

GroupWise® Mobility Service Installation Guide

October 2023

Legal Notices

Copyright 1993 - 2023 Open Text.

The only warranties for products and services of Open Text and its affiliates and licensors ("Open Text") are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Open Text shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Contents

About This Guide	5
1 GroupWise Mobility Service Product Overview	7
Mobility Server Configuration	7
Single Mobility Server System	8
Multiple Mobility Server System	8
Synchronization Capabilities	9
2 GroupWise Mobility Service System Requirements	11
Mobility Server Requirements	11
Hardware Requirements	11
Operating System Requirements	12
Directory Requirements	13
Web Browser Requirements for the Mobility Admin Console	13
GroupWise Requirements	13
Mobile Device Requirements	14
3 GroupWise Mobility Service Installation	15
Planning a Mobility System	15
Planning the Configuration of Your Mobility System	15
Selecting Mobility Servers	16
Gathering GroupWise Information	16
Preparing GroupWise as the User Source for Your Mobility System	16
Gathering GroupWise System Information	17
Gathering Mobile Device Information	19
Planning the Mobility Database	21
Establishing Mobility System Security	21
Preparing to Install the Mobility Service	22
Preparing the Linux Server	22
Opening Required Ports	23
Verifying GroupWise System Availability	23
Verifying Certificate Availability	24
Installing GroupWise Mobility Service	24
Obtaining the GroupWise Mobility Service 23.4 ISO	25
Running the Mobility Service Installation Program	25
Checking the Status of the Mobility Service	26
Using the Mobility Admin Console	26
Uninstalling the Mobility Service	26
Adding Users to Your Initial Mobility System	27
Testing Your Initial Mobility System	28
Managing Initial Synchronization of Users	28
Helping Mobile Device Users Understand Synchronization	29
Testing Synchronization	30
Integrating with Mobile Device Management Applications	30

Using OpenText ZENworks Mobile Management	30
What's Next.	32
Managing Your Mobility System.	32
Managing the GroupWise Sync Agent	32
Managing the Device Sync Agent	33
GroupWise Mobility Service Installation Worksheet	33
 4 Upgrading from GMS 18.3.1 or a Later Version	35
System Requirements.	35
Upgrading the GroupWise Mobility Service	35
Checking the Status of GMS after the Upgrade	35
 5 Migrating from GMS 18.3.0 or Earlier	37
Preparing to Migrate to GMS 18.4.x or Later Version	37
Installing a New GMS Server	38
Adding and Syncing Users and Data with the New GMS Server	38
Connecting Users with the New GMS Server	38
If Users Connect through DNS	38
If Users Connect Using an IP Address.	39
Decommissioning the Old GMS Server	39
 A GroupWise Mobility Service Installation Troubleshooting	41

About This Guide

This *GroupWise Mobility Service Installation Guide* helps you to understand and set up a GroupWise Mobility system by installing the GroupWise Mobility Service, which includes the GroupWise Sync Agent and the Mobility Sync Agent.

- ♦ [Chapter 1, “GroupWise Mobility Service Product Overview,” on page 7](#)
- ♦ [Chapter 2, “GroupWise Mobility Service System Requirements,” on page 11](#)
- ♦ [Chapter 3, “GroupWise Mobility Service Installation,” on page 15](#)
- ♦ [Chapter 4, “Upgrading from GMS 18.3.1 or a Later Version,” on page 35](#)
- ♦ [Chapter 5, “Migrating from GMS 18.3.0 or Earlier,” on page 37](#)
- ♦ [Appendix A, “GroupWise Mobility Service Installation Troubleshooting,” on page 41](#)

Audience

This guide is intended for network administrators who install a Mobility system to provide data synchronization between GroupWise and mobile devices.

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comment feature at the bottom of each page of the online documentation.

Additional Documentation

Additional GroupWise Mobility Service documentation is found on the [GroupWise Documentation website](http://www.novell.com/documentation/groupwise) (<http://www.novell.com/documentation/groupwise>) and comprises:

- ♦ [GroupWise Mobility Service Release Notes](#)
- ♦ [GroupWise Mobility Service Administration Guide](#)
- ♦ [GroupWise Mobility Quick Start for Mobile Device Users](#)

In addition to the GroupWise Mobility Service product documentation, the following resources provide information about the Mobility Service:

- ♦ [OpenText Support and Knowledgebase](https://www.microfocus.com/en-us/support/) (<https://www.microfocus.com/en-us/support/>)
- ♦ [GroupWise Community](https://community.microfocus.com/t5/GroupWise-Products/ct-p/GW) (<https://community.microfocus.com/t5/GroupWise-Products/ct-p/GW>)
- ♦ [GroupWise Support Forums](https://community.microfocus.com/t5/GroupWise/ct-p/GroupWise) (<https://community.microfocus.com/t5/GroupWise/ct-p/GroupWise>)
- ♦ [GroupWise Product Website](https://www.microfocus.com/en-us/products/groupwise/overview) (<https://www.microfocus.com/en-us/products/groupwise/overview>)

1 GroupWise Mobility Service Product Overview

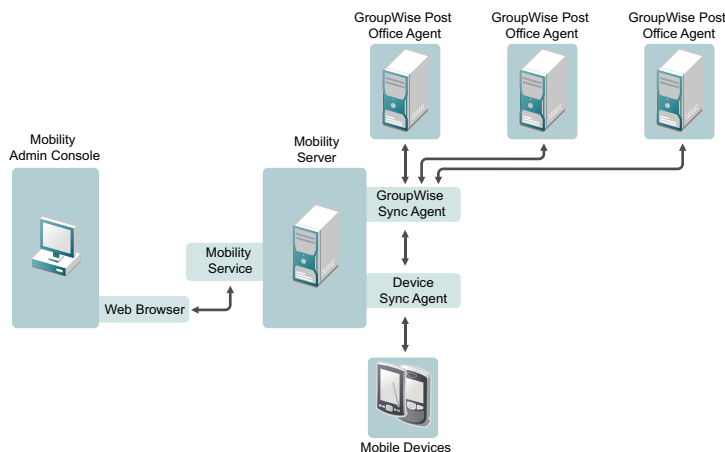
The GroupWise Mobility Service provides data synchronization between GroupWise mailboxes and mobile devices for synchronizing email, appointments, contacts, tasks, notes, and phone messages. The GroupWise Mobility Service is fast, reliable and scalable, and supports the latest device operating systems.

The GroupWise Mobility Service, the GroupWise Sync Agent, and the Device Sync Agent are installed together on a Linux server. A small Mobility system can consist of a single Mobility server. A large Mobility system can consist of multiple Mobility servers.

- ♦ [“Mobility Server Configuration” on page 7](#)
- ♦ [“Single Mobility Server System” on page 8](#)
- ♦ [“Multiple Mobility Server System” on page 8](#)
- ♦ [“Synchronization Capabilities” on page 9](#)

Mobility Server Configuration

The Mobility server must be able to communicate with other servers in your network and with mobile devices outside your firewall.



Component	Required Configuration
Sync Agents	The Mobility server has one instance of each sync agent. The GroupWise Sync Agent communicates with the GroupWise POA to obtain items from users' mailboxes. The Device Sync Agent transfers GroupWise mailbox items to and from users' mobile devices.

Component	Required Configuration
Mobility Admin Console	The web-based Mobility Admin console communicates with the Mobility Service to enable you to configure the sync agents and monitor your Mobility system.
User Source	You add users to your Mobility system from a GroupWise system. You access the Mobility Admin console as the <code>root</code> user of the server where the Mobility Service is installed.
GroupWise POA	<p>The Mobility Service must be able to communicate with one GroupWise Post Office Agent (POA) during installation. That POA, as well as additional POAs where mobile device users' mailboxes are located, must be configured to support Simple Object Access Protocol (SOAP) communication.</p> <p>The initial POA uses the native GroupWise redirection process to inform the GroupWise Sync Agent how to communicate with the additional POAs throughout your GroupWise system. Thereafter, the GroupWise Sync Agent communicates directly with each POA where mobile device users' mailboxes are located.</p> <p>IMPORTANT: A Mobility server can be configured to communicate with one GroupWise system. If you have multiple GroupWise systems, you must set up a Mobility server for each GroupWise system.</p>

Single Mobility Server System

A Mobility system with a single Mobility server can meet the synchronization needs of approximately 750 users with up to 1000 devices.

Multiple Mobility Server System

You might need to set up a Mobility system that includes multiple Mobility servers to support the following situations:

- ♦ **Number of Devices:** You need to support synchronization for more than 750 users with up to 1000 devices.

Setting up multiple Mobility servers in virtual machines can be a convenient way to support a large number of devices.
- ♦ **Location of Users:** You need to support users that are located in distant geographical locations where synchronization performance could be adversely affected by the network connections between users and a remote Mobility server.
- ♦ **Location of Synchronized Applications:** GroupWise has meaningful organizational segments (domains and post offices). Having a Mobility server associated with each post office helps balance the synchronization load across all GroupWise users.
- ♦ **Quality of Service:** Certain segments of your user population, such as executives of your organization, might expect and require a higher level of synchronization performance than other users. This higher quality of service can be accomplished by setting up a Mobility server specifically for such high-profile users.
- ♦ **Address Book Visibility:** The GroupWise Address Book is displayed on mobile devices from the point of view of a specific GroupWise user. As an example, you might have a group of mobile device users who need access to Address Book information about upper-level management in

your company and another group of mobile device users who should not have this Address Book information. To meet such needs, you would set up two Mobility servers, one with Address Book visibility that includes upper-level management, and a second one where such Address Book visibility is not provided.

Synchronization Capabilities

The following GroupWise item types can be synchronized to and from mobile devices:

- ♦ Email
- ♦ Appointments
- ♦ Tasks
- ♦ Notes
- ♦ Address books
- ♦ Contacts
- ♦ Phone messages
- ♦ Folders

As time passes, the following events can affect existing items, and the resulting changes in the items are also synchronized:

Items	Actions That Synchronize
Emails	<ul style="list-style-type: none">♦ Send/receive messages♦ Forward/reply to messages♦ Mark messages read/unread♦ Delete messages
Calendar Items	<ul style="list-style-type: none">♦ Send/receive appointments♦ Accept/decline appointments♦ Modify appointments♦ Post reminder notes
Tasks	<ul style="list-style-type: none">♦ Send/receive/post tasks♦ Accept/decline tasks♦ Mark tasks completed♦ Receive notifications of task completion♦ Change the due date and priority for posted tasks♦ Delete tasks
Contacts	<ul style="list-style-type: none">♦ Add new contacts♦ Delete contacts♦ Modify contact information, including all contact fields and photos
Phone Messages	<ul style="list-style-type: none">♦ Receive phone messages♦ Delete phone messages

Items	Actions That Synchronize
Folders	<ul style="list-style-type: none"> ♦ Add/delete folders ♦ Select/deselect folders for synchronization
Attachments	<ul style="list-style-type: none"> ♦ Forward full attachments even when the attachment size limit has been exceeded (on mobile devices that support Smart Forward functionality)

2 GroupWise Mobility Service System Requirements

Before you install the GroupWise Mobility Service, ensure that the Mobility server meets the following system requirements:

- ♦ [“Mobility Server Requirements” on page 11](#)
- ♦ [“Directory Requirements” on page 13](#)
- ♦ [“Web Browser Requirements for the Mobility Admin Console” on page 13](#)
- ♦ [“GroupWise Requirements” on page 13](#)
- ♦ [“Mobile Device Requirements” on page 14](#)

Mobility Server Requirements

This section contains information about hardware and operating system requirements.

- ♦ [“Hardware Requirements” on page 11](#)
- ♦ [“Operating System Requirements” on page 12](#)

Hardware Requirements

GroupWise hardware requirements include the following:

- ☐ x86-64 processor
- ☐ 2.8 GHz multi-processor system with a 4-Core CPU recommended
- ☐ Static IP address
- ☐ Adequate server memory depending on the number of devices supported by the Mobility server
 - ♦ 8 GB RAM to support approximately 300 devices
 - ♦ 12 GB RAM to support up to the maximum of 750 users with up to 1000 devices
- ☐ 45 MB of disk space for the Mobility Service software
- ☐ 200 GB of disk space recommended for data storage during system operation

Data storage disk space varies widely depending on the amount of data being synchronized, the number of devices participating in synchronization, the logging level for Mobility Service log files, and other variables specific to your Mobility system implementation.

The largest consumers of disk space are the Mobility database (`/var/lib/pgsql`) and Mobility Service log files (`/var/log/datasync`). You might want to configure the Mobility server so that `/var` is on a separate partition to allow for convenient expansion.

Another large consumer of disk space is attachment storage in the `/var/lib/datasync/mobility/attachments` directory.

Operating System Requirements

Mobility is supported on SLES 15 SP3 or later. Make sure your server meets the base server requirements and the requirements for the version of SLES you are using.

NOTE: Mobility is not supported on OES.

- ♦ [“Base Server Requirements” on page 12](#)
- ♦ [“SUSE Linux Enterprise Server \(SLES\) 15 SP3 or Later Requirements” on page 12](#)

Base Server Requirements

GroupWise base server requirements include the following:

- ☐ **Dedicated Server Required:** You should install GroupWise Mobility on its own server (virtual or physical) separate from other applications, including GroupWise.
- ☐ **File System Recommendation:** OpenText recommends EXT4 as the GMS server’s File System, which requires a manual change to the SLES installation defaults.
- ☐ **No Proxy Server with GMS:** Using a proxy server causes problems with the Mobility connection to the GroupWise server.
- ☐ **Registration Required or RMT Configured:** To receive the packages necessary to install Mobility, your SLES server must be registered or you must have a SLES Repository Mirroring Tool configured to provide them to the SLES server.

NOTE: An RMT is required to use the **air gap** option during the installation.

- ☐ **DNS Required:** Your Mobility server must be DNS resolvable.
- ☐ **Time Synchronization Required:** For the most reliable synchronization of time-sensitive items, such as appointments, the Mobility server and GroupWise servers should have their time synchronized as closely as possible. This is especially important on virtual machines.

In order for you to log in to the Mobility Admin console, your workstation and the Mobility server should have their time synchronized.

SUSE Linux Enterprise Server (SLES) 15 SP3 or Later Requirements

SLES 15 SP3 or later requires the following SLES modules/extension before you can install Mobility:

- ♦ Base system Module 15 (included with registration)
- ♦ Server Applications Module (included with registration)
- ♦ Desktop Applications Module (provides GNOME desktop)
- ♦ SUSE Package Hub

The easiest way to add modules and extensions is during the SLES 15 SP3 or later install. For more information on modules and extensions, see SUSE documentation, [Modules and Extensions Quick Start](#).

Directory Requirements

The GroupWise Mobility Service obtains users and groups directly from a GroupWise system, which might or might not utilize an LDAP directory for its user and group information.

See [GroupWise Requirements](#) for complete details.

Web Browser Requirements for the Mobility Admin Console

Any of the following web browsers:

- ☐ Mozilla Firefox - latest version
- ☐ Microsoft Edge - latest version
- ☐ Safari - latest version
- ☐ Google Chrome - latest version

GroupWise Requirements

In order for Mobility to interact successfully with GroupWise, your GroupWise system must meet the following requirements:

- ☐ GroupWise maintenance must be current. For more information, see “[Licensing](#)” in the *GroupWise Administration Guide*.
- ☐ GroupWise 18 or later domain.

For best synchronization performance, the latest version of GroupWise is strongly recommended.

NOTE: While newer version GroupWise domains are required, your POAs do not have to be updated to GroupWise 18 or later versions to work with these version of GroupWise Mobility Service.

- ☐ You must have at least a basic GroupWise system (one domain and one post office) set up and running. For more information, see “[GroupWise System Creation](#)” in the *GroupWise Installation Guide*.
- ☐ The GroupWise Post Office Agent (POA) that the GroupWise Sync Agent communicates with must have SOAP enabled.

The POA must also be configured with an HTTP user name and password on the Agent Settings property page of the POA object in the GroupWise Admin console (or in ConsoleOne in older GroupWise systems). This enables you to monitor SOAP threads in the POA web console.

The initial POA uses the native GroupWise redirection process to inform the GroupWise Sync Agent how to communicate with the additional POAs throughout your GroupWise system. Thereafter, the GroupWise Sync Agent communicates directly with each POA where mobile device users’ mailboxes are located.

IMPORTANT: All POAs that have Mobility users must have the same SSL setting--either all enabled for SSL or all disabled for SSL. All POAs should use the same SSL certificate, either GW Self-signed or Public.

- ❑ A GroupWise trusted application key is required so that the GroupWise Sync Agent can authenticate to GroupWise mailboxes without needing GroupWise users' mailbox passwords. For more information, see "[Creating a Trusted Application and Key](#)" in the *GroupWise Administration Guide*.
- ❑ A Mobility server can be configured to communicate with one GroupWise system. If you have multiple GroupWise systems, you must set up a Mobility server for each GroupWise system.

Mobile Device Requirements

The Device Sync Agent communicates with mobile devices by using the [Microsoft ActiveSync](#) protocol version 16.0.

If a mobile device uses an earlier version of ActiveSync, the device can still successfully communicate with the Device Sync Agent, but functionality specific to 16.0 is not available. If a mobile device uses a later version of ActiveSync, the device can still successfully communicate with the Device Sync Agent, because later versions of ActiveSync are backward compatible with version 16.0.

Supported mobile device operating systems include:

- ♦ Android 10 and 11 (latest version minus 1)
- ♦ Apple iOS 16 and 17 (latest version minus 1)

IMPORTANT: iOS 13 and later have new requirements for certificates. You need to make sure your certificates comply with these requirements for iOS 16 devices to connect to Mobility. The list of requirements can be found at <https://support.apple.com/en-in/HT210176>.

- ♦ Windows 10 Mail and Calendar Applications

A user can synchronize data to multiple mobile devices as needed.

Mobile devices communicate directly with the Device Sync Agent to synchronize data. Some mobile devices require a data plan to accomplish this. Others work successfully with a Wi-Fi connection. Some mobile devices can be configured to use either method. Your mobile device carrier is not involved in the synchronization process.

NOTE: The Device Sync Agent does not work with POP, IMAP, SMTP, or other message transfer protocols.

3 GroupWise Mobility Service Installation

The GroupWise Mobility Service Installation program available in YaST helps you install the Mobility Service software. You then use the Mobility Administration console to set up your Mobility system.

- ♦ [“Planning a Mobility System” on page 15](#)
- ♦ [“Preparing to Install the Mobility Service” on page 22](#)
- ♦ [“Installing GroupWise Mobility Service” on page 24](#)
- ♦ [“Adding Users to Your Initial Mobility System” on page 27](#)
- ♦ [“Testing Your Initial Mobility System” on page 28](#)
- ♦ [“Integrating with Mobile Device Management Applications” on page 30](#)
- ♦ [“What’s Next” on page 32](#)
- ♦ [“GroupWise Mobility Service Installation Worksheet” on page 33](#)

Planning a Mobility System

You can use the [GroupWise Mobility Service Installation Worksheet](#) to gather the information you need so that you are prepared to provide the information requested by the Mobility Service Installation program.

The topics in this section present the required information in a convenient planning sequence. The Installation Worksheet organizes the information in the order in which you need it during the installation process.

- ♦ [“Planning the Configuration of Your Mobility System” on page 15](#)
- ♦ [“Selecting Mobility Servers” on page 16](#)
- ♦ [“Gathering GroupWise Information” on page 16](#)
- ♦ [“Preparing GroupWise as the User Source for Your Mobility System” on page 16](#)
- ♦ [“Gathering GroupWise System Information” on page 17](#)
- ♦ [“Gathering Mobile Device Information” on page 19](#)
- ♦ [“Planning the Mobility Database” on page 21](#)
- ♦ [“Establishing Mobility System Security” on page 21](#)

Planning the Configuration of Your Mobility System

A Mobility system can consist of a single Mobility server or multiple Mobility servers. For planning guidelines, review the following sections as needed:

- ♦ [Single Mobility Server System](#)
- ♦ [Multiple Mobility Server System](#)

MOBILITY SERVICE INSTALLATION WORKSHEET

Print one copy of the [GroupWise Mobility Service Installation Worksheet](#) for each Mobility server that you are planning for your Mobility system.

If you plan to install the Mobility Service on multiple servers, you can proceed through the planning sections server by server, or you can apply each planning section to all planned servers, and then proceed to the next planning section.

IMPORTANT: For best security, plan to install the Mobility Service software on servers inside your DMZ.

Selecting Mobility Servers

Each server where you install the Mobility Service must meet the system requirements listed in [GroupWise Mobility Service System Requirements](#). The Mobility Service requires a static IP address.

MOBILITY SERVICE INSTALLATION WORKSHEET

Under **Mobility Service Server Information**, specify the IP address or DNS hostname of the server where you plan to install the Mobility Service software.

Gathering GroupWise Information

Mobility requires a GroupWise license to run. Mobility automatically connects to GroupWise to get the license information. During the install, you need to specify information for Mobility to connect to GroupWise.

MOBILITY SERVICE INSTALLATION WORKSHEET

Under **GroupWise Server Information**, specify the IP address or DNS hostname of the GroupWise server, along with the Admin Port (default is 9710), GroupWise Admin user, and GroupWise Admin password.

Preparing GroupWise as the User Source for Your Mobility System

The GroupWise Mobility Service obtains information about users and groups of users from a GroupWise system.

Use the GroupWise Admin console to manage the users and GroupWise groups that are added to your Mobility system.

This keeps user management in a single location for both your GroupWise system and your Mobility system.

Gathering GroupWise System Information

In order to configure the GroupWise Sync Agent as you run the Mobility Service Installation program, you need to gather certain information about the GroupWise system where users want to synchronize data to mobile devices.

- ♦ [“GroupWise Administration Agent” on page 17](#)
- ♦ [“GroupWise Trusted Application” on page 17](#)
- ♦ [“GroupWise Post Office Agent SOAP URL” on page 18](#)
- ♦ [“GroupWise Address Book User” on page 19](#)

GroupWise Administration Agent

The GroupWise Administration Agent is used to connect to the primary domain of the GroupWise system. You need to know the DNS name of the primary domain server, the port the admin service uses, and the credentials of a user that has admin privileges in GroupWise.

MOBILITY SERVICE INSTALLATION WORKSHEET

Under **GroupWise Administration Agent**, specify the DNS name of the primary domain server, the admin service port, and the admin user credentials.

GroupWise Trusted Application

A GroupWise trusted application can log in to a GroupWise Post Office Agent (POA) in order to access GroupWise mailboxes without needing personal user passwords. The GroupWise Sync Agent requires such mailbox access in order to synchronize GroupWise data with mobile devices. In addition, the Device Sync Agent uses trusted application ion through the GroupWise Sync Agent in order to access the GroupWise Address Book. This provides contact lookup beyond the contacts that are downloaded to users’ devices from personal address books.

Before you install the Mobility Service, you must set up the GroupWise Sync Agent as a GroupWise trusted application. You might name the trusted application `MobilityService` or `GroupWiseSyncAgent`.

A trusted application uses a key that consists of a long string of letters and numbers to provide ion for the GroupWise POA. The key file is initially created in a location that is accessible to GroupWise. You must transfer the key file to a location that is accessible to the Mobility Service Installation program.

When you set up the GroupWise Sync Agent as a trusted application, you must fill in *only* these three fields in the New Trusted App Key dialog box in the GroupWise Admin console (or in the Create Trusted Application dialog box in ConsoleOne in older GroupWise systems):

- ♦ **Name**
- ♦ **Location for Key File**
- ♦ **Name of Key File**

IMPORTANT: Do not fill in any other fields.

For more information, see “[Creating a Trusted Application and Key](#)” in the *GroupWise Administration Guide*.

Copy the key file to a convenient location on the Mobility server. The Installation program automatically transfers the trusted application key from the key file into the configuration of the GroupWise Sync Agent.

IMPORTANT: Do not use an existing trusted application key that is already in use by another application.

MOBILITY SERVICE INSTALLATION WORKSHEET

Under **GroupWise Trusted Application**, specify the name of the trusted application that you created and the location where the Mobility Service Installation program can access the trusted application key file.

You need to create only one trusted application key for the GroupWise Sync Agent, regardless of the number of servers where you install the Mobility Service, and regardless of the number of domains and post offices in your GroupWise system.

NOTE: If your GroupWise system connects to any external GroupWise domains, the external GroupWise system needs its own Mobility Service installation on an additional Mobility server, along with its own separate trusted application key.

GroupWise Post Office Agent SOAP URL

The GroupWise Sync Agent accesses your GroupWise system by communicating with a Post Office Agent (POA). The selected POA must be configured for SOAP.

The Mobility Service Installation program and the GroupWise Sync Agent need the IP address or DNS hostname of the server where the POA is running. In addition, they need the POA SOAP port. The default POA SOAP port is 7191.

Typically, the same port number is used regardless of whether the POA is configured for a secure SSL SOAP connection. The Mobility Service Installation program and the GroupWise Sync Agent need to know whether the connection is secure because they use one of the following URLs to communicate with the POA:

Non-Secure SOAP URL:	<code>http://poa_server_address:soap_port/soap</code>
Secure SOAP URL:	<code>https://poa_server_address:soap_port/soap</code>

MOBILITY SERVICE INSTALLATION WORKSHEET

Under **GroupWise Post Office Agent**, specify the IP address or DNS hostname of the server where a POA configured for SOAP is running. Specify the SOAP port, and whether or not the POA requires a secure SSL SOAP connection.

IMPORTANT: By default, the POA communicates with the GroupWise Sync Agent using port 4500 on the Mobility server. If there is a firewall between the Mobility server and the POA server, be sure to configure the firewall on the Mobility server to allow communication on port 4500 from the POA server. If necessary, you can configure the GroupWise Sync Agent to listen on a different port number after installation. For setup information, see [“Changing the GroupWise Sync Agent Listening Port”](#) in the *GroupWise Mobility Service Administration Guide*.

GroupWise Address Book User

The Device Sync Agent needs to be able to access the GroupWise Address Book to obtain user information. The Device Sync Agent establishes this access through the GroupWise Sync Agent.

The Device Sync Agent needs Address Book access that is equivalent to a typical user. You control what users see in the GroupWise Address Book by controlling object visibility. You want the Device Sync Agent to access the GroupWise Address Book with the same visibility that a typical GroupWise user has when viewing the GroupWise Address Book. For more information, see [“Controlling Object Visibility”](#) in the *GroupWise Administration Guide*.

You need to select a user whose view of the GroupWise Address Book matches what you want the Device Sync Agent to be able to access. You do not need to provide the password for the GroupWise user because the Device Sync Agent accesses the GroupWise Address Book through the GroupWise Sync Agent, which has trusted application status.

As an example, you might have a group of mobile device users who need access to Address Book information about upper-level management in your company and another group of mobile device users who should not have this Address Book information. To meet such needs, you would set up two Mobility servers, one with Address Book visibility that includes upper-level management, and a second one where such Address Book visibility is not provided. You would achieve this by setting up each Mobility server with an Address Book user whose Address Book visibility provides the visibility appropriate for all users on that Mobility server.

MOBILITY SERVICE INSTALLATION WORKSHEET

Under **GroupWise Address Book User**, specify a valid GroupWise user name that the Device Sync Agent can use to access the GroupWise Address Book to obtain contact information.

Gathering Mobile Device Information

The Device Sync Agent needs certain configuration information about the mobile devices that it synchronizes GroupWise data with.

- ♦ [“Device Connection Port” on page 20](#)
- ♦ [“Server Certificate” on page 20](#)

Device Connection Port

By default, the Device Sync Agent uses all available IP addresses on the Mobility server. You can bind the Device Sync Agent to a specific IP address after installation. For setup information, see “[Binding to a Specific IP Address](#)” in the *GroupWise Mobility Service Administration Guide*.

Typically, the Device Sync Agent uses port 443 for secure SSL HTTP connections with mobile devices and port 80 for non-secure HTTP connections. If mobile devices connect directly to the Device Sync Agent, a secure HTTP connection is strongly recommended. If mobile devices connect to the Device Sync Agent through a security application such as OpenText Access Manager or OpenText ZENworks Mobile Management, the Device Sync Agent can appropriately be configured with a non-secure HTTP connection. For more information, see [Integrating with Mobile Device Management Applications](#).

MOBILITY SERVICE INSTALLATION WORKSHEET

Under **Device Connection Port**, mark whether you want to configure the Device Sync Agent to use a secure or non-secure HTTP port to communicate with mobile devices. Specify the port number used by the mobile devices that your Mobility system supports.

IMPORTANT: If there is a firewall between the Mobility server and users’ mobile devices, be sure to configure the firewall to allow communication on the selected HTTP port (443 or 80).

Server Certificate

In order to use a secure SSL HTTP connection between the Device Sync Agent and mobile devices, a CA-signed server certificate is required. If you do not already have a certificate signed by a certificate authority (CA) for the Mobility server, the Mobility Service Installation program can generate a self-signed certificate for you. However, you must obtain and install a commercially signed certificate in order for iOS 13 and later devices to connect to the Mobility Service.

IMPORTANT: The list of certificate requirements for iOS 13 and later devices is found at <https://support.apple.com/en-in/HT210176>.

If you have the installation program generate a temporary self-signed certificate, you must replace it as soon as possible with a CA-signed replacement by doing the following.

- 1 On the Mobility server, navigate to `/var/lib/datasync`.
- 2 Rename the `gms_mobility.pem` certificate file to `gms_mobility.pem.old`.
- 3 Copy the CA-signed replacement certificate file to `/var/lib/datasync`.
- 4 Rename the CA-signed file to `gms_mobility.pem`.

IMPORTANT: Do not modify or replace the `gms_server.pem` file. This is used only within the GMS server itself

- 5 At the terminal prompt, enter `gms restart`.

All devices should now be able to connect to the Mobility server.

MOBILITY SERVICE INSTALLATION WORKSHEET

Under **Mobile Device Port**, specify the location of the CA-signed certificate file. Ensure that the location is accessible to the Mobility Service Installation program on the Mobility server.

For more information about certificates, see “[Securing Communication between the Device Sync Agent and Mobile Devices](#)” in the *GroupWise Mobility Service Administration Guide*.

Planning the Mobility Database

When you run the Mobility Service Installation program, it creates a PostgreSQL database that is used to store the Mobility system configuration information that you see in the Mobility Admin console. It also stores pending events when synchronization is interrupted.

The Mobility Service database is named `datasync`, and the user that has access is named `datasync_user`. You must supply the password for the Mobility Service database user.

IMPORTANT: Choose the password carefully, because you cannot change it. Do not use an asterisk (*) or a semi-colon (;) in the password.

MOBILITY SERVICE INSTALLATION WORKSHEET

Under **Mobility Database**, specify the password that you want to use for the Mobility Service database.

Establishing Mobility System Security

Configuration and administration of your Mobility system is performed through the Mobility Administration console. From the Mobility Admin console, you can do the following:

- ♦ Add users, groups of users, and resources to your Mobility system
- ♦ Configure and monitor the sync agents
- ♦ Configure integration with other applications such as ZENworks Mobile Management and KeyShield SSO

To protect your Mobility system operation and configuration, the Mobility Admin console is protected by a user name and password. You log in to the Mobility Admin console by using the `root` user name and password.

MOBILITY SERVICE INSTALLATION WORKSHEET

Under **root Access to Mobility Admin Console**, specify the `root` password on the Mobility server.

You can add more users as Mobility administrators after installation. For more information, see “[Adding GroupWise Users as Mobility Administrators](#)” in the *GroupWise Mobility Service Administration Guide*.

Preparing to Install the Mobility Service

The Mobility Service Installation program cannot run successfully unless you have properly prepared the environment where you run it.

- ♦ [“Preparing the Linux Server” on page 22](#)
- ♦ [“Opening Required Ports” on page 23](#)
- ♦ [“Verifying GroupWise System Availability” on page 23](#)
- ♦ [“Verifying Certificate Availability” on page 24](#)

Preparing the Linux Server

To prepare the Linux server for the Mobility Service installation:

- 1 Ensure that the Linux server where you plan to install the Mobility Service meets the system requirements listed in [GroupWise Mobility Service System Requirements](#).
- 2 Ensure that the Mobility server has a static IP address.
- 3 Ensure that the Mobility server has a valid hostname. This should be the same FQDN that is in the SSL certificate for communicating with the GroupWise agents.

You can check this using the following command:

```
hostname -f
```

If your SLES server is properly configured, this command returns the hostname of the server.

If you need to configure the server with a hostname:

- 3a In YaST, click **Network Devices** > **Network Settings**.
 - 3b Click the **Hostname/DNS** tab.
 - 3c In the **Hostname** field, specify the hostname of the Mobility server, then click **OK**.
 - 3d Exit YaST.
 - 3e Repeat the `hostname -f` command to verify the hostname.
- 4 Ensure that the Linux operating system media is available.

The Mobility Service Installation program might need to install additional operating system RPMs that are required by the Mobility Service. The Mobility Service Installation program can access the operating system files from a SUSE repository or from a SLES Repository Mirroring Tool (RMT) if you have one configured for the Mobility server.

NOTE: An RMT is required to use the **air gap** option during the installation.

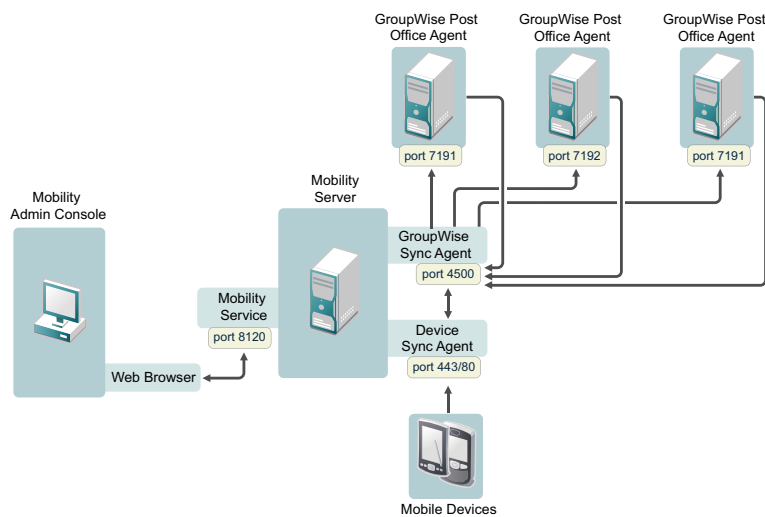
- 5 Continue with [Opening Required Ports](#).

Opening Required Ports

To open the required ports for the Mobility Service installation:

- 1 Ensure that any firewalls between the Mobility server and other applications have been configured to allow communication on the following ports:

Port Number	On Server	Description
7191	POA	GroupWise Post Office Agent (POA) SOAP port
4500	Mobility	GroupWise Sync Agent listening port for event notifications
443/80	Mobility	Mobile device secure or non-secure port
8120	Mobility	Mobility Admin console port



The GroupWise Sync Agent initially communicates with the POA that you specify during Mobility Service installation on the SOAP port that you specify. As users connect their mobile devices, the GroupWise Sync Agent determines from the initial POA the IP addresses and port numbers of all POAs where mobile device users have their mailboxes. Therefore, the GroupWise Sync Agent can communicate with multiple POAs throughout your GroupWise system.

- 2 Continue with [Verifying GroupWise System Availability](#).

Verifying GroupWise System Availability

To verify the GroupWise system is available:

- 1 Ensure that the GroupWise trusted application key for the GroupWise Sync Agent is accessible to the Mobility Service Installation program on the Mobility server.

For more information, see “[Creating a Trusted Application and Key](#)” in the *GroupWise Administration Guide*.

- 2 Ensure that the GroupWise POA that the GroupWise Sync Agent will communicate with is configured for SOAP.

- 3 Ensure that the GroupWise POA is currently running.
- 4 Continue with [Verifying Certificate Availability](#).

Verifying Certificate Availability

To verify certificate availability:

- 1 Assuming that you have a signed certificate from a certificate authority (CA) as required for configuring secure HTTP connections with mobile devices, do the following:
 - 1a Ensure that the certificate file is accessible to the Mobility Service Installation program on the Mobility server.
 - 1b If the key file that you received with the certificate included a password, ensure that the password has been removed.
 - 1c If you received the certificate as multiple files, ensure that you have combined the files into one certificate file.

For instructions, see “[Securing Communication between the Device Sync Agent and Mobile Devices](#)” in the *GroupWise Mobility Service Administration Guide*.
- 2 Continue with [Installing GroupWise Mobility Service](#).

Installing GroupWise Mobility Service

Before you run the Mobility Service Installation program, ensure that you have done the following:

- ☐ Review [Planning a Mobility System](#).
- ☐ Fill out the [GroupWise Mobility Service Installation Worksheet](#).

If you are setting up a multi-server Mobility system, ensure that you have an Installation Worksheet for each Mobility server. Each Mobility server is independent of other Mobility servers, so you can set them up in whatever order is convenient, based on the overall configuration of your Mobility system.
- ☐ Complete the tasks in [Preparing to Install the Mobility Service](#).

The following sections step you through the process of installing the Mobility Service and configuring a Mobility system.

- ♦ “[Obtaining the GroupWise Mobility Service 23.4 ISO](#)” on page 25
- ♦ “[Running the Mobility Service Installation Program](#)” on page 25
- ♦ “[Checking the Status of the Mobility Service](#)” on page 26
- ♦ “[Using the Mobility Admin Console](#)” on page 26
- ♦ “[Uninstalling the Mobility Service](#)” on page 26

Obtaining the GroupWise Mobility Service 23.4 ISO

To download the GroupWise Mobility Service installation package:

- 1 GroupWise Mobility Service software is available through the [OpenText Customer Care Center](#).
- 2 Download the GroupWise Mobility Service ISO to a convenient temporary directory on the Mobility server.

```
groupwise-mobility-service-23.4-x86_64-build_number.iso
```

- 3 Continue with [Running the Mobility Service Installation Program](#).

Running the Mobility Service Installation Program

Mobility is supported on SLES 15 SP3, which uses an ISO based install.

If you encounter any problems during the installation, check the Mobility Service Installation program log file for information about the problem:

```
/var/log/datasync/install.log
```

For additional assistance, see [GroupWise Mobility Service Installation Troubleshooting](#).

- 1 Before running the installation program, make sure your SLES 15 SP3 server meets all the of [GroupWise Mobility Service System Requirements](#).
- 2 Browse to the location where the Mobility Service ISO is located in a terminal and mount the ISO by running the following command:

```
mount groupwise-mobility-service-23.4-x86_64-build_number.iso /mnt
```

- 3 Browse to /mnt in the terminal and run the following command to run the install:

```
./install.sh
```

NOTE: When prompted about the **air gap** install, you should enter “no” unless you are using an air gap-type environment where your GMS server is connected to a SLES Repository Mirroring Tool (RMT) to get any required SUSE packages without connecting directly to SUSE.

The Mobility Service Installation program creates the following directories and files:

```
/opt/novell/datasync
/usr/sbin/gms (symbolic link)
/etc/datasync
/var/lib/datasync
/var/log/datasync
/var/run/datasync
/var/lib/pgsql
```

- 4 Once the files have installed, use the [GroupWise Mobility Service Installation Worksheet](#) to configure GroupWise Mobility Service.

Checking the Status of the Mobility Service

The Mobility Service Installation program starts the Mobility Service for you. If the installation proceeded normally, all components of the Mobility Service should be running.

- 1 In a terminal window on the Mobility server, become `root` by entering `su -` and the root password.
- 2 Use the following command to check the status of the Mobility Service:

```
gms status
```

- 3 Use the following commands to manually start and stop the Mobility Service:

```
gms start
gms restart
gms stop
```

Using the Mobility Admin Console

The Mobility Service Installation program starts the GroupWise Sync Agent and the Device Sync Agent for you. Use the Mobility Admin console to check sync agent status.

- 1 In your web browser, access the Mobility Admin console at the following URL:

```
https://mobility_server_address:8120
```

Replace *mobility_server_address* with the IP address or DNS hostname of the server where the Mobility Service is installed.

- 2 Log in as the Mobility administrator.

The sync agents should display a status of **Running**.

- 3 (Conditional) If you encounter problems starting the sync agents, see the following troubleshooting resources:
 - ♦ [GroupWise Mobility Service Installation Troubleshooting](#)
 - ♦ “[GroupWise Mobility System Troubleshooting](#)” in the *GroupWise Mobility Service Administration Guide*
 - ♦ “[Working with Log Files](#)” in the *GroupWise Mobility Service Administration Guide*
- 4 Skip to [Adding Users to Your Initial Mobility System](#).

Uninstalling the Mobility Service

IMPORTANT: When you uninstall the Mobility Service software, certificate files are also deleted. If you have obtained commercially signed certificates for use in your Mobility system, back them up before you uninstall the Mobility Service software.

- 1 In a terminal window on the Mobility server, become `root` by entering `su -` and the root password.
- 2 Change to the following directory:

```
/opt/novell/datasync
```

3 Run the Mobility Uninstallation script:

```
./uninstall.sh
```

The Uninstallation script stops the Mobility Service, the sync agents, and the PostgreSQL database server. It also uninstalls all Mobility Service RPMs, drops the Mobility Service PostgreSQL database, and deletes the following directories and files from the Mobility server:

```
/opt/novell/datasync  
/usr/sbin/gms (symbolic link)  
/etc/datasync  
/var/lib/datasync  
/var/log/datasync  
/var/run/datasync  
/var/lib/pgsql
```

Adding Users to Your Initial Mobility System

After you install the Mobility Service, use the Mobility Administration console to add users to your Mobility system. Initially, add a small number of users for testing purposes. The initial users should be active GroupWise users.

1 In your web browser, access the Mobility Admin console at the following URL:

```
https://mobility_server_address:8120
```

Replace *mobility_server_address* with the IP address or DNS hostname of the server where the Mobility Service is installed.

2 Log in as the Mobility administrator.

3 In the [Mobility Admin console](#), click **Users**, and then click **Add Users**.

4 In the **Search** field, type the first or last name of a specific user, and then click **Search**.

or

Click **Search** to list the users in the user source that the Mobility Admin console has been configured to search.

5 Select one or more users to add to your Mobility system.

6 Click **Add** to add the users to your Mobility system.

7 After you have tested your Mobility system, add the rest of your mobile device users.

For instructions, see “[GroupWise Mobility User Management](#)” in the *GroupWise Mobility Service Administration Guide*.

8 Continue with [Testing Your Initial Mobility System](#).

Testing Your Initial Mobility System

After you have added a few users to your Mobility system, you can watch the initial synchronization of their devices and send a few test messages.

- ♦ [“Managing Initial Synchronization of Users” on page 28](#)
- ♦ [“Helping Mobile Device Users Understand Synchronization” on page 29](#)
- ♦ [“Testing Synchronization” on page 30](#)

Managing Initial Synchronization of Users

From your point of view as the Mobility administrator, initial synchronization means that GroupWise data has been synchronized from GroupWise to the Mobility System. This means that the data is ready to be synchronized to users’ mobile devices as soon as users configure their devices to connect to the Mobility system.

Initial synchronization provides the following synchronization of GroupWise items:

- ♦ **Contacts** from all personal address books, excluding the Frequent Contacts address book

You can change this personal address book selection setting for users after installation in the Mobility Administration Console. For instructions, see [“Customizing a User’s Synchronization Settings”](#) in the *GroupWise Mobility Service Administration Guide*. Users can also change their own synchronization settings on the [Mobility Settings](#) page in the Mobility Administration Console. For more information, see the [GroupWise Mobility Quick Start for Mobile Device Users](#).

The GroupWise Address Book cannot be synchronized to mobile devices. However, users can still access individual contacts in the GroupWise Address Book if their mobile devices can do a Global Address List (GAL) lookup. As an alternative, users can create a personal address book that is a subset of the GroupWise Address Book to synchronize to their mobile devices.

- ♦ **Calendar items** (appointments and reminder notes) from the last two weeks and all future calendar items

Shared calendars are synchronized only for the owners of the shared calendars. If shared calendars are very important to users, shared calendar owners can post them to the Internet. For more information, see [“Publishing Personal Calendars on the Internet”](#) in the *GroupWise Client User Guide*.

After the owner publishes the calendar, other users can view the calendar URL in the web browser on their mobile devices.

To provide this functionality, at least one Calendar Publishing Host must be set up in the GroupWise system. For more information, see [“Setting Up the GroupWise Calendar Publishing Host”](#) in the *GroupWise Installation Guide*.

- ♦ **Email messages** in the Mailbox folder for the last three days

If users want to receive more existing email messages on their devices, they can configure their mobile devices to request additional existing email messages.

- ♦ **Tasks** with due dates in the last two weeks and all future tasks

Completed and uncompleted tasks are synchronized. Posted and group tasks are synchronized. Tasks that originate as other GroupWise item types (such as emails or calendar items) are synchronized as tasks when they are dragged to the Tasklist, when they are displayed in the Tasklist, or when they are changed to tasks.

The GroupWise Tasklist does not synchronize to mobile devices. You cannot create a tasklist on a mobile device that is associated with a GroupWise account.

- ♦ **Phone messages** for the last three days
- ♦ **Folders** in the Cabinet (but not items in folders until users request them by opening folders on their mobile devices)
- ♦ **Attachments** if they do not exceed your Mobility system size limits

If an item has an attachment that does not synchronize, a message notifies the user. For more information, see “[Controlling Synchronization Size Limits](#)” in the *GroupWise Mobility Service Administration Guide*.

When you add several users to your Mobility system at the same time, initial synchronization is performed for four users at a time. When it finishes with one of the four users, it starts on another user.

You can monitor the progress of initial synchronization in the Mobility Administration Console. For instructions, see “[Monitoring User Status](#)” and “[Monitoring Device Status](#)” in the *GroupWise Mobility Service Administration Guide*.

IMPORTANT: You should complete initial synchronization before you notify users to configure their mobile devices. Initial synchronization can take a substantial amount of time, depending on the amount of data to synchronize.

Occasionally, initial synchronization fails, and troubleshooting is required. For assistance, see “[Device Troubleshooting](#)” in the *GroupWise Mobility Service Administration Guide*.

Helping Mobile Device Users Understand Synchronization

Connecting to the Mobility system requires that Users correctly configure their mobile devices.

To help them, we strongly recommend that you do one or both of the following:

1. Print and distribute the [GroupWise Mobility Quick Start for Mobile Device Users](#) to them.
2. Email them the link to the Quick Start https://www.novell.com/documentation/groupwise23/pdfdoc/gwmob_qs_user/gwmob_qs_user.pdf.

TIP: To make the configuration process easier, see “[Using Autodiscovery to Simplify Mobile Device Setup](#)” in the *GroupWise Mobility Service Administration Guide*.

Testing Synchronization

To test GroupWise synchronization with mobile devices:

- 1 Test GroupWise data synchronization by logging in to your GroupWise mailbox and sending yourself an email message.
- 2 Reply to the message from your mobile device.
If the message synchronizes to your mobile device and the reply on your mobile device synchronizes back to GroupWise, your basic Mobility system is up and running.
- 3 (Conditional) If the message does not synchronize successfully, see the following troubleshooting resources:

In this *GroupWise Mobility Service Installation Guide*:

- ♦ [GroupWise Mobility Service Installation Troubleshooting](#)

In the *GroupWise Mobility Service Administration Guide*:

- ♦ [“Device Troubleshooting”](#)
- ♦ [“Mobility Service Troubleshooting”](#)
- ♦ [“GroupWise Sync Agent Troubleshooting”](#)
- ♦ [“Device Sync Agent Troubleshooting”](#)

- 4 To customize and expand your Mobility system, see [What’s Next](#).

Integrating with Mobile Device Management Applications

The GroupWise Mobility Service can be used with mobile device management (MDM) applications to manage your mobile devices. Because GroupWise Mobility Service 23 supports ActiveSync 16.0, it can be used any MDM solution that supports ActiveSync 16.0.

To configure Mobility to use an MDM, populate the Mobility Admin console > **Config** > **General** > **MDM Server** field with the IP address of your MDM server.

If you are using OpenText ZENworks Mobile Management, follow the steps in [Using OpenText ZENworks Mobile Management](#) for detailed instructions on configuring ZENworks Mobile Management and Mobility.

Using OpenText ZENworks Mobile Management

When you configure ZENworks Mobile Management to work with your Mobility system, all of the powerful features of ZENworks Mobile Management are available for managing the mobile devices of your GroupWise users.

- 1 Follow the instructions in [“Configuring an ActiveSync Server”](#) and [“Connecting to a New ActiveSync Server”](#) in the *ZENworks Mobile Management Reference*.

NOTE: OpenText ZENworks Mobile Management is a mobile device management solution that provides centralized management and control of mobile devices throughout your enterprise network. For complete information, see the [ZENworks Mobile Management Reference](#) on the [ZENworks Documentation website](#).

- 2 Ensure that your GroupWise mobile device users have been added to ZENworks Mobile Management.
- 3 Configure your Mobility system with information about ZENworks Mobile Management:
 - 3a In the [Mobility Administration Console](#), click **Config**.
 - 3b On the **General** page, scroll down to the **MDM Server** field.
 - 3c Specify the IP address of the ZENworks Mobile Management server where you provided information about your Mobility server.
 - 3d (Conditional) If you configured multiple ZENworks Mobile Management servers with information about your Mobility server, specify the IP addresses in a comma-delimited list.
 - 3e Click **Save** to save the new setting(s).
 - 3f Restart the Mobility Service:

```
gms restart
```
- 4 View the GroupWise mobile device users that have been added to ZENworks Mobile Management:
 - 4a From the ZENworks Mobile Management Dashboard, click **Users**.
 - 4b Scroll horizontally to view various types of information about GroupWise users and their mobile devices, including the following:
 - ♦ Time of last synchronization
 - ♦ Phone number
 - ♦ Mobile device model
 - ♦ Mobile device operating system and version
- 5 Verify that the configuration is successful:
 - 5a In the [Mobility Administration Console](#), click **Users**, and then click a user who has a device to add.
 - 5b Add the new device through ZENworks Mobile Management.
 - 5c When the device appears on the User/Device Actions page, verify that it has `_zmm` appended to the device ID.

The `_zmm` on the device ID shows that the user connected the device to your Mobility system through ZENworks Mobile Management.

If you require existing mobile device users to re-add their devices through ZENworks Mobile Management, they initially have two device IDs, one with `_zmm` and one without. This prevents ZENworks Mobile Management requests from conflicting with regular device requests. The old device ID disappears from the User/Device Actions page in about a month.

What's Next

See the sections below for information about managing the GroupWise Mobility Service and its components.

- ♦ [“Managing Your Mobility System” on page 32](#)
- ♦ [“Managing the GroupWise Sync Agent” on page 32](#)
- ♦ [“Managing the Device Sync Agent” on page 33](#)

Managing Your Mobility System

After your Mobility system is running smoothly, see the following sections in the [GroupWise Mobility Service Administration Guide](#) for instructions on maintaining your Mobility system:

- ♦ [“GroupWise Mobility Administration Console”](#)
- ♦ [“GroupWise Mobility System Management”](#)
- ♦ [“GroupWise Sync Agent Configuration”](#)
- ♦ [“Device Sync Agent Configuration”](#)
- ♦ [“GroupWise Mobility System Monitoring”](#)
- ♦ [“GroupWise Mobility User Management”](#)
- ♦ [“GroupWise Mobility Device Management”](#)
- ♦ [“GroupWise Mobility System Security”](#)
- ♦ [“GroupWise Mobility System Troubleshooting”](#)

Managing the GroupWise Sync Agent

After the GroupWise Sync Agent is successfully synchronizing data for the initial set of GroupWise users, see the following sections in the [GroupWise Mobility Service Administration Guide](#) for instructions on customizing and maintaining the GroupWise Sync Agent:

- ♦ [“Selecting GroupWise Items to Synchronize”](#)
- ♦ [“Increasing GroupWise Sync Agent Reliability or Performance”](#)
- ♦ [“Ignoring Old GroupWise Items”](#)
- ♦ [“Clearing Accumulated GroupWise Events”](#)
- ♦ [“Changing the GroupWise Sync Agent Listening Port”](#)
- ♦ [“Enabling and Disabling SSL for POA SOAP Connections”](#)
- ♦ [“Matching GroupWise Configuration Changes”](#)
- ♦ [“Modifying or Preventing Synchronization of Specified Items by Using an XSLT Filter”](#)

Managing the Device Sync Agent

After the Device Sync Agent is successfully synchronizing data for the initial set of mobile device users, see the following sections in the [GroupWise Mobility Service Administration Guide](#) for instructions on customizing and maintaining the Device Sync Agent:

- ♦ [“Blocking/Unblocking All Incoming Devices”](#)
- ♦ [“Enabling a Device Password Security Policy”](#)
- ♦ [“Quarantining New Devices to Prevent Immediate Connection”](#)
- ♦ [“Controlling the Maximum Number of Devices per User”](#)
- ♦ [“Removing Unused Devices Automatically”](#)
- ♦ [“Controlling the Maximum Number of Devices per User”](#)
- ♦ [“Binding to a Specific IP Address”](#)
- ♦ [“Enabling a Device Password Security Policy”](#)
- ♦ [“Changing the Address Book User”](#)

GroupWise Mobility Service Installation Worksheet

NOTE: If you are using any versions of Python 3, do not use exclamation mark (!) or period (.) characters in any of the passwords listed in the worksheet; otherwise the installation could fail.

Installation Field	Value for Your Mobility System	For More Information, See
(optional) Air Gap		Base Server Requirements
SLES Repository Mirroring Tool (RMT) is required prior to installation.		
Mobility Server Information		Selecting Mobility Servers
♦ IP address		
♦ Hostname		
GroupWise Server Information		
♦ Hostname		
♦ Port (9710)		
♦ Admin User name		
♦ Admin Password		
GroupWise User Source		Preparing GroupWise as the User Source for Your Mobility System

Installation Field	Value for Your Mobility System	For More Information, See
Mobility Service Database		Gathering Mobile Device Information.
<ul style="list-style-type: none"> ♦ Database name: <code>datasync</code> ♦ Database user: <code>datasync_user</code> ♦ Database password 		
GroupWise Administration Agent		GroupWise Administration Agent.
<ul style="list-style-type: none"> ♦ Admin Agent DNS hostname ♦ Admin Agent port Default port: 9710 ♦ User with admin privileges 		
GroupWise Trusted Application		GroupWise Trusted Application.
<ul style="list-style-type: none"> ♦ Trusted application name ♦ Trusted application key file 		
GroupWise Post Office Agent		GroupWise Post Office Agent SOAP URL.
<ul style="list-style-type: none"> ♦ POA IP address or DNS hostname ♦ POA SOAP port Default port: 7191 ♦ Secure: Yes / No 		
GroupWise Address Book User:		GroupWise Address Book User.
root Access for Mobility Admin Console		Establishing Mobility System Security
<ul style="list-style-type: none"> ♦ root password 		

4 Upgrading from GMS 18.3.1 or a Later Version

IMPORTANT: The upgrade process described in this chapter only applies to existing GMS 18.3.1 or later version GMS servers.

If you are running GMS 18.3.0 or earlier, you must follow the process in [Migrating from GMS 18.3.0 or Earlier](#)

Complete the following steps to update to the latest version of GroupWise Mobility Service:

- “System Requirements” on page 35
- “Upgrading the GroupWise Mobility Service” on page 35
- “Checking the Status of GMS after the Upgrade” on page 35

System Requirements

Make sure your server meets the requirements found in [GroupWise Mobility Service System Requirements](#).

Upgrading the GroupWise Mobility Service

Follow the steps below to upgrade a GMS 18.3.1 or later server to a later version of GMS:

- ☐ Download the ISO for GMS 18.3.1 or later from the OpenText Customer Center.
- ☐ In a terminal, mount the GMS ISO using the following command:

```
mount <path to the GMS ISO> /mnt
```
- ☐ Browse to `/mnt` and run the `install.sh`.
- ☐ Follow the prompts to upgrade GMS.

Checking the Status of GMS after the Upgrade

The Mobility Service installation script starts GMS for you. If the update proceeded normally, all components of GMS should be running.

- 1 In a terminal window on the GMS server, become `root` by entering `su -` and the root password.
- 2 Use the following command to check the status of GMS:

```
gms status
```

3 Use the following commands to manually start and stop GMS:

```
gms start  
gms restart  
gms stop
```

5 Migrating from GMS 18.3.0 or Earlier

The following sections offer suggestions for migrating to GMS 18.3.2 system with as little disruption to your current GMS system as possible.

- ♦ [“Preparing to Migrate to GMS 18.4.x or Later Version” on page 37](#)
- ♦ [“Installing a New GMS Server” on page 38](#)
- ♦ [“Adding and Syncing Users and Data with the New GMS Server” on page 38](#)
- ♦ [“Connecting Users with the New GMS Server” on page 38](#)
- ♦ [“Decommissioning the Old GMS Server” on page 39](#)

Preparing to Migrate to GMS 18.4.x or Later Version

Terminology:

- ♦ **Server1:** Your current GMS server.
- ♦ **IP1:** The static IP address assigned to your current GMS server.
- ♦ **DNS1:** The DNS name associated with IP1.
- ♦ **Server2:** Your new GMS server.
- ♦ **IP2:** The static IP address that you assign to Server2.
- ♦ **DNS2:** The DNS name associated with IP2.

Prerequisites:

- ☐ A GMS 18.3.0 or earlier server (Server1) that currently provides mobility services for your GroupWise mobile-device users.
- ☐ (Preferred) Your mobility users connect to Server1 using an assigned DNS name (DNS1).
(Migrations where users connect with only an IP address are possible, but the process requires more user downtime.)
- ☐ A new SLES 15 SP3 or later server (Server2) for exclusive use by GMS 18.4.x or later version that meets all of the requirements outlined in [Mobility Server Requirements](#).

IMPORTANT: Make sure to check Server1’s percentage of free storage space on the disk containing the `/var` folder. If free space is getting low, be sure to allocate more when installing the new server.

- ☐ An IP address (IP2) and associated DNS name (DNS2) to assign to the new GMS server
- ☐ Adequate time for the initial synchronization of users’ data before the planned cut-over date.
Initial data synchronization can take an extended period of time, depending on the quantity of data and the number of shared folders and calendars.

Installing a New GMS Server

To install a new GroupWise Mobility Service server:

- 1 Install a new SLES 15 SP3 or later server (Server2) and give it a static IP address (IP2) and DNS hostname (DNS2).

For instructions, see [Preparing the Linux Server](#).

- 2 Install Mobility 23.4 on Server2.

For instructions, see [Installing GroupWise Mobility Service](#).

Adding and Syncing Users and Data with the New GMS Server

To add and synchronize users with the GroupWise Mobility Service server:

- 1 After the new GMS server is installed and running on Server2, add your GMS users to Server2 by using the GMS Web Admin console.

For instructions, see [Adding Users to Your Initial Mobility System](#).

- 2 Adding users automatically begins the data synchronization process, which can take some time to complete. See [Managing Initial Synchronization of Users](#).
- 3 When you have verified that data synchronization is complete, continue with the next section,

Connecting Users with the New GMS Server

When all users display the status **Synced** in the GMS Web Admin Console, you can begin to transition them to Server2. For help, see [Helping Mobile Device Users Understand Synchronization](#). Make sure that users understand that because the GMS server is new, their devices must re-sync the GroupWise data.

Your next steps depend on how your mobility users connect with GMS.

IMPORTANT: Do not shut down your old GMS server (Server1) until you are directed to do so.

If Users Connect through DNS

If your users connected to Server1 using its DNS name (DNS1), change your DNS server's configuration so that DNS1 resolves to IP2 instead of IP1.

The next time mobile devices connect with GMS, they are automatically redirected to Server2.

Because Server2 is new, GroupWise data on each device is resynchronized.

NOTE: Having the old IP address (IP1) and its old related DNS name (DNS1) can be very useful going forward if you ever need to perform a server migration again, or if you need to set up a second GMS server for fail-over redundancy.

If Users Connect Using an IP Address

If your users connected to Server1 using its IP address (IP1), you must do the following:

- 1 Open the GMS Admin Console on Server1.
- 2 Delete all of the mobile users on Server1.
This temporarily makes GMS unavailable to mobile users.
- 3 Shut down Server1.
- 4 Add IP address IP1 to Server2.
Server2 now has two IP addresses assigned.
- 5 User devices begin connecting to Server2 through IP1 and their GroupWise data re-syncs.

Decommissioning the Old GMS Server

After verifying that your mobile users are successfully using the new GMS server, do the following:

- ♦ If your users connect using an IP address, you should have already deleted them from Server1 and shut it down.
- ♦ If your users connect using DNS, do the following:
 1. Open the GMS Admin Console on Server1.
 2. Delete all of the mobile users on Server1.
 3. Shut down Server1.

IMPORTANT: Deleting mobile users from Server1 while it is still connected to GroupWise, clears the server's user event configurations from the GroupWise POA, an important housekeeping task.

You can now re-purpose Server1 as needed.

A GroupWise Mobility Service Installation Troubleshooting

Possible causes and actions you can are provided for the issues below:

- ♦ [“The GroupWise Mobility Service Installation program does not behave as documented” on page 41](#)
- ♦ [“The GroupWise Mobility Service Installation program cannot communicate with the GroupWise POA” on page 41](#)
- ♦ [“The GroupWise Mobility Service Installation program cannot communicate with any required application” on page 42](#)
- ♦ [“The Mobility Service does not start” on page 42](#)
- ♦ [“You cannot access the Mobility Admin console after installation” on page 42](#)

See also the following sections in the GroupWise Mobility Service Administration Guide:

- ♦ [“Device Troubleshooting”](#)
- ♦ [“GroupWise Sync Agent Troubleshooting”](#)
- ♦ [“Device Sync Agent Troubleshooting”](#)
- ♦ [“Working with Log Files”](#)

The GroupWise Mobility Service Installation program does not behave as documented

Possible Cause: You are trying to install the GroupWise Mobility Service on 32-bit hardware.

Action: Install the GroupWise Mobility Service on 64-bit hardware that meets the system requirements described in [Mobility Server Requirements](#).

The GroupWise Mobility Service Installation program cannot communicate with the GroupWise POA

Possible Cause: A firewall is blocking communication between the Installation program and the POA server.

Action: Ensure that communication through the firewall is allowed on port 4500.

Possible Cause: The POA is not running.

Action: Start the POA.

Possible Cause: You specified the POA server settings incorrectly.

Action: Double-check the POA server settings you entered in the Installation program.

Possible Cause: There is a problem with the GroupWise trusted application key file.

Action: Re-create the GroupWise trusted application key file. You need to fill in only these three fields in the New Trusted App Key dialog box in the GroupWise Admin console (or in the Create Trusted Application dialog box in ConsoleOne in older GroupWise systems): **Name**, **Location for Key File**, and **Name of Key File**. Do not fill in any other fields.

The GroupWise Mobility Service Installation program cannot communicate with any required application

Possible Cause: The required port number is not open.

Action: Review the list of required port numbers in [Opening Required Ports](#).

Action: Use telnet to test whether ports are open.

- 1 Enter the following command in a terminal window:

```
telnet application_host port_number
```

Replace *application_host* with the IP address or DNS hostname of the server where the application is running.

Replace *port_number* with the port number on which the installation program is attempting to communicate with the application.

- 2 (Conditional) If the terminal windows goes blank, with the cursor in the upper-left corner, enter `quit` to exit the telnet session.

The port is open. The Installation program should be able to communicate with the application.

- 3 (Conditional) If a `Connection failed` message displays, open the port through the firewall to enable the Installation program to communicate with the application.

The Mobility Service does not start

Possible Cause: PostgreSQL is not running on the Mobility server.

Action: Check the status of PostgreSQL on the Mobility server, and start it manually if necessary.

```
rcpostgresql status  
rcpostgresql start
```

You cannot access the Mobility Admin console after installation

Possible Cause: The date and time on the Mobility server does not match the date and time on the GroupWise server.

Action: Reset the time on the Mobility server to match the time on the GroupWise server. This Mobility system requirement is listed in [Mobility Server Requirements](#).