Novell GroupWise® Mobile Server, Powered By Intellisync*

7

www.novell.com

ADMINISTRATION GUIDE

June 15, 2006

Novell®

Legal Notices

Novell, Inc. makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc. makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export, or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. Please refer to www.novell.com/info/exports/ for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

Novell, Inc. has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed at http://www.novell.com/company/legal/patents/ and one or more additional patents or pending patent applications in the U.S. and in other countries.

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
U.S.A.
www.novell.com

Online Documentation: To access the online documentation for this and other Novell products, and to get updates, see www.novell.com/documentation.

Novell Trademarks

For a list of Novell trademarks, see the Novell Trademark and Service Mark (http://www.novell.com/company/legal/trademarks/tmlist.html).

Third-Party Materials

All third-party trademarks are the property of their respective owners.

Contents

About This Guide

This Novell® *GroupWise*® *Mobile Server Administration Guide* helps you administer a GroupWise Mobile Server system. The guide is divided into the following sections:

Audience

This guide is intended for network administrators who install and administer GroupWise Mobile Server.

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, or go to www.novell.com/documentation/feedback.html and enter your comments there.

Documentation Updates

For the most recent version of the *GroupWise Mobile Server Administration Guide*, visit the Novell GroupWise 7 Documentation Web site (http://www.novell.com/documentation/gw7).

Additional Documentation

For additional GroupWise Mobile Server documentation, see the following guides at the Novell GroupWise 7 Documentation Web site (http://www.novell.com/documentation/gw7):

- *GroupWise Mobile Server Installation Guide*
- *Client Guides*

In addition to the electronic versions of the manuals, the following online help systems are available via the Help menu:

- *Email Accelerator Help*
- *Management Help*
- *Profile Settings Help*

Documentation Conventions

In Novell documentation, a greater-than symbol (>) is used to separate actions within a step and items in a cross-reference path.

A trademark symbol (®, ™, etc.) denotes a Novell trademark. An asterisk (*) denotes a third-party trademark.

When a single pathname can be written with a backslash for some platforms or a forward slash for other platforms, the pathname is presented with a backslash. Users of platforms that require a forward slash, such as Linux*, should use forward slashes as required by your software.

When a startup switch can be written with a forward slash for some platforms or a double hyphen for other platforms, the startup switch is presented with a forward slash. Users of platforms that require a double hyphen, such as Linux, should use double hyphens as required by your software.

Introducing GroupWise Mobile Server

1

This chapter introduces you to GroupWise Mobile Server and provides information for using GroupWise Mobile Server effectively.

1.1 Overview

Using GroupWise Mobile Server, you can synchronize Personal Information Manager (PIM) and e-mail data from Novell® GroupWise to Windows* CE, Windows Mobile*-based Smartphones, Symbian* OS, Palm OS* handheld devices, and SyncML* devices.

The GroupWise Mobile Server includes the following modules from Intellisync:

- E-mail Accelerator (excluding POP3, IMAP, Exchange Connector, Lotus Notes* Connector, Workgroup, and PC Monitor)
- GroupWise Connector
- Mobile device synchronization

NOTE: GroupWise Mobile Server requires a database such as Sybase* ASA or SQL Server to operate. If no database is present, Sybase ASA is available on the installation download, and you can use it for installations with close to 1000 users. For a production environment, you should use SQL Server 2000 (Service Pack 3). This full-version database environment offers expanded support for a large number of simultaneously connected clients. If you choose to use SQL Server, it should be installed prior to installing GroupWise Mobile Server.

1.1.1 GroupWise Mobile Server

Using GroupWise Mobile Server, you can synchronize PIM and e-mail data from GroupWise to Windows CE, Windows Mobile-based Smartphones, Symbian OS, and Palm OS handheld devices and SyncML devices. You can also access corporate e-mail, calendar entries, address book, and to-do lists from any Web browser or Internet-ready mobile phone.

For supported devices, you can set up the Push feature so your device receives new mail as it comes in, without any intervention from you.

GroupWise Mobile Server can be configured to connect to only one GroupWise POA. If you have users on multiple POAs, GroupWise Mobile Server uses GroupWise redirecting to find the users on other POAs during the initial search for the users. GroupWise Mobile Server always connects to the POA that the users are on.

1.2 GroupWise Mobile Server Components

GroupWise Mobile Server is built around a set of core technologies that provide a common structure and user interface for all components. This framework extends your enterprise systems to include a wide variety of devices and networks.

GroupWise Mobile Server offers an intuitive user interface, an administrative console, a secure gateway for mobile communications, and a collection of shared services, such as user management, profiles, logging, and reporting.

1.2.1 Intellisync Mobile Suite Client

The Intellisync Mobile Suite Client provides users with easy access to information available through your system.

The Intellisync Mobile Suite Client runs on client mobile devices, and is the only application the end user needs to stay connected to while away from the office.

The client has an easy-to-use user interface and serves as the user's launch pad for delivery of all mobile information.

After a communications session, the user sees a summary of the new information. The user can also view summary information for previous sessions.

For additional information about the Intellisync Mobile Suite Client, see the Novell GroupWise 7 Documentation Web site (http://www.novell.com/documentation/gw7).

1.2.2 Intellisync Mobile Gateway

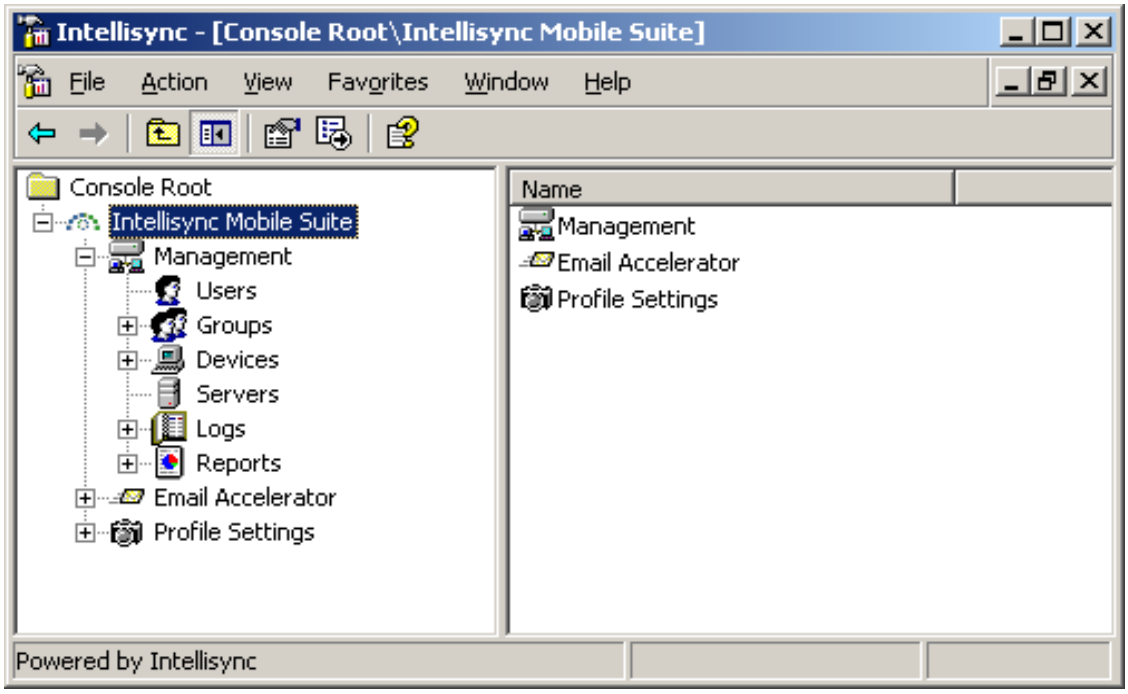
The Intellisync Mobile Gateway handles communications, connections, security, encryption, and user authentication. The gateway serves as the connection between the Intellisync Mobile Suite server and the outside world. gateway installs as part of the server installation, and the client software contains the components required to connect to the server through the gateway.

For additional information about the Intellisync Mobile Gateway, see "Using the Secure Gateway" in the *GroupWise Mobile Server 7 Installation Guide*.

1.2.3 Intellisync Mobile Suite Control

The Intellisync Mobile Suite control, which is part of the Microsoft* Management Console (MMC), helps you manage all GroupWise Mobile Server products and functions. The Intellisync Mobile Suite control is sometimes referred to as the Admin Console.

Figure 1-1 *Intellisync Mobile Suite Control*



From the Intellisync Mobile Suite control, you can complete many administrative tasks, including the following:

- Managing users and groups
- Managing settings and other variables specific to each Intellisync Mobile Suite product
- Managing profile settings
- Configuring connectivity settings

Because the Intellisync Mobile Suite control is a snap-in for MMC, you can integrate it with other MMC-compatible products. You can set up a custom console to include all your MMC-compatible products, giving you one central place to manage users for all products. Microsoft SQL Server is an example of MMC-compatible products that you can add and manage from the Intellisync Mobile Suite control.

The Intellisync Mobile Suite control installs as part of the server installation.

1.3 Intellisync Mobile Suite Products

The Intellisync Mobile Suite infrastructure contains the basic elements in your mobile solution, as well as Intellisync Wireless Email. In addition to this framework, three separate products are available for you to purchase to support your mobile workforce:

- Intellisync Data Sync
- Intellisync File Sync
- Intellisync Systems Management

These products snap into the GroupWise Mobile Server framework. You can use the products together or separately.

1.3.1 Intellisync Wireless Email

Intellisync Wireless Email offers centralized e-mail and personal information manager (PIM) synchronization capabilities for your users. With Intellisync Wireless Email, users can synchronize e-mail, contacts, memos, calendars, and to-do items among all their mobile devices, eliminating the need for duplicate data entry.

This same data is also accessible from any Internet-capable mobile phone and the Web browser on any computer connected to the Internet. Intellisync Wireless Email is included as part of the GroupWise Mobile Server product.

1.4 Other Components

GroupWise Mobile Server relies on other software components to function properly. Some of these key components include:

- Microsoft Management Console
- A server database

NOTE: For a complete list of installation requirements, see the *GroupWise Mobile Server 7 Installation Guide*.

1.4.1 Microsoft Management Console

The Microsoft Management Console (MMC) provides a structured user interface and environment for running management applications. The Intellisync Mobile Suite control is an MMC snap-in, and therefore requires MMC to run. MMC installs automatically as part of Windows 2000 and 2003 server.

1.4.2 Server Database

Intellisync Mobile Suite requires a database to operate. The database stores your users, groups, publications, logs, and other important data. Intellisync Mobile Suite works with the database to store and retrieve information as needed.

The server installation program includes and establishes a database for a production environment.

Using the Intellisync Mobile Suite Control

2

This section covers information for setting up and using the Intellisync Mobile Suite control.

2.1 Overview

With the Intellisync Mobile Suite control, you can complete many administrative tasks, including:

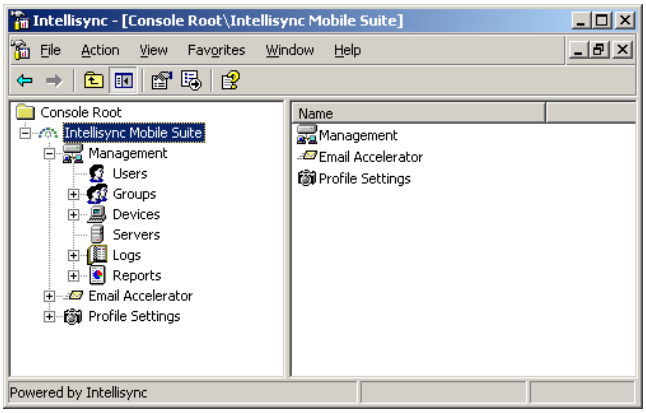
- Managing users and groups
- Managing settings and other variables
- Managing profile settings
- Configuring connectivity settings

Before using the Intellisync Mobile Suite control, you must configure database and authentication settings for GroupWise® Mobile Server. See the *GroupWise Mobile Server 7 Installation Guide*, or use the online help for instructions to set up the Intellisync Mobile Suite control.

2.2 Getting Started

The Intellisync Mobile Suite control is available on the server computer. Use the following instructions to start the Intellisync Mobile Suite control:

1 Click *Start* > *Programs* > *Intellisync Mobile Suite* > *Admin Console*. The Intellisync Mobile Suite control appears.



2 From the console tree, select *Intellisync Mobile Suite* to expand it. The Management and Profile Settings controls appear, in addition to Email Accelerator.

3 Select a control to view additional information.

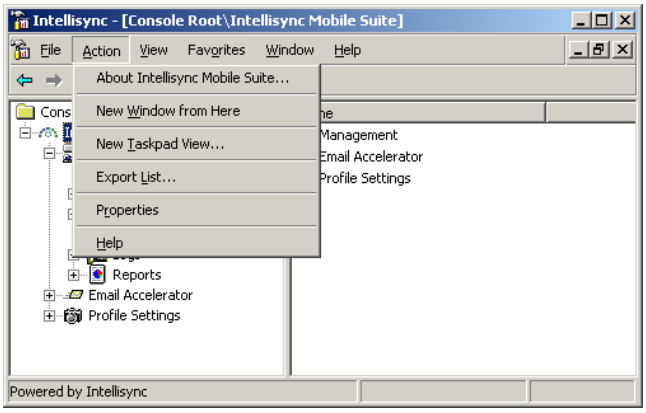
If you are using other MMC-compatible products to manage GroupWise Mobile Server, you can add those products to the console. Microsoft SQL Server, for example, is MMC-compatible. If you use these products, you can add them to the console, giving you one central place to manage functions related to GroupWise Mobile Server operations.

2.3 Actions and Properties

The Intellisync Mobile Suite control *Action* menu offers specific actions and settings that are important for configuring and maintaining your system.

1 From the console tree, select *Intellisync Mobile Suite*.

2 Click *Action*.



Because the Intellisync Mobile Suite control is an MMC snap-in, it uses many of the same operating conventions and terminology that you may be familiar with from using other MMC products. For example, the area on the left is called the console tree pane, and the area on the right is the details pane.

In addition to the *Action* menu items, which are available from most areas in MMC, there are two menu items specific to the Intellisync Mobile Suite control:

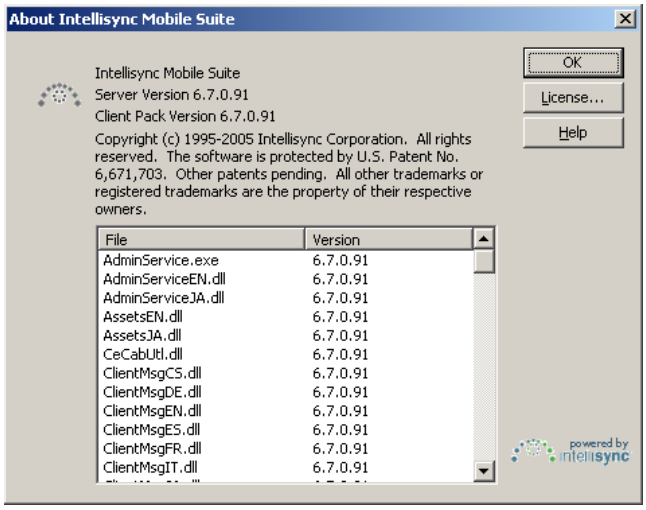
- Section 2.3.1, “About Intellisync Mobile Suite,” on page 16
- Section 2.3.2, “Intellisync Mobile Suite Properties,” on page 17

2.3.1 About Intellisync Mobile Suite

To view the About window:

1 From the console tree, select *Intellisync Mobile Suite*.

2 Click *Action* > *About Intellisync Mobile Suite*.

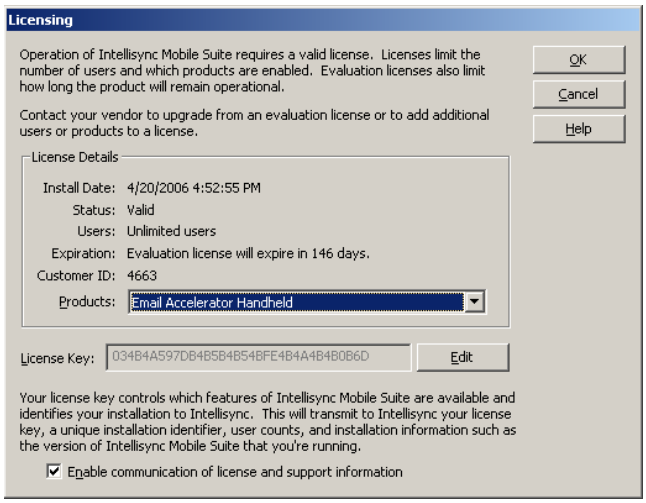


The About window shows copyright information and version numbers for the Intellisync software and your Intellisync Mobile Suite components.

Viewing Your License Information

1 From the console tree, select *Intellisync Mobile Suite*.

2 Click *Action* > *About Intellisync Mobile Suite*, then click *License*.



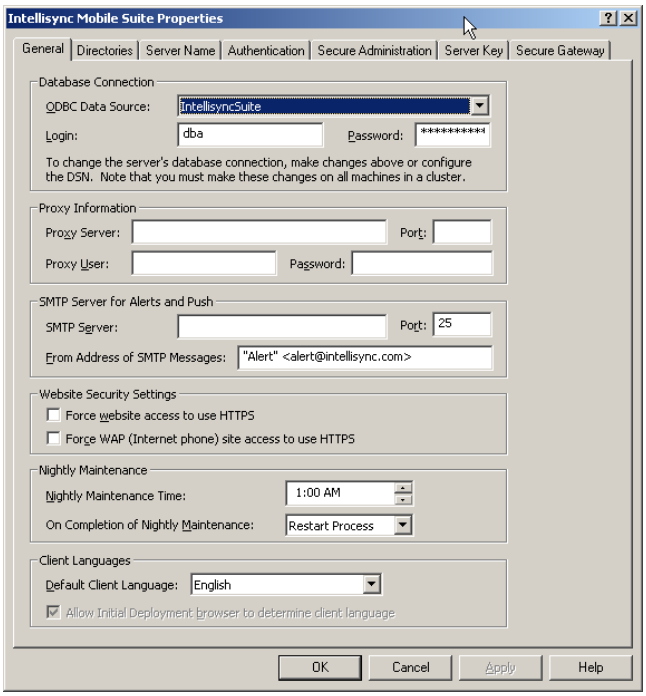
You license is based on the products and number of licenses you purchase. Evaluation licenses expire, but production licenses do not.

2.3.2 Intellisync Mobile Suite Properties

To view the Intellisync Mobile Suite properties:

1 From the console tree, select *Intellisync Mobile Suite*.

2 Click *Action* > *Properties*.

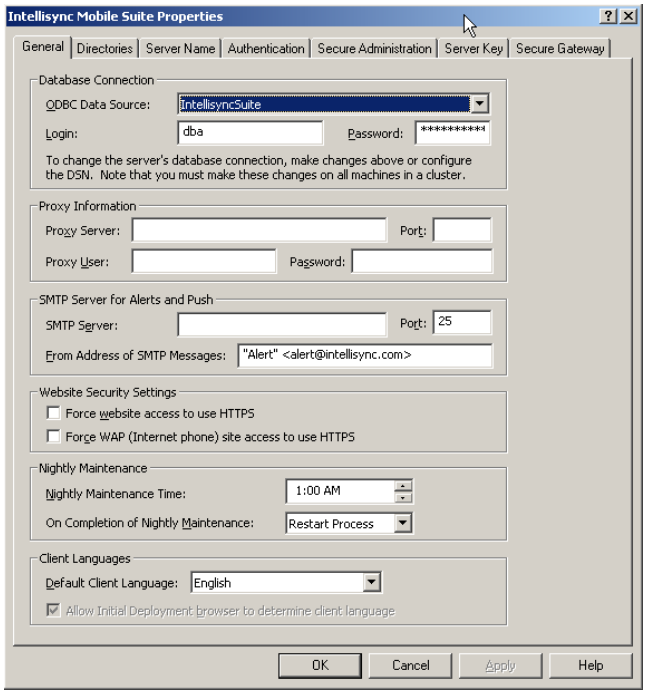


General Tab

The *General* tab allows you to set your database connection, proxy and SMTP information, Web site security, nightly maintenance schedule, and your default client language.

1 From the console tree, select *Intellisync Mobile Suite*.

2 Click *Action* > *Properties*.



Database Connection

The Intellisync Mobile Suite control stores information about users, groups, publications, and so forth, in a database. When you install the GroupWise Mobile Server software, the installation program creates an ODBC data source to connect to the database. The default data source name is *Intellisync Mobile Suite*.

- **ODBC Data Source:** Displays the name of the current ODBC data source. Do not change this value unless you created a new database.
- **Login:** Type the login name for the current ODBC data source.
- **Password:** Type a password for the current ODBC data source, or you can leave the password field empty.

NOTE: If you use the Windows Control Panel to modify the ODBC data source, or if you change the login name and password in the database, you must also modify the Database Connection properties in the Intellisync Mobile Suite control.

Proxy Information

Use the Proxy Information fields for Intellisync Mobile Suite servers that must use a proxy server for access to the Internet.

- **Proxy server:** Type the name of the computer acting as the proxy.
- **Port:** Type the port number for the proxy server.
- **Proxy User:** Type the user ID for the proxy server. (Complete this field only if you are using an authenticated proxy.)

- **Proxy Password:** Type the password for the proxy server user ID. (Complete this field only if you are using an authenticated proxy.)

SMTP Server for Alerts and Push

If you plan to use Alerts or Push, you must specify the SMTP server information.

- **SMTP Server:** Type the name of the SMTP server.
- **Port:** Type the port number of the SMTP server.
- **From address of SMTP messages:** Type the text you want to appear in the *From* address field of your SMTP messages. This entry is only for messages that do not have a *From* address, such as alerts generated by GroupWise Mobile Server.

Website Security Settings

For additional security, you can force Web access, WAP access, or both to use HTTPS, which is an extension to the HTTP protocol that supports sending data securely over the World Wide Web. This redirects users to a secure URL when necessary.

- **Force website access to use HTTPS:** Forces all Web site access to use HTTPS as the communications protocol.
- **Force WAP Access to use HTTPS:** Forces all WAP access to use HTTPS as the communications protocol.

Nightly Maintenance

Use this section to change settings for nightly maintenance.

- **Nightly Maintenance Time:** You can configure the Intellisync Mobile Suite server to run nightly maintenance services at a preset time. The maintenance service completes by restarting the server. The default time for running the services is 3:00 a.m.
- **On Completion of Nightly Maintenance:** Use this setting to control whether the server restarts at the end of the maintenance process. Novell strongly recommends that you select the default setting, *Restart Process*.

Client Languages

Use this section to set the default client language.

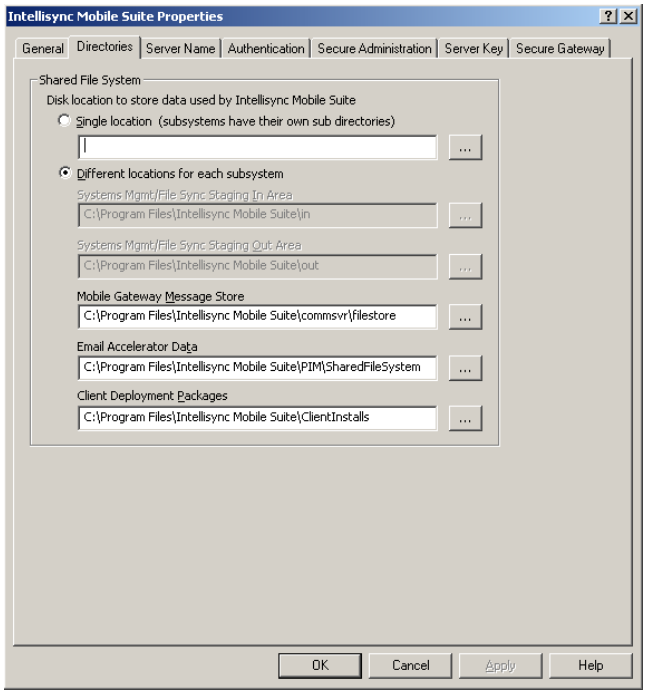
- **Default Client Language:** Select the default client language: English, German, French, Italian, Czech, Portuguese, or Spanish.
- **Allow Initial Deployment browser to determine client language:** Use this setting to allow the browser to determine the client language.

Directories Tab

Use the *Directories* tab to specify the disk location to store data used by GroupWise Mobile Server.

1. From the console tree, select *Intellisync Mobile Suite*.

2 Click *Action* > *Properties*, then click the *Directories* tab.



Single Location

Select this location to have all data stored in a single directory with each subsystem having its own subdirectory.

Type the parent directory location in the *Single Location* field or browse to and select the location.

Different Location

Select this location if you need to have a different location to store data for each subsystem.

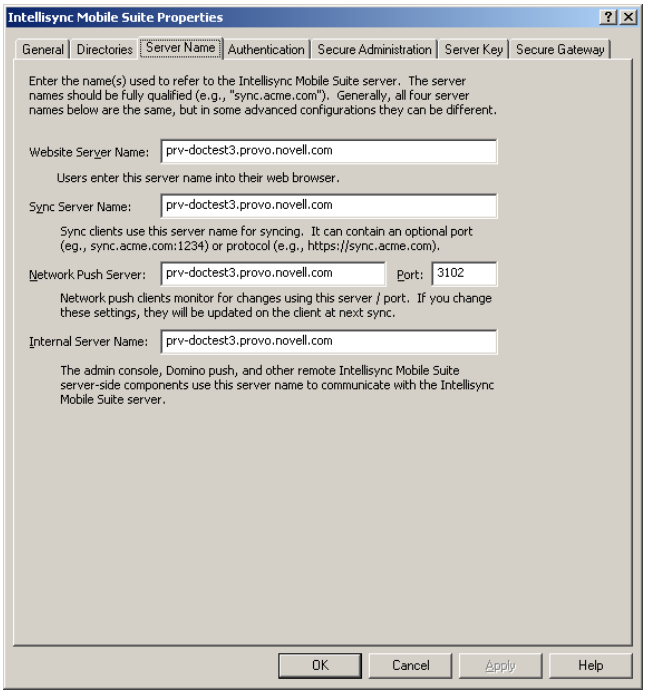
- **Systems Mgmt/File Sync Staging In Area:** This option is dimmed greyed out because system management and file sync are not part of GroupWise Mobile Server.
- **Systems Mgmt/File Sync Staging Out Area:** This option is dimmed greyed out because system management and file sync are not part of GroupWise Mobile Server.
- **Mobile Gateway Message Store:** Specify the location to store the Mobile Gateway message store data.
- **Email Accelerator Data:** Specify the location to store the Email Accelerator data.
- **Client Deployment Packages:** Specify the location to store the client deployment packages.

Server Name Tab

Use the *Server Name* tab to specify the server names that are part of your GroupWise Mobile Server system. Use fully qualified server names. Usually, all server names are the same, but in some advanced configurations, the server names might be different from each other. The Web site and sync server names might point to a reverse proxy, for example, at least for communications coming

from outside the firewall. The internal server name is used only inside the firewall and should never go through a reverse proxy because it is used for non-HTTP traffic.

1. From the console tree, select *Intellisync Mobile Suite*.
2. Click *Action* > *Properties*, then click the *Server Name* tab.



Use the following information to set options related to server names.

- **Website Server Name:** The server name that users type into their browser to access the Web site.
- **Sync Server Name:** The server name used for synchronization. This name is stored on client devices.
- **Network Push Server:** The name of the server that handles network or IP push.
- **Port:** The port number for the network push server.
- **Internal Server Name:** The server name that the Intellisync Mobile Suite control (local or remote), Domino* push, and other internal components use to communicate with the Intellisync server.

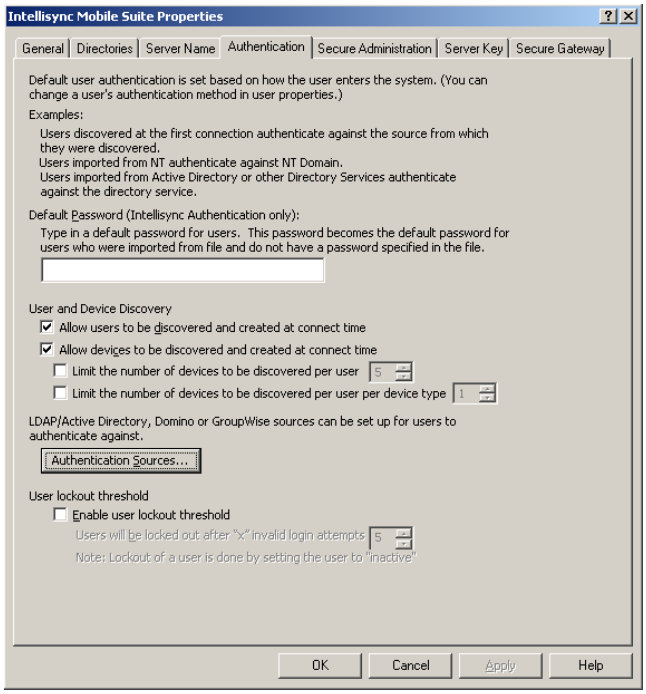
Authentication Tab

By default, GroupWise Mobile Server authenticates users by their GroupWise user ID and password.

To view and edit the current authentication settings:

1. From the console tree, select *Intellisync Mobile Suite*.

2 Click *Action* > *Properties*, then click the *Authentication* tab.



Use the following information to set options related to authentication.

- **Default Password (Intellisync Authentication only):** Use this field to supply a password for imported users who do not have a password specified in the import file. (This field applies for Intellisync authentication only.)
- **Allow users to be discovered and created at connect time:** User discovery is a feature whereby users are recognized and have user accounts created for them when they connect to the server for the first time. Select this option to enable this feature.
- **Allow devices to be discovered and created at connect time:** Select this option to allow the system to discover, authenticate, and add devices that are not in the system. By not selecting this option, you can authenticate only devices that already exist in the system.
- **Authentication Sources:** Click Authentication Sources if you want to set up additional authentication sources. GroupWise and Intellisync authentication are available as soon as GroupWise Mobile Server software installation finishes.

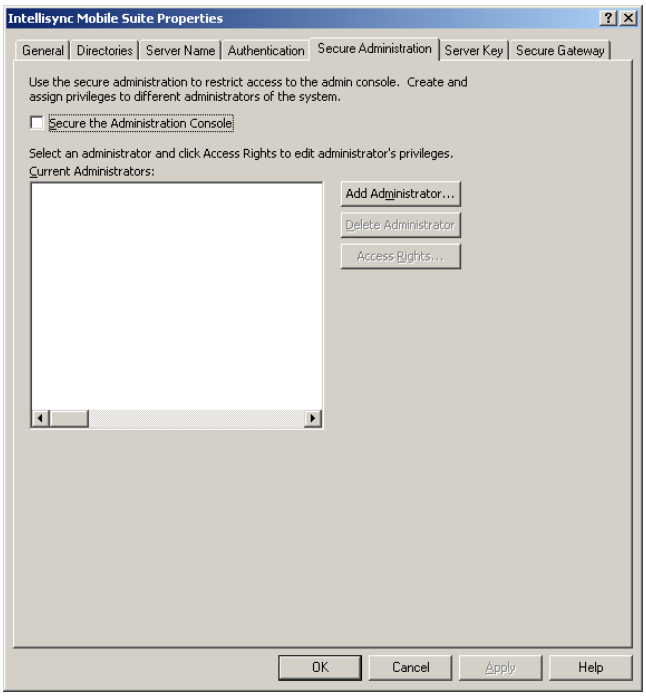
For additional information and guidelines for setting up authentication, see Chapter 6, "Authenticating Users," on page 77.

Secure Administration Tab

Use the *Secure Administration* tab to set permissions and restrict access to the Intellisync Mobile Suite control.

1 From the console tree, *select Intellisync Mobile Suite*.

2 Click *Action* > *Properties*, then click the *Secure Administration* tab.



Use the following information to set access options for the Intellisync Mobile Suite control.

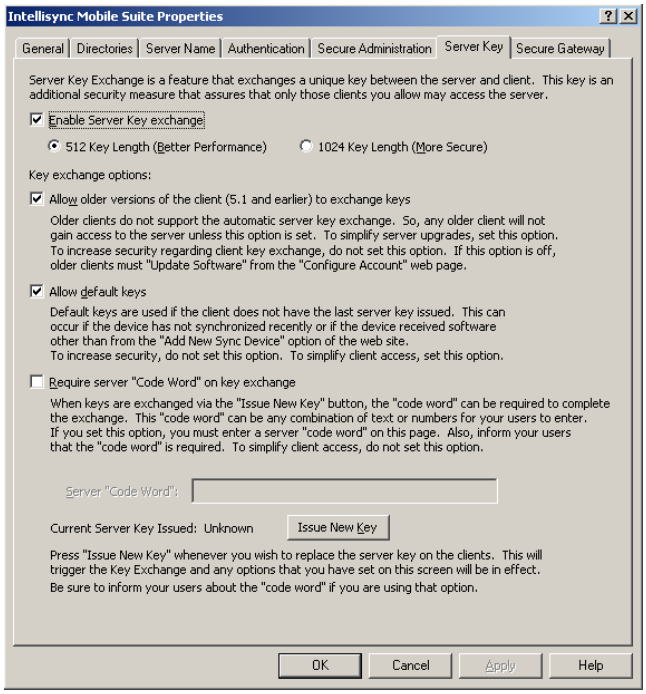
- **Secure the Administration Console:** Select this option to restrict access to the Intellisync Mobile Suite control. Only users you specify as administrators can access the Intellisync Mobile Suite control when you enable this option.
- **Add Administrator:** Click *Add Administrator* to create control administrators and grant permission to additional users.

Server Key Tab

Use the *Server Key* tab to enable Server Key Exchange, a security feature that exchanges a unique key between the server and the clients.

1 From the console tree, select *Intellisync Mobile Suite*.

2 Click *Action* > *Properties*, then click the *Server Key* tab.



Use the following information to enable Server Key Exchange, a security feature that exchanges a unique key between the server and the clients.

- **Enable Server Key exchange:** Select this feature to ensure that only clients you specify can access the server. Select the key length you want to use.
  - 512-key length (Better Performance)
  - 1024-key length (More Secure)

  Client devices cannot connect if you disable key exchange and issue a new key.

Use the following information to set the key exchange options.

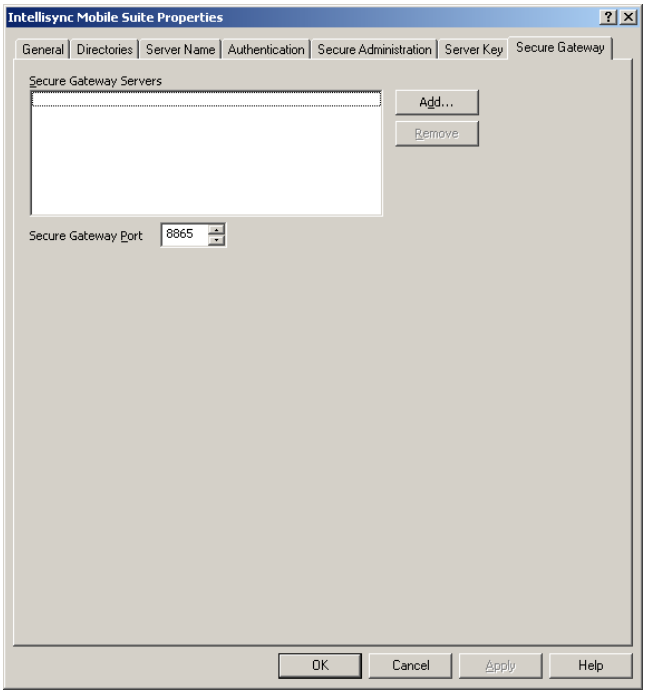
- **Allow older versions of the client to exchange keys:** Select this option to allow older versions of the client to exchange keys with the server. If you diable this option, only clients running current software can participate in key exchange. That is, devices running older versions of client software cannot connect.
- **Allow default keys:** Although this setting slightly decreases security, it simplifies access for clients. With this option set, Intellisync Mobile Suite uses default keys if the client does not have the most recent server key. This can happen if a device does not synchronize often or if the device received client software in a manner other than the Add New Sync Device page of the Web site. To increase security, do not set this option.
- **Require server "Code Word" on key exchange:** You can add a special code that users must enter to complete the key exchange.
  - **Server Code Word:** The code word can be any combination of text or numbers. If you add a code word, inform your users of the code to ensure successful synchronizations.

- **Issue New Key:** Click *Issue New Key* to replace the server key for the clients. This action triggers the Key Exchange process the next time the client connects, and implements any options you set on this panel.

Secure Gateway Tab

Use the *Secure Gateway* tab to add, remove, and change the port of any Secure Gateway servers. The server intercepts the HTTP requests from mobile devices and then routes the requests through TCP/IP to a specific port that you define. The process encrypts all traffic end-to-end.

1. From the console tree, select *Intellisync Mobile Suite*.
2. Click *Action* > *Properties*, then click the *Secure Gateway* tab.



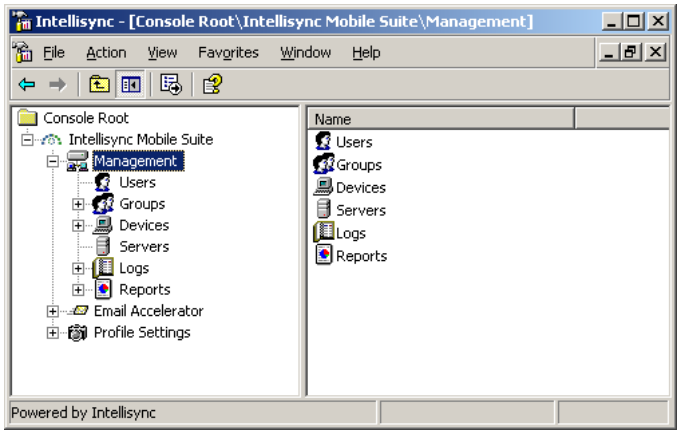
Use the following information to set Secure Gateway servers for the Intellisync Mobile Suite control.

- **Add Administrator:** Click *Add Administrator* to create control administrators and grant permission to additional users.
- **Secure Gateway Port:** Specify the port number to use for GroupWise Mobile Server to communicate with the Secure Gateway server.

2.4 Management

The Management control is a standard part of the Intellisync Mobile Suite control, and is always present regardless of the individual Intellisync Mobile Suite products installed on your server.

Figure 2-1 *Intellisync Mobile Suite Control: Management*



Use the Management control to complete the following tasks:

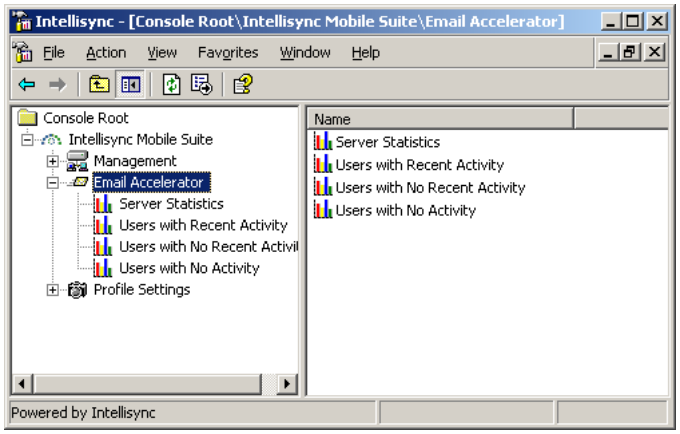
- Manage users and groups
- View a list of devices
- View logs
- Configure server clusters
- Use reporting functions
- Set up alerts (for Systems Management or File Sync only)

Most dialog boxes have *Help* buttons, or you can access context-sensitive online help by pressing F1. For more information on the Management control, see Chapter 3, “Using Management Tools,” on page 29.

2.5 Email Accelerator

Email Accelerator has its own control in the Intellisync Mobile Suite control. The license key you entered at installation allows the use of the Email Accelerator.

Figure 2-2 *Intellisync Mobile Suite Control: Email Accelerator*

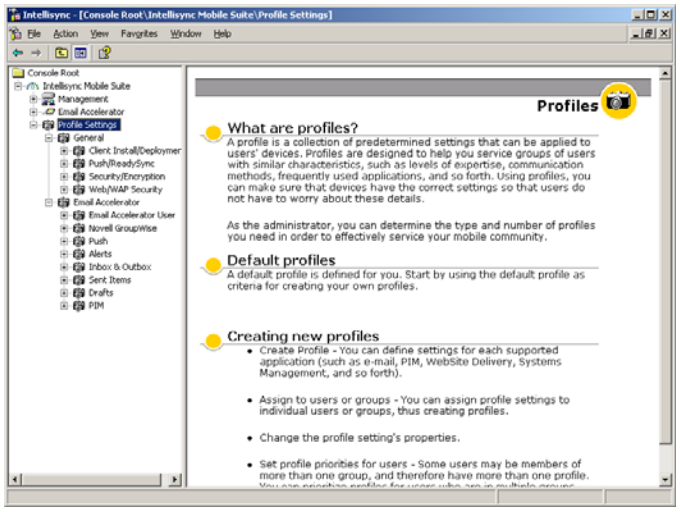


Email Accelerator provides you with statistics about your server and about user activity.

2.6 Profile Settings

GroupWise Mobile Server provides Profile Settings as a standard part of the Intellisync Mobile Suite control. You can use Profile Settings to create, modify, and manage user profiles.

Figure 2-3 *Intellisync Mobile Suite Control: Profile Settings*



For more information on Profile Settings, see Chapter 4, “Profile Settings,” on page 45. In addition to this resource, most dialog boxes have *Help* buttons, or you can access context-sensitive help by pressing F1.

Using Management Tools

3

The Management control gives you easy access to functions that apply to the entire Intellisync Mobile Suite application, such as managing users and groups, monitors, logs, and reports. This section covers the Management control and its functions.

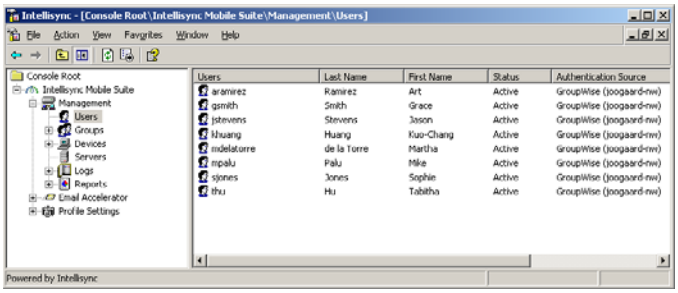
3.1 Overview

The Management control gives you easy access to functions that apply to the entire suite, such as managing users and groups, using the Real-Time Monitor, and using logs and reports. When you expand the Intellisync Mobile Suite control, the Management control is available at the top of the list.

3.2 Working With Users

All Intellisync Mobile Suite products share a common list of users and groups. Select the Users control to view a list of all users in the details pane.

Figure 3-1 *Intellisync Mobile Suite control: Users*



Each person who sends and receives information must have a unique user account. When a user connects, the server needs the user ID to identify the user and determine which information the user can access or update.

This section contains the following information:

- Section 3.2.4, “Assigning or Editing User Profiles,” on page 34
- Section 3.2.5, “Deleting a User,” on page 35
- Section 3.2.6, “Using the Properties Dialog Box to Manage User Information,” on page 35

This guide provides a general overview of each task. You can click *Help* for step-by-step instructions for completing the tasks.

3.2.1 Adding a New User

Depending on how your system is set up, you can add new users to your system through the Intellisync Mobile Suite control.

The method you are using to authenticate users determines the way in which you add new users. For example, if you are using GroupWise® authentication, new users are added automatically when connecting for the first time (after the server is set up and configured properly). If you are using Intellisync authentication, then add or import new users using the Intellisync Mobile Suite control.

Adding Users Through Auto Discovery

If you are using GroupWise authentication, there is no need to manually add users through the Intellisync Mobile Suite control. The feature that enables the server to recognize a new user and create a record upon the first connection is called auto discovery. Accounts created through auto discovery appear in the list of users along with all other user accounts.

Auto discovery is enabled by default. To change this setting:

1. From the console tree, select *Intellisync Mobile Suite*.
2. Click *Action* > *Properties*, then click the *Authentication* tab.
3. Deselect *Allow users to be discovered and created at connect time*.

For more information about GroupWise Authentication, see Chapter 6, “Authenticating Users,” on page 77.

Adding Users Through the Intellisync Mobile Suite Control

To add users manually using the Intellisync Mobile Suite control, complete the following steps.

1. From the console tree, click *Management* > *Users*.
2. Click *Action* > *Create User*.
3. Add a unique user ID, password, and optional information as needed.

For more information on completing this task, click *Help*.

The Intellisync Mobile Suite control creates an account for the new user and places an entry in the details pane. You must create the user account before the user connects for the first time unless you are using auto discovery.

Users you add manually through the Intellisync Mobile Suite control are set up for Intellisync Authentication by default. You can view and change the authentication method for a user on the *General* tab of the user’s properties.

NOTE: If you are using the auto discovery option through GroupWise authentication, Intellisync Mobile Suite adds new users when they connect for the first time. If you are using GroupWise authentication, do not manually add users through the Intellisync Mobile Suite control.

3.2.2 Importing Users

To save time, you can import and synchronize users rather than creating an account for each user manually or through auto discovery. You can import users from a text file.

Importing Users From a Text File

To create user IDs for a large number of users, you can prepare a text file containing the user IDs and import the users from the file.

1. Prepare a text file containing user information.

   The text file should have one user ID per line.
2. In the console tree, click *Management* > *Users*.
3. Click *Action* > *Import Users from File*.
4. Locate the text file and click *Open*.
5. Use the Properties dialog box to enter additional information and a password for each new user.

For more information on completing this task, click *Help*.

GroupWise Mobile Server imports user information and creates the user IDs. The imported users are not assigned to a device type. When a user connects with a specific device, that device type is registered for the user.

Adding users this way allows you to use Intellisync Authentication by default. You can view and change the authentication method for a user on the *General* tab of the user's properties.

NOTE: If you specify a default password in the *Authentication* tab of the Intellisync Mobile Suite control properties, this is the password for the new users unless you define a different one in the text file.

Using Tokens with Text Files

If you want to import additional user information, you can use tokens separated by tabs to include various properties for each user. The following tokens are available to use in your text files:

- $password=<password for this user>
- $description=<descriptive text about this user>
- $firstname=<user's first name>
- $lastname=<user's last name>
- $addtogroup=<group name to which the user should be a member>
- $active=<f0 or 1, where 0 indicates inactive and 1 indicates active>
- $alertdevice=<phone, pager, or e-mail>
- $alertphonenumber=<phone number of the alert device>

- $alertemailaddr=<e-mail address to receive alerts>
- $alertcarrier=<Verizon, Sprint, AT&T Wireless, Alltel, T-Mobile, or Cingular>
- $emailAddress=<user's e-mail address>
- $language=<two-character country code. Valid entries are EN (English), FR (French), ES (Spanish), DE (German), JA (Japanese)>
- $timezone=<time zone specification>

  For a list of possible time zones, see "Time Zone Reference" on page 32.
- $authtype=<GroupWise identification source ID>

  If you select to use $authtype, you must use the GroupWise identification source ID. You must get the GroupWise identification source ID from the GroupWise Mobile Server database. For instructions on how to do this, contact Intellisync support.
- $sync=<1. This triggers a sync after configuration>
- $serverdevice=<GroupWise,<ID> where the ID is the XML translator identifier; for example, 100.>

  If $serverdevice is specified, then any parameters following $serverdevice will be passed to the server connection until the end of line or another $serverdevice is specified.
- If $serverdevice= GroupWise:
  - $GWServer=<GroupWise server>
  - $GWPort=<GroupWise port number>
  - $GWUuid=<GroupWise user unique ID>
  - $GWDisplayName=<GroupWise user full name>
  - $GWUser=<GroupWise user name>
  - $GWPassword=<GroupWise user password. This parameter is not required for trusted application access>
- If $serverdevice = XML,<ID>:
  - $XMLUser=<followed by the XML user ID>
  - $XMLPassword=<XML password for the user>
  - $XMLCompany=<company name on the server>

To ensure a successful import, review the tokens for accuracy and separate each with a tab.

Time Zone Reference

"Abu Dhabi, Muscat"
"Adelaide"
"Alaska"
"Almaty, Novosibirsk"
"Amsterdam, Berlin, Rome, Vienna"
"Arizona"
"Astana, Dhaka"
"Athens, Istanbul, Minsk"
"Atlantic Time (Canada)"
"Auckland, Wellington"

“Azores”
“Baghdad”
“Baku, Tbilisi, Yerevan”
“Bangkok, Hanoi, Jakarta”
“Beijing, Chongqing, Hong Kong, Urumqi”
“Belgrade, Bratislava, Budapest, Prague”
“Bogota, Lima, Quito”
“Brisbane”
“Brussels, Copenhagen, Madrid, Paris”
“Bucharest”
“Buenos Aires, Georgetown”
“Cairo”
“Calcutta, Chennai, Mumbai, New Dehli”
“Canberra, Melbourne, Sydney”
“Cape Verde Is.”
“Caracas, La Paz”
“Casablanca, Monrovia”
“Central America”
“Central Time (US & Canada)”
“Chihuahua, La Paz, Mazatlan”
“Darwin”
“Dublin, Edinburgh, Lisbon, London”
“Eastern Time (US & Canada)”
“Ekaterinburg”
“Fiji, Marshall Is.”
“Greenland”
“Guam, Port Moresby”
“Harare, Pretoria”
“Hawaii”
“Helsinki, Tallinn”
“Hobart”
“Indiana (East)”
“International Date Line West”
“Irkutsk, Ulaan Bataar”
“Islamabad, Karachi, Tashkent”
“Jerusalem”
“Kabul”
“Kathmandu”
“Krasnoyarsk”
“Kuala Lumpur, Singapore”
“Kuwait, Riyadh”
“Mexico City”
“Mid-Atlantic”
“Midway Island, Samoa”

“Moscow, St. Petersburg, Volgograd”
“Mountain Time (US & Canada)”
“Nairobi”
“Newfoundland”
“Noronha”
“Nuku'alofa”
“Osaka, Sapporo, Tokyo”
“Pacific Time (US & Canada); Tijuana”
“Perth”
“Rangoon”
“Santiago”
“Sao Paulo”
“Sarajevo, Sofija, Warsaw, Zagreb”
“Saskatchewan”
“Seoul”
“Solomon Is.”
“Sri Jayawardenepura”
“Taipei”
“Tehran”
“Vladivostok”
“West Central Africa”
“Yakutsk”

3.2.3 Changing a User’s Group Memberships

After you create user and group accounts, you can add or remove a user as needed. All new users are automatically assigned to the New Users and All Users groups.

To add or modify group memberships for a user:

1. From the console tree, click *Management* > *Users*.
2. In the details pane, select the user ID whose group memberships you want to change.
3. Click *Action* > *Add User to Group*.
4. Click *Add* or *Remove* to change the groups to which the user belongs.
5. Click *OK*.

3.2.4 Assigning or Editing User Profiles

Generally, profiles are assigned to groups; however, you can assign profiles to individual users. These user profiles take precedence over the profile for the group to which the user belongs.

In the console tree, the *Edit Profiles* option is available if the user already has a profile. If the user does not have an assigned profile, the *Assign Profiles* option appears. Users with no assigned profile, either individually or through groups, automatically receive a default profile.

1. From the console tree, click *Management* > *Users*.
2. In the details pane, select the user ID to which you want to assign or edit profiles.

3 Click Action > *Assign Profiles* or *Edit Profiles*.

4 Use the tabs and lists to select profiles for each of the user's devices.

5 Click *OK*.

3.2.5 Deleting a User

You can delete user accounts that you no longer need. When you delete a user, GroupWise Mobile Server deletes the Mobile Suite information for the user and forwards the delete request onto all of your installed Mobile Suite products. The products ensure that data files and database entries specific to that user are removed from the system.

1 From the console tree, click *Management* > *Users*.

2 In the details pane, select the user ID you want to delete.

3 Click *Action* > *Delete*.

4 Click Yes.

3.2.6 Using the Properties Dialog Box to Manage User Information

After you create a user account, you can use the Properties dialog box to add or change user information. This gives you easy access to the same user information you can access using menu options. To make several changes for one user, you might find that using the Properties dialog box is faster than using the menus.

From the Properties dialog box, you can:

- Modify or add information about a user
- Assign or remove a user from a group
- Add or remove publications subscriptions

To use the Properties dialog box:

1 From the console tree, click *Management* > *Users*.

2 In the details pane, select the user ID.

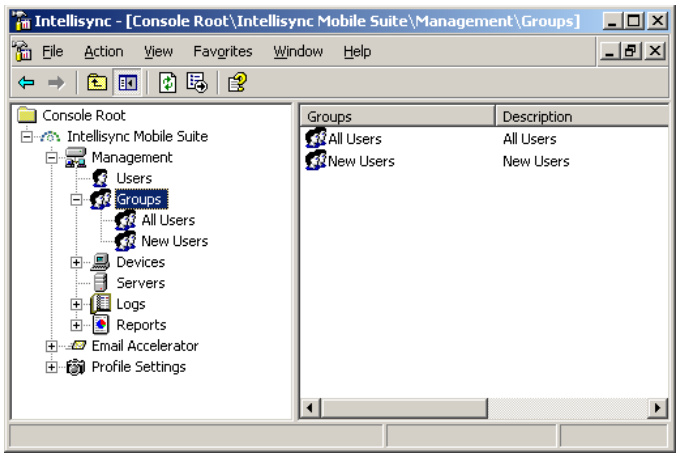
3 Click *Action* > *Properties*.

3.3 Working with Groups

After you create users, you can create groups and assign users to the groups. You can create groups of users who share similar characteristics. For example, you can create groups based on department, job function, geographical area, or user's computer type. Assigning publications to groups is often more efficient than assigning publications to individual users.

Select the Groups control to view a list of all groups in the details pane.

Figure 3-2 *Intellisync Mobile Suite control: Groups*



This section contains the following information for working with groups:

- Section 3.3.1, “Creating a Group,” on page 36
- Section 3.3.2, “Importing and Synchronizing Groups,” on page 36
- Section 3.3.3, “Adding or Removing Users From a Group,” on page 37
- Section 3.3.4, “Assigning or Editing Group Profiles,” on page 37
- Section 3.3.5, “Deleting a group,” on page 37
- Section 3.3.6, “Using the Properties Dialog Box to Manage Group Information,” on page 38

3.3.1 Creating a Group

1. From the console tree, click *Management*, > *Groups*.
2. Click *Action* > *Create Group*.
3. Type a group name and a description.
4. Click *OK*.

The Intellisync Mobile Suite control creates the group and places an entry in the details pane. For more information about creating groups, click *Help*.

NOTE: You cannot remove a user from the All Users group.

3.3.2 Importing and Synchronizing Groups

To save time and effort, you can import and synchronize groups rather than creating groups and adding each user individually. You can import and synchronize groups from the following sources:

- Windows NT or Windows 2000 groups
- Active Directory/LDAP groups

Windows NT or Windows 2000 Groups

If the groups you want to add are already registered Windows NT* or Windows 2000 groups, you can import and synchronize these groups into the Intellisync Mobile Suite control. This eliminates the need to create and manage groups in two areas.

1. From the console tree, click *Management* > *Groups*.
2. Click *Action* > *Import/Synchronize Groups* > *NT Domain Groups*.
3. Follow the prompts in the Import/Synchronize Groups Wizard.

Active Directory LDAP Groups

To import and synchronize groups from an Active Directory LDAP server into the Intellisync Mobile Suite control:

1. From the console tree, click *Management* > *Groups*.
2. Click *Action* > *Import/Synchronize Groups* > *Active Directory/LDAP Groups*.
3. Follow the prompts in the Import/Synchronize Groups Wizard.

3.3.3 Adding or Removing Users From a Group

1. From the console tree, click *Management* > *Groups*.
2. In the details pane, select the name of the group.
3. Click *Action* > *Add User to Group*.
4. Click *Add* or *Remove* to add or remove user membership in this group.

NOTE: You cannot remove a user from the All Users group.

3.3.4 Assigning or Editing Group Profiles

You can assign profiles to groups, which is often more efficient than assigning profiles to individual users one at a time.

In the console tree, the *Edit Profiles* option is available if the group already has a profile. If the group does not have a profile, the *Assign Profiles* option appears. Groups with no assigned profile automatically receive a default profile.

To assign or edit profiles for a group:

1. From the console tree, click *Management* > *Groups*.
2. In the details pane, select the name of the group to which you want to assign or edit a profile.
3. Click *Action* > *Assign Profiles* or *Edit Profiles*.
4. Use the tabs and lists to select profiles for the group for each member's device.

3.3.5 Deleting a group

To delete groups you no longer need:

1. From the console tree, click *Management* > *Groups*.

2 In the details pane, select the name of the group you want to delete.

3 Click *Action* > *Delete*.

When you delete a group, the individual users who are members of the group remain active in the system.

NOTE: You cannot delete the New Users group or the All Users group.

3.3.6 Using the Properties Dialog Box to Manage Group Information

After creating a group, you can use the Properties dialog box to add or change information about the group. This gives you easy access to the same group information you can access using menu options. To make several changes for one group, you might find that using the Properties dialog box is faster than using the menus.

From the Properties dialog box, you can:

- Modify information about a group
- Assign or remove users from a group
- Add or remove publication subscriptions for a group

To change properties for a group, complete the following steps.

1 From the console tree, click *Management* > *Groups*.

2 In the details pane, select the name of the group.

3 Click *Action* > *Properties*.

4 Change the values as necessary.

For more information about using the Properties dialog box, click *Help*.

3.4 Devices

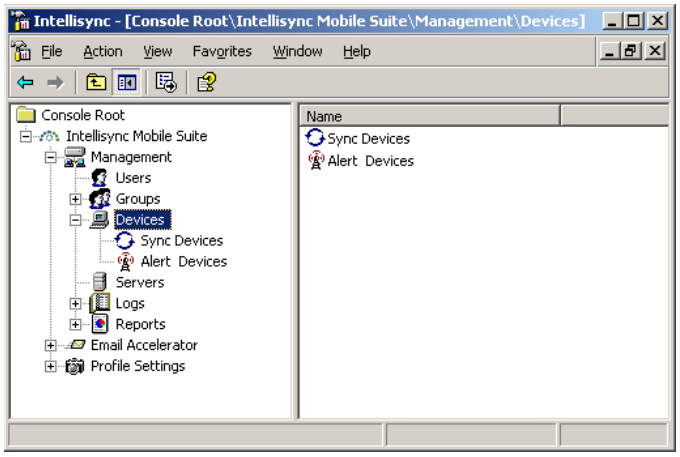
Use the Devices control to view the status of devices in service. Devices are separated by the following device types might appear in more than one list:

- Sync Devices
- Alert Devices

To view the status of a device, complete the following steps.

1 From the console tree, click *Management* > *Devices*.

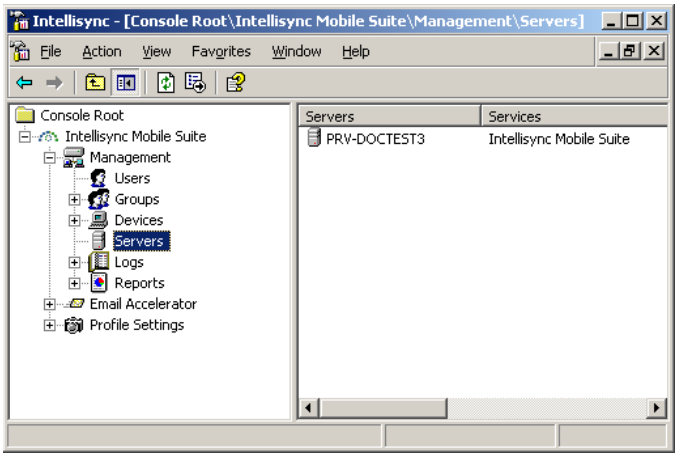
2 Select a device type. The status appears in the details pane.



3.5 Servers

The Servers control is for viewing the configuration and status of GroupWise Mobile Server components on a specific server, and for configuring servers in a cluster.

Figure 3-3 *Intellisync Mobile Suite Control: Server*



WARNING: You must contact an Intellisync support engineer for assistance before making changes to the status or the configuration of Intellisync Mobile Suite components on a server. Failure to do so might cause irreparable damage to your system.

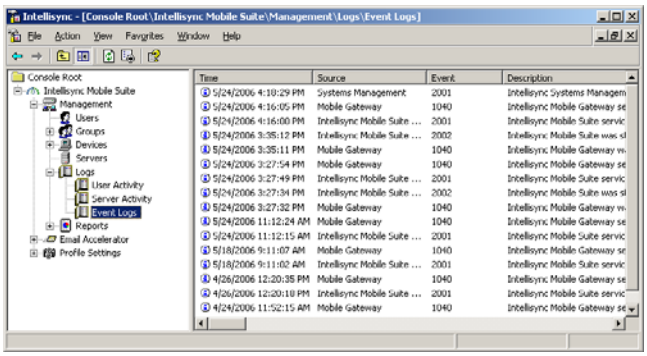
For more information on configuring clusters, click *Help*.

3.6 Logs

Logs allow you to view historical information about your system. For user and server activity logs, you can select the date and time ranges you want to view.

1 From the console tree, click *Management* > *Logs*.

2 Select the type of log you want to view. The log information appears in the details pane.



3.6.1 Log Levels

You can select the level of log entries you want to view. Select from the following levels.

- Minimum. Shows only warnings and error messages.
- Standard. Shows general information messages and minor warnings, in addition to serious warnings and error messages.
- Verbose. Shows all log messages.

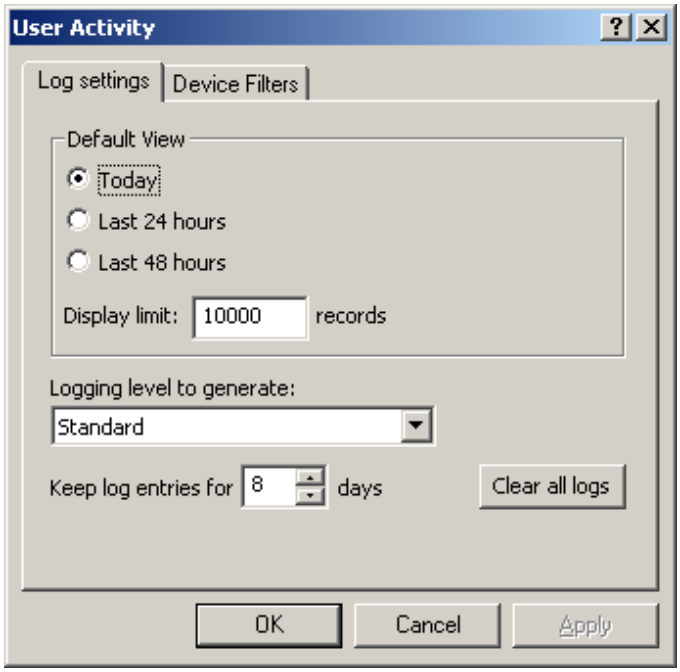
NOTE: For the User Activity summary, you can view only the message detail level you elected to capture from the client users (or a less selective level). For example, if client logging is set to Standard, Verbose messages are not captured.

3.6.2 Changing Log Defaults and Settings

The User Activity and Server Activity logs include a Settings button to change the default view or to set how long you want to keep log entries in the system.

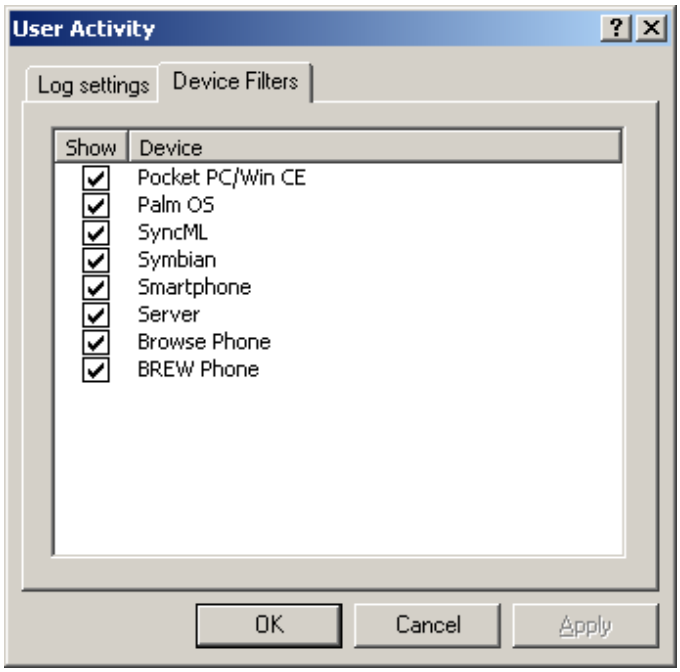
The following figure shows the Log settings panel on the User Activity Settings dialog box.

Figure 3-4 *Sample Log Settings*



The following figure shows the Device Filters panel on the User Activity Settings dialog box.

Figure 3-5 *Sample Device Filter Settings*



The values you can set are different depending on which log you are viewing. For more information on log settings, refer to the online help.

3.6.3 Available logs

The following logs are available:

- **User Activity:** Displays connection information on a user-by-user basis. You can select the user, start date, end date, and time.
- **Server Activity:** Displays server activity for the start date, end date, and time you specify. Unlike the Event Logs, which display log entries for the computer you choose, the Server Summary displays log entries for the entire system.
- **Event Logs:** Mirrors the contents of the Windows NT Event Log for the Intellisync Mobile Suite server you select. You can see start and stop times for services, as well as critical error information.

For more information on logs, refer to the online help.

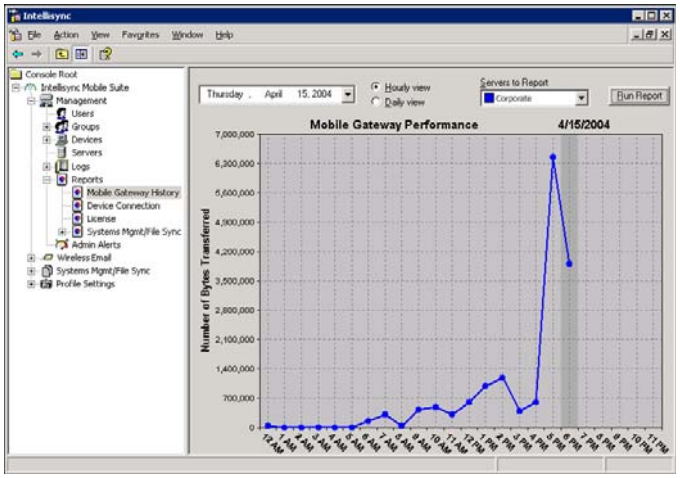
3.6.4 Log Files

Log files are stored in the `Intellisync\Log` directory (or the `Synchrologic\Log` directory), depending your system setup. These logs contain the same information you can view from the Intellisync Mobile Suite control. If you are having problems with your system, an Intellisync support engineer might ask you to send these files for analysis.

3.7 Reports

You can use reports to see information about your system. After you provide the appropriate input data at the top of the page, click *Run Report* to generate an on-screen report.

Figure 3-6 *Sample Report (Mobile Gateway History)*



For more information on using reports, refer to the online help.

3.7.1 Available reports

You can run the following reports:

- “Mobile Gateway History” on page 43

Mobile Gateway History

The Mobile Gateway History report provides an indication of the load on the Mobile Gateway. The report shows the number of bytes transferred for the date range you specify. Daily and hourly views are available.

Device Connection

The Device Connection report provides an overview of which devices are connecting and when. Daily and hourly views are available.

License

The License report shows the number of licenses you purchased for each product and the number of licenses in use.

Profile Settings

4

This section contains the information you need to effectively use Profile Settings in the Intellisync Mobile Suite control.

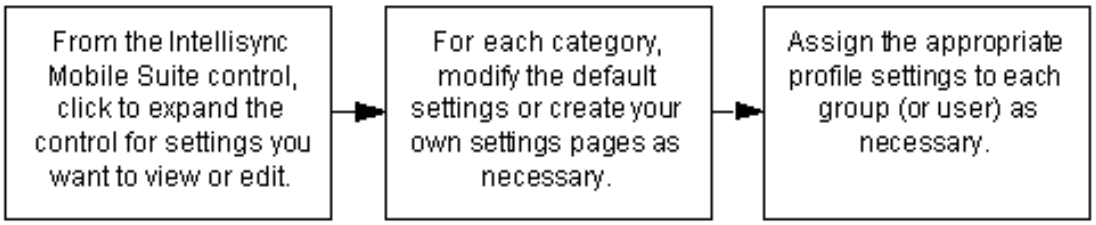
4.1 Overview

Profiles are collections of general and application settings that define how GroupWise Mobile Server is set up for a specific user or group. With Profiles, you can define settings for options such as ReadySync, security/encryption, Web/WAP security, e-mail, calendars, contacts, file delivery, and so forth. You can then assign these settings to appropriate groups or users.

For example, if a group of users synchronizes highly confidential information on a regular basis, you can assign a profile to this group with options and settings that reflect these characteristics. You can set intervals for synchronization through ReadySync and you can add security/encryption settings. Then you can assign the ReadySync and the security/encryption settings to the group, forming a profile.

From the Intellisync Mobile Suite control, you can create profile settings, access profile properties to review or change, assign profiles to users and groups, prioritize profile assignments, and delete profile settings.

Figure 4-1 *Process overview: Working with Profile Settings*



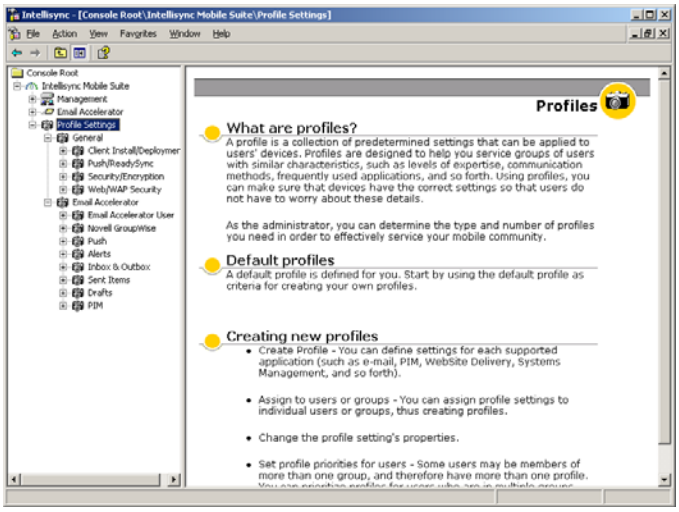
NOTE: You do not need to make changes to profile settings for users to connect and synchronize with GroupWise Mobile Server. The default profile settings automatically apply to each user and group. You might want to see how your system operates with the default settings before making any changes.

4.1.1 Understanding Profile Settings

Profile Settings help you manage groups of users with similar characteristics, such as levels of expertise, communication methods, frequently used applications, and so forth. Using profiles, you

can make sure that users' devices have the correct settings. You can manage profile settings from the Intellisync Mobile Suite control.

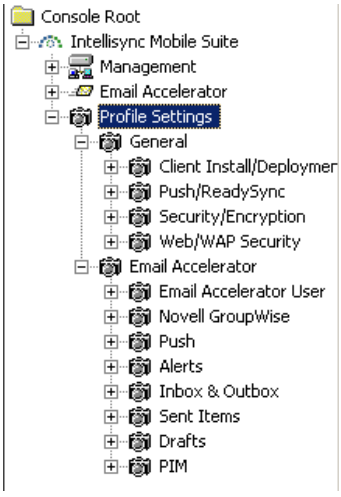
Figure 4-2 *Intellisync Mobile Suite Control: Profile Settings*



When you select *Profile Settings*, an overview of how profile settings work appears in the details pane. When you expand Profile Settings, you see a General control and a control for each Intellisync Mobile Suite product installed on your server. In addition, you might see controls for Email Accelerator.

When you expand the General control, controls for Client Install/Deployment, ReadySync, Security/Encryption, and Web/WAP Security appear. Expand these options to see the associated profile settings.

Figure 4-3 *Profile Settings Hierarchy*

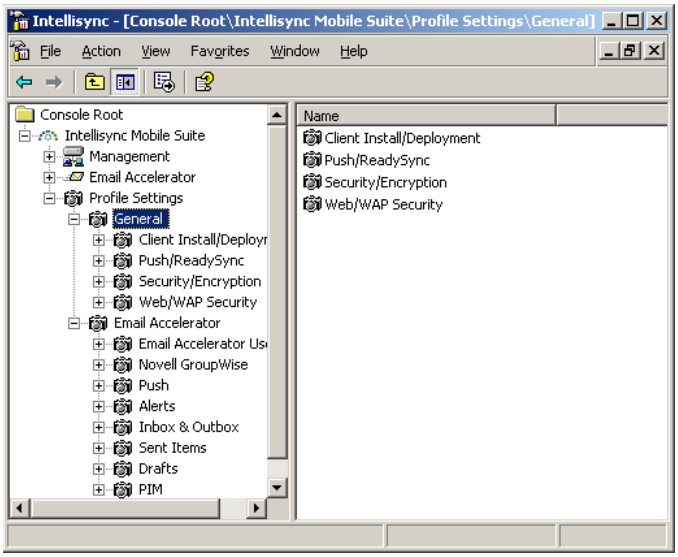


Several profile settings are set up for you in advance, and the default settings explained in this ssection might be sufficient for you. However, if you want to create new profile settings, you can use the default settings as a starting point. For more information, see Section 4.4.1, "Creating Profile Settings," on page 69.

4.2 General Settings

The General control includes settings that are not application specific, but apply to the entire suite. Profile settings for Client Install/Deployment, ReadySync, Security/Encryption, and Web/WAP security are in the General control.

Figure 4-4 *Intellisync Mobile Suite Control: General Settings*

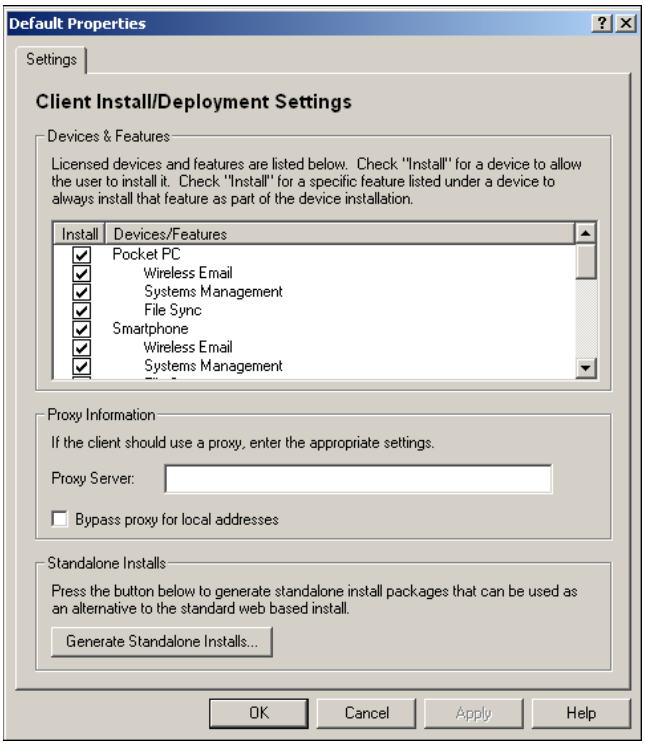


4.2.1 Client Install/Deployment Settings

Use Client Install/Deployment to create a set of Intellisync Mobile Suite applications for various installation and deployment profiles. The applications you specify become part of every device installation for users assigned to a particular profile.

1. From the console tree, click *Intellisync Mobile Suite*.
2. Expand *Profile Settings* > *General*, then click *Client Install/Deployment*.
3. In the details pane, select the profile you want to view.
4. Click *Action* > *Properties*.

5 On the Settings page, specify the applications you want to install for each user in this profile. Complete the proxy information if necessary.



6 Click *Generate Standalone Install* when you are ready to complete an installation package to distribute to your users. With a standalone installation, users are not required to use the Web site to install software.

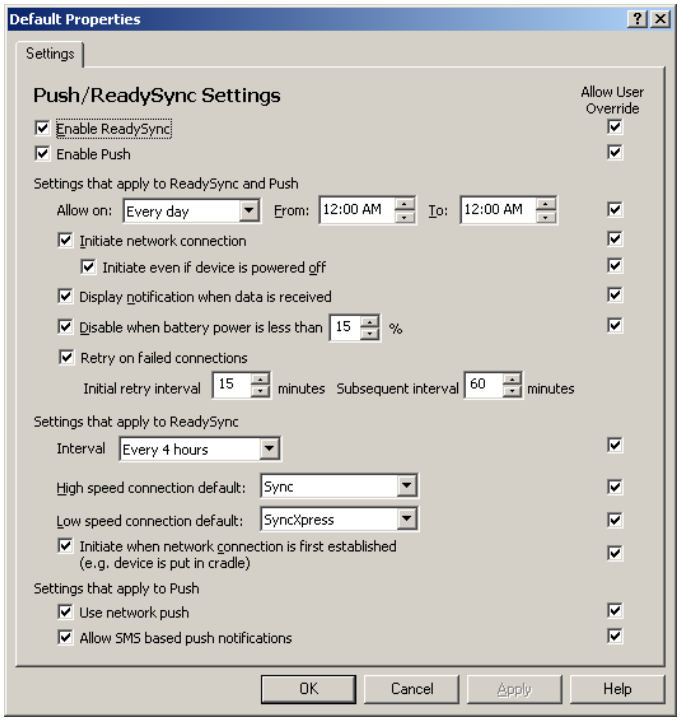
For more information on creating and assigning these profiles, refer to the online Help.

4.2.2 Push/ReadySync Settings

Use this panel to create and edit profile settings for Push (both network push and SMS push) and ReadySync.

ReadySync is a feature that allows you to synchronize data automatically at intervals you define. Push is a feature that allows users to receive e-mail messages on their devices soon after the e-mail arrives on the server. The available settings are similar to those shown in the following figure:

Figure 4-5 *Push/ReadySync Settings*



You can create different profile settings by varying the values for the options. The list of available Push/ReadySync settings includes the following:

- **Enable ReadySync:** Select or deselect the check box to enable or disable the feature.
- **Enable Push:** Select or deselect the check box to enable or disable the feature.

NOTE: You can use ReadySync and Push together; they are not mutually exclusive.

ReadySync and Push Settings

- **Allow on:** Select whether to allow ReadySync sessions and Push to take place every day or weekdays only.

  From: starttime To: stoptime: Use these fields to set the hour range for Push and ReadySync sessions.

- **Initiate network connection:** If you enable this feature, the device dials for a connection when a ReadySync session begins. Select or deselect the check box to enable or disable the feature.
  - **Initiate even if device is powered off:** This option is only available if you select *Initiate network connection*. This feature allows the device to dial for a connection even if the device is turned off. Select or deselect the check box to enable or disable the feature.
- **Display notification when data is received:** Select this option to have the device notify the user when it receives data.
- **Disable when battery power is less than *x* %:** Select this option to disable the ReadySync feature if battery power falls below a specific percentage.
- **Retry on failed connections:** Select this option to specify the intervals between initial retry and subsequent interval retries. Intervals are measured in minutes.

ReadySync Settings

- **Interval:** Select the frequency with which you want ReadySync to connect. Options range from every 10 minutes to every 24 hours.
- **High-speed connection default:** Select Sync or SyncXpress. With this option, you can define whether Sync or SyncXpress items synchronize when the device has a high-speed connection for a ReadySync session. Sync sessions usually contain items that require more transfer time or faster connections, and therefore are set up for high-speed connections.
- **Low-speed connection default:** Select Sync or SyncXpress from the list. SyncXpress sessions are usually optimized for low-speed connections and therefore contain limited information.
- **Initiate when network connect is first established:** If you enable this option, a ReadySync session begins as soon as the user places the device in the cradle.

Push Settings

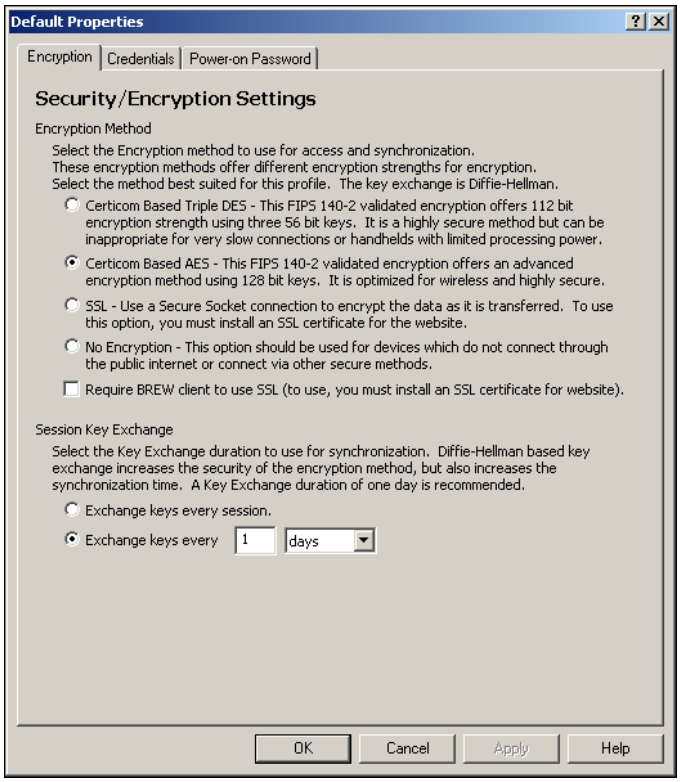
- **Use network push:** Select this option to enable network (IP) push for devices you support.
- **Allow SMS-based push notifications:** Select this option to have SMS-based push send any new e-mail messages to devices upon receipt.

4.2.3 Security/Encryption Settings

With Security/Encryption profile settings, you can define the encryption method you want to use for access to the server and data synchronization. You can also select storage options for the client authentication credentials.

The available settings are similar to those shown in the following example:

Figure 4-6 *Security/Encryption Settings*



Encryption Method

This is the encryption method used to access the server and synchronize information. The methods have varying levels of security, which allows you to select the method best suited for a particular user or group. The key exchange is Diffie-Hellman.

- **Certicom Based Triple DES:** FIPS 140-2 validated encryption. This highly secure method has 112-bit encryption strength using three 56-bit keys. Novell® does not recommend this option for slow connections or devices with limited processing power.
- **Certicom Based AES:** FIPS 140-2 validated encryption. This advanced encryption method uses 128-bit keys. It provides a highly secure connection and is optimized for wireless connectivity.
- **SSL:** Secure Sockets Layer (SSL) encrypts data as it is transferred. Clients and servers authenticate each other and establish a secure link, or "pipe," across the Internet or intranet to protect the information you are transmitting.
- **No Encryption:** Select this option if a device does not connect through the Internet or if the device connects through other secure methods.
- **Require Symbian client to use SSL:** Select this option to require Symbian devices to use SSL. If you enable this option, your Web site must have an SSL certificate.

Session Key Exchange

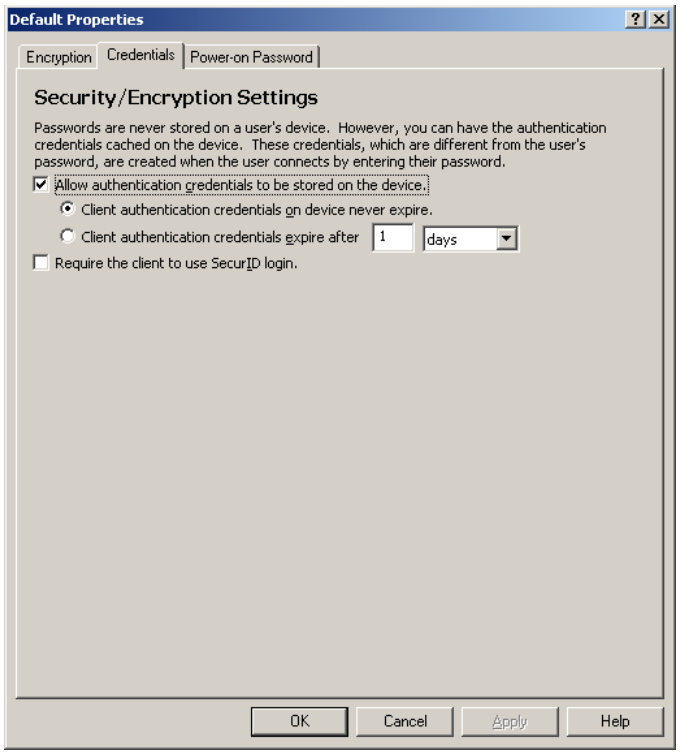
This settings specifies the duration of the key exchange between server and devices. A key exchange based on Diffie-Hellman increases the security of the encryption method, but also increases the synchronization time.

- **Exchange keys every session:** Select this option to exchange keys every session. However, exchanging keys every session slows down the synchronization process.
- **Exchange keys every *x*:** Select this option to exchange keys at the specified interval.

Credentials Management

Intellisync Mobile Suite does not store users' passwords on the device. However, you can use the Password page to have authentication credentials cached on the device. These authentication credentials are created when the user connects by entering a password.

Figure 4-7 *Security/Encryption Settings: Credentials*



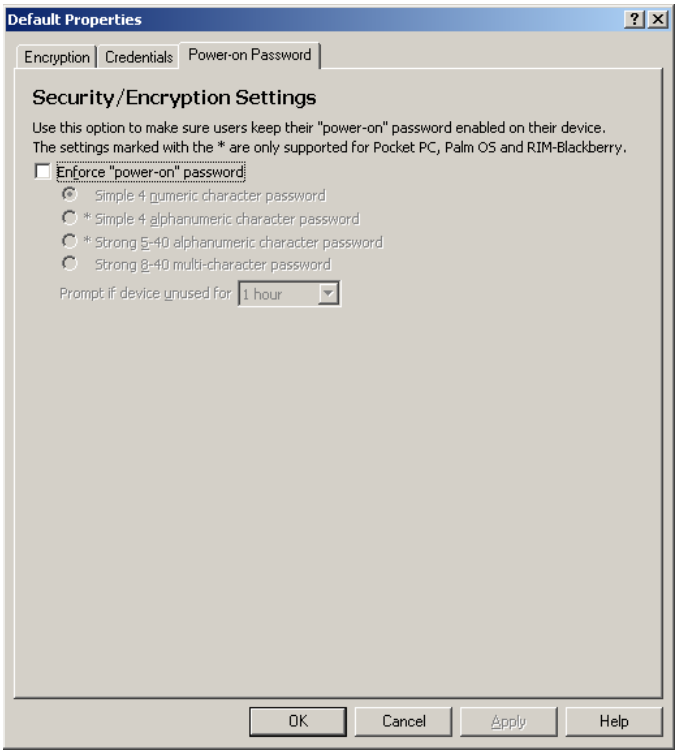
- **Allow authentication credentials to be stored on the device:** Select or deselect the check box to enable or disable this feature.
  - **Client authentication credentials on the device never expire:** This option is only available if you select *Allow authentications credentials to be sotred on the device*. Select this option to indefinitely store authentication credentials on the user's device.
  - **Client authentication credentials expire after *x*:** This option is only available if you select *Allow authentication credentials to be stored on the device*. Select this option to set how long authentication credentials remain valid on the user's device.

NOTE: The *Client authentication credentials expire after x* option is only for Pocket PC and Palm devices.

Power-On Password Management

Use this option to make sure users keep their power-on password enabled on their devices.

Figure 4-8 *Security/Encryption Settings: Power-On Password*

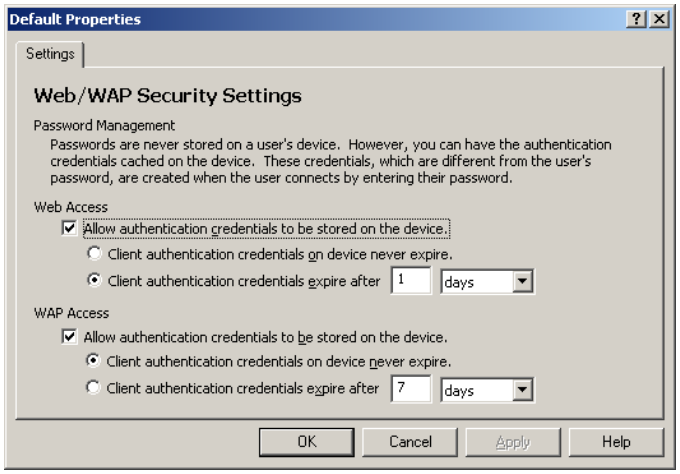


- **Enforce "power-on" password:** If you select this option, you require users to enter a password when the device is powered on. If the user enters an incorrect password, the dialog box does not close and the user cannot exit the screen until the correct password is entered. Select the type of password you want to require.
  - Simple 4-digit password
  - Simple 4-digit alphanumeric password
  - Strong password (more than 4 digits, alpha or numeric, no change in case)
  - Strong alphanumeric password
- **Prompt if device unused for *x*:** Set the amount of inactive time that must pass before the user must enter the password again.

4.2.4 Web/WAP Security Settings

You can create and edit profile settings for Web/WAP security. The available settings are similar to the ones shown in the following figure:

Figure 4-9 *Web/WAP Security Settings*



Intellisync Mobile Suite does not store users' passwords on the device. However, you can use the Web/WAP Security Settings to cache authentication credentials on the device. These authentication credentials are created when the user connects by entering a password.

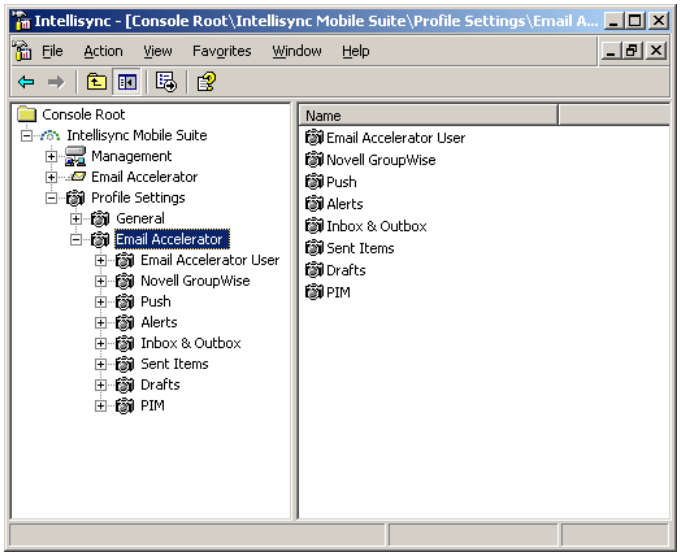
- **Allow authentication credentials to be stored on the device:** Select or deselect the check box to enable or disable this feature.
  - **Client authentication credentials on the device never expire:** This option is only available if you select *Allow authenication credentials to be stored on the device*. Select this option to store authentication credentials on user devices indefinitely.
  - **Client authentication credentials expire after *x*:** This option is only available if you select *Allow authentication credentials to be stored on the device*. Select this option to set how long authentication credentials should remain on the user's device.

You can set these values separately for Web and WAP access.

4.3 Email Accelerator Settings

Email Accelerator controls are included in the Intellisync Mobile Suite control if you have Email Accelerator installed on your server.

Figure 4-10 *Intellisync Mobile Suite Control: Email Accelerator Settings*



You can set profile settings for the following categories.

- Section 4.3.1, “Email Accelerator User Settings,” on page 55
- Section 4.3.2, “Novell GroupWise Settings,” on page 58
- Section 4.3.3, “Push Settings,” on page 62
- Section 4.3.4, “Alerts Settings,” on page 63
- Section 4.3.5, “Inbox and Outbox Settings,” on page 64
- Section 4.3.6, “Sent Items Settings,” on page 65
- Section 4.3.7, “Drafts Settings,” on page 66
- Section 4.3.8, “PIM Settings,” on page 67

4.3.1 Email Accelerator User Settings

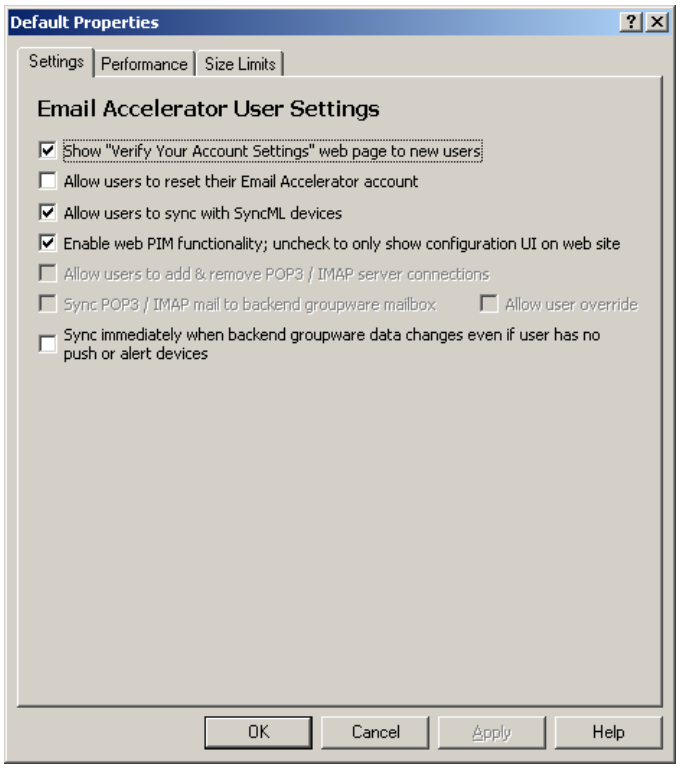
With Email Accelerator User Settings, you can set user options and permissions, and define how long you want to keep items in the Inbox, Sent Items, and Calendar folders. Email Accelerator User Settings are separated into three tabbed pages:

- Settings
- Performance
- Size Limits

Email Accelerator User Settings: Settings Tab

Use the Email Accelerator User Settings page to set user options and permissions for your users.

Figure 4-11 *Email Accelerator User Settings: Settings*



Available options and capabilities include the following.

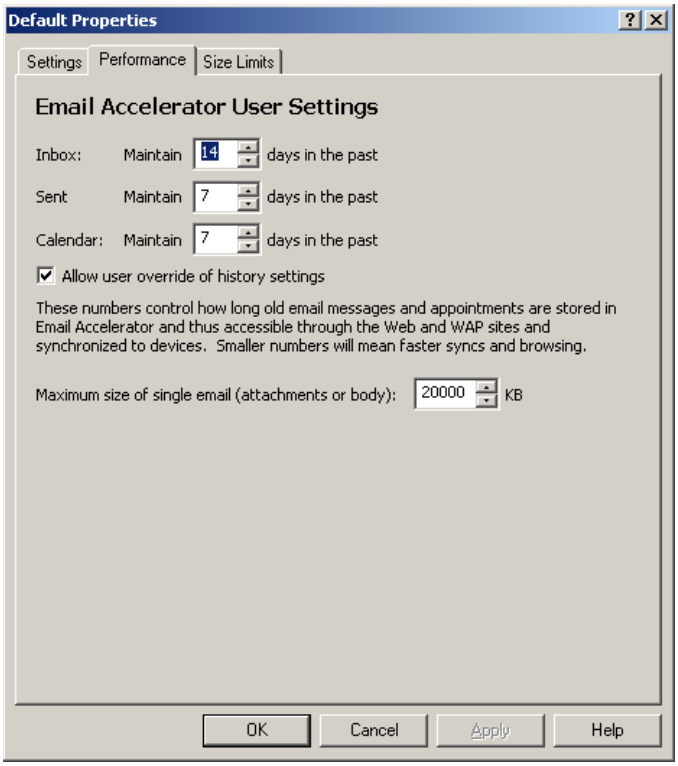
- **Show "Verify Your Account Settings" web page to new users:** This page appears after the user logs in, and includes fields for the user's Exchange mailbox, the user's address, and identifying information. If you enable user discovery, these fields automatically populate. The user can edit the information. Select this option to allow the user to view the page.
- **Allow users to reset their Wireless Email account:** Select this option to enable users to resynchronize their e-mail accounts and devices.
- **Allow users to sync with SyncML devices:** Select this option to allow users to synchronize data to a SyncML device.
- **Enable web PIM functionality; uncheck to only show configuration UI on web site:** Controls whether end users can see and use full Web client functionality. If you deselect this option, users can only use the Web site to set up devices.
- **Allow users to add and remove POP3/IMAP server connection:** Grants users permission to add connections for POP3/IMAP map without an administrator's assistance. This setting is disabled by default, and not part of GroupWise Mobile Server.
- **Sync POP3/IMAP mail to backend groupware mailbox:** Allows users to synchronize mail from other sources with their corporate GroupWise account. This setting is disabled by default, and not part of GroupWise Mobile Server.

- **Sync immediately when backend groupware data changes even if user has no push or alert devices:** Allows for almost immediate synchronization between the mail server and the Intellisync Mobile Suite server for users who do not have push or alert devices. Setting this option allows for immediate import of e-mailed itineraries. For optimum system performance Novell recommends that you do not use this option.

Email Accelerator User Settings: Performance Tab

With Email Accelerator User Settings, you can control how long items should remain in a user's Inbox, Sent Items, and Calendar folders. In addition, you can control whether users can override these settings.

Figure 4-12 *Email Accelerator User Settings: Performance*



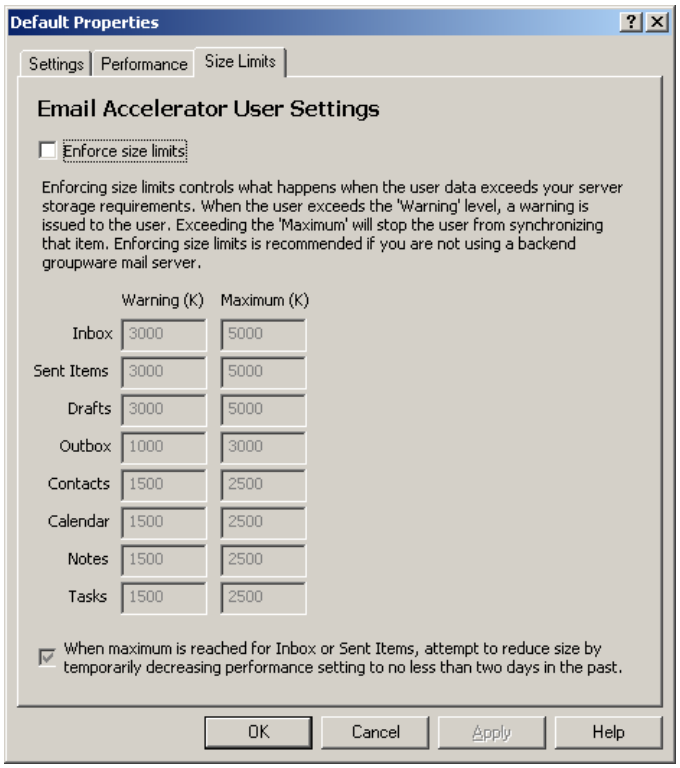
You can set the length of time that appointment information and e-mail messages remain on the device. The list of history settings includes the following:

- **Inbox: Maintain *x* days in the past:** Specify the number of days items should remain in the user's Inbox.
- **Sent Items: Maintain *x* days in the past:** Specify the number of days items should remain in the user's Sent Items folder.
- **Calendar: Maintain *x* days in the past:** Specify the number of days a user's appointments and other calendar items should remain on the device.
- **Allow user override of history settings:** Select this option to allow the user to change any history settings you define.
- **Maximum size of single email:** Specify the maximum size on a single email message including attachments can be, represented in kilo bytes.

Email Accelerator User Settings: Size Limits Tab

Use the Size Limits tab to control what happens when a user's data exceeds the server storage limits.

Figure 4-13 *Wireless Email User Settings: Size Limits*



Available settings include:

- **Enforce size limits:** Select this option to enable the size limits feature. If you deselect this option, other settings on this page become unavailable.
- **Warning:** Set a warning limit for each category. When the user's data exceeds this value, the user receives a warning message.
- **Maximum:** Set a maximum limit for each category. When the user's data exceeds this value, the user cannot synchronize the current item.
- **When maximum size is reached for Inbox or Sent Items:** Select this option to temporarily decrease performance settings (that is, the number of days in the past for which items are stored) when the user reaches the Maximum value for Inbox or Sent folder items.

4.3.2 Novell GroupWise Settings

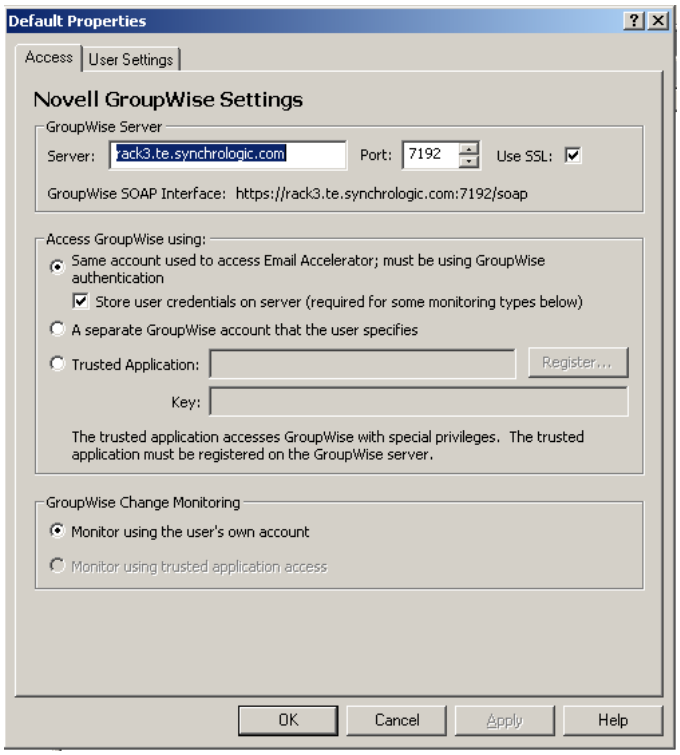
Novell GroupWise profile settings allow you to set values for the server, access methods, user options, and system address book sync sessions. The options are located on the Access tab and the User Settings tab.

For more information on selecting access methods, see Chapter 6, "Authenticating Users," on page 77.

Novell GroupWise Settings: Access Tab

The settings on the Access tab allow you to enter a GroupWise server and select an access method for the user. The available settings are similar to those shown in the following figure:

Figure 4-14 *Novell GroupWise Settings: Access*



GroupWise Server

Use this section to manage the GroupWise server, which has the following components:

- **Server:** Specify the name of the GroupWise server.
- **Port/SSL:** Define the name, port number and SSL state of the GroupWise server, which runs the SOAP listener.

Access GroupWise

Use this section to determine how users should connect to the GroupWise server.

- **Same account used to access Wireless Email; must be using GroupWise authentication:** Select this option if you want users to connect to the GroupWise server using the same GroupWise user account they use for accessing Email Accelerator.
- **A separate GroupWise account that the user specifies:** Select this option if you want users to connect to the GroupWise server using a different GroupWise user account.
- **Trusted Application:** If a trusted application is used, it should be registered on the Novell GroupWise server. You can use `GWTrustedApp.exe` and `GWTApp.dll`, located in the `PIM` directory, to register the Intellisync Mobile Suite trusted application.
- **Key:** If a trusted application is used, specify the application key for the registered trusted application.

For more information, see “Creating a Trusted Application With GroupWise” on page 60.

GroupWise Change Monitoring

Use this section to monitor for Push and Alerts. The choices include the following:

- **Monitor using the user’s own account:** Select this option to use the same GroupWise user account used to access GroupWise.
- **Monitor using trusted application access:** Select this option to use the trusted application used to access GroupWise.

Creating a Trusted Application With GroupWise

When you create a trusted application with GroupWise, you must register GroupWise Mobile Server with GroupWise as a trusted application. When GroupWise Mobile Server has been registered a key is assigned to GroupWise Mobile Server for accessing GroupWise.

If a trusted application is used, it should be registered on the Novell GroupWise server. You can use `GWTrustedApp.exe` and `GWTApp.dll`, located in the `PIM` directory, to register the Intellisync Mobile Suite trusted application.

Before creating the trusted application with GroupWise, you must first have a drive mapped to the location of the primary domain.

1. From the GroupWise Mobile Server machine, open a command window.
2. Change to `C:\Program Files\Intellisync Mobile Suite\PIM`.
3. From `C:\Program Files\Intellisync Mobile Suite\PIM`, enter the following command to register with GroupWise as a trusted application and get the key:

   `GWTrustedApp.exe “pathtoprimarydomain”`

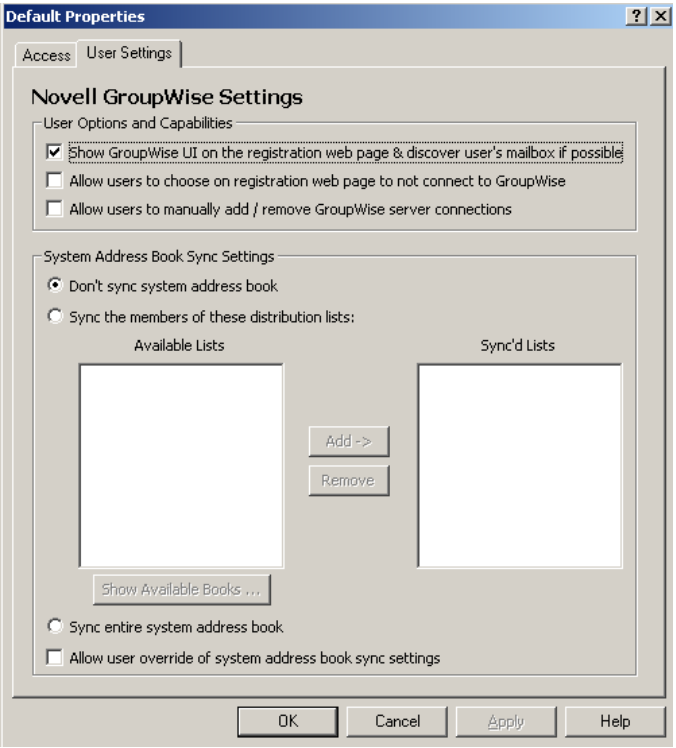
   A message is displayed, stating that trusted application was successfully registered. It displays your trusted application key.
4. Copy the key.
5. From the Intellisync Mobile Suite control console tree, click *Intellisync Mobile Suite*.
6. Expand *Intellisync Mobile Suite* > *Profile Settings* > *Email Accelerator* > *Novell GroupWise*.
7. Select *Default*, then click *Action* > *Properties*.
8. Select *Trusted Application*, then paste the key into the *Key* field.
9. Click *OK*, then specify a valid user ID and password of a user on the POA.
10. Click *OK*.

To apply the settings, reboot the GroupWise Mobile Server machine.

Novell GroupWise Settings: User Settings Tab

The User Settings tab has settings for user options and system address book synchronization. The available settings are similar to those shown in the following figure:

Figure 4-15 *Novell GroupWise Settings: User Settings*



User Options and Capabilities

In this section, you can control whether users can view Novell GroupWise information when registering, set information about Novell GroupWise devices, and synchronize external e-mail. The available options include the following:

- **Show GroupWise UI on the registration web page & discover user's mailbox if possible:** Select this option if you want the user to view the Novell GroupWise user interface when registering. If you select this option and user discovery is enabled, the user's mailbox information populates the appropriate fields.
- **Allow users to choose on registration page to not to connect to GroupWise:** Select this option to give users the choice of having a handheld device that uses Novell GroupWise as the messaging platform.
- **Allow users to manually add / remove GroupWise server connections:** Controls whether users can add or remove handheld devices that are using Novell GroupWise as their messaging platform.

System Address Book Sync Settings

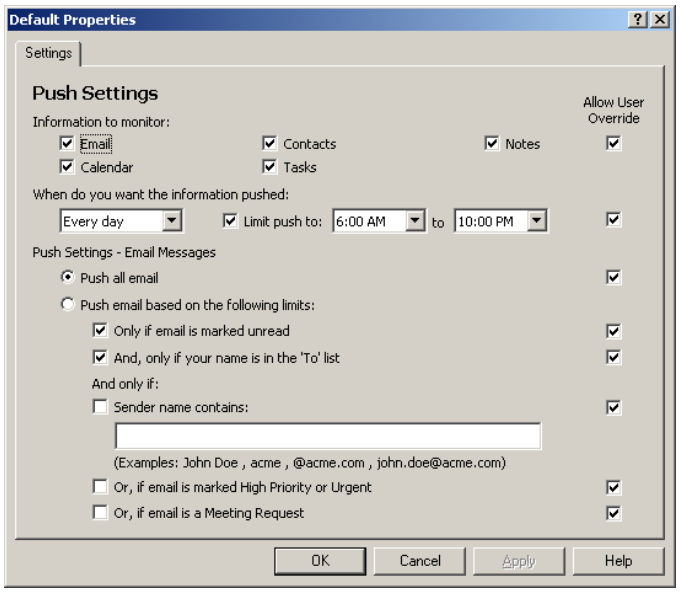
In this section, you can specify databases and database directories for a user's address book. The available options include the following:

- **Don't sync system address book:** Select this option so the system address book does not synchronize.
- **Sync the members of these distribution lists:** Select specific groups you want to synchronize, if any.
- **Sync entire system address book:** Select this option to synchronize the entire system address book.
- **Allow user override of system address book sync settings:** Select this option to allow the user to override the system address book synchronization you define here.

4.3.3 Push Settings

Use the settings on this panel to configure Push values.

Figure 4-16 *Push Settings*



Available options include:

- **Information to monitor:** Select each information type you want to monitor for Push.
  - Email
  - Contacts
  - Notes
  - Calendar
  - Tasks
- **When do you want the information pushed:** Select whether you want to push information every day or only on weekdays.

- **Limit push to *starttime* to *stoptime*:** Use the list to select the time range for which you want users associated with the profile to receive pushes.

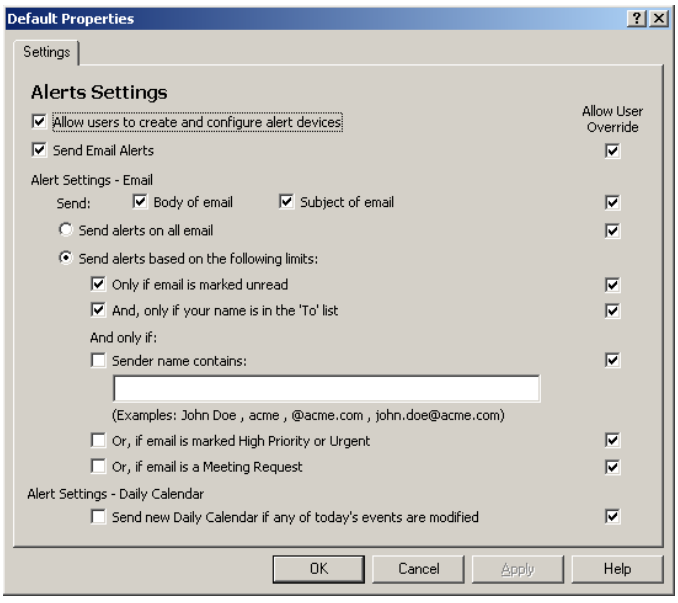
Push Settings - Email Messages

- **Push all email:** Select this option to have all e-mail messages pushed, regardless of other factors.
- **Push email based on the following limits:** By selecting from the following criteria, you can set limits on the types of e-mail messages you want to receive.
  - *Only if email is marked unread*
  - *And, only if your name is in the "To" list*
  - *Sender name contains*
  - *If email is marked High Priority or Urgent*
  - *If email is a Meeting Request*

4.3.4 Alerts Settings

Use the settings on this page to configure Alert values.

Figure 4-17 *Alert Settings*



Available options include:

- **Allow users to create and configure alert devices:** Select this option to give users permission to create and set up alert devices.
- **Send Email Alerts:** Select this option to alert users when they receive an e-mail message.
- **Alert Settings – Email Alerts:** Select whether users should receive the body of an e-mail or only the subject in the alert.

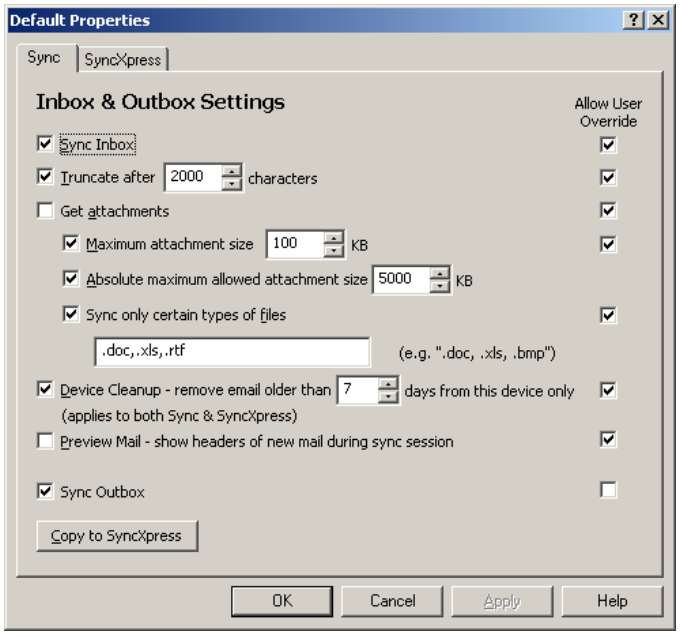
- **Send alerts on all email.** Select this option to send alerts upon arrival of all e-mail messages, regardless of other factors.
- **Send alerts based on the following limits:** By selecting from the following criteria, you can set limits on the types of e-mail to generate alerts.
  - *Only if email is marked unread*
  - *And, only if your name is in the "To" list*
  - *Sender name contains*
  - *If email is marked High Priority or Urgent*
  - *If email is a Meeting Request*
- **Send new Daily Calendar if any of today's events are modified:** This option allows users assigned to this profile to receive a new calendar if any of the day's events are modified.

4.3.5 Inbox and Outbox Settings

You can create profile settings for the user's Inbox and Outbox by setting combinations of values for such options as message truncation, attachment limitations, old mail deletion, and preview. There are two tabs for settings for the Inbox and Outbox: the *Sync* tab and the *SyncXpress* tab. The options on both tabs are identical, and the values for both Sync and SyncXpress can be set the same way. However, Sync settings are usually for a more comprehensive synchronization session. Sync sessions usually include items that require more transfer time or a faster connection. SyncXpress settings are usually for scaled-down, wireless data exchange sessions.

The available settings for both Sync and SyncXpress sessions are similar to those shown in the following figure:

Figure 4-18 *Inbox and Outbox Settings*



Available settings include:

- **Sync Inbox:** Select whether to synchronize Inbox information.

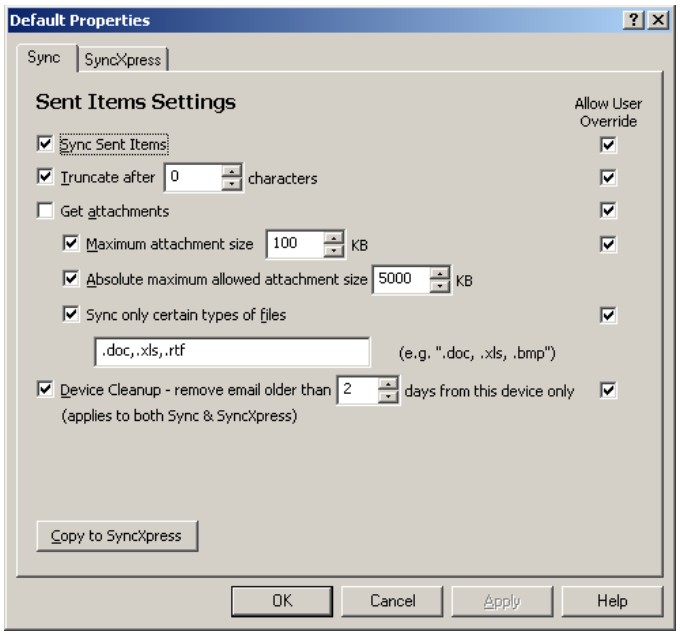
- **Truncate after *x* characters:** You can specify the number of characters, counting left to right, to allow before truncating an Inbox message.
- **Get attachments:** Select this option to allow the device to receive file attachments in e-mail.
  - **Maximum attachment size (in KB):** To conserve space and minimize download times, specify a size limit (in kilobytes) for the attachments.
  - **Absolute maximum attachment size (in KB):** Specify a size limit (in kilobytes) for the largest attachment you can send to the device. Even if the user requests the attachment (in Preview Mail), the file does not download if it exceeds the value you set here.
  - **Sync only certain types of files:** You have the option to synchronize only attachments of a certain file type (such as `.doc`, `.xls`, and so forth).
- **Device Cleanup – remove e-mail older than *x* days from this device only (applies to both Sync & SyncXpress):** Specify the number of days to keep e-mail on the user's device.
- **Preview Mail – show headers of new mail during sync session:** Use this option to enable or disable the Preview Mail feature, which allows users to decide whether they want to download each e-mail message based on the message header.
- **Sync Outbox:** Select this option to synchronize Outbox information.
- **Copy to SyncXpress/Copy to Sync:** If you set values on the Sync tab and want to apply the same settings to the *SyncXpress* tab, click *Copy to SyncXpress*. If you set values on the *SyncXpress* tab and want to apply the same settings to the *Sync* tab, click *Copy to Sync*.
- **Allow User Override:** For each option on this page, you can control whether users can override the values you set.

4.3.6 Sent Items Settings

Profile settings for a user's Sent items include truncation, attachment options, and e-mail deletion. There are two tabs for settings for Sent items, the *Sync* tab and the *SyncXpress* tab. The options on both tabs are identical, and the values for both Sync and SyncXpress can be set the same way. However, Sync settings are usually for a more comprehensive synchronization session. Sync sessions usually include items that require more transfer time or a faster connection. SyncXpress settings are usually for scaled-down, wireless data exchange sessions.

Settings for both Sync and SyncXpress sessions are similar to those shown in the following figure.

Figure 4-19 *Sent Items Settings*



The following settings are available:

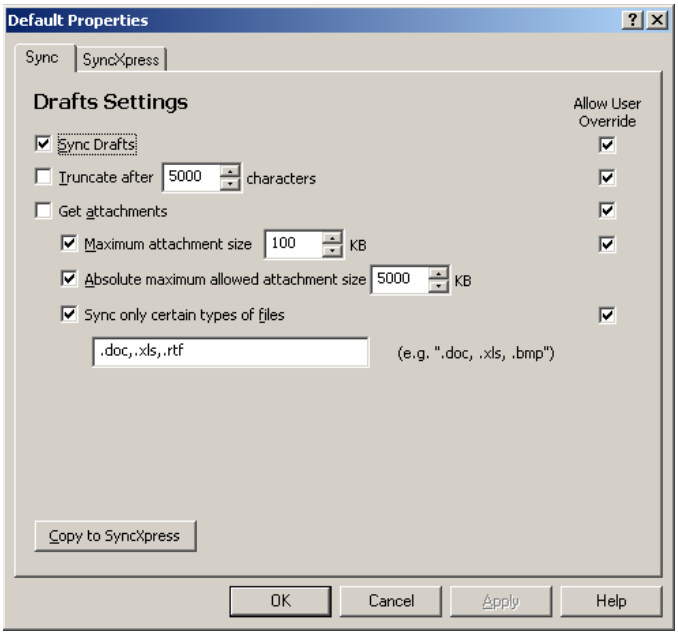
- **Sync Sent Items:** Select this option to synchronize Sent items.
- **Truncate after *x* characters:** You can specify the number of characters, counting left to right, to allow before truncating a sent message.
- **Get attachments:** Select this option to allow the device to receive file attachments in e-mail.
  - **Maximum attachment size (in KB):** To conserve space and minimize download times specify a size limit (in kilobytes) for the attachments.
  - **Absolute maximum attachment size (in KB):** Specify a size limit (in kilobytes) for the largest attachment you can send to the device. Even if the user requests the attachment (in Preview Mail), the attachment is not sent if it exceeds the value you set here.
  - **Sync only certain types of files:** You have the option to synchronize only attachments of a certain file type (such as `.doc`, `.xls`, and so forth).
- **Device Cleanup – remove e-mail older than *x* days from this device only (applies to both Sync & SyncXpress):** Specify the number of days to keep sent e-mail on the user's device.
- **Copy to SyncXpress/Copy to Sync:** If you set values on the Sync tab and want to apply the same settings to the *SyncXpress* tab, click *Copy to SyncXpress*. If you set values on the *SyncXpress* tab and want to apply the same settings to the *Sync* tab, click *Copy to Sync*.

4.3.7 Drafts Settings

Profile settings for draft messages are similar to the Inbox and Sent Items settings, and include truncation and attachment options. There are two tabs for setting the Drafts Settings: *Sync* and *SyncXpress*. The options on both tabs are identical, and the values for both Sync and SyncXpress can be set the same way. However, Sync settings are usually for a more comprehensive synchronization session. Sync sessions usually include items that require more transfer time or a faster connection.

SyncXpress settings are usually for scaled-down, wireless data exchange sessions. The available settings for both Sync and SyncXpress sessions are similar to those shown in the following figure:

Figure 4-20 *Drafts Settings*



The following settings are available:

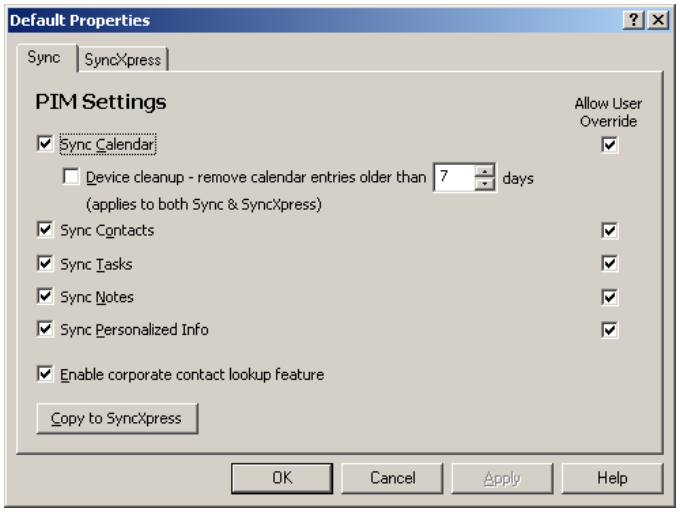
- **Sync Drafts:** Select this option to synchronize Drafts information.
- **Truncate after *x* characters:** You can specify the number of characters, counting left to right, to allow before truncating a draft message.
- **Get attachments:** Select this option if you want the device to receive e-mail attachments.
  - **Maximum attachment size (in KB):** To conserve space and minimize download times specify a size limit (in kilobytes) for the attachments.
  - **Absolute maximum attachment size (in KB):** Specify a size limit (in kilobytes) for the largest attachment you can send to the device. Even if the user requests the attachment (in Preview Mail), it is not sent if it exceeds the value you set here.
  - **Sync only certain types of files:** You have the option to synchronize only attachments of a certain file type (such as `.doc`, `.xls`, and so forth).
- **Copy to SyncXpress/Copy to Sync:** If you set values on the *Sync* tab and want to apply the same settings to the *SyncXpress* tab, click *Copy to SyncXpress*. If you set values on the *SyncXpress* tab and want to apply the same settings to the *Sync* tab, click *Copy to Sync*.

4.3.8 PIM Settings

Profile settings for PIM include Calendar, Contacts, Tasks, Notes, and Personalized Information options. There are two tabs for setting PIM settings, *Sync* and *SyncXpress*. The options on both tabs are identical, and the values for both Sync and SyncXpress can be set the same way. However, Sync settings are usually for a more comprehensive synchronization session. Sync sessions usually include items that require more transfer time or a faster connection. SyncXpress settings are usually for scaled down, wireless data exchange sessions.

The available settings for both Sync and SyncXpress sessions are similar to those shown in the following figure:

Figure 4-21 *PIM Settings*



The following settings are available:

- **Sync Calendar:** Select this option to synchronize users' Calendar information.
- **Device Cleanup – remove calendar entries older than "x" days (applies to both Sync & SyncXpress):** Specify the number of days to store calendar entries on users' devices.
- **Sync Contacts:** Select this option to synchronize users' Contacts.
- **Sync Tasks:** Select this option to synchronize users' Tasks.
- **Sync Notes:** Select this option to synchronize users' Notes.
- **Sync Personalized Info:** Select this option to synchronize users' personalized information.
- **Enable corporate contact lookup feature:** The corporate contact lookup feature might be appropriate for very large companies with too many employees to synchronize to the device. When you enable this feature, users can browse to access a contact lookup page to view the information they need.
- **Copy to SyncXpress/Copy to Sync:** If you set values on the *Sync* tab and want to apply the same settings to the *SyncXpress* tab, click *Copy to SyncXpress*. If you set values on the *SyncXpress* tab and want to apply the same settings to the *Sync* tab, click *Copy to Sync*.

4.4 Working with Profile Settings

A profile setting is a collection of values for settings of an application. A profile can consist of one or more profile settings. Assigning profile settings to users and groups creates profiles for the users and groups.

From the Intellisync Mobile Suite control, you can:

- Section 4.4.1, "Creating Profile Settings," on page 69
- Section 4.4.2, "Using Properties to Change Profile Settings," on page 69
- Section 4.4.3, "Applying Profiles to Users and Groups," on page 69

4.4.1 Creating Profile Settings

GroupWise Mobile Server provides default profile settings for each option. These default settings might be sufficient for your company for certain features. You can also create custom profile settings. When you define a profile setting, you can allow users to override certain values within the profile setting. You can also enable or disable features.

1. From the console tree, expand *Profile Settings*.
2. Navigate to the option beneath the location where you want to create a profile setting, and then select the option.
3. Click *Action* > *Create New Setting*.
4. In the *New Setting Name* field, type a name for the setting.
5. (Optional) From the list, select an existing profile setting where values are similar to the setting you want to create. This decreases the setup time for the new setting.
6. Click *OK*.
7. Select the values for the profile setting.
8. To allow the user to override a value if necessary, select the option to the right of the value.
9. Click *OK*.

4.4.2 Using Properties to Change Profile Settings

After you create a profile setting, you can use the Properties dialog box to add or change information.

1. From the console tree, expand *Profile Settings*.
2. Navigate to the profile setting you want to change.
3. Select the profile.
4. Click *Action* > *Properties*.
5. Complete the changes for the setting.
6. Click *OK*.

4.4.3 Applying Profiles to Users and Groups

You can assign profile settings to individual users and groups. Profile settings you assign to an individual user take precedence over settings you assign to the user as a member of a group. For more information on assigning profile settings to users and groups, see Section 3.2.4, “Assigning or Editing User Profiles,” on page 34 and Section 3.3.4, “Assigning or Editing Group Profiles,” on page 37.

4.4.4 Prioritizing Profile Assignments

Users who are members of more than one group have multiple profiles. You can determine which profile has priority for these users. Profiles you assign directly to a user take priority and override all other profiles assigned through groups.

To prioritize multiple profiles for users who are in multiple groups:

1. From the console tree, select *Profile Settings*.
2. Click *Action > Prioritize Profile Assignments*.
3. In the *Profile Priority* list, select the group name to which you want to assign the highest priority.
4. Click *Move Up* to move the group name to the top of the list.
5. Continue this process using *Move Up* and *Move Down* until the group list is in profile priority order from highest to lowest.
6. Click *OK*.

4.4.5 Deleting Profile Settings

You can delete profile settings you no longer need.

1. From the console tree, expand *Profile Settings*.
2. Navigate to the profile setting you want to delete.
3. Select the profile.
4. Click *Action > Delete*.
5. Click *OK* to confirm the deletion.

NOTE: You cannot delete a profile settings page if it is assigned to a user or group. Assign a new profile settings page to the affected users and groups. You can delete the profiles setting page after it is no longer in use.

Security

5

This section contains an overview of GroupWise® Mobile Server's security capabilities and how you can use these strategies with your corporate security plan.

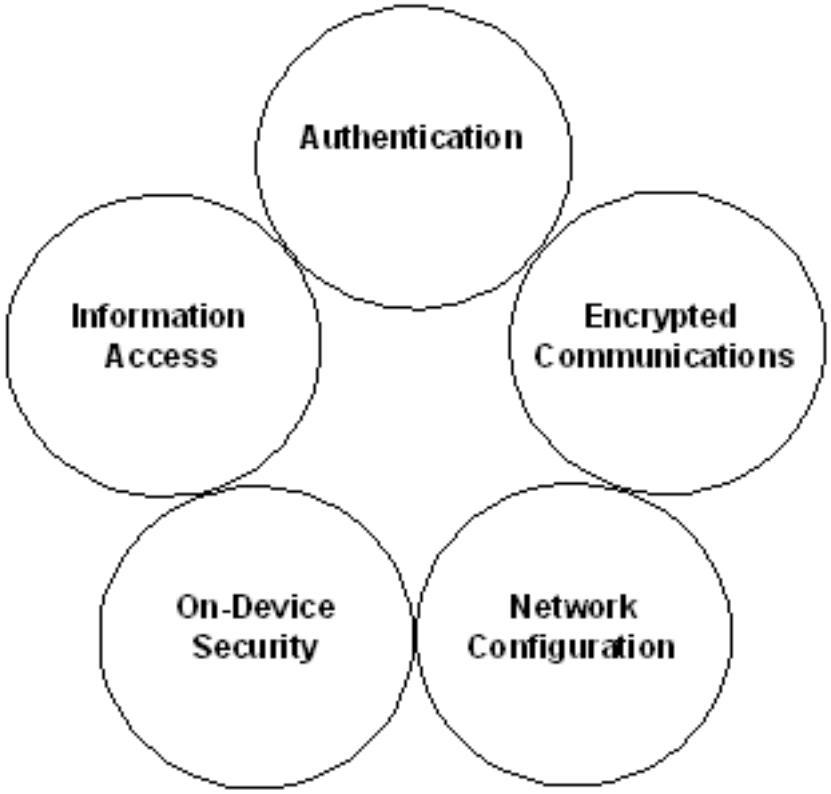
5.1 Overview

Access to corporate information assets using mobile computing devices creates a variety of security challenges. GroupWise Mobile Server provides a solution that securely manages the flow of information among corporate servers and mobile and remote devices including laptops, handheld devices, and smart phones.

GroupWise Mobile Server's security strategy addresses the following areas:

- **Authentication:** Guaranteeing users are authorized to connect.
- **Information Access:** Managing access and authorization to control the information delivered to users.
- **Encrypted Communications:** Securing information in transit to and from the mobile user.
- **On-Device Security:** Protecting information on the device from unauthorized users.
- **Network Configuration:** Locating the Intellisync Mobile Suite server relative to existing firewalls and allowing it to communicate with other servers.

Figure 5-1 *Key Elements of GroupWise Mobile Server's Security Strategy*



Highlights of GroupWise Mobile Server security include the following:

- Section 5.1.1, "New Session Keys," on page 72
- Section 5.1.2, "Encrypting All Data," on page 72
- Section 5.1.3, "Encrypting User Credentials," on page 72
- Section 5.1.4, "Storing User Credentials on the Device," on page 73

5.1.1 New Session Keys

For key exchange, GroupWise Mobile Server uses Diffie-Hellman with elliptical curve strengths of up to 1024-bit RSA. Each new sync session negotiates encryption and randomly generates new session-based keys for added security.

5.1.2 Encrypting All Data

GroupWise Mobile Server encrypts all packets of information, from the first to the last. No "clear text" user data is ever sent between client and server, unless you disable the encryption capabilities.

5.1.3 Encrypting User Credentials

GroupWise Mobile Server always encrypts user credentials as they are passed from client to server for authentication, unless you disable the encryption capabilities.

5.1.4 Storing User Credentials on the Device

GroupWise Mobile Server does not store user passwords on the device. The password is only an element of an encrypted credentials token, and the key is never transmitted or stored on the device. Therefore, you cannot encrypt or decrypt the password on the device. Depending on your configuration, the device can store user credentials and send this information to the server for each sync session.

Maintaining or Expiring User Credentials on the Device

You can keep user credentials on the device indefinitely or have credentials expire after a certain period of time. If user credentials expire, the user must enter the password to continue. Using this option provides better security in case the device is lost or stolen. If credentials never expire, the user must enter the password only when connecting for the first time.

5.2 Authentication

Before a user can reach your corporate computer system, the user's identification must go through an authentication process. The process guarantees that only authorized users are able to gain access to corporate information.

The following authentication approaches are available:

- **GroupWise Authentication.** Authenticate users through the GroupWise server.
- **LDAP Authentication.** Authenticate users through an LDAP source, such as eDirectory™.
- **Intellisync Authentication.** Authenticate users by using a list of users created and maintained through the Intellisync Mobile Suite control.

Your security strategy can incorporate more than one of these approaches. Different users and groups can be authenticated using different authentication methods.

NOTE: This section offers an introduction to authentication as it relates to GroupWise Mobile Server's security strategies. For more information on selecting and implementing authentication strategies, refer to Chapter 6, "Authenticating Users," on page 77.

5.2.1 GroupWise or LDAP Authentication

You might be able to leverage the authentication methods you currently use to avoid duplicate effort in entering and maintaining user lists. For example, if you use Groupwise authentication, users can log on using their existing GroupWise user names and passwords. This approach to authentication can simplify the user experience and maintenance for you.

Changes to the corporate user directory automatically appear in the Intellisync administrative area. This feature eliminates any need for duplicate user administration activity. For example, it eliminates the need to remove an ex-employee from multiple directories.

5.2.2 Intellisync Authentication

Intellisync also offers an internally managed authentication option, referred to as Intellisync Authentication. With this authentication approach, user names and passwords are managed through the Intellisync Mobile Suite control. Some companies prefer this option for administrative reasons.

Even if you select GroupWise authentication, you can use Intellisync Authentication for particular subsets of users. For example, you can use Intellisync Authentication for a temporary workforce, for giving business partners access to limited information, or for testing and evaluation purposes.

5.2.3 Multiple Approaches to Authentication

As mentioned in the previous section, you can authenticate users using different approaches. A combined approach can be useful for testing or for migrating from one authentication approach to another. Intellisync Mobile Suite authenticates each user with only one method, but you can use any method for a given user.

5.2.4 Authentication and User Access

For GroupWise Mobile Server, there are two requirements for allowing a user to connect and access e-mail and PIM data:

- Authentication with GroupWise Mobile Server
- Access to the mail server

Chapter 6, “Authenticating Users,” on page 77 contains more information about authenticating users for all products. Chapter 7, “Granting Access to the Mail Server,” on page 83 includes mail server information and applies only to Email Accelerator.

5.3 Information Access

After the user passes authentication, GroupWise Mobile Server determines the information each user can access. For example, access to e-mail and PIM information is set up using profile settings. However, you can control delivery of software and files using a publish-and-subscribe model. For more information, see Section 5.5.3, “Enabling or Preventing User Credential Storage on the Device,” on page 76

5.3.1 E-Mail and PIM Access

After a user connects and passes authentication, the system determines whether the user can access e-mail and PIM information. Email Accelerator uses profile settings to control how users access the mail server. Depending on the mail server you are using, there are several options for granting access.

Granting users access to the corporate mail server is integral to a successful e-mail and PIM implementation. For more information, see Chapter 7, “Granting Access to the Mail Server,” on page 83.

5.3.2 Automated Discovery For New Users and New Devices

When you enable user discovery, any new user with the Intellisync Mobile Suite client and proper network credentials can access the system. GroupWise Mobile Server automatically assigns the new user to the New User group. As the system administrator, you can routinely review new users and change the assignment to other groups or create individual settings as appropriate.

When you enable device discovery, you can authenticate and add devices not already in the system. If you do not select this option, you can only authenticate devices already in the system.

You can set user and device discovery with the Intellisync Mobile Suite control.

1. From the console tree, select *Intellisync Mobile Suite*.
2. Click *Action* > *Properties*.
3. Click the *Authentication* tab.

5.4 Encrypting Communications

GroupWise Mobile Server includes a client component that communicates with the servers through a communications layer.

The following encryption options are available:

- **Certicom Based Triple DES:** This highly secure option has 112-bit encryption strength using three 56-bit keys. Novell does not recommend this option for slow connections or devices with limited processing power.
- **Certicom Based AES:** This advanced encryption option uses 128-bit keys, which provides a highly secure connection and is optimized for wireless connectivity.
- **SSL:** Secure Sockets Layer (SSL) encrypts data as it is transferred. Clients and servers authenticate each other and establish a secure link, or pipe, across the Internet or intranet to protect the information you are transmitting.
- **No Encryption:** Select this option if a device does not connect through the Internet or if the device connects through other secure methods.

You can set encryption for the server from the Intellisync Mobile Suite control.

1. From the console tree, expand *Profile Settings*.
2. Expand *General Settings*, then select *Security/Encryption Settings*.

5.5 On-Device Security

After information is on the device, you can secure it in a variety of ways. If you require high levels of security, keep in mind that GroupWise Mobile Server is compatible with a variety of third-party products.

On-disk data encryption protects data stored in memory on a server or device. This type of encryption prevents a user from viewing the actual data on the server or device. For handheld devices, GroupWise Mobile Server works with third-party tools such as Certicom's movianCrypt*.

Novell also recommends effective device password management.

5.5.1 Requiring a Password For Power On

1. From the console tree, expand *Profile Settings*.
2. Expand *General Settings*, then select *Security/Encryption Settings*.
3. Click *Action* > *Properties*, then click the *Power-on Password* tab.
4. Select *Enforce power-on password*, then select the password requirements.
5. Click *OK*.

5.5.2 Requiring a Password to Sync

If you cannot store user credentials on the device, you can require the user to enter a password to synchronize.

5.5.3 Enabling or Preventing User Credential Storage on the Device

You can store user credentials on the device or require the user to enter credentials for each synchronization session.

Encrypting User Credentials on the Device

Storing encrypted user credentials on the device is convenient for the user because the device connects automatically several times per day for an “always connected” experience.

Preventing User Credential Storage on the Device

Users must enter a password during each synchronization session if you do not store user credentials on the device. You can set this option using the Intellisync Mobile Suite control.

5.6 Network Configuration

Network configuration is another key element in your corporate security strategy. There are several options for placing GroupWise Mobile Server in your company’s network. For detailed information on installing and configuring the Secure Gateway, refer to “Using the Secure Gateway” in the *GroupWise Mobile Server 7 Installation Guide*.

Authenticating Users

6

This section provides an overview of setting up authentication so user can connect to GroupWise® Mobile Server.

6.1 Overview

All users who connect remotely to GroupWise Mobile Server must be able to authenticate with the server to establish a connection. GroupWise Mobile Server is flexible and you can configure it to work within a wide variety of network environments. As you plan your system implementation, consider how you want to authenticate your users.

By default, GroupWise Mobile Server authenticates a user by how the user enters the system. For example, Novell® GroupWise users who enter the system through auto-discovery are set up for GroupWise authentication.

6.2 User Authentication Options

There are three approaches to authenticating users with the Intellisync Mobile Suite server:

6.2.1 GroupWise Users: GroupWise Authentication

For GroupWise users entering the system through automatic discovery, GroupWise Mobile Server uses GroupWise authentication by default. When a user connects for the first time, GroupWise Mobile Server authenticates the user against the GroupWise Post Office Agent (POA) to automatically create a new user account. With other approaches to authentication, you must configure additional options to grant access to the GroupWise server. If your system includes e-mail and PIM synchronization (covered in Chapter 7, “Granting Access to the Mail Server,” on page 83), using GroupWise authentication simplifies the process of granting mail access.

6.2.2 Intellisync Authentication

With Intellisync Authentication, you are authenticating users against the GroupWise Mobile Server database. To use this approach, you must have a GroupWise Mobile Server account set up for each user before the user attempts to connect for the first time. Otherwise, the user is unable to connect.

You can create user accounts in one of several ways:

- Create the account directly in the Intellisync Mobile Suite control (using the Create User dialog box), see Section 3.2.1, “Adding a New User,” on page 30.
- Import users from a text file, see Section 3.2.2, “Importing Users,” on page 31.
- Import users from a list of LDAP users, see Section 6.4.1, “Creating an AD/LDAP Information Source,” on page 80.

If users need access to a GroupWise POA, you must enter additional information to facilitate that connection. For more information on creating new user accounts and adding connection information, see Section 3.2, “Working With Users,” on page 29.

Intellisync Authentication is a simple, straightforward, and self-contained solution because authentication relies entirely on the GroupWise Mobile Server database, eliminating the need to access other servers during the authentication process.

6.2.3 LDAP Authentication

With LDAP authentication, you are authenticating users against a specific LDAP source.

If your system includes e-mail and PIM synchronization, you must select *Other Option*. In addition, you must map your LDAP fields before connecting.

6.3 Setting Default Authentication For New Users

The authentication approach for a new user is based on the way the user enters the system. The following table show the default authentication approach for users entering the system in various ways.

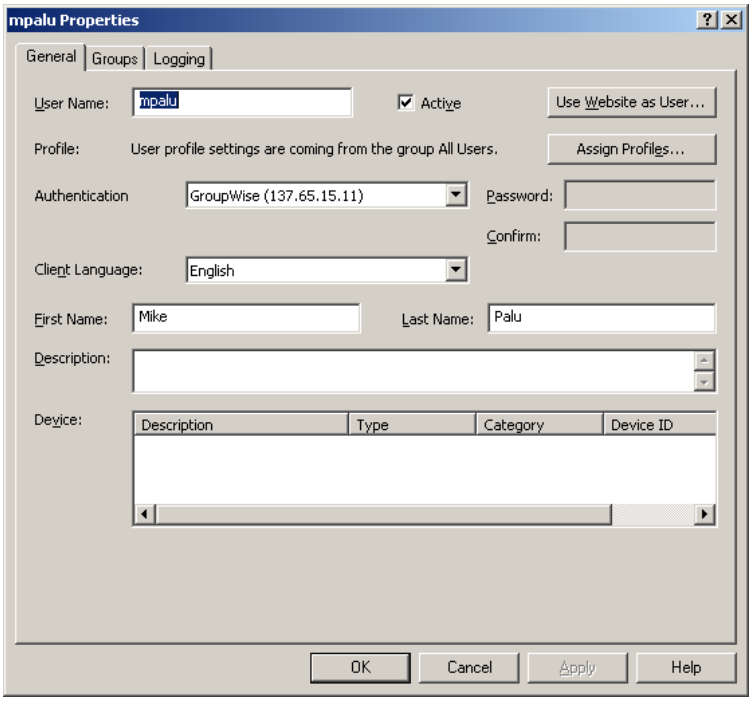
Table 6-1 *Default Authentication Approaches*

User Entry Source	Default Authentication
Auto-discovery: GroupWise	GroupWise
Imported: LDAP	LDAP
Imported: other Directory Service	Specific Directory Service
Manually created: Intellisync Mobile Suite control	Intellisync Authentication **NOTE:** Although Intellisync Authentication is the default, you can select GroupWise authentication when you create the user.

To view or change the authentication approach for a user:

1. From the console tree, click *Management* > *Users*.
2. Select the user you want to change.

3 Click *Action* > *Properties*.



4 In the *Authentication* field, select the authentication type.

5 Click *OK*.

6.4 Selecting Authentication Types

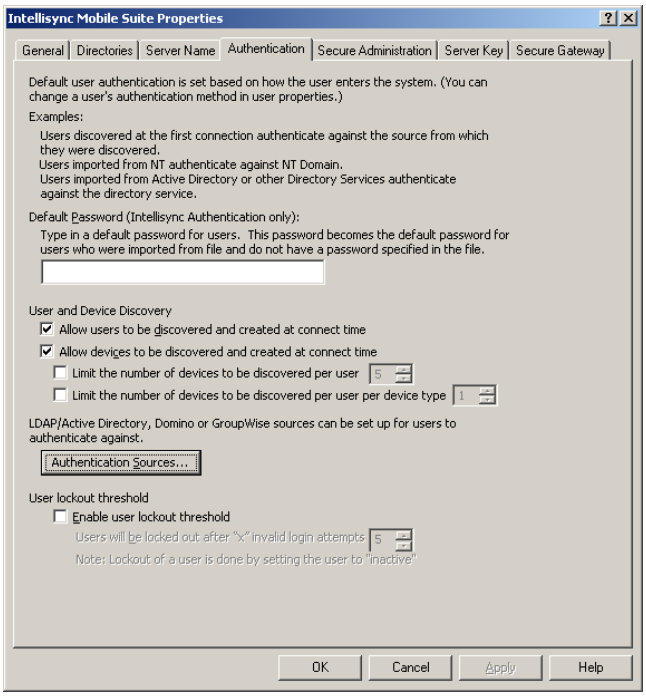
Intellisync Authentication is available as soon as you install GroupWise Mobile Server software. If you want to use GroupWise or LDAP authentication, you must provide more information before you can use these sources.

To add GroupWise or LDAP authentication to your system:

1 From the console tree, select *Intellisync Mobile Suite*.

2 Click *Action* > *Properties*.

3 Click the *Authentication* tab.



4 Click *Authentication Sources*.

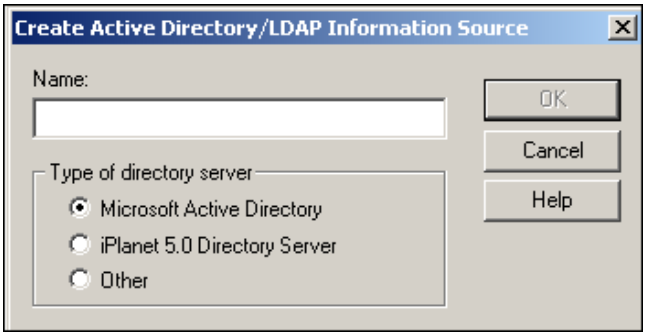
5 Click *Create AD/LDAP* or *Create GroupWise*.

Depending on your selection, continue to Section 6.4.1, “Creating an AD/LDAP Information Source,” on page 80 or Section 6.4.2, “Creating a GroupWise Authentication Source,” on page 82.

6.4.1 Creating an AD/LDAP Information Source

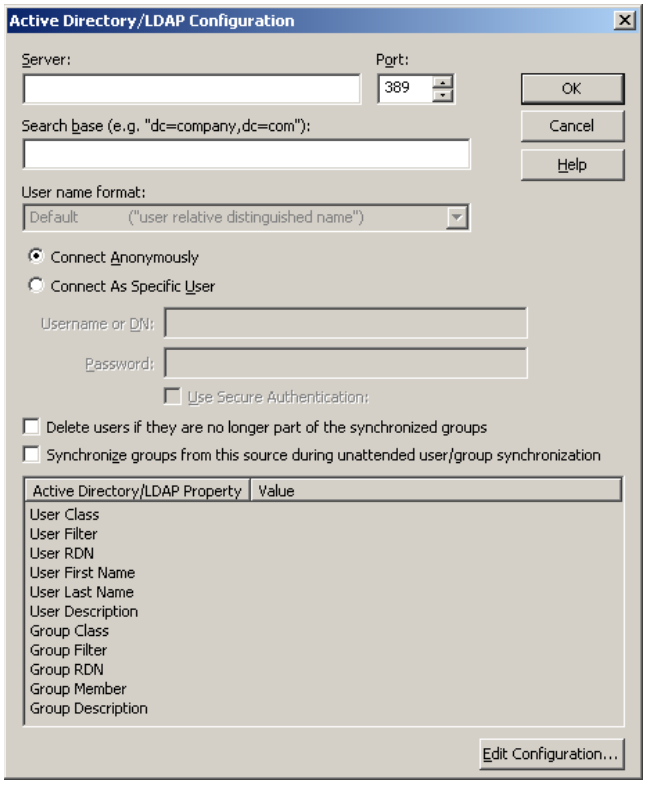
If you choose to create a AD/LDAP information source, you should have a through understanding of LDAP and how it works before proceeding.

1 If you clicked *Create AD/LDAP*, the following dialog box appears.



2 Select *Other*, then click *OK*.

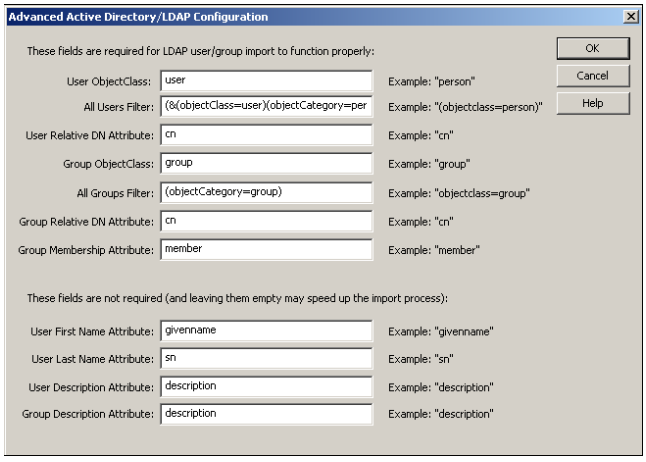
3 Specify the IP address or full DNS hostname, port number, and search base.



4 Select *Connect As Specific User*, then specify the username or DN and password.

5 Click *Edit Configuration*.

The examples provided for most fields work well with eDirectory™.



6 Make the necessary changes, then click *OK*.

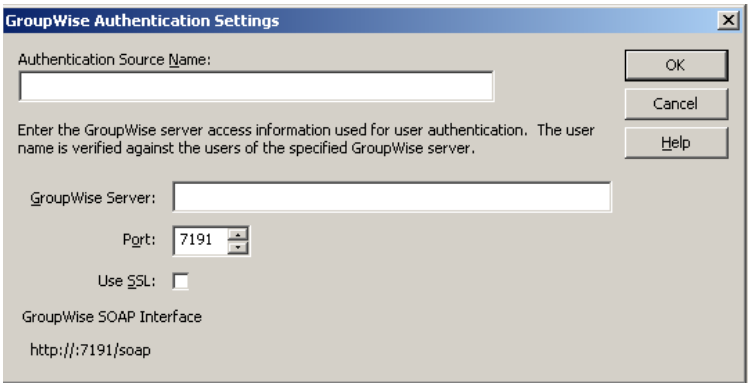
7 Click *OK* to display the Authentication Sources dialog box.

8 Click *Close* to display the Authentication page.

9 Click *OK*.

6.4.2 Creating a GroupWise Authentication Source

1 Click *Create GroupWise*.



2 Specify the authentication source name, GroupWise POA IP address or DNS hostname, SOAP port, and if you want to use SSL.

The default SOAP port is 7191.

3 Click *OK*, then click *Close*.

4 Click *OK*.

Granting Access to the Mail Server

7

This section provides steps to grant user access to the mail server.

7.1 Overview

As covered in Chapter 6, “Authenticating Users,” on page 77, all users who connect remotely to the GroupWise® Mobile Server machine must be set up to authenticate with the server. However, if synchronization for e-mail and PIM is part of your system, you must grant user access to the mail server.

Although authentication is on a user-by-user basis, you can set up access to the mail server through Profile Settings in the Intellisync Mobile Suite control. You can create and apply general specifications for groups of users that share similar characteristics.

Default profile settings are always in place until you make changes. Therefore, you do not need to create or modify profile settings to start using GroupWise Mobile Server.

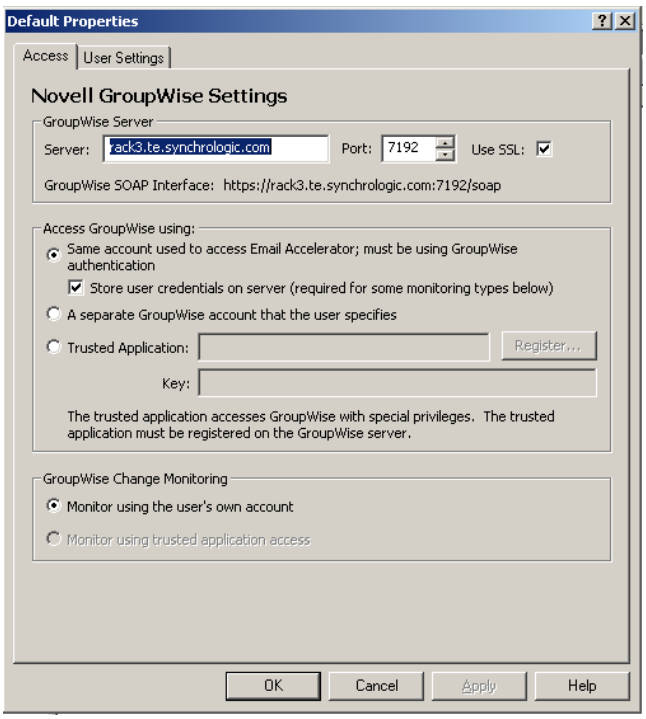
NOTE: You must be familiar with Chapter 4, “Profile Settings,” on page 45 before implementing the procedures in this section.

7.2 Novell GroupWise: Granting Access to the Mail Server

Email Accelerator accesses Novell® GroupWise mailboxes using a GroupWise user account or a trusted application account. To set up access, create, or modify the GroupWise profile settings, and then assign the profile to appropriate groups (or users).

1. From the console tree, expand the following:
   - Intellisync Mobile Suite
   - Profile Settings
   - Email Accelerator Settings
   - Novell GroupWise Settings
2. Select the profile you want to modify.

3 Click *Action* > *Properties*.



4 Make selctions or edit the information, then click *OK*.

For more information, see Chapter 4, “Profile Settings,” on page 45 or online Help.

7.2.1 Accessing GroupWise Using a GroupWise User Account

Authenticating against a user’s GroupWise user account is the most secure approach for authenticating with the GroupWise Mobile Server machine and then accessing the PIM and e-mail server. With this option, the GroupWise Mobile Server machine authenticates users based on the user’s GroupWise account credentials. To connect, the user must provide the GroupWise user name and password.

When a user connects for the first time, the GroupWise Mobile Server machine automatically creates a new user account based on the user’s GroupWise account credentials. Therefore, manually creating a user account using the Intellisync Mobile Suite control is not necessary. This feature, called auto discovery, automatically discovers the user’s mailbox name and GroupWise server and adds the user name to the list in the Intellisync Mobile Suite control. There is no need to manually add information to the properties for the user. Auto discovery is not available with Intellisync Authentication. GroupWise authentication is recommended for most situations.

7.2.2 Accessing GroupWise Using a Trusted Application

If you are using GroupWise Authentication to authenticate users with the GroupWise Mobile Server machine, you can also access the GroupWise server using a trusted application. A trusted application has full access rights to the Novell GroupWise server and every user’s mailbox. The trusted application must be registered on the Novell GroupWise domain with which it is synchronized. When a user requests e-mail, this account has the authority to retrieve the user’s messages. The same

applies when a user requests any other operation on e-mail messages, including deletions. Using Intellisync Mobile Suite as an intermediary is transparent to the user. Using a trusted application to access the mail server access is simple and easy to manage.

For information on how to create a GroupWise Trusted Application with GroupWise and GroupWise Mobile Server, see “Creating a Trusted Application With GroupWise” on page 60.

7.3 Authentication and Access Strategies

When deciding on an authentication and access strategy, it is important to consider your environmental variables. For most situations, Novell recommends that you consider using GroupWise authentication between the user’s handheld device and the GroupWise Mobile Server machine. Then, use the user’s GroupWise user account to gain access to the GroupWise server.

Maintaining GroupWise Mobile Server

8

As a system administrator, you are aware of the importance of backing up your directory structure, files, and data on a regular basis. However, with GroupWise® Mobile Server, it is not necessary because the information is already stored in the GroupWise database. If you do back up GroupWise Mobile Server it becomes very easy for items to become out of synchronization.

If you have purchased the Intellisync File Sync, Data Sync, or System Management components from Nokia*, then you should see their administration guides for information on how to back up these components.

If you need to restore GroupWise Mobile Server, simply reinstall the software and re-prime your database.

Push Rules

A

This section covers the rules that cause a push to happen in the GroupWise Mobile Server system. Pushes can come from either the server to device or from the device to the server. There are three categories that can cause pushes:

- **Insert:** Insert a new item.
- **Update:** A change to an item.
- **Delete:** When an item is deleted.

A.1 Client-Side Pushes

Table A-1 *Inbox and Outbox Client-Side Pushes*

	Inbox			Outbox		
Client-Side Push	Insert	Update	Delete	Insert	Update	Delete
Palm > Server	yes	yes	yes	yes	yes	yes
PPC > Server	yes	yes	yes	yes	yes	yes
Smartphone > Server	yes	yes	yes	yes	yes	yes
Symbian > Server	no	no	no	yes	yes	yes

Table A-2 *Calendar and Contacts Client-Side Pushes*

	Calendar			Contacts		
Client-Side Push	Insert	Update	Delete	Insert	Update	Delete
Palm > Server	no	no	no	no	no	no
PPC > Server	yes	yes	yes	yes	yes	yes
Smartphone > Server	yes	yes	yes	yes	yes	yes
Symbian > Server	no	no	no	yes	yes	yes

Table A-3 *Sent Items and Drafts Client-Side Pushes*

	Sent Items			Drafts		
Client-Side Push	Insert	Update	Delete	Insert	Update	Delete
Palm > Server	yes	yes	yes	yes	yes	yes
PPC > Server	yes	yes	yes	yes	yes	yes
Smartphone > Server	yes	yes	yes	yes	yes	yes

		Sent Items			Drafts	
Symbian > Server	no	no	no	yes	yes	yes

Table A-4 *Tasks Client-Side Pushes*

	Tasks		
Client-Side Push	Insert	Update	Delete
Palm > Server	no	no	no
PPC > Server	yes	yes	yes
Smartphone > Server	yes	yes	yes
Symbian > Server	no	no	no

A.2 Server-Side Pushes

Table A-5 *Inbox and Outbox Server-Side Pushes*

	Inbox			Outbox		
Server-Side Push	Insert	Update	Delete	Insert	Update	Delete
Palm > Server	yes	no	no	no	no	no
PPC > Server	yes	no	no	no	no	no
Smartphone > Server	yes	no	no	no	no	no
Symbian > Server	yes	no	no	no	no	no

Table A-6 *Calendar and Contacts Server-Side Pushes*

	Calendar			Contacts		
Server-Side Push	Insert	Update	Delete	Insert	Update	Delete
Palm > Server	yes	yes	yes	yes	yes	yes
PPC > Server	yes	yes	yes	yes	yes	yes
Smartphone > Server	yes	yes	yes	ye	yes	yes
Symbian > Server	yes	yes	yes	yes	yes	yes

Table A-7 *Sent Items and Drafts Server-Side Pushes*

	Sent Items			Drafts		
Server-Side Push	Insert	Update	Delete	Insert	Update	Delete

		Sent Items			Drafts	
Palm > Server	no	no	no	no	no	no
PPC > Server	no	no	no	no	no	no
Smartphone > Server	no	no	no	no	no	no
Symbian > Server	no	no	no	no	no	no

Table A-8 *Tasks Server-Side Pushes*

	Tasks		
Server-Side Push	Insert	Update	Delete
Palm > Server	no	no	no
PPC > Server	no	no	no
Smartphone > Server	no	no	no
Symbian > Server	no	no	no