installing MSP 3.3 Server.....	21
Upgrading from MSP 3.2.1 to MSP 3.3.....	29
Installing Microsoft SQL Server Management Studio Express.....	31
Smartphone Files Installed with the Vocera Client Gateway.....	31
Logging into the MSP Console.....	32
MSP Console Quick Reference.....	34
3. Administrative Setup.....	37
Copying Files from the Vocera Client Gateway Computer.....	37
Updating Your MSP License Key.....	37
Uploading the Network.WLAN.EWP Setting Definition Document.....	38
Uploading the EWP Persistent REG Install Package Template.....	39
Uploading the Vocera Root Certificate Install Package Template.....	39



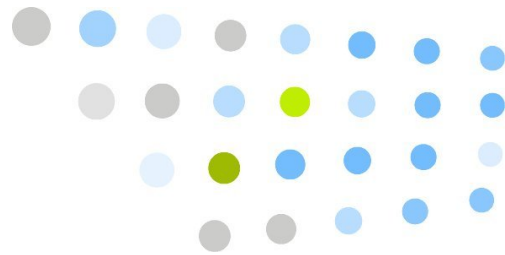
Creating a Relay Server Object.....	40
Creating a Network Settings Object.....	42
Creating a Site Object.....	45
4. Uploading and Creating Content Objects.....	49
Understanding Content Objects.....	49
Uploading Packages for Vocera Smartphones.....	50
Predefined Vocera Packages.....	52
Creating Settings.....	53
Creating a Date and Time Settings Object.....	53
Creating a Certificate Settings Object.....	54
Creating a Vocera Server SSL Certificates Package.....	56
Managing SSL Certificates.....	58
Optional Content Objects.....	58
Creating Conditions.....	58
Creating Message Set Objects.....	59
Creating Bundles.....	59
Using Production Site Bundles.....	63
5. Using Staging to Configure Vocera Smartphones.....	65
Staging Prerequisites.....	65
How Staging Works.....	66
Creating a Staging Profile.....	67
Creating a Staging Profile Without Network Settings.....	69
How to Use Staging.....	70
Viewing Staging Status.....	74
Best Practices.....	74
6. Using Provisioning to Update Vocera Smartphones.....	75
Provisioning Prerequisites.....	75
How Provisioning Works.....	75
Creating a Provisioning Bundle.....	77
Managing Package Versions.....	77
Creating a Provisioning Policy.....	78
How to Use Provisioning.....	79
Viewing Provisioning Status.....	80
Best Practices.....	80
7. Verifying Smartphone Configuration.....	83
Testing the Smartphone.....	83
Viewing Smartphone Information.....	86



8. Troubleshooting.....	89
Troubleshooting Staging.....	89
Troubleshooting Provisioning.....	91
Changing the Vocera Client Gateway IP Address.....	92
Restarting MSP Services.....	93
Troubleshooting the Relay Server.....	94
Changing the Relay Server after Staging.....	95
Configuring FileZilla Server as a Relay Server.....	96
Uploading Smartphone Logs to an FTP Server.....	98
IIS FTP Server Requirements.....	98
Uploading Logs.....	98
Downloading Logs.....	99
Log for Vocera Apps.....	100
Master Clearing a Smartphone.....	100
MSP Client Error Codes.....	100
 A. Installation Checklists.....	 105
Pre-Installation Checklist for IT.....	105
Pre-Installation Tasks for the MSP Server.....	105
Pre-Installation Tasks for the Configuration Computer.....	105
Installation Checklist.....	106
MSP Server Installation Tasks.....	106
Configuration Computer Installation Tasks.....	106
Post-Installation Checklist.....	107
Administrative Setup Tasks.....	107
Content Objects Tasks.....	108
Staging Tasks.....	108
Provisioning Tasks.....	108
 B. Tethered Configuration of Smartphones.....	 109
Tethered Configuration Checklist.....	109
Setting Up a Computer to Configure Smartphones.....	110
Installing the Motorola EWP Provisioning Tool.....	111
Collecting Network and Security Information.....	112
Configuring a Smartphone.....	113
Using the Motorola EWP Provisioning Tool.....	113
Copying Vocera CAB Files.....	119
Installing Vocera CAB Files.....	122
Optional CAB Files.....	124
Installing Vocera Server SSL Certificates on a Smartphone.....	126
Setting the Date and Time.....	127
Restoring the Rapid Deployment Client Shortcut.....	127



C. Configuring Smartphones for PEAP or EAP-TLS	
Authentication.....	129
Upgrading Smartphones to PEAP or EAP-TLS.....	129
Authentication Servers and Certificates.....	130
Device Authentication versus User Authentication.....	130
Certificates from Trusted Certificate Authorities.....	130
Self-Signed Certificates.....	131
Vocera Manufacturer Certificates Not Supported on Smartphones.....	131
Installing a Certificate on the Smartphone.....	131
Configuring PEAP Using MSP.....	132
Configuring EAP-TLS Using MSP.....	133
Configuring PEAP or EAP-TLS Using the Motorola EWP Provisioning Tool.....	135
D. IP Port Usage.....	137
Index.....	139

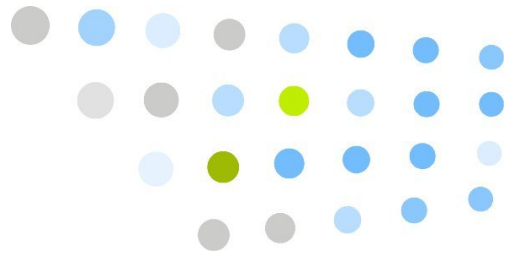


List of Figures

1.1. Typical MSP setup for Vocera smartphones.....	13
2.1. Application Server components.....	18
2.2. MSP 3.3 CD Launcher dialog box.....	22
2.3. MSP 3.3 Server Installer - Welcome.....	23
2.4. MSP 3.3 Server Installer - License Agreement.....	23
2.5. MSP 3.3 Server Installer - Destination Folder.....	24
2.6. MSP 3.3 Server Installer - Ready to Install the Program.....	24
2.7. MSP 3.3 Install Point Installer - Installer Completed.....	25
2.8. MSP 3.3 Server Installer - Installation Scenario.....	25
2.9. MSP 3.3 Server Installer - MSP Control Components.....	26
2.10. MSP 3.3 Server Installer - MSP Core Database.....	26
2.11. MSP 3.3 Server Installer - SQL Core Database Review.....	27
2.12. MSP 3.3 Server Installer - MSP Runtime Windows Authentication.....	27
2.13. MSP 3.3 Server Installer - MSP Authentication to SQL Database.....	28
2.14. MSP 3.3 Server Installer - Initial MSP Users.....	28
2.15. MSP 3.3 Server Installer - Review Installation Settings.....	29
2.16. MSP 3.3 Server Installer - Install Progress.....	29
2.17. MSP Server Installer Information dialog box.....	30
2.18. SQL Core Database Review dialog box.....	31
2.19. MSP Console Start Page tab.....	33
3.1. Create Relay Server wizard.....	40
3.2. Create Setting wizard.....	42
3.3. Create Site wizard.....	46
4.1. Content Objects.....	50
4.2. Create Setting wizard, Step 2.....	55
4.3. Create Package wizard.....	56
4.4. Package Files scree.....	57
4.5. Bundle Step Add page.....	62
5.1. On-demand staging of Vocera smartphones.....	66
5.2. Profile Create wizard.....	68
5.3. Profile Create wizard, Step 2.....	69
5.4. Staging server is turned off.....	71
5.5. Staging server is turned on.....	71



5.6. Connecting the phone to a computer.....	71
5.7. Rapid Deployment - Search Connected Networks.....	72
5.8. Rapid Deployment - Remove device prompt.....	73
5.9. Rapid Deployment - Staging Complete dialog box.....	73
6.1. Provisioning content onto Vocera smartphones.....	76
6.2. Package Management page.....	77
6.3. Policy Create wizard.....	78
7.1. Phone after successful startup.....	83
7.2. Phone stuck "Searching for Gateway".....	84
7.3. Phone with no network connection.....	84
7.4. Information dialog box.....	86
7.5. WLAN Information dialog box.....	87
7.6. VCG Information dialog box.....	87
7.7. Wireless Security Information dialog box.....	87
7.8. Log Upload dialog box.....	88
7.9. About dialog box.....	88
8.1. WiFi Login dialog box.....	90
8.2. MSP Administration Program.....	94
8.3. Users dialog box.....	96
8.4. Add User Account dialog box.....	96
8.5. FileZilla Shared Folders page.....	97
8.6. Log Upload dialog box.....	99
8.7. Log Upload success.....	99
B.1. Supported Platforms dialog box.....	112
B.2. Motorola EWP Provisioning Tool window.....	114
B.3. Connecting the phone to a computer.....	120
B.4. Connecting the phone to a computer.....	121
B.5. Date and Time window.....	127
C.1. Root Certificates dialog box.....	131
C.2. Create Setting wizard for PEAP configuration.....	133
C.3. Create Setting wizard for EAP-TLS configuration.....	134



List of Tables

1.1. Vocera Client Gateway requirements.....	14
1.2. Configuration hardware requirements.....	14
2.1. Smartphone-related directories on the Vocera Client Gateway.....	32
2.2. MSP quick reference.....	34
3.1. Network settings.....	42
4.1. Predefined MSP packages for Vocera smartphones.....	52
4.2. Date and Time settings.....	54
4.3. Certificate settings.....	55
4.4. Condition Object purposes.....	59
4.5. Vocera smartphone bundle steps.....	60
8.1. MSP client error codes.....	100
B.1. Network and security information.....	112
B.2. Motorola EWP Provisioning Tool fields.....	115
B.3. Optional radio settings CAB files.....	125
B.4. Logging CAB files.....	126
C.1. Smartphone firmware required for PEAP and EAP-TLS.....	129
D.1. MSP Server IP port usage.....	137





Introduction

The Vocera smartphone provides the one-touch, instant communication capability of a Vocera client in a familiar phone form factor. With the smartphone, users have the additional flexibility to use keypad dialing if necessary.

The process of configuring and updating Vocera smartphones is different from the process used to configure and update Vocera badges, and the tools you use for both are also different. The key difference is that Motorola Mobility Services Platform (MSP) is the updater software required for Vocera smartphones instead of the Vocera Badge Configuration Utility and Badge Properties Editor.

The purpose of this guide is to describe how to use MSP to configure and update Vocera smartphones. It is intended to supplement Motorola's documentation for MSP, not replace it. For complete details on how to use MSP, see the Motorola documentation.

Smartphone Configuration Overview

Staging and Provisioning using MSP

Motorola's Mobility Services Platform (MSP) is a scalable software solution that provides a single point of control for managing large numbers of mobile devices within your Enterprise.

The MSP Server can manage thousands of mobile devices through the MSP Client Software on the devices. The interface for MSP Server is called MSP Console UI.

MSP is a 3-tier management system that always manages mobile devices indirectly through one or more intermediary Relay Servers (FTP Servers) located within your Enterprise. This layered architecture makes it possible for MSP to be configured to manage large numbers of mobile devices from a central point, using a single MSP Server.

Note: For configuration of Vocera smartphones, a single Relay Server should be sufficient, and you can install it on the same computer as the MSP Server.

MSP is available in three editions: MSP Stage Edition, MSP Provision Edition, and MSP Control Edition. Vocera provides a license for the MSP Provision Edition to use for configuring Vocera smartphones.

This manual does not cover all MSP features. It focuses instead on the following tasks:

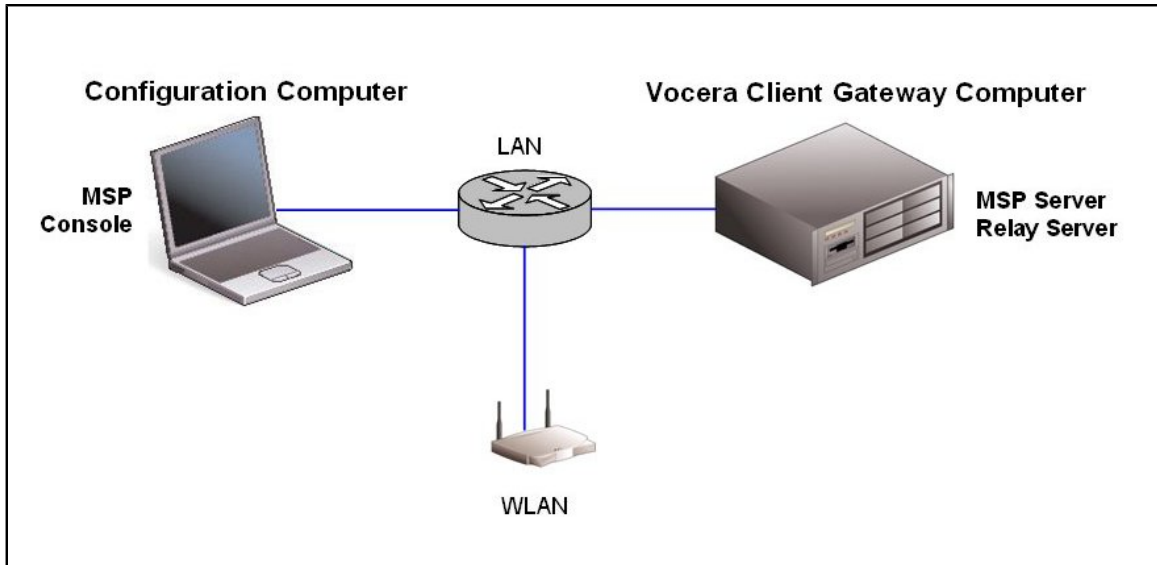
- **Staging** – Vocera smartphones must be configured for use on your Enterprise network and appropriate software must be installed before the phones can be used. Staging is a manual process initiated by the person configuring the device.
- **Provisioning** – Ongoing configuration and installation of software and settings onto Vocera smartphones is accomplished through Provisioning. It is done remotely under the control of the MSP Server.

Important: MSP 3.3 supports *dynamic deployment* of content to mobile devices, allowing you to render content differently to different devices. Vocera smartphones currently do not support dynamic deployment. The same content must be deployed statically to all Vocera smartphones.

Typical MSP Setup

In the typical setup of MSP for Vocera, you install MSP on the Vocera Client Gateway computer, as shown in the following figure. A configuration computer is used to perform initial staging of content onto Vocera smartphones using a browser plugin called the On Demand Server. The MSP system installed on the Vocera Client Gateway computer is used to perform provisioning of software updates.

Figure 1.1. Typical MSP setup for Vocera smartphones



This typical setup of MSP components simplifies the deployment and meets the following requirements:

- All MSP Components are installed on the same computer, the Vocera Client Gateway computer. This includes Microsoft SQL Server 2005 Express and Microsoft Internet Information Services (IIS).
- SQL Authentication is used for runtime connections to the SQL database.
- Microsoft SQL Server 2005 Express is recommended.

Tethered Configuration

If you have only a few Vocera smartphones to configure, it may be more practical to manually configure them by tethering them to a computer using a USB cable rather than using MSP to configure them over the air. For details, see [Appendix B, Tethered Configuration of Smartphones](#) on page 109.

MSP Server Requirements

MSP Requirements on the Vocera Client Gateway Computer

The Vocera Client Gateway has the following requirements:

Table 1.1. Vocera Client Gateway requirements

Component	Requirement
Operating System	Windows Server 2003 Standard or Enterprise editions with SP2 or higher
Processor Hard Disk Capacity Internal Memory	See the Vocera Server Sizing Matrix¹ .
Video Card	256 colors
Network Interface Controller	1 network interface controller

MSP Requirements on the Configuration Computer

Vocera requires the following hardware for the configuration computer used to configure Vocera smartphones.

Important: The configuration computer that you use to run the MSP Console to configure Vocera smartphones can be different from the computer used to configure Vocera badges. It does not need to be connected to an isolated access point. However, it requires a LAN or WLAN connection to the MSP Server computer.

Table 1.2. Configuration hardware requirements

Component	Requirement
Configuration Computer	Any notebook or desktop computer running Windows 7, Windows Server 2003 Standard edition, Windows Server 2003 Enterprise edition, or Windows XP Professional edition.

¹ <http://www.vocera.com/products/documents/VoceraServerSizingGuidelines.pdf>

Component	Requirement
Network Interface Controller	An Ethernet port to connect to the MSP Server over the LAN. Note: You could also use a wireless network interface controller to connect to the MSP Server over the WLAN.
.NET Framework 2.0 SP2	.NET Framework 2.0 SP2 is required to run the MSP Console in Internet Explorer.
Windows Mobile Device Center or Microsoft ActiveSync	Windows Mobile Device Center or ActiveSync is needed on any computer on which you tether a phone.
USB port and a USB cable	The USB cable connects phones to the configuration computer.

Browser Requirements

A Web browser is required to use the MSP Console. You can access the MSP Console on the MSP Server or from another computer connected to the network. Motorola recommends using Microsoft Internet Explorer™ versions 6 or 7.

Note: On-Demand Staging is supported only with Internet Explorer.

MSP Requirements on VMware

MSP 3.3 is supported for use in a VMware virtualized environment. VMware can be installed and run on any "host" operating system (the one VMware itself is running on) that is supported by VMware. However, the "guest" operating system (the one running inside the virtual machine and on which MSP is installed) must be one of the supported Microsoft operating systems as described in the *MSP 3.3 Software Installation Guide*.

Note: Vocera recommends installing Vocera Client Gateway and Motorola MSP on separate VMs.

Prerequisite Software

The following prerequisite software must be installed with MSP 3.3:

- Microsoft Internet Information Services (IIS) 6
- Microsoft .NET Framework 2.0 SP2
- Microsoft SQL Server 2005 Express
- Windows Installer 4.5 Update

Note: To install Microsoft IIS 6, you will need the Windows Server 2003 CD. .NET Framework 2.0 SP2, SQL Server 2005 Express, and Windows Installer 4.5 Update are included on the MSP 3.3 CD.

MSP Documentation

This manual describes how to use MSP to configure and update Vocera smartphones. For complete information on how to use MSP, see the following Motorola documentation:

- *Mobility Services Platform Software Installation Guide*
- *Using Mobility Services Platform*
- *Mobility Services Platform Release Notes*



Installation

This chapter describes how to install MSP Server and all the prerequisite software.

Note: When you set up the MSP Server, make sure you use the installation checklists. See [Appendix A, Installation Checklists](#) on page 105.

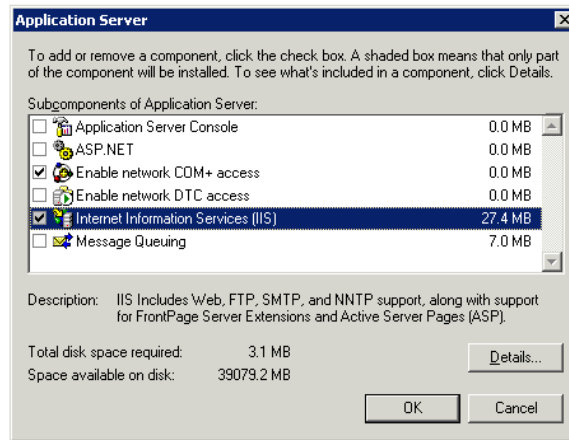
Installing Microsoft IIS

Follow these steps to install Microsoft Internet Information Services (IIS).

To install IIS 6 on Windows Server 2003:

1. Log in to the MSP Server computer with administrator privileges.
2. Choose **Start > Settings > Control Panel > Add or Remove Programs**.
3. Click the **Add/Remove Windows Components** tab in the left pane. The Windows Components wizard appears.
4. In the list of Windows Components, select **Application Server** and click **Details**.
5. In the list of Application Server subcomponents, check the box for **Internet Information Services (IIS)**, and then click **Details**.

Figure 2.1. Application Server components



6. In the list of IIS subcomponents, make sure the following components are selected:

- **Common Files**
- **File Transfer Protocol (FTP) Service**
- **Internet Information Services Manager**
- **World Wide Web Service**

Click **OK**.

7. In the Application Server dialog box, click **OK**.

8. In the Windows Components dialog box, click **Next**. The installation program will prompt you for the Windows CD that was used to install the operating system. Follow the prompts to complete the installation of IIS.

9. When installation is completed, click **Finish** to close the Windows Components wizard.

10. To verify that IIS has been installed correctly:

- a. Choose **Start > Programs > Administrative Tools**.
- b. Verify that **Internet Information Services (IIS) Manager** is listed as one of the Administrative tools.

Configuring the FTP Server

This section describes how to configure the Windows IIS FTP Service.

- [Creating an MSP FTP Folder](#) on page 19
- [Configuring Windows IIS FTP Service as a Relay Server](#) on page 19

Creating an MSP FTP Folder

As a best practice, you should create a home folder for the FTP server different from the default setting. For example, you could create a folder on the **d:** drive named **MSP_FTP** to easily identify where MSP FTP files are stored.

Configuring Windows IIS FTP Service as a Relay Server

This section describes how to configure Windows IIS FTP Service as a Relay Server for MSP Server.

To configure Windows IIS FTP Service:

1. Log in to the MSP Server computer with administrator privileges.
2. Create a Windows user account to use for the IIS FTP Service. If appropriate, add the account to a Windows user group.
 - a. Choose **Start > Programs > Administrative Tools > Computer Management**.
 - b. In the console tree, right-click the **System Tools > Local Users and Groups > Users** folder, and choose **New User** from the pop-up menu.
 - c. In the New User dialog box, type the username and password (for example, **vocera** for both).
 - d. Make sure the **User Must Change Password at Next Logon** box is unchecked.
 - e. Make sure the **Password Never Expires** box is checked.
 - f. Click **Create** to create the user account.
 - g. Click **Close** to close the New User dialog box.

Note: Write down the **Username** and **Password** for the account. You will need to know them when you configure a Relay Server in the MSP Console.

3. Choose **Start > Programs > Administrative Tools > Internet Information Services (IIS) Manager**.

4. In IIS Manager, click the local computer, right-click the **FTP Sites** folder, point to **New**, and then click **FTP Site**.
The FTP Site Creation Wizard appears.
5. On the **Welcome to the FTP Site Creation Wizard** page, click **Next**.
6. On the **FTP Site Description** page, enter **vocera**, and then click **Next**.
7. On the **IP Address and Port Settings** page, DO NOT change the default settings for the IP address of the server and the desired port number. Click **Next**.
8. On the **FTP User Isolation** page, click **Isolate users**, and then click **Next**.
This setting determines a unique home directory for each user that logs into the FTP server based on the user name.
9. On the **FTP Site Home Directory** page, enter the MSP FTP folder you created in [Creating an MSP FTP Folder](#) on page 19 (for example, **d:\MSP_FTP**).
10. On the **FTP Site Access Permissions** page, make sure both the **Read** and **Write** boxes are checked. Click **Next**.
11. Click **Finish**.
12. Create user home directories for the **vocera** user and anonymous users:
 - a. For the **vocera** user, create the **LocalUser\vocera** directory under the FTP root directory.
For example, if FTP site home directory is **d:\MSP_FTP**, the full path of the **vocera** user directory is **d:\MSP_FTP\LocalUser\vocera**.
 - b. For anonymous users, create the **LocalUser\Public** directory under the FTP root directory.
For example, if the FTP site home directory is **d:\MSP_FTP**, the full path of the anonymous user directory is **d:\MSP_FTP\LocalUser\Public**.
13. Stop the Default FTP Site. Right-click the **Default FTP Site**, and choose **Stop**.
14. Start the Vocera site. Right-click the **Vocera** site, and choose **Start**.
15. Verify that you can access the FTP directory from a different computer.
 - a. Open Internet Explorer on a different computer and enter the following in the Address field of the browser window:
ftp://MSP_Server_IP_Address
 - b. To view the site, choose **View > Open FTP Site in Windows Explorer**.

c. To log in as the **vocera** user, choose **File > Login As**.

A login dialog box should appear. Enter the **User Name** and **Password**, and then click **Logon** to see the contents of the MSP FTP folder.

Installing .NET Framework

The MSP Server computer requires .NET Framework 2.0 SP2 (or later), which you can install from the MSP 3.3 CD.

The Motorola EWP Provisioning Tool, which should be installed on the Vocera configuration computer for tethered configuration of smartphones, requires .NET Framework 3.5 (or later). You can download the installer for .NET Framework 3.5 Service Pack 1 and installation instructions from the following Microsoft site:

[Download Microsoft .NET Framework 3.5 Service Pack 1¹](http://www.microsoft.com/en-us/download/details.aspx?id=22)

Installing MSP 3.3 Server

This section describes how to install MSP 3.3 Server. During installation of MSP 3.3, you will also install .NET Framework 2.0 SP2, Windows Installer 4.5 Update, and Microsoft SQL Server 2005 Express.

To install MSP 3.3:

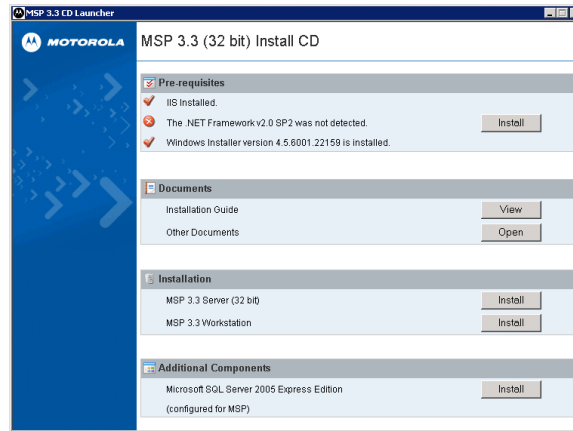
1. Log in to the MSP Server computer with administrator privileges.
2. Insert the MSP 3.3 Installation CD in the drive.

Important: You must install from the MSP 3.3 Installation CD. You cannot copy the files on the CD to another location (such as a hard disk) and run the installer from there.

The MSP 3.3 CD Launcher dialog box appears automatically.

¹ <http://www.microsoft.com/en-us/download/details.aspx?id=22>

Figure 2.2. MSP 3.3 CD Launcher dialog box



If this screen does not appear, browse to root of the MSP 3.3 Installation CD and run the following file:

- **Launch_CD_Menu.bat**

3. If .NET Framework version 2.0 SP2 is NOT detected, click the **Install** button for it. Otherwise, skip to step 4.
 - a. Click **I have read and ACCEPT the terms of the license agreement**, and then click **Install**.
 - b. When .NET Framework installation is finished, the Setup Complete dialog box appears. Click **Exit**.
 - c. A message box says that installation completed successfully. Click **OK**.
4. If Windows Installer 4.5 Update is NOT detected, click the **Install** button for it. Otherwise, skip to step 5.
 - a. When the Software Update Installation Wizard appears, click **Next**.
 - b. In the License Agreement dialog box, select **I Agree**, and then click **Next**.
 - c. When the installation is finished, make sure the **Do Not Restart** box is unchecked. Click **Finish** to apply the changes.
 - d. A message box says that installation completed successfully. Click **OK**.
5. If Microsoft SQL Server 2005 Express is NOT installed and configured for MSP 3.3, click the **Install** button for it. Otherwise, skip to step 6.

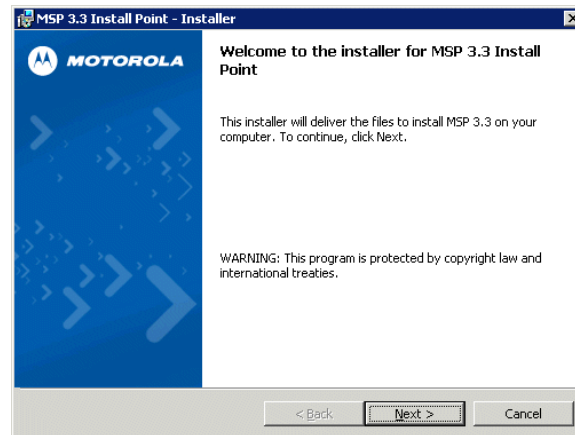
Microsoft SQL Server 2005 Express installation proceeds without user interaction and takes several minutes.

When the installation is finished, a message box says that installation completed successfully. Click **OK**.

6. To install MSP Server, click the **Install** button for it.

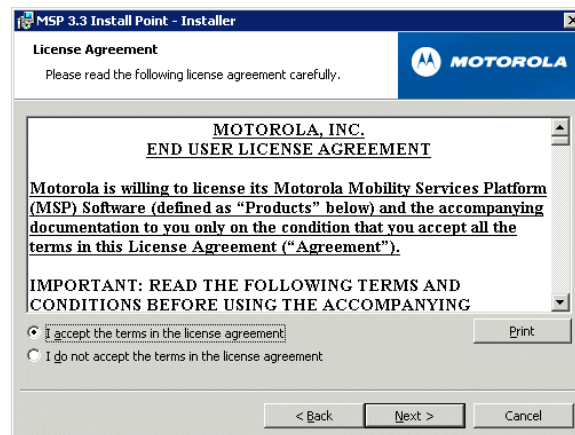
7. In the Welcome dialog box, click **Next**.

Figure 2.3. MSP 3.3 Server Installer - Welcome



8. In the License Agreement dialog box, click **I accept the terms of the license agreement**, and then click **Next**.

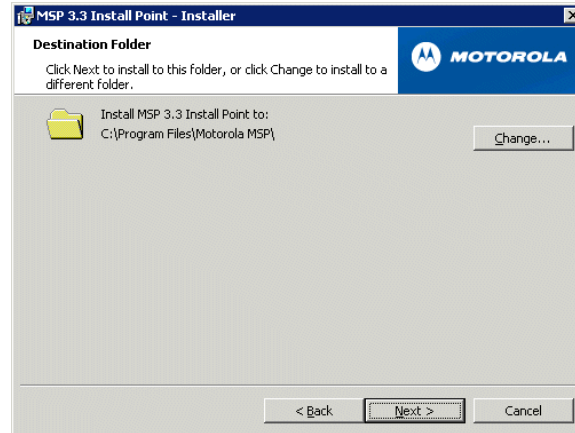
Figure 2.4. MSP 3.3 Server Installer - License Agreement



9. In the Destination Folder dialog box, accept the destination folder. Click **Next**.

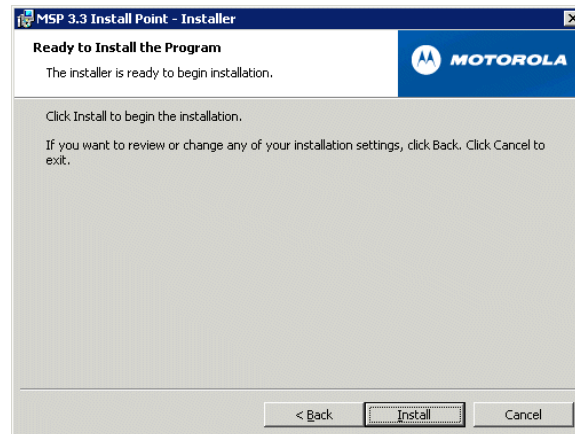
Note: DO NOT specify a destination different from the default folder. Scripts provided by Vocera to set up MSP Server after installation refer to this default location.

Figure 2.5. MSP 3.3 Server Installer - Destination Folder



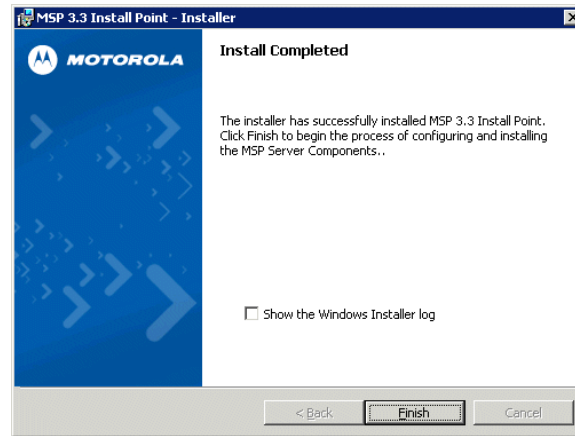
10. In the Ready to Install the Program dialog box, click **Install**.

Figure 2.6. MSP 3.3 Server Installer - Ready to Install the Program



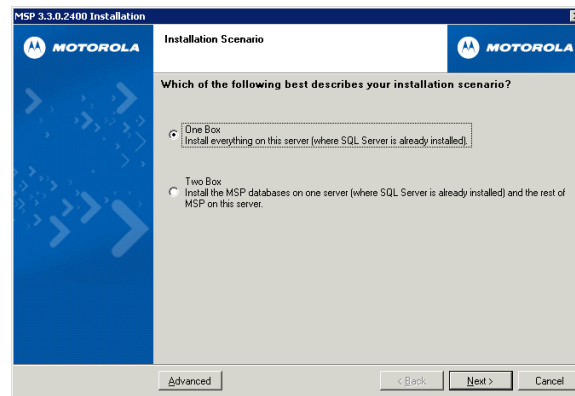
Wait while the installer installs the MSP 3.3 Install Point. This may take a few minutes.

11. When the Installer Completed dialog box appears, click **Finish**.

Figure 2.7. MSP 3.3 Install Point Installer - Installer Completed

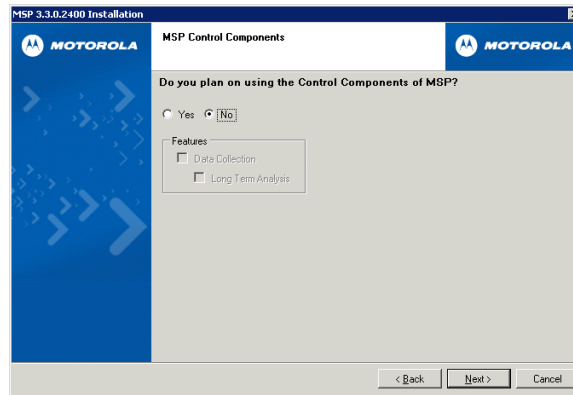
Note: At this point, installation of the MSP 3.3 Install Point is completed, but MSP 3.3 Server installation is NOT finished yet.

12. When the Installation Scenario dialog box appears, click **One Box**, and then click **Next**.

Figure 2.8. MSP 3.3 Server Installer - Installation Scenario

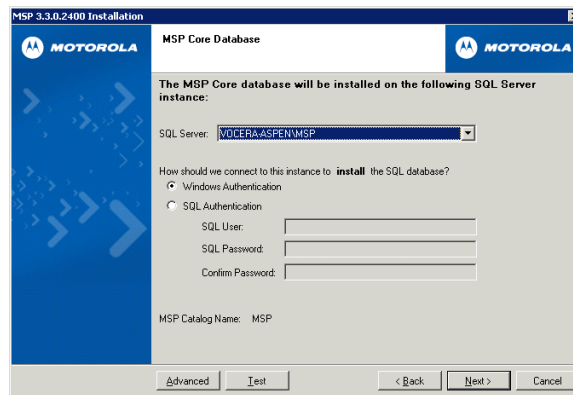
13. If the MSP 3.3 Server Installer displays a message saying it cannot find a SQL Server Express instance, click **OK**.
14. When the MSP Control Components dialog box appears, click **No**, and then click **Next**.

Figure 2.9. MSP 3.3 Server Installer - MSP Control Components

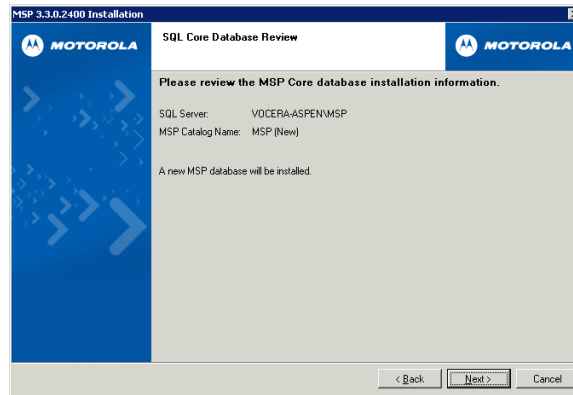


15. When the MSP Core Database dialog box appears, accept the default settings, and click **Next**.

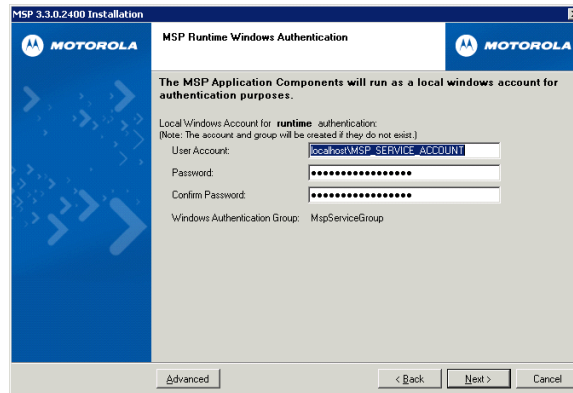
Figure 2.10. MSP 3.3 Server Installer - MSP Core Database



16. When the SQL Core Database Review dialog box appears, click **Next**.

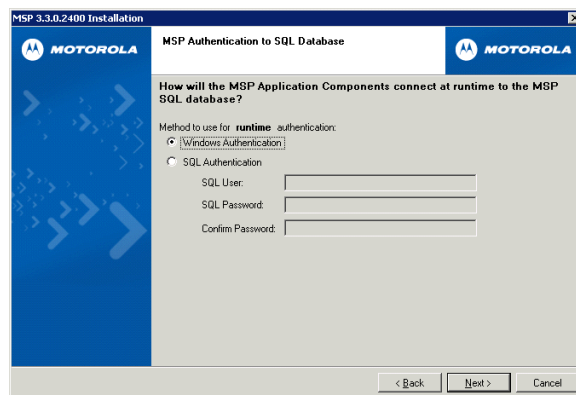
Figure 2.11. MSP 3.3 Server Installer - SQL Core Database Review

17. When the MSP Runtime Windows Authentication dialog box appears, accept the defaults and click **Next**.

Figure 2.12. MSP 3.3 Server Installer - MSP Runtime Windows Authentication

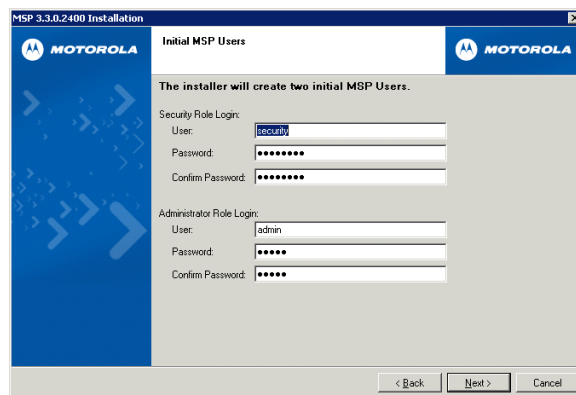
18. When the MSP Authentication to SQL Database dialog box appears, accept the defaults and click **Next**.

Figure 2.13. MSP 3.3 Server Installer - MSP Authentication to SQL Database

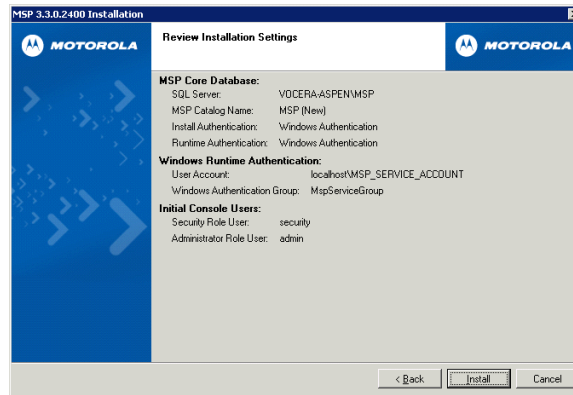


19. When the Initial MSP Users dialog box appears, accept the defaults and click **Next**.

Figure 2.14. MSP 3.3 Server Installer - Initial MSP Users

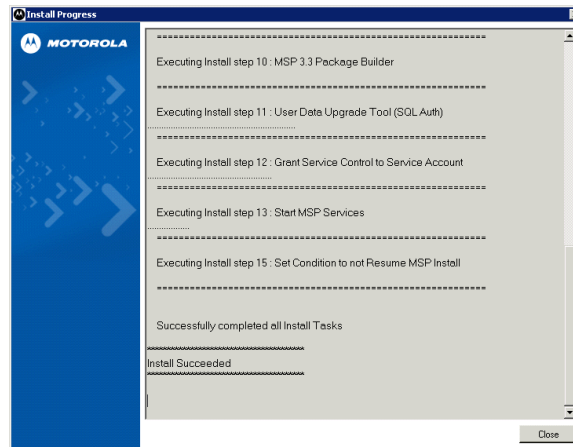


20. When the Review Installation Settings dialog box appears, accept the settings and click **Install**.

Figure 2.15. MSP 3.3 Server Installer - Review Installation Settings

21. An Install Progress window opens, displaying the progress of MSP 3.3 Server installation.

Several minutes later when MSP 3.3 Server installation is finished, the Install Progress window displays "Install Succeeded." Click **Close**.

Figure 2.16. MSP 3.3 Server Installer - Install Progress

22. Close the MSP 3.3 CD Launcher window.
23. Reboot the computer.

Upgrading from MSP 3.2.1 to MSP 3.3

You can upgrade from MSP 3.2.1 to MSP 3.3, maintaining your existing data. You do not need to reinstall prerequisite software such as .NET Framework 2.0 SP2 or Microsoft SQL Server 2005 Express.

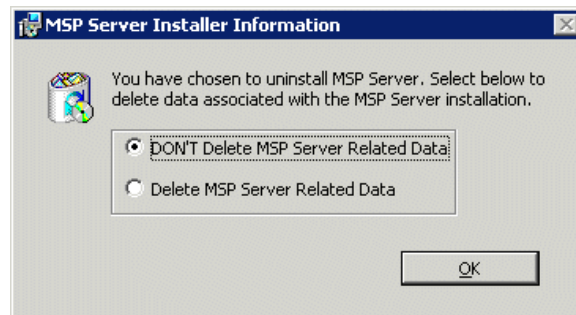
To upgrade from MSP 3.2.1 to MSP 3.3:

1. Use the Microsoft SQL Server Management Studio Express to back up your MSP 3.2.1 database.

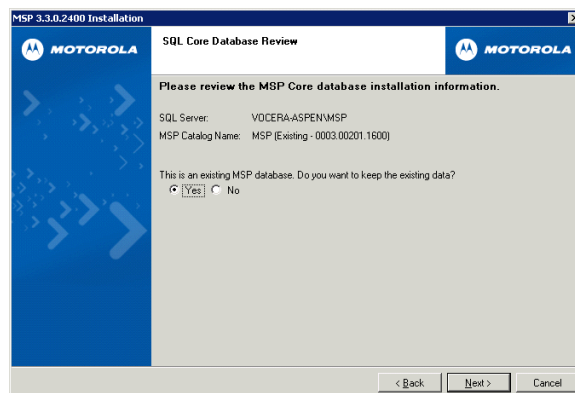
See [Installing Microsoft SQL Server Management Studio Express](#) on page 31 for information about how to download Microsoft SQL Server Management Studio Express. For information about how to use Microsoft SQL Server Management Studio Express to back up the MSP database, see *Using Mobility Services Platform*.

2. Uninstall MSP 3.2.1.
 - a. Choose **Start > Control Panel > Add or Remove Programs**.
 - b. Select **MSP Package Builder**, and click **Change**.
 - c. In the Welcome dialog box, click **Next**.
 - d. In the Remove the Program dialog box, click **Remove**.
 - e. When the Installer Completed dialog box appears, click **Finish**.
 - f. In the Add or Remove Programs window, select **MSP Server**, and then click **Change**.
 - g. In the Welcome dialog box, click **Next**.
 - h. In the MSP Server Installer Information dialog box, select **DON'T Delete MSP Server Related Data**. Click **OK**.

Figure 2.17. MSP Server Installer Information dialog box



- i. In the Remove the Program dialog box, click **Remove**.
 - j. When the Installer Completed dialog box appears, click **Finish**.
 - k. Close the Add or Remove Programs window.
3. Install MSP 3.3 Server. See [Installing MSP 3.3 Server](#) on page 21.
- During MSP 3.3 Server installation, in the SQL Core Database Review dialog box make sure you choose to keep the existing MSP data.

Figure 2.18. SQL Core Database Review dialog box

When you finish MSP 3.3 Server installation, reboot the computer.

4. After the computer reboots and the MSP services are started, upload the latest Network.WLAN.EWP Setting definition document. See [Uploading the Network.WLAN.EWP Setting Definition Document](#) on page 38.

The version of **Network.WLAN.EWP.setting.xml** required for MSP 3.3 is 6.4 or later.

Installing Microsoft SQL Server Management Studio Express

To back up the MSP database, you must install Microsoft SQL Server Management Studio Express, which is not included in the basic installation of Microsoft SQL Server 2005 Express. You can download it from the following location:

[Download Microsoft SQL Server Management Studio Express²](#)

For more information about how to use Microsoft SQL Server Management Studio Express to back up the MSP database, see *Using Mobility Services Platform*.

Smartphone Files Installed with the Vocera Client Gateway

MSP Server is typically installed on the same computer as the Vocera Client Gateway. When you install the Vocera Client Gateway, the following smartphone-related directories are also installed:

² <http://www.microsoft.com/en-us/download/details.aspx?id=8961>

Table 2.1. Smartphone-related directories on the Vocera Client Gateway

Directory	Description
\\vocera\config\smartphone	Files for configuring Vocera smartphones by tethering them to another computer using a USB cable rather than using Motorola MSP Note: These files are intended for the Vocera smartphone only. They cannot be used to configure other types of devices.
\\VoceraMSP\setup	Files for using Motorola MSP to configure Vocera smartphones over the air. Note: If Vocera Client Gateway and MSP Server are installed on separate machines (whether physical or virtual), you should copy the \\VoceraMSP folder on the Vocera Client Gateway computer and paste it to the root of the drive where MSP is installed on the MSP computer.

Logging into the MSP Console

After you install MSP Server components, you are ready to log into the MSP Console. You can access the MSP Console on the MSP Server or from another computer connected to the network. Motorola recommends using Microsoft Internet Explorer™ versions 6 or 7.

To log into the MSP Console:

1. Launch the Internet Explorer browser.
2. If you are working on the MSP Server computer, enter the following in the Address field of the browser window:

`http://local_machine/MSP.Web`

where *local_machine* is one of the following values: the IP address 127.0.0.1, the name localhost, or the numeric IP address or the DNS name of the local computer.

Note: On the MSP Server computer, you can also launch the MSP Console by choosing **Start > Programs > Motorola MSP > MSP Web Console**, which points to localhost.

3. If you are accessing the MSP Console from any computer other than the MSP Server computer, enter the following in the Address field of the browser window:

`http://msp_server/MSP.Web`

where *msp_server* is either the numeric IP address or the DNS name of the MSP Server.

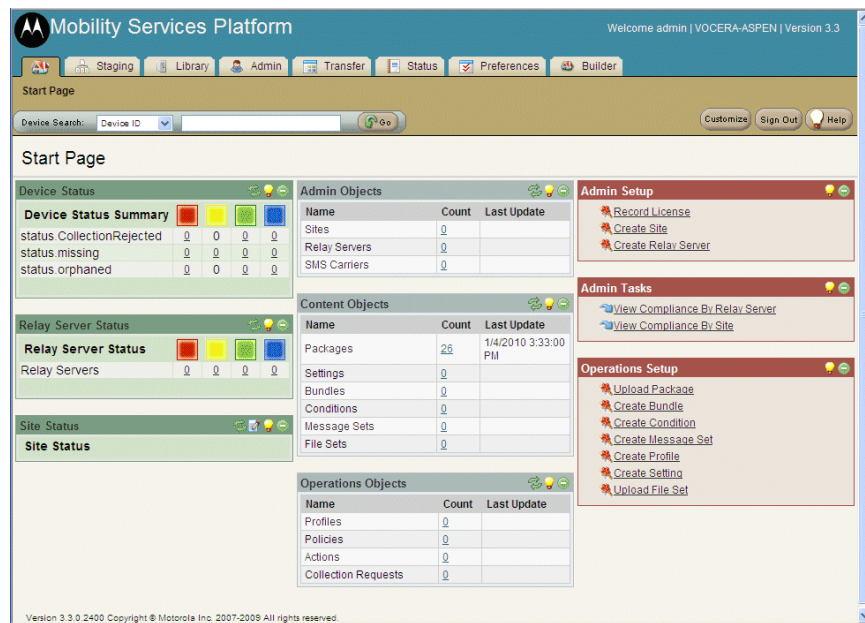
Note: You might want to create a Favorites link (also called a bookmark) in your browser for the MSP Console URL.

- On the Login page, enter the **Username** and **Password**, and then click **Sign In**.

Note: The default username/password is admin/admin.

After you log in, the MSP Console Start Page appears.

Figure 2.19. MSP Console Start Page tab



MSP Console Quick Reference

The following table shows how to perform different operations in the MSP Console UI.

Table 2.2. MSP quick reference

Feature	Location in MSP Console UI
Customization	
Configure "widgets" to streamline your access to the tasks and information most important to you	Start Page
Staging	
Create or view Staging Profiles	Staging > Staging Profiles
View Staging History	Staging > Staging History
Provisioning	
Create or manage provisioning policies	Provisioning > Policy Management
View provisioning compliance information	Provisioning > Compliance Summary Provisioning > Compliance By Relay Server Provisioning > Compliance By Site
Content Objects	
View or upload Package objects	Library > Packages
Create Package objects	Builder > Create Package
Upload a Package template	Builder > Templates > Upload Builder > Upload Template
Create or view Settings objects	Library > Settings
Create or view Bundle objects	Library > Bundles
Create or view Condition objects	Library > Conditions

Feature	Location in MSP Console UI
Create or view Message Set objects	Library > Message Sets
Create or view Attributes	Library > Attributes
Administration	
Create or view user accounts	Admin > User Accounts
Create or view sites	Admin > Sites
Create or view Relay Servers	Admin > Relay Servers
View or upload MSP definition documents	Admin > DefDocs
View MSP license information, or update your license key	Admin > Licensing
Import and Export	
Import CSV data into MSP	Transfer > CSV Import
Export XML data from MSP	Transfer > XML Export
Import XML data into MSP	Transfer > XML Import
Status	
View device status	Status > Device Status
View Relay Server status	Status > Relay Server Status
View site status	Status > Site Status
Preferences	
Create customized views configured by and applicable to each individual user	Preferences > Custom Views
Create default views for users who do not have customized views	Preferences > Global Views



Administrative Setup

This chapter describes the administrative tasks you must perform after installation MSP to prepare the system to be used to update Vocera smartphones.

Copying Files from the Vocera Client Gateway Computer

When you install Vocera Client Gateway, files for using Motorola MSP to configure Vocera smartphones over the air are installed into the following folder:

%vocera_drive%\VoceraMSP\setup

If Vocera Client Gateway and MSP Server are installed on separate machines (whether physical or virtual), you should copy the **\VoceraMSP** folder on the Vocera Client Gateway computer and paste it to the root of the drive where MSP is installed on the MSP computer.

Updating Your MSP License Key

After you finish installing MSP, you may need to update your license key in the MSP Console to enable MSP functionality, particularly Provisioning. For more information, see the separate license key instructions provided by Vocera.

Important: Each time your organization purchases additional smartphones from Vocera, you must update your MSP license key to ensure that you have enough Provisioning seats for them.

To create a license key:

1. Copy the new license key provided by Vocera to the Clipboard.
2. In the MSP Console, click the **Admin** tab.
3. Click **Licensing**.
4. Click **Create**. The License window appears.

5. Paste your new MSP license key into the **License Key** field, and then click **Add**.

Note: After updating the license key, you must log out of the MSP Console and then log back in to enable features activated by the license and to update the License Compliance window.

To delete a license key:

1. In the MSP Console, click the **Admin** tab.
2. Click **Licensing**.
3. Select the check box(es) for the appropriate license, and click **Delete**.

Uploading the Network.WLAN.EWP Setting Definition Document

When MSP is first installed, it lacks a Network Setting definition document for Vocera smartphones. Therefore, to configure network settings for Vocera smartphones, you must upload a file to the MSP Object Library called **Network.WLAN.EWP.setting.xml**.

The **Network.WLAN.EWP.setting.xml** file is located in the following folder on Vocera Client Gateway computer:

%vocera_drive%\VoceraMSP\setup\xml

Note: For PEAP authentication support, make sure the **Network.WLAN.EWP.setting.xml** file is version 6.6 (or later). To view the version of **Network.WLAN.EWP.setting.xml** that is currently installed in the MSP Console, click **Admin > DefDocs**, and then look at the Version column. To view the version of the **Network.WLAN.EWP.setting.xml** file in an XML viewer, open the file in Internet Explorer. The last parameter of the <dataDocDefn> tag is the version.

To upload the Network.WLAN.EWP.setting.xml file:

1. In the MSP Console, click the **Admin** tab.
2. Click **DefDocs**.
3. Click **Upload**.
4. Click **Browse** to select the **Network.WLAN.EWP.setting.xml** file from a local drive.

Note: Do not select the file from a network drive.

5. Click **Upload**.
6. If you are prompted whether to overwrite an existing file, click **Yes**.

Uploading the EWP Persistent REG Install Package Template

One of the common types of packages you need to create in MSP is a package containing registry settings for Vocera smartphones. To create packages for registry settings, you need a special package template called **EWP Persistent REG Install**. You can upload this template from an XML file named **EWP_REG.xml**.

The **EWP_REG.xml** file is located in the following folder on the Vocera Client Gateway computer:

%vocera_drive%\VoceraMSP\setup\xml

To upload the EWP Persistent REG Install Package template:

1. In the MSP Console, click the **Builder** tab.
2. Click **Upload Template**.
3. In the **File Template File** field, click **Browse** and select the **EWP_REG.xml** file from a local drive.

Note: Do not select the file from a network drive.

4. Click **Upload**.
5. The Related Tasks list appears. Select one of the options.

Uploading the Vocera Root Certificate Install Package Template

To install a self-signed certificate on smartphones using MSP, you must first upload a special package template called **Vocera Root Certificate Install**. You can upload this template from an XML file named **Vocera_Cert.xml**.

The **Vocera_Cert.xml** file is located in the following folder on the Vocera Client Gateway computer:

%vocera_drive%\VoceraMSP\setup\xml

Note: If you do not plan to enable SSL on your Vocera system, you can skip this setup task.

To upload the Vocera Root Certificate Install Package template:

1. In the MSP Console, click the **Builder** tab.
2. Click **Upload Template**.
3. In the **File Template File** field, click **Browse** and select the **Vocera_Cert.xml** file from a local drive.

Note: Do not select the file from a network drive.

4. Click **Upload**.
5. The Related Tasks list appears. Select one of the options.

Creating a Relay Server Object

When you create a Relay Server object in MSP, you are providing the information MSP needs to interact with an FTP Server. You should not create the Relay Server object in MSP until the FTP Server already exists. If you followed the instructions to install Microsoft IIS, the IIS FTP Service should already be installed on the MSP Server. For more information, see [Installing Microsoft IIS](#) on page 17

Note: If you create a Relay Server object in MSP before the FTP Server exists, MSP will periodically attempt to contact the nonexistent server, thus unnecessarily increasing the load on MSP and on the network.

By using external relay servers (that is, FTP servers located on computers other than the MSP Server computer), you can distribute the load more effectively and scale the system to support more devices. However, you must ensure that the MSP Server has reliable connectivity with all relay servers. Otherwise, system performance will degrade significantly. For more information on complex deployments using multiple relay servers, see *Using Mobility Services Platform*.

To create a Relay Server Object:

1. Click the **Admin** tab.
2. Click **Relay Servers**.
3. Click **Create**. The Create Relay Servers wizard appears.

Figure 3.1. Create Relay Server wizard

Relay Servers > Create Relay Server

1 SERVER INFO 3 PRIVATE ACCESS INFO 4 PUBLIC ACCESS INFO

1. SERVER INFO

Name:

Description:

Stg/Prov Start Time:

Stg/Prov End Time:

Timezone:

Min Contact (hrs):

Max Jobs:

Next Cancel

4. In the **Name** field, enter a name for the Relay Server. The name does not have to be the actual server name, but it should be meaningful.
5. In the **Description** field, enter a meaningful description of the Relay Server. This box is optional.
6. Use the default settings for the other fields on this screen. Click **Next** to display the Private Access Info page. The Private Access Info page defines the communications between MSP and the FTP Server.
7. In the **Protocol** field, use the down arrow to define the FTP Server Protocol. Select FTP.

Note: Although FTPS is one of the listed protocols, it is not recommended.

8. In the **Server Address** field, enter the IP address of the FTP Server.
9. In the **Port** field, enter the Port address for the FTP Server. The Port defaults to 21, but this may not be correct.
10. Leave the **Path** field blank. MSP will use the Shared Folder or Home Directory of your FTP server to store all the Contents (Packages, Bundles, and network Settings) from your MSP Server.
11. In the **User** and **Password** fields, enter the User ID and Password required to access the FTP Server. For example, the username/password could be vocera/vocera.
12. Make sure the **Public Same As Private** box is checked, which causes the Public Access Info page of the wizard to share the same settings as the Private Access Info page.
13. In the **Passive Mode** field, select **True** (the default) to use the Passive mode.
14. Click **Next** to display the Public Access Info page. The Public Access Info page defines the communications between the FTP Server and the Mobile Devices.

You should not need to change anything on the Public Access Info page because it shares the same information from the Private Access Info page.

15. Click **Finish**.
16. The Related Tasks screen appears. Click **Activate** to activate the new Relay Server.

Important: If you change any part of the Relay Server configuration or move the Relay Server to a different machine after software has already been staged on the phones, you must create a new Relay Server object and then provision it to phones. See [Changing the Relay Server after Staging](#) on page 95.

Creating a Network Settings Object

For each Site object that you create, you should create a Network Settings object. This will be used to configure devices to connect to the wireless network.

To create a Network Settings object:

1. Click the **Library** tab.
2. Click **Settings**.
3. Click **Create**. The Create Setting wizard appears.

Figure 3.2. Create Setting wizard

4. In the **Type** field, select **Network.WLAN.EWP.setting.xml**.

Note: If Network.WLAN.EWP.setting is not listed, you did not upload the required definition document. See [Uploading the Network.WLAN.EWP Setting Definition Document](#) on page 38.

5. In the **Name** field, enter a name for the setting.

Best Practice: Identify the network settings by Site and SSID:
sanjose.taurus

6. Click **Next**.
7. Enter the following network settings:

Table 3.1. Network settings

Field	Description
Description	Enter an optional description for the setting.
SSID	Enter the WLAN network ESSID.

Field	Description
Authentication	<p>Select the Network Authentication type. Depending on your selection, the subsequent options will change.</p> <p>Available authentication types are:</p> <ul style="list-style-type: none"> • Static WEP • IEEE802.1X with Dynamic WEP • WPA-Personal (PSK) • WPA-Enterprise (EAP) • WPA2-Personal (PSK) • WPA2-Enterprise (EAP)
WEP Key Type Selection	<p>Select the type of WEP key:</p> <ul style="list-style-type: none"> • ASCII WEP 40 – keys are set with 5 ASCII characters. • ASCII WEP 104 – keys are set with 13 ASCII characters. • HEX WEP 40 – keys are set with 10 HEX characters. • HEX WEP 104 – keys are set with 26 HEX characters.
Key 0 Key 1 Key 2 Key 3	<p>If you selected WEP in the Authentication field, enter either the hexadecimal or ASCII keys that the access point and Vocera smartphones use to transmit data. Each hexadecimal key is 26 characters, and each ASCII key is 13 characters.</p> <p>The best practice is to enter all four keys. That way, if a security administrator changes the position that the access point uses to transmit, Vocera smartphones will continue to work.</p>
Encryption	<p>Select an encryption type, either TKIP or AES-CCMP.</p> <ul style="list-style-type: none"> • If WPA-PSK or WPA-EAP authentication is selected, select TKIP encryption. • If WPA2-PSK or WPA2-EAP authentication is selected, select AES-CCMP encryption. <p>If your authentication type is Static WEP or IEEE802.1X with Dynamic WEP, the Encryption field is not available.</p>
PSK Key Type Selection	<p>Select either "HEX Pre-Shared Key" or "ASCII Pre-Shared Key". Only needed for WPA-Personal (PSK) or WPA2-Enterprise (PSK).</p>
PSK	<p>If your network uses WPA-Personal (PSK) authentication, specify the ASCII passphrase used by your wireless network. Alternatively, you can also specify the 64-character, hexadecimal value for the pre-shared key.</p>

Field	Description
EAP	Select one of the following the EAP authentication types: <ul style="list-style-type: none"> • TLS • PEAP • LEAP • EAP-FAST
Identity	Specify the authentication username for PEAP, LEAP, EAP-FAST, or IEEE802.1X with Dynamic WEP authentication.
Password	Enter the authentication identity password for PEAP, LEAP, EAP-FAST, or IEEE802.1X with Dynamic WEP authentication.
Disable Identity Protection	If you want to disable identity protection for PEAP or EAP-FAST authentication, select "Yes".
Server Certificate Selection	Select the type of certificate you are using for EAP-TLS or PEAP authentication. Select either "Use Standard CA Certificates" or "Use Custom Certificates." Standard CA certificates are certificates purchased from a trusted certificate authority, such as Go Daddy. Custom certificates are certificates created by your own certificate authority. Note: Do NOT select "Use CEC Certificates" since the device manufacturer CA certificates may not be installed on all Vocera smartphones.
Client Certificate (Issued By)	Enter the name of the issuer of the client certificate for EAP-TLS authentication.
PAC Provisioning Method	Select either Automatic or Manual provisioning of Protected Access Credentials (PACs) for EAP-FAST authentication. The default is Automatic. Important: If you select Manual PAC provisioning, you must create a new PAC on the Cisco ACS and install the PAC file in the Windows folder on smartphones <i>before</i> configuring this setting.
PAC File	If you selected Manual PAC provisioning for EAP-FAST authentication, enter the name of the PAC file. The password for the manual PAC file must be the same as the RADIUS password.
Provision Auto-PAC on Expiry	Select "Yes" to enable automatic provisioning of a new PAC when it expires.

Field	Description
CCKM	<p>If your wireless network has enabled Cisco Certified Key Management, select "Enable".</p> <p>CCKM is a form of fast roaming supported on Cisco access points and on various routers. Using CCKM, Vocera smartphones can roam from one access point to another without any noticeable delay during reassociation. After a smartphone is initially authenticated by the RADIUS authentication server, each access point on your network acts as a wireless domain service (WDS) and caches security credentials for CCKM-enabled client devices. When a Vocera smartphone roams to a new access point, the WDS cache reduces the time it needs to reassociate.</p> <p>By default, CCKM is disabled. In order to take advantage of this feature, your access points must support CCKM and have it enabled, and you must use WPA-PEAP or WPA2-PEAP.</p>

8. Click **Finish**.

9. The Related Tasks list appears. Select one of the options.

Creating a Site Object

Optionally, you can create Site objects in MSP to define locations within the Enterprise where devices are used. For example, if different locations use different WLAN network settings for Vocera smartphones, you should create different sites for them in MSP.

Sites can also use different relay servers. Relay servers can be located anywhere within the Enterprise to meet the needs of devices and to compensate for any connectivity issues or limitations that may exist. In many cases, locating a relay server at a remote site may be the best way to avoid unnecessary traffic over slow links. In other cases, wide area connectivity may be adequate to allow for a centralized relay server.

Although Site objects are optional, they can make your Staging and Provisioning processes simpler and easier to understand, particularly if you deploy devices to different physical locations. If network settings or relay servers vary per location, then you should consider creating Site objects.

Note: Do not confuse MSP Site objects with Vocera Site objects. Although Sites in the Vocera system can be used to identify different physical locations, they are not associated with configuring network settings of devices.

To create a Site object:

1. Click the **Admin** tab.
2. Click **Sites**.
3. Click **Create**. The Create Sites wizard appears.

Figure 3.3. Create Site wizard

The screenshot shows the 'Create Site' wizard interface. At the top, it says 'Sites > Create Site'. Below this, there are two tabs: '1 SITE INFO' and '2 ADDRESS AND CONTACT INFO'. The '1 SITE INFO' tab is active. The form contains the following fields:

- Name:** A text input field.
- Description:** A larger text area with a scroll bar.
- Network Settings:** A search box followed by a dropdown menu currently showing 'No Network Settings Required'.
- Type:** A dropdown menu currently showing 'Both'.
- Relay Server:** A search box followed by a dropdown menu currently showing 'No Relay Server Required'.
- Timezone:** A dropdown menu currently showing 'GMT-5 Eastern US'.

At the bottom of the form are two buttons: 'Next' and 'Cancel'.

4. In the **Name** field, type a unique name for the site. Although the name can be arbitrary, it should be meaningful. You can use periods in the site name (us.west.ca.sanjose), but spaces are not allowed.
5. In the **Description** field, type a description of the Site. This field is optional.
6. In the **Network Settings** field, use the down arrow to select the appropriate network settings. Use the text box next to the drop-down list to search and limit the settings shown in the drop-down list. If you created settings in the Library Settings module, specify those settings. If you do not know the settings or do not want to specify any, select No Network Settings Required.
- See [Creating a Network Settings Object](#) on page 42.
7. In the **Type** field, use the down arrow to specify if the site is Production, Staging, or Both. A Production site is where the mobile devices are actually used. A Staging site is where the settings and software are loaded onto the mobile devices.

Best Practice: If devices will be both staged and used at the same location, select Both for the **Type** field. Otherwise, select Production or Staging.

8. In the **Relay Server** field, use the down arrow to select the relay server that you want to be associated with the Site. Use the text box next to the drop-down list to search and limit the Relay Servers shown in the drop-down list. You can select No Relay Server Required if you choose not to associate a relay server with the Site.
9. In the **Time Zone** field, select the appropriate time zone.
10. Click **Next** to display the Address and Contact Info page.
11. Optionally, enter the appropriate address and contact information for the site.
12. Click **Finish**.

Uploading and Creating Content Objects

This chapter describes how to upload predefined packages for Vocera smartphones, and also create new Content objects to use for staging and provisioning.

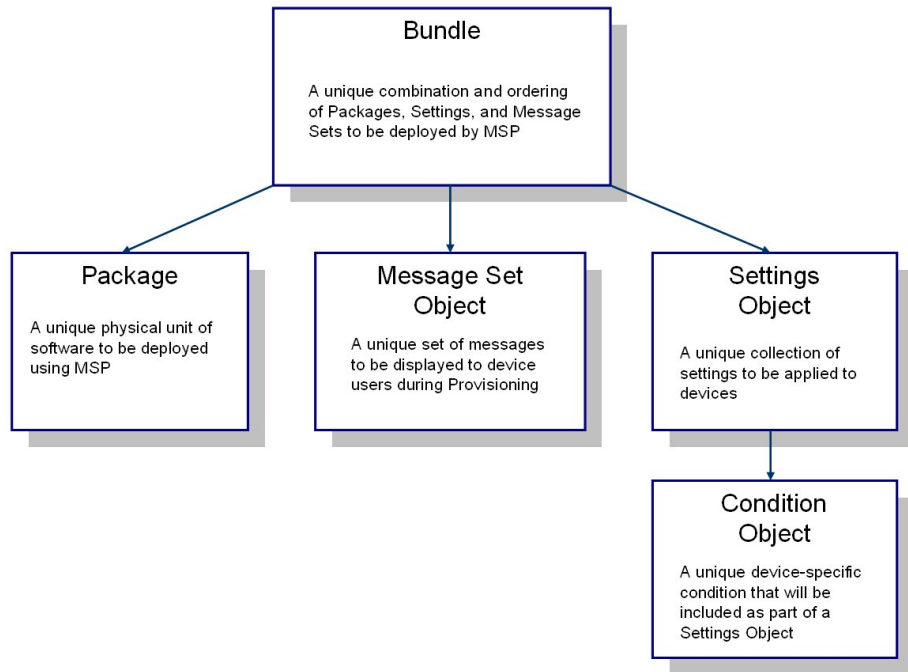
Understanding Content Objects

Content Objects are used to define the information that will be stored in MSP and delivered to devices that are managed by MSP. All MSP users can use Content Objects, but only users with a role of "Operators" or higher can manage Content Objects.

You are ready to create Content Objects as soon as you have defined the Enterprise Objects (Relay Server, Site, Users) needed for your MSP server.

If a Content Object references another Object, the other Object must be created first. The following figure illustrates the various types of Content Objects and identifies which Content Objects reference other Objects and how and when they are most commonly used.

Figure 4.1. Content Objects



Note: MSP comes with several predefined Content Objects to support MSP.

Uploading Packages for Vocera Smartphones

To prepare for staging and provisioning content on Vocera smartphones, you need to upload several predefined packages into the MSP Object Library. You also need to create a package containing the Vocera Client Gateway IP address to configure Vocera smartphones to connect to the Vocera Client Gateway.

When you install Vocera Client Gateway, Vocera provides the following batch file that creates the Vocera Client Gateway IP address package and uploads it and the other predefined packages into the MSP Object Library:

```
%vocera_drive%\VoceraMSP\setup\ vocera  
\upload_packages.bat
```

To upload predefined packages for Vocera smartphones:

1. If Vocera Client Gateway and MSP Server are running on different machines (whether physical or virtual), copy the **%vocera_drive%\VoceraMSP** folder on the Vocera Client Gateway computer, and paste it to the root of the drive where MSP Server is installed on the MSP computer.

2. Run the following batch file on the MSP computer:

```
%msp_drive%\VoceraMSP\setup\ vocera  
\upload_packages.bat
```

Note: This is a simple batch file that provides no error checking. You must enter valid values when you use it. Also, this batch file requires that MSP Server is installed in the default location (%system_drive%\Program Files \Motorola MSP).

3. A Command Prompt window opens, and the batch file prompts for the first VCG IP address.

Type the IP address of the first VCG server in dotted-decimal notation (for example, 192.168.15.10), and then press Enter.

4. The batch file prompts for the second VCG IP address.

Type the IP address of the second VCG server, and then press Enter. If you do not have a second VCG server, press Enter without typing anything.

Respond to other VCG IP address prompts as appropriate.

5. When you finish entering VCG IP addresses, the batch file prompts for the first VS IP address.

Type the IP address of the first Vocera Server, and then press Enter.

6. The batch file prompts for the second VS IP address.

Type the IP address of the second Vocera Server, and then press Enter. If you do not have a second Vocera Server, press Enter without typing anything.

Respond to other VS IP address prompts as appropriate.

7. When you finish entering VS IP addresses, the batch file prompts whether to enable SSL.

Important: You should only enable SSL on Vocera smartphones after SSL has already been enabled on all Vocera Servers.

To enable SSL, type **Yes** and then press Enter. If you do not want to enable SSL, type **No** and then press Enter.

8. Press any key.

9. The script prompts that one file has been moved and several have been copied.

Press any key to close the Command Prompt window.

In a minute or two, the Vocera packages will be visible in the **Library > Packages** page in the MSP Console.

Note: You can update the **VoceraClientGatewayIPAddress** package by running **upload_packages.bat** again. See [Changing the Vocera Client Gateway IP Address](#) on page 92.

Predefined Vocera Packages

The following table describes the predefined packages for Vocera smartphones not included in the default installation of MSP Server:

Table 4.1. Predefined MSP packages for Vocera smartphones

Package	Description
VoceraApps.apf	Installs Vocera Apps, which provides contacts and text messaging functionality.
VoceraCAB.apf	Installs core Vocera functionality.
VoceraClientGatewayIPAddress.apf	Sets the IP address of the Vocera Client Gateway server, which allows Vocera smartphones to communicate with the Vocera Server and the Vocera Telephony Server or Vocera SIP Telephony Gateway. Note: This package is created when you run the upload_packages.bat file.
VoceraJBlendJVM.apf	Updates the JBlend JVM on the device.
VoceraRadio80211d-disable.apf	Disables 802.11d.
VoceraRadio80211d-enable.apf	Enables 802.11d.
VoceraRadioBand-a.apf	Sets the radio to use 802.11a data rates.
VoceraRadioBand-abg.apf	Sets the radio to use 802.11a, b, and g data rates.
VoceraRadioBand-bg.apf	Sets the radio to use 802.11b and g data rates.
VoceraRadioBGChannels-1611.apf	If the device is set to use 802.11b and g data rates, this package sets it to scan only on channels 1, 6, and 11.

Package	Description
VoceraRadioBGChannels-14711.apf	If the device is set to use 802.11b and g data rates, this package sets it to scan only on channels 1, 4, 7, and 11.
VoceraRadioBGChannels-14811.apf	If the device is set to use 802.11b and g data rates, this package sets it to scan only on channels 1, 4, 8, and 11.

Note: There may be additional predefined packages included in subsequent releases.

Creating Settings

Settings objects define configuration changes to be made to a device. Settings objects can be applied directly to devices by referencing them from a Staging Profile. They can also be used as Content by referencing them from a Bundle object as "Content – Setting". For Vocera smartphones, you will typically need to create the following types of Settings objects:

- Clock.DateAndTime Settings
- Network.WLAN.EWP Settings
- Certificate Settings

In the MSP Console, create Settings objects by choosing **Library > Settings > Create**. In the Settings Create wizard, click the **Help** button for assistance.

For an example of how to create a Network Settings object, see [Creating a Network Settings Object](#) on page 42.

For more information about the different types of Settings objects, see *Using Mobility Services Platform*.

Creating a Date and Time Settings Object

To configure the date and time and time zone for Vocera smartphones, you need to create a Date and Time Settings object.

To create a Clock.DateAndTime Settings object in MSP:

1. Click the **Library** tab.
2. Click **Settings**.
3. Click **Create**. The Create Setting wizard appears.
4. In the **Type** field, select **Clock.DateAndTime.setting.xml**.

5. In the **Name** field, enter a name. For example, name the Settings objects after the time zone of the site: **Pacific**, **Mountain**, **Central**, or **Eastern**.
6. Click **Next**.
7. Enter the following date and time settings:

Table 4.2. Date and Time settings

Field	Description
Description	Enter an optional description for the setting.
Set time zone?	Select Set time zone on device .
Select Time Zone	Select the desired time zone from the drop-down list.
Set device clock?	Select Set clock on device .
URL	<p>Specify the URL of a valid Web Server (HTTP Server) reachable from the device. The Web Server must be properly configured with the current date and time. The time zone of the Web Server is irrelevant since the absolute time is used.</p> <p>If the MSP Server is reachable from the device, you can specify an MSP Server URL. The URL would have the form: <code>http://msp_server_ip/MSP.Web/</code> where <i>msp_server_ip</i> is the IP Address of the MSP Server.</p>

8. Click **Finish**.
9. The Related Tasks list appears. Click **View Detail** to view the date and time settings object you created.

Creating a Certificate Settings Object

If you are planning to configure Vocera smartphones for PEAP or EAP-TLS authentication, you will need to install one or more public key certificates on Vocera smartphones *before* you configure the phone's network settings.

To create a Certificate Settings object in MSP:

1. Click the **Library** tab.
2. Click **Settings**.
3. Click **Create**. The Create Setting wizard appears.
4. In the **Type** field, select **Certificate.setting.xml**.

- 5. In the **Name** field, enter a name for the setting.
- 6. Click **Next** to see step 2 of the the Create Setting wizard.

Figure 4.2. Create Setting wizard, Step 2

Settings > Setting Create

1

2

1. Certificate.setting.xml

Name:

PEAPCertSetting

Description:

Device date and time:

Do not change

Certificate Type:

Server

Certificate File:

Browse...

Root Certificate:

False

Enable Certificate 27:

False

Enable Certificate 37:

False

Enable Certificate 47:

False

Enable Certificate 57:

False

Enable Certificate 67:

False

Enable Certificate 77:

False

Enable Certificate 87:

False

Back

Finish

Cancel

- 7. Enter the following certificate settings:

Table 4.3. Certificate settings

Field	Description
Description	Enter an optional description for the setting.
Device Date and Time	Select "Do not change" (the default).
Certificate Type	Select "Server" or "Client."
Certificate File	Click Browse to select the certificate file.
Root Certificate	Select "Yes" or "No" to identify whether the certificate is a root certificate.
Certificate Password	Enter the client certificate password.
Enable Certificate <i>n</i>	Select "True" to add another certificate to the Certificate Setting object. Otherwise, select "False."

- 8. Click **Finish**.
- 9. The Related Tasks list appears. Select one of the options.

Creating a Vocera Server SSL Certificates Package

If SSL is enabled for your Vocera system, you need to install the self-signed certificate from each Vocera Server on each smartphone. Otherwise, the Vocera Apps software, which provides contacts and text messaging functionality, will be unable to connect with the server.

Before you can create a Vocera Server SSL Certificates package, you must first upload a special package template called **Vocera Root Certificate Install** to the MSP Server. See [Uploading the Vocera Root Certificate Install Package Template](#) on page 39.

Note: If SSL is not enabled on your Vocera system, you can skip this section.

To create a Vocera Server SSL Certificates package in MSP:

1. Create a folder to store the SSL certificates on your configuration computer. For example, the folder could be **%vocera_drive%\vocera\config\smartphone\certs**.
2. Copy the SSL certificate from each Vocera Server to the SSL certificates folder on your configuration computer.

On the Vocera Server, the certificate is found in the following folder:

%vocera_drive%\apache\Apache2\conf\ssl

Important: Make sure you copy the certificate with a **.cer** filename extension. The smartphone does not support certificates with a **.crt** filename extension.

3. In the MSP Console, click the **Builder** tab.
4. Click **Create Package**. The Create Package wizard appears.

Figure 4.3. Create Package wizard

The screenshot shows the 'Create Package' wizard interface. At the top, there's a title bar 'Create Package'. Below it, a progress bar shows six steps: 1. PACKAGE INFO (active), 2. GENERAL PACKAGE INFO, 3. PACKAGE FILES, 4. COMMAND DEFINITION, 5. REVIEW, and 6. RESULTS. The main content area for step 1 is titled '1. Package Info' and contains two text input fields labeled 'Name:' and 'Version:'. Below these is a checkbox labeled 'Validate Name/Version in MSP:' which is checked. At the bottom of the form are two buttons: 'Next' and 'Cancel'.

5. In the **Name** field, enter **VoceraServerSSLCertificates**.

6. In the **Version** field, enter a version for the package. Best practice is to enter the IP address for one or more of the Vocera Server computers followed by the date the certificate was created, for example, **10.37.43.101_02-01-11**.

7. Click **Next**.

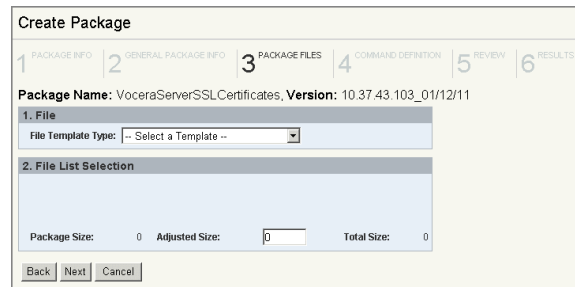
The General Package Info screen appears.

8. On the General Package Info screen, use the default settings. Click **Next**.

9. Click **Next**.

The Package Files screen appears.

Figure 4.4. Package Files scree



10. In the **File Template Type** field, select Vocera Root Certificate Install. The **File To Add** field appears.

11. In the **File To Add** field, click **Browse** to select the Vocera Server certificate file, and then click **Add**.

If you have multiple Vocera Servers, add other certificate files to the package in the same way.

12. After all certificates for your Vocera Servers have been added, click **Next**.

The Command Definition screen appears.

13. On the Command Definition screen, use the default settings. Click **Next**.

The Review screen appears.

14. Review the package settings, and then click **Create Package**.

15. The Related Tasks list appears. Click **Upload to MSP** to upload the package you created to the MSP Server.

Managing SSL Certificates

When you enable SSL on each Vocera Server, a self-signed certificate is generated that is set to expire in 1825 days (5 years). The long duration of the certificate is intended for your convenience so that you do not need to replace it frequently on each Vocera Server and on all Vocera smartphones.

Make sure you update SSL certificates on the Vocera Servers before they expire. See [Creating a New SSL Certificate](#) in the *Vocera Administration Guide*. When you generate new SSL certificates for the Vocera Servers, you need to update your **VoceraServerSSLCertificates** package to provision the certificates to the phones.

You can verify the expiration date of a certificate by opening the certificate file. On the smartphone screen, you can read the expiration date of root Vocera Server certificates that have already been installed.

To view root certificates for Vocera Servers already installed on the smartphone:

1. Press **Start > All Programs > Settings > More (7) > Security > Certificates > Root**.

The Root Certificates dialog box appears.

2. Select a root certificate for the IP address of a Vocera Server—you may need to select **More...** a few times to see it—and press **Menu > View**.

Optional Content Objects

This section briefly describes optional content objects you can add to bundles.

- [Creating Conditions](#) on page 58
- [Creating Message Set Objects](#) on page 59

Creating Conditions

Condition objects are used to test the current state of a device. You can use Condition objects to prevent the MSP Agent on a device from performing an operation until the specified condition is met on that device.

In the MSP Console, create Condition objects by choosing **Library > Conditions > Create**. In the Condition Create wizard, click the **Help** button for assistance.

Condition Objects can be used for the following purposes:

Table 4.4. Condition Object purposes

Purpose	Description
Readiness Conditions	Readiness Conditions in Policies can reference Condition objects to prevent Jobs sent to devices from executing until the conditions are met on each device.
Conditions in Settings	Settings objects can reference Condition objects to configure devices to change their behavior based on conditions in effect on the device. For example, you could have a Condition object referenced by an Agent.30 Settings Object to control when the MSP Agent is allowed to contact the Relay Server. Such conditions are called Check-In Conditions.

For more information about Condition objects, see *Using Mobility Services Platform*.

Creating Message Set Objects

Message Set objects allow you to display messages on a device during Provisioning. When you create a Bundle, you can specify which Message Set objects will be displayed to users of the mobile device when the Bundle is deployed.

In the MSP Console, create Message Set objects by choosing **Library > Message Sets > Create**. In the Message Create wizard, click the **Help** button for assistance.

Note: Message Set objects are only used during Provisioning. They are not used during Staging.

Creating Bundles

Bundle objects are the primary unit of deployment in MSP. Bundle objects define the Deployment Steps to be performed when Content is deployed as part of a Staging Profile or a Provisioning Policy.

In the MSP Console, create Bundle objects by choosing **Library > Bundles > Create**. In the Bundle Create wizard, click the **Help** button for help on the wizard options.

Each Bundle object can specify up to 40 deployment steps. There are three types of deployment steps:

- **Install Package** – Installs a package on the mobile device.
- **Uninstall Package** – Removes a package(s) from the mobile device.

- **Reboot** – Causes the mobile device to be rebooted.

Tip: When you create a Bundle object in the MSP Console, maximize the browser window. Otherwise, MSP Console popup windows may not display correctly.

To create a bundle for Vocera smartphones:

1. Click the **Library** tab.
2. Click **Bundles**.
3. Click **Create**. The Bundle Create wizard appears.
4. On the Bundle Info screen, enter a unique **Name** for the Bundle, such as **VoceraBundle**. Optionally, enter a **Description**.
5. Click **Next** to go to the Deployment Steps screen.
6. Add the bundle steps in the exact order listed in the following table. The final bundle step is a reboot step.

Table 4.5. Vocera smartphone bundle steps

Bundle Step Type	Package Type	Package Name	Reboot Type	Force Install
Install Package	User-Defined	abup30 - dwp_7.02.79 Updates the MSP Agent on devices.	N/A	False
Install Package	User-Defined	DateAndTime Control module that enables the date, time, or time zone to be set on devices using MSP.	N/A	False
Install Package	User-Defined	GetAdapters Control Module to report active adapters. Needed to create custom device status views that include the MAC address and IP address.	N/A	False
Install Package	Content - Setting	Clock.DateAndTime - TimeZone Sets the date, time, and time zone on devices. See Creating a Date and Time Settings Object on page 53.	N/A	False

Bundle Step Type	Package Type	Package Name	Reboot Type	Force Install
Install Package	User-Defined	enable30 - 2.0 Updates the MSP Agent on the device to check in with the relay server every 15 minutes. Important: There are two packages named enable30 on your MSP Server. Use the enable30 package version 2.0. This is the version that is signed.	N/A	False
Install Package	User-Defined	VoceraJBlendJVM Updates the JBlend JVM on the device.	N/A	False
Install Package	User-Defined	VoceraClient- GatewayIPAddress Sets the IP address of the Vocera Client Gateway server, which allows Vocera smartphones to communicate with the Vocera Server and the Vocera Telephony Server or Vocera SIP Telephony Gateway. This package must be added before VoceraCAB in the Vocera bundle. See Uploading Packages for Vocera Smartphones on page 50.	N/A	False
Install Package	User-Defined	VoceraServer- SSLCertificates Installs root Vocera Server SSL certificates to the certificate store of phones. This package should only be installed if SSL is enabled on all Vocera Servers. Otherwise, it should not be included in the bundle. See Creating a Vocera Server SSL Certificates Package on page 56.	N/A	False
Install Package	User-Defined	VoceraCAB Installs core Vocera functionality.	N/A	False
Install Package	User-Defined	VoceraApps Installs Vocera Apps, which provides contacts and text messaging functionality.	N/A	False

Bundle Step Type	Package Type	Package Name	Reboot Type	Force Install
Install Package	User-Defined	<p>[One or more of the predefined VoceraRadio packages]</p> <p>Optionally, add one or more of the predefined VoceraRadio packages here to set the device radio to use 802.11 a, b, or g data rates and scan on specific channels.</p> <p>See Uploading Packages for Vocera Smartphones on page 50.</p>	N/A	False
Install Package	Content - Setting	<p>Network.WLAN.EWP.Site.SSID</p> <p>Sets network settings on devices.</p> <p>See Creating a Network Settings Object on page 42.</p>	N/A	False
Install Package	Content - Relay Server	<p>RelayServer</p> <p>Sets the Relay Server to use.</p> <p>See Creating a Relay Server Object on page 40.</p>	N/A	False
Reboot	N/A	N/A	Warm with RegMerge	N/A

To add a bundle step, click the **Add Step** button. The Bundle Step Add page appears.

Figure 4.5. Bundle Step Add page

Bundle Step Add

Type of Step: ☒ Install Package ☐ Uninstall Package ☐ Reboot

Package Type: ☒ User-Defined ☐ Content - Setting ☐ Content - Relay Server

Package Name: abup30 - ddd_7.02.79

Additional: ☐ Force Install ☐ Disconnect

Add Bundle Step Cancel Add

Complete the options for each bundle step according to the information in the above table.

For each bundle step, make sure the **Disconnect** box is unchecked. This ensures that the device does not disconnect from the relay server before the installation command is executed.

When you are finished defining a bundle step, click **Add Bundle Step**.

7. After you finish adding bundle steps, click **Finish**.

8. The Related Tasks screen appears. If you are ready to create a staging profile, click **Create Profile**. This will automatically associate the new staging profile with the user-defined staging bundle.

Using Production Site Bundles

When you define a Production Site (a Site object whose type is Production or Both), MSP automatically creates a Bundle for that Site. This is known as a Production Site Bundle, and it includes Settings Packages for the Network Settings Object and/or Relay Server Object, if any, referenced by that Site.

If you deploy a Production Site Bundle to a device, the Network Settings Object and/or Relay Server Object referenced by that Site are applied to the device, and the device is assigned to that Site.

Using Staging to Configure Vocera Smartphones

This chapter describes the Staging process. Staging is the process of initially configuring and installing software on a mobile device by initiating a request from the device. Each Staging operation is defined by creating a unique Staging Profile object. Staging settings, such as Network Settings and Relay Server Settings, can be deployed early in the Staging operation, followed by Staging Content objects (Packages and Settings), which are deployed from a Bundle. When the Staging operation is finished, the Vocera smartphone can be updated remotely under the control of the MSP Server using Provisioning.

Staging Prerequisites

There are several prerequisites for staging:

- Install .NET Framework 2.0 SP2 on the configuration computer.

See [Installing .NET Framework](#) on page 21

- Install **Windows Mobile Device Center** or **Microsoft ActiveSync** on the configuration computer.

Both Windows Mobile Device Center and Microsoft ActiveSync are free programs that let you synchronize data and information between your computer and a Windows Mobile device, such as a Vocera smartphone. These applications can also be used to copy files from your computer to Vocera smartphones.

- Obtain a USB cable to connect the phone to the USB port of the configuration computer.
- Vocera smartphones must be available for staging. Staging is an on-demand procedure, so each device must be manually set to begin the staging process.
- Make sure the Relay Server is active. If it is not, click **Activate** in the Related Tasks list.

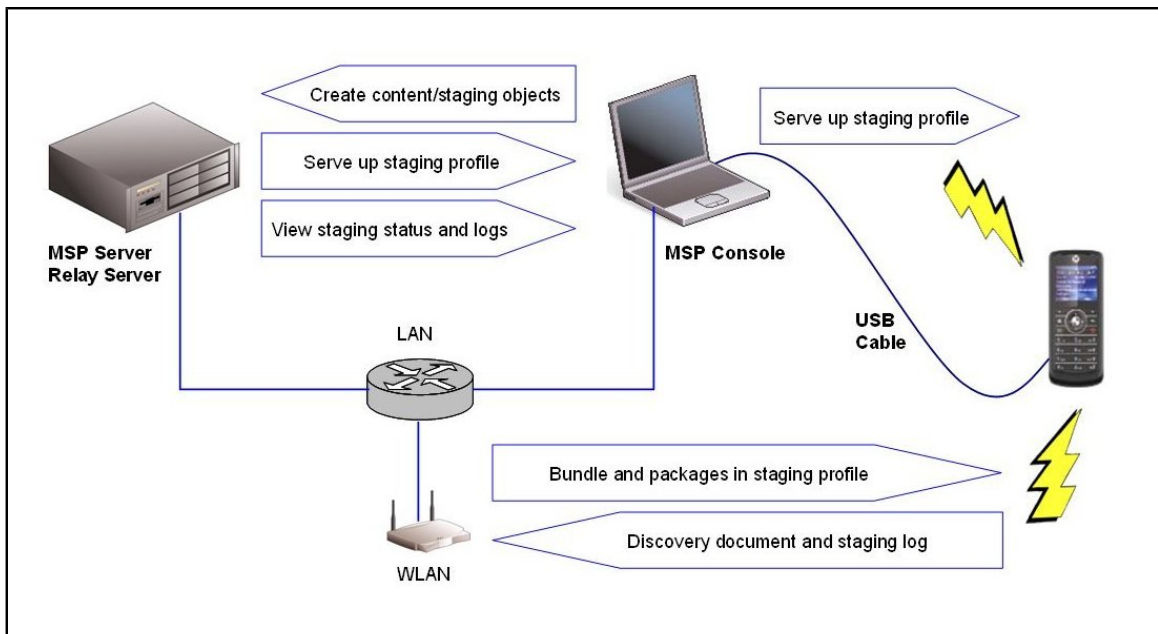
- At least one Staging Profile must be made available to Vocera smartphones. Click the **Staging** tab in the MSP Console and find the Profile in the list of Profiles. To turn on the staging server for that Staging Profile, click the **On Demand** link in the Method column.

How Staging Works

Vocera smartphones support On-Demand (Electronic) Staging. Barcode-based Staging and SMS Staging are not supported.

The following figure illustrates the On-Demand Staging method.

Figure 5.1. On-demand staging of Vocera smartphones



On a configuration computer, an MSP user connects the phone to the computer using a USB cable. The user then runs the MSP Console in an Internet Explorer window, which connects to the MSP Server. In the MSP Console, the user clicks the **On Demand** link for the Staging Profile, which launches a special page known as the On Demand Server that receives Profiles from the MSP Server and provides them to mobile devices. On the On Demand Server page, the user turns on the staging server by clicking the **Turn Staging server on** button.

Now the user can turn on the tethered Vocera smartphone, start the Rapid Deployment client, and select **Search Connected Networks** to download the Staging Profile from the computer. The Rapid Deployment client configures the device as specified by the staging profile, contacts the relay server running on the same computer as the MSP Server, downloads the bundle, and performs the deployment steps.

During the staging process, the Rapid Deployment client on the Vocera smartphone pushes the following files to the relay server:

- a **discovery document** (.XML file) describing the device to the DISCOVERY subfolder on the relay server
- a **staging log** (.completed or .failed file) describing the results of the staging operation to the LOGS subfolder of the relay server

The MSP Server pulls the discovery document from the relay server and adds the device to the Staging History list. It also pulls the staging logs and stores them in the MSP Database.

In the MSP Console, a user can see which devices have been staged by choosing **Staging > Staging History**. For any device, the user can also check the staging logs to troubleshoot any staging issues.

Creating a Staging Profile

The Staging Profile object defines the types of Staging operations to be performed on devices using MSP. It can reference settings objects, a Relay Server object, and other content.

To create a staging profile:

1. Click the **Staging** tab. The Staging Profiles pages is selected by default.
2. Click **Create**. The Profile Create wizard appears.

Figure 5.2. Profile Create wizard

The screenshot shows the 'Profile Create' wizard with four tabs: 1 PROFILE INFO, 2 STAGING SETTINGS, 3 DEPLOYMENT STEPS, and 4 STAGING OPTIONS. The first tab is active, showing three sections:

- 1. Name and Describe the Profile**: Contains a 'Name:' text field and a 'Description:' text area.
- 2. Specify Device Attributes**: Contains a 'Device Model:' dropdown menu set to 'ANY', an 'OS:' dropdown menu set to 'ANY', and a 'Wireless LAN:' dropdown menu set to 'ANY'.
- 3. Staging Settings**: Contains a description and two radio buttons: 'Select pre-defined settings' (selected) and 'Inherit from site'.

At the bottom of the first tab are 'Next' and 'Cancel' buttons.

3. Enter a **Name** and **Description** for the staging profile. The name is required.
4. In the **Specify Device Attributes** pane, use the default setting, ANY.
5. In the **Network Access Settings** pane, select whether to **Select Pre-defined settings** or **Inherit from Site** to get the network settings from the site where the devices are staged. Select **Inherit from Site** if you associate a network setting with a site.
6. Click **Next**. The Staging Settings page appears. This page displays different choices depending on whether you selected **Select pre-defined settings** or **Inherit from site** on the previous page.

If you selected **Select pre-defined settings** on the previous page, specify the **Network Access Setting** and the **MSP Relay Server Setting** fields by selecting the correct values from the drop-down lists.

If you selected **Inherit from site** on the previous page, select the **Staging Site** and the **Production Site** options. You can choose to specify a site explicitly, or specify the site at staging (also known as Late Site Binding).

If you need assistance, click **Help**.

7. In the **Additional Settings Options** pane, DO NOT select any additional settings. If any are selected, click **Clear Additional Settings**.
8. Click **Next**. The Deployment Steps page appears.
9. In the **Bundles** pane, select **User-Defined**, and then select the bundle you created earlier from the drop-down list.
10. Click **Next**. The Staging Options page appears.
11. In the **Bar Code Staging** pane, uncheck the **Allow Bar Code Staging** box. Bar Code Staging is not supported on Vocera smartphones.
12. In the **Electronic Staging** pane, check the **Allow Electronic Staging** box.
13. In the **Automatic Staging** pane, make sure the **Enable Automatic Staging** box is unchecked. Automatic staging is not recommended for Vocera smartphones.
14. Click **Finish**.
15. The Related Tasks screen appears. Click **View Detail** to review the profile you created.

Creating a Staging Profile Without Network Settings

You cannot stage PEAP network settings on a smartphone with firmware that does not support PEAP. For example, if you are staging new smartphones for PEAP authentication and the phones have firmware earlier than version 2.1.1, you should NOT include network settings in the staging profile.

On Step 2 of the Profile Create wizard, make sure you select "Network Settings Not Applicable" for the **Network Access Setting** field.

Figure 5.3. Profile Create wizard, Step 2

The screenshot shows the 'Profile Create' wizard at Step 2, 'Staging Settings'. The breadcrumb trail at the top is 'Staging Profiles > Profile Detail > Profile Create'. The wizard has four steps: 1. PROFILE INFO, 2. STAGING SETTINGS (active), 3. DEPLOYMENT STEPS, and 4. STAGING OPTIONS. In Step 2, the '1. Name' section has a text field with 'MyStagingProfile'. The '2. Network Access Setting' section has a dropdown menu set to 'Network Settings Not Applicable'. The '3. MSP Relay Server Setting' section has a dropdown menu set to 'MyRelay'. To the right of these settings is a large empty box labeled '4. Additional Settings Options' with buttons for 'Add', 'Move Up', 'Remove', and 'Move Down'. At the bottom are 'Back', 'Next', and 'Cancel' buttons.

Important: When you stage the smartphone using a staging profile without network settings, keep the phone tethered to the configuration computer during the entire staging process.

How to Use Staging

After you have prepared a staging Bundle and created one or more Staging Profiles, you are ready to configure Vocera smartphones using On-Demand Staging. Before turning on the staging server in the MSP Console, gather the phones you want to configure.

To perform On-Demand Staging on Vocera smartphones:

1. On the configuration computer, run the MSP Console and create the Content objects needed for staging. These include:
 - Site and Relay Server objects as necessary
 - Package objects
 - Settings objects
 - A Bundle object that describes the exact deployment steps, installing any required Packages or Settings objects, as well as uninstalling any desired Packages, all in the proper, relative order.

For more information about bundles, see [Creating Bundles](#) on page 59.

2. Create a Staging Profile that references the Bundle, network settings, the Relay Server, and any other Settings objects.

See [Creating a Staging Profile](#) on page 67.

3. In an Internet Explorer window, log into the MSP Console, which connects to the MSP Server.

The URL for the MSP Console is:

`http://msp_server/MSP.Web`

where *msp_server* is either the numeric IP address or the DNS name of the MSP Server.

4. In the MSP Console, click the **Staging** tab, and then click the **On Demand** link for the Staging Profile.

Note: If this is the first time you are staging a phone on this computer, a security warning appears asking if you would like to install **onDemand.dll**. Click **Install**. The **onDemand.dll** file, which is also known as the On Demand Server, receives Profiles from the MSP Server and provides them to mobile devices.

5. The Staging Server page appears. It indicates that the staging server is turned off.

Figure 5.4. Staging server is turned off



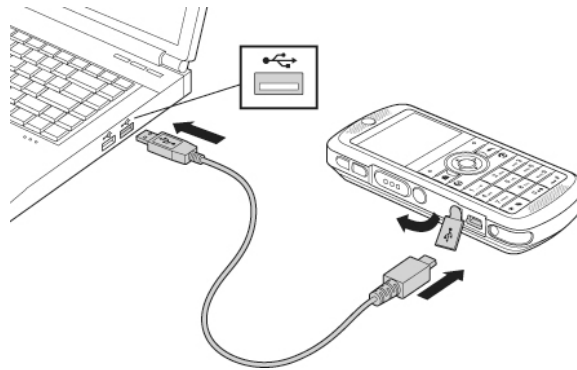
6. Click the **Turn Staging server on** button. The Staging Server page now shows that the staging server is turned on.

Figure 5.5. Staging server is turned on



7. Using a USB cable, plug a Vocera smartphone into your computer, as shown in the following figure.

Figure 5.6. Connecting the phone to a computer



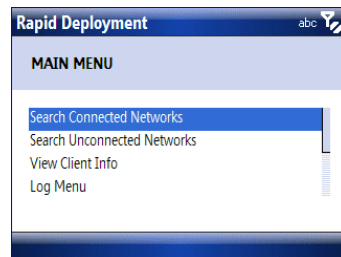
8. If you have **Windows Mobile Device Center**:

When the Windows Mobile Device Center window appears, click **Connect without setting up your device**.

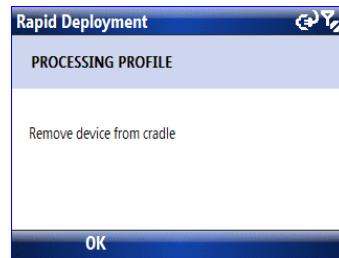
If you have ActiveSync:

- a. If Microsoft Outlook is *not* installed on the computer, you are prompted that you can synchronize only non-Outlook items. If so, click **OK**.
 - b. When the Synchronization Setup Wizard appears, click **Cancel**. The Microsoft ActiveSync window appears. Leave the Microsoft ActiveSync window open.
9. On the Vocera smartphone, press **Start > All Programs > Rapid Deployment**.
- Note:** If the Rapid Deployment shortcut is missing, either copy it from the configuration computer to the **\Windows\Start Menu** folder of your phone (see [Restoring the Rapid Deployment Client Shortcut](#) on page 127), or use File Manager to run the **\Windows\rdclient.lnk** file on the phone. **DO NOT** run the **\Windows\rdclient.exe** file as it defaults to barcode scanning, which is not supported on the phone.
10. Select **Search Connected Networks**, which causes the Rapid Deployment client to try all connected adapters, including USB, to locate an On-Demand Profile Server.

Figure 5.7. Rapid Deployment - Search Connected Networks



11. The Rapid Deployment client locates the On Demand Server running on the computer and downloads a Staging Profile from it.
- Note:** If the MSP staging server has been turned on for multiple Staging Profiles, you will be prompted at this point to select a profile.
12. If your staging profile contains network settings, you are prompted to remove the device from the cradle.

Figure 5.8. Rapid Deployment - Remove device prompt

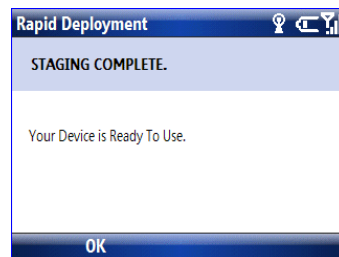
You can disconnect the device from the USB cable. At this point, you can connect another phone to stage it. Follow steps Step 7 through Step 12.

Note: If your staging profile does NOT contain network settings, keep the phone tethered to the configuration computer during the entire staging process.


13. The Rapid Deployment client configures the device as specified by the Staging Profile, contacts the Relay Server specified in the Staging Profile, downloads the Bundle, and performs the deployment steps, including installing or uninstalling Packages or performing specified reboot(s).

Note: If Staging fails on the device for any reason, repeat steps Step 7 through Step 12 again until Staging succeeds.

14. When Staging is finished on each phone, the Rapid Deployment client displays the following dialog box:

Figure 5.9. Rapid Deployment - Staging Complete dialog box

Press **OK** (the left soft key).

15. Press **Start**. A new MSP Agent status icon  appears in the status bar at the top of the screen, indicating that the MSP Agent is running and will check for updates that are provisioned for the device.

Note: After a phone has been staged, the Rapid Deployment and MSP Agent shortcuts (but not the client applications) are removed from the Start screen of the phone to prevent users from accidentally misconfiguring the phone.

Viewing Staging Status

If you staged content on one or more Vocera smartphones, you can view the staging status in the MSP Console. A device appears in the Staging History only when it successfully completes Staging and uploads a Staging Log to the Relay Server where it can be obtained by the MSP Server.

To view staging status:

1. Click the **Staging** tab.
2. Click **Staging History**.
3. Click the link to a device in the **Device ID** column to display the Detail page for the device, which provides detailed information regarding the device and the Staging performed for it.

Best Practices

Follow these best practices when staging content for Vocera smartphones:

- To simplify the staging and provisioning of Content on Vocera smartphones, use the same bundle for both. You can then update the bundle when you receive subsequent software updates from Vocera or when you need to change device settings.
- Include Settings objects in a Bundle to make them persistent.

If the Settings need to be Persistent, and cannot be inherited from a Production Site, then they should be included in the Bundle referenced by the Profile rather than add Additional Settings to the staging profile.

- Use Production Site Bundles to simplify Bundles needed for Staging and Provisioning.

If you use Production Site Bundles, you do not need to include site-specific network settings and relay server settings in the Staging Content Bundle. At the end of the Staging process, after the Staging Content Bundle has been deployed, the Production Site Bundle for that Site will also be automatically deployed. See [Using Production Site Bundles](#) on page 63.

For more information about these recommendations, see *Using Mobility Services Platform*.

Using Provisioning to Update Vocera Smartphones

Provisioning is the installation and configuration of software onto mobile devices *remotely* by the MSP Server. Once Vocera smartphones have gone through Staging, they are enabled for Provisioning. Provisioning requires no action by the device user; it is controlled entirely by the MSP Server and the MSP administrator.

Provisioning Prerequisites

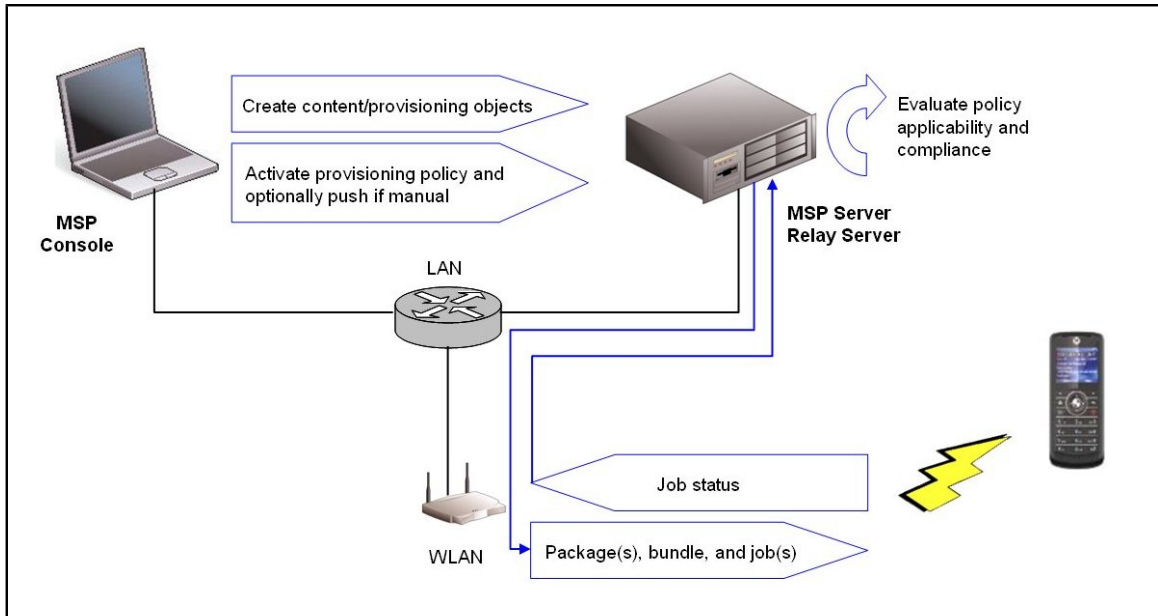
Before you can perform Provisioning on Vocera smartphones, the following prerequisites must be met:

- **MSP Provisioning Seats Are Available for Each Smartphone** – Each time your organization purchases additional smartphones from Vocera, you must update your MSP license key to ensure that you have enough Provisioning seats for them. See [Updating Your MSP License Key](#) on page 37.
- **Devices Are Already Staged** – The devices must have been previously staged to configure them to connect to the production WLAN.
- **Provisioning Bundle is Ready** – A Bundle object must be created that contains the settings and content to install on the devices. This is likely the same Bundle object used for staging.
- **Provisioning Policy Object is Ready** – A Provisioning Policy object must be created that defines the types of Provisioning operations to be performed on devices.

How Provisioning Works

The following figure illustrates provisioning of Content objects for Vocera smartphones.

Figure 6.1. Provisioning content onto Vocera smartphones



The Provisioning process is driven by the Provisioning Policy, which defines the types of Provisioning operations to be performed on devices and establishes which devices are applicable.

- A Policy is either active or inactive. You cannot edit or delete a Policy unless it is inactive.
- To determine if a device is compliant, MSP evaluates the Bundle referenced by the Policy and checks to make sure all the deployment steps in the bundle have been deployed.
- There are two types of provisioning Policies: **On-Going** and **Manual**. If the type is On-Going, MSP automatically sends Jobs to noncompliant devices as needed. If the type is Manual, someone must use the MSP Console to push Jobs out to devices. Vocera recommends using On-Going Policies.
- If a Policy fails for a device, MSP stops evaluating the Policy for that device. This prevents Jobs from being continuously sent to the devices where they will simply fail.

Creating a Provisioning Bundle

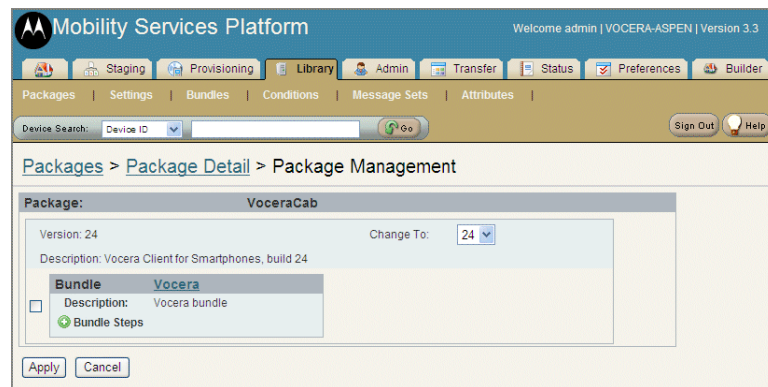
The packages that you use for a provisioning Bundle can be the same as the ones used to stage Vocera smartphones. For information on how to create the Bundle and the typical packages and settings that should be included in it, see [Creating Bundles](#) on page 59.

Managing Package Versions

Although you can edit a Bundle to remove one version of a Package and add another version, this can be time-consuming process if the same Package is referenced by many Bundles. Also, any active Policies that reference the Bundle must be deactivated before you can edit the Bundle.

If you need to modify a Bundle to use a different version of a particular Package, use the Package Management page in the MSP Console.

Figure 6.2. Package Management page



To change the version of a Package used in a Bundle:

1. Click the **Library** tab in the MSP Console.
2. Click **Packages**.
3. Click the Package you want to manage. The Package Details page appears.
4. In the **Related Tasks** list, click **Manage**. The Package Management page appears.
5. In the **Change To** drop-down list, select the version you want to use.
6. For each Bundle that you want to use the selected version of the Package, check the box next to the Bundle name.
7. Click **Apply**.

Important: By default, all Policies that are affected by changes to Bundles using the Package Management feature are automatically deactivated before the changes are made to each Bundle. You can reactivate these afterwards to cause them to deploy the new Package versions.

Creating a Provisioning Policy

A Provisioning Policy is an object that controls how a Bundle is provisioned to devices. The Policy references the Bundle, which contains the settings and packages to install, and it establishes which devices are applicable.

To create a provisioning Policy:

1. Click the **Provisioning** tab.
2. Click **Policy Management**.
3. Click **Create**. The Policy Create wizard appears.

Figure 6.3. Policy Create wizard

The screenshot shows the 'Policy Create' wizard in the 'Policy Management' section. The wizard is divided into five steps: 1. POLICY INFO, 2. APPLICABILITY RULES, 3. DEPLOYMENT STEPS, 4. READINESS CONDITIONS, and 5. DETACHED CONDITIONS. Step 1 is the active step, titled '1. General Policy Details'. It contains the following fields and controls:

- Name:** A text input field.
- Description:** A larger text area with a scroll bar.
- Type:** A dropdown menu currently set to 'On-Going'.
- Pause/Resume:** Radio buttons for 'True' and 'False', with 'False' selected.
- Compl. Activity Max:** A text input field containing the value '10'.
- Buttons:** 'Next' and 'Cancel' buttons at the bottom.

4. Enter a **Name** and a **Description** for the Policy.
5. In the **Type** box, select **On-going** to provision automatically, or select **Manual** if you want an MSP user to push the policy to devices.
6. For **Pause/Resume**, select **True** to specify that if a job is interrupted because of a connectivity problem, it will resume when connectivity is restored.
7. Click **Next** to go to the Applicability Rules page.
8. For **Rule Type**, select **Affect All Devices** or **Custom Rule**.

If you select **Custom Rule**, the Custom Rule Builder window appears. Optionally, construct a rule so that the Policy applies only to a set of devices, such as Vocera smartphones. If you need assistance at any time, click **Help**. For example, the following rule causes the provisioning policy to apply only to Vocera smartphones.

```
identity.deviceModel = 'Moto EWP'
```

Note: If 'Moto EWP' is not a value listed in the Value drop-down list, you can type the value.

9. Click **Next** to go to the Deployment Steps page.
10. In the **Deployment Type** pane, select **Bundle**.
11. In the **Bundles** pane, select **User-Defined**, and then select the user-defined bundle (for example, "VoceraBundle") from the drop-down list.

Note: The packages that you use for a provisioning Bundle can be the same as the ones used to stage Vocera smartphones. Use the Package Management page of the MSP Console to update package versions for provisioning.

12. Click **Next** to go to the Readiness Conditions page.
13. Apply Conditions to the Policy by selecting them in the left pane and moving them to the right pane with the Arrow button.
For information on creating Conditions, see [Creating Conditions](#) on page 58 and *Using Mobility Services Platform*.
14. Click **Finish**.
15. The Related Tasks screen appears. If you are ready to activate the Policy, click **Activate**. Otherwise, you can activate it later on the Policy Management page.

How to Use Provisioning

Once you create a provisioning Policy, you are ready to activate it to begin updating Vocera smartphones. By default, Vocera smartphones check in with the Relay Server every 15 minutes for updates, so it may take longer to provision updates to smartphones than badges.

To activate a Policy:

1. Click the **Provisioning** tab.
2. Click **Policy Management**.

3. For any inactive policy, click the **Activate** link in the **Modify Status** column.

To edit or delete a Policy:

1. Click the **Provisioning** tab.
2. Click **Policy Management**.
3. If the policy you want to edit or delete is active, click the **Deactivate** link in the **Modify Status** column.
4. Click the policy to edit or delete.
5. Click **Edit** or **Delete** in the Related Tasks list.

Viewing Provisioning Status

You can view the results of provisioning on the Compliance Summary pages of the **Provisioning** tab. Click the following links to view provisioning status:

- **Compliance Summary** – view provisioning status by Policy
- **Compliance by Relay Server** – view provisioning status by Relay Server
- **Compliance by Site** – view provisioning status by Site

Best Practices

Follow these best practices when provisioning updates for Vocera smartphones:

- Use the same Bundle for Staging and Provisioning.

The Bundle that you use for Provisioning can be the same one used for Staging, with newer versions of some packages.

- For a planned change to VLAN security settings, provision new network settings to move devices to another VLAN temporarily.

If you plan to make a change your VLAN security settings, you should first provision new network settings to move the mobile devices to another VLAN temporarily. After the original VLAN security settings have been updated, you can provision network settings again to switch the devices back to the original VLAN.

- Avoid frequently activating and deactivating On-Going Policies.

When you activate an On-Going Policy, Jobs are sent to devices. When you deactivate it, cancellation files are sent. To reduce traffic, only activate or deactivate On-Going Policies when necessary.

- Use the Package Management page in the MSP Console to effectively manage package versions for Provisioning. See [Managing Package Versions](#) on page 77.

If you receive an updated package from Vocera that you need to provision to devices, the Package Management feature allows you to selectively change the version of a Package used in a Bundle.

- Use Applicability Rules so Provisioning Policies apply only to Vocera smartphones

You can specify the rule **identity.deviceModel='Moto EWP'** to make a Policy applicable only to Vocera smartphones.



Verifying Smartphone Configuration

This chapter describes how to verify whether a Vocera smartphone has been configured correctly.

Testing the Smartphone

This section describes how to test a smartphone after it has been configured, and helps you troubleshoot problems connecting to the network or to the Vocera Client Gateway.

To verify that you can log into Vocera and make a call:

1. After configuring the phone, remove the USB cable from the phone to disconnect it from the configuration computer.

If the phone is still rebooting, wait until it is completely finished. This may take a couple minutes.

2. When the phone is finished starting up, the Vocera Apps screen appears.

Press the **Home** key to display the Home screen. It should look like one of the following screens:

- a. **Successful Startup:** If the phone is configured properly, it will connect to your Vocera Client Gateway and will display "Logged Out" in the center of the screen.

Figure 7.1. Phone after successful startup



If you see "Logged Out" in the center of the screen, proceed to the next step to log in.

- b. **Searching for Gateway:** If the Vocera Client Gateway IP address is wrong, the phone will display "Searching for Gateway" in the center of the screen:

Figure 7.2. Phone stuck "Searching for Gateway"



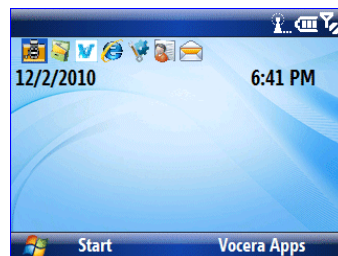
Make sure the Vocera Client Gateway IP address and port that you configured the phone with are correct, and make sure the Vocera Client Gateway is running. The "Searching for Gateway" message could also appear if the phone is unable to connect to the Vocera Client Gateway, or if the Vocera Client Gateway is not running or cannot connect to the Vocera Server.

You can verify the Vocera Client Gateway IP address and port that the phone is using in the Vocera Smartphone Information application. See [Viewing Smartphone Information](#) on page 86.

If this problem occurs, you may need to reconfigure the phone.

- c. **No Network Connection:** If the wireless network settings on the phone are wrong, the phone will display nothing in the center of the screen:

Figure 7.3. Phone with no network connection



If this problem occurs, you may need to reconfigure the phone. It could occur for one or more of the following reasons:

- The SSID is specified incorrectly, perhaps in the wrong case.
- The WEP key index is wrong.
- The pre-shared key is specified incorrectly.
- There is an encryption mismatch between the phone and the access points.
 - If WPA-PSK or WPA-EAP authentication is selected, select TKIP encryption.
 - If WPA2-PSK or WPA2-EAP authentication is selected, select AES-CCMP encryption.
- The specified username or password is incorrect.
- The certificate is not installed in the smartphone's certificate store.
- The CCKM setting on the phone is inconsistent with the CCKM setting on the access points.

You can view wireless network information and security information in the Vocera Smartphone Information application. See [Viewing Smartphone Information](#) on page 86.

3. If the phone started up successfully, put the phone to your ear—by default, the phone is in handset mode—and press the Call button on the side of the phone. Wait for the Genie to answer.
 - **If the Genie asks for your name**, say your first and last names.
 - **If the Genie answers by saying "Vocera" or by playing a tone**, say "Log me in as *<your first and last name>*" (for example, "Log me in as *John Smith*").
4. After logging in successfully, try to make a call. Press the Call button on the side of the phone, wait for the Genie to answer, and then say:
Call <person's first and last names>.
5. After verifying that the phone can make calls, press **Vocera Apps**. Make sure the **Favorites** and **Company Directory** apps work.

If the application is unable to connect, the screen displays "Lost Connection." If this happens, make sure port 80 or 443 (if SSL is enabled) of the Vocera Server is accessible from the phone.

Viewing Smartphone Information

The smartphone has an application called **Vocera Smartphone Information** that allows you to view the following categories of information:

- wireless network information
- Vocera Client Gateway information
- wireless security information
- version information

The Vocera Smartphone Information application also allows you to upload smartphone logs to an FTP server.

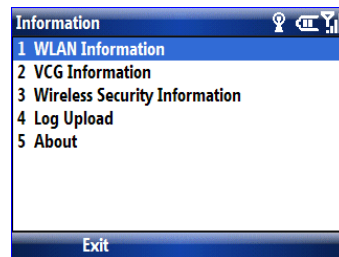
Note: The Vocera Smartphone Information application replaces the Vocera SP About application provided in earlier releases.

To view Vocera Smartphone information:

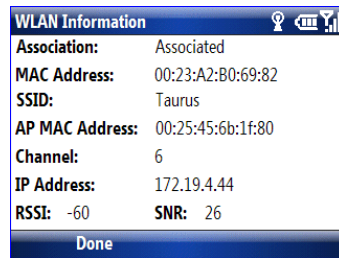
1. Press **Start > All Programs > Vocera Smartphone Information**.

The Information dialog box appears.

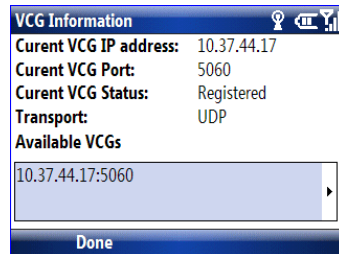
Figure 7.4. Information dialog box



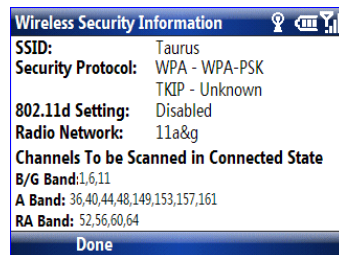
2. Select one of the Smartphone Information categories:
 - **WLAN Information** – The WLAN information is updated every half-second, displaying real-time wireless network information. It displays whether the phone has associated with an AP, the SSID, the phone's MAC and IP address, the AP MAC address and current channel, and signal strength (RSSI) and signal-to-noise (SNR) values.

Figure 7.5. WLAN Information dialog box

- **VCG Information** – Displays the current Vocera Client Gateway IP address(es) and ports, and whether the phone has registered with the gateway.

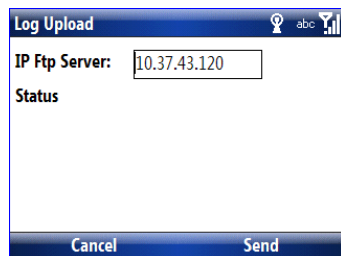
Figure 7.6. VCG Information dialog box

- **Wireless Security Information** – Displays the SSID, the type of authentication and encryption, whether 802.11d is enabled, which 802.11 data rates are being used, and which channels are scanned for different radio bands.

Figure 7.7. Wireless Security Information dialog box

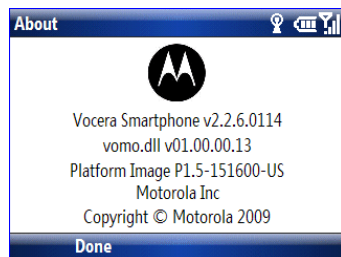
- **Log Upload** – Allows you to upload smartphone logs to a specified FTP server. For more information, see [Uploading Smartphone Logs to an FTP Server](#) on page 98.

Figure 7.8. Log Upload dialog box



- **About** – Displays version information for Vocera Smartphone firmware, the Vocera Client (vomo.dll), and the Motorola platform image.

Figure 7.9. About dialog box





Troubleshooting

This chapter describes how to troubleshoot problems you might have configuring Vocera smartphones using MSP.

Troubleshooting Staging

If the staging server fails to turn on, make sure .NET Framework 2.0 SP2 is installed on the client.

If you try to turn on the staging server from the MSP Console, it may result in the following error:

The onDemand control is not in memory

This means that the client on which you are running Internet Explorer does not have .NET Framework 2.0 SP2 installed. Make sure you install .NET Framework 2.0 SP2 on that machine, and try turning on the staging server again.

If a device is unable to communicate with the relay server, check the device-side staging logs.

During successful staging, staging logs are uploaded to the relay server and are then made available to the MSP Console. However, if a device is unable to communicate with the relay server, the staging logs are not uploaded. In this situation, you have to use the MSP Agent to look at the staging logs on the device.

To view staging logs on the Vocera smartphone:

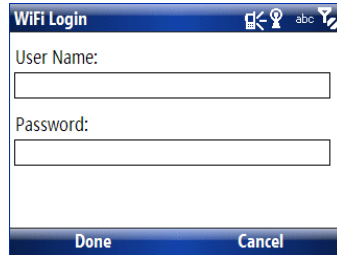
1. Press **Start > All Programs > MSP Agent**.
2. Select **Log Menu**.
3. Select **View Log**.

Note: The selected log level determines what information is contained in the logs. To change the log level, select **Log Menu > Log Level**. Available log levels are Critical, Error, Warning, Info, and Verbose.

During staging, a WiFi Login dialog box appears.

After the phone is configured by the Staging Profile, a WiFi Login dialog box may appear. You can ignore this dialog, or press **Cancel** to close it.

Figure 8.1. WiFi Login dialog box



During staging, an "API busy" error message appears in the Rapid Deployment client.

This error may indicate that MSP services need to be restarted on the MSP Server. See [Restarting MSP Services](#) on page 93.

Staging fails, and the device-side log has the following error: "rdclient ERR Unregistered setting plug-in."

This error indicates that you are trying to install a Settings object before the plugin for that object has been installed on the phone. For example, you cannot install a date and time Settings object before installing the DateAndTime package. Make sure you add the bundle steps in the correct order. See [Table 4.5, "Vocera smartphone bundle steps"](#) on page 60.

When you create the Staging Profile, do not select Additional Settings Options. As a best practice, you should include Settings objects in a Bundle to make them persistent.

Staging succeeds, but the phone cannot connect to the wireless network.

Perhaps you selected the wrong encryption type in your network settings package.

- If WPA-PSK or WPA-EAP authentication is selected, select TKIP encryption.
- If WPA2-PSK or WPA2-EAP authentication is selected, select AES-CCMP encryption.

Troubleshooting Provisioning

The Provisioning tab is missing from the MSP Console.

To enable the Provisioning tab, update your MSP license key. See [Updating Your MSP License Key](#) on page 37.

Updates to Vocera smartphones are not being provisioned successfully.

Make sure the **abup - dwp_7.02.79** package is listed first in the Vocera bundle. See [Creating Bundles](#) on page 59.

Not all of the smartphones are being updated at the same time.

If you activated a provisioning policy and only some of the smartphones are being updated, it could be because you have not updated your MSP license key with enough Provisioning seats for all the phones. See [Updating Your MSP License Key](#) on page 37.

Make sure Pause/Resume is set to True.

In the Provisioning Policy, make sure the Pause/Resume option is set to True. This specifies that if a job is interrupted because of a connectivity problem, it will resume when connectivity is restored.

Handle failed jobs by Deactivating and then Activating a Provisioning Policy.

A job is considered failed when the MSP Agent starts the job and it does not complete. The failed job may be orphaned if it is left in a started state. To complete the job, deactivate and then activate the Provisioning Policy in the MSP Console. Alternatively, the user of the phone can reboot the phone. After the phone is rebooted, the MSP Agent will automatically try to resume the job.

You can view a list of failed jobs on the **Compliance Summary > Compliance Status** page in the MSP Console.

Note: If a failed job does not restart after you deactivate and then activate a Provisioning Policy, you may need to restart MSP services. See [Restarting MSP Services](#) on page 93.

Restart MSP services if the compliance summary for a policy shows "Processing" for more than 5 minutes.

If you modify a Bundle that is used in an active Provisioning Policy, it should automatically determine how many devices are compliant with the policy. On the Compliance Summary page, if the Compliant column shows "Processing" for more than 5 minutes, you should restart MSP services to resolve the problem. See [Restarting MSP Services](#) on page 93.

Changing the Vocera Client Gateway IP Address

Before you can stage and provision content on a Vocera smartphone, you need to upload several predefined packages into the MSP Object Library. One of these packages is called **VoceraClientGatewayIPAddress**, which is created when you run the **upload_packages.bat** file.

You may need to update the **VoceraClientGatewayIPAddress** package for the following reasons:

- You entered the wrong IP address for the Vocera Client Gateway when you ran the **upload_packages.bat** file.
- You moved the Vocera Client Gateway to a different computer.
- You installed Vocera Client Gateway on additional computers.

To update the **VoceraClientGatewayIPAddress** package, run the **upload_packages.bat** file again to generate a new version of the **VoceraClientGatewayIPAddress** package with the correct IP address(es).

Note: If you configured the smartphone by tethering it to another computer using a USB cable rather than using MSP, you can update the Vocera Client Gateway IP address(es) using the Motorola EWP Provisioning Tool. See [Using the Motorola EWP Provisioning Tool](#) on page 113.

To change the Vocera Client Gateway IP address package in MSP:

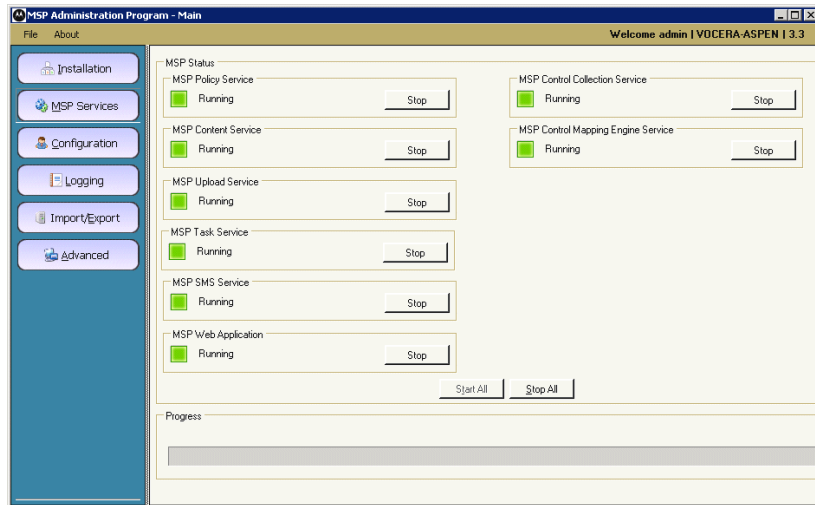
1. Run **upload_packages.bat** again, and specify the new IP address(es) of the Vocera Client Gateway computer(s) when prompted.
See [Uploading Packages for Vocera Smartphones](#) on page 50.
2. In the MSP Console, choose **Library > Packages**. Refresh the page every minute until you see the **VoceraClientGatewayIPAddress** package. It may take a few minutes.
3. In the MSP Console, update the version of the **VoceraClientGatewayIPAddress** package used in your Vocera bundle. See [Managing Package Versions](#) on page 77.

Restarting MSP Services

If you notice that a Provisioning Policy fails to activate successfully, there may be a problem with one or more of the MSP services. You can stop and start the MSP services using the MSP Administration Program.

The MSP Administration Program is a client application installed on the MSP server. It displays a summary of MSP components and allows you to start and stop MSP services. It also allows you to specify logging options and the location of MSP files.

Figure 8.2. MSP Administration Program



To restart MSP services:

1. Log into the MSP server as a user with Administrator privileges.
2. Choose **Start > Programs > Motorola MSP > MSP Admin**.
3. Click **MSP Services**.
4. Click **Stop All** to stop all MSP services.
5. Click **Start All** to start all MSP services.

For more information about how to use the MSP Administration Program, see *Using Mobility Services Platform*.

Troubleshooting the Relay Server

If a Relay Server object is defined incorrectly, the MSP Server will be unable to connect with the associated FTP server, preventing MSP staging and provisioning from working.

To check the status of a relay server in the MSP Console, click the **Status** tab, and then click **Relay Server Status**. All of the status icons should be green. If any are red, there is a problem connecting with the relay server.

If a Relay Server object that you created is not listed on the status page, it has not been activated. Make sure you activate the Relay Server before using it for staging or provisioning.

Here is a list of common problems to check:

- Make sure the FTP Publishing Service is running.

Choose **Start > Administrative Tools > Services** to open the Services window. The status of the FTP Publishing Service should be Started. If it is not Started, perform these steps:

1. Double-click the service to open the Properties dialog box.
2. In the **Startup Type** field, select Automatic, and then click **Start**.
3. Click **OK** to save your changes and close the Properties dialog box.

- Make sure the FTP Service has Read and Write access to the specified home directory. See [Configuring Windows IIS FTP Service as a Relay Server](#) on page 19.
- Open the Relay Server object in MSP Console, and make sure it is configured correctly.
 - Make sure the Relay Server is active. If it is not, click **Activate** in the Related Tasks list.
 - Make sure the user and password are specified correctly. They should match exactly the user and password you created for the FTP Service. See [Configuring Windows IIS FTP Service as a Relay Server](#) on page 19.
 - Make sure the correct FTP Server IP address is specified. It should be the same IP address as the MSP Server.
 - Make sure the FTP protocol is specified. Do not select FTPS.
 - Make sure the correct FTP port is specified. The default is port 21.

Changing the Relay Server after Staging

The Relay Server that the Vocera smartphone uses for provisioning is determined by the bundle that you staged on the phones. If you change any part of the Relay Server configuration (including the home directory, username, or password) or move the Relay Server to a different machine after software has already been staged on the phones, you must use the MSP Console to create a new Relay Server object, and then add it to the bundle. The new Relay Server will then be provisioned to the phones, and phones will be able to connect to it. Once all phones have been provisioned with the new Relay Server object, you can delete the old one.

For information on creating a Relay Server object in the MSP Console, see [Creating a Relay Server Object](#) on page 40.

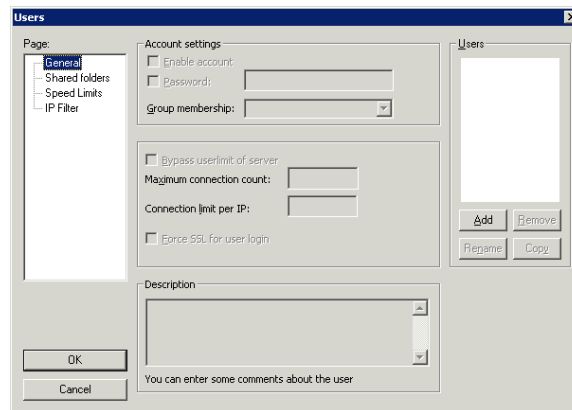
Configuring FileZilla Server as a Relay Server

If you are unable to get the IIS FTP Service to work successfully as a relay server for MSP, you can choose to set up the free FileZilla Server instead. FileZilla may be easier to install and configure than IIS FTP Service. In addition, the FileZilla Server Interface provides extensive logging capabilities that may help you troubleshoot problems.

To configure FileZilla Server as a relay server:

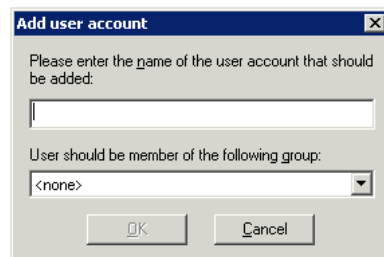
1. Log in to the MSP Server computer with administrator privileges.
2. Download FileZilla Server from <http://filezilla-project.org/> and install it.
3. After FileZilla is installed, choose **Start > Programs > Filezilla Server > Filezilla Server Interface**.
4. Choose **Edit > Users**. The Users dialog box appears.

Figure 8.3. Users dialog box



5. In the Users pane, click **Add**. The Add User Account window appears.

Figure 8.4. Add User Account dialog box



6. In the Add User Account dialog box, enter the Username and click **OK**. For example, enter **vocera**. The username you entered appears in the User pane.
7. In the Account Setting pane, make sure the **Password** box is checked.
8. In the **Password** field, enter a password.

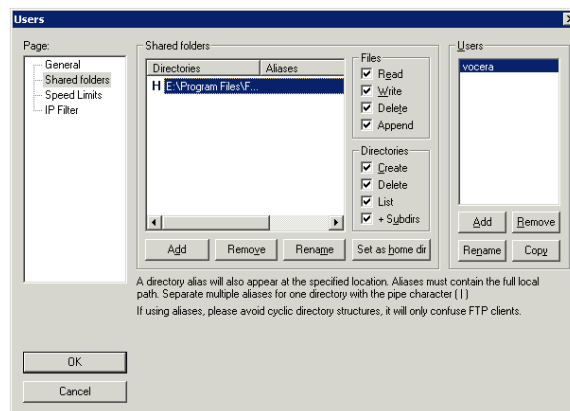
Note: Write down the **Username** and **Password** you chose for the account. You will need to know them when you configure a Relay Server in the MSP Console.

9. Click the **Shared Folders** page and click **Add**.
10. Select a folder from your system (for example, **d:\MSP_FTP**) and click **OK**. The selected folder appears in the Shared Folders pane.

All the Contents (Packages, Bundles, and network Settings) from MSP will be delivered to this folder.

11. Enable the following options under the Files and Directories panes:
 - **Files:** Read, Write, Delete, Append
 - **Directories:** Create, Delete, List, +Subdirs

Figure 8.5. FileZilla Shared Folders page



12. In the Users pane, click **Add** again. The Add User Account window appears.
13. In the **Username** field, enter **anonymous**, and then click **OK**.
14. In the Account Setting pane, make sure the **Password** box is unchecked.
15. Click the **Shared Folders** page and click **Add**.
16. Select a folder from your system (for example, **d:\SmartphoneLogs**) and click **OK**. The selected folder appears in the Shared Folders pane.

All smartphone logs that you upload using the Log Upload tool will be delivered to this folder.

17. Click **OK**.

18. Verify that you can access the FTP directory from a different computer.

For example, open Internet Explorer on a different computer and enter the following in the Address field of the browser window:

`ftp://MSP_Server_IP_Address`

19. Once you have configured FileZilla for use as an MSP Relay Server, you must create a Relay Server Object in MSP with the details pertaining to the FTP Server. See [Creating a Relay Server Object](#) on page 40.

Uploading Smartphone Logs to an FTP Server

Vocera provides a Log Upload tool with the Vocera Smartphone Information application. If a user experiences a problem with a smartphone that you need to troubleshoot, you can use the Log Upload tool to upload log files from the smartphone to an FTP server.

Important: The FTP server you specify must be configured to allow anonymous access.

IIS FTP Server Requirements

If you are using IIS FTP Server, make sure the FTP site uses **Isolate Users** mode so that all users that access the site, including anonymous users, have their own home directory. See [Configuring Windows IIS FTP Service as a Relay Server](#) on page 19. If the IIS FTP Site was is not currently set to **Isolate Users** mode, see the following site for instructions on how to convert it:

[Converting an Existing FTP Site to Isolate Users Mode](#)¹

Uploading Logs

This section describes how to upload log files from the smartphone to an FTP server.

To upload smartphone logs to an FTP server:

1. Press **Start > All Programs > Vocera Smartphone Information**.

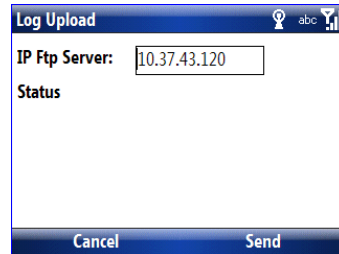
The Information dialog box appears.

¹ <http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/b63de8ef-e3c5-456d-a8ca-7af4198819d4.mspx?mfr=true>

2. Select **Log Upload**.

The Log Upload dialog box appears.

Figure 8.6. Log Upload dialog box



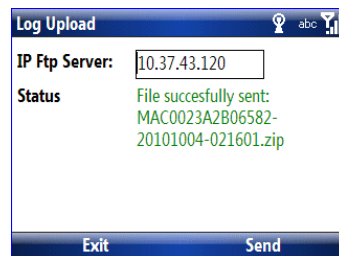
3. In the **IP Ftp Server** field, enter the IP address of an FTP server in dotted-decimal notation (for example, 192.168.15.10).

The default IP address of FTP server used by the Log Upload tool depends on how the smartphone was configured. If MSP was used to configure the phone, the default FTP server is the IP address of the MSP relay server. If the phone was configured manually by tethering it to a configuration computer, the default FTP server is the IP address of the active Vocera Client Gateway server, which may not be running an FTP server. If necessary, specify the IP address of another FTP server.

4. Press **Send**.

The **Status** field indicates whether the file was sent successfully.

Figure 8.7. Log Upload success



Downloading Logs

When you use the Log Upload tool, it zips up the phone's log files into a single file named **MacAddress_Date_Time.zip**, and it then sends the file anonymously to the specified FTP server. To view the logs, download the ZIP file from the FTP server and then extract its contents using any ZIP utility.

Log for Vocera Apps

The Log Upload tool does not upload the separate log file for Vocera Apps, which includes the smartphone's contacts and text messaging functionality. When logging for Vocera Apps is enabled, the log for Vocera Apps is saved to the following file on the smartphone:

\\Windows\\JBlend_VM.trace.txt

Note: Logging for Vocera Apps is disabled by default.

Master Clearing a Smartphone

If you need to clear all settings on a smartphone and restore the factory settings, you can Master Clear the phone.

Important: Only an administrator responsible for configuring phones should Master Clear a phone. After you Master Clear a phone, it will no longer connect to the wireless network nor offer the Vocera functionality. You need to reconfigure it so that it can be used again.

To Master Clear a smartphone:

1. On the phone, press **Start > All Programs > System Tools > Master Clear**.
2. An Alert dialog box prompts whether you are sure. Press **Yes**.
3. In the Enter Master Code dialog box, type six zeros (000000), and then press **Done**.

MSP Client Error Codes

MSP Client components on the Vocera smartphone (Rapid Deployment and the MSP Agent) can return error codes in the -8xx range and the -10xx range.

Table 8.1. MSP client error codes

Error Code	Description
-801	Fatal error during creation of file on mobile computer.
-802	Package does not exist in host package directory.
-803	Format error in AirBEAM package.
-805	Insufficient memory to load package (and subpackages).
-806	Invalid FTP user.

Error Code	Description
-807	Invalid FTP password for FTP user.
-808	Invalid FTP account.
-810	Error attempting to set binary mode for FTP transfer.
-811	Error connecting to the FTP server.
-812	Error resolving FTP server name.
-813	Error occurred during file transfer.
-815	Error occurred while determining available disk space.
-816	Invalid path specified for mobile computer file.
-817	Error occurred in mkdir() call.
-822	Missing temporary package directory (\application\airbeam_pt).
-823	Missing package directory (\application\airbeam\pkg).
-836	Error occurred while uploading a file.
-837	Error occurred while reading host directory.
-838	Host file existed prior to upload in safe mode.
-839	Error client file to be uploaded.
-840	Too many install command line arguments.
-841	Error occurred while executing the install command line.
-842	Error occurred while executing the uninstall command line.
-843	Error occurred while opening package definition file.
-845	Error creating WNMS information file.
-846	Error uploading WNMS information file.
-847	Missing/invalid AirBEAM license file.
-848	Corrupt package definition file (.apd).
-849	Error occurred renaming a file on the server.

Error Code	Description
-850	Error occurred trying to restart an FTP download.
-851	Error occurred getting a file list from server.
-852	AirBEAM Client is already running.
-853	Error occurred initializing AirBEAM Client.
-854	Background synchronization already in progress.
-855	Specified command file was not found.
-856	Invalid L2 command.
-857	Missing path information.
-858	Downloaded file length error.
-1001	A Job was orphaned. A Job is considered orphaned when the MSP Agent starts and the Job was left in a started state. This can occur if a program within the Job reboots the Device (i.e., osupdate) without returning to the agent.
-1002	A pending Job was cancelled.
-1003	An error occurred opening the MSP Client log file.
-1004	An error occurred reading the MSP Client log file.
-1005	Buffer length error. This is an internal error code used by the logging logic and should never be reported by the agent.
-1006	Invalid plug-in class error. This error code is not returned by the agent. It is used by custom plug-ins to indicate an unsupported plug-in class value was specified.
-1007	Invalid plug-in provider error. This error indicates the Provider registry value is missing from the plug-in registration. In other words, the HKLM\Software\MSP\Plugins\<vendor>\Provider registry entry is missing.
-1008	Error reading registry value. This error is returned when an unexpected lowlevel error occurs reading the Device registry.
-1009	No plug-in provider. This error indicates that a plug-in is not registered correctly. In other words, the HKLM\Software\MSP\Plugins\<vendor> registry key is missing.

Error Code	Description
-1010	Missing Bundle error. This error indicates a Bundle specified in a Staging Profile, or a job, was not found on the Relay Server.
-1011	Error connecting to FTPS server. This error is usually caused by missing/invalid server certificate when VerifyServer is enabled.
-1012	Invalid Bundle error. This error indicates a Bundle file has invalid Contents.
-1013	Invalid Job error. This error indicates a file has invalid Contents.
-1014	Error occurred during FTP file deletion.
-1015	Error occurred creating Bundle.
-1016	Error occurred writing Bundle.
-1017	Invalid message file. Messages are limited to 50 characters.
-1018	Invalid blob header. This error indicates a blob header has invalid Contents.
-1019	Invalid Device UUID. This error indicates an error occurred while trying to obtain the Device's UUID from the CE system calls.
-1020	Too many attributes. This is an internal error code used by the User attribute logic and should never be reported by the agent.
-1021	No MSP Client mutex error. This error indicates the low-level Staging/Provisioning engine is in-use by another process.
-1022	Provisioning cancelled error. This error indicates the Provisioning process was cancelled by a Staging process.
-1023	Error writing registry entry. This error is returned when an unexpected lowlevel error occurs writing the Device registry.
-1024	Error processing condition. This error indicates a condition plug-in returned a failure.
-1025	Error occurred during FTP CWD command.
-1026	Error occurred processing Relay Server info file.
-1027	Insufficient buffer space for Relay Server info file site list. This is an internal error code used by the Relay Server info file processing logic and should never be reported by the agent.

Error Code	Description
-1028	Plug-in (setting or condition) entry point is undefined.
-1029	Missing plug-in DLL. The specified plug-in DLL does not exist on the Device.
-1030	Error returned from setting plug-in entry-point.
-1031	Maximum concurrent jobs exceeded. This error is returned if the optional "maximum number of concurrent jobs" limit is exceeded.
-1032	Launch command error. This error indicates one of the new proxy plug-in commands failed. It only applies to MPA, so maybe we shouldn't list it in the regular MSP client document.



Installation Checklists

This appendix provides checklists you can follow to set up your MSP Server.

Pre-Installation Checklist for IT

Before installing prerequisite software and MSP Server software, make sure someone from IT has completed the following checklists to prepare the MSP Server computer and the configuration computer for installation.

Pre-Installation Tasks for the MSP Server

<input type="checkbox"/>	1. Provision the MSP Server computer. Make sure the hardware conforms to specifications. Typically, you install MSP Server on the Vocera Client Gateway computer. See MSP Server Requirements on page 14.
<input type="checkbox"/>	2. Install Windows Server 2003 (Standard Edition or Enterprise Edition) with SP2 or higher on the MSP Server computer.

Pre-Installation Tasks for the Configuration Computer

<input type="checkbox"/>	1. Make sure the Vocera Configuration Computer can connect to the MSP Server using either a network interface controller or a wireless network interface controller.
<input type="checkbox"/>	2. Obtain a USB cable to connect the phone to the USB port of the configuration computer.

Installation Checklist

MSP Server Installation Tasks

<input type="checkbox"/>	1. Install Microsoft IIS from the Windows CD. See Installing Microsoft IIS on page 17.
<input type="checkbox"/>	2. Create a home folder for the IIS FTP Service specifically for MSP Server files. See Creating an MSP FTP Folder on page 19.
<input type="checkbox"/>	3. Configure the Windows user account needed for the IIS FTP Service, and then configure the IIS FTP Service. If someone else is responsible for configuring a Relay Server in the MSP Console, provide that person the username and password for the account. See Configuring Windows IIS FTP Service as a Relay Server on page 19.
<input type="checkbox"/>	4. Install .NET Framework 2.0 SP2 from the MSP 3.3 CD. See Installing MSP 3.3 Server on page 21.
<input type="checkbox"/>	5. Install Microsoft SQL Server 2005 Express from the MSP 3.3 CD. See Installing MSP 3.3 Server on page 21.
<input type="checkbox"/>	6. Install Windows Installer 4.5 Update (if needed) from the MSP 3.3 CD. See Installing MSP 3.3 Server on page 21.
<input type="checkbox"/>	7. Install MSP 3.3 Server from the MSP 3.3 CD. See Installing MSP 3.3 Server on page 21.
<input type="checkbox"/>	8. For backup purposes, install Microsoft SQL Server Management Studio Express. See Installing Microsoft SQL Server Management Studio Express on page 31.

Configuration Computer Installation Tasks

<input type="checkbox"/>	1. Install .NET Framework 3.5 (or later). See Installing .NET Framework on page 21.
<input type="checkbox"/>	2. Install Windows Mobile Device Center or Microsoft ActiveSync.

<input type="checkbox"/>	<p>3. Install the Motorola EWP Provisioning Tool.</p> <p>The Motorola EWP Provisioning Tool is an application you use to generate CAB files to configure network, Vocera Server, Vocera Client Gateway, and time zone settings on Vocera smartphones.</p> <p>See Installing the Motorola EWP Provisioning Tool on page 111.</p>
--------------------------	---

Post-Installation Checklist

Administrative Setup Tasks

<input type="checkbox"/>	<p>1. If Vocera Client Gateway and MSP Server are installed on separate machines, copy the \\VoceraMSP folder on the Vocera Client Gateway computer and paste it to the root of the drive where MSP is installed on the MSP computer.</p> <p>See Copying Files from the Vocera Client Gateway Computer on page 37.</p>
<input type="checkbox"/>	<p>2. Update your MSP license key.</p> <p>See Updating Your MSP License Key on page 37.</p>
<input type="checkbox"/>	<p>3. Upload MSP definition documents and package templates provided by Vocera.</p> <p>See the following topics:</p> <ul style="list-style-type: none"> • Uploading the Network.WLAN.EWP Setting Definition Document on page 38 • Uploading the EWP Persistent REG Install Package Template on page 39 • Uploading the Vocera Root Certificate Install Package Template on page 39
<input type="checkbox"/>	<p>4. Create a Relay Server object.</p> <p>See Creating a Relay Server Object on page 40.</p>
<input type="checkbox"/>	<p>5. Create a Network Settings object. If you have multiple locations (or SSIDs) with different network settings, create a separate Network Settings object for each.</p> <p>See Creating a Network Settings Object on page 42.</p>
<input type="checkbox"/>	<p>6. Optionally, create Site objects for locations with different network settings.</p> <p>See Creating a Site Object on page 45.</p>

Content Objects Tasks

<input type="checkbox"/>	1. Upload predefined packages provided by Vocera. See Uploading Packages for Vocera Smartphones on page 50.
<input type="checkbox"/>	2. Create a Date and Time Settings object. If you have multiple sites with different time zones, create a Date and Time Settings object for each. See Creating a Date and Time Settings Object on page 53.
<input type="checkbox"/>	3. If SSL is enabled on your Vocera system, create a package to install the self-signed certificate from each Vocera Server on each smartphone. See Creating a Vocera Server SSL Certificates Package on page 56.
<input type="checkbox"/>	4. Optionally, create Message Set objects to prompt users during Provisioning. See Creating Message Set Objects on page 59.
<input type="checkbox"/>	5. Create a Bundle to use for both Staging and Provisioning. See Creating Bundles on page 59.

Staging Tasks

<input type="checkbox"/>	1. Create a Staging Profile. See Creating a Staging Profile on page 67.
<input type="checkbox"/>	2. Perform On-Demand Staging of Vocera smartphones. See How to Use Staging on page 70.
<input type="checkbox"/>	3. View the Staging status. See Viewing Staging Status on page 74.

Provisioning Tasks

<input type="checkbox"/>	1. If you need to update the settings or software on Vocera smartphones, update the appropriate packages, and change the package versions used in the Bundle. See Managing Package Versions on page 77.
<input type="checkbox"/>	2. Create a Provisioning Policy, and activate it. See Creating a Provisioning Policy on page 78.
<input type="checkbox"/>	3. View the Provisioning status. See Viewing Provisioning Status on page 80.



Tethered Configuration of Smartphones

This appendix describes how to manually configure a Vocera smartphone by tethering it to a computer using a USB cable rather than using MSP to configure the phones. If you are configuring only a handful of phones, the tethered procedure may be simpler and faster.

Tethered Configuration Checklist

The following checklist provides a high-level overview of the tethered configuration steps:

<input type="checkbox"/>	1. Set up the configuration computer with the required software and USB cable. See Setting Up a Computer to Configure Smartphones on page 110
<input type="checkbox"/>	2. Collect the wireless network and security information needed to configure smartphones from your IT department. Also, if you are using EAP-TLS or PEAP authentication, collect the certificate files you need to configure smartphones. See Collecting Network and Security Information on page 112.
<input type="checkbox"/>	3. Use the Motorola EWP Provisioning Tool to create a provisioning CAB file for the phone with network, Vocera Server, Vocera Client Gateway, and time zone settings. See Using the Motorola EWP Provisioning Tool on page 113.
<input type="checkbox"/>	4. Connect the phone to the configuration computer using a USB cable.
<input type="checkbox"/>	5. Copy the CAB files provided by Vocera for tethered configuration as well as the CAB file created by the Motorola EWP Provisioning Tool into the \Temp folder on the phone. See Copying Vocera CAB Files on page 119.

<input type="checkbox"/>	6. Install each of the CAB files on the phone. See Installing Vocera CAB Files on page 122.
<input type="checkbox"/>	7. If SSL is enabled for your Vocera system, install the certificate from each Vocera Server on each phone. See Installing Vocera Server SSL Certificates on a Smartphone on page 126.
<input type="checkbox"/>	8. Optionally, set the date and time on the phone. See Setting the Date and Time on page 127. This step may be completed by the person assigned to use the phone.
<input type="checkbox"/>	9. Verify that the phone has been configured correctly. See Chapter 7, Verifying Smartphone Configuration on page 83.

Setting Up a Computer to Configure Smartphones

Before you can begin to configure a smartphone manually, you must perform the following setup tasks on the configuration computer:

1. Install **Windows Mobile Device Center** or **Microsoft ActiveSync**.

Both Windows Mobile Device Center and Microsoft ActiveSync are free programs that let you synchronize data and information between your computer and a Windows Mobile device, such as a Vocera smartphone. These applications can also be used to copy files from your computer to Vocera smartphones.

Windows Mobile Device Center is the replacement for ActiveSync on Windows Vista and Windows 7 computers. When you connect a Windows Mobile device to a Windows 7 computer, drivers for Windows Mobile Device Center are installed automatically.

On Windows 7 computers, you can also use Windows Explorer to copy files to Vocera smartphones.

2. Install the **Motorola EWP Provisioning Tool**.

The Motorola EWP Provisioning Tool is an application you use to generate CAB files to configure network, Vocera Client Gateway, and time zone settings on Vocera smartphones.

See [Installing the Motorola EWP Provisioning Tool](#) on page 111.

3. Create a working folder on the configuration computer in which to place smartphone CAB files (for example, **c:\vocera\config\smartphone**).

4. On the Vocera Client Gateway computer, copy the **%vocera_drive%\vocera\config\smartphone** folder and its subfolders to the working folder on the configuration computer. The **%vocera_drive%\vocera\config\smartphone** on the Vocera Client Gateway computer contains predefined CAB files needed to configure the phones.
5. Obtain a USB cable to connect the phone to the USB port of the configuration computer.

Installing the Motorola EWP Provisioning Tool

The Motorola EWP Provisioning Tool is a software application used to configure network, Vocera Server, Vocera Client Gateway, and time zone settings on the smartphone while it is connected to another computer using a USB cable. It can be used to configure a small number of phones quickly, rather than setting up MSP to configure them.

After you install Vocera Client Gateway, the Motorola EWP Provisioning Tool installation program (**MotorolaEWPProvisioningToolSetup.msi**) is located in the following folder on the Vocera Client Gateway computer:

%vocera_drive%\vocera\config\smartphone\ ProvisioningTool

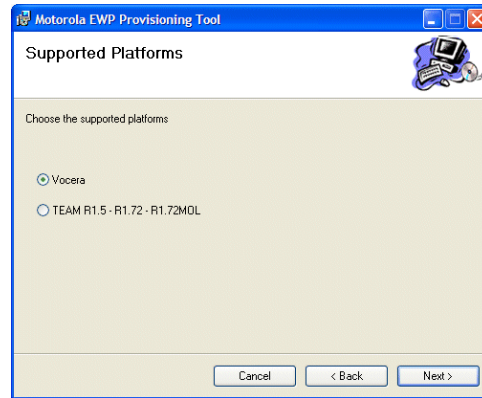
Note: The Motorola EWP Provisioning Tool requires .NET Framework 3.5 (or later). Install .NET Framework *before* you install the Motorola EWP Provisioning Tool. See [Installing .NET Framework](#) on page 21.

To install the Motorola EWP Provisioning Tool:

1. Install Vocera Client Gateway. For complete Vocera Client Gateway installation instructions, see the *Vocera Installation Guide*.
2. Install the latest Vocera Smartphone Firmware update on the Vocera Client Gateway computer.
3. On the Vocera Client Gateway computer, open the **%vocera_drive%\vocera\config\smartphone\ProvisioningTool** folder.
4. Copy the **MotorolaEWPProvisioningToolSetup.msi** file to the desktop of your configuration computer.
5. On the configuration computer, run the **MotorolaEWPProvisioningToolSetup.msi** file.
6. In the install wizard, respond appropriately to any prompts to install the application.

Important: On the **Supported Platforms** page of the install wizard, make sure you select **Vocera**.

Figure B.1. Supported Platforms dialog box



7. On the last wizard dialog box, click **Close** to exit.
8. To start the application, choose **Start > Programs > Motorola EWP Provisioning Tool**, or click the **Motorola EWP Provisioning Tool** shortcut icon on the desktop.

Collecting Network and Security Information

Before you begin to configure Vocera smartphones, you must obtain wireless network and security information from your IT department. The following table lists the information you need for each authentication protocol.

Table B.1. Network and security information

Information Needed	WEP	WPA-PSK or WPA2-PSK	WPA-EAP or WPA2-EAP
Vocera Server IP address(es) and port	✓	✓	✓
Vocera Client Gateway IP address (port is optional)	✓	✓	✓
SSID	✓	✓	✓
Authentication protocol	✓	✓	✓
Encryption type (TKIP or CCMP)	✓	✓	✓
WEP key and index	✓		
Pre-shared key		✓	

Information Needed	WEP	WPA-PSK or WPA2-PSK	WPA-EAP or WPA2-EAP
PEAP, LEAP, or EAP-FAST authentication identity password			✓
Certificates for EAP-TLS or PEAP authentication			✓
Whether CCKM is enabled on the WLAN	✓	✓	✓
Whether SSL is enabled on the Vocera Server	✓	✓	✓

Configuring a Smartphone

This section describes how to configure a phone using a tethered connection to a configuration computer.

- [Using the Motorola EWP Provisioning Tool](#) on page 113
- [Copying Vocera CAB Files](#) on page 119
- [Installing Vocera CAB Files](#) on page 122

Note: These configuration instructions are intended for the Vocera smartphone only. They cannot be used to configure other types of devices.

Using the Motorola EWP Provisioning Tool

The Motorola EWP Provisioning Tool is a software application you can use to create a provisioning CAB file for the phone with network, Vocera Server, Vocera Client Gateway, and time zone settings.

For instructions on how to install the Motorola EWP Provisioning Tool, see [Installing the Motorola EWP Provisioning Tool](#) on page 111.

To use the Motorola EWP Provisioning Tool:

1. Log into the configuration computer with administrator privileges.

Note: You can also use the **Run As** command to run the Motorola EWP Provisioning Tool program as an administrator.

2. Choose **Start > Programs > Motorola EWP Provisioning Tool**.

The Motorola EWP Provisioning Tool window appears.

Figure B.2. Motorola EWP Provisioning Tool window

3. In the **Platform** list, select VOCERA.
4. In the **Vocera Server IP Addresses** field, enter the Vocera Server IP address(es) in dotted-decimal notation (for example, 192.168.15.10). If you have a Vocera cluster, enter one IP address per row.
5. In the **Vocera Server Port** field, enter the Web server port used by the Vocera Server. The default is port 80.
6. If your Vocera system has SSL enabled, make sure the **Enable SSL** box is checked. If you check this box, you need to also install Vocera Server SSL certificates on each phone. See [Installing Vocera Server SSL Certificates on a Smartphone](#) on page 126.
7. In the **VCG Servers** box, enter the IP address(es) of the Vocera Client Gateway and the port(s). If you leave the port blank, the default port (5060) is used.
8. In the **WLAN Profile** box, specify values for your wireless network settings, such as the SSID, authentication and encryption type, and security certificate.
9. In the **CAB Parameters** box, specify the **Output Folder** in which to save the CAB file.

Make sure the output folder location is identical to the working folder where other smartphone CAB files are stored (for example, **c:\vocera\config\smartphone**).

10. Save the settings to an XML file so that you can load and edit the settings later:

- a. Choose **Profile > Save**.
- b. Specify the name and path of the XML file to store the settings, and then click **Save**.

11. Click **Generate** to create a CAB file in the specified output folder.

The CAB file has the name of the specified SSID. If you prefer a different name for the file, you can rename it.

Table B.2. Motorola EWP Provisioning Tool fields

Field	Description
Platform	Select the Motorola EWP platform. For the Vocera smartphone, select "VOCERA".
Vocera Server IP Addresses	Enter the Vocera Server IP address in dotted-decimal notation (for example, 192.168.15.10). If you have a Vocera cluster, enter the IP address of each Vocera Server on a separate row.
Vocera Server Port	Enter the Web server port used by the Vocera Server. The default is port 80.
Enable SSL	<p>If your Vocera system has SSL enabled, make sure this box is checked.</p> <p>If you check the Enable SSL box, the Vocera Server Port field automatically changes to 443. Similarly, if you uncheck the Enable SSL box, the Vocera Server Port field automatically changes to 80. In either case, you can change the port to something other than 443 or 80.</p> <p>You also need to install Vocera Server SSL certificates on the phone. See Installing Vocera Server SSL Certificates on a Smartphone on page 126.</p>
VCG Server IP	Enter the Vocera Client Gateway IP address in dotted-decimal notation (for example, 192.168.15.10). If you have multiple Vocera Client Gateway servers, enter the IP address of each Vocera Client Gateway on a separate row.
VCG Server Port	Enter the port used by each Vocera Client Gateway. If you leave this field blank, the default port (5060) is used.

Field	Description
Time Zone	Select the time zone where the phone will be used. After you configure a phone by installing CAB files, you can set the date and time on the phone. See Setting the Date and Time on page 127.
SSID	Enter the Service Set Identifier, or SSID, of the wireless network the Vocera smartphones will use. This field is case sensitive.
Security Mode	Select the authentication protocol used by your wireless network. Choose from the following values: <ul style="list-style-type: none"> • Static WEP • WPA-Personal (PSK) • WPA-Enterprise (EAP) • WPA2-Personal (PSK) • WPA2-Enterprise (EAP) • IEEE802.1X with Dynamic WEP
PSK	Select either ASCII or HEX for the type of pre-shared key for WPA/WPA2 - PSK protocol. In the text box to the right of the PSK field, enter either the ASCII passphrase or the HEX key (64 characters).
Encryption	Select the type of encryption used by the authentication type. Supported encryption types: TKIP or CCMP. <ul style="list-style-type: none"> • If WPA-PSK or WPA-EAP authentication is selected, select TKIP encryption. • If WPA2-PSK or WPA2-EAP authentication is selected, select CCMP encryption.
Alphabetic	If WEP authentication is selected, specify the alphabetic key (Hex or ASCII): <ul style="list-style-type: none"> • ASCII WEP 40t – keys are set with 5 ASCII characters. • ASCII WEP 104 – keys are set with 13 ASCII characters. • HEX WEP 40t – keys are set with 10 HEX characters. • HEX WEP 104 – keys are set with 26 HEX characters.
Key_0 Key_1 Key_2 Key_3	Select the index of the WEP key used to transmit data. The default is Key_0. In the text box to the right of the key, enter the key values for WEP encryption.

Field	Description
EAP	<p>Select one of the following the EAP authentication types:</p> <ul style="list-style-type: none"> • TLS • PEAP • LEAP • EAP-FAST
Identity	Specify the authentication username for PEAP, LEAP, EAP-FAST, or IEEE802.1X with Dynamic WEP authentication.
Enable CCKM	<p>If your wireless network has enabled Cisco Certified Key Management, make sure this box is checked.</p> <p>CCKM is a form of fast roaming supported on Cisco access points and on various routers. Using CCKM, Vocera smartphones can roam from one access point to another without any noticeable delay during reassociation. After a smartphone is initially authenticated by the RADIUS authentication server, each access point on your network acts as a wireless domain service (WDS) and caches security credentials for CCKM-enabled client devices. When a Vocera smartphone roams to a new access point, the WDS cache reduces the time it needs to reassociate.</p> <p>By default, this property is not selected. In order to take advantage of this feature, your access points must support CCKM and have it enabled, and you must use WPA-PEAP or WPA2-PEAP.</p>
Password	Enter the authentication identity password for PEAP, LEAP, EAP-FAST, or IEEE802.1X with Dynamic WEP authentication.
Disable Identity Protection	If you want to disable identity protection for PEAP or EAP-FAST authentication, check this box.
Certificate Selection	<p>Select the type of certificate you are using for EAP-TLS or PEAP authentication. Select either "Standard CA Certificate" or "Custom Certificate." Standard CA certificates are certificates purchased from a trusted certificate authority, such as Go Daddy. Custom certificates are certificates created by your own certificate authority.</p> <p>Note: Do NOT select "CEC Certificate" since the device manufacturer CA certificates may not be installed on all Vocera smartphones.</p>
Server Certificate File	If you are using a custom certificate for EAP-TLS or PEAP authentication, select the server certificate file.

Field	Description
Client Certificate Issuer Name	Enter the name of the issuer of the client certificate for EAP-TLS authentication.
Client Certificate File	Select the client certificate file for EAP-TLS authentication.
Client Certificate Password	Enter the client certificate password for EAP-TLS authentication.
PAC Provisioning Method	<p>Select either Automatic or Manual provisioning of Protected Access Credentials (PACs) for EAP-FAST authentication. The default is Automatic.</p> <p>If you select Manual PAC provisioning, create a new PAC on the Cisco ACS, copy the PAC to your computer, and then select the file in the PAC File field.</p>
PAC File	If you selected Manual PAC provisioning for EAP-FAST authentication, select the PAC file to install on each phone.
Provision Auto-PAC on Expiry	Check this box to enable automatic provisioning of a new PAC when it expires.
Output Folder	<p>Select the output folder where the CAB file will be created. The default is C:\Documents and Settings \username\Desktop. The text field is not editable directly. To select a different output folder, click the ".." button to the right.</p> <p>Make sure the output folder you select is identical to the working folder where other smartphone CAB files are stored (for example, c:\vocera\config\smartphone). Otherwise, after you click Generate, you will need to copy the CAB file to the working folder.</p>

Saving and Loading Provisioning Tool Settings

The Motorola EWP Provisioning Tool allows you to save its settings to an XML file that you can load and edit later. If you need to revise a pre-shared key, WEP key, password, or certificate for a particular network setting, you can load the XML file, specify the new setting, and then generate a new CAB file used to configure smartphones.

To save Provisioning Tool settings to an XML file:

1. In the Motorola EWP Provisioning Tool, choose **Profile > Save**.
2. Specify the name and path of the XML file to store the settings, and then click **Save**.

To load Provisioning Tool settings from an XML file:

1. In the Motorola EWP Provisioning Tool, choose **Profile > Load**.
2. Select an XML file you previously saved with the Provisioning Tool, and then click **Open**.

Encrypted Settings

All wireless network security settings are encrypted on the Vocera smartphone to prevent the settings from being copied and used on other devices. Consequently, the Motorola EWP Provisioning Tool stores wireless network settings in encrypted format.

Copying Vocera CAB Files

The following steps describe how to copy CAB files onto the Vocera smartphone using Windows Mobile Device Center or Microsoft ActiveSync.

To copy Vocera CAB files to the smartphone using Windows Mobile Device Center:


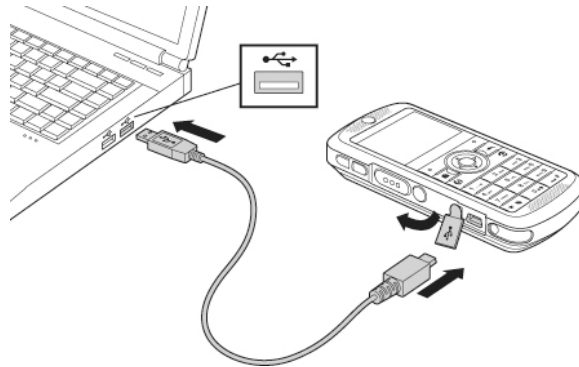
1. On the configuration computer, open the working folder (for example, **c:\vocera\config\smartphone**), and copy the following files to the Clipboard:
 - **ewpsecuritypolicyoff.cab** – Provides permission to replace the JBlend JVM.
 - **installer_SW_REL_number.CAB** – Installs the Vocera Client.
 - **JBlendWM_Vocera.CAB** – Installs the JBlend JVM.
 - **VoceraDeleteRDCIcon.CAB** – Removes the Rapid Deployment client shortcut from the phone, preventing users from accidentally misconfiguring the phone.
 - **SSID.CAB** – Installs network settings that you created with the Motorola EWP Provisioning Tool. See [Using the Motorola EWP Provisioning Tool](#) on page 113.
 - **VoceraAppsSettings.CAB** – Installs application settings for Vocera Apps.
 - **VoceraAppsInstaller.CAB** – Installs Vocera Apps, which provides contacts and text messaging functionality.
2. Turn on the phone by pressing and holding the Power/End  key for one to two seconds.
3. Using a USB cable, plug the phone into your configuration computer, as shown in the following figure.

Figure B.3. Connecting the phone to a computer



4. When the Windows Mobile Device Center window appears, click **Connect without setting up your device**.
5. Choose **File Management > Browse the contents of your device**.
A Windows Explorer window opens.
6. Double-click the root folder to open it.
7. Double-click the **Temp** folder to open it.

Note: If you don't see the **Temp** folder, choose **Tools > Folder Options**, click the **View** tab, and make sure the **Hide protected operating system files** box is cleared.

8. Paste the CAB files into the **Temp** folder on the phone.
9. Optionally, copy additional CAB files to the smartphone following the steps above. For example, you can install CAB files to update smartphone radio settings or enable or disable logging features. See [Optional CAB Files](#) on page 124.

To copy Vocera CAB files to the smartphone using Microsoft ActiveSync:

1. On the configuration computer, open the working folder (for example, **c:\vocera\config\smartphone**), and copy the following files to the Clipboard:
 - **ewpsecuritypolicyoff.cab** – Provides permission to replace the JBlend JVM.
 - **installer_SW_REL_number.CAB** – Installs the Vocera Client.
 - **JBlendWM_Vocera.CAB** – Installs the JBlend JVM.


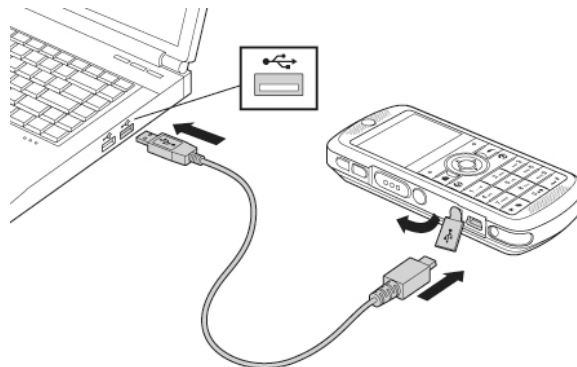
- **VoceraDeleteRDCIcon.CAB** – Removes the Rapid Deployment client shortcut from the phone, preventing users from accidentally misconfiguring the phone.
 - **SSID.CAB** – Installs network settings that you created with the Motorola EWP Provisioning Tool. See [Using the Motorola EWP Provisioning Tool](#) on page 113.
 - **VoceraAppsSettings.CAB** – Installs application settings for Vocera Apps.
 - **VoceraAppsInstaller.CAB** – Installs Vocera Apps, which provides contacts and text messaging functionality.
2. Turn on the phone by pressing and holding the Power/End  key for one to two seconds.
 3. Using a USB cable, plug the phone into your configuration computer, as shown in the following figure.

Figure B.4. Connecting the phone to a computer



4. If Microsoft Outlook is *not* installed on the computer, you are prompted that you can synchronize only non-Outlook items. If so, click **OK**.
 5. When the Synchronization Setup Wizard appears, click **Cancel**. The Microsoft ActiveSync window appears. Leave the Microsoft ActiveSync window open.
- Note:** The Synchronization Setup Wizard appears each time you restart the phone. Each time it appears, click **Cancel**.
6. In the Microsoft ActiveSync window, click **Explore**.
 7. Double-click **My Windows Mobile-Based Device** to go to the root directory of the device.
 8. Double-click the **\Temp** folder to open it.

9. Paste the CAB files into the **\Temp** folder on the phone.







Note: If ActiveSync prompts that it may need to convert files when synchronizing between your computer and the phone, click **OK**.

10. Optionally, copy additional CAB files to the smartphone following the steps above. For example, you can install CAB files to update smartphone radio settings or enable or disable logging features. See [Optional CAB Files](#) on page 124.

Installing Vocera CAB Files

The following steps describe how to install CAB files on the Vocera smartphone to configure it.

To install Vocera CAB files on the smartphone:

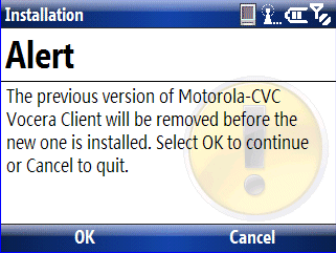
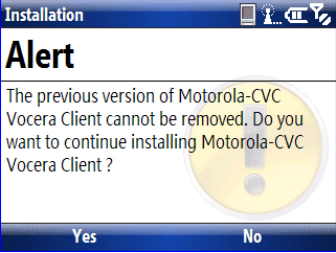
1. On the phone, press **Start > All Programs > File Manager**.
2. Use the navigation key  to select the  icon, and press the center key  to go back one level to the root folder.
3. Select the **\Temp** folder, and press the center key  to open it.
4. Use the navigation key  to scroll to a file and then press the center key  to install it.

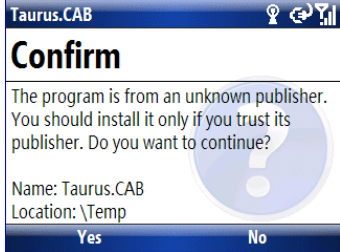
You must install the CAB files in the following order:

- **ewpsecuritypolicyoff.cab**
- **installer_SW_REL_number.CAB**
- **JBlendWM_Vocera.CAB**
- **VoceraDeleteRDCIcon.CAB**
- **SSID.CAB**
- **VoceraAppsSettings.CAB**
- **VoceraAppsInstaller.CAB**

Note: If there are multiple files with the name **installer_SW_REL_number.CAB** in that folder, select the one with the highest version number.

5. Respond to prompts as appropriate for each file.

CAB File	Prompts
installer_SW_ REL_number.CAB	<p>When you run installer_SW_REL_number.CAB, the following alert dialog box appears:</p>  <p>Press OK (the left soft key) to continue.</p> <p>Another alert dialog box appears:</p>  <p>Press Yes (the left soft key) to continue.</p> <p>When you are prompted to reboot, press Cancel.</p>
JBlendWM_Vocera.CAB	<p>When you are prompted to reboot, press OK only if you are enabling SSL on the phone. Otherwise, press Cancel.</p> <p>Note: If you are enabling SSL on the phone, you must reboot the phone after installing the JBlendWM_Vocera.CAB file. Otherwise, you will encounter a Java exception when you install subsequent CAB files.</p>

CAB File	Prompts
SSID.CAB	<p>When you run SSID.CAB, a confirmation dialog box appears if you are installing network settings on a previously configured phone:</p>  <p>Press Yes (the left soft key) to continue.</p> <p>When the file is finished being installed, press Done.</p>
<i>All Other CAB files</i>	<p>When the file is finished being installed, press Done.</p>

6. Install other CAB files as needed. For example, you could install optional CAB files to update smartphone radio settings and enable or disable logging features. See [Optional CAB Files](#) on page 124.
7. Reboot the phone to load the updated settings.

Optional CAB Files

Vocera provides optional CAB files you can use to update smartphone radio settings and enable or disable logging features.

- [Updating Radio Settings](#) on page 124
- [Enabling and Disabling Logging](#) on page 125

Updating Radio Settings

The following table lists the optional radio settings CAB files found in the **\vocera\config\smartphone\advanced** folder on the Vocera Client Gateway computer. You should copy these files to your configuration computer. To install these CAB files, copy one or more of them to the **\Temp** folder of the phone, run the file(s) in File Manager to install the settings, and then reboot the phone.

Table B.3. Optional radio settings CAB files

File	Description
VoceraRadio80211dDisable.cab	Disables 802.11d. This is the default setting.
VoceraRadio80211dEnable.cab	Enables 802.11d.
VoceraRadioABG.cab	Sets the radio to use 802.11a, b, and g data rates. This is the default setting.
VoceraRadioAChannelsDefault.cab	Sets the radio to use the following default 802.11a channels: 36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161
VoceraRadioAOnly.cab	Sets the radio to use 802.11a data rates.
VoceraRadioBGChannels-1611.cab	If the device is set to use 802.11b and g data rates, this CAB file sets it to scan only on channels 1, 6, and 11.
VoceraRadioBGChannels-14711.cab	If the device is set to use 802.11b and g data rates, this CAB file sets it to scan only on channels 1, 4, 7, and 11.
VoceraRadioBGChannels-14811.cab	If the device is set to use 802.11b and g data rates, this CAB file sets it to scan only on channels 1, 4, 8, and 11.
VoceraRadioBGonly.cab	Sets the radio to use 802.11b and g data rates.

Enabling and Disabling Logging

The following table lists the optional CAB files found in the **\vocera\config\smartphone\debug** folder on the Vocera Client Gateway computer that enable or disable Motorola logging features on the smartphone. You should copy these files to your configuration computer. To install these CAB files, copy one or more of them to the **\Temp** folder of the phone, run the file(s) in File Manager to install the settings, and then reboot the phone.

All Vocera smartphone log files are saved to the **\Logs** folder.

Vocera Client logging is *always* enabled on the phone. Vocera Client log files, which contain information about Vocera calls, begin with the **vomo** prefix. Motorola platform logs, which contain wireless network information, begin with the **VoceraLogs** prefix.

Table B.4. Logging CAB files

File	Description
DisableLocalRTA.cab	Disables logging for the local realtime analyzer. This is the default setting.
DisableLogs.cab	Disables Motorola platform logging.
EnableLocalRTA.cab	<p>Enables logging for the local realtime analyzer, providing information about the wireless radio.</p> <p>Note: By default, local realtime analyzer logs are disabled on the smartphone as they affect performance. You should only enable local realtime analyzer logs if told to do so by Vocera Technical Support for troubleshooting purposes. Realtime analyzer data is saved to a binary file named RtaDefault.bin that only Vocera Technical Support can view using an internal debugging tool.</p>
EnableLogs.cab	Enables Motorola platform logging. This is the default setting.

Installing Vocera Server SSL Certificates on a Smartphone

Note: If SSL is not enabled on your Vocera system, skip this setup task.

To install Vocera Server SSL certificates on a smartphone:

1. On the configuration computer, create a folder to store the SSL certificates. For example, the folder could be **%vocera_drive%\vocera\config\smartphone\certs**.
2. Copy the SSL certificate from each Vocera Server to the SSL certificates folder on your configuration computer.

On the Vocera Server, the certificate is found in the following folder:

%vocera_drive%\apache\Apache2\conf\ssl

Important: Make sure you copy the certificate with a **.cer** filename extension. The smartphone does not support certificates with a **.crt** filename extension.

3. Connect the smartphone to the configuration computer using a USB cable.

4. Use Windows Mobile Device Center, ActiveSync, or Windows Explorer to paste the certificate(s) to the **\My Documents\certs_to_install** folder on the phone.
5. On the smartphone, open File Manager and navigate to the **\My Documents\certs_to_install** folder.
6. Run each certificate file. The certificates are automatically added to the phone's certificate store.
7. For security reasons, delete the certificate file(s) in the **\My Documents\certs_to_install** folder. This prevents the file(s) from being copied to other devices.
8. Reboot the phone to load the certificates.

Note: If you do not reboot the phone to load the certificates, audio prompts that indicate when you have received or sent a text message are not played on the phone.

Setting the Date and Time

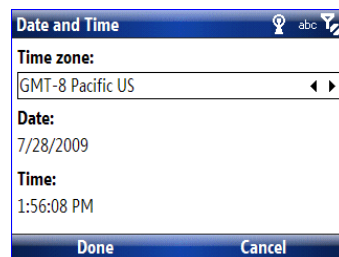
After you configure a smartphone by installing CAB files, you can set the correct date and time on it.

To set the date and time on the smartphone:

1. Press **Start > All Programs > Clock & Alarm > Date and Time**.

The Date and Time window appears.

Figure B.5. Date and Time window



2. Enter the correct date and time. Press **Done** to save your settings.

Restoring the Rapid Deployment Client Shortcut

The Rapid Deployment client is software installed on the phone for MSP staging functionality.

During tethered configuration of the phone, you install a CAB file (**VoceraDeleteRDIcon.CAB**) that removes the Rapid Deployment client shortcut. This prevents users from accidentally misconfiguring the phone. However, if you want to transition from tethered configuration to using MSP to update the phone, you should restore the Rapid Deployment client shortcut.

Note: Even without the Rapid Deployment client shortcut, you can still run the Rapid Deployment client by running the **rdclient.lnk** file in the **\Windows** folder on the phone. **DO NOT** run the **rdclient.exe** file in the **\Windows** folder as it defaults to barcode scanning, which is not supported on the phone.

To restore the Rapid Deployment Client shortcut on the phone:

1. On the configuration computer, open the **\vocera\config\smartphone** folder, and then navigate to the **\debug\VoceraReplaceRDIcon** subfolder, and copy the following file to the Clipboard:

- **Rapid Deployment**

Note: If the configuration computer does not have a **\vocera\config\smartphone** folder, copy the **%vocera_drive%\vocera\config\smartphone** folder on the Vocera Client Gateway computer to the configuration computer.

2. Using a USB cable, plug the phone into your configuration computer.
3. Use Windows Mobile Device Center, ActiveSync, or Windows Explorer to paste the Rapid Deployment Client shortcut to the **\Windows\Start Menu** folder on the phone.

Note: If ActiveSync prompts that it may need to convert files when synchronizing between your computer and the phone, click **OK**.

After you restore the Rapid Deployment client shortcut, you can start Rapid Deployment by pressing **Start > All Programs > Rapid Deployment**.



Configuring Smartphones for PEAP or EAP-TLS Authentication

This appendix describes how to configure Vocera smartphones to use PEAP or EAP-TLS authentication.

Upgrading Smartphones to PEAP or EAP-TLS

The following table lists the Vocera smartphone firmware versions that support PEAP and EAP-TLS:

Table C.1. Smartphone firmware required for PEAP and EAP-TLS

Protocol	Firmware Required
PEAP	Smartphone Firmware 2.1.1 or later
EAP-TLS	Smartphone Firmware 2.3.5 or later

If your smartphones have an earlier version of the firmware, you cannot provision PEAP or EAP-TLS network settings on smartphones until the firmware has been updated. This is true whether you are using MSP or the Motorola EWP Provisioning Tool to configure Vocera smartphones.

If you are staging new smartphones for PEAP or EAP-TLS authentication and the phones do not have the required firmware, do NOT include network settings in the staging profile. Instead, stage the phone and keep it **tethered to the configuration computer during the entire staging process**. The phone can then successfully download the bundle, install the new **VoceraCAB** package, and then install the PEAP or EAP-TLS network settings.

Important: The PEAP or EAP-TLS network settings package should be listed *after* **VoceraCAB** in the bundle.

For more information about creating a staging profile without network settings, see [Creating a Staging Profile Without Network Settings](#) on page 69.

Authentication Servers and Certificates

If you are implementing PEAP or EAP-TLS, you will need an authentication server. Vocera has tested smartphones configured for PEAP and EAP-TLS using **Cisco Access Control Server (ACS)**.

For information on how to add a server certificate, set up a certificate authority, and install a trusted certificate on your authentication server, see your authentication server documentation:

- **Cisco ACS – PEAP/EAP-TLS Configuration Scenario**¹

For instructions on how to install a self-signed certificate on the smartphone, see **Installing a Certificate on the Smartphone** on page 131.

Device Authentication versus User Authentication

The PEAP protocol typically requires each user in a network environment to be authenticated with a unique set of credentials. However, Vocera supports device authentication, not user authentication. Consequently, each Vocera smartphone must have the same security properties. All Vocera smartphones must present the same set of credentials for network authentication.

Certificates from Trusted Certificate Authorities

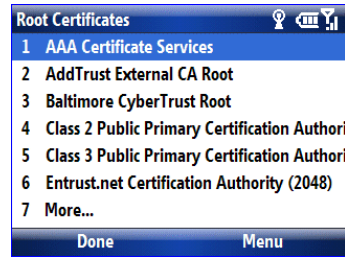
You will need to obtain a public key certificate to use for authenticating Vocera smartphones. If you purchase the certificate from a trusted Certificate Authority (such as Go Daddy), the root certificate is most likely already installed on the smartphone.

To view root certificates already installed on the smartphone:

1. Press **Start > All Programs > Settings > More (7) > Security > Certificates > Root**.

The Root Certificates dialog box appears.

¹ http://www.ciscosystems.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.1/configuration/guide/peap_tls.html

Figure C.1. Root Certificates dialog box

2. Select a root certificate—you may need to select **More...** a few times to see it—and press **Menu > View**.

Self-Signed Certificates

Self-signed certificates, like certificates from a trusted Certificate Authority, provide a secure, encrypted connection. With a self-signed certificate, the person who created the certificate assures that it is legitimate, rather than relying on a trusted Certificate Authority.

If you generate your own self-signed certificate, you will need to install it on every smartphone. See the next section.

Vocera Manufacturer Certificates Not Supported on Smartphones

Vocera provides client- and server-side certificates for B2000 and B3000 badges called Vocera Manufacturer Certificates. However, Vocera Manufacturer Certificates are not pre-installed on Vocera smartphones. If you want to use EAP-TLS authentication for Vocera smartphones, you need to either obtain certificates from a trusted CA, or generate your own certificates.

Installing a Certificate on the Smartphone

If you generated a self-signed certificate rather than purchasing a certificate from a trusted Certificate Authority, you need to install it on each smartphone.

To install a certificate on the smartphone using MSP:

1. Log into the MSP Console.
2. Create a Certificate Settings object and add the certificate(s) to it. See [Creating a Certificate Settings Object](#) on page 54
3. Deactivate provisioning policies that use the Vocera bundle.
4. Add the new Certificate Setting object to the Vocera bundle. Make sure the Certificate Setting object is listed before the VoceraCAB package.

5. Reactivate provisioning policies that use the Vocera bundle to push the certificate(s) to the phones.

To install a certificate on the smartphone by tethering it to a computer:

1. Connect the smartphone to the configuration computer using a USB cable.
2. Use Windows Mobile Device Center, ActiveSync, or Windows Explorer to copy the certificate to the **\My Documents\certs_to_install** folder on the phone.
3. On the smartphone, open File Manager and navigate to the **\My Documents\certs_to_install** folder.
4. Run the file. It is automatically added to the phone's certificate store.
5. For security reasons, delete the certificate file in the **\My Documents\certs_to_install** folder. This prevents the file from being copied to other devices.

Configuring PEAP Using MSP

This section describes how to use MSP to configure smartphones for PEAP.

To configure a smartphone for PEAP using MSP:

1. If you are using a self-signed certificate, first install the certificate on each smartphone. See [Installing a Certificate on the Smartphone](#) on page 131.

If you are using a certificate from a trusted Certificate Authority, you may not need to install the certificate on the phone.
2. Upload the latest version of **Network.WLAN.EWP.setting.xml** to the MSP Server. See [Uploading the Network.WLAN.EWP Setting Definition Document](#) on page 38.
3. Create a Network Settings object for your PEAP SSID. See [Creating a Network Settings Object](#) on page 42.

Figure C.2. Create Setting wizard for PEAP configuration

Settings > Setting Create

1 SETTING TYPE 2 SETTING INFO

1. Network.WLAN.EWP.setting.xml

Name: Virgo

Description: PEAP settings on Virgo

SSID: Virgo

Authentication: WPA-Enterprise (EAP)

WPA Enterprise:

Encryption: TKIP

EAP: PEAP

Identity: vocera

Password: *****

Disable Identity Protection: No

Server Certificate Selection: Use Standard CA Certificate

CKM: Enable

Back Finish Cancel

4. Add the latest **VoceraCAB** package to the Vocera bundle. Make sure the PEAP network settings package is listed *after* **VoceraCAB** in the bundle. For more information, see the following topics:
 - [Creating Bundles](#) on page 59
 - [Managing Package Versions](#) on page 77
5. Provision new PEAP network settings to Vocera smartphones that have been updated with the latest firmware. See [How to Use Provisioning](#) on page 79.
6. If you are staging new smartphones for PEAP authentication and the phones have firmware earlier than version 2.1.1, do NOT include network settings in the staging profile. See [Upgrading Smartphones to PEAP or EAP-TLS](#) on page 129.

Configuring EAP-TLS Using MSP

This section describes how to use MSP to configure smartphones for EAP-TLS.

Note: For EAP-TLS authentication, you do not need to specify an authentication username. Instead, the CN (common name) of the client certificate is the identity used during authentication.

To configure a smartphone for EAP-TLS using MSP:

1. Either generate your own self-signed, client- and server-side certificates or obtain certificates from a trusted Certificate Authority (CA).

Note: Note the password used to encrypt the client key. You will need this when you create a Certificate Settings object in the MSP Console.

2. Download the server-side certificates to your authentication server.
3. Install the certificates on each smartphone. See [Installing a Certificate on the Smartphone](#) on page 131.
4. Upload the latest version of **Network.WLAN.EWP.setting.xml** to the MSP Server. See [Uploading the Network.WLAN.EWP Setting Definition Document](#) on page 38.
5. Create a Network Settings object for your EAP-TLS SSID. See [Creating a Network Settings Object](#) on page 42.

Figure C.3. Create Setting wizard for EAP-TLS configuration

The screenshot shows a web-based configuration wizard titled 'Settings > Setting Create'. It has two tabs: '1 SETTING TYPE' and '2 SETTING INFO'. The '2 SETTING INFO' tab is active. Below the tabs, there's a section titled '1. Network.WLAN.EWP.setting.xml'. This section contains several form fields: 'Name' (text box with 'Capricorn'), 'Description' (text box with 'EAP-TLS on Capricorn'), 'SSID' (text box with 'Capricorn'), 'Authentication' (dropdown menu with 'WPA-Enterprise (EAP)' selected), 'WPA Enterprise' (text box), 'Encryption' (dropdown menu with 'TKIP' selected), 'EAP' (dropdown menu with 'TLS' selected), 'Server Certificate Selection' (dropdown menu with 'Use Standard CA Certificate' selected), 'Client Certificate (Issued By):' (text box), and 'CCKM' (dropdown menu with 'Disable' selected). At the bottom of the form are three buttons: 'Back', 'Finish', and 'Cancel'.

6. Add the latest **VoceraCAB** package to the Vocera bundle. Make sure the EAP-TLS network settings package is listed *after* **VoceraCAB** in the bundle. For more information, see the following topics:
 - [Creating Bundles](#) on page 59
 - [Managing Package Versions](#) on page 77

7. Provision new EAP-TLS network settings to Vocera smartphones that have been updated with the latest firmware. See [How to Use Provisioning](#) on page 79.
8. If you are staging new smartphones for EAP-TLS authentication and the phones have firmware earlier than version 2.3.5, do NOT include network settings in the staging profile. See [Upgrading Smartphones to PEAP or EAP-TLS](#) on page 129.

Configuring PEAP or EAP-TLS Using the Motorola EWP Provisioning Tool

For instructions on how to use the Motorola EWP Provisioning Tool to configure PEAP or EAP-TLS, see [Using the Motorola EWP Provisioning Tool](#) on page 113.



IP Port Usage

The following tables indicate the ports used by MSP Server for IP communication:

Table D.1. MSP Server IP port usage

Description	Protocol	Port No
Browser ↔ MSP Console	TCP	80 and 443 (for SSL)
FTP Server ↔ Smartphone	TCP	20 and 21
Note: Different ports are required based on the FTP mode used (Active vs. Passive). See below.	UDP	> 1023

Ports used when the FTP Server is in Passive Mode:

- FTP Server's port 21 from anywhere
(Client initiates connection)
- FTP Server's port 21 to ports > 1023
(Server responds to client's control port)
- FTP Server's ports > 1023 from anywhere
(Client initiates data connection to random port specified by server)
- FTP Server's ports > 1023 to remote ports > 1023
(Server sends acknowledgments and data to client's data port)

Ports used when the FTP Server is in Active Mode:

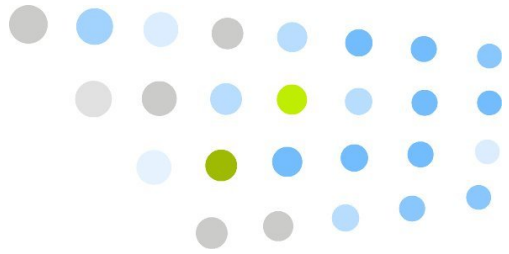
- FTP Server's port 21 from anywhere
(Client initiates connection)
- FTP Server's port 21 to ports > 1023
(Server responds to client's control port)
- FTP Server's port 20 to ports > 1023



(Server initiates data connection to client's data port)

- FTP Server's port 20 from ports > 1023

(Client sends acknowledgements to server's data port)



Index

Symbols

.NET Framework, installation, 21

A

abup30 package, 60
ActiveSync, 65, 110
authentication, 43, 116
 device, 130

B

backing up data (see database backup)
browser requirements, 15
Bundles
 creating, 59
 deployment steps, 59
 production site, 63
 provisioning, 77

C

CAB files
 DisableLocalRTA.cab, 126
 DisableLogs.cab, 126
 EnableLocalRTA.cab, 126
 EnableLogs.cab, 126
 ewpsecuritypolicyoff.cab, 119, 120, 122
 installer_SW_REL_number.cab, 119, 120, 122
 JBlendWM_Vocera.CAB, 119, 120, 122
 Provisioning Tool CAB, 119, 121, 122
 VoceraAppsInstaller.CAB, 119, 121, 122
 VoceraAppsSettings.CAB, 119, 121, 122
 VoceraDeleteRDCIcon.cab, 119, 121, 122
 VoceraRadio80211dDisable, 125
 VoceraRadio80211dEnable, 125



- VoceraRadioABG, 125
- VoceraRadioAChannelsDefault, 125
- VoceraRadioAOnly, 125
- VoceraRadioBGChannels-14711, 125
- VoceraRadioBGChannels-14811, 125
- VoceraRadioBGChannels-1611, 125
- VoceraRadioBGonly, 125
- CCKM, 45
- Certificate Settings, 53, 54
- certificates
 - self-signed, 131
 - trusted Certificate Authorities, 130
- checklist, post-installation, 107
- Clock.DataAndTime - TimeZone package, 60
- Clock.DateAndTime, 53
- Clock.DateAndTime Settings, 53
- Conditions, 58
- configuration computer, requirements, 14
- Content objects, 49

D

- database backup, 31
- DateAndTime package, 60
- debug folder, 125
- DisableLocalRTA CAB file, 126
- DisableLogs CAB file, 126
- dynamic deployment, 12

E

- EAP-TLS authentication, 129
- Enable CCKM, 117
- enable30 package, 61
- EnableLocalRTA CAB file, 126
- EnableLogs CAB file, 126
- encryption, 43, 116
- EWP Persistent REG Install, 39
- EWP_REG.xml, 39
- ewpsecuritypolicyoff CAB file, 119, 120, 122

F

- failed jobs, 92
- FileZilla, 96
- FTP Server
 - configuring, 19
 - troubleshooting, 94



G

GetAdapters package, 60

I

installation, 17

installer_SW_REL_number CAB file, 119, 120, 122

Internet Information Service (IIS)

FTP Service, 19

Internet Information Services (IIS)

installation, 17

Isolate Users mode, 98

J

JBlend_VM.trace.txt, 100

JBlendWM_Vocera CAB file, 119, 120, 122

L

Late Site Binding, 68

license key, 37

Log Upload tool, 98

logging, 125

Logs folder, 125

Vocera Apps, 100

M

Master Clear, 100

Message Set objects, 59

Microsoft SQL Server Management Studio Express, 31

Motorola EWP Provisioning Tool, 110, 111

MSP

administrative setup, 37

database backup, 31

documentation, 16

installation, 21

license key, 37

overview, 11

requirements, 14

MSP Administration Program, 93

MSP Agent shortcut, 74

MSP Console

logging in, 32

quick reference, 34

N

network and security information, collecting, 112



- Network Settings object, 42
- Network.WLAN.EWP, 53
- Network.WLAN.EWP.setting.xml, 38
- Network.WLAN.EWP.Site.SSID package, 62

O

- orphaned jobs, 92

P

Packages

- abup30, 60
- Clock.DataAndTime - TimeZone, 60
- DateAndTime, 60
- enable30, 61
- GetAdapters, 60
- managing versions, 77
- Network.WLAN.EWP.Site.SSID, 62
- uploading, 50
- VoceraApps, 52, 61
- VoceraCAB, 52, 61
- VoceraClientGatewayIPAddress, 52, 61
- VoceraJBlendJVM, 52, 61
- VoceraRadio80211d-disable, 52
- VoceraRadio80211d-enable, 52
- VoceraRadioBand-a, 52
- VoceraRadioBand-abg, 52
- VoceraRadioBand-bg, 52
- VoceraRadioBGChannels-14711, 53
- VoceraRadioBGChannels-14811, 53
- VoceraRadioBGChannels-1611, 52
- VoceraServerSSLCertificates, 61
- PEAP authentication, 129
- Policy object, 78
- post-installation checklist, 107
- prerequisite software, 16
- provisioning, 75
 - best practices, 80
 - Bundle, 77
 - Policy, 78
 - prerequisites, 75
 - status, 80

R

- radio settings, 124
- Rapid Deployment client, 67, 72
 - shortcut, 74, 119, 121, 122, 127



- Readiness Conditions, 59
- Relay Server object, 40
 - changing, 95

S

- Searching for Gateway message, 84
- self-signed certificates, 131
- Settings, 53
 - Certificate, 54
 - Date and Time, 53
- Site object, 45
- SSL, 39, 56
- staging, 65
 - best practices, 74
 - on-demand, 66
 - prerequisites, 65
 - profile, 67
 - status, 74
- system requirements, 14

T

- troubleshooting, 89
- trusted certificate authority, 130
- typical setup, 12

V

- verifying smartphone configuration, 83
- VMware support, 15
- Vocera Client Gateway computer, requirements, 14
- Vocera Root Certificate Install, 39
- Vocera Smartphone Information application, 86
- Vocera Smartphone software version, 86
- Vocera SP About application, 86
- Vocera_Cert.xml, 39
- VoceraApps package, 52, 61
- VoceraAppsInstaller CAB file, 119, 121, 122
- VoceraAppsSettings CAB file, 119, 121, 122
- VoceraCAB package, 52, 61
- VoceraClientGatewayIPAddress package, 52, 61, 92
- VoceraDeleteRDCIcon CAB file, 119, 119, 121, 121, 122, 122
- VoceraJBlendJVM package, 52, 61
- VoceraRadio80211d-disable package, 52
- VoceraRadio80211d-enable package, 52
- VoceraRadio80211dDisable CAB file, 125
- VoceraRadio80211dEnable CAB file, 125
- VoceraRadioABG CAB file, 125



- VoceraRadioAChannelsDefault CAB file, 125
- VoceraRadioAOnly CAB file, 125
- VoceraRadioBand-a package, 52
- VoceraRadioBand-abg package, 52
- VoceraRadioBand-bg package, 52
- VoceraRadioBGChannels-14711 CAB file, 125
- VoceraRadioBGChannels-14711 package, 53
- VoceraRadioBGChannels-14811 CAB file, 125
- VoceraRadioBGChannels-14811 package, 53
- VoceraRadioBGChannels-1611 CAB file, 125
- VoceraRadioBGChannels-1611 package, 52
- VoceraRadioBGonly CAB file, 125
- VoceraServerSSLCertificates package, 61

W

- Windows Mobile Device Center, 65, 110