GroupWise Mobility Service 18

Administration Guide

May 2023

Legal Notices

Contents

4 Device Sync Agent Configuration   45

5 GroupWise Mobility System Monitoring   51

6 GroupWise Mobility User Management   61

A GroupWise Mobility System Troubleshooting **101**

About This Guide

The *GroupWise Mobility Service 18 Administration Guide* helps you to manage your GroupWise Mobility system after you have set it up.

Audience

This guide is intended for network administrators who administer a Mobility system that provides 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 18 Documentation website (http://www.novell.com/documentation/groupwise18) and comprises:

- GroupWise Mobility Service 18 Release Notes
- GroupWise Mobility Service 18 Installation 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:

- Micro Focus Support and Knowledgebase (https://www.microfocus.com/support/GroupWise)
- GroupWise Community (https://community.microfocus.com/t5/GroupWise-Products/ct-p/GW)

- GroupWise Support Forums (https://community.microfocus.com/t5/GroupWise/ct-p/GroupWise)
- GroupWise Product Website (https://www.microfocus.com/en-us/products/groupwise/overview)

1 GroupWise Mobility Administration Console

Configuration of your GroupWise Mobility system is done through the Mobility Administration console. When you log in as the Mobility administrator, you can configure your Mobility system. When users log in using their user names and passwords they can control various aspects of data synchronization.

- "Accessing the Mobility Admin Console as an Administrator" on page 9
- "Accessing the Mobility Admin Console as a Mobile Device User" on page 10
- "Configuring the Mobility Admin Console" on page 10
- "Unlocking the Mobility Admin Console" on page 11

For a list of supported web browsers, see "Web Browser Requirements for the Mobility Admin Console" in the *GroupWise Mobility Service 18 Installation Guide*.

Accessing the Mobility Admin Console as an Administrator

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 Specify the user name of the Mobility administrator, either the `root` user or any other GroupWise user that has been added as a Mobility administrator (see Adding GroupWise Users as Mobility Administrators).

3 Specify the password for the user, then click **Login**.

   Mobility system configuration and administration is performed using the Mobility Admin console. For instructions, see the following sections:

   - Chapter 2, "GroupWise Mobility System Management," on page 13
   - Chapter 3, "GroupWise Sync Agent Configuration," on page 37
   - Chapter 4, "Device Sync Agent Configuration," on page 45
   - Chapter 5, "GroupWise Mobility System Monitoring," on page 51
   - Chapter 6, "GroupWise Mobility User Management," on page 61
   - Chapter 7, "GroupWise Mobility Device Management," on page 67

4 Click **Logout** to exit the Mobility Admin console.

Accessing the Mobility Admin Console as a Mobile Device User

Mobile device users can use the Mobility Admin console URL to access the Mobility Settings page by logging in with their personal user names and passwords. Users log in with their GroupWise (mailbox) user names and passwords.

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. Specify your GroupWise user name and password, then click **Login**.

3. View or print the *GroupWise Mobility Quick Start for Mobile Device Users* to learn how to use the Mobility Admin console Mobility Settings page.

Configuring the Mobility Admin Console

You can change the configuration of the Mobility Admin console to meet your administrative needs.

- ◆ "Adjusting the Mobility Admin Console Polling Rate for Groups of Users" on page 10
- ◆ "Using the Mobility Admin Console with a Single Sign-On Solution" on page 11
- ◆ "Adding GroupWise Users as Mobility Administrators" on page 11

Adjusting the Mobility Admin Console Polling Rate for Groups of Users

The Mobility Admin console locates GroupWise groups based on their `group_name.post_office.domain` location in your GroupWise system

When you add a group of users to your Mobility system, the group's existing members are added to the group as displayed in the Mobility Admin console. Subsequently, the Mobility Admin console polls for updates to group membership. This ensures that the group membership that is displayed in the Mobility Admin console always matches the membership in the GroupWise system.

By default, the Mobility Admin console polls the user source for changes in group membership every 1800 seconds (30 minutes).

1. In the Mobility Admin console, click **Config** > **User Source**.

2. Adjust the poll rate as needed to synchronize the group membership in the Mobility Admin console with current group membership in the GroupWise system.

3. Click **Save** to save the new setting(s).

4. Restart the Mobility Service:

   `gms restart`

Using the Mobility Admin Console with a Single Sign-On Solution

If you are using a single sign-on solution such as NetIQ Access Manager or KeySheild SSO, the Mobility Admin console does not require authentication when you are already logged in to the single sign-on solution.

 ◆ For Access Manager, no extra configuration is required.
 ◆ For KeyShield SSO, you must provide Keyshield SSO settings on the Single Sign-On page in the Mobility Admin console. For more information, see KeyShieldSSO (http://www.keyshieldsso.com).

Adding GroupWise Users as Mobility Administrators

By default, when you use GroupWise as your Mobility system's user source, you must log in to the Mobility Admin console using the `root` user name and password.

You can configure the Mobility Service to allow specific users to log in using their GroupWise username and password. Then the `root` user name and password can continue to be used as well.

1 In a terminal window on the Mobility server, become `root` by entering `su –` and the root password.

2 Change to the following directory:

   `/etc/datasync/configengine`

3 Open the `configengine.xml` file in a text editor.

4 Add the following section:

```
<gw>
    <admins>
        <username>GroupWise_Username</username>
        <username>GroupWise_Username</username>
    </admins>
    <enabled>true</enabled>
</gw>
```

   Replace *GroupWise_Username* with the appropriate GroupWise user name. You can add as many GroupWise users as needed.

5 Save the `configengine.xml` file, then exit the text editor.

6 Restart the Mobility Service to put the new settings into effect:

   `gms restart`

Unlocking the Mobility Admin Console

As a security precaution, the Mobility Admin console locks you out if you give the wrong user name or password more than three times. Use the following command on the command line of the Mobility server to restart the Mobility Admin Service and release the lock on the console:

`systemctl restart datasync-webadmin.service`

2 GroupWise Mobility System Management

When you install the GroupWise Mobility Service, your initial Mobility system is configured with default settings that are generally appropriate. After installation, you can customize your Mobility system configuration.

Starting, Stopping, and Checking GroupWise Mobility

1 In a terminal window on the Mobility server, become `root` by entering `su –` and the root password.

2 Use the commands indicated to perform the tasks listed:

Task	Command
Restore automatic starting of Mobility if it has been disabled through the `gms disable` command.	`gms enable`
Prevent Mobility from starting automatically when the system starts up.	`gms disable`
Display Status	`gms status`
Manually Start the service	`gms start`
Manually Stop the service	`gms stop`
Manually Restart the service	`gms restart`

Using MCheck to Simplify User, Certificate, and Database Management

NOTE: Beginning with GMS 18.4, MCheck is expanded and enhanced to include functionality previously available only in a support tool named **dsapp**.

The **dsapp** tool let Micro Focus Support personnel manage multiple users and groups, perform certificate-management tasks without requiring terminal prompt commands, and directly affect the health and content of the GMS databases.

MCheck now makes those popular features available to GW Mobility Service Administrators.

To run MCheck:

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/tools/mcheck`

3 Run the following command:

`python3 mcheck.pyc`

The top-level MCheck menu displays:

```
1 System
2 Users
3 Database
4 Checks & Queries
0 Exit

Select Option:
```

4 Access the various MCheck tasks by typing numbers to navigate the menu structure shown in the left column of Table 2-1 below.

The right column outlines what MCheck does when the task number from one of the options below is entered:

1. System

2. Users

3. Database

4. Checks & Queries

Table 2-1 *Navigating and Using the MCheck utility*

Task Navigation Path	Steps and/or Results - log file path is `/opt/novell/datasync/tools/mcheck/logs`
1. System	Typing 1 exposes the system integrity checks and SSL/TLS certificate-related maintenance tasks explained below.
1. Get Mobility Configuration	This option 1. Retrieves and checks GMS Configuration settings. 2. Records the settings in the following log file: **Log file name:** `mobConfiguration_yyyy-mm-ddThh:mm:ss.log`

Task Navigation Path	Steps and/or Results - log file path is `/opt/novell/datasync/tools/mcheck/logs`
2. GroupWise System Address Book Check	This option 1. Analyzes the accuracy and integrity of the GroupWise System Address book. 2. Reports any problems found in the following log file:. **Log file name:** `sab_`*`yyyy-mm-dd`*`T`*`hh`*`:`*`mm`*`:`*`ss`*`.log` 3. Recommends corrective action if needed.

3. SSL Check	This option
	
	1. Assesses whether the GMS server and its associated POAs are ready for SSL/TLS certificate verification, by checking the following
	
	    ◆ The Mobility Default POA is a host name.
	
	    ◆ The associated Mobility POAs are host names.
	
	    ◆ The Mobility default POA uses SSL.
	
	    ◆ The GMS server has a valid Mobility Certificate Store (`/var/lib/datasync/mobility/mob_ca.pem`.
	
	    ◆ The Mobility Default POA certificate can be verified.
	
	    ◆ The associated Mobility POAs' certificates can be verified.
	
	2. Logs the results and recommends corrective action if needed:
	
	Log file name: `sslCheck_`*`yyyy-mm-dd`*`T`*`hh`*`:`*`mm`*`:`*`ss`*`.log`

Task Navigation Path	Steps and/or Results - log file path is `/opt/novell/datasync/tools/mcheck/logs`

3. Fix Mobility Encryption (Conditional - appears only when the hostname changed and GMS requires fixing)	**IMPORTANT:** If you change the GMS server's host name after installing and configuring GMS, for example as part of an upgrade process, encryption breaks and GMS stops working.
	
	When that happens, only a restricted **System** is available with two options:
	
	◆ **1. Certificates**
	◆ **2. Fix Mobility Encryption**.
	
	To repair GMS, do the following:
	
	1. Type `2`.
	2. Enter the old host name or the server.
	   a. MCheck stops GMS and Mobility.
	   b. Then it updates and fixes various configuration files.
	   c. And finally it prompts whether you want to start Mobility services.
	3. Enter `y`, the service restarts, and you are prompted to press Enter again.
	
	   Mobility encryption is now fixed, and the next time you start MCheck, the standard options appear.
	4. Type 0 twice to exit MCheck.
	
	Log file name: `fixHostname_yyyy-mm-ddThh:mm:ss.log`

4. GroupWise Maintenance Verification	This option 1. Verifies that the GroupWise license is current and other associated data is correct. 2. Logs the results and recommends corrective action if needed. **Log file name:** `GWLicenseCheck_yyyy-mm-ddThh:mm:ss.log`
5. Certificates **1. Certificates** (This becomes the first option if Mobility Encryption requires fixing.)	Provides guided certificate generation and maintenance tasks as documented below.

Task Navigation Path	Steps and/or Results - log file path is `/opt/novell/ datasync/tools/mcheck/logs`
1. Generate CSR & Private Key	Guides you through the process of generating a private key and creating a Certificate Signing Request (CSR) to submit to a trusted third-party Certificate Authority.

This option

1. Lets you generate a private key as follows:

   a. Asks that you specify where to store the key. If the path doesn't exist, you can have MCheck create it.

   b. Prompts you to enter and confirm a password for the key file.

   c. When the password is confirmed, generates an RSA private key.

2. Prompts you for the information needed to generate a Certificate Signing Request (CSR):

   a. MCheck prompts for all the fields in a standard request, but only the following four are mandatory:

      ◆ **Country:** This is your country's two-digit country code. For example. `US` for the United States, `IN` for India, `JP` for Japan.

      ◆ **State or Locality:** This is the full name of the state or locality. For example, `California` or `Barcelona`.

      ◆ **Organization Name:** This is the full legal company or personal name as registered in your locality.

      ◆ **Common Name:** This must be the fully qualified domain name (FQDN) of the system this certificate will secure. For example `gms_01.servers.example.com`.

3. When you have entered the information, MCheck displays the paths and file names of the Private Key just generated and the CSR file.

4. Then it prompts whether you want to generate a self-signed-certificate from the CSR just created.

   We strongly recommend that you

   a. Answer `n` to all of the prompts that follow.

   b. Obtain a third-party-certified public certificate by submitting the CSR just created to one of the reliable Certificate Authorities on the web.

   c. When you receive the third-party certificate, continue with 3. Apply certificates (Generate PEM).

   WARNING: If you answer `y` to the prompt, MCheck generates and installs a self-signed certificate. This poses a security risk and is not recommended.

   If you must use a self-signed certificate temporarily, replace it as soon as possible.

Task Navigation Path	Steps and/or Results - log file path is `/opt/novell/` `datasync/tools/mcheck/logs`
2. Generate self-signed certificate	Although not recommended as a best practice, this option lets you generate a self-signed certificate from a previously created CSR. For example, the CSR that you created in 1. Generate CSR & Private Key.

1. You must specify

    ◆ The path to where the CSR and private key are located and what they are named. (You can list the files in the specified directory if needed.)

    ◆ How many days you want the self-signed certificate to be valid for.

    ◆ A passphrase for the key.

    MCheck signs the certificate and then prompts whether you want to apply the certificates (generate a PEM file).

2. If you type `y`, MCheck prompts for the key's passphrase (just entered above).

3. MCheck verifies the passphrase and then asks whether to apply the self-signed certificates (generate a PEM file).

4. If you type `y`, MCheck again prompts for the key's passphrase.

5. MCheck verifies that the certificate and key pair match and asks whether there are previously generated intermediate certificate files or bundles.

6. After following the prompts, the self-signed certificate is applied.

Task Navigation Path	Steps and/or Results - log file path is `/opt/novell/datasync/tools/mcheck/logs`
3. Apply certificates (Generate PEM)	After you receive the signed public certificate from a certified CA, use this option to apply the certificates by following the prompts as briefly explained below. 1. Specify the location of the working directory where you have copied your Private key file, the Public certificate that you received from the CA, and any intermediate certificate files or bundles that you want to include in the certificate store. For example, /root/Downloads/pub. 2. List the files in your working directory so you have their exact names. 3. Specify the name of the Private key that you created in Generate CSR & Private key. (page 17). 4. Specify the name of the Public certificate that you received from the third-pary CA. 5. Enter the pass phrase for your Private key, two times, as prompted. MCheck verifies that the Public certificate and Private key match. 6. If you need to include any intermediate certificate files or bundles in the certificate store, answer `y` to the prompt and enter the name of an intermediate certificate (`.crt` file) or bundle (`.pem` file). 7. Repeat the previous step until all of your intermediate files and bundles are entered. Then answer `n` to the prompt. 8. Enter the pass phrase for the Private key file for the third time. MCheck then creates the `gms_mobility.pem` file in your working directory and displays its location. **IMPORTANT:** When MCheck Generates the PEM, it removes the key passphrase as required for seamless access by mobile devices. 9. Enter `y` to install the PEM certificate store.
4. Verify certificate / key pair	Use this option if you simply need to verify that a certificate and key pair match.
5. Update GMS Services certificates	GMS services rely on an internal certificate store named `gms_server.pem`. You must never manually change or modify this certificate store. On the other hand, the certificates eventually expire. When that happens, use this option to update the certificates and renew the gms_server.pem certificate store.
0. Back to System Menu	

Task Navigation Path	Steps and/or Results - log file path is `/opt/novell/datasync/tools/mcheck/logs`
0. Main Menu	
2. Users	Typing 2 in the main menu, exposes the user and group tasks explained below.
1. Check User	Use this option to view the GMS statistics for a given user, discover any problems with the account, and see what actions will correct the problems.
	1. MCheck prompts you to enter the GroupWise User ID:
	It then displays the user that you specifed and reports statistics, problems found, and any actions required
	2. Press Enter to continue.
	Log file name: *GWuser_id_yyyy-mm-dd*T*hh*:*mm*:*ss*.log
	NOTE: You can also run Check User directly from the command line without accessing the menu by running the command:
	`python3 mcheck.pyc --user` *userID*
2. Remove Old Event Configurations	Use this option to remove all event configurations that contain the MAC address that you enter.
	1. MCheck displays a brief summary of the action to be taken, followed by the Mobility server's MAC address as a Hexidecimal number.
	Type the server's displayed MAC address and press Enter.
	2. MCheck then
	Checks each user.
	Removes event configurations that contain the Mobility server MAC address and logs the actions taken in
	Log file name:
	`removeEventConfigurations_`*yyyy-mm-dd*T*hh*:*mm*:*ss*`.log`
	3. Press Enter to return to the Users menu.
3. Remove and reinitialize users options	

Task Navigation Path	Steps and/or Results - log file path is `/opt/novell/datasync/tools/mcheck/logs`
1. Force remove user(s)/ group(s) db references	GMS uses databases to track which GroupWise users are registered for Mobility services and the data and messages, etc. that are associated with them. If you are unable to remove users or groups using the Web Console, you can use this option to force the removal of users and/or groups from the databases. Users, groups, and data on the GroupWise system are not affected. 1. MCheck prompts for a comma-delimited list of user and/ or group IDs. **NOTE:** The process doesn't provide lists to pick from; you must manually enter each ID. 2. MCheck displays the issues discovered on the screen along with the action recommended to resolve the issue. For example, you might need to restart GMS to complete user and group removal. **Log file name:** `userActions_yyyy-mm-ddThh:mm:ss.log`
2. Reinitialize user(s)/ group(s)	If one or more of you Mobility user accounts has problems, for example they are missing calendar or other data, MCheck can clear their data and messages and then restore everything from the backend GroupWise system. 1. MCheck prompts for a comma-delimited list of user and/ or group IDs. **NOTE:** The process doesn't provide lists to pick from; you must manually enter each ID. 2. MCheck clears all data associated with the IDs you have entered and then reinitializes the accounts. **Log file name:** `userActions_yyyy-mm-ddThh:mm:ss.log`
3. Reinitialize all failed users	If multiple Mobility users show a Failed state in the admin console, you can use this option to reinitialize all of them rather than using the admin console to reinitialize one of them at a time. This removes associated data from the database and synchronizes with GW again. **Log file name:** `userActions_yyyy-mm-ddThh:mm:ss.log`

Task Navigation Path	Steps and/or Results - log file path is `/opt/novell/datasync/tools/mcheck/logs`
4. Reinitialize all users	**IMPORTANT:** If you choose to continue after the initial prompt, this will take some time to complete.
	Also, a device configured with a user being reinitialized will be unable to connect to the server until that user is reinitialized.
	1. MCheck prompts whether you want to continue.
	2. Enter `y` to continue or `n` to return to the **Remove and Reinitialize Users Options** menu.
	Log file name: `userActions_yyyy-mm-ddThh:mm:ss.log`
0. Back to System Menu	
0. Main Menu	
3. Database	To enter the Database sub-menus, you must stop Mobility.
	MCheck prompts you as follows:
	1. Stop Mobility Now [y/n]
	If you type `n`, MCheck returns to Main Menu.
1. Vacuum Database	Consider using this option when your mobility databases seem larger than expected.
	Vacuuming a database tightens up data records, making previously used space fragments once again available for database use.
	Although PostgreSQL includes a process that performs incremental vacuum operations, these are not as thorough as a full vacuum.
	This option performs a full vacuum of the mobility databases. You should follow this up with next Database option to re-index the database.
	Log file name: `dbActions_yyyy-mm-ddThh:mm:ss.log`
2. Re-index Database	If users are experiencing performance delays, reindexing the database might help.
	This options rebuilds all of the indexes.
	Keep in mind that reindexing can take a while if the Mobility databases are large.
	Log file name: `dbActions_yyyy-mm-ddThh:mm:ss.log`
3. CUSO (Clean-up Start Over	

Task Navigation Path	Steps and/or Results - log file path is `/opt/novell/datasync/tools/mcheck/logs`
1. Cleanup and Start Over (Except Users)	This removes everything from the mobility databases except the User and Group records, which are reinitialized when the cleanup process concludes. **Log file name:** `dbActions_yyyy-mm-ddThh:mm:ss.log`
2. Cleanup and Start Over (Everything)	This removes everything from the mobility databases, essentially restoring the mobility server to where it was when the initial install completed. **Log file name:** `dbActions_yyyy-mm-ddThh:mm:ss.log`
4. Change PostgreSQL datasync_user password	This option enables you to change the password for the *datasync_user* account in the event of a lost password. The *datasync_user* account is used to access the PostgreSQL databases for the GroupWise Mobility Service.

0. Back	Because MCheck's database operations required stopping the service, you are prompted as follows:
	
	1. Do you want to restart Mobility now? [y/n]
	
	   If you type y, Mobility restarts and MCheck returns you to the Main Menu.
	
	   If you type n, MCheck returns to Main Menu without restarting Mobility. As a result, Mobility services are not available to users and some MCheck operations fail until Mobility is restarted.

4. Checks & Queries	Typing 4 in the main menu, exposes the checks and queries explained below. If you detect any unresolvable issues from running any of these checks, contact Customer Support.

1. General Health Check	The General Health Check runs and displays a series of tests that populate a status in the terminal. After all the checks are run, you can view more detailed information about each check in the mcheck logs at:
	
	`/opt/novell/datasync/tools/mcheck/logs`
	
	To find issues in an open log, search for `/Failed`.
	
	NOTE: You can also run the General Health Check directly from the command line without accessing the menu by running the command:
	
	`python3 mcheck.pyc --healthCheck`
	
	TIP: The first time this option is run, the `gh.conf` file is created in the `/opt/novell/datasync/tools/mcheck/conf` directory. This file is used for the NTP server time check. If you are getting an NTP failure when running the General Health Check, you can modify the file to point to a different NTP server.

Task Navigation Path	Steps and/or Results - log file path is `/opt/novell/datasync/tools/mcheck/logs`
2. GW Pending Events by User (consumerevents)	This option displays data about events that users execute on their devices that are pending processing in the mobility service.
3. Mobility Pending events by User (syncevents)	This option displays data about user events driven by the mobility service that have not yet synced with user devices.
0. Back	
0. Exit	Return to the terminal prompt.

Using Autodiscovery to Simplify Mobile Device Setup

By default, mobile users must know the IP address or DNS host name of their GMS server to add their email account in their device's email app.

GMS supports ActiveSync's Autodiscovery service. This lets you configure DNS so that users only need to enter their email address and password to add their account.

Use the information in the following sections to understand Autodiscovery for GMS and how to implement it on your network.

How Autodiscovery Works with GMS

When mobile users add their GroupWise email accounts in a device's mail application, the application tries to configure the accounts automatically by default.

Figure 2-1 illustrates the process, which is further explained in Table 2-2 on page 25.

Figure 2-1 *GMS Autodiscovery Visual Overview*
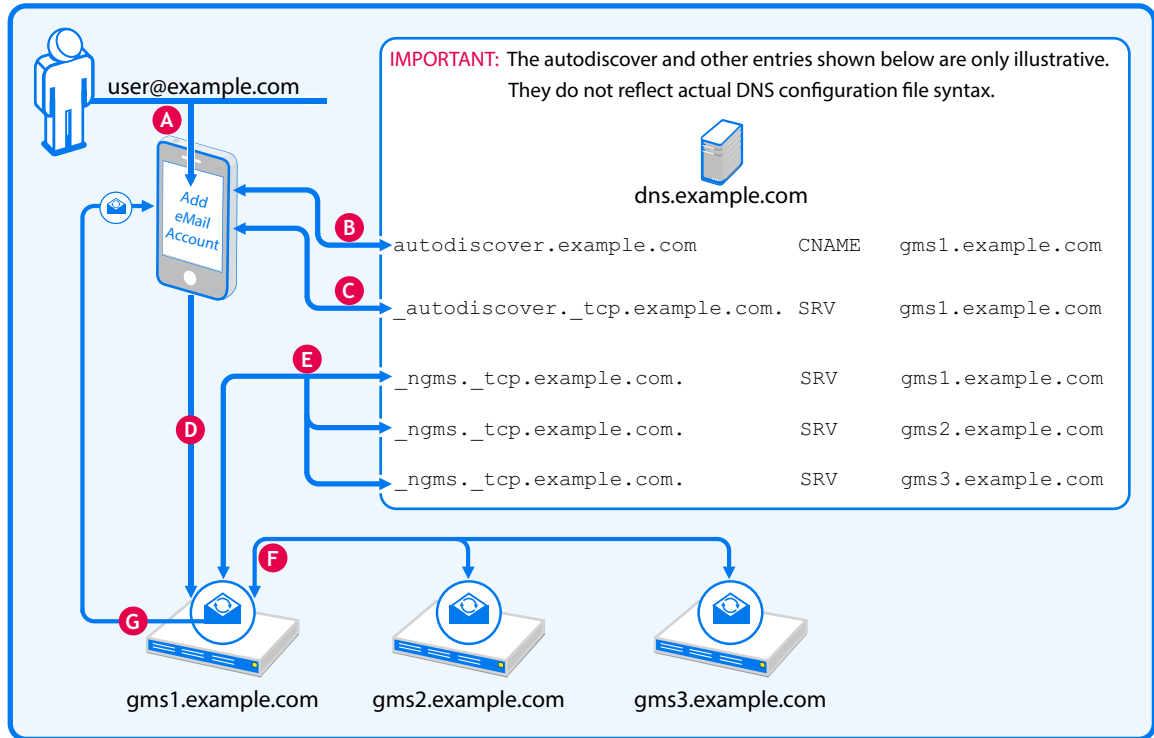
Table 2-2 *Connecting to GMS Through Autodiscovery*

Letter	Description
A	A user in the example.com organization begins adding their GroupWise account to their mail app on their mobile device. iPhone example, 1. The user taps **Settings > Mail > Accounts > Add Account > Microsoft Exchange**. 2. After entering their Email address, they tap **Next**. 3. The device prompts for the Email Password.
B	The device checks DNS for a canonical name (`CNAME`) associated with the alias, `autodiscover`. In this case, the `CNAME` is `gms1.example.com`.
C	The device then checks DNS for an _autodiscover service (SRV) entry that specifies an associated email service. The associated service is running on gms1.example.com.
D	The device then contacts the specified email service on gms1.example.com for the user-specified email account (user@example.com). If the account is located, GMS skips to letter G, below. If not the process continues with letter E

Letter	Description
E	If the user account is not found on gms1.example.com, the GMS service queries DNS for entries that specify where additional _ngms (GMS) services (SRV) are located.
	In this case, gms1.example.com, gms2.example.com, and gms3.example.com are each specified as potential candidates where the user account might be located.
	IMPORTANT: If additional GMS services are not configured in DNS, the attempt at autodiscovery and configuration fails, and the user is prompted to configure the account manually.
F	The first GMS server then queries each specified server in turn until the user account is located.
	IMPORTANT: If the user account is not located, the attempt at autodiscovery and configuration fails, and the user is prompted to configure the account manually.
G	When the user account is located, GMS sends the required configuration settings back to the device, which then adds the account and signs in to the GMS service that has the user account.

Setting Up SSL for the Autodiscover Service

IMPORTANT: Autodiscovery requires SSL.

Your GMS deployment must meet each of the conditions below.

- **SSL Certificate:** Each GMS server must have a current, valid, and trusted SSL certificate installed.
- **Accessible Certificate Chain:** Mobile devices must be able to follow the certificate chain from the certificate on the GMS server to the root CA certificate.
- **One Wildcard Cert That Covers All GMS Servers:** This must be an SSL certificate with Subject Alternative Names (SANs) so that you can specify a list of host names that are protected by it.

  For information about configuring GMS with a certificate, see Securing Communication between the Device Sync Agent and Mobile Devices.

When these conditions are met, continue with Setting Up the Autodiscover Service.

Setting Up the Autodiscover Service

To set up the Autodiscover Service, you must configure DNS as follows:

IMPORTANT: We recommend that you use the DNS configuration tools provided with your DNS service to complete the following steps.

Only required fields are included in the instructions. Of course, you can adjust additional parameters to meet your network's DNS requirements. Additional information about DNS CNAME and SRV records is available on the Web.

1 As illustrated and described in "How Autodiscovery Works with GMS" above, ActiveSync's Autodiscover mechanism begins by finding the GMS server (the CNAME) associated with the alias name `autodiscover`.

   Using your DNS management interface, create an Alias (CNAME) Resource Record in your DNS service by using the information in the following table.

Variable	Value	Example	Description
alias	`autodiscover.`*your.domain*	autodiscover.example.com	Set the alias to `autodiscover.`
canonical name	*your_gms_server.your.email. domain* Or alternatively *your_external_nat/ port_forward.your.email.do main*	gms.example.com Or alternatively nat.example.com	One of your GMS server's host name. Alternatively, if your GMS servers are fronted by a NAT or port forward, specify the host name of the NAT or port forward.

2 At a terminal prompt, check that the autodiscover alias is configured correctly by entering the following command:

`dig autodiscover.`*your.email.domain* `CNAME +short`

Your GMS server canonical name is returned:

your_gms_server.your.email.domain

Continue with

3 Next, you must create an _autodiscover service (SRV) record for the email domain.

Using your DNS management interface, create an SRV Resource Record by using the information in the following table.

Variable	Value	Example	Description
service	`_autodiscover`	n/a	Set the service to `_autodiscover`.
protocol	`_tcp`	n/a	Set the protocol to `_tcp`.
port	443	n/a	Set the port to `443`.
target	*your_gms_server.your.e mail.domain* Or alternatively *your_external_nat/ port_forward.your.email .domain*	gms.example.com Or alternatively nat.example.com	The GMS server that you specified as the CNAME for autodiscover in . Alternatively, if your GMS servers are fronted by a NAT or port forward, specify the host name of the NAT or port forward.

4 At a terminal prompt, check that the _autodiscover service is configured correctly by entering the following command:

`dig _autodiscover._tcp.`*your.email.domain* `SRV +short`

A string similar to the following is returned that includes the port number you specified and your GMS server's DNS name:

10 0 443 *your_gms_server.your.email.domain*

NOTE: If you have only one GMS server, you have successfully configured DNS for Autodiscovery. GroupWise users can now automatically configure mail accounts on their mobile devices.

5 (Conditional) If you have more than one GMS server, you must create an _ngms service (SRV) record for each GMS server.

As illustrated and described in "How Autodiscovery Works with GMS" above, when the first attempt to find a user account fails, the first GMS server then queries other GMS servers in turn, utilizing the _ngms SRV records in DNS, until the user account is found.

Using your DNS management interface, create an SRV Resource Record for each GMS server (including the server you specified in previous steps), by using the information in the following table.

Variable	Value	Example	Description
service	_ngms	n/a	Set the service to _ngms.
protocol	_tcp	n/a	Set the protocol to _tcp.
port	443	n/a	Set the port to 443.
target	*your_gms_server.your.e mail.domain*	gms.example.com	Set the target to your GMS server.

IMPORTANT: Make sure to create an SRV record for each one of your GMS servers. Only then can Autodiscover find them.

6 At a terminal prompt, check that every _ngms service (SRV) is configured correctly by entering the following command:

```
dig _ngms._tcp.your.email.domain SRV +short
```

Strings similar to the following are returned, one for each GMS server, and each including the port number you specified and a GMS server's DNS name ending with a period.

```
0 0 443 first_gms_server.your.email.domain.
```

```
0 0 443 second_gms_server.your.email.domain.
```

```
0 0 443 third_gms_server.your.email.domain.
```

```
etc.
```

NOTE: If the test succeeds, you have successfully configured DNS for Autodiscovery on multiple GMS servers.

GroupWise users can now automatically configure mail accounts on their mobile devices.

Controlling Synchronization Size Limits

Synchronizing large quantities of data between GroupWise and mobile devices can put a substantial load on the sync agents. The GroupWise Sync Agent controls the maximum size of the individual attachments that can synchronize with an item to mobile devices. The Device Sync Agent controls the maximum size of an item (along with all attachments) that can synchronize to GroupWise.

- ◆ "Controlling Maximum Attachment Size from GroupWise to Mobile Devices" on page 29
- ◆ "Controlling Maximum Send Mail Size from Mobile Devices to GroupWise" on page 29

Controlling Maximum Attachment Size from GroupWise to Mobile Devices

By default, attachments are synchronized from GroupWise to the mobile devices if they are smaller than 500 KB. Attachments larger than 500 KB are dropped by the GroupWise Sync Agent and do not synchronize to mobile devices.

When a user receives an item on the mobile device for which attachments have not been synchronized from GroupWise, the item includes a list of the attachments that are on the original item but not on the synchronized item. This lets the user know that attachments are available in the GroupWise mailbox.

1 In the Mobility Admin console, click **Config**.

2 In the **Maximum Attachment Size** field, adjust the maximum attachment size as needed.

   This setting causes large attachments that exceed the size limit to be stripped from a message as it synchronizes from GroupWise to mobile devices. Small attachments that are within the size limit are still synchronized.

3 Click **Save** to save the new setting(s).

4 Restart the Mobility Service:

   ```
   gms restart
   ```

Controlling Maximum Send Mail Size from Mobile Devices to GroupWise

By default, if an item is larger than 500 KB when it is sent from a device, all attachments are stripped from the item before it is sent to GroupWise. In place of each stripped attachment, the user receives a text attachment indicating that the original attachment was stripped because of the size limit and what the size limit is.

1 In the Mobility Admin console, click **Config**.

2 In the **Maximum Send Mail Size** field, adjust the maximum message size as needed.

   This setting causes all attachments to be stripped from an item as it synchronizes from a mobile device to GroupWise if the size of the item plus all attachments exceeds the size limit.

3 Click **Save** to save the new setting(s).

4 Restart the Mobility Service:

   ```
   gms restart
   ```

Maintaining the Mobility Database

The Mobility Service database is a PostgreSQL database. As with any database, the Mobility Service database requires regular maintenance in order to perform reliably. If you are new to managing a PostgreSQL database, see "Routine Database Maintenance Tasks" (http://www.postgresql.org/docs/8.3/interactive/maintenance.html) on the PostgreSQL Documentation website for assistance.

Backing Up Your Mobility System

All of the user data that exists at any time in your Mobility system also exists in GroupWise. Therefore, if there is a problem with your Mobility system, you can always resynchronize in order to restore your user data to a current working state.

However, you can back up your entire Mobility system in order to preserve the Mobility Service software, configuration files, certificate files, and database.

- "Understanding What to Back Up" on page 30
- "Backing Up a Mobility System after Stopping It" on page 31
- "Backing Up a Mobility System While It Is Running" on page 31
- "Restoring Your Mobility System" on page 32

Understanding What to Back Up

- Use your backup software of choice to back up the following directories on your Mobility server:

Directory	Description
/opt/novell/datasync	Mobility Service software
/etc/datasync	Configuration files
/var/lib/datasync	Certificate files

- Use a PostgreSQL-supported backup solution to back up the Mobility Service database in the following directory:

  /var/lib/pgsql

- Decide how you want to back up the data:
  - Backing Up a Mobility System after Stopping It
  - Backing Up a Mobility System While It Is Running

Backing Up a Mobility System after Stopping It

Stopping your Mobility system before backing it up is the safest way to ensure a completely consistent backup.

1 In a terminal window on the Mobility server, become `root` by entering `su -` and the root password.

2 Create a directory for storing your backup files, for example:

   `mkdir /var/gmsbackup`

3 Create a script similar to the following:

```
#!/bin/bash
# back up stopped Mobility system
gms stop
systemctl stop postgresql.service
#
tar -czvpf /var/gmsbackup/pgsql.tgz /var/lib/pgsql
tar -czvpf /var/gmsbackup/vardatasync.tgz /var/lib/datasync
tar -czvpf /var/gmsbackup/optdatasync.tgz /opt/novell/datasync
tar -czvpf /var/gmsbackup/etcdatasync.tgz /etc/datasync
#
systemctl start postgresql.service
gms start
```

   For example, you could create a script named `gmsbackup.sh` in the `/opt/novell/datasync` directory.

4 Add execute permissions to the backup script:

   `chmod +x script_name.sh`

5 Execute the backup script.

6 Change to the directory where you backed up the Mobility files to verify that the `.tgz` files were successfully created.

Backing Up a Mobility System While It Is Running

For convenience, you might want to back up your Mobility system while it is still running.

1 In a terminal window on the Mobility server, become `root` by entering `su -` and the root password.

2 Create a script to back up the Mobility Service database:

   2a Create a file named `.pgpass` in the `root` user's home directory (`/root`).

   2b Put the following contents in the `.pgpass` file.

   `*:*:*:datasync_user:database_password`

   The Mobility Service database user is `datasync_user`. The Mobility Service database password was established during installation.

2c Create a database backup script similar to the following, using the pg_dump (http://www.postgresql.org/docs/8.4/static/app-pgdump.html) command to back up just the Mobility Service databases:

```
#!/bin/bash
# back up Mobility Service database
pg_dump -U datasync_user mobility > /tmp/mobility.out
pg_dump -U datasync_user datasync > /tmp/datasync.out
/usr/bin/bzip2 /tmp/mobility.out
/usr/bin/bzip2 /tmp/datasync.out
```

For example, you could create a database backup script named gmsdbbackup.sh in the /opt/novell/datasync directory.

2d Add execute permissions to the backup script:

```
chmod +x script_name.sh
```

2e Execute the backup script.

3 Create a script to back up the Mobility Service directories:

3a Create a directory for storing your backup files, for example:

```
mkdir /var/gmsbackup
```

3b Use the following script to back up the rest of your Mobility system while it is sill running:

```
#!/bin/bash
# back up running Mobility system
tar -czvpf /var/gmsbackup/vardatasync.tgz /var/lib/datasync
tar -czvpf /var/gmsbackup/optdatasync.tgz /opt/novell/datasync
tar -czvpf /var/gmsbackup/etcdatasync.tgz /etc/datasync
```

For example, you could create a script named gmsdirbackup.sh in the /opt/novell/datasync directory.

3c Add execute permissions to the backup script:

```
chmod +x script_name.sh
```

3d Execute the backup script.

3e Change to the directory where you backed up the Mobility files to verify that the .tgz files were successfully created.

Restoring Your Mobility System

1 Change to the directory where you backed up the Mobility files.

2 Use the following tar command to restore the backed-up Mobility directories:

```
tar -xzvf file_name.tgz
```

3 (Conditional) If you used the pg_dump (http://www.postgresql.org/docs/8.3/static/app-pgdump.html) command to back up the Mobility Service databases separately, use the psql (http://www.postgresql.org/docs/8.3/static/app-psql.html) command to restore it.

Changing the IP Address or Host Name of the Mobility Server

For a Mobility system with just a small number of users on a single server, the simplest approach is to reinstall the Mobility Service software, and then have users reinitialize their mobile devices.

For a Mobility system with a large number of users, where having users reinitialize their mobile devices after reinstalling the Mobility Service software could be problematic, you can reconfigure your Mobility system with a new IP address, and then have users change the IP address that their mobile devices use to access the Mobility system.

- "Changing the IP Address for a Small Mobility System" on page 33
- "Changing the IP Address for a Large Mobility System" on page 33
- "Changing the Host Name of a Mobility Server" on page 34

Changing the IP Address for a Small Mobility System

1 Uninstall the Mobility Service software.

  For instructions, see "Uninstalling the Mobility Service" in the *GroupWise Mobility Service 18 Installation Guide*.

2 Change the IP address of the server.

3 Reinstall the Mobility Service software.

  For instructions, see "Running the Mobility Service Installation Program" in the *GroupWise Mobility Service 18 Installation Guide*.

4 Instruct your mobile device users to delete their accounts from their mobile devices, set them up using the new IP address, then reinitialize their mobile devices.

Changing the IP Address for a Large Mobility System

1 Stop the Mobility Service:

  ```
  gms stop
  ```

2 Change the IP address of the server.

3 Use MCheck to clear event configurations:

  3a In a terminal window on the Mobility server, become `root` by entering `su -` and the root password.

  3b Change to the following directory:

  ```
  /opt/novell/datasync/tools/mcheck
  ```

  3c Run the following command:

  ```
  python3 mcheck.pyc
  ```

The main MCheck menu displays.

```
1 System
2 Users
3 Database
0 Exit

Select Option:
```

     3d Select **2 Users**.

     3e Select **2 Remove Old Event Configuration**.

     3f Enter the MAC address for the Mobility server whose IP address you changed.

        MCheck reads all users on the Mobility server and retrieves their event configurations. If the MAC address you entered matches the MAC address in an event configuration, it removes the event configuration.

        When MCheck is finished, the console displays 1) a list of all event configurations that were removed and 2) a total of all event configurations that were removed.

  4 Start the Mobility Service:

```
gms start
```

  5 Instruct your mobile device users to reconfigure their accounts with the new IP address.

Changing the Host Name of a Mobility Server

If you need to change the host name of your mobility server, use the administrative tools and methods associated with your OS platform. Here are a few GMS-specific general guidelines to follow:

1. Stop GMS.
2. Change the host name using your platform's tools.
3. Adjust the network DNS entries, etc. associated with GMS.
4. Install new certificates, and so on as needed. See MCheck > Certificates.
5. Using MCheck, Fix your Mobility Encryption.
6. Restart GMS.
7. Instruct your mobile device users to reinitialize their accounts.

Providing Anonymous Feedback about Your Mobility System

Micro Focus is striving to focus engineering efforts on the real-world needs of our GroupWise Mobility Service users. When you are willing to submit anonymous feedback from your Mobility system to Micro Focus, you assist in these efforts to improve Mobility Service performance.

When you enable anonymous feedback, a script runs daily to gather statistics about the usage of your Mobility system. The statistics are sent daily to Micro Focus.

You can enable and disable the sending of feedback at any time. You can review the usage data that has been collected before it is sent to Micro Focus.

- ◆ "Enabling/Disabling Anonymous Feedback" on page 35
- ◆ "Viewing the Collected Feedback" on page 35

Enabling/Disabling Anonymous Feedback

1 In the Mobility Admin console, click **Config**, then scroll down to the **Send Anonymous Feedback** field.

2 Select or deselect **Send Anonymous Feedback**.

3 Click **Save** to save the new setting(s).

4 Restart the Mobility Service:

```
gms restart
```

Viewing the Collected Feedback

You can feel comfortable about letting Micro Focus gather usage data from your Mobility system. The data is collected by the following script:

```
/opt/novell/datasync/tools/getstats.sh
```

The script is run by the following cron job:

```
/etc/cron.daily/gw-mobility-feedback
```

The cron job runs once a day at midnight. The results are stored in `*.gz` files in the following directory:

```
/var/log/datasync/configengine
```

The files are saved for 90 days and then deleted.

Use the following command to extract the data from a *.gz file:

```
tar xvfz gwmobility_stats_string_date_time.gz
```

By viewing the gathered usage data, you can assure yourself that no personal data of any kind is being collected by Micro Focus. The following is an example of the type of data that is collected:

```
GWMobilityVersion,SLESVersion,CPUCount,CPUType,SYSKBMemory,SYSType,
    GroupWiseEventUserCount,FolderItemAdd,ItemMarkRead,ItemMarkUnread,

GWCAttachmentSize,MCAttachmentSize,TotalAttachments,Attachment1MB,Attachme
nt2MB,

Attachment3MB,Attachment4MB,Attachment5MBPlus,BlockedAttachments,MailFromD
evice,

ReadFromFromDevice,DeleteFromFromDevice,MoveFromFromDevice,UserCount,DevCo
unt,
    DevPerUser2,DevPerUser3,DevPerUser0,DevPerUser1,DevPerUser4,DevPerUser5,

DevPerUser6Plus,iPad,AndroidTablet,OtherDevices,iPhone,WindowsPhone,iPod,
    AndroidPhone,WindowsTablet,BlackBerry,WindowsOther,iOSOther,Android2,
    BlackBerryOther,BlackBerry10,iOS5,Windows8,iOS7,iOS6,Android5,Android4,
    Android3,AndroidOther,OtherOS

2.0.0.349,SLES11SP3,1,Intel(R)Core(TM)i7-
2600CPU@3.40GHz,1017680,VMwareInc.,1,8,4,

1,500,500,1,1,0,0,0,0,0,0,0,0,0,3,0,0,0,3,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,
    0,0,0,0,0,0,0,0,0,0
```

Thank you in advance for enabling Anonymous Feedback and submitting your Mobility system usage data to help improve the GroupWise Mobility Service.

3 GroupWise Sync Agent Configuration

After you have installed the GroupWise Mobility Service, you can refine the configuration of the GroupWise Sync Agent to meet your Mobility system's needs.

Monitoring and Configuring the GroupWise Sync Agent

You use the Mobility Admin console to monitor and configure the GroupWise Sync Agent.

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 If the GroupWise Sync Agent is not running and does not start normally, refer to GroupWise Sync Agent Troubleshooting for assistance.

4 In the Mobility Admin console, click **Config**, then click **GroupWise** to display the GroupWise Sync Agent Configuration page.

For more information about the Mobility Admin console, see GroupWise Mobility Administration Console.

Selecting GroupWise Items to Synchronize

By default, all GroupWise items are synchronized to mobile devices.

1 In the Mobility Admin console, click **Config**, then click **GroupWise** to display the GroupWise Sync Agent Configuration page.

2 In the **GroupWise Items to Sync** section, select and deselect items as needed to configure the GroupWise Sync Agent to synchronize more items or fewer items.

3 Click **Save** to save the new setting(s).

4 Restart the Mobility Service:

```
gms restart
```

The following sections contain information about settings that can also affect item synchronization:

- Ignoring Old GroupWise Items
- Controlling Maximum Item Synchronization

Synchronizing Sticky Notes

The Sticky Notes option allows notes to be synchronized between mobile devices and GroupWise:

- *Mobile device*: Synchronizes notes created using the device's Notes app. The Notes app varies depending on the device operating system. On iOS devices, the native *Notes* app is supported. On Blackberry devices, the native *Remember* app is supported. On Android devices, the *Tasks and Notes for MS Exchange* app is supported.

- *GroupWise client*: Synchronizes Discussion Note and Personal Message items created in or moved to the *Mobile Notes* folder. GroupWise automatically creates the *Mobile Notes* folder when the Sticky Notes option is enabled. In some cases, the folder might be named *Notes* rather than *Mobile Notes*.

Sticky Notes synchronization is bidirectional. Notes that are created, modified, or deleted on the device are synchronized to the *Mobile Notes* folder. Discussion Note/Personal Message items that are created, modified, or deleted in the *Mobile Notes* folder are synchronized to the mobile device.

1 In the Mobility Admin console, click **Config**, then click **GroupWise** to display the GroupWise Sync Agent Configuration page.

2 In the **Sticky Notes** field, select **Enable** to synchronize Sticky Notes or deselect it to disable synchronization.

3 Click **Save** to save the new setting(s).

4 Restart the Mobility Service:

```
gms restart
```

The following sections contain information about settings that can also affect Sticky Note synchronization:

- Ignoring Old GroupWise Items
- Controlling Maximum Item Synchronization

Synchronizing Proxy Calendars

Added in 18.1. The Proxy option allows Proxy Calendars to be synchronized between mobile devices and GroupWise. This option is disabled by default. To enable Proxy Calendars:

1 In the Mobility Admin console, go to **Config** > **GroupWise**.

2 Select **Proxy Calendars** to enable synchronization.

3 Click **Save**.

4 Restart the Mobility Service:

```
gms restart
```

When enabling Proxy Calendars, be aware of the following:

Requirements

◆ GroupWise 18 or later POAs are required for Proxy Calendars for Proxy users.

General Information

◆ We recommend that you do not enable Proxy Calendars during the initial Mobility synchronization, but that you enable it during off peak hours as the data needs to be cached on the Mobility server and can increase the time to synchronize significantly.

◆ The Proxy Calendar(s) shows up on your mobile device as a separate, selectable calendar.

◆ GroupWise Proxy rights are enforced. Rights are enforced at the Mobility server and not on the device. For example, if a user doesn't have delete rights, a device delete appears to work. However, on the next device sync the deleted item is restored.

◆ Appointments, Reminder Notes, Alarms, and Private appointments sync to mobile devices depending on your proxy rights.

Known Limitations

◆ Some Android devices aggregate all calendars into one calendar and you cannot select the calendars that are displayed.

◆ Private appointments are synced to mobile devices even if you do not have proxy rights to private appointments. The private appointments do not show any information including subject, users, and body if you do not have proxy rights.

Synchronizing Shares

IMPORTANT: The Microsoft Outlook Client doesn't support all of the synchronization features described in this section. For example, the version of ActiveSync that the client uses does not support shared folders, calendars, or address books.

For more information, see Known Outlook Client Limitations.

The Shares option allows shared folders, calendars, and contacts to be synchronized between mobile devices and GroupWise. This option is disabled by default. To enable shares:

1 In the Mobility Admin console, go to **Config** > **GroupWise**.

2 Select **Shares** to enable synchronization.

3 Click **Save**.

4 Restart the Mobility Service:

```
gms restart
```

When enabling shares, be aware of the following:

Requirements

 ◆ GroupWise 2014 R2 SP1 or later POAs are required for share owners and recipients to enable shares for users.

General Information

 ◆ We recommend that you do not enable shares during the initial Mobility synchronization, but that you enable it during off peak hours as shared data needs to be cached on the Mobility server and can increase the time to synchronize significantly.

 ◆ The Mobility server startup time might be slower with shares enabled. The amount the startup is slowed depends on the number of shared folders in your system.

 ◆ Dashboard alerts let you know if there is a problem with individual shares. Check the log files for more information.

 ◆ GroupWise share rights are enforced. Rights are enforced at the Mobility server and not on the device. For example, if a user doesn't have delete rights, a device delete appears to work. However, on the next device sync the deleted item is restored.

 ◆ Share owners do not need to be Mobility users.

Known Limitations

 ◆ Share notifications can only be accepted in the GroupWise client.

Increasing GroupWise Sync Agent Reliability or Performance

If the GroupWise POA encounters an error and stops notifying the GroupWise Sync Agent about GroupWise events, GroupWise events stop synchronizing to mobile devices. By default, the GroupWise Sync Agent polls the POA for new events every 3600 seconds (1 hour).

You can configure how often the GroupWise Sync Agent polls the POA for events that have not yet been synchronized. Decreasing the poll cycle causes the GroupWise Sync Agent to poll more frequently, so that synchronization is more reliable. However, if you have a large number of users, you might want to increase the poll cycle in order to improve GroupWise Sync Agent performance.

1 In the Mobility Admin console, click **Config**, then click **GroupWise** to display the GroupWise Sync Agent Configuration page.

2 In the **Poll POA for Events** field, increase or decrease the poll cycle as needed.

Set the poll cycle to 0 (zero) to disable the sweep cycle.

3 Click **Save** to save the new setting(s).

4 Restart the Mobility Service:

```
gms restart
```

Ignoring Old GroupWise Items

Removed in 18.1. By default, the GroupWise POA does not transfer items to the GroupWise Sync Agent if they are older than 30 days. Typically, mobile device users have an even shorter time window during which they want items retained on their mobile devices. Allowing the GroupWise Sync Agent to accept items into your Mobility system that will ultimately be discarded by the Device Sync Agent is not an efficient use of system resources.

You can decrease this setting in order to decrease sync agent traffic for old items and to align more closely with the needs of mobile device users. If necessary, you can increase this setting to a maximum of 60 days.

1 In the Mobility Admin console, click **Config**, then click **GroupWise** to display the GroupWise Sync Agent Configuration page.

2 In the **Ignore Events After** field, increase or decrease the item age as needed.

3 Click **Save** to save the new setting(s).

4 Restart the Mobility Service:

```
gms restart
```

Clearing Accumulated GroupWise Events

When the GroupWise Sync Agent stops synchronizing for some reason, GroupWise events accumulate in users' GroupWise mailbox databases until the GroupWise Sync Agent resumes synchronization.

By default, when the GroupWise Sync Agent restarts, it processes all accumulated events. This default behavior prevents the loss of events and is the desired behavior for normal GroupWise Sync Agent functioning. However, when you are troubleshooting a problem with the GroupWise Sync Agent, you might find it helpful to skip processing accumulated events so that the GroupWise Sync Agent starts processing current events more quickly.

To clear old events (not recommended unless you are troubleshooting):

1 In the Mobility Admin console, click **Config**, then click **GroupWise** to display the GroupWise Sync Agent Configuration page.

2 In the **Clear Old Events** field, select **Enable**.

This causes the GroupWise Sync Agent to discard accumulated events and start processing new events immediately. The discarded events are never processed.

3 Click **Save** to save the new setting(s).

4 Restart the Mobility Service:

```
gms restart
```

IMPORTANT: As soon as you are finished troubleshooting, return to the GroupWise Sync Agent Configuration page and deselect **Clear Old Events**, so that GroupWise events are not accidentally lost during normal GroupWise Sync Agent functioning.

Changing the GroupWise Sync Agent Listening Port

By default, the GroupWise Sync Agent communicates with the GroupWise POA using port 4500. If necessary, you can configure the GroupWise Sync Agent to use a different port.

1 In the Mobility Admin console, click **Config**, then click **GroupWise** to display the GroupWise Sync Agent Configuration page.

2 In the **Port** field, change the port number as needed.

3 (Conditional) If there is a firewall between the Mobility server and the POA server, make sure that the specified port is open.

4 Click **Save** to save the new setting(s).

5 Restart the Mobility Service:

```
gms restart
```

Enabling and Disabling SSL for POA SOAP Connections

During installation, you chose whether to use SSL for connections between the GroupWise Sync Agent and the GroupWise POA. The default is to use SSL. You can change the setting after installation as needed. All of your POAs need to have SSL enabled or disabled

1 On the POA, enable or disable SSL as needed for the SOAP connection.

2 In the Mobility Admin console, click **Config**, then click **GroupWise** to display the GroupWise Sync Agent Configuration page.

3 In the **Secure** field, select **Enabled** to enable SSL.

4 Click **Save** to save the new setting(s).

5 Restart the Mobility Service:

```
gms restart
```

Matching GroupWise Configuration Changes

Changes in your GroupWise system can require changes to the configuration of the GroupWise Sync Agent.

1 In the Mobility Admin console, click **Config**, then click **GroupWise** to display the GroupWise Sync Agent Configuration page.

2 Change GroupWise Sync Agent settings to match changes in your GroupWise system configuration as needed.

If the POA is reconfigured to change whether it uses SSL, the **Enabled** must be changed in the **Secure** field.

If you create a new trusted application, you must update both the trusted application name and key at the same time. When you copy in a new trusted application key, the new key is obfuscated when it is saved.

3 Click **Save** to save the new setting(s).

4 Restart the Mobility Service:

```
gms restart
```

Configuring the GroupWise Sync Agent with an External IP Address and Port

On the GroupWise Sync Agent Configuration page in the Mobility Admin console, you specify the GroupWise Sync Agent server IP address and port for internal communication within your local network. However, you need to configure the GroupWise Sync Agent to use an external IP address and port for the following configurations:

- ◆ There is a firewall between the GroupWise Sync Agent and the POA that it communicates with.
- ◆ The GroupWise Sync Agent and the POA are located on two different logical networks with NAT (network address translation) between them.
- ◆ The GroupWise Sync Agent is running in a virtual machine.

To configure the GroupWise Sync Agent to use an external IP address and port:

1 In a terminal window on the Mobility server, become `root` by entering `su -` and the root password.

2 Change to the following directory:

```
/etc/datasync/configengine/engines/default/pipelines
                                        /pipeline1/connectors/
groupwise
```

3 Open the `connector.xml` file in a text editor.

4 Add the following lines between the <custom> and </custom> tags:

```
<externalAddress>external_ip_address</externalAddress>
<externalPort>external_port_number</externalPort>
```

5 Replace *external_ip_address* and *external_port_number* with the IP address and port number for the GroupWise Sync Agent to communicate with the POA across whatever network configuration lies between them.

6 Save the `connector.xml` file, then exit the text editor.

7 Restart the Mobility Service:

```
gms restart
```

Modifying or Preventing Synchronization of Specified Items by Using an XSLT Filter

If you are familiar with XSLT, you can configure the GroupWise Sync Agent to modify or drop specified items. The sample filter below drops items that contain a specified subtype or that have a subject equal to a specified string. With a little XSLT knowledge, you can modify this sample filter to meet your needs.

1 Create the following directory:

```
/var/lib/datasync/groupwise/filter
```

2 Copy the following sample filter into a text editor:

```
<?xml version='1.0' encoding='utf-8'?>

<xsl:stylesheet version='1.0' xmlns:xsl='http://www.w3.org/1999/XSL/
                                                    Transfor
m'>

<xsl:variable name="subtype" select="//*[local-name()='subType']"/>
<xsl:variable name="subject" select="//*[local-name()='subject']"/>
<xsl:template match="node()|@*">
  <xsl:if test="not(contains($subtype, 'SearchText') or
                contains($subtype, 'SearchText') or
                ($subject = 'put_the_subject_here'))">
    <xsl:copy>
      <xsl:apply-templates select="node()|@*"/>
    </xsl:copy>
  </xsl:if>
</xsl:template>

</xsl:stylesheet>
```

This sample file is available in the following location:

```
/opt/novell/datasync/syncengine/connectors/groupwise/filter/
                                                    sourceCustomExamp
le.xslt
```

3 Save the text file as `sourceCustomSample.xslt` in the new `groupwise/filter` directory that you created in Step 1.

4 Modify the file to identify the items that you want the GroupWise Sync Agent to drop.

5 Save the `sourceCustomSample.xslt` file, then exit the text editor.

6 When you are ready to put the new filter into effect, rename `sourceCustomSample.xslt` to `sourceCustom.xslt`, then restart the GroupWise Sync Agent.

7 (Conditional) If you need to remove the new filter, rename the `sourceCustom.xslt` file to a different name, then restart the GroupWise Sync Agent.

4 Device Sync Agent Configuration

After you have installed the GroupWise Mobility Service, you are ready to refine the configuration of the Device Sync Agent to meet your Mobility system's needs.

- "Monitoring and Configuring the Device Sync Agent" on page 45
- "Blocking/Unblocking All Incoming Devices" on page 46
- "Enabling a Device Password Security Policy" on page 46
- "Quarantining New Devices to Prevent Immediate Connection" on page 47
- "Controlling the Maximum Number of Devices per User" on page 48
- "Removing Unused Devices Automatically" on page 48
- "Controlling Maximum Item Synchronization" on page 49
- "Binding to a Specific IP Address" on page 49
- "Enabling and Disabling SSL for Device Connections" on page 50
- "Changing the Address Book User" on page 50

Monitoring and Configuring the Device Sync Agent

You use the Mobility Admin console to monitor and configure the Device Sync Agent.

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. If the Device Sync Agent is not running and does not start normally, refer to Device Sync Agent Troubleshooting for assistance.

4. In the Mobility Admin console, click **Config**, then click **Device Sync Agent** to display the Device Sync Agent Configuration page.

For more information about the Mobility Admin console, see GroupWise Mobility Administration Console.

Blocking/Unblocking All Incoming Devices

You can prevent all users from connecting their devices to the Mobility system, and then allow access when you are ready. This is helpful when you are installing an update to the Mobility Service software.

1 In the Mobility Admin console, click **Config**, then click **Device** to display the Device Sync Agent Configuration page.

2 Deselect **Enable** in the **Allow Connections** field.

3 Click **Save** to save the new setting(s).

4 Restart the Mobility Service:

   ```
   gms restart
   ```

5 When you are ready to allow access again, select **Enable** in the **Allow Connections** field, then restart the Mobility Service.

NOTE: Whenever you block or unblock a device, notify the device owner of the change in device status.

Occasionally, you might encounter synchronization problems with specific users or devices. For example, a problem with a specific user or device might start to consume an inappropriately large amount of system resources on your Mobility server. If this occurs, see Blocking/Unblocking Specific Devices for assistance with resolving the problem.

Enabling a Device Password Security Policy

As an administrator, you can control several aspects of the behavior of mobile devices that connect to your Mobility system. By establishing a security policy for the passwords that users set on their mobile devices, you help prevent unauthorized access to your Mobility system from lost or misplaced devices.

1 In the Mobility Admin console, click **Config**, then click **Device** to display the Device Sync Agent Configuration page.

2 Select **Enable** in the **Device Security Policy** field.

   When you enable the security policy, users are informed of the specific security settings that are in effect when they create their mobile device accounts and set their device passwords. Users are prevented from configuring their mobile devices to connect to the Mobility system without following the security policy you establish.

   If a user's device uses another locking method, like a lock pattern, that method is overridden by the Mobility system's device password security policy when they attempt to connect for the first time.

NOTE: When mobile devices connect for the first time to a system that has been updated from the Data Synchronizer Mobility Pack to GroupWise Mobility Service 18, some devices automatically switch from ActiveSync 2.5 to 16. When this occurs, some devices prompt users to accept a new "security policy," which can sound like a substantial change. In reality, no substantial change is being made, and users should simply accept the "policy" when prompted.

---

3 Set the security policy options as needed for the level of device password security that you want for your Mobility system:

Both Letters and Numbers: By default, any combination of characters is permitted in device passwords. Enable this option to require complex device passwords. Valid options for his settings are 1 (lowest complexity) - 4 (highest complexity). Devices behave differently to this setting depending on the type of OS.

Minimum Password Length: By default, the user can set a device password of any length. Enable this option to specify the minimum number of characters required in device passwords. The minimum value is 0; the maximum value is 18. If you specify 0, the security policy does not require the user to set a password on the device.

Inactivity Time: By default, the mobile device does not lock itself in the absence of user activity. Enable this option to specify the number of minutes after which a mobile device locks itself when no user activity occurs.

Reset Device after Failures: By default, an external Reset command must be sent to the mobile device in order to wipe personal data from it. Enable this option to specify the number of failed password attempts after which the mobile device automatically resets itself to factory default settings.

4 Click **Save** to save the new setting(s).

5 Restart the Mobility Service:

```
gms restart
```

Quarantining New Devices to Prevent Immediate Connection

By default, when a user configures a new mobile device to synchronize GroupWise data, the device can immediately connect to your Mobility system and start synchronizing data. If you prefer, you can configure your Mobility system to prevent new devices from connecting until you allow access.

1 In the Mobility Admin console, click **Config**, then click **Device** to display the Device Sync Agent Configuration page.

2 Select **Enable** in the **Quarantine New Devices** field so that new devices cannot connect to your Mobility system until you allow them to.

3 Click **Save** to save the new setting(s).

4 Restart the Mobility Service:

```
gms restart
```

5 Configure the Mobility Service to notify you when users connect new devices.

For instructions, see Enabling System and Service Notifications.

6 Skip to Releasing a New Device from the Quarantine.

Controlling the Maximum Number of Devices per User

When a single user has multiple devices, the user's data is duplicated in your Mobility system. To control data duplication and improve performance, you can control the number of devices that each user is allowed to connect to your Mobility system.

By default, each user can connect to your Mobility system with as many devices as he or she wants. When you set the maximum limit, a user who is above the limit is not prevented from connecting with existing devices. However, the user cannot connect with any additional devices until the number of devices is within the limit that you have set.

1   In the Mobility Admin console, click **Config**, then click **Device** to display the Device Sync Agent Configuration page.

2   In the **Maximum Devices per User** field, set the maximum number of devices that each user can connect with.

    To remove an existing limit, delete the number for an unlimited number of devices.

3   Click **Save** to save the new setting(s).

4   Restart the Mobility Service:

    ```
    gms restart
    ```

Removing Unused Devices Automatically

By default, mobile devices that have not connected to your Mobility system for 30 days are automatically removed from your Mobility system. You can change the time interval after which unused devices are automatically removed.

NOTE: To remove a device immediately, see Deleting a Device.

---

1   In the Mobility Admin console, click **Config**, then click **Device** to display the Device Sync Agent Configuration page.

2   In the **Remove Unused Devices** field, adjust the number of days as needed to control the proliferation of unused devices.

3   Click **Save** to save the new setting(s).

4   Restart the Mobility Service:

    ```
    gms restart
    ```

Controlling Maximum Item Synchronization

Users can configure their mobile devices to request synchronization for all email and calendar items. However, you might not want to allow users to synchronize that much data.

By default, users are allowed to synchronize a maximum of 30 days of email and 180 days of calendar items. You can set the allowed maximums higher or lower as needed.

1 In the Mobility Admin console, click **Config**, then click **Device** to display the Device Sync Agent Configuration page.

2 In the **Maximum Email Sync Limit** field, adjust the maximum number of days for email.

   The maximum setting is 730 days (2 years).

   NOTE: This setting also applies to Sticky Notes.
   ---

3 In the **Maximum Calendar Sync Limit** field, adjust the maximum number of days for calendar items.

   The maximum settings for these fields is 730 days (2 years).

   If users try to configure their mobile devices to synchronize more days of data than you have allowed, they receive a warning message.

4 Click **Save** to save the new setting(s).

5 Restart the Mobility Service:

   ```
   gms restart
   ```

Binding to a Specific IP Address

By default, the Device Sync Agent uses all available IP addresses on the Mobility server. You can reconfigure the Device Sync Agent to use only one specific address.

1 In the Mobility Admin console, click **Config**, then click **Device** to display the Device Sync Agent Configuration page.

2 In the **IP Address** field, specify the IP address that you want to bind the Device Sync Agent to.

   The default of `0.0.0.0` indicates that the Device Sync Agent is not bound to a specific IP address.

3 Click **Save** to save the new setting(s).

4 Restart the Mobility Service:

   ```
   gms restart
   ```

Enabling and Disabling SSL for Device Connections

During Mobility Service installation, you chose whether to use SSL for connections between the Device Sync Agent and mobile devices. By default, the Device Sync Agent uses a secure SSL connection on port 443. You can change the setting after installation as needed.

1 In the Mobility Admin console, click **Config**, then click **Device** to display the Device Sync Agent Configuration page.

2 Select or deselect **Enable** in the **Secure** field to change whether SSL is in use.

3 Click **Save** to save the new setting(s).

4 Restart the Mobility Service:

```
gms restart
```

Changing the Address Book User

The Device Sync Agent accesses the GroupWise Address Book to obtain contact information for synchronization to mobile devices. The Device Sync Agent can obtain the information it needs by logging in as any valid GroupWise user. An initial Address Book user was specified during installation. You might want to change to a different user for whom either more or fewer contacts are visible in the GroupWise Address Book.

NOTE: The Device Sync Agent uses this user name only to access and search the GroupWise Address Book. It does not use this user name to access any personal aspects of the specified user's mailbox.

1 In the Mobility Admin console, click **Config**, then click **Device** to display the Device Sync Agent Configuration page.

2 In the **Address Book User** field, specify the GroupWise user name of the user whose view of the GroupWise Address Book best meets the needs of your mobile device users.

3 Click **Save** to save the new setting(s).

4 Restart the Mobility Service:

```
gms restart
```

5 GroupWise Mobility System Monitoring

GroupWise mobile device users rely on their devices for many aspects of their professional and personal lives. By carefully monitoring your Mobility system, you can keep device synchronization functioning quickly and reliably.

- "Using the Mobility Dashboard" on page 51
- "Enabling System and Service Notifications" on page 53
- "Monitoring User Status" on page 53
- "Monitoring Device Status" on page 55
- "Monitoring Disk Space Usage" on page 57
- "Working with Log Files" on page 57
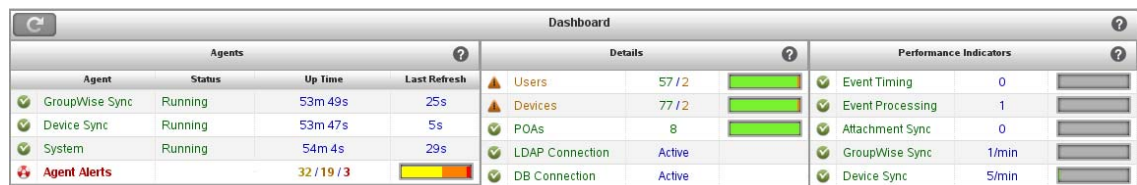- "Monitoring GroupWise SOAP Processing" on page 59

Using the Mobility Dashboard

The Mobility Dashboard provides statistics about the functioning of your Mobility system. At the same time, colorful indicators draw your attention to those details that matter most.

- "Exploring the Dashboard" on page 51
- "Configuring Dashboard Data Retention" on page 52

Exploring the Dashboard

1 In the Mobility Admin console, click **Dashboard**.

The initial three panels provide high-level information about your Mobility system.

2 Click **Users**, then click a specific user to open three additional panels with user-specific information.

3 Click a specific type of information in any panel to open the **Listing** panel to display detailed statistics.

4 Click the **Listing** drop-down menu on the left side of the **Listing** panel header to select a specific listing or to create a customized listing view.

When you customize a listing in any way, the customization remains until you log out of the Admin console.

5 Click a graph in a listing to display a large, detailed version of the graph.

6 Click **Help** ❓ in any panel for explanations of all the statistics and graphs.

7 Click **Search Filter** 🔍 on the right side of the **Listing** panel header, type a search string, then press Enter to restrict the content of the listing.

8 Click **Export Table** 📇 to export the listing to a CSV file for use in a spreadsheet program.

9 Click Configure Columns ⚙ to select the columns to display in the listing.

In addition to the Dashboard, the Mobility Admin console provides the User page for monitoring synchronization of users and devices. For usage instructions, see:

- Monitoring User Status
- Monitoring Device Status

Configuring Dashboard Data Retention

The Dashboard continuously collects data about your Mobility system to produce the indicators and statistics listings that it displays. You can configure how long alerts remain active and how long historical data for graphs is stored.

1 In the Mobility Admin console, click **Config**.

2 In the **Alert Retention** field, adjust how long you want alerts to display.

By default, alerts are retained for 14 days or until you manually delete them.

3 In the **Statistic History Retention** field, adjust how long you want the data used to generate graphs to be stored.

By default, the historical data used to generate the graphs is retained for 30 days.

4 Click **Save** to save the new setting(s).

5 Restart the Mobility Service:

```
gms restart
```

Enabling System and Service Notifications

You can configure the Mobility system to notify specified users when critical situations arise that require administrator attention.

1 In the Mobility Admin console, click **Config**.

2 In the **Notification Enabled** field, select **Enabled**.

3 Fill in the following fields:

SMTP IP Address: Specify the IP address of an SMTP host for sending email. This could be a GroupWise GWIA server, but you can also use another email system such as sendmail on a Linux server or a personal email account.

SMTP Port: The port number on which the Mobility Service can communicate with the SMTP host.

Authentication User Name: The email user name to send the notification messages from.

Authentication User Password: (Conditional) The email password if one is required on the email account.

System Notifications: A comma-delimited list of email addresses to send a notification to when the Mobility server encounters a critical (red) alert or condition.

Service Notifications: A comma-delimited list of email addresses to send a notification to when a new device needs to be released from the quarantine.

For more information about the quarantine, see Quarantining New Devices to Prevent Immediate Connection and Releasing a New Device from the Quarantine.

4 Click **Save** to save the new setting(s).

5 Restart the Mobility Service:

```
gms restart
```

Monitoring User Status

The Users page helps you monitor synchronization progress as data transfers from GroupWise through the GroupWise Sync Agent to the Device Sync Agent in preparation for transfer to mobile devices.

1 In the Mobility Admin console, click **Users**.

A **Group** icon 👥 to the left of a **User** icon 👤 shows that the user was added to your Mobility system as a member of a group. If you mouse over the Group icon, the name and context of the group displays.

A synchronized resource is identified with the **Resource** icon 🟧.

2 Check the **User State** column for each user.

The **User State** column displays the following states that indicate the progress of initial synchronization from GroupWise into the Mobility system:

User State	Explanation
Queued	The initial synchronization process from GroupWise to the Mobility system has not yet started for this user.
Configuring	The initial user configuration is in progress.
Configured	The initial user configuration is completed.
Syncing-Init	The initial synchronization process is in progress. As many as four users can be synchronizing at once. As one user is finished, initial synchronization for the next user starts.
Sync-Validate	The Mobility system has received all of the user's GroupWise data, and is in the process of comparing the data in the Mobility system with the data in GroupWise to verify the completeness of the data transfer.
Synced	The initial synchronization process is complete.
Syncing-Days+	After initial synchronization, users can request more email in addition to the default of the email in the Mailbox folder for the last three days.
Syncing-PAB	The Mobility system is synchronizing the user's Personal Address Book.
Blocked	The specific user is currently blocked from connecting any devices.
Failed	The initial synchronization process has failed. For failed users, the GroupWise Sync Agent automatically retries as many as four times after all other users have been synchronized.
Delete	The user is in the process of being deleted from your Mobility system. If the user has a large amount of data and attachments in the system, the deletion process can take some time.
Re-Init	The user is in the process of being reinitialized. During reinitialization, the user's GroupWise data is deleted from the Mobility system and is requested again from the GroupWise system. If the user has a large amount of GroupWise data and attachments, the reinitialization process might take a long time.

See also Monitoring Device Status.

3 (Condition) For users in the **Queued** state, be patient until the state progresses from **Queued** to **Syncing** to **Synced**.

4 (Conditional) For users in the **Syncing** state, refresh the Users page until the status changes to **Synced**.

5 (Conditional) For users in the **Synced** state, notify the users to configure their mobile devices to connect to the Mobility system.

After users have configured their mobile devices to connect to the Mobility system, they can configure their devices to synchronize additional items beyond the defaults. For more information about initial synchronization, see "Managing Initial Synchronization of Users" in the

GroupWise Mobility Service 18 Installation Guide. For such users, their **Synced** state can change to **Syncing** again as additional items are retrieved, and then return to **Synced** when the additional synchronization is finished.

6 (Conditional) If a user is in the **Blocked** state because all of his or her devices are blocked, click **Unblock Device** ▶ in the **User Actions** column to unblock the user and all devices.

For more information, see Blocking/Unblocking All Incoming Devices and Blocking/Unblocking Specific Devices.

7 (Conditional) If a user is in the **Failed** state:

7a Click the user name to display the User/Device Actions page.

7b In the **Actions** column, click ↻.

Reinitialization deletes the user from the Device Sync Agent, adds the user again, then starts the synchronization process over from the beginning.

7c (Conditional) If reinitializing the user still does not allow the user to connect, delete the user from the Mobility system, then re-add the user.

For instructions, see Managing Mobile Device Users.

7d Click **Users** 🌐 to return to the Users page.

8 To display more detailed user status, click **Dashboard**, then click **Users**.

For more information about the Dashboard, see Using the Mobility Dashboard.

Monitoring Device Status

After GroupWise data has successfully transferred from GroupWise into the Mobility system, the Device Sync Agent is then responsible for transferring the data to and from mobile devices.

1 In the Mobility Admin console, click **Users**.

2 Check the **Device State** column for each user.

If there are multiple lines in the **Device State** column. the user has multiple devices. Hover over the device state icon to display the device ID.

The **Device State** column displays the following states that indicate the status of each device's connection to the Mobility system:

Device State	Explanation
❓ Never Connected	The user has not yet configured the device to connect to the Mobility system. Device synchronization has not yet begun.

Device State	Explanation
✔ Normal	The device has successfully connected to the Mobility system and synchronization to the device is complete.
🚫 Blocked	The device is being prevented from connecting to the Mobility system for either of these conditions: ◆ All devices have been prevented from connecting by using the Block All Devices setting on the Device Sync Agent Configuration page. ◆ An individual device has been manually blocked on the User/Device Actions page because it was having a problem that was adversely affecting the Mobility system.
⚠ Quarantined	A new device is being prevented from connecting until you release it from the device quarantine.
⏻ Removing	A command has been sent to the device to remove the user's GroupWise account and all associated data from the device.
⏻ Removed	The device has acknowledged the Remove command and all GroupWise data is removed from the device.
⏻ Resetting	A command has been sent to the device to wipe all data and return to its factory default settings.
⏻ Reset	The device has acknowledged the Reset command, has been successfully wiped and is returning or has returned to its factory default settings.

See also Monitoring User Status.

3 (Optional) In the **Search** field, type all or part of a user's first name, last name, or GroupWise user name to filter the list.

4 (Optional) Use the drop-down menu to the right of the **Search** field to filter the list by device state.

5 Click the user name of the device owner to display the User/Device Actions page.

For each device, the device type, device operating system, ActiveSync version, and time of last synchronization are listed. The **Device State** column displays the same states that are displayed on the User page.

6 (Conditional) If a device is in the **Blocked** state, click **Unblock Device** ▶ in the **Device Actions** column to unblock the device.

For more information, see Blocking/Unblocking All Incoming Devices and Blocking/Unblocking Specific Devices.

7 (Conditional) If a device is in the **Quarantined** state, click **Allow Device** ✔ to release the device from the quarantine.

For more information about the quarantine, see Quarantining New Devices to Prevent Immediate Connection and Releasing a New Device from the Quarantine.

8 To display more detailed device information, such as the last time each device connected to your Mobility system, click **Dashboard**, then click **Devices**.

If a device has not connected to the Mobility system for 30 days, the nightly maintenance process automatically removes the inactive device from the Mobility system.

For more information about the Dashboard, see Using the Mobility Dashboard.

9 (Optional) Click **Folder List** to display the totals of pending and synchronized items in each folder in the user's GroupWise mailbox.

This information is helpful when troubleshooting a synchronization problem for the user.

Monitoring Disk Space Usage

Every effort should be made to provide adequate disk space on the Mobility server. An abnormal shutdown because of insufficient disk space can result in data loss in your Mobility system.

The `datasync-diskcheck.sh` script runs automatically along with the Mobility Service and monitors disk space usage in the `/var` partition where log files are stored.

IMPORTANT: If disk space usage exceeds 90%, the script shuts down the Mobility Service normally, to prevent the potential data loss associated with an abnormal shutdown.

The `datasync-diskcheck.sh` script runs every hour. When it detects a low disk space condition, it writes an entry to the `/var/log/datasync/datasync_status` log file. No other notification of the condition is provided before the script shuts down the Mobility Service.

After a low disk space condition occurs, you can do one or more of the following things to prevent future problems:

- Improve your database maintenance practices. See Maintaining the Mobility Database.
- Remove old log files. For the location of log files, see Working with Log Files.
- Add more disk space to the Mobility server.

Working with Log Files

Log files provide useful information about the functioning of the various Mobility system components.

- "Understanding Log Files" on page 57
- "Setting the Log Level" on page 58
- "Configuring Log File Rotation" on page 59

Understanding Log Files

The Mobility Service components generate a set of log files that are created in subdirectories under the following directory:

`/var/log/datasync`

The log file subdirectories under `/var/log/datasync` and the log file names are as follows:

Internal Mobility Service Component	Log File Subdirectory under /var/log/datasync	Log File Name
Sync Engine	syncengine	engine.log

Internal Mobility Service Component	Log File Subdirectory under /var/log/datasync	Log File Name
Config Engine	`configengine`	`configengine.log`
Web Admin	`webadmin`	`server.log`
Connector Manager	`syncengine`	`connectorManager.log`

Sync Agents	`connectors`	`groupwise-agent.log`
		`groupwise.log`
		`mobility-agent.log`
		`mobility.log`

Use the following command to check the most recent additions to a log file:

```
tail -f log_file_name.log
```

Setting the Log Level

All Mobility log files use the same log level, which you set on the General page in the Mobility Admin console.

1 In the Mobility Admin console, click **Config**.

2 In the **Log Level** field, select from the following log levels:

- **Info:** Logs informational messages about normal synchronization processing. This log level is suitable for a Mobility administrator who wants to observe the functioning of the Mobility system.

   Info is the default log level and is strongly recommended because it balances the amount of data logged, the amount of disk space required for log files, and the load on the Mobility system.

- **Debug:** Logs large quantities of developer-level data. This log level is appropriate for troubleshooting purposes. It puts a heavy load on the Mobility system and should be used only until the troubleshooting activities are completed.

- **Warning:** Logs problems that should not adversely affect synchronization processing but should be investigated and resolved for optimum performance. This log level can be appropriate for a smoothly running Mobility system where you only want to be notified of warnings and errors.

- **Error:** Logs error messages that indicate critical problems in synchronization processing. This log level puts the least load on the Mobility system because it logs only critical errors, but it does not log sufficient data to help resolve any errors that occur.

3 Click **Save** to save the new setting(s).

4 Restart the Mobility Service:

```
gms restart
```

NOTE: The user interface instructs you to restart the Mobility Service, because this is required for all other settings on this page.

Configuring Log File Rotation

The Mobility log files are automatically compressed and rotated by a `logrotate cron` job. The schedule is set by the `DAILY_TIME="00:30"` line in the `/etc/sysconfig/cron` file, which means that the log files are checked at 12:30 a.m. each night. Any Mobility log files that have exceeded 4 MB in size are compressed and rotated at that time. After 30 days or 99 instances of each log file have accumulated, the oldest log file is deleted when a new log file is created.

Log rotation is controlled by the following files:

```
/etc/logrotate.d/datasync-syncengine
/etc/logrotate.d/datasync-configengine
/etc/logrotate.d/datasync-webadmin
/etc/logrotate.d/datasync-monitorengine
```

By default, `gzip` is used to compress old log files. You can change the compression method by changing the following line in the files listed above:

```
compresscmd /usr/bin/gzip
```

For example, to change from `gzip` (http://en.wikipedia.org/wiki/Gzip) compression to `bz2` (http://en.wikipedia.org/wiki/Bzip2) compression, use the following line:

```
compresscmd /usr/bin/bzip2
```

Using `bz2` compression produces smaller log files but uses more system resources during compression.

For more information, see the Linux `logrotate` (http://linux.about.com/od/commands/l/blcmdl8_logrota.htm) command.

Monitoring GroupWise SOAP Processing

The GroupWise Sync Agent uses the SOAP protocol to communicate with the GroupWise POA. GroupWise includes tools for monitoring those SOAP connections.

- "Using the GroupWise POA Web Console" on page 59
- "Using GroupWise Monitor" on page 59

Using the GroupWise POA Web Console

The POA web console provides information about SOAP events that are passing between the GroupWise Sync Agent and the POA. For more information, see "Monitoring SOAP Events" in the *GroupWise 18 Administration Guide*.

Using GroupWise Monitor

GroupWise Monitor can be configured to notify you when a POA is running out of SOAP threads. When you receive the notification, you can restart the POA. Configure GroupWise Monitor to notify you when the `poaSOAPThreadBusy` variable exceeds a threshold of 20. For more information, see "Configuring Email Notification for Agent Problems" in the *GroupWise 18 Administration Guide*.

6 GroupWise Mobility User Management

You can add GroupWise users, groups of users, and GroupWise resources to your GroupWise Mobility system. Some aspects of GroupWise system management affect management of mobile device users.

- ◆ "Managing Mobile Device Users" on page 61
- ◆ "Managing Groups of Users" on page 63
- ◆ "Managing Synchronized Resources" on page 64
- ◆ "Managing Changes in the GroupWise System" on page 65

Managing Mobile Device Users

You should add GroupWise users to your Mobility system when they express the need to synchronize their GroupWise data to their mobile device.

IMPORTANT: Do not add GroupWise users to your Mobility system who do not have a current need for data synchronization. When you add a user to your Mobility system, GroupWise data continually synchronizes from GroupWise into your Mobility system. If that data is not being used on a mobile device, that synchronization produces unnecessary overhead in your Mobility system.

- ◆ "Adding Individual Users" on page 61
- ◆ "Adding Users through a GroupWise Group" on page 62
- ◆ "Customizing a User's Synchronization Settings" on page 62
- ◆ "Deleting a User" on page 62
- ◆ "Using Multi-Factor Authentication" on page 63

For information about new, moved, and deleted GroupWise users, see Managing Changes in the GroupWise System.

Adding Individual Users

All users in the GroupWise Address Book are available to add to your Mobility system.

Adding users individually is appropriate for a small number of users. Maintenance of large numbers of users is much easier if you add them as members of GroupWise groups.

To add a user to your Mobility system:

1 In the Mobility Admin console, click Users.

2 Click Add User.

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

   or

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

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

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

Adding Users through a GroupWise Group

As the preferred alternative to adding individual users in the Mobility Admin console, you can add users to any GroupWise group. You can use the GroupWise Admin console to manage GroupWise groups.

Users who are added to groups are added to the Mobility system based on the Group Membership Polling Rate setting. For setup instructions, see Adjusting the Mobility Admin Console Polling Rate for Groups of Users.

You can also poll groups immediately. For instructions, see Updating a Group of Users in Your Mobility System.

For more information, see Managing Groups of Users.

Customizing a User's Synchronization Settings

The GroupWise Mobility Quick Start for Mobile Device Users describes the synchronization settings that are available to users on the Mobility Settings page of the Mobility Admin console. You can also control users' synchronization settings as an administrator. The settings most recently saved by either you or the user become the user's current settings.

To change a user's synchronization settings:

1 In the Mobility Admin console, click **Users**.

2 Select a user.

3 (Conditional) To set GroupWise settings for users, click **Edit GroupWise Settings**.

4 (Conditional) To set device settings, click **Edit Device Settings**.

5 Select and deselect options as needed to customize the user's data synchronization.

6 Click **Save**, then click **Close Window**.

The user's synchronization settings are immediately changed.

Deleting a User

The method that you use to delete a user from your Mobility system depends on how you added the user:

- "Deleting a User Directly" on page 63
- "Deleting a User from a Group of Users" on page 63

Deleting a User Directly

If you added an individual user, you delete the user in the Mobility Admin console.

1 In the Mobility Admin console, click **Users**.

2 Click **Delete** to the right of the user, then click **Delete User** to confirm.

   The user's status changes briefly to **Deleting**, then the user disappears from the list.

Deleting a User from a Group of Users

If you added a user account to your Mobility system by adding it to a GroupWise group, you must delete the user account from the group in order to delete it from your Mobility system. You can use the GroupWise Admin console to manage GroupWise groups.

In your Mobility system, the user is removed from the group according to the group polling rate. For background information, see Adjusting the Mobility Admin Console Polling Rate for Groups of Users.

You can also poll immediately. For instructions, see Adding Users through a GroupWise Group.

Using Multi-Factor Authentication

Incorporating multi-factor authentication (MFA) for users to access GroupWise provides another layer of security that you can add to Mobility. GroupWise supports MFA through NetIQ Advanced Authentication, which enables you to protect your IT infrastructure and sensitive data more effectively and securely.

For information about configuring MFA, see Multi-Factor Authentication.

Managing Groups of Users

You can use the GroupWise Admin console to manage GroupWise groups.

All GroupWise groups in the GroupWise Address Book are available to add to your Mobility system.

- "Adding a Group of Users to Your Mobility System" on page 63
- "Updating a Group of Users in Your Mobility System" on page 64
- "Deleting a Group of Users from Your Mobility System" on page 64

Adding a Group of Users to Your Mobility System

1 In the Mobility Admin console, click **Users**, then click **Groups**.

2 Click **Add Groups**.

3 Click **Search** to list the groups of users that are available in the user source.

   or

   In the **Search** field, type part of the group name, then click **Search**.

4 Select the group of users to add to your Mobility system.

5 Click **Add** to add the group.

The group is immediately added to your Mobility system and Users are immediately listed on the Users page.

NOTE: Starting with GMS 18.4, initial account synchronization time has been significantly reduced by implementing the following ordered process.

1. Each user's initial **User State** is `Configuring`, meaning that they are being added to the Mobility database.

2. After all of the users are added to the database, their **User State** changes to `Configured`, meaning that they are confirmed ready for the initial synchronization of their data from GroupWise.

3. When all users are in a `Configured` state, then data synchronization begins.

    When a User State changes to `Synced`, the GroupWise data is in GMS and ready to be accessed.

Updating a Group of Users in Your Mobility System

GroupWise is the source from which users and groups of users can be added to your Mobility system. For background information, see "Preparing GroupWise as the User Source for Your Mobility System" in the *GroupWise Mobility Service 18 Installation Guide*.

By default, the Mobility Admin console polls the user source for group membership changes every 30 minutes. For background information, see Adjusting the Mobility Admin Console Polling Rate for Groups of Users. However, you can poll the user source immediately to get the latest updates.

1 In the Mobility Admin console, click **Config**> **User Source**.

2 In the **Group Membership** field, click **Poll Now**.

Deleting a Group of Users from Your Mobility System

Deleting a group of users deletes the users in that group from your Mobility system.

1 In the Mobility Admin console, click **Users**, then click **Groups**.

2 Click **Delete** for the group to delete, then click **Yes** to confirm the deletion.

Managing Synchronized Resources

You can add GroupWise resources to your Mobility system as if they are users.

Whenever you create a new resource that you want to synchronize to mobile devices, you must proxy in to the resource mailbox and set its mailbox password before it is available for synchronization. Accessing the mailbox creates the Frequent Contacts address book and establishes the default personal address book for the mailbox. These address books must exist in order for the GroupWise Sync Agent to successfully process address book information for the mailbox.

GroupWise users with rights to a synchronized resource mailbox can then configure their mobile devices with an account for the resource mailbox just as they create an account for their own mailbox. This enables GroupWise users who are resource owners to monitor the contents of resource mailboxes from their mobile devices.

To add and manage resources in your Mobility system, follow the instructions in Managing Mobile Device Users.

Managing Changes in the GroupWise System

The following changes in the GroupWise system affect the functionality of your Mobility system:

- "When New Users Are Added to the GroupWise System" on page 65
- "When a Mailbox Moves" on page 65
- "When a GroupWise Account Is No Longer Available" on page 65

When New Users Are Added to the GroupWise System

When you add new users to GroupWise, they are not immediately available in the Mobility Admin console for adding to your Mobility system. They automatically become available within 30 minutes of when the Mobility Global Address List (GAL) is updated from the GroupWise Address Book.

You can use the **Poll Now** option in the Mobility Admin console to update the Mobility GAL immediately. For instructions, see Updating a Group of Users in Your Mobility System.

Whenever you create a new GroupWise user, the user must log in to the GroupWise client or WebAccess to prepare the mailbox for synchronization. Accessing the mailbox creates the Frequent Contacts address book and establishes the default personal address book for the mailbox. These address books must exist in order for the GroupWise Sync Agent to successfully process address book information for the mailbox.

NOTE: If you are running GroupWise 8, you must manually reinitialize the user. For instructions, see Reinitializing a User.

When a Mailbox Moves

When the GroupWise administrator moves a mailbox from one post office to another, the following changes occur in your Mobility system:

- In the Mobility Admin console, the Dashboard displays the user as **Moved**.
- The moved user is automatically reinitialized to associate it with the new post office and POA.

  NOTE: If you are running GroupWise 8, you must manually reinitialize the user. For instructions, see Reinitializing a User.

When a GroupWise Account Is No Longer Available

When the GroupWise administrator disables, expires, or deletes a GroupWise account, the following changes occur in your Mobility system:

- In the Mobility Admin console, the Dashboard displays the user as **Disabled**, **Expired**, or **Deleted**.
- The GroupWise Sync Agent stops contacting the POA for items to synchronize to the user's mobile device.

- The Device Sync Agent drops any items from the user's mobile device that would otherwise synchronize to GroupWise.

- If the GroupWise administrator re-establishes the account, the user must re-add the account to the device.

7 GroupWise Mobility Device Management

When you install the GroupWise Mobility Service, the sync agents start automatically. You can monitor the synchronization of data to and from mobile devices in the Mobility Admin console.

Managing Mobile Devices

After users have configured their mobile devices and connected to the Mobility system, additional options are available on the User/Device Actions page in the Mobility Admin console.

1. In the Mobility Admin console, click **Users**.

2. Click the user name of the device owner to display the User/Device Actions page.

3. Use the options in the **Device Actions** column to manage devices where synchronization is active:

Device Action	Description
Resync Device	Resynchronizes the mobile device with the Mobility system. Use this option to resolve the following problems:
	• Synchronization from the Mobility system to a mobile device might occasionally stop, perhaps because abnormal cellular network conditions resulted in dropped synchronization data.
	• Data on a mobile device might not match data as displayed in the GroupWise mailbox.
	A user can accomplish the same thing by removing the account from the mobile device and re-adding it, so that the GroupWise data resynchronizes from the Mobility system to the mobile device.
	If resynchronizing the device does not resolve discrepancies between data on the device and data in GroupWise, you must reinitialize the user. During reinitialization, the user's GroupWise data is deleted from the Mobility system and requested again from the GroupWise system. If the user has a large amount of GroupWise data and attachments, the reinitialization process might take a long time.

Device Action	Description
Block Device	Prevents the mobile device from connecting to the Mobility system. Use this option when a mobile device is temporarily disrupting your Mobility system by using excessive system resources.
Unblock Device	Enables a blocked mobile device to connect again to your Mobility system.
Allow Device	Allows a quarantined device to connect for the first time to your Mobility system.
Reset Device Options	Depending on the version and vendor implementation of ActiveSync, clicking this exposes one or more of the following possible actions: ◆ **Remove Account:** Use this to remove the GroupWise account and its associated data from the device. No other functionality or data is affected. ◆ **Reset Device:** Use this when a device is clearly lost or stolen. The Device Sync Agent requests that all data be erased and the device be restored to its original settings. Some devices refer to this as a "remote wipe" or "kill pill." How the Reset command is executed varies by device type. For example, some devices require that a security policy is previously set on the device. ◆ **Cancel:** Use this to close the options pop-up. IMPORTANT: The options display only when a device supports them.
Re-allow Device	Allows GroupWise to be added after a device has executed the Remove Account or Reset Device action. When GMS removes a GroupWise account or resets a device to its factory default settings, it sets a system flag that doesn't allow the GroupWise account to be added again to the device, unless you do one of the following: ◆ Allow the device to add the GroupWise account again by clicking this option. Or ◆ Delete the device, which removes all data regarding the device from the user's Mobility settings.
Delete Device	Deletes the mobile device from your Mobility system. Use this option when a user is no longer using a particular mobile device. The device can be added again.

For more information about device states and actions, see:

- Resynchronizing a Device
- Blocking/Unblocking Specific Devices
- Releasing a New Device from the Quarantine
- Resetting a Device to Factory Default Settings

    See also Enabling a Device Password Security Policy

- ◆ Removing a GroupWise Account from a Device
- ◆ Deleting a Device
- ◆ Reinitializing a User

Resynchronizing a Device

Occasionally, synchronization problems arise between mobile devices and GroupWise:

- ◆ Synchronization from the Mobility system to a mobile device might occasionally stop, perhaps because abnormal cellular network conditions resulted in dropped synchronization data.

- ◆ Data on a mobile device might not match data as displayed in the GroupWise mailbox.

Resynchronizing the device can resolve these problems. Resynchronization causes existing GroupWise data on the device to be deleted, and then synchronized again from the Mobility system. The user can accomplish the same thing by removing the account from the mobile device and adding it again.

1 In the Mobility Admin console, click **Users**.

2 Click the user name of the device owner to display the User/Device Actions page.

3 In the **Actions** column in the **Devices** section, click **Resync Device** ⟳.

   You are prompted to confirm the action.

4 Click **OK** to acknowledge completion of the action.

   The device is resynchronized the next time it tries to connect to the Mobility system.

5 (Conditional) If resynchronizing the device does not resolve data discrepancies between the device and GroupWise, you must reinitialize the user.

   For instructions, see Reinitializing a User.

Blocking/Unblocking Specific Devices

As you monitor your Mobility system, you might notice that a device starts to consume an inappropriately large amount of system resources on your Mobility server. This can impact synchronization performance for all mobile device users. If this occurs, you can prevent the problem device from connecting to the Mobility system while you resolve the issue.

1 In the Mobility Admin console, click **Users**

2 Click the user name of the device owner to display the User/Device Actions page.

3 In the **Actions** column in the **Devices** section, click **Block Device** ⊘.

   If you click **Block User** ⊘ in the **User** column, it blocks all devices for the user. This is convenient when the user has multiple mobile devices, or when the user's mobile device has multiple device IDs.

   You are prompted to confirm the action.

4 Click **Block Device** so that the device can no longer connect to your Mobility system.

5 Click **OK** to acknowledge completion of the action.

At this point, **Normal** changes to **Blocked** for the device ID, and **Block Device** ⊘ changes to **Unblock Device** ▶.

6 Resolve the problem with the mobile device.

7 To unblock the device so that it can connect to your Mobility system again, click **Unblock Device** ▶.

   You are prompted to confirm the action.

8 Click **Unblock Device** to allow the device to connect.

9 Click **OK** to acknowledge completion of the action.

   The user can again connect to the Mobility system.

Releasing a New Device from the Quarantine

After you enable the device quarantine, new mobile devices cannot connect to your Mobility system until you release them from the quarantine. For background information, see Quarantining New Devices to Prevent Immediate Connection. You can configure the Mobility Service to notify you when users connect new devices. For instructions, see Enabling System and Service Notifications.

IMPORTANT: After you enable the quarantine, you must manually release quarantined devices in a timely manner.

1 In the Mobility Admin console, click **Users**.

2 Click the user name of the device owner to display the User/Device Actions page.

   The user's state displays as **Synced** because data has synchronized from the user's GroupWise mailbox to the Device Sync Agent, but the data has not yet synchronized to the user's mobile device.

3 In the **Actions** column in the **Devices** section, click **Allow Device** ✓ to free the device from the quarantine, and thereby allow the new device to connect to your Mobility system and receive the GroupWise mailbox data.

   You are prompted to confirm the action.

4 Click **Allow Device**.

5 Click **OK** to acknowledge completion of the action.

   GroupWise data begins synchronizing to the user's device.

Resetting a Device to Factory Default Settings

If a user loses a mobile device, it is important to wipe all data from the lost device as quickly as possible. If the device is recovered, it can be reset and used again.

WARNING: Because this action removes all data from the device, both business and personal, this is a very serious step to take with a mobile device. If you only want to remove a GroupWise account from the device, go to Removing a GroupWise Account from a Device.

1 In the Mobility Admin console, click **Users**.

2 Click the user name of the device owner to display the User/Device Actions page.

3 In the Actions column in the Devices section, click **Reset Device Options** ⏻.

4 In the dialog that displays, click the **Reset Device** button.

IMPORTANT: The **Reset Device** button only displays when a device can respond to a Reset command.

Additionally, some devices do not respond to a Reset command unless a security policy has been set on the device. See Enabling a Device Password Security Policy.

5 A message displays that the reset flag has been set for the device and the next time the device tries to connect with GMS, it will be reset to factory default settings.

Click **OK** to acknowledge the message and close the dialog.

6 The user's device status changes to **Resetting** and then to **Reset** when the action completes, at which point the device has returned or is in the process of returning to its factory default state.

Because the reset flag is set in GMS for the user/device, the user can no longer connect the device to its GroupWise account through GMS. Each connect request is answered with a Reset command from GMS.

If you want to allow the user to add GroupWise on the device again, you must either

◆ Delete the device from your Mobility System, which removes all data regarding the device from Mobility, allowing it to be added as a new device.

Or

◆ Change GMS to allow the device to add the GroupWise account, see Step 7

7 (Conditional) If you want to put the device back into service without deleting it from Mobility, do the following:

7a In the **Actions** column in the **Devices** section, click the **Re-allow device** ⊗ icon that replaced the Device Reset Options icon ⏻)

7b In the dialog that displays, click **Allow Device**.

7c Click **OK** to acknowledge completion of the action.

The user can now reconfigure the device to connect to the Mobility system and start synchronizing data.

Removing a GroupWise Account from a Device

If you need to remove a GroupWise account from a device for any reason, for example if the device is being assigned to a different user, complete the following instructions.

NOTE: This action removes all of the configuration settings and data for a GroupWise account from the device. Although, you can re-add the same GroupWise account and synchronize the data again (as described below), you cannot simply undo the account removal.

1 In the Mobility Admin console, click **Users**.

2 Click the user name of the device owner to display the User/Device Actions page.

3 In the Actions column in the Devices section, click **Reset Device Options** ⏻.

4 In the dialog that displays, click the **Remove Account** button.

5 A message displays that the remove account flag has been set for the device and the next time the device tries to connect with GMS, the user's GroupWise account will be removed.

   Click **OK** to acknowledge the message and close the dialog.

6 The user's device status changes to **Removing** and then to **Removed** when the action completes, at which point the user no longer has a GroupWise account on the device.

   Because the reset flag is set in GMS for the user/device, the user can no longer connect the device to its GroupWise account through GMS. Each connect request from the user is answered with a Reset command from GMS.

   If you want to allow the user to add GroupWise on the device again, you must either

   ◆ Delete the device from the user's Mobility account, which removes all data regarding the device from the account and allows the user to add GroupWise again.

      Or

   ◆ Re-allow the device in GMS, as explained in Step 7.

7 (Conditional) If you want to allow the user to add its GroupWise account to its device without first deleting the device from the user's Mobility account, you must do the following:

   7a In the **Actions** column in the **Devices** section, click the **Re-allow device** ⊗ icon that replaced the Device Reset Options icon ⏻.

   7b In the dialog that displays, click **Allow Device**.

   7c Click **OK** to acknowledge completion of the action.

      The user can now add GroupWise to the device through the Mobility service and start synchronizing data.

Deleting a Device

When a user is no longer using a device, you should promptly delete it from your Mobility system. Deleting the device does not delete the user from your Mobility system. If necessary, the user can again configure the device to connect to the Mobility system.

NOTE: By default, mobile devices that have not connected to your Mobility system for 30 days are automatically removed from your Mobility system. For more information about automatic deletion, see Removing Unused Devices Automatically.

To immediately remove a device from your Mobility system:

1 In the Mobility Admin console, click **Users**

2 Click the user name of the device owner to display the User/Device Actions page.

3 In the **Actions** column in the **Devices** section, click **Delete** ⊗.

   You are prompted to confirm the action.

4 Click **Delete Device** to remove the device from the Mobility system.

5 Click **OK** to acknowledge completion of the action.

Reinitializing a User

IMPORTANT: Starting with GMS 18.4, the MCheck utility lets you reinitialize multiple users at the same time. For more information, see Using MCheck to Simplify User, Certificate, and Database Management > Users.

If resynchronizing a device does not resolve discrepancies between data on a mobile device and data as displayed in GroupWise, you must reinitialize the user. For background information about resynchronizing, see Resynchronizing a Device,

During reinitialization, the user's GroupWise data is deleted from the Mobility system and is requested again from the GroupWise system. If the user has a large amount of GroupWise data and attachments, the reinitialization process might take a long time.

1 Have the user delete the GroupWise account from his or her mobile device.

2 In the Mobility Admin console, click **Users**.

3 Click the user name of the device owner to display the User/Device Actions page.

4 In the **Actions** column in the **User** section, click **Reinitialize User** ↻.

   You are prompted to confirm the action.

5 Click **Reinitialize User** to remove the user's GroupWise data from the Mobility system and request it again from the GroupWise system.

6 Click **OK** to acknowledge completion of the action.

7 Have the user re-add the GroupWise account to the mobile device to complete the reinitialization process.

8 (Conditional) If reinitializing the user still does not resolve discrepancies between data on the device and data as displayed in GroupWise, delete the user from the Mobility system, and then re-add the user.

   See Managing Mobile Device Users.

8 GroupWise Mobility for Microsoft Outlook

GroupWise Mobility Service 18 allows the Microsoft Outlook 2013, 2016, and 2019 clients for Windows and the Microsoft Outlook app to run against a GroupWise backend via Microsoft ActiveSync 14.0 protocol.

- "Configuring GroupWise Mobility Service to Support Microsoft Outlook Clients" on page 75
- "Setting Up Microsoft Outlook Clients" on page 76
- "Known Outlook Client Limitations" on page 81

Configuring GroupWise Mobility Service to Support Microsoft Outlook Clients

Complete the tasks in the following sections to enable your GroupWise Mobility system to support Microsoft Outlook clients.

- "Microsoft Outlook Support in GroupWise Mobility Service" on page 75
- "Provisioning Users in GroupWise Mobility Service" on page 75

Microsoft Outlook Support in GroupWise Mobility Service

By default, Outlook client support is enabled for GroupWise Mobility Service. You can select which types of Outlook devices to connect to GMS: the Outlook client, the Outlook Mobile app, or both. Outlook client is selected by default.

If possible, each Mobility server that you enable should be using a trusted certificate rather than a self-signed certificate. On Mobility servers that use self-signed certificates, Outlook client users can receive frequent warning messages and Outlook app users will not be able to connect at all. For more information, see Self-Signed Certificates.

To change the Outlook client support:

1 In the Mobility console, go to **Config** > **Device**.

2 Make sure **Allow Connections** is enabled.

3 Enable or disable **Outlook Client** or **Outlook Mobile App** to allow or disallow Outlook devices to connect to GMS.

4 Click **Save**.

Provisioning Users in GroupWise Mobility Service

GroupWise users who will use the Outlook client must be added to the GroupWise Mobility system. For information about adding users to your GroupWise Mobility system, see Managing Mobile Device Users.

Setting Up Microsoft Outlook Clients

Complete the tasks in the following sections to set up Outlook clients to access GroupWise:

Supported Microsoft Outlook Clients

- Microsoft Outlook 2013, 2016, and 2019 for Windows
- Microsoft Outlook App

Adding a GroupWise Account to the Microsoft Outlook Client

The Outlook client must be configured to access a user's GroupWise account. The following instructions assume that the Outlook client is already installed on the desired machine.

1 On the machine, open **Control Panel** > **User Accounts and Family Safety**.

2 Click **Mail**.

3 (Conditional) If a Mail Setup dialog box is displayed, click **Show Profiles** to display the Mail dialog box.
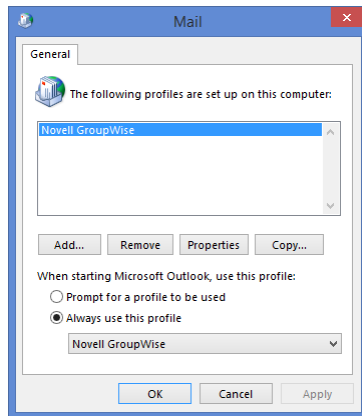
If GroupWise is installed on the machine, the Profiles list includes a **GroupWise** profile, as shown in the screenshot above. You need to keep this profile and create a new profile.

4 Click **Add** to create a new profile.
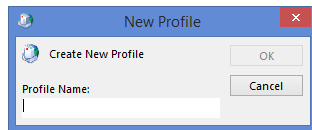
5 Specify a name for the profile (for example, *Outlook GroupWise Account*), then click **OK** to display the Add Account dialog box.
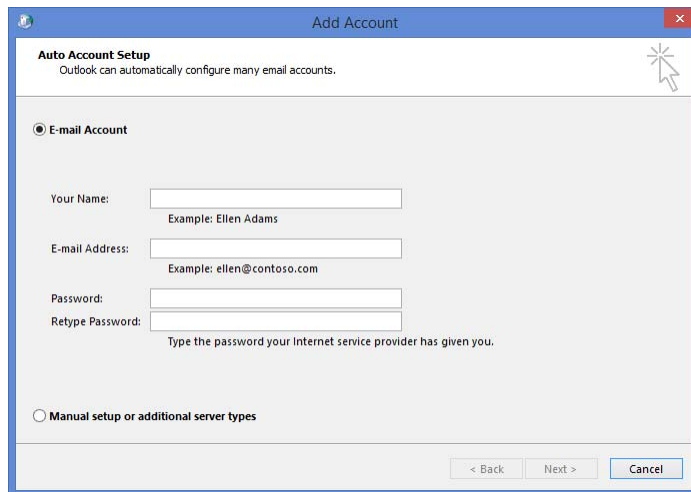
6 Select **Manual setup or additional server types**, then click **Next**.
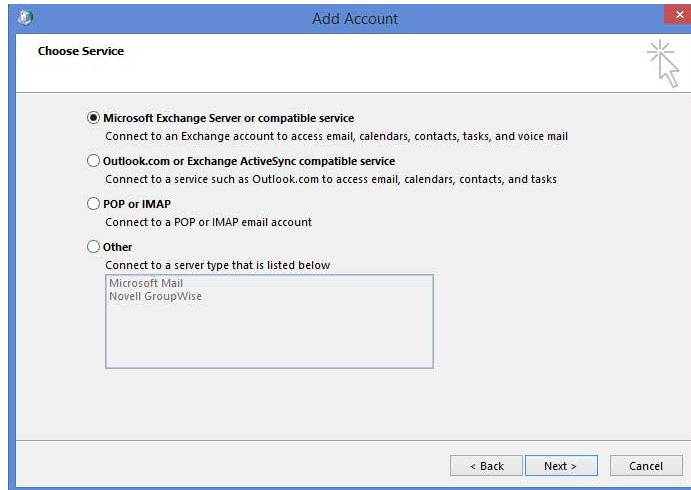
7 Select **Outlook.com or Exchange ActiveSync compatible service**, then click **Next**.
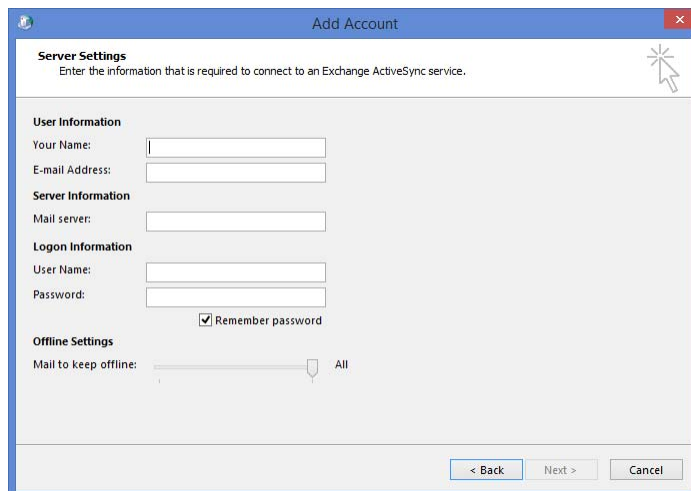
8 Provide the following information, then click **Next**.

Your Name: The GroupWise user's full name (for example, Sarah McBride).

E-mail Address: The user's GroupWise address (for example, smcbride@acme.com).

Mail Server: The GroupWise Mobility Server name or IP address (for example, gms.acme.com).

User Name: The GroupWise user name.

Password: The password associated with the user name.

9 When the account settings have been verified, click **Close** to dismiss the verification dialog box.

10 Click **Finish** to return to the **Mail** profiles dialog box.
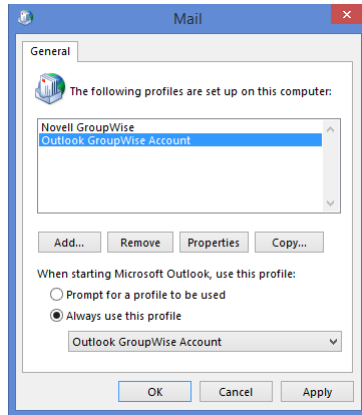
11 Select one of the following options, then click **OK** to save your changes.

- **Prompt for a profile to be used:** Select this option if the Outlook client will be used to access multiple email accounts and the user wants to be prompted to select an account when starting the client.

- **Always use this profile:** Select this option if the user wants to always open the GroupWise account when starting the client, then select the Outlook GroupWise account in the list.

12 Launch the Outlook client.

The client begins synchronizing data from the GroupWise account.

(Optional) Configuring GroupWise Address Lookup in the Microsoft Outlook Client

There are two ways that you can configure address lookups in Outlook: the GroupWise System Address Book or LDAP.

Using the GroupWise System Address Book

To use the GroupWise System Address Book, complete the instructions in the following sections.

Create an Admin App in GroupWise

To create an admin app for Mobility using the GroupWise Admin service, do the following:

1 Create the admin app by running the following curl command on your GroupWise primary domain server, replacing the items in the command by referring to the list that follows it.

```
curl -k --user gw_sys_admin:admin_password -X POST -H "Content-
Type:application/json" --data
"{\"name\":\"admin_app\",\"password\":\"admin_app_password\",\"descrip
tion\":\"app_description\"}" https://GW_domain_ip:9710/gwadmin-service/
system/adminapps
```

The following items need to be replaced in the curl command:

- **gw_sys_admin:** Specify your GroupWise system admin username.
- **admin_password:** Specify the password of your GroupWise system admin.
- **admin_app:** Specify a name for your admin app.
- **admin_app_password:** Specify a password for your admin app.
- **app_description:** Specify the purpose of the admin app. In this case it is for GMS.
- **GW_domain_ip:** Specify the IP address of your GroupWise primary domain server.

NOTE: If you are running this command on a Windows server that doesn't have curl installed, you can download it here.

2 Continue with the next section.

Create a New Address Book in Outlook

1 In Outlook, create a new Address Book using the following information:

- Select **Internet Directory Service (LDAP)** for the address book type
- For the **Server Name**, specify the DNS name or IP address of your GroupWise server.
- For **Logon Information**, the user name is the Admin App name in the following format:

    `cn=admin_app_name`

    The password is the password of the Admin App.

- In **More Settings** > **Search**, specify the custom base as `o=GroupWise_system_name`, replacing *GroupWise_system_name* with the name of your GroupWise system.

2 After saving, exit and restart Outlook to make the address book available.

Using LDAP

1 From the main Microsoft Outlook window, click **File** > **Account Settings**.

2 Click the **Address Books** tab, then click **New**.

3 Select **Internet Directory Service (LDAP)**, then click **Next**.

4 Enter the server name (for example, `ldap.myidomain.com`).

5 Enter additional settings as required by your configuration (port, SSL, credentials).

6 Save the LDAP information.

7 Exit and restart Outlook.

The LDAP address book will be available for name search/selection from the Address Book list in Outlook.

(Optional) Configuring GroupWise Free/Busy Search in the Microsoft Outlook Client

Microsoft Outlook has not implemented the ActiveSync 14.*x* ability to look up contact availability (Free/Busy information).

However, GroupWise provides a Calendar Publishing Host that you can use to make Free/Busy information available in the Outlook client. For information, see "Setting Up the GroupWise Calendar Publishing Host" in the *GroupWise 18 Installation Guide*.

To configure the Outlook client to use Free/Busy information made available by the GroupWise Calendar Publishing Host:

1 From the main Microsoft Outlook window, click **File** > **Options**.

2 In the left panel, click **Calendar**.

3 In the **Calendar Options** section, click the **Free/Busy Options** button.

4 Select the **Publish at Location** box, change the value in the box to 36 months or less, then uncheck the **Publish at Location** box.

5 In the **Search Location** field, enter the Free/Busy URL for your published Internet Free Busy path, replacing your user name with `%NAME%` and your domain with `%SERVER%`. For example:

   `http://groupwise.acme.com/gwcal/freebusy/%NAME%@%SERVER%`

   You can find your IFB in the GroupWise client, under **Tools** > **Options** > **Calendar** > **Busy Search**.

6 Click **OK** to save the changes.

   When you go to Scheduling in the Outlook client and add a GroupWise user to the Attendees list, the user's Free/Busy information is displayed.

Known Outlook Client Limitations

Your experience running the Microsoft Outlook client against a GroupWise backend should be roughly equivalent to running Outlook against an Outlook.com or Hotmail account. Known limitations are caused by several factors, including Outlook, the ActiveSync protocol, GroupWise Mobility Service, and general differences between GroupWise and Outlook features.

Supported Clients

- Microsoft Outlook 2016 and 2019 clients for Windows are the only supported Outlook clients.
- The Mail metro app included with Windows 8 and newer versions includes ActiveSync. Micro Focus has not tested or documented support for this configuration.
- The Outlook app for iOS and Android includes ActiveSync. Micro Focus has not tested or documented support for this configuration. To explicitly enable or disable Outlook app access to your Mobility servers, see Microsoft Outlook Support in GroupWise Mobility Service.
- NitroDesk TouchDown supports ActiveSync on iOS and Android. Micro Focus has not tested or documented support for this configuration.
- SyncEvolution claims support for ActiveSync. Micro Focus has not tested or documented support for this configuration.

- The following configurations will not work:
    - Hotmail Connector for Microsoft Outlook 2010
    - Microsoft Outlook 2011 for Mac
    - Microsoft Outlook 2013 for Mac
    - Native Mac OS Mail, Contact and Calendar applications
    - Ximian Evolution

Performance/Scalability

- We expect user response times to be good for operations such as accessing item lists, performing queries, and reading attachments because GroupWise data synchronizes to a local Outlook cache (OST) file.
- If any scale issues exist, they will most likely be related to additional load on GroupWise Mobility Service and will likely result in synchronization delays with the cache.
- GroupWise Mobility Service can be configured to allow, to exclusively allow, or to prevent Outlook connections to give administrators control if Outlook impacts overall performance. See Microsoft Outlook Support in GroupWise Mobility Service.

Initial Synchronization

- The initial synchronization of data is limited by the GroupWise Mobility Service configuration set by the administrator. For instance, if you choose to keep all data offline but GroupWise Mobility Service is configured to allow 60 days worth of data, the initial sync will only synchronize the most recent 60 days of data.

Address Book/Contacts

- Personal groups do not synchronize to Outlook.
- Outlook does provide search capabilities against LDAP. To configure LDAP address lookups, see (Optional) Configuring GroupWise Address Lookup in the Microsoft Outlook Client.
- When using LDAP address lookups, ensure that the display name is populated for users. If it is not, quick lookups do not work and advanced search must be used.
- If an LDAP Address Book is not added to the Mobility Outlook email client, the Address Book drop down selection is empty. In this case, Outlook creates name completion for personal contacts and recipients from sent items.
- Outlook supports contacts but does not support Personal Address Books (PAB). GroupWise Mobility Service improves this experience by aggregating contacts from all sync-configured PABs when syncing to Outlook.
- Contacts created in Outlook are created in the default PAB as specified in the **GroupWise** settings section of the GroupWise Mobility configuration for each user.

Compose

 - Outlook does not create server-side drafts. They are stored locally and are not available even from other workstations running Outlook.
 - Name completion data is not synchronized to GroupWise or between clients using GroupWise Mobility Service.

Tasks

 - ActiveSync 14.*x* does not support Outlook/GroupWise `%Complete`.
 - ActiveSync 14.*x* does not support GroupWise Priority. It does map the priority settings on the Send Options tab to Outlook's `High`/`Standard`/`Low` priorities.
 - On an Outlook task, the details view has many fields that do not sync to GroupWise. They are:

   1. `Date Completed`
   2. `Total/Actual Work`
   3. `Milage`
   4. `Billing Information`
   5. `Company`

 - On a GroupWise task, only `High`, `Standard`, and `Low` priority settings sync to Outlook. All other settings are GroupWise only settings.
 - ActiveSync does not support recipients on tasks. Tasks are personal items when synced to Outlook.
 - GroupWise distributed tasks sync the `Subject`, `Start Date`, `Due Date`, `Message Body`, `Priority (High, Standard, Low)`, `Complete`, `Alarm`, and `Recurrences` as a personal task in Outlook. If you modify the distributed task in Outlook, only a `Subject` change is applied by GroupWise and when GroupWise syncs with Outlook again, any other changes in Outlook are overwritten by the GroupWise settings.
 - Distributed tasks created in Outlook sync as a distributed in GroupWise 18 or higher only. Outlook tasks with embedded items or attachments do not sync to GroupWise.

Availability and Meeting Requests

 - Outlook has not implemented the Exchange ActiveSync 14.*x* ability to look up contact availability (Free/Busy information). Users must configure Outlook to use a global Internet Free/Busy path to check attendee Free/Busy status.

   An administrator must also configure and enable the GroupWise Calendar Publishing Server for users to publish Internet Free/Busy information. The administrator can choose to publish all Free/Busy information, or the administrator can enable publishing but leave the decision to publish Free/Busy information to individual users.

   For instructions, see (Optional) Configuring GroupWise Free/Busy Search in the Microsoft Outlook Client.

- The entered email address must match exactly the email address for which the .ifb is published on GroupWise CalPub. For instance, if the name is published as *user@novell.com*, then only this email address will return Free/Busy information to Outlook even though the user might also be addressable via other iDomains or address formats (for example, *user@gw.novell.com*, *user@attachmate.com*, and *first.last@novell.com*).

- Outlook does not allow configuration of multiple global internet Free/Busy search paths, so Outlook users on a mixed system can only configure availability searches against GroupWise users or against Exchange users.

- Outlook Internet Free/Busy (IFB) lookups will not work with self-signed certificates. The IFB server must be configured for HTTP or the certificate chain must include a trusted root CA. With a self-signed certificate, Outlook does not prompt the user as is the case in normal browsers, and allows him or her to continue even though the IFB server isn't trusted. As a result, Outlook eventually presents a generic error message stating that there is a problem with the Free/Busy URL.

- Outlook does not auto-add the organizer as an attendee for meeting requests. The organizer needs to manually add himself in order to show on the GroupWise calendar and to block out Free/Busy time in GroupWise.

- No support for online meeting requests.

- No support for Lunar calendar.

- If you have Outlook users who are running against an Exchange back end, you can use the GroupWise Free/Busy Service to allow GroupWise and Outlook users to perform Free/Busy searches on each others' calendars.

Folders

- Online email search is not available in Outlook or GroupWise Mobility Service.

- Outlook does not have a Notes folder/application. Notes created in GroupWise or on devices such as the iPhone will not be available within Outlook.

- No ActiveSync support for shared folders, calendars, or address books.

- Folder permissions are grayed out in Outlook.

- No support for **Always Move Messages in a Conversation or From a Particular Sender**.

- Outlook does not allow posting of an item to a folder (**New Items** > **More Items** > **Post in this Folder**).

- Outlook does not allow moving an item from another store (for example, PST, Hotmail, or IMAP) to ActiveSync folders.

- Outlook does not allow using ActiveSync folders for POP3 mailboxes.

- Outlook search folders are not synchronized.

Rules

- In Outlook, you cannot create rules that will execute on the server (for example, vacation, auto-reply, auto-forward). Client-side rules are available, but the Outlook client must be running in order for the rule to execute.

- Creating rules in an Outlook/GroupWise configuration is more difficult than creating those same rules in an Outlook/Exchange configuration. For example, creating a client-side vacation rule requires the user to browse to and select a previously saved message template rather than giving the user the ability to edit the rule directly during rule creation. For more information, see http://www.ablebits.com/office-addins-blog/2014/02/20/create-email-templates-outlook/.
- Junk mail handling does not synchronize.

External System Integration

- Outlook does not provide a way to import external data into a store.
- No support for SharePoint file links proxied through ActiveSync.

GroupWise Features Not Available in Microsoft Outlook

- **Proxy:** Outlook cannot proxy GroupWise user mailboxes.
- **Sent Item Properties:** Outlook does not provide properties for sent items.
- **Calendar Publishing Host:** Outlook cannot publish user availability through the Calendar Publishing Host for others to consume.
- **Reminder Notes/Personal Reminder Notes:** Outlook displays GroupWise reminder notes and personal reminder notes as all-day events.
- **Phone Messages:** Outlook displays GroupWise Phone messages as email.
- **Editors:** Outlook does not support OpenOffice/LibreOffice as an editor.
- **Send Options:** Outlook does not support GroupWise Send options such as concealed subject, recipient notification, and reply requested. Delayed message delivery, expiration, and redirected replies do not work.
- **Security Classifications:** Outlook maps the GroupWise Security classifications (proprietary, secret, top secret, and for your eyes only) to the Outlook sensitivities of personal, private, or confidential.
- **Resources:** Outlook cannot manage GroupWise resources.
- **Meeting Requests:** Outlook filters out meeting requests from mail folders, including the Sent Items folder. These are only accessible through the calendar.

Miscellaneous

- **Categories:** Categories do not sync between Outlook and GroupWise. Categories will sync between Outlook and other GroupWise Mobility connected devices.
- **Message Retraction:** Message recall (retraction) is not available over Exchange ActiveSync.
- **Self-Signed Certificates:** If your server is using self-signed certificates (not signed by a trusted CA), users might experience frequent warning messages. If you have enabled your GroupWise Mobility server to support the Microsoft Outlook app (see Microsoft Outlook Support in GroupWise Mobility Service), the server must be configured to use a trusted certificate. If you use the self-signed certificate that GroupWise Mobility Service generates, the Outlook app will not be able to connect.
- **Voting Buttons:** Voting buttons do not work.

◆ **Remote Wipe:** Outlook does not honor remote wipe requests from GroupWise Mobility Service.

9 GroupWise Mobility System Security

Large amounts of personal and confidential information pass between GroupWise and mobile devices. Securing the synchronization process is a vital aspect of securing your GroupWise system.

Security Administration

It is vital to secure each stage in the communication path between GroupWise and mobile devices.

Securing Communication between the GroupWise Sync Agent and the GroupWise POA

The GroupWise Sync Agent communicates with the GroupWise POA as a SOAP client. In order to secure communication between the GroupWise Sync Agent and the GroupWise POA, the POA must be configured for secure SSL SOAP. SSL SOAP security is enabled by default in GroupWise 18.

You can enable and disable SSL for the POA SOAP connections on the GroupWise Sync Agent Configuration page in the Mobility Admin console. For instructions, see Enabling and Disabling SSL for POA SOAP Connections.

Securing Communication between the Device Sync Agent and Mobile Devices

In order to provide a secure SSL connection between the Device Sync Agent and mobile devices, you must provide a server certificate on the Mobility server.

Using a Self-Signed Certificate on the Mobility Server

IMPORTANT: You should obtain a commercially signed certificate for use with your Mobility system as quickly as possible.

Starting with GMS 18.4, the entire process of obtaining a certificate has been automated in the MCheck utility. For details see, Using MCheck to Simplify User, Certificate, and Database Management > Generate a Private Key and Certificate Signing Request.

When you have the Mobility Service Installation program create a self-signed certificate for you, two certificate files are created in the `/var/lib/datasync` directory:

```
gms_mobility.pem
gms_mobility.cer
```

NOTE: `/var/lib/datasync` also contains a system-use only file named `gms_server.pem`. Do not modify or replace this file.

When a mobile device connects to the Device Sync Agent, the Device Sync Agent passes the self-signed certificate file (`gms_mobility.pem`) to the mobile device. In most cases, the mobile device accepts the self-signed certificate and connects successfully.

Some mobile devices do not automatically accept self-signed certificates in PEM format. If you choose to use a self-signed certificate and if users encounter connection problems with particular mobile devices, explain the procedure in Manually Downloading a Certificate to a Mobile Device to the users who are encountering connection problems. This procedure enables users to use the `gms_mobility.cer` file instead of the `gms_mobility.pem` file on their mobile devices.

The self-signed certificate generated by the Installation program is issued to "DataSync Web Admin" rather than to a specific hostname. Some mobile devices require that a self-signed certificate be associated with a specific hostname.

Using a Commercially Signed Certificate on the Mobility Server

IMPORTANT: You should obtain a commercially signed certificate for use with your Mobility system as quickly as possible.

Starting with GMS 18.4, the entire process of obtaining a certificate has been automated in the MCheck utility. For details see, "Using MCheck to Simplify User, Certificate, and Database Management" on page 13 > Generate a Private Key and Certificate Signing Request.

Obtaining the Certificate

When you have selected a certificate authority, request a certificate in PEM format. If necessary, you can use a chained certificate or a wildcard certificate with your Mobility system.

In order to obtain a certificate, you need to send the certificate authority a certificate signing request (CSR). For example, you can use OpenSSL to generate the CSR.

1 In a terminal window on the Mobility server, become `root` by entering `su -` and the root password.

2 Change to a convenient directory where you want to create the CSR.

3 Create the key file:

   3a Enter the following command:

   ```
   openssl genrsa -des3 -out key_file_name.key 2048
   ```

   Replace `key_file_name.key` with a convenient name for the private key file, such as `gw.key`.

   3b Enter and verify a pass phrase for the key file.

4 Create the CSR:

   4a Enter the following command:

   ```
   openssl req -new -key key_file_name.key -out csr_file_name.csr
   ```

   Replace `key_file_name.key` with the key file that you created in Step 3.

   4b Enter the pass phrase for the key file.

   4c Enter the two-letter code for your country, such as `US` for the United States, `DE` for Germany, and so on.

   4d Enter your state or province.

   4e Enter your city.

   4f Enter the name of your company or organization.

   4g Enter your department or other organizational unit.

   4h Enter your name.

   4i Enter your email address.

   4j (Optional) Enter a password for the CSR, or simply press Enter.

   4k (Optional) Enter a secondary name for your company or organization, or simply press Enter.

NOTE: Depending on the method that you use to generate the CSR, you might be prompted for the type of web server where you plan to install the certificate. The Mobility Service uses the CherryPy web server.

The certificate authority returns one or more files to you. Save the files to a convenient location. These files might require modification for use in your Mobility system.

 ◆ You must remove the pass phrase from the key file. For instructions, see Removing a Pass Phrase from a Key File.
 ◆ If the certificate authority provided multiple files, combine them into a single file. For instructions, see Combining Files Received from a Certificate Authority.

Removing a Pass Phrase from a Key File

If the key file that you created in Step 3 on page 89 includes a pass phrase, you need to remove it in order to use the file in your Mobility system.

1 Check to see if the key file includes a pass phrase.

   A pass-phrase-protected key file includes the following line:

   ```
   Proc-Type: 4,ENCRYPTED
   ```

2 Use the following command to remove the pass phrase:

   ```
   openssl rsa -in original_file_name.key -out pass-phrase-
   less_file_name.key
   ```

Combining Files Received from a Certificate Authority

If you receive more than one file from the certificate authority, such as a certificate file and a key file, you must combine the contents into a single file with the following format:

```
-----BEGIN RSA PRIVATE KEY----- several_lines_of_private_key_text
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE----- several_lines_of_server_certificate_text
-----END CERTIFICATE-----
```

If the certificate authority provided an intermediate certificate, place it at the end of the file after the private key and the actual certificate.

Installing a Commercially Signed Certificate on the Mobility Server

1 (Conditional) If you have been using a self-signed certificate, rename the existing /var/lib/datasync/gms_mobility.pem file.

2 Copy the certificate file received from the certificate authority to /var/lib/datasync.

3 Rename it to gms_mobility.pem.

4 Restart the Mobility Service.

IMPORTANT: If you uninstall the Mobility Service, the certificate files associated with your Mobility system are also deleted. Back up commercially signed certificates in a location outside of /var/lib/datasync.

Manually Downloading a Certificate to a Mobile Device

NOTE: When GMS starts or restarts, a new `gms_mobility.cer` file is generated automatically from the existing `gms_mobility.pem` file.

1 Access the Mobility Settings page of the Mobility Admin console on your mobile device at the following URL:

`https://mobility_server:8120`

Replace `mobility_server` with the IP address or DNS hostname of the server where you installed the Mobility Service.

2 Log in using your network user name and password to display the Mobility Settings page on your mobile device.

3 Tap **Device Settings**.

4 In the **Mobility Certificate File** field, tap **Download Certificate File**.

5 Save the `gms_mobility.cer` file to a convenient location on your mobile device.

6 Import the certificate file into the certificate store on your mobile device.

For device-specific instructions, see the GroupWise Mobility Service Devices Wiki (http://wiki.novell.com/index.php/GroupWise_Mobility_Devices).

7 (Conditional) If you are not able to access the Mobility Settings page from your particular mobile device:

    7a Access the Mobility Settings page in a web browser on your Windows or Linux desktop, then click **Device Settings**.

    7b Click **Download Certificate File**.

    7c Save the `gms_mobility.cer` file on your Windows or Linux workstation.

    7d Set up an IMAP email account on your mobile device, then email the `gms_mobility.cer` file from your workstation to your mobile device.

        or

        Physically connect your mobile device to your workstation so that it appears as a drive on your workstation, then copy the `gms_mobility.cer` file from your workstation to your device.

8 Import the certificate file into the certificate store on your mobile device.

Enabling and Disabling SSL for Device Connections

For instructions, see Enabling and Disabling SSL for Device Connections.

Enabling a Password Security Policy for Device Connections

For instructions, see Enabling a Device Password Security Policy.

Security Policies

Appropriate security policies help you keep users' personal GroupWise data and Mobility system information secure.

- "Certificate Considerations" on page 92
- "Securing Your Mobility Data" on page 92
- "Securing Your Mobility System" on page 92

Certificate Considerations

When creating certificates for your GroupWise system, we recommend the following:

- Consolidate to one CA for your GroupWise system.
- Use a public CA for your GroupWise system.
- Use a wildcard certificate for all of your POAs.

Securing Your Mobility Data

Your Mobility server must be kept secure.

- "Limiting Physical Access to Mobility Servers" on page 92
- "Securing File System Access" on page 92

Limiting Physical Access to Mobility Servers

Servers where Mobility data resides should be kept physically secure, in locations where unauthorized persons cannot gain access to the server consoles.

Securing File System Access

Encrypted file systems should be used on all Mobility servers. Only Mobility administrators should have direct access to Mobility data.

Securing Your Mobility System

Locations where GroupWise users' personal data and Mobility system information might be obtained must be kept secure.

- "Setting Up SSL Connections" on page 93
- "Setting Up a Device Password Security Policy" on page 93
- "Securing the Mobility Admin Console" on page 93
- "Protecting Mobility Configuration Files" on page 93
- "Protecting Mobility Log Files" on page 94

Setting Up SSL Connections

Secure SSL connections should be used between your Mobility system and the following external components:

- GroupWise Post Office Agent (POA)
- Browser connection for the Mobility Admin console
- Mobile devices

For instructions, see Security Administration.

Setting Up a Device Password Security Policy

To increase your control over mobile device access to your Mobility system, you should establish a device password security policy to ensure that users set up secure passwords on their mobile devices. For instructions, see Enabling a Device Password Security Policy.

Securing the Mobility Admin Console

The `root` user on the Mobility server is the Mobility Administrator.

IMPORTANT: The number of people who know how to log in to the Mobility Admin console should be kept to a minimum.

The Mobility Admin console can be integrated with a single sign-on solution. For more information, see Using the Mobility Admin Console with a Single Sign-On Solution.

Protecting Mobility Configuration Files

The configuration files for all internal Mobility components should be protected from tampering. Configuration files are found in the following default locations:

Internal Mobility Component	Configuration File
Sync Engine	/etc/datasync/syncengine/engine.xml
Web Admin	/etc/datasync/webadmin/server.xml
Config Engine	/etc/datasync/configengine/configengine.xml
Connector Manager	/etc/datasync/syncengine/connectors.xml

Protecting Mobility Log Files

The log files for all internal Mobility components should be protected against unauthorized access. Some log files contain very detailed information about your Mobility system and users. Mobility log files are found in the following locations:

Internal Mobility Service Component	Log File Subdirectory under /var/log/datasync	Log File Name
Sync Engine	`syncengine`	`engine.log`
Config Engine	`configengine`	`configengine.log`
Web Admin	`webadmin`	`server.log`
Connector Manager	`syncengine`	`connectorManager.log`

Sync Agents	`connectors`	`groupwise-agent.log`
		`groupwise.log`
		`mobility-agent.log`
		`mobility.log`

If you set the Mobility Service log level to Debug, Subject lines are included in log files for troubleshooting purposes. This information identifies items that are experiencing synchronization problems.

If you use the Debug log level, ensure that log files are kept secure to protect users' personal information. The Info log level is strongly recommended for a smoothly functioning Mobility system.

No text about recipients or from message bodies is included in log files.

Certificate Verification

GroupWise Mobility Service 18 allows verification of the POA TLS/SSL certificate. After the installation or upgrade, certificate verification is disabled by default.

 * Prerequisites
 * Gathering CA Certificates
 * Verifying the CA Certificates
 * Adding the CA Certificates
 * Enabling Certificate Verification
 * Troubleshooting Certificate Verification

Prerequisites

 * In the GroupWise Admin Console, the POA TCP/IP address needs to have the DNS name specified.
 * In the Mobility Admin Console, the POA SOAP address needs to have the DNS name specified instead of the IP address.

Gathering CA Certificates

Follow the section that matches how you generated your POA certificates for each CA that you need to gather:

- GroupWise 18 Certificate Authority
- NetIQ Certificate Server
- Trusted Commercial Certificate Authority

GroupWise 18 Certificate Authority

If your CA is GroupWise (18 or later), you can use one of the two methods below to get the certificate.

Method 1

1 Open a browser to `https://primarydomainip:adminport/gwadmin-service/system/ca`.

   For example: `https://10.10.10.10:9710/gwadmin-service/system/ca`

2 Enter your GroupWise admin credentials.

3 Save the certificate to the GMS server in `/var/lib/datasync/mobility`.

4 Continue with Verifying the CA Certificates if you have gathered all of your CA certificates.

Method 2

1 Open a terminal on your GMS linux server.

2 Enter the following command:

   `curl -k --user username -o filename https://primarydomainip:adminport/gwadmin-service/system/ca`

   Replace `username` with your admin username and `filename` with the name of the saved file.

3 Copy the certificate and then save it to the GMS server in `/var/lib/datasync/mobility`.

4 Continue with Verifying the CA Certificates if you have gathered all of your CA certificates.

NetIQ Certificate Server

If your CA is a NetIQ Certificate Server, follow the steps below:

1 Login to iManager.

2 Select **NetIQ Certificate Server**.

   It may be called **Novell Certificate Server** depending on your version of iManager.

3 Select **Configure Certificate Authority**.

4 Select the **Certificates** tab.

5 Select the **Self Signed Certificate** check box.

6 Select **Export**.

7 Unselect **Export private key**.

8 Select export formate as Base64.

9 Select **Next**.

10 Select **Save the exported certificate file**. Save it to the GMS server in `/var/lib/datasync/ mobility`.

11 Continue with Verifying the CA Certificates if you have gathered all of your CA certificates.

Trusted Commercial Certificate Authority

If your CA is a commercial CA, follow the steps below:

1 Verify if your certificate is in the Mozilla trusted root CA store by checking the `/var/lib/ datasync/mobility/cacert.pem` file on the GMS server where the CA store is stored. If your CA is in the list, continue with Verifying the CA Certificates if you have gathered all of your CA certificates.

or

2 If your CA is not in the list, you need to find your CA public root certificate and place it on the GMS server in `/var/lib/datasync/mobility`. Continue with Verifying the CA Certificates if you have gathered all of your CA certificates.

Verifying the CA Certificates

Once you have your CA certificate, make sure it meets the following requirements:

- Base64-encoded format
- In the `Basic Constraints`, ensure that `Subject Type=CA` is specified.
- Ensure that the current date is between the `Valid from` and `Valid to` dates.
- The `Issuer` and the `Subject` match.

You can verify these requirements by viewing the details of the certificate or by running an openssl command to view the certificate information.

If your CA meets these requirements, continue with Adding the CA Certificates.

Adding the CA Certificates

For the certificate verification to work, the CA certificates found previously needs to be added to the mob_ca.pem file. Follow the section that matches each CA certificate you gathered previously:

GroupWise 18 Certificate Authority

1 In a terminal on your GMS server, go to `/var/lib/datasync/mobility/`.

2 Add your CA certificate to the `mob_ca.pem` file using the following command:

```
cat yourCACertficate.pem >> mob_ca.pem
```

NOTE: You may need to add a hard return in the `mob_ca.pem` after the certificate before you add any other certificates to the file.

3 Continue with Enabling Certificate Verification if you have added all of your CA certificates.

NetIQ Certificate Server

1 In a terminal on your GMS server, go to `/var/lib/datasync/mobility/`.

2 Add your CA certificate to the `mob_ca.pem` file using the following command:

```
cat yourCACertficate.pem >> mob_ca.pem
```

NOTE: You may need to add a hard return in the `mob_ca.pem` after the certificate before you add any other certificates to the file.

3 Continue with Enabling Certificate Verification if you have added all of your CA certificates.

Commercial Certificate Authority

1 In a terminal on your GMS server, go to `/var/lib/datasync/mobility/`.

2 If your CA is not in the Mozilla CA certificate list, add your CA public certificate to the `mob_ca.pem` file using the following command:

```
cat yourCACertificate.pem >> mob_ca.pem
```

or

If your CA is in the list, copy the cacert.pem file to `mob_ca.pem` using the following command:

```
cat cacert.pem >> mob_ca.pem
```

NOTE: You may need to add a hard return in the `mob_ca.pem` after the certificate before you add any other certificates to the file.

3 Continue with Enabling Certificate Verification if you have added all of your CA certificates.

Enabling Certificate Verification

Before you enable certificate verification, take a backup of the `/var/lib/datasync/mobility/mob_ca.pem` file.

1 Login to the GMS WebAdmin

2 Select **Config** > **GroupWise**.

3 Select **SSL Certification Verification**.

4 Select **Apply**.

5 In a terminal on the GMS server, restart GMS using the following command:

```
gms restart
```

Troubleshooting Certificate Verification

You may experience SSL problems the first time you enable certificate verification. The following are helpful OpenSSL commands:

- Verify POA Connection
- Verify a Certificate
- View Certificate Information
- Get POA Certificate
- View Certificate Purpose

Verify POA Connection

```
openssl s_client -showcerts -CAfile CA_public_certificate -connect
poa_DNS:soap_port
```

Example: `openssl s_client -showcerts -CAfile gwcacert.pem -connect gw.provo.novell.com:7191`

Verify a Certificate

```
openssl verify -issuer_checks -CAfile CA_public_certificate
POA_certificate
```

Example: `openssl verify -issuer_checks -CAfile cacert.pem gwpoa.pem`

View Certificate Information

```
openssl x509 -in certificate -noout -text
```

Example: `openssl x509 -in gwcacert.pem -noout -text`

Get POA Certificate

```
openssl s_client -showcerts -connect poa_DNS:soap_port
```

Example: `openssl s_client -showcerts -connect gw.provo.novell.com:7191`

View Certificate Purpose

```
openssl x509 -in certificate -noout -purpose
```

Example: `openssl x509 -in gwcacert.pem -noout -purpose`

Secure Message Gateway (GWAVA 7) Integration

Mobility 18 provides an integration with Secure Message Gateway (GWAVA 7) to secure your device emails. Device emails are scanned and accepted or rejected. If accepted, the message is delivered to GroupWise. If rejected, the sender receives an email explaining that the email was rejected by the Secure Message Gateway scan.

For this integration to work, you must do the following:

1 An Interface must be created in Secure Message Gateway for Mobility. For information on creating an interface see SMT Interface (http://support.gwava.com/documentation/GWAVA/70/html/index.html#t=SMTP_Interface.htm) in the Secure Message Gateway documentation.

2 Open the following file on the Mobility server:

```
/etc/datasync/configengine/engines/default/pipelines/pipeline1/
connectors/mobility/connecter.xml
```

3 Add the following elements in the <custom> section:

Element	Value
`<securegatewayEnable>0</` `securegatewayEnable>`	A "0" is disabled. A "1" is enabled. Set the value to "1" if you want to use Secure Message Gateway.
`<securegatewayHost>`*`securegatewayhost`*`</` `securegatewayHost>`	securegatewayHost should be set to the value found in the Secure Message Gateway Admin > **Module Management** > **Interfaces** > **3rd Party Application Manager** > *<Name of Interface created for GMS>* > **Server Address**.
`<securegatewayPort>`*`securegatewayport`*`</` `securegatewayPort>`	securegatewayPort should be set to 80 if not using SSL and 443 if using SSL.
`<securegatewaySecure>`*`securegatewaysecure`*`</securegatewaySecure>`	A "0" is non-secure or HTTP. A "1" is secure or HTTPS. Set the value to what you are using for Secure Message Gateway.
`<securegatewayAppkey>`*`securegatewayAppkey`*`</securegatewayAppkey>`	securegatewayAppkey should be set to the value found in the Secure Message Gateway Admin > **Module Management** > **Interfaces** > **3rd Party Application Manager** > *<Name of Interface created for GMS>* > **Application Key**.

4 Restart Mobility.

Multi-Factor Authentication

Multi-Factor Authentication (MFA) enables you to protect your GroupWise system by adding additional authentication on top of your GroupWise login. GroupWise supports MFA through NetIQ Advanced Authentication that allows you to add different methods of authentication to your GroupWise LDAP password login.

MFA must be configured in the GroupWise Admin Console for Mobility to use it. The steps to configure MFA and a full list of the methods available to Mobility can be found in "Multi-Factor Authentication" in the *GroupWise 18 Administration Guide*.

Mobility only supports Generic Events with UI-less methods that can be appended to the users' password with the "&" symbol. For example,(`password&token`). These include: Limited Use License - *Emergency Password*, *OATH OPT*, *HOTP*, *TOTP,* and *Password*; Full License - *BankID*, *Smartphone*, *Swisscom Mobile ID*, and *Voice*. For a full list, see "Table of NetIQ Auth Methods and GroupWise Client Compatibility" in the *GroupWise 18 Administration Guide*.

A   GroupWise Mobility System Troubleshooting

Device Troubleshooting

Initial synchronization fails

Possible Cause: The Device Sync Agent is not getting the information it needs from the GroupWise Sync Agent.

Action: Ensure that the user has a valid GroupWise account.

Possible Cause: Varied.

Action: Remove the user from the Mobility system, then add the user again.

The user's mobile device cannot connect to the Mobility System

Possible Cause: The user has not configured the mobile device correctly.

Action: Refer the user to the *GroupWise Mobility Quick Start for Mobile Device Users*, and provide the user with the details specific to your Mobility system.

Possible Cause: You have configured the Mobility Service for a secure SSL connection and the certificate is not working properly.

Action: Try using a non-secure connection. If a non-secure connection works and a secure connection does not work, ensure that the certificate is correctly set up. For setup instructions, see Securing Communication between the Device Sync Agent and Mobile Devices.

Action: For more detailed information, see GroupWise Mobility Service Device Sync Agent SSL Issues (http://wiki.novell.com/index.php/ Data_Synchronizer_Mobility_Connector_SSL_Issues).

Possible Cause: The user's device is not accepting the self-signed certificate created by the Mobility Service Installation program.

Action: See Manually Downloading a Certificate to a Mobile Device for assistance.

The user's mobile device has stopped synchronizing

Possible Cause: Varied.

Action: Resynchronize the device. For instructions, see Resynchronizing a Device. This removes the GroupWise data that is currently on the device and replaces it with the GroupWise data that is currently available in the Mobility system

The data on the user's mobile device does not match what displays in GroupWise

Possible Cause: Varied.

Action: Resynchronize the device. For instructions, see Resynchronizing a Device. This removes the GroupWise data that is currently on the device and replaces it with the GroupWise data that is currently available in the Mobility system

Action: Have the user remove the account from the device, and then re-add the account. This is a manual way of resynchronizing the device.

Action: If reinitializing the device does not resolve the problem, have the user remove the account from the device. Then reinitialize the user. For instructions, see Reinitializing a User. This removes the GroupWise data that is currently in the Mobility system and requests current data from GroupWise. The process of deleting the data in the Mobility system and requesting current GroupWise data can take a long time.

After you reinitialize the user, have the user re-add the account so that the current GroupWise data in the Mobility system transfers to the device.

Action: If reinitializing the user does not resolve the problem, delete the user from the Mobility system, and then re-add the user. See Managing Mobile Device Users.

The timestamps on calendar items do not match between a user's mobile device and the GroupWise mailbox

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" in the *GroupWise Mobility Service 18 Installation Guide*.

Some items never synchronize to the mobile device

Possible Cause: Some events automatically synchronize to mobile devices. Other events do not synchronize to mobile devices unless users request them. The user has not yet requested the optional events.

Action: None. This is normal. The unsynchronized events eventually expire.

Possible Cause: The Device Sync Agent might not be transferring the events to the mobile device.

Action: Check the user's synchronized items in the Dashboard. Observe the **Pending** column and the **Synced** column to see if progress is still being made.

If events are still transferring to the device, wait while the process completes.

If events are not transferring to the device, restart the Device Sync Agent.

Possible Cause: The user's GroupWise mailbox contains a damaged message, or the user's mailbox is damaged. Mailbox damage can cause the GroupWise Sync Agent to synchronize unusable data to the Device Sync Agent.

Action: Repair the user's mailbox. For more information, see "Maintaining User/ Resource and Message Databases" in the *GroupWise 18 Administration Guide*.

Possible Cause: Varied.

Action: Remove the user from the Mobility system, and then add the user again.

The specific actions suggested above have not resolved a synchronization problem

Possible Cause: Varied.

Action: Perform the following procedure to start over for a particular mobile device user, similar to rebooting a computer:

1 Remove the user's account from the mobile device.

2 Remove the user from the Mobility system.

3 Restart the Mobility Service.

4 Add the user to the Mobility system.

5 Add the user's account to the mobile device.

Mobility Service Troubleshooting

See also:

- "Working with Log Files" on page 57

You cannot access the Mobility Admin console after installation

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

Action: Reset the time as needed so that the workstation and the Mobility server match. This Mobility system requirement is listed in "Mobility Server Requirements" in the *GroupWise Mobility Service 18 Installation Guide*.

The process of adding users does not proceed as expected

Explanation: When you add a large number of users to the Mobility Service in a group, the Admin console might not display progress as expected. Refreshing the page might give an invalid server error.

Possible Cause: A timing issue between the Add User process and the display of the Admin console page occasionally causes this problem.

Action: Wait for a while, and then refresh your browser.

GroupWise Sync Agent Troubleshooting

See also:

- "Working with Log Files" on page 57

The GroupWise Sync Agent cannot communicate with the GroupWise Post Office Agent (POA)

Explanation: The GroupWise Sync Agent must be able to communicate with a POA in order to synchronize mailbox data. The GroupWise Sync Agent is unable to establish the connection.

Possible Cause: The POA is not running.

Action: Start the POA.

Data does not transfer between GroupWise and the GroupWise Sync Agent

Possible Cause: Varied.

Action: Ensure that the required ports are open on the GroupWise POA server and the GroupWise Sync Agent server. For instructions, see "Opening Required Ports" in the *GroupWise Mobility Service 18 Installation Guide*.

Action: Check the GroupWise Sync Agent log file. For instructions, see Working with Log Files.

The GroupWise Post Office Agent (POA) shows errors communicating with the GroupWise Sync Agent

Explanation: As you monitor the POA, you might see 890F and 8910 error codes.

Possible Cause: The connection between the GroupWise Sync Agent and the POA has temporarily closed.

Action: None. The connection is re-established automatically. These error codes are benign and can be ignored.

The GroupWise Sync Agent takes a long time to start

Possible Cause: The GroupWise Sync Agent services users that are scattered throughout your GroupWise system. Therefore, POA-to-POA communication is required in order to gather the events from the GroupWise users and return them to the GroupWise Sync Agent.

Action: None. When all GroupWise user events have been received, the status changes to **Running**.

The GroupWise Sync Agent fails to start after working successfully

Possible Cause: Another application that communicates with the POA using SOAP has created SOAP event configurations that are causing a problem for the GroupWise Sync Agent.

Action: Delete residual SOAP event configurations:

1 Stop the GroupWise Sync Agent.

2 In the POA web console, click **Configuration**.

3 In the **Internet Protocol Agent Settings** section, click **Event Configuration List**.

4 Click each user, select **Delete Event Configuration**, then click **Submit**.

5 After all event configurations have been cleared, start the GroupWise Sync Agent.

Device Sync Agent Troubleshooting

See also:

The Device Sync Agent does not start

Possible Cause: The GroupWise Sync Agent is not running.

Action: Start the GroupWise Sync Agent.

Possible Cause: The Mobility Service is not running.

Action: Check the current status of the Mobility Service. If needed, start or restart the Mobility Service. For instructions, see Starting, Stopping, and Checking GroupWise Mobility.

Possible Cause: An application on the Mobility server is using ports 80 and 443. These ports need to be available for use by the Device Sync Agent for communicating with mobile devices.

Action: Stop and disable the other application that is using ports 80 and 443 on the Mobility server.